МИНИМАЛЬНЫЕ ПРАВА

ИИ-агент и CRM: границы доступа

Начните с конкретной роли и данных

Доступ — часть сценария, а не настройка «на потом». Сначала определите, что агенту действительно нужно увидеть и какое действие нельзя выполнить без человека.

Паспорт доступа

Процесс: _____. Владелец CRM: _____. Владелец сценария: _____. Набор данных: _____. Срок пересмотра: _____.

Матрица прав

Объект	Чтение	Изменение	Условие
Карточка клиента	Только нужные поля	Нет по умолчанию	Маскировать лишнее
Задача / обращение	Статус и контекст	Создать черновик	Проверка владельцем
Сделка / этап	Только для сценария	Только после подтверждения	Журнал причины
Контакты и теги	По необходимости	Нет без отдельного правила	Проверяемое основание

Чтение и изменение

Чтение не означает право менять. Даже безопасное на вид обновление может повлиять на отчёт, маршрут или коммуникацию. Для первого пилота предпочтительны просмотр, подготовка черновика и явное подтверждение человека перед записью.

КОНТРОЛЬ ИЗМЕНЕНИЙ

Назначьте согласование и откат

Ответственность должна быть ясна до первого изменения. Не используйте общие учётные записи и не разрешайте агенту обходить действующие правила CRM.

Поток для изменения данных

- Агент показывает предлагаемое изменение: поле, старое и новое значение, основание.
- Уполномоченный сотрудник подтверждает или отклоняет изменение.
- CRM сохраняет автора действия, время, версию сценария и ссылку на исходный запрос.
- При сомнении агент создаёт задачу владельцу вместо изменения записи.

Роли

Роль	Ответственность
Владелец процесса	Утверждает цель, метрику и допустимые действия.
Администратор CRM	Выдаёт минимальные права, пересматривает доступ и журнал.
Подтверждающий	Принимает изменения данных в согласованной очереди.
Ответственный за откат	Отключает доступ, отменяет изменение и фиксирует инцидент.

Проверка перед запуском

Как отозвать токен или роль: _____. Кто делает это вне рабочих часов: _____. Как найти и отменить последнее изменение: _____. Какой срок хранения журнала согласован: _____.

ИСТОЧНИКИ И СЛЕДУЮЩИЙ ШАГ

От проверки — к ограниченному пилоту

Редакция от 5 октября 2026 года. Это рабочий материал для команды, а не гарантия безопасности или результата. Проверьте свои требования к данным, доступам и контролю изменений до запуска. Материал не описывает и не обещает функции конкретного продукта.

Anthropic: Building effective agents
https://www.anthropic.com/engineering/building-effective-agents

Google Cloud Architecture Center: Choose agentic AI architecture components
https://docs.cloud.google.com/architecture/choose-agentic-ai-architecture-components

Начните с одного процесса

Назначьте владельца, подготовьте безопасную тестовую выборку и заранее зафиксируйте условие остановки. Расширяйте область только после разбора результатов пилота.

Вернуться к статье →