UDC 658.1:005.334:004.056
JEL D81, G32, L86, M15, O33
DOI: https://doi.org/10.32782/2786-8273/2026-15-34

Inna Sytnyk
Doctor of Economic Sciences, Professor,
Head of the Department of Economic Theory,
National University of Food Technologies
ORCID: https://orcid.org/0000-0002-3906-770X
Ситник І.П.
Національний університет харчових технологій

Oleksandr Bosenko
PhD in Economics,
Associate Professor of the Department of Economic Theory,
National University of Food Technologies
ORCID: https://orcid.org/0009-0004-3414-8908
Босенко О.С.
Національний університет харчових технологій

Tatiana Shved
Senior Lecturer of the Department of Economic Theory,
National University of Food Technologies
ORCID: https://orcid.org/0000-0002-9385-4819
Швед Т.В.
Національний університет харчових технологій

ECONOMIC SECURITY OF A DIGITAL ENTERPRISE AMID GROWING CYBER THREATS AND FINANCIAL RISKS

ЕКОНОМІЧНА БЕЗПЕКА ЦИФРОВОГО ПІДПРИЄМСТВА В УМОВАХ ЗРОСТАННЯ КІБЕРЗАГРОЗ І ФІНАНСОВИХ РИЗИКІВ

Abstract. Introduction. *For an enterprise that sells through marketplaces, accepts payments via payment service providers and keeps its records in the cloud, an outage of digital infrastructure means that revenue simply stops. A cyber incident starts as a technical event but within hours becomes a financial one, bringing lost sales, recovery costs, frozen funds and customer claims. Yet most methods for assessing enterprise economic security still add the digital dimension as one more component of an integral index and treat the components as independent of each other.* ***Purpose.*** *The article seeks to substantiate the theoretical and methodological basis for assessing the economic security of a digital enterprise, to develop a set of indicators covering financial, operational, cyber, platform and information risks, and to propose an integral assessment that takes into account how threats spread from one security component to another.* ***Methods.*** *We use systemic and structural analysis, abstraction and generalisation, threshold-based normalisation of indicators, the analytic hierarchy process to derive weights, a cross-impact matrix of threat transmission, weighted geometric aggregation and scenario analysis.* ***Results.*** *Threats are grouped by the channel through which they turn into economic losses: revenue generation, payment flows, assets, costs and liabilities, and market position. We propose 18 indicators in five components, among them the coverage ratio of digital losses, actual recovery time relative to maximum tolerable downtime, the concentration of sales channels and reliance on a single payment service provider. The integral index is computed twice, as an actual value and as a value adjusted for cascading effects, and the gap between the two is treated as latent cascade vulnerability. For a conditional e-commerce company, the additive estimate (0.606) proved noticeably higher than the cascade-adjusted one (0.526), and a ransomware stress scenario pushed the adjusted index down to 0.272.* ***Conclusion.*** *The approach expresses digital threats in economic terms and helps decide which measures to take first. In our calculations, business continuity planning gave the largest gain, followed by vulnerability management, cyber insurance and a backup payment provider, while the cascade adjustment exposed weaknesses that conventional additive aggregation leaves unnoticed.*

Keywords: *enterprise economic security, digital enterprise, cyber risks, financial risks, digital platforms, digital payment systems, business continuity, economic resilience.*

Анотація. *Стаття присвячена оцінюванню економічної безпеки підприємств, діяльність яких залежить від цифрових платформ, інформаційних систем та електронних платежів. Запропоновано класифікувати загрози за каналами, через які вони перетворюються на економічні втрати, і сформовано систему з 18 показників за фінансовою, операційною, кібербезпековою, платформною та інформаційною складовими. Розроблено методику інтегрального оцінювання, у якій показники нормуються щодо критичних і цільових значень, ваги визначаються методом аналізу ієрархій, а рівні складових коригуються з урахуванням каскадного поширення загроз. Апробація на умовному підприємстві електронної комерції показала, що адитивна оцінка завищує рівень безпеки, а найбільший ефект дають заходи із забезпечення безперервності бізнес-процесів.*

Ключові слова: *економічна безпека підприємства, цифрове підприємство, кіберризики, фінансові ризики, цифрові платформи, цифрові платіжні системи, безперервність бізнес-процесів, економічна стійкість.*

© Inna Sytnyk, Oleksandr Bosenko, Tatiana Shved, 2026
Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

Problem statement. Until recently, a website outage was, for most Ukrainian enterprises, a nuisance to be dealt with by the system administrator; for a company that sells through marketplaces, accepts payments via payment service providers, keeps its accounts in the cloud and manages logistics through an ERP system, the same event today means that revenue simply stops flowing, and an incident that began as a purely technical one turns into a financial one within a matter of hours.

The scale of the problem is evident from recent data: according to IBM, the global average cost of a data breach in 2025 was USD 4.44 million [15], while in the Allianz survey cyber incidents have topped the list of business risks for the fifth year running (42% of responses), with business interruption, which is most often their consequence, ranking third (29%) [9]. Ukrainian statistics are no less telling, as CERT-UA handled 5,927 cyber incidents in 2025, 37% more than a year earlier [6], and losses from payment card fraud rose by 24% to UAH 1.4 billion, with social engineering accounting for 90% of this amount [7].

Meanwhile, Ukrainian methods for assessing enterprise economic security usually just add the digital component to the integral index alongside the others, and, in our view, this misses the essential point: digital threats are never given an economic dimension, and the components are treated as independent, even though in a digital business a weak spot in cybersecurity quickly makes itself felt in operations and, subsequently, in the enterprise's financial position.

Analysis of recent research and publications. The economic view of information security has a fairly long history, and its starting point is usually considered to be the model of L. Gordon and M. Loeb, who showed that, for typical vulnerability functions, investing more than about 37% (1/*e*) of the expected loss from an incident in protection is not justified [14], after which cybersecurity came to be regarded as a matter of economic choice. S. Kamiya and co-authors found that attacks involving the leakage of customers' financial data reduce shareholder value far more than direct costs can explain, and attributed this gap to reputational losses [16], while C. Florackis, C. Louca, R. Michaely and M. Weber showed that the market prices cyber risk, as the shares of highly exposed companies fall markedly when cyber threats intensify [13]. Of particular interest for our study is the conclusion of I. Aldasoro and co-authors that higher IT spending reduces subsequent losses, whereas dependence on cloud providers increases the likelihood of extreme losses [8]. M. Eling, M. McShane and T. Nguyen argue for a focus on cyber resilience [11], and D. Cutolo and M. Kenney have described the imbalance of power between platforms and the entrepreneurs who depend on them and have to accept that a platform may unilaterally change its rules or suspend an account [10].

Ukrainian authors mostly approach the problem from the standpoint of the economic security system: O. A. Yermolenko and R. S. Nasrullaiev formulated the principles of building such a system under digitalisation [1], D. O. Serhieieva and I. I. Nahorna proposed an integral assessment method with a separate digital component [2], and works [4; 5] treat cybersecurity and digital security as core components of economic security. We have previously examined the payment dimension of the problem using the example of Ukraine's payment system [12] and e-commerce [3], and in [18; 19] we substantiated the shift towards proactive risk management in digital business based on intelligent technologies.

At the same time, several issues remain open, since the digital component is still aggregated additively, indicators of platform and payment dependence are almost absent from existing methods, and the mechanism by which threats are transmitted between the components of economic security has not been formally described.

The purpose of the article is to substantiate the theoretical and methodological foundations for assessing the economic security of a digital enterprise amid growing cyber threats and financial risks, to develop a system of indicators for a comprehensive assessment of threats, and to devise an approach to ensuring the economic resilience of enterprises whose activities depend on digital platforms, information systems and electronic payments.

Research methods. The components of economic security were identified by means of systemic and structural analysis, and threats were classified using abstraction and generalisation; the indicators were normalised against threshold values and aggregated by a weighted geometric mean with weights derived by the analytic hierarchy process [17], while the cascading spread of threats was described by a cross-impact matrix. The method was tested through scenario analysis, and the calculations were performed in Python on model data for a conditional enterprise.

Presentation of the main research material. ***Transformation of economic threats to the enterprise under the digitalisation of business processes.*** By a *digital enterprise* we mean a business entity for which most of its revenue, settlements with customers and key business processes critically depend on information systems and external digital infrastructure – platforms, payment services and cloud environments. Accordingly, we understand its *economic security* as the ability to maintain revenue, solvency and market position when its own or external digital infrastructure is compromised, unavailable or subject to unilateral changes in terms of use by its owner, and to restore them within an acceptable time and at an acceptable cost. We have deliberately included the time and cost of recovery in the definition, because the losses of a digital enterprise are counted in hours, while the average incident lifecycle, according to IBM, is 241 days [15].

As regards the threats themselves, we see at least five shifts: business value is increasingly concentrated in information assets (customer databases, advertising accounts, platform ratings), threats materialise much faster, control over critical processes is handed over to marketplaces, payment service providers and cloud services although dependence on them does not go away [8; 10], attacks increasingly target people rather than technology (in Ukraine, 90% of card fraud losses are caused by social engineering [7]), and attackers seek not to steal data quickly but to gain a long-term foothold in the infrastructure, which only increases the final losses. Under these circumstances, conventional classifications of threats by source or by area of manifestation are of little use, since the same phishing attack is at once external and internal, technological and personnel-related, so we propose a different criterion – the *channel through which a threat is transformed into economic losses*, i.e. the element of the economic mechanism through which it reduces the value of the enterprise (Table 1).

Table 1

Classification of threats to the economic security of a digital enterprise by channels of their transformation into economic losses

Transformation channel	Typical digital threats (superimposed on traditional ones)	Economic consequences: primary → secondary
1. Revenue generation	Website unavailability (DDoS, cloud failures), suspension of a marketplace account, changes in ranking algorithms	Lost revenue and margin → lower conversion and market share
2. Payment flows	Payment fraud, social engineering, payment provider limits, funds withheld by the acquirer, chargebacks	Direct losses → weaker liquidity, disrupted settlements
3. Assets	Data encryption (ransomware), account compromise, theft of commercial information	Loss of intangible assets → loss of competitive advantages
4. Costs and liabilities	Recovery costs, sanctions for personal data protection breaches, customer lawsuits	Unplanned costs → lower profitability, legal liabilities
5. Market position and reputation	Public leak of customer data, phishing clones of the brand, loss of a partner platform's trust	Customer churn → lower business value

Source: developed by the authors

Since each channel maps directly onto accounting indicators – revenue, liquidity and profitability – this classification not only puts threats in order but also suggests which indicators the assessment system should be built from.

Financial, operational and cyber risks in the economic security system of a digital enterprise. The analysis usually begins with financial, operational and cyber risks, but for a digital business we believe two more groups should be added – platform dependence risks and information risks (Table 2). We have singled out platform risks for a reason, as the suspension of an account on a marketplace or a change in its ranking algorithm may occur without any security incident at all, while the blow to revenue will be no smaller [10].

The crucial point is that these risks do not exist in isolation, as a typical scenario clearly shows: an employee opens a phishing email, an attacker gains access to an administrator account and, after two weeks of undetected presence in the system, encrypts the ERP server and the website. For several days the enterprise can neither sell through its own website nor process marketplace orders, the payment service provider restricts payouts after noticing unusual activity, and then come the costs of incident response and customer compensation and, if there is no liquidity buffer, delayed payments to suppliers. The technical damage is thus multiplied along the chain, and it is the size of this "multiplier" that determines how well the enterprise is protected economically. The links between risk groups are asymmetric: cyber risks are mostly the primary source, operational failures almost immediately become financial losses, whereas financial weakness affects cybersecurity indirectly and with a lag – through underfunding of protection, and it is this asymmetry that we formalise below by means of threat transmission coefficients.

System of indicators for assessing the economic security of a digital enterprise. We selected the indicators so that they could be calculated from data the enterprise already has (financial statements, management accounts, IT monitoring, platform and payment provider reports) and so that each of them would be linked to one of the channels listed in Table 1. Two thresholds are set for each indicator – a critical value x_{cr}, at which the security component is effectively lost, and a target value x_t, beyond which further improvement makes no economic sense (Table 3).

Alongside well-known financial indicators, which ultimately reflect the consequences of all threats, the system includes indicators that we have not encountered in methods for assessing enterprise economic security. The *digital loss coverage ratio* (F3) answers the question of whether the enterprise would survive a realistic incident without losing solvency, while the *ratio of recovery time to maximum tolerable downtime* (O2) translates a technical parameter into economic terms, since a value above one means that the enterprise would take longer to recover than it can hold out without irreversible losses. Indicators P1–P4 make it possible to quantify platform and payment dependence, which is usually described only qualitatively. The thresholds were selected for medium-

Table 2

Risk groups in the economic security system of a digital enterprise and the links between them

Risk group	Main manifestations	Typical economic consequences	Groups from which threats are received
Financial	Payment fraud, unauthorised transactions, disruption of payment operations	Direct losses, cash gaps, falling liquidity	Cyber, operational, platform, information
Operational	Information system failures, platform unavailability, interruption of business processes	Downtime, lost revenue, unplanned costs	Cyber, platform; financial (with a lag)
Cyber	Cyberattacks, phishing, ransomware, unauthorised access	Response costs, data loss, sanctions	Primary source
Platform	Unilateral rule changes, account suspension, concentration of sales and payments	Loss of a sales channel, higher fees	External source
Information	Data leaks, access violations, loss of information integrity	Regulatory sanctions, lawsuits, reputational losses	Cyber

Source: developed by the authors based on [8; 10; 11]

Table 3

System of indicators for assessing the economic security of a digital enterprise and their values for conditional enterprise "A"

Code	Indicator (unit)	Type	x_{cr}	x_t	Base	Stress
Financial component (F)						
F1	Current liquidity ratio	S	1	2	1.45	1.27
F2	EBITDA margin, %	S	2	12	8.4	5.6
F3	Digital loss coverage ratio: (free cash + cyber insurance limit) / stress-scenario losses	S	0.5	1.5	0.9	0.62
F4	Direct losses from digital incidents, % of revenue	D	2	0.1	0.35	1.45
Operational component (O)						
O1	Unplanned downtime of critical systems, hours/year	D	72	8	21	68
O2	Ratio of actual recovery time to maximum tolerable downtime (RTO/MTPD)	D	1.5	0.5	0.8	1.3
O3	Share of critical processes covered by tested continuity plans, %	S	30	90	55	55
Cybersecurity component (C)						
C1	Significant cyber incidents per 100 employees, per year	D	5	0.5	1.6	3.2
C2	Share of critical vulnerabilities remediated on time, %	S	50	95	72	72
C3	Mean time to detect an incident (MTTD), days	D	30	1	9	14
C4	Share of accounts with multi-factor authentication, %	S	50	100	81	81
Platform component (P)						
P1	Share of revenue through the largest platform, %	D	70	25	48	48
P2	Herfindahl–Hirschman index of sales channels, points	D	6,000	2,500	3,448	3,448
P3	Share of receipts through a single payment provider, %	D	90	40	74	74
P4	Time to switch to a backup channel, days	D	14	1	6	6
Information component (I)						
I1	Leaks of personal data and commercial information, per year	D	3	0	1	2
I2	Share of information resources protected in line with policy, %	S	40	95	68	68
I3	Share of employees who passed a phishing test, %	S	50	95	77	77

Note: S – stimulant, D – destimulant; "Base" and "Stress" – values for the baseline and stress scenarios (model data). Source: developed by the authors

sized e-commerce enterprises and will therefore need to be adjusted for other industries.

Methodological approach to the comprehensive assessment of the economic security of a digital enterprise. The proposed approach consists of five stages that form a monitoring cycle (Fig. 1).

Once the threats have been identified and the links between risk groups established, the partial indicators are normalised against the threshold values:

$$z_{ij} = min\left\{1; max\left\{0; \frac{x_{ij} - x_{ij}^{cr}}{x_{ij}^{t} - x_{ij}^{cr}}\right\}\right\} \quad (1)$$

where z_{ij} is the normalised value of the i-th indicator of the j-th component; x_{ij} is the actual value; x_{ij}^{cr}, x_{ij}^{t} are the critical and target values. Formula (1) is suitable for both stimulants and destimulants, since for the latter $x^{cr} > x^{t}$ and z_{ij} decreases as the indicator grows, and the security level of the k-th component is defined as the mean of the normalised values of its n_k indicators:

$$S_k = \frac{1}{n_k}\sum_{i=1}^{n_k} z_{ik} \quad (2)$$

The main novelty of the approach is the adjustment of component levels for the cascading spread of threats, for which we denote by $d_{lk} \in [0; 1]$ the threat transmission coefficient, i.e. the share of the "security deficit" $(1 - S_l)$ of component l that passes to component k. The adjusted security level of a component is then:

$$S_k^{*} = S_k \cdot \left(1 - \sum_{l \neq k} d_{lk}\left(1 - S_l\right)\right) \quad (3)$$

We set the coefficients by expert judgement in view of the asymmetry described above, and the non-zero ones are $d_{CO} = 0.20$; $d_{CF} = 0.15$; $d_{CI} = 0.25$; $d_{OF} = 0.20$; $d_{PF} = 0.15$; $d_{PO} = 0.10$; $d_{IF} = 0.10$; $d_{FO} = 0.05$ (C – cybersecurity, O – operational, F – financial, P – platform, I – information components). The components are aggregated by a weighted geometric rather than arithmetic mean, because high profitability should not "offset", say, the absence of recovery plans, so the actual and cascade-adjusted integral indices take the form:

$$I_{act} = \prod_{k=1}^{5} S_k^{w_k} \quad (4)$$

$$I_{adj} = \prod_{k=1}^{5} \left(S_k^{*}\right)^{w_k} \quad (5)$$

where w_k is the weight of the k-th component. We propose to call the difference between them the *cascade vulnerability index*, which shows what share of its security level the enterprise may lose because its components are interlinked:

$$\Delta = I_{act} - I_{adj} \quad (6)$$

The weights were determined by the analytic hierarchy process [17]: the financial component, in which the consequences of all other threats accumulate, was given a moderate preference (2) over the operational and cybersecurity components and a stronger one (3) over the platform and information components, while the operational and cybersecurity components were considered equally important and moderately more important (2) than the last two. As a result, the weights $w_F = 0.369$; $w_O = w_C = 0.206$; $w_P = w_I = 0.109$ were obtained with a consistency ratio CR = 0.003, well below the acceptable 0.1, and we propose interpreting the integral index on the following scale: [0.75; 1] – high level of economic security; [0.60; 0.75) – sufficient; [0.45; 0.60) – unstable; [0.30; 0.45) – low; [0; 0.30) – critical.

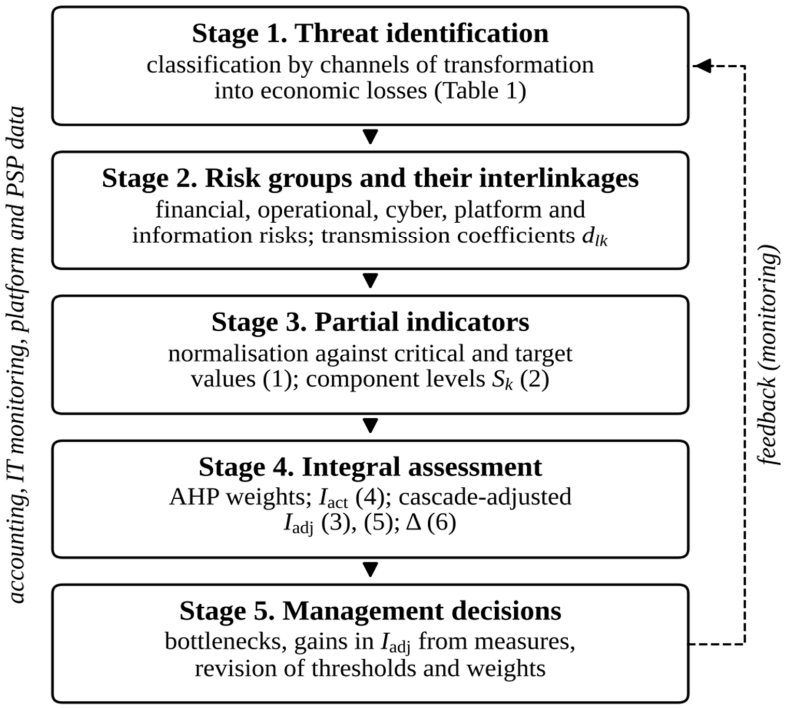


Figure 1. Stages of the methodological approach to the comprehensive assessment of the economic security of a digital enterprise

Source: developed by the authors

The method was tested on a conditional enterprise "A", an online retailer of household electronics with annual revenue of UAH 180 million and a staff of 125, which earns almost half of its revenue (48%) through a single marketplace, 30% through its own website, 12% through social commerce and 10% from B2B sales (Herfindahl–Hirschman index of 3,448 points), while 74% of its cashless receipts pass through a single payment service provider. The stress scenario reproduces the chain described above (68 hours of downtime, a leak of the customer database, payment provider limits), under which direct losses reach 1.45% of revenue (about UAH 2.6 million) and the EBITDA margin falls from 8.4% to 5.6%, whereas structural indicators cannot change within a few days (indicator values are given in Table 3 and the results in Table 4).

Under normal conditions, the additive (0.606) and actual (0.605) indices suggest that the enterprise's security level is sufficient, albeit only just, but the adjusted index I_{adj} = 0.526 lowers this assessment to the unstable level, and the index Δ = 0.079 means that about 13% of the "formal" security is in fact conditional. The stress scenario confirms this conclusion, as the actual index falls to 0.337 and the adjusted one to 0.272, i.e. to the low and critical levels respectively. Notably, it is not the cybersecurity component, where the threat first materialised, that suffers most (0.647 → 0.515), but the operational (0.638 → 0.226) and financial (0.590 → 0.260) components, which, in our view, once again shows that digital threats are first and foremost an economic problem, all the more so since even in the baseline scenario the financial component turns out to be the weakest once cascading effects are taken into account (S_F^* = 0.451). The impact of management measures, which constitute the final stage of the assessment, is shown in Table 5.

Table 4

Component levels and integral indices of economic security of conditional enterprise "A"

Component	Baseline: S_k	Baseline: S_k^*	Stress: S_k	Stress: S_k^*
Financial (F)	0.590	0.451	0.260	0.169
Operational (O)	0.638	0.550	0.226	0.186
Cybersecurity (C)	0.647	0.647	0.515	0.515
Platform (P)	0.538	0.538	0.538	0.538
Information (I)	0.592	0.540	0.481	0.423
Integral indices				
Additive (for comparison)	0.606		0.360	
Actual I_{act} / adjusted I_{adj}	0.605	0.526	0.337	0.272
Cascade vulnerability index Δ		0.079		0.065

Source: calculated by the authors on model data

Table 5

Impact of management measures on the integral economic security index of the conditional enterprise

Measure	Change in indicators	I_{act}	I_{adj}	ΔI_{adj}
Baseline	–	0.605	0.526	–
M1. Connecting a backup payment provider and a backup sales channel	P3: 74 → 45%; P4: 6 → 2 days	0.628	0.558	+0.032
M2. Developing and testing business continuity and disaster recovery plans (BCP/DRP)	O3: 55 → 85%; O2: 0.8 → 0.6	0.645	0.574	+0.047
M3. Cyber insurance and a dedicated liquidity reserve	F3: 0.90 → 1.30	0.641	0.558	+0.032
M4. Vulnerability management process and 24/7 monitoring	C2: 72 → 90%; C3: 9 → 4 days	0.631	0.560	+0.034
M5. Developing the company's own web sales channel	P1: 48 → 35%; P2: 3,448 → 3,150	0.616	0.540	+0.014
Package of measures M1–M5		0.749	0.700	+0.173

Source: calculated by the authors on model data

The adjusted index increases most as a result of business continuity and recovery plans (+0.047), which is explained by the fact that the operational component is a kind of "hub" that receives threats from the cybersecurity and platform components and passes them on to the financial one, while vulnerability management, cyber insurance and a backup payment provider have a similar effect (+0.032…+0.034). Taken together, the measures raise I_{adj} to 0.700, i.e. to a sufficient level, and the cascade vulnerability index falls to 0.049. The method can also be used for budgeting: if the probability of the stress scenario is estimated at 20% per year and the total losses from it at about UAH 5 million, then, according to the Gordon–Loeb model, investing more than UAH 0.37 million per year in protection against this threat is not economically justified [14].

Conclusions. We have proposed classifying threats to the economic security of a digital enterprise by the channels through which they turn into economic losses (revenue generation, payment flows, assets, costs and liabilities, market position), since this approach links threats directly to accounting indicators.

The system of 18 indicators developed in the study covers five components and contains critical and target values; it includes, in particular, the digital loss coverage ratio, the ratio of recovery time to maximum tolerable downtime, and indicators of platform and payment dependence.

The methodological approach takes into account the cascading spread of threats between components, and a corresponding index is proposed to measure latent vulnerability. Testing showed that the additive assessment overstates the level of economic security, that the operational and financial components suffer the greatest losses during a cyber incident, and that business continuity measures are the most effective way to raise the level of security.

The threshold values and threat transmission coefficients are still based on expert judgement, and the method has so far been tested only on a conditional enterprise, so we see their calibration on data from real enterprises as the next step.

References:

1. Yermolenko, O. A., & Nasrullaiev, R. S. (2025). Pryntsypy zabezpechennia systemy ekonomichnoi bezpeky pidpryiemstv v umovakh tsyfrovizatsii [Principles of ensuring the economic security system of enterprises in the context of digitalization]. *Problemy ekonomiky*, *1*(63), 158–164. DOI: https://doi.org/10.32983/2222-0712-2025-1-158-164 (in Ukrainian)

2. Serhieieva, D. O., & Nahorna, I. I. (2025). Osoblyvosti zabezpechennia ekonomichnoi bezpeky pidpryiemstva v umovakh tsyfrovoi transformatsii [Features of ensuring the economic security of an enterprise in the context of digital transformation]. *Efektyvna ekonomika*, (11). DOI: https://doi.org/10.32702/2307-2105.2025.11.124 (in Ukrainian)

3. Sytnyk, I. P., Shved, T. V., & Bosenko, O. S. (2025). Horyzonty rozvytku elektronnoi komertsii u hlobalnykh trendakh ta ukrainskykh realiiakh [Horizons of e-commerce development in global trends and Ukrainian realities]. *Efektyvna ekonomika*, (12). DOI: https://doi.org/10.32702/2307-2105.2025.12.26 (in Ukrainian)

4. Stoliarenko, O. M., & Tiutchenko, S. M. (2025). Napriamy pidvyshchennia tsyfrovoi bezpeky yak krytychnoi skladovoi ekonomichnoi bezpeky [Directions for enhancing digital security as a critical component of economic security]. *Efektyvna ekonomika*, (7). DOI: https://doi.org/10.32702/2307-2105.2025.7.5 (in Ukrainian)

5. Khalina, O. V., & Shmahalo, V. I. (2025). Stratehiia rozvytku ekonomichnoi bezpeky pidpryiemstv v umovakh tsyfrovykh transformatsii [Strategy for developing the economic security of enterprises in the context of digital transformations]. *Ekonomika ta suspilstvo*, (73). DOI: https://doi.org/10.32782/2524-0072/2025-73-138 (in Ukrainian)

6. Khandusenko, N. (2026, January 8). U 2025 rotsi kilkist vorozhykh kiberatak zrosla na 37%: koho atakuiut naichastishe [In 2025, the number of hostile cyberattacks grew by 37%: who is attacked most often]. *DEV.UA*. https://dev.ua/news/u-2025-rotsi-kilkist-kiberatak-zrosla-na-37-1767858414 (in Ukrainian)

7. National Bank of Ukraine. (2026). *Shakhraistvo z platizhnymy kartkamy u 2025 rotsi: kilkist vypadkiv znyzylasia, suma zbytkiv – zrosla* [Payment card fraud in 2025: the number of cases decreased, while losses increased]. https://bank.gov.ua/ua/news/all/shahraystvo-z-platijnimi-kartkami-u-2025-rotsi-kilkist-vipadkiv-znizilasya-suma-zbitkiv--zrosla (in Ukrainian)

8. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, *60*, 100989. DOI: https://doi.org/10.1016/j.jfs.2022.100989

9. Allianz Commercial. (2026, January 14). *Allianz Risk Barometer 2026*. https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2026.html

10. Cutolo, D., & Kenney, M. (2021). Platform-dependent entrepreneurs: Power asymmetries, risks, and strategies in the platform economy. *Academy of Management Perspectives*, *35*(4), 584–605. DOI: https://doi.org/10.5465/amp.2019.0103

11. Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93–125. DOI: https://doi.org/10.1111/rmir.12169

12. Sytnyk, I., Pugachov, M., Pugachov, V., Kudrenko, N., Dovgaliuk, V., & Sytnyk, B. (2023). Features functioning of the payment system of Ukraine. *Financial and Credit Activity: Problems of Theory and Practice*, *1*(48), 42–63. DOI: https://doi.org/10.55643/fcaptp.1.48.2023.3962

13. Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies*, *36*(1), 351–407. DOI: https://doi.org/10.1093/rfs/hhac024

14. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. DOI: https://doi.org/10.1145/581271.581274

15. IBM. (2025). *2025 Cost of a Data Breach Report: Navigating the AI rush without sidelining security*. https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai

16. Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. DOI: https://doi.org/10.1016/j.jfineco.2019.05.019

17. Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, *1*(1), 83–98. DOI: https://doi.org/10.1504/IJSSCI.2008.017590

18. Sytnyk, I. P., Bosenko, O. S., & Shved, T. V. (2026). Artificial intelligence as a technological basis for modern business models in entrepreneurship and trade in the context of economic digitalization and business competitiveness for risk assessment and decision-making. *Biznes Inform*, (5), 140–148. DOI: https://doi.org/10.32983/2222-4459-2026-5-140-148

19. Sytnyk, I., Bosenko, O., & Shved, T. (2026). Intellectual technologies and big data analysis as anti-crisis consulting tools for decision-making in digital business. *Ekonomika ta suspilstvo*, (83). DOI: https://doi.org/10.32782/2524-0072/2026-83-24

Бібліографічний список:

1. Єрмоленко О. А., Насруллаєв Р. С. Принципи забезпечення системи економічної безпеки підприємств в умовах цифровізації. *Проблеми економіки*. 2025. № 1 (63). С. 158–164. DOI: https://doi.org/10.32983/2222-0712-2025-1-158-164

2. Сергеєва Д. О., Нагорна І. І. Особливості забезпечення економічної безпеки підприємства в умовах цифрової трансформації. *Ефективна економіка*. 2025. № 11. DOI: https://doi.org/10.32702/2307-2105.2025.11.124

3. Ситник І. П., Швед Т. В., Босенко О. С. Горизонти розвитку електронної комерції у глобальних трендах та українських реаліях. *Ефективна економіка*. 2025. № 12. DOI: https://doi.org/10.32702/2307-2105.2025.12.26

4. Столяренко О. М., Тютченко С. М. Напрями підвищення цифрової безпеки як критичної складової економічної безпеки. *Ефективна економіка*. 2025. № 7. DOI: https://doi.org/10.32702/2307-2105.2025.7.5

5. Халіна О. В., Шмагало В. І. Стратегія розвитку економічної безпеки підприємств в умовах цифрових трансформацій. *Економіка та суспільство*. 2025. Вип. 73. DOI: https://doi.org/10.32782/2524-0072/2025-73-138

6. Хандусенко Н. У 2025 році кількість ворожих кібератак зросла на 37%: кого атакують найчастіше. *DEV.UA*. 08.01.2026. URL: https://dev.ua/news/u-2025-rotsi-kilkist-kiberatak-zrosla-na-37-1767858414

7. Шахрайство з платіжними картками у 2025 році: кількість випадків знизилася, сума збитків – зросла / Національний банк України. 2026. URL: https://bank.gov.ua/ua/news/all/shahraystvo-z-platijnimi-kartkami-u-2025-rotsi-kilkist-vipadkiv-znizilasya-suma-zbitkiv--zrosla

8. Aldasoro I., Gambacorta L., Giudici P., Leach T. The drivers of cyber risk. *Journal of Financial Stability*. 2022. Vol. 60. Article 100989. DOI: https://doi.org/10.1016/j.jfs.2022.100989

9. Allianz Risk Barometer 2026 / Allianz Commercial. 14.01.2026. URL: https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2026.html

10. Cutolo D., Kenney M. Platform-dependent entrepreneurs: power asymmetries, risks, and strategies in the platform economy. *Academy of Management Perspectives*. 2021. Vol. 35, No. 4. P. 584–605. DOI: https://doi.org/10.5465/amp.2019.0103

11. Eling M., McShane M., Nguyen T. Cyber risk management: history and future research directions. *Risk Management and Insurance Review*. 2021. Vol. 24, No. 1. P. 93–125. DOI: https://doi.org/10.1111/rmir.12169

12. Features functioning of the payment system of Ukraine / I. Sytnyk et al. *Financial and Credit Activity: Problems of Theory and Practice*. 2023. Vol. 1, No. 48. P. 42–63. DOI: https://doi.org/10.55643/fcaptp.1.48.2023.3962

13. Florackis C., Louca C., Michaely R., Weber M. Cybersecurity risk. *The Review of Financial Studies*. 2023. Vol. 36, No. 1. P. 351–407. DOI: https://doi.org/10.1093/rfs/hhac024

14. Gordon L. A., Loeb M. P. The economics of information security investment. *ACM Transactions on Information and System Security*. 2002. Vol. 5, No. 4. P. 438–457. DOI: https://doi.org/10.1145/581271.581274

15. IBM. 2025 Cost of a Data Breach Report: navigating the AI rush without sidelining security. 2025. URL: https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai

16. Risk management, firm reputation, and the impact of successful cyberattacks on target firms / S. Kamiya et al. *Journal of Financial Economics*. 2021. Vol. 139, No. 3. P. 719–749. DOI: https://doi.org/10.1016/j.jfineco.2019.05.019

17. Saaty T. L. Decision making with the analytic hierarchy process. *International Journal of Services Sciences*. 2008. Vol. 1, No. 1. P. 83–98. DOI: https://doi.org/10.1504/IJSSCI.2008.017590

18. Sytnyk I. P., Bosenko O. S., Shved T. V. Artificial intelligence as a technological basis for modern business models in entrepreneurship and trade in the context of economic digitalization and business competitiveness for risk assessment and decision-making. *Бізнес Інформ*. 2026. № 5. С. 140–148. DOI: https://doi.org/10.32983/2222-4459-2026-5-140-148

19. Sytnyk I., Bosenko O., Shved T. Intellectual technologies and big data analysis as anti-crisis consulting tools for decision-making in digital business. *Економіка та суспільство*. 2026. Вип. 83. DOI: https://doi.org/10.32782/2524-0072/2026-83-24

Дата надходження статті: 29.09.2026
Дата прийняття статті до публікації: 06.11.2026
Дата публікації статті: 19.11.2026