SMS в экосистеме MikroTik RouterOS для задач автономного управления и оповещения

19 августа 2026 года

В эпоху повсеместной IP-конвергенции и доминирования облачных систем уведомлений (Email, Telegram-боты, SNMP-ловушки), технология коротких текстовых сообщений (SMS) может показаться анахронизмом. Однако в контексте управления периферийным (Edge) оборудованием и обеспечения отказоустойчивости сетей, SMS остается критически важным, независимым от IP-связности каналом коммуникации.

Экосистема MikroTik RouterOS предоставляет нативную, полнофункциональную подсистему для работы с SMS, интегрированную непосредственно в ядро операционной системы. Настоящая статья рассматривает архитектурные принципы работы SMS-модуля, методологию его конфигурирования, recente улучшения и практики безопасного применения для задач Out-of-Band (OOB) управления.

---

1. Архитектурные основы и взаимодействие с модемом

Подсистема SMS в RouterOS (`/tool/sms`) абстрагирует сложность низкоуровневого взаимодействия с сотовыми модемами. Независимо от того, используется ли встроенный LTE/5G модуль (например, R11l-LTE7, FG621-EU) или внешний USB-модем, RouterOS взаимодействует с ним посредством стандартизированных AT-команд (3GPP TS 27.005).

Ключевые компоненты архитектуры:
1. **Драйвер модема (PPP/QMI/MBIM):** Обеспечивает физическую и канальную связь с базовой станцией оператора.
2. **SMS-шлюз RouterOS:** Программный модуль, который формирует PDU (Protocol Data Unit) или текстовый режим команд, управляет очередями отправки и обрабатывает входящие уведомления (New Message Indication).
3. **Скриптовый движок:** Позволяет привязывать пользовательские скрипты RouterOS к событиям отправки и получения SMS, трансформируя модем в полноценный шлюз для автоматизации.

---

2. Эволюция и recente улучшения

В последних релизах RouterOS разработчики MikroTik продолжили оптимизацию подсистемы SMS, уделяя внимание корректности кодирования и интеграции с графическими интерфейсами.

* **Расширение поддержки кодировки GSM7:** В свежих обновлениях **добавлена поддержка дополнительных символов стандарта GSM7** (`sms - added some GSM7 symbols to SMS tool`).
* *Инженерное значение:* Стандарт GSM 7-bit является базовым для SMS и позволяет передавать до 160 символов в одном сегменте. Расширение таблицы поддерживаемых символов (включая специфические национальные символы и расширения) минимизирует необходимость автоматического переключения на менее эффективную кодировку UCS-2 (которая ограничивает длину сообщения 70 символами). Это повышает емкость одного SMS-сообщения и снижает затраты на трафик при массовых рассылках.
* **Интеграция с WinBox:** В графическом интерфейсе WinBox добавлен ввод «SIM PIN» в разделе «Tools/SMS», что упрощает процедуру разблокировки SIM-карты при «холодной» перезагрузке роутера без необходимости использования CLI.

---

3. Сценарии применения в сетевой инфраструктуре

3.1. Out-of-Band (OOB) оповещение и аварийное восстановление
Когда IP-каналы (как основные, так и резервные) полностью деградируют, IP-based системы мониторинга (Zabbix, PRTG) теряют связь с устройством. SMS-шлюз MikroTik, инициируя передачу через сотовую сеть, обеспечивает гарантированную доставку алерта.
* *Интеграция:* SMS-отправка легко интегрируется со скриптами Netwatch. При падении критического линка Netwatch вызывает скрипт, который отправляет SMS инженеру.

3.2. Удаленное управление (Remote Command Execution)
RouterOS может выступать в роли SMS-модема, выполняя команды на основе входящих текстовых сообщений. Это позволяет инженерам перезагружать устройство, изменять конфигурацию или собирать диагностику (supout) с удаленных объектов, где IP-адрес является динамическим или недоступным извне.

3.3. Управление SIM-картой и биллингом
Подсистема позволяет отправлять USSD-запросы для проверки баланса, статуса пакета услуг или IMEI модема, а также вводить PIN-код для автоматической разблокировки SIM-карты после перезагрузки.

---

4. Методология конфигурирования

Шаг 1: Базовая настройка и SMSC
Для корректной работы необходимо указать адрес SMS-центра (SMSC) оператора связи. Обычно он определяется автоматически при регистрации в сети, но в роуминге или при использовании MVNO может потребоваться ручное задание.

```
/tool/sms/settings set port=usb1 smsc="+79990000000" receive-action=yes
```

Шаг 2: Отправка SMS (Алертинг)
Базовый синтаксис для отправки сообщения:

```
/tool/sms/send channel=usb1 phone="+79111234567" text="ALERT: Uplink ether1 is DOWN on Router-Branch-01"
```

Шаг 3: Настройка обработки входящих SMS (Автоматизация)
Для выполнения команд по входящим SMS необходимо включить функцию `receive-action` и создать скрипт-обработчик.

```
# Включаем обработку входящих SMS
/tool/sms/settings set receive-action=yes


# Создаем скрипт-обработчик
/system/script/add                                                    name="sms-handler"
policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon  source={
:local senderPhone $phone
:local msgText $text

# Проверка авторизации (Whitelist)
:if ($senderPhone = "+79111234567") do={
:if ($msgText = "reboot") do={
/system/reboot
}
:if ($msgText = "supout") do={
/tool/sup-output/output
# Далее скрипт отправки файла (требует дополнительной логики)
}
} else={
/log warning "Unauthorized SMS attempt from $senderPhone"
}
}

# Привязываем скрипт к настройкам SMS
/tool/sms/settings set receive-script="sms-handler"
```

---

5. Безопасность и эксплуатационные практики

Использование SMS для управления сетью несет специфические риски, такие как SMS-спуфинг (подмена номера отправителя) и перехват сообщений. Для митигации этих угроз необходимо соблюдать строгие политики:

1. **Защита SIM-карты (PIN-код):**
Обязательно установите PIN-код на SIM-карту и настройте его автоматический ввод в RouterOS (`/tool/sms/settings set sim-pin="1234"`). Это предотвратит использование SIM-карты в случае ее физического извлечения из устройства.
2. **Строгая аутентификация отправителя (Whitelisting):**
Никогда не выполняйте команды, поступающие по SMS, без предварительной проверки номера отправителя (`$phone`). Реализуйте жесткий whitelist в скрипте-обработчике.
3. **Отказ от передачи конфиденциальных данных в тексте:**
SMS в сотовых сетях передается в открытом виде (или с минимальным шифрованием на уровне радиоинтерфейса). Никогда не отправляйте пароли, конфигурации или чувствительные данные в теле SMS-сообщения.
4. **Ограничение частоты отправки (Rate Limiting):**
При интеграции с Netwatch или системными триггерами существует риск "шторма" SMS при массовом сбое сети. Рекомендуется

реализовывать в скриптах механизмы подавления повторов (throttling), чтобы не отправить 100 одинаковых алертов за одну минуту.

---

6. Диагностика и мониторинг

Для верификации работы подсистемы и диагностики проблем с доставкой сообщений в RouterOS предусмотрены следующие инструменты:

* **Просмотр входящих/исходящих сообщений:**

```
/tool/sms/inbox/print
/tool/sms/outbox/print
```

* **Мониторинг состояния модема:**

```
/interface/lte/info lte1
```

(Позволяет убедиться, что модем успешно зарегистрирован в сети и имеет доступ к сервису SMS).
* **Логирование:** Все события, связанные с ошибками отправки или синтаксическими ошибками в скриптах-обработчиках, фиксируются в системном логе (`/log/print where topics~"sms"`).

---

7. Заключение

Подсистема SMS в MikroTik RouterOS — это не просто рудимент прошлого, а специализированный, высоконадежный инструмент для обеспечения автономности сетевой инфраструктуры. В сочетании с механизмами Out-of-Band управления, она гарантирует, что администратор сохранит контроль над устройством и получит критические алерты даже в сценариях полного отказа IP-транспорта.

Последние улучшения, такие как расширение поддержки символов GSM7 и упрощение ввода SIM PIN в графическом интерфейсе, подтверждают внимание разработчиков к деталям и удобству эксплуатации. При условии строгого соблюдения практик безопасности (whitelisting, защита PIN-кода, шифрование чувствительных данных), SMS-шлюз MikroTik становится неотъемлемой частью архитектуры отказоустойчивых корпоративных и провайдерских сетей.