# AITalon AIGate

Единая платформа управления AI-доступом, политиками безопасности моделей и агентов и контроль биллинга

AIGate ставит понятный контроль между сотрудниками, AI-агентами и внешними моделями: проверяет запросы, скрывает чувствительные данные и сохраняет полный журнал действий.

## 1. Единая платформа управления AI-доступом

### Управляющий контур и политики

- ✓ **Единая панель:** Интеграции, роли, бюджеты, аудит и правила задаются из одного административного контура.
- ✓ **Понятное масштабирование ИИ:** Встраивание в вашу архитектуру ИИ станет значительно легче через включение компонентов шлюза как безопасного барьера.
- ✓ **Защита от утечек:** Персональные данные, ключи, секреты, лимиты и настройки доступа остаются в защищенном контуре.

### Шлюзы и маршрутизация

- ✓ **Единая точка входа:** Один API для LLM, агентских инструментов, MCP и корпоративных интеграций.
- ✓ **Гибкие маршруты:** Переключение между провайдерами, моделями и бэкенд-сервисами без изменения клиентского кода.
- ✓ **Применение политик на лету:** Сервисная аутентификация, служебные заголовки и проверки исполнения выполняются в gateway-контуре.

| 1 | 100% | 0 |
|---|---|---|
| ЕДИНАЯ ТОЧКА ВХОДА | ПОЛНЫЙ ЖУРНАЛ ДЕЙСТВИЙ | ПРЯМЫХ КЛЮЧЕЙ В ПОЛЬЗОВАТЕЛЬСКИХ ПРИЛОЖЕНИЯХ |

## 2. Защита данных и корпоративных правил

### Маскирование данных и защита запросов

AIGate ставит понятный барьер между пользователем, агентом и внешней моделью: проверяет содержание запроса до отправки и фиксирует причины срабатываний.

- ✓ **Маскирование PII и секретов:** Номера телефонов, email, паспортные данные, секреты и коммерческая тайна скрываются до обращения к модели.
- ✓ **Контроль риска:** Prompt injection, обход защит, запрещенные темы и другие опасные сценарии можно предупреждать или блокировать.
- ✓ **Единый журнал:** Все решения политики, блокировки и модификации данных попадают в аудит для ИТ и ИБ.

## 3. Контроль AI-агентов и MCP/API

### Управляемые действия агентов

- ✓ **Подключение инструментов:** Корпоративные API и MCP-сервисы публикуются как управляемые функции для AI-агентов.
- ✓ **Явные разрешения:** Агент получает только те действия и методы, которые разрешены политикой и ролью.
- ✓ **Согласование риска:** Чувствительные write, delete и restart-операции можно переводить на подтверждение человеком.

### Единый контур для API и MCP

- ✓ **Один входной слой:** AIGate контролирует не только диалоги с LLM, но и HTTP, API и MCP-вызовы агентских приложений.
- ✓ **Изоляция и устойчивость:** Маршрутизация, сервисная аутентификация, разделение контуров и fallback работают в одном контуре.
- ✓ **Прозрачное исполнение:** Видны маршруты, бэкенд-сервисы и события пограничного или API-уровня без ручного разбора логов.

## 4. Управление доступом и запуском

### Подключение команд без операционного хаоса

Платформа помогает быстро вывести AI в рабочие процессы, не раздавая ключи и не множа несвязанные настройки.

- ✓ **Один способ подключения:** Команды, IDE и внутренние сервисы получают единый адрес и единые правила доступа.
- ✓ **SSO, роли и квоты:** Доступ пользователей и подразделений управляется централизованно.
- ✓ **Разделение сред:** Пилот, прод, локальный стенд и демо-контур можно изолировать друг от друга.

## 5. Биллинг, аудит и локальный контур

### Прозрачный биллинг и аналитика

- ✓ **Сквозная трассировка:** Видно, кто использует AI, какие модели и агенты вызываются и во сколько это обходится.
- ✓ **Лимиты и бюджеты:** Ограничения задаются по пользователям, моделям, периодам и проектам.
- ✓ **Основа для отчетности:** Данные подходят для расследований, управленческих отчетов и интеграции с SIEM.

### Локальное и защищенное размещение

- ✓ **Локальные полигоны:** Можно безопасно тестировать политики, чат, demo-app и агентские сценарии до выхода в прод.
- ✓ **Локальный контур и частное облако:** Данные, ключи, аудит и политики остаются внутри контролируемого контура.
- ✓ **Масштабирование без пересборки:** AIGate подходит и для пилота, и для enterprise-развертывания.