

УТВЕРЖДЕНО

ВУ.РТНК.00001-04.1 34 01-6-ЛУ

Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1»

Руководство администратора

Инициализация

ВУ.РТНК.00001-04.1 34 01-6

Листов 7

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

Содержание

Инициализация шлюза безопасности Bel VPN Gate 4.1 на вычислительных системах архитектуры Intel x86/x86-64	3
Инициализация ключевого носителя информации	4
Инициализация носителя типа AvPass	4
Инициализация носителя типа AvBign	4
Подготовка программно-аппаратного комплекса к инициализации	5
Инициализация шлюза безопасности Bel VPN Gate 4.1 при первом старте	6

Инициализация шлюза безопасности Bel VPN Gate 4.1 на вычислительных системах архитектуры Intel x86/x86-64

В этом разделе описана инициализация программно-аппаратного комплекса «Шлюз безопасности Bel VPN Gate 4.1» на вычислительных системах архитектуры Intel x86/x86-64.

Программно-аппаратный комплекс поставляется в инсталлированном состоянии.

На ПАК установлены:

- ОС Debian GNU/Linux 6 (32-bit или 64-bit),
- программный комплекс «Шлюз безопасности Bel VPN Gate 4.1»,
- внешнее устройство хранения информации: AvPass (ИЯТА.467532.002) или AvBign (ИЯТА.467532.003)

Для инициализации ПАК требуется:

- персональный компьютер под управлением операционной системы семейства Windows, включающий:
 - устройство чтения компакт-дисков (CD-ROM/DVD-ROM);
 - последовательный (COM) порт, если аппаратная платформа ПАК Шлюз безопасности поддерживает управление через последовательный интерфейс;
- монитор и клавиатура

или

- нуль-модемный кабель, если аппаратная платформа ПАК Шлюз безопасности поддерживает управление через последовательный интерфейс.

Инициализация ключевого носителя информации

Для хранения личного ключа электронной цифровой подписи в ПАК Шлюз безопасности используются ключевые носители AvPass 11-E-02/04, AvBign 128-C-01, которые необходимо инициализировать перед использованием.

Для инициализации носителей типа AvPass используется утилита командой строки AvPassInit.exe (поставляется на компакт-диске S-Terra Bel Gate 4.1. Documentatin, каталог Utils).

Инициализация носителя типа AvPass

- Шаг 1:** Подключить ключевой носитель к usb-порту персонального компьютера.
- Шаг 2:** Вставить компакт-диск S-Terra Bel Gate 4.1. Documentatin в устройство считывания компакт-дисков.
- Шаг 3:** Запустить командную строку (`cmd.exe`) и перейти в каталог Utils, размещенный на компакт-диске.
- Шаг 4:** Вызывать утилиту `avpassinit.exe` с параметром «`-pin=`», указав после «`=`» новый пароль.

Пример:

```
avpassinit.exe -pin=s3CR3tPassWorD
```

- Шаг 5:** Отключить ключевой носитель от ПК и подключить его к ПАК Шлюз безопасности.

Инициализация носителя типа AvBign

- Шаг 1:** Подключить ключевой носитель к usb-порту персонального компьютера.
- Шаг 2:** Вставить компакт-диск S-Terra Bel Gate 4.1. Documentatin в устройство считывания компакт-дисков.
- Шаг 3:** Запустить командную строку (`cmd.exe`) перейти в каталог Utils, размещенный на компакт-диске.
- Шаг 4:** Вызвать утилиту `avtoksvc.exe` с параметром `info`, найти номер слота, к которому подключен ключевой носитель. Номер будет указан в строке `CK_SLOT_ID`.
- Шаг 5:** Вызывать утилиту `avtoksvc.exe` с параметрами `newpasswd -slot=номер-слота -password=пароль-пользователя -new_password=новый-пароль-пользователя`.

В случае успеха будет выведено сообщение

```
User PIN changed.  
Done in 0:00:00.577.  
Testing new user password...  
New user password passed OK.
```

В случае неуспешного выполнения операции смены пароля, сообщение будет следующее:

```
C_Login(U) returned 0xa0 PIN INCORRECT
```

Пример:

```
avtoksvc.exe newpasswd -slot=0 -password=P2Ss!0Rd  
-new_password= P2Ss!0Rd  
User PIN changed.  
Done in 0:00:00.577.  
Testing new user password...  
New user password passed OK.
```

- Шаг 6:** Отключить ключевой носитель от ПК и подключить его к ПАК Шлюз безопасности.

Подготовка программно-аппаратного комплекса к инициализации

В качестве терминала для аппаратной платформы (АП), на которой установлен программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1», можно использовать монитор и клавиатуру или последовательный интерфейс, подключенные к соответствующим разъемам АП.

Шаг 1: Подключить к ПАК монитор и клавиатуру или последовательный порт компьютера в качестве терминала, используя нуль-модемный кабель (5 проводов).

На компьютере используйте терминальную программу, например, Windows HyperTerminal или Putty.

В программе HyperTerminal выполните настройки:

File-> Properties-> Settings-> Emulation-> VT100

Во вкладке Connect To нажать кнопку Configure и выполнить следующие настройки COM-порта:

```
Bits per second: 115200  
Data bits: 8  
Parity: None  
Stop bits: 1  
Flow control: None
```

Шаг 2: Подключить ПАК к сети переменного тока и нажать кнопку питания на АП.

В процессе загрузки указать, что будет использоваться в качестве терминала для аппаратной платформы:

- 1) монитор и клавиатура
Bel VPN Gate
- 2) последовательный порт
Bel VPN Gate (serial)

Шаг 3: После загрузки ОС войти в систему, используя следующие реквизиты:

```
имя пользователя – root  
пароль – пустой.
```

Шаг 4: Выполнить процедуру инициализации программного комплекса S-Terra Gate, описанную в разделе [«Инициализация шлюза безопасности Bel VPN Gate 4.1 при первом старте»](#).

Инициализация шлюза безопасности Bel VPN Gate 4.1 при первом старте

При старте программно-аппаратного комплекса после загрузки ОС появляется предупреждение "System is not initialized. Please run /opt/VPNagent/bin/init.sh to start initialization procedure" и приглашение для входа в ОС.

Ниже пошагово описаны действия, которые необходимо выполнить для инициализации шлюза безопасности Bel VPN Gate.

Шаг 1: Запустить скрипт /opt/VPNagent/bin/init.sh для старта процедуры начальной инициализации шлюза безопасности Bel VPN Gate.

Во время выполнения, инициализационный скрипт может быть прерван нажатием комбинации клавиш Ctrl+C.

При возникновении ошибки процесс инициализации прерывается и на экран выдается сообщение об ошибке.

Шаг 2: Далее проводится инициализация начального значения ДСЧ.

Шаг 3: Далее запрашивается лицензионная информация на Шлюз безопасности Bel VPN Gate (сведения, необходимые для ввода находятся на бланке «Лицензии на использование программно-аппаратного комплекса «Шлюз безопасности Bel VPN Gate», входящем в комплект поставки):

```
You have to enter license for Bel VPN Gate
```

Предлагаются следующие пункты для ввода:

```
Available product codes:
```

```
GATE100  
GATE100B  
GATE100V  
GATE1000  
GATE1000V  
GATE3000  
GATE7000  
GATE10000  
RVPN  
RVPNV  
BELVPN  
BELVPNV  
UVPN  
UVPNV  
KZVPN  
KZVPNV
```

```
Enter product code: – ввести код продукта
```

```
Enter customer code: – ввести код конечного пользователя
```

```
Enter license number: – ввести номер лицензии
```

```
Enter license code: – ввести код лицензии
```

- Шаг 4:** Следует вопрос о корректности введенных данных: "Is the above data correct?". После получения подтверждения инициализация продолжается без дополнительных вопросов. Если получен отрицательный ответ – предлагается ввести лицензионную информацию повторно.
- Шаг 5:** Далее запускается vpn-демон, создается пользователь "cscons" с назначенным ему начальным паролем "csp".

Если инициализация завершилась успешно, то выдается сообщение: "Initialization complete". При последующих стартах системы предупреждение о необходимости инициализации системы не выдается.

Если инициализация завершилась неуспешно, то об этом выдаётся соответствующее сообщение. При следующем старте комплекса администратору снова будет выдаваться предупреждение об инициализации.

При инициализации шлюза безопасности Bel VPN Gate устанавливается политика безопасности, при которой интерфейсы шлюза безопасности не пропускают пакеты – Default Driver Policy = Dropall. Выдается информационное сообщение:

```
Default driver policy is configured to block network traffic.
Network is inaccessible in this mode.
You can change it using "${AgentRoot}bin/dp_mgr" utility or load security
policy.
```

Для входа в Cisco-like интерфейс командной строки нужно использовать имя пользователя "cscons" (начальный пароль "csp"),

Для входа в ОС предназначено имя "root" (изначально без пароля).

Сразу после инициализации программного комплекса автоматически запускается утилита `cspvpn_verify` для проверки целостности установленного Продукта шлюз безопасности Bel VPN Gate, которая описана в документе [«Шлюз безопасности Bel VPN Gate 4.1. Специализированные команды»](#). При нарушении целостности восстановите содержимое жесткого диска ПАК из образа жесткого диска, который входит в комплект поставки. Выполните эту процедуру согласно документу – [«Шлюз безопасности Bel VPN Gate 4.1. Инструкции по восстановлению ПАК»](#).

Далее перейдите к настройке Bel VPN Gate, описанной в документе [«Шлюз безопасности Bel VPN Gate. Общие настройки»](#).

Утилита управления ключевыми контейнерами `cryptoscont` размещается в каталоге `/opt/Avest/bin`. Подробное описание данной утилиты приведено в документе «Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1». Руководство администратора. Специализированные команды».

После инициализации шлюза безопасности Bel VPN Gate 4.1 следует перейти к настройке шлюза безопасности, которая описывается в документе «Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1». Руководство администратора. Общие настройки».