Маркетинг

УДК 339.5:005.52:005.334

DOI https://doi.org/10.5281/zenodo.20603862

Теоретико-методичні засади дослідження маркетингових ризиків у забезпеченні конкурентоспроможності цифрових бізнес-структур

Леонов Ігор Олександрович,

аспірант кафедри торговельного підприємництва, товарознавства та управління бізнесом, Одеський національний технологічний університет,, м. Одеса, 65039, Україна, https://orcid.org/0009-0001-2973-357X

Прийнято: 22.05.2026 | Опубліковано: 30.05.2026

Анотація. Мета. *Дослідження спрямоване на обґрунтування теоретико-методичних засад аналізу маркетингових ризиків, з якими стикаються бізнес-структури в умовах цифровізації економіки. У роботі визначено роль цих ризиків у забезпеченні довгострокової конкурентоспроможності підприємств за допомогою інтеграції чинників кібербезпеки до капіталу бренда.*

Методи. *Методологічну основу дослідження становить комплекс загальнонаукових та спеціальних підходів. Переосмислення класичних концепцій конкуренції здійснено із застосуванням системного та ситуаційного підходів. Джерела формування ринкових переваг ідентифіковано через призму ресурсного та інституційного аналізу. Для побудови архітектури кібермаркетингових ризиків використано методи логічного узагальнення, декомпозиції та структурно-функціонального моделювання, а для інтегральної оцінки цифрових загроз — метод аналізу ієрархій Томаса Саати.*

Результати. *У межах роботи розширено концептуальне розуміння сутності маркетингових загроз у сучасному макроекономічному середовищі. Сформульовано авторське визначення дефініції «кібермаркетинговий ризик». Цей феномен розглядається як специфічна форма маркетингової загрози, що постає внаслідок вразливості інформаційно-комунікаційної інфраструктури компанії. Її наслідками стають несанкціонований доступ, витік або маніпулювання клієнтськими даними, що руйнує бренд-капітал, еродує репутацію та призводить до втрати ринкових позицій. Автором запропоновано теоретичну модель, яка пов'язує рівень кіберзахищеності підприємства із динамікою лояльності його споживачів (NPS). Систематизація методичних підходів дозволила обґрунтувати доцільність спільного використання якісних і кількісних індикаторів, серед яких виокремлено коефіцієнт відновлення довіри (Trust Recovery Rate) та обсяг збереженого прибутку під загрозою (Cyber-VaR).*

Висновки*. Дослідження доводить, що тотальна діджиталізація практично нівелює межу між технічним захистом інформації та комерційним успіхом компанії. Кібербезпека трансформується із суто операційної функції IT-підрозділу на стратегічну детермінанту конкурентоспроможності. Обґрунтовано доцільність впровадження концепції «Safety Branding», яка виступає інструментом формування випереджаючої ринкової переваги у вигляді «премії за довіру» від споживачів. Сформовані висновки та методичні положення створюють надійне підґрунтя для побудови прикладних систем моніторингу маркетингових ризиків.*

Ключові слова: *кібермаркетинговий ризик, бренд-капітал, цифрова трансформація, безпека даних, лояльність споживачів, премія за довіру, метод аналізу ієрархій.*

ISSN: 2786-9431

Theoretical and Methodological Foundations of Researching Marketing Risks in Ensuring the Competitiveness of Digital Business Structures

Igor Leonov,

PhD Student, Department of Commercial Entrepreneurship, Commodity Science, and Business Management, Odessa National Technological University, Odessa, Ukraine, https://orcid.org/0009-0001-2973-357X

Abstract. Purpose. *The study aims to substantiate the theoretical and methodological foundations for analyzing marketing risks faced by business structures amid the digitalization of the economy. The paper determines the role of these risks in ensuring the long-term competitiveness of enterprises by integrating cybersecurity factors into brand equity.*

Methods. *The methodological framework of the research comprises a complex of general scientific and specialized approaches. Classic concepts of competition are re-evaluated using systemic and situational approaches. The sources of market advantages are identified through the lens of resource-based and institutional analysis. To construct the architecture of cyber-marketing risks, methods of logical generalization, decomposition, and structural-functional modeling are applied, while Thomas Saaty's Analytic Hierarchy Process serves as the methodological basis for the integral assessment of digital threats.*

Results. *The paper expands the conceptual understanding of marketing threats within the modern macroeconomic environment. The author provides an original definition of the "cyber-marketing risk" definition. This phenomenon is viewed as a specific form of marketing threat arising from vulnerabilities in a company's information and communication infrastructure. Its consequences include unauthorized access, data breaches, or manipulation of customer data, which degrades brand equity, erodes reputation, and leads to a critical loss of market positions. The author proposes*

a theoretical model linking a company's cyber-protection level with its customer loyalty dynamics (NPS). The systematization of methodological approaches justifies the combined use of qualitative and quantitative indicators, specifically highlighting the Trust Recovery Rate and Cyber Value at Risk (Cyber-VaR).

Conclusions. *The study proves that total digitalization virtually blurs the line between technical data protection and a company's commercial success. Cybersecurity transforms from a purely operational IT function into a strategic determinant of competitiveness. The paper substantiates the implementation of the "Safety Branding" concept, which serves as a tool for gaining a proactive competitive advantage in the form of a "trust premium" from consumers. The formulated conclusions and methodological guidelines establish a solid foundation for developing applied marketing risk monitoring systems.*

Keywords*: cyber-marketing risk, brand equity, digital transformation, data security, customer loyalty, trust premium, Analytic Hierarchy Process.*

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими чи практичними завданнями

Сучасний глобальний економічний простір перманентно трансформується під впливом технологій, і це докорінно змінює саму природу ринкового суперництва. Бізнес-процеси масово мігрують у віртуальне середовище, розгортаються багатоканальні платформи цифрової дистрибуції, а управління клієнтським досвідом тепер будується на основі великих даних (Big Data). Усе це висуває принципово нові вимоги до забезпечення життєздатності комерційних підприємств. На перший погляд, традиційні фактори лідерства на кшталт масштабу виробництва, доступу до дешевої сировини чи класичних капіталовкладень мають працювати й далі. Але ні. Вони поступово втрачають домінантний статус. Натомість ключовим ресурсом і, що важливо,

 ISSN: 2786-9431

найуразливішим елементом ринкової стійкості стає інформаційна взаємодія між брендом та споживачем.

Звідси постає гостра наукова та практична проблема. Стрімка діджиталізація маркетингу хоч і відкриває безпрецедентні можливості для оптимізації комунікацій, але паралельно плодить специфічні деструктивні загрози. Корпоративні бази даних стають вразливими, канали зв'язку компрометуються, алгоритми пошукової оптимізації зазнають атак, а репутаційним профілем компанії в мережі штучно маніпулюють. По суті, ми маємо абсолютно нове поле ризиків. Воно безпосередньо б'є по капіталу бренда, рівню лояльності клієнтів і руйнує стратегічну конкурентоспроможність бізнес-структур.

Ситуація посилюється тим, що вітчизняний бізнес змушений функціонувати в умовах жорсткого подвійного тиску: з одного боку — макроекономічна нестабільність, з іншого — цілеспрямовані агресивні кібератаки на критичну та комерційну інфраструктуру. Примітно, що традиційний менеджмент, який звик трактувати інформаційну безпеку як виключно інженерно-технічну турботу IT-відділу, виявляється геть неспроможним оцінити реальний масштаб репутаційних та ринкових втрат від цифрових інцидентів. Отже, теоретичне обґрунтування та методичне оформлення інтерфейсу між маркетинговими ризиками й системою забезпечення конкурентоспроможності — це критичний крок. Крок, необхідний для створення прикладних інструментів захисту національного бізнесу.

Аналіз останніх досліджень і публікацій

Теоретичний фундамент для аналізу конкурентних відносин та природи ринкових переваг заклали класики економічної науки. Наприклад, базові положення ресурсного підходу, де фокус спрямовано на унікальні внутрішні компетенції підприємства, детально висвітлив Б. Вернерфельт [1, p. 172]. Концептуальні засади стратегічного вибору та позиціонування бізнес-структур

ISSN: 2786-9431

розкриті в теорії конкурентних сил М. Портера [2, с. 45]. Питання того, як сформувати ринкову орієнтацію як інтегральну філософію управління, знайшли відображення у працях Ж.-Ж. Ламбена [3, с. 112]. Наступний крок зробив Ф. Котлер. В епоху Четвертої промислової революції він запропонував концепцію «Маркетинг 5.0», де обґрунтував необхідність синергії між технологічними інноваціями та гуманістичним підходом, окремо наголосивши на важливості захисту приватних даних користувачів [4, с. 88].

Проблематику ідентифікації та мінімізації маркетингових ризиків в інноваційній діяльності активно досліджують вітчизняні науковці. Зокрема, Ілляшенко С.М детально описує механізми адаптації підприємств до умов невизначеності під час виведення на ринок нових продуктів [5, с. 210]. Питання стратегічного аналізу й формування адаптивного маркетингового потенціалу компаній висвітлені у дослідженнях Н. В. Куденко [6, с. 154]. Слід визнати, що більшість класичних підходів вітчизняної школи ризикології досі зосереджена на операційних, товарних або цінових ризиках. Специфіка віртуального простору залишається поза увагою.

Емпіричний аналіз сучасної архітектури цифрових загроз спирається на щорічні глобальні звіти провідних міжнародних інституцій. Згідно з даними аналітичного центру IBM Security «Cost of a Data Breach Report 2024», фінансові наслідки витоків інформації мають виражений довгостроковий репутаційний ефект і призводять до стрімкого відтоку клієнтів [7]. Дослідження компанії Gartner підтверджують: параметри конфіденційності та цифрової безпеки трансформувалися з нудних регуляторних вимог у ключовий фактор диференціації брендів на ринку [8, p. 48]. Соціологічні зрізи Edelman Trust Barometer фіксують пряму залежність між рівнем технологічної захищеності компанії та загальним індексом довіри споживачів до її продукції [9]. Крім того, математичний інструментарій для оцінювання складних багатокритеріальних

ISSN: 2786-9431

систем покладено в основу класичної праці Т. Сааті щодо методу аналізу ієрархій [10, с. 67].

Попри значний масив наукових напрацювань, залишається низка методологічних суперечностей. Більшість існуючих публікацій чітко розмежовують технічні аспекти кібербезпеки (Information Security) та економічні параметри маркетингу. Як саме технічні вразливості трансформуються в ринкові деструкції? Як це позначається на підсумковій конкурентоспроможності бізнес-структури? Ці питання досі не отримали цілісного концептуального висвітлення.

Виділення невирішених раніше частин загальної проблеми

Поза увагою дослідників залишається механізм конвертації параметрів цифрової безпеки у структуру бренд-капіталу. Наукова спільнота детально вивчає технологічні методи захисту баз даних на кшталт шифрування чи брандмауерів, але методичного апарату, який дозволив би перевести ці інженерні параметри на мову маркетингового менеджменту, просто немає. Зокрема, ніхто не визначив систему показників (KPI), здатну кількісно виміряти ерозію репутації компанії після кібератак. Так само відсутні моделі, що описують виникнення «премії за довіру» за умови безпечного поводження з клієнтськими даними. Усе це зумовлює необхідність формування нової парадигми дослідження маркетингових ризиків у цифровому середовищі.

Формулювання цілей статті (постановка завдання)

Мета цієї статті полягає в комплексному обґрунтовуванні теоретико-методичних засад дослідження маркетингових ризиків та їхнього безпосереднього впливу на формування конкурентоспроможності бізнес-структур в умовах діджиталізації. При цьому ми виокремлюємо специфічну категорію «кібермаркетингових ризиків» і систематизуємо методи їхнього інтегрального оцінювання.

Для досягнення цієї мети ми поставили перед собою такі завдання:

1. Систематизувати та критично переосмислити існуючі наукові підходи до трактування конкурентоспроможності підприємства в епоху цифрової економіки.
2. Розкрити сутність і внутрішню структуру маркетингових ризиків нового покоління, запропонувати авторську дефініцію кібермаркетингового ризику та побудувати логічну модель його впливу на ринкові позиції компанії.
3. Проаналізувати та структурувати методичні підходи до оцінювання маркетингових ризиків, обґрунтувавши доцільність використання інтегральних моделей для прийняття стратегічних управлінських рішень.

Виклад основного матеріалу дослідження

1.1. Наукові підходи до формування конкурентоспроможності бізнес-структур

Класичне розуміння конкурентоспроможності суб'єктів господарювання тривалий час ґрунтувалося переважно на статичних параметрах. Проте системна цифрова трансформація макроекономічного середовища зумовлює необхідність глибокого переосмислення традиційних наукових підходів. Доцільно розглянути три провідні теоретичні концепції крізь призму сучасних ринкових реалій:

- Ресурсний підхід. У межах цієї концепції, методологічно заснованої на працях Б. Вернерфельта [1], конкурентоспроможність підприємства визначається наявністю унікальних, складно копійованих внутрішніх активів. В умовах цифрової економіки цей підхід зазнає суттєвих трансформацій: матеріальні чинники (виробничі потужності, обладнання) поступаються першістю нематеріальним інформаційним ресурсам. Ключовими активами стають структуровані масиви даних, патенти, клієнтські бази та алгоритми штучного інтелекту. Відповідно, спроможність забезпечити надійну безпеку цих інформаційних масивів від

ISSN: 2786-9431

зовнішніх засягань перетворюється на першочергову умову утримання ринкового лідерства.

- Інституційний підхід. Фокусує увагу на зовнішніх правилах функціонування ринку, регуляторних обмеженнях та специфіці взаємодії із соціально-економічними інститутами. На сучасному етапі цей підхід вимагає від бізнес-структур бездоганного дотримання жорстких міжнародних та національних регламентів щодо захисту конфіденційності даних (зокрема, GDPR [8]). Невідповідність цим інституційним стандартам здатна миттєво ізолювати підприємство від глобальних ланцюгів створення вартості, що критично знижує його конкурентні позиції.
- Системний (ситуаційний) підхід. Розглядає підприємство як відкриту систему, що перебуває у постійному процесі обміну інформацією та ресурсами із зовнішнім середовищем [3]. В умовах діджиталізації цей підхід набуває особливої ваги, оскільки швидкість реакції системи на ринкові імпульси стає визначальним критерієм її виживання. Конкурентоспроможність у цьому контексті трактується як динамічна здатність підприємства гнучко адаптувати свої маркетингові канали до непередбачуваних змін споживчих пріоритетів та технологічних викликів.

Узагальнення зазначених концепцій дозволяє дійти висновку, що сучасна конкурентоспроможність бізнес-структури є не статичним станом, а динамічною властивістю системи. Вона полягає у здатності оперативно адаптуватися до змін, захищати власні інформаційні активи та генерувати високий рівень споживчої довіри в умовах перманентної ринкової невизначеності.

1.2. Дослідження сутності маркетингових ризиків та їхньої ролі у формуванні конкурентоспроможності бізнес-структур

Трансформація економічних систем у цифровий формат спричиняє видозміну традиційної природи маркетингових ризиків. Якщо в класичному розумінні маркетинговий ризик розглядався переважно як ймовірність

ISSN: 2786-9431

недоотримання прибутку через помилки в ціноутворенні, збутовій політиці чи рекламній діяльності [5], то в сучасному високотехнологічному просторі спектр загроз суттєво розширився. Це зумовлює необхідність введення в науковий обіг дефініції «кібермаркетинговий ризик».

Кібермаркетинговий ризик — це специфічна форма маркетингової загрози, яка виникає внаслідок вразливості інформаційно-комунікаційної інфраструктури бізнес-структури й може призвести до несанкціонованого доступу, витоку або маніпулювання даними споживачів, що спричиняє деструкцію бренд-капіталу, репутаційну ерозію та критичне падіння конкурентоспроможності компанії на ринку.

Внутрішня архітектура зазначеної категорії дозволяє виокремити такі ключові вектори деструктивного впливу:

1. Ризик компрометації персональних даних (Data Breach Risk) — загроза несанкціонованого розголошення чи витоку конфіденційної інформації клієнтів, що руйнує базовий рівень довіри до компанії.
2. Ризик деструкції цифрових каналів комунікації (Channel Hijacking) — несанкціоноване захоплення або злам офіційних веб-ресурсів, платформ чи корпоративних акаунтів у соціальних мережах з метою поширення викривленої інформації від імені бренда.
3. Ризик недобросовісної цифрової конкуренції (Ad Fraud / SEO-attacks) — штучне маніпулювання показниками ефективності інтернет-реклами за допомогою бот-трафіку або цілеспрямована песимізація позицій корпоративного сайту в пошукових системах через агресивні зовнішні втручання.

Механізм деструктивного впливу кібермаркетингового ризику на інтегральний рівень конкурентоспроможності бізнес-структури має характер послідовної ланцюгової реакції (рис. 1).

ISSN: 2786-9431

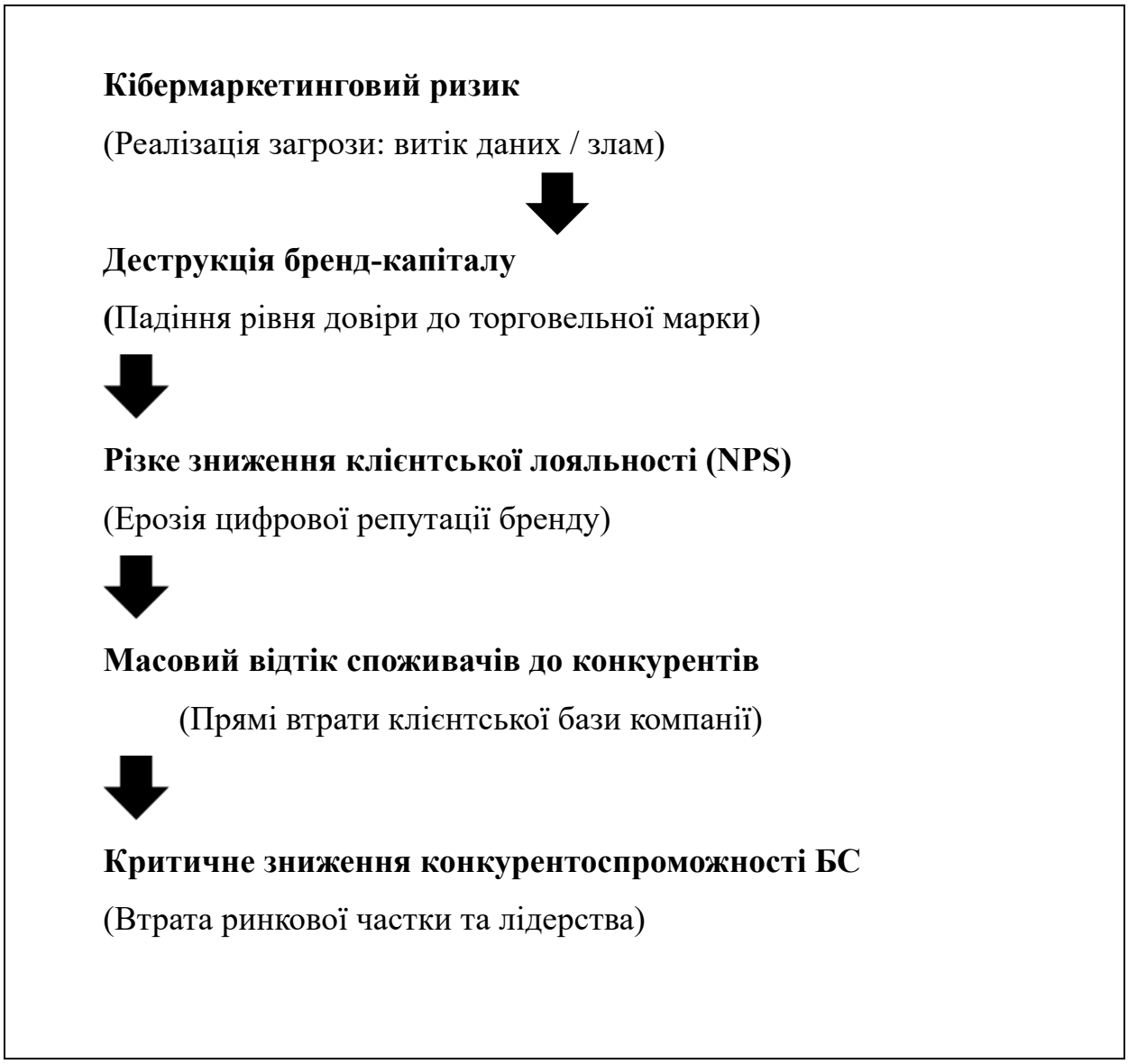

Рис. 1. Логічна модель деструктивного впливу кібермаркетингового ризику на конкурентоспроможність бізнес-структури

Джерело: власна розробка автора

Досліджуваній категорії притаманна виражена дуалістична природа. З погляду деструктивного потенціалу, ігнорування кібермаркетингових загроз неминуче призводить до деградації ринкових позицій суб'єкта господарювання. Водночас свідома інтеграція інструментів управління цими ризиками до загальної корпоративної стратегії здатна трансформувати загрози на джерело додаткових переваг. Підприємство, яке спроможне гарантувати споживачеві

надійний захист його «цифрового сліду», забезпечує формування так званої «премії за довіру» (*Trust Premium*). За таких умов клієнти свідомо віддають перевагу безпечнішому бренду, демонструючи низьку еластичність попиту за ціною на тлі високої еластичності за безпековим фактором.

1.3. Методичні підходи до дослідження маркетингових ризиків та конкурентоспроможності

Формування надійного аналітичного інструментарію передбачає синергетичне поєднання якісних та кількісних методів оцінювання ризиків. Специфіка сучасного цифрового середовища нівелює можливість ефективного використання виключно класичних фінансових показників. Останні характеризуються значним часовим лагом і відображають лише фактичні, вже завдані підприємству збитки, що унеможливлює оперативне реагування. З огляду на це постає гостра потреба в інтеграції та практичному застосуванні предиктивних (випереджаючих) індикаторів.

Комплексну порівняльну характеристику базових методичних підходів до аналізу ризиків у розрізі їхнього впливу на конкурентоспроможність бізнес-структур узагальнено в табл. 1.

Напрям методики	**Ключові аналітичні інструменти**	**Переваги та обмеження застосування в аналізі конкурентоспроможності**
Якісний аналіз	Модернізований SWOT-аналіз, метод сценаріїв, експертні панелі (Delphi)	*Переваги:* Дозволяє оперативно ідентифікувати слабкі місця в системі безпеки. *Обмеження:* Високий рівень суб'єктивізму оцінок експертів.
Кількісний аналіз	Розрахунок показника ROMI, аналіз волатильності попиту, моделювання Монте-Карло	*Переваги:* Дає чіткі фінансові орієнтири втрат маркетингового бюджету. *Обмеження:* Ігнорує важковимірювані репутаційні активи та лояльність.
	Метод аналізу	*Переваги:* Синтезує якісні параметри сприйняття бренду клієнтами із суворими математичними моделями фінансових втрат.

ISSN: 2786-9431

Комплексний (інтегральний) підхід	ієрархій (Т. Сааті), розрахунок індикаторів *Cyber-VaR* та *Trust Recovery Rate*	*Обмеження:* Потребує постійного моніторингу великих масивів первинних даних.

Джерело: власна розробка автора на основі аналізу джерел [5, 6, 10]

У контексті дослідження інтеграційного інтерфейсу «ризик — конкурентоспроможність» найбільш обґрунтованим видається комплексний підхід, заснований на методі аналізу ієрархій (MAI) Томаса Сааті [10]. Застосування цього математичного інструментарію забезпечує можливість декомпозиції генеральної мети — досягнення максимального рівня конкурентоспроможності бізнес-структури — на окремі взаємопов'язані рівні. До структури зазначеної моделі інтегруються базові критерії (фінансові, репутаційні, клієнтські) та відповідні альтернативи, що відображають варіанти стратегічних рішень спрямованих на мінімізацію ризиків.

Завдяки процедурі попарного порівняння чинників на основі поєднання експертних оцінок та емпіричних даних здійснюється розрахунок векторів пріоритетів. Отримані матричні значення дозволяють чітко ідентифікувати, який саме елемент кібермаркетингового ризику (наприклад, загроза витоку баз даних CRM-систем чи несанкціоноване втручання в роботу веб-ресурсів) чинить найбільш деструктивний вплив на ринкову частку підприємства. Це створює об’єктивне методичне підґрунтя для переформатування фінансового забезпечення безпеки із категорії суто операційних витрат у стратегічний складник інвестицій у довгострокову конкурентоспроможність компанії.

ВИСНОВКИ

1. Систематизація ресурсного, інституційного та системного підходів доводить: у цифровому середовищі конкурентоспроможність компаній прямо залежить від їхньої здатності управляти інформаційними потоками та захищати активи. Статичні переваги більше не працюють, поступаючись місцем динамічній адаптивності.

2. Концептуальний аналіз маркетингових загроз дозволив нам сформулювати авторське визначення «кібермаркетингового ризику» як інтегральної загрози для бренд-капіталу. Створена логічна модель описує, як технічні вразливості інфраструктури переходять у фінансові втрати через падіння лояльності клієнтів (NPS) та їх відтік до конкурентів.
3. Аналіз методичних підходів підтвердив, що оцінювання таких ризиків потребує комплексного інструментарію. Ми обґрунтували доцільність поєднання методу аналізу ієрархій Т. Сааті зі специфічними індикаторами (Trust Recovery Rate, Cyber-VaR). Це дає керівникам бізнесу математичну основу для прийняття стратегічних рішень в умовах невизначеності.

Наші подальші дослідження ми зосередимо на зборі первинних емпіричних даних через масштабне анкетування споживачів. Це необхідно для практичного розрахунку запропонованих коефіцієнтів та побудови прикладних економетричних моделей.

Список використаних джерел

1. Wernerfelt B. A resource-based view of the firm. *Strategic Management Journal*. 1984. Vol. 5, No. 2. P. 171–180.
2. Портер М. Конкурентна стратегія: методики аналізу галузей і конкурентів / пер. з англ. А. Олійник. Київ: Наш Формат, 2021. 392 с.
3. Ламбен Ж.-Ж. Менеджмент, ориентированный на рынок / пер. с англ. под ред. В. Б. Колчанова. Санкт-Петербург: Питер, 2007. 800 с.
4. Котлер Ф., Картаджая І., Сетіаван Г. Маркетинг 5.0. Технології для людства / пер. з англ. Київ: КМ-Букс, 2022. 288 с.
5. Ілляшенко С. М. Маркетинг інновацій і інновації в маркетингу: монографія. Суми: ВТД «Університетська книга», 2008. 615 с.
6. Куденко Н. В. Стратегічний маркетинг: навч. посібник. Київ: КНЕУ, 2006. 523 с.

7. IBM Security. Cost of a Data Breach Report 2024. URL: https://www.ibm.com/reports/data-breach (accessed: 15.04.2026).

8. Gartner Research. Predicts 2025: Privacy and Cybersecurity as Core Brand Competitiveness Drivers. *Gartner IT Practices*. 2024. Vol. 14. P. 45–52.

9. Edelman. 2024 Edelman Trust Barometer. URL: https://www.edelman.com/trust/2024-trust-barometer (accessed: 18.04.2026).

10. Саати Т. Принятие решений. Метод анализа иерархий / пер. с англ. Москва: Радио и связь, 1993. 278 с.

11. Назарова Г. В., Іванова О. А. Управління ризиками бізнес-структур в умовах діджиталізації економіки. *Економіка та суспільство*. 2023. Вип. 49. С. 112–119.

12. Скриль В. В. Модернізація системи маркетингового менеджменту підприємства під впливом кіберзагроз. *Маркетинг і менеджмент інновацій*. 2022. № 3. С. 84–93.

13. Chigada J., Madzingira I. Cyber-security threats and mitigation strategies in digital marketing ecosystems. *Journal of Digital Marketing Strategy*. 2021. Vol. 9, No. 4. P. 312–325.

14. Reshetnikova I., Smerichevskyi S. Strategic marketing choices of business structures under conditions of digital landscape volatility. *Information Systems and Management*. 2023. Vol. 11, No. 2. P. 145–153.

15. Попова Л. О., Каніщенко О. Л. Формування довіри до бренду через призму безпеки клієнтських даних в електронній комерції. *Вісник Київського національного університету імені Тараса Шевченка. Економіка*. 2024. Вип. 2(225). С. 34–41.

ISSN: 2786-9431