

# Модуль подсистемы “Сбор данных” <SNMP>

Модуль:	SNMP
Имя:	SNMP клиент
Тип:	DAQ
Источник:	daq_SNMP.so
Версия:	0.6.1
Автор:	Роман Савоченко
Описание:	Предоставляет реализацию клиента SNMP-сервиса.
Лицензия:	GPL

## Оглавление

<a href="#">Модуль подсистемы “Сбор данных” &lt;SNMP&gt;</a>	1
<a href="#">Введение</a>	1
<a href="#">1. SNMP</a>	2
<a href="#">1.1. MIB</a>	2
<a href="#">1.2. Адресация</a>	3
<a href="#">1.3. Взаимодействие</a>	3
<a href="#">1.4. Авторизация</a>	3
<a href="#">2. Модуль</a>	4
<a href="#">2.1. Контроллер данных</a>	4
<a href="#">2.2. Параметры</a>	6

## Введение

Протокол SNMP был разработан с целью проверки функционирования сетевых маршрутизаторов и мостов в 1988 году. Впоследствии сфера действия протокола охватила и другие сетевые устройства, такие как хабы, шлюзы, терминальные сервера и даже устройства, имеющие отдалённое отношение к сети: принтеры, источники бесперебойного питания, PLC и т.д. Кроме того, протокол допускает возможность внесения изменений в функционирование указанных устройств. На данное время протокол SNMP стандартизирован как RFC-1157, -1215, -1187, -1089.

Данный модуль предоставляет возможность собирать информацию и вносить изменения у различных устройств по SNMP протоколу. Также модулем реализуются функция горизонтального резервирования, а именно совместная работа с удалённой станцией этого же уровня.

# 1. SNMP

Основными взаимодействующими "лицами" протокола являются агенты и системы управления. Если рассматривать эти два понятия на языке «клиент-сервер», то роль сервера выполняют агенты, то есть те самые устройства, для опроса состояния которых и был разработан протокол. Соответственно, роль клиентов отводится системам управления – сетевым приложениям, необходимым для сбора информации о функционировании агентов. Помимо этих двух субъектов в модели протокола можно выделить также еще два: управляющую информацию и сам протокол обмена данными.

Вся информация об объектах системы-агента содержится в так называемой MIB (management information base) – базе управляющей информации, другими словами MIB представляет собой совокупность объектов (MIB-переменные), доступных для операций записи-чтения.

На данный момент существует четыре типовых базы MIB:

1. Internet MIB – база данных объектов для обеспечения диагностики ошибок и конфигураций. Включает в себя 171 объект (в том числе и объекты MIB I).
2. LAN manager MIB – база из 90 объектов – пароли, сессии, пользователи, общие ресурсы.
3. WINS MIB – база объектов, необходимых для функционирования WINS сервера.
4. DHCP MIB – база объектов, необходимых для функционирования DHCP сервера, служащего для динамического выделения IP адресов в сети.

Кроме вышеуказанных типовых баз, MIB могут дополнительно подгружаться в виде модулей.

## 1.1. MIB

Все имена MIB имеют иерархическую структуру. Существует десять корневых алиасов:

1. System — данная группа MIB II содержит в себе семь объектов, каждый из которых служит для хранения информации о системе (версия ОС, время работы и т.д.).
2. Interfaces — содержит 23 объекта, необходимых для ведения статистики сетевых интерфейсов агентов (количество интерфейсов, размер MTU, скорость передачи, физические адреса и т.д.).
3. AT (3 объекта) — отвечают за трансляцию адресов. Более не используется. Была включена в MIB I. В SNMP v2 эта информация была перенесена в MIB для соответствующих протоколов.
4. IP (42 объекта) — данные о проходящих IP пакетах (количество запросов, ответов, отброшенных пакетов).
5. ICMP (26 объектов) — информация о контрольных сообщениях (входящие/исходящие сообщения, ошибки и т.д.).
6. TCP (19) — все, что касается одноименного транспортного протокола (алгоритмы, константы, соединения, открытые порты и т.п.).
7. UDP (6) — аналогично, только для UDP протокола (входящие/исходящие датаграммы, порты, ошибки).
8. EGP (20) — данные о трафике Exterior Gateway Protocol (используется маршрутизаторами, объекты хранят информацию о принятых/отосланных/отброшенных кадрах).
9. Transmission — зарезервирована для специфических MIB.
10. SNMP (29) — статистика по SNMP – входящие/исходящие пакеты, ограничения пакетов по размеру, ошибки, данные об обработанных запросах и многое другое.

## 1.2. Адресация

Каждый из корневых алиасов представляется в виде дерева, растущего вниз. Например, к адресу администратора можно обратиться посредством пути: `system.sysContact.0`, ко времени работы системы `system.sysUpTime.0`, к описанию системы (версия, ядро и другая информация об ОС) : `system.sysDescr.0`. С другой стороны, те же данные могут задаваться и в точечной нотации. Так `system.sysUpTime.0` соответствует значению 1.3.0, так как `system` имеет индекс "1" в группах MIB II, а `sysUpTime` – 3 в иерархии группы `system`. Ноль в конце пути говорит о скалярном типе хранимых данных. В процессе работы символьные имена объектов не используются, то есть если менеджер запрашивает у агента содержимое параметра `system.sysDescr.0`, то в строке запроса ссылка на объект будет преобразована в "1.1.0", а не будет передана «как есть».

В целом, существует несколько способов записи адреса к MIB-переменной:

1. "1.3.6.1.2.1.1" — Прямая кодовая адресация для объекта "System" (корневой алиас System). При такой адресации каждая MIB переменная кодируется идентификатором, а полный адрес записывается в виде последовательности идентификаторов разделённых точкой, слева на право. Данная запись адреса является основной и все другие способы записи приводятся к ней.
2. "1.3.0" — Сокращённая кодовая адресация, относительно корневого алиаса (объект "System.sysDescr").
3. ".iso.org.dod.internet.mgmt.mib-2.system" — Полная символьная к прямой кодовой адресации для объекта "System".
4. "system.sysDescr" — Простая, не полным путём, адресация относительно корневого алиаса (объект "System").
5. "SNMPv2-MIB::sysDescr" — Адресация из MIB базы от имени модуля для "system.sysDescr".

## 1.3. Взаимодействие

В SNMP клиент взаимодействует с сервером по принципу запрос-ответ. Сам по себе агент способен инициировать только одно действие, называемое ловушкой прерыванием. Помимо этого, все действия агентов сводятся к ответам на запросы, посылаемые менеджерами.

Существует 3 основные версии протокола SNMP (v1 & v2 & v3), которые не являются совместимыми. В SNMP v3 включена поддержка шифрования трафика, для чего, в зависимости от реализации, используются алгоритмы DES, MD5. Это ведет к тому, что при передаче наиболее важные данные недоступны для прослушивания. В качестве транспортного протокола в SNMP обычно используется протокол UDP, Хотя, на самом деле, SNMP поддерживает множество других транспортных протоколов нижнего уровня.

## 1.4. Авторизация

Одним из ключевых понятий в SNMP является группа (group). Процедура авторизации менеджера представляет собой простую проверку на принадлежность его к определенной группе, из списка, находящегося у агента. Если агент не находит группы менеджера в своем списке, их дальнейшее взаимодействие невозможно. По умолчанию используются группы: `public` (для чтения) и `private` (для записи). В протоколе SNMP v3 для аутентификации используется понятие пользователя с паролем аутентификации и приватности, в зависимости от уровня секретности.

## 2. Модуль

Данный модуль поддерживает работу со всеми версиями протокола SNMP (1, 2 и 3) в режимах чтения и записи MIB-параметров.

### 2.1. Контроллер данных

Для добавления источника данных SNMP создаётся и конфигурируется контроллер в системе OpenSCADA. Пример вкладки конфигурации контроллера данного типа изображен на рис.1.

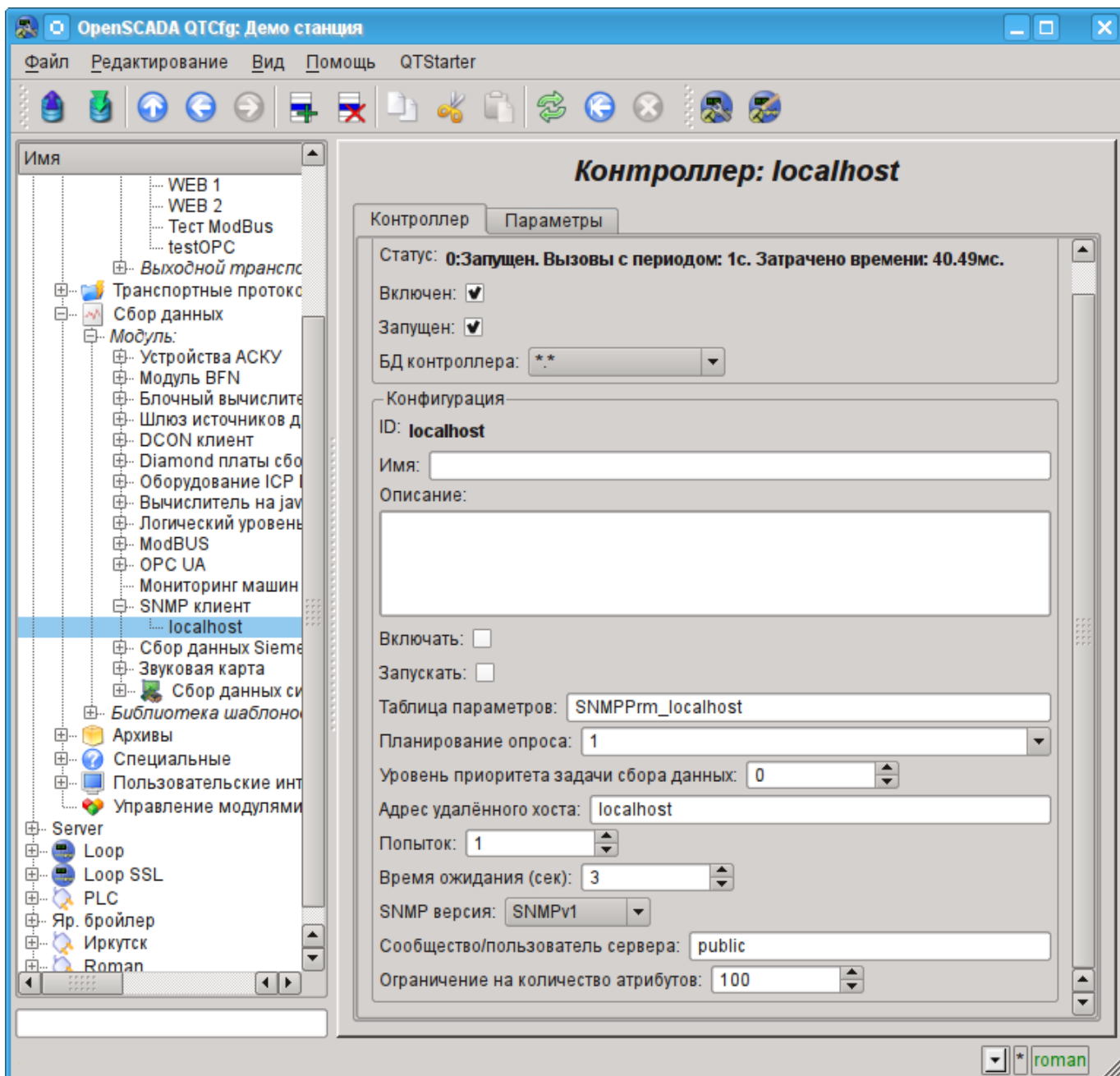


Рис.1. Вкладка конфигурации контроллера.

С помощью этой вкладки можно установить:

- Состояние контроллера, а именно: Статус, "Включен", Запущен" и имя БД содержащей конфигурацию.
- Идентификатор, имя и описание контроллера.
- Состояние в которое переводить контроллер при загрузке: "Включен" и "Запущен".

- Имя таблицы для хранения конфигурации параметров контроллера.
- Политика планирования и приоритет задачи сбора данных.
- Адрес удалённого хоста агента.
- Количество попыток отправки запроса.
- Время ожидания ответа, в секундах.
- Используемую версию протокола SNMP.
- Сообщество или пользователя подключения.
- Ограничение на количество атрибутов в одном параметре.
- Уровень безопасности для v3 (Нет авториз/Нет приватн; Авториз/Нет приватн; Авториз/Приватн).
- Протокол (MD5, SHA) и пароль аутентификации для v3.
- Протокол (DES, AES) и пароль приватности для v3.

## 2.2. Параметры

Модуль *SNMP* предоставляет только один тип параметров – “Стандарт”. Дополнительным конфигурационным полем параметра данного модуля (рис.2) является список MIB-параметров, ветки которых подлежат считыванию.

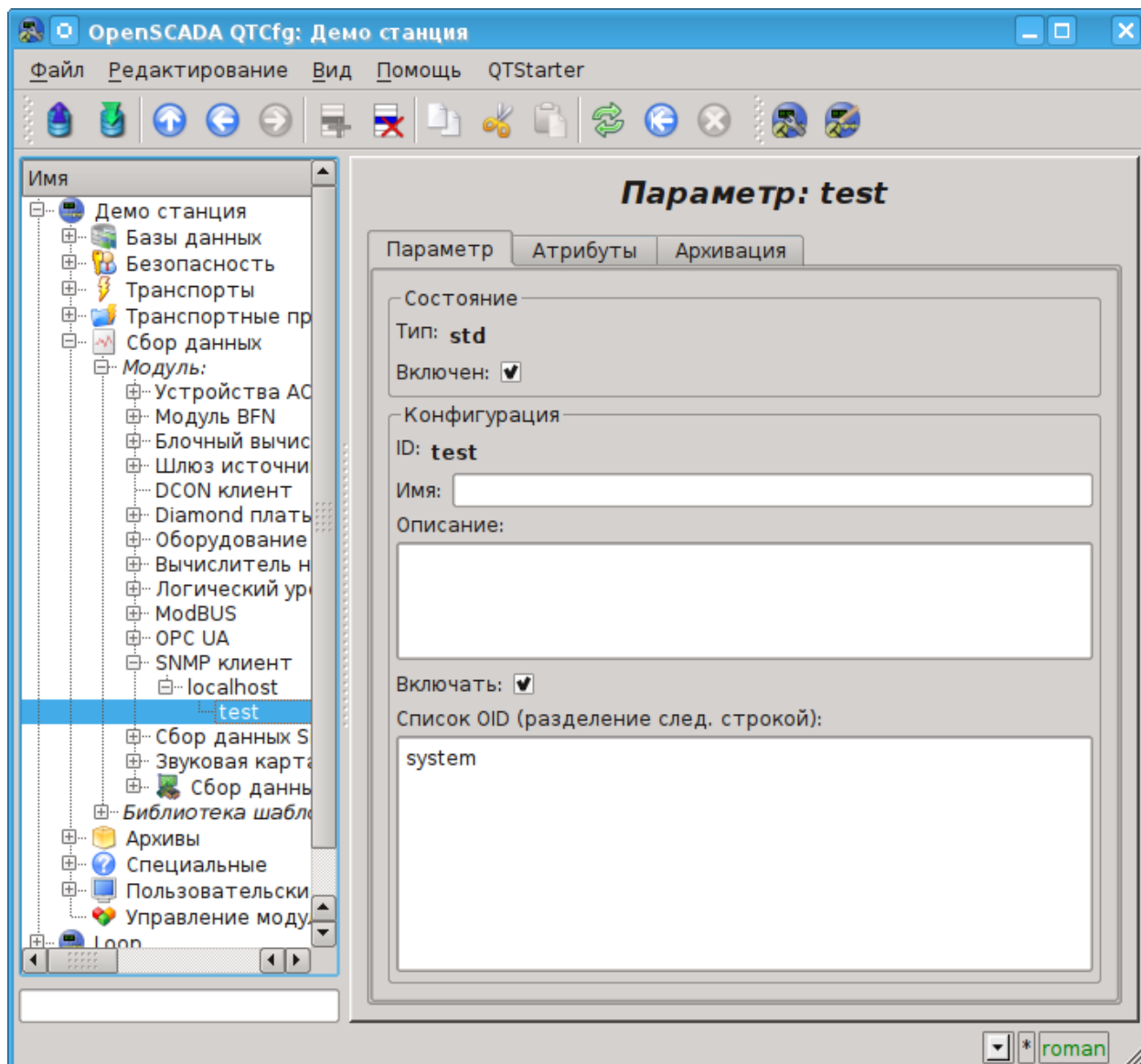


Рис.2. Вкладка конфигурации параметра.

В соответствии с указанным списком MIB-параметров выполняется опрос их ветвей и создание атрибутов параметра. В дальнейшем выполняется обновление значений параметров. Атрибуты именуются в соответствии с кодовой адресацией MIB-параметров, в качестве идентификатора, и адресации от базы MIB объектов, в имени атрибута (рис.3).

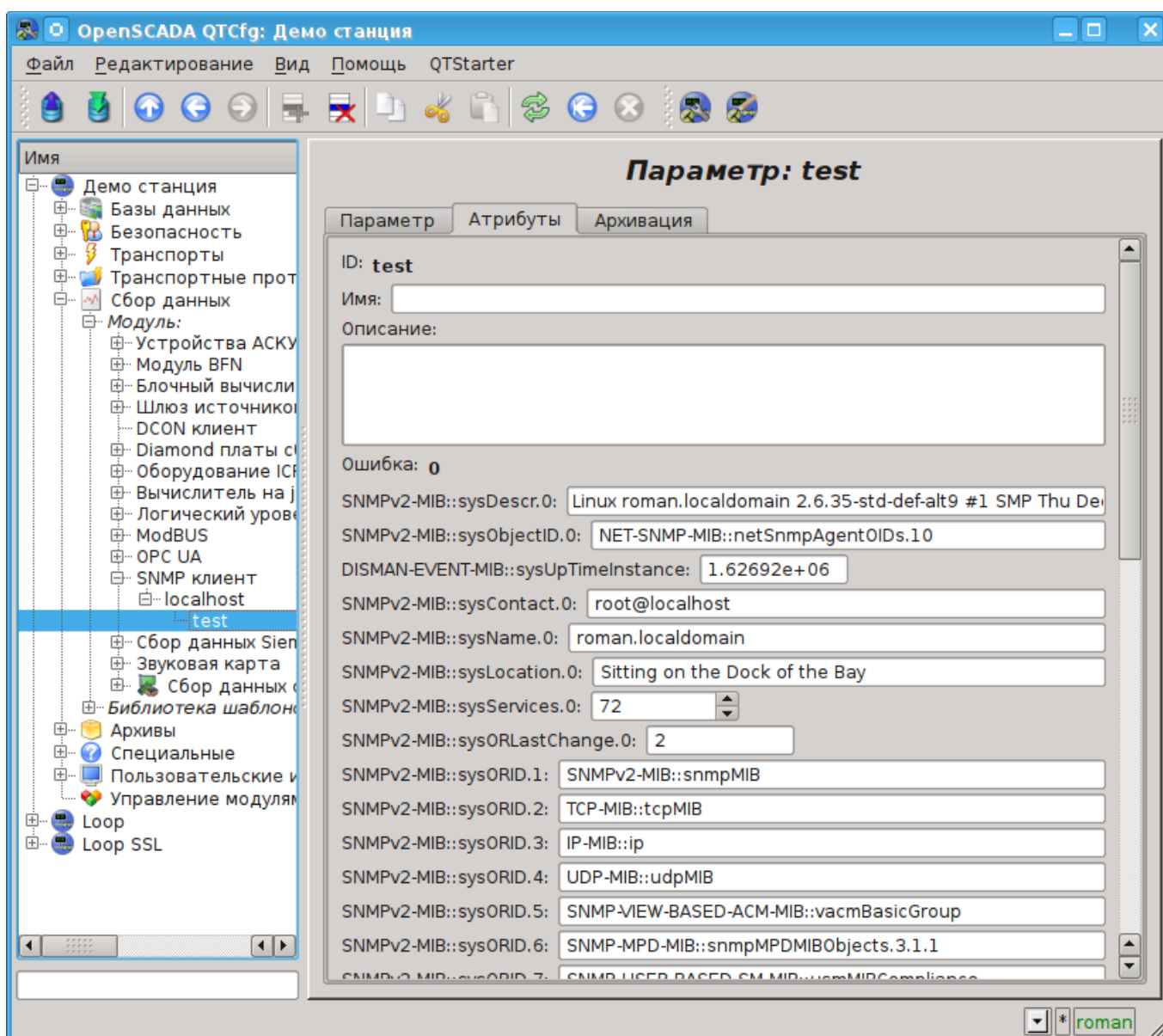


Рис.3. Вкладка атрибутов параметра.