# Бюджетный агент SNMP для корпоративных систем управления

**Александр Елисеев (г. Вильнюс, Литва)**

**Представленное в статье устройство, реализованное на открытой аппаратной платформе ARM-Dominator 4, является недорогим перепрограммируемым контроллером ввода-вывода, работающим по протоколу SNMP через сеть Ethernet. Устройство можно интегрировать в системы наблюдения и поддержания функционирования корпоративных информационных сетей.**

## Что такое SNMP-агент?

Как только появились компьютерные сети, возникла необходимость наблюдения за функционированием их аппаратного и программного обеспечения (к аппаратному обеспечению можно отнести маршрутизаторы, мосты, шлюзы, модемы, серверы, рабочие станции и т.д.; программным обеспечением являются операционные системы, СУБД, web-серверы и т.д.).

С этой целью в информационные сети на базе протоколов семейства TCP/IP была внедрена технология на основе протокола SNMP (Simple Network Management Protocol – простой протокол управления сетью), выделены основные характеристики аппаратного и программного обеспечения, которые следует наблюдать, разработана кодировка для передачи параметров по сети. Также была разработана концепция использования и обработки получаемых от оборудования данных. Всё это превратилось в стандарты RFC специальной комиссии по интернет-разработкам (IETF – Internet Engineering Task Force), касающиеся SNMP.

Иногда вводит в заблуждение наличие в названии протокола SNMP слова «простой». В данном случае это не означает, что протокол прост для реализации (хотя встречаются и такие утверждения). Скорее, протокол реализует только часть функциональности, которую предусматривает глобальная концепция системы управления сетями, принятая Международным союзом электросвязи.

Но даже при такой ограниченной функциональности в стандарте SNMP упомянуты сотни параметров, которые необходимо наблюдать, и не меньшее количество типов сообщений, которые оборудование должно асинхронно посылать в центры сбора информации.

Однако в инфраструктуре информационных сетей задействовано не меньшее количество вспомогательного оборудования: основные и резервные источники питания, различные преобразователи и зарядные устройства, шкафы для установки оборудования, системы кондиционирования, системы контроля доступа, отопления и т.д. Это оборудование также требует наблюдения, поскольку оказывает влияние на надёжность функционирования сетей. Крупные предприятия связи предпочитают использовать единый стандарт для наблюдения за всем оборудованием в своих информационных системах. Стандарты SNMP прочно утвердились в этой отрасли и обеспечены большим ассортиментом программных и аппаратных средств.

Представленный в данной статье контроллер KPV-4M назван SNMP-агентом, поскольку содержит в себе программный модуль, преобразующий данные с внешних входов устройства и события на входах в сообщения протокола SNMP. Помимо этого, контроллер реализует целый ряд дополнительных стандартов SNMP, что обеспечивает ему совместимость с широким кругом сторонних программных продуктов, выполняющих функции центральных менеджеров SNMP.

Контроллер построен на базе платформы ARM-Dominator 4. Подробную информацию об этой платформе можно получить на интернет-странице www.alylab.eu. Доступная элементная база и компактность программного кода делают контроллер более дешёвым, чем большинство присутствующих на рынке образцов с аналогичными характеристиками.

Несмотря на то что контроллер нацелен на использование в больших сетях, он также может быть использован и в небольших приложениях. Стандартные наборы параметров, сообщаемые по протоколу SNMP, могут быть интересны и индивидуальным пользователям устройства. Доступные программные инструменты для персональных компьютеров позволяют наблюдать в удобной древовидной форме все состояния на входах устройства, управлять состояниями выходов и даже автоматизировать процессы удалённого управления. Наличие протокола PPP позволяет контроллеру передавать информацию не только по сети Ethernet, но и через внешние модемы, в частности модемы GSM. И, конечно, полезна масштабируемость решений на SNMP, т.е. нет препятствий для перехода от обслуживания одного контроллера к обслуживанию десятков, сотен и даже тысяч контроллеров.

Ещё одной особенностью контроллера является открытая спецификация разработки интерактивных интернет-страниц для встроенного web-сервера. Эти страницы могут использовать технологию AJAH или Adobe Flash для доступа ко всем переменным контроллера и многим командам.

## Краткий обзор протокола SNMP

Протокол SNMP изначально был разработан с целью поддержания работоспособности сетей связи. Он не должен был загружать сети собственным трафиком, когда они работоспособны, и, тем более, не должен вызывать «шторм» повторных пересылок, когда сеть функционирует с перебоями. Поэтому транспортным протоколом для SNMP был выбран протокол UDP поверх протокола IP.

Протокол UDP не является протоколом с гарантированной доставкой, но в концепции применения SNMP это вполне оправданно. Инициаторы обмена по SNMP в этом случае имеют больше возможностей по регулированию интенсивности обмена пакетами на физическом уровне сети, поскольку одной из задач механизма поддержания работоспособности сети является предотвращение перегрузки этой сети.

Данные в протоколе SNMP не посылаются в виде открытого текста, как, например, в протоколе HTTP, а кодируются в специальный двоичный вид, описанный спецификацией ASN.1 (Abstract Syntax Notation One). Это – довольно сложная для освоения спецификация, формализующая описание данных и их кодирование. Причём для одинаково описанных данных может быть применено разное кодирование при передаче по каналам связи с различной степенью компактности: BER (Basic Encoding Rules), PER(Packed Encoding Rules), LWER (Light-Weight Encoding Rules), MBER (Minimum Bit Encoding Rules) и т.д. Одной из первых стала кодировка BER, которая применяется в SNMP и в некоторых источниках отождествляется с ASN.1.

Всех агентов SNMP в сети обслуживает один или несколько SNMP-менеджеров. В больших корпоративных сетях, как правило, менеджеров несколько. Менеджеры в любой момент могут запросить какой-либо параметр от SNMP-агента или изменить значение какого-либо параметра, если этот параметр разрешён для изменения. Какие параметры вообще доступны в SNMP-агенте, и какие из них доступны для изменений по SNMP, – менеджер узнаёт из MIB-файлов (MIB – Management Information Base, база данных управления), которыми должна сопровождаться документация на SNMP-агенты. Поскольку протокол SNMP стандартизован, стандартные MIB-файлы к документации не прилагаются, а вместо них даётся ссылка на стандарты RFC.

Файлы MIB написаны на языке ASN.1. Этот язык обязаны понимать все SNMP-менеджеры, чтобы работать с нестандартными SNMP-агентами. Именно расширение функций SNMP-агентов за счёт нестандартных возможностей и делает эту технологию привлекательной. Описываемый в статье контроллер интересен, прежде всего, нестандартными функциями входов-выходов, хотя имеет и стандартный набор параметров.

Во время запуска SNMP-менеджеры загружают указанные пользователями файлы MIB и компилируют их, проверяя синтаксис, связывая со стандартными файлами MIB и превращая в удобную для программ двоичную форму. Если SNMP-менеджеру не будет предоставлен файл MIB от SNMP-агента, то менеджер не сможет эффективно обслуживать этого агента, хотя и сохранит возможность обмена данными с агентом. Файлы MIB являются единственным источником информации, через который SNMP-менеджеры узнают о свойствах SNMP-агентов. Все файлы MIB – и стандартные, и специфичные, – складываются в единое непротиворечивое дерево файлов MIB. После обработки информации из заданного набора файлов MIB, SNMP-менеджеры представляют её пользователям в виде удобной древовидной структуры на экране компьютера. Иногда используются утилиты командной строки, но их рассмотрение можно опустить ввиду наличия более удобных альтернатив.

Как было указано выше, информация из файлов MIB представляется в виде древовидной структуры. Так было решено ещё до того, как SNMP-менеджеры научились рисовать эти структуры на экране. Первые ветви этого дерева были стандартизированы, и теперь их уже нельзя ни переименовать, ни удалить в собственных файлах MIB-агентов. Более того, в файлах MIB-агентов эти ветви не описываются, а просто даётся ссылка на стандартные файлы MIB. Свою фантазию производитель может проявлять, только начиная с узла enterprises в дереве файлов MIB.

На рисунке 1 показано дерево файлов MIB SNMP-агента KPV4M. Как следует из рисунка, агент содержит стандартные параметры, известные как MIB-II (RFC 1213), и частные или специфичные для данного устройства параметры, расположенные под узлом enterprises. Специфичные для агента параметры начинаются узлом alylab. Узлы в дереве файлов MIB для краткости также могут быть представлены в числовом формате (каждому узлу присвоен номер, и положение узла в дереве записывают в числовой нотации, начиная от корня). Эта запись называется идентификатором объекта (object identifier – OID).

Положение узла alylab будет тогда записано как 1.3.6.1.4.1.28311. Эту запись можно увидеть в нижней части окна на рисунке 1. Здесь узел alylab имеет номер 28311. Этот номер не может быть выбран произвольно, он называется IANA Private Enterprice number, и его выделяет предприятиям международная организация Internet Assigned Numbers Authority. Выдача номера производится совершенно бесплатно, и основанием для выдачи может быть просьба, высланная по электронной почте. Получив уникальный номер

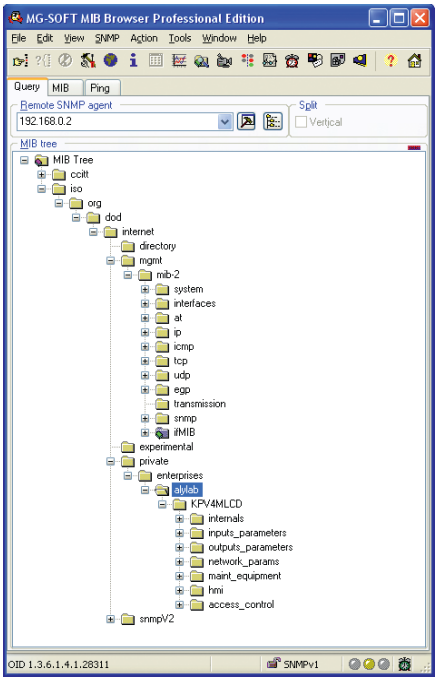


**Рис. 1. Дерево файлов MIB SNMP-агента контроллера KPV4M**

предприятия, можно не беспокоиться, что файлы MIB вашего SNMP-агента окажутся в конфликте с файлами MIB других агентов.

На рисунке 1 показаны только основные корневые узлы дерева файлов MIB-агента. Под ними скрываются узлы и параметры более глубоких уровней. В общей сложности в стандартном поддереве MIB-II содержится до 185 объектов. В поддереве alylab представленного здесь SNMP-агента находится 190 объектов. Объектами могут быть числовые или строковые параметры, а также таблицы. Таблицы удобно применять, когда количество параметров некоторого типа может быть переменным и заранее неизвестным. Это, например, записи таблицы маршрутизации. Количество этих записей периодически изменяется, и в MIB-файле нельзя заранее задать описание каждого маршрута. Тогда применяется объект «таблица», прочитать который SNMP-менеджер может только итеративно, считывая все записи до появления признака отсутствия последующих записей.

Помимо объектов (параметров), которые можно читать и записывать, в SNMP существуют специальные асинхронные trap-сообщения. Они формируются SNMP-агентами без запроса со стороны менеджера и могут нести значения некоторых параметров из MIB-дерева агента, которые производитель считает нужным передать с этим сообщением. Всего специфицировано

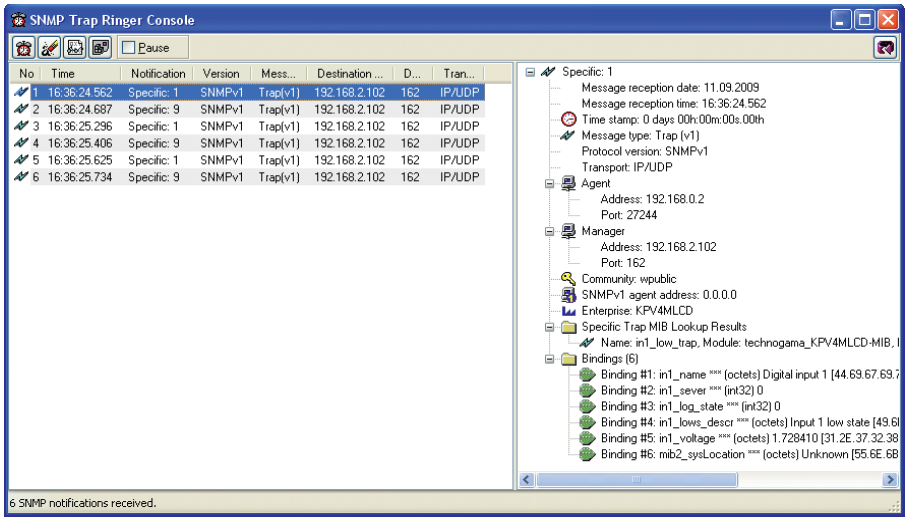


**Рис. 2. Пример консоли менеджера SNMP**

шесть стандартных типов trap-сообщений: холодный старт, горячий старт, выключение коммуникационного интерфейса, включение интерфейса, ошибка аутентификации и отключение партнёра по уже устаревшему протоколу EGP. Седьмой тип сообщения может нести произвольную информацию, определяемую производителем. Этот тип и используется SNMP-агентом для передачи специфических сообщений об изменениях состояний или тревогах. В сообщении имеется поле specific-trap, в котором задаётся уникальный номер типа специфического trap-сообщения.

На рисунке 2 представлен вид консоли одного из SNMP-менеджеров с полученными trap-сообщениями. В правой части окна отображено содержание первого сообщения. Это сообщение об изменении состояния на первом цифровом входе устройства. Наряду с типом самого сообщения, пользователь получает дополнительно данные о названии входа, степени важности сообщения, текущем логическом состоянии входа, описание состояния, абсолютное значение напряжения на этом входе и информацию о географическом расположении устройства. Консоли развитых SNMP-менеджеров способны проводить разбор данных из таких сообщений и предпринимать решения по фильтрации этих сообщений, передаче их другим службам, включении тревожной сигнализации и т.д.


**Рис. 3. Внешний вид контроллера KPV-4M**

В протоколе SNMP предусмотрены облегчённые механизмы защиты от несанкционированного доступа. Это некие аналоги паролей, называемые community. Поле community передаётся в каждом пакете SNMP. Агент при несовпадении community с его собственным игнорирует такие пакеты. Также предусмотрены community только для чтения, для чтения-записи и community, передаваемые в trap-сообщениях. Описываемый здесь SNMP-агент поддерживает все типы community и дополнительно поддерживает фильтрацию по IP-адресам из задаваемого списка. Также возможна поддержка community, позволяющих работать только с отдельными ветвями MIB-дерева.

Всё вышесказанное относилось к общему подмножеству возможностей протокола SNMP, реализованных в версии SNMP v1. Но существуют более совершенные версии этого протокола: SNMP v2 и SNMP v3. Во второй версии протокола SNMP были модернизированы средства передачи больших блоков данных, усовершенствованы сообщения об ошибках, введены новые типы данных; trap-сообщения приобрели новый формат, и появилась возможность подтверждения их доставки, которой в SNMP v1 не было. В третьей версии протокола SNMP появилось шифрование протокола SNMP, авторизация и команды обмена сообщениями между SNMP-агентами.

## Описание контроллера

Контроллер KPV-4M (см. рис. 3) построен на аппаратной платформе ARM-Dominator 4 и предназначен для выполнения функций контроля внешних датчиков с выходными сигналами в виде «сухих» релейных контактов, для контроля работы инверторов фирмы Gamatronic и для измерения сигналов с различных резистивных датчиков температуры и др.

Устройство имеет восемь аналоговых входов и пять цифровых выходов типа открытый коллектор. Сенсорная бесконтактная клавиатура и ЖК-дисплей позволяют редактировать параметры и установки прибора, а также просматривать журналы событий и состояний на его входах и выходах.

Журналы событий и системная информация сохраняются на SD-карту ёмкостью 2 Гб и могут быть легко прочитаны на компьютере либо через внешние интерфейсы устройства, либо напрямую с SD-карты через соответствующие адаптеры. Журналы содержат полный отчёт о системных событиях, передаваемые через интерфейсы данные и диагностические сообщения с метками времени с точностью до 1 мкс.

В качестве коммуникационных интерфейсов в устройстве используется: RS-232, Ethernet 10/100Base-T, USB 2.0. Контроллер KPV-4M оснащён программным обеспечением, выполняющим, помимо прочего, функции SNMP-агента. Это позволяет контроллеру работать в составе сетевых систем мониторинга, управляемых такими программными пакетами, как HP OpenView или OpenNMS.

Агент SNMP контроллера сообщает центральному серверу системы мониторинга о всех изменения логического состояния на входах устройства, об изменениях состояния инвертора Gamatronic и об изменениях во внутреннем состоянии устройства.

Технические характеристики контроллера KPV-4M:

- напряжение питания .....8...16 В;
- ток потребления ..... .....220 мА при напряжении 12 В;
- количество входов .....8;
- уровень измеряемого потенциала на входах .....3,3 В;
- внутреннее сопротивление входов .....10 кОм;
- количество выходов .....5;
- максимальное коммутируемое напряжение на выходах .....50 В;
- максимальный коммутируемый выходами ток .....5 А;

- габариты .....140 × 110 × 35 мм.

Внешние интерфейсы контроллера KPV-4M (см. рис. 4):

- интерфейс RS232 с разъёмом RJ6 для подключения инверторов фирмы Gamatronic и другого оборудования; скорость до 256 Кбит/с;
- интерфейс RS-232 с разъёмом DB9 (DCE) для подключения к компьютеру; скорость до 256 Кбит/с;
- интерфейс Ethernet 10/100Base-T для подключения в сеть мониторинга;
- интерфейс USB 2.0 со скоростью до 12 Мбит/с для подключения к компьютеру.

Протоколы, поддерживаемые устройством по интерфейсу RS-232:

- для подключения к инверторам Gamatronic используется фирменный пакетный протокол ASCII в режиме <9600,8,n,1>;
- для подключения к компьютеру используется потоковый протокол ASCII для эмуляции терминала VT100 в режиме <115200,8,n,1>;
- при загрузке нового программного обеспечения используется пакетный протокол Y-modem в режиме <115200,8,n,1>;

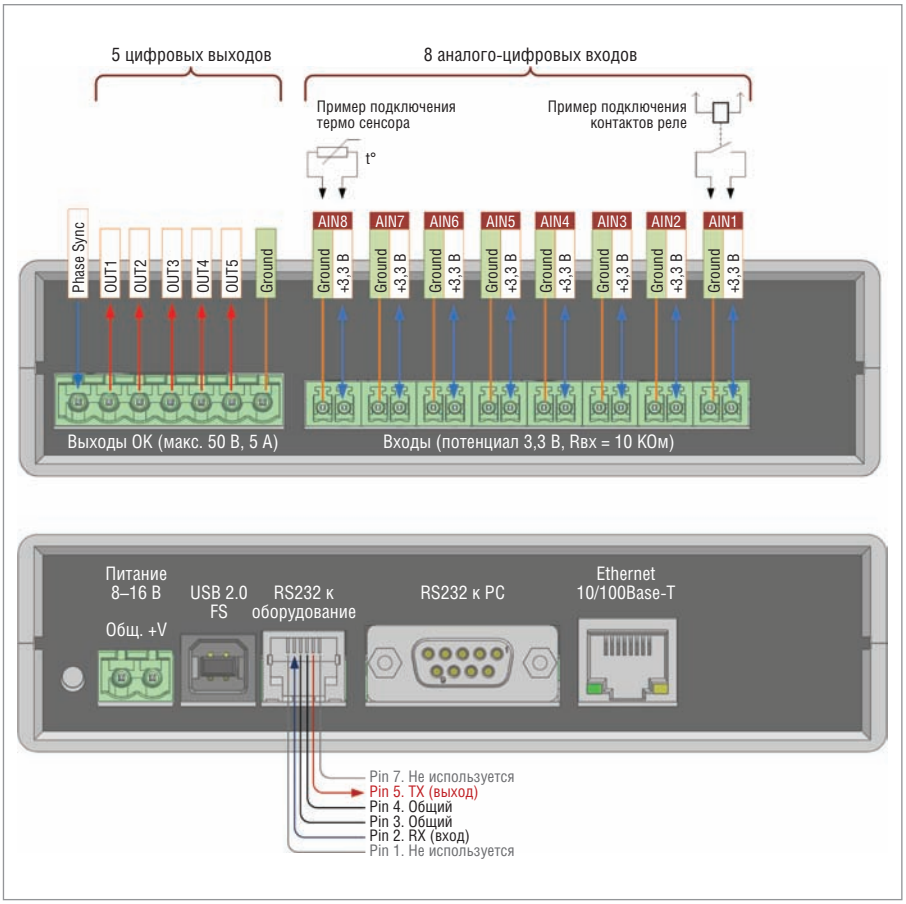


**Рис. 4. Внешние интерфейсы контроллера**

- PPP для связи с внешней сетью по TCP/IP через модем или компьютер.

Протоколы, поддерживаемые устройством по интерфейсу Ethernet:

- протокол ARP для идентификации MAC-адреса устройства в сети;
- протокол ICMP, и в частности, поддержка запросов PING;
- протокол DHCP для автоматического получения IP-адреса контроллером в сетях, где предусмотрен такой механизм;
- протокол DNS для определения IP-адресов по доменным именам;
- протокол NTP для получения точного времени от внешних серверов времени;
- протокол FTP-клиента для загрузки и выгрузки файлов с удалённого FTP-сервера;
- протокол FTP-сервера для управления файлами в файловой системе контроллера с удалённых FTP-клиентов;
- протокол Telnet для управления устройством с удалённого терминала Telnet таким же образом, как через интерфейс RS-232 в режиме эмуляции терминала VT100;
- протокол HTTP для организации web-сервера в контроллере с поддержкой технологии SSI и CGI; web-сервер предоставляет возможность управления устройством, просмотра состояний его входов и выходов и других административных действий;
- протокол агента SNMP v1 для передачи сообщений центральному серверу SNMP-мониторинга и для просмотра внутренних параметров и состояний контроллера.

Может быть установлен протокол SNMP v2 или SNMP v3. Устройство поддерживает стандартный набор переменных MIB RFC1213 и специальный набор переменных, специфицированных в файле KPV4M.MIB.

Протоколы, поддерживаемые устройством по интерфейсу USB: протокол виртуального COM-порта, поверх которого используется потоковый протокол ASCII виртуального терминала VT100 в режиме <115200,8,n,1>.

### Конфигурирование контроллера

После подачи питания или сигнала сброса контроллер KPV-4M производит конфигурирование своих внутренних параметров. Вначале параметры заполняются значениями по умолчанию, хранящимися в самой программе контроллера. Вслед за этим с SD-карты устройства считываются параметры, записанные в файле PARAMS.INI. Если данный файл на SD-карте отсутствует, то он создаётся на SD-карте заново с использованием значений по умолчанию.

Файл с параметрами PARAMS.INI является простым текстовым файлом, содержащим записи в формате {ключ}={значение}, где {ключ} – сокращённое название параметра, а {значение} является строкой со значением, присваиваемым параметру. Кроме того, файл содержит комментарии с описанием параметров и их порядковый номер в файле.

Пример содержания файла «PARAMS.INI»:

```
;--------------------------------
; Ethernet interface parameters
;--------------------------------

; N=011 MAC address
MAC="00:1A:07:AC:22:09"

; N=012 Device IP addr
HIP="192.168.0.2"

; N=013 Network mask
NMSK="255.255.255.000"

; N=014 Default gateway
DGTW="192.168.0.1"
```

В приведённом выше примере показан фрагмент с четырьмя заданными параметрами. Параметр с номером 011 является MAC-адресом устройства, параметр с номером 012 является IP-адресом устройства и т.д. Комментарии в файле начинаются с символа ';'. Числовые значения параметров записываются без пробелов и кавычек. Десятичная точка всегда обозначается точкой (не запятой). Параметры, которые могут содержать символы, строки и пробелы, заключаются в скобки. Символ скобок должен быть такой, какой указан в примере.

Дополнительные настройки прибора можно произвести изменением значений соответствующих параметров в файле PARAMS.INI на SD-карте контроллера. Если файл был отредактирован с помощью FTP-клиента, т.е. без извлечения карты из устройства, то для вступления параметров в силу устройство необходимо перегрузить. Отметим, что SD-карту нельзя извлекать из устройства при включенном питании.

Помимо прямого редактирования параметров, в файле PARAMS.INI параметры устройства можно просматривать и редактировать с помощью web-браузера через интерфейс Ethernet, с помощью терминальной программы в режиме эмуляции терминала VT100 через интерфейс RS-232 и с помощью программы SNMP-менеджера.

### Конфигурирование интерфейса Ethernet

Для работы в сети Ethernet в устройстве должны быть сконфигурированы три параметра:

- IP-адрес самого устройства (N=012 Device IP addr); по умолчанию 192.168.0.2;
- маска сети (N=013 Network mask); по умолчанию 255.255.255.000;
- адрес шлюза в общую сеть (N=014 Default gateway); по умолчанию 192.168.0.1.

Если в одном сегменте сети будут работать несколько устройств KPV-4M, то следует также изменить MAC-адреса остальных устройств, сделав их разными. Для этого можно увеличивать на единицу число в пятой паре цифр MAC-адреса для каждого устройства.

Иногда в сети Ethernet используют возможность автоматического назначения IP-адреса устройствам с помощью протокола DHCP. В таком случае нет необходимости устанавливать параметры IP-адресов и маски, но требуется правильно указать сетевое имя устройства и включить DHCP (параметры 016 и 015 в файле PARAMS.INI соответственно).

### Конфигурирование протокола SNMP

Контроллер KPV-4M по умолчанию работает по протоколу SNMP v1. Чтобы внешние программы SNMP-менеджеров могли обмениваться информацией с контроллером, они должны иметь общие с контроллером имена (или пароли), называемые community. В контроллере предусмотрены отдельные community для чтения и для записи (соответственно 096 и 097 в файле PARAMS.INI).

Если SNMP-менеджер будет использовать community, предназначенный только для чтения, то он не сможет изменить ни один параметр устройства. Поэтому следует внимательно устанавливать community. Если оба имени

community в контроллере будут одинаковы, то для SNMP-менеджера с таким community будут открыты и чтение, и запись.

При необходимости в устройстве можно изменить уникальный номер IANA предприятия и три системных параметра SNMP с номерами 098 – 100. Параметр 101 (Enable IP filtering), установленный в «1», позволяет фильтровать обращения от SNMP-менеджеров и пропускать только те обращения, которые приходят с IP-адресов, указанных в параметрах 102 – 105.

### Использование MIB-файлов

Чтобы SNMP-менеджеры могли отобразить на дисплее дерево параметров устройства с их описаниями и правильным обозначением типов, им необходимо предоставить описание параметров устройства в каком-то виде. Для этой цели служат т.н. MIB-файлы.

Файлы MIB представляют собой текстовые файлы, обычно с расширением .mib, содержащие подробное описание всех параметров устройства, которые должны быть видны SNMP-менеджеру. Файлы MIB используют сложную нотацию специального языка ASN1. Менеджеры SNMP, как правило, преобразуют MIB-файлы в собственный формат и отображают пользователю информацию, хранящуюся в MIB-файле, в виде древовидной структуры.

Как упоминалось выше, существуют стандартизированные MIB-файлы, описанные в рекомендациях RFC, и специфичные MIB-файлы, индивидуальные для каждого типа устройств и создаваемые производителями устройств. Менеджеры SNMP уже содержат стандартные MIB-файлы; специализированные MIB-файлы должен предоставлять пользователь.

В контроллере KPV-4M специфичный MIB-файл хранится на SD-карте в директории MIB под названием KPV4M.MIB. В этом файле описано более сотни различных параметров контроллера KPV-4M, а также несколько десятков типов сигнальных сообщений (trap).

### Программы для тестирования и работы с агентом SNMP

Известны десятки доступных программ – менеджеров SNMP. Они подключаются к SNMP-агентам и предоставляют пользователю удобный диалог с устройствами. Рекомендуемые автором SNMP-менеджеры:

- MG-SOFT MIB Browser Professional Edition компании MG-SOFT Corporation;
- OidView MIB Browser компании Byte-Sphere.

Оба перечисленных пакета являются коммерческими, но доступны (бесплатно) их полнофункциональные версии, работающие в течение 30 дней с момента инсталляции.

### Настройка прибора и работа через виртуальный терминал VT100 и Telnet

Контроллер KPV-4M может быть сконфигурирован локально с ПК через интерфейсы RS-232 или USB. При подключении ПК к контроллеру через USB на компьютере с ОС Windows создаётся виртуальный COM-порт. При создании виртуального COM-порта система может потребовать драйвер устройства; в ответ на такой запрос следует предоставить системе файл stmcdc.inf, поставляемый в приложении к контроллеру.

При наличии физического COM-порта следует соединить контроллер

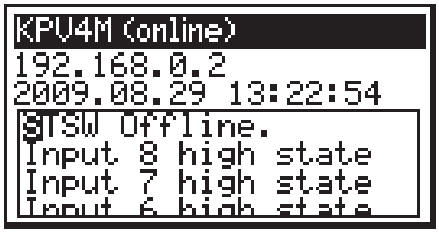


**Рис. 5. Вид основного экрана после включения контроллера и присоединения к сети**

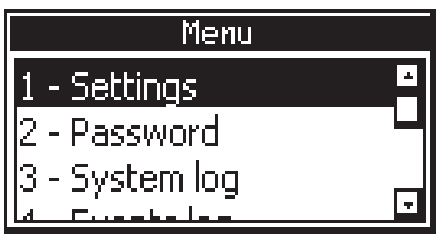


**Рис. 6. Основное меню контроллера**

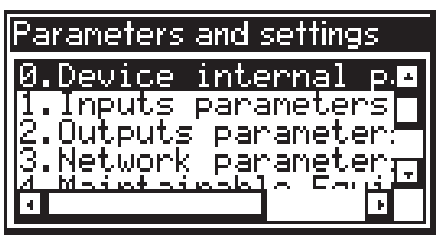


**Рис. 7. Окно при входе в редактирование параметров контроллера**


**Рис. 8. Пример окна редактирования первого IP-адреса назначения SNMP-трапов**

и компьютер обычным, «прямым» кабелем RS-232 . На ПК должна быть запущена терминальная программа, настроенная на режим <115200,8,n,1>. После подачи питания на контроллер на экране терминала должна появиться запись с версией начального загрузчика:

```
Bootloader started. Ver: Aug 29
2009 21:20:58
SD card initialized.
```

Далее отобразится информация о процессе обновления программного обеспечения или его проверки.

Чтобы начать работу с меню устройства, следует нажать кнопку Enter на ПК. Работа с программным монитором и меню контроллера через терминальную программу рассматривается в документе «Работа с монитором KPV-4M», поставляемом в приложении.

Чтобы удалённо подсоединиться к контроллеру через протокол Telnet, необходимо включить контроллер в сеть Ethernet. Если такая связь установлена, то одним из возможных способов подключения к контроллеру будет следующий:

- в системе Windows в меню Start Run ввести команду cmd;
- в открывшемся окне набрать команду telnet {IP-адрес контроллера};
- если команда прошла успешно, то в окне появиться диалог, аналогичный терминальной программе.

Контроллер запрограммирован для поддержки не более двух одновременных telnet-сессий.

### Использование web-интерфейса

Контроллер KPV-4M имеет встроенный web-сервер. Для работы с web-сервером можно использовать любой web-браузер. Чтобы открыть главную страницу web-сервера, в строке URL следует ввести адрес контроллера по умолчанию (http://192.168.0.2). На главной странице web-сервера контроллера расположена информация о работе внешнего подключенного инвертора фирмы Gamatronic. С главной страницы также можно перейти:

- в меню редактирования параметров устройства;
- в панель состояния входов/выходов и установки состояний выходов;
- в диагностическую панель состояния центрального процессора контроллера;
- в панель редактирования списка привилегированных пользователей;
- в другие диагностические панели.

Для редактирования и просмотра параметров устройства web-сервер запрашивает аутентификацию пользователя. По умолчанию в контроллере установлен пользователь Developer с административными правами. При запросе аутентификации следует ввести:

- Name: Developer
- Password: 14789632

### Настройка и работа с клавиатурой и дисплеем

Клавиатура и дисплей контроллера позволяют просматривать текущий журнал событий контроллера, дату и время, IP-адрес устройства в сети и т.д. На рисунке 5 показано основное окно контроллера. В верхней строке выводится сетевое имя контроллера и его статус подключения к сети. В следующей строке выводится IP-адрес устройства. Ниже – текущая дата и время. Если контроллер не смог связаться с серверами точного времени, то вместо даты и времени будет прочерк. В контроллере можно задать до двух произвольных IP-адресов серверов точного времени либо отключить функцию синхронизации.

Нижнюю половину экрана занимает журнал текущих событий. Вверху отображаются более поздние события. Журнал можно прокручивать вверх и вниз кнопками стрелок. Журнал можно стереть, нажав кнопку [Del].

Для перехода в основное меню прибора (см. рис. 6) необходимо нажать кнопку [Menu]. Из меню можно перейти в режим редактирования параметров, в режим просмотра различных журналов и в режим ввода пароля. Для этого нужно стрелками вверх и вниз установить выделение на нужном пункте и нажать кнопку [Enter]. Для возврата на предыдущий уровень меню следует нажать кнопку [Esc]. Пароль требуется вводить, только если в настройках прибора включен режим ограничения доступа.

По умолчанию ввод пароля для редактирования параметров устройства не требуется. В контроллере предусмотрено два пароля: один позволяет только считывать параметры, второй позволяет их редактировать. Также в приборе можно ввести пароль для разблокирования клавиатуры после некоторого времени простоя. Блокировка клавиатуры по умолчанию отключена.

При входе в меню редактирования параметров (см. рис. 7) выбор требуемого пункта производится стрелками вверх-вниз, также возможен прямой выбор пункта по номеру нажатием соответствующей цифровой кнопки. Меню параметров имеет древовидную структуру. Возврат на предыдущий уровень производится кнопкой [Esc]. Если название пункта меню не помещается целиком на экране, то его можно прочитать, используя кнопки со стрелками влево и вправо. При входе в режим редактирования параметра появляется окно, показанное на рисунке 8.

При редактировании цифровых параметров можно вводить только цифры и символы точки и знака. При редактировании строковых параметров дополнительно появляется диалог выбора символов. Дополнительные символы есть на всех цифровых клавишах,

а также на кнопках точки, нуля и знаков плюс/минус. После выбора символа следует нажать [Enter].

Если параметр введён правильно, то после нажатия кнопки [Enter] он сразу же записывается в файл параметров на SD-карте. Если требуется отменить редактирование, нажимается кнопка [Esc]. Для перемещения курсора при редактировании можно использовать кнопки стрелок влево/вправо, вверх/вниз, [Del], [Insert], [End], [Home], [BackSp].

## Технология обновления программного обеспечения в контроллере

Программное обеспечение можно обновить двумя путями:

- записью файла boot.bin в корневую директорию SD карты;
- записью файла boot.bin в корневую директорию FTP-сервера контроллера.

Файл boot.bin содержит зашифрованный образ программного кода, загружаемого во внутреннюю флэш-память микроконтроллера. Помимо файла boot.bin, может понадобиться заменить файл PARAMS.INI, чтобы с обновленной программой вступили в действие новые параметры устройства.

Для записи на SD-карту её следует извлечь из выключенного устройства. Файловая система SD-карты имеет формат FAT16, доступный для ПК. Для более надёжного и быстрого чтения контроллером файла boot.bin желательно иметь недавно отформатированную карту без лишних файлов. После записи файла на SD-карту, её вставляют в контроллер и затем включают питание. Спустя примерно минуту контроллер включается и начинает работать по обновлённой программе.

При записи файла boot.bin через FTP-сервер контроллера надо сначала присоединиться к его FTP-серверу. Параметры доступа по умолчанию к FTP-серверу контроллера:

- user name: anonymous
- password: 123@123

После того как файл boot.bin будет записан на FTP-сервер контроллера, следует отключиться от FTP-сервера и подключиться к контроллеру через Telnet (см. настройку прибора и работу через терминал VT100 и Telnet). В главном меню монитора прибора следует выбрать пункт <5> – Reset device. После этого связь с контроллером прервётся. Спустя минуту можно предпринять попытку нового подключения к устройству.

## Демонстрационное программное обеспечение и возможности модернизации устройства

Демонстрационную версию программного обеспечения контроллера KPV-4M можно скачать с интернет-страницы http://www.alylab.eu. Платформа ARM-Dominator 4, на которой сделан контроллер KPV-4M, сохраняет достаточно неиспользованных ресурсов и позволяет расширять функциональность устройства, добавляя в него новые протоколы и интерфейсы.

Так, например, контроллер может служить шлюзом между SNMP-менеджерами и сетями устройств, работающими по протоколу MODBUS или CANopen. Также контроллер применялся для конвертирования данных в SNMP с различных счётчиков электроэнергии, работающих по протоколу IEC 62056-21.