DOI: https://doi.org/10.36910/6775-2524-0560-2026-64-11
УДК 004.056:004.738.5:004.77
Григор'єв Костянтин Сергійович, аспірант
https://orcid.org/0009-0003-1316-4354
Павленко Володимир Іванович, к.ф.-м.н., доцент
https://orcid.org/0000-0002-3958-0415
Відкритий міжнародний університет розвитку людини «Україна», м. Київ, Україна

МЕХАНІЗМ МИТТЄВОГО ВІДКЛИКАННЯ ПРАВ ДОСТУПУ В ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ НА ОСНОВІ СТАТУСНИХ ЗМІН У СМАРТ-КОНТРАКТІ

Григор'єв К. С., Павленко В. І. Механізм миттєвого відкликання прав доступу в децентралізованих системах на основі статусних змін у смарт-контракті. У статті розглянуто проблему оперативного відкликання прав доступу в децентралізованих інформаційних системах, зокрема тих, що функціонують на основі блокчейн-технологій та смарт-контрактів. Актуальність дослідження зумовлена зростанням кількості розподілених сервісів, у яких критично важливо забезпечити своєчасне обмеження доступу при зміні стану суб'єкта або виникненні загроз безпеці. Показано, що традиційні підходи до управління доступом, включаючи рольові моделі, списки контролю доступу та токен-орієнтовані механізми, не забезпечують необхідного рівня швидкодії у випадках динамічної зміни стану суб'єкта, що створює ризики несанкціонованого доступу, затримок у реагуванні системи та потенційного порушення цілісності даних. Запропоновано механізм миттєвого відкликання прав доступу, який базується на використанні моделі станів, інтегрованої безпосередньо у смарт-контракт. У межах підходу право доступу визначається динамічно під час кожного запиту на основі поточного стану суб'єкта, що дозволяє уникнути додаткових процедур анулювання дозволів, скоротити кількість транзакцій та знизити навантаження на систему. Розроблено концептуальну модель, архітектуру смарт-контракту та алгоритм функціонування механізму, який забезпечує негайну реакцію системи на зміну стану суб'єкта без необхідності синхронізації або затримок. Проведено аналіз обчислювальної ефективності, який підтверджує зниження витрат ресурсів за рахунок мінімізації кількості транзакцій і спрощення логіки відкликання доступу. Окрему увагу приділено можливості інтеграції механізму в середовища Internet of Things (IoT), кіберфізичні системи та edge-архітектури, де обмежені обчислювальні ресурси та енергоспоживання вимагають оптимізованих і полегшених рішень. Отримані результати демонструють підвищення швидкодії, гнучкості, масштабованості та рівня безпеки у порівнянні з існуючими підходами, що підтверджує доцільність використання запропонованого механізму в сучасних децентралізованих системах різного призначення та рівня критичності.
Ключові слова: децентралізовані системи, смарт-контракт, управління доступом, відкликання прав доступу, модель станів, блокчейн.

Hryhoriev K., Pavlenko V. Mechanism for instant revocation of access rights in decentralized systems based on status changes in a smart contract. The article addresses the problem of immediate access rights revocation in decentralized information systems, particularly those based on blockchain technology and smart contracts. The relevance of this study is driven by the rapid growth of distributed digital infrastructures, where ensuring timely restriction of access in response to state changes or security incidents is critically important. It is shown that traditional access control approaches, including role-based models, access control lists, and token-based mechanisms, do not provide the required responsiveness in scenarios involving dynamic changes in subject states. This limitation leads to increased risks of unauthorized access, delayed system reactions, and potential violations of data integrity and confidentiality. A mechanism for instant access revocation is proposed, based on a state-driven model integrated directly into the smart contract logic. Within this approach, access rights are not statically assigned but dynamically evaluated during each access request according to the current status of the subject. This eliminates the need for additional revocation procedures, synchronization mechanisms, or token invalidation processes, while also reducing the number of transactions and overall system overhead. The paper presents a conceptual model, a smart contract architecture, and an operational algorithm that ensures immediate and consistent system response to any status changes without introducing additional latency. An analysis of computational efficiency demonstrates reduced resource consumption due to the elimination of redundant operations and the simplification of access control logic. Special attention is given to the applicability of the proposed mechanism in Internet of Things (IoT) environments, cyber-physical systems, and edge computing architectures, where limited computational power, memory, and energy resources require lightweight and efficient solutions. The obtained results confirm improved performance, adaptability, scalability, and security compared to existing approaches, highlighting the practical value, robustness, and feasibility of implementing the proposed mechanism in modern decentralized environments across a wide range of application domains.
Key words: decentralized systems, smart contract, access control, access revocation, state model, blockchain.

Постановка проблеми та її зв'язок із важливими науковими чи практичними завданнями. Стрімкий розвиток децентралізованих інформаційних систем, зокрема на базі технологій блокчейн, зумовлює необхідність переосмислення підходів до управління правами доступу в умовах відсутності централізованого контролю [1]. У таких середовищах механізми автентифікації та авторизації реалізуються переважно через смарт-контракти, що забезпечують прозорість, незмінність і верифікованість правил доступу [2]. Водночас традиційні підходи до

відкликання прав доступу, які ефективно функціонують у централізованих системах, виявляються малопридатними для децентралізованих архітектур через їхню інерційність, залежність від зовнішніх сервісів або необхідність повторного розгортання контрактів.

Актуальність задачі миттєвого відкликання прав доступу зростає у сценаріях, де обробляються чутливі дані або виконуються критичні операції, зокрема в децентралізованих фінансових сервісах, системах електронного голосування, кіберфізичних системах та мережах IoT [3]. У таких умовах навіть незначна затримка між моментом компрометації облікових даних або зміни статусу суб'єкта та фактичним обмеженням доступу може призвести до суттєвих порушень цілісності, конфіденційності або доступності інформації [4].

Існуючі підходи до управління доступом у децентралізованих системах, включаючи рольові моделі та списки контролю доступу, зазвичай не враховують динамічний характер змін стану суб'єктів або об'єктів системи. Більшість реалізацій передбачає або періодичну перевірку умов доступу, або оновлення даних у смарт-контракті через транзакції, що створює часові затримки та додаткові обчислювальні витрати [5]. Крім того, незмінність коду смарт-контрактів ускладнює оперативне реагування на інциденти без попереднього закладення відповідних механізмів у логіку контракту.

Особливої складності набуває задача узгодження між станом суб'єкта доступу та логікою авторизації в умовах розподіленого середовища, де зміни статусу можуть ініціюватися різними учасниками системи або зовнішніми подіями. Це потребує розроблення механізмів, здатних забезпечити негайну реакцію системи на зміну статусу без необхідності повного перегляду політик доступу або втручання централізованих компонентів.

У цьому контексті виникає науково-практична задача розроблення ефективного механізму миттєвого відкликання прав доступу, який би інтегрувався у смарт-контрактну логіку, враховував статусні зміни суб'єктів та забезпечував мінімальні затримки при прийнятті рішень щодо авторизації. Такий підхід має відповідати вимогам ресурсної ефективності, масштабованості та сумісності з обмеженими обчислювальними можливостями вузлів децентралізованих мереж.

Метою дослідження є розробка механізму миттєвого відкликання прав доступу в децентралізованих системах на основі статусних змін у смарт-контракті, який забезпечує оперативне блокування доступу суб'єктів при зміні їхнього стану з урахуванням обмежень обчислювальних ресурсів та вимог до безпеки розподілених середовищ.

Аналіз останніх досліджень та публікацій. Дослідження механізмів управління доступом у децентралізованих системах активно розвиваються у контексті поширення блокчейн-технологій та смарт-контрактів [6]. Значна частина наукових праць присвячена адаптації класичних моделей контролю доступу, зокрема рольової моделі (RBAC) [7] та атрибутивної моделі (ABAC) [8], до умов розподілених середовищ. У таких підходах смарт-контракти виконують функцію децентралізованого посередника, який зберігає політики доступу та забезпечує їх виконання без участі довіреного центру. Водночас більшість реалізацій орієнтована на статичні або квазідинамічні політики, що не враховують необхідність оперативного реагування на зміну стану суб'єктів [9].

Окремий напрям досліджень зосереджений на використанні списків контролю доступу (ACL) [10], які реалізуються у вигляді структур даних у смарт-контрактах. Такі підходи забезпечують прозорість та контрольованість доступу, проте характеризуються обмеженою гнучкістю та значними витратами на оновлення стану через необхідність виконання транзакцій. У результаті процес відкликання прав доступу може супроводжуватися затримками, що є критичним для систем із високими вимогами до оперативності.

У сучасних роботах також розглядаються механізми делегування прав доступу, зокрема на основі криптографічних примітивів та токенів доступу [11]. Такі підходи дозволяють передавати права між суб'єктами без централізованого контролю, однак проблема відкликання делегованих прав залишається недостатньо вирішеною. У більшості випадків відкликання потребує або завершення строку дії токена, або виконання додаткових транзакцій, що не гарантує миттєвої реакції системи.

Останні дослідження приділяють увагу подієво-орієнтованим механізмам управління доступом, де рішення про авторизацію приймається з урахуванням поточного стану системи або зовнішніх подій [12]. Зокрема, пропонуються підходи, у яких смарт-контракти взаємодіють з оракулами для отримання актуальної інформації про статус суб'єктів або середовища [13]. Проте залежність від зовнішніх джерел даних створює додаткові ризики, пов'язані з довірою, затримками

передачі інформації та потенційними атаками на канали взаємодії.

У роботах, присвячених безпеці кіберфізичних систем та IoT, акцент робиться на ресурсній ефективності механізмів контролю доступу [14]. Пропонуються полегшені криптографічні схеми та оптимізовані протоколи взаємодії, які дозволяють зменшити енергоспоживання та обчислювальне навантаження. Водночас питання інтеграції таких рішень із децентралізованими механізмами управління доступом, зокрема у контексті миттєвого відкликання прав, залишається недостатньо дослідженим.

Аналіз існуючих підходів свідчить про відсутність універсального механізму, який би поєднував децентралізованість, миттєвість відкликання прав доступу та адаптивність до змін статусу суб'єктів. Більшість рішень або орієнтована на статичні політики, або потребує додаткових транзакцій для оновлення стану, що знижує оперативність системи. Це зумовлює необхідність розроблення нових підходів, у яких логіка авторизації безпосередньо враховує статусні зміни у смарт-контракті та забезпечує негайну реакцію на них.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Концептуальна модель механізму миттєвого відкликання прав доступу ґрунтується на інтеграції логіки авторизації безпосередньо у смарт-контракт із урахуванням поточного статусу суб'єкта. У межах моделі визначаються основні сутності: суб'єкт доступу, який ініціює запит; об'єкт доступу, до якого здійснюється звернення; статус суб'єкта як динамічна характеристика його стану; політика доступу, що визначає умови взаємодії між суб'єктом і об'єктом. На відміну від традиційних підходів, де права доступу задаються статично або змінюються через окремі транзакції, запропонований механізм передбачає безпосередню залежність дозволу на доступ від актуального статусу, який зберігається у смарт-контракті.

Логіка прийняття рішень реалізується у вигляді функції перевірки доступу, що виконується під час кожного звернення суб'єкта до об'єкта. Така функція враховує поточний статус та політику доступу, що дозволяє миттєво обмежити доступ у разі зміни стану суб'єкта без необхідності додаткових операцій відкликання. У цьому випадку відкликання прав доступу не є окремою процедурою, а виступає наслідком зміни статусу, яка автоматично впливає на результат авторизації.

На рис. 1 наведено загальну схему взаємодії між суб'єктом, смарт-контрактом та статусною моделлю.

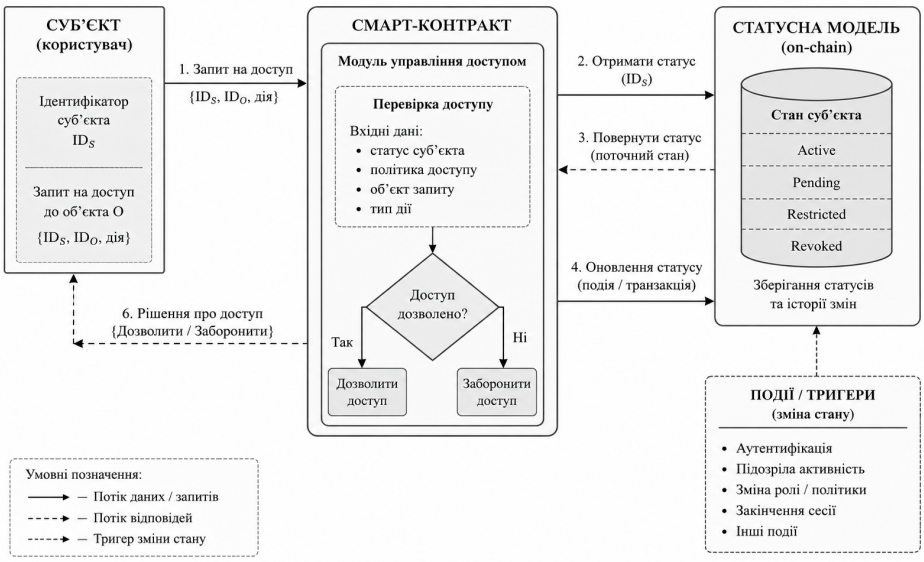

Рис. 1. Загальна схема механізму взаємодії суб'єкта, смарт-контракту та статусної моделі

На схемі відображено, що кожен запит на доступ проходить через смарт-контракт, який здійснює перевірку відповідності поточного статусу суб'єкта встановленим умовам. Зміна статусу ініціюється окремими подіями або транзакціями та негайно впливає на результат перевірки доступу, що забезпечує миттєву реакцію системи.

Для опису статусних змін вводиться множина можливих станів суб'єкта $S = \{s_1, s_2, \dots, s_n\}$, де кожен стан відповідає певному рівню довіри або прав доступу. Переходи між станами визначаються функцією переходів $T: S \times E \to S$, де E – множина подій, що впливають на зміну

статусу. Доступ до об'єкта визначається функцією $A: S \times O \rightarrow \{0,1\}$, де O – множина об'єктів, а значення 1 або 0 відповідає дозволу або забороні доступу.

Миттєве відкликання прав доступу реалізується через зміну значення функції А при переході суб'єкта до іншого стану. У цьому випадку відсутня необхідність у додаткових механізмах відкликання, оскільки доступ автоматично обмежується при невідповідності нового статусу встановленим умовам. Такий підхід забезпечує постійну актуальність рішень авторизації та мінімізує часові затримки.

У таблиці 1 відображено залежність між поточним статусом суб'єкта та набором дозволених операцій. Статус Active відповідає повному доступу до ресурсів системи, включаючи адміністративні дії та роботу з чутливими даними. Статус Pending передбачає обмежений рівень взаємодії, що використовується на етапах перевірки або первинної автентифікації. Статус Restricted означає суттєве обмеження доступу, а статус Revoked забезпечує повне блокування будь-яких дій у системі, що реалізує миттєве відкликання прав доступу.

Таблиця 1 – Відповідність статусів суб'єкта та дозволених операцій доступу

Статус суб'єкта	**Доступ на читання**	**Доступ на запис**	**Виконання операцій**	**Адміністративні дії**	**Доступ до чутливих даних**	**Статус суб'єкта**
Active	Дозволено	Дозволено	Дозволено	Дозволено	Дозволено	Active
Pending	Дозволено	Обмежено	Обмежено	Заборонено	Заборонено	Pending
Restricted	Обмежено	Заборонено	Заборонено	Заборонено	Заборонено	Restricted
Revoked	Заборонено	Заборонено	Заборонено	Заборонено	Заборонено	Revoked

На рис. 2 представлено діаграму переходів статусів суб'єкта.

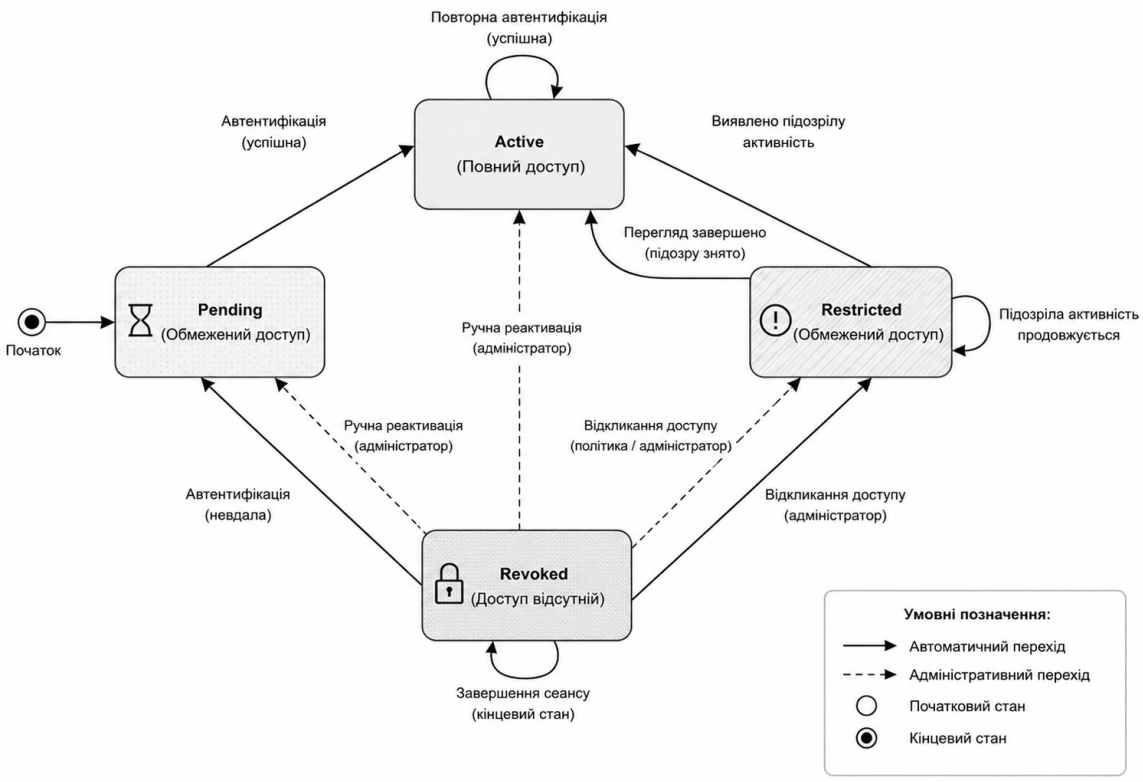

Рис. 2. Діаграма переходів статусів

Діаграма ілюструє можливі переходи між станами під впливом подій, таких як автентифікація, виявлення підозрілої активності або завершення сеансу. Кожен перехід супроводжується зміною умов доступу, що дозволяє реалізувати механізм миттєвого відкликання прав без додаткових процедур або затримок.

Архітектура смарт-контракту для реалізації запропонованого механізму передбачає розподіл логіки на кілька функціональних компонентів: модуль зберігання статусів, модуль перевірки доступу, модуль обробки змін стану та модуль журналювання подій. Такий поділ дозволяє

відокремити дані про поточний стан суб'єктів від логіки прийняття рішень, що підвищує прозорість роботи контракту та спрощує його подальшу перевірку.

Модуль зберігання статусів відповідає за фіксацію поточного стану кожного суб'єкта у вигляді запису в структурі даних смарт-контракту. Для кожного суб'єкта зберігається ідентифікатор, поточний статус, час останньої зміни та, за потреби, ознака причини зміни стану. Такий підхід дозволяє не лише перевіряти актуальність прав доступу, а й відстежувати історію критичних змін.

Модуль перевірки доступу виконує ключову роль у механізмі миттєвого відкликання прав. Під час кожного запиту до ресурсу смарт-контракт перевіряє поточний статус суб'єкта та зіставляє його з політикою доступу. Якщо статус відповідає дозволеним умовам, запит виконується. Якщо статус змінено на Restricted або Revoked, доступ блокується без додаткової процедури відкликання.

Модуль обробки змін стану забезпечує оновлення статусу суб'єкта на основі події, адміністративної дії або результату перевірки. Саме цей модуль є точкою запуску механізму відкликання: після зміни статусу всі наступні звернення суб'єкта автоматично обробляються з урахуванням нового стану. Модуль журналювання подій фіксує зміну статусу, спроби доступу та рішення щодо авторизації, що має практичне значення для аудиту й аналізу інцидентів.

На рис. 3 наведено структурну схему смарт-контракту для реалізації механізму миттєвого відкликання прав доступу.

Алгоритм миттєвого відкликання прав доступу базується на принципі, за яким право доступу не зберігається як незмінний дозвіл, а щоразу обчислюється на основі поточного статусу суб'єкта. У момент зміни статусу не потрібно виконувати окрему операцію видалення прав або оновлення списків доступу. Достатньо змінити статус суб'єкта у смарт-контракті, після чого всі наступні запити автоматично отримують новий результат перевірки.

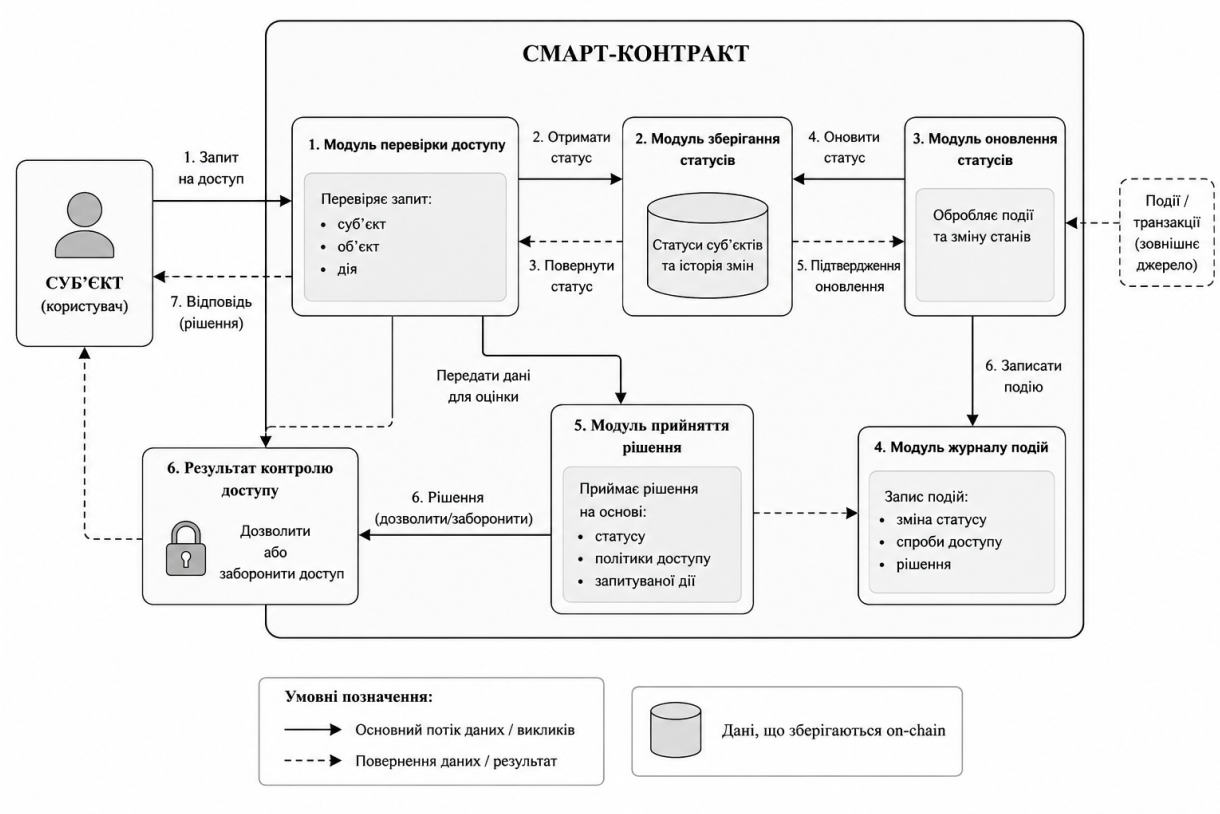

Рис. 3. Структурна схема смарт-контракту

Послідовність роботи механізму визначається таким чином:

1. Суб'єкт надсилає запит на виконання операції з певним об'єктом.
2. Смарт-контракт отримує ідентифікатор суб'єкта, об'єкта та тип запитуваної дії.
3. Модуль перевірки доступу звертається до сховища статусів.
4. Поточний статус суб'єкта зіставляється з політикою доступу.

5. Якщо статус дозволяє виконання операції, смарт-контракт надає доступ.
6. Якщо в системі виникає подія, що потребує обмеження прав, модуль обробки змін стану змінює статус суб'єкта.
7. Після зміни статусу всі наступні запити перевіряються вже за новими умовами.
8. У разі статусу Revoked доступ блокується для всіх операцій без додаткової процедури відкликання.

Моментом відкликання доступу в запропонованому механізмі є не завершення окремого процесу видалення прав, а фіксація нового статусу суб'єкта у смарт-контракті. Це дозволяє зменшити часовий проміжок між виявленням події та фактичним блокуванням доступу. Практична перевага такого підходу полягає в тому, що система не очікує завершення строку дії токена, синхронізації зовнішніх списків або ручного оновлення політик.

У табл. 2 наведено порівняння сценаріїв доступу до та після зміни статусу суб'єкта.

Таблиця 2 – Порівняння сценаріїв доступу до та після зміни статусу

Сценарій	**Статус до зміни**	**Дозволені дії до зміни**	**Подія зміни статусу**	**Статус після зміни**	**Результат після зміни**
Успішна автентифікація	Pending	Читання з обмеженнями	Підтвердження автентичності	Active	Повний доступ відповідно до політики
Виявлення підозрілої активності	Active	Читання, запис, виконання операцій	Фіксація аномальної поведінки	Restricted	Блокування критичних операцій
Адміністративне відкликання	Active	Повний доступ	Рішення адміністратора або політики	Revoked	Повне блокування доступу
Завершення сеансу	Active	Доступ у межах активної сесії	Закінчення часу дії сесії	Pending	Перехід до обмеженого доступу

З таблиці 2 видно, що зміна статусу безпосередньо впливає на результат авторизації. Найбільш критичним є перехід до статусу Revoked, оскільки він одразу припиняє можливість виконання будь-яких операцій. Перехід до Restricted не завжди означає повне блокування, але обмежує доступ до критичних функцій, що дозволяє зберегти контрольовану взаємодію із системою.

На рис. 4 представлено часовий граф процесу відкликання доступу.

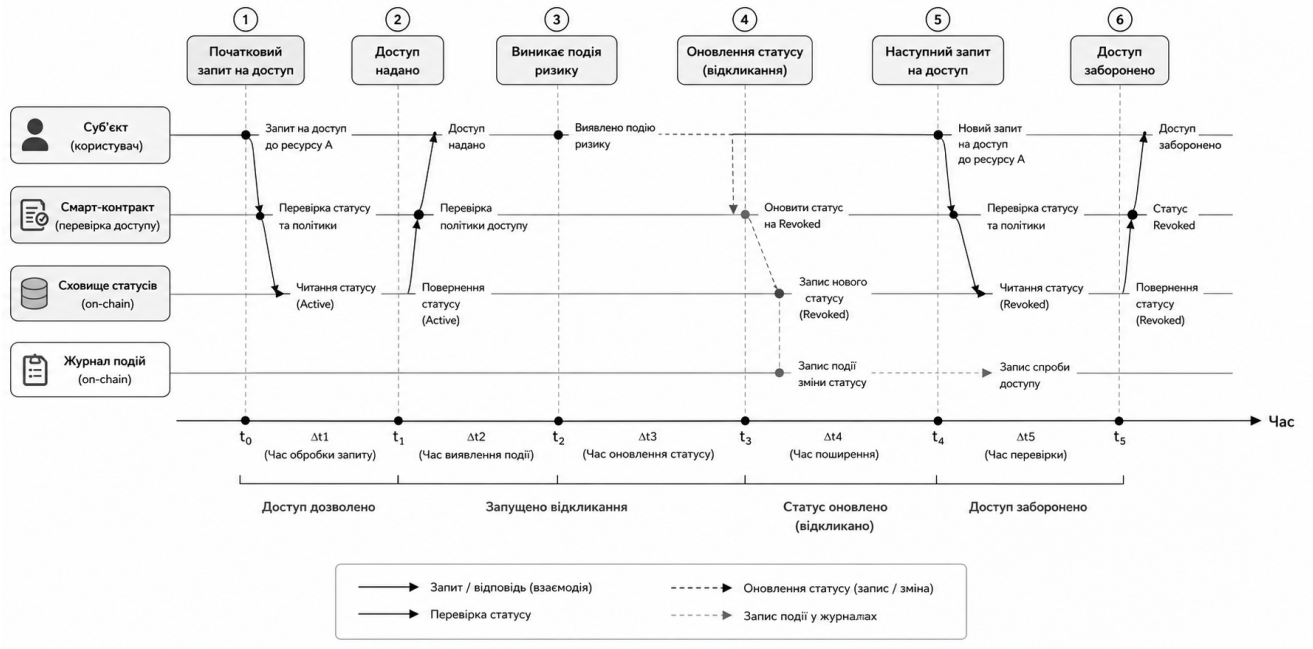

Рис. 4. Часовий граф процесу відкликання доступу

На графі відображено послідовність подій у часовому вимірі, що характеризують процес відкликання доступу від моменту ініціалізації запиту до його повного блокування після зміни стану суб'єкта. Показано, що після виникнення події ризику та оновлення статусу у смарт-контракті всі

наступні запити автоматично обробляються з урахуванням нового стану без необхідності виконання додаткових операцій. Часова діаграма демонструє відсутність окремого етапу відкликання прав доступу як самостійної процедури, оскільки обмеження доступу відбувається безпосередньо під час перевірки авторизації. Це підтверджує, що затримка між виявленням загрози та фактичним блокуванням доступу мінімізується і визначається лише швидкістю фіксації нового стану в системі, що є ключовою перевагою запропонованого механізму.

Оцінка обчислювальної ефективності та затримок у запропонованому механізмі базується на аналізі витрат виконання основних операцій смарт-контракту, зокрема перевірки доступу, зміни статусу та обробки запитів суб'єктів. На відміну від традиційних підходів, де відкликання прав доступу реалізується як окрема транзакція або набір операцій, у запропонованому рішенні відсутня необхідність виконання додаткових процедур, що безпосередньо впливає на зменшення обчислювального навантаження.

Перевірка доступу виконується як виклик функції смарт-контракту, що включає отримання статусу суб'єкта та його зіставлення з політикою доступу. Така операція має сталу складність і не залежить від кількості попередніх змін стану. Зміна статусу реалізується як одноразове оновлення запису у сховищі, що потребує мінімальних витрат ресурсів. У результаті механізм забезпечує ефективну обробку великої кількості запитів без суттєвого збільшення вартості виконання.

Затримка відкликання доступу визначається інтервалом між моментом фіксації нового статусу та наступною спробою доступу. Оскільки рішення про авторизацію приймається динамічно, система не потребує часу на синхронізацію або оновлення зовнішніх структур даних. Це дозволяє досягти практично миттєвого відкликання прав доступу у межах одного виклику функції смарт-контракту.

У табл. 3 наведено порівняння витрат на виконання операцій для запропонованого механізму та існуючих підходів.

Таблиця 3 – Порівняння витрат (gas/час виконання) для різних підходів

Підхід	**Перевірка доступу (gas/час)**	**Відкликання доступу (gas/час)**	**Додаткові операції**	**Загальна затримка**
Запропонований механізм	Низькі	Низькі (оновлення статусу)	Відсутні	Мінімальна
ACL на блокчейні	Середні	Високі (оновлення списків)	Потрібні	Середня
RBAC у смарт-контракті	Середні	Середні	Часткові	Середня
Токен-орієнтований доступ	Низькі	Високі (анулювання/очікування)	Потрібні	Висока

У таблиці показано, що запропонований механізм забезпечує найменші витрати на відкликання доступу за рахунок відсутності окремих процедур анулювання прав. Основна перевага полягає у зменшенні кількості транзакцій, що є критичним для систем із обмеженими ресурсами або високим навантаженням.

Інтеграція механізму у децентралізовані та ресурсно-обмежені системи передбачає його адаптацію до умов обмеженої обчислювальної потужності, пам'яті та енергоспоживання. У середовищах IoT та кіберфізичних системах вузли часто виконують лише базові операції та не можуть підтримувати складні протоколи управління доступом. У цьому контексті запропонований механізм є ефективним, оскільки основна логіка обробки доступу переноситься на рівень смарт-контракту, а пристрої виконують лише мінімальні запити.

В edge-середовищах механізм може бути інтегрований як частина проміжного шару, що забезпечує перевірку доступу перед передачею даних до хмарних або розподілених сервісів. Це дозволяє зменшити навантаження на центральні вузли та підвищити швидкість реакції системи. Водночас статусна модель може синхронізуватися між різними вузлами через блокчейн, що забезпечує узгодженість даних. На рис. 5 відображено схему інтеграції механізму у IoT/edge-архітектуру.

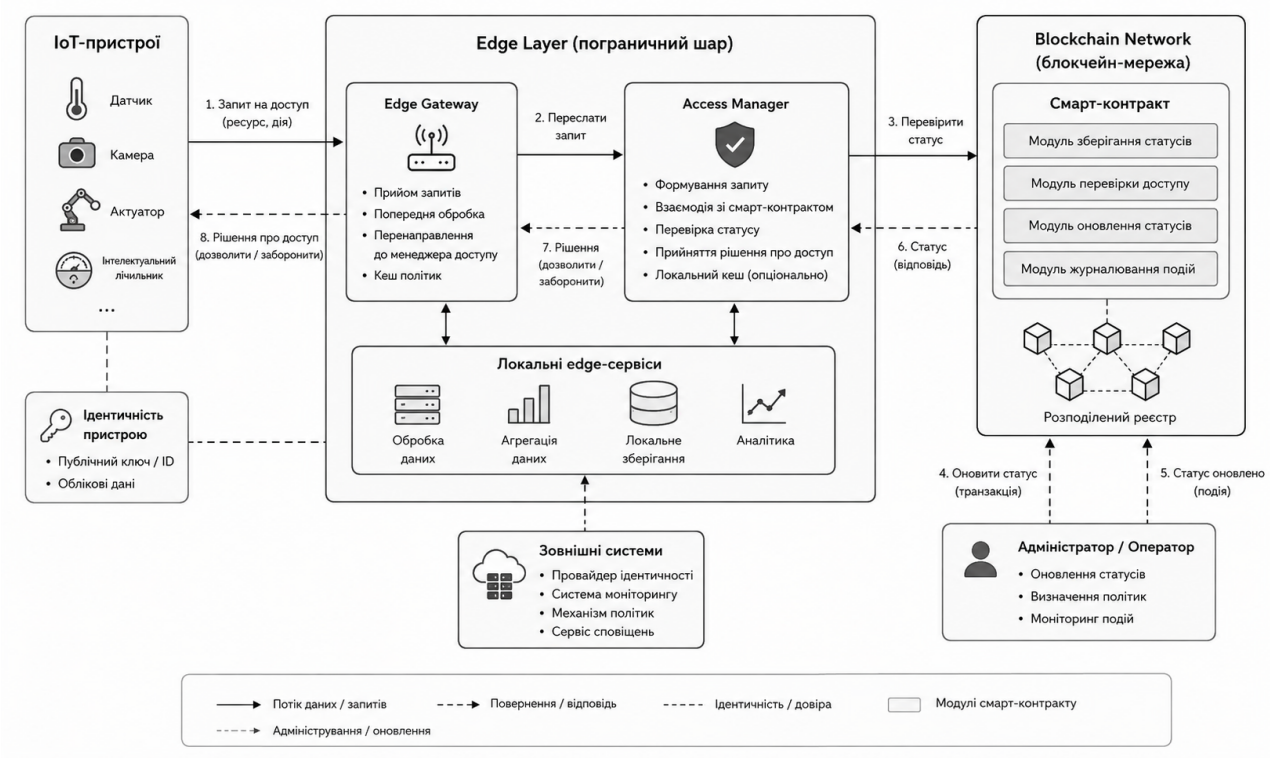

Рис. 5. Схема інтеграції механізму у IoT/edge-архітектуру

Результати дослідження підтверджують, що використання статусно-орієнтованого підходу до управління доступом дозволяє досягти високої швидкодії та адаптивності системи. Запропонований механізм забезпечує миттєве відкликання прав доступу без необхідності виконання додаткових процедур або очікування завершення строку дії дозволів.

Практична цінність механізму полягає у можливості його застосування в системах з підвищеними вимогами до безпеки, де критичною є швидка реакція на зміну стану суб'єкта. Це включає фінансові системи, медичні інформаційні системи, кіберфізичні комплекси та мережі IoT. Запропонований підхід дозволяє мінімізувати ризики несанкціонованого доступу та зменшити навантаження на систему управління доступом.

У табл. 4 наведено порівняльну характеристику запропонованого механізму та існуючих підходів.

Таблиця 4 – Порівняльна характеристика підходів до управління доступом

Критерій	**Запропонований механізм**	**ACL**	**RBAC**	**Токен-орієнтований підхід**
Швидкодія	Висока	Середня	Середня	Низька при відкликанні
Гнучкість	Висока	Низька	Середня	Середня
Витрати ресурсів	Низькі	Середні	Середні	Високі
Миттєве відкликання	Забезпечується	Відсутнє	Часткове	Відсутнє
Стійкість до атак	Висока	Середня	Середня	Залежить від реалізації

Отримані результати демонструють, що запропонований механізм перевершує існуючі підходи за ключовими характеристиками, зокрема за швидкістю реакції на зміну статусу та ефективністю використання ресурсів. Це підтверджує доцільність його використання у сучасних децентралізованих системах з високими вимогами до безпеки та масштабованості.

Висновки та перспективи подальшого дослідження. У результаті проведеного дослідження запропоновано механізм миттєвого відкликання прав доступу в децентралізованих системах, який базується на використанні статусних змін у смарт-контракті як основного критерію прийняття рішень авторизації. На відміну від існуючих підходів, де відкликання реалізується як окрема процедура або залежить від строку дії дозволів, у запропонованому рішенні доступ визначається динамічно під час кожного запиту, що забезпечує негайну реакцію системи на зміну стану суб'єкта.

Розроблена концептуальна модель дозволяє інтегрувати механізм відкликання

безпосередньо у логіку смарт-контракту, що усуває потребу у додаткових транзакціях для анулювання прав доступу. Запропонована архітектура контракту забезпечує розмежування функціональних компонентів, зокрема зберігання статусів, перевірки доступу та обробки змін стану, що підвищує прозорість, масштабованість і керованість системи.

Проведений аналіз обчислювальної ефективності підтверджує зниження витрат ресурсів за рахунок відсутності окремих операцій відкликання та мінімізації кількості транзакцій. Визначено, що затримка відкликання доступу обмежується лише моментом оновлення статусу у смарт-контракті, що дозволяє досягти практично миттєвого блокування доступу без необхідності синхронізації або очікування.

Результати інтеграції механізму у середовища Internet of Things, кіберфізичні системи та edge-архітектури демонструють його придатність до використання в умовах обмежених обчислювальних ресурсів. Перенесення логіки авторизації на рівень смарт-контракту дозволяє зменшити навантаження на периферійні пристрої та забезпечити узгодженість політик доступу у розподіленому середовищі.

Отримані результати підтверджують, що запропонований механізм перевищує існуючі підходи за критеріями швидкодії, гнучкості та ефективності використання ресурсів, а також забезпечує підвищений рівень стійкості до несанкціонованого доступу. Це обґрунтовує доцільність його застосування у децентралізованих інформаційних системах із високими вимогами до оперативності управління доступом та безпеки даних.

Список бібліографічного опису

1. Ibor, A., Edim, E., & Ojugo, A. (2023). Secure health information system with blockchain technology. *Journal of the Nigerian Society of Physical Sciences,* 992–992. https://doi.org/10.46481/jnsps.2023.992
2. Григор'єв, К., & Павленко, В. (2026). Система забезпечення конфіденційності транзакцій з даними з використанням протоколів нульового розголошення. *Measuring and Computing Devices in Technological Processes*, (1), 208–214. https://doi.org/10.31891/2219-9365-2026-85-26
3. Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex & Intelligent Systems,* 8(4), 3559–3591. https://doi.org/10.1007/s40747-022-00667-z
4. Routray, K., Bera, P., & Mishra, S. (2025). Efficient and secure fine-grained authorization for fog-enabled cyber-physical systems: Towards trust and autonomy in digital sovereignty. *Procedia Computer Science*, 254, 240–249. https://doi.org/10.1016/j.procs.2025.02.083
5. Wahab, A., Wang, J., Shojaei, A., & Ma, J. (2023). A model-based smart contracts system via blockchain technology to reduce delays and conflicts in construction management processes. *Engineering, Construction and Architectural Management*, 30(10), 5052–5072. https://doi.org/10.1108/ECAM-03-2022-0271
6. Alam, T. (2023). Blockchain and big data-based access control for communication among IoT devices in smart cities. *Wireless Personal Communications*, 132(1), 433–456. https://doi.org/10.1007/s11277-023-10617-8
7. Al Neyadi, D., Puthal, D., Dutta, J., & Damiani, E. (2023). Role-based access control in private blockchain for IoT integrated smart contract. *In IFIP International Internet of Things Conference* (pp. 227–245). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-45882-8_16
8. Awan, S. M., Azad, M. A., Arshad, J., Waheed, U., & Sharif, T. (2023). A blockchain-inspired attribute-based zero-trust access control model for IoT. *Information,* 14(2), 129. https://doi.org/10.3390/info14020129
9. Pang, T., Suh, H. T., Yang, L., & Tedrake, R. (2023). Global planning for contact-rich manipulation via local smoothing of quasi-dynamic contact models. *IEEE Transactions on Robotics*, 39(6), 4691–4711. https://doi.org/10.1109/TRO.2023.3300230
10. De Oliveira, M. T., Reis, L. H. A., Verginadis, Y., Mattos, D. M. F., & Olabarriaga, S. D. (2022). SmartAccess: Attribute-based access control system for medical records based on smart contracts. *IEEE Access*, 10, 117836–117854. https://doi.org/10.1109/ACCESS.2022.3217201
11. Mukta, R., Pal, S., Chowdhury, K., Hitchens, M., Paik, H. Y., & Kanhere, S. S. (2025). Zero trust driven access control delegation using blockchain. *Blockchain: Research and Applications*, 100319. https://doi.org/10.1016/j.bcra.2025.100319
12. Akhtar, A., Barati, M., Shafiq, B., Rana, O., Afzal, A., Vaidya, J., & Shamail, S. (2024). Blockchain based auditable access control for business processes with event driven policies. *IEEE Transactions on Dependable and Secure Computing*, 21(5), 4699–4716. https://doi.org/10.1109/TDSC.2024.3356811
13. Bian, H., Zhang, W., & Chang, C. K. (2024). Situ-oracle: A learning-based situation analysis framework for blockchain-based IoT systems. *Blockchains*, 2(2), 173–194. https://doi.org/10.3390/blockchains2020009
14. Faure, E., Rozlomii, I., & Naumenko, S. (2025). Cryptographic load sharing method in critical infrastructure sensor networks. *In Proceedings of the Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'25)* (pp. 5–15).

References

1. Iriani, Ibor, A., Edim, E., & Ojugo, A. (2023). Secure health information system with blockchain technology. *Journal of the Nigerian Society of Physical Sciences,* 992–992. https://doi.org/10.46481/jnsps.2023.992
2. Hrigoriev, K., & Pavlenko, V. (2026). A system for ensuring the confidentiality of data transactions using zero-

disclosure protocols. *Measuring and Computing Devices in Technological Processes*, (1), 208–214. https://doi.org/10.31891/2219-9365-2026-85-26
3. Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex & Intelligent Systems,* 8(4), 3559–3591. https://doi.org/10.1007/s40747-022-00667-z
4. Routray, K., Bera, P., & Mishra, S. (2025). Efficient and secure fine-grained authorization for fog-enabled cyber-physical systems: Towards trust and autonomy in digital sovereignty. *Procedia Computer Science*, 254, 240–249. https://doi.org/10.1016/j.procs.2025.02.083
5. Wahab, A., Wang, J., Shojaei, A., & Ma, J. (2023). A model-based smart contracts system via blockchain technology to reduce delays and conflicts in construction management processes. *Engineering, Construction and Architectural Management*, 30(10), 5052–5072. https://doi.org/10.1108/ECAM-03-2022-0271
6. Alam, T. (2023). Blockchain and big data-based access control for communication among IoT devices in smart cities. *Wireless Personal Communications*, 132(1), 433–456. https://doi.org/10.1007/s11277-023-10617-8
7. Al Neyadi, D., Puthal, D., Dutta, J., & Damiani, E. (2023). Role-based access control in private blockchain for IoT integrated smart contract. *In IFIP International Internet of Things Conference* (pp. 227–245). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-45882-8_16
8. Awan, S. M., Azad, M. A., Arshad, J., Waheed, U., & Sharif, T. (2023). A blockchain-inspired attribute-based zero-trust access control model for IoT. *Information,* 14(2), 129. https://doi.org/10.3390/info14020129
9. Pang, T., Suh, H. T., Yang, L., & Tedrake, R. (2023). Global planning for contact-rich manipulation via local smoothing of quasi-dynamic contact models. *IEEE Transactions on Robotics*, 39(6), 4691–4711. https://doi.org/10.1109/TRO.2023.3300230
10. De Oliveira, M. T., Reis, L. H. A., Verginadis, Y., Mattos, D. M. F., & Olabarriaga, S. D. (2022). SmartAccess: Attribute-based access control system for medical records based on smart contracts. *IEEE Access*, 10, 117836–117854. https://doi.org/10.1109/ACCESS.2022.3217201
11. Mukta, R., Pal, S., Chowdhury, K., Hitchens, M., Paik, H. Y., & Kanhere, S. S. (2025). Zero trust driven access control delegation using blockchain. *Blockchain: Research and Applications*, 100319. https://doi.org/10.1016/j.bcra.2025.100319
12. Akhtar, A., Barati, M., Shafiq, B., Rana, O., Afzal, A., Vaidya, J., & Shamail, S. (2024). Blockchain based auditable access control for business processes with event driven policies. *IEEE Transactions on Dependable and Secure Computing*, 21(5), 4699–4716. https://doi.org/10.1109/TDSC.2024.3356811
13. Bian, H., Zhang, W., & Chang, C. K. (2024). Situ-oracle: A learning-based situation analysis framework for blockchain-based IoT systems. *Blockchains*, 2(2), 173–194. https://doi.org/10.3390/blockchains2020009
14. Faure, E., Rozlomii, I., & Naumenko, S. (2025). Cryptographic load sharing method in critical infrastructure sensor networks. *In Proceedings of the Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'25)* (pp. 5–15).

Історія статті:
Отримано: 24.05.2026 Доопрацьовано: 06.08.2026 Прийнято до друку: 23.09.2026 Опубліковано: 29.09.2026