DOI: https://doi.org/10.32782/2524-0072/2024-70-55

УДК 658.8:004.056

МАРКЕТИНГ В УМОВАХ ЦИФРОВОГО ШАНТАЖУ

MARKETING IN THE CONTEXT OF DIGITAL BLACKMAILING

Тарасова Кристина Ігорівна
кандидат економічних наук, доцент,
Одеський національний економічний університет
ORCID: https://orcid.org/0000-0002-9072-0591

Сало Яна Вікторівна
кандидат економічних наук, доцент,
Одеський національний економічний університет
ORCID: https://orcid.org/0000-0003-1066-783X

Новак Ганна В'ячеславівна
викладач,
Одеський національний економічний університет
ORCID: https://orcid.org/0000-0002-9384-3204

Tarasova Krystyna, Salo Yana, Novak Hanna
Odesa National Economic University

Стаття присвячена аналізу впливу кіберзагроз на цифровий маркетинг у сучасному бізнес-середовищі. Розглянуто ключові аспекти цифрового шантажу, включаючи атаки програм-вимагачів, витоки даних та маніпуляції інформацією, які стають викликом для забезпечення репутації брендів. Особливу увагу приділено ролі соціальних мереж у поширенні дезінформації та наслідкам таких атак для маркетингових стратегій. Висвітлено значення інтеграції кібербезпеки у маркетингову діяльність через впровадження технологій захисту, шифрування даних, багатофакторної аутентифікації та кризового управління. Зроблено висновок, що кіберзагрози вимагають нових підходів до управління ризиками та побудови стійких комунікаційних систем, які дозволяють бізнесу зберігати конкурентоспроможність і адаптуватися до швидкої еволюції цифрового середовища.

Ключові слова: цифровий маркетинг, кіберзагрози, цифровий шантаж, репутація бренду, кібербезпека.

The article explores the impact of cybersecurity threats on digital marketing in the contemporary business environment. It examines the theoretical and practical implications of cyber extortion, including ransomware attacks, doxing, data breaches, and misinformation campaigns, which pose significant challenges to brand reputation and consumer trust. The study highlights the increasing vulnerability of digital marketing strategies to evolving cyber threats, particularly those relying on social media, big data, and automated systems. Special emphasis is placed on the role of social media platforms as both key tools for marketing and primary targets for cybercriminals. The study examines the ramifications of fake reviews, spam attacks, and data leaks, emphasizing how these factors can disrupt marketing campaigns and erode customer confidence. The research further discusses the rising prevalence of AI-driven disinformation campaigns and their potential to manipulate public opinion, causing businesses reputational damage and financial losses. The article underscores the necessity of integrating robust cybersecurity measures into marketing strategies. It advocates for implementing advanced data encryption, multi-factor authentication, and regular system updates as essential tools for mitigating risks. The study also explores the importance of proactive reputation management and crisis response frameworks, focusing on transparency and effective communication to rebuild trust following cybersecurity incidents. Additionally, the research identifies the critical need for businesses to adapt their marketing strategies in response to shifting consumer behaviours and increased demands for data privacy. It highlights the role of personalized communication, ethical practices, and the adoption of resilient digital tools to navigate the dual challenges of leveraging digital marketing opportunities while safeguarding against cyber threats. The findings reveal that the synergy between marketing and cybersecurity is vital for sustaining competitive advantage in the digital era. By fostering a culture of security awareness, investing in advanced technological solutions, and prioritizing consumer trust, businesses can effectively address cybersecurity risks while optimizing their marketing efforts. The study concludes that integrating cybersecurity into marketing strategies is not merely a technical necessity but a strategic imperative, ensuring resilience and long-term growth in a rapidly evolving digital landscape.

Keywords: digital marketing, cyber threats, digital blackmail, brand reputation, cybersecurity.

Постановка проблеми. Цифровий маркетинг став невід'ємною частиною сучасного бізнес-середовища, відкриваючи перед компаніями нові можливості для досягнення аудиторії за допомогою соціальних мереж, пошукової оптимізації, контент-маркетингу та інших інструментів. Завдяки швидкому розвитку технологій, компанії отримують унікальні переваги: персоналізовані комунікації, глобальний доступ до клієнтів та оперативне коригування кампаній у реальному часі. Однак цей прогрес супроводжується й суттєвими ризиками.

Однією з найбільших загроз для цифрового маркетингу є зростання кіберзлочинності, зокрема цифрового шантажу. Цей феномен включає в себе як атаки програм-вимагачів, так і більш складні форми, такі як злом корпоративних ресурсів або загрози публікації конфіденційної інформації. У багатьох випадках підприємства стикаються з ситуаціями, коли вони змушені платити за «вирішення» створених хакерами проблем, навіть якщо немає гарантій повного відновлення доступу до вкрадених даних чи уникнення повторних атак.

Ще одним аспектом цифрового шантажу є доксинг – розкриття персональних або корпоративних даних для публічного приниження або маніпуляції. Це може викликати як миттєві ризики для репутації та безпеки, так і довгострокову тривожність щодо потенційного витоку інформації господарюючого суб'єкта.

Кіберзлочинці знаходять нові способи впливати на бізнес, використовуючи не лише викрадення даних, але й злом обладнання, маніпуляції виробничими процесами та навіть загрози блокування діяльності через атаки типу DDoS. Злочинці, як правило, спрямовують свої зусилля на фінансові вигоди, змушуючи компанії сплачувати викупи в криптовалюті або іншими способами.

Незважаючи на складність правового врегулювання цих злочинів, важливо розуміти їх природу, щоб захистити бізнес від потенційних втрат. У даній статті ми досліджуємо загрози цифрового шантажу, аналізуємо його вплив на маркетинг та пропонуємо шляхи запобігання таким атакам.

Аналіз останніх досліджень і публікацій. Проблематика функціонування маркетингових систем у цифровому середовищі є предметом уваги багатьох науковців. У зарубіжній літературі цей аспект досліджували, зокрема, Д. Гревал, С. М. Нобл, Дж. Нордфельт і А. Л. Роггевен, які акцентують на впливі цифрових технологій на побудову маркетингових комунікацій, використання великих даних та адаптацію до змін у поведінці споживачів у цифрову епоху.

Серед українських дослідників, таких як В. Г. Гноєвий, О. М. Корень, М. А. Окландер, Т. О. Окландер, О. І. Яшкіна, де особливу увагу приділено дослідженню цифрового маркетингу як моделі маркетингу XXI століття, а також сучасним тенденціям, що впливають на формування маркетингових стратегій. Їхні праці охоплюють аналіз цифрових каналів взаємодії з клієнтами, виклики, пов'язані з конфіденційністю даних, та переваги персоналізованих підходів у маркетинговій діяльності.

Дослідження також розкривають використання штучного інтелекту у цифровому маркетингу, зокрема при аналізі неструктурованих даних і впровадженні інноваційних підходів до управління клієнтськими даними. Це підкреслює важливість адаптації до нових викликів, які супроводжують розвиток цифрового середовища.

Виділення невирішених раніше частин загальної проблеми. Попри розвиток цифрового маркетингу, питання захисту від цифрового шантажу залишаються недостатньо вивченими. Кіберзлочинці все частіше атакують корпоративні системи, викрадають дані клієнтів і шантажують компанії, підриваючи їхню репутацію та довіру клієнтів. Швидка адаптація злочинців до нових технологій створює унікальні виклики, особливо у використанні алгоритмів, які маркетологи застосовують для аналізу поведінки споживачів. Додатковим ризиком є шантаж, спрямований на порушення виробничих процесів чи дистрибутивних ланцюгів, що може завдати значної шкоди репутації бренду. Конфіденційність клієнтських даних залишається під загрозою, що підриває довіру до бізнесу. Ці виклики вимагають нових підходів до кібербезпеки, управління репутацією та взаємодії з клієнтами, що є ключовими для ефективного використання цифрового маркетингу в сучасному середовищі.

Формулювання цілей статті. Мета цієї статті полягає у дослідженні впливу цифрового шантажу на маркетингову діяльність у сучасному цифровому середовищі. Основна увага зосереджена на вивченні теоретичних аспектів взаємодії між цифровими технологіями та маркетингом, зокрема аналізі загроз, які виникають у зв'язку з розвитком кіберзлочинності. Стаття також розглядає можливості використання сучасних підходів, таких

як автоматизація та машинне навчання, для виявлення та запобігання ризикам у маркетингових стратегіях.

У рамках дослідження буде проаналізовано, як цифровий шантаж впливає на довіру споживачів і ефективність маркетингових кампаній, а також висвітлено перспективи подальших наукових досліджень у цій галузі. Особлива увага приділяється питанням забезпечення стійкості маркетингових стратегій у контексті швидкої еволюції технологій і зростання кіберзагроз.

Виклад основного матеріалу дослідження. Цифровий маркетинг є важливою складовою сучасної бізнес-екосистеми, яка розвивається надзвичайно стрімко. Протягом останнього десятиліття цей напрямок суттєво трансформувався, забезпечуючи компанії численними інструментами для досягнення цільової аудиторії. Водночас використання цифрових технологій відкриває нові виклики, зокрема пов'язані з кіберзагрозами, які можуть порушувати нормальне функціонування маркетингових кампаній.

Цифровий маркетинг базується на інтеграції онлайн- і офлайн-інструментів, включаючи соціальні мережі, веб-сайти, мобільні додатки, аналітику великих даних та автоматизовані системи. Всі ці технології спрямовані на підвищення якості взаємодії між бізнесом і клієнтами, забезпечення персоналізації та швидкої адаптації до змін у потребах споживачів [1–2]. Однак саме використання таких складних систем робить компанії вразливими до кіберзлочинності, включаючи шантаж через викрадення даних, злом виробничих процесів або поширення дезінформації.

Однією з ключових тенденцій є посилення ролі аналізу даних у маркетингу. Завдяки інструментам big data бізнес може розуміти поведінку споживачів і пропонувати індивідуалізовані рішення. Проте хакери, маючи доступ до цих даних, здатні не лише викликати збої у процесах, але й використовувати конфіденційну інформацію для шантажу.

Іншим важливим аспектом є активна присутність у соціальних мережах, яка стала невід'ємною частиною стратегії цифрового маркетингу. Водночас платформи соціальних мереж є одними з найвразливіших до кіберзагроз. Поширення фальшивих акаунтів, маніпуляція даними та спрямовані атаки на репутацію брендів створюють нові виклики для маркетологів [3, с. 97].

Швидка адаптація до змін та орієнтація на сучасні технології надає компаніям змогу залишатися конкурентоспроможними. Однак у процесі цифровізації необхідно приділяти особливу увагу забезпеченню кібербезпеки, оскільки будь-яка втрата даних або їх зловмисне використання може підірвати довіру споживачів, що є критичним для успіху маркетингових стратегій.

Таким чином, цифровий маркетинг пропонує унікальні можливості для залучення клієнтів, але водночас створює ризики, які потребують детального аналізу та впровадження нових підходів до захисту даних і репутації брендів.

Згідно з новим звітом Orange Cyberdefense [4], кібершантаж продовжує залишатися однією з найбільших загроз для бізнесу, незалежно від його масштабу чи галузі. Дані звіту Cy-Explorer 2024 [5] свідчать, що кількість жертв кіберзлочинців, які використовують методи шантажу, зросла на 77% порівняно з 2023 р. Особливу небезпеку цей тип атак становить для малих підприємств, які піддаються кіберзагрозам у чотири рази частіше, ніж середній та великий бізнес.

У період із першого кварталу 2023 р. до першого кварталу 2024 р. 60 різних груп шантажистів здійснили атаки на 4374 підприємства. У першому кварталі 2024 р. 1046 організацій стали жертвами подвійного шантажу, який включає як викрадення даних, так і загрозу їх публікації [6].

Реальне число жертв, імовірно, значно вище, оскільки статистика базується лише на даних, знайдених у даркнеті. Наприклад, після ліквідації груп ALPHV/BlackCat і LockBit правоохоронці повідомили, що реальна кількість постраждалих компаній була в 1,61 і 1,52 рази більшою, ніж передбачалося раніше. Загалом, дані свідчать, що фактичний масштаб кібершантажу в 2023 і 2024 рр. був на 50-60% більшим, ніж раніше оцінювали експерти [7].

Ця ситуація підкреслює важливість побудови стійких маркетингових стратегій, які враховують ризики, пов'язані з кіберзагрозами. Для компаній не лише важливо мати сильну репутацію, але й забезпечувати безпеку своїх цифрових активів. Втрата даних клієнтів чи загроза оприлюднення конфіденційної інформації може не лише підірвати довіру споживачів, а й завдати серйозної шкоди маркетинговим кампаніям.

Зростання кількості кібератак найінтенсивніше відбувається в регіонах із потужним економічним розвитком та спільними мовними групами. Так, у США, Великобританії та Канаді кількість атак зросла на 108%, 96% та

76% відповідно. У Європі цей показник становив 60%. Проблема кібершантажу має глобальний характер: із 2020 р. 75% країн світу стикалися з таким видом атак [6].

Кіберзлочинці атакують підприємства всіх галузей, але найбільше постраждали виробництво, професійні, наукові та технічні послуги, а також оптова торгівля. У період із 2023 р. по 2024 р. кількість атак на організації, що надають медичні та соціальні послуги, зросла на 160%, попри ризики негативного суспільного та політичного резонансу.

Одним із методів тиску, що його застосовують хакери, є публікація викрадених даних на спеціальних майданчиках у даркнеті. Це значно збільшує імовірність виплати викупу, оскільки компанії намагаються мінімізувати шкоду своїй репутації. Багато жертв кібершантажу стикаються з повторними витоками даних, що додатково посилює тиск і карає за відмову платити викуп. У деяких випадках інформація однієї компанії розміщувалася на кількох платформах і різними групами хакерів.

Для маркетингу ці виклики мають особливе значення, оскільки витоки даних можуть негативно впливати на репутацію бренду, знижувати довіру клієнтів та ускладнювати реалізацію маркетингових стратегій. Публікація конфіденційної інформації або компрометація цінностей бренду може стати вирішальним фактором, що змушує компанії змінювати стратегію просування та управління репутацією.

Онлайн-шантаж залишається складним викликом для господарюючих суб'єктів, оскільки загроза розголошення конфіденційної інформації може суттєво вплинути на їхню репутацію. Однак багато підприємств усвідомлюють, що виплата викупу не гарантує вирішення проблеми. Часто це лише посилює ситуацію, перетворюючи її на цифрову версію рекету, коли злочинці знову і знову вимагають гроші в обмін на мовчання.

Незважаючи на це, шантаж може бути ефективним через кілька причин. Одна з них – встановлення викупу на рівні, що сприймається підприємством як прийнятна ціна за захист бренду. Наприклад, у випадку з Bell Canada, коли компанія відмовилася платити хакерам, витік даних викликав негативну реакцію в медіа, і репутація бренду постраждала [6]. Інший приклад – Uber, яка в 2016 р. заплатила 100 тис. дол. хакерам за приховування інформації про викрадення даних 57 мільйонів користувачів. Попри це, через рік компанія розкрила факт атаки, що викликало нову хвилю критики [7].

Ключовий виклик для маркетологів у таких ситуаціях полягає в тому, як зберегти довіру клієнтів і репутацію бренду. Підприємства, що піддаються шантажу, ризикують не лише втратити дані, але й втратити своїх споживачів, оскільки витоки інформації викликають недовіру до здатності бренду захищати конфіденційність.

Цікаво, що шантаж часто стає більш ефективним у випадках із чіткими часовими рамками, наприклад, під час виборчих кампаній або перед запуском нового продукту. Коли репутаційні ризики досягають піку, компанії можуть бути змушені діяти негайно, щоб уникнути довгострокових втрат. Це створює додатковий тиск на маркетингові команди, які повинні не лише реагувати на кризу, але й запобігати подібним інцидентам у майбутньому.

Масові атаки та цілеспрямовані шантажі також мають різні наслідки для бізнесу. У цілеспрямованих атаках хакери зазвичай шукають компрометуючі дані про керівників або бренди, що робить маркетинг більш вразливим. Такі ситуації змушують компанії розглядати нові стратегії управління репутацією, що включають як технологічний захист, так і побудову стійких відносин із клієнтами.

Зрештою, успішна маркетингова стратегія в умовах цифрового шантажу залежить не лише від здатності компанії запобігати атакам, але й від готовності реагувати на репутаційні кризи, забезпечуючи прозорість і довіру клієнтів.

Соціальні мережі стають дедалі поширенішим інструментом для кіберзлочинців, які використовують їх для шантажу. Один із методів – поширення фейкової інформації про підприємства із подальшою вимогою оплати за припинення цієї наклепницької кампанії. Такі атаки можуть включати як поширення негативних чуток, так і створення інформаційного «шуму», який шкодить репутації жертви.

Цей підхід особливо небезпечний у цифровому світі, де інформація зберігається набагато довше, ніж у традиційних медіа. Наприклад, наклепницька кампанія, розпочата кілька років тому, може все ще з'являтися у верхніх рядках пошукових систем, продовжуючи завдавати шкоди репутації господарюючого суб'єкта. Крім того, швидкість поширення новин у соціальних мережах забезпечує злочинцям ефективний інструмент для нанесення ударів по репутації брендів.

Підприємства, які покладаються на соціальні мережі для маркетингового просування, особливо вразливі до таких атак. Наприклад, кампанії з просування продукції чи послуг можуть бути під загрозою через спам-атаки, що створюють «забруднення» хештегів або дезінформацію. Це може не лише знизити ефективність маркетингових зусиль, але й викликати втрату довіри клієнтів.

Однією з найбільших загроз є поширення фейкових відгуків або шкідливої інформації про продукти. Це може мати руйнівний вплив на суб'єкти, які залежать від краудсорсингових платформ, таких як Amazon або Yelp, де відгуки споживачів відіграють ключову роль у прийнятті рішень. Готелі, ресторани та інші підприємства сфери послуг є особливо чутливими до рейтингових систем, і наклепницькі кампанії можуть завдати їм значних збитків [8].

Технологічний прогрес створює нові можливості для таких атак. Наприклад, розробка інструментів для підробки відео та аудіо за допомогою ШІ дозволяє злочинцям створювати реалістичні відеозаписи з фейковими заявами від імені компаній або окремих осіб [9–10]. Такі матеріали, поширені в соціальних мережах, можуть значно ускладнити маркетингові зусилля підприємств, викликати сумніви у клієнтів та завдати значної шкоди репутації бренду.

Попри зростання обізнаності користувачів про фейкові новини та необхідність перевірки фактів, більшість людей все ще схильна довіряти вражаючим або сенсаційним повідомленням, особливо якщо вони супроводжуються візуальними чи аудіоелементами. Це підкреслює важливість для маркетологів не лише захищати репутацію своїх брендів, але й активно боротися з дезінформацією в соціальних мережах, впроваджуючи механізми протидії фейкам та розробляючи стратегії кризового управління.

Згідно зі звітом The Global Risks Report 2024: 19th edition, ризики, пов'язані з використанням штучного інтелекту для створення дезінформації та фальшивої інформації, займають друге місце серед найбільш впливових глобальних ризиків на найближчі два роки [11]. П'ятий за важливістю ризик стосується кіберзагроз, які продовжують загрожувати як урядам, так і приватному сектору. Ці ризики мають значний вплив не тільки на політичну та соціальну сфери, але й на маркетингову діяльність компаній.

Використання дезінформації, особливо в періоди виборів, може створити середовище недовіри та поляризації. Близько трьох мільярдів людей у найближчі два роки візьмуть участь у виборах у країнах, включаючи США, Велику Британію, Індію, Індонезію та Пакистан. У таких умовах фейкові новини та маніпуляції громадською думкою можуть підірвати легітимність не лише урядів, але й брендів, які залежать від довіри споживачів.

Дезінформація про продукти, послуги чи етичні стандарти підприємств може поширюватися через ті ж платформи, що й політична пропаганда, завдаючи шкоди маркетинговим кампаніям. Наприклад, фейкові відгуки або маніпулятивні заяви про господарюючий суб'єкт можуть впливати на громадську думку так само, як і політична дезінформація, спричиняючи втрату довіри клієнтів.

Кіберзагрози, які посідають п'яте місце серед глобальних ризиків у звіті, також становлять серйозну проблему для маркетингу. Кібератаки, спрямовані на викрадення клієнтських даних або злам платформ соціальних мереж, можуть підірвати як репутацію компанії, так і її маркетингові ініціативи. Наприклад, кампанії, які покладаються на аналітику даних або активність у соціальних мережах, можуть бути зупинені через цілеспрямовані атаки, включаючи DDoS або розголошення конфіденційної інформації.

У довгостроковій перспективі зростання маніпуляцій і фейкових новин також може вплинути на ефективність цифрових інструментів маркетингу. Уряди можуть запроваджувати суворі регуляції щодо використання інтернету, соціальних мереж і платформи даних, що зменшить свободу маркетологів у розробці та впровадженні інноваційних кампаній.

Для підприємств це означає необхідність впровадження стратегій управління репутацією та кібербезпеки. Прозорість, активна взаємодія зі споживачами та швидке реагування на можливі інформаційні атаки стають ключовими елементами успішного маркетингу в сучасному середовищі.

Великі кіберзагрози, спрямовані на корпорації по всьому світу, демонструють, наскільки вразливими є компанії в цифрову епоху. Наприклад, у 2021 р. атака на Colonial Pipeline паралізувала роботу найбільшого трубопроводу США, спричинивши паливну кризу та змусивши компанію сплатити викуп у розмірі 4,4 млн. дол. Інший відомий випадок – злом PlayStation Network у 2011 р., внаслідок якого були викрадені дані 77 млн. користувачів, включаючи номери кредитних карток.

Такі інциденти завдають не лише фінансових втрат, але й шкодять репутації компаній, що робить їх маркетингові зусилля значно складнішими [7].

В Україні кібербезпека стала особливо актуальною з початком війни у 2022 р. За словами О. Кацуби, кількість кібератак на українські підприємства зросла в рази, а їх складність і руйнівний ефект значно посилилися. У 2023 р. було зафіксовано понад 1500 значних атак, спрямованих як на державні установи, так і на приватний сектор. Атаки включали DDoS-удари, злам баз даних і викрадення конфіденційної інформації [12].

Такі загрози створюють додатковий тиск на бізнес, змушуючи компанії витрачати значні ресурси на відновлення даних та підтримку репутації. Як свідчить випадок однієї з великих українських IT-компаній, яка зазнала масованої атаки, наслідки включали витік даних тисяч клієнтів і фінансові втрати в мільйони гривень. Відновлення довіри клієнтів стало важким і довготривалим процесом.

Таким чином, кібербезпека – це не лише технічний виклик, але й стратегічний фактор, який впливає на маркетингову діяльність компаній. Забезпечення захисту даних та швидка реакція на інциденти є ключовими для підтримки довіри клієнтів і конкурентоспроможності брендів.

Кібершантаж, зокрема атаки програм-вимагачів, залишається однією з найсерйозніших загроз для сучасного бізнесу. Зловмисники постійно вдосконалюють свої стратегії, спрямовуючи атаки на галузі з найбільшим потенціалом прибутку, такі як охорона здоров'я, виробництво та критична інфраструктура. У цих секторах дані мають вирішальне значення для роботи, а будь-які збої або втрати інформації можуть завдати непоправної шкоди. Наприклад, лікарні залежать від доступу до історій пацієнтів, а фабрики – від безперервності виробничих процесів.

Особливо небезпечними стають цільові атаки, коли шкідливе програмне забезпечення налаштовується на пошук і шифрування даних, найбільш критичних для конкретної галузі. У таких випадках шантаж може включати динамічне ціноутворення, що враховує масштаби та ресурси постраждалої організації. Це робить атаки більш персоналізованими та потенційно руйнівними для компаній.

Для маркетингу подібні інциденти можуть стати значним викликом. По-перше, атаки програм-вимагачів можуть паралізувати цифрові платформи, соціальні мережі чи CRM-системи, на які компанії покладаються для комунікації зі споживачами. По-друге, витік або пошкодження даних можуть серйозно підірвати довіру клієнтів до бренду, адже споживачі очікують надійного зберігання їхньої конфіденційної інформації.

Ще одним ризиком є погіршення якості резервних копій через нові методи, такі як «забруднення даних». У таких випадках шкідливе програмне забезпечення поступово змінює резервні копії, роблячи їх непридатними для відновлення. Це ускладнює реагування на атаки та підвищує вразливість до шантажу.

Ці ризики підкреслюють важливість інтеграції кібербезпеки в маркетингову стратегію. Компанії повинні інвестувати в сучасні технології захисту, регулярно оновлювати системи, впроваджувати багатофакторну аутентифікацію та забезпечувати надійне резервне копіювання. Захист даних і репутації бренду – це не лише питання безпеки, а й ключовий елемент довгострокового успіху на конкурентному ринку.

Захист від кіберзагроз є важливою складовою стратегії сучасного бізнесу, особливо в умовах цифрового шантажу та зростання атак. Як зазначає О. Кацуба, компанії повинні не лише реагувати на загрози, але й активно впроваджувати превентивні заходи. Інвестиції в сучасні системи кібербезпеки, навчання персоналу, впровадження багатофакторної аутентифікації, шифрування даних та регулярні оновлення програмного забезпечення допомагають мінімізувати ризики [12].

Важливим елементом є резервне копіювання даних, що дозволяє швидко відновлювати роботу компанії без виплати викупу. Також слід обмежувати доступ до критичних систем та регулярно перевіряти вразливості. У контексті України, де кіберзагрози є особливо серйозними через геополітичну ситуацію, такі заходи стають не просто рекомендацією, а обов'язковою умовою для забезпечення стійкості бізнесу.

Комплексний підхід до кібербезпеки є не лише технічним питанням, а й стратегічною необхідністю, що забезпечує захист репутації бренду, довіру клієнтів та стабільність у швидкозмінному цифровому середовищі.

Висновки. Цифровий маркетинг, попри свої численні переваги, зіштовхується з серйозними викликами, пов'язаними зі зростанням кіберзагроз. Атаки програм-вимагачів, витоки даних і дезінформація стають не лише технічними проблемами, але й серйозно впливають на маркетингові процеси, зокрема

на довіру клієнтів, репутацію бренду та ефективність комунікацій.

Аналізуючи сучасні кіберзагрози, можна стверджувати, що для збереження конкурентоспроможності підприємствам необхідно впроваджувати інноваційні підходи до управління кібербезпекою. Це включає впровадження сучасних технологій захисту даних, шифрування, багатофакторної аутентифікації, а також розвиток системи резервного копіювання. Окрім технічних рішень, важливим є створення прозорих комунікацій із клієнтами та ефективне управління репутацією.

Особливої уваги потребує інтеграція кібербезпеки у маркетингові стратегії. Забезпечення захисту даних клієнтів та адаптація до нових загроз є ключовими для збереження довіри до бренду. В умовах швидкої цифровізації бізнесу та посилення кіберзлочинності саме синергія маркетингу та кібербезпеки дозволить господарюючим суб'єктам не лише мінімізувати ризики, але й ефективно використовувати можливості цифрового середовища.

Таким чином, подальший розвиток цифрового маркетингу вимагає переосмислення підходів до захисту бренду, створення стійких комунікаційних систем і впровадження інновацій для протидії кіберзагрозам. Це не лише підвищить ефективність маркетингових зусиль, але й дозволить бізнесу зміцнити свої позиції у глобальному конкурентному середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Окландер М. А., Окландер Т. О., Яшкіна О.І. та ін. Цифровий маркетинг – модель маркетингу XXI сторіччя: монографія; за ред. М. А. Окландера. Одеса : Астропринт, 2017. 292 с.

2. Гноєвий В. Г., Корень О. М. Сучасні тенденції цифрового маркетингу та їх вплив на формування маркетингової стратегії. *Академічний огляд*. 2021. № 1 (54). С. 49–55.

3. Гревал Д., Нобл С. М., Роггевен А. Л., Нордфельт Дж. Майбутнє технологій у магазинах. *Журнал Академії маркетингових наук*. 2020. № 48. С. 96–113.

4. Cyberdefense: Build a safer digital society. URL: https://www.orangecyberdefense.com (дата звернення: 13.01.2025).

5. Cy-Xplorer 2024: When bits turn to blackmail - all about ransomware and cyber extortion. URL: https://www.orangecyberdefense.com/be/resourses/cy-xplorer-2024 (дата звернення: 13.01.2025).

6. Digital Extortion: A Forward-looking View. URL: https://documents.trendmicro.com/assets/wp-digital-extortion-a-forward-looking-view.pdf?utm_source=chatgpt.com (дата звернення: 13.01.2025).

7. Найвідоміші хакерські атаки, про які говорив увесь світ. URL: https://root-nation.com/ua/articles-ua/tech-ua/ua-naybilshi-hakerski-ataki/ (дата звернення: 13.01.2025).

8. Fake News and Cyber Propaganda: The Use and Abuse of Social Media. URL: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media (дата звернення: 13.01.2025).

9. Кузьомко В. М., Репнікова І. П. Використання штучного інтелекту у цифровому маркетингу. *Економіка та управління підприємствами*. Випуск 13. 2017. С. 112–118.

10. Хрупович С. Є., Борисова Т. М. Використання штучного інтелекту при маркетинговому аналізі неструктурованих даних. *Маркетинг і цифрові технології*. 2021. № 1. С. 17–26.

11. The Global Risks Report 2024: 19th edition. URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf (дата звернення: 13.01.2025).

12. Олександр Кацуба: Як кібербезпека стала новим викликом для українських підприємців. URL: https://sdamkvartiry.com/oleksandr-kaczuba-yak-kiberbezpeka-stala-novym-vyklykom-dlya-ukrayinskyh-pidpryyemcziv/?utm_source=chatgpt.com (дата звернення: 13.01.2025).

REFERENCES:

1. Oklander M.A., Oklander T.O., Yashkina O.I. et al. (2017). Digital marketing – model of marketing of the XXI century [Digital marketing – a model of marketing of the XXI century], monograph. Odesa: Astroprint, 292 p.

2. Hnoievyi V. H., Koren O. M. (2021). Suchasni tendentsii tsyfrovoho marketynhu ta yikh vplyv na formuvannia marketynhovoi stratehii [Modern trends in digital marketing and their influence on the formation of a marketing strategy]. *Akademichnyi ohliad,* no. 1 (54), pp. 49–55.

3. Hreval D., Nobl S. M., Rohheven A. L., Nordfelt Dzh. (2020). Maibutnie tekhnolohii u mahazynakh [The future of technology in stores]. *Zhurnal Akademii marketynhovykh nauk*, no. 48, pp. 96–113.

4. Cyberdefense: Build a safer digital society. Available at: https://www.orangecyberdefense.com (accessed 13 January 2025).

5. Cy-Xplorer 2024: When bits turn to blackmail – all about ransomware and cyber extortion. Available at: https://www.orangecyberdefense.com/be/resourses/cy-xplorer-2024 (accessed 13 January 2025).

6. Digital Extortion: A Forward-looking View. Available at: https://documents.trendmicro.com/assets/wp-digital-extortion-a-forward-looking-view.pdf?utm_source=chatgpt.com (accessed 13 January 2025).

7. Naividomishi khakerski ataky, pro yaki hovoryv uves svit [The most famous hacker attacks that the whole world talked about]. Available at: https://root-nation.com/ua/articles-ua/tech-ua/ua-naybilshi-hakerski-ataki/ (accessed 13 January 2025).

8. Fake News and Cyber Propaganda: The Use and Abuse of Social Media. Available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media (accessed 13 January 2025).

9. Stebliuk, N. F., & Kopieikina, Ye. V. (2019) Tekhnolohii shtuchnoho intelektu v marketynhu [Technologies of Artificial Intelligence in Marketing]. *Pryazovskyi ekonomichnyi visnyk*, vol. 3 (14), pp. 462–466.

10. KhrupovychS. Ie., BorysovaT. M. (2021). Vykorystannia shtuchnoho intelektu pry marketynhovomu analizi nestrukturovanykh danykh [Use of artificial intelligence in marketing analysis of unstructured data]. *Marketynh i tsyfrovi tekhnolohii*, no. 1, pp. 17–26.

11. The Global Risks Report 2024: 19th edition. Available at: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf (accessed 13 January 2025).

12. Oleksandr Katsuba: Yak kiberbezpeka stala novym vyklykom dlya ukrayinskykh pidpryyemtsiv [Oleksandr Katsuba: How cybersecurity has become a new challenge for Ukrainian entrepreneurs]. Available at: https://sdamkvartiry.com/oleksandr-kaczuba-yak-kiberbezpeka-stala-novym-vyklykom-dlya-ukrayinskyh-pid-pryyemcziv/?utm_source=chatgpt.com (accessed 13 January 2025).