

Чек-лист внедрения skills для coding agents

PDF для скачивания: короткая проверка перед тем, как подключать skills или похожие контекстные пакеты к coding agents в команде.

1. Зафиксируйте источник и статус

- Проверьте, откуда взят skill: официальный репозиторий, внутренняя документация или сторонний пакет.
- Зафиксируйте URL, дату проверки и commit или версию, если они доступны.
- Отдельно отметьте, является ли пакет официально поддерживаемым продуктом или открытой заготовкой без SLA.
- Не подключайте skill из непроверенного источника к агенту, который имеет доступ к репозиториям или секретам.

2. Проверьте актуальность API и SDK

- Сверьте, какие SDK, endpoint и API-паттерны skill рекомендует использовать.
- Проверьте migration notes и запреты на deprecated-пакеты.
- Прогоните агент на нескольких типовых задачах генерации кода.
- Сравните результат с актуальной документацией и сборкой проекта.

3. Управляйте skill как зависимостью

- Добавьте версию или commit skill в инженерную документацию команды.
- Назначьте владельца, который отвечает за обновление контекста.
- Проверяйте изменения skill на тестовых задачах перед использованием в рабочих репозиториях.
- Храните историю обновлений и причин, по которым версия была изменена.

4. Не заменяйте инженерный контроль

- Оставьте обязательные тесты, code review и security review.
- Проверьте, не предлагает ли агент устаревшие импорты или небезопасные способы авторизации.
- Для enterprise-сценариев отдельно настройте права доступа, журналирование и human-in-the-loop.
- Не трактуйте показатели из README как гарантию production reliability.