

# Защита устройств Mikrotik от взлома или сброса настроек при помощи Protected RouterBOOT

 [interface31.ru/tech\\_it/2024/06/zashhita-ustroystv-mikrotik-pri-pomoshhi-protected-routerboot.html](https://interface31.ru/tech_it/2024/06/zashhita-ustroystv-mikrotik-pri-pomoshhi-protected-routerboot.html)

## Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Защита устройств Mikrotik от взлома или сброса настроек при помощи Protected RouterBOOT

Говоря о безопасности, часто подразумевается безопасность сетевая, связанная с возможным удаленным доступом злоумышленника к устройству. Но не меньшее значение имеет безопасность физическая, когда третьи лица получили или могут получить непосредственный доступ к устройству. Это порождает отдельный набор различных угроз, связанный как с потерей конфигурации устройства, так и получения конфиденциальных данных с него. Поэтому в данной статье мы рассмотрим, как можно противодействовать им с помощью встроенных средств Mikrotik.



### Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

Прежде чем настраивать защиту следует понять какие именно действия можно произвести с устройством имея к нему физический доступ. Самое простое - сброс настроек. Это актуально для сетевых устройств, установленных на конечных точках или филиалах, где к ним могут иметь доступ местные администраторы (чаще проходящие) или сотрудники провайдера.

Сбросить устройство можно двумя методами: через кнопку Reset или через Netinstall. В обоих случаях конфигурация будет потеряна, но в случае сброса через Reset сохраняется содержимое внутренней памяти, а там могут находиться сертификаты с закрытыми ключами или выгрузки конфигурации содержащие конфиденциальные сведения, например, пароли.

В данном случае мы получаем две возможные угрозы: несанкционированный сброс конфигурации устройства и возможный доступ к конфиденциальным данным.

Если говорить о целенаправленном взломе, то имеется возможность физического доступа к устройству, можно выполнить понижение прошивки через Netinstall с сохранением конфигурации и последующим взломом через эксплуатацию уязвимости CVE-2018-14847. При этом уязвимости подвержены устройства с версиями RouterOS:

- Longterm: 6.30.1 - 6.40.7
- Stable: 6.29 - 6.42
- Beta: 6.29rc1 - 6.43rc3

Да, сегодня не все устройства можно откатить на указанные версии прошивки, но все еще очень многие. Для примера взяли два роутера из находящихся у нас в эксплуатации. На один из них, из партии поновее, выполнить атаку на понижение версии ОС уже не получится, а на второй - запросто.

The image displays two screenshots of the RouterBOARD configuration window, stacked vertically. Both windows have a blue title bar with the text 'RouterBOARD' and standard window controls (minimize, maximize, close). The top window shows the configuration for a 'RouterBOARD 952Ui-5a...' with a 'Factory Firmware' of 3.41 (highlighted in red) and a 'Current Firmware' of 6.48.4. The bottom window shows the configuration for an 'RB951Ui-2nD' with a 'Factory Firmware' of 6.44 (highlighted in cyan) and a 'Current Firmware' of 6.49.1. Both windows include fields for 'Model', 'Serial Number', 'Firmware Type' (qca9531L), 'Upgrade Firmware' (6.49.15), and buttons for 'OK', 'Upgrade', 'Settings', 'USB Power Reset', and 'Reset Button'.

Field	Top Window (RouterBOARD 952Ui-5a...)	Bottom Window (RB951Ui-2nD)
Model	RouterBOARD 952Ui-5a...	RB951Ui-2nD
Serial Number	[Redacted]	[Redacted]
Firmware Type	qca9531L	qca9531L
Factory Firmware	3.41	6.44
Current Firmware	6.48.4	6.49.1
Upgrade Firmware	6.49.15	6.49.15

Чтобы противодействовать всем возможным попыткам сброса или переустановки RouterOS, не имея административного доступа к роутеру предназначена функция **Protected RouterBOOT**. Она отключает любой доступ к настройкам конфигурации RouterBOOT через консольный кабель и отключает работу кнопки сброса для изменения режима загрузки (Netinstall также будет отключен). Ее можно включить

или выключить только из RouterOS, а если такого доступа нет, то альтернативой становится полное форматирование NAND с последующей чистой установкой RouterOS.

Но и это сделать не так просто, для выполнения сброса нужно удерживать кнопку Reset ровно нужное число секунд и отпустить в указанном интервале, например между 50 и 60 секундами. При этом данный временной интервал можно задать достаточно большим, скажем в несколько минут.

Если вы забыли установленные временные параметры, то сбросить устройство, не зная пароля администратора будет невозможно!

В актуальных версиях RouterOS данные параметры недоступны через графический интерфейс и все настройки выполняются только в терминале.

Прежде всего посмотрим текущие значения:

```
/system routerboard settings print
```

По умолчанию установлено следующее:

```
protected-routerboot: disabled  
reformat-hold-button: 20s  
reformat-hold-button-max: 10m
```

Разберем их значения подробнее:

- **protected-routerboot** - включает режим Protected RouterBOOT, по умолчанию выключено
- **reformat-hold-button** - указывает необходимое время удержания кнопки сброса для начала форматирования, допустимые значения 5с .. 300с, по умолчанию 20 сек.
- **reformat-hold-button-max** - указывает максимальное время удержания кнопки сброса для начала форматирования, допустимые значения 15с .. 600с, по умолчанию 10 мин.

Для форматирования устройства нужно удерживать кнопку сброс не менее времени указанного в **reformat-hold-button** и отпустить не позднее чем до времени, указанного в **reformat-hold-button-max**. Минимальное значение между этими параметрами - 10 сек.

Таким образом указав, например, 120 - 130 секунд мы сделаем попытки подбора этого значения крайне затруднительными. Чтобы облегчить подсчет времени Mikrotik в этом режиме будет моргать индикатором каждую секунду, т.е. светодиод загорится на 1 секунду и погаснет на следующую.

Перед тем как включать данную функцию следует убедиться, что текущая версия RouterOS не ниже 6.33, а версия Factory Firmware не ниже 3.41. Если это не так, то прошивки надо обновить. Для обновления Factory Firmware воспользуйтесь

рекомендациями на официальном сайте:

### Manual:RouterBOARD settings

Для включения защиты выполните:

```
/system routerboard settings  
set protected-routerboot=enabled  
export
```

После чего внимательно изучите вывод команды export, там вы должны увидеть сообщение:

```
# press button within 60 seconds to confirm protected routerboot enable
```

Это означает, что для подтверждения включения Protected RouterBOOT вы должны нажать на кнопку в течении 60 секунд, в противном случае команда будет автоматически отменена.

Данная предосторожность сделана для того, чтобы исключить включение защиты, не располагая физическим доступом к устройству, например, после его взлома.

После чего следует обязательно изменить временные диапазоны для форматирования устройства, со значениями по умолчанию включение защиты не имеет смысла.

```
/system routerboard settings  
reformat-hold-button=120s  
reformat-hold-button-max=130s
```

Как видим, защитить Mikrotik от возможного несанкционированного доступа третьих лиц не так уж и сложно, однако сам производитель считает данные настройки опасными и поэтому взвешенно подходите к этому вопросу чтобы не создать проблем на ровном месте самому себе.

### **Онлайн-курс по MikroTik**

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на углубленном курсе по администрированию MikroTik. Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.