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 Android, к защищенной подсети с аутентификацией по протоколу BSTS

СЮИК.465634.001 ИС52

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 мобильных устройств «БАС-А» BY.СЮИК.00441-01 (далее – КП «БАС-А»), предназначенный для организации защищенного VPN-подключения устройства, работающего под управлением ОС Android, к ПАК «БАС».

Настоящая инструкция является расширением Руководства по эксплуатации ПАК «БАС» СЮИК.465634.001 РЭ и Руководства оператора КП «БАС-А» BY.СЮИК.00441-01 34 01 и предназначена для облегчения работы администратора при создании типовой схемы подключения КП «БАС-А» к ПАК «БАС» для построения защищенного соединения.

Настоящая инструкция предназначена для администратора, имеющего навыки работы с ОС Linux и ОС Android, 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-А» администратор должен ознакомиться с документом «Комплекс программный криптографической защиты информации мобильных устройств «БАС-А». Руководство оператора» BY.СЮИК.00441-01 34 01 прежде, чем преступить к настройкам согласно данной инструкции.

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

1 Описание соединения (стенда)

Схема подключения мобильного устройства, работающего под управлением ОС Android, с установленным КП «БАС-А» 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-А» на мобильное устройство, работающее под управлением ОС Android проводится в соответствии с Руководство оператора» BY.СЮИК.00441-01 34 01.

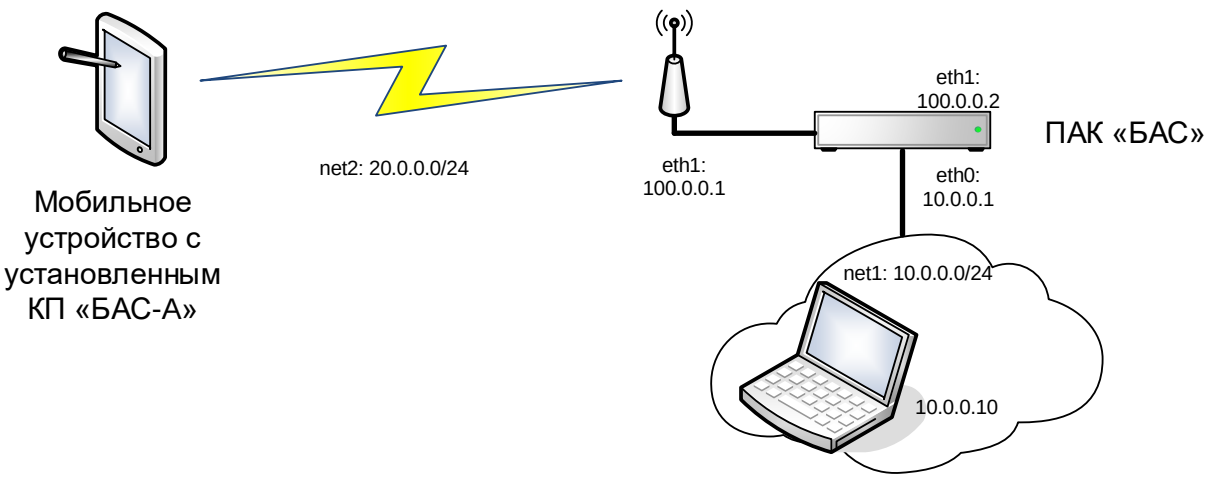


Рисунок 1 – Схема стенда

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-А».

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-А» 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-А»

При настройке КП «БАС-А» будем исходить из того, что значение времени и даты, а также сетевые настройки получены мобильным устройством от оператора связи.

После запуска КП «БАС-А» отображается главное окно (Рисунок 1), в котором расположены следующие элементы:

1 – кнопка добавления профиля;

2 – кнопка вызова меню;

3 – панель статуса подключения;

4 – список настроенных профилей.

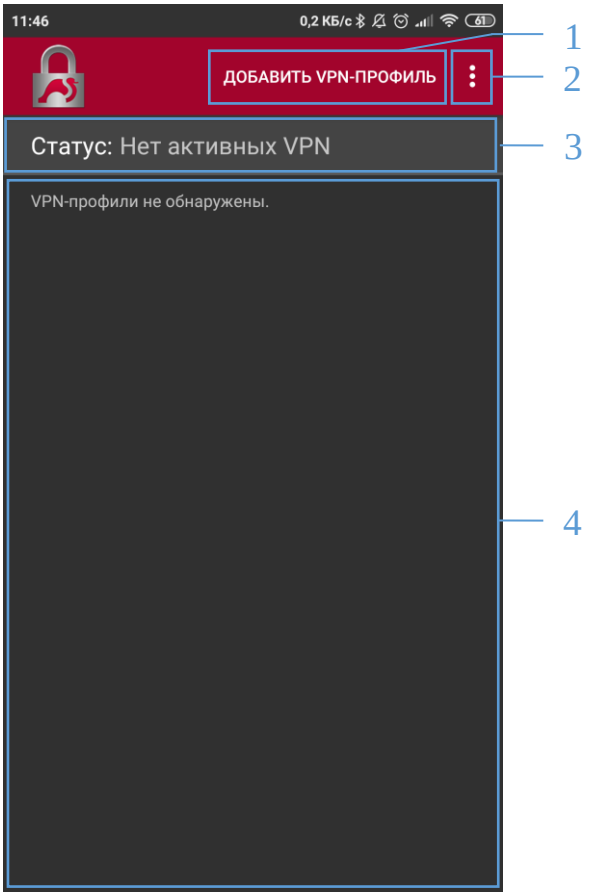


Рисунок 1

2.3.1 Формирование запроса на выпуск сертификата

В КП «БАС-А» есть возможность сгенерировать ключевую пару для аутентификации, сформировать контейнер защищенного личного ключа и запрос на получение сертификата. Для этого необходимо в главном окне нажать кнопку вызова меню и выбрать пункт «Запрос на получение сертификата» (Рисунок 2).

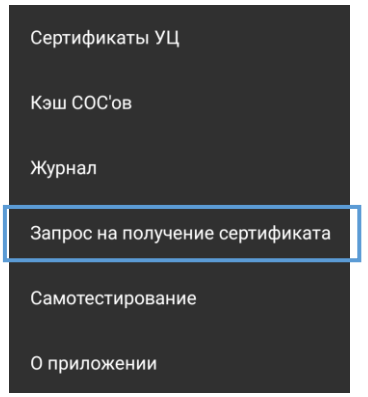


Рисунок 2

Откроется окно, отображенное на Рисунке 3.

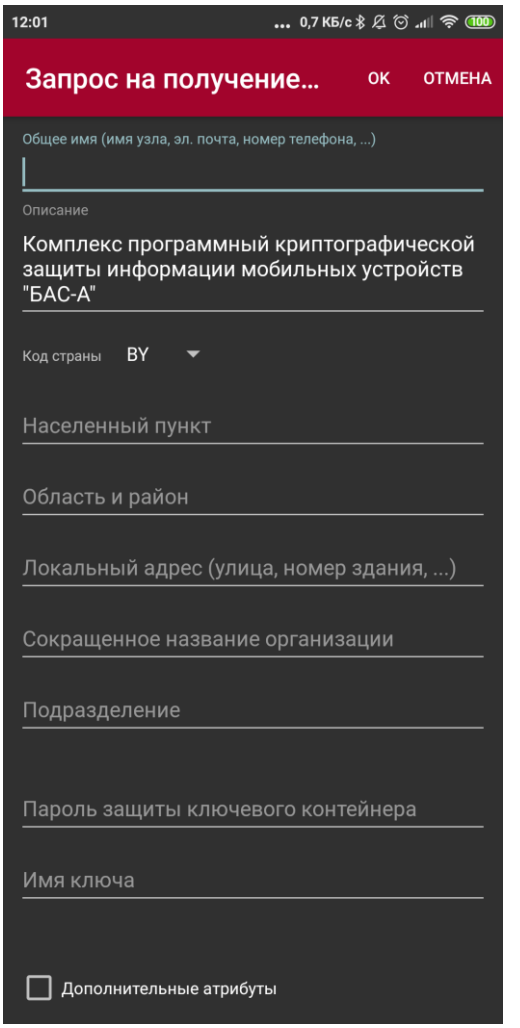
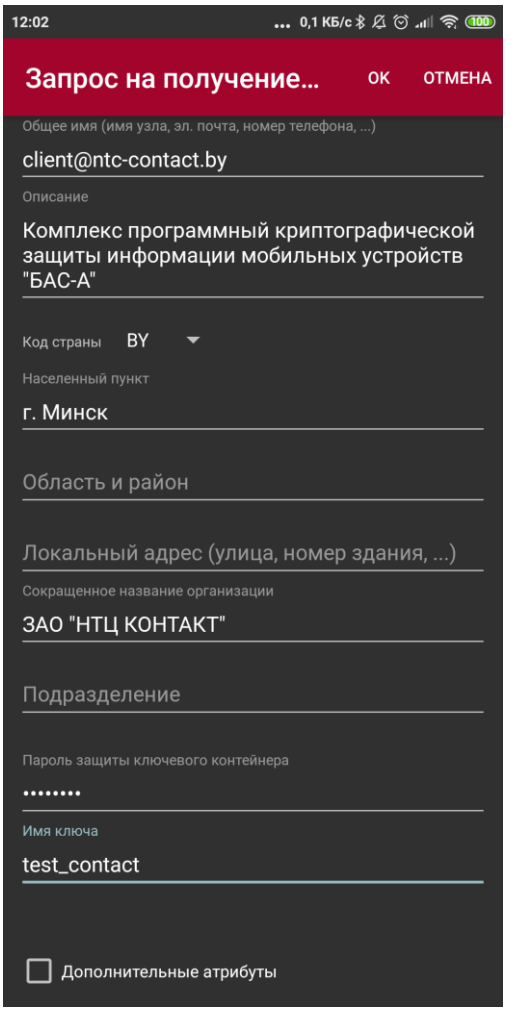


Рисунок 3

Необходимо заполнить поля. Обязательными являются «Общее имя», «Населенный пункт», «Сокращенное название организации», «Пароль защиты ключевого контейнера» и «Имя ключа». Пример заполнения полей представлен на Рисунке 4.



Рисунке 4

Значение поля «Имя ключа» будет частью названия файлов ключевых контейнеров и запроса на получение сертификата, а в сам запрос эта информация не будет включена. Имя ключа должно быть уникальным.

В нижней части окна есть галочка «Дополнительные атрибуты». Если ее выбрать, отобразятся дополнительные поля (Рисунок 5).

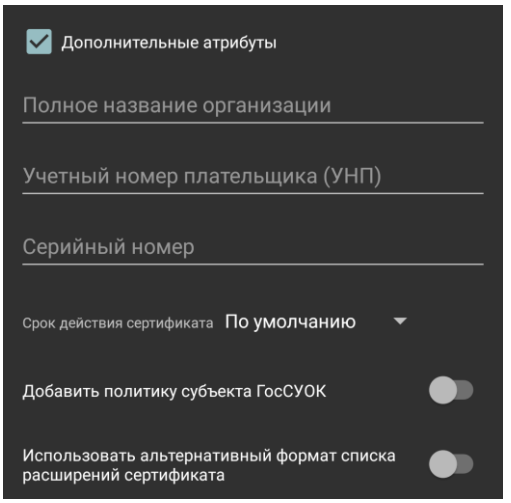


Рисунок 5

Дополнительные атрибуты могут понадобиться для специфических требований Удостоверяющего центра, который будет выпускать сертификат. Так, например, для Удостоверяющего центра ГосСУОК необходимо установить переключатель «Добавить политику субъекта ГосСУОК».

Для продолжения формирования ключевых контейнеров и запроса после заполнения полей необходимо нажать на кнопку «ОК» в верхнем правом углу окна. Если какие-то из обязательных полей не будут заполнены или заполнены некорректно, то сообщения от этом отобразятся в виде подсказки под полем.

Если поля корректно заполнены, после нажатия на кнопку «ОК» откроется окно «Генерация ключевой пары». В нем необходимо поводить пальцем по экрану для накопления случайности для инициализации криптографического генератора псевдослучайных чисел. По мере накопления случайности будет заполняться индикатор (Рисунок 6).

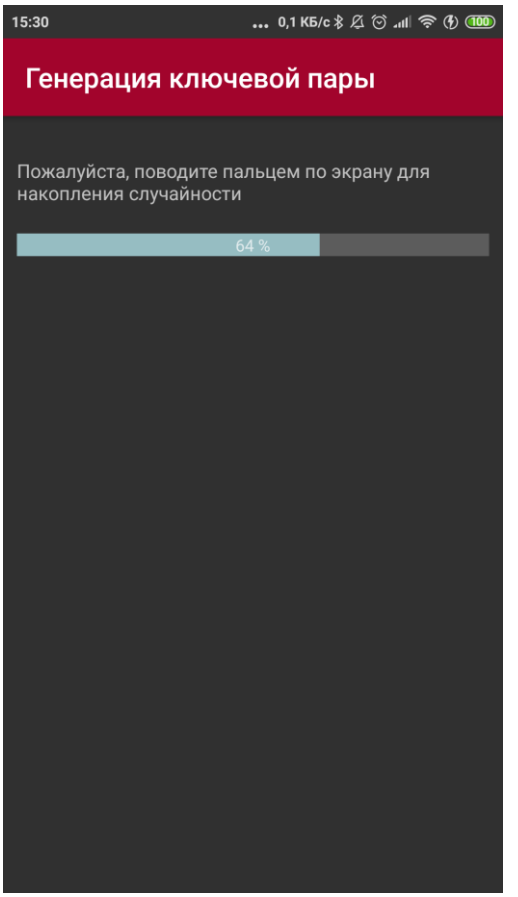


Рисунок 6

В случае успеха в директория «strongSwanCont» будут сформированы Запрос на выпуск сертификата с именем *CertReq_[имя_ключа].der* и Защищенный контейнер с ключевым секретом с именем *KeyContainer_[имя_ключа].ssc* и будет сформировано сообщение с предложением отправить запрос в УЦ (Рисунок 7).

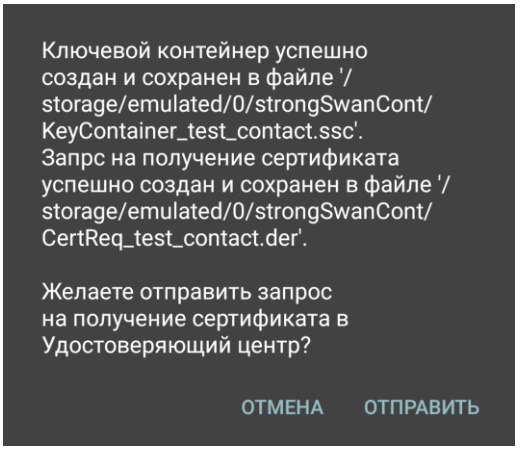


Рисунок 7

Если нажать кнопку «Отправить», откроется окно с выбором доступного приложения для отправки файла запроса (например, как на Рисунке 8).

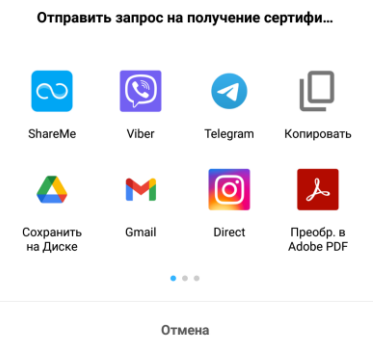


Рисунок 8

2.3.2 Импорт сертификатов УЦ

После получения СОК от УЦ, они (Сертификат КП «БАС-А» и корневые Сертификаты УЦ) они должны быть помещены в файловую систему мобильного устройства. Рекомендуется использовать директорию «strongSwanCont».

Корневые Сертификаты УЦ необходимо импортировать в КП «БАС-А» для использования в качестве доверенных.

Для просмотра списка доверенных сертификатов УЦ необходимо в главном окне нажать кнопку вызова меню и выбрать пункт «Сертификаты УЦ» (Рисунок 9).

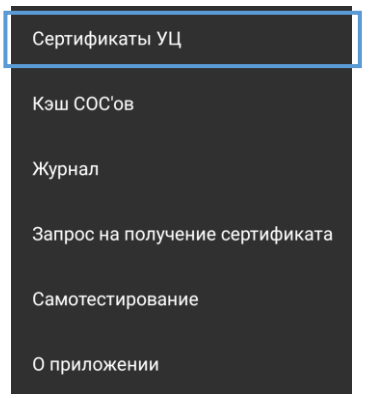


Рисунок 9

После этого откроется окно «Сертификаты УЦ», в котором расположены три вкладки: «Система», «Пользователь» и «Импорт» (Рисунок 10).

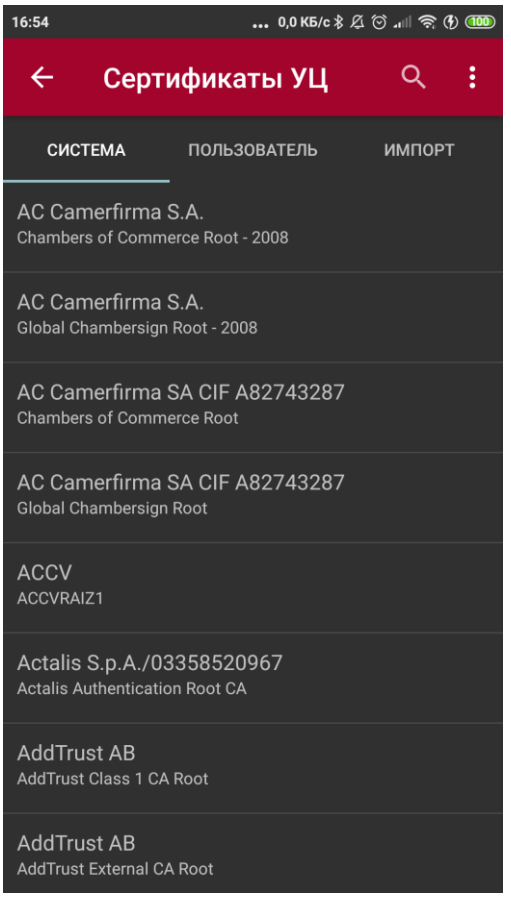


Рисунок 10

Вкладка «Система» содержит список системных доверенных сертификатов.

Вкладка «Пользователь» содержит список сертификатов УЦ, которые пользователь устройства добавил в качестве доверенных через меню системных настроек.

Вкладка «Импорт» содержит список сертификатов УЦ, которые оператор КП «БАС-А» импортировал с помощью функции импорта сертификатов УЦ.

Для импорта сертификата УЦ необходимо в окне «Сертификаты УЦ» нажать кнопку вызова меню и выбрать пункт «Импортировать сертификат» (Рисунок 11).

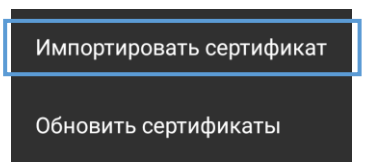


Рисунок 11

После этого откроется системное окно выбора файла, в котором необходимо выбрать файл сертификата УЦ.

После выбора файла сертификата в случае успешного разбора сертификата отобразится окно с подтверждением импорта (Рисунок 12). В сообщении указывается описание субъекта (владельца) сертификата УЦ. После нажатия на кнопку «Импортировать сертификат» поверх окна «Сертификаты УЦ» появится всплывающее уведомление с текстом: «Сертификат успешно импортирован», а в список сертификатов УЦ на вкладке «Импорт» добавится импортированный сертификат (Рисунок 13).

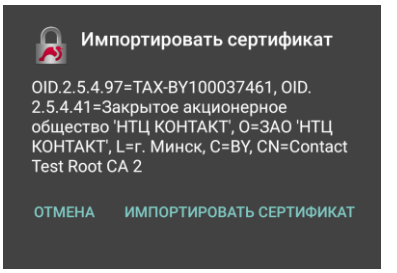


Рисунок 12

Рисунок 13

Данную процедуру необходимо повторить для всех Сертификатов УЦ.

2.3.3 Создание VPN-профиля

Для создания VPN-профиля необходимо в главном окне нажать кнопку «Добавить VPN-профиль» (Рисунок 14).

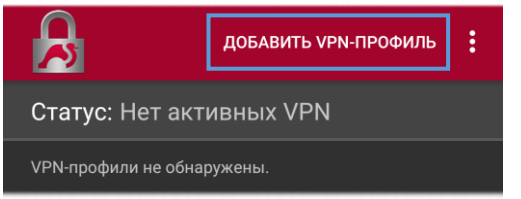


Рисунок 14

Набор основных характеристик профиля изменяется в зависимости от выбранного типа VPN. Выберите «**IKEv2 EAP-BSTS (Сертификат)**» – аутентификация EAP протоколом BSTS в соответствии с СТБ 34.101.66, п. 7.5.

Окно добавления профиля с аутентификацией протоколом BSTS представлено на Рисунке 15.

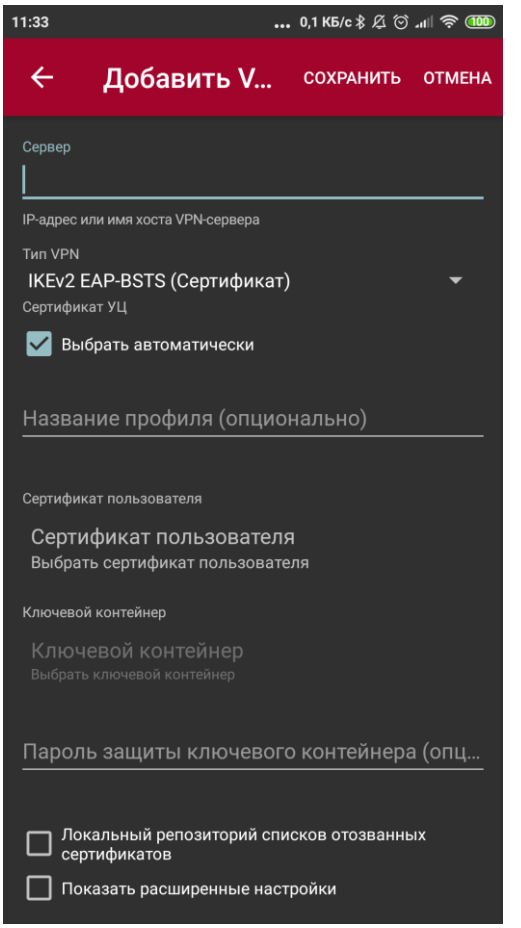


Рисунок 15

Будут доступны следующие основные поля для настройки:

– поле «Сервер», обязательное для заполнения. Должно содержать IP-адрес и/имя хоста VPN-сервера;

– область «Сертификат УЦ». Позволяет указать сертификат УЦ, которым должен быть выпущен сертификат сервера. По умолчанию область содержит отмеченную галочку «Выбрать автоматически». Это означает, что во время подключения программа переберет все доступные доверенные сертификаты УЦ на устройстве. Если галочку «Выбрать автоматически» снять, появится возможность выбора конкретного сертификата УЦ.

Выбор конкретного сертификата УЦ сократит время перебора сертификатов УЦ до одного, что ускорит аутентификацию и установку защищенного соединения.

Если нажать на «Выбрать сертификат УЦ», то откроется окно «Сертификаты УЦ» (Рисунок 10), в котором на вкладке «Импорт» необходимо выбрать сертификат УЦ. Если пользователь выберет сертификат, то в области «Сертификат УЦ» отобразятся два поля из выбранного сертификата: «Название организации» и «Общее имя»;

– поле «Название профиля», необязательное для заполнения. Название будет отображаться в главном окне в списке профилей. Если название не будет задано, по умолчанию названием профиля будет установлено значение, указанное в поле «Сервер»;

– область «Сертификат пользователя». В области необходимо нажать на «Выбрать сертификат пользователя» и в открывшемся окне выбрать файл сертификата пользователя. После чего в области «Сертификат пользователя» отобразятся два поля из выбранного сертификата: «Общее имя» и «Название организации» (Рисунок 16);

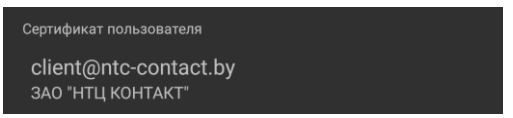


Рисунок 16

– область «Ключевой контейнер». В области необходимо нажать на «Выбрать ключевой контейнер» и в открывшемся окне выбрать файл защищенного контейнера с ключевым секретом. Имя файла должно соответствовать шаблону «*KeyContainer_[имя_ключа].ssc*», где *[имя_ключа]* – это введенное пользователем значение поля «Имя ключа» в окне «Запрос на получение сертификата» при формировании запроса. После выбора в области «Ключевой контейнер» отобразится путь к выбранному файлу (Рисунок 17);

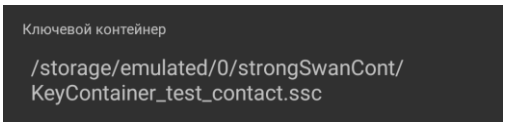


Рисунок 17

– поле «Пароль защиты ключевого контейнера», необязательное для заполнения. Может содержать пароль для снятия защиты с контейнера. Если поле оставить пустым, то программа запросит пароль непосредственно во время подключения;

– параметр «Локальный репозиторий списков отозванных сертификатов». По умолчанию репозиторий не задан. Для того, чтобы установить репозиторий необходимо установить галочку «Локальный репозиторий списков отозванных сертификатов» и в появившейся ниже области нажать на «Выбрать репозиторий списков отозванных сертификатов». После этого откроется окно выбора файла, в котором необходимо выбрать файл списка отозванных сертификатов. Директория, из которой был выбран файл, и станет локальным репозиторием. Путь к этой директории отобразится в области под параметром «Локальный репозиторий списков отозванных сертификатов» (Рисунок 18).

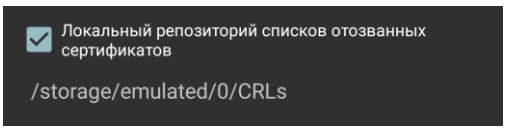


Рисунок 18

Пример заполнения основных полей профиля с аутентификацией протоколом BSTS представлен на рисунке 19.

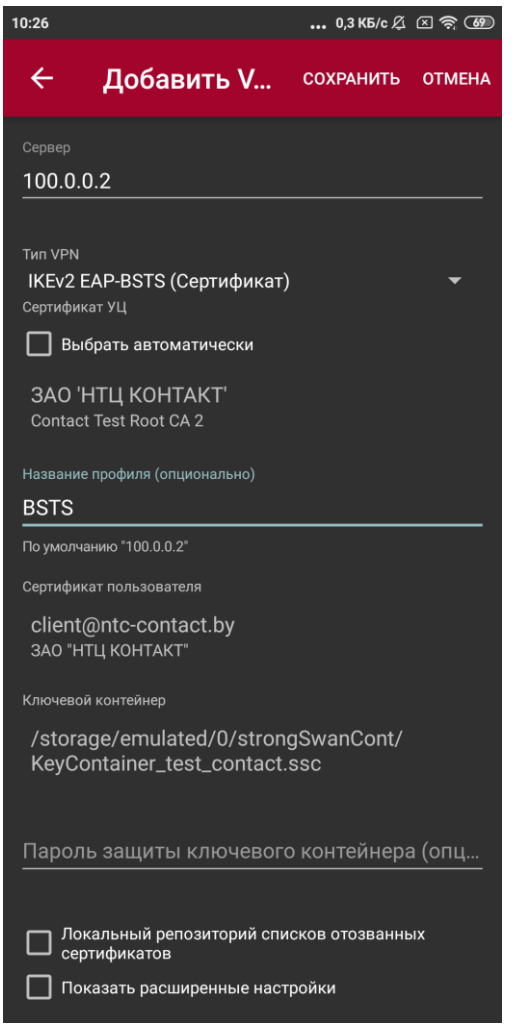


Рисунок 19

Для установки расширенных параметров необходимо установить галочку «Показать расширенные настройки» (Рисунок 20).

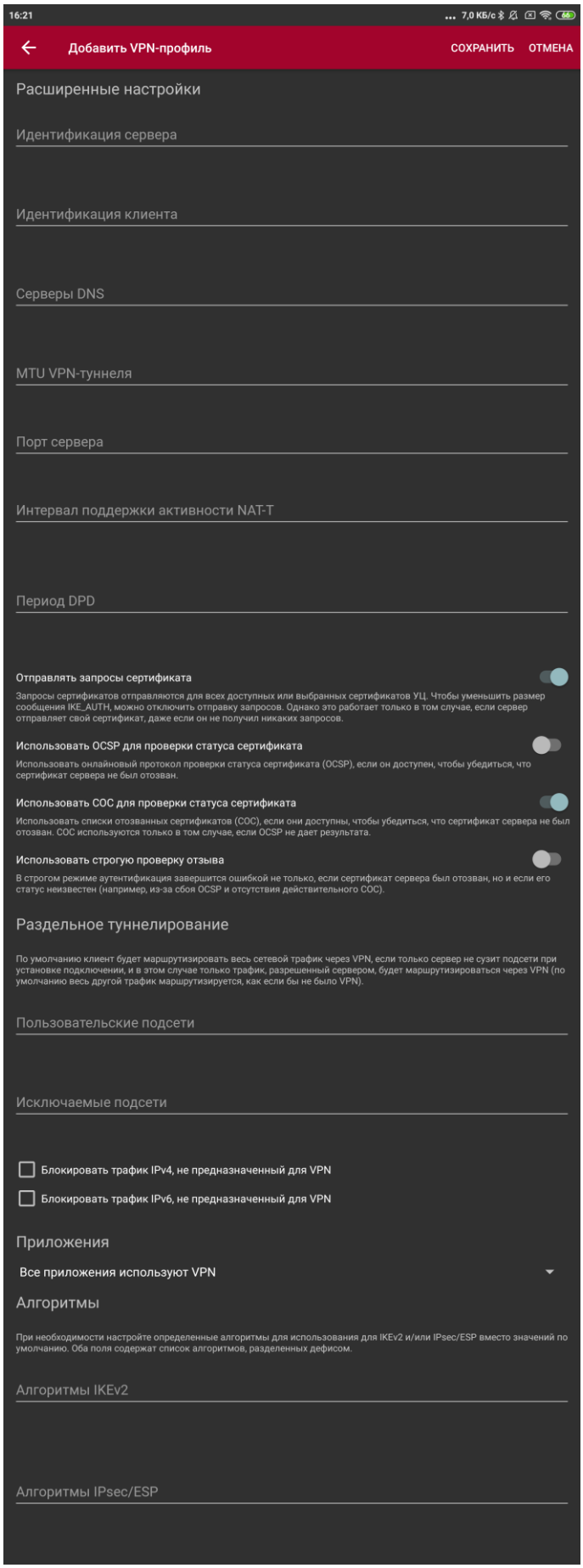

16:21
7,0 КБ/с
Добавить VPN-профиль
СОХРАНИТЬ
ОТМЕНА
Расширенные настройки
Идентификация сервера
Идентификация клиента
Серверы DNS
MTU VPN-туннеля
Порт сервера
Интервал поддержки активности NAT-T
Период DPD
Отправлять запросы сертификата
Запросы сертификатов отправляются для всех доступных или выбранных сертификатов УЦ. Чтобы уменьшить размер сообщения IKE_AUTH, можно отключить отправку запросов. Однако это работает только в том случае, если сервер отправляет свой сертификат, даже если он не получил никаких запросов.
Использовать OCSP для проверки статуса сертификата
Использовать онлайновый протокол проверки статуса сертификата (OCSP), если он доступен, чтобы убедиться, что сертификат сервера не был отозван.
Использовать CDC для проверки статуса сертификата
Использовать списки отозванных сертификатов (CDC), если они доступны, чтобы убедиться, что сертификат сервера не был отозван. CDC используются только в том случае, если OCSP не дает результата.
Использовать строгую проверку отзыва
В строгом режиме аутентификация завершится ошибкой не только, если сертификат сервера был отозван, но и если его статус неизвестен (например, из-за сбоя OCSP и отсутствия действительного CDC).
Раздельное туннелирование
По умолчанию клиент будет маршрутизировать весь сетевой трафик через VPN, если только сервер не сузит подсети при установке подключении, и в этом случае только трафик, разрешенный сервером, будет маршрутизироваться через VPN (по умолчанию весь другой трафик маршрутизируется, как если бы не было VPN).
Пользовательские подсети
Исключаемые подсети
Блокировать трафик IPv4, не предназначенный для VPN
Блокировать трафик IPv6, не предназначенный для VPN
Приложения
Все приложения используют VPN
Алгоритмы
При необходимости настройте определенные алгоритмы для использования для IKEv2 и/или IPsec/ESP вместо значений по умолчанию. Оба поля содержат список алгоритмов, разделенных дефисом.
Алгоритмы IKEv2
Алгоритмы IPsec/ESP

Рисунок 20

Большинство расширенных параметров содержат подробное описание. Оно отображается при нажатии на поле параметра (например, рисунок 21).

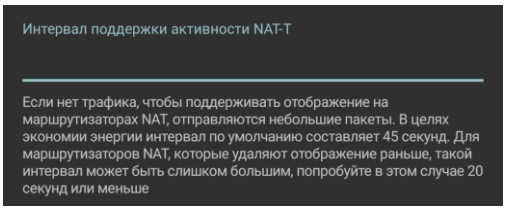


Рисунок 21

В расширенных настройках можно указать раздельное туннелирование (секция «Раздельное туннелирование»). По умолчанию весь сетевой трафик будет маршрутизироваться через VPN. Можно указать конкретные подсети, которые будут маршрутизироваться через VPN, а остальной трафик нет. Либо, наоборот, указать те подсети, которые не нужно маршрутизировать через VPN, а весь остальной трафик пройдет через VPN.

Также можно заблокировать трафик, не предназначенный для VPN, установив соответствующие галочки для трафика IPv4 и IPv6. Это позволит повысить безопасность устройства.

Также можно указать приложения, которые будут (или не будут) использовать VPN (секция «Приложения»). Есть три варианта настройки:

– все приложения используют VPN;

– исключить выбранные приложения из VPN;

– только выбранные приложения используют VPN.

Для сохранения параметров профиля необходимо в верхнем правом углу окна нажать кнопку «Сохранить».

В случае корректности заполненных полей окно «Добавить VPN-профиль» закроется, а в главном окне в списке профилей появится запись сохраненного профиля (Рисунок 22).

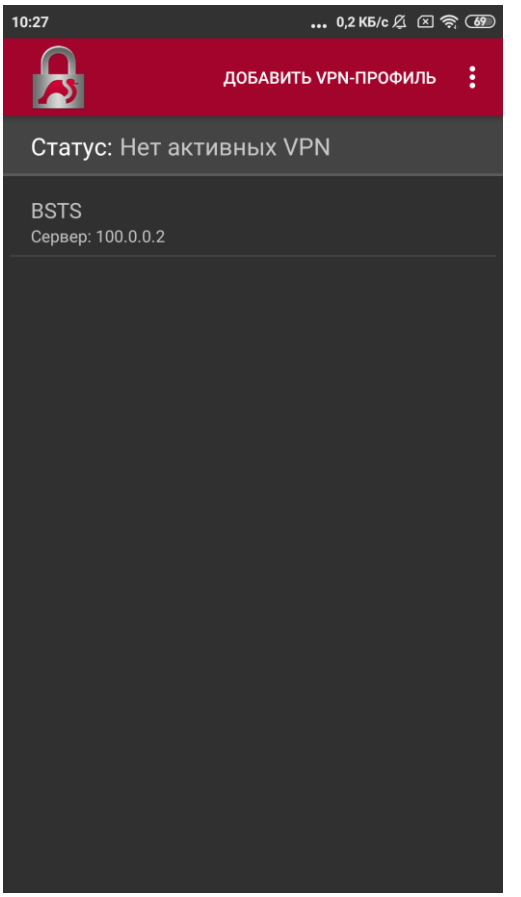


Рисунок 22

2.3.4 Установка подключения к VPN-серверу

Для того чтобы установить подключение к VPN-серверу необходимо в главном окне в списке сохраненных профилей нажать на запись с нужным профилем.

При первом подключении КП «БАС-А» запросит разрешение на подключение к сети VPN (Рисунок 23).

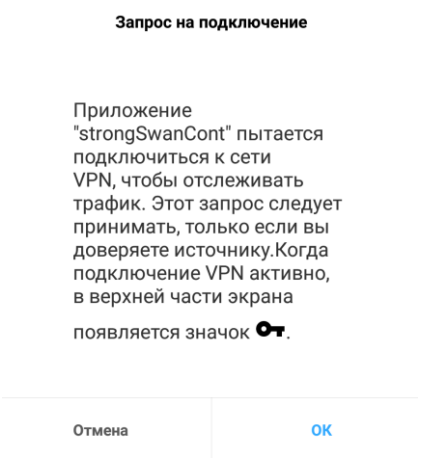


Рисунок 23

Далее отобразится диалоговое окно (Рисунок 24) с сообщением о внесении КП «БАС-А» в белый список устройства (список приложений, которые игнорируют оптимизацию батареи). После нажатия на кнопку ОК, КП «БАС-А» запросит разрешение на внесение приложения в белый список (Рисунок 25).

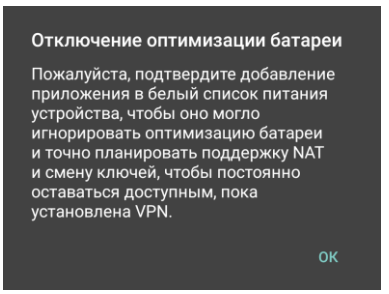


Рисунок 24

Рисунок 25

Во время подключения на панели статуса отображается статус «Подключение…», имя подключаемого профиля и индикатор процесса подключения (Рисунок 26).

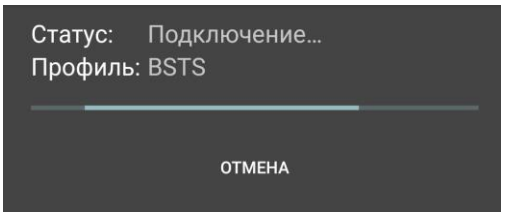


Рисунок 26

После успешно подключения в VPN-серверу на панели статуса отобразится статус «Подключен» (Рисунок 27).

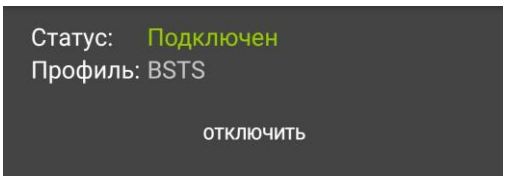


Рисунок 27

3 Проверка работоспособности

Для проверки работоспособности соединения (стенда) необходимо с мобильного устройства обратиться к ПК из защищенной подсети. Для этого можно воспользоваться приложением Ping.

При помощи приложения Ping выполните команду ping 10.0.0.10 и убедитесь в получении ответа.

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]...20.0.0.2[CN=client@ntc-contact.by, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс программный криптографической защиты информации мобильных устройств "БАС-А"]
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 === 50.0.0.1/32**, по туннелю было передано по 3 пакета в каждую сторону), защищенных при помощи алгоритмов **BELT_CFB_256/BELT_MAC**.