ISSN (Online): 3083-7782
Електронний науковий журнал «ЕКОНОМІЧНА ПАРАДИГМА»

УДК 339.138:004

Гановський Василь Леонідович
доктор філософії,
асистент кафедри економічної теорії та конкурентної політики
Державний торговельно-економічний університет
ORCID: 0000-0002-9897-7754

DOI: https://doi.org/10.25313/3083-7782-2026-6-26

ОМАНЛИВІ РЕКЛАМНІ ПРАКТИКИ У ЦИФРОВОМУ СЕРЕДОВИЩІ

Анотація. *Вступ. Цифрова реклама перетворилася на домінуючий медіаканал сучасності, що формує переважну частину світових рекламних бюджетів та характеризується глобальним охопленням, автоматизацією процесів і високим рівнем конкуренції. Перехід рекламної індустрії в онлайн-середовище змінив саму природу відносин між рекламодавцем і споживачем, якщо у традиційному середовищі оманлива реклама зводилася переважно до недостовірних тверджень про товар, то у цифровому вона набуває системного, архітектурного характеру. Оманливими стають не лише зміст повідомлення, а й дизайн інтерфейсу, послідовність кроків, спосіб подання ціни, механізми оформлення підписки тощо. Впровадження автоматизованої закупівлі реклами та генеративного штучного інтелекту підвищило ефективність таргетингу, проте водночас розширило простір для оманливих практик – від маніпулятивного дизайну інтерфейсів і оманливої гейміфікації до рекламного шахрайства та deepfake-реклами. Тому цілком очевидно постає необхідність визначення сутності, типології та регуляторних меж оманливих рекламних практик у цифровому середовищі з позицій економічних, технологічних та регуляторних вимірів.*

Мета. Метою дослідження є розкриття економіко-правових засад функціонування оманливих рекламних практик у цифровому середовищі задля впорядкування багаторівневої типології таких практик та їх ідентифікації за рівнем здійснення обману, що дозволяє диференціювати регуляторні підходи на рівні окремих юрисдикцій та сформулювати рекомендації для регуляторів, бізнесу та користувачів.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правове забезпечення регулювання оманливих рекламних практик у цифровому середовищі (зокрема акти Європейського Союзу, США та України); 2) офіційні матеріали регуляторних органів та аналітичні дані щодо масштабів і поширеності оманливих практик; 3) праці вітчизняних та зарубіжних авторів у царині економіки цифрових ринків, захисту економічної конкуренції та прав споживачів.

У процесі здійснення дослідження було використано такі наукові методи: теоретичного узагальнення та групування (для побудови типології оманливих практик і таксономії темних патернів, а також виокремлення оманливої гейміфікації як самостійного феномену); порівняльно-правовий (для зіставлення регуляторних режимів ЄС, США та України); системно-структурний і кейс-метод (для аналізу регуляторних справ); формалізації, аналізу та синтезу (для встановлення зв'язків між економічним, технологічним і правовим вимірами явища); логічного узагальнення результатів (формулювання висновків).

Результати. У статті розкрито економіко-правову природу та структуру оманливих рекламних практик у цифровому середовищі й запропоновано їх багаторівневу типологію, побудовану за критерієм рівня, на якому реалізується введення в оману, – на рівнях повідомлення, інтерфейсу, ринкової

екосистеми та синтетичного контенту. Систематизовано таксономію маніпулятивних патернів за основними родинами; окремо аргументовано доцільність виокремлення оманливої гейміфікації як самостійного об' єкта дослідження, що інтегрує ознаки кількох родин маніпулятивного дизайну та зумовлює підвищені ризики для вразливих категорій споживачів, насамперед неповнолітніх. Визначено місце оманливих практик у системі економічних відносин учасників рекламного ринку та охарактеризовано природу шкоди, що завдається споживачам, рекламодавцям і цифровим платформам. Обґрунтовано тезу про системний, а не епізодичний характер досліджуваного явища; встановлено конвергенцію регуляторних підходів трьох юрисдикцій, що за відмінності інституційних механізмів підпорядкована спільній меті – захисту автономії споживчого вибору.

Перспективи. У подальших наукових дослідженнях пропонується зосередити увагу на дослідженні стійкості автономних систем штучного інтелекту до впливу темних патернів, оцінюванні непрямих витрат сумлінних учасників ринку на протидію оманливим практикам, а також на поглибленому аналізі гармонізації українського законодавства з ЄС в частині регулювання темних патернів і оманливої гейміфікації, які наразі прямо не врегульовані національним законодавством. Це надасть змогу вдосконалити нормативно-правове забезпечення та правозастосовну практику у сфері захисту прав споживачів у цифровому середовищі.

Ключові слова: *оманлива реклама, цифрове середовище, темні патерни, оманлива гейміфікація, рекламне шахрайство, недобросовісна конкуренція, ринок цифрової реклами, deepfake.*

Постановка проблеми. Цифровізація рекламної діяльності докорінно змінила механізми взаємодії між суб'єктами рекламного ринку. Якщо в умовах традиційного ринку введення в оману реалізовувалося переважно через недостовірний зміст рекламного повідомлення, то в цифровому середовищі обман вбудовується в саму архітектуру взаємодії — у дизайн інтерфейсу, послідовність дій користувача, спосіб подання цінової інформації та механізми оформлення договірних відносин. Унаслідок цього оманлива реклама перетворюється на системне явище, що пронизує структуру цифрових ринків і безпосередньо впливає на економічну поведінку споживача та конкурентні відносини між учасниками ринку.

Гострота проблеми посилюється тим, що масштаб цифрового рекламного ринку прямо пропорційний масштабу потенційних втрат, які розподіляються між користувачами, сумлінними рекламодавцями та цифровими платформами. Упровадження автоматизованої закупівлі реклами та генеративного штучного інтелекту знизило граничні витрати на створення оманливого контенту й водночас ускладнило його виявлення, що зумовлює стійкий розрив між темпами появи нових форм обману та спроможністю регуляторних механізмів на них реагувати. Ситуацію ускладнює фрагментарність наукового осмислення проблеми, за якої економічний, технологічний і регуляторний виміри досліджуються відокремлено. Це актуалізує потребу в комплексному економіко-правовому дослідженні оманливих рекламних практик у цифровому середовищі.

Аналіз останніх досліджень і публікацій. Проблематика оманливих практик у цифровому середовищі перебуває у фокусі уваги насамперед у зарубіжних дослідників, що репрезентують різні наукові традиції — економічну, правову та поведінкову. Зокрема, А. Гупта (A. Gupta) [1] засобами теорії галузевих ринків моделює оманливу рекламу за умов присутності споживачів, нездатних розпізнати введення в оману, та оцінює вплив регуляторного втручання на ринкову рівновагу й добробут. Дж. Баумейстер (J. Baumeister) та ін. [2] на підставі систематичного огляду консолідували 157 темних патернів у типологію на основі моделі Лейзера (Leiser), побудованої навколо інформаційної асиметрії та придушення вільного вибору споживача. Дж. Ансельмо (G. Anselmo), Дж. Маннайолі (G. Mannaioli) та А. Сардо (A. Sardo) [3], поєднавши споживче право з прагма-когнітивною лінгвістикою, розкрили механізми експлуатації когнітивних викривлень в оманливому маркетингу за участю лідерів думок. С. Бенауда (S. Benaouda) та Р. Сабер (R. Saber) [4] зіставили механізми правового захисту електронного споживача від оманливої реклами в низці юрисдикцій, окремо розглянувши заборону темних патернів у статті 25 Регламенту ЄС про цифрові послуги. С. Санетра-Полґрабі (S. Sanetra-Połgrabi) та З. Тетлак (Z. Tetlak) [5] на емпіричному дослідженні України виокремили вісім типів оманливих рекламних практик та окреслили перспективні рекламні технології, що потребуватимуть посилення захисту прав споживачів. М. Ботма (M. Bothma) та Б. ван Стаден (B. van Staden) [6] емпірично довели, що сприйнята оманливість реклами знижує задоволеність споживачів, а через неї — їхню лояльність і наміри повторної купівлі.

Разом з тим залишаються не розв'язаними проблемні питання в частині побудови цілісної багаторівневої типології оманливих практик в єдину систему; розкриття економічного виміру таких практик — їхнього впливу на добросовісну конкуренцію, споживчий добробут і ефективність рекламного ринку; а також аналізу новітніх форм цифрового обману (рекламного шахрайства, оманливої гейміфікації та реклами на основі діпфейків) у контексті адаптації українського законодавства до права ЄС.

Метою статті є розкриття економіко-правових засад функціонування оманливих рекламних практик у цифровому середовищі задля впорядкування багаторівневої типології таких практик та їх ідентифікації

за рівнем здійснення обману, що дозволяє диференціювати регуляторні підходи на рівні окремих юрисдикцій та сформулювати рекомендації для регуляторів, бізнесу та користувачів.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правове забезпечення регулювання оманливих рекламних практик у цифровому середовищі (зокрема акти Європейського Союзу, США та України); 2) офіційні матеріали регуляторних органів та аналітичні дані щодо масштабів і поширеності оманливих практик; 3) праці вітчизняних та зарубіжних авторів у царині економіки цифрових ринків, захисту економічної конкуренції та прав споживачів.

У процесі здійснення дослідження було використано такі наукові методи: теоретичного узагальнення та групування (для побудови типології оманливих практик і таксономії темних патернів, а також виокремлення оманливої гейміфікації як самостійного феномену); порівняльно-правовий (для зіставлення регуляторних режимів ЄС, США та України); системно-структурний і кейс-метод (для аналізу регуляторних справ); формалізації, аналізу та синтезу (для встановлення зв'язків між економічним, технологічним і правовим вимірами явища); логічного узагальнення результатів (формулювання висновків).

Виклад основного матеріалу. Розуміння масштабів оманливих практик неможливе поза контекстом самого ринку, на якому вони виникають. Цифрова реклама демонструє стійке динамічне зростання, що робить її і найприбутковішим, і найвразливішим до зловживань сегментом маркетингу. Оцінки різних аналітичних агенцій відрізняються методологією, проте сходяться у висновку, що ринок реклами постійно зростає. Станом на 2025 рік Grand View Research оцінює його у 567,9 млрд. дол. із прогнозом зростання до 1692,9 млрд. до 2033 року (CAGR 14,3%) [7] рис. 1. Портал Statista наводить ще вищу цифру рекламних витрат — 798,7 млрд. дол. у 2025 році, з яких найбільший сегмент — пошукова реклама (334,4 млрд. дол.) [8]. Галузеві агрегатори фіксують перетин позначки у 700 млрд. доларів уперше в історії, що становить близько 69% сукупних світових рекламних бюджетів [9; 10].

Економічні втрати від оманливих рекламних практик зростають пропорційно до масштабів ринку цифрової реклами. За оцінкою Світової федерації рекламодавців (WFA), ще у 2016 році прогнозувалося, що протягом десятиліття рекламне шахрайство стане другим за масштабами видом організованої злочинності після наркоторгівлі [11]. Відтак дослідження оманливих практик неможливе без урахування тенденцій розвитку самого рекламного ринку.

У широкому сенсі оманливі рекламні практики онлайн — це комерційні комунікації або пов'язані з ними інтерфейсні, алгоритмічні чи організаційні механізми, які вводять споживача в оману, приховують істотну інформацію, спотворюють його свободу вибору або експлуатують його вразливість. Оманливі практики у цифровому середовищі доцільно класифікувати за рівнем, на якому відбувається обман. Пропонується чотирирівнева модель, яка охоплює як практики, що спрямовані на споживача, так і ті, що завдають шкоди рекламодавцям і платформам. Зокрема: рівень повідомлення (класична оманлива реклама); рівень інтерфейсу: (деталізована таксономія темних патернів); рівень екосистеми (рекламне шахрайство); рівень синтетичного контенту (deepfake-реклама та ШІ-обман).

Рис. 1. Динаміка та прогноз обсягу світового ринку цифрової реклами

Джерело: побудовано автором самостійно на основі [8]

Класична оманлива реклама — найдавніший тип, де недостовірні твердження про властивості, ціну чи походження товару забезпечували економічні прибутки рекламодавцям. У цифровому середовищі він зберігається, але масштабується, оскільки одне оманливе твердження може бути показане мільйонам користувачів із мікротаргетингом за вразливостями. Типові прояви: приписування товарам неіснуючих лікувальних властивостей, фальшиві знижки за схемою «було/стало», приховані умови кредитування, маскування реклами під редакційний контент (native advertising без позначки) тощо.

Сучасні оманливі рекламні практики дедалі рідше ґрунтуються на поширенні неправдивої інформації в рекламному повідомленні. Натомість основний вплив на поведінку споживача здійснюється через проєктування цифрових інтерфейсів, які формують архітектуру вибору та спонукають користувача до прийняття рішень, що не завжди відповідають його реальним інтересам. Саме тому в сучасній науковій літературі дедалі більшого поширення набуває поняття «темні патерни» (dark patterns), яке охоплює сукупність інтерфейсних рішень, спрямованих на маніпулювання поведінкою користувачів шляхом використання когнітивних упереджень, асиметрії інформації та особливостей цифрової взаємодії. На основі підходів ОЕСР, Федеральної торгової комісії США та таксономії К. Грей та ін. (2024) [12–14] темні патерни можуть бути систематизовані у шість основних груп, що відображають різні механізми впливу на процес прийняття рішень користувачами рис. 2.

Практика приховування ґрунтується на повному або частковому приховуванні інформації, що має істотне значення для прийняття рішення споживачем. Маніпуляція досягається шляхом відкладеного розкриття умов придбання, автоматичного додавання товарів чи послуг або маскування довгострокових фінансових зобов'язань під виглядом одноразової операції. До основних проявів належать приховані платежі, коли додаткові збори стають відомими лише на завершальному етапі оформлення замовлення; автоматичне додавання товарів чи послуг до кошика без прямої згоди користувача; а також приховані підписки, за яких разова покупка фактично передбачає автоматичне регулярне списання коштів.

Прикладом використання прихованих платежів є практика авіакомпанії Ryanair, яка тривалий час за замовчуванням включала до замовлення страхування та пріоритетну посадку, покладаючи на користувача обов'язок самостійно відмовитися від цих послуг. Аналогічно, Центральний орган із захисту прав споживачів Індії (CCPA) визнав порушенням практику платформи BookMyShow, яка автоматично додавала до вартості квитка благодійний внесок у розмірі однієї рупії через попередньо встановлену позначку [15].

На відміну від практик приховування, які ґрунтуються на нерозкритті суттєвої інформації, темний патерн створення перешкод спрямований на штучне ускладнення дій, що є небажаними для суб'єкта госпо-

Рис. 2. Таксономія темних патернів за родинами
Джерело: складено автором самостійно шляхом синтезу [12–14]

дарювання. Найпоширенішим проявом є створення інтерфейсів, у яких користувач може легко оформити підписку або зареєструватися, проте процес відмови від послуги чи скасування підписки є навмисно тривалим, заплутаним і потребує виконання значної кількості додаткових дій. До цієї групи також належать практики, що ускладнюють порівняння цін, тарифів або умов придбання товарів і послуг, обмежуючи можливість споживача здійснити обґрунтований вибір.

Показовим прикладом є процедура скасування підписки Amazon Prime, яка є багатоступеневою та навмисно ускладненою структурою, що має на меті стримувати користувачів від відмови від сервісу.

Сутність патерну маніпулювання інтерфейсом полягає у візуальній або мовній маніпуляції ієрархією подання варіантів вибору, спрямованій на те, щоб непомітно схилити користувача до вигідного для бізнесу рішення. На відміну від практик приховування, суттєва інформація тут формально доступна, проте подана у спосіб, що спотворює сприйняття та ускладнює раціональну оцінку альтернатив. До типових проявів належать передвибір — заздалегідь установлені позначки згоди, які користувач має самостійно скасувати; маніпулятивне формулювання запитань через двозначні конструкції з подвійним запереченням, що дезорієнтують користувача (показовим є приклад провайдера Sky UK, де формулювання на кшталт «натисніть, щоб відмовитися» фактично залишало особу підписаною за замовчуванням, а також візуальне відвертання уваги, за якого кнопку згоди оформлено яскраво й помітно, тоді як можливість відмови подано дрібним малопомітним посиланням.

Сутність примушування до дії полягає у примусовому виконанні небажаної дії як неодмінної умови доступу до послуги чи контенту, унаслідок чого користувач позбавляється реального вибору. До типових проявів належать примусова реєстрація, за якої перегляд контенту стає можливим лише після створення облікового запису та передання персональних даних; автоматичне платне продовження, коли після завершення безкоштовного періоду підписка мовчазно переходить у платну без окремого підтвердження користувача (показовим є приклад численних стримінгових і цифрових сервісів, що оформлюють пробний доступ із прив'язкою платіжних даних); а також блокування функцій, за якого доступ до можливостей сервісу штучно обмежується доти, доки користувач не виконає вигідної для платформи дії.

Фальшива терміновість і дефіцит — родина темних патернів, що ґрунтується на експлуатації страху втрати (так званого FOMO) через створення штучних часових і кількісних обмежень, які спонукають користувача до поспішного рішення всупереч раціональній оцінці. До типових проявів належать фейкові таймери зворотного відліку, які лише імітують завершення вигідної пропозиції й скидаються при перезавантаженні сторінки; повідомлення про вичерпання запасу на кшталт «залишився останній товар» за фактичної його доступності; а також фальшиве соціальне підтвердження, що демонструє вигадані дані про активність інших користувачів (наприклад, «15 осіб переглядають цей готель зараз»). Показовими є практики платформи Booking.com, які стали предметом розслідування європейських регуляторів, після чого компанія зобов'язалася відображати лише достовірні дані.

Завершальною в цій класифікації є нав'язливість та емоційний тиск — родина темних патернів, що ґрунтується на виснаженні опору користувача через повторювані заклики або емоційну маніпуляцію. Найвиразнішим її проявом є присоромлення за відмову, коли варіант відхилення пропозиції формулюється так, щоб викликати в користувача почуття провини чи незручності. Хрестоматійним прикладом слугує сервіс MyMedic, у якого кнопка відмови від підписки була оформлена як саркастичне «Ні, я краще стечу кров'ю» [16]. До цієї ж родини належить настирливість — повторюване нав'язування одного й того самого запиту, що поступово долає спротив користувача, наприклад, випливаючі вікна без можливості остаточної відмови.

Якщо попередні рівні стосувалися обману, спрямованого на споживача, то на рівні ринкової екосистеми жертвою введення в оману стає вже сам рекламодавець, який оплачує покази та переходи, згенеровані не реальними користувачами, а автоматизованими програмами, фермами кліків чи підробленими ресурсами. До основних технік належать імітація кліків, трафік ботів, підміна доменів, накладання оголошень, підробка ідентифікаторів застосунків, упровадження фальшивих переходів, а також ресурси, створені виключно задля генерування рекламних показів. Показовою є схема SlopAds, яку у 2025 році викрили компанії HUMAN Security та Google, в якій понад дві сотні мобільних застосунків приховано відтворювали рекламу в невидимих для користувача вікнах, сягаючи в піковий період близько 2,3 млрд. фальшивих рекламних запитів на добу [17]. На відміну від темних патернів, що спотворюють вибір окремої особи, рекламне шахрайство підриває економічну ефективність усього рекламного ланцюга, відводячи кошти від сумлінних учасників ринку та викривлюючи конкурентні умови.

Найновішим і найдинамічнішим типом оманливих практик є реклама, побудована на синтетичному контенті, який генерує штучний інтелект. Сучасні генеративні технології дають змогу створювати переконливі фальшиві відео- та аудіозвернення нібито від імені знаменитостей, лікарів чи політиків, надаючи шахрайській пропозиції видимості авторитетної рекомендації. Показовою ілюстрацією є хвиля deepfake-реклами 2024 року, у якій згенерований образ підприємця Ілона Маска просував фіктивні інвестиційні та криптовалютні схеми, унаслідок чого окремі ошукані особи втрачали значні суми коштів [18]. На відміну від попередніх

рівнів, цей тип поєднує одразу два виміри шкоди — введення в оману споживача через фальшиву рекомендацію та порушення прав третіх осіб через несанкціоноване використання їхнього образу й репутації.

Окремої уваги в межах запропонованої типології потребує гейміфікація, суть якої полягає у застосуванні ігрових механік (балів, рівнів, нагород, індикаторів прогресу) у неігрових цифрових продуктах. Сама по собі гейміфікація є нейтральним і часто корисним інструментом залучення, проте вона набуває оманливого характеру тоді, коли ігрові механіки спрямовуються не на досягнення цілей користувача, а на експлуатацію його когнітивних викривлень задля комерційної вигоди. Доцільність виокремлення цього явища в самостійний об'єкт аналізу зумовлена тим, що оманлива гейміфікація не зводиться до жодної з розглянутих вище родин темних патернів, а інтегрує ознаки кількох із них, а саме емоційного тиску, фальшивої терміновості та примусу, і тому потребує окремого аналітичного підходу.

Принциповим для оцінювання гейміфікації є не сама наявність ігрової механіки, а її спрямованість. Та сама механіка здатна як мотивувати користувача, забезпечуючи прозорий поступ до його власної мети, так і експлуатувати його, підтримуючи штучну залученість заради монетизації за рахунок добробуту самого користувача. Тож гейміфікацію доцільно розглядати не як бінарну опозицію «корисне — шкідливе», а як неперервний спектр, на одному полюсі якого перебуває етична мотивація, а на протилежному — маніпулятивна експлуатація рис. 3

Рис. 3. Спектр гейміфікації від етичної мотивації до маніпулятивної експлуатації
Джерело: складено автором самостійно

Розмежувати ці полюси дає змогу так званий тест автономії: чи допомагає певна механіка користувачеві досягати його власних усвідомлених цілей чи, навпаки, її створено для того, щоб в обхід раціонального рішення впливати на нього через емоції, звичку або азарт. Щойно механіка починає придушувати автономний вибір, гейміфікація втрачає мотиваційну функцію й перетворюється на різновид оманливої практики.

Підвищену небезпеку цього типу оманливих практик зумовлюють три взаємопов'язані чинники. По-перше, гейміфікація маскує комерційну мету під видимістю гри чи турботи про користувача, чим знижує його критичність і послаблює здатність розпізнати маніпуляцію. По-друге, вона особливо результативна щодо вразливих категорій, насамперед дітей і підлітків, чия здатність до самоконтролю ще не сформована. По-третє, на відміну від разового оману, гейміфікація діє накопичувально, поступово формуючи звичку та компульсивну поведінку. Саме цим пояснюється те, що проєкт Закону ЄС Про цифрову справедливість (Digital Fairness Act) [19] окремо виокремлює адиктивний дизайн як пріоритетний об'єкт регулювання, передбачаючи посилений захист неповнолітніх.

Запропонована типологія набуває аналітичної цінності лише за умови співвіднесення з конкретними, документально підтвердженими випадками. Найпоширеніші оманливі практики провідних цифрових платформ уже зафіксовано дослідниками й регуляторними органами, що дає змогу впорядкувати їх у вигляді матриці відповідності між видами практик і платформами, на яких їх виявлено рис. 4.

Найвиразніше поєднання фальшивої терміновості та штучного дефіциту демонструє маркетплейс Temu. У його інтерфейсі зафіксовано таймери зворотного відліку, що створюють відчуття невідкладності, повідомлення про вичерпання запасу за фактичної доступності того самого товару, а також ігрову механіку «колеса фортуни» з гарантованим «подарунком», який розблоковується лише після купівлі або в межах штучно обмеженого часового вікна. Таке нашарування механік спрямоване на придушення раціонального рішення на користь імпульсивної покупки.

Еталонним прикладом перешкоджання стала практика Amazon Prime. Легкому, майже автоматичному оформленню підписки протиставлявся навмисно ускладнений процес її скасування, який компанія

ISSN (Online): 3083-7782
Електронний науковий журнал «ЕКОНОМІЧНА ПАРАДИГМА»

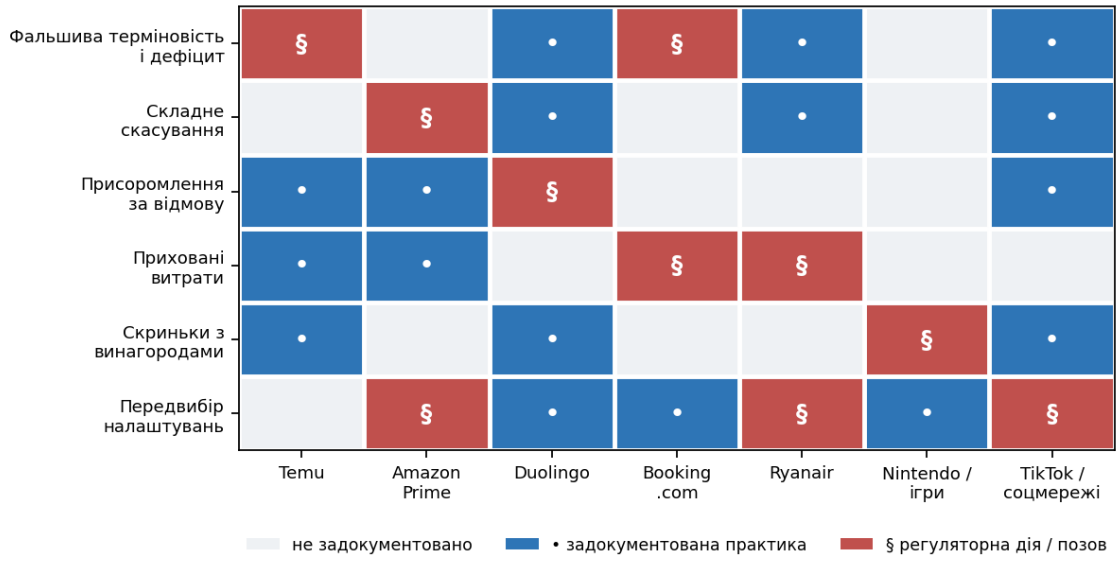

Рис. 4. Матриця відповідності оманливих практик і цифрових платформ
Джерело: складено автором самостійно

у внутрішніх документах називала «Iliad». Підсумком розслідування стало рекордне врегулювання з ФТК на суму 2,5 млрд. дол. та структурні зобов'язання щодо симетричності процедур оформлення й скасування підписки [20].

Показовими у сфері туристичних онлайн-сервісів є практики Booking.com і Ryanair. Перший тривалий час застосовував сигнали штучного дефіциту на кшталт повідомлень про останній доступний номер чи кількість осіб, які переглядають пропозицію, і лише після втручання європейських регуляторів зобов'язався відображати винятково достовірні дані. Другий вдавався до приховування витрат, додаючи страхування та пріоритетну посадку за замовчуванням, що згодом, під тиском скарг і регуляторів, було замінено на активний вибір користувача.

Окремої уваги заслуговує платформа Duolingo, що ілюструє сіру зону гейміфікації. Поєднання емоційно забарвлених стріків, фіктивного соціального тиску, проміжної валюти та обмежених у часі знижок на підписку робить цей приклад цінним саме своєю неоднозначністю: він демонструє, що не всяка інтенсивна гейміфікація автоматично є обманом і що її оцінка потребує тесту автономії, а не простого підрахунку застосованих механік.

Соціальні платформи також застосовують механіки захоплення уваги, через нескінченну стрічку, автоматичне відтворення контенту та усунення природних точок зупинки, що спираються на той самий принцип змінних винагород, який лежить в основі грального автомата, задля максимізації часу користувача в застосунку. До цього додаються і маніпулятивні налаштування конфіденційності за замовчуванням, ілюстрацією яких є справа TikTok, оштрафованого ірландським регулятором на 345 млн. євро за налаштування акаунтів неповнолітніх за замовчуванням на користь публічності [21].

Темні патерни перейшли з категорії поодиноких зловживань до категорії галузевої норми, про що свідчать постійні незалежні дослідження останніх років. Зокрема, поведінкове дослідження недобросовісних практик, проведене Європейською Комісією у 2022 році за методом «таємного покупця», виявило, що 97% найпопулярніших сайтів і застосунків, якими користуються споживачі ЄС, застосовували щонайменше один темний патерн. Найпоширенішими серед них виявилися приховування інформації та спотворення її ієрархії, вибір за замовчуванням, нав'язливість, ускладнене скасування й примусова реєстрація [22].

Подальшу динаміку засвідчила перевірка, проведена у 2024 році ФТК спільно з міжнародними мережами ICPEN і GPEN, що охопила 642 підписні сервіси у 26 країнах. За її результатами, 75,7% сервісів використовували щонайменше один темний патерн, а 66,8% — два і більше. Окремий зріз, присвячений захисту приватності, виявив наявність маніпулятивного патерну приблизно у 97% інтерфейсів за спроби користувача ухвалити рішення на користь приватності, окрім цього 81% сервісів застосовували автоматичне продовження підписки, а 70% не давали змоги вимкнути його безпосередньо під час оформлення купівлі [23; 24].

Зіставлення цих даних дає підстави для важливого висновку, що попри певне зниження показника в підписному сегменті порівняно з електронною комерцією, маніпулятивний дизайн залишається радше правилом, аніж винятком. Саме цим пояснюється перехід регуляторів від розгляду поодиноких справ до системного підходу в регулюванні (рис. 5).

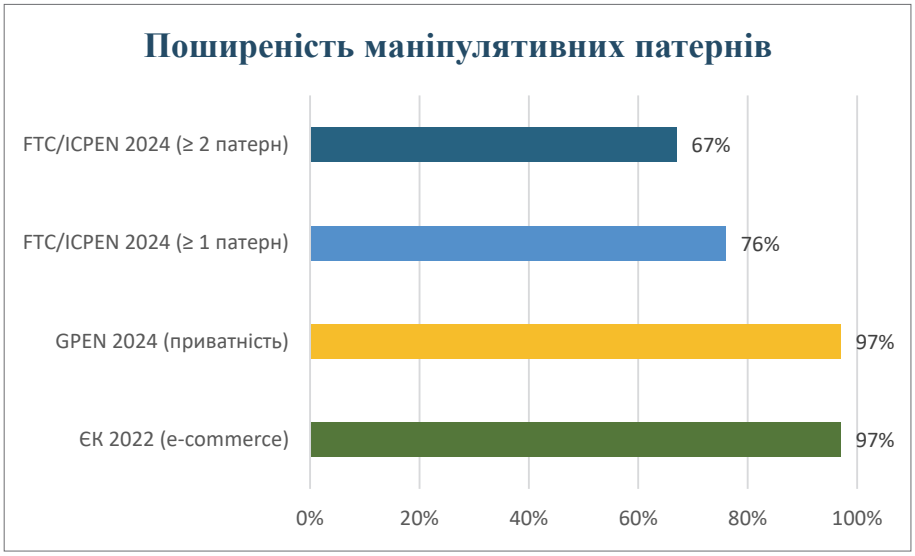

Рис. 5. Поширеність маніпулятивних патернів на платформах
Джерело: складено автором на основі [22–24]

Рекламне шахрайство, на відміну від темних патернів, спрямованих на окремого споживача, завдає шкоди ефективності рекламного ринку загалом. Водночас це найбільш кількісно вимірюваний прояв досліджуваної проблеми, хоча наявні оцінки помітно різняться, передусім через відмінності в методології та в самому трактуванні поняття недійсного трафіку. Так, втрати від рекламного шахрайства у 2025 році оцінюють у діапазоні від 32,6 млрд. дол. (за результатами аналізу Spider Labs, що охопив понад шість мільярдів кліків) до 41,4 млрд. дол. за попереднім звітом цієї ж компанії й навіть до 50 млрд. дол. за консервативними розрахунками Всесвітньої федерації рекламодавців [25–27]. Така амплітуда оцінок є симптоматичною, оскільки вона відображає непрозорість автоматизованого рекламного ланцюга, у якому точне вимірювання шахрайства залишається технічно складним.

За структурою недійсного трафіку переважає імітація кліків — 76,6%, за якою йдуть ботова активність і трафік центрів обробки даних. Тривожною тенденцією 2025 року стало чотирнадцятикратне зростання виявлених розміщень на ресурсах, створених виключно задля генерування показів, а також підвищений рівень шахрайства у форматі короткого відео — 12,79%, що приблизно у 2,7 раза перевищує середній показник рис. 6 [25].

Окремої уваги заслуговує ключовий парадокс доби штучного інтелекту, де автоматизація закупівлі реклами, покликана підвищити її ефективність, водночас знижує прозорість самого процесу. Що більшу частку рішень про ставки та розміщення ухвалює алгоритм, то складніше рекламодавцеві встановити, чи

Рис. 6. Структура недійсного трафіку за типами
Джерело: складено автором самостійно на основі [25]

навчається його кампанія на реальному споживчому інтересі, чи на недійсному трафіку. Показово, що за даними Spider Labs, у кампаніях, оптимізованих за допомогою штучного інтелекту, ризик шахрайства зростає вдвічі [25].

Якщо темні патерни маніпулюють вибором споживача, а рекламне шахрайство привласнює рекламні бюджети, то реклама на основі діпфейків підриває саму основу довіри, а саме здатність відрізнити справжнє повідомлення від фальшивого. Саме це робить її, ймовірно, найнебезпечнішим оманливим явищем цифрової доби.

За оцінкою Surfshark, у 2026 році на знаменитостей та урядовців припадало 52% усіх втрат від діпфейк-шахрайства — близько 1,13 млрд. дол., причому домінуючим сценарієм залишалися фальшиві інвестиційні рекомендації [28]. Компанія Deloitte прогнозує, що уможливлене штучним інтелектом шахрайство у США сягне 40 млрд. доларів до 2027 року [29], а Vectra AI зафіксувала зростання шахрайства з використанням генеративного штучного інтелекту на 1 210% упродовж 2025 року [30].

Аналіз задокументованих випадків дає змогу виокремити три найпоширеніші сценарії такого шахрайства. Перший і найбільш збитковий — інвестиційні та криптовалютні схеми, побудовані на фальшивих відео підприємців, бізнес-лідерів і політиків, що обіцяють швидке примноження капіталу. Зокрема, мешканка канадської провінції Онтаріо втратила близько 1,7 млн. дол., довірившись підробленому відео за участю Ілона Маска в соціальній мережі Facebook [31]. Другий сценарій — псевдомедичні «дива», тобто підроблені відеозвернення лікарів і знаменитостей, що рекламують непідтверджені засоби від діабету, гіпертензії та інших захворювань, нерідко супроводжувані фальшивими сертифікатами регуляторних органів. Третій пов'язаний із використанням образів знаменитостей у шахрайській рекламі.

Картину довершує підсилювальна роль самих платформ. За даними ФТК у 2021–2023 роках втрати від шахрайських схем, що починалися в соціальних мережах, сягнули 2,7 млрд. дол. США, перевищивши втрати за будь-яким іншим каналом первинного контакту з потерпілими. При цьому розслідування свідчать, що така реклама нерідко долає автоматичну модерацію й повторно з'являється навіть після блокування, що додатково ускладнює протидію цьому явищу [32].

Розглянуті вище масштаби й типологія оманливих практик закономірно ставлять питання про спроможність наявних регуляторних механізмів їм протидіяти. Порівняння підходів ЄС, США та України виявляє спільну для них мету, яка полягає у захисті автономії споживчого вибору, якої кожна з юрисдикцій прагне досягти власним шляхом і з неоднаковою швидкістю, відповідно до особливостей своєї правової традиції та інституційної архітектури.

Правова база ЄС у цій сфері наразі має багатошаровий характер, оскільки оманливі та маніпулятивні практики регулюються одночасно кількома актами. Директива про недобросовісні комерційні практики (2005/29/ЄС) встановлює загальну заборону таких практик у відносинах із споживачами на основі індивідуального аналізу кожного випадку [33]; стаття 25 Регламенту про цифрові послуги (2022/2065) прямо забороняє темні патерни в інтерфейсах онлайн-платформ [34]; стаття 7 Загального регламенту про захист даних унеможливлює маніпулятивне отримання згоди на обробку персональних даних [35]; а оновлена Директива про права споживачів запроваджує заборону темних патернів і механізм відкликання згоди у сфері дистанційних фінансових послуг [36].

Така множинність регуляторних інструментів створює ризик паралельного правозастосування й термінологічної неузгодженості, адже різні акти оперують відмінними поняттями від «примусу» та «введення в оману» до «маніпулювання» та «суттєвого спотворення» поведінки споживача. Відповіддю на цю фрагментацію має стати Закон про цифрову справедливість (Digital Fairness Act) — запланована горизонтальна ініціатива Європейської Комісії, спрямована проти темних патернів, оманливого маркетингу за участю лідерів думок, адиктивного дизайну та несправедливої персоналізації, з особливим захистом неповнолітніх.

На відміну від ЄС, США не мають єдиного спеціального закону про темні патерни й спираються натомість на параграф 5 Закону про Федеральну торгову комісію, що забороняє несправедливі або оманливі дії та практики, доповнений галузевими правилами [37]. Регуляторну стратегію тут визначає не нове законодавство, а активне правозастосування. У 2022 році Комісія оприлюднила доповідь «Висвітлюючи темні патерни» [38], після чого перейшла до серії показових стягнень, зокрема щодо Amazon Prime.

Врегулювання ФТК проти Amazon (вересень 2025 року) на 2,5 млрд. дол. стало найбільшим у історії у справах про темні патерни. Структурно вона складається з 1 млрд. дол. цивільного штрафу та 1,5 млрд. дол компенсацій споживачам. А право на відшкодування (приблизно по 51 долару) потенційно мають близько 35 млн. користувачів [39].

Особливої уваги заслуговує економічний контекст цього стягнення. Попри рекордний розмір, сума виявляється еквівалентною приблизно тридцяти трьом годинам продажів Amazon, що порушує принципове питання про достатність суто грошових санкцій як стримувального чинника. Саме тому поряд із фінансовими виплатами ФТК застосувала й структурні зобов'язання поведінкового характеру, а саме

вимогу про чітку кнопку відмови, прозоре розкриття умов підписки та спрощену процедуру її скасування, які в перспективі здатні вплинути на практику компанії суттєвіше, ніж сам штраф.

В Україні оманлива реклама регулюється переважно на перетині двох нормативно-правових актів: Закону «Про рекламу», що у статтях 9–10 забороняє недобросовісну та приховану рекламу [40], і Закону «Про захист від недобросовісної конкуренції», стаття 15–1 якого стосується поширення інформації, що вводить в оману [41]. Ключовим органом правозастосування є Антимонопольний комітет України, а санкція за наведення неправдивих даних у рекламі може сягати п'яти відсотків доходу компанії за попередній рік.

Практика АМКУ останніх років засвідчує посилення регуляторного тиску, особливо в сегменті дієтичних добавок і лікарських засобів, де найпоширенішим порушенням є приписування товарам неіснуючих лікувальних властивостей. Судова практика 2025–2026 років дедалі частіше підтримує позицію регулятора, визнаючи результати опитувань споживачів належним доказом введення в оману. Якщо у 2020 році сукупні штрафи у сфері недобросовісної конкуренції становили 218,8 млн. грн [42], то у 2025 році лише за напрямом дієтичних добавок АМКУ наклав 81,9 млн. грн у межах 16 рішень, визначивши цей ринок пріоритетним і на 2026 рік [43]. Водночас Україна перебуває у процесі адаптації національного законодавства до правової бази ЄС, що передбачає поступове наближення до його стандартів.

Висновки і перспективи подальших досліджень. Підсумовуючи, оманливі практики у цифровому середовищі є не сукупністю поодиноких зловживань, а структурною характеристикою сучасних цифрових ринків, що потребує системного, а не епізодичного підходу до її осмислення. Запропонована багаторівнева типологія, яка охоплює рівні повідомлення, інтерфейсу, ринкової екосистеми та синтетичного контенту, разом із виокремленням оманливої гейміфікації як самостійного феномену, дає змогу впорядкувати різноманіття таких практик у єдину аналітичну систему. Порівняльний аналіз засвідчив конвергенцію регуляторних підходів трьох юрисдикцій навколо спільної мети — захисту автономії споживчого вибору, а також перехід від декларативних застережень до дієвих фінансових і структурних санкцій, що мають доповнювати одне одного задля досягнення стримувального ефекту.

У подальших наукових дослідженнях пропонується зосередити увагу на вивченні стійкості автономних систем штучного інтелекту до впливу темних патернів, кількісному оцінюванні непрямих витрат сумлінних учасників ринку на протидію оманливим практикам, а також на гармонізації українського законодавства з правом ЄС у частині регулювання темних патернів і оманливої гейміфікації. Це надасть змогу вдосконалити нормативно-правове забезпечення та правозастосовну практику у сфері захисту прав споживачів у цифровому середовищі.

ДОДАТКОВА ІНФОРМАЦІЯ

ФІНАНСУВАННЯ: Автори не отримували фінансування для цього дослідження.
ЗАЯВА ПРО ДОСТУПНІСТЬ ДАНИХ: Не застосовується.
КОНФЛІКТ ІНТЕРЕСІВ: Автори заявляють про відсутність конфлікту інтересів.

Література

1. Gupta A. Deceptive advertising, regulation and naive consumers. *International Journal of Industrial Organization*. 2023. Vol. 91. Article 102992. DOI: https://doi.org/10.1016/j.ijindorg.2023.102992

2. Baumeister J., Park J.-Y., Cunningham A., Von Itzstein S., Gwilt I., Davis A., Walsh J. Patterns in the Dark: Deceptive Practices in Online Interactions. Landscape Assessment: Dark Patterns. A Report to the Data Standards Chair. Adelaide: University of South Australia, 2024. 92 p. URL: https://dsb.gov.au/sites/dsb.gov.au/files/2024–11/report-patterns-in-the-dark.pdf (дата звернення: 12.04.2026).

3. Anselmo G., Mannaioli G., Sardo A. Ensuring Fairness in the Digital Marketplace: A Communicative and Cognitive Analysis of Deceitful Influencer Marketing within Regulatory Frameworks and Benchmarks. *International Journal for the Semiotics of Law*. 2026. Vol. 39, No. 1. P. 189–224. DOI: https://doi.org/10.1007/s11196-025-10290-z

4. Benaouda S., Saber R. Legal Protection Mechanisms for Electronic Consumers from Misleading Advertising. *Law and World*. 2025. Vol. 11, No. 36. P. 151–164. DOI: https://doi.org/10.36475/11.4.8

5. Sanetra-Polgrabi S., Tetlak Z. Consumer Protection in Advertising of the Future in the Context of Economic Instability. *Futurity Economics&Law*. 2022. Vol. 2, No. 3. P. 25–45. DOI: https://doi.org/10.57125/FEL.2022.09.25.02

6. Bothma M., Van Staden B. The influence of perceived deceptive advertising on consumer behaviour in the online fashion environment: A stimulus-organism-response perspective. *South African Journal of Economic and Management Sciences*. 2025. Vol. 28, No. 1. Article a6398. DOI: https://doi.org/10.4102/sajems.v28i1.6398

7. Digital Advertising Market Size, Share & Trends Analysis Report, 2026–2033. *Grand View Research*. 2026. URL: https://www.grandviewresearch.com/industry-analysis/digital-advertising-market-report (дата звернення: 14.04.2026).

8. Digital Advertising — Worldwide. *Statista Market Forecast.* 2025. URL: https://www.statista.com/outlook/dmo/digital-advertising/worldwide (дата звернення: 14.04.2026).

9. Digital Advertising Statistics 2026: 180+ Data Points. *DigitalApplied.* 2026. URL: https://www.digitalapplied.com/blog/digital-advertising-statistics-2026-data-points (дата звернення: 16.04.2026).

10. Digital Advertising Statistics 2026: 92+ Stats & Insights. *Marketing LTB.* 2026. URL: https://marketingltb.com/blog/statistics/digital-advertising-statistics/ (дата звернення: 16.04.2026).

11. WFA warns that ad fraud will hit $50bn a year by 2025. *The Drum.* 2016. URL: https://www.thedrum.com/news/2016/06/06/wfa-warns-ad-fraud-will-hit-50bn-year-2025 (дата звернення: 14.04.2026).

12. *Dark commercial patterns*. OECD Digital Economy Papers. 2022. No. 336. DOI: https://doi.org/10.1787/44f5e846-en

13. *Bringing Dark Patterns to Light: An FTC Workshop*. 2021. URL: https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop

14. Gray C. M., Santos C., Bielova N., Mildner T. An Ontology of Dark Patterns Knowledge: Foundations, Definitions, and a Pathway for Shared Knowledge-Building. *Proceedings of the CHI Conference on Human Factors in Computing Systems.* 2024. DOI: https://doi.org/10.1145/3613904.3642436

15. Commerce platforms take corrective action after CCPA intervention against dark patterns. *Press Information Bureau.* 2024. URL: https://www.pib.gov.in/PressReleseDetailm.aspx? PRID=2086980 (дата звернення: 13.04.2026).

16. Testimonium Ltd. Confirmshaming. *Deceptive Design.* URL: https://deceptive.design/types/confirmshaming (дата звернення: 12.04.2026).

17. Abel L., Kaye L., Marques J., Parthasarathy V., Santos J., Sell A. Satori Threat Intelligence Alert: SlopAds Covers Fraud with Layers of Obfuscation. *HUMAN Security*. 2025. URL: https://www.humansecurity.com/learn/blog/satori-threat-intelligence-alert-slopads-covers-fraud-with-layers-of-obfuscation/ (дата звернення: 12.04.2026).

18. Elon Musk Deepfake Crypto Scam on YouTube. *OECD AI Incidents Monitor.* 2024. URL: https://oecd.ai/en/incidents/2024–06–23-c4e2 (дата звернення: 12.04.2026).

19. Commission launches open consultation on the forthcoming Digital Fairness Act. *European Commission.* 2025. URL: https://digital-strategy.ec.europa.eu/en/consultations/commission-launches-open-consultation-forthcoming-digital-fairness-act (дата звернення: 14.04.2026).

20. FTC Secures Historic $2.5 Billion Settlement Against Amazon. *Federal Trade Commission.* 2025. URL: https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-secures-historic-25-billion-settlement-against-amazon (дата звернення: 12.04.2026).

21. DPC announces €345 million fine of TikTok. *Data Protection Commission.* 2023. URL: https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok (дата звернення: 12.04.2026).

22. Directorate-General for Justice and Consumers. Behavioural study on unfair commercial practices in the digital environment: Dark patterns and manipulative personalisation: Final report. *European Commission.* URL: https://tinyurl.com/5xvu5yrc (дата звернення: 14.04.2026).

23. FTC, ICPEN, GPEN Announce Results of Review of Use of Dark Patterns Affecting Subscription Services, Privacy. *Federal Trade Commission.* 2024. URL: https://tinyurl.com/45dah9fs (дата звернення: 14.04.2026).

24. International Consumer Protection and Enforcement Network. Dark Patterns in Subscription Services Sweep: Public Report. 2024. URL: https://www.icpen.org/sites/default/files/2024–07/Public%20Report%20ICPEN%20Dark%20Patterns%20Sweep.pdf (дата звернення: 14.04.2026).

25. 2026 Ad Fraud White Paper Report. *Spider Labs Inc.* 2026. URL: https://spideraf.com/2026-annual-ad-fraud-white-paper (дата звернення: 12.04.2026).

26. Spider Labs Releases 2025 Ad Fraud Report: Estimated Global Losses Surpass $37.7 Billion. *Spider Labs Inc.* 2025. URL: https://spideraf.com/press-releases/spider-labs-releases-2025-ad-fraud-report-estimated-global-losses-surpass-37-7-billion (дата звернення: 12.04.2026).

27. The Hunt for Digital Decimals: Ad Fraud. *World Federation of Advertisers.* 2016. URL: https://wfanet.org/knowledge/item/2016/06/06/The-Hunt-for-Digital-Decimals-Ad-Fraud (дата звернення: 12.04.2026).

28. Deepfake scams: celebrities and government officials account for 52% of losses. *Surfshark.* 2026. URL: https://surfshark.com/research/deepfake-scams (дата звернення: 12.04.2026).

29. AI-enabled fraud: The next wave of financial crime. *Deloitte Center for Financial Services.* 2024. URL: https://www2.deloitte.com/us/en/insights/industry/financial-services/ai-enabled-financial-fraud.html (дата звернення: 16.04.2026).

30. The State of AI Cybersecurity Report 2025. *Vectra AI.* 2025. URL: https://www.vectra.ai/reports/state-of-ai-cybersecurity-2025 (дата звернення: 16.04.2026).

31. Ontarian loses $1.7M in a crypto scam that used an AI-generated deepfake of Elon Musk. *Yahoo Finance Canada.* 2026. URL: https://ca.finance.yahoo.com/news/ontarian-loses-1-7m-crypto-130800904.html (дата звернення: 18.04.2026).

32. FTC Data Shows Consumers Report Losing $2.7 Billion to Social Media Scams Since 2021. *Federal Trade Commission.* 2023. URL: https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-data-shows-consumers-report-losing-27-billion-social-media-scams-2021 (дата звернення: 12.04.2026).

33. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive). *European Parliament and the Council of the European Union.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-:32005L0029 (дата звернення: 14.04.2026).

34. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). *European Parliament and the Council of the European Union.* URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/en (дата звернення: 12.04.2026).

35. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection. *European Parliament and the Council of the European Union.* URL*:* https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 16.04.2026).

36. Directive (EU) 2023/2673 of the European Parliament and of the Council of 22 November 2023 amending Directive 2011/83/EU as regards financial services contracts concluded at a distance and repealing Directive 2002/65/EC. *European Parliament and the Council of the European Union.* URL: https://eur-lex.europa.eu/eli/dir/2023/2673/oj/en (дата звернення: 16.04.2026).

37. Federal Trade Commission Act. 15 U.S.C. § § 41–58. *United States Congress.* URL: https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter2&edition=prelim (дата звернення: 12.04.2026).

38. Bringing Dark Patterns to Light. *Federal Trade Commission.* 2022. URL: https://www.ftc.gov/reports/bringing-dark-patterns-light (дата звернення: 16.04.2026).

39. Federal Trade Commission v. Amazon.com, Inc. Settlement. 2025. URL: https://www.subscriptionmembershipsettlement.com (дата звернення: 17.04.2026).

40. Про рекламу : Закон України від 03.07.1996 № 270/96-ВР. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80 (дата звернення: 14.04.2026).

41. Про захист від недобросовісної конкуренції : Закон України від 07.06.1996 № 236/96-ВР. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80 (дата звернення: 14.04.2026).

42. Звіт Антимонопольного комітету України за 2020 рік. *Антимонопольний комітет України.* 2021. URL: https://amcu.gov.ua/static-objects/amcu/uploads/public/605/4a0/e26/6054a0e268fc0702551413.pdf (дата звернення: 13.04.2026).

43. АМКУ схвалив Звіт про виконання заходів в рамках реалізації пріоритетів за 2025 рік. *Антимонопольний комітет України*. 2026. URL: https://amcu.gov.ua/news/amku-skhvalyv-zvit-pro-vykonannia-zakhodiv-v-ramkakh-realizatsii-priorytetiv-za-2025-rik (дата звернення: 13.04.2026).

References

1. Gupta, A. (2023). Deceptive advertising, regulation and naive consumers. *International Journal of Industrial Organization, 91*, Article 102992. https://doi.org/10.1016/j.ijindorg.2023.102992

2. Baumeister, J., Park, J.-Y., Cunningham, A., Von Itzstein, S., Gwilt, I., Davis, A., & Walsh, J. (2024). *Patterns in the dark: Deceptive practices in online interactions. Landscape assessment: Dark patterns* (Report to the Data Standards Chair). University of South Australia. https://dsb.gov.au/sites/dsb.gov.au/files/2024-11/report-patterns-in-the-dark.pdf

3. Anselmo, G., Mannaioli, G., & Sardo, A. (2026). Ensuring fairness in the digital marketplace: A communicative and cognitive analysis of deceitful influencer marketing within regulatory frameworks and benchmarks. *International Journal for the Semiotics of Law, 39*(1), 189–224. https://doi.org/10.1007/s11196-025-10290-z

4. Benaouda, S., & Saber, R. (2025). Legal protection mechanisms for electronic consumers from misleading advertising. *Law and World, 11*(36), 151–164. https://doi.org/10.36475/11.4.8

5. Sanetra-Polgrabi, S., & Tetlak, Z. (2022). Consumer protection in advertising of the future in the context of economic instability. *Futurity Economics & Law, 2*(3), 25–45. https://doi.org/10.57125/FEL.2022.09.25.02

6. Bothma, M., & Van Staden, B. (2025). The influence of perceived deceptive advertising on consumer behaviour in the online fashion environment: A stimulus-organism-response perspective. *South African Journal of Economic and Management Sciences, 28*(1), Article a6398. https://doi.org/10.4102/sajems.v28i1.6398

7. Grand View Research. (2026). *Digital advertising market size, share & trends analysis report, 2026–2033*. https://www.grandviewresearch.com/industry-analysis/digital-advertising-market-report

8. Statista. (2025). *Digital advertising — Worldwide*. Statista Market Forecast. https://www.statista.com/outlook/dmo/digital-advertising/worldwide

9. DigitalApplied. (2026). *Digital advertising statistics 2026: 180+ data points*. https://www.digitalapplied.com/blog/digital-advertising-statistics-2026-data-points

10. Marketing LTB. (2026). *Digital advertising statistics 2026: 92+ stats & insights*. https://marketingltb.com/blog/statistics/digital-advertising-statistics/

11. The Drum. (2016, June 6). *WFA warns that ad fraud will hit $50bn a year by 2025*. https://www.thedrum.com/news/2016/06/06/wfa-warns-ad-fraud-will-hit-50bn-year-2025

12. Organisation for Economic Co-operation and Development. (2022). *Dark commercial patterns* (OECD Digital Economy Papers No. 336). https://doi.org/10.1787/44f5e846-en

13. Federal Trade Commission. (2021). *Bringing dark patterns to light: An FTC workshop*. https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop

14. Gray, C. M., Santos, C., Bielova, N., & Mildner, T. (2024). An ontology of dark patterns knowledge: Foundations, definitions, and a pathway for shared knowledge-building. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3613904.3642436

15. Press Information Bureau. (2024). *Commerce platforms take corrective action after CCPA intervention against dark patterns*. https://www.pib.gov.in/PressReleseDetailm.aspx? PRID=2086980

16. Testimonium Ltd. (n.d.). *Confirmshaming*. Deceptive Design. https://deceptive.design/types/confirmshaming

17. Abel, L., Kaye, L., Marques, J., Parthasarathy, V., Santos, J., & Sell, A. (2025). *Satori threat intelligence alert: SlopAds covers fraud with layers of obfuscation*. HUMAN Security. https://www.humansecurity.com/learn/blog/satori-threat-intelligence-alert-slopads-covers-fraud-with-layers-of-obfuscation/

18. Organisation for Economic Co-operation and Development. (2024). *Elon Musk deepfake crypto scam on YouTube*. OECD AI Incidents Monitor. https://oecd.ai/en/incidents/2024-06-23-c4e2

19. European Commission. (2025). *Commission launches open consultation on the forthcoming Digital Fairness Act*. https://digital-strategy.ec.europa.eu/en/consultations/commission-launches-open-consultation-forthcoming-digital-fairness-act

20. Federal Trade Commission. (2025). *FTC secures historic $2.5 billion settlement against Amazon*. https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-secures-historic-25-billion-settlement-against-amazon

21. Data Protection Commission. (2023). *DPC announces €345 million fine of TikTok*. https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok

22. Directorate-General for Justice and Consumers. (n.d.). *Behavioural study on unfair commercial practices in the digital environment: Dark patterns and manipulative personalisation: Final report*. European Commission. https://tinyurl.com/5xvu5yrc

23. Federal Trade Commission. (2024). *FTC, ICPEN, GPEN announce results of review of use of dark patterns affecting subscription services, privacy*. https://tinyurl.com/45dah9fs

24. International Consumer Protection and Enforcement Network. (2024). *Dark patterns in subscription services sweep: Public report*. https://www.icpen.org/sites/default/files/2024–07/Public%20Report%20ICPEN%20Dark%20Patterns%20Sweep.pdf

25. Spider Labs Inc. (2026). *2026 ad fraud white paper report*. https://spideraf.com/2026-annual-ad-fraud-white-paper

26. Spider Labs Inc. (2025). *Spider Labs releases 2025 ad fraud report: Estimated global losses surpass $37.7 billion*. https://spideraf.com/press-releases/spider-labs-releases-2025-ad-fraud-report-estimated-global-losses-surpass-37-7-billion

27. World Federation of Advertisers. (2016). *The hunt for digital decimals: Ad fraud*. https://wfanet.org/knowledge/item/2016/06/06/The-Hunt-for-Digital-Decimals-Ad-Fraud

28. Surfshark. (2026). *Deepfake scams: Celebrities and government officials account for 52% of losses*. https://surfshark.com/research/deepfake-scams

29. Deloitte Center for Financial Services. (2024). *AI-enabled fraud: The next wave of financial crime*. https://www2.deloitte.com/us/en/insights/industry/financial-services/ai-enabled-financial-fraud.html

30. Vectra AI. (2025). *The state of AI cybersecurity report 2025*. https://www.vectra.ai/reports/state-of-ai-cybersecurity-2025

31. Yahoo Finance Canada. (2026). *Ontarian loses $1.7M in a crypto scam that used an AI-generated deepfake of Elon Musk*. https://ca.finance.yahoo.com/news/ontarian-loses-1–7m-crypto-130800904.html

32. Federal Trade Commission. (2023). *FTC data shows consumers report losing $2.7 billion to social media scams since 2021*. https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-data-shows-consumers-report-losing-27-billion-social-media-scams-2021

33. European Parliament and the Council of the European Union. (2005). *Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005L0029

34. European Parliament and the Council of the European Union. (2022). *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).* https://eur-lex.europa.eu/eli/reg/2022/2065/oj/en

35. European Parliament and the Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* https://eur-lex.europa.eu/eli/reg/2016/679/oj

36. European Parliament and the Council of the European Union. (2023). *Directive (EU) 2023/2673 of the European Parliament and of the Council of 22 November 2023 amending Directive 2011/83/EU as regards financial services contracts concluded at a distance and repealing Directive 2002/65/EC.* https://eur-lex.europa.eu/eli/dir/2023/2673/oj/en

37. United States Congress. (n.d.). *Federal Trade Commission Act* (15 U.S.C. § § 41–58). https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter2&edition=prelim

38. Federal Trade Commission. (2022). *Bringing dark patterns to light*. https://www.ftc.gov/reports/bringing-dark-patterns-light

39. Federal Trade Commission v. Amazon.com, Inc. (2025). *Settlement*. https://www.subscriptionmembershipsettlement.com

40. Verkhovna Rada Ukrainy. (1996, July 3). *Pro reklamu: Zakon Ukrainy vid 3 lypnia 1996 roku № 270/96-VR* [On Advertising: Law of Ukraine No. 270/96-VR of July 3, 1996]. https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80 [in Ukrainian].

41. Verkhovna Rada Ukrainy. (1996, June 7). *Pro zakhyst vid nedobrosovisnoi konkurentsii: Zakon Ukrainy vid 7 chervnia 1996 roku № 236/96-VR* [On Protection Against Unfair Competition: Law of Ukraine No. 236/96-VR of June 7, 1996]. https://zakon.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80 [in Ukrainian].

42. Antymonopolnyi komitet Ukrainy. (2021). *Zvit Antymonopolnoho komitetu Ukrainy za 2020 rik* [Annual Report of the Antimonopoly Committee of Ukraine for 2020]. https://amcu.gov.ua/static-objects/amcu/uploads/public/605/4a0/e26/6054a0e268fc0702551413.pdf [in Ukrainian].

43. Antymonopolnyi komitet Ukrainy. (2026). *AMKU skhvalyv Zvit pro vykonannia zakhodiv v ramkakh realizatsii priorytetiv za 2025 rik* [AMCU Approved the Report on the Implementation of Measures Within the Framework of the 2025 Priorities]. https://amcu.gov.ua/news/amku-skhvalyv-zvit-pro-vykonannia-zakhodiv-v-ramkakh-realizatsii-priorytetiv-za-2025-rik [in Ukrainian].

Дата першого надходження статті до видання: 30.04.2026
Дата прийняття статті до друку після рецензування: 25.05.2026
Дата публікації: 01.06.2026

ISSN (Online): 3083-7782
Електронний науковий журнал «ЕКОНОМІЧНА ПАРАДИГМА»

Hanovskyi Vasyl
PhD in Economics, Assistant of the Department of Economic Theory and Competition Policy State University of Trades and Economics

DECEPTIVE ADVERTISING PRACTICES IN THE DIGITAL ENVIRONMENT

Summary. *Introduction. Digital advertising has become the dominant media channel of our time, accounting for the majority of global advertising expenditure and characterised by global reach, process automation, and a high level of competition. The migration of the advertising industry to the online environment has altered the very nature of the relationship between advertiser and consumer: whereas in the traditional setting, deceptive advertising was largely confined to false claims about a product, in the digital environment, it acquires a systemic, architectural character. Deception now resides not only in the content of the message but also in the design of the interface, the sequence of steps, the manner in which prices are presented, the mechanisms for subscription enrolment, and so forth. The adoption of automated advertising procurement (programmatic advertising) and generative artificial intelligence has enhanced the effectiveness of targeting, yet it has simultaneously widened the scope for deceptive practices – from manipulative interface design and deceptive gamification to advertising fraud and deepfake advertising. There thus arises a clear need to determine the essence, typology, and regulatory boundaries of deceptive advertising practices in the digital environment from the economic, technological, and regulatory perspectives.*

Purpose. The purpose of the study is to elucidate the economic and legal foundations of deceptive advertising practices in the digital environment to systematise a multi-level typology of such practices and to identify them according to the level at which deception is effected, which makes it possible to differentiate regulatory approaches across individual jurisdictions and to formulate recommendations for regulators, businesses, and users.

Materials and methods. The materials of the study comprise: 1) the legal and regulatory framework governing deceptive advertising practices in the digital environment (in particular, the acts of the European Union, the United States, and Ukraine); 2) official materials of regulatory authorities and analytical data on the scale and prevalence of deceptive practices; 3) the works of domestic and foreign scholars in the field of the economics of digital markets, the protection of economic competition, and consumer protection.

In the course of the study, the following scientific methods were employed: theoretical generalisation and grouping (to construct a typology of deceptive practices and a taxonomy of dark patterns, as well as to distinguish deceptive gamification as a separate phenomenon); the comparative-legal method (to juxtapose the regulatory regimes of the EU, the United States, and Ukraine); the systemic-structural method and the case-study method (to analyse regulatory cases); formalisation, analysis, and synthesis (to establish the connections between the economic, technological, and legal dimensions of the phenomenon); and logical generalisation of the results (to formulate conclusions).

Results. The article elucidates the economic and legal nature and structure of deceptive advertising practices in the digital environment and proposes a multi-level typology thereof, constructed according to the criterion of the level at which deception is effected – namely, the

levels of the message, the interface, the market ecosystem, and synthetic content. The taxonomy of manipulative patterns is systematised by principal families; in addition, the study substantiates the case for distinguishing deceptive gamification as a separate object of inquiry, one that integrates the features of several families of manipulative design and engenders heightened risks for vulnerable categories of consumers, primarily minors. The place of deceptive practices within the system of economic relations among participants in the advertising market is determined, and the nature of the harm inflicted upon consumers, advertisers, and digital platforms is characterised. The thesis of the systemic, rather than episodic, character of the phenomenon under study is substantiated; a convergence of the regulatory approaches of the three jurisdictions is established, which, notwithstanding differences in institutional mechanisms, is subordinated to a common objective: safeguarding the autonomy of consumer choice.

Prospects. Further research is proposed to focus on examining the resilience of autonomous artificial-intelligence systems to the influence of dark patterns, on estimating the indirect costs borne by bona fide market participants in countering deceptive practices, and on an in-depth analysis of the harmonisation of Ukrainian legislation with that of the EU regarding the regulation of dark patterns and deceptive gamification, which are not yet directly governed by national law. This will make it possible to improve the legal and regulatory framework and enforcement practice in the sphere of consumer protection in the digital environment.

***Key words**: deceptive advertising, digital environment, dark patterns, deceptive gamification, advertising fraud, unfair competition, digital advertising market, deepfake.*