**UDC 338.2:005.52**
**JEL L23, G32, O33**

# STRATEGIC RISK MANAGEMENT OF DIGITAL TRANSFORMATION IN THE ECONOMIC SECURITY OF INDUSTRIAL ENTERPRISES

**Mihail Ivanov**
Technical University of Varna,
Varna, Bulgaria
ORCID ID: 0009-0004-4121-2293

**Larysa Martseniuk**
Ukrainian State University of Science and Technologies,
Dnipro, Ukraine
ORCID ID: 0000-0003-4121-8826

**Miglena Angelova**
University of National and World Economy,
Sofia, Bulgaria
ORCID ID: 0000-0002-4460-133X

**Serhii Faifer ***
Ukrainian State University of Science and Technologies,
Dnipro, Ukraine
ORCID ID: 0009-0002-2788-5200

*Corresponding author:
E-mail: fayfer1984@gmail.com

**Received**: 07/04/2025
**Revised**: 12/06/2025
**Accepted**: 25/06/2025

DOI: 10.61954/2616-7107/2025.9.2-9

**Introduction.** Digital transformation has become a determinant factor influencing enterprises' economic security, especially during crises and global concurrences. Despite its numerous advantages, digitalisation poses new risks, such as cyber threats, regulatory instability, and information leaks. Digitalisation as an infrastructure for innovation has become a strategic priority, primarily through the extension of digital government services, cloud resolutions, and metadata analytical tools to support the economic development of industry enterprises.

**Aim and tasks.** This study aims to develop an integrated system of strategic risk management for digital transformation in industry enterprises' economic security to minimise economic losses, increase adaptiveness to digital changes, and eliminate risks in industry enterprises' economic security.

**Results.** This study analyses modern approaches to ensuring economic security: systemic, risk-oriented, resource-oriented, and integrated approaches. The analysis revealed that only 25.6% of IT enterprises utilise Big Data analytics, while 7.1% employ AI technologies, highlighting the substantial untapped potential for further digital transformation. This study developed a structural model of a digital economic security management platform, including risk analytics, threat management, cyber protection, monitoring, and reporting. A formalised risk estimation model was built, considering financial, operational, and external factors. An integrated approach is suggested to build a digital platform for the management of enterprises' economic security, which combines risk-oriented methods, cyber-protection, and big data analytics.

**Conclusions.** This study proposes an approach for digital transformation in economic security management, featuring module architecture to monitor, forecast, and respond to threats. It presents formalised module architecture and a platform structural model for economic security monitoring, comprising four subsystems: financial, operational, risk-oriented, and external factors. The model enables rational resource allocation, threat forecasting, and adaptive decision-making in post-conflict scenarios. Enterprise digital transformation in strategic management and economic security is a key requirement for restoring, strengthening, and safeguarding the national interest.

**Keywords**: digitalisation, economic security, management, digital innovation, risk management.

## 1. Introduction.

Digital transformation influences enterprises' economic security by creating preconditions for optimising business processes, increasing effectiveness, and reducing costs by introducing innovative technologies. However, digitalisation creates new risks and threats alongside its advantages, requiring appropriate strategic economic security management mechanisms.

The rise in funding for the development processes of digital technologies and appropriate infrastructure allows countries to be leaders, preserving the status of key actors in the global digital technologies market. Forrester Research (O'Grady, 2024) estimates that the United States and China provide 42 % of the world's expenses for digital technologies. Meanwhile, the global digital economy is projected to grow at an average annual rate of 7% and reach $16.5 trillion by 2028.

EU countries have also actively integrated digital technologies into key economic sectors. In particular, cloud calculations for businesses vary between 70% and 78% in Finland, Sweden, and Denmark, respectively. The EU defines strategic priorities in digital transformation, foreseeing a basic level of digital maturity for more than 90% of enterprises (including small and medium enterprises) by 2030 and the development of cloud technologies, big data, and AI analysis in 75% of companies. The manufacturing and finance service fields are the main branches displaying high rates of digital economy development (SecurityDive, 2024).

An enterprise's economic security further depends on its ability to adapt to digital challenges, manage risks, and depend on external digital platforms and the continuation of disruption in manufacturing. Strategic risk management of digital transformation is necessary to preserve competitiveness and provide sustainability against domestic and external threats in the digital economy.

Thus, strategic risk management of business digital transformation ensures enterprises' economic security, particularly by minimising technological, cybernetic, and operational threats during digital integration (Harahulia et al., 2023).

Digital transformation's strategic risk management seeks to enhance enterprises' economic security, driving more Ukrainian companies to adopt cloud services (Microsoft Azure, Amazon Web Services, and Google Cloud). These solutions ensure critical data preservation, maintain a stable digital infrastructure, and safeguard business process continuity. Simultaneously, organisational and procedural innovations substituting traditional business models are challenging to implement without introducing big data analytics and resolutions based on AI, permitting the elimination of operational risks, improving forecasting market changes, and raising enterprises' sustainability against external threats.

## 2. Literature Review.

The strategic management of digital transformation is of special relevance to the active implementation of digital technologies in the industry and the increasing dependence of enterprises' economic security on their digital maturity. Recent research indicates that risk assessment and management tools in the digital economy use a matrix approach to integrate digital technologies into enterprises' strategic management (Schallmo et al., 2019; Stender et al., 2024). The approach foresees the necessity to build an evident interdependence between the level of digital maturity of the enterprise and the choice of technological tools within the scope of the general transformation strategy.

Zachosova et al. (2022) studied the impact of digitalisation on enterprises' economic security, considering the choice of economic security strategy and the formation of the management mechanism of the enterprise's financial and economic security under Industry 4.0, which depends on digitalisation.

Dvorsky et al. (2021) determined that the ability of security systems to be transformed is a definite factor in adaptation to new conditions, especially in digitalisation. Flexibility in forming managerial decisions enables one to choose the most effective strategies in situations of in determination, reducing the impact of external threats, particularly for small- and medium-sized enterprises.

Spivakovskyy et al. (2021) have analysed the impact of digital transformation on the economic security of Ukraine. In particular, the problems of digital inequality in labour market changes, industrial espionage, and personal data manipulation have been examined. In addition, it was suggested that the mechanism softens the negative impact of digital transformation on economic security.

Kalinin et al. (2023) and Rauniyar et al. (2023) developed frameworks to assess economic security while drafting investment projects related to digital transformation risks. In particular, these studies identified the types of risks that can affect global supply chains, including the systematisation of key indicators and provision of information transparency during investment project realisation.

Brunetti et al. (2020) have presented the process of public administration digital transformation with an emphasis on servicisation and granting quality public services via digital channels. Because digitalisation favours the improvement of public authorities' service activities, it is an important aspect of economic security in the digital economy.

Shkolnyk et al. (2022) have studied the impact of financial transformation on ensuring Ukraine's economic security. In particular, this study analysed the role of digital financial tools in maintaining financial system stability. It proved that financial sector digitalisation favoured the formation of economic security reserves, which permitted financial system functioning.

Bondarenko et al. (2021) studied the modelling of enterprises' digital security during digital transformation. In particular, it examined methods for assessing risks and threats related to digital technologies. Bondarenko et al. (2021) built a structured model of an adapted enterprise economic security system that considered the impact of digital transformation and allowed it to respond effectively to new challenges.

Kraus et al. (2023) analysed technological and organisational contexts in which strategic risk management of digital transformation becomes a key tool for ensuring enterprises' economic security.

This includes new threats such as cyber risks, technological instability, and staff challenges. Furthermore, this requires a new approach to risk management, including scenario planning, sustainability of disruptions, and flexibility in security strategies.

Samoylenko et al. (2023) studied the impact of digital transformation on the economic security of enterprises in Ukraine. The authors suggest an assessment methodology for enterprises' economic security levels and analyse the risks related to the digitalisation of business processes.

Kochubei et al. (2021) and Stender et al. (2024) studied the impact of digital transformations on Ukraine's economic security, including the essence of the digital economy, and identified the features of the economy's functioning in digitalisation. It systematised the problems of economic security in the digital economy and identified systemic, structural, and industrial concerns.

Voronenko et al. (2024) conducted meta- and bibliometric analyses of research on digital transformation in Ukraine and the world for 2019–2023 using data from Scopus, and revealed a significant increase in academic interest in the topic of recent years' digital transformation and the polybranch character of existing studies.

This research synthesis concludes that digital transformation is a determining factor in modernising Ukraine's economic security system, particularly during wartime and post-war recovery. These studies emphasise the need to rethink traditional management models of enterprise security and state-concerned digital risks, information instability, cyber threats and technology dependence.

## 3. Methodology.

The methodological basis of the study is a multi-aspect approach based on the analysis of academic publications on digital transformation, and the integrated application of theoretical and empirical methods aimed at analysing strategic risk management in the context of the economic security of industrial enterprises. The following mathematical model was used for risk assessment in this study:

– Expected Loss Model: The probabilities of risk realisation and potential losses are calculated.

– Sensitivity Analysis Model: Risk changes and influencing risk factors were considered.

– Scenario Analysis Model: The parameters are scenario probability and such scenario realisation losses.

– Monte Carlo Simulation Model: Impact of uncertainty on key risk indicators by generating random values for variables.

– Probabilistic Risk Assessment Model: The event's probability and consequences' costs are calculated.

The risk assessment was performed using a Scenario Analysis Model based on the following formula:

$$R = \sum_{i=1}^{n} P_i * I_i, \tag{1}$$

where:

$R$ – expected risk level;

$P_i$ – probability of scenario $i$ occurrence;

$I_i$ – potential loss amount for scenario $i$ (in consistent units with R);

$n$ – total number of considered scenarios.

The Expected Loss (EL) is calculated using the following model:

$$EL = P * I, \tag{2}$$

where:

$EL$ – expected loss;

$P$ – probability of risk realisation;

$I$ – potential losses in the case of risk realisation.

The best risk estimation method for enterprise economic security in wartime is a scenario analysis model for complicated conditions with considerable uncertainty. They enable the consideration of different variants of event development and their consequences. The expected loss model is suitable for estimating simple and straightforward risks during post-war restoration.

The determination of the risk realisation probability *(P)*, depending on the risk types and accessible data, is also important. An expert estimation model is used if there is a lack of statistical data or if the risk is new, which is especially important during wartime.

The algorithm of the method is as follows: there is an involvement of branch experts (managers, analytics, and auditors), every expert estimates the risk realisation probability (e.g. in percentage), and an arithmetic mean of their assessments is used.

Independent experts are, as a rule, leading specialists in this industry or those concentrating on investigating an appropriate issue. Expert evaluations included descriptions of the inner and outer environmental factors. The average probability is calculated as follows:

$$P = \frac{\sum_{i=1}^{n} P_i}{n}, \tag{3}$$

where:

$P$ – average probability (dimensionless, range [0,1]);

Pi – probability estimate provided by the i$i$-th expert (dimensionless, range [0,1]);

n – total number of experts (integer, n≥1).

The basic parameters that influence the state were determined for economic security monitoring.

The calculation of the integral indicator of the economic security state is recommended using a weighted sum of the main factors using the following formula:

$$ESI_t = \omega_1 F_t + \omega_2 O_t + \omega_3 R_t + \omega_4 Z_t, \tag{4}$$

where:

$F_t$ – financial indicators sub-model;

$O_t$ – operational indicators sub-model;

$R_t$ – risks sub-model;

$Z_t$ – external factors sub-model;

$\omega_1$, $\omega_2$, $\omega_3$, $\omega_4$ – these are, respectively, the weighting coefficients (which are determined by experts).

The indicators sub-model used in Formula (1) is calculated using the following component formulas.

1. Financial component ($F_t$):

$$F_t = \alpha_1 \frac{P_t}{R_t} + \alpha_2 L_t; \tag{5}$$

where:

$\alpha_1$, $\alpha_2$ – weights of financial indicators;

$P_t$ – net profit;

$L_t$ – current ratio, which is a useful test of the short-term solvency of any business.

2. Operational component ($O_t$):

$$Q_t = \beta_1 \gamma_t + \beta_2 \frac{Q_t}{S_t}, \qquad (6)$$

where:

$Q_t$ – Production output or services delivered (units);

$S_t$ – Sales volume (units);

$\gamma_t$ – supply-demand ratio ($\gamma_t = S_t/Q_t$);

$\beta_1$, $\beta_2$ – weights of operational indicators.

3. Risk-oriented component ($R_t$):

$$R_t = \sum_{i=1}^{n} \delta_i K_i, \qquad (7)$$

where:

$K_i$ – appropriate risks (cyber risks, logistic risks, physical threats);

$\delta_i$ – their weights.

4. External factors component ($Z_t$):

$$Z_t = \lambda_1 G_t + \lambda_2 E_t + \lambda_3 U_t, \qquad (8)$$

where:

$G_t$ – geopolitical situation (risk index);

$E_t$ – macroeconomic stability (e.g., inflation index or Ukraine's GDP);

$U_t$ – consumer activity level (index);

$\lambda_1$, $\lambda_2$, $\lambda_3$ – weights for external factors.

The weighting coefficients are calculated through expert analysis and the hierarchy analysis method's (AHP) mean.

## 4. Results.

Amidst contemporary global economic crises and the digital revolution, strategic management is crucial for ensuring the state's and its entities' economic security. One of the key tools for achieving long-term stability and competitiveness in countries' economies is a digital transformation strategy that is increasingly integrated into the general strategic development system. Strategic management, as the process of long-term goal formation, the development of politics, and the mechanisms for achieving them, considering the outer and inner environment, is important for Ukraine during wartime and post-war restoration.

This process should cover three key components: estimating risks and threats to enterprises' economic security, integrating digital tools into the management system, and ensuring the adaptiveness of managerial decisions to change (Table 1).

**Table 1. Economic Sectors Digital Transformation Strategy Matrix.**

| Branch | Key Digital Technologies | Strategic Transformation Goals |
|---|---|---|
| Public administration | E-government, registers, blockchain, AI analytics for political processes, digital passports and ID | Transparency, combating corruption, simplifying access to services, electronic interaction with citizens |
| Industry | Internet of Things, digital twin, robotisation, predictive analytics, smart factory, AI | Reduction costs, increasing of quality and effectiveness of manufacturing, flexibility under crises |
| Finance sector | FinTech, blockchain, digital currencies, antifraud, cloud bank platforms | Transaction safety, integration with international financial infrastructure |
| Agriculture | Drones, satellite monitoring, IoT sensors, yield analytics, and ERP | Increase in yield, optimisation of expenses, delivery tracking, food security |
| Logistics and infrastructure | Intellectual transport systems, digital infrastructure, GPS navigation, warehouse automation | Delivery chain optimisation, adaptiveness to war challenges, infrastructure sustainability |
| Health care | Telemedicine, biometrics, e-health records, IoT patient monitoring | Accessibility of health care, personalised treatment, preserving life in resource shortage |
| Education and science | Video-platforms, AI -tutors, digital laboratories, open data | Continued education, digital literacy, and staff quality for the digital economy |
| Small and medium-sized enterprises | E- business, digital marketplaces, CRM, online finances, automated taxation | Ease of business entry, scaling, participation in global chains, tax transparency |
| Energy | Demand forecasting, digital counters, automated capacity management | Energy effectiveness, system stability under damage conditions, load balancing |
| Economic security | Digital platforms for risk management, big data threats forecasting, digital audit | Economic stainability to cyber and hybrid threats, protection of infrastructure, control over strategic assets |

*Source: based on Cheng et al. (2023) and Wysokińska (2021).*

Innovative development and the introduction of digital technologies have led to significant economic changes. This, known as digital transformation, involves the integration of digital technologies into various aspects of economic activity. This has led to the reconfiguration of business models, the emergence of new industries, and the alteration of traditional economic structures. Digital transformation, caused by digital technologies, changes economic and social relations and influences organisations across all sectors.

Alongside the introduction of technologies, the digital transformation strategy is a holistic rethinking of business processes, public administration structure, decision-making logic, and creation value model. Although digital transformation is based on technologies, and it is necessary to introduce digital technologies, these factors are insufficient. Digital transformation strategies are considered from multiple perspectives.

From a business-oriented perspective, they transform products, processes, and organisational aspects owing to new technologies. By 2024, Ukraine's digital economy will demonstrate rapid development, attracting attention even at the international level. Ukraine has achieved significant indicators of digital infrastructure and technological integration.

In response to global trends in digital society development, and with 66.3% of its population already utilising the Internet, Ukraine vigorously pursues digital expansion. (Ministry of Digital Transformation of Ukraine, 2022).

The data supporting this analysis are listed in Table 2. Ukrainian enterprises actively integrate advanced technologies, particularly business-analytical software, cloud services, and AI, to improve their productivity and strengthen their competitive positions. However, their usage remains low.

**Table 2. Digital Technology Use in Ukrainian Industrial Enterprises, 2024.**

| **Entrepreneurship directions** | **Access to Internet** | | **Share of enterprises with a client mobile app, %** | **Share of enterprises, having web-portal, %** |
|---|---|---|---|---|
| | **Number of enterprises** | **% of total enterprises** | | |
| Field of raw processing | 8530 | 94% | 2% | 46.7% |
| Food industry and manufacture of beverages and tobacco products | 1765 | 96.5% | 3.2% | 38.3% |
| Manufacture of chemicals and materials | 411 | 97% | 2.3% | 53% |
| Manufacture of basic medicines and pharmacy products | 106 | 96.9% | 3.8% | 70% |
| Metallurgy and manufacture of ready-metal products | 974 | 91.8% | 0.7% | 50% |
| Machinery industry; manufacture as well as technical service, repair and mounting of machines and capacities | 2420 | 94.3% | 1.3% | 54.4% |
| Production of electronic, computer and optical devices | 191 | 97.2% | 2.3% | 71% |
| Manufacture of motor vehicles, trailers and other transport equipment | 231 | 90.6% | 2.3% | 62.3% |

*Source: based on data from the State Statistics Service of Ukraine (2024).*

The statistical data analyses concerning their technologies are presented in Table 3. In the digital age, strategic management security components cannot be considered separately from digital strategy. For example, electronic government services, big data systems, and digital identities are, at the same time, sources of effectiveness and a new risk vector.

Economic security is a critical component of the ongoing digital transformation that it relies on the level of technological equipment, and reliability of the available data. Approaches to economic security ensure the use of risk-management intellectual systems, digital platforms for economic situation analysis, and tools for automatic threat monitoring.

**Table 3. Digital Technology Usage in Ukrainian Enterprises, 2024.**

| Entrepreneurial Activity | Percentage of economic entities analysing big data, % | Share of enterprises using cloud computing services, % | Share of enterprises implementing AI technologies, % |
|---|---|---|---|
| Field of raw processing | 14,1% | 12,1% | 5,1% |
| Food industry and manufacture of beverages and tobacco products | 21,5% | 11,5% | 4,6% |
| Manufacture of chemicals and materials | 13,5% | 10,5% | 7% |
| Manufacture of basic medicines and pharmacy products | 19,5% | 16,5% | 1,8% |
| Metallurgy and manufacture of ready-metal products | 7,5% | 11,3% | 4,4% |
| Machinery industry; manufacture of furniture and other products, as well as technical service, repair and mounting of machines and capacities | 12,5% | 12,5% | 5,7% |
| Production of electronic, computer and optical devices | 13,7% | 13,2% | 2,8% |
| Manufacture of motor vehicles, trailers and other transport equipment | 14,6% | 16,3% | 6,7% |
| Construction | 10,1% | 9,2% | 5,3% |
| Retail trade | 21,4% | 17,5% | 5,6% |
| Development of software, IT-consulting and adjacent types of activities; IT-services | 25,6% | 33,1% | 7,1% |

*Source: based on the State Statistics Service of Ukraine (2024).*

The American Chamber of Commerce (2024) researched the directors and managers of Ukrainian businesses. The results show that the structure of the key challenges to enterprises' economic security changed with the onset of hostility (Figure 1). Thus, a triangle of strategic influence has been formed in Ukraine: strategic management, digital transformation, and economic security.

This interconnection can be described as follows:

– Strategic management defines digital transformation priorities.

– Digital transformation creates infrastructure and tools for effective risk management.

– Economic security is the goal and criterion for successful transformation strategies.

A holistic approach to studying them foresees developing integrated strategies combining digital transformation with risk management systems. The key methodological approaches for forming an economic security management system under digital transformation are as follows:

1. A systemic approach treats economic security as a multidimensional system that integrates all critical elements. This approach foresees the introduction of digital technologies into business processes and the forming of a unified digital environment for threat monitoring and counteraction.

2. The risk-oriented approach emphasises the detection, analysis, and reduction of risks caused by digital transformation. This encompasses the identification of new challenges, diagnostics, risk management, and permanent control.

3. The resource-oriented approach highlights the importance of the availability of appropriate financial, human, and technological resources for successful digital transformation. Such resource shortages may pose a critical threat to economic security in the future.

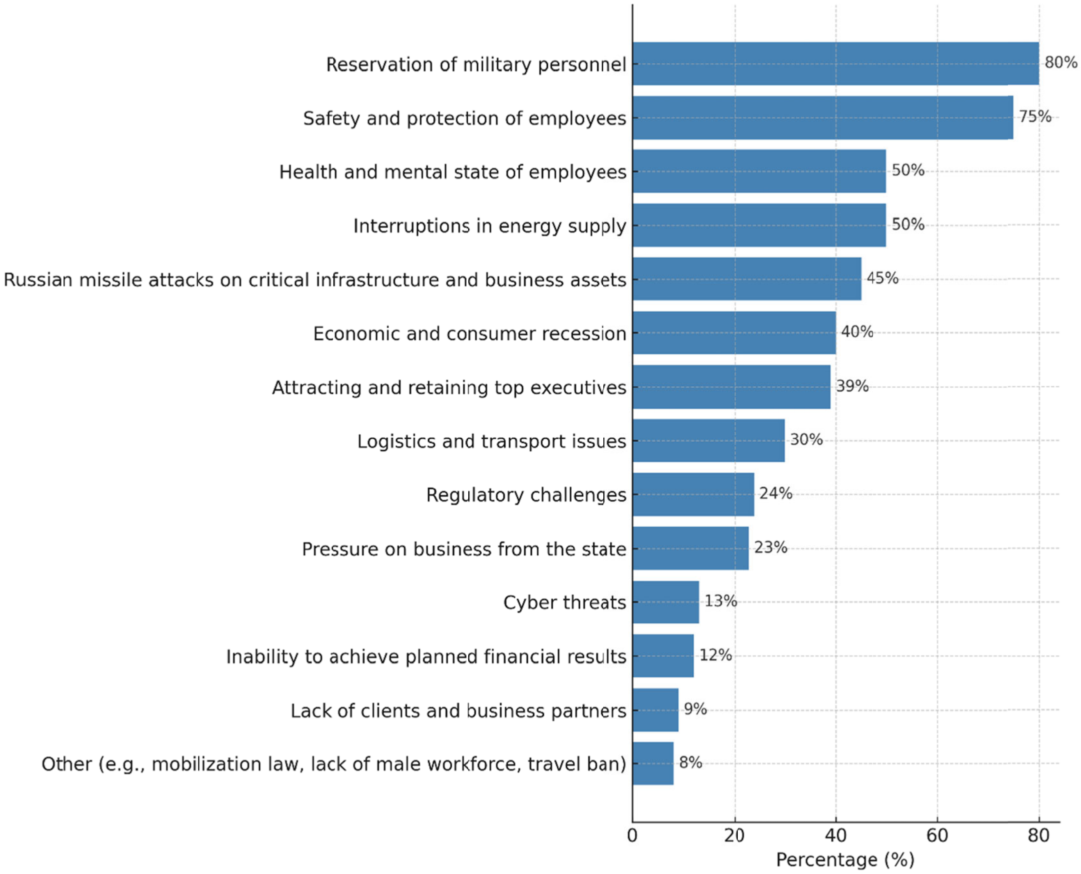

**Fig. 1. Dynamics of Key Business Security Challenges (2023-2024).**

*Source: based on American Chamber of Commerce of Ukraine (2024).*

Table 4 presents an analysis of the main approaches to forming mechanisms of economic security management under digital transformation and martial law.

The essence of the integrated strategy for creating an economic security system is that a comprehensive combination of different methods and technologies into a single system provides permanent risk monitoring, analysis and forecasting. The principal idea of an integrated approach is to build a digital ecosystem that synchronises the financial, operational, informational, and strategic aspects of economic security. This approach is based on general automation, end-to-end analytics, information system integration, and advanced digital technologies (Big Data, AI, the Internet of Things, blockchain, cyber security, ERP).

Digital economic security management platform (DESMP) must be a comprehensive decision-unifying tool for collection, analysis and risk management.

e-ISSN 2786-8958
ISSN-L 2616-7107

**Table 4. Approaches to Economic Security Management under Digital Transformation and Martial Law.**

| Approach | Essence of the approach | Key methods | Advantages |
|---|---|---|---|
| Risk-oriented approach | Focus on detection, analysis and management of risks that may threaten financial stability. | 1. Analysis of probabilities of the emergence of risks using machine learning.<br>2. Introduction of automated early warning systems (AI-driven Risk Detection).<br>3. Drafting scenarios of crisis situations response. | • Provides risks comprehensive analysis in real-time mode.<br>• Enable to draft business adaptation scenarios to external environment changes.<br>• Promotes financial expenses reduction du to quick risks response. |
| Approach, founded on big data technologies (Big Data) and predictive analytics | Use of big data analysis to predict potential economic threats and support making decision process. | 1. Collection and analysis of financial, market and operational data.<br>2. Use of machine learning algorithms to predict future events and economic risks.<br>3. Monitoring behaviour patterns of suppliers, clients and partners.<br>4. Automated analysis of macroeconomic factors to assess influence on the enterprise. | • High accuracy of economic risks prediction.<br>• Optimisation of financial flows and business processes.<br>• Detection of latent threats through analysis of untypical patterns in data. |
| Approach on the basis of cyber-security and digital control | Protection of enterprises digital assets through strengthening of cyber-security and management of access to critical important information. | 1. Use of block-chain technologies to protect financial transactions.<br>2. Implementation of cyber-security decisions on the AI basis.<br>3. Control over financial data access through multilevel authentication (MFA). | • Prevention of leaks of confidential information.<br>• Reduction of fraud risks and attacks on corporate data.<br>• Automated detection and blocking threats. |
| Integrated approach (Comprehensive Security Management) | Unification of all levels of economic security management into a single digital system. | 1. Integration of ERP, CRM, SCADA and other corporate systems into a single information network.<br>2. Implementation of end-to-end analytics to assess risks in entities.<br>3. Use of AI for optimisation of business processes. | • Maximum adaptation to conditions of digital transformation.<br>• The single control point for all processes.<br>• Flexibility in the choice of tools for risks management. |

*Source: created by the authors.*

The platform must have a modular architecture that enables it to adapt to the specific needs of the Ukrainian economy. The basic components of this platform are listed in Table 5.

When using a comprehensive approach, the following components must be added to the digital platform model:

1. Integration of corporate (information) systems, that is, connection to ERP, CRM, HRM, SCADA system, and Internet of Things (IoT), for automated data collection and processing and establishment of a single risk management centre, and on its basis, creation of a digital environment to analyse all security aspects.

e-ISSN 2786-8958
ISSN-L 2616-7107

2. Automated risk management systems, including risk forecasting with AI modules, automatically assess threats and make dynamic assessments of counterparties (checking suppliers' and partners' reliability systems).

3. Increasing cyber security levels, including the use of blockchain technologies for financial operation security, increasing transaction transparency, and introducing zero-trust security concepts for data access.

4. Automatisation of crisis management, including the building of such elements as a quick response incident module that is automated, blocking frauds, dashboards, and end-to-end analytics to reflect KPI risks in real-time, crisis response scenarios with automatic working out of strategies in case of threats.

5. Integration with government registers and external analytical platforms, in particular, building a legislative amendment checking the system for tracking new state regulators' requirements and market risk monitoring, as well as for the operative processing of macroeconomic information in real-time.

**Table 5. Key Elements of the Economic Security Management Platform.**

| Modules | Purpose | Functional |
|---|---|---|
| Risks analytics module | Automated risk analysis, threat detection and crisis prediction. | − Automated data collection from internal (ERP, CRM, financial systems) and outer sources (market analytical platforms, stock-exchange indicators, macroeconomic data).<br>− Risk assessment under different criteria (financial, operational, cyber-threats).<br>− Risk forecasting based on machine learning methods. |
| Risks management module | The digitalisation of procedures and mechanisms of risk management and elaboration of minimisation threats strategies. | − Classification of risks according to influence and probability of immersion.<br>− Drafting response scenarios and formation of risk management policy.<br>− Visualisation of risks in the form of dashboards and integrated charts.<br>− Automated algorithm of data-based decision making. |
| Monitoring and early threats detection module | Ensuring constant control over economic indicators and early risk detection. | − Constant monitoring of financial indicators, liquidity level, solvency and operational effectiveness.<br>− Anomalies detection and potential risks signalisation (AI + Big Data).<br>− Automated sending of alerts to management in case of critical threats.<br>− Analysis of interconnection of risks to forecast chain reactions. |
| Cyber-security and data protection module | Information threats prevention and cyber-security protection of digital assets. | − Integration with systems of information security management.<br>− Quick detection and neutralisation of cyber-threats in a real time mode.<br>− Automated reserve copying of critically important data.<br>− Access control to confidential information. |
| Crisis situation management module | Quick response to critical threats and economic crises prevention. | − Generation of anti-crises management plans.<br>− Simulation of crisis scenarios to train management staff.<br>− Automated deployment of crisis strategies under advanced determined protocols.<br>− Interaction between government structures and anti-crises services. |
| Reporting and decision-making module | Making detailed analytical reports and recommendations for management authorities. | − Generation of reports on the economic security level.<br>− Assessment of the effectiveness of introduced risk management measures.<br>− Recommendations for management authorities on security. |

Integrating the aforementioned components transformed the platform from an analytical tool into a completely automated governing system. The structural model of the platform is shown in Fig. 2.

The functioning of the economic security management digital platform is based on the use of various data sources to function its modules. Primary sources can be divided into internal and external.

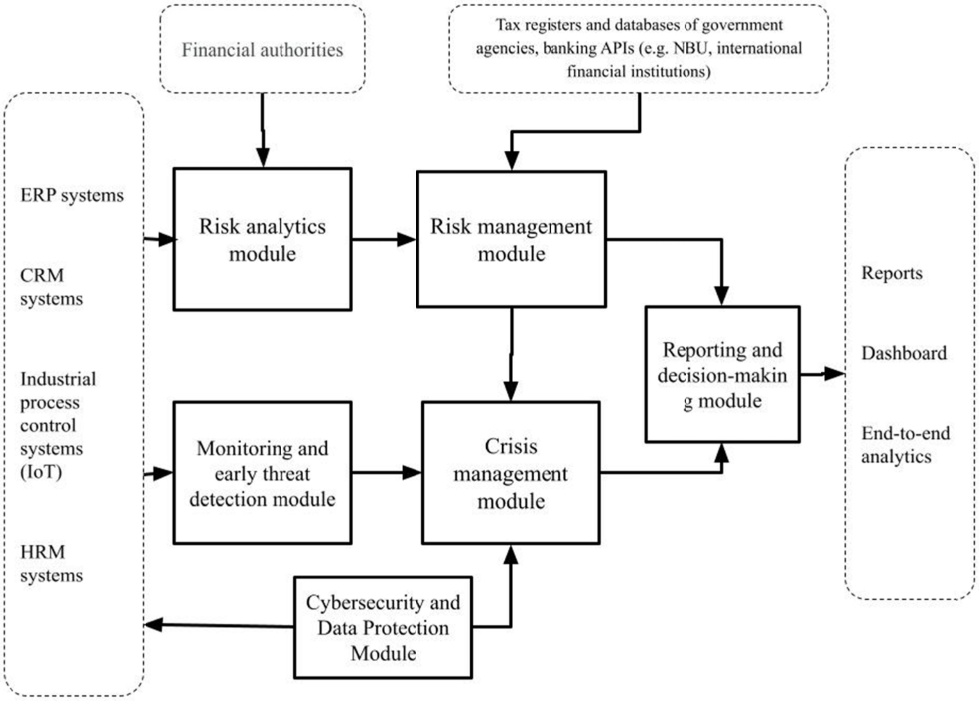
Financial authorities
Tax registers and databases of government agencies, banking APIs (e.g. NBU, international financial institutions)
ERP systems
CRM systems
Industrial process control systems (IoT)
HRM systems
Risk analytics module
Risk management module
Reporting and decision-makin g module
Monitoring and early threat detection module
Crisis management module
Cybersecurity and Data Protection Module
Reports
Dashboard
End-to-end analytics

**Fig. 2. Structural Model of a Digital Economic Security Management System.**

*Source: created by the authors.*

The information flow and platform data sources are listed in Table 6. It was built an optimisation mathematical model for the economic security monitoring system module (Kalinin, 2024).

This optimisation model aims to minimise the overall risk of economic losses in war conditions while ensuring financial stability, operational efficiency, and adaptation to external factors.

The model considers four sub-models:

1. Financial component (cash flow, investments, and profit management).
2. Operational component (production efficiency, resources, and logistics).
3. Risk-oriented component (identification, assessment, and minimisation of threats).
4. External factors component (especially economic, political, and military risks).

The description of this model includes an objective function that is represented as minimising the losses integral risk:

$$\min Z = \sum_{i=1}^{n} W_i * R_i + \sum_{j=1}^{m} W_j * F_j + \sum_{k=1}^{p} W_k * O_k \quad (9)$$

where:

$R_i$ – risks from the risk sub-model (e.g., cyber threats, staff issues);

$F_j$ – financial risks (asset depreciation, capital deficit);

$O_k$ – operational risks (logistics problems, production failures);

$W_i$, $W_j$, $W_k$ – weighting coefficients of the each risk group's impact.

$$\sum_{i=1}^{n} C_i X_i \leq B,$$

where:

$Ci$ – costs of risk protection;

$Xi$ – investment in protection measures;

$B$ – available budget.

**Table 6. Information Flows Making the Basis of Digital Security Management System.**

| Inner data sources | | Outer data sources | |
|---|---|---|---|
| **Source** | **Data type** | **Source** | **Data type** |
| ERP-enterprises systems (Enterprise Resource Planning) | Finance reporting.<br>Assets and resources management.<br>Logistics and supplying chains data.<br>Balance and cash flows | Finance and economic sources | Bank API (e.g., NBU, international financial institutions).<br>Stock-exchanges (NASDAQ, NYSE, London Stock Exchange).<br>Financial analytical services (Bloomberg, Reuters, Yahoo Finance) |
| CRM-systems of enterprises (Customer Relationship Management) | Clients and counterparties' data.<br>Sales and marketing campaigns analytics. Assessment of partners' creditworthiness | State registers and regulatory base | Tax registers and public authorities' database.<br>Government tenders, customs declarations.<br>Counterparties court decisions database |
| Finance management systems | Banking operations and transactions.<br>Debt obligations and financial risks.<br>Liquidity forecasting | Marketing and market data | Market trends and consumer behaviour data (Google Trends, Statista).<br>User feedback and reputation analysis (Glassdoor, Trustpilot).<br>Social media analytics (Facebook, LinkedIn, Twitter) |
| Enterprise production process control systems (Internet of Things) | Equipment state.<br>Assessment of productivity and efficiency levels.<br>Detection of failures or risks of production stoppage | Cybersecurity and external threat tools | Databases of known threats and attacks (VirusTotal, Shodan, Have I Been Pwned).<br>OSINT-services for open information collection.<br>Data leaks information |

*Source: created by the authors.*

Liquidity should be within a safe level:

$$\frac{GK}{ZF} \geq L_{min}$$

where:

$GK$ – cash;

$ZF$ – obligations;

$L_{min}$ – minimum liquidity level.

Operational constraints include supply chains continuity:

$$S_d \geq S_{min}$$

where:

$S_d$ – available raw materials amount;

$S_{min}$ – minimum required level.

Correspondingly, production capacity cannot be exceeded:

$$P_{\text{fact}} \leq P_{max}$$

where:

$P_{max}$ – maximum possible productivity.

Furthermore, it is necessary to define the following risk limits: the overall risk cannot exceed the critical level:

$$\sum_{i=1}^{n} R_i \leq R_{max}$$

The percentage of financial losses due to risks should not exceed the permissible level:

$$\frac{\sum_{i=1}^{n} R_i}{A} \leq \gamma$$

where:

$A$ – general assets;

$\gamma$ – maximum affordable loss rate.

External factors should be considered, and inflationary losses should not exceed a critical level.

$$F_{inf} \leq F_{max}$$

The hostilities impact on logistics cannot exceed a safe level either.

$$O_{log} \leq O_{max}$$

where:

$O_{log}$ – actual disruption in logistics caused by conflict (e.g., damaged infrastructure, blocked routes);

$O_{max}$ – the critical threshold beyond which logistics operations become unsustainable.

Accordingly, the task is to find the optimal solution to minimise the overall risk level by choosing between risk management options (material stock, financial reserves, changes in logistics, etc.).

In the context of digital transformation and increasing uncertainty in the external environment, especially in times of crisis, strategic risk management is key to ensuring the economic security of enterprises and the economy as a whole. Forming a mathematical model that minimises total risk through the optimal distribution of management measures is relevant.

The model aims to find a set of management decisions that provide the lowest level of weighted risk while adhering to established restrictions on critical impact categories. The model input parameters (Table 7) are as follows:

1. Expected economic losses for each risk category (conventional units).

2. Weighting factors (from 0 to 1), reflecting the relative criticality of the risks.

3. Restrictions on the permissible levels of individual risk groups.

The objective of the model is to minimise the total weighted risk, represented by the following function:

$$Z = w_1x_1 + w_2x_2 + w_3x_3 + w_4x_4 + w_5x_5 + w_6x_6 \rightarrow min$$

where:

$x_i$ – the level of risk for category $i$;

$w_i$ – the weight assigned to risk $x_i$.

The minimisation is subject to the following constraints:

1. Total risk constraint (e.g., maximum allowed losses):

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 \leq R\_total$$

2. Financial risk constraint:

$$x_2 + x_5 \leq R\_financial$$

3. Operational risk constraint:

$$x_1 + x_3 \leq R\_operational$$

4. External risk constraint:

$$x_4 \leq R\_external$$

The specific values for $A_i$ (if applicable), the weights $w_i$, and the risk limits $R*$ are determined based on a comprehensive risk assessment conducted in a given study, project, or strategic context. The model is flexible and can be adapted to any industry or regional context. Linear programming methods such as the simplex method or software tools can be used to obtain conditional values. (Excel Solver, Python-PuLP, R-optimisation, etc.).

With historical data in the economic security management system, it is possible to use the ARIMA model, which will provide a reliable short-term prediction of loss dynamics for the next three months. This allows enterprises to respond promptly to potential financial and operational challenges by optimising resources and revising risk management strategies (Wang et al., 2021; Almeida, & Gonçalves, 2022).

For extended periods, it is possible to use forecasting methods such as Random Forest Regression, which is suitable when there are many covariates (Zhang, 2024). Thus, based on data analysis, it is necessary to develop a strategy for adapting to macroeconomic conditions, including forecasting inflation in financial planning to monitor migration processes, prepare a human resource reserve to avoid a shortage of qualified workers, develop mechanisms to support mobilised workers (adaptation programs upon return).

**Table 7. Risk Categories and Associated Economic Impact (Conditional Values).**

| Risk category | Estimated losses | Variable | Weighting coefficient | Managerial interpretation example |
|---|---|---|---|---|
| Logistical | $A_1$ | $x_1$ | $w_1$ | Damage to infrastructure, blocking of ports and transport routes restrictions |
| Financial | $A_2$ | $x_2$ | $w_2$ | Exchange rate fluctuations and restrictions on foreign exchange transactions led to losses |
| Staff | $A_3$ | $x_3$ | $w_3$ | Mobilization, migration, and employee losses have caused a personnel shortage |
| Foreign threats | $A_4$ | $x_4$ | $w_4$ | Direct losses from hostilities, including destruction or damage to businesses |
| Inflation | $A_5$ | $x_5$ | $w_5$ | Frequent amendments in legislation and regulatory environment |
| Technological | $A_6$ | $x_6$ | $w_6$ | High inflation has led to rising costs for raw materials, energy, and other resources |

It is also necessary to ensure cybersecurity by strengthening data protection systems due to the increase in adversary cyberattacks. This will make it possible to minimise risks and strengthen economic security during wartime. Transparency is also a critical factor for the trust and effectiveness of an economic security ecosystem. It helps prevent corruption, and financial fraud; promotes international cooperation; and ensures the accountability of all participants. A model is proposed to ensure increased transparency and sustainability of enterprise management decision chains during post-war reconstruction. The analysis of documentation and procedures is the most clearly formalised approach for determining the initial transparency level of each management decision within the organisational structure.

This method is based on the assumption that the degree of transparency is determined by three key factors.

– Documentation (D): Presence of regulatory documents governing specific decision-making procedures.

– Procedure Clarity (P): The extent to which the decision-making algorithm is clearly and transparently described, including the identification of responsible parties, process stages, and acceptance criteria.

– Information Availability (A): The accessibility of information about the decision-making process or its outcomes to internal or external stakeholders.

The chain of managerial decision-making should be modelled as a directed graph, where:

– Nodes are specific management decisions or decision-making stages;

– Edges are the transfer of information or the influence between decisions.

– Transparency is a numerical score (from 0 to 1) that reflects the level of accessibility, documentation, and clarity of a decision.

– Edge weight coefficients are used to preserve transparency during the transfer between stages.

A directed graph can be described as follows.

$$G = (V, E), V = \{v_1,\ v_2, \dots, v_n,\}, \quad (10)$$

where:

$v_1$ – managerial decision;

$(v_i, v_j) \in E$ – influence or information transmission;

$T(v_i) \in [0,1]$ – initial level of solution transparency $v_i$;

$\omega_{i,j} \in [0,1]$ – coefficient of preserving transparency between solutions $v_i \rightarrow v_j$.

To quantify each solution's transparency, three parameters are assigned values ranging from 0 to 1, where 0 indicates the complete absence of the corresponding characteristic and 1 indicates its full implementation. Each solution is automatically or manually assessed for the presence of regulatory documentation (e.g., regulations, provisions, and procedures), formalised indicators and digital trails (e.g., electronic solutions and data logs), and open access to results.

A binary or quantitative indicator represents each parameter. The formula estimates the initial transparency score.

$$T_i = \alpha_1 * D_i + \alpha_2 * P_i + \alpha_3 * A_i, \quad (11)$$

where:

$T_i$ – transparency level of the 1st decision;

$D_i$, $P_i$, $A_i$ – respectively, documentation levels, procedural clarity and information availability for the 1st node;

$\alpha_1, \alpha_2, \alpha_3$ – weighting coefficients set by the expert according to the priority of factors (for example, $\alpha_1$=0.4, $\alpha_2$=0.3, $\alpha_3$=0.3).

The advantage of this method is that it is easy to integrate into digital audit and control systems. It also allows for quantitative transparency assessment without subjective surveys and is easily adaptable to the specifics of different organisations.

This approach was used to build a program to estimate the initial state of the nodes in the management system model. The value of $Ti$ for each model node is further used as a basis for transparency impact modelling between management decision links. The developed program based on the model made it possible to obtain a graph of the transparency of management decisions (Fig. 4).

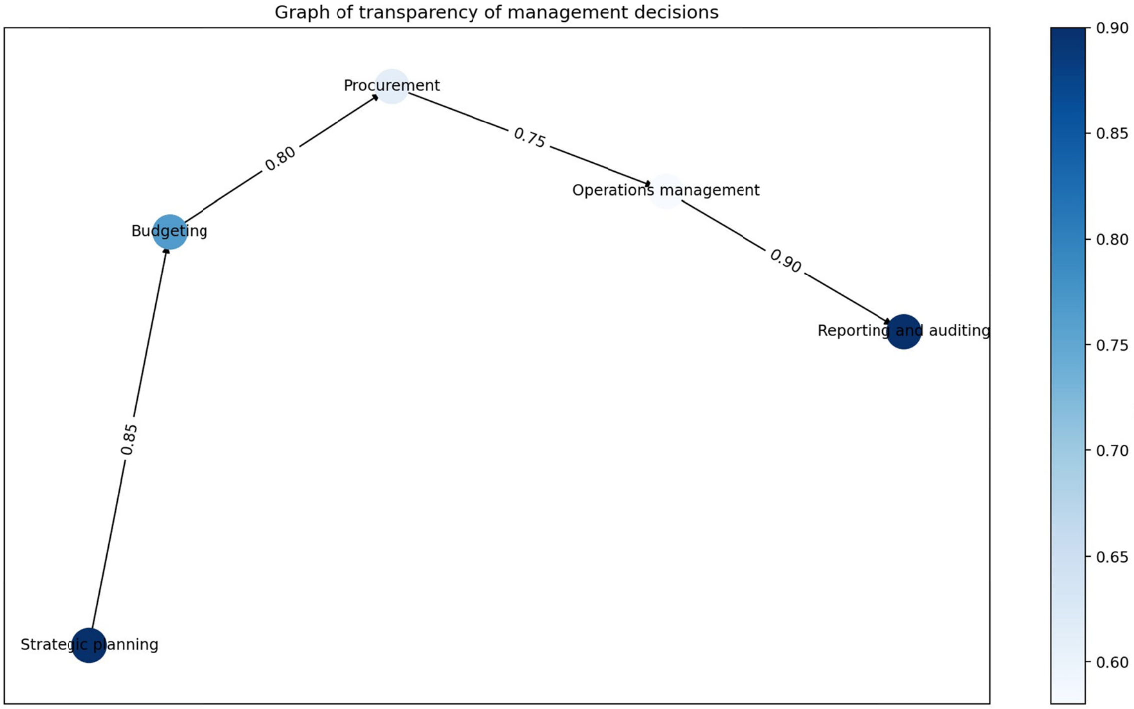

**Fig. 4. Transparency Graph of Management Decisions in Industrial Enterprises.**

The outcomes reveal that each node is not evaluated manually, but based on formalised parameters. Transparency is transmitted along the chain according to the retention coefficients, and visualisation helps to see the "bottlenecks" in management. The initial transparency of the high-level solution decreases when moving to lower management levels, depending on how well information is transmitted (edge weights).

This is shown in the graph as the transparency retention coefficients, which are indicated on the links between the stages (Strategic planning –> Budgeting: 0.85; Budgeting –> Procurement: 0.80; Procurement –> Operations management: 0.75 and Operations management –> Reporting and auditing: 0.90). The transparency levels across various management decision areas were as follows: strategic planning – 0.940, budgeting – 0.799, procurement – 0.639, operational management – 0.580, and reporting and audit – 0.940. The software application results demonstrate that each node is evaluated not manually but based on formalised parameters. Transparency is propagated along the management chain by conservation coefficients, and visualisation enables the identification of "bottlenecks" within the system.

Moreover, transparent management allows building a single information field that counteracts disinformation and strengthens public trust in government actions. This, in turn, will increase society mobilisation, contribute to consolidating efforts around strategic goals, and facilitate coordination with international donors.

## 5. Conclusions.

Despite the wartime challenges, Ukrainian enterprises are actively integrating digital technologies. In 2024, 97.7% of software development companies had access to the Internet, and 10.9% of retail enterprises used mobile apps for customers. However, the number of advanced technologies used, such as big data analysis, cloud services, and AI, remains low. For example, only 25.6% of software development companies analyse big data, and only 7.1% use artificial intelligence technologies.

This study analysed and proposed the use of an integrated approach to build a digital platform for managing the economic security of industrial enterprises. This approach combines risk-based methods, cyber-defence tools, big data analytics, and AI algorithms into a single functional system. A formalised structure of such a digital platform with a modular architecture has been presented, which will provide real-time threat forecasting and detection and automated anti-crisis response by the state, considering the industry sectoral characteristics in post-conflict conditions.

The optimisation mathematical model of the economic security monitoring system was modified, which included four interconnected subsystems (financial, operational, risk, and external factors) and minimised the risk of losses through rational resource allocation within the given constraints. A model was developed to ensure the transparency and sustainability of enterprise management decision chains during post-war reconstruction.

The proposed model provides a quantitative basis for making management decisions under uncertainty, allowing management mechanisms to adapt to external environmental changes and the military economy. Under current conditions, the national economy is at a stage of development where strategic management, digital transformation, and economic security should be considered within a single strategy of socio-economic development as autonomous areas, but instead requires a comprehensive, interconnected approach. Their integration is necessary to restore, grow, and protect national interests. Further research should be directed towards developing models for assessing an enterprise's digital readiness level in the context of economic security risks and creating dynamic simulations of digital security for government and corporate structures. This will make it possible to increase the adaptability of management systems to digital challenges.

**Acknowledgment.**

This study was supported by project NID-NI22/2025 "Modern Methods for Algorithmic Management in Bulgaria", funded by the University of National and World Economy.

## REFERENCES

Almeida, J., & Gonçalves, T. C. (2022). A Systematic Literature Review of Volatility and Risk Management on Cryptocurrency Investment: A Methodological Point of View. Risks, 10(5), 107. https://doi.org/10.3390/risks10050107

American Chamber of Commerce of Ukraine. (2024) AmCham/Citi Survey. Ukraine Wartime Business Assessment. https://chamber.ua/news/amcham-citi-survey-ukraine-wartime-business-assessment/

Bondarenko, S., Tkachuk, H., Klochan, I., Mokhnenko, A., Liganenko, I., & Martynenko, V. (2021). Modeling of economic security of the enterprise at change of investment maintenance. Estudios de Economía Aplicada, 39(7). https://doi.org/10.25115/eea.v39i7.5011

Brunetti, F., Matt, D. T., Bonfanti, A., De Longhi, A., Pedrini, G., & Orzes, G. (2020). Digital transformation challenges: strategies emerging from a multi-stakeholder approach. The TQM Journal, 32(4), 697–724. https://doi.org/10.1108/tqm-12-2019-0309

Cheng, Y., Zhou, X., & Li, Y. (2023). The effect of digital transformation on real economy enterprises' total factor productivity. International Review of Economics & Finance, 85, 488–501. https://doi.org/10.1016/j.iref.2023.02.007

Dvorsky, J., Belas, J., Gavurova, B., & Brabenec, T. (2021). Business risk management in the context of small and medium-sized enterprises. Economic Research-Ekonomska Istraživanja, 34(1), 1690–1708. https://doi.org/10.1080/1331677x.2020.1844588

Harahulia, A., Suslov, V., & Horovoy, O. (2023). Management of economic security of enterprises in the context of digital transformation. Baltic Journal of Economic Studies, 9(5), 87-93. https://doi.org/10.30525/2256-0742/2023-9-5-87-93

Kalinin, O. (2024). Investment Security in the Development of the Digital Economy. Economics Ecology Socium, 8(2), 73–84. https://doi.org/10.61954/2616-7107/2024.8.2-6

Kalinin, O., Kaminsky, O., & Teslenko, T. (2023). Digitalization of Economic Security Management in Investment Security of Ukraine. Economics. Ecology. Socium, 7(4), 83–95. https://doi.org/10.61954/2616-7107/2023.7.4-7

Kochubei, O., Shebanina, O., Sokhatska, O., Yaroshenko, I., & Nych, T. (2021). The Impact of Digital Transformation on the Economic Security of Ukraine. Estudios de Economía Aplicada, 39(3), 1–15.

Kraus, K., Kraus, N., Manzhura, O., Ishchenko, I., & Radzikhovska, Y. (2023). Digital transformation of business processes of enterprises on the way to becoming industry 5.0 in the gig economy. WSEAS Transactions on Business and Economics, 20, 1008–1029. https://doi.org/10.37394/23207.2023.20.93

Ministry of Digital Transformation of Ukraine. (2022). Digital transformation Index of regions of Ukraine: results of 2022. https://thedigital.gov.ua/

O'Grady, M. (2024). The global digital economy will reach $16.5 trillion and capture 17% of global GDP by 2028. Forrester. https://www.forrester.com/blogs/the-global-digital-economy-will-reach-16-5-trillion-and-capture-17-of-global-gdp-by-2028/

Rauniyar, K., Wu, X., Gupta, S., Modgil, S., & Lopes de Sousa Jabbour, A. B. (2023). Risk management of supply chains in the digital transformation era: contribution and challenges of blockchain technology. Industrial Management and Data Systems, 123(1), 253–277. https://doi.org/10.1108/imds-04-2021-0235

Samoylenko, Y., Britchenko, I., Levchenko, Y., Losonczi, P., Bilichenko, O., & Bodnar, O. (2023). Economic security of the enterprise within the conditions of digital transformation. Economic Affairs, 68(3), 1–10. https://doi.org/10.37394/232032.2023.1.5

Schallmo, D., Williams, C. A., & Lohse, J. (2019). Digital strategy — integrated approach and generic options. International Journal of Innovation Management, 23(08), 1940005. https://doi.org/10.1142/s136391961940005x

SecurityDive. (2024). Global cybersecurity ranking 2024: Which countries are most at ris? https://securitydive.in/2024/05/14/global-cybersecurity-ranking-2024-which-countries-are-most-at-risk/

Shkolnyk, I., Frolov, S., Orlov, V., Datsenko, V., & Kozmenko, Y. (2022). The impact of financial digitalization on ensuring the economic security of a country at war: New measurement vectors. Investment Management and Financial Innovations, 19(3), 119–138. https://doi.org/10.21511/imfi.19(3).2022.11

Spivakovskyy, S., Kochubei, O., Shebanina, O., Sokhatska, O., Yaroshenko, I., & Nych, T. (2021). The impact of digital transformation on the economic security of Ukraine. Studies of Applied Economics, 39(5). https://doi.org/10.25115/eea.v39i5.5040.

State Statistics Service of Ukraine. (2024). Complex Statistical Publications. https://www.ukrstat.gov.ua

Stender, S., Bulkot, O., Iastremska, O., Saienko, V., & Pereguda, Y. (2024). Digital transformation of the national economy of Ukraine: Challenges and opportunities. Financial and Credit Activity: Problems of Theory and Practice, 2(55), 333–345

Voronenko, I., Bohush, A., Voronenko, O., Klymenko, N., Kostenko, I., & Kudrina, O. (2024). Digital transformation research trends in Ukraine and the world: Meta-bibliometric analysis. Knowledge and Performance Management, 8(1), 74–90. https://doi.org/10.21511/kpm.08(1).2024.06

Wang, J., Zhao, L., & Huchzermeier, A. (2021). Operations-finance interface in risk management: Research evolution and opportunities. Production and Operations Management, 30(2), 355–389. https://doi.org/10.1111/poms.13269

Wysokińska, Z. (2021). A review of the impact of the digital transformation on the global and European economy. Comparative Economic Research, 24(3), 75–92. https://doi.org/10.18778/1508-2008.24.22

Zachosova, N., Kutsenko, D., & Koval, O. (2022). Strategy and mechanism of enterprises financial and economic security management in the conditions of war, Industry 4.0 and bani world. Financial and Credit Activity Problems of Theory and Practice, 4(45), 223–233. https://doi.org/10.55643/fcaptp.4.45.2022.3819

Zhang, J. (2024). Impact of an improved random forest-based financial management model on the effectiveness of corporate sustainability decisions. Systems and Soft Computing, 6(200102), 200102. https://doi.org/10.1016/j.sasc.2024.200102