

Чек-лист: запуск UI-агента в рабочем интерфейсе

Памятка для команды, которая готовит Computer Use или другой UI-агент к работе с реальными данными. PDF-версия предназначена для сохранения и использования при внедрении.

До доступа к интерфейсу

- Проверить завершение staging и наличие ожидаемого артефакта.
- Проверить чтение временного файла и штатный health-check runtime.
- Проверить жизнеспособность helper-процесса в контрольном окне.
- Зафиксировать версии приложения, runtime, Node.js и операционной системы.
- Проверить sandbox, требуемые права и совместимость среды.

Перед изменяющей операцией

- Провести read-only проверку приложения, workspace и целевого объекта.
- Связать результат проверки с последующим действием.
- Выдать короткоживущее разрешение только на задачу и допустимый тип операции.
- Определить idempotency-ключ или другой способ исключить дублирование.
- Задать независимую проверку postcondition.

При сбое

- Разделить runtime_not_ready, ui_not_found, action_failed и postcondition_failed.
- Повторять только запуск, health-check и безопасные read-only шаги.
- Не повторять мутацию, пока не проверен результат предыдущей попытки.
- Выбрать fallback: коннектор, API, черновик, очередь или человек.
- Зафиксировать, был ли открыт интерфейс и начиналось ли реальное действие.