Міністерство освіти і науки України

Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Навчально-науковий інститут фінансів, економіки,
управління та права
Кафедра фінансів, банківського бізнесу та оподаткування

ЕКОНОМІЧНА БЕЗПЕКА: ДЕРЖАВА, РЕГІОН, ПІДПРИЄМСТВО

Матеріали IX Міжнародної
науково-практичної конференції

15 травня 2025 р.

Полтава
2025

UDC 330.341.1:004.738.5:355.45(477)

Buriak Alona,
PhD, Associate Professor
National University «Yuri Kondratyuk Poltava Polytechnic»

SECURITY-ORIENTED INFORMATION ENVIRONMENT AS A STRATEGIC RESOURCE FOR UKRAINE'S ECONOMIC SECURITY IN WARTIME AND POST-WAR RECOVERY[1]

Since the full-scale Russian invasion of Ukraine in February 2022, the information sphere has transformed from a communication space into a battleground for hybrid warfare. Under the conditions of war, information has acquired the characteristics of a strategic resource, the effective management of which directly influences both the defense capability and economic resilience of the state. The formation of a security-oriented information environment (SOIE) has become not only a component of the national security concept but also a crucial element of economic security, both in the short- and long-term perspectives.

This paper aims to provide a theoretical and methodological justification for the role of SOIE in ensuring Ukraine's economic security during wartime and the subsequent recovery period, as well as to outline the strategic directions for its institutional development.

Ukraine's current information environment operates under conditions of multifaceted destabilization: systemic cyberattacks, waves of disinformation, erosion of trust in state institutions, psychological pressure on society, and manipulation of economic

[1] Тези підготовлено в межах виконання НДР молодих учених «Формування безпекоорієнтованого інформаційного середовища для підвищення економічної безпеки України у воєнний та повоєнний періоди», державний реєстраційний номер 0124U000615

data [1]. These factors undermine not only public confidence but also directly affect economic processes – investment climate, operations of strategic enterprises, the banking system, capital markets, and financial behavior of households.

The development of SOIE requires a comprehensive approach combining institutional, technological, regulatory, and cultural components. Its key functions include:

Protection of critical economic information. This involves cybersecurity in both the public and private sectors, data leakage prevention, and protection of the information infrastructure of critical infrastructure facilities, including energy, transport, and finance.

Counter-propaganda and resistance to economic disinformation. Russian information-psychological operations often aim to provoke panic about supply shortages, financial instability, and loss of macroeconomic control [2]. It is crucial to develop both governmental and civic mechanisms for rapid verification and debunking of economic disinformation.

Building public trust in national institutions. Transparency of fiscal policy, effective communication with businesses and the population, and the digitalization of public services are factors that directly contribute to economic resilience during martial law.

Coordination between state authorities, the private sector, and international partners. In wartime, a unified information platform for exchanging threat intelligence and cyber incident data becomes critical.

Education and awareness-raising on information security for economic actors [3]. Businesses, especially small and medium enterprises, need access to educational resources on cyber hygiene, financial security, and appropriate responses to information attacks.

In the post-war period, the role of SOIE will further increase. As the Ukrainian economy recovers and investment potential grows, the state will face competition for financial and human

capital amid ongoing geopolitical tensions [4]. Information transparency, adherence to European standards, secure digital services, and a positive international information image will become key factors of national attractiveness.

Priority tasks for this stage include [5]:

– institutionalization of strategic communication in economic policy;

– implementation of a national digital risk monitoring system;

– development of cybersecurity certification systems for digital services;

– establishment of an independent platform for analyzing economic disinformation;

– international cooperation within EU digital resilience initiatives (e.g., Cyber Solidarity Act).

The establishment of a security-oriented information environment must be recognized as a strategic national priority, especially in light of the unprecedented hybrid threats faced by Ukraine since the onset of full-scale military aggression. SOIE plays a pivotal role in safeguarding economic sovereignty by ensuring the continuity and integrity of critical economic functions, protecting national digital assets, and enhancing public and investor confidence in the resilience of the Ukrainian state.

An effectively designed SOIE contributes to early threat detection, rapid response mechanisms, and prevention of cascading economic disruptions caused by cyberattacks or information manipulation. It ensures that state institutions and economic actors operate within a trusted digital ecosystem, where strategic communication, data protection, and transparency are fundamental principles. In such an environment, both domestic and international stakeholders – including businesses, donors, and development partners – are more likely to engage in long-term economic activities, knowing that information-related risks are systematically monitored and mitigated.

Moreover, the role of SOIE extends beyond reactive defense mechanisms. It must also serve as a proactive driver of economic transformation in the post-war period. This involves embedding digital trust, data ethics, and security-by-design principles into all levels of economic governance – from public procurement to digital banking and e-governance platforms. By doing so, Ukraine will not only restore economic stability but also position itself as a digitally resilient state aligned with European standards of cybersecurity and strategic autonomy.

References

1. Masliy O.A., Buriak A.A. (2023) Transformation of threats for the economic security and security of the infor-mation environment of Ukraine in the conditions of a full-scale war. State and regions. Series: Economics and Business, no. 3(129), pp. 28–32.

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. Buriak A., Masliy O. Strategic foundations of security-oriented international space: economic, informational and ecological dimensions. Економіка і регіон. 2024. №1 (92). С. 281–287. DOI: https://doi.org/10.26906/EiR.2024.1(92).3341.

4. Buriak A., Levchenko I. The role of international organizations in the formation of a security-oriented information environment and the implementation of strategies for ensuring the economic and ecological security of Ukraine. Current problems of sustainable development. 2024. No 1. Vol. 1. P. 7–12.

5. Buryak, A.A., Makhovka, V.M., & Storozhuk, L.M. (2023). Strategy and mechanisms for implementing the digital economy in the EU and Ukraine as a condition for overcoming the crisis. Economy and Region, 2(89), 53-59. DOI: https://doi.org/10.26906/eip.v0i2(89).2934.