УДК 004.89

РАЗРАБОТКА ДИАЛОГОВОГО ИНТЕРФЕЙСА ДЛЯ АНАЛИЗА СИСТЕМНЫХ ЛОГОВ С ИСПОЛЬЗОВАНИЕМ LLM НА БАЗЕ ПРОТОКОЛА MCP И VICTORIA LOGS

Рахманов В. А. (ИТМО)
Научный руководитель – Преподаватель факультета инфокоммуникационных технологий Самохин Н. Ю.
(ИТМО)

Введение. Современные микросервисные архитектуры генерируют огромные объемы неструктурированных данных, анализ которых требует глубоких технических компетенций. Проект представляет собой диалоговый интерфейс (AI-ассистент), интегрированный с базой данных логов, который снижает порог входа для работы с данными наблюдаемости. Система ориентирована на три группы пользователей:

– DevOps-инженеры (для оперативного поиска причин сбоев и глубокого анализа инфраструктуры);

– Разработчики (для отладки приложений и понимания контекста ошибок без изучения синтаксиса базы данных);

– IT-менеджеры (для получения сводных отчетов о стабильности системы и метриках качества на естественном языке).

Основная часть. Для создания инфраструктуры интеллектуального анализа логов используется подход, основанный на открытых стандартах и высокопроизводительных компонентах:

VictoriaLogs – выбрана в качестве хранилища данных благодаря архитектуре без индексов для тела лога (структуры MergeTree), что обеспечивает высокую скорость вставки и сжатия данных, критичную для микросервисных сред.

Model Context Protocol (MCP) – используется как унифицированный слой абстракции, позволяющий LLM безопасно взаимодействовать с внешним контуром данных. MCP-сервер транслирует намерения пользователя в оптимизированные запросы LogsQL.

LLM (Large Language Model) – выполняет роль аналитического ядра, обеспечивая семантический поиск, автоматическую классификацию инцидентов и генерацию понятных отчетов (Summary) для управленческого персонала.

Архитектура решения предполагает развертывание в Docker-контейнерах, где MCP-агент выступает шлюзом безопасности (Read-Only) к данным, предотвращая несанкционированные изменения.

Выводы. Реализация данного подхода позволяет автоматизировать рутинные операции по мониторингу (MTTR), устранить семантический разрыв между техническими логами и

бизнес-показателями, а также обеспечить прозрачность процессов эксплуатации для всех участников команды разработки.

Список использованных источников:

1. Официальная документация Model Context Protocol [URL: https://modelcontextprotocol.io/introduction]
2. Valialkin A. Why we generate & collect logs: About the usability & cost of modern logging systems // VictoriaMetrics Blog. – 2023. [Electronic resource]
3. Официальная документация Victoria Metrics [URL: https://docs.victoriametrics.com/victorialogs/]