КОД безопасности

Средство криптографической защиты информации

Континент-АП
Версия 4 (исполнения 4, 5, 6)

Руководство по эксплуатации

RU.АМБС.58.29.12.004 91

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Список сокращений

АП	Абонентский пункт
ЗПС	Закрытая (замкнутая) программная среда
КС	Контрольная сумма
КЦ	Контроль целостности
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПУ	Программа управления
СД	Сервер доступа
СЗИ	Средство или система защиты информации
СКЗИ	Средство криптографической защиты информации
УКЦ	Утилита "Континент-АП Контроль целостности"
CDP	CRL Distribution Point
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DNS	Domain Name System
IP	Internet Protocol
LVM	Logical Volume Manager
NTLM	NT LAN Manager
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator

Введение

Руководство предназначено для пользователей и администраторов изделия "Средство криптографической защиты информации "Континент-АП". Версия 4 (исполнения 4, 5, 6)" RU.АМБС.58.29.12.004 (далее — СКЗИ "Континент-АП", "Континент-АП", абонентский пункт, СКЗИ). В нем содержатся сведения, необходимые для установки, настройки и эксплуатации СКЗИ "Континент-АП" на базе операционных систем семейства Linux.

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

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505- 30- 20 или по электронной почте support@securitycode.ru.

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.

Глава 1
Общие сведения

Назначение и основные функции

СКЗИ "Континент-АП" предназначено для установления защищенного соединения и обмена зашифрованными данными с сервером доступа изделий "Аппаратно-программный комплекс шифрования "Континент". Версия 3.7" RU.88338853.501430.006 и "Аппаратно-программный комплекс шифрования "Континент". Версия 3.9" RU.88338853.501430.022 (далее — АПКШ "Континент") через общедоступные (незащищенные) сети.

"Континент-АП" реализует следующие основные функции:

- установление защищенного соединения и обмен зашифрованными данными с СД АПКШ "Континент";
- регистрация событий, связанных с функционированием СКЗИ;
- управление инфраструктурой открытых ключей;
- контроль целостности программного обеспечения, передаваемой и хранимой информации.

"Континент-АП" реализуется в трех исполнениях:

- исполнение 4 соответствует требованиям ФСБ России к криптографическим средствам класса КС1;
- исполнение 5 соответствует требованиям ФСБ России к криптографическим средствам класса КС2, работает совместно с АПМДЗ, соответствующим требованиям, действующим на территории Российской Федерации, для соответствия требованиям, установленным для класса защиты КС2;
- исполнение 6 соответствует требованиям ФСБ России к криптографическим средствам класса КС3, работает совместно с АПМДЗ и ОС/СЗИ, обеспечивающей функцию ЗПС, которые соответствуют требованиям, действующим на территории Российской Федерации, для соответствия требованиям, установленным для класса защиты КС3.

СКЗИ "Континент-АП" устанавливается на компьютеры, удовлетворяющие следующим системным требованиям:

Элемент	Требование
Операционная система	См. стр. **41**
Процессор, оперативная память	В соответствии с установленной ОС
Жесткий диск (свободное место)	300 Мбайт
Привод	Привод DVD/CD-ROM
Дополнительное аппаратное и/или программное обеспечение	• АПМДЗ (для исполнений 5, 6); • ОС/СЗИ с функцией обеспечения ЗПС (для исполнения 6)

"Континент-АП" представляет собой устанавливаемое на компьютер пользователя ПО, функционирующее совместно с комплексом "Континент". Для подключения к СД пользователь создает защищенное соединение в соответствии с настройками, переданными ему администратором. При этом обеспечивается зашифрование данных информационного обмена.

"Континент-АП" поддерживает соединение с СД по протоколу версий 3.X и 4.X.

При подключении к СД по протоколу версий 3.X:

- для соединения могут использоваться протоколы TCP или UDP;
- аутентификация пользователя выполняется с помощью сертификата.

При подключении к СД по протоколу версий 4.X:

- для соединения используется протокол TCP;
- аутентификация пользователя выполняется с помощью сертификата или логина и пароля учетной записи пользователя.

В процессе эксплуатации неизменность содержимого ПО СКЗИ "Континент-АП" контролируется с помощью утилиты контроля целостности.

Для диагностики проблем в работе ПО используется утилита "Сбор диагностической информации".

Внимание!

- Все службы, реализующие штатные механизмы удаленного управления операционной системой, должны быть отключены.
- Пропускная способность сетевого канала, по которому устанавливается соединение СКЗИ "Континент-АП" с СД, должна быть не менее 9,6 Кбит/с.
- При использовании "Континент-АП" совместно с ПАК Соболь" необходимо перед установкой "Континент-АП" установить ПАК "Соболь" и выполнить его инициализацию согласно эксплуатационной документации.
- Если установка операционной системы была выполнена с применением менеджера логических томов (LVM), совместная работа "Континент-АП" с ПАК "Соболь" в исполнениях 5 и 6 не поддерживается из-за функциональных ограничений ПАК "Соболь".

Принципы функционирования "Континент-АП"

При подключении "Континент-АП" к СД выполняется процедура установления соединения в соответствии с протоколом TLS, в ходе которой осуществляется взаимная аутентификация "Континент-АП" и СД. Завершается процедура установления соединения генерацией сеансового ключа, который используется для шифрования трафика между "Континент-АП" и СД.

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

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 34.10-2012.

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

В зависимости от требований, предъявляемых к доступу удаленных пользователей к защищаемым ресурсам, на "Континент-АП" может использоваться произвольное количество подключений, каждое из которых имеет индивидуальную настройку параметров.

Например, если в состав защищаемой сети входит несколько СД, для соединения данного "Континент-АП" с каждым из них (для протокола версий 3.X) используется отдельный профиль подключения.

При использовании протокола версий 4.X в настройках профиля формируется список подключений к доступным СД. Таким образом возможно соединение с несколькими СД в рамках одного профиля.

Правила безопасности

1. Никому не передавайте ключевые носители с закрытыми ключами.
2. В ситуациях, связанных с работой СКЗИ "Континент-АП", 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.

Уровни безопасности

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

Уровень безопасности	Описание
Низкий (исполнение 4)	Устанавливаются: • ПО абонентского пункта; • криптопровайдер "Код Безопасности CSP"
Средний (исполнение 5)	Требуется наличие АПМДЗ, соответствующего требованиям, действующим на территории Российской Федерации, для соответствия требованиям, установленным для класса защиты КС2. Устанавливаются: • ПО абонентского пункта; • криптопровайдер "Код Безопасности CSP"
Высокий (исполнение 6)	Требуется наличие АПМДЗ и ОС/СЗИ с функцией обеспечения ЗПС, которые соответствуют требованиям, действующим на территории Российской Федерации, для соответствия требованиям, установленным для класса защиты КС3. Устанавливаются: • ПО абонентского пункта; • криптопровайдер "Код Безопасности CSP"

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 (стр. **42**).

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.

По умолчанию "Континент-АП" запускается в обычном режиме. Для входа в режим администратора пользователь должен выбрать в списке главного меню приложений нужную утилиту или "Континент-АП (Режим Администратора)" и ввести пароль, подтверждающий права суперпользователя.

После входа в режим администратора пользователю становятся доступными операции, связанные с расширенными настройками "Континент-АП".

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 цифровой подписью удостоверяющего центра сертификации.

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

- сертификаты в кодировках 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 работы СКЗИ "Континент-АП" требуются следующие сертификаты:

- сертификат сервера доступа — для подтверждения подлинности сервера доступа, взаимодействующего с абонентским пунктом;
- сертификат удаленного пользователя — для аутентификации пользователя на сервере доступа;
- корневой сертификат — для подтверждения подлинности сертификата сервера доступа и сертификата пользователя.

Пользователь получает сертификаты от администратора безопасности любым защищенным способом или 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/истек;
- сертификат скомпрометирован;
- отсутствует сертификат удостоверяющего центра.

Необходимо использовать только действительные сертификаты.

Предусмотрена проверка сертификатов по CRL. CRL загружается и обновляется с помощью средств "Континент-АП".

Назначение ключевых носителей

Персональный ключевой носитель, выдаваемый пользователю администратором, предназначен для хранения и передачи ключевой информации — контейнера с закрытым ключом и пароля к нему. Могут использоваться USB-флеш-накопители и аппаратные носители следующих типов:

- USB-ключи и смарт-карты — Рутокен ECP, Рутокен Lite, Рутокен ECP 2.0, Рутокен S, Esmart, Esmart GOST, JaCarta PKI, JaCarta GOST, JaCarta 2 GOST, JaCarta GOST LT;
- идентификаторы DS1995, DS1996.

Для использования аппаратных носителей требуется установка их драйверов и сопутствующего ПО.

Контроль целостности

Функция контроля целостности предназначена для слежения за неизменностью содержимого файлов установленного ПО "Континент-АП" и связанных с ним библиотечных файлов ОС Linux и производится с помощью утилиты "Континент-АП Контроль целостности", входящей в дистрибутив "Континент-АП".

Производится сравнение текущих значений контрольных сумм контролируемых файлов и эталонных значений, рассчитанных в ходе установки СКЗИ "Континент-АП". Выполнение процедуры пересчета эталонных значений доступно пользователю с правами администратора ОС Linux.

Список файлов "Континент-АП", подлежащих контролю, и значения контрольной суммы для каждого из них хранятся в конфигурационном файле. Конфигурационный файл формируется при установке инсталляционного пакета.

КЦ установленного ПО осуществляется:

- при запуске СКЗИ "Континент-АП";
- установлении соединения с СД;
- вручную, с помощью УКЦ;
- по расписанию (настраивается с помощью УКЦ, по умолчанию ежедневно в 17:00 по системному времени).

Если в ходе проведения КЦ будет обнаружена ошибка, пользователь получит информационное сообщение о нарушении целостности.

Если в ходе проведения регламентной проверки целостности УКЦ будет обнаружено нарушение целостности и при этом "Континент-АП" будет активным, рабочие сессии с защищенными ресурсами будут продолжаться. При этом создание новых сессий будет заблокировано, а значок приложения в панели индикации ОС Linux будет дополнен предупреждающим элементом. В случае обнаружения нарушения целостности при неактивном ПО "Континент-АП" будет сделана соответствующая запись в журнале событий.

При нарушении целостности пользователю будет показываться сообщение о необходимости ее восстановления:

- при каждом запуске "Континент-АП";
- при каждой попытке установления соединения с СД комплекса "Континент" (если нарушение целостности обнаружено в ходе регламентного контроля целостности при наличии активного соединения).

Если "Континент-АП" используется совместно с ПАК "Соболь", проверка контрольных сумм также выполняется при загрузке операционной системы.

Результаты проверки заносятся в журнал событий.

Аудит

Все события от узлов сети, служб "Континент-АП", а также любые другие системные события, удовлетворяющие минимальным требованиям к хранению в журнале, фиксируются и хранятся в журнале. Сведения о данных событиях могут быть просмотрены пользователем.

В случае необходимости с помощью утилиты "Сбор диагностической информации", входящей в дистрибутив "Континент-АП", может быть создан архив с диагностической информацией о работе ПО.

Глава 2
Установка, удаление и обновление

Установка

Для установки ПО СКЗИ "Континент-АП" пользователь должен иметь права суперпользователя.

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

Название	Описание
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, с высоким — ks3
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, Рутокен и ESMART

Пакеты зависимостей, поставляемые совместно с дистрибутивом "Континент-АП", не являются обязательными к установке. При наличии в доступных официальных репозиториях ОС более новых версий пакетов рекомендуется использовать их. В таком случае переходите к п. **8**.

Если нет возможности использовать официальные репозитории ОС, то для установки используйте зависимые пакеты, поставляемые в комплекте с "Континент-АП", как описано далее в пп. **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, GosLinux, RHEL), используйте команду:

   ```
   yum localinstall *.rpm --disablerepo=*
   ```

   Для группы ОС, использующих менеджер пакетов deb (Astra, Debian, Ubuntu, HP ThinPro), используйте команду:

   ```
   dpkg -i *.deb
   ```

   Для ОС Альт 8 СП, Альт Линукс СПТ 7.0 используйте команду:

   ```
   apt-get install *.rpm
   ```

Для ОС ROSA используйте команду:

```
urpmi *.rpm
```

Для ОС Suse Linux используйте команду:

```
zypper --no-gpg-checks -n install *.rpm
```

4. Для поддержки внешних носителей следует установить дополнительное ПО. Перейдите в каталог token libs и далее перейдите в подкаталог с номером версии используемой операционной системы, например:

```
cd /token_libs/rpm/x86_64
```

5. Установите пакеты, содержащиеся в подкаталоге (см. п. **3**).

Внимание! Для корректной работы с абонентским пунктом для поддержки стороннего ПО рекомендуется устанавливать пакеты, размещенные в дистрибутиве "Континент-АП".

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 ОС, 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/rpm/x86_64
```

В подкаталоге хранятся три установочных пакета абонентского пункта: для низкого, среднего и высокого уровней безопасности.

8. Установите пакет, соответствующий требуемому уровню безопасности. Для этого используйте нужную команду, указав имя пакета.

Для группы ОС, использующих менеджер пакетов rpm (CentOS, GosLinux, RHEL), используйте следующие команды:

- для низкого уровня безопасности:

```
yum localinstall cts-4.1.0-415.ks1.el.x86_64.rpm
--disablerepo=*
```

- для среднего уровня безопасности:

```
yum localinstall cts-4.1.0-415.ks2.el.x86_64.rpm
--disablerepo=*
```

- для высокого уровня безопасности:

```
yum localinstall cts-4.1.0-415.ks3.el.x86_64.rpm
--disablerepo=*
```

Для группы ОС, использующих менеджер пакетов deb (Astra, Debian, Ubuntu, HP ThinPro), используйте следующие команды:

- для низкого уровня безопасности:

```
dpkg -i cts-4.1.0-415.ks1_amd64.deb
```

- для среднего уровня безопасности:

```
dpkg -i cts-4.1.0-415.ks2_amd64.deb
```

- для высокого уровня безопасности:

```
dpkg -i cts-4.1.0-415.ks3_amd64.deb
```

Внимание! Установка "Континент-АП" на компьютеры с ОС Astra Linux 1.6 среднего и высокого уровней безопасности имеет некоторые особенности. Подробнее процедуру установки см. на на стр. 42.

Для ОС Альт 8 СП, Альт Линукс СПТ 7.0 используйте команду:

- для низкого уровня безопасности:

```
apt-get install cts-4.1.0-415.ks1.el.x86_64.rpm
--disablerepo=*
```

- для среднего уровня безопасности:

```
apt-get install cts-4.1.0-415.ks2.el.x86_64.rpm
--disablerepo=*
```

- для высокого уровня безопасности:

```
apt-get install cts-4.1.0-415.ks3.el.x86_64.rpm
--disablerepo=*
```

Для ОС ROSA используйте следующие команды:

- для низкого уровня безопасности:

```
urpmi cts-4.1.0-415.ks1.el.x86_64.rpm
```

- для среднего уровня безопасности:

```
urpmi cts-4.1.0-415.ks2.el.x86_64.rpm
```

- для высокого уровня безопасности:

```
urpmi cts-4.1.0-415.ks3.el.x86_64.rpm
```

Для ОС Suse Linux 15 используйте следующие команды:

- для низкого уровня безопасности:

```
zypper --no-gpg-checks -n install
cts-4.1.0-415.ks1.el.x86_64.rpm
```

- для среднего уровня безопасности:

```
zypper --no-gpg-checks -n install
cts-4.1.0-415.ks2.el.x86_64.rpm
```

- для высокого уровня безопасности:

```
zypper --no-gpg-checks -n install
cts-4.1.0-415.ks3.el.x86_64.rpm
```

После установки пакета в 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. 15).

10. Перезагрузите компьютер.

После перезагрузки компьютера на экране в области уведомлений появится значок абонентского пункта.

Цвет пиктограммы указывает на состояние соединения с сервером доступа:

Пиктограмма	Цвет	Пояснение
	Серый	Отключено (соединение не установлено)
	Серый/зеленый (с предупреждением)	• Выключена проверка по CRL; • Незарегистрированная копия ПО
	Зеленый	Соединение установлено

В главном меню (например, в группе "Сеть") ОС Linux появятся значки приложений, входящих в "Континент-АП".

Внимание! Расположение пункта меню для запуска графического менеджера пакетов будет различным у каждой ОС.

Станут доступны следующие приложения:

Название	Описание
Континент-АП	Запуск ПО "Континент-АП"
Континент-АП (Режим Администратора)	Запуск ПО "Континент-АП" (в режиме администратора)
Континент-АП Сбор диагностической информации	Экспорт отчета о состоянии работоспособности "Континент-АП"
Континент-АП Сбор диагностической информации (Режим Администратора)	Экспорт отчета о состоянии работоспособности "Континент-АП" (в режиме администратора)
Континент-АП Импорт закрытого ключа	Адаптация и добавление закрытого ключа, сформированного на основе принципов в ОС семейства Windows, для использования на компьютерах с установленной ОС семейства Linux
Континент-АП Регистрация	Регистрация ПО на сервере регистрации компании "Код Безопасности"
Континент-АП Контроль целостности	Контроль целостности дистрибутива и установленного на компьютере ПО "Континент-АП"
Континент-АП Контроль целостности (Режим Администратора)	Контроль целостности дистрибутива и установленного на компьютере ПО, пересчет контрольных сумм"Континент-АП" (в режиме администратора)

Удаление

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".

   Внимание! Расположение пункта меню для запуска графического менеджера пакетов будет различным у каждой ОС.

2. В окне графического пакетного менеджера удалите установленный пакет "Континент-АП".

Для удаления с помощью консольного пакетного менеджера:

- Запустите консоль и выполните команду удаления пакета.

  Для группы ОС, использующих менеджер пакетов rpm (CentOS, GosLinux, RHEL), используйте команду:

  ```
  yum remove cts
  ```

  Для группы ОС, использующих менеджер пакетов deb (Astra, Debian, HP ThinPro, Ubuntu), используйте команду:

  ```
  dpkg -P cts
  ```

  Для ОС Альт 8 СП, Альт Линукс СПТ 7.0 используйте команду:

  ```
  apt-get remove cts
  ```

  Для ОС ROSA используйте команду:

  ```
  urpme cts
  ```

  Для ОС Suse Linux используйте команду:

  ```
  zypper remove cts
  ```

Обновление

Для обновления ПО абонентского пункта:

1. Выполните процедуру установки программного обеспечения абонентского пункта, как описано на стр. **12**.
2. Выполните обновление списка файлов для расчета контроля целостности.

   Для этого выполните от имени суперпользователя следующую команду:

   ```
   /usr/share/cts/bin/autoctsic
   ```

3. Перезагрузите компьютер.

Изменение уровня безопасности

При необходимости изменить уровень безопасности ПО абонентского пункта выполните следующие действия:

1. Выполните процедуру удаления программного обеспечения абонентского пункта, как описано на стр. **15**.
2. Выполните установку ПО абонентского пункта (см. стр. **12**), используя команды для требуемого уровня безопасности.

Глава 3
Настройка и эксплуатация

Ввод в эксплуатацию

Подготовка к работе

Ввод "Континент-АП" в эксплуатацию состоит из следующих последовательных этапов:

1. Установка "Континент-АП" (см. стр. **12**).
2. Регистрация ПО (см. стр. **18**).
3. Настройка профилей подключения (см. стр. **22**).
4. Установка корневых и пользовательских сертификатов (см. стр. **32**).
5. Получение необходимых сертификатов безопасности (см. стр. **28**).
6. Установка серверных сертификатов (см. стр. **32**).
7. Установка CRL (если необходима проверка сертификатов по CRL, см. стр. **34**).
8. Настройка параметров работы "Континент-АП" (см. стр. **36**).

Запуск "Континент-АП"

СКЗИ "Континент-АП" стартует автоматически после запуска ОС.

На экране появляется основное окно программы, а на панели задач отображается значок  .

Для запуска "Континент-АП":

- Откройте главное меню приложений и выберите в нем, например в разделе "Сеть", "Континент-АП".

  На экране появится основное окно "Континент-АП", а в правом углу панели задач ОС Linux появится значок программы.

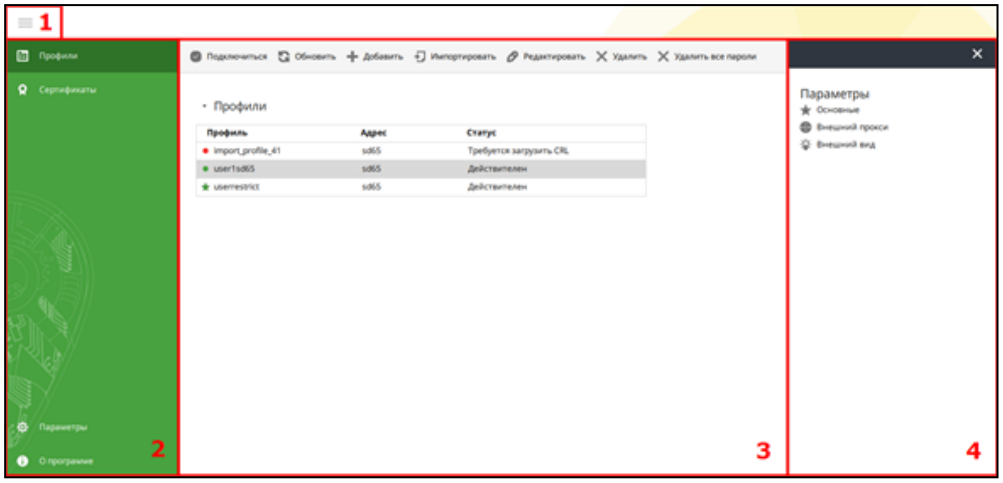
Вызов контекстного меню "Континент-АП" с панели задач ОС Linux позволяет выполнить следующие действия:

- выполнить подключение с профилем по умолчанию;
- разорвать текущее соединение или установить настроенное соединение;
- открыть настройки параметров работы ПО;
- завершить работу ПО (при этом, по умолчанию, приложение закроется, но установленное подключение разорвано не будет).

При двойном нажатии на значок "Континент-АП" на панели задач ОС Linux устанавливается или разрывается соединение с использованием профиля по умолчанию.

Примечание. Также для свертывания основного окна "Континент-АП" можно использовать кнопки  и  в правом верхнем углу окна. Для закрытия программы выберите в контекстном меню пункт "Выход".

Пользовательский интерфейс основного окна



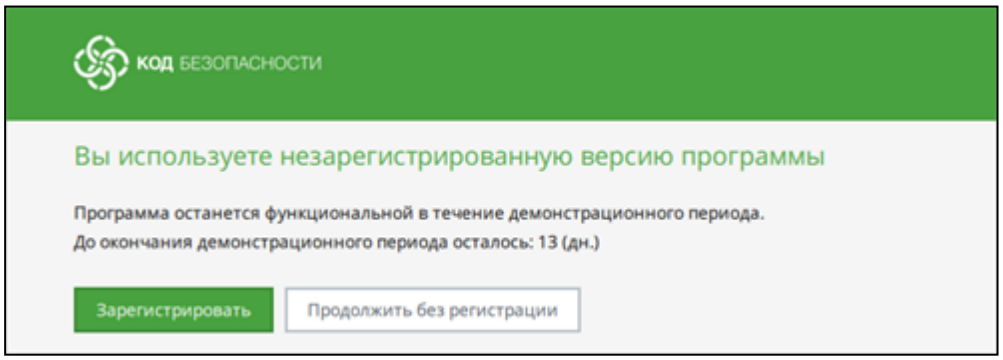
В верхней части основного окна расположена кнопка (1) переключения развернутого/свернутого вида главного меню.

В левой части основного окна расположен список разделов главного меню (2), в центральной отображаются подробности настройки параметров работы "Континент-АП" (3), в правой — список параметров (4). По умолчанию открывается список профилей подключения.

Внимание! Некоторые кнопки навигации могут быть темно-серого цвета. Это означает, что они неактивны, так как не все поля диалога, необходимого для дальнейшей работы, заполнены. После того как все необходимые данные будут введены, кнопка будет активирована и сменит цвет на зеленый.

Регистрация "Континент-АП"

Если "Континент-АП" не зарегистрирован, то при его запуске появится предложение зарегистрировать программу на сервере регистрации компании "Код Безопасности". Доступны онлайн- и офлайн-регистрация.

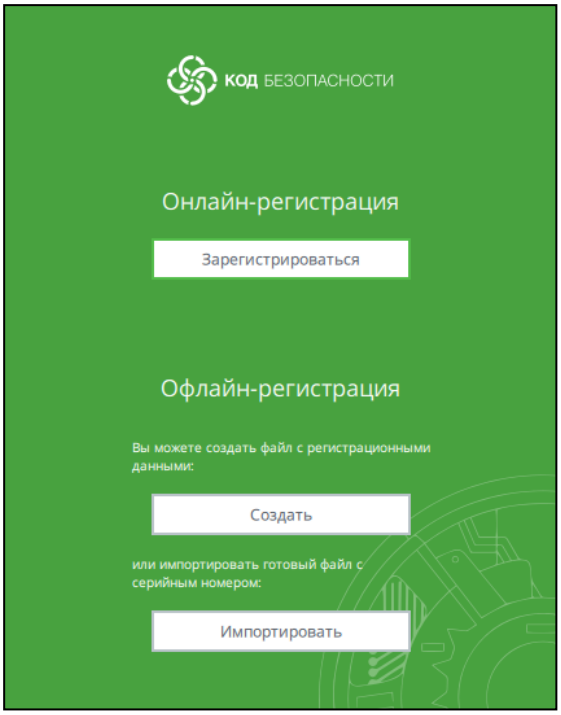


Срок демонстрационного периода работы "Континент-АП" ограничен и составляет 14 дней со дня установки ПО. Количество дней, оставшихся до окончания демонстрационного периода, отображается в разделе "О программе". Если в течение этого срока "Континент-АП" не зарегистрировать, то при каждом следующем запуске на экране будет появляться предложение зарегистрировать ПО, значок на панели задач будет дополнен синим восклицательным знаком. В случае отказа от регистрации по истечении 14 дней работа "Континент-АП" будет прекращена.

Для онлайн-регистрации "Континент-АП":

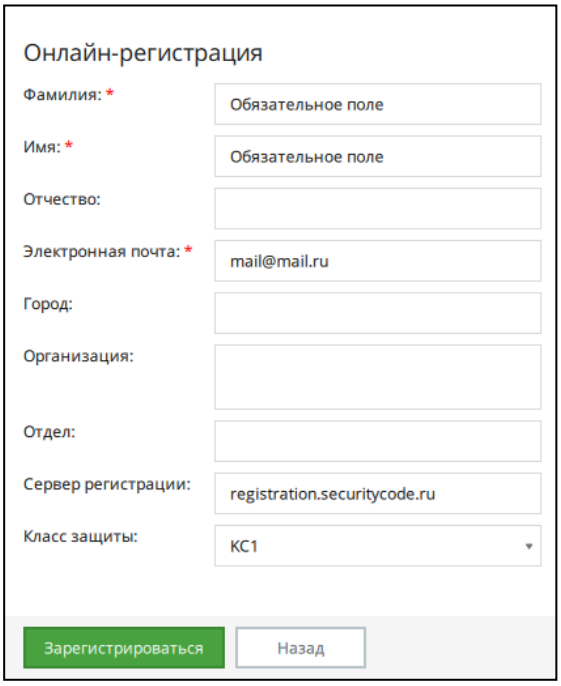
1. Нажмите кнопку "Зарегистрировать" в окне регистрации или выберите в главном меню приложений "Континент- АП Регистрация".

   Откроется окно регистрации.



2. Выберите онлайн-регистрацию, нажав кнопку "Зарегистрироваться".

   На экране появится диалоговое окно регистрации.



3. Введите требуемые параметры и нажмите кнопку "Зарегистрироваться".

   Начнется процесс регистрации и подключения к указанному серверу. При его успешном завершении на экране появится соответствующее информационное окно.

После регистрации "Континент-АП" в разделе "О программе" появится регистрационный номер программы.

Для офлайн-регистрации "Континент-АП":

1. В случае отсутствия доступа к серверу регистрации откройте окно регистрации, выберите офлайн-регистрацию и нажмите кнопку "Создать".

   На экране появится диалоговое окно регистрации.

   Примечание. Если вы ранее вводили данные в поля формы для онлайн-регистрации, они будут сохранены автоматически и повторно заполнять форму не потребуется.

2. Заполните требуемые параметры и нажмите кнопку "Готово".

   На экране появится стандартное окно сохранения файла.

3. Сохраните файл с данными и передайте его на сервер регистрации для получения файла с серийным номером.

4. После получения файла с серийным номером нажмите кнопку "Импортировать" в окне регистрации "Континент-АП".

   На экране появится стандартное окно выбора файла.

5. Укажите нужный файл и нажмите кнопку "Открыть".

   При успешном завершении процесса регистрации на экране появится соответствующее информационное окно.

Настройка подключений

О профилях подключений

Для подключения к серверу доступа пользователь "Континент-АП" использует профиль, представляющий собой набор настраиваемых параметров.

Профиль подключения создается и настраивается администратором или самим пользователем.

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

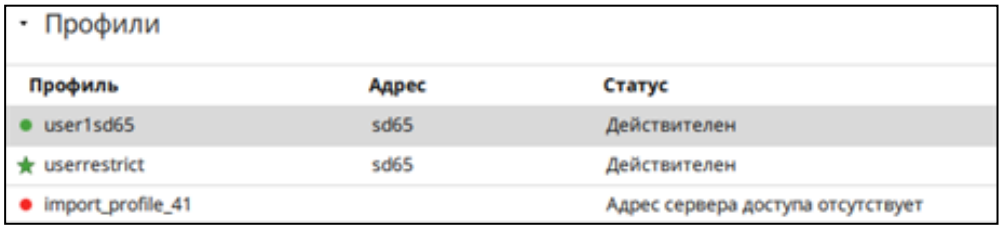
Если к серверу доступа должны подключаться несколько зарегистрированных на компьютере пользователей, для каждого такого пользователя необходимо создать отдельный профиль подключения.

Примечание. Каждый пользователь видит только собственные профили подключения.

Список профилей подключений

Список профилей подключений отображается в соответствующем разделе меню настроек абонентского пункта. Оно же по умолчанию является основным окном "Континент-АП".

Зеленый цвет отметки указывает на то, что профиль настроен верно. Звездочкой отмечен профиль, назначенный профилем подключения по умолчанию.



Примечание. Если профиль подключения заполнен неверно или неполно, отметка рядом с профилем будет красной, а в поле "Статус" появится сообщение об ошибке.

Для вызова списка профилей подключений:

- Откройте раздел "Профили" в главном меню "Континент-АП".

Примечание. Если главное меню будет развернуто из значка на панели задач, раздел "Профили" со списком подключений будет открыт по умолчанию.

В основной части окна в разделе "Профили" отобразится список созданных (настроенных или импортированных) профилей пользователя, от имени которого выполнен вход в систему. Если профили не были созданы, список будет пуст.

При работе со списком профилей подключений предусмотрено выполнение следующих операций:

- подключение к СД с выбранным профилем;
- обновление списка профилей;
- создание нового профиля подключения;
- импорт профиля подключения;
- просмотр и редактирование параметров профиля;
- удаление профиля из списка;
- удаление сохраненного пароля из выбранного профиля;
- удаление всех сохраненных паролей.

Параметры профиля подключения

Параметры настроек делятся на универсальные и те, которые зависят от версии применяемого протокола соединения с СД:

Параметр	Описание
Использовать по умолчанию	Профиль, с помощью которого автоматически будет устанавливаться соединение с СД после запуска "Континент-АП" (если настройка активирована)
Имя профиля	Наименование профиля, отображаемое в списке используемых профилей
Версия протокола	Номер версии протокола соединения с СД
Тип аутентификации (только для версий 4.X)	Выбор типа аутентификации пользователя по сертификату или паре "логин–пароль"
Сертификат	Имя выбранного сертификата пользователя
Ключевой контейнер	Имя выбранного ключевого контейнера. Для выбора ключевого контейнера предназначена кнопка "Установить". При ее использовании открывается дополнительное окно выбора среди доступных ключевых контейнеров. Любая операция с ключевым контейнером должна быть подтверждена паролем
Список подключений (только для версий 4.X)	Перечень подключений к нескольким СД, созданным с помощью комплекса "Континент" версии 4. Для просмотра или редактирования элементов списка предназначена кнопка "Добавить". При ее использовании открывается дополнительное окно управления элементами списка подключений
Адрес подключения (только для версий 4.X)	Адрес подключения к СД в формате "адрес:порт"
Адрес (только для версий 3.X)	IP-адрес или имя сервера доступа
Удаленный порт (только для версий 3.X)	Порт СД для установления соединения
Протокол (только для версий 3.X)	Тип используемого транспортного протокола (TCP/UDP)

Создание, редактирование и удаление профиля подключения

Создание нового профиля подключения

Для связи с СД комплекса "Континент" необходимо создать и настроить профиль подключения или импортировать профиль, ранее созданный и настроенный средствами СД.

Описание параметров настройки профиля см. стр. **21**.

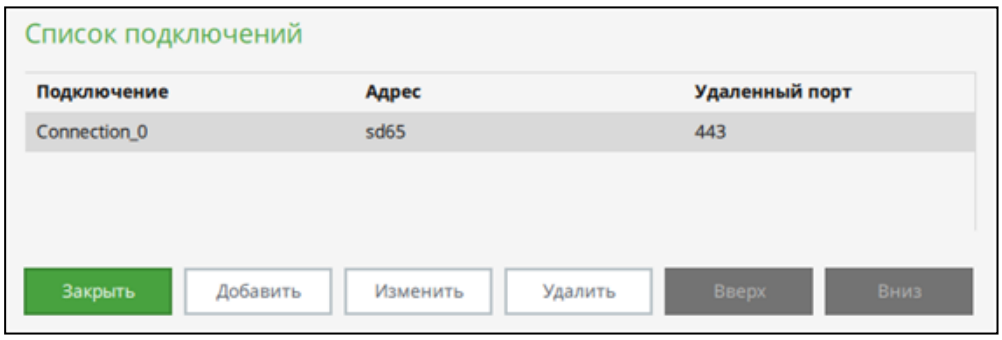
Внимание! Перед созданием нового профиля подготовьте файл сертификата пользователя, полученный от администратора сервера доступа, и внешний носитель с ключевым контейнером, если ключевой контейнер сохранен на нем, а не в Системном хранилище локального компьютера (Системе). Файл сертификата можно сохранить на жестком диске или на внешнем носителе.

Для соединения с различными СД (для протокола версий 4.X) с помощью одного профиля предусмотрен список подключений.

Если не было установлено соединение с первым СД, "Континент-АП" автоматически перейдет к попытке соединения со следующим СД, и так до тех пор, пока соединение не будет успешно установлено.

Подключения в списке заполняются в порядке попыток соединения с СД. Порядок соединений и их параметры можно менять.

При выборе типа аутентификации по логину и паролю учетной записи пользователя (для протокола версий 4.X) необходимо набрать энтропию для биологического датчика случайных чисел для обеспечения шифрования канала при использовании профиля.

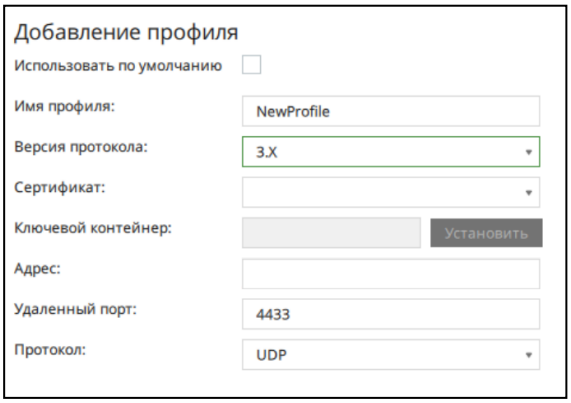


Для создания нового профиля и настройки его параметров (для протокола версий 3.X):

1. Запустите "Континент-АП".
2. В главном меню "Континент-АП" выберите раздел "Профили".

   В области отображения информации откроется список имеющихся профилей подключения.
3. Для добавления нового профиля подключения нажмите кнопку "Добавить" на панели инструментов.

   В правой части основного окна появится список настроек профиля.



Примечание. Если планируете в дальнейшем использовать этот профиль для подключения по умолчанию, поставьте отметку в соответствующем поле.

4. Укажите адрес СД, имя профиля и версию протокола.

Внимание! При смене протокола значение в поле "Порт" меняется автоматически. Если выбран протокол версий 4.X, в поле "Адрес" необходимо указывать значение, которое указано в поле "CommonName" сертификата сервера. Имя должно представлять собой DNS-имя или IP-адрес сервера. Должно быть написано латиницей без пробелов, может содержать цифры, символы "**.**" и "**-**", не может начинаться или оканчиваться этими символами. Максимальное количество символов — 256.

5. Выберите используемый пользовательский сертификат из раскрывающегося списка доступных сертификатов. Имя сертификата появится в поле, а в поле "Ключевой контейнер" появится имя соответствующего ключевого контейнера.

Примечание. Если был добавлен новый сертификат, поле "Ключевой контейнер" останется пустым и его надо будет добавить вручную. Значение появится только в том случае, если ранее на этом компьютере (даже для другого профиля) была сохранена пара "Сертификат" – "Ключевой контейнер".

6. Укажите номер порта вручную, при необходимости.
7. Выберите тип протокола.
8. Нажмите кнопку "Сохранить" внизу окна.

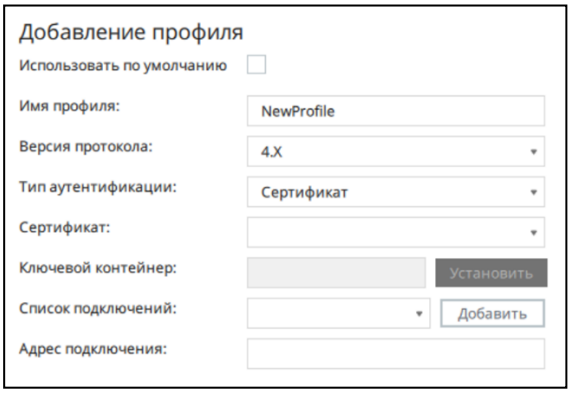
   Профиль будет сохранен и появится в общем списке профилей.

Для создания нового профиля и настройки его параметров (для протокола версий 4.X):

1. Запустите "Континент-АП".
2. В главном меню "Континент-АП" выберите раздел "Профили".

   На экране появится список имеющихся профилей подключения.
3. На панели инструментов нажмите кнопку "Добавить".

   На экране появится список настроек профиля, подобный следующему.



Примечание. Если планируете в дальнейшем использовать этот профиль для подключения по умолчанию, поставьте отметку в соответствующем поле.

4. Укажите адрес СД, имя профиля и версию протокола.

Внимание! Если выбран протокол версий 4.X, в поле "Адрес" необходимо указывать значение, которое указано в поле "CommonName" сертификата сервера. Имя должно представлять собой DNS-имя или IP-адрес сервера. Должно быть написано латиницей без пробелов, может содержать цифры, символы "**.**" и "**-**", не может начинаться или оканчиваться этими символами. Максимальное количество символов — 256.

5. Из раскрывающегося списка выберите тип аутентификации:
   - аутентификация с помощью сертификата пользователя;
   - аутентификация по логину и паролю учетной записи пользователя.

6. Если выбрана аутентификация с помощью сертификата пользователя, выберите используемый пользовательский сертификат из раскрывающегося списка доступных сертификатов.

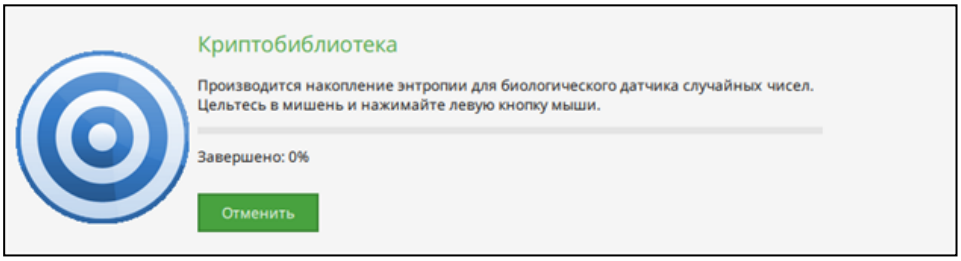
   Имя сертификата появится в поле, а в поле "Ключевой контейнер" появится имя соответствующего ключевого контейнера. Перейдите к п. **9**.

   Примечание. Если был добавлен новый сертификат, поле "Ключевой контейнер" останется пустым. Значение появится только в том случае, если ранее на этом компьютере (даже для другого профиля) была сохранена пара "Сертификат" – "Ключевой контейнер".

7. Если была выбрана аутентификация по паре "логин– пароль", введите в открывшиеся поля данные учетной записи пользователя.
8. Выберите подключение из списка или добавьте новое.
9. Проверьте правильность введенных параметров и нажмите кнопку "Сохранить" внизу окна.

   Если была выбрана аутентификация по сертификату, профиль будет сохранен и появится в общем списке профилей.

   Если была выбрана аутентификация по паре "логин–пароль", начнется процесс накопления энтропии для биологического датчика случайных чисел (для исполнения 4). Следуйте инструкциям на экране.



   После завершения процесса накопления энтропии появится сообщение о том, что созданный профиль подключения зарегистрирован.

Для редактирования профиля подключения:

1. Выберите нужный профиль и нажмите кнопку "Редактировать" на панели инструментов.

   Внимание! Изменять настройки можно только для профиля, не используемого для активного подключения.

   В правой части основного окна появится список настроек профиля.
2. Внесите необходимые изменения и нажмите кнопку "Сохранить".

Для импорта профиля подключения:

1. Для импорта ранее созданного с помощью ПУ СД профиля подключения нажмите кнопку "Импортировать" на панели инструментов.

   Откроется окно менеджера файлов ОС Linux.
2. Выберите нужный конфигурационный файл и нажмите кнопку "Открыть".

   Появится сообщение о вводе пароля импорта конфигурации.
3. Введите полученный от администратора пароль импорта профиля конфигурации и нажмите кнопку "ОК".

   Откроется окно ввода пароля доступа к ключевому контейнеру.

   Введите полученный от администратора пароль доступа к ключевому контейнеру и нажмите кнопку "ОК".

   Откроется окно выбора ключевого носителя для сохранения закрытого ключевого контейнера.
4. Выберите нужный ключевой носитель и нажмите кнопку "ОК".

   Появится сообщение об успешном завершении импорта.
5. Нажмите кнопку "ОК".

Если профиль был импортирован без ключевого контейнера, появится сообщение о необходимости выбора ключевого контейнера в настройках профиля.

После того как все параметры будут назначены, появится сообщение, предлагающее произвести пробное подключение с использованием импортированного профиля.

6. Для установки пробного подключения нажмите кнопку "Да", для возврата в раздел "Профили" нажмите кнопку "Нет".

Для удаления профиля подключения:

1. Для удаления профиля подключения выберите нужный профиль и нажмите кнопку "Удалить" на панели инструментов.
2. Нажмите кнопку "ОК" в появившемся окне подтверждения.

Подключение к серверу доступа

Внимание!

- Подключение к СД 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 СД необходимо, чтобы другие пользователи выполнили выход из системы.
- Перед подключением к СД необходимо подключить к компьютеру ключевой носитель с закрытым ключом пользователя.

"Континент-АП" позволяет подключиться к СД двумя способами:

- автоматическое подключение после старта "Континент-АП" с профилем, назначенным по умолчанию;
- подключение в ручном режиме.

При необходимости можно сохранить пароль для профиля подключения. Для этого необходимо установить соответствующий флажок в окне подключения и успешно установить соединение с СД. При следующих подключениях пароль для этого профиля запрашиваться не будет.

Примечание. При аутентификации по сертификату сохраняются пароли закрытого ключа и ключевого носителя.

Для удаления сохраненного пароля требуемого профиля или всех сохраненных паролей необходимо использовать кнопки "Удалить пароль" или "Удалить все пароли" соответственно.

Автоматическое подключение с профилем по умолчанию

Для настройки подключения:

1. Выберите в меню параметров пункт "Основные", раздел "Режим запуска" и уставите отметку в поле "Автоматическое подключение с профилем по умолчанию"(подробнее о настройках режима запуска см. стр. **36**).
2. Если ранее при создании или импорте профилей не был назначен профиль по умолчанию, выберите один из списка и поставьте в его настройках отметку "Использовать по умолчанию".

Внимание! Если в настройках разрешено автоматическое подключение при старте системы, но не будет назначен профиль по умолчанию, при следующем запуске системы соединение установлено не будет. Чтобы назначить профиль по умолчанию, выполните п. **2**.

При следующем запуске системы подключение с данным профилем будет установлено автоматически.

Внимание! Если в настройках указано не разрывать соединение при выходе из "Континент-АП", при следующем входе подключение с профилем по умолчанию будет произведено в фоновом режиме и появится сообщение о том, что соединение установлено.

В ОС без 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.

Подключение в ручном режиме

Данный способ подключения используется, когда политика безопасности компании запрещает автоматическое подключение к СД при старте системы.

Для подключения к СД в ручном режиме из панели задач ОС Linux:

1. Запустите "Континент-АП".
2. Наведите указатель на значок программы в области панели задач и нажмите правую кнопку мыши.
3. Выберите пункт "Установить соединение", а затем — имя требуемого профиля.

   Примечание. При выборе профиля с помощью пункта "Установить соединение" пользователь видит только наименования профилей, без указания их типа.

   Начнется процесс подключения с выбранным профилем. При подключении к СД значок на панели задач станет зеленым.

Для подключения к СД в ручном режиме с профилем по умолчанию:

Внимание! Если ранее при создании или импорте профилей ни один не был назначен профилем по умолчанию, предварительно выберите один профиль из списка и поставьте в его настройках отметку "Использовать по умолчанию" (подробнее о редактировании профиля см. на стр. 22).

1. Запустите "Континент-АП".
2. Наведите указатель на значок программы в области панели задач и дважды нажмите левую кнопку мыши.

   Начнется процесс подключения с профилем по умолчанию. При подключении к СД значок на панели задач станет зеленым.

Для подключения к СД в ручном режиме из основного окна АП:

1. Запустите "Континент-АП".
2. В главном меню "Континент-АП" выберите раздел "Профили".

   На экране появится список имеющихся профилей подключения.
3. В списке профилей выберите требуемый профиль.
4. На панели инструментов нажмите кнопку "Подключиться".

   Начнется процесс подключения с выбранным профилем. При подключении к СД значок на панели задач станет зеленым.

Разрыв соединения с сервером доступа

Для разрыва соединения с СД из панели задач ОС Linux:

- Наведите указатель на значок программы в области панели задачи и дважды нажмите левую кнопку мыши.

  Соединение с СД будет разорвано, значок на панели задач станет серым.

Для разрыва соединения с СД из основного окна АП:

1. В главном меню "Континент-АП" выберите раздел "Профили".
2. В списке профилей выберите профиль, который используется для активного подключения.
3. На панели инструментов нажмите кнопку "Отключиться".

   Соединение с СД будет разорвано, значок на панели задач станет серым.

Внимание !

- Если после установления соединения с СД была выполнена блокировка пользователя ОС, соединение не разрывается.
- Если при установленном соединении с СД выполнить смену пользователя и войти в ОС под другим пользователем, у первого будет выполнен разрыв соединения.
- При одновременном входе двух и более пользователей в ОС соединение не сможет установить никто из них.

Вход в режим администратора

Режим администратора предназначен для управления УКЦ и более тонких настроек работы "Континент-АП".

По умолчанию "Континент-АП" запускается в обычном режиме. Для входа в режим администратора пользователь должен выбрать в списке главного меню приложение "Континент-АП" или его утилиты, доступные в режиме администратора, и ввести пароль, подтверждающий права суперпользователя.

В режиме администратора пользователю доступны следующие операции:

- расширенные настройки работы "Континент-АП":
  - управление запросами добавления других серверных сертификатов;
  - управление проверкой сертификатов по CRL;
  - управление настройкой работы системы после истечения срока действия CRL;
  - управление автоматическим скачиванием CRL;
  - управление периодом скачивания CRL;
- пересчет контрольных сумм с помощью УКЦ;
- добавление и удаление корневых сертификатов;
- просмотр журнала событий;
- добавление файлов дампов при экспорте диагностической информации.

Для запуска "Континент-АП" в режиме администратора:

1. Завершите работу "Континент-АП", если он включен.
2. Откройте главное меню приложений и выберите в нем, например в разделе "Сеть", "Континент-АП (Режим Администратора)".
3. Введите пароль для подтверждения прав администратора.

   "Континент-АП" будет запущен, на панели задач появится его значок, на экране откроется основное окно интерфейса.
4. Для возврата в обычный режим перезапустите "Континент-АП", выбрав в главном меню пункт "Континент-АП" без пометки "Режим Администратора".

Для запуска УКЦ в режиме администратора:

1. Откройте главное меню приложений и выберите в нем, например в разделе "Сеть", "Континент-АП Контроль целостности (Режим Администратора)".
2. Введите пароль для подтверждения прав администратора.

   УКЦ "Континент-АП" будет запущена, и на экране появится окно утилиты с результатом проверки контрольных сумм.

Для запуска утилиты сбора диагностической информации в режиме администратора:

1. Откройте главное меню приложений и выберите в нем, например в разделе "Сеть", "Континент-АП Сбор диагностической информации (Режим Администратора)".
2. Введите пароль для подтверждения прав администратора.

   Утилита будет запущена, и на экране появится окно для настройки параметров сбора диагностической информации.

Глава 4
Управление сертификатами

СКЗИ "Континент- АП" позволяет добавлять сертификаты в хранилище, создавать запросы на издание сертификата пользователя и осуществлять запись закрытых ключей на съемный носитель или в Систему (хранилище на локальном компьютере пользователя).

Для работы с "Континент- АП" необходимы корневые сертификаты, сертификаты пользователя и сертификаты сервера, получаемые в соответствии с общим порядком, установленным конкретным удостоверяющим центром. Процедура создания запроса на выдачу сертификата по алгоритму ГОСТ Р 34.10–2012 приводится на стр. **28**.

Примечание. Допустимо использовать действительный уникальный сертификат пользователя, выпущенный ранее удостоверяющим центром.

Для передачи сертификатов рекомендуется использовать отчуждаемый носитель.

Примечание. В качестве ключевых носителей в комплексе могут использоваться аппаратные носители следующих типов:

- USB-флеш-накопители;
- USB-ключи и смарт-карты — Рутокен ECP, Рутокен Lite, Рутокен ECP 2.0, Рутокен S, Esmart, Esmart GOST, JaCarta PKI, JaCarta GOST, JaCarta 2 GOST, JaCarta GOST LT;
- идентификаторы DS1995, DS1996.

После получения всех сертификатов пользователь должен установить сертификаты в локальное хранилище компьютера средствами ПО "Континент- АП" (см. стр. **32**).

Создание запроса

Запрос на получение сертификата создается пользователем средствами ПО "Континент-АП" по требованию администратора безопасности. Одновременно с запросом средствами криптопровайдера генерируется закрытый ключ пользователя.

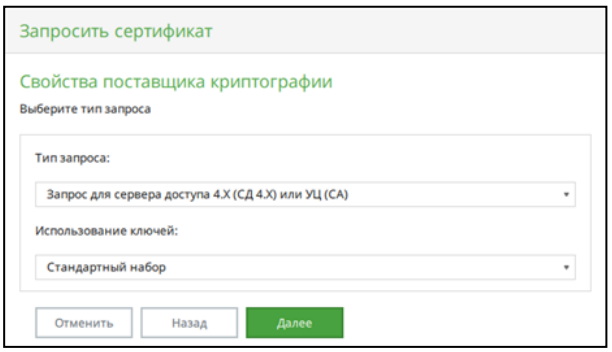
Запрос в виде файла сохраняется в указанную пользователем папку, ключевой контейнер с закрытым ключом сохраняется на ключевом носителе, указанном в настройках.

Примечание. Перед тем как приступить к созданию запроса, приготовьте чистый отформатированный ключевой носитель для записи ключевого контейнера.

Для создания запроса на получение сертификата:

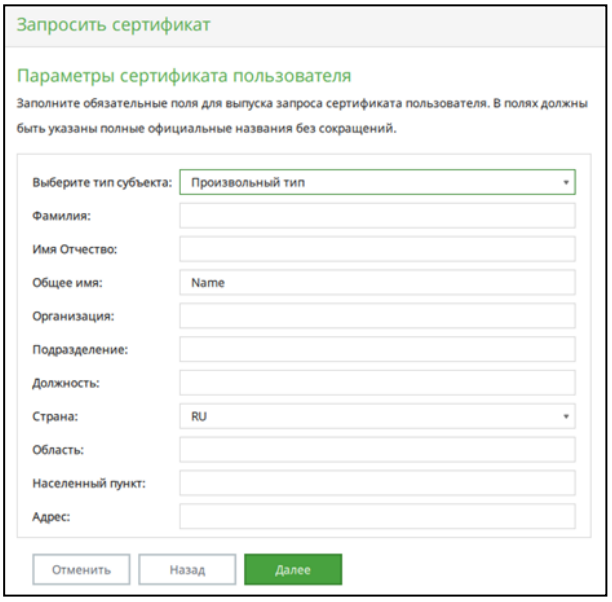
1. Выберите в главном меню "Континент-АП" пункт "Сертификаты" и перейдите на вкладку "Пользовательские сертификаты".
2. На панели инструментов нажмите кнопку "Создать запрос".

   На экране появится диалог, подобный следующему.



3. Выберите нужные пункты меню:
   - в поле "Тип запроса" выберите в раскрывающемся списке тип запроса на сертификат:
     - "Запрос для менеджера конфигурации 4.X (СД 4.X) или УЦ (CA)" (по умолчанию) — формат запроса для создания сертификата менеджером конфигурации (или СД 3.9.1 в режиме работы протокола 4.X) или внешним центром сертификации (алгоритм по ГОСТ Р 34.10–2012);
     - "Запрос для сервера доступа 3.X (СД 3.X)" — формат запроса для создания сертификата в ПУ СД (алгоритм по ГОСТ Р 34.10–2012);
   - в поле "Использование ключей" выберите из раскрывающегося списка набор использования ключей:
     - Стандартный набор (минимально необходимые параметры для функционирования ключа шифрования);
     - Расширенный набор (выбор использования дополнительных параметров ключа шифрования, если это предусмотрено политикой информационной безопасности компании).
4. Нажмите кнопку "Далее".

   На экране появится диалог для ввода параметров запроса.

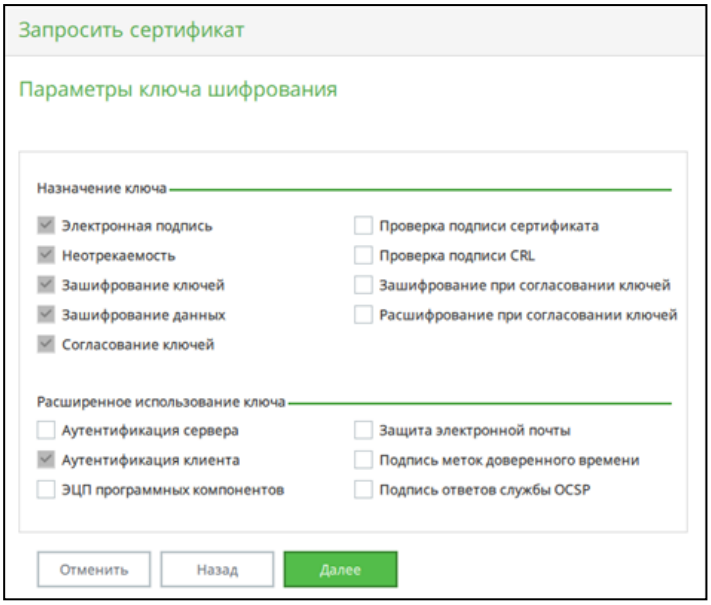


5. В поле "Выберите тип субъекта" укажите в раскрывающемся списке тип пользователя, создающего запрос:
   - Произвольный тип (по умолчанию);
   - Физическое лицо;
   - Физическое лицо с доверенностью от юридического;
   - Индивидуальный предприниматель;
   - Юридическое лицо.
6. Заполните остальные параметры диалога.

   Внимание! Поля, подчеркнутые красной линией и помеченные красным восклицательным знаком, обязательны для заполнения.
7. Нажмите кнопку "Далее".

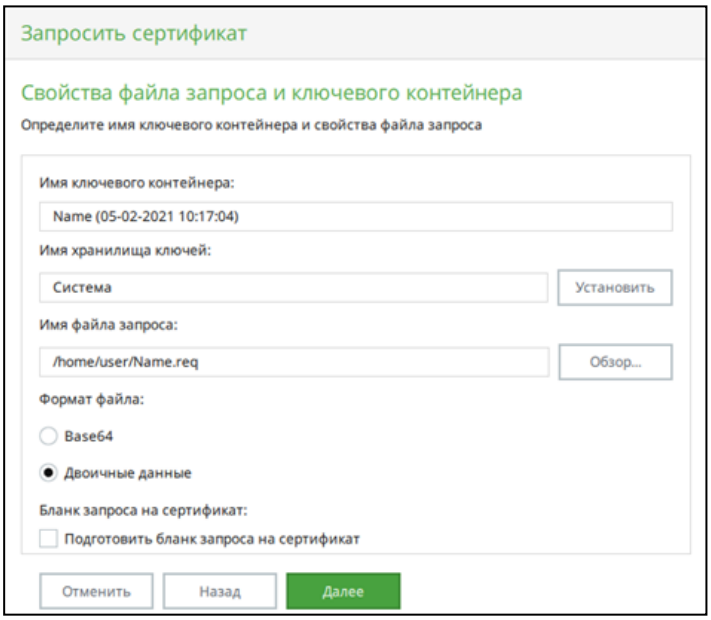
   Если был выбран расширенный набор параметров использования ключа (см. стр. **29**), на экране появится диалог выбора параметров.

   Примечание. Если был выбран стандартный набор параметров использования ключа, на экране появится диалог для ввода имени ключевого контейнера и имени файла для запроса сертификата. Перейдите к п. **9**.



8. Укажите необходимые параметры ключа шифрования и нажмите кнопку "Далее".

На экране появится диалог для определения свойства файла запроса и ключевого носителя.



9. Укажите:

- имя ключевого контейнера;

  Примечание. По умолчанию запрос сохраняется в файле с расширением *.req и именем, содержащим имя пользователя, создающего запрос, а также текущие время и дату.

- тип ключевого носителя, введя название ключевого хранилища (по умолчанию закрытый ключ сохраняется в Системе) (для исполнений 4, 5). Для выбора ключевого хранилища нажмите кнопку "Установить" и выберите в открывшемся окне тип ключевого носителя;
- формат, в котором будет сохранен файл;
- в поле "Подготовить бланк запроса на сертификат" установите отметку, если необходимо сохранить версию запроса для печати.

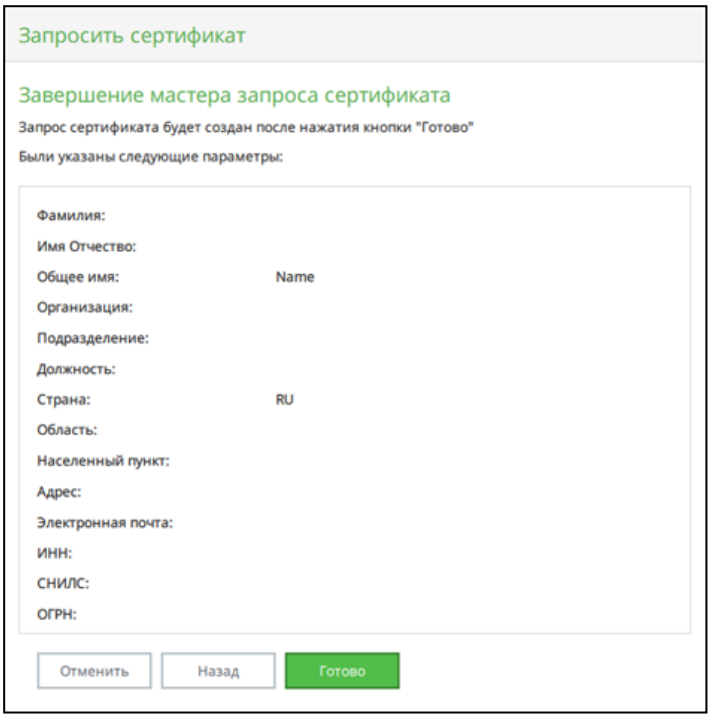
  Примечание. По умолчанию запрос сохраняется в файле с расширением *.html и именем, содержащим имя пользователя, создающего запрос, а также текущие время и дату.

Для изменения расположения или имени файла с электронной или бумажной формой запроса нажмите кнопку "Обзор…", расположенную справа от соответствующего поля. В открывшемся окне менеджера файлов ОС Linux, появившемся на экране, выполните следующие действия:

- укажите диск (папку) для создания файла;
- укажите имя файла запроса;
- нажмите кнопку "Сохранить".

10. Нажмите кнопку "Далее".

Появится сообщение о завершении работы мастера запроса сертификата, и на экране отобразятся параметры создаваемого запроса.



11. Нажмите кнопку "Готово".

Криптопровайдер приступит к созданию закрытого ключа.

Процедура создания закрытого ключа описана на стр. **31**.

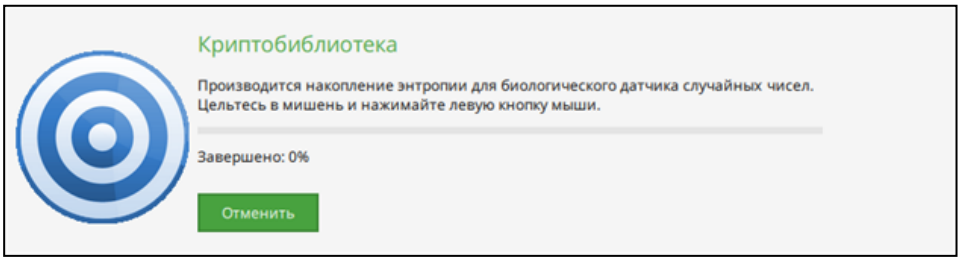
После завершения процедуры на экране появится сообщение о завершении создания запроса на сертификат.

12. Нажмите кнопку "ОК" в окне сообщения для завершения процедуры создания запроса.

Передайте созданный файл запроса администратору безопасности. При этом можно пользоваться общедоступной сетью передачи данных, например, переслать файл как вложение электронной почты.

Для формирования закрытого ключа:

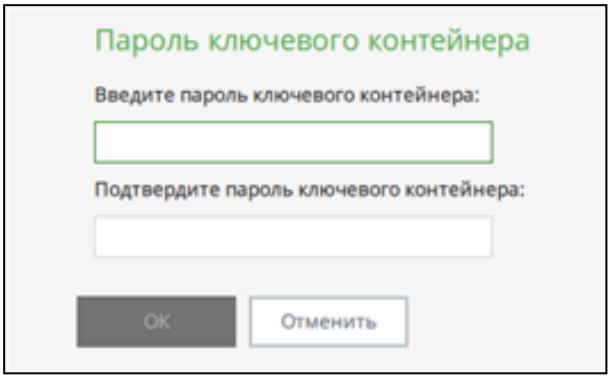
1. После нажатия в окне завершения работы мастера запроса сертификата кнопки "Готово" на экране появится окно накопления энтропии для биологического датчика случайных чисел.



Примечание. Если используется физический датчик случайных чисел ПАК "Соболь", набор энтропии выполняется автоматически и на экране не отображается. Вместо окна накопления энтропии появится окно ввода пароля. Перейдите к п. **3**.

2. Следуйте указаниям инструкции на экране и дождитесь завершения набора энтропии.

   После завершения процедуры на экране появится диалог ввода пароля для доступа к содержимому ключевого контейнера.



3. Введите и подтвердите пароль для доступа к создаваемому ключевому контейнеру и нажмите кнопку "OK".

Примечание. Длина пароля должна быть не менее 6 символов.

Начнется создание запроса и криптографического контейнера. После успешного завершения операции на экране появится соответствующее информационное сообщение.

Внимание! Если используемый съемный носитель содержит файлы, имена которых совпадают с именами записываемых файлов, то:

- файлы на USB-флеш-накопителе будут автоматически переименованы и сохранены;
- файлы на Рутокен будут перезаписаны.

4. Нажмите кнопку "OK" и извлеките носитель, если закрытый ключ был сохранен на нем.

Импорт и удаление сертификатов

Для импорта сертификатов:

1. Выберите в главном меню "Континент-АП" раздел "Сертификаты" и вкладку с нужным видом сертификата.

   В области отображения информации появится список установленных сертификатов.

2. На панели инструментов выберите категорию и нажмите кнопку "Импортировать".

   На экране появится стандартное окно открытия файла.

3. Укажите файл загружаемого сертификата и нажмите кнопку "Открыть".

   Начнутся загрузка и установка сертификата. После успешного завершения операции на экране появится соответствующее информационное сообщение.

4. Нажмите кнопку "OK".

Внимание! Сертификат пользователя не может быть удален, если он привязан к профилю подключения.

Для удаления сертификата пользователя:

1. Выберите в главном меню "Континент-АП" раздел "Профили" и откройте окно редактирования профиля.

2. Выберите другой возможный сертификат пользователя и нажмите кнопку "Сохранить".
3. Выберите в главном меню "Континент-АП" раздел "Сертификаты" и вкладку "Пользовательские сертификаты".

   В области отображения информации появится список установленных сертификатов.
4. На панели инструментов выберите категорию и нажмите кнопку "Удалить".

   На экране появится информационное сообщение о необходимости подтверждения операции.
5. Нажмите кнопку "ОК".

Для удаления корневого или серверного сертификата:

1. Выберите в главном меню "Континент-АП" раздел "Сертификаты" и вкладку с нужным видом сертификата.

   В области отображения информации появится список установленных сертификатов.
2. На панели инструментов выберите категорию и нажмите кнопку "Удалить".

   На экране появится информационное сообщение о необходимости подтверждения операции.
3. Нажмите кнопку "ОК".

Импорт закрытого ключа

"Континент-АП" может использовать закрытые ключи, созданные на других компьютерах с помощью других ОС.

Администратор безопасности формирует ключевой контейнер с закрытым ключом пользователя, сохраняет его 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.

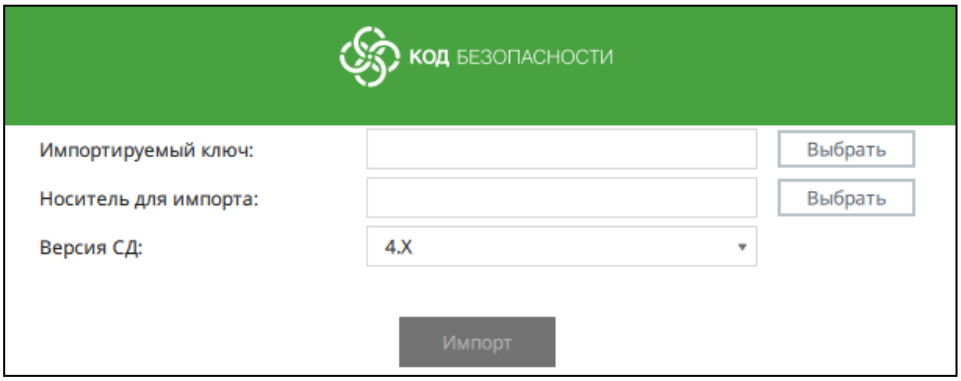
Для сохранения импортируемого закрытого ключа могут быть использованы:

- локальное хранилище компьютера (для исполнений 4, 5);
- исходный носитель с закрытым ключом, полученный от администратора безопасности;
- другой внешний носитель.

Для импорта закрытого ключа:

1. Вставьте ключевой носитель, полученный от администратора безопасности.
2. В главном меню (например, в группе "Сеть") ОС Linux выберите утилиту "Континент-АП Импорт закрытого ключа".

   На экране появится окно утилиты импорта ключей.



3. Для того чтобы указать место, где находится импортируемый ключевой контейнер, нажмите кнопку "Выбрать" и выберите хранилище ключей в открывшемся окне.
4. Нажмите кнопку "ОК".
5. Для того чтобы указать место, куда будет сохранен импортируемый ключевой контейнер, нажмите кнопку "Выбрать" и выберите хранилище ключей в открывшемся окне.
6. Выберите версию протокола соединения с СД в открывающемся списке.
7. Нажмите кнопку "Импорт".
8. Следуйте указаниям инструкции на экране и дождитесь завершения.

   Импортируемый ключ будет сохранен.

Просмотр сведений о сертификате

Получить сведения о сертификате можно с помощью средств "Континент-АП".

Для просмотра сведений о сертификате:

1. Выберите в главном меню "Континент-АП" пункт "Сертификаты", а затем вкладку с требуемым типом сертификатов на панели инструментов.

   В области отображения информации появится список установленных сертификатов.
2. Вызовите окно сведений о сертификате двойным щелчком левой кнопки мыши по соответствующей строке списка установленных сертификатов.

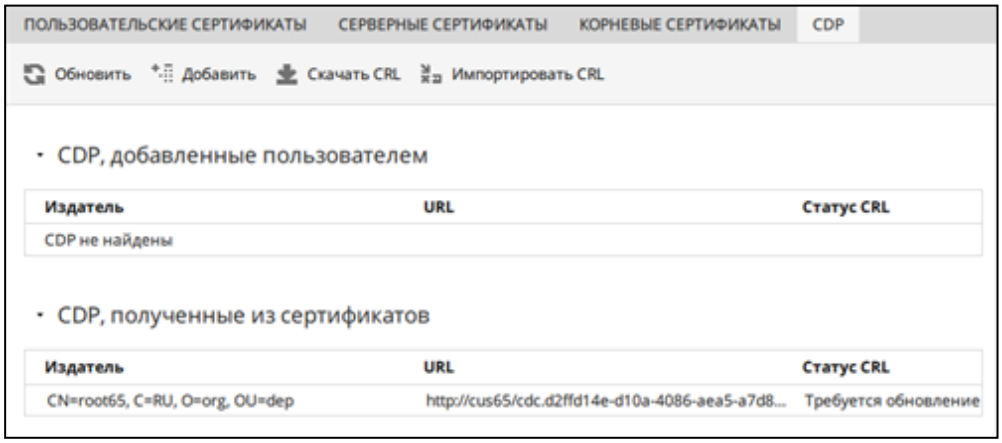
   Откроется стандартное окно сведений о сертификате.

Управление CRL

СКЗИ "Континент-АП" позволяет в автоматическом или ручном режиме получать CDP, а также скачивать CRL для проверки валидности используемых сертификатов.

Настройка CDP

Если используемые сертификаты содержат информацию о CDP, "Континент-АП" получит ее при импорте сертификатов. Для автоматической загрузки CDP импортируйте пользовательский, корневой или серверный сертификаты, как описано на стр. 32. Ниже приведен пример CDP, полученных из корневого сертификата, который был импортирован в систему.



Если же импортированные сертификаты не содержат CDP, то можно добавить список CDP вручную.

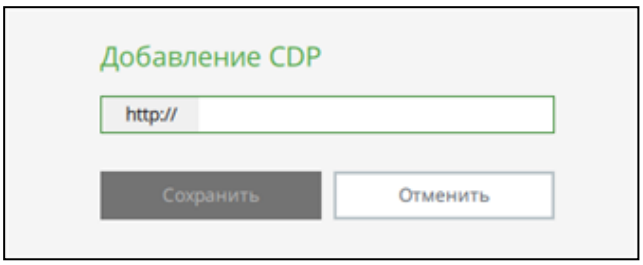
Для настройки списка CDP вручную:

1. Выберите в главном меню "Континент-АП" пункт "Сертификаты", вкладку "CDP".

   В области отображения информации основного окна появится список используемых CDP.

2. Нажмите кнопку "Добавить".

   На экране появится окно для ввода URL CDP.



3. Введите адрес CDP и нажмите кнопку "ОК".

   На экране произойдет возврат во вкладку "CDP" с обновленным списком параметров.

4. Для редактирования или удаления добавленного пользователем CDP выберите его в соответствующем списке и нажмите на панели инструментов кнопку "Редактировать" или "Удалить".

5. Подтвердите вносимые изменения.

Загрузка CRL

Автоматическая загрузка CRL происходит в результате добавления CDP после импорта сертификатов.

CRL также может быть добавлен вручную с помощью кнопки "Скачать CRL".

Если по какой-либо причине CRL не удалось скачать или он был удален из системы, в таблице CDP отобразится соответствующее состояние CRL.

Чтобы обновить сразу весь список CRL, выполните скачивание CRL вручную.

Для импорта файла CRL:

1. Выберите в главном меню "Континент-АП" раздел "Сертификаты" и вкладку "CDP".

   В области отображения информации появится список имеющихся CDP.

2. Нажмите кнопку "Импортировать CRL".

   На экране появится стандартное окно открытия файла.

3. Укажите загружаемый файл CRL и нажмите кнопку "Открыть".

   Начнется загрузка. После успешного завершения операции на экране появится соответствующее информационное сообщение.

4. Нажмите кнопку "ОК".

Для загрузки файлов CRL вручную:

1. Выберите в меню настроек "Континент-АП" пункт "Управление сертификатами", а затем вкладку "CDP" на панели инструментов.

   В области отображения информации основного окна появится список CDP.

   Примечание. Если CDP не прописан в установленном сертификате или не добавлен пользователем ранее, то необходимо добавить CDP (см. выше процедуру настройки списка CDP).

2. Нажмите на панели инструментов кнопку "Скачать CRL".

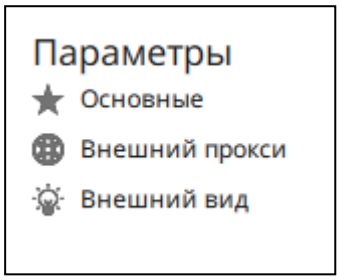
   Начнется загрузка. После успешного завершения операции на экране появится соответствующее информационное сообщение.

3. Нажмите кнопку "ОК".

Глава 5
Управление работой "Континент-АП"

Настройка параметров работы "Континент-АП"

Изменение параметров ПО "Континент- АП" осуществляется через меню настроек, вызов которого происходит при выборе пункта "Параметры" в главном меню основного окна "Континент-АП".



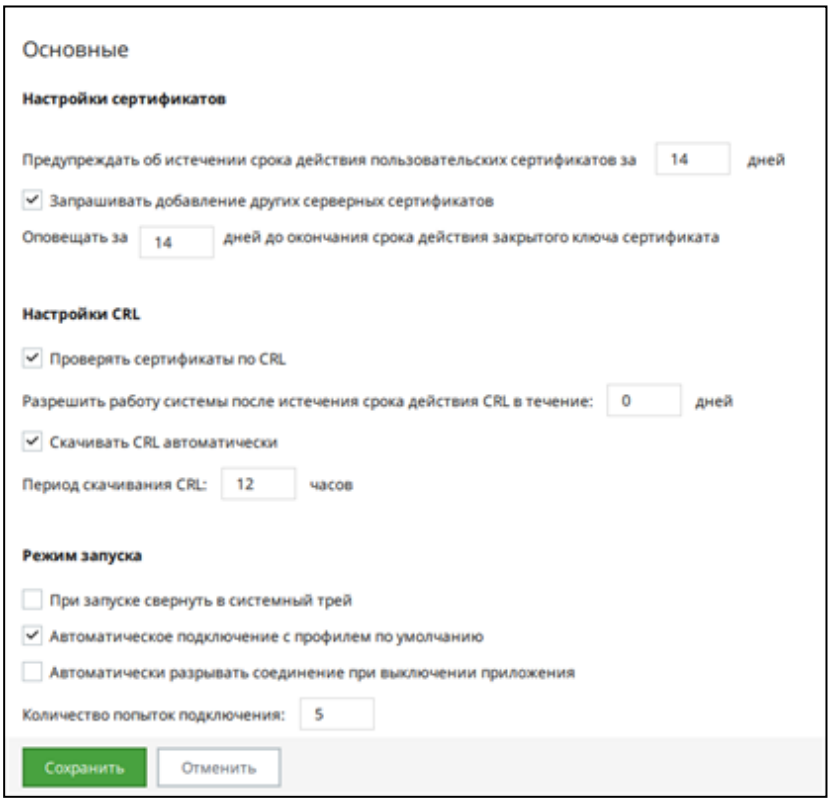
Основные настройки

Для настройки "Континент-АП":

1. Выберите в меню настроек пункт "Основные".

   В области отображения информации основного окна откроется соответствующее подменю.

Внимание! Для изменения настроек сертификатов и CRL необходимо запустить АП от имени администратора.



2. Выберите период для старта получения предупреждения об истечении срока действия сертификата пользователя.

3. Если политика информационной безопасности компании позволяет, для автоматического добавления серверного сертификата СД при первом подключении к данному серверу установите отметку в поле "Запрашивать добавление других серверных сертификатов".

Внимание! Для корректной работы "Континент-АП" необходимо заранее выполнить импорт издателя (корневого сертификата) сертификата сервера.

4. Для организации проверки подлинности сертификата по CRL установите флажок "Проверять сертификаты по CRL".

Внимание!
- Проверка по CRL выполняется только для профилей с протоколом версий 4.X.
- Отключение проверки сертификатов по CRL понижает уровень безопасности. Также при выключении данной настройки ранее отозванные сертификаты вновь будут считаться действительными.

5. Для настройки периода автоматического обновления сертификата CRL установите флажок "Скачивать CRL автоматически" и укажите нужный период в соответствующем поле.
6. Выберите режим отображения ПО после запуска.
7. Для автоматического подключения с профилем по умолчанию после старта системы установите отметку в соответствующее поле. Для ручного выбора профиля подключения снимите отметку.
8. Для настройки автоматического разрыва соединения после выхода из "Континент-АП" установите отметку в соответствующем поле (по умолчанию опция не активирована).
9. При необходимости укажите требуемое количество попыток подключения (по умолчанию — 5).

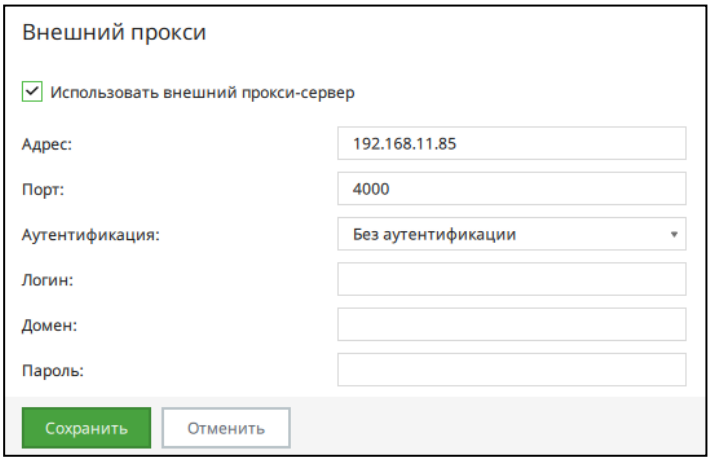
Внешний прокси

Внимание! Данные настройки прокси-сервера будут использоваться при соединении с СД и при онлайн-регистрации.

Для настройки подключения через внешний прокси-сервер:

1. Выберите в меню настроек пункт "Внешний прокси".

   На экране появится список параметров прокси, подобный следующему.



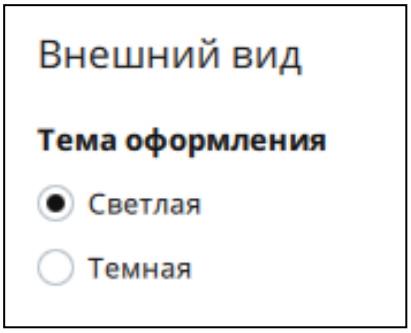
2. Установите отметку в поле "Использовать внешний прокси-сервер".
3. В поле "Адрес" введите IP-адрес или имя прокси-сервера. В поле "Порт" — порт для подключения к прокси-серверу.
4. Выберите способ аутентификации из раскрывающегося списка.
5. При необходимости укажите имя домена, логин и пароль.
6. Для завершения настройки и применения введенных или исправленных значений параметров нажмите кнопку "Сохранить".

Внешний вид

Для настройки вида интерфейса "Континент-АП":

1. Выберите в меню настроек пункт "Внешний вид".

   В области отображения информации основного окна появится соответствующий список настроек.



2. Выберите тему оформления.

   Внешний вид интерфейса "Континент-АП" и его утилит будет изменен.

Просмотр событий

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

Примечание. При высоком уровне безопасности (исполнение 6) только Администратор имеет право на чтение файла логов.

Для просмотра событий:

- С помощью любого приложения для просмотра текста откройте файл с событиями журнала:

  ```
  /var/log/cts.log
  ```

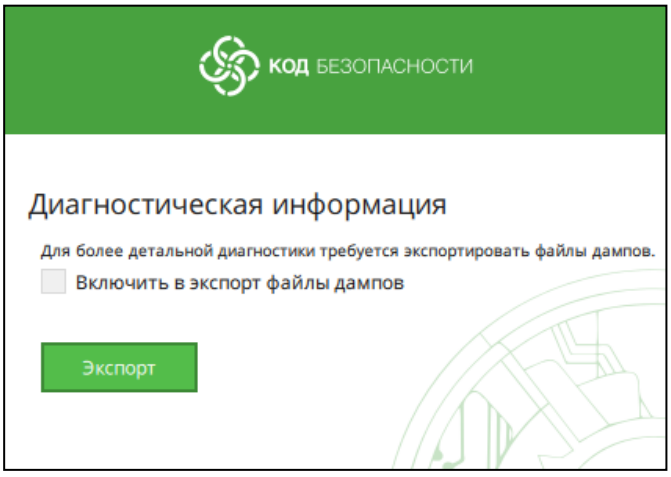
  Для каждого события приводятся следующие сведения:

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

Для сбора диагностической информации:

1. Запустите "Континент-АП Сбор диагностической информации".

   Появится предложение об экспорте диагностической информации.



2. Для включения в сборку файлов дампов поставьте отметку в соответствующее поле (доступно только в режиме администратора).

   Примечание. При включении файлов дампов в экспортный файл формирование отчета занимает более продолжительное время.

3. Нажмите кнопку "Экспорт".

   На экране появится окно для работы с файловой системой.

4. Укажите место хранения и название файла архива и нажмите кнопку "Сохранить".

   В случае успешного сохранения файла появится соответствующее сообщение.

Контроль целостности

Контроль целостности у "Континент-АП" осуществляется:

- при запуске ПО;
- при установлении соединения с СД;
- вручную, с помощью УКЦ;
- по расписанию (настраивается с помощью УКЦ, по умолчанию ежедневно в 17:00 по системному времени).

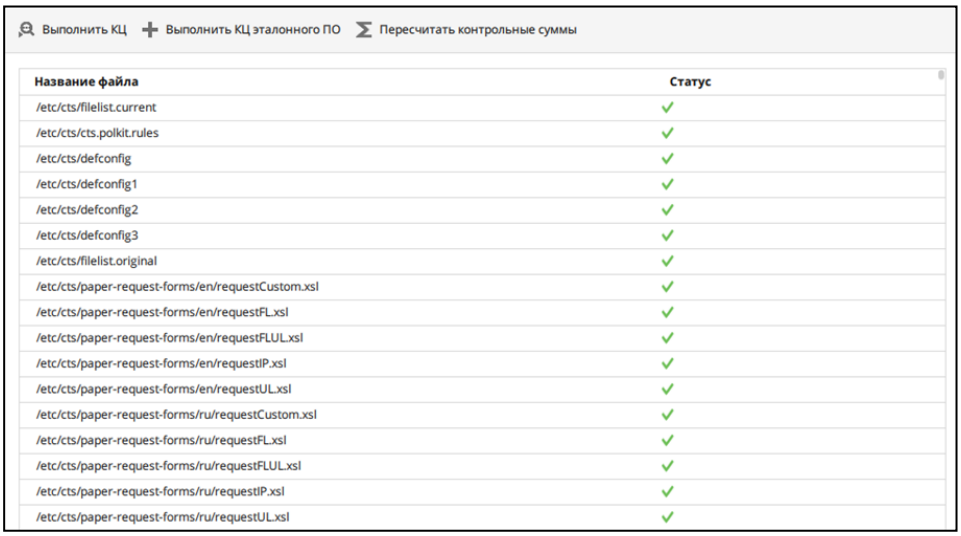
Для того чтобы пересчитать контрольные суммы, необходимо запустить СКЗИ "Континент-АП" в режиме администратора.

Для запуска УКЦ:

- Откройте главное меню приложений и выберите в нем, например, в разделе "Сеть", "Континент-АП Контроль целостности".

  Проверка начнется автоматически, и на экране появятся основное окно утилиты с результатом проверки и информационное сообщение о том, что проверка КЦ выполнена.

  Значок ✓ означает, что файл успешно прошел проверку.



Для пересчета контрольных сумм:

1. Откройте главное меню приложений и выберите в нем, например в разделе "Сеть", "Континент-АП Контроль целостности (Режим Администратора)".

   На экране появится окно подтверждения прав администратора.

2. Введите пароль и нажмите кнопку "Да".

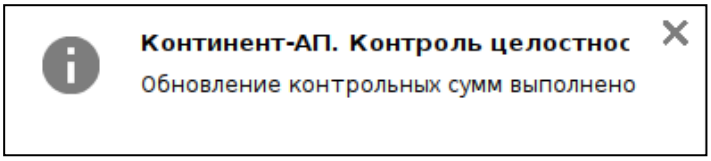
   Проверка КЦ начнется автоматически, и на экране появятся основное окно утилиты с результатом проверки и информационное сообщение о том, что проверка КЦ выполнена.

3. В основном окне УКЦ выберите на панели инструментов пункт "Пересчитать контрольные суммы".

   На экране появятся окно подтверждения запуска процедуры и предупреждение о том, что эталонные значения контрольных сумм будут обновлены.

4. Нажмите кнопку "ОК".

   Будет выполнен пофайловый пересчет контрольных сумм "Континент-АП". После его успешного завершения на экране появится информационное окно.

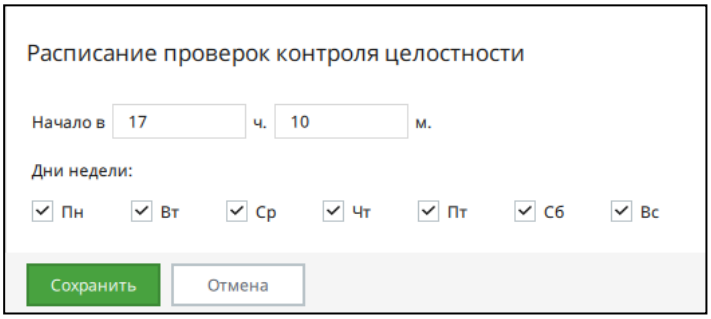


Для настройки расписания КЦ:

Внимание! Настройка расписания КЦ доступна только в режиме администратора.

1. В левом нижнем углу окна УКЦ нажмите кнопку "Параметры" ( ).

   На экране появится окно настройки расписания, подобное следующему.



2. Укажите время начала процедуры проверки.
3. Укажите дни недели, когда требуется выполнить проверку, установив соответствующие флажки.
4. Нажмите кнопку "Сохранить".

   На экране появится соответствующее информационное сообщение.

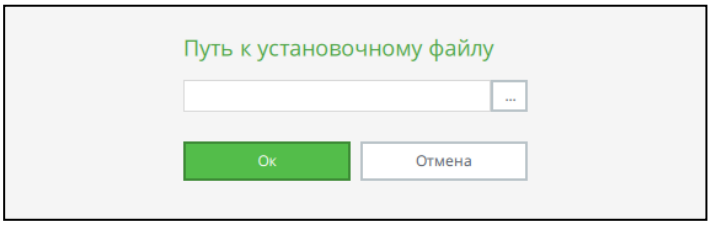
5. В окне сообщения нажмите кнопку "ОК".

   Проверка целостности файлов, поставленных на контроль, будет выполняться в указанные дни и время.

Для проверки целостности дистрибутива "Континент-АП":

1. На панели инструментов основного окна УКЦ нажмите кнопку "Выполнить КЦ эталонного ПО".

   На экране появится окно, подобное следующему.



2. Укажите путь до каталога, в котором находятся установочный пакет АП и файл, содержащий его КС.
3. Нажмите кнопку "ОК".

   Будет выполнена проверка целостности указанного дистрибутива, по завершении которой на экране появится соответствующее сообщение.

Приложение

Список поддерживаемых ОС семейства Linux

ОС	Версия
HP ThinPro	7.1 x86_64
Astra Linux	Common Edition 1.9 "Орел" x86_64
	Common Edition 1.11 "Орел" x86_64
	Common Edition 2.12 "Орел" x86_64
	Special Edition 1.5 "Смоленск" x86_64
	Special Edition 1.6 "Смоленск" x86_64
	Special Edition 1.7 "Смоленск" x86_64
	Special Edition 4.2.1 "Новороссийск" ARM
CentOS	6.5 i386/x86_64
	7.3.1611 x86_64
	7.6.1810 x64
Debian	7.6 wheezy i386/x86_64
	9.6 i386/x86_64
GosLinux	6.4 i686/x86_64
Oracle Linux	7.2 x86_64
	7.3 x86_64
RHEL	6.5 Desktop i386/x86_64
	6.5 Server i386/x86_64
	6.8 Desktop i386/x86_64
	6.8 Server i386/x86_64
	7 Desktop x86_64
	7 Server x86_64
	7.6 Desktop x86_64
	7.6 Server x86_64
ROSA	Enterprise Desktop X3 i586/x86_64
SUSE	Linux Enterprise 15 x86_64
Ubuntu	14.04 LTS Desktop i386/x86_64
	14.04 LTS Server i386/x86_64
	18.04 LTS Desktop x86_64
	18.04 LTS Server x86_64
Альт Линукс	СПТ 7.0 i586/x86_64
Альт	8 СП i586/x86_64
РЕД ОС	7.1 МУРОМ x64
	7.2 x86_64

Astra Linux SE 1.6. Особенности установки и настройки "Континент-АП"

Корректные установка и работа "Континент-АП" на компьютер, где используется ОС Астра 1.6 SE с настроенными доступными пользователю ненулевыми мандатными метками, требуют некоторых дополнительных операций.

Для корректной установки и дальнейшей работы:

1. Зайдите пользователем с нулевым уровнем конфиденциальности и высоким уровнем целостности.
2. Установите "Континент-АП". Не перезагружайте компьютер.
3. Под root запустите скрипт:

   ```
   /usr/share/cts/install/adapt_to_parsec
   ```

4. Выдайте пользователю с ненулевым уровнем конфиденциальности разрешение **PARSEC_CAP_PRIV_SOCK**.

   Внимание!
   - Рекомендуем делать это через графический конфигуратор, вызвав из главного меню "Панель управления → Безопасность → Политика безопасности → Пользователи → <Имя пользователя> → Вкладка "Привилегии" и установив в колонке Parsec галочку в поле parsec_cap_priv_sock. Если этого не сделать, вход пользователя с ненулевым уровнем конфиденциальности после выполнения вышеупомянутого скрипта будет невозможен.
   - "Континент-АП" также работать не будет.

5. Перезагрузите компьютер.
6. Войдите в систему, используя учетные данные пользователя и те настройки безопасности, которые планируются для данного пользователя при работе с абонентским пунктом, и добавьте необходимые профили в АП.

   Примечание. Это ограничение обусловлено особенностями реализации мандатного доступа в ОС: домашний каталог для одного и того же пользователя с разными настройками безопасности располагается в разных местах на жестком диске.

7. Если для создания профиля на СД требуется создание запроса на машине пользователя, создайте его, войдя с нужными настройками безопасности (мандатными метками).

Права пользователей и администраторов

Ниже приведены функции абонентского пункта, доступные пользователям в зависимости от их роли. Пользователи с правами администратора имеют возможность изменять все настройки абонентского пункта. Обычные пользователи имеют ряд ограничений, указанных в таблице ниже:

Функция АП	КС1	КС2	КС3	Примечание
Профили: добавление	+	+	-	
Профили: импорт	+	+	+	При импорте профиля доступен импорт всех сертификатов. Вручную можно импортировать только сертификат пользователя
Профили: редактирование	+	+	-	
Профили: удаление	+	+	-	
Запрос на сертификат	+	+	+	

Функция АП	КС1	КС2	КС3	Примечание
Сертификаты пользовательские: импорт	+	+	+	
Сертификаты пользовательские: удаление	+	+	-	
Сертификаты серверные: импорт	+	+	-	Для КС3 запрещено добавление серверного сертификата при подключении. Необходим корневой сертификат
Сертификаты серверные: удаление	+	+	-	
Сертификаты корневые: импорт	+	+	-	
Сертификаты корневые: удаление	+	+	-	
CDP: добавление	+	+	-	
CDP: редактирование	+	+	-	
CDP: удаление	+	+	-	
CRL: импорт	+	+	-	
Настройки сертификатов	-	-	-	
Настройки CRL	-	-	-	Для КС2, КС3 запрещено отключение проверки по CRL
Режим запуска	+	+	-	
Внешний прокси	+	+	-	

Управление абонентским пунктом из командной строки

В данном разделе приведено описание специализированной утилиты **cts**, расположенной в каталоге /usr/share/cts/bin, используемой для управления абонентским пунктом. В этом каталоге содержатся все исполняемые файлы"Континент-АП".

Утилита используется при выполнении следующих функций:

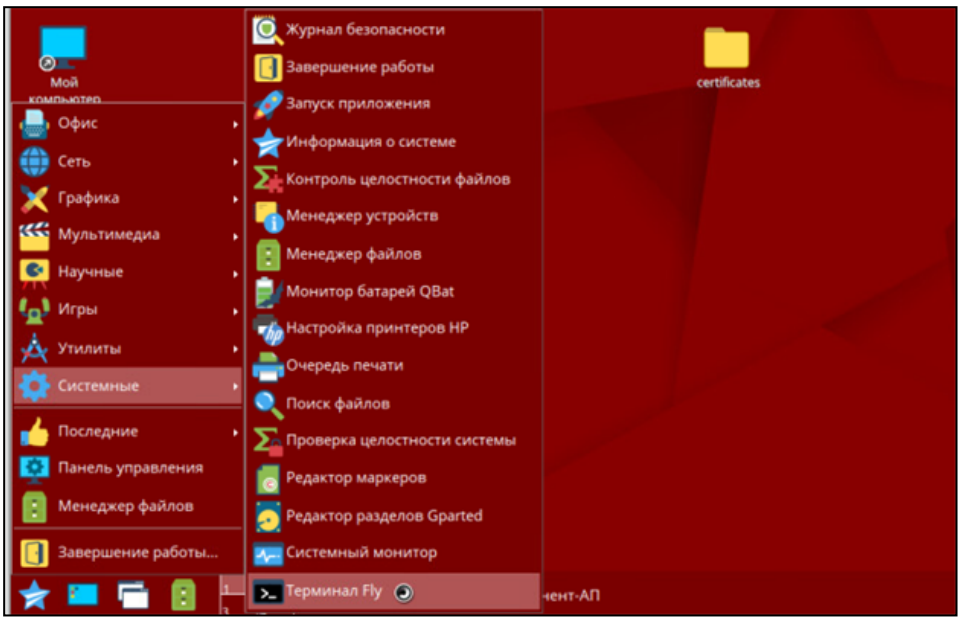
- подключение к СД;
- создание запросов на сертификат с сохранением закрытого ключа на различные ключевые носители;
- работа с корневым сертификатом;
- импорт профиля;
- управление профилем пользователя;
- работа с сертификатами пользователя;
- работа с серверными сертификатами;
- работа с CRL и CDP;
- просмотр информации о профилях, сертификатах и СД;
- просмотр журнала;
- просмотр сведений о программе.

Также в консольном режиме используются следующие утилиты:

- autoctsic — для повторного создания списка файлов, подлежащих КЦ;
- cts — для управления "Континент-АП";
- ctsic — для контроля и расчета КЦ;
- ctsreg — для регистрации.

Для вызова командной строки (на примере ОС Astra Linux Special Edition 1.6 "Смоленск" x64):

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



На экране появится окно консоли.

Формат вызова утилиты:

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

Для каждой команды имеется свой уникальный набор параметров. В квадратных скобках указываются опциональные параметры. Список команд и их описание приведены в таблице ниже:

Команда	Описание
help/--help/-help/-h	Вызов инструкции по использованию утилиты
version/--version/-version/-v	Просмотр версии АП
connect	Подключение к СД
disconnect	Отключение от СД
request	Создание запроса на сертификат
import key	Импорт закрытого ключа
import profile	Импорт профиля из файла конфигурации
events	Просмотр журнала событий
show profile	Просмотр параметров профиля
show certificate/cert	Просмотр данных сертификата

Команда	Описание
show config/parameter	Просмотр конфигурации пользователя
show stats	Просмотр статистики подключений
show settings	Просмотр всех текущих настроек
show settings general	Просмотр текущих основных настроек
show settings proxy	Просмотр текущих настроек прокси
show settings gui	Просмотр текущих настроек графического интерфейса приложения
show cdp	Просмотр списка CDP
add profile	Создание профиля пользователя
add connection	Добавление подключения к СД в существующий профиль пользователя
add cert	Добавление сертификатов
add cdp	Добавление адреса CDP
edit/modify profile	Редактирование профиля пользователя
edit/modify connection	Редактирование параметров подключения к СД для профиля
edit/modify cdp	Редактирование адреса CDP
edit/modify settings proxy	Редактирование настроек прокси
edit/modify settings general	Редактирование основных настроек
edit/modify settings gui	Редактирование настроек графического интерфейса приложения
delete/del profile	Удаление профиля пользователя
delete/del connection	Удаление подключения к СД для профиля
delete/del cdp	Удаление адреса CDP
delete/del cert	Удаление сертификата
delete/del pass	Удаление пароля (паролей)
update keypass	Обновление пароля ключевого контейнера
update crl	Обновление списка отозванных сертификатов

Команда help/--help/-help/-h

Команда осуществляет вывод инструкции по использованию утилиты, а также перечень всех команд.

Пример использования

```
cts help
```

Команда version/--version/-version/-v

Команда осуществляет вывод информации об установленной версии абонентского пункта.

Пример использования

```
cts version
```

Команда connect

Команда осуществляет подключение к СД. Содержит следующие параметры:

Параметр	Описание
Опциональные	
auto/-auto	Подключение к СД с использованием профиля по умолчанию
-profile <NAME>	Имя профиля подключения
-password/-pass	Пароль профиля
-pin	ПИН-код контейнера
-store-password	Сохранить пароль после успешного подключения
-store-pin	Сохранять ПИН-код после успешного подключения

Пример использования

Подключение к серверу доступа под профилем TR07 и указанным паролем:

```
cts connect -profile TR07 -pass 5$rt2t
```

Команда disconnect

Команда осуществляет отключение от СД. Содержит следующий параметр:

Параметр	Описание
Опциональный	
-profile <NAME>	Имя профиля

Пример использования

Разрыв активного соединения с СД:

```
cts disconnect
```

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 нем закрытого ключа.

Команда import key

Команда осуществляет импорт закрытого ключа. В ходе выполнения команды будет выполнен диалоговый скрипт для выбора ключевого носителя с закрытым ключом, хранилища для импортируемого ключа и набора энтропии. Содержит следующий параметр:

Параметр	Описание
Обязательный	
-ras-version/-ras <number {3, 4 (default)}>	Версия СД

Команда import profile

Команда осуществляет импорт конфигурационного файла профиля. В ходе выполнения команды будет выполнен диалоговый скрипт. Содержит следующие параметры:

Параметр	Описание
Обязательный	
-file-path/-path	Путь к файлу
Опциональные	
-file-pass	Пароль доступа к файлу
-key-pass	Пароль ключевого контейнера
-ras-version/-ras {3, 4}	Версия СД

Пример использования

Импорт конфигурации профиля 4 версии с паролем P@ssw0rd и паролем закрытого ключа:

```
cts import profile -file-path /home/user/profile1.ts4
-file-pass P@ssw0rd -key-pass 123456 -ras-version 4
```

Команда events

Команда предназначена для просмотра журнала событий. Содержит следующие параметры:

Параметр	Описание
Опциональные	
-category/-cat {INFO, ERROR, DEBUG}	Категория события
-start-time/-from <dd.mm.yyyy:hh:mm:ss>	Время начала
-end-time/-to <dd.mm.yyyy:hh:mm:ss>	Время окончания
-user <NAME>	Имя пользователя

Пример использования

Просмотр списка зафиксированных в журнале сообщений об ошибках, произошедших в период с 4 июля 2016 года по текущий момент для всех профилей подключений пользователя AdministratorGTC:

```
cts events -cat ERROR -from 04.07.2016:00:00:00
-user AdministratorGTC
```

Команда show profile

Команда предназначена для просмотра списка профилей. Содержит следующие параметры:

Параметр	Описание
Опциональные	
-name <REG_EXP>	Имя профиля
-server <REG_EXP>	IP-адрес сервера
-user <NAME>	Имя пользователя

Пример использования

Просмотр списка профилей пользователя Admin:

```
cts show profile -user Admin
```

Команда show certificate/cert

Команда предназначена для просмотра информации о сертификатах. Содержит следующие параметры:

Параметр	Описание
Опциональные	
-type {user, ca, as, crl}	Тип сертификата
-subject-cn <regular_expression>	Имя владельца сертификата
-subject-org <regular_expression>	Организация владельца сертификата
-issuer-cn <regular_expression>	Имя издателя сертификата
-issuer-org <regular_expression>	Организация издателя сертификата
-user <NAME>	Имя пользователя
-hide-expired	Скрывать просроченные сертификаты

Пример использования

Просмотр корневых сертификатов от издателя SecurityCode, исключая истекшие:

```
cts show cert -issuer-o SecurityCode -hide-expired
```

Команда show config/parameter

Команда предназначена для просмотра информации о конфигурации пользователя. Содержит следующий параметр:

Параметр	Описание
Опциональный	
-user <NAME>	Имя пользователя

Команда show stats

Команда предназначена для просмотра информации об активном подключении. Содержит следующий параметр:

Параметр	Описание
Опциональный	
-user <NAME>	Имя пользователя

Пример использования

Просмотр информации о подключениях к СД SP30:

```
cts show stats -server SP30
```

Команда show settings

Команда предназначена для вывода всех текущих настроек приложения.

Команда show settings general

Команда предназначена для вывода текущих основных настроек приложения.

Пример использования

Вывод текущих основных настроек приложения:

```
cts show settings general
```

Команда show settings proxy

Команда предназначена для вывода текущих настроек прокси.

Команда show settings gui

Команда предназначена для вывода текущих графических настроек приложения.

Команда show cdp

Команда предназначена для вывода списка CDP.

Команда add profile

Команда предназначена для создания профиля подключения. Содержит следующие параметры:

Параметр	Описание
Обязательный	
-name <NAME>	Имя профиля
Опциональные	
-server <HOST>	Адрес сервера
-port <number {0..65535}>	Порт сервера доступа
-proto/-protocol {udp, tcp}	Протокол соединения (для версий 3.X)
-cert-path	Путь к сертификату
-login	Логин пользователя
-auth {login, cert}	Тип аутентификации
-user <NAME>	Имя пользователя
-ras-version/-ras {3, 4}	Версия СД
-select-cert	Выбрать сертификат
-select-key	Выберите ключевой контейнер

Пример использования

Создание профиля подключения для пользователя User2 к серверу 192.168.10.10 под профилем TR07 по указанному сертификату. Тип аутентификации выбран по сертификату, используется протокол версий 3.X:

```
cts add profile -name TR07 -server 192.168.10.10
-cert-path /home/user/user.cer -user User2 -auth-type cert
-ras-version 3
```

Внимание!

- Один из параметров — логин пользователя или путь до сертификата является обязательным.
- Если при подключении имя пользователя должно вводиться в формате domain\user, необходимо использовать следующий синтаксис: domain\\user.

Команда add connection

Команда предназначена для добавления подключения в существующий профиль. Содержит следующие параметры:

Параметр	Описание
Обязательные	
-profile <NAME>	Имя профиля
-server <HOST>	Адрес сервера

Параметр	Описание
Опциональные	
-name <NAME>	Имя соединения
-user <NAME>	Имя пользователя
-port <number {0..65535}>	Порт СД
-number <number {1..}>	Порядковый номер соединения

Пример использования

Добавление в существующий профиль TR06 подключения к СД по адресу 192.168.0.20 по TCP-порту 443:

```
cts add connection -profile TR06 -name conn_2
-server 192.168.0.20 -conn-type tcp -tcp-port 443
```

Команда add cert

Команда предназначена для добавления сертификатов. Содержит следующие параметры:

Параметр	Описание
Обязательные	
-type {user, ca, as, crl}	Тип сертификата
-path	Путь к сертификату
Опциональный	
-user	Имя пользователя

Пример использования

Добавление корневого сертификата из каталога /home/user/root.cer:

```
cts add cert -cert-type ca -cert-path /home/user/root.cer
```

Команда add cdp

Команда предназначена для ручного добавления адреса CDP. Содержит следующий параметр:

Параметр	Описание
Обязательный	
<url>	Ссылка на CDP

Пример использования

Добавление CDP для скачивания CRL:

```
cts add cdp http://172.17.7.27/certnroll/new.crl
```

Команда edit/modify profile

Команда предназначена для редактирования профиля пользователя. Содержит следующие параметры:

Параметр	Описание
Обязательный	
-name <NAME>	Имя профиля
Опциональные	
-server <HOST>	Адрес сервера
-port <number {0..65535}>	Порт сервера доступа

Параметр	Описание
-proto/-protocol {udp, tcp}	Протокол соединения (для версий 3.X)
-cert-path	Путь к сертификату
-login	Логин пользователя
-auth {login, cert}	Тип аутентификации
-user <NAME>	Имя пользователя
-ras-version/-ras {3, 4}	Версия СД
-select-cert	Выбрать сертификат
-select-key	Выбрать ключевой контейнер

Пример использования

Редактирование профиля TR07, изменение типа аутентификации на "логин–пароль", задание логина пользователя на СД и пароля:

```
cts modify profile -name TR07 -user -auth-type login
-user-login tr07 -user-password 123456
```

Команда edit/modify connection

Команда предназначена для редактирования существующего подключения в профиле. Содержит следующие параметры:

Параметр	Описание
Обязательные	
-profile <NAME>	Имя профиля
-name <NAME>	Имя соединения
Опциональные	
-user <NAME>	Имя пользователя
-server <HOST>	Адрес сервера
-port <number {0..65535}>	Порт СД
-number <number {1..}>	Порядковый номер соединения

Пример использования

Редактирование существующего подключения conn_2 в профиле TR06, изменение типа на UDP и порта на 4433:

```
cts modify connection -profile TR06 -name conn_2
-server 192.168.0.20 -conn-type UDP -tcp-port 4433
```

Команда edit/modify cdp

Команда предназначена для редактирования адреса CDP, введенного вручную. Содержит следующие параметры:

Параметр	Описание
Обязательные	
-number/-N <number {1..}>...	Номер CDP
-url	Ссылка на CDP

Команда edit/modify settings proxy

Команда предназначена для настройки прокси-соединения. Содержит следующие параметры:

Параметр	Описание
Опциональные	
-use <boolean {on, off, yes, no}>	Использовать/не использовать прокси
-server <HOST>	Адрес прокси-сервера
-port <number {0..65535}>	Порт прокси-сервера
-auth {no (default), basic, ntlm}	Тип аутентификации прокси-сервера
-domain	Домен пользователя
-login	Логин пользователя
-password	Пароль пользователя

Пример использования

Настройка прокси- сервера с адресом 192.168.0.25 и портом 3128 с типом аутентификации basic. Логин — user, пароль — 12345678:

```
cts modify settings proxy -use on -server 192.168.0.25
-port 3128 -auth basic -login user -password 12345678
```

Команда edit/modify settings general

Команда предназначена для изменения основных настроек приложения. Содержит следующие параметры:

Параметр	Описание
Опциональные	
-keys-warning-days <дн. {14..365}>	Количество дней до появления уведомления об истечении срока действия закрытого ключа
-cert-warning-days <дн. {1..30}>	Количество дней до появления уведомления об истечении срока действия сертификата
-cert-allow-adding <boolean {yes, no}>	Запрашивать добавление других серверных и корневых сертификатов
-cert-check-on-crl <boolean {yes, no}>	Проверять сертификаты по CRL
-crl-extra-days <дн. {0..30}>	Количество дней, позволяющих системе работать после истечения срока действия CRL
-crl-auto-update <boolean {yes, no}>	Скачивать CRL автоматически
-crl-update-period <часы {1..48}>	Период скачивания CRL

Пример использования

Отключение проверки сертификатов по CRL:

```
cts edit settings -cert-check-on-crl no
```

Команда edit/modify settings gui

Команда предназначена для изменения графических настроек приложения. Содержит следующие параметры:

Параметр	Описание
Опциональные	
-auto-connect <boolean {true, off, false, yes, on, no, y, n}>	Автоматическое подключение с профилем по умолчанию при запуске графического приложения
-auto-disconnect <boolean {true, off, false, yes, on, no, y, n}>	Автоматически разрывать соединение при выключении графического приложения
-color-theme {light, dark}	Тема оформления графического приложения
-minimize-on-start <boolean {true, off, false, yes, on, no, y, n}>	При запуске графического приложения свернуть в системный трей

Команда delete/del profile

Команда предназначена для удаления профиля пользователя. Содержит следующие параметры:

Параметр	Описание
Обязательный	
-name <NAME>	Имя профиля
Опциональный	
-user <NAME>	Имя пользователя

Пример использования

Удаление профиля TR07:

```
cts del profile -name TR07
```

Команда delete/del connection

Команда предназначена для удаления существующего подключения в профиле. Содержит следующие параметры:

Параметр	Описание
Обязательный	
-profile <NAME>	Имя профиля
-name <NAME>	Имя соединения
Опциональный	
-user <NAME>	Имя пользователя

Пример использования

Удаление существующего подключения conn_2 в профиле TR06:

```
cts del connection -profile TR06 -name conn_2
```

Команда delete/del cdp

Команда предназначена для удаления адреса CDP, введенного вручную. Содержит следующие параметры:

Параметр	Описание
Опциональные	
-number, -N <number {1..}>	Номер CDP
-url	Ссылка на CDP

Команда delete/del cert

Команда предназначена для удаления сертификатов. Содержит следующие параметры (требуется использовать как минимум один опциональный параметр):

Параметр	Описание
Обязательный	
-type {user, ca, as, crl}	Тип сертификата
Опциональные	
-user	Имя пользователя
-subject-cn <regular_expression>	Имя владельца сертификата
-subject-org <regular_expression>	Организация владельца сертификата
-issuer-cn <regular_expression>	Имя издателя сертификата
-issuer-org <regular_expression>	Организация издателя сертификата

Пример использования

Удаление корневого сертификата с именем владельца RootSC:

```
cts del cert -cert-type ca -subject-cn RootSC
```

Команда delete/del pass

Команда предназначена для удаления сохраненных паролей профилей у пользователя. Содержит следующие параметры:

Параметр	Описание
Опциональные	
-profile <NAME>	Имя профиля
-all	Удаление паролей всех профилей пользователя

Команда update keypass

Команда предназначена для смены пароля ключевого контейнера пользовательского сертификата. Содержит следующие параметры:

Параметр	Описание
Обязательные	
-profile <NAME>	Имя профиля
-password	Пароль ключевого контейнера

Пример использования

Смена пароля ключевого контейнера пользовательского сертификата в профиле TR05:

```
cts update keypass -profile TR05 -key-pass 123456
```

Команда update crl

Команда для ручного запуска обновления CRL.

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/share/cts/bin/ctsic**.

Для просмотра списка:

- Вызовите командную строку (см. стр. **43**) и введите команду:

```
ctsic check --print
```

Повторное создание списка файлов, подлежащих контролю

Список файлов, подлежащих контролю целостности, содержится в файле **/etc/cts/filelist.current**. 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/share/cts/bin**.

Внимание! Запустить утилиту может только пользователь с правами администратора.

Для создания списка:

- Вызовите командную строку (см. стр. **43**) и введите команду:

```
autoctsic
```

Перерасчет контрольных сумм

Для перерасчета контрольных сумм:

1. Повторно создайте список файлов, подлежащих контролю целостности (см. выше).
2. Рассчитайте новые контрольные суммы для файлов, содержащихся в повторно созданном списке. Для этого выполните команду:

```
ctsic compute
```

Внимание! При совместной работе абонентского пункта среднего или высокого уровня безопасности с ПАК "Соболь" после выполнения приведенных выше операций необходимо повторно настроить механизм контроля целостности в ПАК "Соболь".

Для проверки целостности дистрибутива "Континент-АП":

- Вызовите командную строку (см. стр. **43**) и введите команду:

```
ctsic check-dist -d <path>
```

<path> — путь до каталога, в котором находятся установочный пакет АП и файл, содержащий его КС.

Для настройки расписания КЦ:

Внимание!
- Настройка расписания КЦ требует наличия прав суперпользователя.
- В данном примере рассматривается настройка расписания проверки целостности ежедневно в 15:00 по системному времени.

- Вызовите командную строку (см. стр. **43**) и введите команду:

```
ctsic schedule -t 15:00 -d 1,2,3,4,5,6,7
```

Сбор диагностической информации

Для сбора диагностической информации:

- Вызовите командную строку (см. стр. **43**) и введите команду:
  - для сбора данных, при котором архив сохраняется в каталог по умолчанию:

    ```
    ctsdiagnostics
    ```

  - для сбора данных, при котором архив сохраняется в каталог по указанному пути:

    ```
    ctsdiagnostics -a
    ```

    -a — путь до каталога, в который требуется сохранить архив с данными;
  - для сбора данных, включая дампы памяти, при котором архив сохраняется в каталог по умолчанию:

    Внимание! Требуется наличие прав суперпользователя.

    ```
    ctsdiagnostics -d
    ```

Утилита регистрации "Континент-АП"

Для работы с утилитой регистрации "Континент-АП":

1. Вызовите командную строку (см. стр. **43**) и введите команду:

   ```
   ctsreg -help
   ```

   Перечень доступных команд и инструкция по работе с утилитой появятся на экране.
2. Выполните требуемые действия, используя соответствующие команды.

Для выполнения онлайн-регистрации:

1. Вызовите командную строку (см. стр. **43**) и введите команду:

   ```
   ctsreg -o
   ```

   В консоли поочередно будут запрошены данные, требуемые для регистрации.
2. Введите запрашиваемые данные.

   При успешном завершении регистрации в консоли появится соответствующее сообщение.

Для выполнения офлайн-регистрации:

1. Вызовите командную строку (см. стр. **43**) и введите команду:

   ```
   ctsreg -r --path <path>
   ```

   <path> — путь до директории с именем создаваемого файла.

   В консоли поочередно будут запрошены данные, требуемые для регистрации.
2. Введите запрашиваемые данные.

   Файл с расширением ".tlsreg" будет создан по указанному пути.
3. Передайте созданный файл на сервер регистрации для получения файла регистрации.
4. После получения файла регистрации в командной строке введите команду:

   ```
   ctsreg -i --path <path>
   ```

   <path> — путь до директории с файлом регистрации.

   При успешном завершении регистрации в консоли появится соответствующее сообщение.