МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

НАЦІОНАЛЬНА АКАДЕМІЯ ПРАВОВИХ НАУК УКРАЇНИ

25 РОКІВ
У СТАТУСІ НАЦІОНАЛЬНОГО
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ЕКОНОМІКО-ПРАВОВЕ ТА ФІНАНСОВО-ОБЛІКОВЕ ЗАБЕЗПЕЧЕННЯ СТАЛОГО РОЗВИТКУ: СУЧАСНІ ВИКЛИКИ ТА ТРЕНДИ

Тези доповідей
Міжнародної науково-практичної конференції
(м. Вінниця, 21 листопада 2025 р.)

Вінниця 2025

УДК [340.12:330.101:342.734](477)
Е45

Друкується за рішенням оргкомітету
відповідно до доручення Харківського національного університету
внутрішніх справ від 28.08.2025 № 64

Е45

Економіко-правове та фінансово-облікове забезпечення сталого розвитку: сучасні виклики та тренди: тези доп. Міжнар. наук.-практ. конф. (м. Вінниця, 21 листоп. 2025 р.) / МВС України ; Харків. нац. ун-т внутр. справ ; Нац. акад. правових наук України. – Вінниця : ХНУВС, 2025. – 240 с.

У збірнику вміщено тези доповідей учасників конференції за такими напрямами: теоретико-методологічні засади економічного зростання; інституційно-правові механізми забезпечення економічного розвитку; фінансові інструменти й інститути підтримки сталого розвитку; обліково-аналітичне забезпечення управління державним сектором; соціально-економічні та екологічні аспекти розвитку суспільства та національної економіки.

УДК [340.12:330.101:342.734](477)

Матеріали друкуються за рішенням оргкомітету конференції, викладені в авторській редакції з незначними коректорськими правками. Відповідальність за точність поданих фактів, цитат, цифр і прізвищ несуть автори. Електронна копія збірника безоплатно розміщується у відкритому доступі на сайті Харківського національного університету внутрішніх справ (http://www.univd.edu.ua) у розділі «Наука», сторінка «Конференції, семінари та круглі столи»), а також у репозитарії ХНУВС (http://dspace.univd.edu.ua/xmlui

ЗМІСТ

СЕКЦІЯ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ЕКОНОМІЧНОГО ЗРОСТАННЯ

Список бібліографічних посилань

1. Шевченко Р. Що таке ВВП та як його розраховують? MixFin : вебсайт. 07.07.2023. URL: https://mixfin.com/ua/blog/shho-take-vvp/
2. Державна служба статистики України : вебсайт. URL: https://www.ukrstat.gov.ua/ (дата звернення: 16.10.2025).
3. Офіційна статистика міста Києва. Головне управління статистики у м. Києві: вебсайт. URL:http://www.kyiv.ukrstat.gov.ua/p.php3?c=435&lang=1
4. Обсяг реалізованої продукції (товарів, послуг) підприємств за видами економічної діяльності промисловості у 2017–2023 роках. Головне управління статистики у Житомирській області : вебсайт. URL: https://zt.ukrstat.gov.ua-/StatInfo/Prom/promobsiag2.htm
5. Промисловість України: статистичний збірник за 2023 р. Державна служба статистики України: вебсайт. URL: https://ukrstat.gov.ua/druk-/publicat/kat_u/2023/zb/11/year_23_u.pdf

Одержано 30.10.2025

UDC 65.012.8:656.2

Hanna Volodymyrivna 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;
Mykhailo Dmytrovych CHELOMBITKO,
applicant of the third (educational and research) level of higher education,
Ukrainian State University of Railway Transport;
Serhii Romanovych POHREBNIAK,
applicant of the second (master) level of higher education,
Ukrainian State University of Railway Transport

THE ROLE OF DIGITAL SECURITY IN ENSURING THE STABILITY OF THE ACTIVITIES OF RAILWAY TRANSPORT ENTERPRISES

Роль цифрової безпеки в забезпеченні стабільності діяльності підприємств залізничного транспорту

На сьогочасному етапі соціально-економічного розвитку можна констатувати масштабне та активне поширення цифрових технологій як у житті окремої особистості та суспільства, так і бізнес-сегментах. Залізнична галузь як один із ключових інфраструктурних секторів також піддається поступовому оцифруванню бізнес-процесів шляхом активного впровадження автоматизованих систем управління рухом, GPS-навігації, електронних квитків, відеоспостереження та аналітики даних. Досліджено ключові кіберзагрози, з якими стикаються суб'єкти залізничної галузі, і окреслено принципи забезпечення їх цифрової безпеки. Запропоновано використання комплексного підходу до забезпечення

цифрової безпеки підприємств залізничного транспорту, що ґрунтується на інтеграції концепції Zero Trust Architecture та цифрового моніторингу інфраструктури залізничного транспорту.

In the 21st century, digital technologies are the basis of a modern lifestyle, penetrating all spheres of human activity: from personal communication, online banking to business and state management. Thus, business entities actively use cloud technologies, CRM systems, e-commerce. Education increasingly relies on online platforms, virtual laboratories and artificial intelligence. Telemedicine, electronic medical records, robotic surgeries are actively being implemented in the medical field. The banking sector uses digital wallets and blockchain solutions. The transport sector, including rail transport, is no less digitized, thanks to the active use of modern digital technologies, such as automated traffic management systems, GPS navigation, electronic tickets, video surveillance and data analytics. These solutions allow you to optimize traffic schedules, increase passenger safety, reduce maintenance costs and provide a more comfortable service. In particular, intelligent systems for monitoring the condition of tracks and rolling stock allow you to detect malfunctions before they become critical. Passengers can buy tickets online, track train arrivals in real time, and receive notifications about schedule changes. Artificial intelligence and machine learning implement passenger flow forecasting capabilities, which helps to optimally plan routes and allocate resources. Thanks to such changes, rail transport becomes not only more efficient, but also more adaptive to the needs of modern society. However, as in other areas, digitalization exacerbates cybersecurity issues, expanding the digital space and the number of points of vulnerability. Each new device connected to the network can become a potential target for cybercriminals. The increase in the amount of data stored and transmitted creates risks of information leakage, attacks on infrastructure, and privacy violations. At the same time, it should be taken into account that cyberattacks on transport infrastructure can have more serious consequences than in other areas, leading to disruptions in the movement of vehicles and posing a threat to the lives of passengers.

In addition to direct cyberattacks (viruses, Trojans, ransomware, DDoS attacks that paralyze the operation of sites and services, hacking of servers, databases, and accounts), it is also worth mentioning the threat of data leakage. Given the growing value of personal and corporate data, which today act as a strategic resource, they are increasingly becoming the object of cyberthreats through unintentional or intentional disclosure of confidential information, insufficient protection of cloud storage or internal systems, loss of devices with unencrypted data, and social engineering. Other cyberthreats include manipulations to gain access to systems through the human factor, phishing (fake emails or sites that force the user to reveal passwords), vishing (voice fraud), and smishing (SMS fraud). The last sufficiently large-scale cyberattack on the services of JSC “Ukrzaliznytsia” took place on March 27, 2025, when the cargo and passenger online platforms stopped working. While the latter were restored quite quickly, it took much more time to ensure the full operation of cargo online services, during which documents for the transportation of goods were issued in

paper form [1]. The above allows us to conclude that digital transformation requires a strategic approach that involves not only the introduction of new technologies, but also their safe use. Therefore, in the context of digital challenges, it is important to pay attention to studying the concept and tools of digital security of railway transport enterprises.

Given the growing complexity of cyber threats and the scale of their consequences and the evolution of digital technologies, proactive, multi-layered and adaptive protection models are increasingly being used.

An interesting and promising approach to digital security at railway transport enterprises may be the Zero Trust Architecture concept discussed above in combination with digital monitoring of critical infrastructure facilities. Since it is this approach that will allow taking into account the specifics of railway transport, namely: the extensiveness of systems, the mobility of facilities, high requirements for continuity of work and counteraction to modern cyber threats. Such an approach can be implemented in the railway industry by identifying users and devices through multi-factor authentication, segmenting the network by dividing it into isolated zones (for example, traffic management systems, ticketing services, internal document flow), access control based on role distribution (each employee has access only to the necessary functions), monitoring and analyzing behavior through the detection of anomalies in real time.

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 security, it is advisable to introduce gamification of cybersecurity training for employees.

Therefore, today digital security plays a key role in ensuring the stable development of railway transport enterprises, contributing to the protection of critical information systems, the continuity of operational processes, reducing the risks of cyber threats and increasing trust from customers and partners. Its effective provision allows enterprises to adapt to the challenges of digital transformation, implement innovative management technologies, and maintain competitiveness in a dynamic economic environment.

References

1. *Unian.ua: web-site* (2024), “Ukrzaliznytsia resumed a number of important online services after a cyberattack”, available at: https://www.unian.ua/economics-/transport/ukrzaliznicya-vidnovila-nizku-vazhlivih-onlayn-poslug-pislya-kiberataki-12963453.html (Accessed 17 Oct 2025).

Received 24.10.2025