ІНФРАСТРУКТУРНА БЕЗПЕКА В ЕПОХУ ЦИФРОВОЇ ЕКОНОМІКИ
INFRASTRUCTURAL SECURITY IN THE AGE OF THE DIGITAL ECONOMY

УДК 330.34:656.08
DOI: https://doi.org/10.32843/bses.58-14

Шраменко О.В.
к.е.н., доцент,
доцент кафедри економіки
та управління виробничим
і комерційним бізнесом
Український державний університет
залізничного транспорту
Савчук Н.І.
магістр
Український державний університет
залізничного транспорту

Shramenko Olena
Ukrainian State University of Railway
Transport
Savchuk Nadiia
Ukrainian State University of Railway
Transport

У статті обґрунтовано пріоритети інфраструктурної безпеки в епоху цифрової економіки. Відзначено, що розвиток галузей інфраструктури ґрунтується на принципах міжгалузевої ув'язки, а також передбачає проведення інтеграції інфраструктури різних країн. Цифрова економіка охоплює всі сфери сучасного життя. Вона базується на використанні якісно нових інформаційних та телекомунікаційних технологій. Наведено ризики, зумовлені упровадженням цифрових технологій. Обґрунтовано необхідність забезпечення захищеності об'єктів критичної інфраструктури в умовах цифровізації. Захист від кібератак виділено як основний пріоритет інфраструктурної безпеки транспорту. Зроблено акцент на тому, що головним завданням забезпечення інфраструктурної безпеки транспорту є проактивний захист транспортної інфраструктури. З одного боку, цей підхід покликаний забезпечити безпечний розвиток та функціонування транспортної інфраструктури в національних масштабах. З іншого боку, він також буде сприяти безпечному транскордонному співробітництву.
Ключові слова: *економічна безпека, інфраструктурна безпека інфраструктура, транспорт, цифрова економіка, кібербезпека.*

В статье обоснованы приоритеты инфраструктурной безопасности в эпоху цифровой экономики. Отмечено, что развитие отраслей инфраструктуры основывается на принципах межотраслевой увязки, а также предусматривает проведение интеграции инфраструктуры разных стран. Цифровая экономика охватывает все сферы современной жизни. Она основывается на использовании качественно новых информационных и телекоммуникационных технологий. Приведены риски, обусловленные внедрением цифровых технологий. Обоснована необходимость обеспечения защищенности объектов критической инфраструктуры в условиях цифровизации. Защита от кибератак выделена как основной приоритет инфраструктурной безопасности транспорта. Сделан акцент на том, что главным заданием обеспечения инфраструктурной безопасности транспорта является проактивная защита транспортной инфраструктуры. С одной стороны, этот подход призван обеспечить безопасное развитие и функционирование транспортной инфраструктуры в национальных масштабах. С другой стороны, он также будет способствовать безопасному трансграничному сотрудничеству.
Ключевые слова: *экономическая безопасность, инфраструктурная безопасность, инфраструктура, транспорт, цифровая экономика, кибербезопасность.*

The article deals with priority of infrastructural security in the age of the digital economy. It was noted that the development of infrastructure sectors is based on the principles of inter-sectoral linkage and coordination. On the other hand, it provides for the integration of the transport infrastructure of different countries. The digital economy embraces and transforms all areas of modern life. The development of the digital economy is carried out at three interrelated levels: the level of markets and industries, the level of platforms and technologies, and the level of the environment. The digital economy is based on the use of qualitatively new information and telecommunication technologies. The risks associated with the introduction of digital technologies are given in the article. The necessity of ensuring the protection of critical infrastructure facilities in the context of digitalization has been substantiated. The institutional framework for ensuring the protection of critical infrastructure in Ukraine is considered. It is noted that the transport system is one of the most vulnerable sectors of the economy from the cybercriminals' point of view. In the digital economy, its activities are characterized by active processes of implementation of software and hardware systems and complexes for automated control of technical objects and technological processes. The main manifestations of cyber threats in this case can be next ones: uncontrolled distortion of information, which is responsible for the safe operation of the infrastructure, and interception or blocking of the management of the infrastructure as a whole or its separate subsystems. In this regard, protection against cyberattacks is highlighted as the main priority of the infrastructure security of transport. The emphasis is made on the fact that the main task of ensuring transport infrastructure security is proactive protection of transport infrastructure. On the one hand, this approach is aimed to ensure the safe development and functioning of the transport infrastructure within the state. On the other hand, it will also contribute to the safe integration of the transport of different countries.
Key words: *economic security, infrastructural security, infrastructure, transport, digital economy, cybersecurity.*

Постановка проблеми. У XXI столітті людство увійшло в епоху цифровізації, де інфраструктурна безпека відіграє важливу роль для забезпечення сталого розвитку економіки та сприятливих умов життєдіяльності населення.

Інфраструктурна безпека – це стан безперебійного функціонування інфраструктури національної економіки, за якого нею забезпечується стійка й ефективна реалізація суспільного відтворювального процесу.

Інфраструктура забезпечує нормальну роботу основних служб і виробничих систем у будь-якому суспільстві.

В епоху нової економіки розвиток науки й техніки надав людству цифрові можливості і здатність враховувати в цифровому відображенні реального фізичного світу ті особливості, які були недоступні раніше для обліку комплексних аспектів буття. Віртуальний цифровий світ колосально розширив можливості людей і дав змогу вирішувати раніше не здійсненні завдання й досягати недосяжних, як раніше здавалося, цілей.

Одна з найсильніших сторін нашого сучасного розвиненого суспільства є також одним з найголовніших його недоліків. У нинішньому взаємопов'язаному світі розвинені високотехнологічні соціуми сильно залежать від роботи низки служб і сервісів, які сьогодні стали життєво необхідними. Останніми роками в усьому світі неухильно зростає рівень кіберзлочинності. Збій в інфраструктурній роботі через природні причини, технічні неполадки або навмисні дії може

мати серйозні наслідки для постачання ресурсів або роботи критичних служб, не говорячи вже про загрозу безпеці.

Отже, слід звернути увагу на інфраструктурну безпеку, бо кібератаки можуть принести збої в роботі, які в будь-якому разі вплинуть на здоров'я, безпеку та добробут громадян країни.

Аналіз останніх досліджень і публікацій. Питаннями економічної безпеки як у національному масштабі, так і на рівні окремих галузей займаються багато вчених як в Україні, так і за кордоном. Значний пласт наукових досліджень щодо вирішення проблем економічної безпеки залізничного транспорту належить керівникові однієї з відомих наукових шкіл України, а саме В.Л. Диканю, а також ученим його школи, якими є І.Л. Назаренко, Т.Г. Сухорукова, І.В. Воловельська [1–3].

Суттєвий вклад у розкриття питань фінансово-економічної безпеки інфраструктури зробила Н.О. Журавльова [4]. Втім, досі інфраструктурна безпека транспорту залишається тією сферою, яка досліджена недостатньо.

Крім того, цифрова економіка формує нові виклики до забезпечення економічної безпеки як у національному масштабі, так і на транспорті. Завдання, які у зв'язку з цим постають перед підприємствами, державою та суспільством, є об'єктом інтенсивного обмірковування серед спеціалістів [5–8].

Постановка завдання. Метою статті є визначення пріоритетів забезпечення інфраструктурної безпеки транспорту в умовах цифровізації. Для цього слід вирішити низку завдань. Перше завдання пов'язане зі встановленням особливостей розвитку транспортної інфраструктури, а друге – з виділенням ризиків цифрової економіки для її розвитку.

Виклад основного матеріалу дослідження. Інфраструктура є елементом суспільного блага. Інфраструктурні обмеження є ключовими обмеженнями з точки зору розвитку економіки країни. Відповідальність за забезпечення розвитку інфраструктури зазвичай лягає на державу. Будівництво автомобільних доріг, розвиток залізничного транспорту, модернізація й спорудження нових морських і повітряних портів є досить капіталомістким процесом, який без участі держави не обходиться в жодній країні. Приватний капітал бере участь в інфраструктурних проєктах у невеликому обсязі не тільки з огляду на високу капіталомісткість, але й через складність повернення інвестицій, якщо йдеться не про будівництво платних доріг або терміналів.

Політика більшості провідних країн світу спрямована на розвиток інфраструктури. Слід зазначити, що розвиток галузей інфраструктури, з одного боку, ґрунтується на принципах міжгалузевої ув'язки та координованості, а з іншого боку, передбачає проведення інтеграції інфраструктури різних країн. План розвитку інфраструктури Великобританії, наприклад, сформований на основі міжгалузевої ув'язки і координації понад 500 проєктів, кожен з яких окремо пов'язаний або буде інтегрований в єдину національну систему інфраструктури. Нині сформована Довгострокова міжгалузева програма фінансування та управління інфраструктурою на період до 2042 р.

Політика розбудови інтегрованого транспортно-логістичного простору нині ефективно реалізується в ЄС в рамках формування європейської транспортної мережі TEN як основи розвитку міжнародних перевезень між державами-членами. Не менші зусилля на формування глобального транспортно-логістичного коридору «Азія – Європа – Африка» докладаються країнами Азіатсько-Тихоокеанського регіону в рамках стратегії розвитку міжнародної торгівлі Китаю «Один пояс – один шлях» [9].

Розвиток транспортної інфраструктури також є одним з пріоритетних напрямів розвитку нашої країни. Розроблена Міністерством інфраструктури України Стратегія "Drive Ukraine 2030" передбачає створення цифрової інфраструктури, забезпечення безпеки на транспорті, впровадження безпілотних автомобілів, розбудову транспортних коридорів, створення єдиної транспортної та інфраструктури мережі з Європейським Союзом [10].

Говорячи про якість розвитку інфраструктури транспорту, вчені переважно досліджують її фізичний стан. Однак сьогодні великого значення набуває такий критерій, як безпека інфраструктури, значимість якого в декілька разів підвищилася в умовах цифровізації.

Безпека інфраструктури в сучасних умовах – це стан інфраструктури, що забезпечує безпеку особистості, господарських суб'єктів, держави загалом; загальний, достатній і надійний доступ до інфраструктури за справедливими цінами; інноваційність і комплексність інфраструктури, необхідні для підтримки конкурентоспроможності економіки; фінансово-економічну безпеку інфраструктури [11].

Формування цифрової економіки є ключовим напрямом Четвертої промислової революції. Цифрова економіка базується на якісно новому типі інформаційних та телекомунікаційних технологій, що охоплюють і перетворюють усі сфери сучасного виробничого та суспільного життя. Хоча вона перебуває в процесі формування, вже сьогодні вона володіє потужним потенціалом, що надає під час його реалізації шанс на досягнення провідних позицій і окремим компаніям, і країнам загалом.

Вчені відзначають, що розвиток цифрової економіки здійснюється на трьох взаємопов'язаних рівнях, а саме на рівні ринків і галузей (сфер діяльності), де здійснюється взаємодія господа-

рюючих суб'єктів; рівні платформ і технологій, де формуються компетенції для розвитку ринків і галузей (сфер діяльності); рівні середовища, яке створює умови для розвитку платформ і технологій, а також ефективної взаємодії суб'єктів ринків і галузей економіки (сфер діяльності) та об'єднує нормативне регулювання, цифрову інфраструктуру, кадри та інформаційну безпеку [12].

Найчастіше цифрові технології не впливають на національну безпеку безпосередньо, а вплив відбувається через вплив на динаміку й вектор соціально-економічного прогресу, тому країни, які «відстають» за темпами й масштабами цифровізації, стикаються з низкою загроз національній безпеці.

Серед загроз цифровій економіці в національних масштабах вчені виділяють такі:

– наздоганяюча роль у світовій економіці;

– обмеження перспектив інноваційного розвитку;

– зниження конкурентоспроможності їх компаній;

– обмеженість інструментарію для забезпечення національної безпеки [13].

Серед ризиків, зумовлених упровадженням цифрових технологій, також виділяють такі [14]:

1) ризики, пов'язані із застосуванням Інтернету речей (вразливість (несанкціонований вплив, кібертероризм) і незаконне застосування технологій (управління відеонаглядом тощо));

2) ризики застосування штучного інтелекту, роботизації, автоматизації (зростання соціального відчуження через втрату робочих місць, підвищення рівня безробіття, соціальна напруженість, тотальне спостереження за населенням, можливий витік інформації, що є комерційною таємницею, тощо);

3) ризики використання технології блокчейн, пов'язані з уразливістю безпеки самої системи блокчейна й побудованої на ній інфраструктури послуг, незмінністю інформації в мережі (неможливість виправити помилку, змінити некоректно введену інформацію), використанням токенів як засобу для відмивання грошей, фінансування тероризму;

4) ризики, пов'язані з використанням імпортної мікроелектроніки (основна частка програмного забезпечення та комп'ютерної техніки, що використовуються в Україні, є імпортованою, тому не виключено, що вони можуть містити спеціальні чіпи для шпигування);

5) ризики, пов'язані із застосуванням хмарних і розподільних обчислень (залежність від надійності функціонування телекомунікаційної системи, розмивання відповідальності за інформаційну безпеку та зниження рівня контролю у зв'язку із їх розподілом між компаніями-користувачами, організацією та власником хмарної платформи, інтернет-провайдером);

6) ризики, пов'язані зі стійкістю роботи Інтернету;

7) ризики впливу на суспільну свідомість (розвиток технологій великих даних, зростання мережевого простору, досягнення в когнітивних і поведінкових науках зумовили появу ефективних розробок, орієнтованих на неявне збирання даних і приховане управління груповою поведінкою великих колективів);

8) ризики, пов'язані з підвищенням рівня складності бізнес-моделей і відсутністю кваліфікованих кадрів.

З огляду на те, що транспорт належить до об'єктів критичної інфраструктури і має стратегічне значення для розвиту держави, врахування цих ризиків є головною умовою ефективного функціонування не тільки самого транспорту, але й економіки країни загалом. Отже, забезпечення інфраструктурної безпеки транспорту в умовах цифрової економіки набуває нового сенсу.

Під захистом критичної інфраструктури розуміються заходи щодо забезпечення безпеки взаємозалежних систем, мереж і активів, що лежать в основі служб, життєво необхідних для функціонування суспільства.

17 лютого 2017 р. Рада Безпеки Організації Об'єднаних Націй одноголосно ухвалила резолюцію 2341 «Про захист критично важливих об'єктів інфраструктури та розширення можливостей держав щодо запобігання нападам на критично важливі об'єкти інфраструктури» та закликала держав-членів протистояти небезпеці терористичних атак на критично важливі об'єкти інфраструктури. Резолюція пропонує державам-членам розглянути можливі превентивні заходи під час розроблення національних стратегій і політики [15].

В Україні у 2020 р. було оновлено Стратегію національної безпеки України. В ній зазначено, що зараз посилюються загрози для критичної інфраструктури, пов'язані з погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, зокрема фізичного й кіберхарактеру, триваючими бойовими діями, а також тимчасовою окупацією частини території України [16].

Зараз в Україні розробляється проєкт Закону України «Про критичну інфраструктуру та її захист» [17]. Особливої актуальності сьогодні набуває необхідність забезпечення захищеності об'єктів критичної інфраструктури від кібератак. За словами А.Б. Авакова, за останні п'ять років кількість кіберзлочинів в Україні зросла у 2,5 рази [18, с. 22].

У 2016 р. питання захисту критичної інфраструктури стало предметом розгляду РНБО України, а 28 січня 2020 р. Президент України підписав Указ «Про створення Національного координаційного центру кібербезпеки при РНБО» [18, с. 13].

Однак питання забезпечення безпеки критичної інфраструктури має не лише вирішуватися на рівні держави, але й включати заходи всередині самих галузей. За відомостями аналітиків, найбільший інтерес для терористів представляють такі сфери, як військова і ядерна, енергетична, фінансова, сфера транспортних перевезень. Транспортна галузь є однією з найбільш вразливих з точки зору кіберзлочинців галузей економіки.

З огляду на те, що останнім часом на транспорті активно відбувається процес впровадження програмно-апаратних систем та комплексів для автоматизованого управління технічними об'єктами та технологічними процесами, сьогодні це має бути одним з головних напрямів забезпечення інфраструктурної безпеки транспорту.

Основними проявами кібернебезпек під час використання програмно-апаратних систем та комплексів на транспортній інфраструктурі можуть бути неконтрольоване спотворення інформації, яка відповідає за безпечне функціонування інфраструктури, перехоплення або блокування управління інфраструктурою загалом або її підсистемами зокрема.

Розміри та вартість усунення наслідків зазначених небезпек оцінити дуже складно, а іноді взагалі неможливо. Можна тільки констатувати, що шкода від кібератак є дуже значною. В середньому збиток від дій хакерів по всьому світі оцінюється в 600 мільярдів доларів щорічно. Дослідники поділяють витрати компаній, пов'язані з проявами кібернебезпек, на шість таких основних категорій: втрата інтелектуальної власності, усунення наслідків кіберзлочинів, втрата бізнес-інформації, порушення безперебійності роботи IT-систем, вартість забезпечення безпеки мереж, а також шкоди репутації в результаті атаки [19]. У зв'язку з цим головним завданням забезпечення інфраструктурної безпеки транспорту має бути проактивний захист транспортної інфраструктури. Він полягає у використанні систем виявлення та усунення втручань.

Висновки з проведеного дослідження. Проведені дослідження показали, що головними особливостями розвитку інфраструктури сьогодні є формування її на принципах міжгалузевої взаємодії та транскордонного співробітництва. За таких умов будь-які загрози транспортній інфраструктурі впливають на можливість ефективного й безпечного функціонування інфраструктур інших галузей та країн. В еру цифрової економіки головною небезпекою для транспортної інфраструктури стає кібернебезпека, прояви якої можуть заподіяти значної шкоди економічного й соціального характеру не тільки в масштабах транспортної галузі, але й у національному та міждержавному масштабі, тому використання проактивного захисту транспортної інфраструктури є головним пріоритетом у забезпеченні інфраструктурної безпеки. Застосування цього підходу дасть можливість вчасно попередити можливі втручання в роботу транспорту та уникнути негативних наслідків від них. З одного боку, цей підхід покликаний забезпечити безпечний розвиток та функціонування транспортної інфраструктури в національних масштабах. З іншого боку, він також буде сприяти безпечному транскордонному співробітництву.

Напрямом подальших наукових досліджень може бути пошук шляхів уникнення загроз для розвитку транспортної інфраструктури, викликаних цифровою економікою.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Дикань В.Л., Назаренко І.Л. Комплексна методика визначення рівня економічної безпеки, оцінки ризиків та ймовірності банкрутства підприємства : монографія. Харків : УкрДАЗТ, 2010. 142 с.

2. Дикань В.Л., Воловельская И.В. Специфические особенности системы обеспечения экономической безопасности железнодорожного транспорта. *Науковий вісник Херсонського державного університету. Серія: Економічні науки*. 2016. Вип. 16. С. 63–66.

3. Назаренко І.Л., Сухорукова Т.Г. Методика оцінки рівня економічної безпеки дистанції колії. *Вісник економіки транспорту і промисловості*. 2014. № 48. С. 64–69.

4. Журавлева Н.А. Финансово-экономическая безопасность инфраструктуры: вопросы теории и методологии : дисс. … докт. экон. наук : спец. 08.00.05. Санкт-Петербург, 2010. 275 с.

5. Дикань В.Л., Обруч Г.В. Управління реалізацією спільних інвестиційних проектів за участю підприємств залізничного транспорту в умовах цифровізації. *Вісник економіки транспорту і промисловості*. 2020. № 69. С. 9–21.

6. Обруч Г.В. Розвиток послуг підприємств залізничного транспорту на основі розбудови цифрових платформ. *Підприємництво та інновації*. 2019. № 10. С. 62–68.

7. Токмакова І.В., Чередниченко О.Ю., Войтов І.М., Паламарчук Я.С. Цифрова трансформація залізничного транспорту як фактор його інноваційного розвитку. *Вісник економіки транспорту і промисловості*. 2019. № 68. С. 125–134.

8. Дульська І.В. Пріоритетні напрями цифровізації національної економіки і суспільства. *Збірник сучасних проблеми економіки і підприємництва*. 2019. Вип. 24. С. 14–24.

9. Корінь М.В. Розроблення моделі спільного управління інфраструктурними проектами розвитку залізничного транспорту в умовах транскордонної співпраці. *Інтелект XXI*. 2019. № 1. С. 37–42.

10. Про схвалення Національної транспортної стратегії України на період до 2030 року : Розпорядження Кабінету Міністрів України від 30 травня 2018 р. № 430-р. [офіційний текст станом на 31 жовтня 2020 р.]. URL: https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80#n13 (дата звернення 08.10.2020).

11. Шраменко О.В. Забезпечення інфраструктурної безпеки. *Вісник економіки транспорту і промисловості*. 2016. № 57. С. 113–119.

12. Рихтер К.К., Пахомова Н.В. Проблемы модернизации и перехода к инновационной экономике. *Проблемы современной экономики*. 2018. № 2 (66). URL: http://www.m-economy.ru/art.php?nArtId=6323 (дата звернення 24.10.2020).

13. Шинкарецкая Г.Г., Берман А.М. Цифровизация и проблема обеспечения национальной безопасности. *Образование и право*. 2020. № 5. С. 254–260.

14. Шевчук І.Б. Цифровізація та її вплив на економіку України: переваги, виклики, загрози й ризики. *Математичні методи, моделі та інформаційні технології в економіці*. 2019. Вип. 47-2. С. 173–177.

15. Защита критически важных объектов инфраструктур от террористических атак: сборник передового опыта. 2018. 148 с. URL: https://www.un.org/sc/ctc/wp-content/uploads/2019/07/RUS-compendium-final.pdf (дата звернення 24.10.2020).

16. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 р. «Про Стратегію національної безпеки України» : Указ Президента України від 14 вересня 2020 р. № 392/2020 [офіційний текст станом на 31 жовтня 2020 р.]. URL: https://zakon.rada.gov.ua/laws/show/392/2020#n5 (дата звернення 24.10.2020).

17. Про критичну інфраструктуру та її захист : Проєкт Закону України. *Офіційний веб-сайт Міністерства економічного розвитку і торгівлі України*. URL: https://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=a91bfd44-d9be-4a74-834f-3feaf92bb886&title=ProektZakonuUkrainiproKritichnuInfrastrukturuTa YiiZakhist (дата звернення: 24.10.2020).

18. Кібербезпека в інформаційному суспільстві. *Інформаційно-аналітичний дайджест*. 2020. № 9 (вересень). 186 с. URL: http://nbuviap.gov.ua/images/vydannya/2019/bezpeka_no_9.pdf (дата звернення 01.11.2020).

19. Світовий збиток від кібератак досягає 600 мільярдів доларів на рік. URL: https://www.epravda.com.ua/news/2018/02/22/634346 (дата звернення 01.11.2020).

REFERENCES:

1. Dykan' V.L., Nazarenko V.L. (2010) *Kompleksna metodyka vyznachennya rivnya ekonomichnoyi bezpeky, otsinky ryzykiv ta ymovirnosti bankrutstva pidpryyemstva* [A comprehensive methodology for determining the level of economic security, risk assessment and probability of bankruptcy] Kharkiv: UkrDAZT. (in Ukrainian)

2. Dikan' V.L., Volovel'skaya I.V. (2016). Spetsificheskie osobennosti sistemy obespecheniya ekonomicheskoy bezopasnosti zheleznodorozhnogo transporta. [Specific features of the system for ensuring the economic security of railway transport]. *Scientific Bulletin of Kherson State University. Series: Economic Sciences*. No. 16, pp. 63–66.

3. Nazarenko I.L., Sukhorukova T.H. (2014) Metodyka otsinky rivnya ekonomichnoyi bezpeky dystantsiyi koliyi [Methods for assessing the level of economic safety of the track distance]. *The bulletin of Transport and Industry Economics*. No. 48, pp. 64–69.

4. Zhuravleva N.A. (2010) Finansovo-ekonomicheskaya bezopasnost' infrastruktury: voprosy teorii i metodologii [Financial and economic security of infrastructure: theory and methodology] (PhD Thesis), Sankt-Peterburg: Saint Petersburg State University.

5. Dykan' V.L., Obruch H.V. (2020) Upravlinnya realizatsiyeyu spil'nykh investytsiynykh proektiv za uchastyu pidpryyemstv zaliznychnoho transportu v umovakh tsyfrovizatsiyi [Management of joint investment projects implementation with the participation of railway transport enterprises in the conditions of digitalization]. *The bulletin of Transport and Industry Economics*. No. 69, pp. 9–21.

6. Obruch H.V. (2019) Rozvytok posluh pidpryyemstv zaliznychnoho transportu na osnovi rozbudovy tsyfrovykh platform [Development railway transport enterprises services based on the development of digital platforms] *Entrepreneurship and innovation*. No. 10, pp. 62–68.

7. Tokmakova I.V., Cherednychenko O.Yu., Voytov I.M., Palamarchuk Ya.S. (2019) Tsyfrova transformatsiya zaliznychnoho transportu yak faktor yoho innovatsiynoho rozvytku [Digital transformation of railway transport as a factor of its innovative development]. *The bulletin of Transport and Industry Economics*. No. 68, pp. 125–134.

8. Dul's'ka I.V. (2019) Priorytetni napryamy tsyfrovizatsiyi natsional'noyi ekonomiky i suspil'stva [Priority areas of digitalization of the national economy and society]. *Collection of modern problems of economics and entrepreneurship*. No. 24, pp. 14–24.

9. Korin' M.V. (2019) Rozroblennya modeli spil'noho upravlinnya infrastrukturnymy proektamy rozvytku zaliznychnoho transportu v umovakh trasnkordonnoyi spivpratsi [Development of a model for joint management of infrastructure projects for the development of railway transport in the context of cross-border cooperation]. *Intelligence XXI*. No. 1, pp. 37–42.

10. Pro skhvalennja Nacionaljnoji transportnoji strateghiji Ukrajiny na period do 2030 r.: Rozporjadzhennja Kabineta ministriv Ukrajiny № 430-r. (ofic. tekst: stanom na 30 travnja 2018 r.) [On approval of the National Transport Strategy of Ukraine for the period up to 2030]. Available at: https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80#Text (accessed 08 October 2020).

11. Shramenko O.V. (2016) Zabezpechennya infrastrukturnoyi bezpeky [Ensuring of infrastructure safety for the railway transport]. *The bulletin of Transport and Industry Economics*. No. 57, pp. 113–119.

12. Rikhter K.K., Pakhomova N.V. (2018) Problemy modernizatsii i perekhoda k innovatsionnoy ekonomike [Problems of modernization and transition to an innovative economy]. *Problems of the modern economy*. No. 2 (66), pp. 22–31. Available at: http://www.m-economy.ru/art.php?nArtId=6323 (accessed 24 October 2020).

13. Shinkaretskaya G.G., Berman A.M. (2020) Tsifrovizatsiya i problema obespecheniya natsional'noy bezopasnosti [Digitalization and the problem of ensuring national security]. *Education and law*. No. 5, pp. 254–260.

14. Shevchuk I.B. (2019) Tsyfrovizatsiya ta yiyi vplyv na ekonomiku ukrayiny: perevahy, vyklyky, zahrozy y

ryzyky [Digitalization and its impact on the economy of Ukraine: advantages, challenges, threats and risks]. *Mathematical methods, models and information technologies in economics*. No. 47-2, pp. 173–177.

15. Zashchita kriticheski vazhnykh ob"ektov infrastruktur ot terroristicheskikh atak: sbornik peredovogo opyta (2018) [Protecting critical infrastructures from terrorist attacks: a compilation of best practices]. Available at: https://www.un.org/sc/ctc/wp-content/uploads/2019/07/RUS-compendium-final.pdf (accessed 24 October 2020).

16. Pro rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 14 veresnja 2020 r. "Pro Strateghiju nacionaljnoji bezpeky Ukrajiny". Ukaz Prezydenta Ukrajiny vid 14 veresnja 2020 r. No 392 [On the decision of the National Security and Defense Council of Ukraine dated September 14, 2020 "On the National Security Strategy of Ukraine". Decree of the President of Ukraine dated September 14, 2020, no. 392]. Available at: https://zakon.rada.gov.ua/laws/show/392/2020#n5 (accessed 24 October 2020).

17. Pro krytychnu infrastrukturu ta jiji zakhyst. Proekt Zakonu Ukrajiny. Oficijnyj veb-sajt Ministerstva ekonomichnogho rozvytku i torghivli Ukrajiny (2020) [On critical infrastructure and its protection. Draft Law of Ukraine. Official website of the Ministry of economic development and trade of Ukraine]. Available at: https://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=a91bfd44-d9be-4a74-834f-3feaf92bb886&title=ProektZakonuUkrainiproKritichnuInfrastrukturuTaYiiZakhist (accessed 24 October 2020).

18. Dovhan' O., Lytvynova L., Dorohykh S. (2020) Kiberbezpeka v informatsiynomu suspil'stvi [Cyberbezpeka in the information support] Information and analytical digest, no. 9, p. 186. Available at: http://nbuviap.gov.ua/images/vydannya/2019/bezpeka_no_9.pdf (accessed 01 November 2020).

19. Svitovyy zbytok vid kiberatak dosyahaye 600 mil'yardiv dolariv na rik [The global damage from cyberattacks reaches $ 600 billion a year]. Available at: https://www.epravda.com.ua/news/2018/02/22/634346/ (accessed 01 November 2020).