© Skladannyi P, Kostiuk Y. A formalized approach to integrating policy-based access control and cryptographic protection in zero trust architecture // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 27-39. © This is an open access article under the CC BY 4.0 International license.*

DOI: 10.18372/2225-5036.32.21643

ФОРМАЛІЗОВАНИЙ ПІДХІД ДО ІНТЕГРАЦІЇ POLICY-BASED ACCESS CONTROL ТА КРИПТОГРАФІЧНОГО ЗАХИСТУ В ZERO TRUST ARCHITECTURE

Павло Складанний, Юлія Костюк

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна



СКЛАДАННИЙ Павло Миколайович, кандидат технічних наук, доцент,
Рік та місце народження: 1992 рік, м. Київ, Україна
Освіта: Державний університет телекомунікацій.
Посада: завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Наукові інтереси: кібербезпека, криптографія, криптоаналіз, математичне моделювання.
Публікації: більше 100 наукових публікацій, серед яких монографії, підручники, посібники, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: p.skladannyi@kubg.edu.ua
Orcid ID: 0000-0002-7775-6039



КОСТЮК Юлія Володимирівна, Phd in Computer Science
Рік та місце народження: 1980 рік, м. Київ, Україна
Освіта: Державний торговельно-економічний університет.
Посада: доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Наукові інтереси: захист інформації, комп'ютерні мережі, інформаційно-комунікаційні системи, інформаційно-інтелектуальні системи, нейронні мережі.
Публікації: більше 100 наукових публікацій, серед яких монографія, посібник, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: y.kostiuk@kubg.edu.ua
Orcid ID: 0000-0001-5423-0985

Анотація. *У статті розглянуто проблему розриву між політично-керованим контролем доступу та криптографічним захистом у корпоративних і хмарних середовищах, що впроваджують Zero Trust Architecture (ZTA). Показано, що у більшості практичних реалізацій ZTA рішення щодо доступу зводяться до логічних результатів типу allow/deny або до узагальнених trust-score-оцінок, тоді як криптографічні механізми захисту – керування ключами, параметри шифрування, токени доступу та криптографічні сесії – залишаються статичними або слабко пов'язаними з політиками доступу. Така ізольованість криптографічного рівня знижує адаптивність системи, збільшує потенційне «вікно атаки» та ускладнює узгоджене реагування на зміну контексту, ризику і рівня довіри в режимі реального часу. Запропоновано формалізований підхід до інтеграції Policy-Based Access Control (PBAC) і криптографічного enforcement у межах ZTA, у якому криптографічний режим трактується як керований результат політичного рішення, а не як незалежний інфраструктурний компонент. Підхід базується на поданні доступу як динамічного стану, що включає ідентичність суб'єкта, ресурс, дію, контекст виконання, рівень довіри, оцінку ризику та криптографічний стан сесії доступу. Формально визначено відображення PBAC, яке повертає не лише логічне рішення доступу, а й криптографічну політику, що задає клас алгоритму, параметри ключа, режим застосування та час життя криптографічної сесії з урахуванням ризику, довіри та чутливості ресурсу. Розроблено алгоритмічний контур взаємодії PDP–PEP–Crypto Engine із циклічною переоцінкою політик за подіївими змінами безпекового стану, що забезпечує безперервну відповідність принципам Zero Trust і динамічне скорочення потенційного вікна компрометації. Практична цінність роботи полягає у створенні теоретичного підґрунтя для проєктування Zero Trust Access Management-систем, у яких криптографічні параметри автоматично узгоджуються з політиками доступу та еволюцією контексту експлуатації.*

Ключові слова: *Zero Trust Architecture, Policy-Based Access Control, криптографічний enforcement, PDP/PEP, керування ключами, ризик-адаптація, динамічна довіра, криптографічні сесії, контекст доступу.*

Постановка проблеми

Сучасні корпоративні та хмарні інформаційні системи дедалі частіше будуються відповідно до парадигми Zero Trust Architecture (ZTA), яка передбачає відмову від неявної довіри, безперервну перевірку суб'єктів доступу та динамічне врахування контексту виконання операцій [1, 5, 8]. У межах ZTA ключову роль відіграють механізми керування доступом, які мають забезпечувати адаптивне прийняття рішень з урахуванням ідентичності користувача, стану пристрою, поведінкових характеристик, рівня довіри та поточного ризику [3, 6, 10-11]. Водночас у більшості практичних реалізацій

© Skladannyi P, Kostiuk Y. A formalized approach to integrating policy-based access control and cryptographic protection in zero trust architecture // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 27-39. © This is an open access article under the CC BY 4.0 International license.*

Zero Trust контроль доступу обмежується логічними рішеннями типу *allow/deny*, тоді як механізми криптографічного захисту залишаються статичними або слабко пов'язаними з політиками доступу.

Policy-Based Access Control (PBAC) розглядається як перспективний підхід до реалізації гнучкого керування доступом у складних динамічних середовищах, оскільки дозволяє формалізувати правила доступу у вигляді політик, що враховують контекст, ризик та бізнес-вимоги [4, 6, 13]. Проте на сьогодні PBAC здебільшого застосовується як логічний механізм прийняття рішень без чітко визначеного зв'язку з криптографічними засобами захисту, такими як керування ключами, параметрами шифрування, токенами доступу та криптографічними сесіями [3, 17]. У результаті криптографічний рівень функціонує ізольовано від системи керування доступом, що суперечить принципам Zero Trust та призводить до надмірних або, навпаки, недостатніх рівнів захисту.

Існуючі підходи до інтеграції криптографічних механізмів у Zero Trust переважно зосереджені на використанні стандартних протоколів захищеного обміну (TLS, VPN, токени доступу), не пропонуючи формалізованої моделі керування криптографічними параметрами на основі політик та динамічного стану безпеки [2, 8-9]. Відсутність формального опису взаємодії між компонентами Policy Decision Point (PDP), Policy Enforcement Point (PEP) та криптографічними механізмами унеможливлює побудову адаптивних систем, у яких рішення про доступ безпосередньо впливають на рівень, режим і параметри криптографічного захисту.

Таким чином, наукова проблема полягає у відсутності формалізованого підходу до інтеграції Policy-Based Access Control та криптографічного захисту в межах Zero Trust Architecture, який би дозволяв розглядати криптографічні механізми як керований елемент політики доступу, а не як незалежний інфраструктурний компонент [1, 3, 5, 10, 17]. Невирішеним залишається завдання побудови алгоритмічної моделі прийняття рішень, у якій оцінка контексту, ризику та довіри використовується не лише для визначення дозволів доступу, а й для динамічного керування криптографічними параметрами, такими як тип алгоритму, розмір ключа, час життя ключів і сесій, а також режими криптографічного захисту.

Розв'язання цієї проблеми є необхідною передумовою для створення адаптивних Zero Trust-систем нового покоління, здатних забезпечити узгоджене та контекстно-залежне поєднання логічного контролю доступу й криптографічного захисту інформаційних ресурсів.

Аналіз останніх досліджень і публікацій

Сучасні дослідження у сфері Zero Trust Architecture (ZTA) свідчать про перехід від периметрових моделей безпеки до динамічних, контекстно-орієнтованих підходів керування доступом. У роботі E. B. Fernandez та A. Brazhuk [1] наведено критичний аналіз Zero Trust Architecture як архітектурної парадигми, у якому обґрунтовується необхідність формалізації процесів контролю доступу та безперервної перевірки суб'єктів. Водночас автори розглядають криптографічні механізми переважно як інфраструктурний рівень, що не інтегрований безпосередньо в політичний контур прийняття рішень.

Подальший розвиток Zero Trust у прикладних доменах, зокрема в IoT, представлено в дослідженні C. Liu, R. Tan, Y. Wu та ін. [2], де систематизовано наукові підходи до реалізації Zero Trust у розподілених середовищах. Автори підкреслюють важливість контекстної та поведінкової оцінки безпеки, однак питання динамічного керування криптографічними параметрами залишаються поза межами розгляду. Аналогічну тенденцію демонструє робота R. Wang, C. Li, K. Zhang та ін. [3], у якій запропоновано модель динамічного контролю доступу для хмарних обчислень у межах Zero Trust, проте криптографічний захист застосовується у фіксованому вигляді та не пов'язується з результатами політичних рішень.

Питання формалізації політик доступу та перевірки їх коректності розглядаються у роботі C. Caserio, F. Lonetti та E. Marchetti [4], де запропоновано формальний підхід до валідації політик XACML 3.0. Хоча цей підхід суттєво підвищує надійність систем керування доступом, криптографічні механізми в ньому залишаються зовнішнім елементом і не інтегруються у формальну модель прийняття рішень.

Систематичний огляд проблем впровадження Zero Trust Architecture у різних галузях представлено у роботі S. Mushtaq, M. Mohsin та M. M. Mushtaq [5]. Автори ідентифікують відсутність узгодженості між політиками доступу та механізмами захисту як одну з ключових практичних проблем, проте не пропонують формалізованого підходу до інтеграції криптографічного захисту в політичний контур Zero Trust.

Значний внесок у розвиток систем керування доступом зробили J. Glöckler, J. Sedlmeir, M. Frank та ін. [6], які проаналізували вимоги до Identity and Access Management у корпоративних середовищах. Автори наголошують на необхідності гнучких політик і контекстної оцінки, однак криптографічні аспекти розглядаються переважно в межах автентифікації та захищеного обміну, без можливості їх адаптації на основі політик доступу.

Окремий напрям досліджень пов'язаний із використанням блокчейн-технологій та сучасних криптографічних схем у Zero Trust. Так, S. Nie, J. Ren, R. Wu та ін. [7] запропонували Zero-Trust-механізм доступу з використанням inner-product encryption у середовищі IoT, а U. Roy та N. Ghosh [9] розробили блокчейн-орієнтовану модель керування доступом. Незважаючи на інноваційність цих рішень, вони орієнтовані на конкретні технології й не формують

© Skladannyi P, Kostiuk Y. A formalized approach to integrating policy-based access control and cryptographic protection in zero trust architecture // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 27-39. © This is an open access article under the CC BY 4.0 International license.*

узагальненої формалізованої моделі інтеграції політик доступу та криптографічного enforcement.

Огляд процедурних та організаційних аспектів Zero Trust подано у роботі B. D. Lund, T.-H. Lee, Z. Wang та ін. [8], де Zero Trust розглядається як набір практик і рекомендацій. Проте формалізований зв'язок між прийняттям рішень щодо доступу та параметрами криптографічного захисту в цій роботі не аналізується.

Моделі доступу, засновані на оцінці довіри, розглянуто у дослідженні E. Jeong та D. Yang [10], де запропоновано trust-score-орієнтований підхід до Zero Trust Architecture. Хоча така модель забезпечує адаптивність логічних рішень доступу, криптографічні механізми в ній залишаються статичними та не залежать від значень довіри й ризику.

Отже, проведений аналіз літературних джерел показує, що, незважаючи на активний розвиток Zero Trust Architecture, Policy-Based Access Control і ризик-орієнтованих моделей доступу, проблема формалізованої інтеграції політик доступу та криптографічного захисту залишається недостатньо дослідженою [1, 3, 5, 8, 15, 17]. У більшості існуючих робіт криптографічні механізми функціонують ізольовано від процесу прийняття рішень щодо доступу, що обґрунтовує актуальність запропонованого у статті підходу.

Проведений аналіз сучасних наукових досліджень свідчить, що, незважаючи на значний прогрес у розвитку Zero Trust Architecture, Policy-Based Access Control та ризик-орієнтованих моделей доступу, у наявних підходах зберігається низка принципових невирішених питань [1, 5-6]. По-перше, у більшості робіт рішення щодо доступу мають переважно логічний характер (allow/deny або trust-score-based), тоді як криптографічні механізми розглядаються як фіксований або наперед визначений рівень захисту, що не інтегрований безпосередньо в політичний контур прийняття рішень [3, 10]. По-друге, відсутній формалізований опис взаємодії між компонентами Policy Decision Point, Policy Enforcement Point та криптографічними механізмами, що унеможливлює побудову алгоритмічно керованих систем, у яких параметри криптографічного захисту динамічно адаптуються до контексту, ризику та рівня довіри [4, 13]. По-третє, наявні моделі Zero Trust здебільшого не розглядають криптографічний стан сесії доступу [19, 21-22] як частину загального стану безпеки системи, що обмежує можливість безперервної адаптації захисту в умовах еволюції безпекового контексту.

Таким чином, залишається відкритим завдання розроблення формалізованого підходу, у якому Policy-Based Access Control і криптографічний захист інтегруються в межах єдиного алгоритмічного контуру Zero Trust Architecture [1, 3, 5, 19], а криптографічні параметри визначаються як результат політичного рішення доступу [16, 20, 24]. Саме усунення зазначеного наукового розриву й становить предмет дослідження, представленого у статті.

Мета та постановка завдання

Метою дослідження є розроблення формалізованого підходу до інтеграції Policy-Based Access Control та криптографічного захисту в межах Zero Trust Architecture, який забезпечує узгоджене й адаптивне керування як логічними рішеннями доступу, так і параметрами криптографічного захисту на основі контексту виконання операцій, рівня довіри та поточного ризику [1, 15, 17]. Запропонований підхід орієнтований на подолання розриву між механізмами прийняття рішень щодо доступу та криптографічними засобами захисту [19-22], які у більшості існуючих реалізацій функціонують ізольовано й не враховують динаміку безпекового стану середовища Zero Trust.

Для досягнення поставленої мети у роботі ставиться завдання формалізувати стан доступу в Zero Trust Architecture як сукупність ідентифікаційних, контекстних, поведінкових і ризик-орієнтованих параметрів, доповнених криптографічним станом сесії доступу [2, 6, 10-11]. Такий підхід дозволяє розглядати криптографічні механізми не як статичний інфраструктурний компонент, а як керований елемент політики доступу, параметри якого можуть змінюватися в процесі виконання операцій відповідно до вимог безпеки.

У межах дослідження передбачається побудова формальної моделі Policy-Based Access Control, у якій результат прийняття рішення визначається не лише дозволом або забороною виконання дії, а й формуванням криптографічної політики, що задає параметри захисту інформаційної взаємодії [3-4, 13]. Така модель має забезпечувати можливість динамічного керування криптографічними параметрами, зокрема вибором алгоритмів, характеристик ключів, режимів шифрування та часу життя криптографічних сесій [7, 15, 17, 23], залежно від поточного рівня довіри, ризику та чутливості інформаційних ресурсів.

Окреме завдання дослідження полягає у формалізації алгоритмічної взаємодії між компонентами Policy Decision Point, Policy Enforcement Point та криптографічними механізмами захисту, що забезпечує узгоджене застосування політик доступу та їх безперервну переоцінку у відповідь на подієві зміни в середовищі Zero Trust [4, 8, 13]. У такій моделі Policy Decision Point виконує функцію оцінювання контексту [10-11, 16], ризику й довіри та визначає як логічні рішення доступу, так і параметри криптографічного захисту, тоді як Policy Enforcement Point забезпечує їхнє виконання та ініціює повторну оцінку політик у разі зміни безпекового стану.

Методологічну основу дослідження становлять методи формалізованого опису систем керування доступом, теорії множин і функціонального аналізу

© Skladannyi P, Kostiuk Y. A formalized approach to integrating policy-based access control and cryptographic protection in zero trust architecture // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 27-39. © This is an open access article under the CC BY 4.0 International license.*

для подання політик та рішень доступу, а також алгоритмічні методи моделювання процесів прийняття рішень у динамічних системах [4, 13]. Для опису взаємодії компонентів Zero Trust Architecture застосовано структурно-функціональний та системний підходи, що дозволяє узгоджено поєднати логічний контроль доступу з криптографічним enforcement [1, 8]. Аналіз адаптивності криптографічного захисту ґрунтується на ризик-орієнтованому підході та методах контекстної оцінки безпеки, які забезпечують зміну параметрів криптографічних механізмів залежно від поточного стану середовища [19-22, 24]. Отримані моделі аналізуються з позицій відповідності принципам Zero Trust та можливості їх практичної реалізації у корпоративних і хмарних інформаційних системах.

Реалізація зазначених завдань дозволяє сформувати цілісну формалізовану модель інтеграції Policy-Based Access Control і криптографічного захисту в Zero Trust Architecture, яка створює теоретичне підґрунтя для побудови адаптивних систем керування доступом із динамічним криптографічним enforcement та відповідає сучасним вимогам до захисту інформаційних ресурсів у корпоративних і хмарних середовищах.

Виклад основного матеріалу дослідження

У межах дослідження Zero Trust Architecture розглядається не як статична архітектурна модель або сукупність технічних компонентів, а як динамічна система керованих станів безпеки, що еволюціонують у часі під впливом контекстних, поведінкових і ризик-орієнтованих факторів [8, 10-11]. Такий підхід дозволяє відійти від традиційного трактування контролю доступу як одноразового акту авторизації та перейти до розуміння доступу як безперервного процесу, у якому кожна операція виконується в межах поточного безпекового стану системи.

На відміну від класичних моделей доступу, де рішення приймається на основі фіксованого набору атрибутів або ролей, Zero Trust у запропонованій інтерпретації описується як простір станів, у якому кожен стан характеризується сукупністю параметрів, що відображають актуальний рівень довіри, ризику та контексту взаємодії [6, 10]. Перехід між станами ініціюється подіями безпеки, змінами середовища виконання або поведінковими відхиленнями, що унеможливлює існування стабільного «довіреного» стану доступу протягом усього часу сесії.

У такій постановці Zero Trust виступає механізмом безперервної адаптації політик доступу, де кожна зміна стану безпеки потребує переоцінки умов виконання операцій. Це означає, що рішення щодо доступу та відповідні механізми захисту мають динамічно узгоджуватися з поточним станом системи, а не визначатися наперед [3, 10]. Зазначена властивість принципово відрізняє Zero Trust від периметрових моделей безпеки та створює підґрунтя для інтеграції адаптивних політично-керованих механізмів захисту.

Розгляд Zero Trust як динамічної системи станів дозволяє формалізувати керування доступом у вигляді процесу, що розгортається у часі та реагує на зміну безпекового контексту. У цьому процесі рішення щодо доступу більше не є бінарними та остаточними, а набувають характеру умовних і тимчасових дозволів, чинність яких залежить від збереження допустимого рівня безпеки. Така модель природним чином підтримує безперервну перевірку суб'єктів і ресурсів, що є базовою вимогою Zero Trust Architecture.

Важливою особливістю запропонованого підходу є те, що динамічний стан Zero Trust визначає не лише можливість виконання дії, а й умови її безпечної реалізації. Це відкриває можливість розглядати механізми захисту, зокрема криптографічні, як змінні параметри системи, що підлягають адаптації разом зі зміною стану безпеки [19, 21-22, 24]. Таким чином, Zero Trust у даній роботі інтерпретується як керована динамічна система, у якій політики доступу та механізми захисту формують єдиний контур прийняття рішень і виконання безпекових вимог.

На рис. 1 подано компактний алгоритмічний контур інтеграції Policy-Based Access Control та криптографічного захисту в Zero Trust Architecture. Рішення щодо доступу формується в Policy Decision Point на основі контексту, оцінки довіри та ризику у вигляді узгодженої пари $\langle d_t, \hat{k}_t \rangle$, що поєднує логічне рішення доступу та криптографічну політику сесії [13, 19]. Policy Enforcement Point виконує рішення та ініціює повторну переоцінку за подіями безпеки, забезпечуючи безперервну адаптацію криптографічного enforcement до динамічного безпекового контексту Zero Trust.

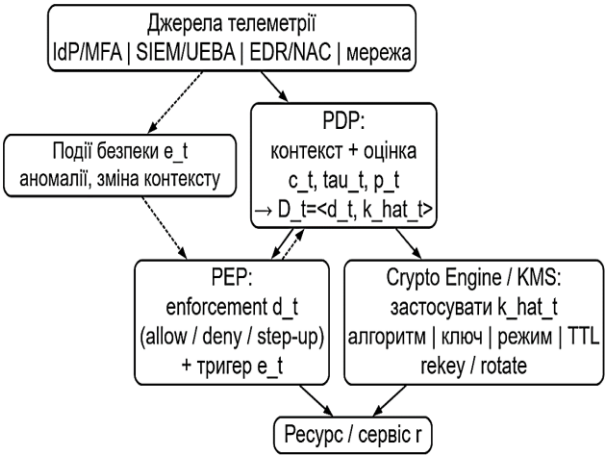


Рис. 1. Алгоритмічний контур інтеграції Policy-Based Access Control та криптографічного enforcement у Zero Trust Architecture

© Skladannyi P, Kostiuk Y. A formalized approach to integrating policy-based access control and cryptographic protection in zero trust architecture // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 27-39. © This is an open access article under the CC BY 4.0 International license.*

Запропоноване трактування Zero Trust Architecture створює концептуальну основу для подальшої формалізації інтеграції Policy-Based Access Control і криптографічного захисту, оскільки дозволяє описувати ці механізми не як незалежні компоненти, а як узгоджені елементи єдиної динамічної системи керування безпекою доступу.

У межах запропонованого підходу криптографічний захист розглядається не як фіксований інфраструктурний рівень, а як керований механізм, параметри якого визначаються безпосередньо результатом політичного рішення Policy-Based Access Control [15, 17]. Така постановка дозволяє інтегрувати криптографічні механізми в контур прийняття рішень Zero Trust Architecture та забезпечити їхню адаптацію до динамічного безпекового стану системи.

Для узгодженого поєднання Policy-Based Access Control і криптографічного enforcement у ZTA криптографічний рівень розглядається як формально керований контур із визначеними цілями безпеки [13]. У межах моделі припускається наявність супротивника типу Dolev–Yao на мережевому рівні, здатного перехоплювати, модифікувати та повторно відтворювати повідомлення (MITM/replay), а також сценарії часткової компрометації секретів сесії (витік токена доступу, витік сеансового ключа або компрометація кінцевого пристрою) [14, 17, 19, 21-22]. Метою запропонованого підходу є мінімізація вікна впливу компрометації за рахунок динамічного скорочення часу життя криптографічних сесій та керованого перегенерування ключового матеріалу.

Формально, для кожної сесії доступу визначається набір криптографічних властивостей, які повинні виконуватися залежно від поточного стану безпеки: конфіденційність даних на рівні сесії (умовна стійкість до пасивного перехоплення), цілісність і автентичність повідомлень (захист від підміни/вставки), стійкість до повторного відтворення (replay resistance), (iv) пряме секретування (forward secrecy) для сценаріїв, де критично обмежити вплив компрометації довгострокових секретів [17, 19, 21-23]. Під час ескалації ризику система має переходити до режимів, у яких властивість прямого секретування та короткоживучі ключі/сесії стають обов'язковими.

Для формалізації контролю replay вводиться параметр криптографічної синхронізації (nonce/sequence epoch), який визначає допустимий інтервал повторного використання ключового матеріалу. Нехай seg_t — монотонна лічильна змінна або номер епохи, тоді будь-яке повідомлення m_t у межах сесії супроводжується тегом автентичності tag_t, що обчислюється на основі seg_t, а політика визначає допустимі правила оновлення seg_t та умови примусового rekey.

Таким чином, криптографія в запропонованій моделі виступає не «фоновим» інфраструктурним компонентом, а формально визначеним механізмом, який має керовано змінювати профіль гарантій у відповідь на динаміку контексту, довіри та ризику в Zero Trust.

Нехай у момент часу t стан доступу описується вектором [3, 6, 10]:

$$S_t = \langle u, r, a, c_t, \tau_t, p_t \rangle, \quad (1)$$

де u — суб'єкт доступу, r — ресурс, a — запитувана дія, c_t — контекст виконання операції, $\tau_t \in [0,1]$ — поточний рівень довіри, $\tau_t \in [0,1]$ — оцінка ризику. На відміну від традиційних моделей керування доступом, у даній роботі вектор стану розширюється криптографічною складовою, що відображає умови захисту інформаційної взаємодії [1, 3]:

$$S_t^* = \langle S_t, k_t \rangle, \quad (2)$$

де k_t — криптографічний стан сеансу доступу.

Криптографічний стан k_t визначається як впорядкована множина параметрів [21-22]:

$$k_t = \langle \mathcal{A}_t, \ell_t, \theta_t, \delta_t \rangle, \quad (3)$$

де $\mathcal{A}_t$ — клас криптографічного алгоритму, ℓ_t — характеристика криптографічного ключа, θ_t — режим застосування криптографічного механізму, δ_t — допустимий час життя криптографічної сесії. Таким чином, криптографія набуває формального опису, що дозволяє розглядати її як змінний параметр у процесі прийняття рішень щодо доступу.

Для усунення неоднозначності трактування криптографічного стану доцільно відокремити (а) опис криптографічних гарантій та обмежень (профіль) від (б) поточного виконуваного стану (епоха/TTL/ознаки прив'язки) [19-23]. Введемо множину криптографічних профілів:

$$\Theta = \{\theta^{(1)}, \theta^{(2)}, \dots, \theta^{(M)}\}, \quad (4)$$

де кожен профіль $\theta \in \Theta$ задає узгоджений набір вимог до захисту сесії: клас механізму (наприклад, AEAD), мінімальну довжину ключа, вимогу прямого секретування (PFS), політику ротації ключів, вимогу прив'язки токена до каналу/пристрою та правила допустимих протокольних параметрів.

Тоді криптографічний стан сесії доцільно представити у вигляді:

$$k_t = \langle \theta_t, epoch_t, \delta_t, p_t, \beta_t \rangle, \quad (5)$$

де $\theta_t \in \Theta$ — активний криптографічний профіль, $epoch_t$ — номер епохи (версія ключового матеріалу), δ_t — час життя криптографічної сесії, p_t — інтервал/умова ротації ключів (rekey policy), β_t — ознака прив'язки (binding) сесії до контексту (наприклад, каналу, пристрою або PoP-токена).

У такій постановці політико-кероване рішення PBAC визначається відображенням:

$$f_{RBAC} : S_t^* \times \prod \to D_t, \quad (6)$$

де $\prod$ — множина політик доступу, а результат рішення [3, 10, 13]:

$$D_t = \langle d_t, \hat{k}_t \rangle, \quad (7)$$

містить не лише логічний дозвіл $d_t \in \{allow, deny, step-up\}$, але й оновлений криптографічний стан $\hat{k}_t$. Таким чином, криптографічний enforcement безпосередньо

© Skladannyi P, Kostiuk Y. A formalized approach to integrating policy-based access control and cryptographic protection in zero trust architecture // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 27-39. © This is an open access article under the CC BY 4.0 International license.*

випливає з політичного рішення та є його невід'ємною складовою.

Формування криптографічного стану визначається [3, 10, 19]:

$$\hat{k}_t = g(\tau_t, p_t, \sigma(r), c_t), \quad (8)$$

де $\sigma(r)$ — функція чутливості ресурсу. Зазначене відображення реалізує принцип ризик-орієнтованого криптографічного захисту, за якого підвищення рівня ризику або зниження довіри призводить до автоматичної корекції параметрів криптографічного механізму.

На рис. 2. наведено двовимірну карту відповідності між рівнем ризику p_t, рівнем довіри τ_t, рішенням доступу d_t та криптографічним профілем θ_t. Кожна зона карти визначає режим криптографічного enforcement і час життя сесії, відображаючи інтеграцію PBAC і криптографічного захисту в Zero Trust.

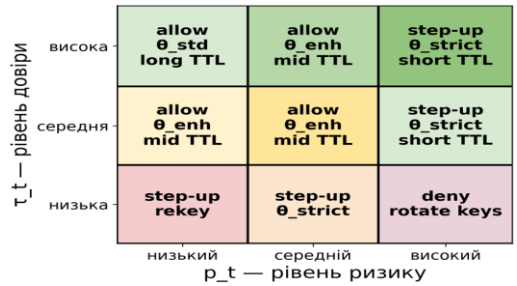


Рис. 2. Двовимірна карта політичного рішення Policy-Based Access Control та криптографічного профілю в Zero Trust Architecture

Для усунення інтерпретаційної неоднозначності двовимірної карти доцільно доповнити її табличною специфікацією профілів θ_t, у якій кожна зона (p_t,τ_t) відповідає формально визначеному набору криптографічних гарантій і обмежень. Така таблиця дозволяє явно пов'язати політичне рішення з параметрами AEAD, вимогою PFS, правилами ротації та прив'язкою токенів, що особливо важливо для практичної реалізації в корпоративних і хмарних ZTA-середовищах. Для однозначної інтерпретації двовимірної карти (p_t,τ_t) введено компактну табличну відповідність зон ризику та довіри криптографічним профілям θ_t (табл. 1).

Таблиця 1

Відповідність ризику та довіри криптографічним профілям

Зона	Умова p_t, τ_t	PBAC	θ_t	Crypto enforcement
1	$p_t < p_1$, $\tau_t \geq \tau_1$	allow	θ_{std}	AEAD, PFS optional, $\delta_t \approx \delta_{max}$
2	$p_1 \leq p_t < p_2$ або $\tau_2 \leq \tau_t < \tau_1$	allow / step-up	θ_{enh}	AEAD+, PFS, $\beta_t = 1, \delta_t \downarrow rekey$
3	$p_t \geq p_2$ або $\tau_t < \tau_2$	step-up / deny	θ_{strict}	PFS, короткий TTL, rekey, revoke, $\beta_t = 1$

Зокрема, час життя криптографічної сесії може бути формалізований як [10, 19]:

$$\delta_t = \delta_{max} \cdot \tau_t \cdot (1 - p_t), \quad (9)$$

що забезпечує скорочення вікна атаки за умов деградації безпекового стану.

Поверхня на рис. 3 ілюструє зменшення TTL зі зростанням ризику та його збільшення зі зростанням довіри, що відображає скорочення потенційного «вікна атаки» у ZTA.

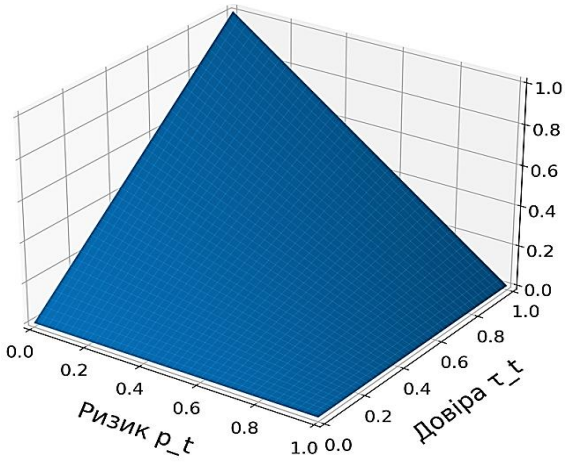


Рис. 3. Поверхня залежності нормалізованого часу життя криптографічної сесії δ_t / δ_{max} від ризику p_t та довіри τ_t

У межах Zero Trust Architecture кожна подія безпеки e_t ініціює перехід системи до нового стану:

$$S^*_{t+1} = \Phi(S^*_t, e_t), \quad (10)$$

де оператор Φ забезпечує переоцінку як логічних, так і криптографічних параметрів доступу [10-11, 19]. Це означає, що криптографічний enforcement не є фіксованим на час сесії, а підлягає безперервному коригуванню відповідно до еволюції безпекового контексту.



Рис. 4. Безперервний цикл Zero Trust enforcement з подієвою переоцінкою доступу та криптографічних параметрів

На рис. 4 подано компактний цикл реалізації Zero Trust, у якому рішення доступу формується на основі поточної оцінки контексту та ризику і супроводжується оновленням криптографічних параметрів сесії. Моніторинг та події безпеки

© Skladannyi P, Kostiuk Y. A formalized approach to integrating policy-based access control and cryptographic protection in zero trust architecture // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 27-39. © This is an open access article under the CC BY 4.0 International license.*

ініціюють повторну переоцінку, що забезпечує доступ як безперервний процес у часі.

Запропонована формалізація дозволяє розглядати криптографічний захист як керований результат політичного рішення PBAC, що принципово відрізняється від традиційних підходів, у яких криптографічні механізми застосовуються незалежно від процесу прийняття рішень щодо доступу [13, 15]. Такий підхід створює єдиний контур керування доступом і захистом, у межах якого логічні та криптографічні механізми узгоджено адаптуються до вимог Zero Trust Architecture.

У межах Zero Trust Architecture криптографічний захист не може розглядатися як статичний набір параметрів, визначених на момент встановлення сесії доступу, оскільки безпековий стан системи є динамічним і змінюється під впливом контекстних та поведінкових факторів. У запропонованому підході адаптація криптографічних параметрів розглядається як безперервний процес, керований оцінкою ризику та рівня довіри, що формується внаслідок аналізу поточного контексту взаємодії.

Нехай контекст доступу в момент часу t задається множиною [11-12]:

$$c_t = c_t^{(1)}, c_t^{(2)}, \dots, c_t^{(n)}, \quad (11)$$

де елементи $c_t^{(i)}$ відображають параметри середовища виконання операції, зокрема характеристики пристрою, мережеві умови, часові обмеження та поведінкові ознаки. Оцінка ризику p_t визначається як агрегована функція контекстних параметрів [10, 12, 16]:

$$p_t = \mathcal{R}(c_t), \quad (12)$$

де $\mathcal{R} : C \to [0,1]$ — функція ризик-орієнтованої оцінки, що відображає ймовірність компрометації або небажаної поведінки в поточному стані системи.

Криптографічні параметри захисту в запропонованій моделі залежать не від окремих значень контексту, а від інтегрованої оцінки ризику та довіри. Зокрема, характеристика криптографічного ключа ℓ_t визначається як монотонно зростаюча функція ризику:

$$\ell_t = \ell_{min} + (\ell_{max} - \ell_{min}) \cdot p_t, \quad (13)$$

що забезпечує автоматичне посилення криптографічного захисту за умов підвищення рівня загрози [19, 21-23]. Аналогічно, допустимий час життя криптографічної сесії δ_t зменшується зі зростанням ризику та зниженням довіри $\delta_t = \delta_{max} \cdot \tau_t \cdot (1 - p_t)$, де $\tau_t \in [0,1]$ — поточний рівень довіри до суб'єкта доступу.

Адаптація режиму застосування криптографічного механізму також формалізується як функція ризику:

$$\theta_t = \begin{cases} \theta_{std}, & p_t < p_1, \\ \theta_{enh}, & p_1 \le p_t < p_2, \\ \theta_{strict}, & p_t \ge p_2, \end{cases} \quad (14)$$

де $\theta_{std}, \theta_{enh}, \theta_{strict}$ відповідають різним рівням криптографічної жорсткості, p_1, p_2 — порогові значення ризику [17, 19]. Такий підхід забезпечує дискретно-неперервну адаптацію криптографічного захисту, що поєднує гнучкість і керованість.

На рис. 5 показано залежність нормалізованого часу життя криптографічної сесії δ_t / δ_{max} від рівня ризику p_t за фіксованих значень довіри τ_t. Зі зростанням ризику допустимий час життя сесії монотонно зменшується, що забезпечує скорочення потенційного вікна атаки. Вертикальні межі відповідають переходам між стандартним, посиленим і строгим криптографічними режимами захисту.

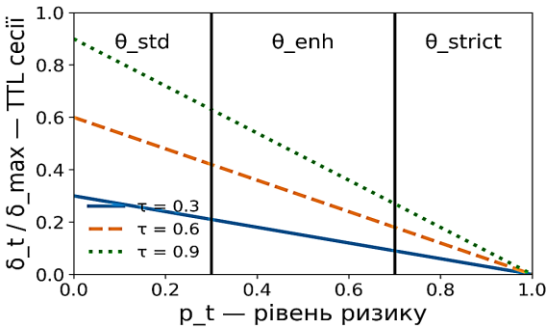


Рис. 5. Адаптація часу життя криптографічної сесії залежно від рівня ризику та довіри

У середовищі Zero Trust кожна подія безпеки ete_tet, що змінює контекст доступу, призводить до переоцінки ризику та, відповідно, до корекції криптографічного стану [8-11]:

$$k_{t+1} = \Psi(k_t, p_t, \tau_t, e_t), \quad (15)$$

де оператор Ψ реалізує механізм безперервної криптографічної адаптації. Таким чином, криптографічний захист стає чутливим до еволюції контексту та здатним реагувати на загрози ще до завершення сесії доступу.

Практична реалізація політико-керованого криптографічного enforcement потребує формалізації життєвого циклу ключового матеріалу в межах Zero Trust [19-23]. У запропонованій моделі використовується ієрархічний підхід до ключів: довгостроковий секрет (кореневий ключ або ключ KMS/HSM) не застосовується безпосередньо для шифрування трафіку чи даних, а використовується для керованого виведення сеансових ключів.

Нехай K^{root} — кореневий секрет (зокрема в KMS/HSM), тоді сеансовий ключ в епосі $epoch_t$ визначається як функція виведення [19, 21, 23]:

$$K_t^{sess} = KDF(K^{root}, ctx_t, epoch_t), \quad (16)$$

де $KDF(\cdot)$ — криптографічно стійка функція виведення ключів, ctx_t — компактне подання

© Skladannyi P, Kostiuk Y. A formalized approach to integrating policy-based access control and cryptographic protection in zero trust architecture // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 27-39. © This is an open access article under the CC BY 4.0 International license.*

контексту сесії (ідентифікатор суб'єкта, ресурсу, каналу, політики тощо). Такий механізм забезпечує розділення ключів (key separation) і зменшує вплив часткової компрометації.

Політика ротації ключів задається як керована функція:

$$epoch_{t+1} = epoch_t + \mathcal{I}\{\Gamma(p_t, \tau_t, e_t) = 1\}, \quad (17)$$

де $\Gamma(\cdot)$ — тригер ротації, $\mathcal{I}\{\cdot\}$ — індикатор. Наприклад, $\Gamma = 1$ при досягненні порогів $p_t \geq p_2$, різкому зростанні ризику $\Delta p_t > \varepsilon$, події компрометації токена/ключа або при переході в режим step-up [10-11, 19]. Таким чином, rekey стає не «плановою процедурою», а частиною реакції Zero Trust на зміну безпекового стану.

Для зменшення вікна впливу компрометації вводиться правило відкликання/анулювання сеансового стану:

$$Revoke(k_t) = 1 \Rightarrow \delta_t \to 0,\ epoch_{t+1} \uparrow,\ d_t \to deny, \quad (18)$$

Це означає, що політика може примусово завершити криптографічну сесію та ініціювати формування нової епохи ключів, узгоджуючи логічне рішення доступу з криптографічними наслідками.

Запропонована контекстно-ризикова модель адаптації криптографічних параметрів принципово відрізняється від традиційних схем, у яких криптографічні параметри фіксуються на час сесії або змінюються лише внаслідок примусової ротації ключів [19, 21]. У даному підході криптографія інтегрується в політично-керований контур Zero Trust та виконує роль активного механізму зменшення поверхні атаки шляхом динамічного скорочення вікна можливих компрометацій.

Таким чином, контекстно-ризикова адаптація криптографічних параметрів забезпечує узгоджене поєднання політичних рішень PBAC і механізмів криптографічного enforcement, що створює основу для побудови адаптивних систем захисту інформаційних ресурсів, здатних підтримувати безперервну відповідність вимогам Zero Trust Architecture.

У межах запропонованого підходу взаємодія між компонентами Policy Decision Point (PDP), Policy Enforcement Point (PEP) та криптографічним механізмом захисту розглядається як єдиний алгоритмічний контур, що забезпечує узгоджене прийняття та виконання рішень у динамічному середовищі Zero Trust Architecture [10, 13, 15]. На відміну від традиційних схем, у яких криптографічні механізми застосовуються після завершення авторизації, у запропонованій моделі криптографічний enforcement інтегрується безпосередньо в процес прийняття політичного рішення та підлягає безперервному коригуванню.

Алгоритмічний контур взаємодії визначається як послідовність операцій, що виконуються при кожному запиті доступу або подієвій зміні безпекового стану. Нехай у момент часу t надходить запит доступу:

$$q_t = \langle u, r, a \rangle, \quad (19)$$

який обробляється PDP з урахуванням поточного стану S_t^*. PDP виконує агрегування телеметрії та контекстних параметрів, формуючи оновлений стан доступу, після чого обчислює політичне рішення $D_t = \langle d_t, \hat{k}_t \rangle$, де d_t — логічне рішення доступу, $\hat{k}_t$ — криптографічна політика, що визначає параметри захисту.

Policy Enforcement Point отримує рішення D_t та виконує його enforcement у двох вимірах: логічному та криптографічному. Логічний enforcement визначає допустимість виконання операції, тоді як криптографічний enforcement ініціює налаштування або оновлення параметрів захисту інформаційної взаємодії [19, 23]. У разі подієвих змін, таких як поведінкові аномалії або зміна контексту, PEP ініціює повторний виклик PDP для переоцінки політики та криптографічного стану.

Формально алгоритмічна взаємодія може бути описана таким чином. Нехай E_t — множина подій безпеки, що виникають у момент часу t. Тоді перехід системи до нового стану визначається композицією функцій [1-3, 10-11]:

$$S_{t+1}^* = \Omega(S_t^*, q_t, E_t), \quad (20)$$

де оператор Ω реалізує повний цикл прийняття та виконання рішення, включаючи оновлення криптографічного стану. Така композиція забезпечує узгоджене функціонування PDP, PEP і Crypto Engine в межах єдиного керованого процесу.

Алгоритм прийняття та виконання рішення у запропонованій моделі може бути поданий у вигляді псевдокоду. На рис. 6 подано алгоритмічну модель взаємодії PDP, PEP та Crypto Engine у межах Zero Trust Architecture. Алгоритм реалізує циклічну політико-керовану переоцінку довіри та ризику з формуванням не лише логічного рішення доступу, а й відповідного криптографічного режиму сесії. Такий підхід забезпечує безперервне enforcement-узгодження між політиками доступу та криптографічним захистом у динамічному безпековому контексті.

У наведеному алгоритмі ключовою особливістю є циклічний характер виконання, що відповідає принципу безперервної перевірки Zero Trust Architecture [13]. Криптографічний механізм не ініціалізується одноразово, а перебуває в постійному зв'язку з PDP та PEP, реагуючи на зміну політичних рішень і безпекового контексту.

© Skladannyi P, Kostiuk Y. A formalized approach to integrating policy-based access control and cryptographic protection in zero trust architecture // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 27-39. © This is an open access article under the CC BY 4.0 International license.*

Algorithm PBAC-ZT-Crypto-Enforcement

Input: access request q_t, current system state S_t:
policy set P, security events E_t
Functions: UpdateTrust(.), UpdateRisk(.), EvaPolicy(.), Enforce(.)
Output: enforced access decision and cryptographic state.

```
Collect context q_t and security events E_t.
τ_t ← UpdateTrust(S_t, q_t, E_t)
ρ_t ← UpdateRisk(S_t, q_t, E_t)
D_t ← EvalPolicy(P, q_t, τ_t, ρ_t)
if D_t = DENY then
    Reject(q_t)
    TerminateSession(S_t)
else
    Enforce(PEP, q_t, D_t)
    ConfigureCrypto(CryptoEngine, κ_t*)
end if
Monitor execution and context changes
if SecurityEventDetected(E_t) then
    goto step 1
Monitor execution and context changes
end if
```

Рис. 6. Алгоритм прийняття та виконання політико-керованого криптографічного рішення в Zero Trust Architecture

Оскільки політико-кероване посилення криптографічних параметрів може впливати на продуктивність і експлуатаційну «вартість» доступу, доцільно формалізувати критерії, за якими оцінюється ефективність запропонованого підходу [14]. Введемо метрику потенційного вікна компрометації (attack window), пов'язану з часом життя криптографічної сесії:

$$W_t \equiv \delta_t, \tag{21}$$

тобто зменшення δ_t безпосередньо зменшує часовий інтервал, у межах якого компрометований ключ/токен залишається чинним.

Водночас введемо оцінку криптографічної вартості (затрати на криптографію) у момент часу t:

$$C_t^{crypto} = \alpha_1 \cdot Lat(\theta_t) + \alpha_2 \cdot CPU(\theta_t) + \alpha_3 \cdot ReKeyRate(p_t), \tag{22}$$

де $Lat(\theta_t)$ — затримка, зумовлена профілем (включно з handshakes), $CPU(\theta_t)$ — обчислювальна вартість, $ReKeyRate(p_t)$ — частота ротації ключів [18-19]. Для режимів step-up додатково враховується експлуатаційна вартість (friction):

$$C_t^{friction} = \alpha_4 \cdot \mathcal{I}\{d_t \equiv step-up\}, \tag{23}$$

Тоді PBAC-керований криптографічний enforcement може розглядатися як задача динамічного балансування:

$$\min_{\theta_t, \delta_t, p_t} \mathbb{E}[W_t] \text{ за умови } \mathbb{E}\left[C_t^{crypto} + C_t^{friction}\right] \le B, \tag{24}$$

де B — допустимий бюджет витрат/затримок [22]. Така постановка підкреслює, що підхід забезпечує не лише посилення криптографії, а й керовану адаптацію з урахуванням обмежень реальної експлуатації.

Наведена оптимізаційна постановка дозволяє формалізувати компроміс між рівнем криптографічної жорсткості та експлуатаційною ефективністю системи, уникаючи як надмірного ослаблення захисту, так і необґрунтованого зростання накладних витрат. У цьому контексті параметри α_1–α_4 виступають коефіцієнтами пріоритезації, що можуть адаптуватися до вимог конкретного домену, SLA або критичності захищуваних ресурсів. Таким чином, PBAC-керований криптографічний enforcement реалізує ризик-адаптивну модель, у якій рішення щодо шифрування, ротації ключів і тривалості сесій приймаються з урахуванням як безпекових, так і економічно-експлуатаційних факторів.

У разі аномалій доступу або зміни контексту події безпеки e_t ініціюють переоцінку ризику p_t і динамічну корекцію криптографічного профілю сесії [12]. Для викрадення токена або downgrade-атак застосовуються прив'язані сесії ($\beta_t = 1$), скорочення часу життя δ_t та ротація ключової епохи. Компрометація сеансового ключа призводить до негайного відкликання та завершення сесії. Спроби ескалації привілеїв обробляються через режим step-up із застосуванням строгих, короткоживучих криптографічних профілів (табл. 2) [14, 24]. Запропонований контур забезпечує узгоджену реакцію на типові атаки шляхом скорочення часу життя сесій, примусової ротації ключів та застосування строгих криптографічних профілів.

Таблиця 2

Реакція PBAC–Crypto на типові атаки

Атака	Подія (e_t)	Рішення PBAC	Криптографічний enforcement
Повторне використання токена	token_anomaly	allow / step-up	$\beta_t = 1, \delta_t \downarrow rekey$
MITM / downgrade-атака	channel_downgrade	strict / deny	фіксовані криптонабори, завершення сесії
Компрометація сеансового ключа	key_leak	deny / step-up	відкликання ключа, $epoch\uparrow$, $TTL \to 0$
Спроба ескалації привілеїв	priv_escalation	step-up	θ_{strict}, короткоживуча сесія

β_t – ознака прив'язки токена/сесії, δ_t – час життя криптографічної сесії.

Щоб забезпечити практичну відтворюваність запропонованої формалізації, Crypto Engine розглядається як протокольно-орієнтований компонент, який реалізує вимоги криптографічного профілю θ_t на рівні транспортного захисту, токенів доступу та/або захисту даних ресурсу [22]. У

© Skladannyi P, Kostiuk Y. A formalized approach to integrating policy-based access control and cryptographic protection in zero trust architecture // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 27-39. © This is an open access article under the CC BY 4.0 International license.*

найпоширенішому сценарії взаємодія реалізується через TLS 1.3, де профіль θ_t визначає допустимі параметри криптографічної сесії (клас AEAD, вимогу PFS, політику resumption, вимоги клієнтської автентифікації mTLS та умови rekey).

У випадку токен-орієнтованого доступу θ_t може вимагати proof-of-possession (PoP) механізмів, за яких токен не є переносимим артефактом, а прив'язується до каналу або ключа клієнта [14, 17]. Це формалізується параметром β_t, який активується в режимах підвищеного ризику:

$$\beta_t = \begin{cases} 0, & p_t < p_1, \\ 1, & p_t \geq p_1 \text{ або } d_t = step - up. \end{cases} \quad (25)$$

Таким чином, при зростанні ризику система переходить від «bearer»-моделі до прив'язаних токенів, що зменшує ймовірність успішного replay/викрадення токена.

Для сценаріїв захисту даних ресурсу (data-at-rest / data-in-use) застосовується envelope encryption: PBAC визначає, чи ключ даних (DEK) виводиться локально, чи видається/обслуговується через KMS/HSM, а також TTL та правила ротації [24]. Це дозволяє реалізувати політико-кероване керування ключами не лише для каналу, а й для криптографічного захисту активів.

Запропонована алгоритмічна модель забезпечує декомпозицію складного процесу керування доступом і криптографічним захистом на формально визначені кроки, що дозволяє здійснювати її аналіз, верифікацію та подальшу практичну реалізацію [13]. Водночас така модель є достатньо узагальненою, щоб бути застосованою в різних сценаріях Zero Trust, включаючи корпоративні мережі, хмарні сервіси та мікросервісні архітектури.

Таким чином, алгоритмічна інтеграція PDP, PEP та Crypto Engine формує єдиний керований контур Zero Trust, у якому політичні рішення PBAC безпосередньо визначають як логічні умови доступу, так і параметри криптографічного enforcement, забезпечуючи адаптивний і контекстно-орієнтований захист інформаційних ресурсів.

Запропонований формалізований підхід до інтеграції Policy-Based Access Control та криптографічного захисту в Zero Trust Architecture характеризується низкою властивостей, які принципово відрізняють його від традиційних моделей керування доступом і використання криптографічних механізмів. Ключовою особливістю підходу є розгляд криптографічного enforcement не як незалежного або допоміжного рівня захисту, а як безпосереднього результату політичного рішення, що формується в межах динамічного контуру Zero Trust.

Першою фундаментальною властивістю запропонованої моделі є контекстна узгодженість. Логічні рішення доступу та криптографічні параметри формуються на основі єдиного вектора стану безпеки, що забезпечує їхню семантичну узгодженість у кожний момент часу [22]. На відміну від класичних схем, у яких шифрування та керування ключами застосовуються заздалегідь визначеними правилами, у даному підході криптографічний режим є контекстно-залежним і змінюється синхронно з еволюцією безпекового стану системи.

Другою важливою властивістю є адаптивність криптографічного захисту, що реалізується через формалізовані залежності між ризиком, довірою та параметрами криптографічного механізму [22, 24]. Така адаптивність дозволяє динамічно скорочувати вікно потенційної атаки шляхом зменшення часу життя криптографічних сесій, посилення режимів шифрування або ініціації повторної генерації ключів у відповідь на зміну контексту. У результаті криптографія переходить із пасивного стану в активний механізм реагування на загрози.

Третьою властивістю є алгоритмічна керованість, яка випливає з чіткої формалізації взаємодії між Policy Decision Point, Policy Enforcement Point та криптографічним механізмом. Наявність формального алгоритмічного контуру дозволяє розглядати запропонований підхід як детерміновану систему прийняття та виконання рішень, придатну до аналізу, верифікації та подальшої оптимізації [13]. Це відкриває можливість застосування методів формальної перевірки коректності політик доступу та властивостей криптографічного enforcement.

Четвертою суттєвою властивістю є відповідність принципам Zero Trust на рівні формалізму, а не лише на рівні архітектурних декларацій. Безперервна переоцінка стану безпеки, відсутність стабільного довіреного стану та циклічний характер прийняття рішень реалізуються у запропонованій моделі безпосередньо через оператори переходу станів і механізми повторної оцінки політик. Таким чином, Zero Trust у даному підході виступає не фоновою концепцією, а формально визначеною динамічною властивістю системи.

З наукової точки зору запропонований підхід має низку важливих наслідків. По-перше, він створює основу для уніфікованого розгляду логічного контролю доступу та криптографічного захисту в межах єдиної моделі прийняття рішень. По-друге, формалізація криптографічного enforcement як результату політичного рішення відкриває можливість подальшого розвитку моделей ризик-адаптивної криптографії, у яких параметри захисту безпосередньо пов'язані з поведінковими та контекстними характеристиками суб'єктів доступу [12, 22-24]. По-третє, алгоритмічна структура запропонованої моделі дозволяє використовувати її як теоретичне підґрунтя для побудови практичних систем Zero Trust Access Management у корпоративних і хмарних середовищах.

Узагальнюючи, запропонований формалізований підхід формує концептуально нове бачення інтеграції Policy-Based Access Control та криптографічного захисту в Zero Trust Architecture, у

© Skladannyi P, Kostiuk Y. A formalized approach to integrating policy-based access control and cryptographic protection in zero trust architecture // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 27-39. © This is an open access article under the CC BY 4.0 International license.*

якому криптографія виступає не ізольованим технічним механізмом, а динамічним, політично-керованим елементом системи керування доступом [13, 22]. Саме така інтеграція створює передумови для переходу до адаптивних систем безпеки нового покоління, здатних узгоджено реагувати на зміну загроз і контексту в режимі реального часу.

Алгоритмічна структура запропонованого контуру PDP–PEP–Crypto Engine дозволяє формально перевіряти коректність узгодження логічного рішення доступу з криптографічним enforcement. Для цього модель зручно інтерпретувати як систему переходів станів $S_t^* \to S_{t+1}^*$, для якої визначаються інваріанти безпеки. Зокрема, для високого ризику має виконуватися обмеження часу життя криптографічної сесії:

$$p_1 \geq p_2 \Rightarrow \delta_t \leq \delta_{strict}, \quad (26)$$

а для забороняючого рішення доступу — узгоджене завершення сесії та анулювання криптографічного стану:

$$d_t = step - up \Rightarrow \beta_t = 1 \wedge \delta_t \leq \delta_{enh}, \quad (27)$$

Такі інваріанти можуть бути використані як основа для формальної верифікації політик і переходів (наприклад, на рівні станів і подій), що підсилює доказовість коректності інтеграції PBAC і криптографічного enforcement у ZTA.

Запропонований підхід покладається на якість і повноту телеметрії та коректність функції ризик-оцінювання $R(c_t)$, що безпосередньо впливає на адекватність адаптації криптографічних профілів [12]. Критичними є сценарії компрометації PDP/PEP або інфраструктури керування ключами (KMS/HSM), які потребують окремих механізмів захисту та резервування довіри [14, 18]. Додатково, агресивна ротація ключів і скорочення δ_t можуть збільшувати протокольні накладні витрати та затримки в режимах високого навантаження; тому в практичних системах важливо враховувати бюджет B і виконувати налаштування порогів p_1, p_2, τ_1, τ_2, відповідно до вимог домену та SLA.

Висновок

У статті запропоновано формалізований підхід до інтеграції Policy-Based Access Control та криптографічного захисту в межах Zero Trust Architecture, у якому криптографічні механізми розглядаються як керований результат політичного рішення, а не як ізольований інфраструктурний рівень. На відміну від традиційних моделей керування доступом, запропонований підхід ґрунтується на динамічному поданні безпекового стану системи та безперервній переоцінці умов доступу з урахуванням контексту, ризику та рівня довіри.

Ключовим результатом дослідження є формалізація криптографічного enforcement як складової Policy-Based Access Control, що дозволяє узгоджено керувати як логічними рішеннями доступу, так і параметрами криптографічного захисту в межах єдиного алгоритмічного контуру Zero Trust. Запропонована модель забезпечує контекстну узгодженість рішень, адаптивність криптографічних параметрів і відповідність базовим принципам Zero Trust на рівні формального опису, а не лише архітектурних рекомендацій.

Розроблена алгоритмічна модель взаємодії Policy Decision Point, Policy Enforcement Point та криптографічного механізму демонструє можливість побудови систем керування доступом, у яких криптографічний захист динамічно змінюється у відповідь на подієві зміни безпекового стану. Такий підхід дозволяє скорочувати потенційне вікно атак, підвищувати стійкість системи до поведінкових і контекстних загроз та формує основу для реалізації ризик-адаптивних механізмів захисту в сучасних корпоративних і хмарних середовищах.

Отримані результати мають не лише теоретичне, а й прикладне значення, оскільки запропонована формалізація може бути використана як методологічна основа для проєктування Zero Trust Access Management-систем, інтегрованих із механізмами керування ключами, токенами доступу та захищеними сесіями взаємодії. Алгоритмічна природа моделі створює передумови для її формальної верифікації, масштабування та адаптації до різних сценаріїв використання.

Перспективи подальших досліджень пов'язані з розвитком запропонованого підходу в кількох напрямах. Зокрема, доцільним є розширення моделі за рахунок інтеграції методів машинного навчання для більш точної оцінки ризику та динамічної адаптації політик доступу. Окремий інтерес становить формальна верифікація властивостей запропонованого алгоритмічного контуру, зокрема щодо коректності прийняття рішень і стійкості до складних сценаріїв атак. Подальших досліджень також потребує практична реалізація підходу в розподілених та мікросервісних архітектурах, а також оцінка його ефективності в умовах реального навантаження та різнорідних загроз.

Таким чином, результати роботи формують підґрунтя для подальшого розвитку формально обґрунтованих, ризик-адаптивних та криптографічно-керованих систем доступу в парадигмі Zero Trust Architecture, що відповідає сучасним вимогам до захисту інформаційних ресурсів і відкриває нові напрями наукових досліджень у цій галузі.

Список літератури

[1] Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces, 89*, 103832. https://doi.org/10.1016/j.csi.2024.103832

[2] Liu, C., Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., Tu, B., & Liu, Q. (2024). Dissecting zero trust: Research landscape and its implementation in IoT. *Cybersecurity, 7*, 20. https://doi.org/10.1186/s42400-024-00212-0

[3] Wang, R., Li, C., Zhang, K., Sun, J., Fang, W., & Qi, H. (2025). Zero-trust based dynamic access control for cloud computing. *Cybersecurity, 8*, 12. https://doi.org/10.1186/s42400-024-00320-x

[4] Caserio, C., Lonetti, F., & Marchetti, E. (2022). A formal validation approach for XACML 3.0 access control policy. *Sensors, 22*(8), 2984. https://doi.org/10.3390/s22082984

[5] Mushtaq, S., Mohsin, M., & Mushtaq, M. M. (2025). A systematic literature review on the implementation and challenges of Zero Trust Architecture across domains. *Sensors, 25*(19), 6118. https://doi.org/10.3390/s25196118

[6] Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2024). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business & Information Systems Engineering, 66*, 421–440. https://doi.org/10.1007/s12599-023-00830-x

[7] Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-trust access control mechanism based on blockchain and inner-product encryption in the Internet of Things in a 6G environment. *Sensors, 25*(2), 550. https://doi.org/10.3390/s25020550

[8] 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/encyclopedia4040096

[9] Roy, U., & Ghosh, N. (2024). BloAC: A blockchain-based secure access control management for the Internet of Things. *Journal of Information Security and Applications, 87*, 103897. https://doi.org/10.1016/j.jisa.2024.103897

[10] Jeong, E., & Yang, D. (2025). A trust score-based access control model for Zero Trust Architecture: Design, sensitivity analysis, and real-world performance evaluation. *Applied Sciences, 15*(17), 9551. https://doi.org/10.3390/app15179551

[11] Wan, T., Shi, B., & Wang, H. (2025). A continuous authentication scheme for zero-trust architecture in industrial Internet of Things. *Alexandria Engineering Journal, 122*, 555–563. https://doi.org/10.1016/j.aej.2025.03.012

[12] Довженко, Н., Іваніченко, Є., & Костюк, Ю. (2025). Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими IOT-компонентами на основі графових моделей. *Кібербезпека: освіта, наука, техніка, 1*(29), 762–776. https://doi.org/10.28925/2663-4023.2025.29.938

[13] Cutler, J., Disselkoen, C., Eline, A., He, S., Headley, K., Hicks, M., Hietala, K., Ioannidis, E., Kastner, J., Mamat, A., McAdams, D., McCutchen, M., Rungta, N., Torlak, E., & Wells, A. (2024). Cedar: A new language for expressive, fast, safe, and analyzable authorization. *Proceedings of the ACM on Programming Languages, 8*, 670–697. https://doi.org/10.1145/3649835

[14] Костюк, Ю., Складанний, П., Рзаєва, С., Мазур, Н., Черевик, В., & Аносов, А. (2025). Особливості реалізації мережевих атак через TCP/IP-протоколи. *Кібербезпека: освіта, наука, техніка, 1*(29), 571–597. https://doi.org/10.28925/2663-4023.2025.29.915

[15] Yaqub, N., Zhang, J., Khalid, M. I., Wang, W., Helfert, M., Ahmed, M., & Kim, J. (2025). Blockchain enabled policy-based access control mechanism to restrict unauthorized access to electronic health records. *PeerJ Computer Science, 11*, e2647. https://doi.org/10.7717/peerj-cs.2647

[16] Kostiuk, Y. (2025). Multi-agent system for detecting and counteracting attacks on the enterprise information system. In *Insider Threats and Security in Corporations* (pp. 205–232). https://doi.org/10.36690/ITSC-205-232

[17] Gai, K., She, Y., Zhu, L., Choo, K.-K. R., & Wan, Z. (2022). A blockchain-based access control scheme for zero trust cross-organizational data sharing. *ACM Transactions on Internet Technology, 23*. https://doi.org/10.1145/3511899

[18] Складанний, П., Костюк, Ю., Рзаєва, С., & Мазур, Н. (2025). Паралельна обробка даних у розширюваних хеш-структурах та оцінка їх продуктивності. *Кібербезпека: освіта, наука, техніка, 3*(31), 242–269. https://doi.org/10.28925/2663-4023.2025.31.1015

[19] Marchesi, L., Marchesi, M., & Tonelli, R. (2024). A survey on cryptoagility and agile practices in the light of quantum resistance. *Information and Software Technology, 178*, 107604. https://doi.org/10.1016/j.infsof.2024.107604

[20] Костюк, Ю., Хорольська, К., Бебешко, Б., Довженко, Н., Коршун, Н., & Пазинін, А. (2025). Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. *Кібербезпека: освіта, наука, техніка, 4*(28), 633–655. https://orcid.org/0009-0002-9506-9539

[21] Näther, C., Herzinger, D., Steghöfer, J. P., Gazdag, S. L., Hirsch, E., & Loebenberger, D. (2024). Toward a common understanding of cryptographic agility: A systematic review. *arXiv*. arXiv:2411.08781

[22] Marchesi, L., Marchesi, M., & Tonelli, R. (2024). Reviewing crypto-agility and quantum resistance in the light of agile practices. In P. Kruchten & P. Gregory (Eds.), *Agile processes in software engineering and extreme programming – Workshops (XP 2022–2023)* (Lecture Notes in Business Information Processing, Vol. 489). Springer. https://doi.org/10.1007/978-3-031-48550-3_21

[23] Rubio García, C., Cano Aguilera, A., Stan, C., Vegas Olmos, J. J., Rommel, S., & Tafur Monroy, I. (2025). Enhanced network security protocols for the quantum era: Combining classical and post-quantum cryptography, and quantum key distribution. *IEEE Journal on Selected Areas in Communications, 43*(8), 2765–2781. https://doi.org/10.1109/JSAC.2025.3568011

[24] Складанний, П. М., Гулак, Г. М., & Костюк, Ю. В. (2025). Генератор хаотичних чисел із нечітким керуванням для криптографічних систем із динамічною довірою. *Телекомунікаційні та інформаційні технології, 4*(89), 137–147. https://doi.org/10.31673/2412-4338.2025.048916

УДК 004.056.5:004.75

Skladannyi P., Kostiuk Y. A Formalized Approach to Integrating Policy-Based Access Control and Cryptographic Protection in Zero Trust Architecture

Abstract. *This paper addresses the problem of the gap between policy-driven access control and cryptographic protection in corporate and cloud environments implementing Zero Trust Architecture (ZTA). It is shown that in most practical ZTA deployments, access decisions are reduced to logical allow/deny outcomes or aggregated trust-score evaluations, while cryptographic protection mechanisms – key management, encryption parameters, access tokens, and cryptographic sessions – remain static or only weakly coupled with access control policies. Such isolation of the cryptographic layer reduces system adaptivity, enlarges the potential attack window, and complicates coordinated real-time responses to changes in context, risk, and trust level. A formalized approach to integrating Policy-Based Access Control (PBAC) and cryptographic enforcement within ZTA is proposed, in which the cryptographic regime is interpreted as a controlled outcome of a policy decision rather than as an independent infrastructural component. The approach is based on representing access as a*

dynamic state that includes subject identity, resource, action, execution context, trust level, risk assessment, and the cryptographic state of the access session. A PBAC mapping is formally defined that returns not only a logical access decision but also a cryptographic policy specifying the algorithm class, key parameters, enforcement mode, and cryptographic session lifetime, adapted according to risk, trust, and resource sensitivity. An algorithmic interaction loop between PDP, PEP, and the Crypto Engine with cyclic policy re-evaluation triggered by security events is developed, ensuring continuous compliance with Zero Trust principles and dynamic reduction of the potential compromise window. The practical value of the proposed approach lies in establishing a theoretical foundation for designing Zero Trust Access Management systems in which cryptographic parameters are automatically aligned with access control policies and the evolving operational context.

Keywords: *Zero Trust Architecture, Policy-Based Access Control, cryptographic enforcement, PDP/PEP, key management, risk adaptation, dynamic trust, cryptographic sessions, access context.*

Складанний Павло Миколайович, кандидат технічних наук, доцент, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Pavlo Skladannyi, PhD, Associate Professor, Head of the Department of Information and Cyber Security named after Professor Volodymyr Buryachok Borys Grinchenko Kyiv Metropolitan University.

Костюк Юлія Володимирівна, PhD, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Yuliia Kostiuk, PhD, Associate Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok Borys Grinchenko Kyiv Metropolitan University.

Дата надходження:	Дата прийняття:	Дата публікації:
03.02.2026	27.02.2026	22.04.2026