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

Білостоцький технологічний університет (Польща)

Університет прикладних наук (Литва)

Відземський університет прикладних наук (Латвія)

Університет «Aurel Vlaicu» в м. Арад (Румунія)

Міжнародний науково-освітній та навчальний центр (Естонія)

Київський національний університет імені Тараса Шевченка
Кафедра фінансів

Донецький національний університет імені Василя Стуса

Національний технічний університет «Дніпровська політехніка»

Луцький національний технічний університет

Одеський національний економічний університет

РОЗВИТОК ФІНАНСОВОГО РИНКУ В УКРАЇНІ: ЗАГРОЗИ, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Матеріали VII Міжнародної науково-практичної конференції

27 листопада 2025 р.

Полтава
2025

6. Підхомний О.М. Фінансова безпека України: інструменти і стратегії формування: монографія. Львів. нац. ун-т ім. І. Франка. - Львів : ЛНУ ім. І. Франка, 2014. 319 с.
7. Oxford Advanced Learner's Dictionary. Oxford, 1995. 1475 p.

UDC 338.2:004.056.5

***Buriak Alona*[1],**
PhD, Associate Professor
National University «Yuri Kondratyuk Poltava Polytechnic» (Ukraine)

TRANSFORMATION OF DIGITAL THREAT MONITORING SYSTEMS IN THE CONTEXT OF BUILDING A SECURITY-ORIENTED INFORMATION ENVIRONMENT OF UKRAINE DURING THE WAR AND POST-WAR PERIODS

As of 2025, the development of a security-oriented information environment has become a critical prerequisite for Ukraine's economic resilience, as the digital sphere has transformed into a central front of hybrid warfare. The increasing number of attacks on critical infrastructure, energy facilities, and the financial sector necessitates the modernization of mechanisms for detecting and neutralizing threats. Contemporary approaches focused on dynamic behavioural analytics, AI-driven detection, and the development of national situational awareness systems create opportunities for establishing a balanced model of economic security [1]. These factors determine the relevance of studying the transformation of digital threat-monitoring systems amid wartime operations and post-war recovery.

In the context of Russia's military aggression against Ukraine, the key trend of 2024–2025 has been a shift from classical DDoS attacks to targeted operations aimed at disrupting and intercepting control over critical infrastructure [2, 3]. This necessitates transitioning from traditional cybersecurity tools to proactive monitoring platforms capable of forecasting behavioural anomalies based on large-scale datasets. As noted by contemporary scholars, structural changes in the digital environment require a conceptual renewal of economic security models through the integration of digital analytics, institutional regulatory tools, and mechanisms of international cooperation [4, 5].

The modernized monitoring system includes the following key elements [6]: machine-learning-based platforms for cyber-incident analytics, capable of self-improvement; a unified information space for data exchange between state and private actors; indicator-metric dashboards for evaluating digital risks, enabling strategic planning of economic security; international cyber-cooperation instruments, which reduce the aggressor's digital sovereignty within global networks. To assess the tendencies in shaping a security-oriented digital environment, the dynamics of incidents that affected state and economically critical systems were analyzed (table 1).

The presented data demonstrate a positive trend toward reducing the number of critical incidents as monitoring platforms are modernized and AI-based threat-assessment models are introduced. The reduction of detection time by more than threefold indicates an increase in the resilience of the information environment, which serves as a fundamental component of economic security during wartime.

In the post-war period, the transformation of monitoring systems should be aimed at preventing economic losses from cyber incidents, enhancing the digital capabilities of

[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

businesses, and integrating Ukraine into the unified European security space. According to modern scientific approaches [7], systematic digital adaptation ensures a synergistic effect between technological, institutional, and economic components of national security.

Table 1

Dynamics of digital incidents affecting Ukraine's economic security (2022–2025)

Indicator	2022	2023	2024	2025 (forecast)	Change 2022–2025, %
Number of critical cyber incidents, units	987	812	690	640	–35,2
Share of attacks targeting the energy sector, %	28	34	37	41	+13
Identified attempts to compromise financial data integrity, units	412	381	345	330	–19,9
Incident detection time, hours	19.4	14.1	8.7	6.5	–66,4

Source: analytical summaries of the State Service for Special Communications and Information Protection of Ukraine and CERT-UA, 2022–2025.

The transformation of digital threat-monitoring systems is a key factor in strengthening Ukraine's economic security during the war and throughout the post-war reconstruction period, as the digital domain has become a decisive arena for both economic resilience and national stability. In modern conditions, monitoring is no longer limited to the passive registration of cyber incidents; instead, it relies on predictive analytics, continuous data correlation, and multi-vector threat attribution, allowing for the early identification of hostile digital activities before they cause damage to critical assets. The implementation of advanced data-analytics platforms, AI-driven risk-assessment tools, and standardized security indicators contributes to the creation of an integrated and adaptive information environment capable of resisting high-intensity hybrid threats, including those aimed at disrupting supply chains, financial systems, and energy infrastructure. These technologies strengthen institutional cooperation between state bodies and private actors, improve economic decision-making processes, and ensure the transparency of information flows essential for macroeconomic stability.

Furthermore, the introduction of automated anomaly-detection systems and unified cross-sectoral data-exchange frameworks enable real-time situational awareness, significantly enhancing the efficiency of national and corporate cybersecurity strategies. The obtained results indicate not only a reduction in critical incidents and improved response efficiency but also demonstrate the formation of long-term patterns of digital resilience, which reduce the vulnerability of key sectors to repeated attacks and accelerate the recovery of damaged assets.

References

1. Buriak A.A., Kudriashova D.O., Storozhuk L.M. Strategy for the Development of the Digital Economy in Ukraine: National Vision and the Challenges of Globalization. *Waste Management System in the Circular Economy: Financial, Social, Environmental and Energy Determinants: Monograph.* Sumy: Sumy State University, 2023, pp. 239–248.

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

3. Onyshchenko, S., Matkovskyi, A., Puhach, A. Analysis of threats to economic security of Ukraine in conditions of innovative economic development. *Economic Annals-XXI,* 2014, 1-2(2), 8-11. URL: http://nbuv.gov.ua/UJRN/ecchado_2014_1-2(2)__3

4. Buriak A.A. UN Priorities in Improving International Information Security. *Sustainable Development: Challenges and Threats in Modern Realities: Proceedings of the II*

International Scientific and Practical Online Conference, June 6, 2024. Poltava: Yuri Kondratyuk National University, 2024, pp. 181–182.

5. Onyshchenko, S., Zhyvylo, Y., Cherviak, A., & Bilko, S. (2023). Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. Eastern-European Journal of Enterprise Technologies, 5(13 (125), 65–76.

6. Buriak A., Maslii O., Kudinova A. Identification of trigger points in the impact of information security on economic stability under conditions of international instability. *International Humanitarian University Herald. Economics and Management*. 2024. No 61. P. 32 – 38. DOI: https://doi.org/10.32782/2413-2675/2024-61-5.

7. Cherviak A.V., Buriak A.A., Tsyganenko K.D. Peculiarities of Forming a Security-Oriented Information Environment of the National Economy. *Scientific Bulletin of Kherson State University. Series "Economic Sciences"*, 2024, No. 52, pp. 19–25. DOI: https://doi.org/10.32999/ksu2307-8030/2024-52-3

УДК 338.242.2

Микитюк Оксана Петрівна,
докторантка економічного факультету, кандидат економічних наук, доцент
Київський національний університет імені Тараса Шевченка (Україна)

ФІНАНСОВА БЕЗПЕКА ЯК БАЗОВА ДЕТЕРМІНАНТА ФОРМУВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННОЇ ТА ПОСТВОЄННОЇ ТРАНСФОРМАЦІЇ

В умовах повномасштабної агресії рф питання стійкості національної економіки отримало інше, значно глибше змістовне наповнення. Економічна безпека у таких обставинах розглядається не лише як теоретична категорія, а як реальний інструмент підтримання життєздатності держави. Її сутність полягає у здатності економічної системи протистояти загрозам різного характеру та забезпечувати умови для відтворення й розвитку навіть за наявності критичних зовнішніх факторів впливу. Особливо вагомою у структурі економічної безпеки є фінансова безпека, яка формує основу макрофінансової стабільності та визначає межі можливого для державної економічної політики [1; 2; 3].

Вторгнення рф суттєво трансформувало структуру загроз і підсилило ті вразливості, які раніше не мали настільки очевидного впливу. Фінансова безпека в цих умовах стала не лише складовою економічної безпеки, а й чинником, що визначає межі державного суверенітету та здатність країни реагувати на наслідки воєнних дій [4; 5]. Зростання фіскального тиску, порушення логістичних ланцюгів, зміна структури економічної активності, збільшення секторальних ризиків — усе це актуалізувало потребу у переосмисленні інструментів управління фінансовою системою.

Структура фінансової безпеки, визначена у методичних підходах Міністерства економічного розвитку і торгівлі України [6], залишається релевантною й у воєнний період. Її складові , зокрема, банківська, бюджетна, боргова, грошово-кредитна, валютна та безпека небанківського сектору, демонструють різний ступінь чутливості до воєнних шоків. Саме їх непослідовна динаміка, як свідчить проведений інтегральний аналіз, у 2022 році сформувала високу волатильність показників фінансової безпеки: зміни військових видатків, частки непрацюючих кредитів, коливань валютного курсу, зовнішнього боргу та резервів пояснили 63,9% варіації інтегрального індексу. Цей результат підтверджує підвищену вразливість фінансової системи до зовнішніх потрясінь. Крім того, навіть до початку війни низка макроекономічних параметрів уже