

ООО «С-Терра СиЭсПи»  
124498, г. Москва, Зеленоград, Георгиевский проспект,  
дом 5, помещение I, комната 33  
Телефон: +7 (499) 940 9061  
Факс: +7 (499) 940 9061  
Эл.почта: [information@s-terra.com](mailto:information@s-terra.com)  
Сайт: <http://www.s-terra.com>



## **Программный комплекс «Шлюз безопасности CSP VPN Gate. Версия 3.1»**

**СПДС «ПОСТ»**

**Руководство пользователя**

РЛКЕ.00009-03 90 01.02

19.03.2015

# Содержание

<b>1.</b>	<b>Требования к программно-аппаратным средствам</b>	<b>3</b>
<b>2.</b>	<b>Подготовка АРМ пользователя к работе</b>	<b>4</b>
2.1.	Настройка BIOS	4
<b>3.</b>	<b>Работа с СПДС «ПОСТ»</b>	<b>5</b>
3.1.	Начало работы с СПДС «ПОСТ»	5
3.2.	Административный режим	7
3.3.	Режим пользователя	7
3.4.	Отображение текущего статуса СПДС «ПОСТ»	9
3.5.	Организация ввода/вывода данных	9
3.6.	Диагностическая информация	9
3.7.	Завершение работы с СПДС «ПОСТ»	10
<b>4.</b>	<b>Приложение</b>	<b>11</b>
4.1.	Настройки BIOS для приоритетной загрузки с USB-носителя	11
4.2.	Настройка параметров сетевого соединения	15
4.2.1.	Создание нового соединения-----	17
4.3.	Настройка системы времени	28

# 1. Требования к программно-аппаратным средствам

---

СПДС «ПОСТ» функционирует совместно с ПЭВМ, имеющей следующий минимальный состав технических и программных средств:

- процессор в архитектуре Intel x86I поддерживающий работу устройств по интерфейсу USB стандарта 1.1 и выше;
- свободный USB-порт;
- сетевой интерфейс – Ethernet, WiFi, WiMAX;
- возможность BIOS ЭВМ осуществлять загрузку с USB-устройств.

## 2. Подготовка АРМ пользователя к работе

---

СПДС «ПОСТ» – это специальный загрузочный носитель (СЗН «СПДС-USB-01»), с установленным СКЗИ CSP VPN Gate 3.1 и функциональным программным обеспечением. Продукт СПДС «ПОСТ» работает через USB-порт АРМ пользователя.

СПДС «ПОСТ» предназначен для создания удаленного автоматизированного рабочего места (АРМ) на основе среды построения доверенного сеанса (СПДС).

Пользователь получает от администратора СПДС «ПОСТ» полностью подготовленный к работе. Администратор предварительно должен установить PIN для доступа к специальному загрузочному носителю, создать и разместить на устройстве сертификат, сформировать политику безопасности, задать сетевые настройки и параметры целевого приложения пользователя.

Пользователю необходимо настроить BIOS, чтобы загрузка ОС производилась с USB-устройства. Если АРМ пользователя уже подготовлено к загрузке с USB-устройства, то перейдите к разделу [«Начало работы с СПДС «ПОСТ»](#), в противном случае – выполните настройку BIOS.

Действия пользователя по подготовке к работе с СПДС «ПОСТ» могут различаться, в зависимости от типа исполнения и сценария использования Продукта. Эти действия могут быть выполнены администратором, если это предусмотрено сценарием использования Продукта.

### 2.1. Настройка BIOS

Настройте BIOS Вашего компьютера для приоритетной загрузки ОС с USB-устройства, выполнив следующие действия:

1. Подключите специальный загрузочный носитель к USB-порту выключенного компьютера (АРМ).
2. Включите компьютер и войдите в программу настройки BIOS. Клавиши, позволяющие попасть в программу настройки BIOS, обычно отображаются на экране монитора.
3. Настройте приоритетную загрузку с USB-носителя (в настройках BIOS специальный загрузочный носитель будет показываться как S-terra Boot Partition).
4. Выйдите из режима настроек с сохранением изменений.
5. Начнется загрузка со специального загрузочного носителя.

Дальнейшие действия описаны в следующем разделе.

Примечание: если у Вас возникли затруднения при настройке BIOS, посмотрите раздел [«Приложение»](#), в котором описано выполнение настроек BIOS для различных устройств.

## 3. Работа с СПДС «ПОСТ»

---

При работе с СПДС «ПОСТ» пользователь получает доступ только к целевому программному обеспечению. Доступ к операционной системе, сторонним приложениям и периферийным устройствам АРМ, за исключением специально разрешенных к использованию исключен, что обеспечивает целостность программной среды терминала удаленного доступа и изоляцию вычислительного процесса клиента удаленного доступа в ходе доверенного сеанса.

Существует два режима работы с СПДС «ПОСТ»:

- административный режим,
- режим пользователя.

Административный режим предназначен для выполнения администратором конфигурационных действий.

В пользовательском режиме выполняется работа с целевым функциональным программным обеспечением. В данном документе описывается работа с функциональным программным обеспечением – RDP-клиент.

Режим работы выбирается только во время загрузки. Чтобы сменить режим работы, надо закончить работу и перезагрузить компьютер.

### 3.1. Начало работы с СПДС «ПОСТ»

Подключите специальный загрузочный носитель к USB-порту выключенного компьютера (АРМ). АРМ пользователя должно быть подготовлено к загрузке ОС с USB-устройства. Включите компьютер. Начнет выполняться загрузка со специального загрузочного носителя:

1. На экране появится текстовое сообщение «С-Терра ПОСТ» и серийный номер СПДС «ПОСТ». Запрашивается PIN пользователя, ввод PIN маскируется знаками «\*».

**Примечание:** Если PIN введен неправильно, дается еще 4 попытки, после чего специальный загрузочный носитель будет заблокирован. Перед тем, как устройство будет заблокировано, выдается диагностическая информация. Разблокировать устройство может пользователь, идентифицированный как администратор. Блокировка производится аппаратными средствами. При утрате паролей пользователя и администратора дальнейшее использование СПДС «ПОСТ» будет невозможно.

2. Затем появляется заставка СПДС «ПОСТ (Рисунок 1). Происходит дальнейшая загрузка, во время которой проверяется подлинность программного обеспечения. На экране отображается информация о происходящем этапе процесса загрузки.



Рисунок 1

3. Из заданных сетевых профилей выбирается первый, приводящий к успешному соединению. Если соединение установить не удалось, то появляется предупреждение (Рисунок 2). Пользователь (если это разрешено) может выполнить настройки сетевого соединения.

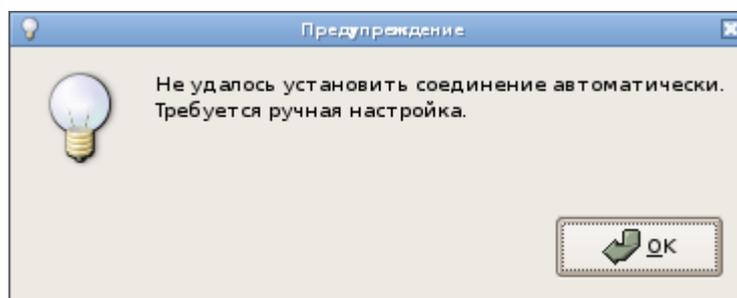


Рисунок 2

4. На панели задач появляются иконки, нажав на которые можно вызвать программы [настройки системы времени](#) и [сетевого соединения](#) (Рисунок 3). Если далее предполагается работать в административном режиме, то рекомендуется выполнить эти настройки до выбора режима работы. Описание настроек приведено в Приложении, в соответствующих разделах – [«Настройка параметров сетевого соединения»](#) и [«Настройка системы времени»](#).



Рисунок 3

5. Далее пользователю предлагается выбрать режим работы. Появится окно (Рисунок 4), с предложением запустить административный режим и убывающим

прогресс-баром (по завершению таймаута будет запущен режим пользователя). Нажмите *OK* для перехода в административный режим либо *Отмена* для перехода в режим пользователя.

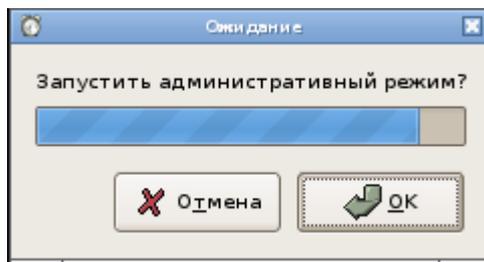


Рисунок 4

6. После выбора режима работы запускается соответствующее функциональное программное обеспечение:
- ♦ в административном режиме – *Клиент управления*,
  - ♦ в режиме пользователя – *Клиент RDP*.

## 3.2. Административный режим

При выборе *Административного режима* запускается административный сеанс, во время которого выполняется обновление конфигурационных настроек СПДС «ПОСТ». При этом будет заблокирован доступ пользователя к управлению операционной системой компьютера и средой функционирования СПДС «ПОСТ».

После окончания обновления произойдет отключение компьютера.

## 3.3. Режим пользователя

В режиме работы пользователя должно установиться соединение с удаленным ресурсом, адрес которого был указан администратором при подготовке СПДС «ПОСТ» к работе, или запускается приложение, дающее пользователю возможность выбора удалённого ресурса, если администратором задан их перечень (Рисунок 5).

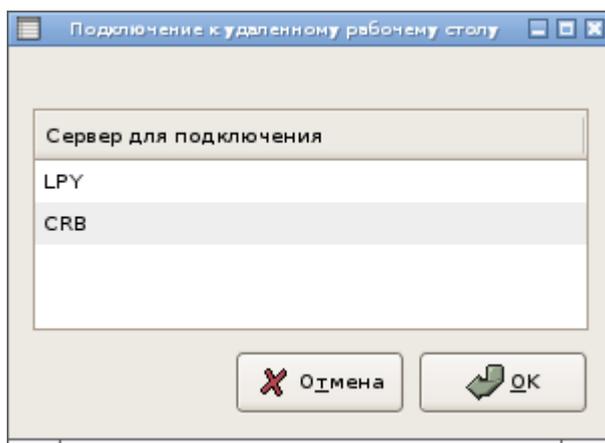


Рисунок 5

В случае если администратор не указал адрес удалённого ресурса или не удалось установить соединение с единственным заданным сервером, то будет запрошен адрес сервера (Рисунок 6).

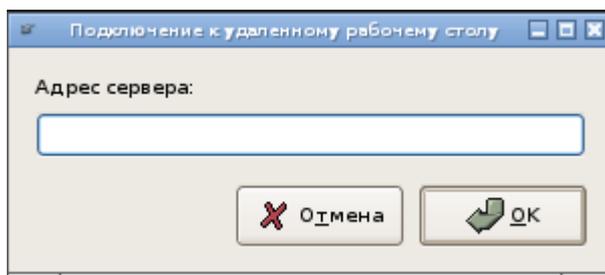


Рисунок 6

После подключения, СПДС «ПОСТ» становится доступен на терминальном сервере в качестве сетевого диска. Пользователь получает возможность обмениваться данными между специальным загрузочным носителем и приложениями терминального сервера. Размер области памяти, доступной пользователю для чтения/записи на специальном загрузочном носителе, составляет: 226Мб при объеме установленной памяти 2Гб и 1834Мб при объеме установленной памяти 4Гб.

### 3.4. Отображение текущего статуса СПДС «ПОСТ»

Наличие защищенного соединения	
VPN соединение отсутствует	
Установлено соединение VPN	
Наличие сетевого соединения	
Сетевое соединение отсутствует	
Сетевое соединение активно	

### 3.5. Организация ввода/вывода данных

Организация ввода/вывода данных определяется сценарием использования СПДС «ПОСТ» и политикой безопасности, заданной администратором.

СПДС «ПОСТ» запрещает доступ к жестким дискам, съемным носителям и системам ввода-вывода АРМ пользователя, за исключением:

- видеокарты,
- клавиатуры (доступ только в режиме работы пользователя),
- мыши (доступ только в режиме работы пользователя).

Если СПДС «ПОСТ» используется для терминального доступа, то пользователь может:

- обмениваться данными между специальным загрузочным носителем и приложениями, работающими на удалённом ресурсе;
- печатать из приложений, работающих на удалённом ресурсе, на сетевой принтер, доступный с ПАК СПДС по локальной сети;
- печатать из приложений, работающих на удалённом ресурсе, на PDF-принтер и сохранять полученный файл на специальном загрузочном носителе.

Настройки сервиса печати выполняются администратором при подготовке СПДС «ПОСТ» к работе и могут быть изменены позднее, в ходе административного сеанса.

### 3.6. Диагностическая информация

Диагностическая информация собирается для каждого сеанса и записывается на специальный загрузочный носитель в каталог `disk/diaginfo` в виде архивного файла. Имя архивного файла содержит идентификатор данного экземпляра СПДС

«ПОСТ», дату и время, а также дополнительный указатель на момент создания файла (*on* – файл создан при загрузке продукта, *off* – при окончании работы, *run* – во время работы продукта).

В архивном файле находятся сведения об аппаратной платформе, на которой выполнялась загрузка СПДС, а также журнал сообщений, формируемый системой протоколирования событий.

Диагностическая информация хранится для пяти последних сессий.

Мониторинг и событийное протоколирование происходит на основе протоколов Syslog и SNMP в составе СКЗИ CSP VPN Gate 3.1.

## 3.7. Завершение работы с СПДС «ПОСТ»

### Административный режим

В административном режиме завершение работы выполняется автоматически – после применения обновлений компьютер выключается.

В критической ситуации, в случае зависания (обрыва) соединения, отключите питание и извлеките специальный загрузочный носитель из USB-разъема компьютера.

### Режим пользователя (Клиент RDP)

Завершение работы с СПДС «ПОСТ» в режиме пользователя можно выполнить, нажав на иконку в верхней левой части экрана (Рисунок 7) и выбрав пункт меню *Завершение работы*.

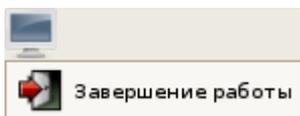


Рисунок 7

В случае, если в настройках присутствует только один RDP-сервер, то завершение работы автоматически выполняется после закрытия RDP-сессии (*Пуск*→*Завершение сеанса*).

В обоих случаях будет запрошено подтверждение на завершение работы.

## 4. Приложение

### 4.1. Настройки BIOS для приоритетной загрузки с USB-носителя

Подключите специальный загрузочный носитель к USB-порту выключенного компьютера (APM).

Клавиши, позволяющие попасть в программу настройки BIOS (BIOS Setup), появляются на экране сразу после включения компьютера. Эти клавиши также можно посмотреть в документации на компьютер. Возможные клавиши или комбинации клавиш для вызова программы настройки приведены в нижеследующей таблице.

Таблица 1

Производитель BIOS	Клавиши
ALR Advanced Logic Research, Inc.	F2, Ctrl+Alt+Esc
AMD (Advanced Micro Devices, Inc.) BIOS	F1
AMI (American Megatrends, Inc.) BIOS	Del
Award BIOS	Del, Ctrl+Alt+Esc
DTK (Datatech Enterprises Co.) BIOS	Esc
Phoenix BIOS	Ctrl+Alt+Esc, Ctrl+Alt+S, Ctrl+Alt+Ins
Производитель ПК	Клавиши
Acer	F1, F2, Ctrl+Alt+Esc
Compaq	F10
Dell	F1, F2, F3, Del, Fn+F1
eMachine	Del
HP (Hewlett-Packard)	F1, F2
IBM	F1, F2, Ctrl+Alt+Ins, Ctrl+Alt+Del
Sony VAIO	F2, F3
Toshiba	Esc, F1

Войдите в программу настройки BIOS. В различных версиях BIOS эти настройки будут отличаться. Далее рассмотрим некоторые возможные варианты настроек.

## Вариант 1

В разделе **Boot** выберите пункт **Boot Device Priority** (Рисунок 8).

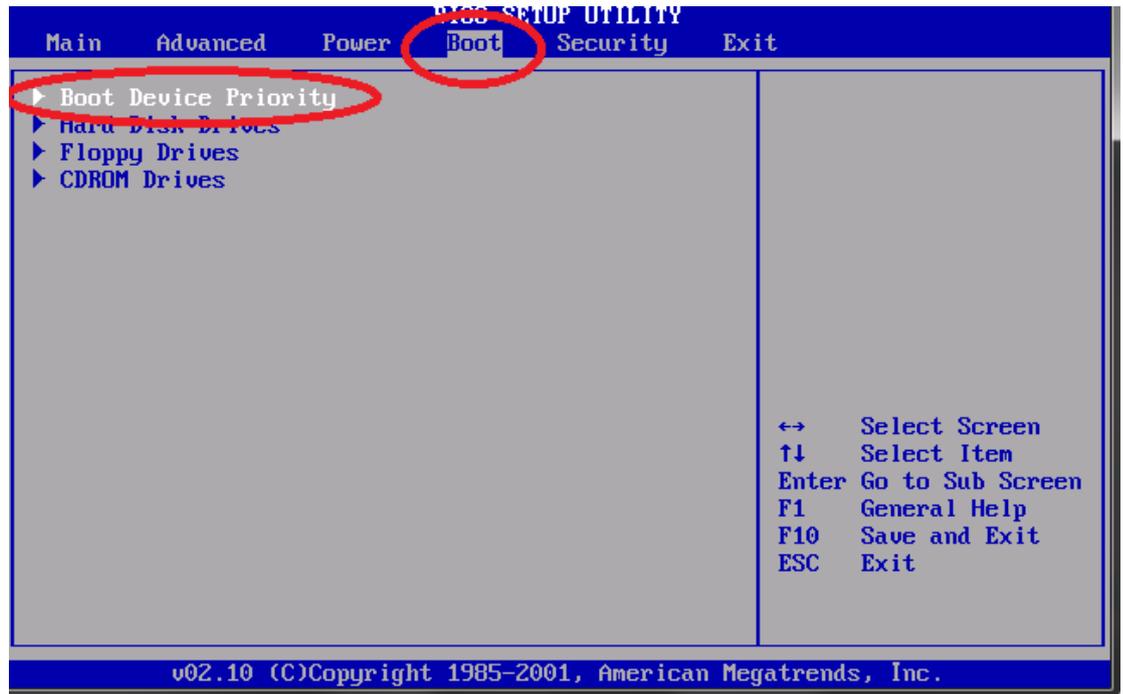


Рисунок 8

В качестве **1st boot device** укажите **S-terra Boot Partition**. Повысить/понижить приоритет устройства можно с помощью клавиш F6/F5, или «+»/«-», или одновременным нажатием Shift и «+»/Shift и «-». В различных BIOS эти клавиши могут отличаться.

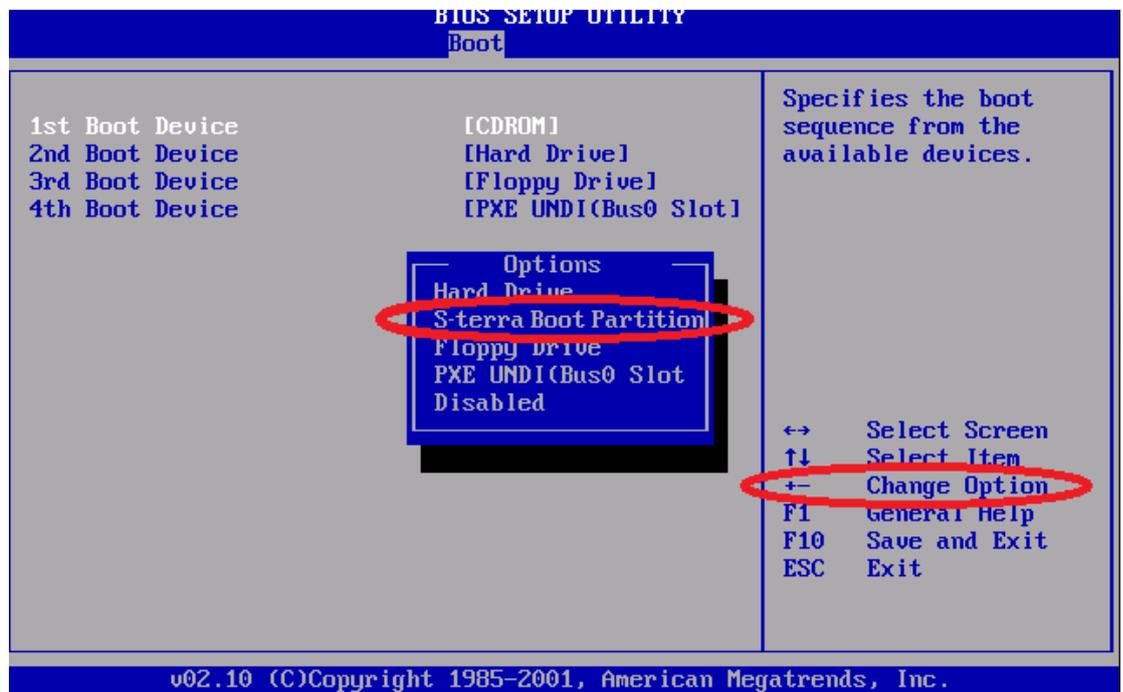


Рисунок 9

Выйдите из программы настройки BIOS с сохранением изменений **Save and Exit**. Обычно это клавиша F10.

## Вариант 2

Выберите раздел **Advanced Setup** (Рисунок 10).

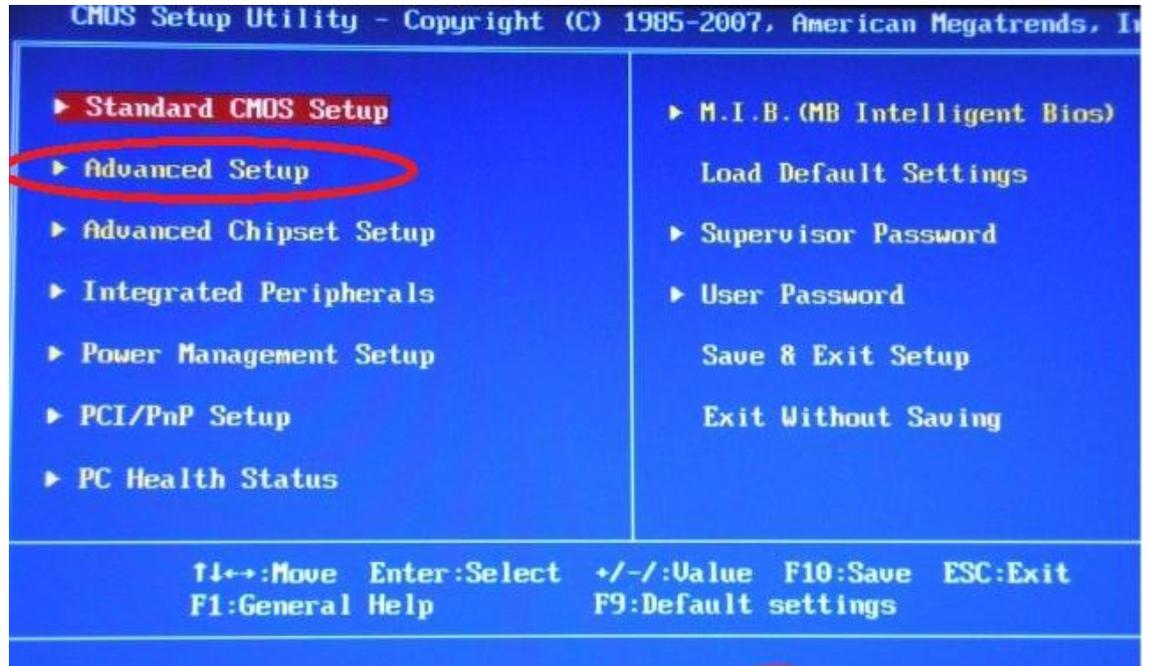


Рисунок 10

В качестве **1st boot device** укажите **S-terra Boot Partition** (Рисунок 11).



Рисунок 11

Выйдите с сохранением изменений – F10.

### Вариант 3

В некоторых BIOS есть опция быстрого выбора устройства, с которого будет осуществляться загрузка (Рисунок 12). Для выбора устройства нажмите **F12**.

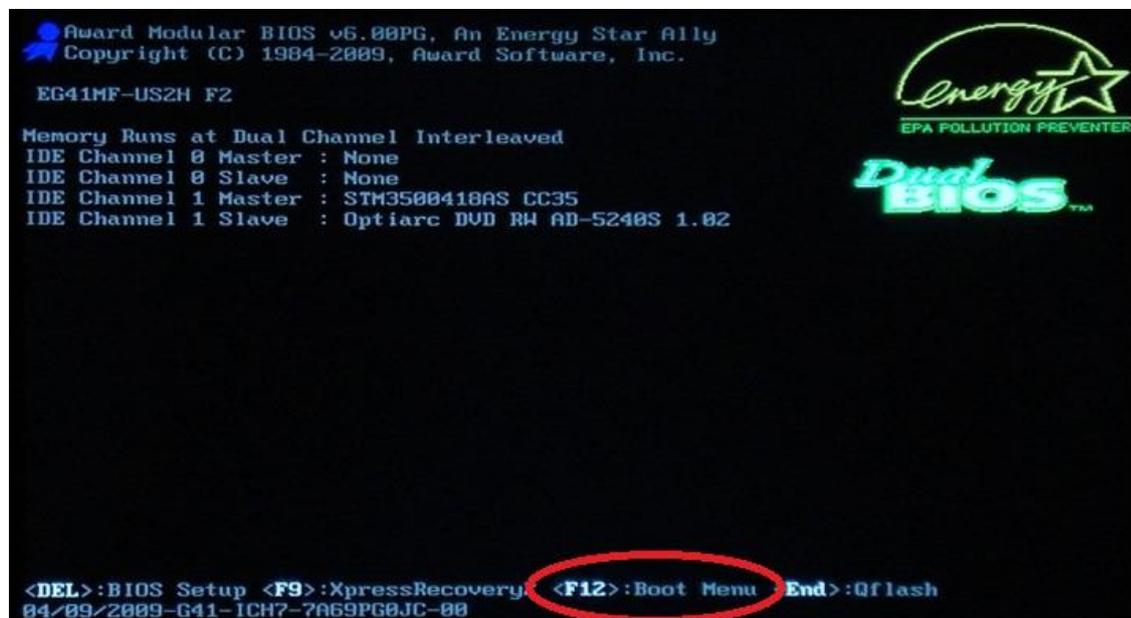


Рисунок 12

В качестве устройства выберите **S-terra Boot Partition** (Рисунок 13).

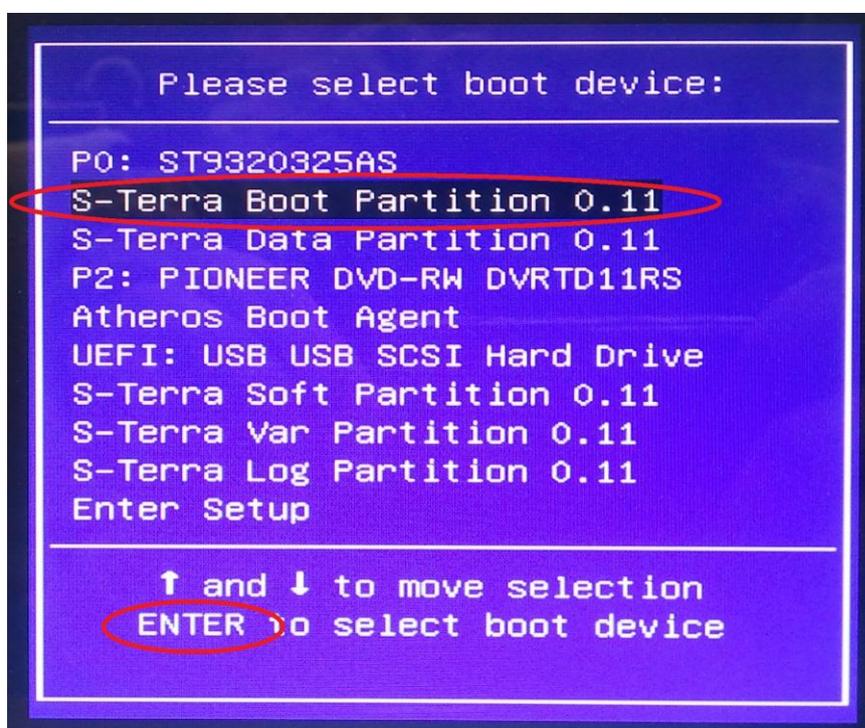


Рисунок 13

## 4.2. Настройка параметров сетевого соединения

Возможность изменять параметры сетевого соединения для пользователя определяет администратор. Если пользователю разрешено настраивать сетевые соединения, то он получает доступ к апплету Network Manager, при помощи которого выполняется настройка сети. Следует отметить, что политика обработки трафика пользователя задается администратором, при настройке СПДС «ПОСТ».

Иконка Network Manager апплета (Рисунок 14) отображается в верхней правой части экрана. Вид иконки зависит от типа соединения и состояния соединения.



Рисунок 14

Если навести указатель на иконку и нажать левую кнопку, то появятся следующие пункты меню:

- *Проводные сети*, со списком доступных проводных сетей. (Сеть WiMax (Yota) работает через Ethernet-интерфейс и показывается/настраивается как проводная сеть.)
- *Беспроводные сети*, со списком доступных видимых беспроводных сетей.

Если навести указатель на иконку и нажать правую кнопку указателя – станет доступно меню (Рисунок 15).

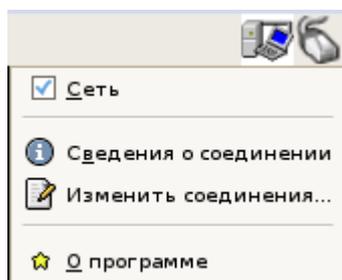


Рисунок 15

Чтобы получить сведения о текущем соединении, наведите указатель на иконку, нажмите правую кнопку указателя и выберите пункт меню *Сведения о соединении*. Появится окно (Рисунок 16).



Рисунок 16

Вы можете изменить сведения о соединении. Для этого наведите указатель на иконку Network Manager, нажмите правую кнопку указателя и выберите пункт меню *Изменить соединения...*

В окне (Рисунок 17) войдите в нужную вкладку сетевого соединения:

- Проводные.
- Беспроводная сеть.

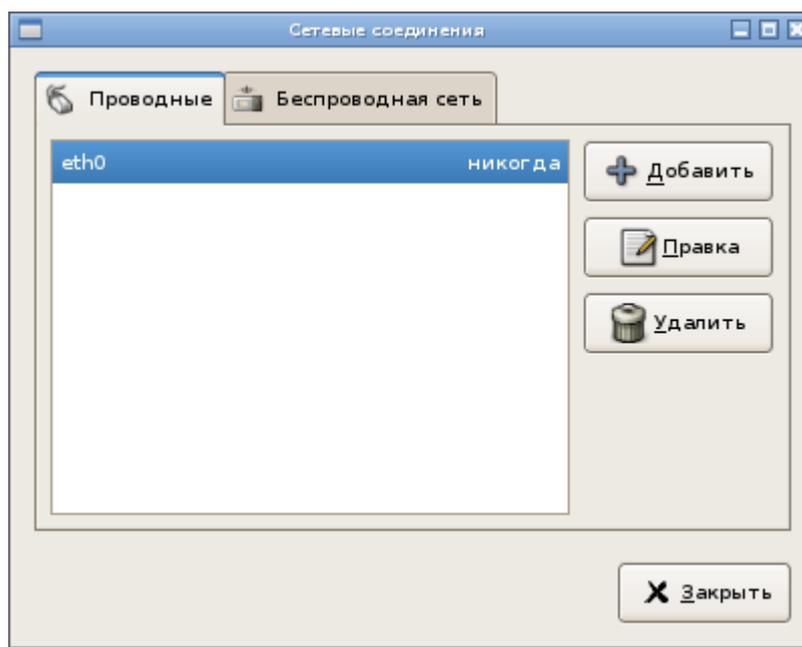


Рисунок 17

Нажмите кнопку *Правка*. Если необходимо создать новое соединение, то нажмите кнопку *Добавить*.

Появится окно, в котором будем производить дальнейшие изменения настроек соединения. Вид окна будет различаться, в зависимости от типа настраиваемого соединения. Далее рассмотрим настройки для различных типов соединений.

Необходимые значения настроек можно узнать у провайдера или у системного администратора.

## 4.2.1. Создание нового соединения

### 4.2.1.1. Создание проводного соединения

В окне **Изменение Проводное соединение 1** (Рисунок 18), во вкладке **Проводные** укажите:

*Имя соединения* – задается имя соединения.

*Подключать автоматически* – если флажок установлен, то при наличии сетевых ресурсов подключение будет выполняться автоматически, иначе подключение придется выполнять вручную.

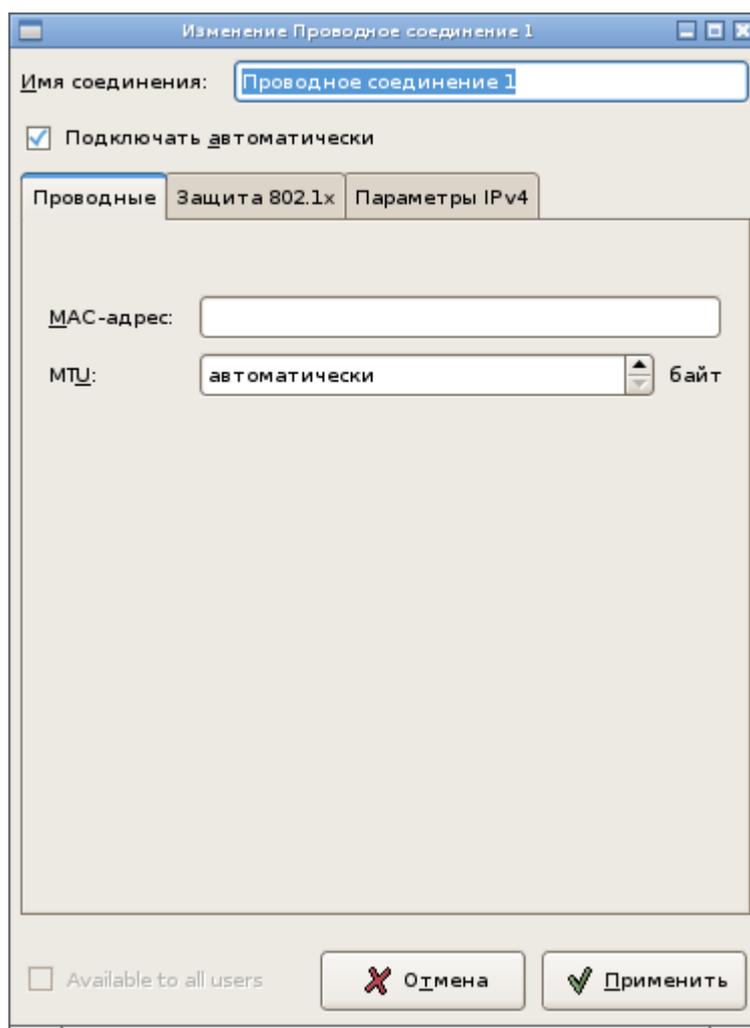


Рисунок 18

*МАК-адрес* – аппаратный адрес сетевой карты.

*MTU* – максимальный размер пакета в байтах, передаваемый без фрагментации. По умолчанию определяется автоматически.

#### Вкладка **Защита 802.1x**

Если нужно использовать аутентификацию по стандарту 802.1x, то установите флажок *Использовать защиту 802.1X для этого соединения* (Рисунок 19). По умолчанию защита не используется.

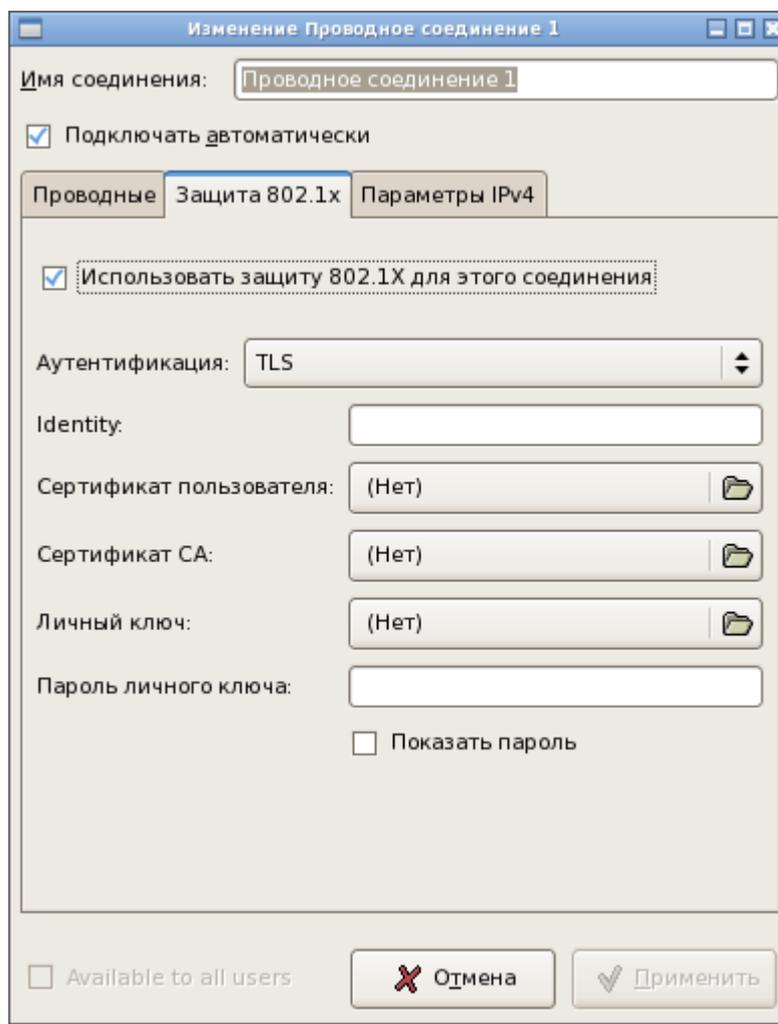


Рисунок 19

При установке флажка доступными становятся следующие поля:

- ◆ *Аутентификация*:
  - TLS – тип метода аутентификации, использующий протокол EAP и протокол защиты транспортного уровня (Transport Layer Security).
  - Туннелированный TLS – Tunnelled Transport Layer Security – определяет протокол и идентификационную информацию, используемую для аутентификации пользователя.
  - Защищено EAP (PEAP) – аутентификационный протокол EAP (Extensible Authentication Protocol) стандарта IEEE 802.1X.
- ◆ *Identity* – идентификационная информация (имя пользователя или логин).

- ◆ Сертификат пользователя.

Появляется окно **Выбрать персональный сертификат...**

- ◆ Сертификат СА

Появляется окно **Выбрать сертификат Центра сертификации...**

- ◆ Личный ключ

Появляется окно **Выбрать личный ключ...**

- ◆ Пароль личного ключа

- ◆ Показать пароль

Во вкладке **Параметры IPv4** (Рисунок 20) можно задать параметры DHCP или статического подключения к Интернету.

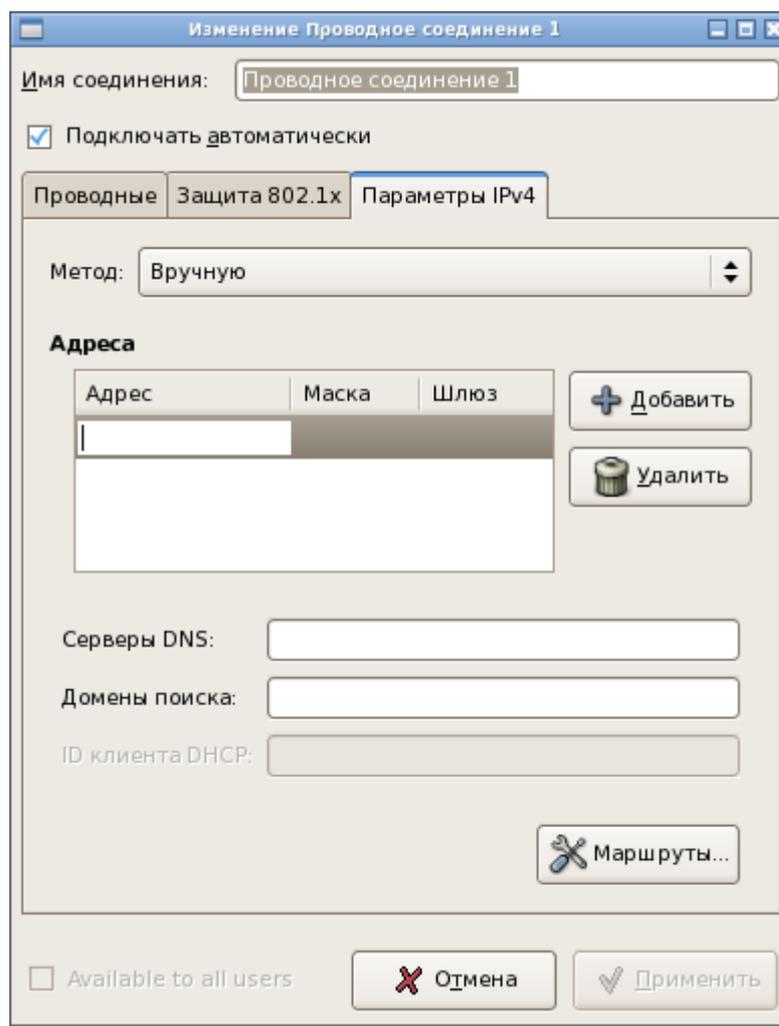


Рисунок 20

Выберите *Метод* подключения:

- ◆ *Автоматически (DHCP)* – операционная система определяет параметры автоматически (по умолчанию).

При выборе этого метода становятся доступными поля:

- *ID клиента DHCP* – локальная машина, которую сервер DHCP может использовать для изменения аренды и параметров DHCP

- и кнопка *Маршруты*, которая вызывает окно (Рисунок 21) с таблицей маршрутизации.
- ◆ *Автоматически (DHCP, только адрес)* – если выбран этот метод, будет использоваться автоматическая настройка адресов DHCP, а поле *Серверы DNS* должно содержать как минимум один IP-адрес

Становятся доступными поля:

- *Серверы DNS*
- *Домены поиска*
- *ID клиента DHCP*
- и кнопка *Маршруты*
- ◆ *Вручную* – если выбран этот метод, будет использоваться статическая адресация, а поле *Серверы DNS* должно содержать как минимум один IP-адрес.

Становятся доступными поля:

- *Адреса*  
*Добавить/Удалить Адрес, Маска, Шлюз*
- *Серверы DNS*
- *Домены поиска*
- кнопка *Маршруты*
- ◆ *Только Link-Local* – если выбран этот метод, интерфейсу будет присвоен локальный адрес в диапазоне 169.254.0.0/16.
- ◆ *Общий с другими компьютерами* – если выбран этот метод (что свидетельствует о том, что это соединение будет обеспечивать доступ к другим компьютерам), то интерфейсу будет присвоен адрес в диапазоне 10.42.x.1/24 и будет запущен сервер перенаправления DNS и DHCP. Дополнительно, будет выполнено NAT-преобразование адреса интерфейса в адрес текущего сетевого соединения, используемого по умолчанию.

Окно **Маршруты IPv4 для Проводное соединение** (Рисунок 21), вызывается кнопкой *Маршруты*. Структура маршрута IPv4 включает четыре 32-битных значения: адрес целевой сети IPv4, маска сети, шлюз и метрика.

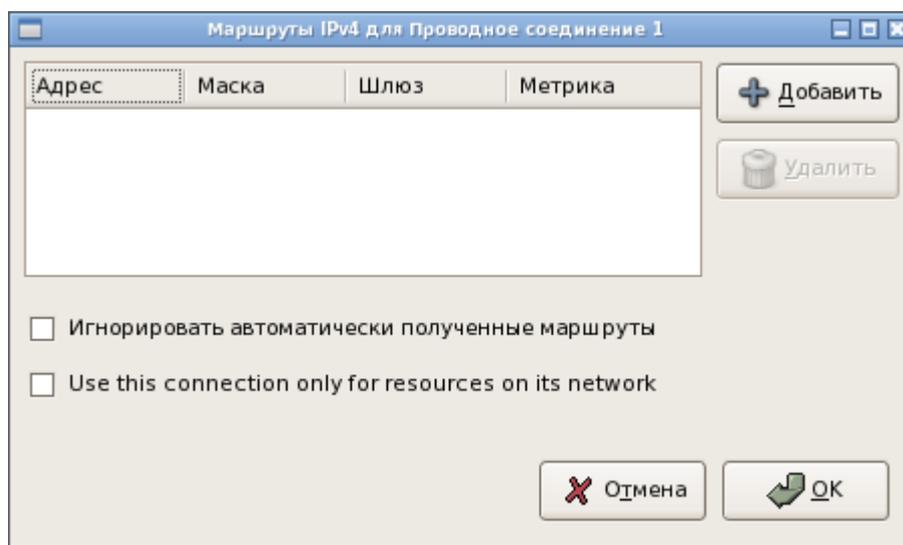


Рисунок 21

## 4.2.1.2. Создание беспроводного соединения

В окне (Рисунок 22), во вкладке **Беспроводная сеть** укажите:

*Имя соединения* – задается имя соединения

*Подключать автоматически* – если флажок установлен, то при наличии сетевых ресурсов подключение будет выполняться автоматически, иначе подключение придется выполнять вручную.

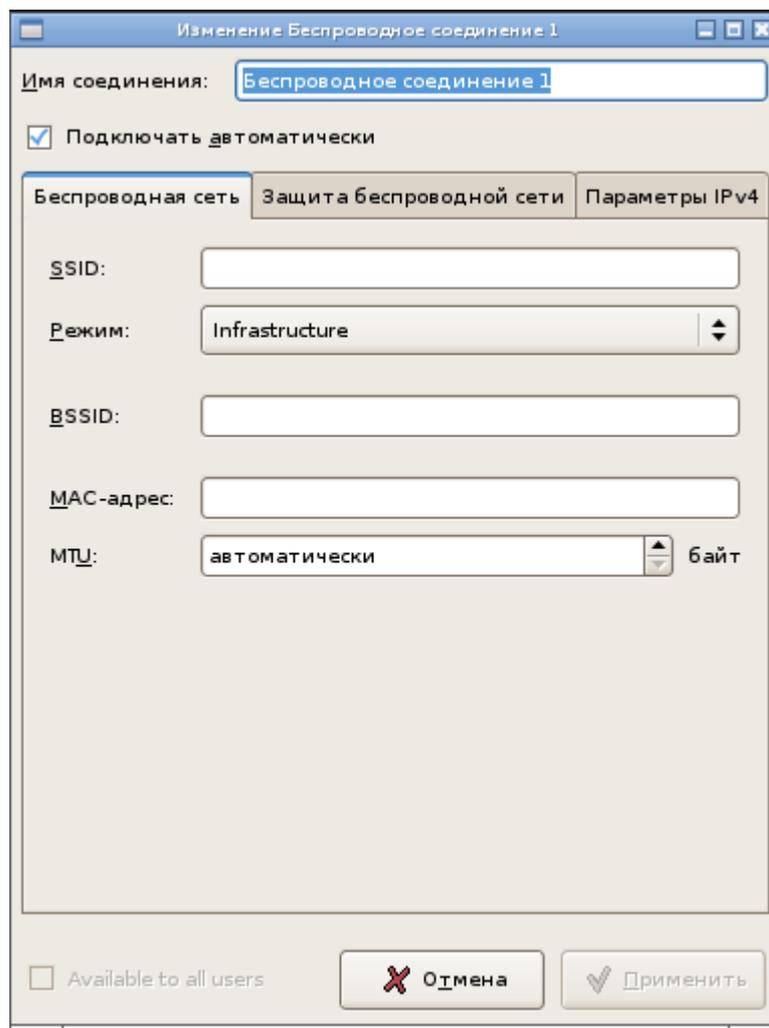


Рисунок 22

*SSID* – идентификатор сети

*Режим* – доступны режимы:

- ◆ Infrastructure – точки доступа (по умолчанию). Подключение к сети выполняется через специальную точку беспроводного доступа.
- ◆ Ad-hoc – точка-точка. Подключение к другому компьютеру осуществляется непосредственно через его адаптер беспроводной связи.

*BSSID* – если определено, то устройство будет сопоставлено только с заданной точкой доступа.

Во вкладке **Защита беспроводной сети** (Рисунок 23) выберите один из методов защиты:

- *Нет*.
- *WEP 40/128-битный ключ* – личный ключ WEP. WEP-шифрование (Wired Equivalent Privacy) использует ключ шифрования для кодирования данных перед их отправкой.
- *WEP 128-битная ключевая фраза* – парольная фраза для расшифровки WEP.
- *LEAP* – защита производится по протоколу LEAP (Light Extensible Authentication Protocol). Аутентификация сервера и клиента 802.1X происходит при помощи пароля, предоставляемого пользователем, шифрование выполняется с использованием индивидуальных динамических ключей.
- *Динамический WEP (802.1x)* – ключ при передаче динамически меняется.
- *WPA & WPA2 Personal* – личный ключ WPA (Wi-Fi Protected Access). Использует для аутентификации предустановленный ключ (Pre-Shared Key).
- *WPA & WPA2 Enterprise* – используется как механизм аутентификации, так и схема шифрования.

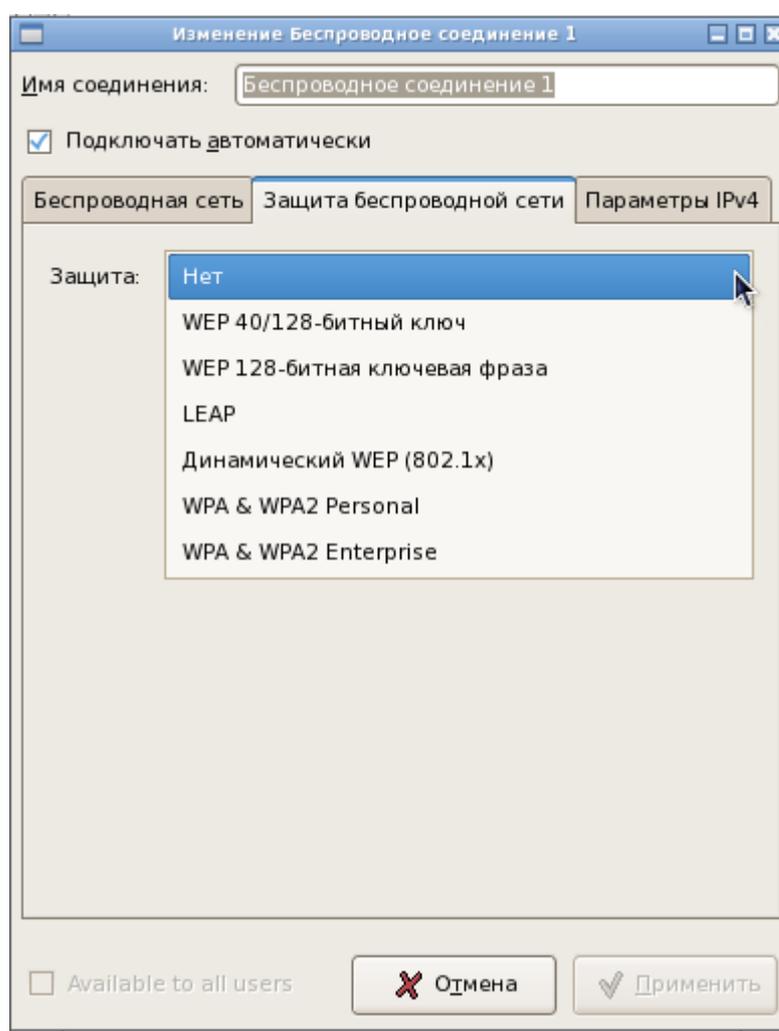


Рисунок 23

В зависимости от выбранного метода защиты будет выведено окно, со списком полей, которые необходимо заполнить.

Если выбран *WEP 40/128-битный ключ* или *WEP 128-битный ключ*, то появится окно (Рисунок 24).

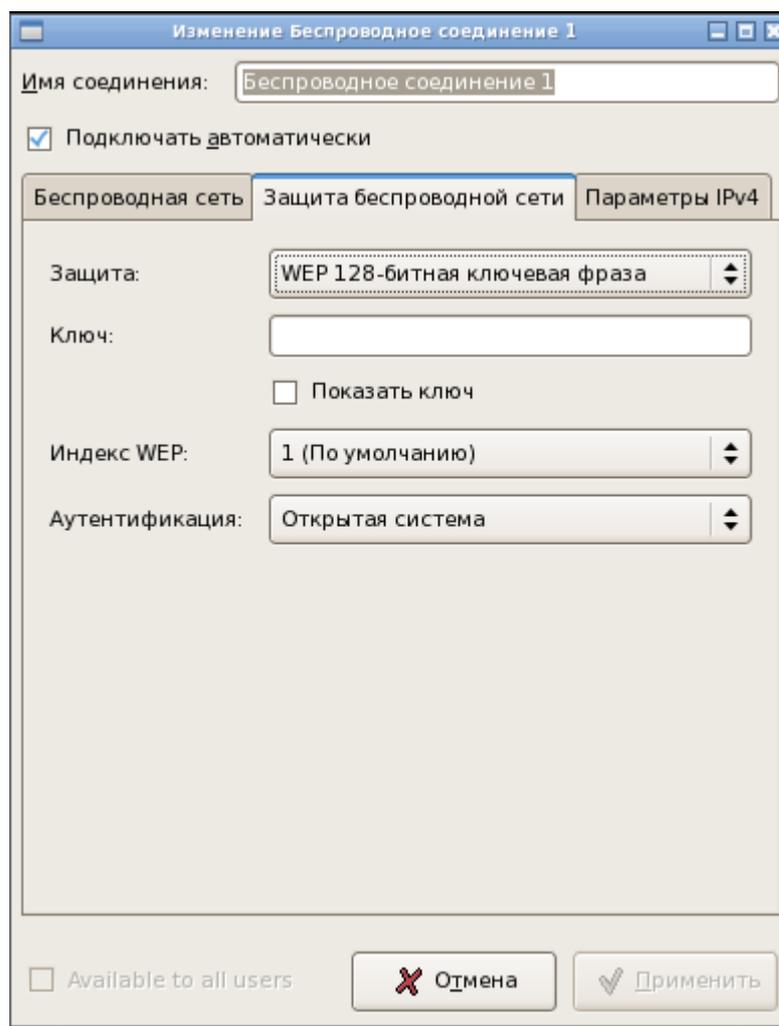


Рисунок 24

*Ключ* – WEP-ключ.

*Индекс WEP* – значение индекса ключа. Станция беспроводной сети может иметь в конфигурации до четырех ключей (значения индекса ключа: 1, 2, 3, 4).

*Аутентификация:*

Открытая система – любое сетевое устройства, имеющее идентификатор SSID (Service Set Identifier) точки доступа может получить доступ к сети.

Общий ключ – выполняется процедура аутентификации с использованием статического WEP-ключа.

Если выбран метод *LEAP*, то появится окно (Рисунок 25), в котором нужно ввести *Имя пользователя* и *Пароль*.

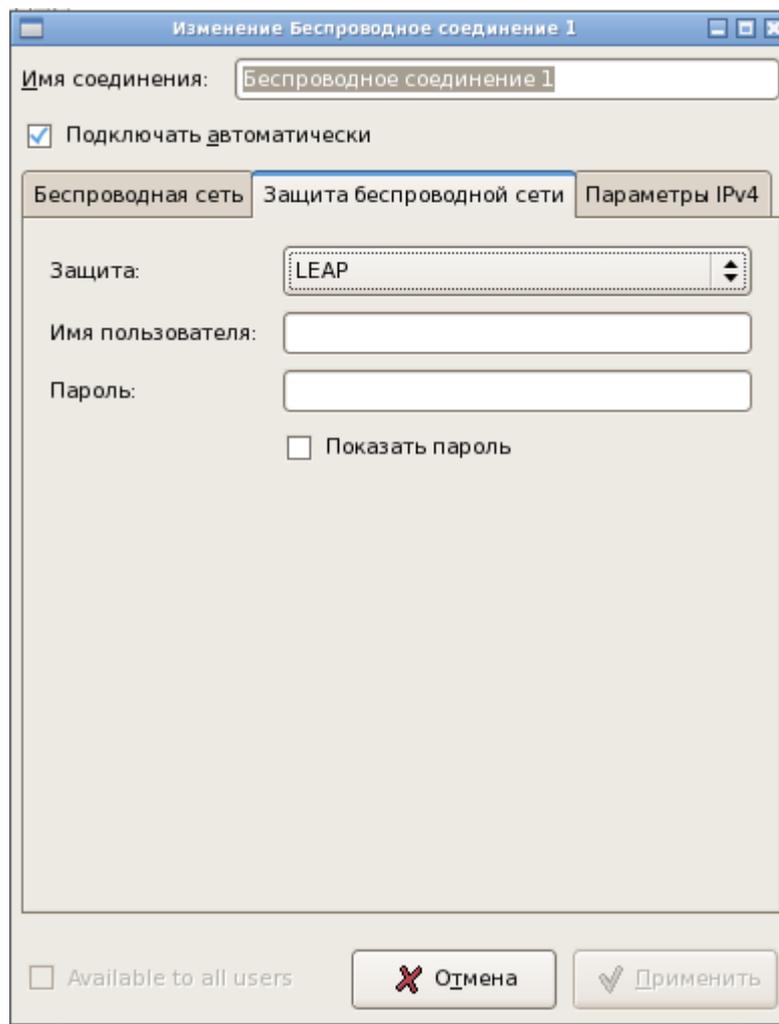


Рисунок 25

Если выбраны методы *Динамический WEP (802.1x)* или *WPA & WPA2 Enterprise*, то в появившемся окне (Рисунок 26), заполните следующие поля:

- *Аутентификация:*
  - ◆ TLS – тип метода аутентификации, использующий протокол EAP и протокол защиты транспортного уровня (Transport Layer Security).
  - ◆ LEAP – используется расширяемый протокол аутентификации (Light Extensible Authentication Protocol), который отвечает за обеспечение процедуры аутентификации и назначение динамического ключа.
  - ◆ Туннелированный TLS – Tunnelled Transport Layer Security – определяет протокол и идентификационную информацию, используемую для аутентификации пользователя.
  - ◆ Защищено EAP (PEAP) – аутентификационный протокол EAP (Extensible Authentication Protocol) стандарта IEEE 802.1X.
- *Identity.*
- *Сертификат пользователя.*

Появляется окно **Выбрать персональный сертификат...**

- *Сертификат CA.*

Появляется окно **Выбрать сертификат Центра сертификации...**

- *Личный ключ.*

Появляется окно **Выбрать личный ключ...**

- *Пароль личного ключа.*

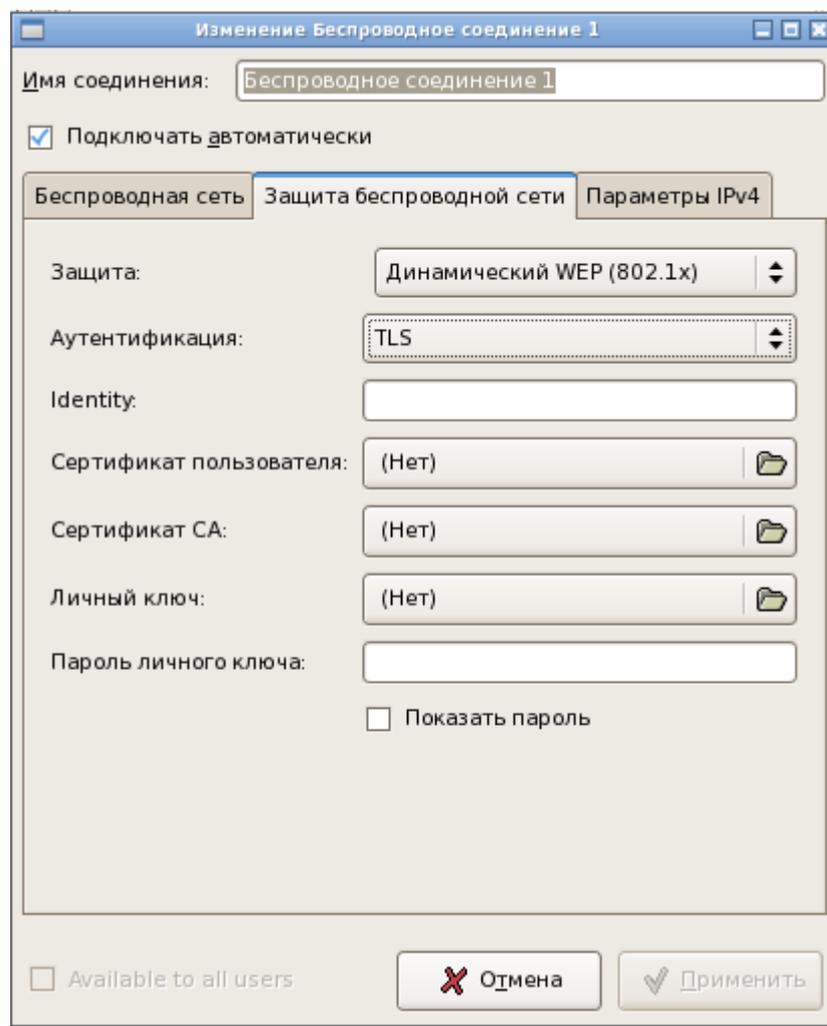


Рисунок 26

Если выбран метод *WPA & WPA2 Personal*, то появится окно (Рисунок 27), в котором нужно ввести *Пароль*.

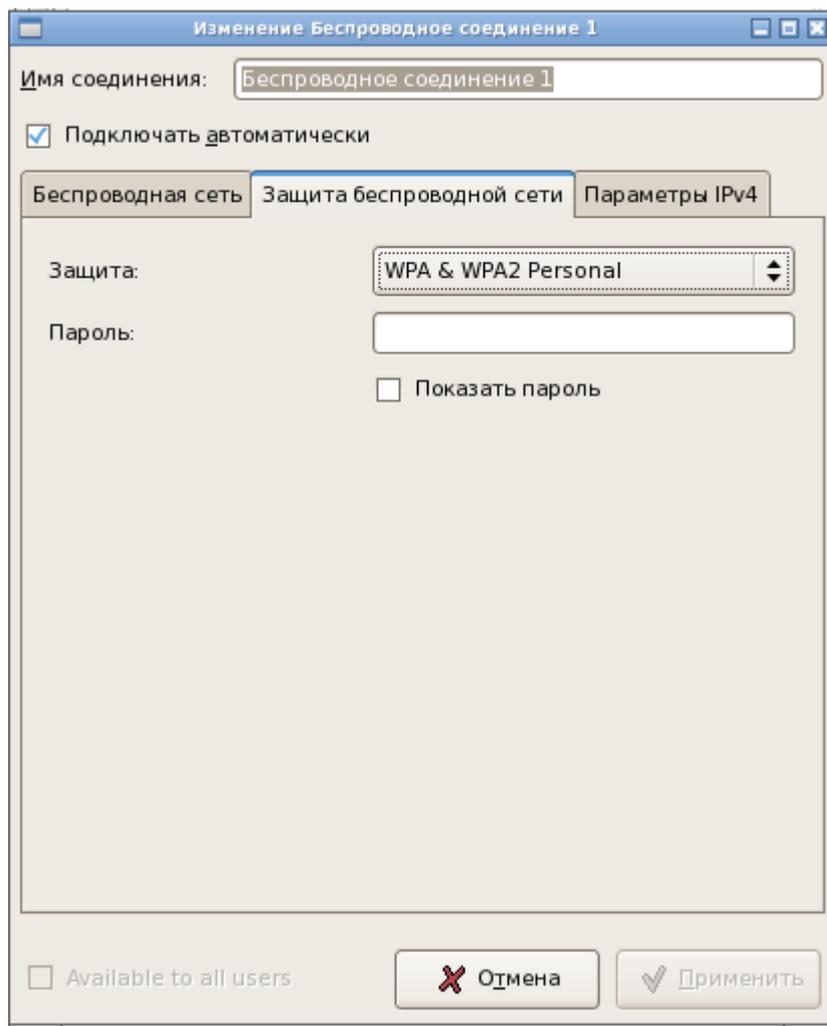


Рисунок 27

Во вкладке **Параметры IPv4** (Рисунок 28) можно задать параметры DHCP или статического подключения к Интернету.

Описание вкладки идентично [описанию для проводных соединений](#).

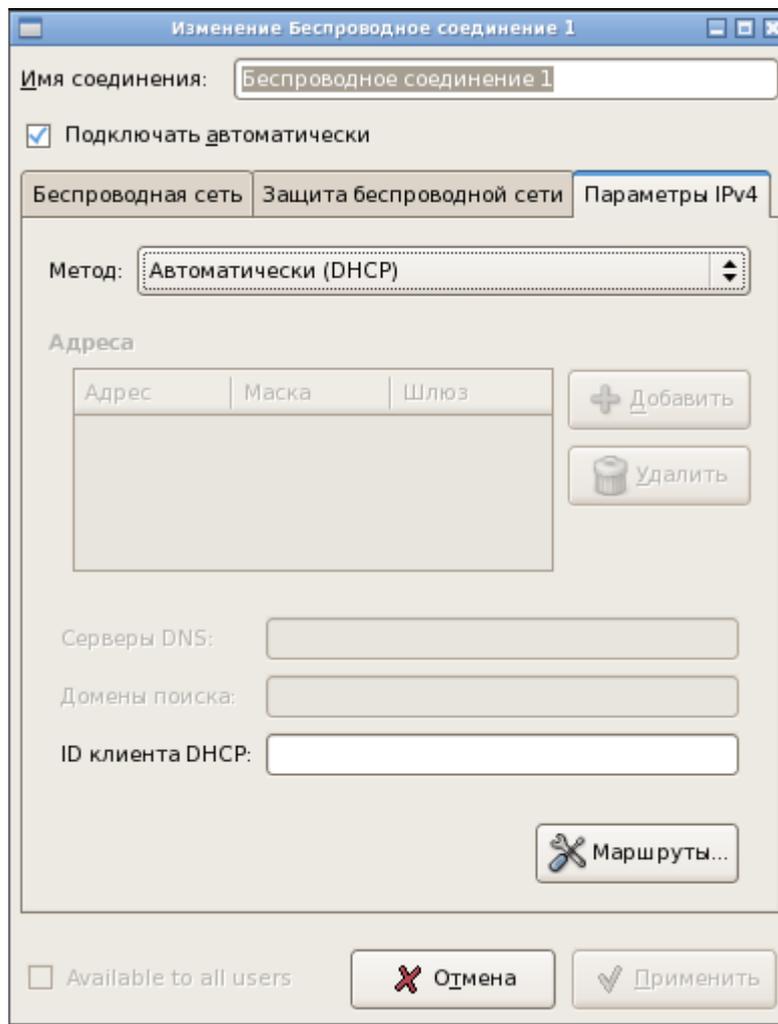


Рисунок 28

## 4.3. Настройка системы времени

В верхней левой части экрана отображается иконка (Рисунок 29), нажав на которую, можно войти в меню *Конфигурирование системы времени* и выполнить настройки системного времени и даты, выбрать часовой пояс и синхронизировать системное время с NTP-сервером точного времени.



Рисунок 29