



Маркетинг

УДК: 339.138:004.9:658.562

DOI <https://doi.org/10.5281/zenodo.19685529>

Цифрові інструменти маркетингового комплаєнсу в системі ідентифікації та запобігання фальсифікації товарів і послуг

Романюк Надія Василівна

кандидат економічних наук, доцент

Чернівецький національний університет імені Юрія Федьковича

ORCID: <https://orcid.org/0000-0002-9852-3023>

Прийнято: 11.03.2026 | Опубліковано: 30.03.2026

Анотація. У статті досліджено концептуальні та прикладні аспекти цифрового маркетингового комплаєнсу як системного інструменту протидії фальсифікації товарів і послуг в умовах глобальної цифрової трансформації ринків. Розмежовано суміжні поняття: маркетинговий комплаєнс, юридичний комплаєнс та корпоративний комплаєнс; фальсифікація, контрафакція, імітація та сурогат; ідентифікація та запобігання як функціонально відмінні механізми. Визначено місце маркетингового комплаєнсу в структурі маркетинг-міксу та обґрунтовано його наскрізну функцію, що пронизує товарну, цінову, збутову та комунікаційну політику підприємства, формуючи brand trust та репутаційний капітал. Систематизовано типологію фальсифікацій за об'єктом маніпуляції – якісна, кількісна, інформаційна, вартісна – з окремим акцентом на фальсифікації послуг у цифровому середовищі: маніпуляції рейтингами, фіктивні відгуки, ghost services та misrepresentation. Проаналізовано технологічний арсенал ідентифікації фальсифікату: блокчейн-трасування ланцюгів постачання (IBM Food Trust, VeChain, Everledger), IoT-маркери та розумну упаковку (NFC, QR,



RFID), алгоритми штучного інтелекту для виявлення підробок і фейкових відгуків, цифрові паспорти продукту (EU DPP) та платформні рішення захисту брендів. Досліджено превентивні інструменти: RegTech-платформи автоматизації регуляторної перевірки (Veeva Vault PromoMats, Red Marker AI), цифрове маркування, споживчі додатки автентифікації та інтеграцію комплаєнс-інструментів у корпоративні інформаційні системи CRM/ERP/SCM. Особливу увагу приділено українським реаліям: нормативній базі захисту прав споживачів, системі е-акцизу як інструменту цифрової трасованості, ролі GS1 Україна, впливу воєнного стану на зростання ризиків фальсифікації та євроінтеграційним вимогам імплементації регламентів ЄС (GPSR, MSR, EPR). Запропоновано триступеневу модель адаптивного цифрового комплаєнсу для українського бізнесу, диференційовану за рівнем ризику товарної категорії, масштабом підприємства та цільовим ринком збуту.

Ключові слова: маркетинговий комплаєнс; фальсифікація товарів і послуг; цифрові інструменти; маркетингова товарна політика; блокчейн-трасування; розумна упаковка; штучний інтелект; цифровий паспорт продукту; RegTech; експертиза товарів.

Digital tools of marketing compliance in the system of identification and prevention of counterfeiting of goods and services

Romaniuk Nadiia Vasylivna

Candidate of Economic Sciences, Associate Professor

Yuriy Fedkovych Chernivtsi National University

ORCID: <https://orcid.org/0000-0002-9852-3023>

Abstract. *The article examines the conceptual and applied aspects of digital marketing compliance as a systemic tool for combating product and service falsification in the context of global digital market transformation. The study distinguishes adjacent*



concepts: marketing compliance, legal compliance, and corporate compliance; falsification, counterfeiting, imitation, and surrogate; identification and prevention as functionally distinct mechanisms. The place of marketing compliance within the marketing mix structure is determined, and its cross-cutting function spanning product, pricing, distribution, and communication policies is substantiated as a driver of brand trust and reputational capital. A typology of falsifications by manipulation object – qualitative, quantitative, informational, and value-based – is systematized, with particular emphasis on service falsification in the digital environment: rating manipulation, fake reviews, ghost services, and misrepresentation. The technological arsenal for counterfeit identification is analyzed: blockchain-based supply chain traceability (IBM Food Trust, VeChain, Everledger), IoT markers and smart packaging (NFC, QR, RFID), artificial intelligence algorithms for detecting counterfeits and fake reviews, digital product passports (EU DPP), and platform-based brand protection solutions. Preventive instruments are investigated: RegTech platforms for automated regulatory review (Veeva Vault PromoMats, Red Marker AI), digital labeling, consumer authentication applications, and integration of compliance tools into corporate CRM/ERP/SCM systems. Special attention is devoted to Ukrainian realities: the consumer protection regulatory framework, the e-excise system as a digital traceability tool, the role of GS1 Ukraine, the impact of martial law on increased falsification risks, and EU integration requirements for implementing EU regulations (GPSR, MSR, ESPR). A three-tier adaptive digital compliance model for Ukrainian businesses is proposed, differentiated by product category risk level, enterprise scale, and target sales market.

Keywords: *marketing compliance; product and service falsification; digital tools; marketing product policy; blockchain traceability; smart packaging; artificial intelligence; digital product passport; RegTech; product expertise.*

Постановка проблеми. Глобальна торгівля фальсифікованими та контрафактними товарами у 2021 році досягла 467 млрд доларів США, що



становить 2,3 % світового імпорту, а імпорт контрафакту до Європейського Союзу оцінено в 99 млрд євро, або 4,7 % загального обсягу ввезення [1]. Масштаб проблеми засвідчує системну неспроможність традиційних методів контролю (візуальної ідентифікації, паперової сертифікації та вибірових перевірок) протидіяти фальсифікації в умовах глобалізованих ланцюгів постачання. Водночас цифрова трансформація маркетингових систем породила нову інституційну функцію – маркетинговий комплаєнс, що виходить за межі юридичної відповідності й охоплює відповідність товарної, цінової, комунікаційної та збутової політики підприємства нормативним вимогам, стандартам якості та етичним очікуванням ринку. Цифрові інструменти (технологічні рішення для моніторингу, верифікації й трасування продукції) перетворюють комплаєнс із реактивної витратної функції на проактивний механізм захисту бренду та споживача. Актуальність дослідження посилюється в українському контексті: євроінтеграційні зобов'язання, зростання е-комерції та ризики воєнного часу створюють безпрецедентний запит на цифрову інфраструктуру протидії фальсифікаціям.

Аналіз потребує попереднього розмежування суміжних категорій, що часто ототожнюються в науковому дискурсі. Фальсифікація (підміна складу, властивостей, походження товару) відрізняється від контрафакції (порушення прав інтелектуальної власності), імітації (наслідування зовнішніх ознак без прямого обману) та сурогату (заміщення одного продукту іншим, нижчої якості). Ідентифікація фальсифікату (встановлення факту невідповідності) є логічно відмінною від запобігання (превентивних механізмів, що унеможливають або ускладнюють фальсифікацію). Маркетинговий комплаєнс не зводиться ані до юридичного комплаєнсу (regulatory compliance), ані до корпоративного комплаєнсу (corporate governance); він інтегрує обидва виміри, доповнюючи їх ринковою орієнтацією – спрямованістю на побудову довіри споживача та захист конкурентних позицій бренду. Так само цифрові інструменти маркетингу (MarTech) відрізняються від RegTech (технологій регуляторного комплаєнсу) та



SupTech (наглядних технологій регуляторів), хоча на практиці ці категорії дедалі частіше перетинаються [6].

Аналіз останніх досліджень і публікацій. Проблематика маркетингового комплаєнсу та протидії фальсифікації товарів і послуг перебуває на перетині кількох наукових дисциплін (маркетингу, товарознавства, інформаційних технологій та права), що зумовлює фрагментованість дослідницького поля. Довіра до бренду як фундаментальна детермінанта споживчої поведінки обґрунтована метааналізом 50 років емпіричних досліджень, який підтвердив прямий зв'язок brand trust з вартістю капіталу та ринковою стійкістю компанії [5]. Концепцію цифрової довіри споживачів розвинули R. E. Hochstein, C. M. Harmeling та T. Perko [18], довівши її роль у підвищенні ефективності користувацького контенту. Зв'язок між даними, технологіями та регулюванням у контексті RegTech розкрито у роботі L. Grassi та D. Lanfranchi [6], а позитивний вплив RegTech на прибутковість компаній, операційну ефективність та ринкову структуру емпірично підтвердили B. Charoenwong, Z. T. Kowaleski, A. Kwan та A. G. Sutherland [9]. Інституціоналізація цифрового комплаєнсу, за результатами опитування 162 німецьких компаній, відбувається переважно під впливом міметичних та нормативних тисків, що засвідчує добровільну природу його впровадження як конкурентної стратегії [8].

Технологічна складова антиконтрафактного захисту активно розвивається у напрямі блокчейн-трасування. N. C. K. Yiu [2] систематизував архітектурні рішення для ланцюгів постачання; J. Naoum-Sawaya, S. Elhedhli та P. De Carvalho [3] розробили стратегічну модель, що визначає умови економічної доцільності блокчейну для стримування контрафакторів; C.-L. Chen та співавтори [7] запропонували блокчейн-систему управління автентичністю предметів розкоші; W. Lu, Y. Jiang, Z. Chen та X. Ji [14] проаналізували бар'єри впровадження блокчейну в ланцюгах постачання. Суміжну проблему IoT-сенсорних технологій для розумної упаковки в харчовій галузі досліджено у систематичному огляді J. Zuo та співавторів [13]. Повний спектр антиконтрафактних технологій для



індустрії моди (від оптичних міток до нейромережевої ідентифікації) систематизували А. С. Bardari, Е. Bottani, А. Rizzi та L. Tebaldi [12].

Інформаційна фальсифікація, зокрема фейкові відгуки, стала предметом окремого напрямку досліджень, де Р. Hajek, L. Hikkerova та J.-M. Sahut [4] застосували аспект-орієнтований сентимент-аналіз, а D. Zhang, W. Li, B. Niu та С. Wu [17] запропонували підхід на основі глибокого навчання, що враховує поведінкові та текстові ознаки рецензентів. Взаємодію антиконтрафактних технологій та правозастосування проаналізували S. Yao, K. Zhu та R. Yang [15]. Цифровий паспорт продукту (Digital Product Passport) як регуляторний інструмент нового покоління отримав концептуалізацію у працях F. Psarommatidis та G. May [16] (контекст циркулярної економіки) та M. Farooque зі співавторами [10] (стале управління ланцюгами постачання). Протиріччя між цифровими технологіями маркетингу та приватністю споживачів розкрили F. De Keyser, G. Van Noort та S. Kruikemeier [11].

В українському науковому дискурсі Н. Ляпун та Н. Коваленко [19] дослідили ідентифікацію товарів та визначення фальсифікації під час проведення судової товарознавчої експертизи. Т. Князева та співавтори [20] проаналізували маркетингові технології в контексті цифровізації з акцентом на українських тенденціях. С. О. Лебедь та А. С. Немченко [21] узагальнили міжнародний досвід боротьби з фальсифікованими лікарськими засобами. Попри значний доробок, лишається невирішеною проблема комплексного аналізу цифрових інструментів маркетингового комплаєнсу як цілісної системи, що охоплює одночасно ідентифікацію та запобігання фальсифікації і товарів, і послуг у контексті українських євроінтеграційних реалій.

Формулювання цілей статті. Метою статті є концептуальне позиціонування цифрового маркетингового комплаєнсу як системного інструменту ідентифікації та запобігання фальсифікації товарів і послуг, аналіз технологічного арсеналу відповідних рішень (блокчейн-трасування, IoT-маркери, AI-ідентифікація, цифрові паспорти продукту, RegTech-платформи) та



оцінка перспектив їхнього впровадження в Україні з урахуванням євроінтеграційних вимог, воєнних ризиків та інституційних бар'єрів.

Виклад основного матеріалу. Традиційна структура маркетинг-міксу (product, price, place, promotion) розглядає кожен елемент як відносно автономний управлінський блок, тоді як комплаєнс функціонує інакше – як наскрізна координаційна функція, що пронизує всі чотири складові. У вимірі товарної політики (product policy) комплаєнс охоплює управління якістю, стандартизацію, сертифікацію, маркування й захист бренду, тобто аспекти, що безпосередньо визначають відповідність продукту декларованим характеристикам та нормативним вимогам. У ціновій площині комплаєнс забезпечує прозорість ціноутворення й протидію обманним практикам; у збутовій – контроль каналів дистрибуції та запобігання потраплянню фальсифікату в легітимні мережі; у комунікаційній – верифікацію рекламних тверджень, відповідність етикеткової інформації та правдивість відгуків [8, 18]. Якщо припустити, що комплаєнс є лише п'ятим елементом міксу, доданим ззовні, його інтеграційний потенціал залишиться нереалізованим; натомість саме наскрізна природа функції дозволяє формувати системну відповідність на кожному етапі маркетингової діяльності.

Принципова еволюція маркетингового мислення полягає у переході від парадигми compliance as cost (комплаєнс як витрата, що мінімізується) до compliance as value (комплаєнс як джерело цінності). Метааналіз емпіричних досліджень споживчої довіри підтверджує, що brand trust є фундаментальною детермінантою споживчої поведінки й формує репутаційний капітал, що безпосередньо впливає на вартість капіталу компанії та її ринкову стійкість [5]. Компанії, які інвестують у комплаєнс-інфраструктуру, отримують конкурентну перевагу через зниження ризиків відкликання продукції, зменшення штрафних санкцій та підвищення лояльності споживачів. Водночас існує загроза імітаційного комплаєнсу (compliance theatre), коли підприємство формально дотримується процедур, не досягаючи реального зниження ризиків.



Цифровізація комплаєнсу здатна протидіяти цьому явищу, але лише за умови, що технологічні рішення спрямовані на вимірювання outcomes (результатів), а не лише outputs (обсягу виконаних процедур). Інституціоналізація цифрового комплаєнсу, за даними опитування 162 німецьких компаній, відбувається переважно під впливом міметичних та нормативних інституційних тисків, а не примусових, що підтверджує добровільну природу його впровадження як конкурентної стратегії [8]. Це дає підстави стверджувати, що маркетинговий комплаєнс дедалі частіше сприймається бізнесом як стратегічний актив, здатний формувати brand equity, а не як адміністративний тягар.

Концептуальні засади маркетингового комплаєнсу набувають практичного змісту лише у зіставленні з тими загрозами, протидія яким становить його основну функцію, – передусім фальсифікацією товарів і послуг. За об'єктом маніпуляції можна виокремити чотири базові типи фальсифікації: якісну (підміна складу, зниження сортності), кількісну (невідповідність заявленої маси, об'єму), інформаційну (хибне маркування походження, складу, терміну придатності) та вартісну (завищення ціни за рахунок створення хибного уявлення про якість) [19]. Товарна експертиза як механізм ідентифікації фальсифікату охоплює органолептичні, фізико-хімічні та інструментальні методи, проте в умовах масового ринку її пропускна здатність лишається обмеженою. Судова товарознавча, споживча та маркетингова товарна експертиза утворюють тріаду інструментів, що потребує цифрової підтримки для масштабування [19].

Фальсифікація послуг, попри меншу дослідженість порівняно з товарною, набуває критичного значення в умовах платформної економіки. Вона охоплює маніпуляцію рейтингами та відгуками на платформах, підроблені сертифікати й ліцензії, ghost services (послуги, що існують лише у цифровому просторі та зникають після оплати), а також misrepresentation у digital-сервісах. За різними оцінками, від 10 до 42 % онлайн-відгуків на платформах е-комерції є неавтентичними. Маркетингові наслідки фальсифікації виходять далеко за межі



прямих фінансових втрат: 66 % споживачів втрачають довіру до бренду після ненавмисної купівлі підробки, 76 % зменшують частоту покупок, а 27 % попереджають рідних та друзів [5, 18]. Ерозія brand equity має кумулятивний характер: навіть бренди, що не зазнають масового підроблення, потерпають від загального зниження довіри до товарної категорії. Деформація конкурентного середовища проявляється у витісненні добросовісних виробників, оскільки фальсифікатор, не несучи витрат на якість, R&D та комплаєнс, пропонує нижчу ціну і створює хибну цінову референцію. За даними спільного звіту Організації економічного співробітництва та розвитку і Відомства Європейського Союзу з інтелектуальної власності за 2025 рік, контрафакт охоплює вже майже 50 із 96 товарних категорій, причому стрімко зростає частка небезпечних підробок: автозапчастин, медикаментів, косметики, іграшок та харчових продуктів [1].

Описана типологія та масштаби фальсифікації засвідчують нездатність традиційних методів контролю реагувати з належною швидкістю та повнотою, що обґрунтовує звернення до цифрових інструментів ідентифікації. Першою за ступенем технологічної зрілості є blockchain-based traceability – розподілені реєстри, що забезпечують незмінний запис транзакцій ланцюга постачання. Платформа IBM Food Trust на базі Hyperledger Fabric дозволила Walmart скоротити час трасування походження манго з 7 днів до 2,2 секунди; VeChain інтегрує блокчейн з IoT-пристроями для верифікації вина, тютюну та предметів розкоші; Everledger створила цифрові двійники понад 2,2 млн діамантів [2, 7, 14]. Ринок блокчейн-рішень для ланцюгів постачання зріс до 2,89 млрд доларів у 2024 році з прогнозом досягнення 44,3 млрд до 2034 року. Водночас систематичний аналіз виявляє суттєві бар'єри: проблему garbage in – garbage out (якість даних залежить від надійності точок введення), обмежену інтероперабельність різних блокчейн-платформ, високу вартість впровадження для малого та середнього бізнесу та складність залучення всіх учасників ланцюга. Стратегічне моделювання засвідчує, що блокчейн є економічно доцільним лише за умови достатнього рівня загрози від контрафакторів, чия



продукція візуально нерозрізна від оригіналу [3, 14]. Видається обґрунтованим припущення, що для товарних категорій із низьким рівнем візуальної підробки менш ресурсомісткі технології (QR-коди, RFID) можуть виявитися раціональнішим вибором.

ІоТ-маркери та розумна упаковка (smart packaging) становлять другу групу ідентифікаційних інструментів. NFC-чіпи (зокрема, NTAG 424 DNA з AES-128 шифруванням), QR-коди та RFID-мітки створюють унікальну цифрову ідентичність кожної одиниці товару [13]. Практичні впровадження демонструють результативність: програма Amazon Transparency захистила понад 900 млн одиниць продукції за допомогою серіалізованих QR-кодів. Глобальний ринок розумної упаковки оцінено в 21 млрд доларів із прогнозом зростання до 30 млрд до 2028 року. Рекомендована стратегія масштабування передбачає використання QR-кодів як базового рівня для товарів масового попиту з переходом на NFC/RFID для високовартісної продукції. Третю групу формують алгоритми штучного інтелекту та машинного навчання: згорткові нейронні мережі аналізують зображення упаковки на рівні пікселів, виявляючи аномалії у логотипах та текстурах із точністю до 94 %, а система Alibaba обробляє до 600 млн зображень на добу з точністю 97,6 % [12, 15]. Для ідентифікації фальшивих відгуків (ключового інструменту фальсифікації послуг) трансформерні моделі досягають точності 97 %, суттєво перевершуючи класичні підходи [4, 17]. Аномальне виявлення в ланцюгах постачання на основі алгоритмів Isolation Forest продемонструвало 87-відсоткову точність та зниження втрат продукції на 47 %. AI-рішення працюють проактивно: Amazon повідомляє, що понад 99 % заблокованих лістингів виявляються автоматичними системами до звернення власників брендів.

Порівняльний аналіз цифрових інструментів ідентифікації фальсифікації (табл. 1) засвідчує, що жоден із них не є універсальним: кожна технологія має специфічну зону ефективності, бар'єри впровадження та обмеження доступності для малого та середнього бізнесу.



Таблиця 1

Порівняльна характеристика цифрових інструментів ідентифікації
фальсифікації

Інструмент	Механізм верифікації	Емпіричні докази ефективності	Бар'єри та обмеження
Блокчейн-трасування	Розподілений реєстр із незмінним записом транзакцій від виробника до споживача; кожна ланка ланцюга постачання фіксується як верифікована подія	Walmart: скорочення часу трасування манго з 7 днів до 2,2 с (IBM Food Trust). Everledger: 2,2 млн діамантів із цифровими двійниками. Ринок: 2,89 млрд дол. (2024) [2, 7, 14]	Garbage in – garbage out; обмежена інтероперабельність платформ; вартість впровадження непідйомна для більшості МСБ [3]
IoT / розумна упаковка (NFC, QR, RFID)	Унікальний цифровий ідентифікатор на кожній одиниці товару; криптографічний захист (AES-128)	Amazon Transparency: 900 млн захищених одиниць. Ринок: 21 млрд дол. [13]	QR-коди легко копіюються без криптозахисту; NFC/RFID потребує спеціалізованого зчитувача або сучасного смартфона
AI / машинне навчання	Розпізнавання зображень упаковки (CNN); NLP-аналіз відгуків; аномальне виявлення у даних продажів	Alibaba: 600 млн зображень/добу, точність 97,6 %. Трансформерні моделі детекції фейкових відгуків: точність 97 % [4, 12, 15, 17]	Потребує великих навчальних датасетів; ризик хибнопозитивних спрацьовувань; висока обчислювальна вартість для real-time аналізу
Цифровий паспорт продукту (DPP)	Структурований запис повного циклу продукту з верифікованим цифровим слідом, доступним через QR/NFC	Поки що на етапі пілотних впроваджень; обов'язковість для акумуляторів – з лютого 2027 р. [10, 16, 22]	Відсутність делегованих актів для більшості товарних категорій; високі витрати на збір та структурування даних
Платформні рішення (Amazon, Alibaba)	Автоматизовані системи сканування лістингів, блокування підозрілих продавців, серіалізація через власні програми	Amazon: >99 % блокувань до звернення брендів. Alibaba: видалення 96–97 % до першого продажу	Контроль лише в межах однієї платформи; незалежний аудит 2025 р. виявив 47 % ймовірного контрафакту на AliExpress

Джерело: систематизовано автором за [1–4, 7, 10, 12–17, 22]



Від ідентифікації, що працює *post factum*, аналіз логічно переходить до превентивного маркетингового комплаєнсу, спрямованого на створення системних бар'єрів для фальсифікації. RegTech-платформи (технологічні рішення автоматизації регуляторного комплаєнсу) є центральним елементом превентивної архітектури. Veeva Vault PromoMats, домінуюча платформа у фармацевтичному секторі, автоматизує повний цикл медично-юридично-регуляторної (MLR) експертизи промоційних матеріалів від створення до відкликання, забезпечуючи відповідність вимогам FDA 21 CFR Part 11. Red Marker AI сканує маркетинговий контент у фінансовому, страховому та споживчому секторах, виявляючи комплаєнс-ризик у 30 разів швидше за ручну перевірку та пропонуючи автоматичні коригування [6, 9]. Глобальний ринок RegTech зростає від 16 млрд доларів у 2025 році до прогнозованих 62 млрд до 2032 року. Застереженням, однак, лишається ризик технологічного перевдягання *compliance theatre*: автоматизація процедур без зміни організаційної культури лише прискорює імітаційний комплаєнс. Якщо припустити, що впровадження RegTech-платформи само по собі гарантує комплаєнс, це призведе до хибної впевненості, яка може завдати більшої шкоди, ніж повна відсутність автоматизації.

Цифровий паспорт продукту (Digital Product Passport, DPP), запроваджений Регламентом (ЄС) 2024/1781 про екодизайн для стійких продуктів (ESPR), є найбільш масштабним превентивним інструментом нового покоління [10, 16, 22]. DPP – структурований цифровий запис, що містить інформацію про походження, матеріальний склад, екологічний вплив, ремонтпридатність та утилізацію продукту, прив'язаний до унікального ідентифікатора через QR-код, NFC або RFID. Обов'язковість DPP для акумуляторів настає з лютого 2027 року, для текстилю, меблів та шин – орієнтовно з 2027–2028 років, з поступовим розширенням на електроніку, будівельні матеріали та інші категорії до 2030 року. Антифальсифікаційний потенціал DPP полягає у створенні верифікованого цифрового сліду, що



дозволяє митним органам, ринковому нагляду та споживачам перевірити автентичність продукту в режимі реального часу. DPP фактично трансформує маркування з пасивного носія інформації на активний інструмент комплаєнсу, інтегрований у систему ринкового нагляду ЄС [23, 24].

Цифровий комплаєнс у сфері послуг, де відсутність фізичного носія ускладнює трасування, потребує окремого аналізу. Превентивні механізми тут охоплюють автоматизовану верифікацію ліцензій та сертифікатів через API-інтеграцію з державними реєстрами, NLP-аналіз відгуків для виявлення координованих кампаній маніпулювання, поведінкову аналітику для ідентифікації ghost services та системи цифрової ідентичності провайдерів послуг. Споживчі додатки автентифікації, зокрема Everledger (для ювелірних виробів та вина), 1TrueID (серіалізовані QR-коди з блокчейн-валідацією), Authentic Vision (фізично неклоновані голографічні мітки, зчитувані смартфоном), переносять точку верифікації безпосередньо до кінцевого споживача, демократизуючи функцію комплаєнсу [2, 12]. Інтеграція цифрових комплаєнс-інструментів у корпоративні системи CRM/ERP/SCM забезпечує single source of truth та предиктивну аналітику ризиків фальсифікації, хоча вимагає значних інвестицій у дані та кваліфікацію персоналу.

Технології трасування генерують детальні дані про переміщення продукції, споживчу поведінку та патерни покупок, що неминуче порушує питання етичних меж цифрового комплаєнсу. Баланс між прозорістю ланцюга постачання та приватністю споживача вимагає архітектурних рішень (розділення даних на рівні доступу, принцип мінімізації даних, вбудована приватність за моделлю privacy by design), а не лише регуляторних заборон [11]. Не виключено, що без адекватного етичного фреймворку цифровий комплаєнс здатний трансформуватися у surveillance creep – систему надмірного стеження, яка підриватиме ту саму споживчу довіру, заради зміцнення якої він створювався.

Нормативну базу протидії фальсифікації в Україні формують Закон «Про захист прав споживачів» (чинна редакція № 1023-XII від 1991 року), новий Закон



№ 3153-IX від 2023 року та Митний кодекс (зі змінами 2019 року щодо контрафакту). Державна служба з питань безпеки харчових продуктів та захисту споживачів здійснює ринковий нагляд, проте її цифрова інфраструктура перебуває на етапі трансформації: Кабінет Міністрів запустив експериментальний проєкт створення єдиної електронної системи, що охопить близько 2 млн суб'єктів господарювання. Новий Закон про захист прав споживачів передбачає запровадження Порталу е-покупець, автоматизованої системи верифікованих продавців та повноважень Держпродспоживслужби блокувати невідповідні вебсайти. Сукупність цих ініціатив засвідчує, що Україна перебуває на початковому етапі формування цифрової інфраструктури маркетингового комплаєнсу, де нормативна рамка вже окреслена, проте технологічне наповнення лишається фрагментарним.

Система е-акцизу, обов'язкова з 1 січня 2026 року (Закон № 3173-IX), є на сьогодні найбільш завершеним цифровим інструментом трасування в Україні. Вона замінює паперові акцизні марки електронними (QR/DataMatrix-коди) для алкогольних напоїв, тютюнових виробів та рідин для електронних сигарет, забезпечуючи реєстрацію всіх операцій від виробника до кінцевого продажу та можливість перевірки легальності товару через застосунок Дія. За оцінками, тіньовий ринок підакцизних товарів спричинив втрати бюджету у 30 млрд грн у 2022 році; впровадження Track & Trace має скоротити нелегальний обіг щонайменше на 15 %. Асоціація GS1 Україна забезпечує ідентифікацію товарів у системі GTIN, верифікацію штрихкодів та підтримку Депозитарію (електронного каталогу вітчизняних товарів), формуючи базову інфраструктуру для ширших комплаєнс-систем.

Воєнний стан суттєво загострив ризики фальсифікації. За даними дослідження, опублікованого в *International Annals of Criminology*, ринок фальсифікованих ліків в Україні перевищує 97 млн євро на рік, при цьому за 2021–2023 роки ухвалено лише один обвинувальний вирок за відповідною статтею Кримінального кодексу [25]. Частка нелегальних тютюнових виробів



зросла з 2 % у 2017 році до 22 % у 2022 році, що свідчить про системну деградацію контрольних механізмів. Руйнування інфраструктури, переміщення підприємств, скорочення кадрового потенціалу Держпродспоживслужби створюють вікно вразливості, яке фальсифікатори активно використовують [21, 25]. Парадоксально, проте саме воєнний стан одночасно прискорює цифровізацію державних сервісів (Дія, єЧерга, е-ветеринарні сертифікати), формуючи інфраструктурне підґрунтя для майбутніх комплаєнс-систем.

Євроінтеграційні зобов'язання вимагають поетапного наближення до стандартів ЄС. Регламент про загальну безпечність продукції (Регламент (ЄС) 2023/988, GPSR), що застосовується з грудня 2024 року, встановлює обов'язкову трасованість (тип, серія, партійний номер), ідентифікацію виробника та внутрішній аналіз ризиків для всієї нехарчової продукції [23]. Регламент про ринковий нагляд (Регламент (ЄС) 2019/1020, MSR) зобов'язує призначати економічного оператора в ЄС для імпортованої продукції та передбачає інструменти контролю онлайн-торгівлі, включно з правом органів нагляду на контрольні закупівлі та вилучення контенту [24]. Цифровий паспорт продукту стане критичним інструментом доступу українських товарів до ринку ЄС після набуття чинності делегованих актів [10, 16, 22]. Бар'єри впровадження цифрового комплаєнсу в Україні є багаторівневими: малий та середній бізнес має обмежені ресурси для інвестицій у блокчейн-інфраструктуру або ERP-інтеграцію, цифрова грамотність населення знижується, а Вищий суд з питань інтелектуальної власності станом на 2024 рік залишається неоперативним через незавершений відбір суддів [20]. Усе це дає підстави стверджувати, що євроінтеграція виступає одночасно і драйвером цифрового комплаєнсу (через зовнішній нормативний тиск), і джерелом додаткового навантаження на бізнес, не підкріпленого достатньою інституційною підтримкою.

Узагальнення проведеного аналізу дозволяє запропонувати триступеневу модель адаптивного цифрового маркетингового комплаєнсу, яка враховує специфіку українського бізнес-середовища та диференціює інтенсивність



технологічних рішень залежно від рівня ризику товарної категорії, масштабу підприємства та цільового ринку збуту (рис. 1).

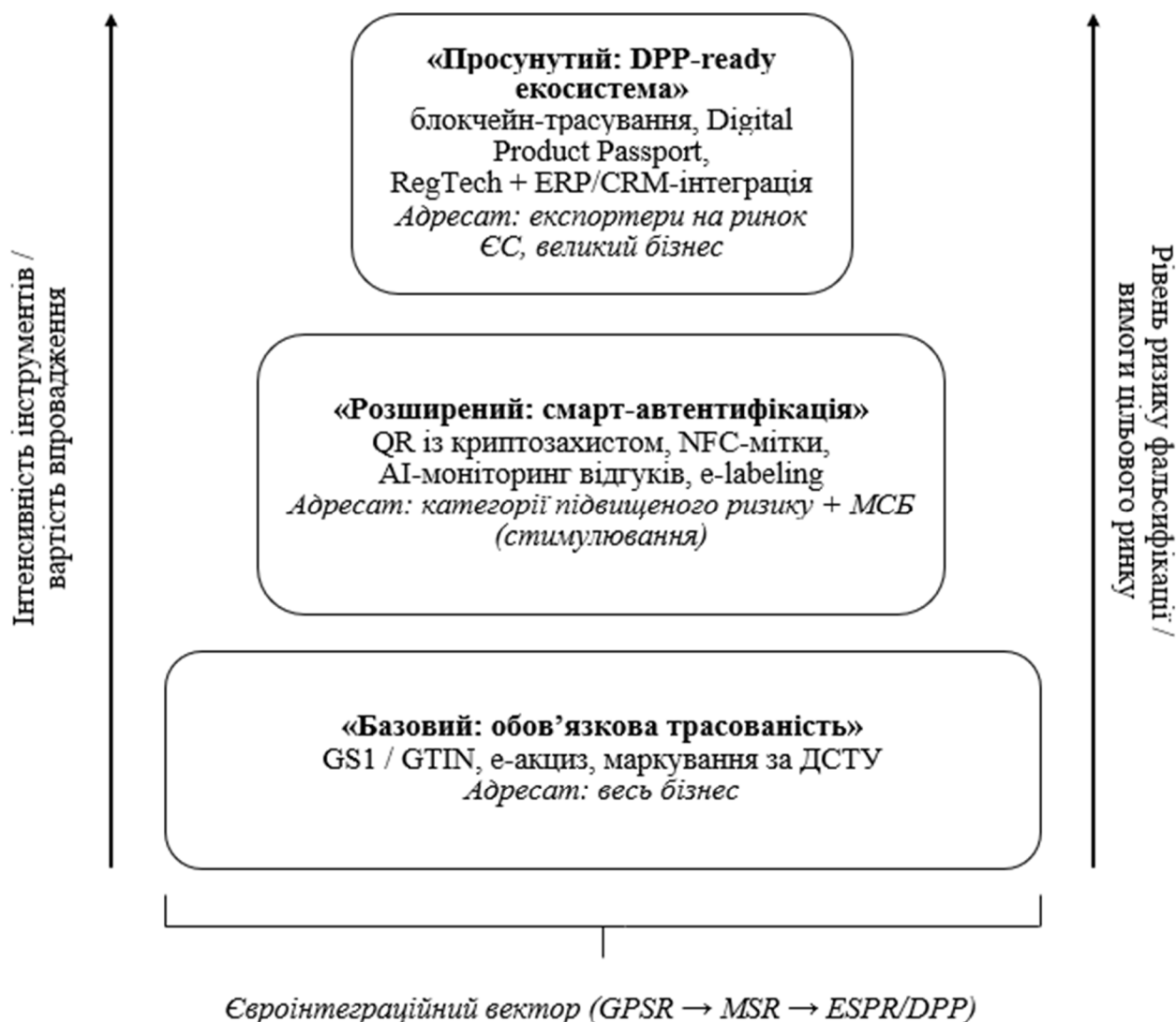


Рис. 1. Треступенева модель адаптивного цифрового маркетингового
комплаєнсу для українського бізнесу

Джерело: розроблено автором

Перший (базовий) рівень охоплює обов'язкові інструменти трасованості – систему GS1 (GTIN-ідентифікація, штрихкодування), е-акциз для підакцизних товарів та мінімальне маркування відповідно до ДСТУ; він поширюється на весь бізнес незалежно від масштабу. Другий (розширений) рівень передбачає впровадження розумної упаковки (QR із криптозахистом, NFC-мітки), AI-



моніторинг відгуків та цінових аномалій, цифрове маркування (e-labeling); він є добровільним, проте стимульованим через податкові преференції та грантові програми, і адресований передусім категоріям підвищеного ризику (фармацевтика, дитяче харчування, косметика). Третій (просунутий) рівень включає блокчейн-трасування ланцюга постачання, DPP-ready інфраструктуру, інтеграцію RegTech-платформ у корпоративні ERP/CRM-системи; він орієнтований на експортерів на ринок ЄС та великий бізнес.

Висновки. Цифровий маркетинговий комплаєнс формується як інтегральна функція, що поєднує технологічний, регуляторний та ринковий виміри протидії фальсифікації товарів і послуг. Аналіз технологічного арсеналу засвідчує наявність зрілих рішень (блокчейн-трасування, AI-ідентифікація, розумна упаковка, цифрові паспорти), що демонструють високу ефективність у пілотних та масштабних впровадженнях. Ключовий парадокс полягає в асиметрії: технологічна спроможність випереджає інституційну готовність, особливо у країнах, що розвиваються.

Для України це означає необхідність одночасного руху у двох напрямках: розбудови національної цифрової інфраструктури комплаєнсу (е-акциз, єдина електронна система Держпродспоживслужби, судова інституція з питань інтелектуальної власності) та гармонізації з європейськими стандартами (GPSR, MSR, DPP). Оптимальна конфігурація передбачає модель адаптивного комплаєнсу (рис. 1), де інтенсивність цифрових інструментів диференціюється залежно від рівня ризику фальсифікації товарної категорії, масштабу підприємства та цільового ринку. Обов'язкова фіксація базового рівня трасованості через систему GS1 та е-акциз; добровільне, але стимульоване, впровадження розумної упаковки для категорій підвищеного ризику (фармацевтика, дитяче харчування, косметика); та інвестиції у RegTech-платформи для експортерів на ринок ЄС – такий триступеневий підхід дозволяє збалансувати витрати малого та середнього бізнесу із євроінтеграційними вимогами.



Пастка compliance theatre залишається головним ризиком: цифровізація процедур без системної зміни організаційної культури та регуляторної спроможності створить лише ілюзію захищеності. Фальсифікація послуг (від фейкових відгуків до ghost services) потребує окремого регуляторного та технологічного реагування, оскільки екстраполяція товарних моделей комплаєнсу на сферу послуг є методологічно некоректною. Перспективами подальших досліджень є емпірична оцінка економічної ефективності цифрового комплаєнсу для українських підприємств різних масштабів, розробка секторальних моделей впровадження Digital Product Passport з урахуванням специфіки вітчизняних ринків та аналіз впливу системи е-акцизу на динаміку нелегального обігу підакцизних товарів.

Список використаних джерел

1. OECD/EUIPO. Mapping Global Trade in Fakes 2025: Global Trends and Enforcement Challenges. Paris : OECD Publishing, 2025. (Illicit Trade series). URL: https://www.oecd.org/en/publications/mapping-global-trade-in-fakes-2025_94d3b29f-en.html
2. Yiu N.C.K. Toward Blockchain-Enabled Supply Chain Anti-Counterfeiting and Traceability. *Future Internet*. 2021. Vol. 13, No. 4. Art. 86. DOI: <https://doi.org/10.3390/fi13040086>
3. Naoum-Sawaya J., Elhedhli S., De Carvalho P. Strategic blockchain adoption to deter deceptive counterfeiters. *European Journal of Operational Research*. 2023. Vol. 311, No. 1. P. 373–386. DOI: <https://doi.org/10.1016/j.ejor.2023.04.031>
4. Hajek P., Hikkerova L., Sahut J.-M. Fake review detection in e-Commerce platforms using aspect-based sentiment analysis. *Journal of Business Research*. 2023. Vol. 158. Art. 113700. DOI: <https://doi.org/10.1016/j.jbusres.2022.113700>
5. Khamitov M., Rajavi K., Huang D.W., Hong Y. Consumer trust: Meta-analysis of 50 years of empirical research. *Journal of Consumer Research*. 2024. Vol. 51, No. 1. P. 7–18. DOI: <https://doi.org/10.1093/jcr/ucad045>



6. Grassi L., Lanfranchi D. RegTech in public and private sectors: the nexus between data, technology and regulation. *Journal of Industrial and Business Economics*. 2022. Vol. 49. P. 441–479. DOI: <https://doi.org/10.1007/s40812-022-00226-0>
7. Chen C.-L., Guo L.-H., Zhou M. et al. Blockchain-Based Anti-Counterfeiting Management System for Traceable Luxury Products. *Sustainability*. 2022. Vol. 14, No. 19. Art. 12814. DOI: <https://doi.org/10.3390/su141912814>
8. Schrödter A., Weißenberger B.E. The institutionalization of digital compliance. *Management Decision*. 2024. Vol. ahead-of-print. DOI: <https://doi.org/10.1108/MD-03-2024-0498>
9. Charoenwong B., Kowaleski Z.T., Kwan A., Sutherland A.G. RegTech: Technology-driven compliance and its effects on profitability, operations, and market structure. *Journal of Financial Economics*. 2024. Vol. 154. Art. 103792. DOI: <https://doi.org/10.1016/j.jfineco.2024.103792>
10. Farooque M. et al. Digital product passport for sustainable and circular supply chain management. *International Journal of Logistics: Research and Applications*. 2024. P. 2513–2540. DOI: <https://doi.org/10.1080/13675567.2024.2374256>
11. De Keyzer F., Van Noort G., Kruikemeier S. et al. Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*. 2022. DOI: <https://doi.org/10.1007/s11747-022-00845-y>
12. Bardari A.C., Bottani E., Rizzi A., Tebaldi L. Anti-Counterfeiting for Luxury Fashion: State-of-the-Art Literature and Technological Analysis. *Journal of the Textile Institute*. 2026. DOI: <https://doi.org/10.1177/17545730251409569>
13. Zuo J., Feng J., Gonçalves Gameiro M. et al. RFID-based sensing in smart packaging for food applications: A review. *Future Foods*. 2022. Vol. 6. Art. 100198. DOI: <https://doi.org/10.1016/j.fufo.2022.100198>



14. Lu W., Jiang Y., Chen Z., Ji X. Blockchain adoption in a supply chain system to combat counterfeiting. *Computers & Industrial Engineering*. 2022. Vol. 171. Art. 108408. DOI: <https://doi.org/10.1016/j.cie.2022.108408>
15. Yao S., Zhu K., Yang R. Combating Counterfeit Products: Anti-counterfeiting Technology and Law Enforcement. *Production and Operations Management*. 2025. DOI: <https://doi.org/10.1177/10591478251335156>
16. Psarommatis F., May G. Digital Product Passport: A Pathway to Circularity and Sustainability in Modern Manufacturing. *Sustainability*. 2024. Vol. 16, No. 1. Art. 396. DOI: <https://doi.org/10.3390/su16010396>
17. Zhang D., Li W., Niu B., Wu C. A deep learning approach for detecting fake reviewers: Exploiting reviewing behavior and textual information. *Decision Support Systems*. 2023. Vol. 166. Art. 113911. DOI: <https://doi.org/10.1016/j.dss.2022.113911>
18. Hochstein R.E., Harmeling C.M., Perko T. Toward a theory of consumer digital trust: meta-analytic evidence of its role in the effectiveness of user-generated content. *Journal of the Academy of Marketing Science*. 2023. DOI: <https://doi.org/10.1007/s11747-023-00948-6>
19. Ляпун Н., Коваленко Н. Ідентифікація товарів та визначення фальсифікації продукції при проведенні судової товарознавчої експертизи. *Молодий вчений*. 2020. № 8(84). С. 240–243. DOI: <https://doi.org/10.32839/2304-5809/2020-8-84-48>
20. Князева Т., Аракелова І., Подольський Р. та ін. Маркетингова технологія в контексті цифровізації: особливості та тенденції в Україні. *Economic Alternatives*. 2023. № 2. С. 409–423. URL: <https://economic-alternatives.com>
21. Лебедь С.О., Немченко А.С. Узагальнення сучасного досвіду боротьби з розповсюдженням фальсифікованих лікарських засобів у високорозвинених країнах. *Управління, економіка та забезпечення якості у фармації*. 2020. № 3. С. 35–46. DOI: <https://doi.org/10.24959/uekj.20.21>
22. Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for



sustainable products (ESPR). *Official Journal of the European Union*. L 2024/1781.

URL: <https://eur-lex.europa.eu/eli/reg/2024/1781/oj/eng>

23. Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety (GPSR). *Official Journal of the European Union*. L 135/1. URL: <https://eur-lex.europa.eu/eli/reg/2023/988/oj>

24. Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products (MSR). *Official Journal of the European Union*. L 169/1. URL: <https://eur-lex.europa.eu/eli/reg/2019/1020/oj>

25. Illicit Trade in Wartime: Ukraine's Trends and Challenges for Counteraction. *International Annals of Criminology*. 2025. Cambridge University Press. URL: <https://www.cambridge.org/core/journals/international-annals-of-criminology/article/B50C0C34E65CCE8E25F77FCEAE57DC45>