

Практический чек-лист для внедрения агентного ИИ

Сохраните этот список как рабочую рамку перед подключением агента к внутренним или внешним системам.

Полномочия и действия

- Разделите обратимые и необратимые действия агента.
- Определите, какие операции агент может выполнять самостоятельно.
- Настройте явное подтверждение для критичных действий.
- Выдавайте агенту минимально необходимые права.
- Опишите маршрут эскалации и условия остановки процесса.

Проверки и наблюдаемость

- Добавьте в evals типовые задачи, ошибки, конфликтные инструкции и неполные данные.
- Проверяйте случаи, в которых агент должен остановиться и запросить человека.
- Фиксируйте версию модели, входную задачу, вызовы инструментов и применённые политики.
- Сохраняйте подтверждения пользователя и значимые решения оркестратора.
- Подготовьте регрессионные проверки и процедуру отката при смене модели или конфигурации.

Приватность и ответственность

- Назначьте владельца процесса и ответственных за доступы.
- Определите сроки хранения журналов с учётом риска и приватности.
- Не собирайте пользовательские данные без необходимости.
- Проверьте, можно ли восстановить цепочку действий после ошибки.
- Регулярно пересматривайте границы автономии по мере расширения функций агента.