DOI: https://doi.org/10.25140/2411-5215-2026-1(45)-247-257
УДК 339.187.44:336.7:004
JEL Classification: G20, G32, E42, L81, L86, O33

Наталія Володимирівна Іванова
доктор економічних наук, професор, завідувач кафедри підприємництва і торгівлі
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: ivanova.nat.vlad@gmail.com. **ORCID:** http://orcid.org/0000-0001-6622-7310
ResearcherID: I-3574-2016

Андрій Анатолійович Бондаренко
аспірант
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: bondarenko_andrii@outlook.com. **ORCID:** https://orcid.org/0009-0006-3547-0864

РОЛЬ ІНФРАСТРУКТУРИ РИНКУ ФІНАНСОВИХ ПОСЛУГ У ФОРМУВАННІ ЦИФРОВОЇ ДОВІРИ ЯК ФАКТОРА КОНКУРЕНТОСПРОМОЖНОСТІ ПІДПРИЄМСТВ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

У статті узагальнено підходи до дефініції «цифрова довіра». Окреслено інфраструктурні фактори ринку фінансових послуг, які впливають на конкурентоспроможність підприємств електронної комерції. Виявлено зв'язок між конкурентоспроможністю та процесом формування цифрової довіри у сфері електронної комерції. Сформовано концепцію процесу управління конкурентоспроможністю підприємств електронної комерції, домінантами якої є ідентифікація складових цифрової довіри, форми прояву та варіанти прийняття рішень компанією. Сформульовано авторське трактування цифрової довіри як інтегрованого нематеріального ресурсу компанії.

***Ключові слова**: ринок фінансових послуг; інфраструктура; конкурентоспроможність; електронна комерція; диджиталізація; цифрові технології; цифрова довіра; підприємство; кредитна установа; управління ризиками.*
Рис.: 1. Табл.: 1. Бібл.: 25.

Постановка проблеми. Цифрова довіра як феномен цифрової економіки, попри ще доволі короткий термін існування, вже набув статусу стратегічного чинника конкурентоспроможності компаній у сфері електронної комерції. Особливо це відчутним є в умовах посилення глобальних викликів і трансформації «архітектури» міжнародних економічних відносин. З одного боку, e-commerce дедалі більше залежить від транскордонних цифрових платформ, платіжної інфраструктури, логістичних екосистем і обігу даних, але з іншого – зростає вразливість до кіберзагроз, шахрайських практик і ризиків репутаційних характерів. Саме в такому середовищі, повному цифрових суперечностей, довіра споживачів і партнерів до безпечності транзакцій, захисту персональних даних та прозорості цифрових процесів перетворюється на ресурс, який є ключовим фактором конкурентоспроможності, а саме: визначає здатність компанії утримувати клієнта, масштабувати діяльність і виходити на міжнародні ринки.

Аналіз останніх досліджень і публікацій. Аналіз останніх досліджень і публікацій як іноземних, так і вітчизняних учених засвідчує, що поняття «цифрова довіра» залишається міждисциплінарним і трактується різнобічно, залежно від предметної сфери. Так, у наукових роботах П. Пєтшака і Й. Такала акцентовано фрагментарність підходів та різну операціоналізацію, тоді як Ю. Савельєва і Т. Волкова пропонують інтегративне розуміння цього феномену як багатовимірної категорії, що поєднує безпеку, надійність, доброчесність, управлінські практики та користувацький досвід. Техніко-безпековий підхід до трактування «цифрової довіри» відстежується в роботах Р. Акрама і Р. Ко, які підкреслюють технологічну верифікацію та «доказовість» довіри, а поведінково-маркетинговий напрям (Р. Гохштайн, К. Гарлінг і Т. Перко) розглядає клієнтську цифрову довіру як чинник зниження сприйнятого ризику та підвищення ефективності цифрових комунікацій і лояльності. В українських наукових публікаціях цифрова довіра найчастіше інтерпрету-

ється як умова надійності цифрових сервісів, інституційної легітимності та безпечної цифрової взаємодії. Так, О. Зайцева, Г. Жосан пов'язують її з впливом соціальних мереж на споживчий вибір; К. Майстренко – зі стійкістю державних цифрових платформ у кризових умовах, С. Ольховий – із правовими механізмами електронної ідентифікації та цифрових підписів, Н. Жидовська, Л. Петришин і О. Прокопишин акцентують на прозорості та незмінності даних у контексті блокчейн-рішень, Є. Тіщенко, С. Зайчук і Т. Мустафаєв поєднують визначення цифрової довіри та кібербезпеки у трансформації фінансових сервісів, а С. Мехович, К. Молчанова і А. Лаушкін зазначають про доцільність використання індикаторів цифрової довіри в аналітиці цифровізації зовнішньоекономічної діяльності.

Незалежно від підходу, незаперечним фактором, який впливає на формування цифрової довіри, є стан та рівень розвитку інфраструктури фінансового ринку. В аспекті проблематики нашого дослідження слід відзначити роботи Д. Даффі, який досліджує системну важливість та стійкість ключових елементів фінансової інфраструктури, Г. Феррарині (аналіз регулювання фінансових ринкових інфраструктур і його вплив на трансформацію ринків після кризи), П. Сагуато (правові та регуляторні аспекти інфраструктури фінансового ринку), Девід А. Вішнік зосереджується на питаннях "реінжинірингу" фінансової ринкової інфраструктури, Д. Тюрінг фокусується на інфраструктурах посттрейдингу, ризиках і практиках функціонування платіжних, клірингових і розрахункових систем; Роберт С. Штайґервальд у своїх роботах досліджує центральних контрагентів як ключову частину фінансової ринкової інфраструктури та питання їхньої стійкості.

Вітчизняні вчені-економісти, серед яких можна зазначити М. Дубину, А. Дробязко, О. Попело, І. Рекуненко, І. Ситник, Н. Татарин, І. Чуницьку та інших, також приділяють значну увагу тенденціям розвитку інфраструктури банківського сегмента фінансового ринку.

Виділення недосліджених частин загальної проблеми. Наявність фрагментованих досліджень підтверджує актуальність подальшої концептуалізації цифрової довіри саме в площині конкурентоспроможності підприємств e-commerce. Проблема посилюється тим, що «ціна недовіри» в e-commerce має прямий економічний вимір. Витоки даних, атаки на платіжні сервіси, зростання частки fraud-операцій, а також недотримання регуляторних вимог щодо приватності та безпеки призводять не лише до короткострокових фінансових втрат, а й до довгострокового зниження конкурентних позицій через падіння конверсії, відтік клієнтів, здорожчання залучення, блокування каналів продажів і обмеження доступу до міжнародних партнерств. В умовах регуляторної фрагментації та ускладнення вимог до обігу даних комплаєнс дедалі частіше виступає не як «витратний» елемент, а як умова легітимної присутності на ринках і водночас як фактор конкурентної диференціації компанії.

Мета статті. Метою дослідження є теоретичне обґрунтування та визначення механізмів, через які цифрова довіра формує конкурентні переваги компаній електронної комерції. Об'єктом дослідження виступає процес формування конкурентоспроможності компаній e-commerce у цифровому середовищі, а предметом – прикладні аспекти, інструменти та механізми управління цифровою довірою як складової конкурентної стратегії. Для досягнення мети передбачено уточнення змісту категорії «цифрова довіра» в контексті електронної комерції, виявлення ключових ризиків і регуляторних чинників, а також формування підходів до оцінювання впливу довіри на результати діяльності компаній.

Виклад основного матеріалу. Еволюціонуючи, електронна комерція набула змін не лише в розвитку платформ, способів обробки та використання інформації та алгоритмах ухвалення рішень, але й стала середовищем появи нових або розширення сфери застосування звичних понять, як-от «довіра». Сьогодні цей термін трансформується з переважно міжосо-

бистісного феномену в системну характеристику цифрового середовища – «цифрову довіру». Огляд публікацій свідчить, що в науковому дискурсі досі немає єдиної дефініції, а саме поняття розгортається на перетині менеджменту, маркетингу, права та кібербезпеки.

У сучасній англомовній науковій літературі термін «digital trust» використовується як міждисциплінарна категорія, яка не має єдиного «канонічного» визначення і варіює залежно від дослідницької традиції. Так, P. Pietrzak та J. Takala у систематичному огляді підкреслюють фрагментованість підходів і відсутність базової дефініції, через що емпіричні роботи акцентують на процесному підході, аналізуючи «формування довіри», але опираються на різні трактування її сутності [1]. Натомість латвійські вчені J. Saveljeva та T. Volkova застосовують інтегральний підхід. Вони синтезують контур наявних визначень і визначають digital trust як «…багатовимірне явище, яке охоплює технічні, організаційні й користувацько-орієнтовані компоненти (зокрема безпеку, надійність, доброчесність та елементи управління та комплаєнсу)» [2]. Отже, закордонні вчені digital trust все частіше розглядають не як технічну категорію, а як інтегрований чинник, що забезпечує прийнятність і стійкість цифрової взаємодії.

Однак існує й техніко-орієнтований напрям досліджень, який інтерпретує digital trust як свого роду безпеку, що підтверджується технологічними механізмами та інституціями. Зокрема, британські вчені R.N. Akram та R.K.L. Ko розглядають digital trust крізь призму «secure trusted computing» і акцентують у своїй роботі, датованій 2014 роком, що в цифрових середовищах довіра має бути підтримана архітектурою безпеки, засобами верифікації та перевіреними обчислювальними механізмами; це відображає позицію, за якої довіра є результатом не лише соціальних очікувань, а й гарантованого технічного захисту [3]. Це дослідження є одним з перших, у яких згадується термін «digital trust». Така домінанта відстежується й у роботах про децентралізовані технології. Так, учений з ОАЕ D.D.H. Shin трактує блокчейн як середовище, у якому цифрова довіра формується через когнітивне сприйняття безпеки та приватності і трансформується в поведінкові наміри користувачів [4]. Отже, у такому вимірі дефініція digital trust є похідною від властивостей інфраструктури ринку фінансових послуг (стійкість, контроль доступу, захист даних), а втрата довіри пов'язується безпосередньо з ризиками інцидентів, шахрайства і компрометації інформації. І саме цей підхід ми вважаємо за один із найбільш актуальних в аспекті надання фінансових послуг у рамках електронної комерції, а отже, й одним із вагомих факторів конкурентоспроможності компаній e-commerce.

Виоремимо ще один, маркетингово-поведінковий напрям, який фокусується на digital trust як чиннику ухвалення рішень споживачем та ефективності комунікацій у цифрових каналах. Американські вчені R.E. Hochstein, C.M. Harmeling та T. Perko розвивають поняття *consumer digital trust* [5] і у своєму дослідженні показують, що цифрова довіра виступає важливою умовою результативності контенту, створеного самими користувачами. За їхньою позицією, довіра знижує рівень сприйнятого ризику в цифровій взаємодії та підвищує готовність споживача покладатися на інформаційні сигнали (відгуки, рекомендації), так звану «рекламу з вуст в уста», що прямо впливає на наміри та поведінку [5]. У такій логіці цифрова довіра стає не лише «захистом від негативу», а й маркетинговим активом, який підсилює конверсію та лояльність, і водночас є вразливою до порушень у прозорості, справедливості та надійності сервісу. Ця позиція узгоджується з інтегративним підходом, де digital trust містить і технічний, і управлінсько-комунікаційний виміри [2]. У маркетинговому дискурсі окреслюють свій підхід до цього питання і вітчизняні вчені О. Зайцева та Г. Жосан. У своїй роботі [6] вони трактують цифрову довіру як особливий тип довірчих відносин, який формується у цифровому середовищі між підписником й інфлюенсером та має «іншу природу», ніж у традиційній рекламі. Вчені розглядають її як основу нової логіки авторитету в соціальних мережах і підкреслюють її роль у прийнятті споживчих рішень [6].

Вивчення закордонного пулу публікацій наукових досліджень дозволило нам виокремити ще один напрям. Так, у менеджменті та дослідженнях інновацій digital trust розглядають як умову міжорганізаційної кооперації й розвитку екосистем. Китайські вчені J. Chen, W. Cai, J. Luo та H. Mao у своїй статті [7] обґрунтовують, що digital trust посилює відкриті інновації, зокрема через механізм обміну знаннями, а також залежить від цифрової зрілості організацій. Вони зазначають, що довіра функціонує як «соціально-технологічний клей», що зменшує бар'єри співпраці в цифровому середовищі. Водночас, але вже у площині цифрових бізнес-екосистем, I. Rychkova (Франція), J. Zdravkovic та J. Stirna (Швеція) підкреслюють релятивну природу довіри, а саме – відносини між цифровими сутностями – і пов'язується із впевненістю в здатності сторін захищати дані та приватність з огляду на потенційну можливість негативних наслідків [8]. Підбиваючи підсумки, відзначимо, що, на нашу думку, закордонні вчені схиляються до трактування digital trust як до комплексного феномену, який одночасно визначається безпекою та приватністю, управлінськими практиками, якістю цифрового сервісу та контекстом екосистемної взаємодії.

В українському науковому полі дефініція «цифрової довіри» формується здебільшого через міждисциплінарний підхід, який найчастіше пов'язують із зниженням ризиків у цифровій взаємодії та підвищенням передбачуваності цифрових сервісів. У публічному управлінні та дослідженнях диджиталізації державних послуг цифрова довіра інтерпретується як умова легітимності та стійкості державних цифрових сервісів у кризових умовах. Так, К. Майстренко [9], аналізуючи платформи «Дія» та «єДопомога», обґрунтовує, що в умовах загострення кібер- та енергетичних викликів цифрова довіра постає не менш важливим елементом безпеки, ніж фізичний захист критичної інфраструктури, і пов'язує її з прозорою та технологічно захищеною комунікацією держави й громадян. Актуальний у зв'язку з цим правовий аспект дефініції цифрової довіри розкривається через необхідність механізмів забезпечення прозорості та правової визначеності в онлайн-середовищі, а саме через застосування інструментів електронної ідентифікації та цифрові підписи. Зокрема, С. Ольховий у роботі про правове регулювання e-commerce прямо зазначає, що у світовій практиці активно розвивається концепт "digital trust", який передбачає використання засобів електронної ідентифікації та цифрових підписів для забезпечення прозорості онлайн-комерції, а для України підкреслює актуальність гармонізації норм із міжнародними стандартами [10].

У спорідненій інституційно-економічній логіці вчені Н. Жидовська, Л. Петришин та О. Прокопишин розглядають цифрову довіру як результат прозорості та незмінності даних [11]. У згаданій роботі автори показують, що застосування блокчейну в податковому адмініструванні здатне зміцнювати цифрову довіру між державою та бізнесом через децентралізований і прозорий облік операцій.

Нарешті, в економічних дослідженнях цифрової трансформації цифрову довіру дедалі частіше подають як параметр технологічного розвитку та конкурентоспроможності, який може фіксуватися через певні індикатори (індекси). Так, у своїй роботі Є. Тіщенко, С. Зайчук і Т. Мустафаєв у контексті трансформації фінансових послуг включають «цифрову довіру та кібербезпеку» до переліку ключових технологічних напрямів, що супроводжують модернізацію фінансової інфраструктури [12]. У своїй науковій роботі С. Мехович із співавторами апелює до міжнародних цифрових індексів, зокрема Digital Trust Index, і розглядає його як аналітичну рамку для обґрунтування можливостей і викликів цифровізації міжнародної торгівлі та підвищення прозорості процесів електронної комерції [13].

Визначення поняття «цифрова довіра», які наведені у роботах зазначених вище авторів та відображають різні підходи до трактування цього феномену, ми зібрали на рис. 1.

Цифрова довіра	«Впевненість у тому, що суб'єкт або цифрове середовище стабільно демонструє компетентність і надійність, підтримує робастну безпеку та безпечну архітектуру, діє чесно й справедливо, забезпечує позитивний користувацький досвід, дотримується норм управління/регуляторних вимог і гарантує аудитованість та простежуваність даних і операцій» [2].
	«Віра впевненості працівників, споживачів/покупців, партнерів та інших стейкхолдерів у здатності організації захищати дані та приватність/конфіденційність індивідів» [1].
	«Довіра, що формується та підтверджується технологічними засобами (повністю або частково), тобто через інструменти оцінювання та верифікації властивостей цифрових сутностей» [3].
	«Довіра до цифрових платформ і процесів, які забезпечують комунікацію та співпрацю, тобто впевненість у цифрових каналах/механізмах взаємодії, через які відбувається обмін і координація між сторонами» [7].
	«Тип відносин між сутностями у цифровому світі, який можна трактувати як міру впевненості довірителя (trustor) у здатності довіреної сторони (trustee) захищати дані та приватність людей у цифровій взаємодії» [8].
	«Впевненість користувачів у здатності людей, технологій і процесів формувати безпечний цифровий світ; при цьому ключовими критеріями (ядром) виступають безпека, конфіденційність і надійність» [14].
	«Очікування особи, що цифрові/віртуальні технології та послуги (і організації, які їх надають) захищатимуть інтереси всіх зацікавлених сторін і підтримуватимуть суспільні очікування та цінності» [15].

Рис. 1. Дефініції цифрової довіри, які базуються на різних підходах

Джерело: сформовано авторами.

Цифрова довіра у сфері електронної комерції формується як багатовимірна категорія, котра відображає ступінь упевненості клієнтів та партнерів у тому, що цифрові канали взаємодії є безпечними, а компанія e-commerce є передбачуваною, надійною та відповідальною щодо обігу даних і виконання зобов'язань. Підсумовуючи вищевикладений огляд підходів, зазначимо, що в сучасній науковій літературі цифрову довіру часто трактують як довіру до людей, процесів і технологій, спрямовану на забезпечення безпечного цифрового середовища; при цьому центральними складовими виступають захист даних і приватність. При цьому зауважимо також зростаючу значущість таких критеріїв довіри, як «відкритість» та «прозорість». В аспекті конкурентоспроможності підприємства на ринку e-commerce така інтерпретація є принциповою, оскільки транзакції відбуваються за умов інформаційної асиметрії, віддаленості сторін та високої залежності від інфраструктури (провайдерів фінансових послуг, маркетплейсів, логістики), а відтак довіра стає «містком» між наміром і фактичною покупкою.

Аналіз публікацій за результатами дослідження феномену цифрової довіри, вивчення підходів до дефініції поняття, а також цілі, завдання та архітектура нашого дослідження дозволила сформувати авторську дефініцію, як *інтегрованого нематеріального ресурсу і керованої здатності підприємства електронної комерції забезпечувати та підтверджувати безпечність, правомірність і передбачуваність на всіх етапах онлайн-взаємодії, що знижує ризики усіх сторін та трансформується у конкурентні переваги*.

На наше переконання, цифрова довіра в контексті забезпечення конкурентоспроможності e-commerce підприємств виступає як інтегральна характеристика та стратегічний нематеріальний актив, який впливає рівень упевненості стейкхолдерів (передусім, споживачів і партнерів) у надійності цифрової взаємодії з компанією. Одним з основних чинників, які обумовлюють її формування у сфері електронної комерції, є стан та рівень розвитку інфраструктури ринку фінансових послуг. Складовими цифрової довіри в такому аспекті є:

– узгоджена система управління кібербезпекою;

– захист персональних даних і приватність взаємодії, тобто цифрові канали взаємодії є надійними;

– комплаєнс, який забезпечує легітимність та доказовість цифрових процесів, а отже, дані захищені та використовуються доброчесно;

– траспарентність правил обслуговування, а принципи взаємодії прозорі та їх чітко дотримуються;

– операційна надійність сервісу на всіх етапах онлайн-транзакції (контакт, ідентифікація, оплата, доставка, підтримка, повернення), заявлена поведінка компанії в онлайні узгоджується з фактичними практиками.

У прикладному вимірі електронної комерції цифрова довіра проявляється через пакет керованих інфраструктурних послуг, серед яких: кібербезпека, стійкість платформ і фінансових сервісів, ідентифікація й автентифікація, приватність, захист персональних даних, прозорість цін, умов покупки, процедур повернення, репутаційні сигнали, доброчесність виконання зобов'язань (доставка, гарантія, підтримка) тощо (табл. 1).

Таблиця 1

Прикладні аспекти формування цифрової довіри як фактору конкурентоспроможності підприємств на ринку електронної комерції

Компонент цифрової довіри	Форма прояву	Дії компанії
Безпека	кіберзахист платформи або додатку	управління доступом до платформи або додатку, стійкість до атак і шахрайства, здатність компанії виявляти інциденти та реагувати на них без втрат для клієнта
Конфіденційність і приватність	правомірність збирання та обробки персональних даних	мінімізація даних, прозоре отримання згоди (consent), обмеження доступу, контроль життєвого циклу даних
Прозорість	зрозумілість правил взаємодії	Оголошення політики приватності, інформування про умови доставки повернення, пояснення використання даних, коректність повідомлень про ризики та інциденти
Надійність	стабільність роботи каналу продажів і виконання зобов'язань	Забезпечення доступності, швидкості, точності доставки, якість допродажної та післяпродажної підтримки
Етичність використання даних	відповідальне ставлення до клієнтської інформації поза межами формального комплаєнсу	недопущення маніпулятивних практик, надмірного профілювання, прихованого передавання даних третім сторонам тощо

Джерело: розроблено авторами.

Саме сукупність цих компонентів визначає, чи перетворюється цифровий контакт на стійкі довірчі відносини, чи, навпаки, провокує відмову від покупки або перехід до конкурентів.

Отже, для зростання рівня конкурентоспроможності підприємства e-commerce мають забезпечити управління цифровою довірою не у вигляді фрагментарних заходів безпеки, а на основі вибудованої цілісної системи політик, процесів, метрик і відповідальностей, котрі підсилюють прогнозованість взаємодії передусім для споживача. У такому вигляді цифрова довіра є не лише "емоційним бонусом" для клієнта, а стає вагомим економічним активом для компанії, оскільки зменшує транзакційні витрати та невизначеність для клієнта, забезпечує формування клієнтської лояльності (підвищує готовність здійснити покупку зараз та повторювати її в майбутньому), а також полегшує доступ компанії до маркетингової, логістичної та фінансової інфраструктури.

Значущість цифрової довіри як чинника конкурентоспроможності підкреслюють і сучасні тенденції на ринку електронної комерції, який у 2025 р. досяг 256 млрд грн і зріс приблизно на 7 %, а частка e-commerce в загальному ритейлі оцінюється на рівні 10 %

[16]. Поведінкові параметри попиту також свідчать про закріплення онлайн-звичок: у середньому на одного українця припадало 17,5 онлайн-покупки із середньою вартістю чека у 1320 грн [16]. Водночас конкурентне середовище в сегменті лідерів є висококонцентрованим. За результатами досліджень, 10 лідерів онлайн-ритейлерів за 9 місяців 2025 року отримали майже 40 млрд грн виторгу, з яких 76 % припадає на дві компанії корпоративної групи Rozetka [17]. Така концентрація підсилює значення цифрової довіри як конкурентної переваги, що належить до групи інфраструктурних факторів. Адже збої в безпеці, доступності або прозорості сервісу у лідерів мають не лише мікроекономічні наслідки, а й системно впливають на сприйняття надійності онлайн-покупок.

Платіжний контур є ключовою ланкою, де цифрова довіра матеріалізується в конверсії та виторгу. За даними НБУ, у 2025 році оплата товарів і послуг в інтернеті становила 13,9 % від кількості та 16,4 % від суми всіх безготівкових карткових операцій, що понад 1,2 млрд операцій на майже 770 млрд грн, а середня сума однієї онлайн-операції становила 608 грн [18]. Масштаб онлайн-платежів означає, що навіть «незначні» відносні втрати (зростання повернень коштів, падіння успішності завершення платежів, короткі простої платіжного маршруту) перетворюються на відчутні негативні економічні ефекти через втрату завершених транзакцій, підвищення витрат на врегулювання спорів та зниження повторних покупок.

Статистика стану інфраструктури фінансового ринку також дозволяє чітко окреслити, де саме концентруються ризики довіри. У 2024 році кількість шахрайських операцій із платіжними картками знизилась до 270 тис., але сума збитків зросла на 37 % (до 1,1 млрд грн). При цьому 83% випадків шахрайства відбулися в Інтернеті, а частка інтернет-шахрайства за сумою збитків становила 93 % [19]. Критичною є структура причин: 84 % збитків було спричинено соціальною інженерією, коли клієнти самостійно розголошують реквізити, коди або паролі. Це напряму пов’язується з етапами ланцюга цифрової довіри: маркетинг і перший контакт (фішинг і підміна бренду), ідентифікація (захоплення акаунтів), завершення платежу (authorized scams), підтримка (соцінженерія через комунікаційні канали). Європейський контекст лише підтверджує цей тренд – у звіті European Payments Council зазначається, що соціальна інженерія та фішинг зростають і залишаються інструментальними у платіжному шахрайстві [20].

Окремого акценту потребує порушення цифрової довіри у вимірі кіберінцидентів і залежності від третіх сторін. За даними IBM, середня глобальна вартість витоку даних у 2024 році досягла USD 4,88 млн (зростання на 10 %), причому ключовими драйверами зростання названо операційні простої та втрату продажів та витрати на реагування після інциденту [21]. Аналітичні звіти Verizon DBIR (Executive Summary) свідчать, що експлуатація вразливостей як вектор первинного доступу до інцидентів зросла до 20 %, а «вірус-вимагач» (який блокує доступ до файлів або системи та вимагає плату за відновлення доступу) був присутній у 44 % проаналізованих порушень [22]. Додатково фіксується посилення залежності від контрагентів: частка порушень, де залучено третю сторону, подвоїлась до 30 % [23]. Для процесів електронної комерції це є принциповим, оскільки ланцюг цифрової довіри об’єктивно спирається на інфраструктуру ринку: провайдерів платежів, логістику, хмарні сервіси, операційні технології сайтів та маркетплейси. Таким чином, управління конкурентоспроможністю має включати не лише «внутрішню» безпеку, а й керування ризиками постачальників.

Важливо уточнити, що цифрова довіра має процесну природу і формується на всіх етапах взаємодії. Тому, на наш погляд, для e-commerce доцільно використовувати поняття «*ланцюга цифрової довіри*» як послідовності стадій клієнтського шляху від першого контакту до доставки і післяпродажної підтримки, на кожній з яких діють «сигнали довіри» та «точки ризику». Саме процесний підхід у прикладному аспекті забезпечення

конкурентоспроможності компаній e-commerce дозволяє перейти від абстрактної категорії «цифрова довіра» до конкретних дій. Наприклад, компанія на основі управлінського аналізу може локалізувати, на якому саме етапі виникає ерозія довіри (наприклад, у checkout через підозрілий платіжний сценарій, або в поверненнях через непрозорі правила), і цілеспрямовано підсилювати слабкі місця, запроваджуючи відповідні механізми.

Висновки і пропозиції. Отже, цифрову довіру доцільно інтерпретувати як керований стратегічний ресурс, а ланцюг цифрової довіри – як процесний механізм, через який цей ресурс створюється, підтримується та трансформується у вимірювані конкурентні результати. На нашу думку, конкурентоспроможність e-commerce-компаній в Україні дедалі більше визначається здатністю керувати ризиками на кожному етапі ланцюга цифрової довіри (від бренд-захисту та антифішингових заходів до стійкості інфраструктури, антифроду, комплаєнсу й SLA сервісу), з урахуванням того, що головна зона втрат довіри формується в інтернет-каналах і посилюється соціальною інженерією.

Список використаних джерел

1. Pietrzak P., Takala J. Digital trust – a systematic literature review. *Forum Scientiae Oeconomia*. 2021. Vol. 9, No. 3. P. 59-71. URL: https://ojs.wsb.edu.pl/ index.php/fso/article/view/411.

2. Saveljeva J., Volkova T. A Survey on Digital Trust: Towards a Validated Definition. *Digital*. 2025. Vol. 5, No. 2. Art. 14. DOI: 10.3390/digital5020014.

3. Akram R. N., Ko R. K. L. Digital Trust – Trusted Computing and Beyond: A Position Paper. *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2014)*: proceedings. Beijing, China, 24-26 September 2014. P. 884-892. DOI: 10.1109/TrustCom.2014.116.

4. Shin D. H. Blockchain: The emerging technology of digital trust. *Telematics and Informatics.* 2019. Vol. 45. Art. 101278. DOI: 10.1016/j.tele.2019.101278.

5. 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*. 2025. Vol. 53, No. 4. P. 1034–1054. DOI: 10.1007/s11747-023-00982-y.

6. Зайцева О., Жосан Г. Вплив соціальних мереж на споживчий вибір. *Scientia fructuosa*. 2025. № 4(162). С. 150-162. DOI: 10.31617/1.2025(162)09.

7. Chen J., Cai W., Luo J., Mao H. How does digital trust boost open innovation? Evidence from a mixed approach. *Technological Forecasting and Social Change*. 2025. Vol. 212. Art. 123953. DOI: 10.1016/j.techfore.2024.123953.

8. Rychkova I., Zdravkovic J., Stirna J. Implications of trust in digital business ecosystem design: A systematic analysis of roles. *CEUR Workshop Proceedings*. 2023. Vol. 3645. P. 1-15. URL: https://ceur-ws.org/Vol-3645/forum2.pdf.

9. Майстренко К. М. Цифрові платформи «єДопомога» та «Дія» як фактор кібер- та енергетичної безпеки соціальної сфери в Україні. *Право та державне управління*. 2025. № 2. С. 215–221. DOI: 10.32782/pdu.2025.2.29.

10. Ольховий С. В. Правове регулювання ринку електронної комерції в Україні та світі. *Держава та регіони. Серія: Економіка та підприємництво*. 2025. № 1(135). С. 94-98. DOI: 10.32782/1814-1161/2025-1-16.

11. Жидовська Н. М., Петришин Л. П., Прокопишин О. С. Ефективність впровадження блокчейн-технологій у системі оподаткування суб'єктів господарювання. *Актуальні питання економічних наук*. 2025. № 10. 20 с. DOI: 10.5281/zenodo.15228009.

12. Тіщенко Є. О., Зайчук С. В., Мустафаєв Т. Т. Трансформація фінансових послуг в умовах повоєнної відбудови. *Економіка та суспільство*. 2025. Вип. 74. С. 114–122. DOI: 10.32782/2524-0072/2025-74-16.

13. Мехович С. А., Молчанова К. М., Лаушкін А. М. Підходи до вирішення проблем цифрових перетворень у зовнішньоекономічній діяльності вітчизняних підприємств. *Енергозбереження. Енергетика. Енергоаудит*. 2026. № 1(216). С. 88–113. DOI: 10.20998/2313-8890.2026.01.07.

14. Стороженко Л. Г., Власенко В. О. Цифрова готовність суспільства як компонент формування нетократичного публічного управління. *Актуальні питання у сучасній науці*. 2024. № 2(20). С. 330-341. DOI: 10.52058/2786-6300-2024-2(20)-330-341.

15. Дехтяр Н. А. Використання технологій метавсесвіту у процесі цифровізації туристичної діяльності. *Економіка та суспільство*. 2024. Вип. 69. DOI: 10.32782/2524-0072/2024-69-76.

16. Українці за 2025 рік витратили на онлайн-покупки 256 млрд грн. *Мінфін*. 22.01.2026. URL: https://minfin.com.ua/ua/2026/01/22/166722098/.

17. Ukrainian Retail Association (RAU). Український e-commerce в 2025 році: виручка лідерів та статистика галузі (дослідження YouControl.Market). 2026. URL: https://rau.ua/news/ukrayinskyyi-e-commerce-v-2025-rotci-vyruchka-lideriv-ta-statystyka-galuzi-doslidzhennia-youcontrol.market/.

18. Операції з платіжними картками у 2025 році: більшість – безготівкові. *Національний банк України.* 16.02.2026. URL: https://bank.gov.ua/ua/news/all/operatsiyi-z-platijnimi-kartkami-u-2025-rotsi-bilshist--bezgotivkovi.

19. Кількість випадків шахрайства з картками знизилася, збитки за ними – зросли. *Національний банк України*. 12.05.2025. URL: https://bank.gov.ua/ua/news/all/kilkist-vipadkiv-shahraystva-z-kartkami-znizilasya-zbitki-za-nimi--zrosli.

20. European Payments Council. 2024 Payments Threats and Fraud Trends Report. EPC162-24. Version 1.0. Date issued: 22/11/2024. URL: https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2024-12/EPC162-24%20v1.0%202024%20Payments%20Threats%20and%20Fraud%20Trends%20Report_0.pdf.

21. IBM Security. Cost of a Data Breach Report 2024. 2024. URL: https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf.

22. Verizon. 2025 Data Breach Investigations Report (DBIR): Executive Summary. 2025. URL: https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf.

23. Державна служба спеціального зв'язку та захисту інформації України; Державний центр кіберзахисту; Оперативний центр реагування на кіберінциденти. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: річний звіт. 2024. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006.

24. Дубина М., Устименко Я. Теоретичні положення обґрунтування сутності банківської цифрової інфраструктури. *Проблеми і перспективи економіки та управління*. 2025. № 2(42). С. 274–285. https://doi.org/10.25140/2411-5215-2025-2(42)-274-285.

25. Tulchynska S., Popelo O., Solosich O., Kasianova N., Kostiunik O., Shchepina T. Artificial intellectualization in the assessment system of the safe development of economic entities. *Journal of Theoretical and Applied Information Technology*. 2024. № 102(8). P. 3323-3334. https://www.jatit.org/volumes/Vol102No8/6Vol102No8.pdf.

References

1. Pietrzak, P., & Takala, J. (2021). Digital trust – a systematic literature review. *Forum Scientiae Oeconomia, 9*(3), 59-71. https://doi.org/10.23762/FSO_VOL9_NO3_4

2. Saveljeva, J., & Volkova, T. (2025). A survey on digital trust: Towards a validated definition. *Digital, 5*(2), Article 14. https://doi.org/10.3390/digital5020014

3. Akram, R. N., & Ko, R. K. L. (2014). Digital trust - Trusted computing and beyond: A position paper. In *Proceedings of the 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2014)* (pp. 884-892). IEEE. https://doi.org/10.1109/TrustCom.2014.116.

4. Shin, D. H. (2019). Blockchain: The emerging technology of digital trust. *Telematics and Informatics, 45*, 101278. https://doi.org/10.1016/j.tele.2019.101278.

5. Hochstein, R. E., Harmeling, C. M., & Perko, T. (2025). 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, 53*(4), 1034-1054. https://doi.org/10.1007/s11747-023-00982-y.

6. Zaitseva, O., & Zhosan, H. (2025). Vplyv sotsialnykh merezh na spozhyvchyi vybir [The impact of social networks on consumer choice]. *Scientia fructuosa – Scientia fructuosa*, (4(162)), 150-162. https://doi.org/10.31617/1.2025(162)09.

7. Chen, J., Cai, W., Luo, J., & Mao, H. (2025). How does digital trust boost open innovation? Evidence from a mixed approach. *Technological Forecasting and Social Change, 212*, 123953. https://doi.org/10.1016/j.techfore.2024.123953.

8. Rychkova, I., Zdravkovic, J., & Stirna, J. (2023). Implications of trust in digital business ecosystem design: A systematic analysis of roles. In *CEUR Workshop Proceedings* (Vol. 3645, pp. 1-15). https://ceur-ws.org/Vol-3645/forum2.pdf.

9. Maistrenko, K. M. (2025). Tsyfrovi platformy «ieDopomoha» ta «Diia» yak faktor kiber- ta enerhetychnoi bezpeky sotsialnoi sfery v Ukraini [Digital platforms "eAid" and "Diia" as a factor of cyber and energy security of the social sphere in Ukraine]. *Pravo ta derzhavne upravlinnia – Law and Public Administration*, (2), 215-221. https://doi.org/10.32782/pdu.2025.2.29.

10. Olkhovyi, S. V. (2025). Pravove rehuliuvannia rynku elektronnoi komertsii v Ukraini ta sviti [Legal regulation of the e-commerce market in Ukraine and worldwide]. *Derzhava ta rehiony. Seriia: Ekonomika ta pidpryiemnytstvo – State and Regions. Series: Economics and Entrepreneurship*, (1(135)), 94-98. https://doi.org/10.32782/1814-1161/2025-1-16.

11. Zhydovska, N. M., Petryshyn, L. P., & Prokopyshyn, O. S. (2025). Efektyvnist vprovadzhennia blokchein-tekhnolohii u systemi opodatkuvannia subiektiv hospodariuvannia [Efficiency of implementing blockchain technologies in the taxation system of business entities]. *Aktualni pytannia ekonomichnykh nauk – Current Issues of Economic Sciences*, (10), 1-20. https://doi.org/10.5281/zenodo.15228009.

12. Tishchenko, Ye. O., Zaichuk, S. V., & Mustafaiev, T. T. (2025). Transformatsiia finansovykh posluh v umovakh povoiennoi vidbudovy [Transformation of financial services in the context of post-war recovery]. *Ekonomika ta suspilstvo – Economy and Society*, (74), 114–122. https://doi.org/10.32782/2524-0072/2025-74-16.

13. Mekhovych, S. A., Molchanova, K. M., & Laushkin, A. M. (2026). Pidkhody do vyrishennia problem tsyfrovykh peretvoren u zovnishnoekonomichnii diialnosti vitchyznianykh pidpryiemstv [Approaches to solving problems of digital transformations in the foreign economic activity of domestic enterprises]. *Enerhozberezhennia. Enerhetyka. Enerhoaudyt – Energy Saving. Power Engineering. Energy Audit*, (1(216)), 88–113. https://doi.org/10.20998/2313-8890.2026.01.07.

14. Storozhenko, L. H., & Vlasenko, V. O. (2024). Tsyfrova hotovnist suspilstva yak komponent formuvannia netokratychnoho publichnoho upravlinnia [Digital readiness of society as a component of forming netocratic public administration]. *Aktualni pytannia u suchasnii nautsi – Current Issues in Modern Science*, (2(20)), 330–341. https://doi.org/10.52058/2786-6300-2024-2(20)-330-341.

15. Dekhtiar, N. A. (2024). Vykorystannia tekhnolohii metavsestu u protsesi tsyfrovizatsii turystychnoi diialnosti [Use of metaverse technologies in the process of digitalization of tourism activity]. *Ekonomika ta suspilstvo – Economy and Society*, (69). https://doi.org/10.32782/2524-0072/2024-69-76.

16. Minfin. (2026, January 22). *Ukraintsi za 2025 rik vytratyly na onlain-pokupky 256 mlrd hrn [Ukrainians spent UAH 256 billion on online purchases in 2025].* https://minfin.com.ua/ua/2026/01/22/166722098/.

17. Ukrainian Retail Association (RAU). (2026). *Ukrainskyi e-commerce v 2025 rotsi: vyruchka lideriv ta statystyka haluzi (doslidzhennia YouControl.Market) [Ukrainian e-commerce in 2025: leaders' revenue and industry statistics (YouControl.Market study)].* https://rau.ua/news/ukrayinskyyi-e-commerce-v-2025-rotci-vyruchka-lideriv-ta-statystyka-galuzi-doslidzhennia-youcontrol.market/.

18. Natsionalnyi bank Ukrainy. (2026, February 16). *Operatsii z platizhnymy kartkamy u 2025 rotsi: bilshist – bezghotivkovi [Payment card transactions in 2025: most are cashless].* https://bank.gov.ua/ua/news/all/operatsiyi-z-platijnimi-kartkami-u-2025-rotsi-bilshist--bezgotivkovi.

19. Natsionalnyi bank Ukrainy. (2025, May 12). *Kilkist vypadkiv shakhraistva z kartkamy znyzylasia, zbytky za nymy – zrosly [The number of card fraud cases decreased, but losses increased].* https://bank.gov.ua/ua/news/all/kilkist-vipadkiv-shahraystva-z-kartkami-znizilasya-zbitki-za-nimi--zrosli.

20. European Payments Council. (2024). *2024 payments threats and fraud trends report* (EPC162-24, Version 1.0; issued November 22, 2024). https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2024-12/EPC162-24%20v1.0%202024%20Payments%20Threats%20and%20Fraud%20Trends%20Report_0.pdf.

21. IBM Security. (2024). *Cost of a data breach report 2024*. https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf.

22. Verizon. (2025). *2025 data breach investigations report (DBIR): Executive summary*. https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf.

23. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy; Derzhavnyi tsentr kiberzakhystu; Operatyvnyi tsentr reahuvannia na kiberintsydenty. (2024). *Systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky: richnyi zvit [Vulnerability detection and response to cyber incidents and cyberattacks: Annual report]*. https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006.

24. Dubyna, M., & Ustymenko, Ya. (2025). Teoretychni polozhennya obgruntuvannya sutnosti bankivskoyi tsyfrovoyi infrastruktury [Theoretical provisions substantiating the essence of banking digital infrastructure]. *Problemy i perspektyvy ekonomiky ta upravlinnya – Problems and prospects of economics and management*, (2 (42), 274-285. URL: https://doi.org/10.25140/2411-5215-2025-2(42)-274-285.

25. Tulchynska, S., Popelo, O., Solosich, O., Kasianova, N., Kostiunik, O., Shchepina, T. (2024). Artificial intellectualization in the assessment system of the safe development of economic entities. *Journal of Theoretical and Applied Information Technology*, 102(8), 3323-3334. https://www.jatit.org/volumes/Vol102No8/6Vol102No8.pdf.

Дата першого надходження статті до видання: 06.02.2026
Дата прийняття статті до друку після рецензування: 12.02.2026

UDC 339.187.44:336.7:004

Nataliia Ivanova

Doctor of Economic Sciences, Professor, Head of Department of Entrepreneurship and Trade
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: ivanova.nat.vlad@gmail.com. **ORCID:** http://orcid.org/0000-0001-6622-7310
ResearcherID: I-3574-2016

Andrii Bondarenko

PhD student
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: bondarenko_andrii@outlook.com. **ORCID:** https://orcid.org/0009-0006-3547-0864

THE ROLE OF FINANCIAL SERVICES MARKET INFRASTRUCTURE IN BUILDING DIGITAL TRUST AS A COMPETITIVENESS FACTOR FOR E-COMMERCE FIRMS

This paper examines digital trust as a strategic driver of competitiveness for e-commerce firms and argues that its formation is conditioned by the infrastructure of the financial services market. Based on a structured review of recent English-language and Ukrainian research, the article systematizes major conceptual approaches to "digital trust" (integrative socio-technical, security and trusted-computing, consumer and marketing, and ecosystem/innovation perspectives) and specifies their implications for online trade. The study links digital trust to measurable performance outcomes-conversion and repeat purchases, customer lifetime value and retention, access to cross-border marketplaces and partner networks, and a lower total cost of risk through reduced fraud, incidents and regulatory penalties. Special attention is paid to infrastructure mechanisms that operationalize trust in e-commerce transactions: cybersecurity governance, personal data protection and privacy, compliance as proof of legal and procedural legitimacy, transparency of service rules, and end-to-end operational reliability across the customer journey (contact – identification – payment – delivery – support or returns). Using Ukrainian market evidence and payment (fraud) statistics, the paper highlights the economic price of distrust and identifies the most vulnerable stages of the digital trust chain. As a practical contribution, a process concept for managing e-commerce competitiveness through digital trust is proposed, including trust components, their manifestations, and managerial decision options. The authors also formulate a definition of digital trust as an integrated intangible asset and a controllable capability to ensure secure, lawful and predictable digital interaction for customers and partners at scale.

Keywords: *financial services market, infrastructure, competitiveness, e-commerce, digitalization, digital technologies, digital trust, enterprise, credit institution, risk management.*

Fig.: 1. Table: 1. References: 25.

Іванова Н. В., Бондаренко А. А. Роль інфраструктури ринку фінансових послуг у формуванні цифрової довіри як фактора конкурентоспроможності підприємств електронної комерції. *Проблеми і перспективи економіки та управління.* 2026. № 1(45). С. 247-257. DOI: https://doi.org/10.25140/2411-5215-2026-1(45)-247-257.