

Руководстве пользователя

Плата сетевого управления ИБП 2

**AP9630, AP9631,
AP9335T, AP9335TH, AP9810**



在公司的网站上 (www.apc.com) 有本手册的中文版。

This manual is available in English on the Web site (www.apc.com).

Dieses Handbuch ist in Deutsch auf der Webseite (www.apc.com) verfügbar.

Este manual está disponible en español en la página web (www.apc.com).

Ce manuel est disponible en français sur le site internet (www.apc.com).

Questo manuale è disponibile in italiano sul sito web (www.apc.com).

Este manual está disponível em português no site (www.apc.com).

Данное руководство на русском языке доступно на сайте (www.apc.com)

Deze handleiding is beschikbaar in het Nederlands op de Website (www.apc.com).

本マニュアル<各国の言語に対応する>はウェブサイト (www.apc.com) からダウンロードできます。

웹사이트 (www.apc.com) 에 한국어 매뉴얼 있습니다 .

This manual is available in English on the enclosed CD.

Dieses Handbuch ist in Deutsch auf der beiliegenden CD-ROM verfügbar.

Este manual está disponible en español en el CD-ROM adjunto.

Ce manuel est disponible en français sur le CD-ROM ci-inclus.

Questo manuale è disponibile in italiano nel CD-ROM allegato.

Este manual está disponível em português no CD fornecido.

Данное руководство на русском языке имеется на прилагаемом компакт-диске.

Deze handleiding staat in het Nederlands op de bijgevoegde cd.

本マニュアルの日本語版は同梱の CD-ROM からご覧になれます。

동봉된 CD 안에 한국어 매뉴얼이 있습니다 .

您可以从包含的 CD 上获得本手册的中文版本。

Введение

Описание устройства

Функции

Две платы сетевого управления Schneider Electric, рассматриваемые ниже, являются продуктами на базе интернет-технологий, имеют сертификат IPv6 Ready и обеспечивают управление устройствами на основе ряда стандартов, включая:



- Протокол передачи гипертекста (HTTP) - Безопасный командный процессор (SSH)
- Простой протокол сетевого управления, - Протокол передачи гипертекста на уровне версии 1 и 3 (SNMPv1, SNMPv3) защищенных сокетов (HTTPS)
- Протокол передачи файлов (FTP) - Secure CoPy (SCP)
- Telnet

Плата сетевого управления **AP9630**:

- Обеспечивает управление ИБП и функции планирования самодиагностики
- Обеспечивает регистрацию данных и журналы событий
- Обеспечивает поддержку утилиты ИБП PowerChute® Network Shutdown
- При поддержке сервера используется протокол динамической конфигурации хост-узла (DHCP) или протокол начальной загрузки (BOOTP), чтобы передать сетевые значения (TCP/IP) на плату управления
- Поддерживает работу со службой удаленного мониторинга (RMS)
- Позволяет сконфигурировать сообщение с использованием регистрации события (платой управления и с помощью системного журнала), электронной почты и SNMP-ловушки. На основании уровня опасности или категории событий можно сконфигурировать сообщение для отдельных событий или для групп событий
- Обеспечивает возможность экспорта пользовательского файла конфигурации (.ini) с настроенной платы на одну или более ненастроенных плат без преобразования файла в двоичный файл
- Обеспечивает выбор протоколов системы защиты для аутентификации или шифрования
- Обеспечивает связь с помощью InfraStruXure® Central или InfraStruXure Manager

Плата сетевого управления **AP9631** включает в себя все функции платы сетевого управления AP9630, а также перечисленные ниже возможности:

- Наличие двух USB-портов.
- Поддержку двух универсальных портов ввода-вывода, к которым можно подключить следующие устройства:
 - датчики температуры или температуры/влажности
 - разъемы релейного ввода вывода для двух контактов на входе и одного выходного реле

Устройства, в которых можно устанавливать плату управления. Плату управления можно устанавливать в следующих устройствах:

- Любая модель Smart-UPS[®], в которой предусмотрен внутренний слот расширения, или любой ИБП Symmetra[®], за исключением ИБП Symmetra PX 250 и Symmetra PX 500
- Блок расширения (AP9600)
- Тройной блок расширения (AP9604)

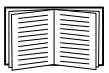
Исходная настройка IPv4

Перед началом работы в сети необходимо задать два параметра TCP/IP для платы управления:

- IP-адрес платы сетевого управления
- IP-адрес шлюза по умолчанию (требуется только в том случае, если вы выходите с сегмента)



Внимание: Не следует использовать шлейфовый адрес (127.0.0.1) в качестве адреса шлюза по умолчанию. Это повлечет за собой отключение платы. В этом случае нужно войти в систему с помощью последовательного интерфейса и установить параметры TCP/IP на значения по умолчанию.



Конфигурация параметров настройки TCP/IP приводится в *Руководстве по установке* платы сетевого управления, которое имеется на компакт диске *Utility* для платы сетевого управления и в печатном виде.

Подробные сведения об использовании сервера DHCP для настройки параметров TCP/IP на плате управления см. в «Настройки TCP/IP линии связи» на стр. 71.

Исходная настройка IPv6

Конфигурация сети IPv6 обеспечивает универсальные возможности для выполнения требований пользователя. Настройка параметров TCP/IP для IPv6 приводится в *Руководстве по установке* платы сетевого управления, которое имеется на компакт- диске для платы сетевого управления в формате PDF и на веб-сайте www.apc.com.

Функции сетевого управления

Эти приложения и утилиты работают с ИБП, который подключается к сети через плату управления.

- PowerChute Network Shutdown—обеспечивается автоматическое корректное отключение компьютеров, подключенных к ИБП устройств
- PowerNet[®] Management Information Base (MIB) со стандартным браузером MIB—выполняются запросы SET и GET протокола SNMP и используются SNMP-ловушки
- InfraStruXure Central—обеспечивается управление электропитанием на предметном уровне и управление агентами, ИБП и устройствами контроля окружения
- Device IP Configuration Wizard—настройка основных параметров одной или более плат управления в сети
- Security Wizard—создание компонентов, необходимых для обеспечения высокой степени защиты платы управления при использовании протокола защищенных сокетов (SSL), соответствующих протоколов и программ шифрования.

Функции внутреннего управления

Обзор

Используйте веб-интерфейс или интерфейс командной строки для просмотра состояния ИБП, управления ИБП и платы управления. Можно также использовать протокол SNMP для контроля состояния ИБП.



Более подробные сведения о внутренних интерфейсах пользователя приведены в «Веб-интерфейс» на стр. 31 и «Интерфейс командной строки» на стр. 8. См. «SNMP» на стр. 80 с описанием того, как с помощью протокола SNMP осуществляется доступ к плате управления.

Приоритетный доступ для входа

На плату управления одновременно может зайти только один пользователь. Предусмотрен следующий приоритет доступа, начиная с максимального:

- Локальный доступ с интерфейса командной строки интерфейса с помощью последовательного подключения к плате управления по последовательному каналу связи
- Доступ Telnet или SSH к интерфейсу командной строки с удаленного компьютера
- Интернет-доступ, прямой или косвенный через InfraStruXure Central



Примечание: Протокол SNMP предусматривает доступ **Запись+** и **Запись**. **Запись+** имеет максимальный приоритет и обеспечивает вход даже в том случае, если к плате уже обратился другой пользователь. Доступ **Запись** эквивалентен Интернет-доступу.

Типы учетных записей

Плата управления имеет три уровня доступа (администратор, устройство и только для чтения), которые защищены именем пользователя и паролем.

- Пользователь с доступом «администратор» может использовать все меню веб-интерфейса и все команды в интерфейсе командной строки. Имя пользователя и пароль по умолчанию задаются как **arc**.
- Пользователь с доступом «устройство» имеет доступ только к перечисленным ниже позициям.
 - В веб-интерфейсе: меню на вкладке **ИБП**, а также журналы событий и данных, доступ к которым осуществляется через заголовки **События** и **Данные** на левой панели управления меню на вкладке **Журналы**. При отображении журналов событий и данных кнопка для стирания журнала не предусматривается.
 - В интерфейсе командной строки: к эквивалентным функциям и опциям.
Имя устройства по умолчанию - **device**, пароль по умолчанию **arc**.
- Пользователь с доступом «только для чтения» имеет перечисленные ниже ограниченные возможности доступа.
 - Доступ только через веб-интерфейс.
 - Доступ к тем же вкладкам и меню, что и при доступе «устройство», но без возможности изменения конфигурации, устройств управления, удаления данных или использования опций передачи файлов. Связь с опциями конфигурации видна, но отключена. При отображении журналов событий и данных кнопка для стирания журнала не предусматривается.
Имя устройства по умолчанию - **readonly**, пароль по умолчанию **arc**.



Чтобы установить значения **Имя пользователя** и **Пароль** для трех типов учетных записей, см. «Настройка доступа пользователя» на стр. 67.

Восстановление утерянного пароля

Для доступа к интерфейсу командной строки можно использовать локальный компьютер, подключенный к последовательному порту на плате сетевого управления.

1. Выберите последовательный порт на локальном компьютере и отключите службу, которая использует этот порт.
2. Подсоедините прилагаемый кабель последовательного интерфейса (номер детали 940-0299) к выбранному порту компьютера и к порту настройки на плате управления.
3. Запустите на компьютере программу эмуляции терминала (например HyperTerminal®) и настройте следующие параметры для выбранного порта: скорость передачи 9600 бит/с, 8 бит данных, без проверки четности, 1 стоповый бит, без контроля потока.
4. Нажмите клавишу ENTER при необходимости несколько раз для отображения запроса на ввод параметра **Имя пользователя**. Если вы не можете отобразить **Имя пользователя**, убедитесь в том, что:
 - Последовательный порт не используется другим приложением.
 - Параметры терминала соответствуют параметрам, указанным в операции 3.
 - Соответствующий кабель используется, как указано в операции 2.
5. Нажмите клавишу **Reset**. Индикатор состояния начнет поочередно мигать оранжевым и зеленым цветом. Нажмите клавишу **Reset** еще раз, пока мигает индикатор, для временного возврата значений по умолчанию имени пользователя и пароля.
6. Нажмите несколько раз клавишу ENTER для повторного отображения запроса **Имя пользователя**, затем укажите значение **арс**, для имени пользователя и пароля. (Если после повторного отображения запроса на ввод параметра **Имя пользователя** процедура входа занимает более 30 секунд, необходимо повторить операцию 5 и процедуру входа.)
7. В интерфейсе командной строки используйте следующие команды для изменения параметров **Имя пользователя** и **Пароль**, заменив значение **арс**:

```
user -an имя_администратора
```

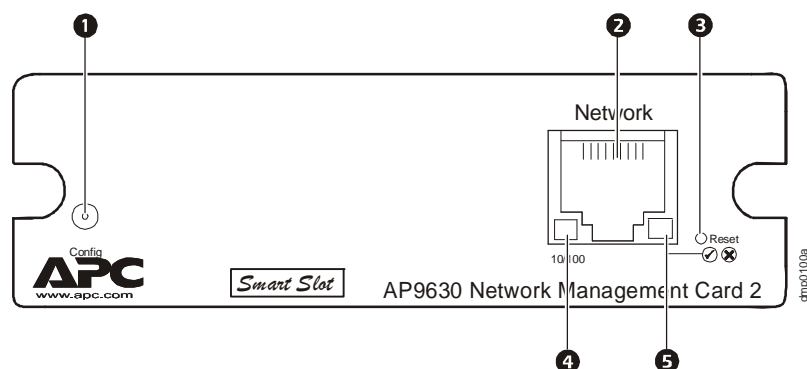
```
user -ар пароль_администратора
```

Например, чтобы изменить имя Administrator на **Admin**, введите:

```
user -an Admin
```

8. Для выхода из системы введите `quit` или `exit`, подключите ранее отсоединенный кабель последовательного интерфейса и повторно запустите отключенную службу.

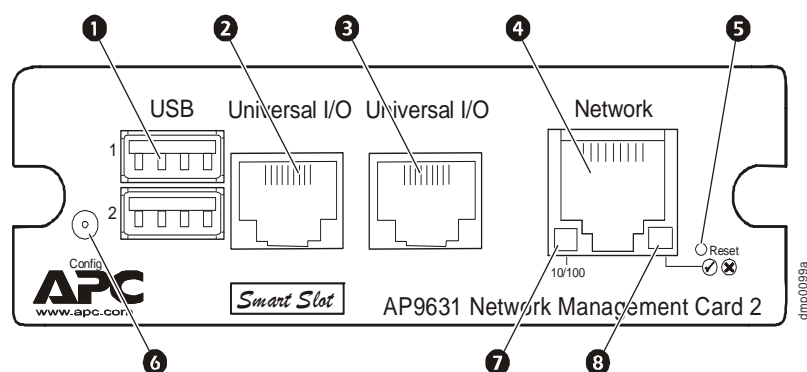
Передняя панель (AP9630)



Функции

	Элемент	Описание
❶	Последовательный конфигурационный порт	Подсоединяет плату управления к локальному компьютеру для настройки исходных параметров сети или для доступа к интерфейсу командной строки.
❷	Разъем 10/100 Base-T	Подсоединяет плату управления к сети Ethernet.
❸	Кнопка сброса	Сброс значений платы управления при включенном питании.
❹	Индикатор активности сети Link – RX/TX (10/100)	См. «Индикатор активности сети Link – RX/TX (10/100)» на стр. 7.
❺	Индикатор состояния	См. «Индикатор состояния» на стр. 6.

Передняя панель (AP9631)



Характеристики

	Элемент	Описание
❶	Порты USB	Зарезервировано для использования.

	Элемент	Описание
2 3	Порты датчиков	Подключаются к датчикам температуры, датчикам температуры/влажности, к разъемам входных-выходных реле, которые подключают два входных контакта и одно выходное реле.
4	Разъем 10/100 Base-T	Подсоединяет плату управления к сети Ethernet.
5	Кнопка сброса	Сброс значений платы управления при включенном питании.
6	Последовательный конфигурационный порт	Подсоединяет плату управления к локальному компьютеру для настройки исходных параметров сети или для доступа к интерфейсу командной строки.
7	Индикатор активности сети Link – RX/TX (10/100)	См. «Индикатор активности сети Link – RX/TX (10/100)» на стр. 7.
8	Индикатор состояния	См. «Индикатор состояния» на стр. 6.

Описание индикаторов состояния

Индикатор состояния

Этот светодиодный индикатор указывает состояние платы управления.

Состояние	Описание
Выкл.	Возможна одна из следующих ситуаций: <ul style="list-style-type: none"> • На плату управления не подается входное питание. • Плата управления работает неправильно. Вероятно, требуется ремонт или замена. Обратитесь в сервисный центр. См. «Всемирная сервисная служба» на стр. 3.
Непрерывный зеленый	Параметры TCP/IP в плате управления заданы правильно.
Непрерывный оранжевый	В плате управления обнаружен аппаратный сбой. Обратитесь в сервисный центр. См. «Всемирная сервисная служба» на стр. 3.
Мигающий зеленый	В плате управления неправильно заданы параметры TCP/IP. ¹
Мигающий оранжевый	Плата управления выполняет запросы BOOTP. ¹
Попеременно мигающий зеленый и оранжевый	Если светодиод мигает с низкой частотой, то плата управления выполняет запросы DHCP. ^{2, 1} Если светодиод мигает часто, то выполняется запуск платы управления.
<p>1. Если сервер BOOTP или DHCP не используется, см. описание настройки параметров TCP/IP платы управления в <i>Руководстве по установке</i> платы сетевого управления в печатном виде и на компакт-диске <i>Utility</i> для платы сетевого управления в формате PDF.</p> <p>2. Об использовании сервера DHCP см. «Настройки TCP/IP линии связи» на стр. 71.</p>	

Индикатор активности сети Link – RX/TX (10/100)

Этот светодиодный индикатор указывает состояние сети в плате управления.

Состояние	Описание
Выкл.	Возможна одна из следующих ситуаций: <ul style="list-style-type: none">• На плату управления не подается входное питание.• Отключен или неисправен кабель, соединяющий плату управления с сетью.• Отключено или неправильно работает устройство, соединяющее плату управления с сетью.• Неправильно работает сама плата управления. Вероятно, требуется ремонт или замена. Обратитесь в сервисный центр. См. «Всемирная сервисная служба» на стр. 3.
Непрерывный зеленый	Плата управления подключена к сети, которая работает со скоростью передачи 10 мегабит в секунду (Мб/с).
Непрерывный оранжевый	Плата управления подключена к сети, которая работает со скоростью передачи 100 мегабит в секунду (Мб/с).
Мигающий зеленый	Плата управления принимает или передает пакеты данных со скоростью передачи 10 Мб/с.
Мигающий оранжевый	Плата управления принимает или передает пакеты данных со скоростью передачи 100 Мб/с.

Функции безопасности

Обзор

Для обнаружения внутренних неисправностей и восстановления рабочего состояния после воздействия непредусмотренных входных сигналов в плате управления используется внутренний общесистемный механизм защиты. При перезапуске после внутреннего сбоя в журнал регистрации событий записывается **Система: Горячий старт**.

Механизм защиты интерфейса сети

Плата управления использует средства защиты, чтобы обезопасить себя от ситуации, когда доступ к сети невозможен. Например, если плата управления не получает из сети трафика в течение 9,5 минут (прямого трафика типа SNMP или широкополосного наподобие запроса протокола разрешения адресов [ARP]), то считается, что сбой произошел внутри интерфейса сети, и происходит перезапуск.

Сброс таймера сети

Чтобы плата управления не перезапускалась при простое в течение 9,5 минут, она пытается обратиться к шлюзу по умолчанию каждые 4,5 минуты. При наличии шлюза он отвечает плате управления, и этот ответный сигнал перезапускает таймер на 9,5 минут. Если для вашего приложения шлюз не требуется или отсутствует, укажите IP-адрес компьютера, работающего в сети и находящегося в той же подсети. Сетевой трафик этого компьютера будет перезапускать таймер на 9,5 минут достаточно часто, чтобы блокировать перезапуск платы управления.

Интерфейс командной строки

Вход в систему

Обзор

Для доступа к интерфейсу командной строки можно использовать локальное подключение (по последовательному каналу связи) или удаленное (Telnet или SSH) подключение с помощью компьютера, находящегося в той же сети, что и плата сетевого управления (ПСУ).

Используйте для входа в систему зависящее от регистра имя пользователя и пароль (по умолчанию для учетной записи администратора используются значения **apc** и **apc** или **device** и **apc** для учетной записи пользователя устройства). Пользователь только для чтения не имеет доступа к интерфейсу командной строки.



Если Вы не помните имя пользователя или пароль, см. «Восстановление утерянного пароля» на стр. 4.

Удаленный доступ к интерфейсу командной строки

Доступ к интерфейсу командной строки можно выполнять с помощью протокола Telnet или SSH. По умолчанию используется протокол Telnet. При включении SSH автоматически отключается Telnet.

Для включения и отключения этих способов доступа используйте веб-интерфейс. Выберите вкладку **Администрирование** и параметр **Сеть** в верхней части строки меню, а затем параметр **доступ** в области **Консоль** в левом меню навигации.

Протокол Telnet для стандартного доступа. Программа Telnet обеспечивает стандартную аутентификацию по имени пользователя и паролю, однако не имеет преимуществ шифрования, обеспечивающих высокий уровень защиты.

Использование Telnet для доступа к интерфейсу командной строки:

1. На компьютере, который имеет доступ к сети с установленной ПСУ, при приглашении к вводу команды наберите `telnet` и IP-адрес ПСУ (например, `telnet 139.225.6.133`, если ПСУ использует по умолчанию порт Telnet 23), и нажмите ENTER.

Если ПСУ использует номер порта не по умолчанию (от 5000 до 32768), то в зависимости от клиента Telnet необходимо использовать двоеточие или пробел между IP-адресом (или именем DNS) и именем порта. (Эти команды относятся к общему случаю: некоторые клиенты не позволяют указывать порт в качестве аргумента, и для некоторых типов Linux могут потребоваться дополнительные команды).

2. Введите имя пользователя и пароль (по умолчанию для учетной записи администратора используются значения **apc** и **apc**, а для учетной записи пользователя устройства — **device** и **apc**).

Протокол SSH для доступа с высоким уровнем защиты. Если для обеспечения надежной защиты веб-интерфейса используется SSL, для доступа к интерфейсу командной строки нужно использовать протокол SSH. Протокол SSH выполняет шифрование имен пользователей, паролей и передаваемых данных. Вне зависимости от способа доступа к интерфейсу командной строки (SSH или Telnet) интерфейс, учетные записи пользователей и права доступа пользователей остаются неизменными. Однако, чтобы пользоваться SSH, необходимо сначала выполнить настройку и установить на компьютере клиентскую программу SSH.

Локальный доступ к интерфейсу командной строки

Для локального доступа к интерфейсу командной строки можно использовать компьютер, подключенный к последовательному порту на плате сетевого управления.

1. Выберите последовательный порт на компьютере и отключите все службы, использующие этот порт.
2. С помощью последовательного кабеля (номер детали: 940-0299) подключите выбранный порт компьютера к порту настройки на ПСУ.
3. Запустите программу терминала (например, HyperTerminal), и установите следующие параметры для выбранного порта: скорость передачи 9600 бит/с, 8 бит данных, без проверки четности, 1 стоповый бит и без контроля потока.
4. Нажмите клавишу ENTER. При появлении запроса введите имя пользователя и пароль.

Основной экран

Пример основного экрана

Ниже приведен пример экрана, который отображается при входе в систему с помощью интерфейса командной строки на плате сетевого управления (ПСУ).

```
American Power Conversion          Network Management Card AOS  vx.x.x
(c) Copyright 2010 All Rights Reserved Symmetra APP                      vx.x.x
-----
Name      : Test Lab                               Date : 10/30/2010
Contact   : Don Adams                             Time  : 5:58:30
Location  : Building 3                            User  : Administrator
Up Time   : 0 Days, 21 Hours, 21 Minutes          Stat  : P+ N+ A+

APC>
```

Поля информации и состояния

Информационные поля основного экрана.

- Два поля идентифицируют версии операционной системы American Power Conversion (AOS) и версии прошивки приложения (APP). Название прошивки приложения определяет устройство, которое подключается к сети с помощью ПСУ. В приведенном выше примере ПСУ использует прошивку приложения для ИБП Symmetra.

```
Network Management Card AOS    vx.x.x
Symmetra APP                   vx.x.x
```

- Три поля идентифицируют название системы, контактное лицо и местоположение ПСУ. (Для установки этих значений в веб-интерфейсе выберите вкладку **Администрирование, Общие** в верхней строке меню и **Идентификация** в левой панели меню управления.)

```
Name    : Test Lab
Contact : Don Adams
Location: Building 3
```

- В поле **Время работы** указывается продолжительность работы ПСУ после последнего запуска или сброса.

```
Up Time: 0 Days 21 Hours 21 Minutes
```

- В двух полях указывается дата и время входа в систему.

```
Date : 10/30/2009
Time : 5:58:30
```

- В поле **Пользователь** указывается способ входа в систему — с использованием учетной записи **Администратор** или **Диспетчер устройств**. (Учетная запись **Пользователь с правами только для чтения** не обеспечивает доступ к интерфейсу командной строки.) При входе в систему в качестве диспетчера устройств (эквивалент пользователя устройства в веб-интерфейсе) у Вас есть доступ к журналу событий, возможности настройки некоторых параметров ИБП и просмотра ряда активных аварийных сигналов.

```
User : Administrator
```

Поля состояния на основном экране.

- Поле **Состояние** указывает на состояние ПСУ. Среднее состояние меняется в зависимости от работы выбранного Вами протокола IPv4, IPv6 или обоих, как указано во второй таблице ниже.

```
Stat : P+ N+ A+
```

P+	Операционная система (AOS) работает нормально.
----	--

Толь-ко IPv4	Толь-ко IPv6	IPv4 и IPv6*	Описание
N+	N6+	N4+ N6+	Сеть работает нормально.
N?	N6?	N4? N6?	Выполняется цикл запроса BOOTP.
N-	N6-	N4- N6-	Сбой ПСУ при подключении к сети.
N!	N6!	N4! N6!	Другое устройство использует IP-адрес ПСУ.
* Значения N4 и N6 могут отличаться. У Вас может быть, например N4- N6+.			

A+	Приложение работает нормально.
A-	Приложение дает неверную контрольную сумму.
A?	Происходит инициализация приложения.
A!	Приложение несовместимо с операционной системой AOS.



Если P+ не отображается, обратитесь в отдел поддержки клиентов. См. «Всемирная сервисная служба» на стр. 3.



Примечание. Для просмотра состояния ИБП наберите `ups -st`.

Использование интерфейса командной строки

Обзор

Интерфейс командной строки предусматривает параметры настройки параметров сети и управления ИБП и его платой сетевого управления (ПСУ).

Ввод команд

В интерфейсе командной строки используйте команды для настройки ПСУ. Для выдачи команды наберите команду и нажмите клавишу ENTER. Команды и аргументы можно вводить в нижнем, верхнем и смешанных регистрах. Параметры зависят от регистра.

При использовании интерфейса командной строки можно также выполнять следующие операции.

- Набрать ? и нажать ENTER, чтобы просмотреть список имеющихся команд на основании типа Вашей учетной записи.
 Для получения информации о назначении и синтаксисе указанной команды наберите команду, пробел и ? или слово help. Например, для просмотра параметра конфигурации RADIUS наберите:

```
radius ?
```

 или

```
radius help
```
- Нажмите клавишу со стрелкой ВВЕРХ для просмотра команды, которая была введена последней в этом сеансе. Используйте клавиши со стрелками ВВЕРХ и ВНИЗ для просмотра списка, в который может входить до десяти команд.
- Наберите по меньшей мере одну букву команды и нажмите клавишу TAB, чтобы просмотреть все команды, которые совпадают с текстом, набранным в командной строке.
- Наберите `ups -st` для просмотра состояния ИБП.
- Наберите `exit` или `quit`, чтобы отключить соединение с интерфейсом командной строки.

Синтаксис команды

Компонент	Описание
-	Параметрам предшествует дефис.
< >	Определения параметров указываются в угловых скобках. Например: -dp <device password>
[]	Если команда принимает различные параметры или параметр принимает взаимоисключающие аргументы, то значения могут указываться в квадратных скобках.
	Вертикальная линия между позициями в квадратных или угловых скобках указывает на взаимоисключающие позиции. Необходимо выбрать одну из позиций.

Примеры синтаксиса

Командная строка, которая поддерживает несколько параметров:

```
user [-an <admin name>] [-ap <admin password>]
```

В этом примере команда `user` получает параметр `-an`, которая определяет имя администратора, а параметр `-ap` определяет пароль администратора. Чтобы изменить имя администратора и пароль на XYZ, нужно выполнить следующие действия.

1. Наберите команду `user`, один параметр и аргумент XYZ:
`user -ap XYZ`
2. После успешного выполнения первой команды наберите команду `user`, второй параметр и аргумент XYZ:
`user -ap XYZ`

Команда, которая принимает для параметра взаимоисключающие аргументы:

```
alarmcount -p [all | warning | critical]
```

В этом примере параметр `-p` принимает только три аргумента: `all`, `warning` или `critical`. Например для просмотра ряда активных критичных аварийных сигналов наберите:
`alarmcount -p critical`

Команда не выполняется при наборе аргумента, который не задан.

Коды реакции на команду

Коды реакции на команду позволяют при выполнении заданных операций (скриптов) достаточно точно определять условия ошибки без необходимости точного совпадения с разбором текста сообщения об ошибке.

Интерфейс командной строки сообщает обо всех командных операциях в следующем формате:

E [0-9] [0-9] [0-9] : *Error message*

Код	Сообщение об ошибке
E000	Успешно
E001	Успешно задана
E002	Для ввода изменений требуется перезагрузка
E100	Сбой команды
E101	Команда не обнаружена
E102	Ошибка параметра
E103	Ошибка командной строки
E104	Отклонение уровня пользователя
E105	Предварительное заполнение команды
E106	Данные отсутствуют
E107	Потеряна последовательная связь с ИБП

Описание команд



Примечание. На различных устройствах ИБП могут быть доступны разные из указанных ниже команд и параметров.

?

Доступ. Администратор, пользователь устройства

Описание. Просмотр списка всех команд интерфейса командной строки для учетной записи Вашего типа. Для просмотра текста справки для конкретной команды наберите эту команду и поставьте после нее знак вопроса.

Пример. Для просмотра списка параметров, которые принимаются командой `alarmcount`, наберите:
`alarmcount ?`

about

Доступ. Администратор, пользователь устройства

Описание. Просмотр информации об аппаратно-программном обеспечении. Эта информация полезна при поиске неисправностей и позволяет определить наличие обновленной прошивки на веб-сайте.

alarmcount

Доступ. Администратор, пользователь устройства

Описание.

Параметр	Аргументы	Описание
-p	all	Просмотр ряда активных аварийных сигналов, о которых поступило сообщение с ПСУ. Информация об аварийных сигналах находится в журнале событий.
	warning	Просмотр ряда активных предупреждающих сигналов.
	critical	Просмотр ряда активных критических сигналов.

Пример. Для просмотра всех активных предупреждающих сигналов наберите:
alarmcount -p warning

boot

Доступ. Только администратор

Описание. Настройка того, как ПСУ будет получать свои сетевые параметры, включая IP-адрес, маску подсети и шлюз по умолчанию. После этого требуется настройка параметров сервера BOOTP или DHCP.

Параметр	Аргумент	Описание
-b <режим загрузки>	dhcp bootp manual	Определите, как будут настраиваться параметры TCP/IP при включении ПСУ, сбросах и перезапусках. См. «Настройки TCP/IP линии связи» на стр. 71 для получения сведений о каждой настройке режима загрузки.
-c	enable disable	Только для режимов загрузки dhcp. Включение или отключение требования выдачи сервером DHCP файла cookie APC.
Значения по умолчанию для этих трех настроек обычно менять не требуется: -v <класс поставщика>: APC -i <идентификатор клиента>: MAC-адрес ПСУ, который дает уникальную идентификацию этой платы в сети -u <класс пользователя>: Название модуля прошивки приложения		

Пример. Чтобы использовать сервер DHCP для получения сетевых параметров, выполните следующие операции.

1. Наберите `boot -b dhcp`
2. Включите требования к серверу DHCP о необходимости выдачи файла cookie APC.
`boot -c enable`

cd

Доступ. Администратор, пользователь устройства

Описание. Поиск папки в структуре каталога ПСУ.

Пример 1. Для изменения папки `ssh` и подтверждения того, что сертификат безопасности SSH был загружен в ПСУ, выполните следующие операции.

1. Наберите `cd ssh` и нажмите ENTER.
2. Наберите `dir` и нажмите ENTER для получения списка файлов, хранящихся в папке SSH.

Пример 2. Для возврата в папку главного каталога наберите:

```
cd ..
```

cfgshutdn

Доступ. Администратор, пользователь устройства

Описание. Настройка параметров выключения: это позволяет отобразить и настроить значения для задержки выключения ИБП, задержки возврата ИБП, продолжительности работы ИБП при низком заряде батареи, времени ИБП в спящем режиме и минимального времени автономной работы ИБП на выходе.



Примечание. Эти параметры доступны не на всех устройствах ИБП.

Параметр	Аргумент	Описание
-all		Отображение всех применимых параметров выключения для данного ИБП.
-sd	000 090 180 270 360 450 540 630	Установка задержки выключения в секундах.
-lo	02 05 08 11 14 17 20 23	Установка продолжительности работы при низком заряде батареи в минутах.
-rd	000 060 120 180 240 300 360 420	Установка задержки возврата ИБП в секундах, которая представляет собой время задержки перед повторным включением ИБП.
-rrt	0–3600	Установка минимального времени автономной работы на выходе в секундах, которое представляет собой время автономной работы батареи для поддержания нагрузки перед повторным включением ИБП.
-sl	0,0–359,9	Установка времени в спящем режиме в часах. Аргумент может принимать значение от 0,0 до 359,9.
-rsc	00 15 30 45 60 75 90	Установка минимального заряда батареи в виде процентного отношения к общей емкости.

cfgpower

Доступ. Администратор, пользователь устройства

Описание. Настройка параметров питания: это позволяет отобразить и настроить точки перехода, чувствительность и выходное напряжение.



Примечание. Эти параметры доступны не на всех устройствах ИБП.

Параметр	Аргумент На различных устройствах могут использоваться разные значения.	Описание
-all		Отображение всех применимых параметров питания для данного ИБП.
-l	97–106	Установка нижней точки перехода в вольтах переменного тока.
-h	127–136	Установка верхней точки перехода в вольтах переменного тока.
-ov	100 120 110	Установка выходного напряжения в вольтах переменного тока.
-s	Normal Reduced Low	Установка чувствительности с использованием одного из трех аргументов.
-bu	127 130 133 136 139 142 145 148	Установка верхнего напряжения байпаса в вольтах переменного тока; когда напряжение превышает это значение, устройство переходит в режим байпаса.
-bl	086 088 090 092 094 096 098 100	Установка нижнего напряжения байпаса в вольтах переменного тока; когда напряжение опускается ниже этого значения, устройство переходит в режим байпаса.

console

Доступ. Только администратор

Описание. Настройка того, могут ли пользователи иметь доступ к интерфейсу командной строки с помощью протокола Telnet, включаемого по умолчанию, или Secure SHell (SSH), обеспечивающего защиту за счет передачи имен пользователей, паролей и данных в зашифрованном виде. Для дополнительной безопасности можно изменить настройку порта Telnet или SSH. Или, наоборот, отключите сетевой доступ к интерфейсу командной строки.

Параметр	Аргумент	Описание
-S	disable telnet ssh	Настройте доступ к интерфейсу командной строки или используйте команду <code>disable</code> (выключить) для запрещения доступа. Включение SSH разрешает SCP и отключает Telnet.
-pt	<telnet порт n>	Определите порт Telnet, используемый для связи с ПСУ (по умолчанию 23).

Параметр	Аргумент	Описание
-ps	<SSH порт n>	Определите порт SSH, используемый для связи с ПСУ (по умолчанию 22).
-b	2400 9600 19200 38400	Настройте скорость передачи последовательного порта (по умолчанию 9600 бит/с).

Пример 1. Чтобы обеспечить доступ SSH к интерфейсу командной строки, наберите:

```
console -S ssh
```

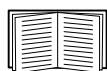
Пример 2. Чтобы изменить порт Telnet на 5000, наберите:

```
console -pt 5000
```

date

Доступ. Только администратор

Описание. Настройте дату, используемую в ПСУ.



Сведения о настройке сервера NTP на определение даты и времени для ПСУ см. в разделе «Задание даты и времени» на стр. 94.

Параметр	Аргумент	Описание
-d	<<строка_даты>>	Задайте текущую дату. Используйте формат данных, задаваемый командой <code>date -f</code> .
-t	<00:00:00>	Настройте текущее время в часах, минутах и секундах. Используйте 24-часовой формат времени.
-f	mm/dd/yy dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd	Выберите цифровой формат, в котором будут отображаться все даты данного пользовательского интерфейса. Каждая буква m (месяц), d (день) и y (год) представляет один разряд. Однозначные дни и месяцы отображаются с ведущим нулем (перед значащей цифрой).
-z	<сдвиг часового пояса>	Для указания Вашего часового пояса задается разница относительно времени по Гринвичу (GMT). Это дает возможность синхронизации с другими людьми в различных часовых поясах.

Пример 1. Для отображения даты в формате гггг-мм-дд наберите:

```
date -f yyyy-mm-dd
```

Пример 2. Чтобы указать дату 30 октября 2009 года в формате, указанном в предыдущем примере, наберите:

```
date -d "2009-10-30"
```

Пример 3. Чтобы задать время 17:21:03, наберите:

```
date -t 17:21:03
```

delete

Доступ. Только администратор

Описание. Удаление файла в файловой системе. (Сведения об удалении журнала событий см. в разделе «eventlog», начиная со стр. 19).

Аргумент	Описание
<имя файла>	Наберите название файла, предназначенного для удаления.

Пример. Чтобы удалить файл, выполните следующие действия:

1. Перейдите в папку, в которой находится нужный файл. Например, для перехода к папке журналов logs наберите:
`cd logs`
2. Для просмотра файлов в папке журналов logs наберите:
`dir`
3. Наберите
`delete <file name>.`

detstatus

Доступ. Администратор, пользователь устройства

Описание. Просмотр подробных сведений о состоянии ИБП. См. также описание параметра -st в разделе «ups» на стр. 26.

Параметр	Аргументы	Описание
-all		Отображение всех применимых сведений о состоянии для данного ИБП.
-rt		Оставшееся время автономной работы в часах и минутах.
-ss		Сводка состояния ИБП: работа от сети, от батарей и т. д.
-soc		Заряд батареи ИБП в виде процентного отношения к общей емкости.
-om		Измерения выходных характеристик: напряжение, частота, коэффициент мощности, процент ВА, ток.
-im		Измерения входных характеристик: напряжение и частота.
-bat		Напряжение батареи
-tmp		Внутренняя температура ИБП
-dg		Результаты диагностического тестирования: результат и дата самодиагностики, результат и дата калибровки.

dir

Доступ. Администратор, пользователь устройства

Описание. Просмотр файлов и папок, хранящихся на ПСУ.

dns

Доступ. Администратор

Описание. Настройка вручную параметров системы доменных имен (DNS).

Параметр	Аргумент	Описание
-OM	enable disable	Блокируются ручные настройки DNS.
-p	<первичный DNS сервер>	Задается первичный DNS-сервер.
-s	<вторичный DNS сервер>	Задается вторичный DNS-сервер.
-d	<имя домена>	Задается имя домена.
-n	<имя домена IPv6>	Задается имя домена IPv6.
-h	<имя хоста>	Задается имя хоста.

eventlog

Доступ. Администратор, пользователь устройства

Описание. Просмотр даты и времени поиска в журнале событий, состояния ИБП и состояния датчиков, подключенных к ПСУ. Просмотр последних событий в устройстве, а также их даты и времени. Для перемещения по журналу событий используются следующие клавиши:

Клавиша	Описание
ESC	Журнал событий закрывается, и экран возвращается к интерфейсу командной строки.
ENTER	Обновляется отображение журнала. Используйте эту команду для просмотра событий, которые были записаны после последней операции поиска и отображения журнала.
ПРОБЕЛ	Просмотр следующей страницы в журнале событий.
В	Просмотр предыдущей страницы в журнале событий. Эта команда отсутствует на главной странице журнала событий.
D	Выполняется удаление журнала событий. Следуйте подсказкам для подтверждения или отклонения удаления. Поиск удаленных событий не выполняется.

exit

Доступ. Администратор, пользователь устройства

Описание. Выход из сеанса интерфейса командной строки.

format

Доступ. Только администратор

Описание. Переформатирование файловой системы ПСУ и удаление всех сертификатов безопасности, ключей шифрования, параметров конфигурации и журналов событий и данных. Будьте осторожны с этой командой.



Примечание. Для сброса ПСУ на настройку по умолчанию используйте команду `resetToDef`.

ftp

Доступ. Только администратор

Описание. Включение или отключение доступа к серверу FTP. Для дополнительной защиты можно также изменить настройку номера порта на номер любого неиспользуемого порта от 5001 до 32768.

Параметр	Аргумент	Описание
-p	<номер порта>	Определение порта TCP/IP, который используется FTP-сервером для связи с ПСУ (по умолчанию 21). Сервер FTP использует как указанный порт, так и порт с номером на единицу меньше.
-S	enable disable	Настройка доступа на FTP-сервер.

Пример. Чтобы изменить порт TCP/IP на 5001, наберите:

```
ftp -p 5001
```

help

Доступ. Администратор, пользователь устройства

Описание. Просмотр списка всех команд интерфейса командной строки (CLI) для учетной записи Вашего типа. Для просмотра текста справки по конкретной команде наберите эту команду и поставьте после нее `help`.

Пример 1. Для просмотра списка команд, разрешенных при входе в систему в качестве пользователя устройства, наберите:

```
help
```

Пример 2. Для просмотра списка параметров, которые принимаются командой `alarmcount`, наберите:

```
alarmcount help
```

netstat

Доступ. Администратор, пользователь устройства

Описание. Выполняется просмотр состояния сети и всех активных адресов IPv4 и IPv6.

ntp

Доступ. Администратор, пользователь устройства

Описание. Просмотр и настройка параметров протокола сетевого времени.

Параметр	Аргумент	Описание
-OM	enable disable	Блокируются ручные настройки.
-p	<первичный сервер NTP>	Укажите первичный сервер.
-s	<вторичный сервер NTP>	Укажите вторичный сервер.

Пример 1. Для включения блокировки ручной настройки наберите:

```
ntp -OM enable
```

Пример 2. Для указания первичного NTP-сервера наберите:

```
ntp -p 150.250.6.10
```

ping

Доступ. Администратор, пользователь устройства

Описание. Определяет, подключено ли к сети устройство с указанным Вами IP-адресом или именем DNS. На адрес отправляется четыре запроса.

Аргумент	Описание
<IP-адрес или имя DNS>	Наберите IP-адрес в формате xxx.xxx.xxx.xxx или имя DNS, сконфигурированное DNS-сервером.

Пример. Чтобы определить, подключено к сети устройство с IP-адресом 150.250.6.10, наберите:

```
ping 150.250.6.10
```

portspeed

Доступ. Администратор

Описание.

Параметр	Аргументы	Описание
-s	auto 10H 10F 100H 100F	Определяется скорость связи с портом Ethernet. Команда auto включает устройства Ethernet для согласования передачи с максимально возможной скоростью. Дополнительную информацию о параметрах настройки скорости передачи порта см. в разделе «Скорость передачи порта» на стр. 75.

Пример. Чтобы настроить порт TSP/IP на связь со скоростью передачи 100 Мбит/с в полудуплексном режиме (единовременная связь только в одном направлении), наберите:

```
portspeed -s 100H
```

prompt

Доступ. Администратор, пользователь устройства

Описание. Настройка подсказки интерфейса командной строки для включения или исключения типа учетной записи для текущего пользователя в системе. Любой пользователь может изменить эту настройку; все учетные записи пользователя будут обновлены для использования новой настройки.

Параметр	Аргумент	Описание
-s	long	Подсказка включает в себя тип учетной записи пользователя, находящегося в данный момент в системе.
	short	Настройка по умолчанию. Длина подсказки составляет четыре символа: APC>

Пример. Чтобы включить тип учетной записи пользователя, находящегося в данный момент в системе, наберите:

```
prompt -s long
```

quit

Доступ. Администратор, пользователь устройства

Описание. Закрытие сеанса интерфейса командной строки (работает так же, как и команда exit).

radius

Доступ. Только администратор

Описание. Просмотр имеющихся параметров RADIUS, включение или отключение аутентификации RADIUS и настройка основных параметров аутентификации, возможная для двух серверов RADIUS.



Краткое описание конфигурации сервера RADIUS и список поддерживаемых серверов RADIUS приводится в руководстве «Конфигурирование сервера RADIUS» на стр. 69.

Дополнительные параметры аутентификации для серверов RADIUS имеются в веб-интерфейсе ПСУ. Дополнительную информацию см. в разделе «RADIUS» на стр. 68.

Для получения информации о настройке сервера RADIUS см. документ *Security Handbook* (Справочник по защите), компакт-диск с *утилитами* для платы сетевого управления и веб-сайт www.apc.com.

Параметр	Аргумент	Описание
-a	local radiusLocal radius	Настройка аутентификации RADIUS: local — RADIUS отключена. Включается локальная аутентификация. radiusLocal — RADIUS, затем локальная аутентификация. Включается RADIUS и локальная аутентификация. Сначала запрашивается аутентификация от сервера RADIUS. Если сервер RADIUS не отвечает, то используется локальная аутентификация. radius — RADIUS включается. Отключается локальная аутентификация.
-p1 -p2	<сервер IP>	Имя сервера или IP-адрес первичного или вторичного сервера RADIUS. ПРИМЕЧАНИЕ. Серверы RADIUS используют для аутентификации пользователей порт 1812 по умолчанию. Чтобы использовать другой порт, добавьте к имени сервера RADIUS или к IP-адресу двоеточие с последующим указанием номера нового порта.
-s1 -s2	<секрет сервера>	Разделенный секрет между первичным или вторичным сервером RADIUS и ПСУ.
-t1 -t2	<время ожидания сервера>	Время в секундах, в течение которого ПСУ ждет ответа от первичного или вторичного сервера RADIUS.

Пример 1.

Для просмотра имеющихся параметров RADIUS для ПСУ наберите `radius` и нажмите клавишу ENTER.

Пример 2. Чтобы включить RADIUS и локальную аутентификацию, наберите:

```
radius -a radiusLocal
```

Пример 3. Чтобы настроить 10-секундный тайм-аут для вторичного сервера RADIUS, наберите:

```
radius -t2 10
```

reboot

Доступ. Администратор

Описание. Перезапуск интерфейса ПСУ.

resetToDef

Доступ. Только администратор

Описание. Сброс всех параметров на значения по умолчанию.

Параметр	Аргументы	Описание
-p	all keepip	Выполняется сброс всех измененных параметров, включая действующие события, параметры устройства и, по желанию, параметры конфигурации TCP/IP.

Пример. Для сброса всех измененных настроек, за исключением параметров TCP/IP для ПСУ, наберите:

```
resetToDef -p keepip
```

snmp, snmpv3

Доступ. Только администратор

Описание. Включение или отключение SNMP 1 или SNMP 3.

Параметр	Аргументы	Описание
-S	enable disable	Включение или отображение соответствующей версии SNMP 1 или 3.

Пример. Для включения SNMP версии 1 наберите:

```
snmp -S enable
```

system

Доступ. Только администратор

Описание. Просмотр и установка имени системы, контактного лица, местоположения и времени работы, а также просмотр даты и времени, текущего пользователя и состояния системы высокого уровня P, N, A (см. раздел «Поля состояния на основном экране»).

Параметр	Аргумент	Описание
-n	<имя системы>	Определяется имя устройства, имя ответственного за это устройство и физическое расположение устройства. ПРИМЕЧАНИЕ. Если для определения значения используется более одного слова, то это значение должно указываться в кавычках. Эти значения используются также InfraStruxure Central и агентом SNMP ПСУ.
-c	<контакт системы>	
-l	<расположение системы>	

Пример 1. Для определения местоположения устройства как Test Lab (Тестовая лаборатория) наберите:

```
system -l "Test Lab"
```

Пример 2. Для задания имени системы Don Adams наберите:

```
system -n "Don Adams"
```

tcpip

Доступ. Только администратор

Описание. Выполняется просмотр и ручная настройка следующих параметров сети для ПСУ:

Параметр	Аргумент	Описание
-S	enable disable	Включение или выключение TCP/IP.
-i	<IP-адрес>	Наберите IP-адрес ПСУ, используя формат xxx.xxx.xxx.xxx
-s	<маска подсети>	Наберите маску подсети для ПСУ.
-g	<шлюз>	Наберите IP-адрес шлюза, используемого по умолчанию. Не используйте шлейфовый адрес (127.0.0.1) в качестве адреса шлюза по умолчанию.
-d	<имя домена>	Наберите имя DNS, сконфигурированное DNS-сервером.
-h	<имя хоста>	Наберите имя хоста, который будет использовать ПСУ.

Пример 1. Для просмотра сетевых параметров ПСУ наберите `tsrip` и нажмите клавишу ENTER.

Пример 2. Для ручной настройки IP-адреса 150.250.6.10 для ПСУ наберите:

```
tsrip -i 150.250.6.10
```

tsrip6

Доступ. Только администратор

Описание. Включение IPv6, просмотр и ручная настройка следующих параметров сети для ПСУ:

Параметр	Аргумент	Описание
-S	enable disable	Включение или выключение IPv6.
-man	enable disable	Разрешение ручной адресации для задания адреса IPv6 ПСУ.
-auto	enable disable	Разрешение автоматической настройки адреса IPv6 ПСУ.
-i	<адрес IPv6>	Задание адреса IPv6 ПСУ.
-g	<шлюз IPv6>	Задание адреса IPv6 шлюза по умолчанию.
-d6	router statefull stateless never	Задание режима DHCPv6: с управляемыми параметрами маршрутизатора, с сохранением состояния (поддержка состояния для адреса и другой информации), без сохранения состояния (состояние информации, отличной от адреса, не поддерживается), отключение.

Пример 1. Для просмотра сетевых параметров ПСУ наберите `tsrip6` и нажмите клавишу ENTER.

Пример 2. Чтобы вручную настроить адрес Pv6 2001:0:0:0:0:FFD3:0:57ab для ПСУ, наберите:

```
tsrip -i 2001:0:0:0:0:FFD3:0:57ab
```

ui0

Доступ. Администратор, пользователь устройства

Описание. Эта команда применяется для платы сетевого управления 2 AP9631 с подключенным дополнительным устройством ввода-вывода с сухими контактами (Dry Contact I/O Accessory) (AP9810).

Параметр	Аргумент	Описание
-rc <UIO порт №>	open close	Изменяется состояние подключенного вывода и указывается номер порта UIO (универсальный ввод-вывод).
-st	<UIO порт №> <UIO порт №>, <UIO порт №> <UIO порт №>—<UIO порт №>	Выполняется просмотр состояния датчиков, подключенных к устройству ввода-вывода с сухими контактами. Для просмотра состояния конкретного датчика или нескольких датчиков наберите номера их портов UIO.
-disc	<UIO порт №> <UIO порт №>, <UIO порт №> <UIO порт №>—<UIO порт №>	Выполняется идентификация подключений нового входного контакта или выходного реле.

Пример 1. Чтобы разомкнуть выход, наберите:

```
uio -rc 2 open
```

Пример 2. Для просмотра состояния устройств, подключенных к устройству ввода-вывода с сухими контактами, которое связано с универсальным портом 2 ввода-вывода, наберите:

```
uio -st 2
```

ups



Примечание. Некоторые параметры команды **ups** зависят от модели ИБП. В некоторых конфигурациях отдельные параметры команды **ups** могут не поддерживаться.

Доступ. Администратор, пользователь устройства

Описание. Управление ИБП и просмотр сведений о состоянии.

Параметр	Аргументы	Описание
-c	off graceoff on reboot gracereboot sleep gracesleep	Выполняется настройка действий ИБП. Дополнительную информацию см. в разделе «Примечание. Страница «Управление» недоступна на ИБП MGE Galaxy 300 и MGE Galaxy 7000.» на стр. 38.
-r	start stop	Выполняется начало или завершение проверки рабочего цикла. При калибровке выполняется пересчет оставшегося времени работы и требуется выполнение следующих условий. <ul style="list-style-type: none">• Поскольку при калибровке существенно расходуется ресурс батарей ИБП, необходимо выполнять калибровку при 100% зарядке батарей.• Для некоторых ИБП нагрузка при калибровке должна быть не менее 7%.
-s	start	Запускается самодиагностика ИБП.
-b	enter exit	Проверяется работа в режиме байпаса. Эта команда зависит от модели и может отсутствовать в Вашем ИБП. Дополнительную информацию см. в разделе «Примечание. Страница «Управление» недоступна на ИБП MGE Galaxy 300 и MGE Galaxy 7000.» на стр. 38.

Параметр	Аргументы	Описание
-o#	Off DelayOff On DelayOn Reboot DelayReboot Shutdown DelayShutdown Cancel	<p>Осуществляется управление любой из трех групп розеток ИБП Smart-UPS XLM. Укажите группу розеток с помощью знака #. Сведения о группах розеток приведены в разделе «Описание групп розеток» на стр. 42.</p> <p>Если группа розеток находится в состоянии on (вкл.), то этот параметр принимает три аргумента:</p> <ul style="list-style-type: none"> • Off — происходит мгновенное отключение группы. • DelayOff — отключение группы происходит спустя определенное время (в секундах), задаваемое как Задержка при отключении питания. • Reboot — происходит мгновенное отключение группы, затем она включается спустя определенное время (в секундах), задаваемое как Продолжительность перезагрузки и Задержка при включении питания. • DelayReboot — отключение группы розеток происходит спустя определенное время (в секундах), задаваемое как Задержка при отключении питания, затем она включается спустя определенное время в секундах, задаваемое как Продолжительность перезагрузки и Задержка при включении питания. • Shutdown — если ИБП работает от сети, выполняется перезагрузка группы розеток. Если ИБП работает от батареи, работа группы завершается до возобновления питания от сети переменного тока. • DelayShutdown — завершение работы группы розеток происходит спустя определенное время (в секундах), задаваемое как Задержка при отключении питания. • Cancel — предыдущие команды, например отключение, отменяются. <p>Если группа розеток имеет состояние off (выкл.), то этот параметр принимает два аргумента:</p> <ul style="list-style-type: none"> • On — происходит мгновенное включение группы. • DelayOn — включение группы происходит спустя определенное количество секунд, задаваемое как Задержка при включении питания. <p>Параметры Задержка при включении питания, Задержка при отключении питания и Продолжительность перезагрузки настраиваются в веб-интерфейсе. Дополнительные сведения см. в разделе «Параметр групп розеток (включая автоматический сброс нагрузки)» на стр. 43.</p>
-os#		<p>Просмотр состояния (вкл., выкл. или перезагрузка) всех групп розеток. Для просмотра состояния конкретной группы розеток укажите ее номер. Например, наберите <code>ups -os1</code> для просмотра состояния группы розеток 1.</p> <p>Примечание. При использовании данного параметра на ИБП с основной группой розеток: 1 обозначает основную группу розеток, 2 обозначает коммутируемую группу розеток 1, 3 обозначает коммутируемую группу розеток 2 и т. д. На ИБП БЕЗ основной группы розеток: 1 обозначает коммутируемую группу розеток 1 и т. д.</p>

Параметр	Аргументы	Описание
-st		Просмотр состояния ИБП.
-a	start	Проверка звукового сигнала ИБП.

Параметры команды `ups` для устройств ИБП MGE Galaxy:



Примечание. Эти команды доступны только на ИБП MGE Galaxy 300 и MGE Galaxy 7000. Некоторые параметры могут быть доступны только на отдельной модели ИБП.

Параметр	Аргумент	Описание
-input	<№ фазы> all	Отображение измерений входных характеристик для выбранной фазы ИБП. При вводе значения «all» отображаются сведения для всех фаз данного ИБП.
	voltage current frequency all	Указание измерений входных характеристик для команды <code>ups</code> . Пример. <code>ups -input 2 frequency</code> Отображение частоты для 2 фазы ИБП.
-bypass	<№ фазы> all	Отображение измерений входных характеристик для выбранной фазы сети байпаса. При вводе значения «all» отображаются сведения для всех фаз сети байпаса.
	voltage current frequency all	Указание измерений входных характеристик для команды <code>ups</code> . Пример. <code>ups -bypass 2 current</code> Отображение тока для 2 фазы сети байпаса.
-output	<№ фазы> all	Отображение измерений выходных характеристик для выбранной фазы ИБП. При вводе значения «all» отображаются сведения для всех фаз данного ИБП.
	voltage current load power perload pf frequency all	Указание измерений выходных характеристик для команды <code>ups</code> . Пример. <code>ups -output 2 perload</code> Отображение процента нагрузки для 2 фазы ИБП.
-batt		Отображение состояния батареи ИБП.
-about		Отображение сведений об ИБП.
-al	<c w>	Отображение всех имеющихся сигналов тревоги. Указание значения «c» или «w» позволяет отобразить только критические (c) или только предупредительные (w) сигналы тревоги.

Пример 1. Для запуска калибровки времени автономной работы наберите:

```
ups -r start
```

Пример 2. Для мгновенного отключения группы розеток 2 для ИБП Smart-UPS XLM наберите:

```
ups -o2 off
```

upswupdate



Примечание. Эта команда доступна только для устройств SMX.

Доступ. Администратор, пользователь устройства

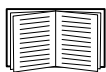
Описание. Запуск обновления прошивки ИБП. Файл обновления прошивки должен быть предварительно загружен на ПСУ с использованием протокола FTP и сохранен в каталоге /upsw/.

Параметр	Аргумент	Описание
-apply	индикатор выполнения	Запуск обновления прошивки.
-status	индикатор выполнения	Проверка состояния уже запущенного обновления прошивки.
-lastresult		Просмотр результатов последнего запущенного обновления прошивки.
-fileinfo		Просмотр сведений о файле обновления прошивки, сохраненного на ПСУ, включая его имя, совместимость с ИБП и версию.

user

Доступ. Только администратор

Описание. Задание имени пользователя и пароля для каждого типа учетной записи, а также задание времени ожидания отсутствия активности.



Сведения о разрешенных действиях для каждого типа учетной записи (администратор, пользователь устройства и пользователь с правами только для чтения) приведены в разделе «Типы учетных записей» на стр. 3.

Параметр	Аргумент	Описание
-an -dn -gn	<имя администратора> <имя устройства> <имя только для чтения>	Для каждого типа учетной записи задается имя пользователя, зависящее от регистра. Максимальная длина — 10 символа.
-ap -dp -gp	<пароль администратора> <пароль устройства> <пароль только для чтения>	Для каждого типа учетной записи задается пароль, зависящий от регистра. Максимальная длина — 32 символа. Пустые пароли (без символов) запрещены.
-t	<минуты>	Выполняется настройка времени (3 минуты по умолчанию), по истечении которого неактивный пользователь отключается от системы.

Пример 1. Чтобы изменить имя администратора и пароль на XYZ, наберите:

```
user -ap XYZ
```

Пример 2. Чтобы изменить время выхода из системы, установив его на 10 мин, наберите:

```
user -t 10
```

web

Доступ. Администратор

Описание. Включение доступа к веб-интерфейсу с использованием HTTP и HTTPS.

Для дополнительной безопасности можно изменить настройку порта для HTTP и HTTPS, задав любой неиспользуемый порт от 5000 до 32768. Пользователи должны использовать двоеточие (:) в адресном поле браузера для указания номера порта. Например, для номера порта 5000 и IP-адреса 152.214.12.114:

`http://152.214.12.114:5000`

Параметр	Аргумент	Описание
-S	disable http https	Настраивается доступ к серверу веб-интерфейса. При включении HTTPS данные шифруются во время передачи и аутентифицируются цифровым сертификатом.
-ph	<http порт №>	Указывается порт TCP/IP, используемый HTTP для связи с ПСУ (по умолчанию 80).
-ps	<https порт №>	Указывается порт TCP/IP, используемый HTTPS для связи с ПСУ (по умолчанию 443).

Пример. Чтобы заблокировать любой доступ к веб-интерфейсу, наберите:

```
web -S disable
```

xferINI

Доступ. Только администратор Эта команда работает только через последовательный интерфейс командной строки (CLI).

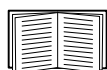
Описание. Использование XMODEM для загрузки .ini файла при доступе к интерфейсу командной строки через последовательный канал связи. После завершения загрузки:

- Если система или сеть изменились, то происходит перезапуск интерфейса командной строки, и необходимо заново войти в систему.
- Если для передачи файлов выбрана скорость в бодах, которая отличается от скорости передачи ПСУ по умолчанию, то для установки связи с ПСУ необходимо переустановить значение скорости на значение по умолчанию.

xferStatus

Доступ. Только администратор

Описание. Просмотр результатов последней передачи файла.



Описание кодов результатов передачи приведено в разделе «Проверка обновлений и исправлений» на стр. 109.

Веб-интерфейс

Введение

Обзор

Веб-интерфейс обеспечивает опции для работы с ИБП и платой управления, а также для просмотра состояния ИБП.



См. раздел «WWW» на стр. 77, в котором приводятся сведения о том, как выбирать, включать и отключать протоколы, управляющие доступом к веб-интерфейсу, а также как определять порты сетевого интерфейса веб-сервера для протоколов.

Поддерживаемые веб-браузеры

Для доступа к плате управления через веб-интерфейс можно использовать браузер Microsoft® Internet Explorer® (IE) версии 7.x или выше (только для операционных систем Windows®) или Mozilla® Firefox® версии 3.0.6 или выше (для всех операционных систем). Другие популярные браузеры также могут использоваться, но они не прошли полную проверку.

Плата управления не может работать с прокси-сервером. Прежде чем воспользоваться интернет-браузером для доступа к веб-интерфейсу платы управления, необходимо выполнить перечисленные ниже операции.

- Настроить браузер на отключение прокси-сервера для платы управления.
- Настроить прокси-сервер так, чтобы он не загружал конкретный IP-адрес платы управления.

Как войти в систему

Общее описание

Можно использовать доменное имя DNS или системный IP-адрес платы управления для адреса URL веб-интерфейса. Для входа в систему используйте зависящее от регистра имя пользователя и пароль. Имя пользователя по умолчанию зависит от типа учетной записи:

- **arc** для Администратора
- **device** для Пользователя устройства
- **readonly** для Пользователя только для чтения

Для всех трех типов учетных записей пароль по умолчанию **arc**.

При входе в систему можно задать язык интерфейса для пользователя, выбрав его из разворачивающегося меню **Язык**.



Примечание: Если в качестве протокола доступа используется HTTPS (SSL/TLS), то реквизиты доступа сравниваются с информацией в сертификате сервера. Если сертификат был сформирован с помощью Security Wizard, а IP-адрес был указан как стандартное имя в сертификате, то для входа на плату управления необходимо указать IP-адрес. Если в качестве стандартного имени в сертификате было указано имя, то для входа в систему необходимо указать имя DNS.



Сведения о странице веб-сайта, которая отображается при входе в систему, приведены в разделе «Начало» на стр. 33.

Форматы URL-адреса

Наберите имя DNS или IP-адрес платы управления в поле URL-адреса веб-браузера и нажмите ENTER. Если в браузере Internet Explorer указывается порт сервера не по умолчанию, то в URL необходимо добавить `http://` или `https://`.

Наиболее распространенные сообщения об ошибках браузера при входе в систему.

Сообщение об ошибке	Браузер	Причина ошибки
«У вас нет прав для просмотра этой страницы» или «Кто-то в данный момент вошел в систему...»	Internet Explorer, Firefox	Кто-то еще вошел в систему.
«Невозможно отобразить данную страницу.»	Internet Explorer	Отключен доступ к сети или неправильно указан адрес URL.
«Подключение невозможно.»	Firefox	

Примеры формата URL.

- Для имени DNS в Web1:
 - `http://Web1`, если HTTP является вашим режимом доступа
 - `https://Web1`, если HTTPS (HTTP с SSL) является вашим режимом доступа
- Для системного IP-адреса 139.225.6.133 и порта сервера веб-сайта (80):
 - `http://139.225.6.133`, если HTTP является вашим режимом доступа
 - `https://139.225.6.133`, если HTTPS (HTTP с SSL) является вашим режимом доступа
- Для системного IP-адреса 139.225.6.133 и порта сервера веб-сайта не по умолчанию (5000):
 - `http://139.225.6.133:5000`, если HTTP является вашим режимом доступа
 - `https://139.225.6.133:5000`, если HTTPS (HTTP с SSL) является вашим режимом доступа
- Для системного IPv6-адреса 2001:db8:1::2c0:b7ff:fe00:1100 и порта сервера веб-сайта не по умолчанию (5000):
 - `http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000`, если HTTP является вашим режимом доступа




Начало

Обзор

На странице интерфейса **Начало**, отображаемой при входе в систему, можно видеть активные аварийные сообщения и последние события, записанные в журнал событий.

Значки состояния

Один и более значков вместе с сопроводительным текстом указывают на текущее рабочее состояние ИБП.

Обозначение	Описание
	Critical: Критический аварийный сигнал, требующий немедленного принятия мер.
	Warning: Тревожная сигнализация требует внимания, поскольку не решенная вовремя проблема может привести к потере данных и порче оборудования, если не устранить вызвавшую ее причину.
	Нет сигналов тревоги: Аварийные сигналы отсутствуют; ИБП и плата управления функционируют нормально.

В верхнем правом углу каждой страницы веб-интерфейса отображаются те же значки, которые отображаются на странице **Начало** с сообщениями о состоянии ИБП:

- Значок **Нет сигналов тревоги** указывает на отсутствие аварийной ситуации.
- Один или оба других значка (**Critical** и **Warning**) указывают на наличие аварийной ситуации, после каждого значка указывается количество активных аварийных сигналов данного уровня серьезности.

Чтобы вернуться к странице **Начало** для просмотра краткого сообщения о состоянии ИБП, включая активные аварийные сигналы, нажмите на значок состояния на любой странице интерфейса.

Последние события в устройстве

На странице **Начало** отображаются **Последние события устройства** в обратном хронологическом порядке: первыми идут последние события с указанием и времени и даты. Нажмите **Дополнительные события** для просмотра всего журнала событий.

Как пользоваться вкладками, меню и ссылками

Вкладки

Помимо вкладки для домашней страницы **Начало** отображаются следующие вкладки. Нажмите на вкладку для отображения набора опций меню:

- **ИБП.** Отображается состояние ИБП, задаются команды управления ИБП, выполняется настройка параметров ИБП, выполняются диагностические тесты, настройка и порядок отключения, просмотр сведений об ИБП и плате управления
- **Окружающая среда.** Просмотр состояния всех температурных датчиков, датчиков температуры и влажности, входного контакта или выходного реле, подключенного к плате управления. Просмотр активных аварийных сигналов и последних событий, связанных с окружающей средой. Настройка пороговых значений и других параметров, связанных с контролем окружающей среды.



Примечание: Для ИБП вкладка **Окружающая среда** отображается только при наличии температурного датчика, датчика температуры и влажности, входного контакта или выходного реле.

- **Журналы.** Просмотр и настройка журналов событий и данных.
- **Администрирование.** Настройка безопасности, связи в сети, уведомления и общих параметров.

Меню

Левая панель меню управления. Каждая вкладка (за исключением вкладки Начало) имеет левую панель меню управления, состоящую из заголовков и опций.

- Если под заголовком указываются опции с отступом вправо, то сам заголовок не является ссылкой. Для отображения или настройки параметров нажмите на какую-либо опцию.
- Если под заголовком указываются опции без отступа, то сам заголовок является ссылкой. Для отображения или настройки параметров нажмите на заголовок.

Верхняя строка меню. Вкладка **Администрирование** представляет собой набор опций в верхней строке меню. Выберите одну из опций для отображения левой панели меню управления

Быстрые ссылки

На каждой странице интерфейса слева внизу предусмотрены три настраиваемые ссылки. По умолчанию эти ссылки выполняют доступ по адресам URL для следующих интернет-страниц:

- **Link 1:** Домашняя страница веб-сайта www.apc.com
- **Link 2:** Демонстрация продукции в Интернете.
- **Link 3:** Сведения о службах удаленного контроля



Перенастройка этих ссылок описана в разделе «Конфигурирование связей» на стр. 97.

Контроль и настройка ИБП



Примечание. Для платы сетевого управления ИБП 2 AP9631 с подключенным устройством ввода-вывода с сухими контактами (AP9810) на вкладке **ИБП** отображаются два параметра в верхней строке меню: **ИБП** и **Политика управления**. Используйте параметр **ИБП** для выполнения задач, описанных в данной главе.



Сведения о параметре **Политика управления** приведены в разделе «Настройка политики управления» на стр. 60.

Страница «Обзор»

Страница **Обзор** отображается по умолчанию при щелчке вкладки **ИБП** или при выборе вкладки **ИБП** и элемента **Обзор** на левой панели меню навигации этой вкладки.

Рабочее состояние

Значки и сопроводительный текст, указывающие рабочее состояние ИБП, появляются под названием модели ИБП и настроенным именем ИБП.

Рабочее состояние	Значок	Описание
Оперативный режим		Нет сигналов тревоги: сигналы тревоги отсутствуют; ИБП и ПСУ функционируют нормально.
В аварийном состоянии (сопроводительный текст указывает на аварийное состояние, и дается краткое описание сигнала тревоги)		Критическое состояние: возникла критическая аварийная ситуация, которая требует принятия незамедлительных мер, чтобы избежать потери данных или порчи оборудования.
		Предупреждение: сигнал тревоги требует внимания, поскольку не устраненная вовремя проблема может привести к потере данных и порче оборудования.

Быстрое состояние

Отображается приведенная ниже информация (некоторые поля зависят от модели и могут не отображаться для Вашей модели ИБП).

- На графиках:

– **Нагрузка (Вт):** график с указанием нагрузки подключенного оборудования в процентах от допустимой нагрузки в ваттах.



Примечание. На ИБП MGE Galaxy 300 и MGE Galaxy 7000 график имеет заголовок **Нагрузка**.

– **Емкость батареи:** график отображает процент общей емкости батареи ИБП, доступный для поддержания работы подключенного оборудования.

- В списке:
 - **Входное напряжение:** напряжение переменного тока, получаемое ИБП, а для трехфазных ИБП — напряжения каждой фазы.
 - **Выходное напряжение:** напряжение переменного тока, которое ИБП или каждая фаза трехфазного ИБП подает на нагрузку.
 - **Температура окружающей среды:** температура воздуха внутри корпуса на входе-выходе ИБП.
 - **Оставшееся время автономной работы:** продолжительность работы ИБП от батареи для поддержания нагрузки.
 - **Последний переход на батарею:** причина последнего переключения на работу от батареи.
 - **Резервирование:** количество модулей питания, которые могут отказать или могут быть удалены, не вызывая переключения ИБП на режим байпаса. Например, при резервировании n+2 два модуля питания могут быть неисправны или сняты без необходимости перехода ИБП в режим байпаса.

Последние события ИБП

Самые последние события, происшедшие в ИБП, приводятся в обратном хронологическом порядке. Для просмотра всего журнала событий щелкните **Дополнительные события**.

Страница «Подробное состояние»/«Состояние»

Для отображения подробной информации о состоянии ИБП щелкните параметр **Подробное состояние** в левом меню навигации на вкладке **ИБП**.



Примечание. Страница «Подробное состояние» недоступна на ИБП MGE Galaxy 300 и MGE Galaxy 7000.

Параметр «Измерения»

Для каждого устройства ИБП отображаются следующие сведения:

Последний переход на батарею — причина последнего переключения на работу от батареи.

Внутренняя температура — температура внутри ИБП.

Оставшееся время автономной работы — продолжительность работы ИБП от батареи для поддержания нагрузки.



Подробные сведения о состоянии конкретного устройства ИБП, связанного с ПСУ, приводятся в интерактивной справке.

Сведения в зависимости от модели включают в себя следующие данные, для 3-фазных моделей ИБП некоторые из них относятся к фазе.

- **Напряжение, ток и частота**, например, входное и выходное напряжение, входной и выходной ток, входная частота, входное напряжение в режиме байпаса, а также минимальное и максимальное входное напряжение за последнюю минуту.
- **Информация о нагрузке ИБП**, например нагрузка ИБП, указываемая в кВА, или в процентах от доступной мощности в кВА или Вт.
- **Информация об отказоустойчивости**, например о резервировании питания.
- **Информация о батарее**, например, доступная емкость батареи в процентах от емкости полностью заряженной батареи, выходной ток батареи, номинальное напряжение батареи, нормированное количество ампер-часов для батарейных шкафов, количество установленных батарей и количество неисправных батарей.
Коэффициент полезного действия на выходе показывает, какой процент входной мощности поступает непосредственно на нагрузку. Оставшийся процент мощности используется ИБП.
Использование выходной мощности показывает фактическую мощность, используемую нагрузкой, начиная с момента последнего сброса ИБП в значения по умолчанию.
- **Состояние внешних и внутренних компонентов**, например, интеллектуального модуля и модуля питания, блока автоматического выключателя, внешнего выключателя и трансформатора.

Параметр «Группы розеток»

Эта страница доступна не для всех устройств ИБП.

На экране «Состояние группы розеток» отображаются имена и текущие состояния всех коммутируемых групп розеток на ИБП.

Параметр «Энергопотребление»

Эта страница доступна не для всех устройств ИБП.

Параметр «Энергопотребление» позволяет отслеживать энергопотребление подключенного к ИБП оборудования. Кроме того, он позволяет узнать другие связанные с энергопотреблением сведения, например, о выбросах углекислого газа и стоимости электроэнергии.

Энергопотребление: приблизительный объем потребленной к настоящему моменту времени электроэнергии в киловатт-часах (кВт.ч). Например, ИБП, питающий лампочку мощностью 350 Вт в течение 1000 часов, потребляет 350 кВт.ч электроэнергии.

Общая стоимость: приблизительная стоимость потребленной электроэнергии в местной валюте. Например, за 1000 часов лампочка потребляет 350 кВт.ч энергии по 0,10 доллара за кВт.ч, что в итоге дает сумму в 35 долларов.

Выделение CO₂: приблизительный общий объем выделенного к настоящему моменту времени углекислого газа (CO₂) в килограммах или фунтах.

Значения общей стоимости и выделения CO₂ в значительной степени зависят от источника энергии и распределительной сети. Для получения приблизительного значения выберите свою страну в раскрывающемся списке **Расположение** и щелкните кнопку **Изменить**. Чтобы ввести собственные значения, щелкните ссылку **Изменить пользовательские настройки**.

(Для ввода своих собственных значений можно также выбрать пункт **Настраиваемое** в раскрывающемся списке и щелкнуть **Изменить**).

Страница «Управление»

Для получения доступа к действиям по управлению ИБП выберите **ИБП** или **Группы розеток** в области «Управление».



Примечание. Страница «Управление» недоступна на ИБП MGE Galaxy 300 и MGE Galaxy 7000.

Параметр «ИБП»

Этот параметр применяется как для отдельных устройств ИБП, так и для синхронизованных групп управления. Дополнительные сведения о синхронизованных группах управления см. в разделе «Параметр управления синхронизацией» на стр. 49

Действия (для отдельных ИБП и синхронизованных групп управления). Используйте действия, описанные в приведенной ниже таблице, для отдельных ИБП и для синхронизованных групп управления в соответствии со следующими указаниями.

- Действия **Перевести ИБП в режим байпаса** и **Вывести ИБП из режима байпаса** поддерживаются:
 - только для отдельных устройств ИБП, но не для синхронизированных групп управления;
 - только для ИБП Symmetra и некоторых устройств Smart-UPS.
- Все действия, *кроме* **Перевести ИБП в режим байпаса** и **Вывести ИБП из режима байпаса**, поддерживаются:
 - для устройств Smart-UPS, включая входящие в синхронизованные группы управления;
 - для отдельных устройств UPS, включая устройства Symmetra.



Примечание. При выборе значения **Инициировать сетевое выключение PowerChute** в веб-интерфейсе запуск действия **Отключить ИБП**, **Перезагрузить ИБП** или **Перевести ИБП в спящий режим** аналогичен выбору GraceOff (мягкое отключение ИБП), GraceReboot (мягкая перезагрузка ИБП) или GraceSleep (мягкий перевод ИБП в спящий режим) в интерфейсе командной строки.



Более подробные сведения о задержках и параметрах, указанных в приведенной ниже таблице, см. в разделах «Страницы «Конфигурация»» на стр. 42 и «Параметр управления синхронизацией» на стр. 49. Использование команды **Тестирование сигнала тревоги ИБП** для синхронизированной группы управления описано в разделе «Страница «Диагностика»» на стр. 53.

Действие	Описание
Включить ИБП (веб-интерфейс) ups -c On (интерфейс командной строки)	Включается питание ИБП. <ul style="list-style-type: none">• Для модели ИБП с группами розеток это действие включает группы розеток в соответствии со значением, указанным для параметра Задержка при включении питания для каждой группы. См. раздел «Параметр групп розеток (включая автоматический сброс нагрузки)» на стр. 43.• Для синхронизированной группы управления после задержки в течение нескольких секунд данное действие включает все устройства группы, на которые подается питание.

Действие	Описание
<p>Отключить ИБП (веб-интерфейс) ups -c Off (интерфейс командной строки)</p>	<p>Выходное питание ИБП и всех групп розеток (для моделей с группами розеток) отключается без задержки выключения. ИБП и все группы розеток остаются отключенными до тех пор, пока снова не будет включено питание.</p> <p>Для синхронизированной группы управления это действие отключает питание всех подключенных членов группы. Параметр Задержка выключения не используется. ИБП отключаются через несколько секунд и остаются отключенными до тех пор, пока Вы не подадите на них питание. См. «Параметр выключения» на стр. 45.</p> <p>ПРИМЕЧАНИЕ. Для действия по синхронизированному отключению, в котором используется значение Задержка выключения запускающего ИБП, используйте протокол SNMP. Для позиции upsAdvControlUpsOff OID установите значение на turnUpsSyncGroupOffAfterDelay (5).</p>
<p>ups -c GraceOff (интерфейс командной строки)</p>	<p>Отключается выходное напряжение ИБП и со всех групп розеток (для моделей ИБП с группами розеток) после истечения времени Макс. требуемая задержка и Задержка выключения. См. раздел «Параметр клиентов PowerChute» на стр. 49.</p>
<p>Перезагрузить ИБП (веб-интерфейс) ups -c Reboot (интерфейс командной строки)</p>	<p>Происходит перезапуск подключенного оборудования после выполнения следующих операций.</p> <ul style="list-style-type: none"> • Отключается питание ИБП после команды Задержки выключения. • Питание на ИБП включается после того, как емкость батареи возвращается к минимальному значению в процентах, заданному для параметра Минимальная емкость батареи или позволяющему поддерживать нагрузку в течение времени, заданного параметром Продолжительность времени автономной работы на выходе. (Этот параметр зависит от модели ИБП.) ИБП ждет в течение времени, указанного в параметре Задержка возврата. См. «Параметр выключения» на стр. 45. • Для ИБП с группами розеток Задержка при включении питания происходит после включения ИБП и перед включением группы розеток. На вкладке ИБП настройте Задержка при включении питания для каждой группы розеток с помощью параметра настройки под заголовком Группы розеток. См. «Параметр групп розеток (включая автоматический сброс нагрузки)» на стр. 43. <p>Для действия синхронизированной группы управления:</p> <ol style="list-style-type: none"> 1. Этот параметр отключает питание от ИБП, входящих в состав группы, по истечении времени ожидания, указанного в параметре Задержка выключения для запускающих ИБП. См. «Параметр выключения» на стр. 45. 2. Запускающий ИБП ждет в течение времени, заданного в секундах в параметре Задержка при синхронизации мощности, чтобы у членов группы было время восстановить входное питание. Если все члены группы уже восстановили входное питание, то остающееся время задержки сбрасывается. Если все члены группы восстанавливают входное питание во время задержки, то остающееся время задержки сбрасывается. Описание настройки Задержка при синхронизации мощности приводится в разделе «Настройка устройства синхронизированной группы управления» на стр. 51. 3. Задержка возврата начинается при запуске ИБП в соответствии с настройкой Минимальная емкость батареи (или Продолжительность времени автономной работы на выходе). См. «Параметр выключения» на стр. 45. <p>Минимальная емкость батареи (или Продолжительность времени автономной работы на выходе) для запускающего ИБП распространяется также и на устройства в группе. Однако можно снизить требования к устройствам, входящим в группу, настраивая параметр Минимальная погрешность емкости батареи (или параметр Погрешность продолжительности времени автономной работы на выходе), например, если при запуске Минимальная емкость батареи 50%, а Минимальная погрешность емкости батареи 5%, то для члена группы емкость батареи для перезагрузки составит 45%. См. раздел «Настройка устройства синхронизированной группы управления» на стр. 51.</p>

Действие	Описание
ups -c GraceReboot (интерфейс командной строки)	<ul style="list-style-type: none"> • Это действие аналогично действию Перезагрузить ИБП, но с дополнительной задержкой перед отключением. Подключенное оборудование отключается только после того, как для ИБП (или для запускающего ИБП синхронизированной группы управления) пройдет время ожидания Макс. требуемая задержка, которая рассчитывается в соответствии с указаниями из раздела «Эти параметры позволяют использовать утилиту сетевого выключения PowerChute для выключения до 50 серверов в сети, где используется клиентская версия этой утилиты.» на стр. 45. • Для ИБП с группами розеток Задержка при включении питания происходит после включения ИБП и перед включением группы розеток. На вкладке ИБП настройте параметр Задержка при включении питания для каждой группы розеток с помощью параметра настройки под заголовком Группы розеток. См. «Параметр групп розеток (включая автоматический сброс нагрузки)» на стр. 43.
Перевести ИБП в спящий режим (веб-интерфейс) ups -c Sleep (интерфейс командной строки)	ИБП переводится в спящий режим за счет отключения его выходного напряжения на определенный период времени: <ul style="list-style-type: none"> • ИБП отключает выходное напряжение по истечении времени, заданного в параметре Задержка выключения. См. «Параметр выключения» на стр. 45. • После восстановления входного питания ИБП включает выходное питание по истечении двух заданных периодов времени: Время в спящем режиме и Задержка возврата. См. «Параметр выключения» на стр. 45. • Для действия синхронизированного управления ПСУ запускающего ИБП ждет определенное время, заданное в секундах в параметре Задержка при синхронизации мощности для устройств, входящих в группу, чтобы восстановить входное питание до начала периода Задержка возврата. Если все члены группы уже восстановили входное питание, то Задержка при синхронизации мощности отменяется. Если все члены группы восстанавливают входное питание во время задержки, то остающееся время задержки сбрасывается. См. раздел «Настройка устройства синхронизированной группы управления» на стр. 51.
ups -c GraceSleep (интерфейс командной строки)	ИБП переводится в спящий режим (отключается выходное напряжение на определенный период времени). <ul style="list-style-type: none"> • ИБП отключает выходное напряжение по истечении периода Макс. требуемая задержка, чтобы дать время для безопасного отключения сервера программой сетевого отключения PowerChute, и периода Задержка выключения. См. разделы «Макс. требуемая задержка» на стр. 45 и «Параметр выключения» на стр. 45. • После восстановления входного питания ИБП включает выходное питание по истечении двух заданных периодов времени: Время в спящем режиме и Задержка возврата. См. раздел «Параметр выключения» на стр. 45. • Для действия синхронизированного управления плата управления запускающего ИБП ждет определенное время, выраженное в секундах, заданное в параметре Задержка при синхронизации мощности, чтобы участники группы могли восстановить входное питание до начала периода Задержка возврата. Если все члены группы уже восстановили входное питание, то Задержка при синхронизации мощности отменяется. Если все члены группы восстановили входное питание во время задержки, то остающееся время задержки сбрасывается. См. раздел «Настройка устройства синхронизированной группы управления» на стр. 51.

Действие	Описание
<p>Перевести ИБП в режим байпаса и Вывести ИБП из режима байпаса (веб-интерфейс):</p> <pre>ups -b Enter</pre> <p>(интерфейс командной строки)</p>	<p>Управление режимом байпаса, позволяющим осуществлять обслуживание ИБП Symmetra и некоторых моделей Smart-UPS, не отключая питание ИБП.</p>

Параметр «Группы розеток»

Для включения, отключения или перезапуска любой группы розеток (пока включено выходное питание ИБП) выберите вкладку **ИБП**, а затем **Управление- Группы розеток**.

На этой странице перечисляются имена и состояния (включено или выключено) каждой группы розеток, которая была сконфигурирована с помощью параметра **Конфигурация - Группы розеток**.

Для группы можно выбрать любые приведенные ниже действия (или отменить выбор всех действий).

- Если группа розеток находится в состоянии **Выкл.:**
 - **Включить немедленно:** происходит мгновенное включение группы.
 - **Включить с задержкой:** включение группы выполняется через несколько секунд, указанных в настройке **Задержка при включении питания**.
- Если группа находится в состоянии **Вкл.:**
 - **Выключить немедленно:** происходит мгновенное выключение группы.
 - **Выключить с задержкой:** отключение группы происходит спустя определенное время в секундах, задаваемое как **Задержка при отключении питания**.
 - **Перезагрузить немедленно:** происходит мгновенное отключение группы, затем она включается спустя определенное время в секундах, задаваемое в параметре **Продолжительность перезагрузки и Задержка при включении питания**
 - **Перезагрузить с задержкой:** отключение группы происходит спустя определенное время в секундах, задаваемое в параметре **Задержка при отключении питания**, затем она включается спустя определенное время в секундах, задаваемое в параметре **Продолжительность перезагрузки и Задержка при включении питания**.
- Для некоторых моделей ИБП в случае, когда состояние группы розеток указано как **Вкл.** и ИБП работает от батареи:
 - **Выключить немедленно, перезапуск питания переменного тока:** происходит мгновенное выключение группы. Через определенное время, заданное в секундах для параметров **Продолжительность перезагрузки и Задержка при включении питания**, проверяется, что имеется напряжение переменного тока и ИБП поддерживает требование минимального времени автономной работы, а затем включается группа.
 - **Выключить с задержкой, перезапуск питания переменного тока:** отключение группы происходит спустя определенное время в секундах, задаваемое в параметре **Задержка при отключении питания**. Через определенное время, заданное в секундах для параметров **Продолжительность перезагрузки и Задержка при включении питания**, проверяется, что имеется напряжение переменного тока и ИБП поддерживает требование минимального времени автономной работы, а затем включается группа.

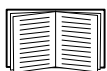
После выбора действия щелкните **Далее>>** для просмотра подробного описания действия, включая данные всех задержек. Щелкните **Применить**, чтобы подтвердить это действие.

Страницы «Конфигурация»



Примечание. Страницы «Конфигурация» доступны только на ИБП MGE Galaxy 300 и MGE Galaxy 7000.

Описание групп розеток



Группирование розеток возможно только для некоторых моделей ИБП. Чтобы определить, поддерживает ли Ваша модель группы розеток, обратитесь к документации по Вашему ИБП.

Разрешенные настройки зависят от модели ИБП. Более подробные сведения о полях и параметрах Вашей модели приводятся в интерактивной справке.

Основные группы розеток. В некоторых моделях ИБП подача питания переменного тока предусмотрена для одной основной группы розеток.



Примечание. *Основная группа розеток управляет распределением питания по всем коммутируемым группам розеток ИБП.*

- Если основная группа розеток отключена, то коммутируемые группы розеток не могут быть включены.
- Если Вы отключаете основную группу розеток, то ИБП сначала отключает коммутируемые группы розеток, а затем основную группу.
- Для включения отключенной коммутируемой группы розеток ИБП необходимо включить сначала основную группу, а затем — коммутируемую.

Коммутируемые группы розеток. Некоторые модели ИБП обеспечивают подачу питания на коммутируемые группы розеток. Каждая группа может выполнять действия независимо от других групп. Удаленное управление группой розеток позволяет осуществлять последовательный запуск и останов устройств и перезапускать заблокированные устройства.

Включение и выключение групп розеток зависит от того, как они настроены, и от того, как включается и выключается ИБП.

- До настройки действий, описанных в разделе «Параметр «Группы розеток»» на стр. 41, и соответствующих задержек, описанных в разделе «Параметр групп розеток (включая автоматический сброс нагрузки)» на стр. 43, при включении выхода ИБП каждая отключенная группа розеток включается по умолчанию и подает питание на устройства, подключенные к розеткам этой группы.
- После настройки операций и задержек эти операции и задержки контролируют включение и выключение групп розеток при включении или выключении ИБП на интерфейсе пользователя платы сетевого управления или на интерфейсе дисплея ИБП.

Параметр групп розеток (включая автоматический сброс нагрузки)

Выберите **Конфигурация - Группы розеток** для отображения данного параметра.

Имя группы розеток и состояние. На этой странице можно просматривать имя и состояние группы розеток. Для просмотра или настройки параметров щелкните имя группы розеток на другой странице экрана (см. раздел «Программные параметры» на этой странице).

Настройка или поле	Описание
Имя	Имя группы розеток, отображаемое с номером группы розеток каждый раз при отображении на дисплее данного номера группы.
Состояние	Отображается состояние группы розеток (вкл. или выкл.).

Программные параметры. Настройки зависят от модели ИБП. Используйте программные параметры, чтобы определить, как ИБП будет реагировать на команды пользователя.

Настройка или поле	Описание
Задержка при включении питания	При отключенной группе розеток выполняется задержка (значение в секундах зависит от конкретного устройства ИБП) перед включением, если выбрано действие Задержка включена, Перезагрузка или Задержка перезагрузки . Флажок Никогда (доступен только на некоторых устройствах ИБП): Для переопределения параметра Задержка при включении питания установите флажок Никогда . В этом случае возможно только действие Включение .
Задержка при отключении питания	При включенной группе розеток выполняется задержка (значение в секундах зависит от конкретного устройства ИБП) перед выключением, если выбрано действие Задержка выключена, Перезагрузка или Задержка перезагрузки . (Во время задержки перезагрузки группа розеток перед включением ждет определенный период времени в секундах, заданный в параметрах Продолжительность перезагрузки и Задержка при включении питания .) Флажок Никогда (доступен только на некоторых устройствах ИБП): Для переопределения параметра Задержка при отключении питания установите флажок Никогда . В этом случае возможно только действие Выключение .
Продолжительность перезагрузки	При включении данной группы розеток: • Если в качестве действия выбирается Переагрузка , то группа розеток немедленно отключается и затем ждет включения с задержкой (значение в секундах зависит от конкретного устройства ИБП). • Если в качестве действия выбирается Задержка перезагрузки , то время ожидания перед включением группы равно сумме трех задержек: Задержка при отключении питания перед отключением, Продолжительность перезагрузки и Задержка при включении питания перед включением.
Минимальное время автономной работы на выходе	Перед повторным включением ИБП должен обеспечить определенное минимальное время для поддержки нагрузки.

Параметры сброса нагрузки. Настройки зависят от модели ИБП. Используйте параметры сброса нагрузки, чтобы определить, как ИБП будет реагировать на сигналы тревоги. ИБП обеспечивает автоматический программируемый сброс нагрузки при возникновении неполадок с входным напряжением или при снижении емкости батареи, а также автоматический программируемый запуск групп розеток после устранения неполадок.

Настройка	Описание
Настройки, отключающие эту группу розеток (некоторые из них доступны не для всех групп розеток)	<ul style="list-style-type: none"> • Когда сбой питания длится больше указанного времени в секундах. • Когда оставшееся время автономной работы ИБП меньше заданного значения в секундах. • ИБП перегружен (требования к питанию устройств, подключенных к ИБП, превышают мощность, которую может обеспечить ИБП). • Устройство пропускает задержки отключения розеток. (Отключение группы происходит немедленно без ожидания времени, задаваемого в секундах в параметре Задержка при отключении питания. По умолчанию этот параметр отключен.) • Устройство остается выключенным после восстановления питания. (Остается выключенным после восстановления переменного напряжения в сети. Этот параметр отключен по умолчанию, и ИБП ждет в течение определенного времени, задаваемого в секундах в параметре Задержка при включении питания, а затем включает группы розеток.)
Настройки для включения данной группы розеток	<ul style="list-style-type: none"> • Группа розеток находится в режиме ожидания в течение заданного времени, указанного в секундах. • Батарея перезаряжается до заданного значения емкости в процентах от полной емкости.

События и прерывания для группы розеток. Изменение состояния группы розеток генерирует событие **ИБП: Группа розеток включена** со степенью серьезности «Информационная» или **ИБП: Группа розеток выключена** со степенью серьезности «Предупредительное». Формат сообщения о событиях — «UPS: Группа розеток *номер_группы*, *имя_группы*, *действие* по *причине*». Например:

UPS: Outlet Group 1, Web Server, turned on.

UPS: Outlet Group 3, Printer, turned off.

По умолчанию событие генерирует запись в журнале событий, в электронной почте и в системном журнале (Syslog).

При настройке приемников прерывания для событий генерируется прерывание 298 во время включения группы розеток и 299 — при выключении группы розеток. Сообщение о событии является аргументом прерывания. Уровень серьезности по умолчанию такой же, как и для события.

Параметр настроек питания

Данный параметр доступен для всех моделей ИБП, кроме MGE Galaxy 300 и MGE Galaxy 7000.



Разрешенные настройки зависят от модели ИБП. Подробная информация о полях и значениях в параметре **питание** для Вашей модели ИБП приводится в интерактивной справке.

Можно настраивать следующие позиции, зависящие от модели:

- Настройки **Напряжение**, определяющие напряжение, при котором начинается автоматическое регулирование напряжения в ИБП или происходит переход на работу от батареи, что определяет чувствительность ИБП к изменениям напряжения.
- Настройки **Байпас** определяют условия, при которых ИБП может переключаться в режим байпаса.
- **Сигнальные пороговые значения** на основании располагаемого времени работы и резервирования питания, а также для нагрузки ИБП.

Параметр выключения

Эти параметры позволяют использовать утилиту сетевого выключения PowerChute для выключения до 50 серверов в сети, где используется клиентская версия этой утилиты:

Настройка	Описание
Продолжительность работы при низком заряде батареи	Время, в течение которого ИБП может работать после появления сигнала низкого напряжения батареи. Примечание. Эта настройка также определяет время, необходимое PowerChute для безопасного выключения серверов в соответствии с параметром Инициировать сетевое выключение PowerChute меню Планирование .
Макс. требуемая задержка	Указывает задержку, определяемую настройкой Макс. требуемая задержка , доступ к которой выполняется через параметр PowerChute на левом меню навигации. Примечание. Сведения о функциях PowerChute, включая определение параметра Максимальное время выключения см. в разделе «Эти параметры позволяют использовать утилиту сетевого выключения PowerChute для выключения до 50 серверов в сети, где используется клиентская версия этой утилиты:» на стр. 45.
Задержка выключения	Для устройств SMX, SMT и SURTD UPS этот параметр применяется только к синхронизированной группе управления. Время ожидания отключения ИБП после получения команды на отключение.
Выключение основной сигнализации	Если включен этот параметр, обеспечивается безопасное отключение системы и уведомление, при этом не используются расширенные функции расширенной аварийной сигнализации. Установите выключение по срабатыванию основной сигнализации, если Ваш компьютер подключен к ИБП с помощью кабеля базовой сигнализации и если модель Вашего ИБП не поддерживает расширенную сигнализацию или ИБП настроен только на основную сигнализацию.
Основная продолжительность работы при низком заряде батареи	Предусматривается только для некоторых моделей ИБП. Определяет возможное время работы от батареи, через которое ИБП передает сигнал для выключения батареи с низким зарядом, если включена система выключения основной сигнализации.
Время в спящем режиме	Время, в течение которого ИБП находится в спящем режиме (отключено выходное напряжение), при использовании в заголовке Управление параметра Перевести ИБП в спящий режим .

Настройка	Описание
Продолжительность времени автономной работы на выходе	Большинство ИБП поддерживает одну из следующих настроек, чтобы обеспечить время для зарядки своих батарей. Затем, если происходит сбой питания вскоре после запуска, ИБП может выполнить мягкое отключение. (До включения ИБП должно пройти некоторое время, задаваемое параметром Задержка возврата .)
Минимальная емкость батареи	Продолжительность времени автономной работы на выходе: время, в течение которого ИБП должен поддерживать работу нагрузки за счет энергии батареи, чтобы ИБП вышел из спящего режима (или включился при перезагрузке) и обеспечивал выходное напряжение. Минимальная емкость батареи: минимальная емкость батареи в процентах от полной емкости, необходимая для того, чтобы ИБП вышел из спящего режима (или включился при перезагрузке) и обеспечивал подачу выходного напряжения.
Задержка возврата	Для устройств SMX, SMT и SURTD UPS этот параметр применяется только к синхронизированной группе управления. Продолжительность ожидания до включения ИБП после отключения, вызванного сбоем питания, или запланированного выключения. ПРИМЕЧАНИЕ. ИБП должен также обладать емкостью, задаваемой настройкой Минимальная емкость батареи , или обеспечивать время работы до включения, задаваемое в параметре Продолжительность времени автономной работы на выходе .
Макс. требуемая задержка - Вынужденное согласование	Отображается задержка, необходимая для того, чтобы у каждого клиента PowerChute было время для безопасного выключения, если ИБП или клиент PowerChute запускает безопасное отключение. Если установлен флажок Вынужденное согласование , то PowerChute опрашивает каждый сервер в списке как клиента сетевого выключения PowerChute для получения информации о времени, необходимом для безопасного выключения. Программа PowerChute пересчитывает эту задержку каждый раз при включении интерфейса ПСУ ИБП или при сбросе. Этот параметр недоступен на MGE Galaxy 300 и MGE Galaxy 7000. Макс. требуемая задержка — наибольшая задержка выключения, которая нужна каждому серверу из списка плюс дополнительные 2 минуты на случай непредвиденных обстоятельств. Согласование может занимать до 10 минут. Если элемент Вынужденное согласование не выбран, то для всех клиентов задержка выключения устанавливается по умолчанию на 2 минуты.
Поведение в режиме «От батареи»	После того как клиенты сетевого выключения PowerChute выключают свои компьютерные системы, этот параметр определяет, будет ли ИБП включаться автоматически или его нужно будет включить вручную после восстановления входного питания. Примечание. Этот параметр недоступен на ИБП MGE Galaxy 300 и MGE Galaxy 7000.
Фраза аутентификации	Фраза, зависящая от регистра, длиной от 15 до 32 символов ASCII должна использоваться во время аутентификации MD5 для PowerChute. Настройка администратора по умолчанию admin user phrase .

Контролируемое раннее выключение. Эти функции доступны не для всех ИБП. С их помощью можно выключить работающий от батареи ИБП при наступлении заданных условий:

- при превышении времени работы от батареи в минутах;
- при достижении минимального остаточного времени работы ИБП в минутах;
- при снижении нагрузки на ИБП до заданного значения в процентах.

В случае настройки этих условий ИБП выключается при наступлении *любого* из условий.

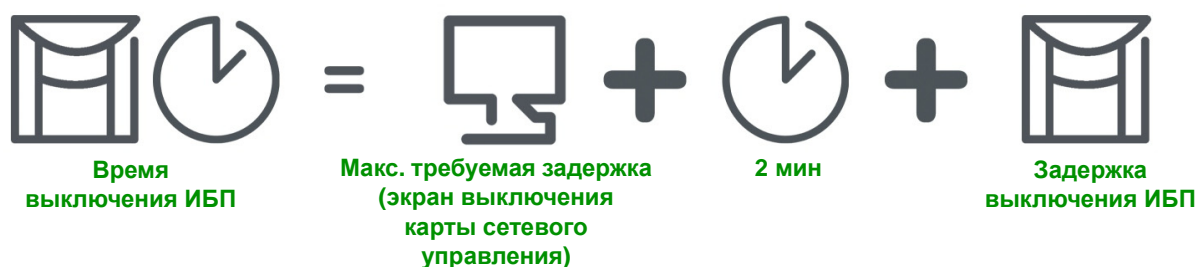
Также можно указать, следует или нет включать ИБП после восстановления питания в сети.

Рекомендуется не использовать данные функции совместно с программным обеспечением, управляющим отключением серверов. Например, можно выбрать пункт **Игнорировать команды выключения PCNS** в разделе **Поведение в режиме «От батареи»** (в нижней части этого экрана). При этом алгоритм выключения ИБП в режиме «От батареи» будет определяться картой сетевого управления, а не PowerChute Network Shutdown.

Задержка выключения и вынужденное согласование. Время выключения ИБП рассчитывается по-разному для устройств *без* групп розеток и устройств *с* группами розеток.

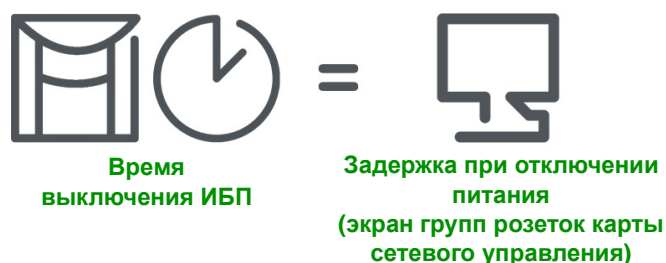
1. Для устройств без групп розеток время выключения — это значение **Макс. требуемая задержка** на экране **Выключение** карты сетевого управления *плюс* 2 минуты *плюс* время задержки выключения ИБП.

ИБП без групп розеток: время выключения



2. Для устройств с группами розеток время выключения — это значение **Задержка при отключении питания** на экране **Группы розеток** карты сетевого управления. (Эта функция доступна не для всех ИБП.)

ИБП с группами розеток: время выключения



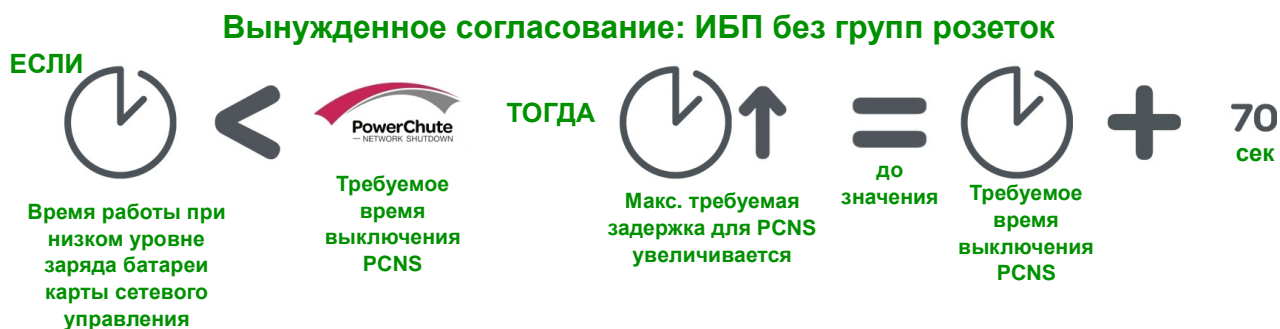
Обратите внимание, что устройства SUM функционируют в соответствии с первым, а не со вторым вариантом.

Время выключения для обоих типов ИБП согласуется картой сетевого управления и PowerChute Network Shutdown (PCNS).

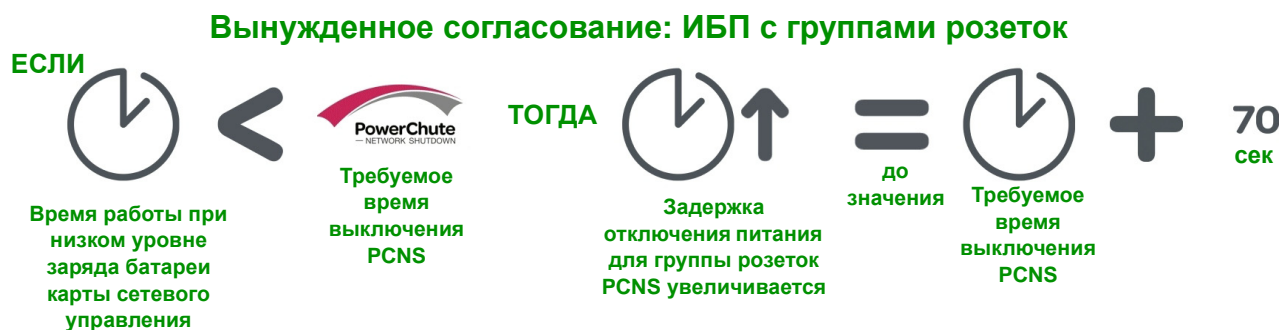
Используйте функцию **Вынужденное согласование**, чтобы перенастроить время задержки при изменении или добавлении клиента PCNS. При выборе этой функции и нажатии кнопки «Применить» операция выполняется автоматически. Подробности приведены ниже.

PCNS анализирует значение параметра **Продолжительность работы при низком заряде батареи** карты сетевого управления, сравнивает его с собственным значением времени выключения и, в случае если время работы от батареи слишком мало, направляет карте сетевого управления сигнал об увеличении значений для указанных ниже пунктов 1 и 2 до уровня **ТРЕБУЕМОЕ ВРЕМЯ ВЫКЛЮЧЕНИЯ PCNS* плюс 70 секунд**.

1. Без групп розеток, Макс. требуемая задержка.



2. С группами розеток, Задержка отключения питания для группы розеток, питающих клиента PCNS.



* ТРЕБУЕМОЕ ВРЕМЯ ВЫКЛЮЧЕНИЯ PCNS = задержка выключения + время действия команды выключения. При добавлении значения по умолчанию 70 сек. время округляется до ближайшей минуты. Например, общее время 3 мин. 50 сек. округляется до 4 мин.; общее время 2 мин. округляется до 3 мин.



Примечания:

70 сек. — это стандартное время выключения операционной системы для PCNS. PCNS не изменяет значение **Продолжительность работы при низком заряде батареи** карты сетевого управления. Значение **Макс. требуемая задержка PCNS v3.x** не используется картой сетевого управления по отношению к ИБП с группами розеток.

Параметр «Общие»

Настройки зависят от модели ИБП. Каждая модель ИБП поддерживает только некоторые функции из перечисленных ниже:

Настройка	Описание
Имя ИБП	Имя для идентификации ИБП.
Позиция ИБП	Физическая установка ИБП: установка в стойке или в виде отдельного блока (напольная).
Звуковой сигнал тревоги	Включение или выключение звуковой сигнализации, а для некоторых моделей ИБП можно задать условие, при котором работает звуковая сигнализация.

Настройка	Описание
Последняя замена батареи	Месяц и год последней замены батарей.
Число батарей или Внешние батареи	Количество батарей, исключая встроенные батареи, имеющиеся в ИБП. На некоторых моделях, в которых используется более 16 батарей, нужно добавлять по 16 батарей (16, 32, 48 и т. д.), но затем это число можно скорректировать до нужного значения.
Внешний батарейный шкаф	Нормированные ампер-часы (емкость батарей) батарейного шкафа для внешнего батарейного источника питания.

Параметр расписания самодиагностики

Используйте этот параметр для настройки времени запуска самодиагностики на ИБП.

Параметр обновления прошивки

Используйте этот параметр для запуска обновления прошивки ИБП. Файл обновления прошивки должен быть предварительно загружен на ПСУ с использованием протокола FTP и сохранен в каталоге /upswf/.

Параметр клиентов PowerChute

Щелкните **Добавить клиент**, чтобы добавить IP-адрес нового клиента сетевого выключения PowerChute. Для удаления клиента щелкните IP-адрес этого клиента в списке, а затем щелкните **Удалить клиент**.

В этом списке может быть до 50 IP-адресов клиентов.



Примечание. При установке клиента сетевого выключения PowerChute в сети он автоматически добавляется в список, при удалении клиента сетевого выключения он автоматически удаляется из списка.

Параметр управления синхронизацией



Примечание. Страница «Управление синхронизацией» недоступна на ИБП MGE Galaxy 300 и MGE Galaxy 7000, а также на ИБП Symmetra.

Процесс синхронизации. Если какое-либо действие выполняется для синхронизированной группы управления, то включенные члены группы ведут себя следующим образом.

- Каждый ИБП получает команду независимо от выходного состояния (например, низкого напряжения батареи).
- При работе используются выдержки времени, (например, **Задержка выключения**, **Время в спящем режиме** и **Задержка возврата**), настроенные для запускающего ИБП.
- В начале работы ИБП, который не может принять участие в действии, сохраняет свое текущее состояние, в то время как остальные ИБП выполняют действия. Если выход ИБП уже находится в состоянии, которое требуется при работе (например, ИБП уже был отключен при запуске и перезагрузке), то в журнале ИБП событие регистрируется, и ИБП выполняет оставшиеся действия.
- Все ИБП, участвующие в процессе, синхронизируют свою работу (в течение одной секунды при идеальных условиях в случае ИБП Smart-UPS, но иногда и дольше).

- При перезагрузке или в спящем режиме.
 - Непосредственно перед началом запуска ИБП находится в режиме ожидания в течение времени, которое указано в параметре **Задержка возврата**, по умолчанию оно может составлять до 120 с (настраивается в параметре **Задержка при синхронизации мощности**) для любого ИБП, у которого нет питания на входе для восстановления питания. Любой ИБП, который не может восстановить питание на входе во время этой задержки, не участвует в синхронизированном перезапуске и ждет восстановления входного питания до перезапуска.
 - Светодиодные индикаторы на передней панели ИБП не мигают поочередно, как это бывает при обычной (не синхронизированной) перезагрузке или переходе в спящий режим.
- О состоянии и событиях ИБП при синхронной работе сообщается так же, как и в случае отдельных ИБП.

Указания для синхронизированных групп управления. Перед тем как настроить данный ИБП для работы в синхронизированной группе управления, ознакомьтесь с приведенными ниже указаниями.

- Все ИБП в синхронизированной группе управления должны быть одной модели.
- Синхронизированные группы управления поддерживаются любым ИБП Smart-UPS со слотом для установки платы сетевого управления.
- Если установлена принадлежность к синхронизированной группе управления, ПСУ блокирует последовательный порт связи ИБП с подключенным устройством управления. Однако ПСУ по-прежнему обеспечивает доступ к интерфейсу командной строки через последовательный порт связи.

Отображение состояния устройства, входящего в синхронизированной группы управления. При включении устройства в группу на дисплее отображается приведенная ниже информация о принадлежности данного устройства к синхронизированной группе управления.

Элемент состояния	Описание
IP-адрес	IP-адрес платы сетевого управления для данного члена группы (ИБП).
Входное состояние	Состояние входного питания для данного члена группы: работает (допустимо) или неисправен (недопустимо).
Выходное состояние	Состояние выходного питания для данного члена группы: Вкл. или Выкл.

Настройка устройства синхронизированной группы управления

Параметр	Описание
Членство в группе	Определяет, является ли член синхронизированной группы управления активным членом этой группы. Если Вы отключаете членство в группе, то данный ИБП функционирует так, как будто он не был членом синхронизированной группы управления. Если Вы подключаете или отключаете членство в группе, то такое изменение вызывает перезагрузку интерфейса управления после следующего выхода из системы. Изменения входят в силу именно в этот момент.
Номер группы управления	Уникальный идентификатор группы синхронизированного управления, членом которой является ИБП с данной ПСУ. Это значение может представлять собой номер от 1 до 65534. ИБП может быть членом только одной синхронизированной группы управления. Все члены синхронизированной группы управления должны иметь одинаковый номер группы управления и групповой IP-адрес.
Групповой IP-адрес	IP-адрес, используемый для связи с членами синхронизированной группы управления. Для IPv6 может использоваться любой действительный групповой адрес IPv6. Для IPv4 допустимый диапазон адресов: 224.0.0.3 – 224.0.0.254. Все члены синхронизированной группы управления должны иметь одинаковый номер группы управления и групповой IP-адрес.
Задержка при синхронизации мощности	Максимальное время (по умолчанию 120 с), в течение которого запускающий ИБП находится при необходимости в режиме ожидания, чтобы остальные устройства группы могли восстановить уровень входного напряжения, при котором произойдет включение запускающего ИБП. По истечении этой задержки запускающий ИБП ждет перезарядки батареи для времени автономной работы, заданного в параметре «Продолжительность времени автономной работы на выходе», или достижения емкости батареи, заданной в параметре «Минимальная емкость батареи», а затем выполняется ожидание в течение времени, указанного в параметре «Задержка возврата», после чего происходит включение. ПРИМЕЧАНИЕ. Сведения о настройке параметра «Продолжительность времени автономной работы на выходе» см. в разделе «Продолжительность времени автономной работы на выходе» на стр. 46. Сведения о настройке параметра «Минимальная емкость батареи» см. в разделе «Минимальная емкость батареи» на стр. 46.

Параметр	Описание
Минимальная погрешность емкости батареи или Погрешность продолжительности времени автономной работы на выходе	ИБП поддерживает только один из этих параметров в зависимости от модели. Это значение можно устанавливать различным для каждого члена синхронизированной группы управления через интерфейс управления этого устройства. Минимальная погрешность емкости батареи: часть емкости батареи в процентах, которая вычитается из минимальной емкости батареи запускающего синхронизацию ИБП, которая определяет емкость батареи для данного члена группы, необходимую для его включения во время действий синхронизации. Сведения о настройке параметра «Минимальная емкость батареи» см. в разделе «Минимальная емкость батареи» на стр. 46. Погрешность продолжительности времени автономной работы на выходе: время в секундах, которое вычитается из продолжительности времени автономной работы на выходе для ИБП, который запускает синхронизацию, для определения допустимого времени автономной работы, необходимого для данного члена группы, чтобы включиться во время действий синхронизации. Сведения о настройке параметра «Продолжительность времени автономной работы на выходе» см. в разделе «Продолжительность времени автономной работы на выходе» на стр. 46.
Фраза аутентификации	Фраза, зависящая от регистра (от 15 до 32 ASCII символов), используется для аутентификации синхронизированной группы управления. Все члены синхронизированной группы управления должны иметь одну и ту же фразу аутентификации. По умолчанию используется SCG auth phrase .
Фраза шифрования	Шифровальный ключ для протокола, обеспечивающего безопасность связи членов синхронизированной группы управления. Все члены синхронизированной группы управления должны иметь одну и ту же фразу шифрования. По умолчанию используется SCG crypt phrase .
Порт синхронизированного управления	Сетевой порт, который синхронизированные группы управления используют для связи. Используйте любой нестандартный порт от 5000 до 32768.

Параметр для параллельных блоков (ИБП Smart-UPS VT)

Настройка	Описание
Конфигурация параллельного блока	Приводится список параллельных блоков (ИБП одного типа с общей нагрузкой, которые обеспечивают подачу питания на нагрузку в случае неисправности параллельного блока). Первым указывается ИБП, в систему которого Вы вошли.
Добавить блок	Используйте эту кнопку для добавления блока (максимум 9 блоков) или для изменения имени настроенного блока. Укажите имя блока (до 8 символов) и его IP-адрес.

Страница «Диагностика»

Для любого ИБП этой компании можно выполнить самодиагностику или калибровку времени автономной работы. Тестирование звукового сигнала тревоги ИБП зависит от конкретной модели и может отсутствовать в Вашем ИБП.



Примечание. Страница «Диагностика» недоступна на ИБП MGE Galaxy 300 и MGE Galaxy 7000.

Поле	Описание
Самодиагностика	Результат (успешный, сбой или отсутствует) и дата последней самодиагностики ИБП.
Калибровка	Результат последней калибровки времени автономной работы. При калибровке выполняется пересчет оставшегося времени работы и требуется выполнение следующих условий. <ul style="list-style-type: none">• Поскольку при калибровке существенно расходуется ресурс батарей ИБП, необходимо выполнять калибровку при 100% зарядке батарей.• Для некоторых ИБП нагрузка при калибровке должна быть не менее 7%.
Запустить	Выберите процедуру диагностики для немедленного выполнения: тестирование звукового сигнала тревоги ИБП, самодиагностика ИБП или калибровка времени автономной работы. При тестировании звукового сигнала тревоги члена синхронизированной группы управления выполняются следующие действия. <ul style="list-style-type: none">• В веб-интерфейсе этот параметр проверяет сигналы тревоги всех подключенных членов группы.• В SNMP можно установить upsAdvControlFlashAndBeep в идентификаторе объекта на flashAndBeep (2) для тестирования отдельного ИБП или на flashAndBeepSyncGroup (3) для тестирования сигналов тревоги всех членов группы.

Страница «Планирование» (для выключений)



Примечание. Страница **Планирование** - ИБП недоступна на ИБП MGE Galaxy 300 и MGE Galaxy 7000.

Для обоих параметров ИБП и групп розеток

Можно настроить выключение — для ИБП в области **ИБП** или для отдельной группы розеток (если возможно) в области **Группы розеток**.

При выборе ИБП или групп розеток настроенные расписания отображаются вдоль верхней части страницы с подробными сведениями, включая сведения о текущем состоянии.

Редактирование, включение, отключение или удаление запланированного выключения. Щелкните имя расписания в списке расписаний в верхней части страницы **ИБП** или **Группы розеток**, чтобы получить доступ к просмотру и изменению параметров запланированного выключения, включая его временное отключение с помощью снятия флажка **Включить** или окончательное удаление.

Создание расписания выключений ИБП или группы розеток.

1. Выберите **ИБП** или **Группа розеток** в области **Планирование**.
2. Выберите тип выключения для планирования — **Одноразовое выключение**, **Ежедневное выключение** или **Еженедельное выключение** (через 1, 2, 4 или 8 недель), а затем щелкните кнопку **Далее**.
3. Чтобы временно отключить расписание, снимите флажок **Включить**.
4. Укажите имя, а также дату и время для расписания.
Для еженедельного выключения укажите интервал в раскрывающемся поле.
5. Укажите, должно ли устройство или группа розеток повторно включаться после выключения:

Повторное включение: укажите, будет ли включаться ИБП в конкретный день и в конкретное время: **Никогда** (ИБП включается вручную) или **Немедленно** (ИБП включается через 6 мин, и время указывается как «Задержка возврата»).



Описание настройки параметра «Задержка возврата» см. в разделе «Задержка возврата» на стр. 46

6. Только для группы розеток укажите группу, щелкнув соответствующую кнопку.
7. **Клиенты сетевого выключения по сигналу PowerChute:** укажите, следует ли уведомлять клиентов, указанных как «Параметр клиентов PowerChute».

Только для параметра ИБП

Планирование синхронизированного выключения. Все запланированные выключения будут синхронизированы, если ИБП, ПСУ которого запускает выключение, является членом синхронизированной группы управления, и он как член группы находится во включенном состоянии. Всегда планируйте все выключения через одного и того же члена группы. Чтобы произошло синхронизированное выключение ИБП, в то время, на которое запланировано действие подключения, должно обеспечиваться сетевое подключение к каждому ИБП.



Внимание! Не планируйте выключения через более чем одного члена группы. Такое планирование может дать непредсказуемые результаты.

Страница «О программе»

Этот параметр позволяет получить сведения об ИБП и прошивке платы сетевого управления.

- **Модель:** название модели ИБП.
- **Позиция:** физическая ориентация ИБП в стойке или **напольная** (только для моделей ИБП, предназначенных для стоек или напольной установки). (Этот параметр недоступен на моделях MGE Galaxy 300 и MGE Galaxy 7000.)
- **Серийный номер:** уникальный идентификационный номер ИБП, указываемый также на корпусе ИБП.
- **Версия прошивки:** номера версий модулей прошивки, установленных в ИБП.
- **Дата изготовления:** дата завершения изготовления данного ИБП. (Этот параметр недоступен на моделях MGE Galaxy 300 и MGE Galaxy 7000.)

На устройствах ИБП MGE Galaxy 300 и MGE Galaxy 7000 доступна следующая дополнительная информация:

- **Название продукта:** торговое название ИБП.
- **Технический уровень:** технический уровень ИБП.
- **Время ИБП:** местное время для расположения ИБП.
- **Страна:** страна, в которой находится ИБП (только для MGE Galaxy 7000).
- **Название производителя:** производитель ИБП.

Контроль окружающей среды



Примечание: Если вы устанавливаете для своей платы управления устройство ввода-вывода с сухими контактами, AP9810, то на вкладке **Окружающая среда** отображается два варианта в строке меню **Универсальный ввод-вывод** и **Окружающая среда**. Настройки, описанные в данной главе, используются для обоих вариантов, если не оговорено особо.

Страница обзора

На странице **Обзор** перечислены устройства контроля состояния окружающей среды, связанные с сетевой платой управления AP9631 в ИБП.

Заголовок	Отображаемая информация
Температура и влажность	Перечислены все датчики, и для каждого датчика даются записи аварийного состояния, текущей температуры и влажности (если поддерживается). Для получения подробных сведений о состоянии или для настройки параметров датчика нажмите на имя датчика.
Входные контакты	Приводится список всех действующих входных контактов, состояние их сигналов тревоги и текущее состояние (замкнут или разомкнут). Для получения подробных сведений о включенном входном контакте или настройке параметров контакта нажмите на имя контакта. Примечание: Для просмотра или настройки отключенного контакта, а также для его включения, необходим выход на страницу интерфейса для этого контакта с помощью заголовка Входные контакты на левой панели меню управления.
Выходное реле	Приводится список аварийных состояний и текущего состояния (включено или выключено) выходного реле встроенного блока контроля параметров окружающей среды. Для получения подробной информации о статусе этого выходного реле или настройки его параметров нажмите на его имя.
Последние события в окружающей среде	В поле Последние события в окружающей среде приводится в обратном хронологическом порядке список последних событий в окружающей среде. Для просмотра всего журнала событий нажмите клавишу Дополнительные события внизу справа.

Страница температуры и влажности

Краткое описание состояния

Нажмите заголовок **Температура и влажность** на левой панели меню управления, чтобы отобразить имя, состояние аварийной сигнализации, температуру и влажность (если поддерживается) для каждого датчика.

Подробное описание состояния и конфигурации

Нажмите имя датчика для получения подробного описания состояния тревоги или для настройки значений его параметров.

Идентификация и состояние сигналов тревоги.

Параметр	Описание
Имя	Имя датчика. <i>Максимум:</i> 20 символов.
Местоположение	Это физическое местоположение датчика. <i>Максимум:</i> 20 символов.

Параметр	Описание
Состояние тревоги	Возможна одна из следующих ситуаций: <ul style="list-style-type: none"> • Нормальное, если датчик не сообщает об аварийной ситуации. • При возникновении тревожной ситуации, текст аварийного сообщения указывает на нарушение порогового значения, а опасность сигнала тревоги указывается цветом (красный - для критической, оранжевый - для предупредительной).
Пороговые значения	В следующих двух разделах дается описание настраиваемых пороговых значений и гистерезиса .

Пороговые значения. Для каждого датчика задаются одинаковые пороговые значения температуры и влажности (если поддерживается такое измерение).

Пороговое значение	Описание
Максимум	При превышении порогового значения максимальной температуры или максимальной влажности для датчика формируется сигнал тревоги.
Высокое	При превышении порогового значения высокой температуры или высокой влажности для датчика формируется сигнал тревоги.
Низкое	Если температура или влажность опускается ниже нижнего порогового значения для датчика, то формируется сигнал тревоги.
Минимум	Если температура или влажность опускается ниже минимального порогового значения для датчика, то формируется сигнал тревоги.

Гистерезис. Это значение указывает, как далеко нужно перейти пороговое значение температуры или влажности, чтобы вернуться в состояние до нарушения порогового значения.

- Для нарушения пороговых значений Максимум и Высокое, точка стирания - это пороговое значение минус гистерезис.
- Для нарушения пороговых значений Минимум и Низкое, точка стирания - это пороговое значение плюс гистерезис.

Следует увеличить гистерезис температуры или гистерезис влажности, чтобы избежать появления многочисленных сигналов тревоги, если температура или влажность, вызвавшая это нарушение, незначительно колеблется. Если значение гистерезиса слишком мало, то такие колебания могут многократно вызывать и устранять нарушения порогового значения.

Пример падения температуры с колебаниями. Минимальное пороговое значение температуры составляет 12,7°C (55°F), а гистерезис температуры - 1,6°C (3°F). Температура падает ниже 12,8°C (55°F), нарушая пороговое значение. Затем она поднимается до 13,3°C (56°F) и снова опускается до 11,7°C (53°F), не доходя до точки стирания события и не вызывая нового нарушения порогового значения. Для удаления имеющегося нарушения необходимо, чтобы температура поднялась выше 14,4°C (58°F) (на 1,6°C (3°F) больше порогового значения).

Пример повышения влажности с колебаниями. Максимальное пороговое значение влажности составляет 65%, а гистерезис влажности равен 10%. Влажность повышается до 65%, приводя к нарушению порогового значения. Затем она опускается до 60% и снова поднимается до 70%, не доходя до точки стирания события и не вызывая нового нарушения порогового значения. Для удаления имеющегося нарушения необходимо, чтобы влажность опустилась ниже 55% (на 10% меньше порогового значения).

Страница входных контактов

Краткое описание состояния

Нажмите на заголовок **Входные контакты** на левой панели меню управления для отображения имени, состояния сигнализации и состояния (замкнут или разомкнут) для каждого входного контакта.

Подробное описание состояния и конфигурации

Нажмите имя входного контакта для получения подробного описания состояния тревоги или для настройки значений.

Параметр	Описание
Входной контакт	Подключение или отключение данного входного контакта. При отключении данный контакт не формирует сигнала тревоги, даже если он находится в ненормальном положении
Имя	Имя данного входного контакта. <i>Максимум: 20 символов.</i>
Расположение	Положение данного входного контакта. <i>Максимум: 20 символов.</i>
Состояние тревоги	Нормальное , если данный входной контакт не сообщает о сигнале тревоги или не сообщает о степени опасности при сообщении о сигнале тревоги.
Состояние	Текущее состояние данного входного контакта. Закрыто или Открыто .
Нормальное состояние	Нормальное (неаварийное) состояние данного входного контакта. Закрыто или Открыто .
Степень опасности	Степень опасности сигнала тревоги, генерируемого ненормальным состоянием данного входного контакта: Предупредительное или Критическая .

Страница выходного реле

Эта опция предусмотрена только для устройств с установленным вспомогательным устройством ввода-вывода с сухими контактами. Выберите вкладку **Окружающая среда**, затем **Универсальный ввод-вывод** в верхней строке меню. Нажмите заголовок **Выходное реле** для отображения состояния выходного реле и настройки значений.

Параметр	Описание
Имя	Имя выходного реле. <i>Максимум: 20 символов.</i>
Местоположение	Положение данного выходного реле. <i>Максимум: 20 символов.</i>
Состояние тревоги	Нормальное , если данное выходное реле не сообщает о сигнале тревоги или не сообщает о степени опасности при сообщении о сигнале тревоги.
Состояние	Текущее состояние данного выходного реле. Закр ыто или Откр ыто.
Нормальное состояние	Нормальное (неаварийное) состояние данного выходного реле. Закр ыто или Откр ыто.
Управление	Пометьте настройку, чтобы изменить текущее состояние данного выходного реле.
Задержка	Время в секундах, в течение которого выбранный сигнал тревоги должен существовать, прежде чем сработает выходное реле. Используйте эту настройку, чтобы избежать активации сигнала тревоги во время коротких переходных процессов. Примечание: Даже в том случае, если после начала периода задержки формируются дополнительные сигналы тревоги, задержка не перезапускается, а продолжается до тех пор, пока не сработает выходное реле.
Удержание	Минимальное время в секундах, в течение которых выходное реле остается активным после подачи сигнала тревоги. Даже в случае корректировки активизирующего сигнала тревоги выходное реле остается включенным, пока не закончится данный период времени.

Страница О программе

Нажмите на заголовок **О программе** на левой панели меню управления в верхней строке меню **Окружающая среда**, чтобы отобразить устройства контроля окружающей среды, используемые в данном ИБП, и версии их аппаратных средств.

Настройка политики управления

В сетевой плате управления AP9631 с двумя подключенными устройствами с сухими контактами ввода-вывода (AP9810) можно настроить выходные контакты на реакцию на события, а ИБП и выходные контакты – на реакцию на входные сигналы тревоги.

Настройка выхода для реакции на событие

1. Выберите вкладку **ИБП**, затем **Политика управления** в верхней строке меню и **по событию** в заголовке **Действия для событий** на левой панели меню управления.
2. Нажмите на имя категории для просмотра всех событий данной категории или нажмите на имя в подразделе категории для просмотра всех событий в этом подразделе.
3. В списке событий просмотрите отмеченные графы, чтобы убедиться, что необходимое событие уже настроено на изменение состояния выходного реле.
4. Для изменения текущей конфигурации нажмите на имя события, выберите выходное реле, которое изменит состояние, когда будет обнаружено это событие, и нажмите клавишу **Применить**.

Настройка ИБП или выхода для реакции на входной сигнал тревоги.

1. Выберите вкладку **ИБП**, затем **Политика управления** в верхней строке меню и **по событию** в заголовке **Действия для событий** на левой панели меню управления.
2. Нажмите **Контакт ввода-вывода**, затем нажмите имя события, предназначенного для настройки.
3. Плата управления поддерживает до четырех входов. Необходимо указать вход, который будет связан с этим событием.
 - a. В разворачивающемся списке **Порт** выберите номер Универсального порта датчика (**1** или **2**), к которому подключается устройство ввода-вывода с сухим контактом.
 - b. В разворачивающемся списке **Zone** выберите букву для зоны (**A** или **B**) контакта, на который подается вход.
4. Определите операцию, которую будет выполнять ИБП при изменении состояния на входе и выберите выход, который изменит состояние при обнаружении данного события.
5. Нажмите **Отобразить** для просмотра этих изменений, а затем нажмите **Применить**.



Примечание: Настраиваемая операция происходит один раз. Если вы восстановите на входе нормальное состояние до удаления условия тревоги, то на выходе состояние не изменится пока условие тревоги не будет сброшено, а затем снова установлено.

Журналы

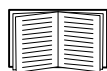
Использование журналов событий и данных

Журнал событий

Путь: **Журналы > События > опции**

Журнал событий можно просматривать, фильтровать или удалять. По умолчанию журнал отображает в обратном хронологическом порядке все события, записанные в течение последних двух дней.

Для получения списков всех настраиваемых событий и их текущих настроек выберите вкладку **Администрирование**, затем позицию **Уведомление** в верхней строке меню и **по событию** под заголовком **Действия для событий** на левой панели меню управления.



См. «Конфигурирование по событию» на стр. 85.

Для отображения журнала событий (**Журналы > События > журнал**):

- По умолчанию журнал событий можно просматривать как страницу веб-интерфейса. Самые последние события записаны на странице 1. В строке навигации под журналом выполните следующие операции.
 - Нажмите номер страницы, чтобы открыть конкретную страницу журнала.
 - Нажмите **Предыдущий** или **Следующий** для просмотра событий, записанных непосредственно до или после событий, указанных на открытой странице.
 - Нажмите << для возврата к первой странице или >> для просмотра последней страницы журнала.
- Для просмотра перечисленных на странице событий нажмите **Запустить журнал в новом окне** со страницы журнала событий, чтобы отобразить журнал в полноэкранном виде.



Примечание: В опциях вашего браузера должен быть включен JavaScript, чтобы можно было использовать кнопку **Запустить журнал в новом окне**.



Для просмотра журнала событий можно также использовать FTP или Secure CoPy (SCP). См. «Как использовать FTP или SCP для поиска файлов в журнале» на стр. 65.

Для фильтрации журнала событий (**Журналы > События > журнал**):

- **Фильтрация журнала по дате или по времени.** Для отображения всего журнала событий или для изменения количества дней или недель, для которых в журнале отображаются последние события, выберите позицию **Последнее**. Выберите временной диапазон из разворачивающегося меню, а затем нажмите **Применить**. Настройка фильтра сохраняется до перезапуска платы управления.
Для отображения событий, зарегистрированных в течение конкретного временного диапазона, выберите **С**. Укажите начальное и конечное время (в 24-часовом формате), а также даты для отображения событий, затем нажмите **Применить**. Настройка фильтра сохраняется до перезапуска платы управления.

- **Фильтрация журнала по событиям:** Для указания событий, отображенных в журналах, нажмите **Фильтровать журнал**. Снимите флажок в окне категории событий или степени опасности (серьезности) сигналов тревоги. Текст в верхнем правом углу страницы журнала событий говорит о том, что фильтр включен.
В качестве администратора нажмите **Сохранить как элемент по умолчанию**, чтобы сохранить этот фильтр для отображения журнала по умолчанию для всех пользователей. Если вы не нажимаете на позиции **Сохранить как элемент по умолчанию**, то фильтр остается активным до тех пор, пока вы его не очистите, или до перезапуска платы управления.
Для удаления активного фильтра нажмите **Фильтровать журнал**, затем **Очистить фильтр (показать все)**.

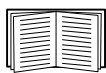


Примечание: События обрабатываются фильтром с помощью логического оператора **ИЛИ**.

- События, которые не выбраны из списка **Фильтровать по степени опасности**, никогда не отображаются в отфильтрованном журнале событий даже в том случае, если событие происходит в категории, выбранной из списка **Фильтровать по категории**.
- События, которые не выбраны из списка **Фильтровать по категории**, никогда не отображаются в отфильтрованном журнале событий даже в том случае, если устройства в данной категории переходит в состояние, вызывающее тревогу, выбранное из списка **Фильтровать по степени опасности**.

Для удаления журнала (Журналы > События > журнал):

Для удаления всех событий, записанных в журнале нажмите **Очистить журнал** на Веб-странице с отображением этого журнала. Поиск удаленных событий не выполняется.



Описание отключения регистрации в журнале событий на основании присвоенной степени опасности или категории события см. в разделе «Конфигурирование по группе» на стр. 86.

Для настройки обратного просмотра (Журналы > События > обратный просмотр):

Обратный просмотр отключен по умолчанию. Включите эту функцию, если у вас отсутствует настроенный сервер DNS или плохо работает сеть из-за плотного трафика.

Если при выключенном обратном просмотре в сети происходит событие, то и IP-адрес и имя домена сетевого устройства, связанного с этим событием, заносятся в журнал событий. Если в устройстве отсутствует запись имени домена, то в связи с событием в журнале регистрируется только IP-адрес. Поскольку доменные имена изменяются реже, чем IP-адреса, то включение обратного просмотра может улучшить идентификацию сетевых устройств, являющихся причиной возникновения событий.

Для изменения размера журнала событий (Журналы > События > размер):

По умолчанию в журнале событий может храниться до 400 событий. Количество событий, хранящихся в журнале, можно изменить. Изменение журнала событий приведет к удалению из журнала всех текущих записей. Чтобы избежать потери данных в журнале, используйте FTP или SCP для поиска (последующего восстановления) информации в журнале, прежде чем ввести новое значение в поле **Размер журнала событий**.



См. «Как использовать FTP или SCP для поиска файлов в журнале» на стр. 65.

После того как журнал заполнен, начинается удаление самых старых записей.

Журнал данных

Путь: Журналы > Данные > *опции*

Просмотр журнала измерений параметров ИБП, входа питания ИБП, а также температуры окружающей среды ИБП и батарей. Для каждой записи данных указывается время и дата регистрации.

Для отображения журнала данных (Журналы > Данные > журнал).

- По умолчанию журнал данных можно просматривать как страницу веб-интерфейса. Самые последние данные записаны на странице 1. В строке навигации под журналом выполните следующие операции.
 - Нажмите номер страницы, чтобы открыть конкретную страницу журнала.
 - Нажмите **Предыдущий** или **Следующий** для просмотра данных, записанных непосредственно до или после данных, указанных на открытой странице.
 - Нажмите << для возврата к первой странице или >> для просмотра последней страницы журнала.
- Для просмотра перечисленных на странице данных нажмите **Запустить журнал в новом окне** со страницы журнала данных, чтобы отобразить журнал в полноэкранном виде.



Примечание: В опциях вашего браузера должен быть включен JavaScript®, чтобы можно было использовать кнопку **Запустить журнал в новом окне**.



Для просмотра журнала данных можно также использовать FTP или SCP. См. «Как использовать FTP или SCP для поиска файлов в журнале» на стр. 65.

Для фильтрации журнала по данным или времени (Журналы > Данные > журнал):

Для отображения всего журнала данных или для изменения количества дней или недель, для которых в журнале отображаются последние данные, выберите позицию **Последнее**. Выберите временной диапазон из разворачивающегося меню, а затем нажмите **Применить**. Настройка фильтра сохраняется до перезапуска устройства.

Для отображения данных, зарегистрированных в течение конкретного временного диапазона, выберите **С**. Укажите начальное и конечное время (в 24-часовом формате), а также даты для отображения данных, а затем нажмите **Применить**. Настройка фильтра сохраняется до перезапуска устройства.

Для удаления журнала данных:

Для удаления всех данных, записанных в журнале, нажмите **Очистить журнал данных** на странице с отображением этого журнала. Поиск удаленных данных не выполняется.

Для установки интервала сбора данных (Журналы > Данные > интервал).

Определите в настройке **Интервал журнала**, как часто производится выборка и сохранение данных в журнале данных и просмотрите расчет количества дней, в течение которых возможно сохранение информации на основании выбранного интервала. После того как журнал заполнен, начинается удаление самых старых записей. Чтобы избежать автоматического удаления старых данных, включите и настройте обновление журнала данных в соответствии с описанием в следующем разделе.

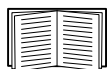
Для настройки обновления журнала данных (Журналы > Данные > обновление):

Создайте защищенный паролем архив журнала данных на указанном FTP-сервере. Включение обновления вызывает прикрепление содержимого журнала данных к файлу с указанным вами именем и местоположением. Обновление этого файла происходит с заданным интервалом загрузки.

Параметр	Описание
Обновление журнала данных	Включение или отключение (по умолчанию) обновления журнала данных.
Адрес FTP-сервера	Местоположение FTP-сервера, на котором хранится файл с архивом данных.
Имя пользователя	Имя пользователя, необходимое для отправки данных в файл с архивом данных. Данный пользователь должен обладать правом доступа к чтению и записи данных в файле архива и к каталогу (папке), в котором этот файл хранится.
Пароль	Пароль, необходимый для отправки данных в файл с архивом данных.
Путь к файлу	Путь к файлу архива данных.
Имя файла	Имя файла архива данных (тестовый ASCII файл).
Задержка X часов между загрузками.	Количество часов между загрузками данных в файл.
Загружать каждые X минут	Количество минут между попытками загрузить данные в файл после сбоя загрузки.
До X раз	Максимальное количество попыток загрузки после исходного сбоя.
До успешного завершения загрузки	Попытка загрузки файла до завершения передачи.

Для изменения размера журнала данных (Журналы > Данные > размер):

По умолчанию в журнале данных может храниться до 400 событий. Количество записей данных, хранящихся в журнале, можно изменить. Изменение размера журнала данных приведет к удалению из журнала всех текущих записей. Чтобы избежать потери данных в журнале, используйте FTP или SCP для поиска в журнале, прежде чем ввести новое значение в поле **Размер журнала данных**.



См. «Как использовать FTP или SCP для поиска файлов в журнале» на стр. 65.

После того как журнал заполнен, начинается удаление самых старых записей.

Как использовать FTP или SCP для поиска файлов в журнале

Администратор или Пользователь устройства может использовать FTP или SCP для поиска разделенного табуляторами файла регистрации событий (*event.txt*) или файла регистрации данных (*data.txt*) и импортирования его в электронные таблицы.

- Файл содержит отчет обо всех событиях и данных с момента последнего удаления журнала или (для журнала данных) усечения после достижения максимального размера.
- Этот файл включает в себя информацию, которая не отображается в файле событий или в файле данных.
 - Версия формата файла (первое поле)
 - Дата и время поиска файла
 - **Имя, Контакт и Расположение**, а также IP-адрес платы управления
 - Уникальный **Event Code** для каждого зарегистрированного события (только файл *event.txt*)



Примечание: В плате управления для записей в журнале используется четырехразрядная запись года. Вы можете выбрать четырехразрядный формат даты в своей программе электронных таблиц для отображения всех четырех разрядов.

Если вы используете протоколы защиты на основе шифрования, то для поиска файла журнала применяется SCP.

Если вы используете нешифрованные методы аутентификации для защиты системы, для поиска файла журнала применяется FTP.



См. *Справочник по защите*, находящийся на компакт-диске *Utility* для платы сетевого управления, а также на веб-сайте (www.apc.com) для получения сведений об имеющихся протоколах и способах установки необходимой защиты.

Использование SCP для поиска этих файлов. Чтобы использовать SCP для поиска файла *event.txt*, воспользуйтесь командой:

```
scp имя_пользователя@имя_узла_или_ip-адрес:event.txt ./event.txt
```

Чтобы использовать SCP для поиска файла *data.txt*, воспользуйтесь следующей командой:

```
scp имя_пользователя@имя_узла_или_ip-адрес:data.txt ./data.txt
```

Использование FTP для поиска этих файлов. Использование FTP для поиска файла *event.txt* или *data.txt*:

1. После появления командной подсказки наберите `ftp` и IP-адрес платы управления, а затем нажмите ENTER.

Если настройка **Порт** для опции **сервер FTP** (устанавливаемая с помощью меню **Сеть** на вкладке **Администрирование**) была изменена со значения по умолчанию (**21**), то в команде FTP необходимо использовать значение не по умолчанию. Для клиентов Windows FTP используйте следующую команду, включая пробелы. (Для некоторых клиентов FTP необходимо использовать двоеточие вместо пробела между IP-адресом и номером порта.)

```
ftp>open ip_адрес номер_порта
```



Описание установки значения порта не по умолчанию для повышения защищенности FTP-сервера приводится в разделе «Сервер FTP» на стр. 82. Можно указать любой порт от 5001 до 32768.

2. Для входа в систему используйте зависящее от регистра **Имя пользователя** и **Пароль** для Администратора или Пользователя устройства. Для Администратора **арс** - это значение для **Имени пользователя** и **Пароля** по умолчанию. Для Пользователя устройства значениями по умолчанию являются **device** для **Имени пользователя** и **арс** для **Пароля**.

3. Используйте команду **get** для передачи текста журнала на ваш локальный диск.

```
ftp>get event.txt
```

или

```
ftp>get data.txt
```

4. Для очистки содержимого любого журнала можно использовать команду **del**.

```
ftp>del event.txt
```

или

```
ftp>del data.txt
```

После этого появится запрос на подтверждение удаления.

- Если вы удаляете журнал данных, то в журнале событий записывается событие по удалению журнала.
- Если вы удаляете журнал событий, то это событие записывается в новом файле *event.txt*.

5. Наберите `quit` по подсказке `ftp>`, чтобы выйти из FTP.

Администрирование: Безопасность

Локальные пользователи

Настройка доступа пользователя

Путь: Администрирование > Безопасность > Локальные пользователи > *опции*

Учетная запись пользователя Администратор всегда обеспечивает доступ к плате управления.

Учетные записи Пользователь устройства и Пользователь только для чтения включаются по умолчанию. Для отключения Пользователя устройства или Пользователя только для чтения выберите учетную запись пользователя на левой панели меню управления, а затем снимите флаг **Включить**.

Точно таким же образом укажите зависящее от регистра имя пользователя и пароль.

Максимальная длина составляет 64 символа для имени пользователя и 64 символа для пароля.

Пустые пароли (без символов) не допускаются.



Сведения о разрешенных действиях для каждого типа учетной записи (Администратор, Пользователь устройства и Пользователь только для чтения) приведены в разделе «Типы учетных записей» на стр. 3.

Тип учетной записи	Имя пользователя по умолчанию	Пароль по умолчанию	Разрешенный доступ
Администратор	apc	apc	Веб-интерфейс и интерфейс командной строки
Пользователь устройства	device	apc	
Пользователь только для чтения	readonly	apc	Только веб-интерфейс

Удаленные пользователи

Аутентификация

Путь: Администрирование > Безопасность > Удаленные пользователи > **Метод аутентификации**

Используйте эту опцию для управления удаленным доступом к плате управления.



Сведения о локальной аутентификации (без использования централизованной аутентификации сервера RADIUS) приводятся в *Справочнике по защите* на компакт-диске *Utility* для платы сетевого управления и на веб-сайте www.apc.com.

поддерживает функции аутентификации и авторизации RADIUS (пользовательская служба удаленной аутентификации).

- Если пользователь осуществляет доступ к сетевой плате управления или к другому сетевому устройству, к которому подключен RADIUS, то аутентификационный запрос передается на сервер RADIUS, чтобы определить уровень допуска пользователя.
- Имена пользователей RADIUS, используемые в сетевой плате управления, ограничены 32 символами.

Выберите один из следующих вариантов:

- **Только локальная аутентификация:** RADIUS отключается. Включается локальная аутентификация.
- **RADIUS, затем локальная аутентификация:** Включается RADIUS и локальная аутентификация. Сначала запрашивается аутентификация от сервера RADIUS. Если сервер RADIUS не отвечает, то используется локальная аутентификация.
- **Только RADIUS:** RADIUS включается. Отключается локальная аутентификация.



Примечание: Если выбирается **Только RADIUS**, а сервер RADIUS недоступен, неправильно идентифицирован или неправильно сконфигурирован, то удаленный доступ невозможен для всех пользователей. Необходимо использовать подключение к интерфейсу командной строки по последовательному каналу связи и изменить настройку доступа на **локальная** или **radius, затем локальная** для восстановления доступа. Например, команда изменения настройки доступа на **локальная** имеет следующий вид:
`radius -a local`

RADIUS

Путь: **Администрирование > Безопасность > Удаленные пользователи > RADIUS**

Используйте эту опцию, чтобы выполнить указанные ниже операции.

- Перечислите серверы RADIUS (максимум), доступные для платы управления и период тайм-аута для каждого из них.
- Нажмите ссылку и настройте параметры для аутентификации нового сервера RADIUS.
- Нажмите на сервер RADIUS из списка для отображения и изменения его параметров.

Настройка RADIUS	Описание
Сервер RADIUS	Имя сервера или IP-адрес (IPv4 или IPv6) сервера RADIUS. Для настройки сервера нажмите на ссылку. Примечание: Серверы RADIUS используют для аутентификации пользователей порт 1812 по умолчанию. Чтобы использовать другой порт, добавьте к имени сервера RADIUS или к IP-адресу двоеточие с последующим указанием номера нового порта.
Секрет	*Общий секрет для сервера RADIUS и платы управления.
Время ожидания ответа	Время в секундах, в течение которого плата управления ждет ответа от сервера RADIUS.
Настройки тестирования	Введите имя пользователя Администратор и пароль для тестирования пути к серверу RADIUS, который вы сконфигурировали.
Пропустить тестирование и применить	Не тестировать путь к серверу RADIUS.

Конфигурирование сервера RADIUS

Краткое описание процедуры конфигурирования

Вы должны сконфигурировать сервер RADIUS для работы с платой управления.



Примеры пользовательских файлов RADIUS с атрибутами, зависящими от поставщика (VSA), и пример записи в словарный файл на сервере RADIUS приведены в *Справочнике по защите*.

1. Добавьте IP-адрес платы управления к списку (файлу) клиентов сервера RADIUS.
2. Пользователи должны быть настроены с атрибутами «тип обслуживания», если не заданы атрибуты поставщика. Если атрибуты «тип обслуживания» не указаны, то у пользователя будет доступ только для чтения (только на веб-интерфейсе).



Сведения о пользовательском файле RADIUS приведены в документации к серверу, примеры можно найти в *Справочнике по защите*.

3. Вместо атрибутов «тип обслуживания», предусматриваемых сервером RADIUS, можно использовать VSA. Для VSA требуется запись в словаре и в пользовательском файле RADIUS. В словарном файле определите имена для ключевых слов АТРИБУТ и ЗНАЧЕНИЕ, но не для цифровых значений. Изменение цифровых значений приводит к сбою аутентификации и авторизации RADIUS. VSA имеет преимущество перед стандартными атрибутами RADIUS.

Конфигурирование сервера RADIUS для UNIX® с теньвыми паролями.

Если файлы теневого пароля UNIX (/etc/passwd) используются вместе со словарными файлами RADIUS, то для аутентификации пользователей можно применить два указанных ниже метода:

- Если все пользователи UNIX имеют административные привилегии, выполните следующие операции для «пользовательского файла» RADIUS. Чтобы допустить только Пользователей устройств, замените Тип обслуживания на Device (устройство).

```
DEFAULT Auth-Type = System
        Service-Type = Admin
```

- Добавьте имена пользователей и атрибуты к «пользовательскому» файлу RADIUS и проверьте пароли для /etc/passwd. Следующий пример относится к пользователям bconners и thawk:

```
bconners Auth-Type = System
        APC-Service-Type = Admin
thawk Auth-Type = System
        APC-Service-Type = Device
```

Поддерживаемые серверы RADIUS

American Power Conversion поддерживает FreeRADIUS и Microsoft IAS 2003. Другие часто используемые приложения RADIUS могут работать, но они не были всесторонне протестированы American Power Conversion.

Время ожидания ответа

Путь: Администрирование > Безопасность > Автоматический выход

Используйте эту опцию для настройки времени (3 минуты по умолчанию), по истечении которого неактивный пользователь отключается от системы. При изменении этого значения необходимо выйти из системы, чтобы изменение вступило в силу.



Примечание: Таймер продолжает работу, если пользователь закрывает окно браузера, не выйдя предварительно из системы нажатием клавиши **Завершение сеанса**, расположенной вверху справа. Поскольку считается, что пользователь все еще в системе, другой пользователь не может войти в систему, пока не истечет время, заданное параметром **Минуты отсутствия активности**. Например, если пользователь закрывает окно браузера, не выйдя из системы, при значении параметра **Минуты отсутствия активности**, заданном по умолчанию, то другой пользователь не может войти в систему в течение 3 минут.

Администрирование: Сетевые характеристики

Настройки TCP/IP линии связи

Настройки TCP/IP

Путь: Администрирование > Сеть > TCP/IP > настройки IPv4

Параметр **TCP/IP** в левом меню навигации, заданный по умолчанию при выборе пункта **Сеть** в верхней строке меню, отображает текущий адрес IPv4, маску подсети, шлюз по умолчанию, адрес MAC и режим загрузки платы управления.



Сведения о DHCP и параметрах настройки — см. **RFC2131** и **RFC2132**.

Настройка	Описание
Включить	С помощью данного флага включается и отключается IPv4.
Ручной	Конфигурирование IPv4 вручную путем задания IP-адреса, маски подсети и шлюза по умолчанию.
BOOTP	<p>Сервер BOOTP задает настройки TCP/IP. С периодом 32 с плата управления запрашивает сетевые настройки у любого из серверов BOOTP:</p> <ul style="list-style-type: none">• Если плата управления получает достоверный отклик, она запускает сетевые службы.• Если плата управления обнаруживает BOOTP-сервер, но запрос данного сервера не удается, либо превышает время ожидания, плата управления прекращает запрос сетевых настроек до момента перезапуска.• По умолчанию, если настройки сети предварительно заданы, а плата управления не получает достоверного отклика на пять своих запросов (исходный и четыре повторных), она будет использовать ранее установленные настройки, то есть останется доступной. <p>Нажмите Следующий>> и перейдите на страницу конфигурации BOOTP, чтобы изменить количество предпринимаемых попыток или действий в случае, если все эти попытки окажутся неудачными ¹:</p> <ul style="list-style-type: none">• Максимальное число попыток: Укажите число попыток, предпринимаемых в случае получения недостоверных откликов, или выберите ноль (0) в случае неограниченного количества попыток.• Если попытки неудачны: Выберите Use prior settings (по умолчанию) или Stop BOOTP request.
<p>1. Обычно параметры, заданные по умолчанию для указанных трех настроек, не требуют изменения:</p> <ul style="list-style-type: none">• Класс поставщика: APC• Идентификатор клиента: MAC-адрес сетевой платы управления, однозначно определяющий ее в локальной вычислительной сети (ЛВС)• Класс пользователя: Название модуля прошивки приложения	

Настройка	Описание
DHCP	<p>Настройка по умолчанию. С периодом 32 с плата управления запрашивает сетевые настройки у любого сервера DHCP.</p> <ul style="list-style-type: none"> • Если плата управления получает достоверный отклик, файл cookie APC из сервера DHCP для получения выделяемых параметров и запуска сетевых служб не требуется. • Если плата управления обнаруживает DHCP-сервер, но запрос данного сервера не удается либо превышает время ожидания, она прекращает запрос сетевых настроек до момента перезапуска¹. • Запрашивать файл cookie, характерный для поставщика, чтобы принять адрес DHCP: С помощью данного флажка включается и отключается запрос на выдачу DHCP-сервером файла cookie APC.
<p>1. Обычно параметры, заданные по умолчанию для указанных трех настроек, не требуют изменения:</p> <ul style="list-style-type: none"> • Класс поставщика: APC • Идентификатор клиента: MAC-адрес сетевой платы управления, однозначно определяющий ее в локальной вычислительной сети (ЛВС) • Класс пользователя: Название модуля прошивки приложения 	

Параметры отклика DHCP

Каждый достоверный отклик DHCP содержит параметры, задающие настройки TCP/IP, необходимые для работы платы управления в сети, а также другую информацию, влияющую на работу платы.

Сведения о конкретном поставщике (параметр 43). Плата управления использует этот параметр отклика DHCP для определения достоверности ответа. Данный параметр содержит относящиеся к APC параметры в формате TAG/LEN/DATA, называемые APC Cookie. По умолчанию этот параметр отключен.

• Cookie APC. Tag 1, Len 4, Data "1APC"

Параметр 43 сообщает плате управления, что сервер DHCP настроен на обслуживание устройств APC.

Далее в шестнадцатеричном формате представлен пример информации, зависящей от поставщика, в которой содержатся данные cookie APC:

Option 43 (Параметр 43) = 0x01 0x04 0x31 0x41 0x50 0x43

Параметры TCP/IP. Плата управления использует для определения своих настроек TCP/IP следующие параметры, содержащиеся в достоверном отклике DHCP. Все указанные параметры, за исключением первого, описаны в **RFC2132**.

- **IP-адрес** (из поля **yiaddr** отклика DHCP, описанного в **RFC2131**): IP-адрес, выдаваемый сервером DHCP плате управления.
- **Маска подсети** (параметр 1): Маска подсети указывает параметры, необходимые для работы платы управления в сети.
- **Маршрутизатор**, т.е. шлюз по умолчанию (параметр 3): Адрес шлюза по умолчанию, необходимый для работы платы управления в сети.
- **IP Address Lease Time** (параметр 51): Промежуток времени, за который выдается IP-адрес для платы управления.
- **Renewal Time, T1** (параметр 58): Время, которое плата управления должна ожидать после выдачи IP-адреса, перед тем как она сможет запросить обновление этого назначения.
- **Rebinding Time, T2** (параметр 59): Время, которое плата управления должна ожидать после выдачи IP-адреса, перед тем как она сможет повторить попытку продлить использование адреса.

Другие параметры. Плата управления также использует следующие параметры, содержащиеся в достоверном отклике DHCP. Все указанные параметры, за исключением последнего, описаны в **RFC2132**.

- **Network Time Protocol Servers** (параметр 42): Плата управле может использовать до двух NTP-серверов: первичный (основной) и вторичный (вспомогательный).
- **Time Offset** (параметр 2): Сдвиг времени подсети платы управления относительно универсального координированного времени (UTC), задаваемый в секундах.
- **Domain Name Server** (параметр 6): Плата управления может использовать до двух серверов доменных имен (DNS) (первичный и вторичный).
- **Имя хоста** (параметр 12): Имя хост-узла, которое использует плата управления (максимальная длина - 32 символа).
- **Имя домена** (параметр 15): Имя домена, которое использует плата управления (максимальная длина - 64 символа).
- **Boot File Name** (из поля **file** отклика DHCP, описанного в **RFC2131**): Полностью определенный путь до пользовательского файла конфигурации (ini-файла), используемого при загрузке. Поле **siaddr** отклика DHCP определяет IP-адрес сервера, с которого плата управления осуществляет загрузку ini-файла. После загрузки плата управления использует ini-файл в качестве загрузочного файла с целью изменения настроек.

Путь: Администрирование > Сеть > TCP/IP > настройки IPv6

Настройка	Описание
Включить	С помощью данного флага включается и отключается IPv6.
Ручной	Конфигурирование IPv6 вручную путем задания IP-адреса и шлюза по умолчанию.
Автоматическая конфигурация	При выборе параметра Автоматическая конфигурация система получает префиксы адресов от маршрутизатора (если таковой имеется). Она использует указанные префиксы для автоматического конфигурирования IPv6-адресов.
Режим DHCPv6	<p>Управляемый маршрутизатор: Выбор указанного режима означает, что DHCPv6 управляется флагами Managed(M) и Other(O), получаемыми в сообщениях маршрутизатора IPv6. При получении сообщения маршрутизатора плата управления проверяет, выставлены ли в нем флаги M или O. Плата управления анализирует состояние «битов» M (флаг Managed Address Configuration (Конфигурация управляемого адреса)) и O (флаг Other Stateful Configuration (Другая конфигурация с сохранением информации)) для следующих случаев:</p> <ul style="list-style-type: none"> • <i>Ни один флаг не задан:</i> Показывает, что сеть не имеет инфраструктуры DHCPv6. Плата управления использует сообщения маршрутизатора и ручные настройки для получения адресов, не являющихся link-local (используемых для связи в пределах одного сегмента сети), а также другие настройки. • <i>Заданы флаги M или M и O:</i> В этом случае имеется полная конфигурация адреса DHCPv6. DHCPv6 используется для получения адресов И прочих настроек конфигурации. Этот режим называется DHCPv6 stateful (с сохранением адресов). Если получен флаг M, конфигурация адреса DHCPv6 остается действительной до того момента, пока рассматриваемый интерфейс не будет закрыт. Такой режим остается в действии, даже если последующие пакеты сообщений маршрутизатора не будут содержать флага M. Если первым будет получен флаг O, а затем — флаг M, плата управления произведет полную конфигурацию адреса по получении флага M • <i>Задан только флаг O:</i> В этом случае плата управления отправляет пакет DHCPv6 Info-Request (пакет запроса информации). DHCPv6 будет использоваться для конфигурирования «других» параметров (таких как местоположение DNS-серверов), НО НЕ для получения адресов. Этот режим называется DHCPv6 stateless (без сохранения адресов). <p>Адрес и другие сведения: При включении этой радио-кнопки DHCPv6 будет использоваться для получения адресов И других параметров настройки. Этот режим называется DHCPv6 stateful (с сохранением адресов).</p> <p>Только сведения, за исключением адресов: При включении этой радио-кнопки DHCPv6 будет использоваться для конфигурации «других» параметров (таких как местоположение DNS-серверов), НО не для получения адресов. Этот режим называется DHCPv6 stateless (без сохранения адресов).</p> <p>Никогда: Выбор данного параметра отключает DHCPv6.</p>

Ответ ping

Путь: Администрирование > Сеть > Ответ ping

Поставьте флаг Включить для параметра **Ответ ping IPv4**, чтобы сетевая плата управления могла отвечать на сигналы эхо-тестирования. Если флаг снят, плата управления не будет откликаться на эхо-запросы. Такой режим не применяется для IPv6.

Скорость передачи порта

Путь: **Администрирование > Сеть > Скорость порта**

Параметр **Скорость порта** задает скорость обмена данными порта TCP/IP.

- При задании параметра **Автосогласование** (задается по умолчанию) устройства Ethernet определяют максимально возможную скорость передачи данных, при этом если скорости передачи данных двух устройств не совпадают, обмен будет вестись на более низкой скорости.
- Как вариант, можно выбрать скорость передачи 10 или 100 мбит/с, задав при этом полу-дуплексный (в каждый момент данные передаются только в одном направлении) или дуплексный (данные передаются в обоих направлениях по одному каналу одновременно) режим.

DNS

Путь: **Администрирование > Сеть > DNS-> параметры**

Используйте параметры пункта **DNS** в левом меню навигации для конфигурирования и тестирования системы доменных имен (DNS):

- Выберите **первичный DNS-сервер** или **вторичный DNS-сервер** для задания адресов IPv4 и IPv6 основного или дополнительного DNS-серверов. Чтобы отправлять электронную почту с помощью платы управления, необходимо, как минимум, указать IP-адрес первичного DNS-сервера.
 - Плата управления ожидает отклика от первичного или вторичного DNS-серверов (если вторичный DNS-сервер указан) в течение 15 секунд. Если плата управления не получает отклика в указанное время, электронное письмо не будет отправлено. Поэтому используйте DNS-серверы в том же или соседнем сегменте, где расположена плата управления (но не в других удаленных сегментах сети [WAN]).
 - После задания IP-адресов DNS-серверов проверьте, чтобы система DNS работала правильно, для чего введите DNS-имя компьютера в вашей сети и посмотрите IP-адрес этого компьютера.
- **Имя хоста:** После задания здесь имени хост-узла и указания доменного имени в поле **Имя домена**, пользователь может указывать имя хост-узла в любом поле интерфейса платы управления (кроме адресов электронной почты), которые работают с доменным именем.
- **Имя домена (IPv4):** Необходимо указать доменное имя только здесь. Плата управления добавит указанное доменное имя во всех других связанных с доменными именами полях интерфейса (кроме адреса электронной почты) только тогда, когда будет введено имя хост-узла.
 - Чтобы иметь возможность задавать все значения расширения указанного имени хост-узла путем добавления доменного имени, задайте значение доменного имени по умолчанию, `somedomain.com`, или значение `0.0.0.0`.
 - Чтобы изменить расширение конкретного имени хост-узла (например, при определении приемника прерываний), поставьте точку (trailing period). Плата управления распознает имя хост-узла с точкой (например, `mySnmpServer.`) как полноценное доменное имя и не будет добавлять доменное имя.

- **Имя домена (IPv6):** Определяет доменное имя IPv6.
- Выберите пункт **тестирование**, чтобы направить DNS-запрос, тестирующий настройки ваших DNS-серверов:
 - В качестве **Типа запроса** укажите один из следующих типов запросов DNS:
 - **по хосту:** URL-имя сервера
 - **по полному доменному имени:** полное доменное имя
 - **по IP-адресу:** IP-адрес сервера
 - **по MX:** система обмена почтой (Mail Exchange), используемая сервером
 - В качестве параметра **Вопрос в запросе** укажите значение, которое будет использовано для выбранного типа запроса:

Выбранный тип запроса	Используемый запрос
по хосту	Адрес URL
по полному доменному имени	полное доменное имя, <i>my_server.my_domain.</i>
по IP-адресу	IP-адрес
по MX	Адрес Mail Exchange

- Посмотрите результаты тестирования запроса DNS в поле **Последний ответ на запрос**.

WWW

Путь: Администрирование > Сеть > WWW > доступ

Опция	Описание
доступ	<p>Чтобы активировать сделанные изменения, выйдите из программы платы управления:</p> <ul style="list-style-type: none">• Выключить: отключает доступ к веб-интерфейсу. (Чтобы вновь открыть доступ, войдите в интерфейс командной строки и введите команду <code>http -S enable</code>. Чтобы получить доступ к протоколу HTTPS, введите команду <code>https -S enable</code>).• Включить HTTP (по умолчанию): Делает доступным обмен данными по протоколу передачи гипертекста (HTTP), который обеспечивает Web-доступ по имени пользователя и паролю, но не шифрует имена пользователей, пароли и передаваемые данные.• Включить HTTPS: Делает доступным обмен данными по протоколу передачи гипертекста (HTTPS) на уровне защищенных сокетов (SSL). Протокол SSL кодирует имена пользователей, пароли и передаваемые данные, а также аутентифицирует плату управления по цифровому сертификату. При включенном режиме HTTPS браузер отображает маленький значок замка. <p>Описание различных способов использования цифровых сертификатов — см. «Создание и установка цифровых сертификатов» в <i>Руководстве по безопасности</i> на компакт-диске <i>Utility</i> для платы сетевого управления.</p> <p>Порт HTTP: Порт TCP/IP (по умолчанию 80), используемый платой управления для обмена данными по протоколу HTTP.</p> <p>Порт HTTPS: Порт TCP/IP (по умолчанию 443), используемый платой управления для обмена данными по протоколу HTTPS.</p> <p>С целью обеспечения дополнительной защиты можно изменить значения настроек любого из указанных портов, выбрав неиспользуемый порт в диапазоне от 5000 до 32768. При указании адреса порта в адресном поле браузера пользователь должен использовать двоеточие (:). Например, для номера порта 5000 и IP-адреса 152.214.12.114:</p> <pre>http://152.214.12.114:5000 https://152.214.12.114:5000</pre>

Опция	Описание
сертификат ssl	<p>Добавление, замена и удаление сертификатов безопасности.</p> <p>Состояние:</p> <ul style="list-style-type: none"> • Не установлен (Not installed). Сертификат не установлен, или был установлен FTP или SCP в неправильном месте. С помощью команды Добавить или заменить файл сертификата установите сертификат в надлежащее место, /ssl на сетевой плате управления. • Генерируется (Generating): Сетевая плата управления генерирует сертификат, поскольку не обнаружен действующий сертификат. • Загружается (Loading): Сертификат должен активироваться на плате управления. • Годный сертификат: Действующий сертификат был установлен или сгенерирован платой управления. Щелкните эту ссылку, чтобы увидеть содержимое сертификата. <p>Если был установлен недействительный сертификат или сертификат не был загружен при включенном SSL, плата управления генерирует сертификат по умолчанию, этот процесс может вызвать задержку обращения к интерфейсу примерно на одну минуту. Сертификат по умолчанию можно использовать для обеспечения основных функций безопасности, путем шифрования данных, но при этом при входе в систему будет выводиться предупреждение о безопасности.</p> <p>Добавить или заменить файл сертификата: Укажите или найдите файл сертификата, созданный программой мастера безопасности Security Wizard.</p> <p>Для выбора метода использования цифровых сертификатов, созданных программой Security Wizard или сгенерированных картой управления, см. «Создание и установка цифровых сертификатов» в <i>Руководстве по безопасности</i> на компакт-диске <i>Utility</i> для платы сетевого управления.</p> <p>Удалить: Удаляет текущий сертификат</p>

Консоль

Путь: Администрирование > Сеть > Консоль > *доступ*

Опция	Описание
доступ	<p>Выберите один из следующих вариантов доступа с использованием протокола Telnet или Secure SHell (SSH):</p> <ul style="list-style-type: none">• Выключить: Отключает доступ к интерфейсу командной строки.• Включить Telnet (настройка по умолчанию): Протокол Telnet передает имена пользователей, пароли и данные без шифрования.• Включить SSH: Протокол SSH передает имена пользователей, пароли и данные в закодированном виде, обеспечивая защиту от попыток перехвата, подделки или искажения данных в процессе обмена. <p>Сконфигурируйте порты, используемые этими протоколами:</p> <ul style="list-style-type: none">• Порт Telnet : Порт Telnet (по умолчанию 23) используется для обмена данными с платой управления. С целью обеспечения дополнительной защиты можно изменить настройку порта, выбрав неиспользуемый порт в диапазоне от 5000 до 32768. Для определения порта, не заданного по умолчанию, необходимо использовать двоеточие (:) или пробел, как требует того клиентская программа Telnet. Например, для порта 5000 и IP-адреса 152.214.12.114 клиентская программа Telnet требует использования одной из следующих команд: <pre>telnet 152.214.12.114:5000 telnet 152.214.12.114 5000</pre>• Порт SSH: Порт SSH (по умолчанию 22) используется для обмена данными с платой управления. С целью обеспечения дополнительной защиты можно изменить настройку порта, выбрав неиспользуемый порт в диапазоне от 5000 до 32768. Формат команд командной строки, необходимых для задания порта, не используемого по умолчанию, приведен в документации программы-клиента SSH.
ключ хоста ssh	<p>Состояние показывает состояние хост-ключа (секретного ключа):</p> <ul style="list-style-type: none">• SSH выключено: отсутствуют используемые ключи хоста. (SSH Disabled: No host key in use.) В отключенном режиме SSH не может использовать хост-ключ.• Генерируется (Generating): Плата управления создает хост-ключ, поскольку не было найдено ни одного действующего ключа.• Загружается (Loading): Хост-ключ активируется на плате управления.• Годный (Valid): Один из следующих хост-ключей находится в директории /ssh (рекомендуемое местоположение на сетевой плате управления):<ul style="list-style-type: none">• 1024- или 2048-битовый хост-ключ создан программой Security Wizard• 2048-битовый хост-ключ RSA создан сетевой платой управления. <p>Добавить или Заменить: Найти или загрузить файл хост-ключа, созданного программой Security Wizard.</p> <p>Как использовать программу Security Wizard, см. <i>Руководство по безопасности</i> на компакт-диске <i>Utility</i> для платы сетевого управления.</p> <p>Примечание: Чтобы сократить время, необходимое для включения SSH, создайте и загрузите хост-ключ заблаговременно. Если вы включили SSH, не загрузив хост-ключ, плата управления потратит примерно минуту для создания ключа, и сервер SSH будет недоступен всё это время.</p> <p>Удалить: Удаляет текущий хост-ключ.</p>

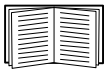


Примечание: Чтобы использовать SSH, необходимо иметь установленный клиент SSH. Большинство платформ Linux и UNIX имеют в своем составе клиент SSH, но операционная система Microsoft Windows не имеет такового. Известны клиентские программы различных производителей.

SNMP

Все имена пользователей, пароли и имена сообществ для SNMP передаются по сети в текстовом формате. Если сеть требует высокую степень защиты, отключите доступ SNMP или установите для всех сообществ доступ на чтение. (Сообщество с доступом на чтение может получать информацию о статусе и использовать прерывания SNMP).

При использовании программы InfraStruXure Manager для управления ИБП в общей сети системы InfraStruXure, необходимо включить SNMP-доступ в интерфейсе платы управления. Доступ на чтение позволяет устройству InfraStruXure получать прерывания от платы управления, а доступ на запись необходим при работе с интерфейсом платы управления для использования устройства InfraStruXure в качестве приемника прерываний.



Дополнительную информацию по улучшению защищенности системы см. в *Руководстве по безопасности* на компакт-диске *Utility* для платы сетевого управления и на веб-сайте www.apc.com.

SNMPv1

Путь: **Администрирование > Сеть > SNMPv1 > доступ**

Опция	Описание
доступ	Включить доступ SNMPv1: Включает SNMP версии 1 в качестве способа обмена данными с указанным устройством.
контроль доступа	<p>Допускается конфигурировать до четырех записей управления доступом, чтобы определить, какая из сетевых систем управления (NMS) имеет доступ к данному устройству. Открываемая страница управления доступом по умолчанию назначает один параметр для каждого из четырех доступных сообществ SNMPv1; эти параметры можно изменить таким образом, чтобы применить к каждому из сообществ более одной записи для обеспечения доступа путем предоставления нескольких конкретных адресов IPv4 и IPv6, имен хост-узлов и масок IP-адресов. Чтобы отредактировать настройки управления доступом для сообщества, щелкните имя этого сообщества.</p> <ul style="list-style-type: none">• Если оставить параметры управления доступом, заданные по умолчанию, неизменными, это сообщество будет обладать доступом к данному устройству из любой точки сети.• Если задать несколько записей управления доступом для одного имени сообщества, ограничение в виде четырех записей потребует, чтобы одно или несколько сообществ не имели записей управления доступом. Если для сообщества не задана запись управления доступом, указанное сообщество не будет иметь доступа к данному устройству. <p>Имя сообщества: Имя, которое система NMS должна использовать для доступа. Максимальная длина составляет 15 символов ASCII, имена, заданные по умолчанию для четырех сообществ, следующие: public, private, public2 и private2.</p> <p>Имя IP-адреса/хоста NMS: Адрес IPv4 или IPv6, маска IP-адреса или имя хост-узла, который управляет доступом систем NMS. Имя хост-узла или определенный IP-адрес (такой как 149.225.12.1) открывает доступ только системе NMS в данном сегменте сети. IP-адреса, содержащие 255, ограничивают доступ следующим образом:</p> <ul style="list-style-type: none">• 149.225.12.255: Доступ NMS только в сегменте 149.225.12.• 149.225.255.255: Доступ NMS только в сегменте 149.225.• 149.255.255.255: Доступ NMS только в сегменте 149.• 0.0.0.0 (настройки по умолчанию), которые могут быть также представлены в виде 255.255.255.255: Доступ любой системы NMS в любом сегменте. <p>Тип доступа: Действия, которые может выполнять NMS в сообществе.</p> <ul style="list-style-type: none">• Чтение: только получать (GET) информацию, в любое время• Запись: получать (GET) в любое время и размещать (SET) информацию, если другие пользователи не работают в веб-интерфейсе или в интерфейсе командной строки.• Запись+: получать (GET) и размещать (SET) информацию в любое время.• Выключить: запрещено получать (GET) и размещать (SET) информацию в любое время.

SNMPv3

Путь: Администрирование > Сеть > SNMPv3 > доступ

Для запросов GET и SET протокола SNMP и приемников прерываний в SNMPv3 при идентификации пользователей используется система профилей пользователей. Пользователь SNMPv3 должен иметь профиль пользователя, назначенный в программе MIB для выполнения операций GET/SET, просмотра MIB и получения прерываний.



Примечание: Для использования SNMPv3 необходимо иметь программу MIB с поддержкой SNMPv3.

Плата управления поддерживает аутентификацию SHA или MD5, а также шифрование AES или DES.

Опция	Описание
доступ	Доступ SNMPv3: Включает SNMPv3 в качестве способа обмена данными с указанным устройством.
профили пользователей	<p>По умолчанию содержит настройки четырех пользовательских профилей, сконфигурированных с именами пользователей от arc snmp profile1 до arc snmp profile4, не требует аутентификации и конфиденциальности (не использует шифрования). Чтобы изменить следующие настройки пользовательского профиля, щелкните имя пользователя в указанном списке.</p> <p>Имя пользователя: Идентификатор профиля пользователя. SNMP версии 3 отображает функции GET, SET и обеспечивает захват в пользовательском профиле в пользовательский профиль путем сличения имени пользователя профиля с именем пользователя в передаваемом пакете данных. Имя пользователя может содержать до 32 символов ASCII.</p> <p>Парольная фраза аутентификации: Фраза, содержащая от 15 до 32 символов ASCII (фраза <code>arc auth</code>, принята по умолчанию) которая удостоверяет, что NMS, обменивающаяся данными с данным устройством через SNMPv3 является именно той системой NMS, за которую она себя выдает; данное сообщение не было искажено в ходе передачи и было передано вовремя, не было задержано и не было скопировано и послано вторично позднее, в несоответствующее время.</p> <p>Конфиденциальная парольная фраза: Фраза от 15 до 32 символов ASCII (по умолчанию фраза <code>arc crypt passphrase</code>), которая гарантирует конфиденциальность данных (с помощью шифрования), передаваемых NMS на данное устройство или получаемых от него по протоколу SNMPv3.</p> <p>Протокол аутентификации: Протокол SNMPv3, реализованный в, поддерживает аутентификацию SHA и MD5. Аутентификация не выполняется до тех пор, пока не будет задан протокол аутентификации.</p> <p>Протокол конфиденциальности: Протокол SNMPv3, реализованный в, поддерживает в качестве протоколов шифрования и дешифрования данных протоколы AES и DES. Конфиденциальность передаваемых данных требует, чтобы был задан протокол конфиденциальности и чтобы в запросе NMS была передана фраза-пароль конфиденциальности. Если протокол конфиденциальности активирован, но NMS не передала фразу-пароль конфиденциальности, запрос SNMP не будет зашифрован.</p> <p>Примечание: нельзя выбрать протокол конфиденциальности, если не выбран протокол аутентификации.</p>

Опция	Описание
контроль доступа	<p>Допускается конфигурировать до четырех записей управления доступом, чтобы определить, какая из систем NMS имеет доступ к данному устройству. Открываемая страница управления доступом по умолчанию назначает по одной записи для каждого из четырех профилей пользователей; эти записи можно изменить таким образом, чтобы применить к каждому из профилей более одной записи, с тем чтобы обеспечить доступ путем предоставления нескольких адресов IP, имен хост-узлов и масок IP-адресов.</p> <ul style="list-style-type: none"> • Если оставить заданные по умолчанию записи управления доступом для данного профиля пользователя без изменения, все системы NMS, использующие этот профиль, будут иметь доступ к указанному устройству. • Если вы задать несколько записей управления доступа для одного профиля пользователя, ограничение в виде четырех записей потребует, чтобы один или несколько профилей не имели записей управления доступом. Если для профиля пользователя не указана ни одна запись управления доступом, то NMS, использующие данный профиль, не будут иметь доступ к указанному устройству. <p>Чтобы отредактировать настройки управления доступа для профиля пользователя, щелкните имя этого пользователя.</p> <p>Доступ: Поставьте флаг Включить, чтобы активировать управление доступом, определяемое параметрами, указанными в данной записи.</p> <p>Имя пользователя: В раскрывающемся списке выберите профиль пользователя, для которого будет применена данная запись управления доступом. Можно выбрать любые из четырех имен пользователей, которые были сконфигурированы с помощью команды профили пользователей в левом меню навигации.</p> <p>Имя IP-адреса/хоста NMS: IP-адрес, маска IP-адреса или имя хост-узла, который управляет доступом NMS. Имя хост-узла или определенный IP-адрес (такой как 149.225.12.1) открывает доступ только системе NMS в данном сегменте сети. Маска IP-адреса, которая содержит число 255, ограничивает доступ следующим образом:</p> <ul style="list-style-type: none"> • 149.225.12.255: Доступ NMS только в сегменте 149.225.12. • 149.225.255.255: Доступ NMS только в сегменте 149.225. • 149.255.255.255: Доступ NMS только в сегменте 149. • 0.0.0.0 (настройки по умолчанию), которые могут быть также представлены в виде 255.255.255.255: Доступ любой системы NMS в любом сегменте.

Modbus.

Путь: **Администрирование > Сеть > Modbus > tcp**

Открытие и закрытие доступа к Modbus TCP путем установки или снятия флага **Включить**.

С помощью поля **Порт** можно указать порт, на котором будет работать протокол Modbus TCP.

Сервер FTP

Путь: **Администрирование > Сеть > сервер FTP**

Настройки **сервера FTP** открывают (по умолчанию) или закрывают доступ к FTP-серверу и определяют порт TCP/IP (по умолчанию - 21), который FTP-сервер использует для обмена данными с платой управления. Сервер FTP использует как указанный порт, так и порт с номером на единицу меньше.

С целью повышения безопасности можно изменить настройку **Порт** на номер любого неиспользуемого порта в диапазоне от 5001 до 32768. Для выбора номера порта, отличного от заданного по умолчанию, необходимо использовать символ двоеточия (:). Например, для порта 5001 и IP-адреса 152.214.12.114 команда должна иметь вид `ftp 152.214.12.114:5001`.



Примечание: Протокол FTP передает файлы без их шифрования. С целью повышения безопасности отключите FTP-сервер и пересылайте файлы с помощью протокола SCP. Выбор и конфигурирование Secure SHell (SSH) автоматически включает SCP.

Всякий раз, когда вы хотите, чтобы ИБП был доступен для управления с помощью InfraStruXure Central, сервер FTP в интерфейсе платы управления этого ИБП должен быть включен.



Дополнительную информацию по улучшению защищенности системы см. в *Руководстве по безопасности* на компакт-диске *Utility* для платы сетевого управления и на веб-сайте.

Администрирование: Уведомление

Действия для событий

Путь: Администрирование > Уведомление > Действия для событий > *опции*

Типы уведомлений

Чтобы добиться требуемой реакции на событие или группу событий, можно конфигурировать действия для событий. Эти действия будут уведомлять пользователя о событии одним из указанных способов:

- Активное, автоматическое уведомление. Указанные пользователи контролируемых устройств будут уведомляться непосредственно.
 - Уведомление по электронной почте
 - Прерывания SNMP
 - Служба удаленного контроля
 - Уведомление системного журнала (Syslog)
- Косвенное уведомление
 - Журнал событий. Если не сконфигурирована передача прямых уведомлений, пользователи должны проверять журнал, чтобы смотреть, какие события произошли



Можно также регистрировать данные о работе системы с целью использования этих данных для контроля работы устройств. См. «Журнал данных» на стр. 63, чтобы ознакомиться с конфигурированием и использованием функции регистрации данных.

- Запросы (SNMP GET)



Дополнительные сведения см. в разделе «SNMP» на стр. 80. SNMP позволяет NMS использовать информационные запросы. В случае протокола SNMPv1, который не обеспечивает шифрования данных перед передачей, задание наиболее ограниченного типа доступа SNMP (ЧТЕНИЕ) позволяет выполнять информационные запросы без риска дистанционного изменения конфигурации.

Карта сетевого управления поддерживает **RFC1628 MIB** (база управляющей информации). Информацию о настройке приемника прерываний см. в разд. «Прерывания SNMP». Группа из трех событий **1628 MIB** совместима только с этой базой управляющей информации, не с альтернативной базой Pownet MIB. Они могут быть настроены, как любое другое событие (см. «Конфигурирование действий для событий» ниже).

Конфигурирование действий для событий

Параметры уведомлений. Для событий, которые имеют связанное событие очистки, можно задать следующие параметры, конфигурируя отдельные события или группы событий, как описано в последующих двух разделах. Чтобы получить доступ к указанным параметрам, щелкните приемник или имя получателя.

Параметр	Описание
Задержка x перед отправкой	Если событие продолжает действовать в течение указанного промежутка времени, посылается уведомление. Если данное условие исчезает до того, как истек заданный интервал времени, уведомление не посылается.
Повторять через интервал x минут	Уведомление посылается в указанный промежуток времени (например, каждые 2 минуты).
До x раз	Пока событие действует, уведомление будет повторено указанное число раз.

Параметр	Описание
До устранения условия возникновения	Уведомление посылается регулярно до того момента, пока условие не исчезнет или не будет устранено.

Конфигурирование по событию. Для определения ответных действий на отдельное событие:

1. Выберите вкладку **Администрирование**, пункт **Уведомление** в верхней строке меню и укажите параметр **по событию** в пункте **Действия для событий** в левом меню навигации.
2. В перечне событий найдите помеченные столбцы, чтобы проверить, сконфигурированы ли те действия, которые вы собираетесь использовать. (По умолчанию, регистрация указана для всех событий).
3. Чтобы посмотреть или изменить текущую конфигурацию, например, получателей, которые будут уведомлены по электронной почте или пейджеру, или систем NMS, которые должны быть уведомлены по прерываниям SNMP, щелкните имя события.



Примечание: Если сервер Syslog не сконфигурирован, пункты, относящиеся к конфигурации Syslog показаны не будут.



При просмотре параметров конфигурации события можно изменить конфигурацию, включить или отключить регистрацию событий или журнал Syslog, или отключить уведомление определенных получателей электронной почты или приемников прерываний, но нельзя добавить или удалить получателей и устройства-приемники. Чтобы добавить или удалить адресаты или устройства-приемники, посмотрите следующее:

- «Идентификация серверов Syslog» на стр. 91
- «Получатели электронной почты» на стр. 88
- «Получатели прерываний» на стр. 89

Конфигурирование по группе. Чтобы сконфигурировать группу событий:

1. Выберите вкладку **Администрирование**, пункт **Уведомление** в верхней строке меню и укажите параметр **по группе** в пункте **Действия для событий** в левом меню навигации.
2. Выберите, каким образом группировать события для конфигурации:
 - Выберите пункт **События по степени опасности**, после чего выберите все события одного или нескольких уровней опасности. Изменять уровень опасности события нельзя.
 - Выберите пункт **События по категории**, после чего выберите все события одной или нескольких предварительно заданных категорий.
3. Нажмите **Следующий>>**, чтобы уйти с указанной страницы, и выполните следующее:
 - a. Выберите действия для события для группы событий.
 - Чтобы выбрать любое из действий, за исключением **Ведение журнала** (по умолчанию), для начала необходимо иметь, как минимум, одного сконфигурированного действительного получателя или одно устройство-приемник.
 - Если вы указали **Ведение журнала** и сконфигурировали сервер Syslog, выберите на следующей странице **Журнал событий** или **Syslog** (или оба журнала).
 - b. Укажите, хотите ли вы сохранить новое сконфигурированное действие на событии для группы событий или отключить данное действие.

Активное автоматическое прямое уведомление

Уведомление по электронной почте

Обзор настроек. Используйте протокол SMTP для отправки сообщений электронной почты сразу четырем получателям при возникновении события.

Чтобы использовать функцию отправки электронной почты, необходимо задать следующие параметры:

- IP-адреса первичного и, дополнительно, вторичного сервера доменных имен (DNS). (См. «DNS» на стр. 75.)
- IP-адрес или имя DNS для параметров **Сервер SMTP** и **Адрес отправителя**. (См. «SMTP» на стр. 87.)
- Адреса электронной почты для четырех получателей (максимум). (См. «Получатели электронной почты» на стр. 88.)



Можно использовать настройку **Адрес получателя** опции **получатели** для отправки электронной почты на текстовый пейджер.

SMTP.

Путь: **Администрирование > Уведомление > Электронная почта > сервер**

Настройка	Описание
Локальный сервер SMTP	Адрес IPv4/ IPv6 или имя DNS локального сервера SMTP. Примечание: Этот параметр требуется определять только в том случае, если Сервер SMTP задан как Локальный . См. «Получатели электронной почты» на стр. 88.
Адрес отправителя	Содержание поля From (От) в сообщениях электронной почты отправляется платой управления: <ul style="list-style-type: none">• В формате <i>пользователь@ [IP_адрес]</i> (если IP-адрес указан как Локальный сервер SMTP)• В формате <i>пользователь@домен</i> (если сконфигурирован DNS, и имя DNS указано как Local SMTP Server (Локальный сервер SMTP)) в сообщениях электронной почты. Примечание: Локальный SMTP-сервер может потребовать учетную запись сервера для задания данной настройки. См. документацию сервера.

Получатели электронной почты.

Путь: Администрирование > Уведомление > Электронная почта > получатели

Определяет до четырех получателей электронной почты.

Настройка	Описание
Адрес получателя	<p>Имя пользователя и доменное имя получателя. Чтобы использовать адрес для уведомления на пейджер, задайте адрес электронной почты шлюза пейджерной учетной записи получателя (например, myacct100@skytel.com). Шлюз пейджера будет генерировать сообщение.</p> <p>Чтобы обойти поиск DNS-имени IP-адреса почтового сервера, в скобках укажите IP-адрес вместо имени домена электронной почты, например, используйте jsmith@[xxx.xxx.x.xxx] вместо jsmith@company.com. Это полезно, когда поиск имен DNS работает неправильно.</p> <p>Примечание: Пейджер получателя должен быть способен получать текстовые сообщения.</p>
Создание сообщения электронной почты	Включает (по умолчанию) или отключает отправку электронной почты получателю.
Сервер SMTP	<p>Выберите один из следующих способов доставки электронной почты:</p> <ul style="list-style-type: none">• Локальный: Через SMTP-сервер управляющей платы. Данная настройка (рекомендуемая) гарантирует, что -сообщение будет отправлено до истечения времени ожидания платы управления, равного 20 с, и, в случае необходимости, повторит попытку отправить сообщение несколько раз. Кроме того, выполните одно из следующих действий:<ul style="list-style-type: none">• Включите пересылку на SMTP-сервере платы управления, с тем чтобы он мог переправлять электронную почту на внешние SMTP-серверы. Обычно SMTP-серверы не сконфигурированы для пересылки электронной почты. Проверьте с администратором ваш SMTP-сервер перед изменением конфигурации с целью разрешить пересылку.• Укажите специальную учетную запись электронной почты для платы управления, чтобы переправлять почту на внешнюю учетную почтовую запись.• Получатель: Непосредственно на SMTP-сервер получателя. С указанной настройкой плата управления попытается опривить электронную почту только один раз. Если удаленный SMTP-сервер занят, настройка времени ожидания может предотвратить отсылку некоторых писем. <p>Если получатель использует SMTP-сервер платы управления, данная настройка не работает.</p>
Формат	Длинный формат содержит имя, местоположение, контакт, IP-адрес, серийный номер устройства, дату и время, код и описание события. Короткий формат содержит только описание события.
Язык	Выберите язык из раскрывающегося списка, и все письма будут отправляться на указанном языке. Можно использовать различные языки для различных пользователей.
Имя пользователя Пароль Подтвердить пароль	Если почтовый сервер требует аутентификации, укажите здесь имя пользователя и пароль. Таким образом будет выполняться простейшая аутентификация, но не SSI.

Тестирование электронной почты.

Путь: **Администрирование > Уведомление > Электронная-почта > тестирование**

Посылает тестовое сообщение указанному получателю.

Прерывания SNMP

Получатели прерываний.

Путь: **Администрирование > Уведомление > прерывания SNMP > приемники прерываний**

Просмотр приемников прерываний по имени IP-адреса/хоста NMS. Можно задать до шести приемников прерываний.

- Чтобы сконфигурировать новый приемник прерываний, щелкните пункт **Добавить получатель прерываний**.
- Чтобы изменить настройки или удалить приемник прерываний, щелкните вначале IP-адрес или имя хост-узла, чтобы получить доступ к его настройкам. (Если вы удалите приемник прерываний, все настройки уведомлений, сконфигурированные в пункте Действия для событий для удаленного приемника прерываний, вернутся в исходное положение, заданное по умолчанию).
- Чтобы указать тип прерывания для данного приемника, задайте с помощью переключателя значение SNMPv1 или SNMPv3. Чтобы система NMS могла получать оба типа прерываний, необходимо сконфигурировать для данной NMS два приемника прерываний, по одному на каждый тип прерывания.

Пункт	Описание
Создание системного прерывания	Включает (по умолчанию) или отключает генерацию прерывания для данного приемника прерываний.
Генерация прерываний Powernet MIB/RFC1628	Выберите один из этих двух типов генерации прерываний для каждого создаваемого прерывания. RFC1628 — это общая стандартная база управляющей информации (MIB) для устройств ИБП. Функция Powernet адаптирована для Schneider Electric и содержит множество дополнительных переменных в соответствии со спецификой продукции компании. При использовании базы RFC1628 MIB также можно использовать три извещения о событиях RFC1628 (см. “Действия для событий”). Их использование позволяет избежать необходимости настройки извещений вне среды NMS, см. RFC1628 MIB .
Имя IP-адреса/хоста NMS	Адрес IPv4/ IPv6 или имя хост-узла данного приемника прерываний. По умолчанию, настройки 0.0.0.0 оставляют приемник прерываний неопределенным.
Язык	Выберите язык из раскрывающегося списка. Он может отличаться от языка интерфейса пользователя и языков других приемников прерываний.

Параметр SNMPv1.

Пункт	Описание
-------	----------

Имя сообщества	Имя (по умолчанию public), используемое в качестве идентификатора при отправке прерываний SNMPv1 на данный приемник.
Аутентификация прерываний	Если данная функция активирована (по умолчанию), система NMS, определяемая настройкой Имя IP-адреса/хоста NMS, будет получать аутентификационные прерывания (прерывания, генерируемые неудачными попытками регистрации на данном устройстве). Чтобы отключить данную возможность, снимите флажок.

Параметр SNMPv3. Задаёт идентификатор профиля пользователя для данного приемника прерываний. (Чтобы увидеть настройки профилей пользователя, определяемые именами пользователей, выбираемых здесь, укажите **Сеть** в верхней строке меню и **профили пользователя** в пункте **SNMPv3** в левом меню навигации).



См. «SNMPv3» на стр. 81 о создании профилей пользователей и о выборе способов аутентификации и шифрования.

Тестирование прерываний SNMP

Путь: Администрирование > Уведомление > SNMP прерывания > тестирование

Последний результат тестирования. Результат последнего теста прерывания SNMP. Успешный тест прерывания SNMP подтверждает только то, что прерывание было отправлено, но не проверяет его получение выбранным приемником прерываний. Тест прерываний считается успешным, если все из перечисленных условий будут верны:

- На данном устройстве доступна одна из версий SNMP (SNMPv1 или SNMPv3), конфигурируемая для указанного приемника прерываний.
- Приемник прерываний включен.
- Если имя хост-узла указывается в поле адреса **К**, данное имя может быть заменено на действительный IP-адрес.

К. Укажите IP-адрес или имя хост-узла, на который будет послан тест прерывания SNMP. Если приемник прерывания не сконфигурирован, будет отображаться ссылка на страницу конфигурации **Получатель прерываний**.

Служба удаленного контроля

Путь: Администрирование > Уведомление > Удаленный контроль

Служба удаленного контроля Remote Monitoring Service (RMS) является дополнительной службой, позволяющей контролировать работу системы дистанционно из центра управления круглосуточно и уведомлять о происходящих системных событиях.



Чтобы приобрести службу RMS, свяжитесь с поставщиком оборудования или щелкните ссылку в верхней части страницы: **веб-сайт RMS**.

Регистрация. Чтобы активировать службу RMS для платы управления, выберите пункт **Включить службу удаленного контроля (RMS) (Enable Remote Monitoring Service)**, выберите параметр **Зарегистрировать компанию и устройство (Register Company and Device)** или **Зарегистрировать только устройство (Register Device Only)**, заполните регистрационную форму и щелкните **Отправить регистрацию в RMS**.

Чтобы отключить указанную службу на время или постоянно (например, если вы заменили плату управления), щелкните флажок **Сброс регистрации в службе удаленного контроля (RMS) (Reset Remote Monitoring Service Registration)**.

Syslog

Путь: Журналы > Syslog > *опции*

Плата управления может посылать сообщения сразу на четыре сервера Syslog в случае возникновения события. Серверы Syslog регистрируют события, произошедшие в сетевых устройствах в журналах, которые обеспечивают централизованную регистрацию событий.



Руководство пользователя не содержит подробных описаний сервера Syslog и его конфигурации. См. **RFC3164** для получения подробной информации о серверах Syslog.

Идентификация серверов Syslog.

Путь: Журналы > Syslog > серверы

Настройка	Описание
Сервер Syslog	Использует адреса IPv4/ IPv6 или имена хост-узлов для идентификации одного из четырех серверов для получения сообщений Syslog, посылаемых платой управления.
Порт	Порт протокола пользовательских датаграмм (UDP), который использует плата управления для отправки сообщений Syslog. По умолчанию имеет значение 514 , порт UDP назначен для Syslog.
Протокол	Выбор протокола UDP или TCP.
Язык	Выбор языка сообщений Syslog.

Настройки системного журнала.

Путь: Журналы > Syslog > настройки

Настройка	Описание
Создание сообщения	Включает (по умолчанию) или отключает функцию системного журнала Syslog.
Код объекта	Выбирает код объекта, назначенный для сообщений системного журнала платы управления (по умолчанию - User (пользователь)). Примечание: Параметр User лучше всего определяет настройки сообщений Syslog, посылаемых платой управления. Не изменяйте эти настройки, не проконсультировавшись с администратором Syslog или системным администратором.

Настройка	Описание
Сопоставление степени опасности	<p>Сопоставляет каждый уровень опасности событий платы управления или среды с соответствующими приоритетами Syslog. Необходимости менять сопоставления нет.</p> <p>Следующие определения взяты из RFC3164:</p> <ul style="list-style-type: none"> • Аварийная ситуация: Система не работает • Оповещение: Следует незамедлительно предпринять меры • Критическая: Критичные условия • Ошибка: Условия ошибки • Предупредительное: Условия предупреждения • Примечание: Нормальные условия, но требуют внимания • Информация: Информационное сообщение • Отладка: Сообщения уровня отладки <p>Ниже приведены настройки, установленные по умолчанию для параметров Local Priority (локальных приоритетов):</p> <ul style="list-style-type: none"> • Параметр Критическая (Severe) соответствует Критическая • Параметр Предупредительное соответствует Предупредительное • Параметр Информация соответствует Info <p>Примечание: Чтобы отключить сообщения Syslog, см. «Конфигурирование действий для событий» на стр. 84.</p>

Пример теста и формата Syslog.

Путь: Журналы > Syslog > тестирование

Отправляет тестовое сообщение на серверы Syslog, сконфигурированные в опции **servers** (серверы).

1. Выберите уровень опасности, который будет присвоен тестовому сообщению.
2. Определите тестовое сообщение согласно требуемым полям сообщения
 - Приоритет (PRI): Приоритет Syslog, указанный для сообщаемого события, а также код объекта сообщений, отправляемых на плату управления.
 - Заголовок: отметка времени и IP-адрес платы управления.
 - Тело сообщения (MSG):
 - Поле TAG, за которым следует двоеточие и пробел, определяет тип события.
 - Поле CONTENT (содержание) представляет собой текст сообщения о событии, за которым следует (дополнительно) пробел и код события.

Например, APC: Тестовый журнал Syslog задействован.

Администрирование: Основные функции

Идентификация

Путь: **Администрирование > Общие > Идентификация**

Определите **Имя** (имя устройства), **Расположение** (местоположение устройства) и **Контакт** (лицо, ответственное за устройство) с помощью программ InfraStruXure Central, InfraStruXure Manager и агента SNMP платы управления. Эти настройки и значения используются для идентификаторов MIB-II **sysName**, **sysContact** и **sysLocation** (OID).



Дополнительные сведения о MIB-II OIDs см. в Справочнике *PowerNet® SNMP Management Information Base (MIB)* на компакт-диске *Utility* для платы сетевого управления, и на веб-сайте по адресу: www.apc.com.

Поля **Имя** и **Расположение** также определяют устройство при регистрации его для использования службы дистанционного контроля Remote Monitoring Service. Дополнительные сведения см. в разделе «Служба удаленного контроля» на стр. 90.

Задание даты и времени

Mode (Режим).

Путь: **Администрация > Общие > Дата и время > режим**

Задаёт время и дату, используемые платой управления. Можно изменять текущие настройки вручную или с помощью сервера сетевого протокола службы времени (NTP):

- **Ручной:** Выполните одно из следующих действий:
 - Введите дату и время для платы управления.
 - Поставьте флажок **Применение локального времени ПК**, чтобы дата и время совпадали с компьютерными часами.
- **Синхронизировать с NTP-сервером:** Дает возможность NTP-серверу задавать дату и время плате управления.



Примечание: По умолчанию, все платы управления на пользовательской стороне InfraStruXure Central получают настройки времени, используя программу InfraStruXure Central в качестве сервера NTP.

Настройка	Описание
Первичный NTP-сервер	Введите IP-адрес или доменное имя первичного NTP-сервера.
Вторичный NTP-сервер	Введите IP-адрес или доменное имя вторичного NTP-сервера, если таковой имеется.

Настройка	Описание
Часовой пояс	Выберите часовой пояс. Количество часов, предшествующее каждому часовому поясу, указанному в списке, показывает смещение относительно универсального координированного времени (UTC), известного ранее как время по Гринвичу.
Интервал обновления	Задаёт промежуток времени в часах, определяющий, как часто плата управления будет обращаться к NTP-серверу для обновления данных. <i>Минимальное значение: 1; Максимальное значение: 8760 (1 год).</i>
Немедленное обновление данных при помощи NTP.	Запускает моментальное обновление даты и времени по NTP-серверу.

Переход на летнее время

Путь: Администрация > Общие > Дата и время > переход на летнее время

Позволяет использовать летнее время США (DST) или указать собственное поясное летнее время в соответствии с правилами установки летнего времени в вашем регионе. По умолчанию параметр DST отключен.

При настройке летнего времени (DST):

- Если местное летнее время всегда начинается и заканчивается в четвертый день недели определенного месяца (например, в четвертое воскресенье), выберите параметр **Четвертый/последний**. Если в данном году в указанном месяце есть пятое воскресенье, переход на летнее время все равно произойдет на четвертое воскресенье.
- Если местное летнее время всегда начинается и заканчивается в последний, четвертый или пятый день недели определенного месяца, выберите параметр **Пятый/последний**.

Формат

Путь: Администрация > Общие > Дата и время > формат даты

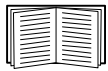
Выберите цифровой формат, в котором будут отображаться все даты данного пользовательского интерфейса. В формате каждая буква m (месяц), d (день) и y (год) отображают одну цифру. Однозначные дни и месяцы отображаются с ведущим нулем (перед значащей цифрой).

Использование файла ini

Путь: Администрирование > Общие > Файл конфигурации пользователя

Используйте настройки одной платы управления, чтобы сконфигурировать другую. Возьмите файл config.ini, содержащий настройки одной платы, измените эти настройки (например, измените IP-адрес) и загрузите обновленный файл в новую плату управления. Имя файла может содержать до 64 символов и должно иметь суффикс ini.

Состояние	Показывает выполнение процесса загрузки. Загрузка будет завершена, даже если файл содержит ошибки, но система сообщит об имеющихся ошибках в журнале событий.
Загрузить	Найдите исправленный файл и загрузите его, так чтобы указанная плата управления могла использовать его для задания собственных настроек.



О том, как получить и редактировать файл для конфигурации платы управления, см. «Экспорт параметров конфигурации» на стр. 100.

Вместо загрузки файла в плату управления, вы можете экспортировать его в несколько плат управления, используя скрипт или командный файл FTP или SCP, и служебную программу ini-файлов, которую можно найти по адресу: www.apc.com/tools/download.

Журнал событий, единицы измерения температуры, язык и загрузочная страница

Путь: Администрирование > Общие > Настройки

Выделения цветом текста в журнале событий

По умолчанию эта функция отключена. Поставьте флажок **Цветовая кодировка журнала событий**, чтобы получить возможность выделять цветом сообщения о неисправностях, регистрируемые в журнале событий. Записи системных событий и изменения конфигурации не изменят свой цвет.

Цвет текста	Опасность неисправности
Красный	Critical: Критический аварийный сигнал, требующий немедленного принятия мер.
Оранжевый	Warning: Тревожная сигнализация требует внимания, поскольку не решенная вовремя проблема может привести к потере данных и порче оборудования, если не устранить вызвавшую ее причину.
Зеленый	Alarm Cleared (Сигнализация сброшена): Условия, которые вызвали тревогу, устранены.
Черный	Normal (Нормальное состояние): Сигналов тревоги нет. Сетевая плата управления и все подключенные к ней устройства работают нормально.

Изменение температурной шкалы, заданной по умолчанию.

Выберите шкалу измерения температуры (по Фаренгейту или по Цельсию), на которой на пользовательском интерфейсе будут отображаться измеренные температуры.

Настройка языка интерфейса пользователя

В поле **Язык** можно указать язык, устанавливаемый по умолчанию для пользовательского интерфейса. Язык также можно указать при загрузке. В раскрывающемся списке выберите один из показанных языков.



Примечание: Можно также задавать различные языки для получателей электронной почты и приемников прерываний SNMP. См. «Получатели электронной почты» на стр. 88 и «Получатели прерываний» на стр. 89.

Задание загрузочной страницы по умолчанию

Укажите веб-страницу, которая будет открываться по умолчанию при загрузке.

Сброс настроек платы управления

Путь: Администрирование > Общие > Сбросить/перезагрузить

Действие	Описание
Перезагрузить интерфейс управления	Перезапуск интерфейса платы управления.
Сбросить все ¹	Уберите флажок в поле Исключить TCP/IP , чтобы сбросить все настройки конфигурации; поставьте флажок Исключить TCP/IP , чтобы сбросить все настройки, кроме настроек TCP/IP
Только перезапустить ¹	Настройки TCP/IP: Задайте для настроек TCP/IP значения DHCP & BOOTP — значения, принятые по умолчанию, которые требуются для того, чтобы плата управления получала свои настройки TCP/IP от серверов DHCP или BOOTP. №. «Настройки TCP/IP линии связи» à pдд. 71.
	Конфигурация события: Сброс всех изменений конфигурации событий в значения, принятые по умолчанию, по событию или группе событий.
	Значения ИБП по умолчанию: Сбрасывает только настройки ИБП в исходные значения, сетевые настройки не меняются.
	Сигналы тревоги при разрыве связи с окружающей средой: Сброс всех сигналов тревоги, которые были вызваны потерей связи с внешними датчиками. Например, если датчик температуры отсоединился, что привело к появлению сигнала тревоги, сброс сигнала потери связи вернет сигнализацию состояния данного датчика в нормальное положение. Примечание: Для сброса сигналов тревоги датчика, подключенного к универсальному порту датчиков сетевой платы управления AP9631, отсоедините и вновь подключите датчик или перезапустите плату.
	Политика управления: Сброс настроек, которые определяют, как управляющая сетевая плата будет реагировать на сигналы тревоги, посылаемые устройством ввода-вывода с сухими контактами.
1. Сброс параметров может занять до одной минуты. Имя ИБП не сбрасывается.	

Конфигурирование связей

Путь: Администрирование > Общие > Быстрые ссылки

Выберите вкладку **Администрирование**, пункт **Общие** в верхнем меню и пункт **Быстрые ссылки** в левом меню навигации, чтобы иметь возможность увидеть и изменить связи URL, показываемые в нижнем левом углу каждого экрана интерфейса.

По умолчанию, указаны три ссылки, ведущие на веб-страницы:

- **Link 1:** Домашняя (начальная) страница www.apc.com.
- **Link 2:** Страница, на которой находятся примеры продуктов, реализованных на основе веб-технологий.
- **Link 3:** Домашняя страница службы удаленного контроля Remote Monitoring Service.

Чтобы изменить конфигурацию одного из указанных ниже элементов, щелкните имя ссылки в столбце **Дисплей**:

- **Дисплей:** Краткое имя ссылки, отображаемое на каждой странице интерфейса
- **Имя:** Имя, которое полностью определяет назначение или сетевой адрес ссылки
- **Адрес:** Любой URL—адрес, например, URL-адрес другого устройства или сервера

О плате управления

Путь: Администрирование > Общие > О программе

Сведения об оборудовании используются Службой технической поддержки при устранении неисправностей платы управления. Серийный номер и MAC-адрес также указаны на самой карте.

Сведения о микропрограммном обеспечении модулей Application Module, American Power Conversion OS (AOS) и Boot Monitor указывают название, версию микропрограммы, а также дату и время создания каждого модуля. Эта информация также используется при устранении неисправностей и позволяет определить, имеются ли обновления микропрограммного обеспечения на сайте.

Параметр **Бесперебойная работа управления** показывает продолжительность непрерывной работы интерфейса.

Мастер конфигурирования IP-параметров устройств

Возможности, требования и установка

Как использовать Мастер для конфигурирования настроек TCP/IP

Мастер конфигурирования IP-адресов устройств APC позволяет конфигурировать IP-адрес, маску подсети и шлюз по умолчанию одной или нескольких сетевых плат управления или сетевых устройств (устройств, имеющих встроенную плату управления). Мастер можно использовать любым из следующих способов:

Системные требования

Мастер работает с операционными системами Microsoft Windows 2000, Windows Server® 2003 и Windows XP.

Установка

Для установки Мастера с компактного диска *Utility*:

1. Если включена функция автозапуска, пользовательский интерфейс компакт-диска запустится после того, как вы вставите компакт-диск в дисковод. Если этого не произошло, откройте файл **contents.htm** на компакт-диске.
2. Щелкните **Device IP Configuration Wizard** и следуйте инструкциям.

Чтобы установить Мастер из загруженного исполняемого файла:

1. Перейдите на страницу загрузки **www.apc/tools/download**.
2. Загрузите программу Мастера Device IP Configuration Wizard.
3. Запустите исполняемый файл из папки, в которую вы его загрузили.

Экспорт параметров конфигурации

Получение и экспорт файла .ini

Краткое описание процедуры

Администратор может получать ini-файлы сетевой платы управления и экспортировать их в другую плату управления или в несколько плат управления.

1. Сконфигурируйте плату управления, чтобы получить настройки, которые вы хотите экспортировать.
2. Получите ini-файл из этой платы управления.
3. Отредактируйте файл, изменив как минимум настройки TCP/IP.
4. Используйте протокол передачи файлов, поддерживаемый платой управления, для загрузки копии файла в одну или несколько плат управления. Для загрузки файла в несколько плат управления используйте скрипт FTP или SCP, или служебную программу для работы с ini-файлами.

Каждая из указанных плат управления использует полученный файл для конфигурации собственных настроек, после чего удаляет его.

Содержание файла ini

Файл config.ini, полученный из платы управления, содержит:

- *заголовки разделов и ключевые слова* (только поддерживаемые устройством, с которого вы получили этот файл): Заголовки разделов представляют собой имена категорий, заключенные в скобки ([]). Ключевые слова в каждом из заголовков раздела представляют собой метки, описывающие определенные настройки платы управления. После каждого ключевого слова следует знак равенства и значение (принятое по умолчанию или заданное при конфигурировании).
- Ключевое слово *Override*: При заданном значении по умолчанию, данное ключевое слово препятствует экспорту одного или нескольких ключевых слов и их значений, определяемых устройством. Например, в разделе [NetworkTCP/IP] значение по умолчанию для слова *Override* (MAC-адрес управляющей карты) блокирует экспорт параметров SystemIP, SubnetMask, DefaultGateway и BootMode.

Подробные процедуры

Получение. Для задания и получения ini-файла для экспорта:

1. Если возможно, используйте интерфейс платы управления для конфигурирования ее настроек для экспорта. Непосредственное изменение содержимого ini-файла может вызвать ошибки.

2. Для использования FTP для получения файла config.ini из сконфигурированной платы управления:

a. Включите связь с платой управления, используя для этого ее IP-адрес:

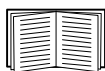
```
ftp> open ip_адрес
```

b. Войдите, используя учетную запись и пароль администратора.

c. Получите файл config.ini, содержащий настройки платы управления:

```
ftp> get config.ini
```

Файл будет сохранен в папке, из которой был запущен FTP.



О том, как получить параметры конфигурации нескольких плат управления и экспортировать их в другие платы управления, см. документ *Примечания к выпуску: Службная программа ini File Utility, версия 1.0*, на компакт-диске *Utility* для платы сетевого управления и в Интернете по адресу: **www.apc.com**.

Настройка. Файл необходимо отредактировать, перед тем как экспортировать его.

1. Для редактирования файла используйте текстовый редактор.

- Заголовки разделов, ключевые слова и предварительно заданные значения не зависят от регистра, но строковые переменные, задаваемые пользователем, зависят от регистра.
- Чтобы указать, что значение не задано, используйте кавычки. Например, LinkURL1=" " показывает, что URL специально не определен.
- Закрывайте в кавычки любые значения, которые содержат предшествующие или последующие разделы или уже заключены в кавычки.
- Для экспорта запланированных событий конфигурируйте значения непосредственно в ini-файле.
- Для экспорта системного времени с максимальной точностью, если принимающая плата управления имеет доступ к серверу протокола сетевого времени, настройте как enabled параметр NTPEnable:

```
NTPEnable=enabled
```

В противном случае, сократите время передачи, путем экспорта раздела [SystemDate/Time] в виде отдельного ini-файла.

- При добавлении комментариев начинайте каждую строку комментария с символа «точка с запятой» (;).

2. Скопируйте отредактированный файл в файл с другим именем в эту же папку:

- Имя файла может содержать до 64 символов и должно иметь суффикс ini.
- Сохраните исходный отредактированный файл для использования в будущем.
Сохраненный вами файл является единственным, который содержит ваши комментарии.

Передача файла на одну плату управления. Для передачи ini-файла на другую сетевую плату управления выполните одно из указанных действий:

- В веб-интерфейсе платы-приемника выберите вкладку **Администрирование**, пункт **Общие** в верхней строке меню и **Файл конфигурации пользователя** в левом меню навигации. Укажите полный путь к файлу или воспользуйтесь командой **Browse** (Обзор).
- Используйте любой из протоколов, поддерживаемых платой управления, например, FTP, FTP Client, SCP или TFTP. В приведенном примере используется протокол FTP:

- а. Из папки, содержащей копию отредактированного ini-файла, запустите FTP, чтобы войти в плату управления, в которую собираетесь экспортировать ini-файл.

```
ftp> open ip_адрес
```

- б. Экпортируйте копию отредактированного ini-файла в корневой каталог управляющей платы-приемника.

```
ftp> put имяфайла.ini
```

Экспорт файла на несколько плат управления. Чтобы экспортировать ini-файл на несколько сетевых управляющих плат:

- Используйте FTP или SCP, но напишите сценарий, который содержит и повторяет операции, используемые для экспорта файла на одну плату управления.
- Используйте пакетный командный файл и утилиту для работы с ini-файлом.



О том, как создать пакетный командный файл и использовать утилиту, см. *Примечания к выпуску: Программа для ini File, версия 1.0* на компакт-диске *Utility* для платы сетевого управления.

Сообщений о событиях загрузки и ошибках

Сообщения о событиях и ошибках, связанных с ним

Следующее событие происходит в том случае, когда принимающая сетевая плата управления заканчивает использование ini-файла для обновления своих настроек.

Configuration file upload complete, with номер valid values

Если ключевое слово, имя раздела или значения оказываются неверными, загрузка в плату управления завершается и выдается дополнительное сообщение об ошибке.

Текст сообщения о событии	Описание
Предупреждение по файлу конфигурации: неверное ключевое слово в строке номер.	Строка с неверным ключевым словом или значением игнорируется.
Предупреждение по файлу конфигурации: Неверное значение в строке номер.	
Предупреждение по файлу конфигурации: Неверная секция в строке номер.	Если имя секции указано неверно, все пары ключевых слов и значений в данной секции игнорируются.
Предупреждение по файлу конфигурации: Ключевое слово обнаружено вне секции в строке номер.	Ключевое слово, введенное в начале файла (то есть перед заголовком секции), игнорируется.
Предупреждение по файлу конфигурации: Размер файла конфигурации превышает предельно допустимый.	Если размер файла велик, происходит неполная загрузка. Уменьшите размер файла или разбейте его на два файла и повторите загрузку еще раз.

Сообщение в файле config.ini

Устройство, связанное с платой управления, с которой загружается файл config.ini, должно быть обнаружено успешно для включения его конфигурации. Если устройство (такое как ИБП) отсутствует или не обнаружено, файл config.ini в соответствующей секции, вместо ключевого слова или значений, будет содержать сообщение. Например:

UPS not discovered

IEM not discovered

Если вы не собираетесь экспортировать конфигурацию устройства как часть импортированного ini-файла, игнорируйте эти сообщения.

Ошибки, генерируемые заблокированными параметрами

При блокировке экспорта параметров ключевое слово `Override` и его значение генерируют сообщения об ошибке в журнале событий.



Сведения о том, какие параметры могут блокироваться, см. «Содержание файла `ini`» на стр. 100.

Поскольку блокируемые параметры относятся к конкретным устройствам и не пригодны для экспорта в другие платы управления, игнорируйте эти сообщения об ошибках. Чтобы предотвратить появление этих сообщений, удалите строки, содержащие ключевое слово `Override`, и строки, содержащие блокируемые параметры. Не удаляйте и не изменяйте строки, содержащие заголовки секций.

Связанные вопросы

В операционных системах Windows, вместо пересылки файлов `ini`, можно использовать программу-мастер конфигурации `Device IP Configuration Wizard`, чтобы изменять основные настройки TCP/IP платы управления и конфигурировать другие настройки через интерфейс пользователя.



См. «Мастер конфигурирования IP-параметров устройств» на стр. 99.

Передача файлов

Порядок обновления прошивки

Преимущества обновления прошивки

При обновлении прошивки платы сетевого управления 2 (ПСУ) ИБП:

- можно исправить ошибки и повысить производительность;
- обеспечить новые функции для использования в работе.

Если на всех серверах, установленных в сети, используется единая версия прошивки, то можно быть уверенным, что все ПСУ единым образом поддерживают одинаковый набор функциональных возможностей.

Файлы прошивки (плата сетевого управления 2)

Версия прошивки состоит из трех модулей: модуля операционной системы American Power Conversion (AOS), модуля приложения и модуля монитора загрузки (bootmon). Каждый модуль содержит один или несколько циклических тестов (CRC) с целью предохранения данных от повреждения при передаче.

Файлы модулей операционной системы American Power Conversion (AOS), приложения и монитора загрузки, используемые ПСУ, имеют одинаковый базовый формат:

```
apc_hardware-version_type_firmware-version.bin
```

- *apc*: обозначает контекст.
- *hardware-version*: *hw0x* указывает версию аппаратного обеспечения, с которым можно использовать этот двоичный файл.
- *type*: указывает, является ли данный файл модулем операционной системы American Power Conversion (AOS), модулем приложения или модулем монитора загрузки ПСУ.
- *version*: номер версии файла.
- *bin*: указывает на то, что это двоичный файл.

Получение новейшей версии прошивки



Примечание. При ручном обновлении можно пропустить установку монитора загрузки, если обновления отсутствуют. При использовании программы NMC2 Firmware Upgrade Utility все обновления монитора загрузки выполняются автоматически.

Службная программа NMC2 Firmware Upgrade Utility для операционных систем Microsoft Windows. Программа обновления прошивки ПСУ (NMC2 Firmware Upgrade) автоматизирует процесс передачи модулей прошивки в любых поддерживаемых операционных системах Windows. Загрузите новейшую версию программы бесплатно по адресу: www.apcc.com/tools/download. На этой веб-странице можно найти новейшие версии прошивки для изделий и программы автоматизации, входящие в комплект. **Не используйте** программу, предназначенную для одного изделия, для обновления прошивки другого изделия.

Обновление вручную, прежде всего для операционных систем Linux. Если ни один из компьютеров в Вашей сети не работает под управлением операционной системы Microsoft Windows, необходимо выполнять обновление прошивки ПСУ, используя отдельно модули операционной системы (AOS) и модули приложений.



Примечание. В случае ручного обновления вначале загрузите монитор загрузки, затем модуль операционной системы и после этого модуль приложения.

Извлечение файлов прошивки:

1. Запустите программу NMC2 Firmware Upgrade Utility.
2. После появления приглашения щелкните **Далее>**, а затем укажите местоположение папки, в которую будут помещены извлекаемые файлы.
3. После появления сообщения **Файлы извлечены** закройте диалоговое окно.

Способы передачи файлов прошивки

Для обновления прошивки ПСУ используйте один из указанных способов:

- На сетевом компьютере, работающем под управлением операционной системы Microsoft Windows, используйте программу NMC2 Firmware Upgrade Utility, загруженную с веб-сайта .



Примечание. Данная программа работает только с ПСУ, имеющими адрес IPv4.

- Для передачи отдельных модулей прошивки операционной системы AOS и приложения на компьютере, подключенном к сети и работающем под управлением любой поддерживаемой операционной системы, используйте FTP или SCP.
- В случае платы сетевого управления, которая не установлена в Вашей сети, используйте XMODEM и порт последовательной связи для передачи отдельных модулей прошивки с компьютера в ПСУ.



Предупреждение. При передаче модулей прошивки на ПСУ модуль операционной системы (AOS) **должен** быть передан до передачи модуля приложения.

- Используйте USB-диск для переноса отдельных модулей прошивки с компьютера на ПСУ (только для AP9631).

Обновление одной платы сетевого управления 2 с использованием протокола FTP или SCP

FTP. Чтобы использовать протокол FTP для обновления одной ПСУ через сеть, выполните следующие действия:

- ПСУ должна быть подключена к сети, должен быть настроен ее системный IP-адрес, маска подсети и шлюз по умолчанию.
- Сервер FTP должен быть разрешен в настройках ПСУ.
- Файлы прошивки должны быть извлечены с помощью программы NMC2 Firmware Upgrade (см. раздел «Извлечение файлов прошивки:»).

Чтобы передать файлы, выполните следующие действия:

1. Откройте на сетевом компьютере окно с командной строкой. Перейдите в папку, содержащую файлы прошивки, и просмотрите их список:

```
C:\>cd apc
```

```
C:\apc>dir
```

В указанных файлах xxx обозначает номер версии прошивки:

- apc_hw05_aos_xxx.bin
- apc_hw05_application_xxx.bin

2. Откройте клиентский сеанс FTP:

```
C:\apc>ftp
```

3. Наберите команду open, затем укажите IP-адрес ПСУ и нажмите клавишу ENTER. Если настройки порта (**port**) FTP-сервера отличаются от значения по умолчанию, равного **21**, необходимо использовать эти новые настройки в строке команды FTP.

- Для клиентов Windows FTP отделяйте номер порта от IP-адреса пробелом. Например:
ftp> open 150.250.6.10 21000
- Некоторые клиенты FTP требуют ставить перед номером порта двоеточие.

4. Войдите в систему с правами администратора; по умолчанию **apc** являются и именем пользователя, и паролем.
5. Выполните обновление операционной системы (AOS). (В примере xxx — номер версии прошивки):

```
ftp> bin
```

```
ftp> put apc_hw05_aos_xxx.bin
```

6. Когда FTP-сервер подтвердит передачу, введите quit, чтобы закрыть сеанс.
7. Через 20 секунд повторите операции с действ. 2 по действ. 6. В действ. 5 используйте имя файла модуля приложения.

SCP. Чтобы обновить прошивку ПСУ при помощи Secure CoPy (SCP), выполните следующие операции:

1. Определите и найдите модули прошивки, описанные в предыдущих командах для FTP.
2. С помощью командной строки SCP выполните передачу модуля прошивки AOS на ПСУ. В данном примере xxx обозначает номер версии модуля AOS:

```
scp apc_hw05_aos_xxx.bin apc@158.205.6.185:apc_hw05_aos_xxx.bin
```

3. Для передачи модуля приложения на ПСУ используйте схожую командную строку SCP, указав имя данного модуля.

Обновление нескольких плат сетевого управления

Программа обновления NMC2 Firmware Upgrade. Если Вы работаете в операционной системе Windows, используйте эту программу для обновления прошивки в IPv4. Программа записывает все шаги процедуры обновления в журнал, что дает возможность удобной проверки правильности обновления.

Настройки конфигурации экспорта. Можно создать командные файлы и использовать программу для получения параметров конфигурации нескольких ПСУ и экспортировать их на другие ПСУ.



См. документ *Release Notes: ini File Utility, version 1.0* (Примечания к выпуску: ini File Utility версии 1.0) на компакт-диске с *утилитами* для платы сетевого управления.

Использование протокола FTP или SCP для обновления нескольких ПСУ. Для обновления нескольких ПСУ с использованием клиента FTP или протокола SCP напишите скрипт, который будет выполнять эту процедуру автоматически.

Использование программы NMC2 Firmware Upgrade для нескольких обновлений

Загрузите программу с сайта, дважды щелкните файл с расширением exe, чтобы запустить программу (которая работает ТОЛЬКО с IPv4), и выполните следующие операции для обновления прошивки ПСУ:

1. Введите IP-адрес, имя пользователя и пароль, нажмите кнопку **Ping**, если хотите проверить IP-адрес.
2. Нажмите кнопку **Список устройств**, чтобы открыть файл `iplist.txt`. Он должен содержать список IP-адресов, имен пользователей и паролей всех устройств, например,
`SystemIP=192.168.0.1`
`SystemUserName=apc`
`SystemPassword=apc`

Новая программа работает со всеми существующими файлами `iplist.txt`, которые использовались старыми версиями этой программы.

3. Чтобы использовать файл `iplist.txt`, установите флажок **Обновить из списка устройств**. Снимите этот флажок, чтобы обновлять прошивку, вводя IP-адрес, имя пользователя и пароль в диалоговом окне.
4. Щелкните кнопку **Обновить**, чтобы запустить обновление прошивки.
5. Выберите **Просмотреть журнал** для проверки обновления.

Использование XMODEM для обновления одной ПСУ

Чтобы использовать XMODEM для обновления одной ПСУ, не находящейся в сети, необходимо извлечь файлы прошивки из программы NMC2 Firmware Upgrade Utility (см. раздел «Извлечение файлов прошивки:»).

Чтобы передать файлы, выполните следующие действия:

1. Выберите последовательный порт на локальном компьютере и отключите все службы, использующие этот порт.
2. С помощью прилагаемого кабеля (номер детали: 940-0299) подключите выбранный порт к последовательному порту ПСУ.

3. Запустите на компьютере программу терминала (например, HyperTerminal) и настройте следующие параметры для выбранного порта: скорость передачи 57600 бит/с, 8 бит данных, без проверки четности, 1 стоповый бит, без контроля потока.
4. Нажмите кнопку **Сбросить** на ПСУ, после чего сразу же дважды нажмите клавишу **Enter** или дождитесь появления приглашения монитора загрузки: VM>
5. Введите XMODEM и нажмите ENTER.
6. В меню программы терминала выберите XMODEM, затем выберите двоичный файл прошивки AOS, который будет передан с помощью XMODEM. По завершении передачи XMODEM на экране появится приглашение монитора загрузки.
7. Чтобы установить модуль приложения, повторите действия 5 и 6. В действии 6 укажите имя файла модуля приложения.
8. Наберите reset или нажмите кнопку «Сбросить», чтобы перезапустить ПСУ.



Дополнительные сведения о формате модулей прошивки см. в разделе «Файлы прошивки (плата сетевого управления 2)» на стр. 105.

Использование USB-диска для переноса файлов (только для AP9631)



Примечание. Перед началом переноса убедитесь, что USB-диск отформатирован с использованием системы FAT32.

1. Загрузите файлы обновлений и разархивируйте их.
2. Создайте на USB-диске папку с именем arcfirm.
3. Поместите извлеченные файлы в каталог arcfirm.
4. Подключите USB-диск к любому порту USB на ПСУ.
5. Выполните сброс ПСУ и дождитесь полной перезагрузки платы.
6. Убедитесь, что обновление было выполнено правильно, используя описанные в разделе «Проверка обновлений и исправлений» на стр. 109 процедуры.

Проверка обновлений и исправлений

Проверка результатов передачи

Чтобы проверить, успешно ли была загружена прошивка, используйте команду `xferStatus`, вводимую в командной строке интерфейса, чтобы увидеть результат последней передачи, или используйте SNMP GET в `mfiletransferStatusLastTransferResult` OID.

Коды результатов последней передачи

Код	Описание
Успешно	Передача файлов была успешной.
Результат недоступен	Нет сообщений о передаче файлов.
Неизвестная ошибка	Последняя передача файлов была неудачной по неизвестной причине.
Сервер недоступен	Не удалось найти сервер TFTP или FTP в сети.
Доступ к серверу закрыт	Доступ к серверу TFTP или FTP закрыт.
Файл не найден	Серверу TFTP или FTP не удалось найти запрашиваемый файл.
Неизвестный тип файла	Файл был загружен, но содержимое его не распознано.
Файл поврежден	Файл был загружен, но, как минимум, один код CRC ошибочен.

Проверка номеров версий установленной прошивки

Используйте веб-интерфейс для проверки версий модулей прошивки, для чего выберите вкладку **Администрирование**, пункт **Общие** в верхней строке меню и **О программе** в левом меню навигации, или используйте команду SNMP GET в MIB II **sysDescr** OID. В интерфейсе командной строки введите команду `about`.

Добавление и изменение языковых пакетов

Файлы языковых пакетов платы сетевого управления 2 содержат информацию, необходимую для отображения элементов пользовательского интерфейса на языках, отличных от английского. Каждый языковой пакет содержит до пяти языков (поэтому раскрывающийся список **Язык** дает возможность выбрать при загрузке один из пяти языков).

Интерфейс пользователя доступен на девяти языках: французском, итальянском, немецком, испанском, бразильском португальском, русском, корейском, японском и упрощенном китайском.

Файлы языковых пакетов находятся в разделе загрузок для ПСУ ИБП на веб-сайте, www.apc.com. Они имеют расширение `.lpk`, а также имя следующего формата:

```
<app name>_<app version>_<language codes>.lpk
```

Например, для 3-фазного приложения Symmetra имя файла будет иметь следующий вид:

```
sy3p_510_esESzhCnjaJAptBrkoKo.lpk
```

где `esESzhCnjaJAptBrkoKo`

обозначает испанский, китайский, японский, бразильский португальский и корейский.

Может потребоваться установить для интерфейса отсутствующий в нем язык. Для этого загрузите языковой пакет с веб-сайта и выполните следующие действия:

1. Подключитесь к ПСУ через протокол FTP.
2. Перешлите требуемый языковой пакет на плату сетевого управления. Например, напечатайте:
`put <full path/language pack name>.lpk`
3. По завершении передачи файла отключите FTP, выполняется перезагрузка ПСУ.
4. После завершения перезагрузки новый языковой пакет будет готов к работе.



Примечание. Все используемые в настоящее время языковые пакеты будут удалены перед загрузкой нового пакета. В случае неудачной загрузки языкового пакета ПСУ не будет иметь ни одного языкового пакета. В этих условиях будет доступен только английский язык. В таком случае попробуйте перезагрузить новый языковой пакет.

Поиск и устранение неисправностей

Проблемы доступа к плате управления



Если здесь нет описания возможных неисправностей, см. диаграммы поиска и устранения неисправностей на компакт-диске *Utility* для платы сетевого управления. Щелкните ссылку **Поиск и устранение неисправностей** на интерфейсе компакт-диска.

Если проблема остается, см. «Всемирная сервисная служба» на стр. 3.

Неисправность	Решение
Невозможно выполнить эхо-тестирование платы управления	Если индикатор состояния платы управления светится зеленым, попробуйте послать команду эхо-тестирования на другой узел того же сегмента сети, в котором расположена плата управления. Если тестирование не работает, то плата управления исправна. Если индикатор состояния горит не зеленым, а другим светом или если эхо-тестирование проходит успешно, проверьте следующее: <ul style="list-style-type: none">• Проверьте, чтобы плата управления была надежно установлена в ИБП.• Проверьте сетевые подключения.• Проверьте IP-адреса управляющей карты, проверьте платы управления и NMS.• Если NMS аппаратно находится в другой сети (или подсети), отличной от сети платы управления, проверьте IP-адрес шлюза по умолчанию (или маршрутизатора).• Проверьте число бит подсети для маски подсети платы управления.
Невозможно выделить коммуникационный порт через программу терминала	Перед тем как использовать программу терминала для конфигурирования платы управления, следует отключить все приложения, службы и программы, которые используют данный коммуникационный порт.
Невозможен доступ через интерфейс командной строки по каналу последовательного обмена	Проверьте, что вы не меняли настройки скорости обмена данными. Попробуйте установить значения 2400, 9600, 19200 или 38400 бит/с.
Невозможен удаленный доступ через интерфейс командной строки	<ul style="list-style-type: none">• Проверьте, что вы используете правильный способ доступа, Telnet или Secure SHell (SSH). Администратор может включить эти способы доступа. По умолчанию включен протокол Telnet. При включении SSH автоматически отключается Telnet.• При использовании SSH плата управления может создавать ключ хост-узла. Плате управления требуется до одной минуты для создания ключа хост-узла, в это время SSH будет недоступен.
Невозможно получить доступ через веб-интерфейс	<ul style="list-style-type: none">• Убедитесь, что доступ HTTP или HTTPS открыт.• Убедитесь, что вы указали правильное значение URL — согласующееся с системой безопасности, используемой платой управления. SSL требует указать параметр https, а не http в начале адреса URL.• Проверьте, чтобы выполнялось эхо-тестирование платы управления.• Убедитесь, что вы используете браузер, поддерживаемый платой управления. №. «Поддерживаемые веб-браузеры» на стр. 31.• Если плата управления только что перезагрузилась, и была установлена система безопасности SSL, возможно, плата управления создает сертификат сервера. Для создания этого сертификата плате управления потребуется до одной минуты, в это время сервер SSL будет недоступен.

Неисправности SNMP

Неисправность	Решение
Невозможно выполнить операцию GET	<ul style="list-style-type: none"> Проверьте имя сообщества (SNMPv1) с правом чтения (GET) или конфигурацию профиля пользователя (SNMPv3). Используйте интерфейс командной строки или веб-интерфейс для проверки доступа NMS. №. «SNMP» на стр. 80.
Невозможно выполнить операцию SET	<ul style="list-style-type: none"> Проверьте имя сообщества (SNMPv1) с правом чтения/записи (SET) или конфигурацию профиля пользователя (SNMPv3). Используйте интерфейс командной строки или веб-интерфейс для проверки того, что NMS имеет доступ на запись (SET) (SNMPv1) или получил доступ к адресу IP в списке управления доступом (SNMPv3). №. «SNMP» на стр. 80.
Невозможно получить прерывания на NMS	<ul style="list-style-type: none"> Проверьте, чтобы тип прерывания (SNMPv1 или SNMPv3) был правильно сконфигурирован для NMS, используемого в качестве приемника прерываний. В случае SNMP v1 пошлите запрос mconfigTrapReceiverTable MIB OID, чтобы проверить, что IP-адрес NMS указан корректно, и что имя сообщества, указанное в NMS, соответствует имени сообщества, указанному в таблице. Если что-либо указано неправильно, используйте команду SET для mconfigTrapReceiverTable OID или используйте интерфейс командной строки или веб-интерфейс, чтобы исправить настройки приемника прерываний. В случае SNMPv3 проверьте настройки профиля пользователя для NMS и запустите тест прерываний. <p>См «SNMP» на стр. 80, «Получатели прерываний» на стр. 89 и «Тестирование прерываний SNMP» на стр. 90.</p>
Прерывания, получаемые NMS, не определены	См. документацию по NMS, чтобы проверить, что прерывания правильно указаны в базе данных сигналов тревоги и прерываний.

Проблемы синхронизации

Неисправность	Решение
Член группы синхронизированного управления не участвует в процессе синхронизации.	Проверьте, чтобы статус члена группы был указан как Включено . Проверьте также емкость его аккумуляторной батареи, если действие синхронизации требует включения ИБП.
Попытка добавить дополнительное устройство в группу синхронизированного управления окончилась неудачей.	Значения группового IP-адреса, номера группы синхронизированного управления и версия микропрограммного обеспечения отличаются от аналогичных параметров других членов группы.

Приложение А: Интерфейс командной строки

?	ntp
about	[-OM [enable disable]]
alarmcount	[-p <primary NTP server>]
[-p [all warning critical]]	[-s <secondary NTP server>]
boot	ping
[-b <dhcp bootp manual>]	<IP address or DNS name>]
[-c <dhcp cookie> [enable disable]]	portspeed
[-v <vendor class>]	[-s [auto 10H 10F 100H 100F]]
[-i <client id>]	prompt
[-u <user class>]	[-s [long short]]
cd	quit
console	radius
[-S <disable telnet ssh>]	[-a <access> [local radiusLocal radius]]
[-pt <telnet port #>]	[-p# <server IP>]
[-ps <ssh port #>]	[-s# <server secret>]
[-b <baud rate> [2400 9600 19200 38400]]	[-t# <server timeout>]
date	reboot
[-d <“datestring”>]	resetToDef
[-t <00:00:00>]	[-p [all keepip]]
[-f [mm/dd/yy dd.mm.yyyy mmm-dd-yy	snmp, snmp3
dd-mmm-yy yyyy-mm-dd]]	[-S [enable disable]]
[-z <time zone offset>]	system
delete	[-n <system name>]
dir	[-c <system contact>]
dns	[-l <system location>]
[-OM [enable disable]]	tcpip
[-p <primary DNS server>]	[-i <IP address>]
[-s <secondary DNS server>]	[-s <subnet mask>]
[-d <domain name>]	[-g <gateway>]
[-n <domain name IPv6>]	[-d <domain name>]
[-h <host name>]	[-h <host name>]
eventlog	tcpip6
exit	[-S [enable disable]]
format	[-man [enable disable]]
ftp	[-auto [enable disable]]
[-p <port number>]	[-i <IPv6 address>]
[-S <enable disable>]	[-g <IPv6 gateway>]
help	[-d6 [router stateful stateless never]]
netstat	uio
	[-rc <dI> [open close]]
	[-st <port # port #]]
	[-disc <port # port #]]

ups

[-c <off | graceoff | on | reboot | gracereboot | sleep | gracesleep>]

[-r <start | stop>]

[-s <start>]

[-b <enter | exit>]

[-o# <off | delayoff | on | delayon | reboot>]

[-os#]

[-st]

user

[-an <Administrator name>]

[-dn <Device User name>]

[-rn <Read-Only User name>]

[-ap <Administrator password>]

[-dp <Device User password>]

[-rp <Read-Only User password>]

[-t <inactivity timeout in minutes>]

web

[-S <disable | http | https>]

[-ph <http port #>]

[-ps <https port #>]

xferINI

xferStatus

Двухлетняя гарантия производителя

Условия настоящей гарантии распространяются только на изделия, приобретенные для собственного использования в соответствии с данным руководством.

Условия гарантии

Компания APC гарантирует, что ее продукция не будет иметь дефектов материалов и изготовления в течение двух лет с даты покупки. Компания APC гарантирует ремонт или замену неисправных изделий, на которые распространяются условия настоящей гарантии. Данная гарантия не распространяется на оборудование, поврежденное вследствие несчастного случая, небрежности или неправильного использования, либо если оно было изменено или доработано каким-либо способом. В случае ремонта или замены неисправного Изделия или его детали исходный гарантийный срок не продлевается. Компоненты, предоставляемые согласно данной гарантии, могут быть либо новыми, либо отремонтированными в заводских условиях.

Гарантия, не допускающая передачи

Данная гарантия относится только к первоначальному покупателю, который должен был соответствующим образом зарегистрировать изделие. Продукт можно зарегистрировать на веб-сайте компании APC: www.apc.com.

Исключения

Компания APC не несет ответственности по гарантии, если в результате тестирования и исследования было обнаружено, что предполагаемый дефект изделия не существует или его причиной явились неправильное использование пользователем или третьим лицом, небрежность, несоответствующая установка или тестирование. В дальнейшем компания APC не будет нести ответственности за несанкционированные попытки ремонта или изменения неадекватного электрического напряжения или подключения, несоответствующие условия эксплуатации на месте, коррозионную атмосферу, ремонт, установку, воздействия окружающей среды, стихийные бедствия, пожар, кражу или установку, противоречащую рекомендациям или спецификациям компании APC, или любое событие, при котором серийный номер APC был изменен, искажен или удален, или любую другую причину вне рамок планируемого использования.

НЕ СУЩЕСТВУЕТ ДРУГИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ПРИНИМАЕМЫХ В СИЛУ ЗАКОНА ИЛИ ИНЫХ, НА ПРОДАВАЕМЫЕ, ОБСЛУЖИВАЕМЫЕ ИЛИ ПРЕДОСТАВЛЯЕМЫЕ ИЗДЕЛИЯ ПО УСЛОВИЯМ ДАННОГО СОГЛАШЕНИЯ ИЛИ В СВЯЗИ С ИЗЛОЖЕННОЙ ЗДЕСЬ ИНФОРМАЦИЕЙ. КОМПАНИЯ APC ОТКАЗЫВАЕТСЯ ОТ ВСЕХ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ КОММЕРЧЕСКОЙ ЦЕННОСТИ, ИСПОЛНЕНИЯ И ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ. ЯВНЫЕ ГАРАНТИИ КОМПАНИИ APC НЕ БУДУТ РАСШИРЕНЫ, СОКРАЩЕНЫ ИЛИ ЗАТРОНУТЫ ВСЛЕДСТВИЕ (И НИКАКИЕ ГАРАНТИИ ИЛИ ОБЯЗАТЕЛЬСТВА НЕ БУДУТ ЯВЛЯТЬСЯ РЕЗУЛЬТАТОМ) ПРЕДОСТАВЛЕНИЯ КОМПАНИЕЙ APC ТЕХНИЧЕСКОЙ ИЛИ ДРУГОЙ КОНСУЛЬТАЦИИ ИЛИ УСЛУГИ В ОТНОШЕНИИ ИЗДЕЛИЙ. ВЫШЕПЕРЕЧИСЛЕННЫЕ ГАРАНТИИ И СРЕДСТВА ВОЗМЕЩЕНИЯ ЯВЛЯЮТСЯ ОГРАНИЧЕННЫМИ И РАВНОСИЛЬНЫМИ ВСЕМ ДРУГИМ ГАРАНТИЯМ И СРЕДСТВАМ ВОЗМЕЩЕНИЯ. ИЗЛОЖЕННЫЕ ВЫШЕ УСЛОВИЯ ГАРАНТИЙ УСТАНАВЛИВАЮТ ЕДИНОЛИЧНУЮ ОТВЕТСТВЕННОСТЬ КОМПАНИИ APC И ИСКЛЮЧИТЕЛЬНЫЕ УСЛОВИЯ ОБСЛУЖИВАНИЯ ПОКУПАТЕЛЕЙ В СЛУЧАЕ ЛЮБОГО НАРУШЕНИЯ ТАКИХ ГАРАНТИЙ. ДЕЙСТВИЕ ГАРАНТИЙ КОМПАНИИ APC РАСПРОСТРАНЯЕТСЯ ТОЛЬКО НА ПОКУПАТЕЛЯ И НЕ РАСПРОСТРАНЯЕТСЯ НА ТРЕТЬИХ ЛИЦ.

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ КОМПАНИЯ APC, ЕЕ СЛУЖАЩИЕ, РУКОВОДИТЕЛИ, СОТРУДНИКИ ФИЛИАЛОВ И ШТАТНЫЕ СОТРУДНИКИ НЕ БУДУТ НЕСТИ ОТВЕТСТВЕННОСТЬ ЗА КОСВЕННЫЙ, СПЕЦИАЛЬНЫЙ, ПОБОЧНЫЙ ИЛИ ШТРАФНОЙ УЩЕРБ, ВОЗНИКШИЙ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ, ОБСЛУЖИВАНИЯ ИЛИ УСТАНОВКИ ИЗДЕЛИЙ, НЕЗАВИСИМО ОТ ТОГО, УПОМИНАЛОСЬ ЛИ О ТАКОМ УЩЕРБЕ В ДОГОВОРЕ ИЛИ ДЕЛИКТЕ,

БУДЬ ТО НЕИСПРАВНОСТЬ, НЕБРЕЖНОСТЬ ИЛИ ЯВНЫЙ НЕДОСТАТОК, ИЛИ ОТ ТОГО, БЫЛА ЛИ КОМПАНИЯ APC ИНФОРМИРОВАНА О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА. В ЧАСТНОСТИ, КОМПАНИЯ APC НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБЫЕ ЗАТРАТЫ И ИЗДЕРЖКИ, ТАКИЕ КАК ПОТЕРЯ ПРИБЫЛИ ИЛИ ДОХОДА, ВЫВЕДЕНИЕ ИЗ СТРОЯ ОБОРУДОВАНИЯ, НЕВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ ОБОРУДОВАНИЯ, ПОТЕРЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ПОТЕРЯ ИНФОРМАЦИИ, СТОИМОСТЬ ЗАМЕНЫ, ИСКИ ТРЕТЬИХ ЛИЦ И ДРУГИЕ.

НИ ОДИН ПРОДАВЕЦ, СОТРУДНИК ИЛИ АГЕНТ КОМПАНИИ APC НЕ УПОЛНОМОЧЕН ДОБАВЛЯТЬ ИЛИ ИЗМЕНЯТЬ УСЛОВИЯ ДАННОЙ ГАРАНТИИ. УСЛОВИЯ ГАРАНТИИ МОГУТ БЫТЬ ИЗМЕНЕНЫ (ЕСЛИ ВООБЩЕ МОГУТ БЫТЬ ИЗМЕНЕНЫ) ТОЛЬКО В ПИСЬМЕННОЙ ФОРМЕ, С ПОДПИСЯМИ ДОЛЖНОСТНОГО ЛИЦА И ЮРИДИЧЕСКОГО ОТДЕЛА КОМПАНИИ APC.

Гарантийные претензии

Клиенты, у которых возникли вопросы по гарантии, могут обратиться в центр сервисного обслуживания APC с помощью страницы “Поддержка” на веб-сайте APC: www.apc.com/support. В верхней части страницы выберите Вашу страну в соответствующем списке. Для получения информации о центрах сервисного обслуживания в Вашем регионе выберите вкладку “Support” (Поддержка).

Всемирная сервисная служба

Сервисное обслуживание для данного или любого другого изделия компании предоставляется бесплатно одним из следующих способов:

- Посетите веб-сайт компании, где вы найдете ответы на наиболее часто задаваемые вопросы (FAQ), сможете просмотреть документы базы знаний и послать запрос сервисной службе.
 - **www.apc.com** (штаб-квартира корпорации)
Посетите локализованные веб-сайты компании для отдельных стран, на каждом из которых содержится информация о технической поддержке.
 - **www.apc.com/support/**
Глобальная поддержка с помощью ответов на часто задаваемые вопросы (FAQ), базы знаний и сети Интернет (e-support).
- Обращайтесь в центр сервисного обслуживания компании по телефону или электронной почте (e-mail).
 - Региональные центры:

Европа, Ближний Восток, Африка	(353)(91)702000 (Ирландия)
Россия	8 800 200 27 22 apcrustech@apc.com

- Местные центры для отдельных стран: см. контактную информацию на веб-сайте **www.apc.com/support/contact**.

По вопросам сервисного обслуживания на месте установки обращайтесь в представительство компании или к дистрибьютору, у которого вы приобрели изделие производства компании.

© 2012 APC by Schneider Electric. The Schneider Electric logo, InfraStruXure, Smart-UPS, Symmetra, PowerNet, and PowerChute are owned by Schneider Electric Industries S.A.S., American Power Conversion Corporation, or their affiliated companies. All other trademarks are property of their respective owners.