МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Чернівецький торговельно-економічний інститут

Державного торговельно-економічного університету

СУЧАСНІ КОНЦЕПЦІЇ ТА ІНСТРУМЕНТИ УПРАВЛІННЯ БІЗНЕС-ПРОЦЕСАМИ В УМОВАХ ІНТЕГРАЦІЇ УКРАЇНИ ДО ЄС

МОНОГРАФІЯ

Чернівці

Технодрук

2026

УДК 005.412:[005.5:005.334]:339.924(477:4-6ЄС)
С-89

Рекомендовано рішенням вченої ради ЧТЕІ ДТЕУ
(протокол № 8, п.19 від 26 червня 2026 р.)

Рецензенти:
Плахута О.І., голова правління ПрАТ «Імпульс»
Кифяк О.В., д.е.н., професор ЧНУ ім. Ю. Федьковича

С-89 СУЧАСНІ КОНЦЕПЦІЇ ТА ІНСТРУМЕНТИ УПРАВЛІННЯ БІЗНЕС-ПРОЦЕСАМИ В УМОВАХ ІНТЕГРАЦІЇ УКРАЇНИ ДО ЄС : монографія / за ред. к.е.н., доц. О.Г. Вдовіченої. Чернівці : Технодрук, 2026. 440 с.
ISBN 978-617-8034-60-3

У монографії висвітлено теоретико-методологічні та прикладні засади управління і трансформації бізнес-процесів в умовах європейської інтеграції, цифровізації та сучасних соціально-економічних викликів. Розкрито сучасні підходи до процесного і стратегічного управління, оцінювання результативності, цифрової трансформації, стандартизації та забезпечення сталого розвитку підприємств. Особливу увагу приділено адаптації українського бізнесу до європейських стандартів, використанню цифрових технологій, удосконаленню управлінських, фінансово-облікових, маркетингових і кадрових процесів, а також галузевим особливостям їх трансформації. Обґрунтовано практичні напрями підвищення ефективності, адаптивності, стійкості та конкурентоспроможності підприємств у європейському економічному просторі.

Монографія буде корисною для науковців, викладачів, аспірантів і здобувачів вищої освіти економічних та управлінських спеціальностей, а також керівників підприємств, підприємців і фахівців у сфері менеджменту, маркетингу, фінансів, обліку, цифрової трансформації та розвитку бізнесу. Видання може бути використане в науково-дослідній роботі, освітньому процесі та практичній діяльності підприємств, орієнтованих на підвищення ефективності, конкурентоспроможності й адаптацію до вимог європейського економічного простору.

УДК 005.412:[005.5:005.334]:339.924(477:4-6ЄС)

ISBN 978-617-8034-60-3
https://doi.org/10.5281/zenodo.23741295

© Автори, 2026
© ЧТЕІ ДТЕУ, 2026
© ПВКФ «Технодрук», 2026

ЗМІСТ

ВСТУП ……. 6

РОЗДІЛ 1. ІНТЕГРОВАНІ УПРАВЛІНСЬКІ ТА ЕКОНОМІЧНІ ПІДХОДИ ДО РОЗВИТКУ БІЗНЕСУ В ЄВРОПЕЙСЬКОМУ ПРОСТОРІ …… 10

Юлія Урсакій. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ УПРАВЛІННЯ БІЗНЕС-ПРОЦЕСАМИ …….. 10

Оксана Верстяк. УПРАВЛІННЯ БІЗНЕС-ПРОЦЕСАМИ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЇ УКРАЇНИ ….……... 44

Ольга Хитрова. ПРАКТИКА УПРАВЛІННЯ БІЗНЕС-ПРОЦЕСАМИ В УКРАЇНІ В УМОВАХ КРИЗИ, ВІЙНИ ТА ВІДНОВЛЕННЯ …… 61

Валентина Чичун. РЕПУТАЦІЙНИЙ КАПІТАЛ ЯК КЛЮЧОВИЙ РЕСУРС ПІДПРИЄМСТВА ..…… 85

Олена Бозуленко, Ірина Лошенюк. МАРКЕТИНГОВІ СТРАТЕГІЇ ФОРМУВАННЯ ДОВГОСТРОКОВОЇ БІЗНЕС-ЦІННОСТІ …… 97

Галина Долга. ОЦІНЮВАННЯ РЕЗУЛЬТАТИВНОСТІ ТА СТРАТЕГІЧНИЙ РОЗВИТОК БІЗНЕС-ПРОЦЕСІВ ..……. 111

Yurii Koroliuk, Anatolii Vdovichen. CYBERSECURITY AND DATA PROTECTION IN DIGITAL BUSINESS PROCESSES …….. 143

Ольга Вдовічена, Данило Вдовічен. ESG-ОРІЄНТОВАНІ БІЗНЕС-ПРОЦЕСИ ЯК ІНТЕГРОВАНИЙ ПІДХІД ДО РОЗВИТКУ БІЗНЕСУ В ЄВРОПЕЙСЬКОМУ ПРОСТОРІ ……. 156

Валерія Пенюк. КОМПЕТЕНТНІСНІ МОДЕЛІ СУЧАСНОГО МЕНЕДЖЕРА ТА МАРКЕТОЛОГА ..……... 177

Алла Шимко. КРОСКУЛЬТУРНІ КОМУНІКАЦІЇ ТА ЄВРОПЕЙСЬКИЙ УПРАВЛІНСЬКИЙ КОНТЕКСТ ……. 191

Андрій Круглянко. АДАПТИВНИЙ КЕЙС-МЕНЕДЖМЕНТ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ОРГАНІЗАЦІЙНОЇ СТІЙКОСТІ БІЗНЕСУ В УМОВАХ ЄВРОІНТЕГРАЦІЇ ……. 203

Yurii Koroliuk ORCID:
https://orcid.org/0000-0001-8732-3731
Doctor of Science in Public Administration, Professor,
Chernivtsi Institute of Trade and Economics of SUTE,
Chernivtsi, Ukraine

Anatolii Vdovichen ORCID:
https://orcid.org/0000-0002-4496-6435
Doctor of Economics, Professor
Chernivtsi Institute of Trade and Economics of SUTE,
Chernivtsi, Ukraine

CYBERSECURITY AND DATA PROTECTION IN DIGITAL BUSINESS PROCESSES

Abstract: *This article provides a comprehensive analysis of cybersecurity and data protection in digital business processes within the context of Ukraine's integration into the European Union. It examines digitalisation trends among EU enterprises by sector between 2020 and 2025, the evolving landscape of cyber threats (with particular emphasis on those related to artificial intelligence), the legal and regulatory framework (including the GDPR, NIS2 Directive, and AI Act), and the current state of problem-solving in Ukraine. Drawing on a systematic literature review, official statistical data, and regulatory documents, the study proposes an integrated model of cybersecurity and data protection. The model incorporates government regulation and support, legal mechanisms, the role of business, the secure deployment of artificial intelligence, and the education and retraining of personnel. The proposed model aims to enhance the resilience of digital business processes, ensure compliance with European standards, and strengthen the competitiveness of Ukrainian enterprises.*

Keywords: *cybersecurity, data protection, digital business processes, artificial intelligence, digital transformation, EU integration, NIS2, GDPR, AI Act.*

Introduction. Digital transformation of business processes has become one of the key drivers of efficiency, flexibility, and competitiveness for enterprises in the context of Ukraine's integration into the European Union. The adoption of cloud technologies, Internet of Things systems, ERP platforms, digital twins, and artificial intelligence tools has substantially altered traditional models of organisational activity, transforming data into a core strategic asset (Ostrovska & Ostrovskyi, 2024). These technologies enable the automation of routine operations, predictive maintenance, optimisation of supply chains, analysis of consumer behaviour, and data-driven managerial decision-making.

At the same time, the rapid digitalisation of business processes is accompanied by a significant increase in cyber threats and risks of compromising the protection of personal and confidential data. According to official European reports, the number of cybersecurity incidents remains high. Moreover, the deployment of emerging technologies, particularly artificial intelligence-based systems, simultaneously creates new opportunities for process optimisation while expanding the attack surface and increasing the potential for data breaches (ENISA, 2025). In Ukraine, where digitalisation has accelerated under martial law through large-scale national initiatives, ensuring the cyber resilience of business processes and compliance with European data protection standards has become particularly critical for maintaining operational continuity and achieving successful integration into the EU single digital market (OECD, 2024; Vasylieva et al., 2025).

The importance of this study is also determined by the need to ensure the cyber resilience of Ukrainian enterprises during post-war economic recovery and their integration into European and global value chains. International partners, investors, and donor organisations increasingly require effective systems for information security management, personal data protection, and business continuity. In these conditions, cybersecurity is no longer only a tool for protecting information resources. It has become a factor of investment attractiveness, digital trust, and competitiveness of Ukrainian enterprises in international markets.

Special attention must be paid to building a cybersecurity culture and developing the digital competencies of personnel. Evidence shows that a significant share of cyber incidents occurs due to the human factor, insufficient employee awareness of modern threats, or failure to comply with information security requirements. Therefore, protecting data in digital business processes requires not only the implementation of technical protection measures but also the creation of a comprehensive system for personnel training, the development of digital literacy, and increased responsibility for the secure use of information resources.

Despite the existence of studies addressing digital transformation and general aspects of cybersecurity, a comprehensive analysis of data protection challenges specifically within business processes that actively employ artificial intelligence technologies, taking into account the Ukrainian context and the requirements of European integration, remains insufficiently developed. Research by Ukrainian scholars indicates substantial gaps between the pace of digital technology adoption and the readiness of protection systems (Shcherban, 2025). Unresolved issues include the development of integrated approaches to managing cyber risks and AI-related risks within a unified business process framework, the adaptation of European regulatory requirements (GDPR, NIS2, and the AI Act) to wartime and post-war recovery conditions, and the creation of practical tools and recommendations for small and medium-sized enterprises, which often lack the resources to implement complex protection systems.

The aim of this article is to analyse current threats, legal mechanisms, and instruments of cybersecurity and data protection in digital business processes, with

particular attention to the role of artificial intelligence, and to formulate recommendations for their implementation in the context of Ukraine's European integration. The object of the study is digital business processes. The subject of the study is cybersecurity, data protection, and the role of artificial intelligence in these processes.

Materials and Methods. An analysis of digitalisation trends among EU enterprises by sector between 2020 and 2025 reveals uneven but generally accelerated adoption of digital technologies, particularly following the COVID-19 pandemic and against the backdrop of geopolitical challenges. Between 2020 and 2022, digitalisation developed most dynamically in the financial sector, retail trade, and public administration, driven by the urgent need to transition to remote working and online services. From 2023 to 2025, the highest growth rates were observed in manufacturing, transport, and logistics, where the Internet of Things, digital twins, and automated systems were actively implemented. According to available data, 72% of large EU enterprises used cloud services, 48% employed Internet of Things technologies, and 28% adopted artificial intelligence solutions (Ostrovska & Ostrovskyi, 2024). The highest levels of digitalisation were recorded in the financial sector and public administration, whereas manufacturing and transport demonstrated comparatively lower but the fastest-growing adoption rates during 2023–2025 (Vărzaru, 2024; European Commission, 2023). Concurrently with digitalisation, the volume of data generated within business processes increased, thereby heightening risks to data protection. In manufacturing and transport, the convergence of IT and OT systems created new vulnerabilities, while the financial sector and public administration faced heightened exposure to ransomware and DDoS attacks. The dynamics observed between 2020 and 2025 indicate a shift from basic digitalisation (cloud services and e-commerce) to advanced technologies (artificial intelligence, Big Data, and the Internet of Things) (Vărzaru, 2024; European Commission, 2023), accompanied by strengthened requirements for cybersecurity and data protection (ENISA, 2025).

Business processes comprise a set of interrelated activities aimed at creating value for customers and achieving an organisation's strategic objectives. In the digital environment, these processes undergo profound transformation through the implementation of cloud technologies, Internet of Things systems, ERP platforms, digital twins, and artificial intelligence tools. Within the European Union, the digitalisation of business processes is regarded as a central element of the Digital Decade Strategy to 2030. According to available data, more than 72% of large EU enterprises use cloud services, and 28% of companies have adopted artificial intelligence solutions (Ostrovska & Ostrovskyi, 2024). In Ukraine, the process of digitalisation has accelerated under martial law through large-scale national initiatives. Research by Ukrainian scholars indicates uneven digitalisation rates: large enterprises and the IT sector demonstrate higher dynamism, whereas small and medium-sized businesses face barriers related to limited resources and insufficient

levels of cyber resilience (Ostrovska & Ostrovskyi, 2024; Shcherban, 2025). The European experience demonstrates that successful digitalisation of business processes is possible only when accompanied by the simultaneous implementation of robust data protection and cybersecurity mechanisms, as confirmed by monitoring results on the progress of EU candidate countries.

Data constitute a central asset of modern business processes. They are generated, processed, and transmitted at all stages – from customer interaction to supply chain management and financial planning. The growing volume of data, particularly personal and confidential information, creates new challenges for its protection. Ukrainian researchers emphasise that under martial law and the active digitalisation of public and business services, data security has become critical for ensuring business continuity and maintaining the trust of counterparties (Vasylieva et al., 2025). In the European context, data protection is governed by the GDPR, which establishes high standards regarding lawfulness of processing, data minimisation, and security. Non-compliance with these requirements may result not only in substantial financial penalties but also in the loss of competitive positions within the EU single digital market.

Digitalisation trends in business processes during 2024–2025 are characterised by the active deployment of artificial intelligence technologies for automation, forecasting, and optimisation. At the same time, a rise in cyber threats that directly affect the resilience of these processes has been observed. According to data from the European Union Agency for Cybersecurity, 4.875 incidents were analysed between July 2024 and June 2025. The most prevalent type were DDoS attacks (76.7%), while phishing remained the primary initial access vector (60%). Artificial intelligence was used in more than 80% of social engineering cases. The most affected sectors were public administration (38.2% of incidents), transport (7.5%), and the financial sector (4.5%). Entities designated under the NIS2 Directive accounted for 53.7% of recorded incidents. These facts indicate that the digitalisation of business processes is occurring amid continuously growing risks that require an integrated approach to security management (ENISA, 2025).

The dynamics of key problems in cybersecurity and data protection within digital business processes over recent years demonstrate clear trends of increasing complexity and scale. Between 2022 and 2025, Ukraine witnessed accelerated digitalisation of public and business services amid martial law, accompanied by a simultaneous rise in cyber incidents targeting the private sector. Whereas attacks on critical infrastructure predominated in 2022–2023, the share of incidents directed at logistics, financial, and manufacturing companies – which actively utilise digital platforms and artificial intelligence – increased significantly in 2024–2025. According to European reports, the dynamics reflect a shift from large-scale DDoS attacks to more targeted campaigns employing artificial intelligence for personalised phishing and evasion of security systems. At the same time, growing risks associated with shadow AI and data poisoning in business processes have been recorded, which

is particularly relevant for companies integrating artificial intelligence into supply chains and customer platforms. In the European context, these dynamics are reflected in the gradual strengthening of regulatory requirements (NIS2 and the AI Act) alongside an increase in incidents within sectors covered by these directives (ENISA, 2025; Vasylieva et al., 2025) (table 1).

Table 1

Main Types of Cyber Incidents and Their Share in the EU (July 2024 – June 2025)

Type of Incident	Share, %	Level of AI Involvement	Main Impact on Business Processes
DDoS attacks	76.7	Low (primarily hacktivism)	Disruption of access to online services and systems
Phishing and social engineering	60	High (over 80% of cases)	Theft of credentials and unauthorised access
Ransomware	81.1*	Medium	Data encryption and interruption of critical processes
Exploitation of vulnerabilities	21.3	Increasing	System compromise and leakage of confidential information

*Share among cybercrime-related incidents.

Compiled on the basis of ENISA (2025)

Note: The percentages do not add up to 100% because the indicators reflect different classifications of incidents according to the ENISA methodology (incident types versus initial access vectors), which are not mutually exclusive. The data refer to the European Union as a whole.

Clients and businesses interact in the digital environment through multiple channels, including web platforms, mobile applications, and artificial intelligence-based systems. This interaction generates substantial volumes of personal data, which become targets for cyberattacks. According to the global study on the cost of data breaches, the average cost of a single incident in 2025 amounted to USD 4.44 million, representing a 9% decrease compared to the previous year, owing to accelerated detection enabled by artificial intelligence tools. At the same time, artificial intelligence technologies were employed by attackers in 16% of breaches, while 97% of affected organisations lacked adequate access controls for AI models and data. Shadow AI was involved in 20% of cases. In Ukraine, clients are increasingly utilising digital services, which heightens the requirements for personal data protection and rapid incident response (IBM, 2025). European studies emphasise that customer trust in digital platforms directly depends on the transparency of data protection policies and the effectiveness of cybersecurity measures.

Data security and prevailing protection trends are determined by the need to combine technical, organisational, and legal measures. The key trend in 2025 has been the dual use of artificial intelligence – both to strengthen protection through automated anomaly detection and incident response, and to conduct attacks. In the context of European integration, Ukrainian businesses are required to adapt their

processes to the requirements of the GDPR, the NIS2 Directive, and the Artificial Intelligence Act. An analysis of regulatory documents and scholarly literature indicates that the harmonisation of Ukrainian legislation with European standards is a necessary condition for successful integration into the EU single digital market (European Commission, 2024; Vasylieva et al., 2025) (table 2).

Table 2

Impact of Artificial Intelligence on Data Security (2025)

Indicator	Value	Implications for Business Processes
Share of data breaches involving AI used by attackers	16%	Increased complexity of attacks (deepfakes, AI-powered phishing)
Organisations experiencing AI-related incidents without access controls	97%	High risks of shadow AI and data/model leakage
Reduction in average breach cost due to AI-based protection	USD 4.44 million (–9%)	Faster detection and containment of incidents
Use of AI in social engineering	Over 80%	Large-scale compromise of personnel and business processes

Compiled on the basis of IBM (2025) and ENISA (2025).
Note: The data represent global averages and are not limited to EU countries.

Digital reputation is directly dependent on a company's ability to protect data and recover rapidly following incidents. A breach of personal data or prolonged unavailability of services due to a cyberattack negatively affects the trust of customers, partners, and investors. Research confirms that companies which respond publicly and transparently to incidents and demonstrate a high level of cyber resilience recover their reputation more quickly and maintain competitive positions. In the context of information confrontations, digital reputation becomes an important intangible asset, particularly for Ukrainian enterprises seeking to integrate into European markets and participate in grant programmes (Ostrovska & Ostrovskyi, 2024; Shcherban, 2025).

Cybersecurity plays a key role in ensuring the resilience of business processes under conditions of information and hybrid confrontations. Since 2022, Ukraine's private sector – particularly logistics, finance, and manufacturing – has been subjected to systematic cyberattacks, some of which bear the hallmarks of state-sponsored activity. Effective cybersecurity ensures not only the technical protection of systems but also the preservation of business continuity, customer trust, and the ability to participate in European value chains. Studies by Ukrainian scholars emphasise that, under martial law and in the post-war recovery period, cybersecurity has become an element of national resilience and a source of competitive advantage for businesses (Vasylieva et al., 2025). International reports indicate that companies with high levels of cyber resilience demonstrate better recovery performance after incidents and a greater capacity to integrate into European economic processes (OECD, 2024; ENISA, 2025).

The dynamics of key cybersecurity problems in the context of information confrontations between 2022 and 2025 are characterised by a shift from

predominantly destructive attacks on infrastructure to hybrid campaigns that combine technical means with information influence. During this period, Ukraine recorded a growing number of incidents targeting businesses, particularly in sectors responsible for logistics and supply. At the same time, positive developments were observed in legislative regulation and international cooperation – notably, Ukraine's access to European cybersecurity mechanisms in 2025. However, the dynamics also reveal a persistent gap between the pace of digitalisation and the level of cyber resilience among small and medium-sized enterprises, creating systemic risks for supply chains and integration into European markets (Vasylieva et al., 2025; ENISA, 2025) (table 3).

Table 3

Comparative Indicators of Business Process Digitalisation and Cyber Resilience in Ukraine and the EU (2024–2025)

Indicator	EU (average)	Ukraine
Cloud services adoption	72% (large enterprises)	Accelerated growth under wartime conditions
AI adoption in business processes	28%	Uneven
Access to EU cybersecurity mechanisms	Full	Partial (since 2025)
Average cost of data breaches	USD 4.44 million	Higher vulnerability of SMEs

Data sources: OECD (2024); ENISA (2025); Ostrovska & Ostrovskyi (2024); Vasylieva et al. (2025); IBM (2025).

Note: The indicators have limited direct comparability due to differences in data collection methodologies and context. EU data come from standardised Eurostat and OECD surveys, while Ukrainian facts are based on national estimates during wartime. The table provides an indicative comparison to illustrate gaps and trends rather than strict statistical equivalence.

Legal regulation of cybersecurity and data protection in digital business processes is a critical factor for ensuring the resilience and competitiveness of enterprises during Ukraine's integration into the European Union. Digital business processes based on cloud technologies, the Internet of Things, ERP systems, and artificial intelligence generate and process large volumes of personal and confidential data. These processes therefore require clear legal safeguards.

The European Union has developed a comprehensive regulatory framework that combines personal data protection, cybersecurity of critical sectors, and the regulation of artificial intelligence technologies. This framework directly affects Ukrainian businesses seeking to integrate into the EU single digital market.

The main legal instrument for personal data protection remains Regulation (EU) 2016/679 (GDPR). It establishes key principles, including lawfulness, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality. For digital business processes, the requirements for privacy by design and privacy by default are particularly important. Organisations must also conduct a

Data Protection Impact Assessment (DPIA) when using technologies that present high risks, such as the processing of large volumes of data in cloud environments or the deployment of artificial intelligence systems. Non-compliance with GDPR can result in fines of up to 4% of a company's annual global turnover.

In the field of cybersecurity, the key instrument is Directive (EU) 2022/2555 (NIS2). This directive expands the scope of the previous NIS Directive and introduces mandatory measures for essential and important entities across 18 sectors, including manufacturing, transport, finance, and digital infrastructure. NIS2 requires a risk-based approach, regular risk assessments, business continuity measures, and incident reporting within 24 hours. For digital business processes, this means mandatory protection of supply chains, cloud environments, and systems that use artificial intelligence. The directive also strengthens requirements for third-party risk management, which is particularly relevant for Ukrainian companies integrated into European supply chains.

Regulation of artificial intelligence is carried out through Regulation (EU) 2024/1689 (AI Act). This regulation classifies AI systems according to their level of risk. High-risk systems, such as those used in critical infrastructure, supply chain management, or credit decisions, are subject to strict requirements regarding transparency, accountability, data protection, and cybersecurity. The AI Act directly links cybersecurity requirements for AI systems to the NIS2 Directive and the GDPR, creating a unified regulatory logic for digital technologies in business processes.

Ukraine's legal framework is undergoing active harmonisation with European standards. The current Law of Ukraine "On Personal Data Protection" (2010) does not meet modern requirements and requires substantial revision. Draft Law No. 8153 aims to implement the principles of the GDPR. The Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" (2017) and the Cybersecurity Strategy of Ukraine (approved by Presidential Decree No. 37/2022) provide the foundation for a national system. However, their implementation in the business sector remains fragmented. In 2025, Ukraine gained access to the European Cyber Reserve. This step represents important practical integration, but further alignment of national legislation with the NIS2 Directive and the AI Act is still required.

The dynamics of legal regulation between 2020 and 2025 show a shift from a fragmented approach to a more comprehensive one. Between 2020 and 2022, the main focus was on personal data protection under the GDPR. Since 2023, the emphasis has moved to cybersecurity of critical sectors under the NIS2 Directive and the regulation of artificial intelligence under the AI Act. For digital business processes, this means the need to comply simultaneously with requirements for data protection, system resilience, and the ethical use of AI. Under martial law, legal aspects have gained additional importance. Ukrainian companies must protect data in cloud environments that are often located outside the country while also meeting national security requirements.

For Ukrainian businesses, especially small and medium-sized enterprises, the main challenges include insufficient awareness of European legal requirements,

limited resources for implementing technical and organisational measures, and the lack of clear state support mechanisms for compliance. At the same time, legal harmonisation creates opportunities for access to European markets, participation in grant programmes, and integration into EU supply chains.

Thus, the legal aspects of cybersecurity and data protection in digital business processes form a unified system of requirements that combines personal data protection, cyber resilience, and technology regulation. For successful integration into the EU, Ukrainian businesses should treat compliance not as a formality but as a strategic tool for increasing competitiveness and resilience in the context of digital transformation.

Scientific studies on cybersecurity and data protection in digital business processes in the context of Ukraine's EU integration widely apply a combination of methods that link theoretical review with empirical analysis of real trends and the regulatory framework. Systematic literature reviews and systematic mapping studies are used to summarise English- and Ukrainian-language research published between 2020 and 2026. These methods help identify key trends in business process digitalisation, threats related to artificial intelligence, and gaps in data protection. Document analysis and comparative legal analysis of EU and Ukrainian regulatory acts are applied to assess the degree of legislative harmonisation, particularly regarding the GDPR, the NIS2 Directive, and the AI Act. Secondary statistical analysis of official data from international organisations and companies makes it possible to quantify the scale of incidents, the economic consequences of data breaches, and sectoral threat dynamics. Case study analysis and process tracing are used to examine real examples of digital business processes in Ukrainian enterprises under martial law and hybrid threats, as well as to compare them with European practices. Risk-based analysis based on international standards and frameworks supports the development of practical tools for integrating cybersecurity directly into business process management.

Several key problems require further in-depth examination. The growing complexity of threats linked to artificial intelligence, including shadow AI, automated phishing, and attacks on models, combines with insufficient control over access to AI systems in business processes. This creates new vulnerabilities for data protection. Insufficient harmonisation of Ukrainian legislation with European standards complicates compliance for companies integrated into European supply chains, especially under active adoption of cloud technologies and artificial intelligence. The high vulnerability of small and medium-sized enterprises to cyber incidents and the economic consequences of data breaches is exacerbated by martial law and limited resources for implementing modern protection measures. Risks in digital supply chains and third-party environments when using cloud platforms, the Internet of Things, and AI directly affect business continuity and require a systematic management approach. The gap between the pace of digitalisation and the level of cyber resilience in enterprises, particularly in manufacturing, transport, and logistics, is compounded by the absence of integrated models for managing cyber risks within

business process systems. Ensuring the resilience of digital business processes under hybrid threats and martial law, as well as meeting the needs of post-war recovery and EU integration, requires practical recommendations tailored to the real capabilities of Ukrainian businesses. Insufficient awareness and digital skills among personnel regarding data protection and cybersecurity when deploying advanced technologies limit the effectiveness of protection measures at the individual enterprise level.

Results and Discussion. An analysis of efforts to address cybersecurity and data protection problems in digital business processes in Ukraine reveals both notable achievements under martial law and persistent systemic gaps that require a comprehensive approach. Between 2022 and 2025, Ukraine demonstrated strong resilience of its digital infrastructure. This was supported by state initiatives such as "Diia" and Diia.Business, as well as active international cooperation, including access to the European Cyber Reserve in 2025. National reports and studies record a decline in critical incidents against state systems compared to 2022–2023. This improvement was achieved through stronger state regulation and public-private partnership.

At the same time, small and medium-sized enterprises remain the most vulnerable segment. Limited resources, insufficient awareness of European standards, and reliance on outdated systems create significant risks for supply chains and business continuity. Threat dynamics have shifted from large-scale DDoS attacks to targeted campaigns that use artificial intelligence. This shift increases the need for integrated risk management. Legal harmonisation with the EU has progressed unevenly. The draft law on personal data protection is approaching GDPR standards. However, the implementation of NIS2 and AI Act requirements in the business environment remains slow. This creates barriers to exports and participation in European value chains.

Overall, current solutions remain largely reactive. They do not yet provide a holistic approach to integrating cybersecurity into the management of digital business processes.

To address the identified problems in a systematic way, the study proposes an integrated model of cybersecurity and data protection in digital business processes. The model is built on the principles of integration, adaptability, and interaction among all key stakeholders. It consists of five interconnected components that provide both strategic and operational levels of protection.

The first component is government regulation and support that involves accelerating the harmonisation of national legislation with European acts (GDPR, NIS2, and the AI Act) and creating state support mechanisms for businesses. Under the model, the government should develop a national strategy for digital business resilience with clear KPIs for different sectors, introduce a voucher system for cybersecurity for small and medium-sized enterprises, and ensure access to European mechanisms for sharing threat information. This approach helps reduce the gap between the pace of digitalisation and the level of cyber resilience, especially during post-war recovery (fig. 1).

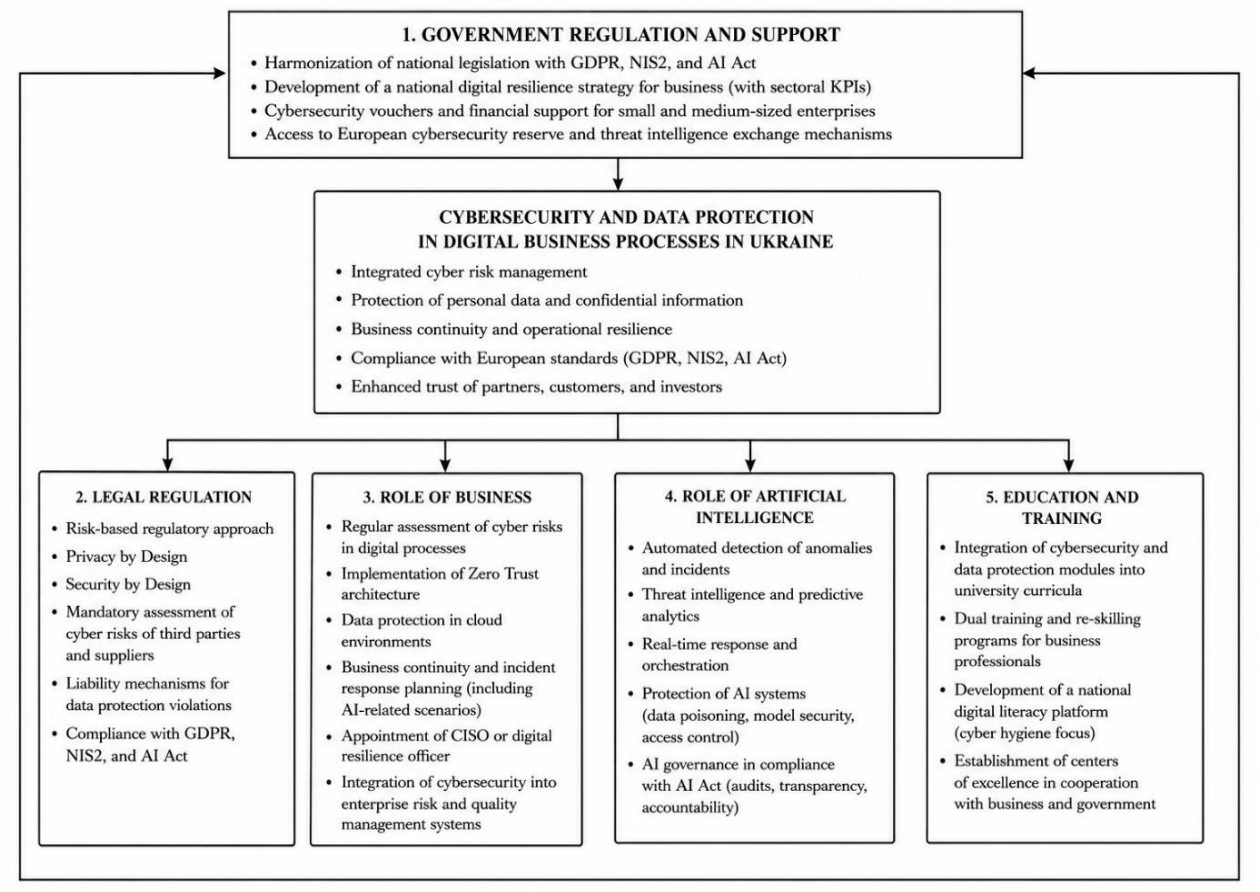


Figure 1. Conceptual Model of Cybersecurity and Data Protection in Ukraine's Digital Business Processes

The second component is legal regulation that is based on implementing a risk-based approach across all digital business processes. The model requires mandatory integration of privacy by design and security by design principles into the development and modernisation of ERP systems, cloud solutions, and artificial intelligence platforms. For supply chains, it proposes mandatory assessment of third-party cyber risks and mechanisms of liability for data protection violations. This legal architecture ensures compliance with European standards and creates a level playing field for Ukrainian businesses in the EU market.

The third component is the role of business that involves implementing an integrated cyber risk management system directly into the architecture of business processes. Companies should conduct regular risk assessments of digital processes, adopt a Zero Trust architecture, protect data in cloud environments, and develop business continuity plans that account for AI-related attack scenarios. The model recommends establishing the position of Chief Information Security Officer (CISO) or a similar role responsible for digital resilience in companies. It also recommends integrating cybersecurity into the enterprise quality and risk management system. This approach transforms cybersecurity from a cost centre into a strategic asset that increases the trust of partners and customers.

The fourth component is the role of artificial intelligence that provides for the dual use of AI technologies: as a tool for strengthening protection and as an object of protection. In the model, AI is used for automated anomaly detection, threat prediction, and rapid real-time incident response. At the same time, an AI governance system is introduced. It includes access control to models, protection against data poisoning, algorithm audits, and compliance with AI Act requirements for high-risk systems. This balanced approach allows businesses to benefit from AI for process optimisation without creating additional vulnerabilities.

The fifth component is the role of education and retraining that ensures the development of human capital. The model proposes integrating cybersecurity and data protection modules into educational programmes in management, digital economy, and information technology. It also recommends creating dual retraining programmes for current business professionals and developing a national digital literacy platform with a focus on cyber hygiene. Educational institutions should collaborate with business and government through centres of competence. This will enable rapid responses to changes in the threat landscape and the training of specialists capable of integrating cybersecurity into process management.

These five components interact through mechanisms of continuous monitoring, information exchange, and adaptation. The government creates the legal framework and support tools, businesses implement practical solutions, artificial intelligence strengthens technical protection, and education develops human capital. This integrated architecture makes it possible to address all identified problems simultaneously: reduce business vulnerability, ensure compliance with European standards, integrate AI safely, and increase the overall resilience of digital business processes under martial law and during post-war recovery. Implementation of the model will not only protect data and systems but also strengthen the competitive position of Ukrainian businesses on the path to full integration into the European Union single digital market.

Conclusions. The article provides a comprehensive analysis of cybersecurity and data protection problems in digital business processes in the context of Ukraine's integration into the European Union. The study finds that rapid digitalisation, accelerated by martial law, is accompanied by increasing complexity of cyber threats – particularly AI-powered attacks and shadow AI – insufficient harmonisation of legislation with European standards, and high vulnerability of small and medium-sized enterprises.

The proposed integrated model of cybersecurity and data protection in digital business processes is built on five interconnected components: government regulation and support, legal regulation, the role of business, the role of artificial intelligence, and the role of education and retraining. This model enables a systematic approach to solving the identified problems. It ensures the integration of cybersecurity directly into business process architecture, compliance with the requirements of the GDPR, NIS2 Directive, and AI Act, safe use of artificial intelligence technologies, and the development of necessary human capital.

Implementation of the model will contribute not only to reducing the risks of data breaches and cyber incidents but also to increasing the resilience of digital business processes, strengthening the trust of partners and customers, and supporting the successful integration of Ukrainian businesses into the European Union single digital market during post-war recovery.

References

Awan, M. (2025). Cybersecurity threats and defensive strategies for small and medium firms: A systematic mapping study. Administrative Sciences, 15(12), 481. https://doi.org/10.3390/admsci15120481

Beska, S. (2025). Cyber resilience in Ukraine: Measuring response to hybrid warfare [Doctoral dissertation, Central European University]. https://www.etd.ceu.edu/2025/beska_solomiia.pdf

European Commission. (2023). Report on the state of the Digital Decade 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023DC0570

European Commission. (2024). State of the Digital Decade 2024. Publications Office of the European Union.

ENISA. (2025). ENISA threat landscape 2025. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

IBM Security. (2025). Cost of a data breach report 2025. IBM Corporation. https://www.ibm.com/reports/data-breach

Ostrovska, H. Y., & Ostrovskyi, O. T. (2024). Digital transformation of industry: Current realities and development priorities. Economic Herald of Donbas, 1-2(75-76), 166–177. https://doi.org/10.12958/1817-3772-2024-1-2(75-76)-166-177

OECD. (2024). Enhancing resilience by boosting digital business transformation in Ukraine. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50/4b13b0bb-en.pdf

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Al Moqren, E. A., & Alshahrani, S. M. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. PMC. https://pmc.ncbi.nlm.nih.gov/articles/PMC10422504/

Vărzaru, A. A. (2024). Digital transformation and innovation: The influence of digital technologies on innovation expenditures and revenues. Systems, 12(9), 359. https://doi.org/10.3390/systems12090359

Vasylieva, T., Kravchenko, O., & et al. (2025). Digital transformations of Ukraine's cybersecurity system during the full-scale war [Monograph].

Shcherban, T. (2025). Assessment of the digital transformation of Ukraine's economy: Challenges, opportunities and strategic prospects. *Economics of Development, 12*(1).