

Благодарим за выбор LTE CPE!

## Справка по LTE CPE

Выпуск 01

Дата 2011-07-15

### **Huawei Technologies Co., Ltd.**

Адрес : Huawei Industrial Base  
Bantian, Longgang  
Shenzhen 518129  
People's Republic of China

Сайт: <http://www.huawei.com>

Эл. почта: terminal@huawei.com

## **Авторские права © Huawei Technologies Co., Ltd. 2011. Все права защищены.**

Ни одна из частей данного документа не может быть воспроизведена или передана по каналам связи в любой форме или любыми средствами без предварительного письменного согласия компании Huawei Technologies Co., Ltd.

## **Товарные знаки**



являются товарными знаками Huawei Technologies Co., Ltd. Другие товарные знаки, продукты, услуги и наименования компаний, упомянутые в данном документе, принадлежат исключительно их владельцам.

## **Примечание**

Некоторые функции оборудования и его аксессуаров зависят от установленного программного обеспечения, производительности и параметров локальной сети. Кроме того, ваш оператор или провайдер услуг может не активировать некоторые функции или настройки сети оператора сотовой связи или провайдера услуг могут ограничивать такие функции. Поэтому приведенное здесь описание может не полностью соответствовать приобретенному продукту или его аксессуарам.

Huawei Technologies Co., Ltd. сохраняет за собой право изменять любую информацию и технические характеристики без предварительного уведомления и обязательств

## **Huawei Technologies Co., Ltd.**

Адрес: Huawei Industrial Base  
Bantian, Longgang  
Shenzhen 518129  
People's Republic of China

Веб-сайт: <http://www.huawei.com>

Эл. почта: [terminal@huawei.com](mailto:terminal@huawei.com)

# Содержание

<b>Содержание.....</b>	<b>ii</b>
<b>1 Начало работы.....</b>	<b>1</b>
1.1 Введение .....	1
1.2 Требования к конфигурации Вашего компьютера.....	1
1.3 Ввод на веб-страницу управления устройством .....	2
<b>2 Статус.....</b>	<b>3</b>
2.1 Интернет.....	3
2.1.1 Статус .....	3
2.1.2 Статистика .....	3
2.2 LAN.....	3
2.2.1 Статус .....	3
2.2.2 Статистика .....	3
2.3 WLAN .....	4
2.3.1 Статус .....	4
2.3.2 Статистика .....	4
<b>3 Общие настройки.....</b>	<b>5</b>
3.1 Настройки SIM-карты .....	5
3.1.1 Просмотр статуса SIM-карты .....	5
3.1.2 Включение проверки PIN-кода .....	5
3.1.3 Отключение проверки PIN-кода .....	5
3.1.4 Проверка PIN-кода .....	6
3.1.5 Изменение PIN-кода .....	6
3.1.6 Установка автоматической проверки PIN-кода .....	6
3.1.7 Проверка PUK-кода .....	7
3.2 Настройки Интернет .....	7
3.2.1 Выбор сетевого режима .....	7
3.2.2 Выбор режима подключения .....	8
3.2.3 Выбор APN для передачи данных .....	8
3.2.4 Создание профиля APN .....	8
3.2.5 Изменение профиля APN .....	9
3.2.6 Удаление профиля APN .....	9
3.3 Настройки DHCP .....	9

3.3.1 Настройки хоста LAN .....	10
3.3.2 Настройки DHCP .....	10
3.4 Настройки WLAN.....	11
3.4.1 Общие настройки .....	11
3.4.2 Профиль интерфейса .....	13
3.5 Безопасное подключение к WLAN .....	15
3.5.1 Настройка безопасного подключения к WLAN .....	15
3.6 WLAN Multi SSID.....	15
3.6.1 Список SSID .....	15
3.7 Ограничение доступа WLAN .....	16
3.7.1 Управление MAC-адресами WLAN .....	16
3.7.2 Список настроек .....	17
3.8 MTU в сети Интернет .....	18
3.9 Настройки маршрутизации .....	18
3.9.1 Динамическая маршрутизация .....	18
3.9.2 Статическая маршрутизация .....	19
<b>4 Настройки безопасности.....</b>	<b>20</b>
4.1 Настройки брандмауэра .....	20
4.1.1 Уровень брандмауэра.....	20
4.2 Фильтрация MAC-адресов .....	21
4.2.1 Белый список MAC-адресов .....	21
4.2.2 Черный список MAC-адресов.....	22
4.3 Фильтрация IP-адресов .....	23
4.3.1 Белый список IP-адресов.....	23
4.3.2 Черный список IP-адресов .....	25
4.4 Фильтрация URL-адресов .....	26
4.4.1 Белый список URL-адресов.....	26
4.4.2 Черный список URL-адресов .....	28
4.5 Управление доступом к услугам .....	29
4.5.1 Список управления доступом .....	29
<b>5 Настройки NAT.....</b>	<b>30</b>
5.1 Настройки DMZ .....	30
5.1.1 DMZ .....	30
5.2 Отображение портов .....	30
5.2.1 Отображение портов .....	31
5.3 Технология UPnP .....	32
5.3.1 UPnP .....	32
5.3.2 Отображение портов UPnP .....	33
5.4 SIP ALG .....	33
<b>6 Управление USB-устройствами.....</b>	<b>34</b>
6.1 Настройки сервера.....	34

6.1.1 Сетевые сервера .....	34
6.1.2 USB-устройство хранения данных .....	34
6.2 Настройки пользователя .....	34
6.2.1 Список пользователей .....	35
6.3 FTP-загрузка .....	35
6.3.1 История загрузок .....	36
<b>7 Система .....</b>	<b>37</b>
7.1 Информация об устройстве .....	37
7.2 Сброс .....	37
7.2.1 Перезагрузить .....	37
7.2.2 Восстановление .....	37
7.3 Резервирование и загрузка .....	38
7.3.1 Резервирование .....	38
7.3.2 Загрузка .....	38
7.4 Модернизация .....	39
7.4.1 Локальное обновление .....	39
7.4.2 Http-обновление .....	39
7.5 Изменение пароля .....	40
7.6 Дата и время .....	40
7.6.1 Настройки .....	40
7.7 Проверка .....	41
7.7.1 Ping-тестирование .....	41
7.7.2 Трассировка маршрутов .....	41
7.7.3 Проверка системы .....	42
7.8 Настройки антенны .....	42
7.8.1 Использование встроенной антенны .....	42
7.8.2 Использование внешней антенны .....	42
7.9 Журнал .....	43
<b>8 Часто задаваемые вопросы .....</b>	<b>44</b>
<b>9 Аббревиатуры и сокращения .....</b>	<b>45</b>

# 1 Начало работы

## 1.1 Введение

В этом документе в качестве оборудования заказчика (CPE) рассматривается маршрутизатор. Пожалуйста, внимательно ознакомьтесь со следующими значками для правильного и безопасного использования маршрутизатора.



Дополнительная информация по данной теме.



Дополнительные методы или ярлыки для выполнения каких-либо действий.



Предупреждение о потенциальных проблемах или правилах, которые должны быть указаны.

## 1.2 Требования к конфигурации Вашего компьютера

Ваш компьютер должен соответствовать требованиям маршрутизатора. В противном случае, рабочие характеристики маршрутизатора будут ухудшены.

Пункт	Требование
ЦП	Pentium 500 МГц или выше
Память	128 Мб ОЗУ или выше
Жесткий диск	Доступно 50 Мб
Операционная система	<ul style="list-style-type: none"><li>• Microsoft: Windows XP, Windows Vista или Windows 7</li><li>• Mac: Mac OS X</li></ul>
Разрешение экрана	1024 x 768 пикселей или выше

Пункт	Требование
Браузер	<ul style="list-style-type: none"><li>• Internet Explorer 7.0 или более поздняя версия</li><li>• Firefox 3.5 или более поздняя версия</li><li>• Opera 10 или более поздняя версия</li><li>• Safari 5 или более поздняя версия</li><li>• Chrome 9 или более поздняя версия</li></ul>

## 1.3 Вход на веб-страницу управления устройством

Веб-страница управления устройством позволяет Вам выполнить конфигурацию и управлять маршрутизатором при помощи браузера.

Далее приведена процедура регистрации на веб-странице управления устройством в ОС Windows XP и программе Internet Explorer 7.0.

1. Подключите маршрутизатор.
2. IP-адрес Вашего компьютера должен находиться в том же сегменте сети, что и IP-адрес маршрутизатора.



По умолчанию IP-адрес маршрутизатора - 192.168.1.1, а маска подсети - 255.255.255.0. Рекомендуется, чтобы IP-адрес назначался автоматически и система доменных имен (DNS) тоже присваивала свое значение автоматически.

3. Запустите программу Internet Explorer, введите в адресной строке <http://192.168.1.1> и нажмите на клавиатуре **Enter**.
4. Введите правильный пароль и нажмите **Вход**. После проверки пароля Вы сможете войти на веб-страницу управления устройством.

# 2 Статус

## 2.1 Интернет

### 2.1.1 Статус

Для просмотра статуса подключения глобальной сети (WAN) выполните следующее:

1. Выберите **Статус > Интернет**.
2. Посмотрите статус подключения WAN.

### 2.1.2 Статистика

Для просмотра статистики порта WAN выполните следующее:

1. Выберите **Статус > Интернет**.
2. Посмотрите статистику порта WAN, включая скорость загрузки и выгрузки, объем загрузки и выгрузки, общий объем трафика, а также продолжительность работы в сети.

## 2.2 LAN

### 2.2.1 Статус

Для просмотра статуса подключения локальной сети (LAN) выполните следующее:

1. Выберите **Статус > LAN**.
2. Посмотрите статус подключения LAN, включая IP-адрес, адрес управления доступом к среде (MAC-адрес), сервер протокола динамической конфигурации хоста (DHCP), а также порты LAN (LAN1, LAN2, LAN3 и LAN4).

### 2.2.2 Статистика

Для просмотра статистики портов LAN выполните следующее:

1. Выберите **Статус > LAN**.
2. Посмотрите статистику по портам LAN, включая общий объем трафика, количество пакетов, количество ошибочных пакетов, а также количество отброшенных пакетов, переданных и полученных на портах LAN.



## 2.3 WLAN

### 2.3.1 Статус

Для просмотра статуса подключения беспроводной локальной сети (WLAN) выполните следующее:

1. Выберите **Статус > WLAN**.
2. Посмотрите статус подключения WLAN, включая SSID, IP-адрес, MAC-адрес, режим широковещания и режим беспроводного шифрования.

### 2.3.2 Статистика

Для просмотра статистики портов WLAN выполните следующее:

1. Выберите **Статус > WLAN**.
2. Посмотрите статистику по портам WLAN, включая общий объем трафика, количество пакетов, количество ошибочных пакетов, а также количество отброшенных пакетов, переданных и полученных на портах WLAN.

# 3 Общие настройки

## 3.1 Настройки SIM-карты

Вы можете управлять PIN-кодом на странице управления SIM-картой и выполнять следующие операции:

- Включение или отключение проверки PIN-кода
- Проверка PIN-кода
- Изменение PIN-кода
- Установка автоматической проверки PIN-кода

### 3.1.1 Просмотр статуса SIM-карты

Для просмотра статуса SIM-карты выполните следующее:

1. Выберите **Общие настройки > Настройки SIM-карты**.  
На экране появится страница **Управление PIN-кодом**.
2. Посмотрите статус SIM-карты в окне **Статус SIM-карты**.

### 3.1.2 Включение проверки PIN-кода

Для включения проверки PIN-кода выполните следующее:

1. Выберите **Общие настройки > Настройки SIM-карты**.  
На экране появится страница **Управление PIN-кодом**.
2. Установите для параметра **Проверка PIN-кода** значение **Включить**.
3. Введите PIN-код (от четырех до восьми цифр) в поле **Введите PIN-код**.
4. Нажмите **Подтвердить**.

### 3.1.3 Отключение проверки PIN-кода

Для отключения проверки PIN-кода выполните следующее:

1. Выберите **Общие настройки > Настройки SIM-карты**.  
На экране появится страница **Управление PIN-кодом**.

2. Установите параметру **Проверка PIN-кода** значение **Отключить**.
3. Введите PIN-код (от четырех до восьми цифр) в поле **Введите PIN-код**.
4. Нажмите **Подтвердить**.

### 3.1.4 Проверка PIN-кода

Если функция проверки PIN-кода включена, то необходимо выполнить проверку PIN-кода. Для проверки PIN-кода выполните следующее:

1. Выберите **Общие настройки > Настройки SIM-карты**.  
На экране появится страница **Управление PIN-кодом**.
2. Введите PIN-код (от четырех до восьми цифр) в поле **Проверьте PIN-код**.
3. Нажмите **Подтвердить**.

### 3.1.5 Изменение PIN-кода

PIN-код можно изменить, только если включена проверка PIN-кода, и PIN-код прошел проверку.

Для изменения PIN-кода выполните следующее:

1. Выберите **Общие настройки > Настройки SIM-карты**.  
На экране появится страница **Управление PIN-кодом**.
2. Установите параметру **Проверка PIN-кода** значение **Включить**.
3. Установите параметру **Изменение** значение **Включить**.
4. Введите текущий PIN-код (от четырех до восьми цифр) в поле **PIN-код**.
5. Введите новый PIN-код (от четырех до восьми цифр) в поле **Новый PIN-код**.
6. Введите снова новый PIN-код в поле **Подтвердите PIN-код**.
7. Нажмите **Подтвердить**.

### 3.1.6 Установка автоматической проверки PIN-кода

Вы можете включить или отключить автоматическую проверку PIN-кода. Если автоматическая проверка включена, то после перезагрузки маршрутизатор будет автоматически проверять PIN-код. Данная функция может быть включена, только если включена функция проверки PIN-кода, и PIN-код прошел проверку.

Для включения функции автоматической проверки PIN-кода выполните следующее:

1. Выберите **Общие настройки > Настройки SIM-карты**.  
На экране появится страница **Управление PIN-кодом**.
2. Установите значение параметра **Проверка PIN-кода** как **Включить**.
3. Установите значение параметра **Сохранить мой PIN-код** как **Включить**.
4. Нажмите **Подтвердить**.

### 3.1.7 Проверка PUK-кода

Если проверка PIN-кода включена, и PIN-код не прошел проверку последовательно в течение трех раз, то PIN-код будет заблокирован. В данном случае необходимо выполнить проверку PUK-кода и изменить PIN-код.

Для проверки PUK-кода, выполните следующее:

1. Выберите **Общие настройки > Настройки SIM-карты**.  
На экране появится страница **Управление PIN-кодом**.
2. Введите PUK-код в окне **PUK-код**.
3. Введите новый PIN-код в поле **Новый PIN-код**.
4. Введите снова новый PIN-код в поле **Подтвердите PIN-код**.
5. Нажмите **Подтвердить**.

## 3.2 Настройки Интернет

На данной странице Вы можете выполнить настройки сети Интернет.

### 3.2.1 Выбор сетевого режима

Вы можете выбрать сетевой режим, для того чтобы маршрутизатор получал доступ к различным сетям. **Сетевой режим** может иметь значения **АВТО**, **Только 4G**, **Только 3G** или **Только 2G**.

Для выбора сетевого режима выполните следующее:

1. Вставьте работающую SIM-карту в маршрутизатор и убедитесь в том, что антенна работает нормально.
2. Включите маршрутизатор и войдите на веб-интерфейс пользователя как пользователь Администратор.
3. Выберите **Общие настройки > Настройки Интернет**.

Появится страница **Настройки Интернет**.

4. Установите для параметра **Сетевой режим** одно из значений, приведенных в следующей таблице:

Значение параметра	Описание
АВТО	Маршрутизатор автоматически выбирает рабочий режим с приоритетом сети 4G, сети 3G и сети 2G.
Только 4G	Маршрутизатор получит доступ к сети 4G.
Только 3G	Маршрутизатор получит доступ к сети 3G.

Значение параметра	Описание
Только 2G	Маршрутизатор получит доступ к сети 2G.

- Нажмите **Подтвердить**.

### 3.2.2 Выбор режима подключения

На данной странице Вы можете выбрать режим подключения к сети. Режим **Всегда Вкл.** означает, что подключение всегда включено. Если позволяют условия, то маршрутизатор всегда подключается к сети Интернет. Режим **Вручную** означает, что Вы можете подключить/разъединить маршрутизатор к/от сети Интернет вручную.

Для выбора режима подключения к сети выполните следующее:

- Выберите **Общие настройки > Настройки Интернет**. Появится страница **Настройки Интернет**.
- Установите для параметра **Режим подключения** одно из значений, приведенных в следующей таблице:

Значение параметра	Описание
Всегда Вкл.	Если сеть разъединена, маршрутизатор получает доступ к сети автоматически.
Вручную	После запуска маршрутизатор не подключен к сети Интернет. Вы можете подключать/отключать маршрутизатор к/от сети Интернет вручную.

- Нажмите **Подтвердить**.

### 3.2.3 Выбор APN для передачи данных

Вы можете установить группу коммутируемых параметров точки доступа для передачи данных (APN) с тем, чтобы маршрутизатор получал доступ к сети Интернет.

Для настройки параметров выполните следующее:

- Выберите **Общие настройки > Настройки Интернет**.  
Появится страница **Настройки Интернет**.
- Установите **APN для передачи данных**, а затем установите группу коммутируемых параметров, соответствующих APN для передачи данных.
- Нажмите **Подтвердить**.

### 3.2.4 Создание профиля APN

Для создания группы коммутируемых параметров APN выполните следующее:

- Выберите **Общие настройки > Настройки Интернет**.

Появится страница **Настройки Интернет**.

2. На странице **Настройки Интернет** выберите **Редактировать профиль APN**.  
На экране появится страница **Профиль APN**.
3. Нажмите **Добавить профиль APN**.
4. На появившейся странице введите **APN, Набрать номер, Имя пользователя и Пароль**.
5. Установите для параметра **Аутентификация** значение **АВТО, PAP** или **CHAP**.
6. Нажмите **Подтвердить**.

### 3.2.5 Изменение профиля APN

Для изменения коммутируемых параметров APN выполните следующее:

1. Выберите **Общие настройки > Настройки Интернет**.  
Появится страница **Настройки Интернет**.
2. На странице **Настройки Интернет** выберите **Редактировать профиль APN**.  
На экране появится страница **Профиль APN**.
3. При входе в изменяемый **Профиль APN** нажмите **Редактировать**.
4. На появившейся странице введите **APN, Набрать номер, Имя пользователя и Пароль**.
5. Установите для параметра **Аутентификация** значение **АВТО, PAP** или **CHAP**.
6. Нажмите **Подтвердить**.

### 3.2.6 Удаление профиля APN

Для удаления существующих коммутируемых параметров APN выполните следующее:

1. Выберите **Общие настройки > Настройки Интернет**.  
Появится страница **Настройки Интернет**.
2. На странице **Настройки Интернет** выберите **Редактировать профиль APN**.  
На экране появится страница **Профиль APN**.
3. При входе на удаляемый **Профиль APN** нажмите **Удалить**. На экране появится сообщение.
4. Нажмите **ОК**.

## 3.3 Настройки DHCP

Локальная сеть (LAN) – это совместно используемая система связи, в которой в непосредственной близости имеется более одного устройства.

При правильной настройке локальной сети сетевые устройства, например компьютеры, могут обмениваться данными по локальной сети LAN при помощи маршрутизатора.

### 3.3.1 Настройки хоста LAN

По умолчанию IP-адрес - 192.168.1.1, а маска подсети - 255.255.255.0. Вы можете изменить IP-адрес на другой индивидуальный IP-адрес, который достаточно просто запомнить. При этом проверьте, чтобы IP-адрес был уникальным в Вашей сети. Если Вы измените IP-адрес маршрутизатора, то Вам необходимо получить доступ к веб-утилите с новым IP-адресом.

Для изменения IP-адреса и маски подсети маршрутизатора выполните следующее:

1. Выберите **Общие настройки > Настройки DHCP**.  
На экране появится страница **Настройки DHCP**.
2. Установите **IP-адрес**.
3. Установите параметр **Маска подсети**.
4. Выберите флажок **Включить** после параметра **DHCP-сервер**.
5. Нажмите **Подтвердить**.

### 3.3.2 Настройки DHCP

DHCP позволяет отдельным клиентам автоматически получать конфигурацию TCP/IP при запуске с сервера.

Вы можете сконфигурировать маршрутизатор как сервер DHCP или отключить его, когда маршрутизатор работает в режиме маршрутизации.

При конфигурировании в качестве сервера DHCP маршрутизатор автоматически предоставляет конфигурацию TCP/IP для клиентов LAN, которые поддерживают возможности клиента DHCP. Если услуги DHCP-сервера отключены, Вы должны иметь другой сервер DHCP в вашей локальной сети LAN, или каждый клиент должен быть настроен вручную.

Для конфигурирования настроек DHCP выполните следующее:

1. Выберите **Общие настройки > Настройки DHCP**. На экране появится страница **Настройки DHCP**.
2. Выберите флажок **Включить** после параметра **DHCP-сервер**.
3. Установите **Начальный IP-адрес**.



Данный IP-адрес должен отличаться от IP-адреса, который установлен на странице **Настройки хоста LAN**, однако они должны находиться в одном сегменте сети.

4. Установите **Конечный IP-адрес**.



Данный IP-адрес должен отличаться от IP-адреса, который установлен на странице **Настройки хоста LAN**, однако они должны находиться в одном сегменте сети.

Конечный IP-адрес должен быть меньше или равен начальному IP-адресу.

5. Установите значение параметра **Срок действия**.



Параметр может иметь значение от 1 до 10 080 минут.

6. Нажмите **Подтвердить**.

В списке устройств представлена информация обо всех активных устройствах.

Для просмотра списка устройств выполните следующее:

1. Выберите **Общие настройки > Настройки DHCP**. Нажмите **Доступные устройства**. На экране появится страница **Доступные устройства**.
2. Просмотрите список устройств. Он включает **Имя ПК**, **MAC-адрес**, **IP-адрес** и **Срок действия**. **Срок действия** означает оставшийся срок действия динамического сервера DHCP. Если статический IP-адрес привязан, то **Срок действия** и **Имя ПК** отображаются как **NA** и **Неизвестно** соответственно.

## 3.4 Настройки WLAN

### 3.4.1 Общие настройки

Основные параметры Wi-Fi влияют на производительность Wi-Fi. Эти настройки помогут Вам достичь максимальной скорости благодаря оптимальной производительности.

Для конфигурирования основных настроек WLAN выполните следующее:


1. Выберите **Общие настройки > Настройки WLAN**.  
На экране будет отображена страница **Настройки WLAN**.
2. Выберите флажок **Включить** после параметра **Включить WLAN**.
3. Установите для параметра **Режим** одно из значений, описанных в следующей таблице:

Значение параметра	Описание
802.11b/g/n	Станция Wi-Fi может подключаться к маршрутизатору в режимах 802.11b, 802.11g или 802.11n. Если станция подключается к маршрутизатору в режиме 802.11n, то используется режим шифрования AES.
802.11b/g	Станция Wi-Fi может подключаться к маршрутизатору в режимах 802.11b или 802.11g.
802.11b	Станция Wi-Fi может подключаться к маршрутизатору в режиме 802.11b.




Значение параметра	Описание
802.11g	Станция Wi-Fi может подключаться к маршрутизатору в режиме 802.11g.
802.11n	Станция Wi-Fi может подключаться к маршрутизатору в режиме 802.11n.


#### 4. Установите параметр **Код страны**.

 Параметр **Канал** может отличаться в зависимости от выбранной страны.


#### 5. Установите параметр **Канал**.

 **Авто** означает, что выбирается канал с наилучшим качеством сигнала. Значения от **1** до **13** указывают на выбранный канал.


#### 6. Установите параметр **Полоса пропускания 802.11n**.

 Если данный параметр имеет значение **20 МГц**, то 802.11n поддерживает только полосу пропускания 20 МГц.  
Если данный параметр имеет значение **20/40 МГц**, то 802.11n поддерживает полосу пропускания 20 МГц или 40 МГц.  
Если параметр **Режим** имеет значение **802.11b** или **802.11g**, то нет никакой необходимости устанавливать данный параметр.

#### 7. Установите параметр **Скорость**.

 Параметр **Скорость** различается в зависимости от выбранного режима.  
Если параметр **Скорость** имеет значение **Авто**, то станция Wi-Fi подключается к маршрутизатору при помощи канала с наилучшим качеством сигнала.  
Если скорость определена, то станция подключается к маршрутизатору на определенной скорости. Если условия канала не соответствуют определенным требованиям, то это может оказать определенное влияние на характеристики подключения.

#### 8. Установите параметр **Мощность передачи**.

 Если данный параметр имеет значение **90% (рекомендуемая)**, то станция Wi-Fi осуществляет передачу на оптимальной мощности.  
Если данный параметр имеет значение **100%**, то станция Wi-Fi осуществляет передачу на полной мощности.

Если данный параметр имеет значение **80%, 60%, 30% или 5%**, то станция Wi-Fi осуществляет передачу на низкой мощности. Если станция Wi-Fi находится вдали от маршрутизатора, то она может не получить доступ к маршрутизатору.

9. Нажмите **Подтвердить**.

### 3.4.2 Профиль интерфейса

После конфигурирования маршрутизатора на странице **Профиль интерфейса** станция Wi-Fi подключается к маршрутизатору, согласно заранее установленным правилам, что улучшает безопасность доступа.

Для конфигурирования маршрутизатора на странице **Профиль интерфейса** выполните следующее:

1. Выберите **Общие настройки > Настройки WLAN**.

На экране будет отображена страница **Настройки WLAN**.

2. Установите **SSID**.



Данный параметр включает от 1 до 32 символов ASCII.

Станция Wi-Fi подключается к маршрутизатору при помощи функции поиска SSID.

3. Установите значение параметра **Максимальное количество разрешенных устройств**.



Данный параметр указывает на максимальное количество станций Wi-Fi, которые могут подключиться к маршрутизатору.

К маршрутизатору может подключиться максимум 32 станции.

4. Выберите флажок **Включить** после параметра **Скрыть широковещание**.

SSID будет скрыт. В данном случае станция не сможет обнаружить информацию Wi-Fi маршрутизатора.

5. Выберите флажок **Включить** после параметра **Изоляция точки доступа**. Станции смогут подключаться к маршрутизатору, однако не смогут взаимодействовать друг с другом.

6. Установите значение параметра **Безопасность**.



Если данный параметр имеет значение **Отсутствует (не рекомендуемая)**, то станция Wi-Fi осуществляет подключение к маршрутизатору напрямую. Это несет определенный риск системе безопасности.

Если данный параметр имеет значение **WEP**, то станция Wi-Fi подключается к маршрутизатору в режиме шифрования на базе веб.

Если данный параметр имеет значение **WPA-PSK**, то станция Wi-Fi подключается к маршрутизатору в режиме шифрования WPA-PSK.

Если данный параметр имеет значение **WPA2-PSK (рекомендуется)**, то станция Wi-Fi подключается к маршрутизатору в режиме шифрования WPA2-PSK. Рекомендуется использовать данный режим, так как он имеет высокий уровень безопасности.

Если данный параметр имеет значение **WPA-PSK+WPA2-PSK**, то станция

Wi-Fi подключается к маршрутизатору в режиме шифрования WPA-PSK или WPA2-PSK.

7. Установите режим шифрования.

Если...	Установлен как	Описание
WEP	Базовая аутентификация	<ul style="list-style-type: none"> <li>● <b>Общая аутентификация:</b> Станция подключается к маршрутизатору в общем режиме аутентификации.</li> <li>● <b>Открытая аутентификация:</b> Станция подключается к маршрутизатору в открытом режиме аутентификации.</li> <li>● <b>Двойная аутентификация:</b> Станция подключается к маршрутизатору в общем или открытом режиме аутентификации.</li> </ul>
	Длина ключа шифрования	<ul style="list-style-type: none"> <li>● <b>128 бит:</b> Может быть введено только 13 символов ASCII или 26 шестнадцатеричных символа в полях <b>Ключ 1~Ключ 4</b>.</li> <li>● <b>64 бита:</b> Может быть введено только 5 символов ASCII или 10 шестнадцатеричных символа в полях <b>Ключ 1~Ключ 4</b>.</li> </ul>
	Текущий индекс ключа	Он может быть установлен как <b>1, 2, 3</b> или <b>4</b> . После выбора индекса ключа, соответствующий ключ вступит в силу.
WPA-PSK	Предварительный ключ WPA	Может быть введено от 8 до 63 символов ASCII или от 8 до 64 шестнадцатеричных символов.
	Шифрование WPA	Данный параметр может иметь значение <b>TKIP+AES</b> , <b>AES</b> или <b>TKIP</b> .
WPA2-PSK (рекомендуется)	Предварительный ключ WPA	Может быть введено от 8 до 63 символов ASCII или от 8 до 64 шестнадцатеричных символов.
	Шифрование WPA	Данный параметр может иметь значение <b>TKIP+AES</b> , <b>AES</b> или <b>TKIP</b> .
WPA-PSK +WPA2-PSK	Предварительный ключ WPA	Может быть введено от 8 до 63 символов ASCII или от 8 до 64 шестнадцатеричных символов.
	Шифрование WPA	Данный параметр может иметь значение <b>TKIP+AES</b> , <b>AES</b> или <b>TKIP</b> .

8. Нажмите **Подтвердить**.

## 3.5 Безопасное подключение к WLAN

### 3.5.1 Настройка безопасного подключения к WLAN

Защищенное беспроводное соединение Wi-Fi (WPS) позволяет с легкостью добавлять беспроводных клиентов к сети, без какой-либо специальной настройки параметров беспроводной сети, например, SSID, режима безопасности и кодовой фразы. Вы можете добавить беспроводного клиента, либо нажав на кнопку, либо используя PIN-код.

Если Вы используете PIN-код, то Вы можете нажать на кнопку WPS маршрутизатора и кнопку WPS на стороне клиента для подключения к сети. Если Вы используете кнопку, то Вы не можете одновременно использовать и PIN-код.

Для конфигурирования настроек WPS WLAN, выполните следующее:

1. Выберите **Общие настройки > Безопасное подключение к WLAN**.

На экране будет отображена страница **Безопасное подключение к WLAN**.

2. Установите флажок **Включить** после параметра **Безопасное подключение**.
3. Установите **Режим подключения**.



Если данный параметр имеет значение **PBC**, то после нажатия кнопки WPS на станции и затем уже на маршрутизаторе, станция будет подключаться к маршрутизатору.

Если данный параметр имеет значение **PIN-код маршрутизатора**, то станция может подключаться к маршрутизатору после правильного введения PIN-кода.

Поддерживается только шифрование WPA или WPA2.

4. Нажмите **Подтвердить**.

## 3.6 WLAN Multi SSID

Данная функция поддерживает максимум четыре SSID. Вы можете установить параметры для этих четырех SSID, например, настроить различные скорости и режимы. По умолчанию, SSID с индексом 1 включен и не может быть отключен, а SSID с индексами 2, 3 и 4 отключены.

### 3.6.1 Список SSID

На странице **Список SSID** представлена информация о четырех конфигурируемых SSID. Для конфигурирования SSID выполните следующее:

1. Выберите **Общие настройки > WLAN Multi SSID**.  
На экране появится страница **Список SSID**.
2. Выберите конфигурируемый SSID и нажмите **Редактировать**.
3. Выберите флажок **Включить** после параметра **Включить R/p**.
4. Установите **SSID**.



SSID должен содержать от 1 до 32 символов ASCII. SSID не может содержать

следующие специальные символы: '/', ' ', '=', '"', '\', '&'.

5. Установите значение параметра **Максимальное количество разрешенных устройств**.



Количество разрешенных устройств должно быть целым числом и находиться в диапазоне от 1 до 32.

6. Выберите флажок **Включить** после параметра **Скрыть широковещание**.
7. Установите значение параметра **Изоляция точки доступа**. Если Вы выберете флажок **Включить**, то станции смогут подключаться к маршрутизатору, но не смогут взаимодействовать друг с другом. Если флажок не выбран, то станции смогут подключаться к маршрутизатору и одновременно взаимодействовать друг с другом.
8. Установите значение параметра **Безопасность**. Если параметр **Режим** имеет значение **802.11n** на странице **Общие настройки**, то параметр **Безопасность** может иметь значения **WPA-PSK**, **WPA2-PSK**, или для параметра может быть задан какой-либо другой режим шифрования.

Если параметр **Безопасность** имеет значение **WPA-PSK**, **WPA2-PSK** или **WPA-PSK+WPA2-PSK**, то должны быть установлены параметры **Предварительный ключ WPA** и **Шифрование WPA**.



Предварительный ключ WPA должен включать от 8 до 63 символов ASCII или 64 шестнадцатеричных символа.

Если параметр **Безопасность** имеет значение **WEP**, то необходимо установить и параметры **Базовая аутентификация**, **Длина ключа шифрования** и **Текущий индекс ключа**.

Если параметр **Длина ключа шифрования** имеет значение **128-бит**, то параметр **Предварительный ключ WPA** должен включать от 8 до 63 символов ASCII или 64 шестнадцатеричных символа.

Если параметр **Длина ключа шифрования** имеет значение **64-бит**, то 64-битный ключ шифрования должен включать 5 символов ASCII или 10 шестнадцатеричных символа.

9. Нажмите **Подтвердить**.

## 3.7 Ограничение доступа WLAN

### 3.7.1 Управление MAC-адресами WLAN

Данная функция позволяет Вам управлять доступом к маршрутизатору. Вы можете установить политики ограничения доступа для каждого SSID.

MAC-адрес каждого SSID может принимать такие значения, как **Отключен**, **Черный список** или **Белый список**.

- Если параметр **MAC-адрес SSID1** имеет значение **Отключен**, то ограничение доступа не вступает в силу.
- Если параметр **MAC-адрес SSID1** имеет значение **Черный список**, то только устройства, которые не находятся в черном списке смогут получить доступ к SSID.

- Если параметр **MAC-адрес SSID1** имеет значение **Белый список**, то только устройства, которые находятся в белом списке смогут подключиться к SSID.

Для конфигурирования настроек управления MAC-адресами WLAN, выполните следующее:

1. Выберите **Общие настройки > Ограничение доступа WLAN**.

На экране будет отображена страница **Управление MAC-адресами WLAN**.

2. Установите **MAC-адрес SSID1**.
3. Установите **MAC-адрес SSID2**.
4. Установите **MAC-адрес SSID3**.
5. Установите **MAC-адрес SSID4**.
6. Нажмите **Подтвердить**.

## 3.7.2 Список настроек

Данная функция позволяет установить политики доступа SSID на основе MAC-адресов. Установите SSID, соответствующий MAC-адресу.

Для добавления пункта к списку настроек выполните следующее:

1. Выберите **Общие настройки > Ограничение доступа WLAN**.

На экране будет отображена страница **Список MAC-адресов WLAN**.

2. Выберите **Список настроек**. На экране будет отображена страница **Список доступа WLAN**.
3. Нажмите **Добавить пункт**.
4. Установите **MAC-адрес**.
5. Для активации MAC-адреса для SSID1 установите флажок **Включить** после поля **Для SSID1**. Все операции с SSID2, SSID3 и SSID4 подобны данной процедуре.
6. Нажмите **Подтвердить**.

Для изменения пункта в списке настроек, выполните следующее:

1. Выберите **Общие настройки > Ограничение доступа WLAN**.

На экране будет отображена страница **Список MAC-адресов WLAN**.

2. Выберите **Список настроек**. На экране будет отображена страница **Список доступа WLAN**.
3. При входе нажмите **Редактировать**.
4. На появившейся странице введите **MAC-адрес**.
5. Для активации MAC-адреса для SSID1 выберите флажок **Включить** после поля **Для SSID1**. Все операции с SSID2, SSID3 и SSID4 подобны данной процедуре.
6. Нажмите **Подтвердить**.

Для удаления пункта из списка настроек выполните следующее:

1. Выберите **Общие настройки > Ограничение доступа WLAN**.  
На экране будет отображена страница **Список MAC-адресов WLAN**.
2. Выберите **Список настроек**. На экране будет отображена страница **Список доступа WLAN**.
3. При входе нажмите **Удалить**. На экране появится сообщение.
4. Нажмите **ОК**.

Для удаления всех пунктов из списка настроек выполните следующее:

1. Выберите **Общие настройки > Ограничение доступа WLAN**.  
На экране будет отображена страница **Список MAC-адресов WLAN**.
2. Выберите **Список настроек**. На экране будет отображена страница **Список доступа WLAN**.
3. Выберите **Удалить все**. На экране появится сообщение.
4. Нажмите **ОК**.

## 3.8 MTU в сети Интернет

Максимальный размер блока передачи (MTU) определяется как максимальный размер пакета (в байтах) на уровне протокола связи. Он взаимодействует с портами связи, например, сетевыми картами и последовательными портами.

Для установки MTU выполните следующее:

1. Выберите **Общие настройки > MTU в сети Интернет**.  
Появится страница **MTU в сети Интернет**.
2. Установите значение **MTU в сети Интернет** в пределах от 576 до 1500.
3. Нажмите **Подтвердить**.

## 3.9 Настройки маршрутизации

### 3.9.1 Динамическая маршрутизация

Данная функция включается, когда в сети Интранет используются каскадные маршрутизаторы и каскадные маршрутизаторы соответствуют требованиям протокола маршрутизации информации (RIP). На данной странице Вы можете включить или отключить RIP, установить версию RIP, а также рабочий режим RIP.

Для конфигурирования настроек динамической маршрутизации выполните следующее:

1. Выберите **Общие настройки > Настройки маршрутизации**.  
На экране появится страница **Настройки маршрутизации**.

2. Нажмите **Настройки** в правом верхнем углу страницы **Динамическая маршрутизация**.  
На экране появится окно параметров конфигурационного элемента.
3. Установите флажок в поле **Включить** после параметра **Включить Rip**.
4. Установите параметр **Операция**. Если он имеет значение **Активный**, то это означает, что маршрутизатор активно уведомляет окружающие маршрутизаторы об изменении маршрута. Если параметр имеет значение **Пассивный**, то маршруты будут меняться пассивным образом.
5. Установите для параметра **Версия** значение **Rip v1**, **Rip v2** или **Rip v1/Rip v2**.
6. Нажмите **Подтвердить**.

### 3.9.2 Статическая маршрутизация

Функции статической маршрутизации аналогичны динамической маршрутизации. Разница заключается в том, что параметры маршрута добавляются вручную с тем, чтобы они согласовались друг с другом и маршруты были достижимыми.

- Если IP-адрес каскадного маршрутизатора является фиксированным, то рекомендуется использовать статическую маршрутизацию.
- Если IP-адрес каскадного маршрутизатора меняется со временем, то рекомендуется использовать динамическую маршрутизацию.

Для конфигурирования настроек статической маршрутизации выполните следующее:

1. Выберите **Общие настройки > Настройки маршрутизации**. На экране появится страница **Статическая маршрутизация**.
2. Нажмите **Добавить пункт** в правом верхнем углу страницы **Статическая маршрутизация**. На экране появится окно параметров конфигурационного элемента.
3. Установите **IP-адрес получателя**.
4. Установите параметр **Маска подсети**.
5. Установите **IP-адрес маршрутизатора**. Данный IP-адрес получается от маршрутизатора и используется для передачи на каскадные устройства. Он должен быть также доступен.
6. Нажмите **Подтвердить**.



# 4 Настройки безопасности

## 4.1 Настройки брандмауэра

### 4.1.1 Уровень брандмауэра

На данной странице приведен порядок настройки уровня брандмауэра. Если параметр **Уровень брандмауэра** имеет значение **Пользовательский**, то конфигурация может быть изменена.

Для того чтобы установить уровень брандмауэра, выполните следующее:

1. Выберите **Настройки безопасности > Настройки брандмауэра**.

На экране появится страница **Настройки брандмауэра**.

2. Установите для параметра **Уровень брандмауэра** одно из значений, описанных в следующей таблице:

Значение параметра	Описание
Отключить	Брандмауэр отключен.
Высокий	Параметры <b>Фильтр MAC-адресов</b> , <b>Фильтр IP-адресов</b> и <b>Фильтр URL-адресов</b> имеют значение <b>Белый список</b> .
Средний	Параметры <b>Фильтр MAC-адресов</b> и <b>Фильтр IP-адресов</b> имеют значение <b>Белый список</b> . Параметр <b>Фильтр URL-адресов</b> имеет значение <b>Черный список</b> .
Низкий	Параметры <b>Фильтр MAC-адресов</b> , <b>Фильтр IP-адресов</b> и <b>Фильтр URL-адресов</b> имеют значение <b>Черный список</b> .
Пользовательский	Параметры <b>Фильтр MAC-адресов</b> , <b>Фильтр IP-адресов</b> и <b>Фильтр URL-адресов</b> могут настраиваться.

3. Нажмите **Подтвердить**.

Для установки функций фильтрации на брандмауэре выполните следующее:

1. Выберите **Настройки безопасности > Настройки брандмауэра**.  
На экране появится страница **Настройки брандмауэра**.
2. Установите значение параметра **Уровень брандмауэра** как **Пользовательский**.
3. Установите **Фильтр MAC-адресов**.
4. Установите **Фильтр IP-адресов**.
5. Установите **Фильтр URL-адресов**.
6. Нажмите **Подтвердить**.

## 4.2 Фильтрация MAC-адресов

Данные могут быть отфильтрованы по MAC-адресу. На данной странице Вы можете сконфигурировать только правила фильтрации MAC-адресов.

### 4.2.1 Белый список MAC-адресов

Для добавления правила фильтрации в белый список MAC-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация MAC-адресов**.  
На экране будет отображена страница **Фильтрация MAC-адресов**.
2. Установите **Режим фильтрации MAC-адресов** как **Белый список**.
3. Нажмите **Добавить пункт**.
4. На появившейся странице введите **MAC-адрес**.
5. Нажмите **Подтвердить**.

Для изменения правила фильтрации в белом списке MAC-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация MAC-адресов**.  
На экране будет отображена страница **Фильтрация MAC-адресов**.
2. Установите **Режим фильтрации MAC-адресов** как **Белый список**.
3. При входе нажмите **Редактировать**.
4. На появившейся странице введите **MAC-адрес**.
5. Нажмите **Подтвердить**.

Для удаления правила фильтрации в белом списке MAC-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация MAC-адресов**.  
На экране будет отображена страница **Фильтрация MAC-адресов**.
2. Установите **Режим фильтрации MAC-адресов** как **Белый список**.
3. При входе нажмите **Удалить**. На экране появится сообщение.
4. Нажмите **ОК**.

Для удаления всех правил фильтрации в белом списке MAC-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация MAC-адресов**.  
На экране будет отображена страница **Фильтрация MAC-адресов**.
2. Установите **Режим фильтрации MAC-адресов** как **Белый список**.
3. Выберите **Удалить все**.
4. Нажмите **ОК**.

## 4.2.2 Черный список MAC-адресов

Для добавления правила фильтрации в черный список MAC-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация MAC-адресов**.  
На экране будет отображена страница **Фильтрация MAC-адресов**.
2. Установите **Режим фильтрации MAC-адресов** как **Черный список**.
3. Нажмите **Добавить пункт**.
4. На появившейся странице введите **MAC-адрес**.
5. Нажмите **Подтвердить**.

Для изменения правила фильтрации в черном списке MAC-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация MAC-адресов**.  
На экране будет отображена страница **Фильтрация MAC-адресов**.
2. Установите **Режим фильтрации MAC-адресов** как **Черный список**.
3. При входе нажмите **Редактировать**.
4. На появившейся странице введите **MAC-адрес**.

5. Нажмите **Подтвердить**.

Для удаления правила фильтрации в черном списке MAC-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация MAC-адресов**.

На экране будет отображена страница **Фильтрация MAC-адресов**.

2. Установите **Режим фильтрации MAC-адресов** как **Черный список**.

3. При входе нажмите **Удалить**. На экране появится сообщение.

4. Нажмите **ОК**.

Для удаления всех правил фильтрации в черном списке MAC-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация MAC-адресов**.

На экране будет отображена страница **Фильтрация MAC-адресов**.

2. Установите **Режим фильтрации MAC-адресов** как **Черный список**.

3. Выберите **Удалить все**.

4. Нажмите **ОК**.

## 4.3 Фильтрация IP-адресов

Данные могут быть отфильтрованы по IP-адресу. На данной странице Вы можете сконфигурировать только правила фильтрации IP-адресов.

### 4.3.1 Белый список IP-адресов

Для добавления правила фильтрации в белый список IP-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация IP-адресов**.

На экране будет отображена страница **Фильтрация IP-адресов**.

2. Установите **Режим фильтрации IP-адресов** как **Белый список**.

3. Нажмите **Добавить пункт**.

4. Установите **Имя приложения**.

5. Установите **Протокол**.

6. В поле **Диапазон адресов источника** введите IP-адрес или сегмент IP-адресов для фильтрации.

7. В поле **Диапазон портов источника** введите номер порта или сегмент номеров портов для фильтрации.
8. В поле **Диапазон адресов получателя** введите IP-адрес или сегмент IP-адресов для фильтрации.
9. В поле **Диапазон портов получателя** введите номер порта или сегмент номеров портов для фильтрации.
10. Нажмите **Подтвердить**.

Для изменения правила фильтрации в белом списке IP-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация IP-адресов**.  
На экране будет отображена страница **Фильтрация IP-адресов**.
2. Установите **Режим фильтрации IP-адресов** как **Белый список**.
3. При входе нажмите **Редактировать**.
4. Задайте **Имя приложения**.
5. Задайте **Протокол**.
6. В поле **Диапазон адресов источника** введите IP-адрес или сегмент IP-адреса для фильтрации.
7. В поле **Диапазон портов источника** введите номер порта или сегмент номеров порта для фильтрации.
8. В поле **Диапазон адресов получателя** введите IP-адрес или сегмент IP-адресов для фильтрации.
9. В поле **Диапазон портов получателя** введите номер порта или сегмент номеров порта для фильтрации.
10. Нажмите **Подтвердить**.

Для удаления правила фильтрации в белом списке IP-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация IP-адресов**.  
На экране будет отображена страница **Фильтрация IP-адресов**.
2. Установите **Режим фильтрации IP-адресов** как **Белый список**.
3. При входе нажмите **Удалить**. На экране появится сообщение.
4. Нажмите **ОК**.

Для удаления всех правил фильтрации в белом списке IP-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация IP-адресов**.

На экране будет отображена страница **Фильтрация IP-адресов**.

2. Установите **Режим фильтрации IP-адресов** как **Белый список**.
3. Выберите **Удалить все**.
4. Нажмите **ОК**.

### 4.3.2 Черный список IP-адресов

На странице **Настройки брандмауэра**, если параметр **Фильтрация IP-адресов** имеет значение **Черный список**, то только IP-адреса из черного списка IP-адресов не смогут получить доступ к услугам.

Для добавления правила фильтрации в черный список IP-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация IP-адресов**.

На экране будет отображена страница **Фильтрация IP-адресов**.

2. Установите **Режим фильтрации IP-адресов** как **Черный список**.
3. Нажмите **Добавить пункт**.
4. Установите **Имя приложения**.
5. Установите **Протокол**.
6. В поле **Диапазон адресов источника** введите IP-адрес или сегмент IP-адресов для фильтрации.
7. В поле **Диапазон портов источника** введите номер порта или сегмент номеров портов для фильтрации.
8. В поле **Диапазон адресов получателя** введите IP-адрес или сегмент IP-адресов для фильтрации.
9. В поле **Диапазон портов получателя** введите номер порта или сегмент номеров портов для фильтрации.
10. Нажмите **Подтвердить**.

Для изменения правила фильтрации в черном списке IP-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация IP-адресов**.

На экране будет отображена страница **Фильтрация IP-адресов**.

2. Установите **Режим фильтрации IP-адресов** как **Черный список**.
3. При входе нажмите **Редактировать**.
4. Задайте **Имя приложения**.
5. Задайте **Протокол**.

6. В поле **Диапазон адресов источника** введите IP-адрес или сегмент IP-адресов для фильтрации.
7. В поле **Диапазон портов источника** введите номер порта или сегмент номеров порта для фильтрации.
8. В поле **Диапазон адресов получателя** введите IP-адрес или сегмент IP-адресов для фильтрации.
9. В поле **Диапазон портов получателя** введите номер порта или сегмент номеров порта для фильтрации.
10. Нажмите **Подтвердить**.

Для удаления правила фильтрации из черного списка IP-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация IP-адресов**.  
На экране будет отображена страница **Фильтрация IP-адресов**.
2. Установите **Режим фильтрации IP-адресов** как **Черный список**.
3. При входе нажмите **Удалить**. На экране появится сообщение.
4. Нажмите **ОК**.

Для удаления всех правил фильтрации в черном списке IP-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация IP-адресов**.  
На экране будет отображена страница **Фильтрация IP-адресов**.
2. Установите **Режим фильтрации IP-адресов** как **Черный список**.
3. Выберите **Удалить все**.
4. Нажмите **ОК**.

## 4.4 Фильтрация URL-адресов

Данный могут быть отфильтрованы по URL-адресу (унифицированный указатель ресурса). На данной странице Вы можете сконфигурировать только правила фильтрации URL-адресов.

### 4.4.1 Белый список URL-адресов

Для добавления правила фильтрации в белый список URL-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация URL-адресов**.  
На экране будет отображена страница **Фильтрация URL-адресов**.

2. Установите **Режим фильтрации URL-адресов** как **Белый список**.
3. Нажмите **Добавить пункт**.
4. Установите **URL-адрес**.
5. Нажмите **Подтвердить**.

Для изменения правила фильтрации в белом списке URL-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация URL-адресов**.  
На экране будет отображена страница **Фильтрация URL-адресов**.
2. Установите **Режим фильтрации URL-адресов** как **Белый список**.
3. При входе нажмите **Редактировать**.
4. На появившейся странице введите **URL-адрес**.
5. Нажмите **Подтвердить**.

Для удаления правила фильтрации в белом списке URL-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация URL-адресов**.  
На экране будет отображена страница **Фильтрация URL-адресов**.
2. Установите **Режим фильтрации URL-адресов** как **Белый список**.
3. При входе нажмите **Удалить**. На экране появится сообщение.
4. Нажмите **ОК**.

Для удаления всех правил фильтрации в белом списке URL-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация URL-адресов**.  
На экране будет отображена страница **Фильтрация URL-адресов**.
2. Установите **Режим фильтрации URL-адресов** как **Белый список**.
3. Выберите **Удалить все**.
4. Нажмите **ОК**.



## 4.4.2 Черный список URL-адресов

На странице **Настройки брандмауэра**, если параметр **Фильтрация URL-адресов** имеет значение **Черный список**, то только URL-адреса из черного списка URL-адресов не смогут получить доступ к услугам.

Для добавления правила фильтрации в черный список URL-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация URL-адресов**.

На экране будет отображена страница **Фильтрация URL-адресов**.

2. Установите **Режим фильтрации URL-адресов** как **Черный список**.
3. Нажмите **Добавить пункт**.
4. Установите **URL-адрес**.
5. Нажмите **Подтвердить**.

Для изменения правила фильтрации в черном списке URL-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация URL-адресов**.

На экране будет отображена страница **Фильтрация URL-адресов**.

2. Установите **Режим фильтрации URL-адресов** как **Черный список**.
3. При входе нажмите **Редактировать**.
4. На появившейся странице введите **URL-адрес**.
5. Нажмите **Подтвердить**.

Для удаления правила фильтрации в черном списке URL-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация URL-адресов**.

На экране будет отображена страница **Фильтрация URL-адресов**.

2. Установите **Режим фильтрации URL-адресов** как **Черный список**.
3. При входе нажмите **Удалить**. На экране появится сообщение.
4. Нажмите **ОК**.

Для удаления всех правил фильтрации в черном списке URL-адресов выполните следующее:

1. Выберите **Настройки безопасности > Фильтрация URL-адресов**. На экране будет отображена страница **Фильтрация URL-адресов**.

2. Установите **Режим фильтрации URL-адресов** как **Черный список**.
3. Выберите **Удалить все**.
4. Нажмите **ОК**.

## 4.5 Управление доступом к услугам

Данная функция позволяет управлять количеством пользователей, подключенных к маршрутизатору.

### 4.5.1 Список управления доступом

В списке управления доступом представлены типы услуг, которые контролируются маршрутизатором. По умолчанию управление доступом для всех типов услуг запрещено. При необходимости установите **Диапазон IP-адресов** и **Статус**.

Для того чтобы настроить список управления доступом, выполните следующее:

1. Выберите **Настройки безопасности > Управление доступом к услугам**.

На экране будет отображена страница **Управления доступом к услугам**.

2. Выберите конфигурируемый пункт и нажмите **Редактировать**.
3. Установите **Диапазон IP-адресов**.



Если параметр **Направление доступа** имеет значение **LAN**, IP-адрес должен находиться в одном сегменте сети, что и IP-адрес, который устанавливается на странице **Настройки хоста LAN**.

Если параметр **Направление доступа** имеет значение **WAN**, IP-адрес должен находиться в другом сегменте сети, в отличие от IP-адреса, который устанавливается на странице **Настройки хоста LAN**.

4. Установите значение параметра **Статус**.
5. Нажмите **Подтвердить**.

# 5 Настройки NAT

## 5.1 Настройки DMZ

### 5.1.1 DMZ

Если включена демилитаризованная зона (DMZ), пакеты, отправляемые глобальной сетью WAN, и которые не соответствуют ни одному правилу, отправляются на компьютер на стороне LAN для анализа или других целей, перед тем как они отбрасываются брандмауэром.

Для включения DMZ выполните следующее:

1. Выберите **Настройки NAT > Настройки DMZ**. На экране появится страница **Настройки DMZ**.
2. Выберите флажок **Включить** после параметра **DMZ**.
3. Установите **Адрес хоста**.



Данный IP-адрес должен отличаться от IP-адреса, который установлен на странице **Настройки хоста LAN**, однако они должны находиться в одном сегменте сети.

4. Нажмите **Подтвердить**.

## 5.2 Отображение портов

Если на маршрутизаторе включена функция трансляции сетевых адресов (NAT), то только IP-адрес на стороне WAN является видимым извне. Если определенные услуги, например FTP-услуга, должны быть включены на компьютере на стороне сети LAN, порт маршрутизатора на стороне WAN должен быть перенаправлен на FTP-порт компьютера на стороне LAN. Таким образом, хост на стороне глобальной сети WAN может получить доступ к хосту на стороне локальной сети LAN при помощи данного порта на стороне WAN.

Каждое правило, представленное на данной странице, может использоваться независимо.

## 5.2.1 Отображение портов

Для добавления правила отображения портов выполните следующее:

1. Выберите **Настройки NAT > Отображение портов**

На экране появится страница **Отображение портов**.

2. Нажмите **Добавить пункт**.
3. Установите **Тип**. Если Вы хотите сконфигурировать определенные правила, то задайте для данного параметра значение **Настройка**.
4. Установите **Протокол**.
5. Установите **Удаленный хост** (Не обязательно).
6. Установите **Диапазон номеров удаленного порта**.



Номера порта находятся в диапазоне от 1 до 65535.

7. Установите **Локальный хост**.



Данный IP-адрес должен отличаться от IP-адреса, который установлен на странице **Настройки хоста LAN**, однако они должны находиться в одном сегменте сети.

8. Установите **Номер локального порта**.



Номера портов находятся в диапазоне от 1 до 65535.

9. Установите значение параметра **Статус** как **Включить** или **Отключить**.
10. Нажмите **Подтвердить**.

Для изменения правил отображения портов выполните следующее:


1. Выберите **Настройки NAT > Отображение портов**

На экране появится страница **Отображение портов**.

2. При входе нажмите **Редактировать**.
3. Установите **Тип**. Если Вы хотите сконфигурировать определенные правила, то задайте для данного параметра значение **Настройка**.
4. Установите **Протокол**.
5. Установите **Удаленный хост** (Не обязательно).
6. Установите **Диапазон номеров удаленного порта**.

 Номера портов находятся в диапазоне от 1 до 65535.

7. Установите **Локальный хост**.

 Данный IP-адрес должен отличаться от IP-адреса, который установлен на странице **Настройки хоста LAN**, однако они должны находиться в одном сегменте сети.

8. Установите **Номер локального порта**.

 Номера портов находятся в диапазоне от 1 до 65535.

9. Установите значение параметра **Статус** как **Включить** или **Отключить**.

10. Нажмите **Подтвердить**.

Для удаления правила отображения портов выполните следующее:

1. Выберите **Настройки NAT > Отображение портов**

На экране появится страница **Отображение портов**.

2. При входе нажмите **Удалить**. На экране появится сообщение.

3. Нажмите **ОК**.

Для удаления всех правил отображения портов выполните следующее:

1. Выберите **Настройки NAT > Отображение портов** На экране появится страница **Отображение портов**.

2. Выберите **Удалить все**.

3. Нажмите **ОК**.

## 5.3 Технология UPnP

На данной странице Вы можете указать следует ли включать функцию UPnP.

### 5.3.1 UPnP

Для включения функции UPnP выполните следующее:

1. Выберите **Настройки NAT > Технология UPnP**.

На экране появится страница **Технология UPnP**.

2. Выберите флажок **Включить** после параметра **Технология UPnP**.

### 5.3.2 Отображение портов UPnP

На данной странице представлены правила отображения портов, которые установлены устройством в сети Интранет по технологии UPnP.

## 5.4 SIP ALG

На данной странице Вы можете включить или отключить SIP ALG.

Для включения SIP ALG, выполните следующее:

1. Выберите **Настройки NAT > SIP ALG**.

На экране появится страница **SIP ALG**.

2. Выберите флажок **Включить** после параметра **SIP ALG**.
3. Установите **SIP-порт**.



Номер порта по умолчанию 5060. Если используется другой номер порта, то ПО VoIP не может использоваться.

4. Нажмите **Подтвердить**.

# 6 Управление USB-устройствами

## 6.1 Настройки сервера

На странице **Настройки сервера** отображается основная информация о USB-устройствах, например, общий объем памяти, используемая память, свободное пространство, а также включен ли FTP-сервер.

### 6.1.1 Сетевые сервера

На странице **Сетевые сервера** Вы можете увидеть и задать статус FTP-сервера.

Для включения FTP-сервера, выполните следующее:

1. Выберите **Управление USB-устройствами > Настройки сервера**.

На экране появится страница **Сетевые сервера**.

2. Выберите флажок **Включить** после параметра **FTP-сервер**.
3. Нажмите **Подтвердить**.

### 6.1.2 USB-устройство хранения данных

На странице **USB-устройство хранения данных** отображается информация о USB-устройстве, например, общий объем памяти, используемую память и свободное место. Для просмотра информации о USB-устройстве, выполните следующее:

1. Выберите **Управление USB-устройствами > Настройки сервера**. На экране появится страница **USB-устройство хранения данных**.
2. Нажмите **Обновить** для обновления USB-устройства хранения данных вручную.

## 6.2 Настройки пользователя

Вы можете добавить пользователя в список пользователей для обмена файлами и целыми каталогами на USB-диске. При помощи созданной учетной записи пользователи смогут получить доступ к FTP-серверу при помощи FTP-клиента.

## 6.2.1 Список пользователей

В списке пользователей Вы можете увидеть добавленных пользователей и соответствующую информацию, например, имена пользователей, общие каталоги и права пользователя на доступ. К тому же, Вы можете добавлять, редактировать или удалять пользователей.

Для добавления пользователя к списку пользователей выполните следующее:

1. Выберите **Управление USB-устройствами > Настройки пользователя**.  
На экране появится страница **Список пользователей**.
2. Нажмите **Добавить пункт**.
3. На появившейся странице установите параметры, связанные с пользователем, включая имя пользователя, пароль, подтверждение пароля, совместно используемое устройство, общий каталог, а также права пользователя на доступ.
4. Нажмите **Подтвердить**.

Для изменения пользователя в списке пользователей выполните следующее:

1. Выберите **Управление USB-устройствами > Настройки пользователя**.  
На экране появится страница **Список пользователей**.
2. При входе нажмите **Редактировать**.
3. На появившейся странице измените настройки параметров, связанные с пользователем.
4. Нажмите **Подтвердить**.

Для удаления пользователя из списка пользователей выполните следующее:

1. Выберите **Управление USB-устройствами > Настройки пользователя**.  
На экране появится страница **Список пользователей**.
2. При входе нажмите **Удалить**. На экране появится сообщение.
3. Нажмите **ОК**.

Для удаления всех пользователей из списка пользователей выполните следующее:

1. Выберите **Управление USB-устройствами > Настройки пользователя**.  
На экране появится страница **Список пользователей**.
2. Выберите **Удалить все**.
3. Нажмите **ОК**.

## 6.3 FTP-загрузка

На данной странице Вы можете загрузить файлы в определенный каталог на USB-диске при помощи FTP, а также просмотреть историю загрузок и текущие загрузки.



### 6.3.1 История загрузок

На странице **История загрузок** отображается история предыдущих загрузок и статус текущей загрузки.

Для добавления задачи загрузки выполните следующее:

1. Выберите **Управление USB-устройствами > FTP-загрузка**.

На экране появится страница **История загрузок**.

2. Нажмите **Загрузка** в верхней правой части страницы.
3. Задайте соответствующие параметры.
4. Нажмите **Подтвердить**.

# 7 Система

## 7.1 Информация об устройстве

На данной странице отображаются основные сведения о маршрутизаторе, например, имя, серийный номер (SN), международный идентификатор мобильного оборудования (IMEI), версия ПО и аппаратная версия.

Для просмотра системной информации выполните следующее:

1. Выберите **Система > Информация об устройстве**.

На экране появится страница **Информация об устройстве**.

2. Просмотрите информацию в каждой строке.

## 7.2 Сброс

### 7.2.1 Перезагрузить

Данная функция позволяет выполнить перезагрузку маршрутизатора, когда он выключен. Настройки параметров вступят в силу только после перезагрузки маршрутизатора.

Для выполнения перезагрузки маршрутизатора выполните следующее:

1. Выберите **Система > Сброс**.

На экране появится страница **Сброс**.

2. Нажмите **Перезагрузить**. Появится диалоговое окно, запрашивающее у пользователя разрешение на перезагрузку маршрутизатора.
3. Нажмите **ОК**. Будет выполнена автоматическая перезагрузка маршрутизатора.

### 7.2.2 Восстановление

Данная функция позволяет восстановить исходные значения параметров маршрутизатора. После восстановления параметров маршрутизатора все сконфигурированные параметры будут заменены исходными значениями.

Для восстановления исходных параметров маршрутизатора выполните следующее:

1. Выберите **Система> Сброс**.

На экране появится страница **Сброс**.

2. Нажмите **Восстановить**. Появится диалоговое окно, запрашивающее у пользователя разрешение на восстановление исходных настроек маршрутизатора.
3. Нажмите **ОК**. Будут восстановлены исходные настройки маршрутизатора.

## 7.3 Резервирование и загрузка

Данная функция позволяет выполнить резервное копирование файла конфигурации на компьютер. При этом файл конфигурации может использоваться для восстановления настроек маршрутизатора при возникновении неисправности.

### 7.3.1 Резервирование

Для резервного копирования существующего файла конфигурации, выполните следующее:

1. Выберите **Система> Резервирование и загрузка**.

На экране появится страница **Резервирование и загрузка**.

2. Нажмите **Рез. копирование** на странице **Резервирование**.
3. В появившемся диалоговом окне выберите путь для сохранения и имя файла конфигурации. Нажмите **Сохранить**. Процедура загрузки файла конфигурации может отличаться в зависимости от используемого браузера.

### 7.3.2 Загрузка

Для загрузки резервного файла конфигурации выполните следующее:

1. Выберите **Система> Резервирование и загрузка**.

На экране появится страница **Резервирование и загрузка**.

2. Нажмите **Обзор** на странице **Загрузка**. В появившемся диалоговом окне выберите резервный файл конфигурации.
3. Нажмите **Открыть**. Диалоговое окно закроется. В поле справа от параметра **Файл конфигурации**, будут отображен путь сохранения файла и имя резервного файла конфигурации.
4. Нажмите **Загрузка**. Появится диалоговое окно, запрашивающее у пользователя разрешение на обновление версии ПО.
5. Нажмите **ОК**. Маршрутизатор загрузит резервный файл конфигурации. После загрузки произойдет автоматическая перезагрузка маршрутизатора.

## 7.4 Модернизация

### 7.4.1 Локальное обновление


Данная функция позволяет обновлять системное ПО до последней версии, так как в новой версии уже исправлены все ошибки предыдущей версии и новая версия является более стабильной. Рекомендуется всегда выполнять обновления. Перед проведением обновления целевая версия ПО должна быть сохранена на компьютере.

Для проведения локального обновления, выполните следующее:

1. Выберите **Система> Обновление**.

На экране появится страница **Обновление**.

2. Нажмите **Обзор** на странице **Локальное обновление**. В появившемся диалоговом окне выберите файл с версией целевого ПО.
3. Нажмите **Открыть**. Диалоговое окно закроется. В поле справа от параметра **Файл обновления**, будет отображен путь сохранения файла и имя файла версии целевого ПО.
4. Нажмите **Обновить**. Появится диалоговое окно, запрашивающее у пользователя разрешение на обновление версии ПО.

 Во время обновления не выключайте маршрутизатор, а также не разъединяйте локальную или беспроводную сеть.

5. Нажмите **ОК**. Начнется обновление ПО. После обновления произойдет автоматическая перезагрузка маршрутизатора, после которой будет использоваться новая версия ПО.

### 7.4.2 Http-обновление

Данная функция позволяет обновлять системное ПО до последней версии, так как в новой версии уже исправлены все ошибки предыдущей версии и новая версия является более стабильной. Рекомендуется всегда выполнять обновления.

Для проведения HTTP-обновления выполните следующее:

1. Выберите **Система> Обновление**.

На экране появится страница **Обновление**.

2. Нажмите **Проверить** для определения последней версии.

Если...	То...
Обнаружена новая версия.	Перейдите к шагу 3
Новая версия не обнаружена.	Обновление завершено.

3. Нажмите **Обновить** для загрузки новой версии.
4. После загрузки обновление будет выполнено автоматически.

- После выполнения обновления, будет выполнена автоматическая перезагрузка маршрутизатора. На экране появится сообщение об успешном выполнении обновления. После этого появится диалоговое окно входа в систему.



При выполнении обновления не выполняйте никаких операций на маршрутизаторе.

- В случае сбоя процесса обновления будет выполнена автоматическая перезагрузка маршрутизатора. После этого появится сообщение с запросом на откат маршрутизатора до исходной версии.

## 7.5 Изменение пароля

Данная функция позволяет изменить пароль на вход пользователя Администратор. После изменения пароля, новый пароль будет использоваться только при последующем входе в систему.

Для изменения пароля выполните следующее:

- Выберите **Система > Изменение пароля**.  
На экране появится страница **Изменение пароля**.
- Введите **Текущий пароль**, **Новый пароль** и **Пароль для подтверждения**. Новый пароль и пароль для подтверждения должны состоять от 6 до 15 символов ASCII.
- Нажмите **Подтвердить**.

## 7.6 Дата и время

### 7.6.1 Настройки

Вы можете вручную установить время системы или выполнить синхронизацию системного времени с сетью. Если выбран параметр **Автоматическая установка сетевого времени**, то маршрутизатор регулярно получает информацию о времени с сервера для выполнения синхронизации. Если включена функция перехода на летнее время (DST), маршрутизатор также выполняет корректировку системного времени на основе летнего времени.

Для установки даты и времени вручную выполните следующее:

- Выберите **Система > Дата и время**.  
На экране появится страница **Настройки**.
- Выберите кнопку **Ручная установка местного времени**.
- Установите **Местное время** или нажмите **Время ПК**.
- Нажмите **Подтвердить**.

Для синхронизации времени с сетью выполните следующее:

- Выберите **Система > Дата и время**.

На экране появится страница **Настройки**.

2. Выберите кнопку **Автоматическая установка сетевого времени**.
3. Задайте **Сервер времени 1**. Это основной сервер для синхронизации времени.
4. Задайте **Сервер времени 2**. Это второй сервер для синхронизации времени.
5. Установите **Часовой пояс**. Различные страны и регионы расположены в различных часовых поясах. Вы можете выбрать необходимый часовой пояс из выпадающего списка.
6. Выберите флажок **Включить переход на летнее время**.

При включении перехода на летнее время необходимо установить время начала перехода на летнее время и время завершения срока действия летнего времени. Маршрутизатор автоматически осуществляет переход на летнее время в зависимости от часового пояса. Могут быть установлены следующие параметры: **Дата и время перехода на летнее время**, **Дата и время завершения летнего времени** и **Сдвиг по времени**.

7. Нажмите **Подтвердить**.

## 7.7 Проверка

Если маршрутизатор не функционирует должным образом, то для предварительного определения проблемы и принятия соответствующих мер, Вы можете войти на страницу **Проверка** и запустить механизм проверки.

### 7.7.1 Ping-тестирование

Когда маршрутизатор не может получить доступ к сети Интернет, то для предварительного определения проблемы выполните ping-тестирование.

Для ping-тестирования выполните следующее:

1. Выберите **Система > Проверка**. На странице **Инструменты** установите параметру **Проверка** значение **Ping-тестирование**.  
На экране появится страница **Ping-тестирование**.
2. В поле **Целевой IP-адрес или домен** введите имя домена, например, [www.google.com](http://www.google.com).
3. Установите **Размер пакета** и **Время ожидания** и выберите флажок **Включить** после поля **Без фрагментации**.
4. Нажмите **Ping-тестирование**.
5. Дождитесь, пока система не выполнит ping-тестирование. В поле **Результат** будут выведены результаты выполнения операции.

### 7.7.2 Трассировка маршрутов

Когда маршрутизатор не может получить доступ к сети Интернет, для предварительного определения проблемы выполните трассировку маршрутов.

Для выполнения трассировки маршрутов выполните следующее:

1. Выберите **Система > Проверка**. На странице **Инструменты** установите параметру **Проверка** значение **Трассировка маршрутов**.  
На экране появится страница **Трассировка маршрутов**.
2. В поле **Целевой IP-адрес или домен** введите имя домена, например, [www.google.com](http://www.google.com).
3. Установите **Макс.число шагов** и **Время ожидания**.
4. Нажмите **Трассировка маршрутов**.
5. Дождитесь, пока система не выполнит трассировку маршрута. В поле **Результат** будут выведены результаты выполнения операции.

### 7.7.3 Проверка системы

Когда маршрутизатор не работает должным образом, то для предварительного определения проблемы выполняется проверка системы.

Для проверки системы выполните следующее:

1. Выберите **Система > Проверка**. На странице **Инструменты** установите параметру **Проверка** значение **Проверка системы**.  
На экране появится страница **Проверка системы**.
2. Нажмите кнопку **Проверка**.
3. Дождитесь, пока система не выполнит проверку. На экране будут отображены возможные причины неисправности.
4. Нажмите **Экспорт** для экспорта данной информации на компьютер. При необходимости отправьте данную информацию персоналу техобслуживания.

## 7.8 Настройки антенны

На данной странице пользователь может выбрать тип антенны. Чтобы открыть эту страницу выберите **Система > Настройки антенны**.

### 7.8.1 Использование встроенной антенны

Чтобы использовать встроенную антенну, необходимо выполнить следующие действия:

1. Выберите **Встроенная**.
2. Нажмите **Подтвердить**.

### 7.8.2 Использование внешней антенны

Чтобы использовать внешнюю антенну, необходимо выполнить следующие действия:

1. Выберите **Внешняя**.
2. Нажмите **Подтвердить**.

## 7.9 Журнал

В журнале записываются пользовательские операции и основные проводимые мероприятия. Для просмотра записей выполните следующее:

1. Выберите **Система > Журнал**.

На экране появится страница **Журнал**.

2. Выберите соответствующий уровень записей из выпадающего списка **Уровень события**. Общее количество записей данного уровня будет отображено справа от выпадающего списка и все записи будут подробно описаны в окне вывода информации.
3. Выберите вид операции.
  - **Очистить**: Будут удалены все записи журнала.
  - **Экспорт**: Экспортирование всех записей журнала в файл для сохранения на компьютере.



# 8

## Часто задаваемые вопросы

<b>Индикатор POWER не горит.</b>
<ul style="list-style-type: none"><li>• Убедитесь в том, что кабель питания подключен правильно и маршрутизатор включен.</li><li>• Убедитесь, что адаптер питания соответствует указанным параметрам.</li></ul>
<b>Не удалось войти на веб-страницу управления устройством.</b>
<ul style="list-style-type: none"><li>• Убедитесь в том, что маршрутизатор включен.</li><li>• Убедитесь в том, что сетевой кабель между компьютером и маршрутизатором подключен правильно.</li><li>• Проверьте, правильно ли установлен IP-адрес компьютера.</li></ul> <p>Если проблема все еще существует, то обратитесь в авторизованный центр по обслуживанию клиентов.</p>
<b>Маршрутизатор не может найти беспроводную сеть.</b>
<ul style="list-style-type: none"><li>• Убедитесь в том, что адаптер питания подключен правильно.</li><li>• Убедитесь в том, что маршрутизатор находится в открытой зоне, далеко от препятствий, таких как бетонные или деревянные стены.</li><li>• Убедитесь в том, что маршрутизатор находится вдали от бытовых электроприборов, которые генерируют сильное электромагнитное поле, например, микроволновые печи, холодильники и спутниковые тарелки.</li></ul> <p>Если проблема все еще существует, то обратитесь в авторизованный центр по обслуживанию клиентов.</p>
<b>Перегревается адаптер питания маршрутизатора.</b>
<ul style="list-style-type: none"><li>• При использовании в течение длительного периода времени маршрутизатор перегревается. Выключайте маршрутизатор, если Вы его не используете.</li><li>• Убедитесь, что маршрутизатор находится в хорошо вентилируемом месте вдали от солнечных лучей.</li></ul>
<b>Параметры приняли исходные значения.</b>
<ul style="list-style-type: none"><li>• Если маршрутизатор неожиданно выключился во время настройки, параметры могут принять исходные значения.</li><li>• Компания Huawei рекомендует выполнять экспорт настроек параметров после их установки для того, чтобы в случае неисправности быстро восстановить предыдущие настройки системы.</li></ul>

# 9

## Аббревиатуры и сокращения

<b>ACL</b>	Access Control List - Список управления доступом
<b>AES</b>	Advanced Encryption Standard - Расширенный стандарт шифрования
<b>ALG</b>	Application Layer Gateway - Шлюз уровня приложения
<b>AP</b>	Access Point - Точка доступа
<b>CPE</b>	Customer-Premises Equipment - Оборудование, размещаемое в помещении пользователя
<b>CWMP</b>	CPE WAN Management Protocol - Протокол управления CPE WAN
<b>DDNS</b>	Dynamic Domain Name Server - Динамический сервер доменных имен
<b>DDoS</b>	Distributed Denial of Service - Распределённый отказ в обслуживании
<b>DHCP</b>	Dynamic Host Configuration Protocol - Протокол динамического конфигурирования хоста
<b>DMZ</b>	Demilitarized Zone - Демилитаризованная зона
<b>DNS</b>	Domain Name Server/Domain Name System - Сервер доменных имен/Служба доменных имен
<b>DoS</b>	Denial of Service - Отказ от обслуживания
<b>DST</b>	Daylight Saving Time - Летнее время
<b>FTP</b>	File Transfer Protocol - Протокол передачи файлов
<b>GSM</b>	Global System for Mobile Communications - Глобальная система мобильной связи
<b>GUI</b>	Graphical User Interface - Графический пользовательский интерфейс
<b>HTTP</b>	Hypertext Transfer Protocol - Протокол передачи гипертекста
<b>ICMP</b>	Internet Control Message Protocol - Протокол управляющих сообщений в сети Интернет
<b>IMEI</b>	International Mobile Equipment Identity - Международный идентификатор мобильного устройства
<b>IP</b>	Internet Protocol - Протокол Интернет
<b>IPSec</b>	Internet Protocol Security - Протокол безопасности Интернет
<b>ISP</b>	Internet Service Provider - Поставщик услуг Интернет
<b>LAN</b>	Local Area Network - Локальная сеть

<b>LTE</b>	Long Term Evolution - Долгосрочная модернизация
<b>MAC</b>	Media Access Control - Управление доступом к среде передачи
<b>MTU</b>	Maximum Transmission Unit - Максимальная единица передачи
<b>NAT</b>	Network Address Translation - Трансляция сетевых адресов
<b>NTP</b>	Network Time Protocol - Протокол сетевого времени
<b>PBC</b>	Push Button Configuration - Настройка нажатием на кнопку
<b>PIN</b>	Personal Identification Number - Личный идентификационный номер
<b>PKM</b>	Privacy Key Management - Управление закрытыми ключами
<b>PPPoE</b>	Point-to-Point Protocol over Ethernet - Протокол передачи от точки к точке через Ethernet
<b>PPTP</b>	Point-to-Point Tunneling Protocol - Протокол туннелирования точка-точка
<b>RIP</b>	Routing Information Protocol - Протокол информации по маршрутизации
<b>RTSP</b>	Real Time Streaming Protocol - Протокол потоковой передачи в режиме реального времени
<b>QoS</b>	Quality of Service - Качество обслуживания
<b>SIM</b>	Subscriber Identity Module - Модуль идентификации абонента
<b>SIP</b>	Session Initiation Protocol - Протокол инициации сессии
<b>SN</b>	Serial Number - Серийный номер
<b>SNTP</b>	Simple Network Time Protocol - Простой протокол сетевого времени
<b>SSID</b>	Service Set Identifier - Идентификатор набора услуг
<b>SSH</b>	Secure Shell - Безопасная оболочка
<b>SYN</b>	Synchronous Idle – Символ синхронизации
<b>TKIP</b>	Temporal Integrity Protocol - Временный протокол целостности
<b>TLS</b>	Transport Layer Security - Безопасность на транспортном уровне
<b>TTLS</b>	Transport Layer Security - Туннелированный протокол безопасности на транспортном уровне
<b>UDP</b>	User Datagram Protocol - Протокол дейтаграмм пользователя
<b>UPnP</b>	Universal Plug and Play - Универсальный механизм Plug and Play ("включи и работай")
<b>URL</b>	Uniform Resource Locator - Унифицированный указатель ресурса
<b>VLAN</b>	Virtual Local Area Network - Виртуальная локальная сеть
<b>VoIP</b>	Voice over Internet Protocol – Передача голоса по протоколу IP
<b>WAN</b>	Wide Area Network - Глобальная сеть
<b>WCDMA</b>	Wideband Code Division Multiple Access - Широкополосный множественный доступ с кодовым разделением каналов
<b>WEP</b>	Wired Equivalent Privacy - Защищенная равнозначная секретность
<b>WLAN</b>	Wireless Local Area Network - Локальная беспроводная сеть

<b>WPA</b>	Wi-Fi Protected Access - Защищенный доступ по Wi-Fi
<b>WPA-PSK</b>	Wi-Fi Protected Access Pre-Shared Key - Предварительный ключ для защищенного доступа в Wi-Fi
<b>WPS</b>	Wi-Fi Protected Setup - Безопасная настройка Wi-Fi