Виктор Холостяков

ПРАКТИЧЕСКОЕ РУКОВОДСТВО ДЛЯ ПРЕДПРИНИМАТЕЛЯ И ПРОДУКТОВОЙ КОМАНДЫ

Как использовать ИИ для разработки и не сломать продукт

Где подходит вайб-кодинг, какие доступы нельзя отдавать агенту и что проверить перед рабочим запуском.

После чтения

Вы сможете разделить прототип и рабочую систему, назначить уровень контроля и пройти чек-лист допуска к запуску.

Работающий экран ещё не рабочая система

ИИ быстро собирает форму, калькулятор, бота или внутренний скрипт. Такой результат помогает проверить идею. Он не подтверждает безопасность, устойчивость и правильную работу на редких данных.

Прототип	Рабочая система
Показывает основной сценарий.	Обрабатывает ошибки, отмену, повтор и неполные данные.
Работает на ограниченном наборе примеров.	Имеет тесты для обычных и неблагоприятных случаев.
Может использовать временные данные.	Соблюдает правила доступа, хранения и удаления данных.
Допускает ручной перезапуск.	Имеет журнал событий, мониторинг и план восстановления.
Нужен для решения «идея полезна или нет».	Нужен для повторяемой работы пользователей.

> Сгенерированный код проходит тот же цикл безопасной разработки, что и код человека: требования, проверку, тесты, выпуск и поддержку.[1]

02 · ЦЕНА ОШИБКИ

Контроль зависит от последствий

Низкий риск

Личный скрипт, черновик формы, локальный калькулятор без рабочих данных и внешних пользователей.

Средний риск

Внутренний инструмент с рабочими данными, ограниченными пользователями и возможностью отката.

Высокий риск

Платежи, авторизация, персональные данные, договоры, медицина, безопасность или автоматические решения для клиента.

Риск	Минимальный контроль	До запуска
Низкий	Просмотр изменений и ручная проверка результата.	Проверить входные данные и возможность удалить прототип.
Средний	Ревью разработчика, тесты, резервная копия и ограниченные права.	Проверить восстановление и журнал ошибок.
Высокий	Профильное ревью безопасности, юридическая проверка и независимые тесты.	Получить формальное разрешение владельца риска.

> Скорость разработки не снижает цену ошибки. Чем шире доступ и серьёзнее последствия, тем больше независимого контроля нужно до запуска.

03 · ДОСТУПЫ И СЕКРЕТЫ

Агент видит больше, чем открытый файл

Инструмент разработки может читать репозиторий, вывод терминала, задачи, комментарии и страницы из сети. В таком контексте встречаются ключи, персональные данные и инструкции, которые меняют поведение агента.[2]

До запуска агента

- Уберите ключи из файлов проекта.
- Ограничьте каталоги и команды, которые доступны инструменту.
- Проверьте, какие данные сервис отправляет провайдеру.
- Сделайте резервную копию или отдельную ветку.

Не передавайте без необходимости

- Файлы `.env`, закрытые ключи и токены.
- Рабочую базу клиентов.
- Доступ к платёжной и производственной среде.
- Права на изменение правил сборки и развёртывания.

`.gitignore` не защищает файл от чтения. Он управляет Git, но не запрещает ИИ-инструменту читать файл с диска. Используйте настройки исключений самого инструмента и системные права доступа.[2]

04 · РЕВЬЮ И ТЕСТЫ

Проверяйте весь список изменений

Описание агента не заменяет просмотр кода. Проверьте каждый изменённый файл, включая зависимости, сценарии установки, сборку и настройки развёртывания.[2]

Проверка	Что искать	Почему важно
Полный diff	Неожиданные файлы, ослабленные проверки, сетевые запросы.	Агент может выйти за границы задачи.
Зависимости	Новые пакеты, версии, скрипты установки и известные уязвимости.	Код пакета выполняется с правами проекта.
Тесты	Удалённые проверки, слабые утверждения и лишние заглушки.	Зелёный тест может закрепить неверное поведение.
Бизнес-логика	Права пользователя, расчёты, статусы и повторные запросы.	Автоматический анализ не знает договорённостей бизнеса.
Ошибки	Пустые ответы, таймауты, повреждённые данные и отмена.	Основной сценарий редко показывает слабые места.

> Ручное ревью и автоматические проверки дополняют друг друга. Отдельно проверяйте бизнес-логику, авторизацию, конфигурацию и выпуск.[3]

05 · ВЫПУСК

Запускайте так, чтобы можно было остановить

1. **Ограничьте пользователей.** Сначала откройте инструмент небольшой внутренней группе.
2. **Ограничьте права.** Выдайте только те доступы, которые нужны для сценария.
3. **Подготовьте откат.** Проверьте резервную копию, предыдущую версию и способ выключить функцию.
4. **Записывайте события.** Сохраняйте ошибки, действия пользователя и критические решения системы.
5. **Следите после запуска.** Проверяйте качество, стоимость запросов, инциденты и изменения данных.

Запретите автоматический выпуск

Агент не должен сам принимать изменения, менять производственную среду или отключать защиту. Для чувствительных файлов настройте обязательное согласование владельца.

> Если продукт обрабатывает персональные данные, платежи или регулируемые решения, этот чек-лист не заменяет юридическую и профильную проверку.

Допуск к рабочему запуску

- [ ] Владелец продукта просмотрел полный список изменений.
- [ ] Разработчик проверил бизнес-логику и доступы.
- [ ] Тесты покрывают ошибочные и редкие входные данные.
- [ ] Зависимости проверены и закреплены по версиям.
- [ ] Секреты и рабочие данные исключены из контекста агента.
- [ ] Резервная копия и откат проверены.
- [ ] Есть журнал ошибок и ответственный за инцидент.

Источники

Проверено 2 августа 2026 года.

1. **[1] NIST SP 800-218A.** Практики безопасной разработки для систем и моделей с генеративным ИИ. Документ дополняет Secure Software Development Framework.
   csrc.nist.gov/pubs/sp/800/218/a/final
2. **[2] OWASP Secure Coding with AI Cheat Sheet.** Полный diff, зависимости, правила агента, секреты, доступ к среде и риски внешнего контекста.
   cheatsheetseries.owasp.org/.../Secure_Coding_with_AI
3. **[3] OWASP Secure Code Review Cheat Sheet.** Ручная проверка бизнес-логики, авторизации, конфигурации и выпуска в дополнение к автоматическим инструментам.
   cheatsheetseries.owasp.org/.../Secure_Code_Review

Проверить прототип перед запуском

Пришлите Виктору ссылку на репозиторий или описание архитектуры. Вы получите перечень проверок и границы первого рабочего выпуска.

Сайт: ai.godkod.ru
Telegram: @godkod_ai
Email: info@godkod.ru