

Чек-лист: как проверить skill и plugin перед внедрением

Этот чек-лист стоит вынести в `downloads/checklist.pdf`. Он помогает команде пройти базовую проверку перед тем, как превращать агентный workflow в устанавливаемый и управляемый компонент.

1. Задача и результат

- Сформулирован конкретный рабочий процесс, а не абстрактная идея внедрения ИИ.
- Понятно, какой результат считается успешным для пользователя или отдела.
- Есть владелец результата: команда или роль, отвечающая за качество output.
- Задача повторяется достаточно часто, чтобы ее имело смысл оформлять как skill.

2. Skill как workflow-артефакт

- Описано, когда skill должен применяться и когда не должен активироваться.
- Заданы входные данные, шаги выполнения, ограничения и правила остановки.
- Указаны случаи, когда агент обязан запросить подтверждение человека.
- Документ можно версионировать, ревьюить и обновлять вместе с процессом.

3. Plugin и доступы

- Понятно, зачем нужен plugin: распространение, интеграции, установка или управление в рабочем пространстве.
- Установка plugin не расширяет права пользователя сверх исходных систем и ролей.
- Описаны внешние приложения, коннекторы и действия, которые может инициировать агент.
- Есть процедура отключения plugin и отзыва доступа.

4. Проверки качества

- Подготовлены типовые входы и ожидаемые признаки качественного результата.
- Есть негативные сценарии: нехватка данных, конфликтующие данные, отсутствие прав, высокий риск.
- Настроены evals или другой процесс регулярной проверки поведения агента.
- Понятна процедура отката изменений, если новая версия skill ухудшила результат.

5. Безопасность и эксплуатация

- Команда безопасности понимает, какие данные видит агент и какие действия он может выполнять.
- Ведутся журналы действий или другой доступный аудит работы agent workflow.
- Определены правила подтверждения необратимых или рискованных операций.
- Есть таксономия skills: названия, владельцы, версии, статус поддержки и область применения.