

Романашенко Ірина Олександрівна, аспірантка
Державного біотехнологічного університету

Romanashenko Iryna, PhD student at the State Biotechnological
University, <https://orcid.org/0009-0003-4902-4652>

СТРУКТУРНІ ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК СКЛАДОВОЇ СТРАТЕГІЧНОГО УПРАВЛІННЯ
ІННОВАЦІЙНИМ РОЗВИТКОМ ПІДПРИЄМСТВА
STRUCTURAL FEATURES OF INFORMATION SECURITY AS A COMPONENT OF STRATEGIC MANAGEMENT OF
ENTERPRISE INNOVATION DEVELOPMENT

Романашенко І. О. Структурні особливості інформаційної безпеки як складової стратегічного управління інноваційним розвитком підприємства. *Український журнал прикладної економіки та техніки*. 2026. Том 11. № 1. С. 44 – 48.

Romanashenko I. Structural features of information security as a component of strategic management of enterprise innovation development. *Ukrainian Journal of Applied Economics and Technology*. 2026. Volume 11. № 1, pp. 44 – 48.

Статтю присвячено питанням забезпечення ефективності стратегічного управління інноваційним розвитком підприємства. Актуальність обраної тематики зумовлена необхідністю обґрунтування засад інтеграції інформаційної безпеки в стратегічне управління інноваційним розвитком підприємства. Стаття має на меті обґрунтувати теоретико-методичні положення щодо інтеграції інформаційної безпеки в систему стратегічного управління інноваційним розвитком підприємства. У статті досліджено наявні підходи до стратегічного управління інноваційним розвитком підприємства, розглянуто концепції динамічних можливостей та організаційної резильєнтності. Обґрунтовано, що здатність підприємства ідентифікувати, інтегрувати та трансформувати ресурси в умовах цифрової економіки нерозривно пов'язана із забезпеченням належного рівня захисту інформаційних активів. Визначено, що інформаційна безпека – це стратегічний чинник підтримки інноваційних процесів. Систематизовано такі основні кіберзагрози: AI-підсилені атаки, кіберзлочини, геополітично мотивовані інциденти, ризики в цифрових ланцюгах постачання та нерівність кіберздатності підприємств різного масштабу. Досліджено вплив кіберзагроз на фінансову стійкість, операційну безперервність, репутацію та інвестиційну привабливість підприємств. Визначено, що прямі та непрямі економічні втрати, порушення бізнес-процесів та зниження довіри стейкхолдерів трансформують інформаційні ризики в стратегічні. Дослідження впливу кіберризиків на стратегічне управління дозволило визначити, що ефективна система інформаційної безпеки повинна ґрунтуватися на принципах інтегрованості, системності, превентивності та адаптивності. Запропоновано рекомендації щодо побудови комплексної системи інформаційної безпеки підприємства, що охоплює організаційні, управлінські, економічні та технологічні складові та узгоджується з міжнародними стандартами управління. Практична цінність запропонованих в дослідженні рекомендацій полягає в можливості їх застосування в діяльності підприємств різних галузей та масштабів задля формування комплексної системи інформаційної безпеки, інтегрованої у стратегічне управління інноваційним розвитком. Обґрунтовані положення, у порівнянні з існуючими, дозволяють перейти від фрагментарного, переважно технічного підходу до кіберзахисту до системної моделі управління, що охоплює організаційні, управлінські, економічні та технологічні засади.
Ключові слова: стратегічне управління, інноваційний розвиток, інформаційна безпека, резильєнтність, динамічні можливості, кіберризик, конкурентоспроможність.

The article is devoted to ensuring the effectiveness of strategic management of enterprise innovation development. The relevance of the chosen topic is determined by the need to substantiate the principles of integrating information security into the strategic management of enterprise innovation development. The article aims to justify the theoretical and methodological foundations for integrating information security into the system of strategic management of enterprise innovation development. The article examines existing approaches to strategic management of enterprise innovation development and considers the concepts of dynamic capabilities and organizational resilience. It is substantiated that an enterprise's ability to identify, integrate, and transform resources in the digital economy is inextricably linked to ensuring an adequate level of protection for information assets. It is determined that information security acts as a strategic factor supporting innovation processes. The main cyber threats are systematized into AI-enhanced attacks, cybercrime, geopolitically motivated incidents, risks in digital supply chains, and disparities in cybersecurity capabilities among enterprises of different sizes. The study investigates the impact of cyber threats on financial stability, operational continuity, reputation, and investment attractiveness of enterprises. It is shown that direct and indirect economic losses, business process disruptions, and reduced stakeholder trust transform information risks into strategic risks. The study of the impact of cyber risks on strategic management allowed determining that an effective information security system should be based on the principles of integration, systemacity, preventiveness, and adaptability. Recommendations are proposed to build a comprehensive enterprise information security system that covers organizational, managerial, economic, and technological components and aligns with international management standards. The practical value of the recommendations lies in their applicability to enterprises across different industries and scales, enabling a comprehensive information security system integrated into the strategic management of innovation development. The substantiated provisions, compared to existing approaches, allow a transition from a fragmented, predominantly technical approach to cybersecurity to a systematic management model encompassing organizational, managerial, economic, and technological foundation.

Keywords: strategic management, innovation development, information security, resilience, dynamic capabilities, cyber risks, competitiveness.

Вступ

Сучасні підприємства функціонують в умовах високої динамічності зовнішнього середовища, посилення глобальної конкуренції, цифровізації бізнес-процесів та зростаючої ролі інновацій як потужного чинника довгострокової конкурентоспроможності. Внаслідок цього стратегічне управління інноваційним розвитком підприємства дедалі більше залежить від рівня захищеності інформаційних ресурсів, цифрових платформ, інтелектуальної власності та управлінських рішень. Інформація перетворюється на стратегічний актив, на якому ґрунтується інноваційний потенціал підприємства, і забезпечує його стійкі конкурентні переваги.

З іншого боку, активна цифрова трансформація господарської діяльності одночасно протікає із зростанням кіберзагроз, витоками конфіденційної інформації, промисловим шпигунством, маніпуляціями даними та деструктивним впливом на інформаційні системи управління. Недостатній рівень інтеграції механізмів інформаційної безпеки у систему стратегічного управління інноваційним розвитком призводить до втрати інноваційних напрацювань, зниження інвестиційної привабливості, погіршення репутації та фінансових результатів підприємства. Тож дослідження інформаційної безпеки з позиції стратегічного управління інноваційним розвитком підприємства є вкрай актуальним.

Проблематика стратегічного управління інноваційним розвитком підприємства широко досліджується в працях вітчизняних та зарубіжних науковців. Вагомий внесок у розвиток теоретичних положень інноваційного розвитку підприємств здійснили Кащена Н. та



This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

© Романашенко Ірина Олександрівна, 2026

Чміль Є. [2], які обґрунтували підходи до аналізу інноваційного розвитку із врахуванням ресурсного потенціалу та стратегічних орієнтирів підприємства. Вчені Сало А. та Артемчук М. [3] розглянули стратегічне управління інноваційним розвитком як процес узгодження довгострокових цілей підприємства з механізмами впровадження інновацій.

Теоретичні нароби щодо динамічних можливостей та забезпечення стійкості стратегічного управління сформовані Тісом Д. та співавторами [4]. Вчені прийшли до висновку, що здатність підприємства інтегрувати, перебудовувати та трансформувати ресурси визначає його конкурентні переваги в умовах змінного середовища. Подальший розвиток концепції представлено в дослідженнях Валензели В. та співавторів [5], Бісвакарми Г. і Бохори Б. [6], які довели, що динамічні можливості безпосередньо впливають на організаційну резильєнтність та результативність підприємства.

Нароби щодо стратегічного управління знаннями представлено в праці Феррейра Ж. та співавторів [7], в якій вчені визначили роль стратегічного менеджменту знань, людського капіталу та організаційного навчання в формуванні інноваційного потенціалу та адаптивності підприємства. Концепція організаційної резильєнтності у сфері інформаційної безпеки розкрита у праці Гербана Б. [10], який обґрунтував необхідність інтеграції систем безперервності бізнесу у стратегічне управління. Дослідники Лінков І. та Трамп Б. [11] розвинули системний підхід до резильєнтності та розглянули її як здатність підприємства відновлюватися після дестабілюючих подій. Доцільність інвестування у кібербезпеку обґрунтовано в дослідженні Гордона Л. та співавторів [12], які визначили залежність між витратами на захист інформаційних систем та зниженням фінансових втрат від кіберінцидентів. Дослідники Бада М. та Нерс Р. [14] відзначили важливість розвитку культури кібербезпеки та освітніх програм для підвищення стійкості підприємства.

Таким чином, проаналізовані праці розглядають питання стратегічного управління інноваційним розвитком, динамічних можливостей, організаційної резильєнтності та кібербезпеки. Проте, незважаючи на повноту викладених положень, подальшого дослідження потребує саме місце інформаційної безпеки в системі стратегічного управління інноваційним розвитком підприємства, що й обумовлює мету і завдання дослідження.

Формулювання цілей статті

Метою дослідження є обґрунтування теоретико-методичних положень щодо інтеграції інформаційної безпеки в систему стратегічного управління інноваційним розвитком підприємства.

Для досягнення поставленої мети окреслено такі завдання дослідження:

- проаналізувати сучасні підходи до розуміння стратегічного управління інноваційним розвитком підприємства та визначити його місце у системі корпоративного управління;
- систематизувати чинники, що забезпечують стійкість та безперервність процесів стратегічного управління інноваційною діяльністю;
- дослідити вплив цифровізації та кіберзагроз на фінансову, операційну, репутаційну та стратегічну діяльність підприємства;
- обґрунтувати роль інформаційної безпеки в формуванні організаційної резильєнтності;
- проаналізувати наслідки кіберзагроз для сучасних підприємств та визначити їх вплив на інноваційний розвиток;
- обґрунтувати рекомендації щодо побудови системи інформаційної безпеки підприємства в контексті стратегічного управління інноваційним розвитком.

Виклад основного матеріалу дослідження

Високий рівень турбулентності, прискорення технологічних змін, цифровізація бізнес-процесів, глобалізація ринків та зростання ролі інтелектуального капіталу вимагають від підприємств безперервного розвитку. Відтак інновації перетворились на фактор забезпечення довгострокової конкурентоспроможності, формування стійких ринкових позицій та створення доданої вартості [1]. А стратегічне управління інноваційним розвитком підприємства стало системоутворюючим в сучасній моделі корпоративного управління.

Цілком погоджуємось із думкою Кащенко Н. та Чміль Є. [2] щодо того, що інноваційний розвиток підприємства – це процес, що охоплює створення, впровадження та комерціалізацію нових продуктів, технологій, організаційних та управлінських рішень. Ефективність цього процесу залежить від здатності керівництва інтегрувати інновації в довгострокову стратегію підприємства та забезпечити узгодженість ресурсного потенціалу з перспективними напрямками розвитку.

Дослідники Сало А. та Артемчук М. [3] зазначають, що стратегічне управління інноваційним розвитком підприємств ґрунтується на систематичному поєднанні довгострокових цілей підприємства із процесами інноваційної діяльності задля забезпечення конкурентоспроможності, адаптації до змін зовнішнього середовища та створення доданої вартості у довгостроковій перспективі.

Узагальнюючи результати досліджень [2; 3], ми прийшли до висновку, що стратегічне управління інноваційним розвитком забезпечує (рис. 1):

- оцінювання внутрішнього потенціалу підприємства та зовнішніх умов ринку;
- формування інноваційних стратегій, що узгоджуються з місією та візією підприємства;
- впровадження комплексних механізмів реалізації інноваційних рішень;
- моніторинг ефективності інноваційної діяльності та її коригування в умовах мінливого середовища.

Ефективна система стратегічного управління інноваційним розвитком охоплює представлені управлінські процеси. Ці процеси спрямовані на комплексне оцінювання внутрішнього потенціалу та аналіз зовнішніх ринкових умов, формування інноваційних стратегій, впровадження інноваційних рішень та відстеження результативності

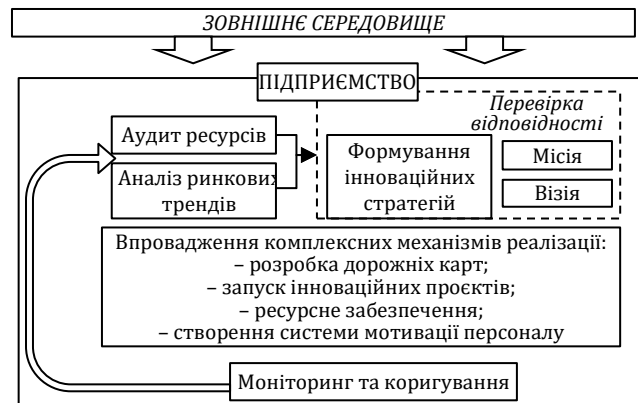


Рис. 1. Місце стратегічного управління інноваційним розвитком в системі функціонування підприємства
Джерело: авторська розробка

інноваційної діяльності з подальшим коригуванням управлінських дій відповідно до динаміки середовища. Далі розглянемо чинники, які забезпечують стійкість та безперервність зазначених процесів. У науковій літературі виявлено велику кількість чинників, що забезпечують ефективність процесів стратегічного управління інноваційним розвитком підприємства в умовах високої динаміки зовнішнього середовища та невизначеності.

Насамперед розглянемо концепцією динамічних можливостей, вперше обґрунтовану вченими Тісе Д та спів-авторами [4]. Згідно з динамічним підходом до розуміння стратегічного менеджменту, підприємство здатне адаптувати свою ресурсну базу та структури задля підтримки конкурентоспроможності та виживання в умовах зміни зовнішнього середовища. Ми підтримуємо позицію вчених щодо того, що саме здатність організації ідентифікувати, засвоювати, інтегрувати та реорганізувати свої ресурси відповідно до викликів визначає її здатність відновлюватися.

Додаткові дослідження [5; 6] говорять, що динамічні можливості безпосередньо впливають на організаційну стійкість, оскільки забезпечують здатність бізнес-структур передбачати зміни, мобілізувати ресурси, адаптуватися до неочікуваних зовнішніх обставин. Такі компоненти, як здатність виявляти можливості та загрози, акумулювати та засвоювати знання, координувати та інноваційно трансформувати процеси, позитивно впливають на здатність підприємств утримувати стратегічну стійкість у конкурентному середовищі.

З іншого боку, група вчених [7] виокремлює фактори людського капіталу, організаційне навчання та розвиток компетенцій персоналу в контексті забезпечення стійкості стратегічного управління. Перераховані чинники формують внутрішньо орієнтовані ресурси підприємства для інноваційних змін, гнучкого реагування на ризики та побудови ефективних механізмів адаптації.

Зростання ролі цифрових технологій та інформаційних систем у процесах стратегічного управління вимагає врахування і інших факторів. Активна цифровізація бізнес-процесів, впровадження хмарних технологій, інструментів великих даних, штучного інтелекту, автоматизованих систем управління зумовлюють необхідність захисту інформаційних ресурсів підприємств. Кіберзагрози здатні впливати і на операційну ефективність підприємства, і на його стратегічні позиції, і на ринкову репутацію, і на інвестиційну привабливість. У дослідженні [8] кібератаки та витоки даних визначені як одні з найпотужніших глобальних ризиків, що впливають на стійкість підприємств в середньостроковій та довгостроковій перспективах. У таблиці 1 ми систематизували негативні наслідки кіберзагроз для сучасних підприємств та компаній.

Таблиця 1. Наслідки кіберзагроз у діяльності сучасних підприємств

Кіберзагроза	Наслідки	Примітка
AI-підсилені вразливості та атаки	Ризики витоків даних, компіляції та маніпуляції з інформацією	87% опитаних компаній повідомили про зростання вразливостей, пов'язаних із штучним інтелектом. Визначено, що вони призводять до витоків даних або несанкціонованого доступу до корпоративної інформації. Наростають стратегічні ризики для інтеграції цифрових технологій у бізнес-моделі та процеси управління
Кіберзлочини та шахрайство	Фінансові втрати, порушення операцій, репутаційний ризик	Кібер-шахрайство (фішинг, соціальна інженерія, шахрайство з даними) стало найпоширенішим. Керівники опитаних компаній зазначили, що таке шахрайство впливає на бізнес-операції та довіру стейкхолдерів
Геополітично мотивовані атаки	Збої у критичних сервісах, порушення стратегічної діяльності	Геополітична напруга змушує компанії включати кібератаки до стратегічних ризик-моделей, оскільки такі атаки можуть бути спрямовані на інфраструктуру та бізнес-процеси
Кіберризик в ланцюгах постачання	Залежність від третіх сторін, системні збитки	Опитані компанії відзначили, що ризики, пов'язані з кібербезпекою третіх сторін та постачальників, перешкоджають стійкості кіберзахисту, оскільки вразливість партнерів призводить до ланцюгових наслідків для підприємства
Нерівність в кіберздатності	Різний рівень захищеності між великими та малими підприємствами	Менші компанії частіше повідомляли про низький рівень готовності до кібератак. Непідготовленість призводить до більш серйозних наслідків для них у порівнянні з великими підприємствами, які мають більше ресурсів на кіберзахист
Технологічні фактори, гендеровані витоки, інфраструктурні атаки	Порушення нормального функціонування інформаційного середовища, технологічні збої	Штучний інтелект не тільки посилює ризик вразливості, він може бути використаний злочинцями для автоматизації атак, що значно ускладнить оперативне управління захистом і реагування

Джерело: складено за [8; 9]

Дослідивши наслідки кіберзагроз, ми прийшли до висновку, що вони різнопланово впливають на діяльність підприємств та їх стратегічне управління:

1. У фінансовому вимірі кібернапади зумовлюють прямі та непрямі економічні втрати. Прямі втрати пов'язані з шахрайством, несанкціонованими фінансовими транзакціями, вимаганням, крадіжкою інтелектуальної власності та необхідністю відновлення пошкоджених інформаційних систем. Непрямі втрати проявляються у зниженні обсягів продажів через тимчасову недоступність сервісів, зменшенні ринкової вартості компанії, підвищенні вартості страхування кіберризиків та сплаті штрафних санкцій за недотримання вимог нормативно-правових актів та міжнародних стандартів захисту даних. У сукупності прямі та непрямі втрати відображаються на фінансовій стійкості підприємства та знижують його інвестиційну привабливість.

2. В операційному вимірі інформаційні ризики порушують безперервність бізнес-процесів. Атаки на інформаційні системи спричиняють збої в роботі виробничого обладнання, логістичних платформ, систем управління запасами, фінансових модулів та клієнтських сервісів. У разі ураження критичної цифрової інфраструктури підприємство вимушене тимчасово призупинити виробництво або обслуговування клієнтів, тоді воно втрапить доходи, порушить контрактні зобов'язання та понесе транзакційні витрати. Відновлення функціонування систем здійснюється за додаткові кошти, що ускладнює реалізацію стратегічних планів та інноваційних проєктів.

3. Інформаційні атаки впливають і на репутацію підприємства, мають довгостроковий характер та часто перевищують за масштабами безпосередні фінансові втрати. Публічне розголошення фактів витоку персональних або комерційно чутливих даних започатковує негативний інформаційний тон навколо підприємства, підриває довіру клієнтів, партнерів, інвесторів, знижує рівень лояльності споживачів. За цифрової економіки, де довіра є основним нематеріальним активом, репутаційні втрати суттєво послаблюють конкурентні позиції підприємства та обмежують його можливості щодо розширення ринкової присутності.

4. У довгостроковій перспективі геополітичні конфлікти, використання кіберінструментів для політичного тиску, складність глобальних цифрових ланцюгів постачання обумовлюють додаткові загрози для інвестиційних

програм та цифрових трансформацій. Вразливість партнерів спричиняє «ефект доміно», а кіберзагрози стають стратегічними ризиками та вимагають обґрунтування засад управління організаційною безпекою.

Сучасні підходи до формування системи інформаційної безпеки ґрунтуються на концепції організаційної резильєнтності. Зокрема, дослідження [10; 11] говорять, що інтеграція систем управління інформаційною безпекою в стратегічне управління підвищує здатність підприємства відновлюватися після кризових подій та зменшувати їх негативні наслідки. Системи безперервності бізнесу мають будуватись як елемент стратегічного управління, а не бути окремим інструментом реагування на інциденти.

Водночас розробка кожного інструменту стратегічного управління потребує вкладання фінансових ресурсів. За результатами дослідження [12], стабільні інвестиції в кібербезпеку знижують ймовірність значних фінансових втрат внаслідок інцидентів безпеки та підвищують довіру інвесторів і партнерів. Стратегічно обґрунтовані витрати на захист інформаційних активів економічно доцільні та сприяють довгостроковій стійкості бізнесу.

Відповідно до міжнародного стандарту ISO 27001 [13], система управління інформаційною безпекою повинна бути інтегрована у загальну систему управління підприємством та узгоджена з його стратегічними цілями. Результати дослідження [14] підтверджують, що підприємства з розвиненими механізмами кіберзахисту мають більшу операційну ефективність та швидше адаптуються до кризових умов.

Таким чином, ми прийшли до висновку, що інформаційна безпека забезпечує:

- захист інтелектуального капіталу та інноваційних розробок;
- безперервність бізнес-процесів та стратегічних ініціатив;
- мінімізацію фінансових та репутаційних ризиків;
- підвищення довіри з боку інвесторів, партнерів і клієнтів;
- формування цифрової резильєнтності як основи довгострокового розвитку.

Узагальнюючи напрацювання провідних дослідників, пропонуємо рекомендації щодо побудови системи інформаційної безпеки підприємства (рис. 2).

Практична цінність запропонованих в дослідженні рекомендацій полягає в можливості їх застосування в діяльності підприємств різних галузей та масштабів задля формування комплексної системи інформаційної безпеки, інтегрованої у стратегічне управління інноваційним розвитком. Обґрунтовані положення, у порівнянні з існуючими, дозволять перейти від фрагментарного, переважно технічного підходу до кіберзахисту до системної моделі управління, що охоплює організаційні, управлінські, економічні та технологічні засади.

Висновки та перспективи подальших розвідок

За зростаючої турбулентності глобального середовища, прискорення технологічних змін та активної цифровізації економіки стратегічне управління інноваційним розвитком набуває вагомого значення для забезпечення довгострокової конкурентоспроможності підприємств. Інновації виступають це не просто інструмент технологічного оновлення, це комплексний механізм формування доданої вартості, адаптації до змін та зміцнення ринкових позицій. Ефективність стратегічного управління інноваційним розвитком залежить від здатності підприємства здійснювати комплексне оцінювання внутрішнього потенціалу, аналізувати зовнішнє середовище, формувати узгоджені інноваційні стратегії та забезпечувати постійний моніторинг їх реалізації. Водночас стійкість зазначених процесів значною мірою визначається рівнем розвитку динамічних можливостей, людського капіталу, організаційного навчання, інформаційною безпекою та здатністю підприємства адаптувати свою ресурсну базу до змін середовища.

Активне впровадження цифрових технологій водночас створює нові можливості для інноваційного розвитку та породжує додаткові ризики, пов'язані з кіберзагрозами. Інформаційна безпека повинна розглядатися як стратегічний ресурс підприємства та інтегрований елемент системи стратегічного управління інноваційним розвитком. Її функції виходять за межі технічного захисту даних та охоплюють забезпечення збереження інтелектуального капіталу, підтримку безперервності бізнес-процесів, мінімізацію фінансових та репутаційних ризиків, підвищення довіри стейкхолдерів та формування цифрової резильєнтності. Запропоновані в дослідженні рекомендації щодо побудови системи інформаційної безпеки підприємства дозволять сформувати комплексну, ризик-орієнтовану та інтегровану модель управління, що поєднуватиме організаційні, управлінські, економічні та технологічні інструменти.

Література

1. Rashed M., Uddin M., Islam M. Building Resilient Organizations: The Role of Technological Capability, Innovation Leadership, and Sustainability. *Glob J Flex Syst Manag.* 2025. Vol. 26, P. 963–995. DOI: <https://doi.org/10.1007/s40171-025-00471-x>.
2. Кащенко Н., Чміль Є. Теоретико-методичні засади аналізу інноваційного розвитку підприємства. *Економіка та суспільство.* 2022. Випуск 43. DOI: <https://doi.org/10.32782/2524-0072/2022-43-56>.
3. Сало А.Я., Артемчук М.О. Стратегічне управління інноваційним розвитком підприємства. *Економіка. Менеджмент. Бізнес.* 2020. № 3 (33). С. 40-44. DOI: <https://doi.org/10.31673/2415-8089.2020.034550>.



Рис. 2. Рекомендації щодо побудови системи інформаційної безпеки підприємства

Джерело: авторська розробка

4. Teece D.J., Pisano G., Shuen A. Dynamic capabilities and strategic management. *Strategic Management Journal*. 1997. Vol. 18 (7). P. 509-533. DOI: [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)](https://doi.org/10.1002/(SICI)1097-0266(199708)).
5. Valenzuela V., Jacobo-Hernandez C., Flores-López J. Dynamic Capabilities and Their Effect on Organizational Resilience in Small and Medium-Sized Commercial Enterprises. *Management & Marketing*. 2023. Vol. 18. P. 496-514. DOI: <https://doi.org/10.2478/mmcks-2023-0027>.
6. Biswakarma G., Bohora B. Dynamic capabilities and organizational performance: the mediating role of organizational resilience in the IT sector. *Future Business Journal*. 2025. Vol. 11. DOI: <https://doi.org/10.1186/s43093-025-00592-w>.
7. Ferreira J., Jens M., Armando P. Strategic Knowledge Management: Theory, Practice and Future Challenges. *Journal of Knowledge Management*. 2020. Vol. 24 (2). P. 121–126. DOI: <https://doi.org/10.1108/JKM-07-2018-0461>.
8. Global Risks Report 2026. World Economic Forum. 2026. 102 p. URL: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf.
9. Global Cybersecurity Outlook 2026. World Economic Forum. 2026. 64 p. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf.
10. Herbane B. Small business research: Time for a crisis-based view. *International Small Business Journal: Researching Entrepreneurship*. 2010. Vol. 28(1). P. 43-64. DOI: <https://doi.org/10.1177/0266242609350804>.
11. Linkov I., Trump B.D. The Science and Practice of Resilience in Risk. Systems and Decisions. Springer. 2019, 202 p.
12. Gordon L.A., Loeb M.P., Lucyshyn W. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*. 2003. Vol. 22(6). P. 461–485. DOI: <https://doi.org/10.1016/j.jaccpubpol.2003.09.001>.
13. ISO 27001. Information security, cybersecurity and privacy protection - Information security management systems. 2022. URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf.
14. Bada M., Nurse J.R. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security*. 2019. Vol. 27 No. 3 P. 393–410, DOI: <https://doi.org/10.1108/ICS-07-2018-0080>.

References

1. Rashed, M., Uddin, M., Islam, M. (2025). «Building Resilient Organizations: The Role of Technological Capability, Innovation Leadership, and Sustainability». *Glob J Flex Syst Manag*. Vol. 26. pp. 963–995. DOI: <https://doi.org/10.1007/s40171-025-00471-x>.
2. Kaschena, N., Chmil', Ye. (2022). «Theoretical and methodological principles of analyzing the innovative development of an enterprise». *Ekonomika ta suspil'stvo*. Issue 43. DOI: <https://doi.org/10.32782/2524-0072/2022-43-56>.
3. Salo, A.Ya., Artemchuk, M.O. (2020). «Strategic management of innovative development of an enterprise». *Ekonomika. Menedzhment. Biznes*. № 3 (33). pp. 40-44. DOI: <https://doi.org/10.31673/2415-8089.2020.034550>.
4. Teece, D.J., Pisano, G., Shuen, A. (1997). «Dynamic capabilities and strategic management». *Strategic Management Journal*. Vol. 18 (7). pp. 509-533. DOI: [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)](https://doi.org/10.1002/(SICI)1097-0266(199708)).
5. Valenzuela, V., Jacobo-Hernandez, C., Flores-López, J. (2023). «Dynamic Capabilities and Their Effect on Organizational Resilience in Small and Medium-Sized Commercial Enterprises». *Management & Marketing*. Vol. 18. pp. 496-514. DOI: <https://doi.org/10.2478/mmcks-2023-0027>.
6. Biswakarma, G., Bohora, B. (2025). «Dynamic capabilities and organizational performance: the mediating role of organizational resilience in the IT sector». *Future Business Journal*. Vol. 11. DOI: <https://doi.org/10.1186/s43093-025-00592-w>.
7. Ferreira, J., Jens, M., Armando, P. (2020). «Strategic Knowledge Management: Theory, Practice and Future Challenges». *Journal of Knowledge Management*. Vol. 24 (2). pp. 121–126. DOI: <https://doi.org/10.1108/JKM-07-2018-0461>.
8. Global Risks Report 2026. World Economic Forum. (2026). Available at: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf.
9. Global Cybersecurity Outlook 2026. World Economic Forum. (2026). Available at: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf.
10. Herbane, B. (2010). «Small business research: Time for a crisis-based view». *International Small Business Journal: Researching Entrepreneurship*. Vol. 28(1). pp. 43-64. DOI: <https://doi.org/10.1177/0266242609350804>.
11. Linkov, I., Trump, B.D. (2009). *The Science and Practice of Resilience in Risk. Systems and Decisions*. Springer.
12. Gordon, L.A., Loeb, M.P., Lucyshyn, W. (2003). «Sharing information on computer systems security: An economic analysis». *Journal of Accounting and Public Policy*. Vol. 22(6). pp. 461–485. DOI: <https://doi.org/10.1016/j.jaccpubpol.2003.09.001>.
13. ISO 27001. Information security, cybersecurity and privacy protection - Information security management systems. (2022). Available at: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf.
14. Bada, M., Nurse, J.R. (2019). «Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)». *Information and Computer Security*. Vol. 27 No. 3 pp. 393–410, DOI: <https://doi.org/10.1108/ICS-07-2018-0080>.

Стаття надійшла до редакції / Received 05.02.2026
Опубліковано / Published 25.02.2026

Прийнята до друку / Accepted 12.02.2026