ISSN (Print) 2307-2318 ISSN (online) 2707-9899

*DOI 10.31558/2307-2318.2026.2.18*

УДК 339.138:004.056
JELClassification: M31; M15; L81

**Присіч А.В.**
аспірант,
Донецький національний університет імені Василя Стуса
ORCID: 0009-0004-1369-8193
E-mail: a.prysich@donnu.edu.ua

## ЦИФРОВИЙ МАРКЕТИНГ ТА КІБЕРБЕЗПЕКА ЯК СТРАТЕГІЧНІ КОМПОНЕНТИ ДИДЖИТАЛ-МЕХАНІЗМУ УПРАВЛІННЯ ПІДПРИЄМСТВОМ

У статті досліджено роль цифрового маркетингу та кібербезпеки як стратегічних компонентів диджитал-механізму управління підприємством. Обґрунтовано, що цифровий маркетинг виходить за межі традиційного просування і стає системним джерелом поведінкових даних для аналітичних та прогнозних моделей управління. Систематизовано ключові фактори розвитку цифрового маркетингу та їх вплив на формування інформаційної бази для прийняття управлінських рішень. Здійснено порівняльний аналіз ефективності цифрових маркетингових каналів за показниками ROMI та CAC. Визначено, що email-маркетинг залишається найбільш ефективним каналом за ROMI (4200%), а його автоматизація є прикладом повної інтеграції маркетингу з управлінським механізмом. Досліджено інструменти автоматизації маркетингу та нові формати контенту. Проаналізовано кібербезпеку як наскрізний стратегічний компонент диджитал-механізму. На основі NIST Cybersecurity Framework систематизовано відповідність функцій безпеки кожному рівню архітектури механізму. Класифіковано основні типи кіберзагроз та порівняно моделі організації Security Operations Center. Встановлено, що ML-моделі кіберзахисту скорочують час виявлення загроз з 204 днів до 15–20 хвилин. Проаналізовано специфіку функціонування цифрового маркетингу та кібербезпеки в українському бізнесі в умовах воєнного стану та зростання кібератак.

***Ключові слова:*** цифровий маркетинг, кібербезпека, диджитал-механізм управління, автоматизація маркетингу, маркетингова аналітика, ROMI, NIST Cybersecurity Framework, Zero Trust, SOC, CRM-система.

Табл. - 5, Літ. - 16.

**Prysich A.**
Postgraduate,
Vasyl Stus Donetsk National University
ORCID: 0009-0004-1369-8193
E-mail: a.prysich@donnu.edu.ua

## DIGITAL MARKETING AND CYBERSECURITY AS STRATEGIC COMPONENTS OF THE DIGITAL MANAGEMENT MECHANISM OF AN ENTERPRISE

The article examines the role of digital marketing and cybersecurity as strategic components of the digital management mechanism of an enterprise. It is substantiated that digital marketing goes beyond traditional promotion and becomes a systemic source of behavioural data for analytical and predictive management models. The key factors of digital

marketing development and their impact on forming the information base for management decisions are systematized. A comparative analysis of the effectiveness of digital marketing channels by ROMI and CAC indicators has been carried out. It is determined that email marketing remains the most effective channel in terms of ROMI (4200%), and its automation is an example of full integration of marketing with the management mechanism. Cybersecurity is analysed as a cross-cutting strategic component of the digital management mechanism. Based on the NIST Cybersecurity Framework, the correspondence of security functions to each level of the mechanism architecture is systematized. The main types of cyber threats are classified and Security Operations Center organizational models are compared. It is established that ML-based cyber defence models reduce threat detection time from 204 days to 15–20 minutes. The specifics of digital marketing and cybersecurity functioning in Ukrainian business under martial law and increasing cyberattacks are analysed.

***Keywords:*** digital marketing, cybersecurity, digital governance, marketing automation, marketing analytics, ROMI, NIST Cybersecurity Framework, Zero Trust, SOC, CRM system

Tab. – 5. Ref. - 16.

**Постановка проблеми:** В умовах стрімкого розвитку цифрових технологій управління підприємством зазнає глибинних структурних змін. Цифровий маркетинг перетворюється з інструменту просування продуктів на системне джерело даних, що інтегрується в управлінські процеси підприємства та живить аналітичні й прогнозні моделі прийняття рішень. Водночас зростаюча цифровізація неминуче підвищує вразливість компаній до кіберзагроз: за даними IBM Security (2023), середня вартість витоку даних у світі досягла рекордних $4.45 млн. Проте значна частина українських компаній, зокрема у ритейлі, впроваджує маркетингові digital-інструменти фрагментарно, без інтеграції з аналітичними системами управління, а кібербезпеку розглядає як допоміжну ІТ-функцію, а не як стратегічний компонент. Це призводить до того, що масиви даних про поведінку клієнтів залишаються невикористаними для стратегічного планування, а порушення кібербезпеки на будь-якому рівні здатне паралізувати весь управлінський механізм. Особливої гостроти ця проблема набуває в умовах воєнного стану, коли кількість кібератак зросла у 3–5 разів, а поведінка споживча стала значно більш мінливою. Тому постає необхідність дослідження цифрового маркетингу та кібербезпеки як взаємопов’язаних стратегічних компонентів диджитал-механізму управління підприємством.

**Аналіз останніх досліджень та публікацій.** Теоретичні засади цифрового маркетингу досліджено у працях Котлера Ф., Картаджайї Г. та Сетіавана І. [1], які обґрунтували концепцію маркетингу 5.0, заснованого на штучному інтелекті, обробці природної мови, IoT та доповненій реальності. Новак Т. П. та Гофман Д. Л. [2] розвинули концепцію data-driven маркетингу, де кожне маркетингове рішення базується на аналізі поведінкових даних клієнтів у реальному часі. Чаффі Д. та Елліс-Чедвік Ф. [3] систематизували метрики ефективності цифрового маркетингу за рівнями маркетингової воронки: від охоплення (reach, impressions) до утримання (LTV, NPS). Кумар В. та Рейнартц В. [4] обґрунтували CLV-орієнтований підхід, де маркетингові дії оцінюються за впливом на довічну цінність клієнта. Пулліці Дж. та Роуз Р. [5] дослідили контент-маркетинг як стратегічний інструмент побудови довгострокових відносин з клієнтами.

У сфері кібербезпеки методологічну основу становлять роботи Холла Дж. К. [6], який обґрунтував кіберризик як одну з найбільш недооцінених категорій операційного ризику. Фреймворк NIST Cybersecurity Framework [6] систематизує практики кіберзахисту у п’ять функцій: Identify, Protect, Detect, Respond, Recover. Бучак А. Л. та

Гувен Е. [7] систематизували методи ML для кіберзахисту, а Сін Ю. та ін. [8] встановили, що глибоке навчання показує точність виявлення кібератак 98–99.5%, що значно перевищує традиційні rule-based підходи (70–85%).

Серед вітчизняних дослідників варто відзначити роботи Обіхода С. В. [9] щодо впровадження ІКТ у систему управління бізнес-процесами, Гринька П. Л. [10] з аналізу цифрової трансформації бізнесу в Україні, Боднаря Д. та Семенюка С. [11] щодо конкурентоспроможності підприємств в умовах цифрової економіки, Тарасенко І. О. та Гавриленко Н. Г. [12] з дослідження тенденцій цифровізації, Лазебник Л. та Войтенко В. [13] щодо інформаційної інфраструктури як бази цифрової трансформації, а також Устенко М. та Руських А. [14] з аналізу діджиталізації як основи конкурентоспроможності.

Попри цінність зазначених досліджень, у них недостатньо висвітлено питання інтеграції цифрового маркетингу та кібербезпеки як взаємопов'язаних компонентів єдиного управлінського механізму. Більшість праць фокусуються або на окремих інструментах цифровізації, або на загальних трендах, проте не охоплюють логіку їх інтеграції у єдину стратегічну рамку. Це створює дослідницьку нішу, яку покликана заповнити дана стаття.

**Метою статті** є обґрунтування ролі цифрового маркетингу та кібербезпеки як стратегічних компонентів диджитал-механізму управління підприємством на основі систематизації інструментів, каналів та метрик цифрового маркетингу, класифікації кіберзагроз, аналізу моделей кіберзахисту та побудови концептуальної моделі їх інтеграції з п'ятирівневою архітектурою управлінського механізму. У межах дослідження узагальнено міжнародний і вітчизняний досвід, визначено специфіку функціонування маркетингу та кібербезпеки в умовах воєнного стану.

**Виклад основного матеріалу.** Цифровий маркетинг являє собою використання цифрових каналів, платформ та технологій для просування продуктів та взаємодії з клієнтами. Принципова відмінність від традиційного маркетингу полягає у вимірюваності: кожна дія у цифровому середовищі фіксується в реальному часі, формуючи масив даних про поведінку споживачів. Котлер Ф., Картаджайа Г. та Сетіаван І. [1] визначили п'ять ключових технологій, що трансформують маркетинг: штучний інтелект (AI), обробку природної мови (NLP), сенсори та IoT, робототехніку та доповнену/віртуальну реальність (AR/VR). Автори обґрунтували, що маркетинг 5.0 передбачає застосування технологій для створення, комунікації, доставки та підвищення цінності протягом усього шляху клієнта (customer journey).

Серед ключових чинників, що сформували сучасний цифровий маркетинг, виділяють технологічні, поведінкові, аналітичні та регуляторні (табл. 1).

Аналіз факторів (табл. 1) свідчить, що сучасний цифровий маркетинг формується під впливом п'яти взаємопов'язаних чинників. Технологічний та поведінковий чинники визначають канали комунікації, аналітичний забезпечує персоналізацію та вимірюваність, а регуляторний задає межі збору та використання даних. Для диджитал-механізму управління це означає, що кожен маркетинговий канал генерує дані, а кожна взаємодія клієнта є точкою збору інформації для аналітичного рівня архітектури.

Новак Т. П. та Гофман Д. Л. [2] обґрунтували концепцію data-driven маркетингу, виділивши три рівні його зрілості: описовий (аналіз того, що відбулося, через звіти про продажі та конверсії), предиктивний (прогнозування LTV клієнтів, churn prediction) та прескриптивний (автоматичні рекомендації щодо персоналізації). Ці рівні кореспондуються з рівнями аналітичної зрілості і підтверджують, що маркетинг є одним з перших бізнес-доменів, де повна інтеграція з диджитал-механізмом дає

вимірюваний ефект.

Таблиця 1 - Ключові фактори розвитку цифрового маркетингу

| **Фактор** | **Ключові тренди** | **Інструменти** | **Вплив на бізнес** |
|---|---|---|---|
| Поширення інтернету | 5+ млрд користувачів, 4G/5G | Mobile-first дизайн, мобільні додатки | Глобальне охоплення аудиторії |
| Соціальні мережі | Facebook, Instagram, TikTok | Таргетована реклама, інфлюенсери | Побудова бренду, пряма комунікація |
| Аналітика та автоматизація | Big Data, AI-алгоритми | Google Analytics, HubSpot, Marketo | Оптимізація ROI та персоналізація |
| Нові формати контенту | Відео, VR/AR, подкасти | YouTube, TikTok, AR-додатки | Захопливий досвід користувача |
| Етика та прозорість | GDPR, CCPA, кібербезпека | Consent Management, DPO | Довіра та лояльність клієнтів |

*Джерело: систематизовано автором.*

Автоматизація маркетингових процесів є ключовим елементом інтеграції маркетингу з управлінським механізмом. Якщо аналітичний рівень генерує рішення — наприклад, відправити персональну знижку клієнту з CLV > 5000 грн — то маркетингова автоматизація виконує це рішення без участі людини: надсилає email, push-повідомлення або таргетовану рекламу. Наступний рівень автоматизації — використання ML-алгоритмів, що самонавчаються на даних попередніх кампаній та автоматично оптимізують ставки, аудиторії та контент. AI-алгоритми дозволяють передбачати поведінку споживачів, рекомендувати продукти та персоналізувати взаємодію.

Для прийняття рішень щодо розподілу маркетингового бюджету між каналами необхідно знати ефективність кожного з них. Порівняння ефективності каналів за показниками ROMI, охоплення та конверсії наведено у табл. 2.

Таблиця 2 - Ефективність цифрових маркетингових каналів у ритейлі

| **Канал** | **Середній ROMI** | **CAC** | **Переваги** | **Обмеження** |
|---|---|---|---|---|
| Email-маркетинг | 4200% | $1–3 | Найвищий ROMI, персоналізація, автоматизація | Спам-фільтри, зниження open rate |
| SEO | 2200% | $5–15 | Довгостроковий ефект, високий trust | Довгий час до результату (3–6 міс) |
| Контекстна реклама (PPC) | 200% | $10–30 | Миттєвий трафік, таргетинг | Зупиняється при зупинці бюджету |
| SMM (соцмережі) | 150–300% | $8–20 | Engagement, brand awareness, UGC | Алгоритмічні зміни, залежність від платформ |
| Інфлюенсер-маркетинг | 500–800% | $5–25 | Довіра аудиторії, нішевий таргетинг | Ризик репутації, вимірюваність |

*Джерело: узагальнено автором на основі даних Litmus (2023), HubSpot (2024) [2, 3].*

Аналіз ефективності каналів засвідчує, що email-маркетинг залишається найбільш ефективним з точки зору ROMI ($42 повернення на кожен $1 витрачений), що пояснюється низькою вартістю відправки та високою персоналізацією через CRM-інтеграцію. У контексті диджитал-механізму email-маркетинг є прикладом рівня автоматизації: тригерні ланцюги листів (welcome series, abandoned cart, re-engagement) виконуються автоматично на основі поведінкових даних клієнта з CRM-системи, без участі маркетолога.

Окремо слід дослідити роль контент-маркетингу як стратегічного інструменту побудови довгострокових відносин з клієнтами. Пулліці Дж. та Роуз Р. [5] обґрунтували, що компанії, які інвестують у контент-маркетинг, отримують у 6 разів вищий рівень конверсії порівняно з тими, хто використовує лише традиційну рекламу. У ритейлі прикладом ефективного контент-маркетингу є тематичні супермаркети, кулінарні блоги, рецепти в мобільних додатках — все це створює емоційний зв'язок з брендом та генерує органічний трафік без прямих рекламних витрат.

Кумар В. та Рейнартц В. [4] обґрунтували CLV-орієнтований підхід до маркетингу, де кожна маркетингова дія оцінюється не за короткостроковим ефектом, а за впливом на довічну цінність клієнта (Customer Lifetime Value). У диджитал-механізмі CLV є одним з ключових показників рівня підтримки рішень: управлінець бачить на дашборді не лише поточні продажі, а й прогнозний CLV кожного клієнтського сегменту, що дозволяє оптимально розподіляти маркетинговий бюджет між каналами залучення та утримання клієнтів.

Персоналізація маркетингових комунікацій на основі ML-моделей є одним з найбільш перспективних напрямків інтеграції маркетингу з диджитал-механізмом. За даними McKinsey [15], компанії, що впроваджують персоналізацію на основі AI, збільшують виручку на 10–15% та підвищують ефективність маркетингових витрат на 10–30%. Для великих ритейлерів із масштабними програмами лояльності персоналізація реалізується через рекомендаційні системи на основі collaborative filtering, динамічні персональні знижки на основі purchase history та CLV-прогнозу, персоналізовані push-повідомлення з урахуванням часу, локації та контексту.

Вплив соціальних мереж на репутаційне управління компанією є ще одним аспектом інтеграції маркетингу з диджитал-механізмом. Аналіз тональності (sentiment analysis) публікацій у соціальних мережах є раннім індикатором репутаційних ризиків та змін у клієнтській лояльності [16]. У контексті диджитал-механізму sentiment analysis інтегрується з моделлю управління ризиками: негативний тренд у тональності згадок бренду автоматично генерує сигнал для менеджменту на дашборді та ініціює розробку плану реагування.

Для українського ритейлу цифровий маркетинг функціонує в унікальних умовах воєнного стану. Після 24 лютого 2022 року маркетингові комунікації зазнали суттєвих змін: бренди переорієнтувалися з продуктового контенту на соціально відповідальний, зросла роль локальних каналів (Viber, Telegram) порівняно з глобальними (Facebook, Instagram), а споживча поведінка стала значно більш волатильною та залежною від ситуативних факторів (міграція, безпекова ситуація, енергетичні обмеження).

Систематизацію взаємозв'язку між каналами цифрового маркетингу та рівнями диджитал-механізму управління наведено у табл. 3. Як свідчить проведений аналіз, цифровий маркетинг інтегрується з усіма п'ятьма рівнями диджитал-механізму, забезпечуючи збір поведінкових даних клієнтів (Рівень 1), їх обробку та сегментацію (Рівень 2), аналітику для прогнозування (Рівень 3), візуалізацію на дашбордах (Рівень 4) та автоматизацію маркетингових комунікацій (Рівень 5). Ця інтеграція підтверджує, що маркетинг не є ізольованою функцією, а органічним компонентом єдиної системи

ISSN (Print) 2307-2318 ISSN (online) 2707-9899

управління.

Таблиця 3 - Інтеграція цифрового маркетингу з диджитал-механізмом управління

| **Маркетинговий канал** | **Дані для механізму** | **Рівень архітектури** | **Використання даних** |
|---|---|---|---|
| CRM / Email | Поведінка клієнтів, сегментація, LTV | Рівень 1 (збір даних) | Прогнозування попиту |
| Програма лояльності | Історія покупок, частота, чек | Рівень 1 (збір даних) | Оптимізація асортименту |
| Web analytics (GA4) | Поведінка на сайті, конверсії | Рівень 2 (обробка) | Ціноутворення |
| SMM analytics | Engagement, sentiment, reach | Рівень 3 (аналітика) | Управління ризиками |
| Programmatic ads | Conversion data, ROAS | Рівень 4 (рішення) | Дашборди для менеджменту |
| Email automation | Тригерні ланцюги, A/B тести | Рівень 5 (автоматизація) | Автоматичні промо-кампанії |

*Джерело: розроблено автором.*

Водночас ефективність диджитал-механізму неможлива без надійного захисту даних, що циркулюють між його рівнями. Кібербезпека є не допоміжним елементом, а структурною умовою функціонування механізму: якщо дані на Рівні 1 скомпрометовані — всі подальші рівні генерують хибні рішення. Холл Дж. К. [6] обґрунтував, що кіберризик є однією з найбільш недооцінених категорій операційного ризику, оскільки його потенційний вплив зростає нелінійно зі збільшенням ступеня цифровізації компанії. За даними IBM Security (2023), середня вартість витоку даних у світі досягла рекордних $4.45 млн. Для ритейлерів цей показник ще вищий: за даними Verizon (2023), роздрібна торгівля є третьою найбільш атакованою галуззю після фінансового сектору та охорони здоров'я.

Найбільш поширеними загрозами залишаються фішингові атаки, ransomware, DDoS-атаки, атаки нульового дня, інсайдерські загрози та атаки на ланцюги постачання. Класифікацію основних типів кіберзагроз з прикладами та методами захисту наведено у табл. 4.

Таблиця 4 -Класифікація основних типів кіберзагроз

| **Тип загрози** | **Опис** | **Приклад** | **Метод захисту** |
|---|---|---|---|
| Фішинг | Обман через підроблені повідомлення | Фальшиві листи від банку | Навчання персоналу, фільтри |
| Ransomware | Шифрування даних з вимогою викупу | WannaCry, NotPetya | Резервне копіювання, оновлення ПЗ |
| DDoS-атаки | Перевантаження серверів запитами | Атаки на держ. сайти України | CDN, WAF, хмарний захист |
| Zero-day | Використання невідомих вразливостей | Exploit до виходу патча | IDS/IPS системи, моніторинг |
| Інсайдерські загрози | Витік даних від працівників | Несанкціоноване копіювання | DLP-системи, контроль доступу |
| Supply chain attacks | Зломи через постачальників ПЗ | SolarWinds attack | Аудит постачальників, Zero Trust |

*Джерело: систематизовано автором на основі [6, 7, 8].*

Для практичної реалізації функцій кіберзахисту у диджитал-механізмі необхідна відповідна організаційна структура. Нею є Security Operations Center (SOC), що забезпечує цілодобовий моніторинг та реагування на інциденти. Існують три основні моделі SOC: внутрішній (in-house — власна команда 5–15 аналітиків), аутсорсинговий (MSSP — Managed Security Service Provider) та гібридний (внутрішня команда + MSSP для 24/7 покриття). Порівняння моделей SOC наведено у табл. 5.

Таблиця 5 - Порівняння моделей організації SOC

| **Модель SOC** | **Вартість/рік** | **Команда** | **Час реакції** | **Рекомендовано для** |
|---|---|---|---|---|
| Внутрішній | $500K–1.5M | 5–15 аналітиків (3 зміни) | 5–15 хвилин | Великий бізнес (>1 млрд грн виручки) |
| Аутсорсинговий (MSSP) | $100K–400K | Зовнішній провайдер | 15–30 хвилин | Середній бізнес (100–500 млн грн) |
| Гібридний | $250K–800K | 2–5 внутрішніх + MSSP 24/7 | 10–20 хвилин | Великий бізнес з оптимізацією витрат |
| Без SOC | $0 (до інциденту) | Відсутня | Дні–тижні | Не рекомендовано для диджитал-механізму |

*Джерело: складено автором на основі даних Gartner (2024).*

Порівняння моделей SOC засвідчує, що варіант «без SOC» є неприйнятним для компанії з диджитал-механізмом управління: час реакції в дні-тижні означає, що кібератака може залишатися невиявленою протягом тривалого часу, завдаючи зростаючих збитків. Для великих ритейлерів вартість гібридного SOC становить менше 0.1% виручки — суттєво менше потенційних втрат від одного серйозного інциденту.

Бучак А. Л. та Гувен Е. [7] систематизували методи ML для кіберзахисту: класифікацію мережевого трафіку, виявлення аномалій через unsupervised learning, прогнозування атак через аналіз патернів. Сін Ю. та ін. [8] встановили, що глибоке навчання показує точність виявлення кібератак на рівні 98–99.5%, що значно перевищує традиційні правила з точністю 70–85%. У контексті диджитал-механізму це означає, що ML-модель виявлення загроз здатна ідентифікувати атаку за 15–20 хвилин (MTTD), порівняно з 204 днями при традиційних методах.

З розвитком хмарних технологій традиційна модель «довіряй, але перевіряй» стала недостатньою. Їй на зміну прийшла концепція Zero Trust (нульова довіра), яка передбачає, що кожен запит має верифікуватися незалежно від його джерела. Для диджитал-механізму, де дані циркулюють між множинними системами (ERP, CRM, WMS, ML-платформи, хмарні сервіси), Zero Trust забезпечує захист на рівні кожного окремого запиту.

Українські реалії диктують свої умови. Державна служба спеціального зв'язку та захисту інформації України зафіксувала зростання кількості кіберінцидентів з 2 194 у 2021 році до понад 6 000 у 2023 році. У відповідь багато українських компаній впровадили захищені хмарні рішення на базі AWS, Azure або GCP із багатофакторною аутентифікацією та шифруванням. Показовим прикладом є Ajax Systems, чия IT-інфраструктура побудована з урахуванням принципів security by default, а також NovaPay, сертифікований за стандартом PCI DSS.

Дослідивши напрацювання Обіхода С. [9], Боднаря Д. [11], Тарасенко І. [12], Лазебник Л. [13] та інших авторів, можна погодитися з тим, що цифровізація впливає не лише на процеси, а й на змістовне наповнення функцій управління. Обіход С. В.

наголошує, що ІКТ є основою управлінських моделей, забезпечуючи гнучкість, інтеграцію даних та оперативний моніторинг. Боднар Д. та Семенюк С. зазначають, що підприємства з CRM та ERP-системами досягають більшої стійкості в умовах нестабільності. Устенко М. та Руських А. [14] пропонують модель багаторівневої цифровізації, де внутрішня автоматизація поєднується з зовнішніми інтеграціями через API та цифрові платформи.

**Висновки.** На основі проведеного аналізу можна зробити висновок, що цифровий маркетинг та кібербезпека є не ізольованими функціями, а взаємопов'язаними стратегічними компонентами диджитал-механізму управління. Маркетинг забезпечує зворотний зв'язок між ринком та системою управління через збір і аналіз поведінкових даних клієнтів, а кібербезпека є «оболонкою», що захищає кожен рівень механізму від зовнішніх та внутрішніх загроз. Порушення безпеки на будь-якому рівні паралізує весь механізм: компрометація рівня збору даних призводить до «отруєння» даних для ML-моделей; злом аналітичного рівня може генерувати помилкові рекомендації; атака на рівень автоматизації може призвести до некоректних автоматичних дій.

У порівнянні з міжнародними практиками, українським компаніям часто бракує інтегрованого підходу. На основі аналізу можна рекомендувати комбінування маркетингових та захисних інструментів у єдину систему, де дані CRM одночасно захищаються згідно з PCI DSS та GDPR, а маркетингова аналітика інтегрується з SIEM-моніторингом для виявлення аномалій у поведінці клієнтів.

Також на основі кейсів українських компаній можна зробити висновок, що цифрова адаптація часто була реактивною (війна, пандемія), а не стратегічно підготовленою. Було б доцільно запровадити регулярний аудит цифрової зрілості компаній із використанням інструментів на кшталт Digital Maturity Assessment, які дозволяють оцінити рівень інтеграції IT-рішень у бізнес-процеси, управління змінами та корпоративну культуру. Слід розглянути можливість створення національного digital-репозиторію ефективних практик цифровізації, який акумулюватиме кейси впровадження ERP, CRM, RPA, AI, SOC тощо. Для прискорення трансформації малого і середнього бізнесу було б доцільно передбачити цільові мікрогранти на цифровізацію базових процесів (облік, логістика, e-commerce, кібербезпека), за аналогією з програмами «єРобота» або EU4Business.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kotler, P., Kartajaya, H., Setiawan, I. (2021). Marketing 5.0: Technology for Humanity. Wiley.
2. Novak, T. P., Hoffman, D. L. (2021). Digital Marketing Strategy. Harvard Business Press.
3. Chaffey, D., Ellis-Chadwick, F. (2022). Digital Marketing. 8th ed. Pearson Education.
4. Kumar, V., Reinartz, W. (2018). Customer Relationship Management: Concept, Strategy, and Tools. 3rd ed. Springer.
5. Pulizzi, J., Rose, R. (2017). Killing Marketing: How Innovative Businesses Are Turning Marketing Cost into Profit. McGraw-Hill.
6. Hall, J. K. (2018). Risk Management and Financial Institutions. 5th ed. Wiley.
7. Buczak, A. L., Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
8. Xin, Y., Kong, L., Liu, Z., et al. (2018). Machine learning and deep learning methods for cybersecurity. IEEE Access, 6, 35365–35381.
9. Обіход С. В. Імплементація інформаційно-комунікаційних технологій у систему

управління бізнес-процесами вітчизняних підприємств у контексті розвитку цифрової економіки. Економіка, управління та адміністрування. 2021. № 4 (98). С. 10–17. DOI: https://doi.org/10.26642/jen-2021-4(98)-10-17
10. Гринько П. Л. Цифрова трансформація бізнесу в умовах розвитку інноваційних процесів в Україні. Бізнес Інформ. 2020. № 3. С. 53–58.
11. Боднар Д., Семенюк С. Конкурентоспроможність підприємства в умовах цифрової економіки. Цифрова економіка як фактор інновацій та сталого розвитку суспільства: матеріали III міжнар. наук.-практ. конф. Тернопіль, 2022. С. 5–7.
12. Тарасенко І. О., Гавриленко Н. Г. Сучасні тенденції цифровізації економіки: проблеми та перспективи розвитку. Міжнародний науковий журнал «Інтернаука». 2021. № 3(47). Т. 1. С. 36–46.
13. Лазебник Л. Л., Войтенко В. О. Інформаційна інфраструктура в цифровізації бізнес-процесів підприємства. Науковий вісник Міжнародного гуманітарного університету. 2020. Вип. 42. С. 18–22. DOI: https://doi.org/10.32841/2413-2675/2020-42-3
14. Устенко М., Руських А. Діджиталізація: основа конкурентоспроможності підприємства в реаліях цифрової економіки. Вісник економіки транспорту і промисловості. 2019. № 68. С. 181–192.
15. McKinsey & Company. (2021). Next in Personalization. URL: https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-value-of-getting-personalization-right-or-wrong-is-multiplying
16. Kitzmiller, C., Wang, T. (2020). Social Media Analytics for Business Intelligence. Journal of Management Information Systems, 37(4), 1020–1049.

**REFERENCES**

1. Kotler, P., Kartajaya, H., & Setiawan, I. (2021). Marketing 5.0: Technology for Humanity. Wiley.
2. Novak, T. P., & Hoffman, D. L. (2021). Digital Marketing Strategy. Harvard Business Press.
3. Chaffey, D., & Ellis-Chadwick, F. (2022). Digital Marketing (8th ed.). Pearson Education.
4. Kumar, V., & Reinartz, W. (2018). Customer Relationship Management: Concept, Strategy, and Tools (3rd ed.). Springer.
5. Pulizzi, J., & Rose, R. (2017). Killing Marketing: How Innovative Businesses Are Turning Marketing Cost into Profit. McGraw-Hill.
6. Hall, J. K. (2018). Risk Management and Financial Institutions (5th ed.). Wiley.
7. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
8. Xin, Y., Kong, L., Liu, Z., et al. (2018). Machine learning and deep learning methods for cybersecurity. IEEE Access, 6, 35365–35381.
9. Obikhod, S. V. (2021). Implementatsiia informatsiino-komunikatsiinykh tekhnolohii u systemu upravlinnia biznes-protsesamy vitchyznianykh pidpryiemstv u konteksti rozvytku tsyfrovoi ekonomiky. Ekonomika, upravlinnia ta administruvannia, 4(98), 10–17. https://doi.org/10.26642/jen-2021-4(98)-10-17
10. Hrynko, P. L. (2020). Tsyfrova transformatsiia biznesu v umovakh rozvytku innovatsiinykh protsesiv v Ukraini. Biznes Inform, 3, 53–58.
11. Bodnar, D., & Semeniuk, S. (2022). Konkurentospromozhnist pidpryiemstva v umovakh tsyfrovoi ekonomiky. In Tsyfrova ekonomika yak faktor innovatsii ta staloho rozvytku suspilstva: materialy III mizhnar. nauk.-prakt. konf. (pp. 5–7). Ternopil.
12. Tarasenko, I. O., & Havrylenko, N. H. (2021). Suchasni tendentsii tsyfrovizatsii

ekonomiky: problemy ta perspektyvy rozvytku. Mizhnarodnyi naukovyi zhurnal "Internauka", 3(47), 1, 36–46.
13. Lazebnyk, L. L., & Voitenko, V. O. (2020). Informatsiina infrastruktura v tsyfrovizatsii biznes-protsesiv pidpryiemstva. Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu, 42, 18–22. https://doi.org/10.32841/2413-2675/2020-42-3
14. Ustenko, M., & Ruskykh, A. (2019). Didzhytalizatsiia: osnova konkurentospromozhnosti pidpryiemstva v realiiakh tsyfrovoi ekonomiky. Visnyk ekonomiky transportu i promyslovosti, 68, 181–192.
15. McKinsey & Company. (2021). Next in Personalization. https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-value-of-getting-personalization-right-or-wrong-is-multiplying
16. Kitzmiller, C., & Wang, T. (2020). Social Media Analytics for Business Intelligence. Journal of Management Information Systems, 37(4), 1020–1049.

*Стаття надійшла до редакції 16.04.2026*
*Стаття прийнята до друку після рецензування 24.04.2026*