

Чек-лист готовности AI-агента к production

PDF-версия чек-листа предназначена для сохранения и обсуждения на встрече продуктовой, инженерной, операционной и ИБ-команд.

Контракт задачи и автономия

- Определите результат задачи и цену ошибки.
- Разделите рекомендательные сценарии и автономные действия.
- Зафиксируйте запрещённые действия и действия, требующие подтверждения человека.
- Назначьте владельца процесса и владельца очереди исключений.

Инженерный и операционный контур

- Версионите модель, промпты, инструменты, данные и policy-конфигурацию.
- Соберите набор типовых, редких, конфликтных и уже проваленных сценариев.
- Настройте трассировки запросов, вызовов модели, поиска, инструментов и ошибок.
- Проверьте новую конфигурацию относительно стабильной до выпуска.
- Определите playbook, аварийную остановку и порядок отката версии.

Доступы, исключения и улучшения

- Выдайте агенту отдельную идентичность и минимально необходимые привилегии.
- Контролируйте разрешённые вызовы инструментов и их параметры.
- Мониторьте завершение задач, эскалации, отмены, ошибки инструментов, стоимость и соблюдение политик.
- Передавайте инциденты владельцу процесса, инженерам или ИБ по назначенному маршруту.
- Превращайте реальные ошибки и пограничные случаи в новые тесты, правила или изменения конфигурации.