УДК 004.75:004.8

Д. В. Педосенко

МЕТОД ІНТЕГРАЦІЇ AI-АГЕНТІВ ІЗ КОРПОРАТИВНИМИ IT-СИСТЕМАМИ НА ОСНОВІ ПРОТОКОЛУ MODEL CONTEXT PROTOCOL

Вінницький національний технічний університет;

Анотація

У роботі досліджено проблему інтеграції автономних агентів на основі великих мовних моделей із корпоративними інформаційними системами. Показано, що класичний підхід зі створенням окремих адаптерів між кожним агентом і кожним джерелом даних чи інструментом призводить до комбінаторного зростання кількості з'єднань і не масштабується для промислових сценаріїв. Запропоновано метод інтеграції, який використовує відкритий протокол Model Context Protocol як універсальний шар діалогу між AI-агентами та корпоративними IT-системами. Сформульовано основні етапи методу та визначено функціональні модулі програмного середовища для його реалізації, що включає реєстр MCP-серверів, шлюз авторизації та сервіс аудиту викликів інструментів.

Ключові слова: інтеграція IT-систем; Model Context Protocol; MCP; AI-агенти; корпоративні системи; шаблони інтеграції; iPaaS.

Abstract

The paper addresses the problem of integrating autonomous large-language-model-based agents with enterprise information systems. It is shown that the classical approach of building dedicated adapters between every agent and every data source or tool leads to combinatorial growth of connection points and does not scale to industrial scenarios. A method is proposed that adopts the open Model Context Protocol as a universal dialogue layer between AI agents and enterprise IT systems. The principal phases of the method are formulated and the functional modules of the supporting software environment are defined, including an MCP-server registry, an authorisation gateway, and a tool invocation audit service.

Keywords: IT systems integration; Model Context Protocol; MCP; AI agents; enterprise systems; integration patterns; iPaaS.

Вступ

Сучасні корпоративні IT-ландшафти складаються з десятків спеціалізованих систем (CRM, ERP, ITSM, систем моніторингу, сховищ даних і шин повідомлень), які впродовж років розвивалися автономно та накопичили значне різноманіття форматів і прикладних інтерфейсів. Поява автономних агентів на основі великих мовних моделей додала ще один клас споживачів інтеграційних інтерфейсів: для виконання реальних бізнес-задач агент повинен читати дані з джерел, виконувати дії над сутностями та взаємодіяти з користувачами через канали, що належать різним системам.

Раніше задачу інтеграції розв'язували побудовою власних коннекторів між кожною парою «застосунок-застосунок», однак така стратегія погано масштабується. Подібну проблему понад двадцять років тому отримала практика Enterprise Application Integration, у відповідь на яку були сформульовані шаблони інтеграції та архітектура корпоративної шини сервісів. На рівні AI-агентів проблема постає у новій формі: кожен агент потребує власної інтеграції з кожним інструментом і джерелом знань, що утворює класичну задачу N×M з'єднань і потребує систематичного підходу до її розв'язання.

Актуальність

Актуальність дослідження зумовлена стрімким зростанням кількості корпоративних застосувань AI-агентів, що зробило задачу їх інтеграції з оточенням однією з критичних. Без стандартного шару взаємодії розробники змушені створювати окремі адаптери для кожної комбінації «модель-інструмент», що збільшує вартість супроводу, ускладнює зміну провайдера моделі та створює прихований технічний борг. Загальний обсяг ринку платформ інтеграції лише за 2024 рік перевищив дев'ять мільярдів доларів і продовжує зростати, що підкреслює промислову вагу задачі.

Окремою проблемою є безпека: AI-агенти, які отримують доступ до корпоративних даних та засобів виконання дій, відкривають нові вектори атак, серед яких ін'єкції у промт та зловмисне використання інструментів. Без формалізованого протоколу та механізмів контролю доступу організації фактично надають мовній моделі прямий доступ до своїх систем без аудиту та можливості

селективного відкликання прав. Тому розроблення методів інтеграції AI-агентів із корпоративними IT-системами на основі стандартизованих протоколів є актуальною науково-практичною задачею.

Метод інтеграції AI-агентів на основі протоколу Model Context Protocol

Сучасний підхід до побудови корпоративної інтеграційної архітектури зміщується від моноблочних шин сервісів у бік API-керованої та подієво-керованої моделі, що поєднує мікросервіси, iPaaS-платформи та шар управління API [1]. Декомпозиція монолітних застосунків на незалежно розгортані сервіси, кожен із яких контролює свій набір даних і операцій, дозволяє масштабувати інтеграційну логіку, проте водночас збільшує кількість стиків, які потрібно описувати, моніторити та захищати, а також ускладнює узгодження семантики даних між службами [2].

У сегменті інтеграції AI-агентів на роль універсального шару діалогу швидко висунувся протокол Model Context Protocol (MCP), запропонований у листопаді 2024 року як відкритий стандарт для з'єднання моделей із зовнішніми інструментами та джерелами даних [3]. Архітектурно MCP побудований на клієнт-серверній моделі з обміном повідомленнями за стандартом JSON-RPC: кожен корпоративний застосунок експонує власний MCP-сервер з описом інструментів, ресурсів і шаблонів промтів, а агент виступає клієнтом, який динамічно виявляє доступні можливості. Поряд із MCP формується ширша екосистема протоколів агентної взаємодії, серед яких варто виділити ACP та A2A, що покривають окремі рівні взаємодії та доповнюють MCP у повноцінному корпоративному стеку [4].

Для подолання обмежень класичного підходу із побудовою окремих адаптерів пропонується метод інтеграції AI-агентів на основі MCP, у якому корпоративні системи представляються однотипними MCP-серверами, а агенти-споживачі залишаються знеособленими щодо конкретного провайдера моделі. Метод доповнюється шаром zero-trust-авторизації та політик відкликання прав, що відповідає сучасним рекомендаціям щодо безпечного впровадження MCP у промислові середовища [5]. Архітектурною особливістю методу є виділення централізованого реєстру MCP-серверів, який забезпечує доменно-залежне відкриття інструментів і узгодження версій між агентами та постачальниками функціональності.

Метод визначає такі основні етапи інтеграції корпоративних систем з AI-агентами:

1) інвентаризація корпоративних IT-систем та формалізація інструментів і ресурсів, що мають бути доступні агентам;
2) реалізація MCP-серверів, що є обгортками над існуючими API ITSM, CRM, ERP та сховищ знань;
3) реєстрація MCP-серверів у централізованому каталозі з описом версій і прав доступу;
4) налаштування шару авторизації та політик RBAC/ABAC для кожної пари «агент-сервер»;
5) підключення агентів через MCP-клієнт із підтримкою динамічного виявлення інструментів;
6) моніторинг викликів інструментів, аудит ухвалених рішень та виявлення аномальної поведінки;
7) еволюція реєстру MCP-серверів за змінами корпоративних систем і вимог.

Для зіставлення запропонованого методу з відомими підходами до інтеграції корпоративних застосувань здійснено порівняльний аналіз ключових архітектурних рішень, результати якого наведено у таблиці 1.

Таблиця 1. Порівняння підходів до інтеграції AI-агентів із корпоративними IT-системами

Підхід	**Спосіб з'єднання**	**Сильні сторони**	**Обмеження**
Спеціалізовані адаптери	Власний код для кожної пари «агент-система»	Повний контроль над поведінкою інтеграції	Комбінаторне зростання кількості інтеграцій
Корпоративна шина сервісів (ESB)	Централізований брокер обміну повідомленнями	Зрілі інструменти, стандартизовані формати	Слабка підтримка семантики LLM-агентів
iPaaS / API-management	Хмарна платформа з готовими конекторами	Швидкий старт та широкий каталог конекторів	Замикання на постачальника платформи

Запропонований метод (MCP)	Універсальний JSON-RPC-протокол	Стандартизація, незалежність від моделі	Нова екосистема, що дозріває

На основі сформульованих етапів методу спроєктовано архітектуру програмного середовища, що його реалізує. Основні функціональні модулі такого середовища наведено у таблиці 2.

Таблиця 2. Функціональні модулі середовища підтримки MCP-інтеграції

Модуль	**Функції**
Реєстр MCP-серверів	Збереження каталогу MCP-серверів, версій і прав доступу
Шлюз авторизації	OAuth/OIDC-аутентифікація агентів і застосування політик
Маршрутизатор інструментів	Визначення цільового MCP-сервера для виклику кожної функції
Адаптер корпоративних API	Обгортка існуючих REST/SOAP-API у формат MCP-tools
Сервіс аудиту викликів	Збір телеметрії викликів і аналіз моделей використання
Менеджер життєвого циклу серверів	Автоматизація розгортання, оновлення та видалення серверів

Реалізація запропонованої архітектури зводить задачу інтеграції AI-агентів із корпоративними IT-системами до додавання нового MCP-сервера або клієнта замість розроблення індивідуальних адаптерів. Це знижує вартість підключення нових систем, спрощує заміну провайдера моделі та забезпечує єдиний механізм аудиту викликів інструментів.

Висновки

У роботі проаналізовано задачу інтеграції AI-агентів із корпоративними IT-системами та показано, що класичний підхід зі створенням окремих адаптерів призводить до неконтрольованого зростання кількості інтеграцій і не масштабується для промислових сценаріїв. Особливе значення проблема набуває в контексті безпеки, оскільки агенти, які отримують доступ до корпоративних даних, відкривають нові вектори атак, що потребують формалізованого протоколу та механізмів контролю доступу.

Запропоновано метод інтеграції AI-агентів на основі відкритого протоколу Model Context Protocol, який поєднує універсальний шар діалогу між моделями та корпоративними системами, централізований реєстр MCP-серверів, шар zero-trust-авторизації та сервіс аудиту викликів. Сформульовано основні етапи методу та визначено функціональні модулі підтримуючого програмного середовища. Емпіричні дослідження екосистеми MCP-серверів свідчать про швидке зростання кількості реалізацій та одночасну необхідність опрацювання питань безпеки, придатності до супроводу та якості коду серверів[6].

Список використаної літератури

1. Chakilam P. K. «Enterprise integration architecture: Bridging digital divides in modern organizations», DOI: 10.30574/wjarr.2025.26.2.1500, 2025. URL: https://wjarr.com/content/enterprise-integration-architecture-bridging-digital-divides-modern-organizations

2. Adusumilli T. «Unraveling microservices architecture for enterprise integration», DOI: 10.30574/wjarr.2025.26.1.1072, 2025. URL: https://wjarr.com/content/unraveling-microservices-architecture-enterprise-integration

3. Hou X., Zhao Y., Wang S., Wang H. «Model Context Protocol (MCP): Landscape, Security Threats, and Future Research Directions», DOI: 10.48550/arXiv.2503.23278, 2025. URL: https://arxiv.org/abs/2503.23278

4. Ehtesham A., Singh A., Gupta G. K., Kumar S. «A survey of agent interoperability protocols: Model Context Protocol (MCP), Agent Communication Protocol (ACP), Agent-to-Agent Protocol (A2A), and Agent Network Protocol (ANP)», DOI: 10.48550/arXiv.2505.02279, 2025. URL: https://arxiv.org/abs/2505.02279

5. Narajala V. S., Habler I. «Enterprise-Grade Security for the Model Context Protocol (MCP): Frameworks and Mitigation Strategies», DOI: 10.48550/arXiv.2504.08623, 2025. URL: https://arxiv.org/abs/2504.08623

6. Hasan M. M., Li H., Fallahzadeh E., Rajbahadur G. K., Adams B., Hassan A. E. «Model Context Protocol (MCP) at First Glance: Studying the Security and Maintainability of MCP Servers», DOI: 10.48550/arXiv.2506.13538, 2025. URL: https://arxiv.org/abs/2506.13538

Педосенко Денис Володимирович - студент групи 1ПІ-25м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: dpedosenko@gmail.com

Науковий керівник: Васильківський Микола Володимирович - канд. техн. наук, доцент, доцент кафедри інфокомунікаційних систем і технологій, Вінницький національний технічний університет, м. Вінниця, e-mail: mvasylkivskyj@vntu.edu.ua

Pedosenko Denys Volodymyrovych - student of group 1PI-25m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: dpedosenko@gmail.com

Academic supervisor: Vasylkivskyj Mykola Volodymyrovych - Cand. Sc. (Eng.), Associate Professor, Associate Professor of Infocommunication Systems and Technologies, Vinnytsia National Technical University, Vinnytsia, e-mail: mvasylkivskyj@vntu.edu.ua