

Чек-лист допуска skills и MCR-инструментов

Материал можно использовать как рабочую памятку перед подключением нового внешнего инструмента к агентному workflow. Для скачивания подготовьте PDF-файл <downloads/checklist-agent-skills-verification.pdf> и добавьте его отдельной строкой на лист Downloads.

Инвентаризация и происхождение

- Зафиксируйте название инструмента, пакет, URL, версию, владельца и зависимости.
- Сохраните описание методов и tool schema, с которыми компонент проходит допуск.
- Определите владельца риска и команду, ответственную за последующие изменения.

Права и данные

- Проверьте доступ к чтению, записи, удалению, файловой системе, shell, внутренней сети и секретам.
- Разделите сервисные аккаунты и OAuth-scopes по задачам и инструментам.
- Зафиксируйте разрешённые категории данных, адреса назначения и сетевые маршруты.

Проверка до production

- Протестируйте инструмент в staging или sandbox на штатных и ошибочных сценариях.
- Проверьте отказы в авторизации, лимиты, неожиданные ответы внешнего сервиса и попытки вывести чувствительные данные.
- Определите действия, для которых требуется подтверждение человека.

Контроль изменений и исполнения

- Настройте повторную проверку при изменении версии, зависимостей, scope, endpoint, schema или владельца.
- Применяйте политику к конкретному tool call, его аргументам, учётной записи и контексту данных.
- Сохраняйте трассу: задача, выбранный tool, аргументы, правило, подтверждение, ответ сервиса и версию компонента.
- Подготовьте механизм быстрого отзыва доступа и блокировки изменившейся версии.