УДК 005.334:658.012.8:004.056.5
JEL: M12; M13; M19
DOI: https://doi.org/10.32983/2222-4459-2026-5-617-625

ВПЛИВ ВИКЛИКІВ КІБЕРБЕЗПЕКИ НА СИСТЕМУ КОРПОРАТИВНОГО МЕНЕДЖМЕНТУ ПІДПРИЄМСТВ

©2026 КОНОНЕНКО О. В., НЕДЕЛКОВА Є. Б.

УДК 005.334:658.012.8:004.056.5
JEL: M12; M13; M19

Кононенко О. В., Неделкова Є. Б. Вплив викликів кібербезпеки на систему корпоративного менеджменту підприємств

У статті досліджено теоретичні та прикладні аспекти впливу викликів кібербезпеки на систему корпоративного менеджменту підприємств в умовах цифровізації економіки та зростання глобальних кіберзагроз. Розглянуто еволюцію наукових підходів до розуміння ролі інформації, цифрових технологій і мережевих систем у сучасному бізнес-середовищі на основі концепцій економіки знань, мережевого суспільства, цифрової довіри та блокчейн-технологій. У роботі узагальнено наукові підходи до трактування кібербезпеки як стратегічного елементу корпоративного управління та визначено її як комплексну систему захисту інформаційного капіталу підприємства, що забезпечує безперервність бізнес-процесів, економічну стійкість і репутаційну надійність компанії. Досліджено вплив сучасних кіберзагроз на ефективність управлінських процесів, фінансову стабільність та організаційну структуру підприємств. Обґрунтовано необхідність інтеграції кібербезпеки в систему стратегічного менеджменту підприємства та визначено роль поведінкового менеджменту, культури кібергігієни та принципів цифрової довіри в забезпеченні корпоративної стійкості. Встановлено, що сучасні системи управління інформаційною безпекою мають базуватися на адаптивності, превентивному контролі ризиків та постійному моніторингу цифрового середовища. У статті запропоновано авторський механізм перед-аудиту як інструмент превентивного управління кіберризиками на підприємстві. Розкрито етапи його реалізації на основі принципу найменших привілеїв, розмежування обов'язків та ревізії прав доступу до корпоративних інформаційних ресурсів. Практична апробація механізму на прикладі Компанії А підтвердила його ефективність у мінімізації інсайдерських ризиків, оптимізації системи внутрішнього контролю, зменшенні downtime та підвищенні рівня економічної безпеки підприємства. Досліджено перспективи автоматизації перед-аудиту із використанням технологій штучного інтелекту, що дозволить здійснювати прогнозування кіберризиків, оперативний моніторинг цифрового периметра та формування сценаріїв реагування на потенційні інциденти. Визначено, що інтеграція механізмів кібербезпеки в корпоративний менеджмент є необхідною умовою забезпечення конкурентоспроможності підприємств, розвитку міжнародного партнерства та формування України як безпечного цифрового хабу в умовах післявоєнного відновлення.

Ключові слова: *кібербезпека; корпоративний менеджмент; цифровізація; кіберризики; перед-аудит; інформаційна безпека; цифрова довіра; управління ризиками; кіберстійкість; штучний інтелект.*
Рис.: *3.* ***Табл.:*** *1.* ***Бібл.:*** *15.*

Кононенко Олег Вікторович *– керуючий партнер, ТОВ «НОКС ФІШЕС» (вул. Вербицького, 30а, офіс 10, Київ, 02121, Україна)*
E-mail: *Olepole2009@gmail.com*
ORCID: *https://orcid.org/0000-0003-4058-6272*
Неделкова Євгенія Богданівна *– випускниця ліцею № 124 «Спаський» (вул. Спаська, 16, Київ, 04070, Україна)*
E-mail: *innanedelkova075@gmail.com*
ORCID: *https://orcid.org/0009-0000-3572-1893*

UDC 005.334:658.012.8:004.056.5
JEL: M12; M13; M19

Kononenko O. V., Nedelkova Ye. B. The Impact of Cybersecurity Challenges on the Corporate Management System of Enterprises

The article examines the theoretical and applied aspects of the impact of cybersecurity challenges on the corporate management system of enterprises in the context of economic digitalization and the growth of global cyber threats. The evolution of scientific approaches to understanding the role of information, digital technologies, and network systems in the modern business environment is considered based on the conceptions of the knowledge economy, network society, digital trust, and blockchain technologies. The study summarizes scientific approaches to the interpretation of cybersecurity as a strategic element of corporate governance and defines it as a comprehensive system for protecting the information capital of an enterprise, ensuring business continuity, economic resilience, and the reputational reliability of a company. The impact of modern cyber threats on the efficiency of management processes, financial stability, and the organizational structure of enterprises is examined. The necessity of integrating cybersecurity into the strategic management system of an enterprise is substantiated, and the role of behavioral management, cyber hygiene culture, and digital trust principles in ensuring corporate resilience is determined. It is found that modern information security management systems should be based on adaptability, preventive risk control, and continuous monitoring of the digital environment. The article proposes an authors' pre-audit mechanism as a tool for preventive cyber risk management at an enterprise. The stages of its implementation based on the principle of least privilege, separation of duties, and revision of access rights to corporate information resources are disclosed. The practical testing of the mechanism using the example of Company A confirmed its efficiency in minimizing insider risks, optimizing the internal control system, reducing downtime, and increasing the level of economic security of the enterprise. The prospects for automating the pre-audit process using artificial intelligence technologies are explored, which will enable cyber risk forecasting, real-time monitoring of the digital perimeter, and the development of response scenarios for potential incidents. It is determined that the integration of cybersecurity mechanisms into corporate management is a necessary condition for ensuring enterprise competitiveness, developing international partnerships, and positioning Ukraine as a secure digital hub in the context of postwar recovery.

Keywords: *cybersecurity; corporate management; digitalization; cyber risks; pre-audit; information security; digital trust; risk management; cyber resilience; artificial intelligence.*
Fig.: *3.* ***Tabl.:*** *1.* ***Bibl.:*** *15.*

Kononenko Oleh V. *– Managing Partner, LLC "NOK'S FISHES" (office 10, 30a Verbytskoho Str., Kyiv, 02121, Ukraine)*
E-mail: *Olepole2009@gmail.com*
ORCID: *https://orcid.org/0000-0003-4058-6272*
Nedelkova Yevheniia B. *– Graduate of Lyceum No. 124 "Spasky" (16 Spaska Str., Kyiv, 04070, Ukraine)*
E-mail: *innanedelkova075@gmail.com*
ORCID: *https://orcid.org/0009-0000-3572-1893*

У 2025–2026 роках цифрова трансформація та активне впровадження штучного інтелекту істотно змінили зміст корпоративного управління: кібербезпека перестала бути лише технічною функцією та стала стратегічним чинником економічної стійкості підприємства. Захищеність інформаційних активів безпосередньо впливає на безперервність бізнес-процесів, інвестиційну привабливість, репутацію та здатність компанії діяти в умовах воєнних і ринкових ризиків. Для України ця проблематика є особливо актуальною через гібридну агресію РФ і необхідність зближення управлінських практик із вимогами Європейського Союзу.

Впровадження ISO/IEC 27001, дотримання вимог NIS2 і застосування ризик-орієнтованих підходів стають передумовою виходу українських компаній на європейські цифрові ринки та зниження трансакційних витрат на довіру. Менеджмент має розглядати кібербезпеку крізь призму цифрового лідерства, відповідальності керівництва та проактивного управління ризиками. Це означає перехід від ситуаційного реагування на інциденти до постійного аналізу цифрового периметра, критичних активів і ролей працівників. Такий підхід відповідає NIST Cybersecurity Framework 2.0, у якому функція GOVERN закріплює кіберризики на рівні політик, ролей і контролю керівництва [9]. Водночас, за висновками World Economic Forum, у 2025 році кіберпростір ускладнюється через геополітичну нестабільність, розвиток нових технологій, взаємозалежність ланцюгів постачання та професіоналізацію кіберзлочинності [11]. Отже, кібербезпека має оцінюватися як управлінська категорія, що впливає на довіру партнерів, вартість компанії та її здатність підтримувати безперервність діяльності.

ISO/IEC 27001:2022 визначає вимоги до створення, підтримання й удосконалення системи управління інформаційною безпекою відповідно до масштабу та ризикового профілю організації [13]. Директива NIS2, своєю чергою, розглядає кібербезпеку як елемент управлінської відповідальності суб'єктів, важливих для економічної та суспільної стійкості ЄС [14].

У післявоєнному відновленні України надійний корпоративний захист цифрових даних стане умовою інституційної довіри міжнародних партнерів. Здатність бізнесу впроваджувати вимоги кіберстійкості дозволить позиціонувати Україну як безпечний цифровий хаб і підвищити конкурентоспроможність вітчизняних підприємств у глобальному економічному просторі.

Аналіз останніх досліджень і публікацій. Проблематика кібербезпеки в корпоративному менеджменті активно досліджується у працях зарубіжних і вітчизняних учених. Теоретичні засади інформаційного суспільства та цифрової економіки розкрито у працях М. Кастельса [1] і К. Шваба [2], а трансформацію бізнес-процесів під впливом цифрових технологій і блокчейну – у працях Д. Тапскотта, А. Тапскотта [3]. Прикладний вимір проблеми представлено в NIST Cybersecurity Framework 2.0 [9], ENISA Threat Landscape 2024 [10], Global Cybersecurity Outlook 2025 [11] та IBM Cost of a Data Breach Report 2025 [12], де кіберризики розглядаються як фактор управлінської, фінансової та інституційної стійкості організації.

В українському науковому полі питання цифрової трансформації кібербезпеки на мікрорівні в умовах воєнного стану досліджено у працях К. М. Краус, Н. М. Краус та О. В. Штепи [4]. Роль кібербезпеки у сталому функціонуванні суб'єктів цифрової економіки висвітлено С. Комовою [5], а проблематику інноваційної безпеки та оцінювання індикаторів безпечного функціонування промислових систем – у роботі О. І. Маслак і співавторів [6].

Попри значну кількість досліджень, недостатньо розробленими залишаються механізми інтеграції кібербезпеки саме в систему корпоративного управління підприємством. У наукових і прикладних роботах часто переважає технічний або нормативний підхід, тоді як управлінський вимір – розподіл відповідальності, культура кібергігієни, контроль доступів, роль керівництва та економічна оцінка наслідків інцидентів – потребує глибшого узагальнення. Саме тому актуальним є пошук інструментів, які поєднують технічний захист із фінансовою, організаційною та репутаційною стійкістю бізнесу.

Формулювання мети та методів дослідження. ***Метою статті*** є узагальнення теоретичних під-

ходів і обґрунтування впливу викликів кібербезпеки на систему корпоративного менеджменту підприємства в умовах цифрової трансформації, воєнної нестабільності та посилення вимог до операційної й економічної стійкості бізнесу.

Методологічну основу становлять аналіз і синтез, порівняльний метод, системний підхід, індукція, дедукція та узагальнення. Аналіз і синтез використано для вивчення еволюції поглядів на роль інформації, цифрових технологій і кібербезпеки в управлінні. Порівняльний метод дав змогу зіставити підходи П. Друкера, М. Кастельса, К. Шваба, Д. Тапскотта та інших дослідників. Системний підхід дозволив розглянути кібербезпеку як елемент корпоративного менеджменту, що взаємодіє з фінансовою, організаційною, технологічною, кадровою та репутаційною складовими підприємства. Індукція та дедукція застосовані для формування висновків про доцільність переходу від реактивної моделі захисту до превентивного управління кіберризиками. Практичний аспект забезпечено прикладним аналізом Компанії А та обґрунтуванням механізму перед-аудиту як інструменту, який дозволяє виявляти слабкі місця в системі доступів до моменту виникнення інциденту.

Наукова новизна полягає в уточненні сутності кібербезпеки як стратегічної складової корпоративного менеджменту, що забезпечує захист інформаційного капіталу, безперервність бізнес-процесів, економічну стійкість і репутаційну надійність компанії. Удосконалено підхід до управління правами доступу через принцип найменших привілеїв, розмежування обов'язків і регулярну ревізію цифрового периметра. Подальшого розвитку набув підхід до інтеграції кібербезпеки в корпоративне управління через поєднання технологічних, організаційних і поведінкових інструментів.

Виклад основного матеріалу дослідження. Фундаментальне переосмислення ролі інформації в менеджменті пов'язане з ідеями П. Друкера, який розглядав інновацію як ключовий інструмент підприємництва, а здатність до навчання – як головну компетентність XXI століття [7]. У цифровій економіці ці положення набувають нового змісту: інформація перетворюється на нематеріальний капітал підприємства, а кібербезпека стає системою його захисту. Отже, цифрова грамотність і кібергігієна мають входити до професійної компетентності сучасного менеджера.

Концепція мережевого суспільства М. Кастельса пояснює, чому контроль інформаційних потоків стає джерелом організаційної влади [1]. У цифровому середовищі підприємство існує не як ізольована структура, а як вузол мережі, що пов'язує працівників, клієнтів, постачальників, фінансові установи та державні сервіси. Тому кібератака здатна порушити не лише окрему інформаційну систему, а й усю логіку взаємодії між учасниками бізнес-процесу. Втрата доступу до даних, компрометація облікових записів або зупинка сервісів може спричинити фінансові втрати, репутаційний удар і втрату довіри партнерів. Саме тому захист даних переходить із площини технічного адміністрування у площину стратегічного корпоративного управління. К. Шваб у праці про Четверту промислову революцію підкреслює злиття фізичних, цифрових і біологічних систем, що формує нову логіку функціонування підприємств [2]. У таких умовах цифрова довіра стає обов'язковою умовою використання ШІ, автоматизації та платформних бізнес-моделей, а кібербезпека – основою стійкості екосистеми Industry 4.0 (*рис. 1*).

Отже, для менеджменту важливо не тільки впроваджувати нові технології, а й відповідати за їх безпечне, етичне та контрольоване використання. Саме в цьому проявляється управлінський зміст цифрової довіри. Д. Тапскотт і А. Тапскотт, аналізуючи технологію блокчейн, показують, що розподілений реєстр може зменшувати залежність від посередників, підвищувати прозорість операцій і посилювати довіру до цифрових транзакцій [3]. Для корпоративного менеджменту це означає можливість будувати системи обліку, контролю та захисту даних, у яких безпека забезпечується не лише адміністративними процедурами, а й технологічною архітектурою.

Водночас блокчейн не усуває управлінських ризиків автоматично: компанія повинна визначити, хто має право створювати, змінювати, перевіряти та використовувати дані. Отже, технологічна прозорість має доповнюватися чіткою політикою доступів, контролем відповідальності та регулярною перевіркою цифрових процесів. Поняття кіберстійкості можна пояснити через теорію антикрихкості Н. Талеба: стійка система не лише витримує стрес, а й удосконалюється під його впливом [8]. У корпоративному менеджменті це означає, що кожен кіберінцидент або виявлена вразливість мають перетворюватися на джерело навчання. Підприємство повинно не тільки відновлювати роботу після атаки, а й переглядати права доступу, посилювати протоколи, аналізувати поведінку персоналу та оновлювати сценарії реагування. Такий підхід формує адаптивну систему управління інформаційною безпекою, здатну ставати сильнішою після кризових впливів.

Для України ця логіка має особливе значення, адже національний цифровий простір фактично функціонує як «кібер-полігон», де кібератаки по-

Рис. 1. Концептуальна модель трансформації бізнес-моделей за К. Швабом: роль кібербезпеки в екосистемі Industry 4.0

Джерело: розроблено Неделковою Є. на основі [2].

єднуються з фізичними та інформаційними загрозами. Підприємства змушені одночасно підтримувати операційну діяльність, захищати клієнтські дані, забезпечувати дистанційні процеси та взаємодіяти з державними електронними сервісами. Звіт ENISA Threat Landscape 2024 виділяє серед ключових загроз для європейського кіберпростору атаки на доступність, ransomware та загрози даним [10], що підтверджує необхідність адаптивного менеджменту і планів безперервності бізнесу. Для українських компаній кіберстійкість стає не лише питанням відповідності стандартам, а й умовою економічного виживання.

Важливим напрямом є інтеграція поведінкового менеджменту в кіберзахист. Людський фактор доцільно розглядати не лише як джерело помилок, а як елемент захисної стратегії: культура кібергігієни, відповідальне ставлення до даних і чіткі правила доступу мають стати частиною корпоративних цінностей. Працівник, який розуміє цінність інформації та межі власних повноважень, знижує ризик випадкового витоку, фішингового компрометування або порушення внутрішніх процедур. Тому навчання персоналу, регулярні інструктажі та зрозумілі політики доступу повинні доповнювати технічні засоби захисту.

Окреме значення має штучний інтелект як інструмент предиктивного менеджменту. ШІ може допомагати виявляти аномалії, оцінювати потенційні економічні наслідки інцидентів і формувати сценарії відновлення. Наприклад, алгоритми можуть відстежувати нетипову активність користувачів, різке зростання запитів до баз даних або нехарактерне використання хмарних сервісів. Водночас застосування ШІ підвищує вимоги до контролю доступів, якості даних і відповідальності керівництва, оскільки автоматизовані рішення можуть посилювати як захисні можливості підприємства, так і ризики помилкової або неконтрольованої обробки інформації.

Механізм перед-аудиту пропонується розглядати як прикладний інструмент попереднього аналізу системи управління доступами. Його мета – ще до виникнення інциденту виявити слабкі місця цифрового периметра, надлишкові повноваження, організаційні розриви

та ризики Shadow IT. На відміну від класичного аудиту, який часто фіксує стан системи за результатом перевірки, перед-аудит має управлінський і превентивний характер: він дає керівництву можливість побачити, які саме ролі, підрозділи або процеси створюють додаткові ризики. Такий підхід знижує невизначеність у взаємодії підрозділів, переводить кібербезпеку з реактивної у проактивну модель і може застосовуватися компаніями різного масштабу [5].

В основу перед-аудиту покладено принцип найменших привілеїв (*Principle of Least Privilege*). Його реалізація передбачає три етапи: інвентаризацію користувачів і функціональних ролей; виявлення надлишкових прав доступу; динамічний перерозподіл і регулярну ревізію повноважень. На *першому етапі* формується актуальна картина відповідальності працівників і фактичного обсягу їхніх повноважень. На *другому етапі* фіксуються ризикові доступи: наприклад, доступ технічного персоналу до фінансової звітності, наявність активних облікових записів звільнених співробітників або право редагування даних у працівників, які виконують лише функцію перегляду. На *третьому етапі* проводиться коригування прав, встановлюється регулярність перевірок і забезпечується розмежування обов'язків (*Separation of Duties*).

Оптимізація доступів мінімізує ризики несанкціонованого витоку, навмисного пошкодження даних і деструктивної інсайдерської активності. Внутрішні загрози є особливо небезпечними, оскільки інсайдер володіє знанням про структуру системи, правила моніторингу та розподіл даних. Наслідки таких дій можуть проявлятися поступово: від некоректного редагування інформації до втрати клієнтських баз, пошкодження інтелектуальної власності або зупинки окремих бізнес-процесів. Перед-аудит дозволяє превентивно захистити нематеріальні активи, скоротити час простою бізнесу (*downtime*) та зменшити витрати на відновлення після інцидентів [6]. Імплементація перед-аудиту спрощує підготовку до сертифікації за ISO/IEC 27001, оскільки попередньо структурує політики доступу, розподіл відповідальності, оцінювання ризиків, контрольні заходи та постійне поліпшення СУІБ [13]. Для менеджменту це важливо, адже сертифікація потребує не лише наявності технічних засобів захисту, а й документованого розуміння ризиків, процедур реагування та відповідальних осіб. Водночас цей інструмент узгоджується з логікою NIST CSF 2.0, яка передбачає встановлення, комунікацію та моніторинг політик кіберризику на рівні організації [9]. Отже, перед-аудит не замінює сертифікаційний аудит, але формує практичну карту підготовки до нього.

Для апробації механізму обрано Компанію А з трирівневою структурою управління: генеральним, операційним і технічним директоратами. Підприємство функціонально поділено на комерційний, технічно-виробничий та адміністративний департаменти. Діагностика «точки нуль» виявила, що основні вразливості пов'язані з некоректною диференціацією прав доступу до корпоративних даних. Окремі працівники мали ширший доступ, ніж вимагали їхні посадові функції, а частина сервісів використовувалася без достатнього контролю з боку адміністрації. Такий стан знижував операційну ефективність і створював ризики для економічної безпеки підприємства.

На базі досліджуваного підприємства було реалізовано перед-аудит за авторським алгоритмом (*рис. 2*). У ході верифікації облікових записів виявлено близько 20% надлишкових повноважень і випадки використання несанкціонованих цифрових сервісів (*Shadow IT*). Це свідчить про наявність не лише технічних, а й управлінських прогалин: відсутність своєчасного перегляду ролей, недостатній контроль за життєвим циклом облікових записів і нечітке розмежування відповідальності між підрозділами.

Економічний ефект перед-аудиту (*рис. 3*) полягає у зменшенні потенційних збитків, захисті клієнтських баз, комерційної таємниці та інтелектуальної власності. Це особливо важливо з огляду на IBM Cost of a Data Breach Report 2025, за яким середня глобальна вартість витоку даних становить 4,44 млн дол. США [12]. Регуляторний аспект посилюється тим, що GDPR покладає на контролерів і процесорів обов'язок забезпечувати захист персональних даних [15], а NIS2 – управлінську відповідальність за кіберстійкість [14]. Оперативне блокування доступів звільнених співробітників зменшує ризики інсайдерської активності та витоку конфіденційних активів. Скорочення часу відновлення після внутрішніх інцидентів підвищує операційну прибутковість, а результати перед-аудиту формують доказову базу для подальших інвестицій у цифровий захист і підготовку до зовнішнього аудиту.

Для керівництва це має практичне значення, оскільки дає змогу обґрунтовувати витрати на кібербезпеку не абстрактними загрозами, а конкретними показниками: кількістю надлишкових доступів, критичністю даних, вартістю простою та потенційними санкціями за порушення регуляторних вимог.

Рис. 2. Етапи реалізації механізму перед-аудиту в Компанії А

Джерело: розроблено Неделковою Є.

Подальша еволюція перед-аудиту пов'язана з автоматизацією на базі штучного інтелекту (*AI-driven auditing*). Така система може автономно виявляти аномалії, формувати прогностичні сценарії та порівнювати економічні наслідки збереження вразливостей із ефектом від упровадження коректив. Для великих компаній це дає можливість перейти від періодичних перевірок до постійного моніторингу цифрового периметра. Механізм адаптується до масштабу компанії (*табл. 1*): малому бізнесу достатньо мінімальних прав і періодичних перевірок; середнім підприємствам потрібне розмежування обов'язків; великим корпораціям – регулярний контроль критичних даних; міжнародним компаніям – автоматизація аудиту, багаторівневий моніторинг і постійне оновлення карти ризиків.

Стратегічним кроком може стати впровадження перед-аудиту для державних підприємств та об'єктів критичної інфраструктури, зокрема енергетичного сектора. Це посилить національну кіберстійкість, забезпечить контроль державних інформаційних ресурсів і зменшить ризики несанкціонованого втручання. У сфері критичної інфраструктури наслідки кіберінцидентів виходять за межі окремої організації, оскільки можуть впливати на безперервність енергопостачання, логістику, фінансові операції та доступ громадян до важливих сервісів. У такому вимірі перед-аудит трансформується з корпоративного інструменту в елемент захисту економічних інтересів і соціальної стабільності.

Впровадження перед-аудиту може посилити інтеграцію українських компаній у Єдиний цифровий ринок ЄС. За умов відповідності європейським стандартам кіберстійкості, зокрема NIS2, такий механізм слугує доказом надійності ланцюга постачання, зменшує витрати на підтвердження відповідності й підвищує довіру іноземних контрагентів. Для партнерів і донорів важливо бачити не лише декларацію про захист даних, а й наявність внутрішніх процедур контролю, регулярної ревізії доступів і відповідальності керівництва. У післявоєнному відновленні це сприятиме формуванню інституційної довіри, залученню інвестицій і позиціонуванню України як безпечного цифрового хабу, здатного працювати в умовах підвищених ризиків.

У дослідженні проаналізовано трансформацію кібербезпеки з технічної функції у стратегічний елемент корпоративного менеджменту. Встановле-

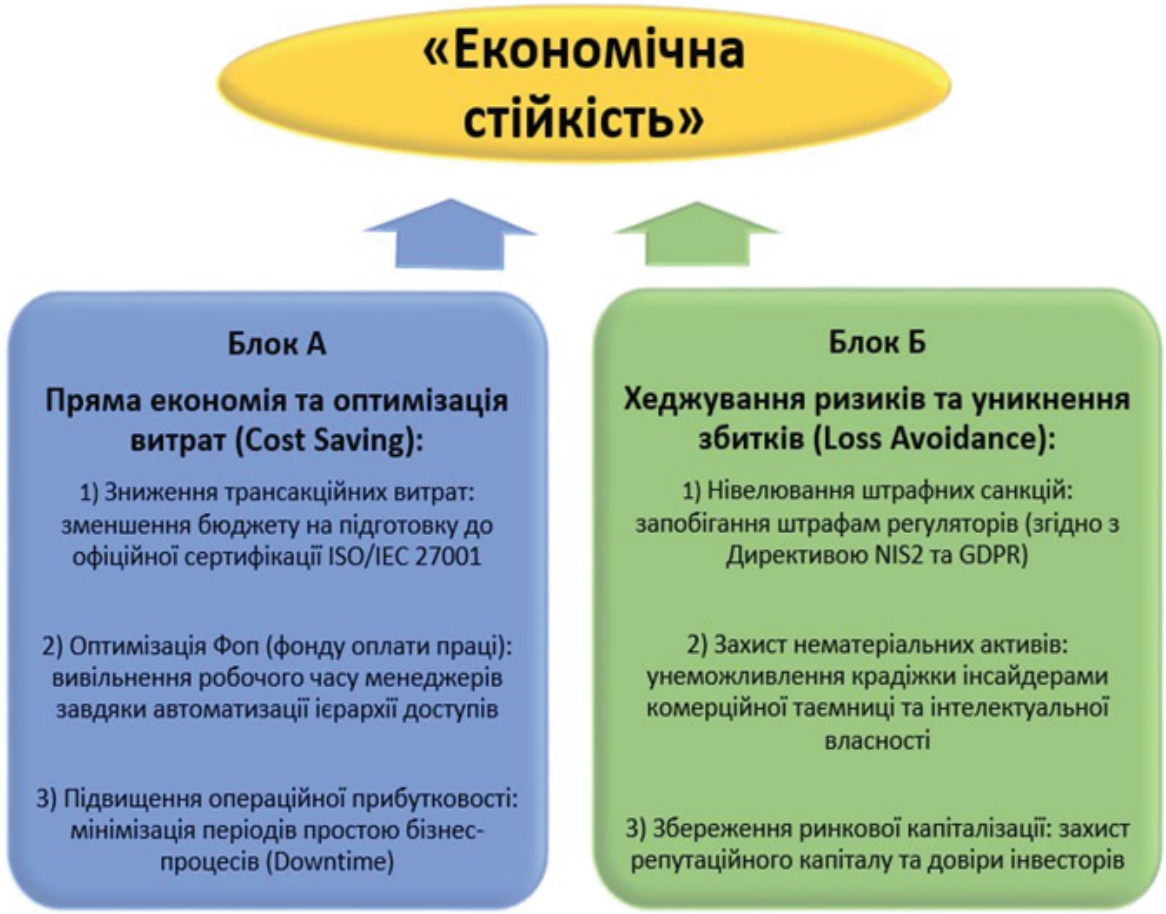

Рис. 3. Модель оцінки економічної ефективності та окупності (ROI) перед-аудиту

Джерело: розроблено Неделковою Є.

Таблиця 1

Інструкція по використанню інструменту перед-аудиту відповідно до управлінської структури компанії

Тип компанії	Структура	Рівень доступу	Основні рекомендації перед-аудиту
Малий бізнес	Простий / Лінійний	Центральний	Мінімальні права, перевірка 1–2 рази на рік
Середнє підприємство	Департаментне	Частково делегований	Розмежування обов'язків, ревізія 2–4 рази на рік
Велика корпорація	Матрична / Складна	Централізований з делегуванням	Контроль критичних даних, щоквартальні ревізії
Міжнародна корпорація	Децентралізована / Глобальна	Багаторівневий	Автоматизація аудиту, постійний контроль ризиків

Джерело: розроблено Неделковою Є.

но, що сучасні кіберінциденти впливають не лише на ІТ-інфраструктуру, а й на фінансову стабільність, репутацію, безперервність бізнес-процесів та інвестиційну привабливість підприємства. Саме тому кібербезпека повинна включатися до системи стратегічного планування, а не розглядатися як допоміжна функція окремого технічного підрозділу. Узагальнення концепцій економіки знань, цифрової довіри, мережевого суспільства й антикрихкості підтвердило, що інформація є ключовим нематеріальним активом, а її захист – умовою створення вартості. Кібербезпека інтегрується в корпоративну культуру, систему прийняття управлінських рішень і політику взаємодії з партнерами. У сучасних умовах довіра до підприємства формується не лише якістю продукції чи фінансовими

показниками, а й здатністю гарантувати цілісність, доступність і конфіденційність даних.

Практична частина засвідчила доцільність авторської методології перед-аудиту, заснованої на принципі найменших привілеїв, ревізії доступів і розмежуванні обов'язків. Запропонований підхід дозволяє превентивно знижувати фінансові, операційні та репутаційні ризики та може бути адаптований до підприємств різного масштабу. Керівництво отримує зрозумілий інструмент оцінки слабких місць цифрового периметра, а підприємство – основу для підготовки до сертифікації, зовнішнього аудиту та інтеграції до європейського цифрового ринку. Отже, кібербезпека є необхідною умовою стійкого розвитку бізнесу та формування України як безпечного цифрового партнера. ■

БІБЛІОГРАФІЯ

1. Castells M. The Rise of the Network Society: The Information Age: Economy, Society and Culture. Vol. 1. 2nd ed. Chichester : Wiley-Blackwell, 2010. 656 p. URL: https://urb.bme.hu/wp-content/uploads/2014/05/manuel_castells_the_rise_of_the_network_societybookfi-org.compressed.pdf
2. Schwab K. The Fourth Industrial Revolution. Geneva : World Economic Forum, 2016. 172 p. URL: https://law.unimelb.edu.au/__data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf
3. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York : Portfolio, 2016. 324 p. URL: https://itig-iraq.iq/wp-content/uploads/2019/05/Blockchain_Revolution.pdf
4. Краус К. М., Краус Н. М., Штепа О. В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability*. 2022. № 3. С. 26–37. DOI: https://doi.org/10.31649/ins.2022.3.26.37
5. Комова С. Кібербезпека в цифровій економіці. *Сталий розвиток міст* : матеріали XVI Всеукраїнської студентської науково-технічної конференції. Ч. 3. Харків : ХНУМГ ім. О. М. Бекетова, 2023. С. 66–68. URL: https://science.kname.edu.ua/images/dok/konferentsii/stalyirozvytok2019/2023/Ch3-Economica_23.pdf#page=67
6. Maslak O. I., Maslak M. V., Grishko N. Y., Yaroslava Y. Y., Hlazunova O. O., Pirogov D. L. Innovative Safety of the Ukrainian Electrical Industry: Benchmarking Indicators for Provision. *2021 IEEE International Conference on Modern Electrical and Energy Systems (MEES)*. Kremenchuk, Ukraine, 2021. P. 1–5. DOI: https://doi.org/10.1109/MEES52427.2021.9598492
7. Drucker P. F. Innovation and Entrepreneurship: Practice and Principles. New York : HarperBusiness, 2006. 288 p.
8. Taleb N. N. Antifragile: Things That Gain from Disorder. New York : Random House, 2012. 581 p.
9. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, 2024. 32 p. DOI: https://doi.org/10.6028/NIST.CSWP.29
10. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024. Athens : ENISA, 2024. DOI: https://doi.org/10.2824/0710888
11. World Economic Forum. Global Cybersecurity Outlook 2025. Geneva : World Economic Forum, 2025. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
12. IBM Security. Cost of a Data Breach Report 2025. Armonk : IBM Corporation, 2025. URL: https://www.ibm.com/reports/data-breach
13. International Organization for Standardization. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : ISO, 2022. URL: https://www.iso.org/standard/27001
14. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive). *Official Journal of the European Union*. 2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Official Journal of the European Union*. 2016. L 119. P. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

REFERENCES

Castells M. (2010). *The Rise of the Network Society: The Information Age: Economy, Society and Culture*. Wiley-Blackwell, Chichester. https://urb.bme.hu/wp-content/uploads/2014/05/manuel_castells_the_rise_of_the_network_societybookfi-org.compressed.pdf

Drucker P. F. (2006). *Innovation and Entrepreneurship: Practice and Principles*. HarperBusiness, New York.

European Parliament & Council of the European Union (2022, December 14). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive). *Official Journal of the European Union*, *L 333*, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

European Parliament & Council of the European Union (2016, April 27). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Official Journal of the European Union, L 119*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

European Union Agency for Cybersecurity (2024). *ENISA Threat Landscape 2024*. ENISA, Athens. https://doi.org/10.2824/0710888

IBM Security. (2025). *Cost of a Data Breach Report 2025*. IBM Corporation, Armonk. https://www.ibm.com/reports/data-breach

International Organization for Standardization. (2022). ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection* – Information security management systems – Requirements. ISO, Geneva. https://www.iso.org/standard/27001

Komova S. (2023). Kiberbezpeka v tsyfrovii ekonomitsi [Cybersecurity in the digital economy]. *Stalyi rozvytok mist*: materialy XVI Vseukrainskoi studentskoi naukovo-tekhnichnoi konferentsii. Ch. 3 [Sustainable development of cities: materials of the XVI All-Ukrainian student scientific and technical conference. Part 3] (p. 66–68). KhNUMH im. O. M. Beketova, Kharkiv. https://science.kname.edu.ua/images/dok/konferentsii/stalyirozvytok2019/2023/Ch3-Economica_23.pdf#page=67

Kraus K. M., Kraus N. M. & Shtepa O. V. (2022). Tsyfrova transformatsiia kiberbezpeky na mikrorivni v umovakh voiennoho stanu [Digital transformation of cybersecurity at the micro level under martial law]. *Innovation and Sustainability, 3*, 26–37. https://doi.org/10.31649/ins.2022.3.26.37

Maslak O. I., Maslak M. V., Grishko N. Y., Yaroslava Y. Y., Hlazunova O. O. & Pirogov D. L. (2021). Innovative Safety of the Ukrainian Electrical Industry: Benchmarking Indicators for Provision. *2021 IEEE International Conference on Modern Electrical and Energy Systems (MEES)* (p. 1–5). Kremenchuk, Ukraine. https://doi.org/10.1109/MEES52427.2021.9598492

National Institute of Standards and Technology (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg. https://doi.org/10.6028/NIST.CSWP.29

Schwab K. (2016). *The Fourth Industrial Revolution*. World Economic Forum, Geneva. https://law.unimelb.edu.au/__data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf

Taleb N. N. (2012). *Antifragile: Things That Gain from Disorder*. Random House, New York.

Tapscott D. & Tapscott A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio, New York. https://itig-iraq.iq/wp-content/uploads/2019/05/Blockchain_Revolution.pdf

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*. World Economic Forum, Geneva. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

Стаття надійшла до редакції / Received: 11.05.2026
Статтю прийнято до публікації / Accepted: 24.05.2026
Оприлюднено / Published: 25.06.2026

УДК 656.073:005.21(436:477)
JEL: H54; L91; O18; R41
DOI: https://doi.org/10.32983/2222-4459-2026-5-625-633

СТРАТЕГІЧНЕ УПРАВЛІННЯ РОЗВИТКОМ ВАНТАЖНОГО ТРАНСПОРТУ: АВСТРІЙСЬКА МОДЕЛЬ ТА МОЖЛИВОСТІ ЇЇ АДАПТАЦІЇ В УКРАЇНІ

©2026 **ВЛАСОВА В. П., ТАРНОВСЬКА І. В., ОЛІХНЕНКО М. А.**

УДК 656.073:005.21(436:477)
JEL: H54; L91; O18; R41

Власова В. П., Тарновська І. В., Оліхненко М. А. Стратегічне управління розвитком вантажного транспорту: австрійська модель та можливості її адаптації в Україні

У статті розглянуто австрійську модель стратегічного управління розвитком вантажного транспорту як можливий орієнтир для модернізації української транспортно-логістичної системи. Дослідження зосереджене на визначенні управлінських, інфраструктурних і організаційних елементів цієї моделі, які можуть бути адаптовані в Україні з урахуванням воєнних ризиків, зміни торговельних маршрутів, перевантаження сухопутних кордонів та інтеграції до транспортного ринку ЄС. Методологічну основу роботи становлять системний підхід, порівняльний аналіз, логічне узагальнення, аналіз наукових публікацій, статистичних матеріалів і стратегічних документів Австрії, ЄС та України. Встановлено, що практична цінність австрійської моделі полягає не лише у високій частці залізничних перевезень, а насамперед у поєднанні довгострокової державної стратегії, термінальної інфраструктури, мультимодальних сервісів, цифрової координації, інституційної взаємодії та передбачуваних умов для бізнесу. Обґрунтовано, що пряме механічне перенесення австрійських інструментів в Україну неможливе через відмінності інфраструктурних умов, різну ширину колії, воєнні ризики, обмежений інвестиційний ресурс і нерівномірний розвиток прикордонних потужностей. Водночас для України релевантними є коридорне планування, розвиток сухих портів і мультимодальних хабів, залізнично-автомобільна кооперація, цифровізація процедур, підтримка регулярних інтермодальних сервісів і запровадження системи моніторингу результатів. Наукова новизна полягає в трактуванні австрійського досвіду не як набору окремих інфраструктурних рішень, а як управлінської моделі, що поєднує транспортну політику, логістичну бізнес-логіку, термінальну інфраструктуру та інституційну координацію. Практична цінність дослідження полягає у визначенні орієнтирів для держави, інфраструктурних операторів і логістичних компаній щодо переходу від фрагментарного кризового реагування до стратегічної інтеграції в європейські ланцюги постачання.

Ключові слова: *стратегічне управління; вантажний транспорт; транспортно-логістична система; мультимодальні перевезення; інтермодальні перевезення; сухі порти; логістичні хаби; цифровізація.*

Рис.: *1.* ***Табл.:*** *3.* ***Бібл.:*** *20.*