УДК: 65.012.8 DOI 10.33111/mise.104.3

Бєгун А.В.,
к.е.н., професор, професор кафедри системного аналізу та кібербезпеки,
КНЕУ імені Вадима Гетьмана
Апостол А.В.,
аспірант кафедри системного аналізу та кібербезпеки,
КНЕУ імені Вадима Гетьмана

Begun A.V.,
PhD in Economics, Professor of the Department of Sy
stems Analysis and Cybersecurity,
KNEU named after Vadym Hetman
Apostol A.V.,
PhD student of the Department of Systems Analysis and Cybersecurity,
KNEU named after Vadym Hetman

ЦИФРОВА ІДЕНТИФІКАЦІЯ ЯК КЛЮЧ ДО НОВИХ БІЗНЕС-МОДЕЛЕЙ ЗАХИСТУ ІНФОРМАЦІЇ

DIGITAL IDENTIFICATION AS THE KEY TO NEW INFORMATION PROTECTION BUSINESS MODELS

***Анотація**. У статті досліджено поняття цифрової ідентичності та цифрової ідентифікації, їхній вплив на трансформацію бізнес-моделей та оптимізацію бізнес-процесів у сучасній цифровій економіці. Розглянуто основні моделі цифрової ідентичності — централізовану, децентралізовану та гібридну — з прикладами їхнього впровадження у світі. Проаналізовано інноваційні бізнес-моделі, які виникли завдяки цифровій ідентичності, зокрема Identity as a Service (IDaaS), Self-Sovereign Identity (SSI), цифрові гаманці та P2P-платформи. Визначено переваги цифрової ідентифікації, включно зі зменшенням витрат, підвищенням довіри, персоналізацією послуг та автоматизацією процесів. Підсумовано, що цифрова ідентифікація є ключовим чинником розвитку сучасної економіки, забезпечуючи ефективність, безпеку та інноваційність бізнесу.*
***Ключові слова**: цифрова ідентичність, цифрова ідентифікація, бізнес-моделі, цифрова економіка, децентралізована ідентичність, Self-Sovereign Identity, Identity as a Service, цифрові гаманці, Verifiable Credentials, інновації, блокчейн.*

***Abstract**. The article explores the concepts of digital identity and digital identification, highlighting their impact on the transformation of business models and the optimization of business processes in the modern digital economy. The study examines the main models of digital identity—centralized, decentralized, and hybrid—with examples of their implementation worldwide. It analyzes innovative business models enabled by digital identity, such as Identity as a Service (IDaaS), Self-Sovereign Identity (SSI), digital wallets, and P2P platforms. The advantages of digital identification are identified, including cost reduction, trust enhancement, service personalization, and process automation. The article concludes that digital identification is a key driver for the development of the modern economy, ensuring efficiency, security, and innovation in business operations.*

***Keywords**: digital identity, digital identification, business models, digital economy, decentralized identity, Self-Sovereign Identity, Identity as a Service, digital wallets, Verifiable Credentials, innovations, blockchain.*

Постановка проблеми. Сучасна економіка базується на транзакціях — обміні товарами, послугами, інформацією чи капіталом між учасниками ринку. Ефективність транзакцій є рушійною силою розвитку бізнесу та економічних систем загалом. У зв'язку з цим, питання швидкості, прозорості та непідробності транзакцій стало одним з ключових для бізнесу і економіки в цілому.

Традиційний «паперовий» підхід до організації транзакцій має значні недоліки. Укладання договорів потребує багато часу через логістичні затримки, необхідність фізичного підпису, штампування документів, а також значні витрати на підтримку архівів — багато компаній створюють окремі відділи для управління документообігом та архівами. Окрім того, ані підпис, ані штамп не гарантують повної непідробності документа — сучасні технічні засоби дозволяють з легкістю підробити і фізичний підпис, і мокру печатку. Така система застаріла, особливо у сучасному світі, пронизаному інформаційними технологіями, де бізнес прагне швидкості, оптимізації витрат і підвищення ефективності.

Логічним рішенням для усунення цих недоліків є цифровізація транзакцій. Вона дозволяє значно скоротити час на обробку документів і забезпечує зручність обміну даними, значно зменшує витрати на логістику, архівування та звітування. Проте питання непідробності залишається відкритим навіть у цифровій сфері, що створює потребу в більш досконалих технологіях захисту даних.

Цифрова ідентифікація є відповіддю на виклики сучасного бізнесу. Вона забезпечує не лише непідробність, але й швидкість обробки транзакцій, підвищує рівень довіри між сторонами, дозволяючи автоматизувати значну частину рутинних процесів. Це докорінно змінює принципи ведення бізнесу, автоматизуючи раніше трудомісткі процеси, такі як документообіг чи ведення фінансів.

У результаті таких трансформацій змінюються традиційні бізнес- моделі, а на їх місці виникають нові, які адаптовані до умов цифрової економіки. Цифрова ідентифікація відкриває шлях до ефективного використання ресурсів, усуваючи бар'єри на шляху до інноваційного розвитку бізнесу та суспільства.

Метою статті є розкриття понять цифрової ідентичності та цифрової ідентифікації, їх взаємозв'язку, а також їх впливу на трансформацію сучасних бізнес-процесів та бізнес-моделей. Основними завданнями є:

1. Розкрити сутність понять «цифрова ідентичність» та «цифрова ідентифікація», окреслити їх взаємозв'язок та значення для сучасних бізнес-процесів і цифрової економіки загалом.

2. Проаналізувати сучасні дослідження та практики у сфері цифрової ідентичності та ідентифікації, висвітлити основні тенденції, проблеми та виклики, які супроводжують їхнє впровадження.

3. Окреслити вплив цифрової ідентифікації на основі цифрової ідентичності на трансформацію бізнес-моделей, зокрема їхню оптимізацію, адаптацію до вимог цифрової економіки, а також стимулювання появи нових інноваційних бізнес-моделей, що здатні відповідати викликам та можливостям сучасного світу.

Виклад основного матеріалу. У сучасному світі цифрова ідентичність (Digital Identity) стає ключовим елементом цифрового середовища, забезпечуючи можливість ідентифікації суб'єкта — особи, організації, тварини, пристрою тощо [1]. Це сукупність електронних даних, які створюють унікальне представлення суб'єкта в цифровому просторі. Цифрова ідентичність виконує важливу функцію у доступі до онлайн- сервісів, автентифікації користувачів і персоналізації транзакцій.

На відміну від фізичної ідентичності, яка базується на матеріальних атрибутах, таких як паспорт або підпис, цифрова ідентичність існує у вигляді електронних даних, зокрема логінів, електронних адрес чи унікальних ідентифікаторів. Її головна перевага — доступність із будь-якої точки світу через Інтернет, що значно спрощує процеси обміну даними. Вона також є динамічною — змінюється в реальному часі залежно від активності користувача або оновлення даних у базах сервісів. Цифрова

ідентичність повинна бути прив'язана до конкретного суб'єкта через унікальні ідентифікатори [1], що забезпечує її неповторність і створює основу для довіри у цифрових транзакціях.

Цифрова ідентичність має ще одну важливу особливість — множинність. У той час як фізична ідентичність є універсальною та прив'язана до офіційних документів, цифрова дозволяє користувачеві створювати різні ідентичності для різних платформ чи цілей [2]. Наприклад, окремий профіль для банківських послуг і для соціальних мереж. Це робить її контекстуальною, тобто дані, які використовуються для однієї платформи, можуть бути непридатними для іншої.

Унікальність, динамічність та масштабованість цифрової ідентичності роблять її важливим інструментом у цифровій економіці завдяки її здатності забезпечувати доступ до ресурсів, автоматизувати процеси та створювати довіру між учасниками ринку.

Зокрема цифрова ідентичність сприяє швидкому укладенню угод, зменшує витрати на адміністрування, спрощує доступ до фінансових послуг і дозволяє персоналізувати клієнтський досвід. Цифрова ідентичність є фундаментом для таких технологій, як електронний підпис, цифрові гаманці та децентралізовані ідентифікаційні системи [1], які відкривають нові можливості для взаємодії між користувачами та організаціями в цифровому середовищі.

Таким чином, цифрова ідентичність не лише замінює традиційні методи ідентифікації, а й відкриває шлях до нових підходів, що визначають сучасний цифровий світ. Її значення постійно зростає, формуючи фундамент для інновацій у бізнесі, державному управлінні та повсякденному житті.

Сьогодні існує декілька підходів до зберігання, обробки та управління ідентифікаційними даними. Вони визначають моделі цифрової ідентичності, які формують спосіб організації таких даних. Ці моделі — централізована, децентралізована та гібридна — забезпечують різні рівні

безпеки, прозорості та контролю, адаптуючись до потреб як окремих користувачів, так і організацій.

Централізована модель передбачає, що всі дані про ідентичність зберігаються в одному місці — централізованій базі даних, керованій єдиним провайдером. Ця модель використовується урядами або великими компаніями, які гарантують автентичність даних користувачів. Централізовані системи спрощують адміністрування, але мають критичний недолік — значний ризик зловживання та витоку даних. Наприклад, Aadhaar в Індії є класичним прикладом централізованої моделі, яка, попри свої переваги, викликала багато питань щодо конфіденційності [2].

Децентралізована модель, зокрема Self-Sovereign Identity (SSI), покладається на розподілені реєстри (DLT, блокчейн), що дозволяють користувачам зберігати та контролювати свої дані самостійно. Це підхід, що отримав підтримку у багатьох країнах, таких як Канада та Німеччина [1]. Децентралізовані системи дозволяють уникнути єдиного джерела вразливості [3], що робить їх надійнішими, хоча вони стикаються з технічними викликами, такими як масштабованість та інтероперабельність. Ключовим елементом цієї моделі є Verifiable Credentials (VC) — перевірювані креденціали, які забезпечують контроль користувача над своїми даними та їхню конфіденційність. Використання VC дозволяє передавати лише необхідну інформацію, зберігаючи решту даних приватними [4], що особливо важливо для забезпечення захисту особистої інформації в розподілених системах. VC

спрощують процес автентифікації, знижують залежність від центральних авторитетних установ і забезпечують прозорість у цифрових транзакціях. Особливу роль у цьому відіграють цифрові гаманці, які інтегрують VC, надаючи ефективні засоби для децентралізованої ідентифікації [1].

Децентралізована модель цифрової ідентичності вичерпно реалізована у системі Sovrin. Sovrin базується на технології блокчейн і дозволяє

користувачам створювати та управляти своїми ідентифікаційними даними через децентралізовані ідентифікатори (DIDs) та перевірювані креденціали. У цій моделі кожен користувач отримує унікальний ідентифікатор (DID), який зберігається у розподіленому реєстрі. Самі дані користувача залишаються локально у його цифровому гаманці. Коли сторонній сервіс, наприклад банк, запитує ідентифікаційну інформацію, користувач передає тільки необхідні дані через VC. Для перевірки автентичності цифровий підпис на VC перевіряється у блокчейні через публічний ключ організації, яка видала креденціал [5]. Це гарантує прозорість та довіру у процесі обміну даними, зберігаючи конфіденційність користувача.

Гібридна модель цифрової ідентичності поєднує переваги централізованих і децентралізованих підходів, створюючи баланс між безпекою, ефективністю та контролем користувача. У цій моделі ключові дані, такі як громадянство чи унікальні ідентифікатори, зберігаються централізовано в державних або корпоративних реєстрах, які виступають як довірені джерела для верифікації. Водночас перевірювані креденціали, що базуються на цих даних, створюються державними чи сертифікаційними органами, але зберігаються локально в цифрових гаманцях користувачів.

Гібридна модель, наприклад, реалізована в ініціативі eIDAS у ЄС, забезпечує централізоване підтвердження базових атрибутів через національні реєстри, але контроль за доступом до цих даних передається користувачам через децентралізовані інструменти [6]. Наприклад, користувач може підтвердити свою особу або місце проживання для банку, використовуючи цифровий гаманець, не розкриваючи додаткової інформації. Використання перевірюваних креденціалів, які зберігаються локально в цифрових гаманцях, дозволяє гібридній моделі поєднувати централізоване зберігання критичних даних із децентралізованим управлінням доступом до них. Це відкриває можливості для використання цифрових ідентифікаційних платформ у різних секторах, від фінансових послуг до державного управління, де потрібен високий рівень безпеки та ефективності.

У той час, як цифрова ідентичність є набором даних, що визначає суб'єкт у цифровому просторі, цифрова ідентифікація є процесом перевірки цих даних для підтвердження особи. Ці поняття взаємопов'язані: ідентичність створює основу, а ідентифікація забезпечує її практичне застосування у транзакціях.

Уявімо, що користувач бажає орендувати квартиру на платформі короткострокової оренди. Для цього платформа потребує підтвердження особи, зокрема інформації про вік орендаря та його платоспроможність. Користувач через свій цифровий гаманець надає платформі DID і VC, видані авторитетними установами, такими як уряд і банк. Наприклад, VC від банку підтверджує платоспроможність, а VC від уряду засвідчує, що користувач досягнув повноліття. Дані, надані користувачем, проходять перевірку на платформі через розподілений реєстр. Платформа використовує відкриті ключі установ, які видали згадані VC, для перевірки їхньої автентичності. Якщо підпис на VC успішно проходить перевірку відкритим ключем, це підтверджує дійсність наданих даних. Завдяки цьому платформа отримує лише необхідну інформацію — підтвердження віку та платоспроможності, без доступу до зайвих деталей, таких як адреса чи сума доходу.

Після успішної перевірки платформа авторизує користувача, дозволяючи завершити бронювання. Це і є прикладом цифрової ідентифікації, яка використовує цифрову ідентичність. Вона демонструє, як можна поєднати безпеку, зручність і конфіденційність.

DID стали ключовим компонентом сучасних систем цифрової ідентифікації, дозволяючи створювати безпечні механізми підтвердження особи. Концепція цифрової ідентичності активно впроваджується, підтримується і розвивається різними державами. Розгляньмо детальніше кілька прикладів успішної реалізації цієї ідеї, зокрема і ті, про які ми згадували вище.

eIDAS (Electronic Identification, Authentication, and Trust Services) є регламентом Європейського Союзу, прийнятим у 2014 році, який створює правову основу для електронної ідентифікації, автентифікації та довірчих послуг у країнах-членах ЄС. Його головна мета — забезпечити взаємодію між національними системами цифрової ідентифікації, що дозволяє громадянам і компаніям користуватися державними та приватними послугами у транскордонному режимі [6].

Основними елементами eIDAS є:

1. Взаємне визнання електронної ідентифікації. Система eIDAS вимагає від країн-членів ЄС взаємного визнання національних електронних ідентифікацій. Це створює уніфікований простір для циф-

рових транзакцій, дозволяючи громадянам і підприємствам використовувати свої eID для транскордонного доступу до послуг. Наприклад, громадянин Німеччини може користуватися електронними послугами в Австрії за допомогою своєї національної електронної ідентифікації.

2. Використання мобільних технологій. eIDAS сприяє впровадженню мобільних eID, які розширюють можливості використання цифрової ідентичності, забезпечуючи її доступність через різні канали. Мобільні рішення дозволяють громадянам виконувати транзакції без фізичних карток, забезпечуючи високий рівень безпеки через криптографічний захист даних.

3. Сумісність з блокчейн-технологіями. У контексті цифрової ідентифікації eIDAS розглядає можливість інтеграції технологій розподілених реєстрів (DLT), що забезпечують прозорість та підвищують довіру до системи цифрової ідентифікації. І хоча зараз це ще не реалізовано, перевірювані креденціали eIDAS повністю сумісні з ідеологією блокчейну.

На практиці eIDAS застосовано, наприклад, у платформі DigiD в Нідерландах [6]. Він забезпечує інтеграцію з міжнародними сервісами, такими як подача податкових декларацій чи отримання медичних послуг. Цей підхід відкриває можливість громадянам отримувати доступ до транскордонних послуг, використовуючи єдину цифрову ідентичність.

Програма e-Residency в Естонії дозволяє нерезидентам отримувати цифрову ідентичність для ведення бізнесу в ЄС. e-Residency також базується на принципах eIDAS, підтримуючи цифрові підписи та транскордонну автентифікацію, що сприяє розширенню міжнародної підприємницької діяльності.

Разом з тим, впроваджуючи eIDAS, держави ЄС стикаються з рядом викликів. Серед них можна перелічити такі:

1. Технічна інтероперабельність. Попри узагальнену правову основу, різні технічні стандарти між країнами ускладнюють інтеграцію національних систем цифрової ідентифікації.

2. Освіченість користувачів. Громадянам та організаціям потрібен час і ресурси для адаптації до нових технологій, що гальмує поширення eIDAS у деяких регіонах.

3. Інвестиції у передові технології. Впровадження високотехнологічних рішень, наприклад мобільних eID, потребує значних фінансових витрат, що може стати бар'єром для країн із обмеженими ресурсами.

Іншим прикладом реалізації цифрової ідентичності та ідентифікації є індійська система Aadhaar. Це масштабна централізована

система цифрової ідентифікації [1], яка надає кожному громадянину унікальний 12-значний ідентифікаційний номер, що пов'язаний з його біометричними даними (відбитками пальців та скануванням райдужної оболонки ока) і

демографічною інформацією. Запущена у 2009 році, система Aadhaar стала важливим інструментом для оптимізації надання державних послуг і боротьби з корупцією.

Основними особливостями Aadhaar є:

1. Надання єдиного ідентифікатора для всіх послуг. Система Aadhaar надає універсальний ідентифікатор, який забезпечує доступ до державних програм, таких як субсидії, соціальні виплати та медичні послуги. Завдяки централізованому зберіганню даних система запобігає дублюванню записів і мінімізує шахрайство.

2. Біометрична автентифікація. Система використовує біометричні дані, що дозволяє точно ідентифікувати особу. Це підвищує надійність перевірки та знижує ймовірність неправомірного використання документів.

3. Мультисекторальність. Aadhaar використовується банківським сектором, мобільними операторами та інших установами для автентифікації клієнтів. Наприклад, вона спрощує процес відкриття банківських рахунків, замінюючи традиційні документи наданими ідентифікаційними даними.

Aadhaar стала основою для багатьох ключових ініціатив. Вона використовується, наприклад, в програмі Direct Benefit Transfer (DBT), яка дозволяє переказувати державні субсидії безпосередньо на банківські рахунки громадян. Завдяки цьому підходу вдається усунути посередників, зменшити рівень корупції та забезпечити цільове використання коштів.

Ще одним прикладом є процес реєстрації SIM-карток — мобільні оператори використовують Aadhaar для оперативного підтвердження особи. Цей процес автоматизований і базується на біометричній автентифікації, що дозволяє знизити ризики шахрайства і забезпечити точність даних користувачів.

Хоча Aadhaar забезпечує значні переваги, такі як оптимізація державних програм, зменшення рівня корупції та розширення доступу до фінансових послуг, система зазнала суттєвої критики через серйозні ризики, зокрема у сферах конфіденційності, безпеки даних та доступності.

Одним із найбільших викликів є забезпечення конфіденційності та безпеки даних. Централізоване зберігання біометричної та демографічної інформації громадян робить систему вразливою до кібератак та неправомірного використання даних. Наприклад, у

2017 році було зафіксовано масштабний витік даних — урядове пенсійне управління штату Керала без дозволу скопіювало дані (фотографії, номери телефонів, особисті ідентифікатори, банківські рахунки) більше ніж 3.5 млн громадян з системи Aadhaar та виклало їх у себе на веб-сайті [1]. Це значно нашкодило іміджеві системи.

Ще однією проблемою є технологічна доступність. У багатьох віддалених регіонах Індії з низьким рівнем доступу до Інтернету використання Aadhaar залишається складним. Це обмежує її ефективність і створює нерівність у доступі до послуг, особливо серед сільського населення.

Також Aadhaar зіткнулася з юридичними бар'єрами. У 2018 році Верховний суд Індії постановив, що приватний сектор не може примусово вимагати в громадян їхні Aadhaar-ідентифікатори. Це рішення обмежило масштаби комерційного застосування системи у приватному секторі, таким чином унеможливлюючи універсальне застосування Aadhaar.

Після аналізу ініціатив eIDAS та Aadhaar, які представляють гібридні та централізовані моделі цифрової ідентифікації, варто звернути увагу на децентралізовані підходи, які набувають все більшого поширення. Одним із яскравих прикладів є Verifiable Organizations Network (VON), ініціатива, розроблена в Канаді, яка демонструє, як технології децентралізованих ідентифікаторів і перевірюваних креденціалів можуть бути інтегровані у бізнесові та державні процеси [1].

Система VON дозволяє організаціям отримувати унікальні цифрові ідентифікатори (DID) разом із наборами VC, які містять ключові атрибути, такі як реєстраційні дані, ліцензії чи сертифікати. Використовуючи цифровий гаманець, організації можуть самостійно управляти цими даними, спираючись на ідеологію SSI. Це забезпечує безпечну, ефективну і прозору взаємодію з державними та приватними установами.

Практичне застосування VON охоплює різноманітні сценарії. Наприклад, під час оновлення ліцензії організація може надати необхідні VC через електронний портал, що дозволяє миттєво перевірити достовірність даних і завершити процес без зайвої бюрократії. Участь у тендерах також спрощується завдяки можливості надання VC, які автоматично підтверджують відповідність тендерним вимогам.

Важливою перевагою VON є зниження ризиків підробки документів через використання блокчейн-технології для зберігання DID. Система автоматизує перевірку документів, що скорочує час

транзакції і підвищує довіру між сторонами. Крім того, організації зберігають контроль над своїми даними, надаючи тільки ту інформацію, яка є необхідною для конкретного запиту.

Однак впровадження VON стикається з викликами. Зокрема, масштабування системи вимагає значних ресурсів, а адаптація правового поля для інтеграції таких ініціатив потребує часу. Незважаючи на це, VON закладає основу для ефективнішої цифрової економіки, пропонуючи рішення для сучасних викликів у взаємодії між організаціями.

Навіть такий короткий огляд показує, наскільки потужною, ефективною та перспективною є ідея цифрової ідентичності та ідентифікації. Вона докорінно змінює традиційні бізнес-моделі, впроваджуючи автоматизацію процесів, знижуючи операційні витрати та підвищуючи ефективність взаємодії між учасниками ринку. Використання децентралізованих ідентифікаторів (DID) та перевірюваних креденціалів (VC) дозволяє бізнесу оптимізувати процес перевірки даних, при цьому зберігаючи конфіденційність і довіру.

Системи цифрової ідентифікації, такі як Aadhaar в Індії, трансформують підхід до надання послуг. Використовуючи єдині ідентифікатори, компанії можуть автоматизувати перевірку особи клієнтів, що знижує витрати та усуває потребу в численних документах. Наприклад, банки використовують Aadhaar для автоматизованого відкриття рахунків, значно скорочуючи час обслуговування та мінімізуючи ризики шахрайства. У Європі ініціатива eIDAS полегшує транскордонну співпрацю завдяки інтеграції національних систем цифрової ідентифікації. Це спрощує вихід компаній на міжнародні ринки, знижуючи бюрократичні бар'єри та дозволяючи бізнесу швидше адаптуватися до нових умов.

Система Verifiable Organizations Network (VON) у Канаді показує, як цифрова ідентифікація трансформує бізнес-процеси. Організації можуть використовувати DID і VC для швидкої перевірки ліцензій, сертифікатів і фінансових даних. Наприклад, участь у тендерах стає простішою: замість паперових документів компанії надають цифрові креденціали, які автоматично перевіряються через блокчейн. Це зменшує час і витрати на підготовку тендерів, підвищуючи прозорість і довіру в процесі.

Цифрова ідентифікація відкриває можливості для персоналізації послуг, дозволяючи компаніям адаптувати свої пропозиції до уподобань і поведінки клієнтів. Використання перевірюваних креденціалів забезпечує доступ лише до необхідної інформації, що дозволяє створювати індивідуальний досвід для кожного клієнта, зберігаючи конфіденційність.

Цифрова ідентичність дала також поштовх до появи нових бізнес-моделей, які трансформують способи надання послуг, управління даними та побудови довіри між учасниками ринку. Ці моделі охоплюють різноманітні сектори — від фінансових послуг до електронної комерції — і ґрунтуються на інноваційних підходах, які створюють нові можливості для монетизації.

Однією з таких моделей є Identity as a Service (IDaaS) — концепція, яка полягає у наданні хмарних рішень для автентифікації, управління доступом і перевірки особи. Okta є провідною компанією, яка впроваджує модель IDaaS, надаючи організаціям платформу для централізованого управління цифровою ідентифікацією, що забезпечує безпечний доступ до додатків, пристроїв і мереж. Okta також активно досліджує перспективи розподілених моделей цифрової ідентичності, вбачаючи в них майбутнє розвитку галузі. Компанія вважає, що децентралізовані підходи сприятимуть підвищенню рівня конфіденційності та контролю користувачів над своїми даними, що стає все більш важливим у сучасному цифровому світі [8].

Питання децентралізованих моделей цифрової ідентифікації активно досліджувалося багатьма компаніями та організаціями, що зрештою призвело до виникнення бізнес-моделі провайдерів згадуваної вище Self- Sovereign Identity (SSI). Ця модель, на відміну від IDaaS, спрямована на те, щоб надати користувачам повний контроль над їхніми ідентифікаційними даними, які зберігаються у захищених цифрових гаманцях. Монетизація таких сервісів зазвичай базується на ліцензіях на програмне забезпечення, інтеграційних послугах та консультаційній підтримці корпоративних та державних клієнтів. Однак провайдери SSI також надають свої рішення для підтримки суспільно важливих ініціатив. Наприклад, компанія Evernym бере участь в ініціативі ID2020, яка об'єднує зусилля міжнародних організацій, урядів і бізнесу для створення етичних та безпечних підходів до ідентифікації. Ці проєкти спрямовані на підтримку найбільш уразливих груп населення, забезпечуючи їх цифровою ідентичністю безкоштовно в рамках гуманітарних ініціатив [10].

Цифрові гаманці, які часто використовуються у рамках моделі SSI, самі по собі стали окремою інноваційною бізнес-моделлю, що виникла під впливом цифрової ідентичності. Вони дозволяють зберігати ідентифікаційні дані, платіжні засоби та перевірювані кредениціали (VC) у захищеному електронному форматі, пропонуючи користувачам зручність у повсякденному житті. Популярні сервіси, такі як Google Wallet чи Apple Pay, не тільки інтегрують

цифрові ідентифікатори, але й слугують платформами для здійснення платежів і підтвердження особи [9]. Монетизація цифрових гаманців базується на комісіях за транзакції, співпраці з ритейлерами та інтеграції з фінансовими установами.

P2P-платформи, такі як сервіси короткострокової оренди житла або продажу товарів, використовують цифрову ідентичність для покращення довіри між користувачами. Наприклад, на основі децентралізованих ідентифікаторів платформи можуть перевіряти репутацію орендодавців та орендарів. Це дозволяє мінімізувати ризики шахрайства і тим самим залучати більше клієнтів. Заробіток таких платформ базується на комісіях із транзакцій, а також на платних послугах, таких як пріоритетне розміщення пропозицій або преміальні підписки для користувачів.

Висновок. Ідентифікація на базі цифрової ідентичності має величезний потенціал і обіцяє трансформувати сучасний економічний ландшафт. Завдяки здатності автоматизувати перевірку даних, усувати посередників і зменшувати операційні витрати, цифрова ідентифікація оптимізує бізнес-процеси та підвищує ефективність у різних секторах. Її використання відкриває нові можливості для персоналізації послуг, створення довіри між учасниками ринку та забезпечення конфіденційності даних.

Цифрова ідентичність стала рушієм для появи інноваційних бізнес-моделей, таких як Identity as a Service (IDaaS), Self-Sovereign Identity (SSI), цифрові гаманці та P2P-платформи. Ці моделі не лише змінюють способи надання послуг, але й створюють нові джерела монетизації, сприяючи зростанню економічної активності. Водночас вони знижують ризики шахрайства, забезпечують високу швидкість транзакцій та підтримують етичні принципи управління ідентифікацією, особливо у гуманітарних ініціативах.

Цифрова ідентифікація не лише відповідає вимогам сучасної цифрової економіки, а й стає її фундаментом, сприяючи інноваціям і довірі. Її впровадження допомагає бізнесу адаптуватися до нових викликів, зменшуючи адміністративний тягар та забезпечуючи клієнтам більш зручний і захищений доступ до послуг. Майбутнє цифрової ідентичності обіцяє ще більше інновацій, зміцнюючи її роль як ключового елемента глобальної цифрової екосистеми.

Бібліографічні посилання

1. Sedlmeir, J., Rieger, A., Fridgen, G., & Urbach, N. (2021). Digital Identities and Verifiable Credentials. Business & Information Systems Engineering, 63(5), 603–613.

Goodell, Geoff & Aste, Tomaso. (2019). A Decentralized Digital Identity Architecture. Frontiers in Blockchain. 2. 17. 10.3389/fbloc.2019.00017.

2. Гончарова А. В. (2024). Елементи цифрової ідентичності. Науковий вісник Ужгородського національного університету. Серія Право, (83), 187–191.

3. Lux, Zoltán & Thatmann, Dirk & Zickau, Sebastian & Beierle, Felix. (2020). Distributed-Ledger-based Authentication with Decentralized Identifiers and Verifiable Credentials. 71–78. 10.1109/BRAINS49436.2020. 9223292.

4. Windley, Phillip. (2021). Sovrin: An Identity Metasystem for Self-Sovereign Identity. Frontiers in Blockchain. 4. 10.3389/fbloc.2021.626726.

Ruiu, Pietro & Saiu, Salvatore & Grosso, Enrico. (2024). Digital Identity in the EU: Promoting eIDAS Solutions Based on Biometrics. Future Internet. 16. 228. 10.3390/fi16070228.

5. Supreme Court Observer. «Constitutionality of Aadhaar Act: Judgment Summary.» Supreme Court Observer, September 26, 2018. https://www.scobserver.in/reports/constitutionality-of- aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain- english/.

6. Okta. «We See Decentralized Identity in Our Future.» Okta Blog, July 2021. https://www.okta.com/blog/2021/07/we-see- decentralized-identity-in-our-future/.

7. Stapelberg, Alan. «How we're working to make digital identity a reality for everyone.» The Keyword: Google Blog, July 20, 2022. https://blog.google/products/google-pay/google-wallet-digital-id-privacy-security/.

8. The Paypers. «Evernym Joins the Red Cross to Develop Digital Identity Project.» The Paypers, January 31, 2019. https://thepaypers.com/news/evernym-joins-the-red-cross-to- develop-digital-identity-project.

Статтю подано до редакції: 14.11.2024