



International periodic scientific journal

—*ONLINE*

www.moderntechno.de



Indexed in
INDEXCOPERNICUS
(ICV: 70.62)

MODERN ENGINEERING AND INNOVATIVE TECHNOLOGIES

Issue №43
Part 3
February 2026

Published by:
Sergeieva&Co
Karlsruhe, Germany

Editor: Shibaev Alexander Grigoryevich, *Doctor of Technical Sciences, Professor, Academician*
Scientific Secretary: Kuprienko Sergey, *PhD in technical sciences*

Editorial board: More than 450 doctors of science. Full list on page:
<https://www.moderntechno.de/index.php/swj/about/editorialTeam>

Expert Board of the journal: Full list on page:
<https://www.moderntechno.de/index.php/swj/expertteam>

The International Scientific Periodical Journal "**Modern engineering and innovative technologies**" has been published since 2017 and has gained considerable recognition among domestic and foreign researchers and scholars.

Periodicity of publication: 6 times a year

The journal activity is driven by the following objectives:

- Broadcasting young researchers and scholars outcomes to wide scientific audience
- Fostering knowledge exchange in scientific community
- Promotion of the unification in scientific approach
- Creation of basis for innovation and new scientific approaches as well as discoveries in unknown domains

The journal purposefully acquaints the reader with the original research of authors in various fields of science, the best examples of scientific journalism.

Publications of the journal are intended for a wide readership - all those who love science. The materials published in the journal reflect current problems and affect the interests of the entire public.

Each article in the journal includes general information in English.

The journal is registered in IndexCopernicus, GoogleScholar.

DOI: 10.30890/2567-5273.2026-43-03

Published by:
Sergeieva&Co
Lußstr. 13
76227 Karlsruhe, Germany
e-mail: editor@moderntechno.de
site: www.moderntechno.de



УДК 005.334:004.056:658.012.4

INFORMATION SECURITY AS AN OBJECT OF RISK-ORIENTED MANAGEMENT OF SUSTAINABLE BUSINESS IN THE DIGITAL ENVIRONMENT

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОБ'ЄКТ РИЗИК-ОРІЄНТОВАНОГО МЕНЕДЖМЕНТУ СТАЛОГО БІЗНЕСУ В ЦИФРОВОМУ СЕРЕДОВИЩІ

Yurchuk N.P. / Юрчук Н.П.

PhD in Economic, assistant-prof. / к. е. н, доцент,

ORCID: 0000-0002-7987-9390

Vinnytsia National Technical University, Vinnytsia, Khmelnytske shose, 95, 21021

Вінницький національний технічний університет, Вінниця, Хмельницьке шосе, 95, 21021

Abstract. The article substantiates the conceptual foundations of risk-oriented information security management as a strategic tool for sustainable business development. It demonstrates the transformation of IS from a technical function into an economic category that determines the cyber resilience and competitiveness of enterprises in the digital economy.

The aim of the work is to develop a model for integrating cyber risk management into the ESG (Environmental, Social, Governance) parameters system. Methods of system analysis, modelling and graphical interpretation are applied.

The study systematises the main information security risks of digital business and demonstrates their impact on economic stability, business continuity and reputation capital. The interconnection between information security and ESG components is established, and the role of cybersecurity in strengthening corporate governance and building digital trust is substantiated. The main result is the development of an author's conceptual model for integrating risk-oriented information security management into the system of sustainable development of an enterprise.

It is concluded that the implementation of a risk-oriented approach increases the cyber resilience of organisations and contributes to the formation of long-term competitive advantages in the digital economy.

Keywords: information security; risk-oriented management; sustainable business; digitalization; ESG; cyber risks; cyber resilience.

Introduction.

In the context of pervasive digitalization (AI, Big Data, Cloud), information security (IS) is becoming a key management issue. The implementation of Business Intelligence tools is becoming a critical factor for sustainability in conditions of high uncertainty and risk [1]. Along with increased efficiency, digital transformation generates threats of data leaks and cyberattacks that threaten the long-term stability of enterprises [2].

The relevance of information security management is driven by its impact on business process continuity, stakeholder trust and reputation [3]. The application of a



risk-oriented approach is a prerequisite not only for technical protection, but also for the socio-economic stability of an organisation [4]. Unlike traditional models, this approach is based on a systematic analysis of dynamic cyber threats and vulnerabilities, ensuring the integration of information security into a sustainable development strategy [2].

Modern models of integrated risk management allow for the simultaneous improvement of cyber resilience and the maintenance of environmental and social responsibility in business [5]. In a competitive environment, information security acquires strategic status: reliable protection of information assets builds digital trust among investors and partners, ensuring long-term market advantages [3]. Therefore, considering information security as a fundamental element of sustainable business management is of great scientific and practical importance.

In the context of global competition, information security is becoming strategically important, as effective risk management not only protects assets but also builds digital trust among stakeholders, which is the foundation of long-term competitive advantage [3]. The recognition of IS as a fundamental element of management capable of ensuring business continuity in the era of digital transformation determines the scientific and practical significance of this study.

The theoretical aspects of risk-oriented digitalization and its impact on the economic security of enterprises and ecosystems have been studied in the works of Stefani E., Costa I., Gaspar M. A., Goes R. d. S., Monteiro R. C., Petrili B. R., Pereira, A. d. P. [6], Ivanov M., Martseniuk L., Angelova M., Faifer S. [5] and Hniedzovskyi O., Domashenko D., Domashenko S., Morozov D., Shylo, S. [4]. The issue of integrating information security into the ESG paradigm and sustainable development of the digital economy is discussed in the works of Li F., Zhang Z. [2], Zhang M., Huang Z. [7] and Shepel T. [12], which focus on transparency of reporting and sustainability of supply chains.

The industry-specific aspects of cyber security, particularly in the financial sector, public finance and the SME sector, are discussed by Bilyavska Yu., Bilyavsky V., Shestak Ya., Dieva N., Kolesnik M., Tryvailo A. [10], Kachula S. [11], Lusiah L.,



Parulian E. [3], Djajasinga N. D., Fatmawati E., Syamsuddin S., Sukomardojo T., Sulistyono A. B. [8], Yurchuk N., Kiporenko S. [1].

Despite the existence of substantial research, the mechanism of direct convergence of information security tools with sustainable business management practices requires additional study, which determined the choice of the research topic.

The purpose of the article is to theoretically substantiate and develop the conceptual foundations of risk-oriented information security management as a strategic tool for ensuring sustainable business development, to reveal the mechanisms of integrating cyber resilience into the ESG (Environmental, Social, Governance) parameters of organisations operating in the digital environment.

Main text.

In today's digital environment, information security has evolved from a purely technical issue into a critical economic and managerial concern, significantly affecting the functioning of organisations and their long-term sustainability. The concept of information security as a system of measures aimed at protecting the data and information assets of an enterprise from external and internal threats encompasses not only ensuring the confidentiality and integrity of information, but also the organisational level of protection that ensures the continuity of business processes and minimises economic losses in the event of cyberattacks or information leaks [6], [7].

Information security is particularly important in a sustainable business environment, as digital technologies and information systems are integrated into all areas of modern companies' activities. The existence of effective mechanisms for protecting digital assets and information security risk management systems contributes to economic stability and business continuity, ensuring the organisation's ability to adapt to external threats while maintaining operational efficiency and reputation in the market [8], [9]. In particular, studies show that reliable information security systems can significantly reduce the risks associated with the costs of recovery from cyberattacks, ensuring the long-term stability of enterprises and increasing their ability to withstand external and internal risks [10].

In addition, contemporary academic literature increasingly focuses on the



relationship between information security and ESG (Environmental, Social, Governance) components, which form the basis of the concept of sustainable business development. Information security is becoming an integral part of corporate governance practices and is seen as a key element in building stakeholder trust and increasing the transparency of companies' activities. Such approaches involve the inclusion of cyber risk management methods in overall sustainable development strategies, which allows companies not only to minimise the negative consequences of digital threats, but also to strengthen their social and managerial responsibility in the long term [11], [12]. Details of the impact of specific information security risks on the relevant ESG components are provided in Table 1.

Table 1 - The impact of information security risks on the components of sustainable business development

ESG components	Information security risks	Implications for sustainable development
Governance	Leakage of confidential reports, data manipulation	Loss of licences, fines, decline in investment attractiveness
Social	General Data Protection Regulation, cyberbullying	Reputation crisis, lawsuits from customers, loss of loyalty
Environmental	Cyberattacks on critical infrastructure (IoT, Smart Grid)	Technogenic accidents, environmental disasters, irrational use of resources

Source: systematised and summarised by the author

Thus, the management aspect of information security in a sustainable business system covers not only technical and operational measures to protect digital infrastructure, but also the strategic integration of information security into corporate governance processes, ESG risk assessment, and ensuring the long-term sustainability of business models in the digital economy. The conceptual architecture of such integration is shown in Fig. 1.

In particular, a deterministic link has been established between asset identification and the formation of digital trust (S-component), as well as between vulnerability monitoring and overall corporate transparency (G-component). This approach ensures not only operational data protection, but also long-term cyber resilience for the organisation in a volatile digital environment.

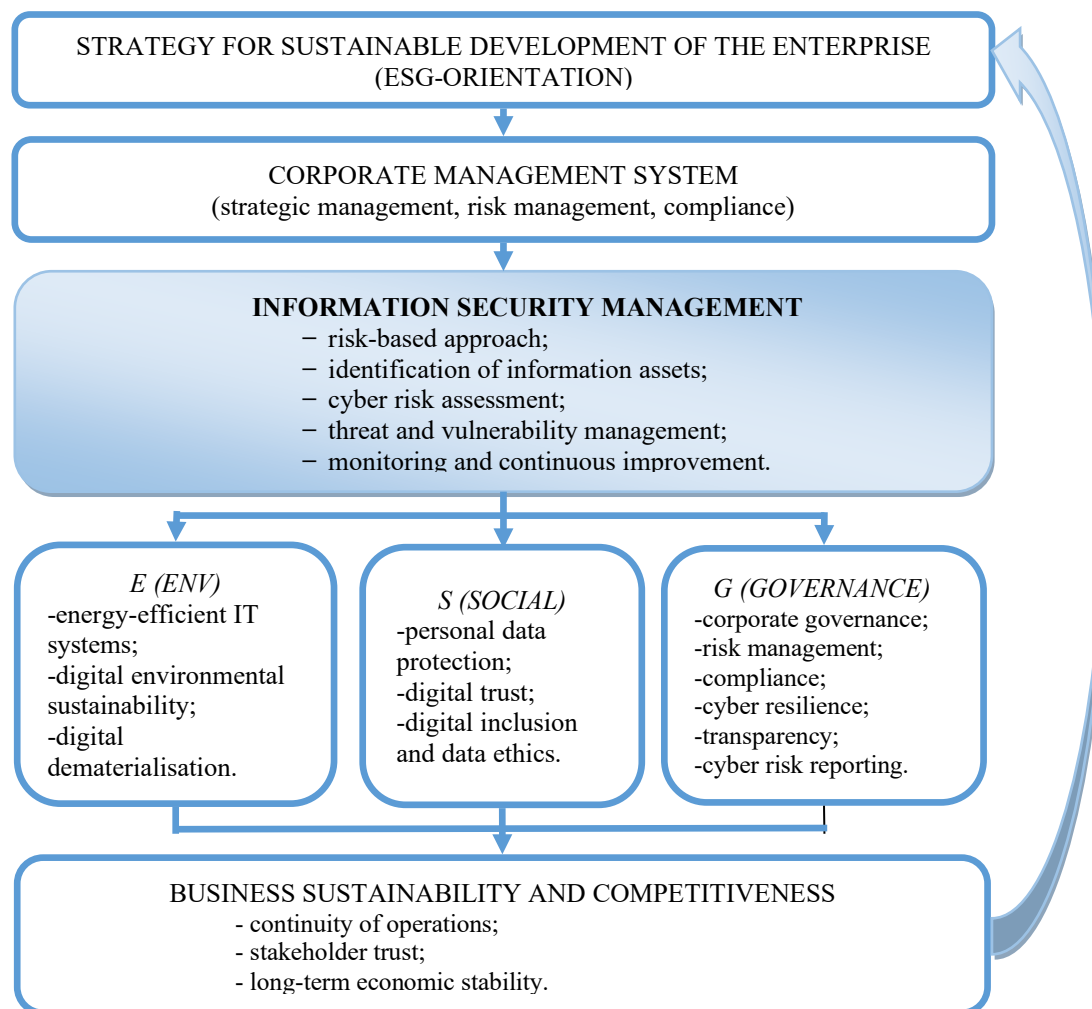


Рисунок 1 - Концептуальна модель інтеграції інформаційної безпеки в систему сталого розвитку підприємства (ESG-підхід)

Джерело: розроблено автором

Conclusions.

The study substantiates that, in the context of digital transformation, information security is becoming a strategic object of risk-oriented management of sustainable business. It has been established that the growth in the use of digital technologies is accompanied by an increase in cyber risks, which directly affect the continuity of business processes, reputation and stakeholder trust. The feasibility of integrating information security management into the ESG system has been proven, where it plays a key role in the Governance component and has an intercomponent impact on social and environmental sustainability. The proposed conceptual model of risk-oriented management ensures the coordination of strategic, process and effective management



decisions in the digital environment. The findings confirm that systematic cyber risk management contributes to the formation of digital trust, increased corporate transparency and long-term cyber resilience of organisations. Overall, information security is defined as a tool for ensuring business competitiveness in the volatile digital economy.

Prospects for further research lie in the development of quantitative indicators for assessing the effectiveness of investments in digital sustainability within the framework of non-financial reporting by enterprises.

References:

1. Yurchuk, N. P. and Kiporenko, S. S. (2025) 'Integration of Business Intelligence into digital management as a factor of sustainable enterprise development', *Investytsiyyi: praktyka ta dosvid*, (21), pp. 190–198. <https://doi.org/10.32702/2306-6814.2025.21.190>.
2. Li, F. and Zhang, Z. (2025) 'Addressing the sustainability challenges: Digital economy information security risk assessment', *Sustainability*, 17(14), pp. 6428. <https://doi.org/10.3390/su17146428>
3. Lusiaha, L. and Parulian, E. (2025) 'Securing sustainable digitalization: An integrative study on data privacy, cybersecurity, and business continuity in SMEs', *Golden Ratio of Mapping Idea and Literature Format*, 5(2), pp. 72–82. <https://doi.org/10.52970/grmilf.v5i2.1475>
4. Hniezdovskyi, O., Domashenko, D., Domashenko, S., Morozov, D. and Shylo, S. (2025) 'Digital solutions for risk management in sustainable development conditions of business ecosystems', *Applied Computer Science*, 21, pp. 51–62. https://doi.org/10.35784/acs_6935
5. Ivanov, M., Martseniuk, L., Angelova, M. and Faifer, S. (2025) 'Strategic risk management of digital transformation in the economic security of industrial enterprises', *Economics, Ecology, Socium*, 9(2), pp. 124–141. <https://doi.org/10.61954/2616-7107/2025.9.2-9>
6. Stefani, E., Costa, I., Gaspar, M. A., Goes, R. d. S., Monteiro, R. C., Petrili, B.



R. and Pereira, A. d. P. (2025) 'Information security risk framework for digital transformation technologies', *Systems*, 13(1), pp. 37. <https://doi.org/10.3390/systems13010037>

7. Zhang, M. and Huang, Z. (2024) 'The impact of digital transformation on ESG performance: The role of supply chain resilience', *Sustainability*, 16(17), pp. 7621. <https://doi.org/10.3390/su16177621>

8. Djajasinga, N. D., Fatmawati, E., Syamsuddin, S., Sukomardojo, T. and Sulisty, A. B. (2023) 'Risk management in the digital era addressing cybersecurity challenges in business', *Branding: Jurnal Manajemen Dan Bisnis*, 2(2). <https://doi.org/10.15575/jb.v2i2.31919>

9. Lehominova, S. and Prymachenko, D. (2025) 'The role of risk management in increasing organizational cyber resilience under hybrid threats', *Cybersecurity: Education, Science, Technique*, 3(31), pp. 792–800. <https://doi.org/10.28925/2663-4023.2025.31.1060>

10. Biliavska, Yu., Biliavskyi, V., Shestak, Ya., Dieieva, N., Kolesnyk, M. and Tryvailo, A. (2025) 'Monitoring of cyber risks in the financial sector of the economy', *Financial and Credit Activity: Problems of Theory and Practice*, 3(62), pp. 355–369. <https://doi.org/10.55643/fcaptp.3.62.2025.4702>

11. Kachula, S. (2025) 'Cybersecurity in the sphere of public finance', *Economy and Society*, (77). <https://doi.org/10.32782/2524-0072/2025-77-69>

12. Shepel, T. (2025) 'Sustainable development through the prism of risks: The role of risk-oriented management and integrated reporting', *Sustainable Development of the Economy*, 6(57), pp. 164–173. <https://doi.org/10.32782/2308-1988/2025-57-22>

Статтю надіслано: 10.02.2026 р.

© Yurchuk N.P.

**CONTENTS****Innovative economics and management**

http://www.moderntechno.de/index.php/meit/article/view/meit43-03-001	3
MANAGEMENT OF ECONOMIC RISKS OF CORPORATE INTEGRATION OF JOINT-STOCK COMPANIES THROUGH BUSINESS ETHICS AND CORPORATE CULTURE <i>Pitel N/, Riabovolyk T/</i>	
http://www.moderntechno.de/index.php/meit/article/view/meit43-03-014	15
STRATEGY OF RESOURCE POTENTIAL FORMATION AS A BASIS FOR ENTERPRISE COMPETITIVENESS <i>Harvat O. A.</i>	
http://www.moderntechno.de/index.php/meit/article/view/meit43-03-016	30
CURRENT TRENDS IN THE DEVELOPMENT OF NEOBANKS IN UKRAINE <i>Adonin S.V., Pashchenko O.V.</i>	
http://www.moderntechno.de/index.php/meit/article/view/meit43-03-019	41
ANALYSIS OF CONSUMER BEHAVIOR IN SOCIAL NETWORKS <i>Trishkina N/</i>	
http://www.moderntechno.de/index.php/meit/article/view/meit43-03-022	53
IMPLEMENTATION OF NEW TYPES OF DIPLOMACY IN THE SPHERE OF FOREIGN RELATIONS <i>Karpov V.V.</i>	
http://www.moderntechno.de/index.php/meit/article/view/meit43-03-024	66
INFORMATION SECURITY AS AN OBJECT OF RISK-ORIENTED MANAGEMENT OF SUSTAINABLE BUSINESS IN THE DIGITAL ENVIRONMENT <i>Yurchuk N.P.</i>	
http://www.moderntechno.de/index.php/meit/article/view/meit43-03-033	73
FORMATION OF A DIGITAL MODEL OF TAX ADMINISTRATION IN UKRAINE <i>Leha O.V., Pryydak T.B., Yaloveha L.V.</i>	
http://www.moderntechno.de/index.php/meit/article/view/meit43-03-034	85
ECONOMIC ESSENCE AND THEORETICAL BASIS OF COWORKING ACCOUNTING <i>Borovych O.V., Tymots M.V.</i>	



International periodic scientific journal

MODERN ENGINEERING AND INNOVATIVE TECHNOLOGIES

Heutiges Ingenieurwesen und
innovative Technologien

Indexed in
INDEXCOPERNICUS
high impact factor (ICV: 70.62)

Issue №43
Part 3
February 2026

Development of the original layout - Sergeieva&Co

Signed: February 28, 2026

Sergeieva&Co
Lußstr. 13
76227 Karlsruhe
e-mail: editor@moderntechno.de
site: www.moderntechno.de

Articles published in the author's edition

