

Чек-лист безопасного старта с Gemini CLI

PDF-чек-лист для [downloads/checklist.pdf](#) помогает команде быстро проверить, готов ли репозиторий и процесс разработки к эксперименту с терминальным AI-агентом.

Перед установкой

- Определите, зачем нужен Gemini CLI: объяснение кода, triage, review, документация, повторяемые изменения или CI/CD.
- Выберите безопасный тестовый репозиторий без production-секретов и чувствительных данных.
- Разделите личный эксперимент и командное использование: для команды заранее назначьте владельца процесса.
- Проверьте, какой канал доступа используется: OAuth, Gemini API key или Vertex AI.
- Зафиксируйте, какие данные допустимо отправлять в облачный API Google.

Права и безопасность

- Проверьте, какие файлы агент может читать и менять.
- Уберите из тестового окружения .env, токены, ключи и внутренние документы, которые не должны попадать в контекст модели.
- Включите подтверждение shell-команд там, где это возможно по настройкам процесса.
- Не запускайте агента с широкими правами в production-репозитории на первом этапе.
- Ограничьте MCP-интеграции только теми инструментами, которые действительно нужны для сценария.

Проектные инструкции

- Подготовьте GEMINI.md или аналогичный файл с правилами проекта.
- Опишите стиль кода, архитектурные ограничения и обязательные тесты.
- Укажите действия, которые агенту запрещены.
- Храните изменения инструкций в репозитории, чтобы их можно было обсуждать на review.
- Проверяйте, не противоречат ли проектные инструкции внутренним правилам безопасности команды.

Релизы и CI/CD

- Не используйте nightly и preview-версии в критичном CI/CD без тестового контура.
- Закрепляйте версии инструмента в автоматизированных сценариях.
- Перед обновлением проверяйте changelog.
- Сначала тестируйте headless-режим на безопасных задачах и небольших репозиториях.
- Логируйте результат работы агента так, чтобы команда могла восстановить цепочку действий.

После первого запуска

- Просмотрите все предложенные изменения до merge.
- Проверьте, какие команды агент предлагал или выполнял.
- Запустите тесты и линтеры вручную или через стандартный pipeline.
- Зафиксируйте, какие сценарии оказались полезными, а какие создают лишний риск.
- Не масштабируйте использование Gemini CLI, пока не понятны права, логи, ответственность и rollback.