

УДК 658:330.341.1

DOI: https://doi.org/10.31521/modecon.V52(2025)-35

Шандова Н. В., доктор економічних наук, професор, завідувач кафедри економіки, підприємництва та економічної безпеки, Херсонський національний технічний університет, м. Хмельницький, Україна

ORCID ID: 0000-0002-6278-1143

e-mail: shandova.nataliya@kntu.edu.ua

Рибась Д. Є., здобувач третього (освітньо-наукового) рівня вищої освіти, Херсонський національний технічний університет, м. Хмельницький, Україна

ORCID ID: 0009-0003-8413-9535

e-mail: rybas.denys@kntu.net.ua

Моделі формування конкурентних стратегій економічної безпеки підприємств малого та середнього бізнесу в умовах цифрової трансформації

Анотація. У статті розглянуто теоретичні та прикладні аспекти формування конкурентних стратегій економічної безпеки підприємств малого та середнього бізнесу (МСП) в умовах цифрової трансформації. Актуальність дослідження зумовлена тим, що зростання кіберзагроз, обмежений доступ до фінансування цифрових технологій та швидкі зміни ринкового середовища суттєво підвищують вразливість МСП, особливо в постконфліктних економіках, таких як Україна. Традиційні підходи до забезпечення економічної безпеки, зосереджені переважно на фізичних та фінансових ризиках, виявляються недостатніми в умовах цифрової економіки, де ключовими активами стають дані, технології та швидкість адаптації.

Метою дослідження є розробка та обґрунтування моделей конкурентних стратегій економічної безпеки МСП, які інтегрують цифрові технології (штучний інтелект, хмарні сервіси, fintech-рішення) та забезпечують стійкість бізнесу до зовнішніх і внутрішніх загроз.

Результати дослідження показали, що запропонована гібридна модель конкурентних стратегій складається з чотирьох взаємопов'язаних компонентів: оцінки цифрових ризиків, інтеграції інноваційних технологій, адаптивного стратегічного планування та моніторингу ефективності через ключові показники (KPI). Особливу увагу приділено розробці концепції гібридного цифрового кооперативу (ГЦК), який дозволяє об'єднувати ресурси МСП для колективної цифровізації та підвищення економічної стійкості. Такий підхід знижує витрати на впровадження технологій, сприяє зростанню продуктивності, зменшує втрати від кібератак та відкриває доступ до глобальних ринків.

Запропоноване дослідження відзначається тим, що адаптовано існуючі концепції цифрової трансформації та економічної безпеки до умов постконфліктної економіки України з акцентом на кіберзагрози та обмежені ресурси підприємств. Практичне значення отриманих результатів полягає у можливості застосування запропонованої моделі як інструменту стратегічного планування для МСП та формування основи для розвитку цифрових екосистем на базі державних ініціатив.

Отримані результати можуть бути використані як основа для подальших досліджень у сфері цифрової безпеки бізнесу, формування державної політики підтримки МСП та розробки інноваційних механізмів кооперації підприємств у цифровому середовищі.

Ключові слова: економічна безпека; конкурентні стратегії; цифрова трансформація; МСП; кіберзагрози; інноваційні моделі; гібридний цифровий кооператив; стратегічне планування.

Shandova Nataliia, Doctor of Economics, Professor, The Head of the Department of Economy, Entrepreneurship and Economic security, Kherson National Technical University, Khmelnytskyi, Ukraine

Rybas Denys, Graduate student of the third (educational and scientific) level of higher education, Kherson National Technical University, Khmelnytskyi, Ukraine

Models of Forming Competitive Strategies for the Economic Security of SMEs under Digital Transformation

Abstract. Introduction. The article addresses the challenges faced by small and medium-sized enterprises (SMEs) in the context of digital transformation, which increases both opportunities for growth and risks to economic security. Rapid technological changes, limited access to financing, low digital skills, and rising cyber threats make traditional approaches to economic security insufficient, particularly in post-conflict economies such as Ukraine.

Purpose. The aim of the study is to develop and substantiate models of competitive strategies for ensuring the economic security of SMEs under conditions of digital transformation, with a focus on integrating advanced technologies such as artificial intelligence, cloud services, and fintech solutions to enhance resilience and competitiveness.

¹ Стаття надійшла до редакції: 27.08.2025

Received: 27 August 2025

Results. Based on a systemic approach that combines comparative analysis and modeling, the article proposes a hybrid model of competitive strategies consisting of four interrelated components: digital risk assessment, technology integration, adaptive strategic planning, and performance monitoring through key performance indicators (KPIs). A distinctive feature of the proposed model is the introduction of a Hybrid Digital Cooperative (HDC), which allows SMEs to pool financial and technological resources, access advanced digital tools on a subscription basis, and benefit from collective knowledge sharing. This cooperative mechanism reduces the individual cost of digitalization, enhances resilience against cyber threats, fosters innovation through shared platforms, and opens opportunities for internationalization. The results demonstrate that such an approach not only mitigates risks but also transforms economic security into a sustainable source of competitive advantage, particularly in the context of Ukraine's post-conflict recovery and integration into the global digital economy.

Conclusions. The study emphasizes that the application of the proposed model can transform economic security into a source of competitive advantage for SMEs. For Ukraine, this approach is particularly relevant as it helps overcome financial and technological constraints, supports post-conflict recovery, and creates prerequisites for the development of digital ecosystems based on state initiatives. The results can serve as a basis for further research in digital business security, SME support policies, and innovative cooperation mechanisms in the digital economy.

Keywords: economic security, competitive strategies, digital transformation, small and medium-sized enterprises (SMEs), cyber threats, innovation models, hybrid digital cooperative, strategic planning.

JEL Classification: L26; M21; G32; O33

Постановка проблеми. У сучасних умовах цифрової трансформації малі та середні підприємства (МСП) стикаються з серйозними викликами, що загрожують їхній економічній безпеці. Зростання кіберзагроз, які спрямовані на 46% бізнесів із чисельністю працівників до 1000 осіб [1], обмежений доступ до фінансування цифрових технологій, особливо в країнах, що розвиваються [2], а також швидкі зміни ринкових умов ускладнюють збереження конкурентоспроможності. Традиційні підходи до забезпечення економічної безпеки, зосереджені на фізичних і фінансових ризиках, не враховують специфіки цифрового середовища, що вимагає розробки нових моделей, які інтегрують цифрові інструменти для захисту бізнесу та посилення його позицій на ринку. Пропонованим рішенням є створення адаптивних моделей конкурентних стратегій економічної безпеки МСП, які базуються на використанні хмарних сервісів, штучного інтелекту (AI) та fintech-рішень. Ці моделі передбачають оцінку цифрових ризиків, оптимізацію ресурсів через цифрові платформи та формування стратегій, що поєднують економічну стабільність із конкурентними перевагами.

У світі такі підходи вже демонструють ефективність. Наприклад, у США 60% МСП використовують хмарні технології, а 25% застосовують AI для аналізу даних і прогнозування ризиків, що сприяє щорічному зростанню продуктивності діяльності на 3-5% [3]. У Кореї 55% МСП інтегрують fintech для підвищення фінансової стійкості, а в Німеччині 50% промислових МСП використовують Інтернет речей (IoT) для оптимізації виробництва [4]. Ці приклади показують, як цифрові інструменти дозволяють МСП знижувати ризики та зміцнювати конкурентні позиції. Однак в Україні впровадження подібних моделей ускладнене через обмежений доступ до фінансування (лише 15% МСП отримують кредити на цифровізацію [2]), низький рівень цифрових навичок (лише 30% МСП мають базові цифрові компетенції [5]) та зростання кібератак (у 2023 році збільшення відбулося на 20% [6]). Постконфліктна економіка та нестабільність додатково ускладнюють інтеграцію цифрових рішень.

Попри ці виклики, Україна має значний потенціал для реалізації таких моделей завдяки державним ініціативам, зокрема, Дія.Бізнес, які сприяють цифровізації МСП, та доступу до відкритих даних через платформи, такі як Є-data [5]. Зростання IT-сектору, який забезпечує 5% ВВП у 2023 році, та підтримка міжнародних організацій, таких як OECD і World Bank, створюють сприятливі умови для впровадження цифрових технологій [7]. Впровадження моделей конкурентних стратегій на основі цифрових інструментів сприятиме відновленню МСП, підвищенню їхньої стійкості до криз і конкурентоспроможності на глобальних ринках. Цифрові рішення дозволять оптимізувати витрати, зменшити втрати від кіберзагроз на 15-20% [6] та розширити ринки через e-commerce і fintech-платформи, що є ключовим для постконфліктного економічного відновлення. Таким чином, дослідження моделей формування конкурентних стратегій економічної безпеки МСП в умовах цифрової трансформації є актуальним, оскільки воно відповідає глобальним тенденціям, вирішує нагальні виклики української економіки та відкриває перспективи для сталого розвитку бізнесу в умовах невизначеності.

Аналіз останніх досліджень та публікацій. Основні аспекти проблеми формування конкурентних стратегій економічної безпеки для підприємств малого та середнього бізнесу в умовах цифрової трансформації формуються навколо інтеграції цифрових технологій, таких як штучний інтелект, хмарні обчислення та Інтернет речей, для посилення стійкості бізнесу до ризиків, включаючи кіберзагрози та ринкові зміни, що дозволяє МСП не лише виживати, але й набирати конкурентні переваги через підвищення продуктивності та інноваційності. У науковій літературі ці аспекти найчастіше розглядаються через призму систематичних оглядів, які аналізують стратегії впровадження цифрових інструментів, бар'єри для МСП та їх вплив на економічну стабільність, з акцентом на емпіричні дані з розвинених економік, таких як ЄС, США та Азія, де цифровізація розглядається як ключовий фактор зростання. Також підкреслюється,

що МСП часто застосовують поступові стратегії цифрової трансформації, починаючи з базових ІКТ, таких як електронна пошта та соціальні мережі, перед переходом до складніших технологій, але стикаються з викликами, такими як, брак ресурсів і навичок, що загрожує їхній конкурентоспроможності та економічній безпеці [8]. Огляд, проведений на основі європейських МСП з порівнянням з США та Азією, показує, що успішні стратегії включають лідерство та розвиток екосистем, але потребують подальших крос-регіональних досліджень для адаптації до локальних контекстів [8].

Значний внесок у вивчення проблеми формування конкурентних стратегій економічної безпеки зробили дослідники Andrea Meier, Robert Eller та Mike Peters [9], які розробили концептуальну рамку для підвищення конкурентоспроможності МСП через цифрову трансформацію, базуючись на критичному реалізмі, де цифровізація виступає ключовим чинником набуття конкурентних переваг, хоча й залежить від технічних, організаційних та культурних факторів, і запропонували багаторівневий план досліджень для емпіричного тестування цих зв'язків. Аналогічно, у науковій праці [10], ґрунтованій на теорії ендогенного зростання, виділено ключові фактори успіху, такі як організаційне навчання, лідерство та співпраця, а також зроблено акцент на фінансовій грамотності та поступових інноваціях для подолання обмежень МСП, що безпосередньо пов'язано з формуванням конкурентних стратегій через вирівнювання ІТ з бізнес-цільями. Організація економічного співробітництва та розвитку (ОЕСР) у своєму звіті 2021 року [4] детально аналізує можливості та виклики цифрової трансформації для МСП, фокусуючись на питаннях цифрової безпеки, таких як, кібератаки та ризики даних, які посилюються пандемією COVID-19, і підкреслює, що МСП, становлячи 99% бізнесів, відстають у впровадженні цифрових технологій через брак інвестицій, але можуть набути відповідних конкурентних переваг через платформи та блокчейн, якщо подолають такі бар'єри, як відсутність навичок та обмеженість фінансування. Дослідження Diana Teresa Parra-Sanchez та колег [11], базоване на сціентометричному аналізі 448 документів, підтверджує зростання інтересу до теми конкурентних стратегій економічної безпеки, виділяючи технології для підвищення продуктивності МСП, такі як AI та великі дані, і наголошує на необхідності рамок готовності до Industry 4.0 для забезпечення конкурентоспроможності та зменшення екологічного впливу. Крім того, аналіз впливу пандемії COVID-19 на цифрову трансформацію МСП у 2024 році демонструє прискорення впровадження технологій, але підкреслює нерівність між фірмами, де цифрові адаптери показують кращу стійкість, що вимагає подальших досліджень щодо впливу довгострокових ефектів на економічну безпеку МСП [12].

У розглянутих роботах зроблено акцент на розробці теоретичних рамок, ідентифікації бар'єрів та успіхів, а також політиках підтримки, що допомагає зрозуміти, як цифровізація посилює конкурентні стратегії через інновації та ефективність, але залишається потреба в емпіричних дослідженнях для постконфліктних економік, таких як українська, де специфічні виклики, зокрема, нестабільність та обмежений доступ до ресурсів, вимагають адаптованих моделей, а також існує потреба у вивченні інтеграції кібербезпеки в стратегії для забезпечення економічної стабільності. Незважаючи на значні напрацювання в літературі, актуальність проблеми зберігається через швидкі технологічні зміни, глобальні кризи та регіональні диспропорції, де МСП у країнах, що розвиваються, продовжують відставати, роблячи необхідними нові моделі, орієнтовані на локальні контексти для сталого розвитку. Таким чином, існуючі дослідження формують основу для розуміння цифрової трансформації як інструменту конкурентної безпеки та відкривають простір для подальшого аналізу адаптивних моделей, що робить обрану тему надзвичайно актуальною для сучасної економіки, особливо в умовах відновлення та невизначеності.

Формулювання цілей дослідження. Метою статті є розробка та обґрунтування моделей формування конкурентних стратегій економічної безпеки малих та середніх підприємств в умовах цифрової трансформації, які інтегрують цифрові технології, такі як штучний інтелект, хмарні сервіси та fintech-рішення, для підвищення стійкості до кіберзагроз, ринкових ризиків і забезпечення конкурентоспроможності, з урахуванням специфіки постконфліктної економіки України та глобальних тенденцій цифровізації.

Методологічною основою дослідження є системний підхід до аналізу конкурентних стратегій економічної безпеки малих та середніх підприємств (МСП) в умовах цифрової трансформації, який поєднує кількісні та якісні методи. Використовуються методи порівняльного аналізу для зіставлення глобальних і локальних тенденцій, а також моделювання для розробки адаптивних стратегій, що враховують кіберзагрози та ринкові виклики в постконфліктній економіці.

Виклад основного матеріалу дослідження. У сучасних умовах цифрової трансформації малі та середні підприємства (МСП), які формують до 60% ВВП у країнах, таких як Італія, та 55% у США [3], стикаються з необхідністю інтегрувати конкурентні стратегії економічної безпеки в свої системи управління, щоб не лише захистити ресурси, але й забезпечити конкурентоспроможність у динамічному цифровому середовищі. Цифровізація відкриває можливості для інновацій через технології, зокрема, штучний інтелект (AI), хмарні обчислення та fintech, але водночас посилює ризики кіберзагрози, які вражають 46% МСП із чисельністю працівників до 1000 осіб [1], та ринкові коливання, що вимагають швидкої адаптації. Без

конкурентних стратегій економічної безпеки МСП ризикують втратити ринкові позиції, адже традиційні підходи, зосереджені на фізичних та фінансових ризиках, не враховують специфіку цифрової економіки, де дані є ключовим активом, а швидкість реакції визначає успіх. Наявність таких стратегій забезпечує МСП значні переваги: оптимізацію витрат,

як у Кореї, де 55% МСП використовують fintech для фінансової стабільності [4], підвищення продуктивності на 3-5% щорічно в США та Німеччині завдяки AI та IoT [3], захист від кібератак, що знижує втрати на 15-20% [6], і доступ до глобальних ринків через e-commerce, що критично для постконфліктних економік, таких як Україна [7] (табл.1).

Таблиця 1 Ключові показники цифровізації та економічної ролі МСП у ТОП-10 країнах

Країна	Продуктивність МСП (зростання, % щорічно, 2020-2023 рр.)	Рівень цифровізації МСП (2025 р.)	Внесок у ВВП (% у 2023 р.)
США	3-5% (високотехнологічні сектори)	60% (хмарні технології), 25% (AI)	~55%
Німеччина	3-4% (промисловість, IoT)	50% (IoT), 40% (цифрова безпека)	~57%
Японія	1-2% (послуги, повільна автоматизація)	30% (AI), 45% (fintech)	~53%
Великобританія	2-3% (fintech, e-commerce)	45% (цифрові інструменти)	~52%
Франція	2-3% (державні програми цифровізації)	40% (хмарні сервіси)	~56%
Італія	1-2% (фрагментовані ринки)	25-30% (базові цифрові інструменти)	~60%
Канада	2-3% (цифрові сервіси)	40% (fintech, e-commerce)	~50-52%
Корея	3-4% (технологічні МСП)	55% (fintech), 40% (цифрова безпека)	~58%
Австралія	2-3% (цифрові сервіси)	40% (хмарні технології)	~50-52%
Іспанія	1-2% (туризм, торгівля)	25-30% (цифрові платформи)	~55%

Джерело: побудовано авторами на основі [4], [3], [7], [2].

Стратегії економічної безпеки перетворюють економічну безпеку на інструмент конкурентного зростання, дозволяючи МСП лідирувати в цифровій економіці. Пропонується формувати моделі конкурентних стратегій економічної безпеки МСП на основі системного підходу, який інтегрує цифрові технології, оцінку ризиків і стратегічне планування, адаптоване до локальних викликів, таких як обмежене фінансування (доступ до кредитування для цифровізації отримують лише 15% МСП [2]), низький рівень цифрових навичок (базові цифрові компетенції притаманні приблизно 30% підприємств [5]) і зростання кіберзагроз (рівень кіберзагроз зріс на 20% у 2023 році [6]).

Модель формування конкурентних стратегій економічної безпеки МСП складається з чотирьох компонентів: оцінка цифрових ризиків (зокрема кіберзагроз і ринкових змін), інтеграція технологій (AI, хмарні сервіси, fintech), адаптивне стратегічне

планування та моніторинг ефективності через KPI (зростання продуктивності, зменшення втрат).

Актуальним рішенням для України є створення гібридного цифрового кооперативу (ГЦК) як частини моделі. ГЦК передбачає об'єднання МСП у цифрові екосистеми через платформу на базі Дія.Бізнес, яка забезпечує спільний доступ до хмарних сервісів, AI-інструментів для аналізу ризиків і fintech-рішень за моделлю передплати, знижуючи індивідуальні витрати на цифровізацію. Це рішення нове для України, оскільки воно використовує відкриті дані (E-data) та державні цифрові ініціативи для створення кооперативних моделей, що дозволяють МСП ділитися ресурсами та експертизою, долаючи бар'єри доступу до технологій і підвищуючи стійкість до кіберзагроз. Модель працює циклічно: оцінка ризиків визначає вразливості, технології інтегруються через ГЦК, стратегії адаптуються до ринкових умов, а ефективність оцінюється через KPI, такі як зростання продуктивності та зменшення втрат (табл. 2).

Таблиця 2 **Модель формування конкурентних стратегій економічної безпеки МСП**

Компонент моделі	Опис	Інструменти	Очікувані результати	Специфіка для України
Оцінка цифрових ризиків	Аналіз кіберзагроз, ринкових ризиків і рівня цифрових навичок МСП для визначення вразливостей.	Аналітика даних (AI), звіти ENISA, опитування МСП.	Визначення ключових загроз (кібератаки, брак навичок).	Використання даних Мінцифри для локального аудиту.
Інтеграція технологій	Впровадження AI, хмарних сервісів і fintech через гібридний цифровий кооператив (ГЦК) для спільного доступу до ресурсів.	Платформа Дія.Бізнес, хмарні сервіси, AI для маркетингу, fintech для фінансів.	Зниження витрат на цифровізацію, підвищення продуктивності на 3-5% (на основі даних [3]).	ГЦК як нове рішення: МСП об'єднуються для доступу до технологій за передплатою, використовуючи E-data.
Адаптивне стратегічне планування	Розробка стратегій, що поєднують захист від ризиків із конкурентними діями (наприклад, вихід на глобальні ринки через e-commerce).	Аналіз ринкових трендів, інструменти прогнозування AI, платформи e-commerce.	Збільшення ринкової частки, стійкість до криз.	Адаптація до постконфліктної економіки: фокус на e-commerce та експорт.
Моніторинг ефективності	Оцінка результатів через KPI: зростання продуктивності, зменшення втрат від кібератак, рентабельність.	Дашборди аналітики, інструменти моніторингу.	Зменшення втрат на 15-20% (за даними [6]), зростання доходів.	Використання звітів Дія.Бізнес для оцінки локальних результатів, інтеграція з відкритими даними.

Джерело: побудовано авторами

Формування конкурентних стратегій економічної безпеки МСП реалізується через трансформацію даних і ресурсів, отриманих на кожному етапі моделі, у конкретні стратегічні рішення, які можна класифікувати як захисні, інноваційні та ринкові стратегії. Наприклад, на етапі оцінки цифрових ризиків ідентифікуються ключові загрози, зокрема, кібератаки або низький рівень навичок, що формує основу для захисних стратегій, таких як впровадження систем кібербезпеки через ГЦК. На етапі інтеграції технологій, використовуючи запропоновані інструменти, формуються інноваційні стратегії, такі як автоматизація бізнес-процесів через AI або використання fintech для оптимізації фінансів, що підвищує продуктивність МСП. Адаптивне стратегічне планування трансформує ці можливості в ринкові стратегії, наприклад, вихід на глобальні ринки через e-commerce, адаптовані до України через платформу Дія.Бізнес для експорту. Моніторинг ефективності стратегій через KPI (наприклад, зменшення втрат від кібератак), забезпечує зворотний зв'язок, дозволяючи коригувати стратегії для максимізації результатів. Таким чином, модель формування конкурентних стратегій економічної безпеки МСП виступає як структурована рамка, що перетворює аналіз ризиків і технологічні ресурси в конкретні стратегії, які відповідають локальним і глобальним викликам.

Новизна запропонованої моделі полягає в її гібридному підході, який поєднує елементи критичного реалізму [9] та теорії ендogenous зростання, адаптованих до постконфліктної економіки України, на відміну від загальних моделей, як у [11], що фокусуються на Industry 4.0 без урахування кібербезпеки чи локальних особливостей. Модель вирізняється інтеграцією кібербезпеки як ключового компонента стратегії та акцентом на доступні цифрові платформи для подолання бар'єрів, таких як низький рівень цифрових навичок. Застосування моделі розв'язує проблеми обмеженого фінансування, низьких цифрових навичок і вразливості до кіберзагроз, сприяючи економічному відновленню через зростання продуктивності та вихід на глобальні ринки, що забезпечує стійкість МСП у невизначеному середовищі.

Висновки. В результаті проведеного дослідження було встановлено, що формування конкурентних стратегій економічної безпеки малих та середніх підприємств (МСП) в умовах цифрової трансформації є критично важливим для забезпечення їхньої стійкості та зростання в динамічному ринковому середовищі. Аналіз ключових аспектів цифровізації, кіберзагроз і ринкових викликів показав, що МСП можуть не лише захищати свої ресурси, але й набувати конкурентних переваг через інтеграцію цифрових технологій, таких

як штучний інтелект, хмарні сервіси та fintech, що сприяє оптимізації витрат, підвищенню продуктивності та доступу до глобальних ринків. Використані системний підхід і емпіричні дані дозволили розробити гібридну модель, яка враховує локальні особливості постконфліктної економіки України, зокрема обмежений доступ до фінансування та низький рівень цифрових навичок. Запропонована модель, що включає оцінку ризиків, інтеграцію технологій через гібридний цифровий кооператив, адаптивне планування та моніторинг ефективності,

забезпечує створення захисних, інноваційних і ринкових стратегій, які знижують втрати від кіберзагроз, підвищують продуктивність і сприяють економічному відновленню. Подальша розробка моделі відкриває перспективи для вдосконалення кооперативних механізмів, розширення доступу МСП до цифрових екосистем і посилення їхньої ролі в сталому розвитку економіки, забезпечуючи довгострокову конкурентоспроможність і стійкість у цифровій епісі.

Література:

1. StrongDM. (2025). Small business cybersecurity statistics. <https://www.strongdm.com/blog/small-business-cyber-security-statistics>.
2. World Bank. (n.d.). SME finance: Data and resources. <https://www.worldbank.org/en/topic/sme/finance>.
3. Organisation for Economic Co-operation and Development. (2025). 2025 OECD D4SME survey: Digitalisation and SMEs. *OECD Publishing*. <https://www.oecd.org/en/data/dashboards/oecd-data-lake-on-smes-and-entrepreneurship.html>.
4. Organisation for Economic Co-operation and Development. (2021). OECD SME and entrepreneurship outlook 2021. *OECD Publishing*. https://www.oecd-ilibrary.org/industry-and-services/oecd-sme-and-entrepreneurship-outlook-2021_97a5a86c-en.
5. Ministry of Digital Transformation of Ukraine. (2023). Digital transformation initiatives and SME digitalization data (Diia.Business). <https://thedigital.gov.ua>.
6. European Union Agency for Cybersecurity. (2023). SMEs cybersecurity surveys. *ENISA*. <https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/smes-cybersecurity>.
7. United Nations. (2024). Global MSMEs report 2024. *United Nations*. <https://www.un.org/sites/un2.un.org/files/globalmsmesreport2024.pdf>.
8. Aliyev, V. (2025). Digital Transformation Strategies and Challenges in Small and Medium Enterprises (SMEs): A Systematic Review and Future Directions. *Technical Report*. <http://dx.doi.org/10.13140/RG.2.2.27245.29924>.
9. Meier, A., Eller, R., & Peters, M. (2025). Creating competitiveness in incumbent small- and medium-sized enterprises: A revised perspective on digital transformation. *Journal of Business Research*, 186, 115028. <https://doi.org/10.1016/j.jbusres.2024.115028>.
10. Sagala, G.H., Óri, D. (2024). Toward SMEs digital transformation success: a systematic literature review. *Inf Syst E-Bus Manage* 22, 667–719. <https://doi.org/10.1007/s10257-024-00682-2>.
11. Parra-Sánchez, D. T., & Talero-Sarmiento, L. H. (2024). Digital transformation in small and medium enterprises: A scientometric analysis. *Digital Transformation and Society*, 3(3), 257–276. <https://doi.org/10.1108/DTS-06-2023-0048>.
12. Holl, A., Rama, R. (2024). SME digital transformation and the COVID-19 pandemic: a case study of a hard-hit metropolitan area. *Science and Public Policy*. <https://doi.org/10.1093/scipol/scae023>.

References:

1. StrongDM. (2025). Small business cybersecurity statistics. <https://www.strongdm.com/blog/small-business-cyber-security-statistics>.
2. World Bank. (n.d.). SME finance: Data and resources. <https://www.worldbank.org/en/topic/sme/finance>.
3. Organisation for Economic Co-operation and Development. (2025). 2025 OECD D4SME survey: Digitalisation and SMEs. *OECD Publishing*. <https://www.oecd.org/en/data/dashboards/oecd-data-lake-on-smes-and-entrepreneurship.html>.
4. Organisation for Economic Co-operation and Development. (2021). OECD SME and entrepreneurship outlook 2021. *OECD Publishing*. https://www.oecd-ilibrary.org/industry-and-services/oecd-sme-and-entrepreneurship-outlook-2021_97a5a86c-en.
5. Ministry of Digital Transformation of Ukraine. (2023). Digital transformation initiatives and SME digitalization data (Diia.Business). <https://thedigital.gov.ua>.
6. European Union Agency for Cybersecurity. (2023). SMEs cybersecurity surveys. *ENISA*. <https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/smes-cybersecurity>.
7. United Nations. (2024). Global MSMEs report 2024. *United Nations*. <https://www.un.org/sites/un2.un.org/files/globalmsmesreport2024.pdf>.
8. Aliyev, V. (2025). Digital Transformation Strategies and Challenges in Small and Medium Enterprises (SMEs): A Systematic Review and Future Directions. *Technical Report*. <http://dx.doi.org/10.13140/RG.2.2.27245.29924>.
9. Meier, A., Eller, R., & Peters, M. (2025). Creating competitiveness in incumbent small- and medium-sized enterprises: A revised perspective on digital transformation. *Journal of Business Research*, 186, 115028. <https://doi.org/10.1016/j.jbusres.2024.115028>.
10. Sagala, G.H., Óri, D. (2024). Toward SMEs digital transformation success: a systematic literature review. *Inf Syst E-Bus Manage* 22, 667–719. <https://doi.org/10.1007/s10257-024-00682-2>.
11. Parra-Sánchez, D. T., & Talero-Sarmiento, L. H. (2024). Digital transformation in small and medium enterprises: A scientometric analysis. *Digital Transformation and Society*, 3(3), 257–276. <https://doi.org/10.1108/DTS-06-2023-0048>.
12. Holl, A., Rama, R. (2024). SME digital transformation and the COVID-19 pandemic: a case study of a hard-hit metropolitan area. *Science and Public Policy*. <https://doi.org/10.1093/scipol/scae023>.

