

Закрытое акционерное общество «НТЦ КОНТАКТ»

УТВЕРЖДАЮ

Директор

ЗАО «НТЦ КОНТАКТ»

_____ А.А.Тепляков

1 июля 2019 г.

**КОМПЛЕКС ПРОГРАММНО-АППАРАТНЫЙ
КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «БАС»**

**Инструкция по настройке защищенного соединения
между двумя сегментами одной сети при помощи протокола L2TPv3
СЮИК.465634.001 ИС20**

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

Содержание

1	Описание соединения (стенда)	4
2	Настройка соединения (стенда)	5
2.1	Настройка ПАК «БАС» 1	5
2.1.1	Смена пароля администратора.....	6
2.1.2	Настройка сетевых интерфейсов	6
2.1.3	Настройка L2TPv3 туннеля	7
2.1.4	Настройка даты и времени	8
2.1.5	Управление ключевой информацией	8
2.1.6	Настройка программного обеспечения	13
2.2	Настройка ПАК «БАС» 2	14
2.3	Настройка ПК 1	16
2.4	Настройка ПК 2	16
3	Проверка работоспособности	17

Подп. и дата		Инв. № дубл.		Взам. Инв. №		Подп. и дата			
Инв. № подл.	Изм.	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС20			
Разраб.	Толстой					Лит.	Лист	Листов	
Пров.	Федоров					0	0 ₁	2	18
Н. контр.	Мухортов					ЗАО «НТЦ КОНТАКТ»			
Утв.	Тепляков					Инструкция по настройке защищенного соединения между двумя сегментами одной сети при помощи протокола L2TPv3			

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.

Настоящая инструкция является расширением Руководства по эксплуатации ПАК «БАС» СЮИК.465634.001 РЭ и предназначена для облегчения работы администратора при создании типовой схемы включения ПАК «БАС» для построения защищенного соединения.

Настоящая инструкция предназначена для администратора, имеющего навыки работы с ОС Linux и 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.

Инструкция описывает порядок настройки ПАК «БАС» для построения защищенного соединения между двумя сегментами одной сети при помощи протокола L2TPv3.

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

Изм	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС20	Лист
						3

1 Описание соединения (стенда)

Схема включения ПАК «БАС» для построения защищенного соединения между двумя подсетями приведена на рисунке 1.

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

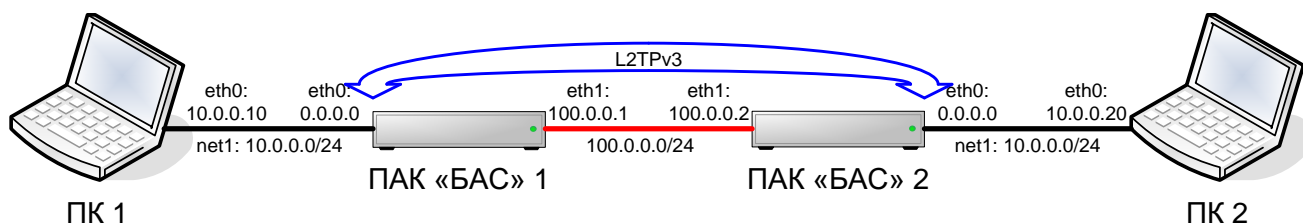


Рисунок 1 – Схема стенда

Данный сценарий описывает возможность объединения двух сегментов одной сети при помощи ПАК «БАС». Объединение происходит на канальном уровне.

Между входами ПАК «БАС» при помощи протокола L2TPv3 (Layer 2 Tunneling Protocol (Version 3)) устанавливается «псевдопроводной» (Ethernet Pseudowire) туннель. Кадры канального уровня, приходящие на вход ПАК «БАС» 1, инкапсулируются в пакеты сетевого уровня и передаются ПАК «БАС» 2 и наоборот. При этом между ПАК «БАС» установлен IPsec туннель, который обеспечивает защиту всего трафика, проходящего по L2TPv3 туннелю.

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

Изм.	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС20	Лист
						4

2 Настройка соединения (стенда)

Для настройки соединения (стенда) необходимо выполнить настройку всех его составляющих: настроить оба ПАК «БАС» и оба ПК из защищаемых подсетей.

Для настройки ПАК «БАС» необходимо выполнить следующие операции:

- смена пароля администратора;
- настройка сетевых интерфейсов;
- настройка L2TPv3 туннеля;
- 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.

2.1 Настройка ПАК «БАС» 1

Для настройки ПАК «БАС» 1 необходимо войти в его консоль, используя транспортный логин **server** и пароль **1111111**.

```
Ubuntu 14.04.3 LTS server tty1
server login: server
Password:
server@server:~$
```

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

Изм.	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС20	Лист
						5

2.1.4 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 061810472019
```

```
[sudo] password for server:
```

```
Аўт Чэр 18 10:47:00 MSK 2019
```

Для вступления всех настроек в силу перезагрузите ПАК «БАС» 1.

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

2.1.5 Управление ключевой информацией

Для генерации запроса на выпуск сертификата открытого ключа необходимо воспользоваться утилитой **RequestBuilder**. Она выполнит самотестирование ПАК «БАС» 1, сгенерирует личный ключ и сформирует запрос на выпуск сертификата открытого ключа.

```
server@server:~$ sudo RequestBuilder
```

```
[sudo] password for server:
```

```
> Контроль Целостности
```

```
Проверка целостности прошла успешно!
```

```
Результаты: /etc/support/IntegrityController.log
```

```
> Тестирование Библиотеки Криптопреобразований
```

```
Тестирование алгоритмов СТБ.34.101.31 выполнено
```

```
Тестирование алгоритмов СТБ 34.101.45 выполнено
```

```
Тестирование алгоритмов СТБ 34.101.47 выполнено
```

```
Тестирование алгоритмов СТБ 34.101.66 выполнено
```

```
Тестирование алгоритмов ГОСТ 28147-89 выполнено
```

Самотестирование библиотеки криптографических преобразований завершено успешно.

```
> Контроль Работоспособности ПАК "Барьер-USB"
```

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата	Подп. и дата	Лист
Изм.	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС20	

На защищённом хранилище не установлена парольная защита!
 Защищённое хранилище готово к работе.
 basctl: Тестирование завершено успешно!
 Желаете отредактировать XML-файл с данными об устройстве
 [/etc/support/PersonalData.xml]
 (Y/N): y

Для выпуска запроса на сертификат необходимо отредактировать XML-файл с данными об устройстве, указав в нем серийный номер устройства, название организации и адрес, где эксплуатируется ПАК «БАС» 1.

```
<?xml version="1.0" encoding="UTF-8"?>
<PersonalData>
  <CommonName Old="2.5.4.3" Description="Серийный номер устройства">
    00001
  </CommonName>
  <Description Old="2.5.4.13" Description="Общее наименование устройства">
    Комплекс программно-аппаратный криптографической защиты
    информации "БАС". Сервер защиты.
  </Description>
  <Organization Old="2.5.4.10" Description="Наименование организации –
    владельца устройства">
    ЗАО "НТЦ Контакт"
  </Organization>
  <Country Old="2.5.4.6" Description="Код страны нахождения организации">
    BY
  </Country>
  <Province Old="2.5.4.8" Description="Область нахождения организации">
  </Province>
  <City Old="2.5.4.7" Description="Населённый пункт нахождения
    организации">
    г.Минск
  </City>
  <StreetAddress Old="2.5.4.9" Description="Адрес нахождения организации">
    пер.Студенческий, д.17
  </StreetAddress>
</PersonalData>
```

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

Установите пароль для доступа к защищенному хранилищу. При необходимости резервирования личного ключа задайте пароль к блобу (резервной копии личного ключа, сохраняемой в файловой системе в защищенном виде).

Введите пароль доступа к защищённому хранилищу (8-24 символа): *****
 Потвердите пароль: *****
 Сохранить личный ключ для возможности восстановления системы? (Y/N): y

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

Задайте пароль доступа к блобу личного ключа (8-24 символа): *****

Потвердите пароль: *****

Заявка на выпуск сертификата открытого ключа успешно сохранена:

[/etc/support/IssueRequestsAndCards/CertificateIssueRequest_BC4A428F9FAEAB417D73AAE48C19BCE7ABAEBE2B677B17104122F6563D7A37B9.der]

Карточка открытого ключа успешно сохранена:

[/etc/support/IssueRequestsAndCards/PublicKeyCard_BC4A428F9FAEAB417D73AAE48C19BCE7ABAEBE2B677B17104122F6563D7A37B9.rtf]

Блоб личного ключа успешно сохранён:

[/etc/support/IssueRequestsAndCards/PrivateKeyBlob_BC4A428F9FAEAB417D73AAE48C19BCE7ABAEBE2B677B17104122F6563D7A37B9.sck]

server@server:~\$

В результате выполнения утилиты **RequestBuilder**, в папке **/etc/support/IssueRequestsAndCards/** были сформированы:

– запрос на выпуск сертификата в соответствии с СТБ 34.101.17:

CertificateIssueRequest_BC4A428F9FAEAB417D73AAE48C19BCE7ABAEBE2B677B17104122F6563D7A37B9.der

– карточка открытого ключа в соответствии с СТБ 34.101.49:

PublicKeyCard_BC4A428F9FAEAB417D73AAE48C19BCE7ABAEBE2B677B17104122F6563D7A37B9.rtf

– блок личного ключа:

PrivateKeyBlob_BC4A428F9FAEAB417D73AAE48C19BCE7ABAEBE2B677B17104122F6563D7A37B9.sck

Для выпуска сертификата открытого ключа необходимо экспортировать запрос на выпуск сертификата из ПАК «БАС» 1 любым удобным способом и передать администратору Удостоверяющего центра.

Экспортируем запрос на выпуск сертификата открытого ключа на съемный USB-носитель. Для этого необходимо подключить USB-носитель к ПАК «БАС» 1.

При помощи команды **fdisk** необходимо определить имя, присвоенное съемному USB-носителю операционной системой ПАК «БАС» 1.

```
server@server:~$ sudo fdisk -l
[sudo] password for server:
```

```
Disk /dev/sda: 120.0 GB, 120034123776 bytes
255 heads, 63 sectors/track, 14593 cylinders, total 234441648 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00022074
Device Boot Start End Blocks Id System
/dev/sda1 * 2048 226275327 113136640 83 Linux
/dev/sda2 226277374 234440703 4081665 5 Extended
/dev/sda5 226277376 234440703 4081664 82 Linux swap / Solaris
```

Изм	Лист	№ докум.	Подп.	Дата

СЮИК.465634.001 ИС20

Лист

10

```
Disk /dev/sdb: 15.5 GB, 15514730496 bytes
255 heads, 63 sectors/track, 1886 cylinders, total 30302208 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xf1725d57
Device Boot Start End Blocks Id System
/dev/sdb1 2048 30302207 15150080 c W95 FAT32 (LBA)
```

Операционная система ПАК «БАС» 1 присвоила подключенному съемному USB-носителю объемом 16 Гбайт имя **/dev/sdb1**.

Для монтирования файловой системы съемного USB-носителя необходимо воспользоваться командой **mount**.

```
server@server:~$ sudo mount /dev/sdb1 /mnt
```

Для копирования файла запроса на выпуск сертификата на съемный USB-носитель необходимо воспользоваться командой **cp**.

```
server@server:~$ cp
/etc/support/IssueRequestsAndCards/CertificateIssueRequest_BC4A428F9FAEAB417D
73AAE48C19BCE7ABAE2B677B17104122F6563D7A37B9.der /mnt/
```

Для того чтобы убедиться, что запрос на выпуск сертификата был успешно скопирован на съемный USB-носитель необходимо воспользоваться командой **ls**.

```
server@server:~$ ls /mnt/
CertificateIssueRequest_BC4A428F9FAEAB417D73AAE48C19BCE7ABAE2B677B1
7104122F6563D7A37B9.der
```

Для размонтирования файловой системы съемного USB-носителя необходимо воспользоваться командой **umount**.

```
server@server:~$ sudo umount /mnt
```

Извлечь съемный USB-носитель и передать администратору Удостоверяющего центра для выпуска сертификата и записи его на носитель. Если файл сертификата был получен в формате **p7b**, необходимо выполнить экспорт в отдельные файлы сертификатов. Экспорт сертификатов из **p7b** файла может быть выполнен при помощи Мастера экспорта сертификатов ОС Windows.

Импортируем сертификат открытого ключа со съемного USB-носителя в ПАК «БАС» 1. Для этого необходимо подключить USB-носитель к ПАК «БАС» 1.

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

Изм.	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС20	Лист
						11

При помощи команды **fdisk** необходимо определить имя, присвоенное съемному USB-носителю операционной системой ПАК «БАС» 1.

```
server@server:~$ sudo fdisk -l
```

Операционная система ПАК «БАС» 1 присвоила подключенному съемному USB-носителю объемом 16 Гбайт имя **/dev/sdb1**.

Произведем монтирование файловой системы съемного USB-носителя и посмотрим его содержимое.

```
server@server:~$ sudo mount /dev/sdb1 /mnt
server@server:~$ ls /mnt/
cert00001.cer
CertificateIssueRequest_BC4A428F9FAEAB417D73AAE48C19BCE7ABAEBE2B677B1
7104122F6563D7A37B9.der
Root.cer
```

В файловой системе съемного USB-носителя находятся три файла: запрос на выпуск сертификата, сертификат открытого ключа и корневой сертификат.

Импортируем сертификаты открытого ключа в ПАК «БАС» 1. Сертификат устройства в папку **/usr/local/etc/ipsec.d/certs/**, корневой сертификат, а также промежуточные (при их наличии), в **/usr/local/etc/ipsec.d/cacerts/**.

```
server@server:~$ sudo cp /mnt/Root.cer /usr/local/etc/ipsec.d/cacerts/
server@server:~$ sudo cp /mnt/cert00001.cer /usr/local/etc/ipsec.d/certs/
server@server:~$ ls /usr/local/etc/ipsec.d/cacerts/
Root.cer
server@server:~$ ls /usr/local/etc/ipsec.d/certs/
cert00001.cer
server@server:~$
```

ВНИМАНИЕ: Если сертификат ПАК «БАС» был выпущен подчиненным удостоверяющим центром, то сертификаты всех удостоверяющих центров, входящих в цепочку доверия, должны быть импортированы в папку **/usr/local/etc/ipsec.d/cacerts/**.

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

2.1.6 Настройка программного обеспечения

Настройка программного обеспечения ПАК «БАС» 1 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"

# Add connections here.
conn %default
    keyexchange = ikev2
    ikelifetime = 24h
    lifetime = 1h
    rekeymargin = 3m
    mobike = no
    ike = belt_cfb-belt_mac-prfbrng_ctr-modp2048-keyrep
    esp = belt_cfb-belt_mac
    left = 100.0.0.1
    leftid = %any
    leftcert = cert00001.cer
    leftauth = eap-bsts
    auto = route

conn simple
    right = 100.0.0.2
    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**.

Запустите (перезапустите) IPsec соединение

```
server@server:~$ sudo ipsec restart
Stopping strongSwanCont IPsec...
Starting strongSwanCont 5.2.0 IPsec [starter]...
```

Убедиться в том, что программное обеспечение ПАК «БАС» 1 подгрузило сертификат открытого ключа и сопоставило его с личным ключом, можно при помощи команды **ipsec listcerts**.

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

СЮИК.465634.001 ИС20

Лист

13

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

List of X.509 End Entity Certificates:

```
subject: "CN=00001, D=Комплекс программно-аппаратный криптографической
защиты информации "БАС". Сервер защиты., O=ЗАО "НТЦ Контакт", C=BY, L=г.Минск,
Street=пер.Студенческий, д.17"
```

```
issuer: "CN=УЦ для тестирования, C=BY, L=г.Минск, Street=пер.
Студенческий, д.7, O=ЗАО 'НТЦ КОНТАКТ', Pseudonym=ContactCA"
```

```
serial: 43:6f:6e:74:61:63:74:00:7e:36:00:00:00:00:00:00:09
```

```
validity: not before Jun 18 11:25:09 2019, ok
```

```
not after Jun 19 02:59:59 2020, ok
```

```
pubkey: BIGN 512 bits, has private key
```

```
keyid: 41:b9:70:dd:77:bf:78:e7:97:cc:45:e1:0d:26:81:8d:ae:49:a0:75
```

```
subjkey: bc:4a:42:8f:9f:ae:ab:41:7d:73:aa:e4:8c:19:bc:e7:
```

```
ab:ae:be:2b:67:7b:17:10:41:22:f6:56:3d:7a:37:b9
```

```
authkey: 63:be:6e:96:3a:ec:3d:84:d5:be:b4:00:6d:d0:e3:60:
```

```
b5:be:dd:db:27:af:15:a6:76:e3:90:cf:83:9e:9c:4c
```

```
server@server:~$
```

О том, что программное обеспечение ПАК «БАС» 1 верно подгрузило сертификат открытого ключа и сопоставило его с личным ключом, свидетельствует запись **pubkey: BIGN 512 bits, has private key.**

2.2 Настройка ПАК «БАС» 2

Настройка ПАК «БАС» 2 проводится аналогично ПАК «БАС» 1, при этом:

– файл **/etc/network/interfaces** будет иметь вид

```
server@server:~$ sudo nano /etc/network/interfaces
```

```
# interfaces(5) file used by ifup(8) and ifdown(8)
```

```
auto lo
```

```
iface lo inet loopback
```

```
iface eth0 inet static
```

```
address 0.0.0.0
```

```
netmask 0.0.0.0
```

```
auto eth0
```

```
iface eth1 inet static
```

```
address 100.0.0.2
```

```
netmask 255.255.255.0
```

```
auto eth1
```

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата	СЮИК.465634.001 ИС20	Лист
						14
Изм	Лист	№ докум.	Подп.	Дата		

– файл **/usr/local/etc/l2tp_BAS/l2tp_BAS.conf** будет иметь вид

```
server@server:~$ sudo nano /usr/local/etc/l2tp_BAS/l2tp_BAS.conf
```

```
# Configuration File for BAS L2TPv3 protocol
```

```
# Включение L2TPv3 туннеля (enable).
l2tp=enable
```

```
# Наименование входного сетевого интерфейса.
input_interface=eth0
```

```
# Идентификатор туннеля – 32-битное целочисленное значение.
# Уникально идентифицирует туннель.
# Должно соответствовать значению peer_tunnel_id партнера (ПАК «БАС» 2).
tunnel_id=2000
```

```
# Идентификатор партнера для туннеля – 32-битное целочисленное значение.
# Уникально идентифицирует партнера для создания туннеля.
# Должно соответствовать значению tunnel_id партнера (ПАК «БАС» 2).
peer_tunnel_id=1000
```

```
# IP-адрес локального интерфейса, который будет использоваться для туннеля.
local_ip=100.0.0.2
```

```
# IP-адрес партнерского интерфейса, который будет использоваться для туннеля.
remote_ip=100.0.0.1
```

```
# Порт источника UDP, который будет использоваться для туннеля.
udp_sport=5000
```

```
# Порт приемника UDP, который будет использоваться для туннеля.
udp_dport=6000
```

```
# Идентификатор сеанса – 32-битное целочисленное значение.
# Уникально идентифицирует сеанс, который создается.
# Должно соответствовать значению peer_session_id партнера (ПАК «БАС» 2).
session_id=4000
```

```
# Идентификатор партнера в сеансе – 32-битное целочисленное значение.
# Должно соответствовать значению session_id партнера (ПАК «БАС» 2).
peer_session_id=3000
```

– файл **/usr/local/etc/ipsec.conf** будет иметь вид

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

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

```
# Add connections here.
conn %default
```

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

Изм.	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС20	Лист
						15

```

keyexchange = ikev2
ikelifetime = 24h
lifetime = 1h
rekeymargin = 3m
mobike = no
ike = belt_cfb-belt_mac-prfbrng_ctr-modp2048-keyrep
esp = belt_cfb-belt_mac
left = 100.0.0.2
leftid = %any
leftcert = cert00002.cer
leftauth = eap
auto = route

```

```

conn simple
right = 100.0.0.1
rightid = %any
rightauth = eap
rightsendcert = never

```

2.3 Настройка ПК 1

Настройка ПК 1 заключается в настройке сетевого интерфейса. В ПК 1 необходимо установить IP-адрес, входящий в подсеть **10.0.0.0/24**:

```

IP-адрес:      10.0.0.10
Маска подсети: 255.255.255.0

```

2.4 Настройка ПК 2

Настройка ПК 2 аналогична ПК 1:

```

IP-адрес:      10.0.0.20
Маска подсети: 255.255.255.0

```

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

Изм	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС20	Лист
						16

3 Проверка работоспособности

Для проверки работоспособности соединения (стенда) необходимо с ПК 2 выполнить **ping** ПК 1.

```
C:\Documents and Settings\Администратор>ping 10.0.0.10
```

Обмен пакетами с 10.0.0.10 по 32 байт:

```
Превышен интервал ожидания для запроса.  
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 = 3, потеряно = 1 (25% потерь),  
Приблизительное время приема-передачи в мс:  
Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

При этом первый пакет инициализирует IPsec соединение, а последующие передаются по защищенному туннелю.

Убедиться в том, что передача данных идет по защищенному туннелю, можно, подав команду **ipsec statusall** в командную строку ПАК «БАС» 1 или ПАК «БАС» 2.

```
server@server:~$ sudo ipsec statusall  
Status of IKE charon daemon (strongSwan 5.2.0, Linux 3.13.11-ckt39-bas, x86_64):  
uptime: 74 seconds, since Jun 18 15:54:43 2019  
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 aes contactcrypto gmp sha1 random nonce x509 revocation  
constraints pubkey usbbar pem hmac attr kernel-netlink resolve socket-default stroke eap-bsts  
updown dhcp  
Listening IP addresses:  
100.0.0.1  
Connections:  
simple: 100.0.0.1...100.0.0.2 IKEv2  
simple: local: [CN=00001, D=Комплекс программно-аппаратный  
криптографической защиты информации "БАС". Сервер защиты., O=ЗАО "НТЦ Контакт",  
C=BY, L=г.Минск, Street=пер.Студенческий, д.17] uses EAP_BSTS authentication  
simple: cert: "CN=00001, D=Комплекс программно-аппаратный  
криптографической защиты информации "БАС". Сервер защиты., O=ЗАО "НТЦ Контакт",  
C=BY, L=г.Минск, Street=пер.Студенческий, д.17"  
simple: remote: uses EAP_BSTS authentication  
simple: child: dynamic === dynamic TUNNEL  
Security Associations (1 up, 0 connecting):
```

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

```

simple[1]: ESTABLISHED 15 seconds ago, 100.0.0.1[CN=00001,
D=Комплекс программно-аппаратный криптографической защиты информации "БАС".
Сервер защиты., O=ЗАО "НТЦ Контакт", C=BY, L=г.Минск, Street=пер.Студенческий,
д.17]...100.0.0.2[CN=00002, D=Комплекс программно-аппаратный криптографической
защиты информации "БАС". Сервер защиты., O=ЗАО "НТЦ Контакт", C=BY, L=г.Минск,
Street=пер.Студенческий, д.17]

```

```

simple[1]: IKEv2 SPIs: 0974252c95682c2f_i 400423a99128d35d_r*, EAP
reauthentication in 23 hours

```

```

simple[1]: IKE proposal: BELT_CFB_256/BELT_MAC/
PRF_BRNG_CTR_HBELT/MODP_2048/BELT_KEYREP_TRANSFORM

```

```

simple{1}: INSTALLED, TUNNEL, ESP SPIs: cbe8a626_i c9e7890e_o

```

```

simple{1}: BELT_CFB_256/BELT_MAC, 252 bytes_i (3 pkts, 13s ago),
252 bytes_o (3 pkts, 13s ago), rekeying in 55 minutes

```

```

simple{1}: 100.0.0.1/32 === 100.0.0.2/32

```

```

server@server:~$

```

Как видно из последних двух строчек, установлен IPsec туннель между адресами **100.0.0.1/32 === 100.0.0.2/32**, по туннелю было передано по 3 пакета в каждую сторону (**ping**), защищенных при помощи алгоритмов **BELT_CFB_256/BELT_MAC**.

Если повторить команду **ipsec statusall** через некоторое время, при этом не пересылать трафик, можно будет увидеть, что количество переданных по IPsec туннелю пакетов увеличилось, это служебные пакеты канального уровня попадают в туннель.

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

Изм.	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС20	Лист
						18