

Руководство пользователя

Ai Control Center (AiCC)

Нижний Новгород

2026

Оглавление

1. Введение	3
1.1. Что такое AiCC	3
1.2. Назначение системы в инфраструктуре заказчика	3
2. Вход в систему	4
3. Главное меню	4
3.1. Наблюдаемость	4
3.2. Настройка ИИ-контуров	4
3.3. Безопасность	4
3.4. Администрирование	5
4.1. Дашборд	6
4.2. ИИ-Платформы	6
4.3. Список LLM	6
4.4. ИИ Агенты	6
4.5. Сканеры безопасности	7
4.6. Профили безопасности	7
4.7. Реестр скиллов	7
4.8. Каталог угроз	7
4.9. Каталог анонимизации	7
4.10. Менеджер словарей	8
4.11. Запросы к LLM	8
4.12. Лимиты токенов	8
4.13. Логи системы	8
4.14. Настройки	8
5. Типовые сценарии	10
5.1. Посмотреть общую ситуацию по системе	10
5.2. Найти причину блокировки	10
5.3. Подключить новую платформу	10
5.4. Подключить новую модель	10
5.5. Создать нового агента	10
5.6. Настроить лимиты	10
6. Полезно помнить	11
7. Контакты технической поддержки	11

1. Введение

1.1. Что такое AiCC

Ai Control Center (AiCC) — централизованная система управления и контроля работы с ИИ-сервисами в организации. Она предназначена для безопасного и управляемого использования языковых моделей, внешних ИИ-платформ и корпоративных ИИ-агентов.

С практической точки зрения AiCC решает несколько задач заказчика:

- подключение внешних ИИ-платформ и моделей
- управление ИИ-агентами
- применение политик безопасности
- ведение журналов запросов и административных изменений
- контроль расхода токенов

AiCC позволяет не просто использовать ИИ-сервисы, а делать это в управляемом, прозрачном и контролируемом контуре. Система помогает обеспечить единые правила доступа, контроль настроек, наблюдаемость, аудит действий и соблюдение внутренних требований заказчика к информационной безопасности.

1.2. Назначение системы в инфраструктуре заказчика

В ИТ-инфраструктуре заказчика AiCC занимает место прикладного управляющего и контрольного слоя между пользовательскими/бизнес-системами и языковыми моделями.

Обычно AiCC используется как единая точка входа для обращений к ИИ-моделям:

- с одной стороны, к AiCC подключаются пользовательские приложения, внутренние сервисы, корпоративные порталы, боты и внешние ИИ-платформы
- с другой стороны, AiCC взаимодействует с подключёнными LLM и провайдерами моделей
- внутри этого контура AiCC применяет настройки доступа, политики безопасности, лимиты, анонимизацию, журналирование и правила использования агентов и скиллов

AiCC не заменяет корпоративные информационные системы заказчика и не заменяет сами языковые модели. Система выполняет иную роль: она объединяет работу с ИИ в едином контролируемом контуре и снижает риски, связанные с прямым и несогласованным доступом к моделям.

Для заказчика это означает, что AiCC становится:

- единой точкой управления подключёнными ИИ-сервисами
- единым местом контроля политик безопасности и доступа
- единым журналом запросов, событий и изменений настроек
- единым интерфейсом для операторов, администраторов и аудиторов

2. Вход в систему

1. Откройте страницу входа AiCC. <https://aicc-ai.ru/cabinet/access/>
2. Введите корпоративный email и пароль.
3. После входа откроется Дашборд.

Если пароль утерян, обратитесь к администратору AiCC. Состав доступных разделов зависит от ваших прав доступа.

ЛИЧНЫЙ КАБИНЕТ

Открыть существующий личный кабинет

Войдите, чтобы открыть клиентский кабинет или административный интерфейс по той же форме входа.

Email

team@company.ru

Пароль

Введите пароль

Забыли пароль?

Войти

Зарегистрироваться

Пользовательское соглашение

Политика обработки персональных данных

3. Главное меню

Главное меню AiCC сгруппировано по четырём блокам: «Наблюдаемость», «Настройка ИИ-контуров», «Безопасность», «Администрирование».

3.1. Наблюдаемость

- **Дашборд** — общая картина по запросам, блокировкам, токенам и стоимости за выбранный период.
- **Запросы к LLM** — подробный журнал обращений к моделям с фильтрами, деталями и выгрузкой.
- **Отчёты** — готовые отчёты по выбранному периоду с выгрузкой в PDF.

- **Логи системы** — журнал административных изменений.

3.2. Настройка ИИ-контуров

- **ИИ-Платформы** — подключение внешних ИИ-систем и управление их доступностью.
- **Список LLM** — каталог доступных моделей и их параметров.
- **ИИ Агенты** — рабочие конфигурации: платформа, модель, системный промпт, профиль безопасности и доступ.
- **Лимиты токенов** — контроль квот по пользователям, группам, агентам и моделям.

3.3. Безопасность

- **Сканеры безопасности** — список проверок входящих запросов и ответов модели.
- **Профили безопасности** — наборы правил и сканеров, которые назначаются объектам.
- **Реестр скиллов** — контроль инструментов и функций, которые используют агенты.
- **Каталог угроз** — справочник угроз и сигнатур, используемых в проверках.
- **Каталог анонимизации** — правила анонимизации данных.
- **Менеджер словарей** — версии словарей анонимизации и их привязка к платформам.

3.4. Администрирование

- **Настройки** — пользователи, группы, роли, интеграция с Active Directory и системные параметры.
- **О системе** — сведения о версии и описании системы.

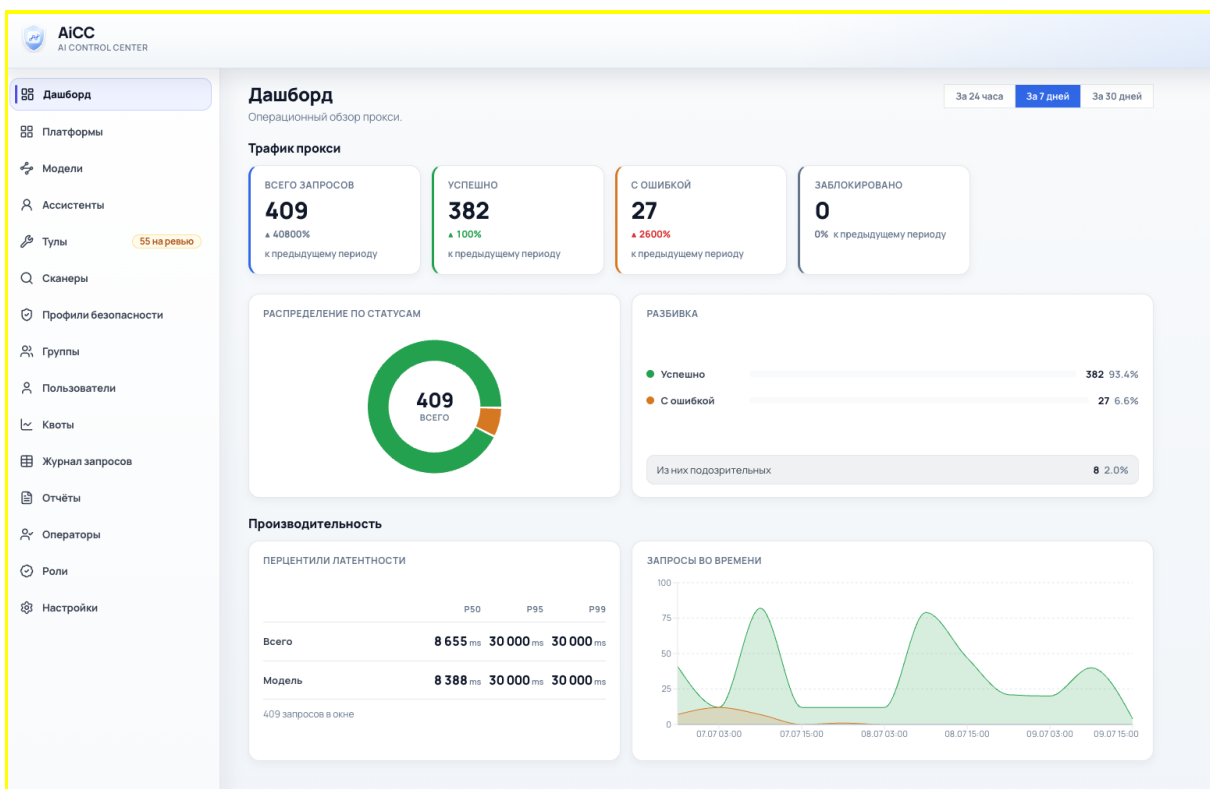
4. Ключевые разделы

4.1. Дашборд

Дашборд помогает быстро оценить текущую ситуацию в системе. В разделе доступны:

- выбор периода: день, неделя, месяц, квартал, год, произвольный
- ключевые показатели по запросам, блокировкам, токенам и стоимости
- графики по активности
- топы по пользователям, агентам и моделям
- список последних запросов

Если нужен разбор конкретного случая, переходите в раздел «Запросы к LLM».

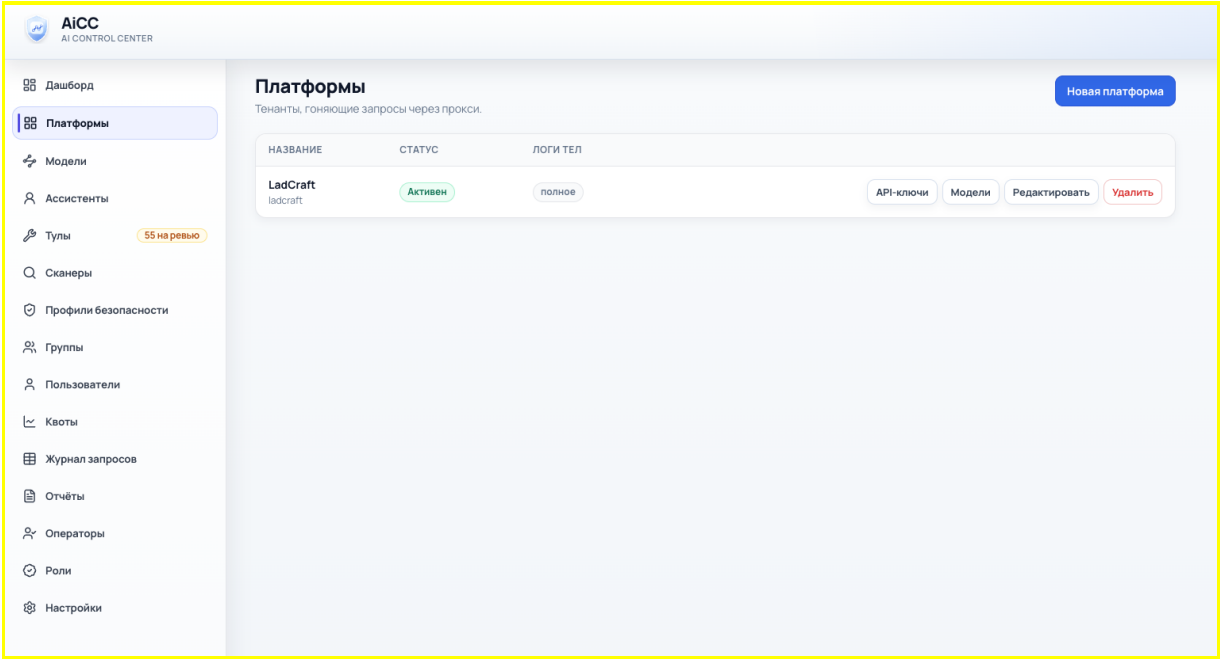


4.2. Платформы

Раздел предназначен для подключения и сопровождения внешних систем, работающих через AiCC. Здесь можно:

- создавать и редактировать платформы
- хранить параметры подключения
- включать и отключать платформы
- просматривать связанные модели и агентов

Отключение платформы сразу останавливает связанный с ней трафик.

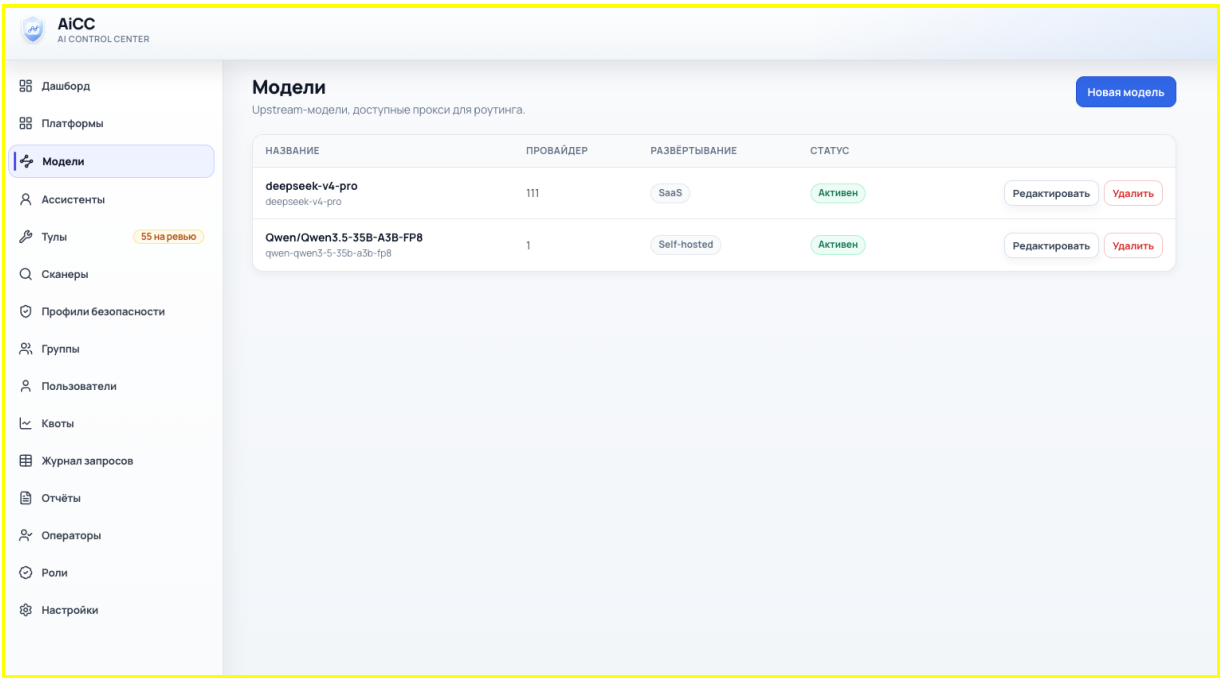


4.3. Модели

Здесь хранится каталог доступных моделей. В карточке модели задаются:

- название и провайдер
- модель и тип размещения
- параметры подключения
- стоимость токенов
- статус активности

Отключение модели делает её недоступной для связанных агентов.

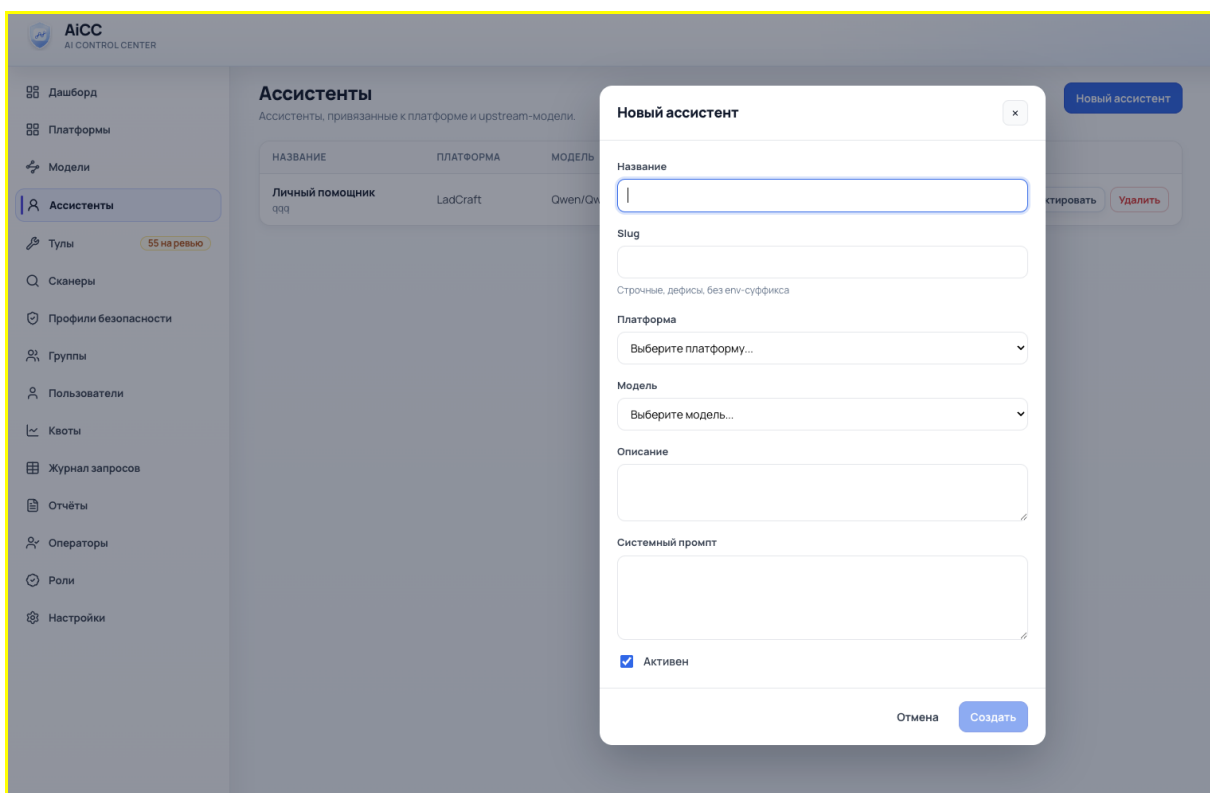
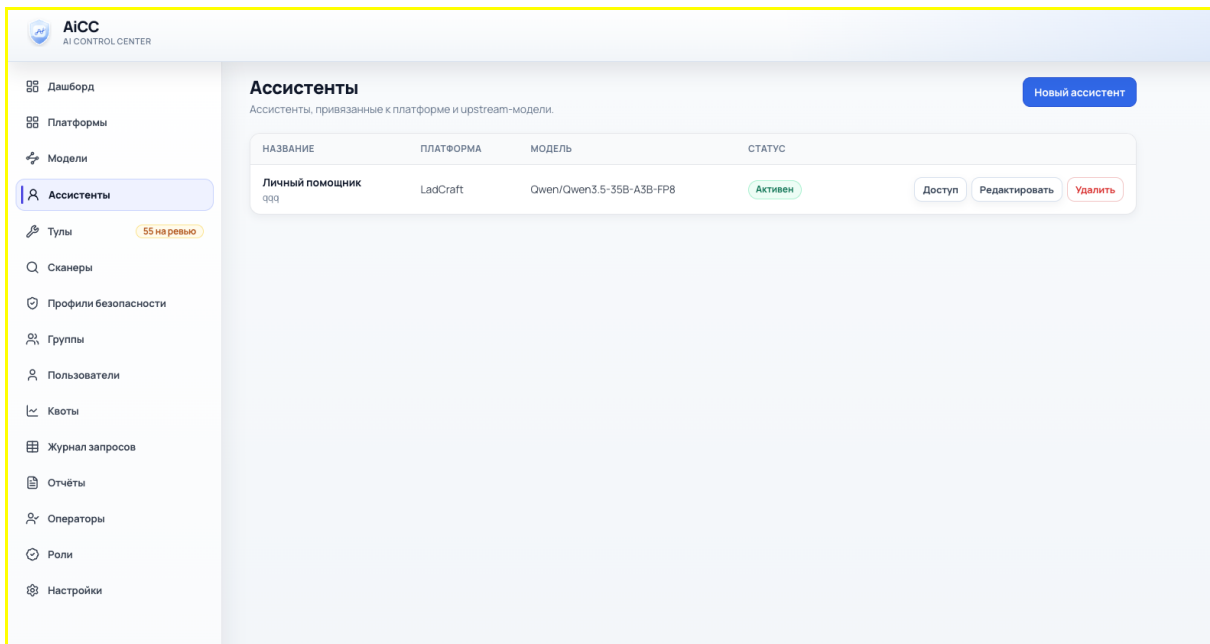


4.4. Ассистенты (Агенты)

Ассистенты — основная рабочая конфигурация в AiCC. В карточке ассистента настраиваются:

- платформа
- модель
- системный промпт
- профиль безопасности
- доступ пользователей и групп
- токен доступа

Ассистента можно временно отключить без удаления настроек.



4.5. Сканеры безопасности

Сканеры проверяют входящие запросы и исходящие ответы. В разделе можно:

- просматривать доступные проверки
- видеть направление работы сканера
- открывать карточку с описанием
- контролировать статус активности

Обычно сканеры применяются через Профили безопасности.

НАЗВАНИЕ	НАПРАВЛЕНИЕ	ВЕРСИЯ	СТАТУС	
Запрещённые темы scanner-ban-topics	оба	v1.0.0	активен	Схема
Вредоносное намерение scanner-harmful-intent	входящий	v1.0.0	активен	Схема
Промпт инъекция scanner-prompt-injection	входящий	v2.0.0	активен	Схема
Разрешённые шаблоны scanner-template-match	входящий	v1.0.0	активен	Схема
Небезопасный код scanner-unsafe-code	исходящий	v1.0.0	активен	Схема

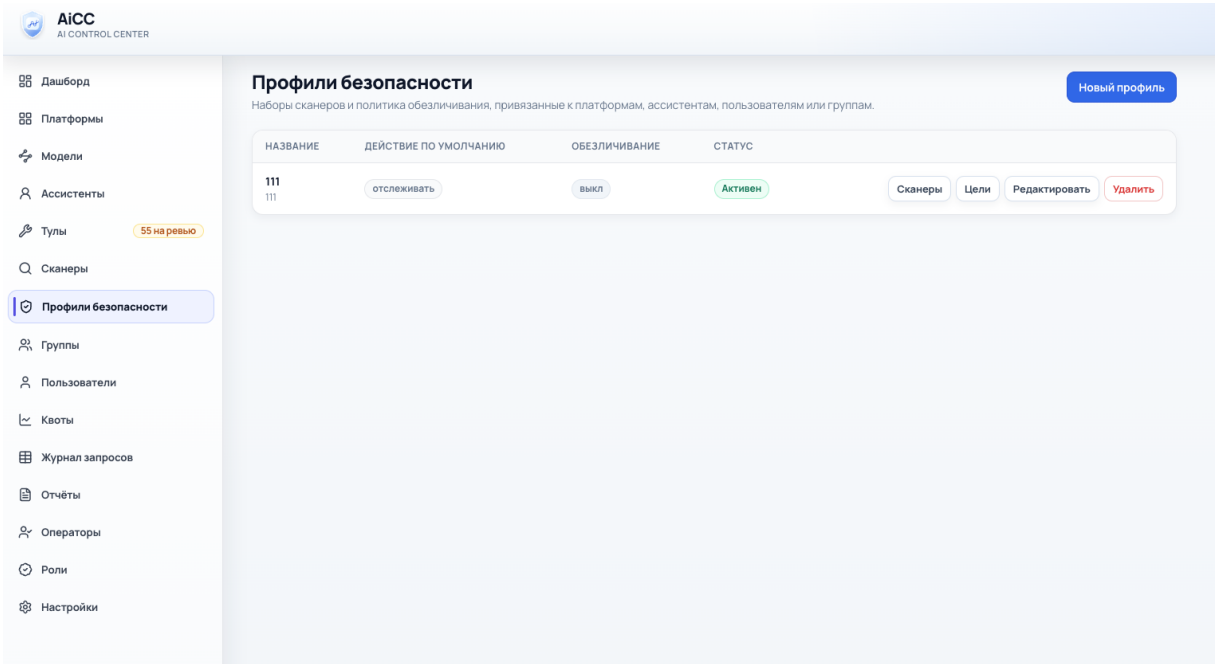
4.6. Профили безопасности

Профиль безопасности объединяет сканеры и правила реакции. Профили позволяют:

- настраивать проверки на входе и на выходе
- задавать действие при срабатывании
- применять одну политику сразу к нескольким объектам

Типовые варианты реакции:

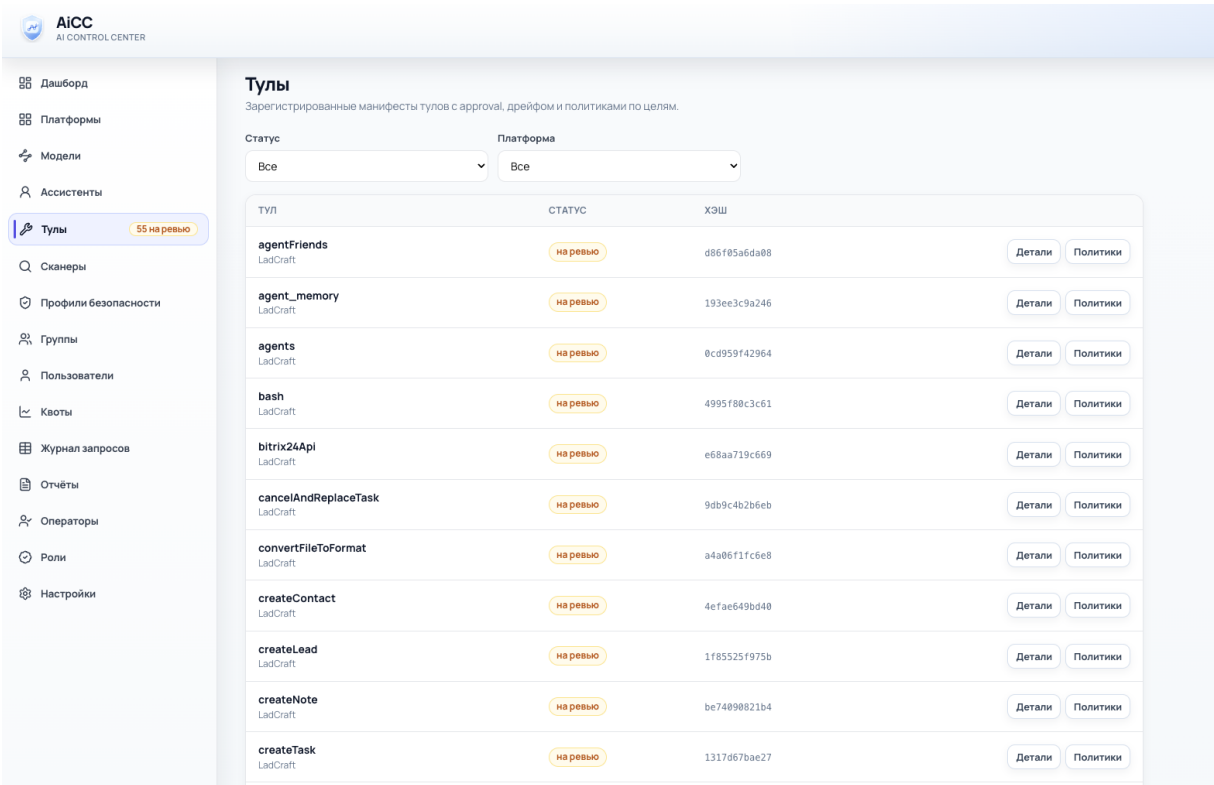
- заблокировать запрос
- пропустить и зафиксировать событие
- использовать только для статистики



4.7. Тулы (Скиллы)

Раздел предназначен для контроля инструментов, которые используют Ассистенты. В нём можно:

- найти нужный тул по фильтрам
- посмотреть его текущий статус
- задать базовую политику использования
- настроить точечные ограничения или разрешения



4.8. Журнал запросов

Это основной журнал работы системы. Раздел позволяет:

- фильтровать записи по периоду, агенту, пользователю, платформе, модели и результату
- открывать полную карточку запроса
- смотреть токены, стоимость, события проверок и статус обработки
- выгружать записи по текущим фильтрам в JSON или CSV

Используйте этот раздел, если нужно понять, что произошло с конкретным запросом.

Журнал запросов
Журнал прокси-запросов: статусы, вердикты сканеров и тела.

всего 410 с ошибкой 28 успешно 382

Платформа: Все Модель: Все Статус: Все С: ДД.ММ.ГГГГ, --:-- По: ДД.ММ.ГГГГ, --:--

ВРЕМЯ	СТАТУС	ПЛАТФОРМА	МОДЕЛЬ	ТОКЕНЫ	HTTP
16:10:34	успешно	LadCraft	deepseek-v4-pro	1449	200
16:00:40	успешно	LadCraft	deepseek-v4-pro	2354	200
15:01:05	успешно	LadCraft	deepseek-v4-pro	2329	200
15:00:46	успешно	LadCraft	deepseek-v4-pro	1397	200
14:56:41	успешно	LadCraft	deepseek-v4-pro	711	200
14:54:30	успешно	LadCraft	deepseek-v4-pro	903	200
14:52:34	успешно	LadCraft	deepseek-v4-pro	1026	200
14:50:41	успешно	LadCraft	deepseek-v4-pro	996	200
14:47:42	успешно	LadCraft	deepseek-v4-pro	1071	200
14:45:12	успешно	LadCraft	deepseek-v4-pro	885	200
14:44:09	успешно	LadCraft	deepseek-v4-pro	985	200
14:42:30	успешно	LadCraft	deepseek-v4-pro	806	200
14:41:02	успешно	LadCraft	deepseek-v4-pro	788	200
14:38:00	успешно	LadCraft	deepseek-v4-pro	846	200

4.9. Квоты

Здесь настраиваются и контролируются квоты потребления. В разделе доступны:

- базовые квоты пользователей
- дополнительные ограничения по группам, агентам и моделям
- визуальный контроль заполнения лимитов

АiCC

AI CONTROL CENTER

Дашборд

Платформы

Модели

Ассистенты

Туты

Сканеры

Профили безопасности

Группы

Пользователи

Квоты

Журнал запросов

Отчёты

Операторы

Роли

Настройки

Квоты использования

Новая квота

Композитные лимиты расхода токенов по пользователю, группе, ассистенту, модели или платформе.

ОБЛАСТЬ	ПЕРИОД	РАСХОД	СТОИМОСТЬ	С МОМЕНТА	
А qq qwen-qwen3-5-35b-a3b-tp8	месяц	Входные0 / 100 000 Выходные0 / 20 000	-	09.07.2026	Редактировать Удалить

Стр. 12 из 14

5. Типовые сценарии

5.1. Посмотреть общую ситуацию по системе

4. Откройте «Дашборд».
5. Выберите нужный период.
6. Проверьте ключевые показатели и последние запросы.
7. При необходимости перейдите в «Запросы к LLM».

5.2. Найти причину блокировки

8. Откройте «Запросы к LLM».
9. Найдите нужную запись через фильтры.
10. Откройте детали строки.
11. Проверьте статус, срабатывания сканеров и сообщение об ошибке.
12. При необходимости откройте связанный профиль безопасности или настройки агента.

5.3. Подключить новую платформу

13. Откройте «ИИ-Платформы».
14. Создайте новую запись.
15. Заполните параметры подключения.
16. Убедитесь, что платформа активна.
17. При необходимости свяжите её с моделями и агентами.

5.4. Подключить новую модель

18. Откройте «Список LLM».
19. Добавьте модель.
20. Заполните параметры подключения и тарификацию.
21. Активируйте модель.
22. Используйте её в карточках агентов.

5.5. Создать нового агента

23. Откройте «ИИ Агенты».
24. Создайте запись.
25. Укажите платформу, модель и системный промпт.
26. Назначьте профиль безопасности.
27. Настройте доступ и при необходимости токен доступа.

5.6. Настроить лимиты

28. Откройте «Лимиты токенов».
29. Проверьте базовые квоты пользователей.

30. При необходимости добавьте лимиты для группы, агента или модели.

31. Следите за цветовой индикацией заполнения.

6. Полезно помнить

- Если раздел недоступен, значит он не входит в ваши права доступа.
- Для анализа конкретного случая чаще всего достаточно разделов «Запросы к LLM» и «Логи системы».
- Перед отключением платформы, модели или агента убедитесь, что это не остановит рабочий трафик.
- Если вы не уверены, где искать информацию, начните с «Дашборд», затем переходите в «Запросы к LLM».

7. Контакты технической поддержки

- **Режим работы технической поддержки:**

Консультации по работе с Системой, а также круглосуточная регистрация заявок, осуществляются по адресу: support@aicc-ai.ru.

Режим работы технической поддержки: по будним дням с 9:00 до 18:00 по МСК (GMT +3).

- **Сайт:** <https://aicc-ai.ru/>