УДК 004.056.5:004.415.5:004.8

ДОСЛІДЖЕННЯ МЕТОДІВ СИСТЕМИ ДИНАМІЧНОГО ПРИЗНАЧЕННЯ РОЛЕЙ У СИСТЕМАХ КЕРУВАННЯ ДОСТУПОМ ПІДПРИЄМСТВА

Ажищев В.Ф., к.т.н., доцент[1]; Качурка Д.І.[2] ; Леус С.О.[3]; Морарь М.І.[4]
[1,2,3,4] Національний університет кораблебудування імені адмірала Макарова
[1,2,3,4] Україна, Миколаїв
[1] viktor.azhyshchev@nuos.edu.ua; [2] danja.kachurka2@gmail.com;
[3] lossmercury@gmail.com; [4]maurettediego@icloud.com

Анотація. *У роботі розглянуто сучасні підходи до управління доступом у корпоративних інформаційних системах із акцентом на впровадження динамічного призначення ролей. Проведено аналіз традиційних моделей керування доступом (DAC, MAC, RBAC) та сучасних гнучких підходів (ABAC, AI-RBAC, Context-Aware Access Control). Показано переваги динамічної системи призначення ролей, що базується на аналітиці поведінки користувачів, контекстних параметрах та машинному навчанні. Запропоновано концептуальну модель інтеграції динамічного керування ролями в корпоративне середовище з урахуванням факторів безпеки, продуктивності та адаптивності.*

Ключові слова: *керування доступом; рольова модель; динамічне призначення ролей; інформаційна безпека; корпоративна система; контекстна автентифікація; RBAC; ABAC.*

Вступ. Зростання обсягів цифрових даних та кількості користувачів у корпоративних інформаційних системах створює потребу у гнучкому та адаптивному механізмі керування доступом. Традиційні підходи, такі як Role-Based Access Control (RBAC), забезпечують централізоване управління, проте є недостатньо гнучкими у динамічному бізнес-середовищі.

В умовах високої динаміки ролей, мобільності співробітників та інтеграції хмарних сервісів виникає необхідність у системах, здатних автоматично змінювати права доступу залежно від контексту, поведінки користувача та політики безпеки. Саме такі системи реалізуються через підхід динамічного призначення ролей (Dynamic Role Assignment, DRA) [1,2].

Метою роботи є дослідження методів побудови систем динамічного призначення ролей у підприємницьких структурах, визначення їх переваг, обмежень та напрямів практичного впровадження.

Основна частина. Моделі DAC (Discretionary Access Control) і MAC (Mandatory Access Control) використовуються для базових політик безпеки, але не забезпечують масштабованості у корпоративних системах [3,4].

Модель RBAC упроваджує концепцію ролей, що відповідають посадовим обов'язкам, проте має обмеження щодо контекстної адаптації та автоматичного оновлення ролей.

З появою ABAC (Attribute-Based Access Control) та Context-Aware Access Control з'явилася можливість призначати доступ на основі атрибутів користувача, пристрою, місця, часу чи ризику [5].

Подальший розвиток цих ідей призвів до створення систем Dynamic Role Assignment (DRA), у яких ролі не фіксовані, а обчислюються в реальному часі.

У методах динамічного призначення ролей як основні є DRA включає атрибутивний підхід — роль визначається за набором атрибутів користувача та ресурсів. Моделі на основі поведінки — аналізуються дії користувачів для прогнозування необхідних прав. Моделі з елементами машинного навчання — система прогнозує оптимальні ролі на основі історії доступів. Політики на основі ризику — враховується рівень загрози чи аномалії у поведінці користувача.

Концепцією інтеграції DRA в корпоративну систему є запропонована архітектура, що включає такі компоненти як модуль аналітики поведінки користувачів (UBA/UEBA), контекстний процесор (місце, пристрій, час, ризик), механізм прийняття рішень (policy engine), модуль аудиту та контролю доступу [6].

Взаємодія між компонентами забезпечує автоматичне, безпечне і прозоре призначення ролей у реальному часі.

Висновки. Дослідження показало, що системи динамічного призначення ролей є перспективним напрямом розвитку корпоративної безпеки. Вони забезпечують адаптивність до змін організаційної структури, знижують ризик надлишкових прав доступу та підвищують рівень захисту інформаційних ресурсів.

Подальші дослідження доцільно спрямувати на розробку гібридних моделей, які поєднують правила ABAC із механізмами штучного інтелекту для підвищення точності та ефективності призначення ролей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security, 4(3), 224–274.

[2] Hu, V. C., Ferraiolo, D. F., Kuhn, D. R., & Sandhu, R. (2015). Attribute-based access control. IEEE Computer, 48(2), 85–88.

[3] Bertino, E., & Sandhu, R. (2005). Database security—Concepts, approaches, and challenges. IEEE Transactions on Dependable and Secure Computing, 2(1), 2–19.

[4] Goyal, V., & Tripathi, A. (2020). Dynamic role-based access control model for cloud computing environment. Journal of Information Security and Applications, 55, 102676.

[5] Alotaibi, B., & Alomar, N. (2022). Context-aware and risk-based access control for enterprise systems. Computers & Security, 116, 102660.

[6] Liu, Q., Zhang, H., & Guo, Z. (2023). AI-driven adaptive access control in enterprise systems. Information Systems Frontiers, 25(4), 1251–1263.

Azhyshchev V. 1, Kachurka D. 2, Leus S. 3, Morar M. 4

Investigation of Methods for Dynamic Role Assignment in Enterprise Access Control Systems

Abstract. *The paper examines modern approaches to access management in corporate information systems, with a focus on implementing dynamic role assignment. An analysis of traditional access control models (DAC, MAC, RBAC) and modern flexible approaches (ABAC, AI-RBAC, Context-Aware Access Control) is presented. The advantages of a dynamic role assignment system based on user behavior analytics, contextual parameters, and machine learning are demonstrated. A conceptual model for integrating dynamic role management into a corporate environment is proposed, taking into account security, performance, and adaptability factors.*

Keywords: *access control; role-based model; dynamic role assignment; information security; corporate system; contextual authentication; RBAC; ABAC.*