УДК 004.8

MCP-ПРОТОКОЛ ЯК СТАНДАРТ ІНТЕГРАЦІЇ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ІЗ ЗОВНІШНІМИ ДАНИМИ ТА ІНСТРУМЕНТАМИ

Науменко Б.В, PhD
Київський національний університет технологій та дизайну
Чупринка Н.В., к.т.н, доцент
Київський національний університет технологій та дизайну

Ключові слова: LLM, MCP, AI-системи, цифрові рішення, інтелектуальні агенти.

У сучасних інформаційних системах великі мовні моделі (LLM) дедалі частіше використовуються не лише як засіб генерації тексту, а і як інтерфейс для роботи з документами, базами даних, корпоративними сервісами та цифровими інструментами. Однією з ключових проблем у цій сфері тривалий час залишалася відсутність уніфікованого способу підключення моделей до зовнішніх джерел контексту. Саме для розв'язання цієї проблеми було запропоновано Model Context Protocol (MCP) — відкритий протокол, що забезпечує стандартизовану взаємодію між AI-застосунками, джерелами даних і програмними інструментами.

MCP можна розглядати як універсальний інтерфейс обміну контекстом для систем штучного інтелекту. Його ідея полягає в тому, що замість створення окремих інтеграцій для кожної моделі, платформи чи сервісу, розробники можуть використовувати єдиний стандарт, який описує правила доступу до ресурсів, виклику інструментів і передавання структурованих підказок. У межах архітектури MCP одна сторона виступає клієнтом, тобто AI-застосунком, а інша — сервером, який надає моделі доступ до ресурсів, функцій або спеціалізованих сценаріїв взаємодії.

Важливою перевагою протоколу є його модульність. У специфікації виділяються базовий протокол, механізми ініціалізації та узгодження можливостей, серверні функції, а також клієнтські можливості. Такий підхід дає змогу гнучко впроваджувати MCP у різних середовищах: від локальних застосунків і середовищ розробки до корпоративних платформ та хмарних агентних систем. Для HTTP-взаємодії також передбачено механізми авторизації, що є важливим кроком до безпечного використання протоколу в реальних виробничих умовах.

Практичне значення MCP полягає в тому, що він зменшує фрагментацію AI-екосистеми. Замість великої кількості несумісних рішень формується єдиний стандарт, який спрощує повторне використання інтеграцій, підвищує переносимість рішень і прискорює розробку інтелектуальних агентів. Це особливо актуально для освіти, науки, бізнесу

та державного сектору, де мовні моделі повинні працювати з перевіреними джерелами даних, внутрішніми документами та спеціалізованими сервісами. Використання MCP дає можливість зробити відповіді моделей більш релевантними, контекстно точними та корисними для прийняття рішень.

В умовах швидкого розвитку штучного інтелекту та постійного вдосконалення великих мовних моделей, MCP має великий потенціал для сталого розвитку інфраструктури на основі AI. Очікується, що протокол буде адаптовано до нових вимог, таких як підтримка більш складних сценаріїв взаємодії, включаючи багаторівневі та мультиагентні системи. Наприклад, у майбутньому можливе розширення MCP для інтеграції з новими типами даних, такими як аудіо, відео або навіть сенсорні дані. Це дозволить створювати ще більш потужні й адаптивні системи для медичних, юридичних та технічних галузей, де точність і контекстуальність інформації є критичними. Крім того, протокол MCP може стати важливим інструментом для міждисциплінарних досліджень, де необхідно об'єднувати знання з різних галузей, таких як екологія, біотехнології, психологія або соціологія. Вдосконалення таких інтеграцій забезпечить ширший доступ до складних знань та сприятиме розвитку більш ефективних моделей для вирішення глобальних проблем. З впровадженням нових підходів до безпеки та етики, MCP може стати основою для довіри до AI-систем у критичних індустріях.

Отже, MCP-протокол є важливим кроком у розвитку інфраструктури сучасних AI-систем. Його впровадження сприяє стандартизації доступу до даних і цифрових інструментів, підвищує безпеку та масштабованість інтеграцій, а також створює підґрунтя для побудови більш надійних і функціональних інтелектуальних агентів.

У перспективі MCP може стати базовим технологічним стандартом для організації взаємодії між мовними моделями та цифровим середовищем.

Список використаних джерел

1. Anthropic. IntroducingtheMCP [Електронний ресурс]. –Режим доступу: https://www.anthropic.com/news/model-context-protocol?utm_source=chatgpt.com

2. MCP. Overview [Електронний ресурс]. – Режим доступу: https://modelcontextprotocol.io/specification/2025-06-18/basic?utm_source=chatgpt.com

3. MCP. Architecture overview [Електронний ресурс]. –Режим доступу:https://modelcontextprotocol.io/docs/learn/architecture?utm_source=chatgpt.com