УДК 65.012.8:656.2

*Г. В. Обруч,*
*д. е. н., доцент, професор кафедри економіки та управління виробничим і комерційним бізнесом, Український державний університет залізничного транспорту*
*ORCID ID: https://orcid.org/0000-0002-9082-2344*
*М. Д. Челомбітько,*
*здобувач третього (освітньо-наукового) рівня вищої освіти, Український державний університет залізничного транспорту*
*ORCID ID: https://orcid.org/0009-0006-2440-6437*
*С. Р. Погребняк,*
*здобувач другого (магістерського) рівня вищої освіти, Український державний університет залізничного транспорту*
*ORCID ID: https://orcid.org/0009-0007-3590-0112*

DOI: 10.32702/2306-6814.2025.21.109

# ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ В УМОВАХ ПОСИЛЕННЯ КІБЕРАТАК

H. Obruch,
Doctor of Economic Sciences, Associate Professor, Professor of the Department of Economics and Management of Production and Commercial Business, Ukrainian State University of Railway Transport
M. Chelombitko,
Applicant of the third (educational and research) level of higher education, Ukrainian State University of Railway Transport
S. Pohrebniak,
Applicant of the second (master) level of higher education, Ukrainian State University of Railway Transport

## ENSURING DIGITAL SECURITY OF RAILWAY TRANSPORT ENTERPRISES IN THE CONDITIONS OF INCREASING CYBERATTACKS

***З'ясовано, що цифрові технології стали невід'ємною складовою сучасного способу життя, охопивши всі сфери діяльності — від особистого спілкування та онлайн-банкінгу до управління бізнесом і державою. Акцентовано увагу на поступовому оцифруванні транспортного сектору, зокрема залізничної галузі, де активно застосовуються автоматизовані системи управління рухом, GPS-навігація, електронні квитки, відеоспостереження та аналітика даних. Визначено ключові кіберзагрози для суб'єктів економічної діяльності, у т. ч. і залізничної галузі, та окреслено принципи забезпечення їх цифрової безпеки. Обґрунтовано доцільність впровадження проактивних, багаторівневих та адаптивних моделей захисту, зокрема концепції Zero Trust Architecture, мультифакторної автентифікації, шифрування даних і спеціалізованих хмарних рішень. Запропоновано інтеграцію підходу Zero Trust Architecture із цифровим моніторингом критичних об'єктів інфраструктури залізничного транспорту, що дозволить врахувати його розгалуженість, мобільність та високі вимоги до безперервності роботи. Доведено, що реалізувати зазначене можливо шляхом автентифікації користувачів та пристроїв, сегментації мережі на ізольовані зони (системи управління рухом, білетні сервіси, документообіг), контролю доступу за ролями та моніторингу поведінки з виявленням аномалій у реальному часі.***

***It was found that digital technologies are the basis of a modern way of life, penetrating all spheres of human activity: from personal communication, online banking to business and state management. It was proven that the transport sector, including rail transport, is no less digitized, thanks to the active use of modern digital technologies, such as automated traffic control systems, GPS navigation, electronic tickets, video surveillance***

***and data analytics. Key cyber threats for economic entities, including the railway industry, were revealed. The principles of ensuring digital security of railway transport enterprises were identified and disclosed. It was emphasized that to implement the principles of digital security in railway transport, it is advisable to use both technical and organizational and legal means and approaches. It is proposed to consider digital security as a set of technological, organizational and legal measures aimed at protecting information systems, data and digital infrastructure objects from unauthorized access, loss, damage or malicious use. Given the growing complexity of cyber threats and the scale of their consequences and the evolution of digital technologies, the feasibility of using proactive, multi-level and adaptive protection models (Zero Trust Architecture approach, multi-factor authentication, data encryption, specific approaches to protecting data and services in the "cloud") has been proven. At railway transport enterprises, it is proposed to implement the Zero Trust Architecture concept in combination with digital monitoring of critical infrastructure objects, which will allow taking into account the specifics of railway transport, namely: the ramification of systems, mobility of objects, high requirements for continuity of work and counteraction to modern cyber threats. It is proposed to implement such an approach 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 real-time anomaly detection.***

*Ключові слова: цифрова безпека, ризики, загрози, підприємства залізничного транспорту, управління, кібератаки, цифровізація, цифрове середовище.*

*Key words: digital security, risks, threats, railway transport enterprises, management, cyberattacks, digitalization, digital environment.*

## ПОСТАНОВКА ПРОБЛЕМИ

На сучасному етапі прискорення цифрових змін та наростання кількості та масштабності кібератак в транспортній галузі питання забезпечення цифрової безпеки набуває особливої актуальності і для підприємств залізничного транспорту. Оскільки залізничні системи дедалі більше інтегруються з інноваційними інформаційними технологіями (автоматизоване управління рухом поїздів, електронні квитки, системи моніторингу інфраструктури, обмін даними між станціями та центральними серверами) слід враховувати, що такі зміни створюють як нові можливості, так і ризики. Окрім того, кібератаки на транспортні об'єкти можуть призвести не лише до фінансових втрат, а й до реальних загроз безпеці пасажирів і персоналу. Зокрема, втручання в системи сигналізації, управління рухом або доступ до конфіденційної інформації може мати критичні наслідки. Тому впровадження комплексного підходу до забезпечення цифрової безпеки підприємств залізничного транспорту з урахуванням технічних, організаційних та правових аспектів їх діяльності наразі варто розглядати як необхідну умову стабільної та безпечної роботи суб'єктів залізничної галузі.

## АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Дослідженню теоретичних аспектів і формуванню практичних рекомендацій щодо забезпечення цифрової безпеки підприємств, у т. ч. залізничного транспорту, приділили увагу такі вчені як: Воловельська І., Дикань В., Кульчицький І., Мазіашвілі А., Обрамич О., Остапюк Б., Передерій Т., Федонюк А., Шостак Л. та ін. [1-6]. Зокрема Дикань В., Остапюк Б. та Черниш В. дослідили сучасні виклики та можливості ризик-орієнтованого управління підприємством [2]. Обрамич О. зосередив увагу на цифровій безпеці та особливостях її формування на підприємстві [4]. Кульчицький І. проаналізував категорії "цифрова економіка" та "економічна безпека підприємства" і сформував стратегії управління економічною безпекою суб'єктів господарювання [3]. Передерій Т. присвятив дослідження особливостям розроблення стратегії цифрової безпеки підприємства як драйверу цифрової трансформації економіки України [5]. Воловельська І. та Мазіашвілі А. грунтовно вивчили проблеми економічної безпеки підприємств України в умовах глобальної цифровізації [1]. Шостак Л., Федонюк А. та Помазун О. розглянули роль кібербезпеки в системі формування бізнес-моделі підприємства в умовах цифрової економіки [6]. Разом з цим, питання забезпечення цифрової безпеки підприємств залізничного транспорту залишилося недостатньо висвітленим і потребує подальших наукових пошуків.

## ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою наукової статті є розкриття ключових принципів, компонентів та інструментів забезпечення цифрової безпеки підприємств залізничного транспорту в умовах посилення кібератак.

## ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У XXI ст. цифрові технології виступають основою сучасного способу життя, проникнувши в усі сфери людської діяльності: починаючи від особистого спілкування, онлайн-банкінгу до управління бізнесом та державою. Так, бізнес-суб'єкти активно використовують хмарні технології, CRM-систем, електронну комерцію. Освіта дедалі більше покладається на онлайн-платформи, віртуальні лабораторії та штучний інтелект. Актив-

но впроваджується в медичній сфері телемедицина, електронні медичні картки, роботизовані операції. Банківський сектор використовує цифрові гаманці та блокчейн-рішення. Не менш оцифрованим є і транспортний сектор, у т. ч. залізничний транспорт, завдяки активному застосуванню сучасних цифрових технологій, таких як автоматизовані системи управління рухом, GPS-навігація, електронні квитки, відеоспостереження та аналітика даних. Ці рішення дозволяють оптимізувати графіки руху, підвищити безпеку пасажирів, зменшити витрати на обслуговування та забезпечити більш комфортний сервіс. Зокрема інтелектуальні системи моніторингу стану колій та рухомого складу дозволяють виявляти несправності ще до того, як вони стануть критичними. Пасажири мають змогу купувати квитки онлайн, відстежувати прибуття поїздів у реальному часі та отримувати сповіщення про зміни в розкладі. Штучний інтелект та машинне навчання реалізують можливості прогнозування пасажиропотоку, що допомагає оптимально планувати маршрути та розподіляти ресурси. Завдяки таким змінам залізничний транспорт стає не лише ефективнішим, а й більш адаптивним до потреб сучасного суспільства. Проте, як і в інших сферах, цифровізація загострює питання кібербезпеки, розширюючи цифровий простір і кількість точок вразливості. Кожен новий пристрій, підключений до мережі, може стати потенційною мішенню для кіберзлочинців. Збільшення обсягів даних, що зберігаються та передаються, створює ризики витоку інформації, атак на інфраструктуру та порушення приватності. Разом з цим слід враховувати і те, що кібератаки на транспортну інфраструктуру можуть мати і більше серйозні наслідки, ніж в інших сферах, призводити до збоїв у русі транспортних засобів і створювати загрозу життю пасажирів.

Окрім безпосередньо кібератак (віруси, трояни, програми-вимагачі (ransomware), DDoS-атаки, які паралізують роботу сайтів і сервісів, зломи серверів, баз даних, облікових записів) слід вказати і на загрозу витоку даних. Зважаючи на зростання цінності персональних та корпоративних даних, які сьогодні виступають стратегічним ресурсом, вони дедалі частіше стають об'єктом кіберзагроз шляхом ненавмисного або навмисного розголошення конфіденційної інформації, недостатнього захисту хмарних сховищ або внутрішніх систем, втрати пристроїв з незашифрованими даними, соціальної інженерії. Серед інших кіберзагроз варто виділити маніпуляції з метою отримання доступу до систем через людський фактор, фішинг (підроблені листи або сайти, що змушують користувача розкрити паролі), вішинг (голосові шахрайства) та смішинг (SMS-шахрайства). Достатньо масштабна за наслідками кібератака на сервіси АТ "Укрзалізниця" відбулася 27 березня 2025 року, коли вантажні та пасажирські онлайн-платформи перестали працювати. Якщо роботу останніх було відновлено доволі оперативно, то для забезпечення повноцінної роботи вантажних онлайн-сервісів знадобилося набагато більше часу, протягом якого документи на перевезення вантажів оформлювалися в паперовому вигляді [7]. Зазначене дозволяє дійти висновку, що цифрова трансформація вимагає стратегічного підходу, який передбачає не просто впровадження нових технологій, а й їх безпечне використання. Тому в умовах цифрових викликів важливо приділити увагу вивченню поняття та інструментів цифрової безпеки підприємств залізничного транспорту.

Серед науковців питання забезпечення цифрової безпеки нині набуло доволі широкого поширення. Так, Обрамич О. [4], відзначаючи надзвичайно важливу роль системи цифрової безпеки на підприємстві, розглядає останню як сукупність методологічних, правових та ресурсних компонентів, які, завдяки управлінським рішенням, сприяють мінімізації ризиків і формуванню безпечного середовища для ефективного використання, обробки та зберігання інформації на підприємстві. Згідно з результатами дослідження [3], успішне функціонування підприємств у цифровій економіці потребує системного підходу до управління загрозами економічної безпеки. Експертний аналіз дозволив автору виокремити ключові стратегії, які сприяють зміцненню економічної стійкості компаній в умовах інформаційних викликів, серед яких: стратегії зростання, вибіркового посилення, адаптації, трансформації та відновлення. Як зазначає дослідник, застосування цих стратегій дозволяє підприємствам формувати цілісну систему економічної безпеки, здатну ефективно протистояти ризикам цифрової епохи [3].

У дослідженні [5] запропоновано методичний підхід до трактування поняття "цифрова безпека підприємства" як стану захищеності його функціональних елементів у процесі ведення господарської діяльності в умовах цифровізації та високої конкуренції. При цьому підкреслено, що цифрова безпека охоплює комплекс заходів і методів, спрямованих на мінімізацію внутрішніх та зовнішніх ризиків, пов'язаних з електронним бізнесом, а також на забезпечення стабільності ключових бізнес-процесів. Запропоновано вченим і стратегічні кроки щодо забезпечення цифрової безпеки держави: на законодавчому рівні закріпити визначення поняття "цифрова безпека підприємства", окреслити її функціональні компоненти, об'єкти захисту та суб'єкти, що беруть участь у реалізації відповідної стратегії; стимулювати підприємства до переходу на нові бізнес-моделі через розвиток партнерств і колаборацій у сфері цифрової безпеки.

Авторами публікації [1] не лише здійснено грунтовний аналіз загроз економічній безпеці українських підприємств в умовах впровадження ними цифрових технологій, але і визначено шляхи їх можливого нівелювання. Зокрема в напрямі забезпечення безпеки цифрових систем запропоновано розвивати внутрішній ринок розроблення, використання та споживання різного роду цифрових технологій. При цьому, на думку авторів, важливою є роль держави, яка використовуючи податкові механізми в змозі забезпечити зниження вартості цифрових технологій, засобів та обладнання.

Шостак Л., Федонюк А. та Помазун О. детально досліджують явище та роль кібербезпеки в системі формування бізнес-моделі підприємства в умовах цифрової економіки, зазначаючи, що інноваційні бізнес-моделі, засновані на цифрових технологіях, стимулюють економічне зростання та забезпечують конкурентоспроможність підприємств. Однак, вчені наполягають і на важливості врахування того факту, що поряд із можливостями зростають і ризики, пов'язані з кібербезпекою.

Для захисту цифрових активів і забезпечення цифрової безпеки підприємства науковцями запропоновано реалізовувати такі стратегії [6]:

— стратегія захисту даних — передбачає впровадження механізмів шифрування, регулярне створення резервних копій, а також використання інших технологій для збереження цілісності та конфіденційності інформації;

— стратегія кібербезпеки — базується на застосуванні сучасних систем захисту, антивірусного програмного забезпечення, а також постійному моніторингу та аналізі потенційних кіберзагроз;

— стратегія відновлення — включає розробку та тестування планів реагування на інциденти, впровадження рішень для швидкого відновлення даних і функціонування цифрової інфраструктури;

— стратегія нульової довіри — передбачає перехід до моделі безпеки, яка обмежує доступ до критично важливих застосунків, даних і внутрішнього середовища підприємства, незалежно від джерела запиту.

Наведені дослідження підкреслюють важливість забезпечення цифрової безпеки як на рівні окремої особистості, так і підприємства та держави. При цьому варто враховувати, що цифрова безпека грунтується на таких фундаментальних принципах, які визначають якість захисту інформаційних систем, як:

по-перше, конфіденційність, що означає здатність системи забезпечити доступ до інформації лише уповноваженим особам або процесам. Конфіденційність передбачає: захист персональних даних користувачів (наприклад, паспортні дані, медична інформація, фінансові реквізити); захист комерційної та службової інформації (бізнес-плани, внутрішні документи, технологічні розробки); використання шифрування, обмеження доступу, автентифікації та політик доступу (наприклад, система купівлі електронного квитку на залізниці повинна гарантувати, що дані пасажира не потраплять до сторонніх осіб;

по-друге, цілісність, яка передбачає, що дані залишаються точними, повними та незмінними без дозволу. Це важливо для запобігання несанкціонованому редагуванню або підробці інформації, виявлення змін у даних (наприклад, через контрольні суми або журнали змін), захисту баз даних, журналів подій, фінансових звітів. Наприклад, якщо особа, що здійснює протиправну діяльність у цифровому середовищі залізниці, зможе змінити розклад руху поїздів, система має зафіксувати, хто і коли вніс зміни;

по-третє, доступність, яка гарантує, що інформаційні ресурси та сервіси доступні користувачам у необхідний для них час. Це включає: захист від DDoS-атак, які можуть паралізувати роботу систем; резервне копіювання та аварійне відновлення; забезпечення стабільної роботи серверів, мереж і додатків. Тобто, наприклад, пасажир повинен мати змогу придбати квиток онлайн у будь-який час, без перебоїв у роботі сайту, незважаючи на кібератаки.

Для реалізації перелічених принципів цифрової безпеки на залізничному транспорті доцільно використовувати як технічні, так і організаційні та юридичні засоби та підходи. Серед технічних засобів ключовими є: антивірусне програмне забезпечення (виявляє та нейтралізує шкідливі програми); фаєрволи (мережеві екрани, які контролюють вхідний і вихідний трафік, блокуючи небезпечні запити); системи виявлення та запобігання вторгненням (IDS/IPS, що аналізують поведінку в мережі та реагують на підозрілі дії); шифрування (забезпечує захист даних при передачі та зберіганні). Неможливо сформувати ефективну систему цифрової безпеки і без організаційних заходів, тобто управлінських та процедурних дій, які формують культуру безпеки: політики безпеки (внутрішні правила щодо доступу, зберігання та обробки даних); аудит безпеки (регулярна перевірка систем на відповідність стандартам і виявлення вразливостей); навчання персоналу (підвищення обізнаності працівників щодо кіберзагроз, фішингу, безпечного поводження з даними); план реагування на інциденти (алгоритм дій у разі порушення безпеки). Щодо юридичних аспектів цифрової безпеки, то вони регулюються законодавством і міжнародними стандартами: GDPR (регламент захисту персональних даних, що накладає обов'язки на організації щодо обробки даних в країнах ЄС); ISO/IEC 27001 (міжнародний стандарт управління інформаційною безпекою); українське законодавство (Закон України "Про захист персональних даних", нормативи Державної служби спеціального зв'язку та захисту інформації України, вимоги до критичної інфраструктури). Наприклад, АТ "Укрзалізниця" при обробці персональних даних пасажирів країн ЄС повинна дотримуватися вимог GDPR.

Отже, наразі цифрову безпеку можна розглядати як сукупність технологічних, організаційних та правових заходів, спрямованих на захист інформаційних систем, даних та об'єктів цифрової інфраструктури від несанкціонованого доступу, втрат, пошкоджень або зловмисного використання. Це охоплює захист персональних даних, конфіденційної інформації, цифрових пристроїв, мереж, програмного забезпечення та онлайн-сервісів. Тобто, на сучасному етапі встановити антивірусні програми чи системи захисту паролів вже недостатньо, цифрова безпека включає стратегії управління ризиками, реагування на інциденти, навчання користувачів, постійне вдосконалення захисних механізмів.

Значну роль у цифровій безпеці відіграє людський фактор, що зумовлено її значущістю у виконанні кожного процесу на підприємстві і забезпеченні його ефективного розвитку. Слід вказати і на те, що технічні засоби захисту часто виявляються недостатніми без належної поведінки користувачів, оскільки саме люди (персонал та топ-менеджмент) приймають рішення, взаємодіють із системами, відкривають файли, переходять за посиланнями, і тим самим можуть як зміцнити, так і підірвати безпеку підприємства. Недостатня обізнаність щодо особливостей виникнення та протікання і масштабності наслідків кіберзагроз, нехтування правилами кібергігієни, використання слабких паролів або небезпечних пристроїв в цілому посилює вразливість підприємств, яку не завжди можна нейтралізувати технічними засобами. Тому ефективна система цифрової безпеки має включати не лише технології, а й культуру безпеки, навчання персоналу, тренінги, інтерактивні симуляції та інші заходи, що формують відповідальну поведінку в цифровому середовищі. Так, підприємства залізничного транспорту можуть щоквартально прово-

дити навчання для персоналу щодо нових кіберзагроз, а також тестувати їх готовність через реалізацію інтерактивних симуляцій, зокрема щодо фішингових атак. Таке інвестування в обізнаність, навчання та створення культури безпеки підприємств галузі дозволить суттєво знизити ймовірність кіберінцидентів.

Зважаючи на зростаючу складність кіберзагроз та масштабність їх наслідків і еволюцію цифрових технологій, все більш активно використовуються проактивні, багаторівневі і адаптивні моделі захисту.

Одним із таких підходів є Zero Trust Architecture (принцип "нульової довіри"), який базується на припущенні, що жоден користувач, пристрій або система не повинні отримувати довіру за замовчуванням, навіть якщо знаходяться всередині корпоративної мережі. При цьому доступ має надаватися лише після ретельної перевірки ідентичності, контексту та рівня ризику. З огляду на це ключовими рисами такого підходу є: постійна верифікація користувачів і пристроїв; мінімізація прав доступу; сегментація мережі та контроль трафіку між зонами; моніторинг поведінки в реальному часі. Значним потенціалом володіє дана концепція і в аспекті застосування для підприємств залізничного транспорту, дозволяючи ізолювати системи управління рухом, обмежити доступ до SCADA-компонентів і зменшити ризик внутрішніх загроз.

Цікавою в контексті посилення цифрової безпеки підприємств залізничного транспорту є мультифакторна автентифікація (MFA), що передбачає підтвердження особи, вимагаючи щонайменше два незалежні фактори автентифікації з трьох можливих категорій: що користувач знає (пароль, PIN); що він має (смартфон, токен, смарт-карта), ким він є (біометричні дані: відбиток пальця, розпізнавання обличчя). Серед переваг такого підходу слід виділити значне зниження ризику компрометації облікових записів, ефективний захист від фішингу та крадіжки паролів, гнучкість у впровадженні. У контексті транспортної галузі MFA може бути критично важливою для захисту доступу до систем бронювання, диспетчерських панелей та внутрішніх порталів.

Бізнес-суб'єкти також використовують і шифрування даних, перетворюючи їх у форму, недоступну для несанкціонованих осіб. У сучасних системах шифрування застосовується як на етапі зберігання, так і під час передачі. При цьому можуть застосуватися різні типи шифрування: асиметричне (з відкритим ключем), яке використовується для захищеної передачі даних; симетричне, що ефективне для шифрування великих обсягів інформації; гібридне, яке передбачає поєднання симетричного та асиметричного шифрування; End-to-end (наскрізне або кінцеве), яке забезпечує, що лише відправник і отримувач мають доступ до вмісту повідомлення. Використання методу шифрування сприяє захисту персональних та фінансових даних, відповідає вимогам регуляторів (GDPR, ISO/IEC 27001, тощо), зменшує наслідки витоку даних. При цьому слід враховувати, що незважаючи на їх ефективність, вони не є абсолютно стійкими, їх можливо зламати за належної спрямованості та витрати ресурсів [8, 9].

Із зростанням популярності хмарних технологій виникає потреба в специфічних підходах до захисту даних та сервісів у хмарі. Ключовими аспектами так званої "хмарної" безпеки є: контроль доступу до хмарних ресурсів; шифрування даних у хмарних сховищах; моніторинг активності та виявлення аномалій; резервне копіювання та відновлення після інцидентів; відповідність стандартам (SOC 2, ISO/IEC 27017, тощо). Однак, слід враховувати і певні виклики: розподілена відповідальність між провайдером і користувачем; ризики неправильного налаштування доступу; потенційна залежність від сторонніх постачальників. Оскільки дедалі більше систем (аналітика трафіку, продаж квитків, відеоспостереження тощо) переміщуються в хмару для залізничного транспорту безпека таких середовищ є критично важливою.

Вивчення сутності та характерних рис підходів до цифрової безпеки дозволяє дійти висновку, що вони грунтуються на принципах гнучкості, багаторівневого захисту та постійного моніторингу. Їх впровадження дозволяє не лише зменшити ризики, а й підвищити довіру до цифрових сервісів, особливо в критичних галузях, таких як транспорт у цілому та залізнична галузь зокрема.

Цікавим і перспективним для впровадження підходом до цифрової безпеки на підприємствах залізничного транспорту може стати вище розглянута концепція Zero Trust Architecture у поєднанні з цифровим моніторингом критичних об'єктів інфраструктури. Оскільки саме такий підхід дозволить врахувати специфіку залізничного транспорту, а саме: розгалуженість систем, мобільність об'єктів, високі вимоги до безперервності роботи і протидії сучасним кіберзагрозам. Реалізувати такий підхід у залізничній галузі можна шляхом ідентифікації користувачів і пристроїв через багатофакторну автентифікацію, сегментації мережі шляхом поділу на ізольовані зони (наприклад, системи управління рухом, білетні сервіси, внутрішній документообіг), контролю доступу на основі розподілу ролей (кожен співробітник має доступ лише до потрібних функцій), моніторингу та аналізу поведінки через виявлення аномалій у реальному часі.

Беручи до уваги той факт, що підприємства залізничного транспорту мають багато фізичних об'єктів (локомотиви, станції, депо), які можуть бути вразливими до атак через IoT-пристрої, SCADA-системи, слід посилити систему протидії кіберзагрозам цифровим моніторингом критичних об'єктів. Це можна практично втілити за рахунок встановлення цифрових сенсорів з захищеним каналом передачі даних, використання AI/ML для прогнозування інцидентів (перевантаження мережі чи спроби несанкціонованого доступу), інтеграції з підрозділом Держспецзв'язку CERT-UA для оперативного реагування на кіберінциденти. Також, можна застосовувати блокчейн-технології для захисту логістичних даних, резервні цифрові платформи для управління рухом у разі атаки. Для формування та розвитку культури цифрової безпеки доцільно впроваджувати гейміфікацію навчання з кібербезпеки для працівників.

## ВИСНОВКИ

Виявлено ключові кіберзагрози для суб'єктів економічної діяльності, у т. ч. і залізничної галузі. Ідентифіковано та розкрито принципи забезпечення цифрової безпеки підприємств залізничного транспорту. Підкрес-

лено, що для реалізації принципів цифрової безпеки на залізничному транспорті доцільно використовувати як технічні, так і організаційні та юридичні засоби та підходи. Запропоновано розглядати цифрову безпеку як сукупність технологічних, організаційних та правових заходів, спрямованих на захист інформаційних систем, даних та об'єктів цифрової інфраструктури від несанкціонованого доступу, втрат, пошкоджень або зловмисного використання. Зважаючи на зростаючу складність кіберзагроз та масштабність їх наслідків і еволюцію цифрових технологій, доведено доцільність застосування проактивних, багаторівневих і адаптивних моделей захисту (підхід Zero Trust Architecture, мультифакторна автентифікація, шифрування даних, специфічні підходи до захисту даних та сервісів у "хмарі"). На підприємствах залізничного транспорту запропоновано впровадження концепції Zero Trust Architecture у поєднанні з цифровим моніторингом критичних об'єктів інфраструктури, що дозволить врахувати специфіку залізничного транспорту, а саме: розгалуженість систем, мобільність об'єктів, високі вимоги до безперервності роботи і протидії сучасним кіберзагрозам. Реалізувати такий підхід у залізничній галузі запропоновано шляхом ідентифікації користувачів і пристроїв через багатофакторну автентифікацію, сегментації мережі шляхом поділу на ізольовані зони (наприклад, системи управління рухом, білетні сервіси, внутрішній документообіг), контролю доступу на основі розподілу ролей (кожен співробітник має доступ лише до потрібних функцій), моніторингу та аналізу поведінки через виявлення аномалій у реальному часі.

Література:

1. Воловельська І. В., Мазіашвілі А. Р. Проблеми економічної безпеки підприємств України в умовах глобальної цифровізації. Вісник економіки транспорту і промисловості. 2024. № 85. С. 51—57.

2. Дикань В. Л., Остапюк Б. Б., Черниш В. В. Ризикорієнтоване управління підприємством: сучасні виклики та можливості. Вісник економіки транспорту і промисловості. 2025. № 90. С. 9—18.

3. Кульчицький І. І. Цифрова економіка та економічна безпека підприємства: стратегії управління. Актуальні питання економічних наук. 2024. № 6. URL: https://a-economics.com.ua/index.php/home/article/view/123 (дата звернення: 12.10.2025).

4. Обрамич О. Особливості формування цифрової безпеки на підприємстві. Економіка та суспільство. 2024. Вип. 68. URL: https://economyandsociety.in.ua/index.php/journal/article/view/4872/4812 (дата звернення: 12.10.2025).

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

6. Шостак Л., Федонюк А., Помазун О. Кібербезпека в системі формування бізнес-моделі підприємства в умовах цифрової економіки. Економіка та суспільство. 2024. Вип. 64. URL: https://economyandsociety.in.ua/index.php/journal/article/view/4240/4166 (дата звернення: 15.10.2025).

7. "Укрзалізниця" відновила низку важливих онлайн-послуг після кібератаки. Unian.ua: веб-сайт. URL: https://www.unian.ua/economics/transport/ukrzaliznicya-vidnovila-nizku-vazhlivih-onlayn-poslug-pislya-kiberataki-12963453.html (дата звернення: 17.10.2025).

8. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються? Hostpro.ua: вебсайт. URL: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/ (дата звернення: 17.10.2025).

9. Що таке end-to-end шифрування, яке часто згадують, говорячи про месенджери? Cip.gov.ua: веб-сайт. URL: https://cip.gov.ua/ua/news/sho-take-end-to-end-shifruvannya-yake-chasto-zgaduyut-govoryachi-pro-mesendzheri (дата звернення: 17.10.2025).

References:

1. Volovelska, I.V. and Maziashvili, A.R. (2024), "Problems of economic security of Ukrainian enterprises in the context of global digitalization", Visnyk ekonomiky transportu i promyslovosti, vol. 85, pp. 51—57.

2. Dykan, V.L., Ostapyuk, B.B. and Chernysh, V.V. (2025), "Risk-oriented enterprise management: modern challenges and opportunities", Visnyk ekonomiky transportu i promyslovosti, vol. 90, pp. 9—18.

3. Kulchytskyi, I.I. (2024), "Digital economy and economic security of the enterprise: management strategies", Aktualni pytannia ekonomichnykh nauk, [Online], vol. 6, available at: https://a-economics.com.ua/index.php/home/article/view/123 (Accessed 12 Oct 2025).

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 12 Oct 2025).

5. Perederii, T.S. (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. Shostak, L., Fedoniuk, A. and Pomazun, O. (2024), "Cybersecurity in the system of enterprise business model formation in the digital economy", Ekonomika ta suspilstvo, [Online], vol. 64, available at: https://economyandsociety.in.ua/index.php/journal/article/view/4240/4166 (Accessed 15 Oct 2025).

7. UNIAN (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).

8. Hostpro.ua (2024), "Encryption: types and algorithms. What are they, how do they differ, and where are they used?", available at: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/ (Accessed 17 Oct 2025).

9. State Service of Special Communications and Information Protection of Ukraine (2024), "What is end-to-end encryption, often mentioned when talking about messengers?", available at: https://cip.gov.ua/ua/news/sho-take-end-to-end-shifruvannya-yake-chasto-zgaduyut-govoryachi-pro-mesendzheri (Accessed 17 Oct 2025).

*Стаття надійшла до редакції 27.10.2025 р.*