

Руководство пользователя

Плата сетевого управления 3 для ИБП

AP9640, AP9641, AP9643

990-91148D-028

03/2021

Правовая оговорка корпорации Schneider Electric

Корпорация Schneider Electric не гарантирует надежность, безошибочность и полноту представленной в настоящем руководстве информации. Данное издание не является заменой подробному оперативному плану, разработанному с учетом конкретных условий монтажа. Таким образом, корпорация Schneider Electric не несет никакой ответственности за ущерб, нарушения законов, неправильно выполненный монтаж, сбой системы и другие проблемы, которые могут возникнуть в связи с использованием настоящего издания.

Информация, содержащаяся в настоящем издании, предоставляется в виде «как есть» исключительно для расчета и проектирования вычислительного центра. Информация для данного издания была добросовестно собрана корпорацией Schneider Electric. Однако не дается никакой гарантии, выраженной или подразумеваемой, в отношении полноты и точности представленной в издании информации.

КОРПОРАЦИЯ SCHNEIDER ELECTRIC ИЛИ ЛЮБАЯ ГОЛОВНАЯ ИЛИ ДОЧЕРНЯЯ КОМПАНИЯ ИЛИ ФИЛИАЛ КОРПОРАЦИИ SCHNEIDER ELECTRIC ИЛИ СООТВЕТСТВУЮЩИЕ СЛУЖАЩИЕ, РУКОВОДИТЕЛИ, СОТРУДНИКИ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБЫЕ ПРЯМЫЕ, КОСВЕННЫЕ, ПОБОЧНЫЕ, ШТРАФНЫЕ, ОСОБЫЕ ИЛИ СЛУЧАЙНЫЕ УБЫТКИ (ВКЛЮЧАЯ, В ТОМ ЧИСЛЕ, УБЫТКИ ИЗ-ЗА УТРАТЫ ПРЕДПРИЯТИЯ, РАСТОРЖЕНИЯ ДОГОВОРА, ПОТЕРИ ВЫРУЧКИ, ДАННЫХ, ИНФОРМАЦИИ ИЛИ ПРЕРЫВАНИЯ ДЕЯТЕЛЬНОСТИ), ВОЗНИКШИЕ В РЕЗУЛЬТАТЕ ИЛИ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ НАСТОЯЩЕГО ИЗДАНИЯ ИЛИ НЕСПОСОБНОСТИ ЕГО ИСПОЛЬЗОВАТЬ, ДАЖЕ ЕСЛИ КОРПОРАЦИЯ SCHNEIDER ELECTRIC БЫЛА НЕПОСРЕДСТВЕННО УВЕДОМЛЕНА О ВОЗМОЖНОСТИ ТАКИХ УБЫТКОВ. КОРПОРАЦИЯ SCHNEIDER ELECTRIC ОСТАВЛЯЕТ ЗА СОБОЙ ПРАВО ИЗМЕНЯТЬ ИЛИ ОБНОВЛЯТЬ СОДЕРЖАНИЕ И ФОРМАТ НАСТОЯЩЕГО ИЗДАНИЯ В ЛЮБОЕ ВРЕМЯ БЕЗ УВЕДОМЛЕНИЯ.

Авторские, интеллектуальные и иные имущественные права на содержание (включая, в том числе программное обеспечение, звуковые и видеофайлы, текст и фотографии) настоящего издания принадлежат корпорации Schneider Electric или ее лицензиарам. Все права на содержание, не предоставленные явным образом в настоящем документе, защищены. Никакие права не передаются, не отчуждаются и не переходят лицам, получающим доступ к данной информации.

Настоящее издание целиком или любая его часть не подлежат перепродаже.

Содержание

Введение	1
Описание продукта	1
Функции	1
Поддерживаемые устройства	2
Исходная настройка IPv4	2
Исходная настройка IPv6	2
Сетевое управление с использованием других приложений ...	3
Функции внутреннего управления	4
Обзор	4
Приоритет доступа при входе в систему	4
Типы учетных записей	4
Сброс настроек ПСУ в случае забытого пароля	5
Передняя панель (AP9640)	6
Передняя панель (AP9641)	7
Передняя панель (AP9643)	8
Описание индикаторов состояния	9
Индикатор состояния	9
Индикатор активности сети Link-RX/TX (10/100/1000)	9
Функции защиты	10
Обзор	10
Механизм сетевого интерфейса Watchdog	10
Сброс таймера сети	10
Автоматический выход из системы	10
Веб-интерфейс пользователя	11
Введение	11
Обзор	11
Поддерживаемые веб-браузеры	11
Вход в систему	11
Обзор	11
Форматы URL-адреса	12
Первое подключение	13
Обзор	13
Значки и ссылки	13

Мониторинг ИБП: меню «Состояние»	14
ИБП в меню состояния	14
Группы розеток в меню состояния	16
Система батарей в меню статуса	16
Универсальный ввод-вывод в меню «Состояние»	17
Сеть в меню состояния	18
Управление ИБП	19
ИБП в меню управления	19
«Группы розеток» в меню управления	21
«Безопасность» в меню управления	22
«Сеть» в меню управления	23
Настройка параметров: 1	24
«Группы розеток» в меню конфигурации	24
Описание групп розеток	24
Настройка групп розеток	25
Настройки питания в меню конфигурации	26
«Выключение» в меню конфигурации	27
Начало выключения	27
Продолжительность выключения	28
Параметры выключения PowerChute	29
Экран «ИБП: общее»	31
Экран «Расписание самодиагностики»	32
Планирование выключения	33
Для обоих параметров: ИБП и «Группы розеток»	33
Экран «Обновление прошивки»	33
Обновление прошивки ИБП с USB-накопителя (только AP9641 или AP9643)	34
Использование FTP для обновления прошивки ИБП	34
Клиенты сетевого выключения PowerChute	35

Экран «Универсальный ввод-вывод»	35
Экран «Температура и влажность»	35
Экран «Входные контакты»	36
Экран «Выходное реле»	36
Настройка политики управления	37
Меню «Безопасность»	38
Экран «Управление сеансом»	38
Ответ ring	38
Локальные пользователи	38
Аутентификация удаленных пользователей	39
Экран RADIUS	40
Конфигурирование сервера RADIUS	40
Экраны брандмауэра	41
802.1 X Конфигурация безопасности	45
Настройка параметров: 2	46
«Сеть» в меню конфигурации	46
Экран настроек TCP/IP для IPv4	46
Экран настроек TCP/IP для IPv6	47
Параметры ответов DHCP	48
Экран «Скорость порта»	49
Экран DNS	49
Экран проверки DNS	50
Экран веб-доступа	51
Веб-экран сертификата SSL	51
Экран консоли	51
Экраны SNMP	52
Экраны Modbus	55
Экран BACnet	55
Конфигурация BACnet	56
Экран сервера FTP	58
Экран Wi-Fi (только AP9641 и AP9643)	58
Меню уведомлений	59
Типы уведомлений	59
Конфигурирование действий для событий	60
Экран уведомлений по электронной почте	61
Экран получателей системных прерываний SNMP	63
Экран тестирования прерываний SNMP	64
Меню «Общие»	65
Экран «Идентификация»	65
Экран даты и времени	65
Создание и импорт настроек с помощью файла конфигурации	66
Экран конфигурирования ссылок	66

Журналы в меню конфигурации	67
Идентификация серверов Syslog	67
Настройки системного журнала	67
Пример теста и формата Syslog	68
Меню «Тесты»	73
Тестирование и калибровка	73
Включение мигания светодиодов PSU	73
Меню «Журналы» и «О программе»	74
Использование журналов событий и данных	74
Журнал событий	74
Журнал данных	75
Использование протокола FTP или SCP для получения файлов журнала	76
Журнал ИБП	78
Потребление энергии	78
Журнал брандмауэра	78
О плате сетевого управления 3	80
Об устройстве ИБП	80
Информация о PSU и модулях микропрограммы	80
Экран поддержки	81
Мастер настройки IP-конфигурации устройств ...	82
Возможности, требования и установка	82
Системные требования	82
Установка	82
Экспорт параметров конфигурации	83
Получение и экспорт файла .ini	83
Краткое описание процедуры	83
Содержание файла ini	83
Подробные процедуры	83
Сообщения о событиях загрузки и ошибках	85
Сообщения о событиях и ошибках, связанных с ним	85
Сообщения в файле config.ini	85
Ошибки, генерируемые заблокированными параметрами ..	85

Связанные вопросы	86
Передача файлов	87
Обновление микропрограммы	87
Способы передачи файлов микропрограммы	87
Использование программы обновления микропрограммы ПСУ	87
Использование FTP или SCP для обновления одной платы сетевого управления	88
Использование XMODEM для обновления одной ПСУ	89
Обновление микропрограммы на нескольких платах сетевого управления	89
Проверка обновлений	90
Коды результатов последней передачи	90
Проверка номеров версий установленного микропрограммного обеспечения	90
Смена языка интерфейса пользователя	91
Устранение проблем	92
Проблемы доступа к плате сетевого управления	92
Неисправности SNMP	93
Проблемы с Modbus	93
Неисправности аппаратного ключа устройства APC USB Wi-Fi (AP9834)	94
Описание индикаторов состояния	95
Двухлетняя гарантия производителя	96
Условия гарантии	96
Гарантия без права передачи	96
Исключения	96
Гарантийные претензии	97

Введение

Описание продукта

Функции

Указанные ниже платы сетевого управления ИБП (ПСУ) производства компании Schneider Electric представляют собой веб-продукты, имеющие сертификат IPv6 Ready. Устройствами с установленными ПСУ можно управлять с использованием различных открытых стандартов, таких как:



Протокол передачи гипертекста (HTTP)	Безопасный командный процессор (SSH)
Простой протокол сетевого управления версий 1, 2с и 3	Протокол передачи гипертекста на уровне защищенных сокетов (HTTPS)
Протокол передачи файлов (FTP)	Secure Copy (SCP)
Telnet	Syslog
RADIUS	Modbus
Сетевой протокол ВАСnet (Building Automation and Control Networks Protocol)	Расширяемый протокол аутентификации (EAP) по локальной сети (EAPoL)

Плата сетевого управления AP9640:

- Обеспечивает управление ИБП и имеет функции планирования самодиагностики.
- Обеспечивает регистрацию данных и журналы событий.
- Позволяет настраивать уведомления с помощью регистрации событий, электронной почты, системного журнала (Syslog) и SNMP-прерываний.
- Обеспечивает поддержку сетевого выключения PowerChute®.
- Обеспечивает поддержку использования сервера протокола динамической конфигурации узла (Dynamic Host Configuration Protocol — DHCP) или протокола начальной загрузки (BOOTstrap Protocol — BOOTP) для предоставления сетевых значений (TCP/IP) платы сетевого управления.
- Предоставляет возможность экспорта пользовательского файла конфигурации (.ini) с настроенной платы на одну или более ненастроенных плат без преобразования файла в двоичный файл.
- Обеспечивает выбор протоколов защиты для аутентификации или шифрования.
- Обеспечивает связь с StruxureWare Data Center Expert, StruxureWare Operations или EcoStruxure™ IT.
- Поддерживает протокол Modbus TCP/IP.
- Поддерживает протокол ВАСnet/IP.

Плата сетевого управления **AP9641** включает в себя все функции платы сетевого управления AP9640, а также перечисленные ниже возможности:

- Оборудована двумя портами USB, которые поддерживают обновление микропрограммы ИБП с флеш-накопителя USB и дополнительного устройства APC USB Wi-Fi (AP9834).
- Поддерживает два универсальных порта ввода-вывода, к которым можно подключить следующие устройства:
 - датчик температуры (AP9335T) или датчик температуры/влажности (AP9335TH);
 - входные-выходные разъемы реле, которые поддерживают два входных контакта и одно выходное реле (с использованием устройства ввода-вывода с сухими контактами AP9810, которое является дополнительным компонентом).
- Поддерживает связь Modbus RTU через универсальный ввод-вывод порта 2 в дополнение к протоколу Modbus TCP/IP. Более подробно о конфигурации Modbus RTU см. в дополнительной документации к Modbus RTU.

Плата сетевого управления (ПСУ) **AP9643** включает в себя все функции платы сетевого управления (ПСУ) AP9640, а также перечисленные ниже возможности.

- Оборудована двумя портами USB, которые поддерживают обновление микропрограммы ИБП с флеш-накопителя USB и дополнительного устройства APC USB Wi-Fi (AP9834).
- Поддерживает один универсальный порт ввода-вывода, к которому можно подключить следующие устройства.
 - Датчики температуры (AP9335T) или температуры/влажности (AP9335TH).
 - Соединения релейного ввода-вывода, которые поддерживают два входных контакта и одно выходное реле (с использованием устройства ввода-вывода с сухими контактами AP9810, которое является дополнительным компонентом).
- Поддерживает связь Modbus RTU через последовательный порт RS485 в дополнение к протоколу Modbus TCP/IP. Более подробно о конфигурации Modbus RTU см. в разделе «Дополнительная документация к Modbus».

Поддерживаемые устройства

Плата сетевого управления 3 совместима со следующими устройствами.

- Устройства Smart-UPS® с разъемом SmartSlot, обладающие префиксами SMT, SMX, SRT и SURTD, и устройства SUA, изготовленные после 2008 г. *
- 1-фазные ИБП Symmetra®.



*Полный список совместимых ИБП, в которые можно установить ПСУ 3, см. в статье [FA237786](#) базы знаний на [веб-сайте APC](#).

Исходная настройка IPv4

Чтобы ПСУ могла работать в сети, необходимо настроить следующие параметры TCP/IP:

- IP-адрес ПСУ;
- маска подсети для ПСУ;
- IP-адрес шлюза по умолчанию (требуется только в том случае, если превышен размер сегмента).

ПРИМЕЧАНИЕ. Если шлюз по умолчанию недоступен, используйте IP-адрес компьютера, который обычно работает и находится в той же подсети, что и ПСУ. ПСУ использует шлюз по умолчанию для проверки сети при низком трафике.

ПРИМЕЧАНИЕ. Плата сетевого управления имеет префикс MAC-адреса 00:C0:B7 или 28:29:86.

Чтобы проверить MAC-адрес ПСУ, перейдите в меню **О программе > Сеть**. Этот префикс MAC-адреса можно использовать для настройки службы DHCP.



ПРИМЕЧАНИЕ. Не используйте адрес обратной связи (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 [веб-сайте APC](#) и в печатном виде.

Подробные сведения об использовании сервера DHCP для настройки параметров TCP/IP на плате сетевого управления см. в разделе «Параметры ответов DHCP».

Исходная настройка IPv6

Конфигурация сети IPv6 обеспечивает универсальные возможности для выполнения требований пользователя. IPv6 можно использовать в любом месте, где в этом интерфейсе вводится IP-адрес. Настройку можно осуществлять вручную, автоматически или с помощью DHCPv6; см. «Экран настроек TCP/IP для IPv6».

Сетевое управление с использованием других приложений

Эти приложения, утилиты и ресурсы работают с ИБП, который подключается к сети через ПСУ.

- Сетевое выключение PowerChute — автоматическое корректное отключение компьютеров, подключенных к устройствам ИБП.
- APC PowerNet[®] MIB — информация о доступе к устройствам ИБП по протоколу SNMP.
- StruxureWare Data Center Expert — управление электропитанием на уровне предприятия и управление агентами SNMP, такими как сетевые устройства ИБП и датчики окружающей среды.
- EcoStruxure IT Gateway — облачное ПО для мониторинга, позволяющее отслеживать устройства ИБП через протоколы SNMP и Modbus.
- Мастер настройки IP-конфигурации устройств — настройка основных параметров одной или нескольких плат сетевого управления в сети; см. «Мастер настройки IP-конфигурации устройств».
- Security Wizard — создание сертификатов сервера безопасности на транспортном уровне (Transport Layer Security — TLS) и хост-ключей Secure Shell (SSH), которые помогают защитить целостность и конфиденциальность связи с ПСУ.

Функции внутреннего управления

Обзор

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



Более подробную информацию об интерфейсе пользователя см. в разделе «Веб-интерфейс пользователя» и [руководстве для интерфейса командной строки на веб-сайте APC](#). См. раздел «Экраны SNMP» для получения информации о контроле доступа к ПСУ по протоколу SNMP.

Приоритет доступа при входе в систему

Можно включить возможность одновременного входа в систему нескольких пользователей, которые обладают равными правами доступа. См. раздел «Экран «Управление сеансом»».

Типы учетных записей

ПСУ обладает различными уровнями доступа — привилегированный пользователь, администратор, пользователь устройства, только чтение, только сеть:

- **Привилегированный пользователь** может использовать все меню интерфейса пользователя и все команды в интерфейсе командной строки. Привилегированный пользователь также определяет дополнительные учетные записи пользователей и устанавливает переменные для других пользователей. При первом входе в систему как имя пользователя, так и пароль по умолчанию `apc`. После входа в систему будет предложено ввести новый пароль.
Примечание. Привилегированного пользователя нельзя переименовать или удалить, но можно выключить. Рекомендуется выключить учетную запись привилегированного пользователя после создания дополнительных учетных записей администратора. Перед выключением привилегированного пользователя убедитесь, что создана как минимум одна учетная запись администратора.
- **Администратор** может использовать все меню интерфейса пользователя и все команды в интерфейсе командной строки. По умолчанию используется имя пользователя `apc`, а перед активацией учетной записи пользователя необходимо установить пароль.
- Пользователь с правами **пользователя устройства** обладает правами доступа для чтения и записи к экранам, относящимся к устройству. Функции администратора, такие как управление сеансами в меню «Безопасность» и «Брандмауэр» в меню «Журналы», заблокированы.

По умолчанию используется имя пользователя `device`, а перед активацией учетной записи пользователя необходимо установить пароль.

- Пользователь с правами **только чтения** обладает следующим ограниченным доступом:
 - Доступ только через интерфейс пользователя.
 - Доступ к тем же меню, что и для пользователя устройства, описанного выше, но без возможности изменения настроек, управления устройствами, удаления данных или использования параметров передачи файлов. Ссылки на параметры конфигурации отображаются, но неактивны. (При отображении журналов событий и данных кнопка очистки журнала для данного пользователя не отображается.)

По умолчанию используется имя пользователя `readonly`, а перед активацией учетной записи пользователя необходимо установить пароль.

- Пользователь с правами **только сеть** может выполнять вход только с помощью веб-интерфейса пользователя и интерфейса командной строки (Telnet/SSH, а не последовательный порт). Имя пользователя и пароль по умолчанию отсутствуют.



По умолчанию учетные записи администратора, пользователя устройства, пользователя с правами «только для чтения» и пользователя с доступом «только к сети» отключены. Их нельзя активировать до тех пор, пока пароль по умолчанию для учетной записи суперпользователя (`apc`) не будет изменен.



Информацию по назначению **имени пользователя** и **пароля** для учетной записи администратора, пользователя устройства и пользователя с правами только для чтения см. в разделе «Локальные пользователи».

Сброс настроек ПСУ в случае забытого пароля



ПРИМЕЧАНИЕ. При сбросе настроек ПСУ произойдет возврат к конфигурации по умолчанию.

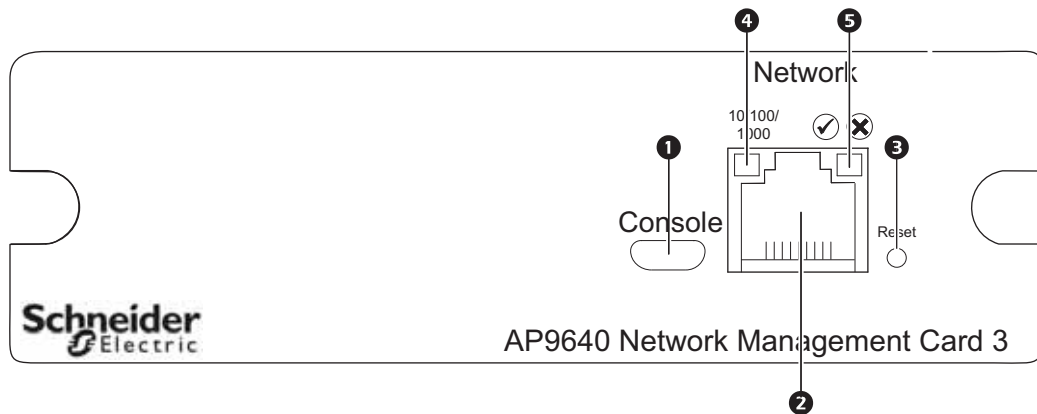
Если вы забыли свой пароль, для удаления настроек вместе с паролем используйте кнопку **Reset (Сброс)** на передней панели ПСУ. Нажмите на кнопку сброса **Reset** и не отпускайте ее в течение 20-25 секунд. Убедитесь, что индикатор состояния мигает зеленым в течение всего указанного времени. Когда индикатор состояния станет желтым или оранжевым, отпустите кнопку сброса. ПСУ завершит процесс перезагрузки.

После перезагрузки ПСУ необходимо повторно настроить ПСУ. Для получения более подробной информации см. [руководство по установке ПСУ](#) на [веб-сайте APC](#) или статью [FA156064](#) в базе знаний на веб-сайте <http://www.apc.com/support>.



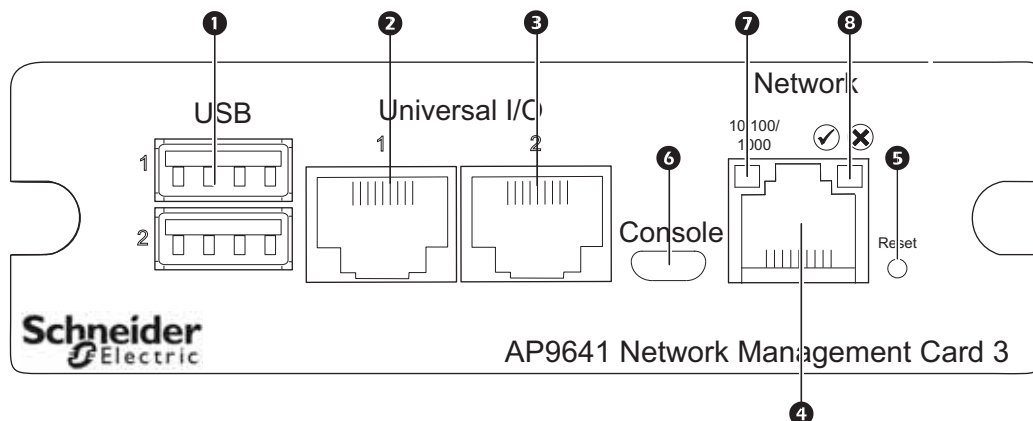
Для предотвращения потери данных в связи с забытым паролем после настройки ПСУ рекомендуется экспортировать INI-файл. См. «Получение и экспорт INI-файла».

Передняя панель (AP9640)



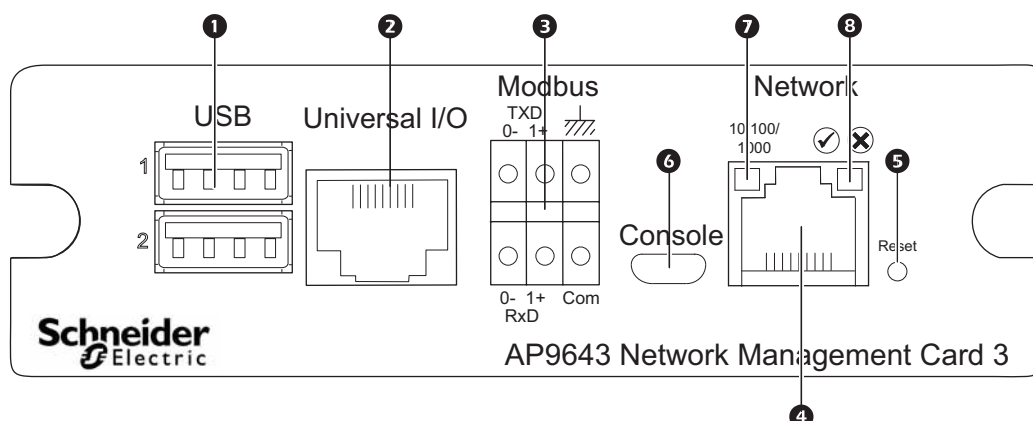
	Компонент	Описание
1	Консольный USB-порт	Подключает ПСУ к локальному компьютеру с помощью кабеля с интерфейсом micro-USB (номер компонента APC 960-0603) для настройки исходных параметров сети или для доступа к интерфейсу командной строки.
2	Разъем Base-T 10/100/1000	Подключает ПСУ к сети Ethernet.
3	Кнопка сброса	Осуществляет сброс интерфейса сетевого управления. Примечание. Это не влияет на выходное питание устройства, в котором установлена ПСУ.
4	Индикатор активности сети Link-RX/TX (10/100/1000)	См. «Индикатор активности сети Link-RX/TX (10/100/1000)».
5	Индикатор состояния	См. раздел «Индикатор состояния».

Передняя панель (AP9641)



	Компонент	Описание
1	Порты USB	Поддержка обновлений прошивки ИБП и дополнительного устройства APC USB Wi-Fi (AP9834). См. разделы «Обновление прошивки ИБП с USB-накопителя (только AP9641 или AP9643)» и «Экран Wi-Fi (только AP9641 и AP9643)».
2 3	Универсальные порты ввода-вывода	Подключают датчики температуры, датчики температуры/влажности и разъемы дополнительного релейного ввода-вывода к универсальному порту ввода-вывода. Дополнительный релейный ввод-вывод имеет два входных контакта и одно выходное реле.
4	Разъем Base-T 10/100/1000	Подключает ПСУ к сети Ethernet.
5	Кнопка сброса	Осуществляет сброс интерфейса сетевого управления. Примечание. Это не влияет на выходное питание устройства, в котором установлена ПСУ.
6	Консольный USB-порт	Подключает ПСУ к локальному компьютеру с помощью кабеля с интерфейсом micro-USB (номер компонента APC 960-0603) для настройки исходных параметров сети или для доступа к интерфейсу командной строки.
7	Индикатор активности сети Link-RX/TX (10/100/1000)	См. «Индикатор активности сети Link-RX/TX (10/100/1000)».
8	Индикатор состояния	Светодиодный индикатор является источником света. См. раздел «Индикатор состояния».

Передняя панель (AP9643)



	Компонент	Описание
1	USB-порты	Поддержка обновлений прошивки ИБП и дополнительного устройства APC USB Wi-Fi (AP9834). См. разделы «Обновление прошивки ИБП с USB-накопителя (только AP9641 или AP9643)» и «Экран Wi-Fi (только AP9641 и AP9643)».
2	Универсальный порт ввода-вывода	Используется для подключения датчиков температуры, датчиков температуры/влажности и разъемов дополнительного релейного ввода-вывода к универсальному порту ввода-вывода. Дополнительный релейный ввод-вывод имеет два входных контакта и одно выходное реле.
3	Разъем Modbus	Используется для подключения ПСУ к системе диспетчеризации инженерного оборудования (Building Management System — BMS). В комплект входят два штыревых разъема для клеммной коробки (номер компонента 730-0532). Чтобы проверить совместимость ИБП с Modbus, см. документацию по ИБП.
4	Разъем Base-T 10/100/1000	Подключает ПСУ к сети Ethernet.
5	Кнопка сброса	Осуществляет сброс интерфейса сетевого управления. ПРИМЕЧАНИЕ. Это не влияет на выходное питание устройства, в котором установлена ПСУ.
6	Консольный USB-порт	Подключает ПСУ к локальному компьютеру с помощью кабеля micro-USB (номер компонента APC 960-0603) для настройки исходных параметров сети или для доступа к интерфейсу командной строки (CLI).
7	Светодиодный индикатор активности сети Link-RX/TX (10/100/1000)	См. «Индикатор активности сети Link-RX/TX (10/100/1000)».
8	Светодиодный индикатор состояния	Светодиодный индикатор является источником света. См. «Индикатор состояния».

Описание индикаторов состояния

Индикатор состояния

Этот светодиодный индикатор указывает состояние ПСУ.

Состояние	Описание
Выключен	Возможна одна из следующих ситуаций: <ul style="list-style-type: none">• На плату сетевого управления не подается входное питание.• Плата сетевого управления работает неправильно. Вероятно, требуется ремонт или замена. Обратитесь в службу технической поддержки. См. раздел «Глобальная служба технической поддержки APC».
Непрерывный зеленый	Параметры TCP/IP в плате сетевого управления заданы правильно.
Непрерывный оранжевый	Возможна одна из следующих ситуаций: <ul style="list-style-type: none">• В плате сетевого управления обнаружена аппаратная неисправность. Обратитесь в службу технической поддержки. См. раздел «Устранение проблем».• ПСУ находится в режиме Bootmonitor. Более подробно см. раздел «Файлы модуля прошивки (Карта сетевого управления 3)».
Мигающий зеленый	В плате сетевого управления неправильно заданы параметры TCP/IP. ¹
Мигающий оранжевый	ПСУ находится в режиме Bootmonitor. Дополнительные сведения см. в разделе «Файлы модулей микропрограммы».
Попеременно мигающий зеленый и оранжевый	Если светодиодный индикатор мигает с низкой частотой, ПСУ выполняет запросы DHCP ² . ¹ Если светодиодный индикатор мигает часто, то выполняется запуск ПСУ.
<p>1. Если сервер BOOTP или DHCP не используется, для настройки параметров TCP/IP ПСУ см. руководство по установке платы сетевого управления в печатном виде и на веб-сайте APC в формате PDF.</p> <p>2. Об использовании сервера DHCP см. раздел «Параметры ответов DHCP».</p> <p>ПРИМЕЧАНИЕ. Если во время загрузки ПСУ подключить кабель micro-USB, ПСУ будет ожидать 90 секунд, чтобы дать время для получения доступа к монитору загрузки. См. раздел «Использование XMODEM для обновления одной ПСУ». На протяжении этой задержки светодиодные индикаторы будут неактивны. Рекомендуется отключить кабель micro-USB, если локальный доступ к интерфейсу командной строки не требуется.</p>	

Индикатор активности сети Link-RX/TX (10/100/1000)

Этот светодиодный индикатор указывает состояние сети ПСУ.

Состояние	Описание
Выключен	Возможна одна из следующих ситуаций: <ul style="list-style-type: none">• На плату сетевого управления не подается входное питание.• Отключен или неисправен кабель, соединяющий ПСУ с сетью.• Отключено или неправильно работает устройство, соединяющее ПСУ с сетью.• ПСУ работает неправильно. Вероятно, требуется ремонт или замена. Обратитесь в службу технической поддержки. См. раздел «Глобальная служба технической поддержки APC».
Непрерывный желтый	ПСУ подключена к сети, которая работает со скоростью передачи 10-100 мегабит в секунду (Мбит/с).
Непрерывный зеленый	ПСУ подключена к сети, которая работает со скоростью передачи 1000 мегабит в секунду (Мбит/с).
Мигающий желтый	ПСУ принимает или передает пакеты данных со скоростью передачи 10-100 Мбит/с.

Состояние	Описание
Мигающий зеленый	ПСУ принимает или передает пакеты данных со скоростью передачи 1000 Мбит/с.

Функции защиты

Обзор

Для обнаружения внутренних неисправностей и восстановления рабочего состояния после воздействия непредусмотренных входных сигналов в ПСУ 3 используется внутренний общесистемный механизм защиты. При перезапуске после внутреннего сбоя в журнал регистрации событий записывается событие **Система: Сетевой интерфейс перезапущен**.

Механизм сетевого интерфейса Watchdog

ПСУ 3 использует средства защиты, чтобы обезопасить себя от ситуации, когда доступ к сети невозможен. Например, если ПСУ 3 не принимает сетевой трафик в течение 9,5 минут (прямой трафик, такой как SNMP, или многоадресный трафик, такой как запрос протокола разрешения адресов [ARP]), то считается, что существует проблема с сетевым интерфейсом, и происходит перезапуск платы.

Сброс таймера сети

Чтобы ПСУ 3 не перезапускалась при отсутствии сетевой активности в течение 9,5 минут, ПСУ 3 пытается обратиться к шлюзу по умолчанию каждые 4,5 минуты. Если этот шлюз доступен, он отвечает ПСУ 3, что приводит к сбросу 9,5-минутного таймера. Если для вашего приложения шлюз не требуется или отсутствует, укажите IP-адрес компьютера, работающего в сети и находящегося в той же подсети. Сетевой трафик от этого компьютера будет сбрасывать 9,5-минутный таймер достаточно часто для предотвращения перезапуска платы NMC 3.

Автоматический выход из системы

По умолчанию пользователи автоматически выходят из веб-интерфейса и интерфейса командной строки ПСУ после 3 минут отсутствия активности. Время выхода из сети по умолчанию для каждого пользователя можно настроить с помощью веб-интерфейса:

Конфигурация > Безопасность > Локальные пользователи > Управление.

- Щелкните гиперссылку имени пользователя учетной записи, которую нужно изменить.
- В меню «Превышено время ожидания сеанса» измените время в минутах.

Автоматический выход из системы	Продолжительность (мин.)
Настройки по умолчанию	3
Минимум	1
Максимум	60 (1 час)

Веб-интерфейс пользователя

Введение

Обзор

Веб-интерфейс пользователя предоставляет параметры для управления ИБП и платой сетевого управления ИБП 3 (ПСУ 3), а также средства просмотра состояния ИБП.



См. раздел «Экран веб-доступа», в котором приводятся сведения о выборе, включении и отключении протоколов, управляющих доступом к интерфейсу пользователя, а также об определении портов сетевого интерфейса веб-сервера для протоколов.

Поддерживаемые веб-браузеры

Веб-интерфейс ПСУ 3 совместим со следующими браузерами:

- Операционные системы Windows®:
 - Microsoft® Internet Explorer® (IE) 8.x или выше с включенным просмотром в режиме совместимости.
 - Последний выпуск Microsoft® Edge®



Примечание. Для просмотра экрана обновления прошивки ИБП в Internet Explorer® используйте версию браузера 10 или выше с выключенным просмотром в режиме совместимости. Экран обновления прошивки ИБП несовместим с браузером Edge®. См. раздел «Экран «Обновление прошивки»» на стр. 33.

- Все операционные системы:
 - Последние выпуски Mozilla® Firefox® или Google® Chrome®

Можно использовать другие общедоступные браузеры, но они не были в полной мере протестированы.

ПСУ не может работать с прокси-сервером. Перед использованием браузера для доступа к пользовательскому интерфейсу ПСУ необходимо выполнить следующие действия:

- Настройте браузер на отключение прокси-сервера для платы сетевого управления ПСУ.
- Настройте прокси-сервер, чтобы он не обрабатывал указанный IP-адрес ПСУ.

Вход в систему

Обзор

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

- `arc` для администратора и привилегированного пользователя.
- `device` для пользователя устройства.
- `readonly` для пользователя с правами только для чтения.

Так же см. раздел «Типы учетных записей».

При входе в систему можно задать язык интерфейса пользователя, выбрав его из раскрывающегося меню **Язык**. См. раздел «Смена языка интерфейса пользователя».



Если протокол HTTPS включен, ПСУ создает собственный сертификат. Этот сертификат согласуется с методами шифрования браузера. Для получения более подробной информации см. [руководство по безопасности](#) на [веб-сайте АРС](#).

Форматы URL-адреса

Наберите имя DNS или IP-адрес ПСУ в поле URL-адреса веб-браузера и нажмите ENTER. При указании порта веб-сервера, отличного от используемого по умолчанию, в поле URL-адреса обозревателя Internet Explorer необходимо добавить к нему `http://` или `https://`.

ПРИМЕЧАНИЕ. Протокол HTTP отключен по умолчанию, а протокол HTTPS включен по умолчанию.

Распространенные сообщения об ошибках в обозревателях при входе в систему.

Сообщение об ошибке	Браузер	Причина ошибки
«This page cannot be displayed.» (Не удастся отобразить данную страницу.)	Internet Explorer	Интернет-доступ невозможен, или URL-адрес указан неправильно.
«Unable to connect.» (Не удастся установить соединение.)	Firefox, Chrome	

Примеры формата URL. См. также «Экран настроек TCP/IP для IPv6».

Пример и режим доступа	Формат URL
DNS-имя Web1	
HTTP	<code>http://Web1</code>
HTTPS	<code>https://Web1</code>
IP-адрес системы 139.225.6.133 и порт веб-сервера по умолчанию (80)	
HTTP	<code>http://139.225.6.133</code>
HTTPS	<code>https://139.225.6.133</code>
IP-адрес системы 139.225.6.133 и порт веб-сервера не по умолчанию (5000)	
HTTP	<code>http://139.225.6.133:5000</code>
HTTPS	<code>https://139.225.6.133:5000</code>
Адрес IPv6 системы 2001:db8:1:2c0:b7ff:fe00:1100 и порт веб-сервера не по умолчанию (5000)	
HTTP	<code>http:// [2001:db8:1:2c0:b7ff:fe00: 1100]:5000</code>

Первое подключение

При первом подключении к ПСУ вам будет предложено изменить пароль (арс), установленный по умолчанию, для учетной записи суперпользователя. После подключения откроется экран с общими сведениями о конфигурации (Configuration Summary Overview). На экране содержится информация о всех системных протоколах и их текущих статусах (напр., включен/выключен). Можно вернуться на этот экран позже, используя следующий путь: **Configuration > Network > Summary**.




Домашний экран

Обзор

Путь: Начало

На экране **Начало** интерфейса можно просматривать активные сигналы тревоги и последние события, записанные в журнале событий.


Один или несколько значков вместе с сопроводительным текстом указывают на текущее рабочее состояние ИБП:

Обозначение	Описание
	Нет сигналов тревоги: сигналы тревоги отсутствуют; ИБП и ПСУ функционируют нормально.
	Предупреждение: аварийный сигнал требует внимания, поскольку не устраненная вовремя проблема может привести к потере данных и порче оборудования.
	Критическое состояние: критический аварийный сигнал, требующий немедленного принятия мер.

В верхнем правом углу каждого экрана такие же значки сообщают о состоянии ИБП. При наличии любого **критического** или **предупредительного** сигнала тревоги также отображается число активных сигналов тревоги.

Для просмотра всего журнала событий щелкните **Дополнительные события**.

Значки и ссылки

Чтобы установить любой экран в качестве домашнего экрана, отображаемого при входе в систему, откройте этот экран и щелкните значок  в верхней правой части.

Щелкните , чтобы восстановить отображение домашнего экрана при входе в систему.

В нижней левой части каждой страницы интерфейса предусмотрены три настраиваемые ссылки на полезные веб-сайты. По умолчанию эти ссылки содержат URL-адреса для следующих веб-страниц:

- Ссылка 1: страница **базы знаний** веб-сайта www.apc.com с полезной информацией по поиску и устранению проблем.
- Ссылка 2: страница **информации о продуктах** веб-сайта www.apc.com с сопроводительной информацией по оборудованию.
- Ссылка 3: страница **загрузки** веб-сайта www.apc.com с доступным программным обеспечением и микропрограммами.



Перенастройка этих ссылок описана в разделе «Экран конфигурирования ссылок».

Мониторинг ИБП: меню «Состояние»

Меню «Состояние» предоставляет сведения о текущем состоянии ИБП и сети.



Можно настроить ИБП и сеть с помощью параметров меню конфигурации. См. разделы «Настройка параметров: 1» и «Настройка параметров: 2».

См. следующие разделы:

- «ИБП в меню состояния»
- «Группы розеток в меню состояния»
- «Система батарей в меню статуса»
- «Универсальный ввод-вывод в меню «Состояние»»
- «Сеть в меню состояния»

ИБП в меню состояния

Путь: Состояние > ИБП

Здесь отображаются сведения о нагрузке ИБП, заряде батареи, напряжении и другая полезная информация.

Поле	Описание
Последний переход на батарею	Причина последнего переключения на работу от батареи (кроме переключения при самотестировании).
Внутренняя температура	Температура внутри ИБП.
Оставшееся время автономной работы	Продолжительность работы ИБП от батареи для поддержания существующей нагрузки.
Вход ИБП	
Входное напряжение	Напряжение переменного тока (В), получаемое ИБП.
Входное напряжение байпаса	Напряжение переменного тока (В), используемое, когда ИБП находится в режиме байпаса. Эта функция доступна не для всех ИБП.
Выход ИБП	
Выходное напряжение	Напряжение переменного тока (В), которое ИБП подает на свою нагрузку.
Ток нагрузки	Ток (А), подаваемый входным напряжением.
Выходная нагрузка	Нагрузка, размещаемая на каждой фазе подключенным оборудованием (кВА).
Выходная нагрузка (%)	Нагрузка, размещаемая на каждой фазе подключенным оборудованием в виде доступного процентного значения (кВА) без избыточности.
Выходная мощность (%)	Нагрузка, размещаемая на каждой фазе подключенным оборудованием в виде доступного процентного значения (кВА).
Вт на выходе	Нагрузка ИБП в виде доступного процентного значения (Вт).
ВА на выходе	Нагрузка ИБП в виде доступного процентного значения (ВА).
Коэффициент полезного действия на выходе	Процентное значение входного питания, подаваемого непосредственно на нагрузку. Входное питание, не подаваемое на нагрузку потребляется ИБП.
Потребление выходной энергии	Энергия, используемая нагрузкой, начиная с момента сброса параметров ИБП на значения по умолчанию.

Поле	Описание
Состояние батарей	
Емкость батареи	Процентное значение емкости батареи ИБП, доступной для поддержки подключенного оборудования.
Напряжение батареи	Напряжение постоянного тока на батареях.
Внешние батареи	Число батарей, подключенных к ИБП, кроме всех внутренних батарей.



Следующие параметры доступны не на всех устройствах ИБП.

Поле	Описание
Номинальное напряжение батареи	Номинальная емкость напряжения батарей ИБП; напряжение постоянного тока, которое батареи должны обеспечивать, когда ИБП использует свою батарею для выходного питания.
Действительное напряжение батарейной шины	Доступное питание постоянного тока.
Ток уставки внешнего батарейного шкафа	Нормированные ампер-часы (емкость батарей) батарейного шкафа для внешнего батарейного источника питания.
Батареи	Общее число батарей (внутренних и внешних), входящих в состав ИБП.
Неисправные батареи	Количество неисправных батарей (батареи, которые должны быть заменены).
Ток батареи	Ток на выходе батареи.
Дата следующей замены батареи	Как и для установленных контейнеров батарей ИБП, для замены батарей существует самая ранняя рекомендуемая дата.
Интеллектуальный модуль	Информация об интеллектуальном модуле. Эту информацию (версия микропрограммы, дата производства, серийный номер и версия оборудования) могут запросить при обращении в центр технической поддержки APC.
Входное напряжение	Напряжение переменного тока (В), получаемое ИБП.
Входное напряжение байпаса	Напряжение переменного тока (В), используемое, когда ИБП находится в режиме байпаса.
Входная частота	Частота (Гц) напряжения, получаемого ИБП.
Частота	Общая частота (Гц) для напряжения на входе и на выходе.
Частота байпаса	Частота (Гц) напряжения, используемого при нахождении ИБП в режиме байпаса.
Выходной ток	Ток (А), подаваемый на нагрузку.
Выходная частота	Частота (Гц) выходного напряжения.
Мощность нагрузки	Нагрузка ИБП в виде доступного процентного значения (Вт).
Полная мощность нагрузки	Нагрузка ИБП в виде доступного процентного значения (ВА).
Модули	Информация о модулях, установленных в ИБП. Эту информацию (версия микропрограммы, дата производства, серийный номер и версия оборудования) могут запросить при обращении в центр технической поддержки APC.
Силовой модуль	Информация о силовых модулях, установленных в ИБП. Эта информация может потребоваться при обращении в центр технической поддержки APC.

Группы розеток в меню состояния

Путь: Состояние > Группы розеток

Эта функция доступна не для всех ИБП. С ее помощью можно просмотреть сведения о состоянии всех групп розеток ИБП. См. также «Группы розеток» в меню управления» и «Группы розеток» в меню конфигурации».

Система батарей в меню статуса

Путь: Статус > Система батарей



Эта функция доступна не для всех ИБП.

Поле	Описание
Статус системы батарей	
Состояние зарядки	Процентное значение емкости батареи ИБП, доступное для поддержания подключенного оборудования.
Оставшееся время автономной работы	Продолжительность работы ИБП от батареи для поддержания существующей нагрузки.
Напряжение положительной шины	Устройство ИБП поддерживает положительное и отрицательное напряжение батарей.
Напряжение отрицательной шины:	
Учетный номер запасного контейнера батареи	Номер по каталогу, который нужно использовать при замене контейнера батареи.
Статус комплекта батарей	
Комплект батарей 1, 2...	Номер комплекта батарей, получаемый методом внутренней нумерации.
Серийный номер	Серийный номер комплекта батарей.
Состояние	Содержит любые системные ошибки комплектов батарей, включая индивидуальные ошибки контейнера. Ошибки протоколируются как события.
Статус	Состояние комплекта батарей, включая состояния индивидуальных контейнеров. Данное значение сообщает, что батарея исправна, приближается окончание срока службы батареи или срок службы батареи превышает соответствующее значение комплекта. Ошибки протоколируются как события.

Щелкните «Комплект батарей 1, 2...», чтобы открыть страницу **Комплект батарей n**.

Поле	Описание
Комплект батарей 1, 2... или внутренний комплект	
Серийный номер (если присутствует)	Серийный номер комплекта батарей.
Версия прошивки	Номер версии комплекта батарей.
Температура	Температура в отсеке батарей, которую передает датчик.

Поле	Описание
Статус комплекта	Ошибки, относящиеся только к комплекту батарей, не включая индивидуальные ошибки контейнера. Ошибки протоколируются как события и могут сообщать следующую информацию: <ul style="list-style-type: none"> • температура вне диапазона • общие ошибки • ошибки связи • отключенная стойка комплекта • микропрограмма несовместима с оборудованием
Контейнер батарей 1 и (если присутствует) Контейнер батарей 2	
Состояние	Данное значение указывает, что батарея исправна, приближается окончание срока службы батареи или измеренные значения батареи указывают о приближении окончания срока службы контейнера. Ошибки протоколируются как события.
Дата установки	Дата установки отдельных контейнеров. Эту дату можно изменить.
Прогнозируемая дата замены	ИБП вычисляет время замены батареи. Поле Состояние вычисляется на основании этой даты.
Статус	Это специальные данные для контейнера. Общие ошибки комплекта см. в вышеприведенном поле «Статус комплекта». Ошибки протоколируются как события и могут сообщать следующую информацию: <ul style="list-style-type: none"> • отключенный контейнер • требуется заменить контейнер • слишком высокая температура контейнера: критическая • слишком высокая температура контейнера: предупреждение. Отображается обычно, но не всегда перед критическим сообщением.

Универсальный ввод-вывод в меню «Состояние»

Путь: Состояние > Универсальный ввод-вывод



Эта функция доступна не для всех ИБП.

Температура и влажность — здесь отображается имя, состояние тревоги, температура и влажность (если поддерживается) для каждого датчика. Щелкните имя датчика, чтобы изменить имя и местоположение или настроить пороговые значения и гистерезис. Дополнительную информацию см. в разделе «Экран «Температура и влажность»».

Входные контакты — здесь отображается имя, состояние тревоги и состояние каждого контакта (открыт или закрыт). Эти данные автоматически получаются и отображаются здесь при установке устройства для мониторинга окружающей среды. Щелкните имя входного контакта для получения подробного описания состояния или для настройки значений. Если настройка контактов выполнена, но они неактивны, эти данные здесь не отображаются. Дополнительную информацию см. в разделе «Экран «Входные контакты»».

Выходное реле — здесь отображается имя и состояние каждого реле (открыто или закрыто). Эти данные автоматически получаются и отображаются здесь при установке устройства для мониторинга окружающей среды. Щелкните имя входного контакта для получения подробного описания состояния или для настройки значений. Дополнительную информацию см. в разделе «Экран «Выходное реле»».

Последние события в окружающей среде — здесь отображаются события, относящиеся к мониторингу окружающей среды, например нарушение порога температуры или сообщение с предупреждением относительно входного контакта монитора окружающей среды. Щелкните ссылку «Дополнительные события», чтобы увидеть полный список недавних событий.

Сеть в меню состояния

Путь: Состояние > Сеть

На экране сети содержатся настройки IP, имени домена и порта Ethernet. Сведения по полям см. в разделе «Сеть» в меню конфигурации».

Управление ИБП

Функции меню управления позволяют предпринимать немедленные действия, влияющие на ИБП и розетки. Среди них есть также некоторые функции безопасности и сетевые функции.

См. следующие разделы:

- «ИБП в меню управления»
- «Группы розеток» в меню управления»
- «Безопасность» в меню управления»
- «Сеть» в меню управления»

ИБП в меню управления

Путь: Управление > ИБП

Если выбрать переключатель и щелкнуть «Далее», на следующем экране появится краткий обзор выполненных действий. Щелкните «Применить» для продолжения действия.

Доступные действия зависят от того, имеется ли ИБП с группой розеток. В двух таблицах далее отдельно рассматриваются эти случаи.

- «Действия на экране ИБП для устройств С группами розеток».
- «Действия на экране ИБП для устройств БЕЗ групп розеток».

Следующие функции флажков применимы к обеим таблицам.

Флажок	Описание
Клиенты сетевого выключения по сигналу PowerChute	Для ИБП с группами розеток этот параметр недоступен, если отсутствуют клиенты PowerChute (см. «Клиенты сетевого выключения PowerChute»). Выберите этот флажок для уведомления всех серверов, настроенных как Клиенты сетевого выключения PowerChute , которые обмениваются информацией с этим ИБП, чтобы выполнять выключение в соответствии со значениями, настроенными в меню Параметры сетевого выключения PowerChute (см. «Выключение» в меню конфигурации). Однако эта функция не будет уведомлять серверы при выполнении действий по управлению в режиме байпаса.
Пропускать задержки при отключении розеток	Данный параметр доступен только для ИБП с группами розеток. Немедленное выключение розеток без применения настроенных задержек для групп розеток. Это может потребоваться в аварийной ситуации или для экономии времени автономной работы. Или в случае, когда устройства нагрузки уже выключены вручную.



Более подробные сведения о задержках и параметрах приведены в разделах ««Выключение» в меню конфигурации», «Экран «Универсальный ввод-вывод»» и ««Группы розеток» в меню управления».

Действия на экране ИБП для устройств С группами розеток

Действие	Описание
Перезапустить группы розеток ИБП	<p>Применение команд немедленного выключения, перезапуска питания переменного тока ко всем группам розеток (см. ««Группы розеток» в меню управления»). Щелкните «Далее» для просмотра дополнительных сведений о синхронизации и задержках.</p> <p>Выключение выходного напряжения группы переключаемых розеток, а затем основной группы розеток (если присутствует). Для любой группы розеток, к которой применяется это действие, используется задержка, продолжительность которой настроена в параметрах «Продолжительность перезагрузки» и «Задержка при включении питания». (Затем группы розеток включаются, если доступно питание переменного тока от сети, или ожидают, когда будет доступно питание переменного тока от сети, чтобы выполнить включение. См. раздел «Описание групп розеток».)</p> <p>ИБП включается, если доступно питание переменного тока от сети, или ожидает, когда будет доступно питание переменного тока от сети, чтобы выполнить включение.</p>
Включить группы розеток ИБП	<p>Включение основной группы розеток (если присутствует), а затем всех групп переключаемых розеток. Эта функция отображается только в том случае, если ИБП в данный момент включен. Щелкните «Далее» для просмотра дополнительных сведений о синхронизации и задержках.</p> <p>Затем включаются ИБП и группы розеток.</p>
Выключить группы розеток ИБП	<p>Выключение выходного напряжения группы переключаемых розеток, а затем основной группы розеток (если присутствует). Любая группа розеток, к которой применяется это действие, остается выключенной, пока их питание не будет снова включено. Щелкните «Далее» для просмотра дополнительных сведений о синхронизации и задержках.</p>
Перевести группы розеток ИБП в спящий режим	<p>Перевод групп розеток ИБП в спящий режим за счет отключения выходного напряжения ИБП на период времени, определенный следующими параметрами. Щелкните «Далее» для просмотра дополнительных сведений о синхронизации и задержках.</p> <ul style="list-style-type: none">• Для групп розеток используется задержка, настроенная в параметре «Задержка при отключении питания», перед выключением их питания.• После восстановления входного питания ИБП включает выходное питание по истечении двух заданных периодов времени: «Время в спящем режиме» и «Задержка при включении питания». <p>Затем ИБП выключается. По истечении времени, указанного для параметра «Время режима сна» ИБП включается, если доступно питание переменного тока от сети, или ожидает, когда будет доступно питание переменного тока от сети, чтобы выполнить включение.</p>
Перевести ИБП в режим байпаса Возврат ИБП из режима байпаса	<p>Эти параметры управляют использованием режима байпаса, что позволяет выполнять обслуживание ИБП, не отключая питание.</p> <p>Эти опции доступны только для ИБП Symmetra и некоторых устройств Smart-UPS.</p>



Дополнительную информацию о задержках и настройках см. в разделах ««Выключение» в меню конфигурации» и ««Группы розеток» в меню управления».

Действия на экране ИБП для устройств БЕЗ групп розеток

Действие	Описание
Перезагрузить ИБП	Происходит перезапуск подключенного оборудования после выполнения следующих операций. (Щелкните «Далее» для просмотра дополнительных сведений о синхронизации и задержках.) <ul style="list-style-type: none"> • Выключение питания ИБП. • Питание на ИБП включается после того, как емкость батареи возвращается к минимальному значению в процентах, заданному для параметра «Минимальная емкость батареи» («Конфигурация» - «Выключение» - «Завершение выключения», см. раздел «Контролируемое раннее выключение» и «Завершение выключения»).
Включить ИБП	Включение питания ИБП. Эта функция отображается, если ИБП выключен. Щелкните «Далее» для просмотра дополнительных сведений о синхронизации и задержках.
Выключить ИБП	Немедленное выключение выходного напряжения ИБП без задержки выключения. ИБП остается выключенным, пока не будет выполнено повторное включение.
Перевести ИБП в спящий режим	ИБП переводится в спящий режим за счет отключения его выходного напряжения на определенный период времени. Щелкните «Далее» для просмотра дополнительных сведений о синхронизации и задержках. <ul style="list-style-type: none"> • ИБП отключает выходное напряжение по истечении времени, заданного в параметре «Задержка выключения». • Когда входное напряжение возвращается, ИБП включает выходное напряжение по истечении времени параметра «Время режима сна».
Перевести ИБП в режим байпаса и Вывести ИБП из режима байпаса	Эти опции управляют использованием режима байпаса, позволяющего осуществлять обслуживание некоторых устройств Smart-UPS, не отключая питание ИБП. Щелкните «Далее» для просмотра дополнительных сведений о синхронизации и задержках. Эти опции доступны только для ИБП Symmetra и некоторых устройств Smart-UPS.

«Группы розеток» в меню управления

Путь: Управление > Группы розеток



Эта функция доступна не для всех ИБП.

Используйте эту функцию для включения, выключения и перезапуска отдельных групп розеток явным образом на ИБП. (На этой странице перечисляются имена и состояния каждой группы розеток ИБП, которая была настроена в функции **Конфигурация - Группы розеток**; см. раздел «Группы розеток» в меню конфигурации»).

Для каждой группы розеток можно выбрать любые приведенные ниже действия (или отменить выбор всех действий). Далее представлены одноразовые действия.

- Если группа розеток находится в состоянии **Выкл.**:
 - **Вкл. немедленно**
 - **Вкл. с задержкой**: включение группы розеток происходит спустя определенное время в секундах, задаваемое в параметре **Задержка при включении питания**. (См. раздел «Выключение» в меню конфигурации»).

- Если группа находится в состоянии **Вкл.**:
 - **Выкл. немедленно**
 - **Выкл. с задержкой**: отключение группы происходит спустя определенное время в секундах, задаваемое в параметре **Задержка при отключении питания** (см. ««Выключение» в меню конфигурации»).
 - **Перезагрузить немедленно**: происходит мгновенное отключение группы, затем она включается спустя определенное время в секундах, задаваемое в параметре **Продолжительность перезагрузки** (см. ««Выключение» в меню конфигурации») и **Задержка при включении питания**.
 - **Перезагрузка 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**.
 - **Выключить немедленно, перезапуск при подаче переменного тока**: происходит мгновенное выключение группы. Через определенное время, заданное в секундах в параметрах **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 при подаче переменного тока**: отключение группы происходит спустя определенное время в секундах, задаваемое в параметре **Задержка при отключении питания**. Через определенное время, заданное в секундах в параметрах **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.

«Безопасность» в меню управления

Путь: Управление > Безопасность > Управление сеансом

На экранах представлены подробные сведения о пользователях, выполнивших вход, используемый ими интерфейс (веб-интерфейс пользователя или интерфейс командной строки), их IP-адрес и длительность присутствия в системе.

При наличии необходимых прав щелкните имя для просмотра средств аутентификации, используемых для проверки личности пользователя. Можно также использовать кнопку **Завершить сеанс** для вывода пользователя из системы.

«Сеть» в меню управления

Путь: Управление > Сеть > Сбросить/перезагрузить

Используйте эти функции для сброса различных функций платы сетевого управления и интерфейса пользователя.

Действие	Описание
Перезагрузка интерфейса управления	Перезагрузка интерфейса управления (например, веб-интерфейса пользователя, интерфейса командной строки) путем выхода из системы. ИБП и плата сетевого управления не перезагружаются.
Сбросить все ¹	Осторожно: при выполнении этой операции все настроенные значения будут сброшены к установленным по умолчанию. <ul style="list-style-type: none">• Если не выбран параметр исключить ТСП/IP, все настроенные значения и параметры сбрасываются к установленным по умолчанию, включая параметр, определяющий, как данное устройство должно получать значения конфигурации ТСП/IP и конфигурации EAPoL. По умолчанию для параметров конфигурации ТСП/IP используется DHCP, значение доступа к EAPoL, «отключено».• Если вы выберете параметр исключить ТСП/IP, все существующие значения и настройки, за исключением параметра, который определяет, как это устройство должно получить свой ТСП/IP, и значения конфигурации EAPoL сбрасываются к установленным по умолчанию.
Только перезапустить ¹	ТСП/IP: сброс параметра, который определяет, как устройство должно получать свои значения конфигурации ТСП/IP, включая конфигурацию EAPoL, которая возвращается к значению «отключено». По умолчанию для параметра конфигурации ТСП/IP используется DHCP, значение доступа к EAPoL — «отключено».
	Конфигурация события: сбрасывает события к настройкам по умолчанию. Любое конкретно настроенное событие или группа событий также вернется к значению по умолчанию. Смотрите «Меню уведомлений».
	Значения ИБП по умолчанию: установка значений по умолчанию только для параметров ИБП, сетевые настройки не меняются.
	Политика управления: сброс настроек, которые определяют, как ПСУ будет реагировать на сигналы тревоги, посылаемые устройством ввода-вывода с сухими контактами.
¹ Сброс настроек может занять около минуты. Настроенное имя ИБП не будет сброшено (см. «Экран «ИБП: общее»»).	

Настройка параметров: 1

С помощью элементов меню конфигурации можно установить значения основных рабочих параметров ИБП и ПСУ.

См. следующие разделы и раздел «Настройка параметров: 2».

- ««Группы розеток» в меню конфигурации»
- «Настройки питания в меню конфигурации»
- ««Выключение» в меню конфигурации»
- «Экран «ИБП: общее»»
- «Экран «Расписание самодиагностики»»
- «Планирование выключения»
- «Экран «Обновление прошивки»»
- «Клиенты сетевого выключения PowerChute»
- «Экран «Универсальный ввод-вывод»»
- «Меню «Безопасность»»



ПРИМЕЧАНИЕ. Некоторые параметры конфигурации можно увидеть на экране с обзором конфигурации Configuration Summary (Configuration > Network > Summary).

«Группы розеток» в меню конфигурации

Путь: Конфигурация > Группы розеток

Эта функция доступна не для всех ИБП. С ее помощью можно отображать и настраивать задержки розеток и последовательностей.

См. также «Группы розеток в меню состояния», ««Группы розеток» в меню управления» и ««Выключение» в меню конфигурации».

Описание групп розеток



Группирование розеток возможно только для некоторых устройств ИБП. Чтобы определить, поддерживает ли устройство ИБП группы розеток, обратитесь к документации по ИБП. Доступные настройки зависят от модели ИБП.

Основные группы розеток. В некоторых устройствах ИБП подача питания переменного тока предусмотрена для одной основной группы розеток. Основная группа розеток управляет распределением питания по всем группам переключаемых розеток ИБП (если они имеются).

- Если основная группа розеток отключена, то группы переключаемых розеток не могут быть включены.
- Если отключить основную группу розеток, ИБП сначала отключает группы переключаемых розеток, а затем основную группу.
- Для включения группы переключаемых розеток ИБП должен сначала включить основную группу розеток.

Группы переключаемых розеток.

- Каждая переключаемая розетка может выполнять действия независимо. Можно запускать или останавливать эти розетки по порядку, а также перезапускать устройства, подключенные к этим розеткам.

Настройка групп розеток

Имя и тип группы розеток. Просмотрите имя, тип и задержки для розеток ИБП на экране **Конфигурация** — **Группы розеток**. Щелкните имя группы розеток в разделе **Группа** для изменения ее настроек, в том числе задержек последовательностей и параметров распределения нагрузки.

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

Поле	Описание
Задержка при отключении питания	Когда эта группа розеток включена, она выжидает эту задержку (в секундах) перед выключением. Установив здесь разное время для розеток, можно задать последовательность их выключения, т. е. указать порядок, в каком они будут выключаться.
Продолжительность перезагрузки	Розетка выжидает это время до перезапуска.
Задержка при включении питания	Когда эта группа розеток выключена и принимает сигнал на включение, выжидает это время (в секундах) перед включением. Установив здесь разное время для розеток, можно задать последовательность их включения.
Минимальное время автономной работы на выходе	Перед повторным включением ИБП должен обеспечить определенное минимальное время для поддержки нагрузки.

Параметры сброса нагрузки. Сброс нагрузки позволяет указать условия, вызывающие потерю питания на отдельных группах переключаемых розеток.



Примечание. Если используется параметр сетевого выключения PowerChute для управления ИБП, не рекомендуется использовать параметры выключения электричества ПСУ, так как они могут конфликтовать с настройками группы розеток, указанными в PowerChute.

Примером использования сброса нагрузки является отключение некритичных нагрузок типа мониторов, когда ИБП работает от батареи или перегружен. Это позволяет сэкономить заряд батареи и продлить время работы важнейших нагрузок. Другим примером является выключение автоматического перезапуска после перегрузки с целью исследования причины перегрузки перед повторным включением группы розеток.

Параметры позволяют выключать группу розеток при соблюдении ЛЮБЫХ из указанных условий:

- при превышении времени работы от батареи в минутах;
- при достижении минимального остаточного времени работы ИБП в минутах; (время работы — это продолжительность работы ИБП от батареи для поддержания текущей нагрузки);
- ИБП перегружен (требования к питанию устройств, подключенных к ИБП, превышают мощность, которую может обеспечить ИБП).

Можно также включить следующие действия:

- **Пропускать задержку при выключении розеток.** (Отключение группы происходит немедленно без ожидания времени, задаваемого в секундах в параметре **Задержка при отключении питания**. По умолчанию этот параметр отключен.)
- **Оставаться в выключенном состоянии после возобновления подачи 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.)

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: Outlet Group 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.

Настройки питания в меню конфигурации

Путь: Конфигурация > Настройки питания



Доступные настройки зависят от модели ИБП.

Номинальное выходное напряжение — это напряжение переменного тока, которое ИБП подаёт на нагрузку при работе от батарей. Можно настраивать следующие элементы, зависящие от устройства:

- Верхнее и нижнее значения параметра **Напряжение** определяют диапазоны, в которых ИБП автоматически регулирует выходное напряжение, подаваемое на нагрузку. Это защищает нагрузку.

При превышении верхнего значения напряжения ИБП использует функцию «Понижение напряжения АРН»; при напряжении ниже нижнего значения ИБП использует функцию «Повышение напряжения АРН» (или переключается на работу от батареи, если ИБП не имеет функции «Повышение напряжения АРН»).

- При включенной функции **Режим сбережения энергии** ИБП работает в режиме байпаса и использует энергию более эффективно. Однако в режиме сбережения энергии уменьшается скорость перехода на питание от батареи ИБП при необходимости. Если в используемой среде необходимо быстрое переключение, можно выключить режим сбережения энергии.
- ИБП реагирует на помехи в линии подачи питания, переключаясь на питание от батареи. Параметр **Чувствительность** позволяет изменить время реакции ИБП на помехи в линии. Используйте значения **Пониженная** и **Низкое**, чтобы позволить ИБП принимать подводимое питание с помехами в течение более длительного периода, прежде чем переключаться на питание от батареи. Используйте значение **Низкое**, когда о подводимом питании известно, что оно сопровождается большим количеством помех в линии, например, когда питание подается от генератора.
- **Мощность розетки в Вт**: максимальная номинальная мощность в соответствии с требованиями устройств нагрузки.
- Настройки **Байпас** определяют условия, при которых ИБП может переключаться в режим байпаса.

«Выключение» в меню конфигурации

Путь: Конфигурация > Выключение

Используйте этот экран для настройки параметров выключения ИБП, см. следующую таблицу и раздел ««Контролируемое раннее выключение» и «Завершение выключения»».

Начало выключения

Определение задержек и продолжительностей, используемых при необходимости выключения ИБП.

Поле	Описание
Продолжительность работы при низком заряде батареи	Для ИБП, работающего от батареи, этот параметр определяет пороговое значение оставшегося времени работы, по истечении которого на ИБП включается состояние низкого уровня заряда батареи. Например, если для параметра «Продолжительность работы при низком заряде батареи» установлено значение в 10 минут и прогнозируемое оставшееся время работы ИБП достигает 10 минут или менее, включается состояние низкого уровня заряда батареи. Если не восстановить питание ИБП от сети, он выключится, когда батарея разрядится. В состоянии низкого уровня заряда батареи все клиенты сетевого отключения PowerChute, связанные с ПСУ, будут выключены.
Макс. требуемая задержка	Рассчитывается задержка, необходимая для того, чтобы у каждого клиента PowerChute было время для мягкого выключения, если ИБП или клиент PowerChute запускает мягкое выключение. <ul style="list-style-type: none">• Это максимальная задержка выключения, необходимая любому из серверов в списке клиентов сетевого выключения PowerChute.• Она рассчитывается при включении или сбросе интерфейса управления ИБП или при выборе параметра <i>Вынужденное согласование</i> и кнопки «Применить». См. раздел «Задержка выключения и сетевое выключение PowerChute».

Базовая сигнализация выключения.

Базовая сигнализация или «простая сигнализация» — это простой способ взаимодействия ИБП с сервером, рабочей станцией или системой стороннего производителя. Плата расширения интерфейса 2 (AP9624) — это дополнительная принадлежность с поддержкой Smart Slot, которая может обеспечить простую сигнализацию для ИБП. Простая сигнализация ИБП может осуществлять уведомление и мягкое выключение системы, но не предоставляет функций непрерывного расширенного мониторинга, доступных при расширенной или интеллектуальной сигнализации.



Примечание. При использовании сетевого отключения PowerChute не рекомендуется использовать базовую сигнализацию выключения. Для некоторых моделей ИБП такие функции, как базовая сигнализация выключения, могут повлиять на выключение ИБП и переопределить продолжительность работы при низком заряде батареи, которая используется программой PowerChute для расчета общего требуемого времени выключения.

Поле	Описание
Базовая сигнализация выключения	Включите параметр «Базовая сигнализация выключения», если к ИБП подключен сервер, рабочая станция или система стороннего производителя с помощью кабеля базовой сигнализации. Включите эту функцию, если используемый ИБП не поддерживает расширенную сигнализацию или настроен на передачу сигналов с помощью базовой сигнализации.

Базовая продолжительность работы при низком заряде батареи	<p>Для ИБП, работающего от батареи, этот параметр определяет пороговое значение оставшегося времени работы, по истечении которого на ИБП включается состояние низкого уровня заряда батареи. При этом ИБП выполнит следующие действия:</p> <ul style="list-style-type: none"> • Отобразит уведомление о низком уровне заряда батареи на дисплее ИБП. • Отправит уведомление о низком уровне заряда батареи с ИБП на подключенные устройства по кабелю простой сигнализации. <p>Если не восстановить питание ИБП от сети, он выключится, когда батарея разрядится. Эта продолжительность доступна только для моделей Smart-UPS SMT, SMX, SRC, SURTD и SRT.</p>
Базовая задержка выключения	<p>Определяет продолжительность ожидания ИБП после уведомления о базовом выключении, прежде чем он выключится. По истечении этого периода ИБП выключится независимо от оставшегося времени работы батареи.</p> <p>Эта задержка доступна только для определенных моделей Smart-UPS SMT, SMX, SRC, SURTD и SRT.</p>

Продолжительность выключения

Определение периода, на который выключается ИБП.

Поле	Описание
Время в спящем режиме	<p>Определение интервала времени, в течение которого ИБП сохраняет выходное питание выключенным при использовании команды спящего режима для ИБП или группы розеток. Когда ИБП или группа розеток выключаются, они снова включаются после заданного здесь времени в спящем режиме с добавлением времени возврата или задержки при включении питания для групп розеток. Если питание от сети не было возобновлено к этому моменту, ИБП подождет его возобновления до включения. См. раздел «Группы розеток» в меню конфигурации» на стр. 24.</p> <p>Команду спящего режима можно подать с помощью дисплея ИБП, «ИБП в меню управления», команды SNMP или программы PowerChute Business Edition.</p>

Параметры выключения PowerChute

Определение параметров выключения, используемых при сетевом выключении PowerChute.

Поле	Описание
Макс. требуемая задержка - Вынужденное согласование	<p>При включении параметра <i>Вынужденное согласование</i> выполняется сброс значения «Макс. требуемая задержка» на значение параметра «Продолжительность работы при низком заряде батареи». ПСУ отправляет пакет обновленного состояния на все зарегистрированные агенты PowerChute. Затем программа PowerChute сравнивает продолжительность работы при низком заряде батареи, отправленную в этом пакете, с общим требуемым временем выключения и увеличивает соответствующим образом значение «Макс. требуемая задержка» или «Задержка при отключении питания» для группы розеток, в которой она зарегистрирована.</p> <p>Программа PowerChute выполняет проверку оставшегося времени работы от батареи каждые 30 секунд, сравнивая при этом общее требуемое время выключения с продолжительностью работы при низком заряде батареи, установленной на ПСУ.</p> <p>При выборе вынужденного согласования задержка при отключении питания для всех групп розеток сбрасывается на такое же значение, что и продолжительность работы при низком заряде батареи.</p> <p>Для расчета значения, необходимого всем клиентам PowerChute, которые зарегистрированы на ПСУ, функции вынужденного согласования может потребоваться до десяти минут. Дополнительные сведения см. в разделе «Задержка выключения и сетевое выключение PowerChute» на стр. 30.</p>
Поведение в режиме «От батареи»	<p>Определение поведения ИБП после выключения питания:</p> <ul style="list-style-type: none"> • Перезапуск после возобновления питания — после возобновления питания от сети ИБП перезапускается. • Выключение без перезапуска — ИБП остается выключенным даже после возобновления питания от сети.
Имя пользователя	Введите имя пользователя учетной записи, настроенной для PowerChute.
Фраза аутентификации	Эта фраза используется для аутентификации между PowerChute и ПСУ. По умолчанию эта фраза пуста. Ее необходимо ввести до активации PowerChute.

«Контролируемое раннее выключение» и «Завершение выключения».



Эти функции доступны не для всех ИБП. Эти функции **недоступны** для моделей Smart-UPS SMT, SMX, SRC, SURTD и SRT. Информацию об управлении ранним выключением групп розеток для этих моделей см. в разделе «Параметры сброса нагрузки» на стр. 25.

Функции «Контролируемое раннее выключение» позволяют выключить устройство ИБП, работающее от батареи, при соблюдении ЛЮБОГО из указанных условий:

- при превышении времени работы от батареи в минутах;
- при достижении минимального остаточного времени работы ИБП в минутах; (время работы — это продолжительность работы ИБП от батареи для поддержания текущей нагрузки);
- при заряде батареи ниже установленного процента от ее общей емкости;
- при снижении нагрузки на ИБП до заданного значения в процентах.

С помощью параметра **Остаться в выключенном состоянии после возобновления подачи питания** можно также указать, должен ли ИБП снова включиться после восстановления питания переменного тока в сети.

Функции **Завершение выключения** позволяют установить условие и время задержки для случаев, когда ИБП может снова включиться после восстановления питания переменного тока в сети. В зависимости от модели ИБП можно указать значение **Минимальная емкость батареи** или **Минимальное время автономной работы на выходе** до повторного включения ИБП.

Задержка выключения и сетевое выключение PowerChute.

В следующем разделе описано, как параметры «Продолжительность работы при низком заряде батареи», «Макс. требуемая задержка» и задержки выключения для групп розеток влияют на последовательность выключения PowerChute.

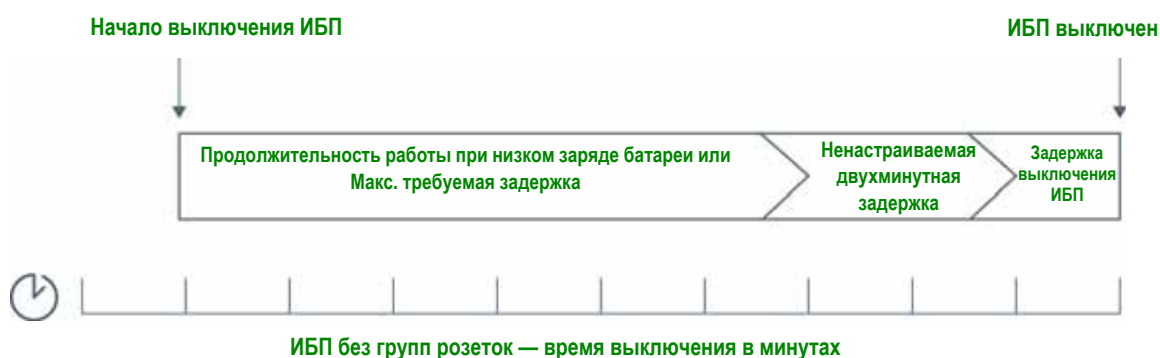


Дополнительную информацию о последовательностях выключения PowerChute см. в *Руководстве по сетевому выключению PowerChute*.

Для обоих типов ИБП, с группами розеток и без них, время выключения определяется путем взаимодействия ПСУ с программой сетевого выключения PowerChute следующим образом.

ИБП без групп розеток

Для ИБП БЕЗ групп розеток время выключения — это большее из значений **Макс. требуемая задержка** и **Продолжительность работы при низком заряде батареи** на экране **Выключение** платы сетевого управления плюс ненастраиваемая 2-минутная задержка плюс время задержки для ИБП.

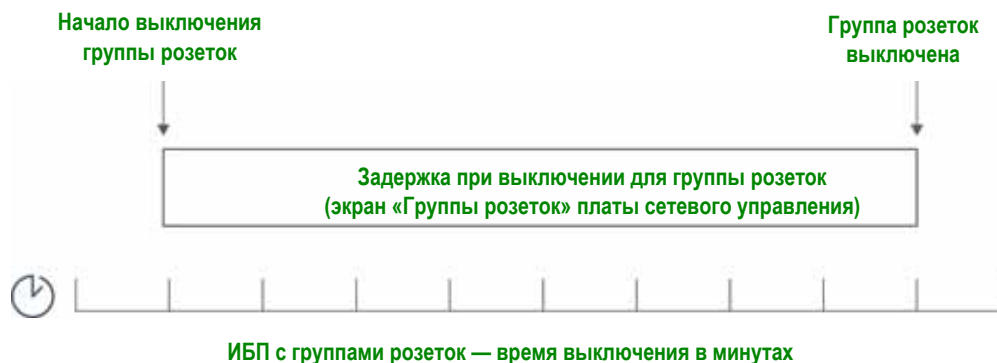


Примечания:

- Если выключение было инициировано состоянием низкого уровня заряда батареи, продолжительность работы при низком заряде батареи имеет более высокий приоритет, чем максимальная требуемая задержка.
- Исключением являются модели ИБП с префиксом SUM, на которых группы розеток используют метод для ИБП без групп розеток для расчета времени выключения ИБП.

ИБП с группами розеток

Для ИБП С группами розеток время выключения — это значение **Задержка при выключении для группы розеток** на экране **Группы розеток** платы сетевого управления, см. «Группы розеток» в меню конфигурации». (Доступно не на всех устройствах ИБП.)





Примечания:

Дополнительную информацию о последовательностях выключения PowerChute см. в разделе «*Sample Shutdown Scenarios*» (Образцы сценариев выключения) [Руководства по сетевому выключению PowerChute на веб-сайте APC](#).

При сравнении требуемого времени выключения PowerChute и максимальной требуемой задержки либо задержки при выключении для группы розеток на ПСУ используется большее значение. Например, если для продолжительности выключения в командной строке клиента PowerChute установлено значение 8 минут, но продолжительность работы ИБП при низком заряде батареи составляет 10 минут, ПСУ будет использовать большее из значений (10 минут) для максимальной требуемой задержки.

При вынужденном согласовании ПСУ опрашивает клиентов PowerChute на предмет установленного на них требуемого времени выключения. В результате для обновления значений максимальной требуемой задержки или задержки при выключении для группы розеток может потребоваться до десяти минут.

PowerChute не изменяет значение **Продолжительность работы при низком заряде батареи** на плате сетевого управления.

Значение **Макс. требуемая задержка** PowerChute Network Shutdown версии 3.x и выше не используется платой сетевого управления по отношению к ИБП с группами розеток.

Экран «ИБП: общее»

Путь: Конфигурация > ИБП



Этот экран доступен не для всех ИБП.

Некоторые из функций, описанных далее, могут НЕ отображаться для некоторых ИБП.

Поле	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 устройств ИБП можно задать условие, при котором работает звуковая сигнализация.
Языковые настройки жидкокристаллического дисплея	Определение языка, используемого на дисплее ИБП.
ЖК-дисплей	Выключение или включение доступа к записи в интерфейсе дисплея ИБП. Если доступ выключен, пользователь по-прежнему имеет доступ на чтение большинства экранов, но не вложенных экранов меню «Управление» и «Конфигурация».
Время предупреждения сигнала тревоги о состоянии батареи	Установка времени (в днях) до появления критического сигнала тревоги о замене батареи на ЖК-дисплее ИБП. Установите значение -1, чтобы не отображать предупреждающее уведомление.
Время сна, сигнал тревоги о состоянии батареи	Установка времени (в днях), в течении которого сигнал тревоги батареи ЖК-экрана ИБП не отображался после первого подтверждения. Установите значение -1, чтобы не отображать дополнительных предупреждений после подтверждения первого предупреждения.
Последняя замена батареи	Ввод месяца и года последней замены батареи ИБП.

Поле	Описание
Число батарей или Внешние батареи	Количество батарей, исключая встроенные батареи, имеющиеся в ИБП. На некоторых устройствах, 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.
Скорость зарядки батарей	<p>С помощью этого поля можно изменить скорость зарядки батарей ИБП в процентах. Здесь 100% представляют скорость зарядки, рекомендуемую производителем. Например, чтобы увеличить в два раза скорость зарядки, установите значение 200%.</p> <p>Например, когда для скорости зарядки батареи установлено значение 100%:</p> <ul style="list-style-type: none"> • При увеличении общей емкости батареи ток зарядки батареи, подаваемый зарядным устройством для батареи ИБП, автоматически увеличивается, чтобы сохранить скорость зарядки 100%, и скорость зарядки менять не требуется. • При уменьшении общей емкости батареи ток зарядки батареи, подаваемый зарядным устройством для батареи ИБП, автоматически уменьшается, чтобы сохранить скорость зарядки 100%, и скорость зарядки менять не требуется. <p>Дополнительную информацию о емкости батареи см. в руководстве пользователя ИБП.</p> <p>Внимание! Зарядка при слишком высокой скорости может привести к закипанию и/или утечке электролита и/или повышению давления газа. Не изменяйте эту настройку, если не обладаете достаточными знаниями в этой области.</p>
Тип батареи	Укажите тип батареи, где VRLA — это «Valve Regulated Lead Acid» (свинцово-кислотная батарея с клапанным регулированием), а Вентилируемая ячейка — это батарея с жидким электролитом (как в автомобилях).
Общая емкость батарей	Используйте этот параметр для определения общей емкости батарей ИБП от 7 до 200 ампер-часов (А-ч). Это значение используется для оценки времени работы и определения тока, необходимого для зарядки батарей. Если на используемом ИБП имеется параметр «Общая емкость батарей», обновляйте его значение при добавлении батарей в ИБП или извлечении их из ИБП. Дополнительную информацию о емкости батареи см. в руководстве пользователя ИБП.

Экран «Расписание самодиагностики»

Путь: ИБП > Конфигурация > Расписание самодиагностики

Используйте этот параметр для настройки времени запуска самодиагностики на ИБП.

Планирование выключения

Путь: Конфигурация > Планирование



Эта функция доступна не для всех ИБП. Функции планирования самотестирования отличаются для разных устройств ИБП.



Примечание. Не создавайте накладывающиеся друг на друга расписания. Пример накладывающихся друг на друга расписаний выключения: ежедневное выключение с 20:00 до 21:00 и разовое выключение с 20:10 до 20:30. Наложение расписаний выключения может привести к неизвестным и непроверенным результатам.

Для обоих параметров: ИБП и «Группы розеток»

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

При выборе **ИБП** или **Группы розеток** любые настроенные расписания отображаются вдоль верхней части экрана с подробными сведениями, включая сведения о том, включены они или выключены.

Редактирование, включение, отключение или удаление запланированного выключения. Щелкните имя расписания в списке расписаний, расположенном вдоль экрана **ИБП** или **Группы розеток**. Отображаются полные сведения, и можно изменить параметры. В том числе можно временно выключить устройство, сняв флажок **Включить**, или удалить устройство полностью.

Создание расписания выключений ИБП или группы переключаемых розеток.

1. В разделе **Планирование** выберите **ИБП** или **группу розеток**.
2. Используйте переключатели для выбора типа выключения, которое надо запланировать: **Одноразовое выключение**, **Ежедневное выключение** или **Еженедельное выключение**, 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 включится после ожидания в 6 минут).

Только для группы розеток укажите группу для выключения, щелкнув соответствующую кнопку.

Клиенты сетевого выключения по сигналу PowerChute: укажите, следует ли уведомлять клиенты PowerChute; см. раздел «Клиенты сетевого выключения PowerChute».



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

Экран «Обновление прошивки»

Путь: ИБП > Конфигурация > Обновление прошивки



Эта функция доступна не для всех ИБП.

Это обновление относится к *прошивке на ИБП*. Не путайте с обновлением прошивки ПСУ (см. раздел «Передача файлов»).



Следуйте инструкциям на экране **Обновление прошивки**, чтобы определить, нужно ли выключить выход ИБП перед обновлением прошивки. Это зависит от определенной модели ИБП.



Примечание. Для просмотра экрана **Обновление прошивки** в Internet Explorer® используйте версию браузера 10 или выше с выключенным просмотром в режиме совместимости. Экран обновления прошивки несовместим с браузером Edge®.

Выполните эти действия для обновления прошивки. (Альтернативный способ см. также в разделе «Использование FTP для обновления прошивки ИБП».)

1. Информацию по получению файла с обновлением прошивки и дальнейшие инструкции см. в статьях с идентификаторами [FA164737](#) и [FA170679](#) в базе знаний на [веб-сайте APC](#).
2. Выберите **Конфигурация - Обновление прошивки**.
3. Щелкните кнопку и найдите загруженный файл обновления на компьютере.
4. Щелкните кнопку **Обновить ИБП**, чтобы обновить прошивку ИБП.
5. По завершении обновления проверьте состояние в разделе **Результат последнего обновления и Текущая версия** или в журнале событий.

Обновление прошивки ИБП с USB-накопителя (только AP9641 или AP9643)

Прежде чем обновлять прошивку ИБП, убедитесь, что USB-накопитель поддерживает USB v1.1 и отформатирован в файловой системе FAT, FAT16 или FAT32.

1. Вставьте USB-накопитель в порт USB на компьютере.
2. Откройте статьи [FA164737](#) и [FA170679](#) в базе знаний на [веб-сайте APC](#), чтобы загрузить правильный файл обновления прошивки для ИБП, и сохраните файл в корневом каталоге USB-накопителя или в каталоге /upsw/ на USB-накопителе.
3. Извлеките устройство USB, содержащее файл прошивки, из порта компьютера и вставьте его в порт USB на ПСУ.
4. Откройте веб-интерфейс ПСУ и перейдите в раздел **«Конфигурация» > «Обновление прошивки»**.
5. Выберите файл прошивки в раскрывающемся списке под панелью обновления с USB-накопителя.
6. Нажмите кнопку **«Обновить ИБП»**, чтобы обновить прошивку ИБП.



ПРИМЕЧАНИЕ. Для обновления может потребоваться несколько минут. Не извлекайте устройство USB из ПСУ, пока обновление прошивки ИБП не будет завершено. Если USB-накопитель будет извлечен до завершения обновления, обновление не будет выполнено успешно.

7. По завершении обновления проверьте состояние в разделе **«Результат последнего обновления»** или в журнале событий.

Использование FTP для обновления прошивки ИБП

Если необходимо обновить слишком много устройств ИБП, можно сделать это быстрее с помощью FTP. Пример нужных действий приведен в следующей процедуре. Этот способ является альтернативным способом «Экран «Обновление прошивки»».



ПРИМЕЧАНИЕ. Протокол FTP отключен по умолчанию. Включите его, прежде чем продолжить. См. раздел «Экран сервера FTP».

1. Информацию по получению файла с обновлением прошивки и дальнейшие инструкции см. в статьях с идентификаторами [FA164737](#) и [FA170679](#) в базе знаний на [веб-сайте APC](#).
2. Передайте файл обновления по FTP в каталог **upsw** на плате, чтобы начать процесс обновления. Передача прошивки по FTP может быть прервана, если файл обновления поврежден или неприменим для ИБП.

Пример загрузки файла обновления с помощью команды DOS FTP:

```
$ ftp <Адрес сетевой платы ПСУ>
Connected to <Адрес сетевой платы ПСУ>.
220 AP9641 Network Management Card AOS vX.Y.Z FTP server ready.
User (<Адрес сетевой платы ПСУ>:(none)): apc
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> bin
200 TYPE Command okay.
ftp> hash
Hash mark printing On ftp:(2048 bytes/hash mark).
ftp> cd upsfw
250 CWD requested file action okay, completed.
ftp> put «<Путь к файлу прошивки ИБП>»
200 PORT Command okay.
150 File status okay; about to open data connection.
226 Closing data connection.
ftp: 121984 bytes sent in 1.39Seconds 87.70Kbytes/sec.
ftp> quit
221 Goodbye.
```

3. По завершении обновления проверьте состояние в разделе **Результат последнего обновления** на странице обновления прошивки веб-интерфейса или в журнале событий.

Клиенты сетевого выключения PowerChute

Путь: ИБП > Конфигурация > PowerChute

Сетевое выключение PowerChute позволяет удаленно выключить устройства ИБП.

При установке клиента сетевого выключения PowerChute он добавляется в этот список автоматически. При удалении клиента сетевого выключения PowerChute он автоматически удаляется.

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.

При наличии групп розеток необходимо также указать, какая группа розеток предоставляет питание клиенту PowerChute.



ПРИМЕЧАНИЕ. PowerChute не может соединиться с ПСУ, если на ПСУ выключен протокол HTTP. Чтобы включить протокол HTTP или HTTPS, см. раздел «Экран веб-доступа».

Экран «Универсальный ввод-вывод»



Меню **Универсальный ввод-вывод** применимо, если установлены датчики температуры и влажности (AP9335T/TH) или устройство ввода-вывода с сухим контактом (AP9810). Использование этих устройств часто называют мониторингом окружающей среды.

Экран «Температура и влажность»

Путь: Универсальный ввод-вывод > Температура и влажность

Здесь отображается имя, состояние тревоги, температура и влажность (если поддерживается) для каждого датчика. Щелкните имя датчика, чтобы изменить имя и местоположение или настроить пороговые значения и гистерезис.

Пороговые значения. Для каждого датчика задаются пороговые значения температуры и влажности (если поддерживается такое измерение). При выходе показателя за пороговые значения звучит сигнал тревоги.

Сообщения **Высокое** и **Низкое** являются предупреждающими. Сообщения **Максимум** и **Минимум** являются критическими и требуют внимания.

Гистерезис. Используйте значение гистерезиса во избежание повторных сигналов тревоги для одного и того же нарушения порогов температуры или влажности.

Когда температура или влажность, вызывающая выход за пороговое значение, склонна к незначительному колебанию вверх и вниз, она может многократно генерировать сигнал. Большое значение гистерезиса может это предотвратить.

Если значение гистерезиса недостаточно велико, колебание может сначала вызывать нарушение пороговых значений, а потом восстанавливать нормальную ситуацию, что означает, что сигнал тревоги может срабатывать несколько раз. См. примеры далее, предварительно обратив внимание на следующие замечания.

- В случае выхода за верхнее и нижнее пороговые значения точкой сброса сигнала тревоги является пороговое значение *минус* указанное значение гистерезиса.
- Для нарушения минимального и низкого порогового значений точка сброса — это пороговое значение *плюс* значение гистерезиса.

Пример повышения влажности с колебаниями. Допустим, *максимальное* пороговое значение влажности составляет 65%, а гистерезис влажности равен 10%. Допустим, что влажность поднимается выше 65%, вызывая сигнал тревоги. После этого она многократно опускается до 60% и поднимается до 70%, однако — благодаря значению гистерезиса в 10% — сигнал тревоги не сбрасывается и поэтому никакой новой тревоги не возникает. Для сброса существующего сигнала тревоги влажность должна упасть ниже 55% (что соответствует значению 65% *минус* 10%).

Пример падения температуры с колебаниями. Допустим, *минимальное* пороговое значение температуры равно 12°C, а гистерезис температуры — 2°C. Допустим, что температура падает ниже 12°C, вызывая сигнал тревоги. После этого она многократно поднимается до 13°C и опускается до 11°C, однако — благодаря значению гистерезиса в 2°C — сигнал тревоги не сбрасывается и поэтому никакой новой тревоги не возникает. Для сброса существующего сигнала тревоги температура должна подняться выше 14°C (что соответствует значению 12°C *плюс* 2°C).

Экран «Входные контакты»

Путь: Универсальный ввод/вывод > Входные контакты

На экране **Входные контакты** отображается имя, состояние тревоги и состояние (открыт или закрыт) каждого контакта. Эти данные автоматически получаются и отображаются здесь при установке устройства для мониторинга окружающей среды.

Щелкните имя входного контакта для получения подробного описания состояния или для настройки значений. При отключении данный контакт не формирует аварийного сигнала, даже если он находится в аномальном положении. Остальные поля рассмотрены далее.

Поле	Описание
Состояние тревоги	Нормальное , если данный входной контакт не сообщает об аварийном сигнале или не сообщает о степени опасности при сообщении об аварийном сигнале. Если это поле выключено для контакта, отображается Отключено .
Состояние	Текущее состояние данного входного контакта: Закрыто или Открыто .
Нормальное состояние	Нормальное (неаварийное) состояние данного входного контакта: Закрыто или Открыто .
Степень опасности	Степень опасности аварийного сигнала, генерируемого аномальным состоянием данного входного контакта: Предупредительное или Критическая .

Экран «Выходное реле»

Путь: Универсальный ввод-вывод > Выходное реле

Выходное реле — здесь отображается имя и состояние каждого реле (открыто или закрыто). Эти данные автоматически получаются и отображаются здесь при установке устройства для мониторинга окружающей среды.

Щелкните имя входного контакта для получения подробного описания состояния или для настройки значений. Поля рассмотрены далее.

Поле	Описание
Состояние	Текущее состояние данного выходного реле. Закрыто или Открыто .
Нормальное состояние	Нормальное (неаварийное) состояние данного выходного реле. Закрыто или Открыто .
Управление	Для изменения текущего состояния данного выходного реле установите этот флажок и щелкните «Применить».

Поле	Описание
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. 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 которого выходное реле остается активным после подачи сигнала тревоги. Даже в случае корректировки активизирующего сигнала тревоги выходное реле остается включенным, пока не закончится данный период.

Настройка политики управления

Путь: Универсальный ввод-вывод > Политика управления

На ПСУ AP9641 или AP9643, к которой подключены устройства ввода-вывода с сухим контактом (AP9810), можно выполнить следующие действия:

- настроить выходные реле на открытие или закрытие на основании событий на ИБП и входных контактах; см. раздел «Настройка выхода для реакции на событие»;
- настроить ИБП на выполнение действий на основании входных контактов; см. раздел «Настройка ИБП или выхода для реакции на входной сигнал тревоги».



Не все устройства ИБП можно настроить на реакцию на входные контакты.

Настройка выхода для реакции на событие.

1. В меню **Конфигурация** выберите **Универсальный ввод-вывод** и **Политика управления**.
2. Щелкните кнопку **Добавить политику**.
3. Щелкните имя категории или подкатегории для просмотра соответствующих событий.
4. Для настройки щелкните имя события, установите флажок выходного реле, которое будет менять состояние в случае этого события, и щелкните **Сохранить политику**.

Настройка ИБП или выхода для реакции на входной сигнал тревоги.

1. В меню **Конфигурация** выберите **Универсальный ввод-вывод** и **Политика управления**.
2. Щелкните кнопку **Добавить политику**.
3. Щелкните подкатегорию **Контакт ввода-вывода**.
4. Выберите событие с той же серьезностью, что и входной контакт. Например, если для входного контакта установлена критическая серьезность, выберите критическое событие.
ПСУ поддерживает до четырех входов. Необходимо указать вход, который будет связан с этим событием.
5. В раскрывающемся списке **Порт** выберите номер универсального **порта** датчика (1 или 2), к которому подключается устройство ввода-вывода с сухим контактом.
6. В раскрывающемся списке **Зона** выберите букву для зоны (А или В) контакта, на который установлен вход.
7. Определите действие, которое ИБП будет выполнять (если оно требуется), когда состояние входа изменяется.
8. Выберите выход, который будет открываться или закрываться (если это требуется).
9. Щелкните **Сохранить политику**.



Настраиваемая операция происходит один раз.

Если восстановить на входе нормальное состояние до сброса условия тревоги, на выходе состояние не изменится, пока условие тревоги не будет сброшено, а затем снова установлено.

Меню «Безопасность»

Экран «Управление сеансом»

Путь: Конфигурация > Безопасность > Управление сеансом

Включение функции **Разрешить одновременные входы** означает, что в систему могут одновременно войти два пользователя или более. Каждому пользователю предоставляется равный доступ, и каждый интерфейс (HTTP, FTP, консоль telnet, консоль с последовательным интерфейсом (CLI) и т. д.) рассматривается как пользователь, вошедший в систему. Функция **Разрешить одновременные входы** обеспечивает возможность одновременного входа восьми пользователей в веб-интерфейс, пяти — в интерфейс командной строки и одного — в консоль с последовательным интерфейсом.

Удаленная аутентификация заблокирована. ПСУ поддерживает хранение RADIUS для паролей на сервере. Однако, если включить это переопределение, ПСУ позволит локальному пользователю выполнить вход с помощью пароля для ПСУ, сохраненного локально на ПСУ. См. также «Локальные пользователи» и «Аутентификация удаленных пользователей».

Ответ ping

Путь: Конфигурация > Безопасность > Ответ ping

Установите флажок **IPv4 Ping Response** (Ответ ping IPv4), чтобы плата сетевого управления 3 могла отвечать на сигналы эхо-тестирования. Такой режим не применяется для IPv6.

Локальные пользователи

Используйте эти пункты меню для просмотра и настройки доступа и отдельных параметров (например, формата отображения даты) интерфейсов пользователя ПСУ. Это применимо к пользователям в соответствии с их именами входа.

Путь: Конфигурация > Безопасность > Локальные пользователи > Управление

Настройка доступа пользователя. С помощью этой функции администратор или суперпользователь может составить список пользователей, которым доступен интерфейс пользователя, и настроить этих пользователей. Щелкните ссылку имени для просмотра сведений, изменения или удаления пользователя.

Щелкните **Добавить пользователя** для добавления пользователя. На открывшемся экране **Конфигурация пользователя** можно добавить пользователя и отозвать доступ, сняв флажок **Доступ**. Максимальная длина имени и пароля составляет 64 байта, при использовании многобайтовых символов это соответствует меньшему числу символов. Необходимо ввести пароль.



Значения длиннее 64 байтов в полях имени и пароля могут быть усечены!

Создайте пароль, используя сочетание символов верхнего и нижнего регистра, чисел и специальных символов. Длина паролей не может превышать 64 символа в формате ASCII.

Используйте параметр **Превышено время ожидания сеанса** для настройки времени ожидания, по истечении которого интерфейс пользователя выполняет принудительный выход пользователя из системы (по умолчанию — три минуты). При изменении этого значения необходимо выйти из системы, чтобы изменение вступило в силу.

Удаленная аутентификация последовательного подключения заблокирована. Выбрав эту функцию, можно обойти RADIUS, используя подключение консоли с последовательным интерфейсом (CLI). На этом экране можно включить данную функцию для выбранного пользователя, однако ее можно включить и глобально; см. раздел «Экран «Управление сеансом»».

См. также «Конфигурация > Безопасность > Локальные пользователи > Настройки по умолчанию» далее. Дополнительную информацию об учетных записях см. в разделе «Типы учетных записей».

Параметры пользователя. . Установите флажок **Цветовая кодировка журнала событий**, чтобы включить функцию выделения цветом текста сообщений об аварийных сигналах, регистрируемых в журнале событий. (Записи системных событий и изменения конфигурации не изменят свой цвет.)

Цвет текста	Серьезность аварийного сигнала
Красный	Критическая: критический аварийный сигнал, требующий немедленного принятия мер.
Оранжевый	Предупредительное: аварийный сигнал требует внимания, поскольку не устраненная вовремя проблема может привести к потере данных и порче оборудования.
Зеленый	Сигнал сброшен: условия, которые вызвали сигнал, устранены.
Черный	Нормальное: сигналов тревоги нет. Плата сетевого управления и все подключенные к ней устройства работают нормально.
Синий	Информационная: сигнал тревоги, предоставляющий информацию. Плата сетевого управления и все подключенные к ней устройства работают нормально.

Формат журнала экспорта. Экспортированные файлы журналов могут быть отформатированы в виде значений, разделенных запятыми (comma-separated values — CSV) или знаками табуляции. См. раздел «Отображение журнала событий».

Выберите шкалу температуры для измерений в этом интерфейсе пользователя. Значение **США, обычная** соответствует градусам Фаренгейта, а **Метрическая** — градусам Цельсия.

Язык пользовательского интерфейса можно указать в поле **Язык**. Язык можно также указать при загрузке.



Можно также задавать различные языки для получателей электронной почты и приемников прерываний SNMP. См. разделы «Получатели электронной почты» и «Получатели прерываний».

Путь: Конфигурация > Безопасность > Локальные пользователи > Настройки по умолчанию

Настройка значений по умолчанию может ускорить добавление пользователей. Используйте это меню для настройки значений по умолчанию для многих параметров; см. раздел «Конфигурация > Безопасность > Локальные пользователи > Управление» выше.

Аутентификация удаленных пользователей

Путь: Конфигурация > Безопасность > Удаленные пользователи > аутентификация

Аутентификация. Укажите способ аутентификации пользователей при входе в систему.



Информацию о локальной аутентификации (без использования централизованной аутентификации сервера RADIUS) см. в *Руководстве по безопасности*, доступном на [веб-сайте APC](#).

Поддерживаются следующие функции аутентификации и проверки подлинности RADIUS (Remote Authentication Dial-In User Service — служба удаленной аутентификации пользователей по телефонным линиям):

- Когда пользователь осуществляет доступ к плате сетевого управления или к другому сетевому устройству с включенными функциями RADIUS, запрос аутентификации передается на сервер RADIUS, чтобы определить уровень допуска пользователя.
- Длина имен пользователей RADIUS, используемых в ПСУ, ограничена 32 символами.

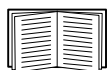
Выберите один из следующих вариантов:

- **Только локальная аутентификация.** RADIUS отключен. См. раздел «Локальные пользователи».
- **RADIUS, затем локальная аутентификация.** Включены обе функции. Сначала запрашивается аутентификация от сервера RADIUS. Если сервер RADIUS не отвечает, то используется локальная аутентификация.
- **Только RADIUS.** Локальная аутентификация отсутствует.



Если выбирается **Только RADIUS**, а сервер RADIUS недоступен, неправильно идентифицирован или неправильно сконфигурирован, то удаленный доступ невозможен для всех пользователей. Для восстановления доступа необходимо использовать подключение к интерфейсу командной строки по последовательному каналу связи и изменить настройку **access** на **local** или **radiusLocal**.

Например, команда изменения настройки доступа на **local** имеет следующий вид:
radius -a local



См. также раздел «Экран RADIUS» далее и «Конфигурирование сервера RADIUS».

Экран RADIUS

Путь: Конфигурация > Безопасность > Удаленные пользователи > RADIUS

Для аутентификации удаленных пользователей можно использовать сервер RADIUS. Используйте эту функцию для выполнения следующих действий:

- Просмотреть список серверов RADIUS (максимум два), доступных для ПСУ, и период времени ожидания для каждого из них.
- Настроить параметры аутентификации для нового или существующего сервера RADIUS, щелкнув ссылку **Сервер RADIUS**.

Настройка RADIUS	Описание
Сервер RADIUS	Имя или IP-адрес сервера (IPv4 или IPv6). Примечание. Для аутентификации пользователей сервер RADIUS по умолчанию использует порт 1812. Чтобы использовать другой порт, добавьте к имени или IP-адресу сервера RADIUS двоеточие с последующим указанием номера нового порта. ПСУ поддерживает порты 1812, 5000–32768.
Секрет	Общий секрет для сервера RADIUS и платы сетевого управления.
Время ожидания ответа	Время в секундах, в течение которого плата сетевого управления ожидает ответа от сервера RADIUS.
Настройки тестирования	Введите имя и пароль администратора, чтобы протестировать настроенный путь к серверу RADIUS.
Пропустить тестирование и применить	Пропуск теста пути к серверу RADIUS.



См. также раздел «Аутентификация удаленных пользователей» выше и «Конфигурирование сервера RADIUS» далее.

Конфигурирование сервера RADIUS

Сводные данные о процедуре настройки.

Необходимо настроить сервер RADIUS на работу с ПСУ; см. действия далее.



Примеры пользовательских файлов RADIUS с атрибутами, зависящими от поставщика (VSA), и пример записи в словарный файл на сервере RADIUS приведены в *Руководстве по безопасности* на [сайте APC](#).

1. Добавьте IP-адрес ПСУ в список (файл) клиентов сервера RADIUS.
2. Пользователи должны быть настроены с атрибутами «тип обслуживания», если не заданы атрибуты поставщика. Если настроенные атрибуты «тип обслуживания» отсутствуют, пользователи будут иметь только доступ для чтения (только в интерфейсе пользователя).



Информацию о файле пользователей RADIUS см. в документации к серверу RADIUS, а пример — в документе *Руководство по безопасности*.

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. При изменении цифровых значений функции аутентификации и авторизации RADIUS перестают функционировать. VSA имеет преимущество перед стандартными атрибутами RADIUS.

Настройка сервера RADIUS в UNIX® с теньвыми паролями.

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

- Если все пользователи UNIX имеют права администратора, добавьте в файл пользователей RADIUS следующие данные. Чтобы допустить только пользователей устройств, замените Тип обслуживания APC на Device (устройство).

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

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

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

Поддерживаемые серверы RADIUS.

Поддерживаются FreeRADIUS версий 1.x и 2.x, а также сервер политики сети (NPS) Microsoft Server 2008 и 2012. Можно использовать другие общедоступные приложения RADIUS, но, возможно, они не были протестированы в полной мере.

Экраны брандмауэра

Путь: Конфигурация > Безопасность > Брандмауэр > Конфигурация

Включение или выключение функции брандмауэра. По умолчанию указана настроенная политика. Установите флажок **Включить**, чтобы включить брандмауэр. По умолчанию этот флажок снят.

- Нажмите кнопку **Применить**, чтобы подтвердить включение выбранной политики. Открывается страница **Подтверждение брандмауэра**.
 - На странице подтверждения приведена рекомендация тестировать брандмауэр перед включением. Эта операция является обязательной.
 - Первая гиперссылка ведет на страницу политики брандмауэра.
 - Вторая гиперссылка ведет на страницу политики тестирования брандмауэра.
 - Нажмите кнопку **Применить**, чтобы включить брандмауэр и вернуться на страницу конфигурации.
 - Нажмите кнопку **Отмена**, чтобы вернуться на страницу конфигурации, не включая брандмауэр.
- Нажмите кнопку **Отмена**: выбранная политика не включается. Вы остаетесь на странице конфигурации.

Путь: Конфигурация > Безопасность > Брандмауэр > Активная политика

Выбор активной политики в раскрывающемся списке «Доступные политики», а также просмотр срока ее действия. По умолчанию отображается текущая активная политика, при необходимости вы можете выбрать в списке другую политику.

- Нажмите кнопку **Применить**, чтобы применить изменения. Если был выбран и включен другой брандмауэр, это изменение применяется немедленно. Если была выбрана новая настроенная политика, рекомендуется протестировать новый брандмауэр перед включением. (См. приведенное выше описание конфигурации.)
- Нажмите кнопку **Отмена**, чтобы восстановить исходную активную политику и остаться на странице активной политики.

Путь: Конфигурация > Безопасность > Брандмауэр > Активные правила

Если брандмауэр включен, на этой странице, доступной только для чтения, отображается список отдельных правил, принудительно примененных текущей активной политикой. См. раздел **Создание/редактирование политики**, где описаны поля «Приоритет», «Назначение», «Источник», «Протокол», «Действие» и «Журнал».

Путь: **Конфигурация > Безопасность > Брандмауэр > Создание/редактирование политики**

Создание новой политики либо удаление или изменение существующей:

Примечание. Хотя удалить активную включенную политику брандмауэра нельзя, используемую политику можно изменить. Однако делать это не рекомендуется, так как изменения применяются немедленно. Вместо этого отключите брандмауэр, измените политику, протестируйте ее и снова включите.

Создание политики: Нажмите кнопку **Добавить политику** и введите имя для нового файла брандмауэра. Это имя должно иметь расширение .fwl. Если не указывать расширение, к имени файла автоматически добавляется .fwl.

- Нажмите кнопку **Применить**: Если имя файла допустимо, создается пустой файл для политики брандмауэра. Он находится в папке /fwl вместе с другими политиками системы.
- Нажмите кнопку **Отмена**, чтобы вернуться на предыдущую страницу, не создавая файл брандмауэра.

Изменение существующей политики:

Выберите **Изменить политику**, чтобы перейти на страницу редактирования. Можно изменить политику брандмауэра, которая не является активной.

Страница предупреждения: Если вы попытаетесь изменить активную включенную политику, открывается страница предупреждения:

«Изменение активной политики брандмауэра приведет к немедленному применению всех изменений. Перед включением политики рекомендуется отключить брандмауэр и протестировать ее.»

- Нажмите кнопку **Применить**, чтобы покинуть страницу предупреждения и вернуться на страницу «Изменение политики».
 - Нажмите кнопку **Отмена**, чтобы покинуть страницу предупреждения и вернуться на страницу «Создание/редактирование политики».
1. Выберите изменяемую политику в раскрывающемся списке **Имя политики**, а затем нажмите кнопку **Изменить политику**.
 2. Нажмите кнопку **Добавить правило** или выберите **Приоритет** для существующего правила, чтобы перейти на страницу **Изменение правила**. На этой странице можно изменить настройки правила или удалить выбранное правило.

Настройка	Описание
Priority	Если 2 правила конфликтуют между собой, применяется правило с наибольшим приоритетом. Наибольший приоритет равен 1, наименьший — 250.
Type	host: в поле «IP/any» введите отдельный IP-адрес. subnet: в поле «IP/any» введите адрес подсети. range: в поле «IP/any» введите диапазон IP-адресов.
IP/any	Укажите IP-адрес или диапазон IP-адресов, к которым применяется это правило, либо выберите одно из следующих значений: <ul style="list-style-type: none"> • any: правило применяется независимо от IP-адреса. • anyip4: правило применяется для любого IPv4-адреса. • anyip6: правило применяется для любого IPv6-адреса.
Port	Укажите порт, к которому применяется правило. <ul style="list-style-type: none"> • None: правило не применяется ни к одному из портов. • Common Configured ports: выберите стандартный порт. • Other: укажите нестандартный номер порта.

Настройка	Описание
Protocol	<p>Укажите протокол, к которому применяется правило.</p> <ul style="list-style-type: none"> • any: любой протокол. • tcp: используется для надежной передачи информации между приложениями. • udp: альтернатива протоколу TCP, используемая для ускорения передачи в условиях меньшей пропускной способности. Хотя в протоколе UDP меньше задержки, протокол TCP надежнее. • icmp: используется для вывода сведений об ошибках для устранения неполадок. • icmpv6: используется для вывода сведений об ошибках для устранения неполадок в приложениях, использующих IPv6-адреса.
Action	<p>allow: разрешить пакет, соответствующий этому правилу. discard: отменить пакет, соответствующий этому правилу.</p>
Log	<p>Если это правило применяется к пакету, то независимо от того, разрешается ли пакет или блокируется, в журнал брандмауэра добавляется запись. См. раздел «Журнал брандмауэра».</p>

Рекомендуется добавить одно из следующих правил в качестве низкоприоритетного правила в политику брандмауэра:

- Чтобы использовать брандмауэр в режиме белого списка, добавьте
`250 Dest any / Source any / protocol any / discard`
- Чтобы использовать брандмауэр в режиме черного списка, добавьте
`250 Dest any / Source any / protocol any / allow`

Удаление политики:

Выберите **Удалить политику**, чтобы открыть страницу «Подтверждение удаления».

Нажмите кнопку **Применить** для подтверждения удаления выбранного файла брандмауэра из файловой системы.

Путь: Путь: Конфигурация > Безопасность > Брандмауэр > Загрузка политики

Загрузка политики (с расширением .fwl) из источника, внешнего для данного устройства.

Путь: Путь: Конфигурация > Безопасность > Брандмауэр > Проверка

Временное применение правил выбранной политики на указанный период.

802.1 X Конфигурация безопасности

Путь: Конфигурация > Безопасность > Безопасность 802.1 X

ПСУ берет на себя роль запрашивающего устройства в архитектуре EAPoL (Расширяемый протокол аутентификации по локальной сети), используемой для управления доступом к сети по порту в IEEE 802.1 X. ПСУ поддерживает EAP-TLS как метод аутентификации, который требует загрузки трех клиентских сертификатов. Закрытый ключ хранится в зашифрованном формате. Вы должны указать действительную парольную фразу, чтобы получить доступ к конфигурации безопасности 802.1 X.

ПРИМЕЧАНИЕ: ПСУ поддерживает только метод аутентификации EAP-TLS.

Веб-интерфейс предлагает следующие варианты настройки EAPoL.

Параметры	Описание
Доступ к EAPoL	Используется для включения или отключения доступа к безопасности 802.1 X. ПРИМЕЧАНИЕ: по умолчанию доступ к безопасности 802.1X отключен. Доступ можно включить только при наличии действительных сертификатов и действительной парольной фразы для закрытого ключа.
Идентификатор запрашивающего устройства	Позволяет задать собственный идентификатор запрашивающего устройства (до 32 символов, включая пробелы). ПРИМЕЧАНИЕ: по умолчанию идентификатор запрашивающего устройства имеет значение «NMC-Supplicant-xx:xx:xx:xx:xx:xx», где набор «xx» это MAC-ID ПСУ.
Сертификат ЦС	Загрузите/замените или удалите корневой сертификат ЦС. Поддерживаемые форматы файлов: PEM (почта с усовершенствованной защитой Privacy Enhanced Mail), DER (особые правила кодирования Distinguished Encoding Rules) и расширения файлов .pem, .PEM, .der, и .DER.
Сертификат закрытого ключа	Загрузите/замените или удалите зашифрованный закрытый ключ. Поддерживаемые форматы файлов: PEM (почта с усовершенствованной защитой Privacy Enhanced Mail), DER (особые правила кодирования Distinguished Encoding Rules) и расширения файлов .key и .KEY. ПРИМЕЧАНИЕ: незашифрованные закрытые ключи недопустимы.
Парольная фраза закрытого ключа	Укажите парольную фразу для дешифровки зашифрованного закрытого ключа. Лимит: 64 символа включая пробелы.
Пользовательский/открытый сертификат	Загрузите/замените или удалите пользовательский/открытый сертификат. Поддерживаемые форматы файлов: PEM (почта с усовершенствованной защитой Privacy Enhanced Mail), DER (особые правила кодирования Distinguished Encoding Rules) и расширения файлов .pem, .PEM, .der, и .DER.

Настройка параметров: 2

С помощью элементов меню конфигурации можно установить значения основных рабочих параметров ИБП и ПСУ.

См. следующие разделы и раздел «Настройка параметров: 1».

- ««Сеть» в меню конфигурации»
- «Меню уведомлений»
- «Меню «Общие»»
- «Журналы в меню конфигурации»



ПРИМЕЧАНИЕ. Некоторые параметры конфигурации можно увидеть на экране с обзором конфигурации Configuration Summary (**Configuration > Network > Summary**).

«Сеть» в меню конфигурации

Экран настроек TCP/IP для IPv4

Путь: Конфигурация > Сеть > TCP/IP > Настройки IPv4

Данная функция позволяет просмотреть любой текущий адрес IPv4, маску подсети, шлюз по умолчанию, MAC-адрес и режим загрузки платы сетевого управления 3 (ПСУ) для ИБП. Нижняя часть экрана используется для настройки этих параметров, в том числе и для отключения IPv4.



Информацию о DHCP и параметрах DHCP см. в стандартах [RFC2131](#) и [RFC2132](#).

Параметр	Описание
Ручной	В этом разделе можно указать адрес IPv4, маску подсети и шлюз по умолчанию.
BOOTP*	Устройство запрашивает через 32-секундные интервалы сетевые настройки у любого из серверов BOOTP: <ul style="list-style-type: none">• Если она получает допустимый ответ, то запускает сетевые службы.• При наличии ранее заданных сетевых параметров и при отсутствии допустимого ответа на пять запросов (исходный и четыре повторных) система по умолчанию использует эти параметры. Это обеспечивает доступность устройства, если сервер BOOTP недоступен.• Если устройство находит сервер BOOTP, но направленный ему запрос не срабатывает или завершается по тайм-ауту, устройство прекращает запрос сетевых параметров до перезапуска.
DHCP*	Устройство запрашивает через 32-секундные интервалы сетевые настройки у любого из серверов DHCP: <ul style="list-style-type: none">• Если сервер DHCP будет найден, но направленный ему запрос не срабатывает или завершается по тайм-ауту, система прекращает запрос сетевых параметров до перезапуска.• Кроме того, можно настроить устройство с помощью параметра Требовать файл cookie, характерный для поставщика, чтобы принять адрес DHCP, что позволяет принимать выдаваемые значения и запускать сетевые службы. См. раздел «Параметры ответов DHCP».

*Класс поставщика: APC.

Идентификатор клиента: MAC-адрес устройства. Если изменить это значение, новое значение должно быть уникальным в ЛС.

Класс пользователя: название модуля микропрограммного обеспечения; см. раздел «Передача файлов».

Экран настроек TCP/IP для IPv6

Путь: Конфигурация > Сеть > TCP/IP > Настройки IPv6

Данная функция позволяет просмотреть любые текущие настройки IPv6 платы сетевого управления 3 (ПСУ) ИБП. Нижняя часть экрана используется для настройки этих параметров, в том числе и для отключения IPv6.

Можно использовать ручную или автоматическую IP-адресацию. Можно также одновременно использовать обе настройки. Для ручной адресации (**Ручной**) установите флажок и введите **Системный IP-адрес** v6 и **Основной шлюз**.

Установите флажок **Автоматическая конфигурация**, чтобы система получала префиксы адресов от маршрутизатора (если таковой имеется). Система будет использовать указанные префиксы для автоматической настройки адресов IPv6.

Возможные форматы IPv6	Описание
fe80:0000:0000:0000:0204:61ff:fe9d:f156	полная форма IPv6
fe80:0:0:0:204:61ff:fe9d:f156	пропуск начальных нулей
fe80:204:61ff:fe9d:f156	сворачивание нескольких нулей в :: в адресе IPv6
fe80:0000:0000:0000:0204:61ff:254.157.241.86	IPv4 с отдельными четырьмя символами, отделенными точкой в конце
fe80:0:0:0:0204:61ff:254.157.241.86	пропуск начальных нулей, IPv4 с отдельными четырьмя символами, отделенными точкой в конце
fe80:204:61ff:254.157.241.86	с отдельными четырьмя символами, отделенными точкой в конце, сворачивание нескольких нулей
::1	localhost
fe80:	префикс link-local
2001:	глобальный одноадресный префикс

Для **Режима DHCPv6** см. следующую таблицу.

Режим DHCPv6 для конфигурации IPv6	
Параметр	Описание
Управляемый маршрутизатор	<p>Когда этот флажок установлен, DHCPv6 управляется флагами М (Managed Address Configuration Flag) и О (Other Stateful Configuration Flag), получаемыми в сообщениях маршрутизатора IPv6.</p> <p>При получении сообщения маршрутизатора ПСУ проверяет, установлены ли флаги «М» и «О». ПСУ интерпретирует их следующим образом:</p> <ul style="list-style-type: none"> • Ни один флаг не задан. Означает, что локальная сеть не имеет инфраструктуры DHCPv6. Плата сетевого 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. • Заданы флаги «М» или «М» и «О». В этом случае имеется полная конфигурация адреса DHCPv6. DHCPv6 используется для получения адресов и прочих настроек конфигурации. Этот режим называется «DHCPv6 с сохранением адресов». После получения флага «М» конфигурация адреса DHCPv6 остается действительной, пока рассматриваемый интерфейс не будет закрыт, даже если последующие пакеты сообщений маршрутизатора поступают без установленного флага «М». Если первым будет получен флаг «О», а затем флаг «М», плата сетевого управления произведет полную конфигурацию адреса по получению флага «М». • Задан только флаг «О». В этом случае плата сетевого управления отправляет пакет DHCPv6 Info-Request (пакет запроса информации). DHCPv6 используется для настройки «других» параметров (таких как местоположение DNS-серверов), НО НЕ для получения адресов. Этот режим называется «DHCPv6 без сохранения адресов».
Адрес и другие сведения	DHCPv6 используется для получения адресов и прочих настроек конфигурации. Этот режим называется «DHCPv6 с сохранением адресов».
Только сведения, за исключением адресов	DHCPv6 используется для настройки «других» параметров (таких как местоположение DNS-серверов), НО НЕ для получения адресов. Этот режим называется «DHCPv6 без сохранения адресов».
Никогда	DHCPv6 НЕ используется для каких-либо настроек конфигурации.

Параметры ответов DHCP

Каждый действительный ответ DHCP содержит параметры с настройками TCP/IP, которые необходимы ПСУ для работы в сети. Каждый ответ также содержит другую информацию, влияющую на работу ПСУ. См. также статью [FA156110](#) в базе знаний.

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

- **Cookie APC. Tag 1, Len 4, Data «1APC»**

Параметр 43 сообщает ПСУ, что сервер DHCP настроен на обслуживание устройств.

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

Параметр 43 = 0x01 0x04 0x31 0x41 0x50 0x43

Параметры TCP/IP. ПСУ 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 ПСУ.
- **Маска подсети** (параметр 1). Маска подсети определяет значение, необходимое для работы ПСУ в сети.
- **Маршрутизатор**, т.е. шлюз по умолчанию (параметр 3). Адрес шлюза по умолчанию, необходимый для работы ПСУ в сети.
- **Время выдачи IP-адреса** (параметр 51). Промежуток времени, в течение которого выдается IP-адрес для ПСУ.
- **Время обновления, T1** (параметр 58): Время, которое ПСУ должна ожидать после выдачи IP-адреса перед тем, как она сможет запросить обновление этого назначения.
- **Время продления использования, T2** (параметр 59). Время, которое ПСУ должна ожидать после выдачи IP-адреса перед тем, как она сможет продлить использование адреса.

Другие параметры. ПСУ также использует следующие параметры, содержащиеся в достоверном отклике DHCP. Все указанные параметры, за исключением двух последних, описаны в RFC2132.

- **Серверы протокола сетевого времени** (параметр 42). До двух NTP-серверов (первичный (основной) и вторичный (вспомогательный)), которые может использовать ПСУ.
- **Сдвиг времени** (параметр 2). Сдвиг времени подсети ПСУ относительно универсального координированного времени (UTC), задаваемый в секундах.
- **Сервер доменных имен** (параметр 6). До двух серверов доменных имен (DNS) (первичный и вторичный), которые может использовать ПСУ.
- **Имя хоста** (параметр 12). Имя хост-узла, которое использует ПСУ (максимальная длина — 32 символа).
- **Имя домена** (параметр 15). Имя домена, которое использует ПСУ (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 ПСУ осуществляет загрузку `ini`-файла. После загрузки ПСУ использует `ini`-файл в качестве загрузочного файла с целью изменения настроек.
- **Полностью определенное имя домена (FQDN, параметр 81)**. Полностью определенное имя домена ПСУ.

Экран «Скорость порта»

Путь: Конфигурация > Сеть > Скорость порта

Параметр скорости порта задает скорость обмена данными порта Ethernet. Текущий параметр отображается в разделе **Текущая скорость**.

Параметр можно изменить, выбрав переключатель в разделе **Скорость порта**:

- При значении **Автосогласование** (по умолчанию) сетевые устройства определяют максимально возможную скорость передачи данных. Если при этом скорости передачи данных двух устройств не совпадают, обмен будет осуществляться на более низкой скорости.
- Можно также выбрать **10** или **100** Мбит/с; для каждого из этих параметров можно указать значение:
 - **полудуплекс** (передача данных только в одном направлении за единицу времени) или
 - **полный дуплекс** (один канал может использоваться для передачи данных сразу в двух направлениях).

ПРИМЕЧАНИЕ. Изменить можно только скорость порта до 1000 Мбит/с, выбрав опцию автосогласования **Auto-negotiation**.

Экран DNS

Путь: Конфигурация > Сеть > DNS > Конфигурация

Значения в разделе **Состояние службы доменных имен** отображают текущее состояние и настройку.

Параметры в разделе **Ручные настройки службы доменных имен** используются для настройки системы доменных имен (DNS):

- Включение меню **Заблокировать ручные настройки DNS** позволяет установить, чтобы данные конфигурации от других источников, таких как DHCP, имели приоритет перед выполненной в этом разделе ручной конфигурацией.
- Укажите адреса IPv4 или IPv6 для параметра **Первичный DNS-сервер** и при необходимости для параметра **Вторичный DNS-сервер**. Чтобы отправлять электронную почту с помощью ПСУ, необходимо как минимум указать IP-адрес первичного DNS-сервера.
 - ПСУ ждет ответа до 15 секунд от первичного или вторичного DNS-сервера. Если ПСУ не получает ответ в указанное время, сообщение электронной почты не будет отправлено. Используйте DNS-серверы в том же сегменте, где расположена ПСУ, или в соседнем сегменте, но не в других удаленных сегментах сети (ГС).
 - После определения IP-адресов серверов DNS выполните их проверку; см. раздел «Экран проверки DNS».
- **Синхронизация имен системы**. Позволяет синхронизировать имя хоста DNS с именем ПСУ. Щелкните ссылку «Имя системы» для определения значения.



Если имя хоста DNS и имя системы ПСУ синхронизированы, длина имени системы ограничена определенным количеством символов в зависимости от DNS RFC. Если они не синхронизированы, имя системы может содержать до 255 символов.

- **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 ПСУ (кроме адресов электронной почты), которые работают с доменным именем.
- **Имя домена (IPv4/IPv6)**. Для интерфейса ПСУ в этом разделе потребуется указать только имя домена. Во всех остальных полях интерфейса пользователя ПСУ (кроме полей адресов электронной почты), работающих с доменными именами, плата сетевого управления по умолчанию добавит данное доменное имя, если будет введено только имя хост-узла.
 - Чтобы переопределить расширение указанного имени хоста посредством добавления имени домена, задайте в поле имени домена значение по умолчанию `somedomain.com` или значение `0.0.0.0`.
 - Чтобы изменить расширение *конкретного* имени хост-узла (например, при определении получателя прерываний), поставьте конечную точку. ПСУ распознает имя хост-узла с точкой (например, `mySnmpServer.`) как полноценное доменное имя и не добавляет доменное имя.
- **Имя домена (IPv6)**. Укажите доменное имя IPv6.

Экран проверки DNS

Путь: Конфигурация > Сеть > DNS > Тестирование

Данная функция используется для отправки запроса DNS, который проверяет настройку DNS-сервера путем поиска по IP-адресу. Процедуру настройки серверов см. в вышеприведенном разделе «Экран DNS».

Посмотрите результаты проверки в поле **Последний ответ на запрос**.

- Для параметра **Тип запроса** укажите метод использования запросов DNS; см. следующую таблицу.
- В поле **Вопрос в запросе** укажите значение, которое будет использоваться для выбранного типа запроса в соответствии с данными таблицы.

Выбранный тип запроса	Используемый запрос
по хосту	Имя хоста, URL
по полному доменному имени	Полное доменное имя вида мой_сервер.мой_домен.com
по IP-адресу	IP-адрес сервера
по MX	Адрес Mail Exchange

Экран веб-доступа

Путь: Конфигурация > Сеть > WWW > Доступ

Данная функция используется для настройки метода доступа к веб-интерфейсу. (Для активации любых изменений, выполненных в этом разделе, потребуется перезагрузить ПСУ. См. раздел «Сеть» в меню управления» на стр. 23.)

С помощью флажков «Включить» можно включить доступ к интерфейсу пользователя по протоколу **HTTP** или **HTTPS** (или по обоим протоколам). Протокол HTTP отключен по умолчанию, а протокол HTTPS включен по умолчанию. Протокол HTTP не выполняет шифрование.

HTTPS также выполняет аутентификацию ПСУ с помощью цифрового сертификата. Описание различных способов использования цифровых сертификатов см. в разделе «Создание и установка цифровых сертификатов» в *Руководстве по безопасности* на [веб-сайте APC](#).

Для дополнительной безопасности для параметра **порты** можно изменить значение, указав любой неиспользуемый порт в диапазоне 5000–32768. Необходимо использовать двоеточие (:) в адресном поле браузера для указания номера порта. Например, для номера порта 5000 и IP-адреса 152.214.12.114:

```
http(s)://152.214.12.114:5000
```

Веб-экран сертификата SSL

Путь: Конфигурация > Сеть > WWW > SSL-сертификат

Добавление, замена и удаление сертификатов безопасности. SSL (Secure Socket Layer) — это протокол, используемый для шифрования данных, передаваемых между браузером и веб-сервером.

Могут использоваться следующие значения параметра **Состояние**:

- **Годный сертификат.** Платой сетевого управления был установлен или создан действительный сертификат. Щелкните эту ссылку, чтобы увидеть содержимое сертификата.
- **Сертификат не установлен.** 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 ПСУ.
- **Создание.** Плата сетевого управления создает сертификат, поскольку не обнаружен действующий сертификат.
- **Загрузка.** Выполняется активация сертификата на плате сетевого управления.



Если был установлен недействительный сертификат или сертификат не был загружен при включенном SSL, плата сетевого управления создает 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.

Добавить или заменить файл сертификата. Найдите файл сертификата, созданный с помощью мастера безопасности. Для выбора метода использования цифровых сертификатов, созданных мастером безопасности или сгенерированных ПСУ, см. раздел «Создание и установка цифровых сертификатов» в *Руководстве по безопасности* на [веб-сайте APC](#).

Удалить. Удаление сертификата. См. также текст на экране.

Экран консоли

Путь: Конфигурация > Сеть > Консоль > Доступ

Путь: Конфигурация > Сеть > Консоль > Ключ хоста SSH

Доступ к консоли. Для обновления микропрограммы ИБП потребуется включить доступ к консоли; см. раздел «Экран «Обновление прошивки»». Доступ к консоли позволяет использовать интерфейс командной строки.

С помощью флажков «Включить» можно включить доступ к интерфейсу командной строки по протоколу **Telnet** или **SSH** (или по обоим протоколам). Протокол Telnet отключен по умолчанию, а протокол SSH включен по умолчанию. Telnet не шифрует имена пользователей, пароли и данные во время передачи, а протокол SSH выполняет шифрование.

Примечание. При включении SSH включается также SCP (SeCure CoPy) для защищенной передачи файлов. Дополнительную информацию об использовании SCP см. в разделе «Передача файлов».

Для параметра **порты**, который будет использоваться для связи с ПСУ, можно присвоить любой свободный порт в диапазоне 5000–32768 для обеспечения дополнительной защиты.

- **Порт Telnet.** По умолчанию имеет значение 23. 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:

```
telnet 152.214.12.114:5000 или telnet 152.214.12.114 5000
```

- **Порт SSH.** По умолчанию имеет значение 22. Формат командной строки, необходимый для задания не используемого по умолчанию порта, приведен в документации программы-клиента SSH. См. также «Ключ хоста SSH» далее.

Ключ хоста SSH. При использовании протокола SSH (Secure Shell Protocol) для доступа к консоли можно добавлять, заменять или удалять ключ хоста на экране «Ключ хоста SSL».

Состояние указывает, является ли ключ хоста (секретный ключ) действительным. Могут использоваться следующие значения параметра «Состояние»:

- **SSH выключено:** отсутствуют используемые ключи хоста.
- **Создание.** Плата сетевого управления создает ключ хоста, поскольку не было найдено ни одного действующего ключа.
- **Загрузка.** Выполняется активация ключа хоста на плате сетевого управления.
- **Допустимая.** Один из следующих допустимых ключей хоста находится в каталоге `/ssh` (рекомендуемое местоположение на плате сетевого управления):
 - 1024- или 2048-разрядный ключ хоста, созданный мастером настройки безопасности
 - 2048-разрядный ключ хоста RSA, созданный платой сетевого управления.

Добавить или заменить ключ хоста. Загрузите файл ключа хоста, созданного мастером настройки безопасности. Информацию об использовании мастера безопасности см. в руководстве по безопасности на [веб-сайте APC](#). Чтобы использовать внешний ключ хоста, загрузите его перед включением (см. раздел «Доступ к консоли» выше).

Примечание. Чтобы сократить время, необходимое для включения SSH, создайте и загрузите ключ хоста заблаговременно. *Если включить SSH, не загрузив ключ хоста, плата сетевого управления потратит примерно минуту для создания ключа, а сервер SSH будет в это время недоступен.*

Удалить. Удаление ключа хоста. См. также текст на экране.

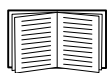


Чтобы использовать SSH, необходимо иметь установленный клиент SSH. Большинство платформ Linux и UNIX имеют в своем составе клиент SSH, но в операционных системах Microsoft Windows он отсутствует (за исключением Windows 10). Доступны клиентские программы Windows различных разработчиков, например программа PuTTY, доступная по адресу www.putty.org.

Экраны SNMP

Все имена, пароли и имена сообществ для SNMP передаются по сети в виде обычного текста. Если сеть требует высокую степень безопасности шифрования, отключите доступ SNMP или установите для каждого из сообществ права доступа на чтение. (Сообщество с доступом на чтение может получать информацию о статусе и использовать прерывания SNMP).

При использовании средства **StruxureWare Data Center Expert** для управления ИБП в открытой сети системы StruxureWare *необходимо* включить SNMPv1 или SNMPv3 в интерфейсе ПСУ. Доступ на чтение позволяет устройству StruxureWare получать прерывания от ПСУ, а доступ на запись необходим при работе с интерфейсом пользователя ПСУ для использования устройства StruxureWare в качестве получателя прерываний.



Дополнительную информацию по управлению безопасностью системы см. в *Руководстве по безопасности* на [веб-сайте APC](#).

SNMPv1.

Путь: Конфигурация > Сеть > SNMPv1 > Доступ и Контроль доступа

Параметр **Доступ** используется для включения или выключения SNMP версии 1 как метода взаимодействия с ПСУ.



По умолчанию SNMPv1 отключен. Необходимо определить имя сообщества **Community Name** до того, как будет установлена связь с протоколом SNMPv1.



Использование SNMPv2c поддерживается с помощью функций SNMPv1.

Контроль доступа. Можно настроить до четырех записей контроля доступа, чтобы определить, какая из сетевых систем управления (NMS) имеет доступ к ПСУ. Для редактирования щелкните имя сообщества.

По умолчанию одна запись назначается на каждое из четырех доступных сообществ SNMPv1. Вы можете изменять эти настройки, чтобы применить *более одной записи для любого сообщества*, для предоставления доступа по нескольким определенным адресам IPv4 и IPv6, именам хостов или маскам IP-адресов.

- По умолчанию сообщество имеет доступ к ПСУ из любого места в сети.
- При настройке нескольких записей управления доступом для сообщества с любым именем это значит, что одно или несколько сообществ имеет доступ к устройству.

Имя сообщества. Имя, которое система управления сетью (Network Management Station — NMS) должна использовать для доступа к сообществу. Максимальная длина — 16 символов в формате ASCII.

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 (например, 149.225.12.1) открывает доступ только системе NMS в данном сегменте сети. IP-адреса, содержащие 255, ограничивают доступ следующим образом:

- 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.

Тип доступа. Действия, которые может выполнять NMS в сообществе.

- **Чтение.** Только операции GET, в любое время.
- **Запись.** Получать (GET) в любое время и размещать (SET) информацию, если другие пользователи не работают в интерфейсе пользователя 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: Конфигурация > Сеть > SNMPv3 > Доступ, Профили пользователей и Контроль доступа

Для запросов GET и SET и получателей 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.



До умолчанию протокол SNMPv3 отключен. Необходимо активировать действительный профиль пользователя, используя парольные фразы (**Authentication Passphrase, Privacy Passphrase**) до того, как будет установлена связь с протоколом SNMPv3.



Для использования SNMPv3 необходимо иметь программу MIB с поддержкой SNMPv3. ПСУ поддерживает аутентификацию SHA или MD5, а также защиту с помощью AES или DES (шифрование).

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

Параметр Включить доступ к SNMPv3 позволяет использовать данный метод взаимодействия с устройством.

Профили пользователей. По умолчанию отображает список настроек для четырех профилей пользователей с именами от **arc snmp profile1** до **arc snmp profile4**, не использующих аутентификацию и защиту (шифрование). Чтобы изменить следующие настройки пользовательского профиля, щелкните имя пользователя в указанном списке.

- **Имя пользователя.** Идентификатор профиля пользователя. SNMP версии 3 отображает функции GET, SET и обеспечивает захват в пользовательский профиль путем сопоставления имени пользователя профиля с именем пользователя в передаваемом пакете данных. Имя пользователя может содержать до 32 символов ASCII.
- **Парольная фраза аутентификации.** Фраза из 15–32 символов ASCII, проверяющая взаимодействие системы NMS с устройством по протоколу SNMPv3, должна быть установлена в системе NMS. Она также проверяет, чтобы сообщение не менялось во время передачи, а также связь с сообщением периодически поддерживалась. Это позволяет узнать, что сообщение не задержано и не было скопировано и повторно отправлено в несоответствующее время.
- **Конфиденциальная парольная фраза.** Фраза из 15–32 символов ASCII, которая обеспечивает конфиденциальность данных, отправляемых системой NMS на данное устройство или принимаемых от данного устройства через SNMPv3.
- **Протокол аутентификации.** Протокол SNMPv3, поддерживающий аутентификацию SHA и MD5. Должно быть выбрано одно из этих значений.
- **Протокол конфиденциальности.** Протокол SNMPv3, поддерживающий в качестве протоколов шифрования и дешифрования данных протоколы AES и DES. Необходимо использовать как протокол конфиденциальности, так и пароль конфиденциальности, в противном случае запрос SNMP не будет зашифрован.

Однако нельзя выбрать протокол конфиденциальности, если не выбран протокол аутентификации.

Контроль доступа. Можно настроить до четырех записей контроля доступа, чтобы определить, какая из сетевых систем управления (NMS) имеет доступ к ПСУ. Для редактирования щелкните имя пользователя.

По умолчанию одна запись назначается на каждый из четырех профилей пользователей. Вы можете изменять эти настройки, чтобы применить *более одной записи для профиля пользователя*, для предоставления доступа по нескольким определенным IP-адресам, именам хостов или маскам IP-адресов.

- По умолчанию все системы NMS, использующие этот профиль, имеют доступ к этому устройству.
- При настройке нескольких записей управления доступом для одного профиля пользователя это значит, что один или несколько других профилей пользователей должны иметь доступ к устройству.

Имя пользователя. В раскрывающемся списке выберите профиль пользователя, для которого будет применена данная запись управления доступом. Для выбора доступны четыре имени пользователя, настроенных с помощью функции «Профили пользователей».

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 (например, 149.225.12.1) открывает доступ только системе NMS в данном сегменте сети. Маска IP-адреса, которая содержит число 255, ограничивает доступ следующим образом:

- 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.

Экраны Modbus

Используйте параметры Modbus, чтобы настроить ПСУ на использование протокола Modbus для подключения системы диспетчеризации инженерного оборудования (Building Management System — BMS). Плата ПСУ AP9640 поддерживает интерфейс Modbus TCP, а платы ПСУ AP9641 и AP9643 поддерживают последовательный интерфейс Modbus.



Дополнительную информацию об использовании протокола Modbus на ПСУ, см. в *Дополнительной документации по протоколу Modbus и Картах регистров протокола Modbus*, которые доступны на [веб-сайте APC](#).

Для получения информации об управлении группой переключаемых розеток с помощью Modbus для моделей Smart-UPS с префиксами SMT, SMX, SURTD, SRC и SRT обратитесь к [Рекомендации по применению № 177](#), доступной на веб-сайте APC.



ПРИМЕЧАНИЕ. Датчики температуры и влажности, подключаемые к универсальным портам ввода-вывода ПСУ AP9641 и AP9643, не поддерживаются при использовании Modbus.

Последовательный порт Modbus (только AP9641 или AP9643).

Путь: Конфигурация > Сеть > Modbus > Последовательный порт

1. Параметр **Доступ** используется для включения или выключения последовательного порта Modbus как метода взаимодействия с ПСУ.
2. Задайте параметры подключения по последовательному порту Modbus:
 - **Скорость передачи** — скорость передачи данных в битах в секунду. Можно задать значение 9600 (по умолчанию) или 19200.
 - **Бит четности** — бит для проверки четности. Можно установить значение «Четный», «Нечетный» или «Нет».
 - **Целевой уникальный идентификатор** — уникальный идентификатор целевого устройства. Можно установить значение от 1 до 247.
3. Щелкните «Применить», чтобы сохранить изменения.

Modbus TCP.

Путь: Конфигурация > Сеть > Modbus > TCP

1. Параметр **Доступ** используется для включения или выключения протокола Modbus TCP как метода взаимодействия с ПСУ.
2. Задайте номер **порта** для соединения TCP. Можно установить значение 502 (по умолчанию) или значение от 5000 до 32768.
3. Щелкните «Применить», чтобы сохранить изменения.

Экран ВАСnet

Используйте параметры ВАСnet, чтобы настроить ПСУ на использование протокола ВАСnet для предоставления данных об ИБП системе автоматизированного управления зданием.



Дополнительные сведения о точках данных ИБП, предоставляемых посредством ВАСnet, см. в документах ВАСnet Application Maps (Карты реализации ВАСnet) на веб-сайте APC www.apc.com.

Конфигурация VASnet

Параметр	Описание
Доступ	Установите этот флажок, чтобы включить VASnet. В противном случае к ПСУ нельзя будет обратиться через VASnet. По умолчанию VASnet отключен. ПРИМЕЧАНИЕ. Невозможно активировать протокол VASnet, пока не установлен пароль для управления связью с устройством Device Communication Control Password .
ID устройства	Уникальный идентификатор для устройства VASnet, используемый для обращения к нему. Допустимый диапазон: 0–4194303.
Имя устройства	Имя данного устройства VASnet, которое должно быть уникальным в рамках сети VASnet. По умолчанию для устройства используется имя в формате «VACn+последние восемь цифр MAC-адреса ПСУ». Минимальная длина равна 1 символу, максимальная — 150, при этом разрешено использовать специальные символы.
Сетевой протокол	Выберите нужный протокол: <ul style="list-style-type: none"> • VASnet/IP
Время ожидания APDU	Срок в миллисекундах, в течение которого ПСУ ожидает ответ на запрос VASnet. Допустимый диапазон: 1000–30000. Стандартное значение — 6000.
Повторные попытки APDU	Число повторных попыток выполнить запрос VASnet, предпринимаемых ПСУ, прежде чем запрос будет прерван. Допустимый диапазон: 1–10. Стандартное значение — 3.
Пароль Device Communication Control	Служба Device Communication Control используется клиентом VASnet, чтобы дать команду удаленному устройству (например, ПСУ с поддержкой VASnet) прекратить отправлять запросы APDU или отвечать на них (кроме относящихся к службе Device Communication Control) в течение заданного периода. Эту службу можно использовать для диагностики. Укажите пароль Device Communication Control, чтобы клиент VASnet не мог управлять взаимодействием с ПСУ через VASnet, не предоставив заданный здесь пароль. Этот пароль должен иметь длину от 8 до 20 символов и содержать следующее: <ul style="list-style-type: none"> • Число • Символ в верхнем регистре. • Символ в нижнем регистре. • Специальный символ. Рекомендуется изменить пароль при первом включении VASnet. Для этого знать текущий пароль не требуется.

VASnet/IP

Параметр	Описание
Локальный порт	Порт UDP/IP, используемый ПСУ для отправки и получения сообщений VASnet/IP. Допустимый диапазон: 5000–65535. Настройка по умолчанию: 47808. Примечание. Адрес ПСУ с поддержкой VASnet/IP определяется в виде IP-адреса ПСУ и локального порта.

Параметр	Описание
<p>Включить регистрацию сторонних устройств</p>	<p>Установите этот флажок, чтобы зарегистрировать ПСУ на устройстве управления ширококешением VASnet (BBMD).</p> <p>Примечание. Вам нужно зарегистрировать ПСУ в качестве стороннего устройства на устройстве BBMD, если в подсети ПСУ сейчас нет устройства BBMD либо ПСУ использует другой локальный порт для BBMD.</p> <p>В приведенном выше примере:</p> <ul style="list-style-type: none"> • BBMD A управляет ширококешательными сообщениями на ПСУ V и W. • BBMD B управляет ширококешательными сообщениями на ПСУ X и Y. • Только ПСУ Z нужно зарегистрировать на устройстве BBMD A или B в качестве стороннего устройства, так как в ее подсети нет BBMD. • После регистрации ПСУ Z может принимать ширококешательные сообщения от BBMD, на котором она зарегистрирована, а также отправлять на него сообщения, которые BBMD транслирует на все устройства в своей подсети, а также на другие устройства BBMD в сети через IP-маршрутизатор.
<p>Статус</p>	<p>Статус регистрации стороннего устройства (FDR):</p> <ul style="list-style-type: none"> • Регистрация сторонних устройств неактивна FDR является неактивной в следующих случаях: <ul style="list-style-type: none"> – FDR включена, а VASnet отключен. – FDR отключена, а VASnet включен. – FDR и VASnet отключены. • Регистрация выполнена Регистрация FDR успешно выполнена. • Регистрация отклонена Регистрация FDR завершена с ошибкой. ПСУ автоматически повторит попытку регистрации, но можно установить флажок Включить регистрацию сторонних устройств, чтобы ПСУ повторила попытку регистрации. • Регистрация отправлена Запрос FDR отправлен, но еще не выполнен.
<p>Устройство управления ширококешением VASnet/IP</p>	<p>IP-адрес или полное доменное имя устройства управления ширококешением VASnet, с которым будет зарегистрирована данная ПСУ.</p>
<p>Порт</p>	<p>Порт устройства BBMD, с которым будет зарегистрирована эта ПСУ.</p>

Параметр	Описание
Срок жизни	Период в секундах, в течение которого VBMД будет считать данную ПСУ зарегистрированным устройством. Если ПСУ не повторит регистрацию до истечения этого срока, VBMД удалит ее из своей таблицы сторонних устройств, после чего ПСУ не сможет отправлять или принимать широкоэвчателъные сообщения через это устройство VBMД. Данный параметр определяет, как часто ПСУ регистрируется на устройстве VBMД, так как ПСУ попытается повторить регистрацию до истечения этого срока.

Экран сервера FTP

Путь: Конфигурация > Сеть > Сервер FTP

Используйте этот экран для разрешения доступа к серверу FTP и определения порта.

Параметр	Описание
Доступ	Сервер FTP передает файлы без шифрования. По умолчанию протокол FTP отключен. Для шифрованной передачи файлов используйте защищенный протокол копирования Secure CoPy (SCP). Протокол SCP (с помощью протокола SSH) включен по умолчанию. Однако передача файлов будет невозможна, пока не изменен пароль суперпользователя (арс), установленный по умолчанию. ПРИМЕЧАНИЕ. В любое время, когда потребуется доступ к устройству через StruxureWare Data Center Expert или Operations, сервер FTP должен быть разрешен в настройках платы сетевого управления данного ИБП. Дополнительную информацию по управлению безопасностью системы см. в <i>Руководстве по безопасности</i> на веб-сайте APC .
Порт	Порт TCP/IP сервера FTP (по умолчанию 21). Сервер FTP использует как указанный порт, так и порт с номером на единицу меньше. Разрешенные, не установленные по умолчанию номера портов указаны на экране: 21 и 5001–32768. Примечание. Использование в настройках сервера FTP порта, не заданного по умолчанию, усиливает защиту, поскольку заставляет пользователей добавлять имя порта к адресу IP в командной строке FTP. Перед добавленным именем порта должен быть пробел или двоеточие, в зависимости от используемого клиента FTP.

Экран Wi-Fi (только AP9641 и AP9643)

Путь: Конфигурация > Сеть > Wi-Fi



ПРИМЕЧАНИЕ. Данный экран актуален, когда дополнительное устройство APC USB Wi-Fi (AP9834) вставляется в USB-порт платы AP9641/AP9643.



ВАЖНО: Не рекомендуется загружать целый файл config.ini, взятый с устройства с проводным соединением, на устройство, подключенное по Wi-Fi. Также не рекомендуется загружать целый файл config.ini, взятый с устройства, подключенного по Wi-Fi, на устройство с проводным соединением, если только весь раздел [NetworkWiFi] не будет удален или закомментирован с помощью точки с запятой (например, ;WiFi = enabled). Раздел [NetworkWiFi] содержит настройки устройства, специфичные для использования Wi-Fi. Эти настройки не следует выгружать на устройство с проводным соединением.

Используйте данный экран для просмотра текущего состояния сети Wi-Fi, включения/отключения Wi-Fi и изменения настроек сети Wi-Fi.



ПРИМЕЧАНИЕ. Включение/отключение Wi-Fi отключит/включит проводное соединение по локальной сети. ПСУ 3 будет перезагружена после внесения настроек Wi-Fi. После перезагрузки проводная сеть будет отключена и ПСУ 3 попытается подключиться к данному **сетевому имени (SSID)**.

Сетевое имя (SSID). Укажите сетевое имя (SSID) сети Wi-Fi. Максимальная длина — 32 символа.

Тип безопасности. Укажите тип безопасности сети Wi-Fi и предоставьте сведения для аутентификации.

Параметр	Описание
WPA	Пароль Wi-Fi. Укажите пароль для сети Wi-Fi. Максимальная длина — 64 символа.
WPA2-AES	
WPA2-Mixed	
WPA2-TKIP	
WPA2-Enterprise	<ul style="list-style-type: none">• Имя пользователя. Имя пользователя для аутентификации в среде WPA2-Enterprise. Максимальная длина — 32 символа.• Пароль. Пароль для аутентификации в среде WPA2-Enterprise. Максимальная длина — 32 символа.• Внешняя идентификация. Укажите внешнюю идентификацию WPA-2-Enterprise. Это дополнительная нешифрованная идентификация, используемая сервером WPA-2-Enterprise. Например: user@example.com или анонимно. Максимальная длина — 32 символа.



Для получения информации о порядке обновления прошивки устройства APC USB Wi-Fi (AP9834) см. команду `wifi` в [руководстве по интерфейсу командной строки \(CLI\) центра управления сетью NMC 3](#).

Порядок устранения неполадок при подключении к устройству APC USB Wi-Fi (AP9834) и описание светодиодов устройства — см. раздел «Неисправности аппаратного ключа устройства APC USB Wi-Fi (AP9834)».

Меню уведомлений

См. следующие разделы:

- «Типы уведомлений»
- «Конфигурирование действий для событий»
- «Экран уведомлений по электронной почте»
- «Экран тестирования прерываний SNMP»
- «Экран получателей системных прерываний SNMP»

Типы уведомлений

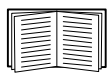
Можно настроить действия уведомления при возникновении определенного события. Можно уведомлять пользователя о событии любым из указанных способов:

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



Можно также регистрировать данные о работе системы с целью использования этих данных для контроля работы устройств. См. раздел «Журнал данных» для ознакомления с настройкой и использованием функции регистрации данных.

– Запросы (SNMP GET)



Дополнительные сведения см. в разделах «Экран получателей системных прерываний SNMP» и «Экран тестирования прерываний SNMP». Протокол SNMP позволяет NMS выполнять информационные запросы. При использовании протокола SNMPv1, который не осуществляет шифрования данных перед передачей, настройка 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 получателя прерываний см. в разделе «Экран получателей системных прерываний SNMP». Группа из трех событий **1628 MIB** совместима только с этой базой управляющей информации, не с альтернативной базой Powernet MIB. Они могут быть настроены, как любое другое событие (см. «Конфигурирование действий для событий» ниже).

Конфигурирование действий для событий

Конфигурация по событию.

Путь: Конфигурация > Уведомление > Действия для событий > По событию

По умолчанию протоколирование настроено для всех событий. Для определения ответных действий на отдельное событие:

1. Выберите меню **Конфигурация**, затем **Уведомление**, **Действия для событий** и **По событию**.
2. Чтобы найти событие, щелкните заголовок столбца для просмотра списков категории **События, связанные с питанием**, **События в окружающей среде** или **События в системе**.

Можно также выбрать подкатегорию под данными заголовками, например **Состояние входной линии** или **Температура**.

3. Для просмотра и изменения текущих настроек, таких как адресаты, оповещаемые по электронной почте, или системы управления сетями (NMS), получающие оповещения путем прерываний SNMP, щелкните имя события. См. раздел «Параметры уведомлений». Установите флажок **Журнал событий**, чтобы включить или выключить запись журнала событий для этого события.



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



Просматривая параметры конфигурации события, можно включить или отключить регистрацию событий или журнал Syslog, либо отключить отправку уведомления определенным получателям электронной почты или приемникам прерываний, но добавить или удалить получателей и устройства-приемники нельзя. Чтобы добавить или удалить адресатов или устройства-приемники, посмотрите следующее.

- «Идентификация серверов Syslog»
- «Получатели электронной почты»
- «Получатели прерываний»

Конфигурирование по группам событий.

Путь: Конфигурация > Уведомление > Действия для событий > По группе

Порядок одновременной настройки группы событий:

1. Выберите меню **Конфигурация**, затем **Уведомление**, **Действия для событий** и **По группе**.
2. Выберите, каким образом группировать события для конфигурации:
 - Выберите пункт **События по степени опасности**, после чего выберите один или несколько уровней опасности. Изменять уровень опасности события нельзя.

- Выберите пункт **События по категории**, после чего выберите все события одной или нескольких предварительно заданных категорий.
3. Для перехода к другому экрану щелкните «Далее». Выполните следующие действия:
- а. Выберите действия по событиям для группы событий.
 - Чтобы выбрать любое из действий, за исключением действия **Ведение журнала** (по умолчанию), для начала необходимо иметь, как минимум, одного сконфигурированного действительного получателя или одно устройство-приемник.
 - При выборе параметра **Ведение журнала** и настройке сервера Syslog на следующем экране выберите **Журнал событий** или Syslog (или оба журнала). (См. раздел «Журналы в меню конфигурации».)
 - б. Укажите, нужно ли сохранить новое сконфигурированное действие по событию для группы событий или отключить данное действие.

См. следующий раздел «Параметры уведомлений».

Параметры уведомлений. Эти настраиваемые поля определяют параметры отправки уведомлений по событиям. См. разделы «Конфигурация по событию» и «Конфигурирование по группам событий».

Как правило, для доступа к ним нужно щелкнуть приемник или имя получателя.

Поле	Описание
Задержка уведомления	Если событие сохраняется в течение указанного промежутка времени, посылается уведомление. Если данное условие исчезает до того, как истек заданный интервал времени, уведомление не посылается.
Интервал повтора	Уведомление периодически отправляется с указанным интервалом (по умолчанию каждые 2 минуты до очистки условия).
Количество уведомлений после начального	Пока событие действует, уведомление будет повторено указанное число раз.
или	
Уведомлять до устранения условия возникновения	Уведомление посылается регулярно до тех пор, пока условие не устранится или не будет урегулировано.

Эти параметры можно также установить для событий, ассоциированных с очисткой события. (Пример события с очисткой ИБП: разорвана связь с блоками батарей и ИБП: восстановлена связь с блоками батарей).

Экран уведомлений по электронной почте

Обзор установки. 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 (необязательно) вторичного сервера доменных имен (DNS). (См. раздел «Экран DNS»)
- IP-адрес или имя DNS для параметров **Сервер SMTP** и **Адрес отправителя**. (См. раздел «Сервер SMTP» далее)
- Адреса электронной почты для четырех получателей (максимум). (См. раздел «Получатели электронной почты»)



Можно использовать значение **Адрес получателя** параметра **получатели** для отправки электронной почты на текстовый экран.

Сервер SMTP.

Путь: Конфигурация > Уведомление > Электронная почта > Сервер

На этом экране указаны первичный и вторичный серверы (см. раздел «Экран DNS») и следующие поля:

Поле	Описание
Конфигурация исходящей почты	
Адрес отправителя	Содержание поля От в сообщениях электронной почты отправляется ПСУ: <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 Локальный сервер SMTP) в сообщениях электронной почты. Примечание. Локальный SMTP-сервер может потребовать учетную запись сервера для задания данной настройки. См. документацию сервера.
Сервер SMTP	Адрес IPv4/ IPv6 или имя DNS локального сервера SMTP. Примечание. Этот параметр требуется определять только в том случае, если для параметра Сервер SMTP установлено значение Локальный . См. раздел «Получатели электронной почты»
Аутентификация	Включите этот параметр, если сервер SMTP требует аутентификации.
Порт	Порт SMTP по умолчанию — 25. Альтернативные порты: 465, 587, 2525, 5000–32768.
Имя пользователя/ Пароль/ Подтвердить пароль	Если почтовый сервер требует аутентификации, укажите здесь имя пользователя и пароль. Таким способом будет выполняться простейшая аутентификация, но не SSI.
Дополнительно	
Использовать SSL/TLS	<ul style="list-style-type: none"> • Никогда. Сервер SMTP не требует и не поддерживает шифрование. • Если поддерживается. Сервер SMTP объявляет о поддержке STARTTLS, но <i>не</i> требует зашифрованного соединения. Команда STARTTLS отправляется после подачи объявления. • Всегда. Сервер SMTP при установлении соединения требует отправки команды STARTTLS. • Неявно. Сервер SMTP принимает только зашифрованные соединения. Сообщение STARTTLS не отправляется на сервер.
Необходим корневой сертификат сертификационного органа	Этот параметр нужно включить только в том случае, если политика защиты организации не разрешает устанавливать явные доверенные соединения SSL. Если этот параметр включен, действительный корневой сертификат сертифицирующего органа должен быть загружен в ПСУ для шифрования отправляемых сообщений электронной почты.
Имя файла	Данное поле зависит от корневого сертификата сертифицирующего органа, установленного на ПСУ, а также от того, требуется ли корневой сертификат сертифицирующего органа.

Получатели электронной почты.

Путь: Конфигурация > Уведомление > Электронная почта > Получатели

Укажите до четырех получателей электронной почты. Для настройки параметров щелкните имя. См. также раздел «Сервер SMTP», приведенный выше.

Поле	Описание
Создание сообщения электронной почты	Включает (по умолчанию) или отключает отправку электронной почты получателю.

Поле	Описание
Адрес получателя	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). Сообщение будет генерировать шлюз пейджера. Чтобы обойти поиск DNS 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. Примечание. Пейджер получателя должен поддерживать работу с текстовыми сообщениями.
Формат	Длинный формат содержит имя, расположение, контакт, IP-адрес, серийный номер устройства, дату и время, код и описание события. Короткий формат содержит только описание события.
Язык	Выберите язык в раскрывающемся списке. Все письма будут отправляться на указанном языке. Можно использовать различные языки для разных пользователей. См. раздел «Смена языка интерфейса пользователя».
Сервер	Выберите один из следующих способов доставки электронной почты: <ul style="list-style-type: none"> • Локальный. С использованием локального сервера SMTP. Этот рекомендуемый параметр обеспечивает отправку электронной почты с помощью локального сервера SMTP. Выбор этого параметра ограничивает задержки, отказы сети и повторную отправку электронной почты. При выборе локального значения необходимо также включить пересылку на сервере SMTP устройства и настроить специальную внешнюю учетную запись для получения пересылаемой электронной почты. Перед внесением этих изменений обратитесь к администратору сервера SMTP. • Получатель. С использованием SMTP-сервера получателя. ПСУ выполняет поиск записи MX в адресе электронной почты получателя и использует полученную информацию в качестве сервера SMTP. Сообщение электронной почты отправляется только один раз, поэтому оно может быть потеряно. • Пользовательский. Данный параметр позволяет каждому получателю электронной почты иметь собственные настройки сервера. Эти настройки зависят от процедуры в вышеприведенном разделе «Сервер SMTP».

Сертификаты SSL электронной почты.

Путь: Конфигурация > Уведомление > Электронная почта > Сертификаты SSL

Загрузка сертификата SSL электронной почты на ПСУ обеспечивает дополнительную защиту. Файл должен иметь расширение .crt или .cer. В любой момент можно загрузить до пяти файлов.

После установки сведения о сертификате отображаются в этой области. Для недопустимого сертификата во всех полях, за исключением имени файла, отображается значение «н/д».

На этом экране можно удалить сертификаты. Любые получатели электронной почты, использующие сертификат, должны быть вручную изменены для удаления ссылки на данный сертификат.

Тестирование электронной почты.

Путь: Конфигурация > Уведомление > Электронная почта > Тестирование

Посылает тестовое сообщение указанному получателю.

Экран получателей системных прерываний SNMP

Получатели прерываний.

Путь: Конфигурация > Уведомление > Прерывания SNMP > Получатели прерываний

С помощью прерывания простого протокола управления сетью (SNMP) можно получать автоматические уведомления о важных событиях ИБП. Это средство используется для мониторинга устройств в сети.

Получатели прерываний отображаются по значению **Имя IP-адреса/хоста NMS**, где NMS означает сетевую систему управления. Можно настроить до шести получателей прерываний.

Чтобы сконфигурировать новый приемник прерываний, щелкните пункт **Добавить получатель прерываний**. Чтобы изменить или удалить одно из значений, щелкните его IP-адрес или имя хоста.

При удалении получателя прерываний всем параметрам оповещения, настроенным в разделе «Конфигурирование действий для событий» для удаляемого получателя прерываний, присваиваются значения по умолчанию.

Выберите переключатель **SNMPv1** или **SNMPv3**, чтобы указать тип прерывания. Чтобы система NMS могла получать *оба* типа прерываний, необходимо отдельно настроить для данной NMS двух получателей прерываний, по одному на каждый тип прерывания.

Поле	Описание
Создание системного прерывания	Включение (по умолчанию) или отключение создания прерывания для данного получателя прерываний.
Генерация прерываний Powernet MIB/ RFC1628	Выберите один из этих двух типов генерации прерываний для каждого создаваемого прерывания. Функция Powernet адаптирована для Schneider Electric и содержит множество дополнительных переменных в соответствии со спецификой продукции компании. RFC1628 — это общая стандартная база управляющей информации (MIB) для устройств ИБП. При использовании базы RFC1628 MIB также можно использовать три извещения о событиях RFC1628 (см. «Конфигурирование действий для событий»). Их использование позволяет избежать необходимости настройки извещений вне среды ПСУ, см. RFC1628 MIB .
Имя IP-адреса/хоста NMS	Адрес IPv4/ IPv6 или имя хост-узла данного приемника прерываний. Значение по умолчанию (0.0.0.0) оставляет получатель прерываний неопределенным.
Язык	Выберите язык в раскрывающемся списке. Он может отличаться от языка интерфейса пользователя и языков других получателей прерываний.
SNMPv1	Имя сообщества: имя, используемое в качестве идентификатора при отправке прерываний SNMPv1 на данный приемник. Аутентификация прерываний. Когда этот параметр включен (по умолчанию), система NMS, определенная с помощью имени хоста или IP-адреса, будет получать прерывания аутентификации (прерывания, сформированные недействительными попытками входа на этом устройстве).
SNMPv3	Имя пользователя: выберите идентификатор профиля пользователя для данного получателя прерываний. См. также «Профили пользователей» в разделе «Экраны SNMP».

Экран тестирования прерываний SNMP

Путь: Конфигурация > Уведомление > Прерывания SNMP > 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 получателем прерываний. Считается, что тест прерываний завершен успешно, если соблюдены все из перечисленных условий:

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

K. Выберите IP-адрес или имя хоста, для которого будет отправлено проверочное прерывание SNMP. Если получатель прерывания не настроен, отображается ссылка на экран конфигурации **Получатель прерываний**. См. вышеприведенный раздел «Экран получателей системных прерываний SNMP».

Меню «Общие»

В данном меню представлены различные элементы конфигурации, включая идентификацию устройства, дату и время, экспорт и импорт конфигурации ПСУ, три ссылки в нижней части экрана и обобщенные данные для поиска и устранения неисправностей.

Экран «Идентификация»

Путь: Конфигурация > Общие > Идентификация

Укажите значения для параметров **Имя** (имя системы ПСУ; см. раздел «Экран DNS»), **Расположение** (физическое расположение) и **Контакт** (ответственное лицо). Эти данные используются следующими компонентами:

- Агент SNMP платы сетевого управления
- StruxureWare Data Center Expert



Например, поле имени используется идентификаторами объектов (OID) **sysName**, **sysContact** и **sysLocation** в агенте SNMP платы сетевого управления. Дополнительную информацию об идентификаторах MIB-II OID см. в *Справочном руководстве к базе управления информацией (MIB) протокола PowerNet® SNMP* на [веб-сайте APC](#).

Экран даты и времени

Режим.

Путь: Конфигурация > Общие > Дата/время > Режим

Задаёт время и дату, используемые ПСУ. Вы можете изменить текущие настройки вручную или с помощью сервера протокола сетевого времени (Network Time Protocol — NTP):

При использовании обоих компонентов времени нужно выбрать **часовой пояс**. Это разница местного времени с универсальным координированным временем (UTC), которое также называется средним временем по Гринвичу (GMT).

- **Ручной режим.** Выполните одно из следующих действий:
 - Введите дату и время для ПСУ или
 - установите флажок **Применение локального времени ПК**, чтобы дата и время совпадали с компьютерными часами, и примените настройки.
- **Синхронизировать с сервером NTP.** Возможность для NTP-сервера (сетевой протокол службы времени) задавать дату и время ПСУ.



По умолчанию все ПСУ на пользовательской стороне StruxureWare Data Center Expert получают настройки времени, используя программу StruxureWare Data Center Expert в качестве сервера NTP.

Поле	Описание
Заблокировать ручные настройки NTP	При выборе этого параметра данные от других источников (как правило, DHCP) получают приоритет над указанными в этом разделе настройками NTP.
Первичный NTP-сервер	Введите IP-адрес или доменное имя первичного NTP-сервера.
Вторичный NTP-сервер	Введите IP-адрес или имя домена вторичного NTP-сервера при наличии такого сервера.
Интервал обновления	Укажите, как часто ПСУ будет получать доступ к серверу NTP для обновления. <i>Минимум: 1; Максимум: 8760 (1 год).</i>

Поле	Описание
Немедленное обновление данных при помощи NTP	Запускает моментальное обновление даты и времени по NTP-серверу.

Переход на летнее время.

Путь: Конфигурация > Общие > Дата/время > Переход на летнее время

По умолчанию переход на летнее время (DST) выключен. Можно включить традиционный переход на летнее время США (DST) или включить и настроить собственное поясное летнее время в соответствии с местными правилами установки летнего времени.

При настройке перехода на летнее время система переводит часы вперед на один час при наступлении времени и даты, указанных в поле **Пуск**, и на один час назад при наступлении времени и даты, указанных в поле **Завершить**.

- Если местное летнее время всегда начинается и заканчивается в *четвертый* день недели определенного месяца (например, в четвертое воскресенье), выберите параметр **Четвертый/последний**. Если в этом месяце наступает пятое воскресенье, необходимо также выбрать параметр **Четвертый/последний**.
- Если местное летнее время всегда начинается и заканчивается в *последний*, четвертый или пятый день недели определенного месяца, выберите параметр **Пятый/последний**.

Создание и импорт настроек с помощью файла конфигурации

Путь: Конфигурация > Общие > Файл конфигурации пользователя

С помощью этой функции можно ускорить и упростить конфигурацию новых устройств с помощью повторного использования существующих настроек. Параметр **Отправить** используется для передачи данных конфигурации в этот интерфейс, а параметр **Загрузить** используется для передачи данных из этого интерфейса (для последующего использования при настройке другого интерфейса). По умолчанию файл имеет имя **config.ini**.



Информацию о загрузке и изменении файла настроенной ПСУ см. в разделе «Экспорт параметров конфигурации».

Экран конфигурирования ссылок

Путь: Конфигурация > Общие > Быстрые ссылки

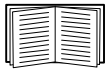
Данный параметр используется для просмотра и изменения ссылок URL, отображаемых в нижней левой части каждого экрана интерфейса.

Для изменения ссылки щелкните название ссылки в столбце **Имя**. Можно восстановить значения по умолчанию ссылок, щелкнув элемент **Восстановлены настройки по умолчанию**.

Журналы в меню конфигурации

Путь: Конфигурация > Журналы > Syslog > *параметры*

ПСУ 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: Конфигурация > Журналы > Syslog > Серверы

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

Настройки системного журнала

Путь: Конфигурация > Журналы > Syslog > Настройки

Поле	Описание
Создание сообщения	Включение формирования (и ведения журнала) сообщений Syslog для событий, которые настроены в Syslog в качестве метода уведомления. См. раздел «Конфигурирование действий для событий».
Код объекта	Выбирает код объекта, назначенный для сообщений системного журнала ПСУ (по умолчанию — Пользователь). Примечание. Параметр Пользователь лучше всего определяет настройки сообщений Syslog, посылаемых ПСУ. <i>Не</i> изменяйте эти настройки без рекомендации сети Syslog или администратора системы.

Поле	Описание
Сопоставление степени опасности	<p>Сопоставляет каждый уровень опасности событий ПСУ или среды с соответствующими приоритетами Syslog. Локальными параметрами являются: «Критическая», «Предупредительное» и «Информационная». Необходимости менять сопоставления нет.</p> <p>Следующие определения взяты из RFC3164:</p> <ul style="list-style-type: none"> • Аварийная ситуация: система непригодна к использованию. • Оповещение: требуется незамедлительное вмешательство. • Критическая: критические состояния. • Ошибка: состояния ошибки. • Предупредительное: состояния, требующие внимания. • Примечание: нормальный режим работы с серьезными состояниями. • Информационная: информационные сообщения. • Отладка: сообщения уровня отладки. <p>Далее приведены настройки, установленные по умолчанию для параметров Локальный приоритет:</p> <ul style="list-style-type: none"> • Параметр Критическая соответствует состоянию критическому состоянию. • Параметр Предупредительное соответствует предупреждениям. • Параметр Информационная соответствует информационным событиям. <p>Примечание. Информацию об отключении сообщений Syslog см. в разделе «Конфигурирование действий для событий».</p>

Пример теста и формата Syslog

Путь: Журналы > Syslog > Тестирование

Позволяет отправить тестовое сообщение на серверы Syslog (настроенные с помощью функции, описание которой приведено в разделе «Идентификация серверов Syslog»). Результат будет отправлен на все настроенные серверы Syslog.

Выберите важность, назначаемую тестовому сообщению, затем укажите тестовое сообщение. Включите в формат сообщения тип события (например: APC, система или устройство) с последующим двоеточием, пробелом и текстом события. Длина сообщения не должна превышать 50 символов.

- Приоритет (PRI). Приоритет Syslog, указанный для сообщаемого события, а также код объекта сообщений, отправляемых на ПСУ.
- Заголовок. Отметка времени и IP-адрес ПСУ.
- Тело сообщения (MSG).
 - Поле TAG, за которым следует двоеточие и пробел, определяет тип события.
 - Поле СОДЕРЖИМОЕ содержит текст события, за которым следует пробел и код события.

Пример. APC: Test Syslog является допустимым.

Меню «Тесты»

Тестирование и калибровка

Путь: Тесты > ИБП



Эта функция доступна не для всех ИБП.

На некоторых устройствах ИБП можно запустить самотестирование, тестирование сигналов тревоги или динамическую калибровку ИБП. В полях **Самодиагностика** и **Калибровка** отображаются результаты последнего теста и калибровки.

В ходе динамической калибровки ИБП пересчитывает доступное время работы в зависимости от текущей нагрузки. Это обеспечивает более высокую точность сообщаемого времени работы. Поскольку при калибровке существенно расходуется ресурс батарей ИБП, необходимо выполнять калибровку при 100% зарядке батарей. Чтобы гарантировать, что калибровка будет принята, нагрузка на ИБП должна составлять не менее 15% без колебаний.



Внимание! Динамическая калибровка глубоко разряжает батареи ИБП, вследствие чего ИБП может быть временно неспособен поддержать подключенное оборудование в случае прекращения подачи электропитания.

Частые калибровки сокращают срок службы батарей.

Выполняйте калибровку при каждом значительном увеличении нагрузки, поддерживаемой ИБП.

Тест сигналов тревоги для ИБП выполняется для конкретного устройства и может быть недоступен для используемого ИБП. Информацию о включении сигнала тревоги см. в разделе «Экран «ИБП: общее»».

- При выборе функции **Тестирование сигнала тревоги ИБП** ИБП подает звуковой сигнал в течение четырех секунд, и его светодиоды горят.
- При выборе функции **Тестирование сигнала тревоги ИБП: непрерывный** ИБП подает звуковой сигнал, а его светодиоды горят до отмены теста. На этом экране отображается отдельный пункт **Отменить тестирование непрерывного сигнала тревоги**. Чтобы отменить тест, выберите этот элемент и щелкните «Применить». Можно также нажать любую кнопку на интерфейсе ЖК-дисплея ИБП. Этот тест полезен для определения расположения ИБП.

Включение мигания светодиодов ПСУ

Путь: Тесты > Сеть > Светодиод мерцает

Если не удастся найти устройство ИБП, укажите количество минут в поле **Длительность мерцания светодиода**, щелкните «Применить», и светодиодные индикаторы на ПСУ начнут мигать. Это может помочь найти физическое устройство.

Меню «Журналы» и «О программе»

Использование журналов событий и данных

В журнал «Журнал событий» заносятся отдельные события. В журнале «Журнал данных» содержатся мгновенные снимки состояния системы, получаемые с помощью записи значений с регулярными интервалами.

Журнал событий

Путь: Журналы > События > *доступные параметры*

По умолчанию в журнале отображаются все события, записанные в течение последних двух дней, начиная с последних событий. См. раздел «Конфигурация по событию».


Кроме того, в журнал заносятся: i) любое событие, которое отправляет прерывание SNMP, кроме попыток аутентификации SNMP; ii) аномальные внутренние системные события.

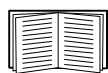
В разделе «Локальные пользователи» меню конфигурации можно включить цветовую кодировку событий.

Отображение журнала событий.

Путь: Журналы > События > Журнал

По умолчанию в журнале событий сначала отображаются последние события. Для просмотра списка событий на одной веб-странице щелкните кнопку **Запустить журнал в новом окне**. Для выполнения этой операции требуется, чтобы в настройках браузера был включен параметр JavaScript.

Чтобы открыть журнал в текстовом файле или сохранить его на диск, щелкните значок дискеты  в строке заголовка **Журнал событий**.



Для просмотра журнала событий можно также использовать FTP или Secure CoPy (SCP). См. раздел «Использование протокола FTP или SCP для получения файлов журнала».

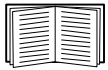
Фильтрация журнала событий. Чтобы не отображать лишнюю информацию в журнале, воспользуйтесь функцией фильтрации.

Фильтрация журнала по дате или по времени	Воспользуйтесь переключателями Последнее или С . (Настройка фильтра сохраняется до перезапуска ПСУ.)
Фильтрация журнала по серьезности или категориям событий	Щелкните Фильтровать журнал . Отмените установку флажка, чтобы отменить его отображение. После нажатия Применить текст в верхнем правом углу страницы журнала событий указывает на то, что фильтр включен. Фильтр активен до его очистки или перезапуска ПСУ. Для удаления активного фильтра щелкните Фильтровать журнал , затем Очистить фильтр (показать все) . В качестве администратора щелкните Сохранить как элемент по умолчанию , чтобы сохранить этот фильтр для отображения нового журнала по умолчанию для всех пользователей.

Важные замечания по фильтрам:

- События обрабатываются фильтром с помощью логического оператора ИЛИ. Работа фильтра не зависит от других фильтров.
- События, очищенные в списке **Фильтровать по степени опасности**, никогда не отображаются в отфильтрованном журнале событий, даже если они выбраны в списке **Фильтровать по категории**.
- Аналогично, события, очищенные в списке **Фильтровать по категории**, никогда не отображаются в отфильтрованном журнале событий.

Удаление журнала событий. Для удаления всех событий щелкните **Очистить журнал**. Поиск удаленных событий не выполняется.



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

Настройка обратного просмотра:

Путь: Журналы > События > Обратный просмотр

Если функция обратного просмотра включена, при возникновении событий, относящихся к сети, вместе с событием в журнал событий заносятся IP-адрес и имя домена сетевого устройства. Если в устройстве отсутствует запись имени домена, то в связи с событием в журнале регистрируется только IP-адрес.

Так как имена доменов, как правило, изменяются реже, чем IP-адреса, включение функции обратного просмотра может улучшить способность определения адресов сетевых устройств, вызвавших событие.

Обратный просмотр выключен по умолчанию. Не включайте эту функцию, если отсутствует настроенный сервер DNS или уменьшается скорость сети из-за плотного трафика.

Изменение размера журнала событий.

Путь: Журналы > События > Размер

Используйте параметр «Размер журнала событий», чтобы указать максимальное число записей журнала.



Внимание! При изменении размера журнала событий с целью указания максимального размера *все существующие записи удаляются*. Для того чтобы не потерять данные из журнала, используйте протокол FTP или SCP для получения журнала, см. раздел «Использование протокола FTP или SCP для получения файлов журнала». Если журнал достигает максимального размера, старые записи удаляются в последовательном порядке.

Журнал данных

Путь: Журналы > Данные > опции

Используйте функцию «Журнал данных» для отображения журнала измерений параметров ИБП, входа питания ИБП, а также температуры окружающей среды ИБП и батарей.

Действия для отображения и изменения размера журнала данных аналогичны действиям для журнала событий, за исключением того, что нужно использовать параметры меню **Данные** вместо **События**. См. разделы «Отображение журнала событий» и «Изменение размера журнала событий».

Для фильтрации журнала данных по дате или времени используйте переключатели **Последнее** или **С**. (Настройка фильтра сохраняется до перезапуска ПСУ.) Для удаления всех данных, записанных в журнале данных, щелкните **Очистить журнал данных**. Поиск удаленных данных не выполняется.

Установка интервала сбора данных (Журналы > Данные > Интервал). В настройках **Интервал журнала** определите частоту поиска данных в журнале. Если выбрать «Применить», число возможных дней хранения вычисляется повторно и отображается в верхней части экрана.

После того как журнал заполнен, начинается удаление самых старых записей. Чтобы избежать автоматического удаления старых данных, см. следующий раздел «Настройка обновления журнала данных (Журналы > Данные > Обновление)».

Примечание. Так как интервал определяет частоту записи данных, то *чем меньше интервал*, тем чаще записываются данные и тем больше файл журнала.

Настройка обновления журнала данных (Журналы > Данные > Обновление). Обновление вызывает добавление содержимого журнала данных к файлу с указанным именем и местоположением. Это значит, что можно сохранить данные перед их удалением; см. вышеприведенный раздел «Установка интервала сбора данных (Журналы > Данные > Интервал)».

Данная функция используется для установки защиты с помощью пароля и других параметров.

Поле	Описание
Сервер FTP	IP-адрес или имя хоста сервера, на котором находится файл.
Имя пользователя Пароль	Имя пользователя и пароль, необходимые для отправки данных в файл с архивом данных. Данный пользователь должен обладать правом доступа на чтение и запись данных для файла архива и для каталога (папки), в котором этот файл хранится.
Путь к файлу	Путь к файлу архива данных.
Имя файла	Имя файла архива данных (текстовый ASCII-файл), например <code>datalog.txt</code> . Все новые данные добавляются в этот файл, они не перезаписывают его.
Уникальное имя файла	Выберите этот флажок, чтобы сохранить журнал данных в формате <code>ммддгггг_<имя_файла>.txt</code> , где «имя_файла» — это значение, указанное в поле Имя файла . Все новые данные добавляются в файл, но каждый день создается новый файл.
Задержка <i>n</i> часов между загрузками.	Количество часов между загрузками данных в файл (максимум 24 часа).
После сбоя выполняйте загрузку каждые <i>n</i> минут(ы)	Количество минут между попытками загрузить данные в файл после сбоя загрузки.
до <i>n</i> раз	Максимальное количество попыток загрузки после исходного сбоя.
до успешного завершения загрузки	Попытка загрузки файла до завершения передачи.

Использование протокола FTP или SCP для получения файлов журнала

Администратор или пользователь устройства может использовать протокол SCP или FTP для получения файла журнала событий (*event.txt*) (с табуляциями в качестве разделителей) или файла журнала данных (*data.txt*) и импортирования его в электронную таблицу. Оба файла находятся на ПСУ.

- Файл содержит отчет обо всех событиях и данных с момента последнего удаления журнала или (в случае с журналом данных) усечения после достижения максимального размера.
- Этот файл включает в себя информацию, которая не отображается в файле журнала событий или в файле данных.
 - Версия AOS ПСУ и приложения.
 - Дата и время получения файла.
 - Значения **Имя**, **Контакт** и **Расположение**, а также IP-адрес ПСУ.
 - Название модели ИБП (только файл *data.txt*)
 - Уникальный **Код события** для каждого записанного события (только файл *event.txt*).
 - В ПСУ для записей журнала используется четырехзначная запись года. Можно выбрать четырехзначный формат даты в программе для работы с электронными таблицами для отображения всех четырех разрядов.



При использовании протоколов защиты на основе шифрования см. раздел «Использование SCP для поиска этих файлов». При использовании методов аутентификации с шифрованием для защиты см. раздел «Использование FTP для поиска файлов».



Для получения сведений о доступных протоколах и способах установки необходимой защиты см. [Руководство по безопасности](#) на [веб-сайте APC](#).

Использование SCP для поиска этих файлов. Включите SSH на ПСУ (см. раздел «Доступ к консоли»). **Примечание.** Следующие команды представлены только в качестве примеров.

Чтобы получить файл *event.txt*, введите следующую команду

```
scp <имя_пользователя@имя_хоста> или <ip_адрес>:event.txt ./event.txt
```


Чтобы получить файл *data.txt*, введите следующую команду

```
scp <имя_пользователя@имя_хоста> или <ip_адрес>:data.txt ./data.txt
```

Использование FTP для поиска файлов. Чтобы с помощью FTP получить файл *event.txt* или *data.txt*, выполните следующие действия:

1. После появления командной подсказки введите `ftp` и IP-адрес ПСУ, а затем нажмите ENTER.

Если настройка **Порт** для параметра **FTP-сервер** (см. раздел «Сервер FTP») отличается от значения по умолчанию (21), необходимо использовать эти новые настройки в строке команды FTP.

Для клиентов FTP Windows используйте следующие команды, включая пробелы. (Для некоторых клиентов FTP между IP-адресом и номером порта необходимо использовать двоеточие вместо пробела.)

```
ftp>open ip_адрес номер_порта
```



Чтобы улучшить защиту, для установки значения порта FTP-сервера, отличного от значения по умолчанию, см. «Сервер FTP». Можно указать любой порт в диапазоне от 5001 до 32768.

2. Для входа в систему используйте зависящее от регистра **Имя пользователя** и **Пароль** для администратора или пользователя. По умолчанию для пользователя с правами администратора используется имя `arc`. Именем пользователя устройства по умолчанию является `device`.
3. Чтобы включить двоичный режим передачи файлов, введите:

```
ftp>bin
```

Для отображения индикатора выполнения в ходе передачи файлов введите:

```
ftp>hash
```

4. Используйте команду `get` для передачи текста журнала на локальный диск.

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

или

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

5. 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 удаляется журнал данных, то в журнале событий записывается событие по удалению журнала.
- При очистке журнала событий это событие записывается в новый файл *event.txt*.

6. Введите `quit` в командной строке `ftp>`, чтобы завершить сеанс FTP.

Журнал ИБП

Путь: Журналы > ИБП



Этот параметр меню доступен не для всех ИБП.

Эта информация поступает от устройства ИБП и отделяется от журналов ПСУ. (Она не имеет прямой связи с платой и не является частью «Журнал событий» ПСУ.)

Данная информация может использоваться службой технической поддержки для устранения проблем.

Журналы передачи ИБП — отображение таблицы хранящихся в ИБП событий перехода в различные состояния, включая переход на работу от батарей и переход в режим байпаса.

Журналы сбоя ИБП — отображение таблицы хранящихся в ИБП ошибок.

Потребление энергии

Путь: Журналы > Потребление энергии



Этот параметр меню доступен не для всех ИБП.

Изображения общего расхода энергии устройства ИБП отображаются в верхней части экрана, а таблица с отделенными по неделям данными расположена в нижней части экрана.

Поле	Описание
Потребление энергии	Значение энергии, потребляемой ИБП к настоящему моменту времени (кВт.ч). Например, ИБП, обеспечивающий питание лампочки мощностью 350 Вт в течение 1000 часов, потребляет 350 кВт.ч электроэнергии.
Общая стоимость	Приблизительная стоимость энергии, используемой до этого момента времени. 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.
Выбросы CO ₂	Приблизительное количество CO ₂ , которое энергетическое предприятие выбрасывает в окружающую среду, чтобы произвести энергию, используемую до этого момента времени.

Значения расходов и выбросов CO₂ в значительной степени зависят от источника энергии и распределительной сети. Для получения приблизительной оценки выберите страну в раскрывающемся списке **Расположение** или воспользуйтесь ссылкой (**редактировать**), чтобы ввести собственные данные о расходах и выбросах.

При изменении местоположения создается настраиваемое местоположение, которое не изменяет рисунки по умолчанию для данного местоположения. Например, если в раскрывающемся списке выбрать значение **IE-Ireland** и изменить данные с помощью ссылки редактирования, запись с именем **Пользовательский (IE-Ireland)** создается в верхней части раскрывающегося списка.

Журнал брандмауэра

Путь: Журналы > Брандмауэр

При создании политики брандмауэра в этом разделе будут протоколироваться соответствующие события. Информацию по использованию политики см. в разделе «Экраны брандмауэра».

Данная информация может использоваться службой технической поддержки для устранения проблем.

В записях журнала содержится информация о трафике и действии правил (разрешено, отклонено). События, которые занесены в этот журнал, не заносятся в главный журнал событий. См. раздел «Журнал событий».

В журнале брандмауэра содержится до 50 последних событий. Журнал брандмауэра очищается при перезагрузке ПСУ.

О плате сетевого управления 3

Об устройстве ИБП

Путь: О программе > ИБП



Информация, отображаемая в разделе ИБП, зависит от используемого устройства.

Поле	Описание
Модель/ Учетный номер/ Серийный номер	Эти поля позволяют идентифицировать устройство ИБП.
Дата изготовления	Дата изготовления ИБП.
Версия прошивки	Номера версий модулей микропрограммы, установленных в ИБП
Версия прошивки 2	Второй номер версии микропрограммы, установленной в ИБП. Используется, если для нескольких процессоров требуются различные версии.
Полная номинальная мощность	Общая мощность ИБП (ВА).
Активная номинальная мощность	Общая нагрузка ИБП (Вт).
Полная номинальная мощность/фаза	Мощность каждой фазы ИБП (ВА). Технически, эта характеристика представляет собой фиксируемую мощность для каждой фазы в вольт-амперах (ВА). Фиксируемая мощность является произведением среднеквадратичных напряжения и силы тока.
Активная номинальная мощность/фаза	Общая нагрузка ИБП (Вт). Текущая активная мощность байпаса для каждой фазы в ваттах (Вт). Активная мощность представляет собой среднее по времени значения мгновенного произведения напряжения и силы тока.
О ПО контроля ИБП	Различная информация о программном обеспечении, получаемая от ИБП по последовательному порту или USB.
Учетный номер внутренней батареи/ Учетный номер внешней батареи	В этих полях указаны номера компонентов батарей. Эта информация может использоваться при устранении проблем.

Информация о ПСУ и модулях микропрограммы

Путь: О программе > Сеть

Завод-изготовитель аппаратного обеспечения: информация об оборудовании используется при устранении неисправностей устройства ПСУ.

Беспробойная работа управления: время непрерывной работы данного интерфейса управления, то есть время, прошедшее после горячего или холодного запуска ПСУ.

Модуль приложения, ОС APC (АОС) и Монитор загрузки: данная информация используется при устранении неисправностей и для поиска обновленной микропрограммы на веб-сайте www.apc.com/shop/us/en/tools/software-firmware.

Метка поля	Описание
Имя	Название модуля микропрограммы. Название Модуль приложения зависит от типа устройства ИБП, например su относится к устройствам Smart-UPS, sy относится к устройствам Symmetra. Модуль APC AOS всегда имеет название aos, а модуль монитора загрузки всегда имеет название boot.
Версия	Номер версии модуля микропрограммы. Номера версий модулей могут отличаться, но совместимые модули выпускаются вместе. См. раздел «Обновление микропрограммы».
Дата/время	Дата и время создания модуля микропрограммы.

См. также «Проверка номеров версий установленного микропрограммного обеспечения».

Экран поддержки

Путь: **О программе > Поддержка**

Эта функция позволяет объединить различные данные этого интерфейса в отдельный файл архива, который используется центром обслуживания клиентов и при устранении неисправностей. В этот файл включены журналы событий и данных, файл конфигурации (см. «Создание и импорт настроек с помощью файла конфигурации») и комплексная информация по отладке.

Щелкните **Создать журналы**, чтобы создать файл, а затем щелкните **Загрузить**. Появляется запрос, который позволяет просмотреть или сохранить файл архива.

Мастер настройки IP-конфигурации устройств

Возможности, требования и установка

Мастер настройки IP-конфигурации устройств может работать с платами сетевого управления (ПСУ), которым не назначен IP-адрес. При обнаружении такой платы и подключении к ней можно настроить для нее параметры IP-адреса.

Можно также найти устройства, которые уже подключены к сети, путем ввода диапазона IP-адресов, чтобы сузить поиск. Данный мастер сканирует IP-адреса в указанном диапазоне и определяет платы, которым DHCP-сервер уже назначил IP-адрес.



ПРИМЕЧАНИЯ:

- Нельзя провести поиск назначенных устройств, уже находящихся в сети, при помощи диапазона адресов IP, пока вы не включите SNMPv1 на ПСУ и не установите параметр Community Name в значение public. Для получения дополнительной информации см. раздел «Экраны SNMP».
- После настройки параметров IP-адреса платы сетевого управления для доступа к веб-интерфейсу пользователя ПСУ через браузер необходимо изменить URL с http на https.



Подробную информацию по данной программе см. в базе знаний на странице поддержки веб-сайта www.apc.com и выполните поиск **FA156064** (идентификатор соответствующей статьи).

В статье **FA156064** базы знаний также содержится информация по использованию параметра 12 протокола DHCP.

Системные требования

Данный мастер работает в Microsoft Windows 2000, Windows Server® 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, а также в 32- и 64-разрядных версиях Windows XP, Windows Vista, Windows 7, Windows 8 и Windows 10.

Данный мастер поддерживает платы с микропрограммой версии 3.0.x или выше и поддерживает только протокол IPv4.

Установка

Порядок установки мастера из загруженного исполняемого файла:

1. Перейдите на страницу www.apc.com/shop/tools/software-firmware.
2. Выполните фильтрацию по ПО/микропрограммному обеспечению — мастера и конфигураторы.
3. Запустите исполняемый файл из папки, в которую он был загружен.

После загрузки мастер доступен с помощью меню Windows.

Экспорт параметров конфигурации

Получение и экспорт файла .ini

Краткое описание процедуры

Администратор может получать ini-файл платы сетевого управления 3 (ПСУ) и экспортировать их в другую плату или в несколько ПСУ. Подробную информацию см. в следующих разделах.

1. Настройте ПСУ с выбором требуемых параметров и экспортируйте их; см. раздел «Создание и импорт настроек с помощью файла конфигурации».
2. Получите ini-файл из этой ПСУ.
3. Отредактируйте файл, изменив как минимум настройки TCP/IP.
4. Используйте протокол передачи файлов, поддерживаемый ПСУ, чтобы передать копию на одну или несколько ПСУ. Для передачи на несколько ПСУ используйте сценарий FTP или SCP либо утилиту для ini-файлов.

Каждая из принимающих ПСУ использует полученный файл для конфигурации собственных настроек, после чего удаляет его.

Содержание файла ini

Файл config.ini, полученный из ПСУ, содержит:

- *Заголовки разделов и ключевые слова* (только те, которые поддерживаются конкретным устройством ИБП или ПСУ, от которого получен файл). **Заголовки разделов** — это названия категорий, указанные в скобках ([]). **Ключевые слова** в каждом из заголовков раздела представляют собой метки, описывающие определенные настройки ПСУ. После каждого ключевого слова следует знак равенства и значение (принятое по умолчанию или заданное при конфигурировании).
- Ключевое слово **Override**: при значении, заданном по умолчанию, данное ключевое слово предотвращает экспорт одного или нескольких ключевых слов и их значений, определяемых устройством. Например, в разделе [NetworkTCP/IP] значение по умолчанию для слова **Override** (MAC-адрес управляющей ПСУ) блокирует экспорт параметров SystemIP, SubnetMask, DefaultGateway и BootMode.

Подробные процедуры

Получение. Порядок настройки и получения ini-файла для экспорта:

1. Если возможно, используйте интерфейс ПСУ для конфигурирования ее настроек для экспорта. (Непосредственное изменение содержимого ini-файла может вызвать ошибки.)
2. В следующем примере показано, как использовать FTP для получения файла config.ini из настроенной платы сетевого управления с помощью клиента командной строки
 - а. Установите соединение с ПСУ, используя ее IP-адрес:

```
ftp> ip_адрес
```
 - б. Зарегистрируйтесь в системе, используя для этого имя пользователя и пароль администратора.
 - в. Чтобы включить двоичный режим передачи файлов, введите:

```
ftp> bin
```

Для отображения индикатора выполнения в ходе передачи файлов введите:

```
ftp> hash
```
 - г. Получите файл config.ini, содержащий настройки ПСУ:

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


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



Для получения параметров конфигурации из нескольких ПСУ и их экспорта на другие ПСУ см. *Записки о выпуске: служебная программа файла INI* на веб-сайте APC или см. статью [FA156117](http://www.apc.com/support) в базе знаний по адресу <http://www.apc.com/support>.

Настройка. Перед передачей файла на другую ПСУ его необходимо отредактировать.

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 настраивайте значения непосредственно в ini-файле.
 - Для экспорта системного времени с максимальной точностью, если принимающие ПСУ имеют доступ к серверу протокола сетевого времени, установите значение `enabled` для параметра `NTPEnable`:

```
NTPEnable=enabled
```

Можно также сократить время передачи путем экспорта раздела `[SystemDate/Time]` в виде отдельного ini-файла.

- Добавляемые строки комментариев должны начинаться с точки 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 расширение `ini`.
 - Сохраните исходный отредактированный файл для использования в будущем. *Сохраняемый файл является единственной записью комментариев.*

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

- В интерфейсе пользователя принимающей ПСУ выберите **Конфигурация — Общие — Файл конфигурации пользователя**. Укажите полный путь к файлу или воспользуйтесь кнопкой **Обзор** на локальном компьютере.
- Используйте любой из протоколов, поддерживаемых платой сетевого управления, например, FTP, FTP Client, SCP или TFTP. В приведенном примере используется протокол FTP:
 - а. Из папки, содержащей копию отредактированного ini-файла, воспользуйтесь протоколом FTP, чтобы войти в ПСУ, в которую собираетесь экспортировать ini-файл.

```
ftp> open ip_адрес
```
 - б. Чтобы включить двоичный режим передачи файлов, введите:

```
ftp> bin
```

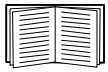
Для отображения индикатора выполнения в ходе передачи файлов введите:

```
ftp> hash
```
 - в. Экпортируйте копию отредактированного ini-файла в корневой каталог принимающей ПСУ:

```
ftp> put имя_файла.ini
```

Передача файла на несколько ПСУ. Вместо этого выполните следующие операции.

- Используйте FTP или SCP, но напишите сценарий, который содержит и повторяет операции, используемые для экспорта файла на одну ПСУ.
- Используйте пакетный файл обработки и утилиту для файлов `.ini`.



Для создания пакетного файла и использования служебной программы см. *Записки о выпуске: служебная программа файла INI* на веб-сайте APC. Или см. статью [FA156117](#) в базе знаний по адресу <http://www.apc.com/support>.

Сообщения о событиях загрузки и ошибках

Сообщения о событиях и ошибках, связанных с ним

Следующее событие происходит в том случае, когда принимающая плата сетевого 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 ПСУ завершается и выдается дополнительное сообщение об ошибке.

Текст сообщения о событии	Описание
Предупреждение файла конфигурации: неверное ключевое слово в строке <i>номер</i> . Предупреждение файла конфигурации: неверное значение в строке <i>номер</i> .	Строка с неправильным ключевым словом или значением игнорируется.
Предупреждение файла конфигурации: недействительный раздел в строке с <i>номером</i> .	Если имя секции указано неверно, все пары ключевых слов и значений в данной секции игнорируются.
Предупреждение файла конфигурации: ключевое слово обнаружено вне секции в строке <i>номер</i> .	Ключевое слово, введенное в начале файла (то есть перед заголовком секции), игнорируется.
Предупреждение файла конфигурации: размер файла конфигурации превышает максимальный размер.	Если размер файла слишком большой, происходит неполная загрузка. Уменьшите размер файла или разбейте его на два файла и повторите загрузку еще раз.

Сообщения в файле config.ini

Устройство, связанное с ПСУ, с которой загружается файл config.ini, должно быть обнаружено 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
```

Если не планируется экспорт конфигурации устройства как части импортированного ini-файла, игнорируйте эти сообщения.

Ошибки, генерируемые заблокированными параметрами

Ключевое слово `Override` и его значение будут создавать сообщения об ошибках в журнале событий при блокировке экспорта значений.



Сведения о том, какие параметры могут блокироваться, см. «Содержание файла ini».

Поскольку блокируемые параметры относятся к конкретным устройствам и не пригодны для экспорта в другие ПСУ, 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 разделов.

Связанные вопросы

В операционных системах Windows вместо пересылки ini-файлов можно использовать мастер настройки IP-конфигурации устройств, чтобы изменить основные настройки TCP/IP платы сетевого управления и настроить другие параметры через интерфейс пользователя.



См. раздел «Мастер настройки IP-конфигурации устройств».

Передача файлов

Обновление микропрограммы

При обновлении микропрограммного обеспечения на плате сетевого управления 3 (ПСУ) для устройства ИБП становятся доступными последние функции, улучшения безопасности и производительности и исправления ошибок. Для обновления ИБП см. раздел «Экран «Обновление прошивки»».

Обновление подразумевает простое копирование файла NMC3 на ПСУ. Процесс установки отсутствует. Регулярно проверяйте веб-страницу www.apc.com/shop/tools/software-firmware на наличие обновлений.

Файл NMC3 имеет следующий формат:

```
apc_версия-оборудования_тип_версия-оборудования.nmc3
```

- `apc`: обозначает контекст.
- `hardware-version`: `hw0n`, где `n` обозначает версию оборудования, на котором можно использовать этот файл.
- `type`: определяет, какой именно модуль; значение `su` указывает на устройство Smart-UPS, а значение `sy` указывает на устройство Symmetra.
- `версия`: номер версии файла.

Способы передачи файлов микропрограммы

Микропрограмму последней версии можно бесплатно загрузить по адресу www.apc.com/shop/tools/software-firmware. Для обновления прошивки одной ПСУ или нескольких используйте один из трех следующих методов.

- В операционной системе Windows используйте **программу обновления микропрограммы**, загруженную с **веб-сайта APC**. См. раздел «Использование программы обновления микропрограммы ПСУ».
- Для передачи файла NMC3 используйте FTP или SCP на любой из поддерживаемых операционных систем. См. раздел «Использование **FTP или SCP** для обновления одной платы сетевого управления».
- Для передачи файла NMC3 с вашего компьютера на плату сетевого управления, находящуюся ВНЕ вашей сети, используйте **XMODEM** через виртуальный порт связи с USB-интерфейсом с помощью загрузчика. См. раздел «Использование XMODEM для обновления одной ПСУ».
- Информацию об обновлении **нескольких плат сетевого управления** см. в разделах «Обновление микропрограммы на нескольких платах сетевого управления» и «Использование программы обновления микропрограммы ПСУ для нескольких обновлений в системе Windows.».

Использование программы обновления микропрограммы ПСУ

Эта программа обновления микропрограммы является частью пакета обновления микропрограммы, доступного на **веб-сайте APC**. (Никогда не используйте программу, предназначенную для одного изделия, для обновления микропрограммы другого изделия.)

Использование программы для обновления в системах Windows. В любых поддерживаемых системах Windows программа обновления микропрограммы ПСУ автоматизирует передачу файла с расширением `.nmc3`.

Распакуйте загруженный файл микропрограммы и дважды щелкните файл с расширением `.exe`. Введите IP-адрес хоста, имя пользователя и пароль в диалоговых полях. Также необходимо выбрать протокол FTP или SCP и связанный с ним порт.

ПРИМЕЧАНИЕ. Выбранный протокол должен быть включен на устройстве ПСУ для завершения обновления микропрограммы. Также см. раздел «Использование программы обновления микропрограммы ПСУ для нескольких обновлений в системе Windows.».

Использование FTP или SCP для обновления одной платы сетевого управления

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

- ПСУ должна быть подключена к сети, иметь IP-адрес, маску подсети и шлюз по умолчанию.
- Сервер FTP должен быть разрешен в настройках ПСУ; см. раздел «Сервер FTP».

Для передачи файла выполните следующие действия.

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

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

Информацию о файлах см. в разделе «Файл NMC3 имеет следующий формат».

2. Откройте клиентский сеанс FTP:

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

3. Введите команду `open` и укажите IP-адрес ПСУ, затем 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. Пример (с пробелом перед 21000):

```
ftp> open 150.250.6.10 21000
```
- Некоторые клиенты FTP требуют ставить перед номером порта двоеточие.

4. Войдите в систему с правами администратора.

5. Обновите прошивку.

```
ftp> bin  
ftp> put apc_hw21_AA_v-v-v-v.nmc3 (где AA - приложение, например su,  
а v-v-v-v - номер версии микропрограммы)
```

6. Когда FTP-сервер подтвердит передачу, введите `quit` для закрытия сеанса.

SCP. Для использования программы Secure CoPy (SCP) с целью обновления микропрограммы ПСУ выполните следующие действия.

1. С помощью командной строки SCP выполните передачу файла NMC3 на ПСУ. В данном примере v-v-v-v показывает номер версии модуля приложения:

```
scp apc_hw21_su_v-v-v-v.nmc3 apc@158.205.6.185:apc_hw21_su_v-v-v-v-  
v.nmc3su_v-v-v-v.nmc3
```

Примечание. Для использования SCP необходимо включить SSH. Информацию о включении SSH см. в разделе «Экран консоли».

Использование XMODEM для обновления одной ПСУ

Чтобы использовать XMODEM для обновления одной ПСУ, не находящейся в сети, необходимо сделать следующее.

1. С помощью прилагаемого кабеля micro-USB (номер детали 960-0603) подключите ПСУ к порту USB локального компьютера.
2. Нажмите кнопку **«Сбросить»** на ПСУ.
3. Когда ПСУ во время загрузки обнаруживает соединение USB, она ожидает 90 секунд, чтобы дать операционной системе достаточно времени на распознавание и настройку виртуального порта связи. Когда виртуальный порт связи будет готов, запустите программу терминала, например HyperTerminal или Tera Term, и выберите этот виртуальный порт.
4. Нажмите клавишу **Enter** дважды или нажимайте ее до тех пор, пока не появится приглашение монитора загрузки: VM>

ПРИМЕЧАНИЕ. Если в течение 90 секунд после начала перезагрузки ПСУ соединение с монитором загрузки установлено не будет, ПСУ продолжит свой обычный процесс загрузки.

5. Введите XMODEM и нажмите **Enter**.
6. В меню программы терминала выберите XMODEM, затем выберите файл .nmc3, который будет передан с помощью XMODEM. По завершении передачи XMODEM на экране появится приглашение монитора загрузки.

Введите `reset` или нажмите кнопку **«Сбросить»**, чтобы перезапустить ПСУ.



ПРИМЕЧАНИЕ. Для подключения к консоли ПСУ в ОС Windows 7 требуется драйвер. Драйвер доступен для загрузки на странице устройства AP9640/AP9641 на веб-сайте **APC**, расположенной в разделе **Software/Firmware**. Для ОС Windows 10 драйвер не требуется.

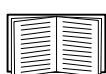
1. При подключении ПСУ через кабель micro-USB в разделе «Другие устройства» будет обнаружено устройство под названием NMC3-CDC.
2. Нажмите правой кнопкой мыши на это устройство и выберите «Обновить драйвер...».
3. Выберите опцию «Выполнить поиск драйверов на этом компьютере» и перейдите к месту загрузки драйвера (`usb_cdc_ser.inf`).
4. Примите сообщение о безопасности неподписанного драйвера.

Теперь Windows распознает ПСУ и назначит устройству COM-порт.

Обновление микропрограммы на нескольких платах сетевого управления

Используйте один из двух следующих методов.

- **Программа обновления микропрограммы ПСУ в Windows.** См. раздел «Использование программы обновления микропрограммы ПСУ для нескольких обновлений в системе Windows.».
- **Использование FTP или SCP.** Для обновления нескольких ПСУ с использованием клиента FTP или протокола SCP напишите скрипт, который будет выполнять эту процедуру автоматически.
- **Настройки конфигурации экспорта.** Можно создать командные файлы и использовать программу для получения параметров конфигурации нескольких ПСУ и экспортировать их на другие ПСУ.



См. *Записки о выпуске: служебная программа файла INI* в базе знаний по адресу <http://www.apc.com/support>.

Использование программы обновления микропрограммы ПСУ для нескольких обновлений в системе Windows. После загрузки программы обновления со страницы загрузки ПСУ на [веб-сайте APC](#) дважды нажмите на файл .exe и извлеките содержимое архива.

1. Найдите файл `devices.txt` в каталоге с программой. Откройте файл и отредактируйте его в текстовом редакторе, чтобы ввести необходимую информацию для каждого обновляемого устройства ПСУ:
 - [Устройство]: Данный заголовок раздела должен быть включен для каждой обновляемой ПСУ.
 - Хост: IPv4-адрес устройства.
 - Протокол: SCP или FTP.
 - Порт: Порт, связанный с SCP или FTP.
 - Имя пользователя: Имя пользователя с правами администратора, включенного на ПСУ.
 - Пароль: Пароль администратора, действующий на ПСУ

Удалите все комментарии и точки с запятой из файла `devices.txt` и сохраните изменения.

Например:

```
[Устройство]
Хост = 192.168.0.1
Протокол = SCP
Порт = 22
Имя пользователя = arc
Пароль = arc
```

Например:

```
[Устройство]
Хост = 192.168.0.2
Протокол = SCP
Порт = 22
Имя пользователя = arc
Пароль = arc
```

Можно использовать имеющийся файл `devices.txt`, если он уже существует.

2. Откройте программу обновления микропрограммы. Если в файле `devices.txt` были предоставлены правильные данные, в программе появится следующее сообщение:
 - Обнаружен и импортирован список устройств, поэтому хосты, перечисленные в окне событий ниже, будут использоваться в качестве активных.
3. Нажмите в программе кнопку «**Начать обновление**», чтобы начать обновление микропрограммы.

Проверка обновлений

Коды результатов последней передачи

Возможные ошибки передачи: сервер TFTP или FTP не найден, сервер отказывает в доступе, сервер не находит или не распознает передаваемый файл, передаваемый файл поврежден.

Проверка номеров версий установленного микропрограммного обеспечения

Путь: **О программе** — **Сеть**

Используйте веб-интерфейс пользователя для проверки версий обновленных модулей микропрограммы. Можно также использовать команду GET для OID `sysDescr MIB II`. В интерфейсе командной строки введите команду `about`.

Смена языка интерфейса пользователя

Интерфейс пользователя ПСУ может отображаться на разных языках. Выберите язык из раскрывающегося списка с языками [Language](#) на экране входа [Login](#).

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

Устранение проблем

Проблемы доступа к плате сетевого управления

Посетите базу знаний по адресу www.apc.com/support для получения пошаговых инструкций по устранению проблем и полезных решений распространенных неполадок. Информацию об обращении в службу поддержки см. в разделе «Устранение проблем».

Проблема	Решение
Не удается выполнить эхо-тестирование ПСУ	<p>Если индикатор состояния ПСУ горит зеленым цветом, попробуйте послать команду эхо-тестирования на другой узел того же сегмента сети, в котором расположена ПСУ. Если тестирование не работает, то плата сетевого управления исправна. Если не светится зеленый индикатор состояния и не удастся установить обмен пакетами, выполните следующие действия.</p> <ul style="list-style-type: none">• Проверьте, что плата сетевого управления надежно установлена в ИБП.• Проверьте сетевые подключения.• Проверьте IP-адреса платы сетевого управления и систему ПСУ.• Если ПСУ находится в другой сети (или подсети), отличной от сети ПСУ, проверьте IP-адрес шлюза по умолчанию (или маршрутизатора).• Проверьте число битов подсети для маски подсети платы сетевого управления.
Не удается назначить коммуникационный порт с помощью программы терминала	<p>Перед использованием программы терминала для настройки платы сетевого управления следует закрыть все приложения, службы и программы, которые используют данный коммуникационный порт.</p>
Невозможен доступ через интерфейс командной строки по каналу последовательного обмена	<p>Убедитесь, что настройки скорости обмена данными не были изменены. Попробуйте установить значения 2400, 9600, 19200 или 38400.</p>
Невозможен удаленный доступ через интерфейс командной строки	<ul style="list-style-type: none">• Убедитесь, что используется правильный способ доступа: Telnet или Secure SHell (SSH). Администратор может включить эти методы доступа. По умолчанию протокол Telnet выключен, а порт SSH включен. Протоколы SSH и Telnet можно включать/отключать независимо друг от друга.• При использовании SSH плата сетевого управления может создавать ключ хост-узла. Плате сетевого управления требуется до одной минуты для создания ключа хост-узла, в это время SSH будет недоступен.
Не удается получить доступ к интерфейсу пользователя (UI)	<ul style="list-style-type: none">• Убедитесь, что доступ HTTP или HTTPS открыт.• Убедитесь, что указан правильный URL-адрес, соответствующий системе безопасности, используемой платой сетевого управления. Для SSL в начале URL-адреса нужно указывать https, а не http.• Убедитесь, что эхо-тестирование платы сетевого управления выполняется успешно.• Убедитесь, что используемый браузер поддерживается платой сетевого управления. См. раздел «Устранение проблем».• Если плата сетевого управления была только что перезагружена и выполняется настройка SSL, возможно, плата сетевого управления создает сертификат сервера. Для создания этого сертификата плате сетевого управления потребуется до одной минуты, в это время сервер SSL будет недоступен.

Неисправности SNMP

Проблема	Решение
Невозможно выполнить операцию GET	<ul style="list-style-type: none"> • Проверьте возможность чтения (GET) имени сообщества (SNMPv1) или конфигурацию профиля пользователя (SNMPv3). • Используйте интерфейс командной строки или интерфейс пользователя для проверки доступа NMS. См. раздел «Экраны SNMP».
Невозможно выполнить операцию SET	<ul style="list-style-type: none"> • Проверьте, включен ли протокол SNMP. Протоколы SNMPv1 и SNMPv3 выключены по умолчанию. • Проверьте возможность чтения/записи (SET) имени сообщества (SNMPv1) или конфигурацию профиля пользователя (SNMPv3). • Используйте интерфейс командной строки или интерфейс пользователя для проверки того, что NMS имеет доступ на запись (SET) (SNMPv1) или получил доступ к IP-адресу в списке управления доступом (SNMPv3). См. раздел «Экраны SNMP».
Не удается получать прерывания в системе NMS	<ul style="list-style-type: none"> • Проверьте, чтобы тип прерывания (SNMPv1 или SNMPv3) был правильно настроен для системы NMS, используемой в качестве приемника прерываний. • В случае SNMP v1 пошлите запрос <code>mconfigTrapReceiverTable</code> 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 <code>mconfigTrapReceiverTable</code> OID или используйте интерфейс командной строки или интерфейс пользователя, чтобы исправить настройки приемника прерываний. • В случае SNMPv3 проверьте настройки профиля пользователя для NMS и запустите тест прерываний. <p>См. разделы «Экраны SNMP», «Получатели прерываний» и «Экран тестирования прерываний SNMP».</p>
Прерывания, получаемые NMS, не определены	См. документацию по NMS, чтобы проверить, что прерывания правильно указаны в базе данных сигналов тревоги и прерываний.

Проблемы с Modbus



Дополнительную информацию по проводке и настройке последовательного порта Modbus для карт AP9641 и AP9643, доступном на компакт-диске Utility и на веб-сайте APC. Подробную информацию о регистрах и описания битов Modbus см. в *Карте регистров Modbus (Modbus Register Map)* на веб-сайте APC.

Неисправности аппаратного ключа устройства APC USB Wi-Fi (AP9834)

Неисправность	Решение
<p>Невозможно подключиться к сети Wi-Fi.</p>	<ul style="list-style-type: none"> • Проверьте, правильно ли вставлено устройство APC USB Wi-Fi в USB-порт платы AP9641/AP9643. • Проверьте правильность настроек Wi-Fi в веб-интерфейсе пользователя или интерфейсе командной строки ПСУ. • В журнале событий ПСУ убедитесь в отсутствии событий, связанных с Wi-Fi. Если настройки Wi-Fi введены неправильно или оставлены пустыми, ПСУ зафиксирует ошибку в журнале событий. Например: «Ошибка устройства USB Wi-Fi. Настройки Wi-Fi». <p>Если неполадка все еще сохраняется, обратитесь к сетевому администратору для диагностики проблем с подключением.</p>
<p>Невозможно решить проблему, в результате которой светодиод устройства постоянно горит красным светом.</p>	<ul style="list-style-type: none"> • Проверьте правильность настроек Wi-Fi в веб-интерфейсе пользователя или интерфейсе командной строки ПСУ. • Решите проблему, связанную с любыми событиями Wi-Fi в журнале событий ПСУ. Например: «Ошибка устройства USB Wi-Fi. Настройки Wi-Fi». • Повторно выполните проводное соединение и измените настройки Wi-Fi альтернативным методом. <ul style="list-style-type: none"> – Веб-интерфейс пользователя (Конфигурация > Сеть > Wi-Fi) – Интерфейс командной строки (команда <code>wifi</code>) – Файл <code>config.ini</code> (раздел <code>NetworkWiFi</code>) <p>Если проводное соединение больше недоступно, подключите кабель микро-USB (960-0603) к консольному порту ПСУ для доступа к интерфейсу командной строки и передайте файл <code>config.ini</code> с помощью команды <code>xferINI</code>. Более подробная информация приведена в руководстве по интерфейсу командной строки (CLI) ПСУ 3.</p> <p>Если неполадка все еще сохраняется, обратитесь в службу технической поддержки. См. раздел «Глобальная служба технической поддержки APC».</p>

Описание индикаторов состояния

Состояние	Описание
Не горит	Возможна одна из следующих ситуаций. <ul style="list-style-type: none">• Устройство не вставлено в USB-порт платы сетевого управления AP9461/AP9463.• Прошивка ПСУ не поддерживает Wi-Fi. Поддержка Wi-Fi доступна в прошивке версии 1.4 и выше. См. раздел «Передача файлов» на стр 87.• Устройство не работает надлежащим образом. Возможно, потребуется отремонтировать или заменить устройство. Обратитесь в службу технической поддержки. См. раздел «Глобальная служба технической поддержки APC».
Непрерывно светится зеленым цветом.	Устройство подключено к точке доступа, но сетевая активность отсутствует.
Мигает зеленым цветом.	Устройство подключено к точке доступа и сеть Wi-Fi активна.
Непрерывно светится красным цветом.	Возможна одна из следующих ситуаций. <ul style="list-style-type: none">• Имеет место систематическая ошибка в устройстве.• Имеет место систематическая ошибка в настройках Wi-Fi ПСУ.• Имеют место неразрешимые проблемы, связанные с точкой доступа.
Мигает красным цветом.	Устройство находится в процессе подключения к точке доступа Wi-Fi.

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 от 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, а также на оборудование, подвергавшееся изменениям или доработке каким-либо способом. В случае ремонта или замены неисправного оборудования или его компонентов исходный гарантийный срок не продлевается. Компоненты, предоставляемые согласно данной гарантии, могут быть либо новыми, либо отремонтированными в заводских условиях.

Гарантия без права передачи

Данная гарантия относится только к первоначальному покупателю, который должен 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.

ПО УСЛОВИЯМ ДАННОГО СОГЛАШЕНИЯ ИЛИ В СВЯЗИ С НИМ НЕ ПРЕДУСМОТРЕНО ИНЫХ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ПРИНИМАЕМЫХ В СИЛУ ЗАКОНА ИЛИ ИНЫМ ОБРАЗОМ, ГАРАНТИЙНЫХ ОБЯЗАТЕЛЬСТВ В ОТНОШЕНИИ ПРОДАВАЕМОЙ, ОБСЛУЖИВАЕМОЙ ИЛИ ПРЕДОСТАВЛЯЕМОЙ ПРОДУКЦИИ. КОМПАНИЯ APC ОТКАЗЫВАЕТСЯ ОТ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙНЫХ ОБЯЗАТЕЛЬСТВ В ОТНОШЕНИИ КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ОБОРУДОВАНИЯ К ОПРЕДЕЛЕННЫМ ЦЕЛЯМ. ПРЕДОСТАВЛЕНИЕ КОМПАНИЕЙ APC ТЕХНИЧЕСКИХ И ИНЫХ КОНСУЛЬТАЦИЙ ИЛИ УСЛУГ В ОТНОШЕНИИ ОБОРУДОВАНИЯ НЕ МОЖЕТ СЛУЖИТЬ ОСНОВАНИЕМ ДЛЯ РАСШИРЕНИЯ ИЛИ СОКРАЩЕНИЯ ИЛИ ИЗМЕНЕНИЯ УСЛОВИЙ ГАРАНТИИ, НАЛОЖЕНИЯ ДОПОЛНИТЕЛЬНЫХ ОБЯЗАТЕЛЬСТВ И ОТВЕТСТВЕННОСТИ. ВЫШЕПЕРЕЧИСЛЕННЫЕ ГАРАНТИИ И СРЕДСТВА ВОЗМЕЩЕНИЯ ЯВЛЯЮТСЯ ИСКЛЮЧИТЕЛЬНЫМИ И ЗАМЕЩАЮТ ЛЮБЫЕ ДРУГИЕ ГАРАНТИИ И СРЕДСТВА ВОЗМЕЩЕНИЯ. ИЗЛОЖЕННЫЕ ВЫШЕ УСЛОВИЯ ГАРАНТИИ УСТАНАВЛИВАЮТ ИСКЛЮЧИТЕЛЬНУЮ ОТВЕТСТВЕННОСТЬ КОМПАНИИ APC И ИСКЛЮЧИТЕЛЬНЫЕ ПРАВА ЗАЩИТЫ ПОКУПАТЕЛЕЙ В СЛУЧАЕ НАРУШЕНИЯ УКАЗАННЫХ ГАРАНТИЙ. ДЕЙСТВИЕ ГАРАНТИЙ КОМПАНИИ APC РАСПРОСТРАНЯЕТСЯ НА ПОКУПАТЕЛЯ, НО НЕ НА ТРЕТЬИХ ЛИЦ.

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ КОМПАНИЯ APC, ЕЕ СЛУЖАЩИЕ, РУКОВОДИТЕЛИ, СОТРУДНИКИ ФИЛИАЛОВ И ШТАТНЫЕ СОТРУДНИКИ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КОСВЕННЫЙ, ОСОБЫЙ, ПОБОЧНЫЙ ИЛИ ШТРАФНОЙ УЩЕРБ, ПОНЕСЕННЫЙ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ, ОБСЛУЖИВАНИЯ ИЛИ УСТАНОВКИ ПРОДУКЦИИ, НЕЗАВИСИМО ОТ ТОГО, УПОМИНАЛОСЬ ЛИ О ТАКОМ УЩЕРБЕ В ДОГОВОРЕ ИЛИ ДЕЛИКТЕ, БУДЬ ТО НЕИСПРАВНОСТЬ, НЕБРЕЖНОСТЬ, ОБЯЗАТЕЛЬСТВА ПО ВОЗМЕЩЕНИЮ УЩЕРБА, ИЛИ ОТ ТОГО, ВЕЛИСЬ ЛИ ПРЕДВАРИТЕЛЬНЫЕ КОНСУЛЬТАЦИИ С КОМПАНИЕЙ APC О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА. В ЧАСТНОСТИ, КОМПАНИЯ APC НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ИЗДЕРЖКИ, ПОНЕСЕННЫЕ В РЕЗУЛЬТАТЕ ПОТЕРИ ПРИБЫЛИ ИЛИ ДОХОДА, ВЫВЕДЕНИЯ ИЗ СТРОЯ ОБОРУДОВАНИЯ, НЕВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ОБОРУДОВАНИЯ, УТРАТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИЛИ ДАННЫХ, ЗАТРАТ НА ЗАМЕЩЕНИЕ, ИСКОВ ТРЕТЬИХ ЛИЦ И Т.Д.

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 со страницы «Support» (Поддержка) сайта APC: www.apc.com/support. В верхней части страницы выберите страну в соответствующем списке. Для получения информации о центрах сервисного обслуживания в конкретном регионе выберите вкладку «Support» (Поддержка).

Авторские права cryptlib Digital Data Security New Zealand Ltd, 1998 г.

Авторские права © Руководство Калифорнийского университета, 1990, 1993, 1994. Все права защищены.

Этот код получен из программного обеспечения, предоставленного Беркли Майком Олсоном (Mike Olson).

Распространение и использование в исходном и двоичном виде с изменением или без такового разрешено только при соблюдении следующих условий:

1. Распространение исходного кода должно учитывать вышеуказанные заявления об авторских правах, перечень условий и следующие ограничения.
2. Распространение в двоичном виде должно учитывать вышеуказанные заявления об авторских правах, перечень условий и следующие ограничения в документации и других материалах, предоставленных для распространения.
3. Рекламные материалы, упоминающие характеристики и использование настоящего программного обеспечения, должны признавать следующее:

Этот продукт содержит программное обеспечение, разработанное Калифорнийским университетом в Беркли и его сотрудниками.
4. Название университета и имена его сотрудников не должны использоваться для поддержки и продвижения продуктов, созданных на основе данного программного обеспечения без предварительного письменного разрешения.

ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЕНО РУКОВОДСТВОМ И СОТРУДНИКАМИ НА УСЛОВИЯХ «КАК ЕСТЬ», И, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ТАКОВЫМИ, ЛЮБЫЕ ЯВНО ВЫРАЖЕННЫЕ ИЛИ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ПРИГОДНОСТИ ДЛЯ ПРОДАЖИ И СООТВЕТСТВИЯ КОНКРЕТНЫМ ЦЕЛЯМ НЕ ПРИМЕНИМЫ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ РУКОВОДСТВО ИЛИ СОТРУДНИКИ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ НИ ЗА КАКИЕ ПРЯМЫЕ, НЕПРЯМЫЕ, СЛУЧАЙНЫЕ, СПЕЦИАЛЬНЫЕ, ШТРАФНЫЕ ИЛИ КОСВЕННЫЕ УБЫТКИ (ВКЛЮЧАЯ, ПОМИМО ПРОЧЕГО, ПРИОБРЕТЕНИЕ ТОВАРОВ ИЛИ УСЛУГ НА ЗАМЕНУ, ПОТЕРЮ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ, ДАННЫХ ИЛИ ПРИБЫЛИ ИЛИ ПРИОСТАНОВКУ БИЗНЕСА) ПО ЛЮБОЙ ПРИЧИНЕ И ПО ЛЮБОЙ ТЕОРИИ ОТВЕТСТВЕННОСТИ, ОБЯЗАТЕЛЬСТВАМ, ВЫРАЖЕННЫМ В КОНТРАКТЕ, СТРОГИМ ОБЯЗАТЕЛЬСТВАМ, ИЛИ ПРИ ГРАЖДАНСКОМ ПРАВОНАРУШЕНИИ (ВКЛЮЧАЯ ХАЛАТНОСТЬ И ПРОЧЕЕ), ВОЗНИКАЮЩИЕ КАКИМ БЫ ТО НИ БЫЛО ОБРАЗОМ ВСЛЕДСТВИЕ ПРИМЕНЕНИЯ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ ПРИ НАЛИЧИИ ИНФОРМАЦИИ О ВОЗМОЖНОСТИ НАНЕСЕНИЯ ДАННОГО УЩЕРБА.

Радиочастотные помехи



Внесение изменений в конструкцию данного устройства без письменного разрешения организации, отвечающей за обеспечение соответствия стандартам, может привести к лишению пользователя прав на эксплуатацию данного оборудования.

США — FCC

Данное устройство прошло испытания, подтвердившие его соответствие ограничениям, предусмотренным требованиями раздела 15 правил Федеральной комиссии по связи (FCC) США к цифровым устройствам класса А. Эти ограничения призваны обеспечивать достаточную защиту от вредных помех во время эксплуатации оборудования в производственных условиях. Данное изделие генерирует, использует и излучает электромагнитные волны в радиодиапазоне и, будучи установленным с отклонением от требований, изложенных в настоящем руководстве, может стать источником радиопомех. Эксплуатация данного оборудования в жилых районах может создавать помехи. Ответственность за устранение таких помех полностью лежит на пользователе.

Канада — ICES

Это цифровое устройство класса А удовлетворяет требованиям стандарта ICES-003 (Канада).

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Япония — VCCI

Это изделие класса А основано на стандарте добровольного совета по контролю помех (Voluntary Control Council for Interference — VCCI) для информационно-технологического оборудования. Использование оборудования в домашних условиях может привести к радиопомехам. В этом случае пользователь должен принять необходимые меры.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると、電波

妨害を引き起こすことがあります。この場合には、使用者が適切な対策を講ずるように要求されることがあります

Тайвань — BSMI

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Австралия и Новая Зеландия

Внимание. Данный продукт является оборудованием класса А. В бытовых условиях такое оборудование может вызывать радиопомехи. В этом случае от пользователя может потребоваться принятие соответствующих мер.

Европейский союз

Данное изделие соответствует требованиям к защите, указанным в директиве совета Европейского союза 2004/108/ЕС, разработанной в соответствии с законодательством государств-членов в отношении электромагнитной совместимости. Компания APC не принимает на себя ответственность за любое невыполнение требований к защите, вызванное несанкционированной модификацией изделия.

Данное устройство было проверено и признано соответствующим ограничениям для ИТ-оборудования класса А в соответствии с CISPR 22/европейским стандартом EN 55022. Ограничения для оборудования класса А были определены для коммерческой и производственной сред и обеспечивают достаточную защиту от помех при использовании лицензированного коммуникационного оборудования.

Внимание. Данный продукт является оборудованием класса А. В бытовых условиях такое оборудование может вызывать радиопомехи. В этом случае от пользователя может потребоваться принятие соответствующих мер.

Корея 한국

A 급 기기 (업무용 방송통신기기)

이 기기는 업무용 (A 급) 으로 전자파적합등록을 한 기기이오니판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의지역에서 사용하는 것을 목적으로 합니다.

Устранение проблем

Пользовательская поддержка данного или любого другого изделия осуществляется бесплатно одним из следующих способов:

- Обратитесь на сайт компании Schneider Electric для доступа к документам базы знаний Schneider Electric и отправки запроса на обслуживание.
 - www.apc.com (центральное отделение)
Обратитесь на локализованные для отдельных стран веб-сайты корпорации Schneider Electric, на каждом из которых содержится информация о технической поддержке.
 - www.apc.com/support/
Глобальная техническая поддержка с помощью поиска в базе знаний компании Schneider Electric и использование системы электронной поддержки.
- Обратитесь в центр технической поддержки компании Schneider Electric по телефону или электронной почте.
 - Региональные центры: см. контактную информацию на веб-сайте www.apc.com/support/contact.

Информацию о местных центрах технической поддержки можно также получить у представителя или у дистрибьютора, у которого было приобретено изделие.

© Schneider Electric, 2021. Все права защищены. Schneider Electric, APC и Плата сетевого управления являются товарными знаками и собственностью Schneider Electric SE, ее дочерних и аффилированных компаний. Все остальные товарные знаки являются собственностью соответствующих владельцев.