Функциональные характеристики

Ai Control Center (AiCC)

Нижний Новгород

2026

Функциональные характеристики AiCC

Назначение

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

AiCC выполняет роль прикладного управляющего и контрольного слоя между пользовательскими/бизнес-системами и языковыми моделями, обеспечивая единые правила доступа, контроль настроек, наблюдаемость, аудит действий и соблюдение внутренних требований заказчика к информационной безопасности.

Целевая аудитория

К целевой аудитории системы Ai Control Center (далее — Система) относятся:

- руководители ИТ- и ИБ-подразделений организации
- администраторы корпоративных ИИ-сервисов и AI-платформ
- сотрудники служб информационной безопасности и аудита
- операторы и аналитики, работающие с журналами обращений к ИИ
- владельцы корпоративных AI-агентов, ассистентов и пилотных AI-продуктов
- сотрудники, использующие подключённые корпоративные ИИ-сервисы (HR, юридические, финансовые, аналитические)

Описание системы

AiCC реализован как набор взаимосвязанных модулей, объединённых в единой веб-консоли управления. С одной стороны к системе подключаются пользовательские приложения, внутренние сервисы, корпоративные порталы, боты и внешние ИИ-платформы; с другой — Система 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.

Система имеет три логических уровня:

- **Уровень данных —** хранилища журналов запросов, конфигураций, профилей безопасности, словарей анонимизации, метрик использования;
- **Уровень приложения —** модули контроля, политик, агентов, скиллов, анонимизации, лимитов и аудита;
- **Уровень презентации —** веб-консоль администратора и API для интеграций с внешними системами.

С функциональной точки зрения система включает следующие основные модули:

- Модуль наблюдаемости (Дашборд, Запросы к LLM, Отчёты, Логи системы)
- Модуль управления ИИ-контурами (ИИ-Платформы, Список LLM, ИИ-Агенты, Лимиты токенов)

- Модуль безопасности (Сканеры, Профили безопасности, Реестр скиллов, Каталог угроз, Каталог анонимизации, Менеджер словарей)
- Модуль администрирования (пользователи, группы, роли, AD-интеграция, системные параметры)

Функциональные возможности

1. Наблюдаемость и аналитика

- Дашборд с ключевыми показателями: запросы, блокировки, токены, стоимость за выбранный период (день/неделя/месяц/квартал/год/произвольный)
- Графики активности, топы по пользователям, агентам и моделям
- Подробный журнал «Запросы к LLM» с фильтрами по периоду, агенту, пользователю, платформе, модели, результату
- Карточка запроса с детализацией: токены, стоимость, события проверок, статус обработки
- Выгрузка журнала в JSON и CSV
- Готовые отчёты с выгрузкой в PDF

2. Контроль и политики безопасности

- Проверка входящих запросов до отправки в LLM
- Проверка и ограничение исходящих ответов модели
- Применение политики ИБ одновременно к нескольким объектам (агентам, платформам)
- Сценарии реакции при срабатывании: блокировка, пропуск с фиксацией события, режим только для статистики

3. Защита данных и анонимизация

- Предотвращение отправки в модель персональных данных, секретов, паролей, токенов, внутренних документов
- Каталог анонимизации с правилами обезличивания
- Менеджер словарей анонимизации с управлением версиями и привязкой к платформам
- Каталог угроз и сигнатур, песочница для тестирования правил

4. Подключение внешних ИИ-платформ и LLM

- Создание и редактирование подключений к внешним ИИ-платформам
- Управление каталогом доступных LLM с параметрами подключения, стоимостью токенов и статусом активности
- Поддержка облачных и локальных LLM
- Включение/отключение платформ и моделей с немедленным эффектом для зависимого трафика

5. Управление ИИ-агентами

- Создание и настройка ИИ-агентов: платформа, модель, системный промпт
- Привязка профиля безопасности к агенту
- Управление доступом пользователей и групп к агенту
- Управление токенами доступа агентов
- Временное отключение агента без удаления настроек

6. Реестр скиллов

- Контроль инструментов и функций, которые используют ИИ-агенты
- Поиск скилла по фильтрам и просмотр текущего статуса
- Задание базовой политики использования (разрешён/запрещён/требует подтверждения)
- Точечные ограничения и разрешения по объектам системы

7. Лимиты токенов и контроль затрат

- Базовые квоты пользователей
- Дополнительные ограничения по группам, агентам и моделям
- Визуальный контроль заполнения лимитов с цветовой индикацией
- Сбор данных об использовании ИИ: запросы, ответы, модели, пользователи, стоимость

8. Управление пользователями, группами и ролями

- Регистрация и аутентификация пользователей
- Управление ролями и правами доступа
- Управление группами пользователей
- Интеграция с Active Directory (AD/LDAP)
- Системные параметры администрирования

9. Журнал административных действий (Логи системы)

- Регистрация всех изменений настроек
- Указание автора изменения, времени, объекта и характера изменения
- Отображение «было/стало» для конфигурационных изменений
- Журнал ведётся отдельно от журнала пользовательских запросов

10. О системе и эксплуатационные сведения

- Раздел «О системе» с сведениями о версии и описании
- Подсказки по доступности разделов в зависимости от прав пользователя

Интерфейс системы

Интерфейс AiCC организован в виде единой веб-консоли с четырьмя группами разделов:

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

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

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

Администрирование

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