

# Автоматическое резервное копирование настроек Mikrotik на FTP

 [interface31.ru/tech\\_it/2019/05/avtomaticheskoe-rezervnoe-kopirovanie-nastroek-mikrotik-na-ftp.html](http://interface31.ru/tech_it/2019/05/avtomaticheskoe-rezervnoe-kopirovanie-nastroek-mikrotik-na-ftp.html)

## Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Автоматическое резервное копирование настроек Mikrotik на FTP

Резервное копирование - это одно из наиболее важных мероприятий в работе системного администратора, но по иронии судьбы о нем обычно вспоминают тогда, когда ничто иное помочь уже не способно. Роутеры Mikrotik не исключение. Широкие возможности RouterOS предполагают гораздо более сложные сетевые конфигурации, нежели у обычных, "бытовых", роутеров, поэтому восстановить все заново бывает весьма и весьма затруднительно, даже если вы точно помните все тонкости настройки. А чтобы до этого не дошло, стоит позаботиться о резервных копиях уже сейчас.



### 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.

Продукция Mikrotik заслуженно славится своей надежностью, но это часто способно сыграть с администратором злую шутку. Ведь если все годами работает, то и резервную копию можно лишний раз не сделать... Согласитесь, такая мысль эпизодически посещала каждого из нас. Поэтому резервное копирование должны быть автоматическим, полностью исключая человеческий фактор. В критической ситуации вариант "есть какой-то бекап" гораздо веселее варианта "никаких бекапов нет". А регулярный автоматический бекап позволяет перестать беспокоиться и спокойно заниматься иными делами.

В каких случаях вам может понадобиться восстанавливать Mikrotik из резервной копии? Самое очевидное - физический выход устройства из строя или критический сбой, в результате которого прошивка будет повреждена. Затем идет неудачное обновление (хотя это случается довольно редко) и ошибки администрирования.

Например, не так давно один мой коллега случайно выключил внутренний мост, при том, что снаружи доступ к устройству был запрещен. Управление устройством было потеряно, сеть оказалась отрезана от внешнего мира. Но благодаря наличию резервных копий восстановление заняло считанные минуты: сбросить конфигурацию устройства и залить в него последний бекап. Большинство пользователей даже ничего не заметило.

Итак, нам нужно организовать резервное копирование конфигурации Mikrotik. На помощь нам придет скриптовый язык RouterOS, возможность создавать и выполнять собственные скрипты на всей линейке роутеров трудно переоценить. Но хранить бекапы нужно отдельно от самого устройства и здесь нам доступны два варианта: отправлять их на почту или FTP-сервер.

Вариант с почтой можно назвать условно приемлемым если у вас одно-два устройства. Если же счет им идет на десятки, то вы получите форменное захламление почтового ящика и очень сложный контроль за наличием актуальных копий.

В этом плане FTP выглядит гораздо более привлекательно. Не нужно гадать, выполнил ли роутер бекап, или это антиспам "балуется", если в директории нет свежих бекапов - значит есть какие-то проблемы и нужно действовать.

Еще один тонкий момент. Mikrotik предлагает нам два варианта резервного копирования :выгрузка резервной копии устройства, которую можно восстановить только на аналогичном устройстве, и экспорт настроек в текстовом формате, которые можно импортировать полностью или частично на любое устройство.

Полный бекап содержит в себе все ключи, сертификаты, админские пароли и т.д, поэтому его крайне нежелательно выгружать в незашифрованном виде. Экспортированный текстовый файл критически важных данных не содержит, но в нем открытым текстом содержатся пароли к Wi-Fi, коммутируемым соединениям и т.д. Поэтому при его хранении тоже следует соблюдать определенные меры безопасности.

Исходя из этих соображений мы будем выгружать и хранить оба варианта. Для этих целей мы написали небольшой и достаточно простой скрипт, несмотря на то что подобных скриптов доступно достаточно большое количество, мы постарались сделать его наиболее понятным и универсальным.

```
#Резервное копирование конфигурации Mikrotik
#Получаем дату в формате ДД-ММ-ГГГГ
```

```
:local tmpdate [/system clock get date];
:local months
("jan","feb","mar","apr","may","jun","jul","aug","sep","oct","nov","dec");
:local month [ :pick $tmpdate03 ];
:local mm ([ :find $months$month -1 ] + 1);
:if ($mm < 10) do={ :set mm ("0" . $mm); }
:local date ([:pick $tmpdate46] . "-" . $mm . "-" . [:pick $tmpdate711])
```

```
#Задаем переменные и параметры доступа к FTP
```

```
:local myname "M2-hAP-ac-lite"
:local fname ($myname."_".$date);
:local bname ($myname."_".$date.".backup");
:local ename ($myname."_".$date.".rsc");
:local ftpuser "mikrotik";
:local ftppass "mYPa$$word";
:local ftpaddr "203.0.113.21";
```

```
#Выгружаем настройки
```

```
/system backup save name=$fname password=BackPa$$word;
:delay 10;
/export file=$fname
:delay 10;
```

```
#Загружаем конфигурацию на FTP
```

```
/tool fetch address=$ftpaddr src-path=$bname user=$ftpuser password=$ftppass
port=21 upload=yes mode=ftp dst-path=$bname
:delay 15;
/tool fetch address=$ftpaddr src-path=$ename user=$ftpuser password=$ftppass
port=21 upload=yes mode=ftp dst-path=$ename
:delay 15;
```

```
#Удаляем файлы с устройства
```

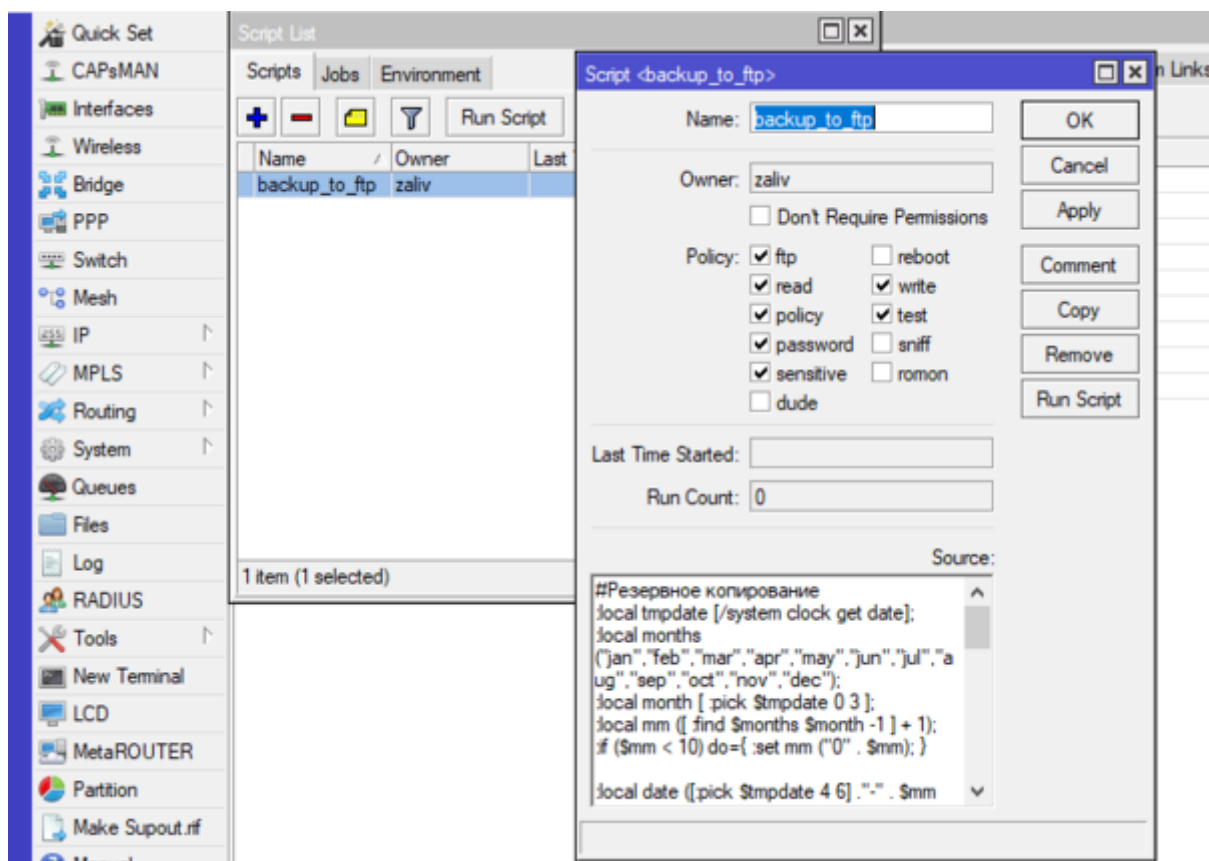
```
/file remove $bname;  
/file remove $ename;
```

Первый блок может показаться избыточно сложным, но это связано с тем, что Mikrotik возвращает месяц в виде трехбуквенной аббревиатуры, а для хранения бекапов лучше использовать полностью цифровые значения даты.

Затем задаем переменные. Как можно заметить, мы задали несколько переменных с именами файлов. Этого можно было не делать и формировать нужные имена прямо в скрипте, но в этом случае сильно страдает его читабельность. Мы не советуем этим пренебрегать, потому что впоследствии, когда подробности уже забудутся, разобраться с сложном скрипте будет сложнее, нежели в простом.

Далее должно быть все понятно, во многом благодаря нашим немного избыточным переменным. Выгружаем полный бекап и экспортируем конфигурацию, отправляем на FTP, удаляем с устройства.

Теперь перейдем на целевое устройство: **System - Scripts** и создадим новый скрипт:



Прежде всего укажем имя скрипта, так как нам потребуется вызывать его в дальнейшем, пробелов в имени быть не должно. Выставляем политики как на скриншоте, хотя это не особо критично, и копируем в поле **Source** наш скрипт.

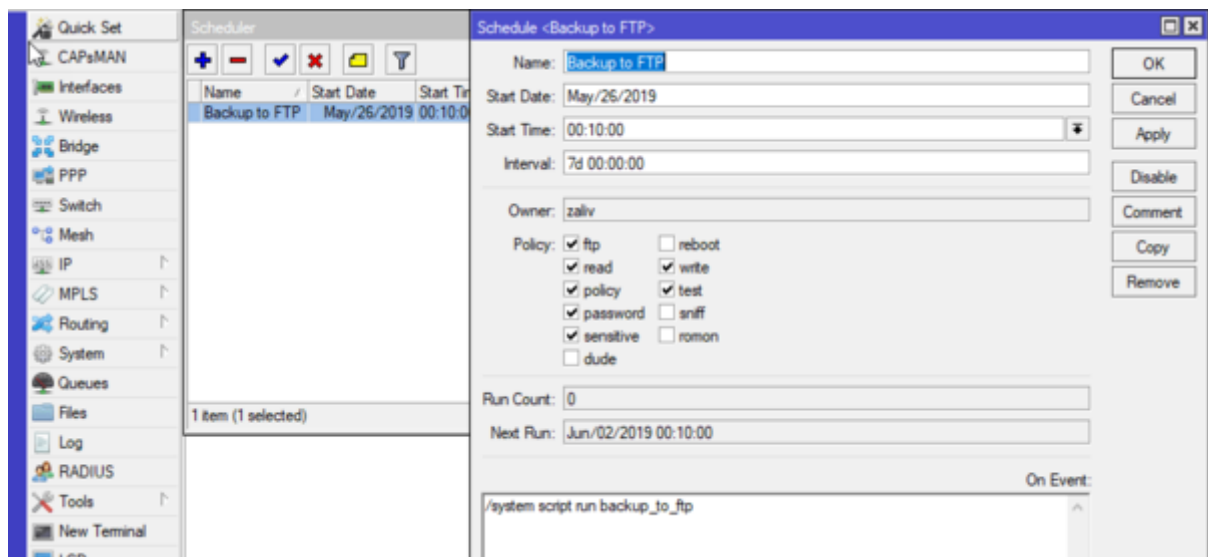
Для того, чтобы отличать конфигурации друг от друга задайте уникальную переменную **myname**. Лично мы используем следующий шаблон:

[идентификатор организации/места нахождения устройства] - [наименование устройства]

Это позволяет быстро определить чей это бекап и для какого устройства предназначен. Хотя вы можете использовать любую свою систему, либо указать любое имя, которое вам нравится.

После того, как вы создали скрипт его следует проверить, нажмите **Run Script** и убедитесь, что он делает все как вам надо. Обязательно проверьте со стороны FTP что файлы приходят и их можно восстановить.

Все работает? Отлично! Самое время добавить его в планировщик. Откроем **System - Scheduler** и добавим новое задание:



Имя задания может быть любым, а вот остальные опции нуждаются в пояснениях. Прежде всего определимся, с какой частотой мы хотим делать копии. Лично мы делаем резервное копирование раз в неделю, по воскресениям. Поэтому в **Start Date** указываем дату прошлого воскресения, в **Start Time** - время начала выполнения задания, в нашем случае - десять минут после полуночи. В поле **Interval** указываем периодичность повторения задания - ровно 7 дней.

Выставляем политики как на скриншоте, что снова не критично, и в поле **On Event** указываем команду запуска созданного нами скрипта:

```
/system script run backup_to_ftp
```

где **backup\_to\_ftp** - его имя.

Теперь каждое воскресенье в указанное время ваше устройство будет делать две резервные копии конфигурации и отправлять их на FTP-сервер. Если устройств несколько, то мы советуем разнести их по времени, чтобы их задания не пересекались.

## 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.

---