Information technologies and information security:

national prospects and european practices



Collective monograph

2026

Co-funded by the European Union

SWorld
Germany

INFORMATION TECHNOLOGIES AND INFORMATION SECURITY: NATIONAL PROSPECTS AND EUROPEAN PRACTICES

Included in International scientometric databases

COLLECTIVE MONOGRAPH

Co-funded by the European Union

ScientificWorld-NetAkhatAV

Karlsruhe 2026

Authors:

Onyshchenko S., Verhal K., Hlushko A., Yanko A., Bilko S., Demydenko M., Derkach T., Desiatko A., Dmytrenko A., Dvirna O., Fesenko A., Fesenko T., Franchuk T., Ivanov Y., Kalashnikova Y., Kapiton A., Klochko L., Kuchma Y., Masliy O., Naboka S., Novosad Z., Raksha V., Toichkina O., Tyshchenko D., Vasyuta V., Vasyuta V., Zhyvylo Y., Zakharov R.

Reviewers:

Homeniuk Serhii, Doctor of Technical Sciences, Professor, Dean of the Faculty of Mathematics, Zaporizhzhia National University, Zaporizhzhia, Ukraine

Mykus Serhii, Doctor of Technical Sciences, Professor, Deputy Head of the Institute of Information and Communication Technologies and Cyber Defense, National Defense University of Ukraine, Kyiv, Ukraine

Pantea Mioara-Florina, PhD in Economics, Associate Professor, Dean of the Faculty of Economic Sciences, Aurel Vlaicu University of Arad, Arad, Romania

Varnalii Zakharii, Doctor of Economics, Professor, Department of Finance, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Yarovenko Hanna, Doctor of Economics, Visiting Professor, Department of Computer Science and Engineering, Universidad Carlos III de Madrid, Madrid, Spain

Information technologies and information security: national prospects and European practices : collective monograph / ed. by S. Onyshchenko, 2026. 401 p.

The monograph was prepared within the framework of the Erasmus+ Jean Monnet project “European Experience of Information Security and Information Protection Systems under Present Large-Scale Cyberattacks” (No. 101127542 – EEISIPS). The collective monograph addresses current issues of digital transformation, cybersecurity, and information protection in Ukraine, taking into account the experience of the European Union countries. It examines issues related to artificial intelligence, the protection of critical information infrastructure, cyber risk management, countering hybrid threats, the development of digital competencies, and the digitalization of higher education. The possibilities of adapting European approaches and practices to strengthen Ukraine’s digital resilience and support its post-war recovery are substantiated.

ISBN 978-3-98924-175-6

DOI: 10.30890/978-3-98924-175-6.2026

Published by:

ScientificWorld-NetAkhatAV
Lußstr. 13
76227 Karlsruhe, Germany
e-mail: *editor@promonograph.org*
site: https://de.promonograph.org

© Collective of Authors, 2026

CONTENTS

INTRODUCTION 4
CHAPTER 1. DIGITAL TRANSFORMATION OF THE ECONOMY AND SOCIETY: CHALLENGES FOR UKRAINE AND THE EXPERIENCE OF EU COUNTRIES 8
1.1. Digital transformation of the economy and society based on artificial intelligence and cybersecurity 8
1.2. Responsible Implementation of Artificial Intelligence as a Factor of Digital Transformation of the Ukrainian Economy: European Experience and Prospects for Adaptation 41
1.3. Institutional and regulatory frameworks for information security in the context of digital transformation: the experience of European Union countries and the adaptation of Ukrainian legislation 74
CHAPTER 2. CYBERSECURITY AND INFORMATION PROTECTION UNDER HYBRID THREATS: NATIONAL AND EUROPEAN APPROACHES 111
2.1. Distributed Cyber Sensors for Monitoring Threats to Ukraine's Critical Information Infrastructure 111
2.2. European Regulation of the Development and Deployment of Intrusion Detection and Prevention Systems 145
2.3. Strategy for Countering Hybrid Threats in the Digital Sphere: An Analysis of National and European Practices 168
2.4. Protection of Critical Information Infrastructure and Cyber Risk Management: European Practices and Opportunities for Implementation in Ukraine 186
CHAPTER 3. HUMAN CAPITAL IN THE IT AND CYBERSECURITY SECTOR: EDUCATION, WORKFORCE TRAINING, AND DIGITAL COMPETENCE DEVELOPMENT 224
3.1. Digital Technologies for Managing University Research Activities: European Experience and Prospects for Implementation in Ukraine 224
3.2. Digitalization of higher education: integration of information quality systems and information security standards 242
3.3. Mathematical model of expert data analysis in information and analytical systems 298
CHAPTER 4. DIGITAL RESILIENCE AND POST-WAR RECOVERY OF UKRAINE: THE ROLE OF INFORMATION TECHNOLOGIES AND CYBERSECURITY 326
4.1. DIGITAL TWIN Technologies in the Digital Transformation of the European Union Economy: Experience for Ukraine and the Concept of a Projective Digital Twin 326
4.2. Unified Digital Platform for Suburban and Intercity Bus Transport Based on the PSO Model with Integrated Anti-Corruption Mechanisms 358
4.3. Institutional architecture of information and cybersecurity as the basis of digital resilience of Ukraine: European experience and directions of implementation 370

INTRODUCTION

Digital transformation is one of the key processes of modern economic and social development. It affects almost all areas of human activity, government, and business. The rapid development of information technologies, artificial intelligence, cloud computing, digital platforms, Internet of Things technologies, automation, and digital twins creates new opportunities to improve the efficiency of economic processes, promote innovation, improve public administration, and ensure the quality of public services. At the same time, the increasing level of digitalization leads to greater dependence of the economy and society on information systems and digital infrastructure. This makes information security, cyber resilience, and data protection increasingly important.

An important factor in modern digital transformation is the rapid development of artificial intelligence technologies. The use of artificial intelligence systems creates new opportunities for analysing large amounts of data, automating management and production processes, forecasting, supporting decision-making, developing education and science. At the same time, the widespread use of these technologies creates new risks related to data protection, cybersecurity, algorithm transparency, information reliability, responsibility for decisions, and the potential use of artificial intelligence to carry out cyberattacks. Therefore, the responsible and secure implementation of artificial intelligence should be considered an integral part of digital transformation.

The European Union is developing a comprehensive approach to the digital environment by combining technological innovation with requirements for security, protection of human rights, reliability of digital systems, and responsible use of new technologies. The development of European legislation in the areas of cybersecurity, personal data protection, digital services, artificial intelligence, and the resilience of critical entities creates a new regulatory framework for the functioning of the digital economy. Studying this experience is particularly important for Ukraine in the context of its European integration and the need to further bring national digital and security policies closer to European approaches.

Another important aspect of digital transformation is the development of human capital. The effective implementation of information technologies and cybersecurity systems requires specialists who can not only use modern digital tools but also understand the principles of their operation, assess risks, and ensure the secure use of information systems. In this context, digital competences, modernization of higher education, development of IT and cybersecurity education, digitalization of research management, and integration of information security standards into educational and management processes are of particular importance.

A separate dimension of the problem is ensuring Ukraine's digital resilience during the war and future post-war recovery. Digital technologies can become one of the key tools for rebuilding the economy, modernizing infrastructure, improving the efficiency of public administration, and developing transport, industry, and other sectors. The use of digital twins, intelligent data analysis, automation, and digital platforms creates conditions for a more efficient, transparent, and resilient economic system. At the same time, digital recovery should take into account cybersecurity requirements, information protection, and the continuity of critical systems.

These issues are particularly relevant for Ukraine, which is carrying out large-scale digital transformation while facing unprecedented hybrid and cyber threats. The full-scale war has demonstrated the critical importance of reliable digital infrastructure, the continuity of information systems, the protection of critical information infrastructure, and the ability of government, educational, and business institutions to withstand cyber incidents. Under these conditions, information technologies and information security are no longer separate areas of development. Instead, they form an interconnected foundation of the digital resilience of the state and society.

The relevance of this research is determined by the need for a comprehensive understanding of the relationship between the development of information technologies, the digital transformation of the economy and society, artificial intelligence, and information security. Particular attention should be paid to the analysis of European experience, current regulatory approaches, and technological practices in order to identify opportunities for their adaptation to Ukrainian conditions. This approach makes it possible to consider information security not only as a means

of responding to cyber threats but also as one of the fundamental conditions for sustainable digital development, economic competitiveness, and social resilience.

The monograph Information Technologies and Information Security: National Perspectives and European Experience is aimed at a comprehensive study of current trends in the development of the digital economy and society, artificial intelligence technologies, information security and cyber protection, the development of digital competences and human capital, as well as the use of digital technologies to ensure Ukraine's resilience and recovery. The study combines theoretical, technological, management, and practical aspects of these issues, making it possible to develop a comprehensive view of current challenges and prospects for digital development. The results of the research may be useful for researchers, academic staff, higher education students, specialists in information technologies, cybersecurity and digital transformation, representatives of public authorities and local governments, as well as practitioners interested in developing a secure and resilient digital environment in Ukraine.

The monograph was prepared within the framework of the Jean Monnet Module project European Experience of Information Security and Information Protection Systems under Present Large-scale Cyber-attacks Conditions (101127542–EEISIPS–ERASMUS-JMO-2023-HEI-TCH-RSCH, 2023–2026), implemented by the Educational and Research Institute of Finance, Economics, Management and Law and the Educational and Research Institute of Information Technologies and Robotics of National University “Yuri Kondratyuk Poltava Polytechnic”.

Funded by the European Union. The views and opinions expressed are, however, those of the authors only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.*The monograph “Information Technologies and Information Security: National Prospects and European Practices” was prepared within the framework of the Jean Monnet Module “European Experience of Information Security and Information Protection Systems under Present Large-scale Cyber-attacks Conditions” (101127542–EEISIPS–ERASMUS-JMO-2023-HEI-TCH-RSCH, 2023–2026), implemented by the*

Educational and Research Institute of Finance, Economics, Management and Law and the Educational and Research Institute of Information Technologies and Robotics of National University "Yuri Kondratyuk Poltava Polytechnic".

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

.

CHAPTER 1. DIGITAL TRANSFORMATION OF THE ECONOMY AND SOCIETY: CHALLENGES FOR UKRAINE AND THE EXPERIENCE OF EU COUNTRIES

1.1. Digital transformation of the economy and society based on artificial intelligence and cybersecurity

Kseniia VERHAL,
National University "Yuri Kondratyuk Poltava Polytechnic"

The rapid development of digital technologies over the past decades has significantly changed the way the modern economy and society function. It has transformed the ways of production, management, communication, and the creation of economic value. The spread of cloud computing, big data, the Internet of Things, digital platforms, and other technologies has created a technological basis for moving from fragmented digitalization of individual processes to comprehensive changes in the activities of businesses, public institutions, and social organizations.

The growing integration of artificial intelligence (AI) into the economy and society is confirmed by the increasing use of AI technologies in the countries of the European Union. According to Eurostat, the statistical office of the European Union, in 2025, AI technologies were used by 20.0% of EU enterprises with at least 10 employees. This was 6.5 percentage points higher than in 2024 and 2.5 times higher than the corresponding indicator in 2023 (Eurostat, 2024; Eurostat, 2025; Eurostat, 2026). At the same time, there is still a significant difference between enterprises of different sizes. In 2025, large enterprises showed a much higher level of AI adoption, reaching 55.03% (Eurostat. Usage of AI technologies increasing in EU enterprises, 2025) (Fig. 1.1).

Differences were also observed between the Member States of the European Union. The highest levels of AI use were recorded in Denmark (42.03%), Finland (37.82%), and Sweden (35.04%). The lowest levels were reported in Romania (5.21%) and Poland (8.36%).

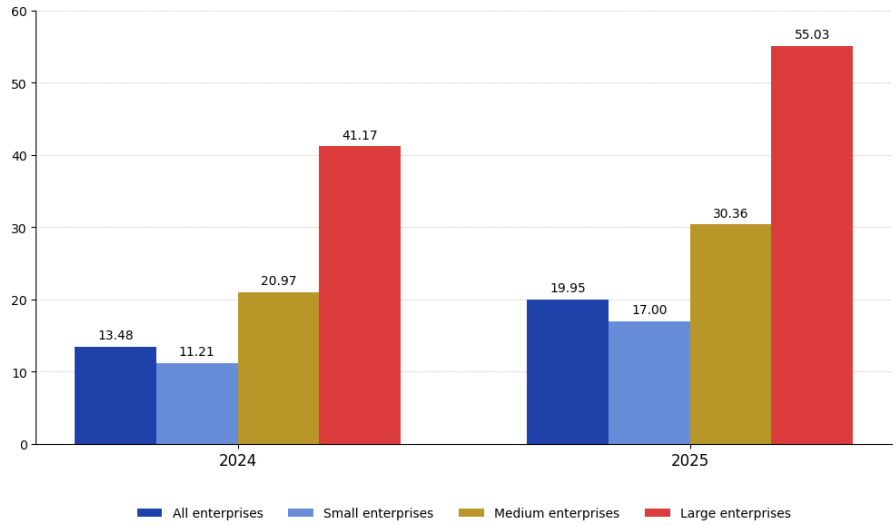


Fig. 1.1. Enterprises using AI technologies by enterprise size, EU, 2024 and 2025, % of total enterprises

Source: Eurostat. Use of artificial intelligence in enterprises. Data 2025. Published 11 December 2025.

Such differences between countries indicate unequal levels of digital maturity, access to technological infrastructure, and the readiness of enterprises to invest in innovative solutions (Fig. 1.2).

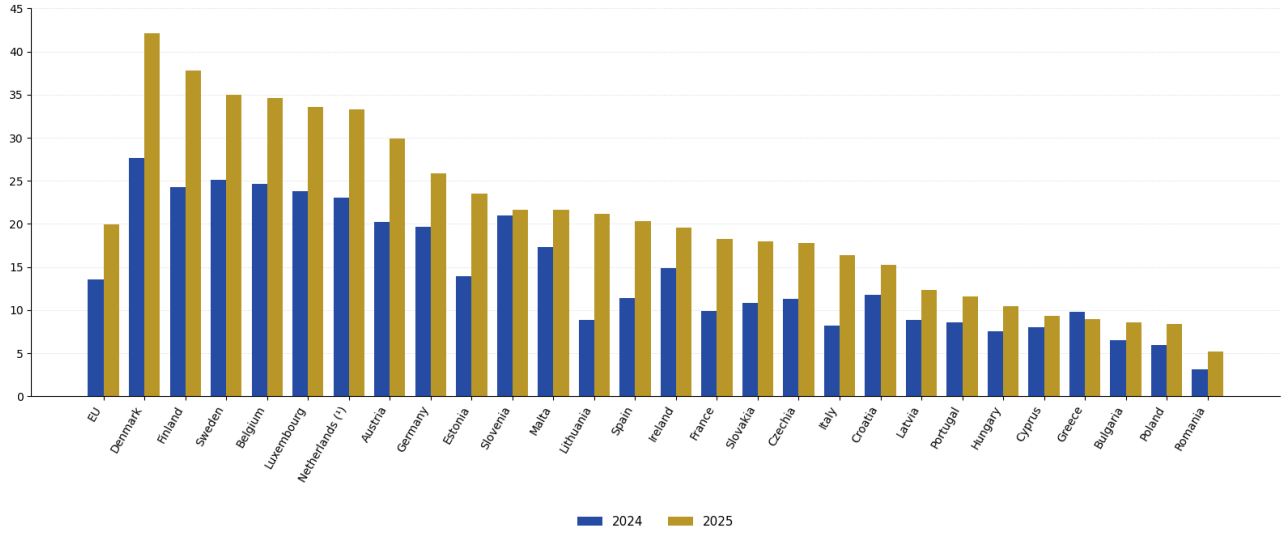


Fig. 1.2. Share of enterprises using artificial intelligence technologies in EU countries, 2024–2025, %

Source: Eurostat. Use of artificial intelligence in enterprises. Data 2025. Published 11 December 2025.

In the study by Drago C. et al., such differences between EU countries in the spread of artificial intelligence are explained by a combination of macroeconomic characteristics and labor market features. The authors identify a positive relationship between the level of AI adoption and GDP per capita, the openness of the economy to international trade, and certain employment structure indicators. In particular, a higher share of employees, employment in the services sector, and self-employment is associated with wider AI diffusion, while a high unemployment rate has a limiting relationship with its spread. This suggests that the pace of AI integration is determined not only by the technological readiness of enterprises, but also by broader national capacity for AI transformation and the overall level of economic development, including economic openness, labor market structure, and the institutional environment (Drago C. et al., 2025).

In terms of functional areas, the most common use of AI was the analysis of written language, which was carried out by 11.8% of enterprises. Generative technologies for creating images, video, sound, or audio were used by 9.5% of enterprises, while technologies for generating written or spoken language were used by 8.8% (Eurostat, 2026). Generative technologies for creating images, video, sound, and audio were used by 9.55% of enterprises, while technologies for generating written or spoken language and software code were used by 8.76%. Another 7.22% of enterprises used technologies for converting spoken language into a machine-readable format. Other areas, including machine learning, workflow automation, decision support, and object or person recognition, had lower levels of adoption. The least common use was technologies that enable the physical movement of machines based on autonomous decisions, at 1.39%.

An important feature of the current stage of artificial intelligence integration into European society is its rapid spread not only in the business environment but also among the population. In 2025, approximately one-third of EU citizens aged 16–74 used generative artificial intelligence technologies, indicating their gradual transformation from a professional tool into a technology used in everyday life [Eurostat. *Digital economy and society statistics – households and individuals*, 2026]. At the same time, the extent of AI use directly depends on people's readiness to interact

with digital technologies, which highlights the importance of digital skills. According to Eurostat, in 2025, only 60% of EU citizens aged 16–74 had at least basic digital skills, while 40% did not reach this level. Significant differences were observed between countries: the share of the population with basic or above-basic digital skills was 84% in the Netherlands, 83% in Ireland, and 81% in both Denmark and Finland. At the same time, the European Union has set a target of ensuring that at least 80% of the population has basic digital skills by 2030 (Eurostat. *Skills for the digital age*, 2026). Thus, even with the active spread of artificial intelligence and other digital technologies, the European Union faces the problem of insufficient digital skills among a significant part of the population, which may limit the effectiveness and equal development of digital transformation.

The data presented above show that the spread of artificial intelligence technologies in the European Union is uneven and depends not only on the availability of the technologies themselves but also on the level of digital readiness of economic and social actors. Under these conditions, AI integration should be considered not as an independent technological process but as a component of broader digital transformation. This transformation involves interconnected technological, organizational, economic, and social changes. Such an approach makes it possible to move from assessing individual indicators of AI technology adoption to analyzing their impact on the ways economic activities are carried out, the organization of work, value creation, and interaction between business, government, and society.

An analysis of current scientific approaches shows that digital transformation should be considered not as a separate process of implementing digital technologies, but as a gradual evolution of organizational, economic, and social changes. Its essence goes beyond the technological modernization of information systems and involves transforming the ways activities are organized, the mechanisms of creating and distributing value, the models of interaction between economic actors, as well as the nature of providing public and government services. This understanding is consistent with the approaches of Ukrainian and foreign researchers, although the emphasis in the definition of digital transformation differs to some extent in the scientific literature.

In particular, V. Silchenko considers digital transformation primarily as changes caused by the implementation and use of digital and information and communication technologies (Silchenko V., 2024). I. Kaida expands this interpretation by defining digital transformation as a comprehensive process of integrating digital technologies into all aspects of an enterprise's activities, aimed at increasing its competitiveness (Kaida I., 2025). A similar focus on the relationship between technological and organizational changes can be found in the study by Yu. Kyrylov, where digital transformation is described as a process of technological and organizational changes, mainly related to the development of digital technologies (Kyrylov Yu. et al., 2024).

Foreign studies add strategic and value-related components to the technological and organizational dimensions. C. Gong and V. Ribiere define digital transformation as a process of fundamental change supported by the innovative use of digital technologies and the strategic use of key resources and competencies. The result is a significant improvement of the organization and a rethinking of its value proposition for stakeholders (Gong C., Ribiere V., 2021). In turn, G. Vial considers digital transformation as a process of improving an organization through significant changes in its characteristics based on the combination of information, computing, communication, and connectivity technologies (Vial G., 2019).

The ambiguity of the concept of digital transformation is reflected not only in differences between scientific approaches but also in differences between its academic and practical understanding. In particular, the results of a study by R. Riedl et al. show significant differences in how digital transformation is understood by representatives of academia and business. While academic approaches mainly associate it with comprehensive organizational changes, the transformation of business models and processes, and changes in value creation mechanisms, business representatives much more often associate digital transformation directly with the implementation of modern digital technologies (Riedl R. et al., 2024).

A comparison of the approaches presented above makes it possible to identify several common characteristics of digital transformation. First, all authors associate it with the active use of digital technologies, which form the basis of transformational changes. Second, digital transformation is not limited to the acquisition or

implementation of technological solutions but involves changes in the activities of the organization. Third, the definitions focus on achieving a certain result, such as increased competitiveness, improved performance, the creation of new value, or a rethinking of how an organization operates.

At the same time, there are significant differences in the scale and depth of transformational changes. Ukrainian studies mainly focus on the implementation of digital technologies in enterprise activities, their integration, and their impact on competitiveness. In contrast, the approaches of the foreign researchers mentioned above place greater emphasis on the fundamental nature of changes, the strategic aspect, the transformation of resources and competencies, and the rethinking of the value proposition. Another important difference is the gap between the technological and transformational understanding of digitalization, which is also highlighted by R. Riedl.

At the same time, the approaches presented above do not sufficiently address the cross-cutting nature of modern digital technologies, particularly artificial intelligence. Unlike digital solutions whose use can be localized within a specific business process, AI technologies can simultaneously affect production, management, financial activities, employment, education, healthcare, public services, and the everyday interaction of citizens with the digital environment. Therefore, digital transformation should be considered not only as the technological and organizational restructuring of an individual enterprise, but also as a multi-level process of changing economic and social relations under the influence of digital technologies, in which artificial intelligence is becoming one of the key tools of transformation.

One of the most consistent conceptual models of this transition was proposed by Verhoef P. C. and co-authors, who consider digital change as an interconnected process consisting of three stages: digitization, digitalization, and digital transformation. A key feature of this model is the consideration of digital transformation as an interdisciplinary phenomenon that goes beyond information technologies and includes strategic management, marketing, innovation management, information systems, and operations (Verhoef P. C., 2021). In this approach, digital technologies are not

considered an end in themselves but as a tool for changing business processes, business models, value creation mechanisms, and interaction with stakeholders.

An important addition to these approaches is the concept of “Digital Ubiquity” proposed by Iansiti M. and Lakhani K. R. According to the authors, the spread of digital technologies and the combination of devices, sensors, data, and analytical capabilities gradually change not only individual operational processes but also the nature of competition, value creation mechanisms, and traditional industry boundaries. A clear example is the transformation of industrial companies, where combining physical equipment with digital sensors, cloud platforms, and data analytics makes it possible to move from selling products to providing digitally supported services and customer outcomes (Iansiti M., Lakhani K., 2014). Thus, digital transformation becomes cross-sectoral because digital technologies change not only the internal processes of enterprises but also the logic of creating and obtaining economic value, interaction with customers, and the structure of the competitive environment.

The rapid development of generative artificial intelligence, autonomous intelligent agents, digital platforms, and European initiatives in the field of artificial intelligence indicates the emergence of a new stage in the development of the digital economy that was not reflected in classical models of digital transformation. While in Verhoef P. C.'s model digital transformation represents the deepest level of digital change, current trends demonstrate a transition towards an economy in which artificial intelligence is becoming not only an individual digital technology but also a basic infrastructure for management decision-making, business process automation, innovation creation, and the development of new digital ecosystems.

In this context, it is appropriate to extend the classical model of digital transformation evolution by identifying the next stage – the AI-driven Economy. This approach makes it possible to reflect the current development logic of the digital economy, where there is a gradual transition from digitizing information and digitalizing individual processes to comprehensive transformation of business models and, subsequently, to the development of intelligent economic systems based on the widespread use of artificial intelligence technologies. At the highest stage of digital transformation, value creation becomes increasingly security-oriented. As noted by A.

O. Kudinova, the use of autonomous and predictive AI systems in leading economic sectors makes it possible to detect cyberattacks at an early stage, forecast crisis situations, and monitor environmental and social parameters (Kudinova A. O., 2025). This transforms the mechanism of value creation from traditional operational efficiency towards the development of multi-level systemic resilience of businesses and the state as a whole.

According to the proposed approach, the evolution of digital transformation can be presented as a conceptual model (Fig. 1.3) covering five successive stages: analog processes → digitization → digitalization → digital transformation → AI-based economy.

Alongside concepts that describe digital transformation as an evolution of digital change, process-oriented approaches are becoming increasingly common in current research. These approaches focus on the mechanisms through which transformation is implemented. In particular, the study by Tian Y. and Ou L. (Tian, Y., & Ou, L., 2024) considers digital transformation as a sequential organizational process implemented through three interconnected phases: initial readiness, implementation, and innovation transformation. Unlike models that describe digital transformation mainly through technological or functional changes, this approach focuses on an organization's readiness for transformational changes, its ability to integrate digital technologies into operations, and its ability to achieve strategic competitive advantages through the radical renewal of its business model.

The “Initial Readiness” phase involves creating the conditions for digital transformation, including the development of digital infrastructure, data collection and management, staff training, development of digital competencies, creation of a digital strategy, and management readiness for organizational changes. This stage provides the basis for the subsequent implementation of digital technologies and defines the strategic directions of the organization's digital development.

The “Intermediate Implementation” phase is characterized by the practical integration of digital technologies into key business processes. At this stage, organizations implement enterprise information systems, cloud services, Internet of Things technologies, big data analytics, digital platforms, and other digitalization tools.

The main result is not only the automation of individual processes but also increased operational efficiency, improved interaction with stakeholders, and the creation of additional value for consumers.

The final phase – "Innovation Transformation" – reflects the transition from gradual process improvement to their radical transformation. At this stage, digital technologies become the basis for revising the business model, creating new products and services, developing digital platforms and ecosystems, and generating new sources of competitive advantage. The organization moves from using digital technologies as tools to support its activities to using them as strategic factors of innovative development.

The combination of these ideas forms the basis of the proposed conceptual model, which complements the traditional sequence of digital changes with a modern stage – the AI-based economy – and reflects the relationship between technological development, organizational maturity, and the creation of economic value (Fig. 1.3). The proposed model summarizes the relationship between the stages of digital development, the corresponding technologies, the level of organizational maturity, and the results of economic value creation. It is based on a sequence from analog processes to an AI-based economy, extending the classical logic of "digitization – digitalization – digital transformation" by taking into account the current development of artificial intelligence.

At the initial stage, analog processes, paper documents, and manual operations are predominant. Digitization involves converting information into digital form through scanning, optical character recognition (OCR), and electronic archives. This stage creates digital data and provides the basis for further transformation. Digitalization is associated with the integration of ERP and CRM systems, cloud technologies, and the Internet of Things, which enables the automation and optimization of individual business processes. At the digital transformation stage, the use of Big Data, digital twins, blockchain, and other digital solutions contributes to deeper organizational changes, the emergence of new business models, and innovation.

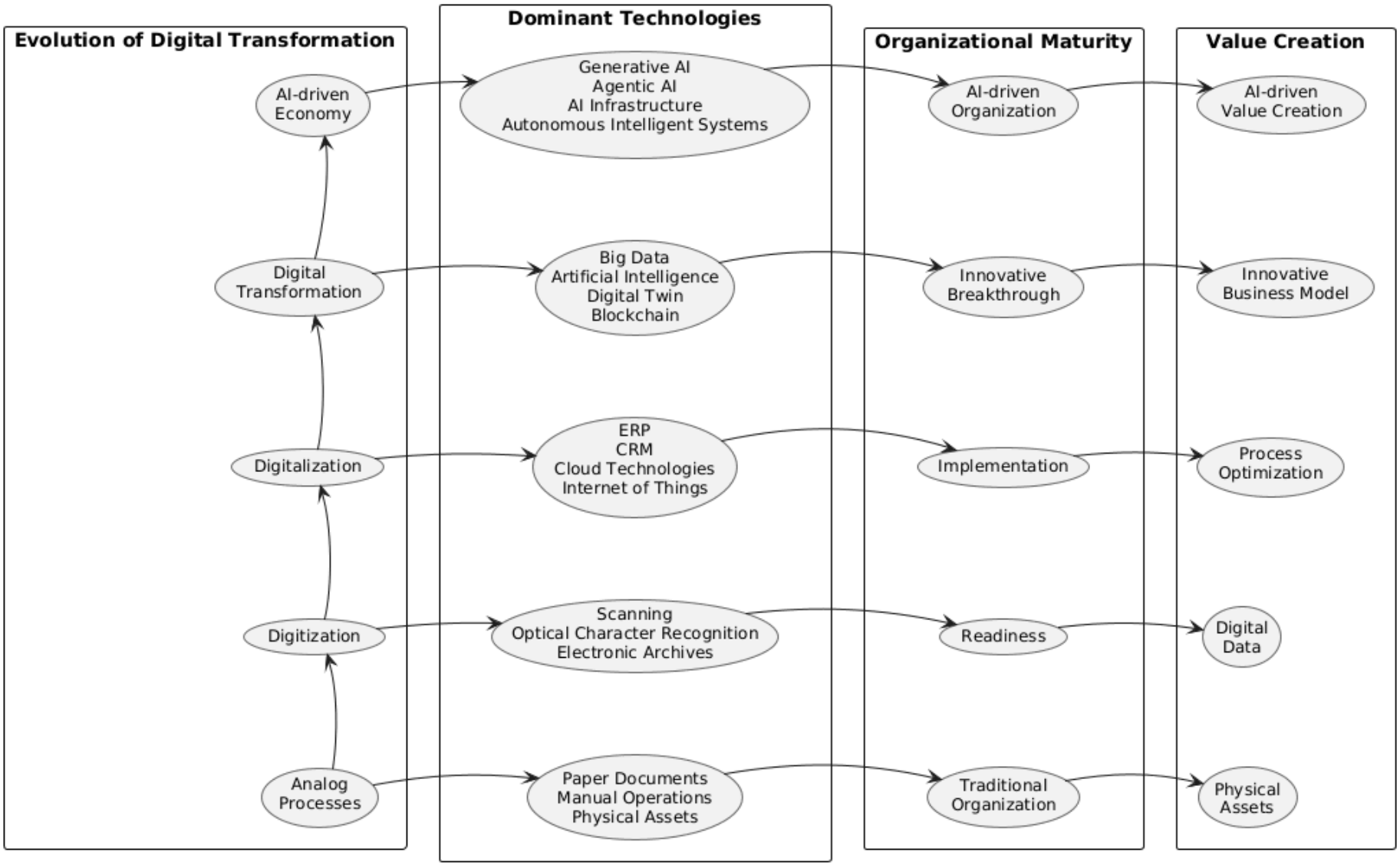


Fig. 1.3. Conceptual model of the transition from digital transformation to an AI-based economy

The next stage of the model is the AI-based economy, in which generative and agentic AI, the related infrastructure, and autonomous intelligent systems become of systemic importance. At this level, the organization moves towards an AI-oriented operating model, while value creation is increasingly linked to the use of AI capabilities for decision-making, innovation development, and the creation of new products, services, and business models.

Thus, the model reflects not only the sequence of technological changes but also the corresponding transformation of organizational maturity and value creation mechanisms: from physical assets and manual operations to digital data, optimized processes, innovative business models, and AI-oriented value creation. Its main feature is the identification of the AI-based economy as a modern continuation of digital transformation, in which AI becomes an important systemic factor in the organization of economic activity.

In the European Union, artificial intelligence is increasingly considered not only as an individual digital technology but also as a tool for the structural modernization of the economy, public administration, and public services. Current EU policy focuses on accelerating the adoption of AI in strategic sectors, including healthcare and pharmaceuticals, transport, robotics, industry, construction, the agri-food sector, energy, the public sector, and cultural and creative industries.

Sectoral differences in AI adoption are one of the key findings of current European research. The European Commission report *The Futures of Artificial Intelligence* proposes dividing economic sectors into three groups depending on the nature and prospects of AI use (Table 1.1) (European Commission. *The Futures of Artificial Intelligence*, 2026): innovation-led sectors, operational-core sectors, and service-envelope sectors. The first group includes information and communication technologies, research and development, and professional services, where AI is moving more rapidly towards systematic integration into the creation of products, services, and business models. In operational-core sectors, including industry, transport, energy, agriculture, and construction, the main focus is on scaling applied AI solutions aimed at automation, forecasting, monitoring, and optimization. In the service sector, including trade, finance, healthcare, education, and public administration, AI

integration is largely related to service personalization, communication automation, and decision support (European Union, 2026).

Table 1.1

Sectoral differentiation of AI technology integration pathways in the EU economy in 2025

Economic sectors	Characteristics	Level and nature of AI integration	Typical areas of AI application
Innovation-led sectors	Information and communication technologies, research and development, professional and technical services; systematic AI integration, development of new products and business models	High level of readiness for the systematic integration of AI into production and management processes	Development of AI products and services; big data analysis; generative AI; programming automation; modeling; creation of new business models
Operational-core sectors of the economy	Manufacturing, transport, energy, agriculture, construction; automation, forecasting, monitoring, and resource optimization	Scaling of applied and specialized AI solutions to optimize core operations	Demand and technical condition forecasting; intelligent monitoring; robotics; optimization of production processes and resources; autonomous systems; detection of anomalies and cyber incidents
Service and customer-interaction sectors	Trade, finance, healthcare, education, culture, public administration; service personalization, communication automation, decision support	Mainly gradual and exploratory implementation of platform-based AI tools; dependence on data quality, skills, and regulatory requirements	Service personalization; chatbots and virtual assistants; automation of document management and communication; decision support; predictive analytics; fraud detection

Source: compiled by the author based on European Commission. The Futures of Artificial Intelligence, 2026

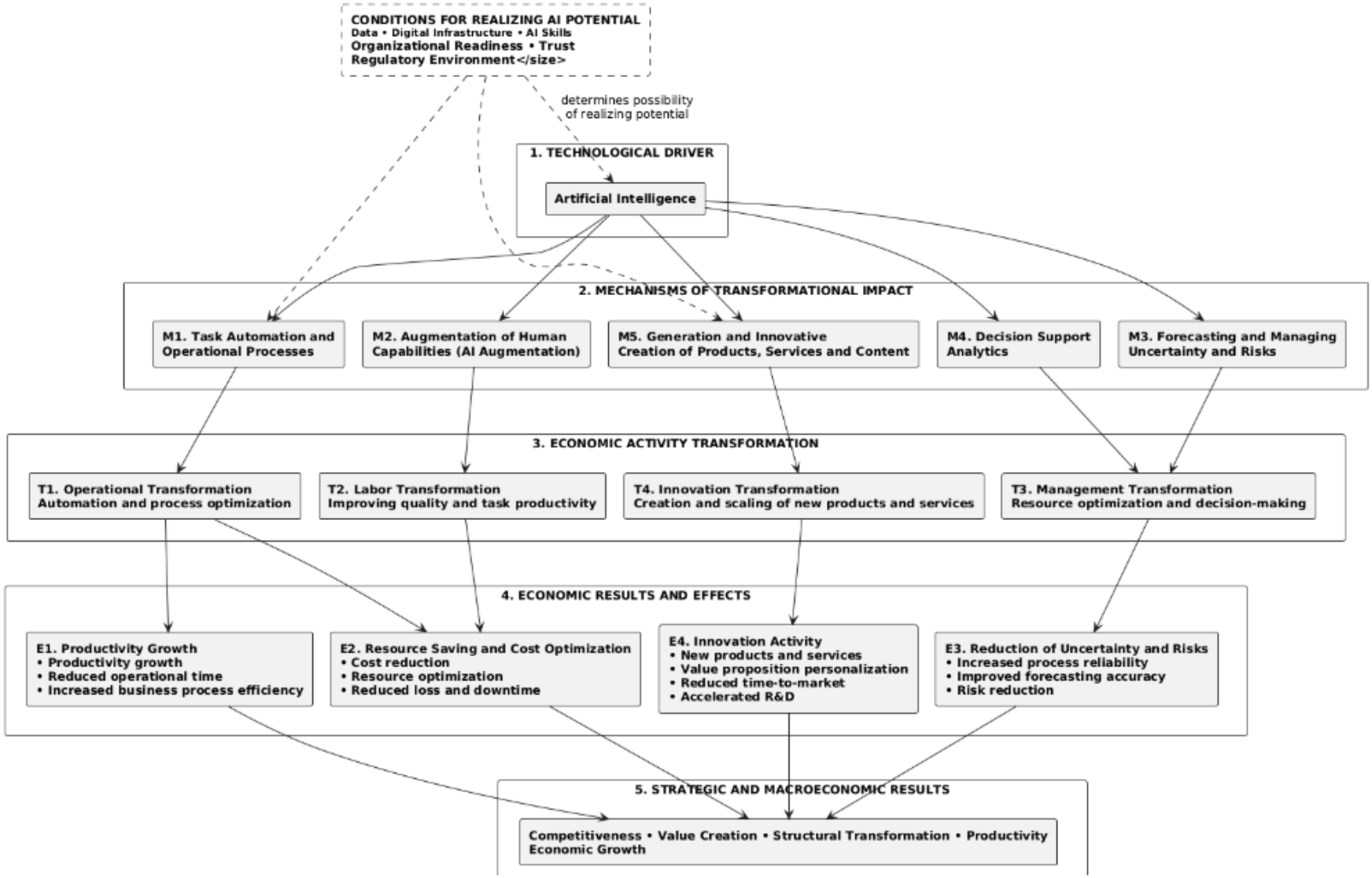


Рис. 1.4. Модель трансформаційного впливу штучного інтелекту на економічну діяльність

An analysis of AI use in different sectors of the economy shows the presence of common mechanisms of its transformational impact, regardless of sector-specific characteristics. These mechanisms include the automation of operational processes, augmentation of human capabilities, forecasting and risk management, analytical decision support, and the generation of new products, services, and content. Their implementation transforms business processes through increased productivity, reduced costs, optimized resource use, personalization of offers, and accelerated innovation. This makes it possible to present this impact as a sequence of interconnected levels: technological driver → transformation mechanisms → changes in economic activity → direct economic results and effects → strategic and macroeconomic consequences (Fig. 1.4).

This approach is consistent with the interpretation of AI as a general-purpose technology, whose potential is realized not through a single technological solution, but through changes in the ways tasks are performed, work is organized, decisions are made, and economic value is created (Filippucci, 2024; Acemoglu D., 2024; Aghion P., 2019).

At the first level, AI acts as a technological driver of transformation, creating new opportunities for information processing, forecasting, automation, and the generation of outputs. Its impact is realized through five interconnected mechanisms: automation of tasks and operational processes, augmentation of human capabilities, forecasting and management of uncertainty and risks, analytical decision support, and the generation and innovative creation of products, services, and content. This differentiation is important because the economic impact of AI cannot be reduced solely to the replacement of human labor. Research shows that, alongside the automation of individual tasks, AI can complement human work, increase employee productivity, support the spread of best practices, and create conditions for the emergence of new types of activities.

At the next level, these mechanisms lead to the transformation of economic activity in four interconnected areas: automation and optimization of operations, transformation of the content and methods of performing work tasks, improvement of

resource management and decision-making, and the creation and scaling of new products and services.

As a result, AI changes not only individual operations but also the organization of economic processes, the structure of work tasks, and the mechanisms of economic value creation. In particular, empirical studies of generative AI use confirm the possibility of simultaneously increasing the speed and quality of intellectual tasks, while macroeconomic models link the scaling of such effects to potential growth in productivity and innovation activity.

The direct results of AI implementation can be systematized into four main categories: productivity growth, increased economic efficiency, improved quality and reliability, and increased innovation activity. The first two categories mainly reflect quantitative changes in the use of labor, capital, and other resources – reduced task completion time, lower costs, reduced downtime, and improved performance. Improved quality and reliability are associated with more accurate forecasting, fewer errors, and lower operational and financial risks. At the same time, the innovation dimension includes faster research and development, the creation of new products and services, personalization of offers, and shorter time to market. Thus, the economic performance of AI is formed as a combination of effects that arise at the level of individual tasks and processes and are gradually aggregated to the level of an enterprise, sector, and the economy as a whole.

At the strategic and macroeconomic levels, the accumulation of these results may be reflected in increased competitiveness, the creation of added value, structural transformation of sectors, productivity growth, and long-term economic growth. At the same time, this cause-and-effect relationship is not automatic. The realization of AI's technological potential depends on a set of prerequisites, among which the availability and quality of data, digital and computing infrastructure, the availability of relevant digital and AI skills, the organizational readiness of enterprises and institutions, as well as the level of trust and the quality of the regulatory environment are of key importance. Studies of the digital intensity of sectors and recent European analytical documents confirm that these factors largely determine differences in the speed and scale of AI adoption across countries, enterprises, and sectors.

The sectoral context determines the specific configuration of mechanisms and outcomes. Thus, in manufacturing, automation, predictive maintenance, and computer-based quality control are dominant; in the financial sector – forecasting, risk assessment, and fraud detection; in healthcare – intelligent diagnostics and treatment personalization; in energy – forecasting of production and consumption and optimization of network operations; and in education and research – learning personalization, information processing, and support for research processes. Therefore, sector-specific characteristics determine the forms of practical AI implementation, while the basic logic of its economic impact remains common: AI technological capabilities are transformed into functional impact mechanisms, then into changes in economic activity and direct outcomes, which, under appropriate institutional, technological, and human conditions, may generate long-term competitive and macroeconomic effects.

The proposed model (Fig. 1.4) makes it possible to consider the transformational impact of AI not as a linear relationship between technology adoption and the achievement of an economic effect, but as a multi-level process in which technological capabilities are transformed into economic outcomes under appropriate organizational, institutional, and infrastructure conditions. At the same time, individual impact mechanisms are not isolated: automation can be combined with the augmentation of human capabilities, forecasting with analytical decision support, and generative technologies with the creation and scaling of new products and services. Accordingly, a single AI technology can simultaneously generate several interconnected economic effects, while the combined effects at the level of enterprises and sectors create the basis for structural changes at the macroeconomic level.

An important feature of the proposed model is that it takes into account the conditions for realizing AI potential, which determine the ability of the technological driver to be transformed into actual economic outcomes. These conditions include access to data, digital infrastructure, and relevant digital skills, organizational readiness, trust in technologies, and the regulatory environment. Their importance lies in the fact that the same technological potential can generate different results depending on the level of readiness of an economic actor to use it in practice. Thus, the economic

effect of AI is determined not only by the level of technological development but also by the ability of enterprises, institutions, and social organizations to integrate relevant technologies into existing business processes, organizational structures, and decision-making mechanisms.

At the same time, the model shows that deeper AI transformation is accompanied by increasing dependence of economic activity on data, digital infrastructure, information systems, and network interactions. At the initial stages of digital development, information security was mainly considered as a function of protecting individual information resources. Under conditions of large-scale AI use, however, it becomes systemic in nature. The automation of critical processes, the use of cloud and network platforms, the integration of large volumes of data, the application of AI models for management decision-making, and the development of autonomous digital systems increase the potential consequences of breaches of information confidentiality, integrity, or availability.

At the same time, the transformational potential of AI is not realized automatically. A key factor is the availability of a favorable environment for its implementation, which includes access to high-quality data, digital and computing infrastructure, relevant human competencies, organizational readiness, financial resources, trust in technologies, and a predictable regulatory and legal environment. Therefore, barriers to AI adoption should be considered not only as individual technical or economic constraints but as a set of interconnected factors that determine the ability of economic actors to transform AI's technological potential into productivity, innovation, and other forms of economic value.

Current Eurostat data confirm that the main barriers to AI adoption among European enterprises are primarily related to skills, regulation, information security, and data protection. In 2025, among EU enterprises that considered using AI technologies but did not implement them, 70.3% identified a lack of relevant expertise as the main barrier, 53.6% reported a lack of clear understanding of the legal implications of AI use, and 52.7% expressed concerns about compliance with data protection and privacy requirements. At the same time, only 17.8% of these enterprises considered AI technologies to be not useful or necessary for their activities. This

indicates an important point: the challenge of AI adoption in the EU is largely not the lack of awareness of its potential value but the insufficient readiness of enterprises to integrate it into practice [Eurostat, 2026].

These barriers have certain sector-specific characteristics. For innovation-led sectors, whose activities are directly related to the creation and scaling of digital technologies, the most critical factors include a shortage of highly qualified AI and machine learning specialists, the high cost of computing resources, intellectual property protection, access to high-quality datasets, as well as dependence on foreign foundation models, cloud services, and computing infrastructure. The latter aspect is becoming strategically important for the European Union: in 2026, the European Commission directly identified limited and geographically concentrated access to computing capacity and dependence on non-European providers of cloud and AI computing services as key structural challenges for the European AI ecosystem.

For operational-core sectors, including manufacturing, energy, transport, and other activities with a high dependence on physical and production infrastructure, the main barriers include the incompatibility of new AI solutions with existing information and production systems, the use of outdated equipment, insufficient data standardization, high costs of technological integration, and functional and cybersecurity risks. This specificity is particularly important for enterprises where AI implementation involves not simply installing a new software product but restructuring the interaction between information systems, production technologies, data, and employees.

For service and customer-interaction sectors, greater importance is attached to personal data protection, legal certainty, users' trust in algorithmic decisions, the risks of inaccurate or biased results, and the level of employees' digital literacy. These factors are particularly important in banking, insurance, healthcare, education, and other areas where the results of automated analysis may directly affect citizens' rights, financial opportunities, or access to services.

In general, the main barriers to realizing the potential of AI in the European economy can be presented as a system of interconnected groups (Table 1.2).

Table 1.2

Barriers to realizing the potential of AI in the EU

Barrier group	Description of the problem
Skills and competencies	Shortage of specialists capable of developing, implementing, integrating, and monitoring AI solutions
Regulatory	Uncertainty regarding legal responsibility, algorithmic transparency, and compliance with regulatory requirements
Information security	Risks of privacy violations, data breaches, and non-compliance with information protection requirements
Technology integration	Incompatibility with legacy IT systems, production equipment, and corporate platforms
Infrastructure	Limited access to computing capacity, cloud resources, data, and digital infrastructure
Economic	High costs of models, computing, integration, cybersecurity, and staff training
Organizational	Lack of a well-defined business case and insufficient readiness of business processes and organizational structures for AI integration
Social and trust-related	Lack of trust in AI results and concerns about bias, lack of transparency, and the lack of control over automated decisions

Source: compiled by the author based on data from (Eurostat, 2026; Ferrando A. et al., 2026; European Commission, 2025, 2026).

Thus, the data presented above show that barriers to AI adoption are systemic in nature and cannot be overcome solely by increasing investment in technologies. The primary challenge remains the development of enterprises' capacity to use these technologies. It is significant that even when there is considerable demand for AI, a lack of relevant skills remains one of the most widespread barriers.

This conclusion is supported by a study of the European Central Bank based on harmonized data from approximately 6,000 enterprises in 12 euro area countries. The

study showed that around 70% of enterprises already use AI to some extent, while only 7% describe their level of use as significant. Among enterprises that do not use AI or use it to a limited extent, the most frequently reported barriers include a lack of relevant skills, incompatibility with existing systems, ethical risks, and doubts about the practical usefulness of the technology (Ferrando A., 2026).

At the same time, the ECB study makes it possible to clarify the relationship between barriers and economic incentives for AI adoption. Enterprises identify the improvement of core and support business processes as the main motives for using AI, accounting for 33% and 29% of the reported reasons for technology adoption, respectively. Support for research and innovation accounts for 13%, reduction of personnel costs for 15%, and expansion of product and service offerings for 10%. At the same time, among enterprises that do not yet use AI, 30% consider it insufficiently useful for their activities, while about 20% report incompatibility with existing systems and a lack of relevant skills.

These results provide an important basis for understanding the mechanism of AI's transformational impact. The economic value of the technology is not created directly at the moment of its acquisition or technical implementation, but through its organizational integration and adaptation to a specific business context. Therefore, there is a kind of "integration gap" between the technological potential of AI and actual economic outcomes. Its size is determined by the availability of data, skills, infrastructure, financing, organizational capabilities, and regulatory mechanisms.

At the macro level, these limitations are complemented by structural features of the European digital economy. The European Commission identifies fragmentation of the digital market, unequal access to digital infrastructure, a shortage of specialists, limited access to capital, dependence on non-European providers of cloud and AI technologies, and the complexity of the regulatory environment among the systemic challenges. In 2026, the European Commission specifically emphasized the limited and geographically concentrated availability of computing capacity in the EU and the dependence of the European economy on non-European providers of cloud and AI computing services (European Commission. Study on Cloud and AI Development in the EU, 2026; European Commission. State of the Digital Decade, 2026).

The issue of technological dependence is particularly important in the context of EU digital sovereignty. According to State of the Digital Decade 2026, in 2026, almost 20% of EU enterprises used artificial intelligence, while the use of cloud technologies reached 46.7% and data analytics technologies 39.9%. At the same time, the EU remains significantly dependent on external providers in areas such as cloud services, cybersecurity, and other strategic digital technologies. The EU's share of the global semiconductor market is only 9%, which further highlights the structural nature of these technological dependencies.

Therefore, barriers to realizing AI potential can be considered as specific "filtering conditions" for the transformational effect, through which technological potential passes on its way to an actual economic outcome. At the enterprise level, these filters include skills, data, system compatibility, financial resources, and trust. At the sectoral level, they are complemented by the characteristics of technological infrastructure, the regulatory environment, and the nature of business processes. At the macroeconomic level, they include access to computing capacity, technological sovereignty, the structure of the digital market, and the ability of public policy to support the scaling of innovation.

In this context, the third block of the proposed model – the conditions for realizing AI potential – is of fundamental importance for explaining differences in the results of digital transformation between enterprises, sectors, and countries. These conditions determine the extent to which AI technological capabilities can be converted into higher productivity, innovation activity, new products and services, business process optimization, and new models of economic value creation.

At the same time, deeper AI transformation is accompanied by increasing dependence of economic activity on data, digital infrastructure, information systems, and network interactions. At the early stages of digital development, information security was mainly considered as a function of protecting individual information resources. Under conditions of large-scale AI use, however, it becomes systemic in nature. The automation of critical processes, the use of cloud and network platforms, the integration of large volumes of data, the use of AI models to support management

decisions, and the development of autonomous digital systems increase the potential consequences of breaches of information confidentiality, integrity, or availability.

Thus, cybersecurity becomes not an external limitation of digital transformation but one of its internal institutional and technological conditions. The deeper AI is integrated into economic processes, the greater the dependence of economic resilience on data reliability, the security of digital infrastructure, the safety of algorithmic systems, and the ability of organizations to detect and neutralize new types of digital threats in a timely manner.

The growing level of digital interdependence among enterprises, public institutions, and society means that the effectiveness of digital transformation increasingly depends not only on the availability of digital infrastructure and the ability to implement innovative technologies, but also on the capacity to ensure the confidentiality, integrity, and availability of information, including personal data, the continuity of critical processes, and the resilience of digital systems to external and internal threats. This is particularly important in the transition to an AI-based economy, in which data, digital infrastructure, cloud services, algorithms, and intelligent systems are becoming critical resources for creating economic value. The concentration of large volumes of data, the integration of information systems, and the spread of autonomous and generative AI solutions expand the range of possible cyber threats and the number of potential targets for cyberattacks (Fig. 1.5). Under these conditions, cybersecurity is no longer exclusively a functional responsibility of the IT departments of enterprises or organizations but becomes a strategic prerequisite for digital transformation and economic resilience.

This creates a need to move from a technology-oriented approach towards a multi-level system of strategic cybersecurity management integrated into the general mechanisms for managing the digital transformation of enterprises and organizations.

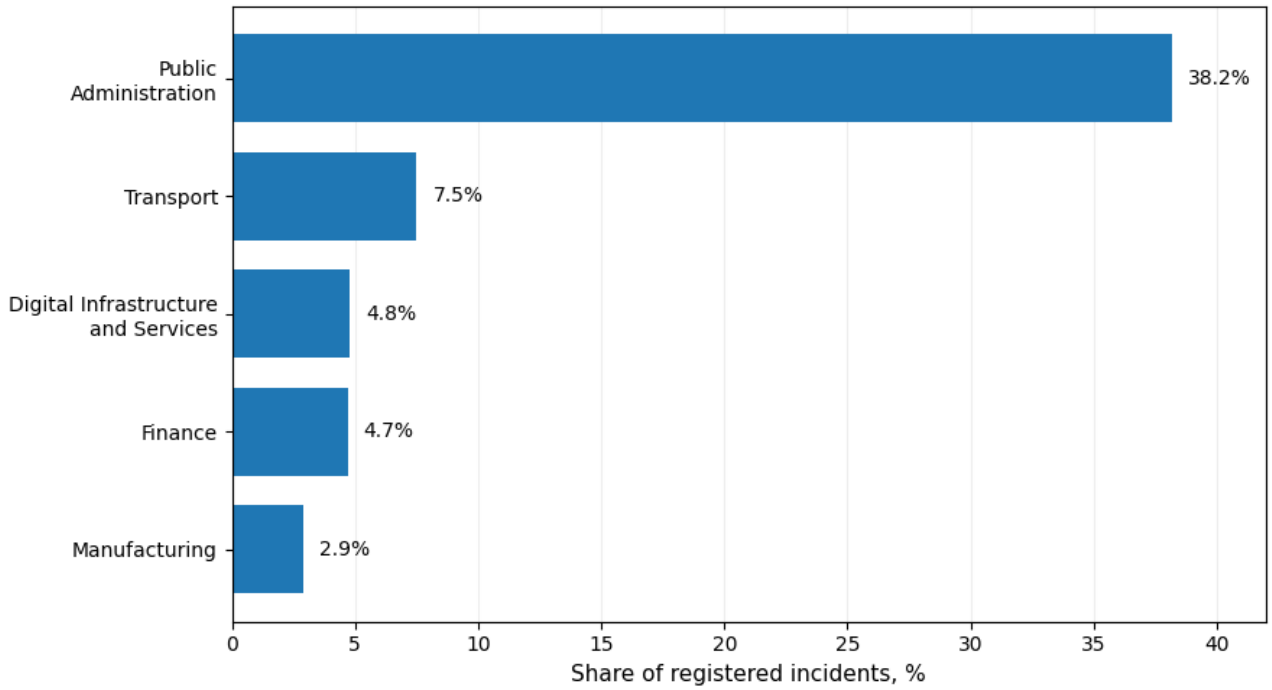


Fig. 1.5. Target sectors of cyberattacks in the EU, 2024–2025

Source: compiled based on ENISA Threat Landscape 2025.

Such a system should include not only technological means of protecting information resources but also organizational, regulatory, institutional, and human-resource mechanisms for ensuring cyber resilience. Its key interconnected strategic directions should include:

1. Strategic management and integration of cybersecurity into corporate governance – establishing a clear structure of responsibility for cybersecurity at the management level of the organization, defining the functions and powers of responsible actors, establishing mechanisms for internal coordination and control, and integrating cybersecurity goals and tasks into the overall digital development and risk management strategy.

2. Regulatory and institutional support for cyber resilience – developing internal cybersecurity policies and strategies, aligning them with international and European regulatory requirements and standards, including NIS2, DORA, GDPR, and the AI Act, creating mechanisms for mandatory or regulated reporting of cyber incidents, assessing risks in supply chains, and ensuring an appropriate level of protection of digital infrastructure.

3. Inter-organizational and international cooperation in cybersecurity – creating an ecosystem for sharing information about cyber threats between the public, private, and academic sectors, developing international cooperation in cybersecurity, particularly within European and Euro-Atlantic mechanisms, creating platforms for collective monitoring, information exchange, and coordinated response to cyber incidents, as well as harmonizing security approaches and standards.

4. Development of human, technological, and organizational cyber-resilience capacity – investing in the development of human capital, attracting and professionally developing cybersecurity specialists, certification in accordance with international standards, implementing modern technological tools for detecting, preventing, and responding to cyber threats, increasing employees' digital and cybersecurity literacy, and developing a sustainable corporate cybersecurity culture.

Cybersecurity is not an external limitation on realizing the potential of AI but one of the conditions for ensuring its sustainable economic impact. Disruption of digital infrastructure or compromise of data may offset the positive results of automation, optimization, and intelligent transformation of processes, while reliable protection of information resources and the ability of systems to resist and recover from cyber incidents become essential components of secure digital transformation.

This relationship should be considered as two-sided. On the one hand, digital transformation and artificial intelligence create new vulnerabilities related to data protection, digital infrastructure security, the reliability of algorithmic decisions, dependence on cloud and platform technologies, and the possibility of using AI technologies to scale cyberattacks. On the other hand, AI technologies themselves create new opportunities to strengthen information and cybersecurity through automated anomaly detection, network traffic analysis, identification of potential incidents, forecasting of cyber threats, detection of fraudulent activities, and support for incident response. Thus, AI technologies simultaneously act as a factor transforming cyber risks and as one of the key tools for their mitigation.

These directions for developing cyber resilience acquire new meaning under the rapid spread of artificial intelligence technologies. The integration of AI into strategic cybersecurity management is gradually changing from a technological modernization

direction into an important component of digital risk management and organizational resilience. This is caused by both the growing potential of AI to improve cybersecurity effectiveness and the expanding range of threats associated with the use of AI systems themselves.

The scale of this transformation is confirmed by recent international studies. According to the Global Cybersecurity Outlook 2026, 94% of surveyed experts consider artificial intelligence to be the most significant factor influencing changes in cybersecurity in the near future (Global Cybersecurity Outlook 2026). At the same time, the share of organizations with formalized processes for assessing the security of AI tools increased from 37% in 2025 to 64% in 2026, indicating the rapid shift of AI security from a technological issue to a strategic management issue. It is also significant that 87% of respondents identified AI-related vulnerabilities as the fastest-growing cyber risk during 2025 (World Economic Forum, 2026).

Considering the relationship between artificial intelligence and cybersecurity, it can be noted that the same technological foundation simultaneously creates new protection opportunities and new cyber threat vectors. On the one hand, machine learning algorithms and generative AI expand the capabilities of automated network traffic analysis, detection of anomalous behavior, classification of malware, correlation of security events, prioritization of alerts, and decision support during incident response. The use of AI makes it possible to process large volumes of heterogeneous data in near real time, which is particularly important in the highly dynamic modern cyber environment.

On the other hand, the spread of generative and autonomous AI creates an additional attack surface. Attackers can use such technologies to scale social engineering and phishing, automate vulnerability discovery, create polymorphic malicious code, generate convincing fraudulent content, and attack AI models themselves. Therefore, the objects of cybersecurity protection include not only traditional information systems and data but also AI models, datasets, software interfaces, model supply chains, computing infrastructure, and human interaction with autonomous systems.

The importance of this approach is confirmed by a study by IBM and the Ponemon Institute. The Cost of a Data Breach Report 2025 states that 97% of organizations reporting AI-related security incidents did not have adequate access controls for AI, while 63% of organizations did not have AI governance policies aimed at controlling its use and distribution (Cost of a Data Breach Report, 2025). At the same time, extensive use of AI in cybersecurity systems was associated with average savings of approximately USD 1.9 million compared with organizations that did not use such solutions (IBM, 2025).

Thus, strategic cybersecurity management under the spread of AI should include not only the use of artificial intelligence to protect digital infrastructure but also the management of risks arising from the use of AI itself. This two-sided perspective requires the development of a separate management framework that combines technological, organizational, regulatory, and human-resource mechanisms.

The first component is the technological integration of AI into the cybersecurity architecture. This includes the use of machine learning algorithms for anomaly detection, analysis of user and network-object behavior, classification of cyber threats, automated event correlation, and support for cybersecurity operations centers. At the same time, the effectiveness of such solutions should not be assessed only by classification accuracy. For strategic management, indicators such as detection and response time, the level of false positives, model resilience to changes in the environment, scalability, and economic efficiency are also of fundamental importance.

The second component is the management of AI-system risks and reliability. Unlike traditional information systems, machine learning models may be vulnerable to specific types of attacks, including evasion attacks, data poisoning, model theft, information leakage, and manipulation of input data. For generative models, additional risks include prompt injection, leakage of confidential information, incorrect generation, and excessive autonomy in decision-making processes. Therefore, ensuring cyber resilience requires continuous testing, validation, and monitoring of models throughout their entire life cycle.

An important methodological basis for this approach is the NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0), which structures AI risk

management around four interconnected functions: Govern, Map, Measure, and Manage. The “Govern” function has a cross-cutting nature and should be integrated into all other risk-management processes throughout the AI system life cycle (NIST, 2023). NIST also identifies validity and reliability, safety, security and resilience, accountability and transparency, explainability and interpretability, privacy protection, and the management of harmful bias among the characteristics of trustworthy AI systems (NIST, 2023).

The third component is the institutionalization of AI governance at the level of corporate and strategic management. The use of AI in critical business processes requires the identification of responsible actors, allocation of powers, establishment of an acceptable level of risk, regulation of human-control procedures, and development of mechanisms for auditing algorithmic decisions. Thus, AI cybersecurity cannot remain exclusively the responsibility of IT or cybersecurity departments. It should be integrated into corporate governance, risk management, internal control, and strategic planning.

The principle of human oversight is particularly important. According to this principle, critical decisions that may have significant financial, legal, or social consequences should not be transferred to automated systems without adequate human control. This approach is consistent with the logic of the NIST AI RMF, according to which effective AI risk management requires continuous involvement of responsible actors, an appropriate distribution of roles and responsibilities, and the integration of assessment, verification, and validation procedures throughout the AI system life cycle (NIST, 2023).

The fourth component is the development of human and organizational capacity to manage AI-related cyber risks. The effectiveness of technological solutions largely depends on the availability of specialists who can simultaneously understand the principles of AI, the specifics of cyber threats, risk management methods, and the organization's business context. Therefore, the development of interdisciplinary teams is a promising direction. Such teams may include cybersecurity specialists, data analysts, machine learning specialists, risk managers, legal experts, and corporate

governance professionals. At the same time, management competencies regarding the capabilities, limitations, and risks of AI use should also be developed.

Thus, the integration of artificial intelligence into strategic cybersecurity management creates a qualitatively new model of cyber resilience in which AI simultaneously acts as a protection tool, an object of protection, and a factor transforming the risk-management system itself. This model involves a shift from reactive response to cyber incidents towards continuous monitoring, forecasting, and adaptive management of cyber risks. In this context, cyber resilience should be understood not only as an organization's ability to withstand cyberattacks but also as its ability to continuously operate, adapt, recover, and transform under the influence of dynamic cyber threats and technological changes. Therefore, AI implementation should be accompanied by appropriate risk-management, control, audit, and human-oversight mechanisms. This approach makes it possible to align technological modernization with economic and organizational resilience and to ensure the secure development of digital transformation.

In the European context, this leads to a gradual transition from the traditional approach to information security, which is mainly focused on protecting individual information systems, towards a comprehensive model of cyber resilience. Its basis is the combination of technological, organizational, regulatory, and human protection mechanisms (Fig. 1.6). Accordingly, secure digital transformation involves not only the implementation of technical information-protection measures but also risk management, business continuity, staff training, the development of a cybersecurity culture, control of digital technology supply chains, and the ability of organizations to quickly detect, contain, and recover from cyber incidents.

The principle of security by design is particularly important. According to this principle, information and cybersecurity requirements should be integrated at the design stage of digital systems, information platforms, and AI solutions rather than implemented only after their deployment. This approach is particularly important for the AI-based digital economy because security should cover not only infrastructure and data but also the life cycle of AI models, the quality and origin of data, access-control

mechanisms, decision-making transparency, monitoring of anomalous behavior, and the possibility of human intervention in critical processes.

Thus, the analysis provides grounds for considering cybersecurity not as an external restrictive factor of digital transformation but as its integral structural component. At the early stages of digital development, the main objective was to ensure the availability and protection of digital information. Under conditions of digital transformation and an AI-based digital economy, the focus shifts towards ensuring systemic cyber resilience, the ability to withstand large-scale and complex threats, and the ability to restore operations after such threats materialize.

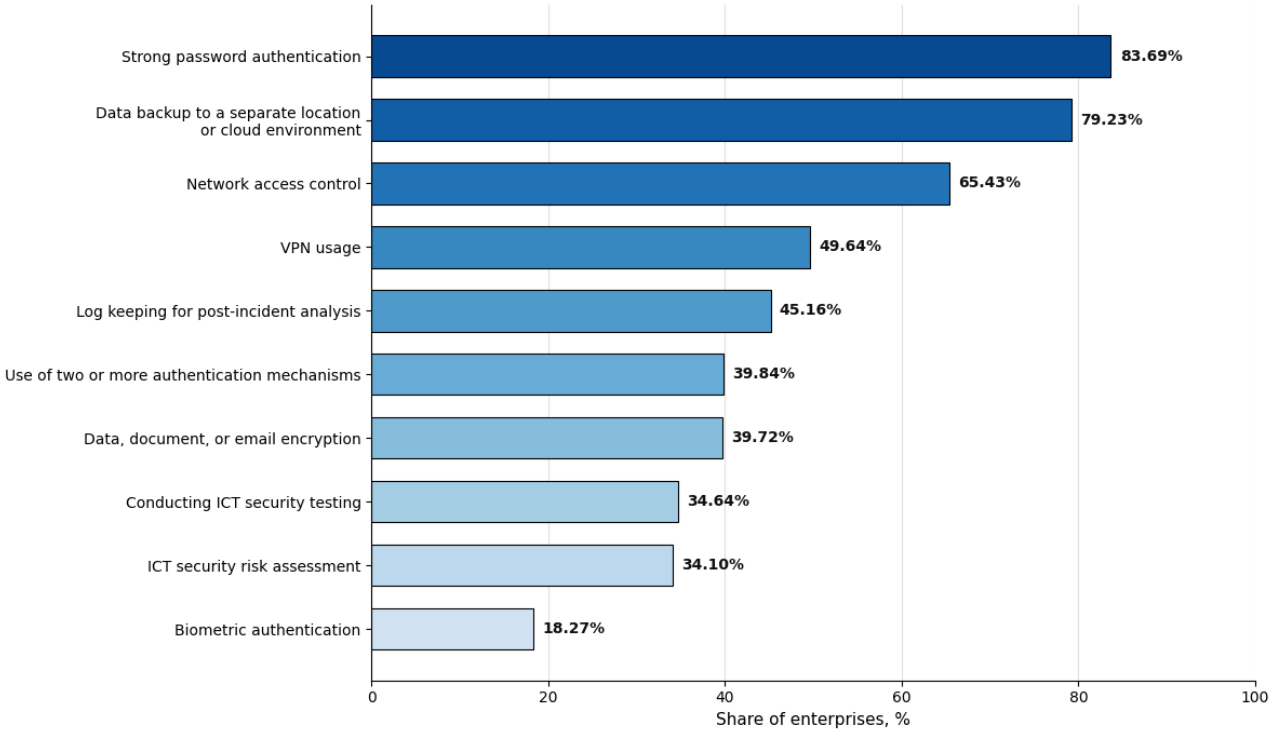


Fig. 1.6. Status of organizational and technical ICT security measures in EU enterprises

Source: compiled based on Eurostat, ICT security in enterprises, 2024.

Therefore, the level of maturity of the digital economy should be assessed not only by the scale of the use of digital and AI technologies but also by the ability of economic and social actors to use them safely.

In this context, the European experience is of particular interest to Ukraine. Large-scale cyberattacks targeting government information resources, critical infrastructure, businesses, and digital public services demonstrate that digital

transformation under current conditions should take place simultaneously with the development of a cyber-resilience system. For Ukraine, adapting European approaches should involve integrating digital transformation, AI development, and cybersecurity into a unified system of state and corporate policies aimed at ensuring the continuity of the digital economy, protecting information resources, and increasing society's resilience to large-scale cyber threats.

Thus, the logic of modern digital evolution can be presented as a gradual transition from the digitization of information and digitalization of individual processes to digital transformation, an AI-based digital economy, and, as its integral dimension, a cyber-resilient economy – an economy capable of creating and using digital value under conditions of continuous cyber threats. It is precisely the combination of technological innovation, institutional capacity, and cyber resilience that determines the quality and long-term effectiveness of the digital transformation of the economy and society.

REFERENCES FOR SUBSECTION 1.1

1. Acemoglu D. The simple macroeconomics of AI. NBER Working Paper. 2024. No. 32487. Cambridge, MA: National Bureau of Economic Research. DOI: 10.3386/w32487. URL: https://doi.org/10.3386/w32487 (accessed: 18.08.2026).

2. Aghion P., Jones B. F., Jones C. I. Artificial intelligence and economic growth. In: The Economics of Artificial Intelligence: An Agenda / eds. A. Agrawal, J. Gans, A. Goldfarb. Chicago: University of Chicago Press, 2019. P. 237–282. URL: https://www.nber.org/books-and-chapters/economics-artificial-intelligence/artificial-intelligence-and-economic-growth (accessed: 18.08.2026).

3. Drago C., Costantiello A., Savorgnan M., Leogrande A. Macroeconomic and Labor Market Drivers of AI Adoption in Europe: A Machine Learning and Panel Data Approach. Economies. 2025. Vol. 13, No. 8. Article 226.

4. European Commission, Joint Research Centre. Advancing AI adoption: strengths and gaps in the European Digital Innovation Hubs Network [Electronic resource]. Luxembourg: Publications Office of the European Union, 2025. URL:

https://publications.jrc.ec.europa.eu/repository/handle/JRC141305 (accessed: 05.09.2026).

5. European Commission. State of the Digital Decade 2026: progress made, but gaps remain [Electronic resource]. Brussels, 17 June 2026. URL: https://commission.europa.eu/news-and-media/news/state-digital-decade-report-progress-made-gaps-remain-2026-06-17_en (accessed: 05.09.2026).

6. European Commission. Study on Cloud and AI Development in the EU [Electronic resource]. Brussels, 2026. URL: https://digital-strategy.ec.europa.eu/en/library/study-cloud-and-ai-development-eu (accessed: 05.09.2026).

7. European Commission. The futures of artificial intelligence [Electronic resource]. Luxembourg: Publications Office of the European Union, 2026. URL: https://op.europa.eu/en/publication-detail/-/publication/3c2e9d55-482a-11f1-8095-01aa75ed71a1/language-en

8. Eurostat. ICT security in enterprises. Statistics Explained. 2024. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises (accessed: 05.09.2026).

9. Eurostat. 8% of EU enterprises used AI technologies in 2023 [Electronic resource]. 2024. URL: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240529-2 (accessed: 13.08.2026).

10. Eurostat. 20% of EU enterprises use AI technologies [Electronic resource]. 2025. URL: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20251211-2 (accessed: 13.08.2026).

11. Eurostat. Digital economy and society statistics – households and individuals [Electronic resource]: Statistics Explained. 2026. URL: https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/33472.pdf (accessed: 13.08.2026).

12. Eurostat. Skills for the digital age [Electronic resource]: Statistics Explained. 2026. URL: https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/124994.pdf (accessed: 13.08.2026).

13. Eurostat. The use of artificial intelligence technologies in the European Union: key results. 2026 edition [Electronic resource]. Luxembourg: Publications Office of the European Union, 2026. 48 p. URL: https://ec.europa.eu/eurostat/web/products-statistical-reports/w/ks-01-26-009 (accessed: 05.09.2026). DOI: 10.2785/9221093.

14. Eurostat. Usage of AI technologies increasing in EU enterprises [Electronic resource]. 2025. URL: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250123-3 (accessed: 13.08.2026).

15. Ferrando A., Lamboglia S., Rariga J., Schmidt M. Adoption and investment in AI across the euro area: insights from harmonised firm-level data [Electronic resource] / A. Ferrando, S. Lamboglia, J. Rariga, M. Schmidt. ECB Occasional Paper Series. 2026. No. 395. 66 p. URL: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op395.en.pdf (accessed: 05.09.2026).

16. Ferrando A., Lamboglia S., Rariga J., Schmidt M. What separates firms that use AI intensively from firms that don’t? [Electronic resource]. The ECB Blog. 2026. 24 June. URL: https://www.ecb.europa.eu/press/blog/date/2026/html/ecb.blog20260624~44f70da110.en.html (accessed: 05.09.2026).

17. Filippucci F., Gal P., Jona-Lasinio C., Leandro A., Nicoletti G. The impact of artificial intelligence on productivity, distribution and growth: key mechanisms, initial evidence and policy challenges. OECD Artificial Intelligence Papers. 2024. No. 15. Paris: OECD Publishing. DOI: 10.1787/8d900037-en. URL: https://doi.org/10.1787/8d900037-en (accessed: 18.08.2026).

18. Global Cybersecurity Outlook 2026. World Economic Forum. 2026. January. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2026/ (accessed: 05.09.2026).

19. Gong C., Ribiere V. Developing a unified definition of digital transformation. Technovation. 2021. Vol. 102. Article 102217. DOI: https://doi.org/10.1016/j.technovation.2020.102217.

20. Iansiti M., Lakhani K. R. Digital ubiquity: How connections, sensors, and data are revolutionizing business. Harvard Business Review. 2014. Vol. 92, No. 11. P. 19–20.

21. IBM. Cost of a Data Breach Report 2025: the AI oversight gap [Electronic resource]. Armonk, NY: IBM Corporation, 2025. URL: https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai (accessed: 05.09.2026).

22. Kyrylov Y., Hranovska V., Savchenko V., Kononenko L., Gai O., Kononenko S. Sustainable Rural Development in the Context of the Implementation of Digital Technologies and Nanotechnology in Education and Business. Nanotechnology Perceptions. 2024. P. 297–323. DOI: https://doi.org/10.62441/nano-ntp.v20iS8.25.

23. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology. 2023. January. NIST SP 1270. URL: https://doi.org/10.6028/NIST.SP.1270.

24. Riedl R., Stieninger M., Muehlburger M. et al. What is digital transformation? A survey on the perceptions of decision-makers in business. Information Systems and e-Business Management. 2024. Vol. 22. P. 61–95.

25. The futures of artificial intelligence: implications for Europe's R&I ecosystem. Part 3, A forward-looking analysis of European industries' artificial intelligence use / Z. Martinaitis, V. Kravchyk, M. Chachava; European Commission, Directorate-General for Research and Innovation. Luxembourg: Publications Office of the European Union, 2025. 76 p. ISBN 978-92-68-35138-3. DOI: 10.2777/5038456. URL: https://op.europa.eu/en/publication-detail/-/publication/3c2e9d55-482a-11f1-8095-01aa75ed71a1/language-en (accessed: 18.08.2026).

26. Tian Y., Ou L. Exploring the influencing mechanisms of different digital transformation stages: an industry perspective. Enterprise Information Systems. 2024. Vol. 18, No. 12. DOI: https://doi.org/10.1080/17517575.2024.2417407.

27. Verhoef P. C., Broekhuizen T., Bart Y., Bhattacharya A., Dong J. Q., Fabian N., Haenlein M. Digital transformation: A multidisciplinary reflection and research agenda. Journal of Business Research. 2021. Vol. 122. P. 889–901.

28. Vial G. Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems. 2019. Vol. 28, No. 2. P. 118–144.

29. The Global Risks Report 2026. World Economic Forum. 2026. 14 January. URL: https://www.weforum.org/publications/global-risks-report-2026/ (accessed: 05.09.2026).

30. Kaida I. F. Digital transformation as a key factor in increasing the competitiveness of Ukrainian business. Economy and Society. 2025. Issue 72. DOI: 10.32782/2524-0072/2025-72-103.

31. Kudinova A. Integration of artificial intelligence technologies into the system of security-oriented management of the national economy in the era of Industry 5.0. Sustainable Development of the Economy. 2025. No. 5 (56). P. 545–553.

32. Silchenko V. proposes defining the relevant phenomenon as changes caused by the implementation and use of digital (information and communication) technologies. In: Silchenko V. V. Approaches to interpreting the definition of "digital transformation". Economy and Society. 2024. No. 66. DOI: https://doi.org/10.32782/2524-0072/2024-66-132.

1.2. Responsible Implementation of Artificial Intelligence as a Factor of Digital Transformation of the Ukrainian Economy: European Experience and Prospects for Adaptation

Victoria VASYUTA,
Vasyl VASYUTA
National University "Yuri Kondratyuk Poltava Polytechnic"

Digital transformation is one of the key factors of modern socio-economic development, significantly changing the principles of functioning of economic systems, business processes, the labour market, and mechanisms of public regulation. One of the key technologies that determines the pace and directions of these transformations is artificial intelligence (AI). Due to its ability to automate complex processes, analyse large amounts of data, support management decision-making, and

create new digital products and services, artificial intelligence technologies are becoming an important driver of innovation and increasing the competitiveness of national economies. At the same time, the rapid spread of AI creates new challenges related to algorithm transparency, protection of fundamental human rights, information security, non-discrimination, responsibility for decisions made, and the development of public trust in digital technologies (Floridi, 2023; OECD, 2024).

For Ukraine, the issue of responsible implementation of artificial intelligence is particularly important in the context of the digital transformation of the economy, post-war recovery, and deeper European integration. Obtaining candidate status for membership in the European Union, harmonisation of national legislation with European standards, development of the digital economy, and implementation of strategic documents in the field of digitalization create the need to adapt modern approaches to the use of AI in accordance with the principles established in European digital policy. In this context, not only the technological implementation of intelligent systems is important, but also the development of an institutional, regulatory, and ethical environment that ensures their safe, transparent, and human-centred use.

In recent years, the European Union has developed a comprehensive approach to the regulation and development of artificial intelligence technologies based on a combination of innovation and responsibility. The adoption of the Artificial Intelligence Act, the implementation of the Digital Europe Programme and the Digital Decade 2030 policy, the European Declaration on Digital Rights and Principles, as well as recommendations of the OECD, UNESCO, and NIST have created the basis for the modern concept of Responsible AI. This concept includes risk management, transparency, accountability, fairness, safety, and respect for human rights in the development and use of artificial intelligence systems. For Ukraine, this experience has significant practical value; however, its effective use requires adaptation to national economic, institutional, and social conditions.

The issues of digital transformation, the development of artificial intelligence technologies, and their legal and ethical regulation are actively studied by both Ukrainian and foreign researchers. L. Floridi, J. Cowls, A. Jobin, M. Coeckelbergh, J. Morley, P. Hacker, and other researchers have made significant contributions to the

development of the concept of responsible artificial intelligence. Important methodological guidelines are also provided by documents of the European Commission, OECD, UNESCO, NIST, the United Nations, and other international institutions, which define modern approaches to the development of the digital economy and the responsible use of AI.

At the same time, an analysis of current scientific studies shows that most research focuses on specific aspects of artificial intelligence use, including regulatory and legal frameworks, ethical principles, risk management, technical characteristics of AI systems, or sector-specific features of their application. At the same time, the comprehensive adaptation of the European experience of responsible artificial intelligence implementation to the conditions of the digital transformation of the Ukrainian economy remains insufficiently developed. Approaches to integrating strategic digital development goals, Responsible AI principles, institutional support, implementation tools, and a system for evaluating results within a single conceptual mechanism require further scientific justification.

The aim of the research is to substantiate the theoretical foundations of responsible artificial intelligence implementation as a factor of the digital transformation of the Ukrainian economy, to generalize European experience, and to develop a conceptual mechanism for its adaptation to national development conditions.

In recent years, the issues of digital transformation of the economy and responsible implementation of artificial intelligence have become one of the key areas of interdisciplinary research. The rapid development of artificial intelligence technologies and their active implementation in production processes, services, public administration, and social life have created the need to reconsider traditional approaches to digitalization. Modern research is gradually shifting its focus from analysing the technological capabilities of artificial intelligence to ensuring its safe, transparent, ethical, and human-centred use, which is reflected in the concepts of Trustworthy AI, Ethical AI, and Responsible AI (Floridi, Cowls, 2019; Jobin et al., 2019; Floridi, 2023).

An analysis of current scientific literature makes it possible to identify several interconnected areas of research. The first area focuses on understanding the role of

artificial intelligence as a driving force of the digital transformation of the economy and society. Studies by international organizations emphasize that artificial intelligence technologies are becoming one of the key factors of economic growth, labour productivity, the development of digital markets, and the creation of new models of value creation (OECD, 2024; Stanford University, 2025; World Economic Forum, 2025). At the same time, researchers emphasize that the effectiveness of digital transformation depends not only on the scale of digital technology implementation but also on the level of public trust in these technologies.

The second area covers research into the ethical foundations of artificial intelligence use. Important works in this field include studies by L. Floridi and J. Cowls, which proposed a system of basic principles for the functioning of artificial intelligence, as well as the work of A. Jobin, M. Ienca, and E. Vayena, which summarized international experience in developing ethical recommendations for the use of artificial intelligence technologies (Floridi, Cowls, 2019; Jobin et al., 2019). These ideas were further developed in the works of M. Coeckelbergh (2020), J. Morley et al. (2020), and L. Floridi (2023), which examine mechanisms for the practical implementation of ethical principles in the development and use of artificial intelligence systems.

A separate area of current research is related to the development of the concept of Trustworthy AI and its transformation into the more comprehensive approach of Responsible AI. Scientific literature indicates that responsible implementation of artificial intelligence involves the integration of technological, ethical, legal, and organizational requirements aimed at ensuring the safe use of artificial intelligence systems, minimizing risks, and protecting fundamental human rights (Díaz-Rodríguez et al., 2023; Morley et al., 2020). Thus, current research considers responsible artificial intelligence not as a separate set of ethical principles, but as a comprehensive model of interaction between technology, public regulation, business, and society.

Official documents of the European Union and international organizations play a special role in the development of this field. The starting point for the formation of the modern European model was the document Ethics Guidelines for Trustworthy AI (High-Level Expert Group on AI, 2019), which for the first time systematized the key

requirements for reliable and human-centred artificial intelligence. These provisions were further developed in the OECD AI Principles (OECD, 2024), the Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021), the Artificial Intelligence Risk Management Framework (NIST, 2023), and the Artificial Intelligence Act (European Parliament and the Council, 2024). This demonstrates the evolution from ethical recommendations to comprehensive legal regulation of artificial intelligence use.

In Ukraine, the development and regulation of artificial intelligence are currently at an active stage of formation. The main strategic documents include the Concept of Development of Artificial Intelligence in Ukraine (Cabinet of Ministers of Ukraine, 2020) and the White Paper on Artificial Intelligence Regulation in Ukraine (Ministry of Digital Transformation of Ukraine, 2024). These documents define the key areas of national policy in the field of artificial intelligence and focus on the gradual harmonization of this policy with European approaches.

At the same time, an analysis of current scientific literature shows that the majority of studies focus on particular aspects of artificial intelligence development, such as ethical principles, legal regulation, risk management, or digital transformation. However, the responsible implementation of artificial intelligence specifically as a factor of the digital transformation of the Ukrainian economy, in the context of adapting the modern European model of AI regulation and development, remains insufficiently studied. This scientific gap determines the relevance and logic of further research.

Digital transformation is one of the key processes in the development of the modern economy. It involves profound changes in the ways value is created, business processes are organized, public institutions operate, and economic actors interact. Unlike digitalization, which primarily involves converting information and individual processes into digital form, digital transformation is characterized by a comprehensive rethinking of economic models based on the widespread use of digital technologies, data, and innovative approaches (European Commission, 2021; OECD, 2024).

The initial stage of the development of the digital transformation concept was mainly associated with the automation of production and management processes, the

development of information and communication technologies, and the implementation of electronic services. During this period, digital technologies were primarily considered as a tool for improving the efficiency of enterprises and public institutions. However, the rapid development of cloud computing, big data, the Internet of Things, and artificial intelligence significantly expanded the meaning of digital transformation, turning it into a systemic process of structural modernization of the economy and society (European Commission, 2021; United Nations, 2024).

At the current stage, artificial intelligence is increasingly recognized as a key technology of digital transformation. Its use enables the automation of decision-making, intelligent analysis of large amounts of data, forecasting of economic processes, optimization of production, development of personalized digital services, and creation of new business models. According to international experts, the widespread implementation of artificial intelligence technologies is one of the main factors contributing to higher labour productivity, innovation activity, and global competitiveness of economies (Stanford University, 2025; World Economic Forum, 2025).

At the same time, accumulated practical experience in the use of artificial intelligence systems has shown that digital transformation cannot be assessed only by the pace of technological development or the scale of automation. The spread of algorithmic decision-making, generative artificial intelligence models, and digital platforms has increased the importance of algorithm transparency, personal data protection, information security, non-discrimination, responsibility for the results of intelligent systems, and public trust in new technologies (Floridi, 2023; Hacker, 2023).

Therefore, the modern understanding of digital transformation is gradually moving beyond the technological approach. Strategic documents of the European Union emphasize that digital development should be human-centred, inclusive, secure, and based on the protection of fundamental human rights (European Commission, 2023; European Commission, 2021). This approach means a transition from the concept of technological digitalization to a model of responsible digital transformation, in which the effectiveness of digital technology implementation is determined not only

by its innovative potential but also by the level of public trust, transparency, and compliance with ethical and legal standards.

In this context, artificial intelligence should be considered not only as a tool of digital transformation but also as a technology whose socio-economic impact directly depends on the model of its implementation. This circumstance has led to the development of new conceptual approaches – Ethical AI, Trustworthy AI, Human-Centric AI, and Responsible AI – which define modern guidelines for the development of the digital economy and have become the basis of European policy in the field of artificial intelligence.

The evolution of the concept of digital transformation of the economy in the context of the development of artificial intelligence technologies is presented in Figure 1.7.

Thus, the evolution of the concept of digital transformation demonstrates a shift in its main focus: from the automation of individual processes and the digitization of information to the comprehensive transformation of economic systems, in which artificial intelligence plays a key role. At the same time, the current stage of development of the digital economy shows that achieving sustainable socio-economic outcomes depends not only on the level of technological development but also on the ability to ensure the responsible implementation of innovations based on the principles of human-centeredness, transparency, safety, and trust.

The rapid spread of artificial intelligence technologies across all areas of economic activity has created not only new opportunities for digital transformation but has also highlighted a range of ethical, social, legal, and technological challenges. While at the early stages of its development artificial intelligence was mainly considered a tool for automating and improving the efficiency of economic processes, the growing autonomy of intelligent systems has led the academic community to pay increasing attention to issues of responsibility for the results of their operation, algorithmic transparency, non-discrimination, protection of human rights, and building trust in digital technologies (Floridi, 2023; Hacker, 2023).

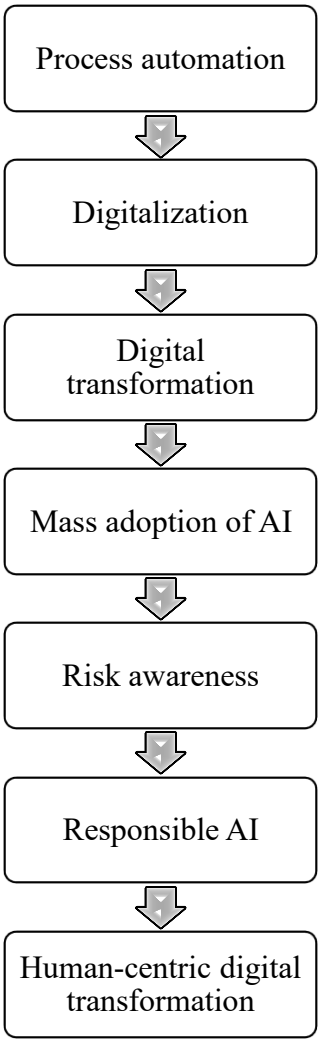


Fig. 1.7. Evolution of the Concept of Digital Transformation of the Economy in the Context of the Development of Artificial Intelligence Technologies

Source: compiled by the authors based on High-Level Expert Group on AI (2019); UNESCO (2021); European Commission (2021, 2023, 2024); OECD (2024).

The evolution of scientific approaches to the use of artificial intelligence demonstrates a gradual shift from a narrow technological perspective to a comprehensive understanding of its role in socio-economic development. One of the first systematic approaches was the concept of "Ethical AI", which focuses on the moral principles underlying the development and use of artificial intelligence systems. Its formation is based on widely recognized ethical principles, including respect for human rights, fairness, non-discrimination, prevention of harm, accountability, and transparency (Floridi, Cowls, 2019). A review of the international experience in developing ethical guidelines conducted by A. Jobin, M. Ienca, and E. Vayena showed

that, regardless of national characteristics, most ethical documents are based on similar fundamental values, although the mechanisms for their practical implementation differ significantly (Jobin et al., 2019).

The further development of conceptual approaches led to the formation of the "Trustworthy AI" model, which combines ethical principles with requirements for the functioning of artificial intelligence systems. The document "Ethics Guidelines for Trustworthy AI", prepared by the High-Level Expert Group on AI at the European Commission, played a key role in its development (High-Level Expert Group on AI, 2019). It proposed a comprehensive approach to assessing the trustworthiness of artificial intelligence, based on the principles of lawfulness, ethics, and technical robustness of AI systems. It also identified seven key requirements, including human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity and non-discrimination, societal and environmental well-being, and accountability.

Further development of digital technologies demonstrated that ensuring trustworthiness characteristics alone is not sufficient for the effective use of artificial intelligence in the economy. This contributed to the development of the broader concept of "Responsible AI", which shifts the focus from the characteristics of an individual technology to the entire life cycle of AI systems – from the design and training of models to their deployment, operation, monitoring, and assessment of their socio-economic impacts. In current research, responsible artificial intelligence is considered as an integration of ethical principles, legal requirements, risk-management mechanisms, and organizational practices that ensure the safe and socially acceptable use of intelligent systems (Morley et al., 2020; Díaz-Rodríguez et al., 2023).

An important stage in the development of the responsible artificial intelligence concept was its establishment in international regulatory and policy documents. The UNESCO "Recommendation on the Ethics of Artificial Intelligence" defined global principles for the development and use of AI, focused on the protection of human rights, inclusiveness, and sustainable development (UNESCO, 2021). The OECD principles specified the need to combine innovation and development with accountability, transparency, and risk management (OECD, 2024). Practical risk-

management mechanisms were proposed in the NIST framework (NIST, 2023), while the adoption of the "Artificial Intelligence Act" represented a logical transition from non-binding recommendations to a comprehensive legal framework for regulating artificial intelligence in the European Union (European Parliament and the Council, 2024).

Thus, the modern understanding of Responsible AI has emerged as a result of the gradual evolution of scientific concepts and international regulatory practice. While the Ethical AI concept defines a system of fundamental values, Trustworthy AI establishes requirements for the characteristics of intelligent systems, and Responsible AI covers the entire process of their development, deployment, and use, integrating ethical, legal, organizational, and technological dimensions. It is precisely this comprehensive approach that currently defines the strategic directions of digital transformation of the economy in the countries of the European Union.

A comparative analysis of modern concepts of the responsible development and implementation of artificial intelligence is presented in Table 1.3.

Table 1.3

Comparative Characteristics of Modern Concepts of the Responsible Development and Implementation of Artificial Intelligence

Concept	**Main Focus**	**Key Characteristics**	**Role in Responsible AI Implementation**
Ethical AI	Ethical values	Fairness, human rights, non-discrimination	Establishes a system of ethical principles
Trustworthy AI	System properties	Transparency, safety, accountability, human oversight	Builds trust in AI systems
Human-Centric AI	Human-centered approach	Priority given to human rights, freedoms, and well-being	Directs AI development towards human needs
Responsible AI	Comprehensive model	Ethical, legal, organizational, and technological mechanisms	Ensures comprehensive responsible implementation of AI in economic and social processes

Source: compiled by the authors based on Floridi, Cowls, 2019; Jobin et al., 2019; High-Level Expert Group on AI, 2019; Morley et al., 2020; Díaz-Rodríguez et al., 2023; OECD, 2024.

The analysis provides grounds for arguing that the concepts of Ethical AI, Trustworthy AI, and Responsible AI are not identical but reflect different stages in the evolution of scientific understanding of the role of artificial intelligence in society and the economy. Their relationship lies in the gradual expansion of their scope: from defining ethical principles to developing a comprehensive model for the responsible implementation and use of artificial intelligence. In this context, Responsible AI can be considered an integral concept that combines ethical values, requirements for system trustworthiness, risk-management mechanisms, and regulatory and legal frameworks, ensuring a balanced combination of innovative development, protection of human rights, and public trust.

The current stage of digital transformation of the economy is characterized not only by the widespread use of digital technologies but also by a significant increase in the role of artificial intelligence as a general-purpose technology capable of changing mechanisms of value creation, the organization of production processes, resource management, and interaction between economic actors. The use of artificial intelligence systems creates new opportunities for automation, intelligent data analysis, forecasting, service personalization, and the development of innovative business models, contributing to higher labor productivity, enterprise competitiveness, and the development of the digital economy (OECD, 2024; Stanford University, 2025).

At the same time, international experience shows that the positive impact of artificial intelligence on economic development is not an automatic consequence of its technological implementation. The use of algorithmic systems without due consideration of ethical, legal, and social aspects may increase the risks of discrimination, violations of the right to privacy, lack of transparency in decision-making processes, declining public trust in digital technologies, and greater regulatory uncertainty (UNESCO, 2021; NIST, 2023; European Parliament and the Council, 2024).

Therefore, the modern European model of digital transformation is based on the understanding that innovation and responsibility are not mutually exclusive categories. On the contrary, the responsible implementation of artificial intelligence is considered a necessary prerequisite for sustainable economic development, as it contributes to

building trust in digital technologies, reducing the risks associated with their use, and creating a predictable regulatory environment for innovation (European Commission, 2023; OECD, 2024).

In this context, the responsible implementation of artificial intelligence should be considered as a comprehensive process covering all stages of the life cycle of intelligent systems – from design and model training to integration, operation, monitoring, and improvement. This approach involves adherence to the principles of human-centeredness, transparency, safety, accountability, fairness, and risk management, ensuring a balance between technological innovation, economic efficiency, and public interests (High-Level Expert Group on AI, 2019; Morley et al., 2020; Díaz-Rodríguez et al., 2023).

From the perspective of economics, the responsible implementation of artificial intelligence creates the conditions for sustainable competitive advantages. A high level of trust in digital technologies encourages their wider use by businesses and consumers, reduces transaction costs associated with controlling and mitigating risks, increases the investment attractiveness of digital innovations, and contributes to the development of new markets for digital products and services. Thus, the economic effect of using artificial intelligence is determined not only by its functional capabilities but also by the quality of the institutional environment in which it is implemented.

For Ukraine, these issues are particularly relevant in the context of European integration, digital modernization of the economy, and post-war recovery. Adapting European principles of responsible AI use should contribute not only to harmonizing national legislation with European Union law but also to developing a modern digital innovation ecosystem focused on increasing economic competitiveness, supporting entrepreneurship, attracting investment, and strengthening trust in digital services.

Summarizing the results of the analysis, it can be argued that under current conditions of digital transformation, the decisive factor in achieving long-term socio-economic effects is not the mere use of artificial intelligence technologies but the model of their implementation. Responsible implementation, which combines innovation with adherence to ethical principles, legal requirements, risk-management mechanisms, and the protection of human rights, builds trust in digital technologies,

creates conditions for their widespread use in the economy, and increases the effectiveness of digital transformation.

Based on the analysis, we propose considering the responsible implementation of artificial intelligence as a comprehensive mechanism for ensuring the digital transformation of the economy that integrates technological, ethical, legal, organizational, and institutional components. Unlike approaches in which artificial intelligence is viewed primarily as a technological resource, the proposed approach emphasizes that the quality of its implementation determines the level of public trust, the scale of practical use, and the final economic outcomes of digital transformation.

In this regard, we propose the following original definition: "Responsible implementation of artificial intelligence is a comprehensive process of developing, integrating, using, and monitoring artificial intelligence systems, carried out on the basis of human-centeredness, ethical principles, transparency, safety, accountability, and risk management, ensuring respect for fundamental human rights, building public trust in digital technologies, and creating conditions for sustainable development and increased economic competitiveness."

The European Union was among the first in the world to develop a comprehensive approach to the regulation and implementation of artificial intelligence that combines support for innovation with the protection of fundamental human rights, the safety of digital technologies, and the development of trust in their use. Unlike models focused primarily on stimulating technological development or minimizing government intervention, the European approach is based on the integration of ethical, legal, technological, and economic mechanisms that ensure the responsible use of artificial intelligence systems (European Commission, 2023; OECD, 2024). The modern European model of responsible AI implementation was developed gradually (Table 1.4).

The first stage involved defining the basic ethical principles for the use of artificial intelligence. In 2019, the High-Level Expert Group on AI published the document Ethics Guidelines for Trustworthy AI, which established the conceptual foundation for subsequent European Union policy. The proposed principles of human-centeredness, transparency, technical robustness, accountability, fairness, and non-

discrimination became the foundation for the development of subsequent regulatory and strategic documents (High-Level Expert Group on AI, 2019).

Table 1.4.

Evolution of the European Model of Responsible Artificial Intelligence Implementation

Stage	Key Document	Main Outcome
Ethical	Ethics Guidelines for Trustworthy AI	Development of responsible AI principles
Strategic	Digital Europe Programme, Digital Decade Policy Programme 2030	Definition of strategic development priorities
International and Practical	OECD AI Principles, UNESCO Recommendation, NIST AI RMF	Development of universal approaches and tools for Responsible AI
Regulatory	Artificial Intelligence Act	Establishment of a comprehensive legal framework

Source: compiled by the authors based on an analysis of regulatory and strategic documents of the EU and international organizations.

The further development of the European approach was associated with a transition from ethical recommendations to the formation of a comprehensive digital transformation policy. The Shaping Europe's Digital Future strategy and the Digital Europe and Digital Decade 2030 programmes identified artificial intelligence as one of the key tools for increasing the competitiveness of the European economy, developing digital skills, strengthening the innovation ecosystem, and expanding digital infrastructure. At the same time, these documents emphasize that economic development should be pursued in compliance with the principles of safety, inclusiveness, human-centeredness, and the protection of fundamental rights (European Commission, 2021; European Commission, 2023).

The next stage involved the development of practical mechanisms for ensuring the responsible use of artificial intelligence. The OECD Principles and the UNESCO Recommendation contributed to the harmonization of international approaches to AI

ethics, while the NIST AI Risk Management Framework provided tools for identifying, assessing, and mitigating risks throughout the life cycle of artificial intelligence systems. Thus, the European model gradually evolved from the normative definition of values to the creation of practical mechanisms for their implementation (UNESCO, 2021; NIST, 2023; OECD, 2024).

The logical culmination of this process was the adoption of the Artificial Intelligence Act, which, for the first time in international practice, introduced a comprehensive legal framework for artificial intelligence based on a risk-based approach. The Act establishes different requirements for AI systems depending on the level of potential risk, combining the protection of human rights with support for innovation. This approach creates a predictable regulatory environment for the development of the digital economy and contributes to increasing business and public trust in the use of artificial intelligence technologies (European Parliament and the Council, 2024).

Thus, the modern European model of responsible AI implementation is the result of the gradual integration of ethical principles, strategic digital development priorities, risk-management tools, and legal regulatory mechanisms. Its distinctive feature is its focus not only on technological progress but also on creating conditions for sustainable economic development, strengthening trust in digital technologies, and ensuring their social acceptance.

The development of the European model of responsible AI implementation is not limited to defining ethical principles or adopting regulatory acts. Its effectiveness is largely ensured by a system of interconnected instruments covering legal, institutional, organizational, financial, and technological mechanisms (Fig. 1.8). Their comprehensive application creates conditions for the balanced development of innovation, risk minimization, and the formation of trust in digital technologies.

A key element of the legal framework of the European model is the Artificial Intelligence Act, which introduces a risk-based approach to the regulation of artificial intelligence systems. Unlike traditional technology regulation, the Act classifies AI systems according to their level of potential risk and establishes differentiated requirements for their development, deployment, and use. This approach makes it

possible to protect human rights while avoiding unnecessary restrictions on innovation, thereby creating a predictable legal environment for businesses (Regulation (EU) 2024/1689, 2024).

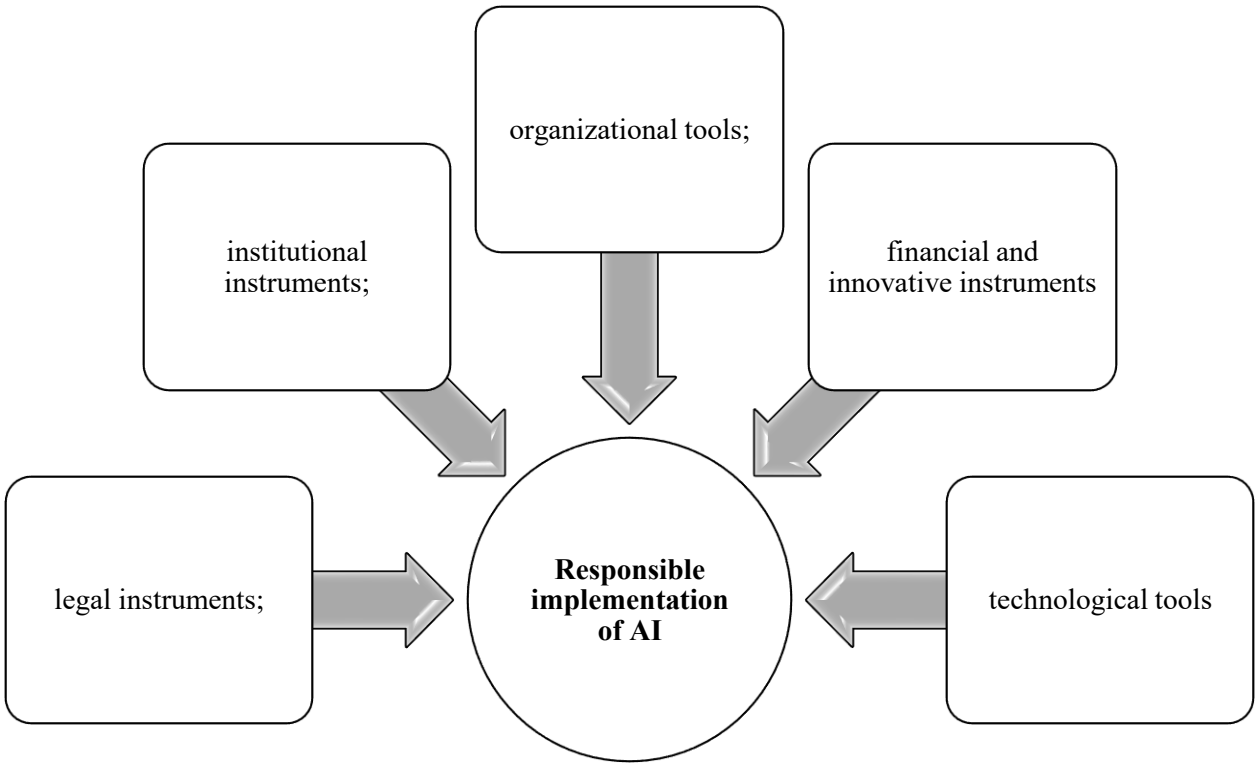


Fig. 1.8. System of instruments for ensuring the responsible implementation of artificial intelligence in the European model of digital transformation
Source: developed by the authors based on Regulation (EU) 2024/1689, 2024; Novelli et al., 2024; NIST, 2023; Morley et al., 2020; European Commission, 2021.

An important component of the European model is the creation of an institutional system for coordinating and overseeing the implementation of artificial intelligence. The AI Act provides for the operation of the AI Office, European Artificial Intelligence Board, and national competent authorities, which ensure consistency in the application of the legislation, coordination among Member States, exchange of experience, and monitoring of technological developments (Novelli et al., 2024). The establishment of such institutions contributes to greater effectiveness of public policy in the field of artificial intelligence and ensures the stability of the regulatory environment.

The European model provides for organizational mechanisms aimed at managing risks throughout the entire life cycle of artificial intelligence systems. These include conformity assessment, documentation of development processes, ensuring human oversight, internal audits, monitoring the operation of systems after their deployment, and mechanisms for responding to identified risks. Particular attention is paid to establishing internal risk-management procedures at the organizational level, which is consistent with current approaches to the corporate governance of digital innovations (NIST, 2023; Morley et al., 2020).

Alongside regulatory mechanisms, the European Union actively uses financial instruments to stimulate digital transformation. The Digital Europe Programme and Horizon Europe are aimed at developing digital infrastructure, supporting scientific research, creating innovation ecosystems, developing digital competencies, and implementing artificial intelligence technologies across various sectors of the economy. European Digital Innovation Hubs also play an important role by providing enterprises, particularly small and medium-sized enterprises, with access to expert support, digital solution testing, and advanced technological infrastructure (European Commission, 2021).

Another area involves technological mechanisms for ensuring the responsible use of artificial intelligence. These include standardization, testing systems before their widespread deployment, the use of AI regulatory sandboxes, data quality assessment, ensuring cybersecurity, and continuous monitoring of algorithm performance. Such tools make it possible to identify potential risks at an early stage, improve the trustworthiness of artificial intelligence systems, and create conditions for the safe implementation of innovation (Regulation (EU) 2024/1689, 2024; NIST, 2023).

The analysis shows that the effectiveness of the European model is ensured not by individual instruments but by their interaction.

Legal mechanisms create a predictable regulatory environment; institutional mechanisms ensure coordination and oversight; organizational mechanisms integrate the principles of responsible AI use into the practices of organizations; financial mechanisms stimulate innovation activity; and technological mechanisms support the safe implementation of digital solutions.

The combination of these instruments creates conditions for increasing trust in digital technologies, reducing transaction costs, increasing the investment attractiveness of digital projects, and strengthening the competitiveness of the economy (Table 1.5).

Table 1.5

Економічне значення інструментів відповідального впровадження ШІ

Instrument	Main Purpose	Expected Economic Effect
Legal	Reduction of regulatory uncertainty	Increased investment attractiveness
Institutional	Coordination and oversight	Improved consistency of digital transformation processes
Organizational	Risk management and process control	Reduced losses and increased efficiency of business processes
Financial and innovation-related	Support for innovation	Accelerated digital transformation of businesses
Technological	Ensuring system trustworthiness	Increased trust in digital solutions

Source: compiled by the authors based on Regulation (EU) 2024/1689; OECD, 2024; NIST, 2023; UNESCO, 2021.

The analysis allows us to conclude that a distinctive feature of the European model of responsible AI implementation is its comprehensive nature.

Unlike approaches that focus primarily on regulatory frameworks or ethical aspects, the European model integrates legal, institutional, organizational, financial, and technological instruments into a unified system. Their interaction ensures not only an appropriate level of safety and trust in artificial intelligence technologies but also creates favorable conditions for innovation and the digital transformation of the economy.

The analysis shows that the European model of responsible AI implementation has developed in conditions of a high level of digital maturity of the economy, a developed institutional environment, stable regulatory and legal frameworks, and significant investment in digital innovation. Therefore, its use in Ukraine cannot be limited to the mechanical adoption of individual regulatory acts or organizational solutions. Much greater attention should be paid to adapting the conceptual foundations of the European approach to Ukraine's national socio-economic conditions, digital development priorities, and European integration course.

Ukraine has already taken a number of important steps towards developing public policy in the field of artificial intelligence. The adoption of the Concept for the Development of Artificial Intelligence in Ukraine and the White Paper on the Regulation of Artificial Intelligence demonstrates an intention to harmonize the national approach with contemporary European principles. At the same time, these documents are primarily strategic in nature and define general development directions, while practical mechanisms for responsible AI implementation are still at the stage of development.

Unlike the European Union, where the Responsible AI model is supported by a developed system of institutions, financial instruments, and risk-assessment mechanisms, digital transformation in Ukraine is taking place under conditions of wartime challenges, the need for post-war economic recovery, limited financial resources, and simultaneous large-scale institutional reforms. Therefore, the priority should not be the complete replication of the European model but the identification of those of its elements that can generate the greatest economic effect in the medium term.

In our view, the priority areas for adapting European experience include the development of a transparent regulatory environment, strengthening institutional capacity in the field of artificial intelligence, integrating risk-management mechanisms into organizational practices, supporting research and innovation, and developing digital competencies. An important factor in successful adaptation is ensuring cooperation among the state, business, the academic community, and civil society, which is consistent with contemporary principles of multi-stakeholder governance of digital transformation.

The economic dimension of responsible AI implementation is of particular importance. Establishing clear rules for the use of intelligent systems, supporting innovation, and increasing trust in digital technologies may contribute to greater investment activity, the development of high-tech entrepreneurship, higher labor productivity, and the integration of Ukrainian companies into the European digital market. In this context, responsible AI implementation should be considered not only as an element of public policy but also as a tool for increasing the competitiveness of the national economy.

Thus, the practical value of European experience for Ukraine lies not in the possibility of directly copying individual regulatory or organizational solutions but in applying a systemic approach to AI development. The comprehensive combination of legal, institutional, organizational, financial, and technological instruments can create trust in digital innovations, establish a favorable environment for their widespread adoption, and increase the effectiveness of digital transformation of the Ukrainian economy.

The analysis leads to the conclusion that adapting European experience should be based not on the principle of "copying regulatory solutions" but on the principle of "adapting a systemic model." Such an approach involves taking into account the specific features of Ukraine's institutional development, the economic challenges of the wartime and post-war periods, and the strategic objectives of European integration. Under these conditions, responsible AI implementation can become one of the factors contributing to the innovation capacity, competitiveness, and resilience of the national economy.

To further specify the proposed conceptual mechanism, it is appropriate to identify the key areas for adapting the European experience of responsible AI implementation to the current conditions of digital transformation of the Ukrainian economy. Such a systematization makes it possible to assess the current state of individual components, determine their development priorities, and outline the expected results of implementing the relevant measures (Table 1.6).

The presented matrix demonstrates that adapting European experience is not limited to the implementation of individual regulatory acts or technological solutions.

Table 1.6.

Matrix for Adapting the European Experience of Responsible Artificial Intelligence Implementation to the Conditions of Digital Transformation of the Ukrainian Economy

Element of the European Model	Current State in Ukraine	Adaptation Priority	Expected Effect
Regulatory Framework	Under development	High	Predictability of the regulatory environment
Institutional System	Partially established	High	Increased effectiveness of public policy
Risk Management	Fragmentary application	High	Reduction of technological and reputational risks
Innovation Support	Developing	Medium	Accelerated digital modernization
Digital Competencies	Require further development	High	Increased labor productivity
Trust in AI	At the development stage	High	Wider adoption of digital technologies

Source: developed by the authors based on an analysis of European Commission, 2024; OECD, 2024; UNESCO, 2021; NIST, 2023.

It involves the comprehensive development of the institutional environment, the risk-management system, human capital, the innovation ecosystem, and mechanisms for building trust in artificial intelligence technologies. The coordinated development

of these components ensures the practical implementation of the proposed conceptual mechanism and creates the conditions for effective digital transformation of the Ukrainian economy.

The results of the analysis show that the European model of responsible AI implementation has developed as an integrated system that combines ethical principles, regulatory and legal frameworks, institutional support, risk-management mechanisms, and instruments for supporting innovation. At the same time, its effectiveness is largely determined by the specific socio-economic conditions of the Member States of the European Union, the level of development of the digital economy, and the institutional capacity of public authorities. This necessitates the adaptation rather than the mechanical transfer of European approaches to Ukraine's national practice.

For Ukraine, responsible AI implementation is particularly relevant in the context of simultaneous digital transformation, pursuit of European integration, and post-war economic recovery. The use of artificial intelligence technologies is gradually expanding in public administration, the financial sector, industry, logistics, healthcare, agriculture, and other areas of economic activity. Alongside new opportunities, there is a growing need to ensure algorithmic transparency, manage risks, protect data, develop digital competencies, and build trust in intelligent systems (Cabinet of Ministers of Ukraine, 2020; Ministry of Digital Transformation of Ukraine, 2024).

An important prerequisite for adaptation is also the harmonization of Ukrainian legislation with European Union law. Granting Ukraine candidate status for EU membership has increased the need for the gradual alignment of the national regulatory environment with European approaches, particularly in the areas of the digital economy and the use of artificial intelligence. At the same time, adaptation should not be reduced to the formal implementation of individual provisions of the AI Act. It is more appropriate to adopt the systemic logic of the European model, which provides for the coordinated functioning of legal, institutional, organizational, financial, and technological instruments.

In our view, the systemic nature of adaptation should determine the further development of public policy in the field of artificial intelligence. Under current conditions, it is important not only to establish an appropriate regulatory framework

but also to develop a mechanism that ensures the practical implementation of the principles of responsible AI implementation in economic activity. Such a mechanism should be aimed at supporting innovation, minimizing risks, increasing trust in digital technologies, and strengthening the competitiveness of the economy.

The synthesis of the results of the first and second sections provides grounds for arguing that the mechanism for adapting the European model should be considered as an interconnected system of elements whose functioning ensures the integration of the principles of responsible AI use into the processes of digital transformation of the Ukrainian economy. Its development should be based on a comprehensive approach that takes into account both international experience and national specificities of socio-economic development.

nlike approaches focused primarily on harmonizing the regulatory and legal framework, the proposed approach considers the adaptation of the European model as a multi-component mechanism in which legal provisions are only one of several interconnected elements. Institutional capacity, the development of digital competencies, innovation support, risk management, and the formation of public trust in artificial intelligence technologies are also of critical importance. It is their comprehensive interaction that creates the conditions for effective digital transformation of the Ukrainian economy.

The analysis of theoretical approaches, international recommendations, and the practice of AI regulation in the countries of the European Union has demonstrated that the effective use of artificial intelligence technologies requires not only an appropriate regulatory and legal framework but also a comprehensive system of interconnected elements that ensure their practical implementation. Therefore, the adaptation of European experience to the conditions of Ukraine should be considered as an integrated mechanism that combines strategic objectives, principles, stakeholders, instruments, and implementation processes for responsible AI implementation. The conceptual model of the proposed mechanism is presented in Figure 1.9.

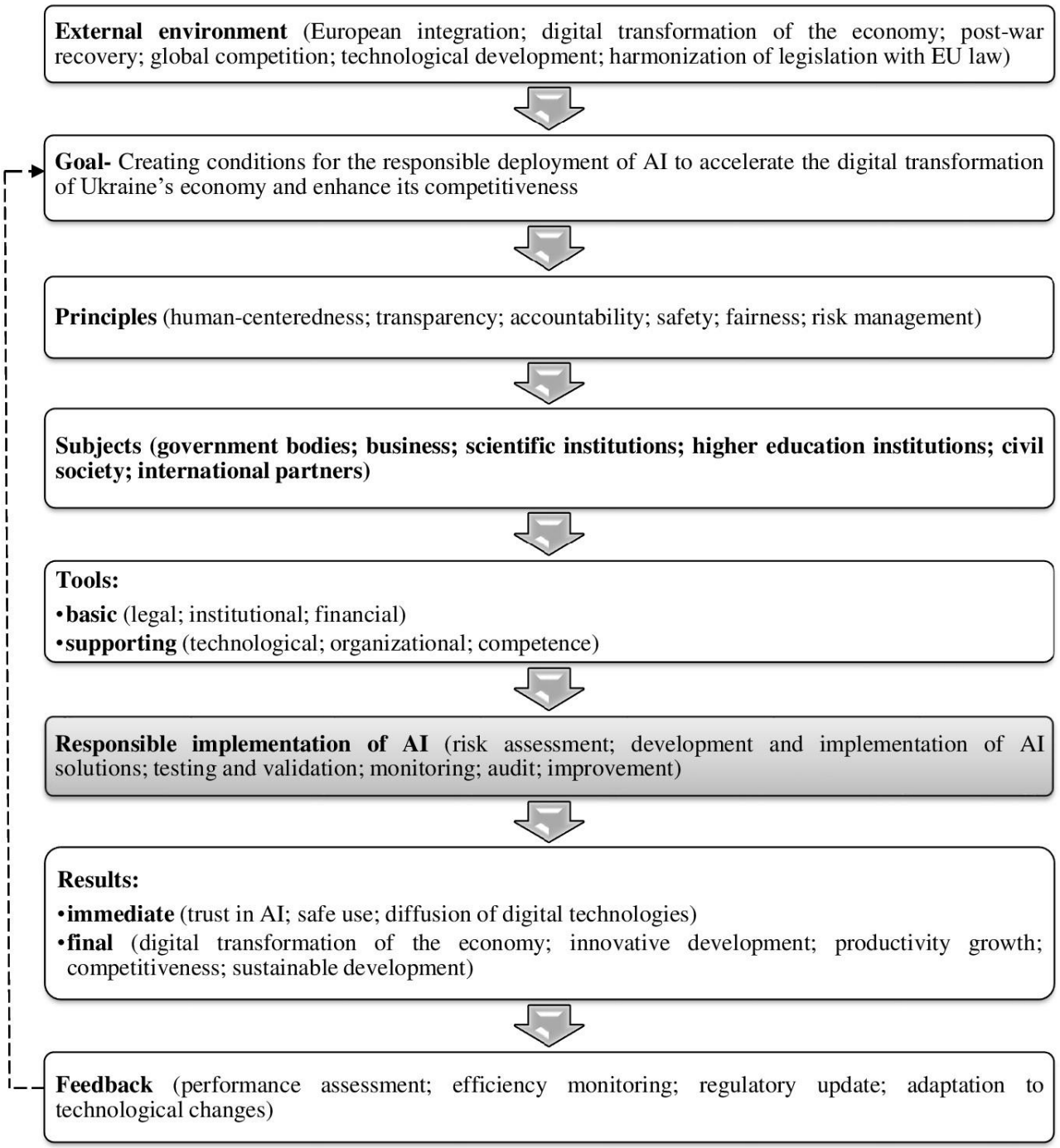


Fig. 1.9. Conceptual Model of the Mechanism for Adapting the European Experience of Responsible Artificial Intelligence Implementation to the Conditions of Digital Transformation of the Ukrainian Economy

Source: developed by the authors based on a synthesis of European approaches to responsible artificial intelligence implementation (AI Act, OECD AI Principles, UNESCO Recommendation on the Ethics of Artificial Intelligence, NIST AI RMF, etc.).

In our view, the mechanism for adapting the European experience of responsible artificial intelligence implementation represents an interconnected set of legal, institutional, organizational, financial, technological, and competency-based instruments. Their implementation ensures the integration of Responsible AI principles into the process of digital transformation of the Ukrainian economy, taking into account national development specificities, current challenges, and the strategic priorities of European integration.

The proposed model is based on a systemic approach, according to which the functioning of the mechanism is determined by the influence of the external environment, which includes the processes of European integration, digital transformation of the economy, post-war recovery of Ukraine, technological development, global competition, and harmonization of national legislation with European Union law. The combination of these factors creates the prerequisites for the implementation of modern digital technologies and determines public policy priorities in the field of artificial intelligence.

The purpose of the mechanism is to create conditions for the responsible implementation of artificial intelligence as one of the key factors of digital transformation of the Ukrainian economy and to increase its competitiveness. This goal is achieved through the implementation of a set of principles consistent with modern international approaches to Responsible AI, including human-centeredness, transparency, accountability, fairness, safety, and a risk-based approach.

An important place in the proposed model is occupied by the stakeholders involved in implementing the mechanism. Their interaction ensures the comprehensive nature of adapting European experience and creates conditions for the coordinated development of the digital economy. Key stakeholders include public authorities, business entities, research institutions, higher education institutions, civil society, and international partners.

The practical implementation of the mechanism is carried out through a system of interconnected instruments. Legal instruments ensure the development of a

regulatory environment for the use of artificial intelligence; institutional instruments support the development of the organizational capacity of relevant authorities and institutions; financial instruments stimulate innovation activity; organizational instruments coordinate interaction among participants in the process; technological instruments support the development of digital infrastructure and the practical use of AI solutions; and competency-based instruments contribute to the development of digital competencies and a culture of responsible AI use.

The central element of the model is the process of responsible AI implementation, which covers risk assessment, development, testing, practical deployment, monitoring, auditing, and continuous improvement of intelligent systems. This process ensures the transformation of regulatory principles and strategic decisions into actual economic outcomes.

The functioning of the mechanism is aimed at achieving two interconnected groups of results. Immediate results include increased trust in artificial intelligence technologies, ensuring their safe use, and the wider adoption of AI solutions across various sectors of the economy. The ultimate results include accelerated digital transformation of the economy, development of innovation activity, increased labor productivity, strengthened competitiveness of the national economy, and sustainable development.

The proposed model has a cyclical nature. Through the feedback system, the results of implementing the mechanism are continuously assessed, making it possible to improve the regulatory and legal framework, adapt instruments to technological changes, and ensure the continuous development of the responsible AI implementation system.

The characteristics of the structural elements of the conceptual model of the mechanism for adapting the European experience of responsible artificial intelligence implementation to the conditions of digital transformation of the Ukrainian economy are presented in Table 1.7.

Table 1.7.

Characteristics of the Structural Elements of the Conceptual Model of the Mechanism for Adapting the European Experience of Responsible Artificial Intelligence Implementation to the Conditions of Digital Transformation of the Ukrainian Economy

Structural Element	Content	Function in the Mechanism
External Environment	European integration, digital transformation of the economy, post-war recovery, technological development, global competition, harmonization of legislation	Creates the prerequisites for the functioning of the mechanism and determines its strategic development directions
Purpose	Creating conditions for the responsible implementation of artificial intelligence as a factor of digital transformation of the Ukrainian economy	Directs the activities of all stakeholders towards achieving strategic outcomes
Principles	Human-centeredness, transparency, accountability, fairness, safety, risk-based approach	Define the fundamental principles of the mechanism and ensure compliance with international Responsible AI standards
Stakeholders	Public authorities, business, research institutions, higher education institutions, civil society, international partners	Ensure the development, coordination, and practical implementation of the mechanism
Instruments	Legal, institutional, organizational, financial, technological, and competency-based	Create organizational, regulatory, resource, and human-capital conditions for responsible AI implementation
Responsible Artificial Intelligence Implementation	Risk assessment, design, testing, deployment, monitoring, auditing, and improvement of AI solutions	Ensures the practical implementation of Responsible AI principles in digital transformation processes
Results	Increased trust in AI, safe use of technologies, development of the digital economy, innovation activity, labor productivity, competitiveness	Reflect the socio-economic effects of implementing the mechanism
Feedback	Monitoring, performance evaluation, updating the regulatory framework, improving instruments, adaptation to technological changes	Ensures continuous improvement of the mechanism in response to changes in the external environment

Source: developed by the authors.

The proposed conceptual model reflects the relationship between the strategic objectives of digital transformation of the Ukrainian economy and the instruments for adapting the European experience of responsible artificial intelligence implementation. Unlike approaches that focus primarily on the regulatory and legal aspects of AI regulation, the proposed model integrates the external conditions of its functioning, a system of principles, the stakeholders involved, a set of instruments, the practical implementation process, and a feedback mechanism. This makes it possible to consider responsible AI implementation not as a separate area of digital policy but as a comprehensive mechanism that ensures the alignment of technological development, institutional capacity, and the economic priorities of the state.

The implementation of the proposed mechanism for adapting the European experience of responsible artificial intelligence implementation is aimed at achieving a set of interconnected outcomes covering the institutional, technological, economic, and social dimensions of digital transformation of the Ukrainian economy. Unlike approaches focused primarily on the regulatory and legal aspects of artificial intelligence, the proposed mechanism is aimed at creating an integrated system of interaction among the state, business, the scientific community, and society, thereby creating the conditions for the large-scale and responsible implementation of AI solutions (Fig. 1.10).

The first group consists of immediate results that characterize the changes arising during the implementation of the mechanism. These primarily include the development of a modern regulatory environment harmonized with European approaches to artificial intelligence regulation, strengthening the institutional capacity of public authorities and other stakeholders involved in digital transformation, and expanding practices of responsible use of AI technologies. An important outcome is an increase in the level of digital competencies among employees, managers, researchers, and citizens, which will contribute to the more effective and safe use of intelligent systems in various areas of economic activity (OECD, 2024; UNESCO, 2021).

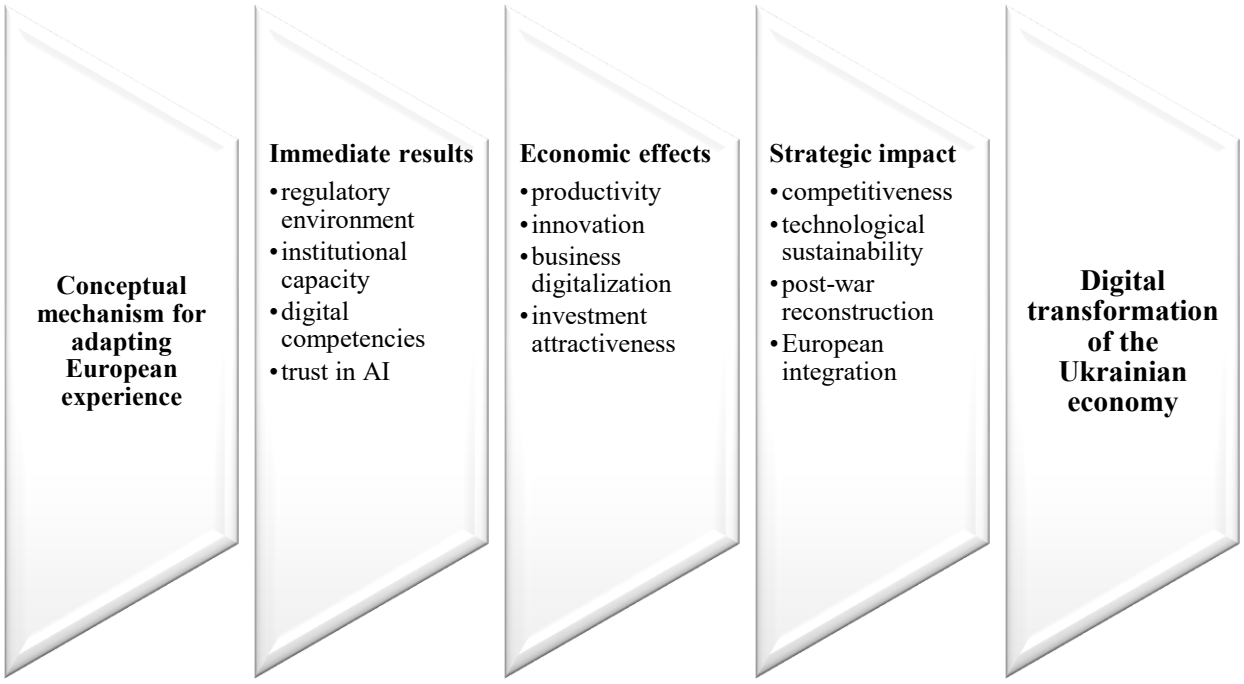


Fig. 1.10. Conceptual Model of the Transformation of Responsible Artificial Intelligence Implementation Outcomes into Strategic Effects of Digital Transformation of the Ukrainian Economy

Source: developed by the author.

Particular importance is attached to increasing public trust in artificial intelligence technologies. International experience shows that user trust, algorithmic transparency, adherence to ethical principles, and effective risk management determine the readiness of businesses and society to adopt innovative digital solutions (Floridi, 2023; OECD, 2024). In this context, responsible AI implementation is not only a technological but also a social prerequisite for digital transformation.

The second group of results is related to the economic effects of implementing the proposed mechanism. The systematic use of artificial intelligence technologies, provided that the principles of Responsible AI are observed, creates conditions for increasing labor productivity, optimizing business processes, reducing transaction costs, accelerating management decision-making, and improving resource efficiency. In addition, the wider adoption of AI solutions will stimulate innovation activity among enterprises, the development of digital entrepreneurship, and the creation of new high-tech jobs, which is consistent with current global trends in the development of the digital economy (Stanford University, 2025; World Economic Forum, 2025).

At the same time, the economic effect of implementing the mechanism is not limited to individual enterprises. At the national economy level, responsible AI implementation will contribute to increasing Ukraine's investment attractiveness, expanding opportunities to participate in European digital initiatives, intensifying international scientific and technological cooperation, and integrating Ukraine into the European Union's Digital Single Market. Taken together, these factors will create additional opportunities for accelerating structural modernization of the economy and developing the innovation ecosystem.

A separate group consists of strategic outcomes that have a long-term nature. They should be considered as the result of the consistent implementation of all elements of the proposed mechanism. These outcomes include increased competitiveness of the national economy, the development of resilient digital infrastructure, strengthened technological capacity of the state, development of human capital, and the creation of conditions for sustainable socio-economic development. These outcomes are particularly important in the context of Ukraine's post-war recovery, when digital technologies can become one of the key instruments for modernizing the economy, improving the efficiency of public administration, developing entrepreneurship, and integrating into the European economic space (European Commission, 2023; United Nations, 2024).

Thus, the proposed mechanism not only ensures the adaptation of the European experience of responsible AI implementation to national conditions but also creates an integrated system of relationships between the strategic objectives of digital transformation, the principles of Responsible AI, the institutional environment, and the expected socio-economic outcomes. Its practical implementation will contribute to a transition from fragmented use of AI technologies to the systemic development of the Ukrainian digital economy based on the principles of safety, transparency, inclusiveness, and innovation.

The study confirmed that, under conditions of rapid digital technology development, responsible AI implementation is of strategic importance as one of the key factors of digital transformation of the Ukrainian economy. Unlike approaches that view artificial intelligence primarily as a technological tool or an object of regulatory

and legal regulation, this article substantiates the need for its comprehensive implementation based on human-centeredness, transparency, safety, accountability, and risk management in accordance with contemporary European and international approaches.

The study established that the modern European model of responsible AI implementation is developing as an integrated system of interconnected legal, institutional, technological, and ethical instruments aimed at ensuring innovative development while simultaneously respecting fundamental human rights, maintaining public trust, and ensuring the safe use of AI technologies. The analysis of European Union regulatory documents, international recommendations, and recent academic research demonstrated that a risk-based approach, the development of digital competencies, cross-sectoral cooperation, and systematic monitoring of effectiveness are key components of successful digital transformation of the economy.

The main result of the study is the development of a conceptual mechanism for adapting the European experience of responsible artificial intelligence implementation to the conditions of digital transformation of the Ukrainian economy. The proposed mechanism combines a strategic objective, the principles of Responsible AI, a set of stakeholders, a comprehensive set of implementation instruments, the process of responsible AI implementation, expected outcomes, and a feedback system. Unlike existing approaches, it focuses not only on adapting individual European practices but also on developing an integrated model for their incorporation, taking into account Ukraine's economic, institutional, and social specificities.

It has been substantiated that the practical implementation of the proposed mechanism will contribute to creating a favorable environment for the responsible use of artificial intelligence, developing digital competencies, increasing the innovation activity of enterprises, strengthening trust in AI solutions, increasing labor productivity, intensifying international scientific and technological cooperation, and harmonizing national approaches with European digital policy. In the strategic perspective, this will create the conditions for increasing the competitiveness of the Ukrainian economy, accelerating its post-war recovery, and deepening its integration into the European digital space.

Therefore, responsible artificial intelligence implementation should be considered not only as one of the factors of digital transformation of the Ukrainian economy but also as a comprehensive process whose effectiveness is determined by the functioning of a mechanism for adapting European experience to national development conditions. The systemic combination of international Responsible AI principles with the needs of the Ukrainian economy provides the foundation for developing a safe, inclusive, innovative, and competitive digital economy.

REFERENCES FOR SUBSECTION 1.2

1. Floridi L. AI as Agency Without Intelligence: On ChatGPT, Large Language Models, and Other Generative Models. Philosophy & Technology. 2023. URL: https://doi.org/10.1007/s13347-023-00621-y

2. OECD. OECD AI Principles. Paris: OECD Publishing, 2024. URL: https://www.oecd.org/en/topics/ai-principles.html

3. Floridi L., Cowls J. A Unified Framework of Five Principles for AI in Society. Harvard Data Science Review. 2019. URL: https://doi.org/10.1162/99608f92.8cd550d1

4. Jobin A., Ienca M., Vayena E. The Global Landscape of AI Ethics Guidelines. Nature Machine Intelligence. 2019. No. 1. P. 389–399. URL: https://doi.org/10.1038/s42256-019-0088-2

5. OECD. OECD Digital Economy Outlook 2024. URL: https://www.oecd.org/en/publications/oecd-digital-economy-outlook-2024-volume-1_a1689dc5-en.html

6. Stanford University. AI Index Report 2025. URL: https://hai.stanford.edu/ai-index/2025-ai-index-report

7. World Economic Forum. The Future of Jobs Report 2025. URL: https://www.weforum.org/publications/the-future-of-jobs-report-2025/

8. Coeckelbergh M. AI Ethics. Cambridge, MA: MIT Press, 2020. URL: https://doi.org/10.7551/mitpress/12549.001.0001

9. Morley J., Floridi L., Kinsey L., Elhalal A. From What to How: An Overview of AI Ethics Tools, Methods and Research to Translate Principles into Practices. Science and Engineering Ethics. 2020. No. 26. P. 2141–2168. URL: https://doi.org/10.1007/s11948-019-00165-5

10. Díaz-Rodríguez N., Del Ser J., Coeckelbergh M. et al. Connecting the Dots in Trustworthy Artificial Intelligence: From AI Principles, Ethics, and Key Requirements to Responsible AI Systems and Regulation. Information Fusion. 2023. Vol. 99. Article 101896. URL: https://doi.org/10.1016/j.inffus.2023.101896

11. High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI. Brussels: European Commission, 2019. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

12. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO, 2021. URL: https://unesdoc.unesco.org/ark:/48223/pf0000380455

13. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg, MD: NIST, 2023. URL: https://doi.org/10.6028/NIST.AI.100-1

14. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

15. Cabinet of Ministers of Ukraine. On Approval of the Concept for the Development of Artificial Intelligence in Ukraine: Resolution of the Cabinet of Ministers of Ukraine No. 1556-r of 2 December 2020. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

16. White Paper on Artificial Intelligence Regulation in Ukraine: Vision of the Ministry of Digital Transformation / comp. H. Rumiantsev. Kyiv: Ministry of Digital Transformation of Ukraine, 2024. 30 p. URL: https://dspace.mipolytech.education/handle/mip/2822

17. European Commission. Digital Europe Programme 2021–2027. URL: https://digital-strategy.ec.europa.eu/en/activities/digital-programme

18. United Nations. E-Government Survey 2024. URL: https://publicadministration.un.org/egovkb/en-us/reports/un-e-government-survey-2024

19. Hacker P. Regulating ChatGPT and Other Large Generative AI Models. In: FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency. 2023. P. 1112–1123. URL: https://doi.org/10.1145/3593013.3594067

20. European Commission. European Declaration on Digital Rights and Principles for the Digital Decade. 2023. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023C0123(01)

21. European Commission. The Digital Decade Policy Programme 2030. URL: https://digital-strategy.ec.europa.eu/en/library/digital-decade-policy-programme-2030

22. European Commission. Shaping Europe's Digital Future. URL: https://digital-strategy.ec.europa.eu/en

23. Novelli C., Hacker P., Morley J., Trondal J., Floridi L. A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities. European Journal of Risk Regulation. 2024. P. 1–25. URL: https://doi.org/10.1017/err.2024.57

1.3. Institutional and regulatory frameworks for information security in the context of digital transformation: the experience of European Union countries and the adaptation of Ukrainian legislation

Svitlana ONYSHCHENKO,
Oleksandra MASLIY
National University "Yuri Kondratyuk Poltava Polytechnic"

The digital transformation of the economy and society is fundamentally altering not only the technological environment but also the very approach to state regulation, risk management and the assurance of information security. The development of artificial intelligence, digital platforms and network infrastructure requires the

simultaneous establishment of an appropriate institutional and legal framework capable of ensuring the security, resilience and accountability of digital processes. Otherwise, a regulatory gap and a mismatch arise between the pace of technological change and the capacity of the state and society to develop the legal, organisational and technical mechanisms required to manage new risks promptly.

Over the past decade, the European Union has developed one of the world's most comprehensive information security regulatory frameworks, encompassing personal data protection, the cybersecurity of critical infrastructure, the security of digital products and the liability of digital platforms. Meanwhile, it is important to clearly distinguish between two levels of analysis of this system, which are often confused in academic discourse despite being essentially different in scope for scholarly research. The first level is supranational, represented by EU directives and regulations establishing minimum harmonised standards for all Member States. The second level is the national level, where each Member State implements these standards through the lens of its own institutional traditions, administrative culture, and security context; as a result, the practical architecture of information security varies significantly even within the EU's single legal space. The divergence of these national models, despite the formal unity of the underlying regulatory framework, is precisely what makes a comparative analysis necessary; without it, the harmonisation of Ukrainian legislation with the EU acquis risks being reduced to a mere formal copying of the texts of directives, without taking into account the institutional prerequisites that make these provisions effective in practice.

This distinction matters for Ukraine not merely in theory but also in practice. The experience of previous rounds of EU expansion, particularly the 2004 Central European wave, represented by Estonia and Poland, demonstrates that the formal adoption of transposed legislation (known as 'paper harmonisation') is a necessary but obviously inadequate condition for functional compliance with the EU acquis. Genuine compliance requires the development of institutional capacity – namely, in terms of human resources, finance and organisation – capable of applying the adopted rules in practice.

The EU's regulatory framework for information security was established not as a single act, but as a series of interlinked legal instruments, each of which addressed the new challenges posed by the next stage of digital transformation.

The cornerstone of the entire personal data protection framework remains 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 (General Data Protection Regulation, GDPR), which became applicable on 25 May 2018. The GDPR introduced a harmonised approach to the processing of personal data across the European Union, enshrining the principles of lawfulness, transparency, purpose limitation and data minimisation. It also established substantial administrative fines of up to EUR 20 million or 4% of the total worldwide annual turnover and, importantly, extended the territorial scope of its provisions to certain controllers and processors established outside the Union where they process the personal data of data subjects in the Union in connection with the offering of goods or services or the monitoring of their behaviour. The Regulation has effectively become an influential global regulatory benchmark, commonly associated in academic literature with the "Brussels effect", subsequently shaping data protection legislation and regulatory practices in numerous jurisdictions beyond the European Union.

The first horizontal cybersecurity instrument was Directive (EU) 2016/1148 (NIS Directive), which established the initial requirements for operators of essential services and digital service providers. Its practical implementation revealed significant shortcomings, including fragmented approaches across the Member States, a limited range of regulated sectors, and weak mechanisms for cross-border coordination. In response, 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 (NIS2 Directive) was adopted (European Parliament and Council of the European Union, 2022). It entered into force on 16 January 2023.

NIS2 has significantly expanded the scope of regulation by introducing a distinction between "essential entities" and "important entities", depending on the type, size and significance of their activities. The scope of the Directive covers 18 sectors,

grouped into two categories: 11 high-criticality sectors and 7 other critical sectors. These include energy, transport, the banking sector, financial market infrastructure, healthcare, water supply and sanitation, digital infrastructure, ICT service management, public administration, the space sector, postal and courier services, waste management, the production, manufacture and distribution of chemicals, the production, processing and distribution of foodstuffs, digital service providers and research organisations.

Another important regulatory development was the measures for managing cybersecurity risks set out in Article 21, which cover, in particular, policies on risk analysis and the security of information systems, incident response, business continuity and crisis management, supply chain security, cryptography and encryption, access control and multi-factor authentication. Article 23 establishes a multi-stage mechanism for the mandatory reporting of significant incidents: an early warning must be submitted within 24 hours of the entity becoming aware of the incident; a report on the incident must be submitted within 72 hours; and a final report must be submitted no later than one month after receipt of such a report.

Furthermore, the governing bodies of major and significant entities are required to approve measures for managing cybersecurity risks, monitor their implementation, and may be held liable for violating the relevant requirements; members of governing bodies must also undergo cybersecurity training. For breaches of the requirements of Articles 21 and 23, the maximum administrative fines for key entities shall be at least €10 million or 2 per cent of the total annual turnover for the previous financial year, and for significant entities – at least €7 million or 1.4 per cent of the relevant turnover, whichever is higher. Member States were required to transpose the provisions of the Directive into national law by 17 October 2024; nevertheless, as discussed in more detail below based on the example of Poland, this process has been delayed in several Member States.

In 2024, the regulatory framework was further complemented by Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act, CRA, 2024). For the first time at the EU level, the CRA introduces mandatory cybersecurity requirements at the design and development stages of

hardware and software, thereby embedding the principle of security by design. It also requires manufacturers to report identified vulnerabilities and actively exploited vulnerabilities within 24 hours and provides for CE marking as evidence of conformity. The Regulation entered into force on 12 November 2024 but will apply from 11 December 2027, thus providing the market with an extended transitional period for adapting production processes.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act, DSA, 2022), which entered into force on 16 November 2022 and has applied since 17 February 2024, complements the legal framework for information security by establishing requirements concerning the moderation of illegal content, the transparency of recommender systems, and the mitigation of systemic risks on very large online platforms. This dimension is of particular importance in the context of hybrid information operations faced by Ukraine.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 deserves special attention on ENISA (the EU Agency for Cybersecurity) and on the certification of information and communication technology cybersecurity (Cybersecurity Act, 2019), which has been in force since 27 June 2019. This legislation fulfils two functions. Firstly, it transformed ENISA, which had been operating since 2004 based on temporary mandates that were periodically renewed, into a permanent agency with a strengthened budget and expanded powers, particularly regarding operational cooperation, capacity-building in Member States and support during large-scale cyber incidents. Secondly, it established the European Cybersecurity Certification Scheme, under which ENISA, on behalf of the European Commission, develops candidate certification schemes for specific categories of ICT products, services and processes; each scheme defines security requirements, assessment methods and one of three levels of assurance – basic, substantial or high. Certificates issued under such a scheme are recognised in all Member States, replacing fragmented national certification schemes (such as the French CSPN or individual schemes of the German BSI) for the categories covered. The first and, to date, the main scheme is the EUCC (Common Criteria-based scheme), formally adopted by Commission Implementing Regulation (EU) 2024/482 in January 2024 and intended for the

certification of ICT hardware and software products, in particular microchips and smart cards; The EUCS scheme for cloud services and the EU5G scheme for fifth-generation networks are also at the development stage; their finalisation is being hampered by political disputes over digital sovereignty requirements concerning cloud service providers outside the EU.

It is worth noting that, unlike the approach involving the adoption of a single "cybersecurity law", the EU's regulatory model is structured as an ecosystem of coordinated horizontal and sector-specific instruments covering, simultaneously, data (GDPR), networks and organisations (NIS2), products (CRA), certification (Cybersecurity Act) and platforms (DSA). This multi-layered architecture is a deliberate institutional choice: it makes it possible to avoid excessive standardisation where the specific nature of sectors requires a differentiated approach, whilst ensuring horizontal consistency in the underlying principles of risk management.

A distinct area of concern within the EU regulatory environment is the governance of the data economy. Although it does not formally fall within the scope of cybersecurity legislation in the narrow sense, it directly shapes the security and trust framework governing cross-border data flows. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act, DGA, 2022), which entered into force on 23 June 2022 and has applied since 24 September 2023, establishes conditions for the re-use of protected public sector data, a mechanism for the notification and supervision of data intermediation services based on the principle of intermediary neutrality, as well as a framework for the voluntary registration of "data altruism" entities. This institutional and regulatory framework for information security is further complemented by Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act), which governs rights of access to data generated by connected products, including Internet of Things devices, and strengthens safeguards against unlawful cross-border requests for access to such data by public authorities of third countries.

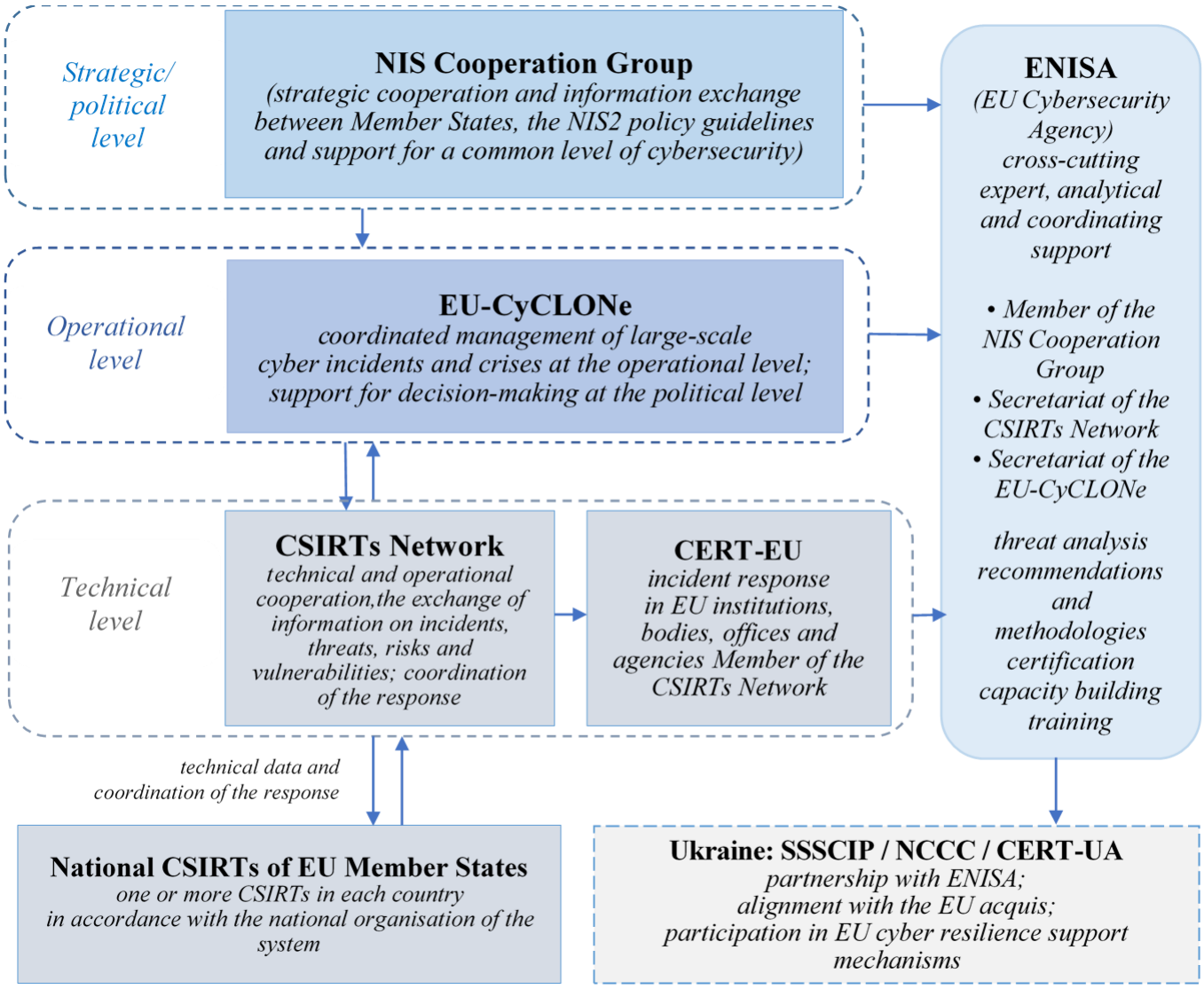
The significance of this regulatory approach for the issues facing the department is twofold. Firstly, it shapes the economic context within which the requirements of NIS2 and the GDPR are implemented: network security and the protection of personal data cannot be viewed in isolation from the broader infrastructure of trust for data

exchange that the DGA is building. Secondly, the logic underlying the DGA and the Data Act—which restricts cross-border access to data from third countries—is structurally akin to the French concept of digital sovereignty; both instruments are designed to safeguard critical data from jurisdictional influence outside the EU, which is directly relevant to the formulation of Ukrainian policy regarding the hosting of government data in the cloud infrastructures of foreign providers.

The effectiveness of the regulatory framework depends, first and foremost, on the level of institutional capacity for its practical implementation. In this regard, the European Union has established a multi-level coordination system, structured across three hierarchical levels. This model (strategic/political, operational and technical levels) serves as an example of institutional implementation that could be adapted in Ukraine, taking into account the country's specific security context, as illustrated in more detail in Fig. 1.3.

ENISA plays a central coordinating and expert-analytical role, carrying out threat analysis and developing technical recommendations for the implementation of NIS2 (in particular the 'NIS2 Technical Implementation Guidance' of June 2025), conducts maturity assessments of critical infrastructure sectors (the annual ENISA NIS360 report, 2025) and publishes the annual ENISA Threat Landscape report.

According to the 2025 edition, which covers the period from July 2024 to June 2025, the agency analysed 4,875 verified incidents. Among the trends in the current EU cyber-threat landscape, ransomware attacks occupy a prominent place; ENISA identifies them as one of the most significant cyber-threats to the European Union. During 2024–2025, the ransomware ecosystem was characterised by further fragmentation, the emergence of new strains and Ransomware-as-a-Service (RaaS) models, occurring, in particular, against a backdrop of large-scale law enforcement operations and intensified internal competition between cybercriminal groups. According to ENISA, 82 variants of ransomware were recorded as having been used against organisations in EU Member States during the period under review (ENISA, 2025).



Note: the diagram illustrates the key coordination mechanisms, rather than a complete list of all EU institutions in the field of cybersecurity.

Fig. 1.3. Institutional framework for information security in the European Union

Source: compiled by the author based on Directive (EU) 2022/2555 (NIS2), Regulation (EU) 2019/881 (Cybersecurity Act), Regulation (EU, Euratom) 2023/2841, the EU Council Recommendation of June 2025 on the EU Cyber Blueprint, and ENISA materials.

At the same time, the use of artificial intelligence technologies in social engineering is on the rise: large language models are being used to create more convincing phishing messages and to automate such attacks. ENISA views the proliferation of artificial intelligence not only as a factor in the scaling up of traditional cyber threats, but also as a source of new vulnerabilities in the digital environment (ENISA, 2025).

Another notable trend is the convergence of different categories of cyber-threat actors: cybercriminal, hacktivist and state-affiliated groups, which manifests itself in the mutual use of tools, infrastructure, tactics, techniques and procedures. ENISA, in particular, has documented the use of ransomware by pro-Russian hacktivist groups. A telling example is CyberVolk, whose activities ENISA characterises as serving Russian interests; since May 2024, the group has used and promoted several variants of ransomware, including AzzaSec, HexaLocker, Parano, LockBit and Chaos (ENISA, 2025).

Alongside monitoring and assessing cyber threats, ENISA also places a strong emphasis on developing human capital and operational readiness in the field of cybersecurity. The European Cybersecurity Skills Framework (ECSF) establishes a common approach to defining the professional roles, competencies, knowledge and skills of specialists, whilst the pan-European Cyber Europe exercises are designed to practise responses to large-scale cyber incidents, identify gaps in procedures and enhance individual and collective capacity for cyber crisis management (ENISA, 2022; ENISA, 2024). Thus, ENISA's toolkit combines analytical and regulatory-methodological mechanisms with the development of professional competencies, operational readiness and cyber resilience at EU and Member State level. Such a system ensures a seamless transition from the detection and technical handling of cyber incidents to the coordination of crisis response and the formulation of strategic decisions. Importantly, for Ukraine in particular, this approach is of interest not as a model to be mechanically replicated, but as an institutional benchmark for further aligning the national cybersecurity system with EU mechanisms, taking into account the specific nature of the security environment and established practices for countering cyber threats.

By examining the technical level of information security in the EU, it is worth noting that the CSIRTs Network, which brings together representatives of incident response teams designated by Member States, as well as CERT-EU, facilitates technical and operational cooperation, the exchange of information on cyber incidents, threats, risks and vulnerabilities, and the coordination of cross-border responses. As a member of the CSIRTs Network, CERT-EU performs specialised functions in

responding to cyber incidents within EU institutions, bodies, offices and agencies. This structure ensures a direct link between national response teams and the institutional framework of the European Union.

At the operational level, the European Cyber Crises Liaison Organisation Network (EU-CyCLONe) plays a decisive role; its functional purpose is the coordinated management of large-scale cyber incidents and crises. Its operations ensure the development of a shared situational awareness, the coordination of Member States' operational actions, and support for decision-making at the political level. The interaction between EU-CyCLONe and the CSIRTs Network creates a mechanism for transitioning from a technical response to an incident to operational coordination should the incident escalate.

At the strategic/political level, the NIS Cooperation Group plays a key role, ensuring strategic cooperation between Member States, the exchange of information and best practices, and facilitating the consistent implementation of the NIS2 requirements. It is at this level that the outcomes of technical and operational responses are transformed into strategic guidelines, recommendations and approaches for the further development of the EU's common cybersecurity policy. At the same time, the functioning of the multi-level institutional framework for cybersecurity coordination established at EU level does not entail the standardisation of national institutional models. At Union level, a system of cooperation between Member States, EU institutions, bodies and agencies has been established, covering the technical, operational and political levels of response to large-scale cyber incidents and crises (Council of the European Union, 2025). A common regulatory framework sets out basic requirements, mechanisms for cooperation and coordination, as well as requirements for national cybersecurity capabilities, whilst the specific organisational arrangements for their implementation are determined by the Member States. NIS2, in particular, requires each Member State to adopt a national cybersecurity strategy, designate one or more competent authorities, a single point of contact, bodies responsible for managing large-scale cyber incidents and crises, and one or more CSIRTs (European Parliament & Council of the European Union, 2022). At the same time, the Directive does not prescribe a single organisational model for these

institutions: Member States determine their structure and the distribution of powers independently, within the established requirements. As a result, the EU's common legal and coordination framework coexists with a diversity of national governance architectures.

A comparative analysis shows that Member States implement common requirements through distinct governance models, shaped by the characteristics of their political systems, the historical development of their institutions, the security environment and administrative practices. Differences can be observed both in the degree of centralisation of cybersecurity governance and in the distribution of powers amongst competent authorities, sectoral regulators and incident response teams. The existence of such differences is also confirmed by the implementation of NIS2, under which Member States designate their own competent authorities and organisational mechanisms within the framework of a common regulatory and legal framework.

Considering the specific features of information security in the European Union, it is worth examining the particular characteristics of the Member States' national cybersecurity models, as it is at the national level that pan-European requirements are given concrete institutional and organisational form. The selection of countries for comparative analysis was based on the principle of maximum variation in institutional structure, provided that they operate within the EU's common legal framework in the field of information and cybersecurity. Four national models were selected for the study, representing distinct approaches to the organisation of cybersecurity and incorporating various institutional solutions that are potentially relevant to Ukraine.

Estonia represents a centrally coordinated but technologically decentralised model, shaped by a high level of state digitalisation and significant practical experience in countering large-scale cyber-attacks. Institutional coordination of cybersecurity is centred primarily within the RIA and its National Cyber Security Centre (NCSC-EE), whilst X-tee/X-Road functions as a distributed environment for secure data exchange between information systems (Information System Authority [RIA], n.d.-a, n.d.-b). Its experience has a direct technological counterpart in Ukraine: the 'Trembita' system for the electronic interaction of state information resources was created on the basis of

technological solutions derived from the Estonian X-Road (e-Governance Academy, 2017).

Germany is characterised by a federal-sectoral model, which combines the coordinating role of the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), multi-level interaction between the federal level and the Länder, and a system of sectoral standards for the protection of critical infrastructure (Federal Office for Information Security [BSI], n.d.-a, n.d.-b).

France demonstrates a more centralised state-security model with a leading role for the National Agency for the Security of Information Systems (Agence nationale de la sécurité des systèmes d'information, ANSSI), which is the national authority in the field of cybersecurity and cyber defence and coordinates the state's defence against cyber-attacks (Agence nationale de la sécurité des systèmes d'information [ANSSI], n.d.-a). The French approach is also characterised by a strong emphasis on strategic autonomy, the protection of critical information systems and the development of trusted digital and cloud services; in particular, the SecNumCloud certification sets high technical, operational and legal requirements for cloud services intended to handle sensitive data (ANSSI, n.d.-b).

Poland represents a multi-level, sectorally coordinated model of a Central and Eastern European state, whose institutional development has taken place in the context of European integration and the subsequent adaptation of the national cybersecurity system to EU requirements. Poland's experience is of particular interest to Ukraine given the combination of a post-socialist institutional legacy, European integration and current security challenges. Poland has been a member of the EU since 1 May 2004 (European Union, 2004), and in 2026 the Act on the National Cybersecurity System (KSC) was amended to implement the requirements of NIS2; the relevant amendment came into force on 3 April 2026 (Ministry of Digital Affairs of Poland, 2026).

The comparison of these models is carried out using a single analytical framework: the institutional prerequisites for the development of the model, the regulatory and legal framework, the key competent authorities and organisational architecture, strengths and institutional constraints, as well as elements relevant to Ukraine. The application of a unified system of criteria ensures the methodological

comparability of national models and makes it possible to identify not a universal ‘best’ model, but rather those institutional solutions that can be taken into account in the further development of Ukraine’s cybersecurity system.

The Estonian model of cybersecurity and digital resilience was shaped to a large extent by experiences of crisis. In April–May 2007, against the backdrop of a political conflict between Estonia and Russia over the relocation of a monument to a Soviet soldier in Tallinn, Estonia’s digital infrastructure was subjected to a large-scale campaign of cyber-attacks. Over a period of 22 days, DDoS attacks targeted the websites of government institutions, the media and the private sector; some attacks also affected online banking and critical network services (Information System Authority [RIA], 2017; Ottis, 2008). The political motivation behind the attacks and their link to the wider conflict surrounding the relocation of the monument are well documented; however, unequivocally attributing these attacks to a specific state remained problematic (NATO, 2007; Ottis, 2008). These events became one of the best-known early examples of a large-scale, politically motivated cyberattack against a state’s digital infrastructure and had a significant impact on the subsequent development of cybersecurity policy in Estonia and NATO.

Meanwhile, the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was not a direct consequence of the 2007 attacks: Estonia proposed the concept to NATO as early as 2004; it was approved in 2006, and the Centre itself was established in Tallinn on 14 May 2008; in October of that year, it received NATO accreditation and the status of an international military organisation (NATO CCDCOE, n.d.). At the same time, the 2007 attacks served as a pivotal catalyst, demonstrating to the Alliance the growing significance of cyber threats and prompting a strengthening of cyber defence policy (NATO, 2019).

The institutional core of the modern Estonian model is the Estonian Information System Authority (Riigi Infosüsteemi Amet, RIA), which coordinates the development and administration of state information systems, ensures their interoperability, organises activities in the field of information security, and responds to incidents in Estonian computer networks (Information System Authority [RIA], 2026). The Estonian National Cyber Security Centre (NCSC-EE) operates within the RIA

structure, whose tasks include round-the-clock monitoring of cyberspace, incident response, protection of critical infrastructure, analysis of cyber threats, crisis management, conducting exercises and developing information security standards (RIA, 2026b).

The technological foundation of the digital state is the X-tee data exchange platform, which is based on X-Road technology. Its architecture is based on a distributed model: information is not stored in a single centralised database but is exchanged between participants' information systems via standardised and secure interaction mechanisms. As of 2026, over 4,500 data exchange services are available via X-tee, with the number of requests standing at around 13 million per day (RIA, 2026). Estonia's well-developed digital infrastructure has enabled the country to achieve the full digitalisation of public services: since December 2024, all the country's public services have been available in electronic format (e-Estonia, 2025).

The concept of a "data embassy" has proved to be an important institutional and technological solution. In fact, on 20 June 2017, Estonia and Luxembourg signed an agreement on the hosting of Estonian data and information systems in Luxembourg's national data centre with the aim of ensuring the country's digital continuity (Government of Estonia, 2017). The project provided for the backup of ten strategically important datasets, including the electronic court system, the State Treasury, the land and commercial registers, the population register, the tax register, identity documents, the cadastral register and the pension register (e-Estonia, n.d.). Legally, the 'digital embassy' is not a diplomatic mission in the traditional sense. Its special legal status is defined by an intergovernmental agreement, which ensures the immunity and protection of Estonian data and information systems hosted in Luxembourg (Riigikogu, 2018). This model aims to ensure the state's digital continuity, that is, the ability to preserve critical data and maintain the functioning of state information systems even in the event of the cessation or disruption of data centre operations within Estonia (Riigikogu, 2018).

Another key component of the Estonian model is the development of public practices in the use of the state's digital tools. Online voting was first introduced in the 2005 local elections and in the 2007 parliamentary elections (Elections in Estonia,

n.d.). The development of e-voting, alongside digital identification, electronic signatures and inter-agency data exchange, has heightened the demands on the reliability and security of the state's digital infrastructure.

The particular relevance of Estonia's experience for Ukraine is confirmed by the direct transfer of technology relating to solutions in the field of inter-agency data exchange. On 26 October 2017, as part of the EGOV4UKRAINE programme, documentation and rights were transferred to the State Agency for Electronic Governance of Ukraine to begin the implementation of the "Trembita" interoperability system, based on the Estonian X-Road (e-Governance Academy, 2017). Subsequently, "Trembita" became one of the key infrastructure components for secure data exchange between state registers and the development of digital public services in Ukraine (e-Governance Academy, 2026).

An analysis of the advantages of the Estonian model for ensuring information security highlights the following strengths. Firstly, the distributed architecture of X-tee/X-Road minimises the risk of a single point of failure: data exchange takes place directly between the participants' information systems, whilst the redundancy of Security Servers ensures service availability in the event of individual components failing (Nordic Institute for Interoperability Solutions, 2025). Secondly, security mechanisms are integrated directly into the data exchange architecture and cover authentication, authorisation, encryption, digital signing and transaction logging, in line with the "security by design" principle (Nordic Institute for Interoperability Solutions, 2025). This was also facilitated by the "no-legacy culture" characteristic of the development of the Estonian digital state, which made it possible to build digital infrastructure without the significant burden of legacy information systems (OECD, 2021). Thirdly, the model relies on a mature system of digital public administration and the reuse of shared infrastructure components, ensuring a high level of interoperability among public information resources (OECD, 2026). Fourthly, the Estonian model is characterised by a significant demonstration effect and the international dissemination of its institutional and technological solutions, one example of which is the adaptation of X-Road technology during the creation of the Ukrainian "Trembita" system (X-Road Security Architecture, 2023).

At the same time, a critical analysis of the Estonian model reveals a series of significant limitations. Firstly, the small domestic labour market exacerbates the problem of staffing for cybersecurity: Estonia's current Cybersecurity Strategy explicitly identifies a shortage of qualified specialists as one of the challenges to the development of national cybersecurity capabilities (Ministry of Economic Affairs and Communications, 2024). The significance of this problem is growing against the backdrop of a steady increase in the number of cyber incidents and the expanding range of entities subject to cybersecurity requirements (Information System Authority, 2026). Secondly, despite the distributed nature of X-tee, its operation depends on a variety of shared trust components and service infrastructure. This creates a risk of simultaneous disruption to the availability of a set of services in the event of failures in shared infrastructure components, as demonstrated, in fact, by the incident involving the X-tee timestamping service in 2026 (Information System Authority, 2026). Thirdly, the effectiveness of the Estonian model is largely linked to the specific trajectory of the digital state's development and the opportunity to build it following the restoration of independence according to the "no-legacy" principle, the high level of uptake of e-services, and the established practice of their everyday use by the population. This limits the scope for mechanically transferring the Estonian model to states with a different institutional structure and necessitates the adaptation of its individual elements to the national administrative and security environment (OECD, 2021).

The German model for ensuring information and cyber security is largely centred on the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), which began operations on 1 January 1991 and is a federal agency operating under the Federal Ministry of the Interior. In accordance with the current legislative framework, the BSI-Gesetz, the BSI acts as the central authority for information security at the national level (Federal Republic of Germany, 2025; Federal Office for Information Security [BSI], n.d.-a). The BSI develops standards and methodological approaches to information security, in particular IT-Grundschutz; certifies IT products and systems; ensures the operation of CERT-Bund and the National IT Situation Centre; and produces a nationwide assessment of the state of cyber security (BSI, n.d. -b, n.d.-c). After the NIS2 Implementation Act came into

force, the BSI assumed the role of the national contact point and central coordinating body, as well as the primary supervisory authority for important and particularly important entities, whilst cooperating with sectoral regulators, in particular the Bundesnetzagentur and BaFin (Federal Republic of Germany, 2025).

An essential element of the German model is the critical infrastructure protection regime (Kritische Infrastrukturen, KRITIS), which is traditionally based on a sectoral approach and quantitative threshold criteria. Prior to the reforms of 2025-2026, the national KRITIS model and the scope of regulation under the BSI-Gesetz did not fully coincide: for example, the 'media and culture' and "government and administration" sectors were part of the broader national KRITIS concept but were not fully covered by the previous BSI-KritisV regime (BSI, 2023). Following the reform, the current KRITIS-Dachgesetz defines ten sectors of critical services: energy; transport and logistics; finance; social insurance and basic services provided by employment centres; healthcare; water supply; food; information technology and telecommunications; the space sector; and household waste management (Federal Republic of Germany, 2026). The identification of critical facilities remains linked to facility categories and threshold values; if the relevant threshold is reached or exceeded, a specific installation or infrastructure facility is deemed critical, and its operator assumes the obligations laid down by law. Meanwhile, until the new subordinate legislation, the Kritisverordnung, comes into force, the relevant transitional provisions of the previous regime remain in force (Federal Republic of Germany, 2025, 2026).

The legal framework of the German model was developed in stages. The first Act on the Enhancement of Information System Security (IT-Sicherheitsgesetz) came into force on 25 July 2015 and implemented special requirements for the protection of IT systems operated by critical infrastructure operators, in particular requirements regarding the implementation of state-of-the-art security measures and the reporting of significant IT incidents (BSI, 2016).

The second version – the IT Security Act 2.0, came into force in May 2021 – expanded the scope of regulated entities, introduced the category of 'undertakings of particular public interest' (Unternehmen im besonderen öffentlichen Interesse, UBI) and explicitly required KRITIS operators to use attack detection systems. Operators

were required to provide the BSI with confirmation of the implementation of such systems for the first time by 1 May 2023 (BSI, 2021, 2023).

The next stage in the development of the regulatory framework relates to the implementation of the European NIS2 and CER Directives; the NIS-2-Umsetzungsgesetz came into force on 6 December 2025, i.e., more than a year after the transposition deadline set by NIS2 – 17 October 2024. The Act significantly expanded the scope of regulation and enshrined in German law the categories of important and particularly important entities, as well as updated requirements regarding cyber risk management, incident reporting and state supervision (BSI, 2025; Federal Republic of Germany, 2025). At the same time, the KRITIS-Dachgesetz, aimed at implementing Directive (EU) 2022/2557 on the resilience of critical entities (CER), came into force on 17 March 2026. The Act established, for the first time at the federal level, a unified cross-sectoral legal framework for the physical resilience of critical infrastructure, providing for the identification of critical facilities, the conduct of risk analysis and risk assessment, the implementation of resilience measures, the preparation of resilience plans, and the reporting of significant incidents. However, the specific details of certain cross-sectoral minimum requirements are to be set out in subordinate legislation, some of which, as of September 2026, are still at the drafting and consultation stage (KRITIS-DachG, BGBl. 2026 I No. 66; Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2026).

Thus, the German experience demonstrates that the implementation of comprehensive European regulation on cybersecurity and the resilience of critical infrastructure may be accompanied by significant delays, even in the presence of a well-developed institutional and regulatory framework.

Examining the advantages of the model, we can note that the concentration of technical expertise within a single specialised body (the BSI) ensures the high quality and consistency of national standards applicable across the entire federation. In addition, a sector-specific approach with clear quantitative thresholds (the KRITIS Regulation) provides businesses with relative legal certainty regarding their status as regulated entities. It is also worth drawing attention to the federal structure of the state, which creates the institutional conditions for the system to function effectively within

a large economy, whilst at the same time making it possible to avoid excessive centralisation of management decisions.

Despite the BSI's high level of institutional and technical capacity, one of the challenges facing the German model remains the complexity of the regulatory framework in the field of information and cyber security. This is shaped by the provisions of the BSI Act, legislation on the implementation of NIS2, the KRITIS Framework Act, as well as sector-specific regulations and special requirements for operators of critical infrastructure. Following the implementation of NIS2, the scope of regulation has expanded significantly: according to federal government estimates, the new requirements now apply to more than 30,000 entities, up from approximately 4,500. At the same time, the government estimated the one-off costs to businesses associated with complying with the new requirements at approximately €2.2 billion, and the annual costs at €2.3 billion. During the legislative process, the German Federal Council (Bundesrat) specifically emphasised the need to improve the practical feasibility of the regulation, reduce the bureaucratic burden and enhance cooperation between the federal and state levels. Consequently, the high level of regulatory detail, whilst ensuring the formalisation of cybersecurity requirements, simultaneously increases organisational and compliance costs for regulated entities (Deutscher Bundestag, 2025a; Deutscher Bundestag, 2025b).

Another challenge is the time taken to adapt national legislation to the new EU requirements. Directive (EU) 2022/2555 (NIS2) set a transposition deadline of 17 October 2024, whilst the German NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz did not come into force until 6 December 2025. In May 2025, the European Commission had already sent Germany a reasoned opinion regarding the incomplete transposition of the directive. A similar delay was observed with regard to Directive (EU) 2022/2557 on the resilience of critical entities (CER): whilst the transposition deadline was set for 17 October 2024, the KRITIS-Dachgesetz came into force on 17 March 2026; as early as July 2025, the European Commission sent Germany a reasoned opinion due to the failure to notify full transposition. The parallel delay in the implementation of two interrelated directives indicates the existence of time and procedural constraints in the mechanism for adapting German

legislation to dynamic changes in the EU legal framework (European Parliament and Council, 2022a, 2022b; European Commission, 2025a, 2025b; Deutscher Bundestag, 2026).

The next aspect relates to Germany's federal structure. The decentralised model creates opportunities to take regional specificities into account and to distribute responsibilities, but at the same time places greater demands on vertical coordination between federal and state authorities. A telling example in this context is the deliberations on the NIS2 legislation: the Bundesrat insisted on more explicit involvement of the Länder in the BSI's support mechanisms, ensuring their access to the information and reporting platform, and improving inter-level information exchange. The current BSI Act also explicitly provides for the BSI's coordinating role in cross-border cooperation between the relevant state authorities. Thus, federalism is both an advantage and a source of additional coordination costs: it reduces excessive centralisation of governance, yet requires well-developed mechanisms for the harmonisation of competences, information exchange and the standardisation of procedures between levels of government (Deutscher Bundestag, 2025a; BSIG, 2025).

An additional challenge is the transitional nature of the current critical infrastructure regulatory framework. Although the KRITIS-Dachgesetz came into force on 17 March 2026, as of September 2026, a range of the subordinate regulations it provides for are still at the drafting and approval stage. In particular, the German Federal Office for Civil Protection and Disaster Assistance (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK) notes that the implementing regulation defining critical facilities has not yet come into force, with the result that the new mechanism for registering operators is not yet fully operational; the development of methodological requirements for risk assessment and resilience plans is also ongoing. This situation creates a temporary gap between the entry into force of the framework law and the full functioning of all the instruments provided for therein (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2026).

A particular institutional challenge for the German model is ensuring public trust in cybersecurity bodies. A telling example in this context was the situation surrounding the former president of the BSI, Arne Schönbaum, who was suspended from his duties

in 2022 following public allegations of possible links to Russian organisations. Subsequent official investigations and court proceedings failed to confirm the existence of sufficient factual grounds for the allegations that he had knowingly maintained contacts with Russian intelligence services. This case demonstrated the importance of institutional trust, proper verification of security-sensitive information, and a clear distinction between reputational risks and confirmed threats to the resilience of the cybersecurity system (Deutscher Bundestag, 2023; Oberlandesgericht München, 2026).

Within the scope of the comparative analysis carried out, the French model of information security is characterised by a high degree of centralisation of its cybersecurity component and the close integration of information systems protection into the national security and defence framework. The central institution is the National Agency for the Security of Information Systems (Agence nationale de la sécurité des systèmes d'information, ANSSI), established in 2009 as the national authority in the field of information systems security. ANSSI reports organisationally to the General Secretariat for Defence and National Security (Secrétariat général de la défense et de la sécurité nationale, SGDSN), which, in turn, ensures the implementation of relevant state policy under the direction of the Prime Minister. ANSSI's functions include inter-ministerial coordination, the development of measures to protect information systems, the detection of and response to incidents, the conduct of audits, and the certification and accreditation of security products and services (Decree No. 2009-834, 2009).

A defining institutional feature of the French model is the separation of civilian, defence and military cyber functions. France's official doctrine is based on a division of responsibilities whereby the protection of information systems at the national level is entrusted to ANSSI, whilst the conduct of offensive military operations in cyberspace falls within the remit of the Ministry of the Armed Forces and the intelligence services. Within the military cyber defence system, a key role is played by the Cyber Defence Command (Commandement de la cyberdéfense, COMCYBER), established in May 2017 and reporting directly to the Chief of the Defence Staff. COMCYBER brings together the cyber defence forces of the Ministry of the Armed Forces and is responsible for planning and conducting defensive, offensive and

information operations in cyberspace. This model ensures an institutional separation between the civil protection of information systems and military operational activities, whilst maintaining mechanisms for their coordination (Ministère des Armées, 2023).

The practical effectiveness of this model was demonstrated during preparations for the 2024 Olympic and Paralympic Games in Paris. ANSSI played a leading role in ensuring the cyber security aspect of the event, coordinating the preparations of public and private entities, organisers and infrastructure operators for over two years. Despite significant media attention and an expanded attack surface for potential cyber-attacks, ANSSI assessed that the incidents recorded had no significant impact on the running of the Games; this was due to the effectiveness of the agency's prior preparation, training and cross-sectoral coordination (ANSSI, 2025).

An important component of the French system is the regime for the protection of operators of vital importance (opérateurs d'importance vitale, OIV). Unlike a purely economic approach, the classification of an entity as an OIV is linked to the significance of its activities for the state's defence and economic potential, national security, the state's ability to function, and the protection of the population's life and health. The regulatory framework for defining OIVs was established as early as Decree No. 2006-212 of 23 February 2006. Meanwhile, the 2013 Military Programming Act (Loi de programmation militaire, LPM) introduced a special cyber-security regime for their critical information systems: mandatory security rules, incident reporting, the possibility of conducting audits, and the application of special measures in the event of large-scale cyber crises. The relevant rules are laid down at the level of the Prime Minister, whilst ANSSI plays a key role in their implementation and in monitoring compliance (Décret No. 2006-212, 2006; Loi No. 2013-1168, 2013).

Another distinct element of the French approach to technological sovereignty is the SecNumCloud certification scheme, developed by ANSSI in 2016 to assess the security and reliability of cloud services. The current version of the SecNumCloud requirements combines technical, operational and legal criteria. Specifically, the supplier's registered office, central administration and principal place of business must be located in an EU Member State; the share of capital and voting rights directly or indirectly held by a single entity from outside the EU must not exceed 24 per cent, and

their combined share must not exceed 39 per cent. Certain requirements are designed to restrict access by non-European third parties to these customers and to mitigate risks associated with the application of extraterritorial legislation of third countries. Thus, SecNumCloud combines technical information protection with legal and organisational mechanisms to ensure control over critical cloud resources (ANSSI, 2022; ANSSI, 2026).

While analyzing the advantages of the French model for ensuring information security, it is worth emphasizing its key strengths first and foremost: firstly, a high level of institutional centralisation ensures unity in strategic leadership and inter-agency coordination in the field of information and cyber security. ANSSI's subordination to the General Secretariat for Defence and National Security under the Prime Minister creates the organisational framework for harmonising the actions of various state authorities within a single management system. In particular, the implementation of the state's digital systems security priorities for 2026–2027 involves monthly inter-agency monitoring involving the relevant departmental units under the auspices of ANSSI (Décret No. 2009-834, 2009; ANSSI, 2026).

Secondly, the direct institutional integration of ANSSI into the national security system ensures a high strategic status for issues relating to the protection of information systems and facilitates the concentration of specialised expertise. The expansion of the agency's functions was accompanied by a significant increase in staffing capacity: as of early 2025, ANSSI had 656 permanent staff, more than double the figure for 2021. At the same time, the further expansion of the regulatory framework, particularly in connection with NIS2, requires additional resources; it is therefore inappropriate to speak of its unconditional stability (Sénat, 2025).

Thirdly, the French model combines cybersecurity with ensuring technological and jurisdictional control over critical digital resources. The SecNumCloud certification scheme sets out not only technical requirements for cloud services, but also criteria regarding the provider's location, ownership structure and the protection of data from the application of extraterritorial legislation of third countries. This approach helps to mitigate jurisdictional risks and critical dependence on providers controlled by entities outside the EU (ANSSI, 2022). It is telling that in 2026 the

European Commission also introduced the Cloud Sovereignty Framework, which demonstrates the gradual spread of digital sovereignty principles at EU level (European Commission, 2026).

The institutional constraints of the French model are twofold. On the one hand, the concentration of coordination, regulatory and technical functions within ANSSI means that the effectiveness of the entire system depends on the agency having sufficient resources. The expansion of the regulatory environment resulting from the implementation of NIS2 and the shift from 500 OIV operators to 15,000 regulated entities creates a risk of institutional overload and is highlighted in parliamentary documents as a mismatch between ANSSI's expanded functions and the resources requested (Sénat, 2024; Sénat, 2025). On the other hand, the focus on digital sovereignty creates a structural trade-off between the level of protection and the competitiveness of the cloud services market: the stringent criteria of SecNumCloud narrow the pool of qualified providers and contribute to market segmentation, as directly noted by the Autorité de la concurrence (2023). Thus, striking a balance between technological sovereignty and the availability of innovative cloud solutions remains a significant challenge for the French model.

The Polish model serves as an important point of comparison for Ukraine, given Poland's experience of post-socialist transformation, its membership of the EU since 2004, and the consistent alignment of its national cybersecurity system with the EU acquis. This experience is particularly relevant for Ukraine, which is currently in the process of negotiating its accession to the EU.

The primary regulatory act is the Act of 5 July 2018 on the National Cybersecurity System (ustawa o Krajowym Systemie Cyberbezpieczeństwa, KSC), which transposed Directive (EU) 2016/1148 (NIS1). The institutional architecture of the KSC is based on a functional division of responsibilities between three national-level incident response teams – CSIRT NASK, CSIRT GOV and CSIRT MON – interacting with sectoral CSIRTs and competent authorities. Information and communication interaction between the system's participants is facilitated by the S46 platform, which is used for incident reporting, the exchange of information on cyber

threats and to support coordination within the KSC (Republic of Poland, 2018; Ministry of Digital Affairs, 2026a).

However, the implementation of NIS2 also demonstrated the complexity of operationally adapting national legislation to the new EU requirements. According to the transposition deadline set by the Directive – 17 October 2024 – the Polish Act amending the KSC was adopted on 23 January 2026 and came into force on 3 April 2026. The amendment has significantly expanded the scope of regulation: according to estimates by the Ministry of Digitalisation, the updated system may cover around 38,000 critical and important entities, including approximately 27,000 public sector entities. This demonstrates the significant scale of the organisational and regulatory transformation associated with the transition from NIS1 to NIS2 (Directive (EU) 2022/2555, 2022; Republic of Poland, 2026; Ministry of Digitalisation, 2026b).

When analysing the Polish model for ensuring information security, attention should first and foremost be paid to its key advantages. The functional separation of CSIRT NASK, CSIRT GOV and CSIRT MON ensures specialisation in responding to civilian, government and military cyber incidents, whilst the S46 system creates a unified environment for information exchange between KSC participants. Of particular interest to Ukraine is precisely this combination of specialised response channels with a centralised digital coordination platform, which enables inter-agency cooperation within the complex, multi-stakeholder institutional environment.

Meanwhile, the need for further strengthening of coordination is reflected in the Republic of Poland's Cybersecurity Strategy until 2029, approved by the Council of Ministers on 10 March 2026. This document provides for the progressive formation, based on the Joint Cyber Security Operations Centre (Polaczone Centrum Operacyjne Cyberbezpieczenstwa, PCOC), of a central coordinating body for the national cyber security system, as well as the further development of sectoral CSIRTs and the S46 system. This indicates a gradual transition from a predominantly decentralised coordination model towards strengthened centralised strategic and operational management (Council of Ministers, 2026; Ministry of Digital Affairs, 2026c).

The institutional limitations and challenges of the model are as follows: firstly, the transposition of NIS2 in Poland was delayed by approximately seventeen months:

although the deadline was set for 17 October 2024, the relevant amendments to the Act on the National Cybersecurity System did not come into force until 3 April 2026. This demonstrates that institutional integration into the EU legal framework does not preclude significant time and procedural delays in the transposition process (European Commission, 2025; Republic of Poland, 2026).

Secondly, the multi-stakeholder structure of the KSC, which brings together three national CSIRTs, sectoral CSIRTs and competent authorities, places greater demands on inter-agency coordination and a clear delineation of responsibilities. This risk is partially mitigated by the S46 system, which provides a centralised digital channel for incident reporting and automated routing of information. However, the phased implementation of the new NIS2 requirements up to 2027 prolongs the transition to the full operation of the updated system (Ministry of Digital Affairs, 2026; Republic of Poland, 2026).

A comparative analysis of four national models reveals that there is no single institutional model for information security within the EU. Common regulatory requirements are implemented through various national systems: centralised coordination with a distributed digital infrastructure in Estonia, a federal-sectoral model in Germany, a centralised model in France and a multi-stakeholder system in Poland (RIA, 2026; BSI, 2026; ANSSI, 2026; Ministry of Digital Affairs, 2026a). Specifically, Estonia's X-tee ensures secure data exchange between autonomous information systems without concentrating them in a single centralised database (RIA, 2026). The differences between the models reflect varying approaches to combining centralised management, functional specialisation, inter-agency coordination and the resilience of the information infrastructure. However, the experience of Germany and Poland illustrates that adapting national legislation to EU requirements can entail significant time and procedural costs, even where well-established national cybersecurity institutions are in place (European Commission, 2025; Ministry of Digitalisation, 2026b).

For Ukraine, the experience of the countries studied provides primarily a source of specific institutional solutions, rather than ready-made models to replicate. Estonia's experience is relevant in terms of a decentralised data-sharing infrastructure; Poland's,

in terms of multi-stakeholder coordination and the development of the KSC; France's, with regard to centralised strategic management; and Germany's, concerning the organisation of cooperation between the federal and state levels (RIA, 2026; Ministry of Digitalisation, 2026a; ANSSI, 2026; BSI, 2026). The Polish Cybersecurity Strategy up to 2029 further provides for enhanced coordination and the development of a national cybersecurity system (Ministry of Digitalisation, 2026c).

Consequently, instead of mechanically replicating a specific national model, it is advantageous for Ukraine to develop its own institutional architecture, taking into account the requirements of the EU acquis, the current security environment and existing administrative capacities, as set out in Table 1.3.

The legal framework for cybersecurity in Ukraine has been developed in stages, with a focus on strengthening institutional coordination and transitioning to risk-based protection mechanisms. The fundamental regulatory act is the Law of Ukraine 'On the Basic Principles of Ensuring Ukraine's Cybersecurity' No. 2163-VIII of 5 October 2017, which established the institutional framework for the national cybersecurity system and defined the powers of the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Police, the Ministry of Defence and the General Staff of the Armed Forces of Ukraine, the intelligence agencies and the National Bank of Ukraine. Coordination functions were assigned to the National Cybersecurity Coordination Centre as a working body of the National Security and Defence Council of Ukraine. At that time, CERT-UA was already operating within the State Service for Special Communications; the legislation cemented its place in the national cyber incident response system (Verkhovna Rada of Ukraine, 2017; CERT-UA, 2026).

A new stage in the development of the regulatory framework is linked to the adoption of Law of Ukraine No. 4336-IX of 27 March 2025, which came into force in April 2025 and implemented several key principles of NIS2.

Table 1.3.

Comparative characteristics of national models for ensuring information security

Country	Type of institutional model	Key institutions	Characteristic features of the model	Institutional constraints and challenges	Elements potentially relevant to Ukraine
Estonia	Centralised coordination within a decentralised digital infrastructure	RIA / NCSC-EE; CERT-EE	X-tee's distributed architecture; absence of a single centralised database; integration of cybersecurity with the functioning of the e-government; round-the-clock monitoring and incident response.	High dependence of government and societal processes on the continuity of digital services; the need to constantly adapt security mechanisms to the growing number and complexity of cyber incidents	Distributed architecture for government data exchange; the NCSC/CERT model; protection of critical information infrastructure; principles of secure inter-agency data exchange.
Germany	Federal, multi-level, sector-specific	BSI; cooperation with state authorities and sectoral regulators	Federal Technical Centre; B3S system of sectoral standards; specific regulation of critical infrastructure; 24/7 National IT Situation Centre.	The complexity of multi-level coordination and the regulatory environment; a lengthy process of adapting to EU legislation. The European Commission has noted Germany's incomplete transposition.	Federal-regional coordination; sectoral standards; critical infrastructure protection system; monitoring, audit and response mechanisms.
France	Centralised, state-coordinated	ANSSI	Concentration of significant regulatory and technical functions within ANSSI; a special protection regime for OIVs and their information systems; a system for classifying trusted solutions, in particular SecNumCloud.	A significant number of specific requirements for the most sensitive information systems and qualification procedures. A particular current challenge is the delay in the full transposition of NIS2: the European Commission has referred the case concerning France to the Court of Justice of the European Union due to the failure to notify full transposition.	Centralised coordination of the protection of critical information systems; the qualification of trusted cloud services; mechanisms for the protection of operators of strategic importance.
Poland	Multi-stakeholder, inter-ministerial and sector-specific	Ministry of Digital Affairs; CSIRT NASK; CSIRT GOV; CSIRT MON	Functional specialisation of the three national CSIRTs; integration of sectoral competent authorities; use of S46 as a shared information and communication environment for the KSC.	The large number of bodies involved highlights the importance of coordination and a clear delineation of responsibilities; in 2026–2027, the system is undergoing the practical implementation of the new NIS2 requirements, the registration of entities and their connection to S46.	Division of functions amongst specialised CSIRTs; a single information-sharing platform, S46; experience of organisational adaptation of the national system to NIS2.

Source: compiled by the authors based on official materials from the Information System Authority of Estonia (RIA), the Federal Office for Information Security (BSI), the French Cybersecurity Agency (ANSSI), the Ministry of Digital Affairs of the Republic of Poland and the national legislation of the countries under study (RIA, 2026; BSI, 2026; ANSSI, 2026;

The Act provided for the establishment of departments and the creation of cybersecurity management posts within public authorities, the designation of responsible persons at critical information infrastructure sites, the development of national response systems and mechanisms for exchanging information on cyber incidents, as well as a shift from a predominantly permissive model of cybersecurity to the authorisation of systems and risk-based management of security throughout their lifecycle (Verkhovna Rada of Ukraine, 2025; State Special Communications Service, 2025).

The need for such a transformation is heightened by the increasing intensity of cyber threats in the context of war. According to CERT-UA, the number of cyber incidents recorded rose from 2,194 in 2022 to 4,315 in 2024, representing an increase of almost 70 per cent compared with 2023. At the same time, these figures should not be directly linked to the effect of Law No. 4336-IX, as the trend described had already taken shape before the law came into force (State Special Communications Service, 2025).

A comparison with the models of EU Member States indicates that the Ukrainian system is gradually aligning with European principles of multi-level response, the division of responsibilities among competent authorities, and risk-based management. In its Ukraine Report 2025, the European Commission noted a significant update to legislation and the creation of a unified national cyber incident response system, whilst emphasising that a set of provisions of the acquis still require full implementation to achieve compliance with NIS2 (European Commission, 2025).

Further development of the regulatory framework has already partially resolved certain discrepancies. Resolution No. 1533 of the Cabinet of Ministers of Ukraine, dated 26 November 2025, introduced reporting deadlines for significant cyber incidents, similar to those set out in Article 23 of NIS2: an initial report must be submitted within 24 hours, a progress report within 72 hours, and a final report within one month. Furthermore, Ukraine has in place a procedure for classifying facilities as critical infrastructure and maintains a Register of Critical Infrastructure Facilities;

therefore, their establishment should no longer be regarded as an unfulfilled harmonisation task (Cabinet of Ministers of Ukraine, 2025; 2026).

Consequently, the main areas for further alignment with the EU acquis remain the completion of the implementation of the provisions of NIS2, the further refinement of mechanisms for cooperation between competent authorities and the CSIRT, and the completion of the personal data protection reform. The latter area remains particularly relevant: the European Commission has noted that the Ukrainian personal data protection system does not sufficiently comply with the EU acquis, whilst Bill No. 8153 'On the Protection of Personal Data' was still undergoing consideration in the Verkhovna Rada of Ukraine as of September 2026 (European Commission, 2025; Verkhovna Rada of Ukraine, 2026).

Special attention should be paid to harmonisation in the field of personal data protection, which is functionally linked to ensuring information and cyber security. Against the backdrop of a significant overhaul of cyber security legislation, the current Law of Ukraine 'On the Protection of Personal Data' of 2010 does not ensure full compliance with the current EU acquis. In its Ukraine Report 2025, the European Commission noted the inadequacy of the current regulatory and institutional framework for personal data protection and the lack of progress in aligning it with the acquis, emphasising the need to adopt new legislation. Draft Law No. 8153, aimed at modernising this area in line with the GDPR, was, as of September 2026, being prepared for its second reading; in parallel, Draft Law No. 6177 on the establishment of a specialised supervisory authority remains under consideration (European Commission, 2025; Verkhovna Rada of Ukraine, 2026a, 2026b). The GDPR, unlike the previous Directive 95/46/EC, establishes an expanded system of data subjects' rights, the role of a data protection officer for certain categories of controllers and processors, and significantly stricter sanction mechanisms (European Parliament and Council, 2016).

The practical dimension of alignment with the EU acquis is supported by the regular Ukraine–EU Cyber Dialogue. The fourth round, held in Kyiv on 16 October 2025, covered the implementation of NIS2, the protection of critical infrastructure, the digital component of Ukraine's Plan, the implementation of EU cybersecurity tools for

5G networks, and cyber defence issues. This format ensures a combination of regulatory alignment with operational and institutional cooperation in the field of cyber resilience (European Commission, 2025b).

Further harmonisation is also integrated into the negotiation process regarding Ukraine's accession to the EU; on 15 June 2026, the first negotiation cluster, "Fundamentals", was opened, whilst Chapter 10, "Digital Transformation and Media", falls under Cluster 3, "Competitiveness and Inclusive Growth"; its bilateral screening took place from 31 March to 1 April 2025 and covered, in particular, cybersecurity, electronic identification and trust services, open data, the DSA, the DMA and P2B. As of September 2026, Cluster 3 has not yet been opened for formal negotiations; Clusters 1 and 6 are open. According to the European Commission's assessment, Ukraine is at a level between moderate and good in terms of preparedness under Chapter 10, whilst some provisions of NIS2, the DSA, the DMA, P2B and other acts of the acquis still require further implementation (European Commission, 2025a).

Consequently, the current trend indicates a gradual convergence of the Ukrainian information security system with the EU's legal and institutional framework; however, the completion of this process requires the further implementation of NIS2, the modernisation of legislation on the protection of personal data, and the completion of the adaptation of regulations governing digital services and trust services.

Ensuring information security in the context of digital transformation is determined not only by the quality of the regulatory framework, but also by the state's institutional capacity to ensure its practical implementation. The analysis carried out has shown that the common EU regulatory framework, comprising the GDPR, NIS2, CRA, DSA, Cybersecurity Act and DGA, is implemented through various national institutional models, the effectiveness of which depends on coordination mechanisms, the distribution of powers, staffing capacity and readiness to respond to cyber threats. Consequently, the further harmonisation of Ukrainian legislation with the EU acquis should envisage not only regulatory alignment but also the development of Ukraine's own institutional architecture for information security, taking into account European experience, national administrative capacities and the specific nature of the security environment in the context of war and post-war reconstruction.

Perspective areas for further research in this field include the quantitative assessment of the relationship between the level of centralisation of the institutional system and the speed of response to cyber incidents; a comparative analysis of public–private partnership models for the protection of critical information infrastructure; research into mechanisms for inter-agency coordination in the context of hybrid threats; and an assessment of the economic efficiency of investments in the development of professional competencies in the field of information security as a component of strengthening Ukraine's human capital during wartime and in the post-war period.

REFERENCES FOR SUBSECTION 1.3

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *(General Data Protection Regulation)*. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 *(NIS2 Directive)*. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
3. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 *(Digital Services Act)*. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
4. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 *(Cyber Resilience Act)*. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
5. ENISA Threat Landscape 2025. *European Union Agency for Cybersecurity,* 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
6. European Commission. Digital Strategy. URL: https://commission.europa.eu/index_en
7. On the Basic Principles of Ensuring Cybersecurity of Ukraine: *Law of Ukraine of 5 October 2017 No. 2163-VIII.* URL: https://zakon.rada.gov.ua/laws/show/2163-19
8. On Amendments to Certain Laws of Ukraine Regarding Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure Facilities: *Law of Ukraine of 27 March 2025 No. 4336-IX.* URL: https://zakon.rada.gov.ua/laws/show/4336-20
9. State Service of Special Communications and Information Protection of Ukraine. Ukraine Is Transforming Its Cybersecurity System in Line with European Standards. *Cabinet of Ministers of Ukraine, 2026.* URL: https://www.kmu.gov.ua/news/derzhspetszviazku-ukraina-transformuie-systemu-kiberbezpeky-za- ievropeiskymy-standartamy
10. Ukraine and the EU Deepen Cybersecurity Cooperation during the 4th Round of the Cyber Dialogue. Delegation of the European Union to Ukraine, 2025. URL: https://eeas.europa.eu/delegations/ukraine/
11. X-Road data exchange platform. *Republic of Estonia Information System Authority* (RIA). URL: https://e-estonia.com/programme/e-estonia-programme-on-x-road/

12. Estonia to establish the world's first data embassy in Luxembourg. *Government of the Republic of Estonia,* 2017. URL: https://valitsus.ee/en/news/estonia-establish-worlds-first-data- embassy-luxembourg
13. Federal Office for Information Security (BSI). *KRITIS-Verordnung, IT-Sicherheitsgesetz 2.0.* URL: https://www.bsi.bund.de
14. Agence nationale de la sécurité des systèmes d'information (ANSSI). *Qualification SecNumCloud.* URL: https://cyber.gouv.fr
15. Ministry of Digital Affairs of Poland. (2026, April 14). Amendment to the Act on the national cybersecurity system. https://www.gov.pl/web/baza-wiedzy/nowelizator-ustawy-o- krajowych-systemie-cyberbezpieczenstwa
16. Council of the European Union. (2025). Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management (C/2025/3445). Official Journal of the European Union. https://eur-lex.europa.eu/eli/C/2025/3445/oj/eng
17. European Parliament & Council of the European Union. (2022). 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 (NIS 2 Directive). Official Journal of the European Union, L 333, 80-152. https://eur-lex.europa.eu/eli/dii72022/2555/oj/eng
18. Information System Authority. (2017, April 26). *Head of CERT-EE: Estonia's capability to manage cyber crises has improved significantly in 10 years,* https://ria.ee/en/news/head- cert-ee-estonias-capability-manage-cyber-crises-has-improved-significantly-lQ-years
19. NATO. (2007, May 23). *Press briefing,* https://www.nato.int/en/news-and-events/events/transcripts/2007/05/23/press-briefing
20. Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In D. Remenyi (Ed.), *Proceedings of the 7th European Conference on Information Warfare and Security* (pp. 163—168). Academic Conferences Limited. https://www.etis.ee/portal/publications/display/c269960c-2e40-44bl-aa43-a7c62e9caaa6
21. NATO Cooperative Cyber Defence Centre of Excellence, (n.d.). *About us.* https://ccdcoe.org/about-us/
22. Information System Authority. (2026). *Tasks and structure of the authority.* https://www.ria.ee/en/authority-news-and-contact/authority-and-management/tasks-and-structure- authority
23. Information System Authority, (n.d.). *National Cyber Security Centre NCSC-EE.* https://www.ria.ee/en/cyber-security/national-cyber-security-centre-ncsc-ee
24. Government of Estonia. (2017, June 20). *Estonia to establish the world's first data embassy in Luxembourg,* https://www.valitsus.ee/en/news/estonia-establish-worlds-first-data- embassy-luxembourg
25. e-Estonia. (n.d.). *Data embassy.* https://e-estonia.com/wp-content/uploads/factsheet data embassy.pdf
26. Elections in Estonia, (n.d.). *Statistics about Internet voting in Estonia.* https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia
27. Kriisa, K. (2025, January 27). *Estonia: 100% digital government services, with divorce as the final step.* e-Estonia. https://e-estonia.com/estonia-100-digital-government-services/
28. e-Governance Academy. (2017, October 26). *Ukraine to begin the implementation of interoperability system,* https://ega.ee/ukraine-to-begin-the-implementation-of-interoperability- system/
29. e-Governance Academy. (2026). *Трембіта - фундамент цифрової держави.* https://ega.ee/uk/trembita/

30. e-Governance Academy. (2017, October 26). *Ukraine to begin the implementation of interoperability system,* https://ega.ee/ukraine-to-begin-the-implementation-of-interoperability- system/

31. Information System Authority. (2026a, February 4). *Cyber security in Estonia: New records, old mistakes,* https://www.ria.ee/en/news/cyber-security-estonia-new-records-old-mistakes

32. Information System Authority. (2026b, July 6). *Situation in cyberspace - June 2026.* https://ria.ee/en/situation-cyberspace-june-2026

33. Ministry of Economic Affairs and Communications. (2024). *Cybersecurity strategy 2024-2030: "Cyber-conscious Estonia".* Republic of Estonia. Cybersecurity Strategy 2024-2030 PDF

34. Nordic Institute for Interoperability Solutions. (2025). *X-Road security architecture* (Version 0.11, Technical Specification ARC-SEC). X-Road Documentation, https://docs.x- road.global/Architecture/arc-sec x road security _architecture.html

35. Organisation for Economic Co-operation and Development. (2021). *The E-Leaders handbook on the governance of digital government.* OECD Publishing. https://doi.org/10.1787/ac7f2531 -en

36. Organisation for Economic Co-operation and Development. (2026). *Digital government outlook 2026: From foundations to transformational impact.* OECD Publishing. https://d0i.0rg/l 0,1787/0496b2bc-en

3. 7. KRITIS Act of March 11, 2026 (BGBl. 2026 I No. 66), as amended by Article 8 of the Act of July 21, 2026 (BGBl. 2026 I No. 221). KRITISDachG - Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen.

38. Federal Office of Civil Protection and Disaster Assistance (BBK). (2026). *FAQ on the KRITIS Umbrella Act.* The BBK explains that the Act entered into force on March 17, 2026, but that implementing ordinances and cross-sectoral minimum requirements are still being drafted. https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Strategien-und-rechtlicher- Rahmen/KRITISDachG/FAQ/faq node.html?utm

39. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. (2026). FAQ zum KRITIS- Dachgesetz. BBK - FAQ zum KRITIS-Dachgesetz https://www.bbk.bund.de/.

40. Bundesministerium der Justiz. (2025). *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI- Gesetz — BSIG) vom 2. Dezember 2025* (BGBl. 2025 I Nr. 301). https://www.gesetze-im- intemet.de/bsig 2025/BJNR12D0B0025.html

41. Bundesministerium der Justiz. (2026). *Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRJTIS-Dachgesetz - KRITISDachG) vom 11. März 2026* (BGBl. 20261 Nr. 66). https://www.gesetze-im-internet.de/kritisdachg/BJNR0420B0026.html

42. Deutscher Bundestag. (2023). *Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der CDU/CSU: Abberufung und Versetzung des früheren Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik Arne Schönbohm* (Drucksache 20/7366). https://dserver.bundestag.de/btd/20/073/2007366.pdf

43. Deutscher Bundestag. (2025). *Gesetz zur Informationssicherheit in der Bundesverwaltung beschlossen,* https://www.bundestag.de/dokumente/textarchiv/2025/kw46-de- nis-2-1123138

44. European Commission. (2025a, May 7). *Commission calls on 19 Member States to fully transpose the NIS2 Directive,* https://digital-strategy.ec.europa.eu/en/news/commission-calls-19- member-states-fully-transpose-nis2-directive

45. European Commission. (2025b, July 17). *July infringements package: Key decisions.* [Section on the transposition of Directive (EU) 2022/2557 on the resilience of critical entities]. https://luxembourg.representation.ec.europa.eu/actualites-et-evenements/actualites/july- infringements-package-key-decisions-2025-07-17 fr

46. European Parliament and Council of the European Union. (2022a). *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 (NIS2 Directive).* Official Journal of the European Union, L 333, 80-152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

47. European Parliament and Council of the European Union. (2022b). *Directive (EU) 2022/255 7 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive).* Official Journal of the European Union, L 333,164-198. https://eur- lex.europa.eu/eli/dir/2022/2557/oj

48. Agence nationale de la sécurité des systèmes d'information. (2026). *What we do.* https://cvber.gouv.fr/en/aboirt-anssi/what-we-do/

49. Bundesamt fur Sicherheit in der Informationstechnik. (2026). *Bund-Länder-Zusammenarbeit.* https://www.bsi.bund.de/DE/Das-BSI/Organisation-und-Aufbau/Abteilungen- inkl-Organigramm/Bund-Laender-Zusammenarbeit/bund-laender-zusammenarbeit node.html

50. Information System Authority. (2026). *Cyber Security in Estonia 2026.* https:/%ww.ria.ee/en/cYber-security-estonia-2026

51. Information System Authority. (2026). *National Cyber Security Centre NCSC-EE.* https://www.ria.ee/en/cyber-security/national-cyber-security-centre-ncsc-ee

52. Ministerstwo Cyfryzacji. (2026). *System S46.* https://www.gov.pl/web/system-s46/o- systemie-s46

53. Oberlandesgericht München. (2026). *Endurteil vom 16.06.2026 - 18 U 217/25 Pre e: Erfolgreicher Eilantrag wegen Berichterstattung über angebliche Kontakte zu russischen Geheimdienstkreisen.* https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B- 2026-N-14114

54. Agence nationale de la sécurité des systèmes d'information. (2022). *Prestataires de services d'informatique en nuage (SecNumCloud) : Référentiel d'exigences, version 3.2.* Premier ministre. https://cyber.gouv.ff/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf

55. Agence nationale de la sécurité des systèmes d'information. (2025). *ANSSI2024 annual review*. https://cyber.gouv.fr/en/publications/annual-reviews/anssi-2024-annual-review/

56. Agence nationale de la sécurité des systèmes d'information. (2026). *FAQ avant de se lancer dans la qualification SecNumCloud.* https://cyber. gouv.fr/enjeux-technologiques/cloud/faq- qualification-secnumcloud/

57. France. (2006). *Décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale.* Journal officiel de la République française. https://www.legifrance.gouv.fr/jorf/id/JORFTEXTOOOOOQ634536

5. 8. France. (2009). *Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».* Journal officiel de la République française. https://www.legifrance.gouv.fr/loda/id/JORFTEXT00002Q828212

59. France. (2013). *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale,* art. 22. Journal officiel de la République française. https://www.legifrance.gouv.fr/jorf/article io/JORFARTI000Q28338907

60. Ministère des Armées et des Anciens combattants. (2023). *Et la cyberdéfense devint une priorité nationale,* https://www.defense.gouv.fr/actualites/cvberdefense-devint-priorite-nationale

61. Agence nationale de la sécurité des systèmes d'information. (2022). *Prestataires de services d'informatique en nuage (SecNumCloud): Référentiel d'exigences, version 3.2.* Premier ministre. https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences- v3.2.pdf

62. Agence nationale de la sécurité des systèmes d'information. (2026). *Publication de la feuille de route des efforts prioritaires en matière de sécurité numérique de l'Etat 2026-202 7.* https://cyber.gouv.fr/actualites/feuille-de-route-des-efforts-prioritaires-en-matiere-de-securite- numerique-de-letat-2026-2027/

63. Autorité de la concurrence. (2023). *Avis n° 23-A-08 du 29 juin 2023 portant sur le fonctionnement concurrentiel de l'informatique en nuage («cloud»),* https://www.autoritedelaconcurrence.fr/fr/article/lautorite-rend-son-avis-sur-le-fonctionnement- concurrentiel-du-secteur-du-cloud

64. European Commission. (2026, June 1). *Sovereign Cloud Framework explained.* https://commission.europa.eu/news-and-media/news/sovereign-cloud-framework-explained-2026- 06-01 en

65. Sénat. (2024). *Projet de loi de finances pour 2023: Direction de l'action du Gouvernement - Coordination du travail gouvernemental,* https://www.senat.fr/rap/a24-146-9/a24- 146-91,html

66. Sénat. (2025). *Projet de loi de finances pour 2026: Direction de l'action du Gouvernement,* https://www.senat.fr/rap/125-139-39/125-139-393.html

67. European Parliament and Council of the European Union. (2022). *Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).* Official Journal of the European Union, L 333, 80-152. https://eur- lex.europa.eu/eli/dir/2022/2555/oj

68. Ministerstwo Cyfryzacji. (2026a). *Czym jest System S46.* https://www.gov.pl/web/system- s46/o-systemie-s46

69. Ministerstwo Cyfryzacji. (2026b). *Nowelizacja ustawy o krajowym systemie cyberbezpieczenstwa (KSC) - kogo obejmuje?* https://www.gov.pl/web/cyfryzacja/nowelizacja- ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc—kogo-obejmuje

70. Ministerstwo Cyfryzacji. (2026c). *Nowa strategia cyberbezpieczenstwa. Polska wzmacnia ochronç przed cyberatakami.* https ://www. gov.pl/web/cyfryzacj a/nowa-strategia-cyberbezpieczenstwa-polska-wzmacnia-ochrone-przed-cyberatakami

71. Rada Ministrow. (2026). *Strategia Cyberbezpieczenstwa Rzeczypospolitej Polskiej.* Uchwala nr 92 Rady Ministrow z dnia 10 marca 2026 r., M.P. 2026 poz. 309. https://monitorpolski.gov.pl/M2026000030901.pdf

72. Republic of Poland. (2018). *Ustawa z dnia 5 lipca 2018 г. o krajowym systemie cyberbezpieczenstwa.* Dz.U. 2018 poz. 1560. https://eli.gov.pl/eli/DU/2018/1560/ogl

73. Republic of Poland. (2026). *Ustawa z dnia 23 stycznia 2026 г. o zmianie ustawy o krajowym systemie cyberbezpieczenstwa oraz niektôrych innych ustaw.* Dz.U. 2026 poz. 252. https://eli.gov.pl/eli/DU/2026/252/ogl

74. Verkhovna Rada of Ukraine. (2017). On the Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine of 5 October 2017 No. 2163-VIII. Legislation of Ukraine Database. https://zakon.rada.gov.Ua/laws/show/2163-19

75. Verkhovna Rada of Ukraine. (2022). Draft Law on Personal Data Protection *No. 8153 of 25 October 2022.* https://itd.rada.gov.ua/billinfo/Bills/Card/40707

76. Verkhovna Rada of Ukraine. (2025). On Amendments to Certain Laws of Ukraine Regarding Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure Facilities: *Law of Ukraine of 27 March 2025 No. 4336-IX.* Legislation of Ukraine Database, https://zakon.rada.gov.ua/laws/show/4336-20

77. State Service of Special Communications and Information Protection of Ukraine. (2025). Russian Cyber Operations: Analysis for the Second Half of 2024. CERT-UA, State Cyber Protection Centre.

78. European Commission. (2025). *Ukraine Report 2025.* Directorate-General for Enlargement and Eastern Neighbourhood, https://enlargement.ec.europa.eu/ukraine-report-2025 en

79. Cabinet of Ministers of Ukraine. (2020). Certain Issues Concerning Critical Infrastructure Facilities: *Resolution of the Cabinet of Ministers of Ukraine of 9 October 2020 No. 1109 (as amended)*. Legislation of Ukraine Database.

80. Cabinet of Ministers of Ukraine. (2023). On Approval of the Procedure for Maintaining the Register of Critical Infrastructure Facilities, Including Such Facilities in the Register, Accessing the Register and Providing Information Therefrom: Resolution of the Cabinet of Ministers of Ukraine of 28 April 2023 No. 415 (as amended in 2026). Legislation of Ukraine Database. https://zakon.rada. gov.ua/go/415-2023-п

81. Cabinet of Ministers of Ukraine. (2025). Certain Issues Concerning Response to Cyber Incidents, Cyberattacks and Cyber Threats: *Resolution of the Cabinet of Ministers of Ukraine of 26 November 2025 No. 1533.* Legislation of Ukraine Database, https://zakon.rada. gov.ua/laws/show/1533-2025- n

82. European Commission. (2025a). *Ukraine 2025 Report. Commission Staff Working Document SWD(2025) 759final.* European Commission.

83. European Commission. (2025b, October 18). *EU and Ukraine deepen cooperation on cyber security at 4th Cyber Dialogue,* https://digital-strategy.ec.europa.eu/en/news/eu-and-ukraine- deepen-cooperation-cvber-security-4th-cyber-dialogue

84. European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 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 (General Data Protection Regulation).* Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

85. Council of the European Union. (2026, June 15). *EU and Ukraine open first accession negotiations cluster,* https://www.consilium.europa.eu/en/press/press-releases/2026/06/15/eu-and- ukraine-open-first-accession-negotiations-cluster/

86. Verkhovna Rada of Ukraine. (2010). On Personal Data Protection: *Law of Ukraine of 1 June 2010 No. 2297-VI.* Legislation of Ukraine Database. https://zakon.rada. gov.ua/laws/show/2297-l 7

87. Verkhovna Rada of Ukraine. (2026a). *Draft Law on Personal Data Protection No. 8153 of 25 October 2022.* https://itd.rada.gov.ua/billinfo/Bills/Card/40707

88. Verkhovna Rada of Ukraine. (2026b). Draft Law on the National Commission for Personal *Data Protection and Access to Public Information No. 6177 of 18 October 2021.* https://itd.rada.gov.ua/billinfo/Bills/Card/38789

89. Ministry of Digital Transformation of Ukraine. (2025, 1 April). The Next Stage of Ukraine's Accession to the EU: *Bilateral Screening Meeting in the Field of Digital Transformation and Media.* https://thedigital.gov.ua/news/nastupniy-etap-vstupu-ukraini-do-es-dvostopoHHa-skrining- zustrich-u-sferi-tsifrovoi-transformatsii-ta-media

CHAPTER 2. CYBERSECURITY AND INFORMATION PROTECTION UNDER HYBRID THREATS: NATIONAL AND EUROPEAN APPROACHES

2.1. Distributed Cyber Sensors for Monitoring Threats to Ukraine's Critical Information Infrastructure

Yevhen ZHYVYLO
Alina YANKO
Tetiana FESENKO
Yuliia KALASHNIKOVA
National University "Yuri Kondratyuk Poltava Polytechnic"
Yurii KUCHMA
LLC Private Higher Education Institution "University of Modern Technologies"

The transformation of today's security environment, greatly intensified by the full-scale armed aggression of the Russian Federation against Ukraine, has moved the protection of critical information infrastructure (hereinafter, CII) from the sphere of purely local technical tasks into the category of strategic imperatives for national survival. As substantiated in the study (Zhyvylo Ye. O., Dokil V. M., 2025), the essence of cybersecurity in the national segment of cyberspace under crisis management is determined by the need to ensure the resilience of critical infrastructure in the face of hybrid threats. This confirms the strategic nature of this task for the national security of the state (Onyshchenko S. et al., 2023). Modern cyberattacks on energy, transport, water supply and electronic communications facilities have taken on the features of coordinated hybrid operations in which the destruction of physical assets precedes destructive interference with technological and information systems or takes place at the same time (Krasnobayev V., Yanko A., Hlushko A., 2023). Clear examples include the attacks on Ukraine's energy system in 2015–2016 using the BlackEnergy and Industroyer malicious software (hereinafter, malware), incidents involving industrial control systems at chemical industry facilities, and systematic campaigns using wiper malware (WhisperGate, CaddyWiper, HermeticWiper) aimed at fully destabilising the operation of state institutions. Studies of cyberattacks as a new front in warfare and

analysis of Ukraine's experience in countering Russia's cyber aggression show the need for a comprehensive approach to CII protection that combines technological, organisational and legal mechanisms (Kalashnikova Yu. V., 2025).

A separate strategic challenge that must be taken into account when designing long-term CII protection architectures is ensuring that systems can withstand future quantum attacks. In particular, integrating post-quantum cryptographic algorithms into defence communications systems and sensor networks is a relevant direction that shapes the further development of national cybersecurity (Fesenko T. M. et al., 2026). Overall, these incidents and the evolution of threats show the urgent need to use comprehensive cyber-risk management technologies to improve the cyber resilience of strategic sectors of the national economy, as systematically examined in (Onyshchenko S. et al., 2024; Yanko A. et al., 2023).

As European integration processes intensify, Ukraine has faced the need not only to harmonise its legal framework but also to fundamentally restructure its national cyber-defence architecture. This process involves implementing key European directives and regulations (Directive (EU) 2022/2555 of the European Parliament and of the Council, 2014; Directive (EU) 2022/2557 of the European Parliament and of the Council, 2022; Regulation (EU) 2024/2847 of the European Parliament and of the Council, 2024; Regulation (EU) 2025/38 of the European Parliament and of the Council, 2024). These international acts effectively form a new paradigm of cyber resilience, in which the key focus is not so much on static perimeter protection as on continuous visibility, deployment of distributed monitoring, and operation of automated cyber-intelligence exchange systems.

At the same time, an analysis of the current state of domestic research and practical work in CII cybersecurity shows a significant imbalance. Most Ukrainian research publications, dissertations and regulatory and methodological documents focus on risk-management tools (ISO/IEC 27001:2022, The NIST Cybersecurity Framework, 2024), concepts for building centralised security operations centres, and the implementation of security information and event management systems. These elements are certainly basic components of cyber defence, but they describe mainly a reactive or

highly aggregated security model that does not fully account for the specific features of operational technology (hereinafter, OT) and deterministic industrial Internet of Things networks.

As a result of this focus, the architecture of distributed cyber-monitoring sensor networks, the role of telemetry-collection agents, and the operation of cyber-intelligence systems directly at the network "edge" remain relatively understudied in Ukrainian research. At the same time, sensors, local agents and distributed subsystems for collecting primary data form the first layer of visibility for CII facilities. The lack of a thorough theoretical basis and understanding of the specific requirements for deploying them in industrial control system environments (ICS/SCADA), deterministic networks and legacy systems means that even the most modern domestic SIEM systems operate on incomplete or distorted data and may be unable to identify complex targeted attacks at the OT level in time.

The European approach established in the above-mentioned legal acts requires a shift from isolated sectoral monitoring to federated distributed sensor networks (Yanko A. S. et al., 2022) that can generate standardised telemetry in near real time. This direction is particularly relevant in the context of developing the European Cybersecurity Operations Centre and the network of national security centres of EU Member States, with which Ukraine seeks to integrate.

The purpose of this monograph section is to address this scientific and technical gap by systematising European practices in the use of distributed cyber sensors; analysing the specific features of their integration into Ukraine's heterogeneous IT/OT CII environment; comparing commercial and open-source solutions; substantiating a three-tier architectural model of a sensor network with intelligent data processing at the edge; and developing practical recommendations for implementation in view of European legislative requirements and the challenges of martial law.

To build an integrated monitoring architecture for CII facilities, it is necessary to clearly distinguish traditional information protection tools (hereinafter, IPTs) from distributed cyber sensors. Traditional IPTs, such as firewalls and intrusion prevention systems, actively block or filter data flows based on known signatures and deterministic

rules. Cyber sensors and local agents, in contrast, are intended for the continuous collection of cyber-intelligence, telemetry and metadata. Their main task is to detect anomalies, transient threats and hidden vectors of infrastructure compromise (Yanko A. S., Makarenko O. I., 2022).

The fundamental difference between these classes of systems is that a cyber sensor is primarily a tool for passive observation and analysis, whereas an IPT enforces security policies. This difference is critical in a CII environment because actively blocking suspicious traffic in an OT segment can very likely disrupt the stability of a technological process, cause emergency equipment shutdown, or even lead to catastrophic physical consequences. Therefore, a modern CII monitoring architecture should be based on the fundamental principle “comprehensive visibility first, coordinated response next”. This approach is fully consistent with the CII risk-management methodology based on the “threats–vulnerabilities–consequences” triad, substantiated in (Zhyvylo Ye., Kuz V., 2023), which emphasises the clear priority of preventive monitoring over purely reactive measures.

In view of this principle, distributed sensors should be classified according to the level at which they interact with the infrastructure and the environment in which they operate.

1. Network-based sensors. The first category consists of network sensors that monitor without interfering with the operation of network equipment. These include passive traffic analysers (TAP/SPAN), specialised hardware devices that duplicate network traffic (Yanko A. S., Padusenko Ya. V., 2026). They are critical for OT segments because optical TAP devices provide complete galvanic and logical isolation from the monitored segment, preventing any reverse effect on the network. They are complemented by flow-telemetry sensors (NetFlow, IPFIX, sFlow), which collect aggregated metadata about network sessions. This makes it possible to detect anomalous communication patterns between ICS controllers and remote terminals, as well as promptly record unauthorised connections.

DNS sensors are used to detect the early stages of compromise. These tools analyse DNS requests and are designed to identify algorithmically generated domain

names used by botnets or command-and-control (C2) server addresses. Identifying these attack vectors at an early stage is a key element of the cyber-risk management system for CII facilities, as described in detail in (Zhyvylo Ye., 2024). In addition, because traffic encryption is widespread, TLS/SSL metadata analysis sensors are used. These modules record parameters of secure connections, including JA3/JA3S hashes, SNI fields and certificate characteristics, without decrypting the traffic itself. This makes it possible to identify malicious activity even in an encrypted environment.

2. Host-based agents and endpoints. The next level of the taxonomy consists of host sensors and agents that monitor endpoints directly. Telemetry-collection agents (eBPF, Wazuh, Osquery) are lightweight software that operates at the operating-system kernel level on engineering workstations, HMI panels and data-historian servers. In particular, the use of eBPF technology minimises computational overhead while providing full monitoring of system calls, registry modifications and process creation.

File integrity monitoring (FIM) sensors are used to protect against targeted modifications. These modules monitor critical configuration files and system directories in SCADA environments. They are highly effective in detecting unauthorised changes to the operating logic of programmable logic controllers, a characteristic attack vector in Triton/Trisis attacks. A further development of this direction is the use of application control and integrity verification mechanisms for PLC firmware.

For protection against targeted modifications, file integrity monitoring (FIM) sensors are used. These modules monitor critical configuration files and system directories in SCADA environments. They are highly effective in detecting unauthorised changes to the operating logic of programmable logic controllers, which is a characteristic vector in Triton/Trisis attacks. Endpoint Detection and Response (EDR) agents further develop this approach by combining detailed log collection with built-in behavioural analysis and machine-learning algorithms on endpoints.

3. OT/ICS protocol-specific sensors. The specific features of the CII environment require a third category, OT/ICS protocol sensors. Industrial protocol decoders play a key role. They perform deep packet inspection and can parse traffic from specific industrial protocols (Modbus TCP/RTU, DNP3, IEC 60870-5-104, IEC 61850,

PROFINET, OPC UA, EtherNet/IP, BACnet). These sensors analyse not only packet structure but also command semantics, such as attempts to change process setpoints without authorisation or to send critical equipment-control commands.

For comprehensive monitoring, these sensors are supplemented by physical-state and IT/OT-convergence sensors that monitor physical-environment parameters, including server-cabinet temperature, equipment vibration, voltage fluctuations and humidity. This makes it possible to detect complex cyber-physical attacks that leave no obvious digital traces in network traffic. Special attention is also paid to sensors on engineering workstations. They provide specialised monitoring of peripheral-device connections and the launch of engineering development environments (TIA Portal, RSLogix, EcoStruxure), reducing the risk of compromising automation firmware.

This classification shows that the main difference between a modern distributed sensor network and a conventional hierarchical SIEM architecture is the implementation of the "Edge-to-Core Analytics" concept. At Ukrainian CII facilities, communication channels between remote technological sites and the central control centre often have limited bandwidth or are unstable because they use microwave radio links, satellite communications or cellular networks. Continuous transfer of all raw traffic to a single security operations centre is therefore technically and economically impossible. As a result, modern edge cyber sensors must have sufficient computing resources to perform primary aggregation and filtering and to run intelligent models directly at the network edge. This approach sends only verified incidents and compressed threat vectors to the central core, enabling effective monitoring even when communications infrastructure is limited.

The European Union has developed a clear and consistent legal framework that effectively sets new standards for CII monitoring architectures. Successful integration of Ukraine into the European security space requires not only formal harmonisation but also the technical adaptation of these regulatory requirements. Distributed sensors are a basic element of the national cyber-intelligence system. The key legal acts and their effect on sensor-network architecture are considered below.

1. The NIS2 Directive and baseline visibility requirements. EU Directive

2022/2555 (NIS2), which significantly expanded the range of CII entities, requires in Article 21 the implementation of comprehensive cybersecurity risk-management measures, including mandatory threat monitoring and incident handling. The NIS2 requirements for continuous monitoring are implemented through distributed sensor infrastructure that operates throughout the CII cyber-risk assessment cycle, from threat identification to analysis of the consequences of compromise. This is consistent with the methodology described in (Zhyvylo Ye., 2024). To implement these requirements in practice, CII operators must deploy sensor networks that provide visibility not only into internal network traffic but also into potential supply-chain compromise vectors. This requires dynamic integration of sensors with software bill-of-materials registries to automatically identify vulnerabilities in deployed automation-system components.

2. The CER Directive and the convergence of physical and cyber resilience. The next step in the development of European regulation was EU Directive 2022/2557 on the resilience of critical entities. It emphasises the need for comprehensive protection against cyber and physical threats at the same time. Architecturally, this requires distributed sensors to support data convergence. Hardware and software monitoring systems must correlate events from physical security systems, including video surveillance, access-control systems and perimeter sensors, with anomalies in network telemetry. In practice, an attempt to gain unauthorised physical access to a control cabinet should automatically initiate enhanced logging and traffic mirroring, including a full PCAP network capture on the relevant switches, for subsequent digital forensic analysis. This convergence of physical and cyber security components reflects current trends in risk assessment and privacy auditing in information systems and is systematically substantiated in (Zhyvylo Ye., Shevchenko D., 2022).

3. The Cyber Resilience Act and embedded telemetry. The further development of the regulatory framework is associated with the implementation of EU Regulation 2024/2847 (Cyber Resilience Act), which establishes horizontal requirements for products with digital elements and obliges manufacturers to apply security-by-default principles. A key requirement of the regulation is that industrial devices include built-in mechanisms for the secure generation and transmission of security telemetry. In this

context, the future architecture of Ukraine's CII will partly be formed through the integration of agents embedded in industrial equipment. This can significantly reduce the cost of deploying third-party sensor systems and enable monitoring at the level of individual components.

4. The Cyber Solidarity Act and standardised data exchange. The regulatory framework is completed by EU Regulation 2024/1084 (Cyber Solidarity Act), which aims to create a common European data-exchange platform, the European SOCC. To ensure interoperability between Ukrainian systems and European partners, CII distributed sensors must normalise events and indicators of compromise in the standard STIX 2.1/TAXII 2.1 formats and provide native integration with MISP threat-sharing platforms. This provides a technical basis for automated cyber-intelligence exchange in near real time.

5. A matrix mapping sensors to EU regulatory requirements. To formalise and systematise these requirements, a compliance matrix has been developed. It links types of distributed cyber sensors to specific articles of European legal acts (Table 2.1).

Table 2.1

Sensor Compliance Matrix with the Requirements of EU Legal Acts

Sensor type	**NIS2 Directive**	**CER Directive**	**CRA Regulation**	**Cyber Solidarity Act**
Passive network TAP sensors	Art. 21(2)(d) – cyber-threat monitoring requirements	Art. 13(2) – technical resilience measures	Art. 13(1) – mandatory product certification	Automated IoC exchange support; integration with the EU platform Participation in European platforms
OT protocol analysers (Modbus, IEC 61850, DNP3, PROFINET)	Art. 24(2)(d) – supply-chain security	Art. 21(2)(d) – convergence of physical and cybersecurity	Art. 4(1) – security by design	
Host agents	Art. 16(1)(a) – technical security measures	Art. 13(1) – comprehensive risk assessment	Art. 4(1) – security by design	
Edge ML models (anomaly detection)	Art. 21(2)(e) – incident management	Art. 13(2) – technical resilience measures	support	

Sensor type	NIS2 Directive	CER Directive	CRA Regulation	Cyber Solidarity Act
Physical IoT sensors (temperature, pressure, vibration)	Art. 16(1)(a) – technical security measures	Art. 13(1) – comprehensive risk assessment	Art. 13(4) – embedded security telemetry	
PMU sensors (IEEE C37.118 for energy)	Art. 13(1) – Mandatory product certification		Art. 46(1) – software update mechanisms	
DNS/cyber-intelligence sensors	Art. 21(2)(d) – cyber-threat monitoring requirements		Not applicable	
Data diodes (one-way gateways)	Integration requirement	Integration requirement	Not applicable	
STIX/TAXII gateways (standardised exchange)	Integration requirement			Mandatory
MISP integration nodes (threat-sharing platforms)	Art. 21(2)(f) – business continuity			Mandatory

Source: compiled by the authors on the basis of Directive (EU) 2022/2555 (NIS2); Directive (EU) 2022/2557 (CER); Regulation (EU) 2024/2847 (Cyber Resilience Act); Regulation (EU) 2024/1084 (Cyber Solidarity Act).

The compliance matrix systematises the relationship between architectural components of distributed sensor networks and the regulatory provisions of the European legal framework for CII protection. The colour coding of the cells illustrates the degree and nature of the impact of specific types of cyber sensors on the implementation of regulatory requirements. A green indicator identifies direct regulatory compliance of a sensor class with specific articles of the directives; blue indicates an indirect or partial contribution to meeting the requirements; and yellow indicates support for the fundamental principles of cyber resilience and security by default. The absence of a visual marker in a cell means that there are no direct regulatory requirements to use the corresponding type of sensor equipment to verify the specific article.

An analysis of international and national legal acts on critical infrastructure

protection shows that their fundamental purpose is to minimise the risks of cyber threats that could disrupt the continuity of critical services, lead to loss of control over technological processes, compromise information resources or cause technological accidents.

At the same time, regulatory documents define only general risk-management principles and do not provide a unified mathematical framework for quantitatively assessing cyber risk when designing distributed cyber-monitoring sensor networks. Therefore, it is appropriate to represent risk as an integral indicator that accounts for both the probability of a threat occurring and the potential consequences of its impact on a critical infrastructure facility.

Thus, the risk of a specific cyber threat is determined by the following relationship:

$$R_i = P_i \cdot I_i, \tag{2.1}$$

where R_i is the risk of the i-th threat; P_i is the probability that the threat will occur; and I_i is the magnitude of the threat's potential impact on a critical infrastructure facility.

In practice, multiple interrelated cyber threats may exist at the same time at a CII facility. Therefore, the total risk is defined as:

$$R_{total} = \sum_{i=1}^{n} R_i, \tag{2.2}$$

where n is the number of current threats to the relevant critical infrastructure facility.

The proposed model makes it possible to quantify the overall level of cyber risk and rank threats by their severity, which is necessary for developing a risk-oriented architecture for a distributed sensor network.

Given the specific features of critical infrastructure facilities, an integral

criticality indicator should be used to set priorities for protecting individual information assets and technological processes:

$$Criticality = \alpha C + \beta I + \gamma A, \tag{2.3}$$

where C is the level of impact on confidentiality; I is the level of impact on integrity; A is the level of impact on availability; and α, β, γ are weighting coefficients for the significance of the respective components, subject to the condition:

$$\alpha + \beta + \gamma = 1, \quad \alpha, \beta, \gamma \in [0, 1]. \tag{2.4}$$

Unlike the classical CIA model, for most critical infrastructure facilities the most important parameter is continuity of technological processes. This makes it appropriate to assign a higher weighting coefficient to availability:

$$\gamma > \alpha, \quad \gamma > \beta. \tag{2.5}$$

For energy, transport and water-supply enterprises, the following distribution of weighting coefficients may be used:

$$\alpha = 0.2, \quad \beta = 0.3, \quad \gamma = 0.5 \tag{2.6}$$

In this case, the integral criticality indicator takes the following form:

$$Criticality = 0.2C + 0.3I + 0.5A. \tag{2.7}$$

The proposed indicator serves as an analytical tool for ranking CII facilities by criticality and setting priorities for cyber-sensor deployment. The resulting values make it possible to optimise the distributed-computing architecture by placing edge and fog nodes rationally. In addition, this tool supports the selection of relevant cyber-incident response scenarios, providing a basis for a comprehensive risk-oriented cyber-defence strategy.

Thus, the proposed formal model enables a shift from qualitative analysis of

regulatory requirements to quantitative risk assessment. It provides a methodological basis for designing distributed cyber-monitoring sensor networks for critical infrastructure facilities using the risk-oriented approach required by NIS2, ISO/IEC 27005, IEC 62443 and Ukrainian national cybersecurity legislation.

The main methodological and engineering problem in designing sensor networks for domestic CII facilities is that classical IT solutions cannot be directly extrapolated to OT environments. Industrial automation and control systems of the ICS/SCADA class have specific architectural and functional features that significantly limit the use of standard monitoring tools. Their key characteristics include strict determinism of operating processes, a long service life for legacy equipment (20 to 30 years), a lack of built-in cryptographic protection inherited from earlier designs, limited computing capabilities of industrial controllers, and zero tolerance for network delays. For these reasons, sensor-network architecture must be adapted to the specific features of each critical sector (Yanko A. S., Vyhivskyi R. A., 2022).

We will consider sensor use, starting with the energy sector, which is the most critical and technologically complex. Main and distribution power-grid facilities, including 330/750 kV substations and dispatch centres, use specific protocols such as IEC 61850 (GOOSE, SV, MMS), DNP3 and IEC 60870-5-104. Standard IT sensors cannot correctly parse the structure and semantics of these packets. An effective threat-detection tool is the deployment of specialised OT-IDS sensors connected to the network through hardware optical traffic splitters, which ensures non-invasive monitoring. Particular attention in the energy sector should be paid to monitoring synchrophasor measurements, which transmit data at a high rate of up to 120 frames per second using the IEEE C37.118 protocol. This requires edge sensors to provide microsecond-accurate timestamps and minimal data-processing latency.

While the energy sector is characterised by high data-transmission speeds and complex real-time protocols, water-supply and wastewater systems face a different challenge, the geographical dispersion of facilities. These systems use low-speed communication channels (GPRS/4G/LoRa) to transmit Modbus RTU/TCP traffic, which has no built-in authentication mechanisms. The optimal approach is to deploy

distributed sensor modules directly at remote telemetry terminals, with deep contextual analysis of industrial commands. Since active blocking of suspicious traffic by a sensor may cause an emergency shutdown of pumping equipment, a passive protection model is used. The sensor creates a cryptographically signed event log and transmits it through secure tunnels (IPsec/WireGuard) to a central aggregation node. A key task is to record anomalous changes in process setpoints, such as pressure or reservoir fill level, which may indicate an attempt to cause physical damage to the infrastructure.

Transport infrastructure is another critical sector that requires specific monitoring approaches. Rail transport (JSC Ukrzaliznytsia), aviation dispatch systems and seaports use highly specialised, often proprietary control protocols such as EBICAB 900, ETCS (European Train Control System) and AIS (Automatic Identification System). Cyber sensors for these systems must undergo strict industry certification and provide non-invasive monitoring of specialised engineering data buses. Integrating these sensors into the general security system requires close interaction with existing traffic-dispatch and navigation systems without disrupting their deterministic operating cycles.

Unlike traditional industrial systems, the telecommunications sector and related financial platforms are based on highly dynamic cloud architectures. Electronic communications network operators use virtualised network functions (NFV), software-defined networks (SDN) and cloud orchestration systems (Kubernetes, OpenStack). Sensor infrastructure in this sector must monitor not only network flows but also configuration files in virtualisation and containerisation environments, as these are primary targets of modern APT groups. The cybersecurity features of electronic communications systems examined in (Zhyvylo Ye. O., 2024) highlight the need for specialised sensors to monitor transaction platforms. Integrating such tools into the overall CII distributed-monitoring architecture is especially relevant for the financial sector as a key element of the state's critical infrastructure, where delays in data processing are unacceptable.

Regardless of sector, a common challenge for all CII sectors is the mistaken belief that Ukraine's OT networks are completely isolated from external cyberspace.

In practice, hidden communication channels exist through engineering USB drives, vendor remote-maintenance modems, or connections to IT segments for business reporting. To securely transfer telemetry from cyber sensors in isolated OT zones to a corporate SOC or cloud analytics systems, one-way hardware data gateways, known as data diodes, must be used. At the physical level, for example, through an optical transmitter with no return receiver, these devices make it impossible to penetrate or affect the technological process in the reverse direction through the threat-monitoring channel. They thus ensure fundamental protection of critical production processes.

To substantiate architectural decisions and select an optimal technology stack, it is necessary to review systematically the OT-monitoring platforms currently available on the market. This analysis covers both commercial solutions from leading global vendors and open-source platforms that can be adapted to the specific needs of Ukraine's CII.

1. Commercial OT platforms. Nozomi Networks (the Guardian platform) is one of the leading systems in the OT/ICS security segment. It uses high-performance passive sensors for automatic asset inventory and behavioural anomaly detection based on machine-learning algorithms. The platform supports more than 100 industrial protocols and provides native integration with external SIEM systems through STIX/TAXII standards and the Apache Kafka protocol.

Claroty (the Continuous Threat Detection platform) offers a sensor architecture focused on real-time anomaly detection. Its key feature is a powerful analytical toolkit for identifying vulnerabilities in legacy equipment without active scanning, as well as extensive support for specific protocols such as IEC 61850 and DNP3.

Dragos (the Dragos Worldview platform) is positioned as a specialised system for identifying attackers' industrial tactics, techniques and procedures. The platform is distinguished by unique sector-specific scenarios developed specifically for the energy and oil and gas sectors.

Comprehensive ecosystems are offered by Fortinet (FortiGate-OT and FortiSIEM) and Palo Alto Networks (IoT Security and Cortex XDR). These solutions combine next-generation firewalls, security-event management systems and network-

access control tools. In particular, Palo Alto's solution focuses on identifying IoT/OT devices and analysing their behaviour, followed by integration with Cortex XDR for extended threat response. Another development direction in commercial solutions is security operations centre automation. Integrated orchestration platforms such as Cisco SecureX can significantly reduce incident-response time and unify distributed sensor operations in complex heterogeneous networks (Fesenko T., Kalashnikova Yu., 2025).

2. Open-source platforms. Unlike commercial ecosystems, open-source solutions offer high flexibility and no dependency on a specific vendor.

Zeek (formerly Bro) is a powerful network analyser specialising in metadata collection and the creation of structured event logs. With support for extensions for industrial protocols (Modbus, DNP3), it serves as the technological foundation for many commercial OT solutions.

Suricata is a high-performance network analyser that supports IDS/IPS/NSM functions (Yanko A. S., Makarenko O. I., 2022). Its flexible rule system makes it highly effective in detecting attacks on OT protocols, and it can be used for both network and host monitoring.

Wazuh is an open-source XDR/SIEM platform that supports both host agents and network sensors. It has specialised OT-security modules and integrates with OpenSearch for scalable data storage and analysis.

OpenDNP3 should also be noted. It is an open-source implementation of the DNP3 protocol and can serve as a basis for building custom OT sensors. Snort is a classic network IPS/IDS that, although less performant than Suricata, remains in demand because of its large community support base. Security Onion completes this list. It is a comprehensive Linux distribution that combines Zeek, Suricata, Wazuh and Elastic Stack in a single integrated security-monitoring platform (Yanko A. et al., 2024).

3. Comparative analysis of technology solutions. To formalise the results of the review, the key characteristics of the platforms considered are summarised in a comparative table (Table 2.2).

Table 2.2.

Comparative Analysis of Commercial and Open-Source Solutions for OT Monitoring

Platform	OT protocols	Edge	SIEM/MISP	STIX/TAXII	IEC 62443	Cost	Adaptation
Nozomi	Full support	Full support	Full support	Full support	Full support	USD 500,000–1 million	Partial support
Claroty	Full support	Full support		Full support	Full support		Partial support
Dragos	Full support	Full support		Full support	Full support		Partial support
Zeek	Partial support	Partial support		Partial support	Absent	Free	Full support
Suricata	Partial support						Full support
Wazuh	Partial support	Full support		Partial support			Full support
Sec. Onion	Full support	Partial support		Full support		USD 50,000–100,000	Full support

Source: compiled by the authors on the basis of official documentation from Nozomi Networks; Claroty; Dragos; Zeek Project; Open Information Security Foundation (Suricata); Wazuh Inc.; Security Onion Solutions.

The comparative analysis shows that commercial platforms (Nozomi Networks, Claroty, Dragos) provide comprehensive support for OT protocols, have IEC 62443 certification and extensive edge-analytics capabilities, but are characterised by high licensing costs and dependence on foreign suppliers. Open-source solutions (Zeek, Suricata, Wazuh, Security Onion), in contrast, offer high flexibility for adaptation, no vendor lock-in and minimal software costs, but require significant investment in integration and configuration and qualified engineering staff.

In view of this, a hybrid approach is the optimal strategy for Ukraine's CII. It involves deploying commercial solutions at facilities of national importance, including nuclear and hydroelectric power plants and main power grids, and implementing adapted open-source platforms at municipally and locally owned facilities. A mandatory condition for this strategy is the unification of data-exchange formats at higher aggregation levels, which leads directly to the need to design a unified architectural model.

Summarising the analysis of European practices, the specific features of Ukraine's CII and the review of available technology solutions, this section proposes

a three-tier architecture for a distributed sensor network. The proposed model provides an optimal balance between monitoring depth, computing performance and cyber-resilience requirements.

The current challenges of ensuring the cyber resilience of Ukraine's CII facilities require a shift from centralised monitoring models to distributed architectures with intelligent data processing at the network edge. Traditional approaches based exclusively on centralised SIEM systems and SOC centres are not effective enough when communication bandwidth is limited at remote energy, water-supply and transport facilities, and when OT must be physically isolated from corporate IT networks.

The Edge-Fog-Core architectural paradigm offers a hierarchical model for distributed processing of cyber-monitoring data. It provides an optimal balance between local autonomy at CII facilities and centralised security management at the national level.

To enable quantitative assessment of the proposed architecture's effectiveness, the critical-infrastructure distributed sensor network can be formalised as a directed graph:

$$G = (V, E)\,, \tag{2.8}$$

where $V = \{v_1, v_2, \dots, v_n\}$ is the set of network nodes and $E = \{e_1, e_2, \dots, e_m\}$ is the set of information links between nodes.

Given the hierarchical structure of the proposed architecture, the set of nodes is defined as:

$$V = V_{Edge} \cup V_{Fog} \cup V_{Core}\,, \tag{2.9}$$

where V_{Edge} is the set of edge sensor nodes; V_{Fog} is the set of aggregation and local-analysis nodes; and V_{Core} is the set of central nodes at the national and international levels.

The following condition is satisfied:

$$V_{Edge} \cap V_{Fog} \cap V_{Core} = \varnothing, \tag{2.10}$$

which ensures the logical and functional separation of the architectural tiers.

The telemetry-transfer process is described by the routing function:

$$f(v_i) = \begin{cases} Fog_j, \ v_i \in V_{Edge}, \\ Core_k, v_i \in V_{Fog}. \end{cases} \tag{2.11}$$

Thus, each node at a lower tier has a uniquely defined aggregation node at the next higher tier.

The data-flow intensity for an individual node is defined as:

$$L_i = \sum_{k=1}^{N} \lambda_k, \tag{2.12}$$

where L_i is the total node load and λ_k is the flow intensity from an individual sensor.

The total delay in information transmission and processing in the system is defined by the expression:

$$D_{total} = D_{Edge} + D_{Fog} + D_{Core}, \tag{2.13}$$

where D_{Edge} is the local-processing delay; D_{Fog} is the aggregation delay; and D_{Core} is the central-analysis delay.

The proposed formalisation makes it possible to model the scalability, fault tolerance and performance of the architecture for different numbers of critical infrastructure facilities.

A fundamental basis of this architecture is local intelligent processing, which involves applying machine-learning algorithms directly on edge-level devices. This

makes it possible to detect anomalies in real time without transferring large volumes of raw data, which is critical for deterministic industrial networks with limited latency.

Another key principle is the physical isolation of operational-technology and information-technology environments, achieved through hardware one-way gateways. This approach ensures that technological processes cannot be compromised through monitoring channels while providing the necessary visibility into the state of OT systems. Cyber-physical data convergence also plays an important role. It is implemented by integrating readings from physical sensors with network telemetry and makes it possible to detect complex cyber-physical attacks that cannot be identified by analysing digital artefacts alone.

In addition, standardised European integration is based on STIX/TAXII 2.1 formats and integration with MISP platforms. This provides semantic interoperability with European cybersecurity infrastructure in line with NIS2, CER and the Cyber Solidarity Act. Federated model training completes this set of principles. It is a decentralised approach to improving machine-learning algorithms. It enables threat-detection quality to be improved collectively without transferring confidential data between critical infrastructure facilities, thereby preserving operators' privacy and trade secrets. Particular attention should be paid to federated GNN-XAI models for predicting account compromise in a Zero Trust environment. These models can detect threats at an early stage without centralising sensitive data, as substantiated in (Fesenko T. M., Kalashnikova Yu. V., 2025).

The proposed architecture accounts for the specific features of Ukraine's critical infrastructure, including the large share of legacy equipment with a service life of 20–30 years, limited resources for upgrading municipal CII facilities, and the need to operate under martial law and hybrid cyberattacks.

Figure 2.1 presents a three-tier architecture of a distributed sensor network for comprehensive cyber-threat monitoring at Ukraine's CII facilities.

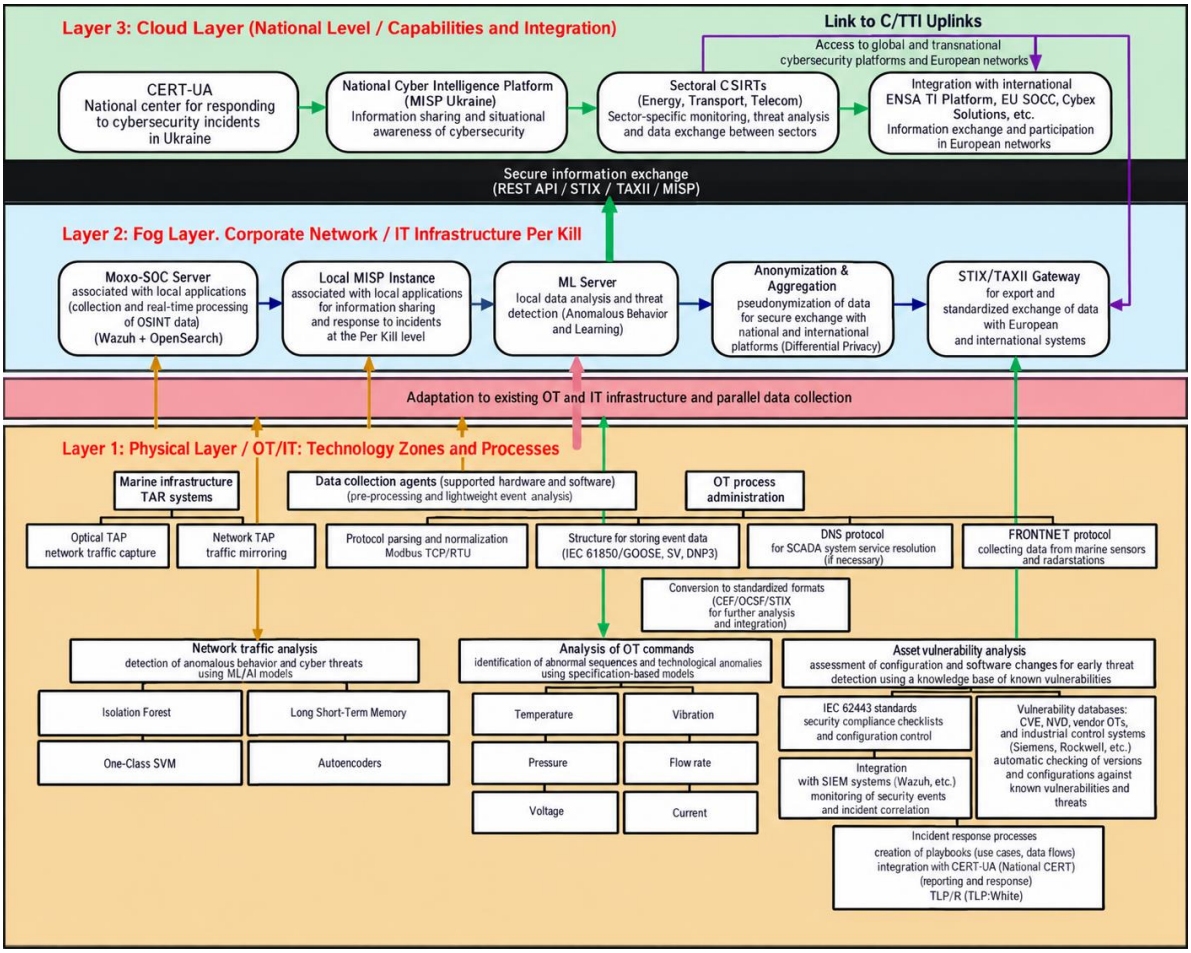


Figure 2.1. General Edge–Fog–Core architecture of a distributed sensor network for Ukraine's CII.

Source: authors' design based on ETSI Multi-access Edge Computing (MEC), OpenFog Reference Architecture (2017), Directive (EU) 2022/2555 (NIS2), and ENISA recommendations on NIS2 implementation.

The Edge tier (Tier 1 zone) is located directly in the operational environment of technological processes. It includes passive optical TAP sensors for duplicating network traffic; industrial protocol analysers (Modbus, IEC 61850, DNP3, PROFINET); eBPF-based host agents that collect telemetry at the operating-system kernel level on HMI stations and engineering workstations; lightweight machine-learning models (Isolation Forest, LSTM) for local anomaly detection; physical IoT sensors that monitor technological-environment parameters (temperature, pressure, vibration); and PMU sensors (IEEE C37.118) for high-precision synchrophasor measurements in power systems.

A Data Diode (the red-strip zone) provides physical one-way isolation between the OT and IT zones. It makes reverse data transmission impossible and protects

technological processes from compromise through monitoring channels. The Fog tier (Tier 2 zone) aggregates and preprocesses data at the level of an individual CII facility. A Micro-SOC server based on Wazuh and OpenSearch provides centralised collection of security events; a local MISP instance correlates them with global threats; an ML server with autoencoders and federated-learning mechanisms performs in-depth analysis to detect complex multi-stage attacks; an anonymisation and aggregation module based on differential privacy prepares data for secure transmission; and a STIX/TAXII gateway transforms information into standard formats for exchange with national and European systems.

The Core tier (Tier 3 zone) represents national and European cybersecurity infrastructure. CERT-UA coordinates responses to cyber incidents at the national scale; the national cyber-intelligence platform (MISP Ukraine) aggregates and correlates threats from different CII sectors; sectoral CSIRTs (energy, transport, telecommunications) provide specialised monitoring of sectoral facilities; and integration with European infrastructure (ENISA TI Platform, EU SOCC, Cyber Solidarity Act) provides access to current cyber intelligence and international mutual-assistance mechanisms.

The data flows are shown by coloured arrows. Orange arrows show the upward telemetry flow from Edge sensors through the Data Diode to the Fog tier. The green arrow marks the secure channel (TLS 1.3/mTLS/IPsec/WireGuard) for transferring aggregated data to the national tier. The purple arrow shows the reverse flow of updates to indicators of compromise and tactics, techniques and procedures from European partners, used to improve local threat-detection systems. Overall, the proposed architecture provides multilayer protection and local autonomy for CII facilities while preserving centralised visibility of threats at the national level. It also fully complies with European cybersecurity legislation for critical infrastructure.

Applying machine-learning algorithms directly at the Edge sensor level addresses the detection of zero-day attacks and anomalous states without placing a significant load on the network. The following mathematical models are substantiated for deployment on CII edge nodes:

Isolation Forest is an asymmetric clustering algorithm characterised by low computational complexity. It is suitable for Edge devices with limited CPU resources because it effectively detects anomalies in multidimensional network-traffic metadata vectors, such as packets per second and packet-length distribution.

Autoencoders are deep-learning models trained only on data from stable technological processes. During operation, anomalous traffic or destructive commands cause a sharp increase in reconstruction error, which serves as an incident trigger.

One-Class Support Vector Machine is a classical method for constructing an optimal separating hyperplane for deterministic data samples. It is suitable for use on local engineering workstations to monitor the stability of command sequences.

Long Short-Term Memory (LSTM) networks are recurrent neural networks designed to analyse time series. They achieve high accuracy in detecting deviations in cyclic industrial processes, for example, by assessing the regularity of GOOSE message transmission in IEC 61850 networks.

Specialised, lightweight and optimised frameworks, including TensorFlow Lite, ONNX Runtime and scikit-learn libraries adapted for POSIX-compatible industrial real-time operating systems, are used to implement these models on Edge sensors. Detecting hidden threats is an important aspect of securing the ML models themselves on edge devices. Stochastic-spectral methods for detecting such threats in neural networks, developed in (Zhyvylo Ye. et al., 2026), can be adapted to ensure the integrity of Edge models that process signals and telemetry.

Ukraine’s implementation of European cybersecurity directives (NIS2, CER, Cyber Solidarity Act) requires a reliable architecture for integrating the national cyber-threat monitoring system with European cybersecurity infrastructure. This task is critical because threat information must be exchanged promptly, responses to cross-border cyber incidents must be coordinated, and Ukraine must participate in European mutual-assistance mechanisms.

Figure 2.2 presents the organisational and technical interaction between the national and European segments, implemented through a specialised integration gateway.

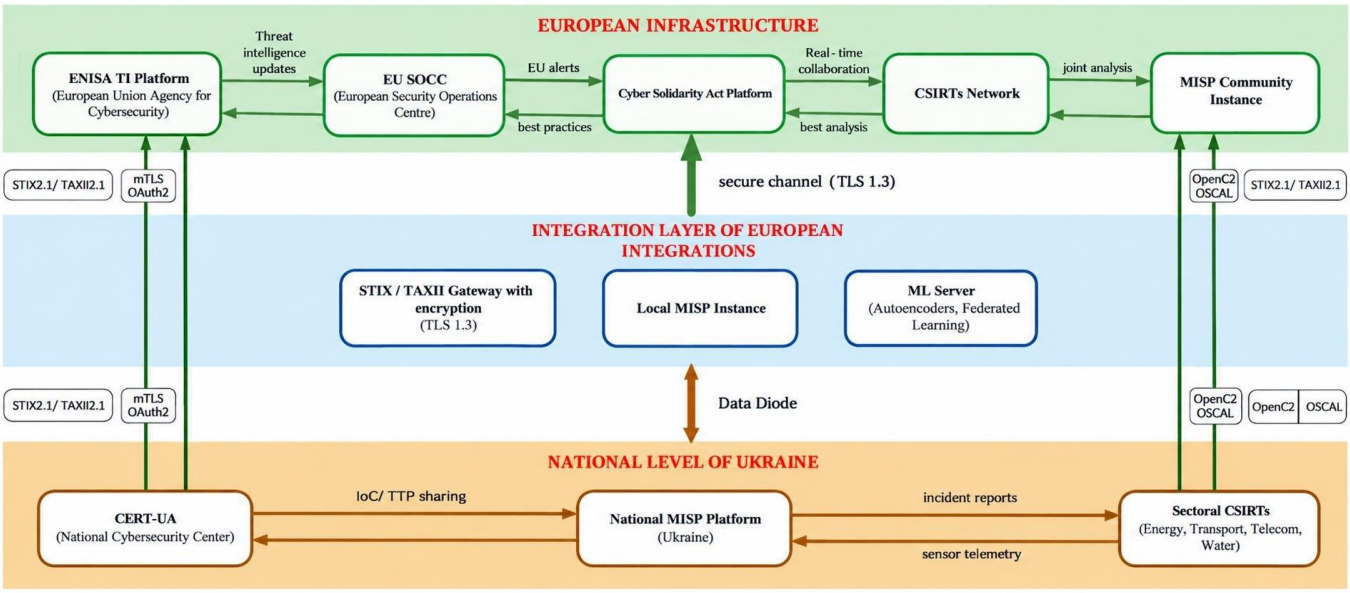


Figure 2.2. Architecture for integrating Ukraine's national sensor network with European cybersecurity infrastructure.

Source: authors' design based on Directive (EU) 2022/2555 (NIS2), Regulation (EU) 2024/1084 (Cyber Solidarity Act), ENISA recommendations on NIS2 implementation, MISP Project Documentation and OASIS STIX™ 2.1/TAXII™ 2.1 specifications.

The national tier of Ukraine (orange zone) includes CERT-UA (the National Cybersecurity Centre), which coordinates responses to cyber incidents and exchanges indicators of compromise (IoC/TTP sharing); the national MISP platform, which aggregates and correlates cyber-intelligence data; and sectoral incident-response centres (Sectoral CSIRTs) in the energy, transport, telecommunications and water-supply sectors, which transmit sensor telemetry and incident reports.

The European integration gateway (blue zone) provides technical integration with European infrastructure through three main components: an encrypted STIX/TAXII gateway (TLS 1.3) that converts data into standard exchange formats; an API integration layer that provides a unified programming interface for system interaction; and a threat-intelligence correlation engine that performs intelligent analysis and detects complex threats. The European infrastructure (green zone) includes the ENISA cyber-intelligence platform (ENISA TI Platform), which

aggregates threats from all Member States; the European Cybersecurity Operations Centre (EU SOCC), which coordinates responses to cross-border incidents; the Cyber Solidarity Act platform, which provides mutual-assistance mechanisms; the network of national CSIRTs of the Member States, for cooperation and exchange of experience; and the community of MISP instances, for decentralised threat sharing.

Data flows between the tiers include threat-intelligence updates from European infrastructure to the national tier; EU alerts about large-scale threats; shared practices and analysis; real-time collaboration; incident reports and sensor telemetry from the national tier to European infrastructure; and IoC/TTP sharing. The security protocols shown in the diagram include STIX 2.1/TAXII 2.1 for standardised cyber-intelligence exchange; mTLS and OAuth2 for authentication and authorisation; OpenC2 for command and control; OSCAL for assessing security controls; TLS 1.3 secure channels for data transmission; and hardware one-way gateways (Data Diodes) for physical isolation of critical segments. The proposed architecture complies with European cybersecurity legislation, ensures prompt exchange of threat information and enables Ukraine to integrate effectively into the European cybersecurity space.

The practical value of the proposed architecture can be demonstrated through a sensor-network deployment at a water-supply critical infrastructure facility in a medium-sized Ukrainian city with a population of 100,000-200,000. This sector was selected because it is critical to the population's daily life, its infrastructure is widely distributed, and it has specific cyber-physical risks associated with possible impacts on the physical parameters of water quality and the integrity of water-supply systems.

The typical structure of a water-supply and wastewater utility in a medium-sized Ukrainian city (Figure 2.3) includes a central dispatch service equipped with SCADA servers, HMI stations and engineering workstations for controlling technological processes. The water-intake infrastructure includes two or three first-lift pumping stations located 10–30 kilometres from the city centre, which supply water from underground or surface sources. The water-treatment system includes filtration stations and chlorination facilities, where water is prepared to drinking-water standards. The distribution network consists of ten to fifteen second-lift pumping stations in different

city districts and five to ten clean-water reservoirs equipped with level and pressure sensors. The wastewater system includes fifteen to twenty sewage pumping stations and a centralised treatment plant.

The total number of programmable logic controllers and remote terminal units is 50-80; there are 20-30 network switches and 5-10 servers. The hybrid communications-network architecture combines dedicated fibre-optic lines for reliable data transmission at some facilities with 4G/LTE cellular modems at others, where laying cable is economically impractical or difficult. This diversity of communication channels and their differing levels of security create additional cybersecurity challenges.

The sensor network is designed in accordance with the three-tier Edge-Fog-Core architecture, adapted to the specific features of a distributed water-supply infrastructure. At the Edge tier, each remote facility is equipped with a passive TAP sensor installed on an OT-zone switch to collect and analyse Modbus TCP traffic, the main communication protocol between RTU controllers and the central control system.

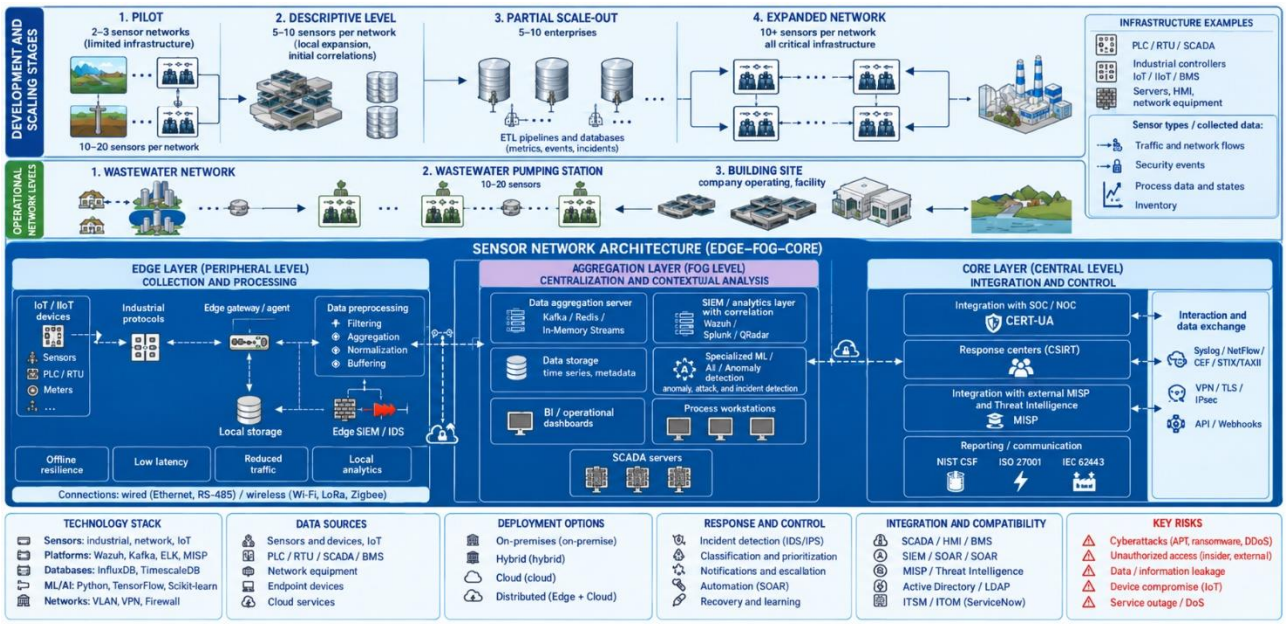


Figure 2.3. Deployment architecture of a distributed sensor network at a water-supply facility in a medium-sized city, with critical monitoring points marked.

Source: authors' design based on IEC 62443, NIST SP 800-82 Rev. 3, ENISA (2024) and CISA recommendations on cybersecurity for water-supply systems.

For local data processing, lightweight Edge analysers are deployed on Raspberry

Pi 4 single-board computers or industrial PCs (IPCs).

They run Zeek software for deep inspection of network traffic, Suricata for signature-based anomaly detection, and an Isolation Forest ML model for real-time anomaly detection without transferring large volumes of raw data to the central system. A critically important component is the installation of hardware one-way gateways (Data Diodes) to physically isolate the OT environment from IT networks while still allowing telemetry to be exported for monitoring.

At the aggregation tier (Fog), deployed in the central dispatch centre, a data-aggregation server (Micro-SOC) runs Wazuh Manager for centralised collection and correlation of security events and OpenSearch for log storage and indexing. A local MISP instance correlates local events with the global cyber-threat database, enriches data with context and generates structured indicators of compromise. A separate machine-learning server implements Long Short-Term Memory (LSTM) models to analyse time series of physical parameters (pressure, water level and flow rate). This makes it possible to detect complex cyber-physical attacks that appear as deviations of physical parameters from normal values. At the national tier (Core), integration with CERT-UA is provided through standard STIX/TAXII interfaces for automated threat-information exchange. Indicators of compromise are also published on the national MISP platform to warn other critical infrastructure operators about detected threats.

Critical monitoring points are identified by analysing the network architecture, identifying critical assets and assessing potential attack vectors. The first monitoring point is the boundary between OT and IT environments (DMZ), where a TAP sensor is installed together with a hardware Data Diode to monitor all traffic crossing this critical boundary. This placement makes it possible to detect attempts at unauthorised access from the corporate network to the technological network and to monitor legitimate data-transfer channels.

Engineering workstations running controller development and configuration environments (TIA Portal, RSLogix, EcoStruxure) are equipped with Wazuh Agent host agents to monitor the launch of engineering software, record connections to PLCs and monitor changes to control programs. This makes it possible to detect unauthorised

modifications to controller logic that could destabilise a technological process. For an additional layer of protection for privileged access to control systems, it is appropriate to use architectural and cryptographic models with intelligent access adaptation (Yanko A. S., Hlushko A. D., 2026). These combine AES symmetric encryption with machine-learning methods to build behavioural profiles of operators. This approach can reduce the probability of unauthorised use of privileges and adapt access levels in real time (Fesenko T. M. et al., 2026).

Each remote RTU controller is equipped with a passive TAP sensor and an Edge analyser for local monitoring of Modbus TCP and DNP3 traffic, detection of anomalous control commands and deviations in communication-session frequency. Particular attention is paid to chlorination stations, which are additionally equipped with physical-parameter sensors for chlorine concentration, pH and oxidation-reduction potential to detect cyber-physical attacks aimed at changing the chemical composition of water. Correlating cyber events, such as a change in dosing setpoints, with physical parameters makes it possible to detect and localise incidents promptly when they could threaten the life and health of the population.

The estimated cost of deploying a sensor network based on a hybrid approach (open-source software combined with industrial equipment) is approximately USD 180,000. Capital costs include the purchase and installation of Edge sensors (50 units × USD 1,500), totalling USD 75,000, including hardware components (Raspberry Pi 4 or industrial IPCs), network TAP adapters and peripheral equipment. Hardware one-way Data Diode gateways (10 units × USD 5,000) cost USD 50,000. This is a critical investment in the physical isolation of the OT environment. Deploying a Fog server with Wazuh and OpenSearch is estimated at USD 30,000, including server hardware, data-storage systems and backup. Commissioning, ML-model configuration, integration with existing systems and staff training cost USD 25,000.

The total project implementation period is estimated at 4-6 months. It includes a preliminary infrastructure audit and detailed project design (1 month); equipment and software procurement (1-2 months); physical installation of sensors and communications infrastructure (1-2 months); configuration of software components

and ML models (1 month); and testing and commissioning (1 month). This period is due to the need to obtain regulatory approvals, the difficulty of integrating with existing technological systems without stopping the process, and the need to train personnel to use the new monitoring systems.

Deploying a distributed sensor network significantly improves the cybersecurity of a critical infrastructure facility across several key indicators. In terms of visibility, it achieves 100% coverage of OT traffic and enables detection of all connections between RTU controllers and the SCADA system, including semantic analysis of industrial protocols at the application level. This removes the blind spots found in traditional monitoring approaches and enables a complete, real-time inventory of OT-environment assets.

Threat-detection time is reduced from hours or days, as is typical for manual log analysis or periodic audits, to seconds or minutes for critical anomalies. This is achieved by applying ML models at the Edge tier and automated event correlation at the Fog tier. It makes it possible to respond to incidents promptly before they cause significant disruption to the technological process or physical damage to equipment.

In terms of integration, automated exchange of indicators of compromise with CERT-UA and European partners is provided through standard STIX/TAXII interfaces. This improves overall situational awareness of threats and enables current cyber intelligence to be received from national and international partners. It meets the requirements of Article 21 of the NIS2 Directive on risk-management measures and Article 23 on incident reporting, thereby ensuring compliance with European legal requirements for cybersecurity of critical infrastructure. It should be emphasised that the results of integrating a distributed sensor network are consistent with cyber-risk management approaches aimed at ensuring the security of the national economic system. This relationship is substantiated in (Onyshchenko S. V. et al., 2024), particularly with regard to minimising operational risks and improving critical-infrastructure resilience.

In Ukraine, the transition from centralised SIEM systems to distributed sensor networks faces a number of specific technical, organisational, regulatory and economic

challenges that require comprehensive solutions at the state and departmental levels.

Technical challenges and dependence on foreign equipment. Most industrial sensors and hardware data diodes are manufactured in EU and US countries. Under martial law, this creates a risk of logistics delays and significant financial dependence. One way to address this challenge is to encourage the development of domestic hardware and software systems based on open-source software (Zeek, Suricata, Wazuh), develop domestic printed circuit boards and involve national laboratories in device certification under IEC 62443.

Regulatory barriers and data protection. Deep packet analysis at CII facilities may conflict with current legislation on the protection of trade secrets and restricted-access information. To address this issue, the State Service of Special Communications and Information Protection of Ukraine should develop new regulations and security profiles that would permit the use of differential privacy and homomorphic encryption when aggregating telemetry in Fog zones.

Staff shortages and operational resilience. Deploying thousands of distributed sensors requires highly qualified staff both at individual CII facilities and at sectoral CSIRTs. Addressing this shortage requires the integration of relevant specialised modules into the curricula of specialised higher education institutions, as well as the creation, under CERT-UA, of a national repository of industrial-threat signatures to provide prompt support to local engineers. These measures are consistent with current research and methodological recommendations on developing professional cybersecurity competencies during the digital transformation of the state (Zhyvylo Ye., 2023). They also take into account the need for joint training of defence forces personnel to perform cyber-defence tasks as part of total defence (Zhyvylo Ye., Zhyvylo I., 2021), which involves directly integrating higher-education programmes with the practical needs of CII operators.

Project funding. Most municipal enterprises cannot finance such systems on their own. This part can be addressed by actively attracting international technical assistance and CII-recovery grants from the World Bank and European funds, making the deployment of cybersecurity sensor systems a mandatory condition for allocating

funds to modernise facilities.

The paradigm for protecting Ukraine's CII is undergoing a fundamental transformation. Moving away from the outdated static model based exclusively on perimeter protection and centralised analysis (SIEM/SOC) in favour of a distributed cyber-sensor architecture is not merely a technical improvement but a strategic condition for ensuring national security and the state's cyber resilience.

The study confirms that distributed cyber sensors and edge-level agents form the initial visibility layer for heterogeneous infrastructure environments. Without this foundation operating properly, higher-level analytical systems (SIEM, SOC) lose effectiveness because their input data are incomplete and fragmented. European legal acts (NIS2, CER, CRA, Cyber Solidarity Act) clearly define the development directions. Sensor systems must be intelligent, native to OT environments and fully interoperable internationally through STIX/TAXII and MISP standards.

The proposed three-tier Edge–Fog–Core architecture, confirmed by a practical case study of a municipal water utility, demonstrates that a highly reliable cyber-monitoring system can be built even when legacy equipment and limited financial resources are used. Further research and practical development in this area should focus on creating domestic hardware and software tools for passive analysis of industrial networks, developing national profiles for cyber-intelligence data exchange, modernising specialised higher education, and fully integrating Ukraine's cybersecurity environment into a unified system of European security operations centres.

REFERENCES FOR SUBSECTION 2.1

1. Zhyvylo Ye. O., Dokil V. M. The Experience of Israel and the Republic of Korea in State Support Mechanisms and Cybersecurity System Organization. *National Interests of Ukraine*. 2025. No. 5 (10). P. 120–139. DOI: https://doi.org/10.52058/3041-1793-2025-5(10)-120-139.

2. The Mechanism of Information Security of the National Economy in

Cyberspace / S. Onyshchenko, A. Yanko, A. Hlushko, O. Maslii, V. Skryl. Proceedings of the 4th International Conference on Building Innovations. ICBI 2022 / ed. by V. Onyshchenko, G. Mammadova, S. Sivitska, A. Gasimov. Cham : Springer, 2023. Vol. 299. P. 791–803. DOI: https://doi.org/10.1007/978-3-031-17385-1_67.

3. Krasnobayev V., Yanko A., Hlushko A. Information Security of the National Economy Based on an Effective Data Control Method. *Journal of International Commerce, Economics and Policy*. 2023. Vol. 14, No. 3. Article 2350021. DOI: https://doi.org/10.1142/S1793993323500217.

4. Kalashnikova Yu. V. Cyberattacks as a New Front of War: Ukraine's Experience in Countering Russian Cyber Aggression. Abstracts of the 77th Scientific Conference of Professors, Lecturers, Researchers, Postgraduate Students, and Students of the University, Poltava, May 16–22, 2025. Poltava : National University "Yuri Kondratyuk Poltava Polytechnic", 2025. P. 524–526. URL: https://reposit.nupp.edu.ua/handle/PoltNTU/19282 (accessed: July 2, 2026).

5. Architectural and Cryptographic Model for Managing Special-User Systems with Intelligent Access Adaptation / T. M. Fesenko, M. O. Plakhtii, E. Yu. Rubin, Yu. V. Kalashnikova. *Modern Information Technologies in the Sphere of Security and Defence*. 2026. Vol. 55, No. 1. P. 84–99. DOI: https://doi.org/10.33099/2311-7249/2026-55-1-84-99.

6. Cyber Risk Management Technology to Strengthen the Information Security of the National Economy / S. Onyshchenko, Ye. Zhyvylo, A. Hlushko, S. Bilko. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu. 2024. No. 5. P. 136–142. DOI: https://doi.org/10.33271/nvngu/2024-5/136.

7. Economic Cybersecurity of Business in Ukraine: Strategic Directions and Implementation Mechanism / A. Yanko, A. Hlushko, S. Onyshchenko, O. Maslii. *Economic and Cyber Security*. Kharkiv : PC TECHNOLOGY CENTER, 2023. P. 30–58. DOI: https://doi.org/10.15587/978-617-7319-98-5.CH2.

8. 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). *Official Journal of the European Union*. 2022. L 333. P. 80–152. URL: http://data.europa.eu/eli/dir/2022/2555/oj (accessed: July 19, 2026).

9. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC (CER Directive). *Official Journal of the European Union*. 2022. L 333. P. 164–198. URL: http://data.europa.eu/eli/dir/2022/2557/oj (accessed: July 19, 2026).

10. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No. 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). *Official Journal of the European Union*. 2024. L 2024/2847. 20 November 2024. URL: http://data.europa.eu/eli/reg/2024/2847/oj (accessed: July 19, 2026).

11. Regulation (EU) 2025/38 of the European Parliament and of the Council 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. L 2025/38. 15 January 2025. URL: http://data.europa.eu/eli/reg/2025/38/oj (accessed: July 19, 2026).

12. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. 3rd ed. Geneva : International Organization for Standardization, 2022. URL: https://www.iso.org/standard/27001 (accessed: July 2, 2026).

13. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD : National Institute of Standards and Technology, 2024. 32 p. DOI: https://doi.org/10.6028/NIST.CSWP.29. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (accessed: July 2, 2026).

14. Yanko A. S., Martynenko A. M., Trykoz V. V. Network Sensors and

Detectors as an Effective Tool for Data Monitoring. *Control, Navigation and Communication Systems*. 2022. No. 1 (67). P. 98–101. DOI: https://doi.org/10.26906/SUNZ.2022.1.098.

15. Yanko A. S., Makarenko O. I. The Concept of a Network Intrusion Detection and Prevention System. *Control, Navigation and Communication Systems*. 2022. No. 2 (68). P. 59–67. DOI: https://doi.org/10.26906/SUNZ.2022.2.059.

16. Zhyvylo Ye., Kuz V. Risk Management of Critical Information Infrastructure: Threats-Vulnerabilities-Consequences. *Theoretical and Applied Cybersecurity*. 2023. Vol. 5, No. 2. P. 68–80. DOI: https://doi.org/10.20535/tacs.2664-29132023.2.280377.

17. Yanko A. S., Padusenko Ya. V. A Distributed Intelligent System for Semantic Monitoring of Heterogeneous Data in the Telegram Messenger Based on Vector Representations. *Taurida Scientific Herald. Series: Technical Sciences*. 2026. No. 3. P. 221–229. DOI: https://doi.org/10.32782/tnv-tech.2026.3.23.

18. Zhyvylo Ye. Stage of Risk Assessment of Critical Infrastructure Cyber Security Breach. Information Control Systems and Technologies (ICST–ODESA–2024) : materials of the XII International Scientific and Practical Conference, Odesa, 23–25 September 2024. Odesa : Helvetica Publishing House, 2024. P. 52–55. URL: https://icst-conf.com/2024.pdf (accessed: July 19, 2026).

19. Zhyvylo Ye. O., Shevchenko D. G. Risk Assessment of Cyber Security and Control of Privacy in Public Administration Information Systems. *Collection of Scientific Works of the Military Institute of Taras Shevchenko National University of Kyiv*. 2022. No. 75. P. 66–77. DOI: https://doi.org/10.17721/2519-481X/2022/75-07.

20. Yanko A. S., Vyhivskyi R. A. Computer Network Protection System. *Control, Navigation and Communication Systems*. 2022. No. 2 (68). P. 91–94. DOI: https://doi.org/10.26906/SUNZ.2022.2.091.

21. Zhyvylo Ye. O. Macroeconomic Stability of the State under Cyber Threats. *Current Issues in Public Administration*. 2024. No. 2 (65). P. 347–369. DOI: https://doi.org/10.26565/1684-8489-2024-2-18.

22. Fesenko T., Kalashnikova Yu. Use of Cisco SecureX for SOC

Automation. *Control, Navigation and Communication Systems*. 2025. No. 4 (82). P. 138–143. DOI: https://doi.org/10.26906/SUNZ.2025.4.138.

23. Detection of LDDoS Attacks Using SDN Networks with Machine Learning Elements / A. Yanko, A. Prokudin, I. Fil, O. Kruk. *Measuring and Computing Devices in Technological Processes*. 2024. No. 4. P. 287–296. DOI: https://doi.org/10.31891/2219-9365-2024-80-36.

24. Fesenko T. M., Kalashnikova Yu. V. Federated GNN-XAI Model for Predicting Account Compromise in a Zero Trust Environment. *Cybersecurity: Education, Science, Technology*. 2025. Vol. 3, No. 31. P. 602–619. DOI: https://doi.org/10.28925/2663-4023.2025.31.1049.

25. Stochastic-Spectral Methods for Detecting Hidden Triggers in Neural Networks for 6G Signal Processing / Ye. Zhyvylo, A. Chornyi, I. Romashko, Yu. Kalashnikova. *Measuring and Computing Devices in Technological Processes*. 2026. No. 2. P. 110–119. DOI: https://doi.org/10.31891/2219-9365-2026-86-14.

26. Yanko A., Hlushko A. A Method for Binary Representation of Residues Based on the Ring Shift Principle to Enhance the Digital Resilience of Cryptographic Systems. *Transactions of Kremenchuk Mykhailo Ostrohradskyi National University*. 2026. No. 2 (157). P. 187–194. DOI: https://doi.org/10.32782/1995-0519.2026.2.19.

27. Zhyvylo Ye. O. Identifying and Acquiring Modern Cybersecurity Workforce Competencies amid the State's Digital Transformation. *Current Issues in Public Administration*. 2023. No. 2 (63). P. 111–127. DOI: https://doi.org/10.26565/1684-8489-2023-2-08.

28. Zhyvylo Ye. O., Zhyvylo I. O. Joint Training of the Cyber Security Defense Forces Personnel in the Conditions of Total State Defense. *Theory and Practice of Public Administration*. 2021. No. 2 (73). P. 144–153. DOI: https://doi.org/10.34213/tp.21.02.16.

2.2. European Regulation of the Development and Deployment of Intrusion Detection and Prevention Systems

Vladyslav RAKSHA

Zaporizhzhia National University

Modern society's digital infrastructure depends on the continuous operation of computer networks, cloud services, industrial control systems, Internet of Things (IoT) devices, transport and communication platforms etc. As these environments expand and become more complex, the attack surface grows, network traffic becomes more heterogeneous, and conditions emerge for multi-stage intrusions and incidents that are difficult to detect. Under these conditions, intrusion detection systems (IDS) and intrusion prevention systems (IPS) are not merely technical tools for analyzing network and system activity; they are also integral to organizational monitoring, incident response, and the continuity of critical services.

Machine learning and deep learning extend IDS/IPS capabilities for detecting anomalous behavior, previously unseen attacks, and complex relationships among network events. Their practical use, however, is complicated by class imbalance, temporal distribution shift, sensitivity to feature engineering, limited cross-domain transferability, and substantial computational cost. IDS/IPS evaluation therefore cannot rely solely on accuracy obtained on a single benchmark dataset. It should also consider detection recall, false-alarm rate, detection latency, robustness to changes in the network environment and adversarial manipulation, secure model updates, and the ability to integrate detection outputs into incident-response workflows.

In the European Union, these technical issues increasingly have a regulatory dimension and are governed by a combination of horizontal, sector-specific, and product-oriented legislation. Comparative analysis of DORA, NIS2, the AI Act, and the Cyber Resilience Act indicates common requirements concerning risk management, technical security controls, monitoring, and incident reporting, although the instruments differ in scope, terminology, reporting timelines, and supervisory mechanisms (Correia A., Gonçalves A., 2024). The European regulatory framework should therefore be viewed as an interconnected system in which requirements for cybersecurity, digital operational resilience, security of products with digital elements,

and responsible use of artificial intelligence complement one another (Bolgouras V. et al., 2025).

At the organizational level, the NIS2 Directive establishes requirements for cybersecurity risk management, monitoring of networks and information systems, incident handling, and business continuity for essential and important entities (European Parliament and Council of the European Union. Directive (EU) 2022/2555, 2022). In the financial sector, these provisions are complemented by DORA, which regulates information and communication technology (ICT) risk management, digital operational resilience testing, third-party provider oversight, and reporting of major incidents (European Parliament and Council of the European Union. Regulation (EU) 2022/2554, 2022). In this context, IDS/IPS support continuous activity monitoring, anomaly detection, alert generation, and collection of data required for incident analysis and response.

A separate regulatory layer applies to IDS/IPS as software or software-hardware products with digital elements. The Cyber Resilience Act (CRA) extends cybersecurity requirements across the entire product life cycle, including secure design, secure configurations, vulnerability management, updates, technical documentation, and conformity assessment (European Parliament and Council of the European Union. Regulation (EU) 2024/2847, 2024). General requirements of EU legislation may be further specified by harmonised standards developed by the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI).

Once a reference to a harmonised standard is published in the Official Journal of the European Union, voluntary application of that standard may provide a presumption of conformity with the legislative requirements covered by it. A product designed and tested in accordance with the applicable provisions of such a standard is therefore presumed to satisfy the corresponding legal requirements unless evidence demonstrates otherwise. A harmonised standard does not replace mandatory legislation; rather, it provides one technical route for demonstrating compliance. Manufacturers may use alternative technical solutions, but must then substantiate conformity through other evidence (Mueck M., Gaie C., 2025). Accordingly, IDS/IPS conformity depends not only on attack-detection performance, but also on product

security, reproducibility of testing, and the security of development, maintenance, and update processes.

For machine-learning-based IDS/IPS, Regulation (EU) 2024/1689, the AI Act, adds another relevant layer. The use of machine-learning algorithms does not automatically make an IDS/IPS a high-risk AI system; applicable requirements depend on the system's intended purpose, deployment context, and the potential consequences of erroneous decisions. For high-risk systems, the AI Act requires appropriate levels of accuracy, robustness, and cybersecurity, consideration of reasonably foreseeable misuse, and protection against data and model poisoning, adversarial examples, and other forms of unauthorized interference (CEN-CENELEC, 2025). Thus, the AI Act addresses properties of the AI system itself, whereas NIS2 and DORA govern the organizational and technological environment in which it operates, and the CRA addresses product security throughout the life cycle.

Existing synthesis studies examine the interaction among NIS2, DORA, the CRA, and the AI Act, the role of harmonised standards, and common requirements for risk management, monitoring, and reporting (Correia A., Gonçalves A., 2024; Bolgouras V. et al., 2025; Mueck M., Gaie C., 2025; Teichmann F., 2026). The compliance-by-design approach requires regulatory obligations to be considered when defining product functions, architecture, controls, testing procedures, and maintenance processes (Canavese D., Ferreira A., Kamm L., 2026). For IDS/IPS, however, this approach must also account for the technical nature of the detection method, the type of processed data, feature and alert generation, dependence on the operational environment, and the expected failure modes.

The research problem is the absence of an integrated systematization linking the technical characteristics and limitations of different IDS/IPS classes to the organizational, product-level, and algorithmic requirements of European regulation. Existing legal instruments prescribe monitoring, logging, response, secure development, and vulnerability-management functions, but do not establish universal numerical thresholds for accuracy, recall, false-positive rate, latency, resource consumption, transferability, or robustness to distribution shift and adversarial manipulation. Regulatory compliance and technical effectiveness are therefore related, but still insufficiently aligned, dimensions of IDS/IPS assessment.

The aim of this section is to systematize the technical characteristics and limitations of contemporary IDS/IPS approaches and to map them to the organizational, product-level, and AI-system requirements established by the European regulatory framework.

The technical characteristics of intrusion detection systems determine not only attack-recognition performance but also requirements for testing, documentation, updating, and integration with response processes. Signature-based, anomaly-based, hybrid, and machine-learning-based systems differ in their decision mechanisms, data requirements, ability to detect previously unseen threats, computational complexity, and failure modes. Analysis of IDS methods is therefore a prerequisite for determining which system components, processes, and characteristics are subject to European regulatory requirements.

This section focuses primarily on intrusion detection systems because detection and classification of suspicious activity form the basis for subsequent response. Intrusion prevention systems are treated as an extension of IDS in which analytical outputs are used to automatically block, isolate, or restrict malicious activity. Most machine-learning and deep-learning studies evaluate attack-recognition performance rather than mechanisms that actively affect traffic. Accordingly, the term IDS is used predominantly in the technical review, while IDS/IPS is used for requirements common to both detection and prevention systems.

By decision method, IDS are commonly divided into signature-based, anomaly-based, and hybrid systems. Signature-based systems match observed events against predefined rules or patterns of known attacks. Their advantages include relative decision transparency, the ability to explain why an alert was generated, and high effectiveness against known threats. Their dependence on an up-to-date rule base, however, limits detection of zero-day, modified, and multi-stage attacks. In distributed Wi-Fi environments, signature-based mechanisms can be supplemented by cooperative multi-channel analysis, although performance remains dependent on the threat model and deployment architecture (Thankappan M. et al., 2024).

Anomaly-based IDS build a model of normal or previously known behavior and detect deviations from that model. This enables detection of previously unseen attacks but creates the problem of distinguishing malicious activity from legitimate changes in

operating conditions. Software updates, new devices, network reconfiguration, or seasonal load changes may increase false positives. Hybrid systems combine signature and anomaly analysis in an attempt to preserve rule-based explainability while detecting unknown threats; however, this increases architectural complexity, threshold-tuning requirements, and the difficulty of interpreting interdependent decisions (Chang V. et al., 2022; Alsubhi K., 2024; Almalawi A. et al., 2025; Al Sawafi Y. et al., 2023).

IDS classification is not limited to the detection method. Deployment location determines the source of monitored events; architecture determines how components are coordinated; and the operational environment determines acceptable computational cost, latency, and consequences of erroneous decisions. The principal classification criteria used in the literature are summarised in Table 2.3.

Table 2.3

Classification of Intrusion Detection Systems

Criterion	Main types	Description
Deployment location	host-based, network-based, hybrid	determines whether local host events, network traffic, or both are analyzed
Detection method	signature-based, anomaly-based, hybrid	determines how decisions are produced and whether previously unseen attacks can be detected
Architecture	centralized, distributed, cooperative	determines computation placement, data exchange, and coordination among components
Operational environment	general-purpose networks, IoT, VANET/IoV, ICS/SCADA, cloud and edge systems	determines data types, resource constraints, acceptable latency, and consequences of errors
Response mode	passive detection, automated prevention	determines whether the system only generates alerts or directly affects traffic and access

Host-based IDS analyze system calls, logs, processes, and local events on an individual host (Sworna Z. T., Mousavi Z., Babar M. A., 2023). Network-based systems use packets, flows, and statistical characteristics of network connections, while hybrid systems combine local and network data sources. Centralized solutions facilitate coordinated analysis but create dependence on a central component. Distributed and cooperative architectures are better suited to geographically dispersed environments, but require secure data exchange, synchronization, and trust management among participants (Thankappan M. et al., 2024; Chang V. et al., 2022; Alsubhi K., 2024;

Belenguer A. et al., 2022; Mármol Campos E. et al., 2022; Bhavsar M. H. et al., 2024; Reis M. J. C. S., 2025; Thein T. et al., 2024; Huang J. et al., 2025).

From a regulatory perspective, this heterogeneity means that identical functional requirements are implemented differently. For a host-based IDS, protection of local logs and access control are critical; for a network-based IDS, visibility and throughput are central; and for a distributed IDS, data-exchange integrity and participant management become particularly important.

Classical machine-learning methods remain widely used in IDS, especially for tabular features derived from network flows. Common approaches include decision trees, random forests, support vector machines, nearest-neighbor methods, Bayesian models, and ensembles (Ahmad I. et al., 2022; Alosaimi S., Almutairi S. M., 2023; Abu Alghanam O. et al., 2023; Ali M. et al., 2023; Fraihat S. et al., 2023; Xu B. et al., 2023; Fatani A. et al., 2023; Ahmed U. et al., 2024). Their advantages include relatively low computational cost, fast inference, and partial interpretability. Tree ensembles and stacking can improve classification robustness by combining decisions from multiple models (Ali M. et al., 2023; Ahmed U. et al., 2024).

The performance of classical models depends strongly on the feature set. Dimensionality reduction and feature selection may use correlation analysis, recursive feature elimination, and optimization algorithms (Ahmad I. et al., 2022; Abu Alghanam O. et al., 2023; Fraihat S. et al., 2023; Xu B. et al., 2023; Fatani A. et al., 2021). Features selected on one dataset do not necessarily remain informative in another network: their value depends on protocols, topology, flow aggregation, user profiles, and represented attack classes. High performance on a single benchmark is therefore insufficient evidence of model transferability.

The construction of training and test sets is another important issue. Random shuffling may place temporally or operationally related flows in different subsets and thereby overestimate generalization. Operational validation is better supported by temporal splits, testing on a different network segment, or evaluation using data collected after changes in the environment configuration.

The main limitation of classical models is therefore not necessarily insufficient classification capacity, but dependence on feature stability and data-generation

conditions. This dependence should be reflected in dataset documentation, reproducibility procedures, and post-deployment model-quality monitoring.

Deep neural networks can learn complex representations of network events automatically. Fully connected networks are applied to tabular features, convolutional networks to local patterns, and recurrent LSTM and GRU models to sequential data. Hybrid CNN-LSTM architectures combine local feature extraction with temporal-dependency modeling (Halbouni A. et al., 2022; Al S., Dener M., 2021; Balla A. et al., 2023; Alaghbari K. A., et al., 2023; Bakhsh S. A., 2023; Almalawi A., et al, 2025; Al Sawafi Y., 2023).

High scores for deep models are often reported on datasets containing pre-engineered and normalized features. A more complex architecture does not guarantee an advantage when input records lack meaningful spatial or temporal structure. Applying a recurrent network to independent aggregated flows may increase computational cost without a corresponding improvement in detection quality. Architecture selection should therefore be driven by data properties rather than by the general expressive capacity of neural networks.

Class imbalance is a separate challenge: rare attacks are often represented by far fewer observations than benign activity or common attack classes. Over- and under-sampling techniques, including SMOTE, ADASYN, Tomek Links, and NearMiss, can partially rebalance the classes (Al S., Dener M., 2021; Balla A. et al., 2023). However, synthetically generated records do not always correspond to valid combinations of network parameters. This is particularly important in cyber-physical and industrial systems, where relationships among features are constrained by protocols and physical processes.

Autoencoders learn to reconstruct input data and use reconstruction error as an anomaly score (Alaghbari K. A. et al., 2023; Ortega-Fernandez I. et al., 2024; Sharmila B. S., Nagapadma R., 2023). They are useful when labeled attack data are scarce, including IoT, SCADA, and edge environments. A high reconstruction error, however, is not conclusive evidence of an attack: it may result from an operating-mode change, a device update, a new traffic pattern, or a sensor fault. Threshold selection is therefore critical because it determines the trade-off between missed attacks and false alerts.

Quantization, pruning, and parameter clustering reduce memory use and inference time for autoencoders, improving their suitability for resource-constrained devices (Sharmila B. S., Nagapadma R., 2023). Computational optimization can nevertheless change the distribution of reconstruction errors; after model compression, the anomaly threshold must therefore be recalibrated and detection performance re-evaluated.

For regulatory assessment of neural IDS, it is important to document the architecture, provenance of training data, class-balancing procedure, threshold-selection method, and changes introduced during model optimization. Without this information, tests cannot be reproduced and changes in false-positive and false-negative rates cannot be adequately explained.

Transformer-based IDS use self-attention to model dependencies between distant elements of a sequence (Wu Z. et al., 2022; Manocchio L. D. et al., 2024; Jiang X. et al., 2025). Their potential advantage is the ability to analyze multi-step attacks and long-range relationships among events. Performance, however, depends on sequence construction, sequence length, and the presence of meaningful temporal structure. If NetFlow records - aggregated descriptions of network flows containing endpoint addresses and ports, protocol, duration, and transferred data volume - are treated as independent observations without temporal and contextual relationships, the benefits of transformer self-attention over simpler machine-learning methods may be limited. Transformer computational cost also affects inference latency and feasibility for streaming deployment.

Large language models do not currently replace specialized network-traffic classifiers, but they can support contextual alert analysis, explanation generation, and retrieval of related information (Houssel P. R. B., 2024). Their explanations require factual verification because linguistic plausibility does not guarantee consistency with actual network events. Knowledge distillation can transfer some capabilities of a complex model to a smaller one and reduce computational requirements (AL-Nomasy N., 2025), but model reduction may degrade recognition of rare classes or alter behavior outside the training distribution.

Graph neural networks represent network infrastructure as nodes and edges corresponding to hosts, devices, flows, or communication events. This representation

can capture topology, recurring interactions, and temporal dynamics. Self-supervised and dynamic graph models may detect structural anomalies without complete labeling (Lo W. W. et al., 2022; Caville E. et al., 2022; Xu R. et al., 2024; Liu J., Guo M., 2025).

A graph, however, is not a neutral representation. Results depend on which objects are defined as nodes, how edges are constructed, the duration of the temporal window, and how the graph is updated. Changing graph-construction rules may affect predictions as strongly as changing model parameters. Further limitations include message-passing scalability, latency, explainability, and attacks on graph structure (Lo W. W. et al., 2022; Zhong M. et al., 2024; Liu J., Guo M., 2025).

Transformer, language, and graph-based models increase reproducibility requirements. Documentation must cover not only training data and model parameters but also the construction of sequences, graphs, contexts, and explanations. These requirements are directly related to auditability, technical documentation, and change control.

Transfer learning is used to adapt IDS to a new environment when only limited locally labeled data are available. This approach has been studied for IoT, automotive CAN networks, VANETs, and industrial systems (Rodríguez E. et al., 2022; Gad A. R. 2021; Khatri N. et al., 2023). A model trained in one domain can provide an initialization for another, but adaptation effectiveness depends on similarity in protocols, features, attack types, and normal operating behavior.

Negative transfer may occur when patterns learned in the source domain do not match the target environment and performance becomes worse than training on local data alone. Evaluation should therefore compare the transferred model with a local baseline and assess performance not only for common but also for rare classes.

Federated learning enables a shared model to be trained without centralizing raw data. Devices or organizations transmit parameter updates that are aggregated centrally or in a distributed manner (Belenguer A. et al., 2022; Mármol Campos E. et al., 2022; Bhavsar M. H. et al., 2024; Reis M. J. C. S. 2025; Thein T. T. et al., 2024; Makris I. et al., 2025). This reduces the need to transfer sensitive logs and network traffic, but does not eliminate the risk of information leakage through model updates.

Non-independent and non-identically distributed local data complicate the construction of a single global model. Participants may use different device types,

traffic profiles, and attack sets. Personalized federated approaches can partly accommodate these differences but increase model-version management complexity. Other risks include communication overhead, long-term traffic drift, unreliable participants, and poisoning of local updates (Mármol Campos E. et al., 2022; Thein T. T. et al., 2024).

A federated IDS must define participant-admission rules, protect update channels, detect anomalous contributions, log aggregation operations, and support rollback to a previous model version. The advantage of decentralized data is therefore accompanied by additional requirements for trust management, change control, and a secure model life cycle.

IDS models may be deliberately manipulated both during training and during operation. Research addresses label and model poisoning, evasion attacks, feature manipulation, and adversarial traffic generation (Jmila H., Ibn Khedher M., 2022; Debicha I. et al., 2023; Papadopoulos P. et al., 2021; Mari A.-G. et al., 2023). Such attacks can reduce the probability of detecting malicious activity or generate excessive false alarms.

A fundamental distinction must be made between modifications in feature space and modifications to realizable network traffic. Numerical perturbation of an individual record cannot always be implemented as a valid packet sequence while preserving the functionality of the attack (Debicha I. et al., 2023). Arbitrary changes in connection duration, packet count, or protocol flags may violate internal feature dependencies. Adversarial-robustness evaluation should therefore account for network semantics and the practical feasibility of adversarial examples.

Domain dependence is evident in studies of IoT, RPL, smart homes, wireless sensor networks, IoV/VANET, CAN, SCADA, industrial, cloud, and edge systems (Alsubhi K., 2024; Balla A. et al., 2021; Almalawi A. et al., 2025; Al Sawafi Y. et al., 2023; Rodríguez E. et al., 2022; Gad A. R. et al., 2021; Khatri N. et al., 2023; Butt N. et al., 2022; Lansky J. et al., 2021). In resource-constrained IoT environments, memory footprint, energy consumption, and inference speed are critical alongside classification quality. Vehicular networks require consideration of node mobility and rapidly changing topology (Gad A. R. et al., 2021; Khatri N. et al., 2023; Bhavsar M. H. et al., 2024; Korium M. S. et al., 2024). In ICS and SCADA, erroneous decisions may have

physical consequences, making latency, stability, and alert explainability particularly important (Balla A. et al., 2023; Almalawi A. et al., 2025; Ortega-Fernandez I. et al., 2024; Rodríguez E. et al., 2022; Mármol Campos E. et al., 2022). Cloud and edge systems require attention to distributed resources, multi-tenancy, and changing data-processing locations (Chang V. et al., 2022; Alsubhi K., 2024; Al S., Dener M., 2021; Sharmila B. S., Nagapadma R., 2023; AL-Nomasy N. et al., 2025; Bhavsar M. H. et al., 2024; Reis M. J. C. S., 2025).

Accordingly, high accuracy or F1 score on a standard dataset is not sufficient evidence of operational suitability. An IDS should be evaluated under conditions that reflect real traffic structure, temporal behavior changes, target-hardware constraints, and the consequences of erroneous decisions.

The literature shows that different IDS classes have distinct sources of uncertainty. Classical models depend on feature stability and sampling strategy. Neural networks are sensitive to label representativeness, class imbalance, and computational constraints. Autoencoders depend critically on anomaly-threshold selection; transformers on sequence construction and meaningful temporal dependencies; and graph models on graph construction and update rules. Transfer and federated learning are complicated by domain differences, heterogeneous local data, and participant trust. Across all machine-learning and deep-learning approaches, adversarial robustness, reproducibility, transferability, and post-deployment degradation remain important concerns.

Thus, IDS/IPS constitute a heterogeneous class of cybersecurity controls that differ in data sources, decision mechanisms, architecture, operational environment, and response mode. Their technical effectiveness cannot be assessed using a single classification metric. Evaluation must account for intended use, interaction with protected infrastructure, acceptable consequences of errors, component security, and the role of IDS/IPS in monitoring and response processes. This systematisation provides a basis for distinguishing European requirements applicable to IDS/IPS as an organizational monitoring control, a product with digital elements, and, where relevant, an AI system.

European regulation of intrusion detection and prevention systems is not confined to a single specialized legal act. IDS/IPS requirements arise at three

interconnected levels: organizational, product, and AI-system level. At the first level, organizations are required to monitor networks and systems, detect anomalous activity, maintain logs, and respond to incidents. At the second, IDS/IPS are treated as products with digital elements, for which secure design, updates, vulnerability management, and conformity assessment are relevant. At the third, properties of AI models are regulated where they are used in high-risk scenarios.

Directive (EU) 2022/2555 (NIS2) requires organizations to implement technical and organizational measures for managing cybersecurity risks in proportion to the threat level and the criticality of their activities. As a directive, NIS2 must be transposed into national law, but it directly defines functions for which IDS/IPS can serve as key technical controls. These include monitoring of networks and information systems, incident handling, business continuity, supply-chain security, secure acquisition, development and maintenance of systems, and vulnerability handling and disclosure.

Commission Implementing Regulation (EU) 2024/2690 further specifies technical and methodological requirements for cybersecurity risk-management measures and significant incidents for certain categories of digital providers. Unlike a directive, the Regulation is directly applicable. It requires monitoring and logging procedures and tools to detect events that may constitute incidents, automation of monitoring to the extent practicable, and continuous monitoring or monitoring at defined intervals. It also explicitly emphasizes minimizing false-positive and false-negative results.

Neither NIS2 nor Implementing Regulation 2024/2690 establishes universal numerical thresholds for accuracy or acceptable false-alarm rates. Compliance must therefore be grounded in risk assessment, asset criticality, organizational operating conditions, and the workload that response processes can reasonably absorb. The regulatory requirement is not the use of a particular model, but the organization's ability to demonstrate that the selected monitoring mechanism is sufficient for timely incident detection and handling.

For the financial sector, IDS/IPS functions are specified in greater detail by Regulation (EU) 2022/2554 (DORA), which is directly applicable in EU Member States. DORA requires financial entities to maintain mechanisms for promptly

detecting anomalous activities, network performance issues, and ICT-related incidents. These mechanisms must support multiple layers of control, define alert thresholds and escalation criteria, automatically notify responsible personnel, and undergo regular testing.

Commission Delegated Regulation (EU) 2024/1774 specifies these requirements at the level of ICT risk-management tools, methods, processes, and policies. Financial entities must log access events, ICT operations, and network activity; protect logs against alteration, deletion, and unauthorized access; and detect failures of logging systems. Detection mechanisms should collect and analyze internal and external factors, threat intelligence, and vendor notifications, automatically generate alerts, prioritize them, and operate both during and outside normal working hours.

These requirements indicate that IDS/IPS can function as components of the broader operational monitoring and incident-response framework of a financial entity. In this context, the effectiveness of detection controls depends not only on detection performance but also on alert manageability, log protection, linkage to response procedures, testability, and recovery capabilities.

Regulation (EU) 2024/2847, the Cyber Resilience Act (CRA), establishes a separate regime for products with digital elements and applies cybersecurity requirements throughout their life cycle. The CRA is directly applicable. The CRA classifies products whose core functionality is that of firewalls or intrusion detection and/or prevention systems as important products with digital elements, Class II. Manufacturers of such products therefore cannot rely solely on internal self-assessment; conformity assessment involving an independent third party is required.

The CRA's essential requirements include security by design and by default, protection against unauthorized access, attack-surface minimization, event logging, secure update mechanisms, coordinated vulnerability disclosure, technical documentation, and provision of security updates for a defined support period (European Parliament and Council of the European Union. Regulation (EU) 2024/2847, 2024). For machine-learning-based IDS/IPS, these requirements may also be relevant to data-preprocessing pipelines, models, feature-generation mechanisms, configurations, and model-update procedures where these elements affect product cybersecurity.

Technical support for CRA implementation is expected from the specialized standard ETSI EN 304 636, “Cybersecurity requirements for firewalls, intrusion detection and/or prevention systems” (Cyber Security (CYBER); CRA, 2026). For consistency, the regulatory and standardisation status in this analysis is assessed as of 5 August 2026. At that date, ETSI EN 304 636 was still a draft standard undergoing approval and harmonisation. Acceptance of the standardisation request by CEN, CENELEC, and ETSI (CEN-CENELEC. Cyber Resilience Act: Standardization request officially accepted by CEN, 2025) does not itself create a presumption of conformity. Such a presumption can arise only after final adoption of the standard and publication of its reference in the Official Journal of the European Union. ETSI EN 304 636 was therefore relevant as an emerging technical specification of CRA requirements, but, at the stated cut-off date, it did not yet provide a harmonised basis for presumption of conformity.

Regulation (EU) 2024/1689 (AI Act) does not automatically classify an IDS/IPS as a high-risk AI system solely because it incorporates machine-learning or deep-learning techniques (European Parliament and Council of the European Union. Regulation (EU) 2024/1689, 2024). Under Article 6, high-risk status depends on the system’s intended purpose and the applicable classification criteria. An AI system may be classified as high-risk where it is used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex I and subject to third-party conformity assessment, or where it falls within one of the use cases specified in Annex III. The latter include certain AI systems intended to be used as safety components in the management and operation of critical digital infrastructure.

For high-risk systems, the AI Act requires an appropriate level of accuracy, robustness, and cybersecurity throughout the life cycle. The system must account for reasonably foreseeable misuse and, where relevant, mitigate training-data and model poisoning, adversarial examples, evasion attacks, exploitation of model flaws, and confidentiality threats (European Parliament and Council of the European Union. Regulation (EU) 2024/1689, 2024). The AI Act therefore focuses primarily on properties of the AI component.

Comparison of the AI Act with NIS2, DORA, and the CRA reveals distinct regulatory planes. NIS2 and DORA govern the organizational environment and

monitoring and response processes; the CRA governs product security across the life cycle; and the AI Act governs AI-model characteristics when the system falls within the high-risk regime. Compliance with the AI Act therefore does not substitute for operational or product-security requirements applicable to IDS/IPS.

Pending completion of specialized harmonisation, a number of general information-security, network-security, incident-management, and industrial cybersecurity standards can provide relevant technical guidance for IDS/IPS development and operation. ISO/IEC 27001 establishes requirements for an information security management system (ISMS), while ISO/IEC 27002 provides guidance on information security controls, including controls related to logging, monitoring, and incident management (ISO/IEC 27001:2022; ISO/IEC 27002:2022). ISO/IEC 27033-1 provides concepts and guidance for network security, including network security requirements, network technical security architectures, and related security controls (ISO/IEC 27033-1:2015), while ISO/IEC 27035-1 defines principles and processes for preparing for, detecting, reporting, assessing, and responding to information security incidents (ISO/IEC 27035-1:2023). For industrial automation and control systems, the IEC 62443 series is particularly relevant: IEC 62443-3-3 specifies system security requirements and security levels, IEC 62443-4-1 addresses secure product development lifecycle requirements, and IEC 62443-4-2 specifies technical security requirements for IACS components (IEC 62443-3-3:2013; IEC 62443-4-1:2018; IEC 62443-4-2:2019). These standards can provide a technical basis for security management, system design, documentation, testing, and lifecycle processes; however, their use should not be equated with the presumption of conformity associated with harmonised European standards under applicable EU legislation.

Despite increasingly detailed regulatory and standardisation requirements, several aspects of quantitative IDS/IPS performance evaluation remain insufficiently standardised. In particular, the reviewed regulatory instruments do not establish:

1) universal numerical thresholds for classification metrics, such as accuracy, recall, F1 score, balanced accuracy, and false-positive and false-negative rates;

2) common quantitative criteria for operational IDS/IPS performance, including detection latency, throughput, alert volume, and operator workload;

3) a common IDS-specific methodology for evaluating model transferability across networks, time periods, device populations, and operational domains;

4) a unified IDS-specific methodology for quantitatively assessing robustness to distribution shift, previously unseen attacks, poisoning, adversarial manipulation, and post-update performance degradation;

5) a unified reproducibility framework for machine-learning-based IDS/IPS covering dataset and model versions, preprocessing procedures, decision thresholds, and evaluation configurations;

6) a common IDS-specific methodology for quantitatively validating alert explainability and auditability, particularly for complex neural, graph-based, transformer-based, and language-model-assisted approaches;

7) a unified methodology for evaluating changes in detection performance following updates to models, signatures, configurations, or software.

The European regulatory system therefore defines the functions and processes that IDS/IPS must support but does not replace scientifically grounded technical model evaluation. An operationally suitable system must simultaneously demonstrate statistical performance, operational manageability, a secure life cycle, reproducible testing, and auditability. Mapping the technical characteristics of specific IDS/IPS classes to regulatory requirements is therefore necessary for constructing a substantiated conformity model.

Systematisation of current intrusion-detection methods shows that operational suitability is determined by more than classification performance. For classical models, the main limitations are instability of selected features and sensitivity to training/test-set construction; for neural networks, label representativeness, class imbalance, and computational cost; for autoencoders, anomaly-threshold selection; for transformers, meaningful sequence structure; for graph models, graph-construction and update rules; and for transfer and federated learning, domain differences, heterogeneous local data, and participant trust. Common requirements across approaches include assessment of transferability, temporal robustness, adversarial resilience, and test reproducibility. High accuracy or F1 score on a single benchmark dataset is therefore insufficient evidence that an IDS is suitable for operation in a particular network or cyber-physical environment.

Analysis of NIS2, Commission Implementing Regulation (EU) 2024/2690, DORA, and Commission Delegated Regulation (EU) 2024/1774 shows that, at the organizational level, IDS/IPS can serve as technical components of continuous monitoring and incident-response processes rather than merely as isolated network-event classifiers. The reviewed European requirements cover logging, anomaly detection, alert thresholds, prioritization, escalation, log protection, and testing of detection mechanisms; Commission Implementing Regulation (EU) 2024/2690 additionally requires monitoring to be implemented in a way that minimises false positives and false negatives. DORA and Commission Delegated Regulation (EU) 2024/1774 provide more detailed requirements for the financial sector than the general NIS2 framework. These acts do not, however, establish universal numerical thresholds for IDS/IPS performance metrics; the adequacy of detection controls must be justified in relation to risk, asset criticality, and acceptable response-process workload.

Distinguishing the regulatory status of IDS/IPS identifies three interconnected levels of requirements: organizational, product, and AI-system. The Cyber Resilience Act classifies standalone firewalls and IDS/IPS as important products with digital elements, Class II, extending control to secure design, updates, documentation, and vulnerability management and requiring third-party conformity assessment. The AI Act imposes additional accuracy, robustness, and cybersecurity requirements only when an IDS/IPS meets the criteria for a high-risk AI system; the mere use of machine learning does not automatically create this status. The draft ETSI EN 304 636 specifies prospective technical requirements for firewalls and IDS/IPS, but as of 5 August 2026 it is not yet a harmonised standard and does not create a presumption of conformity with the CRA.

Mapping technical IDS/IPS limitations to European regulatory requirements shows that formal compliance and real operational effectiveness are related but not identical. The current framework defines monitoring functions, secure life-cycle processes, incident-response processes, and robustness requirements, but does not standardise training-data composition, model architecture, feature and threshold construction, or methods for assessing transferability, temporal degradation, adversarial robustness, and explainability. A practical outcome of this systematisation is a basis for developing a differentiated requirements profile and test programme for

a specific IDS/IPS. Such a programme should combine classification metrics with assessment of latency, resource consumption, alert volume, update security, reproducibility, and auditability, thereby aligning technical verification with intended use, operational environment, and the applicable layer of European regulation.

REFERENCES FOR SUBSECTION 2.2

1. Correia A., Gonçalves A. Regulatory convergence and divergence: A study on the synergies and conflicts among key cybersecurity European legislation. Mediterranean Conference on Information Systems 2024 : proceedings. 2024. Paper 4. URL: https://aisel.aisnet.org/mcis2024/4 (accessed: 07.08.2026).

2. Bolgouras V., Zarras A., Leka C., Stylianou I., Farao A. et al. EU regulatory ecosystem for ethical AI. AI and Ethics. 2025. Vol. 5. P. 5063–5080. DOI: 10.1007/s43681-025-00749-x .

3. Mueck M., Gaie C. (eds.). European Digital Regulations. Springer Cham, 2025. 247 p. DOI: 10.1007/978-3-031-80809-8.

4. Teichmann F. Risk, reasonableness and residual harm under the EU AI Act: A conceptual framework for proportional ex-ante controls. European Journal of Risk Regulation. 2026. Vol. 17, No. 2. P. 611–635. DOI: 10.1017/err.2025.10077.

5. Canavese D., Ferreira A., Kamm L., Quesada Rodriguez A. Uncovering challenges of cybersecurity cross-regulation in EU legislation. Information and Software Technology. 2026. Vol. 193. Art. 108033. DOI: 10.1016/j.infsof.2026.108033.

6. Thankappan M., Rifà-Pous H., Garrigues C. A distributed and cooperative signature-based intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. International Journal of Information Security. 2024. Vol. 23. P. 3527–3546. DOI: 10.1007/s10207-024-00899-9.

7. Chang V., Golightly L., Modesti P., Xu Q. A., Doan L. M. T., Hall K., Boddu S., Kobusińska A. A survey on intrusion detection systems for fog and cloud computing. Future Internet. 2022. Vol. 14, No. 3. Art. 89. DOI: 10.3390/fi14030089.

8. Alsubhi K. A secured intrusion detection system for mobile edge computing. Applied Sciences. 2024. Vol. 14, No. 4. Art. 1432. DOI: 10.3390/app14041432.

9. Ahmad I., Ul Haq Q. E., Imran M., Alassafi M. O., AlGhamdi R. A. An efficient network intrusion detection and classification system. Mathematics. 2022. Vol. 10, No. 3. Art. 530. DOI: 10.3390/math10030530.

10. Alosaimi S., Almutairi S. M. An intrusion detection system using BoT-IoT. Applied Sciences. 2023. Vol. 13, No. 9. Art. 5427. DOI: 10.3390/app13095427.

11. Abu Alghanam O., Almobaideen W., Saadeh M., Adwan O. An improved PIO feature selection algorithm for IoT network intrusion detection system based on ensemble learning. Expert Systems with Applications. 2023. Vol. 213. Art. 118745. DOI: 10.1016/j.eswa.2022.118745.

12. Ali M., Haque M.-ul-, Durad M. H., Usman A., Mohsin S. M., Mujlid H., Maple C. Effective network intrusion detection using stacking-based ensemble approach. International Journal of Information Security. 2023. Vol. 22. P. 1781–1798. DOI: 10.1007/s10207-023-00718-7.

13. Fraihat S., Makhadmeh S., Awad M., Al-Betar M. A., Al-Redhaei A. Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm. Internet of Things. 2023. Vol. 22. Art. 100819. DOI: 10.1016/j.iot.2023.100819.

14. Xu B., Sun L., Mao X., Ding R., Liu C. IoT intrusion detection system based on machine learning. Electronics. 2023. Vol. 12, No. 20. Art. 4289. DOI: 10.3390/electronics12204289.

15. Fatani A., Abd Elaziz M., Dahou A., Al-Qaness M. A. A., Lu S. IoT intrusion detection system using deep learning and enhanced transient search optimization. IEEE Access. 2021. Vol. 9. P. 123448–123464. DOI: 10.1109/ACCESS.2021.3109081.

16. Ahmed U., Jiangbin Z., Almogren A., Khan S., Sadiq M. T., Altameem A., Ur Rehman A. Explainable AI-based innovative hybrid ensemble model for intrusion detection. Journal of Cloud Computing: Advances, Systems and Applications. 2024. Vol. 13. Art. 150. DOI: 10.1186/s13677-024-00712-x.

17. Halbouni A., Gunawan T. S., Habaebi M. H., Halbouni M., Kartiwi M., Ahmad R. CNN-LSTM: Hybrid deep neural network for network intrusion detection system. IEEE Access. 2022. Vol. 10. P. 99837–99849. DOI: 10.1109/ACCESS.2022.3206425.

18. Al S., Dener M. STL-HDL: A new hybrid network intrusion detection system for imbalanced dataset on big data environment. Computers & Security. 2021. Vol. 110. Art. 102435. DOI: 10.1016/j.cose.2021.102435.

19. Balla A., Habaebi M. H., Elsheikh E. A. A., Islam M. R., Suliman F. M. The effect of dataset imbalance on the performance of SCADA intrusion detection systems. Sensors. 2023. Vol. 23, No. 2. Art. 758. DOI: 10.3390/s23020758.

20. Alaghbari K. A., Lim H.-S., Saad M. H. M., Yong Y. S. Deep autoencoder-based integrated model for anomaly detection and efficient feature extraction in IoT networks. IoT. 2023. Vol. 4, No. 3. P. 345–365. DOI: 10.3390/iot4030016.

21. Bakhsh S. A., Khan M. A., Ahmed F., Alshehri M. S., Ali H., Ahmad J. Enhancing IoT network security through deep learning-powered intrusion detection system. Internet of Things. 2023. Vol. 24. Art. 100936. DOI: 10.1016/j.iot.2023.100936.

22. Almalawi A., Hassan S., Fahad A., Iqbal A., Khan A. I. Hybrid cybersecurity for asymmetric threats: Intrusion detection and SCADA system protection innovations. Symmetry. 2025. Vol. 17, No. 4. Art. 616. DOI: 10.3390/sym17040616.

23. Al Sawafi Y., Touzene A., Hedjam R. Hybrid deep learning-based intrusion detection system for RPL IoT networks. Journal of Sensor and Actuator Networks. 2023. Vol. 12, No. 2. Art. 21. DOI: 10.3390/jsan12020021.

24. Ortega-Fernandez I., Sestelo M., Burguillo J. C., Piñón-Blanco C. Network intrusion detection system for DDoS attacks in ICS using deep autoencoders. Wireless Networks. 2024. Vol. 30. P. 5059–5075. DOI: 10.1007/s11276-022-03214-3.

25. Sharmila B. S., Nagapadma R. Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset. Cybersecurity. 2023. Vol. 6. Art. 41. DOI: 10.1186/s42400-023-00178-5.

26. Wu Z., Zhang H., Wang P., Sun Z. RTIDS: A robust transformer-based approach for intrusion detection system. IEEE Access. 2022. Vol. 10. P. 64375–64387. DOI: 10.1109/ACCESS.2022.3182333.

27. Manocchio L. D., Layeghy S., Lo W. W., Kulatilleke G. K., Sarhan M., Portmann M. FlowTransformer: A transformer framework for flow-based network intrusion detection systems. Expert Systems with Applications. 2024. Vol. 241. Art. 122564. DOI: 10.1016/j.eswa.2023.122564 .

28. Jiang X., Xu L., Yu L., Fang X. MFT: A novel memory flow transformer efficient intrusion detection method. Computers & Security. 2025. Vol. 148. Art. 104174. DOI: 10.1016/j.cose.2024.104174.

29. Houssel P. R. B., Singh P., Layeghy S., Portmann M. Towards explainable network intrusion detection using large language models. 2024 IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT). 2024. P. 67–72. DOI: 10.1109/BDCAT63179.2024.00021.

30. AL-Nomasy N., Alamri A., Aljuhani A., Kumar P. Transformer-based knowledge distillation for explainable intrusion detection system. Computers & Security. 2025. Vol. 154. Art. 104417. DOI: 10.1016/j.cose.2025.104417.

31. Lo W. W., Layeghy S., Sarhan M., Gallagher M., Portmann M. E-GraphSAGE: A graph neural network based intrusion detection system for IoT. 2022 IEEE/IFIP Network Operations and Management Symposium (NOMS) : proceedings. 2022. P. 1–9. DOI: 10.1109/NOMS54207.2022.9789878.

32. Caville E., Lo W. W., Layeghy S., Portmann M. Anomal-E: A self-supervised network intrusion detection system based on graph neural networks. Knowledge-Based Systems. 2022. Vol. 258. Art. 110030. DOI: 10.1016/j.knosys.2022.110030.

33. Xu R., Wu G., Wang W., Gao X., He A., Zhang Z. Applying self-supervised learning to network intrusion detection for network flows with graph neural network. Computer Networks. 2024. Vol. 248. Art. 110495. DOI: 10.1016/j.comnet.2024.110495.

34. Zhong M., Lin M., Zhang C., Xu Z. A survey on graph neural networks for intrusion detection systems: Methods, trends and challenges. Computers & Security. 2024. Vol. 141. Art. 103821. DOI: 10.1016/j.cose.2024.103821.

35. Liu J., Guo M. DIGNN-A: Real-time network intrusion detection with integrated neural networks based on dynamic graph. Computers, Materials & Continua. 2025. Vol. 82, No. 1. P. 817–842. DOI: 10.32604/cmc.2024.057660.

36. Rodríguez E., Valls P., Otero B., Costa J. J., Verdú J., Pajuelo M. A., Canal R. Transfer-learning-based intrusion detection framework in IoT networks. Sensors. 2022. Vol. 22, No. 15. Art. 5621. DOI: 10.3390/s22155621.

37. Gad A. R., Nashat A. A., Barkat T. M. Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset. IEEE Access. 2021. Vol. 9. P. 142206–142217. DOI: 10.1109/ACCESS.2021.3120626.

38. Khatri N., Lee S., Nam S. Y. Transfer learning-based intrusion detection system for a Controller Area Network. IEEE Access. 2023. Vol. 11. P. 120963–120982. DOI: 10.1109/ACCESS.2023.3328182.

39. Belenguer A., Navaridas J., Pascual J. A. A review of federated learning in intrusion detection systems for IoT. arXiv. 2022. arXiv:2204.12443. URL: https://arxiv.org/abs/2204.12443 (accessed: 07.08.2026).

40. Mármol Campos E., Fernández Saura P., González-Vidal A., Hernández-Ramos J. L., Bernal Bernabé J., Baldini G., Skarmeta A. Evaluating federated learning for intrusion detection in Internet of Things: Review and challenges. Computer Networks. 2022. Vol. 203. Art. 108661. DOI: 10.1016/j.comnet.2021.108661.

41. Bhavsar M. H., Bekele Y. B., Roy K., Kelly J. C., Limbrick D. FL-IDS: Federated learning-based intrusion detection system using edge devices for transportation IoT. IEEE Access. 2024. Vol. 12. P. 52215–52228. DOI: 10.1109/ACCESS.2024.3386631.

42. Reis M. J. C. S. Edge-FLGuard+: A federated and lightweight anomaly detection framework for securing 5G-enabled IoT in smart homes. Future Internet. 2025. Vol. 17, No. 8. Art. 329. DOI: 10.3390/fi17080329.

43. Thein T. T., Shiraishi Y., Morii M. Personalized federated learning-based intrusion detection system: Poisoning attack and defense. Future Generation Computer Systems. 2024. Vol. 153. P. 182–192. DOI: 10.1016/j.future.2023.10.005.

44. Jmila H., Ibn Khedher M. Adversarial machine learning for network intrusion detection: A comparative study. Computer Networks. 2022. Vol. 214. Art. 109073. DOI: 10.1016/j.comnet.2022.109073.

45. Debicha I., Cochez B., Kenaza T., Debatty T., Dricot J.-M., Mees W. Review on the feasibility of adversarial evasion attacks and defenses for network intrusion detection systems. arXiv. 2023. arXiv:2303.07003. URL: https://arxiv.org/abs/2303.07003 (accessed: 07.08.2026).

46. Papadopoulos P., Thornewill von Essen O., Pitropakis N., Chrysoulas C., Mylonas A., Buchanan W. J. Launching adversarial attacks against network intrusion detection systems for IoT. Journal of Cybersecurity and Privacy. 2021. Vol. 1, No. 2. P. 252–276. DOI: 10.3390/jcp1020014.

47. Mari A.-G., Zinca D., Dobrota V. Development of a machine-learning intrusion detection system and testing of its performance using a generative adversarial network. Sensors. 2023. Vol. 23, No. 3. Art. 1315. DOI: 10.3390/s23031315.

48. Butt N., Shahid A., Qureshi K. N., Haider S., Ibrahim A. O., Binzagr F., Arshad N. Intelligent deep learning for anomaly-based intrusion detection in IoT smart home networks. Mathematics. 2022. Vol. 10, No. 23. Art. 4598. DOI: 10.3390/math10234598.

49. Aljanabi M., Ismail M. A., Hasan R. A., Sulaiman J. Intrusion detection: A review. Mesopotamian Journal of Cybersecurity. 2021. P. 1–4. DOI: 10.58496/MJCS/2021/001.

50. Korium M. S., Saber M., Beattie A., Narayanan A., Sahoo S., Nardelli P. H. J. Intrusion detection system for cyberattacks in the Internet of Vehicles environment. Ad Hoc Networks. 2024. Vol. 153. Art. 103330. DOI: 10.1016/j.adhoc.2023.103330.

51. Sadia H., Farhan S., Ul Haq Y., Sana R., Mahmood T., Bahaj S. A. O., Khan A. R. Intrusion detection system for wireless sensor networks: A machine learning based approach. IEEE Access. 2024. Vol. 12. P. 52565–52582. DOI: 10.1109/ACCESS.2024.3380014.

52. Makris I., Karampasi A., Radoglou-Grammatikis P., Episkopos N., Iturbe E., Rios E., Piperigkos N., Lalos A., Xenakis C., Lagkas T., Argyriou V., Sarigiannidis P. A comprehensive survey of Federated Intrusion Detection Systems: Techniques, challenges and solutions. Computer Science Review. 2025. Vol. 56. Art. 100717. DOI: 10.1016/j.cosrev.2024.100717.

53. Bilot T., El Madhoun N., Al Agha K., Zouaoui A. Graph neural networks for intrusion detection: A survey. IEEE Access. 2023. Vol. 11. P. 49114–49139. DOI: 10.1109/ACCESS.2023.3275789.

54. Sworna Z. T., Mousavi Z., Babar M. A. NLP methods in host-based intrusion detection systems: A systematic review and future directions. Journal of Network and Computer Applications. 2023. Vol. 220. Art. 103761. DOI: 10.1016/j.jnca.2023.103761.

55. Huang J., Chen Y., Wang X., Ouyang Z., Du N. Optimization scheme of collaborative intrusion detection system based on blockchain technology. Electronics. 2025. Vol. 14, No. 2. Art. 261. DOI: 10.3390/electronics14020261.

56. Lansky J., Ali S., Mohammadi M., Majeed M. K., Karim S. H. T., Rashidi S., Hosseinzadeh M., Rahmani A. M. Deep learning-based intrusion detection systems: A systematic review. IEEE Access. 2021. Vol. 9. P. 101574–101599. DOI: 10.1109/ACCESS.2021.3097247.

57. 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 (NIS2 Directive). Official Journal of the European Union. 2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (accessed: 07.08.2026).

58. European Commission. Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and significant incidents. Official Journal of the European Union. 2024. L 2024/2690. URL: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj (accessed: 07.08.2026).

59. European Parliament and Council of the European Union. Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union. 2022. L 333. P. 1–79. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj (accessed: 07.08.2026).

60. European Commission. Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 with regulatory technical standards specifying ICT risk management tools, methods, processes and policies. Official Journal of the European Union. 2024. L 2024/1774. URL: https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj (accessed: 07.08.2026).

61. 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. L 2024/2847. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj (accessed: 07.08.2026).

62. ETSI EN 304 636 V1.0.0 (2026-07). Cyber Security (CYBER); CRA; Cybersecurity requirements for firewalls, intrusion detection and/or prevention systems : draft under approval. ETSI, 2026. URL:

https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=74859 (accessed: 03.08.2026).

63. CEN-CENELEC. Cyber Resilience Act: Standardization request officially accepted by CEN, CENELEC and ETSI. 2025. URL: https://www.cencenelec.eu/news-events/news/2025/newsletter/ots-62-cra/ (accessed: 07.08.2026).

64. European Parliament and Council of the European Union. Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024. L 2024/1689. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (accessed: 07.08.2026).

65. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : ISO, 2022.

66. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. Geneva : ISO, 2022.

67. ISO/IEC 27033-1:2015. Information technology – Security techniques – Network security – Part 1: Overview and concepts. Geneva : ISO, 2015.

68. ISO/IEC 27035-1:2023. Information technology – Information security incident management – Part 1: Principles and process. Geneva : ISO, 2023.

69. IEC 62443-3-3:2013. Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels. Geneva : IEC, 2013.

70. IEC 62443-4-1:2018. Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements. Geneva : IEC, 2018.

71. IEC 62443-4-2:2019. Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components. Geneva : IEC, 2019.

2.3. Strategy for Countering Hybrid Threats in the Digital Sphere: An Analysis of National and European Practices

Alla KAPITON,

National University

"Yuri Kondratyuk Poltava Polytechnic"

Tamara FRANCHUK,

Dmytro TYSHCHENKO,

Alona DESIATKO,

Rostyslav ZAKHAROV,

State University of Trade and Economics

In analyzing the regulatory experience of advanced democracies and the fundamental principles of the European strategy for developing artificial intelligence, contemporary researchers emphasize the need for a strict balance among three basic dimensions: technological and state autonomy in the digital sphere; market competition that drives innovation; and unconditional protection of human rights and freedoms against potential abuses of artificial intelligence (AI). In an era of hybrid confrontation, cybersecurity extends beyond the purely technical protection of computer systems. It has become a multilayered defense against coordinated hostile campaigns. Such aggressive actions combine several destructive elements: technical cyberattacks, information and psychological operations (IPOs), and digital espionage. Whereas technical cyberattacks seek to penetrate networks, block services, and destroy data, IPOs aim to spread disinformation on a large scale to manipulate public consciousness. Digital espionage, conducted to collect confidential data and intelligence, merits separate examination.

The principal objective of these coordinated strikes is not merely to disable individual computers but to achieve a broad geopolitical and social effect. Their primary aims are to paralyze critical infrastructure by disrupting energy systems, transport, the financial sector, and government communications; to destabilize the sociopolitical situation by sowing panic, chaos, distrust of public institutions, and internal conflict; and to steal data on a large scale, gaining access to state secrets, citizens' personal data, and strategic information for subsequent use in exerting pressure on the country.

A number of researchers focus above all on substantiating and developing an integrated model of state information security policy that systematically combines strategic communications, cyber defense measures, and mechanisms for strengthening societal resilience. Other studies seek to develop a comprehensive framework of indicators for verified monitoring and evaluation of the implementation of Ukraine's information strategy. Their many applied findings can directly inform the introduction and modernization of the country's legal framework in the security and digital spheres, optimize strategic communications at national and regional levels, and strengthen the

overall information and cyber resilience of public institutions. Introducing new tools and their modernized applications is now essential to identify, contain, and neutralize hostile disinformation campaigns under martial law.

Several scholars examine the implementation of state policy and its associated challenges, including the approved Strategy for the Digital Development of Innovation until 2030. They focus on building domestic innovation infrastructure as the foundation for modernization at enterprises (Tyshchenko D. et al., 2024; Franchuk T. et al., 2025; Kapiton A. et al., 2024; Bidzilia Yu. M., 2025; Melykh O., Korbut A., 2020). The current situation, systemic gaps, and practical difficulties faced by Ukrainian enterprises are also subjects of research that identifies the specific contribution of infrastructure components to the final outcomes of innovation activity (Kapiton A. et al., 2026; Geraskova O., Stechenko D., 2026). The technical aspects and specifics of protecting the information infrastructure of business entities are examined in joint research on this issue (Shestak Ya. et al., 2025; Pashkovskyi V. F., 2025). At the same time, a substantial body of academic literature shows rapidly growing interest in an integrated study of innovation's role in infrastructure development and sustainable industrial progress through the lens of the security transformation of digital space in leading European countries and elsewhere (Swire P. et al., 2024; Dede G. et al., 2024; Mahmood S. et al., 2024).

Despite the considerable volume of research, a set of theoretical and practical questions concerning information security remains insufficiently addressed. Most scholars consider the following gaps urgent: finding a consensus between the protection of state digital sovereignty and strict observance of fundamental human rights and freedoms; the methodological absence of unified, quantifiable metrics for assessing society's media resilience; and a coordination imbalance caused by the lack of effective cooperation between state institutions and civil society in repelling hybrid attacks. Current institutional and infrastructure deficiencies include uncoordinated interagency cooperation, inadequate methods for forecasting the risks of destructive information influence, and the vulnerability of digital networks under martial law.

Domestic and global processes considerably accelerate these threats: rapid digitization of public administration (e-government) creates new vulnerabilities to cyberattacks; the mediatization of social processes moves public and political life into social networks that are poorly controlled and easily manipulated by algorithms; and, in global information competition, the speed with which a narrative spreads often matters more than its truth. This makes an integrated information policy model necessary, capable of providing three levels of protection at once: technological protection (cybersecurity and infrastructure resilience); institutional protection (effective cooperation among public authorities, intelligence and security services, and civil society); and communicative protection (the state's ability to formulate clear, truthful, and persuasive narratives of its own).

The worldwide integration of information systems and internet resources into every sphere of life has made digital protection a basic and indispensable condition for society. The shift to remote work that accelerated after the pandemic opened new opportunities for sophisticated targeted cyberattacks, forcing private and public organizations to modernize their security perimeters urgently. The constant evolution of threats, evident in mass phishing campaigns and service disruption, causes enormous financial losses for multinational corporations. For Ukraine, meanwhile, the reliability of cyberspace has become a matter of national security: uninterrupted state operations now depend directly on digital integrity, readiness to repel network intrusions, and rapid data exchange between military and civilian agencies. These challenges are complex, manifesting in attacks on civilian and military sectors intended to paralyze government resources and management systems, and in pervasive disinformation spread through coordinated networks of fabricated content that distort reality.

Threats also include targeted IPOs designed to manipulate public sentiment and deliberately inflame domestic divisions, together with attacks on strategic communications intended to discredit Ukraine's official information sources and undermine trust in democratic institutions both domestically and among international partners. Although every industrial sector contributes significantly to favorable macroeconomic trends, solving problems in intellectual capital development, the

commercialization of scientific ideas, and the adoption of innovations based on scientific and technological progress must become a central direction of development. During this difficult period for the country, efforts should stimulate progressive scientific, technical, and technological changes in enterprises. This will directly increase the competitiveness of domestic products, optimize service processes, and improve the culture of consuming the outputs of production. More efficient use of natural resources, stronger state information security, stable national cybersecurity, and modernization of the entire system of strategic mechanisms serving national defense, quality of life, and economic development are also especially important.

In considering the emerging paradigm of digital security, it should be noted that the scientific and theoretical foundations of cyber and information security are undergoing fundamental change. The field is moving beyond a narrow technical or technocratic approach toward integrated, multidimensional models. In these new concepts, decisive determinants of protection are prudent state policy in the digital sphere, national digital sovereignty, and general societal resilience, which enables destructive hybrid influences to be distinguished and blocked effectively.

Cyber resilience as a foundation for technological progress is a separate issue for analysis. In this context, cyber resilience is understood as a basic, indispensable condition for safely deploying and scaling the Internet of Things (IoT) infrastructure that underpins modern smart systems. It also matters to the global goals of sustainable development and technological progress, since the stability of critical digital ecosystems directly affects society's economic, environmental, and social progress.

Another subject of scholarly debate is so-called "digital sovereignty," especially excessive localization of data within national borders, which creates a dilemma between data localization and cybersecurity vulnerability. Experts argue that rigid territorial data-storage requirements often have the opposite effect: they degrade cybersecurity. They artificially slow information exchange among international security institutions, introduce technical delays in urgent access to vital intelligence, and prevent cloud infrastructure from immediately mirroring and backing up data in safe jurisdictions during crises.

In this study, it is important to assess the risk of weakening human rights in global anti-crime agreements. Members of the academic community also express serious concern about trends in the drafting of new global conventions and agreements against cybercrime. There is a real risk that international human rights standards will be substantially lowered to expand the powers of law-enforcement agencies. The authors emphasize that overly vague language on cyber justice could enable authoritarian regimes to legitimize pervasive digital surveillance, censorship, and political persecution under the pretext of fighting crime.

Conceptualizing multidimensional threats in the "gray zone" and bringing these factors together enables researchers to analyze the nature of modern hybrid threats operating in an "invisible zone," below the threshold of open armed conflict (jus ad bellum). These influences are multidimensional because they combine legal pressure, cyberattacks, AI manipulation, and restrictions on access to information. This combination allows an aggressor to pursue strategic geopolitical objectives without directly escalating to conventional war.

The new paradigm of international relations is marked by a fundamental change in the nature of interstate conflict. Classical kinetic clashes and purely conventional methods of warfare increasingly give way to, or become integrated with, complex hybrid confrontations. In this changing structure of global rivalry, virtual and information spaces have become strategic theaters of operations in their own right. The information environment is no longer merely a channel for news but a principal instrument of modern warfare. It is used to gain political influence internationally and within opposing states, reshape public consciousness, alter citizens' values and identity, and undermine sovereignty from within, without necessarily first sending armored columns across a border. Research into the practical and theoretical results of implementing cybersecurity and information-protection tools under hybrid threats is therefore exceptionally relevant.

Ukraine currently faces persistent and growing existential challenges under aggression. Establishing an effective information security system is a matter not merely of national interest but of the state's physical and political survival. At the center of

full-scale armed aggression and daily information and psychological pressure, the country confronts an unprecedented range of threats.

The present configuration of these challenges is complex and includes:

• cyberattacks against civilian and military sectors, intended to paralyze government resources and control systems;

• pervasive disinformation through coordinated networks spreading falsehoods that distort reality;

• targeted IPOs that manipulate public attitudes and deliberately stir up internal contradictions and divisions;

• attacks on strategic communications that seek to discredit Ukraine's official information sources and undermine trust in democratic institutions at home and among international partners.

Outdated reactive methods cannot meet these challenges. They require a proactive, scientifically validated, long-term state strategy and a reconsideration of the security paradigm and new technological factors. Present realities demand moving beyond the narrow understanding of security as border protection alone. Information security is now a foundation of overall national resilience, a key element in protecting statehood, a principal factor in maintaining social cohesion, and an important component of Ukraine's standing as an international actor.

The pronounced disparity in countries' ability to adapt to globalization, caused by striking differences in financial, human, and cultural development, laid the groundwork for current international crises. Together these factors radically altered the structure of domestic economies and prompted national governments to delegate some powers to international organizations. The current interdependence of global systems and the recurring emergence of serious geopolitical, environmental, and financial disruptions make joint, coordinated action by the international community the only viable way to maintain overall balance.

Comprehensive scientific analysis of the strategic foundations of information security is crucial both for current defense and over the long term. Developing and applying new approaches to protecting the information space is a prerequisite for:

• successful postwar recovery, which will require a secure investment and digital environment;

• full Euro-Atlantic and European integration, in which Ukraine can contribute its unique practical experience in countering hybrid threats rather than simply seek assistance;

• building a resilient democratic system able to defend its freedoms and elections against future authoritarian interference from abroad.

A central direction is comprehensive protection of information and production networks by securing their external and internal perimeters and introducing safeguards for specialized services such as email and web access. Security rests on in-depth threat analysis, proactive endpoint protection, secure communication channels, and data loss prevention (DLP) systems. Organizational resilience is also developed through staff training, including cyber ranges for hands-on specialist exercises and cyber hygiene courses for all personnel (Yakovenko Y., 2026).

Implementing innovative projects requires reliable achievement of the intended positive results, which depends directly on a carefully developed long-term strategy. The central concepts should therefore be studied in their systemic interrelationships, using a creative and comprehensive approach to the life cycle of the entire structure, including design, deployment, and continuous operation. Information security has a special place in this architecture. The rapid diversification of ways to protect data against potentially destructive influences is now a priority for preserving the viability of an organization and its scientific, production, information, and technical clusters. Protection extends beyond maintaining network channels: the widespread use of distributed data processing, remote server capacity, and cloud resources demands a model of work in which operations involving confidential corporate information remain inaccessible to outsiders and potential attackers (Yakovenko Y., 2026; Tarasovsky Yu., 2026).

Distributed systems and cloud storage technologies, along with specialized protection systems for cloud information, require continuous, systematic updates. Effective prevention and response depend on an integrated cybersecurity system across

the entire ecosystem of scientific, production, information, and technical clusters. It must give equal attention to personal data and document workflows and to the processing and transmission of that data over communications channels. Regular modernization of specialized software, including antivirus solutions, cryptographic protocols, and SSL certificates, is especially relevant today, as is the use of specialized anonymization tools and anti-detection browsers to protect researchers' and developers' workstations.

Efficient operation of scientific, production, information, and technical clusters at the present stage depends on a comprehensive analysis of the factors shaping their emergence, design, practical operation, and subsequent strategic development. In examining the technical architecture that sustains the ecosystem of such technology sites, scholarly attention increasingly turns to optimizing data-protection systems and strengthening cybersecurity during operation of their digital infrastructure. Many researchers stress the necessity of a protected virtual environment and secure digital transformation as basic conditions for the resilience and integrity of the entire innovation ecosystem.

Understanding digital ecosystems as spaces where productive communities work, promising evidence-based solutions are generated, and entrepreneurial ideas take shape highlights the need for comprehensive security. A protected environment is a basic condition for specialists to work comfortably, channeling their potential into creative activity rather than purely technical troubleshooting, and developing creative ideas, startup projects, and other innovations. Once the technical requirements for uninterrupted digital infrastructure have been met, particular attention should be paid to risks arising from failures to observe digital security standards. Analyzing the most effective cybersecurity models, which ensure information resilience and the safety of data processing in a protected virtual environment, makes it possible to implement effective financial and organizational mechanisms of digital transformation based on prudent regulatory policy across industries.

Today, qualitative growth and effective socioeconomic mechanisms in any developed state are possible only through comprehensive, scientifically grounded

interaction among legal, organizational, economic, social, and other institutional instruments. Maintaining stable digital ecosystems and continuing economic progress are undeniable imperatives, made much more difficult by present geopolitical challenges. These circumstances intensify the need for a sound, balanced model for modernizing the national economy. Such a model calls for fundamental restructuring: a move away from an industrial focus on raw materials toward knowledge-intensive sectors based on intellectual potential, commercialization of new ideas, and greater innovation activity.

Given the specificity and diversity of current challenges and dangers, identifying which tasks require the most immediate action is difficult. Nevertheless, a comprehensive analysis of innovation and digital infrastructure clearly has both theoretical and applied significance, encompassing risk management, digital security, and information resilience. Reliable data protection becomes the central element and a fundamental basis for effective, stable business activity within a unified secure digital environment.

Particular attention should be paid to the difficulties businesses face in the contemporary Ukrainian market and to domestic legislation, which is continually changing and being updated. A deep understanding of citizens' current needs makes it possible to anticipate the demands and expectations of other key participants who support and strategically develop innovation. At the same time, distinguishing and identifying the particular characteristics of domestic digital ecosystems amid current political and economic disruption require focused scientific analysis, especially of the introduction of advanced digital solutions and the positive effects of digitization in general.

Another promising direction is attracting sufficient numbers of potential investors with modest initial capital who wish to become partners, coauthors, or cofounders of innovative companies. Such companies need no large initial investment and can rapidly begin implementing new developments. Modern corporations are directly introducing digitalization programs for workplace safety. Since 2024, several major initiatives have been launched to bring occupational safety to a new level. One

key digital innovation is the SafetyCulture (iAuditor) mobile platform, which enables safety audits, reporting, data analysis, and incident notifications from mobile devices (Digital security transformation, 2026).

The government's approved Strategy for the Digital Development of Innovation in Ukraine (WINWIN) through 2030 provides for comprehensive national financing and stimulation of innovation. This initiative will encompass all essential infrastructure components, with particular emphasis and priority funding for the leading and most promising fields explicitly defined in the strategy (WINWIN, 2026). The industrial and innovation sectors that form the foundation for new developments and the country's strategic progress under WINWIN are illustrated in Figure 2.4.

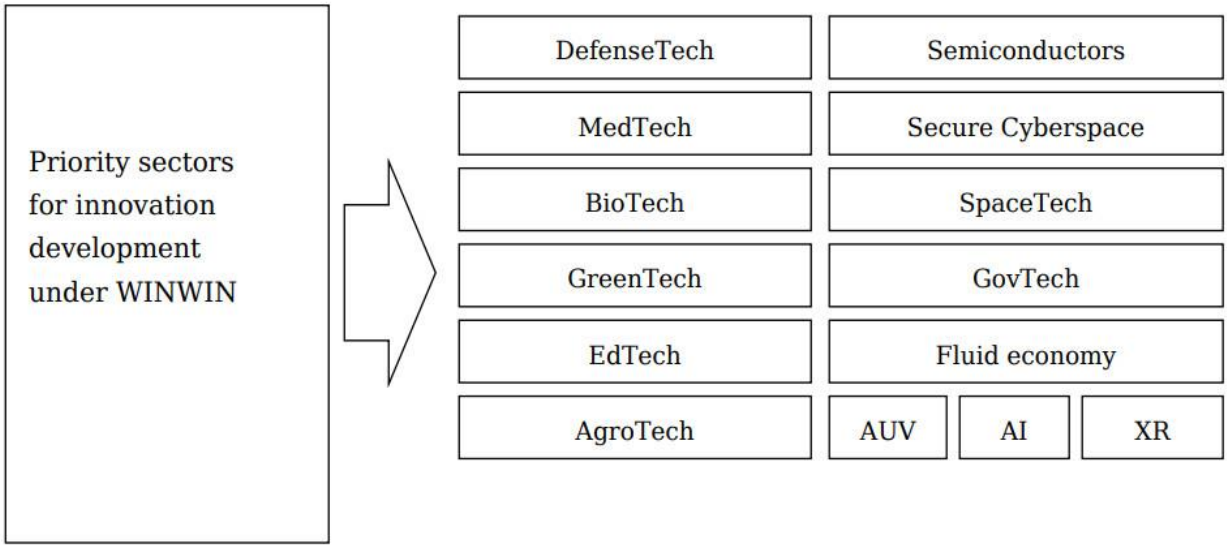


Figure 2.4. Priority sectors for innovation development under WINWIN

Given the way scientific, production, information, and technical clusters operate, particular attention should be paid to building a comprehensive cybersecurity system capable of mitigating threats to digital infrastructure. Because a creative cluster is closely integrated with cloud services, distributed data-processing systems, and Internet of Things (IoT) networks, the perimeter of this ecosystem must be protected at every level of operation.

The main task is to introduce proactive security models based on zero trust architecture. This entails continuous authentication of every user and device, whether they are on the enterprise premises or working remotely through distributed servers.

Particular attention should go to encrypting communication channels with modern cryptographic protocols, using secure VPN tunnels, and integrating data loss prevention (DLP) systems. These steps minimize the risk of unauthorized access to residents' intellectual property and startups' confidential data. The flexible ecosystem of scientific, production, information, and technical clusters also requires regular updates to specialized software, antivirus suites, and intrusion detection and prevention systems (IDS/IPS). Since structural components continually change and their relative importance shifts, security infrastructure must adapt dynamically to newly connected devices or robotics laboratories, which often become potential entry points for cyberattacks. Continuous network traffic monitoring and clear incident response procedures help preserve stable business processes in the digital ecosystem even under targeted hybrid or cyber pressure.

Analysis of digital ecosystems demonstrates the critical importance of data protection and cybersecurity for their digital infrastructure, directly influencing their future development strategies. Recent specialist studies confirm that regulation of information protection is increasingly relevant because technological facilities must remain cyber resilient during ongoing digital transformation. At the same time, funding security measures and assessing economic risks arising from global challenges and threats require strict oversight by both the state and prospective investors. Designing new security-management systems or modernizing existing ones is therefore essential, including improvements to cybersecurity protocols in line with the national strategy for developing the digital environment.

The European Union's information security framework has substantially expanded the powers of ENISA, authorizing it to introduce a common certification scheme for IT products. The agency is now responsible for developing protection standards and ensuring transparency through a public register of issued certificates. The entry into force of the NIS2 Directive marked another stage in digital security development, setting strict requirements for key economic sectors, with specific attention to postal operators and cryptographic data protection. At the same time, the

EU-CyCLONe network supports effective responses to systemic challenges across the EU through reliable notification of detected cyber incidents.

Worldwide dependence on information technology and the internet has made cybersecurity vital to modern society. The rapid expansion of remote work after the pandemic markedly increased the likelihood of sophisticated digital attacks, compelling organizations at every level to strengthen their defenses. The continual escalation of cyber threats, especially waves of phishing and DDoS attacks, inflicts enormous financial losses on global business.

Information security has recently assumed strategic importance for Ukraine. To develop steadily, the state must ensure digital resilience, effectively deter hostile online operations, and coordinate all defense bodies. Ukraine remains a major target for cyber aggressors. Threats range from blocked websites to data encrypted by ransomware, so protection must be comprehensive. Reliable antivirus software, cryptographic encryption, and regular staff training have accordingly become critical security measures in public and private institutions alike.

Expanding the network of modern digital ecosystems is a strategic priority of state policy, within which public infrastructure funding yields new jobs and attracts substantial private investment. Continuously updating a database of promising sites allows investors to evaluate locations in detail, considering logistical potential and fiscal preferences. This comprehensive approach stimulates capital inflows and encourages industrial modernization based on efficient resource use and circular production.

Modern innovation, technology, and industrial parks, along with digital ecosystems, are becoming hubs for leading domestic and international corporations and promising developers. Their physical and technical facilities combine attractive design with stringent building requirements; highly practical spaces are enhanced by advanced energy efficiency technologies and reliable digital protection. The USAID Critical Infrastructure Cybersecurity project provides specialized analytical products and cybersecurity services. Its work seeks to prevent the interception of confidential data, ensure anonymity and privacy during work, and introduce comprehensive

analysis and monitoring systems for detecting unlawful operations (Kapiton A. et al., 2026; Cybersecurity, 2026).

Ukraine is now at the center of a global confrontation in digital space, with one fifth of all cyberattacks worldwide directed against the country. Expert reports show how these threats have become more complex, ranging from attempts to block government resources to large-scale cyber extortion. Basic safeguards are no longer enough; an integrated security ecosystem with advanced encryption and a strong digital security culture among personnel is urgently needed.

An important practical step in public support for innovation was the opening of the Sikorsky Challenge Additive Technologies Science Park, demonstrating the successful transformation of universities into major centers of applied science. Its distinguishing feature is direct integration with the Prosthetics and Rehabilitation Center, creating a unified technology hub for biomedical engineering and comprehensive assistance to veterans. The park supports engineering startups, trains biomedical specialists, and provides inclusive education for former service members. Partnerships with IT market leaders, including appflame, EPAM, Genesis for Ukraine, and OBRIO, enabled a modern 3D-printing laboratory for prosthetics, specialized 3D-modeling courses for veterans, and a fully accessible learning environment to help defenders adapt professionally. These initiatives offer innovative strategies in which advanced technology serves as an effective tool for rehabilitation and education. They support affected people and actively involve them in developing new technological solutions. Such scientific and digital ecosystems should exemplify how effective cooperation among state institutions, business, and society can overcome difficult social challenges (Science park of additive technologies, 2026).

The European Union's present model for protection against complex information threats centers on shared digital resilience and a harmonized legal framework for securing strategically important facilities against planned cyber intrusions. The updated NIS2 Directive occupies a central place: it has greatly expanded the number of regulated sectors and increased penalties for failure to comply with cybersecurity rules. ENISA's broader powers have enabled common standards for certifying software

and equipment throughout the EU, helping identify and block potentially unsafe IT solutions in government and business in advance. To contain major cross-border threats quickly, the EU-CyCLONe network reports digital attacks in real time and coordinates countermeasures among European authorities. This integrated approach reflects a qualitative shift in security architecture, from defending individual local networks to creating a broad secure perimeter capable of resisting cryptanalytic attempts, mass DDoS campaigns, and covert cyber sabotage (Directive on Network and Information Security; Enhanced Cybersecurity Rules in the European Union).

Uneven national readiness for globalization, rooted in deep differences in economic, demographic, and sociocultural capacity, has been a primary cause of current worldwide challenges. The combined effect of these factors profoundly transformed national economies and led governments to delegate some sovereign powers to supranational institutions. In the present circumstances, countries' close interdependence and recurrent large crises in security, the environment, and the economy make coordinated international action indispensable to overall stability.

New global challenges have deeply destabilized the national economy, directly causing impoverishment, a surge in unemployment, and deterioration of the domestic market. These adverse developments have pushed Ukraine out of global competitive markets and rapidly expanded the shadow economy. Such crises cannot be overcome effectively without fundamental modernization of the country's economic capacity. International experience indicates that only developed, financially stable systems can successfully capitalize on globalization while minimizing its associated risks. A crucial protective element is the deployment of real-time monitoring systems that immediately identify and neutralize anomalous network activity.

At the present stage of technological development, specialists are moving en masse to remote work through distributed systems. Virtual collaboration, however, has substantial drawbacks: no single integrated environment for resolving complex tasks and crises quickly; communication gaps; and less effective teamwork owing to the absence of a physical or high-quality virtual hub and fragmented project-management tools. The effort to overcome these problems drives developers to optimize the

workspace. New digital platforms aim not only to bring specialists together but also to create a protected ecosystem that encourages effective solutions. Under these conditions, secure data processing is a fundamental priority, guaranteeing confidentiality, information integrity, and strong resistance by distributed infrastructure to external cyber threats.

Ukraine is at the forefront of confrontation in the information sphere and faces intensive attacks by hacker groups. The wide variety of threats, from destructive DDoS attacks to systems blocked by malicious software, requires multilayered defense. Security in government and commerce therefore calls for advanced antivirus controls, robust information-encryption algorithms, and continuous improvement in employees' digital literacy. Particular attention should be given to challenges arising from force majeure, which require threat-prevention and proactive protection systems to be designed, implemented, and flexibly modified, with an emphasis on the safety of end users and their workstations.

In a globalized digital environment, secure communication channels and effective systems for preventing information leaks are prerequisites for the stable operation and development of diverse institutions. Because cyber threats change continually and demand an ongoing response, researchers should focus more closely on cyber hygiene through practical analysis of active attacks and their mechanisms. Stable operation and progress in high-technology industries require comprehensive improvement of their core components. In practice, this means a fundamental change in current approaches to designing and carrying out research initiatives as a priority of state policy.

The necessary institutional foundation is a favorable legal and regulatory environment with targeted incentives, a lighter tax burden, reduced overall financial pressure, and partial or full public financial support for innovative businesses. At the same time, dynamic infrastructure development requires regular updates and flexible modification of cybersecurity tools, especially within distributed systems, which are highly effective at these technology sites. Minimizing risks to corporate data and ensuring the resilience of information and production networks demand continuous,

multilayered protection of the network perimeter, including monitoring and filtering both external and internal traffic. Developing and integrating new ways to protect specialized services that sustain the complex architectures of modern enterprises is especially relevant. In light of the sharp growth in the number and scale of additional destructive influences during the current crisis, further research and practical work should examine vulnerabilities and strengthen the cybersecurity of the technical components of this innovation infrastructure.

REFERENCES FOR SUBSECTION 2.3

1. Tyshchenko D., Franchuk T., Stepashkina K., Karpunin I. System design and development corporate electronic document management. European Scientific Journal of Economic and Financial Innovations. 2024. No. 1(13), pp. 200-207.

2. Franchuk T., Tyshchenko D., Desiatko A., Karpunin I. Features of accounting digitalization processes. Galician Economic Journal. 2025. Vol. 95, no. 1, pp. 61-66.

3. Tyshchenko D., Franchuk T., Zakharov R., Moskalenko V. Supporting dynamic security needs with VPN tools. Control, Navigation and Communication Systems. 2024. No. 3(77), pp. 149-152.

4. Kapiton A., Franchuk T., Tyshchenko D., Desiatko A., Zakharov R. Requirements for modern processors for secure operation of information systems and networks. Control, Navigation and Communication Systems. 2025. No. 3(77), pp. 111-117.

5. Bidzilia Yu. M. State information security policy under hybrid threats. Ukrainian Political and Legal Discourse. 2025. No. 17, pp. 30-36. URL: https://ppdnz.com.ua/index.php/home/article/view/457/356 (accessed June 20, 2026).

6. Melykh O., Korbut A. Entertainment media in the context of hybrid war in the post-Soviet countries: the case of Ukraine. Economic Annals-XXI. 2020. Vol. 182(3-4), pp. 25-33. URL: http://ea21journal.world/index.php/ea-v182-03/ (accessed June 20, 2026).

7. Kapiton A., Franchuk T., Tyshchenko D., Desiatko A. Integration of cybersecurity into the infrastructure of innovation parks: conceptual and methodological foundations for creating a secure digital environment. Khmelnytskyi Scientific Bulletin. Technical Sciences. 2026. 363(2), pp. 386-390.

8. Kapiton A., Franchuk T. M., Tyshchenko D. O., Desiatko A. M., Zakharov R. G. Formation of cybersecurity architecture of innovation parks in the context of digital transformation and global technical and economic challenges. Tavria Scientific Bulletin. Technical Sciences Series. 2026. Issue 3, pp. 79-85.

9. Geraskova O., Stechenko D. Economic efficiency of functioning of infrastructure for innovative activity in Ukraine. URL: http://www.economy.nayka.com.ua/?op=1&z=3002 (accessed June 20, 2026).

10. Shestak Ya., Zavgorodnya Ye., Krasnoshchok V. Technical protection of the information infrastructure of a commercial enterprise. Development of Education, Science and Business: Results. 2025. URL: http://www.wayscience.com/wp-content/uploads/2025/12/Conference-Proceedings-December-18-19-2025.pdf (accessed June 20, 2026).

11. Pashkovskyi V. F. Identification of political and legal mechanisms of state information security under hybrid warfare. Political Life. 2025. No. 3, pp. 114-120.

12. Swire P., Kennedy-Mayo D., Bagley D., Krasser S., Modak A., Bausewein C. Risks to cybersecurity from data localization, organized by techniques, tactics and procedures. Journal of Cyber Policy. 2024. Vol. 9, no. 1, pp. 20-51.

13. Dede G., Petsa A. M., Kavalaris S., Serrelis E., Evangelatos S., Oikonomidis I., Kamalakis T. Cybersecurity as a contributor toward resilient Internet of Things (IoT) infrastructure and sustainable economic growth. Information. 2024. Vol. 15, no. 12, 798.

14. Mahmood S., Chadhar M., Firmin S. Countermeasure strategies to address cybersecurity challenges amidst major crises in the higher education and research sector: An organisational learning perspective. Information. 2024. Vol. 15, no. 2, 106.

15. Digital security transformation: change that works. URL: https://ohoronapraci.kiev.ua/article/news/cifrova-transformacia-bezpeki-zmini-aki-pracuut (accessed June 20, 2026).

16. WINWIN. Global innovation strategy of Ukraine. URL: https://winwin.gov.ua/ (accessed June 20, 2026).

17. Cybersecurity. URL: https://amintegrator.com/cybersecurity/ (accessed June 20, 2026).

18. Yakovenko Y. The importance of cybersecurity in shaping the digital economy. URL: https://www.researchgate.net/publication/383193213_Znacenna_kiberbezpeki_u_formuvanni_cifrovoi_ekonomiki (accessed June 20, 2026).

19. Tarasovsky Yu. Ukraine has approved the Strategy for the Digital Development of Innovation until 2030. URL: https://forbes.ua/news/ukraina-zatverdila-strategiyu-tsifrovogo-rozvitku-innovatsiy-do-2030-roku-shcho-vona-peredbachae-14012025-26270 (accessed June 20, 2026).

20. Science park of additive technologies. URL: https://www.amsp.com.ua/26270 (accessed June 20, 2026).

21. Directive on Network and Information Security. URL: https://nis2.org.ua/?gad_source=1&gad_campaignid=23017071562&gbraid=0AAABBThWcdWCFXVbeUIPC10mJmbhR0zl&gclid=EAIaIQobChMI1dvk4NDvlAMV_5qDBx1opjDYEAAYASAAEgLBKfD_BwE (accessed June 20, 2026).

22. Enhanced cybersecurity rules in the European Union. URL: https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua (accessed June 20, 2026).

2.4. Protection of Critical Information Infrastructure and Cyber Risk Management: European Practices and Opportunities for Implementation in Ukraine

Olena DVIRNA,

Serhii NABOKA

National University "Yuri Kondratyuk Poltava Polytechnic"

The rapid development of cloud technologies and the widespread adoption of distributed, hybrid, and multi-cloud environments have increased the relevance of efficient computing resource management. Dynamic workload variations, resource heterogeneity, and the need to ensure a specified level of quality of service require the simultaneous consideration of multiple criteria, including execution time, resource usage cost, and energy consumption. Therefore, the resource allocation problem in cloud systems is inherently multi-objective, and the application of evolutionary methods, which enable the generation of a set of Pareto-optimal solutions, represents a promising approach to its solution (Chen J., Du T., Xiao G., 2021; Malti A.N., Hakem M., Benmammar B., 2022).

At the same time, optimization based exclusively on performance and economic efficiency indicators does not fully meet the current requirements for cloud systems. Distributed architectures, containerization, microservices, application programming interfaces, and remote access introduce additional cybersecurity risks. The major threats to cloud environments include identity and access management issues, insecure APIs, misconfigurations, security architecture deficiencies, and software supply chain risks (Cloud Security Alliance, 2022). This necessitates the consideration of the level of cyber risk directly when selecting a cloud resource allocation strategy.

One of the approaches to ensuring the security of modern cloud environments is the Zero Trust concept, according to which access to resources should not be based on implicit trust associated with the network or physical location of a user or resource (Rose S. et al., 2020). In cloud-native and multi-cloud environments, these principles involve the verification of subjects and resources and the application of context-dependent access policies (Chandramouli R., Butcher Z., 2023). Accordingly, trust and security characteristics should be integrated into decision-making procedures for the placement and reallocation of computing resources.

This approach is especially important in the context of the European policy on digital resilience. ENISA pays significant attention to cybersecurity risks related to cloud services and to the development of mechanisms that increase trust in these services (ENISA, 2023). At the same time, EU Directive 2022/2555 (NIS2) extends

cybersecurity risk management requirements to cloud computing service providers and data centre operators (European Parliament and Council of the European Union, 2022). For Ukraine, in the context of European integration, this creates a need to align cloud infrastructure management approaches with European principles of cybersecurity and digital resilience.

Therefore, multi-objective optimization of resource allocation is an important task in which security is considered not only as a set of additional constraints but also as a separate optimization criterion. In general, this problem can be represented by the following vector objective function:

$$F(x) = \left(T(x), C(x), E(x), R(x)\right) \to min, \tag{2.14}$$

where x is a variant of computing resource allocation; $T(x)$ is the task execution time or an overall measure of time efficiency; $C(x)$ is the cost of using cloud resources; $E(x)$ is energy consumption; and $R(x)$ is an overall assessment of cyber risk. This formulation makes it possible to move from searching for one optimal solution to creating a set of compromise solutions. The final solution can be selected depending on the current workload, performance requirements, economic limitations, and the acceptable level of risk.

The aim of the research is to develop an approach to multi-objective resource allocation optimization in cloud computing systems by including cyber risk as an optimization criterion and considering Zero Trust principles and European approaches to digital resilience. To achieve this aim, it is necessary to formalize the system of optimization criteria, define the role of cyber risk in the resource allocation model, study the possibilities of using multi-objective evolutionary methods to find Pareto-optimal solutions, and develop recommendations for applying the proposed approach in accordance with current European requirements for cloud infrastructure security.

The efficiency of cloud computing systems largely depends on how well the available resources are allocated among users' tasks. Virtualization makes it possible to separate physical processor, network, and storage resources from their hardware and

represent them as a set of virtual resources that can be provided according to the current needs of users and applications. As cloud platforms become larger, resource allocation becomes more complex because of the differences between physical nodes, dynamic workloads, different application performance requirements, and the need to meet defined quality-of-service requirements. Therefore, resource allocation and task scheduling are among the main tasks of cloud infrastructure management (Chen J., Du T., Xiao G., 2021; Zhang H., Wu Y., Sun Z., 2022).

In general, a cloud computing infrastructure can be represented as a set of physical nodes $H = \{h_1, h_2, \ldots, h_m\}$,, each of which is characterized by available processing power CPU_i, RAM_i capacity, disk space S_i, network bandwidth B_i, and other parameters. Virtual machines or containers are deployed on these physical nodes and form the logical resource layer $V = \{v_1, v_2, \ldots, v_n\}$.. A set of tasks must then be allocated to these virtual resources $J = \{j_1, j_2, \ldots, j_k\}$.

Thus, the optimization problem is to determine an allocation of tasks to available resources that meets resource and technological constraints and, at the same time, provides the best values of the defined criteria. Even the problem of scheduling a set of tasks on heterogeneous resources is generally a complex combinatorial problem. This significantly limits the use of exact methods when the size of the system increases (Malti A.N., Hakem M., Benmammar B., 2022).

It is important to distinguish between the optimization of virtual machine or container placement and task scheduling. In the first case, the goal is to determine which physical nodes should host the virtualized resources, taking into account their CPU, RAM, storage, and network requirements. In the second case, computational tasks are assigned to the available virtual resources.

In practice, these processes are closely connected. Inefficient placement of VMs or containers can lead to an uneven workload of physical servers, while inefficient task scheduling can increase execution time and energy consumption and may cause violations of SLA requirements. For this reason, modern models increasingly consider resource allocation and task scheduling as interconnected levels of a single optimization problem.

The main criteria for cloud resource optimization are execution time, cost, energy consumption, and latency. Let these criteria be denoted as $T(x)$, $C(x)$, $E(x)$ and $L(x)$, where x represents a specific resource allocation solution. The criterion $T(x)$ may represent the total task execution time or the makespan, which is the time when the last task is completed: $T(x) = \max\limits_{j \in J} t_j^{finish}$.

Minimizing $T(x)$ improves the overall performance of the system. However, it does not guarantee minimum cost or balanced resource utilization. Studies of modern scheduling algorithms confirm that makespan remains one of the main criteria for evaluating the efficiency of task allocation in cloud environments (Malti A.N., Hakem M., Benmammar B., 2022; Mangalampalli S., Karri G.R., Kose U., 2023).

The cost criterion $C(x)$ represents the cost of using computing resources. In a simplified form, it can be defined as $C(x) = \sum\limits_{i=1}^{n} p_i t_i$, where p_i is the cost per unit of time for using the i-th resource, and t_i is the duration of its use. For public and multi-cloud platforms, this criterion is especially important because providers offer different prices, virtual machine types, and payment models. Cost minimization may require the use of less powerful resources, which can increase task execution time. Therefore, there is a natural conflict between the $T(x)$ and $C(x)$ criteria.

The energy consumption criterion $E(x)$ represents the amount of energy required to operate the computing resources involved. Its value depends on the number of active physical servers, their utilization level, task execution time, and power management mechanisms. In modern research, energy efficiency is considered not only as a way to reduce the operating costs of data centres but also as a separate measure of scheduling algorithm efficiency. In particular, the EHEFT-R algorithm focuses on task execution efficiency, QoS, and energy consumption at the same time (Zhang H., Wu Y., Sun Z., 2022).

The criterion $L(x)$ represents the delay in data processing or transmission. This criterion is especially important for interactive services, real-time systems, and distributed applications, where the physical location of resources and the current

network conditions directly affect the quality of service. Therefore, the general optimization problem can be represented as

$$minF(x) = (T(x), C(x), E(x), L(x)), \tag{2.15}$$

subject to a set of constraints on the available processing, memory, network, and other resources.

Depending on the type of input parameters, cloud resource optimization models can be divided into static and dynamic models. A static model assumes that the sets of tasks and resources, as well as their main characteristics, are known before the optimization process starts and do not change significantly during the considered time period. Under these conditions, the optimization algorithm can create a complete resource allocation plan before the tasks are executed. The advantage of this approach is the possibility of performing a more detailed global search. However, its efficiency decreases when the workload changes rapidly.

In dynamic models, user requests arrive at different times, while the availability and characteristics of resources may change during system operation. Therefore, resource allocation should be adjusted according to the current state of the cloud infrastructure. Dynamic behaviour is one of the main characteristics of real cloud environments: heterogeneous tasks come from different sources, while their number, size, and computing requirements change over time (Mangalampalli S., Karri G.R., Kose U., 2023). This creates a need for adaptive algorithms that can perform repeated optimization or quickly adjust an existing solution.

Exact, heuristic, metaheuristic, and evolutionary methods are used to solve resource allocation problems. Exact mathematical programming methods can provide an optimal solution when the model is correctly defined and the problem size is acceptable. However, the combinatorial growth of the solution space makes these methods difficult to use in large cloud systems. For this reason, algorithms that do not guarantee a mathematically exact global optimum but can provide high-quality solutions within an acceptable time are of significant practical interest.

Heuristic methods use rules developed according to the structure of a specific problem. These methods include algorithms that select the most or least loaded resource, priority-based task allocation rules, and different list-scheduling approaches. Their main advantages are simple implementation and relatively low computational costs. For example, algorithms from the HEFT family use task ranking and estimated completion times to select suitable resources. In EHEFT-R, additional priority rules are used to improve the initial solution, while a modified HEFT mechanism is applied to find a more efficient schedule (Zhang H., Wu Y., Sun Z., 2022).

A disadvantage of heuristic methods is their strong dependence on the specific features of the problem. A rule that is effective for one type of workload may produce worse results when the task structure or resource characteristics change. In addition, the local focus of many heuristic methods limits their ability to explore a large space of alternative resource allocation solutions.

Metaheuristic methods are more universal because they define a general search strategy and can be adapted to different optimization problems. In cloud computing, genetic algorithms (GA), Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Whale Optimization Algorithm (WOA), Flower Pollination Algorithm (FPA), and other population-based and nature-inspired approaches are used. For example, a method based on flower pollination behaviour has been proposed for multi-objective task scheduling. In this method, the Pareto principle is combined with the TOPSIS method. Makespan, execution cost, and task allocation reliability are considered as optimization criteria (Malti A.N., Hakem M., Benmammar B., 2022).

Evolutionary algorithms have a special place among metaheuristic approaches. They work with a population of possible solutions instead of a single solution and use selection, crossover, and mutation mechanisms. This makes it possible to explore different areas of the solution space and reduces the dependence of the final result on a single initial point. This feature is especially important for cloud optimization problems because task and resource allocation has a discrete and combinatorial nature.

The use of evolutionary methods is especially promising for multi-objective optimization. The traditional approach is to combine several criteria into a single scalar objective function

$$F(x) = w_1 T(x) + w_2 C(x) + w_3 E(x) + w_4 L(x), \quad (2.16)$$

where $w_1, \ldots, w_4$ are weighting coefficients. However, the choice of weights is subjective, and changes in user priorities or the system state require the weights to be defined again. In addition, combining several criteria into one value may hide information about possible trade-offs.

An alternative approach is to use the principle of Pareto optimality. A solution x_1 dominates a solution x_2, if it is not worse than x_2 for all criteria and is better for at least one criterion. The set of non-dominated solutions forms the Pareto front, where each point represents a specific trade-off between the criteria. This approach does not require a single set of weights to be defined in advance. Instead, it provides a set of alternative solutions that can be selected according to the current system requirements. In particular, Chen, Du, and Xiao proposed a multi-objective cloud resource allocation model and the modified RAA-PI-NSGAII algorithm. This algorithm is designed to improve the quality and distribution of the obtained solutions and to speed up the search process (Chen J., Du T., Xiao G., 2021).

The potential of the multi-objective approach is also confirmed by the fact that reliability and trust characteristics are gradually being added to traditional optimization criteria. For example, in the model proposed by Malti, Hakem, and Benmammar, task-to-resource mapping reliability is optimized together with makespan and cost (Malti A.N., Hakem M., Benmammar B., 2022). In the study by Mangalampalli, Karri, and Kose, the multi-objective scheduler considers task and VM priorities as well as trust indicators. These indicators are defined through the availability of virtual resources, successful task execution, and task processing time efficiency. The proposed approach also aims to reduce makespan and energy consumption (Mangalampalli S., Karri G.R., Kose U., 2023).

A general comparison of the main approaches is presented in Table 2.4.

Table 2.4

Comparative Characteristics of Approaches to Cloud Resource Optimization

Approach	**Advantages**	**Limitations**	**Suitability for Dynamic Cloud Systems**
Exact methods	Ability to obtain an optimal solution	High computational complexity as the problem size increases	Low/Medium
Heuristic methods	Fast operation, simple implementation	Dependence on specific rules and problem structure	Medium/High
Metaheuristic methods	More global search, ability to work with complex nonlinear models	Dependence on parameters, no guarantee of finding the global optimum	High
Evolutionary methods	Ability to work with discrete solutions and explore a large space of alternatives	High computational cost	High
Multi-objective evolutionary methods	Formation of the Pareto front, simultaneous consideration of conflicting criteria	Difficulty in selecting the final solution and increased computational cost	High

Source: compiled by the authors based on (Chen J., Du T., Xiao G., 2021; Malti A.N., Hakem M., Benmammar B., 2022; Zhang H., Wu Y., Sun Z., 2022; Mangalampalli S., Karri G.R., Kose U., 2023).

The comparison shows that multi-objective metaheuristic and evolutionary approaches are the most promising for scalable cloud systems with heterogeneous

resources and dynamic workloads. These approaches make it possible to consider conflicting criteria and create a set of alternative resource allocation solutions without the need to define a single trade-off in advance. At the same time, recent studies show a gradual expansion of optimization criteria: together with execution time, cost, and energy consumption, reliability, availability, and trust are also considered.

However, even these models are mainly focused on performance and quality of service. A trust indicator based on availability, success rate, or SLA is not the same as a cyber risk assessment. Cyber risk should also consider the probability of threats, vulnerability characteristics, access context, and the potential impact of a security incident. Therefore, the next stage in the development of cloud resource optimization models is to include security directly in the system of decision-making criteria. This creates the need to study cyber risk as a separate factor in cloud infrastructure optimization and to define the corresponding criterion $R(x)$, which is the subject of the next section.

The spread of cloud technologies is accompanied not only by increased computing capabilities but also by a larger attack surface. Resource virtualization, shared use of physical infrastructure by different users, containers and microservices, application programming interfaces (APIs), remote access, and automated orchestration tools create additional sources of cyber risk. Therefore, the efficiency of a specific cloud system configuration cannot be evaluated only by execution time, cost, energy consumption, and latency. Decisions about the placement of computing tasks and services directly affect their level of security.

The most significant threats to cloud systems include weak identity and access management mechanisms, configuration errors, insecure APIs, weaknesses in security architecture, software supply chain risks, data leakage or loss, and attacks aimed at disrupting service availability (Cloud Security Alliance, 2022; ENISA, 2024). A specific feature of cloud environments is the interdependence of their components. A threat affecting one node, account, or service may also affect other components of the system. Therefore, the level of security depends not only on the characteristics of individual resources but also on how they interact and on the configuration of the infrastructure as a whole.

Another important characteristic is the dynamic nature of cyber risk. The state of cloud infrastructure changes over time because of scaling, migration of virtual machines and containers, the arrival of new tasks, changes in network routes, access policies, and workloads. At the same time, external conditions may also change: new vulnerabilities may appear, the intensity of attacks may increase or decrease, and the level of trust in specific components may change. ENISA reports consider threat assessment and resilience as parts of a continuous cybersecurity management process, which is especially important for digital infrastructure and cloud services (ENISA, 2023; ENISA, 2024).

For a formal description of these factors, it is useful to apply the concept of cyber risk as a characteristic that combines the probability of a specific threat and the possible consequences of the related incident. For a specific threat q a simplified risk assessment can be represented as $r_q = p_q \cdot I_q$, where p_q is the estimated probability of the q-th threat, and I_q is the estimated potential impact of this threat on the system. In a cloud environment, these parameters may depend on the resource configuration. Therefore, it is reasonable to write $r_q(x) = p_q(x) \cdot I_q(x)$, where x represents a specific task and resource allocation solution. This representation makes cyber risk different from a fixed external parameter: a change in \(x\) can affect not only system performance but also its level of security.

For example, two allocation options for the same task may have similar execution time and cost but may differ significantly in their level of risk. Placing a critical service on a node with a less secure access configuration, insufficient segmentation, or higher exposure to an external network may be more cost-effective but may also create a higher cyber risk. Similarly, placing several critical services on one physical node may reduce energy consumption through resource consolidation, but at the same time increase the possible consequences if this node is compromised. Therefore, conflicts may arise between economic efficiency, energy efficiency, and security, which is typical of multi-objective optimization problems.

Considering these relationships is the basis of the **security-aware resource allocation** approach, in which security parameters are directly integrated into the

resource scheduling and allocation process. Unlike the traditional approach, where a configuration is first optimized for performance and security mechanisms are applied afterwards, the security-aware approach evaluates security during the process of creating the solution. Research on security-aware scheduling in heterogeneous hybrid clouds shows that security requirements can be included in the resource selection process together with time constraints (*Security-aware task scheduling with deadline constraints on heterogeneous hybrid clouds*, 2021). A similar trend can be found in trust-aware models, where resource trust characteristics are considered during multi-objective task scheduling (Mangalampalli S., Karri G.R., Kose U., 2023).

For a set of threats $Q=\{q_1,q_2,\ldots,q_s\}$ the overall risk of a specific resource allocation solution can be defined as $R(x)=\sum_{q=1}^{s} w_q p_q(x) I_q(x),$ where w_q is the importance coefficient of the corresponding threat. The weighting coefficients can be defined according to the type of data, the criticality of the service, SLA requirements, or the category of the information resource. This model makes it possible to compare alternative cloud infrastructure configurations quantitatively according to their potential level of cyber risk.

At the same time, in a dynamic cloud environment, it is important to consider changes in threat intensity over time. For this purpose, a function $\lambda q(t)$ can be introduced to represent the intensity or relevance of the q -th threat at time t. Then, the risk assessment over the time interval [0, T] can be represented as

$$R(x,T)=\sum_{q=1}^{s} w_q \int_0^T \lambda_q(t)\, p_q(x,t)\, I_q(x,t)\, dt\,.$$

This representation makes it possible to consider not only the static characteristics of resources but also the current state of the cloud system and changes in the security situation. As a result, a resource allocation solution that is acceptable at time t_1 may no longer be optimal at time t_2 , This creates the need for adaptive resource reallocation.

Therefore, cyber risk should be considered as a separate optimization criterion rather than only as a constraint on solution feasibility. If the security requirement is defined only as $R(x) \le R_{max}$, all solutions that meet the defined threshold are considered equal from the security point of view. However, including $R(x)$ in the vector of optimization criteria makes it possible to evaluate the trade-off between risk reduction and other system characteristics. Therefore, the basic multi-objective resource allocation model (2.15) should be extended to a security-aware formulation

$$minF(x) = \left(T(x), C(x), E(x), L(x), R(x)\right) \tag{2.17}$$

subject to the established system of resource, technological, and security constraints.

The proposed extension makes it possible to create Pareto-optimal configurations that represent different trade-offs between performance, cost, energy efficiency, latency, and security. At the same time, minimizing $R(x)$ does not mean that the most secure but potentially very expensive solution should always be selected. The task is to determine a resource allocation solution in which the level of cyber risk is balanced with other requirements of the cloud system. Further formalization of this approach requires the identification of factors that influence $R(x)$, including identity management, access control, segmentation, and continuous trust verification. In modern cloud-native environments, these mechanisms are directly related to the Zero Trust concept. The integration of Zero Trust into cloud resource management is discussed below.

Traditional information security models are mainly based on the concept of a protected network perimeter. Resources and users located inside a corporate network usually receive a higher level of trust than external users and systems. However, this model is not sufficient for modern cloud systems because the boundaries of corporate infrastructure are becoming less clear. Computing resources can be located in both private and public clouds, applications can operate as a set of microservices, and users and administrators can access them from different networks and devices. Under these

conditions, being located within a specific network segment cannot be considered a sufficient reason for trust.

An alternative to the perimeter-based approach is the Zero Trust concept. According to this concept, trust should not be automatically given to a user or resource only because of its physical or network location. Zero Trust Architecture requires the verification of the user and device before establishing an access session to a corporate resource. Authentication and authorization are considered separate functions that must be performed before access is granted (Rose S. et al., 2020). Thus, the basic principle of Zero Trust can be summarized as “never trust automatically, always verify.”

One of the main components of Zero Trust is identity-based access control, which means that access decisions are made based on the verified identity of the subject. In a cloud environment, identity becomes one of the key elements of security because a user, service, or software component can interact with resources regardless of their physical location. Access decisions should consider not only user credentials but also the context of the request, including device characteristics, resource type, level of criticality, current security status, and other parameters. For cloud-native applications, NIST considers the implementation of Zero Trust using identity-tier and network-tier policies, which makes it possible to apply granular access policies in multi-cloud environments (Chandramouli R., Butcher Z., 2023).

The second principle is least privilege, according to which a user, service, or process receives only the minimum set of permissions required to perform its functions. From the point of view of cloud infrastructure management, this principle is important not only for user accounts. It also applies to interactions between virtual machines, containers, microservices, and application programming interfaces. Limiting unnecessary privileges reduces the possibility of lateral movement by an attacker if one component is compromised and, therefore, reduces the potential impact of a security incident.

An important mechanism for implementing Zero Trust is microsegmentation, in which the infrastructure is divided into logically isolated segments and communication between them is controlled according to defined policies. In a cloud system, this makes it possible to isolate individual VMs, containers, applications, or groups of resources

even when they are located on shared physical infrastructure. In cloud-native environments, such policies can be supported by service mesh technologies, which provide control over communication between microservices and support attribute-based access control (Chandramouli R., Butcher Z., Chetal A., 2021). Microsegmentation reduces the potential area of attack spread and helps to limit the consequences of a compromised component.

Another important principle is continuous verification, which means continuous checking of the conditions under which access was granted. In a dynamic cloud system, successful authentication at one moment does not guarantee that the level of risk will remain the same during the whole session. Changes in the state of a device, location or type of access, user behaviour, threat level, or resource configuration may require additional verification or changes to the access policy. Therefore, Zero Trust represents a transition from static control to continuous assessment of the interaction context.

These principles are especially important for cloud-native and multi-cloud environments. An application can be distributed across several cloud platforms, while its individual components can be dynamically created, scaled, moved, or removed. NIST SP 800-207A directly adapts the Zero Trust model to cloud-native applications in multi-cloud environments and considers granular resource access policies regardless of network location (Chandramouli R., Butcher Z., 2023). In such an architecture, security control should be connected not so much with a fixed IP address or physical server but with the identity and characteristics of the resource itself.

In the study by H. V. Holovko, O. A. Dvirna, and S. V. Naboka, Zero Trust is considered from the perspective of its practical implementation under the limited resources of small and medium-sized businesses. The authors emphasize the need to adapt the model to the real capabilities of companies that may have limited budgets, a small number of IT specialists, and outdated infrastructure. The proposed approach is not based on simplifying the Zero Trust concept itself but on its step-by-step implementation according to the available resources of the organization (Holovko H.V., Dvirna O.A., Naboka S.V., 2026). This idea is also important for cloud resource optimization: the level of security cannot be considered separately from the financial and computing resources required to provide it.

From the optimization perspective, it is especially important that the implementation of Zero Trust can change the characteristics of a specific cloud system configuration. Additional authentication, policy verification, encryption of communication between services, monitoring, and the use of service mesh components require additional computing and network resources. Microsegmentation, in turn, may introduce restrictions on possible placement options for interconnected services. Therefore, a higher level of security may require additional costs and may also affect execution time and latency.

On the other hand, the choice of a resource allocation solution affects the possibility of implementing Zero Trust principles. Let each resource v_i have a set of security characteristics $Z_i = \{I_i, P_i, M_i, V_i\}$, where I_i is the level of identity and authentication support; P_i is the level of implementation of the least privilege principle; M_i is the microsegmentation characteristic; and V_i is the ability to provide continuous verification and access control. Therefore, placing the same task on resources v_i and v_j may result in different levels of cyber risk even if these resources have the same CPU, RAM, and other computing characteristics.

This relationship should be included in the risk function introduced in the previous section:

$$R(x) = R(x, Z(x), Q(t)), \tag{2.18}$$

where x is a resource allocation solution; $Z(x)$ is the set of Zero Trust characteristics of the resources used in configuration x; $Q(t)$ represents the current threat state. In this case, changing the placement of a task may change $R(x)$, even if the functional characteristics of the task remain unchanged.

For example, let task j_k be executed on one of two resources v_1 and v_2. The first resource provides lower cost and shorter execution time but has a lower level of segmentation and access control. The second resource requires higher costs but provides MFA, granular access control, microsegmentation, and continuous

monitoring. Therefore, if only the $T(x)$ and $C(x)$ criteria are considered, selecting v_1 may be optimal:

$$T(v_1) < T(v_2), C(v_1) < C(v_2), \tag{2.19}$$

However, after including the security criterion, the following relationship may be observed:

$$R(v_1) > R(v_2). \tag{2.20}$$

Therefore, there is no single "best" resource. Instead, a trade-off appears between performance, economic efficiency, and cyber risk.

Considering this, Zero Trust principles should be integrated not only into the security architecture but also directly into the decision-making process for cloud resource allocation. For critical tasks, the algorithm can exclude resources that do not meet the minimum requirements for identity verification, privilege management, or segmentation. For other tasks, the level of Zero Trust implementation can affect the value of $R(x)$, and, therefore, the position of the corresponding solution on the Pareto front. As a result, security-aware optimization combines two mechanisms: strict security constraints for unacceptable configurations and minimization of residual cyber risk for the set of feasible solutions.

Thus, Zero Trust provides a conceptual basis for moving from traditional cloud resource optimization to a risk-oriented management model, where security is considered a property of a specific resource configuration. Identity-based access control, least privilege, microsegmentation, and continuous verification can be formalized as parameters that affect the value of $R(x)$, while the implementation of these mechanisms requires additional resources. This explains the need to find trade-off solutions between $T(x)$, $C(x)$, $E(x)$, $L(x)$ and $R(x)$. Such a formulation provides a basis for further mathematical formalization of the multi-objective cloud resource allocation problem, taking into account cyber risk and Zero Trust principles.

The development of cloud computing in the European Union is accompanied by the formation of a comprehensive approach to cybersecurity, where technical security mechanisms are combined with risk management, certification, regulatory requirements, and digital resilience. A special role in this process belongs to the European Union Agency for Cybersecurity (ENISA), whose activities are aimed at improving the common level of cybersecurity across the EU. For cloud technologies, this approach is especially important because a disruption in the operation of one provider may affect a large number of organizations, information systems, and digital services at the same time.

In the Cloud Cybersecurity Market Analysis, ENISA considers cloud cybersecurity as an important separate segment of the European cybersecurity market. Among the main problems of cloud environments, special attention is given to misconfigurations, insecure APIs, and the lack of qualified specialists. Secure cloud architectures, edge computing, and fog computing are identified as promising areas for future development (ENISA, 2023). This confirms that security should not be considered only as an additional element of cloud infrastructure, but as one of the main factors in its design, configuration, and optimization.

The importance of a risk-oriented approach is increasing because of changes in the nature of cyber threats. According to the ENISA Threat Landscape 2024, the main threats include attacks against availability, ransomware, threats against data, malware, social engineering, and supply chain attacks. Attacks against availability were among the leading categories of the threats analysed (ENISA, 2024). This is directly relevant to cloud systems because availability is both an indicator of service quality and an important part of security. Therefore, resource allocation decisions should consider not only the performance of individual nodes but also the possible consequences of their unavailability or compromise.

An important part of the European approach is the development of cybersecurity certification mechanisms for cloud services. ENISA developed the candidate European Cybersecurity Certification Scheme for Cloud Services (EUCS) within the European cybersecurity certification framework. EUCS is aimed at assessing the cybersecurity of cloud services and developing a common approach to confirming their level of

security (ENISA, 2020). In the context of this research, it is important that the certification approach creates a basis for formalizing the security characteristics of cloud resources, which can be used when evaluating alternative resource allocation configurations.

The Directive (EU) 2022/2555 (NIS2) has a significant regulatory impact on cyber risk management in the EU. Its provisions directly cover cloud computing service providers and data centre service providers. NIS2 is based on the need for a high level of harmonization of requirements for these organizations because of the cross-border nature of their activities (European Parliament and Council of the European Union, 2022).

Importantly, NIS2 focuses not on the implementation of separate and isolated security measures but on systematic cyber risk management. These measures should include incident prevention, business continuity, crisis management, supply chain security, security in the acquisition, development, and maintenance of network and information systems, assessment of the effectiveness of cybersecurity measures, access management, and other areas. Special attention is also given to risks related to suppliers and third-party services (European Parliament and Council of the European Union, 2022).

For cloud infrastructure optimization, this means that security parameters may be related not only to a specific physical or virtual resource but also to the provider, the supply chain, and the service deployment model. For example, two resources with the same CPU, RAM, cost, and performance characteristics may differ in the provider's level of security, implemented access control mechanisms, fault tolerance, backup capabilities, and characteristics of related suppliers. Therefore, when defining the cyber risk function \(R(x)\), it is reasonable to consider not only the technical characteristics of a specific resource but also the characteristics of the environment in which it operates.

In general, for the i-th cloud resource, a vector of security parameters can be defined as

$$S_i = \left(s_i^{id}, s_i^{acc}, s_i^{seg}, s_i^{mon}, s_i^{res}, s_i^{sup} \right), \tag{2.21}$$

where s_i^{id} represents identity and authentication mechanisms; s_i^{acc} represents access management; s_i^{seg} is the level of segmentation; s_i^{mon} represents monitoring capabilities; s_i^{res} describes the resilience and recovery capabilities of the resource; and s_i^{sup} represents risks related to the provider and the supply chain. The overall risk of a configuration can then be defined as a function of not only the resource allocation x, but also the characteristics of the resources involved:

$$R(x) = R\left(x, S_1, S_2, \ldots, S_n, Q(t)\right), \tag{2.22}$$

where $Q(t)$ represents the current state of cyber threats at time t.

This approach is directly related to the concept of digital resilience. For a cloud system, resilience does not mean the complete elimination of all threats, which is practically impossible. Instead, it means the ability to maintain critical functions, adapt to negative events, and recover after an incident. Therefore, resource allocation optimization can focus not only on reducing the probability of an incident but also on limiting its possible consequences. Resource redundancy, distribution of critical components across independent nodes, avoidance of a single point of failure, and the ability to quickly migrate workloads may increase cost or energy consumption, but at the same time they can improve the resilience of the system.

For Ukraine, the implementation of European approaches to cloud cybersecurity should be considered not only as a matter of regulatory alignment but also as a basis for developing practical methods of digital infrastructure management. A promising direction is the use of the NIS2 risk-oriented model, ENISA approaches to threat analysis and cloud cybersecurity, and the principles included in the candidate EUCS scheme to define requirements for national cloud platforms, government information systems, enterprises, and critical infrastructure. At the same time, it is especially important to move from static compliance checks to continuous risk assessment and adaptive resource management.

Thus, the European approach demonstrates a transition from considering cybersecurity as a set of separate technical measures to a comprehensive model of risk management and digital resilience. For the problem of multi-objective cloud resource optimization, this provides a basis for including NIS2 requirements, ENISA recommendations, Zero Trust characteristics, and cloud service security parameters in the formation of the $R(x)$ criterion. As a result, a configuration can be selected not only according to performance, cost, energy consumption, and latency, but also by considering the ability of the system to resist cyber threats and maintain its functionality during security incidents. This integration of European cyber risk management principles with mathematical optimization methods provides the basis for the formalization of the multi-objective cloud resource allocation model in the next section.

Effective cloud infrastructure management requires the formalization of the process of allocating computing tasks among available resources while considering performance, cost, energy consumption, and security at the same time. Unlike traditional models, where security characteristics are mainly defined as additional constraints, the proposed formulation considers cyber risk as an independent optimization criterion. This makes it possible to consider possible trade-offs between task execution speed, economic efficiency, energy consumption, and the security level of a specific cloud system configuration.

Let a set of computing tasks be given as

$$J = \{j_1, j_2, \ldots, j_n\}, \tag{2.23}$$

and let the set of available cloud resources be

$$V = \{v_1, v_2, \ldots, v_m\}. \tag{2.24}$$

Each task j_i is characterized by a set of computing resource requirements:

$$d_i = (cpu_i, ram_i, bw_i, s_i), \tag{2.25}$$

where cpu_i is the required processing capacity; ram_i is the required amount of RAM; bw_i is the required network bandwidth; and s_i represents additional service requirements, including acceptable latency, availability level, or other SLA parameters.

Each resource v_j is characterized by a vector of available capacities

$$r_j = \left(CPU_j, RAM_j, BW_j\right), \tag{2.26}$$

as well as by cost, energy consumption, performance, and security parameters. To describe the resource allocation process, a binary variable is introduced:

$$x_{ij} = \begin{cases} 1, & \text{if task } j_i \, n\text{is assigned to resource } v_j, \\ 0, & \text{otherwise.} \end{cases} \tag{2.27}$$

Then, each task must be assigned to exactly one resource:

$$\sum_{j=1}^{m} x_{ij} = 1, i = 1, \ldots, n. \tag{2.28}$$

In addition, the constraints related to available resources must be satisfied. For processing capacity:

$$\sum_{i=1}^{n} cpu_i x_{ij} \le CPU_j, j = 1, \ldots, m. \tag{2.29}$$

For RAM:

$$\sum_{i=1}^{n} ram_i x_{ij} \le RAM_j, j = 1, \ldots, m. \tag{2.30}$$

For network bandwidth:

$$\sum_{i=1}^{n} bw_i x_{ij} \le BW_j, j = 1,\ldots,m. \tag{2.31}$$

Thus, a configuration \(x\) is considered feasible only if all tasks are allocated among the resources and the available processing, memory, and network capacities are not exceeded.

A separate group includes constraints related to the quality of service. If the maximum acceptable latency L_i^{max} is defined for task j_i then the following condition must be satisfied:

$$L_i(x) \le L_i^{max}. \tag{2.32}$$

Similarly, if the SLA defines a minimum level of availability A_i^{min}, the corresponding availability constraint must be satisfied.

This group may also include constraints related to the geographical location of data, the type of cloud provider, the permitted data storage region, or requirements for using resources with a specific level of security certification.

The first optimization criterion is task execution time. For task j_i, assigned to resource v_j, the execution time can be represented as

$$t_{ij} = \frac{w_i}{p_j} + l_{ij}, \tag{2.33}$$

where w_i is the computational workload of the task; p_j is the performance of resource and l_{ij} is the additional network or communication delay.

The overall makespan of the system is then defined as

$$T(x) = \max_{i=1,\ldots,n} t_i^{finish}. \tag{2.34}$$

Minimizing $T(x)$ is aimed at reducing the overall workload processing time and improving the performance of the cloud system.

The second criterion is the cost of resource usage. If c_j is the cost per unit of time for using resource v_j, the total cost can be defined as

$$C(x) = \sum_{i=1}^{n} \sum_{j=1}^{m} c_j t_{ij} x_{ij}. \tag{2.35}$$

The function $C(x)$ takes into account that different resources may have different pricing models and that a more powerful resource is not necessarily the most cost-effective option.

The third criterion is energy consumption. In a simplified form, it can be represented as

$$E(x) = \sum_{j=1}^{m} P_j(u_j) \cdot \tau_j, \tag{2.36}$$

where $P_j(u_j)$ is the power consumed by resource v_j at utilization level u_j; τ_j is the duration of its active use. This formulation makes it possible to consider the effect of resource consolidation: reducing the number of active nodes can decrease energy consumption, but at the same time it may affect system performance and the level of risk.

The fourth criterion is the overall cyber risk $R(x)$. For each resource, parameters can be defined to describe its level of security, including the implementation level of identity mechanisms, access control, microsegmentation, monitoring, backup, and resilience. Let each threat $q \in Q$ be characterized by the probability of its occurrence $p_q(x,t)$ and its potential impact $I_q(x,t)$. Then, the current cyber risk can be represented as

$$R(x,t) = \sum_{q=1}^{s} w_q \, p_q(x,t) I_q(x,t), \tag{2.37}$$

where w_q is the weighting coefficient that represents the importance of the corresponding threat.

Since the cloud environment is dynamic, it is also reasonable to consider changes in threat intensity over time. For this purpose, a function $\lambda_q(t)$ is introduced, which represents the intensity, relevance, or relative probability of the q-th threat at time t. Then, the overall risk over the time interval $[0,T]$ can be defined as

$$R(x) = \sum_{q=1}^{s} w_q \int_0^T \lambda_q(t)\, p_q(x,t)\, I_q(x,t)\, dt. \tag{2.38}$$

The function $\lambda_q(t)$ makes it possible to consider changes in the external security situation, such as the appearance of new vulnerabilities, an increase in attack intensity, or a change in the level of trust in a specific group of resources. If the threat environment is relatively stable, $\lambda_q(t)$ can be considered constant. In dynamic scenarios, it can be determined based on monitoring data, event logs, or external threat indicators.

In this formulation, cyber risk depends not only on the external environment but also on the resource allocation solution x. For example, placing several critical tasks on the same node may reduce cost and energy consumption but increase the potential consequences if this node is compromised. Similarly, using a resource with a lower level of segmentation or less strict access policies may improve $T(x)$ or $C(x)$, but increase $R(x)$. Therefore, cyber risk should be considered not only as a threshold constraint

$$R(x) \le R_{max}, \tag{2.39}$$

but also as a separate optimization criterion.

As a result, the problem takes the form of a multi-objective optimization problem:

$$min\, F(x) = \left(T(x), C(x), E(x), R(x)\right) \tag{2.40}$$

subject to the system of resource, SLA, and security constraints.

If necessary, latency $L(x)$ can also be added to the vector of criteria. However, in the further model, it is reasonable to consider it either as a component of or as an SLA constraint. This makes it possible to avoid an excessive number of interdependent criteria and keep the model interpretable.

Because the objective functions are conflicting, in the general case there is no single solution that simultaneously minimizes $T(x)$, $C(x)$, $E(x)$ and $R(x)$. Therefore, a natural approach to solving this problem is to use the principle of Pareto optimality.

Let $x^{(1)}$ and $x^{(2)}$ be two feasible solutions. Solution $x^{(1)}$ dominates $x^{(2)}$, if $f_k\left(x^{(1)}\right) \le f_k\left(x^{(2)}\right)$ for all criteria k, and a strict inequality holds for at least one criterion. If there is no other feasible solution that dominates a given solution, this solution is Pareto-optimal.

The set of such solutions can be represented as $P^* = \{x \in X : \text{y}\, y \in X, \quad F(y)\,\text{p}\; F(x)\}$, where X is the set of feasible configurations, and the symbol \(\prec\) represents Pareto dominance.

The formation of the Pareto front makes it possible to obtain not one solution but a set of trade-off solutions. One solution may provide the minimum cost with a slightly higher level of risk, another may provide the minimum cyber risk at the cost of additional expenses, while a third may provide a balance between performance and energy consumption. This is especially important for cloud systems, where priorities may change depending on the type of workload, task criticality, and the current level of cyber threats.

Thus, the proposed mathematical model combines the classical parameters of cloud resource allocation with a dynamic cyber risk criterion. Its key feature is that $R(x)$ depends not only on the external threat environment but also on the resource configuration itself. This makes it possible to directly consider Zero Trust parameters,

resilience, and provider security characteristics during the optimization process. To find a set of Pareto-optimal solutions, it is reasonable to use a multi-objective evolutionary algorithm, particularly NSGA-II, adapted to consider dynamic cyber risk and security-aware constraints.

To solve the formulated multi-objective cloud resource allocation problem, it is reasonable to use the NSGA-II (Non-dominated Sorting Genetic Algorithm II) evolutionary algorithm. Its selection is based on the discrete nature of the problem, the large number of possible resource allocation configurations, and the presence of several conflicting criteria. Unlike approaches that combine several criteria into a single weighted objective function, NSGA-II makes it possible to generate a set of non-dominated solutions within one optimization process and analyse the trade-offs between execution time $T(x)$, cost $C(x)$, energy consumption $E(x)$, and cyber risk $R(x)$. The effectiveness of NSGA-II modifications for multi-objective resource allocation problems in cloud environments is supported by recent research (Chen J., Du T., Xiao G., 2021).

A specific feature of the proposed approach is the combination of NSGA-II with a security-aware solution evaluation mechanism and adaptation to changes in cyber risk. This makes it possible not only to find trade-off resource configurations but also to adjust the search process when the state of the threat environment changes. Thus, NSGA-II is used as the basic multi-objective search mechanism, while additional procedures for risk assessment, security constraint checking, and adaptive parameter adjustment form its modified version.

A solution to the problem is encoded as a chromosome $X = (x_1, x_2, \ldots, x_n)$, where n is the number of computing tasks, and the value $x_i = j$ means that task i_i is assigned to cloud resource v_j, $j \in \{1, \ldots, m\}$. This representation is compact and directly corresponds to the matrix of binary variables x_{ij} introduced in the mathematical model. For example, the chromosome $X = (2,1,4,2,3)$ v_2, the second task on v_1, the third task on v_4, and the fifth task on v_3.

At the first stage, the initial population is generated $P_0 = \{X_1, X_2, \ldots, X_N\}$, where N is the predefined population size. The simplest approach is to generate assignments randomly. However, a significant number of such solutions may violate CPU, RAM, or bandwidth constraints. Therefore, it is reasonable to use a hybrid approach to initial population generation: some individuals are generated randomly to ensure diversity, while others are created using heuristic rules. In particular, tasks can be assigned to resources with sufficient remaining capacity, minimum predicted execution time, or an acceptable level of cyber risk. This approach combines the global search capabilities of the evolutionary algorithm with the advantages of heuristic generation of initial solutions.

After each individual is generated, its feasibility is checked:

$$\sum_i cpu_i x_{ij} \le CPU_j, \quad \sum_i ram_i x_{ij} \le RAM_j, \quad \sum_i bw_i x_{ij} \le BW_j. \tag{2.41}$$

In addition, SLA requirements and defined critical security requirements are checked. If a solution violates resource constraints, a repair procedure can be applied. This procedure moves individual tasks to resources with sufficient remaining capacity. This makes it possible to avoid the accumulation of a large number of infeasible configurations in the population.

For each feasible individual X the vector of criteria is calculated $F(X) = (T(X), C(X), E(X), R(X))$.

The values of $T(X), C(X)$ and $E(X)$ are determined according to the mathematical model presented in the previous section. The value of $R(x)$ is evaluated by considering the characteristics of the resources, Zero Trust mechanisms, and the current state of the threat environment. Thus, two solutions with similar performance characteristics may receive significantly different evaluations because of different levels of cyber risk.

To consider the dynamic nature of cyber risk, the threat intensity function $\lambda_q(t)$ is used. For the current time interval, the risk value is defined as $R(X,t)=\sum_{q=1}^{s} w_q \lambda_q(t)\, p_q(X,t) I_q(X,t)$.

The parameters $p_q(X,t)$ and $I_q(X,t)$ depend on the resource configuration. In particular, they can be adjusted depending on the availability of multi-factor authentication, privilege levels, microsegmentation, monitoring, backup, and other Zero Trust characteristics. Accordingly, a resource with a higher level of security reduces the risk component of the solution, but its use may increase $T(X), C(X)$ or $E(X)$.

For critical tasks, it is reasonable to introduce an additional minimum acceptable security level. Let Z_j represent the overall level of Zero Trust implementation for resource v_j and let Z_i^{min} represent the minimum security requirement for task j_i. Then, the following condition must be satisfied $x_{ij}=1 \Rightarrow Z_j \geq Z_i^{min}$.

Thus, security is considered in the proposed method in two ways: solutions that do not meet the security requirements are rejected as infeasible, while the residual cyber risk $R(x)$ is minimized among feasible configurations. This mechanism makes it possible to avoid situations in which the algorithm selects a low-cost and high-performance solution that is unacceptable from a security perspective.

The next stage of NSGA-II is non-dominated sorting. The population is divided into a sequence of fronts:

$$F_1, F_2, \ldots, F_k, \tag{2.42}$$

where F_1 contains solutions that are not dominated by any other solution in the current population. After these solutions are removed, F_2 is identified, followed by F_3 and so on. Individuals from the first front receive the highest priority during selection. In the proposed formulation, dominance is determined simultaneously according to four criteria.

Thus, solution X_a dominates X_b if

$$T(X_a) \le T(X_b),\ C(X_a) \le C(X_b),$$
$$E(X_a) \le E(X_b),\ R(X_a) \le R(X_b), \tag{2.43}$$

and at least one of these inequalities is strict.

To maintain the diversity of solutions within the same front, crowding distance is used. For each criterion, the individuals are sorted according to the corresponding value. Then, for each internal point, the normalized distance between neighbouring solutions is calculated as:

$$CD_i = \sum_{k=1}^{K} \frac{f_k^{i+1} - f_k^{i-1}}{f_k^{max} - f_k^{min}}, \tag{2.44}$$

where $K = 4$ is the number of criteria. Preference is given to solutions with a larger crowding distance, which prevents the population from becoming concentrated in only one area of the Pareto front and ensures the representation of different trade-offs between performance, cost, energy consumption, and cyber risk.

New solutions are generated using crossover and mutation operators. During the crossover of two parent chromosomes, some task assignments are inherited by the first offspring from one parent, while the remaining assignments are inherited from the other parent. After the crossover operation, resource and security constraints are checked. Mutation involves changing the assigned resource for one or more tasks:

$$x_i = j \to x_i = j', j' \ne j. \tag{2.45}$$

The mutation operator generates new configurations and reduces the probability of premature convergence of the algorithm.

To improve efficiency, it is proposed to use an adaptive mutation mechanism related to changes in cyber risk. Let $\bar{\lambda}(t)$ is the aggregated intensity of current threats. The mutation probability can be defined as:

$$p_m(t) = p_m^{min} + \left(p_m^{max} - p_m^{min}\right)\frac{\bar{\lambda}(t)}{\lambda_{max}}, \tag{2.46}$$

where p_m^{min} and p_m^{max} are the minimum and maximum mutation probabilities. When the security situation is stable, the algorithm operates with a lower intensity of changes, preserving the efficient configurations that have already been found. When the intensity of threats increases $p_m(t)$ increases, the mutation probability also increases, which expands the search and improves the probability of quickly finding an alternative and more secure resource allocation solution.

The hybridization of the method also includes the use of a local security-aware heuristic for some of the obtained solutions. If a specific task makes a significant contribution to $R(x)$, the algorithm analyses alternative resources that meet the task requirements and performs local reassignment if it reduces the risk without an unacceptable deterioration of the other criteria. Thus, the global evolutionary search of NSGA-II is combined with targeted local improvement of resource configurations.

The general pseudocode of the proposed adaptive hybrid method is as follows.

Input:

J – set of tasks;

V – set of cloud resources;

N – population size;

$G_{\max}$ – maximum number of generations;

$Q(t)$ – current characteristics of cyber threats.

1. Generate the initial population $P0$:

   generate some solutions randomly;

   generate some solutions using heuristic rules.

2. For each $X \in P0$:

   check CPU, RAM, bandwidth, and SLA constraints;

   check security/Zero Trust constraints;

   if necessary, apply the repair procedure;

   calculate $T(X)$, $C(X)$, $E(X)$, $R(X,t)$.

3. For $g = 1,...,G_{max}$:

update $\lambda_q(t)$ and the risk parameters;

perform non-dominated sorting;

calculate the crowding distance;

perform tournament selection of parents;

apply crossover;

determine the adaptive mutation probability $p_m(t)$;

apply mutation;

check the feasibility of offspring and apply the repair procedure;

apply security-aware local improvement to selected solutions;

calculate $T(X)$, $C(X)$, $E(X)$, $R(X,t)$ for the new individuals;

combine the parent and offspring populations;

perform non-dominated sorting of the combined population;

generate the next population P_g according to rank and crowding distance.

4. Return the set of non-dominated solutions P^*.

Output:

the Pareto set of trade-off cloud resource allocation configurations.

Thus, the proposed method is an adaptive security-aware modification of NSGA-II, in which the classical Pareto optimization mechanism is extended by three components: dynamic cyber risk assessment using $\lambda_q(t)$, security constraints on the feasible placement of critical tasks, and a local heuristic for resource reassignment. Adaptive adjustment of the evolutionary search parameters makes it possible to respond to changes in threat intensity without the need to completely revise the mathematical model.

The result of the algorithm is not a single configuration but a set of Pareto-optimal solutions $P^* = \left\{X^{(1)}, X^{(2)}, \ldots, X^{(k)}\right\}$, from which a solution can be selected according to the current operating conditions of the system. Under a normal threat level, priority may be given to cost and performance. However, when $\lambda(t)$ increases, it becomes reasonable to move to configurations with a lower $R(x)$, even if they have slightly higher costs or execution time. This feature provides a connection between

multi-objective resource optimization, Zero Trust principles, and adaptive cyber risk management in a dynamic cloud environment.

To evaluate the proposed adaptive security-aware approach to multi-objective cloud resource allocation optimization, it is reasonable to consider several simulation scenarios with different workload levels and cyber threat intensities. The basic scenario represents the normal operating mode of the system with a stable workload and a low value of $\lambda(t)$. The second scenario includes an increase in the number of tasks and the utilization of computing resources, while the third scenario considers an increase in cyber threat intensity. In addition, a combined scenario can be considered, where both the workload and the level of cyber risk increase at the same time. This approach makes it possible to evaluate the ability of the algorithm to adapt resource allocation to changes in both computing and security conditions.

The comparison between traditional and security-aware optimization should be performed using the same sets of tasks and resources. In the traditional case, the solution is generated according to the criteria $F_{trad}(x) = \big(T(x), C(x), E(x)\big),$ while the proposed approach uses the extended vector $F_{sec}(x) = \big(T(x), C(x), E(x), R(x)\big).$

The main difference between these formulations becomes clear when a resource with a low cost or high performance is characterized by increased cyber risk. A traditional algorithm does not have a separate criterion for distinguishing such configurations according to their security level. In contrast, security-aware optimization makes it possible to exclude solutions that do not meet the defined security constraints and to consider $R(x)$ when forming the set of non-dominated solutions.

The result of multi-objective optimization should be analysed using the Pareto front, where each point represents a feasible resource allocation configuration. Moving from three to four criteria expands the space of possible trade-offs. For example, solution x_1 may provide the minimum cost $C(x)$, but have a higher cyber risk $R(x)$; solution x_2 may provide the minimum execution time $T(x)$ but have higher energy consumption; and solution x_3 may provide lower cyber risk by using more secure but more expensive resources. Therefore, the Pareto front makes it possible to avoid

defining a single fixed relationship between the weights of the criteria in advance and to select a configuration according to the current state of the cloud system.

The behaviour of the model when the function $\lambda(t)$ changes is especially important. When the threat intensity is low, priority may be given to solutions with lower $T(x)$, $C(x)$ and $E(x)$. An increase in $\lambda(t)$ increases the contribution of the corresponding threats to $R(x)$. As a result, some configurations that were previously efficient may lose their advantage. The algorithm can then move to another area of the Pareto front, where resources with a higher level of Zero Trust implementation, better segmentation, access control, and monitoring are used. In this way, resource allocation can adapt to changes in the security situation.

The practical application of the proposed approach is especially appropriate for hybrid and multi-cloud systems, where it is possible to choose between resources with different levels of performance, cost, and security. For non-critical tasks under a low threat level, cost-effective configurations can be used. For tasks related to critical services or sensitive data, it is reasonable to define minimum security and Zero Trust requirements and select only resources that meet these requirements. If $\lambda(t)$ increases, the system should provide a repeated evaluation of the Pareto set and, if necessary, workload migration.

Thus, the practical advantage of security-aware optimization is not the unconditional minimization of cyber risk at the cost of other system characteristics, but the possibility of making a controlled trade-off between cost, performance, energy consumption, and cyber risk. The proposed approach can be used as a component of decision support systems for cloud infrastructure management, where current monitoring data and threat assessments are used to dynamically update $R(x)$ and select the most appropriate resource configuration. This provides a connection between mathematical optimization, Zero Trust principles, and risk-oriented management of the digital resilience of cloud systems.

REFERENCES FOR SUBSECTION 2.4

1. Chen J., Du T., Xiao G. A multi-objective optimization for resource allocation of emergent demands in cloud computing. Journal of Cloud Computing. 2021. Vol. 10. Art. 20. DOI: 10.1186/s13677-021-00237-7.

2. Shi F., Lin J. Virtual Machine Resource Allocation Optimization in Cloud Computing Based on Multiobjective Genetic Algorithm. Computational Intelligence and Neuroscience. 2022. Vol. 2022. Art. 7873131. DOI: 10.1155/2022/7873131.

3. Malti A. N., Hakem M., Benmammar B. Multi-objective task scheduling in cloud computing. Concurrency and Computation: Practice and Experience. 2022. Vol. 34, № 25. Art. e7252. DOI: 10.1002/cpe.7252.

4. Zhang H., Wu Y., Sun Z. EHEFT-R: multi-objective task scheduling scheme in cloud computing. Complex & Intelligent Systems. 2022. Vol. 8. P. 4475–4482. DOI: 10.1007/s40747-021-00479-7.

5. Latreche I., Slatnia S., Kazar O., Batouche M. A third generation genetic algorithm NSGA-III for task scheduling in cloud computing. Journal of King Saud University – Computer and Information Sciences. 2022. Vol. 34, No. 9. P. 7515–7529. DOI: 10.1016/j.jksuci.2022.03.017.

6. Sissodia R., Rauthan M. M. S., Naithani K. A Survey on Multi-Objective Tasks and Workflow Scheduling Algorithms in Cloud Computing. International Journal of Cloud Applications and Computing. 2022. Vol. 12, № 1. P. 1–16. DOI: 10.4018/IJCAC.297100.

7. Mangalampalli S., Karri G. R., Kose U. Multi objective trust aware task scheduling algorithm in cloud computing using whale optimization. Journal of King Saud University – Computer and Information Sciences. 2023. Vol. 35. P. 791–809. DOI: 10.1016/j.jksuci.2023.01.016.

8. Luo Z.-Y., Chen Y.-N., Liu X.-T. Research on Sparrow Search Optimization Algorithm for multi-objective task scheduling in cloud computing environment. Journal of Intelligent & Fuzzy Systems. 2023. Vol. 45, № 6. DOI: 10.3233/JIFS-232527.

9. Wang X., Lou H., Dong Z., Yu C., Lu R. Decomposition-based multi-objective evolutionary algorithm for virtual machine and task joint scheduling of cloud

computing in data space. Swarm and Evolutionary Computation. 2023. Vol. 77. Art. 101230. DOI: 10.1016/j.swevo.2023.101230.

10. Prathiba S., Sankar S. Energy-efficient resource allocation in cloud infrastructure using L3F-MGA and E-ANFIS. Measurement: Sensors. 2024. Vol. 31. Art. 100965. DOI: 10.1016/j.measen.2023.100965.

11. Çağlar İ., Altılar D. T. Look-ahead energy efficient VM allocation approach for data centers. Journal of Cloud Computing. 2022. Vol. 11. Art. 11. DOI: 10.1186/s13677-022-00281-x.

12. Liu J., Liu X. Energy-efficient allocation for multiple tasks in mobile edge computing. Journal of Cloud Computing. 2022. Vol. 11. Art. 71. DOI: 10.1186/s13677-022-00342-1.

13. Wang B., Wang C., Huang W., Song Y., Qin X. Security-aware task scheduling with deadline constraints on heterogeneous hybrid clouds. Journal of Parallel and Distributed Computing. 2021. Vol. 153. P. 15–28. DOI: 10.1016/j.jpdc.2021.03.003.

14. Wang B., Liu F., Lin W., Ma Z., Xu D. Energy-efficient collaborative optimization for VM scheduling in cloud computing. Computer Networks. 2021. Vol. 201. Art. 108565. DOI: 10.1016/j.comnet.2021.108565.

15. Saxena D., Singh A. K. A proactive autoscaling and energy-efficient VM allocation framework using online multi-resource neural network for cloud data center. Neurocomputing. 2021. Vol. 426. P. 248–264. DOI: 10.1016/j.neucom.2020.08.076.

16. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg : National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.SP.800-207.

17. Chandramouli R., Butcher Z. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments. NIST Special Publication 800-207A. Gaithersburg : National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.SP.800-207A.

18. Chandramouli R., Butcher Z., Chetal A. Attribute-based Access Control for Microservices-based Applications Using a Service Mesh. NIST Special Publication

800-204B. Gaithersburg : National Institute of Standards and Technology, 2021. DOI: 10.6028/NIST.SP.800-204B.

19. Chandramouli R. Implementation of DevSecOps for a Microservices-based Application with Service Mesh. NIST Special Publication 800-204C. Gaithersburg : National Institute of Standards and Technology, 2022. DOI: 10.6028/NIST.SP.800-204C.

20. Chandramouli R., Kautz F., Torres-Arias S. Strategies for the Integration of Software Supply Chain Security in DevSecOps CI/CD Pipelines. NIST Special Publication 800-204D. Gaithersburg : National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.SP.800-204D.

21. Chandramouli R., Hales W. A Data Protection Approach for Cloud-Native Applications. NISTIR 8505. Gaithersburg : National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.IR.8505.

22. Chandramouli R., Butcher Z., Callaghan J. Service Mesh Proxy Models for Cloud-Native Applications. NIST Special Publication 800-233. Gaithersburg : National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.SP.800-233.

23. Sehgal N. K., Bhatt P. C. P., Acken J. M. Cloud Computing with Security: Concepts and Practices. 2nd ed. Cham : Springer, 2020. 355 p. DOI: 10.1007/978-3-030-24612-9.

24. Calles M. A. Serverless Security: Understand, Assess, and Implement Secure and Reliable Applications in AWS, Microsoft Azure, and Google Cloud. Berkeley : Apress, 2020. 347 p. DOI: 10.1007/978-1-4842-6100-2.

25. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing v5. Cloud Security Alliance, 2024.

26. Cloud Security Alliance. Top Threats to Cloud Computing: Pandemic Eleven. Cloud Security Alliance, 2022.

27. European Union Agency for Cybersecurity. Cloud Cybersecurity Market Analysis. Athens : ENISA, 2023.

28. European Union Agency for Cybersecurity. EUCS – Cloud Services Scheme. Draft Candidate Scheme v1.0. ENISA, 2020. ENISA, 2020.

29. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024. Athens : ENISA, 2024.

30. European Union Agency for Cybersecurity. NIS Investments 2024. Athens : ENISA, 2024.

31. Dvirna O. A., Naboka S. V. Cloud Service Performance Optimization: Methods and Their Effectiveness. Control, Navigation and Communication Systems. 2026. No. 1 (83). P. 62–68. DOI: 10.26906/SUNZ.2026.1.062.

32. Holovko H. V., Dvirna O. A., Naboka S. V. Zero Trust for Small and Medium-Sized Businesses. Taurida Scientific Herald. Series: Technical Sciences. 2026. Issue 1, Part 1. P. 84–92. DOI: 10.32782/tnv-tech.2026.1.1.9.

33. 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). Official Journal of the European Union. 2022. L 333. 27.12.2022. P. 80–152.

CHAPTER 3. HUMAN CAPITAL IN THE IT AND CYBERSECURITY SECTOR: EDUCATION, WORKFORCE TRAINING, AND DIGITAL COMPETENCE DEVELOPMENT

3.1. Digital Technologies for Managing University Research Activities: European Experience and Prospects for Implementation in Ukraine

Tetiana DERKACH,
Andrii DMYTRENKO,
National University "Yuri Kondratyuk Poltava Polytechnic",
Lina KLOCHKO,
Geological Bureau BEG SA, Switzerland

Contemporary developments in science, education and digital technologies call for better mechanisms to manage research and research and development activities in higher education institutions (OECD, 2023; UNESCO, 2023). Universities are increasingly adopting digital tools to support research, manage research outputs and monitor research performance (European University Association, 2021).

The quality of specialist training depends substantially on integrating education with research. The active involvement of academic staff in research projects, publishing, international collaboration and the implementation of research findings helps create a modern educational environment that develops students' professional competencies, creative thinking and research skills.

At the same time, the continuing growth of scientific information, the increasing number of publications and the need to prepare numerous reports place an additional burden on academic staff. A considerable amount of time is spent on administrative procedures associated with collecting, organising and analysing data on research achievements, reducing the time available for research itself.

One promising response is to introduce specialised information systems to support research activities. Such systems provide centralised information storage,

automate report preparation, monitor research indicators and integrate with external bibliometric resources. Modern information technologies can substantially accelerate data processing, reduce errors and make management processes more transparent.

In the context of digital transformation, automating the collection, analysis and use of research information is particularly important. Growing volumes of research data require modern research information management systems that integrate information resources and support management decisions (Bryant et al., 2021).

One priority in developing research infrastructure is to implement open science principles and ensure access to research findings (Schuetze et al., 2024; Wilkinson et al., 2016). In this context, international researcher identification and bibliometric platforms such as ORCID and Google Scholar are important for monitoring researchers' publication activity and citations.

The digitisation of research is especially significant in the context of European Union initiatives to develop the European Research Area (ERA). Current European research policy prioritises open science, digital research infrastructure and integrated research information management systems. Horizon Europe places considerable emphasis on effective management of research outputs, open access to research data and stronger international scientific collaboration. The European Open Science Cloud (EOSC) is an important means of achieving these goals, providing researchers with a shared digital environment for storing, processing and disseminating research data. These initiatives shape current trends in research management information systems and provide a conceptual basis for the digital transformation of higher education institutions.

Intelligent information systems can automate a substantial share of the administrative procedures associated with supporting research, thereby improving the efficiency of educational and research institutions (Bryant et al., 2021).

The aim of this study is to develop an intelligent information system for managing a department's research and research and development activities. The system is intended to automate the recording, analysis and presentation of research outputs and improve information support for academic staff.

The digital transformation of higher education institutions has encouraged the adoption of specialised platforms to support research, manage research outputs and monitor research performance. In today's research environment, these systems are important tools for collecting, analysing and disseminating scientific knowledge (European University Association, 2021; OECD, 2023; Smith, 2023; UNESCO, 2023).

ORCID is one of the most widely used international tools. It provides unique researcher identifiers and supports the integration of information on publications, projects and professional activities. Its use improves the reliability of authorship data and facilitates interaction among information platforms.

Google Scholar plays an important role in scholarly communication by automatically indexing publications and calculating key bibliometric indicators. Given its broad coverage of sources, it is one of the most accessible tools for assessing researchers' scholarly activity.

Academic social networks, particularly ResearchGate and Academia.edu, have also become widespread. They support scholarly communication, the exchange of research findings and the formation of professional research communities (Bryant et al., 2021; Wilkinson et al., 2016). However, these platforms primarily disseminate research materials and do not provide comprehensive support for management processes within higher education institutions.

Universities increasingly use current research information systems (CRIS) to manage research outputs centrally (Schuetze et al., 2024; Wilkinson et al., 2016). Prominent examples include Pure, Converis and Symplectic Elements. These systems bring information on researchers, publications, grants, projects, patents and other research outputs together in a single information environment (Leal Filho et al., 2023; Wilkinson et al., 2016).

A comparison of existing platforms indicates that most focus either on collecting bibliometric information or on supporting scholarly communication. Automation of internal research management processes at the level of university departments and other units often remains insufficiently addressed. This creates a need for specialised

information systems adapted to the way research is organised at individual institutions (Leal Filho et al., 2023).

The system developed in this study differs from existing solutions by focusing on the automation of a department's internal research management processes, report preparation, monitoring of research indicators and integration of research outputs within a single information environment. This approach combines the recording, analysis and management of research resources in one software system.

The development of modern research management systems is influenced by EU strategic initiatives aimed at creating a common digital research environment and implementing open science principles. Within the ERA, research management processes are being digitised, research outputs made more accessible and information resources integrated internationally.

Horizon Europe is one of the EU's key initiatives and its largest framework programme supporting research and innovation. The programme emphasises digital research infrastructure, open data, collaboration between institutions and modern research management information systems.

The development of the European Open Science Cloud (EOSC) is particularly significant. EOSC gives researchers access to an integrated environment for storing, processing, analysing and reusing research data. It brings together resources from universities, research centres and international organisations in a shared digital research environment.

Current research information systems (CRIS) aligned with the standards of euroCRIS are being adopted across EU countries. The CERIF standard (Common European Research Information Format) enables interoperability among university and research institution systems, facilitating automated exchange of information about researchers, projects, publications, grants and research outputs.

European open science policy plays a substantial role in the digital transformation of research. It calls for open access to scientific publications, research data and the outputs of publicly funded research. Applying open science principles

makes research more transparent, strengthens international collaboration and improves the use of research resources (European Commission, 2021, 2022, 2023).

These approaches and technologies can inform the development of research management information systems in Ukrainian higher education institutions. Integration with international digital platforms, support for open science standards and the adoption of European research information management models can improve research efficiency and expand international academic collaboration.

Information system design is a key stage of development: it establishes the conceptual structure of the future software product, defines how its components interact and sets principles for scalability, reliability and further development (Galliers and Leidner, 2020; Galliers and Stein, 2025; Ivanova et al., 2024; Tekli et al., 2025).

The intelligent information system for managing a department's research and research and development activities was developed using contemporary approaches to multilayer information systems. The main priorities were coherent information flows, efficient data processing and a convenient means of interaction between users and the software environment.

The first design stage analysed functional requirements based on how higher education institutions organise research. This identified the main business processes to be automated and defined the information objects and their relationships.

The system architecture is based on modularity and the distribution of functions among distinct layers. This gives components independence, simplifies software maintenance and supports future upgrades.

The overall structure of the information system is shown in Fig. 3.1.

The software system has three principal layers. The first enables user interaction and presents information. The second implements application logic, processes requests and performs data analysis. The third stores, retrieves and manages the system's information resources.

Reusing software components is especially important in the design process. Standard libraries, service modules and exception handling mechanisms shorten development time and improve software reliability.

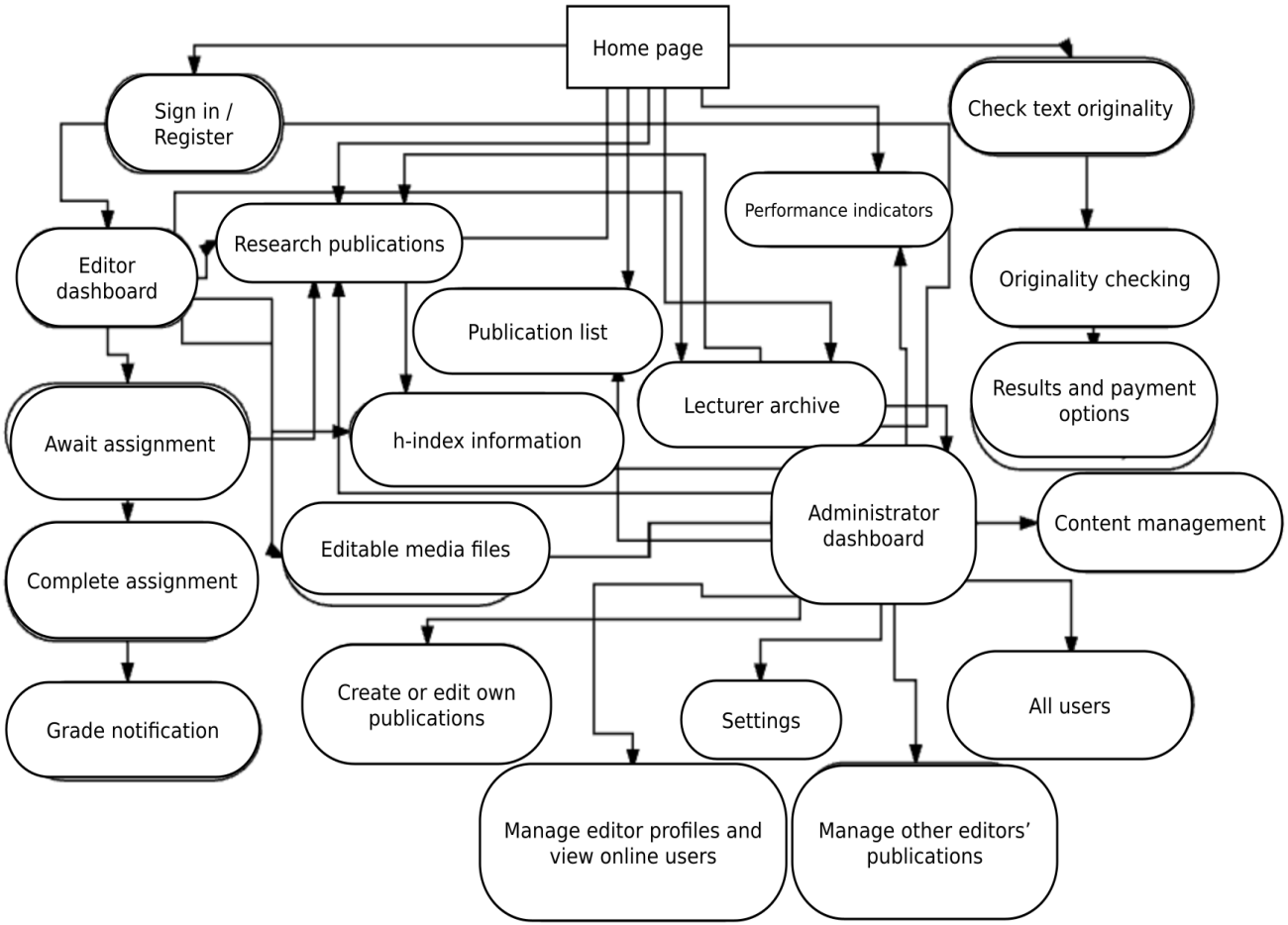


Fig. 3.1. Overall structure of the information system

Object oriented modelling tools were used to formalise the system structure and describe interactions among its components. This approach visualises the software architecture, describes system functions and defines scenarios for user interaction with the software environment.

Modelling the information system provided a coherent understanding of its structure before implementation began. This reduced risks associated with later functional expansion and helped align the functional requirements with technical solutions.

The architectural design stage produced a conceptual model of the research and research and development management system. It defines interactions among users, software modules and the database, and provides a basis for implementing the software.

An important stage in creating the information system is formalising functional requirements and describing user interaction with the software environment. Functional modelling was therefore performed to define the main services, user access rights and the logic of key business processes.

The system's functional model uses scenarios describing typical sequences of user actions involving information resources. At the design stage, this helps establish the system's functional boundaries, assess whether the requirements are fully addressed and identify potential conflicts among software components.

The study identified three main user categories, each with its own functions and level of access to information resources.

The first category comprises system administrators, who manage the software environment, oversee user registration, keep reference information up to date and maintain the information services. Administrators have access to all functional modules and are responsible for configuring them.

The second category comprises editors: lecturers, academic staff, postgraduate students and researchers authorised to create, edit and publish research materials. Their

functions include managing publications, checking texts, preparing information on research outputs and maintaining a personal profile.

The third category consists of external users, who cannot edit information but may view published materials, statistical reports and information on the department's research. This supports access to research outputs and dissemination of information to interested parties.

Formalising interactions between users and functional modules established the system's principal use cases: user authentication, creation and editing of research publications, profile management, report generation, viewing statistical indicators, monitoring bibliometric data and checking texts for originality.

Particular attention was given to the system's operating dynamics. Analysis of the sequence of operations defined the flow of information among users, application modules and the database. The resulting model shows the sequence from receipt of a request to delivery of the required result to the user. Figure 3.2 shows the administrator activity diagram.

Functional modelling provided the basis for subsequent database design, software module implementation and user interface development. It also aligned functional requirements with architectural decisions made during system development. The system use case diagram is shown in Fig. 3.3.

The effectiveness of any information system depends substantially on the quality of its database design. The database is the central element of the information environment, collecting, storing, processing and retrieving the information needed to support management and research processes.

A logical data model was developed for the department's research and research and development management system, representing the structure of research information and the relationships among its main elements. This domain includes many interrelated objects, including academic staff, students, research publications, conferences, research projects, performance indicators and reporting documents.

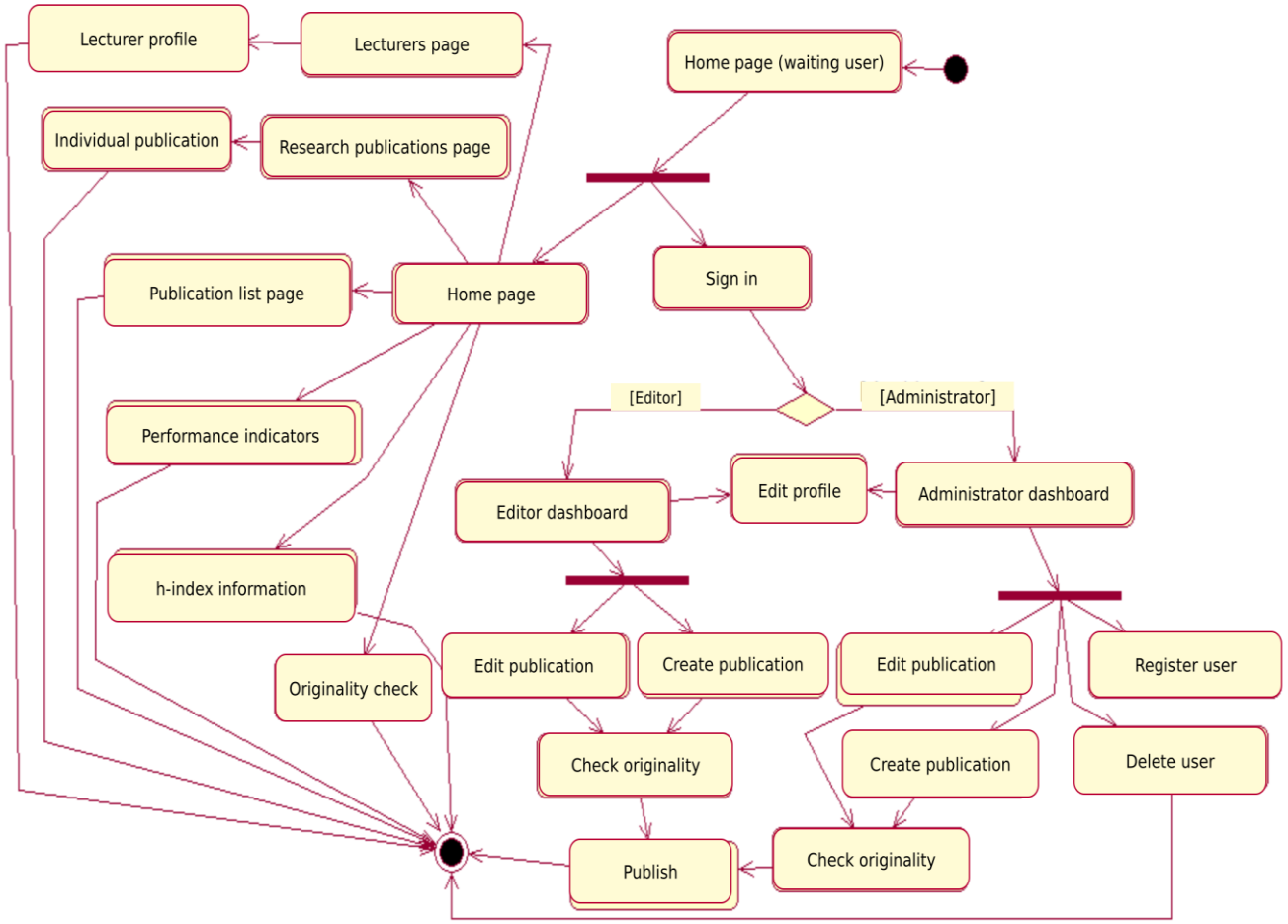


Fig. 3.2. Administrator activity diagram

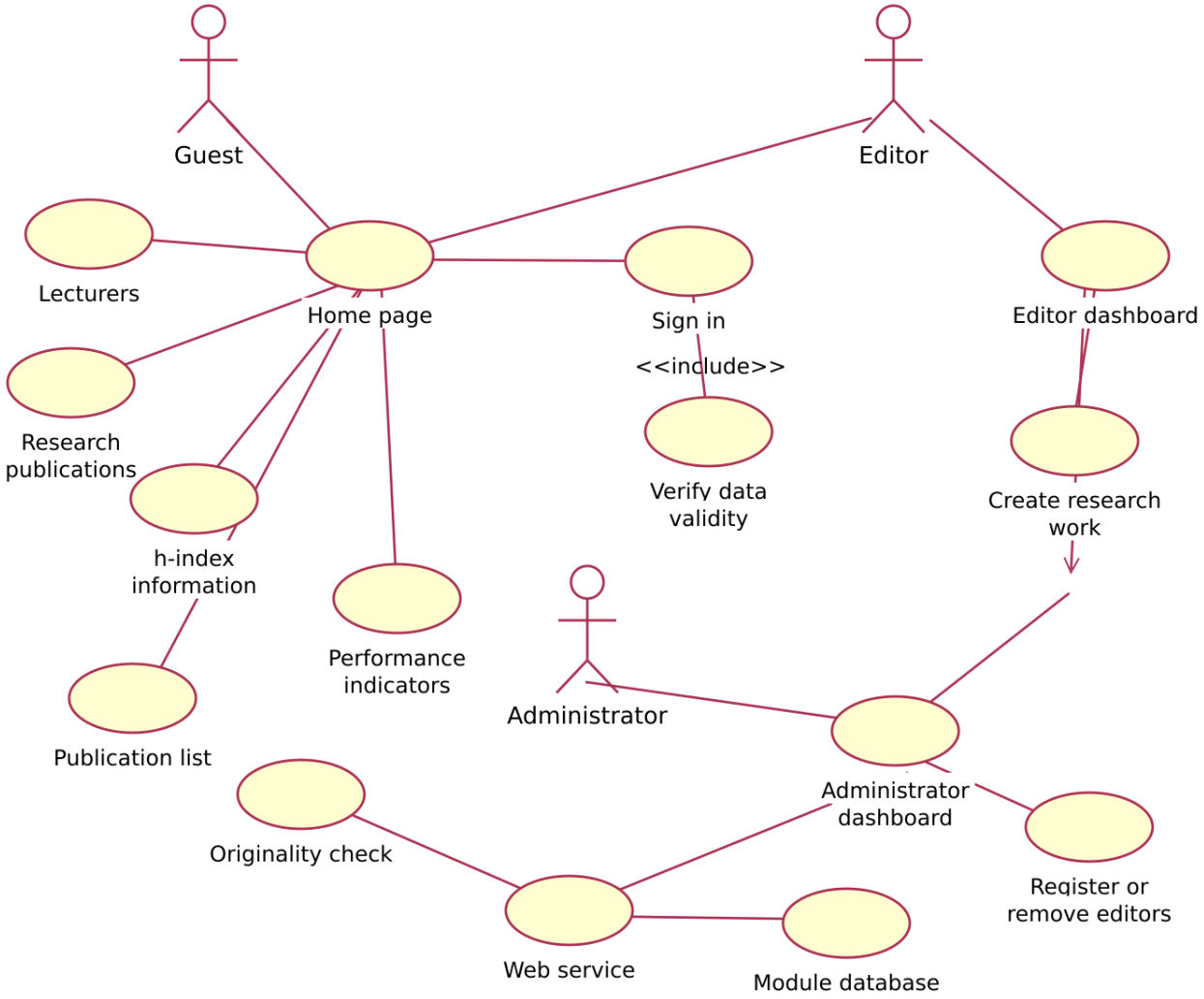


Fig. 3.3. Use case diagram

Database design focused on data integrity, minimising duplication and enabling efficient analytical queries. Relational modelling principles were used to represent complex information objects through interconnected tables (Akhtar, 2023; Amer-Yahia et al., 2023; Tekli et al., 2025).

The database distributes information among separate entities according to their functions. This provides flexibility in managing and updating data and allows the system's functions to be expanded without substantial changes to its architecture.

Maintaining consistency between research outputs and their authors is particularly important. Logical links between information objects keep data current and ensure correct report generation. These links increase information reliability and reduce the likelihood of processing errors (Bauer et al., 2023; Galliers and Leidner, 2020).

A key system requirement was the ability to accommodate changing information. Details of publications, academic degrees, citation indicators and other aspects of research activity are continually updated. The database was therefore structured to allow prompt changes without compromising the integrity of the information environment.

Search and reporting were also optimised during design. The database structure enables rapid retrieval of statistical indicators, preparation of analytical reports and selection of records by different criteria. This supports management decisions and comprehensive analysis of research outputs.

The resulting database model provides a reliable information foundation for the research and research and development management system, enabling effective storage, analytical processes and future software development.

The quality of user interaction with the software environment is another important determinant of system effectiveness. Regardless of the software's functional complexity, ease of access to information and intuitive core operations directly affect its usefulness.

The department's research management information system was designed with particular attention to a clear, logically organised interface. The principal goal was an environment that provides rapid access to system functions and minimises the time users spend on routine operations.

Interface design was based on the professional needs of the main user categories. The working practices of academic staff, administrators and external users informed a navigation structure aligned with the most common usage scenarios.

Functional consistency across all interface elements was an important design principle. Information blocks, menus, navigation and search were arranged so users could find what they needed and complete tasks without additional training (OpenStax, 2025).

The organisation of the system's information space is particularly important. A hierarchical presentation of data was implemented to make information easier to understand and allow users to access additional detail as needed. This reduces information overload and improves work with large volumes of research data.

The interface design also considered visual consistency. Common design principles create a coherent information environment, strengthen users' confidence in the system and contribute to a positive user experience.

User guidance is an important interface component. Notifications, hints and feedback on completed operations support effective interaction. They inform users promptly about data processing status, help prevent errors and make the software's functions easier to learn.

Search and filtering also received particular attention. Because the system handles substantial volumes of research materials and statistical data, rapid access to relevant information is essential. Search tools enable users to retrieve information promptly using defined criteria and work conveniently with information resources.

The resulting user interface supports effective interaction with the software environment, improves productivity and makes the information system easier to use in research management.

A key functional component of the system is its reporting and analytical data processing subsystem. It automates the collection, organisation and aggregation of information on the department's research and research and development outputs.

Higher education institutions continually monitor research activity indicators, which requires processing large volumes of information. Conventional report preparation often involves manually collecting data from multiple sources, taking considerable time and increasing the risk of errors. Automated reporting substantially improves the speed and reliability of the resulting information.

The system includes tools for producing statistical, reference and analytical indicators. It automatically generates reports on departmental staffing, academic staff publication activity, lecturer and student participation in research events, and research outcomes.

Analysis of early career researchers' activities is particularly important for assessing their involvement in research and identifying directions for developing research groups. The system also generates reports on student participation in research, an important indicator of integration between the educational and research functions of the university.

The analytical module aggregates indicators for individual departments and other organisational units. This enables comparisons of research performance, assessment of trends in research areas and an evidence base for management decisions.

An important feature is automatic calculation of indicators describing publication activity, research productivity and individual academic staff contributions to overall departmental results. These data can support internal reports, accreditation, assessment of organisational units and planning future research.

The reporting subsystem thus automates routine tasks and supports management processes aimed at improving research effectiveness in a higher education institution.

Implementing the department's research and research and development management system involved creating an integrated software environment that supports the collection, processing, analysis and presentation of research outputs.

The system's functional structure follows a modular architecture. This makes software components independent, simplifies maintenance and permits future functional expansion.

The user management module forms the core of the software system, handling authentication, authorisation and access control. Role based access enables different interaction scenarios according to user category and responsibilities.

A research publication management module is central to the architecture. It supports the complete lifecycle of research materials, from creation and editing through publication and archiving. This centralises research output storage and provides a shared information environment for academic staff.

The bibliometric indicator management module is another important component. It collects and analyses publication, citation and other research performance data. This functionality provides prompt access to current information on the research achievements of individual staff members and the department as a whole.

A text analysis module supports quality control of research materials. It assesses text originality and identifies potential matches with existing information resources. Integration into the information environment automates preliminary checks of research materials before publication.

The analytical reporting module is essential to system operation. It automatically generates statistical and analytical materials about departmental research outputs. This reduces the time needed to prepare reports and increases the reliability of the results.

Personalised workspaces make the system more convenient. Each user accesses a set of functions suited to their permissions and professional needs. This improves work efficiency and supports effective use of the software.

Particular attention was paid to system administration. The administration module manages users, configures software settings, maintains reference resources and oversees information security. Centralised administration supports stable and secure operation.

The software can adapt to changes in the organisation of research. Categories of research materials can be expanded, report structures changed and new information services integrated without major changes to the architecture.

The implementation results indicate the value of modern information technology for automating research management. The software environment centralises research information management, improves data processing and strengthens information support for the institution’s educational and research activities.

The study addressed a practical research problem: improving the management of research and research and development activities in higher education through modern information technology. Analysis of existing approaches to research information support showed a need for specialised software that automates the collection, processing and analysis of research information.

The study developed a concept for an intelligent system to manage a department’s research and research and development activities. It integrates information resources, automates report preparation and supports management decisions based on current research output data.

Analysis of the subject area informed a software architecture integrating modules for user management, research publications, bibliometric indicators, analytical reporting and quality control of research materials. The modular approach provides scalability, flexibility and capacity for further development in response to the needs of the educational and research environment.

Functional modelling formalised the main business processes, defined user interaction scenarios and aligned functional requirements with technical solutions.

The database structure reliably stores information on research outputs, supports complex analytical queries and enables effective management of departmental information resources. The data processing mechanisms automate statistical and analytical reports used to assess research performance.

Particular attention was devoted to a user interface that supports effective interaction with the system. The proposed solutions improve usability and reduce the time needed for typical operations.

The practical value of the findings is that the system can automate research management in individual departments and other units of higher education institutions. The approach can be adapted to different organisational settings and integrated with external information resources, bibliometric databases and electronic document management systems.

Future research may develop intelligent methods for analysing research data, apply artificial intelligence to management decision support, automate forecasts of research performance indicators and expand integration with international research information platforms.

The findings support the use of intelligent information systems as effective tools for the digital transformation of research in higher education institutions and provide a basis for further development of research knowledge management technologies.

Current trends in digital research across the EU underscore the relevance of these findings. EU initiatives within the ERA, Horizon Europe and EOSC demonstrate the need for integrated systems that manage research data effectively, support open science and enable digital interaction among research institutions. The proposed system aligns with the main directions of digital transformation set out in European research and innovation policy and provides a basis for further integration of Ukrainian higher education institutions into the international research information environment.

Future research may develop intelligent analysis of research data, apply artificial intelligence to management decision support, automate forecasts of research performance indicators, expand integration with international research information platforms and implement European research information management standards, including FAIR and open science principles and the CERIF standard used by modern CRIS platforms.

REFERENCES FOR SUBSECTION 3.1

1. Akhtar A. Popularity ranking of database management systems [Electronic resource] / A. Akhtar // arXiv. – 2023. – Available at: https://doi.org/10.48550/arXiv.2301.00847

2. Amer-Yahia S., Bonifati A., Chen L. et al. From large language models to databases and back: a discussion on research and education / S. Amer-Yahia, A. Bonifati, L. Chen et al. // DASFAA 2023 Proceedings. – 2023. – DOI: 10.1007/978-3-031-30637-2_26.

3. Bauer C., Carterette B., Ferro N., Fuhr N. Frontiers of information access experimentation for research and education / C. Bauer, B. Carterette, N. Ferro, N. Fuhr // Dagstuhl Reports. – 2023. – DOI: 10.4230/DagRep.13.8.1.

4. Bryant R. Practices and patterns in research information management: findings from a global survey / R. Bryant, A. Clements, P. de Castro. – Dublin: OCLC Research, 2021. – 94 p. – DOI: 10.25333/QXR6-D439.

5. European Commission. ERA Policy Agenda 2022–2024. – Brussels: European Commission, 2022. URL:https://european-research-area.ec.europa.eu/policy-agenda-2022-2024

6. European Commission. European Open Science Cloud (EOSC). – Luxembourg: Publications Office of the European Union, 2023. URL: https://digital-strategy.ec.europa.eu/en/policies/open-science-cloud

7. European Commission. Horizon Europe 2021–2027. – Luxembourg: Publications Office of the European Union, 2021. URL: https://op.europa.eu/en

8. European University Association. Universities without walls: a vision for 2030. – Brussels: EUA, 2021. – 78 p. URL: https://www.eua.eu/publications/positions/universities-without-walls-eua-s-vision-for-europe-s-universities-in-2030.html

9. Galliers R. Strategic information management: theory and practice / R. Galliers, D. Leidner. – 5th ed. – London: Routledge, 2020. URL: https://www.routledge.com/Strategic-Information-Management-Theory-and-Practice/Galliers-Leidner-Simeonova/p/book/9780367252519

10. Galliers R. The Routledge companion to management information systems / R. Galliers, M.-K. Stein. – 2nd ed. – London : Routledge, 2025. URL: https://www.routledge.com/The-Routledge-Companion-to-Management-Information-Systems/Galliers-Stein-Baiyere/p/book/9781032690469

11. Leal Filho W. Digital transformation and sustainable development in higher education in a post-pandemic world / W. Leal Filho, C. Shiel, A. Paço et al. // Environment, Development and Sustainability. – 2023. – Vol. 25. – P. 567–589. – DOI: 10.1080/13504509.2023.2237933.

12. Modern information technologies in scientific research and educational activities : monograph / L. Ivanova, V. Kaverinskiy, S. Kotlyk et al.; editor-in-chief S. Kotlyk. – Ames, IA: Iowa State University Digital Press, 2024. – 273 p. – DOI: 10.31274/isudp.2024.151.

13. OECD. Digital education outlook 2023: towards an effective digital education ecosystem. – Paris: OECD Publishing, 2023. – 312 p. – DOI: 10.1787/c74f03de-en.

14. OpenStax. Foundations of information systems. – Houston: Rice University, 2025. – 497 p. URL: https://openstax.org/details/books/foundations-information-systems

15. Schuetze H. G. Digitalization of higher education: an introduction / H. G. Schuetze, W. de Vries, G. Álvarez Mendiola // Journal of Comparative and International Higher Education. – 2024. – Vol. 16, No. 2. – P. 6–12. – DOI: 10.32674/jcihe.v16i2.

16. Smith M. D. The abundant university: remaking higher education for a digital world / M. D. Smith. – Cambridge: MIT Press, 2023. – 296 p. DOI: 10.7551/mitpress/14247.001.0001

17. Tekli J. New trends in database and information systems / J. Tekli, J. Gamper, R. Chbeir et al. – Cham: Springer, 2025. – 402 p. – DOI: 10.1007/978-3-031-15743-1.

18. UNESCO. Global education monitoring report 2023: technology in education. – Paris : UNESCO Publishing, 2023. – 547 p. – DOI: 10.54676/UZQV8501.

Wilkinson M. D. The FAIR guiding principles for scientific data management and stewardship / M. D. Wilkinson, M. Dumontier, I. J. Aalbersberg et al. // Scientific Data. – 2016. – Vol. 3. – Article 160018. – DOI: 10.1038/sdata.2016.

3.2. Digitalization of higher education: integration of information quality systems and information security standards

Alla KAPITON
National University "Yuri Kondratyuk Poltava Polytechnic"

In the context of the European course toward the digital decade and the automation of production, purely technical and algorithmized skills are losing their status as a market advantage, since they can easily be delegated to artificial intelligence. In accordance with the concepts of the European Education Area, the key value is shifting toward uniquely human competencies, such as critical and creative thinking, reflection, and ethical maturity. It is precisely this human-centered approach, enshrined in the strategies of the European Union (EU), that enables the transformative power of technology to serve the goals of sustainable development and social inclusion.

Extrapolating current trends in pedagogical innovation and computer science makes it possible to state that artificial intelligence (AI), Big Data, Educational Data Mining, and machine learning (ML) technologies will form the fundamental basis of the architecture of higher education for the coming decade. However, the large-scale diffusion of emergent AI tools (in particular, generative models and adaptive learning systems) into educational practice not only optimizes processes but also fundamentally transforms the threat model. Designing future educational trajectories requires the implementation of the concept of Secure AI by Design, since the use of large volumes of personal and academic data creates new vectors for cyberattacks, including the leakage of confidential information, manipulation of learning analytics, and data poisoning in machine learning algorithms [1-7].

Within the framework of the implementation of the EU Digital Education Action Plan, generative and predictive artificial intelligence has become a systemic driver of

modernization for all participants in the educational process at universities - from students and lecturers to the leadership of higher education institutions (HEIs). The introduction of these technologies into the European higher education area makes it possible to scale models of adaptive (hyper-personalized) learning, automate routine knowledge assessment, and implement predictive analytics for forecasting and reducing the risks of dropout or declining academic performance. At the same time, the role of AI as a global catalyst of systemic educational change directly correlates with institutions' capacity to minimize the accompanying cyber risks. The creation of a secure digital educational space of the future presupposes the implementation of mechanisms for the cryptographic protection of AI tools, authentication of AI agents, counteraction to denial-of-service (DDoS) attacks on educational platforms, as well as the development of ethical and security protocols for data use, which is critically important for ensuring the cyber resilience of the entire system of higher education [1-8, 30-37].

Given contemporary requirements of cyber hygiene, higher education institutions must transform their paradigm from the simple reproduction of knowledge to the formation of the agency of future professionals. This entails the development of autonomous critical thinking, capacity for self-regulation, and the cultivation of a high degree of empathy and social responsibility. The integration of these qualities is a necessary condition for effective interdisciplinary collaboration, constructive civic participation, and addressing the complex challenges of today's globalized world.

A pressing problem is the need to help students in higher education develop a strong sense of professional competence formation. This does not mean copying and pasting solutions from other higher education institutions or countries, but rather seriously and dispassionately examining best practice in our own countries and others in order to understand what works in which context [8-16].

The depth and nature of the impact of these fundamental transformations depend directly on society's capacity for a solidary, systemic, and proactive response to new challenges. In European practice of state-level planning, education is recognized as a strategic foundation of national security and competitiveness. It is precisely through

the modernization of the educational ecosystem, as recorded in the strategies of the European Education Area, that the foundation is laid for the successful long-term development and resilience of the country as a whole. Given that the trends of the present century must be taken into account in this sphere, information technologies in education are enjoying particular popularity. Information technologies in education can take several forms. Each is necessary for full-fledged learning and for making this process comfortable and enjoyable for all parties involved. Above all, information technologies have greatly helped lecturers. They provide an excellent means of obtaining all the necessary information and of competently composing up-to-date and modern lessons. Teaching systems are constantly changing, and an enormous number of discoveries are being made, yet with the help of the internet it is easy to stay up to date at all times and to make one's lessons as useful as possible for people today. It is also impossible not to emphasize the form of teaching itself.

It is beyond dispute that information technologies in education make it possible to find not only texts but also videos, slides, and much more on a given subject. Learning is now interesting and enjoyable, since it takes place not only in the form of narration but also with the help of computers, technical equipment, and projectors, presenting information in the most convenient format for learners. Many people have even come to enjoy pursuing higher education at various institutions, although this was previously a considerable difficulty [17-23].

Above all, technology has made it possible to obtain information in any quantity, rather than being limited to a fixed volume. The ability to use the network has become indispensable. Students have also gained the opportunity to display their creative abilities through various presentations, among other things. It is worth speaking separately about how new information technologies in education have made possible the emergence of entirely new projects that support self-directed learning and distance education, which in turn helps maintain the connection between lecturers and students. Moreover, this no longer requires visits to archives and libraries - it is enough simply to have a personal computer with internet access. Higher education is, without doubt, very important, yet there are people who live too far from institutions or who lack

sufficient time. Completing assignments, projects, and examinations remotely is an excellent way of replacing the classical form of education. Lecturers can now teach by means of software, and also have the opportunity to learn languages with students or acquire a new profession that is not too demanding. New trends and strategies for integrating ICT into daily educational practice are a necessary condition for the modernization of the education system. Digital learning materials differ from traditional ones and offer the possibility of managing them (Tyshchenko D. et al., 2024; Kapiton A. et al., 2026; Shestak Ya. et al., 2025; Bidzilya Yu. M., 2025).

Digital educational technologies open up an unprecedented range of opportunities, the scope of which integrally exceeds the basic expectations of higher education students. Contemporary European experience, drawing on the EU Digital Education Action Plan, demonstrates the rapid penetration of innovative solutions into the academic process. The systematic use of videoconferencing platforms, interactive teaching aids, open educational resources (OER), and networked tools for professional communication is transforming traditional didactics, ensuring the flexibility, inclusiveness, and quality of contemporary learning (International Standards and Guidelines: European Higher Education Area; Standards and Guidelines for Quality Assurance in the European Higher Education Area, ESG). On this basis, the purpose of the study is to analyze existing systems and to develop an improved automated system that should enhance the quality of educational services, raise the level of training of future specialists, improve the performance indicators of the department and the higher education institution, and take a step toward the informatization of the education system. In the course of the work, a number of tasks were defined:

- a comparative analysis of the architecture of contemporary higher education quality management systems: an examination of existing quality management models, with particular emphasis on their vulnerability to external destructive influences, and an analysis of how the centralization or decentralization of educational data within these systems affects their overall level of protection against unauthorized access and manipulation of performance indicators;

- a study of the digitalization of the educational space through the lens of cyber resilience: a comprehensive analysis of the digital transformation processes of HEIs, taking into account the expansion of the "attack surface"; an examination of how the integration of cloud technologies, electronic dean's offices, and learning management systems (LMS) is changing the security architecture of the modern educational environment and what new vectors of cyber threats this creates;
- an assessment of risks, exploitation of vulnerabilities, and justification of methods for their minimization: a systematization of the negative consequences arising from the functioning of current information circuits (for example, the risks of personal data leakage, compromise of digital diplomas, or DDoS attacks on critical educational services), and the development of an incident-management strategy along with the implementation of Zero Trust policies to neutralize identified threats;
- the design, architectural modeling, and deployment of a secure information system for HEIs: the development and practical implementation of a comprehensive information system for managing the educational process on the basis of Security by Design principles, envisaging mechanisms for the cryptographic protection of data, strict user authentication, security-event logging, and the assurance of business-process continuity for the educational institution under conditions of cyberattack.

The main theoretical and practical aspects of the work carried out have been presented in the publications of numerous researchers and have been made public at international, European, and all-Ukrainian scientific and practical conferences, whose publications served as a source of inspiration for the study, analysis, and design of future projects.

The synchronization of ICT solutions with life-support systems has actualized the European approach to cybersecurity as a cross-cutting element of national and supranational resilience. Drawing on the EU Cybersecurity Strategy, the protection of critical infrastructure from hybrid threat vectors has become a basic standard of the sustainable functioning of society. This requires institutions to engage in continuous monitoring and proactive response to digital-space risks. The large-scale diffusion of

remote and hybrid employment models, driven by the consequences of the pandemic and the escalation of geopolitical military conflicts, has substantially broadened the landscape of cyber threats and increased the potential attack surface. This has provoked the transformation of hacking activity into the domain of highly technological, targeted threat vectors of the Advanced Persistent Threat (APT) type, which has forced actors in both the private and public sectors to undertake a forced modernization of corporate and departmental security architecture, in particular through a transition to the Zero Trust Architecture concept (the Network and Information Security Directive; the rules of enhanced cybersecurity in the European Union; *Analysis of the Digital Transformation of Higher Education*; Network Detection and Response; *All About Access Control: Everything Covered from Definition, Types, to Features and How-Tos*; UEBA).

In the geopolitical context of Ukraine, ensuring the cyber resilience of the national segment of cyberspace has become a dominant vector in guaranteeing national security and defense. The continuity of the functioning of state institutions, the preservation of the integrity of information resources, and the stability of critical information infrastructure (CII) depend directly on the state's capacity to neutralize network intrusions and to ensure secure interdepartmental interaction in real time (particularly within the framework of "military-civilian synergy"). The complex nature of contemporary hybrid threats manifests itself through coordinated cyberattacks on critical government services, automated process-control systems, and military logistics, aimed at disorganizing state governance. These destructive factors underscore the critical need for a reconfiguration of the system for training and upskilling cybersecurity specialists. This process must be based on the integration of advanced experience from NATO and EU member states (in particular, ENISA and NIST standards), the adaptation of joint incident-response models, and the implementation of practical cyber-defense cases in higher education (the Network and Information Security Directive).

Guided by the standards of the European Research Area (ERA), post-industrial development requires the continuous acquisition of new knowledge and the integration

of emergent technologies into management practice. In the countries of the European Union, the transformation of complex sociotechnical and scientific processes is based on agile management methodologies [32-35]. This makes it possible to turn the constant renewal of intellectual capital into a key factor in sustainable social development and innovative leadership. Any architectural or operational vector of activity in the IT industry and in the field of information protection is subject to a strict data-processing life cycle. This cycle correlates directly with the classical concept of the cybersecurity triad and risk management, encompassing the stages of consolidating primary data, their intelligent analysis through data mining, integrity verification, identification of threat vectors, multifactor optimization of solutions, and strategic planning of targeted infrastructural changes.

In the current architecture of the global information society, the academic environment of higher education institutions - in particular the teaching staff and students - operates under conditions of the permanent exponential growth of heterogeneous data volumes. The psychophysiological and cognitive limitations of the human subject make it impossible to adequately perceive, verify, and fully analyze these vast information arrays (Big Data) in real time. This objective civilizational challenge drives the intensification of the processes of total informatization and digitalization, which act as the principal determinants of societal development. The current stage in the evolution of the information society imperatively requires ensuring a high level of data quality, authenticity, accessibility, and security, which, in turn, depends directly on the reliability and resilience of the telecommunications infrastructure supporting these processes. The comprehensive process of digitalizing the modern educational ecosystem is a multifaceted vector of development aimed at forming a high-tech educational environment. In the context of contemporary security challenges, this process must proceed along two strategic lines: the training of highly qualified IT specialists and the comprehensive assurance of the cybersecurity of all elements of the infrastructure and of learning participants (Shestak Ya. et al., 2025; Pashkovsky V.F., 2025; Yakovenko Y., 2026; Bidzilya Yu. M., 2025).

At the current stage of the development of the information society, there is a destructive tendency toward the predominance of a recreational and entertainment-oriented use of digital technologies among students, which significantly hinders their integration into academic and research activity. The transformation of young people's consumer interests into productive educational and scientific trajectories is directly determined by the level of professional competence of academic staff. A competent lecturer acts as a key facilitator in laying the foundations of digital literacy, preparing future IT specialists for the safe conduct of life and the professional operation of complex information systems.

Accordingly, the successful implementation of the goals of the EU Digital Education Action Plan is impossible without the involvement of highly qualified experts whose profile meets the requirements of the European DigCompEdu framework. Such specialists must combine a deep understanding of the architecture of contemporary didactic processes with advanced methodologies for integrating IT into their field of activity (*Digital Education Action Plan: Policy Background*; the EU NIS2 Directive: what it is, for what needs it was developed, and why Ukraine is implementing it; *Digital Education Action Plan 2021-2027*). At the same time, their high level of general cultural and scientific erudition is a basic condition for forming a high-quality and secure digital educational environment. At the same time, the process of digitalizing education is characterized by significant institutional and structural-functional contradictions. Most lecturers, in the course of teaching their specialized disciplines, encounter poor architectural quality and vulnerability of software, as well as substantial technical and technological barriers in organizing digital learning. These factors exponentially increase the level of technical stress experienced by educators, provoke methodological regression, and lead to a forced refusal to implement computer technologies in the educational process. In the context of training personnel in the field of IT and cyber defense, this gives rise to a critical contradiction: an educational institution's inability to provide reliable, ergonomic, and cyber-secure infrastructure negates the pedagogical efforts aimed at educating future engineers, since the educational process becomes isolated from the industry's real, state-of-the-art toolset.

A significant proportion of the information and communication technologies implemented in domestic educational institutions operate under conditions of an acute shortage of licensed and specialized software. In the context of the strategic design of a unified information educational space, this destructive factor determines the emergence of such critical problems as the absence of unified software architecture standards and a chronic shortage of qualified engineering and technical personnel capable of ensuring the continuous monitoring, maintenance, and cyber protection of hardware systems. This infrastructural asymmetry and insufficient material and technical provision of schools and regional higher education institutions significantly degrade the effectiveness of the didactic process, acting as a direct consequence of limited state funding and a deficit of targeted capital investment in the digitalization of the material assets of the education sector.

An additional destabilizing factor in this process is the conservatism of static educational publications on local information carriers and the use of outdated methodological approaches to designing monolithic software architecture. A consequence of this inertia is a high rate of moral obsolescence of educational content, as well as a complete absence of architectural flexibility for the prompt scaling, reconfiguration, or integration of new modules according to contemporary industrial principles of continuous integration. A separate scientific and practical solution is required for the development of specifications and the further standardization of educational informatization technologies, since, without the normative-technical regulation of these processes on the basis of international frameworks, it is impossible to ensure the basic criteria for the functioning of electronic learning complexes, in particular their manageability, interoperability, accessibility, and stability. At the same time, the practical implementation of electronic courses in the real educational process is constrained by an unsatisfactory level of digital and security competencies among academic staff, as well as by the poor quality of methodological support for existing digital solutions. Within the training of specialists in the field of information technology and cyber defense, these systemic deficits create a critical gap between academic theory and the current technology stack of the industry. The isolation of the

educational environment from real cloud architectures, cyber-defense tools, and proactive threat-hunting systems makes it impossible to form a competitive human capital capable of creating a sovereign and secure national innovation product (Tyshchenko D. et al., 2024).

An analysis of the empirical experience of implementing EU blended-learning models shows that the realization of these educational technologies is a phased, systemically determined process whose architecture encompasses the conceptual, technological, and operational levels. At the initial, conceptual stage, goal-setting is carried out with a clear orientation toward the verification of defined learning outcomes, which involves the formation, cognitive consolidation, systematization, or descriptive refinement of knowledge, as well as monitoring the level of mastery of the relevant competencies. The next, technological stage requires an expert audit and the selection of optimal digital learning resources, whereas the operational stage focuses on functional analysis and the study of parameters of interoperability and secure interaction with the chosen software-and-hardware environment. In strategic and tactical lesson planning, there is an imperative need to take into account the incoming level of students' propaedeutic preparation, the methodological architecture of the classes (lectures, seminars, or laboratory sessions), as well as the psychological, pedagogical, and technical readiness of future specialists to perceive information arrays with the help of innovative technologies (the Network and Information Security Directive; the rules of enhanced cybersecurity in the European Union; *Analysis of the Digital Transformation of Higher Education*).

In the context of training personnel in the field of information technology and cyber defense, the technological and operational stages acquire a specific security-related content, since the selection and analysis of software resources must be based on the principles of Security by Design and on the study of the architectural vulnerabilities of real-world software. The integration of e-learning models makes it possible to intensify the processes of information perception and to significantly improve the quality of training through the introduction of active and interactive didactic forms, which is an imperative requirement of the modern higher school. The

effective implementation of most such methods depends critically on the use of high-technology computing and telecommunications equipment, including specialized cloud laboratories and virtualized cyber ranges, where future engineers and security analysts practice the skills of proactive threat hunting and the deployment of endpoint security systems.

The successful deployment of an e-learning ecosystem requires the consolidation and mobilization of a substantial volume of resources, in particular infrastructural, technical, human, and instructional-methodological ones. Although the creation of such a security-oriented educational environment is associated with a high intensity of financial, time, and intellectual expenditure, the degradation of risks is fully compensated by the high productivity of the educational process and the resilience of the competencies formed. Ultimately, investment in developing lessons involving contemporary information and communication technologies is methodologically justified and highly effective, since it eliminates the gap between academic theory and the requirements of the IT industry, forming a competitive human capital capable of ensuring the digital sovereignty and cyber resilience of the state.

The practical implementation of innovative didactic approaches is ensured through the design and integration, into the educational process of modern higher education institutions, of high-tech information-and-education environments, which are positioned as the most relevant and effective architectural form among the software tools available for educational purposes. The use of such integrated environments is highly productive both within classroom-based engineering training and in the process of the autonomous research activity of future specialists. The systemic potential of such digital platforms makes it possible to fully realize the technological capabilities of the modern computer industry, which directly optimizes the processes of cognitive assimilation of specialized material by increasing its interactivity, visual clarity, and information density. Moreover, the digitalization of didactic content provides the opportunity for comprehensive modeling and analysis of the systems under study, substantially expands the arsenal of methodological techniques for representing

scientific data, and optimizes the time resources required for presenting complex architectural concepts.

According to an analysis of EU experience, in the context of training highly qualified personnel in the field of information technology and cyber defense, the functioning of such information-and-education environments becomes a strategically important security task. Since these platforms constitute the central node for the accumulation of personal data and the university's intellectual property, their design must be based on the principles of fault tolerance, vulnerability isolation, and the Zero Trust concept. Students' autonomous information-search activity within such a secure environment allows them not only to study technology stacks in depth (cloud computing, big data analysis, DevOps) but also to simultaneously master practical cyber-hygiene skills and to study the behavioral factors of threats and endpoint-security algorithms. In this way, the modernized educational environment becomes not merely an instrument for the visualization of material but a simulation ground for developing forward-looking competencies in the design of an architecturally resilient and sovereign national innovation product capable of withstanding persistent hacker attacks and internal destructive influences (Moroz V. et al., 2025; Shestak Ya. et al., 2025; Pashkovsky V.F., 2025).

The implementation of intelligent models and invariants for managing the didactic process creates a synergetic foundation for designing an adaptive and architecturally resilient educational space. In the context of European standards for the modernization of the higher school, this ensures a transition toward flexible personalization (adaptive learning) and a clear structural differentiation of professional training. This approach makes it possible to optimize students' educational trajectories in accordance with the requirements of the dynamic European labor market. Proactive stochastic analysis of current academic performance grants students the ability to dynamically validate their individual pace and trajectory of mastering scientific content, as well as to decompose praxeological tasks according to levels of cognitive complexity and systemic destructiveness. In conjunction with this, the total digitalization of assessment procedures and the automation of predictive monitoring of

professional-competency formation ensure the maximum objectivity of control-and-verification measures, minimizing anthropogenic subjective factors and exponentially strengthening the internal motivational component of learning. The institutionalization of the autonomous cognitive mastery of the theoretical-methodological landscape acts as a key catalyst for the capitalization of intellectual potential and the development of the critical, divergent thinking of the future expert. A specially structured heterogeneous information environment, built on the principles of multifunctionality, determines the optimal organizational and methodological conditions for professional self-determination, systemic self-actualization, and the acmeological realization of the individual under conditions of the digital transformation of society (the Network and Information Security Directive; the rules of enhanced cybersecurity in the European Union; *Analysis of the Digital Transformation of Higher Education*).

In the narrow discourse of the advanced training of highly qualified human capital in the field of information technology and cyber defense, these processes of intellectualization, automation, and orchestration acquire imperative strategic significance. The adaptive diversification of individual educational trajectories allows students to pursue in-depth specialization in high-tech and knowledge-intensive segments, in particular in the field of secure software architecture development (DevSecOps), the methodology of proactive threat hunting, and the administration of layered endpoint-security systems. At the same time, the intelligent automation of knowledge and practical-skills verification is implemented through simulation scenarios based on cloud-oriented virtualized cyber ranges. The objectivity and validity of assessment in such environments is based on empirical time-based and qualitative metrics for reflecting coordinated APT attacks, in particular on recording indicators of mean time to detect (compromise) and mean time to respond to an incident. The systematic autonomous work of students in such a high-intensity and architecturally secure environment cultivates a stable paradigm of continuous professional development (lifelong learning), which is a fundamental criterion for the viability of the contemporary IT engineer or security architect under conditions of persistent and

polymorphic cyber threats and the risks of degradation of critical information infrastructure.

The dynamic and persistent development of information technology architecture acts as a key determining factor in the transformation of contemporary society. The objective process of global societal informatization exerts an imperative influence on the goal-setting, structure, and content of didactic systems, placing forward-looking demands on the professional training of personnel in the field of the operation and design of computing equipment. Under these conditions, the fundamental criterion of the professional fitness of an academic staff member, regardless of their disciplinary profile, becomes a high level of digital competence, a developed information culture, the ability to effectively orchestrate diverse software products in order to achieve defined learning outcomes, and a deep understanding of the functional, engineering, and didactic capabilities of IT infrastructure. The lecturer's principal strategic function within the modernized educational space is shifting from the reproductive transmission of knowledge to facilitating the comprehensive development of the future specialist and their proactive personal and acmeological formation (the Network and Information Security Directive).

The exponential acceleration of the digital transformation of the European higher education area is driven by the synergetic influence of a set of interrelated internal and external factors. According to analytical reports of the European Commission, this process is stimulated both by internal institutional needs of universities (endogenous factors) and by the global demands of the European labor market and the technological challenges of the EU Digital Decade (exogenous factors). First, there is a marked increase in the complexity of the architecture of the pedagogical process under conditions of interdisciplinary convergence of specialized subjects, which requires the deployment of flexible dual-learning models and the strategic synergy of higher education institutions with leading IT corporations, research institutions, and specialized cyber-incident response centers. Second, there is a permanent expansion of the subject-matter and cognitive world of the student, accompanied by an avalanche-like increase in the volume of scientific and technical information, which actualizes the

need to apply intelligent tools for its aggregation, selection, and synthesis. Third, the diversification of future specialists' professional activity areas delegates to the education system the task of forming robust skills for solving polymorphic problems, in particular design-engineering, research, and technological ones. Finally, a significant driver is the intensive diffusion into the didactic space of advanced technologies based on cutting-edge computing tools and secure telecommunications protocols (the rules of enhanced cybersecurity in the European Union; *Analysis of the Digital Transformation of Higher Education*; Network Detection and Response; *All About Access Control*; UEBA).

In the context of training highly qualified human capital in the field of information technology and cyber defense, these factors acquire critical security significance. The modernized digital culture of the educator must necessarily include developed cyber-hygiene skills and an understanding of the Security by Design concept, in order to design learning trajectories that take into account the contemporary threat landscape. Close integration between HEIs and leading IT companies makes it possible to involve leading security architects in creating practice-oriented cases for repelling targeted hacker attacks (APT groups) and analyzing malicious software (ransomware). At the same time, the expansion of the volume of educational material and the increasing complexity of professional tasks requires the use of specialized virtualized cyber ranges, cloud laboratories, and automated knowledge-monitoring tools based on real technical metrics. Thus, the incorporation of advanced computing tools and endpoint-security systems into the educational process ensures the transformation of the classical educational environment into a secure corporate ecosystem capable of training competitive engineers and analysts ready to guarantee the digital sovereignty and cyber resilience of the state.

Summarizing the above, the implementation of information technologies in the educational process should be regarded as a natural determinant and a relevant response to the transformational shifts in the system of higher professional education, oriented toward optimizing and intellectualizing the management of students' cognitive activity. The systematic fulfillment of the outlined infrastructural and didactic

conditions directly catalyzes the achievement of the strategic goal of education modernization, which lies in the verified improvement of the quality of learning, the assurance of inclusive access to knowledge, and the satisfaction of the needs for the harmonious acmeological development both of the individual and of the information society as a whole. At the present stage of scientific and practical discourse, there is an imperative need for a deep understanding and expert assessment of the potential of digital tools for the comprehensive capitalization of students' personal potential, as well as for identifying methodological patterns for their most organic integration into the architecture of the educational process. At the same time, the problem of determining the functional role of contemporary information technologies in the processes of improving and structurally reconfiguring traditional educational systems has remained persistently relevant over recent decades. The successful implementation of state and institutional digital-modernization programs requires not only advanced material and technical equipment for universities but also the advanced training of academic staff and administrative personnel.

Within the European academic space, digital technologies are regarded as a powerful instrument for professional development, self-realization, and the building of an equitable, inclusive partnership with the student community. In accordance with the European DigCompEdu framework, mastery of these tools is an integral part of the lecturer's professional imperative. The use of modern IT enables lecturers to ensure high standards of quality in higher education, transforming classical teaching into a flexible and human-centered process. This directly stimulates the growth of pedagogical authority, transforms functional literacy, and substantially raises the overall level of the lecturer's professional culture, expanding opportunities for scaling and disseminating innovative experience and one's own scientific and methodological views. This vector of development ensures a barrier-free transition of the academic staff member from the reproductive role of transmitter of knowledge to the proactive position of teacher-tutor (facilitator), who organizes, models, and guides the autonomous cognitive activity of students. Ultimately, information technologies play a fundamental role in the development and evolution of teaching methodology, since

the practical activity and innovative pursuits of each individual educator have significant heuristic value for the development of methodological and pedagogical science as a whole. In the context of training highly qualified personnel in the field of information technology and cyber defense, these processes acquire critically important security and industrial significance. Optimizing the management of students' cognitive activity in this domain requires a transition from classical lessons to work within architecturally secure corporate ecosystems that function according to the principles of Security by Design and the Zero Trust Architecture concept. The transformation of the lecturer into the role of tutor and facilitator makes it possible to effectively guide students in choosing individual educational trajectories within such knowledge-intensive niches as secure software development (DevSecOps), proactive threat hunting, and the administration of endpoint-security systems. At the same time, the professional culture and digital literacy of the educator themselves must be based on impeccable cyber hygiene, the ability to model threat landscapes, and the use of cloud-oriented virtualized cyber ranges to automate knowledge assessment on the basis of real technical metrics for repelling hacker attacks. Such high-tech interaction between the mentor-lecturer and the student-researcher ensures the continuity of learning (lifelong learning), eliminates the gap between academic theory and the demands of the IT industry, and forms a resilient human capital capable of guaranteeing the digital sovereignty and cyber resilience of the state in the face of coordinated attacks. In the context of a systemic analysis of higher education quality management, its essential nature is extrapolated into the domain of situational management, whose fundamental basis is determined by processes of multivariate modeling of alternative management decisions and the optimization of tasks of current and strategic planning for the development of didactic systems. Drawing on the current legal and regulatory framework governing the higher education system, it can be stated that the adoption of any management decision in the educational space must imperatively be based on forward-looking methodological developments from both domestic and international scholarly discourse, with obligatory consideration of the unique architectural, ethnocultural, and structural-functional characteristics of national educational

ecosystems. Analyzing European experience, it can be said that no state is capable of ensuring constant progress or maintaining high standards of academic training solely by preserving the existing institutional status quo. The current stage of development actualizes the need for a fundamental rethinking of traditional approaches, the deconstruction of orthodox concepts, and the overcoming of systemic complacency (inertia), which has long dominated the higher-education sector.

The implementation of this strategy demonstrates that no actor in educational activity - regardless of its status as a classical university or a private provider of educational services - is capable of effectively scaling quality indicators until every stakeholder, including academic staff and researchers, internalizes personal, genuine responsibility for shaping a positive educational experience for students and for verifying final learning outcomes. A formal understanding of this responsibility solely at the level of senior administration (rectors, vice-chancellors, or quality managers) is destructive and insufficient to achieve an emergent effect. Moreover, no external quality-assurance body or regulator will be able to sustain the viability of the system by relying exclusively on passive compliance or retrospective audit and assessment of formal processes. The strategic task of the present day is to move toward measuring real, praxeological learning outcomes, even those that appear highly problematic and, at first glance, seem unattainable in terms of forming a general academic consensus.

In the focus of training highly qualified human capital in the field of information technology and cyber defense, the situational character of quality management acquires particular acuteness owing to the high dynamics of technology-stack renewal and the persistent shifting of the cyber-threat landscape. The modeling of management-decision options in this sphere must take into account the concept of Security by Design, whereby the quality of education is determined not by the number of paper reports but by the architectural resilience and sovereignty of the digital products developed by students. Every IT-department lecturer must bear direct responsibility for the relevance of didactic content, integrating into curricula advanced industrial practices of secure development (DevSecOps), proactive threat hunting, and endpoint-security protection. At the same time, regulatory bodies and university internal quality-

assurance systems must move away from the formal checking of syllabi in favor of objectively measuring students' practical skills on the basis of cloud-oriented virtualized cyber ranges. Only recorded technical metrics - such as the mean time to detect anomalies and the speed of disaster recovery under conditions of a simulated APT attack - can serve as a valid criterion of higher-education quality, one that eliminates the gap between academic theory and the real requirements for ensuring the state's cyber resilience.

The institutionalization and establishment of regulatory bodies based on standards with a dual level of responsibility for normative regulation and quality auditing of higher education constitutes a systemically disruptive event within the overall academic landscape of many states. Within this methodology, such a disruptive incident is defined as a purposeful action that in some way interrupts the constant continuity and inertia of the system, while simultaneously acting as a constructive and healthy element in shaping state security and education policy. A direct consequence of such a determined disruption of institutional homeostasis is deep reflection, forced modernization, and the operational-crisis mobilization of all stakeholders in the educational process. Any educational organization characterized by high parameters of stability, dynamism, and adaptive responsiveness to external stimuli is capable of thriving effectively under such a regulatory challenge, promptly identifying and implementing new strategic directions for continuous improvement and the diffusion of innovation. In itself, an artificially created disruptive situation is not an exhaustive equivalent of effective state policy, yet it is capable of challenging conservative academic orthodoxy, neutralizing destructive levels of complacency and psychological comfort, and serving as a trigger for developing and optimizing new regulatory practices. Accordingly, the controlled disruption of stasis in the educational landscape can and should be transformed into a direct outcome of the implementation of innovative thinking within state management, reflecting the government's fundamental commitment to the permanent modernization of state education policy. In the narrow discourse of training highly qualified personnel in the field of information technology and cyber defense, the concept of disruptive management acquires critically important

applied significance, since the contemporary landscape of cyberattacks functions exclusively as a persistent disruptive event. The advanced training of IT specialists under the current conditions of hybrid confrontation is impossible without the artificial modeling of stressful and destructive situations within the educational process itself. The design of educational trajectories must be based on the principle of readiness of systems and personnel for continuous disruption of stability, whereby architects and analysts are trained within the paradigm of Design for Failure and Zero Trust architecture (Mahmood S. et al., 2024; Swire P. et al., 2024; Dede G. et al., 2024; Shnaoli Chakraborty A., 2026; Gangmei N. et al., 2022; Chugh R., 2023).

In this sense, the introduction of new regulatory standards is pushing universities to abandon outdated static programs and is stimulating the creation of flexible learning models integrated with advanced practices of secure development (DevSecOps), proactive hidden-threat hunting, and endpoint-security protection. Genuine innovation in state education policy must be expressed in a transition from passive paper-based compliance to the active testing of HEI resilience. This entails the introduction of automated systems for assessing students' knowledge and lecturers' professional capacity on virtualized cyber ranges, using empirical technical metrics - the time to detect anomalies and the speed of service recovery after incidents (disaster recovery). Thus, the disruptive impulse of state regulation transforms the academic environment from a passive consumer of technology into a dynamic, secure corporate ecosystem capable of generating competitive human capital and ensuring the state's digital sovereignty under conditions of constant cyber threats.

Within the scope of this study, taking into account the standards of the European Higher Education Area (EHEA), critical components of the educational environment requiring conceptual rethinking and modernization have been identified. Orientation toward European benchmarks for university development has made it possible to clearly outline those vectors of the internal ecosystem of HEIs whose reform is a priority for achieving compliance with contemporary criteria of quality and flexibility of learning (Tyshchenko D. et al., 2024; Bidzilya Yu. M., 2025; Tarasovsky Yu., 2026):

- relevance of educational architectures and information resilience. The system-forming destructive factor that undermines the quality of personnel training is the low rate of renewal of educational content. Some state institutions continue to reproduce outdated didactic materials that fail to take into account the current cyberattack landscape and the architecture of modern information systems. In order to ensure national security and form relevant skills for countering cyber threats, higher education institutions must introduce mechanisms for the regular monitoring and proactive updating of syllabi in accordance with the standards of the cyber-defense industry;

- technological integration and digital security of infrastructure. Innovative technologies form the core of a sovereign digital infrastructure and determine the vector of the state's strategic development. At present, there is a cognitive gap between the theoretical base of textbooks and real technological trends, as a result of which students are deprived of practical experience working with secure cloud computing, vulnerability-detection systems, and cryptographic protection tools. Universities must act as drivers of technology transfer, creating secure virtual laboratories and encouraging the effective, safe, and pragmatic mastery by students of advanced software-and-hardware tools;

- cross-border academic mobility and the protection of information exchange. International academic exchange programs constitute a promising and dynamic sector of the educational infrastructure, substantially optimizing both research potential and the sociocultural adaptation of future specialists. Expanding the network of international partnerships and involving students in studying foreign experience requires higher education institutions to establish secure communication channels and to protect the confidential data of participants in mobility programs during the cross-border transfer of information in the global cyberspace;

- digital inclusiveness of education and the security of distance-learning platforms. Key barriers to the full engagement of young people in the educational process are the deficit of regional infrastructure in rural areas and the forced economic activity of students. The optimal tool for overcoming this gap and ensuring equal

access to knowledge is the development and scaling of distance-learning systems. The digitalization of remote education must be accompanied by the deployment of secure web resources, the use of user-authentication technologies, and counteraction to cyberattacks on the electronic databases of educational institutions, which guarantees the stability, continuity, and security of the educational process across the entire state;

- interactive verification of knowledge and the development of analytical potential in the cyber domain. Traditional forms of learning oriented toward rote memorization and textual reproduction during assessment do not ensure graduates' readiness to counter contemporary threats in cyberspace. Genuine engineering and analytical expertise is formed through students' involvement in discussion panels, team projects for developing information-protection systems, and practical simulations such as Capture the Flag (CTF) competitions. The introduction of such innovative methodologies stimulates the development of students' heuristic thinking and their ability to conduct a comprehensive analysis of the vulnerabilities of complex information systems;

- financial optimization and the development of a secure material and technical base. Strategically ensuring high quality of education is a key factor in the state's national security. At present, a constraining factor for many institutions is the unsatisfactory condition or absence of functioning specialized computer laboratories and a shortage of licensed software for network-security monitoring. The state must diversify and increase targeted funding for educational institutions in order to procure high-tech equipment, deploy secure local networks, and create infrastructure that meets contemporary international standards of cyber defense;

- verification of digital competence and updating the knowledge of teaching staff. The current staffing landscape of universities, represented both by contract employees and by lecturers with long tenure, shows a tendency toward insufficient renewal of educational material, which is unacceptable given the rapid evolution of cyber threats. Since academic staff directly transmit professional patterns to future specialists, there is a need for their thorough mastery of advanced security tools and IT-industry standards. Achieving this goal is made possible through the

implementation of systems of periodic assessment, qualification audits, and mandatory internships for lecturers at specialized cyber centers;

- activation of research potential and the development of innovations in the field of cybersecurity. Fundamental and applied research not only stimulates the development of students' heuristic and analytical thinking but also serves as a driving force for raising the university's international standing and strengthening the state's defense potential in cyberspace. Behavioral absenteeism and the low engagement of today's youth in scientific work require systemic disruption. Higher education institutions must transform into drivers of scientific inquiry, creating student R&D laboratories for research into artificial intelligence, cloud-environment security, and counteracting social engineering, which will make it possible to generate innovative patents and raise the overall level of protection of national infrastructure;

- optimizing the numerical ratio of participants in the educational process and cyber hygiene of the environment. The current tendency toward the hyper-concentration of student numbers in lecture halls significantly reduces the efficiency of teaching activity, making it impossible to conduct personalized monitoring of knowledge acquisition and identity verification of students. In order to increase the effectiveness of didactic control and to ensure an adequate level of information security during classes, there is a need to normatively reduce the maximum size of academic groups, which will make it possible to implement the concept of personalized support;

- formation of secure digital learning environments and the security of educational platforms. Notwithstanding the traditional effectiveness of offline interaction, higher education institutions must proactively increase the share of digitalized classes. The deployment of virtual classrooms using secure repositories for storing video lectures and interactive feedback tools makes possible continuous and secure communication around the clock. The application of cloud technologies with encrypted communication channels provides students with secure access to global information resources, while the implementation of automated testing systems guarantees the validity and immediate verification of knowledge-assessment results, laying the groundwork for the universities' future technological development.

An analysis of European practices in building contemporary universities has made it possible to identify, within the scope of this study, the basic parameters of the educational environment requiring systemic optimization and conceptual change. Taking into account EU experience in implementing "smart" and inclusive campuses, the key areas of educational infrastructure and methodology subject to transformation for improving overall learning effectiveness have been identified.

The heads of contemporary educational institutions bear a broad range of strategic and operational responsibilities that extend far beyond the direct regulation of didactic and scientific-methodological processes. The systemic management of a higher education institution requires the continuous orchestration of human resources, the rational allocation of financial resources, as well as the design, modernization, and protection of both the material-technical and the heterogeneous digital environment. This process is persistently accompanied by the need for strict compliance with rigorous regulatory, financial-compliance, and legal requirements, which forces the administrative apparatus to operate under conditions of high intensity in resolving complex logistical, material-technical, and bureaucratic tasks. In view of this, in the professional discourse of top management in the education sector, the dominant priority is defined as ensuring institutional resilience, that is, the unconditional guarantee of the continuity of the organization's operational functioning and the stable provision of educational services under any external conditions.

In light of the implementation of the European NIS2 Directive and the tightening of cyber-resilience requirements, the rapid evolution of cyber threats compels universities to continuously modernize their material-technical and methodological base. In accordance with the European course toward cloud sovereignty, the training of a new generation of specialists must focus on the architecture of geographically distributed systems, cloud computing, and edge-computing technologies. It is precisely this technological foundation that today dominates the deployment of innovative platforms and cyber ranges in EU countries (the EU NIS2 Directive). In the context of training highly qualified personnel in the field of information technology and cyber defense, the task of ensuring the viability of the educational institution acquires a

specific security-related and infrastructural content. For the contemporary head of an HEI, the obligation to keep the institution "afloat" is transformed into a requirement to build a highly effective cyber-resilience system. Since the university's digital environment is a target for coordinated APT attacks and attempts at destructive influence on critical information infrastructure, administrative management must be based on the principles of proactive risk management. This entails not merely formal oversight of computer classrooms but the implementation of Zero Trust Architecture, endpoint-security/EDR tools, and intelligent network monitoring.

Moreover, ensuring the continuity of the educational process under force-majeure circumstances (martial law or man-made disasters) requires management to develop and validate clear strategies for the disaster recovery of digital assets and for business-process continuity. Human and material resource management within this model is integrated with the tasks of deploying cloud laboratories and virtual cyber ranges, which allows IT students to continue practical learning even in the event of losing physical control over the HEI's local infrastructure. Thus, the crisis management of the higher-school leader is transformed into a technological foundation that protects academic sovereignty and creates a reliable platform for forming the state's competitive human capital.

Drawing on the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG), the study identifies key aspects of the functioning of the university environment that require structural change. The identified directions of conceptual transformation correlate with European experience in creating a human-centered, secure, and digitalized space for all participants in the academic process (Standards and Guidelines for Quality Assurance in the European Higher Education Area, ESG).

European experience in university management shows that the effective strategic planning of education leaders is often blocked by the need to respond to reactive and situational challenges. The day-to-day activity of HEI heads is complicated by force-majeure expenditures on infrastructure restoration and modernization, a shortage of teaching space, and a deficit of academic and administrative personnel. This forces

management to balance operational crisis response against long-term development goals, a situation characteristic of many European universities during periods of transformation; moreover, the volatility of the pool of higher-education applicants acts as a destabilizing factor that reduces management effectiveness and imposes tight budgetary constraints. The integration of predictive analysis and data-driven management facilitates a transition from a reactive to a proactive model of administration, ensuring the preventive identification of potential risks. In particular, the implementation of artificial-intelligence algorithms makes it possible to optimize energy-consumption expenditure through the dynamic regulation of heating and electricity supply in accordance with actual needs and predictive machine-learning models built on retrospective data. In addition, the digitalization of management processes opens up opportunities for modernizing human-resource management and developing contingency plans for crisis situations. The automation of reporting, the optimization of resource planning, and the introduction of multifunctional analytical dashboards provide the management team with relevant information in real time, in accordance with their functional responsibilities. Contemporary higher education institutions are actively combining AI and Internet of Things (IoT) technologies to maximize operational efficiency and minimize the transaction costs caused by unforeseen situations.

In the context of integration into the European Higher Education Area, one of the most complex systemic challenges for university management is the attraction and institutional retention of highly qualified academic staff. European experience shows that, under conditions of high academic mobility and competition from the business sector, educational institutions need to move from classical administration toward flexible HR strategies that ensure comfortable logistics, competitive motivation, and talent retention within the organization. The shortage of competent personnel has a synergetic impact not only on the individual academic achievements of students but also on the institutional culture and overall viability of the institution. On the global scale, the systemic staffing crisis in the education sector has given rise to a phenomenon defined by the World Bank as a "learning crisis." Artificial-intelligence

technologies are not capable of diversifying sources of staff recruitment or of fully and relevantly replacing human resources. However, the integration of AI makes it possible to optimize monitoring and to minimize staff-turnover rates by neutralizing the destructive factors of professional burnout. It has been empirically demonstrated that educators' priority needs include the expansion of professional autonomy, an increase in the time available for direct didactic activity and methodological preparation, and a reduction of the bureaucratic burden associated with administering testing and preparing reports. Through the algorithmic personalization of individual educational trajectories to differentiate and meet students' specific needs, as well as through the automated real-time generation of analytical reporting, AI eliminates systemic factors of professional frustration. This ensures the optimization of educators' core activities and raises their level of professional self-actualization. The phenomenon of academic attrition at all levels of the educational process is determined by a complex of multifaceted factors. In this regard, a low level of academic performance often acts not as the root cause but as a consequence of destructive tendencies in students' learning activity. The timely identification and predictive analysis of dropout risks allow educational organizations to allocate limited resources in a targeted and rational manner for the implementation of preventive measures.

The analytical potential of artificial intelligence in aggregating and integrating diversified data arrays from heterogeneous sources - in particular, learning management systems (LMS), performance-tracking information systems, and attendance-monitoring systems - ensures the generation of operational triggers and predictive alerts. For higher education institutions, a decline in student numbers generates significant financial, economic, and reputational risks. The early termination of studies by students leads to direct budgetary losses due to a reduction in revenue from tuition-paying students or a decrease in the volume of per-capita state funding. At the macro level, a shortage of graduates correlates negatively with the institution's marketing attractiveness for prospective applicants, and a shift in the ratio of student numbers to teaching staff may necessitate a forced reduction of staff potential. For students themselves, an unfinished educational cycle is equivalent to a decline in labor-

market competitiveness, a reduction in future income, and the accumulation of overdue debt on educational loans. Alongside the classic triggers of attrition - financial deprivation, sociogenic crises, somatic disorders, difficulties in socio-psychological adaptation, and the intensification of cognitive load under conditions of initial separation from the nuclear family - contemporary scholarly discourse draws particular attention to latent threats. In particular, the deterioration of mental health and the psycho-emotional state of students has been recognized as a critical destabilizing factor, requiring the introduction of new systems of psychological support. Addressing the psycho-emotional and material-economic well-being of higher-education students is a priority vector of university management, given the pervasive manifestations of anxiety disorders, distress, and depressive states. This trend, determined both by an objective increase in morbidity and by the destigmatization of mental health in academic discourse, necessitates the formation of a proactive security-oriented environment. In this context, the convergence of psychological-support systems with the cyber-defense infrastructure of the educational institution acquires particular importance.

Drawing on EU experience in countering disinformation and managing digital content, artificial intelligence (in particular, machine-learning methods) is the most effective tool for realizing this convergence. European practice confirms that the automation of contextual analysis and monitoring of the information space with the help of AI makes it possible to promptly detect anomalies, structure data flows, and make accurate management decisions. The development of AI-based cybersecurity architecture in HEIs makes it possible not only to prevent unauthorized access to confidential databases and to protect students' personal information from cyber threats, but also to perform the function of intelligent socio-technical audit. The analysis of students' online behavior, search descriptors, and semantic markers on the network enables cyber-defense algorithms to verify latent suicidal intentions or risks of self-harm. This ensures the generation of automated triggers for the timely involvement of relevant academic staff and the implementation of intervention measures.

In the context of European data-protection standards (GDPR) and the requirements of the EU AI Act, the activation of participatory interaction among educational stakeholders is a priority for HEI management. The experience of EU countries shows that optimizing the tripartite cooperation among administration, local communities, and parents depends directly on the construction of a secure digital architecture. The integration of AI tools into the communication platforms of European educational institutions is carried out according to the "security by design" principle, which guarantees the confidentiality, integrity, and authenticity of information exchange and protects the ecosystem from contemporary cyber threats (the EU NIS2 Directive; International Standards and Guidelines: European Higher Education Area; ERA-UA; *Digital Education Action Plan 2021-2027*; the General Data Protection Regulation, GDPR).

The effective functioning of a verified and cyber-secure information dialogue between the educational organization and the local community optimizes feedback processes for the management apparatus. Secure systems of intelligent public-opinion monitoring allow institutional leadership to conduct the operational collection, depersonalization, and multi-aspect analysis of diversified viewpoints without the risk of leaking personal information or of unauthorized external manipulation of data. The valid data arrays obtained in this way serve as a reliable basis for predictive modeling, the development of security policies, and the strategic planning of the long-term development of the educational institution.

The evolution and systemic modernization of the information society of the EU and the world determine the vector of Ukraine's strategic development. The intensification of market relations in the digital environment necessitates continuous monitoring, comparative analysis, and the systematization of ongoing processes. The dynamism of this environment and the pervasive nature of the threat landscape necessitate predictive modeling of situations for the prompt adjustment of management strategies and the adaptation of management style to conditions of complex cyber risks, with a view to minimizing the consequences of destructive external and internal influences (the Network and Information Security Directive).

Drawing on the experience of the countries of the European Union in forming a common digital space, the systemic development of the information society in Ukraine requires a clearly determined state policy and a unified management approach. The cornerstone of this strategy, following the example of the EU Cybersecurity Strategy, is the creation of resilient infrastructure to protect critically important sectors. This makes it possible to combine technological innovation with strict standards of security and resilience against contemporary hybrid threats. This doctrine must be transformed into a legitimized strategic plan with clear legislative consolidation of the functional duties, roles, and boundaries of responsibility of key stakeholders (the commercial sector, state institutions, local self-government bodies) and civil society within a unified, secure information space (Kapiton A. et al., 2025, 2026; Tyshchenko D. et al., 2024; Franchuk T. et al., 2025).

Given that the quality-audit procedure places strict demands on the competency descriptors of the verifier - which combine inherent personal characteristics with the ability to apply expertly the knowledge and skills acquired through specialized training, practical activity, and validated auditing experience - these parameters must be built into the architecture of the designed digital system.

The development of the functional specification and algorithmic support for automated security-audit systems must be based on European practice in certifying cybersecurity specialists. The algorithms of the system must verify the auditor's profile against a set of professional criteria that correlate with harmonized EU standards, namely:

- multidisciplinary cognitive flexibility: possession of a broad scientific and practical outlook in the field of information security and related disciplines;
- psycho-emotional resistance and volitional stability: the ability to maintain objectivity, composure, and consistency of action under conditions of high stress load and destructive external influences;
- a high level of analytical-synthetic and logical thinking: the ability to conduct a systemic analysis of anomalies, identify hidden correlations, and predictively identify cyber risks;

- expert situational awareness and systemic vision: the ability to make a relevant derivative assessment of the security landscape, to decompose complex processes within the overall cyber-defense strategy, and to understand the functional role and architecture of individual structural units within the organization's overall information-security framework.

It should be taken into account that the professional profile of an auditor in the field of cybersecurity and information protection is determined by the presence of verified knowledge and practical skills in the following conceptual domains:

- the methodological basis of auditing: fundamental principles, standardized procedures, and verified methods for conducting security and systemic audits;
- the architecture of information-security management systems (ISMS): the structure of management systems, reference models, and normative-technical documentation regulating cyber-defense processes;
- the specific operation of the audited object: operational-technological features of activity, the topology of the information infrastructure, and the organization's business processes;
- compliance control and legal support: legal and regulatory acts, specialized legislation in the field of personal-data protection and cybersecurity, as well as contractual obligations and regulatory requirements;
- sector-specific cyber-defense descriptors: specialized knowledge in the field of security engineering specific to a particular market segment or critical infrastructure;
- predictive risk management: principles, mathematical methods, and technical tools for identifying, assessing, minimizing, and monitoring information and cyber risks.

Relevant normative standards regulate the architectural requirements and methodological descriptors for their practical implementation with respect to the following structural processes of an integrated information quality-management system (IIQMS):

Product life-cycle processes (a cluster of basic operational processes):

- determination and specification of technical and security requirements for the final product and related services;
- design and development of products and services based on the concept of a secure software development life cycle (Secure SDLC), taking cyber defense into account at the creation stage;
- end-to-end administration and monitoring of the circuit of interrelated processes within a secure information environment;
- direct production of goods and provision of services under conditions of continuous verification of the integrity of technological data;
- multi-aspect verification, validation, and security audit of product release and service operations;
- management of, and operational response to, deviations and results of processes that demonstrate non-conformity with determined parameters and cybersecurity standards.

Resource management (a cluster of processes for the provision, optimization, and protection of resource potential in accordance with European standards of institutional resilience):

- determination, engagement, and reliability monitoring of human resources, taking into account personnel-security requirements;
- identification, design, and assurance of the resilience of hardware-and-software infrastructure and cyber-defense tools;
- modeling, deployment, and maintenance of a secure environment for the uninterrupted functioning of operational processes;
- allocation and protection of technical resources for the monitoring, measurement, and audit of the quality of processes, products, and services;
- the structuring, storage, and provision of authorized access to intellectual knowledge in order to ensure the compliance of information assets with cybersecurity norms;

- verification and enhancement of the required competence of staff in the field of information protection;
- ensuring the permanent awareness of staff in the domain of cyber hygiene and a culture of quality;
- the generation, regular updating, and cryptographic protection of documented information against unauthorized modification.

Strategic responsibility of the leadership (a cluster of processes for institutional and security management based on human-centered practices and EU corporate standards):

- delimitation of the scope of practical application of the IQMS and definition of the boundaries of the cyber-defense perimeter of the information circuit;
- identification of the IQMS's business processes and regulation of access policies to documented information in order to ensure their stability;
- the assignment of functions, the delegation of authority, and the personification of top management's responsibility for the system's effectiveness and the organization's state of cyber resilience;
- the development, legitimization, and implementation of a comprehensive Quality and Information Security Policy;
- the functional distribution of duties, powers, and responsibility matrices among staff;
- predictive planning of actions, assessment, and proactive neutralization of cyber risks and potential threats;
- the determination of quality and security targets and the development of roadmaps for their achievement;
- strategic planning of architectural changes to the IQMS, taking into account the dynamics of external and internal threat-landscape factors;
- the regulation of protocols and channels for secure internal and external information exchange;
- long-term planning and administration of processes at all stages of the secure life cycle of products and services.

Metrology, analysis, and optimization (a cluster of processes for information-analytical support, cyber audit, and institutional development):

- the identification, continuous monitoring, and comparative analysis of destabilizing factors in the organization's macro- and micro-environment;
- the determination and analytical assessment of the needs, expectations, and compliance requirements of key stakeholders;
- the monitoring, measurement, multi-aspect analysis, and verification of operational-activity results;
- the conduct of regular internal and external security audits of quality and cyber defense;
- a comprehensive review-analysis of the IQMS's operational effectiveness by senior management;
- the identification of potential areas of growth and the formation of innovative opportunities for improving system performance;
- the elimination of identified deviations and non-conformities and the implementation of corrective and preventive measures;
- the permanent evolutionary optimization and enhancement of the cyber resilience of all functional subsystems of the organization.

An analysis of European experience in regulating the digital educational space shows that, within the institutional requirements for an IQMS, the operational circuit for administering ERP systems remains denotatively unexplicated. In this connection, in order to systematically identify risks and verify information security in accordance with EU directives, it is justified to use the following adapted system of concepts:

- proactive quality and cybersecurity planning: a set of predictive actions for establishing quality targets and designing the secure architectural processes and resources needed to achieve these determinants;
- preventive assurance of quality and cyber resilience: systemic actions aimed at forming verified confidence that the regulated requirements for quality and the criteria for the security of information arrays will be fully differentiated and fulfilled;

- operational quality control and security monitoring: regulatory actions and instrumental methods directly aimed at fulfilling quality requirements, compliance control, and protecting the ERP circuit from destructive cyber influences;
- evolutionary quality improvement and cyber-defense modernization: permanent measures aimed at intensifying the system's capacity to fulfill and scale quality requirements, as well as at raising the overall level of resistance of the digital ecosystem to dynamic threat landscapes.

A study of the architecture and operational structure of ERP-system administration on the basis of the APQC classifier makes it possible to synchronize management processes with international standards. Given the European vector of information-security development, adapting this framework to guarantee the cyber defense of the institutional environment involves decomposing it into the following complex of operational domains:

Modeling and determination of quality and cybersecurity requirements:

- identification of parameters and metrics critical for ensuring data quality and security;
- development and implementation of preventive and prophylactic measures for ensuring the cyber resilience of the information circuit;
- verification of the compliance of the formed plan with security-compliance criteria;
- audit and assessment of the system's potential capabilities for ensuring compliance with regulated requirements;
- finalization, validation, and approval of a comprehensive data-quality and data-protection plan.

Expert assessment and verification of compliance:

- instrumental control and audit of process compliance with the approved security and quality plan;
- multi-aspect analysis and evaluation of the results of stress testing, trials, and technical monitoring of the system.

An analysis of European experience has been taken into account in implementing incident management and non-conformity resolution:

- assessment of the potential destructive impact of identified deviations, anomalies, or cyber incidents on the organization's business processes;
- the development and immediate implementation of tactical measures to contain the threat and minimize its consequences;
- causal analysis and identification of the root causes of non-conformities or vulnerabilities;
- the elimination of defects, the remediation of vulnerabilities, and the implementation of long-term preventive security measures;
- the verification of results and the final closure of the incident (non-conformity) record.

Integration, maintenance, and evolution of the enterprise's cyber-secure ERP-system architecture:

- forming a strategy for the intelligent management and protection of the enterprise's information assets;
- the planning, architectural design, and deployment of specialized software and cyber-defense tools for the ERP circuit (with a clear definition of the scope of action, target benchmarks, and objectives);
- delimiting key processes, assigning administrative actors (governing bodies), and defining the system's KPIs;
- the development, standardization, and legitimization of regulations, security policies, operating procedures, and management indicators for the ERP circuit;
- the regular monitoring and assessment of the system's overall performance, resilience, and security;
- the formation of a secure operational environment and the development of staff's professional competencies in the field of cyber hygiene, with a view to the permanent modernization of the management system.

The standard in question presents a formalized textual description of the ERP-system management process, adapted to European standardization and technology requirements, structured according to the following key parameters:

- purpose (objective): ensuring the relevance of products, services, and the management process itself to the organization's strategic and project goals, and determining a high level of customer satisfaction;

output artifacts (results): verification and realization of organizational goals, management policies, and procedures; substantiation of criteria and methodology for quality assessment; allocation of resources and relevant information to support the functioning and monitoring of quality-assurance measures; aggregation and implementation of quality-assessment results; the continuous optimization of ERP-system management policies and procedures on the basis of retrospective project and organizational indicators; functional tasks and operations: strategic and operational planning, monitoring assessment, and the implementation of corrective and preventive measures within the ERP-system management circuit.

In addition to the parameters noted above, the standard also regulates the working artifacts (input and output data) of the quality-management assessment process. On the basis of the resulting information base, an original model of the "ERP-System Management" process is proposed. At the same time, the normative provisions of the standard state that improvement activity varies in scale and intensity - from continuous local improvements to strategic transformations at the level of the entire organization. Given this specificity, the "Quality Improvement" stage within the developed model is determined through the lens of the functional operation "Non-Conformity Resolution" within the structure of the "ERP-System Management" process, and is also singled out as an independent operation, "Improvement Initiation," within the IQMS process group "Measurement, Analysis, and Improvement."

Within the operational component "Quality Control" of the developed model, the assessment of performance and the determination of the IQMS's maturity level are implemented through the mechanisms of internal audit and self-assessment, respectively. Internal audit, as an imperative regulatory requirement of the standard,

constitutes a systematic, independent, and documented process of verifying and objectively evaluating audit evidence for its relevance to established criteria. On the basis of audit findings, a comparative analysis and assessment of the IQMS's compliance is carried out with respect to: the organization's own (endogenous) requirements for the system's functioning; the regulatory provisions of the international standard ISO 9001; and the determined criteria for its effective implementation and subsequent maintenance.

Beyond confirming compliance, the functional purpose of internal audits consists in:

- identifying best practices for their further diffusion and scaling to other areas of the enterprise's activity;
- identifying latent opportunities for the continuous improvement of processes.

The methodological toolkit for accumulating audit evidence includes:

- surveys (interviews, as well as the use of checklists and structured questionnaires);
- systematic analysis of regulatory and operational documentation;
- empirical observation of the course of processes and production activity.

To formalize and descriptively model the relationships between objects and processes within the quality-audit circuit, the use of a semantic network is justified. The implementation of the quality-audit process presupposes that auditors comply with regulated competency criteria that integrate determined personal characteristics with the ability to effectively apply theoretical knowledge and practical skills acquired during academic training, professional activity, specialized preparation, and direct expert practice. The regulated requirements for the personal characteristics of an auditor include: a broad worldview, emotional stability (composure), purposefulness, and developed logical thinking and analytical abilities. The professional profile of the specialist presupposes the ability to objectively assess situational context, to perceive complex processes systemically through the lens of the organization's strategic benchmarks, and to understand the structural-functional relationships between its

subdivisions. The competency base of the auditor's professional knowledge and practical skills must integrate the following determinants: the methodological principles, regulations, and toolkit for conducting audits; the architecture and specifics of interpreting management-system standards and related normative-reference documentation; the organizational-functional features and context of the enterprise's activity; the legal, contractual, and other forms of regulatory support binding on the audited object; specialized expertise in the specific subject area of management; and the methodological approaches, technical techniques, and risk-management tools implemented within the overall management system.

In accordance with European standards for the auditing of information systems and the requirements of the ENISA ECSF framework, the effectiveness of implementing security procedures is directly determined by the deontological culture of specialists and by the specification of their individual psychological profile. In EU practice, where particular attention is paid to professional integrity and compliance ethics, the following imperatives are singled out within the structure of an auditor's personal qualities: ethicality - the implementation of principles of integral honesty, truthfulness, authenticity, and rational judiciousness; cognitive openness and axiological impartiality - perceptual readiness for the objective reproduction and analysis of alternative concepts or divergent points of view; diplomacy - tactfulness and adherence to the norms of business etiquette in the context of interpersonal and professional communication; observational acuity - the ability to conduct continuous proactive monitoring of the operational environment and the course of processes; receptivity - a high level of contextual awareness and the ability to cognitively model and relevantly understand situational factors; versatility - adaptive flexibility ensuring the prompt reconfiguration of activity under dynamic conditions; persistence - volitional purposefulness and a stable orientation toward achieving the teleological objectives of the audit; decisiveness - the timely adoption of validated decisions on the basis of praxeological analysis and logical synthesis; professional autonomy (independence) - the ability to fulfill functional duties independently while maintaining a constructive interface of interaction with other process actors; integrity of principle -

readiness to perform duties responsibly in accordance with professional ethical norms under conditions of potential destructive pressure, cognitive dissonance, or open confrontation; striving for self-improvement - the permanent accumulation of knowledge in the course of practical activity and orientation toward maximizing the effectiveness of the audit process; sociocultural compliance (a high standard of conduct) - a presumption of respect for the endogenous corporate culture, traditions, and values of the audited object; and the ability to collaborate - synergetic intersubjective interaction within the audit team and with the personnel of the object being assessed.

In order to intensify the development of the professional competencies of quality-audit actors, a parametric model has been substantiated and constructed in the form of an invariant IT Infrastructure Assessment Report (ITIAR), which ensures the consolidation of the normative requirements and recommendations of relevant international and national standards. Depending on the determined specifics of the subject area, this set of parameters is subject to adaptive modification, taking into account the relevant requests of stakeholders, the organization's contextual environment, and the basic qualification profile of the experts involved. The modeling of the audit life cycle, integrating the stages of pre-project preparation, direct verification, and retrospective analysis of results, is proposed for implementation on the platform of the business-modeling software environment "Business Studio." The systemic integration of data is ensured through the functional content of the repositories and directories of the specialized "IQMS" module. On the basis of the verified information array of the audit registration circuit, the algorithmic automated generation of a unified reporting form, the "Audit Results Report," is envisaged. The functional potential of the tool under study ensures the architectural realization of the developed ITIAR, which is integrated into the organization's overall designed document-management structure. The logical architecture of the data repository provides for the following determination: the nomenclature of audit parameters is imported into the attribute field "Section" of the document card, while their semantic content (actual value) is recorded in the "Comment" field. The normative-regulatory

requirements for the parameters being verified are localized in the "Comment" field of the corresponding attribute section of the object. The use of the system directory "Object Attribute Sections" optimizes the procedure of conceptual modeling, since the implementation of the single-data-entry principle, with the possibility of its further cumulative updating, guarantees the repeated automated diffusion of this information into analytical reports for various modifications of ITIAR. For the unified description of the architecture (template) of the ITIAR document, the use of standard customization tools and the generation of custom reporting forms of the "Business Studio" system is justified. The final result of implementing this algorithm is the design of the ITIAR document in a regulated format. In order to aggregate, verify, and cross-tabulate information on audits conducted and recorded in the "Business Studio" database, Object Linking and Embedding (OLE) automation technology has been implemented, creating the technological basis for the automatic generation of comprehensive summary reports in a spreadsheet environment.

In light of European trends in developing a secure educational and scientific space, the proposed "ERP-System Management" process model, in combination with the ITIAR architecture, serves as a fundamental basis for competency management. The integration of international reference security practices into this model makes it possible to create a resilient system for the long-term extension and validation of professional knowledge. This ensures that the competencies of cyber-defense actors and verified stakeholders remain adaptive and relevant to the contemporary challenges of the information society. The implementation of the "Business Studio" tool determines a transition to proactive risk management, enabling the systematic analysis and preventive neutralization of vulnerabilities, the continuous development of the expert potential of information-security auditors, and the permanent monitoring and quantification of the effectiveness of countermeasures aimed at resolving incidents and optimizing the overall circuit of the cybersecurity management system. Algorithmic guidance for developing a customized ITIAR analytical report within the "Business Studio" business-modeling architecture is available for download through the author's verified feedback interface on the author's specialized website.

The proposed process model and ITIAR architecture, which codifies the requirements of international cybersecurity and information-protection standards, provide a conceptual basis for determining and extending the professional competencies of personnel and relevant stakeholders within the enterprise's cyber-defense circuit. The use of the analytical toolkit of the "Business Studio" platform makes possible a transition to a proactive management paradigm: the regular monitoring of vulnerabilities, the preventive neutralization of cyber threats, the continuous verification of the qualification level of security auditors, and the quantification of the effectiveness of countermeasures aimed at containing incidents and optimizing the information-security management system.

In the process of developing an audit program, architectural and logical priority should be given to a set of determinants that includes: the degree of criticality of a subdivision's functional processes for ensuring the organization's overall cybersecurity circuit; a retrospective analysis and the verification status of previously identified vulnerabilities or compliance non-conformities based on the results of prior inspections; and the cumulative results of top management's strategic review and validation of the effectiveness of the ERP-system's security management circuit. An unscheduled internal cyber-defense audit is initiated when it is necessary to verify readiness for certification compliance, or when triggers defined by the institution's leadership in administrative documents call for the urgent assessment of infrastructure security. In this case, the planning procedure must implement a continuous audit of every process within the area of responsibility of the structural subdivision integrated into the overall ERP security ecosystem.

Guided by European approaches to the security of audit procedures, during the preparatory stage a verified group of experts develops questionnaires and accompanying documentation on the basis of a legitimate technical assignment. In order to comply with the strict information-security protocols adopted in EU countries, access to these working files is isolated within the audit circuit. This preventive measure makes it possible to neutralize the threats of unauthorized access and guarantees the impartiality and confidentiality of the entire inspection process. Among

the basic criteria for the internal audit of a department, in the context of assessing its cyber resilience and the security of its information assets, is the verification of infrastructural provision, encompassing the audit of the material and technical base, in particular specialized classrooms, computer laboratories, and personal computers involved in the educational process and requiring network-security control. Alongside this, the content component and documentary support are subject to assessment, namely, the availability and completeness of course syllabi, methodological support for coursework and final-qualification assessment, sets of comprehensive assessment tasks, information on internship placements, and records of educational literature and specialized periodicals, which are regarded as information resources of the department. Particular attention is paid to the protection and analysis of research-activity data, including its funding, the architecture of task distribution, the parameters of scientific schools, staffing, publication activity, exhibition activity, and intellectual property. Within the unified information space, the following are analyzed: the monitoring of graduate adaptation, the parameters of international cooperation and the training of foreign specialists, the effectiveness of postgraduate studies, the publication activity of academic staff, forms of knowledge-quality control, and the integration of the department's staff into the overall security architecture of the institution's ERP system.

The architectural components of an integrated system for monitoring the quality of the educational process within the cyber-defense circuit consist of sequentially interconnected procedures, beginning with the permanent monitoring and diagnostics of the state of security of the information environment. The next stage is the determination of regulatory standards and the establishment of baseline security profiles, on the basis of which the quantification of measurable parameters and the formalization of clear criteria for assessing the system's cyber resilience are carried out. The process concludes with an in-depth analysis of the verified data obtained and the implementation of appropriate preventive or corrective countermeasures, accompanied by the verification of their effectiveness in accordance with current security regulations and management functions oriented toward optimizing secure

information provision and enhancing the overall effectiveness of managing the institution's IT infrastructure.

The empirical results of comprehensive monitoring serve as a fundamental determinant in the process of ensuring the quality of educational activity, since they provide management bodies with valid information on the relevant state of the educational system and its structural elements. This toolkit makes it possible to verify destructive anomalies and latent problems arising at the stage of achieving strategic goals, as well as to forecast general industry-development trends for the further design of effective public-management policy. In this context, monitoring the quality of education is transformed into a basic, cyber-secure instrument for administering its ERP system, one that guarantees the authenticity, integrity, and resilience of analytical data arrays against external and internal destabilizing cyber influences. The university's quality-assurance doctrine, synchronized with the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG), is implemented end-to-end across all vectors of the HEI's institutional activity. It is oriented toward forming a resilient internal culture of quality, strategic coordination, and encouraging members of the academic community to make verified (data-based) decisions within the framework of the permanent modernization of the didactic process.

In the context of implementing European approaches to higher-education quality assurance, the security and education policy developed demonstrates full congruence with state standards, legitimate accreditation criteria, and legal regulators. It acts as an organic element of the HEI's overall compliance system, ensuring the interconnection between academic requirements and security standards across all functional domains of the modern digital university's operation. In formulating a quality-assurance doctrine, the management of the higher education institution has determined the following fundamental imperatives, which define the methodological principles governing the functioning and management architecture of a cyber-secure ERP system within the university environment:

- harmonization with international standards: the implementation and legal-regulatory adaptation of the basic principles of the Bologna Declaration within a unified, secure digital space;
- digital transformation of administration: the introduction of a comprehensive automated system for managing the processes of training highly qualified personnel, based on an integrated and cyber-resilient ERP circuit;
- diversification of educational derivatives: expanding the range of educational services through the introduction of innovative technologies oriented toward ensuring sustainable financial and economic development and the protection of intellectual capital;
- resource compliance control: systemic methodological, infrastructural, and staffing support for the design of new specialties, innovative fields of training, and specialized academic disciplines;
- permanent optimization of the didactic process: the modernization of teaching technologies and the introduction of intelligent tools for monitoring students' learning trajectories;
- intensification of cognitive validation: the systematic enhancement of the quality and competitiveness of student training, ensuring the integrity and confidentiality of assessment results;
- inclusiveness and accessibility of digital infrastructure: ensuring unobstructed, verified, and secure access to higher education for citizens while maintaining protocols of user identification and authentication;
- integration into the market environment: the introduction of an automated system for the predictive promotion of graduate employment and the optimization of processes of their professional adaptation to the dynamic requirements of the labor market.

To summarize the above, ensuring high quality of the educational process is a dominant imperative of contemporary socioeconomic development. This necessitates the design and implementation of cyber-secure, intelligent systems for the mass reflection of the outputs of educational institutions and their structural units. These

platforms must operate on the basis of secure tools for comprehensive monitoring, security auditing, and the validation of the cognitive potential of both academic staff and students. The integration of such innovative solutions into the circuit of ERP systems for managing educational services requires the development of a resilient cyber-defense architecture to prevent unauthorized modification and the leakage of reputational and personal data. The modernization of the institution's digital ecosystem will ensure the verified transparency of assessment, minimize the risks of cyberattacks on testing systems, and form a synergetic trigger for the permanent professional self-improvement of both individual actors and the organization's structural units as a whole.

In the context of the European benchmarks of the Digital Decade and post-industrial development, the transformation of society is accompanied by an imperative transition toward diversified models of remote and hybrid employment. European practice in regulating the labor market demonstrates that the effective functioning of such flexible formats is possible only on the basis of a resilient architecture of geographically distributed information-and-communication systems and heterogeneous cloud computing, which ensure business-process continuity and data protection. However, the large-scale decentralization and deconcentration of business processes give rise to a complex of specific structural-functional, architectural, and critical-level security vulnerabilities. In the context of a systemic analysis of security risks, the leading destructive factor is the fragmentation of the unified communication circuit, caused by the deficit of a unified, secure environment for operational monitoring and management (a Common Operational Picture), which critically undermines the effectiveness of incident management and coordination of action in crisis (entropic) situations. The dispersal and uncontrolled diffusion of project-management tools, classified as the "Shadow IT" phenomenon, not only degrades the synergetic effect of team engineering interaction but also exponentially expands the overall potential attack surface. This creates unregulated, latent channels for the leakage of confidential data and intellectual property through the compromise of unprotected peripheral endpoints. This spectrum of threats delegates to the IT higher

school the task of forcibly modernizing didactic models for training specialists. The contemporary IT engineer, cloud architect, and cybersecurity analyst must possess forward-looking, cross-functional competencies in the areas of designing systems according to Zero Trust Architecture methodology, centralized identity and access management (IAM/PAM), the orchestration of secure channels (SD-WAN/SASE), as well as auditing infrastructure to detect hidden Shadow IT components.

To neutralize and minimize these destructive (entropic) factors, European digital-transformation practice highlights the need for a paradigmatic shift from discrete application software products toward integrated next-generation digital platforms. In accordance with European requirements for technological sovereignty and interoperability, such solutions must function as architecturally secure corporate ecosystems that ensure the seamless and secure exchange of data among all process participants. The design and deployment of such environments must be determined by the imperative implementation of Security by Design principles and the conceptual provisions of Zero Trust Architecture, within which every subject, verified device, and information session is subject to continuous, context-dependent dynamic authentication and proactive verification.

Under such conditions, the cryptographic resilience of telecommunication channels, the determined delimitation of access rights on the basis of role-based and attribute-based models (RBAC/ABAC), and the integration of intelligent data-loss-prevention systems become fundamental imperatives of systems engineering. The security of the processes of data storage, transit, and heterogeneous processing is positioned not as an isolated technical requirement but as a systemic criterion of the architecture's viability, one that guarantees adherence to the classical information-security triad (confidentiality, integrity, availability - the CIA triad) and defines a high level of cyber resilience of distributed critical infrastructure under conditions of persistent coordinated attacks and insider threats.

In light of the modernization of the European Higher Education Area, the technological context presented determines a fundamental restructuring of the architecture of educational programs for IT specialties. The content of professional

training must evolve from the applied mastery of programming-language syntax toward the development of higher-order cognitive and metacognitive capacities, in particular systemic architectural thinking. It is precisely this vector that guarantees the institutional compliance of university education with the requirements of European professional standards and the long-term competitiveness of specialists. Future software engineers, cloud-solution architects, and cyber-defense experts must possess forward-looking, cross-disciplinary competencies in the mathematical modeling of security policies, cryptographic design, and automated incident management, which is the guarantee of creating a sovereign digital product resilient to external influences.

Under the determined conditions of contemporary hybrid warfare, the geopolitical space of Ukraine has become a key experimental macro-arena of intensive conventional and unconventional confrontation in the info-sphere, containing the coordinated destructive expansion of highly qualified pro-government APT groups. The polymorphic and stochastic nature of contemporary cyberattacks - ranging from high-intensity, application-layer (L7, per the OSI model) DDoS incidents to the targeted compromise of systems via ransomware and fileless malware - imperatively necessitates the institutionalization of a layered, adaptive system of national cyber defense.

Ensuring the architectural resilience and cyber resilience of critical information infrastructure objects requires not only the diffusion of innovative EDR/XDR (Endpoint/Extended Detection and Response) class technological solutions and the implementation of post-quantum cryptographic protocols, but also the forced capitalization of the human factor within the concept of human-centric security. This security imperative determines a fundamental transformation of the educational and scientific paradigm for training specialists in the field of knowledge "Information Technology." Future IT engineers, cybersecurity analysts, and systems architects must possess forward-looking, cross-functional competencies in the fields of proactive risk management, behavioral analysis, and the modeling of a resilient culture of organizational cyber hygiene as a fundamental basis for minimizing anthropogenic cyber risks.

A separate theoretical-methodological and scientific-practical discourse is required for the determination and classification of cyber threats extrapolated from the consequences of martial-law force-majeure circumstances and kinetic and man-made destruction. Minimizing and neutralizing their destructive, entropic impact on critical information infrastructure delegates to the higher IT education system the strategic function of forming a pool of highly qualified personnel possessing competencies in the architectural modeling, deployment, and dynamic reconfiguration of adaptive systems for the proactive monitoring and detection of cyberattacks.

The contemporary paradigm for training software engineers and cybersecurity architects is shifting toward the imperative mastery of the concept of layered endpoint security (Endpoint Security/EDR) and the containerized isolation of vulnerabilities across diversified remote workplaces under conditions of stochastic connectivity, the degradation of data-transmission channels, or the complete loss of physical control over the hardware perimeter of the infrastructure.

Accordingly, the modernization of higher-education standards and syllabi in the field of knowledge "Information Technology" necessitates the convergence of the theoretical base with verified practical cases of real-world experience in repelling targeted attacks. The training process must be institutionalized through the implementation of virtualized cyber-range technologies and must focus on developing skills in designing fault-tolerant systems, business-continuity algorithms, and flexible strategies for the disaster recovery of digital assets.

Under conditions of the total digitalization of societal processes and the escalation of cyber confrontation, the architecture of the resilient functioning of state and corporate institutions depends critically on the availability of secure network infrastructure and the integration of next-generation intelligent DLP systems. Such a technological imperative places fundamentally new demands on the training of specialists in information technology and software engineering. The contemporary IT specialist must possess the skills to design fault-tolerant, zero-trust systems in which cryptographic security and leak protection are integrated directly into the software-development life cycle.

The dynamic and highly technological nature of contemporary cyberattacks necessitates a fundamental transformation of the academic and research vectors in IT education at HEIs worldwide and within the EU. The training of personnel must evolve from the passive study of cyber-hygiene regulations toward an in-depth practical analysis of the mechanisms of threat realization and the study of adversaries' tactics and procedures within the framework of the threat-hunting concept. The higher school, together with the scientific community, must ensure a transition to practice-oriented learning using cloud-based cyber ranges and reverse-engineering tools, which will enable future IT analysts to develop predictive, AI-based defense algorithms.

Ensuring the constant and balanced development of knowledge-intensive and high-tech sectors of the national economy under conditions of global geopolitical transformation necessitates a fundamental reconceptualization of state policy in the info-sphere and in the field of cybersecurity. At the current stage, the dominant priority is to achieve an emergent effect from the synergetic interaction between the research and innovation hubs of higher education institutions and the industrial demands of real-sector economic actors.

In light of the European transition to the concept of "Industry 5.0" and the implementation of the EU Digital Education Action Plan, the modernization of the contemporary paradigm of higher IT education requires a decisive rejection of classical reproductive learning models. European experience demonstrates the need to implement forward-looking, human-centered, and security-oriented strategies. This approach makes it possible to train specialists capable not only of adapting to technological breakthroughs but also of designing digital systems that take into account ethical norms and the EU's strict requirements for cyber resilience. This process entails the implementation of flexible dual-education trajectories, the architectural and financial stimulation of university R&D centers, and the institutionalization of public-private partnership through the direct integration of leading IT architects, software engineers, and cyber-defense experts into the processes of developing and updating higher-school standards.

The fundamental reconfiguration of the architecture of educational and research systems must be based on the principles of Security by Design. Such an integrated approach is a key determinant in forming competitive human capital - a consolidated pool of highly qualified specialists (security engineers, zero-trust architecture developers, cyber-threat analysts). It is precisely this personnel potential that is capable of ensuring the development, scaling, and implementation of a sovereign national innovation product, architecturally resilient to destructive (entropic) external and internal cyberattacks, thereby guaranteeing the state's digital sovereignty and cyber resilience.

A mandatory institutional foundation for developing a sovereign IT sector and training highly qualified specialists is the formation of an adaptive legal and regulatory framework. This entails the introduction of stimulating economic levers, in particular tax preferences for knowledge-intensive business, the minimization of financial pressure on startup ecosystems, and targeted state grant funding for university R&D centers. This approach makes it possible to create innovation clusters based at higher education institutions, where future IT architects and cybersecurity engineers have the opportunity to work on real high-tech projects.

The task of minimizing risks to corporate data and ensuring the resilience of information-production networks requires the transformation of educational programs to include the study of network-perimeter defense in depth (Defense-in-Depth). Future specialists must master technologies for end-to-end monitoring and intelligent traffic filtering within the concept of Network Detection and Response (NDR), analyzing anomalies in both external and internal (east-west) network traffic.

In this context, particular relevance is acquired by the formation, in future specialists, of competencies in protecting and verifying specialized microservice architectures and APIs that sustain the operation of complex ERP/CRM and PLM ecosystems of modern enterprises. Given the sharp intensification of APT attacks and cyber sabotage under the current crisis conditions of hybrid war, the vector of scientific and practical research in higher IT education must be shifted toward studying the vulnerabilities of technical infrastructure components. This includes training personnel

to conduct penetration testing, source-code security analysis (SAST/DAST), and the protection of industrial ICS/SCADA systems. This is a fundamental condition for ensuring the technological resilience of the domestic industrial complex.

Contemporary experience of European universities demonstrates that predictive and generative AI has become a basic instrument for improving effectiveness for the key stakeholders of the higher school. The technological solutions being implemented in the European educational ecosystem are transforming routine practice: they adapt content to individual student needs, optimize the grading of assignments, and provide administration with reliable predictive data for the preventive response to educational crises and risks. Extrapolating digital-transformation trends allows us to assert that, over the coming decade, artificial-intelligence technologies will form the fundamental didactic and architectural basis of higher IT education. The diffusion of emergent AI tools (in particular, generative models, predictive analytics, and adaptive learning systems) is being integrated directly into the training trajectories of specialists in computer science and cybersecurity. This requires the implementation of the concept of Secure AI by Design in the educational process, since future IT engineers must not only use AI to automate development or anomaly analysis but also understand the specific threat vectors targeting AI systems themselves, such as data poisoning, attacks on machine-learning models, and the leakage of confidential information through LLM interfaces.

REFERENCES FOR SUBSECTION 3.2

1. Kapiton A., Franchuk T., Tyshchenko D., Kurbanova O. Formation of cybersecurity architecture of innovation parks in the context of digital transformation and global technical and economic challenges. Control, Navigation and Communication Systems. 2026. Vol. 2 (84), pp. 120-124.

2. Tyshchenko D., Franchuk T., Stepashkina K., Karpunin I. System design and development corporate electronic document management. European Scientific Journal of Economic and Financial Innovations. 2024. No. 1(13), pp. 200-207.

3. Franchuk T., Tyshchenko D., Desiatko A., Karpunin I. Features of accounting digitalization processes. Galician Economic Journal. 2025. Vol. 95, No. 1, pp. 61-66.

4. Tyshchenko D., Franchuk T., Zakharov R., Moskalenko V. Supporting dynamic security needs with VPN tools. Control, Navigation and Communication Systems. 2024. No. 3 (77), pp. 149-152.

5. Kapiton A., Franchuk T., Tyshchenko D., Desiatko A., Zakharov R. Requirements for modern processors for secure operation of information systems and networks. Control, Navigation and Communication Systems. 2025. No. 3 (77), pp. 111-117.

6. Kapiton A., Franchuk T., Tyshchenko D., Desiatko A. Integration of cyber defense into innovation-park infrastructure: conceptual and methodological foundations for forming a secure digital environment. Khmelnytskyi Scientific Bulletin. Technical Sciences. 2026. No. 363(2), pp. 386-390.

7. Kapiton A., Franchuk T. M., Tyshchenko D. O., Desiatko A. M., Zakharov R. G. Formation of cybersecurity architecture of innovation parks in the context of digital transformation and global technical and economic challenges. Tavriya Scientific Bulletin. Series: Technical Sciences. 2026. Issue 3, pp. 79-85.

8. Mahmood S., Chadhar M., Firmin S. Countermeasure strategies to address cybersecurity challenges amidst major crises in the higher education and research sector: An organisational learning perspective. Information. 2024. Vol. 15, No. 2, art. 106.

9. Swire P., Kennedy-Mayo D., Bagley D., Krasser S., Modak A., Bausewein C. Risks to cybersecurity from data localization, organized by techniques, tactics and procedures. Journal of Cyber Policy. 2024. Vol. 9, No. 1, pp. 20-51.

10. Dede G., Petsa A. M., Kavalaris S., Serrelis E., Evangelatos S., Oikonomidis I., Kamalakis T. Cybersecurity as a contributor toward resilient Internet of Things (IoT) infrastructure and sustainable economic growth. Information. 2024. Vol. 15, No. 12, art. 798.

11. Daisy G. Digitalization of higher education: opportunities and threats. URL:https://www.researchgate.net/publication/383057099_ digitalization _of higher_education_ Opportunities_and_Threats (accessed 28 June 2026).

12. Shnaoli Chakraborty A. Implementation of NEP 2020 in Higher Education: The Open University Example. Available at: shodhgyan.org (accessed 28 June 2026).

13. Atabik A., Nurfuadi N., Imam H., Masruri M., Nur S. Digitalization of educational quality management in higher education. URL: https: https://www.researchgate.net/publication/381388103_Digitalization_of_Educational_ Quality_Mana gement_in_Higher_Education/link/666c2323a54c5f0b9464ff02/download?_tp=eyJjb250ZXh0Ijp7Imp1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19 (accessed 28 June 2026).

14. Gangmei N., Thomas N. Use of Information and Communication Technology for Quality Education. The Barcelona Conference on Education 2022: Official Conference Proceedings. 2022. pp. 375-385.

15. Chugh R. Implementing educational technology in Higher Education Institutions: A review of technologies, stakeholder perceptions, frameworks and metrics. Education and Information Technologies. 2023. No. 28, pp. 16403-16429.

16. Yampol Y. Using information and digital technologies for improving education quality management in general secondary education institutions. Information Technologies and Learning Tools. 2024. Vol. 102, No. 4, pp. 148-162.

17. Moroz V., Tereshchenko A., Buka S., Kruhlov V., Moroz S. Information technologies in ensuring the quality of higher education: approaches, challenges and prospects. Information Technologies and Learning Tools. 2025. Vol. 107, No. 3, pp. 120-134.

18. Shestak Ya., Zavgorodnya Ye., Krasnoshchok V. Technical protection of the information infrastructure of a commercial enterprise. Development of Education, Science and Business: Results. 2025. URL: http://www.wayscience.com/wp-

content/uploads/2025/12/Conference-Proceedings-December-18-19-2025.pdf (accessed 28 June 2026).

19. Pashkovsky V.F. Identification of political and legal mechanisms of information security of the state under conditions of hybrid war. Life Is More Political. 2025. No. 3, pp. 114-120.

20. Yakovenko Y. The importance of cybersecurity in shaping the digital economy. URL:https://www.researchgate.net/publication/383193213_Znacenna_ kiberbezpeki_ u_formuvanni_cifrovoi_ekonomiki (accessed 28 June 2026).

21. Bidzilya Yu. M. State policy of information security under conditions of hybrid threats. Ukrainian Political and Legal Discourse. 2025. No. 17, pp. 30-36. URL: https://ppdnz.com.ua/index.php/home/article/view/457/356 (accessed 28 June 2026).

22. Tarasovsky Yu. Ukraine has approved the Digital Development Strategy to 2030. URL: https://forbes.ua/news/ukraina-zatverdila-strategiyu-tsifrovogo-rozvitku-nnovatsiy- do-2030-roku-shcho-vona-peredbachae-14012025-26270 (accessed 28 June 2026).

23. Plakhotnik O., Zlatnikov V., Strazhnikova I., Bidyuk N., Shkodyn A., Kuchai O. Use of information technologies for quality training of future specialists. Amazonia Investiga. 2023. Vol. 12, No. 65, pp. 49-58.

24. Directive on the Security of Networks and Information Systems. URL: https://nis2.org.ua/?gad_source=1&gad_campaignid=23017071562&gbraid=0AAAA BBThWcdW CFXVbeUIPC10mJmbhR0zl&gclid=EAIaIQobChMI1dvk4NDvlAMV_5qDBx1opjD YEAAYASA AEgLBKfD_BwE (accessed 28 June 2026).

25. Rules of Enhanced Cybersecurity in the European Union. URL: https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua (accessed 28 June 2026).

26. Analysis of the Digital Transformation of Higher Education: The Digital Leap in East Asia. URL: https://en.ichei.org/en/news/information/4033.html (accessed 28 June 2026).

27. Network Detection and Response. URL: https://oberig-it.com/statti/shho-take-network-detection-and-response/ (accessed 28 June 2026).

28. All About Access Control: Everything Covered from Definition, Types, to Features and How-Tos. URL: https://www.supremainc.com/en/hub/insights-access-control.asp (accessed 28 June 2026).

29. UEBA (User and Entity Behavior Analytics) for when traditional cybersecurity can't protect your network. Northforge Innovations. URL: https://gonorthforge.com/ueba/ (accessed 28 June 2026).

30. Digital Education Action Plan: Policy Background. URL: https://education.ec.europa.eu/focus-topics/digital-education/actions/plan (accessed 28 June 2026).

31. The EU NIS2 Directive: what it is, for what needs it was developed, and why Ukraine is implementing it. URL: https://cip.gov.ua/ua/news/direktiva-yes-nis2-sho-ce-take-dlya-yakikh-potreb-rozroblena-ta-dlya-chogo-ukrayina-yiyi-implementuye (accessed 28 June 2026).

32. International Standards and Guidelines: European Higher Education Area. URL: https://naqa.gov.ua/2020/02/%D0%BC%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D1%96-%D0%BE%D1%81%D0B2%D1%96D1%82%D0%BDD1%96%D0%BF%D1%80%D0%B0%D0%BA%D1%82%D0%B8%D0%BA%D0%B8/ (accessed 28 June 2026).

33. Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG). URL: https://ihed.org.ua/recommends/standarty-i-rekomendatsiyi-shhodo-zabezpechennya-yakosti-v-yevropejskomu-prostori-vyshhoyi-osvity-esg/ (accessed 28 June 2026).

34. ERA-UA. Roadmap for Ukraine's Integration into the European Research Area. URL: https://mon.gov.ua/tag/era-ua (accessed 28 June 2026).

35. A New European Research Area Platform Has Been Established. URL: https://horizon-europe.org.ua/uk/news/info/stvoreno-novu-platformu-yevropejskogo-doslidnyczkogo-prostoru/ (accessed 28 June 2026).

36. Digital Education Action Plan 2021-2027. URL: https://education.ec.europa.eu/focus-topics/digital-education/actions (accessed 28 June 2026).

37. General Data Protection Regulation (GDPR). URL: https://gdpr-text.com/uk/ (accessed 28 June 2026).

3.3. Mathematical model of expert data analysis in information and analytical systems

Zoriana NOVOSAD,

Olena TOICHKINA

Lviv University of Trade and Economics

In the context of the ongoing digital transformation of society, information and analytical systems are becoming increasingly important as tools for supporting managerial decision-making. Their effectiveness largely depends on the application of mathematical methods of data analysis capable of identifying hidden patterns, establishing relationships between the objects under study, and providing a scientifically grounded interpretation of the results. Such methods are particularly relevant when processing expert information, where traditional statistical analysis does not fully capture the structure of relationships among the factors under investigation. In this regard, a promising approach is to combine methods of expert evaluation, mathematical statistics, and graph theory to develop mathematical models suitable for use in information and analytical decision-support systems.

Under conditions of uncertainty, managerial decisions are based on analysis, forecasting, optimization, economic justification, and the selection of the best alternative when the available information is insufficient or incomplete. This creates a need for methodological guidelines on decision-making under information scarcity that can enhance the adaptability and stability of organizational systems. Effective managerial decision-making requires consideration of both internal and external factors, as well as the quantity and quality of the information available for analysis.

Borsh V. V. and Osochenko I. V. (2006), as well as Shurlenkova R. K. and Demko I. I. (2016), classify managerial decision-making methods according to the degree of information available to business entities. When sufficient information is available, economic and mathematical modelling methods are among the most appropriate tools for managerial decision-making.

When sufficiently complete information is available, statistical methods, the goal tree method, and scenario analysis can be applied. Under conditions of information scarcity, game-theoretic methods, heuristic approaches, and expert methods are commonly used. Therefore, effective managerial decision-making under limited information (Oleksiienko R., Donets A., 2021) requires a combination of different methods. This makes it possible to conduct a comprehensive analysis of the problem and identify potential solutions and strategies.

The Strategy for the Development of Higher Education in Ukraine for 2022–2032 aims to facilitate Ukraine's integration into the European community as an equal partner. According to the document, the primary goal of higher education development is to promote the intellectual, cultural, and professional development of individuals, foster high-quality human capital, and build a cohesive society capable of supporting a competitive economy and high standards of living (Government Portal, 2022). To achieve this goal, five key objectives have been identified:

1. Establishing an effective and socially responsible higher education governance system.
2. Building trust among citizens, the government, and businesses in the educational, research, and innovation activities of higher education institutions.
3. Ensuring high-quality, competitive, and accessible education for all segments of the population.
4. Promoting the internationalization of higher education.
5. Increasing the attractiveness of Ukrainian higher education institutions for study and research careers.

An important area in the development of modern higher education is the expansion of international academic mobility among students and the strengthening of cooperation between higher education institutions in different countries. One of the key

instruments for achieving these objectives within the European Higher Education Area is the European Union's Erasmus+ programme. In particular, it supports learning mobility, international cooperation, the enhancement of educational quality, the acquisition of new knowledge and competencies by students, and the exchange of educational experience between universities.

International academic mobility broadens opportunities for students to develop individual learning pathways. It enables them to complete selected educational components at higher education institutions in other countries, become familiar with different approaches to organizing the educational process, and gain experience of studying in an international environment.

The practical implementation of academic mobility within the educational and professional programme "Computer Science" at the second (Master's) level of higher education at Lviv University of Trade and Economics can be illustrated by the participation of its students in studies at Pavol Jozef Šafárik University in Košice, Slovakia, during the second semester of the 2025–2026 academic year. According to the individual academic mobility study plan, part of the second-semester educational components was completed at the partner university. As a result, the students earned 21 credits for six educational components: *Algorithms and Data Structures* (4 credits), *Data Analysis Project I* (4 credits), *Programming Language Python* (4 credits), *Data Management Seminar* (2 credits), *Machine Learning* (5 credits), and *Technologies of Big Data Processing* (2 credits).

The educational and professional programme at Lviv University of Trade and Economics includes such components as "Machine Learning Systems", "Agile Methodology for Information Systems Development in Business", "Computer Vision Systems", "Risk Management in Innovation Activities", and "Efficiency of Information Systems in Business", as well as elective components. The total workload of the programme is 90 ECTS credits, including 66 credits for compulsory components and 24 credits for elective components.

A comparison of the two programmes reveals substantial content alignment between the *Machine Learning* course at Pavol Jozef Šafárik University and the "Machine Learning Systems" component at Lviv University of Trade and Economics.

At the same time, *Data Analysis Project I*, *Programming Language Python*, *Data Management Seminar*, and *Technologies of Big Data Processing* complement students' professional training in data analysis, programming, data management, and modern big data processing technologies. The identified areas of content overlap make it possible to determine the main directions of academic mobility and to identify opportunities for complementing educational components.

Thus, academic mobility within Erasmus+ adds a practical European dimension to the approaches to educational programme analysis considered in this study. The proposed research makes it possible to identify the structure of factors affecting students' learning and to determine similarities between educational programmes based on the way these factors manifest themselves. International academic mobility, in turn, creates additional opportunities for developing individual learning pathways and acquiring professional competencies in an international educational environment. Combining these approaches may contribute to the improvement of educational programmes, the expansion of international cooperation between higher education institutions, and the further integration of Ukrainian higher education into the European Higher Education Area.

Harmonizing education with European standards and shaping future educational policy in the context of globalization require appropriate strategic decisions. Therefore, another area considered in this study is the expert evaluation method.

Today, decision-making is becoming increasingly complex due to the growing number of influencing factors and the increasing volume of information, which require comprehensive approaches. Although mathematical methods remain important, they are not sufficient to ensure highly effective managerial decisions. For this reason, expert methods are increasingly used to support decision-making when the available information is limited or unreliable.

Expert methods are among the most widely used approaches in both scientific research and practical applications. They comprise a set of logical, mathematical, and statistical methods and procedures related to expert evaluation and the subsequent processing of the information obtained. The use of expert methods is particularly appropriate when data for risk assessment are unavailable or insufficient, since these

methods rely on the subjective judgments of experts who possess specialized knowledge and practical experience in the relevant field.

Expert methods make it possible to:

– develop a comprehensive understanding of the potential consequences of implementing managerial decisions at different levels;

– develop alternative scenarios that can serve as a basis for formulating consistent action plans;

– forecast future developments when statistical data are unavailable or insufficient.

Such methods are widely used to address business, economic, technical, and scientific problems, particularly when statistical methods prove ineffective. This is especially relevant in studies where quantitative data are difficult to obtain, for example, when assessing human abilities or the consumer properties of products.

Expert methods involve:

– collecting information from experts on a specific issue;

– processing the collected information using mathematical and statistical methods to identify optimal solutions.

Although the assessments obtained in this way reflect the collective opinion of experts, a high degree of agreement among them generally increases confidence in the results. At the same time, individual experts may provide more accurate assessments even when their opinions differ from the majority view. Expert methods combine logical and mathematical procedures and incorporate both quantitative techniques and heuristic approaches. This makes them an effective tool for addressing complex and poorly formalized problems in management, economics, and science (Martynova O. V., Shevchenko O. K., 2021; Nikitin O. A., 2020).

When applying the expert evaluation method, a specially selected group of experts, usually consisting of five to seven members, is surveyed to determine the values of individual variables required to assess the problem under study. The experts provide professional judgments on the most effective approaches to solving the problem, attracting investment, determining the time required to achieve the stated objectives, and establishing criteria for selecting the optimal solution.

The effectiveness of the expert evaluation method largely depends on the competence of the experts involved. Key requirements include in-depth knowledge of the subject under study, a high level of professional expertise, the ability to formulate clear and well-reasoned conclusions promptly, and impartiality in evaluating the proposed alternatives. Experts should have no personal interest in any of the possible solutions to the problem under consideration.

Experts are generally selected according to formal professional criteria, including position, academic degree, length of professional experience, and other indicators of qualification. This approach helps ensure the involvement of highly qualified specialists with substantial practical experience in the relevant field.

The use of expert evaluation methods makes it possible to determine the relative importance of factors affecting the learning of higher education students enrolled in particular educational programmes, rank these factors, and assess the degree of agreement among experts. The corresponding statistical indicators provide a quantitative measure of the similarity or consistency of the results. However, they do not fully reflect the internal structure of relationships among educational programmes, the factors under investigation, and the expert assessments obtained.

For example, similar correlation coefficient values may correspond to different configurations of relationships among individual factors. To provide a structural interpretation of the research results and visualize the relationships among the objects under study, graph-theoretic methods can be applied. Graph theory is widely used to model complex systems, analyse relationships among objects, and support decision-making in various fields, including economics, social research, and education [Filenta P., Kydros D., 2023; Golędzinowski W., Błocki W., 2023].

A graph model makes it possible to represent educational programmes, influencing factors, or experts as vertices of a graph, while the relationships of similarity, preference, or significant influence established between them can be represented as edges or weighted arcs indicating the strength of the corresponding relationship. This approach shifts the focus from analysing isolated numerical characteristics to examining the overall structure of relationships.

Using a graph model, it is possible to identify the most important factors affecting the learning of higher education students within a particular educational programme, distinguish groups of factors with similar patterns of influence, identify educational programmes with common problems, and determine factors that are universal and significant for most educational programmes.

The aim of this subsection is to construct a graph model and investigate the system of relationships between educational programmes and the factors affecting the learning of higher education students. It also seeks to identify structural features that cannot be revealed solely through importance coefficients, rank correlation, and concordance.

The expert evaluation method is applied to the educational process at Lviv University of Trade and Economics.

The group expert evaluation method, which takes into account the competence of the experts, is used to identify the most significant issues for improving educational activities. Its application is illustrated using the educational process for first-cycle (Bachelor's) students enrolled in six educational and professional programmes: "Computer Science", "Management", "Tourism", "Logistics and Sales Management", "Advertising in Business", and "Law".

To implement the methodology, a specially designed questionnaire containing a broad range of questions and response options was used. A scoring scale was also introduced to enable the subsequent processing of the collected data.

Thus, to investigate the factors affecting students' learning within educational programmes, a survey was conducted among students of Lviv University of Trade and Economics during the 2024–2025 academic year. The survey aimed to assess the extent to which teaching and learning methods and formats complied with the principles of academic freedom and a student-centred approach. The expert assessments were calculated using the survey results of first-cycle (Bachelor's) students enrolled in six educational and professional programmes: "Computer Science", "Management", "Tourism", "Logistics and Sales Management", "Advertising in Business", and "Law".

Table 3.1 presents the scores of the indicators calculated using the following formula:

$$V = k \cdot p, \qquad (3.1)$$

where k is the weighting coefficient selected according to the number of students enrolled in each educational programme, and p is the students' score.

Table 3.1.

Initial data

Indicators (factors affecting learning within the educational programme)	**Scores of indicators provided by students of educational and professional programmes**					
	Computer Science	Advertising in Business	Management	Logistics and Sales	Tourism	Law
Insufficient level of school preparation	32	37	16	25	13	52
Insufficient provision of teaching and methodological materials (textbooks, study guides, methodological instructions)	14	6	19	24	12	28
Inconvenient timetable	22	15	23	17	30	20
Excessive academic workload	44	18	14	25	27	48
Need to combine study and work	10	34	26	50	46	35
Disappointment with the educational programme (speciality)	15	17	13	15	18	24
Personal lack of organization	23	7	41	34	36	20
Lack of interest in studying	12	14	5	28	30	7
Influence of other students that discourages the student from studying during classes	35	22	16	18	14	33
Lack of employment prospects	5	8	39	43	30	9

Source: calculated and compiled by the author.

Based on the compiled table, we will:

1) calculate the importance coefficient for each indicator;

2) determine the ranks of the indicators;
3) assess the agreement between all possible pairs of experts using Spearman's rank correlation coefficient;
4) assess the agreement among three experts using Kendall's coefficient of concordance.

In this part of the study, we will use the Pandas software library and the Google Colab platform.

Pandas is a powerful Python library for data analysis and processing (Nikitiuk A. I., 2021). It provides convenient tools for working with tabular data, series, and structured datasets, and supports a wide range of operations, from data loading to advanced analysis.

One of the key features of Pandas is the ability to read and write data in various formats:

- CSV: pd.read_csv('file.csv'), df.to_csv('file.csv');
- Excel: pd.read_excel('file.xlsx'), df.to_excel('file.xlsx');
- SQL, JSON, HDF5 and other formats.

ColabVebPro is an innovative platform for integrating digital technologies into education. It is used to develop modern educational courses, facilitate collaboration between students and teachers, and manage the learning process. Its primary goal is to improve the quality of education by providing access to interactive tools for learning and knowledge sharing.

The seventh factor, the need to combine study and work, received the highest overall rank, while insufficient provision of teaching and methodological materials ranked tenth.

Agreement among experts is assessed through the relationship between their evaluations and is based on nonparametric methods for measuring the strength of association.

The following Spearman rank correlation coefficients were obtained: $\rho_{26} = 0,72$ and $\rho_{24} = -0,05$. The Spearman coefficient between the second and sixth experts, $\rho_{26} = 0,72$, indicates a positive and moderate association between their evaluations.

The coefficient between the second and fourth experts, $\rho_{24} = -0,05$, indicates a negative and very weak association between their evaluations, suggesting almost no agreement between their opinions.

The value of Kendall's coefficient of concordance, 0,28, indicates a low level of agreement among students enrolled in the six educational and professional programmes: "Computer Science", "Management", "Tourism", "Logistics and Sales Management", "Advertising in Business", and "Law".

```
In [6]: df
```

Out[6]:

	Scores of indicators provided by students of educational and professional programmes	Unnamed: 1	Unnamed: 2	Unnamed: 3	Unnamed: 4	Unnamed: 5	Unnamed: 6
0	Indicators (factors affecting learning within the educational programme)	Computer Science	Advertising in Business	Management	Logistics and Sales Management	Tourism	Law
1	Insufficient level of school preparation	32	37	16	25	13	52
2	Insufficient provision of teaching and methodological materials	14	6	19	24	12	28
3	Inconvenient timetable	22	15	23	17	30	20
4	Excessive academic workload	44	18	14	25	27	48
5	Need to combine study and work	10	34	26	50	46	35
6	Disappointment with the educational programme (speciality)	15	17	13	15	18	24
7	Personal lack of organization	23	7	41	34	36	20
8	Lack of interest in studying	12	14	5	28	30	7
9	Influence of other students that discourages the student from studying during classes	35	22	16	18	14	33
10	Lack of employment prospects	5	8	39	43	30	9

Fig. 3.1. Scores of the indicators

Source: calculated and compiled by the author based on the indicator scores provided by students enrolled in the educational and professional programmes.

Let us construct the *weights* list of dictionaries of indicator importance coefficients.

```
[ ]  weights = []
     for i in range(nrow - 2):
       s = sumopp[i] / allsum
       dict = {'ep': s, 'nep': epn[i + 1]}
       print(dict['ep'], "-->", dict['nep'])
       weights.append(dict)
```

```
0.12384996461429583 --> Insufficient level of school preparation
0.07289455060155697 --> Insufficient provision of teaching and methodological materials (textbooks, study guides, methodological instructions)
0.08987968860580325 --> Inconvenient timetable
0.12455767869780608 --> Excessive academic workload
0.14225053078556263 --> Need to combine study and work
0.07218683651804671 --> Disappointment with the educational programme (speciality)
0.11394196744515216 --> Personal lack of organization
0.06794055201698514 --> Lack of interest in studying
0.09766454352441614 --> Influence of other students that discourages the student from demonstrating abilities during classes
0.06794055201698509 --> Lack of employment prospects
```

Fig. 3.2. List of dictionaries of indicator importance coefficients

Source: calculated and compiled by the author

Within the survey conducted on students' learning in educational and professional programmes at Lviv University of Trade and Economics, excessive academic workload was the most frequently reported factor among students enrolled in the "Marketing" and "Advertising in Business" programmes. However, students in the "Law" programme did not consider this factor to be as significant. The next most frequently reported issue was an inconvenient timetable. Interestingly, compared with students in the other two programmes, students enrolled in the "Law" programme placed greater emphasis on the influence of other students that may hinder the expression of individual abilities during classes. The results also showed that, on average, the need to combine study and work was an important factor for students across all three educational programmes.

Based on the expert evaluation of learning within the educational and professional programmes "Marketing", "Advertising in Business", and "Law", the following issues were identified as priorities for further analysis:

- the need to combine study and work (overall rank 1);
- insufficient level of school preparation (rank 2);
- excessive academic workload (rank 3).

At the same time, the following issues were considered to be of low priority or of no particular relevance for further analysis:

- insufficient provision of teaching and methodological materials (textbooks,

study guides, methodological instructions) (rank 10);

- lack of interest in studying (rank 9);
- disappointment with the educational and professional programme (rank 8).

Thus, a well-designed survey of higher education students can contribute to assessing their intentions and identifying priorities for the further development of educational activities, particularly under conditions of uncertainty caused by both internal and external factors.

We present the results of the expert evaluation as a system of three interconnected graphs, each representing a particular aspect of the problem under study. The basic concepts of graph theory used in this study are well established and can be found, for example, in Bondy and Murty (2008) and Diestel (2017).

Let $P = \{P_1, P_2, ..., P_6\}$ be the set of educational and professional programmes in which the students participating in the study are enrolled, where

P_1 is “Computer Science”;

P_2 is “Advertising in Business”;

P_3 is “Management”;

P_4 is “Logistics and Management”;

P_5 is “Tourism”;

P_6 is “Law”.

Let $F = \{F_1, F_2, ..., F_{10}\}$ be the set of factors affecting learning within the educational programme, where

F_1 is “Insufficient level of school preparation”;

F_2 is “Insufficient provision of teaching and methodological materials”;

F_3 is “Inconvenient timetable”;

F_4 is “Excessive academic workload”;

F_5 is “Need to combine study and work”;

F_6 is “Disappointment with the educational programme (speciality)”;

F_7 is “Personal lack of organization”;

F_8 is “Lack of interest in studying”;

F_9 is “Influence of other students that hinders the expression of a student’s abilities during classes”;

F_{10} is “Lack of employment prospects”.

For an educational programme $P_i \in P$ $(i = 1,...,6)$, let e_{ij} denote the importance of factor $F_j \in F$ $(j = 1,...,10)$. We then obtain the matrix $E = \left(e_{ij}\right)_{6\times 10}$ which provides the data for constructing the graphs defined below.

We call the matrix $E = \left(e_{ij}\right)$ the matrix of weighted expert (score-based) assessments of the factors, where e_{ij} is the weighted score assigned to the j-th factor for the i-th educational programme.

The value of e_{ij} is calculated using formula 3.1. Therefore,

$$E = \begin{pmatrix} 32 & 14 & 22 & 44 & 10 & 15 & 23 & 12 & 35 & 5 \\ 37 & 6 & 15 & 18 & 34 & 17 & 7 & 14 & 22 & 8 \\ 16 & 19 & 23 & 14 & 26 & 13 & 41 & 5 & 16 & 39 \\ 25 & 24 & 17 & 25 & 50 & 15 & 34 & 28 & 18 & 43 \\ 13 & 12 & 30 & 27 & 46 & 18 & 36 & 30 & 14 & 30 \\ 52 & 28 & 20 & 48 & 35 & 24 & 20 & 7 & 33 & 9 \end{pmatrix}.$$

Define the weight function $w: P \times F \to \mathbb{R}_{\geq 0}$ which assigns to each pair $\left(P_i, F_j\right)$, $i = 1,...,6$, $j = 1,...,10$, the weighted score e_{ij} of the j-th factor for the i-th educational programme.

According to the data of the matrix E, we construct three graphs, each of which characterises a particular aspect of the expert assessment, namely:

1) the graph G_{PF}, which represents the relationships between the educational programmes and the influencing factors;
2) the graph G_F, which represents the grouping of the influencing factors;
3) the graph G_P, which provides a comparison of the educational programmes.

We construct the weighted bipartite graph $G_{PF} = (V, E_{PF}, w)$, where $V = P \cup F$, $E_{PF} = P \times F$, and the weight function $w: E_{PF} \to \mathbb{R}_{\geq 0}$ is defined by $w(P_i, F_j) = e_{ij}$, where e_{ij} $(i = 1,...,6,\ j = 1,...,10)$ is the weighted score (strength of influence) of the j-th factor $F_j \in F$ for the i-th educational programme $P_i \in P$, obtained from the expert assessment of the students enrolled in this programme.

Thus, each entry e_{ij} of the matrix E determines the weight of the edge between the corresponding educational programme and factor; hence, E is the edge-weight matrix of the bipartite graph G_{PF}.

Since the constructed bipartite graph G_{PF} is complete, the degree of each vertex $P_i \in P \subset V$ $(i = 1,...,6)$ is equal to 10, while the degree of each vertex $F_j \in F \subset V$ $(j = 1,...,10)$ is equal to 6; hence, these degrees are not informative. At the same time, the graph G_{PF} is weighted, so we can define the weighted degree $s(v)$ of a vertex as the sum of the weights of all edges incident to that vertex.

Proposition. *The weighted degree of a vertex P_i $(i = 1,...,6)$ of the bipartite graph G_{PF} is equal to the sum of the entries in the i-th row of the matrix E, while the weighted degree of a vertex F_j $(j = 1,...,10)$ is equal to the sum of the entries in the j-th column of the matrix E.*

Indeed, each edge incident to the vertex P_i, $i = 1,...,6$, has weight e_{ij}, $j = 1,...,10$. Therefore, the sum of the weights of all edges incident to this vertex is $\sum_{j=1}^{10} e_{ij}$, which is the sum of the entries in the i-th row of the matrix E. Similarly, for the vertices F, the incident edges correspond to the entries in the respective columns of the matrix E.

Since each edge is counted exactly once in the row sums and exactly once in the column sums, we have

$$\sum_{i=1}^{6} s(P_i) = \sum_{j=1}^{10} s(F_j) = \sum_{i=1}^{6} \sum_{j=1}^{10} e_{ij}$$

For the vertices F_j, $j=1,...,10$, of the graph G_{PF}, we obtain (Table 3.2):

Table 3.2

Weighted degrees of the factor vertices of the bipartite graph G_{PF}

	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
P1	32	14	22	44	10	15	23	12	35	5
P2	37	6	15	18	34	17	7	14	22	8
P3	16	19	23	14	26	13	41	5	16	39
P4	25	24	17	25	50	15	34	28	18	43
P5	13	12	30	27	46	18	36	30	14	30
P6	52	28	20	48	35	24	20	7	33	9
$s(F_j)$	175	103	127	176	201	102	161	96	138	134

Source: calculated and compiled by the author based on the scores of the indicators provided by the students enrolled in the educational programmes.

Thus, $s(F_1)=175$, $s(F_2)=103$, $s(F_3)=127$, $s(F_4)=176$, $s(F_5)=201$, $s(F_6)=102$, $s(F_7)=161$, $s(F_8)=96$, $s(F_9)=138$, $s(F_{10})=134$.

For each factor $F_j \in F$, $j=1,...,10$, we use the weighting coefficient q_j, obtained from the statistical processing of the expert assessments. The values of these coefficients are given in Table 3.3.

Table 3.3

Weighting coefficients of the factors

Factor, F_j	**Weighting coefficient,** q_j
F_1	0,12384996461429583
F_2	0,07289455060155697
F_3	0,08987968860580325
F_4	0,12455767869780608
F_5	0,14225053078556263
F_6	0,07218683651804671
F_7	0,11394196744515216
F_8	0,06794055201698514
F_9	0,09766454352441614
F_{10}	0,09483368719037509

Source: compiled by the author based on the list of weighting coefficients.

Hereafter, the coefficients q_j will be used as numerical characteristics of the corresponding vertices of the graph G_{PF}. Since the weighting coefficients are calculated for the factors under study, additional numerical characteristics are assigned only to the vertices of the set F. The vertices of the set P, corresponding to the educational programmes, are used in the constructed model to represent the structure of the relationships between the programmes and the factors and therefore do not require analogous characteristics.

We rank the influencing factors according to the weighted degrees of the corresponding vertices F_j, $j = 1,...,10$ (Table 3.4).

Table 3.4

Ranking of factors by the weighted degrees of the vertices

Vertex	**Weighted degree**	**Rank**
F_1	175	3
F_2	103	8
F_3	127	7
F_4	176	2
F_5	201	1
F_6	102	9
F_7	161	4
F_8	96	10
F_9	138	5
F_{10}	134	6

Source: calculated and compiled by the author.

Proposition. *The ranking of the factors by their weighting coefficients coincides with the ranking of the corresponding vertices of the bipartite graph by their weighted degrees.*

Indeed, since the weighting coefficient of the factor $F_j \in F$, $j = 1,...,10$, is defined by $q_j = \dfrac{s(F_j)}{\sum_{k=1}^{10} s(F_k)}$, and the denominator is the same positive constant for all factors, normalisation does not change the ordering of the values $s(F_j)$. Therefore, the two rankings coincide.

We construct the factor similarity graph. To each factor $F_j \in F$, $j = 1,...,10$, we assign the vector $f_j = (e_{1j}, e_{2j}, ..., e_{6j}) \in \mathbb{R}^6$, where f_j is the j-th column of the matrix E; for example, $f_1 = (32,37,16,25,13,52)$, $f_2 = (14,6,19,24,12,28)$ etc.

These vectors describe the pattern of the corresponding factor across the six educational programmes.

To assess the relationship between the factors F_j and F_k, we use the Pearson correlation coefficient, which is calculated between the vectors f_j and f_k using the formula:

$$r_{jk} = \frac{\sum_{i=1}^{6} \left(e_{ij} - \bar{e}_j\right)\left(e_{ik} - \bar{e}_k\right)}{\sqrt{\sum_{i=1}^{6} \left(e_{ij} - \bar{e}_j\right)^2} \sqrt{\sum_{i=1}^{6} \left(e_{ik} - \bar{e}_k\right)^2}},$$

where $\bar{e}_j = \dfrac{1}{6}\sum_{i=1}^{6} e_{ij}$, $\bar{e}_k = \dfrac{1}{6}\sum_{i=1}^{6} e_{ik}$.

The calculations were performed using Microsoft Excel and are presented in Table 3.5.

On the set of factors F, we construct the graph $G_F = (F, E_F)$, where $(F_i, F_j) \in E_F \Leftrightarrow |r_{ij}| \geq 0{,}6$ for any $F_i, F_j \in F$ (Fig. 3.3).

Table 3.5

Values of the Pearson Correlation Coefficients between the Factors

	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
F1	1	0,310512	-0,58388	0,639202	-0,19257	0,716357	-0,75631	-0,47547	0,794292	-0,72877
F2	0,310512	1	-0,08034	0,423139	0,204394	0,358992	0,367027	-0,16981	0,22334	0,293772
F3	-0,58388	-0,08034	1	0,081631	0,009213	0	0,616163	0,261341	-0,28431	0,226802
F4	0,639202	0,423139	0,081631	1	-0,30972	0,636949	-0,26363	-0,16411	0,849444	-0,59968
F5	-0,19257	0,204394	0,009213	-0,30972	1	0,241572	0,216724	0,69996	-0,63583	0,564169
F6	0,716357	0,358992	0	0,636949	0,241572	1	-0,42164	-0,10298	0,435929	-0,48584
F7	-0,75631	0,367027	0,616163	-0,26363	0,216724	-0,42164	1	0,262499	-0,55473	0,837805
F8	-0,47547	-0,16981	0,261341	-0,16411	0,69996	-0,10298	0,262499	1	-0,51674	0,432426
F9	0,794292	0,22334	-0,28431	0,849444	-0,63583	0,435929	-0,55473	-0,51674	1	-0,80959
F10	-0,72877	0,293772	0,226802	-0,59968	0,564169	-0,48584	0,837805	0,432426	-0,80959	1

Source: calculated and compiled by the author.

Thus, the correlation graph G_F has 10 vertices corresponding to the identified factors affecting learning across the six educational programmes and 12 edges representing correlations between the influencing factors. The edges shown by solid lines represent positive (direct) correlations, whereas the dashed lines represent negative (inverse) correlations. The graph is undirected since the correlation table is symmetric, i.e. $r\left(F_i,F_j\right)=r\left(F_j,F_i\right),$ which is consistent with the mutual nature of the relationships between the factors under consideration.

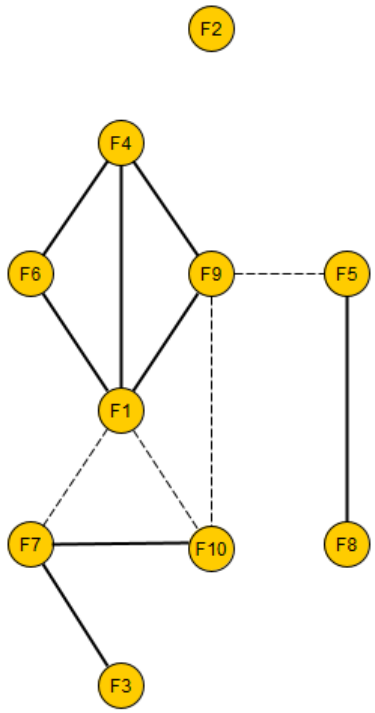


Fig. 3.3. Correlation graph between the factors for the threshold value $\left|r_{ij}\right|\geq 0,6$

Source: created by the author.

The graph contains an isolated vertex F_2 and is therefore disconnected, consisting of two connected components. The isolation of the vertex F_2 indicates that the factor "Insufficient provision of educational and methodological materials" has no strong correlation with any of the other factors under study at the selected threshold value. Thus, despite the importance of providing students with appropriate educational and methodological materials, this factor does not demonstrate strong relationships

with the other factors considered. This may indicate its relatively independent influence on the learning process.

The vertex F_1 has the highest degree ($deg(F)_1 = 5$). This indicates that insufficient school preparation is the factor with the largest number of relationships with the other factors and is strongly associated with students' subsequent perception of the learning process. The vertex F_9 ("Influence of other students that hinders the manifestation of a student's abilities during classes") also has a high degree. Therefore, these two factors can be regarded as the most interconnected factors in the system under study.

The strongest positive correlation (0.849) is observed between the factors F_4 and F_9, indicating a close relationship between the perception of the academic workload and the students' social environment. A fairly strong (0,838) and quite logical correlation is observed between the factors F_7 ("Personal disorganisation") and F_{10} ("Lack of employment prospects"). Similarly, the relationship (0.7) between the factors F_5 ("The need to combine study and work") and F_8 ("Lack of interest in studying") appears natural.

The density of the correlation graph G_F is equal to $D = \frac{2 \cdot m}{n(n-1)} = \frac{2 \cdot 12}{10 \cdot 9} = \frac{24}{90} \approx$ $\approx 0,267$, that is, the graph contains approximately 27 % of all possible edges. This indicates a relatively sparse structure of strong correlations at the selected threshold value: most of the factors under study are not strongly correlated with one another, while the most pronounced relationships are concentrated around particular factors, primarily F_1 and F_9. Therefore, practical measures should be targeted not at the entire set of factors simultaneously, but rather at key interconnected groups of factors.

The average vertex degree is $\bar{d} = \frac{2m}{n} = \frac{2 \cdot 12}{10} = 2,4$, meaning that, on average, each factor has approximately two to three correlations with other factors.

The analysis of the structure of the correlation graph revealed two triangles, $F_1F_4F_6$ and $F_1F_4F_9$, indicating strong pairwise correlations among the factors within each triangle.

The first triangle is formed by the factors F_1 ("Insufficient level of school preparation"), F_4 ("Excessive academic workload"), and F_6 ("Disappointment with the educational programme"). The presence of strong pairwise correlations among these factors may indicate that students' difficulties in adapting to their studies are complex in nature: an excessive academic workload combined with insufficient basic preparation may contribute to the development of a negative attitude towards studying within the chosen educational programme.

The second triangle is formed by the factors F_1 ("Insufficient level of school preparation"), F_4 ("Excessive academic workload"), and F_9 ("Influence of other students that hinders the manifestation of a student's abilities during classes"). This may indicate a close relationship between academic difficulties and the social learning environment, suggesting the need to take into account both academic and socio-psychological factors when organising the educational process.

It should be noted that both triangles share the common edge F_1F_4. It is likely that these two factors ("Insufficient level of school preparation" and "Excessive academic workload") form a kind of 'core' of this local group of interconnected factors. Thus, the structure of the correlation graph G_F indicates the existence of local groups of influencing factors that do not occur in isolation but rather as an interconnected complex.

We construct the programme similarity graph. For each educational programme $P_i \in P$, $i = 1,...,6$, we calculate the so-called coefficient of influence of negative factors $S_i = \sum_{j=1}^{10} e_{ij}$, where $e_{ij} \in E$ is the value of the j-th factor for the i-th educational programme. Clearly, an increase in S_i indicates an increase in the overall influence of negative factors on learning within the corresponding educational programme. The calculations were performed using Microsoft Excel and are presented in Table 3.6.

Table 3.6

Coefficients of the influence of factors on the educational programmes

	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	Si
P1	32	14	22	44	10	15	23	12	35	5	212
P2	37	6	15	18	34	17	7	14	22	8	178
P3	16	19	23	14	26	13	41	5	16	39	212
P4	25	24	17	25	50	15	34	28	18	43	279
P5	13	12	30	27	46	18	36	30	14	30	256
P6	52	28	20	48	35	24	20	7	33	9	276

Source: calculated and compiled by the author

Thus, $S_1 = 212,\ S_2 = 178,\ S_3 = 212,\ S_4 = 279,\ S_5 = 256,\ S_6 = 276.$

We rank the educational programmes according to the degree of severity of the problems under study (Table 3.7).

Table 3.7

Ranking of the educational programmes by the coefficient of influence of the factors

Educational programme	**Coefficient of influence,** S_i	**Rank**
P_1	212	4,5
P_2	178	6
P_3	212	4,5
P_4	279	1
P_5	256	3
P_6	276	2

Source: calculated and compiled by the author.

The integral indicator S_i characterises the overall level of manifestation of the negative factors under study for each educational programme. The highest value of this indicator is obtained for P_4 ("Logistics and Management"), indicating the highest overall level of severity of the problems under study among the programmes considered. A similar value is obtained for P_6 ("Law"), whereas the lowest value is observed for P_2 ("Advertising in Business"), indicating the lowest level of manifestation of the negative factors under study.

Since $S_1 = S_3$, the programmes P_1 ("Computer Science") and P_3 ("Management") have the same average rank of 4,5. However, the main factors negatively affecting learning in "Computer Science" are F_1 ("Insufficient level of school preparation"), F_4 ("Excessive academic workload"), and F_9 ("Influence of other students that hinders the manifestation of a student's abilities during classes"), whereas in "Management" the main factors are F_7 ("Personal disorganisation") and F_{10} ("Lack of employment prospects"). Thus, the same value of the integral indicator S_i may conceal different factors underlying its formation.

To each educational programme $P_i \in P$, $i = 1,...,6$, we assign the vector $p_i = (e_{i1}, e_{i2}, ..., e_{i10}) \in \mathbb{R}^{10}$, where p_i is the i-th row of the matrix E; for example, $p_1 = (32,14,22,44,10,15,23,12,35,5)$, $p_2 = (37,6,15,18,34,17,7,14,22,8)$ etc. These vectors describe the pattern of influence of the ten factors on students' learning within each educational programme.

For each pair of educational programmes P_i and P_k, we calculate the Pearson correlation coefficient between the vectors p_i and p_k using the formula:

$$r_{ik} = \frac{\sum_{j=1}^{10} \left(e_{ij} - \bar{e}_i\right)\left(e_{kj} - \bar{e}_k\right)}{\sqrt{\sum_{j=1}^{10} \left(e_{ij} - \bar{e}_i\right)^2} \sqrt{\sum_{j=1}^{10} \left(e_{kj} - \bar{e}_k\right)^2}},$$

where $\bar{e}_i = \frac{1}{10}\sum_{j=1}^{10} e_{ij}$, $\bar{e}_k = \frac{1}{10}\sum_{j=1}^{10} e_{kj}$.

The calculations were performed using Microsoft Excel and are presented in Table 3.8.

Table 3.8

Values of the Pearson correlation coefficients between the educational programmes

	P1	P2	P3	P4	P5	P6
P1	1	0,29338	-0,29798	-0,48327	-0,34988	0,726269
P2	0,29338	1	-0,31414	0,121407	0,02073	0,683931
P3	-0,29798	-0,31414	1	0,576842	0,459018	-0,26071
P4	-0,48327	0,121407	0,576842	1	0,726673	-0,145
P5	-0,34988	0,02073	0,459018	0,726673	1	-0,30345
P6	0,726269	0,683931	-0,26071	-0,145	-0,30345	1

Source: calculated and compiled by the author.

The analysis of the correlation matrix showed that the educational programmes can be divided into two groups with similar patterns of manifestation of the factors under study. The first group comprises the programmes P_1 ("Computer Science"), P_2 ("Advertising in Business"), and P_6 ("Law"), between which strong positive correlations are observed. The second group consists of the programmes P_3 ("Management"), P_4 ("Logistics and Management"), and P_5 ("Tourism"), which are also characterised by a similar pattern of influence of the negative factors. This suggests that similar approaches to improving the educational process may be appropriate within each group, whereas different management decisions may be required for the two groups.

On the set of educational programmes P, we construct the graph $G_P = (P, E_P)$, where $(P_i, P_j) \in E_P \Leftrightarrow |r_{ij}| \geq 0{,}55$ for any $P_i, P_j \in P$.

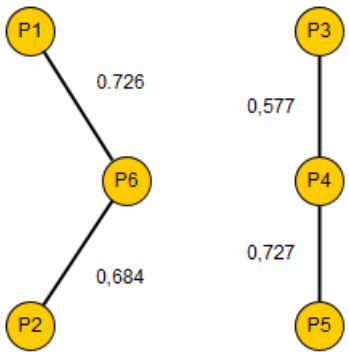


Fig. 3.4. Correlation graph G_P between the educational programmes for the threshold value $r \geq 0{,}55$.

Source: created by the author.

The graph G_P makes it possible to identify educational programmes with similar patterns of manifestation of the negative influencing factors. The vertices of the graph represent the educational programmes, while the edges connect those pairs of programmes for which the Pearson correlation coefficient is at least 0,55. The constructed graph is undirected and disconnected and consists of two connected components. The first connected component comprises the educational programmes P_1, P_2, and P_6, while the second comprises P_3, P_4, and P_5. This indicates the existence of two groups of educational programmes characterised by similar patterns of manifestation of the negative factors under study.

The obtained result complements the analysis of the integral indicators. In particular, although the educational programmes P_4 and P_6 have almost identical values of the integral indicator ($S_4 = 279$, $S_6 = 276$), they belong to different connected components of the graph, indicating substantial differences in the structure of the negative factors. At the same time, the programmes P_1 and P_3 have identical integral indicators ($S_1 = S_3 = 212$) but also do not belong to the same connected component. This confirms that the same overall level of manifestation of negative factors does not imply the same structure of their influence.

The study developed a graph-based model for analysing the factors affecting students' academic performance across different educational programmes. Based on the results of the expert assessment, a bipartite graph was constructed to represent the relationships between the educational programmes and the factors under study, together with a factor correlation graph that made it possible to identify the structure of the relationships among these factors. The analysis showed that some factors form local groups with strong relationships, whereas others are isolated and are practically unrelated to the remaining factors. This made it possible to identify the factors that are most strongly integrated into the system of negative influences, as well as those whose influence is relatively independent.

To quantitatively assess the level of manifestation of negative factors within the educational programmes, an integral indicator was used, which made it possible to rank

the programmes according to the overall severity of the problems under study. At the same time, further analysis of the correlation matrix between the educational programmes and the construction of their similarity graph showed that similar values of the integral indicator do not necessarily correspond to the same structure of negative factors. Thus, the similarity graph made it possible to identify groups of educational programmes with similar patterns of factor manifestation and demonstrated that the same overall level of the integral indicator may result from different combinations of negative factors.

Thus, the use of graph-theoretic methods substantially extends the capabilities of traditional statistical analysis. The proposed approach makes it possible to analyse the research results simultaneously at two levels: the level of relationships between the factors and the level of similarity between the educational programmes in terms of the patterns of manifestation of these factors. The combination of these two levels of analysis provides a more comprehensive understanding of the causes of students' learning difficulties across different educational programmes and makes it possible to identify directions for improving the educational process on a more substantiated basis. The proposed mathematical model can be integrated into information and analytical systems as a tool for expert data analysis and decision support. The combination of expert assessment methods, correlation analysis, and graph-theoretic methods makes it possible not only to quantify the factors but also to investigate their structural relationships. This enhances the informativeness of the analysis results and creates opportunities for applying the proposed model to monitoring, forecasting, and analytical support for management decision-making in various subject areas.

REFERENCES FOR SUBSECTION 3.3

1. Bondy J.A., Murty U.S.R. *Graph Theory*. London : Springer, 2008. XII, 651 p.

2. Diestel R. *Graph Theory*. 5th ed. Berlin ; Heidelberg : Springer, 2017. XVIII, 428 p.

3. Filenta P., Kydros D. The Application of Social Network Analysis to Economic and Regional Development: Tertiary Educational Attainment by Sex and NUTS 2 Regions. *Studies in Business and Economics.* 2023. Vol. 18, No. 2. P. 124–139.

4. Golędzinowski W., Błocki W. Social Network Analysis: From Graph Theory to Applications. *Social Communication.* 2023. Vol. 24, No. 1. P. 151–164.

5. LVIV UNIVERSITY OF TRADE AND ECONOMICS, 2024, [The results of surveys of applicants of higher education of the first bachelor's level on the subject of determining the degree of compliance of forms, methods of learning and teaching with the principles of academic freedom and a student-centered approach during education], http://www.lute.lviv.ua/osvita/monitoring-jakosti-osviti/anketuvannja-zdobuvachiv-vishchoji-osviti/anketi-dlja-opituvannja-zdobuvachiv-vishchoji-osviti/?L=966

6. Borshch, V. V., Osochenko, I. V. (2006). Metody pryiniattia rishen u menedzhmenti [Decision-making methods in management]. *Naukovi pratsi MAUP*, 2(14), 61–63.

7. Martynova, O. V., Shevchenko, O. K. (2021). Zastosuvannia metodu ekspertnykh otsinok v ekonomichnykh doslidzhenniakh [Application of the expert assessment method in economic research]. *Molodyi vchenyi*, 2(90), 259–266.

8. Nikitin, O. A. (2020). *Ekspertna otsinka ta yii analiz* [Expert assessment and its analysis]. Kharkiv: Ranok.

9. Nikitiuk, A. I. (2021). *Osnovy prohramuvannia movoiu Python* [Fundamentals of programming in Python]. Kharkiv: Folio.

10. Oleksiienko, R., Donets, A. (2021). Mistse ekspertnoi otsinky u pryiniatti upravlinskykh rishen [The role of expert assessment in management decision-making]. *Ekonomika i suspilstvo*, 26, 1–7.

11. Cabinet of Ministers of Ukraine. (2022). *Pro skhvalennia Stratehii rozvytku vyshchoi osvity v Ukraini na 2022–2032 roky: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 23 liutoho 2022 r. № 286-r* [On approval of the Strategy for the Development of Higher Education in Ukraine for 2022–2032: Order of the Cabinet of

Ministers of Ukraine of 23 February 2022 No. 286-r]. Verkhovna Rada of Ukraine legislation database (accessed 3 March 2022).

12. Shurpenkova, R. K., Demko, I. I. (2016). Evrystychni metody heneruvannia, otsinky i vyboru alternatyv [Heuristic methods for generating, evaluating and selecting alternatives]. *Socio-Economic Problems of the Modern Period of Ukraine*, 2(118), 151–154.

CHAPTER 4. DIGITAL RESILIENCE AND POST-WAR RECOVERY OF UKRAINE: THE ROLE OF INFORMATION TECHNOLOGIES AND CYBERSECURITY

4.1. DIGITAL TWIN Technologies in the Digital Transformation of the European Union Economy: Experience for Ukraine and the Concept of a Projective Digital Twin

Yurii IVANOV
National University "Yuri Kondratyuk Poltava Polytechnic"

Digital twins have developed from an engineering modelling tool into one of the core technologies of Europe's green and digital transition. They are used in industry, energy, climate modelling, ocean management, cities, transport, buildings, and complex infrastructure systems (European Commission. Destination Earth (DestinE); European Commission. European Digital Twin Ocean; European Commission. Digital Europe Programme; European Commission, Directorate-General for Research and Innovation. Industry 5.0).

The European Commission considers Destination Earth a flagship initiative for creating a highly accurate digital model of the Earth that can monitor, model, and predict the interaction between natural phenomena and human activity. The European Digital Twin Ocean develops a similar approach for ocean systems by combining heterogeneous data, models, and decision-support tools (European Commission. Destination Earth (DestinE)).

In manufacturing, Horizon Europe and Digital Europe support the transition from isolated digital models to interoperable twins, industrial data spaces, and distributed intelligence systems. The Change2Twin, MODAPTO, CONVERGING, and TwinEU projects show that a Digital Twin is becoming not a separate software product but an element of a digital ecosystem (European Commission. Destination Earth (DestinE); European Commission. European Digital Twin Ocean; European

Commission. Digital Europe Programme; European Commission, Directorate-General for Research and Innovation. Industry 5.0).

At the same time, most modern digital twins start with a physical object that already exists and aim to represent its current state, predict its behaviour, or optimise its operating mode. The opposite direction is much less formalised: first creating a digital model of the desired physical result, then building the process for achieving it, generating control instructions, receiving actual feedback, and adaptively changing the uncompleted part of the process.

The purpose of this study is to systematise current European approaches to Digital Twin and to justify the concept of a projective digital twin as a new functional class of digital models focused on forming a future physical state.

The relevance of the topic is strengthened by the fact that in the EU Digital Twin technology is increasingly viewed not as a separate visualisation tool but as infrastructure for testing policies, engineering solutions, and scenarios before they are implemented in the physical world. This change of scale creates new requirements: a digital twin must work with heterogeneous data, explain assumptions, support several time horizons, be compatible with other models, and preserve the possibility of human control.

The object of the study is the development and application of digital twins in European digital and manufacturing ecosystems. The subject of the study includes the conceptual, architectural, and organisational foundations of Digital Twin, as well as the possibility of extending them to form and manage the achievement of a future physical state.

In the broadest sense, a Digital Twin is a digital representation of a defined physical entity, process, or system, supported by data and used for analysis, modelling, forecasting, or control. However, there is still no universal definition. Different disciplines define the sufficient level of connection between the physical and digital worlds, the role of bidirectional exchange, and the boundaries of the life cycle in different ways (Nativi S. et al., 2020; Kritzinger W. et al., 2018; Fuller A. et al., 2020; Rasheed A. et al., 2020).

The classical distinction between a digital model, a digital shadow, and a digital twin is based on the nature of data exchange. A digital model may exist without an automatic connection to a physical object. In a digital shadow, data transfer is mainly directed from the physical object to the model. A fully functional digital twin involves bidirectional interaction: a change in the physical state updates the model, while the results of digital analysis may influence the physical process (Kritzinger W. et al., 2018).

This classification remains useful, but it no longer covers all modern cases. For example, a climate twin does not "control" the Earth in the usual technical sense, but it provides high-accuracy scenario modelling for policy and management decisions. At the same time, a manufacturing twin may generate equipment operating parameters in a closed loop. Therefore, digital twins should be compared not by the presence of one formal attribute but by a set of functions: representation, synchronisation, diagnostics, forecasting, optimisation, scenario modelling, decision support, and control.

It is important to distinguish forecasting from design. Forecasting answers the question of what is likely to happen under given conditions. Design determines which state is desirable and which sequence of actions can achieve it. In many digital twins, both functions are partly present, but the model for moving from a target state to specific physical operations usually remains an external planning module.

From a life-cycle perspective, a digital twin can support the concept, design, manufacturing, operation, maintenance, and decommissioning of an object. At the early stages, the physical object may not yet exist; therefore, the digital entity acts as a specification of the future object. After the object is created, the focus shifts to synchronisation and observation. During operation, diagnostics, failure prediction, and optimisation become central, while at the end of the life cycle the focus is on reuse, recycling, and environmental impact.

The Digital Twin technology stack includes IoT and sensor networks, computer vision, cyber-physical systems, cloud and edge computing, semantic models, artificial intelligence, simulation, high-performance computing, and visualisation tools. Practical maturity is determined by integration rather than by the presence of any single component.

Standardisation has a dual role. It establishes common terminology and architectural roles, but it should not prematurely limit new functional classes. ISO 23247 provides a digital twin framework for manufacturing, IEC 63278 links the digital representation of industrial assets with the Asset Administration Shell, and European data spaces develop organisational mechanisms for sovereign and controlled exchange (ISO 23247-1:2021; IEC 63278-1:2023; European Commission. Common European data spaces).

From the perspective of economic theory, a digital twin can be considered a mechanism for reducing information asymmetry between the state of a physical asset and the decision-maker. The more completely the model represents relevant parameters, the lower the costs of information search, diagnostics, coordination of actions, and performance control. At the same time, creating and maintaining a twin generates its own transaction costs: data verification, system integration, maintenance of semantic interoperability, and access-right management. Thus, the economic effect does not arise from digitalisation itself, but when the reduction of costs and risks in the physical process exceeds the total cost of the digital infrastructure.

An important methodological distinction is the difference between a digital twin and a conventional simulation model. A simulation model may be accurate but have no systematic connection with a specific physical object. A digital twin maintains the identity of the relevant asset or process, is updated with life-cycle data, and makes it possible to compare a forecast with the actual result. This capability turns modelling into an organisational learning tool: a forecasting error is not only recorded but is also used to improve subsequent decisions.

The maturity level of a Digital Twin should be determined not by the volume of accumulated data or the complexity of three-dimensional visualisation, but by the depth of its integration into the management cycle. At the initial level, the model performs a descriptive function; at subsequent levels, it provides diagnostics, forecasting, optimisation, and adaptive control. Such a gradation allows an organisation to relate the expected result to investment and avoid a situation in which a technologically complex system does not improve the quality of decisions.

Table 4.1

Digital Twin maturity levels

Level	Twin function	Management result	Key maturity condition
1	Description and visualisation	Transparency of the asset state	Identified data and objects
2	Diagnostics	Identification of causes of deviations	Data quality and traceability
3	Forecasting	Assessment of future states and risks	Validated model and uncertainty
4	Optimisation	Comparison of alternative decisions	Formalised criteria and constraints
5	Adaptive control	Adjustment of the physical process	Feedback, safety, and human oversight

Source: developed by the author.

The European approach to Digital Twin is developing at the intersection of digital and green transformations. It differs from the narrow implementation of individual corporate platforms because it combines technological, legal, ethical, and social requirements. The main focus is on scalability, open interfaces, model reuse, control of data access, and algorithmic accountability.

In the digital economy of the European Union, Digital Twin technologies are gradually changing from a local engineering tool into an infrastructure mechanism for coordinating data, models, and decisions. Their economic value lies in the ability to move part of experimentation from the physical environment to the digital one, test scenarios in advance, reduce the cost of error, and shorten the period between making a management decision and implementing it in practice.

For industrial enterprises, a digital twin supports coordination between design, manufacturing, operation, and asset maintenance. In logistics, it makes it possible to model material flows, warehouse operations, transport loading, and supply-chain resilience. In energy, digital twins are used to coordinate distributed sources, forecast loads, and assess emergency scenarios. In construction and urban management, they

combine data on facilities, infrastructure, resources, and user behaviour in a single decision-support environment.

The macroeconomic effect of Digital Twin is associated with higher capital productivity, reduced downtime, resource savings, and faster innovation. The possibility of comparing alternative scenarios before physical investment reduces uncertainty and supports better allocation of resources. However, value is created only when the digital model is included in the real decision-making cycle and when its accuracy, costs, and risks are aligned with a specific economic task.

The European model of Digital Twin development is based on a combination of market incentives, research funding, standards, and legal regulation. The Digital Decade programme sets digital transformation targets up to 2030, while Digital Europe and Horizon Europe provide financial and research support for supercomputing, artificial intelligence, cybersecurity, data spaces, and digital skills.

There is no single EU law specifically on digital twins. Their use is regulated by a set of legal acts depending on the data, algorithms, sector, and level of risk. The Data Governance Act creates mechanisms for trusted data reuse and voluntary data sharing, while the Data Act, applicable from 12 September 2025, establishes rules for access to data from connected products and related services (European Commission. Data Governance Act; European Commission. Data Act). For digital twins, this defines the legal conditions for obtaining machine and sensor data without which models cannot be kept up to date.

If a digital twin uses artificial intelligence for forecasting, risk assessment, or the generation of control decisions, the requirements of the AI Act apply. The Regulation establishes a risk-based approach and requirements for data quality, documentation, transparency, and human oversight. For the concept of a projective digital twin, this means that automatic generation of a target state and transition trajectory must be accompanied by safety checks, explainable criteria, and the possibility of operator intervention (European Commission. AI Act: Regulatory framework for artificial intelligence).

The cybersecurity environment is shaped by NIS2 and the Cyber Resilience Act. NIS2 establishes a common cyber-risk management framework for critical sectors,

including energy, transport, healthcare, and digital infrastructure. The Cyber Resilience Act introduces mandatory requirements for products with digital elements throughout their life cycle (European Commission. NIS2; European Commission. Cyber Resilience Act). Therefore, protection of a digital twin must cover not only the central model but also sensors, communication channels, storage systems, interfaces, and actuators.

The EU legal framework effectively turns digital twin quality from a purely technical category into a socio-economic one. A model must be not only accurate but also lawful, safe, accountable, and auditable. This corresponds to the European focus on digital sovereignty, trust in data, and human-centred transformation.

For Ukraine, European experience is important in two areas. First, alignment with EU rules creates conditions for Ukrainian enterprises to participate in common data spaces, research programmes, and cross-border production chains. Second, digital twins can become a recovery tool by modelling infrastructure, energy networks, construction projects, logistics routes, and the use of scarce resources before capital-intensive physical actions are undertaken.

The Industry 5.0 concept complements the Industry 4.0 focus on automation and productivity with three interconnected principles: human-centricity, sustainability, and resilience. The European Commission emphasises that technological progress should create value for a wider range of stakeholders, respect planetary boundaries, and place worker well-being at the centre of the production process (European Commission, Directorate-General for Research and Innovation. Industry 5.0).

For Digital Twin, human-centricity means transparent presentation of recommendations, the possibility of human intervention, and consideration of ergonomics, safety, skills, and the distribution of responsibility. Sustainability requires assessment of energy consumption, material flows, emissions, repairability, and circularity. Resilience involves modelling disruptions, resource shortages, cyberattacks, supplier failures, and rapid replanning.

Therefore, the optimal solution cannot be determined only by minimum cost or duration. It should result from multi-criteria assessment in which productivity is

balanced with safety and with social and environmental consequences. This requirement directly affects the concept of the projective digital twin proposed below.

Destination Earth (DestinE) is a flagship European Commission initiative to create a highly accurate digital model of the Earth. Its first operational release was launched on 10 June 2024, and the system is planned to develop in stages until 2030. The architecture includes the Core Service Platform under ESA responsibility, the Data Lake under EUMETSAT responsibility, and thematic digital twins developed by ECMWF (European Commission. Destination Earth (DestinE)).

The first thematic components were twins for climate-change adaptation and extreme weather events. They combine real-time observations with high-resolution predictive modelling. The user receives not only a dataset but an environment in which scenarios can be created, consequences analysed, and applied services developed. This demonstrates a key change: the digital twin becomes a platform for producing verifiable knowledge.

DestinE shows that a large-scale twin requires a clear distribution of roles. The platform provides access and service orchestration; the data lake provides storage, data-proximate processing, and scalability; thematic twins provide domain models and simulations. This division reduces dependence on a single provider and makes it possible to gradually connect new domains, including the ocean, biodiversity, and geophysical risks.

The European Digital Twin Ocean develops a virtual representation of the ocean by integrating satellite observations, marine sensor data, historical datasets, and numerical models. The scientific value of the initiative lies in combining observation with scenario analysis: users can explore the impact of climate, environmental, and economic decisions without directly experimenting on the natural system (European Commission. European Digital Twin Ocean).

The ocean twin also shows the limits of a literal interpretation of bidirectionality. Modelling results do not create an automatic control signal for the ocean, but they can change policies, regulation, spatial planning, and user behaviour. Thus, physical impact may be mediated by an institutional decision. For Digital Twin theory, this means that

the feedback channel should be described not only through technical commands but also through decisions made by people and organisations.

The Digital Europe Programme is mainly focused on deploying digital capabilities: supercomputing, artificial intelligence, cybersecurity, digital skills, and broad technology adoption. Horizon Europe funds research novelty, demonstration, and validation of new architectures. Together, they create a pathway from research to operational infrastructure (European Commission. Digital Europe Programme; European Commission. Horizon Europe — Cluster 4).

Change2Twin supported manufacturing small and medium-sized enterprises for which the barriers include not only software costs but also the lack of adequate-quality data, competencies, and a clearly defined business case. The project experience highlighted the need to diagnose digital maturity, introduce technology in stages, and demonstrate measurable value (CORDIS).

MODAPTO creates flexible manufacturing systems in which modules are enhanced by distributed intelligence through interoperable digital twins. Module interfaces are standardised using the Asset Administration Shell, while collective intelligence supports production design and reconfiguration. The project is important because it moves from one monolithic twin to a coordinated set of local twins (CORDIS. MODAPTO).

TwinEU is creating a federated ecosystem of digital twins for the European electricity system. It covers transmission, distribution, and market operations and combines physical and AI models, standard interfaces, data spaces, and high-performance computing. As of 2026, a reference architecture is being developed and validated in eight large demonstration environments (CORDIS. TwinEU).

A common result of these projects is a change in the unit of analysis. The object is no longer a single machine or line, but a federation of twins that exchange data, models, and assessment results. This requires semantic interoperability, coordination of time scales, model version management, and trust mechanisms.

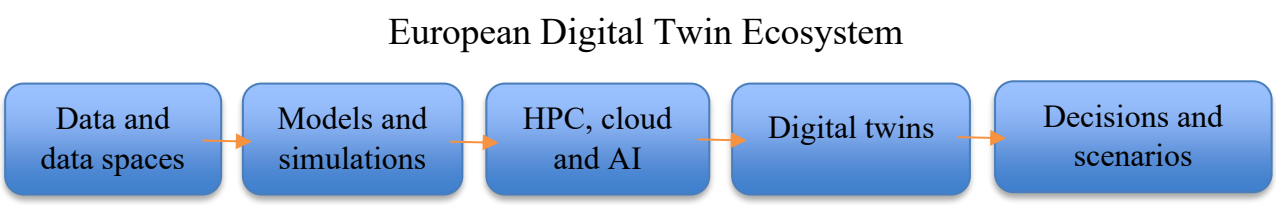


Fig. 4.1. Generalised logic of the European Digital Twin ecosystem

Source: developed by the author.

Table 4.2

Levels of digital twin implementation

Level	European example	Dominant function	Key requirement
Planetary	Destination Earth	Scenario modelling of climate and extremes	HPC, data, scientific verification
Natural system	Digital Twin Ocean	Integration of observations and models	Openness and interdisciplinarity
Infrastructure	TwinEU	Federation of power-system twins	Interoperability and cybersecurity
Manufacturing	MODAPTO	Reconfiguration of modular systems	AAS and distributed intelligence
Enterprise	Change2Twin	Practical implementation in SMEs	Maturity, competencies, business value

Source: developed by the author.

The standardisation basis of European digital twins is formed at several levels. ISO/IEC 30173:2023 establishes basic concepts, the context of a digital twin system, the life cycle, functional views, and the range of stakeholders (ISO/IEC 30173:2023). The ISO 23247 series specifies the framework for manufacturing: it defines general principles, a reference architecture, digital representations of manufacturing elements, and information-exchange requirements. IEC 63278-1:2023, in turn, formalises the

Asset Administration Shell as a standardised digital representation of an asset that provides unified access to information and services throughout the life cycle.

The combined use of these standards creates an important methodological hierarchy. ISO/IEC 30173 provides common terminology; ISO 23247 describes functional roles and interaction in a manufacturing context; AAS creates a machine-readable container for the data and services of a specific asset. However, the standards do not define a single optimisation method or mandatory decision-making algorithm. Therefore, applied systems should combine standardised exchange with domain models while preserving the ability to verify the origin of each parameter and the version of the algorithm.

Legal regulation of data influences architecture no less than technical standards. The Data Act differentiates access to data from connected products and related services but does not remove requirements concerning trade secrets, personal data, and security. Therefore, a federated digital twin should support differentiated rights: one participant may see raw measurements, another an aggregated indicator, and a third only the result of a constraint check. Such an access model reduces the risk of unjustified data distribution while preserving inter-organisational interaction.

If artificial intelligence is used within the digital twin loop, legal assessment should be based on the function and consequences of the specific application rather than on the name of the technology. For systems whose decisions may affect safety, human rights, or critical infrastructure, risk management, data quality, technical documentation, logging, human oversight, and the ability to reproduce decision logic are especially important. In a projective digital twin, these requirements should be built in at the stage of generating alternative target states rather than added after the algorithm has been developed.

Despite significant progress, the spread of Digital Twin is limited by a combination of technical, organisational, and methodological problems. The first is fragmentation of definitions. The same term may refer to a static 3D model, an asset information model, a simulator, a monitoring dashboard, or an adaptive cyber-physical system. This makes results difficult to compare and creates a risk of inflated expectations.

The second problem is interoperability. The formal availability of an API does not guarantee that two systems interpret an object, event, measurement quality, or acceptable delay in the same way. Common information models, semantics, identifiers, version policies, and machine-readable access rules are needed. This is why data spaces and AAS play an increasing role in European projects.

The third problem concerns data quality and provenance. A digital twin may produce convincing visualisation even when the data are incomplete or biased. Responsible use requires tracing the source, time, accuracy, preprocessing method, and limits of data applicability. The model should communicate not only the result but also uncertainty.

The fourth problem is model validation in a changing environment. Initial correspondence with the physical object does not guarantee continued accuracy because of wear, reconfiguration, changes in operating modes, or user behaviour. Continuous calibration, drift detection, and rules for safe transition to a fallback mode are required.

The fifth problem is cybersecurity. The more closely a digital twin is connected with control, the greater the potential impact of data, model, or command substitution. Protection must cover the entire chain: sensor, transmission channel, storage, model, decision interface, and actuator. A federated ecosystem additionally requires a clear distribution of responsibility among participants.

The sixth problem is economic feasibility. High detail increases the cost of sensors, computing, and maintenance but does not always increase decision value. Therefore, the level of accuracy should correspond to the specific task. A practically useful twin is not the largest model but the minimum sufficient model with a proven impact on decisions.

The seventh problem is the human in the loop. An automated recommendation may conflict with a worker’s non-formalised experience. Completely ignoring such experience reduces system acceptance, while uncontrolled manual intervention destroys reproducibility. An interface is needed that allows a person to confirm, reject, or modify a plan while recording the reason.

The eighth problem is the environmental cost of digital technologies themselves. Complex models, large datasets, and HPC consume energy. The positive effect of optimising the physical system should be compared with the digital footprint. The European logic of the twin transition directly requires digital and green transitions to reinforce each other rather than merely being declared (Muench S. et al., 2022).

A critical review reveals a separate functional gap. Most systems answer the questions “what is happening?”, “why did it happen?”, “what will happen?”, and “which operating mode is better?” quite well. The full cycle is less formalised: “what physical result should be created?”, “what alternatives are feasible?”, “what sequence of actions will move the system to the selected state?”, and “how should the uncompleted part of the plan be changed after an actual deviation?”

Table 4.3

Classes of twins

Twin class	Main question	Typical output	Limitation
Descriptive	What exists and what is happening?	Current digital state	Does not create a future result
Diagnostic	Why did a deviation occur?	Cause or component state	Reacts after the event
Predictive	What is likely to happen?	Forecast and risk	Does not necessarily contain an action plan
Optimisation	Which operating mode is better?	Recommended parameters	The target is often set externally
Projective	What state should be created and how can it be achieved?	Target state, trajectory, instructions	Requires feasibility control

Source: developed by the author.

A separate limitation is computational complexity. As the number of objects, permitted orientations, resources, and time dependencies increases, the space of possible configurations grows combinatorially. In spatial placement or scheduling

tasks, exhaustive search quickly becomes unacceptable. Practical implementation therefore requires a combination of exact methods for small subtasks, heuristics and metaheuristics for finding acceptable solutions, and early elimination of options that violate hard constraints. The quality criterion is not a mathematically absolute optimum but the best proven feasible solution obtained within the time available for control.

The risk of false synchronisation arises when the digital model has formally been updated but the actual data arrived late, were incomplete, or belonged to another state of the physical system. To reduce this risk, each observation should include a timestamp, source identifier, accuracy estimate, and validation status. In critical operations, a confidence threshold should be established: if total uncertainty exceeds the acceptable value, automatic control is suspended or requires operator confirmation.

Organisational barriers are often more significant than technological ones. Data may belong to different departments, use incompatible reference systems, or be used without a clearly defined quality owner. Overcoming this barrier requires a data-governance model: roles of owner, steward, and user; rules for changing reference data; quality indicators; and incident-review procedures. Without this, a digital twin automates the contradictions of the existing organisation instead of improving controllability.

A scenario approach is appropriate for risk assessment. For each critical function, the hazardous event, its cause, probability, scale of consequences, detectability, and compensating mechanism are identified. Examples include sensor failure, RFID-tag substitution, drift of a computer-vision model, loss of communication, conflict between local and central twins, or incorrect learning from an unsuccessful scenario. Such analysis links cybersecurity, functional safety, and model quality into one management system.

To address the identified gap, the concept of a projective digital twin is proposed. It is a single structured digital model of one possible future state of a physical system and the predicted method of transition from the current state to that state. It includes not only an image of the result but also a model of the process for creating it, resources, constraints, risks, criteria, and expected indicators.

The term “projective” has two interconnected meanings. In the temporal sense, it refers to projecting a physical system into a possible future state. In the spatial-interface sense, the result or the next action may be visually projected onto a work surface, container, or other physical space. The second meaning is a possible implementation method but is not a mandatory feature of the concept.

The fundamental difference lies in the direction of causality. A traditional twin mainly moves from the physical state to its digital representation and then to a forecast. A projective twin starts with a set of feasible future states, selects or agrees on one of them, transforms it into a trajectory and control actions, and then verifies actual achievement.

A projective digital twin should be represented as a composition of interconnected models: the physical system; initial state; target state; transition; resources; constraints; risks; assessment criteria; observation mechanism; and adaptation rules.

The system may generate one twin if the decision is unambiguous, or a set of alternative twins. In the second case, each alternative describes not simply another result but another “result–method of achievement” pair. This is important because the same final state may require different resources, time, and levels of risk.

The initial stage is to obtain data on the actual system. Sources may include sensors, machine-vision cameras, information systems, digital catalogues, and user input. The data are transformed into a consistent state description that records not only values but also their accuracy and relevance.

Next, goals and constraints are formalised. A goal should not be reduced to one number. For example, packaging requires simultaneous consideration of capacity, compatibility, fragility, retrieval order, weight, material costs, and ease of execution. In the Industry 5.0 context, worker safety, environmental impact, and resilience to disruptions are added.

On this basis, a space of feasible future states is formed. The algorithm eliminates physically impossible or legally unacceptable solutions, evaluates the remaining ones using a vector of criteria, and presents one or more options. Selection may be automatic, human, or mixed.

The selected state is transformed into a transition model. For each operation, prerequisites, the expected intermediate state, resource, acceptable deviation, and verification method are defined. The link between the future configuration and the physical sequence of actions creates the management value of the model.

During execution, the system receives actual feedback. If a deviation is within acceptable limits, the already achieved part of the state is accepted and the uncompleted part may be rebuilt. If a deviation violates safety or makes the target unreachable, the system stops the process, changes the target, or returns to an alternative twin.

Functional Cycle of the Projective Digital Twin

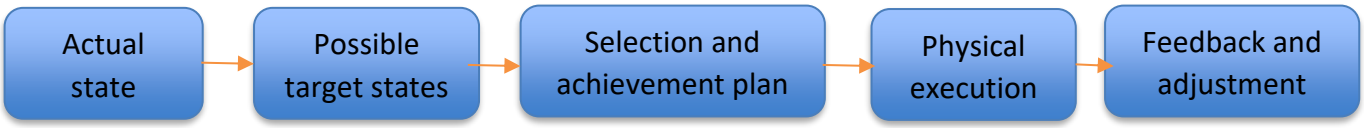


Fig. 4.2. Functional cycle of the projective digital twin
Source: developed by the author.

In formalised form, the projective digital twin can be represented as the structure $D^p = \langle x_0, G, P, U, R, C, Q, F \rangle$, where x_0 is the estimated initial state; G is the set of feasible target states; P is the predicted transition trajectory; U is the sequence of control actions; R represents resources; C is the system of constraints; Q represents assessment criteria; and F is the feedback mechanism. This notation emphasises that the model of the future result is only one component: without a trajectory, resources, and verification of the actual state, it remains a digital design rather than a twin of a controlled physical process.

The choice of an alternative can be described as a multi-criteria assessment problem $D^* = \arg\min J(D_k)$, $D_k \in \Omega$, where Ω is the set of physically feasible projective twins. Function J aggregates normalised indicators of time, cost, energy, risk, ergonomics, and resilience. Since reducing criteria to one number may hide conflicts between priorities, responsible decisions should additionally form a Pareto set and show the user which indicator makes one alternative preferable to another.

The architecture of a projective twin has at least four logical levels. The data level identifies physical objects, the environment, and events; the model level

maintains the current state and generates possible target states; the decision level checks constraints, compares alternatives, and performs planning; the execution level transfers instructions to a person or machine and receives confirmation. Formalised data contracts should exist between the levels so that replacing a sensor, optimisation algorithm, or interface does not damage system integrity.

Validation of the concept should be performed separately for the state model, the transition model, and the adaptation mechanism. For the state model, the accuracy of reconstructing the physical configuration is assessed; for the transition model, the share of executable instructions, duration, and resource costs are evaluated; for adaptation, the ability to preserve target achievability after a deviation is assessed. Comparison should be made with baseline modes: manual execution, a static digital instruction, and a traditional twin without automatic replanning.

A representative area of application is order picking, packaging, palletising, and internal logistics. Here the future physical result has a clear spatial structure, while errors arise from incomplete data, the human factor, changes in order composition, unsuitable packaging, or actual displacement of objects.

The system creates a digital model of each material object involved in picking, placement, or packaging processes. The digital model contains a set of parameters describing the physical, geometric, and operational properties of the object that are required for automated analysis and modelling of its placement in physical space.

To support automated generation of a digital twin for picking, placement, and packaging processes, the system creates a digital model of the available physical space intended for placing material objects. The digital model of physical space is a structured set of parameters describing geometric characteristics, constraints, and environmental features within which operations with material objects are performed.

Physical space may include packaging, transport containers, boxes, bags, pallets, racks, work surfaces, production zones, vehicle cargo compartments, warehouse cells, or other objects intended for the placement of material objects.

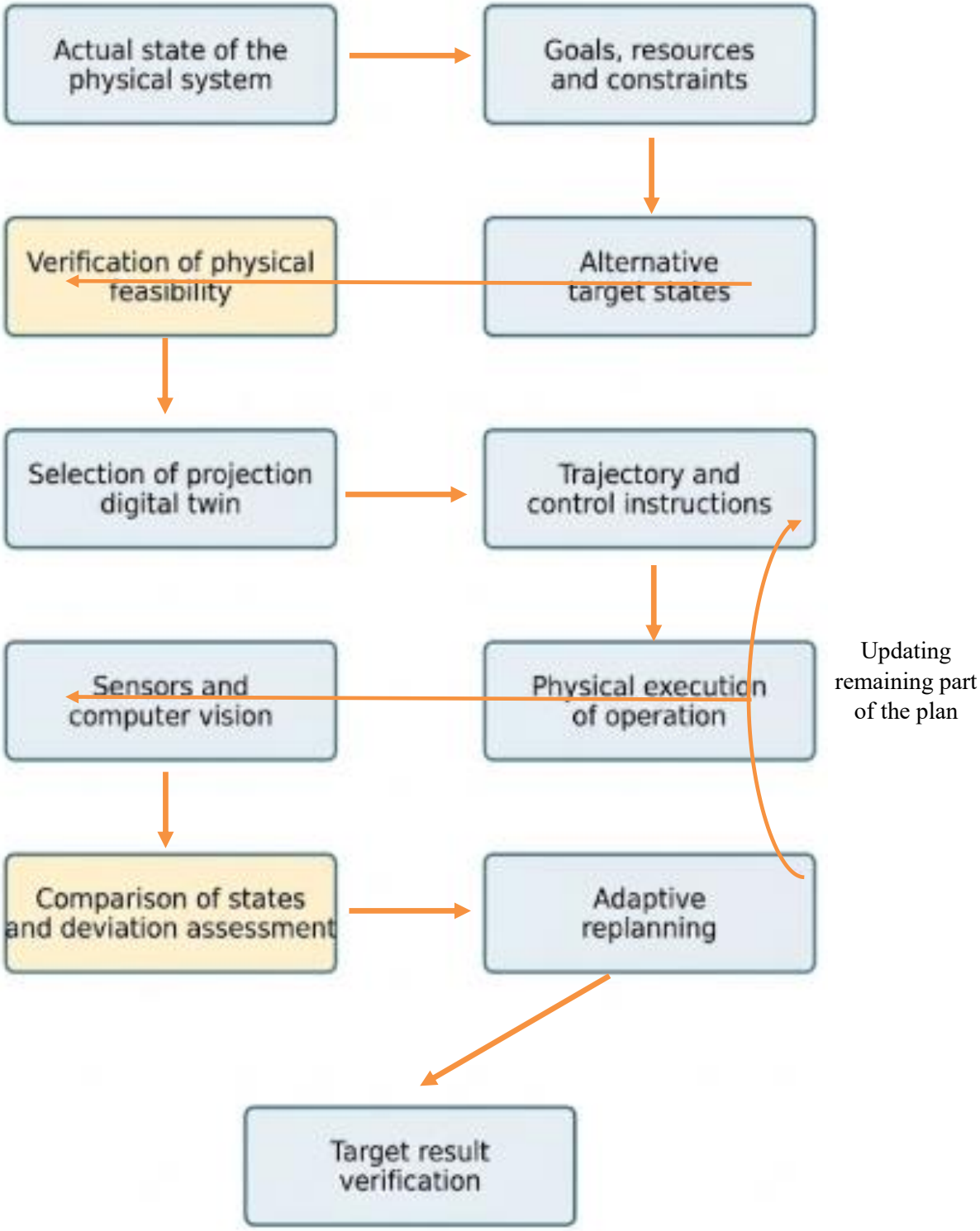


Fig. 4.3. Projective digital twin operation algorithm

Source: developed by the author.

The system performs automated analysis of digital models of material objects and digital models of the available physical space in order to determine one or more possible options for their spatial placement. During the analysis, the system considers the geometric parameters of material objects, their quantity, weight, permitted orientations, compatibility characteristics, placement constraints, and the parameters of the physical space in which the operation is planned.

Based on these data, the system automatically generates a set of possible placement options for material objects in the available physical space and evaluates them according to specified criteria. After a set of feasible spatial-placement options has been generated, the system evaluates them according to defined criteria and automatically determines an optimal option.

The optimal option may be the one that provides the most efficient use of available physical space, minimises the consumption of packaging materials, reduces the number of packaging units used, meets transport-safety requirements, or satisfies other criteria established by the system rules.

After determining the optimal option, the system allows the user to review one or more alternative placement options that also meet the established constraints and can be implemented in the physical environment.

The system controls the feasibility of the user’s choice by automatically checking whether the selected option complies with the geometric parameters of material objects, the parameters of physical space, and other constraints used in modelling. If the user selects an option that does not allow complete or correct placement of material objects, the system automatically blocks the choice or offers the closest feasible alternatives.

In particular, the system may allow the selection of larger packaging, another geometric form, several packaging units, or other feasible placement options provided that all material objects can be physically placed according to the established rules.

The system automatically updates the digital placement model when the composition of objects, the parameters of physical space, or user actions change. When material objects are added, removed, or replaced, the system re-analyses the available

physical space and automatically generates an updated spatial-placement option based on the new input data.

The system enables interactive user interaction with the digital twin by changing the position of individual objects, selecting alternative stacking options, or changing the type of packaging used. When the user makes changes, the system automatically checks whether the proposed option can be implemented, taking into account object geometry, available space, and established constraints.

If the proposed changes are feasible, the digital twin is updated and used for further generation of instructions and execution of operations. If the proposed option cannot be physically implemented, the system automatically rejects it or offers the closest feasible alternatives.

Based on digital models of material objects, digital models of available physical space, and the results of automated analysis of placement options, the system forms a digital twin of the picking, placement, or packaging process.

The digital twin is a digital model of the future physical result of an operation. It contains information about the set of material objects, their spatial positions, orientation, placement sequence, packaging used, and other parameters required to implement the process. The digital twin may be formed before physical operations begin and used to analyse, visualise, verify, approve, or optimise modelling results.

The system can generate one or more digital twins for different placement options, followed by comparison and selection of the most suitable option. Based on the generated digital twin, the system automatically creates control instructions for picking, placement, packaging, transport, or other processing of material objects.

Control instructions are generated according to the spatial model of object placement, the sequence of operations defined by the system, and established technological or logistics rules. The system automatically determines the order of operations and forms the sequence of actions required to achieve the result represented by the process digital twin.

To keep the digital twin up to date, the system receives and processes feedback from the physical execution of operations with material objects. Feedback may come

from users, enterprise employees, automated identification tools, sensor systems, scanning devices, measuring equipment, robotic systems, transport systems, or other data sources that monitor operations in the physical environment.

The system provides automatic dynamic adjustment of the digital twin based on data received during physical operations, changes in the parameters of material objects, characteristics of physical space, or other factors affecting process implementation. After new data are received, the system analyses their impact on the current state of the digital twin and determines whether it must be updated.

If deviations between the planned and actual process states are detected, the system automatically changes the digital model to keep it consistent with the current state of material objects and the physical environment. After the digital twin has been generated or adjusted, the system automatically transfers current control instructions to the performer involved in the relevant physical process.

Instructions may be transferred directly to enterprise employees, end users, automated control systems, robotic systems, transport systems, or other technical means that perform operations with material objects.

For example, the system receives the geometric characteristics of three objects and a container. The algorithm forms a feasible target configuration, determines the placement order, and visually indicates the position of the first object. If the worker places it with a displacement, but the object remains within the container and does not violate constraints, there is no need to require an exact return to the planned position. The system records the actually occupied area and rebuilds the positions of the next two objects.

This mechanism is fundamentally different from a static projection prompt. A static system repeats the initial template and treats any displacement as an error. A projective digital twin evaluates the meaning of the deviation: whether the target remains achievable, whether constraints remain satisfied, and whether a feasible residual plan exists.

Practical performance indicators may include operation duration, error rate, number of repacking operations, volume utilisation ratio, packaging-material

consumption, number of damaged items, ergonomic load, and training time for a new worker. Scientific validation of the concept requires comparison of at least three modes: work without prompts, a static digital instruction, and an adaptive projective twin.

Practical implementation of the concept requires compliance with a number of principles. Based on the analysis of European programmes, research projects, and modern approaches to Digital Twin development, a set of strategic, technical, and organisational recommendations can be formulated. Their implementation should support the transition from isolated digital models to interoperable, adaptive, and human-centred systems that can not only represent and predict the state of physical objects but also form and manage the achievement of a future physical result.

A primary condition for scalable use of digital twins is interoperability. Monolithic and isolated solutions limit model reuse, complicate data exchange, and create dependence on a specific technology provider. Therefore, Digital Twin architecture should include standardised interfaces, unified asset descriptions, including the Asset Administration Shell, open APIs, and mechanisms for interaction with European data spaces. This creates the basis for integrating local digital twins into federated manufacturing, energy, and infrastructure ecosystems.

The level of detail of a digital model should be defined according to the specific management task. Excessive accuracy does not always increase the practical value of a Digital Twin, but it requires additional sensors, computing resources, data-transfer channels, and maintenance costs. Therefore, the principle of minimum sufficient accuracy is proposed: the model should contain only the volume and level of data detail necessary for informed decision-making and safe control of the physical process.

When evaluating Digital Twin efficiency, it is necessary to consider not only the optimisation results of the physical system but also the digital environmental footprint of the technology itself. Energy costs of high-performance computing, artificial-intelligence algorithms, cloud infrastructure, and storage of large datasets should be compared with the resource, economic, and environmental effects achieved in the

physical environment. This approach corresponds to the European concept of interconnected digital and green transitions — the Twin Transition.

Data provenance traceability should be a mandatory component of a digital twin. Together with a modelling result or recommended decision, the system should provide information about the data source, time of receipt, accuracy, preprocessing method, degree of uncertainty, and limits of applicability of the relevant model. This improves the justification of decisions and reduces the risk of using digital-modelling results outside the conditions for which the model was developed and validated.

Cybersecurity should be ensured throughout the information and control loop: from the sensor, transmission channel, and data storage to the mathematical model, user interface, and actuator. The history of model versions, input data, automatically generated recommendations, operator decisions, and actually performed actions should also be retained. Such logging ensures system accountability and creates a basis for allocating responsibility among the developer, data provider, operator, and organisation that operates the digital twin.

In processes focused on creating a specific material result, it is appropriate to move from reactive to projective Digital Twin logic. Traditional logic mainly moves from the physical object to its digital representation and then to forecasting its behaviour. Projective logic begins with the formation of a digital model of a feasible target state, after which the method of achievement, control actions, sequence of physical operations, and mechanism for verifying the actual result are determined.

One of the central principles of a projective digital twin should be adaptive replanning. A minor deviation made by a worker, robot, or other actuator should not automatically require the system to return to the initial state. If the actual deviation does not violate safety, spatial, technological, or resource constraints and does not make the target impossible to achieve, the system should accept the current actual state as a new starting point. Only the uncompleted part of the trajectory is then rebuilt, while the already created feasible part of the physical result is preserved.

It is appropriate to provide one or more alternative projective digital twins. Each alternative should describe an interconnected “future physical result — method of

achievement" pair. Alternatives may be compared using a multi-criteria function that considers execution time, cost, energy consumption, material use, ergonomic load, safety, risks, and resilience to possible disruptions. If the criteria conflict, a set of Pareto-optimal solutions should be generated and the final choice should remain with an authorised user.

Feedback between the digital model and the physical process should be formalised using sensors, machine-vision cameras, RFID tools, weight sensors, or other available information sources. The data obtained should be used to determine the actual position of objects, verify completion of individual operations, detect deviations, and automatically update the uncompleted part of the projective digital twin.

In accordance with the human-centred Industry 5.0 approach, a digital twin should not remove people from the decision-making process but expand their capabilities. The system should propose recommended scenarios and explain the criteria for their selection while allowing the worker or operator to choose another feasible option, change priorities, or adjust the sequence of operations.

Changes proposed by the user should be automatically checked for physical feasibility. If a worker chooses a personal option for spatial placement, packaging, or execution of an operation, the system should verify geometric parameters, object compatibility, resource constraints, stability, safety, and achievability of the final result. Physically impossible or unsafe decisions should be blocked, with the reason explained and the closest feasible alternative generated at the same time.

An important development direction is controlled self-learning of the projective digital twin. This requires accumulating data on generated scenarios, user choices, actual trajectories, deviations, replanning cases, and final performance indicators. If a particular alternative scenario regularly provides a better result under comparable conditions, the system may gradually increase its priority. At the same time, changes in algorithmic priorities should be transparent and verifiable and should not automatically reinforce incorrect or unsafe actions.

Thus, practical implementation of a projective digital twin requires a combination of three interconnected components: technological interoperability,

adaptive control of the physical process, and preservation of meaningful human control. This combination makes it possible to align the proposed concept with Industry 5.0 principles and transform the digital twin from a tool for observation and forecasting into an instrument for forming, implementing, and verifying a future physical result.

A step-by-step picking scenario begins with identification of the order, packaging, and available work area. After geometric and technological characteristics are obtained, the system eliminates incompatible objects and prohibited orientations, generates several feasible configurations, evaluates them, and selects a placement sequence. The worker is not shown the entire model at once but receives a contextual instruction for the next action. After each step, a camera or another sensor confirms the identity and position of the object and compliance with constraints, reducing the accumulation of unnoticed errors.

If the first object is placed with a displacement, the algorithm first classifies the deviation. A geometrically acceptable displacement is accepted as a new condition; the occupied area is recorded, and the residual problem is solved for the objects not yet placed. A deviation that creates instability, blocks access, or violates compatibility is not accepted: the system explains the reason and proposes a corrective action. Thus, adaptability does not mean weaker control but a differentiated response to acceptable and dangerous changes.

Another scenario concerns a change in order composition during execution. After an object is added, the system should not automatically cancel all completed work. It first checks whether the new object can be included in the remaining space without violating constraints. If this is impossible, options for local repacking, changing packaging, or splitting the order are compared. Each option is assessed by additional time, material costs, risk of damage, and convenience for further logistics.

For palletising, the criteria are supplemented by stack stability, permitted load, unloading sequence, and centre of mass. A projective twin can model not only the final configuration but also intermediate states, because a physically stable final result does not guarantee a safe trajectory for creating it. This illustrates a general principle: feasibility of the target state and feasibility of the transition process are different conditions that should be checked simultaneously.

The effectiveness of the adaptive loop should be assessed using a system of indicators: the share of operations without repeated execution, average time from detecting a deviation to updating the plan, percentage of successfully accepted feasible deviations, number of unsafe decisions blocked before execution, and relative change in resource costs. Cognitive load and user trust should also be measured, because a complex but unclear recommendation may be systematically ignored.

For Ukraine, the introduction of digital twins should be linked not to mechanical copying of individual European platforms but to the formation of a compatible institutional and information base. Priorities should include standardised asset models, access to high-quality data, staff training, cybersecurity, and the ability to connect to European federated ecosystems.

The greatest short-term effect is possible in the recovery of critical infrastructure, energy, construction, transport, and logistics. Projective digital twins make it possible to compare alternative future states of an object, assess resources and risks, and form a sequence of physical actions before work begins. This is especially important when financing, materials, and time are limited.

Ukraine's participation in Digital Europe and Horizon Europe creates an opportunity not only to receive funding but also to include Ukrainian organisations in common standards, research networks, and demonstration projects. At the same time, practical implementation should be accompanied by assessment of economic feasibility, the digital footprint, data availability, and the organisation's readiness to change its own processes.

The first perspective is the integration of projective twins into federated ecosystems. A local twin of a work operation can use asset models provided through AAS, receive data from a corporate data space, and transfer aggregated results to a production-line twin. This makes it possible to combine detailed physical execution with system-level planning.

The second perspective is the use of generative and causal artificial intelligence. Generative models can propose alternative configurations, but their results must be checked against physical and regulatory constraints. Causal models can explain why a particular action leads to a result, which is especially important for safe control.

The third perspective is integration with augmented reality and spatial interfaces. Visual projection or AR overlay reduces the gap between the digital model and the work area. However, the interface should be an implementation tool rather than a substitute for the model: without a target state, feasibility rules, and adaptation, visualisation remains an electronic instruction.

The fourth perspective is learning from execution history. A database can accumulate generated twins, actual trajectories, causes of deviations, worker decisions, and final performance indicators. This creates a basis for refining criteria, forecasting complexity, personalising instructions, and identifying systemic constraints.

The fifth perspective is expansion from local operations to construction, maintenance services, medical logistics, emergency response, and urban infrastructure. Common features are the existence of a material result, a set of feasible scenarios, physical constraints, and the need to adapt the plan using execution data.

In the European context, the concept is consistent with Industry 5.0 if automation does not remove the worker from the loop but strengthens the ability to make safe decisions. The system should explain the reason for replanning, show uncertainty, allow recommendations to be rejected, and learn only from verified results.

Legal responsibility requires separate research. If a target state is generated by an algorithm, a worker follows a visual instruction, and the result causes harm, responsibility must be allocated among the model developer, data provider, operator, and organisation. Therefore, logging versions, decisions, and interventions is part of a scientifically grounded architecture rather than merely a technical function.

Further empirical validation should cover the accuracy of physical-state reconstruction, speed of alternative generation, frequency and effectiveness of replanning, worker cognitive load, resilience to incomplete data, and the digital energy footprint. Such experiments will make it possible to identify the conditions under which a projective twin has advantages over a conventional decision-support system.

For practical implementation in Ukraine, a phased model is appropriate. The first stage is an audit of the process, data, and economic problem; the second is a pilot in a limited area with measurable indicators; the third is model standardisation and integration with corporate systems; and the fourth is scaling and connection of external

participants. Transition between stages should depend on achieving criteria rather than on the formal completion of equipment procurement.

A policy of technological neutrality is especially important. Public and corporate customers should define requirements for interoperability, security, data portability, and model verification but avoid unjustified commitment to one format or provider. This reduces long-term dependence and facilitates integration of Ukrainian solutions with European data spaces.

Investment assessment should combine financial and non-financial indicators. Financial indicators include reductions in downtime, defects, material costs, and cycle time; non-financial indicators include improved safety, resilience, decision transparency, and the ability to train personnel. The costs of digital infrastructure, cyber protection, data maintenance, and revalidation after changes in the physical system should be considered separately.

A pilot implementation of a projective digital twin should be organised as a controlled quasi-experiment. First, baseline process indicators are recorded over a representative period without digital support: operation duration, error frequency, non-productive losses, number of repeated actions, and worker load. After implementation, the same indicators are measured for a static digital instruction and an adaptive projective twin. Operations of comparable complexity should be compared, because a simple comparison of averages without considering task composition may create a false impression of technology effectiveness.

The evaluation methodology should consider not only the average result but also the variation of indicators and the stability of the effect. If time reduction is achieved only by experienced operators or under ideal data quality, the solution cannot be considered ready for scaling. Therefore, results should be grouped by operation complexity, worker experience, frequency of deviations, and completeness of sensor data. Cases in which the system could not form a feasible plan or transferred the decision to a person should be analysed separately. This makes it possible to identify the actual limits of model applicability.

Economic justification should be based on total cost of ownership rather than only on the price of the initial software. Costs include sensors, computing

infrastructure, integration, preparation of digital models, cybersecurity, staff training, maintenance of reference data, and revalidation after changes in the physical process. Benefits include reductions in defects, downtime, material consumption, and time, as well as lower damage risk and lower costs of training new workers. A scaling decision should be based on the total discounted effect and sensitivity analysis of key assumptions.

Criteria for pilot readiness for industrial use should include confirmed state-reconstruction accuracy, stable economic effect, acceptable replanning time, absence of critical safety violations, manageable model versions, and positive user evaluation. If at least one critical criterion is not met, scaling should be postponed and the root cause removed. Such a staged approach reduces the risk of turning the digital twin into a formally implemented but practically unused information system.

After the pilot is completed, the external validity of the results should also be checked — the possibility of transferring them to other sites, enterprises, or types of operations. The conditions under which the effect was achieved should be recorded: object characteristics, data quality, staff qualifications, technical environment, and accepted constraints. Scaling without such a description creates a risk that a successful local model will be used outside its area of applicability. Therefore, the pilot result should include not only the value of an economic indicator but also a formalised profile of the conditions under which the solution can be reproduced.

The study has shown that Digital Twin in the European Union is moving from local digital replicas to federated, cross-sectoral, and socially significant ecosystems. Destination Earth and the European Digital Twin Ocean demonstrate scenario modelling of natural systems; TwinEU demonstrates interoperability of infrastructure twins; MODAPTO demonstrates distributed intelligence in manufacturing; and Change2Twin demonstrates mechanisms for spreading the technology among SMEs.

The European approach is defined not only by technological scale but also by the Industry 5.0 regulatory framework. Human-centricity, sustainability, and resilience become criteria for architecture and evaluation. At the same time, problems of semantic interoperability, data quality, model validation, cybersecurity, economic feasibility, and responsibility remain.

A scientific gap has been identified between representing or forecasting a state and the integrated formation of a future physical result together with the method for achieving it. To address this gap, the concept of a projective digital twin is proposed — a model of the target state, transition trajectory, resources, constraints, risks, criteria, control actions, and adaptive feedback.

The scientific novelty lies in functionally identifying a class of digital twins focused not only on representation and forecasting but on the controlled creation of a physical result. The key property is the ability to accept an admissible actual deviation, record the part of the state already created, and rebuild the uncompleted part of the trajectory.

Practical feasibility is demonstrated using the example of spatial placement of material objects with visual guidance and adaptive replanning. Further research should focus on experimental validation, development of metrics, integration with standard information models, and identification of conditions for safe use in human-centred manufacturing systems.

REFERENCES FOR SUBSECTION 4.1

1. European Commission. Destination Earth (DestinE) — digital model of the Earth. URL: https://digital-strategy.ec.europa.eu/en/policies/destination-earth (дата звернення: 30.07.2026).

2. European Commission. European Digital Twin Ocean. URL: https://research-and-innovation.ec.europa.eu/research-area/environment/oceans-and-seas/european-digital-twin-ocean-european-dto_en (дата звернення: 30.07.2026).

3. European Commission. Digital Europe Programme. URL: https://digital-strategy.ec.europa.eu/en/activities/digital-programme (дата звернення: 30.07.2026).

4. European Commission, Directorate-General for Research and Innovation. Industry 5.0: Towards a sustainable, human-centric and resilient European industry. Luxembourg: Publications Office of the European Union, 2021.

5. Nativi S., Mazzetti P., Craglia M. Destination Earth: Survey on “Digital Twins” technologies and activities, in the Green Deal area. JRC Technical Report JRC122457. 2020.

6. Kritzinger W., Karner M., Traar G., Henjes J., Sihn W. Digital Twin in manufacturing: A categorical literature review and classification. IFAC-PapersOnLine. 2018. Vol. 51(11). P. 1016–1022. DOI: 10.1016/j.ifacol.2018.08.474.

7. Fuller A., Fan Z., Day C., Barlow C. Digital Twin: Enabling Technologies, Challenges and Open Research. IEEE Access. 2020. Vol. 8. P. 108952–108971. DOI: 10.1109/ACCESS.2020.2998358.

8. Rasheed A., San O., Kvamsdal T. Digital Twin: Values, Challenges and Enablers From a Modeling Perspective. IEEE Access. 2020. Vol. 8. P. 21980–22012. DOI: 10.1109/ACCESS.2020.2970143.

9. ISO 23247-1:2021. Automation systems and integration — Digital twin framework for manufacturing — Part 1: Overview and general principles.

10. IEC 63278-1:2023. Asset Administration Shell for industrial applications — Part 1: Asset Administration Shell structure.

11. European Commission. Common European data spaces. URL: https://digital-strategy.ec.europa.eu/en/policies/data-spaces (дата звернення: 30.07.2026).

12. European Commission. Horizon Europe — Cluster 4: Digital, Industry and Space. URL: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-4-digital-industry-and-space_en (дата звернення: 30.07.2026).

13. CORDIS. Change2Twin: Digital Twin for every manufacturing SME! Project information and results. URL: https://cordis.europa.eu/project/id/951956.

14. CORDIS. MODAPTO: Modular Manufacturing and Distributed Control via Interoperable Digital Twins. Project 101091996. URL: https://cordis.europa.eu/project/id/101091996.

15. CORDIS. TwinEU: Digital Twin for Europe. Project 101136119. URL: https://cordis.europa.eu/project/id/101136119.

16. Muench S. et al. Towards a green & digital future. JRC Science for Policy Report JRC129319. Luxembourg: Publications Office of the European Union, 2022.

17. European Commission. Industry 5.0, a transformative vision for Europe: Governing systemic transformations towards a sustainable industry. 2022.

18. Jones D., Snider C., Nassehi A., Yon J., Hicks B. Characterising the Digital Twin: A systematic literature review. CIRP Journal of Manufacturing Science and Technology. 2020. Vol. 29. P. 36–52. DOI: 10.1016/j.cirpj.2020.02.002.

19. Tao F., Zhang H., Liu A., Nee A.Y.C. Digital Twin in Industry: State-of-the-Art. IEEE Transactions on Industrial Informatics. 2019. Vol. 15(4). P. 2405–2415. DOI: 10.1109/TII.2018.2873186.

20. Lu Y., Liu C., Wang K.I.-K., Huang H., Xu X. Digital Twin-driven smart manufacturing: Connotation, reference model, applications and research issues. Robotics and Computer-Integrated Manufacturing. 2020. Vol. 61. 101837. DOI: 10.1016/j.rcim.2019.101837.

21. Barricelli B.R., Casiraghi E., Fogli D. A Survey on Digital Twin: Definitions, Characteristics, Applications, and Design Implications. IEEE Access. 2019. Vol. 7. P. 167653–167671. DOI: 10.1109/ACCESS.2019.2953499.

22. Semeraro C., Lezoche M., Panetto H., Dassisti M. Digital twin paradigm: A systematic literature review. Computers in Industry. 2021. Vol. 130. 103469. DOI: 10.1016/j.compind.2021.103469.

23. Errandonea I., Beltrán S., Arrizabalaga S. Digital Twin for maintenance: A literature review. Computers in Industry. 2020. Vol. 123. 103316. DOI: 10.1016/j.compind.2020.103316.

24. European Commission Joint Research Centre. MyDigitalTwin: Exploratory Research report. JRC129917. 2022.

25. Craglia M., Scholten H. (eds.). Digitranscope: The governance of digitally-transformed society. JRC Science for Policy Report. Luxembourg, 2021.

26. Monti A., Dolley B., Palensky P., Parisot A. Building a Digital Twin for European Energy Infrastructure: The Role of Open Source. IEEE Electrification Magazine. 2024. Vol. 12. DOI: 10.1109/MELE.2024.3423168.

27. Thwe M.M., Ştefanov A., Rajkumar V.S., Palensky P. Digital Twins for Power Systems: Review of Current Practices, Requirements, Enabling Technologies, Data Federation, and Challenges. IEEE Access. 2025. Vol. 13. DOI: 10.1109/ACCESS.2025.3580055.

28. European Commission. Industry 5.0 Community of Practice: Final report of the pilot phase 2023–2024. Brussels, 2024.

29. European Commission. ERA industrial technologies roadmap on human-centric research and innovation for the manufacturing sector. Publications Office of the European Union, 2024. DOI: 10.2777/0266.

30. Матеріали авторської розробки «Спосіб проекційного керування просторовим розміщенням матеріальних об’єктів з адаптивним перепланування». 2026.

31. European Commission. Data Governance Act. URL: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act (дата звернення: 30.07.2026).

32. European Commission. Data Act. URL: https://digital-strategy.ec.europa.eu/en/policies/data-act (дата звернення: 30.07.2026).

33. European Commission. AI Act: Regulatory framework for artificial intelligence. URL: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (дата звернення: 30.07.2026).

34. European Commission. NIS2 Directive: securing network and information systems. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (дата звернення: 30.07.2026).

35. European Commission. Cyber Resilience Act. URL: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (дата звернення: 30.07.2026).

36. ISO/IEC 30173:2023. Digital twin — Concepts and terminology. Geneva: International Organization for Standardization, 2023.

4.2. Unified Digital Platform for Suburban and Intercity Bus Transport Based on the PSO Model with Integrated Anti-Corruption Mechanisms

Anton FESENKO
Maksym DEMYDENKO
National University Yurii Kondratiuk Poltava Polytechnic

The current state of Ukraine's suburban and intercity passenger bus transport

market is characterized by a large shadow economy, fragmented service delivery and low passenger comfort.

The traditional model – where operators run purely on a commercial basis – leads to the degradation of socially critical yet low-margin routes, particularly in rural areas. Direct cash transactions with drivers make it impossible to accurately track passenger flows, ensure full tax compliance or provide transparent state compensation for subsidized passenger categories.

In the context of European integration and post-war infrastructure reconstruction, Ukraine's strategic priority is transitioning to the European PSO (Public Service Obligation) model. Under this model, the state procures transport services via open tenders, paying operators a fixed fee based on transport work completed rather than ticket sales. However, rolling out the PSO model amid severe corruption risks demands strict oversight, as conventional inspection methods reliant on manual field audits fall short due to human collusion.

Addressing this challenge requires developing a comprehensive information system built on the Zero Trust Architecture paradigm (Zero Trust Architecture, 2020), where trip execution verification and passenger counting are automated through the cross-monitoring of digital ticket sales, geospatial data and hardware telemetry.

The aim of this study is to design the architecture and develop a software model for a unified digital suburban and intercity bus transport platform that automates PSO tender management and ticketing while providing algorithmic, anti-corruption trip execution control.

To achieve this aim, the following research objectives were set:

- Design a software architecture that segments business logic across isolated portals: passenger, carrier, state regulator and bus station;

- Develop a hybrid passenger identity verification model (with potential integration into the Diia application) to ensure targeted provision of social fare discounts and eliminate speculation;

- Formulate mathematical anomaly detection algorithms based on the fusion of Automated Passenger Counting (APC) sensor data and route geofencing telemetry.

The contemporary suburban and intercity passenger transport market in Ukraine

operates under heavy fragmentation and technological obsolescence. Historically, cash handed directly to the driver has remained the predominant payment method on regional routes. This paradigm fosters a widespread shadow economy with corrosive consequences across the transport ecosystem: for the state, compliant carriers and passengers alike.

State regulatory bodies lack the tools for objective passenger-flow analytics. Operators self-report passenger numbers, opening substantial leeway for manipulation: companies underreport actual revenues to evade taxes while inflating the number of subsidized passengers carried to extract ungrounded state budget reimbursements. Under these conditions, any infrastructure planning or route network optimization relies on distorted baseline data.

The purely commercial orientation of the market drives operators to concentrate resources strictly on high-yield corridors, such as connections between major urban centers. Conversely, routes serving remote rural communities are operated on a residual basis – relying on obsolete rolling stock that fails environmental and accessibility standards, paired with critically low service frequencies. This systemic issue undermines citizens' fundamental right to mobility.

While several disparate commercial ticketing platforms exist on the market, they do not resolve the sector's fundamental problem. Existing systems are built on the premise of complete trust in the operator, assuming that drivers or conductors will diligently use mobile validators or handheld terminals to register every passenger. However, as transit experience in transition economies demonstrates, whenever a financial incentive exists – namely, the opportunity to pocket cash – the human factor invariably becomes the weakest link. Mere ticketing digitization without hardware-level oversight and a Zero Trust paradigm simply automates chaos without eliminating underlying corruption risks.

Resolving these structural failures requires overhauling the very model of engagement between the state and transport operators: specifically, transitioning to the European public service framework.

To overcome this regional transit crisis, the strategic vector for Ukraine's transport infrastructure is the transposition of European public passenger transport

service rules grounded in the PSO framework under Regulation (EC) No 1370/2007 (Public Service Obligation) (Regulation (EC) No 1370/2007).

The core premise of PSO is that ensuring population mobility is recognized as a social obligation of the state rather than a purely commercial activity. Instead of an operator generating revenue solely through ticket sales – a model that renders rural routes unprofitable – the state or local transport authority acts as the sole contracting authority. The transport authority conducts a competitive tender and awards a contract under which the carrier receives a fixed fee for completed "transport work" (actual vehicle-kilometers operated according to the published timetable).

In this paradigm, all ticket revenue is consolidated into a single digital platform (deposited directly into the organizing authority's accounts), stripping the carrier of any financial incentive to conceal passenger volumes or collect unrecorded cash. However, the viability of such a framework hinges entirely on the state's capacity to audit contract compliance accurately: verifying whether the scheduled trip was actually executed, adhered to the timetable, and serviced designated stops.

Yet, despite adopting a Zero Trust paradigm at the vehicle level (deploying hardware sensors to monitor onboard crew behavior), the information system operates within a broader socio-political context. This exposes the platform to insider threat vectors originating from executive leadership, tender evaluation committees and system administrators.

According to secure system design methodologies, software architecture alone cannot eliminate the corrupt intent of administrative personnel. Its function, however, is to minimize the attack surface and enforce an immutable digital audit trail.

The primary administrative threat vectors and their architectural mitigations include:

1. Tender specification tampering. Attack scenario: an official configures tender requirements within the system (e.g., passenger capacity thresholds, environmental standards) tailored specifically so only a predetermined operator can qualify. System mitigation: operating deterministically, the platform cannot evaluate subjective corrupt intent when parameters are defined. However, the system maintains an immutable, cryptographically verifiable log of tender creation and

revision history, enabling anti-corruption oversight bodies (such as NABU and SAPO) to perform retrospective audits on discriminatory criteria.

2. Unauthorized penalty waivers. Attack scenario: hardware sensors log a non-compliance event (e.g., unticketed passengers), triggering the platform to issue an automated fine. A corrupt official with administrative privileges manually voids the penalty in the system. Architectural mitigation: the platform utilizes the Apache Kafka event broker as an immutable event-sourced store. Administrators are structurally prevented from deleting violation records from the database; they can only append a new compensation event documenting the cancellation rationale, permanently bound to their digital signature. This pulls the corrupt act out of the shadows and into an auditable, transparent plane.

Engineering this information system demands a fine balance between high throughput, operational resilience and deployment simplicity. For a regional Minimum Viable Product (MVP), adopting a traditional microservices architecture often introduces excessive infrastructure overhead, network latency penalties and complex distributed transaction integrity challenges.

To implement the platform's backend, the "Modular Monolith" architectural pattern (Architect Modern Web Applications with ASP.NET Core and Azure) based on the .NET 10 platform was selected. This approach involves deploying the system physically as a single server process with a unified PostgreSQL database, while enforcing strict logical separation of code into independent bounded contexts according to Domain-Driven Design (DDD) principles.

The system architecture encapsulates the following isolated modules:

- Ticketing Module: responsible for seat reservations, ticket sales and multimodal route calculation;
- Tender Management Module: handles PSO contract administration, route publication and the registry of carriers' assigned fleets;
- IoT Engine: a high-throughput module designed for ingesting and analyzing geospatial telemetry alongside hardware sensor data.

Inter-module communication occurs exclusively via strictly defined in-code

interfaces or through an event broker.

Upon successful completion of the pilot project in Poltava Oblast and subsequent nationwide rollout, the modular monolith architecture enables seamless extraction of any domain (such as the IoT engine) into a standalone microservice.

The user interface architecture is tailored to the distinct needs of system actors while minimizing overall development time. Rather than engineering numerous fragmented front-end applications, the system is streamlined into two core portals developed using Blazor technology.

The first application is a universal passenger portal and self-service terminal. Built on a responsive design pattern, it serves a dual role by addressing the requirements of both online users and passengers purchasing tickets on-site.

Its mobile mode functions as a standard web application in smartphone browsers, allowing passengers to select routes and generate digital QR tickets. The kiosk mode – running off the identical codebase – operates on hardware self-service terminals deployed across bus stations. This entirely removes the overhead of developing and maintaining a dedicated ticket clerk workstation interface.

To implement the MVP and ensure maximum accessibility (particularly for elderly passengers), the authorization flow was radically streamlined. Rather than introducing complex integrations with state registries or the Diia platform, a user or terminal operator needs only to enter a full name and phone number to complete a ticket purchase.

The second application is the state regulator control dashboard. This portal is designed exclusively for dispatchers, auditors and transport authority officials. It serves as the primary monitoring hub, consolidating all platform telemetry and analytics.

Because the dashboard demands real-time rendering of large, dynamic datasets, it was built on the Blazor Server architecture. In this model, all UI processing executes on the server, while the client browser receives instantaneous DOM-tree updates over a persistent binary connection. This allows the system to push critical alerts directly to an inspector's screen the exact millisecond a background worker detects passenger-count discrepancies, completely bypassing the need for complex client-side polling

mechanisms.

A major hurdle in ensuring rural mobility is the economic unfeasibility of running direct routes between every settlement. Traditional commercial models neglect this constraint, forcing travelers to coordinate their own transfers. The proposed system resolves this algorithmically by adopting a hub-and-spoke network topology.

In this topology, major bus stations (such as the central bus station in Poltava) act as transit hubs, while feeder routes serving surrounding rural communities function as spokes. The integrated ticketing module automatically constructs multimodal route itineraries. When a passenger searches for a route from "Village A to Village B," the platform traverses the graph of available PSO services to produce an itinerary featuring a guaranteed transfer in Poltava, factored against transfer buffer times.

Instead of navigating fragmented transactions, the passenger receives a single unified digital ticket. From the perspective of the state as the contracting authority under PSO agreements, this architecture maximizes cost-effectiveness: it eliminates the need to subsidize underutilized direct routes between rural settlements while securing consistent patronage flows across central transit hubs.

Graph-traversal and route-planning algorithms rely on complex, aggregation-heavy SQL queries executed against the PostgreSQL database, continuously cross-referencing thousands of timetables, intermediate stops and real-time seat inventories. During peak load windows – such as early morning hours when ticket purchasing spikes – this generates acute database contention.

To maintain high availability and low read latency, the system implements a multi-tier caching strategy powered by the hybrid caching framework built into .NET 10, backed by Redis as the distributed tier.

This pattern establishes a two-level (L1/L2) data access architecture. The L1 tier (in-memory cache) serves ultra-low-latency lookups for high-frequency routes directly from local server RAM. The L2 tier (distributed Redis cache) keeps cache states coherent across backend application instances, offloading timetable datasets from the primary PostgreSQL instance.

Traditional dispatch and fare-collection monitoring systems rely on a presumption of trust. The state or contracting authority trusts the carrier to operate the service according to the timetable, while the carrier trusts the driver or conductor to ensure every passenger holds a valid ticket. As established in previous sections, the persistence of cash transactions renders this reliance on trust an inevitable driver of corruption and state budget leakages during PSO subsidy disbursements.

To address this fundamental flaw, the architecture of the proposed platform is anchored in the Zero Trust paradigm. In cybersecurity, this principle translates to "never trust, always verify." In the domain of passenger transport, it manifests as the following operational axiom: the information system rejects any human-generated or manually entered data unless it is corroborated by hardware telemetry.

The backbone of this architecture is the platform's integration with onboard Internet of Things (IoT) hardware (Buyya et al., 2016), specifically Automated Passenger Counting (APC) systems.

Rather than relying on ticket validation counts from onboard card readers – which a driver can easily disable – system deploys optical sensors mounted above every vehicle doorway. Modern APC sensors leverage 3D stereoscopic cameras or Time-of-Flight (ToF) technology. These devices reliably register doorway threshold crossings, determine directional movement (boarding vs. alighting) and distinguish adult passengers from children or bulky luggage by analyzing thermal and volumetric profiles.

Passenger volume metrics alone hold little value without spatial and temporal context. Consequently, the onboard hardware architecture aggregates three independent data streams via a unified IoT gateway:

1. APC metrics: the precise count of passengers boarding and alighting.

2. Door status: an open/closed binary signal pulled directly from the bus telemetry.

3. GPS positioning: high-precision vehicle coordinates and instantaneous velocity.

The onboard gateway continuously ingests these data points, packages them into lightweight JSON payloads and transmits them at high frequency (e.g., every 5-10

seconds or triggered by a "door opened" event) across a 4G/LTE cellular network to the central platform API.

A critical architectural consideration is the full autonomy of the onboard hardware. The driver lacks physical access to disconnect or power down sensors without breaking tamper-evident seals or de-energizing the entire system – an action instantly flagged by the backend as a critical incident, automatically freezing payment disbursement for the service.

The platform's mathematical engine executes as a background worker, continuously cross-referencing incoming telemetry against geospatial coordinates. Any logical discrepancy across these data streams is classified as an attempted fraud vector. Below are three primary algorithmic "traps" embedded within the system architecture.

1. Fare Evasion Trap (Unticketed Passenger Detection). This algorithm identifies the classic scenario where a driver accepts cash directly from a passenger without requiring them to scan a ticket. The system treats each bus stop as a distinct episode defined by the door-open interval.

The algorithm cross-references the number of individuals physically boarding the cabin against the volume of digital tickets validated within that exact time window. Only a minimal tolerance threshold is permitted (e.g., 1-2 passengers) to account for infants carried in arms or edge cases in optical sensor performance. If physical boardings exceed scanned tickets beyond this allowable threshold, the background worker instantly triggers a fare-evasion incident.

An additional layer of validation monitors residual onboard capacity: if the calculation indicates that passengers remain onboard at the final terminus after all passengers should have alighted, it serves as an indicator that the driver intentionally obstructed the sensor during egress to conceal unticketed riders.

2. Equipment Sabotage/Tampering Trap. Under stringent hardware oversight, drivers may attempt to physically incapacitate the APC sensor – for example, by taping over the camera lens or obstructing its field of view. This algorithm detects sabotage through a logical paradox, using the transaction log as definitive proof.

The system triggers when the optical sensor reports zero physical boardings, yet the central server records successful ticket validations from the onboard validator. This yields a physical impossibility: tickets are being scanned by passengers who, by sensor records, never boarded the vehicle. Detecting this pattern automatically flags the vehicle as hardware-compromised, establishing formal grounds to immediately suspend PSO subsidy disbursements for that route pending a technical audit.

3. Off-Route/Unauthorized Stop Trap. To collect unrecorded cash, drivers frequently make unauthorized stops outside designated bus stations and stops – at road intersections, shoulders or commercial plazas. Route compliance monitoring is enforced by constructing virtual geofences and calculating proximity based on GPS coordinates.

The algorithm continuously correlates the bus's real-time geolocation with its door-status telemetry. For each authorized stop in the route manifest, a designated buffer radius is defined (e.g., a 50-meter geofence centered on the boarding platform). If the telemetry registers door actuation outside all authorized geofences, the platform classifies the event as an unauthorized passenger boarding or alighting maneuver.

Processing continuous telemetry streams (GPS coordinates, door statuses, APC sensor metrics, validator transactions) across hundreds of buses concurrently places extreme load on the server infrastructure. To ensure platform resilience and scalability, the backend architecture incorporates the Apache Kafka distributed event streaming platform. Within this system, Kafka performs two mission-critical functions: it guarantees the mathematical precision of analytical algorithms and produces a tamper-proof digital audit trail.

The core challenge of ingesting IoT telemetry within multithreaded systems is the risk of out-of-order event delivery. Due to cellular network latency variations, signals dispatched from onboard hardware may reach the server with minor timing skews and be consumed by background workers at differing rates. For instance, if the system processes a "5 passengers boarded" event prior to processing an out-of-sequence "doors opened" event, the mathematical model would generate a false-positive fraud alert.

Traditional message brokers (such as RabbitMQ) do not guarantee strict ordering semantics under parallel consumer pool workloads. Apache Kafka resolves this structural constraint at the architectural layer via partition key routing.

When streaming any telemetry event, the system designates the bus unique identifier as the partition key. This guarantees that all events originating from a given vehicle (movement, stop dwell, ticket scans, door status transitions) are consistently routed to the same partition and processed sequentially by consumers in the exact chronological order of their physical occurrence. Consequently, the anomaly detection algorithms described in the previous section receive a fully coherent, chronologically validated context for real-time analysis.

The second – and from a public administration standpoint, paramount – function of Apache Kafka is the mitigation of the administrative threat vectors outlined in the opening section (such as unauthorized penalty voids and corrupt influence on regulatory officials).

Conventional relational databases remain vulnerable to tampering by privileged accounts or database administrators. A corrupt official could technically execute an UPDATE or DELETE query to expunge records of carrier infractions or void automatically calculated penalties without leaving a trace.

Apache Kafka is grounded in the Event Sourcing paradigm and operates as an append-only transaction log [5]. Data written to Kafka is inherently immutable.

Within the developed platform, every critical state transition – such as an algorithm flagging unticketed passengers and issuing a fine, or an administrator manually altering the status of that fine – is concurrently published as an independent event to a dedicated, isolated topic. If an administrator attempts to void a sanction, the system does not delete the infraction entry; instead, it appends a new compensating event cryptographically bound to the administrator's digital signature and timestamped down to the exact millisecond.

REFERENCES FOR SUBSECTION 4.2

1. Regulation (EC) No 1370/2007 of the European Parliament and of the Council of 23 October 2007 on public passenger transport services by rail and by road and repealing Council Regulations (EEC) Nos 1191/69 and 1107/70. Official Journal of the European Union. [Електронний ресурс]. Режим доступу: https://eur-lex.europa.eu/eli/reg/2007/1370/oj/eng

2. Architect Modern Web Applications with ASP.NET Core and Azure. Microsoft Docs [Електронний ресурс]. Режим доступу: https://learn.microsoft.com/en-us/dotnet/architecture/modern-web-apps-azure/

3. Zero Trust Architecture (NIST Special Publication 800-207). Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). National Institute of Standards and Technology [Електронний ресурс]. Режим доступу: https://www.nist.gov/publications/zero-trust-architecture

4. Internet of Things: Principles and Paradigms. Buyya, R., Dastjerdi, A. V. (Eds.). (2016).

5. The Log: What every software engineer should know about real-time data's unifying abstraction. Kreps, J. (2013) [Електронний ресурс]. Режим доступу: https://www.scribd.com/document/276130136/The-Log-What-Every-Software-Engineer-Should-Know-About-Real-time-Data-s-Unifying-Abstraction

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).

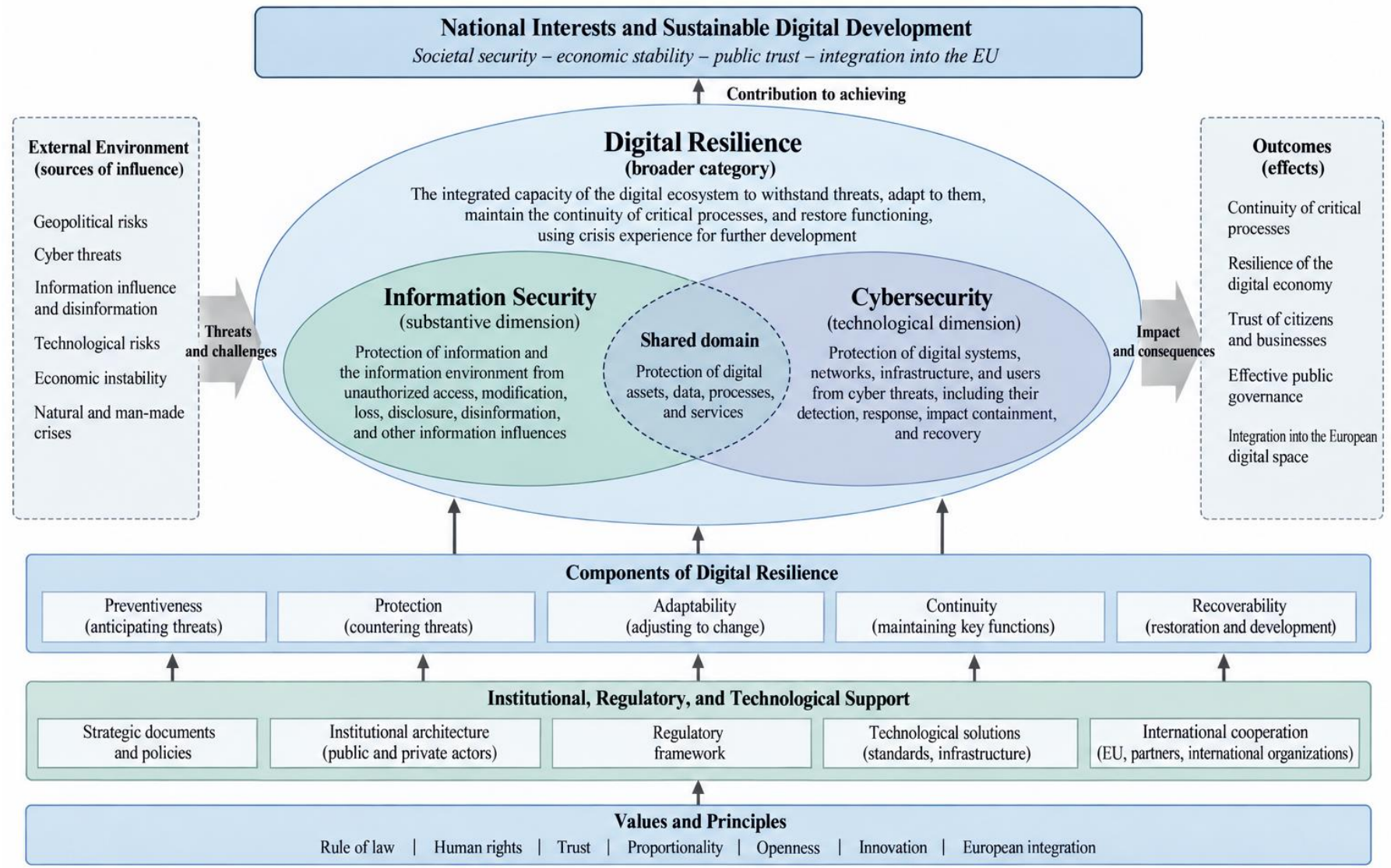


Fig. 4.4. Model of the relationship between the categories ‘information security’, ‘cybersecurity’ and ‘digital resilience’
Source: developed by the authors

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.

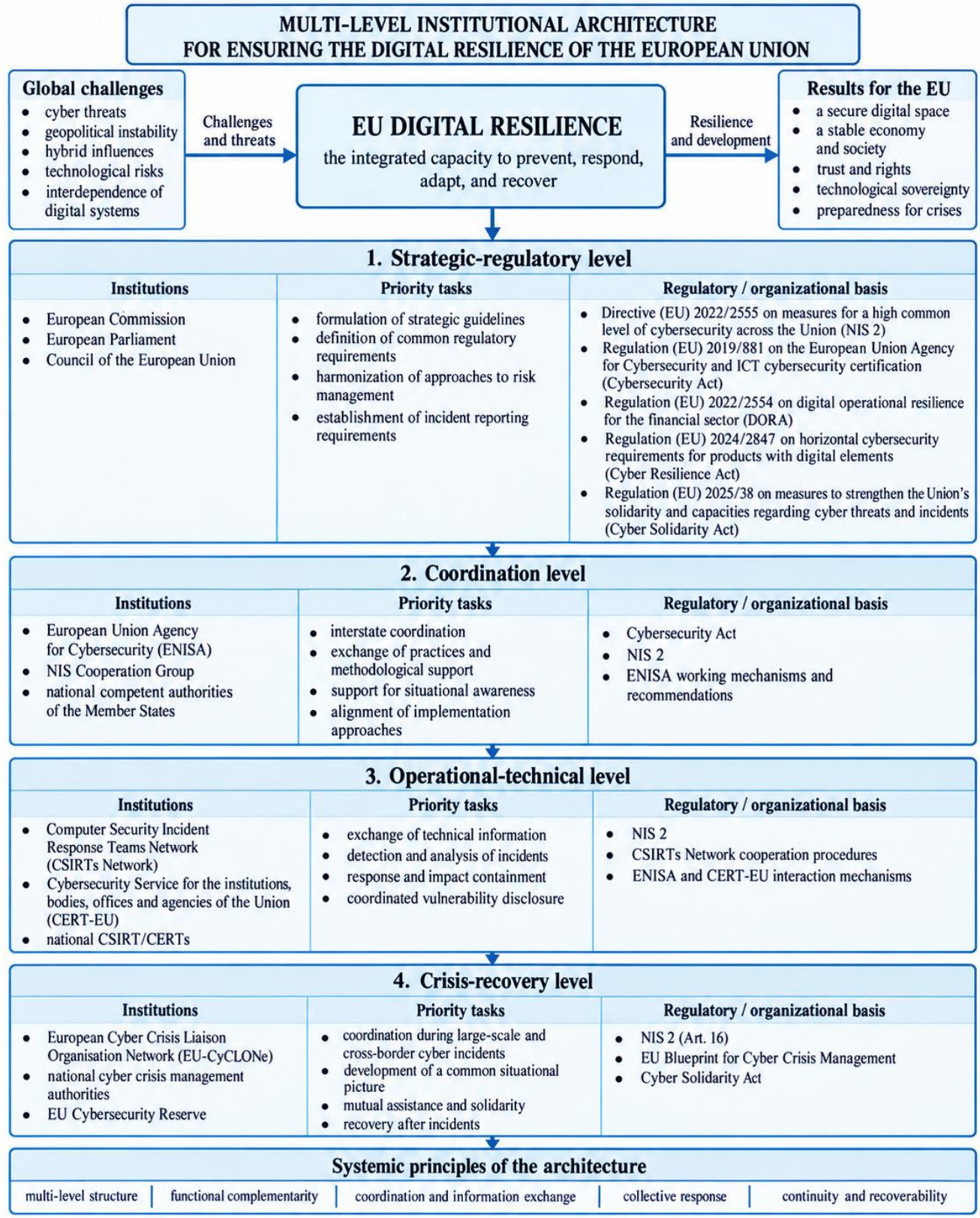


Fig. 4.5. Multi-level institutional architecture for ensuring digital resilience of the European Union

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.

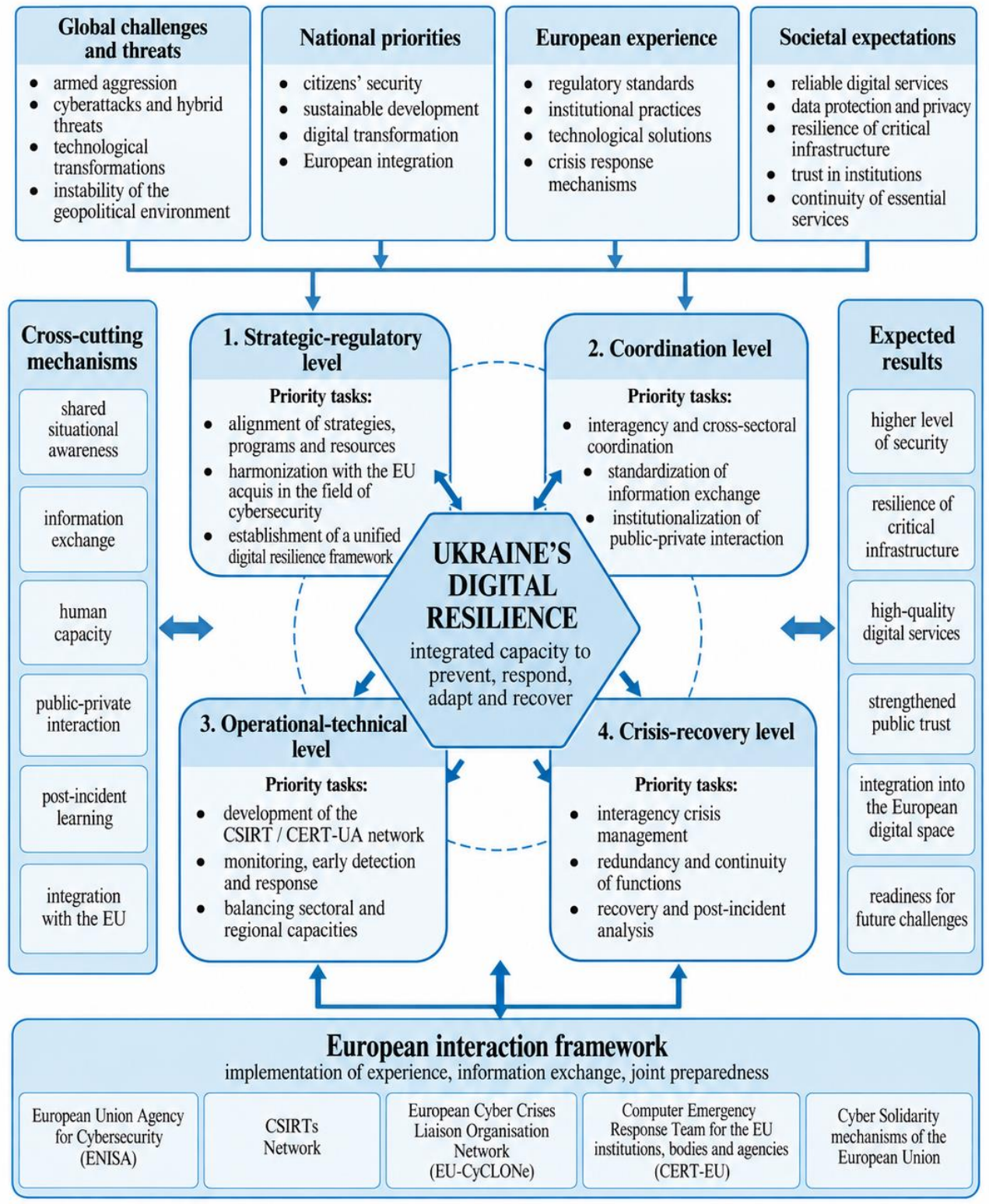


Fig. 4.6. Conceptual model for modernizing the institutional architecture of digital resilience in Ukraine, taking into account European experience

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

SCIENTIFIC EDITION

COLLECTIVE MONOGRAPH

edited by Svitlana Onyshchenko

INFORMATION TECHNOLOGIES AND INFORMATION SECURITY: NATIONAL PROSPECTS AND EUROPEAN PRACTICES

Authors:

Onyshchenko S., Verhal K., Hlushko A., Yanko A., Bilko S., Demydenko M., Derkach T., Desiatko A., Dmytrenko A., Dvirna O., Fesenko A., Fesenko T., Franchuk T., Ivanov Y., Kalashnikova Y., Kapiton A., Klochko L., Kuchma Y., Masliy O., Naboka S., Novosad Z., Raksha V., Toichkina O., Tyshchenko D., Vasyuta V., Vasyuta V., Zhyvylo Y., Zakharov R.

Monograph published in the author's edition

The monograph is included in International scientometric databases

Authorized for printing 16.10.2026.
Order No. MGE14-2026. Contracted price.

Published:
ScientificWorld -NetAkhatAV
Lußstr 13,
Karlsruhe, Germany

e-mail: editor@promonograph.org
https://de.promonograph.org

ISBN 978-3-98924-175-6

