



**Підприємництво, торгівля та біржова діяльність**

**УДК 658**

**DOI** <https://doi.org/10.5281/zenodo.15585336>

**Забезпечення інформаційної безпеки як детермінанта  
конкурентоспроможного розвитку підприємства**

**Топалов Володимир Миколайович**

аспірант, кафедра підприємництва, торгівлі та логістики

Луцький національний технічний університет,

вул. Львівська, 75 м. Луцьк Волинська обл. 43018, Україна,

[vtopalov.dev@gmail.com](mailto:vtopalov.dev@gmail.com),

ORCID iD: <https://orcid.org/0009-0006-1745-3171>

**Прийнято: 19.04.2025 | Опубліковано: 29.04.2025**

***Анотація.** У сучасних умовах цифрової трансформації економіки, забезпечення інформаційної безпеки стає невід'ємною складовою стратегічного розвитку підприємств та визначальним чинником їх конкурентоспроможності. **Метою дослідження** є визначення ролі інформаційної безпеки як стратегічного чинника, що впливає на конкурентоспроможність підприємств в умовах цифрової трансформації економіки. **Методи.** Методологічною основою дослідження є багатофакторний аналіз чинників, які впливають на рішення підприємств щодо інвестування в інформаційну безпеку. У дослідженні використано елементи структурно-функціонального, системного та порівняльного аналізу для вивчення внутрішніх і зовнішніх детермінант, що формують політику безпеки на підприємстві. Зокрема, досліджено такі фактори, як регуляторні вимоги, рівень цифрової зрілості, наявність IT-інфраструктури, репутаційні*



ризиків, досвід кіберзагроз, а також стратегічні пріоритети керівництва. **Результати.** Систематизовано бар'єри, що перешкоджають ефективному впровадженню інформаційної безпеки (фінансові, технічні, організаційні), а також стимули (регуляторні, економічні, репутаційні та стратегічні), які сприяють формуванню проактивної безпекової політики. Запропоновано концептуальний підхід до аналізу взаємозв'язку між рівнем інформаційної безпеки та конкурентоспроможністю підприємства, що дозволяє оцінити ефективність управлінських рішень у цій сфері. Встановлено, що інтеграція заходів кіберзахисту в бізнес-стратегію підвищує стійкість підприємств до зовнішніх загроз, зміцнює їх ринкові позиції та сприяє розвитку цифрової культури. **Висновки.** Доведено доцільність подальших досліджень, спрямованих на розробку моделей оцінювання ефективності інвестицій в інформаційну безпеку з урахуванням специфіки підприємств різного масштабу. Представлені результати мають практичне значення для керівників бізнесу, фахівців з інформаційної безпеки та дослідників, які працюють у сфері цифрового управління ризиками.

**Ключові слова:** інформаційна безпека, конкурентоспроможність підприємства, цифрова трансформація, стратегія управління, інвестиції в безпеку, бізнес-стійкість.

## **Ensuring information security as a determinant of the competitive development of an enterprise**

**Topalov Volodymyr Mykolayovych**

Postgraduate Student, Department of Entrepreneurship, Trade and Logistics

Lutsk National Technical University,

75 Lvivska St., Lutsk Volyn region 43018, Ukraine,

[vtopalov.dev@gmail.com](mailto:vtopalov.dev@gmail.com),

ORCID iD: <https://orcid.org/0009-0006-1745-3171>



**Abstract.** *In the current conditions of digital transformation of the economy, ensuring information security is becoming an integral part of the strategic development of enterprises and a determining factor in their competitiveness. **The purpose** of the study is to determine the role of information security as a strategic factor that affects the competitiveness of enterprises in the conditions of digital transformation of the economy. **Methods.** The methodological basis of the study is a multifactor analysis of factors that influence enterprises' decisions to invest in information security. The study uses elements of structural-functional, systemic and comparative analysis to study internal and external determinants that shape the security policy of the enterprise. In particular, factors such as regulatory requirements, the level of digital maturity, the availability of IT infrastructure, reputational risks, experience with cyber threats, as well as strategic priorities of management were investigated. **Results.** The barriers that hinder the effective implementation of information security (financial, technical, organizational), as well as the incentives (regulatory, economic, reputational and strategic) that contribute to the formation of a proactive security policy, are systematized. A conceptual approach to analyzing the relationship between the level of information security and the competitiveness of an enterprise is proposed, which allows assessing the effectiveness of management decisions in this area. It is established that the integration of cyber protection measures into the business strategy increases the resilience of enterprises to external threats, strengthens their market positions and promotes the development of digital culture. **Conclusions.** The feasibility of further research aimed at developing models for assessing the effectiveness of investments in information security, taking into account the specifics of enterprises of various scales, is proven. The presented results are of practical importance for business managers, information security specialists and researchers working in the field of digital risk management.*

**Keywords:** *information security, enterprise competitiveness, digital transformation, management strategy, security investments, business resilience.*



**Постановка проблеми.** У сучасних умовах цифрової трансформації питання забезпечення інформаційної безпеки стає важливим чинником стабільного функціонування та розвитку підприємств. Зростаюча кількість кіберзагроз, витоків конфіденційної інформації та кіберінцидентів безпосередньо впливає на репутацію, фінансову стійкість та довіру до бізнесу з боку клієнтів і партнерів. Недостатній рівень захисту інформаційних ресурсів може не лише ускладнити операційну діяльність, а й стати бар'єром для інноваційного розвитку та виходу на нові ринки. Відтак, інформаційна безпека розглядається не лише як технічна необхідність, а як стратегічна детермінанта конкурентоспроможності підприємства.

**Аналіз останніх досліджень і публікацій.** Упродовж останніх років дослідники активно вивчають інформаційну безпеку як чинник конкурентоспроможності підприємств. Білько С. [1] провів оцінювання взаємозв'язку між інформаційною та економічною безпекою, підкреслюючи їх взаємодію в контексті стратегії бізнесу. У роботах Дубницького В. та Науменка Н. [2] окреслено методологічні засади формування інформаційної безпеки на регіональному рівні, що дозволяє екстраполювати висновки на мікроекономічний рівень. Дослідження Крауса К. [3] розкривають особливості цифрової трансформації кібербезпеки під час воєнного стану, акцентуючи увагу на ролі державної політики. Ковальська Л. [4] аналізують економічну сутність інформаційної безпеки регіону як базису стабільності.

Публікації, як Кузьомка В. [5] та Леоненко Н. і Поступної О. [6], розкривають вплив цифровізації на інформаційну безпеку в умовах новітніх загроз. У контексті економічного аналізу заслуговують на увагу праці Науменка Н. [7] щодо наукових напрямів у сфері інформаційної безпеки, а також дослідження Шостак Л. та Помазуна О. [8], які акцентують на зв'язку між інноваційними бізнес-моделями та захистом даних. Яковенко Я. [9] доповнюють тематику, аналізуючи стратегічні орієнтири цифрової трансформації. Практичні аспекти діяльності державних інституцій



висвітлено на сайті Департаменту кіберполіції України [10], що демонструє актуальність державного втручання у сферу безпеки.

Попри наявні досягнення, у дослідженнях залишаються суттєві прогалини, зокрема: недостатньо вивченими є механізми інтеграції інформаційної безпеки у систему стратегічного управління підприємством; бракує моделей оцінки ефективності інвестицій у кіберзахист з погляду конкурентоспроможності. Для їх подолання варто звернутися до новітніх міжнародних джерел: Chotia V. [11] досліджує вплив цифрової трансформації та кібербезпеки на стратегічний управлінський облік підприємств; звіт TEKsystems [12] аналізує цифрову трансформацію як рушій конкурентних переваг; аналітичний матеріал World Economic Forum [13] підкреслює необхідність посилення екосистеми кібербезпеки для безперервності бізнесу. У звіті ЕУ [14] відзначено розрив у сприйнятті кіберзагроз між керівниками, що впливає на стійкість організацій, а дослідження Infotech [15] пропонує практичну модель побудови інформаційної безпеки для малого і середнього бізнесу.

**Виділення невирішених раніше частин загальної проблеми.** Попри наявні теоретичні напрацювання у сфері інформаційної безпеки, залишаються недостатньо дослідженими питання її інтеграції в систему стратегічного управління підприємством з урахуванням чинників конкурентоспроможності. Зокрема, бракує моделей, що дозволяють оцінити ефективність інвестицій у безпеку в контексті досягнення довгострокових бізнес-цілей, а також індикаторів, що відображають вплив рівня кіберзахисту на ринкові позиції підприємства. Існуючі підходи здебільшого орієнтовані на технічні аспекти, ігноруючи економічні, організаційні та репутаційні чинники. Крім того, мало уваги приділяється вивченню бар'єрів, з якими стикаються підприємства різного масштабу, особливо малі та середні, у впровадженні систем захисту. Запропоноване дослідження покликане заповнити ці прогалини, проаналізувавши взаємозв'язок між інформаційною безпекою та



конкурентоспроможністю підприємства, і тим самим розширити існуючі наукові уявлення про стратегічний потенціал кібербезпеки.

**Формулювання цілей статті (постановка завдання)** Метою статті є дослідження інформаційної безпеки як важливого чинника забезпечення конкурентоспроможного розвитку підприємства в умовах цифрової трансформації економіки. З огляду на зростання загроз кіберпростору, посилення регуляторного тиску та зростання цінності інформаційних активів, актуальність теми зумовлюється необхідністю формування нових підходів до управління інформаційними ризиками на стратегічному рівні. У межах дослідження передбачається:

- систематизувати зовнішні та внутрішні чинники, що впливають на рішення підприємств щодо інвестування в інформаційну безпеку;
- визначити виклики та бар'єри, з якими стикаються суб'єкти підприємництва різного масштабу у процесі організації системи захисту інформації;
- проаналізувати стимули (регуляторні, економічні, репутаційні та стратегічні), що спонукають бізнес до впровадження ефективних заходів у сфері інформаційної безпеки;
- обґрунтувати доцільність інтеграції інформаційної безпеки у загальну систему стратегічного управління підприємством як детермінанту його конкурентоспроможності.

Досягнення зазначених цілей дозволить сформувати науково обґрунтовані рекомендації для підприємств щодо розробки та впровадження адаптивної політики інформаційної безпеки, яка мінімізує ризики та створює додаткові можливості для сталого розвитку в цифрову епоху.

**Виклад основного матеріалу дослідження.** У сучасних наукових дослідженнях значна увага приділяється забезпеченню економічної безпеки підприємств, складовою якої є інформаційна безпека. Вчені наголошують, що ефективний захист інформаційних ресурсів є важливим чинником стабільного



функціонування бізнесу, оскільки дозволяє мінімізувати ризики фінансових втрат, запобігти витоку конфіденційних даних та уникнути зловживань з боку конкурентів, кіберзлочинців [1, 2]. Дослідження підкреслюють взаємозв'язок між рівнем цифрової безпеки та загальною конкурентоспроможністю підприємства, адже високий рівень інформаційного захисту сприяє підвищенню довіри з боку партнерів, споживачів і державних інституцій.

В умовах цифровізації бізнес-процесів та зростання кіберзагроз питання забезпечення інформаційної безпеки набуває стратегічного значення для підприємств різних галузей [3]. Інформація перетворюється на основний ресурс, а її захист – на важливу умову стабільного функціонування, збереження конкурентних переваг і довіри з боку партнерів та споживачів. Прийняття рішень щодо інвестування в інформаційну безпеку потребує врахування як зовнішніх викликів, так і внутрішніх характеристик підприємства, що обумовлює актуальність дослідження чинників, які впливають на ці процеси [4]. Багатофакторний підхід до аналізу рішень підприємств інвестувати в інформаційну безпеку представлено на рис. 1.

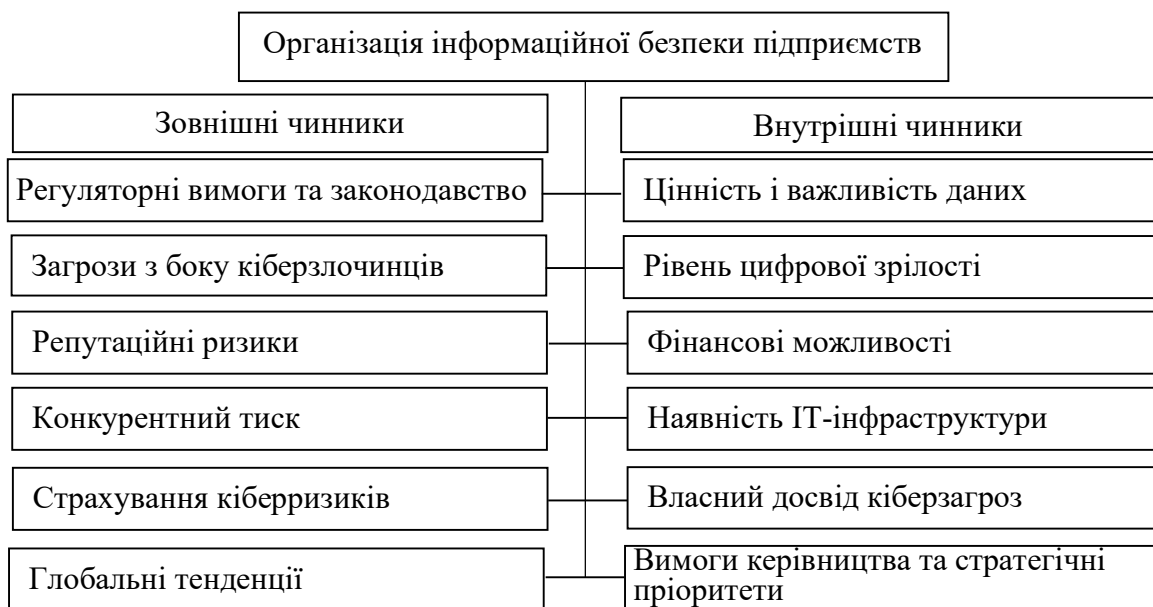


Рис. 1. Чинники впливу на рішення суб'єктів підприємництва інвестувати в інформаційну безпеку.

Джерело: складено на основі [5, 6, 7, 8].



Комплекс системи чинників впливу на рішення суб'єктів підприємництва інвестувати в інформаційну безпеку, відображає системний підхід до управління інформаційною безпекою як до складового елементу стратегічного розвитку підприємства. Зовнішні чинники включають регуляторні вимоги та законодавство, загрози з боку кіберзлочинців, конкурентний тиск, глобальні тенденції й розвиток страхування кіберризиків, що формує зовнішнє середовище функціонування підприємства, в якому забезпечення інформаційної безпеки є умовою дотримання правових норм, збереження ринкових позицій і протидії новітнім загрозам.

Внутрішні чинники включають фінансові можливості підприємства, рівень цифрової зрілості, наявність IT-інфраструктури, власний досвід зіткнення з кіберзагрозами, репутаційні ризики, вимоги керівництва та стратегічні пріоритети, а також оцінку цінності інформаційних активів [9]. Вони формуються у межах самої організації та є результатом її управлінських підходів, ресурсної бази та накопиченого досвіду, а також визначають готовність підприємства інтегрувати інформаційну безпеку у загальну бізнес-стратегію, адаптувати відповідні технології та механізми захисту відповідно до специфіки своєї діяльності. Врахування визначених чинників є необхідною умовою формування ефективної системи інформаційної безпеки, що сприяє сталому та конкурентоспроможному розвитку підприємства. Усвідомлення цінності даних як стратегічного активу стає важливим мотиватором для створення інтегрованої системи інформаційної безпеки, що є передумовою сталого та конкурентоспроможного підприємства.

Загрозу становлять застарілі IT-інфраструктури, слабкий контроль доступу до інформаційних ресурсів, низький рівень цифрової культури та слабка взаємодія з державними інституціями у сфері кіберзахисту [10]. Усе це ускладнює своєчасне реагування на інциденти безпеки та знижує загальну стійкість підприємства до зовнішніх і внутрішніх загроз, що вимагає стратегічного переосмислення підходів до інформаційної безпеки на всіх



рівнях управління. Аналіз цих викликів і бар'єрів дає змогу сформувати цілісне уявлення про проблематику інформаційної безпеки в підприємницькому середовищі та визначити напрямки для підвищення її ефективності [11]. Виклики та можливі бар'єри забезпечення інформаційної безпеки суб'єктів підприємництва систематизовано на рис. 2.



Рис. 2. Виклики та можливі бар'єри забезпечення інформаційної безпеки суб'єктів підприємництва.

Джерело: власна розробка автора



Систематизований комплекс викликів та бар'єрів, що стоять перед підприємствами в процесі забезпечення інформаційної безпеки дозволяє визначити основні перешкоди на шляху до створення системи інформаційного захисту. Виклики охоплюють технічні та організаційно-управлінські аспекти: зростання кіберзагроз, розширення цифрових периметрів, забезпечення безпеки в умовах гібридної війни, економічні обмеження, що є важливим в умовах сучасного бізнес-середовища, яке залежить від цифрових технологій. Диференціація проблем за розміром підприємства визначає різницю в ресурсному забезпеченні та стратегічному підході до безпеки [12, 13].

До основних груп бар'єрів віднесено фінансові, технічні, організаційні, які перешкоджають ефективному впровадженню політик кібербезпеки. Наприклад, для малих підприємств критичним є брак ресурсів і обізнаності, тоді як великі підприємства стикаються зі складністю управління складними системами захисту та відповідністю міжнародним стандартам [14]. Такий підхід відповідає тенденціям ризик-орієнтованого управління та є важливою основою для формування обґрунтованої політики інформаційної безпеки.

Стимули забезпечення інформаційної безпеки суб'єктів підприємництва систематизовано на рис. 3.

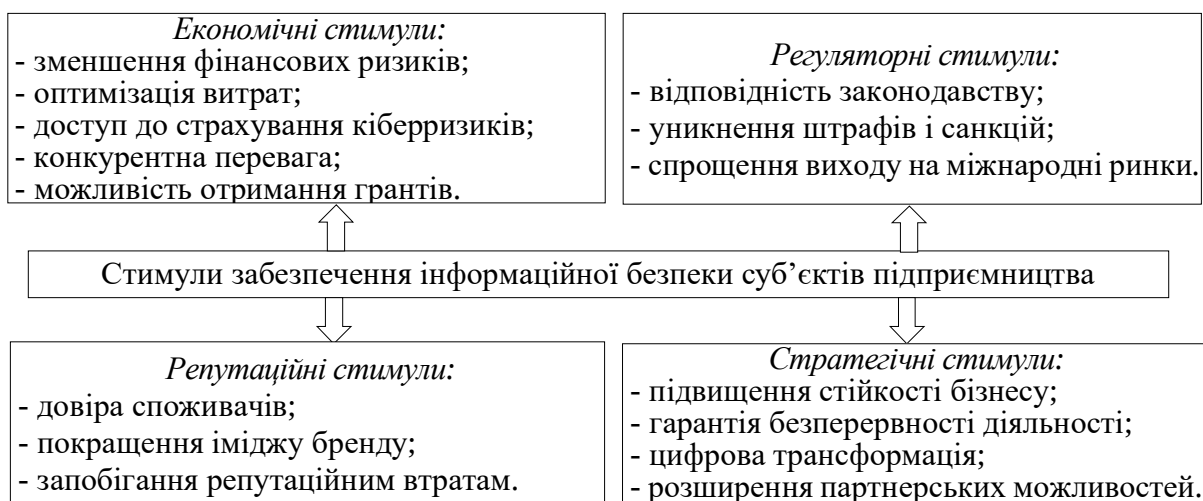


Рис. 3. Стимули забезпечення інформаційної безпеки суб'єктів підприємництва.

Джерело: власна розробка автора



Система стимулів забезпечення інформаційної безпеки суб'єктів підприємництва охоплює чотири вектори: регуляторні, економічні, репутаційні та стратегічні. Така класифікація дозволяє розглядати інформаційну безпеку як багатовимірний інструмент розвитку бізнесу. Регуляторні стимули ґрунтуються на необхідності відповідності чинному законодавству, уникненні штрафних санкцій та спрощенні міжнародної експансії, що особливо актуально в умовах інтеграції українського бізнесу до глобального економічного простору. Економічні стимули вказують на прагматичну вигоду від впровадження заходів безпеки: зменшення фінансових ризиків, оптимізація витрат, доступ до страхування кіберризиків і можливість залучення фінансової підтримки [15].

Репутаційні та стратегічні стимули формують більш довгострокову мотивацію: підвищення довіри споживачів, укріплення іміджу бренду, запобігання кризовим ситуаціям, забезпечення стійкості та цифрової трансформації бізнесу. Ці фактори дозволяють розглядати інформаційну безпеку як інтегрований елемент стратегічного управління, що не тільки знижує ризики, а й створює передумови для зростання. Наукове осмислення даної схеми свідчить про необхідність розробки уніфікованих підходів до оцінювання впливу різних видів стимулів на поведінку підприємств у сфері інформаційної безпеки, а також про доцільність міждисциплінарного підходу, який поєднує правові, економічні, соціальні та технологічні аспекти у процесі формування безпечного бізнес-середовища.

**Висновки.** Інформаційна безпека сьогодні є визначальним чинником конкурентоспроможності підприємств в умовах цифрової трансформації. Комплексний підхід до аналізу зовнішніх і внутрішніх чинників, що впливають на прийняття рішень щодо інвестування в інформаційну безпеку, дозволяє стверджувати про необхідність стратегічної інтеграції безпекових рішень у систему корпоративного управління. Підвищення цифрової зрілості, розвиток IT-інфраструктури, врахування регуляторних вимог і загроз з боку



кіберзлочинців є ключовими передумовами формування ефективної політики захисту інформаційних ресурсів. Аналіз бар'єрів і стимулів до впровадження інформаційної безпеки свідчить про важливу роль управлінських рішень, фінансової підтримки та організаційної культури в досягненні стійкості підприємства до кіберзагроз. Чинники, що стимулюють процес забезпечення інформаційної безпеки (регуляторні, економічні, репутаційні та стратегічні) мають бути враховані при формуванні проактивної безпекової політики, що здатна зменшити ризики та забезпечити довгострокові переваги. Отримані результати мають практичне значення для розробки адаптивних стратегій кіберзахисту, які відповідають потребам підприємств різного масштабу і галузевої приналежності в умовах зростаючої цифрової взаємозалежності.

### **Список використаних джерел**

1. Білько С. Інформаційна та економічна безпека: оцінювання рівня та взаємозв'язку. *Науковий вісник Полісся*. 2022. 1 (24), С. 58-77.
2. Дубницький В.І., Наumenко Н.Ю. Методологічне забезпечення формування інформаційної безпеки в сфері економічної безпеки регіону. *Вісник економічної науки України*. 2019. №1. URL: <http://dspace.nbu.gov.ua/handle/123456789/151638>
3. Краус К.М., Краус Н.М., Штепа О.В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability*. 2022. № 3. С. 26-37.
4. Ковальська Л., Топалов В., Топалов Р. Інформаційна безпека регіону: підходи до розгляду та економічна сутність. *Економічний форум*. 2023. № 13 (2), С. 18-24.
5. Кузьомко В. Інформаційна безпека бізнесу в умовах цифрової трансформації економіки. *Інноваційне підприємництво: стан та перспективи розвитку*: збірник матеріалів VI Всеукраїнська науково-практична конференція (м. Київ, 29-30 березня 2021 р.). Київ: КНЕУ. 2021. С. 26-28.



6. Леоненко Н.А., Поступна О.В. Інформаційна безпека України: механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. *Вісник Національного університету цивільного захисту України*. Серія: Державне управління. 2022. №2 (17). URL: <http://repositsc.nuczu.edu.ua/handle/123456789/16883>.

7. Науменко Н.Ю. Аналіз економічних наукових напрямків у сфері інформаційної безпеки. *Електронне наукове фахове видання з економічних наук «Modern Economics»*. 2019. №16. С. 115-120. URL: <http://dspace.mnau.edu.ua/jspui/bitstream/123456789/6290/1/naumenko.pdf>.

8. Шостак Л., Помазун О. Інформаційна безпека в контексті інноваційного розвитку бізнес-моделі вітчизняних підприємств в умовах цифрової економіки. *Цифрова економіка та економічна безпека*. 2024. № 5 (14), С. 160-165.

9. Яковенко Я.Ю., Білик М.Ю., Олійник Є.В. Цифрова трансформація бізнес-структур: стратегічні орієнтири в епоху інновацій та технологічних змін. *Економічний простір*. 2024. № 190. С. 355-360.

10. Офіційний сайт Департаменту кіберполіції Національної поліції України. URL: <https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadžhennya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/> (дата звернення: 25.03.2025).

11. Chotia V., Yadav R., Rao A. The role of Cyber Security and Digital Transformation in gaining Competitive Advantage through Strategic Management Accounting. *ResearchGate*. 2025. <https://www.researchgate.net/publication/389364533> (дата звернення: 4.04.2025).

12. *State of Digital Transformation* 2025. TEKsystems. 2025. <https://www.teksystems.com/en/insights/state-of-digital-transformation-2025> (дата звернення: 25.03.2025).



13. *Global Cybersecurity Outlook 2025*. World Economic Forum. 2025. [https://reports.weforum.org/docs/WEF\\_Global\\_Cybersecurity\\_Outlook\\_2025.pdf](https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf) (дата звернення: 20.03.2025).

14. *C-suite disconnect on cybersecurity threatens business value and resilience*. Ernst & Young. 2025. [https://www.ey.com/en\\_us/newsroom/2025/04/c-suite-disconnect-on-cybersecurity-threatens-business-value-and-resilience-ey-study-finds](https://www.ey.com/en_us/newsroom/2025/04/c-suite-disconnect-on-cybersecurity-threatens-business-value-and-resilience-ey-study-finds) (дата звернення: 4.04.2025).

15 *Build an Information Security Strategy for Small Enterprises*. Info-Tech Research Group. 2023. <https://www.infotech.com/research/ss/build-an-information-security-strategy-for-small-enterprises> (дата звернення: 10.02.2025).