

Вопросы безопасности

Платформа работает с физическими устройствами, поэтому контроль доступа и безопасность — обязательная часть конфигурации.

Роли

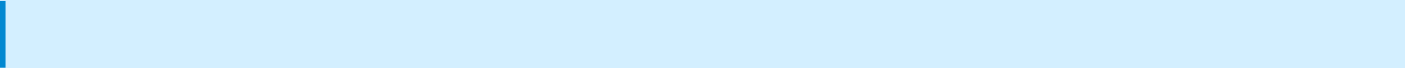
Роль	Права
Администратор	Управление платформой через WEB-портал: мониторинг роботов и операторов, настройка видимости роботов, настройка хранения данных, управление пользователями и API-ключами
Оператор	Подключение к доступным ему роботам, просмотр видео и телеметрии, управление, запуск своих моделей ИИ, мониторинг их работы
Модель ИИ	Сервисная учётная запись: чтение видео и телеметрии назначенных роботов, отправка команд управления
Робот	Устройство: передача видео и телеметрии, получение команд
Зритель (соревнования)	Просмотр трансляции и лидерборда без права управления

Меры безопасности

- **JWT** — авторизация пользователей веб-интерфейса и WebSocket-подключений.
- **RBAC** — ролевая модель: какие роботы видны оператору и какие действия ему разрешены.
- **API-ключи** — для моделей ИИ и внешних систем.
- **SSH-ключи** — для администрирования серверов.
- **Rate limiting** в Gateway — защита от перегрузки командами.

Права доступа

Администратор ограничивает, каких роботов видит каждый оператор. Оператор может подключиться и управлять только видимыми ему роботами; модели ИИ оператора получают доступ к тем же роботам.



На этапе демо-прототипа форма ограничения «видимости» роботов для операторов реализуется без функционала (только форма). Поле «Безопасность» в таблице подключений зарезервировано под будущие настройки прав доступа.

????????? ???????????

Одновременно роботу могут отправлять команды оператор и модели ИИ. Правила:

1. Команды **Стоп** и **DISARM** от любого авторизованного источника исполняются немедленно.
2. Команда оператора имеет приоритет над командой модели ИИ (режим «подстраховки»).
3. Модель ИИ управляет роботом, пока оператор не вмешался; после вмешательства управление возвращается модели по решению оператора.

????????? ?????????????? ??????????????????

- Перед запуском автономного режима проверьте работу кнопки **Стоп** на конкретном роботе.
- Бортовое ПО должно останавливать приводы при потере связи с сервером (см. [Примеры роботов](#) в книге «ПО для робота»).
- Для дронов после посадки всегда выполняйте **DISARM**.
- Используйте отдельную сеть (VLAN / Wi-Fi) для роботов полигона.
- Храните секреты (JWT, пароли, ключи) только в переменных окружения / Secrets, не в репозитории.
- Для публичного доступа используйте HTTPS/WSS (TLS-терминация на Ingress или обратном прокси).

Revision #3

Created 2026-09-23 09:32:03 UTC by Маслов Алексей

Updated 2026-09-23 09:34:56 UTC by Маслов Алексей