

Памятка: как оценить локального агента с DeepSeek

PDF для [downloads/checklist.pdf](#) должен дублировать практический блок статьи в удобном для печати виде: что проверить перед использованием DeepSeek в локальном или браузерном агентном workflow.

Маршрут интеграции

- Определите основной маршрут: официальный API DeepSeek, браузерная сессия или гибридная схема.
- Проверьте, какие модели используются: deepseek-v4-flash, deepseek-v4-pro или старые имена deepseek-chat и deepseek-reasoner.
- Учтите миграционный срок для старых имён моделей: 24 июля 2026 года 15:59 UTC.
- Опишите fallback: что делает агент, если DeepSeek, браузерная сессия или другой провайдер недоступны.

Безопасность локального рабочего пространства

- Разделите личные и рабочие браузерные профили.
- Проверьте, где хранятся cookies, сессии и логи агента.
- Ограничьте доступ агента к файлам и директориям минимально необходимым набором.
- Включите allow-list команд и запретите опасные операции без подтверждения.
- Используйте sandbox для действий с кодом и файлами.

Наблюдаемость и контроль результата

- Ведите журнал вызовов инструментов и маршрутов между моделями.
- Показывайте diff-before-write перед изменением файлов.
- Запускайте тесты перед применением изменений в рабочем проекте.
- Добавьте human-in-the-loop для операций с высоким риском.
- Оценивайте не только tokens/s, но и время до полезного результата.

Оценка качества модели

- Сравнивайте бенчмарки DeepSeek V4 с собственными тестами на рабочих задачах.
- Учитывайте hallucination risk и проверяйте факты человеком или тестами.
- Не переносите выводы из чата напрямую на агентный workflow с файлами и командами.
- Фиксируйте, когда система выбирает DeepSeek, Qwen или ChatGPT, чтобы маршрут был объяснимым.