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

Программный комплекс CSP VPN Gate. Версия 3.11

Руководство администратора

Инициализация CSP VPN Gate при использовании СКЗИ «КриптоПро CSP 3.6R2»

РЛКЕ.00005-02 90 03

18.05.2015

Содержание

Инициализация CSP VPN Gate при использовании СКЗИ «КриптоПро CSP 3.6R2»

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

Программно-аппаратный комплекс поставляется в инсталлированном состоянии: установлены ОС Red Hat Enterprise Linux 5 или CentOS 5 или Crossbeam Systems Linux 9, продукты CSP VPN Gate, СКЗИ «КриптоПро CSP 3.6R2» или СКЗИ «КриптоПро CSP 3.6».

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.

Исполнения класса защиты КС1

Шаг 1: К АП, на которой установлен CSP VPN Gate 3000/7000, а также к АП Kraftway Credo VV22 и Kraftway Credo VV23, на которых установлен CSP VPN Gate 100/100B/100V/1000/1000V, подключите к разъемам монитор и клавиатуру в качестве терминала и перейдите к Шагу 2.

К АП, на которой установлен CSP VPN 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.

Шаг 3: После загрузки ОС войдите в систему

имя пользователя – `root`
пароль – пустой.

Шаг 4: При необходимости переключить ввод/вывод с последовательного порта на монитор и клавиатуру или наоборот, воспользуйтесь скриптом `consoleswitch` (см. раздел «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

имя пользователя – `root`
пароль – пустой.

Шаг 5: Выполните процедуру инициализации программного комплекса CSP VPN Gate, описанную в разделе «Инициализация CSP VPN Gate при первом старте».

Исполнения класса защиты КС2 с АПМДЗ

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

Шаг 1: К АП, на которой установлен CSP VPN Gate 3000/7000, подключите к разъемам монитор и клавиатуру в качестве терминала и перейдите к Шагу 2.

К АП, на которой установлен CSP VPN 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.

Загрузите операционную систему.

Шаг 5: После загрузки ОС войдите в систему

имя пользователя – `root`
пароль – пустой.

Шаг 6: При необходимости переключить ввод/вывод с последовательного порта на монитор и клавиатуру или наоборот, воспользуйтесь скриптом `consoleswitch` (см. раздел «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

имя пользователя – `root`
пароль – пустой.

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

Исполнения класса защиты КС2 с СЗН СПДС-USB-01

Шаг 1: К АП, на которой установлен CSP VPN Gate 3000/7000, а также к АП Kraftway Credo VV22 и Kraftway Credo VV23, на которых установлен CSP VPN 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 CSP VPN Gate, 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.

Шаг 3: Убедитесь, что BIOS ПЭВМ настроен на запуск ОС с USB.

Шаг 4: При появлении на экране или в терминале приглашения ввода PIN СЗН СПДС-USB-01, введите PIN по умолчанию – 12345678.

Шаг 5: После загрузки ОС войдите в систему

имя пользователя – `root`
пароль – пустой.

Шаг 6: Установите PIN-код пользователя СЗН СПДС-USB-01:

```
cspgate:~# spds_set_pin
Enter current User's PIN: 12345678
Enter new User's PIN: ********
Retype current User's PIN: ********
```

Длина PIN-кода должна быть не менее 4 символов, пароль должен содержать цифры, буквы верхнего и нижнего регистров, специальные символы (@, #, $, &, *, % и т.п.). Требования по периодичности смены пароля и режиму сохранения его в тайне совпадают с требованиями к паролю администратора безопасности.

Примечание: Если PIN-код пользователя введен неправильно, дается еще 4 попытки, после чего специальный загрузочный носитель (СЗН) будет заблокирован. Разблокировать устройство может пользователь, идентифицированный как администратор. Если устройство будет заблокировано из-за неправильного ввода PIN-кода администратора, то дальнейшее использование СЗН будет невозможно. Для разблокировки используйте «Инструкцию по восстановлению PIN-кода пользователя на СЗН СПДС-USB-01».

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

Исполнения класса защиты КС3

Для защиты от несанкционированного доступа к АП используется АПМДЗ, кроме этого, обеспечивается разграничение прав доступа пользователей к ОС и настройке программного комплекса.

Шаг 1: Подготовьте программно-аппаратный комплекс класса защиты КС3 к инициализации CSP VPN Gate аналогично описанию в разделе «Исполнения класса защиты КС2 с АПМДЗ»

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 CSP VPN Gate, описанную в разделе «Инициализация CSP VPN Gate при первом старте»

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

Инициализация CSP VPN 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 CSP VPN Gate.

Шаг 1: Запустите скрипт `/opt/VPNagent/bin/init.sh` для старта процедуры начальной инициализации CSP 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: 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 «O».

При вводе неверного номера лицензии предлагается ввести его еще раз.

Шаг 3: Инициализируется ДСЧ: "`You should initialize RNG. Press <Enter> to proceed…`"

Для исполнений класса защиты КС1 проводится «биологическая» инициализация начального значения ДСЧ: поэтому предлагается понажимать клавиши: "`Press keys… [ ]`". По окончании выдается сообщение "Initialization SUCCESS".

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

Шаг 4: 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 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 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 безопасности – **Default Driver Policy = Passdhcp**, при которой интерфейсы шлюза безопасности пропускают только пакеты DHCP и в незащищенном виде.

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, имена пользователей задаются администратором. Подробнее описано в разделе «Разграничение доступа».

Графический интерфейс Web-based GUI не устанавливается вместе с CSP VPN Gate. Инсталляция графического интерфейса выполняется отдельно. Описание инсталляции приведено в документе «Web-based интерфейс управления: инструкция по установке и использованию».

Сразу после инициализации программного комплекса, в случае исполнения Продукта класса защиты КС1 и КС2, 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 CSP VPN 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 `msm_auth_login`.

Шаг 1: Администратор должен подготовить для всех пользователей контейнеры с секретными ключами, защищенные паролем, используя СКЗИ «КриптоПро CSP»,. Контейнеры могут располагаться на носителях HDIMAGE и AKS ifdh (eToken). Например, можно использовать утилиту `csptest`:

```
/opt/cprocsp/bin/ia32/csptest -keyset -newkeyset -container
'<имя контейнера>' -machinekeyset -password <пароль>
```

например,

```
/opt/cprocsp/bin/ia32/csptest -keyset -newkeyset -container
'HDIMAGE\\contadmin' -machinekeyset -password 123456
```

Шаг 2: Администратор должен выполнить необходимые настройки в конфигурационном файле `msm_auth_login.ini`, где для каждого пользователя указывается уровень доступа и имя контейнера, а также некоторые дополнительные параметры (см.раздел «Настройки конфигурационного файла»).

Изначально в конфигурационном файле присутствует пользователь `administrator`, для которого заданы:

```
role=admin
container=HDIMAGE\\defaultadmin
config_user=cscons
```

Измените имя данного пользователя и его пароль, который является паролем к контейнеру с ключевой парой, пересоздав заново контейнер.

Настройки конфигурационного файла

Настройки утилиты `msm_auth_login` выполняются в конфигурационном файле `/opt/VPNagent/etc/msm_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 экспортирования публичного ключа из контейнера в файл выполните, например, команду: `/opt/cprocsp/bin/ia32/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`.

`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 `msm_auth_login.ini`:

```
! 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
```

Описание работы утилиты

При старте утилита `msm_auth_login` пишет свое название:

```
CSP VPN Gate administrative console.
```

Если утилита запускается первый раз после рестарта системы и разрешен автологин, то берется первый присутствующий администратор и делается попытка проверить пустой пароль. При успешной проверке выполняются действия, аналогичные команде start, и 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 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
```

выполняется остановка исполнения на 1 секунду

ОС автоматически перезапускает утилиту для повторения попытки аутентификации.

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»).

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 CSP VPN 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/msm_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/msm_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/msm_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/msm_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.

Сообщения, выдаваемые на консоль

Список сообщений выдаваемых на консоль приведен в Таблица 3.

Таблица 3

Сообщение	Тип	Дублируется в syslog	Пояснение
CSP VPN 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/msm_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/msm_auth_login_cmd.xml	ошибка	+	Не удалось прочитать базу команд.
% Warning: configuring as user root. Check the 'config_user' setting in /opt/VPNagent/etc/msm_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.

Переключение консоли на последовательный порт или монитор и клавиатуру

Переключение вывода консоли возможно на всех аппаратных платформах, кроме МСМ, Kraftway Credo VV22, Kraftway Credo VV23 и платформ, оснащённых СЗН СПДС-USB-01.

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 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.

