

Чек-лист: как защитить сессии агента от пустого callId

Материал предназначен для отдельной загрузки в `downloads/checklist.pdf`. В DOCX чек-лист следует оформить штатными заголовками и маркированными списками Word без ссылки на файл.

До записи в журнал

- Проверить, что идентификатор tool call является непустой строкой.
- Не считать пустую строку эквивалентом отсутствующего значения.
- Не позволять позднему streaming-чанку перезаписывать ранее валидный ID пустым значением.
- Проверить соответствие toolCallId и source.callId в результате инструмента.
- Применять к событию перед commit те же инварианты, которые проверяет loader при restore.

Для streaming и интеграций

- Протестировать последовательности: валидный ID, пустой ID, отсутствующее поле, null, повторный ID и несколько параллельных вызовов.
- Проверять resume после ошибки инструмента, а не только после успешного tool call.
- Запускать контрактные тесты для собственной связки модели, endpoint, прокси, SDK, версии Harness и набора инструментов.
- Логировать raw streaming-чанки отдельно от нормализованной истории сессии.

При инциденте

- Не ослаблять read-side validation только ради открытия журнала.
- Сделать резервную копию до любой ручной repair-операции.
- Фиксировать все изменения, внесённые в журнал вручную.
- Не исправлять один tool/result изолированно: проверить связанные tool-call события и поля, которые сопоставляет loader.
- Направлять некорректные события в quarantine с диагностикой, а не коммитить их в каноническую историю.