***Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292. Ефективна економіка. 2026. № 1. ISSN 2307-2105***

**DOI: http://doi.org/10.32702/2307-2105.2026.1.5**

**УДК 65.012.8:656.2**

*V. Dykan,*

*Doctor of Economics, Professor, Head of the Department of Economics and Management of Production and Commercial Business,*

*Ukrainian State University of Railway Transport*

*ORCID ID: https://orcid.org/0000-0002-5173-2469*

*M. Korin,*

*Doctor of Economics, Professor, Professor of the Department of Economics and Management of Production and Commercial Business,*

*Ukrainian State University of Railway Transport*

*ORCID ID: https://orcid.org/0000-0002-4671-5162*

*H. Obruch,*

*Doctor of Economics, Associate Professor, Professor of the Department of Economics and Management of Production and Commercial Business,*

*Ukrainian State University of Railway Transport*

*ORCID ID: https://orcid.org/0000-0002-9082-2344*

# STRATEGY FOR ENSURING DIGITAL SECURITY OF RAILWAY TRANSPORT ENTERPRISES

*В. Л. Дикань,*
*д. е. н., професор, завідувач кафедри економіки та управління виробничим і комерційним бізнесом,*
*Український державний університет залізничного транспорту*
*М. В. Корінь,*
*д. е. н., професор, професор кафедри економіки та управління виробничим і комерційним бізнесом,*
*Український державний університет залізничного транспорту*
*Г. В. Обруч,*
*д. е. н., доцент, професор кафедри економіки та управління виробничим і комерційним бізнесом,*
*Український державний університет залізничного транспорту*

# СТРАТЕГІЯ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

*It has been established that in the process of digital transformation, railway transport enterprises are increasingly integrating automated traffic management systems, GPS monitoring, IoT devices and electronic document management in order to increase the efficiency of business processes and competitiveness. It has been proven that such digital changes, stimulating positive developments in the work of railway transport enterprises, increase their vulnerability to cyber threats, which are constantly evolving and gaining new scales. It is substantiated that the increase in the number of attacks on critical infrastructure in the world actualizes the need to form a comprehensive digital security strategy that will protect information systems, data and processes from unauthorized access, abuse and violations. The scientific novelty of the study lies in the development of a multi-level strategy for ensuring the digital security of railway transport enterprises, which combines technical, organizational and personnel measures. The proposed strategy includes the stages of risk analysis and identification of critical assets,*

*implementation of modern tools, organizational planning, personnel training and formation of a cyber-hygiene culture, system testing and penetration testing, as well as efficiency auditing using KPIs.*

*The practical significance of the work lies in the possibility of using the proposed strategy to increase the level of digital resilience of railway transport enterprises, ensure the continuity of transportation and protect critical data. The multi-level approach covers the basic level (infrastructure protection and network segmentation), the operational level (backup, multi-factor authentication, security audit), the HR level (employee training, attack simulations, rules for using corporate devices) and the innovative level (artificial intelligence for anomaly analysis, blockchain solutions for data protection, IoT monitoring of wagons and locomotives). It is emphasized that the proposed strategy forms a holistic digital security system that allows railway transport enterprises not only to counteract modern cyber threats, but also to ensure sustainable development and digital transformation of the industry.*

*Встановлено, що в процесі цифрової трансформації підприємства залізничного транспорту дедалі більше інтегрують автоматизовані системи управління рухом, GPS-моніторинг, IoT-пристрої та електронний документообіг з метою підвищення ефективності бізнес-процесів та конкурентоспроможності. Доведено, що такі цифрові зміни, стимулюючи позитивні зрушення в роботі підприємств залізничного транспорту, посилюють і їх вразливість до кіберзагроз, які постійно еволюціонують і набувають нових масштабів. Обґрунтовано, що зростання кількості атак на критичну інфраструктуру актуалізує потребу у формуванні комплексної стратегії цифрової безпеки, що забезпечить захист інформаційних систем, даних та процесів від несанкціонованого доступу, зловживань і порушень. Наукова новизна дослідження полягає у розробленні багаторівневої стратегії забезпечення цифрової безпеки підприємств залізничного транспорту, яка поєднує технічні, організаційні та кадрові заходи.*

*Запропонована стратегія включає етапи аналізу ризиків та ідентифікації критичних активів, впровадження сучасних інструментів, організаційного планування, навчання персоналу та формування культури кібергігієни, тестування систем і проведення penetration-тестів, а також аудит ефективності із застосуванням KPI.*

*Практична значущість роботи полягає у можливості використання запропонованої стратегії для підвищення рівня цифрової стійкості підприємств залізничного транспорту, забезпечення безперервності перевезень та захисту критично важливих даних. Багаторівневий підхід охоплює базовий рівень (захист інфраструктури та сегментація мережі), операційний рівень (резервне копіювання, багатофакторна автентифікація, аудит безпеки), HR-рівень (навчання працівників, симуляції атак, правила використання корпоративних пристроїв) та інноваційний рівень (штучний інтелект для аналізу аномалій, блокчейн-рішення для захисту даних, IoT-моніторинг вагонів і локомотивів). Підкреслено, що запропонована стратегія формує цілісну систему цифрової безпеки, яка дозволяє підприємствам залізничного транспорту не лише протидіяти сучасним кіберзагрозам, але й забезпечувати стійкий розвиток та цифрову трансформацію галузі.*

***Keywords:*** *digital security, economic security, threats, risks, railway transport enterprises, management, strategy, digitalization.*

***Ключові слова:*** *цифрова безпека, економічна безпека, загрози, ризики, підприємства залізничного транспорту, управління, стратегія, цифровізація.*

***Introduction.*** In the context of large-scale and accelerated digitalization, transport enterprises, including railway transport, are actively implementing automated traffic management systems, GPS monitoring, IoT devices and electronic document management. Such technologies increase work efficiency and

competitiveness, but at the same time create new risks associated with cyber threats. The increase in the number of attacks on critical infrastructure in the world confirms the need to strengthen digital security, which ensures the protection of information systems, data and processes from unauthorized access, abuse and violations.

The problem is particularly urgent because cyber incidents in the transport sector can have not only financial consequences, but also directly affect traffic safety, lead to the suspension of transportation and reduce the trust of customers and partners. Therefore, railway transport enterprises must move from basic cyber protection measures to comprehensive digital security systems that include modern technologies: artificial intelligence for anomaly detection, blockchain for data protection, multi-level authentication and integrated incident management systems.

Thus, research into the problem of ensuring digital security of industrial railway transport enterprises is extremely relevant, as it is aimed at guaranteeing the continuity of transport processes, minimizing the risks of cyber incidents, and increasing the competitiveness of the industry in the context of global digital transformation and aggravation of cyber threats.

***Analysis of research and publications***. Active attention was paid to the study of theoretical aspects and the development of practical tools for ensuring digital security of enterprises, including railway transport, by such scientists as: Avanesova N., Volovelska I., Kasyanova N., Maziashvili A., Perederii T., Tokmakova I., Shtangret A., etc. [1-8]. Thus, Avanesova N., Mordovtsev O. and Kolodyazhna T. investigated the features of the formation of the digital security mechanism of industrial enterprises of Ukraine, emphasizing the integration of different levels of protection [1], while Kasyanova N., Bilychenko M. and Severynenko A. considered the modeling of digital security of an enterprise as a tool for assessing risks and building strategies [2]. The mechanism for ensuring the economic security of railway transport enterprises was analyzed by Maziashvili A. and Volovelska I. [3], focusing on digital solutions in the transport sector, and the features of the formation of digital security were highlighted by Obramych O.,

paying attention to the practical aspects of implementation [4]. At the same time, the issue of developing an effective strategy for ensuring the digital security of railway transport enterprises remains insufficiently covered.

***Formulation of the article's objectives.*** The purpose of the scientific article is to develop a strategy for ensuring digital security of railway transport enterprises.

***Presentation of the main research material.*** In today's digital transformation environment, economic entities are increasingly dependent on information technologies, automated management systems, and electronic services. On the one hand, this simplifies and accelerates the execution of various operations and business processes, and on the other, it increases the vulnerability of enterprises to cyber threats, which are constantly becoming more complex, taking on new scales and forms.

According to analytical studies, an increase in cases of unauthorized access, virus attacks and DDoS attacks is recorded every year. In 2024, global economic losses from them were estimated at over $9 trillion, and in 2025 they are already predicted at $10.5 trillion. With such annual costs, the world spends approximately $333 thousand per minute on cybercrime. At the same time, a significant number of crimes remain unregistered. In the latest FBI report for 2024, 859.5 thousand complaints of Internet crimes and losses in the amount of over $16 billion were recorded, which is 33% more than the previous year. This indicates a rapid increase in the number of attacks. In practice, in 2023, a cyberattack hit businesses or individuals approximately every 39 seconds. According to APWG, more than 1.0 million phishing incidents were recorded. Gartner and WEF identify it as a top global risk. The FBI notes that even with proactive disruption efforts like LockBit blocking, losses are still rising. Trend Micro recorded 161 billion threats blocked in 2023, highlighting the scale and automation of today’s attacks. This global surge is why tracking statistics is critical [9, 10].

Among the most popular types of cybercrime attacks during 2024-2025, the following should be noted (Fig. 1) [10]: phishing and spoofing; ransomware;

Business Email Compromise (BEC) and fraud; malware; identity theft/fraud; data leaks, etc.


**Fig. 1. The most popular types of cybercrime attacks during 2024-2025 [10]**

It should be noted that in the context of accelerated scientific and technological progress and technological development, cyber threats and cyber-attacks have significantly evolved from simple viruses, such as viruses and worms, to multi-vector campaigns that combine technical, organizational and psychological methods. The development of clouds, mobility, IoT and industrial systems (OT/ICS) has expanded the attack surface, and the economization of crime (cybercrime as a service) has made attacks larger and more accessible. In such conditions, it is important for enterprises, especially critical infrastructure, to monitor these changes in order to adapt in time.

This acceleration of threat evolution is due to the influence of the following factors:

first, the development of cloud technologies and mobility and, as a result, blurred perimeters, the complexity of access control. This poses challenges for enterprises in identification, in particular multi-factor, privilege management (PAM);

secondly, IoT and OT/ICS, new vulnerable protocols and devices, long equipment life cycle. This poses challenges for enterprises in OT segmentation, anomaly monitoring, patch management in industrial networks;

thirdly, cybercrime services (Crime-as-a-Service) and lowering the “entry threshold” for attackers. This poses challenges for enterprises in proactive threat intelligence, blocking criminals’ infrastructure;

fourthly, the human factor and social engineering, bypassing technical barriers through the user. This poses challenges for enterprises in training, phishing simulations, and least rights policies.

Given the above, the development of a comprehensive strategy for ensuring the digital security of an enterprise is of particular importance, the formation of which should begin with identifying key risks and opportunities in the digital environment, analyzing the current level of digital maturity of the enterprise, and forming strategic goals aimed at ensuring the continuity of business processes and protecting critical data.

A digital security strategy should be based on a proactive approach that organizations take to mitigate the impact of cyber threats and disruptions on their operations, data, and reputation. It also includes implementing a combination of technical controls, employee training, incident response plans, and collaboration with cybersecurity partners to strengthen protection and ensure business continuity in the face of cyberattacks. A digital security strategy aims to build adaptive and flexible business processes that can effectively withstand and recover from cyber incidents.

Based on research [1-10], the following conditions and measures can be identified for the successful implementation of strategic digital security initiatives.

First, one of the most effective ways to improve digital security is to invest in cybersecurity training and education for employees. It is necessary to ensure that regular training sessions are held to familiarize staff with common cyber threats, phishing scams, and data protection best practices. Equipping employees with the

knowledge and skills to identify and mitigate risks will help create a culture of cybersecurity awareness throughout the organization.

Second, it is important to implement multi-layered security measures. A robust cybersecurity strategy should include multi-layered protection against different types of cyber threats. Firewalls, antivirus software, intrusion detection systems, and encryption technologies should be implemented to protect network infrastructure and sensitive data. In addition, you should consider implementing multi-factor authentication to provide an additional layer of protection for user accounts and prevent unauthorized access.

Third, it is advisable to keep software and systems up to date. Outdated software and systems are often vulnerable to cyberattacks due to known security vulnerabilities. It is necessary to ensure that all software applications, operating systems and firmware are regularly updated with the latest patches and fixes. A patch management process should be established to monitor updates and apply them promptly to minimize the risk of cybercriminals exploiting vulnerabilities.

Fourth, you should pay attention to conducting regular security audits and risk assessments. Regular security audits and risk assessments are important for identifying weaknesses in business systems and processes. Comprehensive assessments should be conducted to identify potential security gaps, analyze existing controls, and prioritize remediation. Through proactive risk management, an enterprise’s digital resilience can be significantly strengthened and the likelihood of cyberattacks reduced.

Fifth, it is important to develop incident response plans. Despite all measures to prevent cyberattacks, the enterprise must be prepared to respond effectively in the event of a security incident. Response plans should be developed that define roles, responsibilities, and procedures for detecting, containing, and mitigating cyberthreats. Regular training exercises and simulations should be conducted to test the effectiveness of these plans to ensure that personnel are prepared for real-world scenarios.

Sixth, one of the key conditions for the success of digital resilience activities is to facilitate collaboration with cybersecurity partners. Collaboration with cybersecurity partners, such as managed security service providers (MSSPs) or consultants, can provide additional expertise and resources to enhance digital resilience. It is necessary to involve reputable companies to conduct security assessments, develop customized solutions, and provide ongoing support and monitoring. Using external expertise allows you to strengthen your company's cybersecurity position and stay ahead of new threats.

Taking into account the fact that railway transport enterprises have many physical objects (locomotives, stations, depots) that may be vulnerable to attacks through IoT devices, SCADA systems, it is necessary to strengthen the system for countering cyber threats by digital monitoring of critical objects. This can be practically implemented by installing digital sensors with a secure data transmission channel, using AI/ML to predict incidents (network overload or unauthorized access attempts), integrating with the CERT-UA unit of the State Special Communications Service for a prompt response to cyber incidents. Also, blockchain technologies can be used to protect logistics data, and backup digital platforms for traffic management in the event of an attack. To form and develop a culture of digital resilience, it is advisable to introduce gamification of cybersecurity training for employees.

At the first stage of developing and implementing a strategy for ensuring digital security of railway transport enterprises, risks should be analyzed by identifying critical assets (traffic control systems, dispatch centers, databases), assessing potential threats (cyberattacks, insider risks, technical failures), and using ISO 31000 and NIST Risk Management Framework methodologies (Fig. 2).

The second stage involves the selection of tools, namely: SIEM for centralized monitoring; EDR/XDR for protecting workstations and servers; Zero Trust for access control; SOAR for automated response; UEBA for analyzing personnel behavior; backup and Disaster Recovery for transportation continuity.

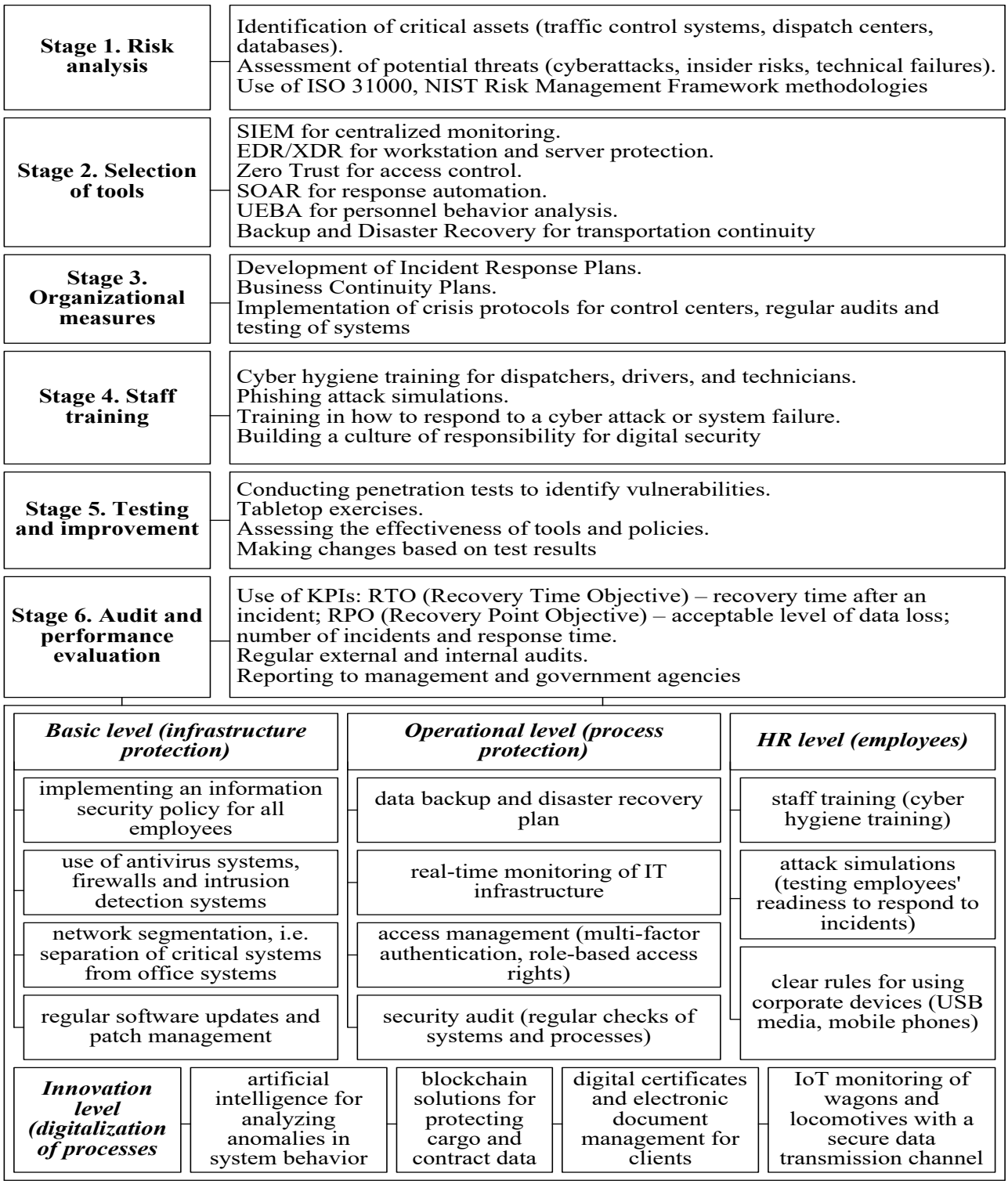


**Fig. 2. Strategy for ensuring digital security of railway transport enterprises (*developed by the authors*)**

Organizational measures are the third stage, which includes the development of Incident Response Plans, Business Continuity Plans, implementation of crisis protocols for control centers, regular audits and testing of systems.

The fourth stage is training personnel through cyber hygiene training for dispatchers, drivers, and technicians, simulations of phishing attacks, training in actions in the event of a cyber-attack or system failure, and forming a culture of responsibility for digital security.

The fifth stage is testing and improvement, which includes: conducting penetration tests to identify weaknesses; tabletop exercises; assessing the effectiveness of tools and policies; and making changes based on test results.

The sixth stage is audit and performance assessment using KPIs (RTO (Recovery Time Objective) – recovery time after an incident; RPO (Recovery Point Objective) – acceptable level of data loss), assessment of the number of incidents and response time, regular external and internal audits, reporting to management and government agencies.

An important component of the strategy is the formation of a multi-level system, ranging from basic to innovative levels. The basic level is infrastructure protection, which involves the implementation of an information security policy for all employees, the use of antivirus systems, firewalls and intrusion detection systems (IDS/IPS), network segmentation (separation of critical systems (SCADA, traffic control) from office systems), regular software updates and patch management.

The operational level is the protection of processes through data backup and a disaster recovery plan (Disaster Recovery Plan), real-time monitoring of IT infrastructure (SIEM systems), access management (multi-factor authentication, role-based access rights), and security auditing (regular audits of systems and processes).

HR level (employees), namely: staff training (cyber hygiene training (phishing, social engineering)); attack simulations (checking employees' readiness to respond to incidents); clear rules for using corporate devices (USB drives, mobile phones).

The innovation level is enabling and includes digitization of processes by using artificial intelligence to analyze anomalies in system behavior, blockchain

solutions to protect cargo and contract data, digital certificates and electronic document flow for customers, IoT monitoring of wagons and locomotives with a secure data transmission channel.

The IT department (technical solutions, monitoring), management (strategy, budget, control), HR department (staff training), and external consultants (audit and implementation of innovative solutions) will be responsible for implementation.

***Conclusions*.** It was found that the digital transformation of railway transport enterprises, on the one hand, provides increased efficiency and competitiveness, and on the other hand, creates new risks associated with cyber threats and technical failures. It was proven that to ensure the stability and continuity of business processes, a multi-level approach to digital security is necessary, which includes technical, organizational and personnel measures. It was substantiated that the strategy for ensuring digital security should include the stages of risk analysis, implementation of modern protection tools, organizational planning, personnel training, system testing and efficiency audit. It was established that a multi-level digital security system should cover the basic level of infrastructure protection, the operational level of processes, the HR level of employees and the innovative level, which involves the use of artificial intelligence, blockchain solutions and IoT monitoring. It was emphasized that the implementation of such a strategy allows to increase the digital stability of railway transport enterprises, minimize risks and ensure the protection of critical data.

## Література

1. Аванесова Н. Е., Мордовцев О. С., Колодяжна Т. В. Формування механізму комплексного забезпечення цифрової безпеки промислового підприємства України. *Вісник НТУ «ХПІ» (економічні науки)*. 2020. Вип. 3. С. 9-14.

2. Касьянова Н. В., Біличенко М. М., Северинeнко А. О. Моделювання цифрової безпеки підприємства. *Modern Economics*. 2023. № 39. С. 54-61.

3. Мазіашвілі А. Р., Воловельська І. В. Механізм забезпечення економічної безпеки підприємств залізничного транспорту. *Вісник економіки транспорту і промисловості*. 2025. № 89. С. 129-136.

4. Обрамич О. С. Особливості формування цифрової безпеки на підприємстві. *Економіка та суспільство*. 2024. Вип. 68. URL: https://doi.org/10.32782/2524-0072/2024-68-20 (дата звернення: 28.12.2025).

5. Передерій Т. Стратегія цифрової безпеки підприємства як драйвер цифрової трансформації економіки України. *Вісник економічної науки України*. 2019. № 2 (37). С. 201-204.

6. Ріль А. О., Талабко О. Ю., Тимкевич М. Б., Хімяк Я. Г., Горбяк А. В. Механізм забезпечення безпеки підприємства у цифровій взаємодії з контрагентами. *Наукові записки Львівського університету бізнесу та права. Серія економічна.* 2023. Вип. 38. С. 454-460.

7. Токмакова І. В., Базилєва М. А., Тиницький О. В. Економічна безпека підприємств в умовах ризикогенного середовища. *Бізнес-навігатор*. 2025. Вип. 5 (82). С. 288-294.

8. Штангрет А. М., Шира Т. Б., Чорненька О. Б. Цифрова трансформація підприємства: об’єктивна необхідність в поточних умовах з позиції забезпечення економічної безпеки. *Східна Європа: економіка, бізнес та управління*. 2024. Вип. 1 (42). С. 97-103.

9. Cybercrime To Cost The World $12.2 Trillion Annually By 2031. *Cybersecurityventures.com : website*. URL: https://cybersecurityventures.com/official-cybercrime-report-2025/ (accessed: 03.01.2026).

10. The cost of cybercrime statistics is projected to be $10.5 trillion annually by 2025. *Deepstrike.io : website*. URL: https://deepstrike.io/blog/cybercrime-statistics-2025 (accessed: 03.01.2026).

**References**

1. Avanesova, N.E. Mordovtsev, O.S. and Kolodiazhna, T.V. (2020), “Formation of a mechanism for comprehensive digital security of industrial enterprises in Ukraine”, *Visnyk NTU “KhPI” (Economic Sciences)*, vol. 3, pp. 9-14.

2. Kasianova, N.V. Bilychenko, M.M. and Severynenko, A.O. (2023), “Modeling enterprise digital security”, *Modern Economics*, vol. 39, pp. 54-61.

3. Maziashvili, A.R. and Volovelska, I.V. (2025), “Mechanism for ensuring economic security of railway transport enterprises”, *Visnyk ekonomiky transportu i promyslovosti*, vol. 89, pp. 129-136.

4. Obramych, O. (2024), “Features of forming digital security at the enterprise”, *Ekonomika ta suspilstvo*, [Online], vol. 68, available at: https://economyandsociety.in.ua/index.php/journal/article/view/4872/4812 (Accessed 28 Dec 2025).

5. Perederii, T. (2019), “Enterprise digital security strategy as a driver of Ukraine’s economic digital transformation”, *Visnyk ekonomichnoi nauky Ukrainy*, vol. 2(37), pp. 201-204.

6. Ril, A.O. Talabko, O.Yu. Tymkevych, M.B. Khimiak, Ya.H. and Horbiak, A.V. (2023), “Mechanism for ensuring enterprise security in digital interaction with contractors”, *Naukovi zapysky Lvivskoho universytetu biznesu ta prava. Seriia ekonomichna*, vol. 38, pp. 454-460.

7. Tokmakova, I.V. Bazylyeva, M.A. and Tynytskyi, O.V. (2025), “Economic security of enterprises in a risk-prone environment”, *Biznes-navigator*, vol. 5 (82), pp. 288-294.

8. Shtangret, A.M. Shyra, T.B. and Chornenka, O.B. (2024), “Digital transformation of the enterprise: objective necessity under current conditions from the perspective of economic security”, S*khidna Yevropa: ekonomika, biznes ta upravlinnia*, vol. 1 (42), pp. 97-103.

9. Cybersecurityventures.com (2025), “Cybercrime To Cost The World $12.2 Trillion Annually By 2031”, available at: https://cybersecurityventures.com/official-cybercrime-report-2025/ (Accessed 03 Jan 2026).

10. Deepstrike.io (2025), “The cost of cybercrime statistics is projected to be $10.5 trillion annually by 2025”, available at: https://deepstrike.io/blog/cybercrime-statistics-2025 (Accessed 03 Jan 2026).

*Стаття надійшла до редакції 13.01.2026 р.*