УДК 004.056 DOI https://doi.org/10.35546/kntu2078-4481.2025.4.3.30

О. І. ФЕДЮШИН
кандидат технічних наук, доцент,
доцент кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-3600-405X

І. К. ТКАЧУК
магістрант кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0009-0007-7756-660X

Р. Ю. ГВОЗДЬОВ
асистент кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-5408-943X

В. В. СТАДНІК
науковий співробітник науково-дослідної лабораторії
факультету автоматизованих систем управління
та наземного забезпечення польотів авіації
Харківський національний університет Повітряних Сил
імені Івана Кожедуба
ORCID: 0000-0002-3784-4165

ДИНАМІЧНЕ КЕРУВАННЯ ПРАВАМИ ДОСТУПУ НА ОСНОВІ ПОВЕДІНКОВИХ МОДЕЛЕЙ КОРИСТУВАЧІВ І СЕРВІСІВ

У статті запропонований підхід до динамічного керування правами доступу, побудований на аналізі поведінкових моделей суб'єктів взаємодії. Особлива увага приділяється характеристикам поведінки, що можуть бути використані як сигнали для адаптації політик доступу, методам їх формалізації та алгоритмічним стратегіям прийняття рішень у режимі реального часу. У межах дослідження здійснено огляд наукових підходів до моделювання поведінки користувачів і сервісів, а також висвітлено обмеження традиційних систем контролю доступу, які ґрунтуються на статично визначених правилах чи атрибутах. Зокрема, проаналізовано проблеми надлишкових привілеїв, повільної реакції на зміну контексту та відсутності механізмів автоматизованої еволюції політик у відповідь на реальні сценарії взаємодії. Крім того, визначено актуальну наукову проблему, що полягає у необхідності створення ефективних та стійких до аномалій механізмів поведінково-орієнтованої адаптації прав доступу, здатних підтримувати безперервний цикл спостереження, аналізу та коригування політик.

Розглядається структура поведінкових моделей, способи їх навчання та інтерпретації, а також принципи інтеграції таких моделей у системи контролю доступу з урахуванням вимог масштабованості, достовірності сигналів та мінімізації ризиків. Додатково окреслено значення таких підходів для підвищення стійкості інформаційних систем до внутрішніх загроз, а також можливість використання поведінкових характеристик як основи для прогнозування потенційно небезпечної активності та формування більш гнучких і самоналаштовних механізмів управління доступом.

Ключові слова: *динамічний контроль доступу, поведінкові моделі, поведінковий аналіз, аномалії активності, профілі користувачів, адаптація політик доступу, ризик-орієнтовані методи, інформаційна безпека, самоналаштовні системи, виявлення відхилень.*

O. I. FEDIUSHYN
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0000-0002-3600-405X

I. K. TKACHUK
Master's Student at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0009-0007-7756-660X

R. YU. GVOZDOV
Assistant at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0000-0002-5408-943X

V. V. STADNIK
Researcher Research Laboratory
at the Faculty of Automated Control Systems
and Ground Support of Aviation Flights
Ivan Kozhedub Kharkiv National University of the Air Force
ORCID: 0000-0002-3784-4165

DYNAMIC ACCESS CONTROL MANAGEMENT BASED ON BEHAVIORAL MODELS OF USERS AND SERVICES

This article proposes an approach to dynamic access rights management based on the analysis of behavioral models of interacting subjects. Particular attention is given to behavioral characteristics that can serve as signals for adapting access policies, methods of their formalization, and algorithmic strategies for real-time decision-making. The study provides an overview of scientific approaches to modeling the behavior of users and services, as well as highlights the limitations of traditional access control systems that rely on statically defined rules or attributes. In particular, issues such as excessive privileges, slow response to contextual changes, and the absence of automated mechanisms for policy evolution in response to real interaction scenarios are analyzed.

The paper identifies the urgent scientific problem of developing effective and anomaly-resistant mechanisms for behavior-oriented adaptation of access rights capable of supporting a continuous cycle of monitoring, analysis, and policy adjustment. The structure of behavioral models, methods of their training and interpretation, and principles of integrating such models into access control systems are discussed with consideration of scalability requirements, signal reliability, and risk minimization. Additionally, the article outlines the importance of these approaches for enhancing information system resilience to insider threats, as well as the potential use of behavioral characteristics as a basis for predicting harmful activity and constructing more flexible and self-adaptive access management mechanisms.

Key words: *dynamic access control, behavioral models, behavioral analysis, activity anomalies, user profiles, access policy adaptation, risk-based methods, information security, self-adaptive systems, anomaly detection.*

Постановка проблеми

Сучасні інформаційні системи функціонують у середовищах, що характеризуються високою мінливістю, динамікою взаємодій та зростаючим обсягом поведінкових даних про діяльність користувачів і сервісів. Традиційні моделі контролю доступу, засновані на фіксованих правилах, статичних атрибутах або наперед визначених ролях, виявляються недостатньо чутливими до цих змін. Їхня статичність призводить до накопичення надмірних привілеїв, зниження адаптивності та втрати відповідності реальним сценаріям використання. Зокрема, такі моделі не враховують актуальну поведінку суб'єктів взаємодії, не розпізнають відхилення від типових патернів та не здатні оперативно коригувати політики доступу у відповідь на нетипові дії чи аномалії.

Проблема ускладнюється тим, що в умовах розподіленості та сервісної орієнтованості сучасних систем взаємодії між компонентами генерують значний обсяг поведінкових сигналів, які потенційно можуть бути використані для підвищення точності та гнучкості рішень щодо доступу. Проте існуючі підходи до керування правами доступу здебільшого не інтегрують такі сигнали у процес ухвалення рішень і не використовують поведінкову динаміку як основу для адаптації політик. Тому виникає наукова та прикладна проблема, що полягає у відсутності ефективних механізмів динамічного керування правами доступу, здатних використовувати поведінкові моделі користувачів і сервісів для автоматизованої адаптації політик у режимі реального часу. Необхідним є розроблення підходів, які забезпечували б безперервне спостереження за поведінкою, її формалізацію, визначення показників нормальності чи аномальності та коригування прав доступу відповідно до отриманих сигналів. Розв'язання цієї проблеми сприятиме підвищенню стійкості інформаційних систем, зменшенню ризиків внутрішніх загроз та побудові більш точних і самоналаштовних систем контролю доступу.

Аналіз останніх досліджень і публікацій

Проблематика динамічного контролю доступу та використання поведінкових характеристик користувачів і сервісів активно досліджується в межах сучасної кібербезпеки. Значна частина наукових робіт зосереджена

на розвитку атрибутивних та контекстуальних моделей доступу, що враховують зміни середовища виконання. Зокрема, у роботі [1] підкреслюється обмеженість традиційних статичних моделей і визначається необхідність переходу до підходів, здатних реагувати на поведінкові сигнали в реальному часі. Подібні висновки подає і дослідження [2], де показано, що поведінкові шаблони можуть бути використані для виявлення аномалій і пом'якшення внутрішніх загроз.

У низці публікацій розглядаються методи побудови поведінкових моделей на основі машинного навчання, зокрема методи класифікації та кластеризації, що дозволяють ідентифікувати відхилення у взаємодії користувачів з системою. У роботі [3] запропоновано інтелектуальний підхід до контролю доступу, який використовує поведінкові профілі для динамічного коригування привілеїв суб'єктів. Дослідження [4] демонструє можливість інтеграції поведінкових характеристик у моделі ризик-орієнтованого доступу, що дозволяє підвищити точність прийняття рішень.

Крім того, наукові праці у сфері самоналаштовуваних систем наголошують на важливості циклу «моніторинг – аналіз – планування – виконання» (концепція MAPE-K), який може бути застосований для автоматизованої еволюції політик доступу. Наприклад, у роботі [5] описано підхід до адаптації поведінки систем на основі знань про їх поточний стан, що узгоджується з концепцією поведінково-орієнтованого контролю доступу.

Узагальнюючи проаналізовані роботи, можна зробити висновок, що сучасні дослідження визнають перспективність інтеграції поведінкових даних у процес керування доступом, проте поки відсутні універсальні моделі, здатні комплексно враховувати поведінку як користувачів, так і сервісів у динамічних умовах функціонування інформаційних систем.

Формулювання мети дослідження

Метою дослідження є розробка підходу до динамічного керування правами доступу на основі аналізу поведінкових моделей користувачів і сервісів, що забезпечує адаптивне коригування політик доступу в реальному часі. Дослідження спрямоване на визначення релевантних поведінкових характеристик, формалізацію їх впливу на процес ухвалення рішень та обґрунтування механізмів, які підвищують точність, гнучкість і безпеку систем контролю доступу в умовах змінного цифрового середовища.

Викладення основного матеріалу дослідження

У межах даного дослідження здійснюється комплексний аналіз підходів до динамічного керування правами доступу, що ґрунтуються на поведінкових моделях користувачів і сервісів. Особлива увага приділяється ідентифікації характеристик поведінки, які можуть виступати індикаторами нормальної або аномальної активності, та визначенню способів їх формалізації для подальшого використання у процесі адаптації політик доступу. Розглядаються механізми побудови поведінкових профілів, методи обробки та класифікації поведінкових даних, а також підходи до інтеграції цих елементів у цикли прийняття рішень у системах контролю доступу.

В роботі проаналізовано актуальні наукові методи й моделі, що забезпечують можливість адаптивного реагування системи на зміну поведінки суб'єктів взаємодії. Зокрема, досліджуються компоненти системи моніторингу поведінки, методи обчислення поведінкових відхилень, алгоритми визначення рівня ризику та механізми коригування прав доступу в реальному часі. Крім того, увагу зосереджено на питаннях узгодженості динамічної еволюції політик із вимогами безпеки, сталості та масштабованості інформаційної системи.

Також деталізуються ключові аспекти побудови поведінково-орієнтованих моделей доступу та демонструють можливі підходи до реалізації адаптивного контролю доступу в умовах змінного цифрового середовища.

Поведінкові характеристики суб'єктів взаємодії та їх формалізація

Поведінкові характеристики суб'єктів взаємодії є фундаментальним елементом динамічного контролю доступу, оскільки вони дозволяють відобразити реальні моделі використання системи та забезпечують основу для адаптивного коригування прав. До таких характеристик належать частота та контекст виконання дій, часові шаблони активності, послідовність звернень до ресурсів, типові маршрути взаємодії, інтенсивність запитів, а також структурні залежності між викликами сервісів. Ці параметри можуть бути визначені як для кінцевих користувачів, так і для автоматизованих сервісних компонентів, що взаємодіють між собою у складних розподілених системах.

Формалізація поведінкових характеристик передбачає визначення векторів ознак, які репрезентують поведінку суб'єкта у вигляді числових, категоріальних або структурованих даних. До базових методів належать статистичні моделі, часові ряди, графові структури взаємодій та ймовірнісні описи переходів між станами. Для комплексних систем доцільним є використання гібридних моделей, що поєднують детерміновані правила з результатами поведінкового аналізу. Формалізовані дані надалі можуть бути використані для побудови профілів нормальної активності, оцінки подібності поточних дій до історичних зразків та виявлення аномалій.

Чітке визначення поведінкових характеристик і способів їх формалізації є необхідною передумовою для побудови адаптивних систем контролю доступу, здатних оперативно реагувати на зміни у сценаріях взаємодії та забезпечувати точніші рішення щодо надання або обмеження прав доступу.

Методи побудови поведінкових профілів користувачів

Поведінковий профіль суб'єкта взаємодії є узагальненою моделлю його типової активності, сформованою на основі історичних даних та поточних спостережень. Побудова таких профілів є ключовим етапом динамічного керування правами доступу, оскільки саме вони визначають межі нормальної поведінки, відносно яких обчислюються відхилення та приймаються адаптивні рішення. Процес створення поведінкового профілю починається зі збору даних про дії користувачів та сервісів, включаючи частоту, типи операцій, часові інтервали, маршрути запитів та взаємозв'язки між компонентами системи. Зазвичай ці дані агрегуються у вигляді статистичних моделей, метрик активності або структурованих графів взаємодії.

Для побудови профілів застосовуються різні підходи: від класичних статистичних методів (середні значення, дисперсія, коваріаційні залежності) до більш складних моделей, зокрема марковських процесів, кластеризаційних алгоритмів та моделей машинного навчання. Особливої актуальності набувають інкрементні методи оновлення профілів, які дозволяють адаптувати модель до змін поведінки без необхідності повного перенавчання. Такий підхід забезпечує стійкість профілю до природних змін активності суб'єкта, але водночас дозволяє своєчасно реагувати на суттєві відхилення.

На рис. 1 наведена структурована схема методів побудови профілів користувачів.

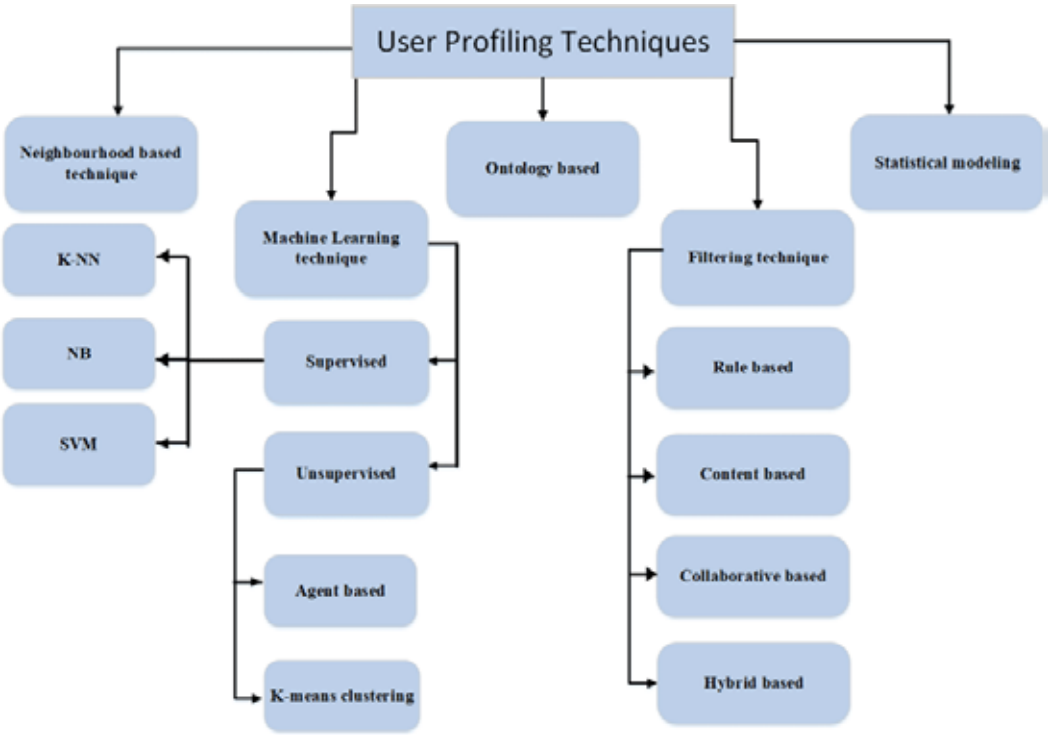

Рис. 1. Класифікація технік побудови поведінкових профілів користувачів

Діаграма систематизує основні техніки моделювання поведінки – від статистичного аналізу та методів на основі відстаней до машинного навчання, фільтраційних підходів та онтологічних моделей. Вона демонструє, що формалізація поведінки може здійснюватися через різні парадигми, кожна з яких дозволяє репрезентувати такі ознаки, як частота та контекст дій, часові шаблони активності, послідовність звернень до ресурсів та структурні залежності між операціями, таким чином підкреслюється багатомодельний характер поведінкового аналізу, який формує основу для побудови адаптивних систем контролю доступу та подальшого виявлення відхилень.

Оновлення поведінкових профілів може здійснюватися як періодично, так і в режимі реального часу, залежно від вимог системи. При цьому важливим є забезпечення балансу між стабільністю профілю та чутливістю до змін. Надмірно чутливий профіль призведе до помилкових сповіщень, тоді як надто стабільний – до несвоєчасного виявлення аномалій. Оптимальна стратегія оновлення повинна враховувати як специфіку домену, так і характер поведінки суб'єктів.

Виявлення аномалій та оцінка поведінкових відхилень контролю доступу

Виявлення аномалій є центральним компонентом динамічного керування правами доступу, оскільки саме цей процес дозволяє ідентифікувати відхилення від типових моделей поведінки та визначати потенційні ризики, пов'язані з діями суб'єктів взаємодії. Аномалії можуть проявлятися у вигляді непередбачуваних запитів до

ресурсів, нетипових маршрутів взаємодії, різкого збільшення інтенсивності операцій або звернень у незвичний час. Важливим є те, що такі відхилення не завжди є ознакою шкідливої активності, тому система контролю доступу повинна забезпечувати коректне розмежування між природними змінами поведінки та потенційними загрозами.

Існують різні підходи до виявлення аномалій, які варіюються від базових методів статистичного аналізу до складних моделей машинного навчання. Статистичні методи включають аналіз контрольних меж, виявлення стрибків у часових рядах, побудову ймовірнісних розподілів і класифікацію відхилень на основі порогових значень. Алгоритми машинного навчання, такі як методи кластеризації, ізоляційні ліси, автоенкодери або гібридні моделі, дозволяють виявляти складні нелінійні залежності у поведінкових даних.

Модель виявлення конфліктів між політиками доступу в контексті аномальної активності наведена на рис. 2. Вона демонструє, як система порівнює поточні дії суб'єкта з наявними правилами, виявляє логічні суперечності та ідентифікує потенційно небезпечні ситуації ще до того, як зміни політик або рішення щодо доступу будуть застосовані.

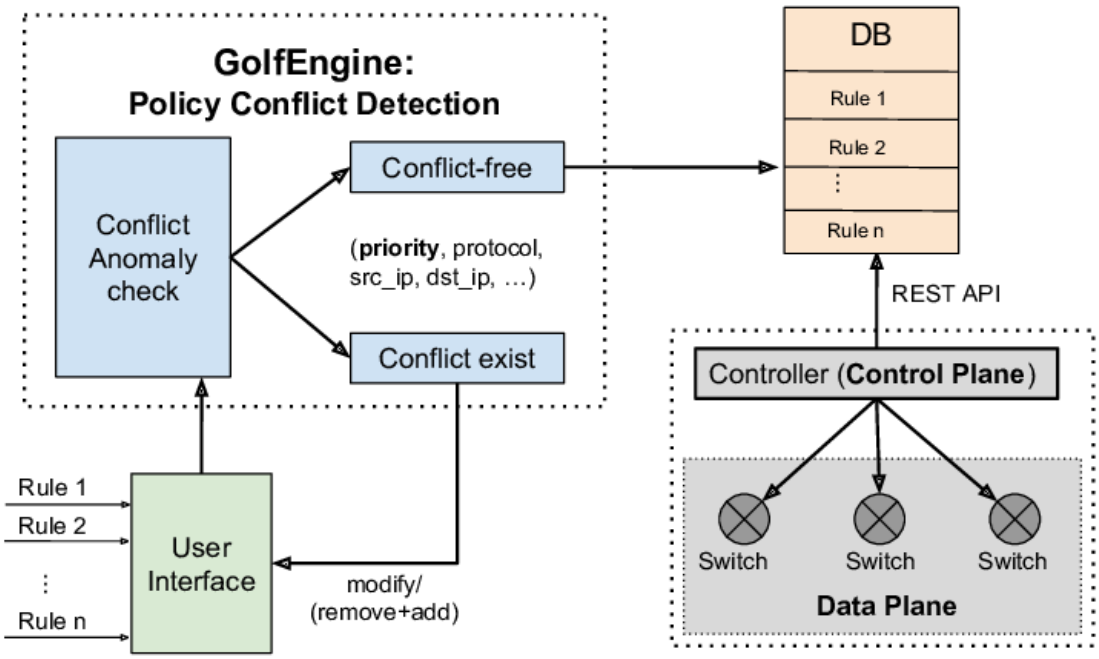

Рис. 2. Модель виявлення конфліктів політик доступу

Оцінка поведінкових відхилень передбачає визначення міри схожості між поточним станом активності та сформованим поведінковим профілем. Це може включати використання метрик відстані, оцінку ймовірності події чи розрахунок ризикового показника. Результат такої оцінки є ключовим входом до механізмів адаптації політик доступу, оскільки дозволяє системі ухвалювати рішення про обмеження, уточнення або тимчасову модифікацію прав.

Для узагальнення найбільш уживаних підходів до виявлення поведінкових відхилень подається порівняльна таблиця методів, що демонструє ключові принципи та відмінності між основними алгоритмами виявлення аномалій.

Таблиця 1

Основні методи виявлення аномалій у поведінкових даних

Метод	Тип методу	Принцип дії
Z-score / IQR	Статистичний	Виявлення відхилень від нормального розподілу
K-Means / DBSCAN	Кластеризація	Групування нормальних точок, а аномалії – поза кластерами
Isolation Forest	ML-алгоритм	Ізоляція аномалій через побудову випадкових дерев
Autoencoder	Глибинне навчання	Висока похибка реконструкції сигналізує аномалію
LOF (Local Outlier Factor)	Щільнісний метод	Уточнює аномалії за локальною щільністю сусідів

Ефективне виявлення аномалій підвищує рівень безпеки системи, зменшує ризик внутрішніх загроз та формує підґрунтя для інтелектуального динамічного контролю доступу.

Алгоритми динамічної адаптації політик доступу

Алгоритми динамічної адаптації політик доступу виконують ключову роль у процесі трансформації поведінкових сигналів у конкретні управлінські рішення щодо надання, обмеження або модифікації прав доступу. Основною функцією таких алгоритмів є інтерпретація результатів поведінкового аналізу та визначення відповідних дій з урахуванням рівня ризику, важливості ресурсу та контексту операції. На практичному рівні адаптація може здійснюватися у вигляді тимчасових обмежень, уточнення привілеїв, застосування додаткових засобів автентифікації або переходу системи у підвищений режим безпеки.

Сучасні підходи до побудови таких алгоритмів включають як детерміновані моделі на основі правил, так і інтелектуальні алгоритми, що використовують машинне навчання. Правил-орієнтовані моделі передбачають попередньо визначені дії у відповідь на конкретні типи відхилень, що забезпечує прозорість та передбачуваність роботи системи. Однак такі моделі можуть бути недостатньо гнучкими в умовах високої варіативності поведінки користувачів.

Натомість алгоритми, що базуються на машинному навчанні або гібридних підходах, здатні адаптуватися до нових ситуацій без необхідності ручного визначення правил. Наприклад, моделі прогнозування можуть оцінювати ймовірність подальшої аномальної активності, у той час як алгоритми оптимізації можуть динамічно визначати мінімальний набір привілеїв для виконання операції. Для узагальнення описаних підходів та забезпечення структурованого подання процесу прийняття рішень у системі динамічного контролю доступу наведено алгоритмічну модель адаптації політик. У таблиці 2 подано основні етапи цього процесу – від аналізу поведінкового сигналу до застосування оновлених правил і їх інтеграції в механізми подальшого навчання системи.

Важливим аспектом є забезпечення збалансованості між безпекою та доступністю ресурсів. Тому алгоритми повинні враховувати як ризиковий профіль суб'єкта, так і критичність системи, мінімізуючи кількість помилкових блокувань і водночас ефективно протидіючи потенційним загрозам.

Забезпечення узгодженості системи при еволюції прав доступу

Забезпечення стійкості та узгодженості системи під час динамічної адаптації прав доступу є критичним аспектом побудови поведінково-орієнтованих механізмів контролю доступу. Динамічні зміни політик, хоча й дозволяють підвищити точність реагування на аномальні або ризиковані дії, можуть водночас створювати ризики порушення цілісності системи, некоректного застосування привілеїв або конфліктів між правилами. Одним із ключових принципів забезпечення стійкості є використання формальних методів і верифікаційних моделей, які дозволяють перевіряти політики на предмет конфліктів, надмірних прав або порушення обмежень безпеки.

Таблиця 2

Алгоритмічна модель адаптації політик доступу

Етап	Опис процесу	Вхідні дані	Результат / Вихід
Аналіз поведінкового сигналу	Оцінювання відхилень від поведінкового профілю та визначення рівня ризику	Поточний вектор поведінки, профіль суб'єкта, метрики відхилення	Класифікація події: нормальна, підозріла або аномальна
Визначення контексту операції	Оцінювання критичності ресурсу та умов доступу (час, місце, тип операції)	Контекстні атрибути, ресурсна політика, історія взаємодій	Контекстний ризиковий коефіцієнт
Вибір стратегії адаптації	Прийняття рішення щодо того, як змінювати політику доступу	Ризиковий профіль користувача/ сервісу, критичність ресурсу	Обрана стратегія: обмежити / уточнити / посилити автентифікацію / заборонити
Модифікація політики доступу	Застосування локальних або тимчасових змін у правах доступу	Набір дій зі стратегії адаптації	Оновлена політика доступу або тимчасовий контрольний режим
Перевірка узгодженості	Переконання, що нові правила не суперечать глобальним політикам	Попередня і нова версія політик, інваріанти безпеки	Верифікована політика, готова до застосування
Застосування рішення в системі	Активування оновлених політик у реальному часі	Верифіковані зміни	Набуття чинності оновленими правами доступу
Логування та оновлення профілів	Фіксація змін та використання події для подальшого навчання профілів	Журнал рішень та результатів поведінки	Актуалізовані профілі суб'єктів для майбутніх рішень.

До таких методів належать моделі доступу на основі логічних формул, перевірка властивостей за допомогою автоматів станів та застосування технік статичного аналізу. Також алгоритми узгодження повинні забезпечити підтримку безперервності роботи системи, при зміні політик у режимі реального часу.

Важливим аспектом стійкості є мінімізація похибок унаслідок хибних спрацьовувань алгоритмів виявлення аномалій. Для цього в системі можуть використовуватися механізми поступового зниження або підвищення прав, багаторівневі моделі ризику та політики відкладеного підтвердження, які дозволяють зменшити кількість необґрунтованих обмежень.

Для ілюстрації логіки узгодження політик доступу наведено узагальнену схему (див. рис. 3), яка демонструє повний життєвий цикл політики від її специфікації до перевірки на відповідність інваріантам безпеки та фінального застосування.

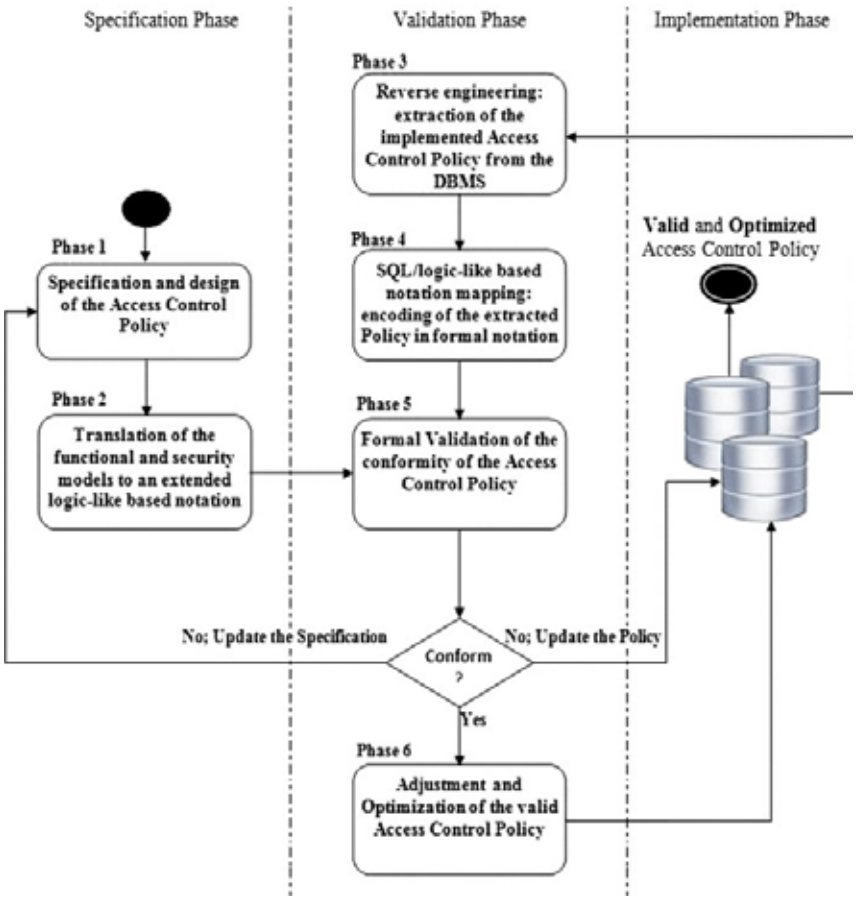

Рис. 3. Методологія розгортання та узгодження політик доступу

Модель показує, як інтегруються етапи валідації, верифікації та аналізу конфліктів, що критичні під час динамічної адаптації правил доступу.

Узгодженість також передбачає збереження глобальних інваріантів безпеки, таких як відсутність циклічних дозволів, дотримання принципу найменших привілеїв та підтримання єдиної логічної структури політик. Реалізація цих принципів забезпечує стабільність системи, підвищує її стійкість до внутрішніх і зовнішніх загроз та гарантує надійність динамічного контролю доступу в умовах змінного цифрового середовища.

Список використаної літератури

1. Hu V. C., Ferraiolo D. F., Kuhn D. R. (2020). Assessment of Access Control Systems. NIST Interagency Report 7316. URL: https://doi.org/10.6028/NIST.IR.7316.

2. Özkan Canay, Ümit Kocabıçak. (2024). Predictive modeling and anomaly detection in large-scale web portals through the CAWAL framework. URL: https://www.sciencedirect.com/science/article/abs/pii/S0950705124013443.

3. Fan Yang, Chris L. Hankin, Flemming Nielson, Hanne Riis Nielson. (2013). Predictive access control for distributed computation. URL: https://www.sciencedirect.com/science/article/pii/S0167642312001104.

4. Yuan Zhai, Haochen Yang, Jingyu Yao, Tao Wang, Yanwei Zhou, Feng Zhu, Bo Yang. (2025). DRAC: A dynamic fine-grained access control scheme for cloud storage with censorship-coerced resistance.URL: https://www.sciencedirect.com /science/article/abs/pii/S2214212625001607.

5. Riaz Ahmed Shaikh, Kamel Adi, Luigi Logrippo. (2012).Dynamic risk-based decision methods for access control systems. URL: https://www.sciencedirect.com/ science/article/abs/pii/S0167404812000399.

References

1. Hu V. C., Ferraiolo D. F., Kuhn D. R. (2020). Assessment of Access Control Systems. NIST Interagency Report 7316. URL: https://doi.org/10.6028/NIST.IR.7316.

2. Özkan Canay, Ümit Kocabıçak. (2024). Predictive modeling and anomaly detection in large-scale web portals through the CAWAL framework. URL: https://www.sciencedirect.com/science/article/abs/pii/S0950705124013443.

3. Fan Yang, Chris L. Hankin, Flemming Nielson, Hanne Riis Nielson. (2013). Predictive access control for distributed computation. URL: https://www.sciencedirect.com/science/article/pii/S0167642312001104.

4. Yuan Zhai, Haochen Yang, Jingyu Yao, Tao Wang, Yanwei Zhou, Feng Zhu, Bo Yang. (2025). DRAC: A dynamic fine-grained access control scheme for cloud storage with censorship-coerced resistance.URL: https://www.sciencedirect.com /science/article/abs/pii/S2214212625001607.

5. Riaz Ahmed Shaikh, Kamel Adi, Luigi Logrippo. (2012).Dynamic risk-based decision methods for access control systems. URL: https://www.sciencedirect.com/ science/article/abs/pii/S0167404812000399.

Дата першого надходження рукопису до видання: 20.11.2025
Дата прийнятого до друку рукопису після рецензування: 16.12.2025
Дата публікації: 31.12.2025