УДК 658.8:005.934:004.738.5
JEL classification: M31, L21, O33, D81

ЦИФРОВА МАРКЕТИНГОВА РОЗВІДКА В СИСТЕМІ КОНКУРЕНТНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

ГАРМАШ Олег[1], ФОРОСТОВЕЦЬ Альона[2]
[1] Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"
https://orcid.org/0000-0003-4324-4411
e-mail: o.harmash.kpi@gmail.com
ЗВО "Відкритий міжнародний університет розвитку людини "Україна"
https://orcid.org/0000-0003-2741-1953
e-mail: akinterdep@ukr.net

У статті розроблено концептуальну та методологічну основу інтеграції цифрової маркетингової розвідки в систему конкурентної безпеки підприємства. Дослідження спрямоване на вирішення управлінської проблеми: підприємства накопичують значні обсяги цифрових даних про клієнтів, конкурентів, канали збуту та платформи, проте ці дані часто використовуються для звітування про результати маркетингових кампаній, а не для раннього виявлення конкурентних загроз і скоординованого реагування на них. У дослідженні застосовано системний підхід, структурований синтез рецензованих наукових праць із конкурентної розвідки, цифрового маркетингу, маркетингової аналітики, аналітики соціальних медіа та динамічних здатностей, порівняльний аналіз, нормалізацію індикаторів, адитивне агрегування та сценарне моделювання. Цифрову маркетингову розвідку визначено як законний, етичний і безперервний процес збирання, перевірки, інтеграції, аналізу та передавання цифрових ринкових сигналів для виявлення конкурентних можливостей і загроз та підтримки своєчасного прийняття рішень у сфері безпеки. Запропоновано п'ятирівневу архітектуру: джерела цифрових сигналів; управління даними та контроль якості; аналітичне перетворення; індикатори загроз і правила раннього попередження; прийняття рішень, дії та зворотний зв'язок. Розроблена концепція розмежовує цифрову маркетингову розвідку, епізодичні маркетингові дослідження, поточну маркетингову аналітику, бізнес-аналітику та конкурентну розвідку в ширшому розумінні. Визначено шість блоків індикаторів: стратегічна активність конкурентів; ціновий та асортиментний тиск; цифрова видимість; клієнтська та репутаційна вразливість; стійкість каналів збуту та платформ; ефективність процесу розвідки. Ризикоорієнтовані та захисні індикатори нормалізуються за єдиною шкалою; ризики окремих блоків агрегуються в інтегральний показник конкурентних загроз, тоді як окремий коефіцієнт достовірності даних запобігає інтерпретації невизначених свідчень як точного знання. Гіпотетичний розрахунок демонструє, як модель визначає пріоритетність залежності від платформ і посилення активності конкурентів та пов'язує ці загрози з визначеними відповідальними за реагування особами і строками перегляду результатів. Усі числові дані, використані в демонстраційному прикладі, є ілюстративними та не відображають діяльність реального підприємства. Науковий внесок полягає у встановленні операційного зв'язку між маркетинговою аналітикою та управлінням конкурентною безпекою через управлінський ланцюг «індикатор – порогове значення – відповідальний – дія – зворотний зв'язок» і чітке розмежування рівня загрози та достовірності доказів. Практичні результати включають поетапну дорожню карту впровадження для підприємств із різними рівнями цифрової зрілості. Запропонована концептуальна основа потребує галузевого налаштування, правової перевірки практик збирання даних та емпіричної валідації на основі довгострокових даних підприємств.

Ключові слова: цифрова маркетингова розвідка; конкурентна безпека; економічна безпека підприємства; маркетингова аналітика; конкурентна розвідка; цифрові сигнали; раннє попередження; індикатори загроз; якість даних.

https://doi.org/10.31891/mdes/2026-22-16

Стаття надійшла до редакції / Received 02.10.2026
Прийнята до друку / Accepted 03.11.2026
Опубліковано / Published 12.11.2026

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

© ГАРМАШ Олег, ФОРОСТОВЕЦЬ Альона

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Цифровізація маркетингу розширила доступ підприємств до оперативних даних про попит, поведінку клієнтів, дії конкурентів, цінові зміни, цифрову видимість брендів і реакції ринку. Однак сама наявність даних не створює захисної здатності. Без правил верифікації, контекстуалізації, ескалації та відповідальності цифрові сліди залишаються фрагментованими метриками кампаній, а не сигналами для управління конкурентною безпекою.

Конкурентну безпеку підприємства доцільно трактувати як здатність зберігати ринкову стійкість, стратегічну автономію, дохідність і довіру стейкхолдерів під впливом законних конкурентних дій, ринкових шоків і маніпулятивних інформаційних впливів. Таке розуміння не зводить безпеку до збереження наявної частки ринку: вона охоплює здатність вчасно розпізнати зміни, вибрати адекватну відповідь і перебудувати ресурси.

Класична конкурентна розвідка виходить за межі епізодичного збору відомостей про конкурентів: вона охоплює постановку інтелектуального завдання, збирання, аналіз, передавання результату користувачеві та зворотний зв'язок [1-3]. Емпіричні дослідження також застерігають, що на практиці розвідка нерідко залишається тактичною і слабо пов'язаною з формуванням стратегії

[4]. Отже, науково-практична проблема полягає в тому, щоб перетворити дисперсні цифрові ринкові сигнали на перевірювані індикатори загроз і вбудувати їх у цикл управління безпекою.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Цифровий маркетинг розглядається як адаптивний процес, у якому цифрові точки контакту, медіа, транзакції та мережеві ефекти змінюють створення і привласнення споживчої цінності [5]. У середовищі, насиченому даними, маркетингова аналітика охоплює моделі, метрики та експерименти, які пов'язують ринкові дані з управлінськими діями [6]. Водночас емпіричні роботи показують, що вплив маркетингової аналітики на конкурентну перевагу опосередковується здатністю організації інтегрувати знання, застосовувати моделі та змінювати процеси, а не самим фактом придбання технології [7; 8].

Окремий блок досліджень стосується аналітики соціальних медіа. Для малих і середніх виробничих підприємств виявлено зв'язок між аналітикою соціальних медіа, конкурентною розвідкою і динамічними здатностями [9]. Аналітика соціальних медіа може підтримувати конкурентну розвідку, але її цінність обмежують неповнота даних, алгоритмічна селекція контенту і складність перетворення сигналу на рішення [10]. Сучасні методи тематичного моделювання і прогнозування залученості демонструють можливість виявляти теми брендів і оцінювати реакцію аудиторії, проте потребують етичного та конфіденційного управління [11]. Для малих і середніх підприємств критичною є не лише якість моделі, а й інтеграція знань між функціями бізнесу [12].

Штучний інтелект посилює прогнозні та прескриптивні можливості маркетингу, водночас загострюючи питання приватності, алгоритмічної упередженості та розподілу відповідальності [13]. Концептуальні моделі аналітики соціальних медіа наголошують на зв'язку між джерелом, методом, бізнес-завданням і оцінкою результату [14]. При цьому збирання, підготовка даних і виявлення тем залишаються самостійними джерелами помилок [15]. У ширшому контексті аналітики великих даних значення мають не тільки обсяг і швидкість, а й варіативність, достовірність і придатність даних до конкретного методу [16]. Ефект від аналітики на результати підприємства також залежить від динамічних здатностей [17], теоретично описаних через процеси розпізнавання змін, захоплення можливостей і трансформації ресурсної бази [18].

У публікаціях цільового журналу маркетингову складову економічної безпеки вже пов'язано з системою показників, нормуванням і агрегуванням [19], а маркетингові чинники розглянуто як частину безпеки бізнесу [20]. Окремо обґрунтовано механізм безпеки на основі маркетингових інновацій [21], проаналізовано цифрові ризики та інформаційну безпеку корпоративного сектору [22]. Логіку побудови індикаторів безпеки розвинено для інтелектуалізованих логістичних послуг [23], а цифрові технології показано як драйвер маркетингових комунікацій [24].

Проведений синтез засвідчує сформовану методичну базу для збирання і аналізу цифрових ринкових даних. Водночас залишається недостатньо розкритою наскрізна архітектура, яка одночасно: 1) відмежовує цифрову маркетингову розвідку від суміжних видів аналітики; 2) пов'язує джерела даних із конкретними індикаторами конкурентної загрози; 3) враховує окремо рівень загрози та довіру до даних; 4) призначає власника реакції і контрольний термін. Саме це становить невирішену частину проблеми.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Незважаючи на значну кількість наукових праць, присвячених конкурентній розвідці, цифровому маркетингу, маркетинговій аналітиці та економічній безпеці підприємства, недостатньо дослідженим залишається питання їх інтеграції в єдину систему управління конкурентною безпекою. У науковій літературі конкурентну розвідку переважно розглядають як інструмент інформаційного забезпечення стратегічного управління, маркетингову аналітику – як засіб підвищення ефективності маркетингових рішень, а економічну безпеку – як окремий напрям ризик-менеджменту підприємства [1-18]. Водночас цифрові маркетингові дані ще недостатньо досліджені як джерело сигналів раннього попередження про конкурентні загрози [19-24].

Недостатньо розробленими залишаються методичні підходи до побудови наскрізного процесу цифрової маркетингової розвідки, який поєднував би джерела даних, процедури їх перевірки, аналітичне опрацювання, систему індикаторів, порогові значення та механізми управлінського реагування. Потребують подальшого наукового обґрунтування способи відокремлення достовірних конкурентних сигналів від інформаційного шуму, помилкових тривог, маніпулятивного контенту та викривлень, спричинених алгоритмами цифрових платформ.

Невирішеним також залишається питання одночасного оцінювання рівня конкурентної загрози та ступеня довіри до даних, на підставі яких вона була ідентифікована.

Крім того, недостатньо опрацьованими є практичні підходи до формування інтегрованої системи індикаторів цифрової маркетингової розвідки, визначення відповідальних осіб, строків реагування та процедур контролю результативності прийнятих рішень. Актуальною є розробка моделі, яка забезпечувала б послідовний перехід від цифрового ринкового сигналу до конкретного управлінського рішення за принципом «індикатор – поріг – власник – дія – зворотний зв'язок». Необхідність концептуального та методичного обґрунтування такої моделі зумовила вибір теми статті, її мету й основні напрями дослідження.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є розроблення концептуально-методичних засад інтеграції цифрової маркетингової розвідки до системи конкурентної безпеки підприємства. Для досягнення мети поставлено завдання: уточнити поняття та межі цифової маркетингової розвідки; сформувати архітектуру її вбудовування у контур безпеки; запропонувати систему індикаторів і алгоритм їх агрегування; визначити правила реагування; продемонструвати логіку моделі на умовному прикладі.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Поняття та межі цифрової маркетингової розвідки.

У цьому дослідженні цифрова маркетингова розвідка (ЦМР) трактується як законний, етичний і безперервний процес збирання, верифікації, інтеграції, аналізу і передавання цифрових ринкових сигналів про конкурентів, споживачів, ціни, продукти, канали, технології та репутаційне середовище з метою раннього виявлення можливостей і загроз та підтримки рішень у системі конкурентної безпеки.

Визначення містить чотири принципові обмеження. По-перше, розвідка не означає несанкціонованого доступу, обходу технічних обмежень, маніпулювання персоналом конкурента чи збирання персональних даних без правової підстави. По-друге, об'єктом є не «усі дані», а сигнали, пов'язані з конкретними управлінськими питаннями. По-третє, результат має містити оцінку довіри, а не лише числовий бал. По-четверте, розвідувальний продукт завершується не дашбордом, а рішенням, власником рішення та перевіркою наслідків.

Таблиця 1

Розмежування цифрової маркетингової розвідки та суміжних понять

Поняття	**Провідне питання**	**Типовий результат**	**Відмінність від ЦМР**
Маркетингове дослідження	Що відбувається на ринку у визначений момент?	Звіт або вибіркове дослідження	ЦМР є безперервною і прив'язаною до сигналів загроз
Маркетингова аналітика	Чому змінилися метрики і як їх оптимізувати?	Метрика, модель, експеримент	ЦМР додає конкурентний контекст, поріг і протокол реакції
Бізнес-аналітика	Що показують внутрішні дані підприємства?	Управлінська звітність і дашборд	ЦМР фокусується на зовнішніх ринкових змінах і їх наслідках
Конкурентна розвідка	Які зовнішні зміни впливають на стратегію?	Інтелектуальний продукт для керівництва	ЦМР – її маркетинговий цифровий контур з частішою періодичністю

Джерело: складено авторами за результатами синтезу [1-6].

Таке розмежування має практичне значення. Маркетингова аналітика може засвідчити падіння конверсії; ЦМР має поєднати цю зміну з динамікою видимості конкурентів, ціновими акціями, зміною пошукової видачі, відгуками клієнтів і збоями каналів, а потім оцінити альтернативні пояснення і визначити дію.

Архітектура ЦМР у системі конкурентної безпеки.

Архітектура ЦМР сформована як замкнений цикл з п'яти рівнів (рис. 1). Перший рівень поєднує внутрішні дані – CRM, продажі, вебаналітику, звернення, експерименти – з дозволеними зовнішніми джерелами: вебсайтами конкурентів, пошуковою видачею, маркетплейсами, магазинами застосунків, соціальними медіа, публічними реєстрами, вакансіями і галузевими

оглядами. Сигнал повинен мати посилання на джерело, часову мітку, власника та статус верифікації.

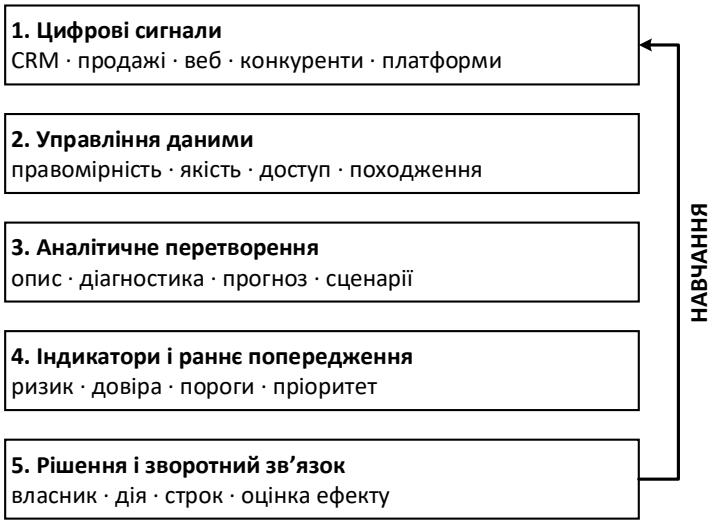


Рис. 1. П'ятирівнева архітектура цифрової маркетингової розвідки

Джерело: авторська розробка.

Другий рівень – управління даними і якістю. Він охоплює правову підставу, мінімізацію персональних даних, розмежування доступу, збереження історії, дедуплікацію, контроль ботів і спаму, визначення порівнюваних сегментів. Третій рівень перетворює дані на знання за допомогою описової, діагностичної, прогнозної та прескриптивної аналітики. Четвертий рівень формує індикатори, пороги, сценарії та пакет доказів. П'ятий призначає власника, строк і варіант відповіді, а зворотний зв'язок коригує пороги і правила.

Таблиця 2

Архітектура цифрової маркетингової розвідки

Рівень	Зміст	Вихід	Власник
1. Сигнали	CRM, продажі, вебаналітика, публічні цифрові сліди ринку	Потік датованих спостережень	Власник даних
2. Управління	Правовість, доступ, якість, походження, зберігання	Верифікований набір даних	Відповідальний за управління даними / юрист
3. Аналітика	Опис, діагностика, прогноз, сценарій	Пояснений сигнал і альтернативи	Маркетинговий аналітик
4. Індиктори	Нормування, пороги, триангуляція, довіра	Картка загрози і пріоритет	Координатор безпеки
5. Реагування	Рішення, строк, власник, ескалація, оцінка ефекту	Закрита дія та оновлене правило	Власник бізнес-рішення

Джерело: авторська розробка.

Принципово важлим є подвійне керування. Керівник маркетингу відповідає за придатність сигналу до ринкового рішення, а координатор економічної безпеки – за порівняння сигналу з іншими ризиками, ескалацію і контроль закриття. Аналітик не повине одночасно бути єдиним верифікатором власного висновку для критичних сигналів.

Система індикторів і метод інтегральної оцінки.

З метою збалансування швидких ринкових сигналів і структурної вразливості запропоновано шість блоків: В1 – стратегічна активність конкурентів; В2 – ціново-асортиментний тиск; В3 – цифрова видимість; В4 – клієнтська та репутаційна вразливість; В5 – стійкість каналів і платформ; В6 – результативність розвідувального процесу. Блок В6 не описує зовнішню загрозу; він показує, наскільки сам контур спостереження здатен вчасно спрацювати.

Для зведення різновимірних показників до шкали [0; 1] задаються нижня L_i і верхня U_i опорні межі. Для дестимулятора, зростання якого означає посилення загрози, нормований ризик r_i розраховується за формулою (1), для стимулятора безпеки – за формулою (2). Значення поза опорним інтервалом обмежуються нулем і одиницею.

$$r_i = min\{1;\ max[0;\ (x_i - L_i)/(U_i - L_i)]\},\ \text{для дестимулятора} \quad (1)$$

$$r_i = min\{1;\ max[0;\ (U_i - x_i)/(U_i - L_i)]\},\ \text{для стимулятора} \quad (2)$$

Опорні межі не слід встановлювати універсально. Їх доцільно калібрувати за галузевим розподілом, власною історією, допустимим апетитом до ризику і валідованими експертними оцінками. До накопичення достатньої історії можна застосовувати консервативні пороги з обов'язковим ручним підтвердженням.

Таблиця 3

Базова система індикторів конкурентної безпеки

Код	Індиктор	Напрям	Основні джерела	Порогова логіка
B1.1	Частота змін цін/промо у конкурентів	↑ ризик	Сайти, маркетплейси	Відхилення від 90-денної бази
B1.2	Інтенсивність продуктових/кадрових сигналів	↑ ризик	Новини, вакансії, патенти	Два незалежні джерела
B2.1	Ціновий розрив до медіани сегмента	↑ ризик	Прайси, маркетплейси	Поза допустимим коридором маржі
B2.2	Індекс перекриття асортименту	↑ ризик	Каталоги, SKU-мапінг	Різка зміна в цільовому сегменті
B3.1	Частка пошуку бренду/категорії	↓ захист	Пошукові тренди, SEO	Падіння поза контрольну межу
B3.2	Відносна видимість у цільових каналах	↓ захист	SEO, соцмережі, медіа	Втрата позицій у 2+ каналах
B4.1	Частка негативних тем із високим охопленням	↑ ризик	Відгуки, соцмережі, сервіс	Злам тональності + охоплення
B4.2	Рівень відтоку/скарг за сегментами	↑ ризик	CRM, сервіс, опитування	Зміна вища за сезонно скориговану
B5.1	Залежність виручки від однієї платформи	↑ ризик	Фінанси, атрибуція каналів	Перевищення ліміту концентрації
B5.2	Готовність резервного каналу	↓ захист	Плани безперервності, тести	Непроходження періодичного тесту
B6.1	Медіанний час від сигналу до верифікації	↑ ризик	Журнал сигналів	Порушення SLA за класом загрози
B6.2	Частка хибних тривог і незакритих дій	↑ ризик	Журнал валідації/дій	Перевищення дедлайну або толерантності

Джерело: авторська розробка; пороги підлягають галузевому калібруванню.

Блокова оцінка B_k і загальний індекс загрози R розраховуються адитивно; w_{ik} і v_k – ваги індикторів і блоків, сума яких на відповідному рівні дорівнює одиниці. Індекс конкурентної безпеки S визначається як доповнення до R (формула 3).

$$B_k = \Sigma_i w_{ik} r_{ik}; \quad R = \Sigma_k v_k B_k; \quad S = 1 - R \tag{3}$$

Робоча інтерпретація S може мати такий вигляд: 0,80-1,00 – стійкий стан; 0,60-0,79 – зона уваги; 0,40-0,59 – підвищена загроза; менше 0,40 – критичний стан. Ці межі є методичними, а не емпірично універсальними. Ваги можна оцінювати за попарними порівняннями, ентропійним методом або за прогнозною силою; для першої ітерації доцільними є рівні ваги, які запобігають хибній точності.

Окремо оцінюється коефіцієнт довіри Q: повнота C, своєчасність T, точність A і надійність джерела D. Ваги α також сумуються до одиниці. Q не множиться на S, оскільки це змішало б два різні виміри: стан безпеки та надійність доказу.

$$Q = \alpha_C C + \alpha_T T + \alpha_A A + \alpha_D D; \quad \Sigma\alpha = 1 \tag{4}$$

Для окремого сигналу пріоритет реакції P_i визначається як добуток нормованого ризику r_i, довіри q_i і оцінки масштабу наслідків h_i. На відміну від S, це оперативний бал черговості, а не індекс стану.

$$P_i = r_i q_i h_i \tag{5}$$

При високому ризику і низькій довірі першою дією є не агресивна ринкова відповідь, а прискорена верифікація і підготовка оборотної дії. За високих R і Q сигнал ескалюється в день виявлення. За низького R, але високої довіри достатньо моніторингу; за низьких R і Q – уточнення джерела або закриття сигналу як неінформативного.

Умовна демонстрація та інтерпретація.

Для перевірки внутрішньої логіки моделі розглянуто умовне підприємство. Числа не отримані з бухгалтерської, CRM, вебаналітичної чи іншої бази реального суб'єкта; тому інтерпретувати їх як емпіричний результ неможна. Всі шість блоків мають рівну вагу 1/6, щоб не імітувати точність непроведеного експертного зважування.

Таблиця 4

Ілюстративне оцінювання блоків для умовного підприємства

Блок	Нормований ризик	Інтерпретація	Перша управлінська дія
B1	0,62	Посилена активність конкурентів	Перевірити сигнали за 2+ джерелами
B2	0,48	Помірний ціново-асортиментний тиск	Оновити карту ціннісних пропозицій
B3	0,57	Ослаблення цифрової видимості	Провести розклад за каналами і запитами
B4	0,39	Контрольована вразливість	Продовжити моніторинг негативних тем
B5	0,71	Висока платформена залежність	План диверсифікації і тест резервного каналу
B6	0,53	Нестабільна результативність процесу	Переглянути SLA та причини хибних тривог

Джерело: авторський умовний приклад. Усі числові значення є ілюстративними.

Інтегральний ризик за рівних ваг становить R = (0,62 + 0,48 + 0,57 + 0,39 + 0,71 + 0,53) / 6 = 0,55. Відповідно S = 1 − 0,55 = 0,45, що за пропонованою методичною шкалою відповідає підвищеній загрозі. Найвищим є ризик стійкості каналів і платформ (0,71), другим – стратегічна активність конкурентів (0,62). Тому першочерговими мають бути не пропорційне збільшення рекламного бюджету, а перевірка залежності від ключових платформ, підготовка резервних каналів і верифікація стратегічних сигналів конкурентів.

У сценарії передбачається, що блок B5 отримав високу довіру до даних, оскільки платформена залежність підтверджена фінансовими даними і аналітикою трафіку. Тому власником дії має бути керівник комерційного напряму, а строком – перші 10 робочих днів для плану диверсифікації. Для B1, якщо довіра середня, перша дія – триангуляція за щонайменше двома незалежними джерелами протягом 48 годин. Повторне обчислення S через один цикл моніторингу показує, чи дії зменшують ризик, чи лише змінюють його метрику.

Управлінське впровадження та обмеження

Впровадження доцільно проводити поетапно. На першому етапі підприємство формулює 3–5 пріоритетних питань безпеки, створює реєстр джерел і карту правових підстав. На другому – запускає мінімальний набір індикторів без передчасної автоматизації всіх каналів. На третьому – валідує хибні та пропущені сигнали, калібрує пороги і закріплює SLA реагування. Лише після цього доцільними є машинне навчання для прогнозу і потокова автоматизація.

Мінімальний управлінський паспорт індиктора має містити: код і назву; бізнес-питання; визначення і формулу; джерело і правову підставу; періодичність; опорні межі; власника даних; власника реакції; строк; правило ескалації; історію змін. Без цього дашборд вимірює середовище, але не створює керованого процесу.

Обмеження запропонованого підходу є суттєвими. По-перше, модель не пройшла емпіричної валідації, тому не доведено її впливу на фінансову стійкість чи частку ринку. По-друге, адитивна згортка може компенсувати критичне значення одного блоку сприятливими значеннями інших; тому для критичних індикторів потрібне додаткове правило вето. По-третє, цифрові джерела можуть змінювати умови доступу, а платформені алгоритми – структуру видимості. По-четверте, якість текстових моделей залежить від мови, домену і появи нових тем. По-п'яте, помилкова кваліфікація загрози може сама спричинити втрати через неадекватну реакцію.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У статті цифрову маркетингову розвідку визначено не як синонім вебаналітики чи моніторингу конкурентів, а як безперервний законний та етичний процес перетворення цифрових ринкових сигналів на перевірені оцінки можливостей і загроз для рішень у системі конкурентної

безпеки. Операційну відмінність запропонованого підходу становить ланцюг «індикатор – поріг – власник – дія – зворотний зв'язок».

Основними результатами є: уточнення меж ЦМР відносно маркетингових досліджень, маркетингової аналітики, BI і ширшої конкурентної розвідки; п'ятирівнева архітектура замкненого циклу; шість блоків індикторів; метод нормування і агрегування; розділення оцінки загрози та довіри до даних; матриця реагування. Умовний приклад підтвердив арифметичну узгодженість моделі, але не її зовнішню валідність.

Практична цінність полягає в можливості запустити ЦМР з мінімального набору джерел і поступово розвивати її за фактичною цінністю сигналів. Пріоритетом мають бути не кількість дашбордів і складність алгоритму, а якість даних, швидкість верифікації, однозначна відповідальність і навчання на наслідках рішень.

Перспективи подальших досліджень охоплюють лонгітюдну валідацію на даних підприємств різних галузей; оцінку прогнозної сили індикторів; порівняння методів зважування; бектестинг порогів; дослідження вартості хибних тривог; аудит упередженості моделей; розроблення галузевих еталонів. Лише після такої валідації можна обґрунтовано судити про каузальний вплив ЦМР на конкурентну безпеку.

ЛІТЕРАТУРА:

1. Dishman P. L., Calof J. L. Competitive intelligence: a multiphasic precedent to marketing strategy. European Journal of Marketing. 2008. Vol. 42, No. 7/8. P. 766–785. DOI: https://doi.org/10.1108/03090560810877141

2. Calof J. L., Wright S. Competitive intelligence: A practitioner, academic and inter-disciplinary perspective. European Journal of Marketing. 2008. Vol. 42, No. 7/8. P. 717–730. DOI: https://doi.org/10.1108/03090560810877114

3. Bose R. Competitive intelligence process and tools for intelligence analysis. Industrial Management & Data Systems. 2008. Vol. 108, No. 4. P. 510–528. DOI: https://doi.org/10.1108/02635570810868362

4. Cavallo A., Sanasi S., Ghezzi A., Rangone A. Competitive intelligence and strategy formulation: connecting the dots. Competitiveness Review. 2021. Vol. 31, No. 2. P. 250–275. DOI: https://doi.org/10.1108/CR-01-2020-0009

5. Kannan P. K., Li H. Digital marketing: A framework, review and research agenda. International Journal of Research in Marketing. 2017. Vol. 34, No. 1. P. 22–45. DOI: https://doi.org/10.1016/j.ijresmar.2016.11.006

6. Wedel M., Kannan P. K. Marketing Analytics for Data-Rich Environments. Journal of Marketing. 2016. Vol. 80, No. 6. P. 97–121. DOI: https://doi.org/10.1509/jm.15.0413

7. Cao G., Duan Y., El Banna A. A dynamic capability view of marketing analytics: Evidence from UK firms. Industrial Marketing Management. 2019. Vol. 76. P. 72–83. DOI: https://doi.org/10.1016/j.indmarman.2018.08.002

8. Hossain M. A., Agnihotri R., Rushan M. R. I., Rahman M. S., Sumi S. F. Marketing analytics capability, artificial intelligence adoption, and firms' competitive advantage: Evidence from the manufacturing industry. Industrial Marketing Management. 2022. Vol. 106. P. 240–255. DOI: https://doi.org/10.1016/j.indmarman.2022.08.017

9. Hassani A., Mosconi E. Social media analytics, competitive intelligence, and dynamic capabilities in manufacturing SMEs. Technological Forecasting and Social Change. 2022. Vol. 175. Art. 121416. DOI: https://doi.org/10.1016/j.techfore.2021.121416

10. Ram J., Zhang C. Examining the Role of Social Media Analytics in Providing Competitive Intelligence: The Impacts and Limitations. Journal of Global Information Management. 2021. Vol. 29, No. 6. P. 1–18. DOI: https://doi.org/10.4018/JGIM.20211101.oa15

11. Ju X. A social media competitive intelligence framework for brand topic identification and customer engagement prediction. PLOS ONE. 2024. Vol. 19, No. 11. e0313191. DOI: https://doi.org/10.1371/journal.pone.0313191

12. Cadden T., Weerawardena J., Cao G., Duan Y., McIvor R. Examining the role of big data and marketing analytics in SMEs innovation and competitive advantage: A knowledge integration perspective. Journal of Business Research. 2023. Vol. 168. Art. 114225. DOI: https://doi.org/10.1016/j.jbusres.2023.114225

13. Davenport T., Guha A., Grewal D., Bressgott T. How artificial intelligence will change the future of marketing. Journal of the Academy of Marketing Science. 2020. Vol. 48, No. 1. P. 24–42. DOI: https://doi.org/10.1007/s11747-019-00696-0

14. Holsapple C. W., Hsiao S.-H., Pakath R. Business social media analytics: Characterization and conceptual framework. Decision Support Systems. 2018. Vol. 110. P. 32–45. DOI: https://doi.org/10.1016/j.dss.2018.03.004

15. Stieglitz S., Mirbabaie M., Ross B., Neuberger C. Social media analytics – Challenges in topic discovery, data collection, and data preparation. International Journal of Information Management. 2018. Vol. 39. P. 156–168. DOI: https://doi.org/10.1016/j.ijinfomgt.2017.12.002

16. Gandomi A., Haider M. Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management. 2015. Vol. 35, No. 2. P. 137–144. DOI: https://doi.org/10.1016/j.ijinfomgt.2014.10.007

17. Wamba S. F., Gunasekaran A., Akter S., Ren S. J.-F., Dubey R., Childe S. J. Big data analytics and firm performance: Effects of dynamic capabilities. Journal of Business Research. 2017. Vol. 70. P. 356–365. DOI: https://doi.org/10.1016/j.jbusres.2016.08.009

18. Teece D. J. Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance. Strategic Management Journal. 2007. Vol. 28, No. 13. P. 1319–1350. DOI: https://doi.org/10.1002/smj.640

19. Чайковська І., Закрижевська І., Карпенко В. Інструментальне забезпечення маркетингової складової економічної безпеки підприємства в умовах цифрової трансформації бізнесу. Herald of Khmelnytskyi National University. Economic sciences. 2025. Vol. 338, No. 1. P. 101–107. DOI: https://doi.org/10.31891/2307-5740-2025-338-14

20. Савченко О. Маркетингові аспекти в системі забезпечення економічної безпеки бізнесу. Herald of Khmelnytskyi National University. Economic sciences. 2025. Vol. 338, No. 1. P. 296–303. DOI: https://doi.org/10.31891/2307-5740-2025-338-44

21. Закусило В., Гавловська Н. Механізм забезпечення економічної безпеки промислових підприємств на основі маркетингових інновацій. Herald of Khmelnytskyi National University. Economic sciences. 2025. Vol. 348, No. 6. P. 33–38. DOI: https://doi.org/10.31891/2307-5740-2025-348-6-4

22. Сороківська О., Кужда Т., Кіналь Н. Цифрові ризики та інформаційна безпека корпоративного сектору. Herald of Khmelnytskyi National University. Economic sciences. 2025. Vol. 342, No. 3(1). P. 95–105. DOI: https://doi.org/10.31891/2307-5740-2025-342-3(1)-14

23. Гармаш О., Марчук В., Федоренко Т. Формування системи індикаторів економічної безпеки підприємства в умовах інтелектуалізації логістичних послуг: корпоративно-управлінський аспект. Herald of Khmelnytskyi National University. Economic sciences. 2026. Vol. 356, No. 4. P. 146–161. DOI: https://doi.org/10.31891/2307-5740-2026-356-21

24. Чайковська І. Цифрові технології як драйвер підвищення ефективності маркетингових комунікацій. Herald of Khmelnytskyi National University. Economic sciences. 2026. Vol. 350, No. 1. P. 153–158. DOI: https://doi.org/10.31891/2307-5740-2026-350-19

REFERENCES

1. Dishman, P. L., & Calof, J. L. (2008). Competitive intelligence: A multiphasic precedent to marketing strategy. European Journal of Marketing, 42(7/8), 766–785. https://doi.org/10.1108/03090560810877141

2. Calof, J. L., & Wright, S. (2008). Competitive intelligence: A practitioner, academic and inter-disciplinary perspective. European Journal of Marketing, 42(7/8), 717–730. https://doi.org/10.1108/03090560810877114

3. Bose, R. (2008). Competitive intelligence process and tools for intelligence analysis. Industrial Management & Data Systems, 108(4), 510–528. https://doi.org/10.1108/02635570810868362

4. Cavallo, A., Sanasi, S., Ghezzi, A., & Rangone, A. (2021). Competitive intelligence and strategy formulation: Connecting the dots. Competitiveness Review, 31(2), 250–275. https://doi.org/10.1108/CR-01-2020-0009

5. Kannan, P. K., & Li, H. (2017). Digital marketing: A framework, review and research agenda. International Journal of Research in Marketing, 34(1), 22–45. https://doi.org/10.1016/j.ijresmar.2016.11.006

6. Wedel, M., & Kannan, P. K. (2016). Marketing analytics for data-rich environments. Journal of Marketing, 80(6), 97–121. https://doi.org/10.1509/jm.15.0413

7. Cao, G., Duan, Y., & El Banna, A. (2019). A dynamic capability view of marketing analytics: Evidence from UK firms. Industrial Marketing Management, 76, 72–83. https://doi.org/10.1016/j.indmarman.2018.08.002

8. Hossain, M. A., Agnihotri, R., Rushan, M. R. I., Rahman, M. S., & Sumi, S. F. (2022). Marketing analytics capability, artificial intelligence adoption, and firms' competitive advantage: Evidence from the manufacturing industry. Industrial Marketing Management, 106, 240–255. https://doi.org/10.1016/j.indmarman.2022.08.017

9. Hassani, A., & Mosconi, E. (2022). Social media analytics, competitive intelligence, and dynamic capabilities in manufacturing SMEs. Technological Forecasting and Social Change, 175, 121416. https://doi.org/10.1016/j.techfore.2021.121416

10. Ram, J., & Zhang, C. (2021). Examining the role of social media analytics in providing competitive intelligence: The impacts and limitations. Journal of Global Information Management, 29(6), 1–18. https://doi.org/10.4018/JGIM.20211101.oa15

11. Ju, X. (2024). A social media competitive intelligence framework for brand topic identification and customer engagement prediction. PLOS ONE, 19(11), e0313191. https://doi.org/10.1371/journal.pone.0313191

12. Cadden, T., Weerawardena, J., Cao, G., Duan, Y., & McIvor, R. (2023). Examining the role of big data and marketing analytics in SMEs innovation and competitive advantage: A knowledge integration perspective. Journal of Business Research, 168, 114225. https://doi.org/10.1016/j.jbusres.2023.114225

13. Davenport, T., Guha, A., Grewal, D., & Bressgott, T. (2020). How artificial intelligence will change the future of marketing. Journal of the Academy of Marketing Science, 48(1), 24–42. https://doi.org/10.1007/s11747-019-00696-0

14. Holsapple, C. W., Hsiao, S.-H., & Pakath, R. (2018). Business social media analytics: Characterization and conceptual framework. Decision Support Systems, 110, 32–45. https://doi.org/10.1016/j.dss.2018.03.004

15. Stieglitz, S., Mirbabaie, M., Ross, B., & Neuberger, C. (2018). Social media analytics – Challenges in topic discovery, data collection, and data preparation. International Journal of Information Management, 39, 156–168. https://doi.org/10.1016/j.ijinfomgt.2017.12.002

16. Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management, 35(2), 137–144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007

17. Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J.-F., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. Journal of Business Research, 70, 356–365. https://doi.org/10.1016/j.jbusres.2016.08.009

18. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. Strategic Management Journal, 28(13), 1319–1350. https://doi.org/10.1002/smj.640

19. Chaikovska, I., Zakryzhevska, I., & Karpenko, V. (2025). Instrumentalne zabezpechennia marketynhovoi skladovoi ekonomichnoi bezpeky pidpryiemstva v umovakh tsyfrovoi transformatsii biznesu [Instrumental support for the marketing component of enterprise economic security in the conditions of digital business transformation]. Herald of Khmelnytskyi National University. Economic sciences, 338(1), 101–107. https://doi.org/10.31891/2307-5740-2025-338-14 [in Ukrainian].

20. Savchenko, O. (2025). Marketynhovi aspekty v systemi zabezpechennia ekonomichnoi bezpeky biznesu [Marketing aspects in the system of ensuring business economic security]. Herald of Khmelnytskyi National University. Economic sciences, 338(1), 296–303. https://doi.org/10.31891/2307-5740-2025-338-44 [in Ukrainian].

21. Zakusylo, V., & Havlovska, N. (2025). Mekhanizm zabezpechennia ekonomichnoi bezpeky promyslovykh pidpryiemstv na osnovi marketynhovykh innovatsii [Mechanism for ensuring economic security of industrial enterprises based on marketing innovations]. Herald of Khmelnytskyi National University. Economic sciences, 348(6), 33–38. https://doi.org/10.31891/2307-5740-2025-348-6-4 [in Ukrainian].

22. Sorokivska, O., Kuzhda, T., & Kinal, N. (2025). Tsyfrovi ryzyky ta informatsiina bezpeka korporatyvnoho sektoru [Digital risks and information security of the corporate sector]. Herald of Khmelnytskyi National University. Economic sciences, 342(3(1)), 95–105. https://doi.org/10.31891/2307-5740-2025-342-3(1)-14 [in Ukrainian].

23. Harmash, O., Marchuk, V., & Fedorenko, T. (2026). Formuvannia systemy indykatoriv ekonomichnoi bezpeky pidpryiemstva v umovakh intelektualizatsii lohistychnykh posluh: korporatyvno-upravlinskyi aspekt [Formation of a system of enterprise economic security indicators under the intellectualization of logistics services: A corporate governance aspect]. Herald of Khmelnytskyi National University. Economic sciences, 356(4), 146–161. https://doi.org/10.31891/2307-5740-2026-356-21 [in Ukrainian].

24. Chaikovska, I. (2026). Tsyfrovi tekhnolohii yak draiver pidvyshchennia efektyvnosti marketynhovykh komunikatsii [Digital technologies as a driver for improving the effectiveness of marketing communications]. Herald of Khmelnytskyi National University. Economic sciences, 350(1), 153–158. https://doi.org/10.31891/2307-5740-2026-350-19 [in Ukrainian].

DIGITAL MARKETING INTELLIGENCE IN THE ENTERPRISE COMPETITIVE SECURITY SYSTEM

HARMASH Oleh[1], FOROSTOVETS Alona[2]
[1] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (Ukraine), Kyiv, Ukraine
https://orcid.org/0000-0003-4324-4411
e-mail: o.harmash.kpi@gmail.com
[2] HEI "Open International University of Human Development "Ukraine"
https://orcid.org/0000-0003-2741-1953
e-mail: akinterdep@ukr.net

The article develops a conceptual and methodological framework for integrating digital marketing intelligence into an enterprise competitive security system. The study addresses a managerial gap: firms accumulate large volumes of digital traces about customers, competitors, channels and platforms, yet these data are often used for campaign reporting rather than for early detection of competitive threats and coordinated response. The research applies a systems approach, a structured synthesis of peer-reviewed studies on competitive intelligence, digital marketing, marketing analytics, social media analytics and dynamic capabilities, comparative analysis, indicator normalization, additive aggregation and scenario modelling. Digital marketing intelligence is defined as a lawful, ethical and continuous process of collecting, validating, integrating, analysing and communicating digital market signals to identify competitive opportunities and threats and to support timely security decisions. A five-layer architecture is proposed: digital signal sources; data governance and quality control; analytical transformation; threat indicators and early-warning rules; decision, action and feedback. The framework distinguishes digital marketing intelligence from episodic marketing research, routine marketing analytics, business intelligence and broader competitive intelligence. Six indicator blocks are specified: competitors' strategic activity; price and assortment pressure; digital visibility; customer and reputational vulnerability; channel and platform resilience; and intelligence-process effectiveness. Risk-oriented and protective indicators are normalized on a common scale; block risks are aggregated into an integral competitive-threat score, while a separate data-confidence coefficient prevents uncertain evidence from being interpreted as precise knowledge. A hypothetical calculation demonstrates how the model prioritizes platform dependence and intensified competitor activity and links them to named response owners and review deadlines. All numerical inputs in the demonstration are illustrative and do not represent a real enterprise. The

scientific contribution is an operational link between marketing analytics and competitive-security management through the control chain "indicator – threshold – owner – action – feedback" and an explicit separation of threat level from evidence confidence. Practical implications include a phased implementation roadmap for enterprises with different levels of digital maturity. The framework requires sector-specific calibration, legal review of data collection practices and empirical validation on longitudinal enterprise data.

Keywords: digital marketing intelligence; competitive security; enterprise economic security; marketing analytics; competitive intelligence; digital signals; early warning; threat indicators; data quality.