

Описание функциональных характеристик Встроенного программного обеспечения контроллера Aliot

версия 2025

1. Назначение системы

Встроенное программное обеспечение контроллера Aliot предназначено для мониторинга климатических параметров серверных помещений, управления доступом к серверным шкафам и контроля периферийных устройств... Используется для контроля параметров работы устройств, подключенных через последовательные интерфейсы, и управления встроенной платформой на ОС семейства Linux.

2. Состав функций системы

2.1. Функции аутентификации и авторизации

- Авторизация пользователя по логину и паролю.
- Возможность восстановления пароля.
- Функция «Запомнить» для сохранения учётных данных.
- Смена пароля администратора с проверкой сложности (не менее 6 символов).

2.2. Функции мониторинга состояния системы

- Отображение статуса аппаратной платформы:
 - Название, модель, архитектура, версия ОС и ядра.
 - Локальное время и время безотказной работы.
 - Загрузка ЦПУ.
 - Температура.
 - Информация о прошивке.
- Мониторинг использования памяти:
 - Оперативная память (ОЗУ).
 - Файл подкачки.
- Мониторинг сетевых интерфейсов:
 - Состояние Bluetooth, Ethernet (eth0), Wi-Fi (wlan0), локальных и виртуальных интерфейсов.
- Мониторинг хранилища:
 - Общий объём, доступное и свободное место.

2.3. Функции управления устройствами

- Отображение списка устройств, подключенных через UART.
- Отображение идентификатора, статуса (онлайн/оффлайн), источника данных.
- Детальная панель управления устройством:
 - График изменения данных в реальном времени.
 - Идентификатор устройства.
 - Журнал последних операций.
- Возможность создания операций для устройства (тип операции выбирается пользователем).

2.4. Функции администрирования системы

- Управление прошивкой:
 - Создание резервной копии конфигурации.
 - Восстановление конфигурации из архива.
 - Прошивка нового образа системы.
- Доступ к системным logs и данным телеметрии.

2.5. Функции работы с сетью

- Присвоение статического IP-адреса (eth0:1).
- Отображение MAC-адресов и состояния сетевых интерфейсов.

3. Требования к интерфейсам и интеграции

- Поддержка устройств с интерфейсом RS-485/UART через преобразователи FTDI.
- Веб-интерфейс на основе HTTP/HTTPS.
- Использование токенов аутентификации (JWT) для доступа к API.
- Поддержка архивирования и восстановления конфигураций.

4. Требования к безопасности

- Аутентификация пользователей.
- Шифрование передаваемых данных (токены JWT).
- Возможность смены пароля с проверкой сложности.
- Разграничение прав доступа (например, роль «администратор»).

5. Эксплуатационные характеристики

- Работа на аппаратной платформе Radxa CM3 с ОС Debian 11.
- Поддержка архитектуры ARM (Cortex-A55).
- Кросс-платформенный веб-доступ к интерфейсу управления.

/ Доможиров Е.В. /