

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 защищенного соединения
между двумя сегментами одной сети при помощи протокола L2TPv3
СЮИК.465634.001 ИС39**

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 даты и времени	7
2.1.4	Управление ключевой информацией	7
2.1.5	Настройка L2TPv3 туннеля	8
2.1.6	Настройка программного обеспечения	9
2.2	Настройка ПАК «БАС» 2	11
2.3	Настройка ПК 1	13
2.4	Настройка ПК 2	13
3	Проверка работоспособности	14

Подп. и дата		Инв. № дубл.		Взам. Инв. №		Подп. и дата		СЮИК.465634.001 ИС39								
Инв. № подл.	Разраб.	Воронцова	Лит.	Лист	Листов	Изм	Лист	№ докум.	Подп.	Дата	Комплекс программно-аппаратный криптографической защиты информации «БАС» Инструкция по настройке защищенного соединения между двумя сегментами одной сети при помощи протокола L2TPv3					
	Пров.	Фёдоров	0	0 ₁	2									2	15	
	Н. контр.	Васильев												ЗАО «НТЦ КОНТАКТ»		
	Утв.	Тепляков														

Настоящая инструкция распространяется на «Комплекс программно-аппаратный криптографической защиты информации «БАС» СЮИК.465634.001 (далее – ПАК «БАС»», предназначенный для защиты информации, циркулирующей в каналах передачи данных.

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 ИС39	Лист
						3

1 Описание соединения (стенда)

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

Данная схема может быть применена при объединении сети двух удаленных офисов или для подключения филиала к центральному офису.

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.

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.

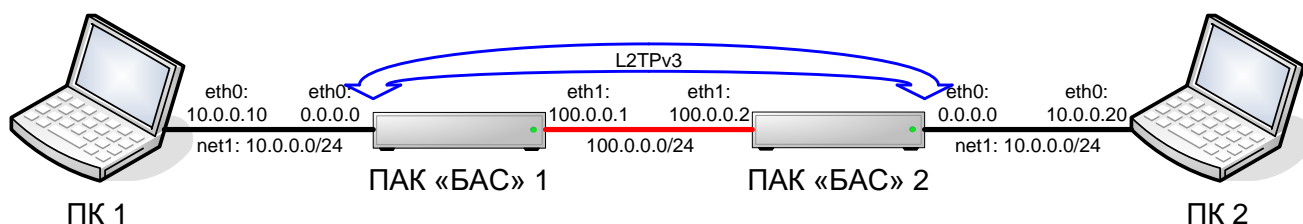


Рисунок 1 – Схема стенда

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

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**.

```
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 ИС39

2.1.1 Смена пароля администратора

ВНИМАНИЕ: СМЕНА ТРАНСПОРТНОГО ПАРОЛЯ ЯВЛЯЕТСЯ ОБЯЗАТЕЛЬНОЙ

Для смены пароля необходимо воспользоваться командой **passwd**, после чего ввести транспортный пароль **1111111**, а затем задать и подтвердить новый. Пароль должен быть не менее 8 символов.

```
server@server:~$ passwd
Смена пароля для server.
current password:
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлен
```

2.1.2 Настройка сетевых интерфейсов

Для настройки сетевых интерфейсов необходимо отредактировать файл **/etc/network/interfaces** при помощи текстового редактора **nano**, задав IP-адрес и маску выходного интерфейса, а также перевести входной в неразборчивый режим.

```
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 manual
up ifconfig eth0 promisc up
down ifconfig eth0 promisc down
auto eth0

iface eth1 inet static
address 100.0.0.1
netmask 255.255.255.0
auto eth1
```

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

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

Изм	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС39	Лист
						6

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» 1.

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

2.1.4 Управление ключевой информацией

Для надежной аутентификации участники IPsec-соединения должны обладать неизвлекаемым личным ключом, а также парным ему открытым ключом в составе сертификата. В связи с этим необходимо выполнить:

- генерацию личного ключа;
- формирование запроса на выпуск сертификата открытого ключа;
- экспорт запроса на получение сертификата открытого ключа;
- импорт сертификата открытого ключа в ПАК «БАС».

Последовательность действия по управлению ключевой информацией описана в документе «Комплекс программно-аппаратный криптографической защиты информации «БАС». Инструкция по управлению ключевой информацией. СЮИК.465634.001 ИС21».

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата	СЮИК.465634.001 ИС39	Лист
						7
Изм.	Лист	№ докум.	Подп.	Дата		

2.1.5 Настройка L2TPv3 туннеля

Настройка L2TPv3 туннелей ПАК «БАС» заключается в редактировании настроечных файлов в директории `/usr/local/etc/l2tp_BAS/` при помощи текстового редактора **nano**. Каждый файл описывает один туннель.

В данном сценарии используется только один L2TPv3 туннель, поэтому в ПАК «БАС» 1 необходимо отредактировать только один файл `/usr/local/etc/l2tp_BAS/l2tp_BAS.conf`.

```
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 виртуального сетевого интерфейса. Обычно l2tpethN.
interface_name=l2tpeth0
# Наименование сетевого моста. Должно иметь вид brl2tpN.
bridge_name=brl2tp0
# Наименование входного сетевого интерфейса.
input_interface=eth0
# IP-адрес локального интерфейса, который будет использоваться для построения туннеля.
local_ip=100.0.0.1
# IP-адрес партнерского интерфейса, который будет использоваться для построения туннеля.
remote_ip=100.0.0.2
# UDP порт источника и приемника, который будет использоваться для туннеля.
port=5000
```

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

Запустите (перезапустите) L2TPv3 туннель

```
server@server:~$ sudo l2tp_BAS restart
l2tp_BAS: Удаление L2TPv3 соединений...
l2tp_BAS: Добавление L2TPv3 соединений...
l2tp_BAS: Неверный формат параметра mtu. Параметр должен принимать значение целого числа.
Принято значение 1500.
l2tp_BAS: Туннель 5000 добавлен.
l2tp_BAS: Сессия 5000 добавлена.
l2tp_BAS: Интерфейс eth0 добавлен в мост brl2tp0.
l2tp_BAS: Мост brl2tp0 поднят.
l2tp_BAS: Интерфейс l2tpeth0 добавлен в мост brl2tp0.
l2tp_BAS: Интерфейс l2tpeth0 поднят.
l2tp_BAS: Модуль L2 загружен успешно. Настройки из файла
/usr/local/etc/l2tp_BAS/l2tp_BAS.conf применены.
```

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

СЮИК.465634.001 ИС39

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, cnt 1"

# Add connections here.
conn %default
    keyexchange = ikev2
    ikelifetime = 24h
    lifetime = 1h
    rekeymargin = 5m
    mobike = no

    ike = belt_cfb-belt_hmac-prfbrng_hmac-ecp256bign-keyrep
    esp = belt_cfb-belt_mac

    left = 100.0.0.1
    leftid = %any
    leftprotoport = udp/5000
    leftcert = cert00001.cer
    leftauth = eap-bsts
    auto = route

    dpdaction = clear
    closeaction = clear

conn BAS1-BAS2
    right = 100.0.0.2
    rightid = %any
    rightprotoport = udp/5000
    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 5.8.4 IPsec [starter]...
```

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

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**.

```
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
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» 1 верно подгрузило сертификат открытого ключа и сопоставило его с личным ключом, свидетельствует запись **pubkey: BIGN 512 bits, has private key.**

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата					
Изм	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС39				Лист
									10

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

# 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 manual
up ifconfig eth0 promisc up
down ifconfig eth0 promisc down
auto eth0

iface eth1 inet static
address 100.0.0.2
netmask 255.255.255.0
auto eth1
```

– 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 виртуального сетевого интерфейса. Обычно l2tpethN.
interface_name=l2tpeth0
# Наименование сетевого моста. Должно иметь вид brl2tpN.
bridge_name=brl2tp0
# Наименование входного сетевого интерфейса.
input_interface=eth0
# IP-адрес локального интерфейса, который будет использоваться для построения туннеля.
local_ip=100.0.0.2
# IP-адрес партнерского интерфейса, который будет использоваться для построения туннеля.
remote_ip=100.0.0.1
# UDP порт источника и приемника, который будет использоваться для туннеля.
port=5000
```

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата	СЮИК.465634.001 ИС39	Лист
						11
Изм	Лист	№ докум.	Подп.	Дата		

– 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, cnt 1"
```

```
# Add connections here.
```

```
conn %default
```

```
    keyexchange = ikev2
```

```
    ikelifetime = 24h
```

```
    lifetime = 1h
```

```
    rekeymargin = 5m
```

```
    mobike = no
```

```
    ike = belt_cfb-belt_hmac-prfbrng_hmac-ecp256bign-keyrep
```

```
    esp = belt_cfb-belt_mac
```

```
    left = 100.0.0.2
```

```
    leftid = %any
```

```
    leftprotoport = udp/5000
```

```
    leftcert = cert00002.cer
```

```
    leftauth = eap-bsts
```

```
    auto = route
```

```
    dpdaction = clear
```

```
    closeaction = clear
```

```
conn BAS2-BAS1
```

```
    right = 100.0.0.1
```

```
    rightid = %any
```

```
    rightprotoport = udp/5000
```

```
    rightauth = eap-bsts
```

```
    rightsendcert = never
```

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата	СЮИК.465634.001 ИС39	Лист
						12
Изм	Лист	№ докум.	Подп.	Дата		

2.3 Настройка ПК 1

Настройка ПК 1 заключается в настройке сетевого интерфейса. В ПК 1 необходимо установить IP-адрес, входящий в защищаемую 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	СЮИК.465634.001 ИС39	Лист
						13
Изм	Лист	№ докум.	Подп.	Дата		

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 5.8.4, 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 ushbar bpkc attr kernel-netlink
resolve socket-default stroke vici updown xauth-generic dhcp counters eap-bsts eap-bpacc
Listening IP addresses:
 100.0.0.1
Connections:
BAS1-BAS2: 100.0.0.1...100.0.0.2 IKEv2, dpddelay=30s
BAS1-BAS2: local: [CN=BAS00001, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс
программно-аппаратный криптографической защиты информации "БАС". Сервер защиты] uses EAP_BSTS
authentication
BAS1-BAS2: cert: "CN=BAS00001, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс
программно-аппаратный криптографической защиты информации "БАС". Сервер защиты"
BAS1-BAS2: remote: uses EAP_BSTS authentication
BAS1-BAS2: child: dynamic[udp/5000] == dynamic[udp/5000] TUNNEL, dpdaction = clear
Security Associations (1 up, 0 connecting):
```

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

```
BAS1-BAS2[1]: ESTABLISHED 15 seconds ago, 100.0.0.1[CN=BAS00001, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты]...100.0.0.2[CN=BAS00002, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты]
```

```
BAS1-BAS2[1]: IKEv2 SPIs: 0974252c95682c2f_i 400423a99128d35d_r*, EAP reauthentication in 23 hours
```

```
BAS1-BAS2[1]: IKE proposal: BELT_CFB/BELT_HMAC/PRF_BRNG_HMAC_HBELT/ECF_256_BIGN
```

```
BAS1-BAS2{1}: INSTALLED, TUNNEL, reqid, ESP SPIs: cbe8a626_i c9e7890e_o
```

```
BAS1-BAS2{1}: BELT_CFB_256/BELT_MAC, 252 bytes_i (3 pkts, 13s ago), 252 bytes_o (3 pkts, 13s ago), rekeying in 55 minutes
```

```
BAS1-BAS2{1}: 100.0.0.1/32[udp/5000] === 100.0.0.2/32[udp/5000]
```

```
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				Лист
Изм.	Лист	№ докум.	Подп.	Дата	СЮИК.465634.001 ИС39			15