

Чек-лист проверки identity-сбоя в LLM

PDF-чек-лист для [downloads/checklist.pdf](#) помогает команде быстро проверить, не путаются ли отображаемое имя модели, фактический backend и текстовое самописание ассистента.

Перед запуском теста

- Зафиксировать endpoint и тип совместимости API.
- Записать исходный model id из конфигурации клиента.
- Отдельно указать, используется ли Anthropic-compatible endpoint.
- Проверить, нет ли Claude-like имен в старых настройках, шаблонах prompt или UI.
- Сохранить версию SDK, gateway, proxy и agent-framework.

Во время запроса

- Сохранять request id и raw response metadata.
- Фиксировать фактический model id после маршрутизации, если он доступен.
- Записывать system prompt, developer-инструкции и пользовательский prompt.
- Указывать temperature и режим thinking или non-thinking.
- Отмечать fallback rules и правила mapping неподдерживаемых имен.

После ответа

- Не считать фразу модели о самой себе доказательством версии.
- Сверять самописание с API-метаданными и журналами инфраструктуры.
- Отмечать расхождения между UI, логами и ответом ассистента.
- Не включать спорные результаты в benchmark без воспроизводимых данных.
- Для production добавить identity checks к приемочным тестам качества, tool calling, latency и длинного контекста.