

23. Orazalin, N. S., Ntim, C. G., & Kalimilo Malagila, J. (2025). Corporate governance, national governance quality, and biodiversity reporting: Global evidence. *Journal of International Accounting, Auditing and Taxation*, 58, 100669. <https://doi.org/10.1016/j.intaccudtax.2024.100669>
24. Toledo, I., Laino, E., Iglesias, G., Palazón, A., & Aragonés, L. (2025). Local authorities or national frameworks? A global review on coastal protection policies. *Environmental Development*, 53, 101119. <https://doi.org/10.1016/j.envdev.2024.101119>
25. Panfilova, E. E., Borisova, V. V., & Raza, H. (2021). Architectonics of «smart city» management system. *Lecture Notes in Networks and Systems*, 155, 1356–1365. https://doi.org/10.1007/978-3-030-59126-7_149
26. Khan, A. A., Akbar, M. A., Lahtinen, V., Alatawi, M. N., & Alotaibi, S. D. (2025). Correction to: Agile meets quantum: A novel genetic algorithm model for predicting the success of quantum software development project. *Automated Software Engineering*, 32(1), 8. <https://doi.org/10.1007/s10515-024-00474-5>
27. León, K. S., Ken, I., & Martin, T. (2024). Capture, commodify, kill: Legitimized harms and industrial meatpacking in the United States. *Crime, Law and Social Change*, 82(4), 1033–1059. <https://doi.org/10.1007/s10611-024-10176-4>
28. Bao, J.-M., Zhang, K., Wu, L., Hong, R.-C., & Wang, M. (2024). Conformity-aware debiased neural news recommendation with causal reasoning. *Chinese Journal of Computers*, 47(10), 2333–2351. <https://doi.org/10.1016/j.aiopen.2024.02.001>
29. Johansson, S., & Bengtsson, S. (2024). Audience research in a cross-cultural framework: When lofty ideals collide with complicated realities. In *The Routledge Companion to Media Audiences* (pp. 511–522). <https://doi.org/10.4324/9781003268543-51>
30. Bal, S. (2021). Human rights norms diffusion through transnational advocacy networks: LGBTI+ rights as a case. *Uluslararası İlişkiler*, 18(71), 109–127. <https://doi.org/10.33458/uidergisi.947584>

DOI 10.33111/vz_kneu.40.25.03.04.025.031

УДК 35.078:004.056.5:330.16:519.83

Апостол Андрій Вікторович

аспірант

кафедра системного аналізу та кібербезпеки

КНЕУ імені Вадима Гетьмана, Київ, Україна

email: apostol.andrii@kneu.edu.ua

ORCID: 0009-0008-6286-6535

+380663295954

ЦИФРОВА ІДЕНТИЧНІСТЬ І ЕКОНОМІЧНА ПОВЕДІНКА: ДИЗАЙН ДОВІРИ

Apostol Andrii

PhD student

department of systems analysis and cybersecurity

KNEU named after Vadym Hetman, Kyiv, Ukraine

email: apostol.andrii@kneu.edu.ua

ORCID: 0009-0008-6286-6535

+380663295954

DIGITAL IDENTITY AND ECONOMIC BEHAVIOR: DESIGNING FOR TRUST

Анотація. Стаття досліджує, чому цифрова ідентичність попри очевидні вигоди часто натрапляє на бар'єри прийняття, і пропонує практичні механізми їх подолання. Теоретична рамка поєднує обмежену раціональність, теорію ігор з мере-

жевими ефектами та інструменти експериментальної економіки. Побудовано координаційну гру з множинними рівновагами, у якій виграш індивіда залежить від частки користувачів та індивідуальних витрат/страхів. Розглянуто три інтервенції — субсидії, соціальні сигнали та архітектура вибору — і показано, що вони знижують поріг критичної маси, переводячи систему зі статус-кво до рівноваги широкого прийняття.

Емпіричну частину сформовано як порівняльний аналіз Естонії, Індії та України. Встановлено, що «дизайн довіри» — прозорі журнали доступу, оскарження несанкціонованого використання, зрозуміла комунікація ризиків — є визначальним для стійкого прийняття навіть за високої технологічної складності. Виявлено три групи бар'єрів: індивідуальні (страх втрати контролю, ефект статус-кво, цифрова нерівність), інституційні (правова невизначеність, низька підзвітність), бізнес-бар'єри (витрати інтеграції, відсутність короткострокових стимулів). Модель кількісно демонструє, що помірні субсидії та сильні соціальні сигнали істотно знижують критичний поріг прийняття; їх поєднання дає найбільший ефект. Запропоновано набір політик: цільові мікросубсидії для першого входу, поведінковий дизайн інтерфейсів за замовчуванням, локалізовані соціальні докази, а також пілотні RCT для оцінювання ефективності.

Наукова новизна полягає у синтезі поведінкових, інституційних і стратегічних підходів у єдиній операціоналізованій моделі з чіткими параметрами інтервенцій та управлінськими метриками. Практична цінність — у дорожній карті переходу від координаційної пастки до позитивної рівноваги через «дизайн довіри», що поєднує право, технологію та nudge-інструменти.

Ключові слова: цифрова ідентичність, економічна поведінка, теорія ігор, довіра, координаційні пастки, nudge, архітектура вибору, мережеві ефекти, пілотні експерименти, політика цифрової трансформації.

Abstract. The paper examines why digital identity systems, despite clear efficiency gains, often face adoption barriers and proposes actionable mechanisms to overcome them. The theoretical framework integrates bounded rationality, game-theoretic coordination with network effects, and tools from experimental economics. We build a coordination game with multiple equilibria in which individual payoffs depend on the share of adopters and individual costs/fears. Three interventions are analyzed — subsidies, social signals, and choice architecture — and shown to reduce the critical mass threshold, shifting the system from status quo to a high-adoption equilibrium.

The empirical component is a comparative analysis of Estonia, India, and Ukraine. We find that a «design of trust» — transparent access logs, remedies for unauthorized use, and clear risk communication — is decisive for sustained adoption even under technological complexity. Barriers cluster into three groups: individual (loss-of-control concerns, status-quo bias, digital divide), institutional (legal ambiguity, low accountability), and business-related (integration costs, lack of near-term incentives). The model quantifies how moderate subsidies and strong social signals materially lower the adoption threshold; their combination yields the largest effect. We propose a policy toolkit: targeted entry micro-subsidies, default-based behavioral interface design, localized social proof, and pilot RCTs to evaluate effectiveness.

The contribution is a synthesized behavioral–institutional–strategic framework operationalized in a tractable model with explicit intervention parameters and managerial metrics. The practical value is a roadmap for moving from a coordination trap to a positive equilibrium via a trust-centered design that jointly leverages law, technology, and nudge instruments.

Keywords: digital identity, economic behavior, game theory, trust, coordination traps, nudge, choice architecture, network effects, pilot experiments, digital transformation policy.

JEL codes: H83, O38, O33.

Постановка проблеми. У XXI столітті цифрова трансформація стала не просто технологічним явищем, а глибоким структурним зрушенням у способі функ-

ціонування економіки, держави та соціальних інститутів. Одним із наріжних каменів цієї трансформації є цифрова ідентичність — сукупність даних і характеристик, що надають людині цифрову присутність і дозволяють здійснювати юридично значущі дії в онлайн-середовищі. Саме вона забезпечує доступ до електронних послуг, підтверджує особу в електронних транзакціях і закладає підґрунтя для цифрової довіри, яке є основою для прийняття eGovernment суспільством [10].

Проте на практиці ці переваги не завжди конвертуються в масове прийняття. Значна частина громадян сприймає цифрову ідентичність з недовірою або байдужістю, вбачаючи в ній радше загрозу, аніж можливість. Причини цього — не лише технічні. На передній план виходять чинники психологічного та інституційного характеру: страх втрати контролю над особистими даними, нерозуміння принципів функціонування систем, слабка прозорість механізмів збору й обробки інформації.

У такому контексті питання впровадження цифрової ідентичності неможливо розглядати ізольовано від поведінкової економіки. Раціональні аргументи, такі як зручність, швидкість, економія, часто не працюють, якщо не подолано глибинні бар'єри сприйняття. Поведінкові упередження, зокрема уникнення ризику, ефект статус-кво, соціальна недовіра, — усе це впливає на рішення «бути чи не бути в цифровому просторі».

Аналіз досліджень і публікацій. Розгляньмо детальніше, чому саме люди можуть протиставитися інноваціям, навіть якщо вигоди від них на перший погляд очевидні. Концепція обмеженої раціональності, сформульована Гербертом Саймоном, пояснює, чому люди часто ухвалюють рішення, що не є оптимальними з точки зору класичної економічної логіки. Його ідею деталізує Д. Канеман у моделі двох систем мислення, де автоматична та інтуїтивна (система 1) часто домінує над аналітичною [1]. У контексті цифрової ідентичності це означає, що навіть очевидні переваги (швидкість, зручність, доступність) не гарантують готовності до її використання. Люди не мають повної інформації, обмежені в когнітивних ресурсах, орієнтуються на евристики — прості правила, які часто ведуть до хибних висновків.

Д. Канеман разом із А. Тверські показали, як когнітивні упередження, зокрема ефект якоря, упередження наявності та страх втрати, впливають на вибір [1]. У цифровому середовищі це може проявлятися в переоцінці ризиків цифрових рішень та недооцінці ризиків паперових чи офлайн-альтернатив. Страх перед новим, відсутність позитивного досвіду, низький рівень цифрової грамотності — все це формує поведінковий бар'єр, який заважає прийняттю інновацій.

Рішення користувачів щодо використання цифрової ідентичності залежать не лише від особистих переваг, а й від дій інших учасників екосистеми — державних органів, цифрових платформ, банків чи роботодавців. Людина не приймає це рішення у вакуумі. Наприклад, якщо користувач сумнівається, що держава забезпечить конфіденційність даних або що його банк визнає електронну ідентифікацію, мотивація до участі в системі знижується.

Цю взаємозалежність добре описує теорія ігор. Ситуація нагадує гру довіри: держава має дотриматись обіцянок захисту даних, а громадянин — скористатися інструментом. Якщо обидві сторони співпрацюють, виграють усі [3]. Але за відсутності впевненості в чесності партнера (наприклад, побоювання зловживань

владою чи комерціалізації персональних даних) громадянин може обрати неучасть, навіть якщо потенційна вигода очевидна.

Подібні ситуації описуються через дилему в'язня — кожен гравець має стимул діяти у власних інтересах, не довіряючи іншому, навіть якщо колективна співпраця принесла б кращий результат [3]. Асиметрія інформації, відсутність прозорих правил, слабка юридична відповідальність — усе це зміщує систему в сторону недовіри.

Щоб змінити ситуацію, необхідно вплинути на очікування гравців — наприклад, гарантувати правовий захист, забезпечити контрольованість використання даних, демонструвати практичні кейси, де цифрова ідентичність працює на користь громадянина — у сфері медицини, освіти чи державних послуг.

Крім впливу зовнішніх гравців, важливим чинником є те, як саме людині пропонують ухвалити рішення. Найочевидніший спосіб — примус чи заборона, коли держава фактично не залишає громадянам іншого вибору. Однак набагато ефективнішими і стратегічно мудрими є поведінкові інтервенції (nudge), запропоновані Річардом Талером та Кассом Санстейном. Їх суть полягає в тому, що замість примусу створюється середовище, яке м'яко підштовхує людину до бажаної дії [2]. В експериментах показано, що архітектура вибору, порядок і форма подання варіантів, суттєво впливає на поведінку користувачів.

Наприклад, якщо за замовчуванням у цифровому сервісі увімкнено опцію використання електронної ідентифікації або збереження профілю (з можливістю відмовитися), більшість користувачів залишають цей варіант — це знижує бар'єр до входу. Також ефективним є використання соціальних норм: повідомлення типу «80 % громадян уже користуються електронними послугами» створюють ефект залученості та нормативного тиску. А правильно сформульовані повідомлення на кшталт «З цифровою ідентифікацією ви отримаєте результат у 2 рази швидше» допомагають змістити фокус з потенційних ризиків на практичну вигоду.

Тобто не лише зміст, а й форма подачі рішень, інтерфейс, послідовність кроків і мова повідомлень суттєво впливають на поведінку. Ігнорування цих деталей може звести нанівець технічні інновації, тоді як грамотне їх врахування — стати ключем до успішного впровадження цифрової ідентичності.

Таким чином, поєднання інституціонального, ігрового й поведінкового підходів створює надійне підґрунтя для розуміння та подолання бар'єрів на шляху впровадження цифрової ідентичності.

Методика дослідження. Комплексний аналіз, що ґрунтується на поєднанні інституціонального підходу, теорії обмеженої раціональності та ігрових моделей взаємодії, дозволяє детально проаналізувати ці психологічні бар'єри. Крім того, він дає можливість побачити потенційні точки впливу — аспекти, на які можна спрямувати зусилля для подолання цих бар'єрів. Такий аналіз допомагає окреслити, що саме стримує громадян від активного використання цифрової ідентичності і які умови мають бути створені, аби подолати цей спротив.

Об'єктом цього дослідження виступають соціально-економічні процеси, пов'язані з цифровою ідентифікацією особи.

Предметом є бар'єри на шляху прийняття цифрової ідентичності та можливості їх подолання шляхом політичних, технологічних і поведінкових інтервенцій.

Метою статті є дослідження взаємозв'язку між економічною поведінкою індивідів, інституційною довірою та механізмами впровадження цифрової

ідентичності. У фокусі — теоретичні засади, міжнародні кейси (зокрема, досвід Естонії, Індії та України), а також авторська модель подолання поведінкових і структурних бар'єрів шляхом інтервенцій у сфері дизайну цифрових систем і державної політики.

Виклад основного матеріалу. Зазначені теоретичні і методологічні засади створюють основу для практичного аналізу проблеми. Розрив між потенційними вигодами цифрової ідентичності та реальним рівнем її прийняття можна логічно пояснити, проаналізувавши поведінкові бар'єри.

Поведінкові фактори на індивідуальному рівні. Переходячи від теоретичних положень до реального життя, передусім слід звернути увагу на індивідуальний рівень — те, як окрема людина сприймає та реагує на впровадження цифрової ідентичності. Одним із найбільш поширених бар'єрів є страх втрати контролю над персональними даними [9]. У суспільній свідомості часто домінує уявлення, що цифрові відбитки, які залишаються після використання онлайн-сервісів, можуть бути використані без згоди, для нагляду, маніпуляцій або навіть кіберзлочинів. Приклади витоків даних із банківських, медичних чи державних реєстрів лише підкріплюють ці страхи.

Наступний бар'єр — ефект статус-кво. Це психологічне упередження на користь збереження звичного способу дій, навіть якщо наявна альтернатива є об'єктивно кращою [4]. Люди, які роками звикли до паперових документів і особистих візитів до державних установ, сприймають цифрові сервіси як щось складне, незрозуміле або ризиковане. Зміна усталеного способу взаємодії з державою вимагає когнітивних зусиль, а іноді і додаткового навчання, що саме по собі є бар'єром.

До цих факторів додається недовіра до державних платформ. Якщо держава або цифрові оператори не мають усталеної репутації захисника інтересів громадян, рівень прийняття цифрової ідентичності знижується [10]. Наприклад, у випадках, коли урядові портали працюють нестабільно, погано пояснюють свої функції або не забезпечують прозорого контролю над даними, користувачі відчують себе вразливими. У цьому контексті позитивні приклади, як-от система е-резидентства в Естонії, демонструють, що довіра значною мірою залежить від відкритої комунікації, прозорих процедур і технічної надійності, що підкріплюється дослідженнями [6].

Не менш важливу роль відіграє особистий досвід — зручність перших спроб використання цифрової ідентичності, доступність підтримки, швидкість обробки запитів. Якщо початковий досвід негативний (наприклад, сервіс не працює або дані не підтверджуються), користувач із високою ймовірністю відмовиться від подальших спроб, навіть попри об'єктивні переваги системи.

Бар'єри на рівні бізнесу. Значні перешкоди виникають і на боці бізнесу, який є важливим учасником екосистеми цифрової ідентичності. Передусім це витрати на адаптацію — інтеграція нових рішень потребує часу, ресурсів, зміни внутрішніх процесів, навчання персоналу, юридичної оцінки та технічного тестування. Особливо це стосується малого та середнього бізнесу, який має обмежені можливості для впровадження нових технологій без зовнішньої підтримки.

Крім того, бізнес часто стикається з невизначеністю правових норм. Якщо законодавство нечітко регламентує використання цифрової ідентичності, якщо існують прогалини або конфлікти в нормативній базі (наприклад, щодо електронного

підпису, збереження згоди, відповідальності за помилки в ідентифікації), компанії обирають утримання від змін як менш ризиковану стратегію [6]. Це особливо важливо у сферах із високою регуляторною відповідальністю — фінанси, медицина, освіта.

Також існує ризик так званого «технологічного боргу» — ситуації, коли компанія вимушено впроваджує застарілі або неповороткі рішення, що погано інтегруються з існуючими системами. Це гальмує інновації, призводить до дублювання процесів і витрат, породжує внутрішній спротив оновленням. Наприклад, компанії, що вже інвестували у власні CRM-системи або внутрішні сервіси перевірки клієнтів, можуть не бачити економічної доцільності в переході на державну платформу цифрової ідентичності.

Ще один бар'єр — брак стимулів. Якщо впровадження цифрової ідентичності не приносить відчутної конкурентної переваги, не знижує витрат або не підвищує лояльність клієнтів, компанії можуть відкласти рішення на невизначений термін. У таких випадках важливо створити фінансові, регуляторні або ринкові стимули: наприклад, пріоритет у державних закупівлях для компаній, що інтегрували цифрову ідентифікацію; спрощене звітування; зниження витрат на перевірку даних.

Проблема «першого кроку»: координаційні пастки. Навіть якщо окрема особа чи компанія готова впроваджувати цифрову ідентичність, ефект буде обмеженим, якщо інші учасники не підтримують цю зміну. Виникає класична координаційна пастка: ніхто не починає, бо чекає, поки почнуть інші [4]. Без критичної маси користувачів інновація не дає очікуваних вигод, а індивідуальні зусилля залишаються ізольованими і малоефективними.

Особливо гостро це проявляється у секторах, де цифрова ідентичність вимагає взаємної інтеграції, наприклад, в охороні здоров'я, освіті чи фінансах. Якщо, скажімо, лікарня переходить на цифрові картки пацієнтів, але інші медичні заклади чи страхові компанії не визнають їх, інновація не реалізує свій потенціал.

Для виходу з такої ситуації потрібен «масовий сигнал» — публічне підтвердження участі ключових гравців. Це можуть бути офіційні ініціативи держави, інтеграція цифрової ідентичності в ключові державні сервіси (як-от податкова система чи система субсидій), демонстрація успішних кейсів за участю великих компаній або організацій. Успішні приклади мають бути не декларативними, а практичними, з вимірюваними вигодами для користувачів.

Крім того, важливим є створення сприятливого регуляторного середовища: чіткі правові гарантії, пільгові умови впровадження, спрощене погодження рішень із регулятором. Також дієвим є механізм «приєднання через авторитет» — участь авторитетних лідерів думок, муніципалітетів чи великих роботодавців, що сигналізують суспільству: «це безпечно», «це вигідно», «це вже працює».

Чим більше учасників залучено з самого початку, тим швидше система переходить у фазу стабільного функціонування, коли кожен новий користувач підсилює цінність для інших — класичний приклад позитивного мережевого ефекту, що робить цифрову ідентичність дедалі привабливішою як для громадян, так і для бізнесу.

Поведінкові бар'єри, розглянуті вище, не є абстрактними, вони по-різному проявляються в конкретних контекстах. Щоб краще зрозуміти, як культурні, інституційні й комунікаційні фактори впливають на прийняття цифрової ідентичності, розглянемо три країни з різними підходами до впровадження: Естонію, Індію та Україну.

Естонія — модельна система. Естонія вважається еталоном цифрової держави. Система eID стала не просто доступною опцією, а обов'язковим стандартом, інтегрованим у всі сфери — від голосування до охорони здоров'я. Вже з початку 2000-х років цифрова ідентифікація була впроваджена на національному рівні й супроводжувалась активною політикою цифровізації публічного сектора. У 2023 році 95.8 % громадян користувалися державними послугами онлайн, що значно перевищує середньоєвропейський показник [11]. Ключовим чинником успіху стала синергія між технологічним лідерством і високим рівнем інституційної довіри: громадяни впевнені, що держава не зловживає повноваженнями та гарантує захист персональних даних.

Цьому сприяла також прозора архітектура X-Road — платформи, яка дозволяє державним і приватним організаціям безпечно обмінюватися даними, зберігаючи контроль над доступом. Використання цифрової ідентифікації в Естонії підтримується законодавчо, а цифровий підпис має таку ж юридичну силу, як і фізичний. Важливо, що естонці можуть бачити, хто і коли переглядав їхні дані, що посилює відчуття контролю і зменшує страх перед цифровим наглядом. Регулярні освітні кампанії, простота користування та обов'язковість використання цифрових ID у повсякденному житті зробили їх невід'ємною частиною громадянської культури. Дослідження стверджують, що саме прозорість і високий рівень цифрової освіти є ключовими факторами у прийнятті цифрової ідентичності [8].

Індія — масштаб без прийняття. Дещо іншою була ситуація в Індії. Ця країна реалізувала одну з наймасштабніших у світі систем цифрової ідентифікації, Aadhaar, яка охоплює понад 1.38 мільярда осіб. Ця система стала ключовим елементом цифрової інфраструктури країни, забезпечуючи доступ до широкого спектру державних та приватних послуг. Aadhaar ілюструє логіку централізованого підходу до управління даними громадян, де держава виконує роль координатора цифрової екосистеми. Такий підхід узгоджується з концепцією оркестрації публічної інфраструктури, що дедалі частіше стає стратегічним вибором урядів [5]. Однак, попри вражаючий масштаб, Aadhaar стикається з численними викликами, пов'язаними з прийняттям, довірою та захистом прав громадян.

Aadhaar був запущений у 2009 році і надавав кожному мешканцю Індії унікальний ідентифікаційний номер, пов'язаний з біометричними та демографічними даними. Станом на жовтень 2024 року понад 1.38 мільярда мешканців Індії зареєстровані в системі Aadhaar та отримали унікальний ідентифікаційний номер. Система активно використовується для ідентифікації при отриманні соціальних виплат, відкритті банківських рахунків, використанні мобільних послуг та інших транзакціях.

Згідно з дослідженням UCLA Anderson Review, 95 % дорослих індійців використовують свій Aadhaar ID щонайменше раз на місяць, а 90 % висловлюють задоволення від програми. Крім того, система дозволила зекономити понад \$12 мільярдів за рахунок зменшення шахрайства та нецільового використання коштів.

Попри переваги, Aadhaar зазнає критики через проблеми з конфіденційністю та безпекою даних. У 2017 році повідомлялося про витік даних понад 3.5 мільйона осіб [12], що суттєво підірвало довіру до системи. Також були випадки несанкціонованого доступу до даних через урядові веб-сайти та приватні компанії.

У 2018 році Верховний суд Індії визнав право на конфіденційність фундаментальним правом, що поставило під сумнів законність деяких аспектів Aadhaar.

Хоча суд дозволив використання Aadhaar для отримання субсидій та інших державних послуг, він заборонив обов'язкове використання системи приватними компаніями без згоди користувачів.

Aadhaar також стикається з критикою через потенційну дискримінацію вразливих груп населення. Як стверджують дослідники, обов'язкове надання біометричних даних може створювати бар'єри для людей похилого віку, осіб з інвалідністю та трансгендерних осіб, які стикаються з труднощами при проходженні біометричної аутентифікації [7].

Крім того, були випадки, коли помилки в системі призводили до відмови у наданні соціальних послуг. Наприклад, у штаті Андхра-Прадеш неправильне зв'язування Aadhaar з даними про споживання електроенергії призвело до помилкової відмови у видачі продовольчих карток для багатьох заявників.

Система Aadhaar демонструє значний потенціал у сфері цифрової ідентифікації та надання державних послуг. Однак для забезпечення її ефективності та справедливості необхідно вирішити питання конфіденційності, безпеки та недопущення дискримінації. Це включає в себе впровадження чітких правових рамок, забезпечення прозорості у використанні даних та створення механізмів захисту прав вразливих груп населення.

Україна — гібридний кейс. Україна демонструє унікальний приклад цифрової трансформації в умовах війни. Запущена у 2020 році платформа «Дія» стала центральним елементом стратегії «держава в смартфоні», об'єднавши понад 70 державних послуг та 14 цифрових документів, включаючи паспорт, водійське посвідчення та свідоцтво про народження. Станом на середину 2024 року кількість користувачів порталу перевищила 21.7 мільйона осіб.

В умовах війни «Дія» стала критично важливим інструментом для підтримки функціонування державних сервісів. Платформа дозволила переміщеним особам отримувати доступ до необхідних документів без фізичних копій, що спростило процедури перетину кордонів та адміністративні процеси. Крім того, Україна адаптувалася до кіберзагроз, впровадивши хмарні рішення та супутниковий інтернет для забезпечення стійкості цифрової інфраструктури.

Попри успіхи, впровадження цифрової ідентичності в Україні стикається з низкою викликів, особливо для вразливих груп. Згідно з дослідженням ПРООН, понад 31 % літніх українців повідомили, що ніколи не користуються інтернетом [13]. Це свідчить про значний цифровий розрив, який ускладнює доступ до електронних послуг для цієї категорії населення.

Крім того, особи без офіційного статусу, такі як особи без громадянства або мешканці окупованих територій, не можуть зареєструватися в «Дії» через відсутність необхідних документів або ризиків, пов'язаних з використанням українських цифрових сервісів в умовах окупації.

Хоча «Дія» значно спростила доступ до державних послуг, питання безпеки та захисту персональних даних залишаються актуальними. Рівень занепокоєння щодо конфіденційності і безпеки персональних даних є високим, насамперед через відсутність у громадян відчуття контролю над тим, як, коли і ким використовуються їхні дані [9]. Ці занепокоєння підсилив витік даних 26 мільйонів водійських посвідчень у 2020 році, що підкреслило вразливість цифрових систем до кіберзагроз [14].

Український досвід впровадження цифрової ідентичності через платформу «Дія» демонструє значний прогрес у цифровій трансформації державних послуг.

Однак для забезпечення інклюзивності та довіри необхідно вирішити питання цифрового розриву, безпеки даних та доступності сервісів для всіх категорій населення.

Розглянуті кейси показують нам, що успішність впровадження цифрової ідентичності значною мірою залежить не лише від технологічного рівня рішень, а й від тонко налаштованої взаємодії між інституційними умовами, поведінковими стимулами та публічною комунікацією.

По-перше, поведінкові інтервенції (nudge) мають бути спрямовані на формування довіри, зменшення бар'єру входу та надання позитивного досвіду першого використання. Простота інтерфейсу, прозорість даних, демонстрація контролю над особистою інформацією (наприклад, як у випадку з X-Road в Естонії) створюють ефект психологічного комфорту та підвищують рівень прийняття.

Також важливою є наявність чітких правових рамок. Як показує кейс Індії, відсутність достатнього нормативного контролю призводить до ризиків дискримінації, витоків даних і зловживань. Законодавче врегулювання повинно не лише регламентувати обов'язки сторін, а й закріплювати права користувачів на захист, виправлення або видалення даних, а також гарантувати неперсоналізоване використання інформації у публічних і приватних сервісах.

Окрім того, комунікаційна стратегія повинна бути адаптована до особливостей аудиторії. Різні вікові, соціальні та освітні групи потребують різного підходу до пояснення переваг цифрової ідентичності. Наприклад, в Україні необхідна цільова інформаційна підтримка для літніх людей та мешканців регіонів із низьким рівнем цифрових навичок. Важливу роль також відіграють амбасадори цифрових змін, кейси успішного використання в медіа, а також побудова комунікації на рівні «людина-людині» — через соціальних працівників, місцеву адміністрацію, волонтерів.

Таким чином, подолання бар'єрів до впровадження цифрової ідентичності вимагає скоординованої роботи на трьох рівнях: дизайн сервісу (поведінкові «підштовхування»), законодавче підґрунтя та публічне залучення. Лише в синергії цих інструментів можливо досягти широкого, справедливого та інклюзивного прийняття цифрової ідентичності.

Як було сказано вище, рішення приймати чи не приймати цифрову ідентичність — це не лише індивідуальний вибір, а стратегічна взаємодія, в якій важливу роль відіграють очікування, довіра до інших і вплив зовнішніх інтервенцій. Щоб формалізувати це, в рамках дослідження була побудована координаційна гра, яка моделює поведінку користувачів у системі з мережевими ефектами, бар'єрами та можливими «підштовхуваннями» (nudge).

Нехай $N = \{1, \dots, n\}$ — множина агентів, кожен з яких обирає дію $A_i \in \{0, 1\}$, де 1 — прийняти цифрову ідентичність, 0 — утриматися. Виграш агента задається функцією:

$$U_i(a_i, A_{-i}) = a_i \cdot \left[B \cdot \frac{1}{n} \sum_{j=1}^n a_j - C \right]$$

де:

- a_i — i -й агент

- A_{-i} — профіль дій усіх інших агентів, окрім i -го
- B — вигода від мережевого ефекту
- C — індивідуальні бар'єри (страх, складність, недовіра)

У цій грі можливі дві стійкі рівноваги: статус-кво (повне неприйняття) і бажане масове прийняття.

Дослідження розглядає три можливі інтервенції:

- S — субсидія — знижує індивідуальні бар'єри C :

$$U_i^{(S)}(a_i, A_{-i}) = a_i \cdot \left[B \cdot \frac{1}{n} \sum_{j=1}^n a_j - (C - S) \right]$$

• δT — соціальний сигнал — підсилює готовність до прийняття цифрової ідентичності. Тут T — інтенсивність соціального сигналу (наприклад, частка знайомих, які вже користуються цифровою ідентичністю), а δ — коефіцієнт сприйняття, що показує, наскільки сильно індивід реагує на цей сигнал:

$$U_i^{(signal)}(a_i, A_{-i}) = a_i \cdot \left[B \cdot \frac{1}{n} \sum_{j=1}^n a_j - (C - \delta T) \right]$$

- Комбінована ($S + \delta T$) — і субсидія, і соціальний сигнал:

$$U_i^{(S+signal)}(a_i, A_{-i}) = a_i \cdot \left[B \cdot \frac{1}{n} \sum_{j=1}^n a_j - (C - S - \delta T) \right]$$

Попри формальну схожість, субсидія й соціальний сигнал мають різну економічну природу. Субсидія — це зовнішній матеріальний стимул (наприклад, бонус за встановлення додатку або можливість користуватися сервісами цифрового підпису безкоштовно), який реально зменшує витрати. Натомість соціальний сигнал — це психологічний або інформаційний вплив (наприклад, повідомлення про популярність сервісу серед знайомих), що змінює сприйняття бар'єру, а не його реальну величину.

Для моделі було обрано такі параметри:

$B = 7$ — це вигода від мережевого ефекту, тобто скільки корисності отримує агент за кожного учасника, який також прийняв цифрову ідентичність. Обрано досить високе значення, щоб відобразити сильну взаємозалежність (у випадку з електронними державними послугами — чим більше користувачів, тим ефективніша взаємодія).

$C = 3$ — це базовий бар'єр, що включає суб'єктивні витрати (час, складність, страх, недовіру). Це умовна одиниця, яка робить порівняння з B зручним. Обрано значення, де за низької частки учасників вигода менша за бар'єр (тобто ситуація координаційної пастки).

$S = 1$ — субсидія, яка зменшує бар'єр $C \rightarrow C - S$. Вибрано помірне значення, щоб змодельовати легку фінансову підтримку (наприклад, держава покриває витрати на ЕЦП або верифікацію).

$\delta = 0.5$, $T = 1$ — соціальний сигнал. Це означає, що якщо сигнал максимально сильний ($T = 1$), то агент відчуває зниження бар'єру на $\delta \times T = 0.5$. Такий ефект може створити, наприклад, рекламна кампанія з довіри до сервісу, особливо коли її транслюють знайомі.

Таблиця 1

**ОЧІКУВАНИЙ ВИГРАШ АГЕНТА ЗАЛЕЖНО ВІД ЧАСТКИ ПРИЙНЯТТЯ ЦИФРОВОЇ
ПРИ РІЗНИХ ІНТЕРВЕНЦІЯХ**

Частка прийняття	Без інтервенції	Субсидія $S = 1$	Соціальний сигнал $d = 0.5, T = 1$	Комбінація $S = 1 + d = 0.5, T = 1$
0 %	-3	-2	-2.5	-1.5
20 %	-1.6	-0.6	-1.1	-0.1
40 %	-0.2	0.8	0.3	1.3
60 %	1.2	2.2	1.7	2.7
80 %	2.6	3.6	3.1	4.1
100 %	4	5	4.5	5.5

Розраховано автором

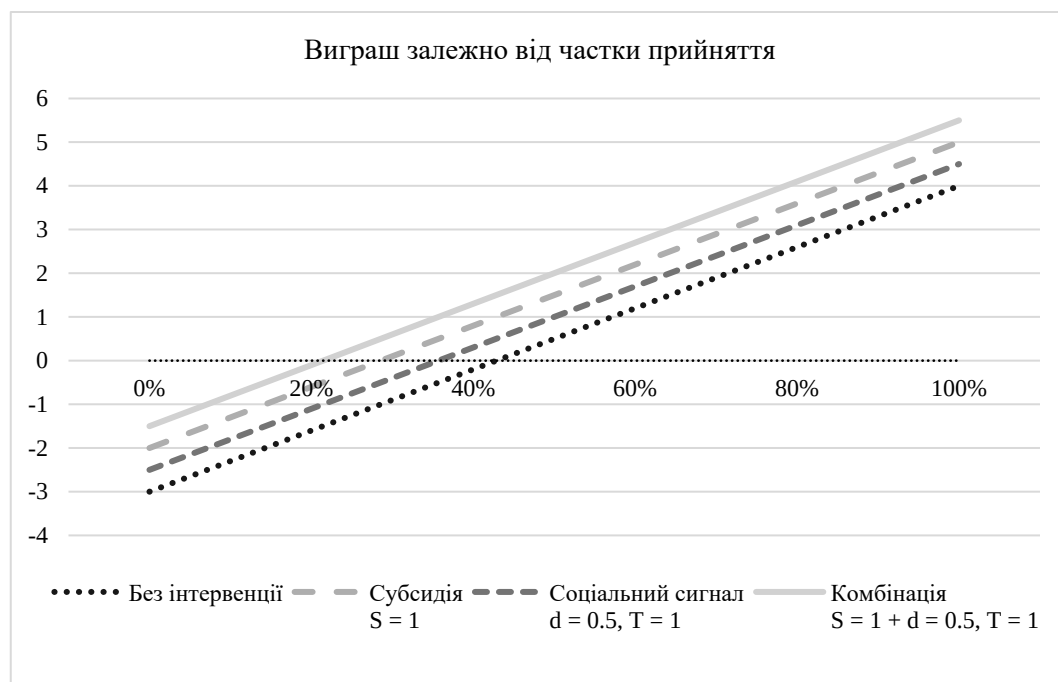


Рис. 1. Динаміка виграшу агента залежно від частки прийняття цифрової ідентичності при різних інтервенціях

Розроблено автором

Дискусія. Результати координаційної гри показують наявність множинних рівноваг і критичного порога участі (за ілюстративної параметризації — близько 40 %), нижче якого система залишається у статус-кво. Матеріальні стимули (субсидія S) та перцептивні інтервенції (соціальний сигнал δT) діють через різні канали: перші зменшують реальні витрати входу, другі — сприйнятий бар'єр та невизначеність очікувань. Їхня комбінація найефективніше зміщує систему в бік високої рівноваги, особливо на ранніх етапах розгортання. Чутливість результатів до параметрів B , C , S , δ підкреслює потребу контекстного калібрування під сектор, регіон та профіль цільових груп.

Спостереження з Естонії, Індії та України узгоджуються з механікою моделі. Прозорі журнали доступів, правові гарантії та технічна підзвітність (естонський «дизайн довіри») еквівалентно зменшують базовий бар'єр у вигляді початкових витрат чи страхів C і стабілізують очікування, полегшуючи проходження порога. Масштабні централізовані рішення за недостатніх гарантій приватності (окремі аспекти Aadhaar) підтримують перцептивні бар'єри, стримуючи рух до високої рівноваги. Український кейс демонструє, що технологічна стійкість у кризових умовах має поєднуватися з інклюзією: цифровий розрив і нерівномірні навички підвищують базовий бар'єр C для вразливих груп, тому мережевих вигод недостатньо без таргетованих інтервенцій.

Інституційні гарантії («дизайн довіри» — аудит доступів, нотифікації користувача, механізми оскарження) є базовою умовою, на яку накладаються поведінкові підказки (архітектура вибору «за замовчуванням», локалізовані соціальні докази) та помірні мікросубсидії. Вибір між добровільністю та елементами обов'язковості має бути контекстно-залежним: у середовищах з низькою довірою пріоритет — посилення підзвітності та контролю користувача; з високою довірою — достатньо «м'яких» nudge-інструментів.

«Підштовхування» має бути прозорим і оборотним (з реальною можливістю відмови), щоб не знецінювати довіру; політика повинна мінімізувати ризики дискримінації вразливих груп (зокрема в біометричних сценаріях) і уникати «перенавантаження стимулів», що може підривати внутрішню мотивацію та легітимність інституцій.

Модель є спрощеною (статична постановка, репрезентативний агент, ілюстративні параметри) і потребує емпіричного калібрування на даних А/В-тестів та RCT, урахування гетерогенності груп і динамічних «шоків довіри» (кіберінциденти, зміни регулювання), а також порівняння централізованих та децентралізованих архітектур eID.

Висновки. Проведене дослідження переводить фокус із суто технологічних характеристик систем цифрової ідентичності на керовані точки впливу економічної поведінки та інституційного дизайну. Запропонована координаційна рамка демонструє, що траєкторія прийняття eID визначається поєднанням мережевих ефектів, «дизайну довіри» та поведінкових інтервенцій, а отже може бути проєктована й оцінена як політика зі зрозумілими важелями та верифікованими результатами.

Стаття пропонує операціоналізований підхід до «дизайну довіри», який інтегрує інституційні гарантії підзвітності з інструментами поведінкової економіки у формальній координаційній моделі з явними параметрами втручання (матеріальні стимули та соціальні сигнали). Новизна полягає у зв'язуванні мікромеханік індивідуального вибору з макрорівневими режимами рівноваги прийняття, що дає

змогу прогнозувати умови переходу від координаційної пастки до стійкої високої рівноваги.

З теоретичної точки зору стаття уточнює роль інституційної довіри у публічній цифровізації, трактуючи прийняття eID як пороговий координаційний процес. Вона поєднує обмежену раціональність, мережеві ефекти та архітектуру вибору у єдиній моделі, яка дозволяє порівнювати альтернативні конфігурації політик не лише за припущеннями, а й за очікуваними рівноважними наслідками.

З практичної точки зору запропоновано послідовність впровадження, що мінімізує ризики примусу та перевитрат: спершу — інституційні гарантії прозорості доступів і контролю над даними; далі — налаштування архітектури вибору (сценарії за замовчуванням, локалізовані соціальні докази); після підтвердження ефективності на пілотах — таргетовані обмежені мікростимули. Для управління потрібен компактний набір метрик: траєкторія частки прийняття і час до першої успішної транзакції, індекс відчуття контролю й довіри, частота інцидентів безпеки та обґрунтованих скарг, показники інклюзії вразливих груп. Саме порогові значення цих індикаторів мають виступати умовами переходу від пілоту до масштабування.

В соціально-економічному аспекті імплементація «дизайну довіри» очікувано знижує транзакційні витрати для громадян і бізнесу, скорочує втрати від помилок і шахрайства, підвищує доступність і передбачуваність публічних послуг, стимулює формалізацію транзакцій і конкуренцію на ринку цифрових сервісів. У середньостроковій перспективі це трансформується в підвищення продуктивності державного сектору, кращу таргетацію соціальних виплат і розширення податкової бази за рахунок цифрових відбитків легальних операцій.

Дане дослідження має перспективи для подальших розробок. Перше — емпіричне калібрування параметрів моделі (вигоди мережі, реальні та сприйняті бар'єри, сила сигналів) на мікроданих A/B-тестів та RCT у різних доменах (охорона здоров'я, соціальні трансфери, освіта тощо) з урахуванням гетерогенності користувачів. Друге — перехід до динамічних та agent-based постановок із «шоками довіри» (кіберінциденти, зміни регулювання), що дозволить оцінювати стійкість політик у часі. Третє — порівняльний аналіз централізованих архітектур eID та децентралізованих рішень на базі верифікованих облікових даних (VC/SSI) з погляду балансу між приватністю, масштабованістю та керованістю. Четверте — розробка методики багатокритеріальної оптимізації політик (поєднання метрик прийняття, приватності, вартості та інклюзії) і створення відкритого «сценарного калькулятора» для органів влади, який дасть змогу тестувати наслідки альтернативних інтервенцій до ухвалення рішень про масштабування.

Таким чином, отримані результати формують цілісну підставу для проектування й оцінювання політик цифрової ідентичності: від науково обґрунтованого «дизайну довіри» та інструментів поведінкового впливу до вимірюваних соціально-економічних результатів на рівні громадянина, інституцій і економіки загалом.

Література

1. Канеман, Д. (2011). *Мислення, швидке й повільне*. Farrar, Straus and Giroux.
2. Талер, Р. Г. та Санстейн, К. Р. (2021). *Підштовхування: остаточне видання*. Penguin.
3. Шеллінг, Т. К. (2015). *Стратегія конфлікту*. Pickle Partners Publishing.
4. Камерер, К., Ловенштейн, Дж. та Рабін, М. (2004). *Досягнення у поведінковій економіці*. Princeton University Press.

5. Деген, К. та Тойбнер, Т. (2024). Війни гаманців чи цифрова публічна інфраструктура? Оркестрування екосистеми даних цифрової ідентичності з урядової перспективи. *Electron Markets* 34, 50 (2024). <https://doi.org/10.1007/s12525-024-00731-1>
6. Боттареллі, М., Епіфаніу, Г., Махмуд, С., Хупер, М. та Мейпл, К. (2025). Оцінювання довірчості систем електронного управління ідентичністю: рамка та висновки від ініціації до розгортання. *Препринт arXiv*. <https://doi.org/10.48550/arXiv.2502.10771>
7. Гейз де Калаф, Е. та Фернандес, К. (2023). Цифрова ідентичність: нові тенденції, дебати та контрверсії. <http://dx.doi.org/10.13140/RG.2.2.23898.56005>
8. Тійтс, М., Калвет, Т. та МакБі, Д. (2024). Крадіжка ідентичності та суспільна прийнятність електронної ідентичності в Європі та Сполучених Штатах. *Препринт arXiv*. <https://doi.org/10.48550/arXiv.2412.07445>
9. Турха, К., Врховец, С. та Бернік, І. (2024). Державне спостереження в цифрову добу: чинники, пов'язані зі ставленням громадян до реєстрів довіри. *Препринт arXiv*. <https://doi.org/10.48550/arXiv.2408.09725>
10. Гупта, П., Худа, А., Джейярадж, А. та ін. (2024). Довіра, ризик, приватність і безпека у використанні електронного уряду: висновки з MASEM-аналізу. *Inf Syst Front*. <https://doi.org/10.1007/s10796-024-10497-8>
11. Європейська комісія. (2024). *Звіт про стан Цифрового десятиріччя 2024*. <https://digital-strategy.ec.europa.eu/en/library/report-state-digital-decade-2024>
12. Седльмаєр, Й., Сметхерст, Р., Піреп, А. та ін. (2021). Цифрові ідентичності та верифіковані облікові дані. *Bus Inf Syst Eng* 63, 603–613 (2021). <https://doi.org/10.1007/s12599-021-00722-y>
13. Програма розвитку Організації Об'єднаних Націй (ПРООН). (2025). *Задоволеність українців державними е-послугами зростає, свідчить опитування КМІС*. Отримано з <https://www.undp.org/ukraine/press-releases/ukrainians-satisfaction-government-e-services-rise-kiis-survey-finds>
14. Громадське. (2020, 22 травня). *Через Telegram-бот «злили» базу з 26 млн водійських посвідчень — за справу взялася СБУ*. Громадське. Отримано з <https://hromadske.ua/posts/cherez-telegram-bot-zlili-bazu-z-26-mln-vodijskih-posvidchen-za-spravu-vzylasya-sbu>

References

1. Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.
2. Thaler, R. H., & Sunstein, C. R. (2021). *Nudge: The Final Edition*. Penguin.
3. Schelling, T. C. (2015). *The strategy of conflict*. Pickle Partners Publishing.
4. Camerer, C., Loewenstein, G., & Rabin, M. (2004). *Advances in behavioral economics*. Princeton University Press.
5. Degen, K., Teubner, T. Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. *Electron Markets* 34, 50 (2024). <https://doi.org/10.1007/s12525-024-00731-1>
6. Bottarelli, M., Epiphaniou, G., Mahmood, S., Hooper, M., & Maple, C. (2025). Assessing the trustworthiness of electronic identity management systems: Framework and insights from inception to deployment. *arXiv preprint*. <https://doi.org/10.48550/arXiv.2502.10771>
7. Hayes de Kalaf, E., Fernandes, K. (2023). Digital Identity: Emerging Trends, Debates and Controversies. <http://dx.doi.org/10.13140/RG.2.2.23898.56005>
8. Tiits, M., Kalvet, T., McBee, D. (2024). Identity theft and societal acceptability of electronic identity in Europe and in the United States. *arXiv preprint*. <https://doi.org/10.48550/arXiv.2412.07445>
9. Turha, K., Vrhovec, S., & Bernik, I. (2024). State surveillance in the digital age: Factors associated with citizens' attitudes towards trust registers. *arXiv preprint*. <https://doi.org/10.48550/arXiv.2408.09725>

10. Gupta, P., Hooda, A., Jeyaraj, A. et al. Trust, Risk, Privacy and Security in e-Government Use: Insights from a MASEM Analysis. *Inf Syst Front* (2024). <https://doi.org/10.1007/s10796-024-10497-8>
11. European Commission. (2024). *Report on the State of the Digital Decade 2024*. <https://digital-strategy.ec.europa.eu/en/library/report-state-digital-decade-2024>
12. Sedlmeir, J., Smethurst, R., Rieger, A. et al. Digital Identities and Verifiable Credentials. *Bus Inf Syst Eng* 63, 603–613 (2021). <https://doi.org/10.1007/s12599-021-00722-y>
13. United Nations Development Programme (UNDP). (2025). *Ukrainians' satisfaction with government e-services on the rise, KIIS survey finds*. Retrieved from <https://www.undp.org/ukraine/press-releases/ukrainians-satisfaction-government-e-services-rise-kiis-survey-finds>
14. Hromadske. (2020, May 22). *Via a Telegram bot, a database of 26 million driver's licenses was leaked — the SBU has launched an investigation*. Hromadske. Retrieved from <https://hromadske.ua/posts/cherez-telegram-bot-zlili-bazu-z-26-mln-vodijskih-posvidchen-za-spravu-vzyalasya-sbu>

DOI 10.33111/vz_kneu.40.25.03.05.032.038

УДК 001.89

Бойко Олексій,
аспірант кафедри регіоналістики і туризму
Київського національного економічного університету ім. Вадима Гетьмана.
e-mail: 3625319@gmail.com
<https://orcid.org/0000-0003-3676-6043>

Оболенський Олексій,
д.е.н., професор кафедри регіоналістики і туризму
Київського національного економічного університету ім. Вадима Гетьмана.
e-mail: knauob@ukr.net
<https://orcid.org/0000-0001-6828-9224>

МЕТОД МОРФОЛОГІЧНОГО АНАЛІЗУ СУЧАСНИХ МОДЕЛЕЙ ПУБЛІЧНОГО УПРАВЛІННЯ

Boiko Oleksii, PhD
student, Department of Regional Studies and Tourism,
Kyiv National Economic University named after Vadym Hetman.
e-mail: 3625319@gmail.com <https://orcid.org/0000-0003-3676-6043>
+380949272319

Obolenskyi Oleksii,
Doctor of Economics,
Professor, Department of Regional Studies and Tourism,
Kyiv National Economic University named after Vadym Hetman.
e-mail: knauob@ukr.net
<https://orcid.org/0000-0001-6828-9224>

THE METHOD OF MORPHOLOGICAL ANALYSIS OF CONTEMPORARY MODELS OF PUBLIC GOVERNANCE

Анотація. У статті здійснено теоретико-методичне обґрунтування застосування морфологічного аналізу для систематизації, порівняння та проектування моделей публічного управління. Проведено аналіз поширених моделей публічного управління — Традиційного публічного адміністрування, Нового публічного