



e-ISSN 3083-6018

СОЦІАЛЬНИЙ РОЗВИТОК: економіко-правові проблеми

<https://www.eu-scientists.com/index.php/sdel>


Вивчення споживчого сприйняття кібербезпеки та маркетингових стратегій на ринку послуг

 Марина В. Зав'ялова ^{1*} ● Сергій М. Іващенко ² ●

 Олександр Л. Лященко ²
¹ Державний університет економіки і технологій (Україна). Доцент кафедри управління бізнесом, канд. екон. наук, доцент.

² Херсонський національний технічний університет (Україна). Аспірант кафедри менеджменту, маркетингу і туризму.

 * Автор-кореспондент, e-mail: zavyalova_mv@kneu.dp.ua

СТАТТЯ

АНОТАЦІЯ

Дослідницька

DOI:

[10.70651/3083-6018/2025.4.29](https://doi.org/10.70651/3083-6018/2025.4.29)

Авторське право

© 2025 авторів



Цей твір
ліцензовано на
умовах Ліцензії
Creative Commons
«Із Зазначенням
Авторства –
Некомерційна 4.0
Міжнародна»
(CC BY-NC 4.0).



У сучасних умовах цифрової трансформації ринку послуг питання кібербезпеки набуває особливої ваги для споживачів. Зростання кількості цифрових сервісів і обсягу персональних даних, що обробляються онлайн, актуалізує потребу у формуванні довіри користувачів до безпечності цих рішень. Низька прозорість політик захисту інформації та нерозуміння механізмів цифрової безпеки з боку клієнтів знижують ефективність маркетингової взаємодії та уповільнюють прийняття цифрових інновацій. Проблема полягає в обмеженій інтеграції аспектів кібербезпеки в маркетингові стратегії компаній, які працюють у цифровому середовищі. Відсутність адаптованих комунікаційних підходів, що враховують обізнаність і очікування споживачів щодо захисту особистих даних, створює розрив між сервісною пропозицією та рівнем довіри клієнтів. Метою дослідження є вивчення того, як споживачі сприймають питання кібербезпеки в контексті отримання послуг, а також розробка маркетингових стратегій, що враховують ці очікування для підвищення ефективності комунікації та лояльності клієнтів. Об'єктом дослідження виступають поведінкові моделі споживачів цифрових послуг, а предметом – зв'язок між рівнем кібербезпеки сервісу та споживчим вибором, а також ефективна трансляція безпекових характеристик у маркетингу. У процесі дослідження використано аналіз вторинних даних: огляд наукових публікацій, звітів міжнародних агентств і кейсів провідних компаній сфери послуг. Проведено порівняльний аналіз стратегій комунікації кібербезпеки та вивчено підходи до формування довіри в цифровому середовищі. Особливу увагу приділено прозорості брендів щодо обробки персональних даних. У ході дослідження визначено типові моделі сприйняття цифрової безпеки, розроблено концепцію інтеграції безпекових повідомлень у бренд-комунікацію, а також сформульовано практичні рекомендації для прозорої взаємодії з клієнтами. Значну увагу приділено диференціації маркетингових підходів залежно від рівня цифрової грамотності. Результати підтверджують: довіра до кібербезпеки позитивно впливає на лояльність споживачів і повторне використання послуг. Компаніям рекомендовано включати безпекові меседжі в маркетингову стратегію, демонструвати заходи захисту даних та інвестувати в навчання персоналу. Це дозволить зміцнити бренд і підвищити конкурентоспроможність на ринку послуг.

КЛЮЧОВІ СЛОВА

маркетингова інформаційна система, кібербезпека, споживче сприйняття, маркетингові стратегії, цифрові послуги, довіра споживачів, інформаційна безпека, бренд-комунікація, туризм.



e-ISSN 3083-6018

SOCIAL DEVELOPMENT: Economic and Legal Issues

<https://www.eu-scientists.com/index.php/sdel>


Study of Consumer Perceptions of Cybersecurity and Marketing Strategies in the Services Market

Maryna Zavialova ^{1*} ● Sergii Ivashchenko ² ● Oleksandr Liashchenko ³

¹ State University of Economics and Technology (Ukraine). Associate Professor of the Department of Business Education, PhD in Economics, Associate Professor.

² Kherson National Technical University (Ukraine). Postgraduate Student at the Department of Management, Marketing and Tourism.

* Corresponding Author, e-mail: zavyalova_mv@kneu.dp.ua

ARTICLE INFO

ABSTRACT

Research Article

DOI:

[10.70651/3083-6018/2025.4.29](https://doi.org/10.70651/3083-6018/2025.4.29)

Copyright © 2025
by authors



This is an open access journal and all published articles are licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0)



In today's digital transformation of the services market, the issue of cybersecurity is gaining particular importance for consumers. The growth in the number of digital services and the volume of personal data processed online highlights the need to build user trust in the security of these solutions. Low transparency of information protection policies and lack of understanding of digital security mechanisms by customers reduce the effectiveness of marketing interaction and slow down the adoption of digital innovations. The problem lies in the limited integration of cybersecurity aspects into the marketing strategies of companies operating in the digital environment. The lack of adapted communication approaches that take into account consumers' awareness and expectations regarding the protection of personal data creates a gap between the service offering and the level of customer trust. The purpose of the study is to study how consumers perceive cybersecurity issues in the context of receiving services, as well as to develop marketing strategies that take into account these expectations to increase the effectiveness of communication and customer loyalty. The object of the study is the behavioral models of consumers of digital services, and the subject is the relationship between the level of cybersecurity of the service and consumer choice, as well as the effective translation of security characteristics in marketing. The study used secondary data analysis: a review of scientific publications, reports of international agencies and cases of leading service companies. A comparative analysis of cybersecurity communication strategies was conducted and approaches to building trust in the digital environment were studied. Particular attention was paid to brand transparency regarding the processing of personal data. The study identified typical models of perception of digital security, developed a concept for integrating security messages into brand communication, and formulated practical recommendations for transparent interaction with customers. Considerable attention was paid to the differentiation of marketing approaches depending on the level of digital literacy. The results confirm that trust in cybersecurity has a positive effect on consumer loyalty and repeated use of services. Companies are advised to incorporate security messages into their marketing strategy, demonstrate data protection measures, and invest in staff training. This will strengthen the brand and increase competitiveness in the services market.

KEYWORDS

marketing information system, cybersecurity, consumer perception, marketing strategies, digital services, consumer trust, information security, brand communication, tourism.

1. Вступ

Швидке проникнення цифрових технологій у повсякденне життя зумовило радикальні зміни у способах надання та споживання послуг. Від банківських операцій до телемедицини, від онлайн-консультування до систем бронювання – практично кожна галузь сьогодні формує свою присутність у цифровому середовищі. Водночас із зростанням кількості сервісів зростає й обсяг персональних даних, які передаються, зберігаються та обробляються онлайн. У цьому контексті кібербезпека перестає бути суто технічним аспектом – вона набуває значення як чинник формування споживчої довіри, визначаючи конкурентоспроможність сервісу на ринку.

Тривалий час цифрова безпека залишалась у «тіні» маркетингових стратегій: її сприймали як внутрішню складову технічної інфраструктури, а не як інструмент зовнішньої комунікації з клієнтом. Проте останні роки демонструють зсув у споживчих очікуваннях – люди дедалі частіше надають перевагу тим брендам, які не лише гарантують захист даних, але й відкрито комунікують про це. Довіра, яка формується в умовах інформаційної прозорості та впевненості у безпеці, стає вирішальним чинником у прийнятті рішення про взаємодію з сервісом.

Особливої актуальності зазначена тематика набуває в умовах зростання кількості кіберзагроз, витоків персональних даних та поширення цифрового шахрайства. Підвищення суспільної чутливості до питань інформаційної безпеки зумовлює необхідність для бізнесу адаптувати свої комунікаційні стратегії, інтегруючи тематику захисту даних у загальну бренд-стратегію. Такий підхід вимагає одночасного дотримання балансу між технічною достовірністю повідомлень та збереженням доступності, зрозумілості й привабливості маркетингових меседжів для цільової аудиторії.

Дане дослідження покликане осмислити сучасні тенденції у сприйнятті кібербезпеки як маркетингової цінності, проаналізувати існуючі практики комунікації з боку провайдерів послуг, а також запропонувати підходи до побудови ефективної стратегії, що поєднує технологічний захист із емоційним зв'язком зі споживачем.

2. Огляд літературних джерел

Аналіз сучасних наукових джерел підтверджує актуальність проблеми кібербезпеки в контексті цифрової трансформації ринку послуг. У дослідженні Cele та Kwenda [1] зроблено висновок про стримувальний вплив кіберзагроз на впровадження цифрового банкінгу, що підтверджує значущість безпеки в споживчому виборі. Вітчизняні автори, зокрема Чміль [2], Білоус, Супрун і Перепелиця [3], а також Вовк, Гаврильченко й Черкаський [4], розглядають ризики цифровізації в економіці та маркетингу, підкреслюючи необхідність інтеграції безпекових підходів у бізнес-практики.

Окрему увагу дослідники приділяють змінам у маркетингових стратегіях. Так, Струк і Сосновська [5] акцентують на необхідності адаптації брендової комунікації до умов цифрового середовища. Із погляду організаційної безпеки, Asbaş і Tuzlukaya [6] аналізують стратегії кіберзахисту для бізнесу, тоді як Thomas і Sule [7] – механізми підтримки кібербезпеки як умову стабільного розвитку компаній. У роботі Jazairi та ін. [8] запропоновано концепцію кіберстійкості в ланцюгах постачання як частину корпоративної безпеки.

Поведінковий аспект цифрового споживання розкрито у дослідженні Лазебника [9], де аналізується роль безпеки в контексті взаємодії з мерчендайзингом. Райко, Дрепін і Масалаб [10] досліджують трансформацію традиційного маркетингу під впливом цифрової економіки, а Florido-Benítez [11] вказує на зростаючу вагу мобільного маркетингу, довіри та безпеки у взаємодії з користувачами в умовах пандемії.

Таким чином, усі проаналізовані джерела підкреслюють комплексний характер взаємозв'язку між цифровою безпекою, маркетингом та поведінкою споживачів, що створює наукове підґрунтя для подальшого дослідження цієї теми в межах обраної проблематики.

3. Постановка завдання

Питання кібербезпеки поступово перетворюється з технічного аспекту на вагомий соціально-поведінковий чинник, що формує довіру до цифрових сервісів. У той час як компанії інвестують у внутрішню інфраструктуру захисту, значна частина з них досі не приділяє уваги комунікації цих зусиль споживачам. Це призводить до розриву між фактичними заходами безпеки та уявленнями про них серед користувачів.

Особливу складність становить робота з молодіжною аудиторією, яка демонструє вищу чутливість до питань цифрової безпеки, але водночас часто стає жертвою шахрайства. В умовах інформаційного перевантаження маркетингові меседжі щодо безпеки або залишаються непоміченими, або не сприймаються як релевантні.

Дослідження покликане проаналізувати, як саме споживачі реагують на тематику кібербезпеки у публічній комунікації брендів, та які підходи можуть стати ефективними для формування довіри в цифровому середовищі. У фокусі – розробка рекомендацій щодо адаптації маркетингових стратегій із урахуванням безпекових аспектів і споживчих очікувань у різних вікових та поведінкових сегментах.

4. Методи та матеріали

У процесі дослідження було використано комплексний підхід до збору та аналізу інформації з метою вивчення споживчого сприйняття кібербезпеки та визначення ефективних маркетингових стратегій у сфері послуг. Методологічну основу становить аналіз вторинних даних, зокрема наукових публікацій, статистичних звітів міжнародних організацій, матеріалів дослідницьких агентств, кейсів компаній, а також публічних комунікацій брендів у цифровому середовищі.

Контент-аналіз маркетингових повідомлень був проведений з метою виявлення частоти та характеру згадок про кібербезпеку у відкритих каналах комунікації (офіційні сайти, соціальні мережі, презентації продуктів тощо). Окремо було здійснено порівняльний аналіз стратегій компаній із різних галузей (банківська справа, телекомунікації, медичні послуги, туристичні послуги), що дозволило простежити специфіку сприйняття безпеки в різних сферах.

Також застосовано елементи якісного аналізу – інтерпретація споживчих очікувань і моделей довіри, сформованих унаслідок взаємодії з цифровими сервісами, на основі існуючих соціологічних досліджень і емпіричних даних. Відбір матеріалів ґрунтувався на принципах релевантності, репрезентативності та актуальності в контексті заявленої проблематики.

Такий підхід дозволив забезпечити багатовимірне бачення досліджуваної теми, виявити ключові тенденції в оцінці цифрової безпеки та сформулювати практичні рекомендації щодо інтеграції кібербезпекових меседжів у маркетингову комунікацію компаній сфери послуг.

5. Результати та обговорення

У науковій літературі кібербезпека розглядається не лише як технологічний інструмент забезпечення конфіденційності, цілісності та доступності даних, але й як соціально-поведінковий феномен, що впливає на рівень довіри споживачів до цифрових продуктів і сервісів. Згідно з концепцією «персоніфікованої безпеки», сформованою на перетині інформаційних технологій та поведінкової економіки, споживачі оцінюють ступінь захищеності не лише за об'єктивними параметрами, але й на основі емоційного сприйняття, прозорості комунікації та попереднього досвіду.

Сучасні підходи до вивчення кібербезпеки у споживчому контексті спираються на інтеграцію знань з психології довіри, цифрового маркетингу та управління ризиками. Дослідники звертають увагу на феномен «усвідомленої безпеки», коли користувачі приймають рішення не тільки на основі технічних характеристик захисту, але й у відповідь на рівень поінформованості, способи подачі інформації про ризики, механізми управління доступом до даних [1].

Зростання ролі кібербезпеки у формуванні споживчої поведінки особливо яскраво проявляється в умовах частих витоків даних, скандалів, пов'язаних із приватністю, та

загострення глобального інформаційного клімату. Теоретичні моделі, такі як Technology Acceptance Model (ТАМ) і Trust-Based Acceptance Model (ТВАМ), адаптовані до цифрового середовища, вказують на вирішальну роль довіри у процесах прийняття рішень споживачами.

Особливий інтерес викликають роботи, що аналізують реакції користувачів на різні форми комунікації безпеки – від текстових описів політик конфіденційності до візуалізованих індикаторів захисту, сертифікатів та відгуків інших користувачів. Згідно з сучасними емпіричними дослідженнями, підвищена відкритість у питаннях безпеки, пояснення прав споживача та простота доступу до інструментів керування персональними даними значно підвищують рівень лояльності до бренду [2].

Отже, сучасна теоретична база підкреслює взаємозалежність між ефективною системою кібербезпеки, прозорою комунікацією з користувачем та споживчим вибором. Це створює підґрунтя для подальшого дослідження ролі безпеки у маркетингових стратегіях та потребує адаптації існуючих моделей взаємодії з клієнтом до умов інформаційної економіки.

У контексті активної цифровізації послуг споживачі дедалі більше усвідомлюють необхідність захисту власних персональних даних. Однак уявлення про ризики й очікування щодо безпеки залишаються різномірними, фрагментарними і залежать як від рівня цифрової грамотності, так і від попереднього досвіду взаємодії з цифровими платформами. Розуміння цих чинників дозволяє краще адаптувати маркетингову комунікацію і зменшити ймовірність втрати довіри до бренду (табл. 1).

Таблиця 1. Ключові ризики та очікування споживачів у сфері цифрової безпеки

Категорія	Типові ризики	Очікування споживачів
Конфіденційність персональних даних	- Несанкціонований доступ до персональної інформації; - Витік чутливих даних через злами, людський фактор або погану політику збереження.	- Гарантований захист персональних даних; - Використання шифрування, надійних серверів, регулярне оновлення систем безпеки; - Впевненість, що їхня інформація не буде передана третім особам без згоди.
Контроль користувача над даними	- Обмежені можливості користувача у керуванні даними (наприклад, неможливість видалити акаунт або змінити налаштування приватності); - Приховані дозволи при встановленні додатків.	- Повний доступ до інструментів керування конфіденційністю; - Прозорі налаштування доступу, повідомлення про зміни; - Легкий вихід із сервісу та видалення особистих даних.
Цифрове шахрайство та зловживання	- Використання фішингових посилань, підроблених інтерфейсів для збору банківських даних; - Підміна цифрових транзакцій або зараження пристроїв вірусами.	- Інформаційна підтримка користувачів щодо шахрайських схем; - Багатофакторна аутентифікація, постійний моніторинг підозрілої активності; - Наявність служби підтримки для оперативного реагування.
Використання даних у маркетингових цілях	- Збір даних без згоди або з надмірним втручанням у приватність; - Агресивна реклама на основі поведінкових даних без інформування.	- Чітке повідомлення про мету збору даних; - Вибірковість згоди користувача на ті чи інші види обробки; - Відмова від нав'язливих реклам без покарання функціональності сервісу.
Комунікація бренду щодо безпеки	- Відсутність публічної позиції щодо кібербезпеки; - Реакція компанії лише після інцидентів, а не превентивна комунікація.	- Постійна, чітка й чесна комунікація безпеки через доступні канали (сайт, застосунок, e-mail); - Публікація політик безпеки у зрозумілій формі; - Прозорість у випадках інцидентів із поясненням дій компанії.
Репутаційна надійність компанії	- Втрата довіри після скандалів, витоків даних або приховування інформації; - Повторення інцидентів без вжиття ефективних заходів.	- Публічне визнання відповідальності у випадку проблем; - Демонстрація реальних змін у політиці після інциденту; - Підкріплення безпеки сертифікацією та зовнішнім аудитом.

Джерело: систематизовано авторами за даними, наведеними у [3–4].

Як демонструє табл. 1, споживачі в цифровому середовищі більше не сприймають безпеку як "бонусну опцію", а вважають її базовою умовою для використання сервісу. Для компаній це означає необхідність не лише технічного вдосконалення, але й роботи над інформаційною відкритістю, формуванням довіри через зрозумілу й послідовну комунікацію. Особливу роль відіграє персоналізація повідомлень, а також вміння адаптувати рівень деталізації до різних груп користувачів.

У сучасному інформаційно насиченому середовищі кібербезпека стає не лише технічним стандартом, а й важливим елементом маркетингової комунікації. Компанії, які надають цифрові послуги, усе частіше інтегрують тематику безпеки у свої комунікаційні стратегії, формуючи довіру та емоційний зв'язок із клієнтами. Цей підхід вимагає від брендів гнучкості, прозорості та здатності говорити про складне просто, зрозуміло й переконливо. На рис. 1 наведено ключові практики, які успішно реалізуються на міжнародному рівні.

1. Контент-маркетинг та освітні ініціативи

- Провідні компанії публікують аналітичні звіти, блоги, гайди та відео, які пояснюють складні аспекти кібербезпеки у доступній формі. Освітні матеріали часто адресовані як широкій аудиторії, так і спеціалізованим сегментам користувачів (бізнес, IT-фахівці, підлітки тощо). Наприклад, Palo Alto Networks активно створює навчальний контент, що підтримує імідж компанії як галузевого лідера та надійного консультанта з безпеки.

2. Інтерактивні інструменти та візуалізація даних

- Використання інфографік, карт кіберзагроз у реальному часі, персоналізованих звітів із порадами для користувачів. Такі візуальні формати дозволяють швидко донести складну інформацію, підвищуючи її засвоєння. Наприклад, IBM Security інтегрує інтерактивні аналітичні панелі у свої публічні ресурси. Компанія Amra and Elma LLC використовує адаптивну візуалізацію ризиків, щоб покращити довіру до клієнтських сервісів.

3. Соціальні кампанії та стратегічні партнерства

- Кампанії з підвищення обізнаності у Facebook, LinkedIn, YouTube, зокрема під час Місяця кібербезпеки. Використання брендових хештегів, флешмобів, онлайн-челенджів. Залучення інфлюенсерів і експертів дозволяє переосмислити тему кібербезпеки через соціальний діалог. Cisco показує приклад ефективного поєднання соціального контенту й корпоративної відповідальності.

4. Подкасти, вебінари та живі трансляції

- Формат живого спілкування дає змогу залучити аудиторію до відкритих дискусій. McAfee реалізувала серію подкастів із практичними порадами, запрошеними експертами та історіями з життя. Вебінари компаній дозволяють не лише просвітити, а й створити спільноту довкола теми цифрової безпеки.

5. Прозорість, відкритість і репутаційна відповідальність

- Компанії, що пережили кризи, зокрема SolarWinds, демонструють важливість відкритої реакції на інциденти. Вони публікують докладні звіти, аналіз причин, список дій у відповідь. Впровадження прозорої політики, відкритість до аудиту та сертифікації зміцнюють довіру до бренду в довгостроковій перспективі.

6. Інтеграція кібербезпеки у стратегії туристичних компаній

- У туристичній індустрії питання кібербезпеки набуває особливої ваги, оскільки компанії працюють із великими обсягами персональних і платіжних даних клієнтів. Провідні гравці ринку, такі як Booking.com, Expedia Group та авіакомпанії на зразок Emirates і Lufthansa, інтегрують комунікацію про захист даних у свої маркетингові стратегії, наголошуючи на безпеці онлайн-бронювання, верифікації транзакцій і відповідності міжнародним стандартам (наприклад, PCI DSS). Важливу роль відіграють прозорість політик конфіденційності, регулярне інформування споживачів про оновлення систем кіберзахисту та проведення освітніх кампаній щодо безпечної взаємодії з сервісами. Такі практики суттєво зміцнюють довіру до бренду і створюють конкурентну перевагу в умовах розвитку цифрового туризму.

Рис. 1. Маркетингові стратегії комунікації кібербезпеки: практики провідних компаній

Джерело: систематизовано авторами за даними, наведеними у [5–6].

Аналіз практик провідних компаній свідчить, що ефективна комунікація безпеки базується на поєднанні технологічної достовірності та соціальної відповідальності. Компанії, які не лише захищають дані, а й відкрито говорять про це мовою, зрозумілою користувачам,

отримують стійку конкурентну перевагу. Впровадження мультимедійного контенту, прозорих політик та живого діалогу з аудиторією дозволяє брендам зміцнити довіру в умовах цифрової невизначеності.

У науковій та прикладній літературі дедалі частіше акцентується увага на гетерогенності споживачів у контексті сприйняття інформаційної безпеки. Вікові, освітні, соціокультурні та поведінкові характеристики впливають не лише на рівень усвідомлення цифрових ризиків, а й на спосіб реагування на маркетингову комунікацію, що стосується кібербезпеки. Таким чином, ефективність стратегії бренду в значній мірі залежить від здатності сегментувати аудиторію за релевантними критеріями й адаптувати інформаційні меседжі відповідно до цих відмінностей.

Особи віком від 18 до 29 років становлять одну з найактивніших груп користувачів цифрових технологій. Вони легко адаптуються до нових сервісів, швидко опановують функціонал додатків і загалом мають високий рівень технічної обізнаності. Однак у питаннях інформаційної безпеки саме ця категорія користувачів нерідко виявляє легковажність. Як показують спостереження, молоді споживачі не завжди приділяють достатньо уваги перевірці джерел, умовам зберігання й обробки даних, а також налаштуванням конфіденційності. Така поведінка часто пов'язана з надмірною довірою до інтерфейсу сервісу або бренду, а також із недооцінкою ризиків. Водночас молодь є найбільш відкритою до прозорості та чесної комунікації з боку компаній: вона позитивно реагує на чітке інформування про механізми захисту даних, цінує можливість самостійного контролю над інформацією та готова взаємодіяти з освітніми ініціативами, що підвищують рівень обізнаності в питаннях цифрової безпеки [9].

Середній віковий сегмент (30–50 років), як правило, виявляє вищу обережність і критичність щодо цифрової безпеки. Ця група частіше перевіряє джерела інформації, оцінює сертифікати захисту, шукає огляди інших користувачів. Для них важливі репутація компанії, наявність юридичних гарантій захисту даних, участь у програмах сертифікації ISO та інших стандартах. Саме серед цього сегменту високий рівень очікувань щодо деталізації умов обробки інформації, а також щодо можливостей самостійного контролю над нею.

Старша вікова категорія (50+) демонструє суперечливі тенденції: з одного боку – зростання зацікавлення цифровими сервісами, з іншого – глибоку настороженість щодо інформаційної безпеки. Для цієї групи характерним є побоювання втрати контролю над персональними даними, що може бути пов'язано з недостатнім рівнем цифрової освіти та попереднім негативним досвідом. Комунікація для цього сегмента має бути гранично прозорою, з акцентом на підтримку, пояснення простими словами, прикладами з реального життя та можливістю безпосереднього контакту з представниками сервісу [10].

Окрему увагу слід приділити рівню цифрової грамотності, який не завжди співвідноситься з віком. У рамках цієї характеристики варто виокремити три умовні групи: базово орієнтовані користувачі, середньо обізнані та цифрові «просунуті» споживачі. Перша група орієнтується здебільшого на емоційне враження, інтерфейс, поради знайомих. Друга група вже користується антивірусними програмами, захищеними підключеннями, але часто діє інтуїтивно. Третя – уважно читає політики, користується VPN, шифруванням, змінює паролі й аналізує активність сервісів [11].

Таким чином, специфіка сприйняття безпеки є багатофакторною і не може зводитись до одного критерію. Вона визначається комбінацією віку, освіти, поведінкових установок, попереднього досвіду та соціального контексту. Відповідно, маркетингова стратегія має враховувати цю складність – через гнучке сегментування аудиторії, адаптацію формату повідомлень, тональності комунікації та способів візуалізації безпекової інформації.

У сучасному цифровому середовищі, де довіра користувача дедалі більше залежить від безпеки його даних, інтеграція теми кібербезпеки у маркетингову та бренд-стратегію компанії перестає бути опціональним елементом – вона стає необхідною умовою сталого функціонування. Споживачі очікують від брендів не лише якісного продукту, а й відповідального ставлення до обробки та захисту інформації. Це особливо актуально для компаній туристичної галузі, де обробляються великі обсяги персональних і платіжних даних клієнтів під час бронювання та подорожей. Відповідно, виникає потреба у системному перегляді підходів до комунікації, побудованої не лише на емоціях, а й на прозорості, обґрунтованості та цінностях безпеки.

Насамперед компаніям рекомендовано включити тему безпеки в основну концепцію бренду – не як додаткову опцію, а як частину корпоративної ідентичності. Такий підхід дозволяє підвищити довіру клієнтів ще на етапі першого контакту з продуктом або сервісом. Для туристичних компаній це може означати активне інформування про безпечні канали оплати, політики обробки даних під час бронювання турів та авіаквитків, а також впровадження міжнародних стандартів захисту інформації. Чітка та послідовна комунікація через сайти, мобільні застосунки, соціальні мережі створює відчуття стабільності, зрілості й відповідальності бренду [7].

Оскільки споживачі значно відрізняються за віком, рівнем цифрової грамотності та поведінковими моделями, надзвичайно важливим є адаптація інформації для різних цільових груп. Технічно орієнтовані користувачі очікують чітких і конкретних даних про політику конфіденційності, інструменти шифрування, сертифікати. Менш досвідчені – реагують краще на просту візуалізацію, приклади, покрокові інструкції. Відтак ефективна стратегія передбачає сегментовану подачу змісту з урахуванням інформаційного фону споживача.

Важливою складовою бренд-комунікації стає освітній контент. Він допомагає не лише інформувати, а й формувати поведінкову культуру, що підвищує загальний рівень цифрової зрілості споживачів. Це можуть бути відео, блоги, посібники, короткі поради – усе, що сприяє розумінню загроз і способів захисту. Освітня комунікація особливо ефективна серед молодшої аудиторії, яка швидко сприймає візуальну інформацію та цінує відкритість бренду [8].

Окремо слід наголосити на важливості регулярної комунікації та швидкої реакції у разі кризових ситуацій. Туристичні компанії, які оперативно інформують клієнтів про можливі інциденти та шляхи їх вирішення, зберігають довіру аудиторії навіть у складних обставинах. Визнання відповідальності, чіткий план дій та доступ до підтримки формують імідж прозорого та сильного бренду.

Усі ці підходи доцільно доповнювати використанням міжнародних стандартів (наприклад, ISO/IEC 27001), публічними аудитами та візуальними елементами підтвердження безпеки в інтерфейсі. Таким чином, кібербезпека стає не лише частиною технічної інфраструктури, а й важливим комунікативним активом, що визначає позиціонування компанії на ринку.

6. Висновки

У результаті проведеного дослідження встановлено, що питання кібербезпеки дедалі більше впливають на споживчу поведінку в цифровому середовищі, формуючи рівень довіри, лояльності та готовності до взаємодії з брендом. Незважаючи на зростання технічної захищеності цифрових сервісів, саме споживче сприйняття безпеки залишається визначальним фактором для прийняття рішень про користування тими чи іншими послугами.

Проаналізовані наукові підходи та маркетингові практики показують, що ефективна комунікація з питань кібербезпеки має бути багатоформатною, адаптивною та соціально відповідальною. Врахування вікових, поведінкових і освітніх відмінностей між цільовими групами дозволяє забезпечити релевантність повідомлень і підвищити рівень розуміння з боку користувачів.

Запропоновані рекомендації спрямовані на інтеграцію кібербезпеки у бренд-стратегію як ключового елементу, що поєднує технічну надійність із прозорістю, зрозумілою для споживача комунікацією. Акцент на освітній контент, регулярне інформування, відкриту реакцію на кризові ситуації та візуалізацію безпекових індикаторів здатен зміцнити ринкові позиції компаній і сформувати довгострокову довіру до бренду.

Таким чином, кібербезпека в сучасному маркетинговому контексті є не лише технологічною необхідністю, а й стратегічною цінністю, яка визначає ефективність комунікації, конкурентоспроможність і соціальну стійкість бізнесу.

References

1. Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, 32(1), 31–48. <https://doi.org/10.1108/JFC-10-2023-0263>

2. Chmil, H. L. Tsyfrovisatsiia diialnosti subiektiv spozhyvchoho rynku: mozhlyvosti ta zahrozy [Digitalization of consumer market entities activity: Opportunities and threats]. *The Journal of V. N. Karazin Kharkiv National University. Series: International Relations. Economics. Country Studies. Tourism*, (13), 124-134. <https://doi.org/10.26565/2310-9513-2021-13-13> (in Ukrainian)
3. Bilous, S., Suprun, D., & Perepelytsia, Ye. (2024). Intehratsiia tsyfrovykh tekhnolohii u marketynhovi protsesy: vyklyky ta perspektyvy [Integration of digital technologies into marketing processes: Challenges and prospects]. *Ekonomichnyi prostir – Economic Space*, (195), 154–158. <https://doi.org/10.30838/EP.195.154-158> (in Ukrainian)
4. Vovk, V., Havrylchenko, O., & Cherkaskyi, O. (2025). Vplyv didzhitalizatsii na formuvannia marketynhovykh stratehii pidpriemstv: vykorystannia digital-instrumentiv [The impact of digitalization on the formation of marketing strategies of enterprises: The use of digital tools]. *Ekonomika ta suspilstvo – Economy and Society*, (72). <https://doi.org/10.32782/2524-0072/2025-72-1> (in Ukrainian)
5. Struk, N. R., & Sosnovska, O. O. (2025). Marketynhovi stratehii torhovelnoho pidpriemnytstva u sferi rozdribnoi torhivli [Marketing strategies of retail business]. *Aktualni pytannia ekonomichnykh nauk – Current Issues in Economics*, (7). <https://doi.org/10.5281/zenodo.14743680> (in Ukrainian)
6. Asbaş, C., & Tuzlukaya, Ş. (2022). Cyberattack and cyberwarfare strategies for businesses. In F. Özsungur (Ed.), *Conflict management in digital business* (pp. 303–328). Emerald Publishing Limited. <https://doi.org/10.1108/978-1-80262-773-220221027>
7. Thomas, G., & Sule, M.-J. (2023). A service lens on cybersecurity continuity and management for organizations' subsistence and growth. *Organizational Cybersecurity Journal: Practice, Process and People*, 3(1), 18–40. <https://doi.org/10.1108/OJ-09-2021-0025>
8. Jazairy, A., Brho, M., Manuj, I., & Goldsby, T. J. (2024). Cyber risk management strategies and integration: Toward supply chain cyber resilience and robustness. *International Journal of Physical Distribution & Logistics Management*, 54(11), 1–29. <https://doi.org/10.1108/IJPDLM-12-2023-0445>
9. Lazebnyk, V. (2024). Povedinka spozhyvachiv yak komponent tekhnolohii merchendaizynhu [Consumer behavior as a component of merchandising technology]. *Ekonomika ta suspilstvo – Economy and Society*, (70). <https://doi.org/10.32782/2524-0072/2024-70-26> (in Ukrainian)
10. Raiko, D., Drepin, I., & Masalab, O. (2024). Adaptatsiia ta optymizatsiia tradytsiinykh marketynhovykh stratehii do vymoh tsyfrovoi ekonomiky: vyklyky ta mozhlyvosti [Adaptation and optimization of traditional marketing strategies to the requirements of the digital economy: Challenges and opportunities]. *Herald of Khmelnytskyi National University. Economic Sciences*, 328(2), 18–23. <https://doi.org/10.31891/2307-5740-2024-328-2> (in Ukrainian)
11. Florido-Benítez, L. (2022). International mobile marketing: A satisfactory concept for companies and users in times of pandemic. *Benchmarking: An International Journal*, 29(6), 1826–1856. <https://doi.org/10.1108/BIJ-06-2021-0303>