

Плата удаленного управления RMCARD205 / RMCARD305

Руководство пользователя

*Плата удаленного управления
позволяет осуществлять управление,
контроль и настройку системы ИБП и
датчика состояния окружающей среды.*

СОДЕРЖАНИЕ

Введение	3
Руководство по установке.....	6
Веб-интерфейс.....	10
Интерфейс командной строки	36
Сброс настроек до заводских по умолчанию / Восстановление настроек в случае утери пароля.....	61
Обновление встроенного ПО платы RMCARD	62
Сохранение и восстановление параметров конфигурации	67
Загрузка SSH хост-ключа с помощью Secure Copy (SCP).....	69
Поиск и устранение неисправностей.....	70
Сертификаты соответствия	71
Приложение 1: Идентификация IP-адреса платы удаленного управления CyberPower.....	72
Приложение 2: Конфигурирование учетной записи пользователя RMCARD на серверах аутентификации.....	74
Приложение 3: Обновление встроенного ПО ИБП.....	75
Приложение 4: Программная поддержка	76
Приложение 5: Руководство по применению адаптера RMCARD	78

Введение

Обзор

Плата удаленного управления CyberPower позволяет осуществлять дистанционный мониторинг и управление подключенным к сети ИБП. После установки аппаратного оборудования и настройки IP-адреса пользователь может получить доступ, обеспечить контроль и управление ИБП из любой точки мира! Для доступа к ИБП используется веб-браузер, поддерживается интерфейс командной строки или SSH-клиент. При использовании программного обеспечения PowerPanel® Business Remote для корректного завершения работы по сигналу платы удаленного управления, серверы и рабочие станции будут защищены от потери данных при сбоях в электропитании.

Функциональные возможности

- Оперативный мониторинг ИБП
- Дистанционное управление и конфигурирование ИБП через веб-браузер, систему сетевого администрирования (NMS) или интерфейс с командной строкой (SSH и Telnet)
- Локальное управление и настройка ИБП через последовательное соединение
- Запуск серверов / рабочих станций при отключении в случае нарушения энергоснабжения с целью предотвращения потери или повреждения данных
- Удаленное запланированное выключение / запуск / перезагрузка ИБП
- Протоколирование событий для отслеживания хронологии функционирования ИБП
- Регистрация информации в графической форме с целью анализа уровня заряда
- Сохранение и восстановление параметров конфигурации, включая текущие параметры ИБП и устройства автоматического включения резерва (ABP).
- Уведомления о событиях по электронной почте, посредством SNMP-прерываний, системного журнала и SMS-сообщений
- Удаленное обновление встроенного ПО ИБП через веб-интерфейс и FTP в разделе «Select UPS Models» (Выбор моделей ИБП)
- Поддержка протоколов IPv4/v6, SNMPv1/v3, HTTP/HTTPS, DHCP, NTP, DNS, SMTP, SSH, Telnet, FTP и протокола системного журнала
- Поддержка защищенных протоколов аутентификации электронных сообщений: SSL, TLS
- Поддержка внешних протоколов аутентификации: RADIUS, LDAP, LDAPS, Windows AD
- Возможность бесплатной загрузки баз управляющей информации (MIB) для SNMP
- Обновление пользователем встроенного ПО через FTP, утилиту обновления и настройки CyberPower и защищенный протокол копирования (SCP)
- Одновременное обновление встроенного ПО и загрузка конфигурационных файлов на нескольких устройствах
- Многоязычный пользовательский интерфейс
- Быстрая установка
- Возможность замены в горячем режиме
- Совместимость с технологией Cisco EnergyWise
- Поддержка датчика состояния окружающей среды (ENVIROSENSOR)

Требования к системе

- 10/100 Мбит/с Ethernet-подключение к существующей сети
- Веб-браузер или SSH-клиент
- *(Дополнительно)* Система управления сетью (NMS), совместимая с протоколом SNMP

Приложение с программным обеспечением PowerPanel® Business

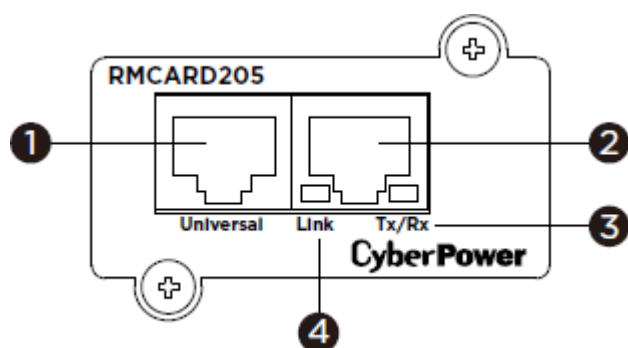


Распаковывание

После получения проверьте плату удаленного управления. Комплект поставки должен содержать:

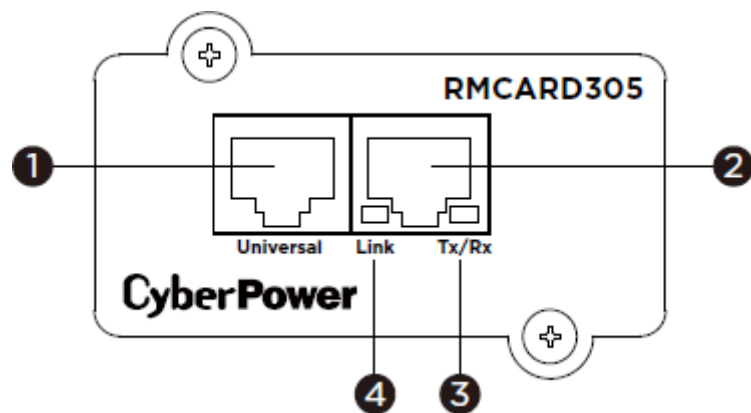
- плату удаленного управления CyberPower
- кабель подключения к последовательному порту RJ45/DB9
- краткое руководство пользователя
- запасную джамперную перемычку
- переднюю панель RMCARD205 (только для платы RMCARD305)

Передняя панель RMCARD205



1. Универсальный порт
2. Ethernet-порт
3. Индикатор передающего и приемного каналов (Tx/Rx)
4. Индикатор канала связи

RMCARD305



Светодиодные индикаторы состояния

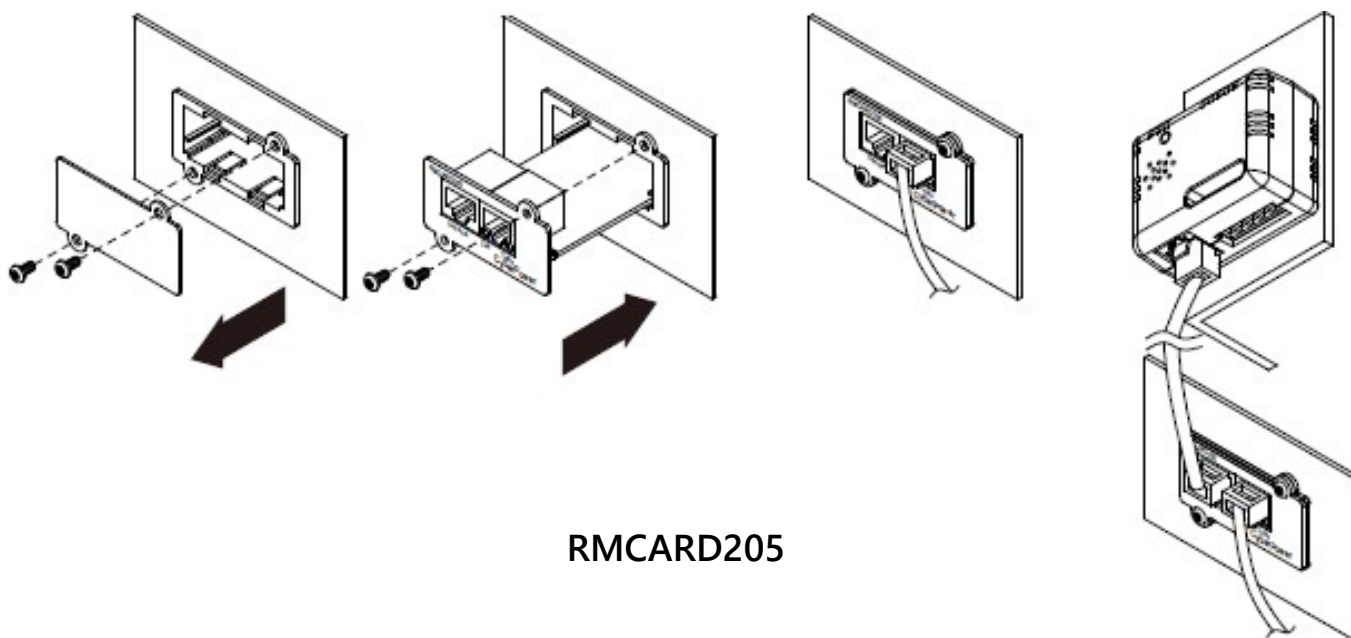
Индикатор соединения	Состояние
Выключен	Плата удаленного управления не подключена к сети / или на плату удаленного управления не подается электропитание
Включен (желтый)	Плата удаленного управления подключена к сети
Индикатор приема-передачи данных	
Выключен	На плату удаленного управления не подается электропитание
Включен (зеленый)	Плата удаленного управления подключена к сети
Мигает (зеленый)	- Прием / передача пакета данных - Перезагрузка завершена

Руководство по установке

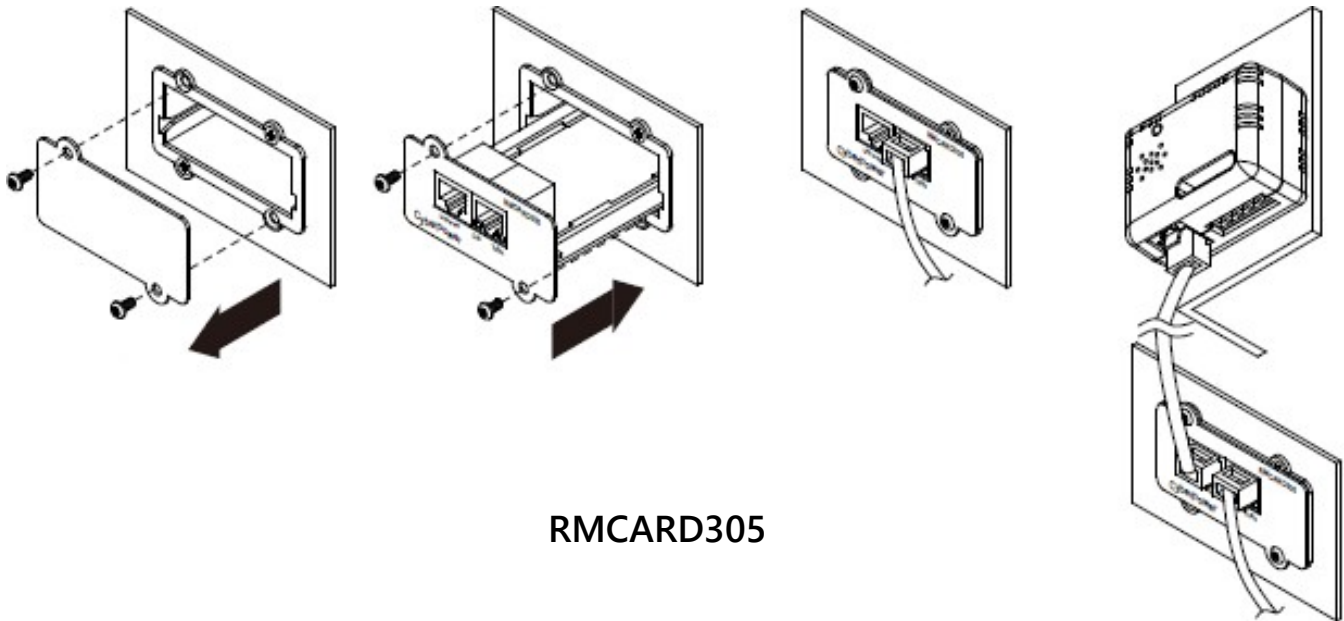
Шаг 1. Установка оборудования

Примечание: Плата удаленного управления CyberPower поддерживает замену в «горячем» режиме, поэтому для ее установки нет необходимости выключать ИБП.

1. Выкрутите два стопорных винта и снимите крышку гнезда расширения.
2. Установите в гнездо расширения плату удаленного управления CyberPower.
3. Вставьте и затяните стопорные винты.
4. Подсоедините Ethernet-кабель к Ethernet-порту платы удаленного управления CyberPower.
5. (*Опция*) Для подключения датчика состояния окружающей среды используйте Ethernet-кабель с разъемом RJ45. Один конец подключите к универсальному порту на плате RMCARD, а другой конец - к датчику. Дополнительная информация приведена в Руководстве по эксплуатации датчика ENVIROSENOR.



RMCARD205



RMCARD305

Шаг 2. Настройка IP-адреса платы удаленного управления CyberPower.

Примечание: Эти инструкции предназначены для ОС Windows. Информация о настройках в других операционных системах приведена в Приложении 4.

Способ 1: С помощью программы Power Device Network Utility

1. Инсталлируйте программу Power Device Network Utility, загрузив ее с сайта www.cyberpowersystems.com.
2. После завершения установки запустите программу «Power Device Network Utility».
3. Главное окно программы Power Device Network Utility показано на рисунке 1. Средство настройки отобразит все CyberPower устройства дистанционного управления, которые присутствуют в подсети локальной сети. Кнопка «Refresh» (Обновить информацию) используется для повторного поиска подсети в локальной сети.

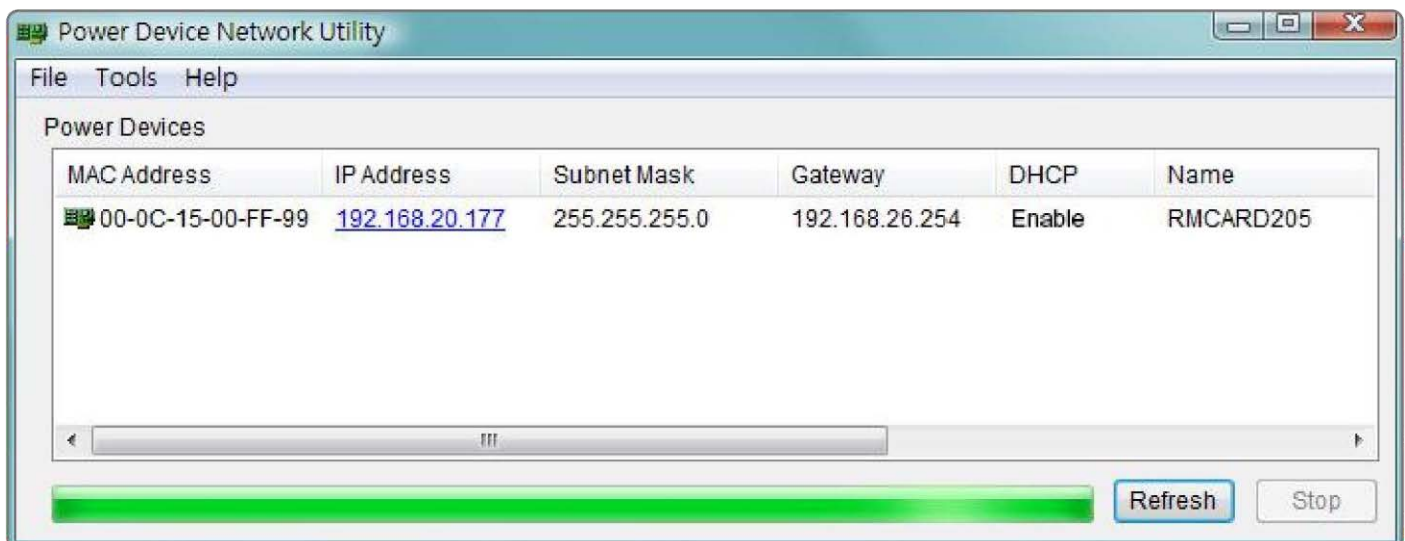


Рисунок 1. Главное окно программы «Power Device Network Utility».

4. Выберите настраиваемую плату удаленного управления. Откройте вкладку «Tools» и выберите «Device Setup» (Настройки устройства) или дважды щелкните по названию устройства, которое хотите настроить.

5. Как видно из рисунка 2, указанные в окне сетевых настроек IP-адрес, маску подсети и адрес шлюза для MAC-адреса устройства, можно изменить. Заводской IP-адрес по умолчанию - 192.168.20.177, а маска подсети по умолчанию - 255.255.255.0.

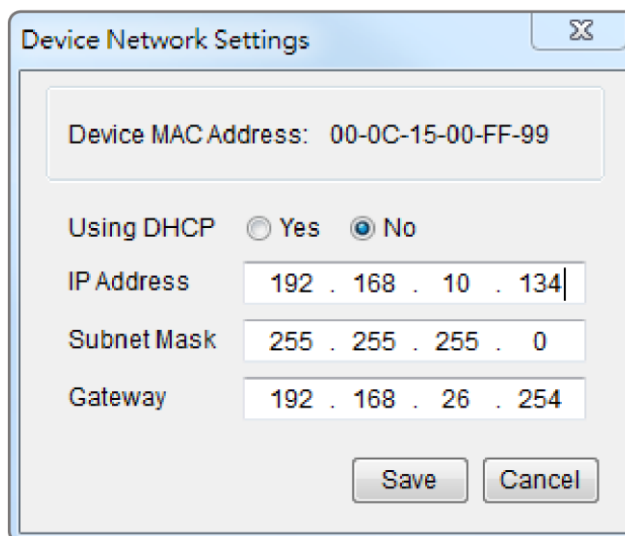


Рисунок 2. Окно настройки сетевых параметров устройства

6. Измените IP-адрес, маску подсети или адрес шлюза. Введите новые адреса в соответствующие поля и нажмите «Save» (Сохранить).
7. Для платы удаленного управления в окне аутентификации необходимо ввести имя пользователя и пароль, как показано на рисунке 3.
- Имя пользователя по умолчанию: **cyber**
 - Пароль по умолчанию: **cyber**

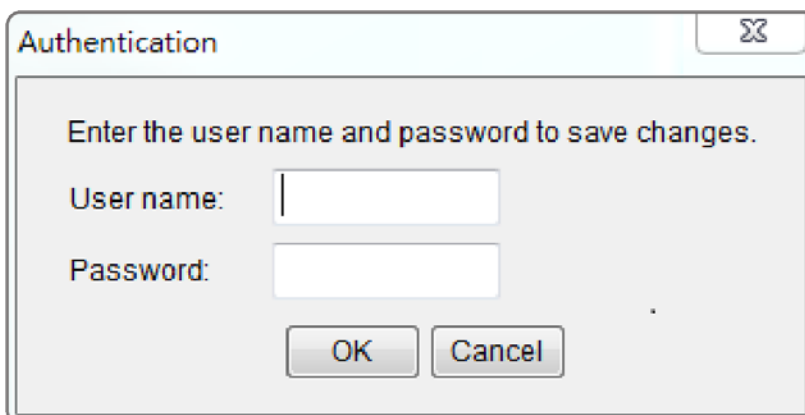


Рисунок 3. Окно аутентификации.

8. В случае успешного изменения IP-адреса появится сообщение, подтверждающее правильную настройку IP-адреса, как показано на рисунке 4.

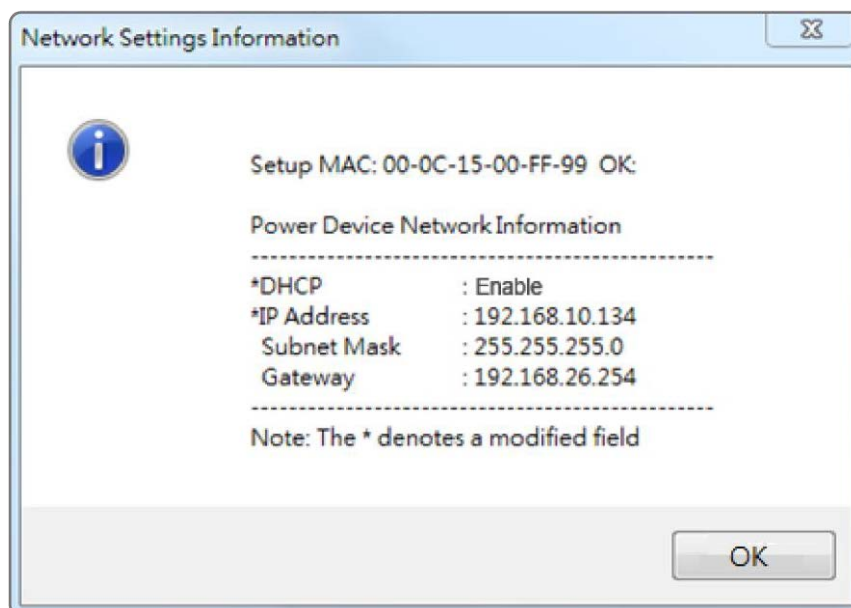


Рисунок 4. Сообщение об успешной настройке IP-адреса

9. В случае неудачного изменения, например, при некорректном значении IP-адреса, появится предупреждающее сообщение. Попробуйте снова внести необходимые изменения. Если проблема сохраняется, обратитесь за помощью к разделу «Поиск и устранение неисправностей».

Способ 2: С помощью командной строки

1. На шильдике платы удаленного управления указан MAC-адрес. Каждая плата управления обладает уникальным MAC-адресом.

Примечание: MAC-адрес указан на плате.

2. Чтобы настроить IP-адрес используйте команду **ARP**.

Пример:

Чтобы назначить IP-адрес 192.168.10.134 плате удаленного управления с MAC-адресом 00-0C-15-00-FF-99, введите его в командной строке ПК, подключенного к той же сети, что и плата удаленного управления.

- (1) В ОС Windows введите с помощью клавиатуры команду «arp -s 192.168.10.134 00-0C-15-00-FF-99»; в ОС Macintosh введите команду «arp -s 192.168.10.134 00:0c:15:00:ff:99», затем нажмите «Enter».

3. Используйте команду **Ping**, чтобы назначить IP-адресу размер 123 байта.

- (1) Введите в командную строку «ping 192.168.10.134 -l 123» и нажмите «Enter».

- (2) После получения ответных сообщений ваш ПК может взаимодействовать с данным IP-адресом.

Информацию о выборе доступного IP-адреса для платы удаленного управления см. в Приложении 1.

Веб-интерфейс

Процедура входа пользователя в систему

Для входа в интерфейс необходимо ввести имя пользователя и пароль. После входа в систему можно выбрать предпочтительный язык интерфейса. Существует два типа учетных записей.

1. Администратор

- Имя пользователя по умолчанию: **cyber**
- Пароль по умолчанию: **cyber**

2. Пользователь с правом только просмотра

- Имя пользователя по умолчанию: **device**
- Пароль по умолчанию: **cyber**

При первом входе в систему будет предложено изменить имя пользователя и пароль. Администратор может получить доступ ко всем функциям, включая активирование/блокирование учетной записи пользователя с правом просмотра. Пользователь с правом просмотра может иметь доступ только в режиме чтения, но не может изменять какие-либо настройки.

Примечание: 1. Учетная запись администратора также используется для входа на сервер, работающий по протоколу FTP, доступа к программе Power Device Network Utility и утилите обновления и настройки конфигурации.

2. В каждый отдельно взятый момент времени только один пользователь может войти в систему и получить доступ к устройству.

Информационное наполнение сайта

Примечание: Языком интерфейса по умолчанию является английский, возможен выбор другого языка.

[Summary] Приведена сводка о функционировании системы и элементов, которая обновляется автоматически; Разные модели системы ИБП могут представлять разные элементы.

Элемент	Определение
Current Condition (Текущее состояние)	Отображение текущего рабочего состояния ИБП и датчика состояния окружающей среды.
UPS Status (Состояние ИБП)	
Battery Capacity (Емкость батареи)	Графическое отображение емкости батареи ИБП (в %) на данный момент
Load (Нагрузка)	График зависимости нагрузки ИБП (в %) от доступной мощности (в Вт)
Remaining Runtime (Оставшееся время работы)	Время, в течение которого ИБП может удерживать нагрузку за счет аккумулятора
Системные данные	
Name (Имя)	Присвоенное ИБП имя
Location (Расположение)	Описание места размещения ИБП
Contact (Контакты)	Контактное лицо, ответственное за данный ИБП
Uptime (Время работы)	Продолжительность непрерывной работы системы
Состояние окружающей среды	
Temperature (Температура)	График текущих показаний температуры датчика окружающей среды
Humidity (Влажность)	График текущих показаний влажности датчика окружающей среды

Элемент	Определение
Данные об окружающей среде	
Name (Имя)	Имя датчика состояния окружающей среды.
Location (Место расположения)	Место расположения датчика состояния окружающей среды.
Recent Device Events (Последние события на устройстве)	Перечень пяти последних событий на устройстве. Все события связаны с изменениями конфигурации.

[UPS] На вкладке **UPS** можно отображать/настраивать нижеследующие элементы; однако в разных моделях ИБП могут отображаться/настраиваться разные элементы.

[UPS->Status] Отображение основной информации о текущем состоянии ИБП. Отображаемые элементы обновляются автоматически.

Элемент	Определение
Вход	
Status (Состояние)	Текущее состояние электропитания, подаваемого на ИБП.
Voltage (Напряжение)	Текущее входное напряжение электропитания, подаваемого на ИБП
Frequency (Частота)	Текущая частота тока, подаваемого на ИБП.
Выход	
Status (Состояние)	Текущее состояние выходной мощности, которую ИБП подает на подключенное оборудование.
Voltage (Напряжение)	Выходное напряжение, которое ИБП подает на подключенное оборудование.
Frequency (Частота)	Выходная частота, которую ИБП подает на подключенное оборудование.
Load (Нагрузка)	Потребляемая мощность подключенного оборудования, выраженная в % от общей нагрузки ИБП и отображаемая в Вт.
Current (Сила тока)	Выходной ток, который ИБП подает на подключенное оборудование.
Non-Critical Load (NCL) (Некритическая нагрузка)	Текущее состояние розеток для некритической (NCL) нагрузки
Energy (Энергия)	Показания счетчика электроэнергии в кВт-ч.
Аккумуляторная батарея	
Status (Состояние)	Текущее состояние батареи ИБП.
Remaining Capacity (Остаточная емкость)	Текущая емкость аккумуляторных батарей, выраженная в процентах от полного заряда.

Элемент	Определение
Remaining Runtime (Оставшееся время работы)	Расчетное время, в течение которого ИБП может удерживать нагрузку
Voltage (Напряжение)	Текущее напряжение батареи ИБП.
Система	
Status (Состояние)	Текущее рабочее состояние ИБП.
Temperature (Температура)	Рабочая температура ИБП.

[UPS->Battery Status] Отображение информации о встроенной батарее и расширенных аккумуляторных модулях (РАМ), включая температуру комплекта аккумуляторных батарей, напряжение каждой батареи в комплекте и систему выравнивания комплекта батарей.

Элемент	Определение
Last Update Date (Дата последнего обновления)	Дата последнего обновления состояния батареи. Update: Используйте эту функцию для определения последнего состояния аккумуляторной батареи.
Pack (блок)	Текущее количество батарейных блоков ИБП / расширенных аккумуляторных модулей (РАМ).
Temperature (Температура)	Текущее показание температуры батарейного блока ИБП / (РАМ).
Voltage (Напряжение)	Текущее значение напряжения каждой батареи ИБП / РАМ.
Equalization Status (Состояние выравнивания)	Отображение текущего состояния выравнивания напряжения аккумуляторной батареи ИБП / РАМ. Active: Функция выравнивания заряда аккумуляторной батареи активна. Inactive: Функция выравнивания заряда аккумуляторной батареи неактивна.

[UPS->Information] Отображение технических характеристик ИБП.

Информация	Описание
Model (Модель)	Название модели ИБП.
Serial Number (Серийный номер)	Серийный номер ИБП.
Voltage Rating (Номинальное напряжение)	Номинальное выходное напряжение (В) ИБП.
Working Frequency (Рабочая частота)	Рабочая частота выходной мощности ИБП.
Power Rating (Номинальная мощность)	Номинальная вольт-амперная характеристика ИБП
Current Rating (Номинальный ток)	Номинальный выходной ток (А) ИБП.
Load Power (Полезная выходная мощность)	Номинальная мощность (Вт) ИБП.
Battery Voltage Rating (Номинальное напряжение аккумуляторной батареи)	Номинальное рабочее напряжение постоянного тока от аккумуляторной батареи.
Firmware Version (Версия встроенного ПО)	Номер версии встроенного программного обеспечения ИБП. Update: используйте эту функцию для обновления встроенного ПО ИБП. Дополнительную информацию см. в Приложении 3.
USB Firmware Version (Версия встроенного ПО USB)	Номер версии встроенного программного обеспечения USB ИБП
LCD Firmware Version (Версия встроенного ПО ЖК-дисплея)	Номер версии встроенного ПО ЖК-дисплея ИБП

Информация	Описание
Дата замены батареи	Дата последней замены батарей. Эту дату необходимо занести вручную после замены батарей или при первой установке устройства. При отсутствии этой даты рекомендуется задать ее немедленно.
NCL Bank (NCL-батарея)	Количество батарей для некритической нагрузки
Extended Battery Modules (PAM) (Внешние аккумуляторные модули)	Количество внешних аккумуляторных модулей, подключенных к ИБП. Количество модулей настраивается вручную, их настроечные параметры зависят от модели модуля.
Installation Place (Место установки)	При нажатии на кнопку «Find it» раздается звуковой сигнал или начинается мигание индикаторов ИБП для уведомления пользователей о месте расположения ИБП. Это помогает пользователям идентифицировать конкретный ИБП в инсталляции с несколькими ИБП.

[UPS->Configuration] Настройка параметров ИБП.

Элемент	Определение
Поставляемая мощность	
Voltage (Напряжение)	Задание выходного напряжения ИБП, которое подается на подключенное оборудование.
Состояние сбоя в электроснабжении	
Utility Sensitivity (Чувствительность к энергоснабжению)	В случае регистрации выхода сетевого напряжения за пределы допустимого диапазона ИБП переключается в режим работы от батареи для защиты подключенного к нему оборудования. Низкой чувствительности соответствует более свободный диапазон изменения напряжений, а подаваемая мощность может варьироваться в более широких пределах. Питание от топливного генератора может привести к более частому переключению ИБП в режим работы от батареи. В этом случае рекомендуется настройка низкой чувствительности с редким переключением ИБП в режим работы от батареи и большей экономией заряда батареи. Высокая чувствительность позволяет ИБП обеспечивать более стабильное питание оборудования и частое переключение в режим работы от батареи.
High/Low Input (or Output) Voltage Threshold Высокий/низкий порог входного (или выходного) напряжения	Если напряжение электросети или выходное напряжение (в зависимости от модели ИБП) выше/ниже порогового значения, ИБП будет подавать на подключенное оборудование питание от батареи.
Frequency Tolerance (Допустимое отклонение частоты)	Задание допустимого диапазона частоты на входе. ИБП будет подавать питание от батареи на подключенное оборудование, если его значение выходит за пределы установленных допусков.
Эксплуатация	
Normal (Нормальная)	Нормальный режим работы ИБП.

Элемент	Определение
Generator Mode (Режим работы от генератора)	Если в качестве входной мощности ИБП используется генератор, эта опция должна обеспечить нормальное функционирование ИБП. При выборе этой опции ИБП будет отказано в переходе в режим байпаса или экономичный режим работы для защиты подключенного оборудования.
ECO Mode (Экономичный-режим)	Экономичный режим работы. Если значение напряжения/частоты на входе будет в пределах настроенного порогового значения, ИБП перейдет в режим байпаса. Как только сетевое напряжение/частота превысят пороговые значения, ИБП переключится в нормальный эксплуатационный режим. Этот режим значительно повысит КПД системы ИБП.
Manual Bypass (Ручной байпас)	Данная опция определяет возможность перехода ИБП в режим ручного байпаса. При активировании этой опции ИБП будет принудительно переведен в режим байпаса (Bypass Mode).
Bypass (Байпас)	Примечание: При такой настроенных параметрах ИБП может автоматически перейти в режим байпаса
Bypass Condition (Условие байпаса)	No Bypass: При выборе этой опции ИБП не перейдет в режим байпаса и перестанет подавать выходную мощность. Check Volt/Freq: Если сетевое напряжение находится в диапазоне пороговых значений напряжения, а частота сети находится в диапазоне допуска по частоте, ИБП перейдет в режим байпаса. В противном случае ИБП перестанет подавать выходную мощность. Check Volt Only: ИБП перейдет в режим байпаса только в том случае, если напряжение в сети находится в диапазоне пороговых значений напряжения. В противном случае ИБП перестанет подавать выходную мощность.
Bypass When UPS Off (Байпас при выключении ИБП)	После выключения ИБП переходит в режим байпаса.
Power Restore (Восстановление энергоснабжения)	После восстановления электроснабжения ИБП автоматически включается и подает питание на подключенное оборудование. Для настройки режима восстановления ИБП используются указанные ниже установочные параметры:
Automatic Restore (Автоматическое восстановление)	Если эта опция активирована, ИБП выйдет на прежний уровень сразу же после восстановления энергоснабжения. Если эта опция отключена, ИБП не вернется в исходный режим функционирования, пока позже не будет включен вручную.
Recharged Delay (Задержка вследствие дозарядки)	При возобновлении сетевого энергоснабжения ИБП перед возвратом в исходный режим функционирования начнет восстанавливать заряд, пока не истечет заданный интервал времени.
Recharged Capacity (Восстановленная емкость)	При возобновлении сетевого энергоснабжения ИБП перед возвратом в исходный режим функционирования начнет восстанавливать заряд, пока не будет достигнута заданная емкость батареи.

Элемент	Определение
Returned Delay (Задержка возврата)	Каждый раз при включении ИБП будет происходить задержка возврата в прежнее состояние.
Line Stable Delay (Задержка при переходе в линейный режим)	Если ИБП работает от батареи (Battery Mode), то после восстановления сетевого электроснабжения ИБП изменит режим работы на линейный (Line Mode) с запаздыванием на определенное время. При уровне заряда батареи ИБП менее нижнего порогового значения после восстановления сетевого электроснабжения ИБП немедленно возвращается в линейный режим.
Аккумуляторная батарея	
Low Battery Threshold (Нижнее пороговое значение батареи)	Если ИБП подает питание от батареи, а оставшаяся емкость меньше нижнего порогового значения, ИБП подаст звуковой сигнал.
External Battery Modules (Внешние аккумуляторные модули)	Назначение количества внешних аккумуляторных модулей. Это позволяет точно оценить время работы с использованием общего количества батарей, подключенных к ИБП.
Periodical Battery Test (Периодическое испытание батареи)	ИБП будет в автоматическом режиме периодически выполнять испытание батарей с целью обеспечения их полной работоспособности. Примечание: Только в ИБП серии Online (OL) поддерживается функция интеллектуального управления батареями (SBM). SBM-функция выполняет испытание батареи даже при отключенном параметре «Periodical Battery Test».
Система	
Cold Start (Холодный запуск)	Настройка возможности запуска ИБП при отсутствии подачи питания. Если эта опция активирована, ИБП можно включить с питанием от аккумуляторной батареи.
Audible Alarm (Звуковой аварийный сигнал)	Если эта опция поддерживается, ИБП будет издавать звуковой сигнал при подаче питания от батареи, при перегрузке на выходе или других условиях (в зависимости от модели ИБП).
Dry Relay Function (Функция сухого контакта реле)	Эта функция настраивает срабатывание сухих контактов реле ИБП при наступлении выбранного состояния. Дополнительную информацию о расширенных функциях сухих контактов реле ИБП см. в руководстве по эксплуатации ИБП. Возможно настроить активацию этой функции при следующих условиях подачи электропитания: (1) Сбой электроснабжения: При сбое в сети электроснабжения ИБП переходит на питание от батареи. (2) Низкий уровень заряда батареи: Емкость аккумулятора слишком низкая, чтобы поддерживать выключение подключенных компьютеров. (3) Аварийный сигнал: При возникновении предаварийной ситуации, как например, перегрузка, ИБП издает звуковой сигнал. (4) Байпас: ИБП переходит в режим байпаса. (5) Отказ ИБП: Возможен отказ ИБП из-за неисправности оборудования.
Screen Save Time (Время перехода в режим ожидания)	При отсутствии в течение этого периода нажатия кнопок ИБП и нарушения энергоснабжения, ЖК-экран переходит в режим ожидания.

Элемент	Определение
Wiring Fault Detecting (Обнаружение неисправности проводки)	Если эта опция активирована, ИБП обнаружит отсутствие заземления/неправильное подключение подводящих кабелей. Рекомендуется сначала обеспечить заземление проводки ИБП.
Over Discharge Protection (Защита от перезаряда)	Если ИБП находится в режиме работы от батареи с заданным временем 0%, плата RMCARD переключит ИБП в режим ожидания, а выход будет отключен.
Enter Sleep Mode After All Remote Shutdown (Переход в режим ожидания после каждого удаленного выключения)	Если эта опция активирована, ИБП перейдет в режим ожидания после завершения программы PowerPanel® Remote + 2 мин. Примечание: Для клиентов PowerPanel® Business Edition: если этот параметр активирован, после сбоя в подаче сетевого питания ИБП перейдет в режим ожидания в течение периода времени, равного оставшегося максимального времени задержки удаленного выключения (MSDT) + 2 мин. Дополнительную информацию о MSDT см. на вкладке UPS -> PowerPanel List.
Розетки батареи для некритической нагрузки	
Turn Off Threshold (Порог выключения)	В режиме подачи питания от батареи ИБП отключит эту NCL-розетку батареи, если оставшаяся емкость батареи ниже заданного порога.
Turn off Delay (Задержка выключения)	В режиме подачи питания от батареи ИБП отключит эту NCL-розетку батареи по истечении заданного времени задержки.
Turn On Delay (Задержка включения)	После восстановления сетевого питания ИБП восстановит выход NCL-розеток батареи по истечении времени задержки. Это предотвращает чрезмерное потребление энергии, обусловленное одновременным запуском всего подключенного оборудования.

[UPS->Master Switch] Включение или выключение выходной мощности ИБП

Элемент	Определение
Reboot UPS (Перезагрузка ИБП)	Выключение и повторное включение ИБП
Turn UPS Off (Выключение ИБП)	Выключение ИБП
UPS Sleep (Переключение ИБП в режим ожидания)	Эта команда доступна в режиме отключения сетевого питания. Она переводит ИБП в режим ожидания до возобновления питания. Примечание: В некоторых моделях ИБП эта команда может не поддерживаться.
Reset (Сброс данных)	Сброс ожидающего выполнения действия для выключения ИБП.
Turn UPS On (Включение ИБП)	Включение ИБП.
Shutdown/Sleep Delay (Задержка выключения / перехода в режим ожидания)	Время ожидания ИБП перед выключением в ответ на команду «Reboot UPS» (Перезагрузить ИБП), «Turn UPS off» (Выключить ИБП) или «UPS Sleep» (Перевести ИБП в режим ожидания).
Reboot Duration (Продолжительность перезагрузки)	После выключения ИБП команда «Reboot Duration» определяет, длительность ожидания ИБП повторного включения в ответ на команду «Reboot UPS» (Перезагрузить ИБП).
Signal PowerPanel® Remote to Shutdown (Сигнал ПО PowerPanel® Remote для выключения)	Выберите этот параметр, чтобы оповестить ПО PowerPanel® Business Remote перед выключением ИБП. Длительность задержки отключения (MST, максимальное время отключения клиентов) для ИБП можно изменить с целью обеспечения корректного завершения работы.

[UPS->Bank Control] Отображение текущего состояния каждой розетки батареи, а также обеспечение управления включением/выключением розеток батареи для некритической нагрузки. Номер розетки и имя устройства идентифицируют имя устройства, связанного с конкретной розеткой.

Элемент	Определение
Параметры управления батареями	
ON (ВКЛ)	Немедленное включение батареи некритической нагрузки.
OFF (ВЫКЛ)	Немедленное выключение батареи некритической нагрузки.
Идентификация имени устройства	
Outlet # (№ розетки)	Номер розетки ИБП в соответствии с конфигурацией розеток (зависит от модели ИБП).
Device Name (Имя устройства)	Имя устройства, соответствующее этой розетке.

[UPS->Diagnostics] На вкладке «**UPS/Diagnostics**» можно проверить, находятся ли батареи ИБП в надлежащем рабочем состоянии. Также можно выполнить калибровку ИБП с целью обеспечения точной оценки подключенной нагрузки.

Элемент	Определение
Battery Test (Испытание батареи)	Функция «Battery Test» на 10 сек переключает ИБП на питание от батареи. Это позволяет пользователю проверить состояние батареи и получить информацию о батарее, включая результаты и дату последнего испытания. Для запуска испытания батареи нажмите кнопку «Start». После завершения испытания батареи будет представлен отчет. Примечание: «N/A» означает, что данная модель ИБП не поддерживает эту функцию.
Last Test Result (Результат последнего испытания)	Результаты последнего испытания батареи. Passed: Батарея во время испытания работала нормально. Failed: Отказ при испытании батареи. В случае непрохождения испытания выполните следующие действия: Повторите испытание батарей и замените батареи в случае повторного отказа. Если проверка батарей дала сбой после их замены, обратитесь за помощью в компанию CyberPower.
Last Test Date (Дата последнего испытания)	Дата последнего испытания батареи.
Runtime Estimation (Оценка времени исполнения)	Функция «Runtime Estimation» разряжает батареи ИБП от емкости батареи на момент запроса оценки до почти нулевой емкости при текущей нагрузке. Результаты выполнения этой функции показывают время выполнения, статус оценки и дату выполнения последней оценки. При запуске оценки времени исполнения подключенное оборудование будет работать от батареи, пока она не разрядится почти до нуля. Как только батареи разрядятся до этого уровня, подключенное оборудование начнет работать от электросети.

Элемент	Определение
Runtime Estimation (Оценка времени исполнения)	После проведения оценки батареи будут автоматически заряжены. Примечание: Расчетное время исполнения может варьироваться в зависимости от нагрузки и уровня заряда батарей при запуске оценки времени работы. После завершения оценки батареи будут заряжены в автоматическом режиме. Пользователи могут нажать кнопку « Start » для запуска оценки времени исполнения. Для прерывания оценки времени исполнения нажмите кнопку « Abort ». После завершения или отмены оценки времени исполнения будет представлен результат
Estimated Runtime (Расчетное время работы)	Расчетное время работы батарей при текущей нагрузке.
Last Estimation Result (Результат последней оценки)	Результаты последней оценки времени исполнения. Passed: Оценка времени исполнения завершена, батареи в порядке. Canceled: Оценка времени исполнения была прервана.
Last Estimation Date (Дата последней оценки)	Дата последнего выполнения оценки времени.

[UPS->Schedule]: Настройка ИБП на автоматическое выключение и перезапуск в запланированное время (однократно/ежедневно/еженедельно). Вкладка **Schedule** управляет запланированными выключениями и содержит перечень всех сконфигурированных расписаний. В строке каждого расписания отображается подробная информация об условии вступления расписания в силу.

[Once]: Пользователь может задать одно временное событие для выключения/перезапуска ИБП.

[Daily]: Установка ежедневного повторения выключения/перезапуска ИБП.

[Weekly]: Установка еженедельного повторения выключения/перезапуска ИБП.

1. Выберите опцию [Once], [Daily] или [Weekly] и нажмите «Next>>», введите дату и время выключения ИБП. Выберите [Never], [Instant] или дату и время последующего включения ИБП. Выберите батарею, которой следует управлять, и нажмите «Shutdown Clients» для настройки всей клиентской части на корректное завершение работы. Можно присвоить имя («Name») этому расписанию.
2. Для добавление в расписание нового элемента нажмите «Apply». Для возврата к настройкам по умолчанию нажмите «Reset».
3. Сохраненные настройки перечислены в меню [Schedule].
4. В случае необходимости удалить запланированное действие просто щелкните по имени элемента, указанного в меню [Schedule], и нажмите «Delete».

Примечание: Система управления допускает до 10 записей в расписании.

[UPS->Wake on Lan] Функция WoL используется для пробуждения компьютера по сигналу из локальной сети. Введите IP-адрес такого компьютера, когда он включен, и система будет искать его MAC-адрес, соответственно. Максимально можно задать 50 IP-адресов.

Элемент	Определение
ПО PowerPanel® Remote	
Load/Sync with Power Panel® Remote List Загрузка/синхронизация с помощью Power Panel® Remote List	Активируйте эту опцию, чтобы загружать список WoL-клиентов и синхронизировать его со списком PowerPanel® Remote List.
Условия пробуждения	
UPS Turn On Включение ИБП	В случае выбора этой опции, при включении ИБП плата RMCARD будет отправлять WoL-сигнал на взаимодействующие с ПО PowerPanel® Remote компьютеры.
Utility Power Restore and Output is Supplied (Восстановление питания от сети и мощности на выходе)	В случае выбора этой опции, при восстановлении электроснабжения и включении выхода ИБП плата RMCARD будет отправлять WoL-сигнал на подключенные к ПО PowerPanel® Remote компьютеры.
WoL-списки	
WoL Remote List (Список дистанционных WoL-клиентов)	Если активирована опция «Load/Sync with PowerPanel® Remote List», будет выведен список IP-/ MAC-адресов ПК с инсталлированным ПО PPB (PowerPanel® Business).
WoL Manual List (Ручной список WoL)	Пробуждение по локальной сети по списку в ручном режиме.

Примечание: Установочные параметры BIOS компьютера с инсталлированным ПО PowerPanel® Remote должны поддерживать WoL-функцию и быть соответствующим образом настроены.

[UPS->EnergyWise] Инициатива EnergyWise направлена на снижение энергопотребления всех устройств, подключенных к сети Cisco. Благодаря этой совместимости плата удаленного управления CyberPower признана совместимой с другими объектами, поддерживающими технологию EnergyWise, и она поддается простому управлению и контролю с целью достижения оптимальной энергоэффективности в рамках комплекса EnergyWise.

Элемент	Определение
Конфигурация	
Version (Версия)	Поддерживаемая версия EnergyWise.
EnergyWise	Активация поддержки комплекса CISCO EnergyWise.
Service port (Сервисный порт)	Номер порта, который используется для связи с устройствами, поддерживающими комплекс EnergyWise (должен быть таким же, как и настроенный в сетевом коммутаторе).
Domain Name (Имя домена)	Доменное имя комплекса EnergyWise (должно быть таким же, как и настроенное в сетевом коммутаторе).
Off-State Cache (Буферная память отключена)	Разрешение/запрет записей удаленных ПК, которые будут храниться в буферной памяти списка EnergyWise коммутатора после перезагрузки.
Secure Mode (Безопасный режим)	Разрешение использовать общий ключ в рамках комплекса EnergyWise.
Shared Secret (Общий ключ)	Ключ к домену EnergyWise.

Элемент	Определение
Node List (Список узлов)	Список родительских/дочерних элементов EnergyWise показывает все объекты EnergyWise и позволяет пользователям настраивать атрибуты объекта EnergyWise.
Name (Имя)	Имя, используемое для идентификации каждой розетки.
Role (Роль)	Этот параметр представляет собой строку символов, которая описывает функцию объекта (максимальная длина 31 символ).
Keywords (Ключевые слова)	Этот параметр представляет собой строку символов, которая описывает объект (максимальная длина 31 символ).
Importance (важность)	Этот параметр, которому присваивается значение от 1 до 100, характеризующее важность объекта от высокой до низкой.

[UPS->PowerPanel® List] Отображение информации о поддерживаемом ПО PowerPanel® Business. Соединение устанавливает ПО PowerPanel® Business. Перечисленная информация будет удалена при отключении на 1 час.

Элемент	Определение
Конфигурация	
Max Remote Shutdown Time (MST) Макс. время удаленного выключения	Максимальное время, необходимое для выключения всех подключенных удаленных объектов.
Max Remote Shutdown Delay Time (MSDT) Максимальное время задержки удаленного выключения (MSDT)	Максимальный период времени от момента сбоя подачи электропитания до корректного отключения всех пользователей.
Список	
Type (Тип)	Тип ПО PowerPanel® Business - удаленное - управление
Shutdown Condition (Условие выключения)	Условие выключения под управлением ПО PowerPanel® Business - Отсутствует - Сбой подачи электропитания - Низкий заряд батареи - Недостаточное время выполнения
Status (Состояние)	Состояние ПО PowerPanel® Business - Подключение - Нормальное выполнение - Обрабатывается процесс выключения - Выключение завершено

Примечание: Не рекомендуется одновременное подключение к плате RMCARD ПО PowerPanel® Business Edition или ПО PowerPanel® Business.

[Envir] На вкладке Envir. можно отображать/настраивать перечисленные ниже элементы. Обратите внимание, что вкладка Envir появляется только в случае подключения к плате RMCARD датчика ENVIROSENSOR.

[Envir->Status] Отображение основной информации о датчике состояния окружающей среды и замыкании входных контактов.

Элемент	Определение
Информация	
Name (Имя)	Название датчика состояния окружающей среды.
Location (Место расположения)	Расположение датчика состояния окружающей среды.
Температура	
Current Value (Текущее значение)	Температура окружающей среды в данный момент.
Maximum (Максимум)	Самая высокая температура и время ее регистрации датчиком состояния окружающей среды.
Minimum (Минимум)	Самая низкая температура и время ее регистрации датчиком состояния окружающей среды.
Влажность	
Current Value (Текущее значение)	Влажность воздуха окружающей среды в данный момент.
Maximum (Максимум)	Самая высокая влажность и время ее регистрации датчиком состояния окружающей среды.
Minimum (Минимум)	Самая низкая влажность и время ее регистрации датчиком состояния окружающей среды.
Contact (Контакт)	Отображение имени и состояния (нормальный/аномальный) каждого входного сухого контакта реле.

[Envir->Configuration] Настройка параметров датчика состояния окружающей среды.

Элемент	Определение
Информация	
Name (Имя)	Имя, используемое для идентификации датчика окружающей среды.
Location (Расположение)	Расположение датчика состояния окружающей среды.
Температура	
High Threshold (Верхний порог)	Верхний предел нормальной температуры.
Low Threshold (Нижний порог)	Нижний предел нормальной температуры.
Hysteresis (Гистерезис)	Точка, в которой разность между верхним и нижним пороговыми значениями температуры изменяется с аномальной на нормальную.
Rate of Change (Скорость изменения)	Скорость определения аномального изменения температуры
Unit (Единица измерения)	Единица измерения температуры.
Влажность	
High Threshold (Верхний порог)	Верхний предел нормальной влажности.
Low Threshold (Нижний порог)	Нижний предел нормальной влажности.
Hysteresis (Гистерезис)	Точка, в которой разность между верхним и нижним пределами влажности изменяется с аномальной на нормальную.
Rate of Change (Скорость изменения)	Скорость определения аномального изменения влажности.
Contact (Контакт)	Ввод имени всех входных реле с сухими контактами и определение нормального состояния каждого из них в выпадающем меню.

[Logs->Event Logs] Отображение списка событий и краткое описание каждого события с отметкой даты и времени их регистрации.

Примечание: 1. Регистрируемые события перечислены в разделе «System->Notifications->Event Action».

2. Время регистрируется в 24-часовом формате.

[Logs->Status Records] На этой вкладке возможен просмотр журналов состояния ИБП и состояния среды; однако для разных моделей могут отображаться разные элементы.

Характеристики всех элементов аналогичны тем, которые применяются при определении состояния ИБП или состояния окружающей среды.

- Input min (V): минимальное входное напряжение электросети, указанное в предыдущей записи.
- Input max (V): максимальное входное напряжение электросети, указанное в предыдущей записи.
- Input (Hz): текущая частота питающей сети, подведенной к ИБП.
- Output (V): выходное напряжение ИБП, подаваемое на подключенное оборудование.
- Output (Hz): выходная частота ИБП, питающая подключенное оборудование.
- Load (%): процент от общей мощности ИБП, подаваемой на подключенное оборудование.
- Capacity (%): процент от текущей емкости батареи ИБП.
- Remaining Runtime: расчетное время, в течение которого ИБП может поддерживать подключенную нагрузку в режиме работы от батарей.
- Temperature (°C or °F): текущая температура датчика состояния окружающей среды (°C или °F).
- Humidity (%RH): текущая влажность датчика окружающей среды (% относительной влажности).

[Logs->Energy Records] На вкладке Energy Records отображается список показателей энергопотребления с отметкой даты и времени их регистрации.

Элемент	Определение
Energy (Энергия)	Энергия, использованная устройством в течение определенного интервала времени, измеренная в кВтч.
Cost (Стоимость)	Стоимость энергии, использованной устройством в течение определенного интервала времени.
CO ₂	Выбросы CO ₂ устройством за определенный интервал времени.
Accumulated Energy (Аккумулятивная энергия)	Кумулятивная энергия, использованная устройством с момента последней перезагрузки, измеренная в кВтч.
Accumulated Cost (Накопленные затраты)	Суммарная стоимость энергии, использованной устройством с момента последней перезагрузки.
Accumulated CO ₂ (Суммарный CO ₂)	Суммарная эмиссия CO ₂ устройством с момента последней перезагрузки.

[Logs->Graphing] На этой вкладке отображаются данные записей о состоянии. Функция построения графиков упрощает просмотр записей о состоянии.

Элемент	Определение
Graph Period (Период построения графика)	Использованный для построения графика период. Для отображения более длительных периодов потребуется больше времени.
Graph Data (Данные графика)	Использованные для построения графика данные. Чем больше выбрано данных, тем больше времени требуется для построения графика.
Graph Node (Узлы графа)	При выборе параметра «Display All Nodes in Detail» будут отображаться все точки вдоль линии; при перемещении курсора в точку на графике отобразится информация об этой точке.
Launch Graph in New Window (Вывод графика в новом окне)	При установке флажка в этой ячейке подробный график откроется в новой вкладке.

[Logs->Maintenance] Эту вкладку используют для выбора настроек журналов событий (Event Logs) и записей о состоянии (Status Records). Приложение предоставляет информацию о количестве зарегистрированных событий до его заполнения

Элемент	Определение
Журналы событий	
Clear All Logs (Очистить все журналы)	Обнуление существующих журналов событий.
The Number of Events (Количество событий)	Количество существующих журналов событий и макс. количество событий, которые могут быть зарегистрированы. По достижении максимального числа событий новые заменяют в памяти самые старые.
Save Event Logs (Сохранить журналы событий)	Сохранение существующих журналов событий в виде текстового файла.
Записи о состоянии	
Recording Interval (Интервал регистрации)	Настройка частоты регистрации данных о состоянии. Короткий интервал обеспечит более частую регистрацию, но быстрое заполнение доступной памяти. Чем длиннее интервал, тем меньшее количество записей, но сохранение данных в течение более длительного периода времени.
Clear All Records (Обнуление всех записей)	Очистка от существующих записей о состоянии.
Remaining Time (Оставшееся время)	Время хранения записей. Меньший интервал между регистрациями = более короткому оставшемуся времени хранения, тогда как при более длительном интервале между регистрациями оставшееся время хранения увеличивается. По достижении максимального числа записей о состоянии новые записи заменяют в памяти самые старые.
Save Status Records (Сохранение записей о состоянии)	Сохранение записей о состоянии в виде текстового файла.
Показатели энергопотребления	
Recording Interval (Интервал записи)	Частота записи данных об энергопотреблении.
Clear Entire Records (Очистить все записи)	Очистка от существующих показателей энергопотребления
Electricity Rate (Тариф на электроэнергию)	Отношение стоимости энергии к количеству потребленной энергии.
CO2 Emissions (Выбросы CO ₂)	Отношение количества выбросов CO ₂ к количеству потребленной энергии
Save Energy Records (Сохранение показателей энергопотребления)	Сохранение существующих журналов событий в виде текстового файла.

Примечание: Журналы событий и записи состояния используют память по принципу «первым поступил-первым удален». После заполнения памяти самые ранние данные будут перезаписаны.

[Logs->Syslog] Настройка пользователями syslog-сервера и отправление тестового сообщения.

Элемент	Определение
Syslog (Системный журнал)	Включение или отключение функции ведения системного журнала.
Facility Code (Код объекта)	Выбор Syslog-объекта.
Server IP (IP-адрес сервера)	IP-адрес сервера системного журнала.
Server Port (Порт сервера)	UDP-порт, используемый Syslog-сервером.
Send Test (Отправить тест)	Отправить тестовое сообщение на Syslog-сервер.

[System->General->Time] Отображение системной даты и времени и разрешение пользователям устанавливать их вручную или с помощью NTP-сервера (по сетевому протоколу синхронизации времени).

Элемент	Определение
Current Settings (Текущие настройки)	Отображение в статусе платы текущей даты и времени до следующего обновления протокола сетевого времени (NTP).
Настройка системного времени	
Time Zone (Часовой пояс)	Выбор часового пояса платы RMCARD по Гринвичу.
Using NTP server (Использование NTP-сервера)	Ввод IP-адреса/доменного имени NTP-серверов, настройка частоты обновления даты и времени с NTP-сервера. Для немедленного обновления нажмите «Update right now»
Manual Setup (Ручная настройка)	Ввод даты и времени в указанном формате

[System->General->Identification] Указание имени системы, контактной информации и местоположения.

Элемент	Определение
Name	Название оборудования
Location	Место расположения силового оборудования
Contact (Контакты)	Ответственное за это оборудование контактное лицо

[System->General->Daylight Saving Time] Перевод часов на летнее время.

Элемент	Определение
Настройка летнего времени (DST)	
Disable (Отключение)	Отключение летнего времени.
Tradition US DST (Традиционный для США режим DST)	Задание традиционных настроек летнего времени в США Начало: 2:00, второе воскресенье марта. Окончание: 2:00, первое воскресенье ноября.
Manual DST (Ручной переход на летнее время)	Ручная настройка даты и времени перехода на летнее время.

[System->Security->Management] Настройка авторизации входа и авторизации программного обеспечения.

Элемент	Определение
Авторизация входа	
Local Account (Локальная учетная запись)	Настройка локальной учетной записи администратора или просмотрщика для входа в систему
RADIUS , Local Account (RADIUS, локальная учетная запись)	Использование для входа в систему параметров конфигурации RADIUS (службы удаленной аутентификации пользователей по телефонным линиям). В случае ошибки RADIUS-аутентификации, для входа будут использоваться настройки локальной учетной записи.
RADIUS Only (Только RADIUS)	Использование для входа в систему параметров конфигурации.
LDAP , Local Account (LDAP, локальная учетная запись)	Использование для входа в систему параметров конфигурации LDAP (упрощенный протокол доступа к сетевым каталогам). В случае ошибки LDAP-аутентификации для входа будут использоваться настройки локальной учетной записи.
LDAP Only (Только LDAP)	Использование для входа в систему параметров конфигурации LDAP.
Авторизация программного обеспечения	
Secret Phrase (Секретная фраза)	Фраза аутентификации, которая используется для взаимодействия с ПО PowerPanel® Business Remote. Примечание: Дополнительные сведения см. в Приложении 4.
Admin/Viewer Manager IP (Диспетчер IP-адресов Администратора/Просмотрщика)	Этот параметр определяет, с какого IP-адреса разрешен доступ к устройству с учетной записью администратора или просмотрщика. Для получения доступа к плате удаленного управления с любого IP-адреса, можно присвоить одному из них значение 0.0.0.0 или 255.255.255.255. Примечание: Путем ввода маски подсети можно разрешить доступ к диапазону IP-адресов. Например, 192.168.20.0/16 означает, что может получить доступ IP-адрес с подсетью 192.168.0.0.

[System->Security->Local Account] Эту вкладку используют для настройки учетной записи для входа.

Информация	Описание
Administrator (Администратор)	Администратор имеет полный доступ к настройкам конфигурации для чтения и записи.
Viewer (Просмотрщик)	Просмотрщик имеет ограниченный доступ - только для чтения.

Изменение учетной записи Администратора:

1. Введите имя пользователя
2. Введите текущий пароль
3. Настройте параметры диспетчера IP-адресов (*необязательно*)
4. Введите новый пароль
5. Введите подтверждение пароля
6. Нажмите «Apply» (Применить)

Примечание: Максимальная длина имени пользователя и пароля составляет 63 символа.

Изменение учетной записи Просмотрщика:

1. Чтобы активировать учетную запись Просмотрщика, выберите «Allow Access»
2. Введите имя пользователя
3. Настройте параметры диспетчера IP-адресов (*необязательно*)
4. Введите новый пароль
5. Введите подтверждение пароля
6. Нажмите «Apply»

Примечание: Максимальная длина имени пользователя и пароля составляет 15 символов.

[System->Security->RADIUS Configuration] После настройки соответствующего RADIUS-сервера плата удаленного управления может использовать для входа в систему имя пользователя и пароль, настроенные на этом RADIUS-сервере.

Элемент	Определение
Server IP (IP-адрес сервера)	IP-адрес/домен RADIUS-сервера
Shared Secret (Общий ключ)	Общий ключ к RADIUS-серверу.
Server Port (Порт сервера)	UDP порт, который использует RADIUS-сервер.
Test Setting (Параметры тестирования)	Тестирование RADIUS-сервера с параметрами имени пользователя и пароля. В случае успешного прохождения аутентификации настройки будут сохранены.
Skip Test (Пропуск тестирования)	Сохранение настроек RADIUS-сервера без тестирования.

Примечание: Для настройки учетной записи на серверах RADIUS см. Приложение 2.

[System->Security->LDAP Configuration] После настройки соответствующего LDAP-сервера плата удаленного управления может использовать для входа имя пользователя и пароль, которые заданы на LDAP-сервере.

Элемент	Определение
LDAP-сервер	
LDAP server	IP-адрес/домен LDAP-сервера.
LDAP SSL	Разрешение установить соединение с LDAP-сервером с помощью SSL версии протокола LDAP - LDAPS (протокол защиты информации).
Порт	TCP-порт, который использует LDAP(S)-сервер.
User Base DN (База поиска пользователя)	База поиска на LDAP-сервере.
Login Attribute (Атрибут входа)	Атрибут входа в систему записи LDAP-пользователя (например: cn или uid).
Аутентификация LDAP	
Authentication Mode (Режим проверки подлинности)	Определение метода, который используется для аутентификации. • Anonymous: Запрос на подключение путем простой аутентификации по уникальному имени связывания нулевой длины и паролю нулевой длины. • Accredited User: Запрос на подключение путем простой аутентификации по уникальному имени связывания и паролю связывания. • By Logon User: Запрос на подключение путем простой аутентификации по базе поиска пользователей и паролю для входа в систему.
Авторизация LDAP	
Authorization Mode (Режим авторизации)	Определение метода авторизации. • By User Attribute: Определение уровня доступа по атрибуту пользователя и значению атрибута пользователя. • By Group: Определение уровня доступа по группе путем поиска такой информации об уникальном имени, как групповая база поиск, атрибут группы и значение атрибута группы.
Тип LDAP-сервера	
Generic LDAP Server (Базовый LDAP-сервер)	Выбор OPENLDAP в качестве типа LDAP-сервера.
Active Directory (AD) (Служба каталогов)	Выбор Windows AD в качестве типа LDAP-сервера.
AD Domain (Домен службы каталогов)	Домен AD сервера активных каталогов.
Тестирование LDAP-сервера	
Test Setting (Параметры тестирования)	Протестируйте сервер LDAP(S), используя параметры имени пользователя и пароля. В случае успешной аутентификации настройки будут сохранены.
Skip Test (Пропуск тестирования)	Сохранение настроек LDAP(S)-сервера без тестирования.

Примечание: Информация о настройке учетной записи на LDAP- и Windows AD-серверах приведена в Приложении 2.

[System->Security->Session Control] Настройка времени ожидания для автоматического выхода из открытых сеансов.

Элемент	Определение
Timeout (Время ожидания)	Период времени (в минутах) перед автоматическим выходом из системы.

[System->Network Service->TCP/IPv4] Отображение текущих установочных параметров TCP/IPv4. Настройка DHCP и DNS-сервера.

Элемент	Определение
Current Configuration (Текущая конфигурация)	Отображение текущих установочных параметров TCP/IP: IP-адреса, маски подсети, шлюза и DNS-сервера.
DHCP	Для получения IP-адреса, маски подсети и шлюза от DHCP-сервера выберите параметр «Enable DHCP» и нажмите «Apply». Для получения IP-адреса от DNS-службы DHCP-сервера выберите параметр «Obtain DNS Address from DHCP» и нажмите «Apply».
Manual (Вручную)	Непосредственный ввод установочных параметров TCP/IP и нажатие кнопки «Apply».

[System->Network Service->TCP/IPv6] Отображение и настройка текущих параметров IPv6.

Элемент	Определение
IPv6 Interface (Интерфейс IPv6)	Отображение текущего интерфейса IPv6-протокола.
IPv6 Gateway (Шлюз IPv6)	Отображение текущего шлюза IPv6-протокола.
Конфигурация IPv6	
Access (Доступ)	Выбор параметра Enable (включен) или Disable (выключен) для IPv6-службы.
Address Mode (Режим доступа)	
Router Control (Управление маршрутизатором)	В соответствии с настроенными параметрами маршрутизатора IPv6-адрес назначается одним из следующих способов: Автоконфигурация адреса без сохранения состояния, DHCPv6 без сохранения состояния или DHCPv6 с сохранением состояния.
Manual (Вручную)	Назначение IPv6-адреса вручную.
Manual IPv6 Address (Ввод IPv6-адреса вручную)	Прямой ввод IPv6-адреса в случае выбора параметра «Manual».

[System->Network Service->SNMPv1 Service] Разрешение пользователям использовать систему управления сетью (NMS) и настроить соответствующие параметры протокола SNMPv1.

Элемент	Определение
Служба SNMPv1	
Allow Access (Разрешить доступ)	Установить для SNMP-службы параметр Enable (Включить) или Disable (Отключить).
Управление SNMPv1-доступом	
Community (Сообщество)	Имя, используемое для доступа к этому сообществу из системы управления сетью (NMS). Поле должно содержать от 1 до 15 символов.

Элемент	Определение
IP Address (IP-адрес)	Доступ к системе NMS может быть ограничен вводом определенного IP-адреса или маски подсети IP-адресов. Для маски подсети применяются следующие правила: • 192.168.20.255: доступ через NMS только к сегменту 192.168.20. • 192.255.255.255: доступ через NMS только к сегменту 192. • 0.0.0.0 (установка по умолчанию) или 255.255.255.255: доступ через любую NMS к любому сегменту.
Access Type (Тип доступа)	Допустимое действие для NMS-системы через сообщество и IP-адрес. • Read Only (Только чтение): Применение команды GET разрешено в любое время; применение команды SET ограничено. • Write/Read (Запись/чтение): Применение команды GET разрешено в любое время; применение команды SET разрешено в любое время, пока сеанс связи пользователя не активен. • Forbidden (Запрещение): Применение команд GET и SET ограничено.

[System->Network Service->SNMPv3 Service] Разрешение пользователям использовать NMS-систему и настроить соответствующие параметры протокола SNMPv3.

Элемент	Определение
Служба SNMPv3	
Allow Access (Разрешить доступ)	Установить для SNMPv3-службы параметр Enable (Включить) или Disable (Отключить).
Управление SNMPv3-доступом	
User Name (Имя пользователя)	Имя для идентификации пользователя SNMPv3. Длина поля от 1 до 31 символа.
Authentication Password (Пароль аутентификации)	Пароль для создания аутентификационного ключа. Длина поля от 1 до 31 символа.
Privacy Password (Пароль конфиденциальности)	Пароль для создания ключа шифрования. Длина поля от 1 до 31 символа.
IP Address (IP-адрес)	Доступ к системе NMS может быть ограничен вводом определенного IP-адреса или маски подсети IP-адресов. Для маски подсети применяются следующие правила: • 192.168.20.255: доступ через NMS только к сегменту 192.168.20. • 192.255.255.255: доступ через NMS только к сегменту 192. • 0.0.0.0 (установка по умолчанию) или 255.255.255.255: доступ через любую NMS к любому сегменту.
Authentication Type (Тип аутентификации)	Хэш-верификация для проверки подлинности.
Privacy Type (Тип конфиденциальности)	Тип шифрования/дешифрования данных.

Примечание: Невозможно выбрать протокол конфиденциальности, если не выбран протокол аутентификации.

[System->Network Service->Web Service] Выбор параметра «Enable» для разрешения доступа к службе HTTP или HTTPS и настройка для них TCP/IP-порта.

Элемент	Определение
Доступ	
Allow Access (Разрешить доступ)	Разрешение доступа к сервису HTTP или HTTPS. HTTPS- протокол поддерживает следующий список алгоритмов шифрования: • AES (256/128 бит) • Camellia (256/128 бит) • 3DES (168 бит) • DES (168 бит)
Установочные параметры Http-протокола	
Http Port (Http-порт)	TCP/IP-порт протокола передачи гипертекста (HTTP) (по умолчанию 80)
Установочные параметры Https-протокола	
Https Port (Https-порт)	TCP/IP-порт защищенного протокола передачи гипертекста (HTTPS) (по умолчанию 443)
Certificate Status (Статус сертификата)	• Valid Certificate (Действительный сертификат) (или Invalid Certificate (Недействительный сертификат)): Для просмотра подробной информации о сертификате щелкните по параметру. • Upload Certificate (Загрузить сертификат): Нажмите эту опции для загрузки и замены текущего сертификата. Примечание: Загрузка сертификата должна выполняться по стандартному PEM-протоколу (электронная почта с повышенной защитой).

[System->Network Service->Console Service] Выбор параметра Enable для разрешения доступа к Telnet- или SSH-службе и настройка TCP/IP-порта, который используется для соединения службой Telnet или SSH.

Элемент	Определение
Доступ	
Allow Access (Разрешить доступ)	Включение доступа к Telnet или SSH версии 2, которые шифруют передачу имен пользователей, паролей и данных
Установочные параметры Telnet-протокола	
Telnet Port (Telnet-порт)	TCP/IP-порт (по умолчанию 23), который протокол Telnet использует для соединения.

Элемент	Определение
Установочные параметры SSH-протокола	
SSH Port (SSH-порт)	TCP/IP-порт (по умолчанию 22), который SSH-протокол использует для соединения.
Hostkey Status (Статус хост-ключа)	- Отображение статуса отпечатка хост-ключа для подтверждения его достоверности или недостоверности. Upload Hostkey (Загрузить хост-ключ): Выберите этот параметр для загрузки и замены текущего хост-ключа. Export Hostkey (Экспортировать хост-ключ): Выберите этот параметр для экспорта текущего хост-ключа.

Примечание: Для повышения уровня безопасности пользователи могут изменить установочный параметр порта на параметр любого неиспользуемого порта от 5000 до 65535. Затем пользователи должны назначить порт, отличный от порта по умолчанию, для получения к нему доступа. Для Telnet-клиентов необходимо, чтобы пользователи добавляли в командную строку пробел и номер порта или двоеточие и номер порта для доступа к консоли управления.

[System->Network Service->FTP Service] Разрешение пользователям включать/отключать службу FTP-сервера и настраивать TCP/IP-порт FTP-сервера (по умолчанию 21).

Элемент	Определение
Allow Access (Разрешить доступ)	Разрешение доступа к FTP-серверу.
Service Port (Сервисный порт)	TCP/IP-порт FTP-сервера (по умолчанию 21). Для повышения уровня безопасности пользователи могут изменить установочный параметр порта на параметр любого неиспользуемого порта от 5000 до 65535.

Примечание: Для обновления встроенного ПО используется FTP-сервер. Дополнительную информацию о процессе обновления см. в разделе «Обновление встроенного ПО».

[System->Notifications->Event Action] Настройка параметров уведомлений для каждого события на устройстве. Для упрощения управления события разделены на категории.

- **Log:** Запись события в журналы регистрации событий.
- **E-mail:** Отправка электронного сообщения конкретному пользователю (необходим доступ к SMTP-серверу).
- **Trap:** SNMP-прерывание, переданное на конкретный IP-адрес.
- **Syslog:** Отправка Syslog-сообщения на конкретный Syslog-сервер. (Необходим доступный Syslog-сервер).
- **SMS:** Отправка короткого сообщения на определенный номер мобильного телефона (необходим доступный поставщик SMS).

[System->Notifications->SMTP Server] После установки соответствующего SMTP-сервера при наступлении определенных событий получателем может быть отправлено электронное сообщение.

Элемент	Определение
Поставщик услуг	Поставщик услуг электронной почты. Возможны две опции: General и Gmail .
General (Общий)	Выберите для поставщика услуг опцию «General». Задайте все настройки поля и нажмите «Apply» для их сохранения.

Элемент	Определение
Gmail	Выберите для поставщика услуг опцию «Gmail». Для авторизации с целью отправки почтового уведомления нажмите «Authorize». Затем введите имя отправителя и нажмите «Apply», чтобы сохранить настройки.
SMTP server address (Адрес SMTP-сервера)	IP-адрес или имя хоста SMTP-сервера, который используется для отправки электронной почты.
Sender's E-mail Address (Электронный адрес отправителя)	Адрес электронной почты, который используется для отправки электронного уведомления.
Authentication (Аутентификация)	Выберите эту опцию, если SMTP-сервер требует аутентификации пользователя.
Account (Учетная запись)	Учетная запись, используемая для аутентификации, максимальная длина которой 63 символа.
Password (Пароль)	Пароль, используемый для аутентификации, максимальная длина которого 63 символа.
Secure connection (Защищенное соединение)	Разрешение использовать TLS- или SSL-протокол защищенной передачи данных.
Service port (Сервисный порт)	Номер порта, который используется для соединения с SMTP-сервером.

[System->Notifications->E-mail Recipients] Настройка до пяти получателей электронной почты для получения уведомлений при наступлении сконфигурированных событий.

Для добавления нового получателя, нажмите «New Recipient». Для изменения или удаления существующего получателя щелкните по адресу его электронной почты. Для проверки правильности настройки SMTP-протокола и получателей электронной почты, нажмите кнопку «TEST», чтобы отправить тестовое сообщение.

[System->Notifications->Trap Receivers] Настройка до 10 получателей SNMP-прерываний по IP-адресу (поддерживается IPv6-протокол). Поддерживаются версии 1 и 3 SNMP-протокола. Перечисленные получатели прерываний будут уведомлены при возникновении событий устройства.

Для добавления нового получателя, нажмите «New Receiver». Для изменения или удаления существующего получателя щелкните по его IP-адресу или имени. Для проверки, правильно ли принимаются прерывания, нажмите кнопку «TEST».

[System->Notifications->SMS Service] Служба коротких сообщений (SMS) - это служба связи, которая используется системами мобильной связи. Использование стандартизованных протоколов связи позволит обмениваться короткими текстовыми сообщениями между мобильными устройствами. Система предоставляет пользователям на выбор 4 способа отправки сообщений.

Элемент	Описание
Service provider is Clickatell (Поставщик услуг - Clickatell)	В поле «SMS Method» выберите опцию Clickatell . Заполните все данные учетной записи, включая поля Username (Логин), Password (Пароль) и HTTP API ID (Идентификатор). Например: User Name Name Password Passwd HTTP API ID 3234599
Service provider accepts HTTP GET (Поставщик услуг принимает метод GET HTTP-запроса)	Эта спецификация от поставщика SMS требуется перед использованием метода HTTP GET . Выберите в поле «SMS Method» опцию HTTP GET . Вставьте E_PHONE_NUMBER в качестве номера мобильного телефона получателя и E_PHONE_MESSAGE в качестве сообщения о событии, описанного в спецификации поставщика SMS и заполните поле URL. Перед отправкой сообщения поставщик SMS заменит эти выражения соответствующим контентом. Например: URL http:// ServiceProviderURL ?user= Name &password= Passwd &api_id= 3234599 &to=E_PHONE_NUMBER&text=E_MESSAGE
Service provider accepts HTTP POST (Поставщик услуг принимает метод POST HTTP-запроса)	Эта спецификация от поставщика SMS требуется перед использованием метода доставки сообщений HTTP POST через поставщиков SMS. Выберите в поле «SMS Method» опцию HTTP POST . Вставьте E_PHONE_NUMBER в качестве номера мобильного телефона получателя и E_PHONE_MESSAGE в качестве сообщения о событии, описанного в спецификации поставщика SMS, и заполните поля POST URL и POST BODY. Перед отправкой сообщения поставщик SMS заменит эти выражения соответствующим контентом. Например: URL http:// ServiceProviderURL Контент user= Name &password= Passwd &api_id= 3234599 &to=E_PHONE_NUMBER&text=E_MESSAGE

Элемент	Определение
Service provider accepts E-mail (SMTP) (Поставщик услуг принимает электронную почту (SMTP))	Эта спецификация от поставщика SMS требуется перед использованием электронной почты для доставки сообщений через поставщиков SMS. Выберите опцию E-mail в поле «Service Provider». Вставьте E_PHONE_NUMBER NUMBER в качестве номера мобильного телефона получателя и E_PHONE_MESSAGE как сообщение о событии, описанное в спецификации поставщика SMS. Введите адрес получателя, тему сообщения и содержание. Перед отправкой сообщения поставщик SMS заменит эти выражения соответствующим контентом. Например: Адрес sample@cyberpower.com Тема TestSubject Контент E_PHONE_NUMBER&text=E_MESSAGE

[System->Notifications->SMS Recipients] Пользователи могут ввести в качестве получателей SMS до 10 номеров мобильных телефонов. Получатели примут короткое уведомление о возникновении настроенных событий.

Для добавления нового получателя, нажмите «New Recipient». Для изменения или удаления существующего получателя щелкните по номеру его мобильного телефона или его имени. Для проверки параметров SMS, нажмите кнопку «TEST» и проверьте, правильно ли получено тестовое сообщение.

[System->Reset/Reboot] Сброс данных или перезагрузка системы RMCARD.

Элемент	Определение
Reboot System (Перезагрузить систему)	Перезапуск системы без выключения и перезапуска ИБП.
Reset System (Сбросить настройки системы)	Сброс системных настроек системы до заводских значений по умолчанию. Система перезапустится. При этом ИБП не выключится и не перезапустится.
Reset System (TCP/IP Settings Reserved) (Сбросить настройки системы - TCP/IP-настройки сохраняются)	Сброс системных настроек до заводских значений по умолчанию, но с сохранением настроек TCP/IP. Система перезапустится. При этом ИБП не выключится и не перезапустится.

[System->About] Отображение системной информации для платы удаленного управления.

Элемент	Определение
Model Name (Имя модели)	Имя модели платы удаленного управления.
Hardware Version (Версия оборудования)	Аппаратная версия платы удаленного управления.
Firmware Version (Версия встроенного ПО)	Текущая версия встроенного ПО, установленного на плате удаленного управления
Firmware Updated Date (Дата обновления встроенного ПО)	Дата последнего обновления встроенного ПО.
Serial Number (Серийный номер)	Заводской номер платы удаленного управления.
MAC Address (MAC-адрес)	MAC-адрес платы удаленного управления.
Save Configuration (Сохранение конфигурации)	Для сохранения файла конфигурации RMCARD нажмите «Save». Имя текстового файла по умолчанию будет иметь формат ГГГГ_ММ_ДД_ЧЧММ.txt.
Restore Configuration (Восстановление конфигурацию)	Используйте эту функцию для восстановления ранее сохраненной конфигурации. Для выбора сохраненного файла конфигурации нажмите «Choose File», а затем «Submit». Примечание: Сохраненный файл конфигурации содержит такие конфиденциальные данные, как имя пользователя и пароль. После завершения восстановления конфигурации предлагается удалить файл, чтобы сохранить защищаемую информацию в безопасности.
Diagnostic Information (Диагностическая информация)	Для сохранения всей диагностической информации в файле нажмите кнопку «Save». Сохраненная информация включает журналы системных событий, записи статуса и другую информацию, имеющую отношение к RMCARD/ИБП/ABP. Рекомендуется сохранить эту информацию на случай обращения за помощью в службу технической поддержки компании CyberPower.

Интерфейс командной строки

Вход в систему

Пользователи могут войти в интерфейс командной строки через консольный доступ к сети (Telnet или SSH) или локальный доступ (последовательный порт).

1. Сетевой доступ к интерфейсу командной строки

При входе пользователя в систему с логином и паролем администратора по Telnet- или SSH-протоколу, доступны два вида интерфейса - интерфейс командной строки (CLI) и интерфейс экранного меню. По умолчанию используется интерфейс командной строки. Для перехода к меню-ориентированному интерфейсу введите команду [menumode]. Для возврата к интерфейсу командной строки необходимо выйти и снова войти в систему RMCARD.

Как использовать интерфейс командной строки для telnet-доступа

Шаг 1: Необходимо убедиться, что компьютер имеет доступ к установленной сети RMCARD.

Введите в командной строке «telnet» и IP-адрес RMCARD (например, telnet 139.225.6.133, если RMCARD использует Telnet-порт по умолчанию 23). Нажмите «Enter».

Шаг 2: Введите имя пользователя и пароль (по умолчанию имя пользователя: cyber, пароль: cyber)

Как использовать интерфейс командной строки для SSH-доступа

Для доступа к интерфейсу командной строки настоятельно рекомендуется использовать SSH-протокол. SSH шифрует имена пользователей, пароли и передаваемые данные. Для применения SSH сначала необходимо настроить конфигурацию SSH и установить на свой ПК клиентскую программу SSH (например, PuTTY, HyperTerminal или Tera Term).

Примечание: Если для конфигурирования SSH-доступа используется PuTTY-клиент, настройте на терминале протокол линии передачи данных и активируйте параметр «Force off» (рис. 5).

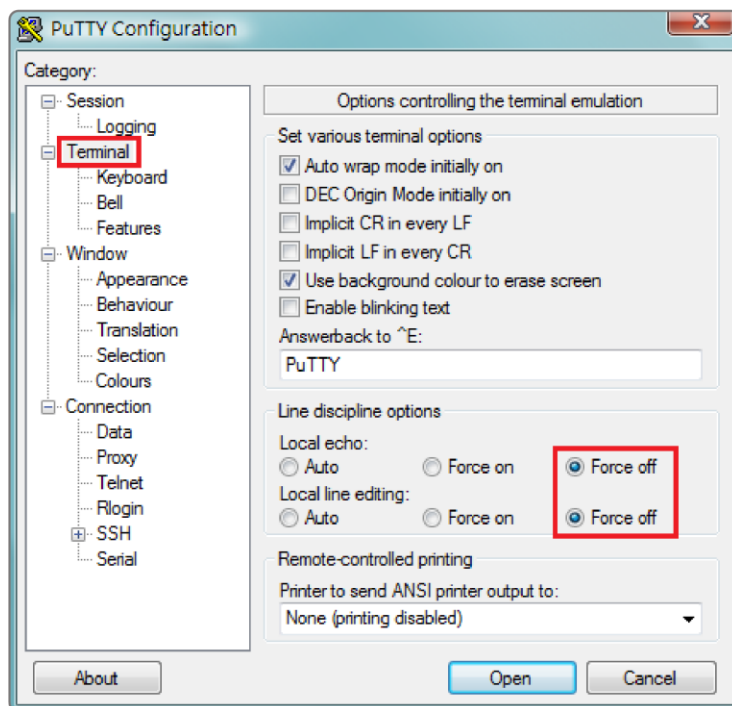


Рисунок 5. Окно конфигурирования PuTTY-клиента.

2. Локальный доступ к интерфейсу командной строки

Для входа в систему через последовательное соединение необходимо подключить ПК/сервер непосредственно к универсальному порту платы RMCARD с помощью прилагаемого кабеля для последовательного порта RJ45/DB9 и выполнить следующие шаги.

Шаг 1. Запустите на своем ПК программу Hyper Terminal (например, PuTTY, HyperTerminal или Tera Term) и выберите для подключения имя и значок.

Шаг 2. Настройте параметры COM-порта, используя следующие значения

- *Bits per second (Биты в секунду): 9600
- *Data bits (Биты данных): 8
- *Parity (Контроль четности): None
- *Stop bits (Стоповые биты): 1
- *Flow control (Управление потоком данных): None

Шаг 3. Нажмите «Enter» для входа в меню аутентификации.

Шаг 4. Введите в меню аутентификации имя пользователя и пароль RMCARD.

Примечание: Последовательное соединение может иметь доступ только к режиму командной строки и не может поддерживать режим меню.

Как использовать интерфейс командной строки

Действия в процессе пользования интерфейсом командной строки:

1. Чтобы закрыть соединение с интерфейсом командной строки → введите с клавиатуры «exit» и нажмите «Enter»
2. Чтобы переключиться в режим меню → введите «**menumode**» и нажмите «Enter»
3. Для просмотра списка доступных команд или аргументов → введите «?» (Например, дата?).
4. Для просмотра последней введенной в сеансе команды → нажмите кнопку со стрелкой ВВЕРХ / ВНИЗ. (Сеанс может запомнить до десяти ранее введенных команд).
5. Команда может поддерживать несколько параметров → при назначении даты, в виде 21 марта 2015 г. (например, дата гггг 2015 мм 3 дд 21).

Коды реакции на команды

Если команда или аргументы не распознаются или являются недопустимыми, интерфейс консоли будет отображать ниже неправильной команды или аргумента значок [^]. Будет выведено следующее сообщение об ошибке:

Command not found (Команда не найдена)	RMCARD не распознает эту команду. Интерфейс консоли отображает список доступных команд
Parameter Error (Ошибка параметра)	Недопустимый тип или формат параметра. Интерфейс консоли отображает список доступных значений или форматов.

Описание команд

ups

Описание: Отображение информации об ИБП, параметрах на входе и на выходе. Использование для управления ИБП главного выключателя.

Функция	Аргумент	Описание
info	show	Отображение параметров ИБП
input	show	Отображение параметров на входе ИБП
output	show	Отображение параметров на выходе ИБП

Пример 1:

Для просмотра параметров ИБП наберите:

CyberPower > ups info show

Параметры ИБП

Модель: OL1000XL

Номинальное напряжение: 100В

Рабочая частота: 40~70 Гц

Номинальная мощность: 1000 ВА

Номинальный ток: 10 А

Полезная выходная мощность: 900 Вт

Номинальное напряжение аккумулятора: 36 В

Версия USB: 0.1В

Дата следующей замены батареи: 10.08.2018

Батарея для некритической нагрузки (NCL): 1

Расширенный аккумуляторный блок: 4

upscntrl

Описание: Разрешение использовать главный выключатель ИБП.

Функция	Аргумент	Описание
reboot	off delay / reboot duration (например, 10/10) off delay (задержка выключения): 0 10 20 30 60 120 180 300 600 reboot duration (продолжительность перезагрузки): 10 20 30 60 120 180 300 600	Выключение и повторное включение ИБП. Указана длительность задержки выключения (в секундах) и продолжительность перезагрузки (в секундах). Пример: «10/10» означает задержку выключения 10 с и продолжительность перезагрузки 10 с.
on		Включение ИБП.
off	0 10 20 30 60 120 180 300 600	Выключение ИБП. Аргумент указывает длительность задержки выключения в секундах.

Функция	Аргумент	Описание
sleep	0 10 20 30 60 120 180 300 600	Эта команда доступна в режиме сбоя подачи электропитания. Она может перевести ИБП в режим ожидания до восстановления энергоснабжения. Аргумент указывает длительность ожидания в секундах.

Пример 1:

Перезагрузка ИБП с задержкой выключения 10 с и продолжительностью перезагрузки 20 с:

CyberPower > **upsctrl reboot 10/20**

upscfg

Описание: Отображение и настройка мощности источника питания ИБП, способности ИБП быстро реагировать на изменение параметров, верхнего порогового значения напряжения ИБП, нижнего порогового значения напряжения ИБП, состояния байпаса ИБП, верхнего порога байпаса ИБП, нижнего порога байпаса ИБП, задержки подзарядки ИБП, емкости подзарядки ИБП, рабочего режима ИБП и задержки восстановления питания ИБП.

Функция	Аргумент	Описание
show		
outpwr	<output power in VAC>	Установка выходного напряжения, которое подается на подключенное оборудование.
sen	high medium low (высокая средняя низкая)	Для низкой чувствительности характерен более свободный диапазон напряжений, а подаваемая мощность может варьироваться в более широких пределах. Питание от топливного генератора может привести к более частому переключению ИБП в режим работы от батареи, в этом случае рекомендуется настройка низкой чувствительности, тогда ИБП редко переключается в режим работы от батареи и в большей степени экономит заряд батареи. Высокая чувствительность позволяет ИБП обеспечивать более стабильное питание оборудования и частое переключение в режим работы от батареи.
hvlimit	<high threshold in VAC> (верхний порог в ВА)	Если напряжение электросети (или выходное напряжение) выше/ниже порогового значения, ИБП будет подавать на подключенное оборудование питание от батареи.
lvlimit	<low threshold in VAC> (нижний порог в ВА)	Если напряжение электросети (или выходное напряжение) выше/ниже порогового значения, ИБП будет подавать на подключенное оборудование питание от батареи.

Функция	Аргумент	Описание
bypasscond	nobypass freqvolt voltonly	No Bypass - При выборе этой опции ИБП не перейдет в режим байпаса и перестанет подавать выходную мощность. Check Volt/Freq - Если сетевое напряжение находится в диапазоне <i>пороговых значений напряжения байпаса</i>, а частота сети соответствует диапазону <i>допуска по частоте</i>, ИБП перейдет в режим байпаса. В противном случае ИБП перестанет подавать выходную мощность. Check Volt Only - ИБП перейдет в режим байпаса только в том случае, если напряжение в сети находится в диапазоне <i>пороговых значений напряжения байпаса</i>. В противном случае ИБП перестанет подавать выходную мощность.
bypassshvlimit	10 15	Задайте верхний порог напряжения байпаса (в %). Если сетевое напряжение превысит пороговые значения, ИБП будет запрещено переходить в режим байпаса.
bypasslvlimit	10 15 20	Задайте нижнее напряжение байпаса (в %). Если сетевое напряжение превысит пороговые значения, ИБП будет запрещено переходить в режим байпаса.
rechargedelay	0 60 120 180 300 600 1200 1800 3600	Установите длительность задержки подзарядки в секундах. При возобновлении сетевого электроснабжения ИБП, прежде чем вернуться в исходный режим функционирования, начнет восстанавливать заряд, пока не истечет заданный интервал времени.
rechargecap	0 15 30 45 60 75 90	Установите емкость подзарядки (в %)х. При возобновлении сетевого энергоснабжения ИБП перед возвратом в исходный режим функционирования начнет восстанавливать заряд, пока не будет достигнута заданная емкость батареи.

Функция	Аргумент	Описание
workmode	normal eco10% eco15% generator bypass	Normal - Нормальный режим работы ИБП. eco10% - Сетевой ИБП переходит в режим экономии 10%. eco15% - Сетевой ИБП переходит в режим экономии 15%. Generator - Если к ИБП подводится питание от генератора, эта опция обеспечивает его нормальное функционирование. При выборе этой опции ИБП будет запрещено переходить в режим байпаса для защиты электротехнического оборудования. Bypass - Определяет, возможность разрешения перехода ИБП в режим ручного байпаса. При активировании этой опции ИБП будет принудительно переведен в режим байпаса.
returndelay	0 ~ 600	При возобновлении сетевого электроснабжения ИБП перед восстановлением выходной мощности начнет заряжаться до истечения заданного времени задержки. Цифры в диапазоне от 1 до 600 секунд - это числа, кратные 5.

Пример 1:

Для просмотра значения доступного уровня напряжения можно установить следующее значение выходной мощности ИБП:

CyberPower > **upscfg supply?**

100

110

115

Пример 2:

Для определения состояния байпаса только с целью проверки сетевого напряжения:

CyberPower > **upscfg bypasscond voltonly**

Пример 3:

Для определения задержки дозарядки ИБП длительностью 2 минуты:

CyberPower > **upscfg rechargedelay 120**

Пример 4:

Для настройки на сетевом ИБП режима питания от генератора:

CyberPower > **upscfg mode generator**

upsbatt

Описание: Отображение информации о батарее, выполнение тестирования батареи и калибровки ИБП.

Функция	Аргумент	Описание
show		Отображение всех данных о батареях для этого ИБП
test		Немедленное выполнение испытания батареи
cal	start stop	Запуск или остановка калибровки ИБП
rdyyyy	<number of year>	Задать год в дате замены батареи
rdmm	<number of month>	Задать месяц в дате замены батареи
rddd	<number of date>	Задать день месяца

Пример 1:

Для выполнения самодиагностики аккумуляторной батареи:

CyberPower > **upsbatt test**

Пример 2:

Для запуска калибровки ИБП:

CyberPower > **upsbatt cal start**

Пример 3:

Задание даты замены батареи 29 мая 2018 г.:

CyberPower > **upsbatt rdyyyy 2018 rdmm 5 rddd 29**

atsoltsta

Описание: Отображение информации о статусе розеток АВР.

Функция	Аргумент	Описание
show		Отображение информации о статусе розеток АВР
index	<1 2 ... outlet number all>	Выбор индекса розетки АВР

Пример 1:

Для отображения состояния всех розеток:

CyberPower > **atsoltsta index all show**

atsoltcfg

Описание: Отображение и настройка параметров розетки устройства ABP.

Функция	Аргумент	Описание
show		Вывод информации о конфигурации розеток ABP
index	<1 2 ... outlet number all>	Выбор индекса розеток ABP
name	<Outlet Name>	Настройка имени розетки ABP
td_on	<-1 0 1 2 ... 7200 >	Настройка задержки включения розетки ABP
td_off	<-1 0 1 2 ... 7200 >	Настройка задержки выключения розетки ABP
td_reboot	<5 6 ... 60>	Настройка длительности перезагрузки розетки ABP.
set	<1 2 ... outlet number all> <Outlet Name> <-1 0 1 2 ... 7200 > <-1 0 1 2 ... 7200 > <5 6 ... 60>	Изменение конфигурации розетки ABP

Пример 1:

Отобразить конфигурации всех розеток:
CyberPower > **atsoltcfg index all show**

Пример 2:

Присвоить розетке №1 имя test_1:
CyberPower > **atsoltcfg index 1 name test_1**

Пример 3:

Установить задержку включения розетки №2 - 3 секунды:
CyberPower > **atsoltcfg index 2 td_on 3**

Пример 4:

Установить задержку выключения розетки №3 - 3 секунды:
CyberPower > **atsoltcfg index 3 td_off 3**

Пример 5:

Установить статус задержки выключения розетки №4 как «никогда не выключать»:
CyberPower > **atsoltcfg index 4 td_off -1**

Пример 6:

Установить длительность перезагрузки розетки №5 5 секунд:
CyberPower > **atsoltcfg index 5 td_reboot 5**

Пример 7:

Присвоить розетке №1 имя test_1, установить задержку включения 3 с, задержку выключения 4 с и продолжительность перезагрузки 5 с с помощью одной команды:
CyberPower > **atsoltcfg set 1 test_1 3 4 5**

atsoltctrl

Описание: Настройка статуса розетки ABP (устройства автоматического включения резерва).

Функция	Аргумент	Описание
index	<1 2 ... outlet number all>	Выбор индекса розетки ABP
act	<on off reboot td_on td_off td_reboot>	Управление розеткой ABP

Пример 1:

Включить розетку №1 немедленно:

CyberPower > **atsoltctrl index 1 act on**

Пример 2:

Включить розетку №2 с задержкой включения:

CyberPower > **atsoltctrl index 2 act td_on**

atssrccfg

Описание: Отображение и настройка предпочтительного источника ABP.

Функция	Аргумент	Описание
show		Отображение параметров предпочтительного источника ABP
prefer	<a b none >	Указание предпочтительного источника ABP

Пример 1:

Для отображения информации о предпочтительном источнике ABP введите с клавиатуры:

CyberPower > **atssrccfg show**

Пример 2:

Для указания предпочтительного источника ABP качестве источника A:

CyberPower > **atssrccfg prefer a**

date

Описание: Отображение и настройка часового пояса, формата даты, даты, времени.

Функция	Аргумент	Описание
show		Отображение параметров системной даты для платы RMCARD
timezone	<time zone offset>	Выбор часового пояса для платы RMCARD (среднее время по Гринвичу).
format	mm/dd/yyyy yyyy/mm/dd dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd	Настройка формата системной даты
yyyy	<number of year>	Задание года системной даты

Функция	Аргумент	Описание
mm	<number of month>	Задание месяца системной даты
dd	<number of date>	Задание дня месяца
time	<00:00:00>	Задание системного времени

Пример 1:

Чтобы задать смещение часового пояса как +08: 00, введите с клавиатуры:
CyberPower > **date timezone +0800**

Пример 2:

Чтобы задать дату 21 марта 2015 г.:
CyberPower > **date yyyy 2015 mm 3 dd 21**

Пример 3:

Чтобы задать время 13:45:12:
CyberPower > **date time 13:45:12**

ntp

Описание: Отображение и настройка IP-адреса NTP-сервера, интервала времени между обновлениями сетевого протокола службы времени (NTP).

Функция	Аргумент	Описание
show		Отображение всей NTP-информации для RMCARD
access	enable disable	Если разрешено, система установит дату и время с NTP-сервера.
priip	<primary ntp server ip>	Настройка IP-адреса/доменного имени основных NTP-серверов
secip	<secondary ntp server ip>	Настройка IP-адреса/доменного имени резервных NTP-серверов
update	now 1-8760	now — Для немедленного обновления выберите опцию « <i>Update right now</i> ». 1-8760 — Настройка частоты обновления даты и времени с NTP-сервера.

Пример 1:

Для включения NTP-сервера укажите дату и время платы RMCARD:
CyberPower > **ntp access enable**

Пример 2:

Чтобы настроить IP-адрес основного NTP-сервера в виде «192.168.26.22»:
CyberPower > **ntp priip 192.168.26.22**

Пример 3:

Для немедленного обновления времени по протоколу NTP:
CyberPower > **ntp update now**

sys

Отображение и настройка идентификации платы RMCARD, сброс данных платы RMCARD.

Функция	Аргумент	Описание
show		Отображение всех системных параметров платы RMCARD
name	<system name>	Назначение имени оборудования
location	<system location>	Задание расположения силового оборудования
contact	<system contact>	Назначение контактного лица, ответственного за это оборудование.
reset	reboot notcpip all	Reboot —Перезагрузка платы RMCARD notcpip —Сброс настроек системы до значений по умолчанию, но с сохранением настроек TCP/IP, и ее перезапуск. all —Настроить все для сброса настроек системы до значений по умолчанию и ее перезапуск.

Пример 1:

Просмотр всех параметров системы:

CyberPower > **sys show**

Имя: RMCARD205 (305)

Место расположения: Серверное помещение

Контактное лицо: Администратор

Модель: RMCARD205 (305)

Аппаратная версия: 1.1

Версия встроенного ПО: 1.0.3

Дата обновления встроенного ПО: 03/08/2015

Серийный номер: TALGY2001975

MAC-адрес: 00-0C-15-00-B9-42

Пример 2:

Сброс настроек платы RMCARD к параметрам по умолчанию.

CyberPower > **sys reset all**

dst

Описание: Отображение и настройка летнего времени.

Функция	Аргумент	Описание
show		Отображение всех параметров летнего времени для платы RMCARD
mode	disable us manual	disable — Запрет перехода на летнее время (DST). us — Традиционный для США режим летнего времени manual — Ручная настройка даты и времени перехода на летнее время. После завершения этой команды последовательно введите время начала и окончания летнего времени. Параметры недели месяца: первая вторая третья четвертая последняя Параметры дня недели: Пн Вт Ср Чт Пт Сб Вс Параметры месяца: Янв Фев Мар Апр Май Июн Июл Авг Сен Окт Ноя Дек

Пример 1:

Настройка летнего времени вручную:

CyberPower > **dst type manual**

Время начала (0~23): **2**

Неделя месяца начала: **second** (вторая)

День недели начала: **Sun** (воскресенье)

Месяц начала: **Mar** (март)

Время окончания (0~23): **2**

Неделя месяца окончания: **first** (первая)

День недели окончания: **Sun** (воскресенье)

Месяц окончания: **Nov** (ноябрь)

Пример 2:

Просмотр настроек перехода на летнее время:

CyberPower > **dst show**

DST: Настройка даты и времени перехода на летне время вручную

Начало: 02:00, второе воскресенье марта

Окончание: 02:00, первое воскресенье ноября

login

Описание: Отображение и настройка аутентификацию для входа.

Функция	Аргумент	Описание
show		Отображение всех параметров входа в систему RMCARD
type	local radiuslocal radiusonly ldaplocal ldaponly	Local - Вход пользователя в систему платы удаленного управления с именем пользователя и паролем локальной учетной записи. Radiuslocal - Вход пользователя в систему платы удаленного управления с именем пользователя и паролем для аутентификации сначала на сервере RADIUS. Если сервер RADIUS не отвечает, будут использоваться имя пользователя и пароль, сконфигурированные в локальной учетной записи. Radiusonly - Вход пользователя в систему платы удаленного управления с именем пользователя и паролем для аутентификации только на RADIUS-сервере. Ldaplocal - Вход пользователя в систему платы удаленного управления с именем пользователя и паролем для аутентификации сначала на сервере LDAP. Если сервер LDAP не отвечает, будут использоваться имя пользователя и пароль локальной учетной записи. Ldaponly - Вход пользователя в систему платы удаленного управления с именем пользователя и паролем для аутентификации только на LDAP-сервере.
Secretphrase (Секретная фраза)	<Authentication Phrase>	Фраза аутентификации, которую используют для взаимодействия с программой PowerPanel® Business Remote.
Timeout (Время ожидания)	1~10	Период времени (в минутах), в течение которого система ожидает автоматического отключения. Диапазон аргументов от 1 до 10 (в минутах).

Пример 1:

Для изменения типа аутентификации для проверки подлинности локальной учетной записи на Radius-сервере:

CyberPower > **login type radiuslocal**

admin / device

Описание: Отображение и настройка основного/вторичного диспетчера IP-адресов, имени пользователя, пароля администратора/пользователя устройства.

Функция	Аргумент	Описание
show		Отображение всей информации об администраторе или устройствах, подключенных к этой плате RMCARD
access	enable disable	Включение или выключение устройства
primip	<primary manager IP>	Назначение основного диспетчера IP-адресов администратора/устройства
secmipac	enable disable	Включение или выключение вторичного диспетчера IP-адресов администратора/устройства
secmip	<secondary manager IP>	Назначение вторичного диспетчера IP-адресов администратора/устройства
name	<user name>	Назначение имени пользователя администратора/устройства
passwd	<user password>	Назначение пароля администратора/устройства

Пример 1:

Для назначения адреса основного диспетчера IP-адресов 192.168.26.0/24:

CyberPower > **admin primip 192.168.26.0/24**

Ввод пароля администратора: **cyber**

Pass

radius

Описание: Отображение и настройка параметров RADIUS-сервера.

Функция	Аргумент	Описание
show		Отображение всех параметров Radius-сервера для RMCARD
pri sec	show	Отображение параметров основного / резервного Radius-сервера.
add		Добавление Radius-сервера, затем ввод IP-адреса/секретной фразы/порта RADIUS-сервера, которые будут затребованы позже.
add	<server IP> <server secret> <server port>	Одновременное добавление параметров RADIUS-сервера, включая IP-адрес/секретную фразу/порт
priip secip	<radius server IP>	Назначение IP-адреса основного / резервного RADIUS-сервера.
priport secport	<radius server port>	Назначение UDP-порта, который используется основным / резервным Radius-сервером
prisecret secsecret	<radius server secret>	Задание общего ключа к основному/резервному Radius-серверу.
pridel secdel		Удаление основного / резервного RADIUS-сервера

Пример 1:

Для просмотра параметров основного RADIUS-сервера:

CyberPower > **radius pri show**

IP-адрес сервера: 192.168.26.33
 Секретная фраза сервера: testsecret
 Порт сервера: 1826

Пример 2:

Для просмотра параметров резервного RADIUS-сервера:

CyberPower > **radius sec show**

IP-адрес сервера: 192.168.30.58
 Секретная фраза сервера: testsecret2
 Порт сервера: 1508

Для добавления информации о конфигурации RADIUS-сервера с помощью одной команды введите следующую команду:

radius add <Server IP> <Share Secret> <Server Port>

Например:

CyberPower > **radius add 192.168.203.55 testsecret 150**

Примечание: Если уже установлены два Radius-сервера, эта команда не может быть выполнена успешно.

Idap

Описание: Отображение и настройка параметров LDAP-сервера.

Функция	Аргумент	Описание
show		Отображение всех параметров LDAP-сервера для платы RMCARD
add		Добавление LDAP-сервера, а затем ввод параметров, которые будут затребованы позже.
pritype sectype	openldap ad	Установка типа LDAP-сервера.
priip secip	<LDAP server IP>	Назначение IP-адреса основного / резервного LDAP-сервера.
prissl secssl	enable disable	Разрешение или запрещение использования протокола LDAPS.
priport secport	<LDAP server port>	Назначение TCP-порта, который используется основным / резервным LDAP-сервером.
pridn secdn	< LDAP server base DN>	Задание базы поиска основного/резервного LDAP-сервера.
priaddomain secaddomain	< LDAP server AD domain>	Задание AD домена основного/резервного сервера активных каталогов.
priattr secattr	< LDAP server login attribute>	Назначение атрибута пользовательской записи для входа в систему основного/резервного LDAP-сервера
pridel secdel		Удаление основного/резервного LDAP-сервера

Пример 1:

Для добавления LDAP-сервера:

CyberPower > **ldap add**

Ввод типа LDAP-сервера [openldap | ad]: **ad**

Ввод IP-адреса: **192.168.26.33**

Использование SSL-протокола [enable | disable]: **disable**

Ввод порта LDAP-сервера: **389**

Ввод базы поиска: **dc=cyber,dc=com**

Ввод атрибута имени пользователя: **cn**

Ввод домена:активного каталога: **cyber.com**

Пример 2:

Для просмотра параметров LDAP-сервера

CyberPower > **ldap show**

Основной LDAP-сервер:

Тип: **Windows AD**

IP-адрес LDAP-сервера: **192.168.26.33**

LDAP SSL: **Disable**

Порт: **389**

База поиска: **dc=cyber,dc=com**

Атрибут имени пользователя: **cn**

Домен активного каталога: **cyber.com**

tcpip

Описание: Отображение и настройка IP-протокола верс.4, IP-адреса, маски сети, шлюза, DNS-системы.

Функция	Аргумент	Описание
show		Отображение всех параметров IPv4 для RMCARD
dhcp	enable disable	Включение или отключение DHCP-протокола
dns	manual auto	Auto — Получить DNS-адрес от DHCP, если DHCP-протокол включен Manual — Получить DNS-адрес от DHCP, если DHCP-протокол выключен
ip	<system IP>	Установить IP-адрес системы
netmask	<system netmask>	Установить маску подсети системы
gateway	<system gateway>	Установить шлюз системы
dnsip	<system dns>	Установить DNS системы

Пример 1:

Для отключения DHCP-протокола и определения IP-адреса 192.168.26.33:

CyberPower > **tcpip dhcp disable ip 192.168.26.33**

tcip6

Описание: Отображение и конфигурирование статуса управления маршрутизатором по IPv6-протоколу, ручная настройка IP-адреса по IPv6-протоколу.

Функция	Аргумент	Описание
show		Отображение всех параметров IP-протокола верс.6 для платы RMCARD
access	enable disable	Включение или отключение услуги IPv6.
routerctrl	enable disable	IP-адрес согласно протокола IPv6 назначается с помощью метода (автонастройки адресов без сохранения состояния, по DHCPv6-протоколу без сохранения состояния или DHCPv6-протоколус сохранением состояния), который определяется настройкой маршрутизатора.
manual	enable disable	Включение или отключение ручной настройки IP-адресов по протоколу IPv6.
ip	<manual IPv6 IP>	Назначение IP-адреса по протоколу IPv6 вручную.

Пример 1:

Для назначения IP-адреса по протоколу IPv6 вручную и последующего отображения информации:

CyberPower > **tcip6 manual enable ip 2001:cdba:0:0:0:0:3257:9652 show**

Доступ: Enable

Управление роутером: Вручную: Enable

Настроенный вручную IPv6-адрес: [2001:cdba::3257:9652]

snmpv1

Описание: Отображение и настройка состояния SNMPv1-протокола.

Функция	Аргумент	Описание
show		Отображение статуса SNMPv1 для RMCARD
index	<1 2 3 4>	Выбор индекса сообщества SNMPv1-протокола.
set	<1 2 3 4>	Изменение параметров сообщества SNMPv1.
access	enable disable	Включение или выключение SNMPv1-протокола.
community	<Community>	Изменение имени сообщества SNMPv1.
ip	<IP-адрес>	Изменение IP-адреса сообщества SNMPv1.
type	<readonly readwrite forbidden>	Изменение типа сообщества SNMPv1.

Пример 1:

Для просмотра параметров второго сообщества SNMPv1:

CyberPower > **snmpv1 index 2 show**

Сообщество: приватное

IP-адрес: 192.169.203.20

Тип: Чтение/Запись

Пример 2:

Для изменения имени сообщества первого SNMPv1-сообщества на «Public1»:

CyberPower > **snmpv1 index 1 community Public1**

Пример 3:

Для изменения IP-адреса третьего сообщества SNMPv1 на 192.168.203.88:

CyberPower > **snmpv1 index 3 ip 192.168.203.88**

Пример 4:

Для изменения типа сообщества четвертого SNMPv1-сообщества на «read/write» (чтение/запись):

CyberPower > **snmpv1 index 4 type readwrite**

Для выполнения настройки всех параметров с помощью одной команды, введите нижеследующую команду:

snmpv1set<1|2|3|4><Community><IP-адрес><readonly|readwrite|forbidden>

Например:

CyberPower > **snmpv1 set 3 CyberPower 192.168.203.91 readonly**

snmpv3

Описание: Отображение и настройка статуса SNMPv3-протокола.

Функция	Аргумент	Описание
show		Отображение статуса SNMPv3 для RMCARD
index	<1 2 3 4>	Выбор индекса пользователя SNMPv3
set	<1 2 3 4>	Изменение информации о пользователе SNMPv3
access	enable disable	Включение или отключение SNMPv3-протокола
name	<User Name>	Изменение имени пользователя SNMPv3
status	<enable disable>	Включение или отключение пользователя SNMPv3
ip	<IP-адрес>	Изменение IP-адреса пользователя SNMPv3
auth	<md5 sha none>	Изменение протокола аутентификации пользователя SNMPv3
authkey	<Auth Key>	Изменение пароля аутентификации пользователя SNMPv3
priv	<aes des none>	Изменение протокола конфиденциальности пользователя SNMPv3
privkey	<Priv Key>	Изменение пароля конфиденциальности пользователя SNMPv3

Пример 1:

Для просмотра параметров первого SNMPv3-пользователя:

CyberPower > **snmpv3 index 1 show**

Имя пользователя: CyberPower

Состояние: Разрешено

IP-адрес: 192.169.30.58

Протокол аутентификации: MD5

Конфиденциальный протокол: aes

Пример 2:

Для изменения имени пользователя второго пользователя SNMPv3 на «CyberPower»:
CyberPower > **snmpv3 index 2 name CyberPower**

Пример 3:

Подключение третьего пользователя SNMPv3:
CyberPower > **snmpv3 index 3 status enable**

Пример 4:

Для изменения IP-адреса четвертого пользователя SNMPv3 на 192.168.203.66:
CyberPower > **snmpv3 index 4 ip 192.168.203.66**

Пример 5:

Для изменения протокола аутентификации второго пользователя SNMPv3 на «md5» и назначения ему пароля аутентификации «test_authkey_123456»:
CyberPower > **snmpv3 index 2 auth md5 authkey test_authkey_123456**

Пример 6:

Для изменения пароля аутентификации первого пользователя SNMPv3 на «test_authkey_123456»:
CyberPower > **snmpv3 index 1 authkey test_authkey_123456**

Пример 7:

Для изменения протокола аутентификации третьего пользователя SNMPv3 на «none» (отсутствует):
CyberPower > **snmpv3 index 3 auth none**

Пример 8:

Для изменения протокола конфиденциальности второго пользователя SNMPv3 на «aes» и назначения ему пароля конфиденциальности «test_privkey_123456»:
CyberPower > **snmpv3 index 2 priv aes privkey test_privkey_123456**

Пример 9:

Для изменения пароля конфиденциальности первого пользователя SNMPv3 на «test_privkey_123456»:
CyberPower > **snmpv3 index 1 privkey test_privkey_123456**

Пример 10:

Для изменения протокола конфиденциальности третьего пользователя SNMPv3 на «none» (отсутствует):
CyberPower > **snmpv3 index 3 priv none**

Для конфигурирования всех параметров с помощью одной команды введите следующую команду:

```
snmpv3 set <1 | 2 | 3 | 4> <User Name> <IP Address> <md5 | sha | none> <Auth Key>
<aes | des | none> <Priv Key>
```

Например:

```
CyberPower > snmpv3 set 1 CyberPower 192.168.203.90 sha test_authkey_123456 des
test_privkey_123456
```

trap

Описание: Отображение и настройка параметров приемника SNMP-прерываний.

Функция	Аргумент	Описание
show		Отображение параметров приемника прерываний для RMCARD.
add		Добавление приемника прерываний к RMCARD.
index	<1 2 ... 10>	Выбор индекса приемника прерываний
name	<Trap Receiver Name>	Изменение имени прерывания приемника прерываний
ip	<Trap Receiver IP>	Изменение IP-адреса приемника прерываний
ver	<v1 v3>	Изменение SNMP-версии приемника прерываний.
status	<enable disable>	Включение или выключение приемника прерываний.
community	<Trap Receiver Community>	Изменение имени SNMPv1-сообщества приемника прерываний
user	<1 2 3 4>	Выбор SNMPv3-пользователя приемника прерываний
delete		Удаление приемника прерываний.

Пример 1:

Для просмотра параметров шестого приемника прерываний:

```
CyberPower > trap index 6 show
Имя прерывания: CyberPower
Состояние: Enable
IP-адрес: 192.168.203.68
Тип: SNMPv1
Сообщество: test_community
```

Пример 2:

Для изменения имени прерывания второго приёмника прерываний для тестирования:

```
CyberPower > trap index 2 name test
```

Пример 3:

Для изменения IP-адреса третьего приёмника прерываний на 192.168.30.85:

```
CyberPower > trap index 3 ip 192.168.30.85
```

Пример 4:

Для изменения версию четвертого приёмника SNMP-прерываний на «SNMPv3»:

```
CyberPower > trap index 4 ver v3
```

Пример 5:

Для изменения статуса пятого приёмника прерываний:

```
CyberPower > trap index 5 status enable.
```

Пример 6:

Для изменения имени сообщества второго приёмника прерываний на «CyberPower» с условием, что версия приёмника SNMP-прерываний должна быть SNMPv1:

CyberPower > **trap index 2 community CyberPower**

Пример 7:

Для изменения пользователя SNMPv3 десятого приёмника прерываний на пользователя «SNMPv3 user2» с условием, что версия приёмника SNMP-прерываний должна быть SNMPv3:

CyberPower > **trap index 10 user 2**

Пример 8:

Для удаления пятого приёмника прерываний:

CyberPower > **trap index 5 delete**

Для добавления конфигурации приемника прерываний с помощью одной команды, введите следующую команду:

Для SNMPv1: trap add <Trap Name> <Trap Receiver IP> v1 <Community>

Например:

CyberPower > **trap add CyberPower 192.168.203.16 v1 test**

Для SNMPv3: trap add <Trap Name> <Trap Receiver IP> v3 <1 | 2 | 3 | 4>

Например:

CyberPower > **trap add cyberpower 192.168.203.12 v3 3**

web

Описание: Отображение и настройка типа веб-доступа, http-порта и https-порта

Функция	Аргумент	Описание
show		Отображение всей веб-информации для RMCARD
access	http https disable	http — Разрешение доступа к http-службе https — Разрешение доступа к https-службе disable — Отключение веб-службы
httpport	<http port>	Порт TCP/IP протокола передачи гипертекста (HTTP) (по умолчанию 80)
httpsport	<https port>	Порт TCP/IP протокола защищенной передачи гипертекста (HTTPS) (по умолчанию 443)

Пример 1:

Для изменения порта HTTP-сервера на 5000

CyberPower > **web httpport 5000**

console

Описание: Отображение и настройка консольного типа доступа к сети, telnet-порта и SSH-порта

Функция	Аргумент	Описание
show		Отображение параметров консоли для RMCARD
access	telnet ssh disable	telnet — Разрешение доступа к Telnet-протоколу ssh — Разрешение доступа к SSH-протоколу disable — Отключение консольной службы
telnet	<enable disable>	enable — Включение Telnet-протокола disable — Отключение Telnet-протокола
ssh	<enable disable reset_hostkey>	enable — Включение SSH-протокола disable — Отключение SSH-протокола reset_hostkey — Сброс настроек SSH хост-ключа к значению по умолчанию
telnetport	<telnet port>	Порт TCP/IP (по умолчанию 23), который Telnet-протокол использует для соединения
sshport	<ssh port>	Порт TCP/IP (по умолчанию 22), который SSH-протокол использует для соединения

Пример 1:

Для разрешения использовать в качестве типа консоли Telnet:

CyberPower > **console telnet enable**

Пример 2:

Для запрещения использования в качестве типа консоли SSH:

CyberPower > **console ssh disable**

Примечание: Реализуется возможность переключения между собой telnet- и ssh-режимов.

Например, после включения ssh-протокола в качестве типа консоли telnet-протокол будет автоматически отключен, и наоборот.

Пример 3:

Для сброса параметров SSH хост-ключа к настройкам по умолчанию

CyberPower > **console ssh reset_hostkey**

Примечание: После сброса параметров SSH хост-ключа RMCARD система перезагрузится со значениями параметров по умолчанию.

ftp

Описание: Отображение и настройка типа FTP-доступа и TCP/IP-порта FTP-сервера.

Функция	Аргумент	Описание
show		Отображение всех FTP-параметров для RMCARD
access	enable disable	Включение или выключение FTP-сервера
port	<ftp port>	TCP/IP-порт FTP-сервера (по умолчанию 21)

Пример 1:

Включение службы FTP:

CyberPower > **ftp access enable**

eventlog

Описание: Просмотр и очистка журнала событий платы RMCARD и ИБП.

Функция	Аргумент	Описание
show		Отображение списка событий и краткое описание каждого события с отметкой даты и времени.
clear		Очистка существующих журналов событий.

Пример 1:

CyberPower > **eventlog show**

12/11/2015 03:32:08 Вход Администратора с IP-адреса 192.168.26.33.

.....

Затем используйте следующие клавиши для навигации по журналу событий.

Клавиша	Описание
SPACE	Просмотр следующей страницы журнала событий.
Q	Закрытие журнала событий и возврат к интерфейсу командной строки.

Пример 2:

Для очистки всех журналов событий.

CyberPower > **eventlog clear**

Вы хотите очистить весь журнал событий [да / нет]: **да**

syslog

Описание: Отображение и настройка параметров SYSLOG-сервера.

Функция	Аргумент	Описание
		Отображение всех параметров системного журнала для RMCARD
s1 s2 s3 s4	show	Отображение параметров сервера системного журнала для 1 - 4 серверов
add		Добавление syslog-сервера, а затем ввод IP-адреса/порта сервера системного журнала, запрос на которые появится позже
add	<server IP> <server port>	Одновременное добавление параметров syslog-сервера, включая IP-адрес / порт
access	enable disable	Включение или отключение системного журнала

Функция	Аргумент	Описание
facility	kernel user mail system auth1 syslog link news uucp clock1 auth2 ftp ntp logaudit logalert clock2 local0 local1 local2 local3 local4 local5 local6 local7	Назначение параметров средств системного журнала.
s1test s2test s3test s4test		Отправка тестового сообщения на сервер системных журналов от 1 до 4 серверов
ip1 ip2 ip3 ip4	<SYSLOG server IP>	Назначение IP-адреса сервера системных журналов для от 1 до 4 серверов
port1 port2 port3 port4	<SYSLOG server port>	Назначение UDP-порта, который сервер системных журналов использует на 1 – 4 серверах
s1del s2del s3del s4del		Удаление сервера системных журналов на 1 - 4 серверах

Пример 1:

Для просмотра информация системного журнала сервера 1:

CyberPower > **syslog s1 show**

IP-адрес: 192.168.26.33

Порт: 514

Пример 2:

Для просмотра информация системного журнала сервера 2:

CyberPower > **syslog s2 show**

IP-адрес: 192.168.203.89

Порт: 268

Пример 3:

Для просмотра информация системного журнала сервера 3:

CyberPower > **syslog s3 show**

IP-адрес: 192.168.30.15

Порт: 101

Пример 4:

Для просмотра информации системного журнала сервера 4:

CyberPower > **syslog s4 show**

IP-адрес: 192.168.26.93

Порт: 358

Для выполнения настройки всех параметров с помощью одной команды введите следующую команду:

syslog add <Server IP address> <Server Port>

Например:

CyberPower > **syslog add 192.168.203.65 180**

Примечание: Невозможно успешное выполнение этой единственной команды, если уже установлены четыре сервера системных журналов.

menumode

Описание: Переключение в режим меню.

clear

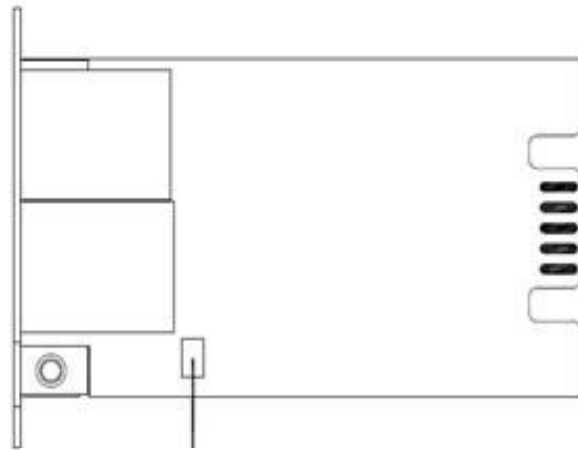
Описание: Очистка экрана консоли.

exit

Описание: Завершение соединения с интерфейсом командной строки.

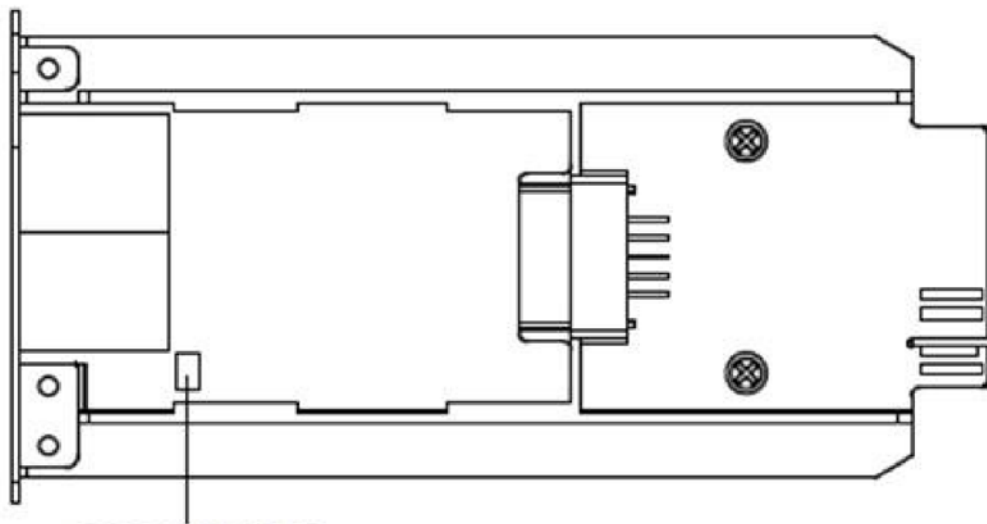
Сброс настроек до заводских по умолчанию / Восстановление настроек в случае утери пароля

Для восстановления заводских настроек платы удаленного управления CyberPower по умолчанию (включая имя пользователя и пароль для веб-входа), выполните следующее:



ПЕРЕМЫЧКА СБРОСА

RMCARD205



ПЕРЕМЫЧКА СБРОСА

RMCARD305

1. Извлеките из ИБП плату удаленного управления, не выключая ИБП / блок распределения питания с автоматическим переключателем резерва (ABP).
2. Снимите джамперную перемычку с контактов сброса, как показано на рисунке. Не утилизируйте перемычку.
3. Вставьте плату в порт расширения ИБП / блока распределения питания с ABP.
4. Подождите, пока не начнет мигать зеленый светодиод Tx/Rx (частота включения/выключения - один раз в секунду).
5. Снова извлеките плату.
6. Снова установите перемычку на контакты сброса.
7. Верните плату в порт расширения и затяните крепежные винты.

Обновление встроенного ПО платы RMCARD

При обновлении встроенного ПО можно получить как новые функции, так и обновления/улучшения существующих функций. Перед попыткой обновления встроенного ПО необходимо включить FTP-службу (Enable). Версию встроенного ПО (Firmware version) можно проверить на вкладке **[System->About]** веб-интерфейса пользователя RMCARD. Для обновления версии встроенного ПО необходимо обновить два файла.

- A. cpsrm2scfw_XXX.bin
- B. cpsrm2scdata_XXX.bin

Примечание: В целях обеспечения актуальности встроенного ПО RMCARD посещайте веб-сайт компании CyberPower каждые 3 месяца, чтобы узнать о наличии обновленной версии встроенного ПО.

Примечание: Во время обновления встроенного ПО не выключайте ИБП.

Примечание: Для успешного обновления встроенного ПО RMCARD проверьте, не заблокированы ли подключения к портам 20 и 21 в брандмауэре.

Способ 1: Использование FTP-команды

Чтобы обновить встроенное ПО, выполните следующие действия:

1. Загрузите последнюю версию встроенного ПО
2. Сохраните загруженные файлы в директории «C: \»
3. Откройте окно командной строки
4. Войдите в систему платы удаленного управления CyberPower с помощью FTP-команды путем ввода с клавиатуры в командной строке:
 - (1) ftp
 - (2) ftp> open
 - (3) To [текущий IP-адрес RMCARD] [порт]; EX: To 192.168.22.12621
 - (4) Введите ИМЯ ПОЛЬЗОВАТЕЛЯ и ПАРОЛЬ (такие же, как в учетной записи Администратора в веб-интерфейсе пользователя, информация о заводских настройках по умолчанию приведена на стр. 6)
5. Загрузите файл А путем ввода в командной строке:


```
ftp > bin
ftp > put cpsrm2scfw_XXX.bin
```
6. Загрузка завершена, введите:


```
ftp > quit
```
7. После введения команды «quit» система перезагрузится
8. Снова войдите в FTP-систему (см. шаг 4)
9. Загрузите файл В путем ввода в командной строке:


```
ftp > bin
ftp > put cpsrm2scdata_XXX.bin
```
10. Загрузка завершена, введите:


```
ftp > quit
```
11. После введения команды «quit» система перезагрузится.

Способ 2: Использование служебной программы обновления и настройки (утилита массового обновления встроенного ПО)

1. Инсталлируйте служебную программу обновления и настройки, разработанную в компании CyberPower, которую можно загрузить с сайта www.CyberPower.com.
2. После завершения инсталляции запустите программу «Upgrade and Configuration Utility».
3. На рисунке 6 показано главное окно программы «Upgrade and Configuration Utility». Средство конфигурирования отобразит все устройства, которые находятся под дистанционным управлением ПО CyberPower Remote Management, присутствующие в подсети локальной сети. Кнопка «Discover» используется для повторного поиска подсети локальной сети.

Примечание: Для выбора элементов для просмотра следует нажать кнопку «View».

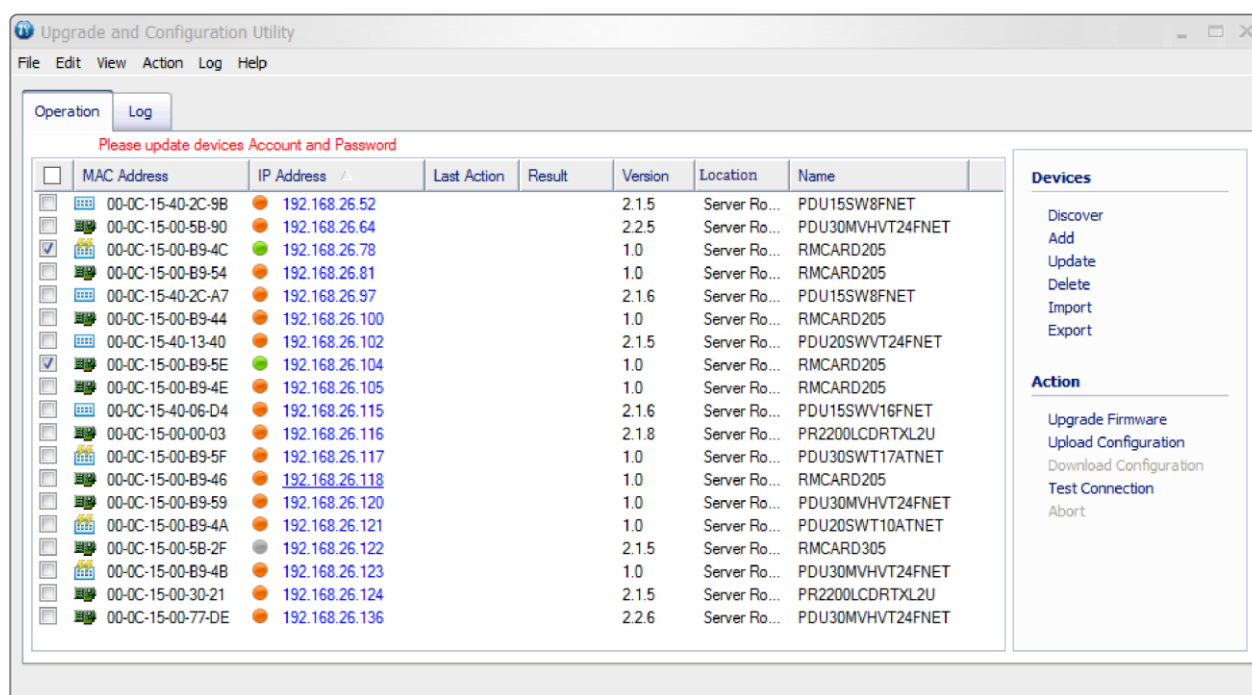


Рисунок 6. Главное окно служебной программы «Upgrade and Configuration Utility»

4. При выборе устройств для обновления установите слева от них флажки и нажмите «Update», чтобы обновить учетную запись пользователя устройства и пароль. После подтверждения обновления цвет значка состояния рядом с IP-адресом изменится с оранжевого на зеленый.

Примечание: Перед обновлением встроенного ПО необходимо обновить учетную запись пользователя устройства и пароль.

5. Отметьте устройства, прошивку которых следует обновить, установив флажки, и нажмите «Upgrade Firmware».

Примечание: Можно обновить встроенное ПО нескольких устройств, использующих одни и те же файлы прошивки (массовое обновление встроенного ПО).

6. Для выполнения обновления встроенного ПО выберите файлы встроенного ПО и файлы данных и нажмите «ОК», как показано на рисунке 7.

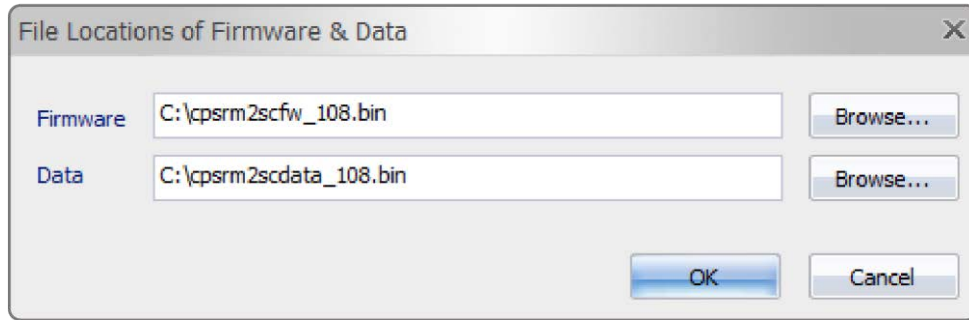


Рисунок 7. Окно расположения файлов встроенного ПО и файлов данных

7. Для запуска обновления встроенного ПО на выбранных устройствах нажмите «Yes», как показано на рисунке 8.

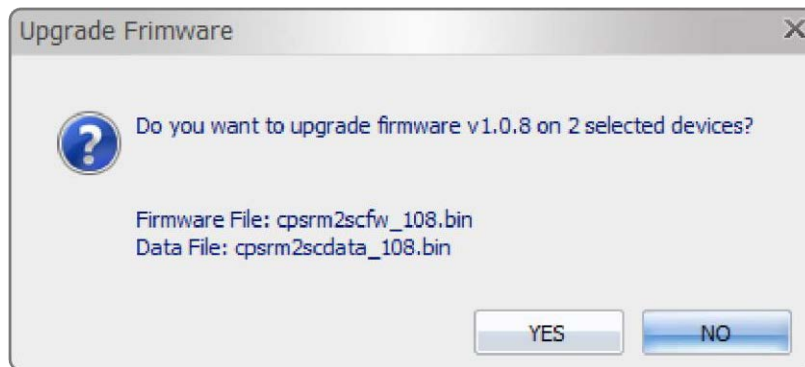


Рисунок 8. Окно сообщения с подтверждением обновления встроенного ПО

8. В случае успешного выполнения обновление встроенного ПО результат отобразится в главном окне, как показано на рисунке 9.

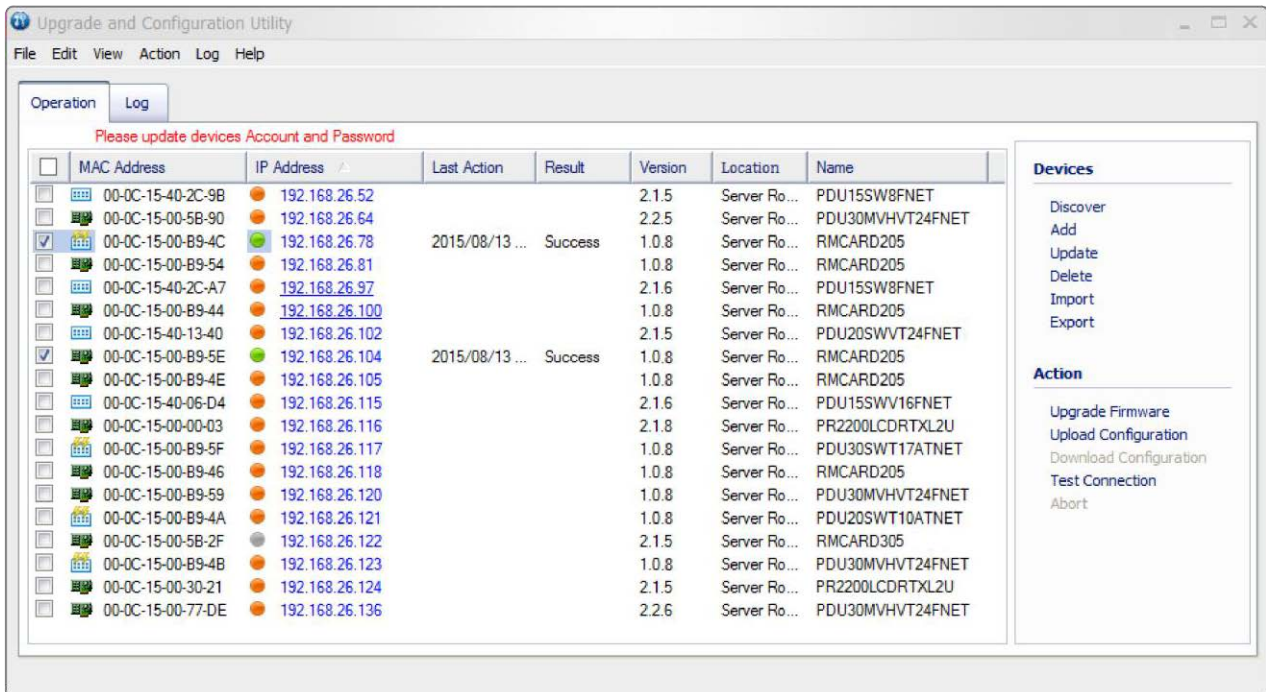


Рисунок 9. Вид главного окна после успешного обновления встроенного ПО

Способ 3: Применение команды Secure Copy (SCP)

Для обновления встроенного ПО с помощью SCP-протокола (защищенного протокола копирования) выполните следующие действия.

Примечание: Функцию обновления встроенного ПО через SCP-протокол поддерживает только версия прошивки 1.1.2 и выше.

Для пользователей ОС Windows:

1. Загрузите утилиту безопасного копирования PuTTY-клиента (PSCP).
2. Сохраните файлы встроенного ПО и утилиту PSCP в одной папке.
3. Откройте интерфейс командной строки и задайте путь к директории, в которой хранятся файлы встроенного ПО и утилита PSCP.
4. Для выполнения обновления встроенного ПО введите следующую команду:

```
pscp -scp <filename> <user>@<IP address of RMCARD>:
```

Примечание:

- (1) С платой RMCARD должно быть установлено SSH-соединение.
- (2) <filename> - это имя файла встроенного ПО. Необходимо загрузить два файла встроенного ПО: cpsrm2scfw_XXX.bin и cpsrm2scdata_XXX.bin. Для обновления версии встроенного ПО необходимо загрузить оба файла. За один раз можно загрузить только один файл встроенного ПО. Рекомендуется сначала загрузить файл встроенного ПО cpsrm2scfw_XXX.bin, а затем файл данных cpsrm2scdata_XXX.bin.
- (3) <user> - это имя пользователя учетной записи SSH на RMCARD.
- (4) Не забудьте после IP-адреса добавить «:».

Например:

```
pscp -scp cpsrm2scfw_xxx.bin cyber@192.168.1.100:
```

Примечание: cpsrm2scfw_xxx.bin - это файл обновляемой версии встроенного ПО.

5. После выполнения этой команды может появиться сообщение с вопросом о доверии к главному компьютеру. Для продолжения в течение 10 секунд введите «y» в случае положительного ответа.
6. На следующем экране введите пароль RMCARD. Пересылка файла встроенного ПО может занять несколько минут. Подождите, пока индикатор хода выполнения процесса не покажет 100%. После завершения пересылки система автоматически завершит сеанс и перезагрузится.
7. Для завершения процесса обновления встроенного ПО повторите шаги с 4 по 6, чтобы загрузить файл данных cpsrm2scdata_XXX.bin.
8. Если передача файла встроенного ПО не удалась, появится сообщение об ошибке. Попробуйте повторно ввести и выполнить команду.

Для пользователей ОС Linux, MacOS и Unix:

1. Инсталлируйте соответствующий дистрибутив SSH- или SCP-клиента, например Openssh-клиент.
2. Откройте терминал и измените путь к каталогу, в котором сохраняются файлы встроенного ПО.
3. Для выполнения обновления встроенного ПО введите следующую команду:
`scp <filename> <user>@< IP address ofRMCARD>:`

Примечание:

- (1) Должно быть установлено SSH-соединение с платой RMCARD.
- (2) <filename> - это имя файла встроенного ПО. Необходимо загрузить два файла встроенного ПО: cpsrm2scfw_XXX.bin и cpsrm2scdata_XXX.bin. Для обновления версии прошивки необходимо загрузить оба файла. За один раз можно загрузить только один файл встроенного ПО. Рекомендуется сначала загрузить файл встроенного ПО cpsrm2scfw_XXX.bin, а затем файл данных cpsrm2scdata_XXX.bin.
- (3) <user> - имя пользователя учетной записи SSH на RMCARD.
- (4) Не забудьте после IP-адреса добавить «:».

Например:

```
scp cpsrm2scfw_xxx.bin cyber@192.168.1.100:
```

Примечание: cpsrm2scfw_xxx.binis - это файл обновляемой версии встроенного ПО.

4. После выполнения этой команды может появиться сообщение с вопросом о доверии к главному компьютеру. Для продолжения в течение 10 секунд введите «y» в случае положительного ответа.
5. На следующем экране введите пароль RMCARD. Пересылка файла встроенного ПО может занять несколько минут. Подождите, пока индикатор хода выполнения процесса не покажет 100%. После завершения пересылки система автоматически завершит сеанс и перезагрузится.
6. Для завершения процесса обновления встроенного ПО повторите шаги с 3 по 5, чтобы загрузить файл данных cpsrm2scdata_XXX.bin.
7. Если передача файла встроенного ПО не удалась, появится сообщение об ошибке. Попробуйте повторно ввести и выполнить команду.

Сохранение и восстановление параметров конфигурации

Способ 1: Через веб-интерфейс

На вкладке **[System->About]** можно легко сохранить конфигурацию устройства на локальный ПК с возможностью ее восстановления в дальнейшем.

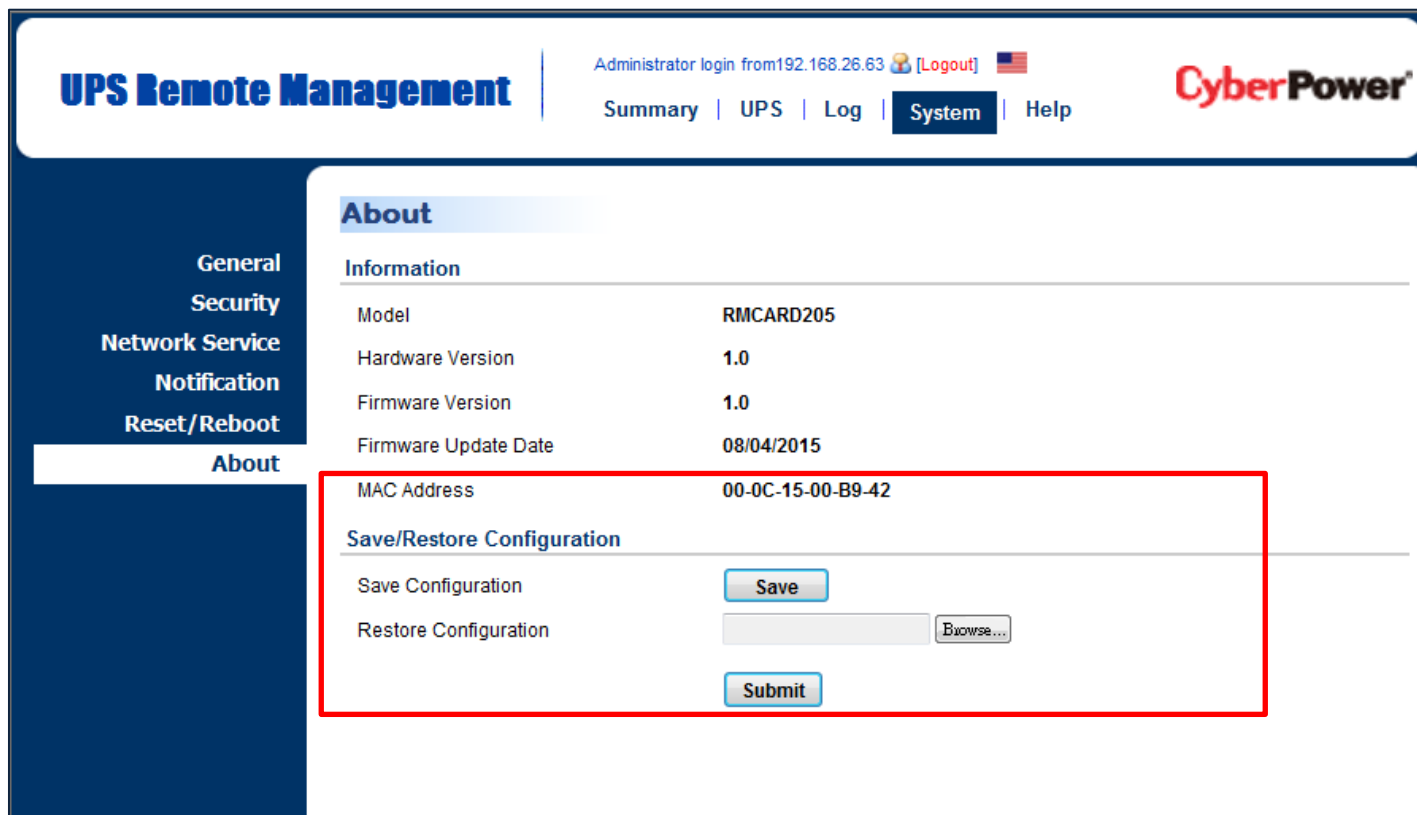


Рисунок 10. Сохранение/восстановление конфигурации в главном окне

Можно легко сохранить и восстановить конфигурацию устройства на локальном ПК на вкладке **[System->About]**, как показано на рисунке 10.

Для сохранения конфигурации на локальном ПК нажмите «Save», чтобы сохранить файл конфигурации. По умолчанию текстовый файл будет иметь формат ГГГГ_ММ_ДД_ЧЧММ.txt. Для восстановления конфигурации нажмите «Browse», чтобы найти сохраненный файл конфигурации, и нажмите «Submit» для восстановления конфигурации, которая была сохранена ранее.

Примечание: Только версия 1.1.5 и выше встроенного ПО поддерживает функцию сохранения и восстановления конфигурации с текущей конфигурацией параметров ИБП и АВР.

Способ 2: При помощи команды Secure Copy (SCP)

Для восстановления конфигурации через SCP-протокол выполните следующие действия.

Примечание: Только версия 1.1.5 и выше встроенного ПО поддерживает функцию восстановления конфигурации через SCP.

Для пользователей ОС Windows:

1. Загрузите утилиту безопасного копирования PuTTY-клиента (PSCP).
2. Сохраните файл конфигурации и утилиту PSCP в одной папке.
3. Откройте интерфейс командной строки и задайте путь к директории, в которой хранятся файл конфигурации и утилита PSCP.
4. Для восстановления конфигурации введите следующую команду:
`pscp -scp <filename> <user>@<IP address of RMCARD>:`

Примечание:

- (1) Должно быть установлено SSH-соединение с платой RMCARD.
- (2) <filename> - это имя файла конфигурации с форматом по умолчанию YYYY_MM_DD_HHMM.txt.
- (3) <user>- это имя пользователя учетной записи SSH на RMCARD.
- (4) Не забудьте после IP-адреса добавить «:»..

Например:

```
pscp -scp YYYY_MM_DD_HHMM.txt cyber@192.168.1.100:
```

Примечание: YYYY_MM_DD_HHMM.txt – это файл конфигурации, которую нужно восстановить.

5. После выполнения этой команды может появиться сообщение с вопросом о доверии к главному компьютеру. Для продолжения в течение 10 секунд введите «y» в случае положительного ответа.
6. На следующем экране введите пароль RMCARD. Подождите, пока индикатор хода выполнения процесса не покажет 100%. После завершения пересылки система автоматически завершит сеанс и перезагрузится.

Для пользователей ОС Linux, MacOS и Unix:

1. Инсталлируйте соответствующий дистрибутив SSH- или SCP-клиента, например Openssh-клиент.
2. Откройте терминал и измените путь к каталогу, в котором сохраняются файлы конфигурации.
3. Для восстановления конфигурации введите следующую команду:
`scp <filename> <user>@< IP address of RMCARD>:`

Примечание:

- (1) Должно быть установлено SSH-соединение с платой RMCARD.
- (2) <filename> - это имя файла конфигурации в формате по умолчанию YYYY_MM_DD_HHMM.txt.
- (3) <user> - имя пользователя учетной записи SSH на RMCARD.
- (4) Не забудьте после IP-адреса добавить «:»..

Например:

```
scp YYYY_MM_DD_HHMM.txt cyber@192.168.1.100:
```

Примечание: YYYY_MM_DD_HHMM.txt is – это файл конфигурации, который нужно восстановить.

4. После выполнения этой команды может появиться сообщение с вопросом о доверии к главному компьютеру. Для продолжения в течение 10 секунд введите «y» в случае положительного ответа.
5. На следующем экране введите пароль RMCARD. Подождите, пока индикатор хода выполнения процесса не покажет 100%. Система автоматически завершит сеанс и перезагрузится.

Загрузка SSH хост-ключа с помощью Secure Copy (SCP)

SSH хост-ключ может быть загружен в RMCARD205 с помощью команд безопасного копирования. Убедитесь, что строка имени загруженного файла начинается с «ssh_hostkey_». Вот некоторые примеры допустимого имени файла:

[ssh_hostkey_sample1.pem](#); [ssh_hostkey_1024.pem](#); [ssh_hostkey_type100.***](#)

Пример процесса загрузки

1. Загрузите утилиту безопасного копирования PuTTY-клиента (PSCP).
2. Поместите файл SSH хост-ключа и утилиту PSCP в одну папку.
3. Откройте командную строку и укажите путь к директории, в которой хранятся файл SSH хост-ключа и утилита PSCP.
4. Введите следующую команду

```
pscp -scp <filename> <admin_account>@<IP address of RMCARD>:
```

Например: [pscp -scp ssh_hostkey_xxx.xxx cyber@192.168.203.66:](#)
5. После выполнения этой команды может появиться сообщение с вопросом о доверии к главному компьютеру. В течение 10 секунд введите «y» в случае положительного ответа.
6. На следующем экране введите пароль Администратора. Пересылка файла может занять несколько минут. Подождите, пока индикатор хода выполнения процесса не покажет 100%. После завершения пересылки система автоматически завершит сеанс и перезагрузится.

Требование к хост-ключам

Версия SSH: SSHv2

Поддерживаемые алгоритмы и длина ключа

- Алгоритм key-exchange (Kex): dh-group-exchange-sha1 / Длина RSA-ключа 4096 бит
- Алгоритм шифрования данных: AES128-CBC, 3DES-CBC
- Алгоритм хэширования, реализуемый хэш-функцией MAC: HMAC-SHA1

Поиск и устранение неисправностей

Проблема	Решение
Невозможно настроить плату удаленного управления способом 1 или 2	1. Проверьте состояние светодиодов, если горят желтый и зеленый светодиоды, это нормально. Если не горит зеленый светодиод: ► Убедитесь, что плата удаленного управления правильно вставлена в устройство, и на устройство подается питание. Если не горит желтый светодиод: ► Убедитесь в надежности сетевого соединения. 2. Убедитесь, что используемый ПК находится в той же подсети локальной сети, что и устройство CyberPower, с которым вы пытаетесь установить соединение. 3. Убедитесь в правильном положении джамперной перемычки на коннекторах сброса.
Невозможно проверить соединение с платой удаленного управления	1. Для получения / настройки правильного IP-адреса платы удаленного управления примените способ 1 и/или 2. 2. Если используемый ПК находится в другой подсети, чем плата удаленного управления, проверьте настройку маски подсети и IP-адреса шлюза.
Утеряны имя пользователя и пароль	См. раздел «Сброс настроек до заводских по умолчанию / Восстановление настроек в случае утери пароля».
Сетевые настройки по умолчанию	IP: 192.168.20.177 Маска подсети: 255.255.255.0 DHCP: On
Невозможно получить доступ к веб-интерфейсу	1. Убедитесь, что в возможности пропинговать плату RMCARD. 2. Убедитесь, что указан правильный URL-адрес. 3. Убедитесь, что HTTP/HTTPS-доступ включен, выполнив вход на плату через интерфейс командной строки (Telnet-или SSH-клиент).
Невозможно получить/установить SNMP-протокол	SNMPv1: проверьте имя сообщества. SNMPv3: проверьте конфигурацию профиля пользователя.
Невозможно получить прерывания	1. Убедитесь в корректной настройке типов прерываний (SNMPv1/SNMPv3) и получателя прерываний. 2. Убедитесь в правильной настройке IP-адреса шлюза, если плата RMCARD и система сетевого администрирования (NMS) находятся в другой сети.

Сертификаты соответствия

Предупреждение Федеральной комиссии по связи США (FCC)

Данное оборудование успешно прошло проверку на соответствие ограничениям для цифровых устройств класса А согласно части 15 правил FCC. Эти ограничения разработаны для обеспечения надлежащей защиты от недопустимых помех при установке устройств в жилых помещениях. Это оборудование генерирует, использует и может излучать энергию радиоизлучения и оно, если установлено и используется без соблюдения приведенных инструкции, может становиться источником вредных помех для средств радиосвязи. Эксплуатация этого оборудования в жилом районе может вызвать недопустимые помехи, и в этом случае пользователь должен будет устранить помехи за свой счет.

В инструкции должны быть указаны все специальные принадлежности, необходимые для соблюдения этих требований.

Данное устройство соответствует требованиям части 15 правил FCC. Его эксплуатация возможна при соблюдении следующих двух условий:

(1) Это устройство не должно создавать вредных помех, и (2) это устройство должно принимать любые радиопомехи, включая те, которые могут вызвать сбой в работе.

Цифровое устройство класса А соответствует всем требованиям Регламента Канады по оборудованию, создающему помехи.

Европейский Союз

Это изделие класса А. В домашних условиях данное изделие может вызывать радиопомехи, и в этом случае от пользователя может потребоваться принятие соответствующих мер.

⚠ ПРЕДУПРЕЖДЕНИЕ: Это изделие может подвергать пользователя воздействию химических веществ, включая стирол, который согласно данным штата Калифорния считается причиной возникновения онкозаболеваний, и бисфенол-А, который согласно данным штата Калифорния считается причиной врожденных дефектов или других нарушений репродуктивной функции. Дополнительную информацию см. на сайте www.P65Warnings.ca.gov.

Приложение 1: Идентификация IP-адреса платы удаленного управления CyberPower

Общее представление

Все устройства в компьютерной сети должны иметь IP-адрес. IP-адрес каждого устройства уникален. Один и тот же адрес нельзя использовать дважды. Чтобы назначить IP-адрес плате удаленного управления CyberPower, необходимо определить диапазон доступных IP-адресов, а затем выбрать неиспользуемый IP-адрес для назначения плате удаленного управления.

Примечание: Для получения доступного IP-адрес может потребоваться помощь сетевого администратора.

Процедуры поиска IP-адреса:

1. Определение подсети платы удаленного управления CyberPower.

Одним из способов определения диапазона возможных IP-адресов является просмотр конфигурации сети на рабочей станции. Нажмите [Start] и выберите [Run]. В открывшемся поле введите с клавиатуры «command» и нажмите [OK]. В командной строке введите «**ipconfig/all**» и нажмите [Enter]. Компьютер отобразит сетевые настройки, как показано ниже:

```
Ethernet-адаптер
DNS-суффикс конкретного подключения .....: xxxx.com
Описание.....: D-Link DE220 ISA PnP LAN-адаптер
Физический адрес .....: 00-80-C8-DA-7A-C0
DHCP включен.....: Да
Автоконфигурация включена.....: Да
IP-адрес.....: 192.168.20.102
Маска подсети .....: 255.255.255.0
Шлюз по умолчанию .....: 192.168.20.1
DHCP-сервер.....: 192.168.20.1
DNS-серверы.....: 211.20.71.202
                  168.95.1.1
```

2. Выбор IP-адреса платы удаленного управления CyberPower

Убедитесь, что IP-адреса компьютера и платы удаленного управления принадлежат одной подсети. Согласно приведенным выше сетевым параметрам IP-адрес платы удаленного управления может быть 192.168.20.* (* - далее обозначает любое число от 1 до 255). Аналогично, если маска подсети 255.255.0.0, для доступа платы удаленного управления к той же подсети, что и компьютер, плате может быть назначен IP-адрес 192.168.*.*.

Для проверки отсутствия иного сетевого оборудования с таким же IP-адресом, запустите в диалоговом окне режима DOS команду «Ping 192.168.20.240», если назначаемым IP-адресом является 192.168.20.240. Если ответ на команду поступит в представленном ниже виде, скорее всего, IP-адрес не используется и может быть назначен плате удаленного управления CyberPower.

Pinging 192.168.20.240 with 32 bytes of data:

Request timed out (Превышен интервал ожидания для запроса)

Request timed out.

Request timed out.

Request timed out.

Если поступит ответ на команду поступит, как показано ниже, IP-адрес уже используется. Попробуйте поискать другой IP-адрес, пока не найдете доступный адрес.

Pinging 192.168.20.240 with 32 bytes of data:

Reply from 192.168.20.240: bytes=32 time<10ms TTL=64

(Ответ от 192.168.20.240: байты=32, время<10 мс TTL = 64)

Reply from 192.168.20.240: bytes=32 time<10ms TTL=64

Reply from 192.168.20.240: bytes=32 time<10ms TTL=64

Reply from 192.168.20.240: bytes=32 time<10ms TTL=64

Приложение 2: Конфигурирование учетной записи пользователя RMCARD на серверах аутентификации

RADIUS-сервер

1. Добавьте новый атрибут в словарь протокола RADIUS - Cyber vendor:
3808 – вендор
2. Добавьте два новых специфических атрибута к понятию «вендор» в интерфейсе RADIUS-сервера:
 - (1) **Cyber-Service-Type** (переменная целочисленного типа)
Атрибут Cyber-Service-Type может принимать три значения целочисленных параметров:
1 – Administrator (Администратор)
2 – Viewer (Просмотрщик)
3 – Outlet User (Пользователь розетки)
 - (2) **Cyber-Outlets** (строковая переменная)
Атрибут Cyber-Outlets может принимать значение строки, описывающей номера розеток. Этот атрибут позволит пользователю розетки получить доступ и управление назначенными розеткам. Например, назначение Cyber-Outlets = «1,2,5» позволяет пользователю управлять розетками 1, 2 и 5.

Примеры атрибутов из файла словаря:

VENDOR(ВЕНДОР)	Cyber	3808	
BEGIN-VENDOR (НАЧАЛО-ВЕНДОР)	Cyber		
ATTRIBUTE (атрибут)	Cyber-Service-Type	1	целочисленная переменная
ATTRIBUTE (атрибут)	Cyber-Outlet	2	строка
VALUE (значение)	Cyber-Service-Type	Администратор	1
VALUE (значение)	Cyber-Service-Type	Просмотрщик	2
VALUE (значение)	Cyber-Service-Type	Розетка	3
END-VENDOR (КОНЕЦ-ВЕНДОР)	Cyber		

LDAP-сервер и Active Directory (AD) в Windows-сервере

Для указания типа учетной записи пользователя и аутентификации в интерфейсе OpenLDAP-протокола или Windows AD добавьте к описанию один из следующих атрибутов:

1. **cyber_admin** (Администратор)
2. **cyber_viewer** (Просмотрщик)
3. **cyber_outlet="string"** (Пользователь розетки)

Введенная в атрибут «cyber_outlet» строка символов указывает, к каким точкам пользователь розетки может получить доступ и управление. Например, запись **cyber_outlet="1,2,5"** позволяет пользователю управлять розетками 1, 2 и 5.

Приложение 3: Обновление встроенного ПО ИБП

Номер версии встроенного ПО можно проверить на вкладке **[UPS->Information]** в веб-интерфейсе пользователя платы RMCARD.

Способ 1: С помощью веб-интерфейса

1. Выключите ИБП последовательным выбором опций [UPS->Master Switch].
2. Перейдите на вкладку версии встроенного ПО, последовательно выбирая опции [UPS->Information->Firmware Version].
3. Загрузите встроенное ПО ИБП, последовательно нажав опции «Update» (Обновить), а затем «Choose File» (Выбрать файл), для выбора файла встроенного ПО ИБП.
4. Чтобы применить обновление, выберите опцию «Submit». После завершения обновления появится окно с сообщением об успешном обновлении.
5. Включите ИБП, последовательно выбирая опции [UPS->Master Switch].

Способ 2: При помощи команды FTP

Перед попыткой обновления встроенного ПО необходимо включить службу FTP. Для обновления встроенного ПО через FTP выполните следующие действия:

1. Выключите ИБП.
2. Загрузите файл обновления в папку «C:\»
3. Откройте окно ввода команды
4. Войдите в систему платы удаленного управления CyberPower с помощью FTP-команды, введите с клавиатуры в командной строке:
 - (1) ftp
 - (2) ftp > open
 - (3) To [текущий IP-адрес платы RMCARD] [порт]; например: To 192.168.22.126 21
 - (4) Введите имя пользователя (USER NAME) и пароль (PASSWORD) (такие же, как в учетной записи администратора в веб-интерфейсе пользователя, информацию о заводских настройках по умолчанию см. на стр. 6)
5. Загрузите файл, введите с клавиатуры:


```
ftp > bin
ftp > put XXX.bin
```
6. Теперь загрузка завершена, введите с клавиатуры:


```
ftp > quit
```
7. Включите ИБП.

Примечание: 1. Обновление может занять ок. 5 мин. Не выполняйте никаких других действий и не извлекайте плату RMCARD в процессе обновления встроенного ПО ИБП.

Примечание: 2. Ход обновления может отображаться только в веб-интерфейсе.

Примечание: 3. При появлении сообщения «Uploaded an invalid UPS firmware» (Загружена недопустимая прошивка ИБП) после загрузки файла встроенного ПО ИБП через веб-интерфейс, проверьте:

- (1) Имеет ли этот файл встроенного ПО ИБП двоичный формат.
- (2) Поддерживает ли файл встроенного ПО имеющуюся модель ИБП.

Приложение 4: Программная поддержка

Программное обеспечение PowerPanel® Business Remote используется для плавного завершения работы операционной системы, если она защищена блоком распределения питания ИБП / устройством автоматического включения резерва (АВР) с установленной платой удаленного управления. ПО PowerPanel® Business доступно на официальном сайте компании CyberPower Systems. Для бесплатной загрузки ПО зайдите на сайт www.CyberPower.com и перейдите в раздел программного обеспечения.

Применение ПО PowerPanel® Business Remote

Требуется аутентификация платы удаленного управления при помощи ПО PowerPanel® Business Remote путем проверки секретной фразы (см. на рисунок 11).

Примечание: Секретная фраза по умолчанию – «powerpanel.encryption.key».

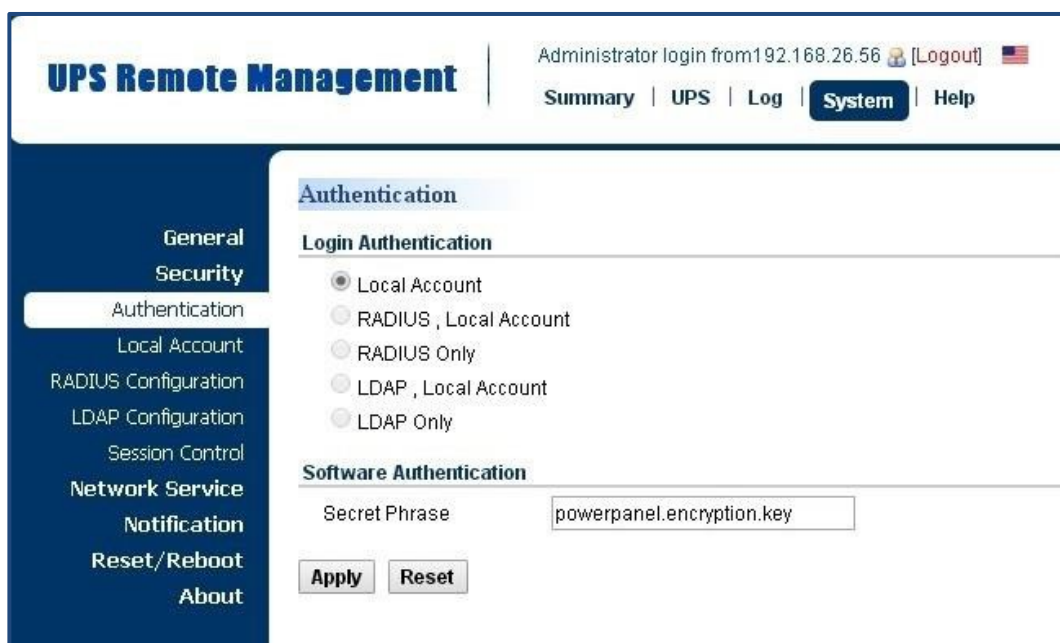


Рисунок 11. Последовательный выбор вкладок «RMCARD System > Authentication» пользовательского интерфейса веб-приложения



Примечание: ПО PowerPanel® Business поддерживает корректное завершение работы хостов VMware ESX/ESXi, а также других платформ виртуализации, как например, Microsoft Hyper-V и Citrix, в автоматическом режиме.

Настройка IP-адреса в операционной системе Linux

Приведенные в разделе «Настройка IP-адреса для платы удаленного управления CyberPower» инструкции предназначены для ОС Windows. В операционной системе Linux используйте ПО PowerPanel® Business Remote для сканирования и получения IP-адреса. Для этого в веб-интерфейсе ПО PowerPanel® Business Remote перейдите в раздел [Power-> Configuration], как показано на рисунке 12. Дополнительная информация приведена в Руководстве пользователя ПО PowerPanel® Business.

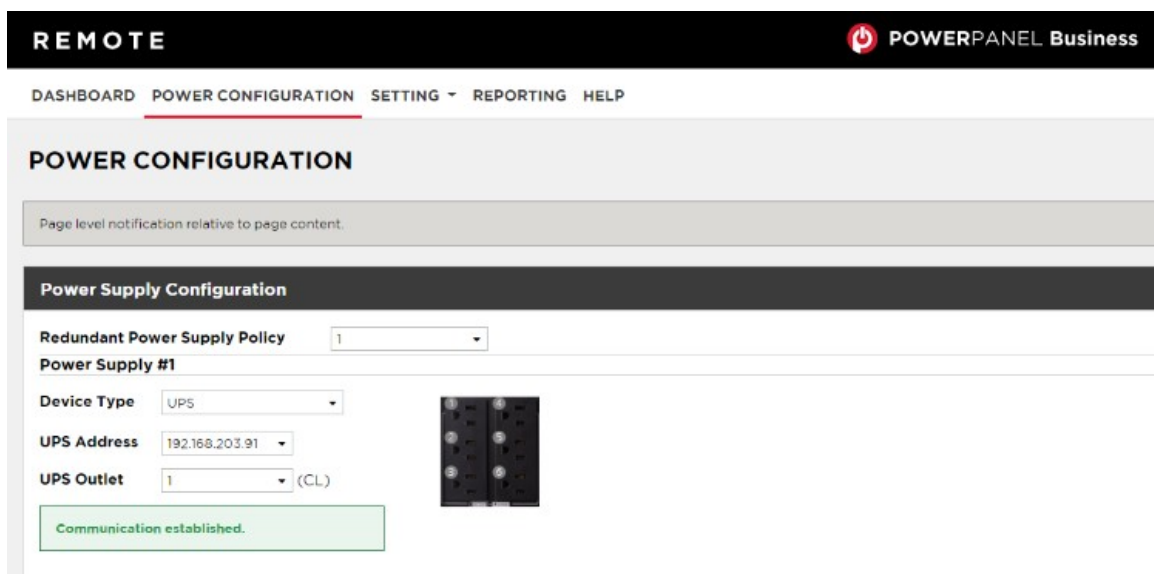
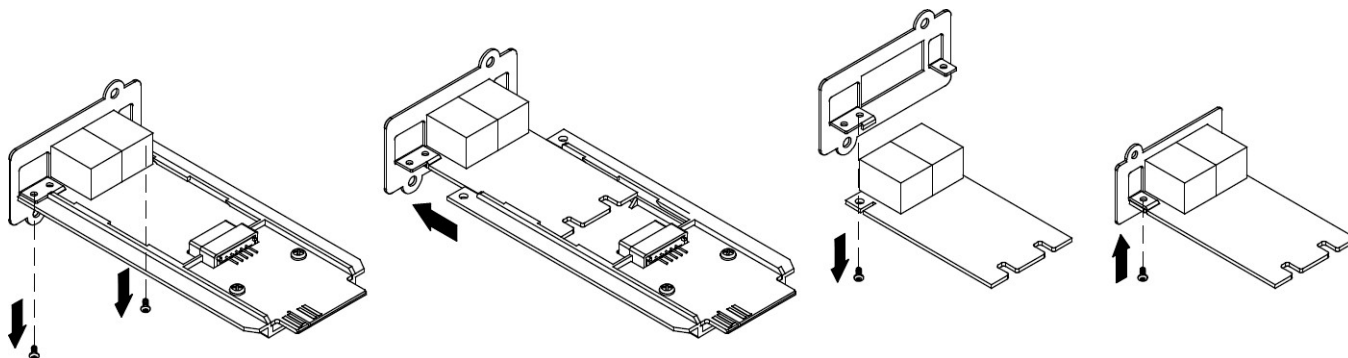


Рисунок 12. Веб-интерфейсе ПО PowerPanel® Business Remote

Приложение 5: Руководство по применению адаптера RMCARD

Для замены RMCARD305 на RMCARD205 извлеките адаптер



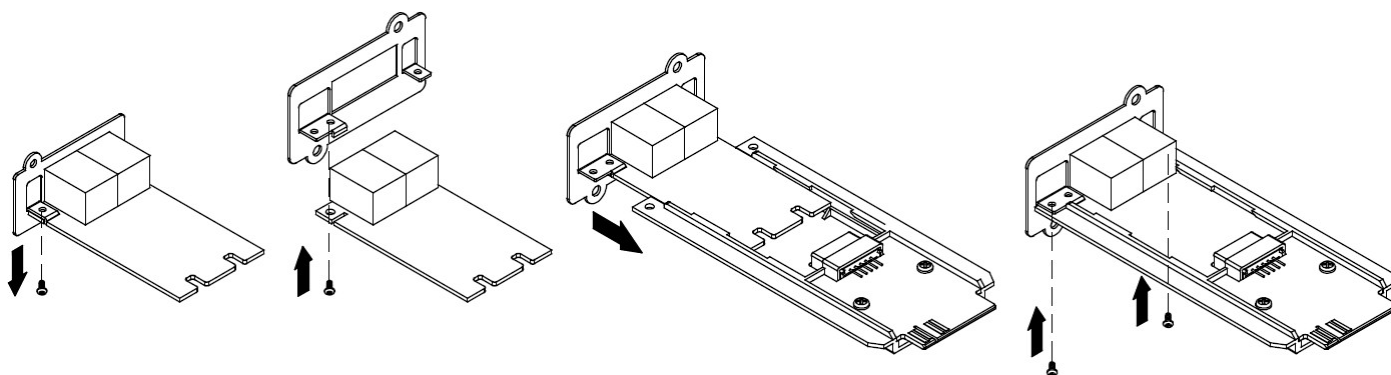
Шаг 1. Выкрутите из адаптера два винта, фиксирующие плату

Шаг 2. Извлеките из адаптера плату

Шаг 3. Выкрутите винт, прикрепляющий переднюю панель к плате RMCARD305

Шаг 4. Присоедините к плате переднюю панель RMCARD205.

Добавление адаптера для преобразования RMCARD205 в RMCARD305



Шаг 1. Выкрутите винт, прикрепляющий переднюю панель к плате, и снимите переднюю панель RMCARD205.

Шаг 2. Прикрутите переднюю панель RMCARD305 к плате.

Шаг 3. Вставьте плату адаптера. Убедитесь, что плата надежно зафиксирована на своем месте

Шаг 4. Закрепите плату двумя винтами

Примечание: Для получения информации для заказа или технической поддержки обратитесь с компанией CyberPower.

Примечание: Плата RMCARD205 рассчитана на порт расширения 43x18 мм (1,69x0,71 дюйма) для SNMP-соединения для CyberPower ИБП серии PR, OR и 1-3 кВА OL и блока распределения питания (PDU) с автоматическим включателем резерва (ABP).

Плата RMCARD305 рассчитана на порт расширения 57x23 мм (2,24x0,91 дюйма) для SNMP-соединения для ИБП CyberPower серии OL6-10 кВА.



CyberPower

CyberPower Systems, Inc.

www.cyberpowersystems.com

Для США и Канады:

4241 12 Авеню Ист, офис 400

г. Шакопи, шт. Миннесота 55379

Бесплатный вызов: (877) 297-6937

Для других регионов:

Контактная информация указана на веб-сайте компании.

