ЕКОНОМІКО-МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ БІЗНЕСОВИХ ПРОЦЕСІВ

UDC: 338.24:658:004
JEL Classification: C44, D81, L20, O33
DOI: https://doi.org/10.20535/2307-5651.35.2025.352405

Kravchenko Maryna
Doctor of Economic Sciences, Professor,
Professor of the Department of Management of Enterprises
(corresponding author)
ORCID ID: 0000-0001-5405-0159

Nemyrovskyi Fedir
PhD student
ORCID ID: 0009-0008-0219-8029
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

ASSESSING THE ECONOMIC SECURITY OF ENTERPRISES UNDER DIGITAL TRANSFORMATION: AN INTEGRATED CRITIC–DEMATEL FRAMEWORK

The accelerating pace of digital transformation is fundamentally reshaping enterprise operations, simultaneously enhancing efficiency and generating new economic security risks related to information infrastructure, innovation intensity, human capital, cybersecurity, and managerial effectiveness. Traditional assessment approaches often rely on isolated indicators or purely financial metrics, which limits their ability to capture the multidimensional and interdependent nature of economic security in digitally transforming enterprises. This study develops an integrated CRITIC–DEMATEL framework to assess enterprise economic security under digital transformation. Combining objective data-driven weighting (Criteria Importance Through Inter-criteria Correlation Method, CRITIC) with causal analysis (Decision Making Trial and Evaluation Laboratory Method, DEMATEL), the framework evaluates five components: information, innovation, personnel, cybersecurity, and management. Empirical analysis of ten Ukrainian enterprises reveals that managerial and innovation components are primary drivers, while information, personnel, and security act as dependent outcomes. The approach enables an integral security index, supporting strategic prioritisation and adaptable application across industries.

Keywords: *Economic Security, Digital Transformation, Strategic Management, Criteria Importance Through Inter-criteria Correlation (CRITIC), Decision Making Trial and Evaluation Laboratory (DEMATEL), Multi-Criteria Decision-Making Method (MCDM).*

Кравченко М. О., Немировський Ф. В.
Національний технічний університет України
«Київський політехнічний університет імені Ігоря Сікорського»

ОЦІНЮВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: ІНТЕГРОВАНА МЕТОДИКА CRITIC–DEMATEL

У статті досліджено проблематику оцінювання економічної безпеки підприємств в умовах цифрової трансформації, яка суттєво змінює характер господарської діяльності, підвищує ефективність управління та водночас формує нові загрози, пов'язані з розвитком інформаційних технологій, інноваційною активністю, людським капіталом і кібербезпекою. Обґрунтовано, що традиційні підходи до оцінювання економічної безпеки, засновані переважно на фінансових показниках або ізольованих індикаторах, не дозволяють повною мірою врахувати багатовимірний і взаємопов'язаний характер сучасних ризиків цифрового середовища. Запропоновано інтегрований методичний підхід на основі поєднання методу визначення важливості критеріїв через міжкритеріальну кореляцію (англ. Criteria Importance Through Inter-criteria Correlation, CRITIC) та методу прийняття та оцінювання рішень (англ. Decision Making Trial and Evaluation Laboratory, DEMATEL),, що забезпечує об'єктивність оцінювання та можливість виявлення причинно-наслідкових зв'язків між ключовими компонентами економічної безпеки підприємства. Метод CRITIC застосовано для визначення ваг показників з урахуванням їх варіативності та міжкритеріальної кореляції, метод DEMATEL – для ідентифікації чинників-рушіїв і залежних елементів системи. Для аналізу сформовано систему з 20 показників, згрупованих у п'ять блоків: інформаційний, інноваційний, кадровий, безпеки даних та управлінський. Проведено апробацію підходу на вибірці підприємств України. Результати свідчать, що управлінський та інноваційний компоненти є ключовими чинниками

впливу на загальний рівень економічної безпеки, тоді як інформаційний, кадровий і безпековий компоненти мають переважно залежний характер. Запропонований підхід може бути використаний для стратегічного управління, моніторингу та підвищення економічної безпеки підприємств у процесі цифрової трансформації.

Ключові слова: *економічна безпека, цифрова трансформація, стратегічне управління, метод визначення важливості критеріїв через міжкритеріальну кореляцію (CRITIC), метод прийняття та оцінювання рішень (DEMATEL), метод багатокритеріального прийняття рішень (MCDM).*

Problem statement. The growing complexity and dynamism of the global economic environment have significantly intensified the challenges faced by enterprises worldwide. Market volatility, geopolitical instability, regulatory pressures, and increasing uncertainty have elevated economic security from a peripheral managerial concern to a strategic imperative for ensuring operational continuity, competitive advantage, and long-term sustainability [1; 2]. In contemporary conditions, economic security is no longer limited to maintaining financial stability; it increasingly encompasses the ability of enterprises to withstand internal and external threats, ensure organisational resilience, and adapt to rapid technological and structural changes.

Digital transformation has emerged as one of the most influential forces reshaping enterprise activities across industries. The widespread adoption of advanced information systems, automation technologies, data analytics, and cloud-based platforms has significantly enhanced operational efficiency, transparency, and decision-making capabilities [3; 4]. At the same time, digitalisation exposes enterprises to new vulnerabilities. Growing dependence on information infrastructure increases risks associated with system failures, cyberattacks, and data breaches. Moreover, the implementation of innovative technologies requires substantial investments in personnel competencies, organisational capabilities, and security mechanisms. As a result, economic security under digital transformation conditions becomes a multidimensional construct that integrates information infrastructure, innovation readiness, human capital, cybersecurity, and managerial effectiveness, all of which interact in complex and non-linear ways.

Traditional approaches to evaluating economic security predominantly rely on financial ratios, isolated operational indicators, or subjective expert assessments. Although these methods provide valuable insights, they exhibit several critical limitations. First, they fail to capture the multidimensional nature of economic security, particularly the interdependencies among technological, human, and managerial factors in digital environments. Second, they do not differentiate between factors that act as drivers of systemic change and those that represent the outcomes of underlying processes, thereby limiting their usefulness for strategic prioritisation. Third, such approaches either rely excessively on subjective judgement or disregard expert knowledge altogether, preventing a balanced integration of data-driven objectivity and domain expertise.

These limitations determine the central objective of this study, which is to develop and validate an integrated assessment framework that combines objective, data-driven weighting techniques with expert-based causal analysis. Specifically, the study proposes a hybrid CRITIC–DEMATEL approach for evaluating the economic security of enterprises under digital transformation conditions. The CRITIC (CRiteria Importance Through Intercriteria Correlation) method is applied to derive objective weights for economic security indicators based on their variability and inter-criteria correlations using empirical enterprise data. The DEMATEL (Decision Making Trial and Evaluation Laboratory) method is employed to analyse cause–effect relationships among higher-level components of economic security based on expert evaluations. By integrating these methods, the proposed framework balances statistical rigour with strategic insight, enabling both diagnostic assessment and prescriptive guidance for prioritising managerial interventions.

Analysis of recent research and publications. The concept of economic security has evolved significantly in response to changes in the global economic landscape. Traditionally, economic security was understood primarily through the lens of financial stability – an enterprise's ability to maintain solvency, liquidity and profitability [2]. However, recent research argues that economic security must encompass a broader set of capabilities, including operational continuity, resilience to disruptions, adaptive capacity and protection against technological and informational threats [1; 5].

The digital transformation, driven by Industry 4.0 technologies, such as Internet of Things (IoT), artificial intelligence, blockchain and cloud computing, has fundamentally reshaped business models and operational processes [4]. While digitalisation offers substantial benefits in terms of visibility, automation and data-driven decision-making, it also introduces new categories of risk. Cybersecurity threats, information infrastructure vulnerabilities, technological dependence and skills gaps in the workforce have emerged as critical concerns [3]. Empirical evidence suggests that enterprises with insufficient IT maturity, limited innovation adoption or weak cybersecurity practices experience greater instability and higher operational risks [1].

Despite growing recognition of these challenges, most existing studies focus on isolated dimensions of economic security, such as financial resilience, cybersecurity or innovation capacity, without offering a holistic framework that integrates these dimensions and captures their interdependencies. This fragmentation limits the strategic value of assessment tools, as managers lack guidance on how improvements in one area (e.g., IT infrastructure) influence others (e.g., personnel capabilities or security outcomes).

The CRITIC (CRiteria Importance Through Intercriteria Correlation) method, introduced by Diakoulaki et al. [6], provides an objective mechanism for calculating criterion weights based on two parameters: (1) the variability of each criterion across decision alternatives, and (2) the level of conflict (correlation) between criteria. Unlike subjective weighting methods such as AHP or direct expert assignment, CRITIC derives weights purely from data characteristics, ensuring reproducibility and eliminating bias [7].

In research, CRITIC has been applied primarily to performance evaluation and provider selection problems.

Keshavarz Ghorabaee et al. [7] combined CRITIC with the Weighted Aggregated Sum Product Assessment (WASPAS) method to evaluate third-party providers, demonstrating improved stability in ranking outcomes. Yin et al. [8] applied CRITIC–TOPSIS to assess smart port performance, revealing strong interdependencies between digital capability indicators and efficiency metrics.

Despite these applications, CRITIC has rarely been used to assess organisational-level constructs such as economic security. Its potential to provide objective, statistically grounded weights for multidimensional security indicators, particularly those reflecting information systems, innovation, personnel and cybersecurity, remains underexplored. Moreover, existing CRITIC applications do not integrate causal analysis, limiting their ability to inform strategic prioritisation.

The DEMATEL (Decision Making Trial and Evaluation Laboratory) method was developed to analyse complex systems characterised by interacting criteria and cause–effect relationships [9]. Unlike ranking-oriented MCDM methods, DEMATEL identifies which factors act as drivers (causes) and which are dependent outcomes, providing insights essential for systemic intervention strategies.

DEMATEL has been widely applied in research. Xu et al. [10] used DEMATEL to assess risk factors, identifying customer information leakage, digital infrastructure vulnerabilities and system integration gaps as the most influential risks. Nila et al. [11] applied a modified DEMATEL framework to identify critical success factors for Industry 4.0 and digital transformation, confirming its efficiency in modelling causal interactions in digitalised environments. Jindal et al. [12] employed fuzzy DEMATEL to analyse interdependencies among determinants, demonstrating the method's suitability for systems with high inter-criteria interaction.

Despite its proven utility in risk analysis and digital transformation studies, DEMATEL has not been widely applied to economic security assessment – particularly frameworks that integrate organisational, technological and human-centred components. Furthermore, most DEMATEL applications rely solely on expert judgement without combining it with objective, data-driven weighting methods, which limits their robustness.

Multi-criteria decision-making (MCDM) methods have become widely adopted in research due to their ability to structure complex evaluation problems involving multiple, often conflicting, criteria. Techniques such as Analytic Hierarchy Process (AHP), Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), Data Envelopment Analysis (DEA) and VIseKriterijumska Optimizacija I Kompromisno Resenje (VIKOR) have been applied to supplier selection, performance benchmarking, risk assessment and network optimisation [12; 13].

Recent studies emphasise that digital transformation intensifies the need for advanced evaluation tools, as performance indicators become strongly interrelated due to automation, data integration and process digitalisation. Khan [14] confirmed that technological infrastructure, top-management commitment and intelligent systems are critical success factors that interact dynamically, reinforcing the importance of MCDM methods capable of capturing causal dependencies rather than merely ranking alternatives.

However, while MCDM methods are widely used for operational and strategic problems – such as selecting service providers, optimising facility locations, or evaluating digital maturity or evaluating digital maturity – their application to economic security assessment remains limited. Most existing MCDM-based studies focus on efficiency, cost or service quality, rather than on holistic security constructs integrating technological, human, managerial and security dimensions.

Identification of previously unresolved aspects of the problem. Thus, the existing body of scientific research provides a solid theoretical foundation for analysing digitalisation and innovation activity of enterprises in the context of economic security. However, despite the growing number of studies addressing digital transformation, cybersecurity risks, innovation capacity, and organisational resilience, the issue of integrating modern information technologies into comprehensive economic security management practices remains insufficiently explored. In particular, current research lacks unified methodological approaches that simultaneously account for objective performance indicators and causal interdependencies among key components of enterprise economic security under digital transformation conditions. This gap highlights the need for further scientific investigation aimed at developing integrated, analytically robust assessment frameworks capable of supporting strategic decision-making in digitally transforming enterprises.

Formulating the purposes of the article. The purpose of this study is to develop and apply an integrated methodological framework for assessing the economic security of enterprises under digital transformation conditions. Specifically, the research aims to identify the most influential factors shaping enterprise economic security, evaluate the ability of enterprises to withstand contemporary information and cybersecurity threats, and determine the role of innovation-oriented and managerial components as drivers of economic security enhancement. To achieve this objective, the study employs a hybrid CRITIC–DEMATEL approach that combines objective data-driven weighting of indicators with causal analysis of interrelationships among key economic security components

Presentation of the main research material. Below are the details and features of the CRITIC and DEMATEL methods used for assessing the economic security of enterprises.

The CRITIC Method is outlined in the following steps:

Step 1.1. Formation of the initial data matrix. Collecting data from enterprises. Based on this data, create a matrix of initial data, where:

$$X = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1i} \\ x_{21} & x_{22} & \cdots & x_{2i} \\ \vdots & \vdots & \ddots & \vdots \\ x_{j1} & x_{j2} & \cdots & x_{ji} \end{pmatrix},$$

where i – the number of enterprises; j – the number of indicators.

Step 1.2. Normalization of indicators. To make the indicators comparable, the min-max normalization method is used:

for stimulants (more = better):

$$x_{ij}^{norm} = \frac{x_{ij} - x_j^{\min}}{x_j^{\max} - x_j^{\min}}$$

for destimulants (less = better):

$$x_{ij}^{norm} = \frac{x_j^{\max} - x_{ij}}{x_j^{\max} - x_j^{\min}},$$

where $x_j^{\min}$ and $x_j^{\max}$ – minimum and maximum values of the *j*-th indicator.

Step 1.3. Calculation of standard deviation. For each indicator, the standard deviation of normalized values is calculated:

$$\sigma_j = \sqrt{\frac{1}{m}\sum_{i=1}^{m}\left(x_{ij}^{norm} - \bar{x}_j^{norm}\right)^2},$$

where $\bar{x}_j^{norm}$ – average value of the j-th normalized indicator.

Step 1.4. Building a correlation matrix. The matrix of pairwise correlations between all indicators is calculated using Pearson's coefficient:

$$r_{jk} = \frac{\sum_{i=1}^{m}\left(x_{ij}^{norm} - \bar{x}_j^{norm}\right)\left(x_{ik}^{norm} - \bar{x}_k^{norm}\right)}{\sqrt{\sum_{i=1}^{m}\left(x_{ij}^{norm} - \bar{x}_j^{norm}\right)^2 \sum_{i=1}^{m}\left(x_{ik}^{norm} - \bar{x}_k^{norm}\right)^2}}.$$

Step 1.5. Calculation of the informativeness index C_j. The degree of informativeness is calculated for each indicator.:

$$C_j = \sigma_j \times \sum_{k=1}^{n}\left(1 - \left|r_{jk}\right|\right),$$

where the first factor (σ_j) reflects the variability of the indicator, and the second factor reflects its independence from other indicators.

Step 1.6. Determining the weights of indicators within blocks. The weight of the indicator within its block is calculated as:

$$w_j^{CRITIC} = \frac{C_j}{\sum_{j \in block} C_j}.$$

The DEMATEL Method is outlined in the following steps:

Step 2.1. Formation of a direct impact matrix. Experts assess the degree of direct influence of each block on other blocks on a scale: 0 – no influence; 1 – low influence; 2 – medium influence; 3 – high influence; 4 – very high influence. A direct influence matrix Z is formed:

$$Z = \begin{pmatrix} z_{11} & z_{12} & \cdots & z_{15} \\ z_{21} & z_{22} & \cdots & z_{25} \\ \vdots & \vdots & \ddots & \vdots \\ z_{51} & z_{52} & \cdots & x_{55} \end{pmatrix}.$$

The geometric mean of the obtained estimates is used for further calculations:

$$z_{ij} = \sqrt[p]{\prod_{e=1}^{p} z_{ij}^{(e)}},$$

where *p* – the number of experts.

Step 2.2. Normalization of the direct effect matrix:

$$X = \frac{Z}{s'},$$

where $s = max(max_i \sum_{j=1}^{5} z_{ij},\ max_j \sum_{i=1}^{5} z_{ij})$.

Step 2.3. Calculation of the full impact matrix. Full impact matrix *T*, which takes into account both direct and indirect links:

$$T = X\,(I - X)^{-1},$$

where *I* – the identity matrix.

Step 2.4. Calculating the sums of rows (r) and columns (c):

$$r_i = \sum_{j=1}^{5} t_{ij},\ \mathrm{i} = 1, 2...5,$$

$$c_i = \sum_{j=1}^{5} t_{ij},\ \mathrm{j} = 1, 2...5,$$

where r_i – the total influence exerted by block i on other blocks; c_j – the total influence received by block j from other blocks.

Step 2.5. Calculating Prominence and Relation indicators:

$$Prominence_i = r_i + c_i$$
$$Relation_i = r_i - c_i$$

Prominence: shows the overall role of the block in the system. Relation: if > 0, then the block belongs to the "causes" group (affects others); if < 0, then the block belongs to the "consequences" group (depends on others).

Step 2.6. Determining the weights of the blocks

$$W_i^{DEMATEL} = \frac{Prominence_i}{\sum_{i=1}^{5} Prominence_i}.$$

The study included 10 enterprises operating in Kyiv and Kyiv region, Ukraine. Enterprise size ranged from 50 to 500 employees. The sample provides sufficient methodological diversity and indicator variability to validate the CRITIC–DEMATEL framework and demonstrate its practical applicability to enterprises.

Thirty people were involved in the expert assessment: 10 company executives; 2 IT directors with over 5 years of experience; 18 company specialists in information security and innovation management.

Based on an analysis of scientific works by researchers and international standards for assessing the digital maturity of enterprises (ISO/IEC 33001, COBIT 2019), a preliminary list of 50 indicators of economic security for enterprises was formed, structured into five blocks: information component (10 indicators), innovation component (10 indicators), personnel (10 indicators), data security and protection (10 indicators), management component (10 indicators).

To ensure the practical applicability of the methodology and reduce the information burden on enterprises, a two-stage procedure for selecting key indicators was carried out. Experts were asked to evaluate each of the 50 indicators according to four criteria on a scale of 1 to 5 points: information accessibility (K_1); representativeness (K_2); measurability (K_3); practical significance (K_4). Greater weight was given to the criteria of measurability and practical significance, since the methodology is intended for practical application.

Based on the results of the expert assessment, four indicators with the highest expert assessment values were selected from each block. This approach ensured the formation of a compact system of 20 indicators (Table 1), which is an optimal balance between the completeness of coverage of all aspects of the economic security of enterprises and the practical possibility of regular data collection and processing.

Application of the CRITIC method

A fragment of the normalization results for selected enterprises and indicators A1-A4 is presented in Table 2.

The results of calculations of the standard deviation of normalized values are presented in Table 3.

The greatest variability is demonstrated by indicators D3 (σ = 0.483) and E4 (σ = 0.483), which indicates significant differentiation among enterprises in terms of the availability of security certificates and transformation strategies. The lowest variability is shown by indicator A3 (σ = 0.280), which indicates a relatively uniform level of digitalisation of business processes among the enterprises studied.

As a result of calculating the matrix of pairwise correlations between all indicators, the strongest positive correlations were found between:

A1 and B4 (r = 0.773) – the level of maturity of IT infrastructure is closely related to innovation activity;

A1 and D3 (r = 0.901) – a developed IT infrastructure is accompanied by the presence of security certificates;

B4 and D3 (r = 0.802) – innovation activity correlates with a systematic approach to security.

The strongest negative correlation: A4 and C1 (r = -0.796) – which may indicate a compensatory effect: with a lower level of system integration, companies compensate for this with a higher proportion of staff with digital competencies.

The results of calculating the weights of indicators using the CRITIC method are presented in Table 4.

In block A, the highest weight was assigned to indicator A4 (0,277) – the level of information system integration, confirming the critical importance of system integration for enterprise information security.

In block B, the most influential indicator is B1 (0,297) – the share of innovative technologies in projects, which reflects the enterprise's strategic orientation toward innovation.

In block C, indicator C2 (0,278) received the highest weight – the share of IT specialists, highlighting the critical role of qualified IT personnel.

In block D, the most significant indicator is D2 (0,290) – cybersecurity expenditures, indicating the importance of adequate security funding.

In block E, indicator E1 (0,275) has the highest weight – the effectiveness of IT project management.

Application of the DEMATEL method

The aggregated direct-influence matrix Z is presented in Table 5.

The normalized matrix X is presented in Table 6.

The results of the total-influence matrix T are presented in Table 7.

The results of the block weight calculations are presented in Table 8.

To visually illustrate the cause–effect relationships between the blocks, an influence map was constructed (Figure 1).

Table 1

System of indicators for assessing the economic security

Code	Indicator	Unit of measurement	Type
	A. Information component		
A1	Level of maturity of IT infrastructure	points (0-5)	Stimulator
A2	Share of IT expenses in total expenses	%	Stimulator
A3	Level of digitization of business processes	%	Stimulator
A4	Level of integration of information systems	points (0-5)	Stimulator
	B. Innovative component		
B1	Share of innovative technologies in projects	%	Stimulator
B2	Number of innovations implemented per year	count	Stimulator
B3	Share of innovation expenditure in total expenditure	%	Stimulator
B4	Innovation Activity Index	points (0-5)	Stimulator
	C. Staff		
C1	Percentage of staff with digital skills	%	Stimulator
C2	Share of IT specialists in the personnel structure	%	Stimulator
C3	Intensity of staff training	persons per year	Stimulator
C4	Employees' perception of readiness for digital change	points (0-5)	Stimulator
	D. Data security and protection		
D1	Number of information security incidents per year	count	Destimulator
D2	Share of cybersecurity spending	%	Stimulator
D3	Availability of safety certificates	binary (0/1)	Stimulator
D4	Level of protection for critical data	points (0-5)	Stimulator
	E. Management component		
E1	Project management effectiveness	%	Stimulator
E2	Proportion of data-driven decisions	%	Stimulator
E3	Readiness for information and innovation transformation	points (0-5)	Stimulator
E4	The existence of a strategy for information and innovation transformation	binary (0/1)	Stimulator

Source: proposed by the author based on expert analysis

Table 2

Normalized values of indicators (excerpt)*

Enterprise	A1_norm	A2_norm	A3_norm	A4_norm
Enterprise 1	1,00	1,00	0,40	0,50
Enterprise 2	0,50	0,75	0,20	1,00
Enterprise 3	0,00	0,50	0,60	0,00
Enterprise 4	0,00	0,25	0,20	0,50
Enterprise 5	0,50	0,25	0,00	0,00
Enterprise 6	0,00	0,50	0,60	0,50
Enterprise 7	1,00	0,00	0,40	1,00
Enterprise 8	0,00	0,50	0,60	0,50
Enterprise 9	0,00	0,25	0,40	0,50
Enterprise 10	1,00	1,00	1,00	0,00

**Note: All normalized values are in the range [0; 1].*

Source: calculated by the author

Table 3

Standard deviation of normalized values

Indicator	Standard deviation (σ)	Indicator	Standard deviation (σ)
A1	0,459	D1	0,316
A2	0,333	D2	0,417
A3	0,280	D3	0,483
A4	0,369	D4	0,412
B1	0,412	E1	0,347
B2	0,306	E2	0,316
B3	0,307	E3	0,369
B4	0,344	E4	0,483
C1	0,316		
C2	0,343		
C3	0,329		
C4	0,354		

Source: calculated by the author

Table 4

Indicator weights calculated using the CRITIC method

Indicator	σ	Σ(1-|*r*|)	*C_j*	*W_j*	Block
A1	0,459	13,680	6,285	0,268	A
A2	0,333	16,847	5,616	0,240	A
A3	0,280	18,007	5,036	0,215	A
A4	0,369	17,580	6,486	0,277	A
B1	0,412	15,827	6,515	0,297	B
B2	0,306	15,152	4,641	0,211	B
B3	0,307	18,762	5,756	0,262	B
B4	0,344	14,690	5,057	0,230	B
C1	0,316	22,501	7,116	0,263	C
C2	0,343	21,909	7,505	0,278	C
C3	0,329	20,708	6,819	0,252	C
C4	0,354	15,842	5,601	0,207	C
D1	0,316	19,000	6,008	0,226	D
D2	0,417	18,486	7,713	0,290	D
D3	0,483	13,158	6,356	0,239	D
D4	0,412	15,849	6,524	0,245	D
E1	0,347	19,365	6,717	0,275	E
E2	0,316	18,891	5,974	0,245	E
E3	0,369	14,578	5,378	0,220	E
E4	0,483	13,158	6,356	0,260	E

Source: calculated by the author

Table 5

The aggregated direct-influence matrix (DEMATEL)

Block	A	B	C	D	E
A. Information	0,000	2,702	2,048	2,930	2,491
B. Innovative	3,104	0,000	2,491	2,297	2,491
C. Staff	2,048	1,783	0,000	2,702	1,644
D. Security	3,288	2,639	2,491	0,000	2,169
E. Management	3,104	3,288	3,776	2,930	0,000

Source: calculated by the author

Table 6

The normalized matrix

Block	A	B	C	D	E
A. Information	0,000	0,206	0,156	0,224	0,190
B. Innovative	0,237	0,000	0,190	0,175	0,190
C. Staff	0,156	0,136	0,000	0,206	0,125
D. Security	0,251	0,201	0,190	0,000	0,166
E. Management	0,237	0,251	0,288	0,224	0,000

Source: calculated by the author

Table 7

The total-influence matrix T

Block	A	B	C	D	E
A. Information	0,429	0,356	0,379	0,365	0,310
B. Innovative	0,387	0,395	0,373	0,386	0,313
C. Staff	0,329	0,303	0,325	0,297	0,264
D. Security	0,389	0,366	0,377	0,417	0,325
E. Management	0,476	0,426	0,428	0,457	0,414

Source: calculated by the author

The calculations revealed the following findings:

The managerial component (E) has the strongest influence on the other blocks (*Relation* = 0,574), confirming the decisive role of management. Strategic decisions made by the leadership create the prerequisites for the development of all other components.

The innovation component (B) also belongs to the "cause" group (*Relation* = 0,010), although its influence is relatively weak. This indicates that innovation activity stimulates the development of other blocks, particularly the information component.

The personnel component (C) is the most dependent block (*Relation* = -0.365), which is logical: personnel development depends on IT infrastructure, innovation processes and managerial decisions.

The information component (A) and the security component (D) also fall into the dependent group, indicating the need to prioritise the development of managerial and innovation components.

Based on the weights, the most important blocks are A (0,207) and E (0,206), confirming the critical importance of information infrastructure and management quality for enterprises.

Calculation of the integral economic security index (IES) of enterprises

For each block, a partial index is calculated.

$$IES = W_A^{DEMATEL} \times I_A + W_B^{DEMATEL} \times I_B + W_C^{DEMATEL} \times I_C + W_D^{DEMATEL} \times I_D + W_E^{DEMATEL} \times I_E,$$

where IES ∈ [0;1].

Table 8

Block weights and characteristics of their mutual influence (DEMATEL)

Block	Influence (*r*)	Received influence (*c*)	Prominence	Relation	Type	Weigh (*W*)
A. Information	1,840	2,010	3,850	-0,170	Dependent	0,207
B. Innovative	1,854	1,845	3,699	0,010	Influencing	0,199
C. Staff	1,518	1,883	3,401	-0,365	Dependent	0,183
D. Security	1,873	1,921	3,794	-0,049	Dependent	0,204
E. Management	2,201	1,627	3,828	0,574	Influencing	0,206

Source: calculated by the author

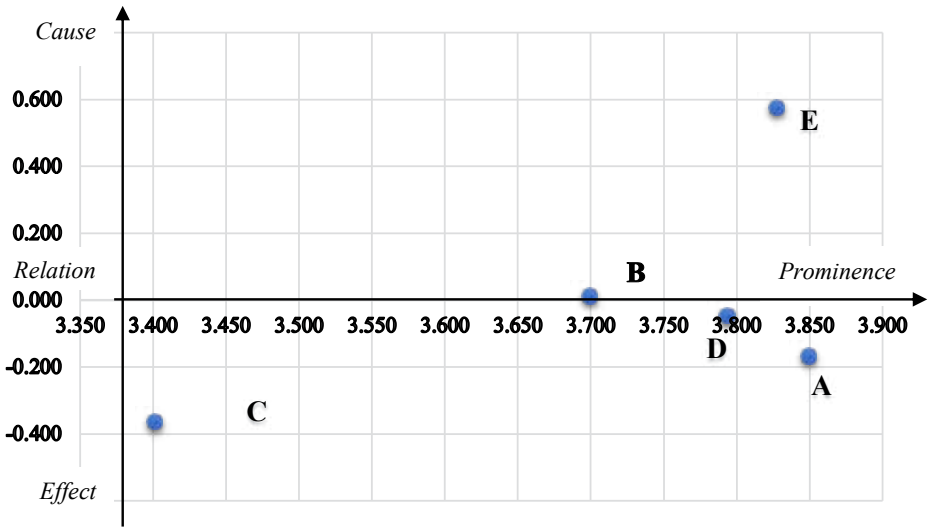

Figure 1 – Cause–effect map of the blocks of the integral economic security index for enterprises (based on DEMATEL results)

Source: calculated by the author

Based on the conducted calculations, the following formula is proposed for determining the integral economic security index of enterprises.

$$IES = 0{,}207 \times I_A + 0{,}199 \times I_B + 0{,}183 \times I_C + 0{,}204 \times I_D + 0{,}206 \times I_E$$

The results of the calculations the IES for the 10 analysed enterprises are presented in Table 9.

Interpretation of the results

To interpret the obtained values, a five-level scale is proposed (Table 10).

The results demonstrate that the hybrid approach offers a comprehensive framework for assessing the economic security of enterprises in the context of digital transformation. The integration of these two methods addresses a critical methodological gap by combining objective, data-driven indicator weighting with expert-based causal relationship analysis.

Methodological Advantages and Comparison with Alternative Approaches. A key strength of the proposed approach lies in its dual-layered assessment architecture. At the indicator level, the CRITIC method eliminates subjectivity by deriving weights solely from statistical parameters – indicator variability and inter-criteria correlation. This ensures reproducibility and objectivity, which are essential

Table 9

Integral economic security index by enterprise)

Enterprise	I_A	I_B	I_C	I_D	I_E	IES
Enterprise 1	0,733	0,799	0,550	0,819	0,846	0,75
Enterprise 2	0,634	0,470	0,686	0,232	0,420	0,48
Enterprise 3	0,249	0,268	0,423	0,303	0,607	0,37
Enterprise 4	0,241	0,164	0,721	0,626	0,412	0,43
Enterprise 5	0,194	0,416	0,521	0,264	0,350	0,34
Enterprise 6	0,387	0,185	0,451	0,471	0,285	0,35
Enterprise 7	0,631	0,738	0,507	0,716	0,833	0,69
Enterprise 8	0,387	0,399	0,524	0,503	0,267	0,41
Enterprise 9	0,284	0,356	0,695	0,097	0,189	0,32
Enterprise 10	0,723	0,563	0,470	0,665	0,460	0,58

Source: calculated by the author

Table 10

Evaluation scale for the economic security of enterprises based on the integral index calculated using the CRITIC–DEMATEL method

Range of values	Security level	Description
0,81 – 1,00	High	Systematic implementation of advanced management practices; proactive development of innovation and information capabilities
0,61 – 0,80	Sufficient	Existence of an enterprise economic security strategy; effective management of information and innovation processes
0,41 – 0,60	Satisfactory	Basic level of economic security; fragmented measures; requires systematic improvement
0,21 – 0,40	Low	Presence of critical issues in ensuring economic security; high information security risks; low innovation activity
0,00 – 0,20	Critical	Absence of a systematic approach to economic security; critical threat level; urgent managerial interventions required

Source: interpreted by the author

for longitudinal monitoring and cross-enterprise benchmarking [1; 8].

At the component level, DEMATEL complements CRITIC by revealing causal relationships within the economic security system. While traditional methods such as TOPSIS or DEA focus on ranking or efficiency measurement, they do not identify which components drive systemic changes. The DEMATEL analysis demonstrates that managerial (*Relation* = 0,574) and innovation (*Relation* = 0,010) components function as "causes", whereas information infrastructure, personnel and security act as "effects". This distinction is critical for strategic prioritisation: investing in dependent components without addressing root causes yields limited systemic improvement [10; 12].

The proposed hybrid approach uniquely combines high objectivity with causal diagnostic capability, making it particularly suitable for assessing multidimensional constructs in digitally transforming environments.

Key Findings. The empirical results reveal several important patterns. First, IT system integration (A4, W = 0,277), innovation intensity (B1, W = 0,297), IT personnel share (C2, W = 0,278) and cybersecurity investment (D2, W = 0,290) emerged as the most influential indicators. This aligns with recent studies emphasising the centrality of digital infrastructure and innovation capability in determining resilience [3; 14].

Second, the strong positive correlation between IT infrastructure maturity (A1) and innovation activity (B4) (r = 0,773) suggests that technological readiness is a prerequisite for successful innovation adoption. Conversely, the negative correlation between system integration (A4) and personnel digital competencies (C1) (r = -0.796) may indicate a compensatory mechanism: enterprises with lower IT integration rely more heavily on skilled personnel to bridge operational gaps.

Third, the DEMATEL results confirm that managerial and innovation components are the primary drivers of economic security. The high "cause" status of the managerial component suggests that strategic leadership and project management effectiveness create cascading effects across all other dimensions. This has significant implications for resource allocation: strengthening managerial capabilities should be the first priority, as improvements in this area amplify the effectiveness of investments in other components.

Managerial Implications. The findings offer three actionable strategic priorities for managers:

1. Prioritise managerial development. Given that the managerial component acts as the strongest "cause" (*Relation* = 0,574), enterprises should invest in leadership training, strategic planning frameworks and data-driven governance systems before expanding infrastructure or innovation initiatives.

2. Balance innovation with security. While innovation drives change, cybersecurity must be strengthened in parallel (D2, W = 0,290) to avoid creating vulnerabilities during rapid digitalisation. A "secure-by-design" approach is recommended.

3. Develop workforce strategically. The high dependency of the personnel component (*Relation* = -0,365) indicates that workforce development outcomes are contingent on prior investments in infrastructure and strategic direction. A phased approach is recommended: establish IT infrastructure and strategic vision first, then build digital competencies through targeted training and recruitment.

Conclusions. This study developed and validated an integrated CRITIC–DEMATEL framework for assessing the economic security of enterprises undergoing digital transformation. Empirical analysis of 10 enterprises demonstrated that IT system integration, innovation intensity, IT personnel capabilities and cybersecurity investment are the most influential factors shaping economic security. The DEMATEL-based causal mapping revealed that managerial and innovation components act as drivers, while information infrastructure, personnel and security function as dependent outcomes – a finding with direct implications for strategic prioritisation.

From a theoretical perspective, this study extends the conceptualisation of economic security beyond traditional financial metrics by demonstrating that it emerges from complex interactions among managerial, technological, human and security-related factors characterised by asymmetric causal relationships. The application of hybrid MCDM methods to organisational-level economic security assessment represents a methodological advancement, showing that combining statistical objectivity (CRITIC) with causal insight (DEMATEL) offers superior diagnostic capability compared to conventional approaches.

From a practical standpoint, the model provides managers with: (1) a ready-to-use assessment tool based on 20 measurable indicators requiring no additional data collection; (2) clear strategic guidance emphasising the

primacy of managerial capability development; and (3) a framework adaptable to continuous monitoring through recalculation of CRITIC weights as new data become available.

Several limitations should be acknowledged. The assessment is cross-sectional, reflecting conditions at a single point in time; longitudinal research would provide insights into temporal dynamics. The sample of 10 enterprises, while sufficient for methodological validation, is not statistically representative. DEMATEL relies on expert judgement, introducing subjectivity despite mitigation through a 30-expert panel. The indicator system was adapted from construction sector practices, and sector-specific refinement may improve precision for specialised operations.

Future research could pursue three promising extensions. First, longitudinal studies incorporating time-series data would enable modelling of how economic security evolves during multi-year transformation programmes. Second, cross-industry validation applying the framework to manufacturing, healthcare or retail would test transferability and enable comparative benchmarking. Third, integration with real-time monitoring systems leveraging IoT and big data analytics could automate indicator collection and provide continuous assessment capabilities.

Given increasing volatility, digitalisation pressures, and cyber threats, economic security assessment requires multidimensional frameworks capable of revealing causal structures and informing strategic interventions.

References:

1. Li, Z., Gao, L., & Wang, W. (2025), The impact of supply chain digitization and logistics efficiency on enterprise competitiveness. *International Review of Financial Analysis.* DOI: https://doi.org/10.1016/j.iref.2024.103759

2. Zhurakovska, A., Lukashova, D., & Pavlov, R. (2024), Challenges and specificity of ensuring the economic security of the enterprise in crisis conditions. *Economy and Society*, no. 68, pp. 659–672. DOI: https://doi.org/10.32782/2524-0072/2024-68-100

3. Li, Y., Li, D., Liu, Y., & Shou, Y. (2023), Digitalisation for supply chain resilience and robustness: The roles of collaboration and formal contracts. *Frontiers of Engineering Management*, no. 10, pp. 5–19. DOI: https://doi.org/10.1007/s42524-022-0229-x

4. Khan, S.., Yu, Z., & Sharif, A. (2019), Role of digitalisation in enhancing supply chain resilience and social sustainability. *Journal of Cleaner Production*, no. 239. DOI: https://doi.org/10.1016/j.jclepro.2019.118024

5. Shirdakova, G. (2025), Digitisation of public procurement as a factor of economic security and regional development in the Kyrgyz Republic. *Economics & Management*, no. 12 (2), pp. 34–46. DOI: https://doi.org/10.52566/msu-econ2.2025.34

6. Diakoulaki, D., Mavrotas, G., & Papayannakis, L. (1995), Determining objective weights in multiple criteria problems: The CRITIC method. *Computers & Operations Research*, no. 22 (7), pp. 763–770. DOI: https://doi.org/10.1016/0305-0548(94)00059-H

7. Keshavarz Ghorabaee, M., Zavadskas, E. K., Olfat, L., & Turskis, Z. (2017), Multi-criteria inventory classification using the EDAS method. *Economic Research – Ekonomska Istraživanja*, no. 30, pp. 1073–1095. DOI: https://doi.org/10.1080/1331677X.2017.1357991

8. Yin, S., Ding, X., & Guo, L. (2023), Evaluating smart port performance using a hybrid CRITIC–TOPSIS model. *Marine Policy*, no. 153. DOI: https://doi.org/10.1016/j.marpol.2023.105114

9. Seyedhosseini, S., Safaei, N., & Asgharpour, M. (2006), Reprioritization of failures in system FMEA using the DEMATEL technique. *Reliability Engineering & System Safety*, no. 91 (8), pp. 872–881. DOI: https://doi.org/10.1016/j.ress.2005.11.018

10. Xu, T., Wang, H., & Feng, L., & Zhu, Y. (2024), Risk factors assessment of smart supply chain in intelligent manufacturing services using DEMATEL method with LINGUISTIC q-ROF information. *Journal of Operations Intelligence*, no. 2 (1), pp. 129–152. DOI: https://doi.org/10.31181/jopi21202417

11. Nila, B., & Roy, J. (2024), Analysis of critical success factors of Logistics 4.0 using D-number based Pythagorean fuzzy DEMATEL. *Decision Making Advances*, no. 2 (1), pp. 92–104. DOI: https://doi.org/10.31181/dma21202430

12. Jindal, A., Sharma, S. K., & Sangwan, K. S. (2021), Modelling supply chain agility antecedents using fuzzy DEMATEL. *Procedia CIRP*, no. 99, pp, 808–813. DOI: https://doi.org/10.1016/j.procir.2021.01.130

13. Taletović, A. (2023), Applications of MCDM methods in warehouse management: A systematic review. *Spectrum of Engineering and Management Sciences*, no. 1 (1), pp. 25–37. DOI: https://doi.org/10.31181/sems11202331t

14. Khan, S. (2022), Exploration of critical success factors of Logistics 4.0. *Logistics*, no. 6 (1). DOI: https://doi.org/10.3390/logistics6010013

Стаття надійшла: 10.11.2025
Стаття прийнята: 27.11.2025
Стаття опублікована: 17.12.2025