УДК 004.056.5:004.7 https://doi.org/10.15407/pp2026.01.066

Ю.В. Костюк, П.М. Складанний, Д.Д. Гнатченко

РИЗИК-АДАПТИВНА АВТОРИЗАЦІЯ В ZERO TRUST ІЗ ДИНАМІЧНОЮ ДОВІРОЮ ТА ТОКЕНАМИ

У статті розв'язується задача ризик-адаптивної авторизації в архітектурі Zero Trust із використанням механізму динамічної оцінки довіри та адаптивного керування токенами доступу. Актуальність дослідження зумовлена зростанням кількості атак, пов'язаних із компрометацією облікових даних, перехопленням сесій та зловживанням привілеями в корпоративних інформаційних системах. Запропонований підхід базується на безперервному аналізі поведінкових характеристик користувача, параметрів пристрою, мережевого контексту та критичності ресурсу, що дозволяє формувати інтегральний показник ризику в реальному масштабі часу. На відміну від традиційних моделей із фіксованим часом життя токенів і статичними політиками доступу, розроблена модель передбачає динамічну зміну рівня довіри протягом усієї сесії взаємодії. Інтегральний показник ризику визначається як функція ймовірності реалізації загрози та потенційного впливу на актив, що забезпечує адаптивне коригування параметрів авторизації: обсягу привілеїв, часу дії токена, необхідності повторної автентифікації або примусової ротації криптографічних ключів. Реалізовано механізм скорочення або продовження життєвого циклу токена залежно від змін безпекового контексту, що мінімізує вікно можливого використання скомпрометованих облікових даних. Особливу увагу приділено забезпеченню балансу між рівнем безпеки, продуктивністю та зручністю користування. Запропонований підхід підвищує стійкість до атак типу session hijacking, credential stuffing та insider misuse і може бути інтегрований у сучасні системи управління доступом без значного збільшення обчислювальних витрат. Результати моделювання підтверджують ефективність застосування динамічної довіри як ключового елементу ризик-адаптивної авторизації.

Ключові слова: ризик-адаптивна авторизація, Zero Trust (нульова довіра), керування доступом, оцінювання довіри, час життя токена, безпека ідентичностей, керування доступом на основі політик

Y. Kostiuk, P. Skladannyi, D. Hnatchenko

RISK-ADAPTIVE AUTHORIZATION IN ZERO TRUST WITH DYNAMIC TRUST AND TOKENS

The article addresses the problem of risk-adaptive authorization in a Zero Trust architecture using a mechanism of dynamic trust assessment and adaptive access token management. The relevance of the study is driven by the increasing number of attacks related to credential compromise, session hijacking, and privilege misuse in corporate information systems. The proposed approach is based on continuous analysis of user behavioral characteristics, device parameters, network context, and resource criticality, enabling the formation of an integral risk indicator in real time. Unlike traditional models with fixed token lifetimes and static access policies, the developed model provides dynamic adjustment of the trust level throughout the entire interaction session. The integral risk indicator is defined as a function of threat likelihood and potential impact on the asset, ensuring adaptive adjustment of authorization parameters, including privilege scope, token lifetime, requirement for re-authentication, or enforced cryptographic key rotation. A mechanism for shortening or extending the token lifecycle depending on changes in the security context is implemented, thereby minimizing the window of opportunity for exploiting compromised credentials. Special attention is paid to maintaining a balance between security level, system performance, and usability. The proposed approach increases resilience against session hijacking, credential stuffing, and insider misuse attacks and can be integrated into modern access management systems without significant growth in computational overhead. Modeling results confirm the effectiveness of dynamic trust as a key element of risk-adaptive authorization.

Keywords: risk-adaptive authorization, Zero Trust, access management, trust evaluation, token lifetime, identity security, policy-based access control.

Вступ

Цифрова трансформація корпоративних інформаційних систем супроводжується зростанням ролі механізмів керування доступом, у межах яких авторизація виступає ключовим елементом забезпечення інформаційної безпеки [1]. Сучасні атаки дедалі частіше спрямовані не на подолання криптографічних механізмів, а на

компрометацію облікових записів, викрадення токенів доступу та зловживання привілеями, що призводить до тривалого несанкціонованого перебування зловмисника в системі [4, 8, 10]. За таких умов традиційні підходи до авторизації, засновані на статичних політиках і фіксованому часі життя сесій, виявляються недостатньо ефективними, оскільки не враховують динаміку ризиків і контекст виконання операцій.

Актуальність цієї проблеми посилюється впровадженням розподілених, хмарних та гібридних архітектур, у яких користувачі, сервіси та пристрої здійснюють доступ до ресурсів поза межами традиційного периметра безпеки [6-7]. У таких середовищах концепція Zero Trust розглядає кожен запит доступу як потенційно небезпечний і вимагає безперервної перевірки не лише ідентичності, а й рівня довіри, поведінки та контексту доступу [2, 12]. Проте на практиці реалізація Zero Trust часто обмежується посиленою автентифікацією, тоді як авторизація та керування токенами доступу залишаються статичними й слабо адаптованими до поточного стану безпеки.

У науковому та прикладному вимірах залишається відкритою задача побудови формалізованих моделей авторизації, здатних поєднувати оцінювання довіри, ризику та керування сесіями в єдиному контурі ухвалення рішень [1, 15]. Особливої уваги потребує проблема зменшення так званого «вікна атаки» — проміжку часу, протягом якого скомпрометований токен або сесія можуть бути використані зловмисником без виявлення та блокування [8-9, 17]. Розв'язання цієї задачі має безпосередній зв'язок із практичними завданнями підвищення стійкості систем керування доступом, мінімізації наслідків інцидентів безпеки та забезпечення безперервності бізнес-процесів.

У цьому контексті доцільним є розроблення ризик-адаптивних підходів до авторизації, які враховують динамічну зміну рівня довіри до користувача або сервісу, контекстні та поведінкові фактори, а також дозволяють керувати часом життя токенів доступу залежно від поточного ризику [5, 12-13, 15]. Такий підхід забезпечує зв'язок між фундаментальними науковими дослідженнями у сфері моделей доступу та практичними задачами впровадження Zero Trust-архітектур у корпоративних інформаційно-комунікаційних системах.

У роботі зроблено такі внески, що визначають її наукову новизну та практичну цінність. По-перше, формалізовано модель ризик-адаптивної авторизації в архітектурі Zero Trust як динамічного контуру ухвалення рішень [12-13], у якому враховуються суб'єкти доступу, активи, привілеї та контекст безпеки, а ключові параметри довіри й ризику оновлюються під час активної сесії. По-друге, запропоновано механізм $TL - TTL$ [15, 18], який пов'язує динамічну оцінку довіри та операційного ризику з адаптивним керуванням часом життя токенів доступу, забезпечуючи подієву реакцію на ризикові ситуації (поведінкові аномалії, зміни контексту, порушення цілісності пристрою) та скорочення потенційного «вікна атаки» у разі компрометації сесії. По-третє, введено систему метрик для кількісного оцінювання ефективності запропонованого підходу [8, 16], зокрема, метрику вікна атаки W, показники частоти додаткових перевірок доступу S та затримки ухвалення рішень L на рівнях PDP/PEP. По-четверте, виконано сценарне порівняльне оцінювання запропонованого методу з базовими моделями авторизації зі статичним та чутливісно-орієнтованим часом життя токенів [10, 12], що дозволило обґрунтувати переваги ризик-адаптивного керування сесіями в різних умовах доступу. По-п'яте, визначено умови застосування підходу та його обмеження [2, 7], пов'язані з якістю сигналів ризикових подій, необхідністю калібрування порогів і вагових коефіцієнтів, а також компромісом між посиленням безпеки та зручністю користувача в корпоративних середовищах.

Незважаючи на активний розвиток технологій керування ідентичностями та доступом, проблема ефективної авторизації в корпоративних інформаційних системах залишається частково невирішеною [1, 5]. Більшість наявних рішень зосереджені на посиленні автентифікації користувачів або розширенні політик доступу, тоді як процес авторизації та керування життєвим циклом токенів доступу часто реалізується за ста-

тичними правилами [10, 12-13]. У результаті системи виявляються недостатньо чутливими до змін контексту, поведінкових аномалій і поточного рівня ризику, що створює умови для тривалого зловживання скомпрометованими сесіями.

Аналіз наукових і практичних підходів показує, що в межах концепції Zero Trust відсутнє єдине формалізоване рішення, яке б інтегрувало оцінювання рівня довіри, ризику операції та керування параметрами сесії в узгоджений механізм ухвалення рішень [2, 10, 19]. Зокрема, залишаються невирішеними такі питання: яким чином кількісно враховувати динамічну зміну довіри до користувача або сервісу під час активної сесії [15, 18]; як поєднати цю оцінку з ризиками конкретної операції та чутливістю активу [4, 13]; як на основі отриманих показників адаптивно змінювати параметри авторизації без надмірного впливу на зручність користувачів і продуктивність системи.

Окремою проблемою є керування часом життя токенів доступу, який у більшості реалізацій визначається наперед і не змінюється у відповідь на ризикові події [10]. Такий підхід не дозволяє оперативно скорочувати «вікно атаки» у разі компрометації облікових даних, викрадення токенів або виявлення аномальної поведінки. Водночас відсутність формалізованих правил адаптивного керування токенами ускладнює оцінювання ефективності запропонованих рішень і їх порівняння з базовими моделями.

У зв'язку з цим постає науково-практичне завдання розроблення ризик-адаптивної моделі авторизації, яка забезпечує узгоджене використання динамічної оцінки довіри, контекстних і поведінкових ризиків та механізмів керування токенами доступу [2, 15, 18]. Така модель має бути формалізованою, придатною для реалізації в системах IAM/PAM та дозволяти кількісно оцінювати її вплив на зменшення потенційного вікна атаки й експлуатаційні характеристики авторизації в умовах Zero Trust.

Модель загроз охоплює атаки, пов'язані з компрометацією токенів доступу та зловживанням сесіями (token theft, session hijacking, повторне використання токена після первинної автентифікації), а також підвищення ризику через контекстні та поведінкові аномалії (нестандартна геолокація, зміна пристрою/мережі, нетипова частота запитів). Припускається наявність джерел телеметрії UEBA/SIEM/IdP/EDR/NAC і можливість анулювання/обмеження сесії протягом інтервалу Δt [8, 16, 20-21]. Поза межами розгляду залишаються сценарії повної компрометації IdP/PDP або відсутності достовірної телеметрії (наприклад, повний контроль зловмисника над endpoint без детектування).

Аналіз існуючих досліджень

У сучасних наукових дослідженнях значна увага приділяється розвитку систем керування ідентичностями та доступом (IAM) і впровадженню архітектури Zero Trust у корпоративних інформаційних системах. У роботах J. Glöckler, J. Sedlmeir, M. Frank та G. Fridgen узагальнено вимоги підприємств до IAM, зокрема, щодо керування життєвим циклом ідентичностей, узгодженості атрибутів, аудиту доступу та зменшення ризиків зловживання привілеями [1]. Автори переконливо показують, що сучасні корпоративні системи потребують більш гнучких і контекстно-орієнтованих механізмів доступу. Водночас запропонований у роботі аналіз має переважно концептуальний характер і не пропонує формалізованого механізму авторизації, який би безпосередньо пов'язував динамічні показники довіри та ризику з параметрами активної сесії й часом життя токенів доступу. У виправленнях і доповненнях до цього огляду [3] уточнюється методологічна коректність систематизації вимог, однак прикладна проблема адаптивного керування авторизаційними сесіями залишається поза межами розгляду.

Дослідження A. Aljohani зосереджене на практичних аспектах реалізації Zero Trust у сучасних корпоративних мережах, де кожен запит доступу розглядається як потенційно небезпечний [2]. Робота демонструє ефективність безперервної перевірки ідентичності та контексту, однак авторизація в більшості сценаріїв реалізується як статичне або напівстатичне рі-

шення на рівні політик доступу. Питання динамічного коригування параметрів сесії після надання доступу, зокрема, часу життя токенів у відповідь на зміну ризику, не отримує достатнього розвитку.

Окрему групу становлять роботи, присвячені формальним моделям доступу. Так M. U. Aftab та співавтори пропонують динамічну RBAC-модель із permission-based separation of duty, спрямовану на зменшення ризиків зловживання повноваженнями [4]. Запропонована модель суттєво підвищує контроль над призначенням ролей і дозволів, однак вона не враховує сценаріїв компрометації вже виданих токенів або активних сесій, що є типовими для сучасних атак на ідентичності.

У контексті хмарних і розподілених середовищ V. Yadav, M. K. Soni та A. Pratap розглядають захищене IAM у хмарних обчисленнях на основі Zero Trust [5]. Автори підкреслюють важливість урахування контексту доступу та чутливості ресурсів, проте запропоновані підходи зосереджені переважно на етапі ухвалення первинного рішення про доступ. Керування життєвим циклом токенів доступу впродовж активної сесії залишається статичним або прив'язаним до наперед визначених профілів ресурсів, що обмежує здатність системи оперативно реагувати на компрометацію токенів чи поведінкові аномалії.

Аналогічні обмеження простежуються у роботі H. Sivaraman, присвяченій Zero Trust IAM у multi-cloud середовищах [6]. Автор детально аналізує проблеми уніфікації політик ідентичностей і доступу між різними хмарними платформами та наголошує на необхідності безперервної оцінки доступу. Водночас у дослідженні не запропоновано формалізованого алгоритму, який би пов'язував результати такої оцінки з адаптивним керуванням параметрами авторизаційних сесій і токенів.

У роботі S. Ahmadi розглянуто застосування Zero Trust у хмарних мережах, а також визначено ключові виклики, пов'язані з масштабованістю, якістю телеметрії та балансом між безпекою і зручністю користувачів [7]. Автор зазначає, що надмірно жорсткі політики можуть негативно впливати на безперервність бізнес-процесів, однак у дослідженні не запропоновано кількісних моделей, які дозволяли б оптимізувати цей компроміс шляхом адаптивного керування часом життя сесій залежно від поточного ризику.

Важливим доповненням до проблематики Zero Trust є дослідження J. Lee та співавторів, у якому запропоновано метод ранжування аномальних активностей у корпоративних мережах [8]. Робота демонструє, як телеметричні дані можуть бути перетворені на числові оцінки аномальності та ризику. Проте результати такого ранжування розглядаються переважно як інструмент для SOC або моніторингу, а не як керуючий сигнал для механізмів авторизації та керування сесіями.

Проведений аналіз наукових публікацій показує, що, незважаючи на активний розвиток концепції Zero Trust і систем IAM, у більшості досліджень авторизація розглядається або як статичне рішення на момент запиту доступу, або як похідна від ролей, атрибутів чи чутливості активів. Питання інтеграції динамічної оцінки довіри, контекстних і поведінкових ризиків та керування параметрами активної сесії в єдиний формалізований контур ухвалення рішень залишається недостатньо вирішеним.

Зокрема, у наявних підходах відсутній узгоджений механізм адаптивного керування часом життя токенів доступу у відповідь на ризикові події, що безпосередньо пов'язано з проблемою мінімізації потенційного «вікна атаки» у разі компрометації сесії. Також бракує кількісних моделей і метрик, які дозволяли б порівнювати ефективність різних підходів до авторизації з точки зору балансу між рівнем безпеки, затримкою ухвалення рішень і зручністю користувачів. У сукупності ці невирішені питання зумовлюють необхідність розроблення ризик-адаптивної моделі авторизації в архітектурі Zero Trust, яка поєднує динамічну довіру, оцінювання ризику та адаптивне керування токенами доступу в одному формалізованому механізмі.

Метою статті є розробка формалізованої ризик-адаптивної моделі авторизації в архітектурі Zero Trust, що поєднує динамічну оцінку рівня довіри до користувачів і сервісів, контекстні та поведінкові фактори

ризику, а також адаптивне керування параметрами сесій і токенів доступу. Запропонований підхід спрямований на зменшення потенційного вікна атак у разі компрометації ідентичностей або токенів, підвищення точності рішень про доступ та забезпечення балансу між рівнем безпеки, продуктивністю системи й зручністю використання в корпоративних інформаційних системах.

Для формалізації проблеми ефективності авторизації доцільно ввести кількісну метрику, що безпосередньо характеризує наслідки компрометації сесій і токенів доступу [10, 12]. Нехай t_c – момент компрометації токена доступу або облікових даних, t_r – момент його відкликання, анулювання або завершення дії. Тоді потенційне вікно атаки визначається як: $W = t_r - t_c$ і характеризує проміжок часу, протягом якого зловмисник може несанкціоновано використовувати скомпрометований доступ [13, 19]. У традиційних моделях авторизації зі статичним часом життя токенів величина W практично еквівалентна заданому значенню TTL, оскільки параметри сесії не змінюються у відповідь на ризикові події [5, 10]. Натомість у ризик-адаптивному підході $TL - TTL$ величина W зменшується за рахунок подієвого коригування часу життя токена, коли виявлення аномальної поведінки, змін контексту або інших ризикових подій призводить до дострокового обмеження або відкликання сесії [12, 18-19]. Таким чином, задача авторизації в умовах Zero Trust формалізується як задача мінімізації потенційного вікна атаки W за умови збереження прийнятних експлуатаційних характеристик системи доступу.

Виклад основного матеріалу дослідження

Методологія дослідження ґрунтується на поєднанні формалізованих моделей керування доступом, ризик-орієнтованих підходів до авторизації та принципів архітектури Zero Trust [2, 10, 12-13, 19]. У межах роботи використано системний підхід до аналізу процесів авторизації в корпоративних інформаційних системах, що дозволяє розглядати керування доступом як динамічний контур ухвалення рішень, залежний від рівня довіри, контексту та поведінки суб'єктів доступу.

Основу дослідження становить формалізація ключових елементів системи Access Management, зокрема множин користувачів, активів і привілеїв, а також відношень доступу між ними. Авторизація розглядається як функція, що відображає атрибути суб'єкта, характеристики ресурсу та поточний контекст безпеки у рішення щодо дозволу, обмеження або заборони доступу. Такий підхід забезпечує можливість інтеграції рольових, атрибутивних і політик-орієнтованих моделей у єдину схему ухвалення рішень.

Для врахування динаміки ризиків у процесі доступу застосовано методи оцінювання довіри та ризику операцій [13, 19]. Рівень довіри до користувача або сервісу визначається на основі сукупності ідентифікаційних, контекстних, пристроєвих і поведінкових факторів та розглядається як змінна величина, що оновлюється впродовж активної сесії [15, 18]. Оцінка ризику операції формується з урахуванням чутливості активів, умов доступу та поточного стану безпеки, що дозволяє адаптувати рішення авторизації до реальних загроз.

Ключовим елементом методології є ризик-адаптивне керування токенами доступу, яке реалізується шляхом динамічного визначення часу їхнього життя залежно від рівня довіри, контексту доступу та критичності ресурсів [5-6, 12]. У дослідженні використано подієвий підхід, за якого виявлення ризикових подій (аномальної поведінки, змін контексту або порушень політик) призводить до коригування параметрів сесії та, за необхідності, ініціювання додаткових перевірок доступу. Це дозволяє мінімізувати потенційне вікно атак без надмірного зниження зручності використання системи.

Джерелом формування ризикових подій у запропонованій методології виступають різнорідні компоненти корпоративної інфраструктури безпеки, зокрема, системи аналізу поведінки користувачів і сутностей (UEBA), системи управління подіями та інцидентами безпеки (SIEM), сервіси керування ідентичностями та доступом (IdP/IAM), засоби захисту кінцевих точок

(EDR), а також механізми мережевого контролю доступу (NAC) [8, 13, 20-21]. Телеметричні дані, що надходять із цих джерел, агрегуються та нормалізуються з метою виявлення подій, які можуть свідчити про зростання ризику доступу, такі як аномальна поведінка, порушення цілісності пристрою, нетипові зміни контексту або спроби зловживання токенами доступу.

Для кожної зафіксованої події формується оцінка серйозності $Sev(RiskEvent)$, яка може визначатися на основі правил (rule-based підхід) або за допомогою моделей машинного навчання у вигляді нормалізованого ризикового скору [8, 16]. Оновлення рівня довіри TL здійснюється динамічно — безпосередньо під час обробки запиту доступу (per-request), періодично з фіксованим інтервалом Δt або асинхронно у відповідь на надходження ризикової події (on-event), залежно від вимог до чутливості та продуктивності системи [12-13, 15]. Узагальнено методологічний конвеєр ризик-адаптивної авторизації можна подати у вигляді послідовності: Telemetry → RiskEvent scoring → TL update → RiskOp evaluation → Decision & TTL update → PEP enforcement, що забезпечує замкнений контур ухвалення рішень, у якому сигнали безпеки безпосередньо впливають на параметри авторизації та керування сесіями в умовах Zero Trust.

Схема на рис. 1 ілюструє архітектуру ризик-адаптивної авторизації в парадигмі Zero Trust, у якій події безпеки з джерел телеметрії (UEBA, SIEM, IdP/IAM, EDR, NAC) агрегуються у формалізований об'єкт RiskEvent та оцінюються за рівнем серйозності. На рівні PDP здійснюється обчислення та оновлення показників динамічної довіри і операційного ризику, на основі яких формується рішення доступу та адаптивно коригується час життя токена (TTL). Рівень PEP забезпечує примусове виконання ухваленого рішення (permit, step-up, deny), а також керування токенами і сесіями (introspection, denylist, revoke, rotation) з одночасним формуванням аудиторських подій. Згенерований аудит повертається до SIEM, утворюючи замкнений контур зворотного зв'язку, що забезпечує безперервну переоцінку довіри та мінімізацію вікна компрометації сесії. Запропонована архітектура забезпечує перехід від статичної моделі авторизації до безперервного контекстно-орієнтованого контролю доступу, у якому параметри безпеки динамічно узгоджуються з поточним рівнем ризику. Такий підхід підвищує стійкість системи до компрометації облікових даних і перехоплення сесій без істотного зростання обчислювального навантаження та збереження прийнятного рівня зручності користування.

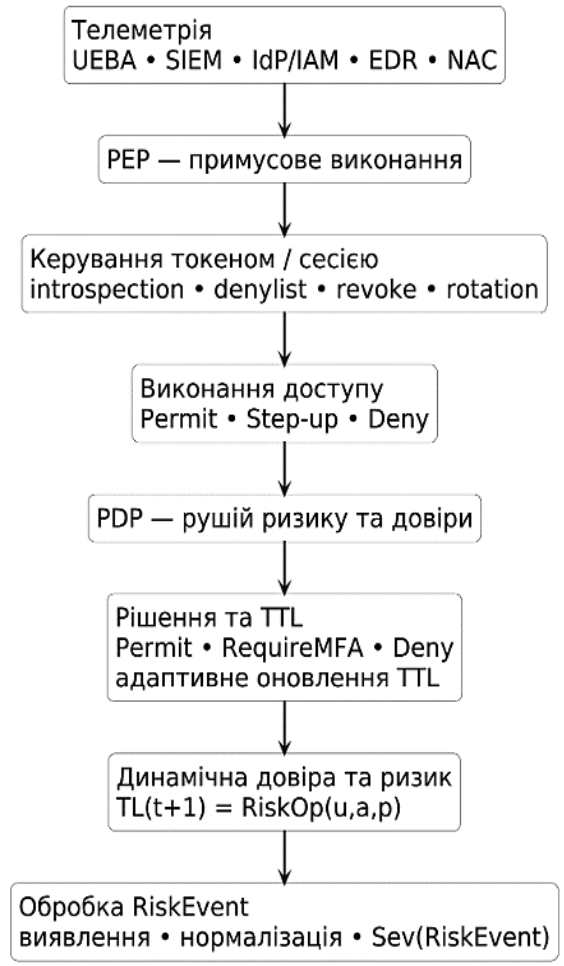

Рис. 1. Архітектура ризик-адаптивної авторизації в Zero Trust (PDP/PEP)

На рис. 2 подано граф подій та керуючих впливів у контурі PDP/PEP архітектури Zero Trust. Після входу користувача та видачі токена зміна контексту доступу (локація, пристрій) ініціює формування $RiskEvent$, для якого обчислюється рівень серйозності $Sev(RiskEvent)$. На основі цієї оцінки PDP ухвалює рішення доступу (*Permit / RequireMFA / Deny*), яке реалізується рівнем PEP через примусове вико-

нання, step-up аутентифікацію або відкликання/ротацію токена. Усі дії журналюються та передаються до SIEM, забезпечуючи кореляцію й збагачення подій, що підкреслює подієву, керовану та пояснювану природу ризик-адаптивної авторизації.

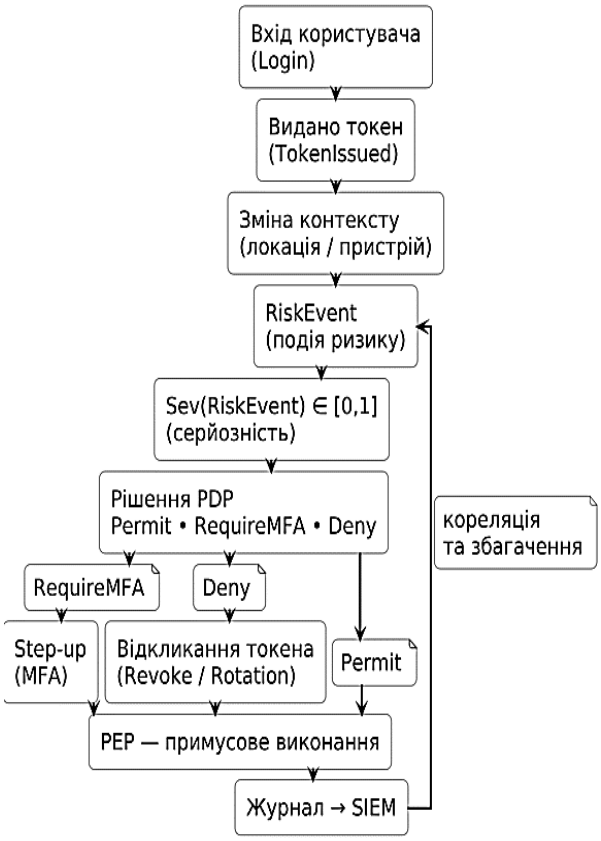

Рис. 2. Граф подій та керуючих впливів RiskEvent у контурі PDP/PEP (Zero Trust)

Оцінювання ефективності запропонованого підходу здійснюється за сценарним принципом із використанням порівняльного аналізу [10, 12-13, 19]. У межах дослідження розглядаються типові сценарії доступу, що включають нормальну роботу, контекстні та поведінкові аномалії, а також компрометацію токенів. Запропонований метод порівнюється з базовими моделями авторизації за показниками тривалості потенційного вікна атаки, частоти додаткових перевірок доступу та експлуатаційних характеристик ухвалення рішень. Такий підхід забезпечує об'єктивну оцінку переваг ризик-адаптивної авторизації в умовах Zero Trust.

Запропонований механізм може бути реалізований у токеноорієнтованих протоколах (OAuth 2.0 / OpenID Connect) через адаптивне керування TTL для access token та політику refresh token з подієвим скороченням строку дії [5-6, 16]. На практиці PDP виконує TL/RiskOp-оцінювання, а PEP застосовує рішення (Permit/RequireMFA/Deny) і параметри токена; ризикові події надходять через SIEM/UEBA або брокер подій, а анулювання може виконуватися через introspection/denylist/rotation залежно від обраної архітектури.

Формальна модель авторизації та довіри. Формалізація процесу авторизації в умовах Zero Trust передбачає опис суб'єктів доступу, ресурсів, привілеїв і контексту безпеки у вигляді взаємопов'язаних множин і функцій, що дозволяє кількісно враховувати довіру та ризик під час ухвалення рішень [13, 19]. На відміну від статичних моделей контролю доступу, запропонований підхід орієнтований на динамічне оновлення параметрів авторизації залежно від поведінки користувача та змін середовища.

Нехай множина користувачів і сервісних суб'єктів доступу корпоративної системи визначається як:

$$U = \{u_1, u_2, \dots, u_m\},$$

де u_j – окремий користувач або сервіс, що ініціює запит на доступ. Кожному суб'єкту відповідає набір атрибутів:

$$Attr(u_j) = \{Role_j, Dept_j, Clearance_j, Device_j, Location_j\},$$

які описують його функціональну роль, рівень повноважень, характеристики пристрою та контекст доступу [1, 13]. У рамках Zero Trust ці атрибути розглядаються як змінні величини, що можуть оновлюватися під час активної сесії.

Множина активів інформаційної системи задається як:

$$A = \{a_1, a_2, \dots, a_n\},$$

де a_i – окремий інформаційний ресурс, сервіс або об'єкт обробки даних [1]. Для кожного активу визначається вектор безпекових характеристик:

$$Attr(a_i) = \{Conf_i, Int_i, Avail_i, Sens_i, Owner_i\},$$

де $Conf_i, Int_i, Avail_i$ відображають вимоги до конфіденційності, цілісності та доступ-

ності, а $Sens_i$ характеризує чутливість активу. На основі цих параметрів формується оцінка ризику активу:

$$Risk(a_i) = f(Conf_i, Int_i, Avail_i, Threats_i, Vuln_i),$$

яка використовується для визначення суворості політик доступу та параметрів авторизації.

Множина дозволених операцій або привілеїв визначається як:

$$P = \{p_1, p_2, \dots, p_k\},$$

де p_k відповідає окремій дії над активом, наприклад, читанню, зміні або адмініструванню. Відношення доступу між користувачами, активами та привілеями описується множиною:

$$Access \subseteq U \times A \times P,$$

причому трійка $(u_j, a_i, p_k) \in Access$ означає, що суб'єкту u_j дозволено виконувати операцію p_k над активом a_i.

Для реалізації політик RBAC, ABAC і PBAC вводяться допоміжні відношення призначення ролей і привілеїв:

$$UA \subseteq U \times Role,\ PA \subseteq Role \times P,$$

У загальному випадку рішення про доступ формується як результат функції авторизації:

$$Decision = PDR(U, A, P, Policies, Context)$$

де $Policies$ – множина формалізованих правил доступу, $Context$ – сукупність параметрів середовища виконання запиту.

Ключовим елементом запропонованої моделі є динамічна оцінка рівня довіри до суб'єкта доступу [13, 19]. Рівень довіри $TL(u_j)$ визначається як зважена агрегація нормалізованих показників ідентичності, стану пристрою, контексту та поведінкових характеристик:

$$TL(u_j) = \sum_{l=1}^{L} w_l \cdot z_l(u_j),\ z_l \in [0,1],$$
$$\sum w_l = 1,$$

де $z_l(u_j)$ – окремі складові оцінки довіри (якість автентифікації, безпечність пристрою, стабільність поведінки), w_l – їхні вагові коефіцієнти. На відміну від статичних моделей, значення TL постійно оновлюється під час сесії відповідно до зафіксованих подій безпеки:

$$TL_{t+1} = clip(0, 1, TL_t - \Delta T(RiskEvent_t)),$$

де $RiskEvent_t$ відображає наявність аномалій або підозрілих дій у момент часу t. Оператор $clip\ (0, 1, \cdot)$ обмежує значення рівня довіри в діапазоні [0,1] і запобігає виходу TL за межі допустимих значень..

Оцінка ризику конкретної операції доступу визначається функцією

$$RiskOp(u_j, a_i, p_k) = \alpha \cdot Risk(a_i) + \beta \cdot \left(1 - TL(u_j)\right) + \gamma \cdot RiskContext,$$

де $RiskContext$ характеризує поточний контекст виконання операції (геолокація, час, тип мережі), а коефіцієнти α, β, γ задають внесок кожного компонента. Така формалізація дозволяє поєднати статичні характеристики активу з динамічною довірою до користувача.

Запропонована модель відрізняється від традиційних підходів тим, що рішення про доступ ухвалюється не лише на основі ролей або атрибутів, а з урахуванням поточного ризику операції та рівня довіри [12-13, 19]. Це створює основу для реалізації ризик-адаптивної авторизації, у межах якої подальше керування токенами доступу та параметрами сесії може бути безпосередньо пов'язане зі значеннями TL і $RiskOp$. Таким чином, формальна модель авторизації та довіри забезпечує математичне підґрунтя для побудови адаптивних Zero Trust-рішень, орієнтованих на мінімізацію вікна атак і підвищення стійкості систем керування доступом.

Запропонований ризик-адаптивний метод керування токенами доступу ($TL - TTL$). Запропонований метод керування токенами доступу ґрунтується на ідеї динамічного коригування параметрів сесії відповідно до поточного рівня довіри та ризику виконуваних операцій [6, 10, 19]. На відміну від традиційних підходів, у яких час життя токена визначається статично або залежить лише від чутливості ресурсу, у межах даного дослідження токен розглядається як адаптивний елемент авторизаційного контуру Zero Trust.

Нехай TTL – час життя токена доступу, що визначає максимальну тривалість дії авторизаційного рішення [12-13]. Запропоновано визначати початкове значення TTL як функцію динамічного рівня довіри до суб'єкта доступу, контекстних ризиків і чутливості активу:

$$TTL = f(TL, RiskContext, Sensitivity),$$

Для практичної реалізації ця залежність може бути задана у вигляді лінійної моделі з обмеженнями:

$$TTL = clip(TTL_{min}, TTL_{max},\ k_1 \cdot TL - k_2 \cdot RiskContext - k_3 \cdot Sensitivity),$$

де TTL_{min} та TTL_{max} – мінімальне і максимальне допустимі значення часу життя токена, $TL \in [0,1]$ – поточний рівень довіри, $RiskContext \in [0,1]$ – оцінка ризику контексту доступу, $Sensitivity \in [0,1]$ – чутливість активу, k_1, k_2, k_3 – коефіцієнти впливу відповідних факторів.

Особливістю запропонованого підходу є підтримка подієвого коригування часу життя токена впродовж активної сесії. У разі фіксації ризикових подій, таких як поведінкові аномалії, зміна геолокації або порушення політик безпеки, здійснюється штрафне зменшення часу життя токена [12-13]:

$$TTL_{t+1} = TTL_t - \Delta t - Penalty(RiskEvent_t),$$

де Δt – час, що минув з моменту попереднього оновлення, $Penalty(RiskEvent_t)$ – штрафна функція, пропорційна серйозності зафіксованої події:

$$Penalty(RiskEvent) = \lambda \cdot Sev(RiskEvent),\ Sev \in [0,1],$$

Отож, навіть за наявності чинного дозволу на доступ токен може бути достроково обмежений або відкликаний у разі зростання ризику, що істотно зменшує потенційне вікно атаки при компрометації сесії.

Запропонований метод інтегрується у стандартну архітектуру PDP/PEP і дозволяє реалізувати ризик-адаптивне керування сесіями без зміни базових механізмів автентифікації. Це забезпечує його сумісність із сучасними системами IAM/PAM та практичну придатність для впровадження в корпоративних інформаційних системах.

Модель ухвалення рішень авторизації. Для формалізації процесу авторизації з урахуванням ризик-адаптивного керування токенами доступу розглянемо модель ухвалення рішень, реалізовану на рівні Policy Decision Point (PDP) з подальшим застосуванням результатів на рівні Policy Enforcement Point (PEP).

Нехай запит доступу описується кортежем [13, 19]:

$$q = \langle u, a, p, ctx, t \rangle,$$

де u – суб'єкт доступу, a – актив, p – операція, ctx – поточний контекст, t – момент часу. На основі цього запиту PDP обчислює рівень довіри $TL(u)$та ризик операції $RiskOp(u, a, p)$.

Рішення авторизації формується як елемент множини [10, 12]:

$Decision \in \{Permit, RequireMFA, Deny\}$,

відповідно до порогових значень довіри та ризику:

$$Decision = \begin{cases} Deny, & TL < T_{deny} \text{ або } RiskOp > R_{max}, \\ RequireMFA, & T_{deny} \le TL < T_{mfa}, \\ Permit, & TL \ge T_{mfa}. \end{cases}$$

де T_{deny} та T_{mfa}– порогові значення рівня довіри, що визначають суворість політики доступу, R_{max} – максимально допустимий ризик операції.

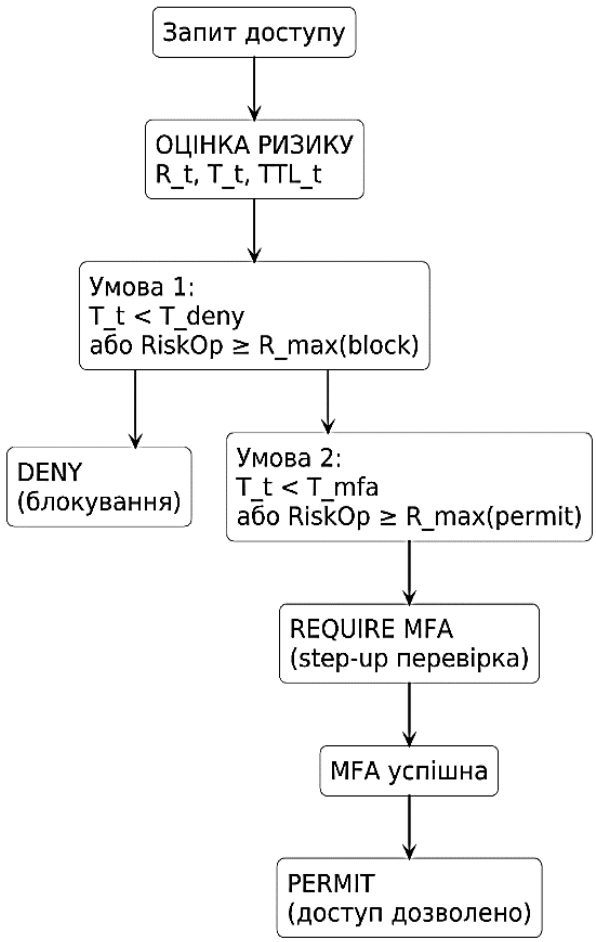

Рис. 3. Діаграма порогових станів і переходів ризик-адаптивної авторизації ($Permit/RequireMFA/Deny$)

На рис. 3 подано діаграму станів ухвалення рішення авторизації в архітектурі

Zero Trust, що реалізує формулу (18) через порогові значення рівня довіри TL та операційного ризику $RiskOp$.

Залежно від співвідношення з порогами $T_{deny}, T_{mfa}, R_{max}$ система переходить у стани $Permit$, $RequireMFA$ або $Deny$, забезпечуючи інтерпретовану та керовану логіку доступу з підтримкою step-up перевірок і блокування.

Параметри моделі (α, β, γ), пороги $(T_{deny}, T_{mfa}, R_{max})$ та коефіцієнти керування токеном (k_1, k_2, k_3, λ) налаштовуються відповідно до політики прийнятного ризику підприємства та історії інцидентів. Практично калібрування може виконуватися як задача мінімізації W за обмежень на експлуатаційні показники: частоту додаткових перевірок $S \leq S_{max}$ і затримку ухвалення рішень $L \leq L_{max}$ [10, 12-14]. Початкові значення параметрів встановлюються експертно (policy-driven), після чого уточнюються на основі журналів доступу та підтверджених інцидентів шляхом підбору, що зменшує W у сценаріях S2–S4 без надмірного зростання S у сценарії S1.

У разі ухвалення рішення Permit або RequireMFA PDP додатково визначає параметри сесії, зокрема оновлене значення часу життя токена TTL_{t+1}, відповідно до запропонованого ризик-адаптивного методу. Отримане рішення разом із параметрами токена передається до PEP, який забезпечує примусове виконання політики доступу, ініціює додаткову автентифікацію або блокує запит.

Таким чином, модель ухвалення рішень авторизації забезпечує тісний зв'язок між оцінкою довіри, ризику та керуванням токенами доступу [13, 15]. Вона слугує перехідною ланкою між формальною моделлю авторизації та практичною реалізацією алгоритму PDP/PEP, створюючи основу для подальшого алгоритмічного опису й експериментального оцінювання ефективності ризик-адаптивної авторизації в умовах Zero Trust.

Алгоритм ризик-адаптивної авторизації $TL - TTL$. Алгоритм ризик-адаптивної авторизації реалізує формалізований процес ухвалення рішень на рівні Policy Decision Point з подальшим примусовим виконанням на рівні Policy Enforcement Point [10, 12, 13]. Його метою є адаптація параметрів авторизації та часу життя токенів доступу до поточного рівня довіри та ризику операцій у межах архітектури Zero Trust.

Вхідними даними алгоритму є запит доступу $q = \langle u, a, p, ctx, t \rangle$, множина політик доступу, поточний рівень довіри $TL_t(u)$, а також параметри порогів і обмежень [13]. Вихідними даними є рішення авторизації та оновлені параметри токена доступу.

Алгоритм ризик-адаптивної авторизації $TL - TTL$ [10, 12-13, 18]:

1. Отримати запит доступу q та зібрати атрибути суб'єкта, активу й контексту.
2. Обчислити поточний рівень довіри $TL(u)$,.
3. Визначити ризик операції $RiskOp = (u, a, p)$.
4. Ухвалити попереднє рішення [11-12]:
   – якщо $TL < T_{deny}$ або $RiskOp > R_{max}$,, то Deny;
   – якщо $T_{deny} \leq TL < T_{mfa}$, то RequireMFA;
   – інакше – Permit.
5. У разі Permit або RequireMFA обчислити базове значення часу життя токена:

$$TTL^{\setminus *} = f(TL, RiskContext, Sensitivity),$$

Якщо зафіксовано ризикову подію, застосувати штрафне коригування:

$$TTL_{t+1} = TTL^{\setminus *} - Penalty(RiskEvent_t), \quad (20)$$

6. Обмежити TTL_{t+1} значеннями TTL_{min} і TTL_{max},.
7. Передати рішення та параметри токена до PEP для виконання.
8. Зареєструвати подію в системі моніторингу безпеки.

Запропонований алгоритм забезпечує безперервну адаптацію параметрів авторизації та дозволяє оперативно реагувати на зміну рівня ризику під час активної сесії.

Сценарії оцінювання та базові моделі. Оцінювання ефективності ризик-адаптивного підходу до авторизації виконується за сценарним методом із порівнянням із базовими моделями доступу [10-13]. Це

дозволяє проаналізувати роботу механізмів авторизації в типових умовах експлуатації як у штатному режимі, так і за підвищених ризиків, з урахуванням загроз компрометації ідентичностей, змін контексту доступу та аномальної поведінки користувачів.

Перший сценарій (S1) відображає нормальний режим доступу, за якого легітимний користувач працює в очікуваному контексті безпеки без фіксації ризикових подій; рівень довіри та параметри авторизації залишаються стабільними. Він використовується як базовий для оцінювання зручності доступу та відсутності надмірних обмежень.

Другий сценарій (S2) моделює контекстну аномалію, спричинену зміною геолокації, типу пристрою або мережевого середовища. У цьому випадку зростає контекстний ризик, що призводить до коригування рівня довіри та перевіряє здатність системи адаптивно реагувати без негайного блокування користувача.

Третій сценарій (S3) пов'язаний із поведінковими аномаліями, такими як нетипова активність або відхилення від звичних шаблонів доступу, і дозволяє оцінити ефективність динамічного зниження довіри та скорочення часу життя токенів у відповідь на ризикові події.

Четвертий сценарій (S4) моделює компрометацію токена під час активної сесії та зосереджується на аналізі вікна атаки, у межах якого зловмисник може зловживати доступом, демонструючи найбільш виразні переваги адаптивного керування часом життя токенів.

Для порівняльного аналізу застосовуються дві базові моделі авторизації: перша використовує статичний час життя токена, незмінний протягом сесії, а друга враховує лише чутливість активу, скорочуючи TTL для критичних ресурсів без урахування динамічних змін довіри та контексту. На відміну від них, запропонований метод поєднує оцінювання рівня довіри та операційного ризику з адаптивним керуванням параметрами токенів доступу.

Оцінювання всіх сценаріїв здійснюється за однакових умов і параметрів доступу, що забезпечує коректність порівняння результатів і дозволяє об'єктивно оцінити вплив запропонованого ризик-адаптивного підходу на безпеку та експлуатаційні характеристики системи авторизації.

Результати та порівняльний аналіз. Оцінювання ефективності запропонованої моделі здійснюється за сценарним підходом (S1–S4), визначеним у розділі методики, із фіксацією середніх значень показників за серією експериментальних запусків. Для кожного сценарію вимірювалися: потенційне вікно атаки W, частота step-up перевірок, затримка ухвалення рішень τ_{dec} та частка необґрунтованих блокувань. Кожен сценарій моделювався не менше, ніж у 30 незалежних ітераціях із фіксацією середніх значень показників.

Обчислювальна складність PDP-оцінювання визначається структурою моделі довіри. Обчислення інтегрального показника TL здійснюється як агрегація L ознак, що зумовлює лінійну складність $O(L)$. Операції обчислення RiskOp та оновлення TTL виконуються за фіксованої кількості параметрів і мають константну складність $O(1)$ [9, 13]. Основний внесок у затримку ухвалення рішення L формують операції отримання контекстних атрибутів і телеметрії (IdP, EDR, NAC), тоді як власне обчислення TL і TTL характеризується незначними накладними витратами.

Результати аналізу підтвердили, що запропонований ризик-адаптивний підхід із динамічним рівнем довіри та керуванням часом життя токенів суттєво підвищує безпеку порівняно з базовими моделями, з найбільшим ефектом у сценаріях компрометації токенів і появи поведінкових або контекстних аномалій.

У сценаріях нормальної роботи (S1) запропонований підхід не призводить до істотного погіршення експлуатаційних характеристик, забезпечуючи затримку PDP/PEP у межах допустимих значень та низьку частоту додаткових перевірок доступу. Водночас у сценаріях підвищеного ризику (S2–S4) динамічне керування часом життя токенів забезпечує суттєве скорочення потенційного вікна атаки – на 75–85 % відносно базової моделі A зі статичним TTL для контекстних і поведінкових аномалій, а в десятки разів у сценарії компроме-

тації токена (S4). Такий ефект досягається за рахунок контрольованого зростання частоти step-up перевірок та помірного збільшення затримки прийняття рішень, що узгоджується з принципами Zero Trust і не порушує безперервність бізнес-процесів. Варіація затримки ухвалення рішень у межах сценаріїв не перевищувала 5–8 %, що свідчить про стабільність роботи моделі за умов зміни контекстних параметрів.

У табл. 1 узагальнено результати порівняльного аналізу, які підтверджують, що запропонований підхід дозволяє зменшити потенційне вікно атак і підвищити адаптивність авторизації без істотного погіршення експлуатаційних характеристик.

Таблиця 1.

Порівняльні результати оцінювання моделей авторизації

Критерій	Базова модель A (статичний TTL токена)	Базова модель B (TTL за чутливістю активу)	Запропонований метод
Потенційне вікно атаки W	$\approx TTL$ (8 год)	↓ ~2×	↓ 10–90×
Реакція на ризикові події	Відсутня	Обмежена	Подієва, динамічна
Частота step-up перевірок	1–3 %	3–6 %	2–15 % (адапт.)
Ймовірність необґрунтованих блокувань	Висока	Середня	Низька
Затримка прийняття рішень τ_{dec}	8–10 мс	10–14 мс	12–25 мс

Показники, наведені в таблиці 1, отримані на основі сценарного моделювання з фіксованими параметрами TTL=8 год для моделі A та диференційованими значеннями TTL за рівнем чутливості активу для моделі B. Для запропонованого методу TTL змінювався адаптивно відповідно до рівня RiskOp і TL.

Як видно з рис. 4, у сценаріях S2–S4 спостерігається нелінійне скорочення W, що зумовлено раннім спрацюванням механізму адаптивного зменшення TTL. У сценарії S4 (компрометація токена) різниця між моделлю A та запропонованим методом є максимальною, що підтверджує ефективність реактивного коригування параметрів сесії.

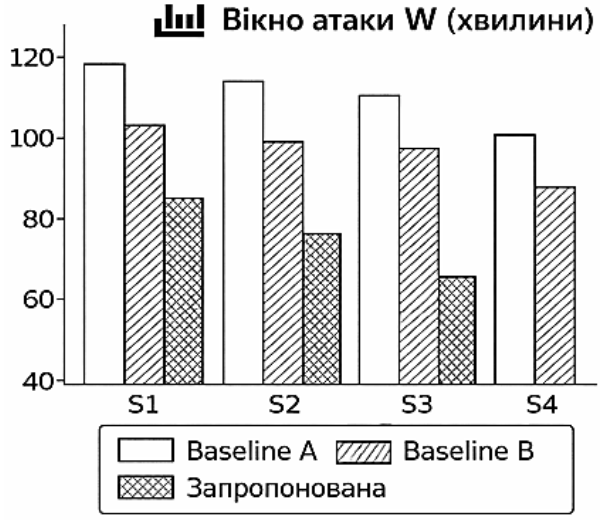

Рис. 4. Порівняльний графік вікна атаки W за сценаріями S1–S4 для Базової моделі A (статичний TTL токена), Базової моделі B (TTL за чутливістю активу) та запропонованого методу.

У випадку використання базової моделі A, що передбачає статичний час життя токена, зловмисник у разі компрометації зберігає можливість доступу до ресурсу протягом усього періоду дії сесії. Це формує значне потенційне вікно атаки, яке не скорочується навіть за наявності додаткових ознак ризику. На відміну від цього, у запропонованому методі час життя токена автоматично коригується у відповідь на зафіксовані ризикові події, що приводить до швидкого обмеження або припинення доступу. Таким чином тривалість потенційного зловживання скомпрометованими обліковими даними суттєво зменшується.

Порівняння з базовою моделлю B, у якій час життя токена визначається виключно чутливістю активу, показало, що такий підхід є недостатньо гнучким у динамічних середовищах. Хоча він дозволяє частково обмежити ризики для критичних ресурсів, відсутність урахування поточного рівня довіри та поведінкових характеристик користувача призводить або до надмірно жорстких обмежень, або до запізнілої реакції на

реальні загрози [11, 13, 18]. Включення динамічної оцінки довіри у запропонованому методі дозволяє більш точно адаптувати параметри авторизації до конкретної ситуації доступу, зменшуючи кількість необґрунтованих блокувань легітимних користувачів і водночас підвищуючи стійкість системи до атак.

Аналіз експлуатаційних характеристик показав, що ризик-адаптивне керування токенами не спричиняє істотного зростання кількості додаткових перевірок доступу: step-up authentication активується переважно у сценаріях підвищеного ризику та залишається мінімальною за нормальної поведінки користувачів [9, 12-14]. Затримки ухвалення рішень у точках реалізації політик не перевищують допустимих меж і не впливають на загальну продуктивність системи.

Отримані результати підтверджують, що ризик-адаптивна авторизація забезпечує перехід від статичної політики $\boldsymbol{TTL}$ до подієво-керованого механізму контролю доступу, в якому параметри сесії безперервно узгоджуються з поточним рівнем довіри та ризику. Це формує формалізований зв'язок між метрикою $\boldsymbol{W}$, динамічною оцінкою $\boldsymbol{TL}$ та механізмом керування токенами, що забезпечує контрольоване зменшення експозиції до атак без непропорційного зростання обчислювальних та експлуатаційних витрат.

Обговорення результатів

Отримані результати демонструють, що перехід від статичних моделей авторизації до ризик-адаптивного керування токенами суттєво підвищує стійкість систем керування доступом (Access Management) до загроз, пов'язаних із компрометацією ідентичностей і сесійних токенів. На відміну від базових підходів із незмінними параметрами доступу протягом усього життєвого циклу сесії, запропонований метод забезпечує зменшення потенційного вікна атаки завдяки динамічному скороченню часу життя токена у відповідь на ризикові події.

У таблиці 2 узагальнено вплив запропонованого підходу на ключові експлуатаційні характеристики системи доступу. Результати підтверджують, що підвищення рівня безпеки досягається без непропорційного зростання обчислювальних витрат і без порушення стабільності роботи сервісів.

Таблиця 2.

Вплив ризик-адаптивної авторизації на експлуатаційні характеристики

Параметр	Тенденція зміни	Практичний ефект
Рівень безпеки	Зростає	Підвищення стійкості до атак
Вікно атаки W	Зменшується	Скорочення часу потенційного зловживання
Частота перевірок доступу	Зростає локально (у S2–S4)	Контрольована адаптація до ризику
Затримка PDP/PEP	Незначне зростання	Придатність до реального використання

Важливо зазначити, що скорочення вікна атаки W має нелінійний характер і прямо залежить від чутливості системи до змін рівня довіри TL. У сценаріях із різкими поведінковими відхиленнями раннє спрацювання механізму адаптивного зменшення TTL забезпечує швидке обмеження сесії, що мінімізує часову експозицію до атак навіть за наявності дійсного токена доступу.

З точки зору системного аналізу запропонований підхід реалізує замкнутий керуючий контур, у якому телеметрія RiskEvent виступає вхідним сигналом, модель довіри TL – регулятором, а час життя токена TTL – керованою змінною. Така інтерпретація дозволяє розглядати процес авторизації як динамічну систему зі зворотним зв'язком, де стабільність визначається балансом між швидкістю реакції на ризик і допустимими коливаннями частоти step-up перевірок. Це створює підґрунтя для подальшої формалізації моделі засобами теорії керування та оптимізації параметрів політики доступу.

Включення динамічного рівня довіри як керуючого параметра авторизації дає змогу точніше відображати поточний стан безпеки та поведінкові характеристики користувача. На відміну від підходів, що враховують лише чутливість активів, запропонований метод забезпечує гнучке коригування доступу залежно від контексту, зменшуючи кількість необґрунтованих блокувань і водночас підвищуючи швидкість реакції на аномальні сценарії, що є критичним для динамічних корпоративних середовищ.

З експлуатаційної точки зору додаткові перевірки активуються переважно у сценаріях підвищеного ризику та не впливають на нормальний режим роботи. Затримки у PDP та PEP залишаються в допустимих межах, що підтверджує практичну придатність моделі для впровадження в системах реального часу. Тож, підхід забезпечує баланс між підвищенням безпеки та зручністю використання відповідно до принципів Zero Trust.

Практичне значення запропонованого підходу полягає у можливості інтеграції механізму адаптивного TTL у наявні IAM/IdP-рішення без зміни архітектури автентифікації. Модель може бути реалізована як надбудова на рівні PDP, що мінімізує витрати на впровадження та забезпечує масштабованість у хмарних і гібридних середовищах.

Отримані результати підтверджують гіпотезу про те, що інтеграція динамічної довіри в механізм керування токенами створює формалізований зв'язок між контекстом доступу, ризиком і тривалістю сесії, перетворюючи TTL із статичного параметра на керовану змінну безпеки.

На відміну від більшості існуючих Zero Trust реалізацій, де механізм авторизації залишається логічно відокремленим від керування криптографічними або сесійними параметрами, запропонований підхід інтегрує ризикову оцінку безпосередньо в механізм управління життєвим циклом токена. Це усуває розрив між політичним рішенням доступу та фактичною тривалістю дії сесії, формуючи єдину адаптивну модель контролю доступу. Така інтеграція забезпечує не лише реактивне, а й превентивне обмеження експозиції до атак.

Обмеження методу пов'язані з якістю та затримками телеметрії RiskEvent: хибнопозитивні події можуть призводити до надмірної активації step-up перевірок, тоді як хибнонегативні події можуть призводити до збереження надмірного TTL та збільшення часової експозиції до атак. Крім того, у розподілених середовищах критичним є коректний вибір часових параметрів (Δt) та калібрування порогів і ваг моделі довіри, оскільки їх некоректне налаштування може спричинити або надмірно жорстку, або занадто лояльну політику доступу.

Подальші дослідження можуть бути спрямовані на використання адаптивних методів машинного навчання для автоматичного калібрування порогів TL і RiskOp, а також на формалізацію метрики оптимального балансу між частотою step-up перевірок і скороченням вікна атаки W. Окремого аналізу потребує вплив затримок телеметрії у мультихмарних і розподілених архітектурах.

Висновки

У роботі запропоновано ризик-адаптивний підхід до авторизації в архітектурі Zero Trust, що базується на динамічній оцінці рівня довіри та керуванні часом життя токенів доступу. Розроблена модель дозволяє перейти від статичних механізмів контролю доступу до адаптивної авторизації, у якій параметри доступу коригуються залежно від поточного рівня ризику та поведінки користувача.

Результати аналізу показали, що застосування динамічного керування токенами приводить до зменшення потенційного вікна атак у сценаріях компрометації токенів і поведінкових аномалій. Порівняно з базовими моделями запропонований метод забезпечує більш точну реакцію на ризикові події, обмежує час зловживання доступом і водночас знижує ймовірність необґрунтованих відмов у доступі для легітимних користувачів. Частота ініціювання додаткових перевірок доступу зростає контрольовано та не призводить до істотного

погіршення експлуатаційних характеристик системи.

Практична значущість отриманих результатів полягає в можливості використання запропонованого підходу як механізму реалізації принципів Zero Trust у корпоративних інформаційних системах без радикальної перебудови існуючої IAM/PAM-інфраструктури. Метод може бути інтегрований у сучасні системи авторизації, що використовують токеноорієнтовані протоколи, та адаптований до різних профілів ризику підприємства.

Подальші дослідження доцільно спрямувати на розширення набору сценаріїв оцінювання з урахуванням складних багатокрокових атак, інтеграцію запропонованої моделі з системами UEBA та SIEM для автоматизованого формування ризикових подій, а також на кількісну оцінку ефективності підходу в реальних виробничих середовищах. Окремий інтерес становить дослідження методів автоматичного налаштування порогових значень рівня довіри та параметрів керування токенами з урахуванням політики прийнятного ризику організації.

Література

1. Glöckler J., Sedlmeir J., Frank M., Fridgen G. A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity // Business & Information Systems Engineering. 2024. Vol. 66. P. 421–440. DOI: https://doi.org/10.1007/s12599-023-00830-x
2. Aljohani A. Zero-trust architecture: Implementing and evaluating security measures in modern enterprise networks // SHIFRA. 2023. P. 1–13. DOI: https://doi.org/10.70470/SHIFRA/2023/008
3. Glöckler J., Sedlmeir J., Frank M., Fridgen G. Publisher correction: A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity // Business & Information Systems Engineering. 2023. DOI: https://doi.org/10.1007/s12599-023-00838-3
4. Aftab M. U., Qin Z., Hundera N. W., Ariyo O., Zakria Z., Son N. T., Dinh T. V. Permission-based separation of duty in dynamic role-based access control model // Symmetry. 2019. Vol. 11, no. 5. Art. 669. DOI: https://doi.org/10.3390/sym11050669
5. Yadav V., Soni M. K., Pratap A. Secured identity and access management for cloud computing using zero trust architecture // Cryptology and Network Security with Machine Learning (ICCNSML 2023). Lecture Notes in Networks and Systems. Vol. 918 / Eds. A. Chaturvedi et al. Springer, 2024. DOI: https://doi.org/10.1007/978-981-97-0641-9_47
6. 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
7. Ahmadi S. Zero trust architecture in cloud networks: Application, challenges and future opportunities // Journal of Engineering Research and Reports. 2024. Vol. 26, no. 2. P. 215–228. DOI: https://doi.org/10.9734/jerr/2024/v26i21083
8. Lee J., Tang F., Thet P. M., Yeoh D., Rybczynski M., Mon Divakaran D. SIERRA: Ranking anomalous activities in enterprise networks. arXiv preprint, 2022. DOI: https://doi.org/10.48550/arXiv.2203.16802
9. Kostiuk Y., Rzaieva S., Khorolska K., Mazur N., Korshun N. Architecture of the software system of confidential access to information resources of computer networks // Proceedings of the Workshop Cyber Security and Data Protection (CSDP 2025). Vol. 4042. CEUR-WS, 2025. P. 37–53.
10. Teerakanok S., Uehara T., Inomata A. Migrating to zero trust architecture: Reviews and challenges // Security and Communication Networks. 2021. Art. 9947347. DOI: https://doi.org/10.1155/2021/9947347
11. Костюк Ю., Бебешко Б., Крючкова Л., Литвинов В., Оксанич І., Складанний П., Хорольська К. Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами // Кібербезпека: освіта, наука, техніка. 2024. № 1(25). С. 229–252. DOI: https://doi.org/10.28925/2663-4023.2024.25.229252
12. Phiayura P., Teerakanok S. A comprehensive framework for migrating to zero trust architecture // IEEE Access. 2023. Vol. 11. P. 19487–19511. DOI: https://doi.org/10.1109/ACCESS.2023.3248622
13. Syed N. F., Shah S. W., Shaghaghi A., Anwar A., Baig Z., Doss R. Zero trust architecture (ZTA): A comprehensive survey // IEEE Access. 2022. Vol. 10. P. 57143–57179. DOI: https://doi.org/10.1109/ACCESS.2022.3174679

14. Складанний П., Костюк Ю., Рзаєва С., Мазур Н. Паралельна обробка даних у розширюваних хеш-структурах та оцінка їх продуктивності // Кібербезпека: освіта, наука, техніка. 2025. № 3(31). С. 242–269. DOI: https://doi.org/10.28925/2663-4023.2025.31.1015
15. Amanlou S., Doss R., Li J. Implementing a dynamic and context-aware trust evaluation model for zero trust architecture (ZTA): A fuzzy logic approach // Proceedings of the 2025 International Wireless Communications and Mobile Computing (IWCMC). IEEE, 2025. P. 404–411. DOI: https://doi.org/10.1109/IWCMC65282.2025.11059668
16. Muhammad A. R., Sukarno P., Wardana A. A. Integrated security information and event management (SIEM) with intrusion detection system (IDS) for live analysis based on machine learning // Procedia Computer Science. 2023. Vol. 217. P. 1406–1415. DOI: https://doi.org/10.1016/j.procs.2022.12.269
17. Костюк Ю., Складанний П., Рзаєва С., Самойленко Ю., Коршун Н. Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid // Кібербезпека: освіта, наука, техніка. 2025. № 2(30). С. 125–156. DOI: https://doi.org/10.28925/2663-4023.2025.30.956
18. P. S. N., Pimpalkar A., Shelke N., Bahadur Saini D. K. J. Zero trust architectures empowered by AI: A paradigm shift in cloud and edge cybersecurity // Proceedings of the 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS 2025). IEEE, 2025. P. 328–335. DOI: https://doi.org/10.1109/ICSCDS65426.2025.11166875
19. He Y., Huang D., Chen L., Ni Y., Ma X. A survey on zero trust architecture: Challenges and future trends // Wireless Communications and Mobile Computing. 2022. Art. 6476274.
20. Цирканюк Д., Соколов В. Методика розслідування інцидентів інформаційної безпеки // Кібербезпека: освіта, наука, техніка. 2024. № 2(26). С. 140–154. DOI: https://doi.org/10.28925/2663-4023.2024.26.675
21. Kostiuk, Y., Skladannyi, P., Sokolov, V., Rzaieva S., Khorolska, K. Machine learning methods for detecting intrusions based on network traffic analysis. Proceedings of the Cybersecurity // Providing in Information and Telecommunication Systems II (CPITS-II 2025), October 26, 2025, Kyiv, Ukraine, Vol-4145, P. 72-94. ISSN 1613-0073

Дата першого надходження до видання: 12.02.2026
Внутрішня рецензія отримана: 19.02.2026
Зовнішня рецензія отримана: 01.03.2026
Дата прийняття статті до друку: 19.03.2026
Дата публікації: 16.04.2026

Про авторів:

[1] Костюк Юлія Володимирівна,
PhD in Computer Science
[1] Kostiuk Julia,
PhD in computer science
http://orcid.org/0000-0001-5423-0985

[1] Складанний Павло Миколайович,
к.т.н., доцент
[2] Skladannyi Pavlo,
Ph.D (technical sciences), associate professor
http://orcid.org/0000-0002-9457-7454.

[2] Гнатченко Дмитро Дмитрович,
PhD in Computer Science
[1] Hnatchenko Dmytro,
PhD in computer science
http://orcid.org/0000-0002-7775-6039.

Місце роботи авторів:

[1] Київський столичний університет
імені Бориса Грінченка
[1] Borys Grinchenko
Kyiv Metropolitan University
тел. +38-044-272-19-02
E-mail: kubg@kubg.edu.ua
Сайт: https://kubg.edu.ua/

[2] Державний торговельно-економічний
Університет
[2] State University of Trade and Economics
тел. +38-044-531-49-84
E-mail: knute@knute.edu.ua
Сайт: https://knute.edu.ua/