

Чек-лист перед запуском агентной системы в продакшен

Этот чек-лист следует сверстать в статье штатными списками Word и отдельно выгрузить в [downloads/checklist.pdf](#). Перед запуском ответьте на каждый пункт документированным решением, а не общим подтверждением команды.

Полномочия и инструменты

- Составлен реестр всех инструментов, внешних зависимостей и фактических прав агента.
- Широкие постоянные ключи заменены минимальными, короткоживущими и отзывными полномочиями.
- Чтение, запись, публикация, удаление и администрирование разделены между разными инструментами и правами.
- Параметры каждого рискованного действия проверяются внешним policy layer.
- Документы, веб-страницы, письма и ответы внешних сервисов считаются недоверенным входом.

Состояние и аудит

- Общая память, очереди и заметки изолированы по tenant, рабочему процессу и run.
- Для артефактов фиксируются происхождение, создатель и срок хранения.
- Логи оркестратора, policy layer, IAM, сети, секретов и бизнес-системы можно сопоставить по идентификаторам.
- Отказы и заблокированные вызовы сохраняются вместе с причинами.
- Агент не может единолично изменить независимое хранилище аудита.

Подтверждения и остановка

- Для передачи данных, прав доступа, платежей, удаления, публикации и production-изменений определён human approval.
- Оператор видит нормализованный эффект операции, получателя, объём, объект и вариант отката.
- Одобрение связано с конкретными аргументами и ограниченным сроком действия.
- Настроены лимиты на tool calls, fan-out, объём данных и внешние направления.
- Kill switch, отзыв временных прав, остановка очереди и восстановление проверены на учебном сценарии.