

Протокол контекста модели (Model Context Protocol)

Синонимы: MCP

MCP (Model Context Protocol) — это стандарт с открытым исходным кодом для подключения приложений искусственного интеллекта (ИИ) к внешним системам, содержащим контекст для работы моделей. Он устраняет необходимость разработки множества специализированных (или индивидуальных) интеграций, позволяя ИИ-приложениям безопасно получать доступ к контексту в реальном времени через стандартизированную клиент-серверную архитектуру.

Основной целью разработки MCP является устранение необходимости самостоятельной реализации механизмов интеграции с внешними источниками данных, содержащими контекст для ИИ-моделей, и предоставление готовой стандартизированной, безопасной и эффективной архитектуры.

Быстрый и надежный доступ к контексту, т.е. информации, которую модели ИИ используют при генерации ответов, обеспечивает их точность и релевантность, а также позволяет снизить вероятность галлюцинаций. Кроме этого, MCP предоставляет универсальный интерфейс для чтения файлов, выполнения функций и обработки контекстных подсказок.

Основными элементами архитектуры MCP являются:

- **хост** — ИИ-приложение, которое координирует и управляет работой одного или нескольких клиентов MCP;
- **клиент** — компонент, обеспечивающий соединение между ИИ-приложениями и сервером MCP;
- **сервер** — обеспечивает соединение ИИ-приложения с внешними источниками данных (контекстом), и предоставляет инструменты для работы с ними.



Хост создает одного клиента для каждого сервера. А каждый клиент, в свою очередь, поддерживает выделенное соединение с соответствующим сервером. При первом подключении хост (ИИ-приложение) запрашивает у сервера перечень доступных инструментов (операций). Эти сведения сохраняются и используются в дальнейшем, поэтому модель «знает», куда обратиться и как сформировать запрос.

В результате пользователь может формулировать задачу на естественном языке, система обрабатывает запрос и возвращает готовое решение без каких-либо посредников, интерфейсов и ручных настроек. Например, может быть сформирован запрос: «Подготовь отчет о продажах за месяц и выдели три наиболее прибыльных направления». В результате модель обращается к соответствующим источникам данных, собирает и анализирует данные и возвращает готовый отчет.

Главное преимущество MCP заключается в устранении разрыва между системой ИИ и информационной инфраструктурой компании. Если в обычном случае каждое подключение требует ручной интеграции, написанной под конкретный сценарий, то MCP делает этот процесс естественным — хост автоматически предоставляет ИИ информацию, как с ним взаимодействовать.

В результате формируется экосистема, в которой данные и процессы не привязаны к конкретным приложениям. ИИ-агент может собрать отчет из CRM, обновить записи в ERP и выполнить анализ данных из аналитической платформы в режиме «единого окна». Например, менеджер может задать вопрос прямо в корпоративном чате, а система соберет ответ из множества источников, сопоставит данные и выдаст реальную картину бизнес-процессов, что позволит принимать более обоснованные решения.

Одним из наиболее перспективных направлений применения LLM является их встраивание в процессы управления бизнесом. Например, с их помощью можно извлекать документы из неструктурированных массивов данных, искать дополнительную информацию о брендах, генерировать новые признаки для обучающих данных. Для интеграции больших языковых моделей в аналитические процессы в платформе Loginom можно использовать библиотеку компонентов LLM Kit.

Более подробно с принципами построения и функционирования MCP можно ознакомиться в статье «MCP — протокол контекстного моделирования для ИИ».

Поддержка протокола MCP реализована в аналитической платформе Loginom.

Подробнее об архитектуре решения и сценариях его применения — в статье [«MCP-server Loginom: от «умных» ответов ИИ к реальным решениям»](#).