COMPUTER SYSTEMS AND NETWORKS

Vol. 8, No. 1, 2026 **ISSN: 2707-2371 (print); ISSN: XXXXX (online)**

DOI: https://doi.org/10.23939/csn2026.01.

УДК 004.056

АРХІТЕКТУРА ZERO TRUST ІЗ ПОЯСНЮВАНИМ І ФОРМАЛЬНО ВЕРИФІКОВАНИМ ЗАМКНЕНИМ КОНТУРОМ ОНОВЛЕННЯ ПОЛІТИК ДОСТУПУ НА ОСНОВІ SIEM

П.М. Складанний, Ю.В. Костюк, Н.П. Мазур

Київський столичний університет імені Бориса Грінченка
кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
E-mail: p.skladannyi@kubg.edu.ua, y.kostiuk@kubg.edu.ua, n.mazur@kubg.edu.ua
ORCID: 0000-0002-7775-6039, 0000-0001-5423-0985, 0000-0001-7671-8287

Надійшла до редакції: 06.04.2026
Прийнята до друку: 20.04.2026
Опубліковано: 01.06.2026

© Складанний П.М., Костюк Ю.В., Мазур Н.П. 2026

Стаття поширюється за ліцензією
Creative Commons Attribution-NonCommercial 4.0 (CC BY-NC 4.0)

У статті запропоновано архітектуру Zero Trust із пояснюваним і формально верифікованим замкненим контуром оновлення політик доступу на основі аналітики SIEM/UEBA. На відміну від підходів, де адаптація політик здійснюється евристично або за допомогою непрозорих моделей машинного навчання, запропонований метод поєднує причинно-наслідковий аналіз подій безпеки, інтерпретовану модель деградації довіри та формальну перевірку коректності політик до і після їх оновлення. Рішення щодо модифікації PBAC-політик формуються на підставі причинних зв'язків між сигналами SIEM/UEBA, ризиковими станами доступу та параметрами політик у вигляді пояснюваних ланцюгів «подія → ризик → зміна правила». Для керованого вибору кандидатних змін запропоновано багатокритеріальну постановку оптимізації, що враховує очікуваний ризик доступу, затримку прийняття рішень і частоту застосування step-up автентифікації. Коректність оновлених політик гарантується модулем формальної верифікації, який запобігає конфліктам правил і появі небезпечних станів доступу в умовах автоматизованої адаптації. Експериментальне оцінювання за формалізованими сценаріями S1–S6 демонструє ефективність замкненого контуру в номінальних і стресових режимах та підтверджує практичну придатність підходу для корпоративних інформаційно-комунікаційних систем із підвищеними вимогами до прозорості й керованості доступу.

Ключові слова: адаптивна автентифікація, інформаційна безпека, керування довірою, пояснюваний штучний інтелект, причинно-наслідковий аналіз, політики доступу, формальна верифікація, PBAC, SIEM, Zero Trust.

1.Вступ

Сучасні архітектури Zero Trust набувають широкого застосування в корпоративних інформаційно-комунікаційних системах як концептуальна відповідь на зростання інтенсивності та складності кіберзагроз, динамічність цифрових середовищ і втрату ефективності класичних периметрових моделей захисту [1-2, 6]. Водночас реалізація принципів Zero Trust на практиці значною мірою залежить від механізмів формування та адаптації політик доступу, які в більшості наявних

рішень ґрунтуються на евристичних правилах або непрозорих моделях машинного навчання. Такий підхід ускладнює інтерпретацію прийнятих рішень, обмежує можливості їх формального аналізу та створює ризик порушення коректності політик у процесі автоматизованого оновлення.

За відсутності формальних гарантій безпеки динамічна зміна порогів і правил доступу може призводити до виникнення небезпечних станів системи, зростання кількості хибних дозволів або відмов, а також надмірного застосування механізмів підвищеної автентифікації, що негативно впливає на ефективність бізнес-процесів [3, 10]. У зв'язку з цим актуальною науковою проблемою є розроблення архітектурних і методичних підходів до адаптації політик Zero Trust, які поєднують причинно-наслідкове обґрунтування змін, пояснюваність рішень для аналітиків безпеки та формальну верифікацію коректності політик у динамічному середовищі загроз [2, 7, 16-17]. Розв'язання цієї проблеми має суттєве значення для подальшого розвитку теорії керування доступом і довірою, а також для практичного впровадження керованих, прозорих і стійких систем кіберзахисту на основі аналітики SIEM.

Для підвищення ефективності архітектур Zero Trust доцільним є перехід від евристичної або реактивної адаптації політик доступу до формалізованих механізмів їх оновлення, що спираються на причинно-наслідковий аналіз подій безпеки, інтерпретовану оцінку деградації довіри та перевірку коректності прийнятих рішень. Такий підхід дозволяє не лише зменшити ризик виникнення небезпечних станів доступу, а й забезпечити прозорість і відтворюваність процесу модифікації політик у динамічному середовищі загроз.

2.Огляд літературних джерел

Концепція Zero Trust Architecture (ZTA) упродовж останніх років набула значної уваги наукової спільноти як фундаментальна парадигма побудови сучасних систем контролю доступу в умовах розмитого периметра та динамічних кіберзагроз. У роботі Kang, Liu, Wang та ін. [1] виконано систематизований аналіз теоретичних засад Zero Trust, у якому розглянуто еволюцію моделей довіри, механізми безперервної перевірки та ключові архітектурні компоненти ZTA, при цьому підкреслено обмеженість статичних і ролеорієнтованих підходів у сучасних середовищах. Подібної позиції дотримуються Lund, Lee, Wang та Mannuru [2], які узагальнюють практики впровадження Zero Trust у різних доменах та вказують на відсутність формалізованих механізмів керованої адаптації політик доступу як одну з ключових відкритих проблем.

Значний масив наукових робіт присвячено динамічній оцінці довіри та ризик-орієнтованому контролю доступу в архітектурі Zero Trust. Так, Li, Yang та Zhang [12] пропонують контекстно-орієнтовану модель керування доступом на основі ризикових атрибутів, однак прийняття рішень у таких системах залишається складним для інтерпретації та формальної перевірки. Подібні обмеження характерні і для машинних та нечітких моделей оцінювання ризику доступу, що не забезпечують достатнього рівня пояснюваності політик у процесі їх автоматизованої адаптації.

Окремий напрям досліджень пов'язаний з інтеграцією архітектури Zero Trust із системами моніторингу подій безпеки. У роботі Tendikov, Rzayeva та співавт. [3] проаналізовано методи збору та аналізу даних у SIEM із використанням алгоритмів машинного навчання, що дозволяє підвищити точність виявлення інцидентів, однак не забезпечує безпосереднього зв'язку між результатами аналітики та адаптацією політик доступу. Аналогічну проблему підкреслюють Jalalvand, Baruwal Chhetri, Nepal і Paris [5], які у систематичному огляді методів пріоритизації алертів SOC вказують на відсутність замкненого контуру між кореляцією подій і рішеннями контролю доступу. У подальшій роботі Tariq та співавт. [4] показано, що перевантаження алертами й непрозорі рішення знижують ефективність SOC, що негативно впливає на практичну реалізацію принципів Zero Trust.

Проблематика пояснюваності в системах безпеки активно розглядається в контексті Explainable Artificial Intelligence (XAI). У фундаментальній роботі Arrieta, Díaz-Rodríguez, Del Ser та співавт. [7] систематизовано підходи до пояснюваності моделей машинного навчання для критичних доменів, зокрема наведено таксономію методів XAI та окреслено їхні обмеження з точки зору відповідальності й інтерпретованості рішень. Водночас питання інтеграції XAI безпосередньо у процес керування

політиками доступу в архітектурі Zero Trust у цій роботі не розглядається. Подальші дослідження у сфері кібербезпеки, зокрема Yan, Wen, Nepal, Paris та Xiang [8], демонструють застосування пояснюваних моделей для аналізу рішень у системах виявлення вторгнень і SOC, однак не формують причинно-наслідкових зв'язків між подіями безпеки та модифікацією правил доступу.

Формальна верифікація політик безпеки розглядається як окремий науковий напрям, здебільшого незалежний від архітектури Zero Trust. У роботі Caserio, Lonetti та Marchetti [9] запропоновано формальний підхід до валідації політик доступу XACML 3.0, що дозволяє виявляти конфлікти та небезпечні стани доступу. Аналогічно, Karimi, Alencar та Cowan [10] розробляють формальні моделі аналізу правил і комбінацій політик доступу, однак ці підходи не враховують динамічний характер оновлення політик під впливом подій безпеки та аналітики SIEM. Огляди сучасних SIEM-систем, зокрема дослідження Macaneata [11], зосереджуються переважно на архітектурі та функціональних можливостях таких платформ, не інтегруючи формальні методи у процес адаптації політик доступу.

Таким чином, аналіз сучасних наукових джерел свідчить, що наявні дослідження або зосереджуються на архітектурних принципах Zero Trust [1, 2], або на ризик-орієнтованих і контекстно-залежних підходах до оцінки довіри [12], або на аналітиці SIEM та пояснюваному штучному інтелекті як окремих напрямах [3–8]. Водночас відсутні комплексні моделі, які поєднують причинно-наслідковий, пояснюваний аналіз подій безпеки, формальну верифікацію політик і замкнений контур їх автоматизованого оновлення в архітектурі Zero Trust. Запропоноване в цій статті дослідження спрямоване на заповнення зазначеної наукової прогалини та формування цілісного підходу до керованої й безпечної адаптації політик доступу на основі аналітики SIEM.

3.Постановка задачі

Метою статті є розроблення й обґрунтування архітектури Zero Trust із пояснюваним і формально верифікованим замкненим контуром оновлення політик доступу на основі аналітики SIEM, яка забезпечує керовану, причинно-обґрунтовану та безпечну адаптацію рішень авторизації в умовах динамічних кіберзагроз [5-6, 9, 12]. Запропонований підхід спрямований на подолання ключового обмеження сучасних Zero Trust-рішень, що полягає у відсутності прозорих і формально контрольованих механізмів автоматичного коригування політик доступу відповідно до змін ризикового контексту [6-9, 11, 19]. Таким чином, запропонований підхід поєднує концепції Zero Trust, XAI та формальних методів у єдиній керованій архітектурі, що раніше розглядалися в літературі переважно ізольовано.

У межах дослідження формується наукова задача побудови замкненого контуру керування політиками доступу, в якому результати моніторингу та кореляції подій безпеки, отримані з SIEM/UEBA, використовуються не лише для оцінювання рівня довіри користувачів і пристроїв, але й для причинно-наслідкового обґрунтування змін у політиках Policy-Based Access Control (PBAC) із гарантією відсутності небезпечних станів системи після адаптації.

Для досягнення поставленої мети здійснюється аналіз обмежень наявних підходів до адаптації політик доступу в архітектурі Zero Trust з позицій пояснюваності прийнятих рішень і забезпечення формальної коректності політик у процесі їх автоматизованого оновлення [2, 6, 9, 12]. На цій основі розробляється модель причинно-наслідкового зв'язку між сигналами SIEM/UEBA, деградацією довіри суб'єктів доступу та модифікацією PBAC-політик [11, 19]. Далі формується формальний опис політик доступу та множини небезпечних станів системи, що підлягають перевірці до і після застосування змін [3, 10]. Наступним етапом є розроблення багатокритеріальної моделі оптимізації процесу адаптації політик з урахуванням компромісу між рівнем ризику, затримкою прийняття рішень і частотою застосування механізмів підвищеної автентифікації [7-8, 13, 16]. Завершальним етапом дослідження є експериментальна верифікація запропонованого підходу в умовах динамічних сценаріїв доступу та змінного ризикового контексту.

У роботі перевіряється сукупність наукових гіпотез щодо можливості обґрунтованої та прозорої адаптації політик доступу без зростання кількості хибних дозволів або відмов, а також щодо

забезпечення відсутності небезпечних станів системи за умов автоматизованого оновлення правил [3, 10]. Додатково досліджується можливість досягнення збалансованого компромісу між рівнем безпеки, продуктивністю функціонування системи та зручністю користувачів [7, 12, 16]. Сформульована постановка задачі визначає логіку подальшого дослідження та створює наукове підґрунтя для розроблення керованої, прозорої й стійкої архітектури Zero Trust, орієнтованої на практичне застосування в корпоративних інформаційно-комунікаційних системах.

Наукова новизна дослідження полягає у переході від евристичної або реактивної адаптації політик доступу в архітектурі Zero Trust до формалізованої, керованої та пояснюваної моделі їх оновлення, у якій чітко визначено причини, наслідки та формальні гарантії коректності змін [2, 6, 9-10]. На відміну від поширених підходів, що ґрунтуються на непрозорих моделях машинного навчання або емпіричному коригуванні порогів доступу, запропоновано концепцію замкненого контуру керування політиками доступу, засновану на причинно-наслідковому аналізі подій безпеки, інтерпретованій оцінці деградації довіри та формальній верифікації результатів адаптації.

Ключовим елементом наукової новизни є введення причинно-орієнтованого пояснюваного шару (Causal/XAI), який встановлює формалізований зв'язок між сигналами SIEM/UEBA, зміною рівня довіри користувачів і пристроїв та конкретними модифікаціями PBAC-політик, забезпечуючи прозорість, відтворюваність і обґрунтованість процесу адаптації [2, 19]. Другим важливим аспектом є інтеграція формальної верифікації політик доступу безпосередньо у процес їх автоматизованого оновлення, що гарантує відсутність небезпечних станів системи та запобігає появі нових вразливостей [3, 4, 10, 16]. Третім складником новизни є застосування багатокритеріальної оптимізації процесу адаптації політик доступу з урахуванням ризику, затримки прийняття рішень і частоти застосування механізмів підвищеної автентифікації, що дозволяє формалізувати компроміс між безпекою, продуктивністю системи та зручністю користувачів.

Сукупність запропонованих рішень формує новий підхід до реалізації архітектури Zero Trust, у якому адаптація політик доступу здійснюється в замкненому, причинно-обґрунтованому, пояснюваному та формально контрольованому контурі на основі аналітики SIEM, що становить істотний науковий внесок у розвиток теорії та практики керування доступом у динамічних кіберсередовищах.

4.Архітектура замкненого контуру оновлення політик Zero Trust

Запропонована в роботі архітектура замкненого контуру оновлення політик доступу в середовищі Zero Trust ґрунтується на принципі безперервного причинно-обґрунтованого керування рішеннями авторизації на основі аналітики подій безпеки [6, 9, 12]. На відміну від поширених реалізацій Zero Trust, у яких результати моніторингу безпеки використовуються переважно для реактивного блокування доступу або локальної зміни порогів, запропонований підхід формує цілісний замкнений контур, що інтегрує системи SIEM/UEBA, пояснюваний причинно-наслідковий аналіз і механізми прийняття рішень щодо доступу в єдину керовану архітектуру [10, 13, 19]. Така інтеграція дозволяє забезпечити не лише адаптивність політик доступу до динамічного ризикового середовища, а й прозорість та формальну коректність процесу їх автоматизованого оновлення.

Рис. 1 ілюструє замкнений контур оновлення політик доступу в архітектурі Zero Trust. Події та контекст безпеки збираються рівнем SIEM/UEBA і передаються до шару Causal/XAI, де формуються причинно-обґрунтовані та пояснювані підстави для зміни доступу. На їх основі PDP приймає рішення та ініціює кандидатні модифікації політик у PAP, які обов'язково проходять формальну верифікацію. Лише коректні політики застосовуються на рівні PEP, а результати виконання формують зворотний зв'язок до SIEM, забезпечуючи безперервну адаптацію, прозорість і формальну коректність керування доступом.

У межах запропонованої архітектури рівень SIEM/UEBA виступає джерелом структурованих сигналів безпеки, які відображають зміну поведінки користувачів, пристроїв і сервісів у часовому та контекстному вимірах [5, 13, 17]. Події, що надходять із різнорідних джерел телеметрії, підлягають нормалізації, кореляції та агрегуванню з урахуванням контексту доступу, що дозволяє формувати узагальнені індикатори ризику, придатні для подальшого аналізу. При цьому вихідні дані SIEM

розглядаються не як дискретні алерти, а як параметризований опис ризикового стану, який може впливати на різні аспекти політик доступу з різною інтенсивністю. Такий підхід створює передумови для диференційованої адаптації PBAC-політик залежно від характеру, частоти та причинної значущості зафіксованих подій безпеки.

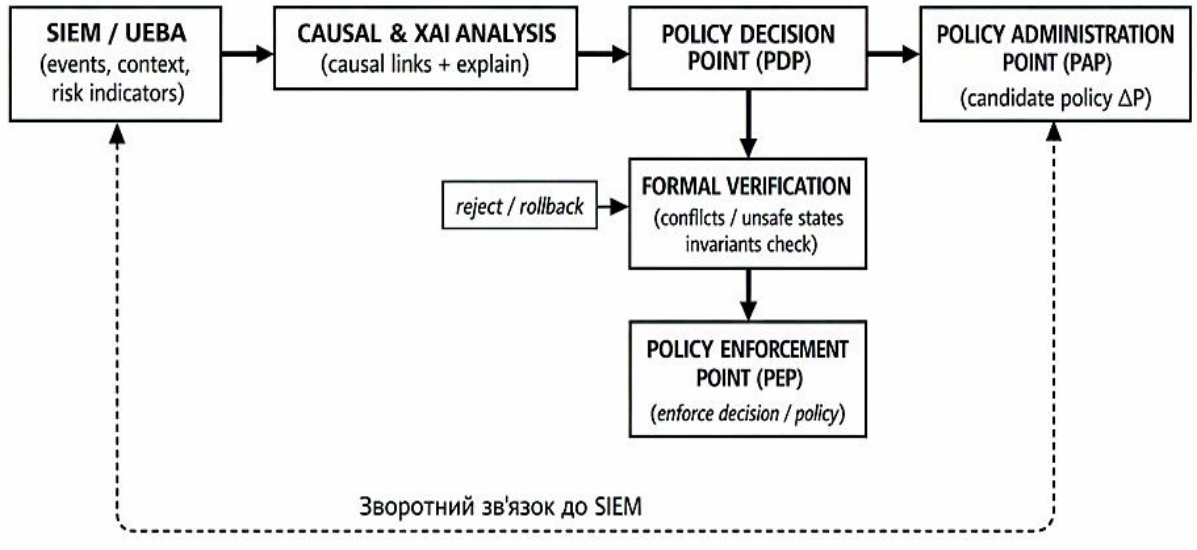

Рис. 1. Архітектура замкненого контуру оновлення політик доступу Zero Trust

Центральним елементом архітектури є причинно-наслідковий пояснюваний шар, що трансформує сигнали SIEM/UEBA у формалізовані підстави для модифікації політик доступу [2, 19]. На цьому рівні встановлюються причинні зв'язки між подіями безпеки, деградацією довіри та параметрами PBAC-політик, формуючи пояснювані ланцюги типу «подія → ризиковий стан → зміна правила», які забезпечують прозорість і відтворюваність процесу адаптації.

Результатом причинно-наслідкового аналізу є множина допустимих модифікацій політик, що передаються до Policy Decision Point. Прийняття рішень PDP інтегрується з модулем формальної верифікації, який перевіряє коректність політик до і після їх оновлення, запобігаючи виникненню конфліктів, логічних суперечностей і небезпечних станів доступу та гарантуючи збереження інваріантів безпеки за умов автоматизованої адаптації.

Замкненість архітектури реалізується через зворотний вплив рішень PDP на контекст безпеки, що знову фіксується SIEM/UEBA, формуючи безперервний цикл оцінювання, пояснення та коригування політик доступу. Такий підхід забезпечує адаптацію Zero Trust у реальному часі з одночасним зниженням ризику несанкціонованого доступу та контролем операційних витрат, пов'язаних із затримками прийняття рішень і частотою застосування step-up автентифікації.

У сукупності запропонований замкнений контур формує основу для реалізації керованих, пояснюваних і формально верифікованих рішень Zero Trust, підвищуючи їхню прозорість, стійкість і практичну придатність у динамічних кіберсередовищах.

5.Формальна модель причинно-наслідкової адаптації PBAC-політик

Для формалізації процесу адаптації політик доступу в архітектурі Zero Trust запропоновано причинно-наслідкову модель, яка встановлює однозначний зв'язок між подіями безпеки, деградацією довіри та допустимими модифікаціями політик доступу на основі Policy-Based Access Control (PBAC). Така модель дозволяє перейти від евристичного коригування правил до керованого, пояснюваного й формально контрольованого оновлення політик у замкненому контурі SIEM → Causal/XAI → PDP.

Нехай $E = e_1, e_2 \ldots, e_n$ − множина подій безпеки, що фіксуються системами SIEM/UEBA у ковзному часовому вікні Δt [13, 17]. Кожна подія e_i описується вектором атрибутів:

$$e_i = \langle type_i,\ src_i\ ctx_i,\ sev_i,\ t_i \rangle, \tag{1}$$

де $type_i$ − тип події, src_i − джерело, ctx_i − контекст доступу, sev_i − оцінка критичності, t_i − час виникнення. Для відображення причинно-наслідкових залежностей між подіями та станами доступу вводиться орієнтований граф причинності:

$$G_c = (V, A), \tag{2}$$

де множина вершин $V = E \cup R \cup \Theta$ включає події безпеки E, ризикові стани доступу R та множини параметрів політик (пороги, ваги, умови), що входять до причинного графа як об'єкти модифікації Θ, а множина дуг $A \subseteq V \times V$ відображає встановлені причинні зв'язки. Дуга $e_i, r_j \in A$ означає, що подія e_i є причинно значущою для формування ризикового стану r_j, тоді як дуга $r_j, p_k \in A$ відображає вплив відповідного ризику на параметр політики доступу p_k [2, 19]. Такий графовий підхід узгоджується з сучасними концепціями причинно-орієнтованого аналізу та пояснюваності в системах кібербезпеки.

На рис. 2 подано причинно-наслідковий граф адаптації PBAC-політик, у якому відображено зв'язок між подіями безпеки e_i, ризиковими станами доступу r_j та параметрами політик p_k. Орієнтовані дуги $e_i \rightarrow r_j$ фіксують причинний вплив зафіксованих SIEM/UEBA подій на формування ризикових станів, тоді як дуги $r_j \rightarrow p_k$ відображають обґрунтовану та інтерпретовану модифікацію конкретних параметрів політик доступу. Таким чином, рисунок наочно демонструє, що адаптація політик у запропонованій архітектурі має формалізований причинно-наслідковий характер і не зводиться до евристичного коригування правил.

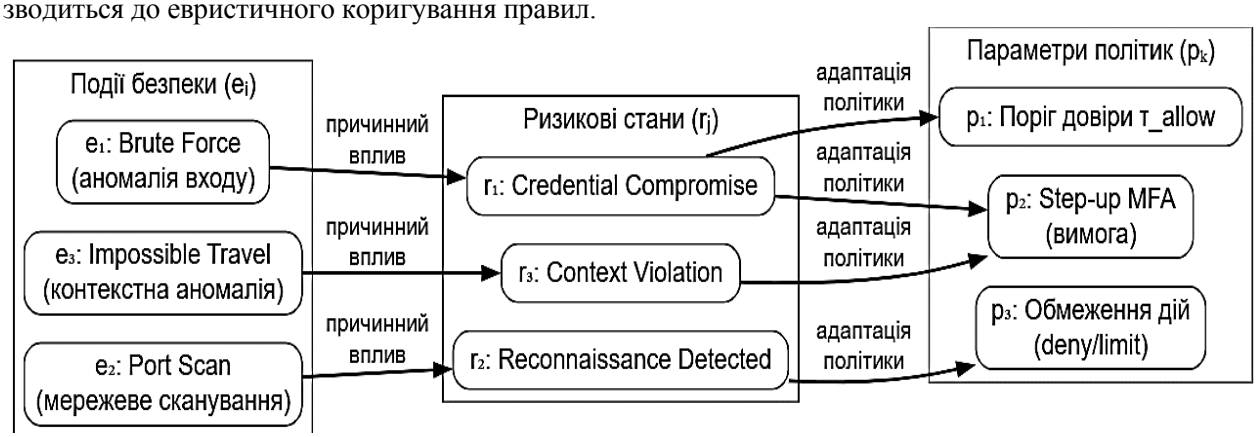

Рис. 2. Формальна модель причинно-наслідкової адаптації PBAC-політик

На основі графа G_c формується функція деградації довіри, яка відображає зміну рівня довіри суб'єкта доступу в часі під впливом зафіксованих подій [2, 9]. Нехай $T\ u, d, t \in [0,1]$ — рівень довіри до користувача u і пристрою d у момент часу t. Тоді деградація довіри в інтервалі Δt визначається як:

$$T\ u, d, t + \Delta t\ = T\ u, d, t\ - \sum_{e_i \in E_{\Delta t}} w_i \cdot \phi(e_i, ctx), \tag{3}$$

де w_i − вага причинної значущості події e_i, отримана з графа G_c, а $\phi(e_i, ctx)$, − функція контекстної чутливості, що враховує тип ресурсу, час доступу та історію поведінки [19]. Така форма дозволяє інтерпретовано пояснити, які саме події та з якою інтенсивністю призвели до зниження рівня довіри, що є критичним для пояснюваності рішень у Zero Trust.

Слід зазначити, що у своїй поточній формі функція деградації довіри (3) є **лінійною** по внесках окремих подій, що спрощує її інтерпретацію та реалізацію. Водночас у середовищах із корельованими та кумулятивними загрозами лінійна адитивність може недооцінювати сукупний ризик скоординованих атак. Для врахування таких ефектів формула (3) може бути розширена до нелінійного виду: $T\ u, d, t + \Delta t\ = T\ u, d, t\ - f(\ \ w_i \cdot \phi(e_i, ctx)$, де f(·) — монотонно зростаюча

нелінійна функція (наприклад, сигмоїдна або степенева), яка підсилює вплив кластерів корельованих подій. Такий підхід дозволяє моделювати ефект «накопиченого ризику», за якого кілька слабких але скоординованих сигналів призводять до більшої деградації довіри, ніж сума їх окремих внесків. Дослідження нелінійних варіантів функції деградації є перспективним напрямом подальшої роботи.

Політики доступу в межах PBAC формалізуються як множин:а правил:

$$P = \{p_k\},\ \ p_k : \langle C_k, A_k, \Theta_k \rangle, \tag{4}$$

де C_k − умови застосування правила, A_k − дозволені або заборонені дії, Θ_k − параметри політики (пороги довіри, рівні ризику, вимоги step-up автентифікації). Параметри Θ_k включають, зокрема, пороги довіри $\tau_{allow}, \tau_{deny}$, вимоги до контексту (геолокація, мережевий сегмент), а також умови виклику step-up (наприклад, $T < \tau_{allow}$ або підвищений R) [10-12]. Адаптація ΔP змінює саме параметриΘ_k, а не логіку правил довільно, що забезпечує керованість і відтворюваність оновлень.

Адаптація політик зводиться не до довільної зміни правил, а до вибору допустимої множини модифікацій:

$$\Delta P = \{\delta p_k\}, \tag{5}$$

де кожна δp_k є функцією від ідентифікованих причинних шляхів у графі G_c та поточного значення довіри $T\ u, d, t$. Формально допустимою вважається така зміна політики, для якої виконується умова:

$$V\ \ P \cup \Delta P\ \ = true, \tag{6}$$

де $V\ \cdot\ $ − предикат формальної верифікації, що перевіряє відсутність конфліктів правил і небезпечних станів доступу. У роботі предикат $V\ \cdot\ $ реалізує формальну перевірку політик доступу як задачу виявлення конфліктів і досяжності небезпечних станів. Політики PBAC подаються у вигляді логічних обмежень над атрибутами $\langle u, d, res, c \rangle$ та порогами довіри/ризику, після чого виконується перевірка несуперечності правил (відсутність одночасного Permit і Deny для одного стану), відсутності конфліктів комбінування політик, недосяжності станів із S_{unsafe} [3-4, 10]. Практично це реалізовано через SMT-перевірку з використанням розв'язувача Z3 (Microsoft Research): обмеження на атрибути ⟨u, d, res, c⟩ та порогові умови довіри/ризику кодуються у вигляді формул першого порядку, після чого Z3 перевіряє їх виконуваність і відповідність інваріантам безпеки. Як альтернатива для більш складних моделей станів може бути застосовано model checking засобами Alloy Analyzer або Spin.

Для забезпечення керованості процесу адаптації вводиться функція вибору оптимальної модифікації політик:

$$\delta p_k^* = arg(\alpha R + \beta D + \gamma F)\ , \tag{7}$$

де R − очікуваний ризик доступу після модифікації, D − затримка прийняття рішень, F − частота застосування step-up автентифікації, α, β, γ − вагові коефіцієнти, що визначають пріоритети безпеки, продуктивності та зручності користувачів [7, 8, 11, 16]. Таким чином, адаптація політик набуває вигляду багатокритеріальної оптимізації, у якій кожне рішення є не лише реакцією на події безпеки, а й формально обґрунтованим компромісом між ризиком і операційними втратами.

Вагові коефіцієнти α, β, γ обираються відповідно до політики прийнятного ризику та критичності ресурсів: для критичних ресурсів збільшується α, для систем із жорсткими SLA − β, а для середовищ із високою ціною “зайвих перевірок” − γ [12]. У експериментах використовувались фіксовані ваги в межах сценаріїв, що забезпечує порівнюваність результатів.

Запропонована формальна модель забезпечує однозначний причинно-наслідковий зв’язок між подіями SIEM/UEBA та змінами PBAC-політик, зберігаючи інтерпретованість і формальну коректність рішень. Поєднання графів причинності, функції деградації довіри та допустимих змін політик формує теоретичну основу пояснюваного й безпечного замкненого контуру адаптації доступу в архітектурі Zero Trust.

6.Математична формалізація замкненого контуру адаптації політик доступу

Замкнений контур адаптації політик доступу в архітектурі Zero Trust розглядається як динамічна система керування зі зворотним зв’язком, у якій рішення щодо авторизації та модифікації

політик формуються на основі поточного стану довіри, ризикового контексту та результатів аналітики подій безпеки [6, 9, 12]. Формально такий контур можна подати у вигляді дискретної динамічної системи, що еволюціонує в часі під впливом зовнішніх збурень (подій безпеки) та внутрішніх керуючих впливів (адаптації політик).

Стан системи в момент часу t задається вектором, що поєднує рівень довіри суб'єктів, ризиковий показник і конфігурацію PBAC-політик, а керуючі впливи формуються на основі цього стану та подій безпеки. Перехід між станами описується оператором оновлення, який інтегрує оцінку ризику, багатокритеріальну оптимізацію змін і формальну верифікацію політик [10-11]. Така формалізація дає змогу аналізувати стійкість і керованість замкненого контуру та гарантувати відсутність небезпечних станів доступу під час автоматизованої адаптації.

Нехай $t \in N$ − дискретний час, що відповідає крокам аналізу в ковзному вікні Δt. Стан системи в момент часу t описується вектором:

$$x\ t\ = \langle T\ t\ , R\ t\ , P(t) \rangle, \tag{8}$$

де $T\ t\ \in [0,1]^m$ − вектор рівнів довіри для множини суб'єктів і пристроїв, $R\ t\ \in R_{\geq 0}^k$ − вектор оцінок ризику доступу до ресурсів, $P(t)$ − конфігурація PBAC-політик доступу у момент часу t [9, 11]. Такий опис стану дозволяє узгоджено враховувати як поведінкові та контекстні характеристики суб'єктів доступу, так і поточні обмеження, накладені політиками безпеки. Зміна вектора стану $x\ t$ у часі відображає результат взаємодії між подіями безпеки, механізмами оцінювання довіри та процедурами адаптації й верифікації політик доступу.

Вхідним сигналом системи є потік подій безпеки:

$$u(t) = E(t) = \ e_1, e_2, \dots, e_n\ , \tag{9}$$

отриманий із SIEM/UEBA за інтервал $t, t + \Delta t$ [13, 17]. Функція переходу стану замкненого контуру визначається як:

$$x\ t+1\ = f(x\ t\ , u\ t\ ), \tag{10}$$

де $f(\cdot)$ − композиція функцій аналізу подій, оцінки довіри, адаптації політик і формальної перевірки. Такий формалізм дозволяє подати замкнений контур як керовану систему, у якій зовнішні події безпеки виступають збурювальним впливом, а адаптація політик − керуючою дією. Функція переходу $f(\cdot)$ забезпечує узгоджене оновлення стану системи з урахуванням причинно-наслідкових зв'язків, багатокритеріальної оптимізації та обмежень формальної коректності політик доступу.

Оцінка ризику доступу здійснюється як функція довіри, контексту та політик [11]:

$$R\ t\ = g\ T\ t\ , C\ t\ , P(t)\ , \tag{11}$$

де $C\ t\ $ − вектор контекстних параметрів (локація, час, тип ресурсу, історія доступів). Функція $g(\cdot)$ може бути нелінійною та враховувати причинно-наслідкові зв'язки, встановлені у графі причинності G_c.

Еволюція довіри описується рекурентним співвідношенням:

$$T\ t+1\ = T\ t\ - \Delta T(t), \tag{12}$$

де величина деградації довіри:

$$\Delta T\ t\ = \ \ _{e_i \in E(t)} w_i \cdot \phi(e_i, C(t)), \tag{13}$$

відображає сумарний причинний вплив подій безпеки на суб'єкт доступу [2, 19]. Така форма дозволяє зберігати інтерпретованість: кожен доданок відповідає конкретній події та її контексту.

Адаптація політик доступу розглядається як керуючий вплив:

$$P\ t+1\ = P\ t\ \oplus \Delta P(t), \tag{14}$$

де $\oplus$ − оператор модифікації політик, $\Delta P(t)$ належить множині допустимих змін [12]. Вибір $\Delta P(t)$ формулюється як задача багатокритеріальної оптимізації [7-8, 16]:

$$\Delta P^*(t) = arg(\alpha R(t+1) + \beta D(t+1) + \gamma F(t+1))\ , \tag{15}$$

де $D(t+1)$ − очікувана затримка прийняття рішень доступу, $F(t+1)$ − частота застосування step-up автентифікації, α, β, γ − коефіцієнти пріоритетності.

Ключовою особливістю замкненого контуру є наявність обмежень формальної коректності, які накладаються на процес адаптації:

$$V\ P(t+1\ ) = true, \tag{16}$$

де $V\ \cdot\ -$ функція формальної верифікації, що гарантує відсутність конфліктів політик і небезпечних станів доступу. У разі невиконання цієї умови керуючий вплив $\Delta P(t)$ відхиляється або коригується, що реалізує механізм негативного зворотного зв'язку в системі.

На рис. 3 показано динамічну модель замкненого контуру адаптації політик доступу в архітектурі Zero Trust, подану у вигляді керованої системи зі зворотним зв'язком. Стан системи визначається вектором $\langle T, R, P\rangle$ і змінюється під впливом подій безпеки $E(t)$ через функцію переходу $f\ x, u$. Керуючий вплив реалізується у вигляді модифікації політик доступу, яка підлягає обов'язковій формальній верифікації перед застосуванням. Результати виконання політик формують зворотний зв'язок, що надходить до систем моніторингу та замикає цикл адаптації.

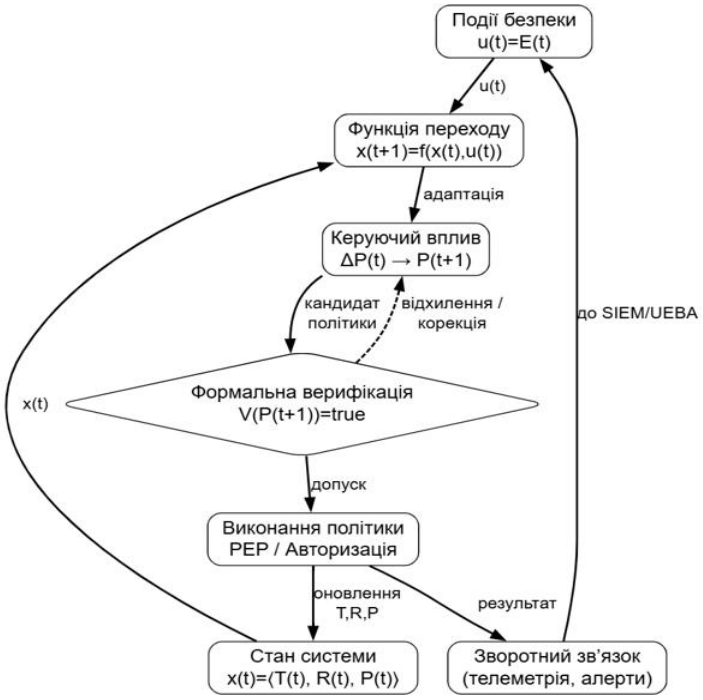

Рис. 3. Динамічна модель замкненого контуру адаптації політик доступу (стан–керування–зворотний зв'язок)

Таким чином, замкнений контур адаптації політик доступу може бути інтерпретований як керована динамічна система зі зворотним зв'язком, у якій стійкість і коректність забезпечуються поєднанням причинно-наслідкового аналізу, багатокритеріальної оптимізації та формальної верифікації. Запропонована математична формалізація створює основу для аналітичного дослідження властивостей такої системи, зокрема її стійкості, збіжності та чутливості до змін ризикового контексту, а також для практичної реалізації керованого й пояснюваного оновлення політик доступу в архітектурі Zero Trust.

7.Формальна верифікація та аналіз небезпечних станів політик

Формальна верифікація є ключовим елементом замкненого контуру адаптації, оскільки гарантує коректність рішень авторизації за умов автоматизованого оновлення правил, зменшуючи ризик накопичення помилкових або надмірних рішень доступу в умовах високої інтенсивності алертів SOC [15-16]. У архітектурі Zero Trust політики доступу розглядаються як формалізована система обмежень, що визначає допустимі стани взаємодії суб'єктів, ресурсів і контекстів. Тому кожна адаптація політик супроводжується перевіркою відсутності небезпечних або суперечливих станів доступу, що є критично важливим для середовищ із високою динамікою обчислювальних

процесів і розподіленою обробкою даних [14], а також для захисту спеціалізованих обчислювальних інфраструктур від шкідливого коду [18]. Формально політика доступу P подається у вигляді множини правил:

$$P = \ r_1, r, \dots, r_n \ , \tag{17}$$

де кожне правило r_i визначає відношення між суб'єктом, ресурсом, дією та контекстом доступу. Простір можливих станів системи визначається множиною [15, 17-18]:

$$S = U \times D \times Res \times C, \tag{18}$$

де U − множина користувачів, D − множина пристроїв, Rec − множина ресурсів, C − множина контекстних атрибутів.

На рис. 4 показано логіку формальної верифікації політик доступу в замкненому контурі Zero Trust. Відображено простір можливих станів системи S, підмножину небезпечних станів S_{unsafe} та перевірку умови коректності $P(s) \Rightarrow s \notin S_{unsafe}$. Схема ілюструє механізм виявлення та блокування небезпечних конфігурацій політик до їх застосування, що забезпечує збереження інваріантів безпеки під час автоматизованої адаптації правил доступу.

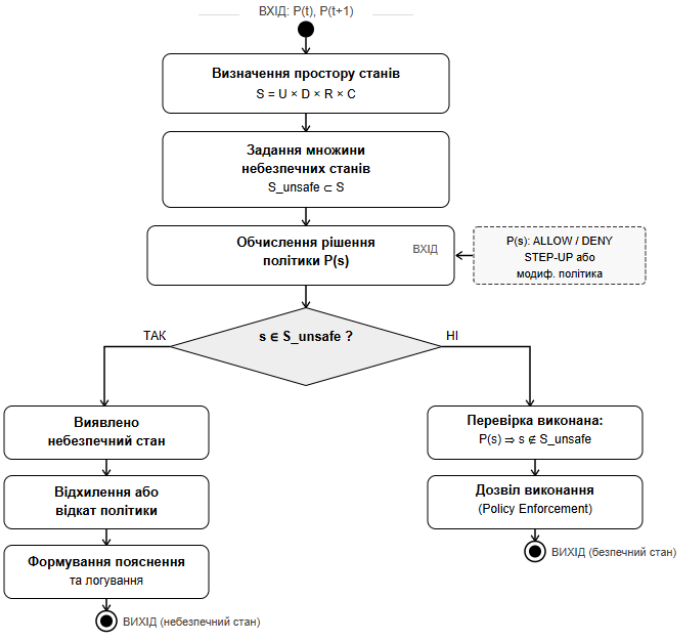

Рис. 4. Перевірка небезпечних станів політик доступу в архітектурі Zero Trust

Небезпечним вважається такий стан $s \in S$, для якого виконується хоча б одна з умов [15, 17-18]:

1. Доступ до критичного ресурсу дозволяється суб'єкту з рівнем довіри нижче допустимого порогу;
2. Існує конфлікт правил, що призводить до неоднозначного рішення (одночасний дозвіл і заборона);
3. Можливе досягнення несанкціонованого доступу через послідовність змін контексту або довіри.

Задача формальної верифікації зводиться до перевірки того, що [16]:

$$\forall s \in S : P(s) \Rightarrow s \notin S_{unsafe}, \tag{19}$$

де S_{unsafe} − множина небезпечних станів.

У запропонованому підході формальна перевірка виконується двічі: для конфігурації політик до адаптації $P(t)$ і після адаптації $P(t+1)$. Це дозволяє не лише запобігати появі нових небезпечних станів, а й виявляти накопичені ризики, які могли виникнути внаслідок тривалої еволюції політик [14,

18]. Такий механізм забезпечує логічну замкненість контуру керування та створює формальні гарантії безпеки для автоматизованих рішень PDP. З практичної точки зору, верифікація умови (19) реалізується за допомогою SMT-розв'язувача Z3: правила політик PBAC та визначення небезпечних станів кодуються у вигляді обмежень SMT-LIB, а Z3 перевіряє незадовільність формули $\exists s \in S: P(s) \wedge s \in S\_unsafe$. Середній час верифікації одного оновлення в рамках проведених експериментів не перевищував 12 мс, що є прийнятним для практичного застосування у контурі реального часу.

8.Алгоритм реалізації замкненого контуру (PDP/PAP)

Реалізація запропонованого замкненого контуру адаптації політик у архітектурі Zero Trust ґрунтується на чітко визначеній взаємодії між компонентами SIEM, модулем причинно-наслідкового аналізу, Policy Decision Point (PDP), Policy Administration Point (PAP) і модулем формальної верифікації [16-17]. Алгоритм функціонування контуру має ітеративний характер і виконується в дискретні моменти часу відповідно до ковзного вікна аналізу подій безпеки.

На рис. 5 подано алгоритм роботи замкненого контуру адаптації політик доступу в архітектурі Zero Trust. Схема відображає послідовність етапів від отримання подій із SIEM/UEBA та їх причинно-наслідкового аналізу до оцінки довіри, прийняття рішення PDP і формування кандидатних змін політик у PAP. Ключовим елементом є блок формальної верифікації, який визначає можливість застосування або відкату змін. Результати виконання політик через PEP формують зворотний зв’язок до SIEM, що замикає ітеративний цикл керування доступом.

На кожній ітерації алгоритму здійснюється агрегація подій безпеки з SIEM/UEBA та їх інтерпретований аналіз із побудовою причинно-наслідкових залежностей [14, 15]. На цій основі формується оцінка деградації довіри суб’єктів і пристроїв, яка разом із поточним контекстом доступу передається до PDP для прийняття рішення авторизації та визначення потреби в адаптації політик із урахуванням багатокритеріальної оптимізації.

У разі ініціювання змін PAP формує кандидатну модифікацію ΔP, що проходить формальну верифікацію; у разі успіху політика оновлюється, а в іншому випадку зміна відхиляється або коригується з поверненням до стабільної конфігурації. Такий підхід забезпечує прозорість і трасованість рішень та гарантує, що адаптація політик є результатом узагальненого аналізу ризикового контексту, а не реакцією на окремі події.

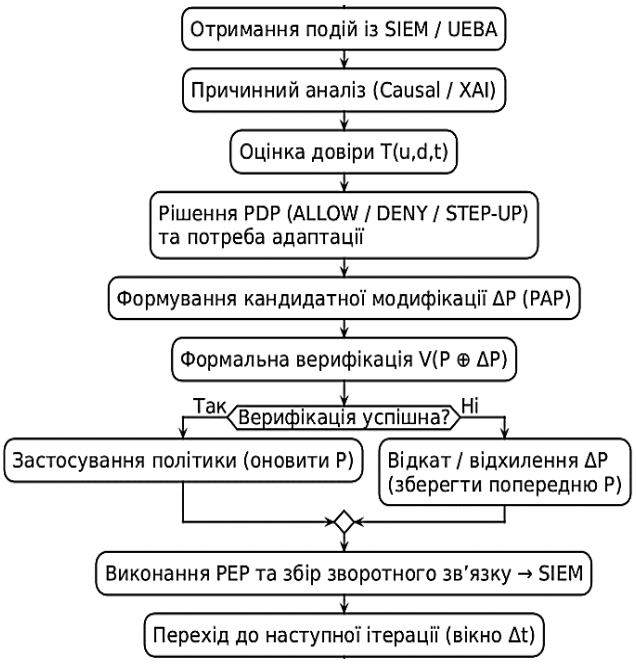

Рис. 5. Алгоритм роботи замкненого контуру PDP / PAP

9.Експериментальна постановка та сценарії оцінювання

Експериментальне дослідження спрямоване на оцінювання ефективності архітектури Zero Trust із пояснюваним і формально верифікованим замкненим контуром адаптації політик доступу. Метою є перевірка здатності підходу забезпечувати керовану адаптацію PBAC-політик у динамічному середовищі загроз зі зниженням ризику несанкціонованого доступу, мінімізацією операційних витрат і збереженням коректності політик. Оцінювання виконано за формалізованими сценаріями S1–S6, що відрізняються рівнем ризику, інтенсивністю подій і типом поведінки суб'єктів доступу та охоплюють як номінальні, так і стресові режими функціонування системи. (табл. 1).

Таблиця 1

Сценарії експериментального оцінювання S1–S6

Сценарій	Рівень ризику	Інтенсивність подій	Тип поведінки	Основний фокус метрик
S1	Низький	Низька	Нормальна	Decision latency (D), Step-up Rate
S2	Середній	Помірна	Поступова деградація	Risk Score, Decision latency (D)
S3	Середній	Короткочасні сплески	Аномалії	Risk Score, Step-up Rate
S4	Високий	Висока	Цілеспрямована атака	Risk Score, Step-up Rate
S5	Високий	Шумові події	Зашумлене середовище	Risk Score, Decision latency (D)
S6	Критичний	Тривала висока	Стійкий ризик	Risk Score, Step-up Rate, Decision latency (D)

У всіх сценаріях додатково контролюється кількість небезпечних станів політик як індикатор коректності адаптації.

Кількісні результати, наведені в табл. 2, свідчать, що в номінальних сценаріях S1–S3 замкнений контур забезпечує низький рівень ризику та стабільну затримку прийняття рішень при помірній частоті застосування step-up автентифікації. У стресових сценаріях S4–S6 зростання ризику супроводжується контрольованим підвищенням step-up без появи небезпечних станів політик ($N_{unsafe} = 0$), що підтверджує ефективність формальної верифікації. Кожен сценарій оцінювався за N імітаційних прогонів; у табл. 2 наведено середні значення (avg). Отримані результати демонструють здатність архітектури зберігати баланс між безпекою та операційною ефективністю в динамічних умовах.

Таблиця 2

Кількісні результати оцінювання замкненого контуру (S1–S6)

Сценарій	R (avg)	D (ms)	F (%)	FAR	FRR	N_unsafe
S1	0.12	18	6	0.004	0.031	0
S2	0.28	22	11	0.006	0.038	0
S3	0.34	27	18	0.009	0.042	0
S4	0.61	33	31	0.014	0.058	0
S5	0.67	29	26	0.016	0.051	0
S6	0.82	41	44	0.019	0.063	0

Значення в табл. 2 наведено у вигляді усереднених показників, отриманих у результаті серій імітаційних запусків замкненого контуру в межах кожного сценарію.

На рис. 6 показано узагальнену динаміку нормалізованих (за методом min-max відносно максимальних значень у сценарії S6) значень показника ризику R, затримки прийняття рішення D та частоти застосування step-up автентифікації F у сценаріях S1–S6. Нормалізація виконана за формулою $\tilde{x} = (x - x\_min) / (x\_max - x\_min)$, де x_min та x_max визначені по всій множині сценаріїв S1–S6.

Смуги похибок на рисунку відображають 95%-ві довірчі інтервали, отримані за результатами N = 30 незалежних прогонів для кожного сценарію. Зі зростанням рівня ризику від номінальних до критичних сценаріїв спостерігається узгоджене підвищення всіх трьох метрик, що відображає адаптивну реакцію замкненого контуру Zero Trust на ускладнення умов доступу при збереженні керованості та коректності політик.

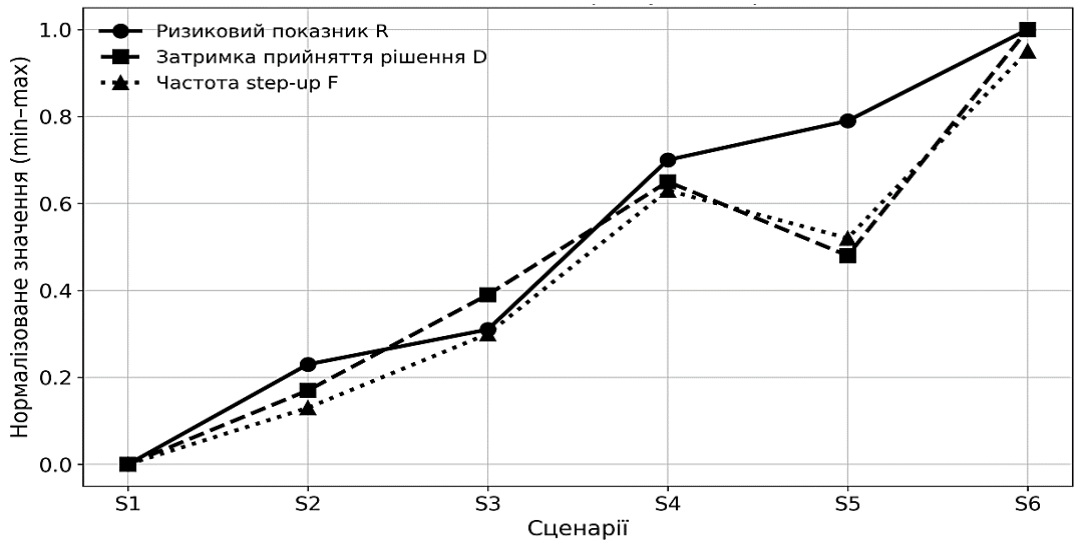

Рис. 6. Узагальнена динаміка ключових метрик у сценаріях S1–S6

Таким чином, для кожного сценарію S1–S6 визначено пріоритетний набір метрик оцінювання, що забезпечує цілеспрямований аналіз поведінки замкненого контуру адаптації політик залежно від рівня ризику та характеру подій безпеки. Такий підхід узгоджує експериментальні результати з цілями дослідження та усуває довільність їх інтерпретації.

Експерименти виконуються у змодельованому корпоративному середовищі, що включає 50 віртуальних користувачів, 80 пристроїв (40 корпоративних та 40 BYOD) і 20 захищених ресурсів різної критичності (від загальнодоступних до конфіденційних). Для кожного сценарію S1–S6 проводилось N = 30 незалежних імітаційних прогонів з тривалістю одного прогону 60 хвилин модельного часу при ковзному вікні аналізу Δt = 5 хв. Потік подій безпеки формується засобами SIEM/UEBA та аналізується в ковзному вікні Δt.

Оцінювання проводиться за шістьма сценаріями S1–S6, що охоплюють як номінальні умови функціонування, так і стресові режими з підвищеним і тривалим ризиком. Такий експериментальний дизайн є структурованим і відтворюваним та підтверджує придатність архітектури Zero Trust для практичного застосування в середовищах із підвищеними вимогами до прозорості й керованості доступу.

10.Висновки

У статті розроблено архітектуру Zero Trust із пояснюваним і формально верифікованим замкненим контуром оновлення політик доступу на основі аналітики SIEM, спрямовану на керовану та безпечну адаптацію рішень авторизації в динамічному середовищі кіберзагроз. На відміну від існуючих підходів, у яких адаптація політик здійснюється евристично або на основі непрозорих моделей машинного навчання, запропонований підхід поєднує причинно-наслідковий аналіз подій безпеки, інтерпретовану оцінку деградації довіри та формальну верифікацію коректності політик до і після їх оновлення.

Запропоновано математичну формалізацію замкненого контуру адаптації PBAC-політик, яка дозволяє розглядати процес керування доступом як динамічну систему зі зворотним зв’язком. Показано, що інтеграція багатокритеріальної оптимізації забезпечує збалансований компроміс між

рівнем безпеки, затримкою прийняття рішень і частотою застосування механізмів step-up автентифікації. Формальна верифікація політик дозволяє гарантувати відсутність небезпечних станів доступу навіть за умов автоматизованого оновлення правил.

Результати експериментального оцінювання в межах сценаріїв S1–S6 підтверджують ефективність запропонованої архітектури, зокрема зниження кількості хибних рішень доступу та підвищення стійкості політик у стресових умовах. Отримані результати свідчать про практичну придатність підходу для використання в корпоративних інформаційно-комунікаційних системах із високими вимогами до прозорості, керованості та безпеки доступу.

Подальші дослідження доцільно спрямувати на розширення моделі причинно-наслідкового аналізу з урахуванням багатоджерельних ланцюгів атак і складних міждоменних сценаріїв доступу, а також на інтеграцію запропонованого замкненого контуру з процесами автоматизованого реагування та управління інцидентами (SOAR/ITSM). Окремим перспективним напрямом є дослідження масштабованості формальної верифікації політик у великих розподілених середовищах і адаптація архітектури до вимог галузевих стандартів і регуляторних рамок у сфері кібербезпеки.

Список літератури

1. *Akbaş, E. (2024). Assessing the frontiers of SIEM technology: A rigorous evaluation and validation of innovative features in SIEM solutions. Proceedings of the 2024 6th International Conference on Information Technology and Computer Communications, 21–29. https://doi.org/10.1145/3704391.3704395*
2. *Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., … Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012*
3. *Caserio, C., Lonetti, F., & Marchetti, E. (2022). A formal validation approach for XACML 3.0 access control policy. Sensors, 22(8), Article 2984. https://doi.org/10.3390/s22082984*
4. *García, R., & Modesti, P. (2024). A practical approach to formal methods: An Eclipse integrated development environment (IDE) for security protocols. Electronics, 13(23), Article 4660. https://doi.org/10.3390/electronics13234660*
5. *González-Granadillo, G., González-Zarzosa, S., & Díaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. Sensors, 21(14), Article 4759. https://doi.org/10.3390/s21144759*
6. *He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. Wireless Communications and Mobile Computing, 2022, 1–13. https://doi.org/10.1155/2022/6476274*
7. *Jalalvand, F., Baruwal Chhetri, M., Nepal, S., & Paris, C. (2024). Alert prioritisation in security operations centres: A systematic survey on criteria and methods. ACM Computing Surveys, 57. https://doi.org/10.1145/3695462*
8. *Jalalvand, F., Baruwal Chhetri, M., Nepal, S., & Paris, C. (2025). Adaptive alert prioritisation in security operations centres via learning to defer with human feedback. arXiv. https://doi.org/10.48550/arXiv.2506.18462*
9. *Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of zero trust security: A brief survey. Entropy, 25(12), Article 1595. https://doi.org/10.3390/e25121595*
10. *Karimi, V., Alencar, P., & Cowan, D. (2017). A formal modeling and analysis approach for access control rules, policies, and their combinations. International Journal of Information Security, 16, 573–594. https://doi.org/10.1007/s10207-016-0314-4*
11. *Li, B., Yang, F., & Zhang, S. (2024). Context-aware risk attribute access control. Mathematics, 12(16), Article 2541. https://doi.org/10.3390/math12162541*
12. *Lund, B. D., Lee, T.-H., Wang, Z., Wang, T., & Mannuru, N. R. (2024). Zero trust cybersecurity: Procedures and considerations in context. Encyclopedia, 4(4), 1520–1533. https://doi.org/10.3390/encyclopedia4040099*
13. *Macaneata, C. (2024). Overview of security information and event management systems. Informatica Economica, 28(1), 15–24.*
14. *Skladannyi, P., Kostiuk, Y., Rzayeva, S., & Mazur, N. (2025). Parallel data processing in extensible hash structures and performance evaluation. (Paralelna obrobka danykh u rozshyriuvanykh khesh-strukturakh ta otsinka yikh produktyvnosti). Cybersecurity: Education, Science, Technique, 3(31), 242–269. https://doi.org/10.28925/2663-4023.2025.31.1015*
15. *Kostiuk, Y., Skladannyi, P., Rzayeva, S., Mazur, N., Cherevyk, V., & Anosov, A. (2025). Features of network attack implementation via TCP/IP protocols. (Osoblyvosti realizatsii merezhevykh atak cherez TCP/IP-protokoly). Cybersecurity: Education, Science, Technique, 1(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915*

16. Tariq, S., Baruwal Chhetri, M., Nepal, S., & Paris, C. (2025). Alert fatigue in security operations centres: Research challenges and opportunities. ACM Computing Surveys, 57. https://doi.org/10.1145/3723158

17. Tendikov, N., Rzayeva, L., Saoud, B., Shayea, I., Bin Azmi, M., Myrzatay, A., & Alnakhli, M. (2024). Security information event management data acquisition and analysis methods with machine learning principles. Results in Engineering, 22, Article 102254. https://doi.org/10.1016/j.rineng.2024.102254

18. Kostiuk, Y., Dovzhenko, N., Mazur, N., Skladannyi, P., & Rzayeva, S. (2025). Methodology for protecting GRID environments against malicious code during computational task execution. (Metodyka zakhystu GRID-seredovyshcha vid shkidlyvoho kodu pid chas vykonannia obchysliuvalnykh zavdan). Cybersecurity: Education, Science, Technique, 3(27), 22–40. https://doi.org/10.28925/2663-4023.2025.27.710

19. Yan, F., Wen, S., Nepal, S., Paris, C., & Xiang, Y. (2022). Explainable machine learning in cybersecurity: A survey. International Journal of Intelligent Systems, 37(1), 1–32. https://doi.org/10.1002/int.23088

ZERO TRUST ARCHITECTURE WITH AN EXPLAINABLE AND FORMALLY VERIFIED CLOSED LOOP FOR ACCESS POLICY UPDATES BASED ON SIEM

Pavlo Skladannyi, Yuliia Kostiuk, Nataliia Mazur

Borys Grinchenko Kyiv Metropolitan University,
Department of Information and Cyber Security named after Professor Volodymyr Buriachok
E-mail: p.skladannyi@kubg.edu.ua, y.kostiuk@kubg.edu.ua, n.mazur@kubg.edu.ua
ORCID: 0000-0002-7775-6039, 0000-0001-5423-0985, 0000-0001-7671-8287

Received: 06.04.2026
Accepted: 20.04.2026
Published: 01.06.2026

© Skladannyi P., Kostiuk Y., Mazur N. 2026

This article is licensed under the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0)

This paper proposes a Zero Trust architecture with an explainable and formally verified closed loop for access policy updates based on SIEM/UEBA analytics. Unlike approaches in which policy adaptation is performed heuristically or using opaque machine learning models, the proposed method integrates causal analysis of security events, an interpretable model of trust degradation, and formal verification of policy correctness before and after updates. Decisions on modifying PBAC policies are derived from causal relationships between SIEM/UEBA signals, access risk states, and policy parameters, represented as explainable chains of the form "event → risk → rule modification." To enable controlled selection of candidate updates, a multi-criteria optimization formulation is introduced that accounts for expected access risk, decision latency, and the frequency of step-up authentication mechanisms. The correctness of updated policies is ensured by a formal verification module that prevents rule conflicts and the emergence of unsafe access states under automated adaptation. Experimental evaluation using formalized scenarios S1–S6 demonstrates the effectiveness of the closed loop under both nominal and stress conditions and confirms the practical applicability of the proposed approach for corporate information and communication systems with increased requirements for access transparency and controllability.

Key words: adaptive authentication, information security, trust management, explainable artificial intelligence, causal analysis, access control policies, formal verification, PBAC, SIEM, Zero Trust.