УТВЕРЖДЕН

BY.СЮИК.00450-01 34 01-ЛУ

КОМПЛЕКС ПРОГРАММНЫЙ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ УСТРОЙСТВ ПОД УПРАВЛЕНИЕМ ОС LINUX «БАС-L»

Руководство оператора

BY.СЮИК.00450-01 34 01

Листов 40

2022

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

№ изм.	Подп.	Дата

Литера O_1

АННОТАЦИЯ

В настоящем документе описывается последовательность действий по установке, запуску и эксплуатации «Комплекса программного криптографической защиты информации устройств под управлением ОС Linux «БАС-L» (КП «БАС- L»).

Для понимания изложенного в документе материала необходимы навыки работы в операционных системах Linux.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1.1. КП «БАС-L» предназначен для организации защищенного VPN-подключения устройства, работающего под управлением ОС Linux, к «Комплексу программно-аппаратному криптографической защиты информации «БАС» СЮИК.465634.001 (далее – ПАК «БАС») или «Комплексу программному виртуальному криптографической защиты информации «БАС-V» BY.СЮИК.00436-01 (далее – КП «БАС-V»).

1.2. КП «БАС-L» обеспечивает криптографическую защиту передаваемых данных посредством полной инкапсуляции IP-пакетов путем их шифрования с использованием криптографических алгоритмов на основе протоколов IPsec.

1.3. Область применения КП «БАС-L» – системы обработки информации ограниченного распространения.

1.4. КП «БАС-L» реализует следующие функциональные возможности:

а) защиту информации путем ее шифрования с использованием криптографических алгоритмов на основе протоколов IPsec;

б) шифрование передаваемых данных в соответствие с СТБ 34.101.31-2020;

в) контроль целостности пакетов данных (вычисление имитовставки) в соответствие с СТБ 34.101.31, СТБ 34.101.47-2017;

г) согласование ключей шифрования и аутентификация в соответствии с СТБ 34.101.66-2014;

д) поддержка режимов аутентификации как с использованием сертификатов открытых ключей (протоком BSTS), так и с использованием предустановленного секрета (протокол BPACE);

е) генерацию ключей и синхропосылок в соответствии с СТБ 34.101.47;

ж) выработку открытых ключей в соответствии с СТБ 34.101.45-2013;

и) формирование запроса на получение сертификата открытого ключа в соответствии с СТБ 34.101.17-2012 и СТБ 34.101.78-2019;

к) обработку сертификатов открытых ключей и списков отозванных сертификатов в соответствии с СТБ 34.101.19-2012 и СТБ 34.101.78;

л) защиту секретных (личных) ключей от несанкционированного раскрытия, модификации и подмены, открытых – от модификации и подмены;

м) проверку работоспособности при включении и по запросу администратора;

н) тестирование следующих параметров;

– тесты криптографических алгоритмов;

– контроль целостности программного обеспечения;

о) возможность работы через NAT при помощи протокола NAT Traversal (NAT-T);

п) ведение журнала аудита;

р) автоматическую смену ключей шифрования при достижении заданного «времени жизни» ключа;

с) получение IP-адреса из пула сервера.

1.5 КП «БАС-L» не ограничивает функциональные возможности устройства, на котором он установлен и работает.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Для выполнения КП «БАС-L» необходимо устройство, работающее под управлением пользовательской ОС Linux, с установленной программой для управления сетевыми соединениями NetworkManager.

КП «БАС-L» для своей работы не предъявляет дополнительных системных требований, отличных от требований ОС Linux.

КП «БАС-L» обеспечивает защиту данных, передаваемых пользователями ОС Linux, вне зависимости от их прав в самой ОС.

В связи с этим, для КП «БАС-L» существует две роли пользователей:

– Администратор;

– Пользователь (оператор).

Администратор – пользователь, обладающий привилегированными правами в ОС Linux.

Администратору доступны следующие функции КП «БАС-L»:

– установка;

– настройка работы с критическими объектами;

– самотестирование;

– просмотр журнала;

– удаление.

Пользователю (оператору) доступны все сервисы, необходимые для организации защищенного канала передачи данных.

Перед началом работы с КП «БАС-L» Администратор ОС Linux должен стандартными средствами ОС выполнить работы по регистрации Пользователей в ОС, созданию их аутентификационных данных и прав. В качестве аутентификационных данных необходимо использовать сложные пароли длиной не менее 8 символов. Это исключает возможность их подбора методом «словаря».

Организация защищенного канала передачи данных с помощью КП «БАС-L» разрешается под непривилегированной учетной записью Пользователя (оператора).

3. ВЫПОЛНЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

3.1. Установка

Установка КП «БАС-L» производится Администратором при помощи менеджера пакетов, используемого в ОС Linux: DPKG для дистрибутивов, основанных на Debian; RPM для дистрибутивов, основанных на RHEL.

Для установки КП «БАС-L» необходимо поместить инсталляционный пакет КП «БАС-L» в файловую систему используемой ОС, открыть терминал и от имени Администратора выполнить команду:

– для дистрибутивов, основанных на Debian:

```
dpkg -i basl-1.0.deb
```

– для дистрибутивов, основанных на RHEL:

```
rpm -i basl-1.0.rpm
```

При использовании КП «БАС-L» совместно с «Комплексом программно-аппаратной защиты информации от несанкционированного доступа «Барьер – USB» СЮИК.467458.004 (далее – ПАК «Барьер – USB») последний должен быть подключен к ПЭВМ в соответствии с его эксплуатационной документацией.

3.2. Выполнение

3.2.1. Формирование запроса на получение сертификата

3.2.1.1. 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.

3.2.1.2. 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!
```

3.2.1.3. 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!
```

3.2.1.4. 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»:

```
<?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)">
      BASL01
    </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>
```

Для сохранения изменений в файле после редактирования необходимо нажать сочетание клавиш «Ctrl+O», затем клавишу «Enter» и выйти из текстового редактора nano, нажав сочетание клавиш «Ctrl+X».

Если оператор отказывается от редактирования файла с данными, то выведется следующее сообщение и модуль RequestBuilder продолжит работу:

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

3.2.1.5. 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:
```

Если оператор ввел имя, ключ с которым в системе уже существует, то оператору будет предложено ввести другое имя до тех пор, пока оператор не введет ранее неиспользованное имя.

```
Задайте имя личного ключа: user_key
Ключ с заданным именем уже существует. Задайте другое имя личного ключа:
```

3.2.1.6. 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.

3.2.1.7. В результате успешной работы модуля RequestBuilder сохраняются файлы, описанные в табл. 1.

Таблица 1

Содержимое файла	Имя файла	Расположение файла
Запрос на получение сертификата	CertReq_*[имя_ключа]*.der	домашняя директория
Защищенный контейнер с личным ключом	PrivKey_*[имя_ключа]*.pkc	системная область
Защищенный контейнер с первым частичным секретом	ShareKey1_*[имя_ключа]*.ssc	системная область
Защищенный контейнер со вторым частичным секретом	KeyContainer_*[имя_ключа]*.ssc	домашняя директория
Карточка открытого ключа	PublicKeyCard_*[имя_ключа]*.rtf	домашняя директория

[имя_ключа] – это имя, введенное оператором во время выполнения модуля RequestBuilder.

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

3.2.1.9. Модуль формирования запроса на получение сертификата открытого ключа может быть настроен Администратором для работы с ПАК «Барьер – USB». Более подробная информация о работе и настройках модуля RequestBuilder приведена в документе «Модуль формирования запроса на получение сертификата открытого ключа. Руководство оператора» BY.СЮИК.00388-03 34 01.

3.2.2. Создание VPN-профиля

3.2.2.1. VPN-профиль – набор параметров и характеристик VPN-подключения, включающий адрес сервера, тип аутентификации, параметры аутентификации, используемые криптографические алгоритмы и др.

КП «БАС-L» выполняет защищенное VPN-подключение к ПАК «БАС» или КП «БАС-V». Поэтому при настройке КП «БАС-L» необходимо учитывать настойки сервера, к которому выполняется VPN-подключение.

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.

Примечание. В разных операционных системах расположение графических элементов, внешний вид меню и названия пунктов могут отличаться от приведенных ниже. Ниже будет приведен пример работы в ОС Ubuntu 20.04.

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» (рис. 1).

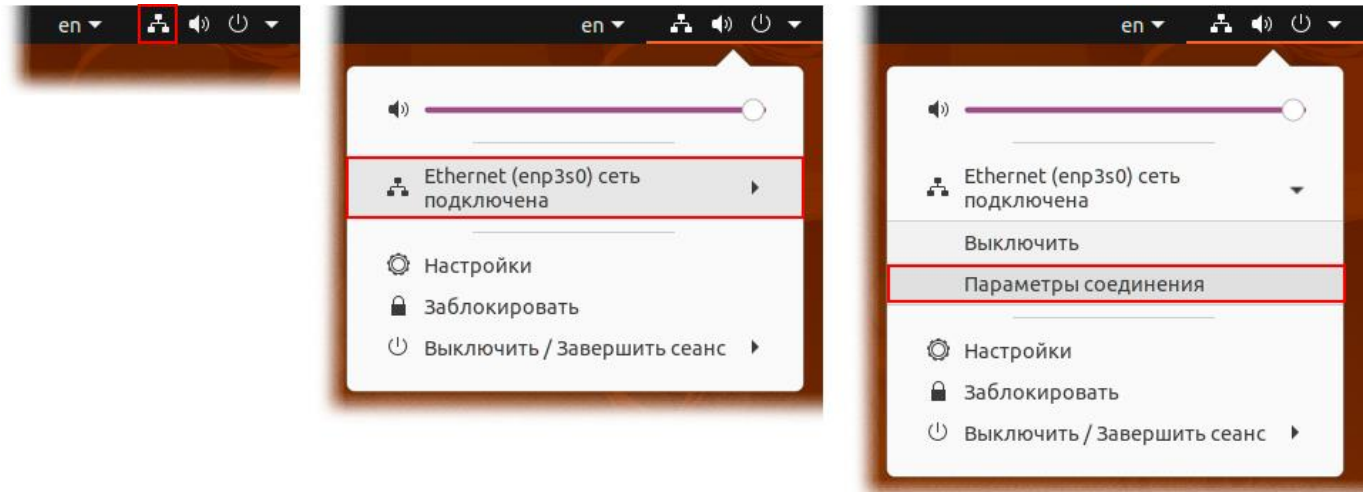

Рис. 1

Откроется окно настройки сети (рис. 2).

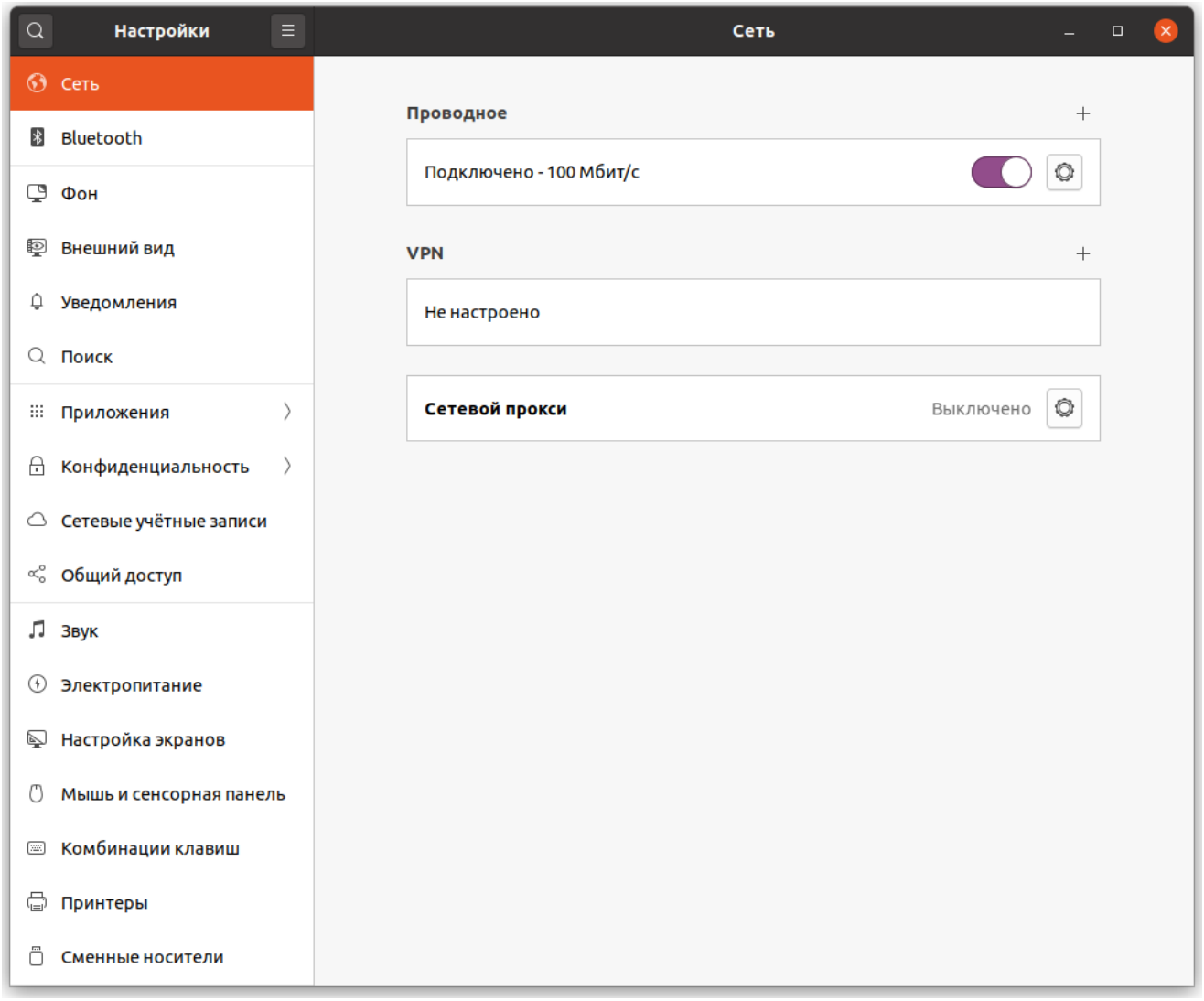

Рис. 2

3.2.2.2. Для создания VPN-профиля необходимо открыть окно настройки сети (рис. 2) и нажать на кнопку добавления VPN-профиля + в секции «VPN». Откроется окно со списком доступных плагинов NetworkManager для настройки VPN.

Примечание. В разных операционных системах этот список может отличаться от приведенного ниже.

В списке необходимо выбрать элемент «IPsec/IKEv2 (strongswancont)» (рис. 3).

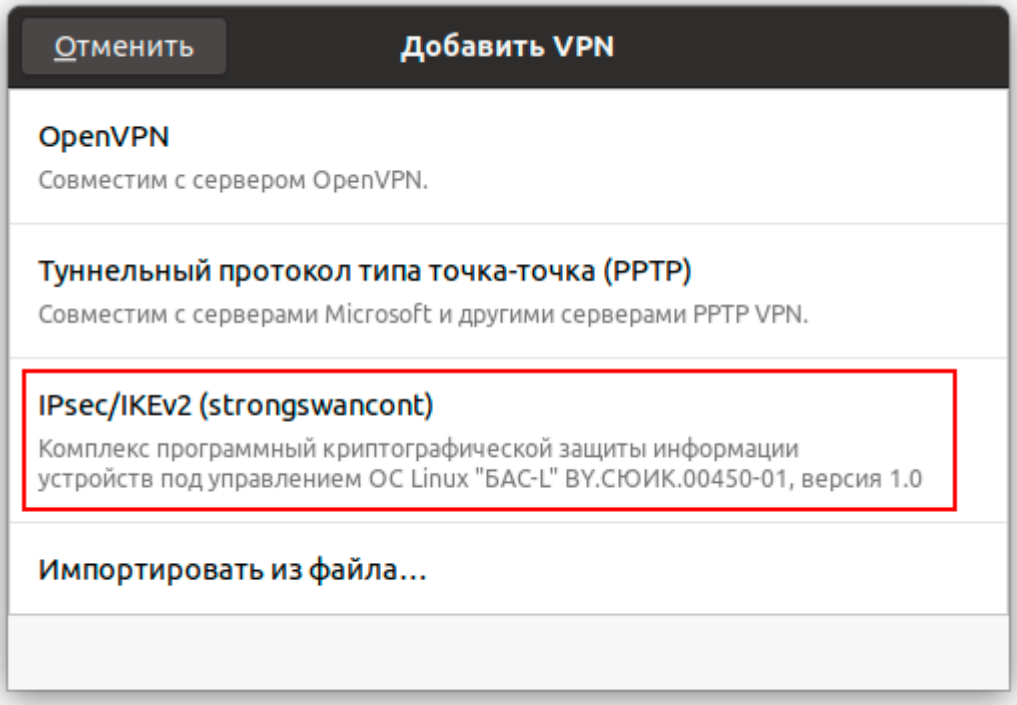

Рис. 3

Откроется окно для настройки и добавления VPN-профиля (рис. 4).

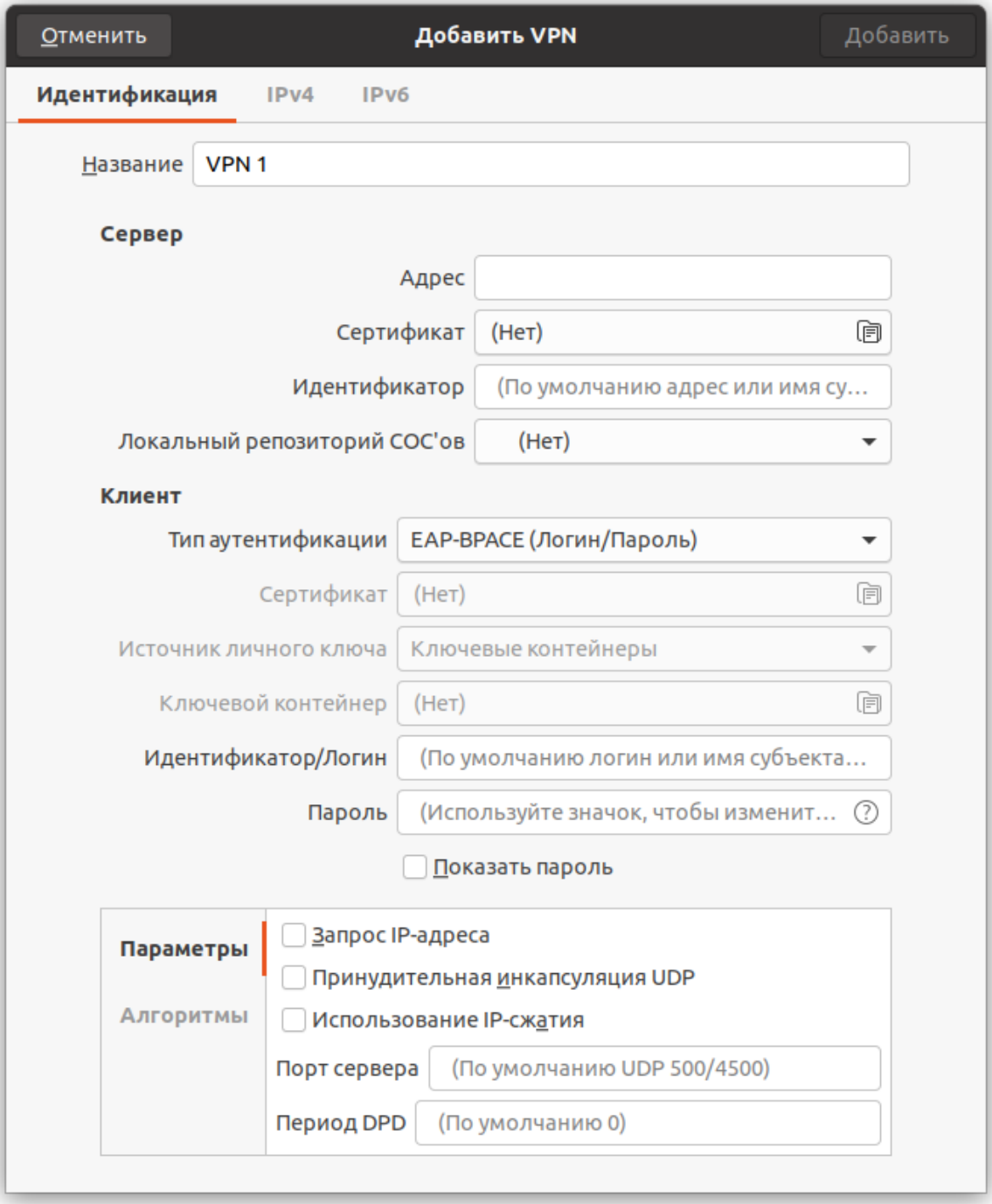

Рис. 4

3.2.2.3. Вкладка «Идентификация» (рис. 4) содержит основные настроечные параметры (характеристики сервера, клиента, тип аутентификации, алгоритмы IKE и ESP и другие).

3.2.2.3.1. Вверху вкладки в поле «Название» указывается название VPN-профиля.

3.2.2.3.2. Набор характеристик сервера содержит следующие поля:

– «Адрес». Обязательное поле для заполнения, должно содержать IP-адрес или имя хоста сервера;

– «Сертификат». Необязательное поле для заполнения. В поле можно указать СОК сервера или УЦ. Если СОК не будет задан, то будут использованы предустановленные сертификаты УЦ;

– «Идентификатор». Необязательное поле для заполнения. В поле можно указать идентификатор сервера. Если значение поля не задано, то по умолчанию будет использоваться адрес сервера либо имя субъекта, указанное в сертификате сервера (если задано);

– «Локальный репозиторий СОС'ов». Необязательное поле для заполнения. В поле можно указать локальную директорию, содержащую файлы списков отозванных сертификатов (СОС'ов).

Пример заполнения секции параметров сервера приведен на рис. 5.

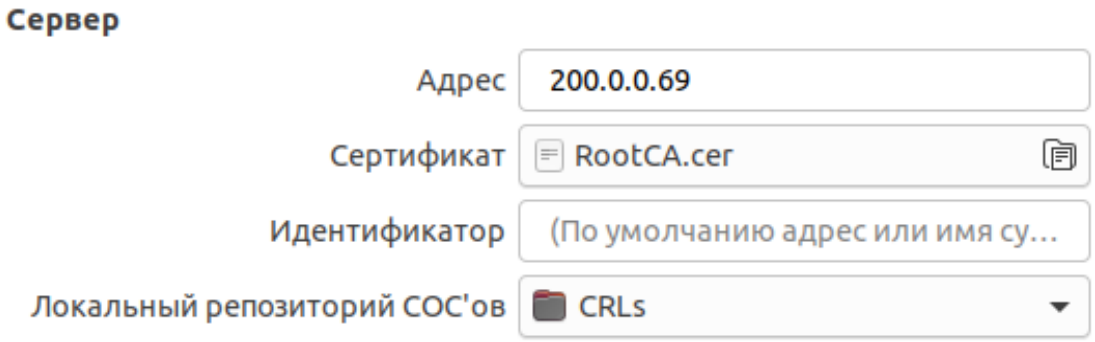

Рис. 5

3.2.2.3.3. Набор характеристик клиента VPN-профиля изменяется в зависимости от выбранного типа аутентификации. Доступно три типа (выпадающий список «Тип аутентификации»):

– «EAP-BPACE (Логин/Пароль)» – аутентификация EAP протоколом BPACE в соответствии с СТБ 34.101.66, п. 7.6;

– «EAP-BSTS (Сертификат/Личный ключ)» – аутентификация EAP протоколом BSTS в соответствии с СТБ 34.101.66, п. 7.5;

– «Сертификат/Личный ключ» – аутентификация IKEv2 с помощью пары «Сертификат – Личный ключ».

3.2.2.3.3.1. Для создания VPN-профиля с типом аутентификации «EAP-BPACE (Логин/Пароль)» в секции клиента необходимо заполнить следующие поля:

– «Тип аутентификации» – выбрать в выпадающем списке «EAP-BPACE (Логин/Пароль)»;

– «Идентификатор/Логин» – необязательное для заполнения поле. Задаётся идентификатор клиента. По умолчанию в качестве идентификатора будет использоваться IP-адрес клиента;

– «Пароль» – необязательное и недоступное для заполнения по умолчанию поле. При использовании настроек по умолчанию пароль будет запрашиваться с помощью окна аутентификации каждый раз при установке подключения (см. п. 3.2.5.).

При сохранении пароля в профиле, он будет передан сервису GNOME Keyring для безопасного хранения.

Примечание. Логин и пароль для аутентификации на сервере должны быть предварительно зарегистрированы Администратором на сервера, к которому будет выполняться подключение, и могут быть получены у Администратора сервера.

Пример заполнения секции параметров клиента для создания профиля с типом аутентификации «EAP-BPACE (Логин/Пароль)» приведен на рис. 6.

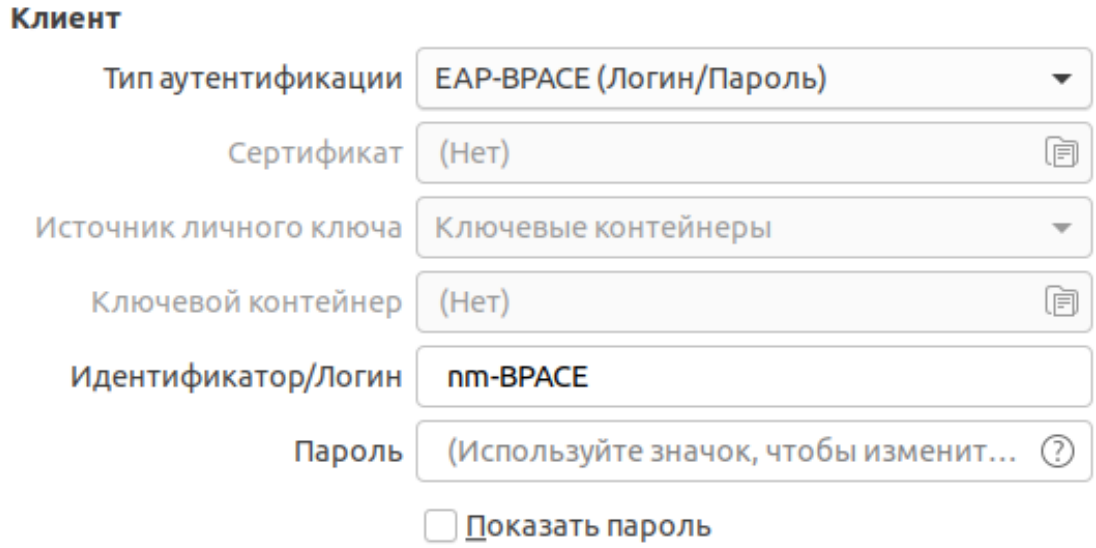

Рис. 6

3.2.2.3.3.2. Для создания VPN-профиля с типом аутентификации «EAP-BSTS (Сертификат/Личный ключ)» или «Сертификат/Личный ключ» в секции клиента необходимо заполнить следующие поля:

– «Тип аутентификации» – выбрать в выпадающем списке «EAP-BSTS (Сертификат/Личный ключ)» или «Сертификат/Личный ключ»;

– «Сертификат» – обязательное для заполнения поле. Указывается пользовательский сертификат;

– «Источник личного ключа» – выбрать в выпадающем списке способ представления личного ключа: «Ключевые контейнеры».

Способ представления личного ключа: «Барьер-USB», может быть использован только при совместном использовании КП «БАС-L» с ПАК «Барьер – USB».

– «Ключевой контейнер» – поле заполняется при выборе в качестве источника личного ключа: «Ключевые контейнеры». Указывается файл ключевого контейнера «KeyContainer*_[имя_ключа]*.ssc», который был сформирован во время работы модуля RequestBuilder (см. п. 3.2.1.);

– «Идентификатор/Логин» – необязательное для заполнения поле. Задаётся идентификатор клиента. По умолчанию в качестве идентификатора будет использоваться имя субъекта сертификата клиента;

– «Пароль» – необязательное и недоступное для заполнения по умолчанию поле. При использовании настроек по умолчанию пароль будет запрашиваться с помощью окна аутентификации каждый раз при установке подключения (см. п. 3.2.5.).

При сохранении пароля в профиле, он будет передан сервису GNOME Keyring для безопасного хранения.

Примечание. При выборе в качестве источника личного ключа: «Ключевые контейнеры» – это пароль снятия защиты с ключевых контейнеров. При выборе в качестве источника личного ключа: «Барьер-USB» – это пароль доступа к защищенному хранилищу ПАК «Барьер – USB». Значение пароля задается при формировании запроса на выпуск сертификата при помощи модуля RequestBuilder;

Пример заполнения секции параметров клиента для создания профиля с типом аутентификации «EAP-BSTS (Сертификат/Личный ключ)» и источником личного ключа «Ключевые контейнеры» приведен на рис. 7.

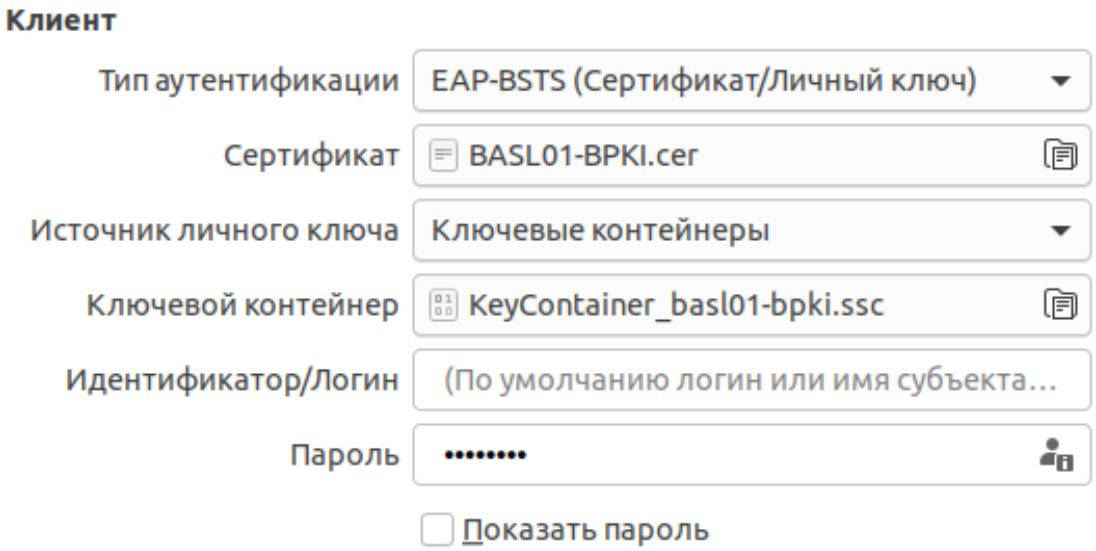

Рис. 7

Пример заполнения секции параметров клиента для создания профиля с типом аутентификации «Сертификат/Личный ключ» и источником личного ключа «Барьер-USB» приведен на рис. 8.

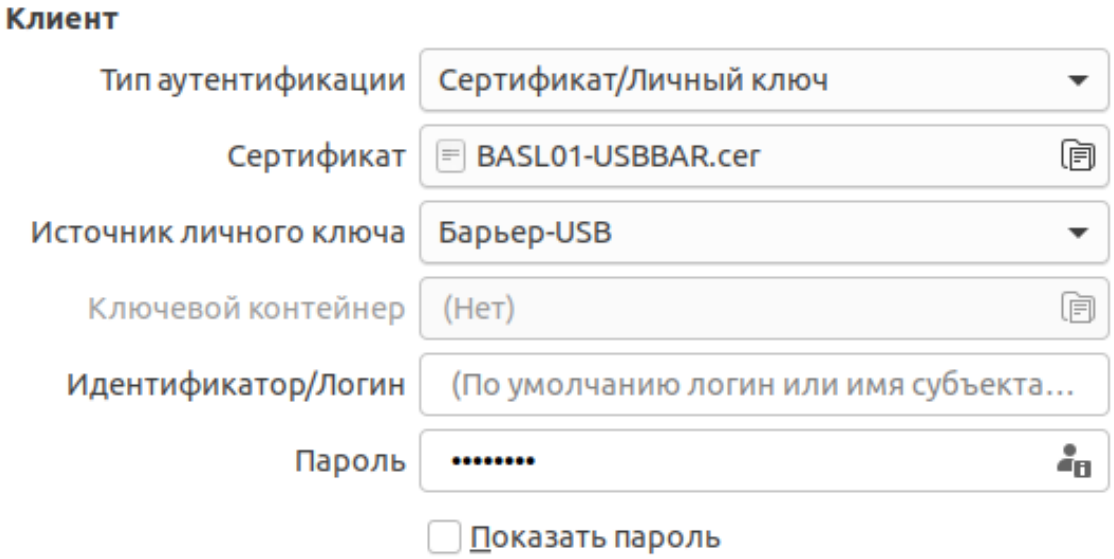

Рис.8

3.2.2.3.4. В нижней части вкладки «Идентификация» есть возможность задать дополнительные параметры VPN-подключения, а также указать криптографические алгоритмы.

3.2.2.3.4.1. В секции «Параметры» можно включить следующие опции:

– «Запрос IP-адреса» – установка данного параметра позволяет клиенту получать IP-адрес из пула адресов, заданного на сервере. При этом в ОС появляется виртуальный интерфейс ipsec0 с адресом, выделенным ему сервером при VPN-подключении. Все запросы к защищаемым ресурсам будут выполняться с этого адреса. Выделение пула адресов для подключаемых клиентов может быть полезно организации маршрутизации;

– «Принудительная инкапсуляции UDP» – установка данного параметра необходима для принудительной инкапсуляции ESP пакетов UDP заголовком. Это обеспечивает беспрепятственную передачу данных в сетях с использованием NAT. Зачастую избыточный параметр, UDP инкапсуляция должна выполняться автоматически;

– «Использование IP-сжатия» – установка данного параметра может увеличить скорость передачи данных за счет сжатия пакетов, однако это требует дополнительных вычислительных ресурсов, что может привести к дополнительной загрузке процессора. Установка данного параметра должна быть предварительно согласована с сервером;

– «Порт сервера» – позволяет использовать нестандартные порты для IPsec-соединения.

– «Период DPD» – период протокола обнаружения отказавших узлов (DPD) в секундах. Определяет временной интервал, с которым периодически отправляются информационные сообщения для проверки работоспособности узла IPsec. По умолчанию период равен 0, что означает, что протокол DPD не используется.

Пример настройки дополнительных параметров VPN-подключения представлен на рис. 9.

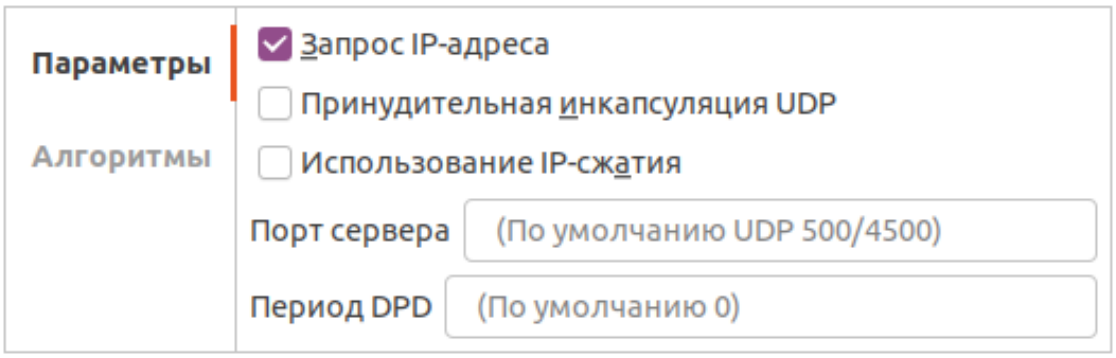

Рис. 9

3.2.2.3.4.2. В секции «Алгоритмы» можно указать криптографические алгоритмы, используемые в протоколах IKE и ESP.

При использовании настроек по умолчанию (пользовательские алгоритмы не указаны) будут использованы алгоритмы, установленные Администратором на сервере.

Для того, чтобы указать пользовательские алгоритмы, необходимо сначала установить флажок «Включить пользовательские алгоритмы».

В поле «IKE» необходимо указать алгоритм шифрования, алгоритм контроля целостности, алгоритм выработки псевдослучайных чисел, алгоритм Диффи-Хеллмана и алгоритм преобразования ключа (опционально). Разделять алгоритмы необходимо символом минуса («-»). Например: belt_cfb-belt_hmac-prfbrng_hmac-ecp256bign.

В поле «ESP» необходимо указать алгоритм шифрования, алгоритм контроля целостности и алгоритм Диффи-Хеллмана (опционально). Разделять алгоритмы необходимо символом минуса («-»). Например: belt_cfb-belt_mac.

Пример настройки пользовательских алгоритмов представлен на рис. 10.

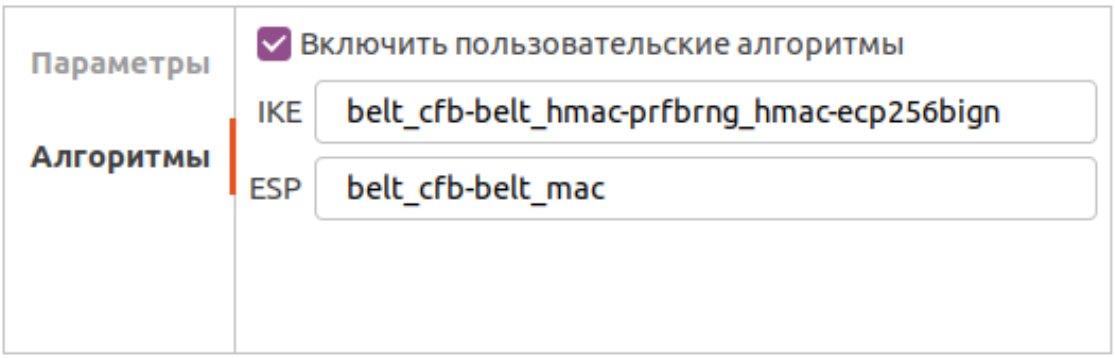

Рис. 10

Полный перечень допустимых значений для каждой группы алгоритмов приведен в Приложении А.

3.2.2.4. Вкладки «IPv4» и «IPv6», являются стандартными вкладками сетевых настроек NetworkManager. Изменение настроек на этих вкладках для создания VPN-профиля обычно не

требуется. Редактирование этих вкладок может выполняться для осуществления специальных настроек, например, добавления маршрута после установки VPN-подключения;

3.2.2.5. После завершения настройки VPN-профиля для его сохранения необходимо нажать кнопку «Добавить» (рис. 11) 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.

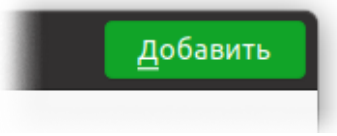

Рис. 11

3.2.2.6. 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 (рис. 12).

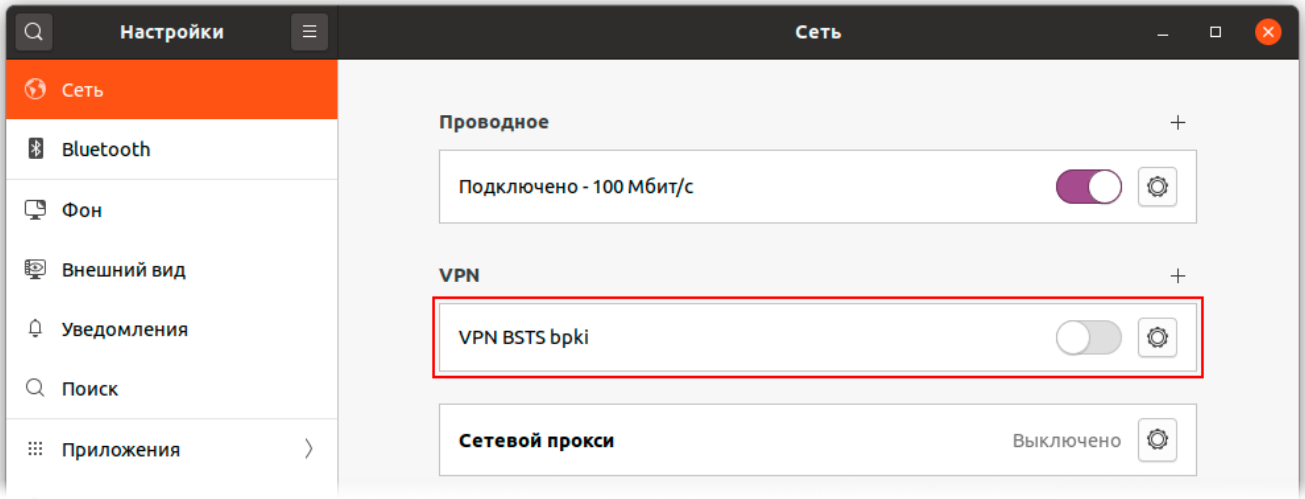

Рис. 12

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

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

3.2.3. Редактирование VPN-профиля

3.2.3.1. Для редактирования VPN-профиля необходимо открыть окно настройки сети (рис. 2) и в секции «VPN» нажать на кнопку настроек в строке VPN-профиля, который нужно отредактировать (рис. 13).

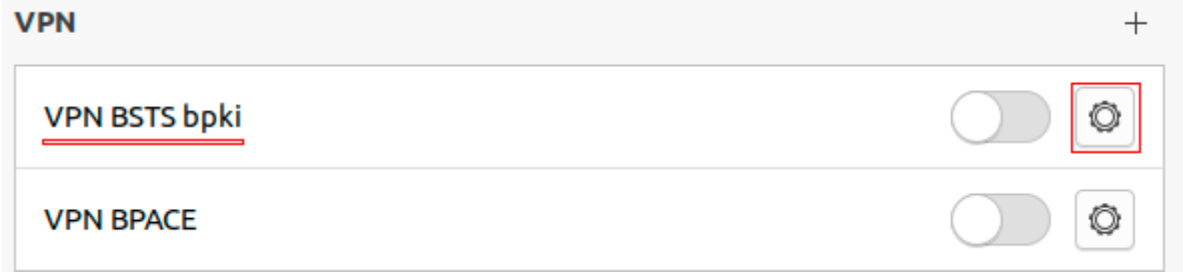

Рис. 13

Откроется окно редактирования VPN-профиля (рис. 14).

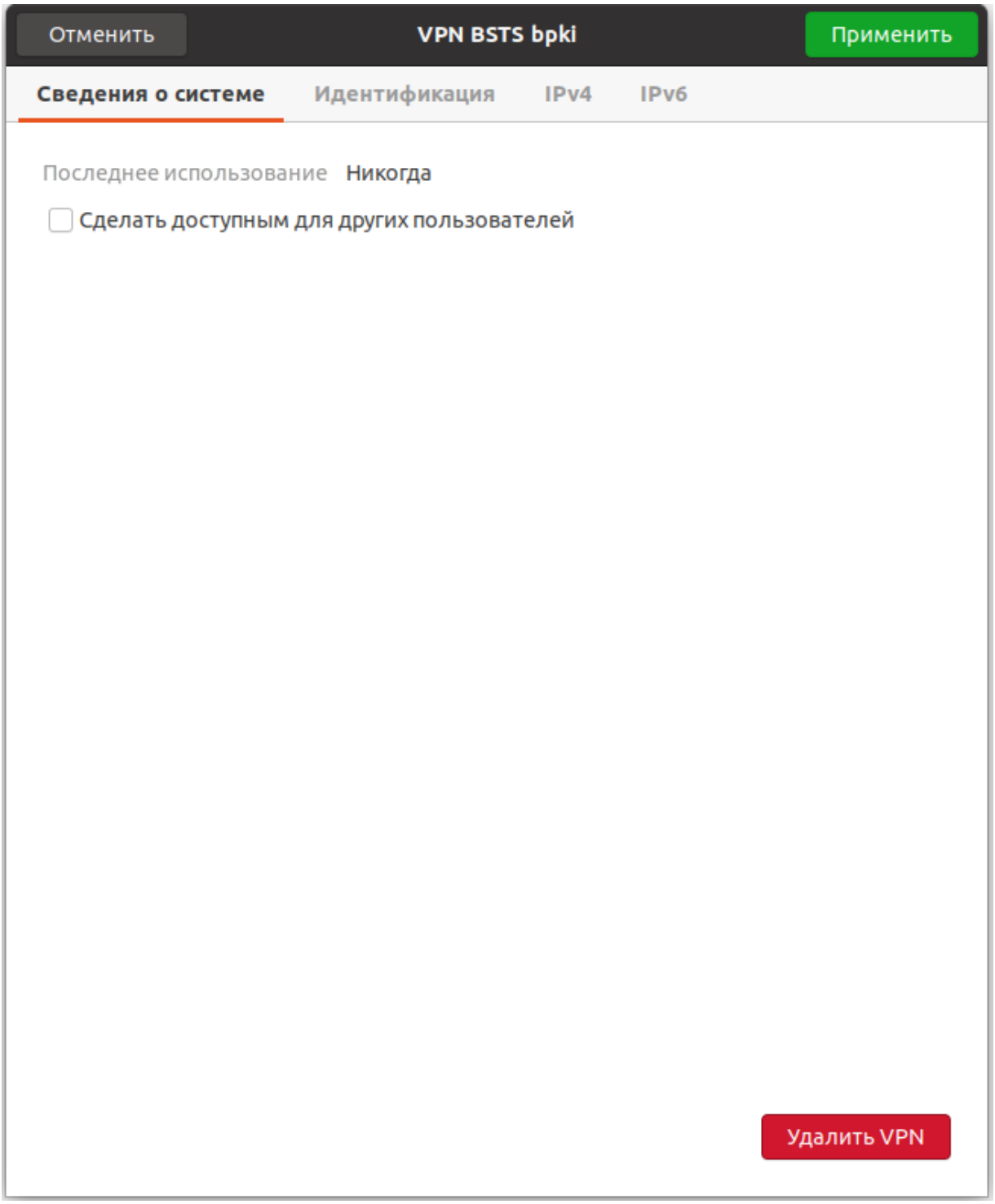

Рис. 14

3.2.3.2. Окно редактирования VPN-профиля содержит четыре вкладки: «Сведения о системе», «Идентификация», «IPv4» и «IPv6».

3.2.3.2.1. Вкладка «Сведения о системе» содержит информацию о последнем использовании выбранного VPN-профиля. На вкладке также можно установить или снять флажок «Сделать доступным для других пользователей». На вкладке «Сведения о системе» располагается кнопка удаления профиля (см. п. 3.2.4.).

3.2.3.2.2. Вкладки «Идентификация», «IPv4» и «IPv6» аналогичны вкладкам окна добавления VPN-профиля (рис. 4). Вкладки описаны в п. 3.2.2.

3.2.3.3. После завершения редактирования VPN-профиля для сохранения изменений необходимо нажать кнопку «Применить» (рис. 15) в верхнем правом углу окна редактирования VPN-профиля.

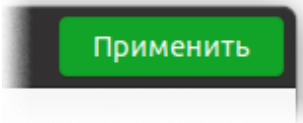

Рис. 15

Чтобы не сохранять внесенные изменения необходимо нажать кнопку «Отменить» (рис. 16) в верхнем левом углу окна редактирования VPN-профиля.

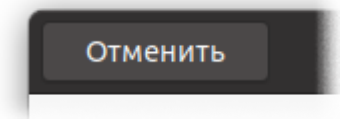

Рис. 16

3.2.3.4. После нажатия на кнопку «Применить» или «Отменить» окно редактирования VPN-профиля закроется и станет активным ранее открытое окно настройки сети.

3.2.4. Удаление VPN-профиля

3.2.4.1. Для удаления VPN-профиля необходимо открыть окно настройки сети (рис. 2) и в секции «VPN» нажать на кнопку настроек в строке VPN-профиля, который нужно отредактировать (рис. 13). Откроется окно редактирования VPN-профиля (рис. 14).

3.2.4.2. Чтобы удалить VPN-профиль в окне редактирования на вкладке «Сведения о системе» необходимо нажать на кнопку «Удалить VPN» (рис. 17) в нижнем правом углу окна.

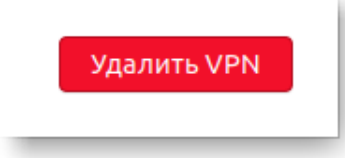

Рис. 17

3.2.4.3. После нажатия на кнопку «Удалить VPN» окно редактирования VPN-профиля закроется и станет активным ранее открытое окно настройки сети. В секции «VPN» из списка доступных VPN-профилей пропадет удаленный VPN-профиль.

3.2.5. Установка подключения к VPN-серверу

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

3.2.5.1. 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» (рис. 18).

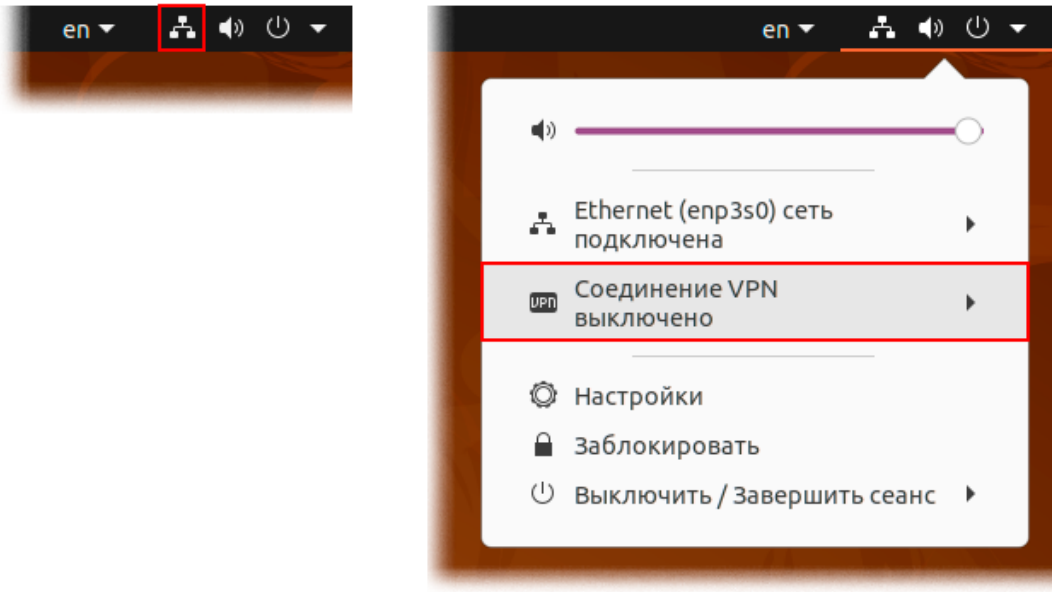

Рис. 18

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 рис. 19. Для установки подключения необходимо выбрать пункт «Соединиться».

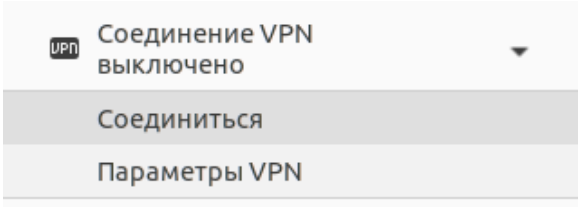

Рис. 19

Если было настроено несколько VPN-профилей, то подменю пункта «Соединение VPN выключено» будет иметь вид, представленный на рис. 20. В подменю отображается список

настроенных и сохраненных VPN-профилей. Для установки подключения необходимо выбрать один из доступных VPN-профилей.

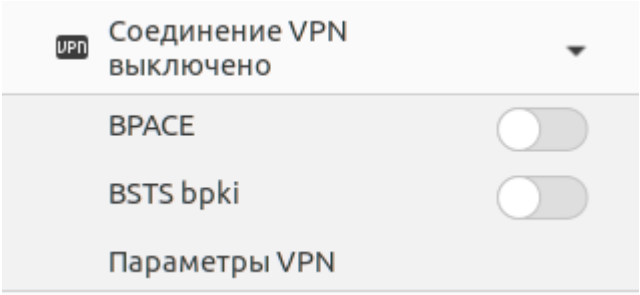

Рис. 20

3.2.5.2. Второй способ установки подключения – через окно настройки сети (рис. 2).

Для установки подключения необходимо открыть окно настройки сети и в секции «VPN» нажать на кнопку-переключатель («включить») в строке VPN-профиля, который нужно использовать для подключения (рис. 21).

Рис. 21

3.2.5.3. Если в VPN-профиле не сохранен пароль аутентификации, то во время подключения он будет запрошен через окно аутентификации с соответствующим сообщением (рис. 22-24).

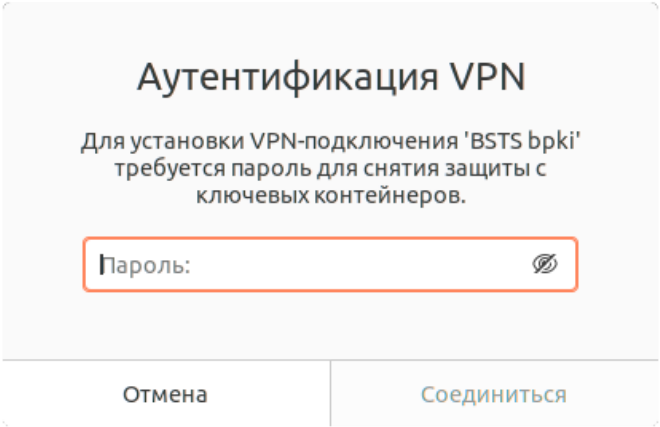

Рис. 22

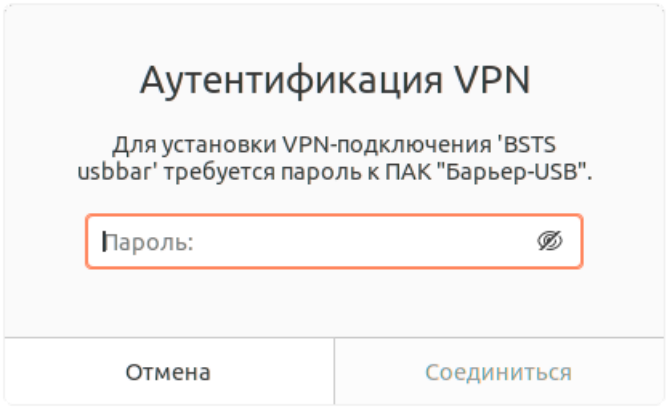

Рис. 23

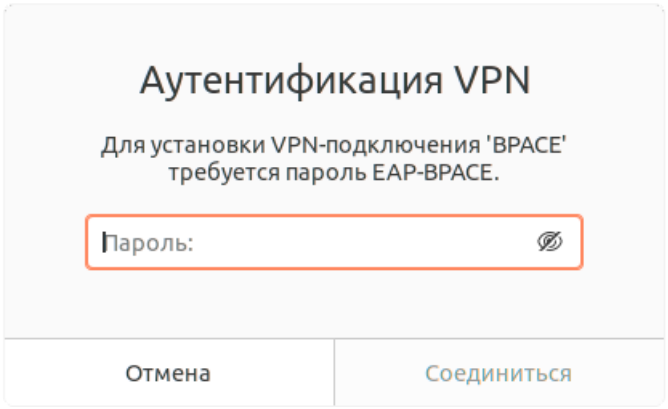

Рис. 24

3.2.5.4. После успешного подключения к VNP-серверу в области уведомлений отобразится значок VNP (рис. 25).

Рис. 25

Также после успешного подключения в меню области уведомления вместо пункта «Соединение VPN выключено» отобразится пункт со значком VNP и названием активного профиля (рис. 26).

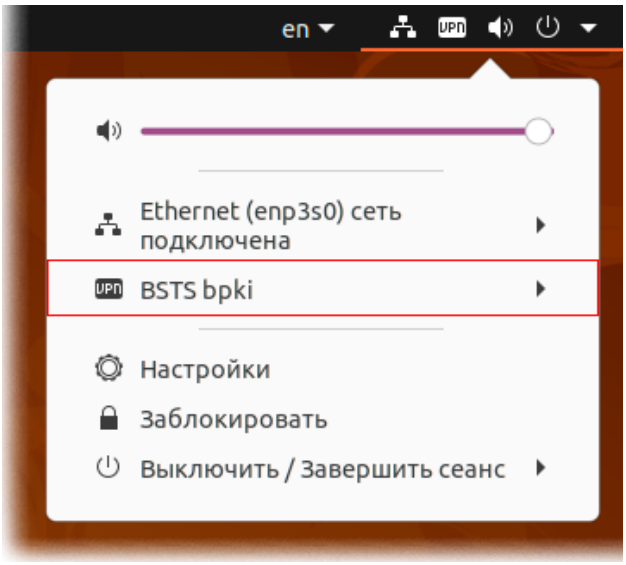

Рис. 26

3.2.5.5. Если во время подключения произошла ошибка, то отобразится всплывающее сообщение (рис. 27).

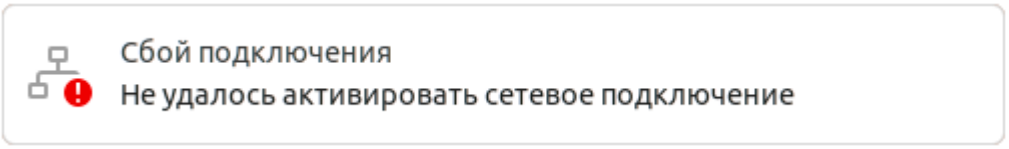

Рис. 27

Записи о причинах возникновения ошибки будут представлены в журнале аудита (см. п. 3.4.).

3.2.6. Отключение от VPN-сервера

После успешного подключения к VNP-серверу отключиться можно двумя способами.

3.2.6.1. Первый способ отключения – через меню области уведомления.

Для отключения необходимо нажать на значок VPN в области уведомлений, в выпавшем меню выбрать пункт со значком VPN и именем активного профиля (рис. 28).

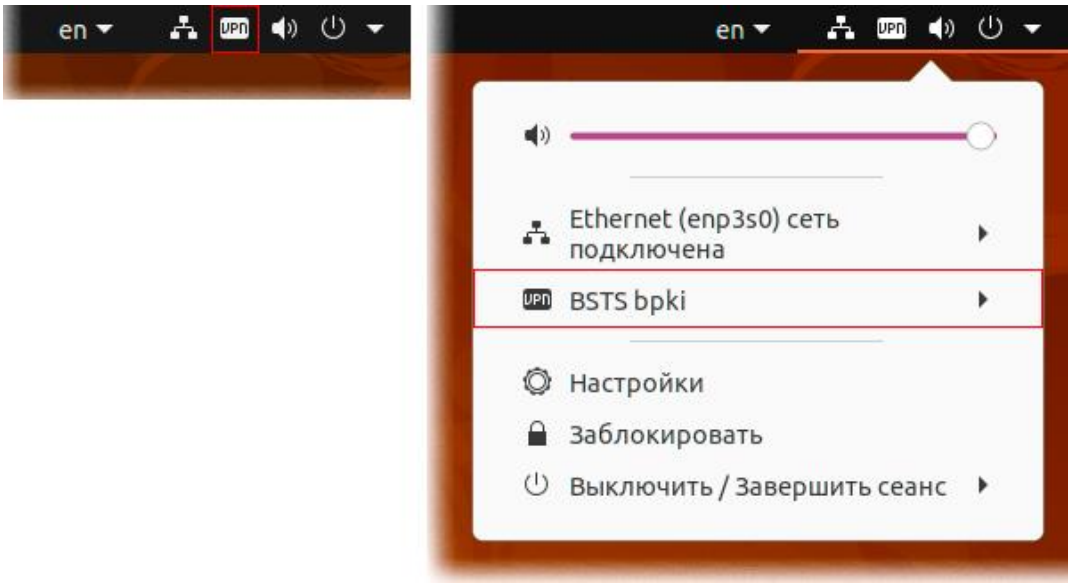

Рис. 28

После выбора пункта со значком VPN и именем активного профиля откроется подменю, вид которого зависит от количества настроенных VPN-профилей.

Если был настроен и сохранен один профиль, то подменю будет иметь вид, представленный на рис. 29. Для отключения активного профиля необходимо выбрать пункт «Выключить».

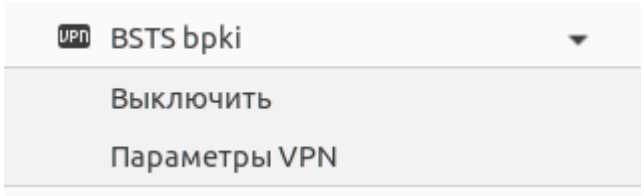

Рис. 29

Если было настроено несколько VPN-профилей, то подменю пункта со значком VPN и именем активного профиля будет иметь вид, представленный на рис. 30. В подменю отображается список настроенных и сохраненных VPN-профилей. Для отключения необходимо выбрать активный VPN-профиль.

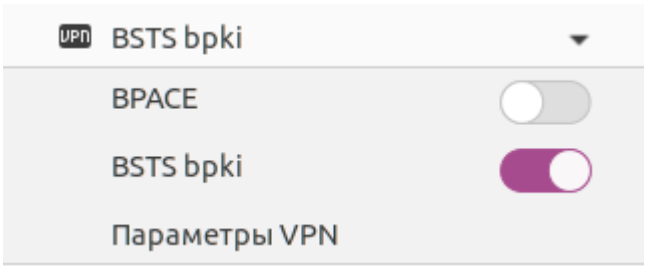

Рис. 30

3.2.6.2. Второй способ отключения VPN-профиля – через окно настройки сети (рис. 2).

Для отключения необходимо открыть окно настройки сети и в секции «VPN» нажать на кнопку-переключатель («отключить») в строке активного VPN-профиля (рис. 31).

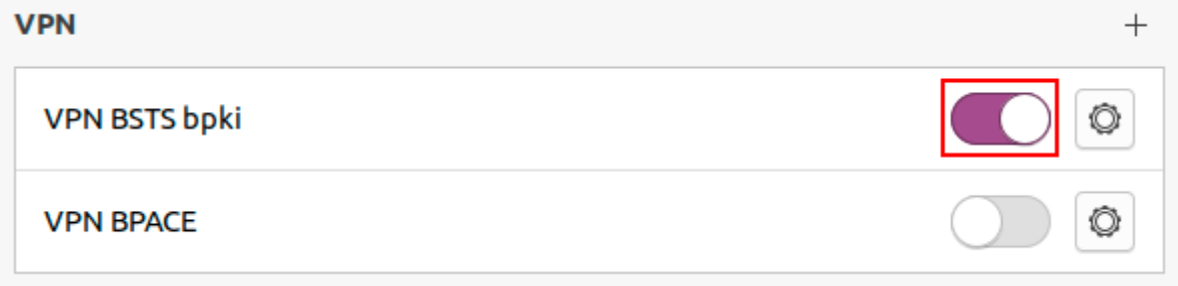

Рис. 31

3.2.7. Удаление ключевой информации

3.2.7.1. Для уничтожения личного ключа, который хранится в виде ключевых контейнеров, необходимо воспользоваться модулем KeyRemover. Модуль KeyRemover уничтожает личный ключ, к которому относится указанный ключевой контейнер.

3.2.7.2. Для уничтожения личного ключа необходимо открыть терминал и выполнить команду «KeyRemover» с обязательным параметром «-k», через пробел от которого необходимо указать путь к ключевому контейнеру второго частичного секрета личного ключа. Имя ключевого контейнера должно иметь вид: «KeyContainer_[имя_ключа].ssc», где [имя_ключа] – это имя, введенное оператором во время выполнения модуля RequestBuilder.

Оператору выведутся предупреждение и вопрос о желании продолжить:

```
user@user:~$ KeyRemover -k /home/user/KeyContainer_user_key.ssc
ВНИМАНИЕ! Удаление личного ключа приведет к его уничтожению без возможности
восстановления.
Желаете продолжить? (Y/N):
```

Для продолжения работы необходимо ввести «y», после чего модуль KeyRemover запрашивает пароль к ключевому контейнеру и выполняет процедуру уничтожения ключевой информации:

```
Желаете продолжить? (Y/N): y
Введите пароль к ключевому контейнеру: ********
Личный ключ удален.
```

Если оператор откажется продолжить работу («n»), то выведется следующее сообщение и модуль KeyRemover завершит работу:

```
Желаете продолжить? (Y/N): n
Действие отменено пользователем.
```

Для получения справочной информации о модуле KeyRemover, необходимо выполнить команду «KeyRemover help» или «KeyRemover help»:

```
user@user:~$ KeyRemover help
```

3.3. Самотестирование

3.3.1. Самотестирование КП «БАС-L» выполняется автоматически при запуске КП «БАС-L» или по запросу Администратора.

3.3.2. Самотестирование КП «БАС-L» включает в себя:

– тестирование криптографических алгоритмов,

– контроль целостности компонентов КП «БАС-L».

3.3.3. Выполнение самотестирования по запросу Администратора осуществляется по команде basctl. Для ее выполнения необходимо иметь привилегированные права в ОС.

```
user@user:~$ sudo basctl
[sudo] пароль для user:
> 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 22 15:49:15 basctl: Тестирование завершено успешно!
```

3.3.4. Если самотестирование завершается ошибкой, КП «БАС-L» блокируется.

3.3.5. При блокировке КП «БАС-L» существующее VPN-подключение завершается, а новое не может быть установлено.

3.3.6. Вывести КП «БАС-L из блокировки» может Администратор путем его переустановки.

3.4. Аудит

3.4.1. Во время работы КП «БАС-L» формирует записи в системный журнал ОС Linux.

3.4.2. При возникновении проблем с VPN-подключением, Администратор может изучить записи системного журнала для определения причины некорректной работы КП «БАС- L».

3.5. Отображение номера версии

3.5.1. КП «БАС-L» предоставляет пользователю информацию о номере версии в графическом виде при создании VPN-профиля (рис. 3).

3.5.2. КП «БАС-L» предоставляет номер версии по запросу Администратора по команде basctl --version. Для ее выполнения необходимо иметь привилегированные права в ОС.

```
user@user:~$ sudo basctl –version
```

3.5.3. Номера версий отдельных компонентов КП «БАС-L» могут быть получены при получении справочной информации о конкретном модуле.

3.6. Работа с ключевой информацией при работе КП «БАС-L» с ПАК «Барьер – USB»

3.6.1. Формирование запроса на получение сертификата

3.6.1.1. Модуль формирования запроса на получение сертификата открытого ключа может быть настроен Администратором для работы с ПАК «Барьер – USB». Более подробная информация о работе и настройках модуля RequestBuilder приведена в документе «Модуль формирования запроса на получение сертификата открытого ключа. Руководство оператора» BY.СЮИК.00388-03 34 01.

3.6.2. Восстановление личного ключа

3.6.2.1. ПАК «Барьер - USB» ведет непрерывный контроль вскрытия корпуса ПЭВМ. При обнаружении вскрытия корпуса ПЭВМ уничтожается личный ключ, хранящийся в защищенном хранилище. ПАК «Барьер – USB» при этом переходит в режим блокировки.

После обнаружения вскрытия корпуса личный ключ КП «БАС-L» считается скомпрометированным и не пригодным для дальнейшего использования. В таком случае необходимо воспользоваться процедурой возврата ПАК «Барьер – USB» к заводским настройкам, а затем заново сформировать ключевую информацию.

Однако, если вскрытие корпуса санкционированное (например, оператором при обслуживании, или имеются другие причины, позволяющие оператору принять решение, что личный ключ КП «БАС-L» не был скомпрометирован), то он может быть восстановлен из контейнеров.

3.6.2.2. Для восстановления личного ключа требуются контейнеры второго частичного секрета основного личного ключа и второго частичного секрета резервного личного ключа (при его наличии). Восстановление личного ключа осуществляется с помощью модуля PrivateKeyRecovery.

3.6.2.3. Для восстановления личного ключа КП «БАС-L» необходимо открыть терминал и выполнить команду «PrivateKeyRecovery» с обязательным параметром «-k», через пробел от которого необходимо указать путь к ключевому контейнеру второго частичного секрета основного личного ключа. Имя ключевого контейнера должно иметь вид: «KeyContainer*_[имя_ключа]*.ssc», где *[имя_ключа]* – это имя, введенное оператором во время выполнения модуля RequestBuilder.

В случае, если восстановление личного ключа прошло успешно, вывод модуля имеет вид:

```
user@user:~$ PrivateKeyRecovery -k /home/user/KeyContainer_basl01-usbbar.ssc
Сброс ПАК "Барьер-USB":
Введите пароль доступа к защищённому хранилищу (8-24 символа): ********
Подтвердите пароль: ********
Операция завершена успешно.
Установка нового пароля защиты ПАК "Барьер-USB":
```

```
Введите пароль доступа к защищённому хранилищу (8-24 символа): ********
Подтвердите пароль: ********
Введите пароль к ключевому контейнеру: ********
Личный ключ восстановлен.
Состояние защиты ПАК "Барьер-USB": защита установлена.
```

3.6.2.4. Через опциональный параметр «-r» можно указать путь к аналогичному файлу ключевого контейнера второго частичного секрета резервного личного ключа (при его наличии).

Если вместе с основным ключом восстанавливается и резервный, то вывод следующий:

```
user@user:~$ PrivateKeyRecovery -k /home/user/KeyContainer_basl01-usbbar.ssc
-r /home/user/KeyContainer_basl01-usbbar2.ssc
Сброс ПАК "Барьер-USB":
Введите пароль доступа к защищённому хранилищу (8-24 символа): ********
Подтвердите пароль: ********
Операция завершена успешно.
Установка нового пароля защиты ПАК "Барьер-USB":
Введите пароль доступа к защищённому хранилищу (8-24 символа): ********
Подтвердите пароль: ********
Введите пароль к ключевому контейнеру: ********
Введите пароль к резервному ключевому контейнеру: ********
Личный ключ восстановлен.
Резервный личный ключ восстановлен.
Состояние защиты ПАК "Барьер-USB": защита установлена.
```

3.6.2.5. В начале работы модуль PrivateKeyRecovery проверяет состояние ПАК «Барьер - USB». Если в ПАК «Барьер – USB» установлена защита, т.е. не было вскрытия корпуса, выведутся следующие сообщения и модуль завершит работу:

```
user@user:~$ PrivateKeyRecovery -k /home/user/KeyContainer_basl01-usbbar.ssc
Состояние ПАК "Барьер-USB":
Защита установлена;
Устройство не готово к работе!
Личный ключ не был восстановлен.
Состояние защиты ПАК "Барьер-USB": защита установлена.
```

3.6.2.6. Для получения справочной информации о модуле PrivateKeyRecovery, необходимо выполнить команду «PrivateKeyRecovery help» или «PrivateKeyRecovery -h»:

```
user@user:~$ PrivateKeyRecovery help
```

3.6.3. Смена ключей

3.6.3.1. Процедура смены ключей в ПАК «Барьер – USB» необходима в том случае, если основная ключевая пара заканчивает свое действие (например, срок действия истекает или истёк). Во время смены ключей очищается защищенное хранилище ПАК «Барьер – USB» и предварительно сформированный резервный личный ключ записывается в основную область защищенного хранилища, т.е. становится основным.

3.6.3.2. Для смены ключей необходимо открыть терминал и выполнить команду «KeysReplacer». Модуль KeysReplacer выполнит сначала контроль целостности и самотестирование КП «БАС-L», а после процедуру смены ключей.

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

```
user@user:~$ KeysReplacer
> 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 20 17:13:24 basctl: Тестирование завершено успешно!
```

3.6.3.4. Далее проверяется состояние ПАК «Барьер – USB». Если защита не была установлена, т.е. в защищенном хранилище нет ни одного личного ключа, оператору выведутся следующие сообщения и модуль KeysReplacer завершит работу:

```
Состояние ПАК "Барьер-USB":
Защита не установлена;
Устройство не готово к работе!
```

Если защита установлена, оператору выведется предупреждение и вопрос о желании продолжить:

```
Выполнение данной программы приведёт к уничтожению текущего личного ключа и установке резервного в качестве основного!
Вы уверены, что хотите продолжить? (Y/N):
```

3.6.3.5. Если оператор соглашается продолжить, то далее предлагается ввести пароль доступа к защищённому хранилищу ПАК «Барьер – USB»:

```
Вы уверены, что хотите продолжить? (Y/N): y
Введите пароль доступа к защищённому хранилищу (8-24 символа): ********
Подтвердите пароль: ********
```

Если же оператор отказывается от продолжения, то выведется следующее сообщение и модуль KeysReplacer завершит работу:

```
Вы уверены, что хотите продолжить? (Y/N): n
Действие отменено пользователем.
```

3.6.3.6. После успешного ввода пароля выполняется процедура смены ключей. Если она завершилась успешно, оператору выведется сообщение:

```
Смена личного ключа выполнена успешно.
```

Если в ПАК «Барьер - USB» отсутствует резервный ключ, оператору выведется следующее сообщение:

```
OnKeysReplace: В устройстве отсутствует резервный личный ключ!
Воспользуйтесь модулем RequestBuilder для генерации резервной ключевой пары.
```

3.6.3.7. После успешной смены ключа, перед использованием новой ключевой пары, необходимо убедиться в корректности настроек VPN-профиля. Скорее всего необходимо указать

путь к новому сертификату с помощью редактирования VPN-профиля (см. п. 3.2.3.). Либо можно создать новый VPN-профиль (см. п. 3.2.2.).

3.6.3.8. Для получения справочной информации о модуле KeysReplacer, необходимо выполнить команду «KeysReplacer help»:

```
user@user:~$ KeysReplacer help
```

3.6.4. Уничтожение ключевой информации

3.6.4.1. Для уничтожения личного ключа, хранящегося в защищенном хранилище ПАК «Барьер – USB», необходимо воспользоваться модулем Uninstaller. Модуль Uninstaller выполняет очистку защищенного хранилища и возврат ПАК «Барьер – USB» к заводским настройкам.

3.6.4.2. Для уничтожения ключевой информации с программно-аппаратной защитой необходимо открыть терминал и выполнить команду «Uninstaller». Оператору выведутся предупреждение и вопрос о желании продолжить:

```
Выполнение данной программы приведёт к откату устройства к заводским настройкам!
Вы уверены, что хотите продолжить? (Y/N):
```

Если оператор согласится («y»), то модуль Uninstaller продолжит работу.

Если оператор откажется («n»), то выведется следующее сообщение и модуль Uninstaller завершит работу:

```
Вы уверены, что хотите продолжить? (Y/N):
n
Отмена.
```

3.6.4.3. Если оператор соглашается продолжить работу, далее модуль Uninstaller проверяет состояние ПАК «Барьер – USB». Если защита установлена, оператору предлагается ввести пароль доступа к защищённому хранилищу и выполняется процедура уничтожения ключевой информации:

```
Вы уверены, что хотите продолжить? (Y/N):
y
Введите пароль доступа к защищённому хранилищу:
********
Подтвердите пароль:
********
Защищённое хранилище успешно очищено!
Очистка завершена! Рекомендуется перезагрузить устройство.
```

Если защита ПАК «Барьер - USB» не установлена, оператору выведутся следующие сообщения и модуль Uninstaller завершит работу:

```
Защита не установлена!
Защищённое хранилище не было очищено!
```

3.6.4.4. Для получения справочной информации о модуле Uninstaller, необходимо выполнить команду «Uninstaller help»:

```
user@user:~$ Uninstaller help
```

3.6.5. Просмотр журнала критических событий

3.6.5.1. Критическим событием считается вскрытие корпуса ПЭВМ, в которой функционирует КП «БАС-L» с ПАК «Барьер – USB». Журнал критических событий КП «БАС-L» содержит записи о вскрытии корпуса.

3.6.5.2. Для просмотра журнал критических событий необходимо открыть терминал и выполнить команду «LogViewer». Модуль LogViewer выполнит контроль состояния ПАК «Барьер – USB» и предоставит время и дату вскрытия корпуса:

```
user@user:~$ LogViewer
Введите пароль доступа к ПАК "Барьер-USB": ********
[22.04.2022 14:34:39] Вскрыт корпус.
```

3.6.5.3 Усли ПАК «Барьер – USB» присутствует, защита установлена, но не произошло критическое событие, будет выведено сообщение об этом:

```
      user@user:~$ LogViewer
Состояние ПАК "Барьер-USB":
Защита установлена;
C_AppMain::Run:Журнал критических событий пуст!
```

3.6.5.4. Если ПАК «Барьер – USB» отсутствует:

```
user@user:~$ LogViewer
Error: Device Opening Failed!
C_AppMain::Run:Ошибка инициализации ПАК "Барьер-USB"
```

4. СООБЩЕНИЯ ОПЕРАТОРУ

КП «БАС-L» не предоставляет специфических сообщений оператору не описанных в данном документе.

Сообщения о результатах работы КП «БАС-L» выводятся в системный журнал (см. п. 3.4.). Сообщения четко описывают причину их появления и не нуждаются в разъяснении.

ПРИЛОЖЕНИЕ А

СПИСОК ОБОЗНАЧЕНИЙ ДОСТУПНЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Таблица А.1 – Список обозначений доступных криптографических алгоритмов

EALG	
belt_cbc	алгоритм шифрования СТБ 34.101.31 в режиме сцепления блоков
belt_cfb	алгоритм шифрования СТБ 34.101.31 в режиме гаммирования с обратной связью
belt_ctr	алгоритм шифрования СТБ 34.101.31 в режиме счётчика
IALG	
belt_mac	алгоритм выработки иммитовставки СТБ 34.101.31
belt_hmac	алгоритм ключезависимого хэширования СТБ 34.101.47
PRF	
prfbrng_ctr	алгоритм выработки псевдослучайных чисел СТБ 34.101.47 в режиме счётчика
prfbrng_hmac	алгоритм выработки псевдослучайных чисел СТБ 34.101.47 в режиме HMAC
DHGROUP	
ecp256bign	Алгоритм Диффи-Хеллмана в соответствии с СТБ 34.101.66 Приложение А.
KEYREP	
keyrep	алгоритм преобразования ключа СТБ 34.101.31
Примечания: – жирным выделены алгоритмы, используемые по умолчанию; – курсивом выделены первые поддерживаемые значения.	

ПРИЛОЖЕНИЕ Б

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе приняты следующие сокращения:

ОС – операционная система

ОЗУ – оперативное запоминающее устройство

ПО – программное обеспечение

СОК – сертификат открытого ключа

СОС – список отозванных сертификатов

УЦ – Удостоверяющий центр

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопрово- дительного докум. и дата	Подп.	Дата
	изменен- ных	заменен- ных	новых	аннули- рованных					