Закрытое акционерное общество «НТЦ КОНТАКТ»

УТВЕРЖДАЮ

Директор

ЗАО «НТЦ КОНТАКТ»

_____А.А.Тепляков

1 декабря 2021 г.

КОМПЛЕКС ПРОГРАММНО-АППАРАТНЫЙ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «БАС»

Инструкция по настройке подключения устройства, работающего под управлением ОС Linux, к защищенной подсети с аутентификацией по протоколу BSTS

СЮИК.465634.001 ИС54

Подп. и дата | Инв. № дубл. | Взам. Инв. № | Подп. и дата | Инв. № подл.

Содержание

Настоящая инструкция распространяется на «Комплекс программно-аппаратный криптографической защиты информации «БАС» СЮИК.465634.001 (далее – ПАК «БАС»), предназначенный для защиты информации, циркулирующей в каналах передачи данных, а также на «Комплекс программный криптографической защиты информации устройств под управлением ОС Linux «БАС-L» BY.СЮИК.00450-01 (далее – КП «БАС-L»), предназначенный для организации защищенного VPN-подключения устройства, работающего под управлением ОС Linux, к ПАК «БАС».

Настоящая инструкция является расширением Руководства по эксплуатации ПАК «БАС» СЮИК.465634.001 РЭ и Руководства оператора КП «БАС-L» BY.СЮИК.00450-01 34 01 и предназначена для облегчения работы администратора при создании типовой схемы подключения КП «БАС-L» к ПАК «БАС» для построения защищенного соединения.

Настоящая инструкция предназначена для администратора, имеющего навыки работы с ОС Linux, а также сетевым администрированием.

Для понимания принципов работы ПАК «БАС» администратор должен ознакомиться с документом «Комплекс программно-аппаратный криптографической защиты информации «БАС». Руководство по эксплуатации» СЮИК.465634.001 РЭ прежде, чем преступить к настройкам согласно данной инструкции.

Для понимания принципов работы КП «БАС-L» администратор должен ознакомиться с документом «Комплекс программный криптографической защиты информации устройств под управлением ОС Linux «БАС-L». Руководство оператора» BY.СЮИК.00450-01 34 01 прежде, чем преступить к настройкам согласно данной инструкции.

Инструкция описывает порядок настройки ПАК «БАС» и КП «БАС-L» для построения защищенного соединения.

1 Описание соединения (стенда)

Схема подключения устройства, работающего под управлением ОС Linux (для создания стенда использовалась ОС Ubuntu 20.04.), с установленным КП «БАС-L» к защищаемой при помощи ПАК «БАС» подсети приведена на рисунке 1.

Безопасное соединение обеспечивается путем шифрования передаваемых данных с использованием белорусских криптографических алгоритмов, определенных в СТБ 34.101.31-2020.

В данном сценарии для создания защищенного соединения будут использованы протоколы IKE (Internet Key Exchange) версии 2 с использованием расширенного протокола аутентификации EAP (Extensible Authentication Protocol), схема которого определена в СТБ 34.101.66-2014 п. 7.5 (EAP-BSTS).

Подключение ПАК «БАС» к сети передачи данных, а также к сети электропитания проводится в соответствии с Руководством по эксплуатации СЮИК.465634.001 РЭ.

Установка КП «БАС-L» на устройство, работающее под управлением ОС Linux проводится в соответствии с Руководство оператора» BY.СЮИК.00450-01 34 01.

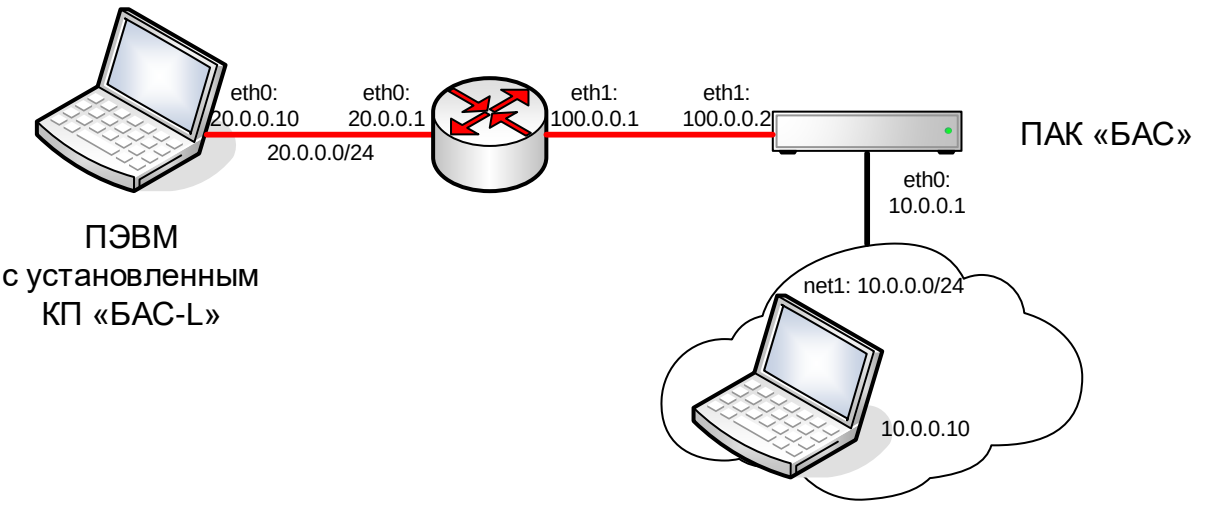

Рисунок 1 – Схема стенда

2 Настройка соединения (стенда)

Для настройки соединения (стенда) необходимо выполнить настройку всех его составляющих: настроить ПАК «БАС», ПК из защищаемых подсетей, а также КП «БАС-L».

Для настройки ПАК «БАС» необходимо выполнить следующие операции:

– смена пароля администратора;

– настройка сетевых интерфейсов;

– настройка даты и времени;

– управление ключевой информацией (генерация ключевой пары, экспорт открытого ключа из устройства в виде запроса на получение СОК и импорт открытого ключа в устройство в виде СОК);

– настройка программного обеспечения.

Для настройки ПК из защищаемых подсетей необходимо выполнить настройку сетевых интерфейсов.

Для настройки КП «БАС-L» необходимо выполнить следующие операции:

– управление ключевой информацией (генерация ключевой пары, экспорт открытого ключа из устройства в виде запроса на получение СОК и импорт открытого ключа в устройство в виде СОК);

– настройка программного обеспечения.

2.1 Настройка ПАК «БАС»

Для настройки ПАК «БАС» необходимо войти в его консоль, используя транспортный логин **server** и пароль **11111111**.

```
server login: server
Password:
server@server:~$
```

2.1.1 Смена пароля администратора

ВНИМАНИЕ: СМЕНА ТРАНСПОРТНОГО ПАРОЛЯ ЯВЛЯЕТСЯ ОБЯЗАТЕЛЬНОЙ

Для смены пароля необходимо воспользоваться командой **passwd**, после чего ввести транспортный пароль **11111111**, а затем задать и подтвердить новый. Пароль должен быть не менее 8 символов.

```
server@server:~$ passwd
Смена пароля для server.
current password:
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлен
```

2.1.2 Настройка сетевых интерфейсов

Для настройки сетевых интерфейсов необходимо отредактировать файл **/etc/network/interfaces** при помощи текстового редактора **nano**, задав IP-адреса и маски интерфейсов.

```
server@server:~$ sudo nano /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

auto lo
iface lo inet loopback

iface eth0 inet static
address 10.0.0.1
netmask 255.255.255.0
auto eth0

iface eth1 inet static
address 100.0.0.2
netmask 255.255.255.0
gateway 100.0.0.1
auto eth1
```

Сохраните изменения в файле, нажав сочетание клавиш **Ctrl+O**, и выйдите из текстового редактора **nano**, нажав сочетание клавиш **Ctrl+X**.

2.1.3 Настройка даты и времени

Для установки даты и времени необходимо воспользоваться командой **date MMDDHHmmYYYY**

где:

MM – месяц;

DD – день;

HH – часы;

mm – минуты;

YYYY – год.

```
server@server:~$ sudo date 010112002022
[sudo] пароль для server:
Сб янв 1 12:00:00 +03 2022
```

Для вступления всех настроек в силу перезагрузите ПАК «БАС».

```
server@server:~$ sudo reboot
```

2.1.4 Управление ключевой информацией

Для надежной аутентификации участники IPsec-соединения должны обладать неизвлекаемым личным ключом, а также парным ему открытым ключом в составе сертификата. В связи с этим необходимо выполнить:

– генерацию личного ключа;

– формирование запроса на выпуск сертификата открытого ключа;

– экспорт запроса на получение сертификата открытого ключа;

– импорт сертификата открытого ключа в ПАК «БАС».

Последовательность действия по управлению ключевой информацией описана в документе «Комплекс программно-аппаратный криптографической защиты информации «БАС». Инструкция по управлению ключевой информацией. СЮИК.465634.001 ИС21».

В связи с тем, что ПАК «БАС» будет использоваться в качестве VPN-сервера для подключения удаленных клиентов, идентификатор Сервера должен быть подтвержден сертификатом. Это необходимо учесть при формировании запроса на выпуск сертификата открытого ключа. Обязательно должно быть заполнено поле **SubjectAltName**. Рекомендуется указать открытый IP-адрес ПАК «БАС».

2.1.5 Настройка программного обеспечения

Настройка программного обеспечения ПАК «БАС» заключается в редактировании файла **/usr/local/etc/ipsec.conf** при помощи текстового редактора **nano**.

```
server@server:~$ sudo nano /usr/local/etc/ipsec.conf

config setup
        charondebug = "ike 1, lib 1, cfg 1, cnt 1"

# Add connections here.
conn %default
        keyexchange = ikev2
        ikelifetime = 24h
        lifetime = 5h
        rekeymargin = 5m
        mobike = yes
        ike = belt_cfb-belt_hmac-prfbrng_hmac-ecp256bign-keyrep
        esp = belt_cfb-belt_mac
        left = 100.0.0.2
        leftsubnet = 10.0.0.0/24
        leftid = 100.0.0.2
        leftcert = cert00001.cer
        leftauth = pubkey
        auto = route
        dpddelay = 1800
        dpdaction = clear
        closeaction = clear

conn BAS-Client
        right = %any
        rightsourceip = 50.0.0.0/24
        rightid = %any
        rightauth = eap-bsts
        rightsendcert = never
```

Сохраните изменения в файле, нажав сочетание клавиш **Ctrl+O**, и выйдите из текстового редактора **nano**, нажав сочетание клавиш **Ctrl+X**.

Установка параметра lifetime = 5h снимает с Сервера задачу контроля времени жизни ключа и перекладывает ее на Клиента. Однако, это не снижает безопасности защищенного соединения, т.к. в КП «БАС-L» реализованы надежные механизмы смены ключа, изменения которых не доступно Оператору.

Установка параметра mobike = yes включает протокол mobike, позволяющий перестроить IPsec-соединение без разрыва связи при изменении IP-адреса Клиента.

Установка параметра dpddelay = 1800 запускает механизм проверки отказавших соединений (DPD) через 1800 с (30 мин) отсутствия от Клиента входящего трафика. Значение осознанно выбрано большим, т.к. отсутствие трафика от удаленного Клиента вполне нормально, а вероятность отключения удаленного Клиента выше, чем вероятность отключения Сервера. Механизм DPD очищает на Сервере информацию об отключенных Клиентах и освобождает выделенные им адреса.

Стоит обратить внимание на параметры leftauth = pubkey и rightauth = eap-bsts. Это приводит к последовательной двухступенчатой аутентификации. Данный механизм повышает надежность аутентификации Клиентов, которые зачастую подключаются к Серверу через недоверенную среду. На первом шаге аутентификации Сервер аутентифицируется перед Клиентом, используя свою ключевую пару. И только после того, как Клиент убедится в том, что пытается подключиться к доверенному серверу, выполняется второй шаг аутентификации – взаимная аутентификация по протоколу EAP-BSTS.

Параметр rightsourceip задает пул IP-адресов, один из которых будет выделен Клиенту. С этого адреса Клиент будет осуществлять защищенное соединение.

Запустите (перезапустите) IPsec соединение

```
server@server:~$ sudo ipsec restart
Stopping strongSwanCont IPsec...
Starting strongSwanCont 5.8.4 IPsec [starter]...
```

Убедиться в том, что программное обеспечение ПАК «БАС» подгрузило сертификат открытого ключа и сопоставило его с личным ключом, можно при помощи команды **ipsec listcerts**.

```
server@server:~$ sudo ipsec listcerts

List of X.509 End Entity Certificates:
  subject:     "CN=BAS00001, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты"
  issuer:      "CN=УЦ для тестирования, C=BY, L=г.Минск, O=ЗАО 'НТЦ КОНТАКТ'"
  validity:    not before    Jan 1 00:00:00 2021, ok
               not after     Jan 1 00:00:00 2023, ok (expired in 365 days)
  serial:      01:23:45:67:89:ab:cd:ef:00:01:23:45:67:89:ab:cd:ef:00
  altNames:    100.0.0.2
  flags:
  certificatePolicies:
               1.2.112.0.2.0.34.101.78.2.70
  authkeyId:   01:23:45:67:89:ab:cd:ef:00:01:23:45:67:89:ab:cd:ef:00
  sudjkeyId:   01:23:45:67:89:ab:cd:ef:00:01:23:45:67:89:ab:cd:ef:00
  pubkey:      BIGN 512 bits, has private key
  keyid:       01:23:45:67:89:ab:cd:ef:00:01:23:45:67:89:ab:cd:ef:00
  subjkey:     01:23:45:67:89:ab:cd:ef:00:01:23:45:67:89:ab:cd:ef:00
```

О том, что программное обеспечение ПАК «БАС» верно подгрузило сертификат открытого ключа и сопоставило его с личным ключом, свидетельствует запись **pubkey: BIGN 512 bits, has private key**.

Стоит обратить внимание на наличие параметра altNames: 100.0.0.2. Это значение было указано в поле SubjectAltName при формировании запроса на выпуск сертификата. Оно же используется в качестве идентификатора Сервера в параметре leftid.

2.2 Настройка ПК

Настройка ПК заключается в настройке сетевого интерфейса. В ПК необходимо установить IP-адрес, входящий в защищаемую подсеть **10.0.0.0/24**, а в качестве основного шлюза указать IP-адрес ПАК «БАС»:

IP-адрес: 10.0.0.10

Маска подсети: 255.255.255.0

Основной шлюз: 10.0.0.1

2.3 Настройка КП «БАС-L»

При настройке КП «БАС-L» будем исходить из того, что значение времени и даты, а также сетевые настройки на устройстве, на котором установлен КП «БАС-L» выполнены корректно.

Работа с VPN-профилями в КП «БАС-L» осуществляется в плагине программы NetworkManager. NetworkManager – это программа для управления сетевыми соединениями в Linux. Вызов плагина осуществляется через апплет NetworkManager (nm-applet). Это апплет системного трея (system tray), который отображает значок в области уведомлений.

2.3.1 Формирование запроса на выпуск сертификата

Для формирования запроса на получение сертификата открытого ключа необходимо открыть терминал и выполнить команду «RequestBuilder». Модуль RequestBuilder выполнит контроль целостности и самотестирование КП «БАС-L», сгенерирует личный ключ и сформирует запрос на получение сертификата открытого ключа.

Вывод контроля целостности и самотестирования КП «БАС-L»:

```
user@user:~$ RequestBuilder
> Контроль Целостности
Проверка целостности прошла успешно!
Результаты: /etc/support/IntegrityController.log
> Тестирование Библиотеки Криптопреобразований
    Зашифрование в режиме простой замены (|X| = 384) +
    Зашифрование в режиме простой замены (|X| = 376) +
    Расшифрование в режиме простой замены (|X| = 384) +
    Расшифрование в режиме простой замены (|X| = 288) +
    Зашифрование в режиме сцепления блоков (|X| = 384) +
    Зашифрование в режиме сцепления блоков (|X| = 288) +
    Расшифрование в режиме сцепления блоков (|X| = 384) +
    Расшифрование в режиме сцепления блоков (|X| = 288) +
    Зашифрование в режиме гаммирования с обратной связью +
    Расшифрование в режиме гаммирования с обратной связью +
    Шифрование в режиме счетчика +
```

```
  Выработка имитовставки (|X| = 104) +
  Выработка имитовставки (|X| = 384) +
  Установка защиты данных +
  Снятие защиты данных +
  Установка защиты ключа +
  Снятие защиты ключа +
  Хэширование (|X| = 104) +
  Хэширование (|X| = 256) +
  Хэширование (|X| = 384) +
  Преобразование ключа (m = 128) +
  Преобразование ключа (m = 192) +
  Преобразование ключа (m = 256) +
Тестирование алгоритмов СТБ.34.101.31 выполнено.
  Генерация пары ключей +
  Выработка электронной цифровой подписи +
  Проверка электронной цифровой подписи +
  Создание токена ключа +
  Разбор токена ключа +
  Извлечение пары ключей +
  Выработка идентификационной электронной цифровой подписи +
  Проверка идентификационной электронной цифровой подписи +
Тестирование алгоритмов СТБ 34.101.45 выполнено.
  Выработка имитовставки (алгоритм hmac-hbelt, keySize = 232) +
  Выработка имитовставки (алгоритм hmac-hbelt, keySize = 256) +
  Выработка имитовставки (алгоритм hmac-hbelt, keySize = 336) +
  Генерация псевдослучайных чисел (алгоритм brng-ctr-hbelt) +
  Генерация псевдослучайных чисел (алгоритм brng-hmac-hbelt) +
Тестирование алгоритмов СТБ 34.101.47 выполнено.
  Разделение секрета (l = 128) +
  Восстановление секрета (l = 128), подмножество пользователей {1,2} +
  Восстановление секрета (l = 128), подмножество пользователей {1,3} +
  Восстановление секрета (l = 128), подмножество пользователей {1,4} +
  Восстановление секрета (l = 128), подмножество пользователей {1,5} +
  Восстановление секрета (l = 128), подмножество пользователей {2,3} +
  Восстановление секрета (l = 128), подмножество пользователей {2,4} +
  Восстановление секрета (l = 128), подмножество пользователей {2,5} +
  Восстановление секрета (l = 128), подмножество пользователей {3,4} +
  Восстановление секрета (l = 128), подмножество пользователей {3,5} +
  Восстановление секрета (l = 128), подмножество пользователей {4,5} +
  Восстановление секрета (l = 128), подмножество пользователей {1,3,5} +
  Восстановление секрета (l = 128), подмножество пользователей {2,3,4,5} +
  Восстановление секрета (l = 128), подмножество пользователей {1,2,3,4,5} +
Тестирование алгоритмов СТБ 34.101.60 выполнено.
  Сеанс протокола BMQV +
  Сеанс протокола BSTS +
  Сеанс протокола BPACE +
  Сеанс протокола Диффи-Хеллмана +
Тестирование алгоритмов СТБ 34.101.66 выполнено.
  Зашифрование в режиме простой замены +
  Расшифрование в режиме простой замены +
```

```
    Зашифрование в режиме гаммирования с обратной связью +
    Расшифрование в режиме гаммирования с обратной связью +
    Шифрование в режиме гаммирования +
    Выработка имитовставки +
  Тестирование алгоритмов ГОСТ 28147-89 выполнено.
Самотестирование библиотеки криптографических преобразований завершено успешно.
<13>Apr 15 15:56:21 basctl: Тестирование завершено успешно!
```

Далее модуль RequestBuilder инициализирует генератор псевдослучайных чисел (ГПСЧ).

Сначала модуль RequestBuilder попытается проинициализировать аппаратный ГСПЧ ПАК «Барьер – USB». В случае успеха модуль RequestBuilder продолжит работу, при его отсутствии выведутся следующие сообщения:

```
Error: Device Opening Failed!
ПАК "Барьер-USB" не обнаружен.
```

Для сбора инициализирующей последовательности для ГСПЧ оператору будет предложено нажимать клавиши клавиатуры:

```
Для инициализации генератора псевдослучайных чисел нажимайте клавиши клавиатуры:
```

Во время ввода с каждой нажатой клавишей (всего необходимо 32) будет выводится символ точки («.»), а по завершении сбора случайности выведется соответствующее сообщение:

```
Для инициализации генератора псевдослучайных чисел нажимайте клавиши клавиатуры: ..............................  Готово!
```

После успешной инициализации ГСПЧ оператору будет предложено отредактировать XML-файл с данными об устройстве и организации, эксплуатирующей КП «БАС-L»:

```
Желаете отредактировать XML-файл с данными об устройстве? [/etc/support/PersonalData.xml] (Y/N):
```

Эти данные используются при формировании запроса на получение сертификата открытого ключа (СОК). Чтобы отредактировать XML-файл необходимо набрать «y» или «Y» и нажать клавишу «Enter». Откроется редактор nano с содержимым файла «/etc/support/PersonalData.xml». Файл необходимо заполнить, указав уникальное значение в поле CommonName:

```
<?xml version="1.0" encoding="UTF-8"?>
<PersonalData>
  <Subject>
    <CommonName OId="2.5.4.3" Description="Общее имя устройства (DNS-имя, IP-адрес, ID
устройства)">
      client@ntc-contact.by
    </CommonName>
    <CountryName OId="2.5.4.6" Description="Код страны нахождения организации"
Type="printable">
      BY
    </CountryName>
    <LocalityName OId="2.5.4.7" Description="Населённый пункт нахождения организации">
      г. Минск
    </LocalityName>
    <StateOrProvinceName OId="2.5.4.8" Description="Область и район нахождения
организации">

    </StateOrProvinceName>
    <StreetAddress OId="2.5.4.9" Description="Улица, дом, корпус, офис">
      пер. Студенческий, д. 7
    </StreetAddress>
    <OrganizationName OId="2.5.4.10" Description="Сокращенное название организации">
      ЗАО "НТЦ КОНТАКТ"
    </OrganizationName>
    <Description OId="2.5.4.13" Description="Описание субъекта">
      Комплекс программный криптографической защиты информации устройств под управлением
ОС Linux "БАС-L"
    </Description>
    <OrganizationUnitName OId="2.5.4.11" Description="Подразделение организации">

    </OrganizationUnitName>
  </Subject>
  <ExtensionRequest OId="1.3.6.1.4.1.311.2.1.14" Description="Расширения сертификата">
    <!--
    <SubjectAltName OId="2.5.29.17" Description="Альтернативное имя устройства">
      <EMail> example@mail.by </EMail>
      <DNS> example.by </DNS>
      <URI> http://example.by </URI>
      <IP> 10.0.0.1 </IP>
    </SubjectAltName> -->
    <!-- For GosSUOK uncomment next -->
    <!--
    <CertificatePolicies OId="2.5.29.32" Description="Политики сертификата">
      1.2.112.1.2.1.1.1.3.2.2|1.2.112.0.2.0.34.101.78.2.70
    </CertificatePolicies> -->
  </ExtensionRequest>
</PersonalData>
```

Сохраните изменения в файле, нажав сочетание клавиш **Ctrl+O**, и выйдите из текстового редактора **nano**, нажав сочетание клавиш **Ctrl+X**.

Далее оператору необходимо ввести имя ключа. Это должен быть уникальный идентификатор, который станет частью имен файлов ключевых контейнеров, запроса на получение СОК, карточки открытого ключа.

```
Задайте имя личного ключа: user_key
```

Далее необходимо ввести пароль доступа к контейнеру личного ключа.

```
Задайте пароль доступа к контейнеру личного ключа (8-24 символа): ********
Подтвердите пароль: ********
Запрос на получение сертификата открытого ключа успешно сохранен: [/home/user/CertReq_user_key.der]
Карточка открытого ключа успешно сохранена: [/home/user/PublicKeyCard_user_key.rtf]
Ключевой контейнер успешно сохранён: [/home/user/KeyContainer_user_key.ssc]
```

Файлы одного ключевого контейнера с частичным секретом, запроса на получения СОК и карточки открытого ключа сохраняются в корень домашней директории. Ключевой контейнер с личным ключом и другой ключевой контейнер с частичным секретом сохраняются в системную область.

Для выпуска сертификата открытого ключа необходимо экспортировать полученный запрос на получение сертификата из устройства, на котором установлен КП «БАС-L» любым удобным способом и передать в Удостоверяющий центр (УЦ).

2.3.2 Импорт сертификатов УЦ

Для успешного подключения к Серверу Клиент должен иметь СОК «точки доверия». Этой «точкой доверия» может быть сам Сервер или УЦ, выпустивший Сертификат для Сервера. В связи с этим, Клиенту необходимо иметь СОК Сервера и/или корневые Сертификаты УЦ, выпустивших СОК Сервера. Для этого СОК Сервера и/или корневые Сертификаты УЦ должны быть помещены в файловую систему устройства, на котором установлен КП «БАС-L». Рекомендуется использовать «домашнюю» директорию.

2.3.3 Создание VPN-профиля

Для работы с VPN-профилями необходимо вызвать меню области уведомления, нажав на значок nm-applet, в выпавшем меню выбрать необходимую сеть и выбрать пункт «Параметры соединения» (рисунок 2).

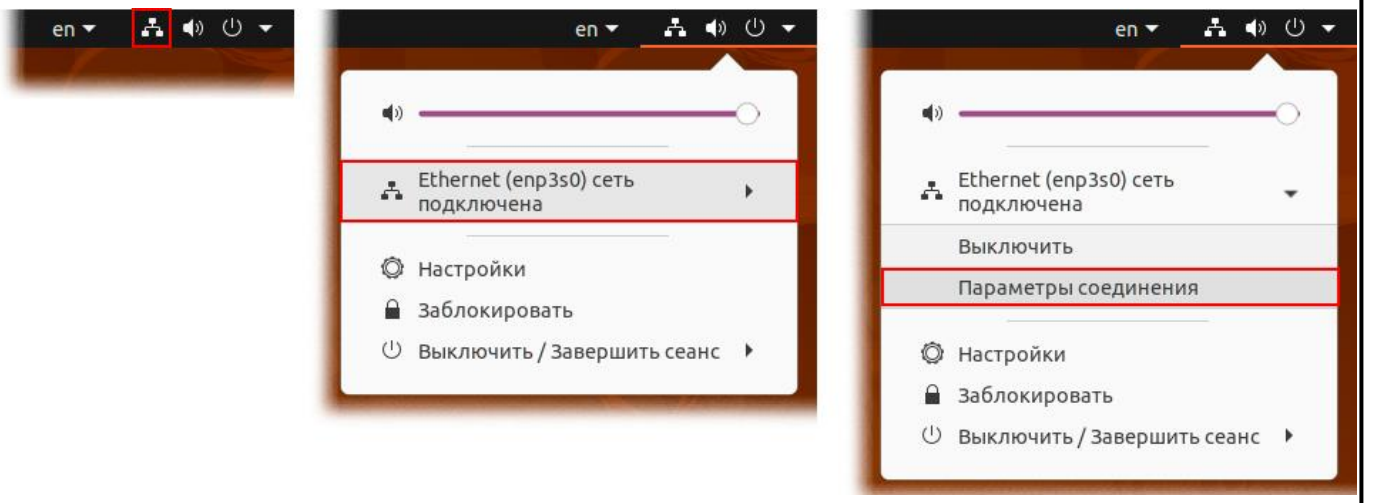

Рисунок 2 – Вызов «Параметры соединения»

После чего откроется окно настройки сети (рисунок 3).

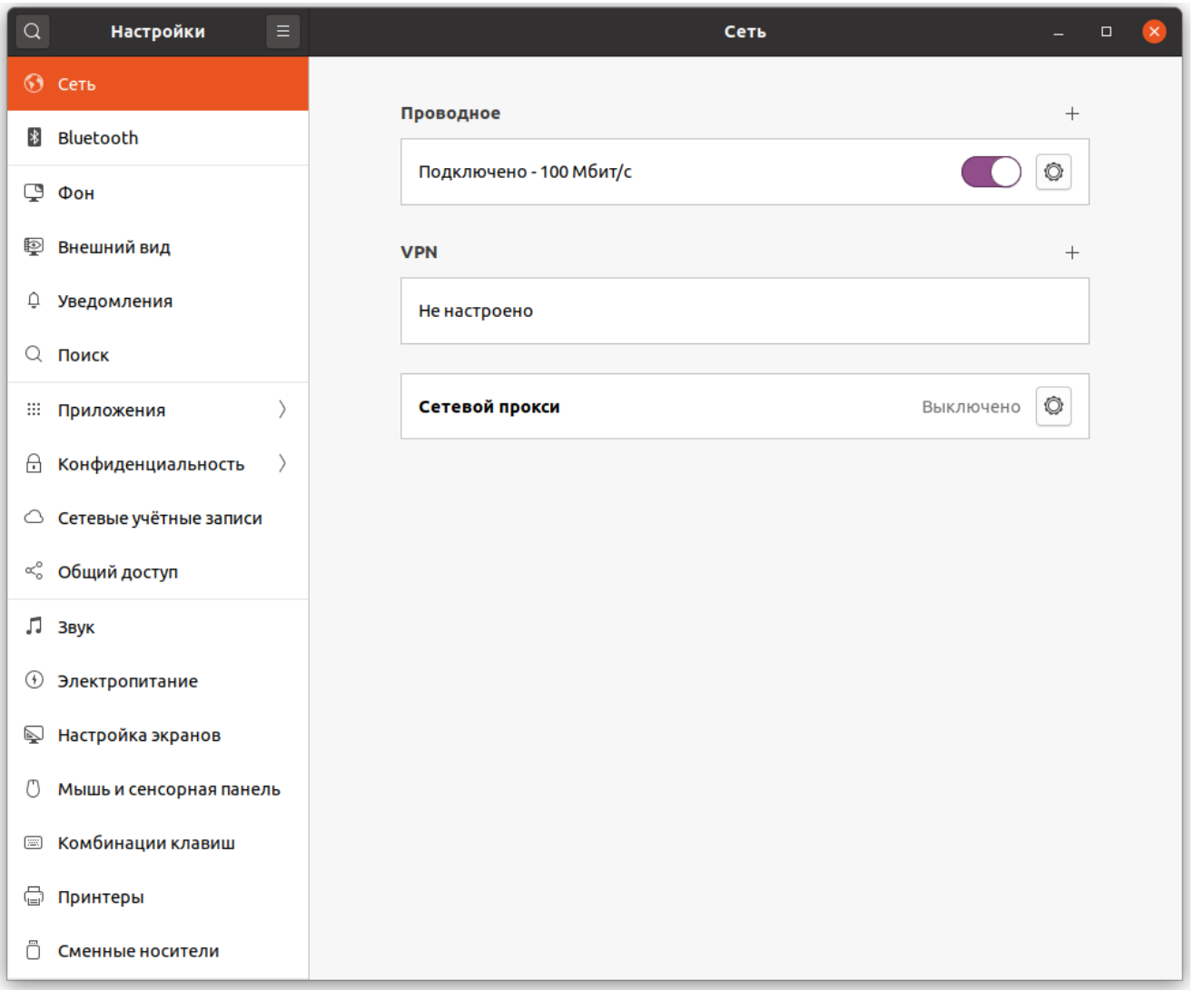

Рисунок 3 – Окно «Настройка сети»

Для создания VPN-профиля необходимо в окне настройки сети нажать на кнопку добавления VPN-профиля + в секции «VPN». Откроется окно со списком доступных плагинов NetworkManager для настройки VPN.

Необходимо выбрать элемент «IPsec/IKEv2 (strongswancont)» (рисунок 4).

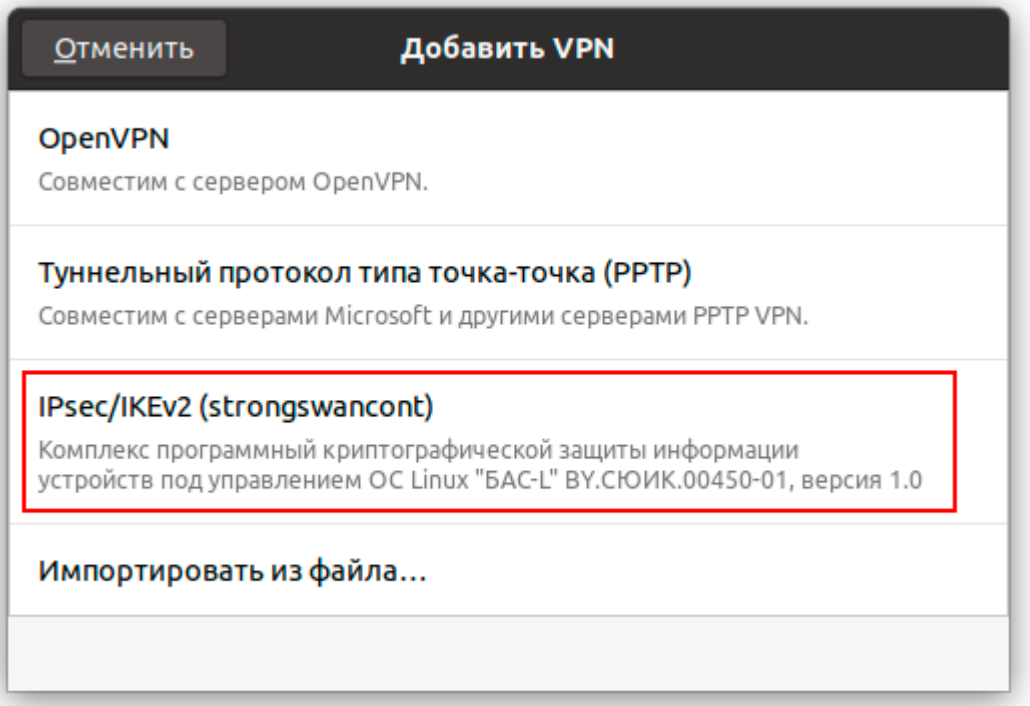

Рисунок 4 – Список VPN-плагинов

Откроется окно для настройки и добавления VPN-профиля (рисунок 5).

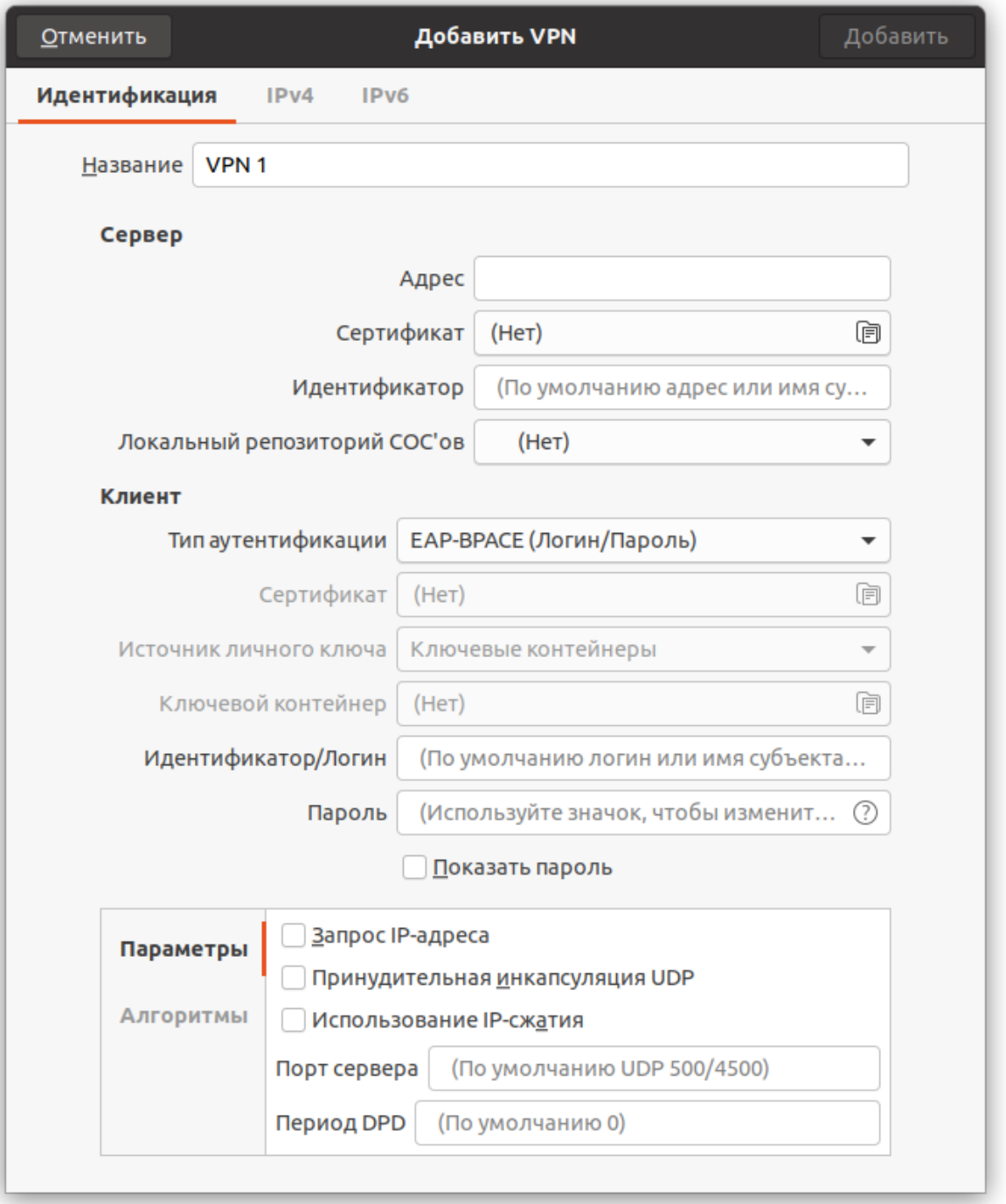

Рисунок 5 – Настройка VPN-профиля

Для создания VPN-профиля необходимо заполнить вкладку «Идентификация» (рисунок 6) и нажать кнопку «Добавить» в верхнем правом углу окна добавления VPN-профиля. Если она неактивна, то это значит, что в какое-то из обязательных полей не было внесено значение или оно некорректно.

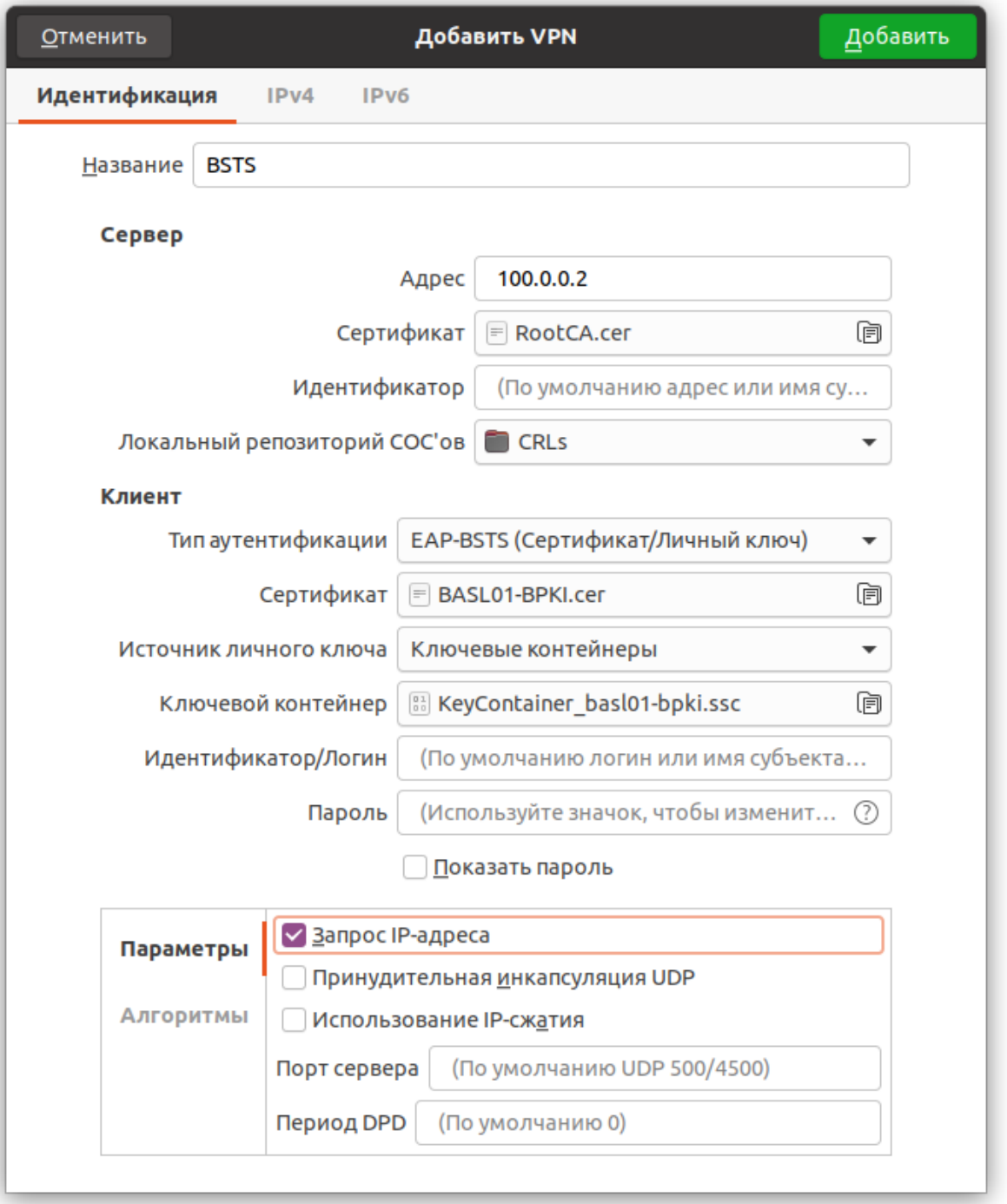

Рисунок 6 – Настроенный VPN-профили

После нажатия на кнопку «Добавить» окно добавления VPN-профиля закроется и станет активным ранее открытое окно настройки сети.

В секции «VPN» отобразится созданный VPN-профиль (рисунок 7).

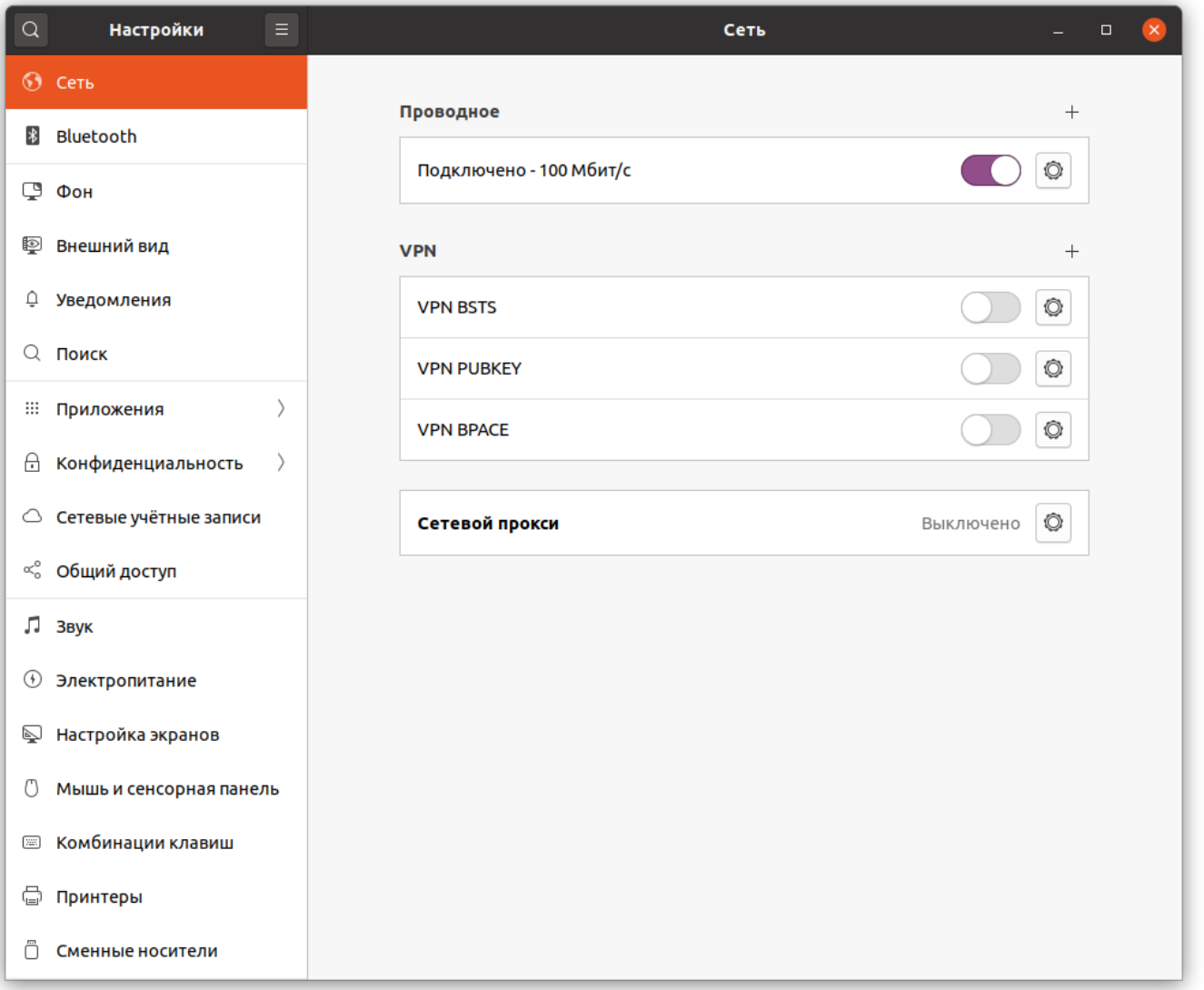

Рисунок 7 – Окно «Настройка сети» с созданными VPN-профилями

Имя VPN-профиля имеет следующий вид: «VPN название», где название – значение, введенное в поле «Название» в окне добавления профиля.

Можно создать любое количество VPN-профилей. Все они будут отображаться в виде списка в секции «VPN».

2.3.4 Установка подключения к VPN-серверу

После настройки и сохранения одного или нескольких VNP-профилей установить подключение к VPN-серверу можно двумя способами.

Первый способ установки подключения – через меню области уведомления.

Для установки подключения необходимо нажать на значок nm-applet в области уведомлений, в выпавшем меню выбрать пункт «Соединение VPN выключено» (рисунок 8).

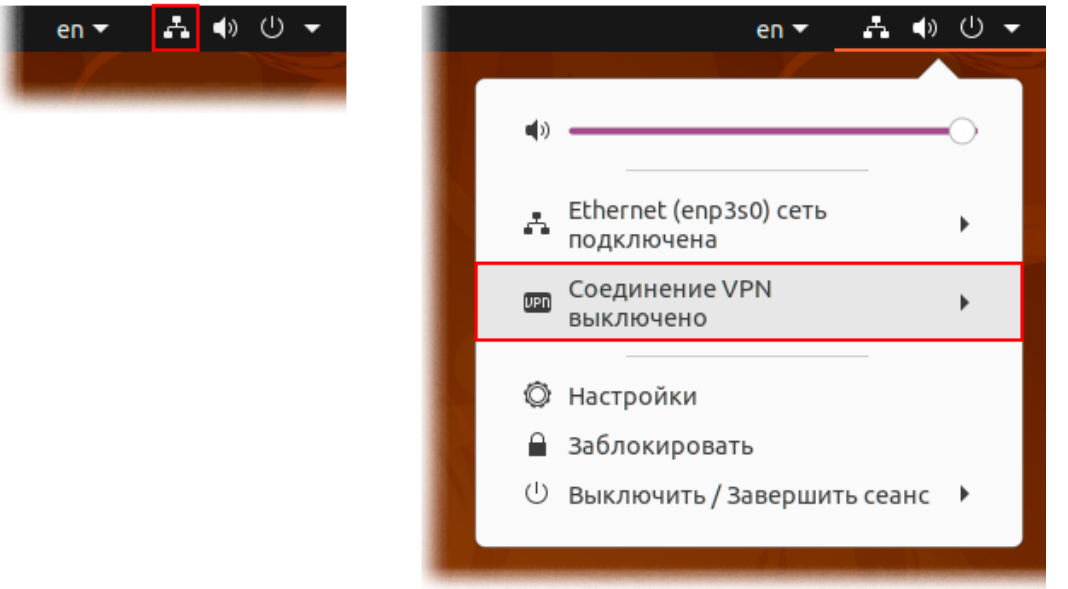

Рисунок 8 – Активация VPN-подключения

После выбора пункта «Соединение VPN выключено» откроется подменю, вид которого зависит от количества настроенных VPN-профилей.

Если был настроен и сохранен один профиль, то подменю будет иметь вид, представленный на рисунке 9. Для установки подключения необходимо выбрать пункт «Соединиться».

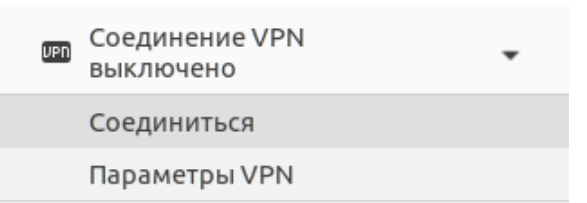

Рисунок 9 – Установка VPN-подключения при наличии одного профиля

Если было настроено несколько VPN-профилей, то подменю пункта «Соединение VPN выключено» будет иметь вид, представленный на рисунке 10. В подменю отображается список настроенных и сохраненных VPN-профилей. Для установки подключения необходимо выбрать один из доступных VPN-профилей.

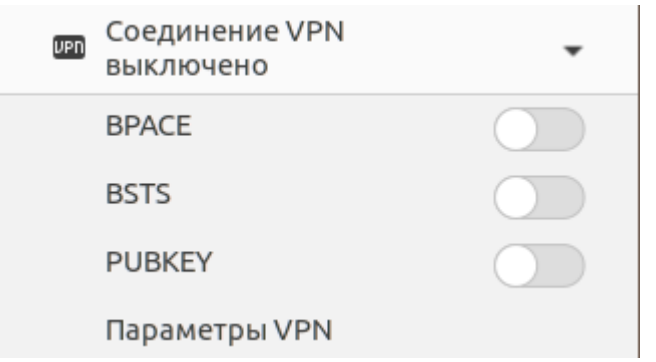

Рисунок 10 – Установка VPN-подключения при наличии нескольких профилей

Второй способ установки подключения – через окно настройки сети.

Для установки подключения необходимо открыть окно настройки сети (рисунок 7) и в секции «VPN» нажать на кнопку-переключатель («включить») в строке VPN-профиля, который нужно использовать для подключения (рисунок 11).

Рисунок 11 – Установка VPN-подключения через окно настройки сети

Если в VPN-профиле не сохранен пароль аутентификации, то во время подключения он будет запрошен через окно аутентификации с соответствующим сообщением (рисунок 12).

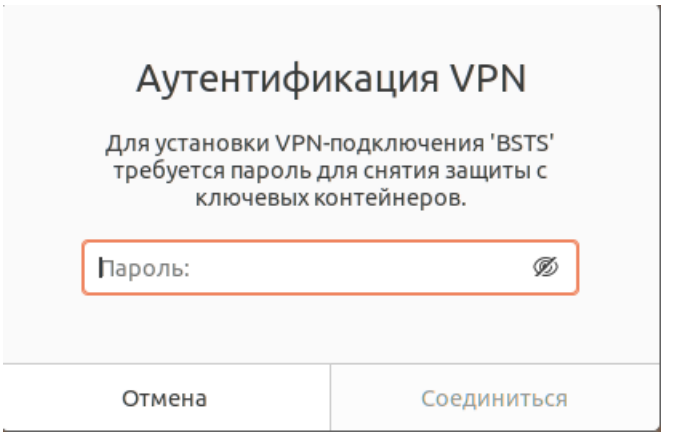

Рисунок 12 – Запрос пароля.

После успешного подключения к VNP-серверу в области уведомлений отобразится значок VNP (рисунок 13).

Рисунок 13 – Значок установленного VPN-подключения

Также после успешного подключения в меню области уведомления вместо пункта «Соединение VPN выключено» отобразится пункт со значком VNP и названием активного профиля.

3 Проверка работоспособности

Для проверки работоспособности соединения (стенда) необходимо с устройства, на котором установлен КП «БАС-L» выполнить **ping** ПК 1.

```
client@client:~$ ping 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10:     icmp_seq=1    ttl=127      time=2.37 ms
64 bytes from 10.0.0.10:     icmp_seq=2    ttl=127      time=2.45 ms
```

Убедиться в том, что передача данных идет по защищенному туннелю, можно, подав команду **ipsec statusall** в командную строку ПАК «БАС».

```
server@server:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.8.4, Linux 4.19.194-ckt-bas, x86_64):
uptime: 60 seconds, since Jan 1 13:00:00 2022
malloc: sbrk 2297856, mmap 0, used 260720, free 2037136
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
loaded plugins: charon random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 dnskey pem fips-prf gmp xcbc cmac hmac contactcrypto usbbar bpki attr kernel-netlink resolve socket-default stroke vici updown xauth-generic dhcp counters eap-bsts eap-bpace
Virtual IP pools (size/online/offline):
  50.0.0.0/24: 254/1/0
Listening IP addresses:
  100.0.0.2
Connections:
BAS-Client:    100.0.0.2...%any IKEv2, dpddelay=1800s
BAS-Client:    local: [100.0.0.2] uses public key authentication
BAS-Client:    cert: "CN=BAS00001, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты"
BAS-Client:    remote: uses EAP_BSTS authentication
BAS-Client:    child: 10.0.0.0/24 === dynamic TUNNEL, dpdaction = clear
Security Associations (1 up, 0 connecting):
BAS-Client [1]:ESTABLISHED 15 seconds ago, 100.0.0.2[100.0.0.2]..20.0.0.10[CN=client@ntc-contact.by, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D= Комплекс программный криптографической защиты информации устройств под управлением ОС Linux "БАС-L"]
BAS-Client [1]:IKEv2   SPIs:   0974252c95682c2f_i   400423a99128d35d_r*,   public   key reauthentication in 23 hours
BAS-Client [1]:IKE proposal: BELT_CFB/BELT_HMAC/PRF_BRNG_HMAC_HBELT/ECP_256_BIGN
BAS-Client {1}:INSTALLED, TUNNEL, requid 1, ESP in UDP SPIs: cbe8a626_i c9e7890e_o
BAS-Client {1}:BELT_CFB_256/BELT_MAC, 252 bytes_i (3 pkts, 13s ago), 252 bytes_o (3 pkts, 13s ago), rekeying in 4 hours
BAS-Client {1}:10.0.0.0/24 === 50.0.0.1/32
```

Как видно из последних двух строк, установлен туннель между подсетями **10.0.0.0/24 === 50.0.0.0/32**, по туннелю было передано по 3 пакета в каждую сторону), защищенных при помощи алгоритмов **BELT_CFB_256/BELT_MAC**.