



КОД БЕЗОПАСНОСТИ

Средство криптографической защиты информации

Континент-АП

Версия 3.7 (исполнения 5, 6)

Руководство администратора

Linux

RU.88338853.501430.007 01 91



КОД БЕЗОПАСНОСТИ

© Компания "Код Безопасности", 2019. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

Почтовый адрес: **115127, Россия, Москва, а/я 66 000
"Код Безопасности"**

Телефон: **8 495 982-30-20**

E-mail: **info@securitycode.ru**

Web: **https://www.securitycode.ru**

Оглавление

Введение	5
Общие сведения	6
Назначение и основные функции	6
Принципы функционирования абонентского пункта	6
Сертификаты открытых ключей	7
Уровни безопасности	7
Ролевая аутентификация	8
Режим администратора	8
Контроль целостности	8
Правила безопасности	9
Установка, удаление и обновление	10
Требования к аппаратному и программному обеспечению	10
Установка	11
Удаление программного обеспечения абонентского пункта	13
Обновление	13
Изменение уровня безопасности	14
Подготовка к работе	15
Управление абонентским пунктом	16
Вызов меню	16
Окно настроек абонентского пункта	16
Настройка подключений	17
О профилях подключений	17
Список профилей подключений	17
Параметры профиля подключения	18
Создание нового профиля подключения	19
Подключение к серверу доступа	20
Автоматическое подключение к серверу доступа	22
Разрыв соединения с сервером доступа	22
Завершение работы абонентского пункта	22
Вход в режим администратора	23
Управление сертификатами	24
Создание запроса	24
Регистрация сертификатов	26
Просмотр сведений о сертификате	27
Удаление корневого сертификата	29
Список доверенных серверов доступа	29
Импорт закрытого ключа	30
Просмотр событий	31
Приложение	32
Права пользователей и администраторов	32
Управление абонентским пунктом из командной строки	32
Команда add cert	33
Команда add profile	34
Команда connect	35
Команда del cert	35
Команда del profile	36
Команда del server	36
Команда disconnect	36
Команда events	36
Команда import	37
Команда modify profile	37
Команда resetparam	38

Команда request	38
Команда setparam	38
Команда show all	39
Команда show cert	39
Команда show parameter	39
Команда show profile	39
Команда show serverlist	40
Команда show stats	40
Команда version	40
Файлы контроля целостности	40
Просмотр списка файлов, поставленных на контроль	40
Повторное создание списка файлов, подлежащих контролю	40
Перерасчет контрольных сумм	41

Введение

Данный документ предназначен для администраторов изделия "Средство криптографической защиты информации "Континент-АП". Версия 3.7 (исполнения 5, 6)" (далее — абонентский пункт). В нем содержатся сведения, необходимые администратору для установки и настройки абонентского пункта на платформе Linux.

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте <https://www.securitycode.ru/products/>.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-800-505-30-20 или по электронной почте support@securitycode.ru. Страница службы технической поддержки на сайте компании "Код Безопасности": <https://www.securitycode.ru/products/techsupport/>.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании <https://www.securitycode.ru/company/education/training-courses/>. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Общие сведения

Назначение и основные функции

Абонентский пункт (далее — АП) является специализированным программным обеспечением, которое устанавливается на рабочих местах удаленных пользователей.

Абонентский пункт предназначен для организации доступа удаленных пользователей по защищенному каналу к ресурсам, защищаемым средствами АПКШ "Континент", а также для криптографической защиты трафика, циркулирующего между удаленными пользователями.

Абонентский пункт обеспечивает решение следующих задач:

- подключение к серверу доступа;
- криптографическая защита канала связи.

Для решения этих задач абонентский пункт выполняет следующие основные функции:

- аутентификация сервера доступа на основе технологии открытых ключей;
- формирование ключевой информации, необходимой для организации сессии;
- установление защищенного соединения между удаленным пользователем и сервером доступа;
- установление защищенных соединений между удаленными пользователями;
- генерация закрытого ключа и формирование на его основе открытого с созданием запроса на получение сертификата стороннего удостоверяющего центра;
- импорт сертификатов;
- регистрация событий, связанных с работой абонентского пункта.

Принципы функционирования абонентского пункта

При подключении абонентского пункта к серверу доступа выполняется процедура установления соединения в соответствии с протоколом TLS. В ходе этой процедуры осуществляется взаимная аутентификация абонентского пункта и сервера доступа. Завершается процедура установления соединения генерацией сеансового ключа, который используется для шифрования трафика между абонентским пунктом и сервером доступа.

Для обмена данными между двумя абонентскими пунктами на первом этапе выполняется их аутентификация на сервере доступа. После этого зашифрованный трафик между абонентскими пунктами проходит через сервер доступа.

При аутентификации используются сертификаты X.509v3. Расчет хэш-функции выполняется по алгоритму ГОСТ Р 34.11-94 или ГОСТ Р 34.11-2012, формирование и проверка электронной подписи — по алгоритму ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012.

Генерация закрытого ключа и формирование на его основе открытого при создании запроса на получение сертификата удостоверяющего центра выполняется средствами встроенного криптопровайдера "Код Безопасности CSP".

В зависимости от требований, предъявляемых к доступу удаленных пользователей к защищаемым ресурсам, на АП может использоваться произвольное количество подключений, каждое из которых имеет индивидуальную настройку параметров. Например, если в состав защищаемой сети входит несколько серверов доступа, для соединения данного АП с каждым из них используется отдельное подключение.

Сертификаты открытых ключей

Сертификат — это цифровой документ, содержащий информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название центра сертификации и т. д. Сертификат заверяется электронной цифровой подписью удостоверяющего центра сертификации.

В зависимости от используемого стандарта существуют различные форматы сертификатов. Абонентский пункт может работать со следующими форматами:

- сертификаты в кодировках Distinguished Encoding Rules (DER) и Base-64 (перевод двоичных данных в читаемый текст). Файл, содержащий один сертификат, обычно имеет расширение *.cer. В файлах с таким расширением хранятся сертификаты пользователя (как правило) и реже — сертификаты корневого центра сертификации;
- сертификаты в формате PKCS 7 (обычно с расширением *.p7b). Могут содержать несколько сертификатов, например, цепочку подтверждающих друг друга сертификатов. В таком формате обычно хранятся сертификаты корневого центра сертификации.

Сертификаты в файлах с расширением *.cer и *.p7b соответствуют стандарту X.509v3 Международного телекоммуникационного союза (ITU-T).

Для создания защищенного соединения между абонентским пунктом и сервером доступа пользователю абонентского пункта необходимо получить у администратора сервера доступа и зарегистрировать на своем компьютере следующие сертификаты:

- сертификат пользователя абонентского пункта;
- корневой сертификат, удостоверяющий сертификат пользователя.

Пользователь получает сертификаты на основании созданного им запроса. Запрос на получение сертификата создается средствами программного обеспечения абонентского пункта. Одновременно с запросом генерируется закрытый ключ пользователя. Запрос в виде файла сохраняется в указанную пользователем папку, ключевой контейнер с закрытым ключом сохраняется на ключевом носителе.

Система автоматически отслеживает статус сертификата — действителен или недействителен. Недействительным сертификат может быть признан по следующим причинам:

- срок действия сертификата не наступил;
- срок действия сертификата истек;
- сертификат скомпроментирован;
- отсутствует сертификат удостоверяющего центра.

Необходимо использовать только действительные сертификаты.

Уровни безопасности

Программное обеспечение абонентского пункта устанавливается и функционирует в соответствии с одним из двух вариантов, обеспечивающим необходимый уровень безопасности:

- низкий;
- средний.

В зависимости от выбираемого варианта установка имеет следующие особенности:

Низкий	Устанавливаются: <ul style="list-style-type: none"> • ПО абонентского пункта, включающее в себя биологический датчик случайных чисел; • криптопровайдер "Код Безопасности CSP"
---------------	--

Средний	<p>Требуется наличие платы и ПО ПАК "Соболь". Устанавливаются:</p> <ul style="list-style-type: none"> • ПО абонентского пункта; • криптопровайдер "Код Безопасности CSP". <p>В качестве физического датчика случайных чисел используется датчик из состава ПАК "Соболь"</p>
----------------	---

Ролевая аутентификация

В соответствии с требованиями безопасности пользователи абонентского пункта разделяются по ролям на администраторов и пользователей.

Администратор абонентского пункта — пользователь компьютера, зарегистрированный с правами суперпользователя. Администратору доступны все функции, связанные с установкой, настройкой и работой абонентского пункта.

Пользователь абонентского пункта — любой зарегистрированный на компьютере пользователь, не имеющий прав суперпользователя. Права пользователя при работе с абонентским пунктом ограничены.

Перечень функций, доступных каждой из ролей, приведен в Приложении (см. стр.32).

Роль пользователя в абонентском пункте определяется по результатам аутентификации при входе в систему.

Режим администратора

В работе абонентского пункта предусмотрен режим администратора, в котором пользователю становятся доступными функции управления абонентским пунктом, требующие наличия прав суперпользователя.

Для работы в режиме администратора необходимо, чтобы в операционной системе был установлен определенный пакет, позволяющий запускать программы с правами суперпользователя.

Выбор пакета зависит от используемой операционной системы и наличия той или иной графической оболочки. Примерами таких пакетов могут быть:

- beesu;
- kdesu;
- gksu;
- fly-su

и другие.

Для входа в режим администратора пользователь должен ввести пароль, подтверждающий права суперпользователя.

После входа в режим администратора пользователю становятся доступными операции, связанные с сертификатами и настройкой подключений для всех пользователей операционной системы, а также расширенный набор зарегистрированных событий при просмотре журнала.

Контроль целостности

Функция контроля целостности (КЦ) предназначена для слежения за неизменностью содержимого файлов программного обеспечения абонентского пункта. Действие функции основано на сравнении текущих значений содержимого контролируемых файлов и значений, принятых за эталон.

Эталонные значения рассчитываются при установке или обновлении программного обеспечения абонентского пункта. Сведения о файлах, подлежащих контролю, и об эталонных значениях приведены в Приложении (см. стр.40).

Проверка контрольных сумм выполняется автоматически в следующих случаях:

- при запуске программного обеспечения "Континент-АП";
- при попытке соединения с сервером доступа.

Если абонентский пункт используется совместно с ПАК "Соболь", дополнительно проверка контрольных сумм выполняется при загрузке операционной системы.

Результаты проверки заносятся в журнал событий.

При отрицательном результате проверки на экран выводится сообщение о нарушении целостности файлов, и установление соединения с сервером доступа становится невозможным.

Правила безопасности

- 1.** Никому не передавайте ключевые носители с закрытыми ключами.
- 2.** Во всех сложных ситуациях, связанных с работой абонентского пункта, которые вы сами не в состоянии разрешить, обращайтесь к администратору. В частности, если имеющихся прав доступа к ресурсам корпоративной сети недостаточно для эффективного выполнения должностных обязанностей, обратитесь к администратору безопасности или другому должностному лицу, отвечающему за распределение прав доступа к ресурсам.

Установка, удаление и обновление

Требования к аппаратному и программному обеспечению

Абонентский пункт предназначен для использования на компьютерах, работающих под управлением операционных систем семейства Linux. Требования к конфигурации компьютеров приведены в Табл.1.

Табл.1 Требования к конфигурации компьютера

Элемент	Минимально	Рекомендуется
Процессор	В соответствии с требованиями операционной системы, установленной на компьютер	
Оперативная память	В соответствии с требованиями операционной системы, установленной на компьютер	
Жесткий диск (свободное пространство)	4 ГБ	20 ГБ
Операционная система	См. след. таблицу	
Установленное ПО	ПАК "Соболь". Только для среднего уровня безопасности	
Ключевое устройство	USB-флеш-накопитель; JaCarta PKI; JaCarta-2 ГОСТ; JaCarta ГОСТ; JaCarta LT; Рутокен ЭЦП 2.0; Рутокен S (с драйвером от производителя); Рутокен Lite; iButton DS1994 - 1996 (при наличии ПАК "Соболь"); ESMART Token USB, ESMART Token ГОСТ	

Табл.2 Поддерживаемые операционные системы

Семейство ОС	Версия	Архитектура
Astra Linux	Astra Linux Common Edition "Опел" 1.9, 1.11, 2.11	x64
	Astra Linux Special Edition "Смоленск" 1.5, 1.6	x64
CentOS	6.5	x86, x64
ContinentOS	4.2	x64
Debian	7.6 wheezy	x86, x64
GosLinux	6.4, исполнение ic2	x86, x64
РЕД ОС	7.1 МУРОМ	x64
RHEL	6.5_Desktop, 6.5_Server	x86, x64
	7.0_Desktop, 7.0_Server	x64
Ubuntu	14.04_LTS_Desktop, 14.04_LTS_Server	x86, x64
Альт Линукс	СПТ 7.0.5	x86, x64
Альт	8 СП	x86, x64
ROSA	ROSA Enterprise Desktop X3	x86, x64

На компьютере должны быть установлены компоненты операционной системы, обеспечивающие работу с сетевыми протоколами TCP/IP.

Внимание!

- Все службы, реализующие штатные механизмы удаленного управления операционной системой, должны быть отключены.
- Пропускная способность сетевого канала, по которому устанавливается соединение абонентского пункта с сервером доступа, должна быть не менее 9,6 Кбит/с.
- При использовании абонентского пункта совместно с ПАК "Соболь" необходимо перед установкой абонентского пункта установить этот продукт и выполнить его инициализацию согласно эксплуатационной документации.
- Если установка операционной системы была выполнена с применением менеджера логических томов (LVM), корректная работа ПАК "Соболь" для среднего уровня безопасности ПО абонентского пункта не поддерживается.

Установка

Для установки программного обеспечения абонентского пункта пользователь должен иметь права суперпользователя.

Программное обеспечение абонентского пункта поставляется на установочном компакт-диске, содержащем четыре каталога:

TS	Установочные пакеты программного обеспечения абонентского пункта. Для каждой поддерживаемой операционной системы в каталоге содержатся два deb- или rpm-пакета (в зависимости от операционной системы). В имени установочного пакета отображается уровень безопасности, которому соответствует устанавливаемое программное обеспечение абонентского пункта. Для установки абонентского пункта с низким уровнем безопасности используется пакет, в имени которого отображается значение ks1, со средним уровнем — ks2
Sable	Программное обеспечение (установочные пакеты) для поддержки совместной работы абонентского пункта с ПАК "Соболь"
third_party	Стороннее программное обеспечение, необходимое для работы абонентского пункта
token_libs	Стороннее программное обеспечение, необходимое для работы с ключевыми носителями JaCarta и ESMART

Внимание! Перед установкой ПО абонентского пункта на RHEL 6.5-подобных операционных системах (RHEL 6.5, RHEL 6.5 Server, CentOS 6.5), если в составе ОС установлен пакет `openct`, его следует удалить. Для удаления пакета `openct` и его зависимостей используйте команду

`yum remove openct --disablerepo=*`.

Пакеты зависимостей, поставляемые совместно с дистрибутивом "Континент-АП", не являются обязательными к установке. При наличии в доступных официальных репозиториях ОС более новых версий пакетов зависимостей рекомендуется использовать их.

Если нет возможности использовать официальные репозитории ОС, то для установки используйте зависимые пакеты поставляемые в комплекте с "Континент-АП", как описано далее в **п. 2, 3**.

Для установки программного обеспечения:

1. Вставьте установочный компакт-диск и перейдите в каталог `third party`.
2. Перейдите в подкаталог с номером версии используемой операционной системы, например:
`cd /third party/RHEL/RHEL-7.0_Desktop-x86_64`.
3. Установите пакеты, содержащиеся в подкаталоге.

Внимание! Установка пакетов осуществляется командами в зависимости от установленной операционной системы.

- Для группы ОС, использующих менеджер пакетов rpm (CentOS, ContinentOS, GosLinux, RHEL), используйте команду **yum localinstall *.rpm --disablerepo=***.
 - Для группы ОС, использующих менеджер пакетов deb (Astra, Debian, Ubuntu), используйте команду **dpkg -i *.deb**.
 - Для ОС Альт Линукс используйте команду **apt-get install *.rpm**.
 - Для ОС ROSA используйте команду **urpmi *.rpm**.
4. Перейдите в каталог token libs и далее перейдите в подкаталог с номером версии используемой операционной системы, например:
cd /token_libs/RHEL/RHEL-7.0_Desktop-x86_64.
 5. Установите пакеты, содержащиеся в подкаталоге (см. п. 3).
 6. Если программное обеспечение абонентского пункта должно соответствовать среднему уровню безопасности, перейдите в каталог Sable/v.3.0/ и далее — в подкаталог с номером версии используемой операционной системы, например:
cd /Sable/v.3.0/RHEL/RHEL-7.0_Desktop-x86_64.
Установите пакет, содержащийся в подкаталоге (см. п.3).
 7. Перейдите в каталог TS и далее перейдите в подкаталог с номером версии используемой операционной системы, например:
cd /TS/RHEL/RHEL-7.0_Desktop-x86_64.
В подкаталоге хранятся два установочных пакета абонентского пункта — для низкого и среднего уровня безопасности.
 8. Установите пакет, соответствующий требуемому уровню безопасности. Для этого используйте нужную команду, указав имя пакета.
 - Для группы ОС, использующих менеджер пакетов rpm (CentOS, ContinentOS, GosLinux, RHEL), используйте команду **yum localinstall cts-3.7.6.ks1.el6.5.x86_64.rpm --disablerepo=*** (для низкого уровня безопасности)
или
yum localinstall cts-3.7.6.ks2.el6.5.x86_64.rpm --disablerepo=* (для среднего уровня безопасности).
 - Для группы ОС, использующих менеджер пакетов deb (Astra, Debian, Ubuntu), используйте команду **dpkg -i cts-3.7.6.ks1.el6.5.x86_64.deb** (для низкого уровня безопасности)
или
dpkg -i cts-3.7.6.ks2.el6.5.x86_64.deb (для среднего уровня безопасности).
 - Для ОС Альт Линукс используйте команду **apt-get install cts-3.7.6.ks1.rpm --disablerepo=*** (для низкого уровня безопасности)
или
apt-get install cts-3.7.6.ks2.rpm --disablerepo=* (для среднего уровня безопасности).
 - Для ОС ROSA используйте команду **urpmi cts-3.7.6.ks1.rpm** (для низкого уровня безопасности)
или
urpmi cts-3.7.6.ks2.rpm (для среднего уровня безопасности).

После установки пакета в окне консоли появится сообщение о необходимости прочитать текст лицензионного соглашения и будет указан путь к файлу текста соглашения.
 9. Прочтите текст соглашения.
Внимание! Если вы не согласны с лицензионным соглашением, удалите установленный пакет (см. стр.13).
 10. Перезагрузите компьютер.

После перезагрузки компьютера на экране в области уведомлений появится пиктограмма абонентского пункта:



Цвет пиктограммы указывает на состояние соединения с сервером доступа:

Пиктограмма	Цвет	Пояснение
	Серый	Отключено (соединение не установлено)
	Зеленый	Соединение установлено

Удаление программного обеспечения абонентского пункта

Внимание! Пользователь, выполняющий удаление программного обеспечения абонентского пункта, должен обладать правами суперпользователя.

Предусмотрено два варианта удаления:

- с помощью графического пакетного менеджера (если графический пакетный менеджер входит в состав операционной системы);
- с помощью консольного пакетного менеджера.

Для удаления с помощью графического пакетного менеджера:

1. На рабочем столе выберите в меню "Система | Администрирование | Установка и удаление программ".

Откроется окно графического пакетного менеджера.

2. Выберите установленный пакет "Continent Terminal Station (VPN)" и удалите его.

Для удаления с помощью консольного пакетного менеджера:

- Запустите консоль и выполните команду удаления пакета, например:
 - для группы ОС, использующих менеджер пакетов rpm (CentOS, ContinentOS, GosLinux, RHEL), используйте команду **yum remove cts**;
 - для группы ОС, использующих менеджер пакетов deb (Astra, Debian, Ubuntu), используйте команду **dpkg -P cts**;
 - для ОС Альт Линукс используйте команду **apt-get remove cts**;
 - для ОС ROSA используйте команду **urpme cts**.

Обновление

Внимание! Перед обновлением ПО абонентского пункта с версии 3.7.5 до версии 3.7.6 в операционных системах, использующих менеджер пакетов rpm, необходимо удалить пакет `openct`. Для удаления используйте команду

yum remove openct --disablerepo=*.

Примечание. Обновление выполняется с сохранением уровня безопасности.

Для обновления ПО абонентского пункта:

1. Выполните процедуру установки программного обеспечения абонентского пункта, как описано на стр. [11](#).
2. Выполните обновление списка файлов для расчета контроля целостности. Для этого введите от имени суперпользователя команду **/usr/bin/autocfsic** и дождитесь ее выполнения.
3. Перезагрузите компьютер.

Примечание. Для ОС Terminal после обновления ПО абонентского пункта с версии 3.7.5 до версии 3.7.6 пользователю с правами root необходимо выполнить команду `/opt/secretnet/sbin/snfc -i`.

Изменение уровня безопасности

При необходимости изменить уровень безопасности ПО абонентского пункта выполните следующее:

1. Выполните процедуру удаления программного обеспечения абонентского пункта, как описано на стр. **13**.
2. Выполните установку ПО абонентского пункта (см. стр. **11**), используя команды для требуемого уровня безопасности.

Подготовка к работе

Для подготовки абонентского пункта к работе:

1. Если абонентский пункт должен работать совместно с ПАК "Соболь", выполните настройку механизма контроля целостности (инструкции по настройке см. в эксплуатационной документации ПАК "Соболь").

Для настройки механизма контроля целостности:

- Определите путь к файлам-шаблонам контроля целостности. Для этого в окне эмулятора терминала выполните команду **scheck --ls-path**.

Примечание. Команда **scheck --ls-path** выполняется только от имени суперпользователя.

- В меню администратора ПАК "Соболь" войдите в раздел "Контроль целостности" и укажите путь к каталогу шаблонов КЦ.
 - С помощью программы управления шаблонами КЦ сформируйте список файлов ПО абонентского пункта, подлежащих контролю.
 - Выполните расчет эталонных значений контрольных сумм.
2. Ознакомьтесь с описаниями меню управления абонентским пунктом (см. стр.16) и окна настроек (см. стр.16).
 3. Если сертификаты должны быть получены по запросу, создайте запрос на получение сертификатов (см. стр.24) и передайте его администратору сервера доступа.
 4. Получите у администратора сертификаты и зарегистрируйте корневой сертификат (см. стр.26).

Если сертификаты должны быть получены без запроса, вместе с сертификатами получите закрытый ключ и выполните его импорт (см. стр.30).

5. Создайте и настройте профиль подключения к серверу доступа (см. стр.19).
6. Установите соединение с сервером доступа (см. стр.20) и попробуйте подключиться к какому-либо доступному ресурсу, находящемуся в защищенном сегменте корпоративной сети.

Если пробное соединение с сервером установлено успешно и подключение к ресурсу корпоративной сети возможно — значит, все подготовительные действия выполнены правильно. С этого момента абонентский пункт готов к работе.

Управление абонентским пунктом

Вызов меню

Управление абонентским пунктом выполняют с помощью специального меню.

Для вызова меню управления абонентским пунктом:

- Наведите указатель мыши на пиктограмму абонентского пункта, расположенную на панели запуска приложений, и нажмите правую кнопку мыши.

На экране появится меню управления абонентским пунктом.

Табл.3 Команды меню управления абонентским пунктом

Команда	Описание
Подключить	Запускает процедуру установления соединения абонентского пункта с сервером доступа. После установления соединения заменяется командой "Разорвать"
Разорвать	Запускает процедуру разрыва соединения абонентского пункта с сервером доступа. После разрыва соединения заменяется командой "Подключить"
Настройка > Параметры...	Вызывает на экран окно настройки абонентского пункта для выполнения операций с сертификатами и настройки подключений
Настройка > Запросить новый сертификат...	Запускает процедуру создания запроса сертификата
Настройка > Импортировать ключ...	Запускает процедуру импорта закрытого ключа, сформированного при создании пользователя средствами программы управления сервером доступа
Настройка > Посмотреть журнал	Просмотр событий, связанных с работой абонентского пункта
Помощь > Справка	Открывает файл руководства администратора в формате pdf
Помощь > О программе...	Вызывает на экран диалог со сведениями о номере версии программы и авторских правах
Режим администратора > Посмотреть журнал	Просмотр событий в режиме администратора (при наличии установленного дополнительного пакета, см. стр.8)
Режим администратора > Параметры	Вызывает на экран окно настройки абонентского пункта для выполнения операций с сертификатами и настройки подключений (при наличии установленного дополнительного пакета, см. стр.8)
Выход	Закрывает графический интерфейс и удаляет пиктограмму абонентского пункта из панели уведомлений

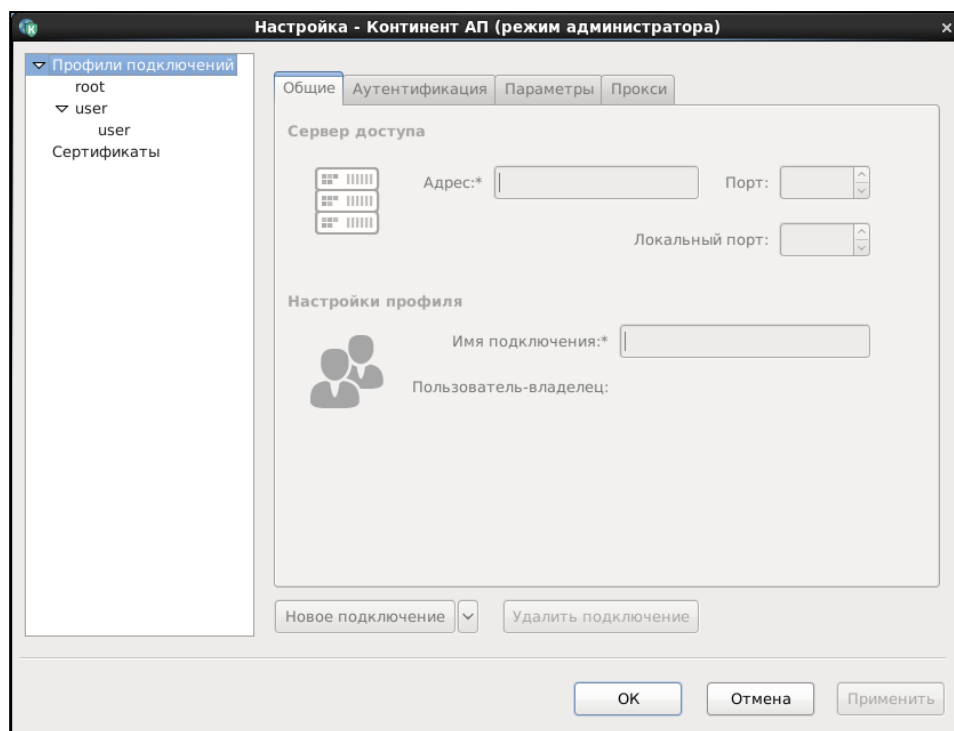
Окно настроек абонентского пункта

Окно предназначено для настройки профилей подключений к серверу доступа и работы с сертификатами.

Для вызова окна настроек:

- Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и выберите команду "Настройка > Параметры...".

На экране появится окно настройки параметров абонентского пункта.



В левой части окна расположено меню выбора требуемых настроек:

Профили подключений	Настройка профилей подключений
Сертификаты	Регистрация корневых сертификатов и сертификатов сервера

В правой части окна отображаются параметры выбранной в меню группы настроек.

Настройка подключений

О профилях подключений

Для подключения к серверу доступа пользователь абонентского пункта использует профиль, представляющий собой набор настраиваемых параметров.

Профиль подключения создается и настраивается администратором или самим пользователем.

Пользователь абонентского пункта может быть зарегистрирован на нескольких серверах доступа. В этом случае для подключения к каждому из этих серверов должен использоваться отдельный профиль.

Если к серверу доступа должны подключаться несколько зарегистрированных на компьютере пользователей, для каждого такого пользователя необходимо создать отдельный профиль подключения.

Список профилей подключений

Список профилей подключений отображается в окне настроек абонентского пункта.

Для вызова списка профилей подключений:

- Откройте окно настроек абонентского пункта (см. стр. 16).

В левой части окна в меню "Профили подключений" отобразится список зарегистрированных на компьютере пользователей со списками их профилей подключений.

Примечание. Если текущий пользователь не обладает правами суперпользователя, ему будет доступен только список "своих" профилей подключения.

При работе со списком профилей подключений предусмотрено выполнение следующих операций:

- просмотр и редактирование параметров профиля;
- удаление профиля из списка;
- копирование существующего профиля подключения;
- создание нового профиля подключения (см. стр.19).

Для просмотра и редактирования параметров профиля:

1. Выберите профиль в списке.
В правой части окна отобразятся параметры профиля, распределенные по вкладкам. Описание параметров см. стр.18.
2. После редактирования параметров для сохранения внесенных изменений нажмите кнопку <Применить>.

Для удаления профиля:

1. Выберите профиль в списке и нажмите кнопку <Удалить подключение>.
Профиль подключения будет удален из списка.
2. Для сохранения изменений нажмите кнопку <Применить>.

Параметры профиля подключения

Для просмотра и редактирования параметров профиля:

1. Вызовите окно настроек абонентского пункта (см. стр.16).
2. В левой части окна раскройте меню "Профили подключений" и выберите в списке нужное подключение.
В правой части окна отобразятся параметры выбранного подключения, распределенные по вкладкам.

Табл.4 Параметры подключения

Вкладка/Параметр	Описание
Общие	
Адрес	IP-адрес или имя сервера доступа
Порт	Порт сервера доступа для обмена сообщениями с абонентским пунктом
Локальный порт	Порт на компьютере пользователя, используемый для соединения с сервером доступа
Имя подключения	Наименование подключения, отображаемое в списке профилей
Пользователь-владелец	Имя пользователя, имеющего доступ к данному подключению
Аутентификация	
Сертификат	Имя сертификата пользователя и соответствующего ему ключевого контейнера, с которым будет осуществляться подключение к серверу доступа. Для просмотра сведений о сертификате используйте ссылку "Посмотреть сведения о сертификате"
Параметры	

Вкладка/Параметр	Описание
Число попыток	Количество автоматических попыток подключения к серверу доступа без участия пользователя. Если за указанное число попыток соединение не будет установлено, на экране появится сообщение об ошибке, после чего пользователь может повторить попытку подключения
Интервал между попытками	Интервал времени, по прошествии которого необходимо повторить попытку соединения
Время простоя до разъединения	Интервал времени, по прошествии которого следует разорвать соединение с сервером доступа в случае, если установленное соединение не используется для передачи информации. Значение по умолчанию "никогда" означает, что соединение не будет разорвано из-за отсутствия передаваемой информации
Вариант активации подключения	Активация подключения выполняется по требованию пользователя или автоматически после входа пользователя в операционную систему
Прокси	
Не использовать прокси	Подключение через прокси-сервер не используется
Ручная настройка прокси	Параметры подключения через прокси-сервер задаются вручную
Сервер	Сетевое имя или IP-адрес прокси-сервера
Порт	Порт прокси-сервера
Тип	Тип аутентификации при подключении через прокси-сервер: <ul style="list-style-type: none"> • Нет (без аутентификации); • Basic; • NTLM
Пользователь	Имя пользователя для аутентификации на прокси-сервере
Пароль	Пароль пользователя для аутентификации на прокси-сервере

Создание нового профиля подключения

Предусмотрено два варианта создания нового профиля подключения:

- создание профиля, включающее в себя настройку всех его параметров;
- копирование уже имеющегося профиля и последующее редактирование одного или нескольких параметров.

Второй вариант рекомендуется использовать в тех случаях, когда в настройки параметров необходимо внести незначительные изменения. Например, если необходимо использовать сертификат для подключения к двум серверам доступа. В этом случае достаточно скопировать уже настроенное подключение к первому серверу доступа, в настройках изменить IP-адрес и выбрать сертификат пользователя и закрытый ключ.

Внимание! Перед созданием нового профиля подготовьте файл сертификата пользователя, полученный от администратора сервера доступа, и внешний носитель с ключевым контейнером. Файл сертификата можно сохранить на жестком диске или на внешнем носителе.

Для создания нового профиля и настройки его параметров:

1. Вызовите окно настроек абонентского пункта (см. стр. **16**) и в меню "Профили подключений" выберите пользователя.
В правой части окна откроется список серверов доступа, для которых настроены профили подключений.
2. В нижней части окна нажмите кнопку "Новое подключение".
В списке профилей подключений появится новое подключение, а в правой части окна появятся вкладки с параметрами профиля.
3. В правой части окна на вкладке "Общие" введите имя нового подключения, укажите нужные значения параметров (описание параметров см. стр. **18**) и перейдите на вкладку "Аутентификация".
4. Укажите сертификат пользователя, который должен использоваться при аутентификации для данного профиля подключения, и имя связанного с ним ключевого контейнера. Для этого используйте кнопки "Обзор".
5. Перейдите на вкладку "Параметры", проверьте значения, установленные по умолчанию, и при необходимости введите нужные значения.
6. При необходимости использовать прокси-сервер перейдите на вкладку "Прокси" и выполните настройку. По умолчанию прокси-сервер не используется.
7. Для сохранения установленных значений параметров нажмите кнопку "Применить".

Примечание. Чтобы сохранить значения параметров и закрыть окно настроек АП, нажмите кнопку "ОК".

Для копирования подключения:

1. Вызовите окно настроек абонентского пункта и раскройте список профилей подключений (см. стр. **17**).
2. Выберите в списке профиль и в правой части окна нажмите кнопку вызова меню, расположенную справа от кнопки "Новое подключение".
Появится список дополнительных команд.
3. Выберите команду "Копировать подключение".
В левой части окна в списке появится копия выбранного подключения.
4. Введите в правой части окна на вкладке "Общие" новое имя подключения, выберите сертификат пользователя и закрытый ключ для данного подключения и далее отредактируйте значение нужного параметра (описание параметров см. стр. **18**).
5. Для сохранения изменений нажмите кнопку "Применить".

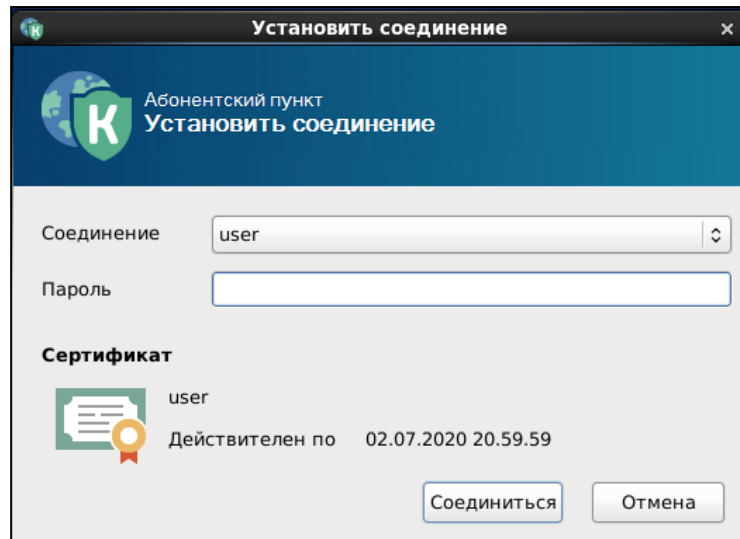
Подключение к серверу доступа

Внимание! Подключение к серверу доступа возможно только в том случае, если вход в ОС был выполнен одним пользователем. Если вход в ОС был выполнен двумя и более пользователями, для подключения одного из них к серверу доступа необходимо, чтобы другие пользователи выполнили выход из системы.

Перед подключением к серверу доступа подсоедините к компьютеру ключевой носитель с закрытым ключом пользователя.

Для подключения к серверу доступа:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и выберите команду "Подключить".
На экране появится диалог "Установить соединение".



2. В поле "Соединение" укажите профиль подключения, выбрав его из раскрывающегося списка.

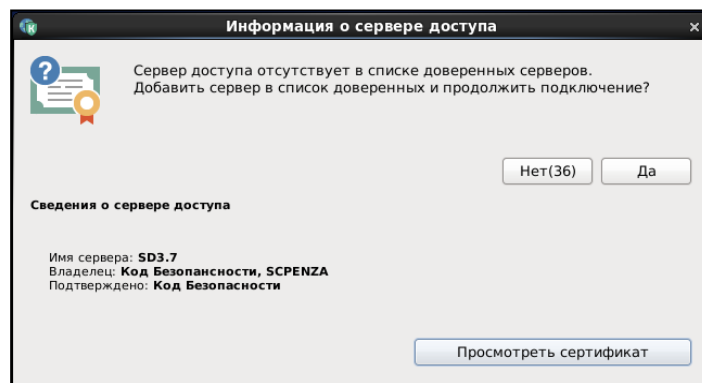
Примечание. Раскрывающийся список содержит только те профили подключения, которые доступны текущему пользователю.

В диалоге отобразится имя сертификата пользователя и срок его действия.

3. Введите пароль доступа к ключевому контейнеру и нажмите кнопку <Соединиться>.

Внимание! Если ключевой носитель не подключен или на нем отсутствует требуемый ключевой контейнер, на экране рядом с пиктограммой абонентского пункта появится всплывающее сообщение об ошибке подключения.

Если сервер доступа не внесен в список доверенных серверов, на экране появится сообщение:



Для внесения сервера доступа в список доверенных серверов нажмите кнопку "Да" (подробнее о списке доверенных серверов см. стр.29).

Внимание! На кнопке "Нет" отображается таймер обратного отсчета. Если в течение 40 секунд не будет нажата кнопка "Да", кнопка "Нет" будет нажата автоматически и подключение к серверу доступа будет отменено.

Автоматическое подключение к серверу доступа

Для автоматического подключения к серверу доступа при входе пользователя в систему необходимо выполнить описанную ниже настройку.

Для настройки автоматического подключения:

1. Вызовите окно настроек абонентского пункта (см. стр. 16).
2. В левой части окна раскройте меню "Профили подключений" и выберите в списке подключение, которое должно выполняться автоматически при входе пользователя в операционную систему.
3. В правой части окна перейдите на вкладку "Параметры" и у параметра "Вариант активации подключения" установите значение "Автоматическое подключение после входа пользователя в систему".
4. Нажмите кнопку "Применить".

Примечание. Для абонентского пункта, соответствующего среднему уровню безопасности и функционирующего совместно с ПАК "Соболь", предусмотрено сохранение не более трех профилей автоматического подключения.

Внимание! В операционных системах, не имеющих графического интерфейса пользователя, для настройки автоматического подключения к СД при входе в систему необходимо выполнить следующее:

1. Средствами консольных команд утилиты cts настроить скрипт автоматического подключения к СД.
2. Добавить настроенный скрипт в автозагрузку.

Разрыв соединения с сервером доступа

Для разрыва соединения с сервером доступа:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач.
2. В контекстном меню активируйте команду "Разорвать".
Соединение с сервером доступа будет разорвано. При этом пиктограмма абонентского пункта на панели задач примет вид "Отключено".

Примечание. Если после установления соединения с сервером доступа была выполнена блокировка пользователя ОС, соединение не разрывается.

Внимание! Если при установленном соединении с сервером доступа выполнить смену пользователя и войти в ОС под вторым пользователем, у первого будет выполнен разрыв соединения.

Завершение работы абонентского пункта

При выполнении операций выхода из системы, перезагрузки или выключения компьютера возможно появление на экране окна ожидания завершения программы ctsg. В этом случае для корректного завершения работы абонентского пункта рекомендуется дождаться автоматического закрытия программы.

Внимание! В операционной системе ContinentOS для корректного завершения работы абонентского пункта при выходе из системы необходимо выбрать пункт "Сохранить сеанс".

Вход в режим администратора

В режиме администратора пользователю доступны следующие операции:

- просмотр расширенного состава зарегистрированных событий в журнале;
- настройка подключений для всех пользователей;
- добавление и удаление доверенных СД для всех пользователей;
- добавление и удаление корневых сертификатов.

Для входа в режим администратора:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и активируйте команду "Режим администратора > Посмотреть журнал" или "Режим администратора > Параметры".

- Если в системе был установлен дополнительный пакет (см. стр. **8**), на экране появится запрос на ввод пароля суперпользователя. В этом случае перейдите к п. **3**.
- Если пакет не установлен, на экране появится сообщение о необходимости установить модуль получения административных привилегий и запрос на продолжение работы в режиме пользователя.

2. Если требуется продолжить работу в режиме пользователя, нажмите кнопку "Да".

В зависимости от выбранного пункта меню на экране появится окно просмотра событий или окно настройки подключений и работы с сертификатами в режиме пользователя.

Примечание. Для отказа от выполнения действий в режиме пользователя нажмите кнопку "Нет" в окне сообщения.

3. Для входа в режим администратора введите пароль суперпользователя. На экране появится окно в соответствии с выбранным пунктом меню.

Управление сертификатами

Создание запроса

Перед тем как приступить к созданию запроса:

- подготовьте чистый отформатированный ключевой носитель для записи ключевого контейнера;
- получите у администратора сервера доступа сведения об используемом криптопровайдере.

Для создания запроса:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и активируйте команду "Настройка > Запросить новый сертификат...".

На экране появится диалог "Параметры сертификата пользователя" мастера запроса сертификата.

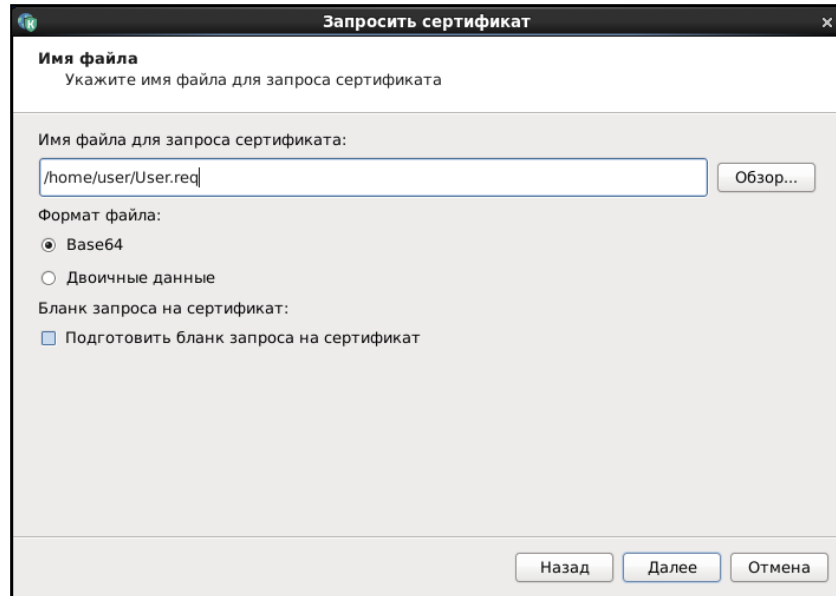
The screenshot shows a dialog box titled "Запросить сертификат" with a close button (X) in the top right corner. The main heading is "Параметры сертификата пользователя". Below the heading is a note: "Заполните обязательные поля для выпуска запроса сертификата пользователя. В полях 'Область, край' и 'Город' должны быть указаны полные официальные названия без". The form contains several input fields: "Полное имя*" (with a cursor), "Описание:", "Электронная почта:", "Организация*", "Подразделение*", "Город:", "Область, край:", and "Страна, регион:" (with a dropdown menu showing "RU" and a refresh icon). A note at the bottom states "Поля под звездочками обязательны для заполнения". At the bottom right are "Далее" and "Отмена" buttons.

2. Заполните поля диалога и нажмите кнопку <Далее>.

На экране появится диалог "Свойства поставщика служб шифрования".

The screenshot shows the same dialog box titled "Запросить сертификат" with a close button (X) in the top right corner. The main heading is "Свойства поставщика служб шифрования". Below the heading is a note: "Выберите поставщика служб шифрования данных". The form contains two sections: "Выберите поставщика служб шифрования данных" with a "Криптопровайдер:" label and a list box containing "Код Безопасности" and "Код Безопасности (режим совместимости 3.6)"; and "Ключевой контейнер:" with a text box containing "User_09_01_2020_13_31_50". At the bottom are "Назад", "Далее", and "Отмена" buttons.

3. Выберите поставщика служб шифрования данных на основании сведений, полученных у администратора СД, и, если необходимо, задайте имя ключевого контейнера. По умолчанию ключевому контейнеру присваивается имя, состоящее из имени пользователя и текущей даты и времени создания запроса.
4. Нажмите кнопку <Далее>.
На экране появится диалог "Имя файла".

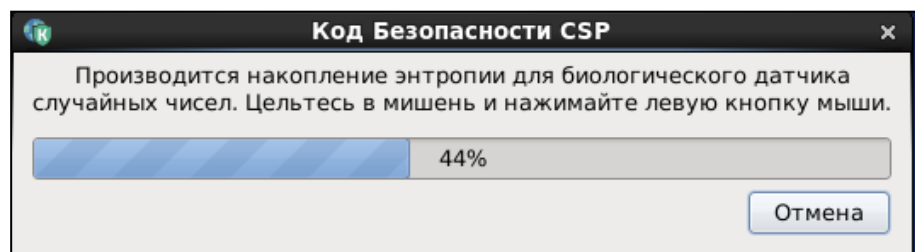


5. Укажите нужные сведения и нажмите кнопку <Далее>.

Имя файла для запроса сертификата	Полный путь и имя сохраняемого файла для запроса сертификата. Для изменения папки по умолчанию используйте кнопку "Обзор..."
Формат файла	Формат файла запроса
Подготовить бланк запроса на сертификат	При наличии отметки формируется файл HTML для печати запроса в бумажной форме. Файл сохраняется в папке, указанной в поле "Имя файла для запроса сертификата"

На экране появится завершающий диалог мастера запроса сертификата, содержащий введенные сведения.

6. Проверьте указанные сведения и нажмите кнопку <Готово>.
 - Если версия ПО абонентского пункта соответствует низкому уровню безопасности, на экране появится окно, предназначенное для накопления энтропии.



Перейдите к следующему пункту процедуры.

- Если версия ПО абонентского пункта соответствует среднему уровню безопасности, на экране появится диалог выбора ключевого носителя.

Перейдите к п. 8.

7. Следуйте указаниям инструкции на экране и дождитесь завершения.

На экране появится диалог выбора ключевого носителя.

Если ключевой носитель не был вставлен, вставьте его и нажмите кнопку "Обновить".

8. Выберите ключевой носитель и нажмите кнопку "ОК".

На экране появится диалог задания пароля для доступа к ключевому контейнеру.

9. Задайте пароль и нажмите кнопку "ОК".

В указанной папке будет сформирован файл запроса сертификата, а на носителе будет записан ключевой контейнер.

На экране появится сообщение об успешном завершении создания запроса.

10. Нажмите кнопку "ОК" в окне сообщения.

11. Извлеките ключевой носитель, а файл запроса передайте администратору.

При необходимости распечатайте запрос.

Внимание! Сгенерированный в результате данной процедуры закрытый ключ пользователя используют для подключения абонентского пункта, работающего только на платформе Linux.

Регистрация сертификатов

На основании запроса администратор сервера доступа создает и передает пользователю в виде файлов user.cer и root.p7b сертификат пользователя и корневой сертификат. Файлы сертификатов рекомендуется сохранить на жестком диске компьютера или на внешнем носителе.

Для подключения абонентского пункта к серверу доступа должны быть установлены корневой сертификат и сертификат пользователя.

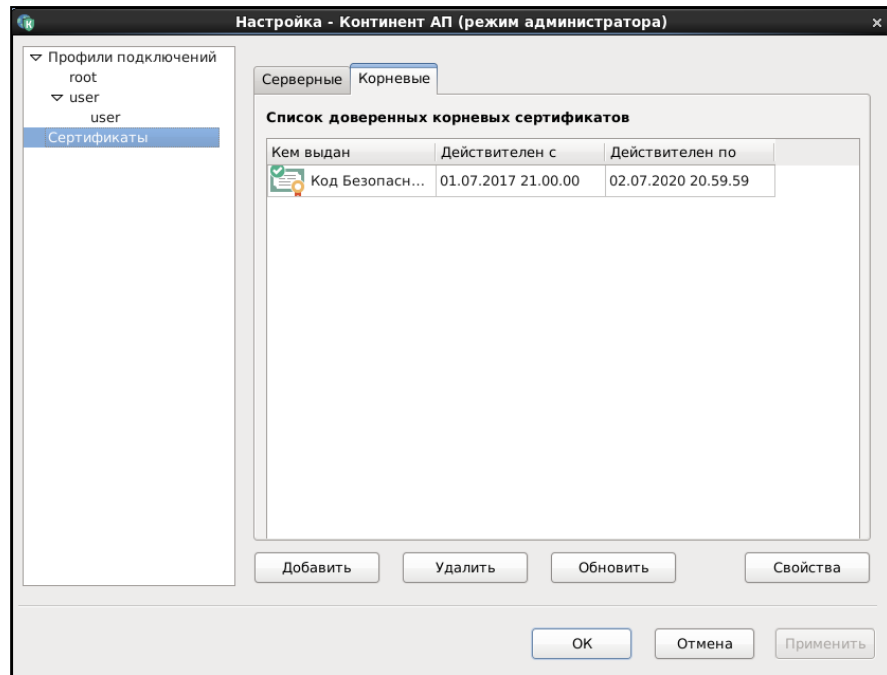
Регистрацию сертификатов выполняют отдельно: регистрация сертификата пользователя осуществляется в процессе настройки профиля подключения (см. процедуру создания нового профиля, стр. 19), а корневой сертификат регистрирует пользователь, имеющий права суперпользователя, в окне настроек абонентского пункта в меню "Сертификаты" (см. процедуру ниже).

Внимание! Регистрация корневого сертификата может быть выполнена пользователем в режиме администратора. Для этого необходимо войти в режим администратора и ввести пароль суперпользователя (см. стр. 23).

Для регистрации корневого сертификата:

1. Откройте окно настроек абонентского пункта (см. стр. 16), выберите в меню пункт "Сертификаты" и в правой части окна перейдите на вкладку "Корневые".

На вкладке отобразится список зарегистрированных корневых сертификатов.

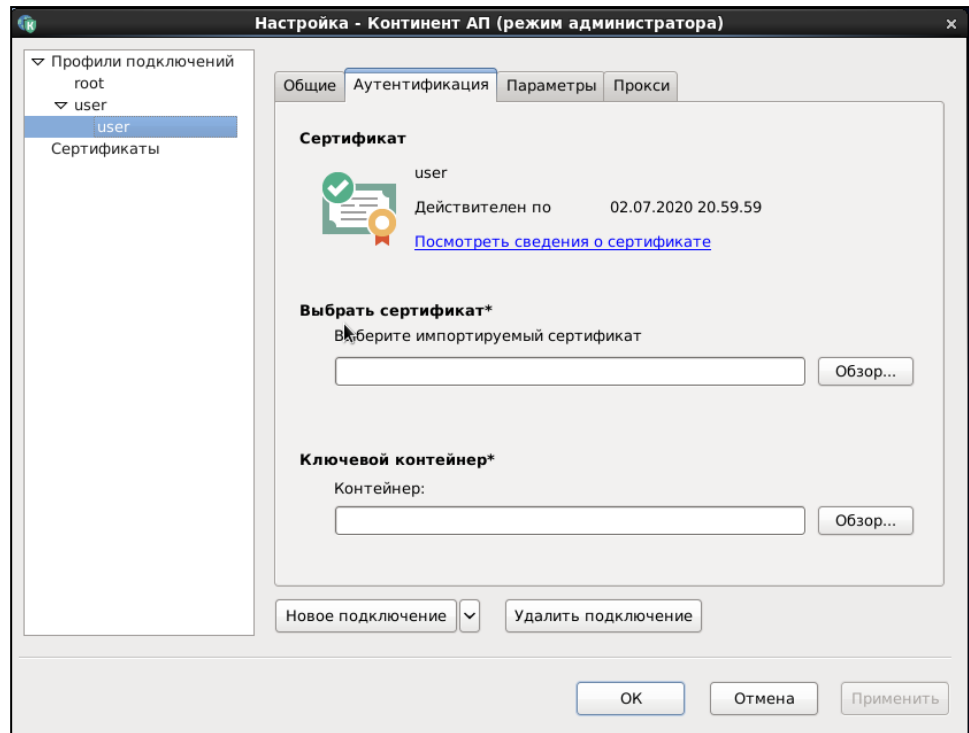


- Нажмите кнопку <Добавить>.
На экране появится стандартное окно выбора файла.
Если файл сертификата был сохранен на внешнем носителе, подключите внешний носитель к компьютеру.
- Откройте папку с корневым сертификатом, выберите его и нажмите кнопку <Открыть>.
Сертификат появится в списке на вкладке "Корневые".

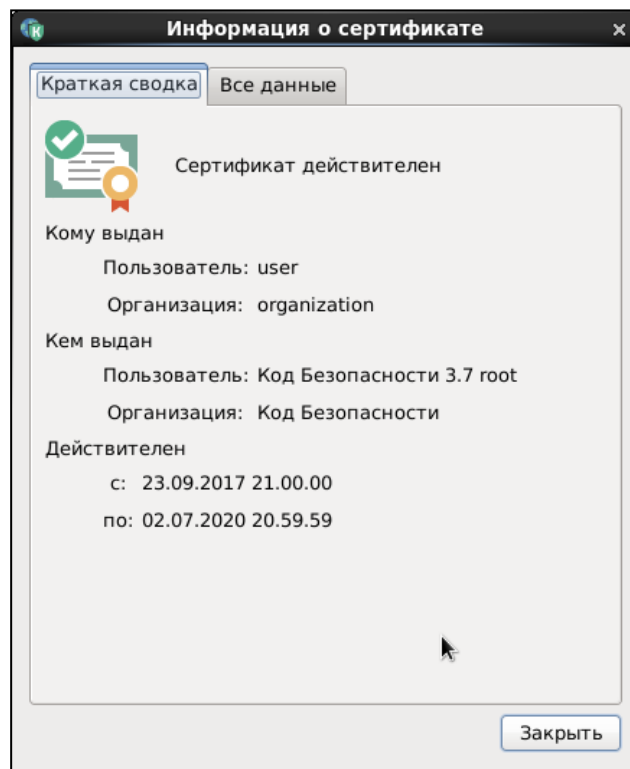
Просмотр сведений о сертификате

Для просмотра сведений о сертификате пользователя:

- Откройте окно настроек абонентского пункта (см. стр. 16), раскройте меню "Профили подключений" и выберите профиль.
В правой части окна отобразятся параметры профиля, распределенные по вкладкам.
- Перейдите на вкладку "Аутентификация" и откройте ссылку "Посмотреть сведения о сертификате".



На экране появится окно "Информация о сертификате", содержащее раздельно краткие и подробные сведения о сертификате пользователя.



3. После просмотра сведений нажмите в окне "Информация о сертификате" кнопку <Закреть>.

Для просмотра сведений о корневом сертификате:

1. Откройте окно настроек абонентского пункта (см. стр. 16) и выберите меню "Сертификаты".

В правой части окна отобразятся списки корневых сертификатов и сертификатов сервера доступа.

2. Перейдите на вкладку "Корневые".
На вкладке отобразится список зарегистрированных корневых сертификатов.
3. Выберите сертификат в списке и нажмите кнопку <Свойства>.
На экране появится окно "Информация о сертификате", содержащее раздельно краткие и подробные сведения о корневом сертификате.
4. После просмотра сведений нажмите в окне "Информация о сертификате" кнопку <Закрыть>.

Удаление корневого сертификата

Удаление корневого сертификата может выполнить только пользователь, имеющий права суперпользователя или пользователь, выполнивший вход в режим администратора (см. стр. 23).

Внимание! Перед удалением корневого сертификата убедитесь, что его удаление не повлияет на подключение пользователей к серверу доступа.

Для удаления корневого сертификата:

1. Откройте окно настроек абонентского пункта (см. стр. 16) и выберите меню "Сертификаты".
В правой части окна отобразятся списки корневых сертификатов и сертификатов сервера доступа.
2. Перейдите на вкладку "Корневые".
На вкладке отобразится список зарегистрированных корневых сертификатов.
3. Выберите сертификат в списке и нажмите кнопку <Удалить>.
На экране появится запрос на подтверждение операции удаления.
4. Нажмите кнопку <Да> в окне запроса.
Сертификат будет удален из списка.

Список доверенных серверов доступа

Для установления соединения сервер доступа, к которому осуществляется подключение, должен входить в список доверенных серверов.

Для просмотра доверенных серверов доступа:

- Откройте окно настроек абонентского пункта (см. стр. 16), выберите меню "Сертификаты" и в правой части окна перейдите на вкладку "Серверные".

На вкладке отобразится список сертификатов доверенных серверов доступа.

Внимание! В списке отображаются только те сертификаты, которые были внесены в список текущим пользователем. Если текущий пользователь имеет права суперпользователя, ему будет доступен полный список сертификатов, внесенных другими пользователями.

Для каждого сертификата приводятся следующие сведения:

- имя пользователя, внесшего сервер доступа в список доверенных;
- имя сервера доступа;
- имя сертификата сервера доступа;
- наименование организации.

Для удаления сервера доступа из списка доверенных:

1. Выберите сертификат сервера доступа в списке и нажмите кнопку <Удалить>.
На экране появится предупреждение об удалении сертификата.
2. Нажмите "Да" в окне предупреждения.
Сертификат будет удален из списка.

Импорт закрытого ключа

При создании нового пользователя администратор сервера доступа средствами программы управления СД формирует ключевой контейнер с закрытым ключом пользователя. Ключевой контейнер администратор сохраняет на отчуждаемом носителе и вместе с паролем передает его пользователю или администратору абонентского пункта. Для работы с таким ключом на абонентском пункте необходимо предварительно выполнить операцию импорта закрытого ключа.

Операция импорта заключается в преобразовании формата ключа и сохранении его в локальном хранилище компьютера или на внешнем носителе.

Для сохранения импортируемого закрытого ключа могут быть использованы:

- локальное хранилище компьютера;
- исходный носитель с закрытым ключом, полученный от администратора сервера доступа;
- другой внешний носитель.

Внимание! Если исходным носителем является iButton, использовать для сохранения ключа другой iButton нельзя.

Если закрытый ключ получен от администратора СД на внешнем носителе iButton 1994, при выполнении операции импорта ключ можно сохранить только в локальном хранилище компьютера или на другом внешнем носителе.

Для импорта закрытого ключа:

1. Вставьте ключевой носитель, полученный от администратора сервера доступа.
2. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и активируйте команду "Настройка > Импортировать ключ...".
На экране появится диалог выбора ключевого носителя.
3. Выберите ключевой носитель с закрытым ключом пользователя и нажмите кнопку "ОК".
На экране появится запрос на ввод пароля доступа к ключевому контейнеру.
4. Введите пароль и нажмите кнопку "ОК".
На экране появится диалог выбора носителя для сохранения ключевого контейнера.
5. Выберите целевой носитель для импортируемого ключа или укажите локальное хранилище и нажмите кнопку "ОК".
 - Если программное обеспечение абонентского пункта соответствует низкому уровню безопасности, на экране появится окно, предназначенное для накопления энтропии. Перейдите к **п. 6**.
 - Если программное обеспечение абонентского пункта соответствует среднему уровню безопасности, на экране появится запрос на задание нового пароля для доступа к ключевому контейнеру. Перейдите к **п. 6**.
6. Следуйте указаниям инструкции на экране и дождитесь завершения.
Импортируемый ключ будет сохранен.

Просмотр событий

События, связанные с работой абонентского пункта и подключениями к серверу доступа, регистрируются в журнале.

Просмотр событий осуществляется в режиме администратора или в режиме пользователя. В режиме пользователя набор отображаемых в журнале событий ограничен.

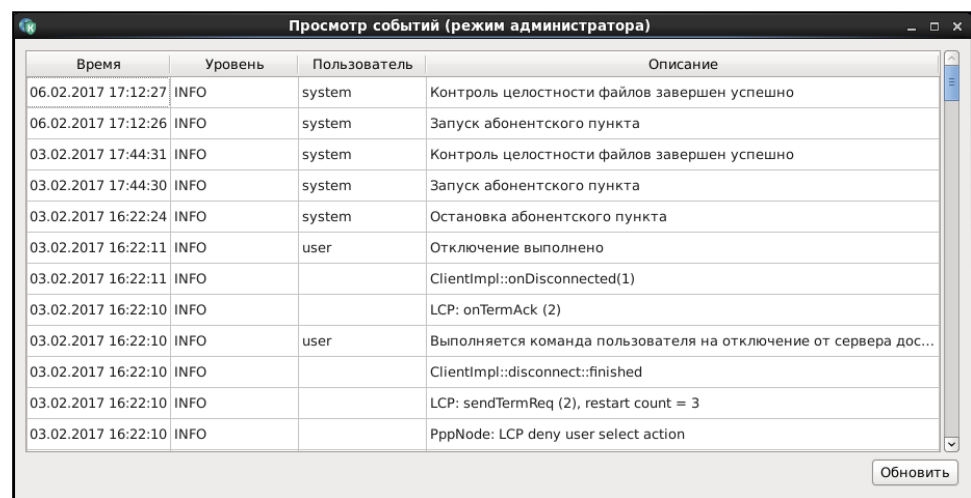
Для просмотра всех событий пользователь должен выполнить вход в режим администратора (см. стр. 23).

Для просмотра событий:

- Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и активируйте команду "Настройка > Посмотреть журнал".

Для просмотра событий в режиме администратора в контекстном меню активируйте команду "Режим администратора > Посмотреть журнал".

На экране откроется журнал событий.



Время	Уровень	Пользователь	Описание
06.02.2017 17:12:27	INFO	system	Контроль целостности файлов завершен успешно
06.02.2017 17:12:26	INFO	system	Запуск абонентского пункта
03.02.2017 17:44:31	INFO	system	Контроль целостности файлов завершен успешно
03.02.2017 17:44:30	INFO	system	Запуск абонентского пункта
03.02.2017 16:22:24	INFO	system	Остановка абонентского пункта
03.02.2017 16:22:11	INFO	user	Отключение выполнено
03.02.2017 16:22:11	INFO		ClientImpl::onDisconnected(1)
03.02.2017 16:22:10	INFO		LCP: onTermAck (2)
03.02.2017 16:22:10	INFO	user	Выполняется команда пользователя на отключение от сервера дос...
03.02.2017 16:22:10	INFO		ClientImpl::disconnect::finished
03.02.2017 16:22:10	INFO		LCP: sendTermReq (2), restart count = 3
03.02.2017 16:22:10	INFO		PppNode: LCP deny user select action

Для каждого события приводятся следующие сведения:

- дата и время;
- категория события;
- имя пользователя (только для событий, инициированных пользователем);
- краткое описание события.

Приложение

Права пользователей и администраторов

Ниже приведены функции абонентского пункта, доступные пользователям в зависимости от их роли.

Функция АП	Пользователь	Администратор
Создание, удаление, изменение профиля подключения к СД	Да	Да
Создание личного запроса на сертификат и ключевого контейнера	Да	Да
Установка корневого сертификата (цепочки корневых сертификатов) в локальное хранилище доверенных сертификатов	Нет	Да
Выбор личного сертификата пользователя для установки соединения с СД	Да	Да
Регистрация сертификата СД	Да	Да
Регистрация корневого сертификата	Нет	Да
Закрытие приложения	Да	Да
Установка, удаление, изменение приложения	Нет	Да
Обновление приложения	Нет	Да
Просмотр журналов	Да	Да
Проведение и просмотр отчета КЦ	Да	Да
Установление соединения	Да	Да

Управление абонентским пунктом из командной строки

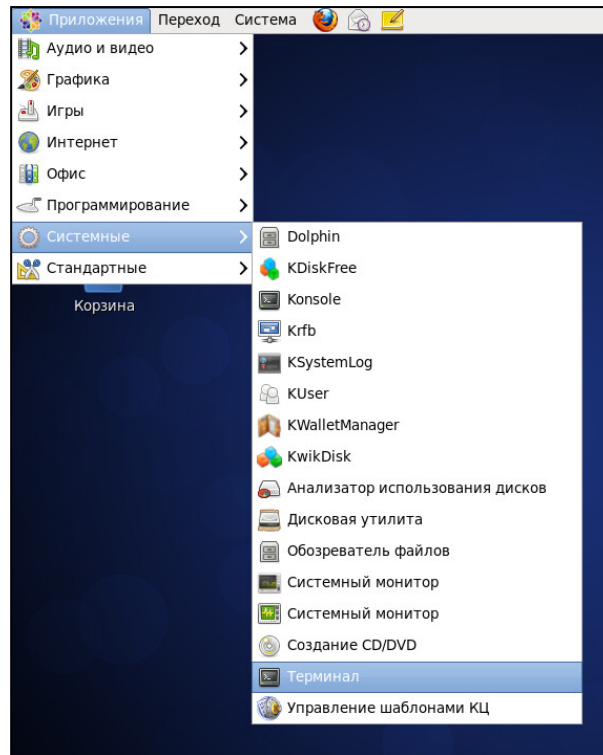
В данном разделе приведено описание специализированной утилиты **cts**, расположенной в каталоге `/usr/bin` и используемой для управления абонентским пунктом в консольном режиме.

Данная утилита используется в следующих задачах:

- создание и сброс настроек по умолчанию;
- подключение к СД;
- добавление и удаление доверенных СД;
- создание запросов на сертификат с сохранением ЗК на различные ключевые носители;
- работа с корневым сертификатом;
- просмотр информации о профилях, сертификатах и СД;
- просмотр журнала;
- просмотр сведений о программе;
- управление профилем пользователя;
- удаление сертификата пользователя.

Для вызова командной строки (на примере ОС Linux 2.6.32 и GNOME 2.28.2):

- Выберите в меню "Приложения" пункт "Системные | Терминал".



На экране появится окно консоли.



Формат вызова утилиты:

```
cts команда [-параметр 1] [-параметр 2]... [-параметр n]
```

Для каждой команды имеется свой уникальный набор параметров. Для ознакомления с полным перечнем команд и их параметров следует вызвать встроенную справку утилиты командой:

```
cts --help
```

Команда add cert

Команда предназначена для добавления сертификатов безопасности.

Внимание! Для использования этой команды пользователь должен обладать правами суперпользователя.

Параметры	Описание
Обязательные	
-cert_path <CERTIFICATE_PATH>	Путь и название сертификата
-cert_type {ca as}	Тип сертификата: корневой/СД

Пример использования:

cts add cert -cert_type ca -cert_path /home/user/root.cer	Добавление корневого сертификата из каталога /home/user/root.cer
---	---

Команда add profile

Команда предназначена для создания профиля подключения.

Параметры	Описание
Обязательные	
-cert_path <CERTIFICATE_PATH>	Путь и название сертификата
-name <NAME>	Имя профиля/соединения
-server <SERVER_ADDRESS>	Имя или IP-адрес сервера
-user <USERNAME>	Имя пользователя
Дополнительные	
-ctc <CONNECT_TRY_COUNT {0-99}>	Число попыток подключения
-cti <CONNECT_TRY_INTERVAL_IN_SEC {1 3 5 10 30 60 120 300 600}>	Интервал в секундах между попытками подключения
-dot {off <TIMEOUT_IN_SEC {0 60 300 600 1200 1800 3600 7200 14400 28800 86400}>}	Установка времени отключения после простоя
-lp <LOCAL_PORT>	Локальный порт
-mtu <MTU>	Количество байт в одном пакете
-proxy_auth {no basic ntlm}	Тип аутентификации при подключении к прокси-серверу.
-proxy_ip <IP off>	IP-адрес или доменное имя прокси-сервера/отключение использования прокси-сервера для подключения к СД
-proxy_login <ID>	Логин прокси-сервера
-proxy_pass <PASS>	Пароль доступа к прокси-серверу
-proxy_port <PORT>	Порт прокси-сервера
-rol <on off >	Включение/отключение переключений при потере соединения.
-sp <SERVER_PORT>	Порт сервера

Пример использования:

<pre>cts add profile -name TR07 -server 192.168.10.10 -cert_path /home/user/user.cer -user Admin -sp 667 -proxy_ip 192.168.10.100 -proxy_port 110 -proxy_auth basic -proxy_login User485 -proxy_pass \$5ty^fDe</pre>	<p>Создание профиля подключения для пользователя Admin к серверу 192.168.10.10 под профилем TR07 по указанному сертификату и номеру порта сервера через указанный прокси-сервер.</p> <p>Если при подключении имя пользователя должно вводиться в формате domain\user, необходимо использовать следующий синтаксис: domain\\user.</p>
--	--

Команда connect

Команда предназначена для подключения к СД.

Параметры	Описание
Дополнительные	
auto	Подключение к СД с использованием профиля по умолчанию.
-pass <PASSWORD>	Пароль профиля подключения
-profile <NAME>	Имя профиля подключения

Пример использования:

<pre>cts connect -profile TR07 -pass 5\$rt2t</pre>	Подключение к серверу доступа под профилем TR07 и указанным паролем.
--	--

Команда del cert

Команда предназначена для удаления корневых сертификатов.

Внимание! Для использования этой команды пользователь должен обладать правами суперпользователя.

Параметры	Описание
Обязательные	
-cert_type ca	Тип сертификата: корневой
Дополнительные	
-issuer_cn <REG_EXP>	Имя издателя сертификата
-issuer_o <REG_EXP>	Организация, выдавшая сертификат
-subject_cn <REG_EXP>	Имя владельца сертификата
-subject_o <REG_EXP>	Организация, для которой выдан сертификат

Внимание! Как минимум один из дополнительных параметров является обязательным.

Пример использования:

<pre>cts del cert -cert_type ca - subject_cn RootSC</pre>	Удаление корневого сертификата с именем владельца RootSC
---	--

Команда del profile

Команда предназначена для удаления профиля пользователя.

Параметры	Описание
Обязательные	
-name <NAME>	Имя профиля подключения
-user <USERNAME>	Имя пользователя

Пример использования:

cts del profile -name TR07 -user AdministratorGTC	Удаление профиля TR07 пользователя AdministratorGTC
--	---

Команда del server

Команда предназначена для удаления СД из списка доверенных.

Параметры	Описание
Обязательные	
-name <NAME>	Имя СД

Команда disconnect

Команда предназначена для отключения от СД.

Параметры	Описание
Дополнительные	
-profile <NAME>	Имя профиля подключения
-server <IP_ADDRESS>	Имя или IP-адрес сервера

Пример использования:

cts disconnect	Разрыв активного соединения с СД
----------------	----------------------------------

Команда events

Команда предназначена для просмотра журнала событий.

Параметры	Описание
Дополнительные	
-cat [INFO], [ERROR], [DEBUG]	Уровень критичности события
-from dd.mm.yyyy:hh:mm:ss	Начальные время и дата события при фильтрации событий
-to dd.mm.yyyy:hh:mm:ss	Конечные время и дата события при фильтрации событий
-user <NAME>	Имя пользователя

Пример использования:

cts events -cat ERROR -from 04.07.2016:00:00:00 -user AdministratorGTC	Просмотр списка зафиксированных в журнале сообщений о ошибках, произошедших в период с начала 4 июля 2016 года по текущий момент для всех профилей подключений пользователя AdministratorGTC
--	--

Команда import

Команда предназначена для импорта закрытого ключа. В ходе выполнения команды будет выполнен диалоговый скрипт для выбора ключевого носителя с закрытым ключом, хранилища для импортируемого ключа и набора энтропии.

Команда modify profile

Команда предназначена для редактирования профиля пользователя.

Параметры	Описание
Обязательные	
-name <NAME>	Имя профиля/соединения
-user <USERNAME>	Имя пользователя
Дополнительные	
-cert_path <CERTIFICATE_PATH>	Путь и название сертификата
-ctc <CONNECT_TRY_COUNT {0-99}>	Число попыток подключения
-cti <CONNECT_TRY_INTERVAL_IN_SEC {1 3 5 10 30 60 120 300 600}>	Интервал в секундах между попытками подключения
-dot {off <TIMEOUT_IN_SEC {0 60 300 600 1200 1800 3600 7200 14400 28800 86400}>}	Установка времени отключения после простоя
-lp <LOCAL_PORT>	Локальный порт
-mtu <MTU>	Количество байт в одном пакете
-proxy_auth {no basic ntlm}	Тип аутентификации при подключении к прокси-серверу
-proxy_ip <IP off>	IP-адрес или доменное имя прокси-сервера/отключение использования прокси-сервера для подключения к СД
-proxy_login <ID>	Логин прокси-сервера
-proxy_pass <PASS>	Пароль доступа к прокси-серверу
-proxy_port <PORT>	Порт прокси-сервера
-rol <on off >	Включение/отключение переключений при потере соединения.
-server <SERVER_ADDRESS>	Имя или IP-адрес сервера
-sp <SERVER_PORT>	Порт сервера

Пример использования:

cts modify profile -name TR07 -user AdministratorGTC -sp 88 -ctc 10 -cti 15	Установка для пользователя AdministratorGTC при подключении по профилю TR07 следующих настроек: <ul style="list-style-type: none"> •подключение через 88 порт сервера •10 попыток подключения с интервалом 15 секунд. Если при подключении имя пользователя должно вводиться в формате domain\user, необходимо использовать следующий синтаксис: domain\user.
---	---

Команда `resetparam`

Команда предназначена для сброса настроек к стандартному набору значений параметров:

- Номер порта на сервере доступа: 4433.
- Номер порта на абонентском пункте: 7500.
- MTU: 1450.
- Журналирование трафика: выкл.
- Количество попыток подключения: 3.
- Интервал между попытками: 10.
- Повторное подключение при обрыве связи: вкл.
- Отключение в случае неактивности: выкл.
- Запрет незащищенных соединений: выкл.
- Ключевое хранилище: RUTOKEN.
- Учетная запись по умолчанию: не задано.

Параметры	Описание
Дополнительные	
<code>-user <USERNAME></code>	Имя пользователя

Команда `request`

Команда предназначена для создания запроса на сертификат. В ходе выполнения команды будет выполнен диалоговый скрипт для получения данных о пользователе, набора энтропии и выбора ключевого носителя для сохранения на нём закрытого ключа.

Команда `setparam`

Команда предназначена для настройки профиля по умолчанию.

Параметры	Описание
Дополнительные	
<code>-ctc <CONNECT_TRY_COUNT {0-99}></code>	Число попыток подключения
<code>-cti <CONNECT_TRY_INTERVAL_IN_SEC {1 3 5 10 30 60 120 300 600}></code>	Интервал в секундах между попытками подключения
<code>-defprof <DEF_PROFILE></code>	Имя профиля подключения при нескольких профилях
<code>-dot {off <TIMEOUT_IN_SEC {0 60 300 600 1200 1800 3600 7200 14400 28800 86400}>}</code>	Установка времени отключения после простоя
<code>-lp <LOCAL_PORT></code>	Локальный порт
<code>-mtu <DEF_MTU></code>	Количество байт в одном пакете
<code>-pass <DEF_PASSWORD></code>	Пароль профиля подключения
<code>-pin <DEF_PIN></code>	Пин-код для файла ключа на носителе Рутокен
<code>-rol <DEF_RECONNECT_ON_LOSS {0-99}></code>	Число переподключений при потере соединения.
<code>-sp <SERVER_PORT></code>	Порт сервера
<code>-user <USERNAME></code>	Имя пользователя

Пример использования:

cts setparam -defprof LIABA01 -pass 7r%ty437u* -dot 28800 -rol 10	Задание профиля LIABA01 с указанным паролем для автоматического подключения при входе пользователя, времени отключения после простоя равным 8 часам (28800 секундам) и 10 переподключений при потере соединения.
---	--

Команда show all

Команда предназначена для просмотра всей информации о профилях.

Параметры	Описание
Дополнительные	
-user <USERNAME>	Имя пользователя

Команда show cert

Команда предназначена для просмотра информации о сертификатах.

Параметры	Описание
Дополнительные	
-cert_type {user ca}	Тип сертификата: пользователя / корневой
-issuer_cn <REG_EXP>	Имя издателя сертификата
-issuer_o <REG_EXP>	Организация, выдавшая сертификат
-hide_expired	Скрывать сертификаты с истекшим сроком действия
-subject_cn <REG_EXP>	Имя владельца сертификата
-subject_o <REG_EXP>	Организация, для которой выдан сертификат
-user <USERNAME>	Имя пользователя

Пример использования:

cts show cert -issuer_o SecurityCode -hide_expired	Просмотр корневых сертификатов от издателя SecurityCode, исключая истекшие
---	--

Команда show parameter

Команда предназначена для просмотра параметров по умолчанию.

Параметры	Описание
Дополнительные	
-user <USERNAME>	Имя пользователя

Команда show profile

Команда предназначена для просмотра списка профилей.

Параметры	Описание
Дополнительные	
-name <REG_EXP>	Имя профиля
-server <REG_EXP>	Имя или IP-адрес сервера

Параметры	Описание
-user <USERNAME>	Имя пользователя

Пример использования:

cts show profile -user Admin	Просмотр списка профилей пользователя Admin
------------------------------	---

Команда show serverlist

Команда предназначена для просмотра информации о доверенных СД.

Команда show stats

Команда предназначена для просмотра информации об активном подключении.

Параметры	Описание
Дополнительные	
-server <IP_ADDRESS>	Имя или IP-адрес сервера
-user <USERNAME>	Имя пользователя

Пример использования:

cts show stats -server SP30	Просмотр информации о подключениях к СД SP30
-----------------------------	--

Команда version

Команда предназначена для просмотра версии абонентского пункта.

Файлы контроля целостности**Просмотр списка файлов, поставленных на контроль**

Для просмотра списка файлов, поставленных на контроль целостности, и соответствующих им контрольных сумм используется специализированная утилита **ctsic**, расположенная в каталоге `/usr/sbin/ctsic`.

Для просмотра списка:

- Вызовите командную строку (см. стр.32) и введите команду

```
ctsic check --print
```

Повторное создание списка файлов, подлежащих контролю

Список файлов, подлежащих контролю целостности, содержится в файле `/etc/cts/filelist`. В некоторых случаях, например при обновлении операционной системы, включающем в себя установку новых версий библиотек, возникает необходимость в повторном создании списка файлов, которые должны быть поставлены на контроль.

Для повторного создания списка используется специализированная утилита `autoctsic`, расположенная в каталоге `/usr/bin`.

Внимание! Запустить утилиту может только пользователь с правами root.

Для создания списка:

- Вызовите командную строку (см. стр.32) и введите команду

```
autoctsic
```


Перерасчет контрольных сумм

Для перерасчета контрольных сумм необходимо выполнить следующее:

1. Повторно создать список файлов, подлежащих контролю целостности (см. стр. **40**).
2. Рассчитать новые контрольные суммы для файлов, содержащихся в повторно созданном списке. Для этого вызовите командную строку и введите команду:

```
ctsic compute
```

Внимание! Для абонентского пункта среднего уровня безопасности после выполнения приведенных выше операций необходимо повторно настроить механизм контроля целостности в ПАК "Соболь" (см. **п. 1** на стр. **15**).