

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%).

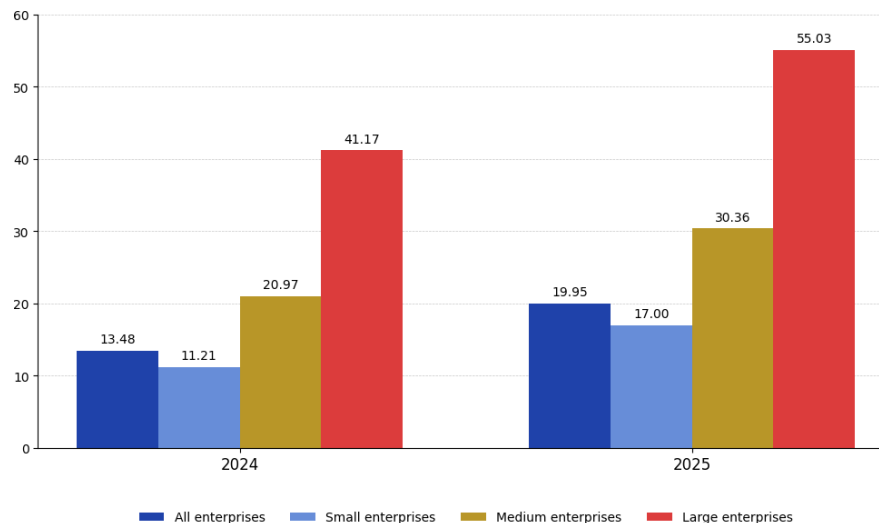


Fig. 1.1. Enterprises using AI technologies by enterprise size, EU, 2024 and 2025, % of total enterprises

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).

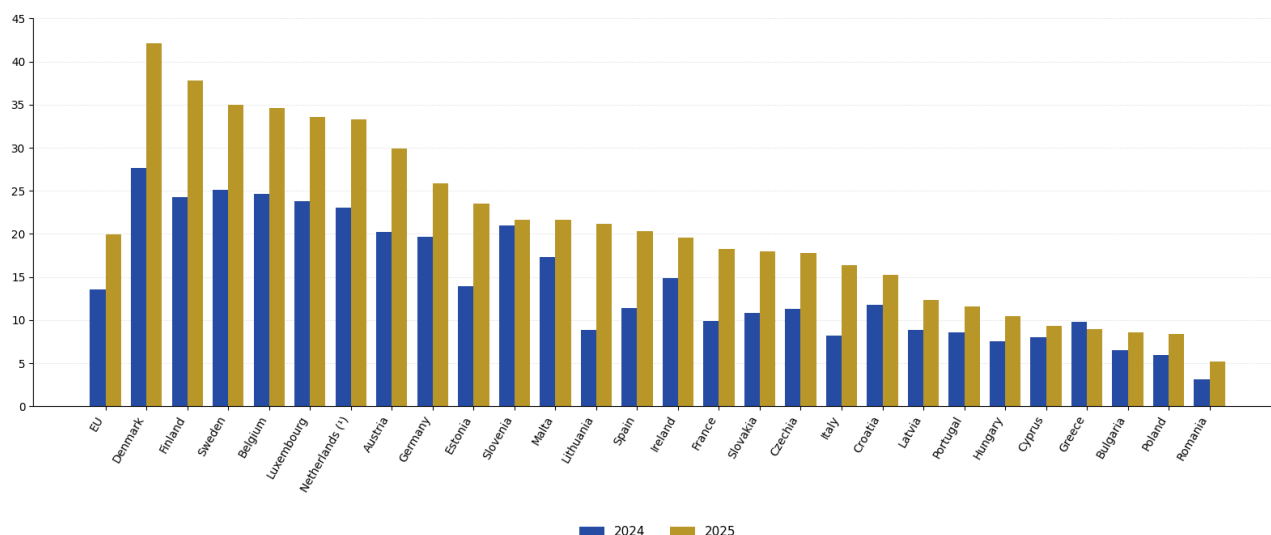


Fig. 1.2. Share of enterprises using artificial intelligence technologies in EU countries, 2024–2025, %

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.

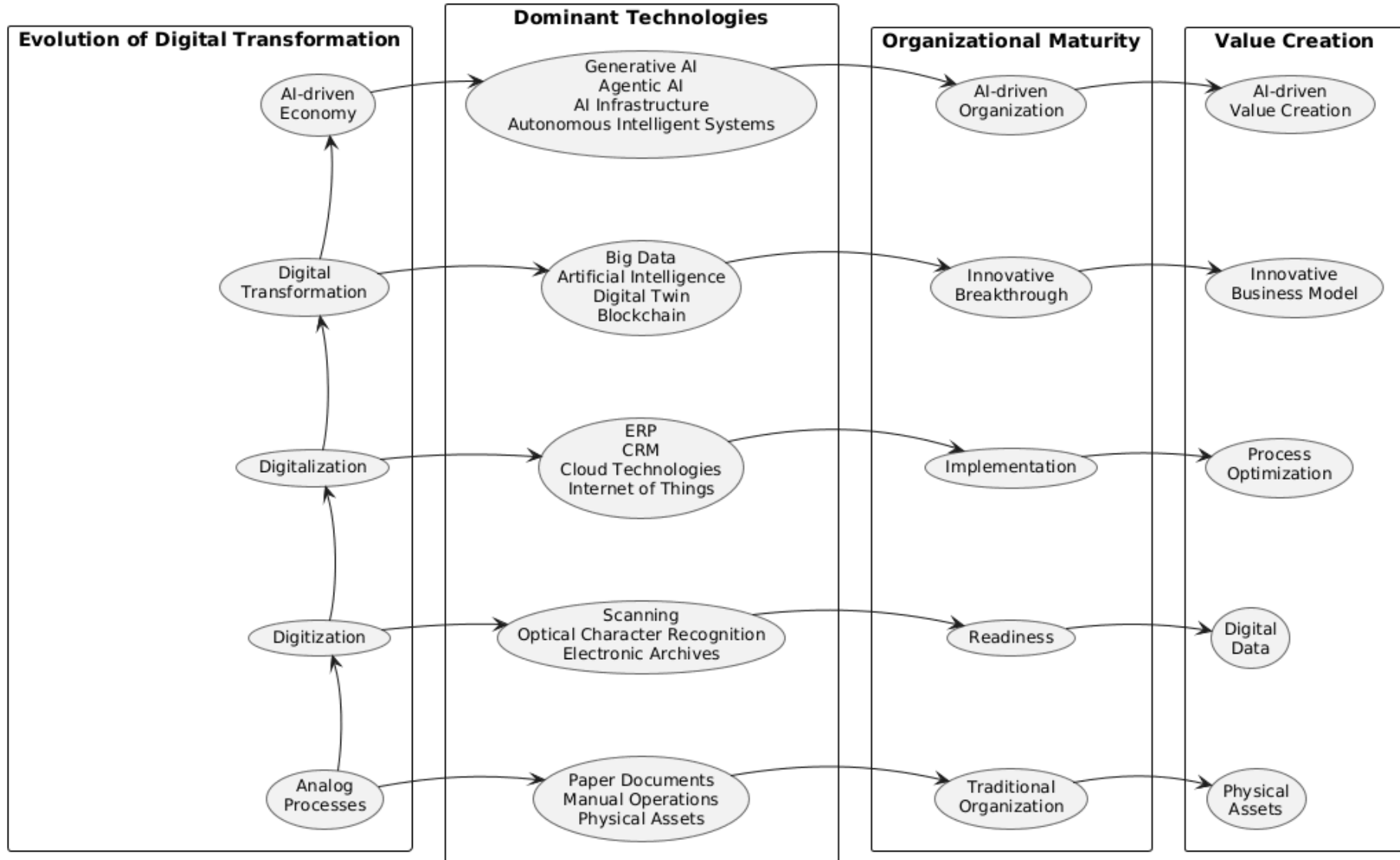


Fig. 1.3. Conceptual model of the transition from digital transformation to an AI-based economy

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

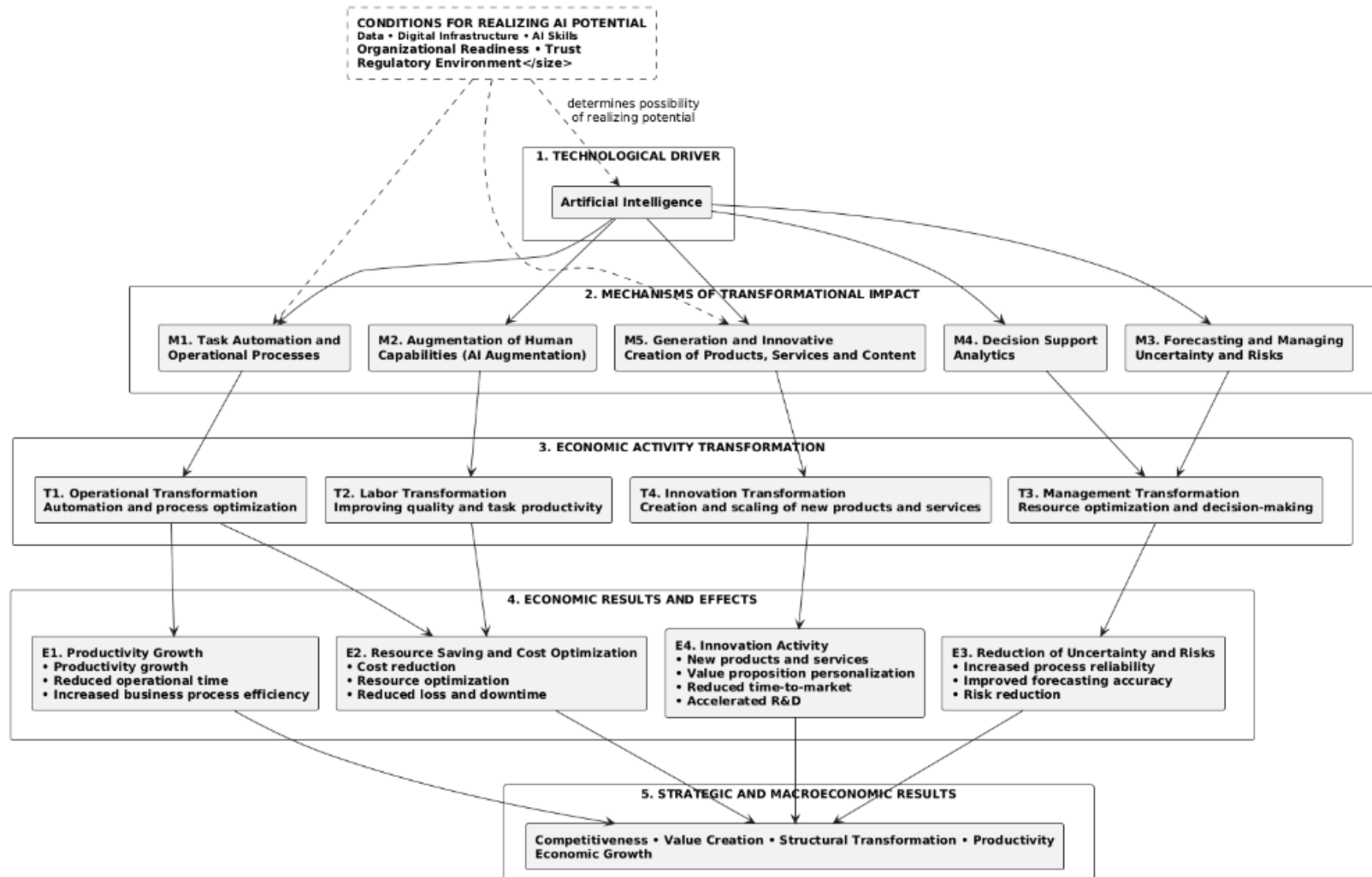


Рис. 1.4. Модель трансформаційного впливу штучного інтелекту на економічну діяльність

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.

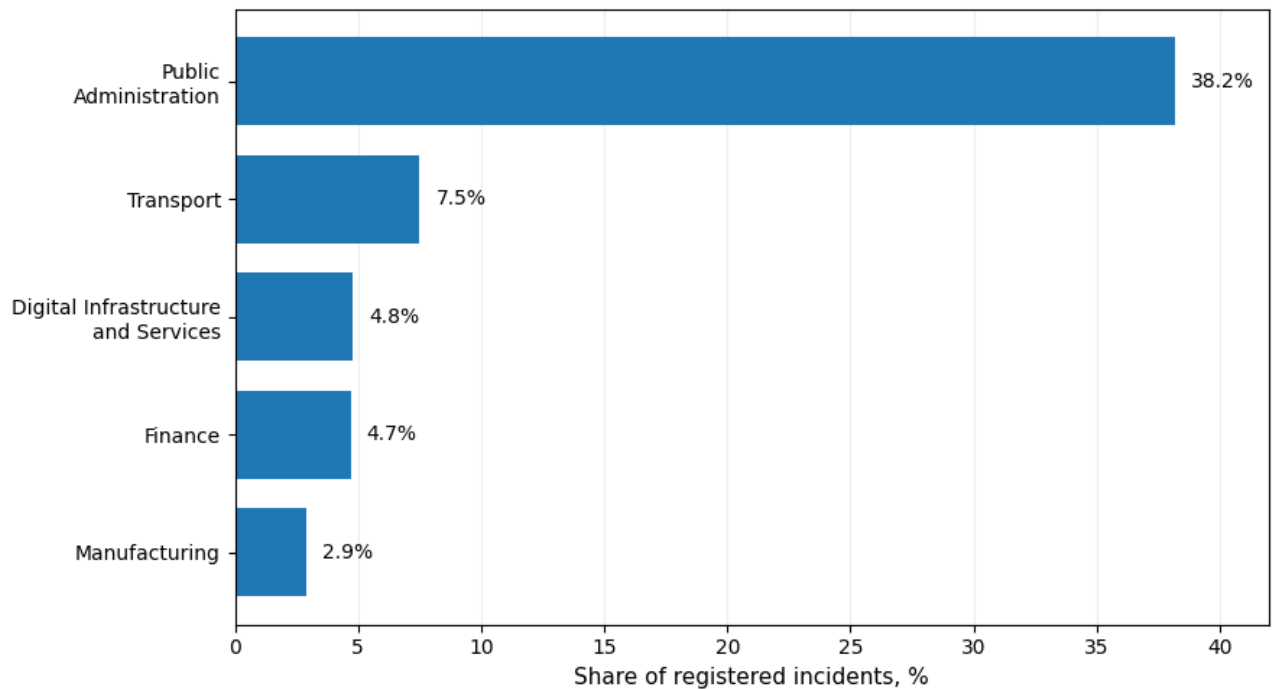


Fig. 1.5. Target sectors of cyberattacks in the EU, 2024–2025

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.

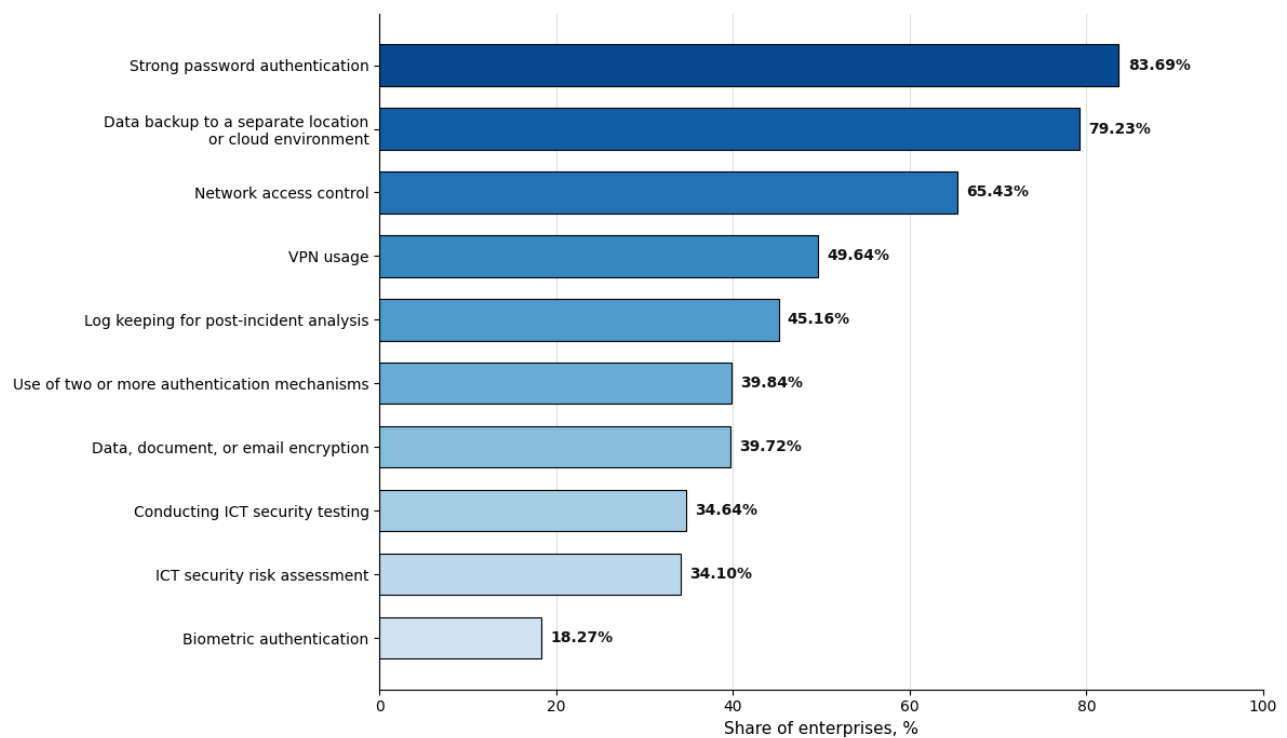


Fig. 1.6. Status of organizational and technical ICT security measures in EU enterprises

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/nanontp.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