УДК 35.077.3(477):004.056.52
DOI https://doi.org/10.32782/2312-1815/2025-21-22

Тарас Курус
ORCID: 0009-0007-8167-2683

ГЛОБАЛЬНИЙ СТАНДАРТ АВТОРИЗАЦІЇ ТА УКРАЇНСЬКА ДЕРЖАВНА ІНФРАСТРУКТУРА: ОГЛЯД, ВИКЛИКИ, МОЖЛИВОСТІ

Стаття висвітлює компонент Diia OAuth інтегрованої системи електронної ідентифікації України (ID.GOV.UA) як один із ключових вузлів, необхідних для практичної реалізації концепції «Government as a Platform» (Тім О'Райлі) [5]. Ця концепція передбачає, що держава концентрується на створенні базової цифрової інфраструктури: відкритих реєстрів, стандартизованих API та сервісів електронної ідентифікації, натомість екосистема приватних і громадських розробників будує кінцеві застосунки для громадян. Центральну увагу приділено Diia OAuth, який слугує державним API-шлюзом для безпечної автентифікації та авторизації користувачів, відкриваючи розробникам можливість інтегрувати перевірені ідентифікаційні дані у власні цифрові послуги.

Результати підтверджують, що Diia OAuth, залишаючись сумісною з базовою логікою authorization code flow протоколу OAuth 2.0, одночасно враховує локальні правові та архітектурні вимоги. Водночас відсутність параметра scope у національній імплементації викликає занепокоєння, адже саме він забезпечує гнучке розмежування прав доступу та надає авторизації більшу глибину, а не зводить процес лише до автентифікації.

Використання світових стандартів формує відкрите середовище, у якому приватний сектор може створювати інноваційні цифрові послуги, що підвищуватимуть ефективність публічних сервісів і сприятимуть технологічному прогресу, зокрема у такій сфері, як електронне голосування.

Практична цінність полягає у формулюванні рекомендацій щодо подальшої стандартизації державних API та підтримки екосистеми приватних розробників. Окрему увагу приділено трирівневій моделі довіри, що поєднує технічну стійкість протоколу з юридичною значущістю ідентифікаційних даних.

Ключові слова: *Government as a Platform, електронна ідентифікація, Diia OAuth, OAuth 2.0, рівні довіри, цифрові державні послуги, Government as a Platform, електронна ідентифікація, Diia OAuth.*

Вступ. Стрімкий розвиток інформаційно-комунікаційних технологій зумовлює масштабну трансформацію соціальних, економічних і адміністративних процесів у цифровий формат. Зростаюча кількість мобільних та вебзастосунків, які інтегруються у повсякденне життя громадян, формує нову норму взаємодії з інформаційними ресурсами. Отримання, передача та обробка інформації дедалі частіше здійснюються за допомогою цифрових сервісів, що стає звичним інструментом у приватному, корпоративному та державному секторах. Одним із найважливіших аспектів інформаційно-комунікаційних технологій та зручностей, які вони надають, є безпека.

Забезпечення захищеного доступу до інформаційних систем, збереження конфіденційності під час передачі персональних даних, а також запобігання несанкціонованому втручанню – це ключові виклики, що постають перед сучасною цифровою інфраструктурою.

Надійні механізми ідентифікації користувачів є необхідною умовою для забезпечення довіри до цифрових сервісів як у приватному, так і в державному секторі. У зв'язку з великим напливом мобільних та вебзастосунків, а також активним зростанням кількості користувачів, які мають визначені ролі в локальних цифрових системах, виникла потреба у забезпеченні інтеграції між різними платформами та використанні спільної сесії користувача між ними задля

підвищення рівня безпеки, зручності та ефективності їх функціонування. Реалізація таких сценаріїв інтеграції вимагала уніфікованих підходів до ідентифікації, аутентифікації та авторизації користувачів у розподіленому середовищі.

Метою статті є дослідження нормативно-правового виміру довіри до схем електронної ідентифікації, що функціонують у межах інтегрованої системи електронної ідентифікації ID.GOV.UA, з особливою увагою до реалізації механізму Дія.OAuth. У роботі здійснено порівняльний аналіз національного підходу до електронної автентифікації у контексті міжнародного стандарту OAuth 2.0, а також розглянуто електронну ідентифікацію як критично важливий компонент для впровадження концепції «Government as a Platform» в Україні.

Матеріал і методи дослідження. У дослідженні використано комплексний порівняльно-технічний підхід, що поєднує елементи правового аналізу, вивчення технічної документації та емпіричний розгляд реалізації протоколів на прикладі Дія.OAuth. Джерельну базу становлять офіційні міжнародні стандарти (зокрема, RFC 6749), технічні специфікації ID.GOV.UA, а також положення Закону України «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII.

Результати та обговорення. Як зазначають C.-J. Chae, K.-B. Kim та H.-J. Cho [1], перша версія протоколу авторизації – **OAuth 1.0** була оприлюднена у 2007 р., а її оновлена версія – **OAuth 1.0a** [2], що усунула виявлені проблеми безпеки, з'явилася у червні 2008 р. У 2010 р. цей протокол був зареєстрований як офіційний стандарт **IETF** (Internet Engineering Task Force) – міжнародної організації, що займається розробленням та підтримкою технічних стандартів для Інтернету. Подальший розвиток концепції авторизації призвів до появи **OAuth 2.0** [3], проєкт якого був представлений у 2012 р., а в жовтні того ж року він був затверджений як стандарт IETF (рис. 1).

Актуальність та глобальне поширення стандарту OAuth підтверджуються динамікою інтересу до цього протоколу в Інтернет-просторі. Згідно з даними Google Trends, починаючи з 2009 р., коли OAuth почав активно впроваджуватися у практиці розроблення цифрових сервісів, рівень зацікавлення неухильно зростав. На графіку простежується стійке зростання запитів, що досягає пікових значень у 2024–2025 рр., що свідчить про широку актуальність протоколу як для технічних спільнот, так і для державного та приватного секторів у всьому світі.

У контексті розвитку електронної ідентифікації в Україні слід відзначити наукові напрацювання низки українських дослідниць, які комплексно аналізують елементи цифрової трансформації публічного управління. О.Б. Мосій у своїх працях зосереджується на впровадженні електронного урядування в діяльність органів місцевого самоврядування, цифрових стратегіях та використанні електронної ідентифікації громадян у наданні онлайн-послуг, зокрема на прикладі Тернопільської області. В.І. Кохан досліджує ширший спектр питань цифровізації,

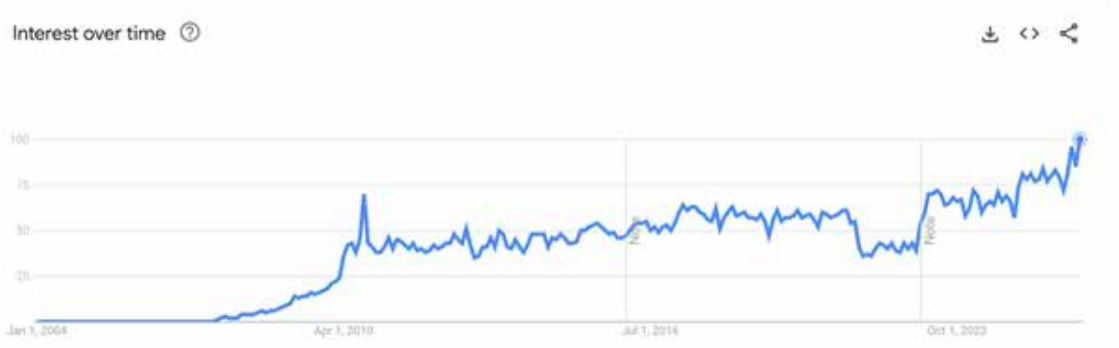

Рис. 1

зокрема цифрові платформи в економіці, розвиток електронних адміністративних послуг, цифрову компетентність громадян та базові правові засади надання е-сервісів. Окрему увагу вона приділяє тематиці електронної ідентифікації та захисту персональних даних у процесі користування державними цифровими послугами. О.В. Лаба у своїх дослідженнях висвітлює етапи розвитку електронного діловодства та аналізує надання електронних послуг крізь призму електронної ідентифікації. Сукупність цих праць формує національний дослідницький дискурс з електронної ідентифікації як ключової компоненти онлайн-сервісів цифрової держави.

В Україні питання електронної ідентифікації регулюється Законом України «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII [4], ухваленим у 2017 р. На виконання цього Закону функціонує **інтегрована система електронної ідентифікації ID.GOV.UA**, яка забезпечує користувачам можливість підтверджувати свою особу в електронному середовищі через різні схеми автентифікації.

Відповідно до ст. 15 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», усі засоби електронної ідентифікації класифікуються за трьома рівнями довіри: **низьким**, **середнім** та **високим**. Така класифікація дає змогу визначати ступінь впевненості у достовірності ідентифікаційних даних користувача, що є особливо важливим у контексті доступу до послуг, пов'язаних із різним рівнем ризику.

Низький рівень довіри стосується засобів електронної ідентифікації, які забезпечують **обмежений ступінь довіри** до заявлених або підтверджуваних ідентифікаційних даних особи. Такі засоби можуть застосовуватися у випадках, де відносно невеликий ризик неправомірного доступу. Вони базуються на мінімальному наборі технічних специфікацій, стандартів і процедур, включаючи базові засоби контролю.

Середній рівень довіри забезпечує **суттєвий ступінь упевненості** у достовірності ідентифікаційних даних. Засоби з таким рівнем довіри застосовують більш складні процедури перевірки особи, а також ефективніші технічні та організаційні заходи, що значно зменшують ризик несанкціонованого доступу чи підміни даних.

Високий рівень довіри характеризується **максимальною впевненістю** у достовірності ідентифікаційних даних користувача. Такі засоби базуються на найбільш жорстких вимогах до технічних специфікацій, криптографічного захисту та організаційних процедур. Вони призначені для використання в контексті дій із високим ступенем юридичної відповідальності, наприклад для підписання електронних договорів або отримання критично важливих державних послуг [4].

Згідно з технічною документацією [6], інтегрована система електронної ідентифікації ID.GOV.UA підтримує низку засобів електронної ідентифікації та автентифікації користувачів, зокрема Дія.Підпис, Дія.OAuth, а також BankID НБУ – сервіс, що забезпечує автентифікацію користувачів через уповноважені банки.

Варто зазначити, що низький рівень довіри до засобу електронної ідентифікації не слід ототожнювати з низьким рівнем технічної безпеки самої схеми автентифікації. У цьому разі йдеться, насамперед, про ступінь упевненості в ідентифікаційних даних особи, а не про криптографічну або протокольну стійкість механізмів доступу. Наприклад, автентифікація користувача в сервісі **Gmail** є технічно безпечною: вона може включати багатофакторну перевірку, токени доступу, шифрування тощо. Однак із погляду державної ідентифікації основними ідентифікаційними даними у цьому разі є **електронна адреса (email)**, яка не має офіційного зв'язку з особою у юридичному розумінні.

Натомість у системах державної електронної ідентифікації, таких як **ID.GOV.UA**, ідентифікація особи здійснюється на основі перевірених державними органами даних: паспортної інформації, податкового номера, ЄДРПОУ тощо. У таких випадках від засобу ідентифікації очікується не лише технічна безпека, а й підтвердження юридично значущого зв'язку між

цифровим профілем і фізичною особою. Саме тому система класифікації за рівнями довіри дає змогу відрізняти надійність технічної реалізації автентифікації від достовірності даних, що ідентифікують користувача.

Варто наголосити, що низький рівень довіри до схеми електронної ідентифікації не означає автоматично низький рівень технічної безпеки самої схеми автентифікації. У цьому контексті йдеться не про стійкість криптографічних алгоритмів або протоколів автентифікації, а про ступінь достовірності ідентифікаційних даних, які пов'язують користувача з його цифровим профілем. Наприклад, автентифікація користувача у сервісі **Gmail** може бути реалізована з високим рівнем технічної безпеки, включаючи двофакторну автентифікацію, використання токенів тощо. Однак сам ідентифікатор у цьому разі – електронна адреса – не є офіційно верифікованим елементом особистості у правовому чи державному значенні.

Натомість у сфері державних електронних послуг ідентифікація повинна базуватися на даних, підтверджених відповідними державними реєстрами, такими як паспортні дані, ІПН тощо або їх мікс (суміш). Тому важливо розділяти технічну безпеку процесу входу в систему (автентифікацію) та надійність і перевіреність даних про особу (ідентифікацію).

У межах розвитку електронних державних сервісів в Україні особливе місце посідає механізм автентифікації **Дія.OAuth**, який функціонує як частина інтегрованої системи електронної ідентифікації та дає змогу стороннім застосункам здійснювати перевірку особи користувача через мобільний застосунок **Дія**. Зовнішній інтерфейс роботи Дія.OAuth наближається до концепції, закладеної у міжнародному протоколі **OAuth 2.0**, що передбачає делегований доступ до захищених ресурсів за допомогою токенів та серверів авторизації. Водночас на практиці реалізація Дія.OAuth має низку концептуальних та технічних відмінностей, які зумовлені як специфікою нормативного середовища, так і архітектурними обмеженнями національної цифрової інфраструктури.

Структура авторизаційного запиту у Дія.OAuth багато в чому повторює логіку протоколу OAuth 2.0. У базовій специфікації OAuth 2.0 визначено чотири основні типи надання прав доступу (*grant types*), кожен з яких має свою сферу застосування:

– **Authorization Code Grant** – найпоширеніший та найбільш безпечний сценарій. Клієнтський застосунок ініціює запит до сервера авторизації, отримує авторизаційний код після згоди користувача, а далі обмінює його на токен доступу. Цей токен використовується для взаємодії з ресурс-сервером без повторного введення облікових даних.

– **Implicit Grant** – застарілий механізм, за якого токен передається безпосередньо через браузер; не рекомендований через високі ризики безпеки.

– **Resource Owner Password Credentials Grant** – використовується в умовах високої довіри до клієнта, коли користувач уводить логін і пароль безпосередньо у застосунок.

– **Client Credentials Grant** – застосовується для міжсервісної взаємодії без участі користувача.

Серед зазначених типів саме **authorization code grant** лежить в основі реалізації **Дія. OAuth**. Що ж, розглянемо порівняльну таблицю 1, яка демонструє відповідність основних елементів реалізації протоколу **OAuth 2.0** у класичному вигляді та у національній реалізації через **Дія.OAuth** у межах інтегрованої системи **ID.GOV.UA**.

Як видно з наведеної таблиці 1, реалізація Дія.OAuth загалом відтворює базові принципи протоколу OAuth 2.0, зокрема логіку сценарію **authorization code grant**. Ключові параметри авторизаційного запиту (response_type, client_id, redirect_uri, state) відповідають стандарту, однак відсутність параметра scope обмежує гнучкість налаштування прав доступу. Водночас у запиті застосовується параметр auth_type, який визначає спосіб автентифікації користувача в межах інтегрованої системи **ID.GOV.UA**.

Наступним етапом після отримання авторизаційного коду є його обмін на **токен доступу**. Згідно зі специфікацією OAuth 2.0 (RFC 6749) [3], цей запит має здійснюватися методом POST із передачею

Таблиця 1

Етап	Протокол	Приклад запиту (curl/http)	Коментар
Авторизаційний запит	OAuth 2.0	curl -G «https://authorization-server.com/authorize» \ --data-urlencode «response_type=code» --data-urlencode «client_id=client_id» --data-urlencode «redirect_uri=https://client.example.com/cb» --data-urlencode «scope=read write» --data-urlencode «state=xyz»	Відповідає RFC 6749 [3]
	Дія.OAuth	curl -G «https://id.gov.ua/» \ --data-urlencode «response_type=code» --data-urlencode «client_id=client_id» --data-urlencode «auth_type=diia_oauth» --data-urlencode «state=state» --data-urlencode «redirect_uri=https://url/redirect»	Відсутній параметр scope, є власний auth_type
Обмін коду на токен	OAuth 2.0	curl -X POST «https://authorization-server.com/token» \ -H «Content-Type: application/x-www-form-urlencoded» \ -d «grant_type=authorization_code» -d «code=AUTH_CODE» -d «redirect_uri=https://client.example.com/cb» -d «client_id=client_id» -d «client_secret=client_secret»	Надсилається як POST, безпечніше, відповідає RFC 6749 [3]
	Дія.OAuth	curl -G «https://id.gov.ua/get-access-token» \ --data-urlencode «grant_type=authorization_code» --data-urlencode «code=code» --data-urlencode «client_id=client_id» --data-urlencode «client_secret=client_secret» curl -X POST «https://id.gov.ua/get-access-token» \ -H «Content-Type: application/x-www-form-urlencoded» \ -d «grant_type=authorization_code» -d «code=code» -d «client_id=client_id» -d «client_secret=client_secret»	Підтримуються обидва методи (GET і POST); відхід від рекомендацій RFC щодо обов'язкового використання POST Згідно пункту 8.1 [6] відправку сервером прикладної системи запита серверу ідентифікації на отримання маркера доступу за кодом завершення ідентифікації (code) методом GET чи POST протоколу HTTPS виду

параметрів у тілі запиту. Такий підхід уважається більш безпечним, оскільки чутливі дані (зокрема, client_secret) не потрапляють до адресного рядка браузера чи журналів проксі-серверів.

Водночас у реалізації **Дія.OAuth** передбачено можливість здійснення запиту на отримання токена не лише методом POST, а й за допомогою GET-запиту до ендпоінту/get-access-token із передачею всіх параметрів у вигляді URL-параметрів. Попри те що обидва варіанти технічно працюють, використання GET у цьому контексті є **відхиленням від стандарту** та потенційно знижує рівень безпеки через підвищену вразливість до логування, кешування та можливого витоку конфіденційної інформації.

Висновки. Розгляд технічних особливостей реалізації механізму Дія.OAuth у контексті міжнародного стандарту OAuth 2.0 дає змогу зробити низку важливих висновків. З одного боку,

інтегрована система електронної ідентифікації ID.GOV.UA використовує знайомі інженерним спільнотам підходи до цифрової ідентифікації, а також протоколи автентифікації та авторизації, зокрема сценарій *authorization code grant*, що забезпечує достатній рівень безпеки та зручності для кінцевого користувача. З іншого боку, реалізація Дія.OAuth має концептуальні та практичні відмінності від класичної специфікації, як у структурі запитів, так і в способах взаємодії клієнта із сервером авторизації.

Серед ключових відмінностей – використання параметра auth_type для вибору способу автентифікації (замість неявного визначення цього процесу через архітектуру взаємодії), а також можливість здійснення запиту на обмін коду на токен за допомогою методу GET, що суперечить рекомендаціям RFC 6749. Окрім того, реалізація Дія.OAuth не передбачає використання параметра scope, який у класичному OAuth 2.0 відповідає за визначення обсягу прав доступу клієнта до ресурсів користувача. Відсутність цього параметра ускладнює деталізацію доступу та може обмежувати контроль над делегованими повноваженнями.

Важливо також зазначити, що Дія.OAuth функціонує у межах законодавчо визначеної системи рівнів довіри до засобів електронної ідентифікації. Така багаторівнева модель дає змогу не лише підвищити юридичну надійність цифрових транзакцій, а й ефективно розмежовувати технічну автентифікацію та правову ідентифікацію особи, що є критично важливим у сфері державних послуг.

Таким чином, Дія.OAuth можна розглядати як приклад локальної адаптації міжнародного стандарту до умов національної цифрової інфраструктури, що водночас відкриває нові перспективи для розбудови безпечного, зручного та нормативно інтегрованого середовища електронної ідентифікації в Україні, а також така адаптація є необхідною передумовою для реалізації концепції **«Government as a Platform»** [5]. Ба більше, упровадження надійних механізмів електронної автентифікації є основою для розвитку таких складних і чутливих компонентів цифрової демократії, як електронне голосування, участь у референдумах чи онлайн-консультаціях із владою. Саме зв'язок між захищеною цифровою ідентичністю та політичною участю громадян становитиме один із головних векторів подальшої трансформації е-урядування в Україні.

Література:

1. Chae C.-J., Kim K.-B., Cho H.-J. A study on secure user authentication and authorization in OAuth protocol. *Cluster Computing*. 2017. DOI: 10.1007/s10586-017-1119-6.

2. Hammer-Lahav E. The OAuth 1.0 Protocol. IETF RFC 5849. 2010. URL: https://datatracker.ietf.org/doc/html/rfc5849

3. Hardt D. The OAuth 2.0 Authorization Framework. IETF RFC 6749. 2012. URL: https://datatracker.ietf.org/doc/html/rfc6749

4. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII від 05.10.2017. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

5. O'Райлі T. Government as a Platform. *Open Government: Collaboration, Transparency, and Participation in Practice* / за ред. D. Lathrop, L. Ruma. O'Reilly Media, 2011. С. 11–40.

6. Технічна документація. Інтегрована система електронної ідентифікації ID.GOV.UA: Обробка інформації про електронну ідентифікацію користувачів. 2023. URL: https://id.gov.ua/downloads/IDInfoProcessingD.pdf

References:

1. Chae, C.-J., Kim, K.-B., & Cho, H.-J. (2017). A study on secure user authentication and authorization in OAuth protocol. Cluster Computing. https://doi.org/10.1007/s10586-017-1119-6

2. Hammer-Lahav, E. (2010). The OAuth 1.0 Protocol (RFC 5849). Internet Engineering Task Force (IETF). Retrieved from: https://datatracker.ietf.org/doc/html/rfc5849

3. Hardt, D. (2012). The OAuth 2.0 Authorization Framework (RFC 6749). Internet Engineering Task Force (IETF). Retrieved from: https://datatracker.ietf.org/doc/html/rfc6749

4. O'Reilly, T. (2011). Government as a platform. In D. Lathrop & L. Ruma (Eds.), Open government: Collaboration, transparency, and participation in practice (pp. 11–40). O'Reilly Media.

5. Technical Documentation. (2023). Integrated electronic identification system ID.GOV.UA: User identification data processing. https://id.gov.ua/downloads/IDInfoProcessingD.pdf

6. Verkhovna Rada of Ukraine. (2017). Law of Ukraine "On Electronic Identification and Electronic Trust Services" No. 2155-VIII. Retrieved from: https://zakon.rada.gov.ua/laws/show/2155-19#Text

Taras Kurus. Global Authorization Standard and Ukrainian State Infrastructure: Review, Challenges, and Opportunities

The article explores the Diia OAuth component of Ukraine's Integrated Electronic Identification System (ID.GOV.UA) as one of the key elements necessary for the practical implementation of the «Government as a Platform» concept (Tim O'Reilly) [5]. This concept envisions the state focusing on the creation of core digital infrastructure – open registries, standardized APIs, and electronic identification services – while an ecosystem of private and civic developers builds end-user applications for citizens. Special attention is given to Diia OAuth, which functions as a state API gateway for secure user authentication and authorization, enabling developers to integrate verified identification data into their own digital services.

The findings confirm that Diia OAuth, while maintaining compatibility with the core logic of the OAuth 2.0 authorization code flow, also reflects local legal and architectural requirements. At the same time, the absence of the scope parameter in the national implementation raises concerns, as this parameter is essential for flexible permission granularity and gives the authorization process depth beyond simple authentication.

The use of international standards fosters an open environment where the private sector can develop innovative digital services that enhance the effectiveness of public services and contribute to technological progress, particularly in areas such as electronic voting.

The practical value of the study lies in formulating recommendations for further standardization of government APIs and for supporting the developer ecosystem. Particular attention is paid to the three-level trust model, which combines the technical robustness of the protocol with the legal significance of identification data.

Key words: *e-government, legal and regulatory framework, information and communication technologies (ICT), transparency, open data, open data publishers (data controllers), data types, standardization, API interfaces (APIs).*

Відомості про автора:
Курус Тарас – аспірант кафедри політології,
Карпатський національний університет імені Василя Стефаника.

Надійшла 11.08.2025
Прийнята 13.08.2025
Опублікована 30.10.2025