Міністерство освіти і науки України
Національна академія наук України
Національний центр «Мала академія наук України»
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
Київський національний університет
будівництва і архітектури
Національний університет «Запорізька політехніка»
Національний технічний університет
«Дніпровська політехніка
Національний університет «Львівська політехніка»

ЗБІРНИК НАУКОВИХ ПРАЦЬ

XVIII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «АКАДЕМІЧНА Й УНІВЕРСИТЕТСЬКА НАУКА: РЕЗУЛЬТАТИ ТА ПЕРСПЕКТИВИ»

09 – 12 грудня 2025 року
Полтава

UDC 338.27:004.056.5

INTEGRATION OF DIGITAL RESILIENCE SYSTEMS AS A FOUNDATION FOR STRENGTHENING UKRAINE'S ECONOMIC SECURITY IN WARTIME AND POST-WAR PERIODS

Buriak A.A.
National University «Yuri Kondratyuk Poltava Polytechnic»
fem.buryak@nupp.edu.ua

Ukraine operates under unprecedented hybrid pressure, where conventional military threats merge with large-scale cyberattacks, disinformation campaigns, and attempts to destabilize economic systems through digital channels. Ensuring economic security in such conditions requires not only reactive cybersecurity tools but the formation of an integrated digital resilience architecture capable of supporting stability in wartime and accelerating recovery in the post-war phase. This aligns with Ukraine's commitments under the EU Digital Decade framework and the updated standards of international information security governance.

The concept of digital resilience has transformed from a technological category into a systemic determinant of national economic security [1]. For Ukraine, which faces continuous disruptions to energy, transport, financial, and communication infrastructure, the integration of resilience mechanisms is no longer an additional protective layer but a structural requirement for maintaining sustainability of both state institutions and the private sector.

Modern cyber incidents demonstrate a trend toward increasing sophistication and simultaneity. According to the State Service of Special Communications and Information Protection, attacks in 2024-2025 increasingly targeted cross-sectoral nodes – data centers, cloud ecosystems, logistics networks – aiming not only to damage individual facilities but to provoke cascading economic failures. This creates the need for next-generation monitoring systems capable of predictive analytics, automated incident response, distributed data storage, and AI-orchestrated risk assessment.

A security-oriented information environment must integrate technological, organizational, institutional, and behavioral components [2]. At the technological level, priorities include [3]: implementation of zero-trust architectures for public sector and critical businesses; development of national cyber threat intelligence platforms; transition to secure cloud infrastructures synchronized with EU standards; mandatory adoption of AI-driven anomaly detection systems in critical industries. At the organizational level, emphasis is placed on forming unified digital resilience protocols across ministries, regional administrations, and large enterprises. This ensures cross-sectoral coordination, standardized reporting, and rapid exchange of threat intelligence.

Institutional transformations involve updating legislation on critical infrastructure protection, harmonizing national cybersecurity norms with NIS2 and the EU Cyber Resilience Act, strengthening CERT-UA's analytical capabilities, and establishing resilience centers in key sectors [4]. An equally important dimension is combating disinformation, which has increasingly targeted economic confidence indicators, financial stability, and public trust in state institutions.

The economic implications of integrating resilience systems are significant. In wartime, they ensure continuity of essential services and prevent large-scale disruptions to production chains. In the post-war phase, they create conditions for attracting foreign investment, integrating into EU digital markets, and rebuilding infrastructure according to resilient-by-design principles. Key indicators of Ukraine's digital security and resilience development in 2022–2025 is shown in table 1.

Table 1

Key indicators of Ukraine's digital security and resilience development in 2022–2025

Indicator	2022	2023	2024	2025 (forecast)	Change 2022–2025, %
Number of recorded cyberattacks, thousand	24,3	20,8	17,6	15,2	–37,5

Share of critical infrastructure protected by resilience systems, %	32	41	53	68	+112,5
Share of public services migrated to secure cloud platforms, %	18	29	45	62	+244,4
Share of enterprises applying AI-based cyber monitoring, %	7	14	27	39	+457,1

Source: compiled by the author based on data from SSSCIP, ENISA, CERT-UA, Ministry of Digital Transformation of Ukraine.

The upward dynamics of resilience indicators reflect structural improvements in digital defense capacity, but they are insufficient without long-term synchronization with European standards. Comprehensive integration into the EU's security frameworks requires the development of cross-border cyber exercises, participation in joint digital risk assessment mechanisms, and expanding research cooperation on resilience technologies.

Integrating digital resilience systems becomes a defining prerequisite for strengthening Ukraine's economic security under wartime cyber pressure and during the post-war reconstruction period. The creation of a security-oriented information environment requires complex technological modernization, institutional reforms, and behavioral adaptation of society to new digital risks.

Reference:

1. Буряк А.А. Інвестиційне співробітництво між Україною та ЄС у промисловості: регіональний розріз. Науковий вісник Міжнародного гуманітарного університету. Серія: «Економіка і менеджмент. 2017. № 25/2017. С. 49 – 53.

2. Буряк А.А., Кудряшова Д.О., Сторожук Л.М. Стратегія розвитку digital-економіки в Україні: національна візія та виклики глобалізації. Система управління відходами в циркулярній економіці: фінансові, соціальні, екологічні та енергетичні детермінанти: монографія. Суми: Сумський державний університет. 2023. С. 239 – 248.

3. Maslii, O., Buriak, A., Chaikina, A., & Cherviak, A. (2025). Improving conceptual approaches to ensuring state economic security under conditions of digitalization. Eastern-European Journal of Enterprise Technologies, 1(13 (133), 35 – 45. https://doi.org/10.15587/1729-4061.2025.319256

4. Буряк А.А. Пріоритети ОНН у напрямі удосконалення міжнародної інформаційної безпеки. Сталий розвиток: виклики та загрози в умовах сучасних реалій: матеріали II Міжнародної науково-практичної Інтернет-конференції, 06 червня 2024 р. Полтава: Національний університет імені Юрія Кондратюка, 2024. С. 181–182.

UDC 658

DIGITALIZATION OF BUSINESS PROCESSES IN UKRAINE IN A NEW ECONOMIC PARADIGM IN THE CONTEXT OF DIGITAL TRANSFORMATION DURING THE WAR

Dmytrenko A.V., doctor of economic sciences, associate professor
Yuriy Kondratyuk National University of Poltava
av_dmitrenko@ukr.net

Abstract. *Digitalization opens up new opportunities and, most importantly, helps to optimize and improve business operations, which is especially important for Ukrainian businesses during the war. Digital technologies not only create a huge potential to increase the productivity of companies, they can also improve economic resilience and support economic recovery during a time of war. Since the start of Russia's full-scale invasion of Ukraine in February 2022, the Ukrainian government has made significant progress in accelerating digital transformation and continues to support digitalization. Digitalization is now the basis for successful customer communications, reducing overall costs and optimizing business processes. Since December 2022, most Ukrainian businesses have been operating with certain restrictions, in an online format, with*