

Чек-лист пилота Gemini-агента в production

PDF-файл для downloads/: короткая памятка для команды, которая проверяет готовность агентного сценария к production или зрелому пилоту.

Задача и границы агента

- Опишите одну основную задачу агента.
- Зафиксируйте действия, которые агент может выполнять сам.
- Перечислите действия, требующие подтверждения человеком.
- Назначьте владельца агента со стороны продукта, ИТ и безопасности.
- Опишите критерии остановки пилота.

Данные и инструменты

- Проверьте, какие корпоративные источники нужны агенту.
- Оцените свежесть, структуру и права доступа к данным.
- Не подключайте инструменты без конкретного сценария.
- Разделите read-only доступ и действия, меняющие состояние систем.
- Зафиксируйте данные, которые нельзя отправлять в модельный или внешний контур.

Runtime и эксплуатация

- Определите проект, регион и среду развертывания.
- Проверьте лимиты, квоты и ожидаемую стоимость.
- Настройте журналирование действий агента и вызовов инструментов.
- Опишите процесс обновления, rollback и удаления агента.
- Назначьте команду поддержки после пилота.

Безопасность и аудит

- Проведите security review workflow и сгенерированного кода.
- Проверьте сетевые маршруты, прокси и доступ к внутренним API.
- Ограничьте права сервисных аккаунтов минимально необходимым набором.
- Настройте хранение и ротацию секретов.
- Проверьте, что инцидент можно расследовать по логам.