

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КОНТРОЛЛЕРА WI-FI  
AQUARIUS WIRELESS LAN CONTROLLER  
Руководство по эксплуатации

Листов 20

## СОДЕРЖАНИЕ

|                                                 |    |
|-------------------------------------------------|----|
| 1. Назначение программы .....                   | 3  |
| 2. Условия выполнения программы .....           | 4  |
| 2.1. Требования к техническим средствам.....    | 4  |
| 2.2. Требования к программному обеспечению..... | 4  |
| 2.3. Требования к персоналу (оператору) .....   | 4  |
| 3. Выполнение программы .....                   | 5  |
| 3.1. Запуск программы .....                     | 5  |
| 3.2. Работа с веб-интерфейсом .....             | 5  |
| 4. Сообщения оператору .....                    | 18 |
| Перечень сокращений .....                       | 20 |

## 1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Программное обеспечение Aquarius Wireless LAN Controller (далее — AQ-WLC) реализует протокол централизованного управления беспроводными точками доступа CAPWAP (Control And Provisioning of Wireless Access Points) в соответствии с RFC 5415 и RFC 5416.

AQ-WLC предназначено для запуска на серверном или встраиваемом оборудовании под управлением Linux и выполняет функции Access Controller (AC) в инфраструктуре беспроводных сетей.

AQ-WLC выполняет следующие функции:

- централизованное управление точками доступа (Wireless Termination Points, WTP);
- поддержание защищённого управляющего канала (CAPWAP Control Plane) с применением DTLS;
- туннелирование пользовательского трафика (CAPWAP Data Plane) через TAP-интерфейсы;
- удалённая настройка параметров WTP через проприетарный протокол на основе VendorSpecificPayload;
- удалённое выполнение shell-команд на WTP (Remote Command);
- веб-интерфейс управления на базе Angular SPA с двухфакторной аутентификацией (TOTP + JWT).

## 2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

### 2.1. Требования к техническим средствам

Требования к составу и характеристикам технических средств представлены в таблице 1.

Таблица 1 — Требования к составу ТС

| ТС                                | Требования к ТС                                                                                      |
|-----------------------------------|------------------------------------------------------------------------------------------------------|
| Процессор                         | Архитектура x86-64 или ARM (Cortex-A53 и выше); не менее 8 ядер с тактовой частотой не менее 1,0 ГГц |
| Объём ОЗУ                         | Не менее 8 ГБ                                                                                        |
| Объём ПЗУ / дисковое пространство | Не менее 1 ГБ для размещения исполняемых файлов и сертификатов                                       |
| Сетевой интерфейс                 | Ethernet 100/1000 Мбит/с; для Data Plane рекомендуется Gigabit Ethernet                              |

Минимальные требования приведены исходя из фактически протестированных аппаратных платформ: Qualcomm IPQ8072A (Cortex-A53, 4 ядра) и Qualcomm IPQ5018 (2 ядра, 800 МГц).

### 2.2. Требования к программному обеспечению

Для запуска AQ-WLC необходима операционная система Linux с ядром версии 5.x и выше. Поддерживаются дистрибутивы на базе OpenWrt (QSDK) и стандартный Linux (Ubuntu, Debian и совместимые).

Зависимости времени выполнения:

- libssl / libcrypto (OpenSSL 1.1 или выше) для поддержки DTLS и HTTPS;
- поддержка TUN/TAP в ядре Linux (модуль TUN) для работы Data Plane;
- браузер (Chrome 90+, Firefox 88+ или совместимые) для доступа к веб-интерфейсу.

Для первоначальной настройки необходимо наличие приложения TOTP-аутентификатора (Google Authenticator, Authy или аналогичного) для получения кода двухфакторной аутентификации.

### 2.3. Требования к персоналу (оператору)

Основными требованиями, предъявляемыми к оператору, являются:

- базовые знания технологии беспроводных сетей стандарта IEEE 802.11;
- навыки работы с браузером и веб-интерфейсами;
- базовые знания стека протоколов TCP/IP;
- ознакомление с настоящим документом RU.AМПР.00202-01 34 01.

### 3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

#### 3.1. Запуск программы

После запуска AQ-WLC на сервере (Access Controller) веб-интерфейс становится доступен по следующему адресу:

```
https://[IP-адрес AC]/
```

По умолчанию веб-сервер прослушивает порт 443 (HTTPS). Для доступа необходимо открыть браузер и перейти по указанному адресу.

Запуск Access Controller из командной строки:

```
sudo output/ac/aq-wlc-AC <IP-адрес AC>
```

Дополнительные параметры командной строки AC представлены в таблице 2:

Таблица 2 — Дополнительные параметры командной строки AC

| Параметр            | Описание                                 |
|---------------------|------------------------------------------|
| ac_ip               | IP-адрес AC (обязательный параметр)      |
| --control-port=PORT | CAPWAP Control Port (по умолчанию: 5246) |
| --data-port=PORT    | CAPWAP Data Port (по умолчанию: 5247)    |
| --data-clear        | Использовать Clear Text Data Channel     |
| --data-dtls         | Использовать DTLS Data Channel           |

#### 3.2. Работа с веб-интерфейсом

##### 3.2.1. Аутентификация

Вход в веб-интерфейс AQ-WLC осуществляется по шестизначному TOTP-коду из приложения-аутентификатора. Отдельный ввод пароля не требуется: TOTP-код является единственным фактором аутентификации на странице входа.

Для входа необходимо:

- открыть браузер и перейти по адресу веб-интерфейса AC;
- открыть приложение-аутентификатор и получить текущий 6-значный код;
- ввести код в поля на странице входа и нажать кнопку «Войти» (рис. 1).

## Страница аутентификации

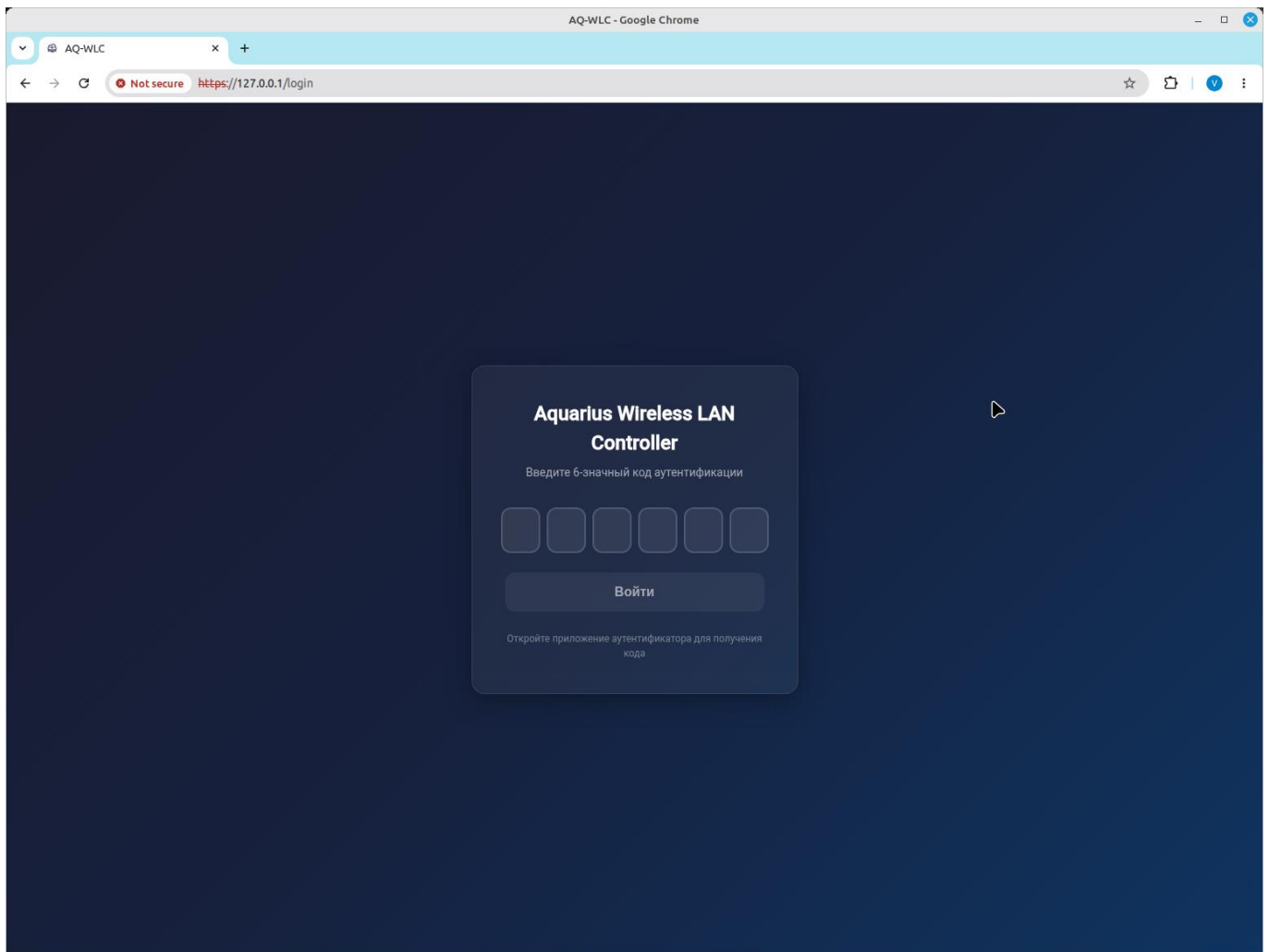


Рисунок 1

Система применяет эскалирующую блокировку при неудачных попытках входа: задержка увеличивается экспоненциально (1 с, 2 с, 4 с и далее), что защищает от подбора кода. После успешной аутентификации выдаётся JWT-токен сессии, хранящийся в HttpOnly-cookie со сроком действия 24 часа.

По истечении срока сессии или после явного выхода (кнопка «Выйти») пользователь перенаправляется на страницу входа.

### 3.2.2. Главная страница «Панель управления»

После успешной аутентификации отображается главная страница «Панель управления» (рис. 2). В текущей версии «Панель управления» является начальной страницей навигации и обеспечивает быстрый доступ к разделу «Устройства WTP» и настройкам системы.

## Главная страница Dashboard

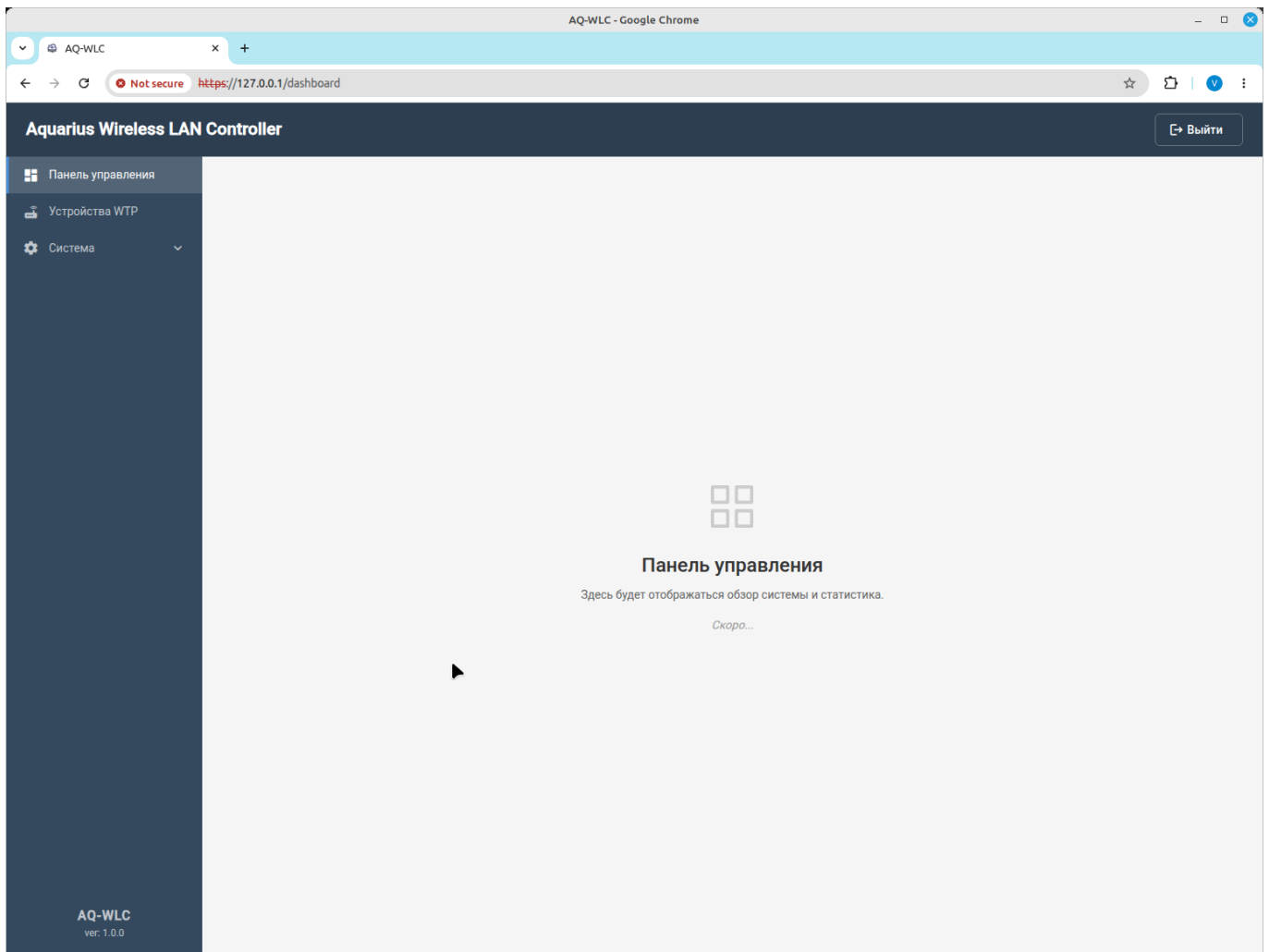


Рисунок 2

Примечание. Расширенный мониторинг и статистика на панели управления находятся в разработке.

### 3.2.3. Список WTP-устройств

Раздел «Устройства WTP» (рис. 3) является основным рабочим разделом интерфейса. В таблице отображаются все WTP-устройства, подключённые к АС в текущий момент.

Список подключённых WTP-устройств

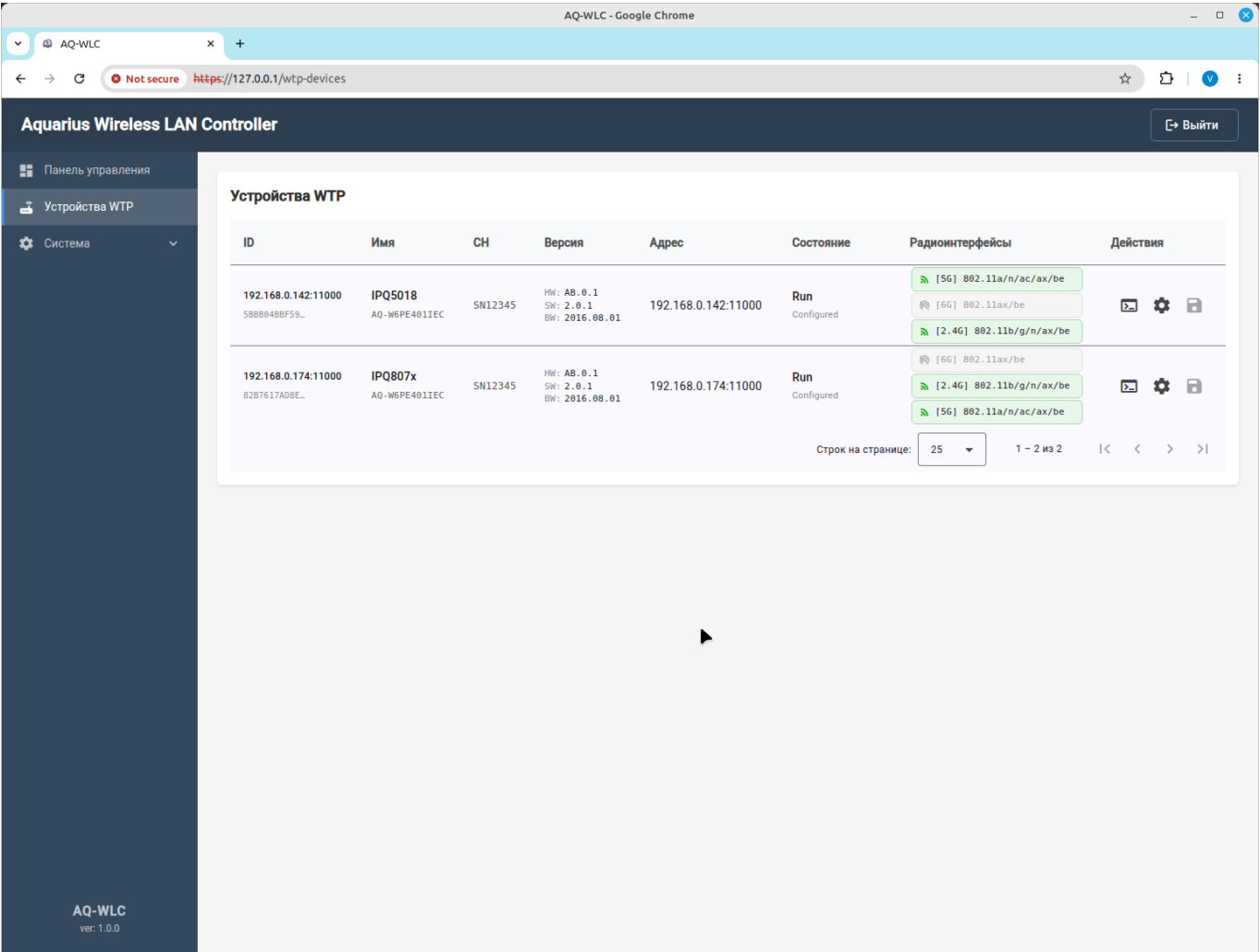


Рисунок 3

Для каждого устройства в таблице отображаются следующие параметры (таблица 1):

Таблица 1 — Параметры WTP-устройств

| Колонка   | Описание                                                                             |
|-----------|--------------------------------------------------------------------------------------|
| ID        | Идентификатор сессии (IP-адрес: порт WTP)                                            |
| Имя       | Имя устройства и модель (из конфигурации WTP)                                        |
| SN        | Серийный номер устройства                                                            |
| Версия    | Версии аппаратного обеспечения (HW), программного обеспечения (SW) и загрузчика (BW) |
| Адрес     | IP-адрес и порт управляющего канала                                                  |
| Состояние | Текущее состояние конечного автомата CAPWAP (Run, Join и т. д.)                      |

| Колонка         | Описание                                                                        |
|-----------------|---------------------------------------------------------------------------------|
| Радиоинтерфейсы | Список радиомодулей с цветовой индикацией (зелёный — включён, серый — выключен) |
| Действия        | Кнопки управления устройством                                                   |
| ID              | Идентификатор сессии (IP-адрес: порт WTP)                                       |

В столбце «Действия» для каждого устройства доступны следующие действия:

- кнопка «>\_» (Терминал) — открыть терминал удалённого выполнения команд;
- кнопка «Настройки» (шестерёнка) — открыть диалог конфигурации WTP;
- кнопка «Применить изменения» (значок диска) — сохранить несохранённые изменения конфигурации в постоянную память WTP (активна только при наличии несохранённых изменений).

#### 3.2.4. Настройка радиомодуля

Для открытия диалога настройки радиомодуля необходимо нажать на индикатор нужного радиомодуля в столбце «Радиоинтерфейсы» таблицы WTP-устройств. Диалог отображает параметры выбранного радиомодуля и позволяет их изменить (рис. 4, 5).

## Диалог настройки радиомодуля

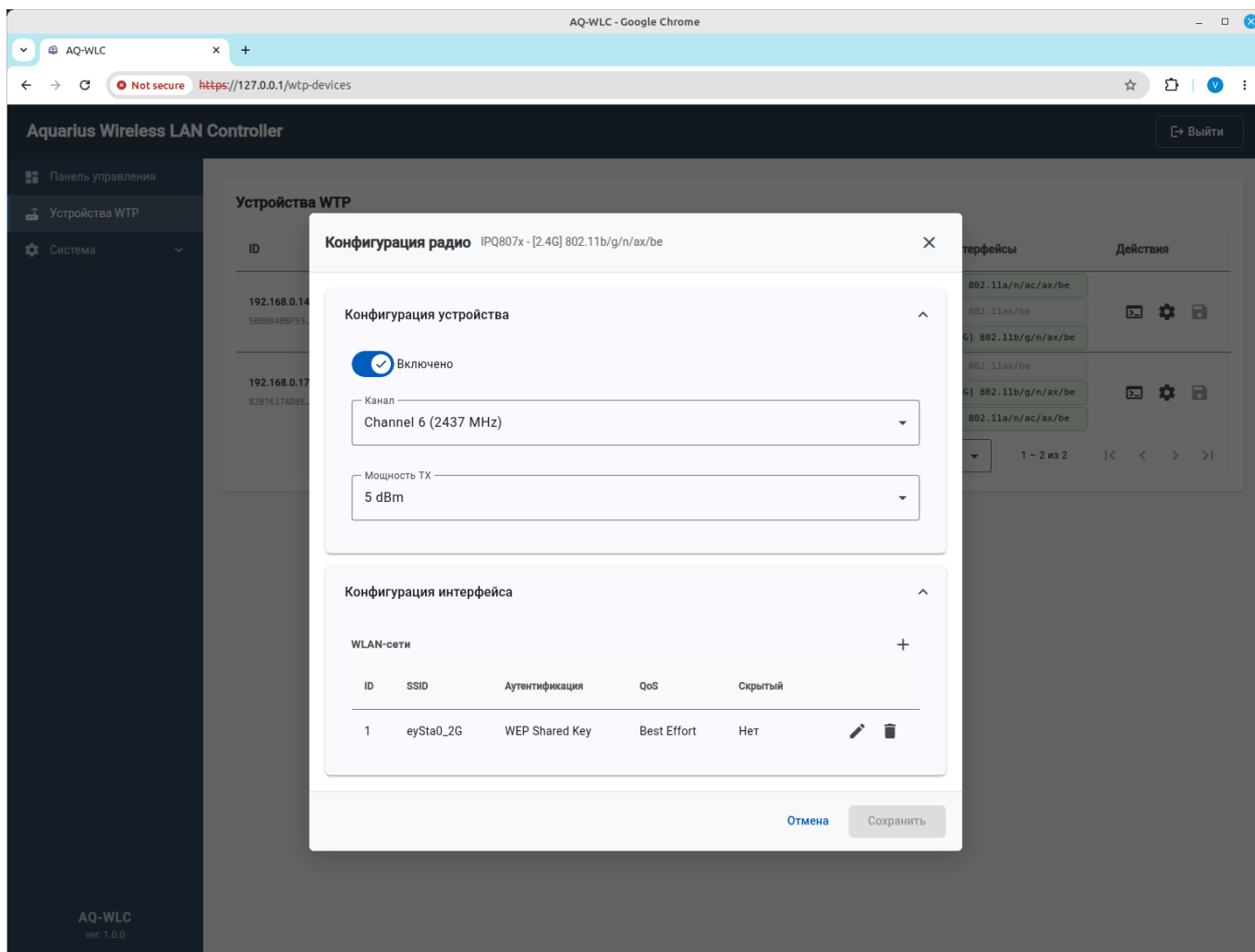


Рисунок 4

## Диалог настройки радиомодуля (заполненные поля)

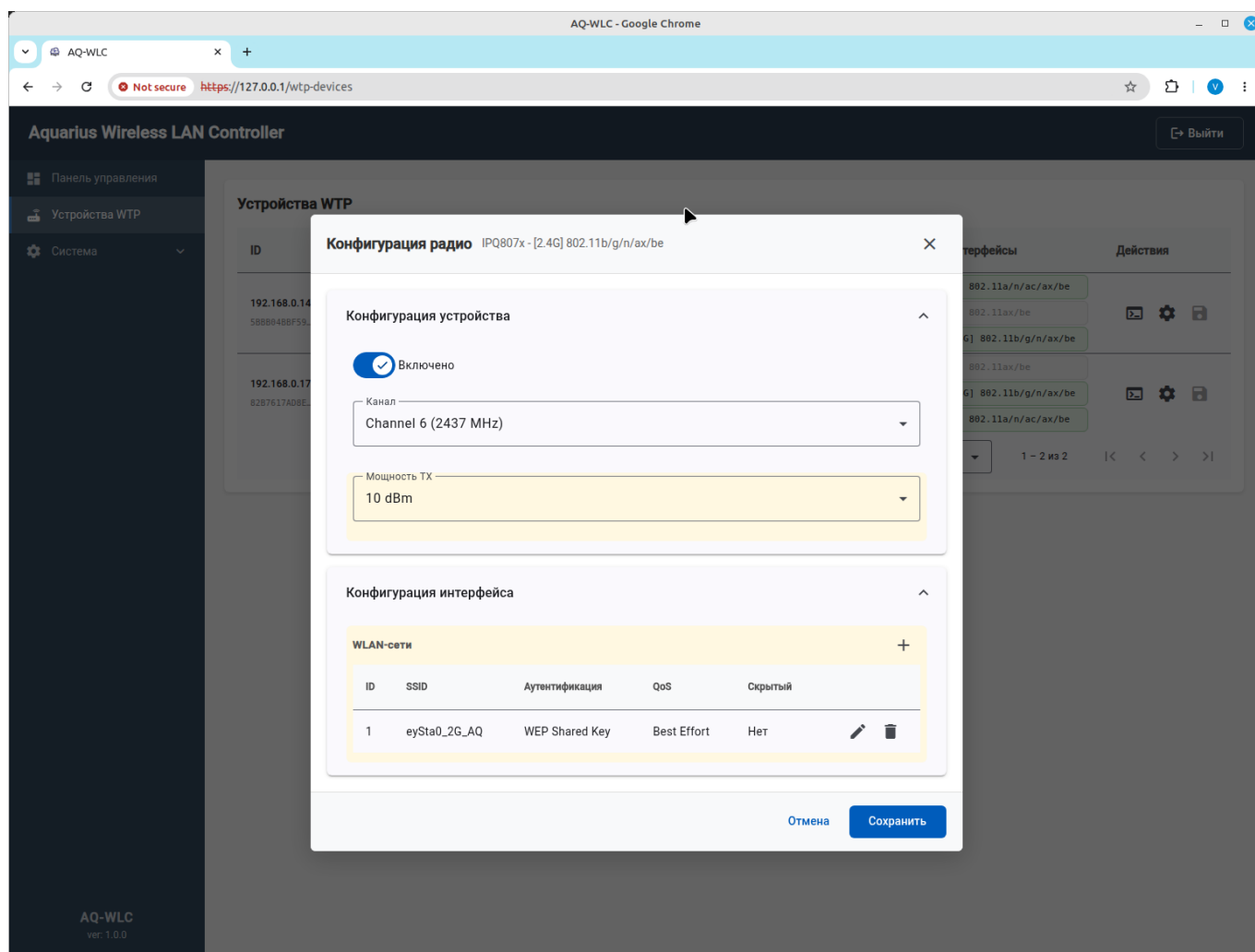


Рисунок 5

Диалог содержит две группы параметров.

Группа «Конфигурация устройства» представлена в таблице 3.

Таблица 3 — Группа «Конфигурация устройства»

| Параметр    | Описание                                                     |
|-------------|--------------------------------------------------------------|
| Включено    | Включение/выключение радиомодуля                             |
| Канал       | Выбор рабочего канала (для 2,4 ГГц: 1–13; для 5 ГГц: 36–165) |
| Мощность TX | Мощность передатчика (от –40 дБм до +20/+23 дБм)             |

Группа «Конфигурация интерфейса» представлена в таблице 4.

Таблица 4 — Группа «Конфигурация интерфейса»

| Параметр | Описание   |
|----------|------------|
| ID       | Номер WLAN |

|                |                                                   |
|----------------|---------------------------------------------------|
| SSID           | Имя беспроводной сети (до 32 символов)            |
| Аутентификация | Тип шифрования: None, WPA2, WPA3, WPA2/WPA3 Mixed |
| QoS            | Quality of Service, определяет приоритет трафика  |
| Скрытый        | Скрывает имя сети                                 |

Наборы каналов и доступные опции шифрования автоматически адаптируются под стандарт конкретного радиомодуля. Для сохранения изменений необходимо нажать кнопку «Сохранить». Для отмены — кнопку «Отмена».

### 3.2.5. Конфигурация WTP-устройства

Диалог конфигурации WTP открывается нажатием кнопки «Настройки» (шестерёнка) в столбце «Действия» для выбранного устройства (рис. 6, 7). Диалог содержит группы параметров устройства.

Диалог конфигурации WTP (группа «Идентификация» раскрыта)

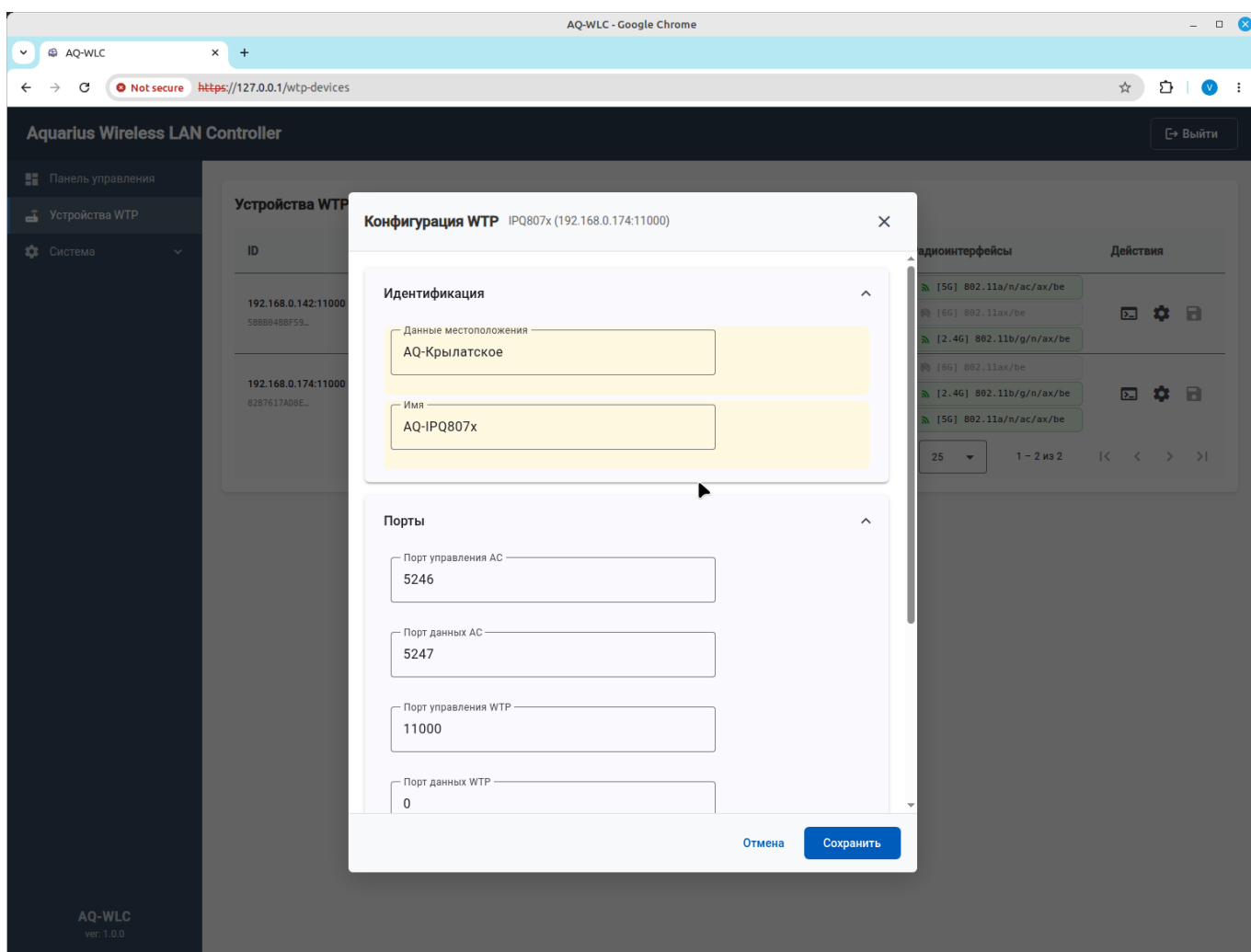


Рисунок 6

## Диалог конфигурации WTP (все группы свёрнуты)

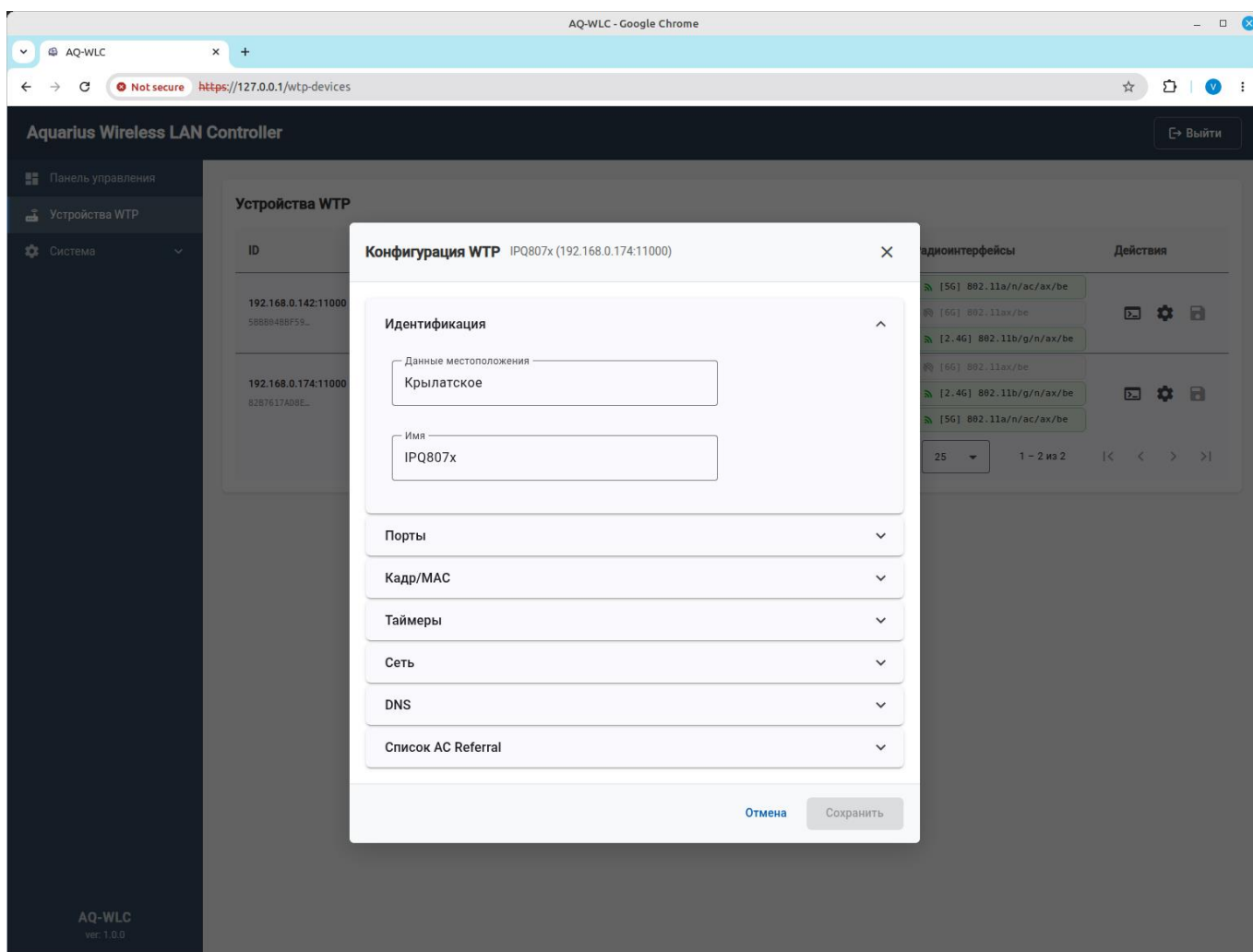


Рисунок 7

Параметры сгруппированы по категориям (таблица 5).

Таблица 5 — Категории параметров

| Группа        | Параметры                                                                                                                     |
|---------------|-------------------------------------------------------------------------------------------------------------------------------|
| Идентификация | Имя (имя устройства), Данные местоположения (местоположение)                                                                  |
| Порты         | Порт управления AC, Порт данных AC, Порт управления WTP, Порт данных WTP                                                      |
| Кадр/MAC      | Локальное переключение, Кадры Native IEEE 802.3, Беспроводные кадры Native, Тип MAC, Поддержка ECN                            |
| Таймеры       | Таймер статистики (с), Интервал повтора (мс), Макс. повторов, Keep Alive канала данных (мс), Dead Interval канала данных (мс) |
| Сеть          | Длина TAP MTU, Размер буфера сокета, Broadcast-настройки                                                                      |
| DNS           | Список DNS-серверов (до 4 записей)                                                                                            |

| Группа             | Параметры                                         |
|--------------------|---------------------------------------------------|
| Список AC Referral | Список AC-серверов для обнаружений (до 8 записей) |

Изменённые параметры подсвечиваются в диалоге. Нажатие кнопки «Сохранить» отправляет изменения на устройство. Нажатие «Отмена» отменяет все несохранённые изменения.

После нажатия «Сохранить» изменения применяются в оперативной памяти WTP, но не сохраняются в постоянную память до явного выполнения операции «Применить изменения» (см. п. 3.2.6).

### 3.2.6. Терминал удалённого выполнения команд

Интерактивный терминал позволяет выполнять shell-команды непосредственно на WTP-устройстве. Для открытия терминала необходимо нажать кнопку «>\_» в столбце «Действия» для нужного устройства (рис. 8, 9).

#### Диалог терминала (до ввода команды)

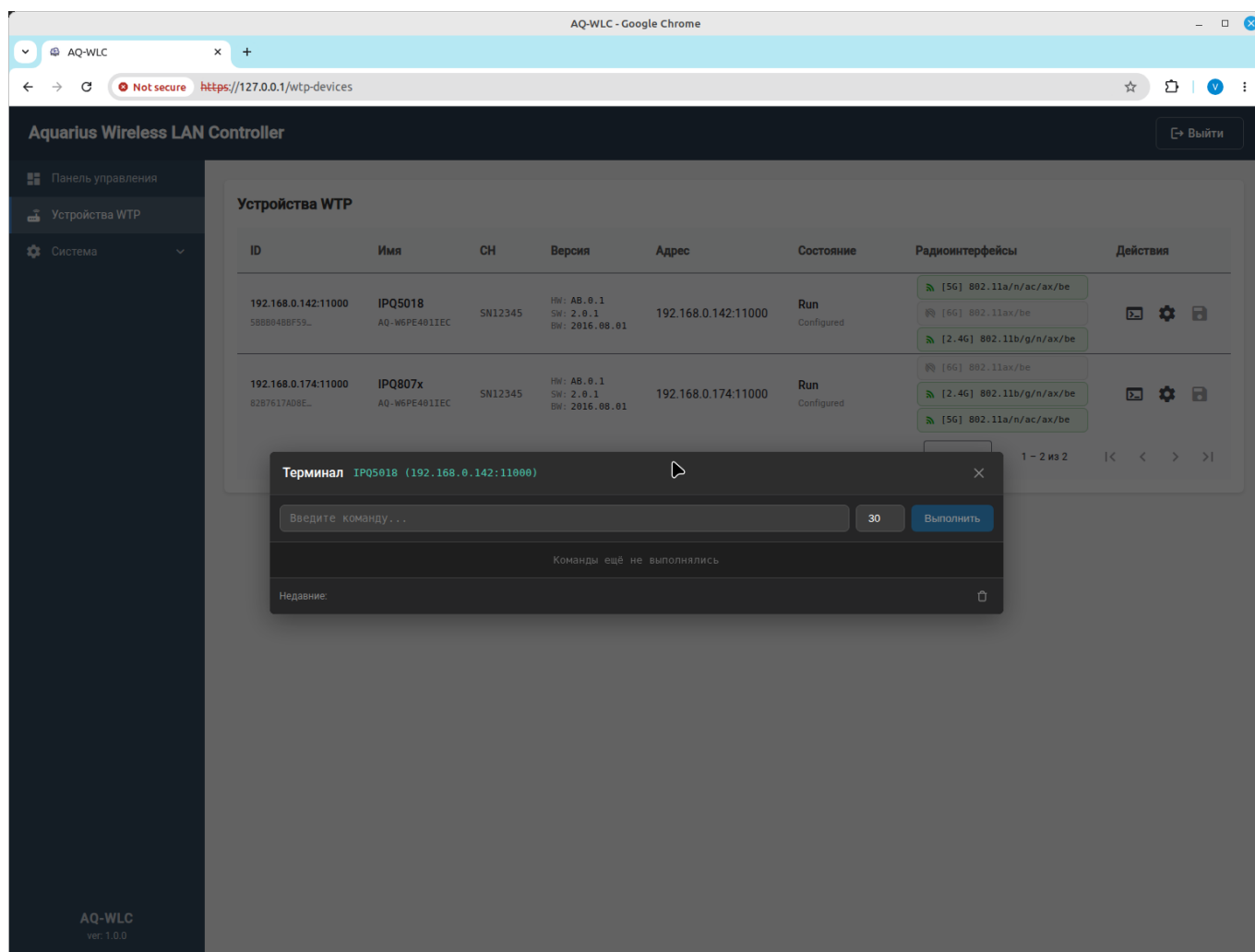


Рисунок 8

## Диалог терминала с выводом выполненных команд

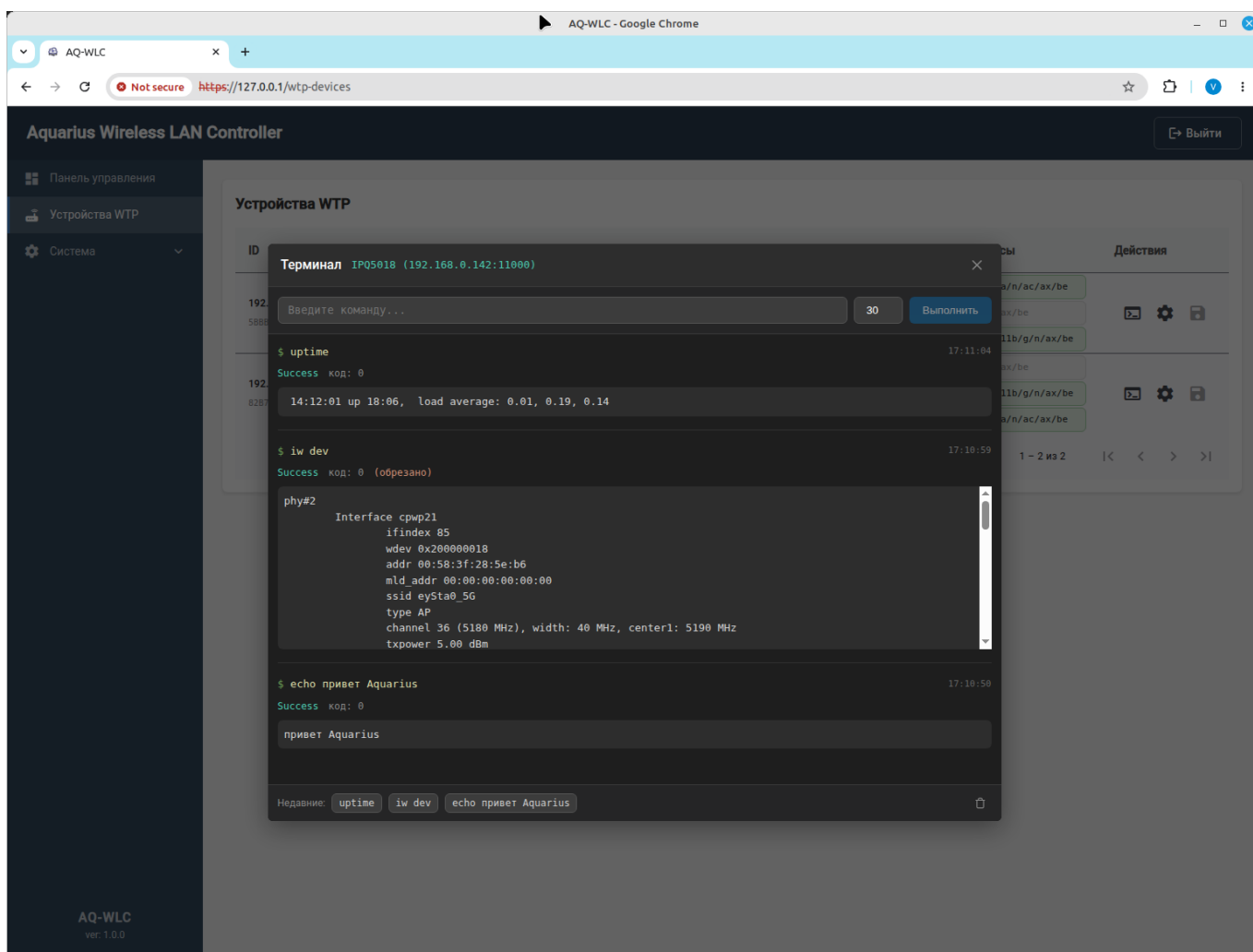


Рисунок 9

Порядок работы с терминалом:

- ввести команду в строку ввода «Введите команду...»;
- при необходимости задать таймаут выполнения в секундах (поле рядом с кнопкой «Выполнить»);
- нажать кнопку «Выполнить» для отправки команды на WTP;
- дождаться отображения результата выполнения в области вывода.

В нижней части терминала отображается история последних команд для быстрого повторного запуска. Кнопка очистки истории удаляет содержимое области вывода.

Выполнение команд может быть ограничено на стороне WTP через список разрешённых (allowlist) или запрещённых (blocklist) команд. При попытке выполнения запрещённой команды возвращается соответствующий код ошибки.

Примечание. Максимальный объём вывода команды составляет 1024 байта. При превышении этого объёма вывод обрывается, о чём сигнализирует соответствующий флаг в ответе.

### 3.2.7. Сохранение изменений конфигурации

После внесения изменений в конфигурацию WTP (через диалог конфигурации или настройку радиомодуля) в таблице WTP-устройств активируется кнопка «Применить изменения» для соответствующего устройства (рис. 10).

Индикатор несохранённых изменений (кнопка «Применить изменения» активна)

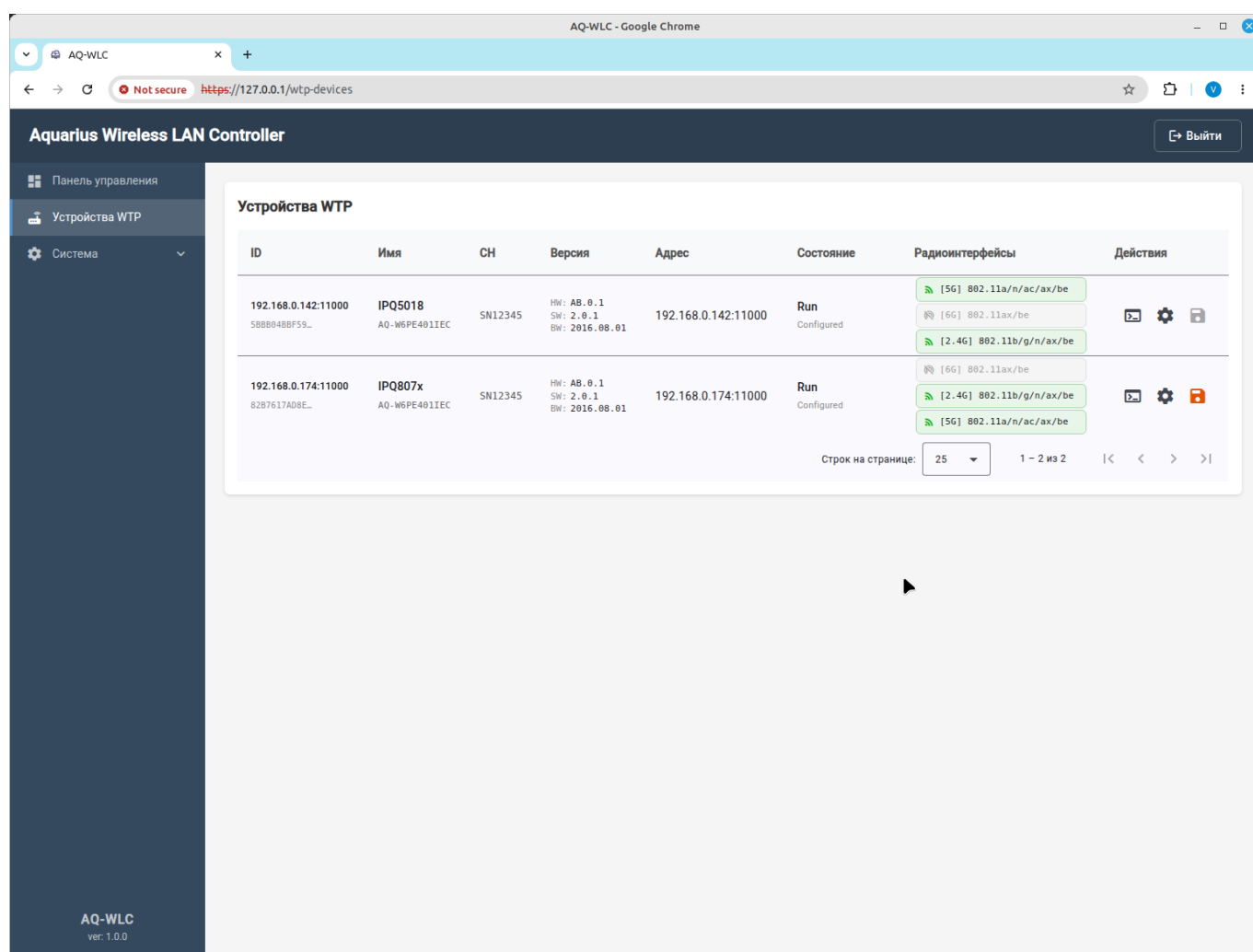


Рисунок 10

Для сохранения изменений в постоянную память WTP необходимо нажать кнопку «Применить изменения». Система запросит подтверждение операции (рис. 11).

## Диалог подтверждения сохранения конфигурации

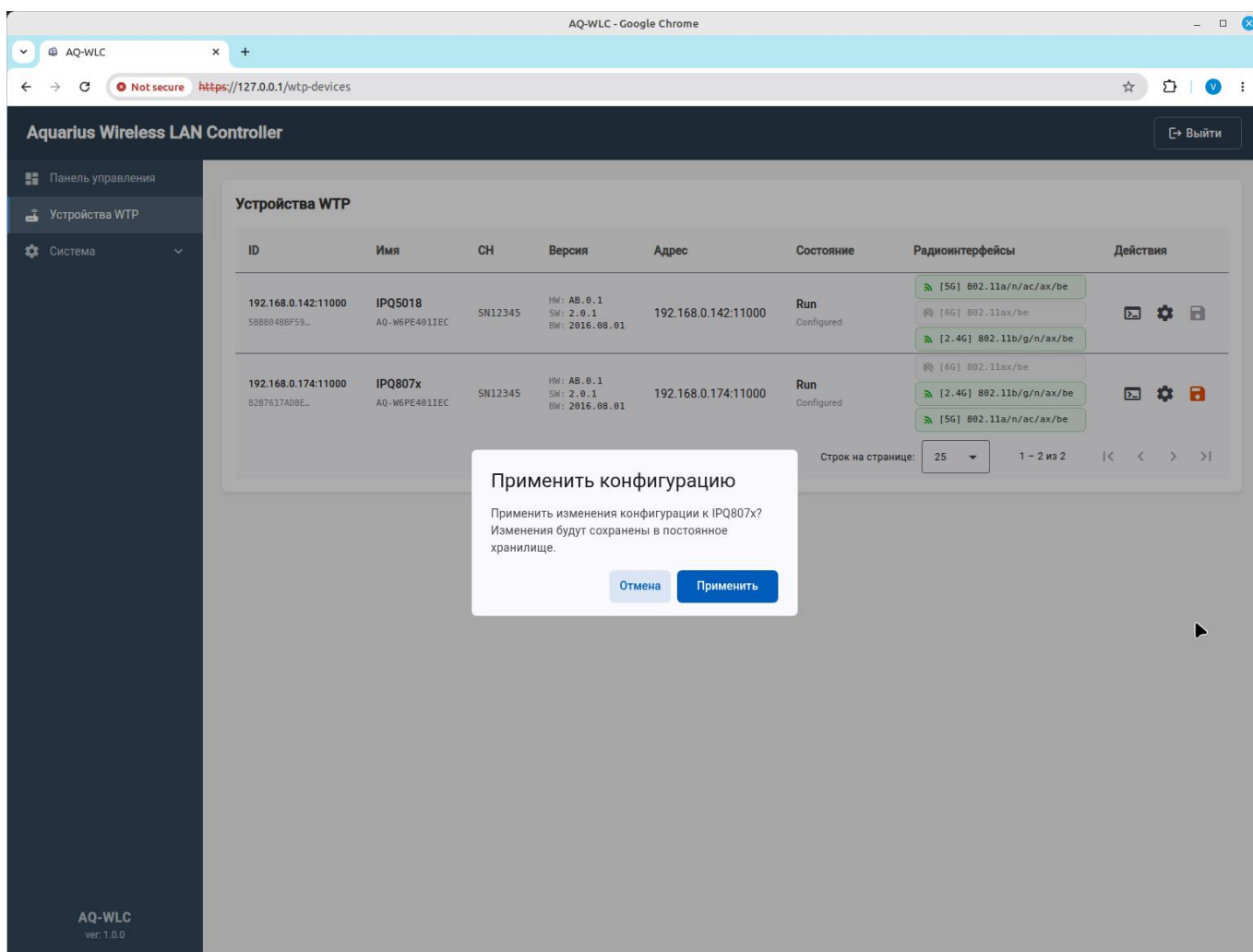


Рисунок 11

После подтверждения конфигурация атомарно записывается в файл постоянной памяти WTP. В случае ошибки сохранения в ответе возвращается соответствующий код результата.

Примечание. Изменения, не подтверждённые командой «Применить изменения», хранятся только в оперативной памяти WTP и будут потеряны при перезагрузке или сбросе устройства.

#### 4. СООБЩЕНИЯ ОПЕРАТОРУ

В процессе работы с AQ-WLC система отображает информационные сообщения и сообщения об ошибках. Основные сообщения и рекомендуемые действия оператора представлены в таблице 6.

Таблица 6 — Сообщения AQ-WLC.

| Сообщение/ситуация                                                | Описание                                                          | Действие оператора                                                                |
|-------------------------------------------------------------------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Страница входа                                                    | Веб-интерфейс АС доступен и ожидает аутентификации                | Открыть приложение-аутентификатор, получить TOTP-код и выполнить вход             |
| Успешный вход                                                     | Аутентификация прошла успешно, выдан JWT-токен сессии             | Начать работу с интерфейсом                                                       |
| Неверный TOTP-код (подсветка ошибки)                              | Введён неверный код аутентификации                                | Дождаться следующего кода (коды обновляются каждые 30 с) и повторить ввод         |
| Задержка после нескольких неудачных попыток                       | Сработала эскалирующая блокировка по числу неудачных попыток      | Дождаться окончания задержки и повторить ввод корректного кода                    |
| Сессия истекла / перенаправление на страницу входа                | Срок действия JWT-токена (24 ч) истёк                             | Выполнить повторную аутентификацию                                                |
| Устройство отображается как Offline                               | WTP не отвечает на Echo Request в течение таймаута                | Проверить сетевую связность между АС и WTP; убедиться в работоспособности WTP     |
| Устройство отображается как Online/Состояние = Run                | WTP успешно подключён, Control Plane активен                      | Можно выполнять операции управления и конфигурации                                |
| Кнопка «Применить изменения» активна (жёлтый/оранжевый индикатор) | На устройстве имеются несохранённые изменения конфигурации        | Нажать «Commit» и подтвердить сохранение для записи изменений в постоянную память |
| Результат команды «Timeout» в терминале                           | Команда на WTP не завершилась в заданное время (таймаут)          | Увеличить значение таймаута или проверить, не зависла ли команда на WTP           |
| Результат команды «Forbidden» в терминале                         | Команда заблокирована фильтром allowlist/blocklist на стороне WTP | Использовать разрешённую команду или скорректировать настройки фильтрации на WTP  |
| Результат «Success» / ненулевой код в терминале                   | Команда выполнена, но завершилась с ненулевым кодом возврата      | Проанализировать вывод команды для выявления причины ненулевого кода              |

| Сообщение/ситуация                            | Описание                                                                                   | Действие оператора                                                                                       |
|-----------------------------------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Ошибка «Сохранить» в диалоге конфигурации WTP | Не удалось отправить изменения конфигурации на WTP (сессия разорвана или ошибка протокола) | Проверить состояние устройства (Online/Offline), при необходимости дождаться переподключения и повторить |
| Ошибка «Применить изменения»                  | Не удалось сохранить конфигурацию в постоянную память WTP                                  | Проверить наличие свободного места на WTP; проверить сетевую связность                                   |

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

|        |   |                                                                                                                                              |
|--------|---|----------------------------------------------------------------------------------------------------------------------------------------------|
| ОЗУ    | – | оперативное запоминающее устройство                                                                                                          |
| ПЗУ    | – | постоянное запоминающее устройство                                                                                                           |
| ТС     | – | технические средства                                                                                                                         |
| AC     | – | access controller, контроллер точек доступа                                                                                                  |
| AQ-WLC | – | aquarius wireless LAN controller, программное обеспечение контроллера Wi-Fi RU.AMPP.00202-01                                                 |
| CAPWAP | – | control and provisioning of wireless access points, протокол централизованного управления беспроводными точками доступа (RFC 5415, RFC 5416) |
| DTLS   | – | datagram transport layer security, протокол защиты транспортного уровня для датаграмм                                                        |
| HTTP   | – | hypertext transfer protocol, сетевой протокол для обмена данными                                                                             |
| HTTPS  | – | hypertext transfer protocol secure, защищенная версия протокола HTTP                                                                         |
| JWT    | – | JSON web token, стандарт токенов для аутентификации                                                                                          |
| MTU    | – | maximum transmission unit, максимальный размер блока данных                                                                                  |
| RFC    | – | request for comments, документы стандартов ietf                                                                                              |
| SPA    | – | single page application, одностраничное веб-приложение                                                                                       |
| TAP    | – | network TAP (terminal access point), виртуальный сетевой интерфейс уровня канала данных в Linux                                              |
| TOTP   | – | time-based one-time password, одноразовый пароль на основе времени                                                                           |
| TUN    | – | network TUN, виртуальный сетевой интерфейс IP уровня                                                                                         |
| WTP    | – | wireless termination point, беспроводная точка доступа в терминологии CAPWAP                                                                 |