

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 VPАСЕ

СЮИК.465634.001 ИС53

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

Содержание

1	Описание соединения (стенда)	4
2	Настройка соединения (стенда)	5
2.1	Настройка ПАК «БАС»	5
2.1.1	Смена пароля администратора.....	6
2.1.2	Настройка сетевых интерфейсов	6
2.1.3	Настройка даты и времени	7
2.1.4	Управление ключевой информацией	7
2.1.5	Настройка программного обеспечения	8
2.2	Настройка ПК	12
2.3	Настройка КП «БАС-L»	13
2.3.1	Импорт сертификатов УЦ	13
2.3.2	Создание VPN-профиля.....	14
2.3.3	Установка подключения к VPN-серверу	20
3	Проверка работоспособности	23

Подп. и дата												
Инв. № дубл.												
Взам. Инв. №												
Подп. и дата												
Инв. № подл.	Изм	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС53			Лит.	Лист	Листов	
	Разраб.	Воронцова				Комплекс программно-аппаратный криптографической защиты информации «БАС» Инструкция по настройке подключения устройства, работающего под управлением ОС Linux, к защищенной подсети с аутентификацией по протоколу VPАСЕ			0	0 ₁	2	23
	Пров.	Фёдоров							ЗАО «НТЦ КОНТАКТ»			
	Н. контр.	Васильев										
	Утв.	Тепляков										

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» ВУ.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» ВУ.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 приступить 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» ВУ.СЮИК.00450-01 34 01 прежде, чем приступить к настройкам согласно данной инструкции.

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

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

Изм	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС53	Лист
						3

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. 7.6 (EAP-VPАСЕ).

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» ВУ.СЮИК.00450-01 34 01.

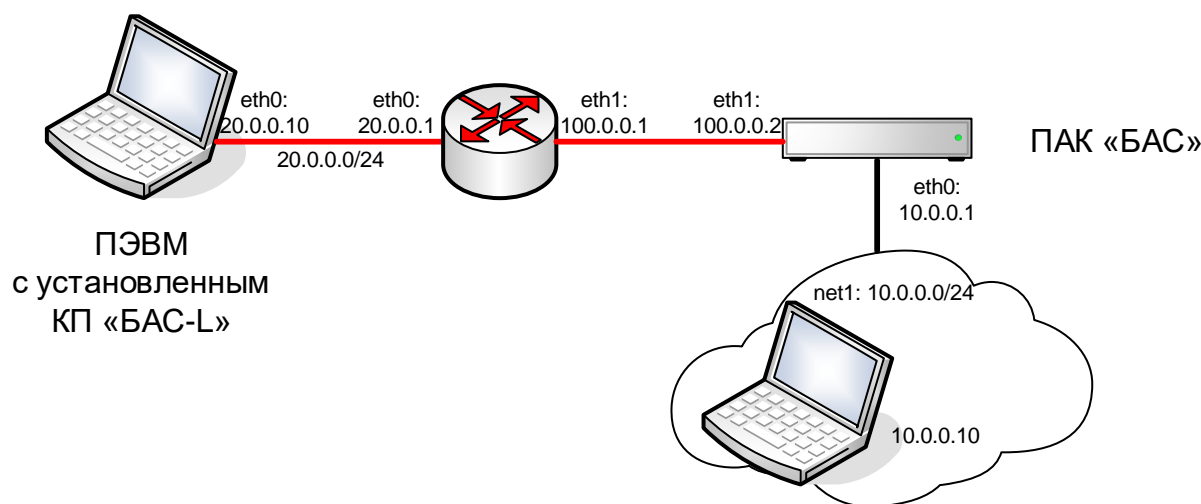


Рисунок 1 – Схема стенда

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

Изм.	Лист	№ докум.	Подп.	Дата

СЮИК.465634.001 ИС53

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 **1111111**.

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

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

Изм.	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС53	Лист
						5

2.1.1 Смена пароля администратора

ВНИМАНИЕ: СМЕНА ТРАНСПОРТНОГО ПАРОЛЯ ЯВЛЯЕТСЯ ОБЯЗАТЕЛЬНОЙ

Для смены пароля необходимо воспользоваться командой **passwd**, после чего ввести транспортный пароль **1111111**, 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**.

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата
Изм.	Лист	№ докум.	Подп.	Дата

СЮИК.465634.001 ИС53

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».

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата
Изм	Лист	№ докум.	Подп.	Дата

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-prfbnrg_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
    rightsourcemap = 50.0.0.0/24
    rightid = %any
    rightauth = eap-bpace
    rightsendcert = never
```

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

Изм.	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС53	Лист
						8

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-расе`. 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-VPACE.

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

Для аутентификации при помощи протокола VPACE оба участника IPsec-соединения должны владеть аутентификационными данными (логин-паролем).

Пароль задается в файле `/usr/local/etc/ipsec.secrets` в следующем формате.

Идентификатор : Тип_аутентификации «Пароль»

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

Изм	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС53	Лист
						9

В качестве идентификатора указывается значение, которое присылает удаленная сторона при запросе IPsec-соединения.

В качестве типа аутентификации необходимо использовать значение EAP.

В качестве пароля необходимо использовать длинные случайные последовательности.

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

```
Client1 : EAP "Password for Client1"  
Client2 : EAP "Password for Client2"  
ClientN : EAP "Password for ClientN"
```

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**.

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

Изм.	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС53	Лист
						10

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.

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

Изм	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС53	Лист
						11

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

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата	СЮИК.465634.001 ИС53	Лист
						12
Изм.	Лист	№ докум.	Подп.	Дата		

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 трей (system tray), который отображает значок в области уведомлений.

2.3.1 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.

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

Изм.	Лист	№ докум.	Подп.	Дата

СЮИК.465634.001 ИС53

2.3.2 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).

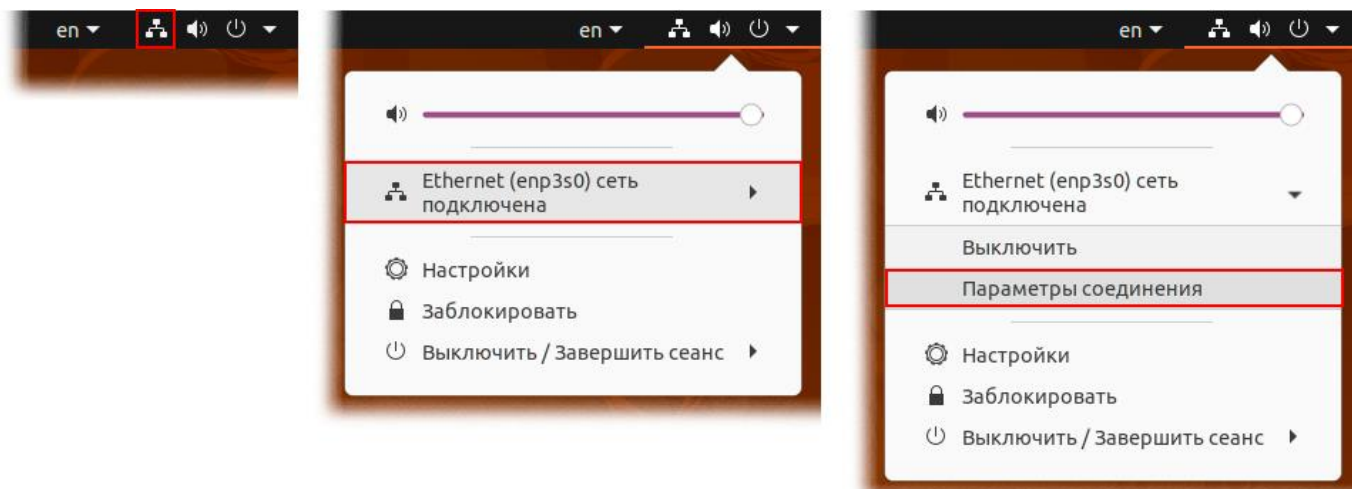


Рисунок 2 – Вызов «Параметры соединения»

После чего откроется окно настройки сети (рисунок 3).

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

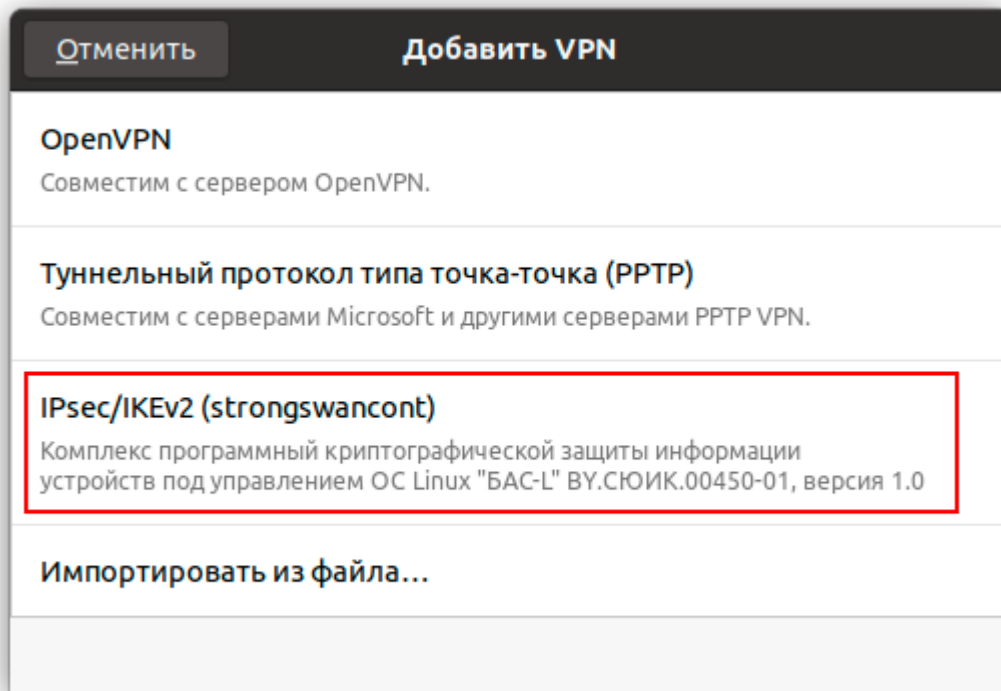


Рисунок 4 – Список VPN-плагинов

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

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата	СЮИК.465634.001 ИС53	Лист
						16
Изм.	Лист	№ докум.	Подп.	Дата		

Отменить
Добавить VPN
Добавить

Идентификация
IPv4
IPv6

Название

Сервер

Адрес

Сертификат

Идентификатор

Локальный репозиторий СОС'ов

Клиент

Тип аутентификации

Сертификат

Источник личного ключа

Ключевой контейнер

Идентификатор/Логин

Пароль

Показать пароль

Параметры

Запрос IP-адреса

Алгоритмы

Принудительная инкапсуляция UDP

Использование IP-сжатия

Порт сервера

Период DPD

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.

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

Изм.	Лист	№ докум.	Подп.	Дата

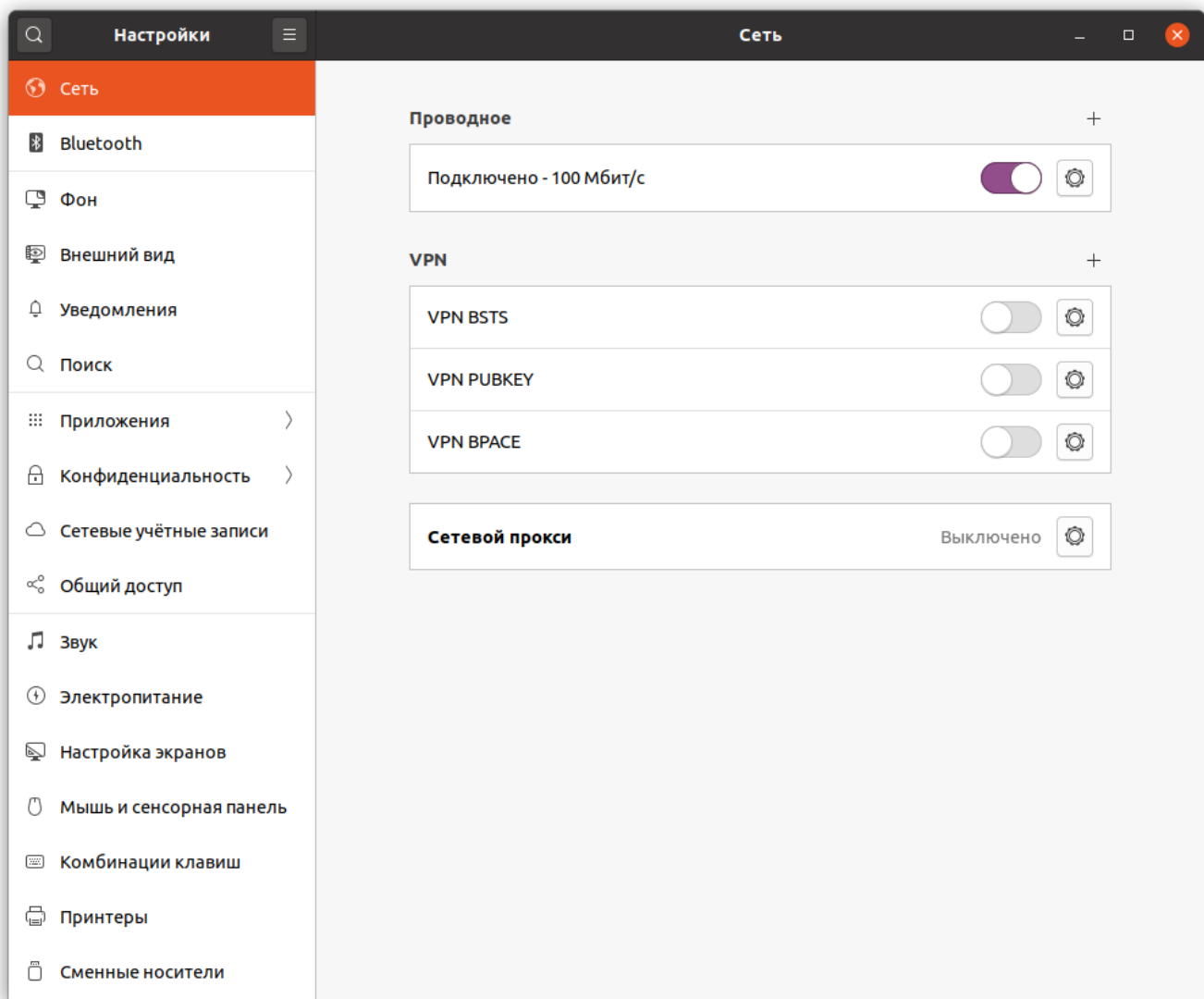


Рисунок 7 – Окно «Настройка сети» с созданными VPN-профилями

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».

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата	Подп. и дата	СЮИК.465634.001 ИС53					Лист				
											19				
						Изм.	Лист	№ докум.	Подп.	Дата					

2.3.3 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).

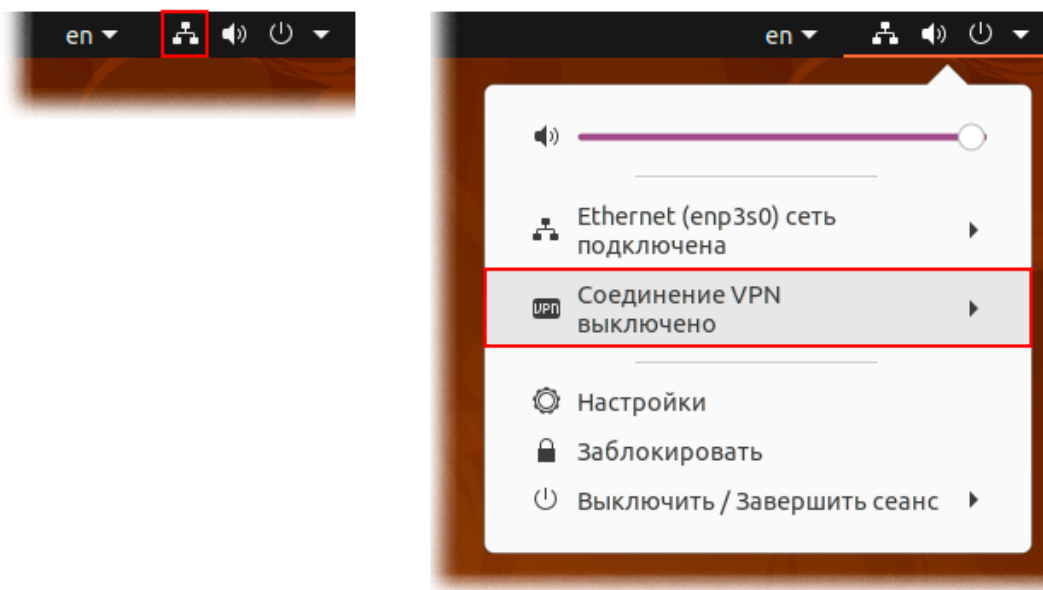


Рисунок 8 – Активация VPN-подключения

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».

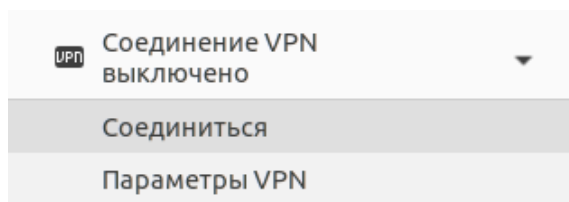


Рисунок 9 – Установка VPN-подключения при наличии одного профиля

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата
Изм.	Лист	№ докум.	Подп.	Дата

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.

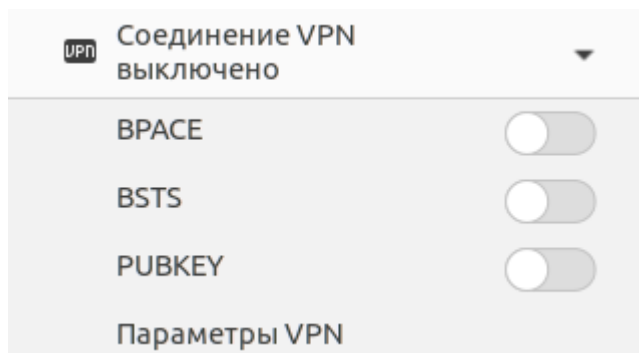


Рисунок 10 – Установка VPN-подключения при наличии нескольких профилей

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).

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

Изм.	Лист	№ докум.	Подп.	Дата

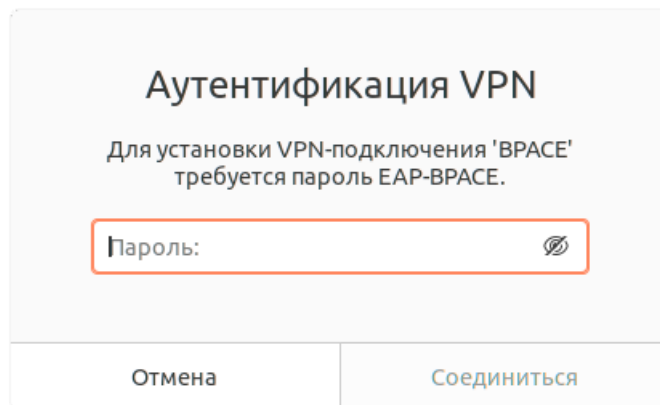


Рисунок 12 – Запрос пароля.

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.

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

Изм.	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС53	Лист
						22

