Безопасность ИИ-агентов

Чек-лист перед подключением команды

Проверьте пункты вместе с ответственными. Отмечайте выполненное на бумаге; для остальных определите следующий шаг.

Руководитель и владелец данных

- [ ] Определены задачи, ответственные, допустимые данные и ожидаемые действия агента.
- [ ] Утверждены поставщик, тариф, договор, страны обработки и сроки хранения.
- [ ] Юрист проверил основания обработки, локализацию и трансграничную передачу, где она возникает.
- [ ] Сотрудники знают, как получить доступ и кому сообщить об ошибке или утечке.

IT и безопасность

- [ ] У каждого сотрудника свой аккаунт; настроены MFA/SSO, где доступны, и отзыв доступа при увольнении.
- [ ] Агент видит только рабочие папки и данные, необходимые его роли.
- [ ] Запись, отправка, публикация, удаление и платежи отделены от чтения и проверяются перед выполнением.
- [ ] Ключи, пароли и токены не лежат в Git, публичных файлах, промптах и логах; есть защищённое хранилище и ротация.
- [ ] Проверены MCP, skills, plugins, hooks и исходящие соединения, включая процессы вне sandbox.
- [ ] Если используется фильтр, он обрабатывает текст, файлы, изображения и результаты инструментов; при сбое отправка блокируется.
- [ ] Для локальной схемы проверены модель, поиск, логи, бэкапы и отсутствие внешнего fallback.
- [ ] Проверены отрицательные сценарии, отзыв ключей, остановка агента и восстановление данных.
- [ ] Перед публикацией приложения проверены авторизация, разграничение доступа и отсутствие секретов в клиентском коде.
- [ ] После обновлений повторяются ключевые проверки; назначен ответственный за поддержку.

Рекомендации для подготовки проекта. Не заменяют оценку конкретной системы и правовых условий обработки данных.