

Літвінов Дмитро Олександрович, доктор філософії з управління та адміністрування, кафедра торговельного підприємництва, товарознавства та управління бізнесом, Одеський національний технологічний університет

Панасюк В'ячеслав Петрович, аспірант кафедри маркетингу, підприємництва і торгівлі, Одеський національний технологічний університет

Матузний Олексій Олександрович, аспірант кафедри маркетингу, підприємництва і торгівлі, Одеський національний технологічний університет

Улич Мар'яна Володимирівна, науковий співробітник Інституту тваринництва НААН

Бірюков Ярослав, аспірант кафедри журналістики та реклами Державного торговельно-економічного університету

Litvinov Dmytro, Doctor of Philosophy in Management and Administration, Department of Trade Entrepreneurship, Commodity Studies and Business Management, Odesa National University of Technology, <https://orcid.org/0000-0001-8612-3834>

Panasyuk Vyacheslav, Postgraduate student of the Department of Marketing, Entrepreneurship and Trade, Odesa National University of Technology, Ukraine, <https://orcid.org/0009-0002-5801-4440>

Matuznyi Oleksii, Postgraduate student of the Department of Marketing, Entrepreneurship and Trade, Odesa National University of Technology, Ukraine, <https://orcid.org/0009-0002-0924-2690>

Ulych Mariana, Research Fellow at the Livestock Farming Institute of the National Academy of Agrarian Sciences of Ukraine, <https://orcid.org/0009-0006-5905-6529>

Biriukov Yaroslav, Postgraduate student at the Department of Journalism and Advertising, State University of Trade and Economics, <https://orcid.org/0009-0006-6198-1617>

ДОВІРА СПОЖИВАЧІВ ТА КІБЕРБЕЗПЕКА У ЦИФРОВОМУ МАРКЕТИНГОВОМУ СЕРЕДОВИЩІ CONSUMER TRUST AND CYBERSECURITY IN THE DIGITAL MARKETING ENVIRONMENT

Літвінов Д.О., Панасюк В. П., Матузний О. О., Улич М. В., Бірюков Я. Довіра споживачів та кібербезпека у цифровому маркетинговому середовищі. *Український журнал прикладної економіки та техніки*. 2026. Том 11. № 1. С. 316 – 320.

Litvinov D., Panasyuk V., Matuznyi O., Ulych M., Biriukov Y. Consumer trust and cybersecurity in the digital marketing environment. *Ukrainian Journal of Applied Economics and Technology*. 2026. Volume 11. № 1. pp. 316 – 320.

Статтю присвячено вивченню ролі кібербезпеки в процесі формування довіри споживачів у цифровому маркетинговому середовищі. Визначено, що використання сучасних цифрових інструментів маркетингу сприяє підвищенню ефективності комунікації з клієнтами, проте водночас підвищує вимоги до захисту персональних даних користувачів. Виявлено високий рівень занепокоєння користувачів щодо можливих витоків персональної інформації під час здійснення онлайн-транзакцій. Визначено, що факти кіберінцидентів впливають на рівень довіри до брендів, знижують готовність споживачів до подальшої взаємодії з компаніями та можуть призводити до втрати значної частини клієнтської бази. Проаналізовано масштабні кібератаки на цифрові платформи: випадки компрометації облікових записів користувачів та витоків персональних даних, що спричинили суттєві репутаційні та економічні втрати для компаній. Обґрунтовано, що забезпечення належного рівня інформаційної безпеки безпосередньо впливає на такі маркетингові показники: рівень лояльності клієнтів, конверсію продажів, репутацію бренду та конкурентоспроможність підприємства. Визначено основні напрями підвищення довіри споживачів до цифрових маркетингових платформ, серед яких впровадження сучасних технологій кіберзахисту, забезпечення прозорості обробки персональних даних, сертифікація цифрових сервісів, підвищення кіберграмотності користувачів та інтеграція принципів інформаційної безпеки у маркетингову стратегію підприємства. Реалізація зазначених заходів сприятиме формуванню безпечного цифрового маркетингового середовища, підвищенню рівня довіри споживачів та забезпеченню сталого розвитку бізнесу в умовах цифрової трансформації економіки.

Ключові слова: цифровізація, маркетинг, цифровий маркетинг, кібербезпека, довіра споживачів, електронна комерція, інформаційна безпека, інтернет-середовище.

The article examines the role of cybersecurity in shaping consumer trust in the digital marketing environment. The relevance of the research topic is confirmed by the growing volumes of collection, processing, and storage of users' personal data amid the rapid digitalization of the economy and the active use of digital marketing tools, which, in turn, are accompanied by personal data leaks and cyber incidents. In this regard, the study aims to determine the role of cybersecurity in shaping consumer trust in the digital marketing environment and to outline directions for developing a system to protect personal data in marketing processes. To achieve this goal, the article examines the features of the transformation of enterprises' marketing activities. It is determined that the use of modern digital marketing tools increases the efficiency of communication with customers; however, it also raises the requirements for protecting users' personal data. A high level of user concern regarding possible personal data breaches during online transactions has been identified. It has been established that cyber incidents influence trust in brands, reduce consumers' willingness interacting with companies, and may lead to the loss of a significant portion of the customer base. Large-scale cyberattacks on digital platforms have been analyzed, including cases of user account compromise and personal data leaks that have caused significant reputational and economic losses for companies. It is substantiated that ensuring an adequate level of information security directly affects the following marketing indicators: customer loyalty, sales conversion, brand reputation, and enterprise competitiveness. The main directions for increasing consumer trust in digital marketing platforms have been identified, including implementing modern cybersecurity technologies, ensuring transparency in the processing of personal data, certifying digital services, increasing users' cyber literacy, and integrating information security principles into enterprises' marketing strategies. The implementation of these measures will help create a secure digital marketing environment, increase consumer trust, and ensure sustainable business development amid the digital transformation of the economy.

Keywords: digitalization, marketing, digital marketing, cybersecurity, consumer trust, e-commerce, information security, internet environment.

Вступ

Цифровізаційні процеси в економіці та стрімкий розвиток інформаційно-комунікаційних технологій останніми роками зумовили трансформацію підходів до формування та реалізації маркетингових стратегій підприємств. Цифрове маркетингове середовище сьогодні є платформою для взаємодії підприємств зі споживачами, яка забезпечує оперативний обмін інформацією, персоналізацію пропозицій та розширення каналів комунікації. Така трансформація супроводжується зростанням ризиків, які пов'язані з кіберзагрозами, витоків персональних даних, шахрайством у мережі та порушенням конфіденційності інформації. Наявність ризиків обумовлює рівень довіри споживачів до цифрових сервісів та



This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.

© Літвінов Дмитро Олександрович,
Панасюк В'ячеслав Петрович,
Матузний Олексій Олександрович,
Улич Мар'яна Володимирівна,
Бірюков Ярослав, 2026

маркетингових комунікаційних каналів підприємств. Довіра споживачів нині є нематеріальним активом підприємства, наявність якого визначає ефективність онлайн-взаємодії та конкурентоспроможність бізнесу. Умови інтенсивного використання цифрових платформ, соціальних мереж, мобільних додатків та систем електронних платежів підвищили значення кібербезпеки маркетингової інфраструктури підприємства. Неналежний рівень захисту інформаційних систем чи недосконалі механізми управління даними призводять до втрати довіри користувачів, зниження репутації бренду і фінансових втрат, отже, необхідність їх удосконалення обумовлює актуальність дослідження.

Питання забезпечення довіри споживачів та організації кібербезпеки в цифровому маркетинговому середовищі широко досліджуються у вітчизняних та закордонних працях. У праці Борисенко О. [1] розкрито аспекти застосування онлайн-платформ, систем аналітики даних і персоналізованих комунікацій та визначено необхідність посилення механізмів захисту даних і формування довіри користувачів до цифрових сервісів. Проблеми оптимізації процесів функціонування електронної комерції та автоматизації обробки замовлень досліджено в праці Седашової О. та Годяцького А. [2], в якій автори прийшли до висновку, що стабільність функціонування цифрових платформ значною мірою залежить від надійності інформаційних систем і безпеки електронних транзакцій. Сучасні тенденції розвитку цифрового маркетингу узагальнено у роботі Сур'янегара Е. та співавторів [3]. У роботі Бахаз С. та співавторів [4] обґрунтовано, що застосування технологій штучного інтелекту в цифровому маркетингу значно підвищує ефективність таргетування та аналізу поведінки споживачів, однак водночас підвищує вимоги до захисту персональних даних. Питання етичного використання даних та конфіденційності інформації досліджено в праці Аданьїн А. [5]. Практичні аспекти забезпечення кібербезпеки розглянуто у роботі Холтхаус Р. та співавторів [6].

Незважаючи на значну кількість праць, присвячених питанням цифрового маркетингу, управління взаємовідносинами зі споживачами та інформаційної безпеки, недостатньо розкритими залишаються питання підтримання кібербезпеки в системі цифрового маркетингу підприємств та її вплив на формування довіри споживачів, чим і обумовлена мета дослідження.

Формулювання цілей статті

Метою статті є визначення ролі кібербезпеки у формуванні довіри споживачів в цифровому маркетинговому середовищі та обґрунтування напрямів щодо формування системи із забезпечення захисту персональних даних в маркетингових процесах.

Для досягнення поставленої мети окреслено такі завдання:

- дослідити особливості трансформації маркетингових процесів під впливом цифровізації економіки та розвитку електронної комерції;
- визначити вплив кіберзагроз та витоків даних на поведінку споживачів і їх рівень довіри до цифрових платформ;
- проаналізувати наслідки кіберінцидентів в цифровому маркетинговому середовищі на прикладі відомих компаній;
- дослідити міжнародний досвід регулювання аспектів кібербезпеки та захисту персональних даних;
- обґрунтувати вплив кібербезпеки на маркетингові показники діяльності підприємств;
- обґрунтувати напрями підвищення рівня цифрової довіри та формування безпечного маркетингового середовища.

Виклад основного матеріалу дослідження

Цифровізація економіки та стрімкий розвиток електронної комерції докорінно трансформували механізми взаємодії підприємств зі споживачами, що зумовило перегляд підходів до організації маркетингової діяльності, каналів комунікації та способів формування споживчої цінності.

Сучасне цифрове маркетингове середовище характеризується активним використанням онлайн-платформ, соціальних мереж, мобільних застосунків, систем персоналізації контенту, технологій штучного інтелекту, аналізу великих даних, тощо. Дослідження провідних науковців [1–4] показали, що залучення зазначених інструментів робить можливим: по-перше, більш ефективний аналіз поведінки споживачів; по-друге, формування персоналізованих маркетингових пропозицій; по-третє, оптимізацію комунікаційних процесів; по-четверте, підвищення результативності реалізації маркетингових стратегій в цифровому середовищі.

Цифровізація маркетингових процесів супроводжується значним зростанням обсягів збору, зберігання та обробки персональних даних користувачів, а це створює нові виклики для інформаційної безпеки та захисту конфіденційності даних. Тож погоджуємось з Борисенко О. [1], що особливого значення набуває проблема формування та підтримки довіри споживачів до цифрових платформ, брендів та каналів електронної взаємодії, оскільки саме довіра споживачів обумовлює рівень залученості клієнтів та їх лояльність.

У дослідженні в сфері електронної комерції [5] обґрунтовано, що довіра споживачів у цифровому маркетинговому середовищі формується під впливом комплексу взаємопов'язаних факторів, серед яких: рівень захисту персональних даних, прозорість політики конфіденційності та обробки інформації, репутація бренду, безпечність платіжних систем, ефективність механізмів кібербезпеки, які застосовуються підприємствами. Саме інтеграція сучасних механізмів інформаційної безпеки з маркетинговими інструментами забезпечує стабільність функціонування електронних каналів комунікації. Активне розповсюдження технологій штучного інтелекту, машинного навчання та аналізу великих даних у сфері роздрібною торгівлі сприяє підвищенню ефективності персоналізації, проте і викликає занепокоєння з боку споживачів щодо рівня конфіденційності даних та ризиків несанкціонованого доступу до їх ресурсів. Належне забезпечення високого рівня кібербезпеки та наявність прозорої системи управління персональними даними стало невід'ємною складовою сучасних стратегій.

Кіберінциденти дуже негативно впливають на споживчу поведінку та репутацію компаній. Згідно з дослідженням [6], близько 58 % споживачів вважають компанії, які зазнали витоку даних, ненадійними та менш безпечними для здійснення подальших онлайн-взаємодій. Крім того, за даними [7] приблизно 70 % клієнтів після кіберінциденту припиняють користуватися послугами бренду або значно скорочують обсяги взаємодії з ним. Додатково дослідження [8] показало, що 66 % користувачів втрачають довіру до компанії після розголошення або несанкціонованого використання їх персональних даних. За даними [9], близько 30 % опитаних споживачів зазначили, що хоча б один раз стикалися з випадками розкриття або витоку персональної інформації після здійснення онлайн-покупок.

Споживачі переймаються і щодо безпеки цифрових транзакцій, зокрема, за даними [10], близько 90 % споживачів висловили занепокоєння можливістю викрадення або несанкціонованого використання їхніх

персональних даних під час здійснення онлайн-покупок (рис. 1). 97 % покупців озвучили насторожене ставлення до незнайомих інтернет-магазинів, що говорить нам про важливість репутації бренду, прозорості інформаційної політики та наявності підтверджених механізмів кіберзахисту. Крім того, приблизно 90 % користувачів хоча б один раз відмовлялися від здійснення покупки в інтернеті через сумніви щодо безпеки веб-сайту або відсутність достатніх гарантій захисту персональних даних [10].

Поряд із поведінковими змінами споживачів, дослідження всесвітньо відомої компанії PwC щодо кіберризиків [11] вказує на значні економічні втрати бізнесу, що пов'язані з кіберінцидентами та витоками даних. Середня вартість витоку інформації для компаній у світі перевищує 3300 тис. дол. Сюди входять витрати на ліквідацію наслідків інцидентів, компенсацію збитків клієнтам, відновлення інформаційних систем та втрати репутаційного характеру. На усунення наслідків від хмарних кіберзагроз витрачено 1254 тис. дол., від витоків даних через сторонніх постачальників витрачено 924 тис. дол., від операцій зі злому та втрати інформації витрачено 1122 тис. дол. (рис. 2). Водночас лише близько 2 % опитаних компаній мали повноцінно сформовану систему кіберстійкості, яка ґрунтується на комплексному управлінні кіберризиками, впровадженні сучасних технологій захисту інформації та систематичному моніторингу кіберзагроз.

Далі дослідимо реальні випадки кібератак та їх наслідки для постраждалих компаній:

1. Хакерська атака на американську компанію «23andMe».

«23andMe» – це компанія, яка знаходиться в Сан-Франциско (штат Каліфорнія), надає послуги персонального генетичного тестування. У 2023 році компанія зазнала масштабної кібератаки на облікові дані, вона передбачала використання раніше викрадених паролів для отримання несанкціонованого доступу до акаунтів користувачів. Тоді було зламано близько 14 тис. облікових записів клієнтів. Проте через особливості роботи компанії, зокрема родичі мають можливість взаємного доступу до генетичних даних один одного, масштаб витоку значно розширився і торкнувся понад 5,5 млн користувачів [12]. Після інциденту компанія була змушена вжити низку термінових заходів для відновлення довіри користувачів: запровадити обов'язкову двофакторну аутентифікацію, посилити політику безпеки облікових записів та провести масове оновлення паролів користувачів.

2. Масовий витік даних з цифрових платформ у 2025 році.

У 2025 році мав місце один із наймасштабніших витоків облікових даних за всю світову історію. Тоді у відкритому доступі з'явилася понад 16 млрд логінів і паролів користувачів різних онлайн-сервісів [13]. Облікові дані використовуються кіберзлочинцями для здійснення подальших атак, несанкціонованого доступу до цифрових платформ, фінансового шахрайства та викрадення персональної інформації. Значні ризики пов'язані із діяльністю брокерів даних, тобто компаній, які спеціалізуються на зборі, аналізі та продажі інформації про користувачів. За оцінками Спільного економічного комітету Конгресу США [14], витоки даних протягом 2025 року спричинили понад 20,9 млрд дол. збитків.

3. Витік даних з платформи з електронної комерції «Ticketmaster».

Платформа електронної комерції Ticketmaster, що спеціалізується на онлайн-продажу квитків, у 2024 р. зазнала масштабного витоку даних користувачів. Внаслідок компрометації стороннього хмарного підрядника «Snowflake» було скомпрометовано персональні дані приблизно 560 млн користувачів. Серед викраденої інформації були імена клієнтів, адреси електронної пошти, номери телефонів, платіжна інформація та історія замовлень. Розслідування показало, що причиною інциденту став несанкціонований доступ до облікових записів співробітників постачальника послуг, через що зловмисники отримали доступ до клієнтських баз даних [15]. Даний випадок підтверджує, що кіберризики виходять за межі внутрішньої інформаційної інфраструктури підприємства та пов'язані з безпекою сторонніх сервісів і цифрових ланцюгів постачання. Після інциденту компанія посилила політику управління доступом, впровадила багатфакторну аутентифікацію та переглянула вимоги до кібербезпеки партнерів.

Проаналізувавши реальні приклади кібератак, ми прийшли до висновку, що масштабні витоки даних, компрометація облікових записів та порушення конфіденційності персональної інформації призводять не лише до фінансових втрат компаній, але також вони створюють довготривалі репутаційні ризики, які суттєво знижують рівень лояльності клієнтів до постраждалих компаній. Тому, як саме компанії можуть уберегтись від кібератак? У різних країнах світу з цією метою сформовано підходи щодо регулювання кібербезпеки, захисту персональної інформації та забезпечення прозорості використання даних, які спрямовані на підвищення рівня довіри споживачів до цифрових маркетингових систем.

Наприклад, в країнах Європейського Союзу розроблено «Загальний регламент про захист даних» [16], документ набув чинності у 2018 році та встановив єдині правила обробки персональної інформації для всіх компаній, які діють на території ЄС або взаємодіють з його громадянами. Регламент ґрунтується на низці таких фундаментальних принципів як: прозорість використання персональних даних; право користувачів на доступ до власної інформації; право на виправлення або видалення персональних даних; принцип мінімізації збору інформації.

Регламент впровадив сувору систему відповідальності за порушення вимог захисту даних – накладення штрафів за порушення принципів, які можуть досягати до 20 млн євро або 4 % від річного обороту компанії. Після практичного запуску цього нормативного акту велика кількість підприємств переглянули свої маркетингові стратегії, політики конфіденційності, процедури збору та обробки даних користувачів.

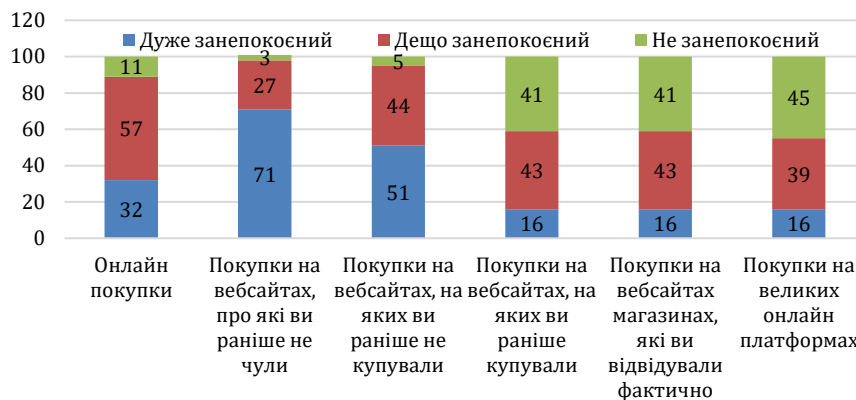


Рис. 1. Стурбованість споживачів щодо можливості витоку персональних даних під час здійснення онлайн-покупок. Джерело: складено за [10]

У США процес забезпечення довіри користувачів ґрунтується на залученні сертифікатів з кібербезпеки та стандартизації цифрових сервісів. У країні запровадили практику «значків довіри», які розміщуються на вебресурсах з електронної комерції та підтверджують відповідність платформ прийнятим стандартам безпеки. Наявність значка дає гарантію захищеності з'єднань, безпечності платіжних систем та надійних механізмів захисту персональних даних. Крім того, на території країни діє міжнародний стандарт безпеки даних індустрії платіжних карток [17], який визначає комплекс вимог до захисту даних платіжних карток під час здійснення електронних платежів. Впровадження цього стандарту дозволяє значно знизити ризики шахрайства, витоку фінансової інформації та несанкціонованого доступу до платіжних систем.

Дослідження [10] підтвердило, що наявність сертифікатів безпеки, захищених платіжних шлюзів та підтверджених механізмів верифікації транзакцій суттєво підвищує рівень довіри споживачів до інтернет-магазинів.

У країнах Азії також активно розвиваються інституційні механізми формування довіри до цифрових сервісів та онлайн-платформ. У Сінгапурі та Південній Кореї вже широко поширена «цифрова система довіри», яка передбачає комплексний підхід до управління цифровою довірою [18]. В азієцькій системі поєднується кібербезпека, захист персональних даних, етичне використання технологій штучного інтелекту та ефективне регулювання діяльності цифрових платформ. Для її підтримання уряди країн активно співпрацюють з приватним сектором, розробляють стандарти кіберзахисту та впроваджують механізми контролю за використанням даних.

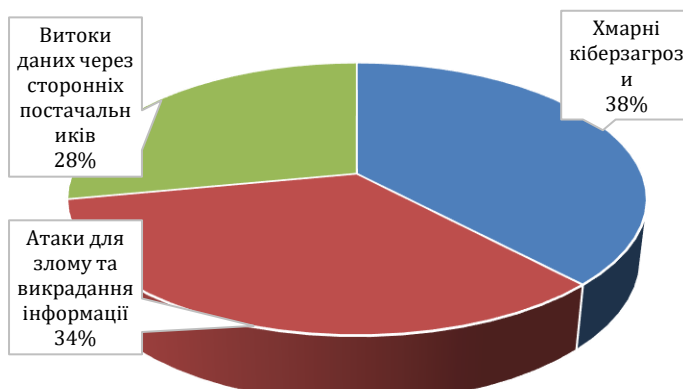


Рис. 2. Розподіл економічних втрат від витоку даних у цифровому середовищі. Джерело: складено за [11]

Проаналізувавши праці провідних учених, реальні випадки кібератак та досвід розвинутих країн щодо організації безпечного маркетингового середовища, ми прийшли до висновку, що забезпечення кібербезпеки має безпосередній вплив на такі ключові маркетингові показники:

- лояльність клієнтів – клієнти охочіше взаємодіють із брендами, які забезпечують захист персональних даних;
- конверсія продажів – відсутність довіри до безпеки сайту знижує ймовірність покупки;
- репутація бренду – витоки даних можуть призводити до довготривалих репутаційних втрат;
- конкурентоспроможність підприємства – компанії з високим рівнем цифрової довіри мають значно вищі показники утримання клієнтів.

Також в якості напрямів підвищення рівня довіри до цифрових маркетингових платформ ми пропонуємо такі:

- впровадження сучасних технологій кібербезпеки (багатофакторна аутентифікація, шифрування даних, системи моніторингу кіберзагроз);
- забезпечення прозорості обробки персональних даних (чітка політика конфіденційності, інформування користувачів про використання їх даних);
- сертифікація цифрових платформ (розробка стандартів безпеки, забезпечення відповідності міжнародним сертифікатам);
- підвищення кіберграмотності користувачів;
- інтеграція положень щодо кібербезпеки в маркетингову стратегію підприємства.

Тож, сформована таким чином система кібербезпеки буде ефективною та забезпечить стабільність взаємодії підприємств зі споживачами, підвищить лояльність клієнтів та сприятиме сталому розвитку бізнесу в умовах цифрової трансформації економіки.

Висновки та перспективи подальших розвідок

Таким чином, цифровізація економіки та активний розвиток електронної комерції суттєво трансформували механізми взаємодії підприємств та споживачів. Зростання обсягів збору та обробки персональної інформації користувачів обумовило появу нових ризиків, пов'язаних із кіберзагрозами, витоками даних та порушенням конфіденційності інформації. Аналіз джерел літератури показав, що кіберінциденти суттєво впливають на поведінку споживачів та репутацію компаній. Значна частка користувачів після витоку даних втрачає довіру до бренду, обмежує взаємодію з цифровими платформами або повністю відмовляється користуватись їх послугами. Крім того, кіберінциденти спричиняють великі грошові втрати, зокрема витрати на ліквідацію наслідків атак, компенсацію збитків клієнтам, відновлення інформаційної інфраструктури та подолання репутаційних ризиків.

Дослідження реальних фактів кібератак на цифрові платформи показало, що сучасні кіберризики пов'язані як і з внутрішніми інформаційними системами підприємств, так і з безпекою цифрових ланцюгів взаємодії з партнерами, підрядниками та постачальниками цифрових сервісів. Вивчення міжнародного досвіду забезпечення кібербезпеки показало, що ефективне забезпечення цифрової довіри ґрунтується на поєднанні інституційного регулювання, технологічних механізмів захисту інформації та прозорої політики управління персональними даними. В країнах Європейського Союзу переважає нормативне регулювання захисту персональної інформації через впровадження «Загального регламенту про захист даних», який встановлює чіткі правила обробки даних та високий рівень відповідальності компаній. В США формування довіри користувачів забезпечується через механізми сертифікації кібербезпеки, стандартизацію платіжних систем та використання спеціальних індикаторів безпеки на цифрових платформах. В азієцьких країнах активно розповсюджується концепція цифрової довіри, яка інтегрує кібербезпеку, захист персональних даних, етичне використання штучного інтелекту та державне регулювання цифрових сервісів.

На основі проведеного дослідження встановлено, що забезпечення кібербезпеки має безпосередній вплив на результуючі маркетингові показники діяльності підприємств: рівень лояльності клієнтів, конверсію продажів, репутацію бренду та загальну конкурентоспроможність компанії на цифрових ринках. З метою підвищення рівня довіри до цифрових маркетингових платформ доцільно впроваджувати сучасні технології кіберзахисту, забезпечувати прозорість використання персональних даних, здійснювати сертифікацію цифрових сервісів

відповідно до міжнародних стандартів, підвищувати рівень кіберграмотності користувачів та інтегрувати механізми інформаційної безпеки у стратегічні маркетингові програми підприємств. Реалізація зазначених заходів сформує безпечне цифрове маркетингове середовище та підвищить довіру споживачів.

Література

1. Борисенко О. Цифрові інструменти маркетингу в роздрібній торгівлі: шлях до ефективності та інновацій. *Економіка та суспільство*. 2025. Випуск 73. DOI: <https://doi.org/10.32782/2524-0072/2025-73-89>.
2. Седашова О., Годяцький А. Оптимізація та автоматизація процесів обробки замовлень у малому e-commerce бізнесі за допомогою it-рішень на основі lean-інструментів: кейс малого бізнесу. *Вчені записки Університету «КРОК»*. 2025. Випуск 4 (80). С. 218–224. DOI: <https://doi.org/10.31732/2663-2209-2025-80-218-224>.
3. Suryanegara E., Indradewa R., Anindita R., Alif M. Systematic analysis of trends and research methods in digital marketing: A scopus literature review 2024-2025. *Multidisciplinary Reviews*. 2026. Vol. 9. P. 2026386. DOI: <https://doi.org/10.31893/multirev.2026386>.
4. Bahaz S., Bedrouni A., Nouacer I. A Bibliometric Review: Artificial Intelligence in Digital Marketing in Scopus. *Economic Sciences, Management and Commercial Sciences*. 2025. Vol. 18. P. 386-406. URL: <https://asjp.cerist.dz/en/downArticle/324/18/2/286619>.
5. Adanyin A. Ethical AI in Retail: Consumer Privacy and Fairness. *European Journal of Computer Science and Information Technology*. 2024. Vol. 12. P. 21-35. DOI: <https://doi.org/10.37745/ejcsit.2013/vol12n72135>.
6. Sutherland T. Data breaches affect consumer trust. 2025. URL: <https://www.securitymagazine.com/articles/101357-data-breaches-affect-consumer-trust>.
7. Vercaara's 2024 Consumer Trust & Risk Report: Breaches Have Less Impact on Trust, but Consumers Remain Unaware of Insider Threats. *Business Wire*. 2024. URL: <https://martechedge.com/news/vercaras-2024-consumer-trust-risk-report-breaches-have-less-impact-on-trust-but-consumers-remain-unaware-of-insider-threats>.
8. 66% of consumers would not trust a company following a data breach. 2024. URL: <https://www.securitymagazine.com/articles/100296-66-of-consumers-would-not-trust-a-company-following-a-data-breach>.
9. Doerer K. How cyber incidents impact consumer trust. 2025. URL: <https://www.customerexperiencedive.com/news/how-cyber-incidents-impact-consumer-trust/736979>.
10. The state of ecommerce trust in 2024. 2024. URL: <https://www.trustedsite.com/resources/consumer-trust>.
11. Only 2% of businesses have implemented firm-wide cyber resilience, even as cyber security concerns are top-of-mind and the average data breach exceeds USD3m. PwC 2025 Global Digital Trust Insights. 2025. PwC. URL: <https://www.pwc.com/th/en/press-room/press-release/2024/press-release-08-11-24-en.html>.
12. Holthouse R., Owens S., Bhunia S. The 23andMe Data Breach: Analyzing Credential Stuffing Attacks, Security Vulnerabilities, and Mitigation Strategies. 2025. DOI: <https://doi.org/10.48550/arXiv.2502.04303>.
13. Murphy D. 16 billion password data breach hits Apple, Google, Facebook and more - LIVE updates and how to stay safe. Latest updates on one of the largest data breaches. *Tom's Guide*. 2025. URL: <https://www.tomsguide.com/news/live/16-billion-passwords-data-breach>.
14. The Economic Impact of Data Breaches in 2025. 2025. URL: <https://www.opencart.com/blog/the-economic-impact-of-data-breaches-in-2025>.
15. Hacking group claims it breached Ticketmaster and stole data for 560 million customers. *CBS News*. 2024. URL: <https://www.cbsnews.com/news/ticketmaster-breach-shinyhunters-560-million-customers/>.
16. General Data Protection Regulation (GDPR). 2018. URL: <https://gdpr-info.eu/>.
17. Payment Card Industry Data Security Standard. URL: <https://www.pcisecuritystandards.org/standards/>.
18. Bolima M. D. Digital Trust as the Cornerstone of Growth: How Asia-Pacific Enterprises Must Reimagine Cybersecurity in 2026. *Cyber Security Asia*. 2026. URL: <https://cybersecurityasia.net/digital-trust-as-the-cornerstone-of-growth/>

References

1. Borysenko, O. (2025). «Digital marketing tools in retail: the path to efficiency and innovation». *Ekonomika ta suspil'stvo*. Issue 73. DOI: <https://doi.org/10.32782/2524-0072/2025-73-89>.
2. Siedashova, O., Hodiats'kyj, A. (2025). «Optimization and automation of order processing processes in small e-commerce business using IT solutions based on lean tools: a case of small business». *Vcheni zapysky Universytetu «KROK»*. Issue 4 (80). pp. 218–224. DOI: <https://doi.org/10.31732/2663-2209-2025-80-218-224>.
3. Suryanegara, E., Indradewa, R., Anindita, R., Alif, M. (2026). «Systematic analysis of trends and research methods in digital marketing: A scopus literature review 2024-2025». *Multidisciplinary Reviews*. Vol. 9. pp. 2026386. DOI: <https://doi.org/10.31893/multirev.2026386>.
4. Bahaz, S., Bedrouni, A., Nouacer, I. (2025). «A Bibliometric Review: Artificial Intelligence in Digital Marketing in Scopus». *Economic Sciences, Management and Commercial Sciences*. Vol. 18. pp. 386-406. Available at: <https://asjp.cerist.dz/en/downArticle/324/18/2/286619>.
5. Adanyin, A. (2024). «Ethical AI in Retail: Consumer Privacy and Fairness». *European Journal of Computer Science and Information Technology*. Vol. 12. pp. 21-35. DOI: <https://doi.org/10.37745/ejcsit.2013/vol12n72135>.
6. Sutherland, T. (2025). Data breaches affect consumer trust. Available at: <https://www.securitymagazine.com/articles/101357-data-breaches-affect-consumer-trust>.
7. (2024). Vercaara's 2024 Consumer Trust & Risk Report: Breaches Have Less Impact on Trust, but Consumers Remain Unaware of Insider Threats. *Business Wire*. Available at: <https://martechedge.com/news/vercaras-2024-consumer-trust-risk-report-breaches-have-less-impact-on-trust-but-consumers-remain-unaware-of-insider-threats>.
8. (2024). 66% of consumers would not trust a company following a data breach. Available at: <https://www.securitymagazine.com/articles/100296-66-of-consumers-would-not-trust-a-company-following-a-data-breach>.
9. Doerer, K. (2025). How cyber incidents impact consumer trust. Available at: <https://www.customerexperiencedive.com/news/how-cyber-incidents-impact-consumer-trust/736979>.
10. (2024). The state of ecommerce trust in 2024. Available at: <https://www.trustedsite.com/resources/consumer-trust>.
11. (2025). Only 2% of businesses have implemented firm-wide cyber resilience, even as cyber security concerns are top-of-mind and the average data breach exceeds USD3m. PwC 2025 Global Digital Trust Insights. PwC. Available at: <https://www.pwc.com/th/en/press-room/press-release/2024/press-release-08-11-24-en.html>.
12. Holthouse, R., Owens, S., Bhunia, S. (2025). The 23andMe Data Breach: Analyzing Credential Stuffing Attacks, Security Vulnerabilities, and Mitigation Strategies. DOI: <https://doi.org/10.48550/arXiv.2502.04303>.
13. Murphy, D. (2025). 16 billion password data breach hits Apple, Google, Facebook and more - LIVE updates and how to stay safe. Latest updates on one of the largest data breaches. *Tom's Guide*. Available at: <https://www.tomsguide.com/news/live/16-billion-passwords-data-breach>.
14. The economic impact of data breaches in 2025. (2025). *OpenCart*. <https://www.opencart.com/blog/the-economic-impact-of-data-breaches-in-2025>.
15. Hacking group claims it breached Ticketmaster and stole data for 560 million customers. (2024, May 31). *CBS News*. <https://www.cbsnews.com/news/ticketmaster-breach-shinyhunters-560-million-customers/>
16. General Data Protection Regulation (GDPR). (2018). *GDPR.eu*. <https://gdpr-info.eu/>
17. Payment Card Industry Data Security Standard (PCI DSS). (n.d.). *PCI Security Standards Council*. <https://www.pcisecuritystandards.org/standards/>
18. Bolima, M. D. (2026). Digital trust as the cornerstone of growth: How Asia-Pacific enterprises must reimagine cybersecurity in 2026. *Cyber Security Asia*. <https://cybersecurityasia.net/digital-trust-as-the-cornerstone-of-growth/>

Стаття надійшла до редакції / Received 25.01.2026

Прийнята до друку / Accepted 15.02.2026

Опубліковано / Published 25.02.2026