ООО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, Георгиевский проспект,
дом 5, помещение I, комната 33
Телефон/Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com
Сайт: http://www.s-terra.com

Программный комплекс С-Терра Шлюз. Версия 4.1

Руководство администратора

Инициализация S-Terra Gate на вычислительных системах архитектуры Intel x86/x86-64

РЛКЕ.00009-01 90 03

27.04.2015

Содержание

Инициализация S-Terra Gate на вычислительных системах архитектуры Intel x86/x86-64

В этом разделе описана инициализация «Программного комплекса С-Терра Шлюз. Версия 4.1» (S-Terra Gate) на вычислительных системах архитектуры Intel x86/x86-64.

Программный комплекс поставляется в инсталлированном состоянии.

На ПАК установлены:

- ОС Debian GNU/Linux 6 (32-bit или 64-bit),
- S-Terra Gate,
- «КриптоПро CSP 3.6R4/3.9» (в случае использования СКЗИ «КриптоПро CSP»).

Подготовка программно-аппаратного комплекса к инициализации

В качестве терминала для аппаратной платформы (АП), на которой установлен Продукт S-Terra Gate, можно использовать:

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

Подготовка ПАК исполнения класса защиты КС1 к инициализации

Шаг 1: К АП, с установленным Продуктом S-Terra Gate 3000/7000, а также к АП Kraftway Credo VV22 и Kraftway Credo VV23, с установленным Продуктом S-Terra Gate 100/100B/100V/1000/1000V, подключите к разъемам монитор и клавиатуру в качестве терминала и перейдите к Шагу 2.

К АП, с установленным Продуктом S-Terra Gate 100/100B/100V/1000/1000V, подключите к последовательному порту компьютер в качестве терминала, используя нуль-модемный кабель (5 проводов):

для АП TONK 1800 подключить следует к COM2-порту
для остальных АП – к COM1-порту.

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.

Укажите, что будет использоваться в качестве терминала для аппаратной платформы (Рисунок 1):

`S-Terra Gate` – монитор и клавиатура
или
`S-Terra Gate (serial)` – компьютер, подключенный к последовательному порту АП

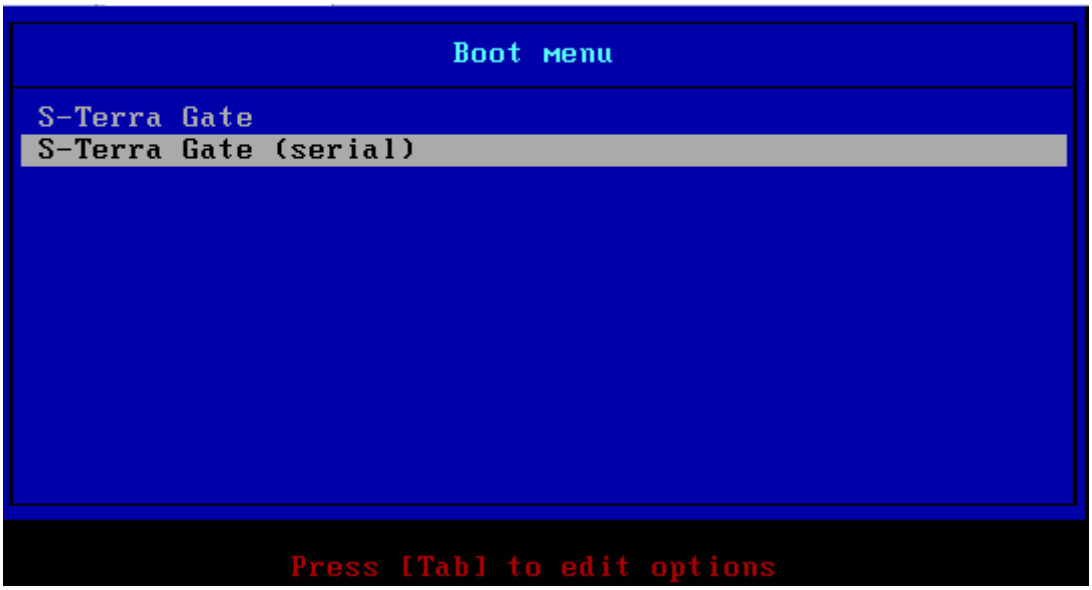

Рисунок 1

Шаг 3: После загрузки ОС войдите в систему

имя пользователя – `root`
пароль – пустой.

Шаг 4: Выполните процедуру инициализации программного комплекса S-Terra Gate, описанную в разделе «Инициализация S-Terra Gate при первом старте».

Подготовка ПАК исполнения класса защиты КС2 с АПМДЗ к инициализации

Для защиты от несанкционированного доступа к АП могут использоваться следующие аппаратно-программные модули доверенной загрузки (АПМДЗ): ПАК «Соболь», «Аккорд-АМДЗ», «КРИПТОН-ЗАМОК», «Тринити АПМДЗ», «МАКСИМ-М1». Если на АП не установлена плата АПМДЗ, необходимо её подключить и инициализировать, руководствуясь эксплуатационной документацией на АПМДЗ.

Шаг 1: К АП, с установленным Продуктом S-Terra Gate 3000/7000, подключите к разъемам монитор и клавиатуру в качестве терминала и перейдите к Шагу 2.

К АП, с установленным Продуктом S-Terra Gate 100/100B/100V/1000/1000V, подключите к последовательному порту компьютер в качестве терминала, используя нуль-модемный кабель (5 проводов):

для АП TONK 1800 подключить следует к COM2-порту,
для остальных АП – к COM1-порту.

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: При необходимости подключите внешний считыватель идентификаторов к разъему АПМДЗ.

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

Шаг 4: При появлении на экране запроса от АПМДЗ предъявите идентификатор:

Выполните необходимые настройки в соответствии с руководством администратора АПМДЗ.

Шаг 5: Укажите, что будет использоваться в качестве терминала для аппаратной платформы (Рисунок 1):

`S-Terra Gate` – монитор и клавиатура
или
`S-Terra Gate (serial)` – компьютер, подключенный к последовательному порту АП

Шаг 6: После загрузки ОС войдите в систему

имя пользователя – `root`
пароль – пустой.

Шаг 7: Выполните процедуру инициализации программного комплекса S-Terra Gate, описанную в разделе «Инициализация S-Terra Gate при первом старте».

Подготовка ПАК исполнения класса защиты КС2 с СЗН «СПДС-USB-01» к инициализации

Шаг 1: К АП, с установленным Продуктом S-Terra Gate 3000/7000, а также к АП Kraftway Credo VV22 и Kraftway Credo VV23, с установленным Продуктом S-Terra Gate 100/100B/100V/1000/1000V, подключите к разъемам монитор и клавиатуру в качестве терминала и перейдите к Шагу 2.

В остальных случаях, к АП, с установленным Продуктом S-Terra Gate, подключите к разъемам монитор и клавиатуру в качестве терминала или подключите к последовательному порту компьютер в качестве терминала, используя нуль-модемный кабель (5 проводов):

для АП TONK 1800 подключить следует к COM2-порту,
для остальных АП – к COM1-порту.

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: В случае внешнего подключения СЗН «СПДС-USB-01» к АП (в этом случае СЗН «СПДС-USB-01» входит отдельно в комплект поставки и на АП наклеен стикер с текстом «перед началом работы следует подключить СПДС-USB-01») подсоедините СЗН напрямую или при помощи кабеля к внешнему USB-порту АП.

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

Шаг 4: Убедитесь, что BIOS ПЭВМ настроен на загрузку ОС с USB-устройства.

Шаг 5: Укажите, что будет использоваться в качестве терминала для аппаратной платформы:

- `S-Terra SPDS-USB Gate` – монитор и клавиатура.
- `S-Terra SPDS-USB Gate (serial_0)` – компьютер, подключенный к последовательному порту COM1 АП.
- `S-Terra SPDS-USB Gate (serial_1)` – компьютер, подключенный к последовательному порту COM2 АП.

Для устройств DEPO Neos 220USF и TONK 1800, чтобы работать через serial-порт, нужно выбрать пункт `S-Terra SPDS-USB Gate (serial_1)`, а для остальных устройств, работающих через serial-порт нужно выбирать `S-Terra SPDS-USB Gate (serial_0)`.

Шаг 6: Во время загрузки ОС в течение 5 секунд есть возможность войти в режим администратора СПДС-USB-01. На терминале появляется подсказка –
Press 'a' to enter to SPDS-USB Administrator mode
or Esc to continue OS loading
OS will continue loading in 5 seconds...

Нажмите клавишу 'a' и войдите режим администратора.

При входе в административный режим требуется ввести PIN администратора (изначально PIN администратора и PIN пользователя – 12345678). После процедуры аутентификации будет выведено меню с

выбором возможных действий, требующих административного права доступа к СЗН «СПДС-USB-01»:
1. To change SPDS-USB Administrator's PIN – изменение PIN администратора СПДС-USB-01.
2. To unblock SPDS-USB User's PIN – восстановление PIN пользователя СПДС-USB-01.
3. To SPDS-USB image recovery – восстановление образа СПДС-USB-01 с внешнего носителя (подробное описание восстановления образа СПДС-USB-01 описано в документе «Инструкции по восстановлению и обновлению ПАК», в разделе «Инструкция по восстановлению ПАК с S-Terra Gate, предустановленным на СЗН «СПДС-USB-01»).
4. To continue OS loading – продолжение загрузки ОС в пользовательском режиме.

Измените PIN администратора и PIN пользователя. Длина пароля администратора должна быть не менее 8 символов, пользователя – не менее 4 символов (подробнее см. документ «Настройка шлюза», раздел «Изменение или восстановление PIN для СЗН «СПДС-USB-01»).

Войти в режим администратора СЗН «СПДС-USB-01» и выполнить описанные выше действия можно после каждой перезагрузки ОС.

Шаг 7: При продолжении загрузки ОС в режиме пользователя появится запрос PIN пользователя СЗН «СПДС-USB-01»:

```
Enter User's PIN:
```

Введите PIN пользователя..

Шаг 8: После загрузки ОС войдите в систему:

имя пользователя – `root`
пароль – пустой.

Шаг 9: Выполните процедуру инициализации программного комплекса S-Terra Gate, описанную в разделе «Инициализация S-Terra Gate при первом старте».

Подготовка ПАК исполнения класса защиты КС3 к инициализации

При исполнении класса защиты КС3, кроме защиты от несанкционированного доступа и обеспечения доверенной загрузки, разграничиваются права доступа пользователей к ОС и настройке программного комплекса.

Шаг 1: Подготовьте программно-аппаратный комплекс класса защиты КС3 к инициализации S-Terra Gate аналогично, описанному выше для класса защиты КС2.

Отличие состоит в том, что для входа в систему используйте

имя пользователя – `administrator`
пароль – `s-terra`

Шаг 2: Войдите в режим настройки системы, выполнив команду:

```
cspgate# system
```

Шаг 3: Выполните процедуру инициализации программного комплекса S-Terra Gate, описанную в разделе «Инициализация S-Terra Gate при первом старте»

Шаг 4: Произведите необходимые настройки, описанные в разделе «Разграничение доступа».

Инициализация S-Terra Gate 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 S-Terra Gate.

Шаг 1: Запустите скрипт /opt/VPNagent/bin/init.sh для старта процедуры начальной инициализации S-Terra 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: Выполняется только в случае использования СКЗИ «КриптоПро CSP»

Запрашивается серийный номер лицензиии 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», входящей в комплект поставки, например: DU36X-D00GR-XXXXX-XXXXX-XXXXX. Не путайте «0» (ноль) и букву «О».

При вводе неверного номера лицензии предлагается ввести его еще раз.

Шаг 3: Инициализируется ДСЧ:

Для исполнений класса защиты КС1 проводится «биологическая» инициализация начального значения ДСЧ.

Для исполнений класса защиты КС2 и КС3 инициализация начального значения ДСЧ выполняется без участия пользователя.

Шаг 4: Далее запрашивается лицензионная информация на S-Terra Gate (эти данные можно взять из «Лицензии на использование программного продукта компании ЗАО «С-Терра СиЭсПи», входящей в комплект поставки):

You have to enter license for S-Terra 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: – 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 5: 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.

Шаг 6: Далее запускается vpn-демон (в случае исполнения Продукта класса защиты КС3, vpn-демон запускаться не будет), 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 S-Terra Gate установлен на все обнаруженные сетевые интерфейсы.

Программный комплекс S-Terra Gate установлен в каталог `/opt/VPNagent`.

При инициализации S-Terra Gate устанавливается политика безопасности, при которой интерфейсы шлюза безопасности не пропускают пакеты – `Default Driver Policy = Dropall` (в релизе 14101 устанавливается политика безопасности `Passdhcp`, при которой интерфейсы шлюза безопасности пропускают только пакеты DHCP и в незащищенном виде). 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.
```

В случае исполнения Продукта класса защиты КС1 и КС2:

- 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).

В случае исполнения класса защиты КС3 администратор, для разграничения прав пользователей на доступ к операционной системе и управление программным комплексом, должен разделить пользователей на привилегированных и непривилегированных и установить для них пароли. Подробнее описано в разделе «Разграничение доступа».

Сразу после инициализации программного комплекса, в случае исполнения Продукта класса защиты КС1 и КС2, автоматически запускается утилита `cspvpn_verify` для проверки целостности установленного Продукта S-Terra 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 – «Инструкции по восстановлению и обновлению ПАК».

Далее перейдите к настройке S-Terra Gate, описанной в документе «Настройка шлюза».

Разграничение доступа

Разграничение прав доступа пользователей к операционной системе и управлению программным комплексом выполняется на этапе аутентификации в исполнениях Продукта класса защиты КС3.

В зависимости от уровня доступа, пользователь может быть привилегированным (администратор) и непривилегированным (пользователь с ограниченными возможностями). После аутентификации, в зависимости от уровня, каждый пользователь может выполнять свой определенный набор команд (см. «Команды уровня администратора», «Команды уровня пользователя»).

При аутентификации у пользователя запрашивается пароль и проверяется доступ по этому паролю к контейнеру с секретным ключом (имя пользователя связано с именем контейнера и уровнем доступа в конфигурационном файле). Эти действия выполняются специальной утилитой `auth_login`.

Изначально в конфигурационном файле `/opt/VPNagent/etc/auth_login.ini` присутствует пользователь `administrator`, для которого указан контейнер с секретным ключом (пароль к контейнеру – `s-terra)`. Измените пароль к контейнеру с ключевой парой, пересоздав заново контейнер.

Для разграничения прав доступа пользователей к операционной системе и управлению программным комплексом выполните следующие действия:

1. Создайте для пользователей контейнеры с секретными ключами, защищенные паролем.
2. Выполните необходимые настройки в конфигурационном файле auth_login.ini, где для каждого пользователя укажите уровень доступа и имя контейнера, а также некоторые дополнительные параметры (см. раздел «Настройки конфигурационного файла»).

Создание контейнеров с секретными ключами

В случае применения СКЗИ «КриптоПро CSP», для создания контейнера можно использовать утилиту `csptest` (утилита находится в каталоге `/opt/cprocsp/bin/ia32` или `/opt/cprocsp/bin/amd64)`, например:

```
csptest -keyset -newkeyset -container 'HDIMAGE\\contadmin' -machinekeyset
-password 123456
```

В случае применения криптобиблиотеки, разработанной компанией «С-Терра СиЭсПи», для создания контейнера используйте утилиту `cont_mgr` (описание утилиты приведено в документе «Специализированные команды»). Пример:

```
/opt/VPNagent/bin/cont_mgr create -cont contadmin –PIN 123456
```

Если для используемого АПМДЗ не поддерживается функциональность ДСЧ, то возможны различные варианты создания контейнеров с секретными ключами, в зависимости того, какая криптографическая библиотека применяется в «С-Терра Шлюз». Для «С-Терра Шлюз» со встроенной криптобиблиотекой компании «С-Терра СиЭсПи», при генерации ключевой пары и создании контейнера возможно применение биологического ДСЧ. Для «С-Терра Шлюз» с СКЗИ «КриптоПро CSP» возможны два варианта:

1. Администратор, используя СКЗИ «КриптоПро CSP», может создать контейнеры на своем рабочем месте и затем доставить их на «С-Терра Шлюз».

   Для создания контейнера используйте утилиту `csptest` (пример см. выше).

Выполните копирование контейнера с секретным ключом с одного ключевого носителя на другой следующей командой, например:

```
csptest -keycopy -machinekeyset -src '\\.\media\src_cont' -dest
'\\.\media\dst_cont'
```

Если на «С-Терра Шлюз» применяется криптобиблиотека от компании «С-Терра СиЭсПи», доставленные контейнеры нужно конвертировать с помощью команды `cpkey_conv` (описание утилиты приведено в документе «Специализированные команды»).

2. Администратор, используя СКЗИ «КриптоПро CSP» (класс защиты КС2/КС3) и электронный замок «Соболь», может изготовить внешнюю гамму, доставить ее безопасным способом на «С-Терра Шлюз» и затем, используя утилиту `csptest` или `cont_mgr`, как это описано выше, создать на «С-Терра Шлюз» контейнеры с секретными ключами.

   Для изготовления внешней гаммы в командной строке запустите утилиту `genkpim`, например:

   ```
   genkpim.exe 500 12121111 f:\gamma
   ```

   `500` – необходимое количество случайных отрезков гаммы для записи на носитель,

   `12121111` – номер комплекта внешней гаммы (8 символов в 16-ричном коде),

   `f:\gamma` – путь на носителе, по которому будет записан файл с внешней гаммой.

   В результате выполнения команды создается файл `kis_1`, который записывается на носитель по пути `f:\gamma` дублированием в два каталога: `DB1` и `DB2`.

   Далее действия будут различаться в зависимости от используемого СКЗИ:

   - В случае использования СКЗИ «КриптоПро CSP», выполните копирование файлов с внешней гаммой с носителя на «С-Терра Шлюз» в следующие каталоги: `/var/opt/cprocsp/dsrf/db1/` и `/var/opt/cprocsp/dsrf/db2/` соответственно.
   - В случае использования криптобиблиотеки от компании «С-Терра СиЭсПи», выполните копирование одного файла с внешней гаммой с носителя на «С-Терра Шлюз», в каталог /var/s-terra/ext-gamma. Переименуйте файл с внешней гаммой в `eg_data`.
     В конфигурационном файле /etc/S-Terra/skzi.conf пропишите путь до каталога с внешней гаммой:

     ```
     ExtGammaPath=/var/s-terra/ext-gamma
     ```

   Надёжно удалите файлы с внешней гаммой с носителя. После этого перезагрузите «С-Терра Шлюз» и создайте контейнеры с секретными ключами.

Настройки конфигурационного файла

Настройки утилиты `auth_login` выполняются в конфигурационном файле `/opt/VPNagent/etc/auth_login.ini`, представляющем обычный текстовый файл.

Строки, начинающиеся с восклицательного знака (!), считаются комментариями и игнорируются. Пустые строки игнорируются.

В начале файла идут опциональные глобальные настройки, а затем – секции.

Глобальные настройки – автологин

Задается глобальный параметр – автологин. Для выполнения автологина необходимо, чтобы далее в настройках присутствовал администратор (пользователь с параметром `role=admin`), у которого указан пустой пароль. Этот администратор должен быть первым по счету.

`autostart={ on | off }`

`on`	автологин включен. При первом старте утилиты делается попытка выполнить автологин.
`off`	автологин отключен (значение по умолчанию).

Секции

В каждой секции задаются параметры отдельного пользователя.

```
[<section_name>]
<param_name>=<param_val>
```

где

`<section_name>`	имя секции задает имя пользователя,
`<param_name>`	имя параметра,
`<param_val>`	значение параметра.

Возможные параметры:

`role={ admin | user }`

`admin`	администратор
`user`	пользователь (значение по умолчанию)

`container=<container_name>`

`container_name`	имя контейнера, к которому производится проверка доступа. Обязательный параметр.

`public_key=<public_key_file_path>`

`public_key_file_path`	путь к файлу с публичным ключом. Опциональная защита от подмены контейнера: проверка подписи с использованием публичного ключа, сохраненного отдельно от контейнера. При отсутствии параметра – подпись не проверяется.

Для экспорта публичного ключа из контейнера в файл, при использовании СКЗИ «КриптоПро CSP», выполните команду `csptest` (`csptest` находится в каталоге `/opt/cprocsp/bin/ia32` или `/opt/cprocsp/bin/amd64`), например:

```
csptest -keyset -container '<container_name>' -keytype signature
-machinekeyset -export <public_key_file_path>
```

Примечание: если в контейнере присутствует только ключ типа exchange, следует заменить в команде `-keytype signature` на `-keytype exchange`.

Экспортировать публичный ключ из контейнера в файл, при использовании криптобиблиотеки, разработанной компанией «С-Терра СиЭсПи», можно командой:

```
/opt/VPNagent/bin/cont_mgr export -cont <container_name> -PIN
<container_password> -ext <public_key_file_path>
```

`config_user=<cs_console_user>`

`cs_console_user`	пользователь ОС, от имени которого происходит вход в режим конфигурирования

(запуск cs_console). Имеет смысл только для администратора. Пользователь <cs_console_user> обязательно должен присутствовать в ОС и иметь cs_console в качестве Shell. При отсутствии параметра делается попытка подставить имя администратора в качестве <cs_console_user>. Если <cs_console_user> отсутствует в ОС или его Shell отличен от cs_console, cs_console запускается от имени пользователя `root`.

Пример конфигурационного файла

Ниже приведен пример файла `auth_login.ini` в случае применения СКЗИ «КриптоПро CSP».

```
! This is a comment

autostart=on

[admin]
role=admin
container=HDIMAGE\\admincont
public_key=/opt/VPNagent/etc/admincont_public_key
config_user=cscons

[user]
role=user
container=HDIMAGE\\usercont
public_key=/opt/VPNagent/etc/usercont_public_key
```

Пример конфигурационного файла при использовании криптобиблиотеки, разработанной компанией «С-Терра СиЭсПи».

```
! This is a comment

autostart=on

[admin]
role=admin
container=file://admincont
public_key=/opt/VPNagent/etc/admincont_public_key
config_user=cscons

[user]
role=user
container= file://usercont
public_key=/opt/VPNagent/etc/usercont_public_key
```


Описание работы утилиты

При старте утилита `auth_login` пишет свое название:

```
S-Terra Gate administrative console.
```

Если утилита запускается первый раз после рестарта системы и разрешен автологин, то для первого, присутствующего в настройках конфигурационного файла администратора, проверяется доступ по пустому паролю к его контейнеру с секретным ключом. При успешной проверке запускается сервис безопасности:

```
Performing autostart as user <admin_name>
Configuring IPsec driver:
Starting IPsec daemon...done.
Autostart finished
```

Если автологин не разрешен, то запрашивается имя пользователя (пустое имя пользователя не допускается – в этом случае выдается повторный запрос):

```
login as:
```

Далее запрашивается пароль (пустой пароль допускается):

```
<name>'s password:
```

Производится проверка, не заблокирован ли данный пользователь (подробнее см. подраздел «Ограничение на количество попыток входа в систему»). На данном этапе может быть выдано сообщение:

```
% The maximum number of login attempts for user <name> has been reached.
User has been blocked
```

Сообщение может появиться .в следующих случаях:

- Реальный пользователь (описанный в файле `/opt/VPNagent/etc/auth_login.ini`) ранее исчерпал допустимые попытки входа в систему и теперь заблокирован.
- Попытка входа в систему неизвестным (не описанным в файле `/opt/VPNagent/etc/auth_login.ini`) пользователем.
- Поврежден (имеет некорректный формат) файл, в котором хранится количество оставшихся попыток входа в систему данного пользователя.
- Системная ошибка (не удалось прочитать или записать количество оставшихся попыток).

Пользователь не может отличить эти ситуации. Однако в логе, доступном администратору, эти ситуации можно различить по коду ошибки в сообщении.

Производится проверка полученного имени и пароля. Если проверка не пройдена:

Выполняется остановка исполнения на промежуток времени от 1 до 3 секунд.

На консоль выдается сообщение об ошибке:

```
% Access denied
```

Если у пользователя еще остались допустимые попытки входа в систему, выдается сообщение об их количестве:

```
% You have <n> attempt(s) left
```

где <n> – число оставшихся попыток (от 1 до 9).

Если была использована последняя попытка входа в систему, выдается сообщение о блокировке пользователя:

```
% The maximum number of login attempts for user <name> has been
reached. User has been blocked
```

Выполняется остановка исполнения на 1 секунду.

ОС автоматически перезапускает утилиту для повторения попытки аутентификации.

При использовании криптобиблиотеки компании «С-Терра СиЭсПи», при проверке полученного имени и пароля, возможно отсутствие инициализированного ДСЧ (например, при первом входе в систему). В этом случае:

На консоль выдается сообщение:

```
RNG initialization is required. Press Enter to continue...
```

Когда пользователь нажимает на `Enter`, запускается программа `rnd_mgr`. Происходит инициализация ДСЧ:

Если присутствует соответствующая аппаратная поддержка (например «Соболь») или если присутствует внешняя гамма, инициализация проходит неинтерактивно.

В противном случае вызывается интерактивная инициализация.

После успешной инициализации на консоль выдается сообщение от утилиты:

```
Successfully initialized RNG.
```

В случае успешной аутентификации пользователь получает доступ к определенному набору команд. Пользователю выдается приглашение командного интерпретатора, вид которого зависит от уровня доступа пользователя:

для администратора: `hostname#`

для пользователя: `hostname>`

где

`hostname` – имя хоста, на котором работает программа.

Ключевые слова команд можно сокращать до того количества символов, при котором их можно однозначно идентифицировать.

При выполнении команд (включая `configure`) работают специальные сочетания клавиш:

Прерывание выполнения запущенного процесса: CTRL+^ (CTRL+SHIFT+6). При работе через консоль Cisco IOS (стандартный режим работы программы) следует нажать указанное сочетание клавиш два раза, поскольку Cisco IOS перехватывает CTRL+^.

Если указанное выше сочетание клавиш не работает (например, внешний процесс завис), можно нажать на CTRL+| – в этом случае будет послан SIGKILL – неперехватываемый сигнал, по которому выполнение внешней программы безусловно прекращается.

Поддерживаются специальные команды редактирования командной строки, аналогичные Cisco-like консоли (см. документ «Cisco-like команды»).

Ограничение на количество попыток входа в систему

Для каждого пользователя допускается 10 попыток входа в систему. Если все попытки входа в систему оказываются неуспешными, пользователь блокируется. При успешном входе в систему количество оставшихся попыток входа в систему возвращается к своему начальному значению (10).

Счетчик допустимого количества попыток входа в систему хранится в файле: `/var/cspvpn/auth_login_count.<name>`, где `<name>` – имя пользователя.

Отсутствие файла обозначает, что допускаются 10 попыток входа в систему.

Файл будет создан при первой попытке входа соответствующим пользователем. Пользователь должен быть описан в конфигурационном файле `/opt/VPNagent/etc/auth_login.ini`. Для неизвестного пользователя, отсутствующего в файле `auth_login.ini`, файл со счетчиком не создается.

Администратор может разблокировать пользователя, удалив соответствующий файл со счетчиком (`/var/cspvpn/auth_login_count.<name>`). **Примечание: если будут заблокированы все администраторы, вход в систему будет невозможен**.

Формат файла `/var/cspvpn/auth_login_count.<name>` – бинарный (owner – root, group – root, mode – 0600). Длина файла – 1 байт. В этом байте в виде числа хранится количество оставшихся попыток входа в систему.

Если в файле хранится число 0 –- это обозначает, что пользователь заблокирован. Если файл имеет неправильный формат (длина отлична от 1 или прочитанное число больше 10), то пользователь также фактически заблокирован. Отличить данную ситуацию от предыдущей можно по коду ошибки (см. раздел «Протоколирование событий», Таблица 2).

Команды уровня администратора

Вход в режим настройки системы (запуск системного shell):

`system`

Команда необходима для начальной настройки системы и в аварийных ситуациях. В остальных случаях рекомендуется пользоваться командой

`configure`

Сначала на консоль выдается сообщение:

```
Entering system shell...
```

Далее запускается интерактивная сессия системного shell.

При выходе из системного shell выдается сообщение:

```
Leaving system shell...
```

При необходимости аварийного завершения выполнения системного shell можно использовать сочетания клавиш `CTRL+^ (CTRL+SHIFT+6)` или `CTRL+|`.

Запуск сервиса безопасности (аналогично `/etc/init.d/vpngate start`):

`start`

Остановка работы системы. Сначала останавливается сервис безопасности, затем происходит останов ОС:

`stop`

Перезагрузка системы. Сначала останавливается сервис безопасности, затем происходит перезагрузка ОС:

`reboot`

Вход в режим настройки S-Terra Gate (запуск cs_console – Cisco-like интерфейс командной строки):

`configure`

Если заданный в настройках пользователь, под которым должен производиться вход в конфигурационный режим, отсутствует в ОС или его Shell отличается от `cs_console`,

cs_console запускается от имени пользователя root с выдачей предупреждения в лог и на консоль:

```
% Warning: configuring as user root. Check the 'config_user' setting
in /opt/VPNagent/etc/auth_login.ini
```

Сначала на консоль выдается сообщение:

```
Entering cs_console...
```

Далее запускается cs_console.

При выходе из cs_console выдается сообщение:

```
Leaving cs_console...
```

Следует учитывать, что приглашения командного интерпретатора cs_console аналогичны приглашениям командного интерпретатора программы. Для того чтобы их отличать, рекомендуется ориентироваться на приведенные выше сообщения.

При необходимости аварийного завершения выполнения cs_console можно использовать сочетания клавиш CTRL+^ (CTRL+SHIFT+6) или CTRL+|

Администратору также доступны команды уровня пользователя.

Команды уровня пользователя

Выдача версии продукта (аналогична запуску утилиты /opt/VPNagent/bin/vershow):

```
show version
```

Выдача информации о текущей конфигурации (аналогична запуску утилиты /opt/VPNagent/bin/lsp_mgr show):

```
show config
```

Выдача текущей информации о статусе защиты (аналогична запуску утилиты /opt/VPNagent/bin/sa_mgr show):

```
show status
```

Выход из утилиты приведет к перезапуску утилиты и запросу имени пользователя:

```
exit
```

Сообщения об ошибках при вводе команд

При вводе синтаксически неправильной команды выдается сообщение об ошибке следующего вида:

```
          ^
% Invalid input detected at '^' marker
```

Маркер '^' указывает на первый ошибочный символ, встреченный при разборе строки.

Если введена незавершенная команда, то выдается сообщение:

```
% Incomplete command
```

Если введена команда, допускающая неоднозначное толкование (как правило, из-за чрезмерного сокращения ключевых слов), выдается сообщение:

```
Ambiguous command: "<введенная_команда>"
```


Протоколирование событий

В процессе работы выдаются сообщения в syslog с использованием `facility=authpriv`.

Список сообщений приведен в Таблица 1.

Таблица 1

Severity	Сообщение	Пояснение
err	% Error: failed to read settings from /opt/VPNagent/etc/auth_login.ini	Не удалось прочитать настройки программы. Отсутствует или испорчен файл. Программа аварийно завершается.
err	% Error: failed to set the root identity	Не удалось выставить идентификатор пользователя root. В нормальной ситуации не должно возникать. Программа аварийно завершается.
err	% Internal error: parser initialization failed	Внутренняя ошибка: проблемы с инициализацией парсера. В нормальной ситуации не должно возникать. Программа аварийно завершается..
err	% Error: failed to read the command list from /opt/VPNagent/etc/auth_login_cmd.xml	Не удалось прочитать базу команд. Отсутствует или испорчен файл. Программа аварийно завершается.
err	Autostart failed	Не удалось выполнить автологин.
info	Autostart failed. Error code: <err_code>	Не удалось выполнить автологин. Выдается вместе с предыдущим сообщением, но с использованием severity=info. Система должна быть настроена так, чтобы сообщения с уровнем info не были доступны не идентифицированному пользователю.
err	Attempt to login as user <name> failed	Не пройдена проверка имени оператора и пароля.
info	Attempt to login as user <name> failed. Error code: <err_code>	Не пройдена проверка имени оператора и пароля. Выдается вместе с предыдущим сообщением, но с использованием severity=info. Система должна быть настроена так, чтобы сообщения с уровнем info не были доступны не идентифицированному пользователю.
err	Failed to set the autostart marker	Не удалось выставить признак выполненного автологина. Может приводить к тому, что попытка выполнения автологина будет делаться при каждом старте утилиты (неопасная

		ситуация). В нормальной ситуации не должно возникать.
notice	User <name> logged in	Оператор с именем <name> успешно получил доступ.
notice	Autostart performed as user <name>	Автологин выполнен успешно от имени оператора <name>.
notice	User <name> called command: <command>	Оператор <name> выполнил команду <command>
notice	User <name> logged out	Оператор <name> вышел из программы
warning	% Warning: configuring as user root. Check the 'config_user' setting in /opt/VPNagent/etc/auth_login.ini	Конфигурирование (запуск cs_console) выполняется от имени пользователя root. Проверьте настройку config_user в файле.

В сообщениях с уровнем info, говорящих об ошибке аутентификации (попытка автологина или входа оператора) пишется код ошибки. Возможные сообщения приведены в Таблица 2.

Таблица 2

Код ошибки	Пояснение
1	В настройках отсутствует администратор (только для сообщения "Autostart failed").
2	Неизвестное имя оператора (отсутствует в настройках; только для сообщения "Attempt to login as user <name> failed").
3	Контейнер не найден.
4	Не удалось загрузить публичный ключ (public_key ссылается на несуществующий или ошибочный файл).
5	Не удалось подписать тестовые данные. Наиболее вероятная причина - введен неправильный пароль.
6	Не удалось проверить подпись. Наиболее вероятные причины - подмененный контейнер или ошибочный публичный ключ.
7	Не удалось получить из контейнера подходящий ключ для подписи тестовых данных.
8	Криптографическая проблема. Наиболее вероятные причины – «КриптоПро» не установлено, не зарегистрировано или нарушена его целостность.
9	Пользователь исчерпал допустимые попытки входа в систему и теперь заблокирован.
10	Поврежден (имеет некорректный формат) файл, в котором хранится количество оставшихся попыток входа в систему данного пользователя или Системная ошибка (не удалось прочитать или записать количество оставшихся попыток).

Сообщения, выдаваемые на консоль

Список сообщений выдаваемых на консоль приведен в Таблица 3.

Таблица 3

Сообщение	Тип	Дублируется в syslog	Пояснение
S-Terra Gate administrative console	информационное		Стартовое сообщение.
Performing autostart as user <admin_name>	информационное		Начало автологина.
Autostart finished	информационное		Завершение автологина.
% Error: failed to read settings from /opt/VPNagent/etc/auth_login.ini	ошибка	+	Не удалось прочитать настройки из файла.
% Error: failed to set the root identity	ошибка	+	Не удалось выставить идентификатор пользователя root.
% Internal error: parser initialization failed	ошибка	+	Внутренняя ошибка: проблемы с инициализацией парсера.
% Error: failed to read the command list from /opt/VPNagent/etc/auth_login_cmd.xml	ошибка	+	Не удалось прочитать базу команд.
% Warning: configuring as user root. Check the 'config_user' setting in /opt/VPNagent/etc/auth_login.ini	предупреждение	+	Конфигурирование (запуск cs_console) выполняется от имени пользователя root. Проверьте настройку config_user в файле.
% Access denied	ошибка		Отказ в доступе.
% System error, can not spawn process.	ошибка		Не удалось породить новый процесс.
% System error, can not run external application.	ошибка		

% System error, can not create pipe.	ошибка		В нормальной ситуации не должно возникать.
% System error, input redirection to child process failed. Error code: <errno>	ошибка		Не удалось запустить внешнее приложение.
% Warning: Terminal setup failed. Interactive applications could be broken.	ошибка		
Entering cs_console...	информационное		В нормальной ситуации не должно возникать. Возможно не установлен продукт или нарушена его целостность.
Leaving cs_console...	информационное		Системная ошибка.
RNG initialization is required. Press Enter to continue...	информационное		Требуется инициализация ДСЧ. Нажмите Enter для продолжения... (При использовании криптобиблиотеки компании «С-Терра СиЭсПи»)

