**Инструкция по установке**

Программный комплекс Bot-Trek TDS предназначен для автоматизированного обнаружения компьютерных атак (вторжений) и вредоносного ПО в сетевом трафике при помощи сигнатурного метода выявления атак и эвристического анализа. Изделие устанавливается на границе сети с целью повышения уровня защищенности ИС, ЦОД, серверов и коммуникационного оборудования, АРМ пользователей.

Сигнатурный анализ трафика выполняется программным комплексом в соответствии с регулярно обновляемым классификатором угроз, созданным на основе лучших мировых практик реагирования на инциденты информационной безопасности, расследований, экспертиз. Источником данных для классификатора являются не только открытые/специализированные Интернет-ресурсы, но и результаты работы подразделений разработчика изделия в указанных выше видах деятельности.

Эвристический анализ трафика выполняется в соответствии с собственной базой правил анализа и выявления аномалий в сетевом трафике.

Программный комплекс Bot-Trek TDS детектирует следующие вторжения – Trojan-Activity, Банковские трояны (Banking), POS-трояны (POS), APT-трояны, Бэкдор-трояны (Backdoor), Нежелательное ПО (Unwanted), Связка эксплойтов (EK), Подозрительная активность (Suspicious), DDoS-трояны, Программы-вымогатели (Ransomware).

Изделие функционирует в среде операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (версия 1.6) Релиз «Смоленск» на отдельно выделенном сервере СОВ.

Для функционирования подсистемы аудита и базы данных системы обнаружения вторжений используется СУБД PostgreSQL версия 9.6 (входит в состав операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (версия 1.6) Релиз «Смоленск»).

Для хранения базы решающих правил используется файловая система ОС «Astra Linux Special Edition».

Для хранения событий, генерируемых сенсором, еще не попавших в базу, используется Redis – сетевое журналируемое хранилище данных типа «[ключ - значение](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_%E2%80%94_%D0%B7%D0%BD%D0%B0%D1%87%D0%B5%D0%BD%D0%B8%D0%B5)» (входит в состав операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (версия 1.6) Релиз «Смоленск»).

# Установка

Для установки компонентов изделия администратор должен обладать навыками работы в системе UNIX/Linux.

## Комплектация поставки/дистрибутива

Состав дистрибутива приведен в таблице 1.

Таблица 1

|  |  |  |
| --- | --- | --- |
| Директория | | Описание |
| TDS\_SENSOR: | | Корневая директория |
|  | libhtp | Директория с пакетом библиотеки libhtp для Suricata |
|  | logrotate | Директория с конфигурационным файлом для ротации логов Suricata |
|  | requirements | Директория с зависимостями для Python кода |
|  | suricata | Директория с пакетом Suricata 4.0.4 |
|  | suricatarules | Директория с пакетом сигнатур Suricata |
|  | tds-api-common | Директория с пакетом REST API продукта |
|  | tds-registry | Директория с пакетом tds-registry |
|  | tds-shell | Директория с пакетом консоли управления tds-shell |
|  | sensor-cert-web | Директория с пакетов веб-интерфейса управления |
|  | install.sh | Установочный скрипт |
|  | backup.sh | Скрипт для резервного копирования |
|  | restore.sh | Скрипт восстановления из бекапа |

Список файлов и их описание приведен в таблице 2.

Таблица 2

| Файл | Путь | Тип файла | Описание |
| --- | --- | --- | --- |
| libhtp2\_0.5.26-1\_amd64.deb | TDS\_SENSOR/libhtp/ | Пакет | Зависимость Suricata |
| suricata | TDS\_SENSOR/logrotate/ | Текст | Файл конфигурации журналирования Suricata |
| suricatarules\_1.0.13-1199\_all.deb | TDS\_SENSOR/suricatarules/ | Пакет | Пакет разрешающих правил Suricata |
| suricata\_4.0.4-2\_amd64.deb | TDS\_SENSOR/suricata | Пакет | Пакет системы обнаружения вторжений Suricata |
| click-6.7-py2.py3-none-any.whl | TDS\_SENSOR/requirements/ | Пакет | Зависимость Python для sensor-cert-web |
| Django-2.0.6-py3.5-none-any.whl | TDS\_SENSOR/requirements/ | Пакет | Зависимость Python для sensor-cert-web |
| Flask-1.0.2-py2.py3-none-any.whl | TDS\_SENSOR/requirements/ | Пакет | Зависимость Python для sensor-cert-web |
| itsdangerous-0.24-py3-none-any.whl | TDS\_SENSOR/requirements/ | Пакет | Зависимость Python для sensor-cert-web |
| Jinja2-2.10-py2.py3-none-any.whl | TDS\_SENSOR/requirements/ | Пакет | Зависимость Python для sensor-cert-web |
| MarkupSafe-1.0-cp35-cp35m-linux\_x86\_64.whl | TDS\_SENSOR/requirements/ | Пакет | Зависимость Python для sensor-cert-web |
| pythondialog-3.4.1-py3-none-any. whl | TDS\_SENSOR/requirements/ | Пакет | Зависимость Python для sensor-cert-web |
| pytz-2018.4-py3-none-any.whl | TDS\_SENSOR/requirements/ | Пакет | Зависимость Python для sensor-cert-web |
| terminaltables-3.1.0-py3-none-any. whl | TDS\_SENSOR/requirements/ | Пакет | Зависимость Python для sensor-cert-web |
| Werkzeug-0.14.1-py2.py3-none-any.whl | TDS\_SENSOR/requirements/ | Пакет | Зависимость Python для sensor-cert-web |
| sensor-api\_1.0.20-1\_all.deb | TDS\_SENSOR/tds-api-common | Пакет | Пакет с REST API |
| tds-registry\_1.1.4-1\_all.deb | TDS\_SENSOR/tds-registry | Пакет | Пакет с вспомогательной утилитой tds-registry |
| tds-shell\_0.1\_all.deb | TDS\_SENSOR/tds-shell | Пакет | Пакет с консольным интерфейсом управления |
| sensor-cert-web\_0.1.0\_all.deb | TDS\_SENSOR/sensor-cert-web | Пакет | Пакет с WEB интерфейсом управления |

## Порядок установки

Последовательность установки программы приведена ниже:

1. Выполнение предварительной подготовки.
2. Настройка локали; Установка зависимостей.
3. Установка Suricata.
4. Установка tds-registry.
5. Установка tds-shell.
6. Установка sensor-api.
7. Установка web.

## Предварительная подготовка к установке

Установка изделия осуществляется на сервер СОВ с установленной ОС «Astra Linux Special Edition».

Пользователь root создается при установке ОС.

При установке ОС «Astra Linux Special Edition» необходимо задать пароль учетной записи ОС root. Данная учетная запись root используется при установке изделия.

В случае если ОС «Astra Linux Special Edition» не установлена на техническое средство необходимо выполнить следующие действия:

1. Вставить в CD/DVD привод диск с ОС «Astra Linux Special Edition».
2. Скопировать образ ОС «Astra Linux Special Edition» на жесткий диск:

dd if=/dev/cdrom of=/opt/cd.iso bs=1M

1. Создать папку для монтирования ISO файла установочного диска:

mkdir /opt/repo

1. Монтировать ISO файл в созданную папку:

mount -o loop /opt/cd.iso /opt/repo

1. Вставить в CD/DVD привод диск разработчиков.
2. Скопировать образ диска разработчиков ОС «Astra Linux Special Edition» на жесткий диск:

dd if=/dev/cdrom of=/opt/cd-dev.iso bs=1M

1. Создать папку для монтирования ISO файла диска разработчиков:

mkdir /opt/repo-dev

1. Монтировать ISO файл в созданную папку:

mount -o loop /opt/cd-dev.iso /opt/repo-dev

1. Указать репозитории в /etc/apt/sources.list:

deb file::///opt/repo smolensk contrib main non-free

deb file::///opt/repo-dev smolensk contrib main non-free

1. Обновить репозитории:

apt-get update

## Установка ПК Bot-Trek TDS

Перед установкой ПК Bot-Trek TDS необходимо:

* проверить правильность подключения клавиатуры и монитора к серверу;
* проверить наличие CD/DVD привода в составе сервера, в случае отсутствия необходимо подключить переносной CD/DVD привод;
* вставить CD-диск с дистрибутивом изделия в CD/DVD привод;
* нажать комбинацию клавиш <Ctrl+Alt+F2> для перехода в консольный режим и ввести имя и пароль пользователя root.

После ввода данных пользователя root будет предоставлен доступ к командной строке ОС.

Установка ПК Bot-Trek TDS выполняется только с помощью установочного скрипта install.sh, который находится в корне дистрибутива ПК Bot-Trek TDS.

Запуск скрипта необходимо осуществлять под пользователем root.

Для установки изделия выполнить следующие действия:

1. монтировать CD-диск с дистрибутивом;
2. найти на CD-диске с дистрибутивом скрипт install.sh;
3. запустить скрипт install.sh;
4. В процессе установки появится всплывающее окно с подтверждением установки пакетов. Подтвердить установку.

### Текст скрипта install.sh

#!/bin/bash #

Create paths

mkdir -p /etc/suricata/gib-rules/

mkdir -p /opt/tds

mkdir -p /var/lib/tds

if [ ! -f /var/lib/tds/registry ]; then

echo -e "{\n \"appliance\_type\": \"sensor\"\n}" > /var/lib/tds /registry

fi

# Install requirements for API and Shell

apt-get install -yqq dialog python3-yaml redis-server postgresql-9.6 python3-requests python3-pip python3-psutil python3-psycopg2 python3-redis acl libhiredis0.13 libhyperscan4 libluajit-5.1-2 libnetfilter-log1 libltdl7 libpcap0.8 libgeoip1 libjansson4 libevent-pthreads-2.0-5 libnet1 libnetfilter-queue1 libpython-stdlib libpython2.7-minimal libpython2.7- stdlib python python-minimal python-simplejson python2.7 python2.7-minimal ethtool

# Install libhtp

dpkg -i libhtp/libhtp2\_\*.deb

# Install Suricata

dpkg -i suricata/suricata\_\*.deb

# Install Suricata rules

dpkg -i suricatarules/suricatarules\_\*.deb

# PyReq

pip3 install wheel --no-deps requirements/\*.whl

# Install tds-registry

dpkg -i tds-registry/tds-registry\_\*.deb

# Install shell

dpkg -i tds-shell/tds-shell\_\*.deb

# Install Sensor API

dpkg -i tds-api-common/sensor-api\_\*.deb

# Install Sensor Web interface

dpkg -i sensor-cert-web/\*.deb

# Configure logrotate

cp logrotate/\* /etc/logrotate.d/

# Add tds user tds

useradd -m -p tds -s /usr/sbin/tds-shell tds

echo "tds ALL=(root) NOPASSWD:/opt/tds/tds-shell/tds\_shell.py" >> /etc /sudoers

# Start services

systemctl start sensor-api.service

systemctl start sensor-cert-alerts.service

systemctl start sensor-cert-web.service

systemctl enable sensor-api.service

systemctl enable sensor-cert-alerts.service

systemctl enable sensor-cert-web.service

Примечание. Скрипт install.sh выполняет действия, описанные ниже.

#### Установка зависимостей

1. Прописание локалей

sudo echo -e 'LANGUAGE=en\_US.UTF-8\nLC\_ALL=en\_US.

UTF-8\nLANG=en\_US. UTF-8\nLC\_TYPE=en\_US.UTF-8\n' >> /etc/default/locale

sudo locale-gen en\_US.UTF-8

sudo dpkg-reconfigure -f noninteractive locale

1. Установка зависимостей (системных пакетов) из состава ОС «Astra Linux Special Edition»:

sudo apt-get -yqq install postgresql-9.6 python3-redis python3-psutil python3-psycopg2 python3-yaml python3-virtualenv python3-pip python3- requests acl dialog libltdl7 geoip-database libgeoip1 libhiredis0.13 libhyperscan4 libluajit-5.1-2 libluajit-5.1-common libnetfilter-log1 libpcap0.8 ethtool redis-server libjansson4

1. Установка зависимостей (внешних пакетов) с CD-диска с дистрибутивом. Установку зависимостей необходимо проводить в следующем порядке:

python3 -m pip install requirements/build/pytz-2018.4-py3-none-any. whl

python3 -m pip install requirements/build/pythondialog-3.4.1-py3-noneany.whl

python3 -m pip install requirements/build/terminaltables-3.1.0-py3- none-any.whl

python3 -m pip install requirements/build/Werkzeug-0.14.1-py2.py3- none-any.whl

python3 -m pip install requirements/build/MarkupSafe-1.0-cp35-cp35mlinux\_x86\_64.whl

python3 -m pip install requirements/build/click-6.7-py2.py3-none-any. whl

python3 -m pip install requirements/build/itsdangerous-0.24-py3-noneany.whl

python3 -m pip install requirements/build/Jinja2-2.10-py2.py3-noneany.whl

python3 -m pip install requirements/build/Flask-1.0.2-py2.py3-noneany.whl

python3 -m pip install requirements/build/Django-2.0.6-py3-none-any. whl

#### Установка Suricata

1. Установить зависимости Suricata:

dpkg -i libhtp/libhtp2\_0.5.26-1\_amd64.deb

1. Установить Suricata:

dpkg -i suricata/suricata\_4.0.4-2\_amd64.deb

1. Установить правила Suricata:

dpkg -i suricatarules/suricatarules\_1.0.13-1199\_all.deb

1. Настроить ротацию логов для Suricata путем создания файла suricata в директории /etc/logrotate.d/ и добавлению в него следующих настроек:

/var/log/suricata/http.log

{

daily

missingok

rotate 14

compress

delaycompress

notifempty

create 640 root adm

sharedscripts

postrotate

/bin/kill -HUP $(cat /var/run/suricata.pid)

endscript

}

/var/log/suricata/stats.log

{

daily

missingok

rotate 14

compress

delaycompress

notifempty

create 640 root adm

sharedscripts

postrotate

/bin/kill -HUP $(cat /var/run/suricata.pid)

endscript

}

/var/log/suricata/fast.log

{

daily

missingok

rotate 14

compress

delaycompress

notifempty

create 640 root adm

sharedscripts

postrotate

/bin/kill -HUP $(cat /var/run/suricata.pid)

endscript

}

/var/log/unified\_purge.log

{

daily

rotate 12

missingok

compress

}

/var/log/suricata/eve.json

{

monthly

rotate 6

missingok

compress

delaycompress

notifempty

create 640 root adm

sharedscripts

postrotate

/bin/kill -HUP $(cat /var/run/suricata.pid)

endscript

}

/var/log/suricata/stats.json

{

daily

missingok

rotate 14

compress

delaycompress

notifempty

create 640 root adm

sharedscripts

postrotate

/bin/kill -HUP $(cat /var/run/suricata.pid)

endscript

}

#### Установка tds-registry

1. Установить tds-registry:

dpkg -i tds-registry/tds-registry\_1.1.4-1\_all.deb

1. Создать конфигурационный файл для registry:

echo -e "{\n \"appliance\_type\": \"sensor\"\n}" > /var/lib/tds /registry

#### Установка tds-shell

1. Установить пакет tds-shell:

dpkg -i tds-shell/tds-shell\_0.1\_all.deb

1. Создать пользователя tds:

useradd -m -p tds -s /usr/sbin/tds-shell tds echo "tds ALL=(root) NOPASSWD:/opt/tds/tds-shell/tds\_shell.py" >> /etc /sudoers

#### Установка sensor-api

Установить пакет tds-api-common:

dpkg -i tds-api-common/sensor-api\_1.0.20-1\_all.deb

#### Установка web

Установить пакет sensor-cert-web:

dpkg -i sensor-cert-web/sensor-cert-web\_0.1.0\_all.deb # sensor\_db, postgres, admin , , .

# Настройка

Для настройки, проверки и восстановления работоспособности изделия используется текстовая консоль, предоставляющая доступ к возможностям диагностики и настройки изделия.

Чтобы войти в текстовую консоль с сервера СОВ необходимо нажать на клавиатуре комбинацию клавиш «Ctrl+Alt+F2».

С правами root ввести команду:

su – tds

на экране появится запрос на ввод имени и пароля пользователя (имя и пароль пользователя по умолчанию tds/tds). После чего будет произведен вход в командную среду пользователя tds (Пользователь tds создается на этапе установки изделия).

Чтобы войти в текстовую консоль удаленно с АРМ администратора необходимо ввести IP-адрес изделия, полученный в ходе настройки изделия, в терминальный клиент. В ответ на запрос ввести имя и пароль пользователя (имя и пароль пользователя по умолчанию tds/tds).

Настройка изделия состоит из следующих действий:

1. Настройка интерфейса управления.
2. Настройка интерфейсов анализа трафика.
3. Создание учетных записей.
4. Настройка NTP серверов.

Перед настройкой настоятельно рекомендуется изменить пароль для служебной учетной записи, используемой для взаимодействия функциональных компонентов СОВ с базой данных, устанавливаемый по умолчанию. Для этого необходимо выполнить следующие действия:

* + если уже был произведен вход в текстовую консоль, то необходимо выйти из нее;
  + войти в операционную систему с правами root выполнив команду:

sudo su

* + изменить пароль в конфигурационном файле для пользователя ADMIN в поле PASSWORD выполнив команду:

nano sensor-web-cert/configs/registry

* + изменить пароль в базе данных выполнив команду:

sudo -u admin psql sensor\_db

* + после чего откроется консоль PostgeSQL;
  + ввести:

ALTER USER admin WITH PASSWORD “новый пароль”

* + выйти из консоли PostgeSQL нажатием комбинации клавиш <Ctrl+Z>.

## Настройка интерфейса управления

Существует два варианта настройки интерфейса управления:

1. По протоколу DHCP.
2. Вручную.

### Настройка интерфейса управления по протоколу DHCP

1. Войти в текстовую консоль под пользователем tds (Пользователь tds создается на этапе установки изделия).
2. В стартовом окне текстовой консоли выбрать <Enter the shell>   
   (рис. 1).

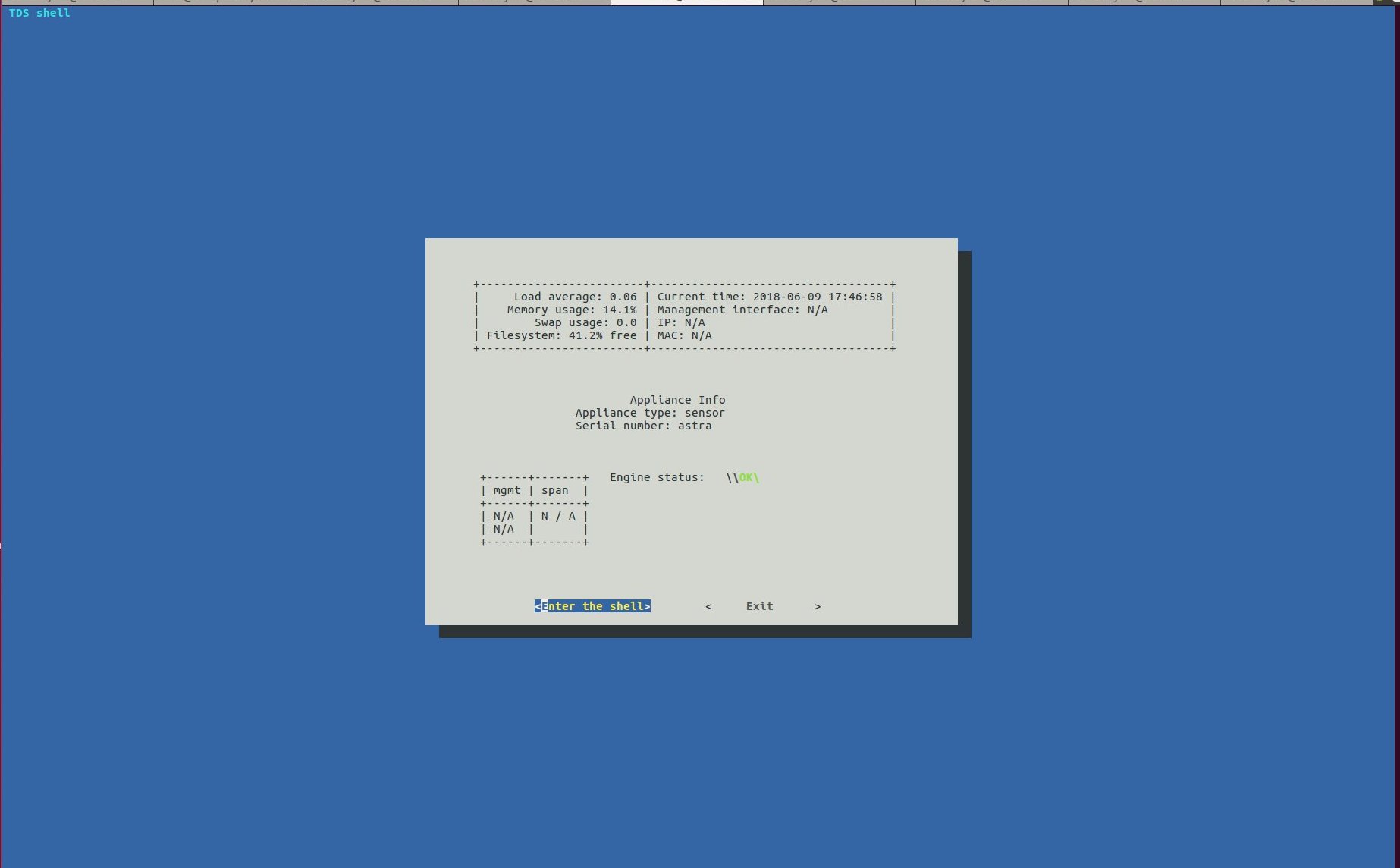


Рис. 1

1. Изменить пароль пользователя tds в соответствии с правилами формирования паролей, для чего в окне «Choose one of the options:» выбрать «Change password»   
   (рис. 2).



Рис. 2

Подтвердить смену пароля нажатием <Yes> (рис. 3).

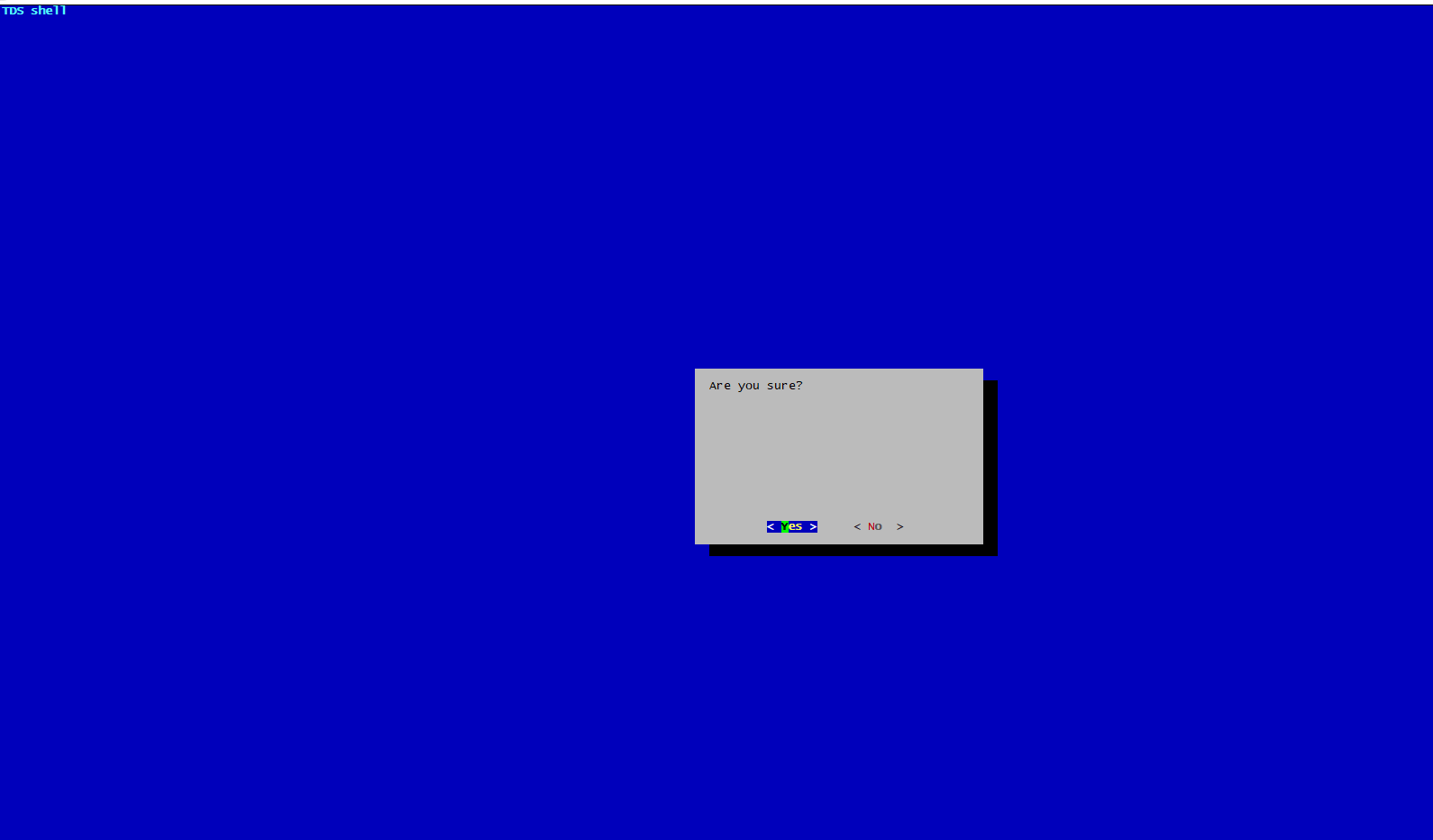


Рис. 3

В ответ на запрос системы ввести старый пароль и дважды ввести новый пароль.

В случае если пароль не соответствует политике безопасности программа выдаст предупреждение о невозможности смены пароля (рис. 4).

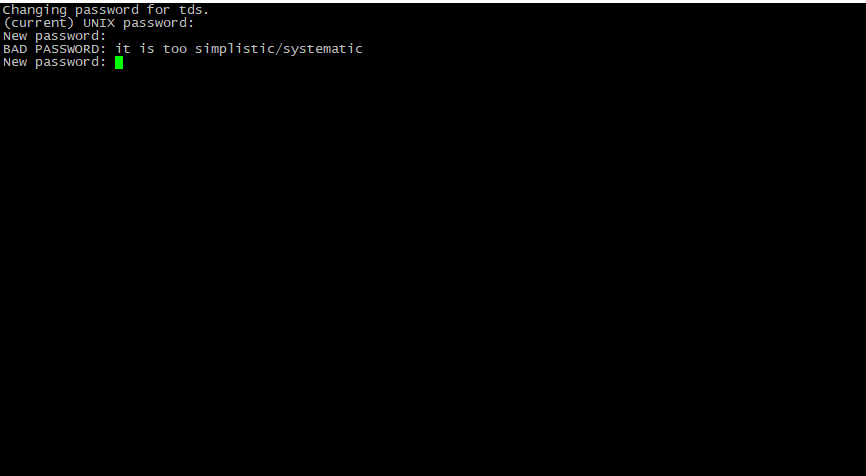


Рис. 4

1. Выбрать «Network menu» (сетевое меню) (рис. 5).

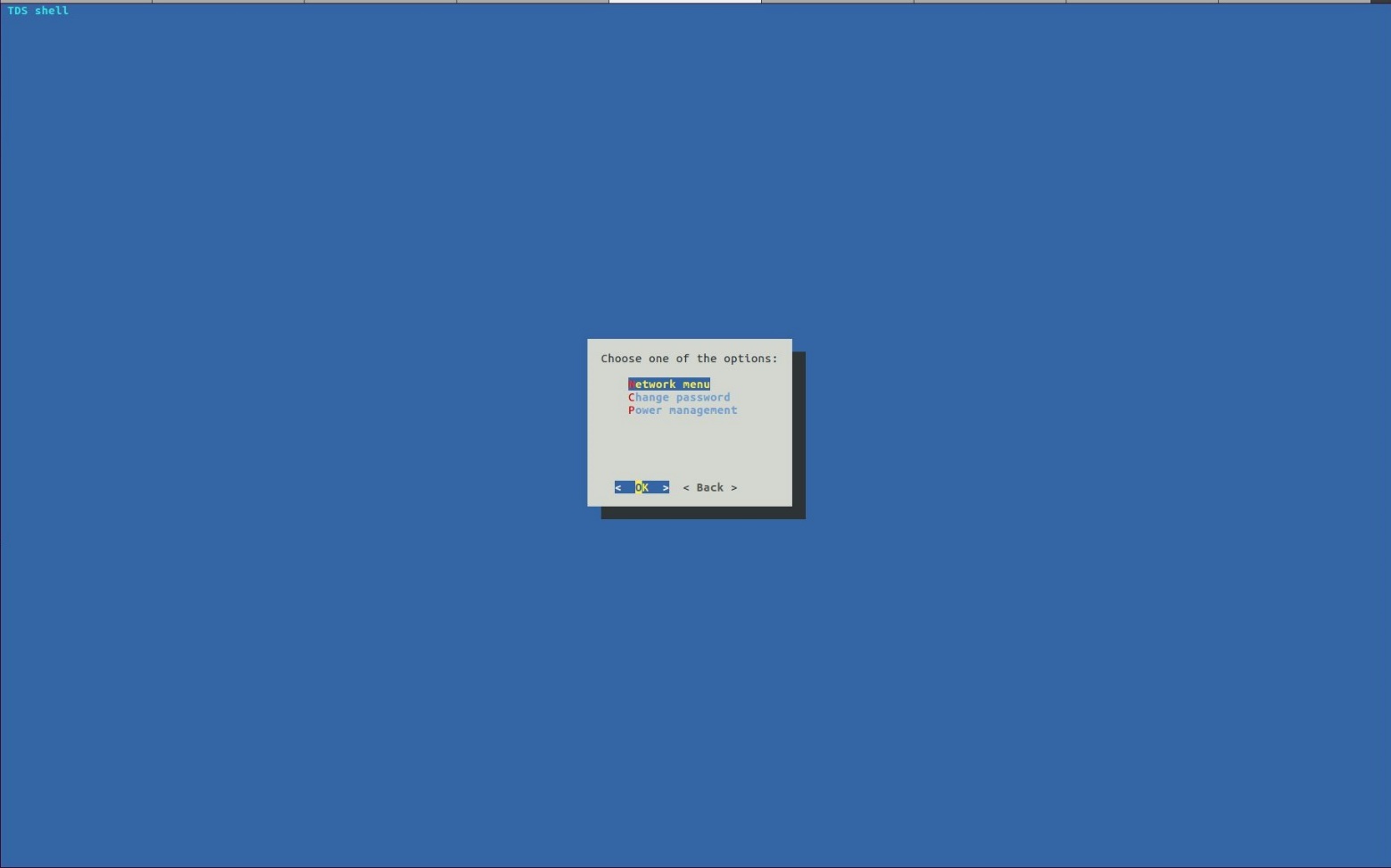


Рис. 5

1. Выбрать «Configure network» (Настройка сети) и нажать «Ок» (рис. 6).

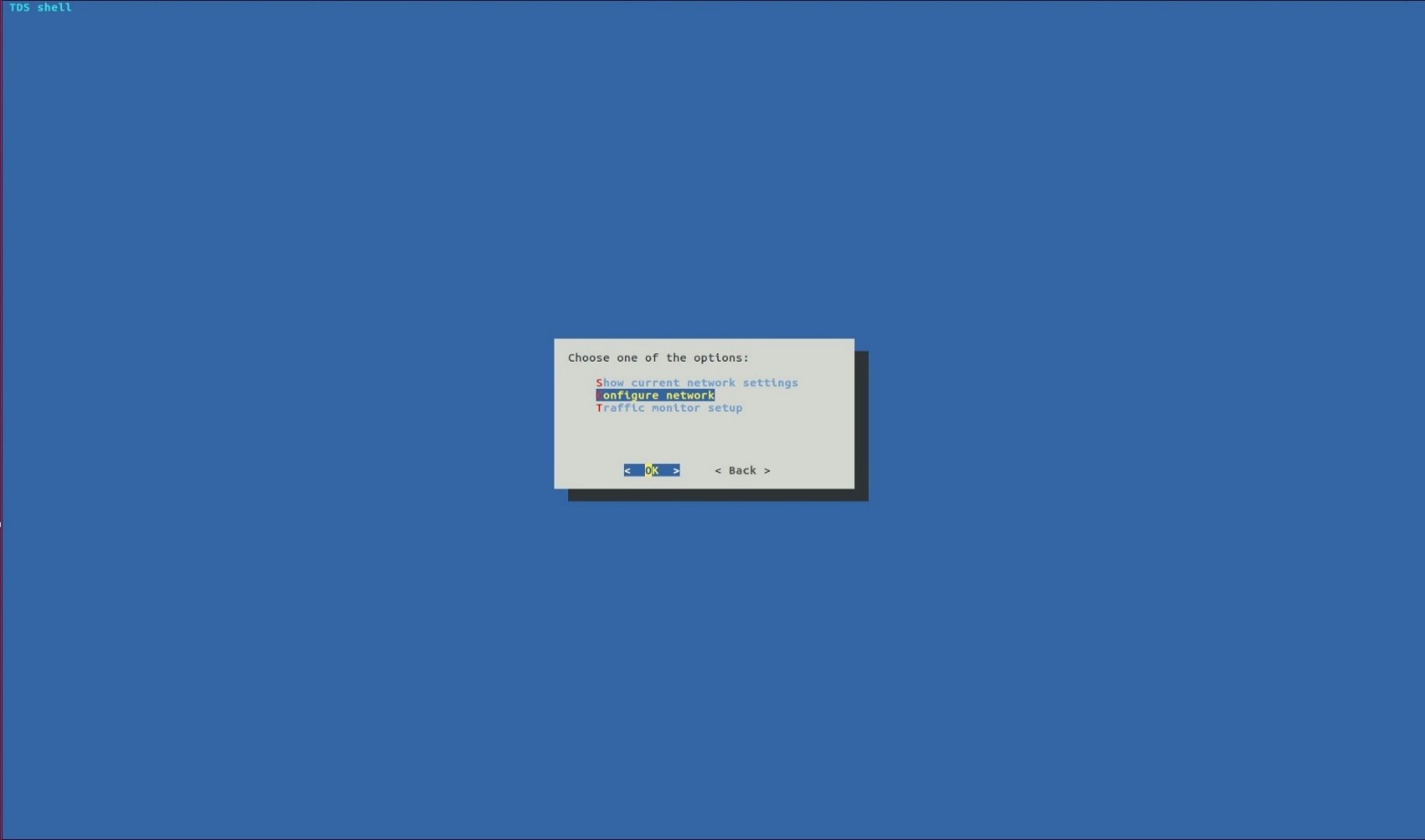


Рис. 6

1. Подтвердить выбор, нажав кнопку «Да» (рис. 7).

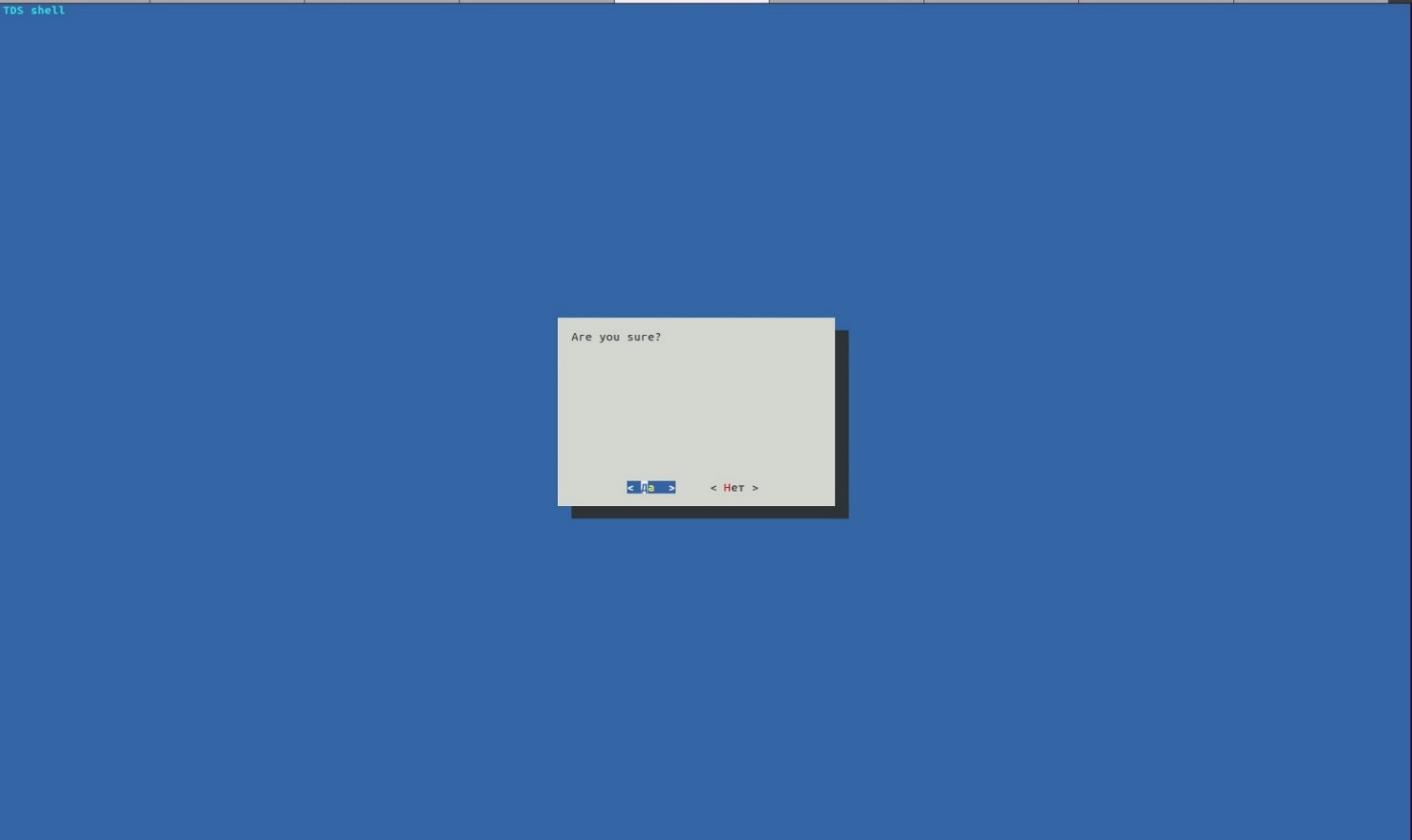


Рис. 7

1. В всплывающем окне «Choose IP address configuration» (Выбрать конфигурацию IP-адреса) выбрать DHCP (рис. 8).

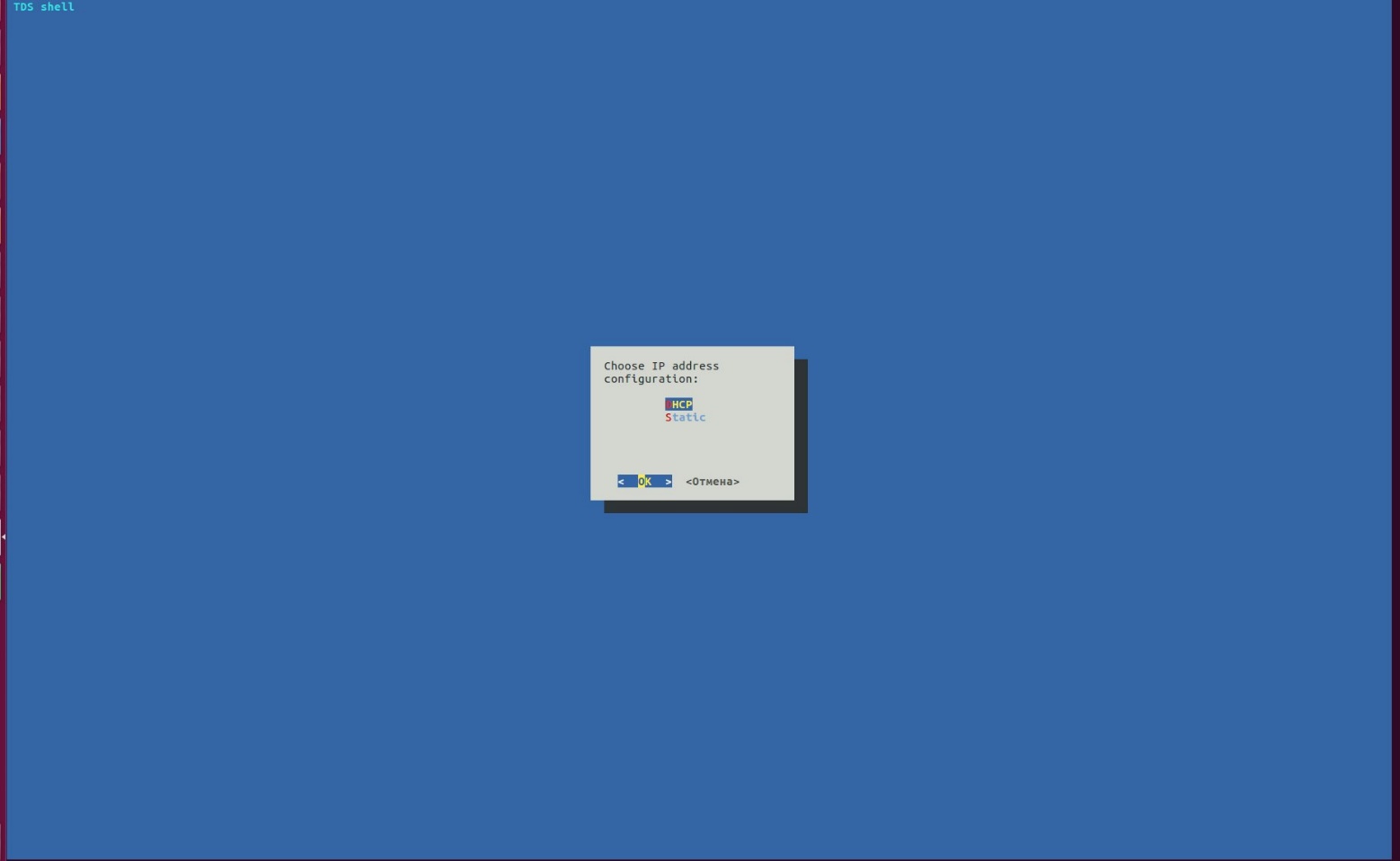


Рис. 8

### Настройка интерфейса управления вручную

1. Войти под пользователем tds (Пользователь tds создается на этапе установки изделия).
2. В стартовом окне текстовой консоли выбрать <Enter the shell> (рис. 9).

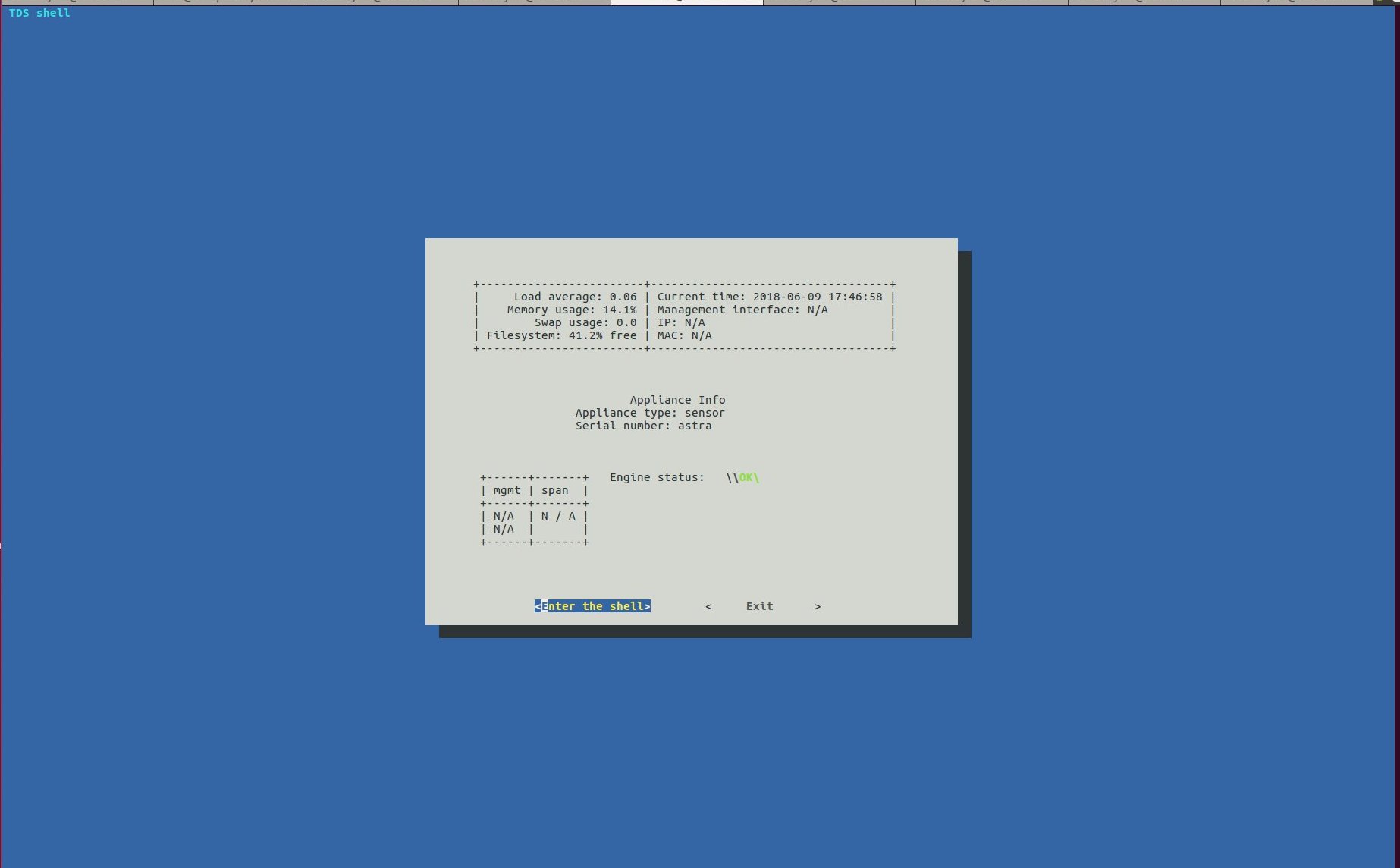


Рис. 9

1. Выбрать «Network menu» (рис. 10).

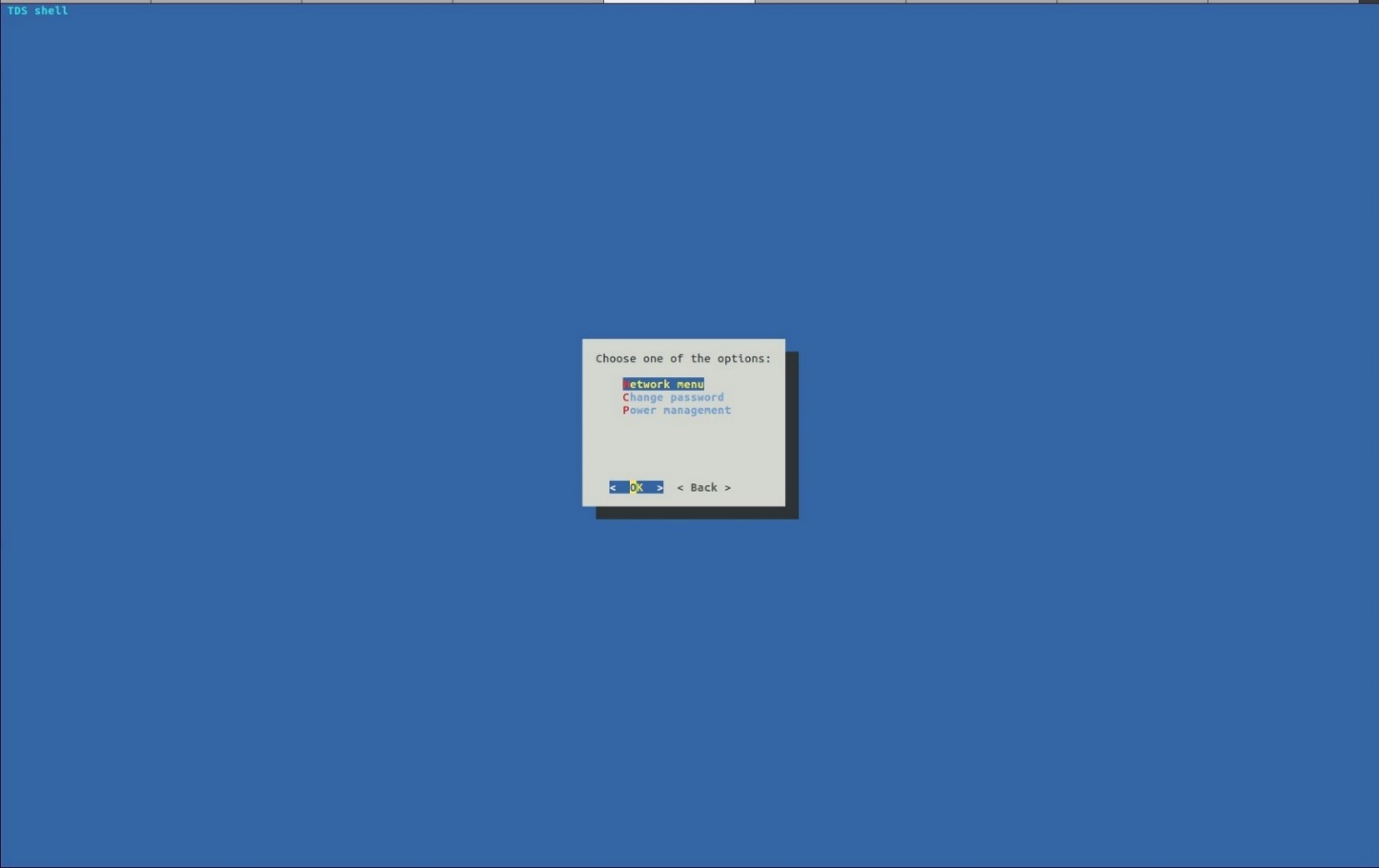


Рис. 10

1. Выбрать «Configure network» и нажать «Ок» (рис. 11).

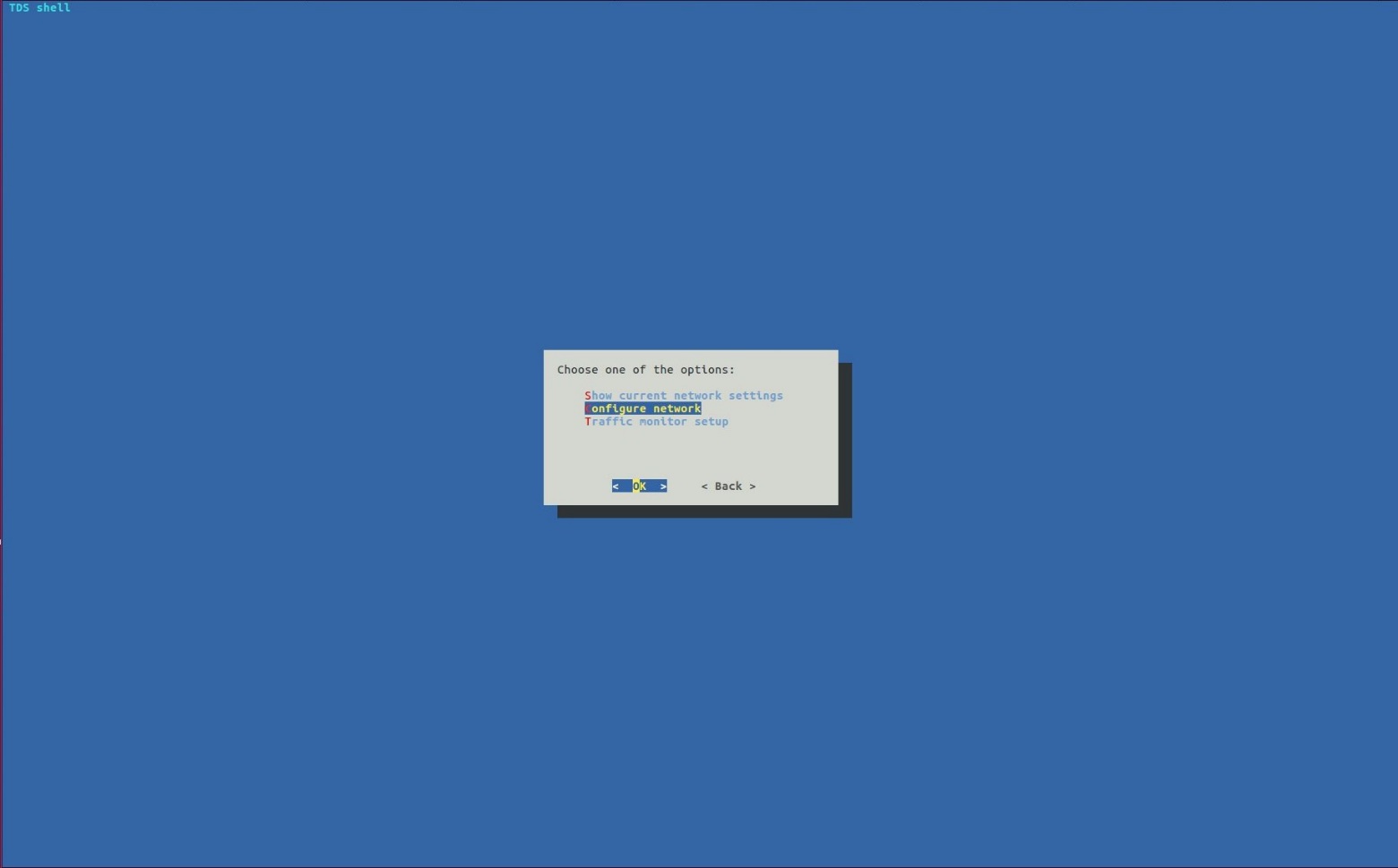


Рис. 11

1. Подтвердить выбор, нажав кнопку «Да» (рис. 12).

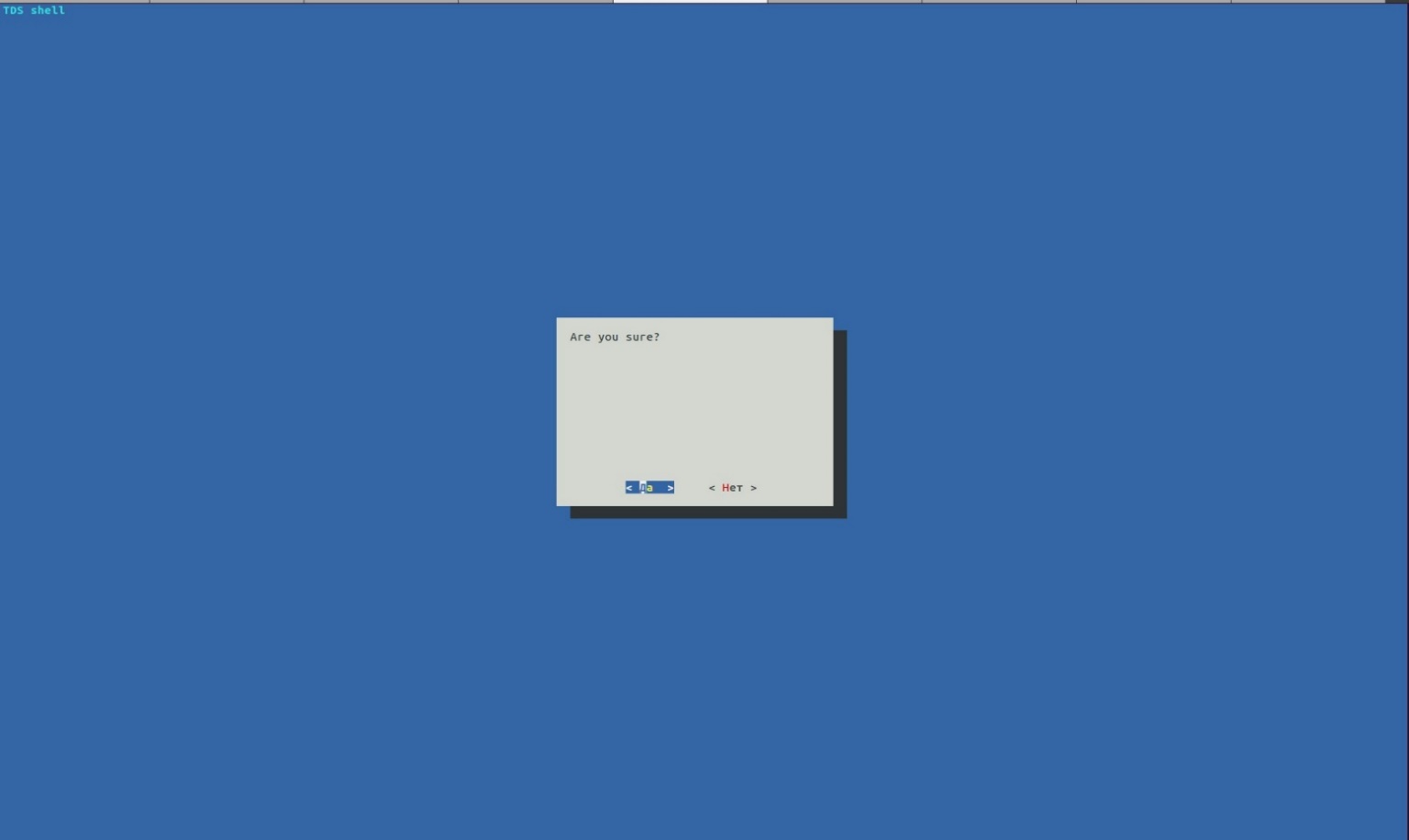


Рис. 12

1. Выбрать «Static» (рис. 13).

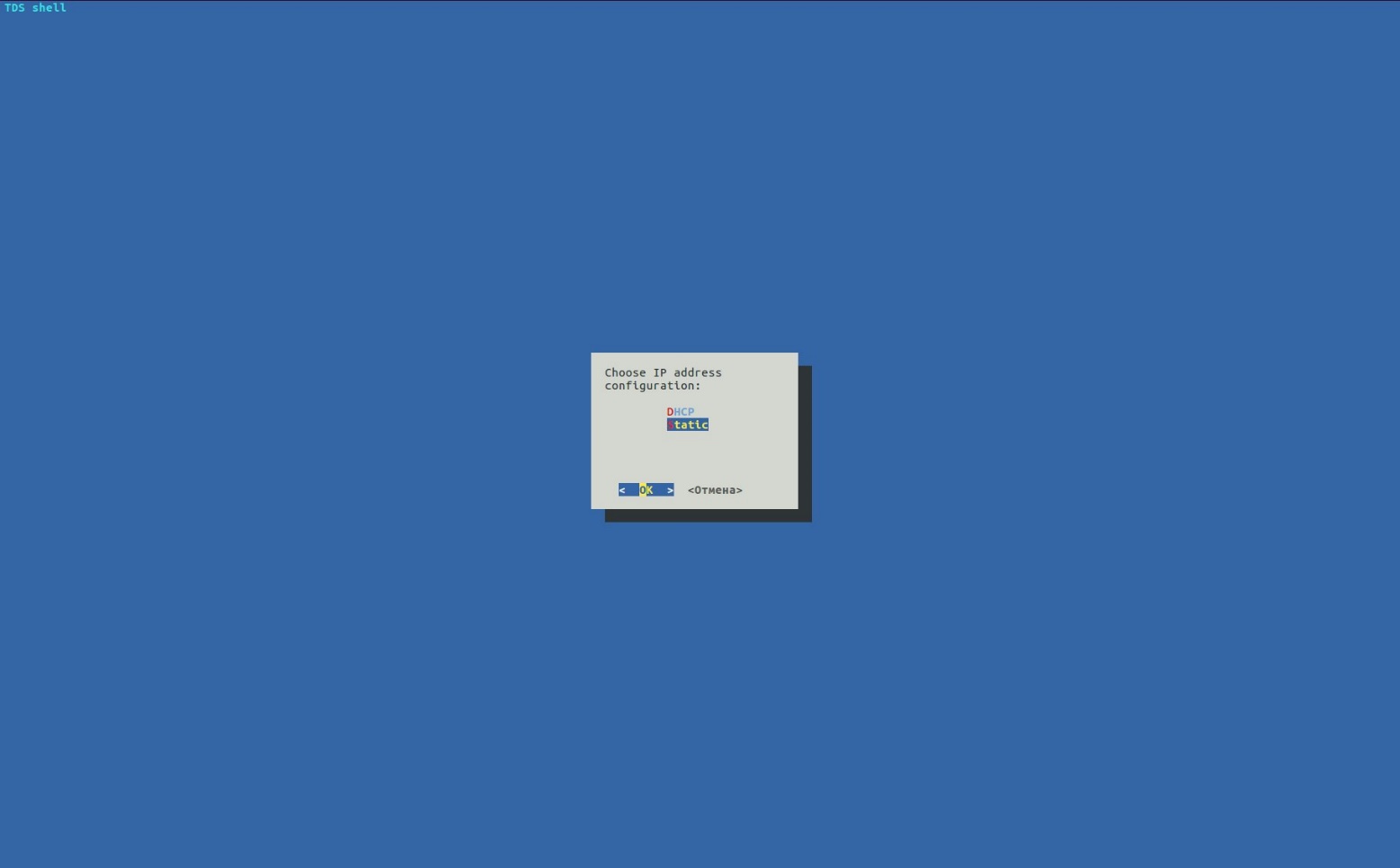


Рис. 13

1. Ввести IP-адрес интерфейса и нажать «ОК» (рис. 14).

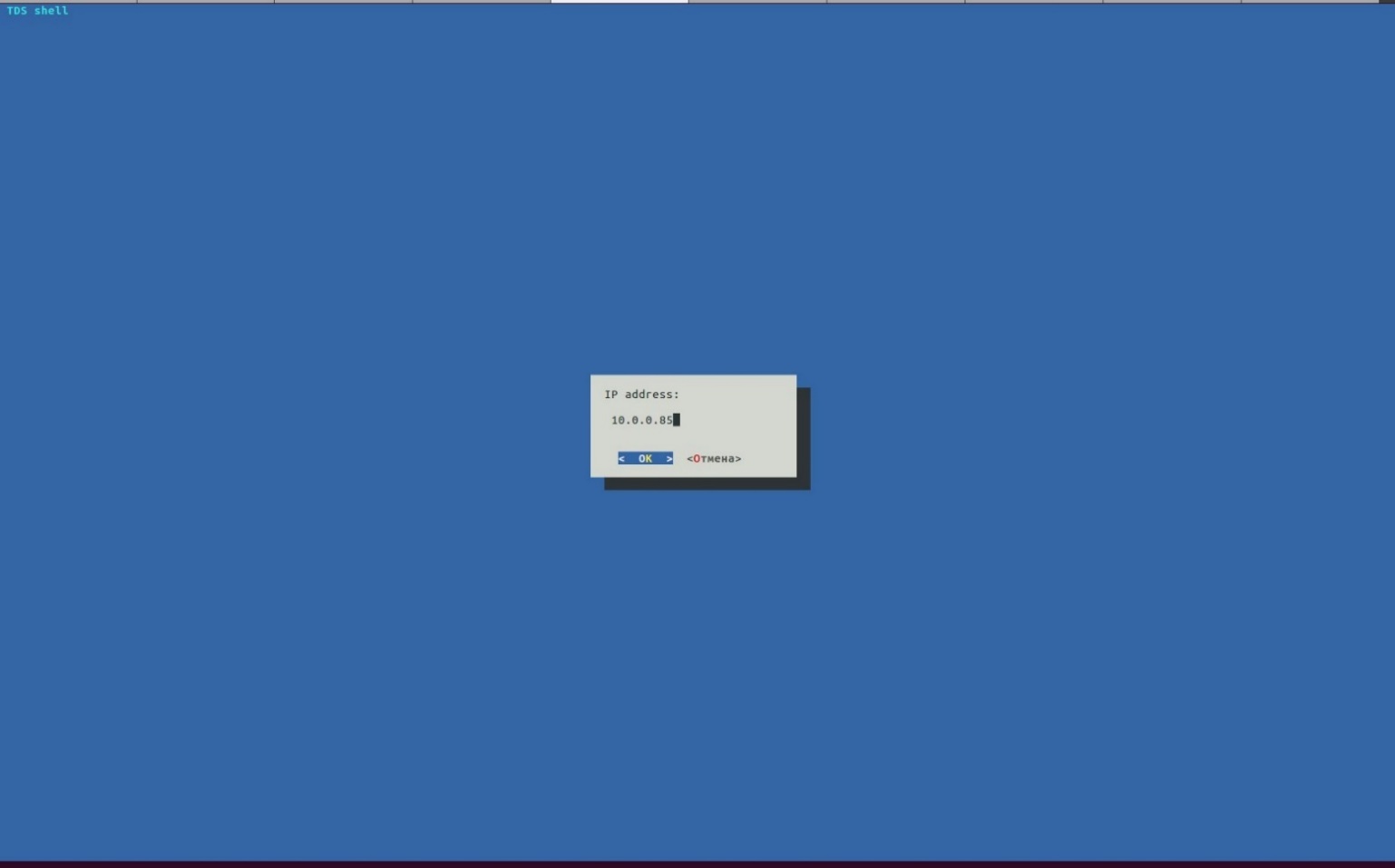


Рис. 14

1. Ввести маску подсети (рис. 15).

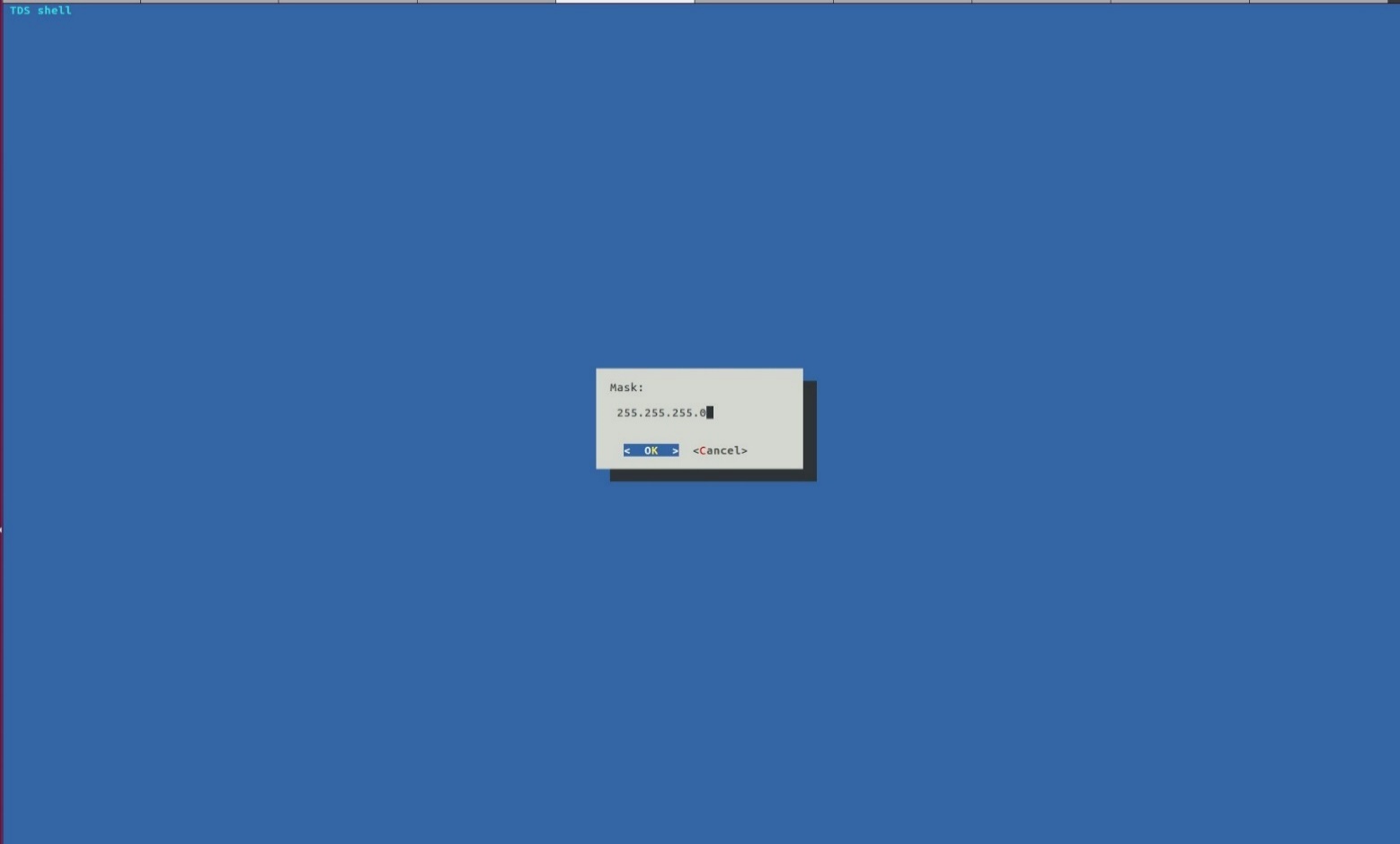


Рис. 15

1. Ввести адрес шлюза (рис. 16).

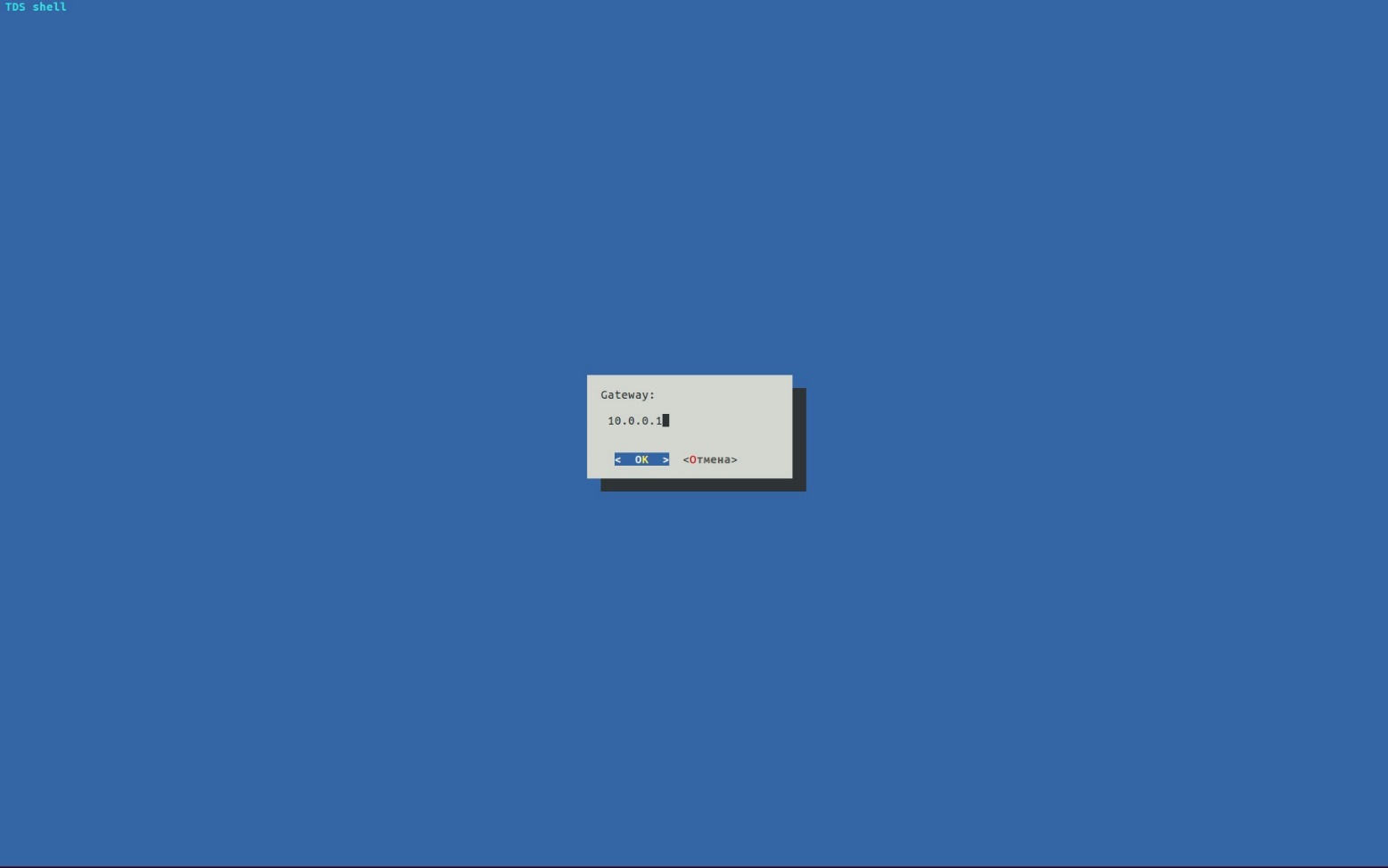


Рис. 16

1. Выбрать адреса DNS по умолчанию (8.8.8.8 и 8.8.8.4) или ввести их вручную.
2. (Опционально) Ввести DNS сервера (если в п.10 выбрали вручную)   
   (рис. 17).

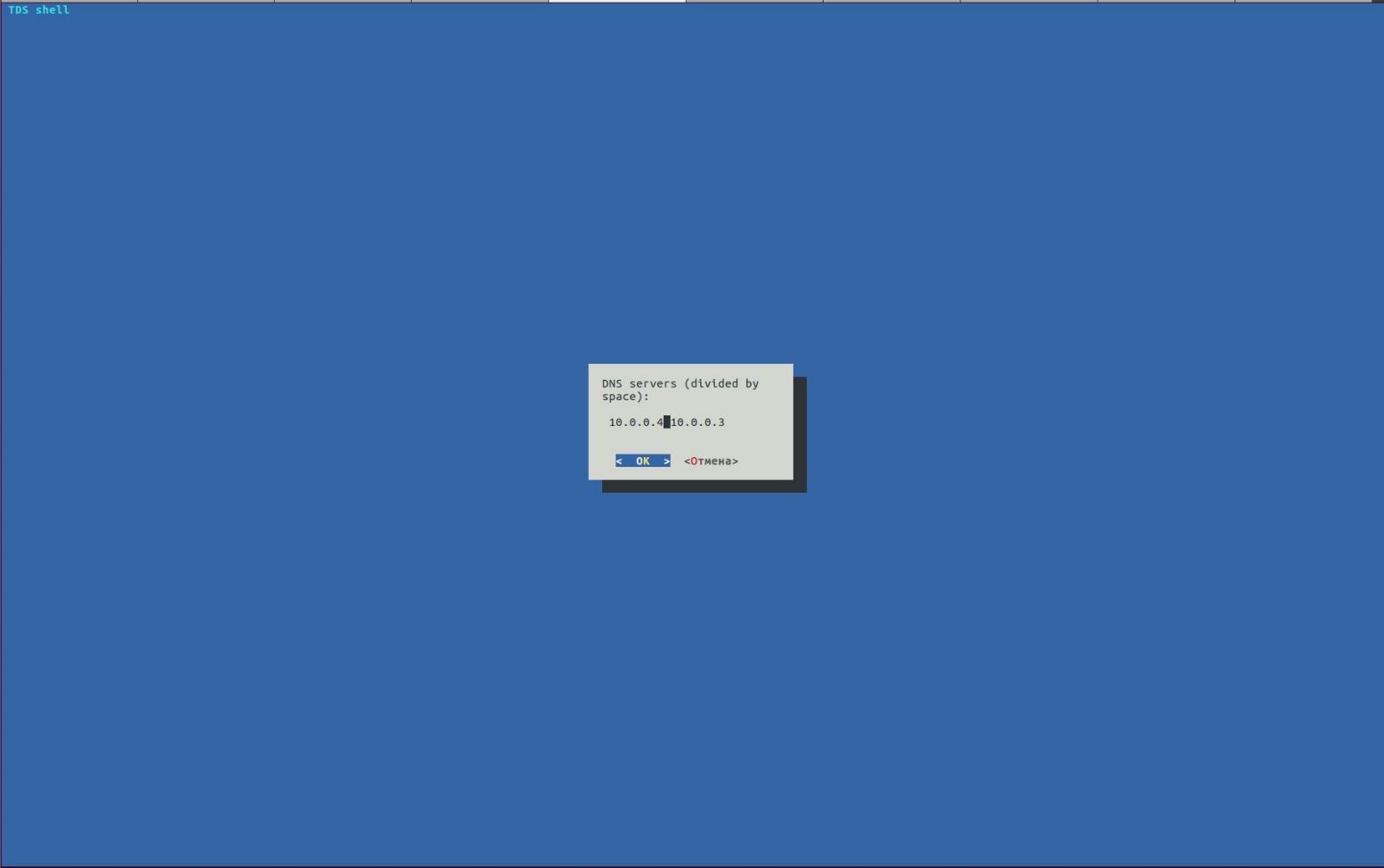


Рис. 17

## Настройка интерфейсов анализа трафика

1. Войти под пользователем tds (Пользователь tds создается на этапе установки).
2. В стартовом окне выбрать <Enter the shell> (рис. 18).

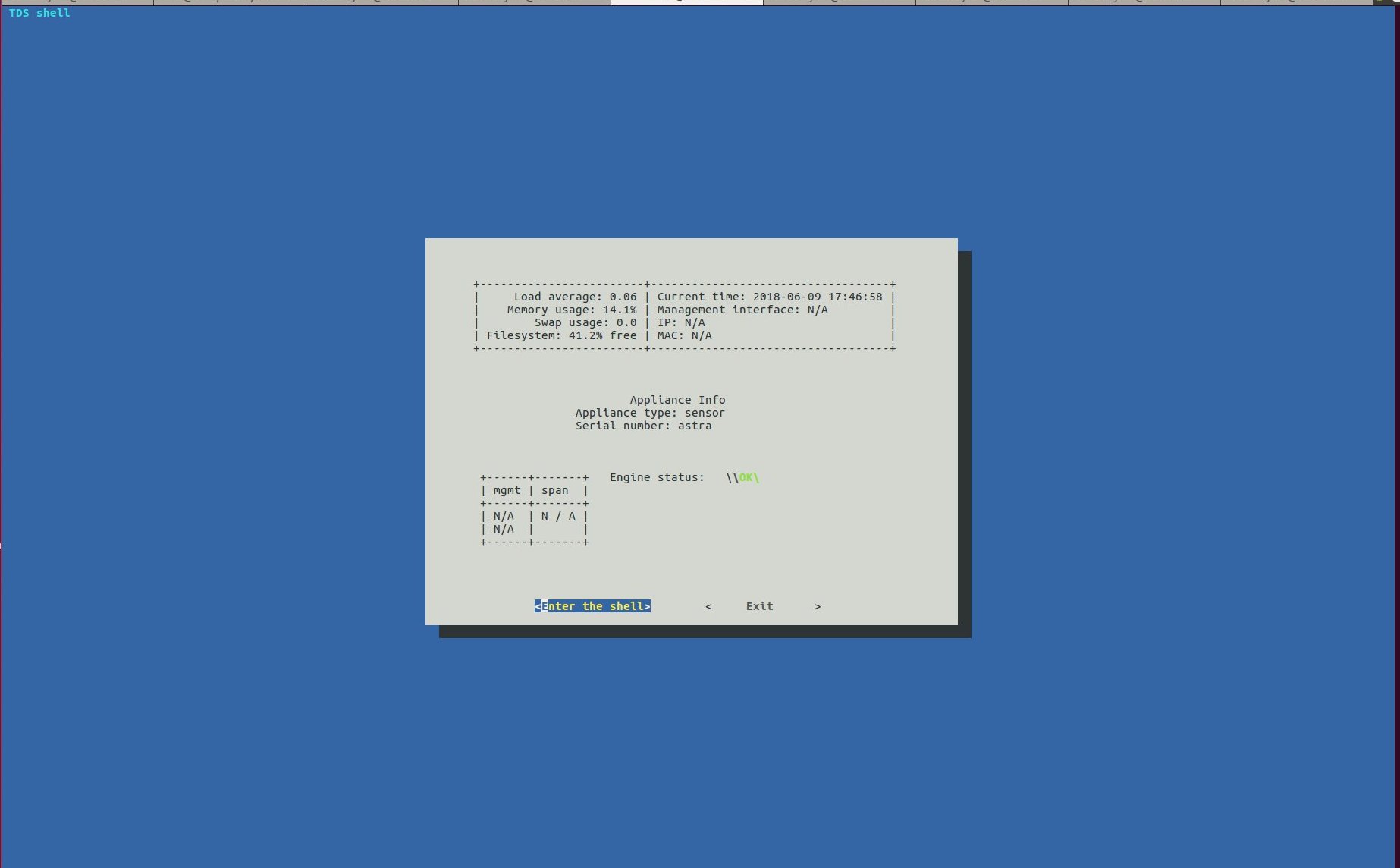


Рис. 18

1. Выбрать «Network menu» (рис. 19).

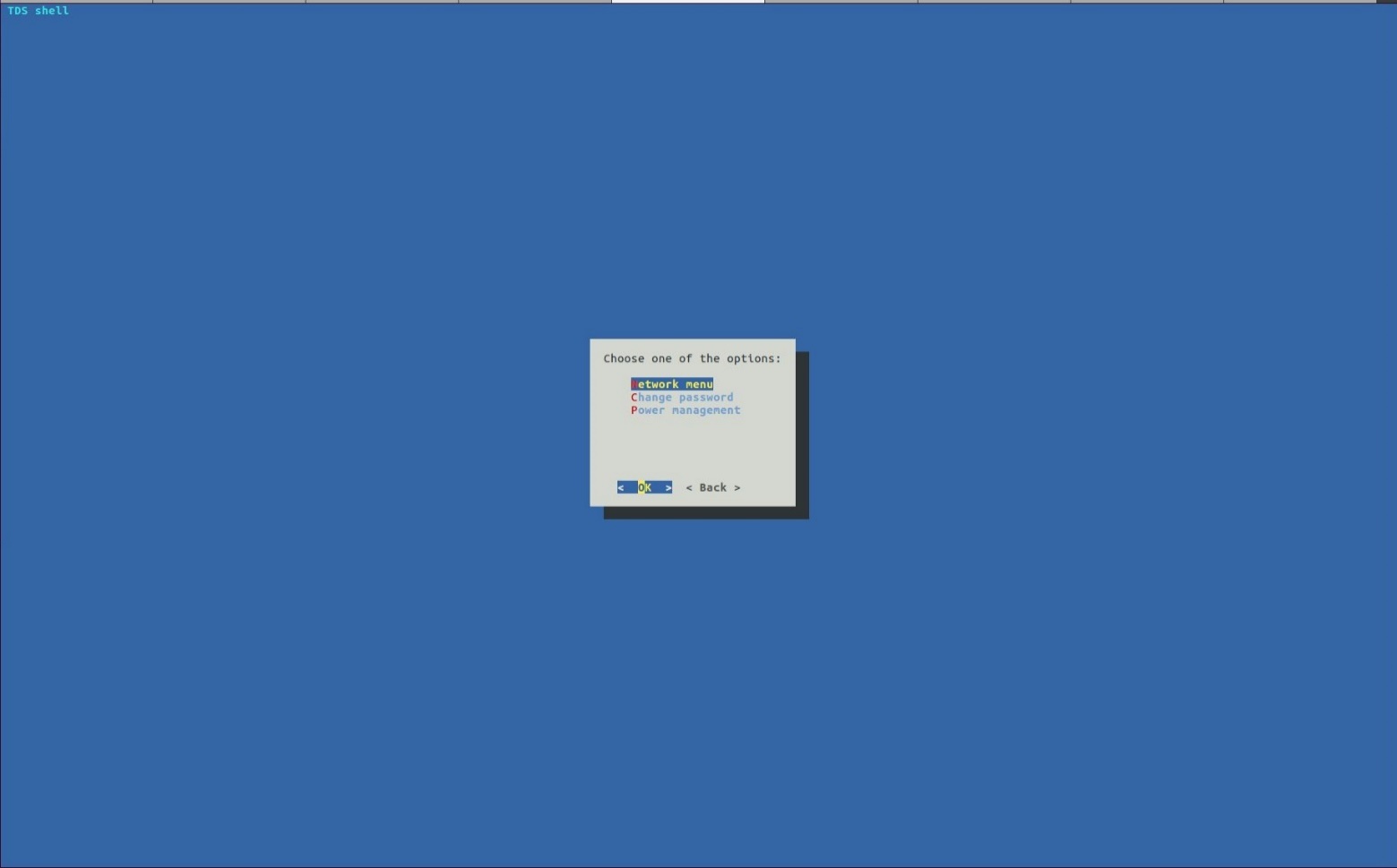


Рис. 19

1. Выбрать «Traffic monitor setup» (рис. 20).

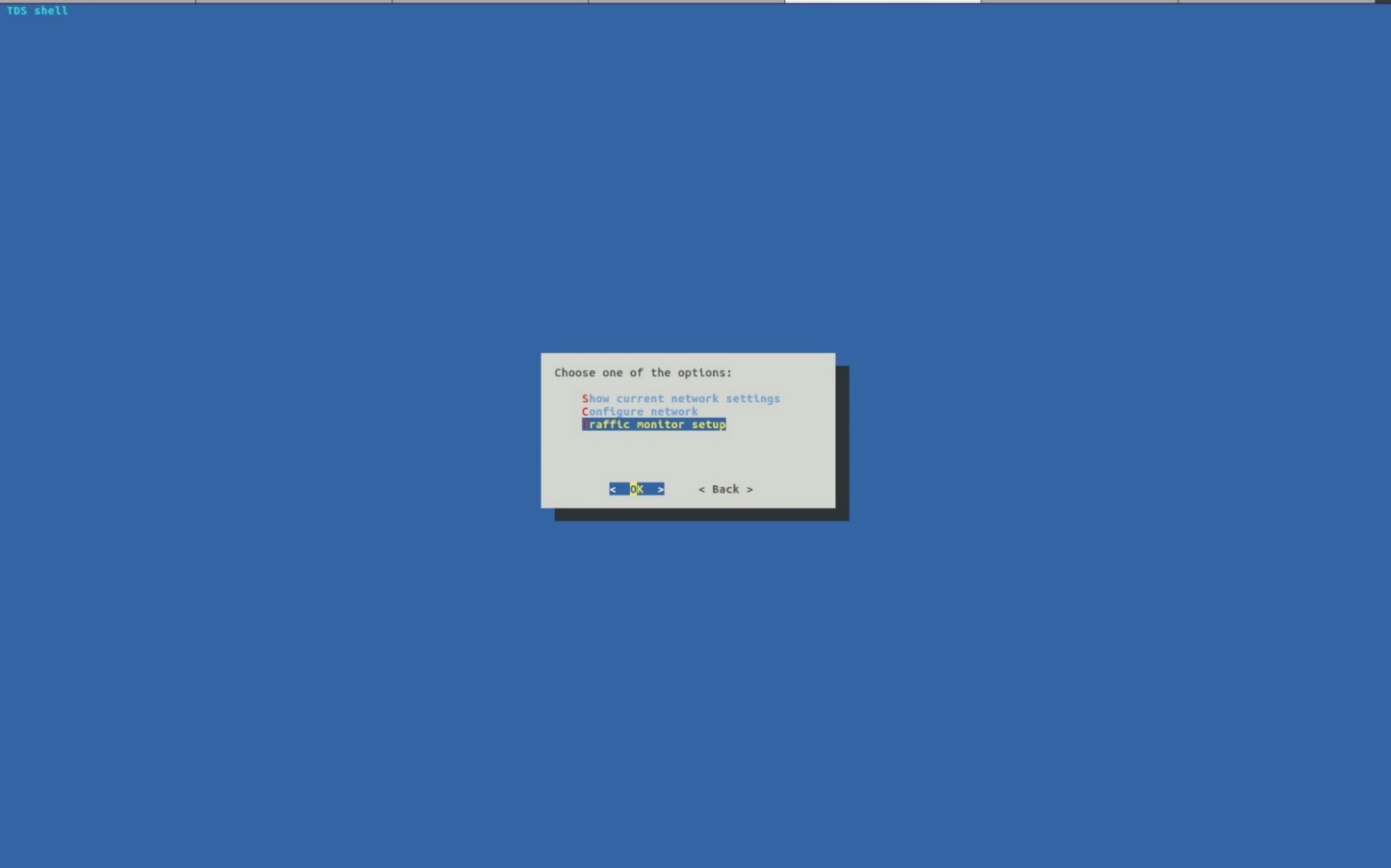


Рис. 20

1. Выбрать интерфейсы на которых будет осуществляться мониторинг   
   (рис. 21).

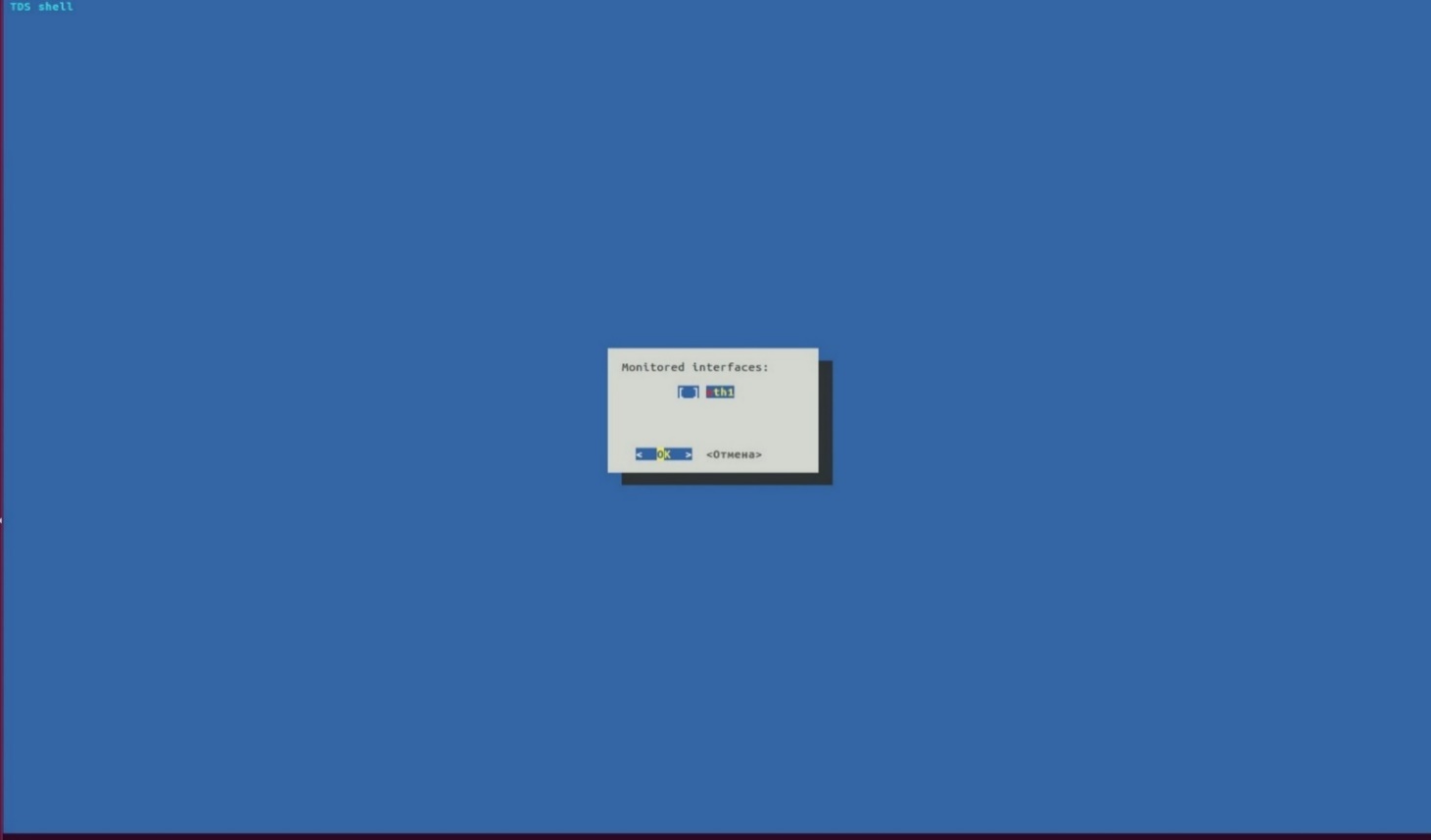


Рис. 21

1. Нажать «ОК».

## Создание учетных записей

1. Войти в графический интерфейс программы с ролью Администратор безопасности.
2. Логин и пароль по умолчанию: admin /tdsadmin.
3. Изменить пароль для администратора безопасности (рис. 22).

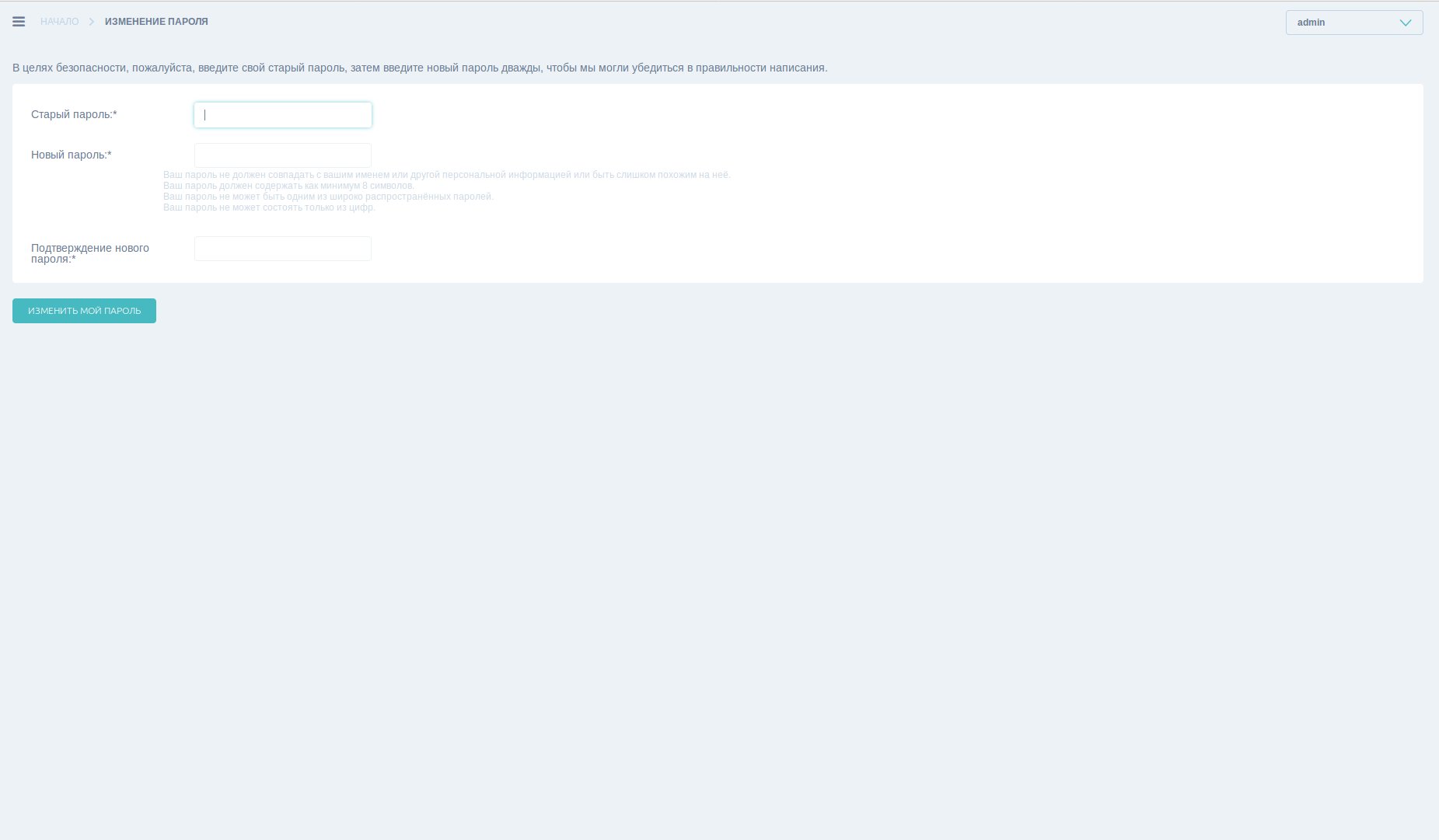


Рис. 22

1. Создать учетную запись аудитора (просмотр событий внутреннего аудита)   
   (рис. 23).

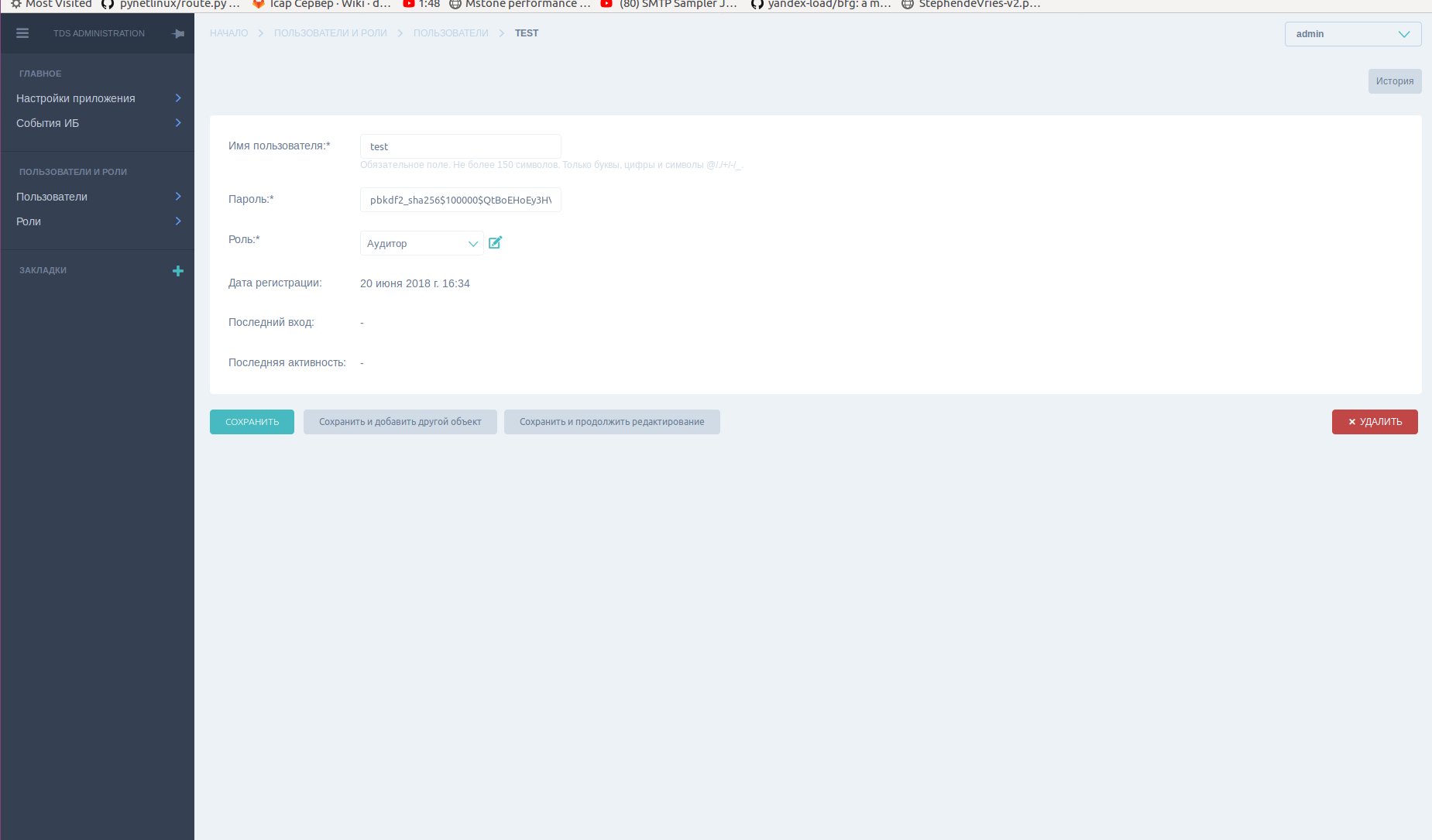


Рис. 23

1. Создать учетную запись пользователя (рис. 24).

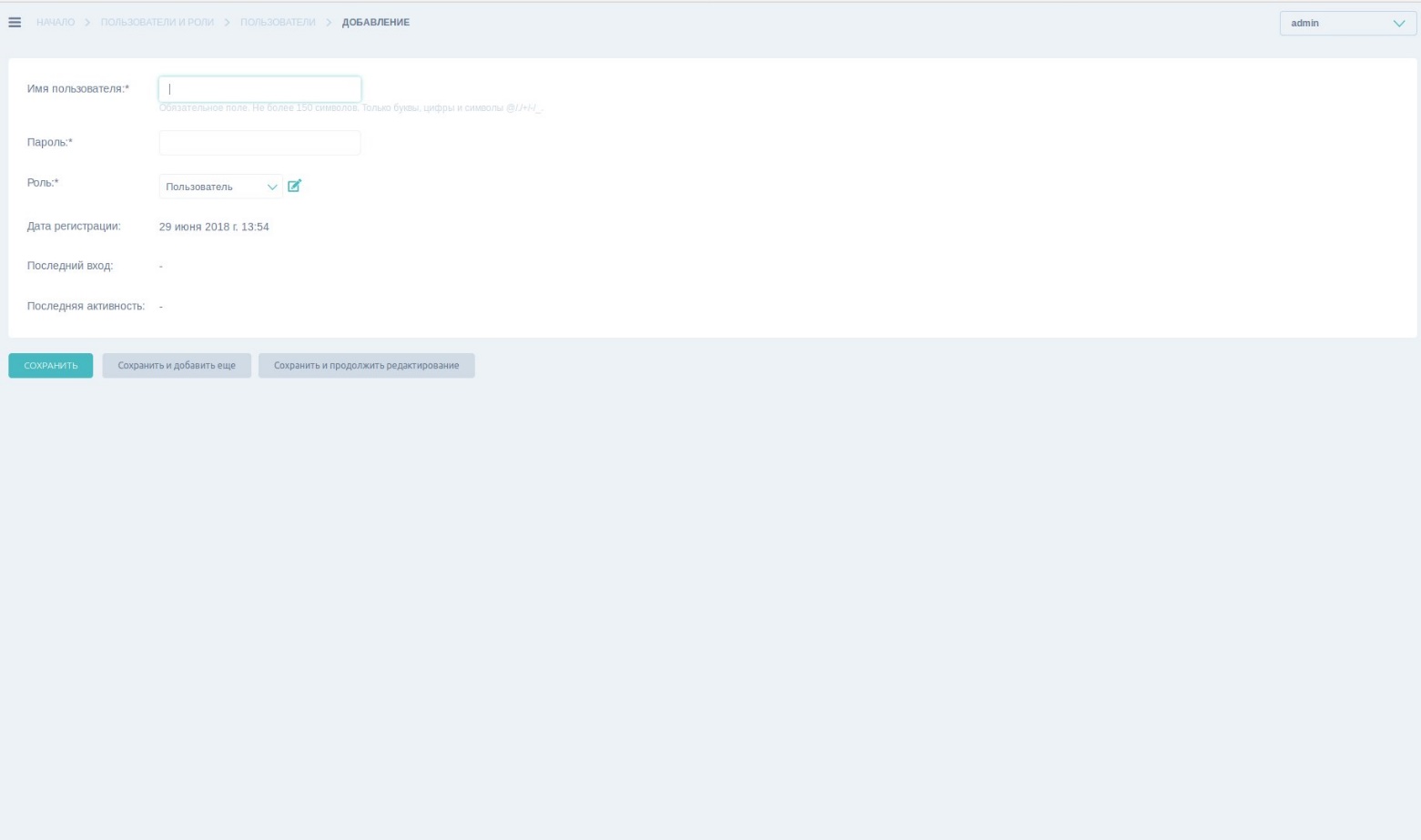


Рис. 24

## Настройка NTP серверов

1. Войти в графический интерфейс программы.
2. Перейти в меню «Настройки приложения» (рис. 25).

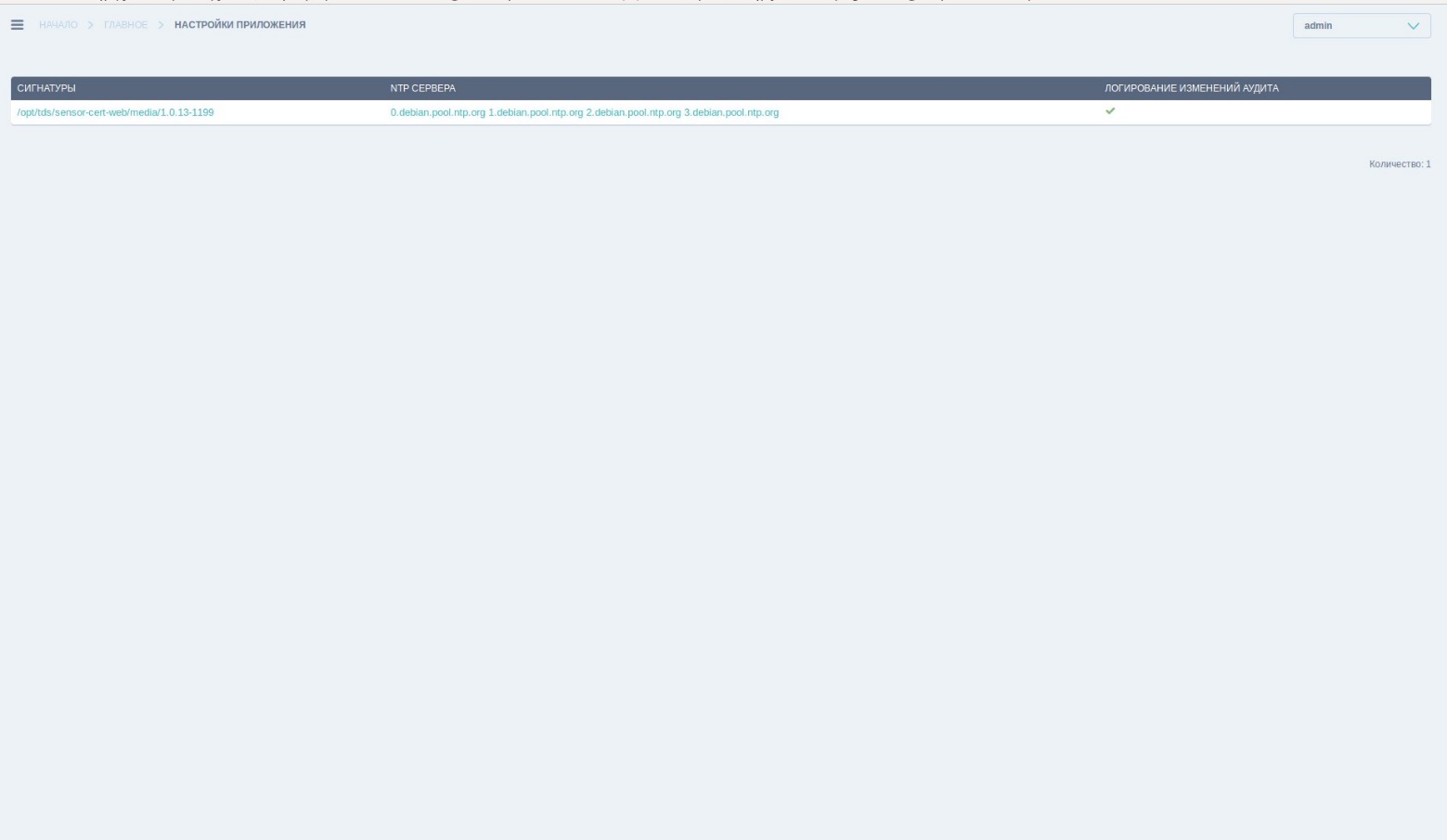


Рис. 25

1. Настроить NTP сервер (рис. 26).

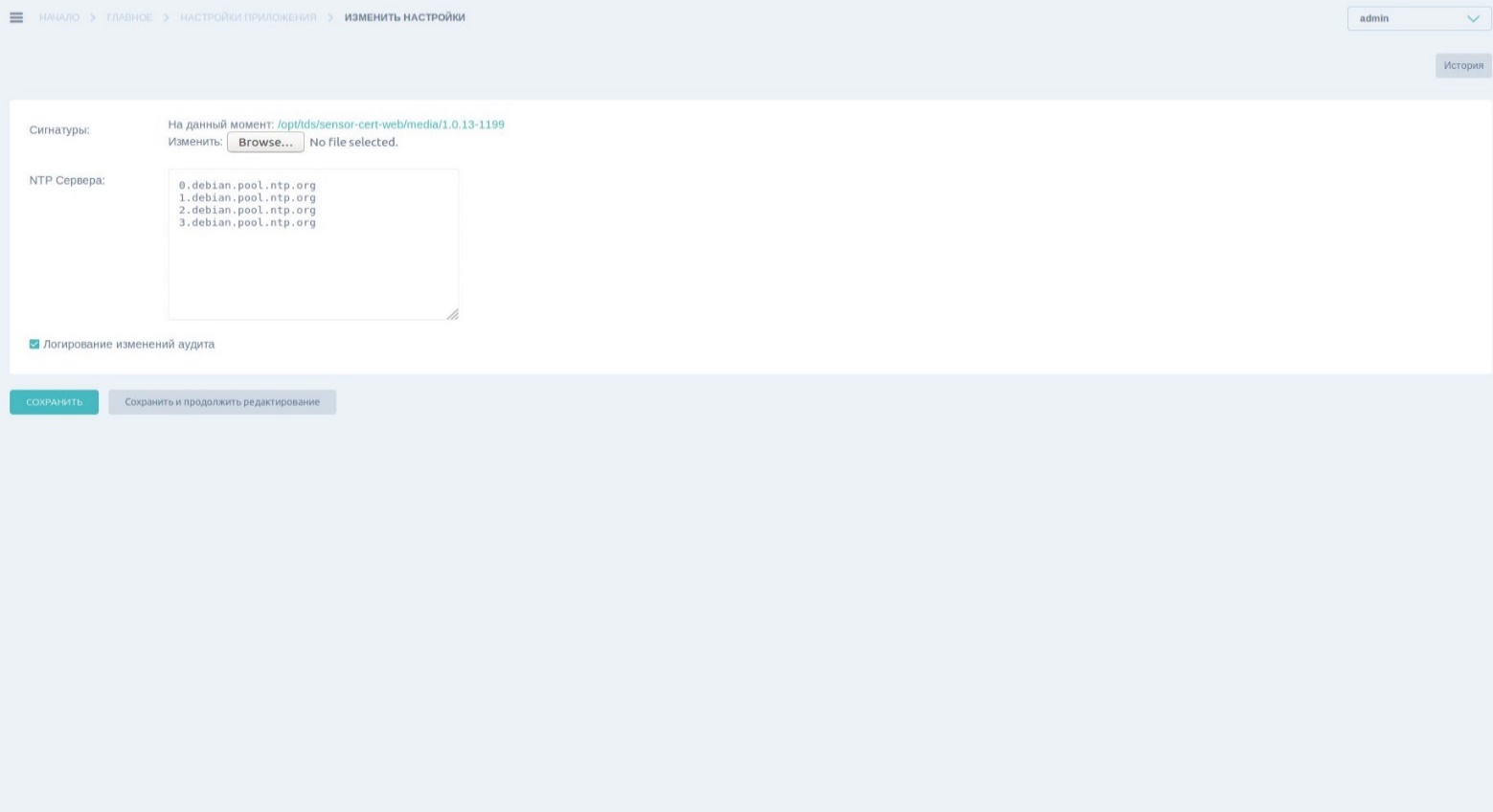


Рис. 26