UDC 339.9:004.056

Matkobozhyk Serhii
PhD Student of the Department of Entrepreneurship, Trade and Tourism Business
Simon Kuznets Kharkiv National University of Economics
ORCID: 0009-0004-9033-5599

Lytvynenko Alina
Candidate of Economic Sciences, Associate Professor of the Department of Entrepreneurship, Trade and Tourism Business
Simon Kuznets Kharkiv National University of Economics
ORCID: 0000-0003-0372-5130

https://doi.org/10.25313/3083-7782-2026-5-96

CYBERSECURITY AS A STRATEGIC PRIORITY FOR INTERNATIONAL DIGITAL BUSINESS MANAGEMENT

Summary. *Introduction. The rapid digitalisation of international entrepreneurship has transformed cybersecurity from a purely technical function into a core strategic priority for cross-border enterprises. Companies operating on digital platforms, cross-border e-commerce channels, and interconnected cloud infrastructures increasingly face cyber risks that generate simultaneous financial, legal, operational, and reputational consequences across several markets at once. As dependence on third-party digital infrastructure grows, a single cybersecurity incident can disrupt entire cross-border value chains and undermine customer trust built over years of international market presence.*

At the same time, the strategic management of international entrepreneurial entities has traditionally treated information security as a supporting or compliance-oriented function rather than a core component of strategy formation. This gap between the growing scale of cyber risk and the still-limited strategic attention devoted to cybersecurity creates a substantial vulnerability for companies seeking to expand internationally through digital channels.

The study systematises the main types and sources of cyber risk relevant to international digital business, assesses their economic scale on the basis of recent global statistics, and proposes a structured model for integrating cybersecurity risk management into the strategic management cycle of internationally operating entrepreneurial entities.

Purpose. The purpose of this study is to substantiate the strategic role of cybersecurity in the management of international digital business, to identify the key types and sources of cyber risk affecting entrepreneurial entities operating across borders, and to develop practical recommendations for integrating cybersecurity risk management into corporate strategy formation in the context of accelerating digitalisation.

Materials and methods. The study relies on a systematic analysis of scientific publications, international industry reports, and statistical data on cybersecurity incidents and their economic consequences for enterprises engaged in international entrepreneurship. Methods of comparative analysis, generalisation, and synthesis were used to examine the interconnection between cybersecurity risk management and strategic management, as well as to assess the scale, structure, and cost of cyber threats affecting cross-border digital operations. Particular attention was paid to the classification of digital risks by area of occurrence, regional and sectoral differences in the cost of data breaches, and the growing role of artificial intelligence in both cyberattacks and cyber defence.

Results. The study demonstrates that cybersecurity has evolved from a purely technical function into a core strategic priority of international business management. Enterprises operating on digital platforms and cross-border e-commerce channels face a growing diversity of cyber risks, including ransomware, phishing, DDoS attacks, supply-chain compromise, and AI-driven automated attacks, which directly affect their competitiveness, financial stability, and reputation in global markets. The analysis of recent statistical data confirms significant regional and sectoral variation in breach-related costs and shows that organisations formally integrating cybersecurity into strategic planning

demonstrate greater resilience and faster recovery. A generalised model of cybersecurity-oriented strategic management is proposed, encompassing prevention, detection, response, and resilience as interrelated stages of a continuous strategic cycle.

Discussion. Further research should focus on the industry-specific features of cybersecurity risk management for internationally operating small and medium-sized enterprises, the development of adaptive governance mechanisms for artificial-intelligence-related risks, and empirical assessment of the relationship between cybersecurity maturity and the long-term competitiveness of entrepreneurial entities in the global digital economy.

Key words: *cybersecurity, strategic management, international business, digital risk, risk management, international entrepreneurship.*

Statement of the problem. The accelerating integration of digital technologies into international entrepreneurship has fundamentally changed the risk landscape in which cross-border enterprises operate. Digital platforms, cloud infrastructure, cross-border payment systems, and data-driven decision-making tools now underpin virtually every stage of international business activity, from market entry to customer engagement and value chain coordination. While these technologies expand the strategic opportunities available to entrepreneurial entities, they simultaneously expose companies to a growing and increasingly sophisticated range of cyber threats that transcend national borders and regulatory jurisdictions.

Enterprises engaged in international e-commerce, platform-based business models, and cross-border digital operations face a distinctive combination of vulnerabilities: dependence on third-party digital infrastructure, exposure to multiple national legal regimes, large volumes of cross-border data flows, and continuous interaction with global customer bases through interconnected digital ecosystems. As a result, a single cybersecurity incident can generate simultaneous financial, legal, operational, and reputational consequences across several markets, making cybersecurity a matter of strategic rather than purely technical concern.

At the same time, the strategic management of international entrepreneurial entities has traditionally treated information security as a supporting or compliance-oriented function rather than as a core component of strategy formation. This gap between the growing scale of cyber risk and the still-limited strategic attention devoted to cybersecurity creates a substantial vulnerability for companies seeking to expand internationally through digital channels.

Therefore, the central problem addressed in this article lies in determining how cybersecurity risk management should be integrated into the strategic management of international digital business, identifying the main types and sources of cyber risk relevant to entrepreneurial entities, and substantiating approaches that allow companies to transform cybersecurity from a reactive cost centre into a proactive driver of competitiveness and resilience in global digital markets.

Analysis of recent researches and publications. The relationship between cybersecurity and strategic management has attracted growing attention from both Ukrainian and international researchers. Khalina O. and Shmahalo V. [1] examine the strategy for the development of enterprises' economic security under digital transformation, identifying risk management, qualified personnel, cybersecurity, digital infrastructure, artificial intelligence, and blockchain technologies as key components of an integrated security-oriented management mechanism. Plesiuk O. [2, p. 65] provides a detailed classification of digital risks — including phishing, ransomware, DDoS attacks, malware, cyber-interdependence, geopolitical risks, deepfakes, and cybercrime — and demonstrates that effective digital risk management is a critical element of strategic planning and functional management rather than an isolated technical task.

Buhrimenko R., Smirnova P., and Smokova L. [3, p. 23] analyse the place of digital security within the overall system of enterprise protection, emphasising the need to combine information security and cybersecurity measures to withstand the risks generated by digital transformation. Prokofieva O. and Bespalova Yu. [4] focus specifically on cyber risks arising under conditions of globalisation and digital transformation, highlighting the growing interdependence between global economic integration and exposure to cyber threats.

The strategic dimension of cybersecurity risk management has also been explored internationally. Mızrak F. [6, p. 98] provides a comprehensive literature review on the integration of cybersecurity risk management into strategic management, revealing a critical interdependence between the two fields and showing how organisations formulate proactive measures to align cyber risk mitigation with broader strategic objectives. Empirical evidence on the scale of the problem is provided by leading industry reports: IBM [7] documents the global costs of data breaches, Verizon [8] analyses the structure and dynamics of confirmed security incidents, and Imperva [9] examines the rapidly growing role of automated, artificial-intelligence-driven traffic in the modern threat landscape.

The present study also builds on previous research into the strategic role of digital platforms and e-commerce in international entrepreneurship [5], which identified cybersecurity risks, technological dependence, and regulatory compliance as key challenges of platform-based international business but did not examine them as an independent strategic priority. This gap forms the basis for the present, more focused analysis.

Despite this substantial body of research, the specific mechanisms through which cybersecurity risk management can be systematically embedded into the strategic management cycle of internationally operating entrepreneurial entities remain insufficiently developed, particularly with regard to the growing influence of artificial intelligence on both attack and defence capabilities. This gap justifies further research aimed at developing a structured approach to cybersecurity-oriented strategic management in international business.

Formulation purposes of article (problem). The purpose of this article is to substantiate the strategic significance of cybersecurity for the management of international digital business. The study aims to systematise the main types and sources of cyber risk affecting entrepreneurial entities operating in cross-border digital markets, to assess the economic scale of cybersecurity incidents based on recent statistical evidence, and to propose a generalised model for integrating cybersecurity risk management into the strategic management process of international entrepreneurship.

The main material. Cybersecurity in the international entrepreneurship context has evolved from a purely technical, compliance-driven function into one of the central pillars of strategic management. As companies deepen their reliance on digital platforms, cloud services, and cross-border data exchange, information security failures translate directly into strategic vulnerabilities: loss of market access, disruption of cross-border value chains, erosion of customer trust, and exposure to regulatory sanctions across multiple jurisdictions. The strategic significance of cybersecurity is therefore no longer confined to protecting technical infrastructure; it extends to safeguarding the continuity, reputation, and competitive positioning of the enterprise as a whole [1].

A necessary starting point for embedding cybersecurity into strategic management is a systematic understanding of the main types and sources of cyber risk faced by internationally operating entrepreneurial entities. These risks differ substantially in their origin, mechanism of impact, and strategic consequences, which requires a structured classification rather than a purely technical inventory of threats. Table 1 summarises the principal categories of cyber risk relevant to international digital business, together with their main strategic implications.

Table 1

Main Types of Cyber Risk in International Digital Business by Area of Occurrence

Area of occurrence	Main risk types	Strategic impact
Technical infrastructure	Ransomware, malware, DDoS attacks	Operational disruption, service downtime, ransom payments
Human and organisational factors	Phishing, social engineering, insider threats	Credential compromise, unauthorised access, data leakage
Supply chain and third parties	Compromise of vendor, logistics and platform systems	Cascading breaches across the value chain, loss of partner trust
Data protection and privacy	Unauthorised data collection, regulatory non-compliance	Legal liability, regulatory fines, reputational damage
Geopolitical and regulatory environment	Cross-border legal fragmentation, state-sponsored attacks	Market access restrictions, rising compliance costs
Emerging technology	AI-driven attacks, deepfakes, automated malicious bots	Fraud, brand impersonation, erosion of customer trust

Source: compiled by the authors on the basis of [2, p. 66; 3, p. 24; 4]

As illustrated in Table 1, cyber risk in international digital business is not limited to technical failures but spans organisational, contractual, regulatory, and technological dimensions. Technical infrastructure risks such as ransomware, malware, and distributed denial-of-service (DDoS) attacks directly disrupt operational continuity and, in cross-border digital platforms, can simultaneously affect customers and partners in multiple markets. Human and organisational risks, including phishing and social engineering, remain among the most common entry points for attackers, as they exploit employee behaviour rather than technical vulnerabilities alone [2, p. 67].

Supply-chain and third-party risks have become increasingly significant for internationally operating enterprises, which typically depend on a dense network of logistics providers, payment processors, cloud vendors, and platform operators located across different jurisdictions. A security failure at any point in this network can cascade through the entire value chain, undermining the resilience of otherwise well-protected core operations [3, p. 25]. This interdependence illustrates why cybersecurity cannot be managed solely at the level of an individual enterprise but must be addressed as part of a broader strategic approach to partner selection, contractual risk allocation, and continuous monitoring.

Data protection and regulatory risks add a further layer of complexity to international operations. Enterprises operating across borders must simultaneously comply with a fragmented and continuously evolving regulatory landscape, including data protection regulations such as the General Data Protection Regulation

(GDPR) in the European Union, sector-specific cybersecurity directives, and national cybersecurity strategies. Recent analytical reviews indicate that a new wave of mandatory regulatory frameworks — including the EU's NIS2 Directive, the Cyber Resilience Act (CRA), and the Digital Operational Resilience Act (DORA) — is transforming cybersecurity from a discretionary risk-management practice into an explicit corporate governance obligation with direct legal liability for company leadership [10]. For internationally active entrepreneurial entities, this means that cybersecurity strategy must be aligned not only with technical best practice but also with an increasingly demanding and jurisdiction-specific compliance environment.

The economic scale of these risks can be assessed through recent global statistics on the cost of cybersecurity incidents. Table 2 summarises the average global and industry-specific cost of a data breach, based on the most recent international benchmarking data.

Table 2

Global Average Cost of a Data Breach by Region and Industry, 2025

Region / industry	Average cost of a data breach, USD million
Global average	4.44
United States	10.22
Healthcare sector	7.42
Financial sector	5.56
Public sector	2.86
Additional cost where the breach involved shadow AI	+0.67

Source: compiled by the authors on the basis of [7]

The data presented in Table 2 confirm that the financial consequences of cybersecurity incidents vary substantially by region and industry, reflecting differences in regulatory penalties, the value of compromised data, and the maturity of incident response capabilities. Although the global average cost of a data breach decreased for the first time in five years, driven largely by faster containment enabled by artificial-intelligence-based defence tools, the United States and highly regulated industries such as healthcare and finance continue to bear substantially higher costs, underscoring the strategic importance of local regulatory context for internationally operating enterprises [7].

A particularly important trend affecting international digital business is the growing dual role of artificial intelligence in both attack and defence. On one hand, AI-based defence tools accelerate breach detection and containment, reducing the operational and financial impact of incidents [7]. On the other hand, cybercriminals increasingly use AI to design more sophisticated and evasive attacks. According to Verizon's most recent global analysis of confirmed security incidents, ransomware attacks rose sharply and were present in 44% of all analysed breaches, compared with 32% in the previous reporting period [8]. At the same time, automated web traffic — a substantial share of which is now driven by AI-based bots — has, for the first time, surpassed human activity, accounting for the majority of global web traffic, with malicious ("bad") bots representing more than a third of all internet traffic and increasingly targeting business logic, application programming interfaces (APIs), and customer-facing digital channels [9]. This trend is especially relevant for enterprises operating international e-commerce platforms and online marketplaces, where automated attacks can directly affect transaction integrity, customer experience, and brand trust [5].

The scale of potential disruption is illustrated by the global information-technology outage triggered by a faulty security-software update in July 2024, which caused an estimated 8.5 million Windows-based systems to fail simultaneously across multiple countries. Although the incident originated from a single vendor's software defect rather than a malicious cyberattack, its consequences illustrate the same strategic vulnerability created by technological dependence and supply-chain concentration described in Table 1: airlines cancelled several thousand flights worldwide, and industry estimates placed direct losses to Fortune 500 companies alone at approximately USD5.4 billion, with the banking and healthcare sectors among the hardest hit [11]. For internationally operating entrepreneurial entities, this episode demonstrates that resilience planning must extend beyond malicious cyber threats to encompass the broader category of technological dependency risk arising from reliance on a small number of globally dominant software and infrastructure providers.

This example also highlights a further strategic consideration for entrepreneurial entities operating across borders: legal and contractual exposure following a cyber or technological incident is rarely confined to a single jurisdiction. Affected companies pursued compensation through multiple national legal systems simultaneously, illustrating that cybersecurity governance must be coordinated not only with technical risk owners but also with legal, insurance, and investor-relations functions at the strategic level, particularly for enterprises with operations, customers, or listed shares in several countries [11].

These findings demonstrate that cybersecurity risk can no longer be treated as an isolated technical issue delegated entirely to information technology departments. Instead, it needs to be systematically integrated into the strategic management cycle of internationally operating entrepreneurial entities. Building on the theoretical foundations proposed in the literature on integrating cybersecurity risk management into strategic management [6, p. 102], this study proposes a generalised model comprising four interrelated stages, illustrated in Figure 1.

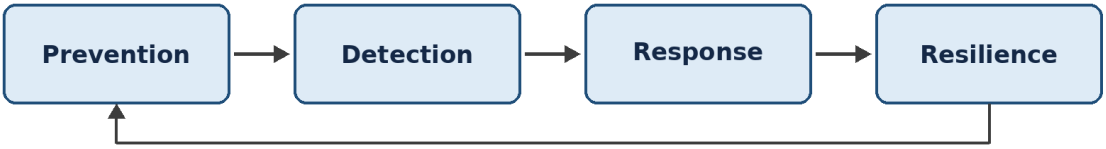

Fig. 1. Key stages of the cybersecurity-oriented strategic management cycle
Source: compiled by the authors on the basis of [1; 6, p. 102]

The first stage, prevention, involves the integration of cybersecurity considerations into strategic planning from the outset, including risk assessment during market entry decisions, vendor selection, and platform adoption, as well as investment in staff training and adherence to recognised international standards such as ISO/IEC 27001. The second stage, detection, requires continuous monitoring of digital infrastructure and transaction flows, increasingly supported by artificial-intelligence-based anomaly detection tools capable of identifying threats across multiple markets and time zones in real time.

The third stage, response, concerns the enterprise's capacity to react rapidly and in a coordinated manner to confirmed incidents, minimising operational disruption and limiting reputational and financial damage across all affected markets simultaneously. The fourth stage, resilience, reflects the enterprise's ability to learn from incidents, adapt its strategic priorities, and strengthen its long-term competitive position by demonstrating reliability and trustworthiness to international partners, regulators, and customers. Together, these four stages form a continuous cycle rather than a linear sequence, requiring periodic reassessment as both the regulatory environment and the technological threat landscape evolve.

For internationally active entrepreneurial entities — and particularly for small and medium-sized enterprises with limited dedicated cybersecurity resources — the practical implementation of this model requires several concrete strategic actions. These include allocating a defined share of the strategic budget to cybersecurity rather than treating it as a residual cost, establishing board-level accountability for cyber risk oversight, conducting regular scenario-based resilience testing that accounts for cross-border regulatory and operational dependencies, and embedding cybersecurity criteria into the selection and ongoing evaluation of foreign partners, platforms, and suppliers. Enterprises that adopt such a proactive and strategically embedded approach are better positioned to transform cybersecurity from a defensive cost centre into a genuine source of competitive differentiation, particularly in digital markets where customer trust is a decisive factor in long-term success [1; 4].

Conclusions of this research and prospects for further research in this area. This study confirms that cybersecurity has become a strategic priority rather than a purely technical concern for entrepreneurial entities operating in international digital markets. The systematisation of cyber risk by area of occurrence demonstrates that technical, organisational, supply-chain, regulatory, and technology-driven risks are deeply interconnected and require a coordinated strategic response rather than fragmented technical fixes. Recent global statistics confirm the substantial and unevenly distributed economic cost of cybersecurity incidents, as well as the accelerating dual role of artificial intelligence in both amplifying cyber threats and improving organisational defence capabilities.

The proposed model of cybersecurity-oriented strategic management, encompassing prevention, detection, response, and resilience, provides a structured framework for integrating cyber risk management into the strategic decision-making process of internationally operating enterprises. The analysis shows that companies which formally embed cybersecurity into strategic planning — through board-level oversight, dedicated budgets, staff training, and continuous monitoring — are better positioned to sustain competitiveness, regulatory compliance, and customer trust in global digital markets.

Further research may focus on the empirical assessment of cybersecurity maturity levels among internationally operating small and medium-sized enterprises, the development of adaptive governance mechanisms for managing artificial-intelligence-related cyber risks, and comparative analysis of regulatory approaches to cybersecurity across major international markets. Such research would further strengthen the theoretical and practical foundations for integrating cybersecurity into the strategic management of international entrepreneurship in the evolving global digital economy.

ДОДАТКОВА ІНФОРМАЦІЯ

ВНЕСОК АВТОРІВ: Усі автори зробили внесок порівну.
ФІНАНСУВАННЯ: Автори не отримували фінансування для цього дослідження.
ЗАЯВА ПРО ДОСТУПНІСТЬ ДАНИХ: Не застосовується.
КОНФЛІКТ ІНТЕРЕСІВ: Автори заявляють про відсутність конфлікту інтересів.

Література

1. Халіна О., Шмагало В. Стратегія розвитку економічної безпеки підприємств в умовах цифрових трансформацій. *Економіка та суспільство.* 2025. № 73. DOI: https://doi.org/10.32782/2524-0072/2025-73-138

2. Плесюк О.С. Цифрові ризики в управлінні розвитком підприємства. *Вісник Сумського національного аграрного університету. Серія: Економіка і менеджмент.* 2025. № 3 (103). С. 65–70. DOI: https://doi.org/10.32782/bsnau.2025.3.10

3. Бугріменко Р.М., Смірнова П.В., Смокова Л.О. Загрози та ризики цифрової трансформації підприємства. *Grail of Science.* 2024. № 38. С. 23–27. DOI: https://doi.org/10.36074/grail-of-science.12.04.2024.001

4. Прокоф'ева О. В., Беспалова Ю.Ю. Кібер-ризики та управління ними в умовах глобалізації та цифрової трансформації. *Ефективна економіка.* 2024. № 5. URL: http://nbuv.gov.ua/UJRN/efek_2024_5_89 (дата звернення: 01.04.2026).

5. Lytvynenko A., Matkobozhyk S. Digital platforms and e-commerce as strategic drivers of international entrepreneurship. *International scientific journal "Internauka". Series: "Economic Sciences".* 2026. № 1. DOI: https://doi.org/10.25313/2520-2294-2026-1-11859

6. Mızrak F. Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management.* 2023. Vol. 10, No. 3. P. 98–108. URL: https://dergipark.org.tr/en/pub/rjbm/article/1372698 (дата звернення: 01.04.2026).

7. Cost of a Data Breach Report 2025. *IBM.* 2025. URL: https://www.ibm.com/reports/data-breach (дата звернення: 01.04.2026).

8. 2025 Data Breach Investigations Report. *Verizon.* 2025. URL: https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf (дата звернення: 01.04.2026).

9. 2025 Bad Bot Report. *Imperva (a Thales company).* 2025. URL: https://www.imperva.com/resources/resource-library/reports/2025-bad-bot-report/ (дата звернення: 01.04.2026).

10. Глобальна індустрія кібербезпеки станом на 2026 рік: основні показники, тенденції та прогнози. *Національний інститут стратегічних досліджень.* 2026. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/hlobalna-industriya-kiberbezpeky-stanom-na-2026-rik-osnovni (дата звернення: 01.04.2026).

11. CrowdStrike disruption direct losses to reach $5.4B for Fortune 500, study finds. *Cybersecurity Dive.* 2024. URL: https://www.cybersecuritydive.com/news/crowdstrike-cost-fortune-500-losses-cyber-insurance/722396/ (дата звернення: 01.04.2026).

References

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

2. Plesiuk, O. S. (2025). Tsyfrovi ryzyky v upravlinni rozvytkom pidpryiemstva [Digital risks in business development management]. *Visnyk Sumskoho natsionalnoho ahrarnoho universytetu — Bulletin of Sumy National Agrarian University*, (3(103)), 65–70. https://doi.org/10.32782/bsnau.2025.3.10 [in Ukrainian].

3. Buhrimenko, R.M., Smirnova, P.V., & Smokova, L.O. (2024). Zahrozy ta ryzyky tsyfrovoi transformatsii pidpryiemstva [Threats and risks of digital transformation of the enterprise]. *Grail of Science*, (38), 23–27. https://doi.org/10.36074/grail-of-science.12.04.2024.001 [in Ukrainian].

4. Prokofieva, O.V., & Bespalova, Yu. Yu. (2024). Kiber-ryzyky ta upravlinnia nymy v umovakh hlobalizatsii ta tsyfrovoi transformatsii [Cyber risks and their management under globalization and digital transformation]. *Efektyvna ekonomika — Efficient Economy*, (5). http://nbuv.gov.ua/UJRN/efek_2024_5_89 [in Ukrainian].

5. Lytvynenko, A., & Matkobozhyk, S. (2026). Digital platforms and e-commerce as strategic drivers of international entrepreneurship. *International Scientific Journal "Internauka". Series: "Economic Sciences"*, (1). https://doi.org/10.25313/2520-2294-2026-1-11859

6. Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: A comprehensive literature review. *Research Journal of Business and Management, 10*(3), 98–108. https://dergipark.org.tr/en/pub/rjbm/article/1372698

7. IBM. (2025). *Cost of a data breach report 2025*. https://www.ibm.com/reports/data-breach

8. Verizon. (2025). *2025 data breach investigations report*. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

9. Imperva, a Thales company. (2025). *2025 bad bot report*. https://www.imperva.com/resources/resource-library/reports/2025-bad-bot-report/

10. National Institute for Strategic Studies. (2026). *Hlobalna industriia kiberbezpeky stanom na 2026 rik: osnovni pokaznyky, tendentsii ta prohnozy [The global cybersecurity industry as of 2026: Key indicators, trends and forecasts].* https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/hlobalna-industriya-kiberbezpeky-stanom-na-2026-rik-osnovni [in Ukrainian].

11. Cybersecurity Dive. (2024). *CrowdStrike disruption direct losses to reach $5.4B for Fortune 500, study finds*. https://www.cybersecuritydive.com/news/crowdstrike-cost-fortune-500-losses-cyber-insurance/722396/

Дата першого надходження статті до видання: 29.04.2026
Дата прийняття статті до друку після рецензування: 24.05.2026
Дата публікації: 31.05.2026

ISSN (Online): 3083-7782
Електронний науковий журнал «ЕКОНОМІЧНА ПАРАДИГМА»

Маткобожик Сергій Володимирович
аспірант кафедри підприємництва, торгівлі та туристичного бізнесу Харківського національного економічного університету імені Семена Кузнеця

Литвиненко Аліна Олександрівна
кандидат економічних наук, доцент кафедри підприємництва, торгівлі та туристичного бізнесу Харківський національний економічний університет імені Семена Кузнеця

КІБЕРБЕЗПЕКА ЯК СТРАТЕГІЧНИЙ ПРІОРИТЕТ УПРАВЛІННЯ ЦИФРОВИМ МІЖНАРОДНИМ БІЗНЕСОМ

Анотація. *Вступ. Швидка цифровізація міжнародного підприємництва перетворила кібербезпеку з виключно технічної функції на ключовий стратегічний пріоритет для транскордонних підприємств. Компанії, що функціонують на цифрових платформах, у каналах транскордонної електронної комерції та в умовах взаємопов'язаної хмарної інфраструктури, дедалі частіше стикаються з кіберризиками, які одночасно спричиняють фінансові, правові, операційні та репутаційні наслідки на кількох ринках. У міру зростання залежності від сторонньої цифрової інфраструктури один кіберінцидент здатний порушити цілі транскордонні ланцюги створення вартості та підірвати довіру клієнтів, сформовану роками присутності на міжнародному ринку.*

Водночас стратегічне управління суб'єктами міжнародної підприємницької діяльності традиційно розглядало інформаційну безпеку як допоміжну або комплаєнс-орієнтовану функцію, а не як невід'ємний компонент формування стратегії. Цей розрив між зростаючим масштабом кіберризиків і все ще обмеженою стратегічною увагою до кібербезпеки створює суттєву вразливість для компаній, що прагнуть міжнародної експансії через цифрові канали.

У дослідженні систематизовано основні види та джерела кіберризиків, релевантні для цифрового міжнародного бізнесу, оцінено їх економічний масштаб на основі актуальних глобальних статистичних даних, а також запропоновано структуровану модель інтеграції управління кіберризиками у стратегічний управлінський цикл суб'єктів міжнародної підприємницької діяльності.

Мета. Метою дослідження є обґрунтування стратегічної ролі кібербезпеки в управлінні цифровим міжнародним бізнесом, визначення основних видів і джерел кіберризиків, що впливають на суб'єктів підприємницької діяльності, які функціонують на міжнародних ринках, а також розроблення практичних рекомендацій щодо інтеграції управління кіберризиками у процес формування корпоративної стратегії в умовах прискореної цифровізації.

Матеріали і методи. Дослідження базується на систематичному аналізі наукових публікацій, міжнародних галузевих звітів та статистичних даних щодо кіберінцидентів і їхніх економічних наслідків для підприємств, які здійснюють міжнародну підприємницьку діяльність. Застосовано методи порівняльного аналізу, узагальнення та синтезу для вивчення взаємозв'язку між управлінням кіберризиками та стратегічним управлінням, а також для оцінки масштабу, структури і вартості кіберзагроз, що впливають на транскордонні цифрові операції. Особливу увагу приділено класифікації цифрових ризиків за сферами виникнення, регіональним і галузевим відмінностям у вартості витоків даних, а також зростаючій ролі штучного інтелекту як у кібератаках, так і в кіберзахисті.

Результати. Дослідження показує, що кібербезпека перетворилася з виключно технічної функції на ключовий стратегічний пріоритет управління міжнародним бізнесом. Підприємства, що функціонують на цифрових платформах і в каналах транскордонної електронної комерції, стикаються з дедалі більшим розмаїттям кіберризиків, включно з програмами-вимагачами, фішингом, DDoS-атаками,

компрометацією ланцюгів постачання та автоматизованими атаками на основі штучного інтелекту, що безпосередньо впливають на їхню конкурентоспроможність, фінансову стійкість і репутацію на глобальних ринках. Аналіз актуальних статистичних даних підтверджує суттєву регіональну та галузеву диференціацію витрат, пов'язаних із витоками даних, і демонструє, що підприємства, які формально інтегрують кібербезпеку у стратегічне планування, характеризуються вищою стійкістю та швидшим відновленням. Запропоновано узагальнену модель стратегічного управління, орієнтованого на кібербезпеку, що охоплює запобігання, виявлення, реагування та стійкість як взаємопов'язані етапи безперервного стратегічного циклу.

Перспективи. Подальші дослідження доцільно зосередити на галузевій специфіці управління кіберризиками для малих і середніх підприємств, що здійснюють міжнародну діяльність, розробленні адаптивних механізмів управління ризиками, пов'язаними зі штучним інтелектом, а також емпіричній оцінці взаємозв'язку між рівнем зрілості кібербезпеки та довгостроковою конкурентоспроможністю суб'єктів підприємницької діяльності в глобальній цифровій економіці.

Ключові слова: *кібербезпека, стратегічне управління, міжнародний бізнес, цифровий ризик, ризик-менеджмент, міжнародне підприємництво.*