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 Windows, к защищенной подсети с аутентификацией по протоколу EAP-TLS

СЮИК.465634.001 ИС55

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

Содержание

Настоящая инструкция распространяется на «Комплекс программно-аппаратный криптографической защиты информации «БАС» СЮИК.465634.001 (далее – ПАК «БАС»), предназначенный для защиты информации, циркулирующей в каналах передачи данных, а также на «Комплекс программный криптографической защиты информации устройств под управлением ОС Windows «БАС-W» BY.СЮИК.00464-01 (далее – КП «БАС-W»), предназначенный для организации защищенного VPN-подключения устройства, работающего под управлением ОС Windows, к ПАК «БАС».

Настоящая инструкция является расширением Руководства по эксплуатации ПАК «БАС» СЮИК.465634.001 РЭ и Руководства оператора КП «БАС-W» BY.СЮИК.00464-01 34 01 и предназначена для облегчения работы администратора при создании типовой схемы подключения КП «БАС-W» к ПАК «БАС» для построения защищенного соединения.

Настоящая инструкция предназначена для администратора, имеющего навыки работы с ОС Linux и ОС Windows, 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-W» администратор должен ознакомиться с документом «Комплекс программный криптографической защиты информации устройств под управлением ОС Windows «БАС-W». Руководство оператора» BY.СЮИК.00464-01 34 01 прежде, чем преступить к настройкам согласно данной инструкции.

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

1 Описание соединения (стенда)

Схема подключения устройства, работающего под управлением ОС Windows (для создания стенда использовалась ОС Windows 10), с установленным КП «БАС-W» к защищаемой при помощи ПАК «БАС» подсети приведена на рисунке 1.

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

В данном сценарии для создания защищенного соединения будут использованы протоколы IKE (Internet Key Exchange) версии 2 с использованием расширенного протокола аутентификации EAP (Extensible Authentication Protocol), схема которого определена в СТБ 34.101.66-2014 п. 7.6 (EAP-BPACE).

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-W» на устройство, работающее под управлением ОС Windows проводится в соответствии с Руководство оператора» BY.СЮИК.00464-01 34 01.

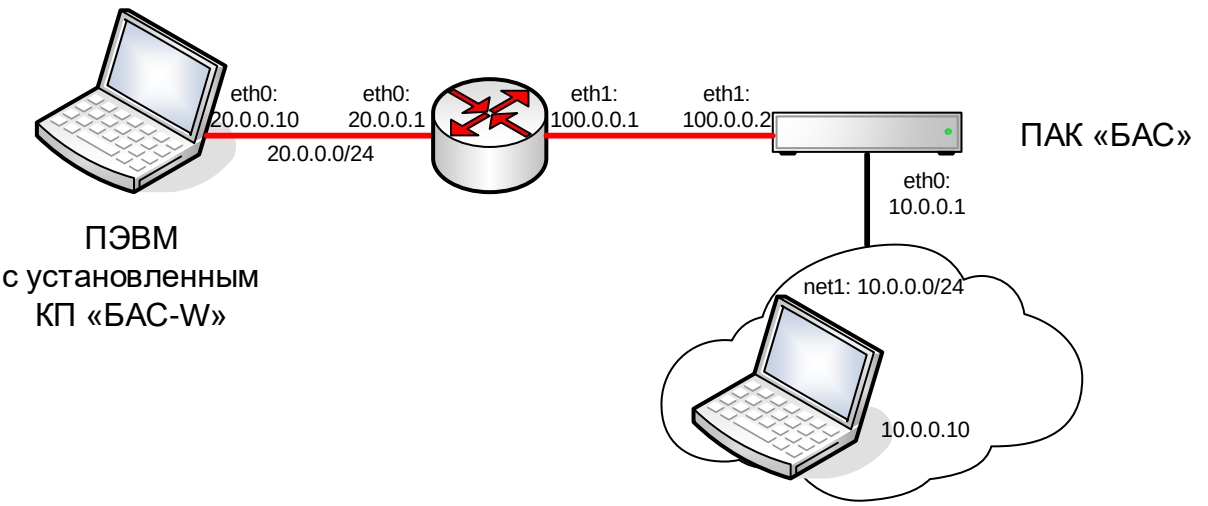

Рисунок 1 – Схема стенда

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-W».

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-W» 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-bpace
        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-W» 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-bpace. 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-BPACE.

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

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

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

```
Идентификатор : Тип_аутентификации «Пароль»
```

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

В качестве типа аутентификации необходимо использовать значение EAP.

В качестве пароля необходимо использовать длинные случайные последовательности.

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

Client1 : EAP “Password for Client1”
Client2 : EAP “Password for Client2”
ClientN : EAP “Password for ClientN”
```

Запустите (перезапустите) IPsec соединение

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

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

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

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

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

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-W»

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

КП «БАС-W» работает в системном трее панели задач ОС Windows (рисунок 2).

Рисунок 2 – Запущенный КП «БАС-W»

Обращение за функциями КП «БАС-W» осуществляется через контекстное меню (рисунок 3), которое вызывается кликом правой клавиши мыши по иконке в системном трее.

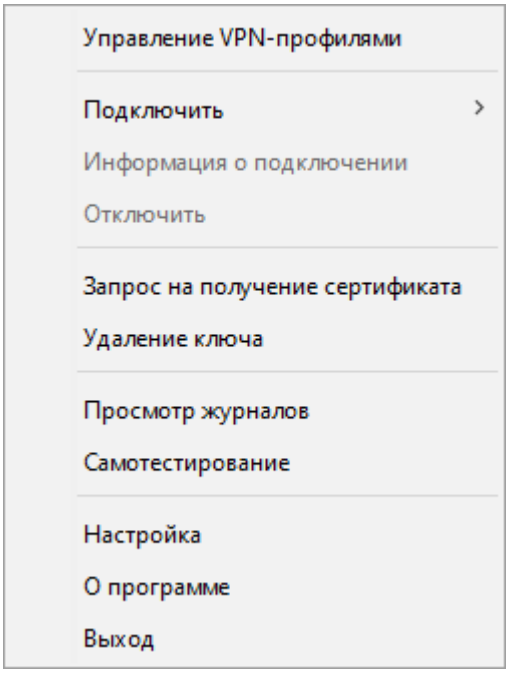

Рисунок 3 – Контекстное меню КП «БАС-W»

КП «БАС-W» поддерживает три языка интерфейса: английский, белорусский и русский. Язык интерфейса устанавливается автоматически в зависимости от языка интерфейса ОС Windows. Настоящий документ описывает работу КП «БАС-W» с использованием русского языка.

2.3.1 Импорт сертификатов УЦ

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

После первого запуска КП «БАС-W» создает свою папку с именем «BAS-W» в папке пользователя ОС (обычно C:\Users\<UserName>\).

Стандартными средствами ОС создадим в папке «BAS-W» папку «CA» и поместим в нее корневые Сертификаты УЦ, выпустивших СОК Сервера.

Стандартными средствами ОС создадим в папке «BAS-W» папку «CRL» и поместим в нее действующий список отозванных сертификатов.

2.3.2 Создание VPN-профиля

Для управления VPN-профилями необходимо в контекстном меню выбрать пункт «Управление VPN-профилями», после чего отобразится окно, представленное на рисунке 4.

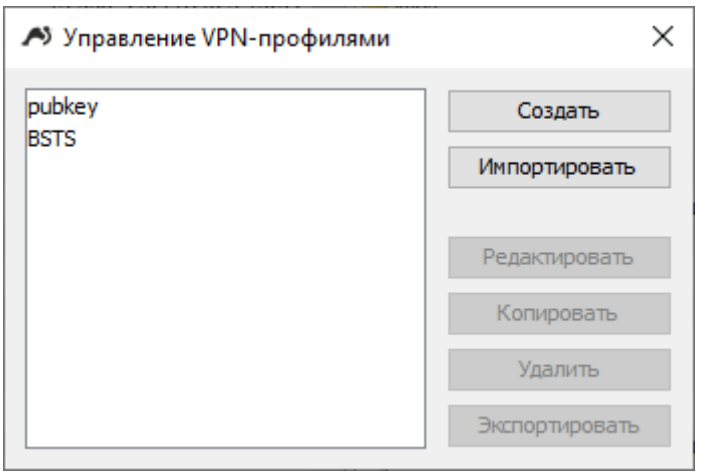

Рисунок 4 – Управление VPN-профилями

В окне «Управление VPN-профилями» расположена область со списком уже существующих VPN-профилей и кнопки для управления. С помощью этого окна можно создавать и импортировать новые VPN-профили, а также редактировать, копировать, удалять и экспортировать уже существующие VPN-профили.

Для создания нового VPN-профиля в окне «Управление VPN-профилями» необходимо нажать кнопку «Создать». Откроется окно «Создание VPN-профиля» (рисунок 5).

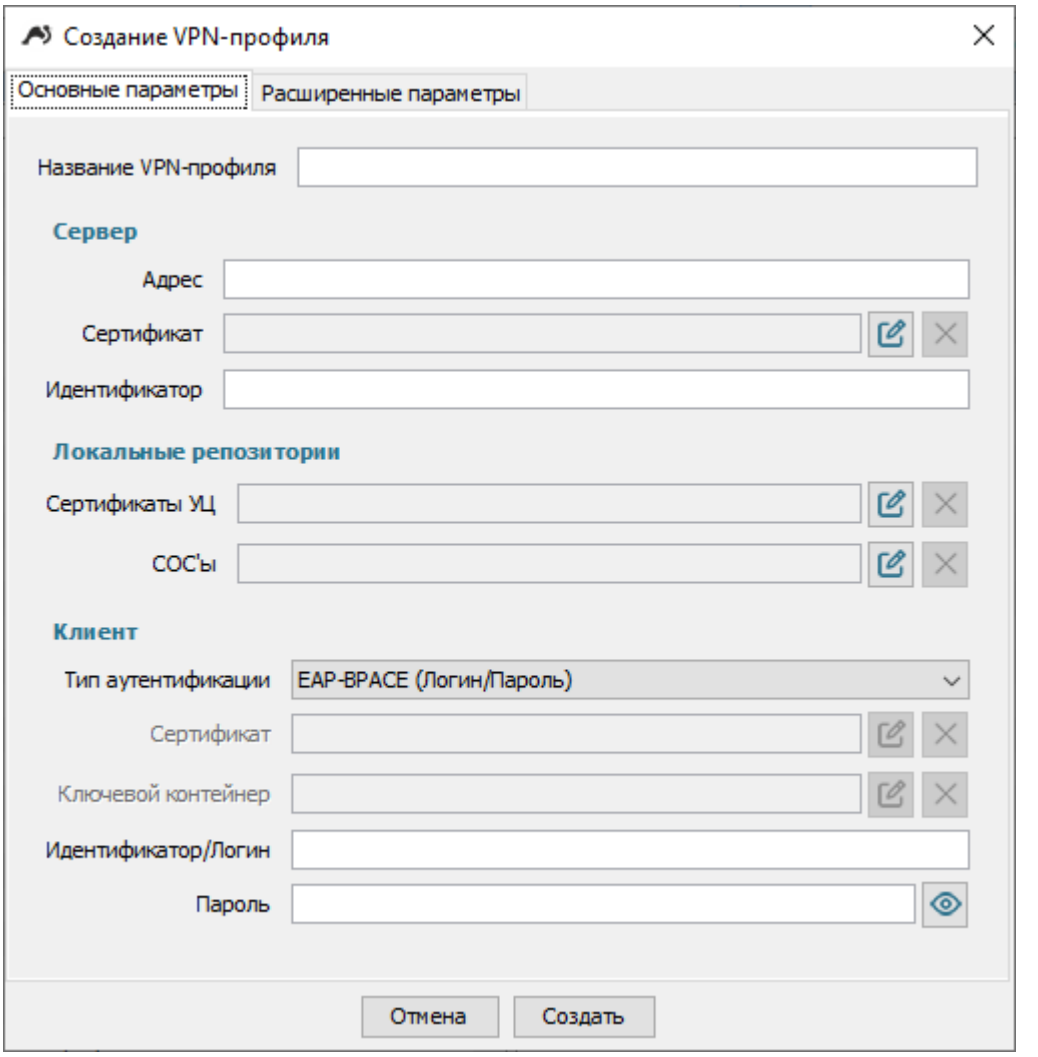

Рисунок 5 – Создание VPN-профиля

Для создания VPN-профиля необходимо заполнить вкладку «Основные параметры» (рисунок 6).

По умолчанию КП «БАС-W» использует «**строгую проверку статуса сертификата**». Это означает, что аутентификация завершится ошибкой не только,

если сертификат сервера был отозван, но и если его статус не удалось установить (например, из-за сбоя OCSP и отсутствия действительного COC).

Если политика организации не требует использования «строгой проверки статуса сертификата», то можно использовать «нестрогую проверку статуса сертификата». Для этого необходимо перейти на вкладку «Расширенные параметры» и снять галочку «Строгая проверка статуса сертификата».

Снятая галочка «Строгая проверка статуса сертификата» означает, что в случае, когда не удалось установить статус сертификата сервера, он считается действительным.

ВНИМАНИЕ: Снимая галочку «Строгая проверка статуса сертификата», Пользователь подтверждает, что он осознает, что его действие может привести к снижению безопасности подключения.

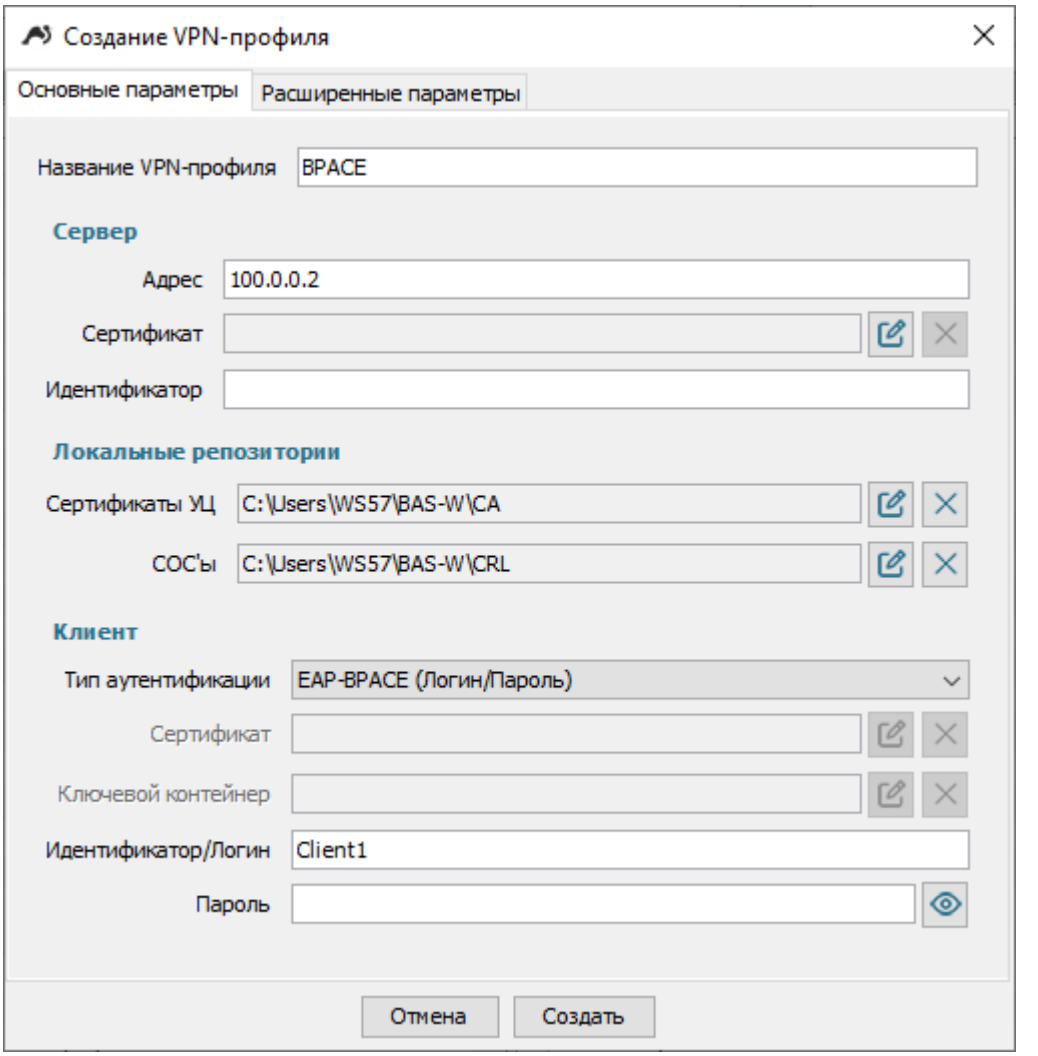

Рисунок 6 – Настроенный VPN-профиль

После заполнения всех параметров необходимо нажать кнопку «Создать» внизу окна создания VPN-профиля.

После нажатия на кнопку «Создать» окно создания VPN-профиля закроется и станет активным ранее открытое окно управления VPN-профилями.

В списке VPN-профилей отобразится созданный VPN-профиль (рисунок 7).

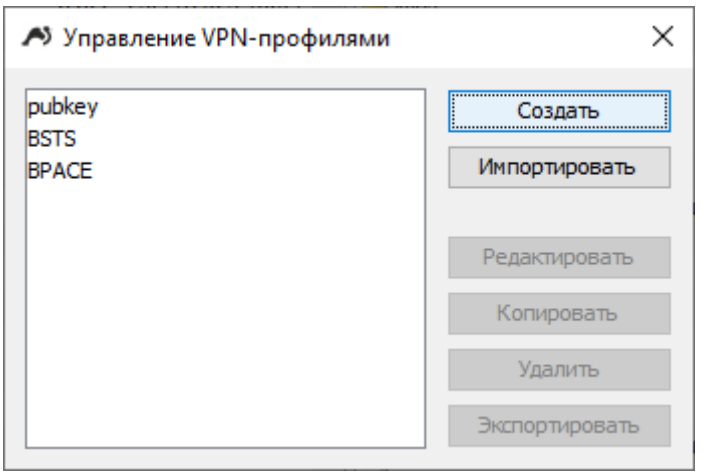

Рисунок 7 – Окно «Управление VPN-профилями» с созданными VPN-профилями

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

Можно создать любое количество VPN-профилей. Все они будут отображаться в виде списка в окне управления VPN-профилями.

2.3.3 Установка подключения к VPN-серверу

Для подключения к VPN-серверу необходимо закрыть окно «Управление VPN-профилями» (если открыто), и вызвать контекстное меню КП «БАС-W», навести курсор мыши на пункт «Подключить» и в появившемся списке подменю выбрать нужный VPN-профиль (рисунок 8).

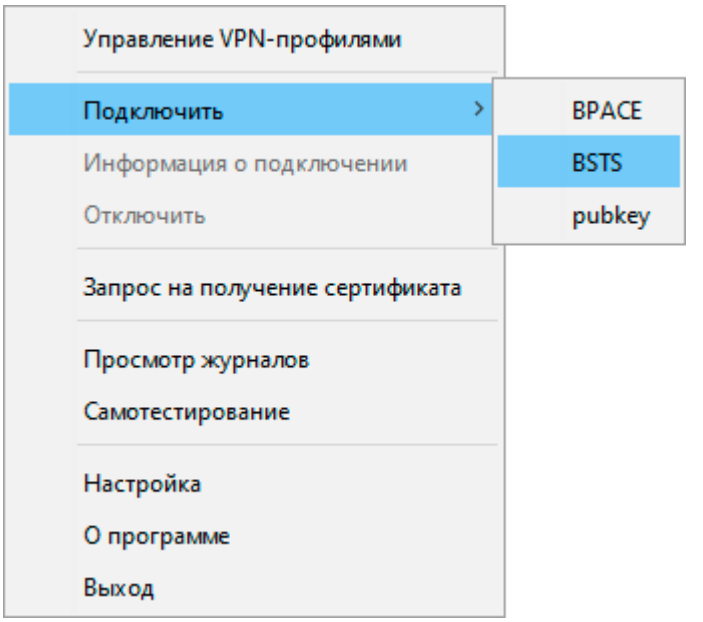

Рисунок 8 – Выбор VPN-профиля для подключения

Если при создании VPN-профиля не был указан пароль аутентификации, то перед подключением он запрашивается с помощью окна с полем для ввода (рисунок 9).

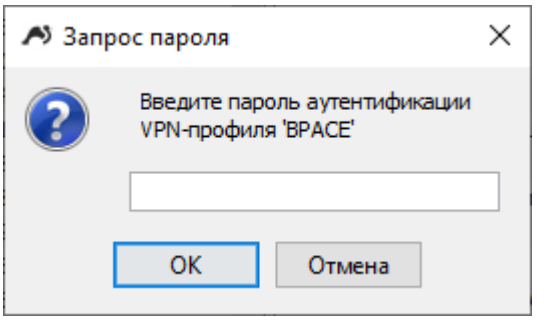

Рисунок 9 – Запрос пароля для подключения по протоколу BPACE

При выполнении подключение VPN-профиля иконка КП «БАС-W» в системном трее меняет цвет фона на желтый, а при наведении курсора мыши на нее всплывает текстовое сообщение, представленное на рисунке 10.

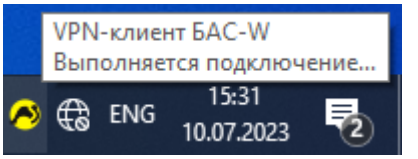

Рисунок 10 – Подключение VPN-профиля

При успешном подключении VPN-профиля отображается всплывающее сообщение (рисунок 11), фон иконки КП «БАС-W» в системном трее становится зеленого цвета, а при наведении курсора мыши на иконку всплывает текстовое сообщение с информацией о том, какой VPN-профиль сейчас подключен, и какой IP-адрес назначен клиенту (рисунок 12).

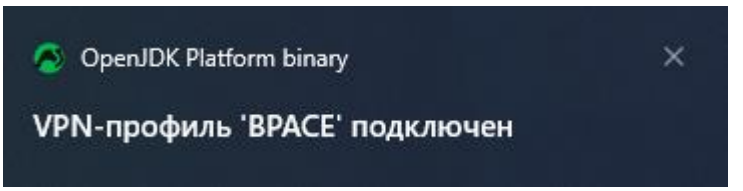

Рисунок 11 – Успешное подключение VPN-профиля

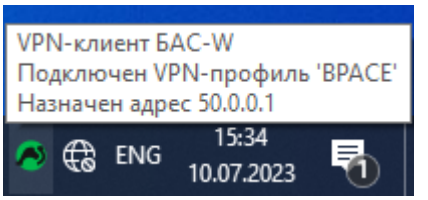

Рисунок 12 – Информация о VPN-подключении

3 Проверка работоспособности

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

```
C:\Documents and Settings\Администратор>ping 10.0.0.10
Обмен пакетами с 10.0.0.10 по 32 байт:
Ответ от 10.0.0.10: число байт=32 время<1мс TTL=64
Ответ от 10.0.0.10: число байт=32 время<1мс TTL=64
Ответ от 10.0.0.10: число байт=32 время<1мс TTL=64
Ответ от 10.0.0.10: число байт=32 время<1мс TTL=64
Статистика Ping для 10.0.0.10:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 1 мсек, Максимальное = 1 мсек, Среднее = 1 мсек
```

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:
  10.0.0.1
  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_BPACE authentication
BAS-Client:    child: 10.0.0.0/24 === dynamic TUNNEL, dpdaction = clear
Security Associations (1 up, 0 connecting):
BAS-Client [1]:ESTABLISHED 15 seconds ago, 100.0.0.2[100.0.0.2]...20.0.0.10[Client1]
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, 240 bytes_i (4 pkts, 13s ago), 240 bytes_o (4 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 4 пакета в каждую сторону, защищенных при помощи алгоритмов **BELT_CFB_256/BELT_MAC**.

Получить информацию о подключении можно и в КП «БАС-W».

Когда VPN-профиль подключен в контекстном меню КП «БАС-W» становится доступен пункт «Информация о подключении», при выборе которого открывается одноименное окно (рисунок 13).

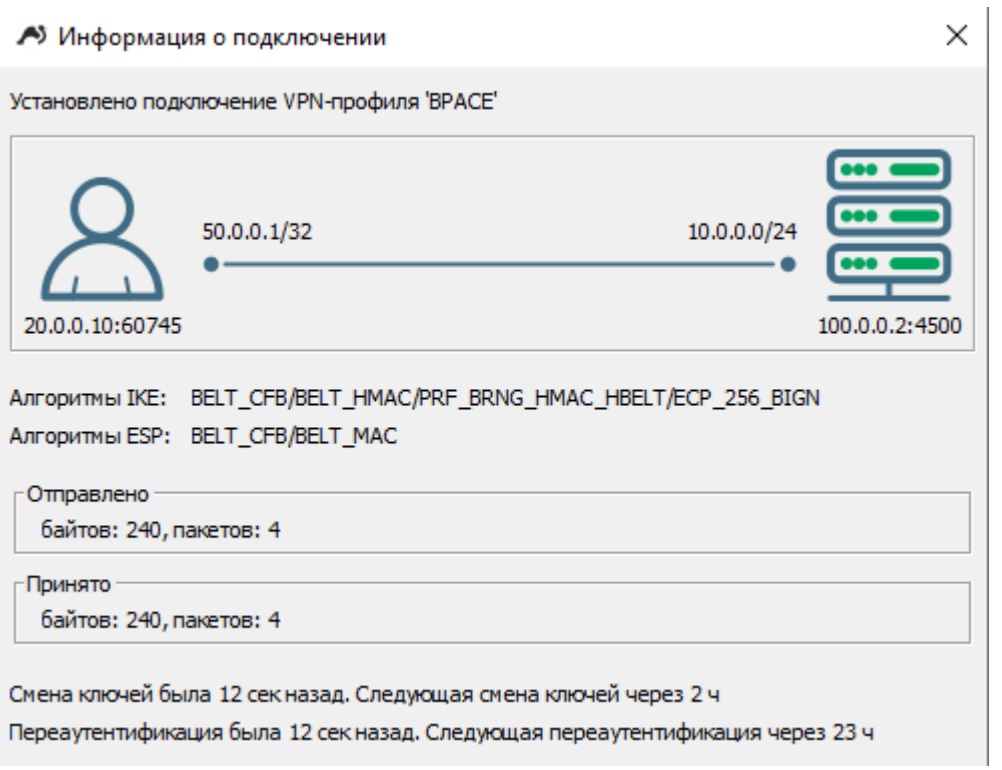

Рисунок 13 – Информация о подключении

Как видно из «Информации о подключении», установлен туннель между подсетями **50.0.0.1/32===10.0.0.0/24**, по туннелю было передано по 4 пакета в каждую сторону, защищенных при помощи алгоритмов **BELT_CFB_256/BELT_MAC**.