DOI: 10.61954/2616-7107/2023.7.4-7 *ISSN 2616-7107*

UDC 005.33
JEL: C810, D810, O320

DIGITALIZATION OF ECONOMIC SECURITY MANAGEMENT IN INVESTMENT SECURITY OF UKRAINE

Oleksandr Kalinin
Mykolas Romeris University,
Vilnius, Lithuania
ORCID iD: 0000-0001-5238-0525

Oleg Kaminsky*
Kyiv National Economic University named after Vadym Hetman,
Kyiv, Ukraine
ORCID iD: 0000-0003-0607-8944

Tetiana Teslenko
Higher Private Educational Institution "Dnipro Humanitarian University",
Dnipro, Ukraine
ORCID iD: 0000-0002-5810-3569

*Corresponding author:
E-mail: olkam@kneu.edu.ua

Received: 11/07/2023
Accepted: 18/12/2023

DOI: 10.61954/2616-7107/2023.7.4-7

Introduction. The study of economic security is relevant due to strengthening competition in the world market and military conflicts, which are becoming critical tasks for the state. Studying economic security makes it possible to identify the problematic aspects of a country's economy, find solutions, and develop strategies to ensure a sustainable investment policy. The specifics of changes in organizational models associated with digitalization also transform investment management systems. The most significant digital changes affect economic security, as the high openness of companies contributes to the emergence of various threats and risks to their activities. Therefore, it is essential to study the problems related to the risks of digital transformation within the framework of economic security management in the investment provision of Ukraine.

Aim and tasks. The purpose of the study is to analyse problems and develop a recommendation for assessing the level of economic security when developing investment projects, taking into account the risks of digital transformation, for better preparation for future projects of post-war reconstruction in Ukraine.

The results. This study developed a conceptual model for assessing the level of economic security, which includes the systematization of critical indicators of economic security and the organization of ensuring end-to-end transparency of information during the implementation of investment projects for the post-war reconstruction of Ukraine based on intelligent technologies. Software for assessing economic security using machine learning methods is proposed, which will allow forecasting the state of the enterprise's economic security for the entire implementation period of the investment project.

Conclusions. This research proved that an enterprise's economic security is a complex and integral economic concept that requires studying the influence of several external and internal factors. Therefore, the established approach to assessing the state of economic security should cover all current investment processes and risks that arise in the context of the digitalization of enterprises, influencing the choice of critical indicators. Post-war reconstruction should be based on the modernization of the economy by improving the security of the business environment (reducing corruption, ensuring private property rights and strengthening the security of business activities) and the transition to a digital society.

Keywords: digitalization, economic security, investment, forecasting, management decisions, cybersecurity.

1. Introduction.

Digitization has become a key factor affecting all spheres of activity, including the economy and management. In particular, digital technologies make it possible to increase labour productivity, reduce costs, improve product quality, ensure more effective decision-making, and make the business processes of enterprises more transparent and accessible. The role of digitalization in managing economic security in today's rapidly evolving global landscape cannot be underestimated. Digital technologies provide more effective control over financial transactions, reduce the risks of fraud and cyber-attacks, and provide more accurate forecasts of market trends. Effective economic security management is critical for countries such as Ukraine seeking to attract foreign investment and foster economic growth in a challenging environment (Redkva et al., 2022).

Foreign and domestic investments are the key drivers of economic growth. Investments attract capital, create jobs, promote innovation, and improve infrastructure.

Modern economic literature lacks publications substantiating the state and function of legal entities' investment activities within the economic security framework. Because economic security issues depend on such a large number of variables, studying them is generally tricky. Investment is becoming increasingly essential to ensure economic security, as evidenced by new economic practices. In this regard, the novelty of researching the role of investment activity and its transition to digital technologies in ensuring economic security and finding adequate forms of implementing this process seems theoretically and practically significant.

According to the analysis and assessment carried out by the Kyiv School of Economics, the total amount of damage caused to infrastructure as of mid-2022 already amounted to more than $95.5 billion (2.6 trillion UAH) (Cabinet of Ministers of Ukraine, 2022). At the same time, the value of undamaged assets in the occupied territories until February 24, 2022, and later were not taken into account. The total amount of loss to the Ukrainian economy was estimated at $126.8 billion (Cabinet of Ministers of Ukraine, 2022).

According to the Ukrainian Recovery Plan, the costs of reconstructing Ukraine's infrastructure may amount to 750 billion US dollars (760 billion euros) (Cabinet of Ministers of Ukraine, 2022). The EU estimated these costs to be $349 billion. The investment volume of various recovery programs varies from 100 to 500 billion US dollars and involves implementation with the help of partners from the US and EU (Cabinet of Ministers of Ukraine, 2022). One of the provisions of the Recovery Plan of Ukraine (Cabinet of Ministers of Ukraine, 2022) established the priority of investment activity and the attraction of direct investments in programs and projects aimed at the post-war recovery and modernization of Ukraine.

Economic security is the foundation for a nation's prosperity and well-being. It covers several factors, including financial stability, protection against economic threats, and the ability to attract investment. For Ukraine, as a country with huge potential but facing security challenges, maintaining and developing economic security is a top priority.

The digitization of enterprises has made noticeable changes to the investment management system. The main changes resulting from digital transformation are aimed at strengthening economic security, given that the increased openness of companies to the external environment creates new threats and risks to their activities (Koval et al., 2023). Investigating the risks associated with companies' digital transformation is crucial for ensuring economic security.

2. Literature review.

Several Ukrainian and foreign researchers once considered the issue of economic security in the digital economy.

Pravdyvets (2022) comprehensively analysed the latest research on the theoretical foundations of the nation's economic security. This analysis identified the main challenges in the theory of economic security; aspects related to the clarification of conceptual and categorical frameworks were considered, and it was proposed to consider "economic security" as a purposeful function of the state.

This should aim to ensure the stable functioning of national security and promote socioeconomic development.

The results of the study by Romanovska et al. (2022) established the reasons for the negative state of the Ukrainian economy, which was caused by military aggression and the long-term economic crisis that arose as a result of military destruction. The slowdown in business activity in 2021, which occurred due to the COVID-19 pandemic, was also analysed.

Research by Hrynkevych et al. (2023) focused on the analysis of regional features of investment activity in Ukraine as a factor of economic security under the conditions of martial law and in the recovery period, based on indicators of investment activity in the pre-war period as well as a plan to restore the socio-economic infrastructure that was destroyed as a result of the war.

The report of the United States Agency for International Development (USAID, 2023) emphasizes that the critical factor in the post-war recovery of Ukraine will be investments from the private sector with the assistance of the state and monitoring each investment project within the appropriate framework.

Moore (2021) conducted an analysis of the data of a global sample for the post-war period from 1970 to 2008 in the field of direct investment and concluded that it is possible to reduce the critical risks for foreign direct investment by strengthening policies in the field of information transparency for reconstruction projects.

Virlics (2013) reviewed the approach to investment decision-making, identified the role of risk and uncertainty in the decision-making process, and emphasized the importance of analyzing investment risks from a behavioural economics perspective.

Marquez-Tejon et al. (2022) analysed the role of economic security, which has the potential to manage crisis situations and should be integrated into the enterprise management system. After analysing more than 400 articles for the period between 1986 and 2019, it was concluded that economic security is an independent scientific direction.

Marton (2023) presented the view of economic security as a controversial concept in the focus of ideological debates about the role of the state and social justice, emphasizing the need to clarify the definition of this term.

Schwertner (2017) examined the opportunities associated with digital business transformation and identified changes resulting from the adoption of digital technologies in various aspects of business. The study found that businesses prioritize the integration of technologies, such as social networks, smart analytics, big data, and cloud computing. Digital transformation makes risk-taking more normalized in its aspirations to increase the level of competitive advantage.

Peng and Tao (2022) analysed enterprise data for the period from 2012 to 2020, applying a special measurement model, and tested whether digital transformation contributes to the stimulation of innovation movement and revealed the internal dynamics of such relationships. They point to a significant increase in the efficiency of the company's activities thanks to digital transformation and note a significant innovative impulse at the enterprises.

Despite the wide range of scientific publications on the aforementioned problems, the study of economic security in correlation with the current stage of the digital transformation of the economy has been neglected. Strategies and tools for ensuring the stability of companies during war and their economic security under increased digitalization have still not been sufficiently studied. Digitization, as a component of economic security, is an actual scientific problem that requires theoretical and practical clarification.

Aim and tasks. The aim of the study is to analyze problems and develop a recommendation for assessing the level of economic security when developing investment projects, taking into account the risks of digital transformation, for better preparation for future projects of post-war reconstruction in Ukraine.

3. Methodology.

The study was based on scientific and theoretical methods, such as: the analysis and synthesis of scientific, technical, and economic literature related to the implementation of digital technologies; cyber security; the development of the digital economy and entrepreneurship; systemic, inductive, and deductive approaches.

The scoring method of assessing the state of economic security is based on an expert survey of specialists, processing the survey results, presenting them in the form of points, and interpreting the obtained score in the form of judgments about risks, threats, and the effectiveness of solving problems. A similar method has been implemented in a number of international standards and software products, such as the ISO 1779910 standard and software products that implement CRAMM methods (CCTA11 Risk Analysis & Management Method). The CRAMM is currently the most widely used method.

$$t = \frac{12V}{(n^2 (a^3 - a))}, \quad (1)$$

where: V is the sum of the squared deviations of all estimates for each object of the average value, a is the number of evaluation directions, and n is the number of experts. The concordance coefficient ranges from 0 to 1, where 1 represents the absolute unanimity of experts, and 0 represents a complete lack of agreement.

4. Results.

There is a widely accepted concept that society is currently experiencing the fourth industrial and technological revolution, called "Industry 4.0". Accordingly, the economy is gradually adopting technological, digital, and even cloud characteristics. Digitization is recognized as a fundamental element of the architecture of the Fourth Industrial Revolution. Innovation plays a significant role in shaping the digital economy, as evidenced by the annual publication of the list of the 50 most innovative companies in the world by the Boston Consulting Group (BCG) (2023).

The rating for 2023 includes companies from 9 countries, of which 50% are located in the USA, 30% in Europe, and 20% in Asia. According to BCG, the most innovative companies in the world for 2023 are considered in Table 1.Examining the information presented in Table 1 makes it possible to conclude that advanced innovative companies are enterprises engaged in developing technologies.

Table 1. The first 10 positions of the Boston Consulting Group (BCG) rating

Positions	Company	Country	Field of activity
1	Apple	USA	IT-technologies
2	Tesla	USA	Automobiles
3	Amazon	USA	Consumer goods
4	Alphabet	USA	IT-technologies
5	Microsoft	USA	IT-technologies
6	Moderna	USA	Biotechnology
7	Samsung	South Korea	IT-technologies
8	Huawei	China	IT-technologies
9	BYD Company	China	Automobiles
10	Siemens	Germany	Electrical engineering, electronics

Source: based on Boston Consulting Group (2023).

The "technological economy" development and the penetration of digital processes and technologies into the production cycle led to the term "digital economy". In the digitalization of the real sector of the economy (retail, tourist services, industry and agriculture, freight transportation, public catering, hotel business, and medicine), this term became more general. It began to include all areas of business based on information technology and telecommunications. Digitization should provide the Ukrainian economy with modern technological solutions, using which companies will ensure an advantage in the rate of reduction of specific operating and investment costs, and optimize innovative development, infrastructure content, and the structure of technological process management.

However, the procedure for making management decisions under the conditions of digitalization is complicated by the presence of uncertainty regarding the impact of digital tools on current processes, conservative views of managers, and a certain "fear of change".

Now, the situation has developed so that new yet unidentified threats may arise in addition to the already classified threats to economic security in the digitalization process. However, an active transition to the implementation of digital technologies will significantly reduce response time to the current challenges of the modern economy and political situation. Digitization should increase economic security at various levels by creating new infrastructure opportunities, ensuring a new qualitative living standard for the population thanks to new service standards and services, and transitioning to an innovative path of economic development.

There was also an increase in the balance and direct foreign investment in Ukraine in 2019 by USD 5.212 million and USD 2.449 million USD in 2023 (MinfinMedia, 2023).

Figure 1 shows the dynamics of direct foreign investment in Ukraine over the past five years. Despite the decrease in the volume of investments at the beginning of 2022 because of hostility, there is a recovery in their growth in 2023.

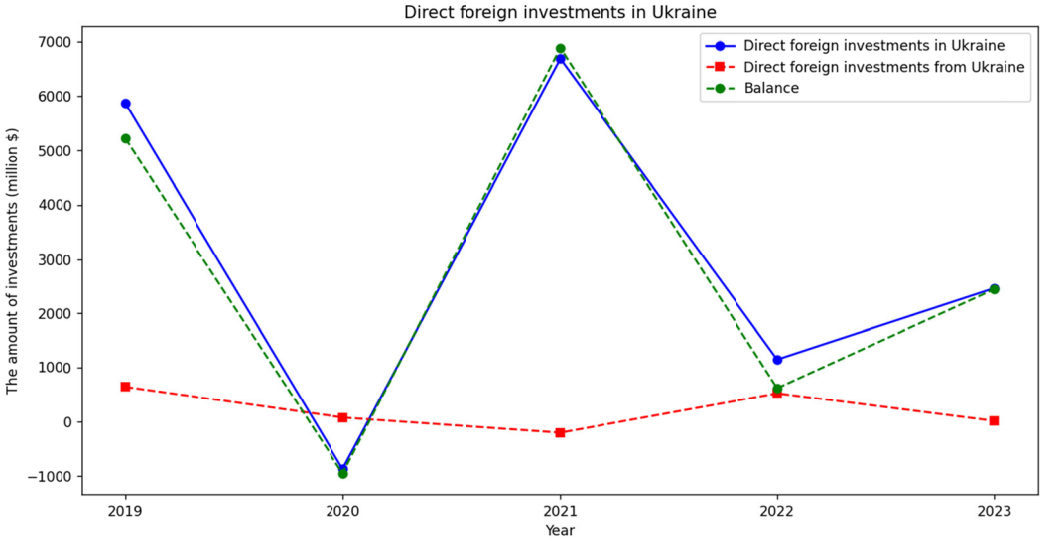

Figure 1. Dynamics of foreign direct investment in Ukraine for 2019-2023.

Source: based on MinfinMedia (2023).

During several years before the war and a year after the war, significant changes took place in Ukraine regarding the digital transformation of public administration, digitalization of business processes, and introduction of new technologies: electronic document flow and electronic declaration were introduced, state institutions provided electronic services, and the launch of ID-passports was accomplished.

According to the OECD (2022), before the start of the war, Ukraine's digital economy was experiencing rapid growth, and the Ministry of Digital Transformation, together with the Ukrainian IT community, intensified its efforts in response to the war.

In 2021, Ukrainian IT exports increased by 36% compared to the previous year, reaching 6,8 billion USD, or 10% of the country's total exports. At the same time, the workforce in the IT industry has grown from 200,000 to 250,000, spanning start-ups, SMEs, and corporations. In the first quarter of 2022, the information technology and communication (ITC) sector generated export revenue of 2 billion USD, representing a growth of 28% compared to the same period last year. Despite the significant disruptions caused by the war, the increased attention of the international community and investment policy can open up critical opportunities for the future development of the digitalization of Ukraine's economy (Hrynkevych et al., 2023).

Research by the Cabinet of Ministers of Ukraine (2022) indicates a progressive increase in the digital economy's contribution to Ukraine's GDP. In 2019, the digital economy accounted for only 4.3% of Ukraine's GDP, but it increased to 5.3% the following year.

However, in 2022, the rate of digitization of the economy slowed due to a full-scale war, which negatively impacted the digital economy's share of GDP. However, forecasts point to a recovery expected to rise to 7.7% in 2024.

The Digital Transformation Index of the regions of Ukraine was introduced by the Ministry of Digital Transformation of Ukraine (2022) to measure the processes of informatization and digitalization in the regions. The analysis results for 2022 show that the Digital Transformation Index of regions within Ukraine is 0.651 points out of 1 possible. Dnipropetrovsk (0.916), Ternopil (0.910), and Odesa (0.836) regions have the highest values. According to the research, the Dnipropetrovsk, Ternopil, and Rivne regions are developing strongly.

The revival of the Ukrainian digital economy depended on mitigating the main risks in the investment climate. This involves maintaining a stable and well-managed military situation, promoting the increase of direct investment in enterprises, ensuring the availability of insurance, reliably protecting information flows, and increasing the transparency of management decision-making processes.

Compared to developed countries, in Ukraine, the legislative framework regarding the execution of electronic (digital) agreements is underdeveloped. Ukraine's legislation does not establish special conditions for the protection of consumers in e-commerce when they receive services, and there are no requirements for the disclosure of information about sellers, goods, and transactions, the features of which are related to e-commerce, as provided for in the recommendations on the protection of consumers in e-commerce (OECD, 2011).

The main challenges and factors hindering the progress of digital transformation in the financial and investment sectors include issues such as an outdated legal framework, the presence of a digital divide, significant expenditures of enterprises for digital transformation, reduction of jobs due to digitization and integration of artificial intelligence tools into business processes, growing disparity in the labour market, and increasing cyber risks during wartime.

In the modern theory of cyber security and information protection, there are more than several dozen classifications of threats according to various parameters: spheres of influence, subjects, causes of occurrence, degree of damage caused, level of predictability of the threat, and other classifications. Without adhering to a single approach to the classification of risks that may arise in the context of economic security under martial law and digitalization, it is possible to rank risks in the context of supporting the economic potential of the company, for which it is necessary to analyse the types and indicators of security (Table 2).

In terms of national and military security, digitalization introduces the possibility of inflicting significant casualties without overt military intervention. The development of digital and information technologies has created the following threats to state security:

– extraction of military and intelligence information;

– spread of fake information and psychological impact on the economy;

– threat of information bases destruction, in particular, state registers;

– use of virus programs for infrastructure attacks.

These risks may be exacerbated by the rapid growth of fintech technologies, new forms of interconnection (cloud computing, operation of big data services, etc.) that are not covered by government regulation. The most significant influence on the effective functioning of fintech under the conditions of digital transformation and martial law is cyber risk (the risk of committing cyberattacks).

Table 2. Classification of threats to the economic security of the enterprise based on their typification and performance indicators.

Threat type	A key indicator of economic efficiency	A threat to economic security
Technological threats	Charge of production capacities	• Inconsistency of the current condition of technical equipment with the requirements for the digital transformation of digitization • Instability of communication channels with remote branches and trade networks under conditions of martial law • Instability of energy supply due to military actions • Threats to information systems as a result of cyber warfare
Investment threats	The effectiveness of the investment plan Timely implementation of projects	• Integration of hardware and software in the context of risky supply • Lack of data analysis systems • Insufficient provision of information transparency for investors
Digital threats	Increasing labor productivity Implementation of additional services	• Lack of competence of personnel in the field of modern IT • Growing unemployment due to the introduction of AI-based technology
Economic threats	Profit from the sale of products and services Reduction of operating costs	• Necessity to invest in new equipment, software, rental of cloud services • Uncertainty of the expected economic effect (the payback period of the investment becomes longer)

Source: developed by the authors.

Several strategic risks characterise the development and use of advanced cyber capabilities. For example, there is the possibility that these capabilities could undermine the safe and secure functioning of the Internet, spread dangerously, or act as a catalyst for escalation, particularly given the lack of clarity regarding the extent to which the recognised boundaries of international law regarding the "real world" apply to cyberspace. There is a risk that cybercriminals' widespread and dangerous everyday use of these cyber capabilities could go unchecked. Since 2018, developed countries have actively promoted the concept of "responsible cyber governance" to rationalise and explain their positions on various international legal and regulatory aspects related to cyber operations.

Freedman and Williams (2023) proposed a bullet-point framework for the responsible use of cyber power.

Countries can explain the relevant principles of responsible cyber governance using this framework:

1) The country recognizes that existing international law can be effectively applied to cyber operations, both in peacetime and wartime, and actively demonstrates this in practice. The basic principle is to evaluate cyber operations by their consequences, not by the means used. Countries should publicly identify the impact of international law on their cyber operations, avoiding an exclusive focus on what they consider wrongful in the international context.

2) The country actively collaborates with others to improve collective cyber security, ensuring collective protection against all forms of hostile cyber intrusion. Also, it carefully monitors the use of offensive cyber operations and determines prohibited targets and parameters, taking into account legal aspects in peacetime and wartime.

3) Countries counter and control the spread of offensive cyber capabilities by providing transparency on the measures they are taking to minimize risks to global cyber security. They are also actively working to prevent dangerous non-state offensive cyber activity and cooperating internationally to counter non-state cyber threats.

4) Countries not only encourage but also actively participate in public debates regarding the responsible use of cyberpower, including discussions of their own use of aggressive cyberattacks.

Adherence to these principles would contribute to the establishment of sufficient international consensus regarding one of the most challenging aspects that arise in the context of advanced cyber operations: determining whether a state is using its cyber potential irresponsibly to the extent that an international response, including the use of proportionate countermeasures, is justified.

Another risk that has the most significant impact on economic security is the spread, under conditions of digitalization, of business models belonging to the ideology of the sharing economy, the so-called sharing economy, which works based on digital technologies. In this direction, it is advisable to pay attention to the details of regulation of digital transformation and protection of consumer interests. Digitization also contains threats of a legal nature:

– First, there is a lack of a formal regulatory and legal framework regulating the relations between subjects in the digital environment. There is a problem with identifying the subjects themselves; in the virtual environment, they can be depersonalized, acting on behalf of a virtual personality.

– Second, digitalization affects understanding the object of legal relations: information becomes the main object. Ownership and access to information are becoming critical in private and public law. New objects of law appear: cryptocurrency, digital goods, and virtual objects. In this situation, adapting the current legal norms regarding economic security is necessary, and it is possible to create entirely new ones.

Based on Table 3 of the risk classification, it is possible to propose a conceptual model for assessing the level of economic security of modern enterprises during the development of investment projects, which is presented in Fig. 2.

To determine the weight of each indicator, it is suggested to use the method of expert evaluations based on the analysis of the importance of the indicator. The integral indicator should include all factors that significantly affect the state of economic security of the enterprise during the preparation of the investment plan, that is, all business processes taking place in it. At the same time, one should avoid overloading, as too many indicators complicate the evaluation process.

For EU governing bodies, transparency is an important investment indicator. Transparency can be interpreted as both an ability and an outcome. It is proposed to define transparency as a component of economic security in terms of capabilities, as the ability to represent the enterprise in the digital space with data sets that can be processed, updated in real time, thus supporting the planning, monitoring and control of the investment program.

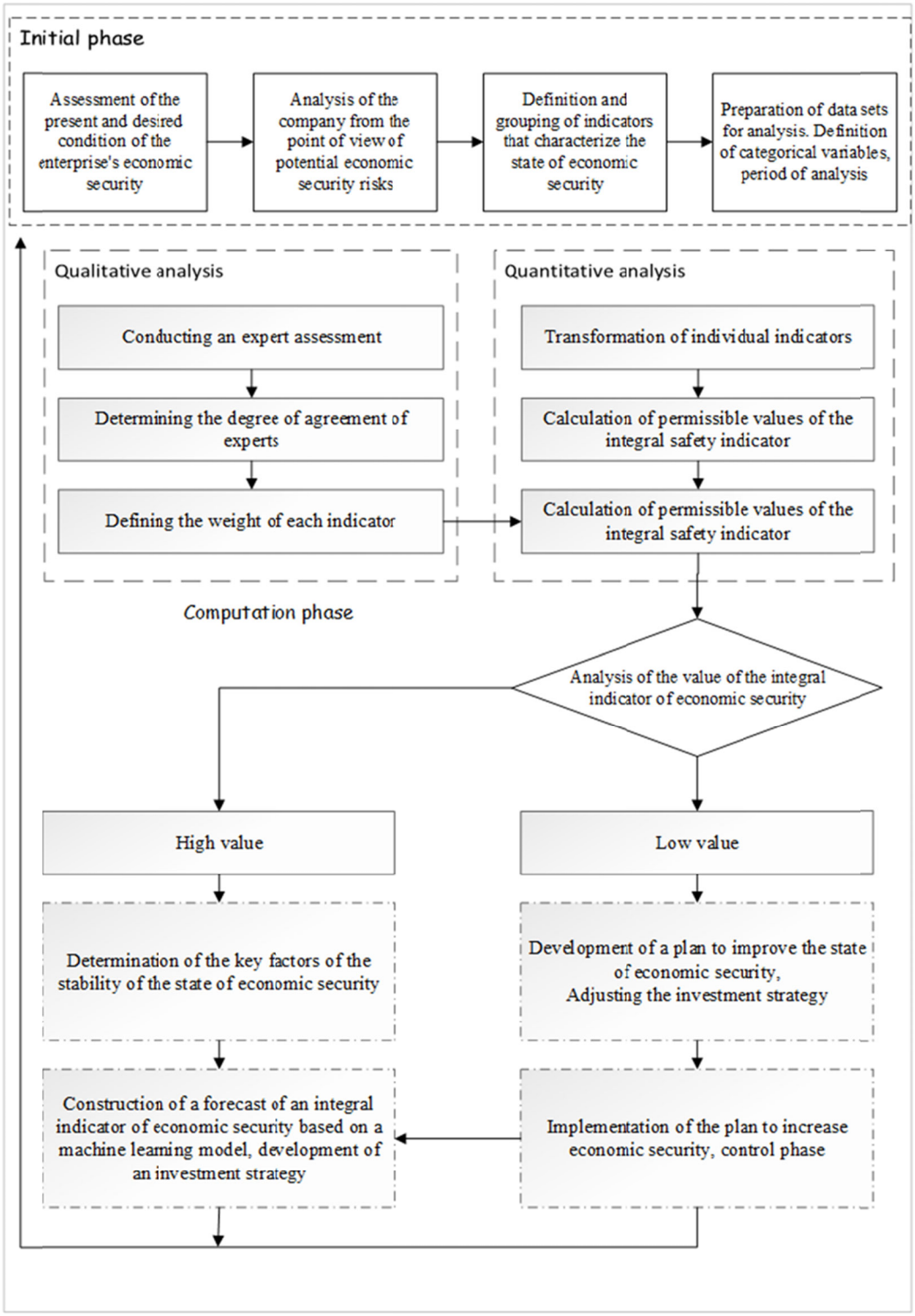

Figure 2. A conceptual model for assessing the level of economic security for the construction of investment strategies.

Source: developed by the authors.

Table 3 represents the indicators used in the proposed evaluation method, according to the type of response to the threats they characterize.

Table 3. Systematization of key indicators of economic security by type.

Threat type	The name of the coefficient	Marking	Target value
Technological threats	Charge of new production facilities	*Lf*	100%
Investment threats	Investment efficiency	*Ie*	≥ 90%
	Implementation of projects, commissioning	*Ip*	≥ 90%
Digital threats	Increasing labour productivity	*Lp*	≥ 5%
	Implementation of additional services	*As*	100%
Economic threats	Profit from the sale of products and services	*Pr*	100%
	Reduction of operating costs	*Loc*	≥0 %
	Transparency of information	*Ti*	≥ 90%

Thus, the calculation of the integral indicator of the assessment of the economic security state will have the following form:

$$E=b_1 \cdot Lf+b_2 \cdot Ie+b_3 \cdot Ip+b_4 \cdot Lp+b_5 \cdot As+b_6 \cdot Pr+b_7 \cdot Loc+b_8 \cdot Ti$$

Where, *bi* is the weight coefficient of indicators of economic security.

To analyse the results and determine the weighting factors, the ranking method is used, in which the expert expresses his opinion about the importance of each indicator. A rank equal to one has the least value for an expert. The most significant indicator corresponds to rank m, and then rank (m-1). A rank equal to one has the least value for an expert.

If there are *i*-th indicators, then as a result of their ranking by the *j*-th expert, each object receives a score $b_{ij,}$ which is the weight assigned to the *i*-th indicator by the *j*-th expert. In this case, the values *i* of b_{ij} are in the range from 1 to n, where n = 8 (Table 4). The ranking of the *j*-th expert is called the sequence of ranks b_{1j}, b_{2j}, …, b_{nj}.

The specific weight of the assessment of each indicator by a separate expert in their total sum is calculated by dividing the assessment of each indicator by 36. The total specific weight (*B*) of each *i*-th indicator is thus calculated according to the following formula:

$$B_i = \sum b_i \quad (2)$$

Table 4. The structure of the questionnaire of experts for determining the weighting factors.

№	The name of the coefficient	Point assessment
1	Charge of new production facilities	1-8
2	Investment efficiency	1-8
3	Implementation of projects, commissioning	1-8
4	Increasing of labour productivity	1-8
5	Implementation of additional services	1-8
6	Profit from the sale of products and services	1-8
7	Reduction of operating costs	1-8
8	Transparency of information	1-8

The total specific weight of the *i-th* indicator is calculated (*Bi*) by the ratio of the indicator to the sum of all indicators ($\sum b_i$). It is also necessary to establish the level of consistency of experts' opinions.

The calculation includes several steps:

1. A consolidated set of expert assessments is filled in.
2. The arithmetic mean of the sum of ranks is calculated by dividing the sum of ranks for each indicator by the number of coefficients.
3. The deviation of the sum of ranks of each coefficient of the average arithmetic sum of ranks is calculated.
4. The deviations of the sum of the ranks of each squared coefficient are summed up, and the obtained values (V) are summed up.

The concordance coefficient ranges from 0 to 1, where 1 is the absolute unanimity of experts, and 0 is a complete lack of agreement (Gearhart et al., 2013). The model for assessing economic security can be enriched with data from physical sources (indicators from the company's ERP system) and cyber source.

The Python program code for calculating the integral indicator of the assessment of the economic security state and its prediction using a machine learning and visualization model can look like this:

```
import pandas as pd
import seaborn as sns
import matplotlib.pyplot as plt
from sklearn.linear_model import
LinearRegression

# Calculating Integral Indicators

# Input data - Replace this with
your actual data
data = {
    'Period': [1, 2, 3, 4, 5],
    'Lf': [95, 98, 97, 100, 96],
    'Ie': [92, 91, 93, 89, 94],
    'Ip': [91, 88, 92, 95, 93],
    'Lp': [6, 5, 7, 4, 6],
    'As': [105, 98, 110, 105, 100],
    'Pr': [102, 98, 105, 110, 108],
    'Loc': [2, 1, 0, 2, 1],
    'Ti': [92, 91, 94, 89, 93]
       }

df = pd.DataFrame(data)
# Weight coefficients
b = [0.11, 0.14, 0.14, 0.09, 0.05,
0.06, 0.13, 0.12]

# Calculate integral indicators
df['E'] = df.apply(lambda row:
sum(row[key] * weight for key,
weight in zip(['Lf', 'Ie', 'Ip',
'Lp', 'As', 'Pr', 'Loc', 'Ti'], b)),
axis=1)
print(df[['Period', 'E']])
# Predicting Changes using Linear
Regression and Visualizing with
Seaborn and Matplotlib

# Prepare data for linear regression
X = df[['Period']]
y = df['E']
# Create linear regression model
model = LinearRegression()
model.fit(X, y)
# Predict future periods
future_periods = [6, 7, 8]
future_X = pd.DataFrame({'Period':
future_periods})
future_predictions =
model.predict(future_X)

# Visualize the results using
Seaborn and Matplotlib
sns.set(style="whitegrid")
plt.figure(figsize=(10, 6))
# Plot actual data
sns.scatterplot(x='Period', y='E',
data=df, label='Actual Data')

# Plot linear regression prediction
sns.lineplot(x=future_periods,
y=future_predictions, label='Linear
Regression Prediction', color='red')
plt.xlabel('Period')
plt.ylabel('Economic Security
Indicator')
plt.title('Economic Security
Indicator with Linear Regression
Prediction')
plt.legend()
plt.show()
```

As a result of testing the program on the test data set of "enterprise X", the calculation of the integral indicator of the economic security state was obtained, which is given in Table 5.

Table 5. Calculation of the integral indicator of the economic security state of "enterprise X" for a period of five months.

Period	E (integral indicator for assessing the state of economic security)
January	59.28
February	58.12
March	60.28
April	59.91
May	60.05

The result of state forecasting using a machine learning model is shown in Figure 3. This methodology for assessing the state of economic security can be transformed by replacing the key security indicators used with those adapted to a specific company.

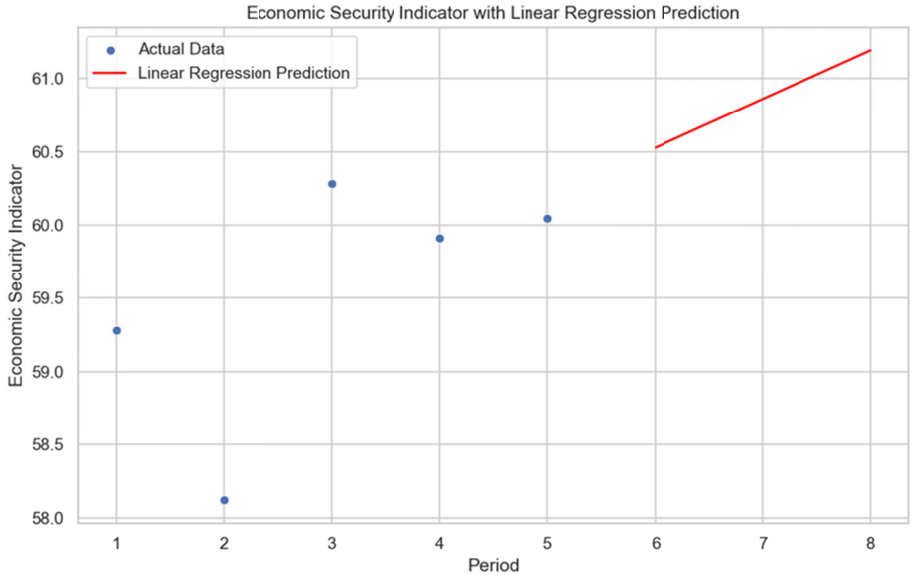

Figure 3. Forecast of the economic security state of "enterprise X" for a period of three months, obtained using a linear regression model.

5. Conclusions.

The aim of this study was to investigate the problems and develop recommendations for assessing the level of economic security in the development of investment projects to be better prepared for future post-war reconstruction projects in Ukraine. The developed conceptual model for assessing the level of economic security contains some innovative ideas regarding the systematization of critical indicators of economic security and the organization of ensuring end-to-end transparency of information during the implementation of investment projects for the restoration of Ukraine based on the use of intelligent technologies, which takes into account the processes of digital transformation of enterprises.

Software was also proposed for calculating the integral indicator of an enterprise's economic security and its forecasting using machine learning models. Calculating a new complex metric obtained from a combination of organizational, economic, managerial, financial, technical, and technological coefficients allows us to identify the key performance indicators for a modern company.

It also makes it possible to determine the main criteria characterizing the state and further prospects of its development, ensuring the stability of the economic subgroup under natural conditions.

In particular, indicators of economic security include end-to-end transparency of information, which can improve investment management and help enterprises carry out investment projects during wartime.

It is important to emphasize that a company's economic security is a complicated and complex economic concept that requires studying the impact of many different external and internal factors. Therefore, the developed methodology for assessing the state of economic security should cover all current business processes, investment plans, and risks that arise of enterprises' digital transformation, influencing the choice of critical indicators.

The post-war reconstruction of Ukraine is possible based on the modernization of the economy by increasing the security of the business environment (reducing corruption, ensuring private property rights, and strengthening the security of business activities) as well as transition to a digital society.

REFERENCES

Boston Consulting Group. (2023). Reaching New Heights in Uncertain Times. Most Innovative Companies 2023. https://www.bcg.com

Cabinet of Ministers of Ukraine. (2022). Ukraine Recovery Plan. https://recovery.gov.ua

Freedman, L., & Williams, H. (2023). Changing the Narrative: Information Campaigns, Strategy and Crisis Escalation in the Digital Age.

Gearhart, A., Booth, D. T., Sedivec, K., & Schauer, C. (2013). Use of Kendall's coefficient of concordance to assess agreement among observers of very high resolution imagery. Geocarto International, 28(6), 517–526. https://doi.org/10.1080/10106049.2012.725775

Hrynkevych, O., Bunyak, V., Kvak, S., & Hrynkevych, V. (2023). Investments in the system of social and economic security factors and recovery of the Ukraine region economies. Visnyk of the Lviv University. Series Economics, 64, 19–32. http://dx.doi.org/10.30970/ves.2023.64.0.6406

Koval, V., Kaminskyi, O., Brednyova, V., & Kosharska, L. (2022). Digital Ecosystem Model of Labour Resources Management in Economic Militarism. Revista Gestion de las Personas y Tecnologia,, 15(45), 21. https://doi.org/10.35588/gpt.v14i45.5902

Marquez-Tejon, J., Jimenez-Partearroyo, M., Benito-Osorio, D. (2022). Security as a key contributor to organisational resilience: a bibliometric analysis of enterprise security risk management. SecurJ35, 600–627 https://doi.org/10.1057/s41284-021-00292-4

Marton, P. (2023). Economic Security. In The Palgrave Encyclopedia of Global Security Studies (pp. 366–371). Springer International Publishing.

MinfinMedia. (2023). Foreign direct investment. https://index.minfin.com.ua/ua/economy/fdi

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

Moore, R. J. (2021). Emerging from war: Public policy and patterns of foreign direct investment recovery in postwar environments. Journal of International Business Policy, 4(4), 455–475. https://doi.org/10.1057/s42214-020-00084-4

OECD. (2022). Digitalisation for recovery in Ukraine. https://www.oecd.org/ukraine-hub/policy-responses/digitalisation-for-recovery-in-ukraine-c5477864.

OECD. (2011) Guide to Measuring the Information Society 2011, OECD, Paris.

Peng, Y., & Tao, C. (2022). Can digital transformation promote enterprise performance?—From the perspective of public policy and innovation. Journal of Innovation & Knowledge, 7(3), 100198. https://doi.org/10.1016/j.jik.2022.100198

Pravdyvets, O. (2022) Economic security as the supreme function of the state. Scientific Notes of the University "KROK", 2(66), 40–43. https://doi.org/10.31732/2663-2209-2022-66-40-43

Redkva, O., Koval, V., Filipishyna, L., Vuychenko, M. (2022) Model of ensuring economic security in mechanical engineering. Access to Science, Business, Innovation in Digital Economy, 3(3), 264-277. https://doi.org/10.46656/access.2022.3.3(6)

Romanovska, Y., Kozachenko, G., Pogorelov, Y., Pomazun, O., & Redko, K. (2022). Problems of development of economic security in Ukraine: Challenges and opportunities. Financial and Credit Activity Problems of Theory and Practice, 5(46), 249–257. https://doi.org/10.55643/fcaptp.5.46.2022.3906

Schwertner, K. (2017). Digital transformation of business. Trakia Journal of Sciences, 15(1), 388-393.

USAID. (2023). A new Ukraine: catalyzing investment in freedom, peace, and prosperity. The USAID Economic Development, Governance and Enterprise Growth (EDGE) Project.

Virlics, A. (2013). Investment decision making and risk. Procedia Economics and Finance, 6, 169–177. https://doi.org/10.1016/s2212-5671(13)00129-9