

ЗАО «С-Терра СиЭсПи»  
124460, г. Москва, Зеленоград, проезд 4806, д.6, этаж 4-й  
Телефон: +7 (499) 940 9061  
Факс: +7 (499) 940 9061  
Эл.почта: [information@s-terra.com](mailto:information@s-terra.com)  
Сайт: <http://www.s-terra.com>



**Программный комплекс  
"Шлюз безопасности  
CSP VPN Gate. Версия 3.1"**

**Руководство  
администратора**

**Инициализация CSP VPN Gate  
при использовании  
СКЗИ «КриптоПро CSP 3.6»**

РЛКЕ.00005-01 90 03

24.11.2011

# Содержание

<b>Инициализация CSP VPN Gate при использовании СКЗИ «КриптоПро CSP 3.6» .....</b>	<b>3</b>
Подготовка программно-аппаратного комплекса к инициализации .....	4
Режим KC1 .....	4
Режим KC2 .....	5
Инициализация CSP VPN Gate при первом старте .....	7
Переключение консоли на последовательный порт или монитор и клавиатуру	9

# Инициализация CSP VPN Gate при использовании СКЗИ «КриптоПро CSP 3.6»

---

В этом документе описана инициализация программного комплекса CSP VPN Gate, установленного на аппаратные платформы. Инициализация программного комплекса CSP VPN Gate на модуле МСМ, установленный в маршрутизатор Cisco, описана в отдельном документе [«Руководство по установке и настройке NME-RVPN модуля \(МСМ\)»](#).

# Подготовка программно-аппаратного комплекса к инициализации

В качестве терминала для аппаратной платформы (АП), на которой установлен Продукт CSP VPN Gate, можно использовать:

- компьютер, подключенный к последовательному порту АП
- монитор и клавиатуру, подключенные к разъемам АП.

Но изначально заданы определенные настройки.

## Режим КС1

**Шаг 1:** К АП с установленным Продуктом CSP VPN Gate 3000/7000 подключите к разъемам монитор и клавиатуру в качестве терминала, и перейдите к [Шагу 2](#).

К АП с установленным Продуктом CSP VPN Gate 100/100B/100V/1000/1000V подключите к последовательному порту компьютер в качестве терминала. Для АП TONK 1800 подключить следует к COM2-порту, для остальных АП – к COM1-порту, используя нуль-модемный кабель (5 проводов). На компьютере используйте терминальную программу, например, Windows HyperTerminal. В программе HyperTerminal выполните настройки:

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

Во вкладке `Connect To` нажмите кнопку `Configure` и выполните следующие настройки COM-порта:

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

**Шаг 2:** Включите шнур питания в сеть переменного тока и нажмите кнопку питания на АП.

**Шаг 3:** После загрузки ОС войдите в систему пользователем `"root"` и пустым паролем.

**Шаг 4:** При необходимости переключить ввод/вывод с последовательного порта на монитор и клавиатуру или наоборот, воспользуйтесь скриптом `consoleswitch`, описанным в разделе [«Переключение консоли на последовательный порт или монитор и клавиатуру»](#). После этого выключите питание платформы командой:

```
cspgate:~# poweroff
```

Дождитесь окончания выполнения команды. Отсоедините шнур питания от сети переменного тока. Выполните необходимые переключения оборудования в качестве терминала. Включите шнур питания в сеть переменного тока. Нажмите кнопку питания на передней панели АП. После загрузки ОС войдите в систему пользователем `"root"` и пустым паролем.

**Шаг 5:** Выполните процедуру инициализации программного комплекса CSP VPN Gate, описанную в разделе [«Инициализация CSP VPN Gate при первом старте»](#).

## Режим KC2

Если Продукт будет работать с СКЗИ «КриптоПро CSP 3.6» в режиме KC2, то для защиты от несанкционированного доступа к АП используется ПАК «Соболь» версии 3.0. На АП уже установлена плата ПАК «Соболь» и инициализирована. В качестве идентификатора пользователя используется iButton DS 1992, а для АП Cisco UCS C200 – идентификатор Rutoken, входящие в комплект поставки ПАК «Соболь».

**Шаг 1:** К АП с установленным Продуктом CSP VPN Gate 3000/7000 подключите к разъемам монитор и клавиатуру в качестве терминала, и перейдите к [Шагу 2](#).

К АП с установленным Продуктом CSP VPN Gate 100/100В/100V/1000/1000V подключите к последовательному порту компьютер в качестве терминала. Для АП TONK 1800 подключить следует к COM2-порту, для остальных АП – к COM1-порту, используя нуль-модемный кабель (5 проводов). На компьютере используйте терминальную программу, например, Windows HyperTerminal. В программе HyperTerminal выполните настройки:

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

Во вкладке **Connect To** нажмите кнопку **Configure** и выполните следующие настройки COM-порта:

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

**Шаг 2:** Подключите внешний считыватель идентификатора iButton к разъему, имеющему на АП маркировку «iButton» (если используется iButton).

**Шаг 3:** Включите шнур питания в сеть переменного тока и нажмите кнопку питания на АП.

**Шаг 4:** На ПАК «Соболь» выставлена настройка - Время ожидания сторожевого таймера – 20 сек. Это интервал времени, в течение которого управление должно быть передано ПАК «Соболь», если это не так, то осуществляется автоматическая перезагрузка компьютера.

При успешной передаче управления на экране появится запрос: «Введите персональный идентификатор». Предъявите идентификатор:

для iButton — плотно приложите идентификатор к внешнему считывателю  
для Rutoken — вставьте USB-ключ в свободный USB-разъем на задней панели АП Cisco UCS C200.

После считывания информации из идентификатора должен появиться запрос на ввод пароля: «Введите пароль». Так как изначально установлен пустой пароль, то запрос на ввод пароля не появляется.

После успешного тестирования датчика случайных чисел на экране появится информационное окно с указанием имени пользователя, номером идентификатора и др. Нажмите любую клавишу.

Далее в появившемся меню выберите предложение «Загрузка операционной системы» и нажмите Enter.

При следующем доступе к АП можно изменить пароль для идентификатора, минимальный размер пароля – 8 символов.

**Шаг 5:** После загрузки ОС войдите в систему пользователем "root" и пустым паролем.

**Шаг 6:** При необходимости переключить ввод/вывод с последовательного порта на монитор и клавиатуру или наоборот, воспользуйтесь скриптом `consoleswitch`, описанным в разделе [«Переключение консоли на последовательный порт или монитор и клавиатуру»](#). После этого выключите питание платформы командой:

```
cspgate:~# poweroff
```

Дождитесь окончания выполнения команды. Отсоедините шнур питания от сети переменного тока. Выполните необходимые переключения оборудования в качестве терминала. Включите шнур питания в сеть переменного тока. Нажмите кнопку питания на передней панели АП. После загрузки ОС войдите в систему пользователем "root" и пустым паролем.

**Шаг 7:** Выполните процедуру инициализации программного комплекса CSP VPN Gate, описанную в разделе [«Инициализация CSP VPN Gate при первом старте»](#).

# Инициализация CSP VPN Gate при первом старте

Программно-аппаратный комплекс поставляется в инсталлированном состоянии: установлена ОС Solaris 10 или Red Hat Enterprise Linux 5 или CentOS 5, продукты CSP VPN Gate, OpenSSH, СКЗИ «КриптоПро CSP 3.6».

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

**Шаг 1:** Войдите в ОС под именем "root" и пустым паролем.

**Шаг 2:** Запустите скрипт /opt/VPNagent/bin/init.sh для старта процедуры начальной инициализации шлюза безопасности.

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 3:** Запрашивается серийный номер лицензии на CryptoPro CSP:

"You have to enter license for CryptoPro CSP. Enter serial number:" Серийный номер можно взять из «Лицензии на право использования СКЗИ «КриптоПро CSP» в системе CSP VPN Gate (NME-RVPN)», входящей в комплект поставки, например:

DU30F-D00GR-XXXXXX-XXXXXX-XXXXXX. Не путайте «0» (ноль) и букву «O».

При вводе неверного номера лицензии предлагается ввести его еще раз.

**Шаг 4:** В режиме KC1 СКЗИ проводится «биологическая» инициализация начального значения ДСЧ: "You should initialize RNG. Press <Enter> to proceed...", поэтому предлагается понажимать клавиши: "Press keys... [ ]". По окончании выдается сообщение "Initialization SUCCESS".

В ОС Solaris 10 в режиме KC2 СКЗИ «биологическая» инициализация ДСЧ не предлагается, а выдается сообщение: csp\_cprng\_init utility KC2 implementation. Перейдите к выполнению следующего шага.

**Шаг 5:** Далее запрашивается лицензионная информация на CSP VPN Gate: "You have to enter license for CSP VPN Gate". Эти данные можно взять из «Лицензии на использование программного продукта компании ЗАО «С-Терра СиЭсПи», входящей в комплект поставки. 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: - введите код продукта, например, GATE1000

Enter customer code: - введите код конечного пользователя, например, GAZREESTRPROM

Enter license number: - введите номер лицензии, например, 55455

Enter license code: - введите код лицензии, например, B123456DFGH567KL

**Шаг 6:** Следует вопрос о корректности введенных данных: "Is the above data correct?" После получения подтверждения инициализация продолжается без дополнительных вопросов. Если подтверждение не получено, то предлагается ввести Лицензию еще раз.

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.

Драйвер Продукта CSP VPN Gate установлен на все обнаруженные сетевые интерфейсы.

Программный комплекс CSP VPN Gate установлен в каталог **/opt/VPNagent**.

При инициализации CSP VPN Gate устанавливается политика

**Default Driver Policy = Passdhcp**, при которой интерфейсы шлюза безопасности пропускают только пакеты DHCP и в незащищенном виде.

Для входа в Cisco-like интерфейс командной строки нужно использовать имя пользователя "cscons" (начальный пароль "csp"). А для входа в ОС предназначено имя "root" (изначально без пароля).

Графический интерфейс Web-based GUI не был установлен вместе с CSP VPN Gate. Установка графического интерфейса описана в документе [«Web-based интерфейс управления: инструкция по установке и использованию»](#).

Сразу после инициализации программного комплекса автоматически запускается утилита `cspvpn_verify` для проверки целостности установленного Продукта CSP VPN Gate, которая описана в документе [«Специализированные команды»](#). При нарушении целостности восстановите содержимое жесткого диска ПАК из образа жесткого диска, который входит в комплект поставки. Выполните эту процедуру согласно документу – [«Инструкция по восстановлению ПАК и замены компакт-флеш карты на модуле»](#).

Далее перейдите к настройке шлюза безопасности, описанной в документе [«Настройка шлюза»](#).

## Переключение консоли на последовательный порт или монитор и клавиатуру

Для переключения вывода консоли рекомендуется использовать скрипт `consoleswitch`, а не редактировать соответствующие конфигурационные файлы ОС.

Для настройки вывода консоли на монитор и клавиатуру выполните команду:

```
consoleswitch keyboard
```

Для настройки вывода консоли в последовательный порт выполните команду:

```
consoleswitch serial [baud[,parity[,bits]]]
```

где

дополнительными настройками порта являются (через запятую, без пробелов):

`baud` - скорость

`parity` - четность

`bits` - биты данных.

По умолчанию установлены следующие значения – 115200,n,8.

На какой именно последовательный порт происходит переключение, зависит от настройки ОС:

в Solaris 10 – `ttya` для COM1, `ttyb` для COM2 и т.д.

в Red Hat Enterprise Linux 5 (CentOS 5) – `ttyS0` для COM1, `ttyS1` для COM2 и т.д.

При вызове без параметров или с неверными параметрами, скрипт выводит краткое описание параметров запуска.

При возникновении ошибки, скрипт выдает сообщение:

```
error: can not set system console.
```

После выполнения команды `consoleswitch` выключите питание, переключите оборудование, запустите систему.