P-ISSN 2411-1031, E-ISSN 2518-1033
Information Technology and Security. January-June 2026. Vol. 14. Iss. 1 (26)

DOI 10.20535/2411-1031.2026.14.1.365482
УДК 004.056.5:004.7

ПАВЛО СКЛАДАННИЙ,
ЮЛІЯ КОСТЮК

МАТЕМАТИЧНА МОДЕЛЬ БЕЗПЕРЕРВНОЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ДИНАМІЧНОЇ ДОВІРИ В АРХІТЕКТУРІ ZERO TRUST (ZTNA)

У статті запропоновано формалізовану математичну модель безперервної аутентифікації в архітектурі Zero Trust Network Access (ZTNA), актуальну для умов віддаленого доступу, хмарних сервісів і мобільних пристроїв, де одноразова перевірка під час входу не гарантує безпеки сесії. Безперервну аутентифікацію подано як керований процес динамічного оцінювання довіри до користувача на основі нормованого багатовимірного вектора ознак, який агрегує параметри ідентичності, стану пристрою, мережевого контексту та поведінкових сигналів із типових джерел, зокрема IdP/IAM, EDR/MDM, мережної телеметрії та систем SIEM/UEBA. Рівень довіри інтерпретовано як кількісну імовірнісну величину, придатну для автоматизованого прийняття рішень у Policy Engine, та обчислено за інтерпретованою логістичною моделлю з вагами впливу ознак. Запропоновано механізм часової деградації довіри, який відображає зниження гарантій безпеки за відсутності підтверджуючих подій і визначає жорсткість політики перевірок у межах сесії доступу. Для врахування нетипової або потенційно ризикованої поведінки введено механізм поведінкової корекції довіри на основі коефіцієнта ризику та параметра чутливості, що забезпечує ранню реакцію системи на внутрішні загрози або компрометацію облікових даних. На основі скоригованого рівня довіри сформовано адаптивну порогову політику керування доступом з урахуванням чутливості інформаційних ресурсів, яка реалізує режими ALLOW, STEP-UP та DENY і забезпечує виконання рішень на рівні Policy Enforcement Point. Для балансування рівня безпеки та зручності користувача введено функціонал втрат, що враховує вартість інцидентів і фрикцію додаткової перевірки та дозволяє оптимізувати параметри політики доступу. Отримані результати підтверджують прикладну придатність запропонованої моделі для інтерпретованого й адаптивного керування доступом у ZTNA та створюють основу для її подальшого розвитку в корпоративних і хмарних середовищах.

Ключові слова: безперервна автентифікація, Zero Trust Network Access, динамічна довіра, керування доступом, поведінковий ризик, адаптивні пороги, політика безпеки, архітектура ZTNA.

Постановка проблеми. Сучасні інформаційні системи функціонують в умовах зростання кількості цілеспрямованих атак, компрометації облікових даних та динамічної зміни контексту доступу користувачів. Традиційні підходи до автентифікації, що ґрунтуються на одноразовій перевірці ідентичності під час входу до системи, не забезпечують належного рівня захисту в умовах віддаленої роботи, використання хмарних сервісів і мобільних пристроїв [1]-[2], [5]-[6]. Навіть за наявності багатофакторної автентифікації компрометація сесії після успішного входу залишається серйозною загрозою для критичних інформаційних ресурсів.

У відповідь на ці виклики широкого поширення набула архітектура Zero Trust Network Access (ZTNA), яка базується на принципі безперервної перевірки користувача, пристрою та контексту доступу протягом усього часу взаємодії з ресурсом. Ключовою ідеєю Zero Trust є відмова від статичної моделі довіри на користь динамічної оцінки ризику, за якої рішення про

доступ приймається не одноразово, а повторно з урахуванням поточного стану середовища та поведінки користувача [3]-[5], [11]. У такій парадигмі автентифікація перетворюється на процес керування ризиками, а не лише на механізм підтвердження облікових даних.

Центральним елементом безперервної автентифікації в архітектурі Zero Trust є поняття довіри до користувача, яке формується на основі сукупності контекстних, поведінкових і технічних параметрів [1], [6], [9]. Рівень довіри повинен бути кількісно вимірюваним, інтерпретованим та придатним для автоматизованого використання в механізмах прийняття рішень [4], [7]-[8]. Разом з тим, у багатьох існуючих реалізаціях Zero Trust оцінка довіри має евристичний характер або реалізується у вигляді набору правил, що ускладнює аналіз властивостей системи, налаштування політик доступу та обґрунтування порогових значень. Тому доцільним є застосування формалізованої кількісної моделі довіри, яка забезпечує прозоре прийняття рішень і адаптивне керування доступом у межах політик Zero Trust у динамічних умовах експлуатації.

У цьому контексті актуальним є розроблення формалізованої математичної моделі динамічної довіри користувача, яка дозволяє описати безперервну автентифікацію як керований процес із чітко визначеними параметрами, порогами та критеріями оптимальності [1], [4]. Така модель має враховувати багатовимірний характер ознак користувача і пристрою, часову деградацію довіри, вплив поведінкових відхилень, а також різну чутливість інформаційних ресурсів до ризику [6]-[7]. Формалізація цих аспектів у вигляді єдиної математичної схеми створює основу для побудови адаптивної політики доступу в межах Zero Trust Architecture.

Аналіз останніх досліджень та публікацій. Сучасні дослідження з кібербезпеки фіксують перехід від периметрових моделей захисту до архітектур, орієнтованих на безперервну оцінку ризику та контексту доступу, зокрема до парадигми Zero Trust. У її межах автентифікація й авторизація розглядаються як динамічні процеси, що супроводжують увесь життєвий цикл взаємодії користувача з ресурсами. Аналіз Zero Trust, поданий Kang та співавт. [1], показує відмову від бінарного трактування довіри на користь її безперервної кількісної оцінки з урахуванням поведінкових і контекстних факторів, що створює передумови для математичного опису довіри як керованої величини.

У роботах Lund та співавторів [2] підкреслюється роль безперервної автентифікації та контекстно залежного контролю доступу, однак оцінка довіри часто залишається описовою й не формалізованою, що ускладнює аналіз і оптимізацію політик доступу. Критичний аналіз Zero Trust, запропонований Fernández та Brazhuk [3], наголошує на необхідності формального зв’язку між архітектурними принципами та конкретними механізмами ухвалення рішень, що вимагає чітко визначених змінних і правил переходу.

Trust-based підхід до динамічного керування доступом розглянуто Wang та співавторами [4], де показано неефективність статичних правил у змінному контексті та доцільність використання кількісної оцінки довіри. Водночас питання часової деградації довіри, поведінкового коригування та оптимізації порогів доступу залишаються відкритими. Порівняльний аналіз моделей Zero Trust Network Model, виконаний Dhiman та співавторами [5], підтверджує, що більшість підходів обмежується архітектурними аспектами й евристичними шкалами довіри, що підсилює потребу у формалізованих математичних моделях.

Дослідження Zero Trust у гетерогенних середовищах, зокрема IoT, показують необхідність урахування ідентичності, стану пристрою, мережевого контексту та поведінки користувача [6]-[7]. Інтеграція Zero Trust з керуванням ідентичністю, запропонована Avirneni [8], додатково обґрунтовує доцільність трактування довіри як керуючого параметра Policy Engine.

Узагальнення робіт [1]-[8] свідчить, що, попри значну увагу до концептуальних і архітектурних аспектів Zero Trust, строгій формалізації безперервної автентифікації, динаміки

довіри та оптимізації порогів доступу приділяється недостатньо уваги. Це формує науковий розрив між принципами Zero Trust і їх формалізованою реалізацією, усунення якого шляхом побудови цілісної математичної моделі безперервної автентифікації визначає актуальність даного дослідження.

Метою даної статті є розроблення формалізованої математичної моделі безперервної автентифікації на основі динамічної довіри користувача в архітектурі Zero Trust Network Access, яка забезпечує кількісну оцінку рівня довіри, його адаптивне оновлення в часі та автоматизоване прийняття рішень щодо доступу до інформаційних ресурсів з урахуванням контексту доступу, поведінки користувача, технічного стану пристрою та критичності захищуваного ресурсу [1]-[2], [5], [15], [17]. Досягнення поставленої мети передбачає аналіз принципів безперервної автентифікації в межах концепції Zero Trust і визначення вимог до кількісної моделі довіри, здатної відображати динамічний характер взаємодії користувача з інформаційною системою [1], [3]-[4], [6], [8], [11]. У межах дослідження формується багатовимірний нормований вектор ознак, що агрегує параметри ідентичності користувача, стану пристрою та контексту доступу, на основі якого будується математична модель обчислення коефіцієнта довіри з використанням логістичної функції.

Особлива увага приділяється формалізації часової динаміки довіри та механізму її деградації в процесі безперервної автентифікації, що дозволяє враховувати тривалість сесії та необхідність повторної перевірки автентичності [1],-[2], [5]. Для підвищення чутливості моделі до нетипової поведінки користувача розробляється механізм поведінкового коригування довіри на основі коефіцієнта ризику, який відображає ступінь відхилення поточних дій від історичних шаблонів [6], [13], [16]. На основі отриманого значення довіри формується порогова політика керування доступом до ресурсів, яка реалізує адаптивне прийняття рішень у режимах дозволу доступу, додаткової перевірки або відмови з урахуванням чутливості інформаційних ресурсів [4], [7], [17]-[18]. Для забезпечення балансу між рівнем безпеки та зручністю користувача вводиться функціонал втрат, що дозволяє кількісно оцінити наслідки помилкових рішень доступу та обґрунтувати можливість оптимального налаштування параметрів політики автентифікації шляхом мінімізації очікуваних втрат.

Основний матеріал дослідження. У межах дослідження безперервна автентифікація в архітектурі Zero Trust Network Access формалізується як процес динамічного оцінювання довіри до користувача, що базується на сукупності параметрів ідентичності, стану пристрою та контексту доступу [15]. Для цього вводиться нормований багатовимірний вектор ознак:

$$X(u,d,c,t) = [x_1, x_2, ..., x_n],\ x_i \in [0,1], \quad (1)$$

де u – користувач;

d – пристрій;

r – ресурс;

c – контекст доступу (геолокація, мережа, час доби тощо);

t – момент часу, а кожна компонента x_i відображає окремий аспект довіри, зокрема рівень автентичності користувача, цілісність і безпеку пристрою, історичну надійність дій або поведінкові характеристики.

Нормування компонентів в інтервалі [0,1] забезпечує можливість агрегування різнорідних параметрів у єдиній математичній моделі.

Практично компоненти вектора $X(u,d,c,t)$ можуть формуватися на основі даних систем керування ідентичностями (IdP/IAM), засобів контролю стану кінцевих пристроїв (EDR/MDM), мережевих атрибутів (тип мережі, репутація IP, TLS-параметри), а також журналів активності (SIEM/UEBA) [10], [12]. Це забезпечує реалізацію моделі в умовах реальних інформаційно-комунікаційних систем без необхідності введення штучних

показників, оскільки всі групи параметрів відповідають типовим сигналам, що вже використовуються в Zero Trust-підходах.

Рівень довіри до користувача трактується як імовірність того, що поточна сесія доступу є безпечною за заданих умов, і визначається як [11]:

$$T(u,d,c,r,t) = P(safe \mid X(u,d,c,t)), \quad (2)$$

де r – інформаційний ресурс, до якого здійснюється доступ.

Таке трактування дозволяє інтерпретувати довіру не як бінарну характеристику, а як кількісний показник ризику, безпосередньо придатний для використання в механізмах прийняття рішень у Zero Trust-архітектурі.

На рис. 1 наведено архітектурну схему інтеграції запропонованої математичної моделі безперервної автентифікації в контур Zero Trust Network Access. Модель реалізується на рівні Policy Engine та використовує сигнали ідентичності, стану пристрою, мережевого контексту й поведінкових характеристик для формування вектора ознак, обчислення динамічної довіри та прийняття адаптивних рішень доступу.

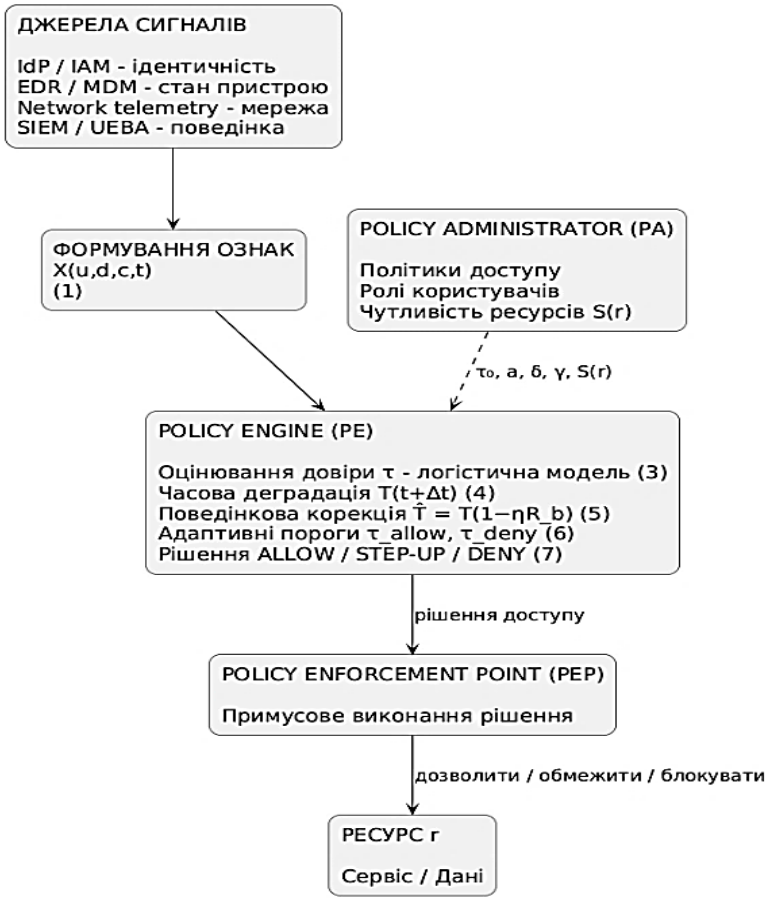

Рисунок 1 – Інтеграція математичної моделі безперервної автентифікації на основі динамічної довіри в контур ZTNA (Policy Engine / Policy Enforcement Point)

Методика застосування запропонованої моделі полягає в послідовному зборі параметрів ідентичності, стану пристрою та контексту доступу з подальшим обчисленням вектора ознак $X(u,d,c,t)$, оцінюванням рівня довіри за логістичною моделлю та його корекцією з урахуванням часової динаміки й поведінкового ризику [13]. Отримане значення довіри використовується Policy Engine для прийняття рішення щодо доступу відповідно до порогової політики, а параметри політики адаптуються шляхом мінімізації функціоналу втрат.

Для практичної реалізації оцінювання довіри використовується логістична модель агрегування параметрів:

$$T = \frac{1}{1+\exp(-(\beta_0 + \sum_{i=1}^{n} \beta_i x_i))}, \quad (3)$$

де β_0 – базовий зсув;

β_i – вагові коефіцієнти впливу відповідних компонентів вектора ознак.

Логістична функція нормує рівень довіри в інтервалі $[0,1]$, забезпечує інтерпретованість внеску окремих параметрів і спрощує інтеграцію оцінювання довіри з адаптивними механізмами прийняття рішень та налаштування порогів доступу в архітектурі Zero Trust.

Оскільки довіра до користувача змінюється в процесі взаємодії з системою, вона моделюється як динамічна величина. Її часову деградацію описує рекурсивна модель:

$$T_{t+\Delta t} = (1-a)T_t + aT_0, \; a = 1 - e^{-\lambda \Delta t}, \quad (4)$$

де T_t – поточне значення довіри;

T_0 – базовий рівень довіри;

λ – коефіцієнт швидкості зниження рівня довіри;

Δt – часовий інтервал між перевірками.

Така форма відображає поступове зниження довіри за відсутності підтверджень, забезпечує безперервну автентифікацію в реальному часі та своєчасну адаптацію рішень доступу до поточного контексту в архітектурі Zero Trust.

На рис. 2 наведено графік часової деградації рівня довіри T_t для різних значень параметра λ, що визначає жорсткість політики безперервної автентифікації в архітектурі Zero Trust [11], [18]. Таким чином, параметр λ виступає регулятором жорсткості політики безперервної автентифікації та дозволяє адаптувати поведінку Policy Engine до критичності ресурсу й профілю загроз.

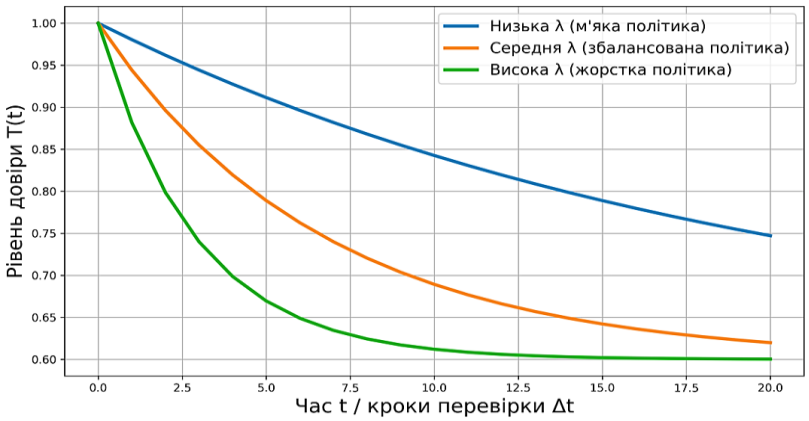

Рисунок 2 – Часова деградація довіри T_t за рекурсивною моделлю (4) при різних значеннях параметра λ

Для врахування нетипової або потенційно ризикованої поведінки користувача вводиться поведінковий коефіцієнт ризику $R_b \in [0,1]$, на основі якого здійснюється корекція поточного рівня довіри [13], [16]:

$$\hat{T} = T(1 - \eta R_b), \quad (5)$$

де η – параметр чутливості моделі до поведінкових відхилень.

Це означає, що навіть за стабільного контексту доступу нетипові дії користувача призводять до зменшення довіри та, відповідно, до посилення контролю доступу.

Отримане скориговане значення довіри використовується для формування адаптивної порогової політики доступу. Для ресурсу з чутливістю $S(r) \in [0,1]$ порогові значення визначаються як [17]:

$$\tau_{allow} = \tau_0 + aS(r),\ \tau_{deny} = \tau_{allow} - \delta, \quad (6)$$

де τ_0 – базовий поріг доступу;

a – коефіцієнт підвищення вимог до критичних ресурсів;

δ – ширина зони невизначеності [15].

Така параметризація дозволяє автоматично підвищувати вимоги до рівня довіри залежно від важливості ресурсу.

Рішення щодо доступу приймається відповідно до правила $ALLOW / STEP-UP / DENY$: якщо $\hat{T} \geq \tau_{allow}$, доступ дозволяється без додаткових перевірок; якщо $\tau_{deny} \leq \hat{T} < \tau_{allow}$, активується додаткова автентифікація; якщо $\hat{T} < \tau_{deny}$, доступ блокується.

Для кількісної оцінки ефективності політики доступу та обґрунтування вибору її параметрів вводиться функціонал втрат [11]:

$$J = C_{breach}(r)(1-\hat{T})^{\gamma} + C_{friction}(r) \cdot 1\{\tau_{deny} \leq \hat{T} < \tau_{allow}\}, \quad (7)$$

де $C_{breach}(r)$ – вартість потенційного порушення безпеки ресурсу;

$C_{friction}(r)$ – "вартість" додаткової автентифікації з погляду зручності користувача;

γ – параметр нелінійності ризику;

$1\{\cdot\}$ – індикаторна функція, що активується в зоні додаткової перевірки.

Наукова новизна запропонованої моделі полягає в тому, що параметри політики доступу розглядаються як змінні, що підлягають оптимізації. Оптимальні значення коефіцієнтів a, δ, γ визначаються шляхом мінімізації математичного сподівання функціоналу втрат:

$$(a^*, \delta^*, \gamma^*) = \arg\min_{a,\delta,\gamma} E[J]. \quad (8)$$

Це забезпечує формалізований компроміс між безпекою та зручністю користувача й дає змогу адаптивно налаштовувати політику безперервної автентифікації відповідно до умов експлуатації Zero Trust.

На рис. 3 наведено дерево рішень Policy Engine, яке формалізує процес прийняття рішень доступу в межах безперервної автентифікації. Рішення щодо надання доступу (ALLOW), ініціювання додаткової автентифікації (STEP-UP) або блокування сесії (DENY) приймається на основі скоригованого рівня довіри користувача $\hat{T}$ та адаптивних порогових значень τ_{allow} і τ_{deny}. Така структура забезпечує детермінований, інтерпретований і придатний до практичної реалізації механізм керування доступом у ZTNA-системах.

Оптимізаційна постановка (8) розглядає параметри політики доступу як адаптивні змінні, що налаштовуються за статистикою середовища та профілем загроз. Мінімізація функціоналу втрат автоматично балансує безпеку й зручність через адаптивне коригування порогів доступу на основі поведінкових та інцидентних даних, підвищуючи стійкість Zero Trust до динамічних загроз. Зміна співвідношення $C_{breach}(r)$ і $C_{friction}(r)$ зсуває політику до жорсткішого або лояльнішого контролю без ручного переналаштування [14], [17].

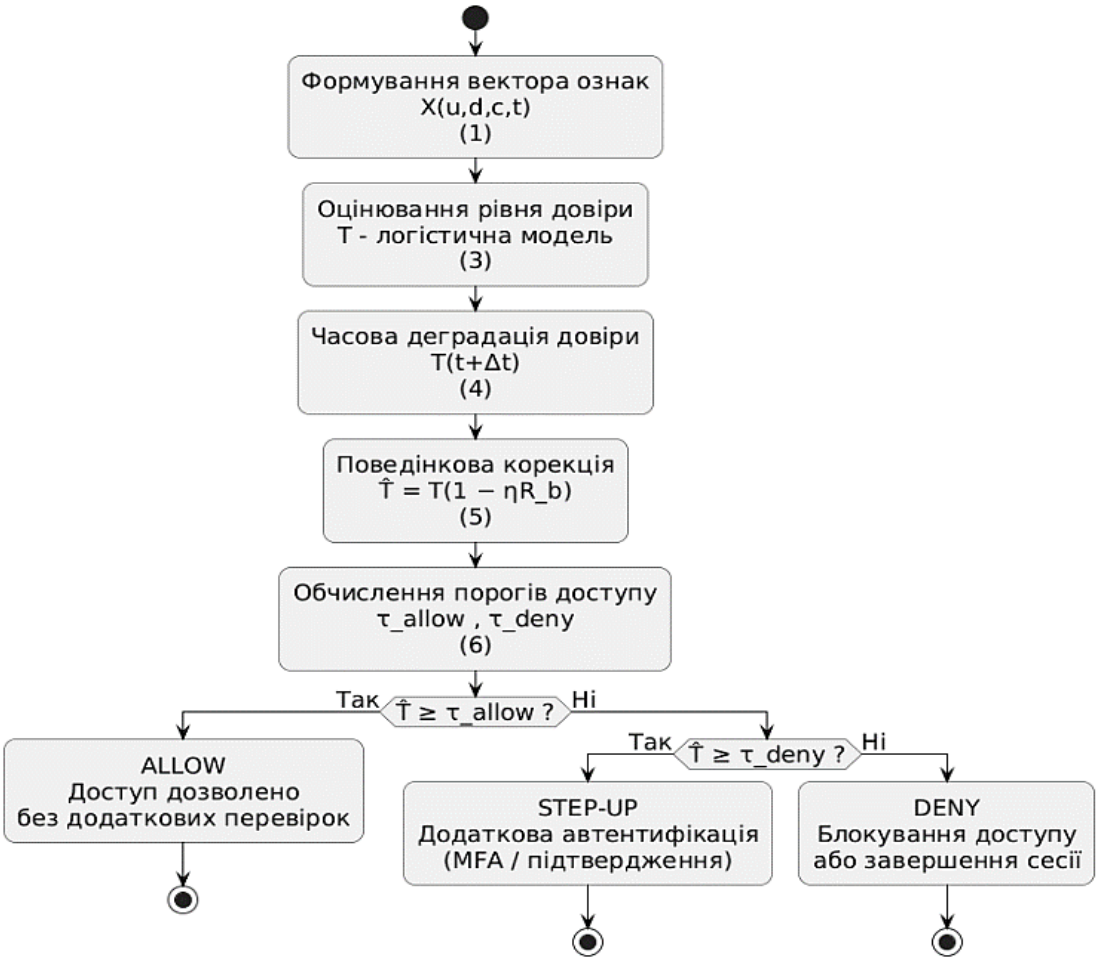

Рисунок 3 – Дерево рішень Policy Engine для безперервної автентифікації в архітектурі Zero Trust Network Access

Табл. 1 демонструє роботу моделі безперервної автентифікації в ZTNA на типових сценаріях доступу [15]: стабільний контекст і низький поведінковий ризик відповідають режиму ALLOW, зміна контексту за збереженої ідентичності – STEP-UP, а високий поведінковий ризик і критичність ресурсу – DENY [13], [16]. Таблиця підтверджує адаптивне розмежування режимів доступу за контекстними та поведінковими факторами.

Таблиця 1 – Прикладна інтерпретація роботи моделі безперервної автентифікації в архітектурі ZTNA

Кейс	Приклади сигналів $X(u,d,c,t)$	Поведінковий ризик R_b	Чутливість ресурсу $S(r)$	Рішення Policy Engine
1	Керований корпоративний пристрій; відповідність політикам безпеки; типова геолокація та робочий час	Низький	0.3	ALLOW
2	Нетипова геолокація; нова мережа або пристрій; збережена коректна ідентичність	Середній	0.7	STEP-UP
3	Аномальна поведінка в сесії; масові запити до ресурсів; відхилення від рольового профілю	Високий	0.9	DENY

Для демонстрації прикладної придатності запропонованої моделі розглянемо типові сценарії ZTNA-доступу, у яких рівень довіри змінюється під впливом контексту та поведінкових факторів і безпосередньо визначає рішення Policy Engine.

Кейс 1 (стандартний корпоративний доступ із керованого пристрою)

Користувач u здійснює доступ до ресурсу середньої критичності r з корпоративного пристрою d, який відповідає політикам безпеки (оновлення, EDR, шифрування диска, відсутність компрометації), та з мережі підприємства у типовий робочий час. У цьому випадку компоненти вектора $X(u,d,c,t)$, що описують ідентичність і стан пристрою, набувають високих значень, поведінковий ризик R_b є низьким, і скоригована довіра $\hat{T}$ перевищує τ_{allow}. У результаті Policy Engine формує рішення ALLOW без додаткових перевірок, дотримуючись принципу мінімальної фрикції за стабільного низькоризикового контексту.

Кейс 2 (віддалений доступ з нетипового контексту – ініціація STEP-UP)

Користувач u з тими самими обліковими даними намагається отримати доступ до ресурсу r у нестандартному контексті c: інша геолокація, нова мережа, нетиповий час доби або новий пристрій d. У такій ситуації частина компонент $X(u,d,c,t)$, що відповідають контексту й довірі до пристрою, зменшуються, а скориговане значення $\hat{T}$ потрапляє в інтервал $\tau_{deny} \le \hat{T} < \tau_{allow}$. Це зумовлює рішення STEP-UP: ініціюється додаткова автентифікація (наприклад, MFA), що підвищує гарантії без блокування доступу за легітимної зміни контексту.

Кейс 3 (внутрішня загроза або компрометація облікових даних – перехід у DENY)

Користувач u має легітимні облікові дані, але в межах активної сесії демонструє нетипову поведінку: швидке зростання кількості запитів до чутливих ресурсів, масове завантаження даних, послідовні звернення до різних сегментів, нехарактерні для його ролі. У моделі це відображається зростанням поведінкового ризику R_b, що призводить до істотного зниження $\hat{T}$ навіть за незмінного контексту доступу. У випадку, коли $\hat{T} < \tau_{allow}$, Policy Engine формує рішення DENY і блокує доступ, тим самим реалізуючи принцип Zero Trust щодо обмеження ризику в межах уже встановленої сесії.

Наведені сценарії підтверджують здатність моделі реалізовувати режими ZTNA (ALLOW/STEP-UP/DENY) на основі динаміки довіри в реальному часі. Урахування поведінкових і контекстних змін підвищує обґрунтованість рішень контролю доступу та узгоджує оцінку ризику з політиками доступу, створюючи умови для масштабування й інтеграції з SIEM/UEBA та SOAR у Zero Trust.

На рис. 4 показано динаміку скоригованого рівня довіри $\hat{T}$ у типових ZTNA-сценаріях: стабільно високі значення відповідають режиму ALLOW, тимчасове зниження – STEP-UP з подальшим відновленням, а падіння нижче τ_{deny} – блокуванню доступу (DENY). Пороги τ_{allow} та τ_{deny} відображають адаптивні умови ухвалення рішень у моделі безперервної автентифікації.

У контексті ZTNA запропонована модель узгоджується з ключовими компонентами архітектури [11]: вектор $X(u,d,c,t)$ формується з атрибутів ідентичності, телеметрії та контексту, після чого Policy Engine обчислює T і $\hat{T}$ та ухвалює рішення ALLOW/STEP-UP/DENY. Реалізація рішення на рівні Policy Enforcement Point забезпечує доступ, додаткову перевірку або блокування [15], що підтверджує сумісність моделі з типовим ZTNA-контуром і її практичну реалізованість.

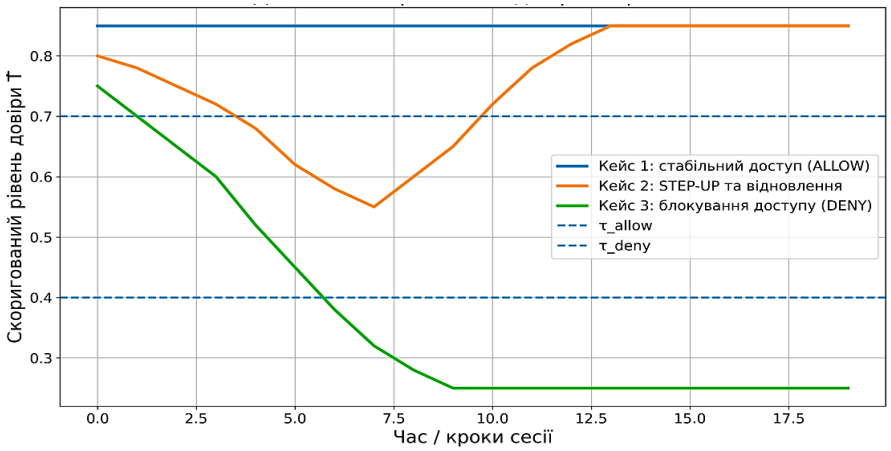

Рисунок 4 – Динаміка скоригованої довіри $\hat{T}$ протягом сесії для типових ZTNA-сценаріїв із порогами τ_{allow} та τ_{deny}

Подана математична модель розглядає безперервну автентифікацію як динамічний керований процес, у якому довіра користувача формується з ідентифікаційних, поведінкових і контекстних факторів та переоцінюється протягом сесії відповідно до принципів Zero Trust. Аналіз моделі деградації довіри (4) показує, що параметр λ визначає чутливість системи до часових інтервалів: великі значення забезпечують швидку реакцію в високоризикових середовищах, а малі – знижують хибні спрацьовування у стабільних сценаріях. Параметр λ регулює жорсткість політики безперервної автентифікації та впливає на ініціювання режимів STEP-UP і DENY [17].

Поведінкова корекція, що визначається параметрами η та R_b, формує нелінійний механізм реагування системи на відхилення від типової поведінки користувача [13], [16]. Навіть за високої початкової довіри незначне зростання поведінкового ризику може призводити до істотного зниження скоригованого рівня довіри, забезпечуючи раннє виявлення потенційних загроз.

Встановлено також залежність між чутливістю ресурсу $S(r)$ і стійкістю сесії доступу: для критичних ресурсів підвищення порогів τ_{allow} та τ_{deny} реалізує більш жорстку політику доступу, зменшуючи ризик компрометації за рахунок підвищених вимог до стабільності поведінки та контексту.

Функціонал втрат (7) дозволяє кількісно оцінити компроміс між ризиком порушення безпеки та негативним впливом надмірних перевірок на користувацький досвід, а мінімізація його математичного сподівання (8) забезпечує адаптивне налаштування політики доступу відповідно до характеристик середовища та профілю загроз.

Модель базується на припущенні нормування всіх ознак $X(u,d,c,t)$ в інтервалі [0,1] та розглядає поведінковий ризик R_b як агрегований показник, спосіб обчислення якого не деталізується в межах дослідження. Також не розглядається автоматичне навчання вагових коефіцієнтів логістичної моделі, що визначає напрями подальших досліджень.

Отримані результати підтверджують сумісність моделі з компонентами Policy Engine і Policy Enforcement Point архітектури ZTNA та її придатність для корпоративних, хмарних і високозахищених систем [12], [14]-[15], [18]. Запропонована цілісна математична модель Zero Trust поєднує оцінку довіри, часову деградацію, поведінкову корекцію й оптимізовану

порогову політику доступу та створює основу для подальшого розвитку, зокрема із застосуванням методів машинного навчання.

Результати цього дослідження. У роботі розроблено формалізовану математичну модель безперервної автентифікації в архітектурі Zero Trust Network Access (ZTNA) на основі динамічної довіри, що забезпечує перехід від одноразової перевірки під час входу до керованого процесу постійного переоцінювання безпеки сесії протягом усього часу доступу. Модель базується на нормованому багатовимірному векторі ознак $X(u,d,c,t)$, який інтегрує параметри ідентичності, стану пристрою, мережевого контексту та поведінкові сигнали з типових джерел (IdP/IAM, EDR/MDM, мережна телеметрія, SIEM/UEBA), що забезпечує її практичну реалізовність у корпоративних і хмарних середовищах.

Рівень довіри T інтерпретовано як кількісну імовірнісну величину та обчислено за інтерпретованою логістичною моделлю з ваговими коефіцієнтами, що дозволяє аналізувати внесок окремих ознак і обґрунтовувати налаштування політик доступу. Для відображення зниження гарантій безпеки за відсутності підтверджуючих подій введено механізм часової деградації довіри, який визначає "жорсткість" контролю в межах сесії доступу.

Для раннього реагування на нетипову активність, внутрішні загрози або компрометацію облікових даних запропоновано механізм поведінкової корекції довіри на основі коефіцієнта ризику R_b та параметра чутливості η. На основі скоригованого рівня довіри сформовано адаптивну порогову політику з урахуванням чутливості ресурсу $S(r)$, яка узгоджується з логікою Policy Engine / Policy Enforcement Point і реалізує режими ALLOW, STEP-UP та DENY.

Для балансування рівня безпеки й зручності користувача введено функціонал втрат і постановку задачі оптимізації параметрів політики шляхом мінімізації очікуваних втрат, що формалізує компроміс між ризиком інцидентів і додатковим навантаженням від перевірок.

Перспективи подальших досліджень. Перспективи подальших досліджень пов'язані з автоматизованим навчанням ваг логістичної моделі на історичних даних доступу, розробленням методів оцінювання поведінкового ризику на основі UEBA/ML, експериментальною апробацією моделі в реальних ZTNA-контурах, аналізом стійкості до обхідних стратегій та врахуванням вимог приватності й мінімізації даних.

Внесок авторів:

– Павло Складанний – концептуалізація дослідження; формалізація математичної моделі безперервної автентифікації; розроблення методики оцінювання динамічної довіри; постановка задачі оптимізації політики доступу; наукове редагування рукопису;

– Юлія Костюк – аналіз наукових джерел та сучасних підходів Zero Trust; підготовка огляду літератури; розроблення прикладних сценаріїв використання моделі; підготовка та візуалізація рисунків і таблиць; перевірка результатів дослідження; підготовка тексту статті.

Подяка, джерела фінансування. Дослідження здійснено в рамках реалізації науково-дослідної теми "Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури" (реєстраційний номер 0122U200483 від 06.07.2022).

Декларація про штучний інтелект. Під час підготовки цієї роботи автори використовували програму штучного інтелекту Grammarly Pro для виправлення граматики тексту та систему Strike Plagiarism для пошуку можливих проявів плагіату. Після використання цих інструментів автори переглянули та відредагували зміст за потреби і несуть повну відповідальність за зміст публікації.

Конфлікт інтересів. Автори заявляють про відсутність конфлікту інтересів та підтверджують, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, “Theory and application of Zero Trust security: A brief survey”, *Entropy*, vol. 25, no. 12, Art. no. 1595, 2023. doi: https://doi.org/10.3390/e25121595.

[2] B.D. Lund, T.-H. Lee, Z. Wang, T. Wang, and N.R. Mannuru, “Zero Trust cybersecurity: Procedures and considerations in context”, *Encyclopedia*, vol. 4, no. 4, pp. 1520-1533, 2024. doi: https://doi.org/10.3390/encyclopedia4040099.

[3] E. Fernández, and A. Brazhuk, “A critical analysis of Zero Trust architecture (ZTA)”, *SSRN Electron. J.*, 16 p. 2022. doi: https://doi.org/10.2139/ssrn.4210104.

[4] R. Wang, C. Li, K. Zhang, and B. Tu, “Zero-trust based dynamic access control for cloud computing”, Cybersecurity, vol. 8, Art. no. 12, 2025. doi: https://doi.org/10.1186/s42400-024-00320-x.

[5] P. Dhiman, N. Saini, Y. Gulzar, S. Turaev, A. Kaur, K.U. Nisa, and Y.A. Hamid, “A review and comparative analysis of relevant approaches of Zero Trust network model”, *Sensors*, vol. 24, no. 4, Art. no. 1328, 2024. doi: https://doi.org/10.3390/s24041328.

[6] C. Liu et al., “Dissecting Zero Trust: Research landscape and its implementation in IoT”, *Cybersecurity*, vol. 7, Art. no. 20, 2024, doi: https://doi.org/10.1186/s42400-024-00212-0.

[7] S. Nie, J. Ren, R. Wu, P. Han, Z. Han, and W. Wan, “Zero-Trust access control mechanism based on blockchain and inner-product encryption in the Internet of Things in a 6G environment”, *Sensors*, vol. 25, no. 2, Art. no. 550, 2025. doi: https://doi.org/10.3390/s25020550.

[8] S.T. Avirneni, “Identity control plane: The unifying layer for Zero Trust infrastructure”, arXiv, 2025. doi: https://doi.org/10.48550/arXiv.2504.17759.

[9] K. Hatakeyama, D. Kotani, and Y. Okabe, “Zero Trust federation: Sharing context under user control towards Zero Trust in identity federation”, in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, 2021, pp. 514-519. doi: https://doi.org/10.1109/PerComWorkshops51409.2021.9431116.

[10] Y. Kostiuk, P. Skladannyi, V. Sokolov, O. Zhyltsov, and Y. Ivanichenko, “Effectiveness of information security control using audit logs”, in *Proc. Workshop Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025)*, vol. 3991, pp. 524-538, 2025. [Online]. Available: https://ceur-ws.org/Vol-3991/paper37.pdf. Accessed on: Jan. 16, 2026.

[11] O. Edo, I. Tenebe, E.-E. Etu, A. Ayuwu, J. Emakhu, and S. Adebiyi, “Zero Trust architecture: Trend and impact on information security”, *Int. J. Emerg. Technol. Adv. Eng*., vol. 12, no. 7, pp. 140-147, 2022. doi: https://doi.org/10.46338/ijetae0722_15.

[12] Y. Kostiuk, K. Khorolska, B. Bebeshko, N. Dovzhenko, N. Korshun, and A. Pazynin, “Instrumental tools for ensuring information security from hidden threats in cloud computing

infrastructure", *Cybersecurity: Education, Science, Technique*, no. 4(28), pp. 633-655, 2025. doi: https://doi.org/10.28925/2663-4023.2025.28.857.

[13] S. Shevchenko, Y. Zhdanova, P. Skladannyi, and S. Boiko, "Insiders and insider information: Essence, threats, activities, and legal responsibility", *Cybersecurity: Education, Science, Technique*, no. 3(15), pp. 175–185, 2022. doi: https://doi.org/10.28925/2663-4023.2022.15.175185.

[14] N. Dovzhenko, Y. Ivanichenko, and Y. Kostiuk, "Methodology for detecting and localizing cyber threats in cloud environments with integrated IoT components based on graph models", *Cybersecurity: Education, Science, Technique*, no. 1(29), pp. 762-776, 2025. doi: https://doi.org/10.28925/2663-4023.2025.29.938.

[15] Т.І. Коробейнікова, І.М. Журавель, А.О. Бодак, та Д.В. Бороденко, "Концепція нульової довіри: сучасні методи забезпечення кібербезпеки в корпоративних мережах", Вісн. Львів. Держ. Унів. Безп. життедіяльності, № 30, с. 67-77, 2024. [Електронний ресурс]. Доступно: https://journal.ldubgd.edu.ua/index.php/Visnuk/article/view/2769/2655. Дата звернення: Січ. 19, 2026.

[16] Y. Kostiuk, P. Skladannyi, S. Rzaieva, N. Mazur, V. Cherevyk, and A. Anosov, "Features of implementing network attacks via TCP/IP protocols", *Cybersecurity: Education, Science, Technique*, no. 1(29), pp. 571-597, 2025. doi: https://doi.org/10.28925/2663-4023.2025.29.915.

[17] V. Borodavka, and V. Yesin, "Implementation of Zero Trust architecture based on the proposed model to ensure enterprise cybersecurity", *Radiotekhnika*, no. 222, pp. 22-54, 2025. doi: https://doi.org/10.30837/rt.2025.3.222.02.

[18] B. Mankovskyi, V. Dovbniak, and I. Opirskyi, "Research on the possibility of implementing the Zero Trust concept in IoT systems", *Cybersecurity: Education, Science, Technique*, no. 1(29), pp. 73-91, 2025. doi: https://doi.org/10.28925/2663-4023.2025.29.864.

REFERENCES

[1] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and application of Zero Trust security: A brief survey", *Entropy*, vol. 25, no. 12, Art. no. 1595, 2023. doi: https://doi.org/10.3390/e25121595.

[2] B.D. Lund, T.-H. Lee, Z. Wang, T. Wang, and N.R. Mannuru, "Zero Trust cybersecurity: Procedures and considerations in context", *Encyclopedia*, vol. 4, no. 4, pp. 1520-1533, 2024. doi: https://doi.org/10.3390/encyclopedia4040099.

[3] E. Fernández, and A. Brazhuk, "A critical analysis of Zero Trust architecture (ZTA)", *SSRN Electron. J.*, 16 p. 2022. doi: https://doi.org/10.2139/ssrn.4210104.

[4] R. Wang, C. Li, K. Zhang, and B. Tu, "Zero-trust based dynamic access control for cloud computing", Cybersecurity, vol. 8, Art. no. 12, 2025. doi: https://doi.org/10.1186/s42400-024-00320-x.

[5] P. Dhiman, N. Saini, Y. Gulzar, S. Turaev, A. Kaur, K.U. Nisa, and Y.A. Hamid, "A review and comparative analysis of relevant approaches of Zero Trust network model", *Sensors*, vol. 24, no. 4, Art. no. 1328, 2024. doi: https://doi.org/10.3390/s24041328.

[6] C. Liu et al., "Dissecting Zero Trust: Research landscape and its implementation in IoT", *Cybersecurity*, vol. 7, Art. no. 20, 2024, doi: https://doi.org/10.1186/s42400-024-00212-0.

[7] S. Nie, J. Ren, R. Wu, P. Han, Z. Han, and W. Wan, "Zero-Trust access control mechanism based on blockchain and inner-product encryption in the Internet of Things in a 6G environment", *Sensors*, vol. 25, no. 2, Art. no. 550, 2025. doi: https://doi.org/10.3390/s25020550.

[8] S.T. Avirneni, "Identity control plane: The unifying layer for Zero Trust infrastructure", arXiv, 2025. doi: https://doi.org/10.48550/arXiv.2504.17759.

[9] K. Hatakeyama, D. Kotani, and Y. Okabe, "Zero Trust federation: Sharing context under user control towards Zero Trust in identity federation", in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, 2021, pp. 514-519. doi: https://doi.org/10.1109/PerComWorkshops51409.2021.9431116.

[10] Y. Kostiuk, P. Skladannyi, V. Sokolov, O. Zhyltsov, and Y. Ivanichenko, "Effectiveness of information security control using audit logs", in *Proc. Workshop Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025)*, vol. 3991, pp. 524-538, 2025. [Online]. Available: https://ceur-ws.org/Vol-3991/paper37.pdf. Accessed on: Jan. 16, 2026.

[11] O. Edo, I. Tenebe, E.-E. Etu, A. Ayuwu, J. Emakhu, and S. Adebiyi, "Zero Trust architecture: Trend and impact on information security", *Int. J. Emerg. Technol. Adv. Eng*., vol. 12, no. 7, pp. 140-147, 2022. doi: https://doi.org/10.46338/ijetae0722_15.

[12] Y. Kostiuk, K. Khorolska, B. Bebeshko, N. Dovzhenko, N. Korshun, and A. Pazynin, "Instrumental tools for ensuring information security from hidden threats in cloud computing infrastructure", *Cybersecurity: Education, Science, Technique*, no. 4(28), pp. 633-655, 2025. doi: https://doi.org/10.28925/2663-4023.2025.28.857.

[13] S. Shevchenko, Y. Zhdanova, P. Skladannyi, and S. Boiko, "Insiders and insider information: Essence, threats, activities, and legal responsibility", *Cybersecurity: Education, Science, Technique*, no. 3(15), pp. 175–185, 2022. doi: https://doi.org/10.28925/2663-4023.2022.15.175185.

[14] N. Dovzhenko, Y. Ivanichenko, and Y. Kostiuk, "Methodology for detecting and localizing cyber threats in cloud environments with integrated IoT components based on graph models", *Cybersecurity: Education, Science, Technique*, no. 1(29), pp. 762-776, 2025. doi: https://doi.org/10.28925/2663-4023.2025.29.938.

[15] T.I. Korobeinikova, I.M. Zhuravel, A.O. Bodak, and D.V. Borodenko, "Concept of Zero Trust: Modern methods for ensuring cybersecurity in corporate networks", Visnyk Lviv State Univ. Life Safety, no. 30, pp. 67-77, 2024. [Online]. Available: https://journal.ldubgd.edu.ua/index.php/Visnuk/article/view/2769/2655. Accessed on: Jan. 19, 2026.

[16] Y. Kostiuk, P. Skladannyi, S. Rzaieva, N. Mazur, V. Cherevyk, and A. Anosov, "Features of implementing network attacks via TCP/IP protocols", *Cybersecurity: Education, Science, Technique*, no. 1(29), pp. 571-597, 2025. doi: https://doi.org/10.28925/2663-4023.2025.29.915.

[17] V. Borodavka, and V. Yesin, "Implementation of Zero Trust architecture based on the proposed model to ensure enterprise cybersecurity", *Radiotekhnika*, no. 222, pp. 22-54, 2025. doi: https://doi.org/10.30837/rt.2025.3.222.02.

[18] B. Mankovskyi, V. Dovbniak, and I. Opirskyi, "Research on the possibility of implementing the Zero Trust concept in IoT systems", *Cybersecurity: Education, Science, Technique*, no. 1(29), pp. 73-91, 2025. doi: https://doi.org/10.28925/2663-4023.2025.29.864.

P-ISSN 2411-1031, E-ISSN 2518-1033
Information Technology and Security. January-June 2026. Vol. 14. Iss. 1 (26)

PAVLO SKLADANNYI,
YULIIA KOSTIUK

MATHEMATICAL MODEL OF CONTINUOUS AUTHENTICATION BASED ON DYNAMIC TRUST IN ZERO TRUST ARCHITECTURE (ZTNA)

This paper proposes a formalized mathematical model of continuous authentication within the Zero Trust Network Access (ZTNA) architecture, which is particularly relevant for remote access, cloud services, and mobile devices, where a single authentication at login does not guarantee session security. Continuous authentication is modeled as a controlled process of dynamic user trust assessment based on a normalized multidimensional feature vector that aggregates identity attributes, device posture, network context, and behavioral signals from typical sources, including IdP/IAM, EDR/MDM, network telemetry, and SIEM/UEBA systems. The trust level is interpreted as a quantitative probabilistic measure suitable for automated decision-making in the Policy Engine and is computed using an interpretable logistic model with feature influence weights. A time-based trust degradation mechanism is introduced to reflect decreasing security assurance in the absence of confirming events and to define the strictness of verification policies during an access session. To account for atypical or potentially risky behavior, a behavioral trust correction mechanism based on a risk coefficient and a sensitivity parameter is proposed, enabling early system response to insider threats or credential compromise. Based on the adjusted trust level, an adaptive threshold-based access control policy is formed with respect to resource sensitivity, implementing ALLOW, STEP-UP, and DENY modes and enforcing decisions at the Policy Enforcement Point. To balance security and user convenience, a loss function is introduced that accounts for incident costs and the friction of additional verification, allowing optimization of access policy parameters. The obtained results confirm the practical applicability of the proposed model for interpretable and adaptive access control in ZTNA and provide a foundation for its further development in corporate and cloud environments.

Keywords: continuous authentication, Zero Trust Network Access, dynamic trust, access control, behavioral risk, adaptive thresholds, security policy, ZTNA architecture.

Складанний Павло Миколайович, кандидат технічних наук, доцент, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка, Київський столичний університет імені Бориса Грінченка, Київ, Україна, ORCID 0000-0002-7775-6039, p.skladannyi@kubg.edu.ua

Костюк Юлія Володимирівна, доктор філософії, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка, Київський столичний університет імені Бориса Грінченка, Київ, Україна, ORCID 0000-0001-5423-0985, y.kostiuk@kubg.edu.ua

Pavlo Skladannyi, candidate of technical sciences, associate professor, head of the academic department of information and cyber security named after professor Volodymyr Buriachok, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine.

Yuliia Kostiuk, PhD, associate professor at the department of information and cyber security named after professor Volodymyr Buriachok, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine.

Стаття надійшла до редакції 06.02.2026.
Стаття прийнята до друку після рецензування 03.06.2026.
Дата оприлюднення: 26.06.2026.