

DOI: <https://doi.org/10.32782/2308-1988/2025-57-117>

УДК 005.8:004

Комеліна Ольга Володимирівна

доктор економічних наук, професор,
професор кафедри менеджменту і логістики,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
ORCID: <https://orcid.org/0000-0001-9297-4985>

Корунський Володимир Володимирович

магістр,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
ORCID: <https://orcid.org/0009-0009-7176-2495>

Olha Komelina, Volodymyr Korunskyi

National University "Yuri Kondratyuk Poltava Polytechnic"

ЦИФРОВІ ТЕХНОЛОГІЇ ТА ІНСТРУМЕНТИ В ПРОЄКТНОМУ УПРАВЛІННІ ОРГАНІЗАЦІЙНОЮ СТІЙКІСТЮ ПІДПРИЄМСТВ

DIGITAL TECHNOLOGIES AND TOOLS IN PROJECT MANAGEMENT OF ENTERPRISE ORGANIZATIONAL RESILIENCE

Анотація. Стаття присвячена дослідженню ролі цифрових технологій та інструментів у проєктному управлінні організаційною стійкістю суб'єктів управління, а також формуванню адаптивних організаційних систем в умовах цифрових трансформацій. Визначено нові можливості для управління організаційною стійкістю через застосування проєктного підходу. Аргументовано, що інтеграція цифрових інструментів у процеси ризик-менеджменту, антикризового планування, управління змінами та забезпечення безперервності бізнесу дозволяє організаціям не лише підвищити швидкість реагування на загрози, але й перетворити виклики на можливості для розвитку. Запропоновано комплексний методичний підхід щодо впровадження цифрових технологій у проєктному управлінні організаційною стійкістю організацій, що враховує як технологічні, так і управлінські аспекти формування адаптивних організаційних систем. Розроблено пропозиції щодо впровадження цифрових інструментів у підвищення організаційної стійкості великих, середніх та малих підприємств.

Ключові слова: організаційна стійкість, цифрові технології, проєктне управління, управління ризиками, антикризове управління, цифрова трансформація, безперервність бізнесу, адаптивність організації.

Summary. The article explores the role of digital technologies and tools in project management as a key factor in enhancing organizational resilience in enterprises operating under conditions of increasing uncertainty and digital transformation. The study focuses on how project-based management approaches enable organizations to build adaptive and resilient systems capable of anticipating, absorbing, and responding effectively to internal and external disruptions. Particular attention is paid to the integration of digital solutions into risk management, crisis preparedness, change management, and business continuity processes. The paper substantiates that the fragmented implementation of digital tools significantly limits their potential impact on organizational resilience. In contrast, a systemic and integrated application of digital technologies within project management frameworks allows enterprises to improve situational awareness, accelerate decision-making, and strengthen coordination across organizational units. The research highlights the role of advanced digital instruments, including data analytics, artificial intelligence, cloud platforms, and collaborative tools, in supporting proactive risk identification and adaptive response mechanisms. A comprehensive methodological approach to the integration of digital technologies into project management of organizational resilience is proposed. This approach combines technological capabilities with managerial and organizational factors, ensuring alignment between digital initiatives, strategic objectives, and resilience requirements. The study also outlines practical recommendations for the implementation of digital tools aimed at strengthening organizational resilience across enterprises of different sizes, taking into account their resource availability, digital maturity, and operational complexity. The findings contribute to the development of contemporary approaches to project management by emphasizing the strategic importance of digitalization for resilience building and sustainable organizational development.

Keywords: organizational resilience, digital technologies, project management, risk management, crisis management, digital transformation, business continuity, organizational adaptability.

Постановка проблеми. Сучасне світове бізнес-середовище характеризується безпрецедентним рівнем турбулентності та непередбачуваності. Згідно з дослідженням World Economic Forum [16] спектр глобальних ризиків швидко розширюється. До традиційних економічних і демографічних ризиків додалися кліматичні катастрофи, екологічні загрози, енергетичні кризи, геополітичні конфлікти, кібербезпека, цифрова трансформація, соціальна поляризація, технологічні невизначеності тощо. У цих умовах організаційна стійкість, зокрема здатність організації передбачати потенційні загрози, адаптуватися до змін, витримувати кризові ситуації та швидко відновлюватися, перетворюється у критичний чинник конкурентоспроможності. Традиційні підходи до управління ризиками у розвитку організацій виявляються недостатньо ефективними в умовах швидких та непередбачуваних змін. За таких умов цифрова трансформація створює нові можливості для управління організаційною стійкістю. Особливо перспективним є застосування проєктного підходу до управління організаційною стійкістю, який дозволяє структурувати діяльність з підвищення адаптивності організації, встановити чіткі цілі та показники, розподілити ресурси та забезпечити системний контроль за результатами. Проте, існує об'єктивна необхідність у проведенні комплексного дослідження ролі цифрових технологій у проєктному управлінні організаційною стійкістю організацій, що враховує як технологічні, так і управлінські аспекти формування адаптивних організаційних систем.

Аналіз останніх досліджень і публікацій. Проблематика організаційної стійкості посідає важливе місце в сучасних наукових дослідженнях у зв'язку зі зростанням невизначеності, кризових явищ і складності бізнес-середовища. У науковій літературі організаційна стійкість розглядається як здатність організації підтримувати безперервність функціонування, адаптуватися до змін та ефективно реагувати на деструктивні впливи. Зокрема, D. Woods трактує організаційну стійкість як динамічну властивість соціально-технічних систем, що ґрунтується на здатності передбачати, моніторити, реагувати та навчатися в умовах мінливого середовища [17].

Подальший розвиток цих ідей відображено в концепції *resilience engineering*, запропонованій E. Hollnagel, у межах якої організаційна стійкість розглядається як системна спроможність організації управляти варіативністю процесів і складністю, забезпечуючи стабільність функціонування за умов невизначеності [18]. Управлінський вимір організаційної стійкості доповнюється в роботах D. Denyer, де наголошується на необхідності інтеграції стратегічних, операційних і поведінкових аспектів управління [4]. Важливу роль у забезпеченні організаційної стійкості відіграє проєктний

підхід. У публікаціях Project Management Institute (PMI) підкреслюється значення проєктного управління для управління ризиками, організаційними змінами та підвищення гнучкості підприємств [9; 10]. У цьому контексті дослідження високонадійних організацій (High Reliability Organizations) акцентують увагу на розвитку організаційної уважності, чутливості до операційних процесів і гнучкого розподілу повноважень як ключових чинниках стійкості [19; 20].

Окремий напрям досліджень присвячений ролі цифрових технологій у підвищенні організаційної стійкості. Зокрема, обґрунтовується вплив технологій Індустрії 4.0, аналітики даних і цифрової інтеграції на зміцнення стійкості бізнес-процесів і ланцюгів постачання [11; 12; 13]. У вітчизняних дослідженнях організаційна стійкість розглядається в контексті економічної безпеки та адаптивності підприємств в умовах криз і гібридних загроз [6; 8; 14; 15].

Узагальнення результатів аналізу наукових публікацій свідчить про зростаючий інтерес до проблем цифрової трансформації управління організаційною стійкістю. Водночас питання комплексної інтеграції цифрових технологій у систему проєктного управління та оцінювання ефективності таких рішень залишаються недостатньо розробленими, що зумовлює актуальність подальших досліджень у цьому напрямі.

Метою даної статті є дослідження ролі цифрових технологій та інструментів у проєктному управлінні організаційною стійкістю організації, а також розробка практичних рекомендацій щодо їх ефективного застосування.

Виклад основного матеріалу дослідження. Організаційна стійкість (*organizational resilience*) визначається як здатність організації передбачати, готуватися, реагувати і адаптуватися до поступових змін та раптових потрясінь для виживання та процвітання [3; 4]. На відміну від традиційного ризик-менеджменту, який фокусується переважно на запобіганні негативним подіям, концепція організаційної стійкості охоплює також здатність організації використовувати кризові ситуації як можливості для розвитку та трансформації.

Проєктний підхід до управління організаційною стійкістю передбачає структуровану діяльність з чітко визначеними цілями, термінами, ресурсами та результатами, спрямовану на підвищення здатності організації протистояти викликам. Такий підхід має низку переваг: можливість фокусування ресурсів на критичних напрямках, встановлення конкретних показників ефективності, забезпечення міжфункціональної координації та систематичного моніторингу прогресу [9].

Організаційна стійкість формується на кількох рівнях. На стратегічному рівні визначаються ключові загрози та можливості, формується культура стійкості, розробляються політики та процедури.

На тактичному рівні впроваджуються конкретні механізми моніторингу ризиків, системи раннього попередження, плани безперервності бізнесу. На операційному рівні забезпечується готовність персоналу, резервування критичних ресурсів, тестування процедур реагування [2].

Ключовими компонентами ОС є: антиципаційна здатність (здатність передбачати потенційні загрози), адаптивна здатність (здатність гнучко реагувати на зміни), абсорбційна здатність (здатність витримувати удари без критичних пошкоджень) та здатність до відновлення (швидке повернення до нормального функціонування або досягнення нового, більш ефективного стану) [4].

Проектне управління ОС включає кілька типів проектів: проекти оцінки вразливостей та загроз, проекти розробки та впровадження систем моніторингу ризиків, проекти створення планів безперервності бізнесу, проекти навчання та підготовки персоналу, проекти модернізації інфраструктури для підвищення стійкості, проекти цифровізації процесів управління стійкістю.

У сучасній практиці проектного управління ОС використовується широкий спектр цифрових інструментів. Платформи Microsoft Project, Asana, Jira, Monday.com дають змогу структурувати діяльність, забезпечувати прозорість виконання завдань, координацію команд та контроль термінів [10]. Проте їх ефективність зростає лише за умови інтегрованого застосування у межах єдиної системи управління стійкістю. У межах цього дослідження пропонується концептуальний підхід до такої інтеграції, який передбачає узгодження цифрових рішень із ключовими елементами проектного управління стійкістю (моніторингом ризиків, адаптивним плануванням, управлінням ресурсами та механізмами реагування). Такий підхід дозволить сформувати структуру, що дозволяє поєднувати різні цифрові інструменти у цілісну методичну модель, яка раніше була відсутня у практиці управління стійкістю, а також забезпечує її інтеграцію з корпоративними інформаційними платформами. Це дає змогу створити єдиний інформаційний простір для підтримки стійкості організації на всіх етапах життєвого циклу проекту.

Сучасна інтеграція цифрових інструментів у систему проектного управління організаційною стійкістю дасть змогу подолати їх фрагментарність та посилити їх роль загальній системі забезпечення стійкості організації. Зокрема, AI-системи забезпечують аналіз великих обсягів даних з внутрішніх та зовнішніх джерел для виявлення ранніх сигналів потенційних загроз [6]. Алгоритми машинного навчання прогнозують ймовірність настання кризових подій, оцінюють потенційний вплив на організацію та рекомендують превентивні заходи. Natural Language Processing (NLP) дозволяє аналізувати новини, соціальні мережі, звіти експертів для виявлення emerging risks.

Існують також спеціалізовані рішення для управління ризиками (Risk Management Systems), такі як RiskWatch, LogicManager, MetricStream, які інтегрують дані з різних джерел, візуалізують карти ризиків, автоматизують процеси оцінки та моніторингу загроз. Інтерактивні дашборди забезпечують управління ОС актуальною інформацією для прийняття рішень у режимі реального часу [3]. Спеціалізовані рішення для управління кризами (Crisis Management Systems) автоматизують процеси ескалації інцидентів, координації антикризових команд, комунікації зі стейкхолдерами. Ці системи забезпечують структуроване документування подій, аналіз ефективності реагування, накопичення досвіду для майбутніх ситуацій.

Сенсори та IoT-пристрої здійснюють безперервний моніторинг стану критично важливого обладнання, виявляють аномалії, попереджають про потенційні відмови [12]. Це особливо важливо для організацій з високими вимогами до безперервності виробництва. Предиктивне обслуговування на основі IoT-даних знижує ризик непланових простоїв. Технологія розподіленого реєстру забезпечує прозорість та відстежуваність ланцюгів постачання, що критично важливо для швидкого реагування на порушення [11]. Блокчейн дозволяє верифікувати постачальників, контролювати якість продукції, оперативно перебудовувати логістичні маршрути при виникненні проблем.

Використовуються і так звані цифрові двійники для сценарного моделювання. Цей процес передбачає створення віртуальних копій бізнес-процесів, об'єктів інфраструктури або всієї організації дозволяє моделювати різні кризові сценарії без ризику для реального бізнесу. Цифрові двійники використовуються для тестування планів реагування, оптимізації ресурсів, навчання персоналу [4].

Відмітимо, що важливими елементами в сучасному проектному управлінні є хмарні платформи для забезпечення безперервності бізнесу, а також платформи колаборації та комунікації. Cloud computing забезпечує швидке масштабування ресурсів при зростанні навантаження, резервування даних у географічно розподілених центрах, доступ до критичних систем з будь-якої точки світу [1; 13]. Хмарні рішення для disaster recovery дозволяють організувати швидке відновлення IT-систем після збоїв.

Інструменти ж типу Microsoft Teams, Slack, Zoom забезпечують безперервну комунікацію команд, особливо у розподілених організаціях. У кризових ситуаціях ці платформи стають критично важливими для координації дій, швидкого обміну інформацією, прийняття колективних рішень.

Проаналізовані цифрові технології і інструменти впливають на різні компоненти організаційної стійкості (табл. 1) [6; 13].

**Таблиця 1 – Особливості впливу цифрових технологій
і інструментів на забезпечення організаційної стійкості у сучасних умовах**

Компоненти ОС	Опис впливу
Підвищення антиципаційної здатності	Предиктивна аналітика на основі AI та Big Data дозволяє виявляти ранні сигнали потенційних загроз задовго до їх матеріалізації. Організації можуть переходити від реактивного до проактивного управління ризиками, що значно знижує потенційний збиток від кризових ситуацій
Прискорення моніторингу та виявлення інцидентів / ризиків	IoT-сенсори, системи автоматизованого моніторингу, AI-алгоритми виявлення аномалій забезпечують безперервний контроль за критичними параметрами у режимі реального часу. Час від виникнення проблеми до її виявлення скорочується з годин або днів до хвилин або секунд
Оптимізація швидкості реагування	Автоматизовані системи управління інцидентами / ризиками, цифрові протоколи реагування, платформи швидкої комунікації дозволяють організувати координоване реагування на кризові ситуації у значно коротші терміни
Покращення адаптивності через сценарне моделювання	Цифрові двійники та симуляційні системи дозволяють тестувати різні сценарії розвитку подій, оцінювати ефективність альтернативних стратегій реагування, навчати персонал без ризику для реального бізнесу
Забезпечення безперервності критичних бізнес-процесів	Хмарні технології, розподілені системи, дублювання інфраструктури у цифровому форматі дозволяють підтримувати критичні бізнес-процеси навіть у разі пошкодження фізичної інфраструктури або недоступності персоналу
Прискорення відновлення	Автоматизовані процедури backup та recovery, cloud-based disaster recovery рішення дозволяють значно скоротити час відновлення після збоїв
Накопичення та використання організаційного досвіду	Цифрові системи документування інцидентів, аналізу after-action reviews, бази знань створюють основу для організаційного навчання. Machine learning алгоритми виявляють закономірності у попередніх кризах та рекомендують покращення процедур реагування

Джерело: сформовано авторами на основі [4; 9–14]

Важливо зазначити, що використання розглянутих цифрових технологій набуває цінності лише за умови їх інтеграції у єдину систему управління ОС. Така система має передбачати поєднання аналітичних інструментів (AI, ML, NLP), операційних рішень (IoT-моніторинг, предиктивне обслуговування), стратегічних платформ (цифрові двійники, blockchain-контроль ланцюгів постачання) та комунікаційних сервісів. У межах такого підходу цифрові інструменти взаємодіють між собою за принципом «дані – аналіз – рішення – реагування», тобто сенсори формують інформаційний потік, аналітичні алгоритми перетворюють дані у прогнози, цифрові двійники моделюють сценарії реагування, а хмарні середовища та комунікаційні платформи забезпечують координацію дій. Таким чином пропонується методичний підхід забезпечує побудову цілісної архітектури цифрового управління ОС, у якій кожен інструмент підсилює загальну здатність підприємства передбачати, адаптуватися та ефективно діяти в умовах невизначеності. Саме така модель дозволяє перейти від фрагментарного використання діджитал-рішень до інтегрованого методичного підходу, що є критично важливим у сучасному проєктному управлінні.

Проте, незважаючи на значний потенціал цифрових технологій для управління організаційною стійкістю їх впровадження стикається з низкою викликів [6; 8]. Інтеграція цифрових технологій у систему управління стійкістю організації

супроводжується низкою викликів: складністю поєднання сучасних рішень із застарілими legacy-системами, фрагментацією IT-ландшафту, ризиками кібербезпеки, що можуть парадоксально знизити рівень стійкості, а також дефіцитом фахівців із необхідними міждисциплінарними компетенціями. Впровадження цифрових систем часто викликає організаційний опір через зміну звичних процесів і ролей, а ефективність інвестицій важко виміряти, оскільки користь проявляється здебільшого у запобіганні кризам. Додатковими ризиками стають залежність від постачальників технологій (vendor lock-in) і формування «помилкової впевненості» – ілюзії повного контролю над ризиками, що може призвести до недооцінки нових загроз.

Саме тому, для подолання зазначених бар'єрів організаціям необхідно формувати цілісну стратегію цифрової трансформації управління власною організаційною стійкістю. Зокрема, перед впровадженням цифрових інструментів управління стійкістю необхідно провести комплексний аудит поточного стану організаційної стійкості, визначити критичні вразливості та рівень цифрової зрілості, використовуючи міжнародні стандарти, зокрема ISO 22316 або NIST Cybersecurity Framework [15].

Таким чином, узагальнення існуючих досліджень і практик впровадження цифрових технологій і інструментів в забезпечення організаційної стійкості підприємства дає змогу запропонувати

комплексний методичний підхід щодо впровадження цифрових технологій у проєктному управлінні організаційною стійкістю різних суб'єктів управління, що враховує як технологічні, так і управлінські аспекти формування адаптивних організаційних систем. Алгоритм реалізації цього підходу містить такі складові:

1) на основі результатів оцінки формується стратегія цифровізації управління стійкістю з визначенням пріоритетних напрямів, етапів впровадження, ресурсів і узгодження її із загальною стратегією розвитку організації та ІТ-стратегією [7];

2) створюється міжфункціональна проєктна команда, до складу якої входять різні фахівці (фахівці з ІТ-технологій, ризик-менеджменту, безпеки, операційної діяльності та HR-менеджменту під керівництвом досвідченого менеджера трансформаційних проєктів [9]. Впровадження пропонуваного підходу доцільно починати з пілотних проєктів у критичних або найбільш готових до змін областях, що дозволяє протестувати технології, виявити проблеми та продемонструвати швидкі результати;

3) визначаються можливості інтеграції нових цифрових інструментів з існуючими корпоративними системами (ERP, CRM, ITSM), щоб уникнути дублювання даних і забезпечити їх коректність використання [4]. Паралельно варто інвестувати у розвиток компетенцій персоналу, організацію тренінгів і симуляцій кризових ситуацій, формуючи культуру передбачливості, адаптивності та довіри до цифрових рішень [14]. Після успішного завершення пілотних проєктів здійснюється масштабування рішень на всі релевантні бізнес-процеси з урахуванням специфіки кожного підрозділу;

4) забезпечується постійний моніторинг, оновлення інструментів, тестування процедур реагування та аналізу кризових ситуацій [10]; визначається рівень кібербезпеки критичних систем через резервування, шифрування, контроль доступу та регулярні аудити [12];

5) здійснюється вимірювання ефективності ОС: встановлення KPI для оцінки часу реагування, рівня готовності персоналу, швидкості відновлення після інцидентів і результатів нейтралізації загроз, що дозволить підтримувати увагу керівництва та забезпечувати сталий розвиток організаційної системи. Це важливо, адже враховуючи комплексність цифрових рішень та різний характер їхнього впливу на бізнес-процеси, оцінювання ефективності стає критичним інструментом управління стійкістю. Під час цього процесу доцільно застосовувати комбінований підхід, що поєднує кількісні метрики (такі як були згадані: час реагування, частота інцидентів, швидкість відновлення, точність прогнозних моделей тощо) та якісні оцінки (рівень взаємодії команд, ступінь

адаптивності, готовність персоналу працювати з новими технологіями).

Для великих корпорацій доцільно інвестувати у комплексні enterprise-рішення для управління організаційною стійкістю, які інтегруються з корпоративною ІТ-екосистемою та забезпечують централізований контроль усіх бізнес-процесів. Рекомендується створення спеціалізованих підрозділів або центрів компетенцій з організаційної стійкості, що відповідають за координацію дій між функціями ризик-менеджменту, ІТ, безпеки та операцій. Великі корпорації можуть дозволити собі розробку індивідуальних (custom) рішень під власні потреби, включно з впровадженням передових технологій – штучного інтелекту, машинного навчання, цифрових двійників та аналітики великих даних [5]. Такі підходи підвищують здатність передбачати ризики, оперативно реагувати на загрози та забезпечувати гнучкість у кризових умовах.

Для середніх організацій оптимальним варіантом є використання хмарних SaaS-рішень, які не потребують значних капітальних інвестицій, забезпечують швидке впровадження та масштабування [13]. Це створює можливості управління ключовими ризиками та забезпечити безперервність критичних бізнес-процесів, кібербезпеку та стійкість ланцюгів постачання. Корисним може бути також долучення до галузевих платформ обміну інформацією про загрози, інциденти та кращі практики, що сприяє колективній стійкості сектору.

Для малих організацій доцільно починати з впровадження базових, економічно ефективних інструментів – безкоштовних або недорогих систем управління проєктами (Trello, Asana Basic), хмарних рішень для резервного копіювання критичних даних та базових систем моніторингу [8]. Слід використовувати готові шаблони планів безперервності бізнесу та процедур реагування на інциденти, а також розглядати можливість об'єднання з іншими організаціями для спільного користування дорогими цифровими інструментами або послугами зовнішніх провайдерів.

Висновки. Таким чином, представлені результати дослідження щодо оптимізації використання цифрових технологій та інструментів в проєктному управлінні організаційною стійкістю підприємств, а також підхід щодо вимірювання їх результативності та підвищення організаційної стійкості в умовах цифрової трансформації дають змогу подолати існуючі проблеми зміцнення конкурентоспроможності підприємств. Нові цифрові інструменти (технології штучного інтелекту, предиктивної аналітики, Інтернету речей, блокчейну та хмарних обчислень тощо) дозволяють організаціям здійснювати моніторинг ризиків у режимі реального часу, швидко реагувати на зміни середовища, оптимізувати ресурси та забезпечувати безперервність критичних бізнес-процесів.

Список використаних джерел:

1. Al-Ruithe M., Benkhelifa E., Hameed K. A systematic literature review of data governance and cloud data governance. *Personal and Ubiquitous Computing*. 2019. Vol. 23. P. 839–859. DOI: <https://doi.org/10.1007/s00779-017-1104-3>
2. Annarelli A., Battistella C., Nonino F. Product service system: A conceptual framework from a systematic review. *Journal of Cleaner Production*. 2016. Vol. 139. P. 1011–1032. DOI: <https://doi.org/10.1016/j.jclepro.2016.08.061>
3. Duchek, S. Organizational resilience: a capability-based conceptualization. *Business Research* no. 13, pp. 215–246 (2020). DOI: <https://doi.org/10.1007/s40685-019-0085-7>
4. Denyer D. Organizational resilience: A summary of academic evidence, business insights and new thinking. BSI and Cranfield School of Management, 2017. P. 23–45.
5. Toolkit: Digital Twins Use Cases for Achieving Business Value. *Gartner Research*. Gartner Inc., 2024. URL: <https://www.gartner.com/en/documents/5508495>
6. Крючкова І., Мельникова О. Цифрова трансформація як чинник підвищення адаптивності підприємств в умовах невизначеності. *Економіка та держава*. 2021. № 8. С. 42–47. URL: https://www.economy.in.ua/pdf/8_2021/6.pdf
7. Лігоненко Л., Ілляшенко С. Антикризисова стійкість підприємства: теоретичні аспекти та методичні підходи до оцінювання. *Механізм регулювання економіки*. 2020. № 1 (87). С. 80–92. URL: http://mer.fem.sumdu.edu.ua/content/articles/issue_54/Liia_O_Lihonenko_Sviatoslav_M_Illiashenko_Crisis_Resistance_of_Enterprise_Theoretical_Aspects_and_Methodological_Approaches_to_Its_Evaluation.pdf
8. Ляпін А., Руденко О. Особливості проєктного управління в умовах кризи: досвід українських підприємств. *Управління проєктами та розвиток виробництва*. 2022. № 3 (83). С. 23–36. DOI: <https://doi.org/10.31734/management2022.03.023>
9. A guide to the project management body of knowledge (PMBOK® guide). Project Management Institute (PMI). 7th ed. Newtown Square, PA : PMI, 2021. URL: <https://www.pmi.org/pmbok-guide-standards/foundational/pmbok>
10. The standard for organizational project management (OPM). Project Management Institute (PMI). Newtown Square, PA : PMI, 2022. URL: <https://www.pmi.org/standards/organizational-project-management>
11. Joshi P, Tewari V, Kumar S, Singh A (2023), "Blockchain technology for sustainable development: a systematic literature review". *Journal of Global Operations and Strategic Sourcing*, Vol. 16 No. 3 pp. 683–717, DOI: <https://doi.org/10.1108/JGOSS-06-2022-0054>
12. Tortorella G., Fogliatto F., Saurin T., Tlapa D. Contributions of Industry 4.0 to supply chain resilience. *International Journal of Logistics Management*. 2021. Vol. 32. № 4. P. 1327–1349. DOI: <https://doi.org/10.1108/IJLM-12-2020-0494>
13. Belhadi A., Kamble S., Jabbour C.J.C., Gunasekaran A., Ndubisi N.O., Venkatesh M. Manufacturing and service supply chain resilience to the COVID-19 outbreak. *Technological Forecasting and Social Change*. 2021. Vol. 163. 120447. DOI: <https://doi.org/10.1016/j.techfore.2020.120447>
14. Vasylytsiv T., Lupak R. Economic security and resilience of enterprises in the context of hybrid threats: Methodology and assessment tools. *Journal of European Economy*. 2022. Vol. 21. № 1. P. 118–135. DOI: <https://doi.org/10.35774/jee2022.01.118>
15. Хаустова Н. Інноваційні підходи до управління змінами на підприємствах в умовах турбулентності. *Проблеми економіки*. 2023. № 2 (56). С. 189–196. DOI: <https://doi.org/10.32983/2222-0712-2023-2-189-196>
16. The global risks report 2023. World Economic Forum. 18th ed. Geneva : World Economic Forum, 2023. URL: <https://www.weforum.org/reports/global-risks-report-2023>
17. Woods D.D. Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*. 2015. Vol. 141. P. 5–9. DOI: <https://doi.org/10.1016/j.res.2015.03.018>
18. Hollnagel, Erik & Puriès, Jean & Woods, David & Wreathall, J.. (2010). *Resilience Engineering in Practice: A Guidebook. Resilience Engineering in Practice: A Guidebook*.
19. Weick K.E., Sutcliffe K.M. Managing the Unexpected: Sustained Performance in a Complex World. 3rd ed. Wiley, 2015. URL: <https://www.wiley.com/en-us/Managing+the+Unexpected%3A+Sustained+Performance+in+a+Complex+World%2C+3rd+Edition-p-9781118862865>
20. Edmondson A.C. The Fearless Organization: Creating Psychological Safety in the Workplace for Learning, Innovation, and Growth. Wiley, 2018. URL: <https://www.wiley.com/enus/The+Fearless+Organization%3A+Creating+Psychological+Safety+in+the+Workplace+for+Learning%2C+Innovation%2C+and+Growth-p-9781119477242>

References:

1. Al-Ruithe M., Benkhelifa E., Hameed K. (2019) A systematic literature review of data governance and cloud data governance. *Personal and Ubiquitous Computing*, vol. 23, pp. 839–859. DOI: <https://doi.org/10.1007/s00779-017-1104-3>
2. Annarelli A., Battistella C., Nonino F. (2020) Product service system: A conceptual framework from a systematic review. *Journal of Cleaner Production*, vol. 227, pp. 1011–1032. DOI: <https://doi.org/10.1016/j.jclepro.2016.08.061>
3. Duchek, S. (2020) Organizational resilience: a capability-based conceptualization. *Business Research*, no. 13, pp. 215–246. DOI: <https://doi.org/10.1007/s40685-019-0085-7>
4. Denyer D. (2017) Organizational resilience: A summary of academic evidence, business insights and new thinking. BSI and Cranfield School of Management, pp. 23–45.
5. Toolkit: Digital Twins Use Cases for Achieving Business Value. *Gartner Research*. Gartner Inc. (2024). Available at: <https://www.gartner.com/en/documents/5508495>

6. Kriuchkova I., Melnykova O. (2021) Tsyfrova transformatsiia yak chynnyk pidvysshchennia adaptyvnosti pidpriemstv v umovakh nevyznachenosti [Digital transformation as a factor in increasing the adaptability of enterprises in conditions of uncertainty]. *Ekonomika ta derzhava – Economy and State*, vol. 8, pp. 42–47. Available at: https://www.economy.in.ua/pdf/8_2021/6.pdf (in Ukrainian)
7. Lihonenko L., Illiashenko S. (2020) Antykryzova stiikist pidpriemstva: teoretychni aspekty ta metodychni pidkhody do otsiniuvannia [Anti-crisis resilience of the enterprise: theoretical aspects and methodological approaches to evaluation]. *Mekhanizm rehuliuvannia ekonomiky – Mechanism of Economic Regulation*, vol. 1(87), pp. 80–92. Available at: http://mer.fem.sumdu.edu.ua/content/acticles/issue_54/Liia_O_Lihonenko_Sviatoslav_M_Illiashenko_Crisis_Resistance_of_Enterprise_Theoretical_Aspects_and_Methodological_Approaches_to_Its_Evaluation.pdf (in Ukrainian)
8. Liapin A., Rudenko O. (2022) Osoblyvosti proiektnoho upravlinnia v umovakh kryzy: dosvid ukrainskykh pidpriemstv [Features of project management in crisis conditions: experience of Ukrainian enterprises]. *Upravlinnia proiektyamy ta rozvytok vyrobnytstva – Project Management and Production Development*, vol. 3(83), pp. 23–36. DOI: <https://doi.org/10.31734/management2022.03.023> (in Ukrainian)
9. A guide to the project management body of knowledge (PMBOK® guide). Project Management Institute (PMI). 7th ed. Newtown Square, PA : PMI. (2021) Available at: <https://www.pmi.org/pmbok-guide-standards/foundational/pmbok>
10. The standard for organizational project management (OPM). Project Management Institute (PMI). Newtown Square, PA : PMI. (2022). Available at: <https://www.pmi.org/standards/organizational-project-management>
11. Joshi P, Tewari V, Kumar S, Singh A (2023), Blockchain technology for sustainable development: a systematic literature review. *Journal of Global Operations and Strategic Sourcing*, Vol. 16 No. 3 pp. 683–717, DOI: <https://doi.org/10.1108/JGOSS-06-2022-0054>
12. Tortorella G., Fogliatto F., Saurin T., Tlapa D. Contributions of Industry 4.0 to supply chain resilience. *International Journal of Logistics Management*. 2021. Vol. 32. № 4. P. 1327–1349. DOI: <https://doi.org/10.1108/IJLM-12-2020-0494>
13. Belhadi A., Kamble S., Jabbour C.J.C., Gunasekaran A., Ndubisi N.O., Venkatesh M. (2021) Manufacturing and service supply chain resilience to the COVID-19 outbreak. *Technological Forecasting and Social Change*. Vol. 163. DOI: <https://doi.org/10.1016/j.techfore.2020.120447>
14. Vasylytsiv T., Lupak R. (2022) Economic security and resilience of enterprises in the context of hybrid threats: Methodology and assessment tools. *Journal of European Economy*. Vol. 21. № 1. P. 118–135. DOI: <https://doi.org/10.35774/jee2022.01.118>
15. Khaustova N. (2023) Innovatsiini pidkhody do upravlinnia zminamy na pidpriemstvakh v umovakh turbulentnosti [Innovative approaches to change management in enterprises under conditions of turbulence]. *Problemy ekonomiky – Problems of Economy*, vol. 2(56), pp. 189–196. DOI: <https://doi.org/10.32983/2222-0712-2023-2-189-196> (in Ukrainian)
16. The global risks report 2023. World Economic Forum. 18th ed. Geneva: World Economic Forum. (2023). Available at: <https://www.weforum.org/reports/global-risks-report-2023>
17. Woods D. D. (2015) Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, vol. 141, pp. 5–9. DOI: <https://doi.org/10.1016/j.ress.2015.03.018>
18. Hollnagel, Erik & Pariès, Jean & Woods, David & Wreathall, J. (2010). Resilience Engineering in Practice: A Guidebook. Resilience Engineering in Practice: A Guidebook.
19. Weick K. E., Sutcliffe K. M. (2015) Managing the Unexpected: Sustained Performance in a Complex World. 3rd ed. Wiley. Available at: <https://www.wiley.com/en-us/Managing+the+Unexpected%3A+Sustained+Performance+in+a+Complex+World%2C+3rd+Edition-p-9781118862865>
20. Edmondson A. C. (2018) The Fearless Organization: Creating Psychological Safety in the Workplace for Learning, Innovation, and Growth. Wiley. Available at: <https://www.wiley.com/enus/The+Fearless+Organization%3A+Creating+Psychological+Safety+in+the+Workplace+for+Learning%2C+Innovation%2C+and+Growth-p-9781119477242>

Стаття надійшла до редакції 12.12.2025