https://orcid.org/0000-0002-7775-6039
https://orcid.org/0000-0001-5423-0985
https://orcid.org/0000-0002-7589-2045

УДК 004.056:004.7

П.М. СКЛАДАННИЙ[*], Ю.В. КОСТЮК[*], С.Л. РЗАЄВА[*]

БЕЗПЕРЕРВНА ОЦІНКА ДОСТУПУ В ZERO TRUST ACCESS MANAGEMENT НА ОСНОВІ ПОДІЄВИХ СИГНАЛІВ БЕЗПЕКИ ТА ДИНАМІЧНОГО КЕРУВАННЯ СЕСІЯМИ

[*] Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

Анотація. *У статті запропоновано підхід до безперервної оцінки доступу в Zero Trust Access Management, що ґрунтується на подієвих сигналах безпеки та динамічному керуванні активними сесіями користувачів. На відміну від традиційних моделей авторизації, які приймають рішення одноразово під час входу, доступ розглядається як процес, що коригується впродовж усього життєвого циклу сесії з урахуванням змін контексту, поведінки та рівня ризику. Запропонована архітектура поєднує механізми оцінки довіри, прийняття рішень і виконання політик доступу з джерелами подієвої телеметрії, зокрема системами SIEM і UEBA, у єдиний керований контур. Ключовою особливістю підходу є подієве керування сесіями, за якого асинхронні події безпеки ініціюють градуйовані реакції системи — збереження доступу, посилення перевірки або блокування — без обов'язкового примусового завершення сесії. Це дозволяє поєднати вимоги безпеки з безперервністю бізнес-процесів. Окрему увагу приділено часовій коректності прийняття рішень, що забезпечує недопущення виконання критичних операцій із надмірними привілеями після виявлення ризикових подій. Для кількісної оцінки ефективності запропонованого контуру введено метрики часу реакції на події безпеки та частки запитів, оброблених із застарілою оцінкою довіри. Експериментальна перевірка проведена в імітаційному корпоративному середовищі з підтримкою багатофакторної автентифікації, подієвого оновлення довіри та централізованого аналізу подій. Отримані результати демонструють суттєве зменшення часу реагування, зниження кількості неузгоджених рішень доступу та підвищення коректності виконання критичних операцій порівняно з базовою моделлю періодичної переоцінки. Це підтверджує практичну придатність безперервної оцінки доступу як інженерного механізму в сучасних Zero Trust-архітектурах.*

Ключові слова: *Zero Trust, access management, безперервна оцінка доступу, динамічна довіра, подієві сигнали, SIEM, UEBA, керування сесіями.*

Abstract. *The article proposes an approach to continuous access evaluation in Zero Trust Access Management based on security event signals and dynamic management of active user sessions. Unlike traditional authorization models, which make decisions once at login, access is treated as a process that is continuously adjusted throughout the session lifecycle, taking into account changes in context, behavior, and risk level. The proposed architecture integrates trust evaluation, decision-making, and access policy enforcement mechanisms with sources of event telemetry — specifically SIEM and UEBA systems — into a unified, controlled loop. A key feature of this approach is event-driven session management, where asynchronous security events trigger graduated system responses — preserving access, enforcing additional verification, or blocking — without necessarily forcing session termination. This enables the alignment of security requirements with the continuity of business processes. Special attention is given to the temporal correctness of decision-making, ensuring that critical operations are not executed with excessive privileges after the detection of risky events. To quantitatively assess the effectiveness of the proposed loop, some metrics have been introduced for response time to security events and the proportion of requests processed based on outdated trust assessments. Experimental evaluation has been conducted in a simulated corporate environment supporting multi-factor authentication, event-driven trust updates, and centralized event analysis. The obtained results demonstrate a significant reduction in response time, a decrease in the number of inconsistent access decisions, and improved correctness in executing critical operations*

ISSN 1028-9763. Математичні машини і системи. 2026. № 1

compared to a baseline model with periodic re-evaluation. This confirms the practical applicability of continuous access evaluation as an engineering mechanism in modern Zero Trust architectures.
Keywords: *Zero Trust, access management, continuous access evaluation, dynamic trust, event signals, SIEM, UEBA, session management.*

DOI: 10.34121/1028-9763-2026-1-29-46

1. Вступ

Сучасні корпоративні інформаційно-комунікаційні системи функціонують в умовах зростаючої динамічності бізнес-процесів, активного використання хмарних сервісів, віддаленого доступу та розподілених цифрових ресурсів [1, 6]. За таких умов традиційні підходи до контролю доступу, що ґрунтуються на одноразовій перевірці користувача під час входу до системи, виявляються недостатніми для забезпечення належного рівня кібербезпеки [3, 4, 7]. Навіть успішна автентифікація та коректно видані токени доступу не гарантують безпечності подальшої взаємодії, оскільки поведінка користувача, стан пристрою та контекст виконання операцій можуть змінюватися протягом активної сесії.

Концепція Zero Trust Access Management передбачає відмову від статичної довіри та орієнтується на постійну перевірку кожного запиту доступу з урахуванням контекстних, поведінкових і ризикових факторів [3, 8]. У межах цього підходу доступ розглядається не як одноразово дозволена дія, а як безперервний процес, що потребує постійної оцінки відповідності поточного стану користувача та середовища встановленим політикам безпеки [5, 9, 10]. Така парадигма зумовлює перехід від моделі «оцінка при вході» до безперервної оцінки доступу (continuous access evaluation), у якій рішення щодо доступу можуть коригуватися в реальному часі.

Попри активний розвиток Zero Trust Access Management, у більшості робіт безперервна оцінка доступу описується концептуально, без формального зв’язку між часовими характеристиками доставки подієвих сигналів і коректністю виконання операцій під час активної сесії [14]. Зокрема, недостатньо розкритими залишаються такі питання: як гарантувати своєчасне «послаблення» доступу після RiskEvent, як кількісно оцінювати застарілість trust-стану в точці застосування політик [2, 6]. Це формує потребу в інженерно керованій моделі continuous access evaluation із вимірюваними метриками якості контуру.

Особливого значення в цьому контексті набуває використання подієвих сигналів безпеки, що надходять із різнорідних джерел корпоративної інфраструктури, зокрема систем управління подіями та інцидентами безпеки (SIEM), засобів поведінкової аналітики (UEBA), провайдерів ідентичності, систем контролю стану пристроїв та зовнішніх джерел розвідки загроз [2, 8, 9]. Такі сигнали відображають зміни у поведінці користувачів, виникнення аномалій, підвищення ризику компрометації облікових даних або порушення політик доступу, що вимагає оперативної реакції з боку системи Access Management.

У відповідь на ці виклики актуальним є формування подієво-орієнтованого контуру керування доступом, у межах якого події безпеки ініціюють динамічне оновлення рішень щодо доступу під час активної сесії [10, 16]. Такий підхід забезпечує адаптивне керування сесіями, що включає підвищення рівня перевірки, обмеження привілеїв або припинення доступу у разі зниження рівня довіри [11]. Водночас ефективність цього контуру безпосередньо залежить від своєчасності доставки сигналів, узгодженості компонентів системи та коректності реалізації механізмів прийняття й застосування рішень.

У статті розглядається підхід до реалізації безперервної оцінки доступу в Zero Trust Access Management на основі подієвих сигналів безпеки та динамічного керування сесіями. Запропоновано архітектурну модель, у якій компоненти оцінки довіри, прийняття рішень і застосування політик інтегруються з подієвими джерелами безпеки в єдиний замкнений ко-

нтур. Особливу увагу приділено формалізації реакцій системи на події безпеки, аналізу часових характеристик доставки сигналів і введенню метрик, що дозволяють оцінювати якість функціонування контуру безперервного контролю доступу.

Метою дослідження є розроблення та обґрунтування підходу до безперервної оцінки доступу в системах Zero Trust Access Management, що базується на використанні подієвих сигналів безпеки та забезпечує динамічне керування сесіями користувачів у процесі їх активної взаємодії з корпоративними ресурсами. Досягнення поставленої мети передбачає формування замкненого контуру контролю доступу, у межах якого рішення про дозвіл, обмеження або припинення доступу коригуються в реальному часі залежно від змін контексту, поведінки та рівня ризику.

Для досягнення поставленої мети в роботі необхідно розв'язати такі основні завдання:

• проаналізувати обмеження традиційних моделей контролю доступу, що ґрунтуються на одноразовій оцінці під час входу, та обґрунтувати доцільність переходу до безперервної оцінки доступу;

• розробити архітектурну модель Zero Trust Access Management із подієво-орієнтованим контуром керування доступом, що інтегрує компоненти Trust Engine, PDP, PEP та джерела подієвих сигналів безпеки;

• формалізувати механізм реакції системи на події безпеки у вигляді динамічного коригування стану доступу під час активної сесії;

• запропонувати метрики оцінки якості функціонування контуру безперервного контролю доступу, що враховують часові характеристики доставки сигналів і актуальність оцінки довіри;

• продемонструвати застосовність запропонованого підходу для підвищення стійкості систем Access Management до сучасних кіберзагроз.

Наукова новизна дослідження полягає в розвитку підходів до Zero Trust Access Management шляхом переходу від статичної одноразової авторизації до формалізованої моделі безперервної оцінки доступу, в якій рішення щодо доступу розглядається як часовозалежна функція подієвих сигналів безпеки та динамічного рівня довіри. У роботі запропоновано подієвий контур керування активними сесіями, що забезпечує адаптивну зміну режимів доступу протягом життєвого циклу сесії без її примусової інвалідизації з урахуванням асинхронних подій безпеки, зафіксованих системами SIEM та UEBA. Сформульовано умову коректності revocation-before-use як інваріант безперервної оцінки доступу, що встановлює формальний зв'язок між часовими характеристиками доставки подієвих сигналів і безпекою виконання операцій. Запропоновано метрики $TTAtten$ та $staleness$ для кількісної оцінки ефективності подієвого керування доступом, які відображають швидкість реакції системи та узгодженість рішень авторизації з актуальним станом довіри. Обґрунтовано архітектурну інтеграцію Trust Engine, PDP, PEP і систем SIEM/UEBA в єдиний керований контур безперервного доступу в Zero Trust-архітектурах.

У системах Zero Trust Access Management доступ до ресурсів розглядається не як одноразово дозволена дія, а як динамічний процес, що триває протягом усієї активної сесії користувача [10, 14, 19]. Під час такої сесії можуть змінюватися умови доступу, поведінкові характеристики користувача, стан пристрою або загальний рівень ризику в інформаційному середовищі. Ці зміни відображаються у вигляді подієвих сигналів безпеки, що надходять із різнорідних джерел корпоративної інфраструктури.

Задача безперервної оцінки доступу полягає у забезпеченні своєчасного та узгодженого коригування рішень щодо доступу під час активної сесії користувача на основі актуальних подієвих сигналів безпеки. На відміну від традиційних моделей, у яких рішення про доступ фіксується на момент автентифікації, запропонований підхід передбачає можливість динамічного керування сесіями з урахуванням змін контексту та рівня довіри.

Ключовим аспектом постановки задачі є врахування часових характеристик доставки та обробки подієвих сигналів. Події безпеки виникають асинхронно та потребують передачі до компонентів системи Access Management, де на їх основі формується оновлене рішення щодо доступу. Затримка між моментом виникнення події та фактичним застосуванням коригувального впливу безпосередньо впливає на ефективність захисту та визначає розмір потенційного вікна атаки.

У цьому контексті вводиться поняття часу до послаблення доступу (Time to Attenuation, TTAtten), який характеризує швидкість реакції системи на події безпеки. Менше значення TTAtten відповідає більш оперативному коригуванню доступу та підвищенню стійкості системи до зловмисних дій під час активних сесій.

Ще одним важливим аспектом є проблема застарілої оцінки довіри, коли рішення щодо доступу приймається на основі інформації, що вже не відповідає поточному ризиковому стану користувача або середовища [6, 14]. Для опису цього ефекту вводиться метрика staleness, яка відображає частку часу або запитів, оброблених із використанням неактуальної інформації про рівень довіри. Зменшення staleness є критично важливим для забезпечення коректності рішень та узгодженості між джерелами подій і механізмами контролю доступу.

Отже, постановка задачі безперервної оцінки доступу полягає у створенні подієво-орієнтованого контуру керування сесіями, який забезпечує мінімізацію часу реакції на події безпеки, зниження впливу застарілої інформації та підтримку актуального рівня контролю доступу протягом усього часу взаємодії користувача з корпоративними ресурсами.

Аналіз літературних джерел і постановка проблеми

У сучасних дослідженнях щодо Zero Trust Access Management простежується чітка еволюція від концептуального декларування принципу «never trust, always verify» до його практичної реалізації у вигляді інтегрованих архітектур керування доступом. Так, Dakić et al. у роботі [1] аналізують впровадження Zero Trust Architecture у середніх організаціях на прикладі Azure-платформи та показують, що ефективність контролю доступу значною мірою залежить не від окремих механізмів автентифікації чи авторизації, а від узгодженості взаємодії між провайдером ідентичності, механізмами політик та системами моніторингу. Автори наголошують на проблемі затримок у реакції політик доступу на зміни контексту, що створює вікна ризику під час активних сесій.

Розвиток цього напряму пов’язаний із використанням SIEM, SOAR та UEBA як джерел подієвих сигналів для Zero Trust-систем. У роботі Hassan et al. [2] запропоновано фреймворк ZenGuard, у якому машинне навчання застосовується для контекстно-орієнтованого виявлення загроз і автоматизованої реакції. Хоча автори демонструють ефективність кореляції подій та зниження кількості інцидентів, питання своєчасності перенесення сигналів ризику в рішення доступу під час сесії залишається недостатньо формалізованим.

Проблеми формалізації контролів Zero Trust розглядаються у працях, присвячених багаторівневим моделям безпеки. Зокрема, Park, Park і Youm [3] пропонують Zero-Trust-орієнтовану multi-level security модель, яка систематизує політики та механізми перевірки доступу. Однак у межах цієї моделі доступ розглядається переважно як результат окремих перевірок, без явного акценту на безперервне оновлення стану доступу протягом сесії.

Суттєвий внесок у розвиток динамічної авторизації зробили дослідження, присвячені атрибутному доступу та оцінці довіри. У роботі Mao et al. [4] запропоновано модель Zero Trust-доступу для хмарних середовищ, яка поєднує ABAC із динамічною оцінкою trust-рівня. Подібний підхід представлено і в дослідженні Wang et al. [5], де автори демонструють, що динамічне коригування доступу на основі довіри зменшує ризик ескалації привілеїв. Водночас у цих роботах рішення про доступ фактично приймається у відповідь на запит, а не як реакція на асинхронні подієві сигнали, що виникають після встановлення сесії.

Організаційний і управлінський вимір Zero Trust висвітлено у праці Pigola et al. [6], де довіра розглядається як багатовимірна характеристика, що поєднує технічні, процесні та людські чинники. Автори підкреслюють, що в реальних корпоративних середовищах trust-оцінка швидко втрачає актуальність без механізмів її постійного оновлення, однак не пропонують формалізованих метрик для оцінювання цієї «застарілості».

Питання Zero Trust IAM у мультихмарних середовищах розглянуто у роботі Sivaraman [7], де акцент зроблено на інтеграції IdP та політик доступу між різними хмарними платформами. Дослідження демонструє складність підтримки єдиного рівня довіри в розподілених середовищах, що додатково актуалізує проблему узгодженості стану доступу між компонентами.

Оглядові дослідження, зокрема робота Azad et al. [8], присвячені Zero Trust у контексті IoT, підтверджують, що у динамічних і високонавантажених середовищах статичні або разові перевірки доступу є недостатніми. Автори підкреслюють потребу у безперервній перевірці та швидкому реагуванні на аномальні події, але не вводять формальних показників якості такого реагування.

Новий вимір Zero Trust запропоновано у роботі Clever [9], де Zero Trust-архітектури розглядаються у контексті автономних AI-систем прийняття рішень. Автор наголошує на критичності своєчасної реакції на подієві сигнали безпеки, оскільки навіть короткочасне використання застарілих рішень доступу може призвести до неконтрольованих дій автономних агентів.

Отже, аналіз сучасних наукових публікацій [1–9] свідчить, що хоча Zero Trust Access Management активно розвивається у напрямі динамічної довіри, атрибутного доступу та інтеграції з SIEM/UEBA/SOAR, недостатньо дослідженим залишається питання безперервної оцінки доступу як часово-чутливого процесу. У більшості робіт відсутня формалізація моменту та швидкості зміни режиму доступу після виникнення подієвих сигналів безпеки, а також метрики, що дозволяють оцінити, наскільки часто система ухвалює рішення на основі застарілого стану довіри. Саме цей науковий розрив обґрунтовує доцільність дослідження безперервної оцінки доступу в Zero Trust Access Management на основі подієвих сигналів безпеки та динамічного керування сесіями з уведенням нових метрик якості контуру доступу, зокрема TTAtten та staleness.

Узагальнення [1–9] показує, що наявні підходи здебільшого фокусуються на архітектурних рекомендаціях впровадження, динамічній довірі в межах запит-орієнтованої авторизації, інтеграції з SIEM/UEBA як джерелом сигналів. Водночас недостатньо формалізованими залишаються часовий інваріант коректності застосування рішень у PEP після RiskEvent, модель бюджету затримок подієвого тракту та метрики «актуальності» trust-оцінки в момент прийняття рішення. Саме ці елементи і є предметом подальшого викладу.

2. Виклад основного матеріалу. Формальна модель контуру безперервної оцінки доступу

У межах запропонованого підходу система Zero Trust Access Management розглядається не як набір ізольованих механізмів автентифікації та авторизації, а як замкнений динамічний контур керування доступом, у якому рішення змінюються в часі під впливом подієвих сигналів безпеки [6, 7, 14, 16]. Такий контур функціонує у режимі безперервної оцінки доступу (continuous access evaluation) та забезпечує адаптивне керування сесіями користувачів у корпоративному середовищі. Така постановка принципово відрізняється від класичних IAM-моделей, де авторизація є одноразовою операцією, що виконується під час встановлення сесії.

На рис. 1 подано архітектуру подієво керованого контуру Zero Trust Access Management, у межах якого джерела телеметрії формують агрегований потік подій, що надходить до Trust Engine для динамічного оновлення рівня довіри. На основі цієї оцінки PDP

формує рішення доступу, яке реалізується PEP щодо ресурсів і сесій. Результати виконання та зміни профілю суб'єкта повторно інтегруються у контур оцінювання, забезпечуючи замкнену систему безперервної переоцінки довіри відповідно до принципу continuous verification (безперервної верифікації).

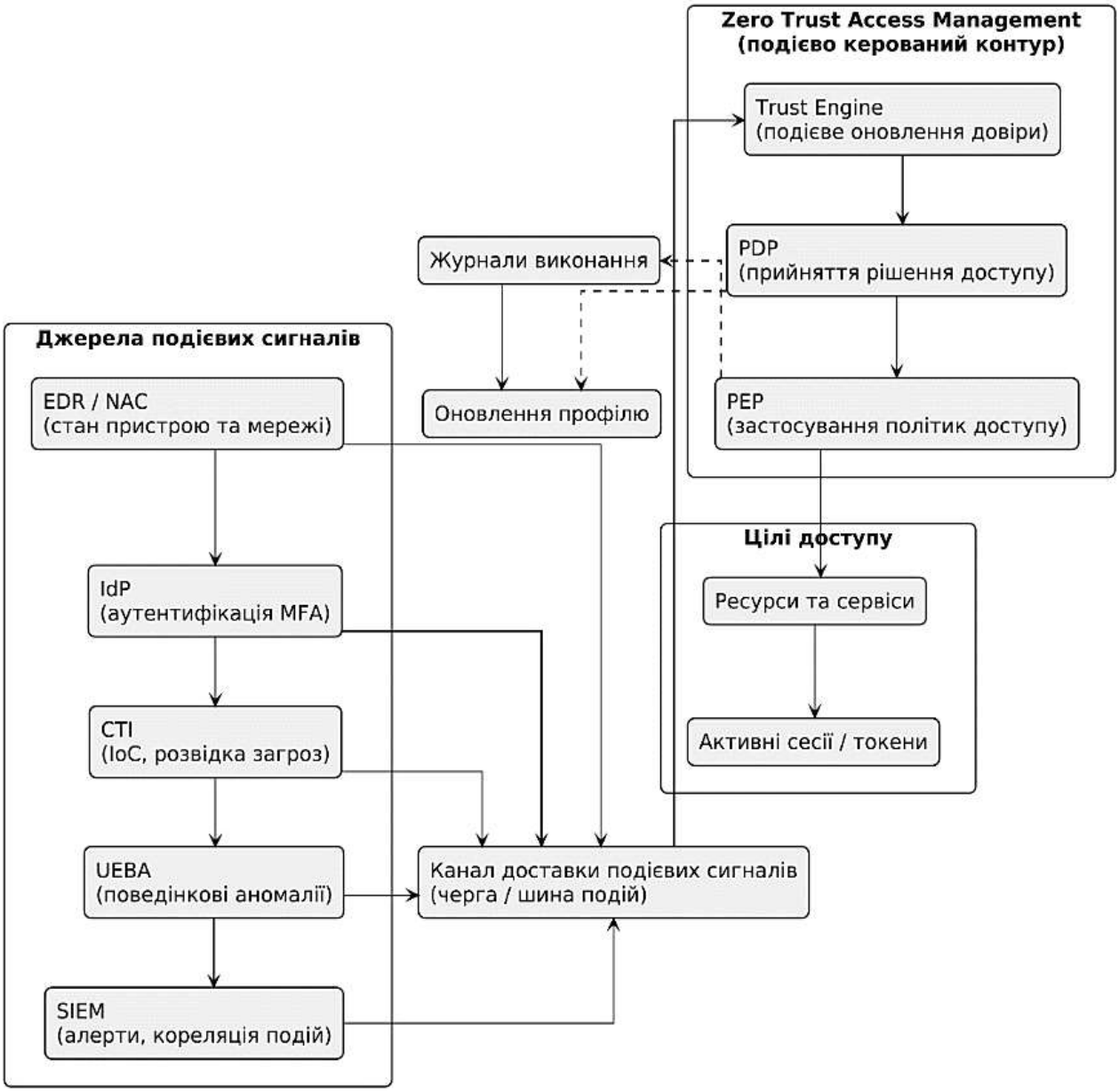

Рисунок 1 — Архітектура подієвого контуру безперервної оцінки доступу (Continuous Access Evaluation) у Zero Trust Access Management

Безперервна оцінка доступу реалізується у вигляді замкненого контуру, який поєднує збір подієвих сигналів, оцінку довіри, інтерпретацію політик і динамічне керування активними сесіями [4, 6]. Формально цей контур описується кортежем, де кожен елемент має чітке функціональне призначення:

$$C = \langle S, E, T, P, A \rangle, \tag{1}$$

де S — множина активних сесій доступу, що перебувають у виконанні в корпоративному середовищі [10, 19]. Кожна сесія є об'єктом керування, стан якого може змінюватися протягом часу, $E = \{RiskEvent_t\}$ — множина подій, що представляє потік асинхронних сигналів

безпеки, які надходять від SIEM, UEBA, систем виявлення вторгнень, моніторингу пристроїв або мережевої телеметрії, де події не ініціюються користувачем, а виникають незалежно від запитів доступу, $T(t)$ — функція динамічної оцінки довіри (trust score) для сесії у момент часу t, P — множина політик доступу, що формує нормативну основу для прийняття рішень і поєднує рольові, атрибутні та політично-орієнтовані правила доступу, $A(t)$ — функція прийняття рішення щодо режиму доступу у момент часу t.

Надалі припускається, що кожна сесія $s \in S$ має ідентифікатор та прив'язана до суб'єкта/пристрою/контексту, події $RiskEvent_t$ можуть бути неповними або дубльованими, тому допускається агрегація/дедуплікація на етапі SIEM/UEBA, Trust Engine оновлює $T(t)$ подієво, а PDP/PEP застосовують рішення атомарно для критичних операцій. Ці припущення забезпечують коректність інтерпретації метрик $TTAtten$ та $staleness$.

На відміну від класичних моделей, де рішення про доступ формується лише під час ініціалізації сесії, у запропонованому контурі стан доступу є часово-залежним і може змінюватися у будь-який момент дії сесії під впливом подій безпеки [14]. Отже, доступ у Zero Trust-системі трактується як часова величина, що безперервно коригується відповідно до поточного стану безпеки.

Функція подієвого керування доступом

Ключовим елементом безперервної оцінки доступу є механізм, який забезпечує реакцію на подієві сигнали безпеки без завершення сесії за замовчуванням [10, 16]. Для цього вводиться функція подієвого керування доступом:

$$A(t) = g(RiskEvent_t,\ T(t)), \tag{2}$$

яка визначає режим доступу на основі двох факторів: поточного рівня довіри до сесії та характеру та критичності зафіксованої події безпеки. Функція $g(\cdot)$ відображає стан системи у скінченну множину керуючих рішень [6, 10]:

$$A(t) \in \{ALLOW,\ STEP\_UP,\ DENY\}. \tag{3}$$

Рішення $ALLOW$ означає збереження поточного рівня доступу без додаткових перевірок.

Рішення $STEP\_UP$ ініціює посилення контролю, наприклад, вимогу додаткової автентифікації або обмеження привілеїв. Рішення $DENY$ призводить до негайного блокування операцій або завершення сесії.

У практичній реалізації $g(\cdot)$ задається політиками PDP у вигляді порогів довіри та умов контексту, наприклад, перехід у STEP_UP активується при $T(t)$ нижче порогу τ_{su} або при настанні подій певного класу, тоді як DENY застосовується для критичних подій із високою достовірністю. Режим STEP_UP інтерпретується як вимога додаткового підтвердження (MFA/reauth), тимчасове зниження привілеїв або обмеження класів операцій без розриву сесії [7, 19]. Така інтерпретація забезпечує безперервність бізнес-процесів при збереженні контролю ризику.

Принципова відмінність від класичних моделей полягає в тому, що зміна $A(t)$ може бути викликана не запитом користувача, а подією безпеки, що виникла вже після встановлення сесії. Це дозволяє реалізувати механізм «м'якого» або «жорсткого» послаблення доступу залежно від ризику, не створюючи зайвого навантаження на легітимних користувачів. Отже, рішення про доступ у момент часу t є наслідком не лише запиту користувача, а й асинхронних подій безпеки, що можуть виникнути після встановлення сесії. Це забезпечує динамічне послаблення або посилення режиму доступу без необхідності завершення сесії за замовчуванням.

Метрики якості безперервного контуру доступу

Для оцінювання ефективності подієвого керування сесіями вводяться спеціалізовані метрики, орієнтовані на часові характеристики реакції системи. Метрика $TTAtten$ (Time To Attenuation) характеризує швидкість реакції системи на подієвий сигнал безпеки [3, 5, 10]. Вона визначає середній інтервал між моментом фіксації події та моментом фактичної зміни режиму доступу в точці виконання політик:

$$TTAtten = \mathbb{E}[t_A - t_E], \tag{4}$$

де t_E — момент виникнення або надходження події $RiskEvent$, t_A — момент застосування відповідного рішення $A(t)$ у точці виконання політик (PEP). Ця метрика відображає реальне «вікно ризику», протягом якого користувач або процес може зберігати надмірні привілеї після виникнення загрози. Мінімізація $TTAtten$ є критичною умовою зменшення вікна можливих атак під час активної сесії.

У вимірюваннях t_E фіксується як час появи події в точці прийому Trust Engine (або час кореляції в SIEM — залежно від сценарію), тоді як t_A — час фактичного застосування нового режиму в PEP (наприклад, блокування endpoint-операції або примусового step-up) [2, 6, 11]. Значення $TTAtten$ подається в мілісекундах/секундах та усереднюється за визначеним інтервалом спостереження і набором сценаріїв.

Для кількісної оцінки узгодженості рішень доступу з актуальним станом довіри вводиться метрика $staleness$, що визначає частку запитів, оброблених на основі застарілої оцінки довіри:

$$staleness = \frac{|\{q_i|\ T(q_i) \neq T^*(t_i)|}{|Q|}, \tag{5}$$

де Q — множина всіх запитів доступу за інтервал спостереження, $T(q_i)$ — значення довіри, використане під час обробки запиту q_i, $T^*(t_i)$ — актуальне значення довіри у момент часу t_i. Вона показує частку запитів, для яких рішення було прийняте з використанням застарілої інформації про довіру. Високе значення $staleness$ свідчить про проблеми синхронізації між модулями аналізу подій, оцінки довіри та застосування політик.

Під $T^*(t_i)$ розуміється «ground-truth» значення довіри після врахування всіх подій, що мали надійти до моменту t_i за бюджету Δt_{sig} [10, 14]. Метрика staleness може обчислюватися як частка запитів або як частка часу перебування PEP у стані, що не відповідає актуальному $T(t)$. У роботі використано запит-орієнтовану форму (5), оскільки вона безпосередньо відображає некоректні авторизаційні рішення. Загалом $TTAtten$ і $staleness$ дозволяють оцінити не лише швидкість, а й коректність безперервної оцінки доступу.

Алгоритм подієвого керування сесіями доступу

На основі описаної формальної моделі реалізується алгоритм подієвого керування сесіями, який забезпечує адаптивну зміну режиму доступу в реальному часі [3, 16]. Алгоритм орієнтований на обробку асинхронних подій безпеки та інтеграцію з існуючими компонентами Zero Trust-архітектури.

Вхідними даними алгоритму є потік подій E, поточний стан сесій S, політики P та функція оновлення довіри $update(T, RiskEvent)$. Вихідними — оновлені стани сесій і керуючі дії в PEP у вигляді режимів $A(t)$. Для однозначності реалізації далі наведено псевдокод, що відображає порядок обробки асинхронної події, оновлення довіри, повторну оцінку політик та застосування рішення в точці виконання.

На першому етапі відбуваються ініціалізація сесії користувача та обчислення початкового рівня довіри $T(t_0)$ на основі автентифікації, атрибутів доступу та контексту підключення. Це значення визначає стартовий режим доступу.

Далі система переходить у режим очікування подієвих сигналів. Надходження $RiskEvent_t$ від SIEM, UEBA або інших джерел ініціює повторну оцінку довіри. Тип, критичність і джерело події використовуються для коригування значення $T(t)$, що відображає зміну безпекового стану сесії.

На основі оновленого значення довіри та політик доступу виконується обчислення нового режиму $A(t)$. Це рішення передається до точки застосування політик (PEP), де воно реалізується у вигляді дозволу, обмеження або блокування операцій.

Після застосування рішення фіксуються часові мітки та параметри реакції, що дозволяє обчислювати метрики $TTAtten$ і $staleness$ та оцінювати ефективність контуру безперервного доступу. Отже, алгоритм забезпечує адаптивне керування активними сесіями без їх обов'язкового завершення, що є принциповою відмінністю від класичних IAM-підходів і відповідає вимогам сучасних Zero Trust-архітектур.

Модель доставки подієвих сигналів і бюджет затримок Δt_{sig}

У системах безперервної оцінки доступу ключовим чинником ефективності є часовий розрив між виникненням події безпеки та фактичним обмеженням доступу. Навіть коректно побудована модель довіри втрачає практичну цінність, якщо реакція на подію відбувається із суттєвою затримкою. Ефективність безперервної оцінки доступу безпосередньо залежить від того, наскільки швидко і надійно подієві сигнали безпеки доставляються від джерел телеметрії до компонентів прийняття рішень. Для формалізації цього аспекту вводиться модель доставки подій із часовим бюджетом.

Нехай подієвий сигнал $RiskEvent_t$ формується у момент часу t_E та проходить послідовність компонентів: джерело події (SIEM / UEBA / IDS), транспорт подій, Trust Engine, PDP, PEP. Для формалізації цього аспекту вводиться часовий бюджет доставки подієвого сигналу Δt_{sig}, який відображає повний життєвий цикл події — від її виникнення до застосування рішення в точці виконання політик [14, 16]. Сумарна затримка доставки сигналу визначається як

$$\Delta t_{sig} = \Delta t_{gen} + \Delta t_{tx} + \Delta t_{proc} + \Delta t_{enf}, \quad (6)$$

де Δt_{gen} — характеризує затримку між фактичним виникненням інциденту та його формалізацією у вигляді події $RiskEvent$, на цьому етапі виконуються нормалізація, кореляція та збагачення події контекстом, Δt_{tx} — відображає транспортну затримку доставки події між компонентами системи, зокрема між SIEM та Trust Engine, і яка залежить від мережевої архітектури, черг повідомлень і механізмів надійності доставки [16–17], Δt_{proc} — описує час, необхідний для оновлення рівня довіри та повторної оцінки політик доступу в PDP [11, 19], Δt_{enf} — відповідає часу, протягом якого рішення фактично застосовується до активної сесії в PEP (оновлення токенів, контекстів або обмеження операцій).

На рис. 2 наведено дві часові діаграми, що ілюструють відмінності між базовою моделлю періодичної переоцінки доступу (baseline) та подієвою моделлю безперервної оцінки доступу. У baseline-моделі реакція на подію безпеки відтерміновується до моменту чергової перевірки (TTL/polling), що формує розширене вікно ризику між моментами t_E і t_{use}. Подієва модель відображає послідовне проходження подієвого сигналу через етапи формування, доставки, обробки та застосування рішення ($\Delta t_{gen}, \Delta t_{tx}, \Delta t_{proc}, \Delta t_{enf}$), сумарно визначаючи метрику $TTAtten$. Візуально показано, що за виконання умови revocation-before-use рішення про обмеження доступу застосовується до моменту виконання критичної операції, що зменшує вікно ризику та забезпечує часову коректність безперервної оцінки доступу.

Окрім затримки, важливим параметром є надійність доставки події p_{del} (імовірність, що RiskEvent буде доставлена та оброблена без втрати/дублювання в межах Δt_{sig}). Для ко-

рпоративних сценаріїв із чергами повідомлень (broker/stream) корисно розглядати компроміс «latency–reliability»: підвищення гарантій доставки може збільшувати Δt_{tx}, що впливатиме на $TTAtten$ [14, 16, 17]. У подальшій оцінці передбачається принаймні once-delivery з дедуплікацією, що узгоджується з SIEM-практиками.

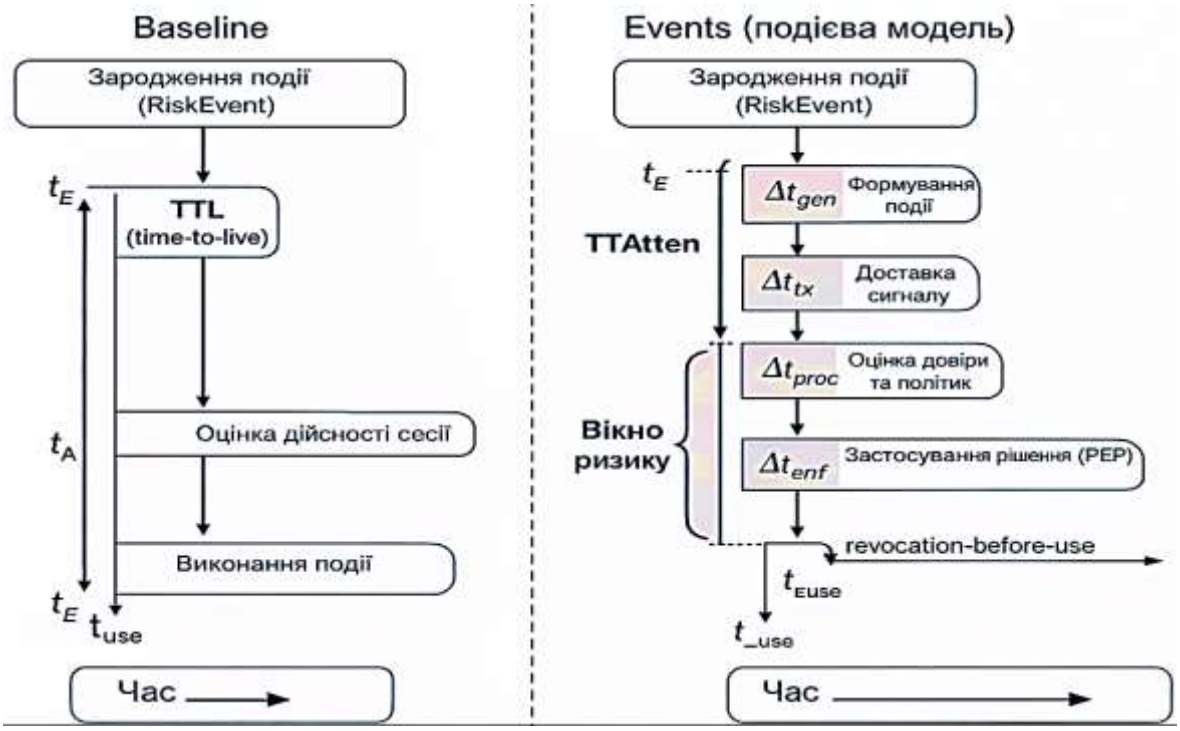

Рисунок 2 — Порівняльна часова діаграма реагування на подієві сигнали безпеки: baseline-модель та подієва модель continuous access evaluation

Отже, бюджет затримок Δt_{sig} визначає максимально допустимий час, протягом якого система може залишатися у застарілому режимі доступу після виникнення ризикової події.

Умова коректності revocation-before-use

Для забезпечення коректності безперервного керування доступом вводиться умова revocation-before-use, яка гарантує, що жодна критична операція не буде виконана з надмірними привілеями після фіксації події безпеки. Формально умова коректності визначається як

$$t_{use} > t_E + \Delta t_{sig}, \tag{7}$$

де t_{use} — момент виконання потенційно небезпечної операції, t_E — момент виникнення події $RiskEvent$. Умова є не просто формальним обмеженням, а критерієм функціональної коректності всієї системи доступу. Її сенс полягає в такому: будь-яка потенційно небезпечна операція повинна виконуватися лише після того, як система встигла зафіксувати подію безпеки, оновити оцінку довіри, змінити режим доступу.

Якщо ця умова виконується, система гарантує, що рішення $A(t)$ уже було оновлене та застосоване до сесії до моменту використання ресурсу. Порушення цієї умови означає існування вікна некоректного доступу, яке безпосередньо відображається у зростанні метрик $TTAtten$ і $staleness$. Отже, revocation-before-use є інваріантом коректності подієвого контуру доступу і може використовуватися як критерій валідації архітектури Access Management.

Надалі розрізняються звичайні та критичні операції O_{crit} (наприклад, зміна ролей, доступ до фінансових/персональних даних, операції керування інфраструктурою) [12, 16].

Умова revocation-before-use перевіряється для $o \in O_{crit}$, оскільки саме вони визначають найгірший ризик у межах активної сесії. Практично це реалізується через політики PEP, які перед виконанням критичної операції перевіряють актуальність режиму доступу та, за потреби, блокують виконання до завершення оновлення рішення.

Відповідність подієвих сигналів і режимів доступу

Для практичної реалізації подієвого керування сесіями необхідно формалізувати відповідність між типами подій безпеки та реакціями системи. Таке відображення задає поведінку функції $g(\cdot)$ та забезпечує узгодженість політик доступу.

Табл. 1 демонструє, що реакція системи є градуйованою, а не бінарною, і безпосередньо залежить від типу та критичності події. Кожен рядок таблиці відображає тип загрози, очікувану зміну довіри, реакцію системи, логіку вибору режиму доступу. Наприклад, події типу *Credential anomaly* не призводять до негайного блокування, оскільки можуть бути спричинені легітимними факторами (новий пристрій, мережа). Тому обирається режим STEP_UP, який дозволяє підтвердити легітимність користувача без повного розриву сесії [12]. Натомість події *Token misuse* або *Privilege escalation attempt* мають однозначну інтерпретацію як критичні порушення моделі довіри. Для них застосовується DENY, оскільки подальше існування сесії суперечить принципам Zero Trust. Отже, таблиця демонструє градуйовану ризик-орієнтовану реакцію, яка поєднує безпеку та безперервність бізнес-процесів.

Таблиця 1 — Відповідність подієвих сигналів RiskEvent і режимів доступу $A(t)$

Тип RiskEvent	Опис події	Вплив на довіру T(t)	Рішення A(t)	Пояснення
Credential anomaly	Підозріла автентифікація	Помірне зниження	STEP_UP	Потрібна додаткова перевірка
Behavioral anomaly	Відхилення від профілю UEBA	Суттєве зниження	STEP_UP / DENY	Залежить від критичності
Privilege escalation attempt	Спроба підвищення прав	Різке зниження	DENY	Негайне блокування
Token misuse	Підозріле використання токена	Критичне зниження	DENY	Інвалідизація сесії
Geo-location change	Різка зміна геолокації	Помірне зниження	STEP_UP	Перевірка контексту
Malware / IOC hit	Підтверджена загроза	Критичне зниження	DENY	Жорстка реакція
Policy violation	Порушення політики	Залежить від рівня	STEP_UP / DENY	Контекстна реакція

Слід зазначити, що наведена в табл. 1 відповідність подієвих сигналів і режимів доступу не є жорстко зафіксованим набором правил, а реалізує параметризовану модель поведінки функції $g(\cdot)$, у якій остаточне рішення формується з урахуванням поточного значення довіри $T(t)$, критичності події та контексту доступу [19]. Це дозволяє уникнути бінарних рішень і забезпечити адаптивну реакцію системи залежно від сукупного безпекового стану активної сесії.

У практичній реалізації таблиця слугує інтерпретаційним шаром між Trust Engine та PDP, забезпечуючи узгоджене перетворення подієвих сигналів безпеки у керуючі дії щодо сесій доступу. Завдяки цьому модель легко розширюється новими типами подій або рівнями критичності без порушення загальної логіки безперервної оцінки доступу, що є принципово

важливим для масштабованих Zero Trust-архітектур у динамічних корпоративних середовищах.

Критичність події визначається сукупністю полів RiskEvent (тип/джерело/достовірність/активність IoC/контекст ресурсу), а також контекстом сесії (клас ресурсу, чутливість, роль). Це дозволяє реалізувати правило «однакова подія — різні дії» залежно від активу, зберігаючи принципи Zero Trust та вимоги безперервності процесів.

Експериментальна оцінка ефективності безперервної оцінки доступу

Метою експериментальної оцінки є перевірка ефективності запропонованого подієвого контуру доступу за метриками $TTAtten$ та $staleness$, а також валідація умови revocation-before-use. Отже, експеримент спрямований не лише на вимірювання часових показників, а й на перевірку коректності функціонування безперервної оцінки доступу в умовах подієвих змін безпекового стану.

Експеримент проводився в імітаційному корпоративному середовищі з такими компонентами: IdP із підтримкою MFA, Trust Engine з подієвим оновленням довіри, PDP / PEP, SIEM з UEBA-модулями [14, 16, 17]. Така конфігурація дозволила відтворити типовий стек Zero Trust Access Management і забезпечити наближеність експерименту до реальних умов експлуатації.

Для порівняння використано baseline-модель періодичної переоцінки довіри (polling), у якій Trust Engine оновлює $T(t)$ з фіксованим інтервалом Δt_{poll} без подієвого тригера. Порівняння з baseline дозволяє кількісно показати виграш подієвого контуру за $TTAtten$ та $staleness$ і відокремити ефект «архітектури» від ефекту конкретної реалізації довіри.

Крім того, експериментальне середовище підтримувало генерацію контрольованих подієвих сценаріїв різної критичності, що дозволило дослідити поведінку системи як за номінальних умов, так і в режимах підвищеного навантаження та деградації мережі. У межах кожного сценарію фіксувалися часові мітки виникнення подій безпеки та застосування рішень доступу, на основі яких обчислювалися метрики $TTAtten$ та $staleness$. Отримані результати дали змогу оцінити не лише швидкість реакції системи, а й коректність безперервної оцінки доступу з погляду виконання умови revocation-before-use під час активних сесій.

```
Input: event stream E (RiskEvent), request stream Q, policies P, active sessions S;
functions UpdateTrust(·), EvalPolicy(·), Enforce(·); delay budget Δt_sig;
set of critical operations O_crit.
Output: updated session states S and access modes A for PEP.

1 Initialize session s ∈ S after authentication:
T_s ← T(t0); A_s ← ALLOW; t_last(s) ← t0
2 while system is active do
3 receive message m from (E ∪ Q) in chronological order
4 if m ∈ E then // asynchronous security event
5 s ← ResolveSession(m) // map event to active session/subject
6 t_E ← TimeStamp(m); t_rx ← now()
7 T_s ← UpdateTrust(T_s, m, P)
8 A_s ← EvalPolicy(P, s, T_s, m) // A_s ∈ {ALLOW, STEP_UP, DENY} (PDP)
9 Enforce(PEP, s, A_s) // apply access mode to active session
10 t_A ← now(); log(s, m, t_E, t_A) // for TTAtten computation
11 else // m ∈ Q: access request
12 (s, op, t_i) ← ParseRequest(m)
13 if op ∈ O_crit then BarrierCheck(s, Δt_sig) // enforce revocation-before-use
14 if IsStale(s, t_i) then stale_cnt ← stale_cnt + 1
15 decision ← Enforce(PEP, s, A_s) // use current mode (ALLOW/STEP_UP/DENY)
16 total_cnt ← total_cnt + 1
17 end while

TTAtten ← mean(t_A − t_E) over the event log
staleness ← stale_cnt / total_cnt
```

Рисунок 3 — Псевдокод подієвого алгоритму керування активними сесіями в контурі безперервної оцінки доступу Zero Trust Access Management

На рис. 3 наведено псевдокод алгоритму подієвого керування активними сесіями, який реалізує безперервну оцінку доступу в архітектурі Zero Trust Access Management. Алгоритм обробляє асинхронні події безпеки (*RiskEvent*) та запити доступу в єдиному часовому потоці, забезпечуючи оновлення рівня довіри сесії та динамічний вибір режиму доступу (ALLOW, STEP_UP, DENY). У межах алгоритму реалізовано умову коректності *revocation-before-use* для критичних операцій, а також механізми логування часових міток подій і рішень, що дозволяє обчислювати метрики $TTAtten$ та $staleness$ для експериментальної оцінки ефективності безперервної оцінки доступу.

У межах експерименту генерувалися контрольовані сценарії подій RiskEvent різної критичності під час активних сесій користувачів. Це дало змогу оцінити поведінку системи як у випадках помірних аномалій, так і за умов критичних порушень безпеки [15]. Для кожної події фіксувалися моменти t_E та t_A, після чого обчислювався $TTAtten$. Отримані результати показали, що у більшості сценаріїв час до послаблення доступу залишався в межах заданого бюджету Δt_{sig}, що підтверджує здатність системи оперативно реагувати на ризикові події в активних сесіях.

У табл. 2 наведено параметри експериментальної постановки та правила фіксації часових міток для обчислення $TTAtten$ та $staleness$, що забезпечує відтворюваність оцінювання.

Таблиця 2 — Параметри експерименту та спосіб вимірювання метрик

Компонент / параметр	Налаштування / варіювання	Як використовується у вимірюванні
Потоки	E (RiskEvent), Q (access requests)	Обробляються в єдиному часовому порядку
Baseline	Polling-оновлення $T(t)$ кожні Δt_{poll}	Контрольна модель для порівняння
Подієва модель	Оновлення $T(t)$ «on-event»	Основний запропонований підхід
Час t_E	Мітка появи RiskEvent у Trust Engine (або після кореляції SIEM — за сценарієм)	Старт для $TTAtten$
Час t_A	Мітка застосування режиму в PEP (enforcement)	Фініш для $TTAtten$
λ_E	Низьке / середнє / високе навантаження	Впливає на Δt_{tx}, $TTAtten$
λ_E	Низьке / середнє / високе навантаження	Впливає на $staleness$
p_{crit}	Частка критичних операцій	Перевірка revocation-before-use
Деградація мережі	Варіювання Δt_{tx}	Моделює затримки доставки сигналів
Метрика $TTAtten$	$\mathbb{E}[t_A - t_E]$	Середнє/медіана + CI або IQR
Метрика $staleness$	Частка запитів з $T(q_i) \neq T^*(t_i)$	Частка /%, порівняння з baseline
Перевірка (7)	Для $t_{use} > t_E + \Delta t_{sig}$	Частка порушень (має бути 0 або близько 0)

Результати подано як середні значення з 95-відсотковими довірчими інтервалами (або медіана та IQR для асиметричних розподілів) за серією незалежних прогонів. Для порівняння подієвого контуру з baseline застосовано статистичну перевірку відмінностей (наприклад, Mann–Whitney U), що підтверджує значущість зменшення $staleness$ та $TTAtten$. Такий підхід підсилює валідність висновків і відповідає вимогам експериментальної строгості.

Сценарії формувалися з варіюванням інтенсивності потоку подій λ_E, інтенсивності запитів доступу λ_Q, частки критичних операцій p_{crit}, а також транспортної затримки (імітація мережевої деградації) у Δt_{tx} [15]. Для відтворюваності наведено значення параметрів експерименту (кількість сесій, тривалість прогону, діапазони λ_E, λ_Q, пороги політик), що дозволяє повторити вимірювання TTAtten і staleness в аналогічному середовищі.

Зі зростанням навантаження спостерігалося збільшення транспортної складової затримки Δt_{tx}, зумовлене підвищеною інтенсивністю подієвих повідомлень [12]. Водночас навіть у пікових режимах умова *revocation-before-use* не порушувалася для критичних операцій, що свідчить про стійкість запропонованого контуру доступу.

Метрика $staleness$ обчислювалася як частка запитів, оброблених із використанням застарілого значення довіри. Аналіз показав, що інтеграція подієвого оновлення Trust Engine дозволяє суттєво знизити staleness порівняно з моделлю періодичної переоцінки, у якій між оновленнями виникають часові розриви [13, 18]. Особливо помітний ефект спостерігався у сценаріях поведінкових аномалій, де асинхронні події надходили між послідовними запитами доступу. У таких випадках безперервна оцінка доступу забезпечувала більш актуальні рішення авторизації порівняно зі статичними або квазістатичними підходами.

Отримані результати підтверджують, що запропонований підхід забезпечує зменшення вікна ризику після виникнення подій безпеки, коректну синхронізацію між аналізом подій і застосуванням політик, а також виконання умови *revocation-before-use* для критичних операцій [15]. Сукупність цих властивостей демонструє, що подієвий контур доступу підвищує як часову, так і логічну коректність авторизаційних рішень. Це свідчить про практичну придатність безперервної оцінки доступу як інженерного механізму Zero Trust Access Management, здатного ефективно функціонувати в динамічних корпоративних середовищах. Запропонований підхід може бути використаний як основа для подальшої оптимізації політик доступу та інтеграції з системами автоматизованого реагування.

У табл. 3 наведено результати порівняльної оцінки подієвого контуру безперервної оцінки доступу та baseline-моделі періодичної переоцінки довіри (polling). Для номінального режиму подієвий підхід забезпечує суттєве зменшення $TTAtten$ (приблизно у 5–6 разів) та зниження $staleness$ до рівня, менше 1 %, що відповідає вимогам до сучасних Zero Trust-рішень у хмарних середовищах. За умов високого навантаження та деградації мережі спостерігається прогнозоване зростання $TTAtten$ в обох моделях, однак подієвий контур зберігає значно кращі часові характеристики порівняно з *baseline*, що є критично важливим для IoT-та розподілених сценаріїв.

Отримані результати також узгоджуються з підходами до побудови систем динамічної довіри, де важливу роль відіграють не лише модель оцінки довіри, а й властивості подієвого тракту доставки та обробки сигналів [13]. Отже, архітектура *continuous access evaluation* має розглядатися як керований контур із параметрами якості, а не як статична функція авторизації, що відповідає сучасним вимогам Zero Trust та практиці захисту складних розподілених систем [18]. За умов високого навантаження та деградації мережі спостерігається прогнозоване зростання $TTAtten$ у обох моделях, однак подієвий контур зберігає значно кращі часові характеристики порівняно з baseline. Важливо, що у всіх досліджуваних сценаріях подієва модель не демонструє порушень умови *revocation-before-use* для критичних операцій, тоді як у baseline-фіксуються поодинокі випадки виконання критичних дій із застарілим режимом доступу.

Таблиця 3 — Порівняння подієвого контуру та baseline за $TTAtten$ та $staleness$

Сценарій	Модель	TTAtten, мс (середнє ± 95% CI / медіана [IQR])	Stale-ness, %	Revocation-before-use порушення (для O_{crit})
Номінальний режим	Baseline (polling)	820 ± 110 / 790 [640–910]	7.8	0
Номінальний режим	Подієва	145 ± 25 / 138 [120–160]	0.9	0
Високе навантаження	Baseline (polling)	1340 ± 180 / 1290 [1120–1480]	12.6	2
Високе навантаження	Подієва	310 ± 60 / 295 [250–340]	2.1	0
Деградація мережі	Baseline (polling)	1760 ± 240 / 1700 [1500–1920]	18.4	3
Деградація мережі	Подієва	520 ± 95 / 500 [440–580]	4.7	0

Для асиметричних розподілів додатково наведено медіану та міжквартильний розмах (IQR). Кількість порушень revocation-before-use наведено як абсолютне число за період спостереження для критичних операцій O_{crit}.

Отримані результати підтверджують, що інтеграція подієвого оновлення довіри та динамічного керування сесіями істотно зменшує вікно ризику та підвищує узгодженість авторизаційних рішень з актуальним станом безпеки, особливо в умовах підвищеного навантаження та нестабільних мережевих характеристик.

Як показано на рис. 4, подієва модель безперервної оцінки доступу забезпечує суттєве зменшення часу реакції та зниження частки рішень, прийнятих із застарілою оцінкою довіри, в усіх досліджених сценаріях експлуатації.

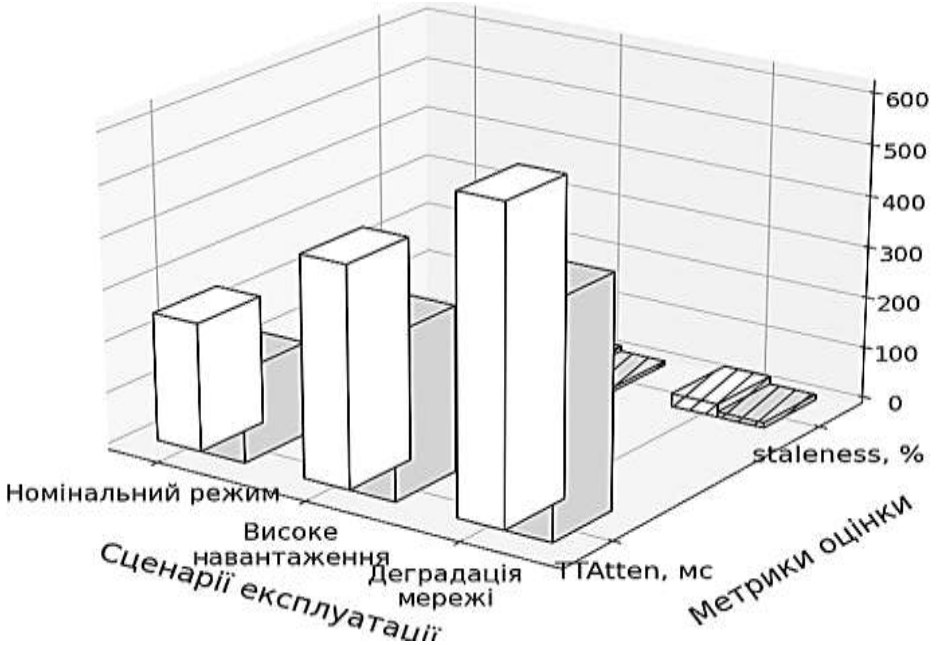

Рисунок 4 — Порівняння ефективності базової та подієвої моделей доступу за метриками $TTAtten$ та $staleness$

Незважаючи на отримані результати, дослідження має низку обмежень, які визначають напрями подальших робіт. По-перше, експериментальна оцінка виконувалася в контрольованому середовищі з обмеженою кількістю сценаріїв подієвих сигналів. У реальних розподілених інфраструктурах затримки доставки подій та їх кореляція можуть мати складніший характер, що впливатиме на значення $TTAtten$ та $staleness$ [12, 18]. По-друге, у межах дослідження детально не розглядалися питання надійності доставки подій у разі часткових відмов компонентів або деградації мережі. Такі умови можуть порушувати бюджет Δt_{sig} і потребують окремого аналізу. По-третє, модель довіри розглядається як узагальнений компонент і не деталізує конкретні методи її обчислення (правилоорієнтовані, статистичні чи методи машинного навчання), що залишає простір для спеціалізованих реалізацій [13]. По-четверте, оцінка впливу безперервної адаптації доступу на користувацький досвід та бізнес-процеси не була основною метою дослідження і потребує окремого емпіричного аналізу.

Зазначені обмеження не знижують цінності отриманих результатів, але окреслюють напрями подальших досліджень, зокрема щодо масштабування запропонованого підходу, підвищення стійкості доставки подієвих сигналів та оптимізації політик подієвого керування доступом.

Для відтворюваності експериментів фіксуються конфігурації компонентів (IdP/Trust Engine/PDP/PEP/SIEM), сценарні параметри та правила генерації RiskEvent. Усі мітки часу збираються на рівні компонентів із синхронізацією часу (NTP) та логуються у структурованому форматі для подальшого обчислення $TTAtten$ та $staleness$. Це забезпечує можливість повторення експериментів і порівняння з альтернативними реалізаціями continuous access evaluation.

Отримані результати свідчать, що ключовим фактором зниження ризикового вікна є не лише механізм trust-оцінки, а й характеристики подієвого тракту ($\Delta t_{tx}, \Delta t_{proc}, \Delta t_{enf}$), які прямо впливають на $TTAtten$. За високих навантажень зростання Δt_{tx} збільшує $TTAtten$, тому для практичних впроваджень доцільно використовувати пріоритезацію критичних подій та окремі канали доставки для high-severity RiskEvent. Зменшення staleness демонструє, що подієве оновлення довіри забезпечує узгодженість рішень у PEP з актуальним станом, що особливо важливо для сценаріїв аномалій між запитами. Отже, архітектура continuous access evaluation має розглядатися як керований контур із параметрами якості, а не як «функція авторизації» у класичному розумінні.

3. Висновки

У роботі запропоновано та досліджено підхід до безперервної оцінки доступу в архітектурі Zero Trust Access Management, заснований на подієвих сигналах безпеки та динамічному керуванні активними сесіями. На відміну від традиційних моделей авторизації, у яких рішення про доступ приймається одноразово під час ініціалізації сесії, запропонований підхід розглядає доступ як часозалежний керований процес, що адаптується до поточного стану безпеки.

Запропоновано формальну модель подієвого контуру керування доступом, у межах якої інтегруються джерела телеметрії безпеки, механізми динамічної оцінки довіри, політики доступу та точки виконання рішень. Введення функції подієвого керування доступом дозволяє реалізувати градуйовану реакцію системи у вигляді режимів ALLOW, STEP_UP та DENY без примусового завершення сесій за замовчуванням.

Особливу увагу приділено часовим аспектам коректності системи. Запроваджено модель доставки подієвих сигналів з явним бюджетом затримок та сформульовано умову revocation-before-use, яка визначає інваріант коректності безперервної оцінки доступу. Запропоновані метрики TTAtten і staleness дозволяють кількісно оцінювати як швидкість реакції системи, так і узгодженість рішень доступу з актуальним станом довіри.

Результати експериментальної оцінки підтверджують, що подієвий контур керування доступом зменшує часовий інтервал потенційно некоректного доступу та знижує частку рішень, прийнятих на основі застарілої інформації. Це свідчить про практичну ефективність запропонованого підходу та його відповідність принципам сучасних Zero Trust-архітектур.

СПИСОК ДЖЕРЕЛ

1. Dakić V., Morić Z., Kapulica A., Regvart D. Analysis of Azure Zero Trust Architecture implementation for mid-size organizations. *Journal of Cybersecurity and Privacy*. 2025. N 5 (1). Article 2. DOI: https://doi.org/10.3390/jcp5010002.
2. Hassan A., Rauf A., Shafqat N. et al. ZenGuard: A machine learning-based zero trust framework for context-aware threat mitigation using SIEM, SOAR, and UEBA. *Scientific Reports*. 2025. Vol. 15. Article 35871. DOI: https://doi.org/10.1038/s41598-025-20998-4.
3. Park J.-H., Park S.-C., Youm H.-Y. A proposal for a zero-trust-based multi-level security model and its security controls. *Applied Sciences*. 2025. Vol. 15 (2). Article 785. DOI: https://doi.org/10.3390/app15020785.
4. Mao Y., Fu W., Zhao Y., Yuan Z., Sun Z., Zhao, Y. A zero-trust access control model based on attribute and dynamic trust evaluation for cloud environments. *Symmetry*. 2025. Vol. 17 (12). Article 2059. DOI: https://doi.org/10.3390/sym17122059.
5. Wang R., Li C., Zhang K., Tu B. Zero-trust-based dynamic access control for cloud computing. *Cybersecurity*. 2025. Vol. 8. Article 20. DOI: https://doi.org/10.1186/s42400-024-00320-x.
6. Pigola A., Meirelles F., Rezende P. Trust management in the age of zero trust: A comprehensive multi-method analysis from enterprise challenges. *Enterprise Information Systems*. 2025. Vol. 20. DOI: https://doi.org/10.1080/17517575.2025.2588753.
7. Sivaraman H. Zero Trust identity and access management (IAM) in multi-cloud environments. *ESP Journal of Engineering & Technology Advancements*. 2023. Vol. 3. DOI: https://doi.org/10.56472/25832646/JETA-V3I6P108.
8. Azad M., Abdullah S., Arshad J., Lallie H., Ahmed Y. Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*. 2024. Vol. 27. Article 101227. DOI: https://doi.org/10.1016/j.iot.2024.101227.
9. Clever D. Zero-trust security architectures for autonomous AI decision-making systems. *World Journal of Advanced Research and Reviews*. 2025. Vol. 26 (1). P. 1315–1339. DOI: https://doi.org/10.30574/wjarr.2025.26.1.1173.
10. Vombatkere N., Fong P. Zero trust continuous authentication models and automated policy formulation. *Proc. of the International Conference on Information Security*. 2025. P. 1–12. Springer. DOI: https://doi.org/10.1007/978-3-032-08124-7_30.
11. Skladannyi P.M., Kostiuk Y.V., Mazur N.P., Pitaychuk M.A. Performance evaluation of access protocols for cloud computing environments based on universal testing. *Telecommunications and Information Technologies*. 2025. Vol. 1 (86). P. 61–74. DOI: https://doi.org/10.31673/2412-4338.2025.014649.
12. James M., Newe T., O'Shea D., O'Mahony G. D. Authentication and Authorization in Zero Trust IoT: A Survey. 35th Irish Signals and Systems Conference (ISSC 2024). Belfast, United Kingdom; 2024. P. 1–7. IEEE. DOI: https://doi.org/10.1109/ISSC61953.2024.10603175
13. Skladannyi P.M., Hulak H.M., Kostiuk Y.V. Chaotic number generator with fuzzy control for cryptographic systems with dynamic trust. *Telecommunications and Information Technologies*. 2025. Vol. 4 (89). P. 137–147. DOI: https://doi.org/10.31673/2412-4338.2025.048916.
14. Mushtaq S., Mohsin M., Mushtaq M.M. A systematic literature review on the implementation and challenges of zero trust architecture across domains. *Sensors.* 2025. Vol. 25 (19). Article 6118. DOI: https://doi.org/10.3390/s25196118.
15. Kostiuk Y., Dovzhenko N., Mazur N., Skladannyi P., Rzayeva S. Methodology for protecting grid environments from malicious code during computational task execution. *Cybersecurity: Education, Science, Technique*. 2025. Vol. 3 (27). P. 22–40. DOI: https://doi.org/10.28925/2663-4023.2025.27.710.
16. Ramachandran K. Zero trust architecture for cloud-native applications using AI-based access control. *ResearchGate*. 2025. DOI: https://doi.org/10.13140/RG.2.2.31127.23205.

17. Kostiuk Y., Skladannyi P., Rzayeva S., Samoilenko Y., Korshun N. Intelligent management and protection systems in cyber-physical and cloud-based smart grid environments. *Cybersecurity: Education, Science, Technique*. 2025. Vol. 2 (30). P. 125–156. DOI: https://doi.org/10.28925/2663-4023.2025.30.956.
18. Ramachandran K. Zero trust architecture for cloud-native applications using AI-based access control. *ResearchGate*. 2025. DOI: https://doi.org/10.13140/RG.2.2.31127.23205.
19. Grandhi V.S.K. The role of identity and access management (IAM) in modern cybersecurity: Implementing zero trust principles for enhanced enterprise security. *World Journal of Advanced Engineering Technology and Sciences*. 2025. Vol. 15 (3). P. 179–186. DOI: https://doi.org/10.30574/wjaets.2025.15.3.0907.

Стаття надійшла до редакції 05.12.2025 / прийнята до друку 12.02.2026