

Руководство оператора AgentOps

Практическое руководство по **ежедневной работе** с платформой AgentOps: вход, интерфейс, агенты, сценарии, стоимость, политики, аудит, аномалии и согласования (HITL).

PDF: полное руководство · отдельные главы

Для кого это руководство

Операторы, аналитики SOC, разработчики агентов и администраторы тенанта, которым нужно ****пользоваться**** уже развёрнутой системой.
Развёртывание и инфраструктура – в Admin Guide и Deployment.
Англоязычный User Guide: User Guide.

Что такое AgentOps

AgentOps — операционная панель управления AI-агентами: оркестрация, контроль затрат, маркетплейс и безопасность (ядро [AegisAI](#)).

Возможность	Зачем оператору
Рабочие процессы (Workflows)	Цепочки агентов, расписание cron, webhook, пауза на согласование
Стоимость (Cost)	Токены, задержки, бюджеты и остановка при превышении
Агенты и Discovery	Реестр агентов, «теневой» AI без регистрации
Политики	GDPR / HIPAA / ФЗ-152, OPA/Rego, fail-closed
Аудит и SIEM	Подписанный журнал действий, экспорт
Аномалии	ML-детектор отклонений поведения
HITL	Ручное одобрение рискованных действий
Маркетплейс	Публикация и установка пакетов агентов

Продакшен: agentops.fun · Документация: agentops.fun/documentation

Быстрый старт для оператора

1. Откройте веб-интерфейс (локально: `http://localhost:5173` , прод: `https://agentops.fun`).
2. Войдите по email/паролю или API-ключу (см. Вход в систему).
3. На **Dashboard** проверьте статус платформы (Online / Degraded) и KPI: Pending HITL, Anomalies, Agents.

4. Обработайте очередь **HITL** и новые **Anomalies**.
5. При необходимости запустите или проверьте **Workflows**, бюджеты в **Cost**.

Интерфейс на английском

Подписи кнопок и пунктов меню в продукте сейчас на ****английском****. В руководстве рядом с русскими названиями указаны английские лейблы UI, например: ****Одобрить**** (*Approve*).

Оглавление

Раздел	Содержание
Вход в систему	Логин, API-ключ, SSO, выход
Роли и права	Viewer → Super Admin, что видно в меню
Интерфейс	Навигация, Dashboard, уведомления
Агенты и Discovery	Реестр, карточка агента, Shadow AI
Рабочие процессы	Создание, запуск, cancel/retry, шаблоны
Стоимость и бюджеты	Spend, лимиты, алерты
Маркетплейс	Publish / Install
Политики безопасности	Шаблоны, создание, policy check
Аудит	Фильтры и экспорт
Аномалии и Prompt Guard	Разбор инцидентов, FP/TP
HITL — согласования	Approve / Reject
Пользователи и настройки	Users, Settings, API-ключи
Ежедневная работа	Чек-листы дня / недели
Реагирование на инциденты	Нарушения политик, бюджет, Shadow AI
Типовые проблемы	Что делать при ошибках
Глоссарий	EN ↔ RU

Схема работы оператора

[Диаграмма опущена в PDF — см. HTML-документацию.]