КОД безопасности

Континент ZTN Клиент для Linux

Руководство по эксплуатации

АМБС.26.20.40.140.003 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

ЗПС	Закрытая (замкнутая) программная среда
КЦ	Контроль целостности
МК	Менеджер конфигурации
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПУ	Программа управления
СД	Сервер доступа
СЗИ	Средство или система защиты информации
УКЦ	Утилита "Контроль целостности – Континент ZTN Клиент"
УЦ	Удостоверяющий центр
CDP	CRL Distribution Point
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DNS	Domain Name System
IP	Internet Protocol
NTLM	NT LAN Manager
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network

Введение

Руководство предназначено для пользователей и администраторов изделия "Континент ZTN Клиент для Linux" АМБС.26.20.40.140.003 (далее — Континент ZTN Клиент, Клиент, изделие). В нем содержатся сведения, необходимые для установки, настройки и эксплуатации изделия 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 "Код Безопасности" 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

Континент ZTN Клиент — программное средство, функционирующее в среде ОС семейства Linux и реализующее следующие основные функции:

- установление защищенного соединения с сервером доступа изделия "Аппаратно-программный комплекс шифрования "Континент" версии 3.9 и узлом безопасности с включенным компонентом "Сервер доступа" изделия "Комплекс безопасности "Континент". Версия 4" (далее — комплекс "Континент");
- установление защищенного соединения с изделием "Средство криптографической защиты информации "Континент TLS-сервер". Версия 2" (далее — TLS-сервер), а также обмен данными с веб-серверами корпоративной сети;
- регистрация событий, связанных с функционированием Клиента;
- контроль целостности ПО Клиента и среды функционирования, передаваемой и хранимой информации.

Изделие имеет технические характеристики, приведенные ниже.

Алгоритм шифрования
В соответствии с ГОСТ 28147-89 и ГОСТ Р 34.12-2015
Защита передаваемых данных от искажения
В соответствии с ГОСТ Р 34.12-2015 в режиме выработки имитовставки
Расчет хэш-функции
В соответствии с ГОСТ Р 34.11-2012
Формирование и проверка электронной подписи
В соответствии с ГОСТ Р 34.10-2012
Двусторонняя аутентификация
С использованием сертификатов X.509v3

Континент ZTN Клиент реализуется в следующих исполнениях:

- исполнение 1 — соответствует требованиям ФСБ России к криптографическим средствам класса КС1;
- исполнение 2 — 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 3 — 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.

Континент ZTN Клиент устанавливается на компьютеры, удовлетворяющие аппаратным и программным требованиям, приведенным ниже.

Элемент	**Требование**
Операционная система	См. стр. **40**
Процессор, оперативная память	В соответствии с установленной ОС
Жесткий диск (свободное место)	300 Мбайт
Привод	Привод DVD/CD-ROM
Дополнительное ПО	• АПМДЗ (для исполнений 2, 3); • ОС/СЗИ с функцией обеспечения ЗПС (для исполнения 3)

Принципы функционирования

Режим VPN

Континент ZTN Клиент в режиме VPN осуществляет установление защищенного соединения с СД комплекса "Континент" через общедоступные (незащищенные) сети.

Для подключения к СД осуществляется настройка параметров подключения. В зависимости от требований, предъявляемых к доступу удаленных пользователей к защищаемым ресурсам, на Клиенте может использоваться произвольное количество подключений, каждое из которых имеет индивидуальную настройку параметров и сохраняется в виде профиля подключения. Если в состав защищаемой сети входят несколько СД, соединение с каждым из них в рамках одного профиля подключения возможно при наличии сформированного списка доступных СД в настройках этого профиля.

Континент ZTN Клиент поддерживает соединение по протоколу версий 4.X. Для соединения используется протокол TCP, а аутентификация производится с помощью сертификата пользователя или логина и пароля.

При подключении к СД выполняется процедура установления соединения в соответствии с протоколом TLS, в ходе которой осуществляется взаимная аутентификация Клиента и СД. Процедура установления соединения завершается генерацией сеансового ключа, который используется для шифрования трафика.

Генерация закрытого ключа и формирование на его основе открытого при создании запроса на получение сертификата удостоверяющего центра выполняются средствами встроенной криптобиблиотеки.

Режим TLS

Континент ZTN Клиент в режиме TLS предназначен для реализации защищенного доступа удаленных пользователей к веб-ресурсам корпоративной сети по каналам связи общих сетей передачи данных с использованием шифрования по ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и ГОСТ Р 34.12-2015.

Для подключения к защищаемым веб-ресурсам корпоративной сети удаленный пользователь должен ввести имя веб-ресурса в адресной строке веб-браузера. По указанному имени Клиент посылает TLS-серверу запрос на создание защищенного соединения. На основании принятого запроса TLS-сервер запускает процедуру аутентификации "клиент–сервер", используя сертификаты открытых ключей. После успешного завершения процедуры аутентификации выполняется генерация сеансового ключа, и между Клиентом и TLS-сервером устанавливается защищенное соединение по протоколу TLS. TLS-сервер направляет запрос Клиенту по указанному пользователем адресу веб-ресурса в защищаемую сеть. Полученный от веб-сервера ответ на запрос TLS-сервер возвращает в рамках защищенного соединения.

В случае невыполнения требований, предъявляемых к аутентификации Клиента и TLS-сервера, защищенное соединение не устанавливается и доступ пользователя к веб-ресурсу блокируется.

Ролевая аутентификация

В соответствии с требованиями безопасности пользователи Клиента разделяются по ролям на администраторов и пользователей с ограниченными правами. Роль пользователя определяется по результатам аутентификации при входе в систему.

Администратор
Пользователь компьютера, зарегистрированный с правами суперпользователя. Администратору доступны все функции, связанные с установкой, настройкой и работой Клиента. По умолчанию Континент ZTN Клиент запускается в обычном режиме. Для входа в режим администратора необходимо выбрать в главном меню приложений ОС пункт "Континент ZTN Клиент (режим администратора)" и ввести пароль, подтверждающий права суперпользователя
Пользователь
Любой зарегистрированный на компьютере пользователь без прав суперпользователя. Пользователь имеет ограниченный доступ к функциям, связанным с установкой, настройкой и работой Клиента

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.

Поддерживается работа с ключами форматов стандарта PKCS#15 и сертификатами форматов кодирования DER, PEM, Base64.

Для работы Клиента требуются сертификаты, приведенные ниже.

Сертификат сервера доступа
Для подтверждения подлинности СД, взаимодействующего с Клиентом
Сертификат TLS-сервера
Для подтверждения подлинности TLS-сервера, взаимодействующего с Клиентом
Сертификат удаленного пользователя
Для аутентификации пользователя на СД/TLS-сервере
Корневой сертификат
Для подтверждения подлинности сертификатов СД, TLS-сервера 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 Клиента (см. стр. **28**). Одновременно с запросом формируется закрытый ключ пользователя. Запрос в виде файла сохраняется в указанную пользователем директорию, ключевой контейнер с закрытым ключом сохраняется на ключевом носителе.

Внимание! Максимальный срок действия закрытого ключа — 15 месяцев от даты формирования закрытого ключа. По истечении этого срока работа с сертификатом будет невозможна. Необходимо осуществить перевыпуск сертификата пользователя с закрытым ключом.

Клиент автоматически отслеживает состояние сертификатов, осуществляя следующие проверки:

- по сроку действия сертификата;
- по CRL;
- путем построения цепочки сертификатов.

Назначение ключевых носителей

Персональный ключевой носитель, выдаваемый пользователю администратором, предназначен для хранения и передачи пользователю ключевой информации — контейнера с закрытым ключом и пароля к нему.

В качестве ключевых носителей могут использоваться USB-флеш-накопители и аппаратные носители, приведнные ниже.

USB-ключи и/или смарт-карты	
• JaCarta PKI; • JaCarta PKI/Flash; • JaCarta PKI/BIO; • JaCarta ГОСТ; • JaCarta PKI/ГОСТ; • JaCarta PKI/BIO/ГОСТ; • JaCarta ГОСТ/Flash; • Рутокен ЭЦП 2.0; • JaCarta-2 PKI/ГОСТ; • JaCarta-2 PKI/BIO/ГОСТ; • JaCarta SF/ГОСТ	• JaCarta PRO; • JaCarta-2 PRO/ГОСТ; • JaCarta LT; • Рутокен ЭЦП PKI; • Рутокен ЭЦП 2.0 Flash; • Рутокен ЭЦП 2.0; • Рутокен ЭЦП 3.0 NFC; • Рутокен Lite; • Рутокен 2151; • ESMART Token; • ESMART Token ГОСТ

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

Контроль целостности

Функция контроля целостности предназначена для слежения за неизменностью содержимого файлов установленного ПО Клиента и связанных с ним файлов ОС Linux. КЦ осуществляется с помощью утилиты "Контроль целостности – Континент ZTN Клиент", входящей в дистрибутив Клиента.

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

Список файлов ПО, подлежащих контролю, и значения их контрольных сумм хранятся в конфигурационном файле. Конфигурационный файл формируется при установке установочного пакета.

КЦ установленного ПО осуществляется в следующих случаях:

- при запуске Клиента;
- до установления соединения с СД и защищенными веб-ресурсами;
- вручную, с помощью УКЦ;
- по расписанию, настраиваемому 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 будет обнаружено нарушение целостности либо отсутствие контролируемого ПО, а Континент ZTN Клиент будет активным, рабочие сессии с защищенными ресурсами будут продолжаться. Установление соединения с СД и создание новых сессий будет заблокировано.

При обнаружении нарушения целостности при неактивном ПО Клиента будет сделана соответствующая запись в журнале событий.

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

- при запуске Клиента;
- при попытке установления соединения с СД и защищенными веб-ресурсами (если нарушение целостности обнаружено в ходе регламентного контроля целостности при наличии активного соединения).

Если Континент ZTN Клиент используется совместно с ПАК "Соболь", проверка контрольных сумм дополнительно выполняется при загрузке операционной системы. Результаты проверки заносятся в журнал событий.

Аудит

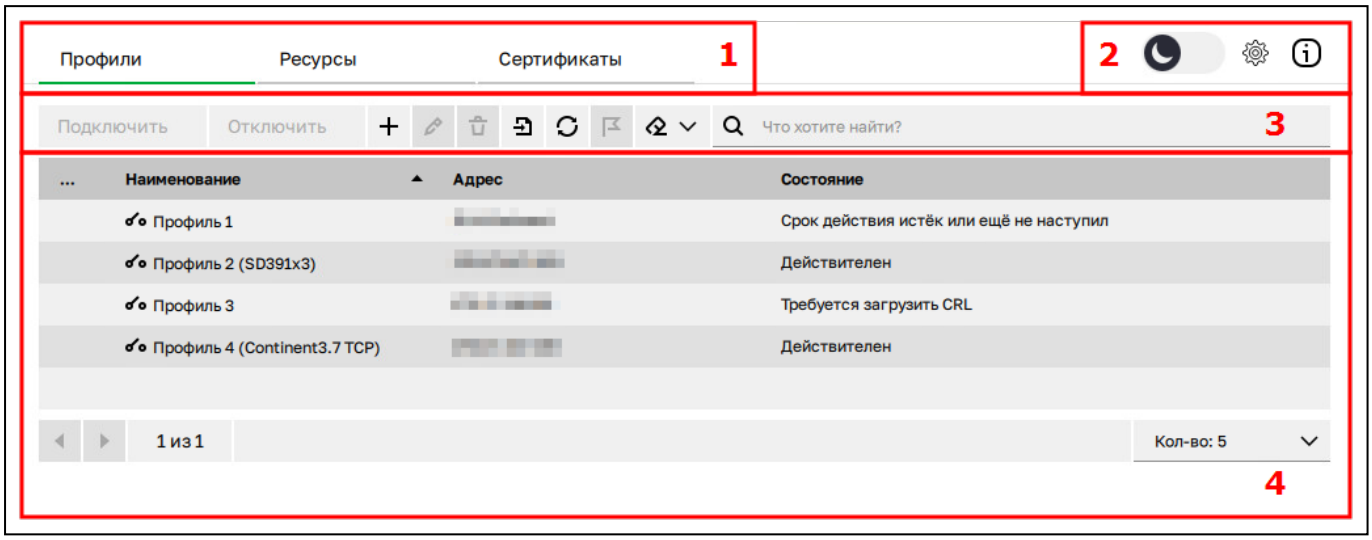
Все события от узлов сети, служб Клиента и любые другие системные события, которые фиксируются и хранятся в журнале, должны удовлетворять минимальным требованиям к хранению в нем.

Информация о событиях может быть просмотрена пользователем.

В случае необходимости с помощью утилиты "Сбор диагностической информации – Континент ZTN Клиент", входящей в дистрибутив Клиента, может быть создан архив с диагностической информацией о работе ПО (см. стр. **37**).

Пользовательский интерфейс основного окна

Для управления Клиентом реализовано специализированное ПО с графическим пользовательским интерфейсом, устанавливаемое на компьютер пользователя.



Основное окно Континент ZTN Клиент содержит элементы, приведенные ниже.

Обозначение	Описание
1	Вкладки для навигации по разделам основного окна
2	Кнопки переключения внешнего вида, "Настройки" и "О программе"
3	Панель инструментов и строка поиска
4	Область отображения информации

Глава 2
Установка, регистрация и удаление

Установка

Установка ПО Клиента может осуществляться только пользователем с правами суперпользователя.

Для установки программного обеспечения:

Внимание! Установка пакетов осуществляется командами в зависимости от установленной ОС.

1. Перейдите в директорию, содержащую установочные пакеты Клиента, и далее — в директорию с названием, соответствующим разрядности ОС, установленной на компьютере.
2. Установите пакет, соответствующий требуемому классу.

   Примечание.
   - При необходимости изменить класс защиты Клиента требуется удалить установленное ПО Клиента (см. стр. 15) и выполнить установку повторно, используя пакет, соответствующий требуемому классу.
   - Класс, которому соответствует установочный пакет, указан в его названии. Например, пакет "cts-4.3.0-201.ks1.el.x86_64.rpm" соответствует классу КС1.

   Для ОС, использующих менеджер пакетов rpm, выполните следующую команду:

   ```
   yum install <ИМЯ_ПАКЕТА>
   ```

   Для ОС, использующих менеджер пакетов deb, и ОС Альт Линукс выполните следующую команду:

   ```
   apt-get install <ИМЯ_ПАКЕТА>
   ```

   После установки пакета в консоли появится сообщение о необходимости прочитать текст лицензионного соглашения и будет указан путь к файлу текста соглашения.
3. Прочтите текст соглашения.

   Внимание! Если вы не согласны с лицензионным соглашением, удалите установленный пакет (см. стр. 15).
4. Перезагрузите компьютер.

   После перезагрузки компьютера на экране в области уведомлений появится значок Клиента.

Вид значка Клиента указывает на состояние соединения.

Значок	Пояснение
	Отключено (соединение не установлено)
	Имеется внутреннее предупреждение. Возможные причины: • выключена проверка по CRL; • незарегистрированная копия ПО
	Соединение установлено, отображение качества связи отключено (подробнее см. на стр. 34)
	Соединение установлено, хорошее/среднее/плохое качество связи
	Соединение установлено, хорошее/среднее/плохое качество связи. Имеется внутреннее предупреждение

В главном меню (например, в группе "Сеть") ОС Linux появятся значки приложений, входящих в состав Континент ZTN Клиент.

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

Станут доступны приложения, приведенные ниже.

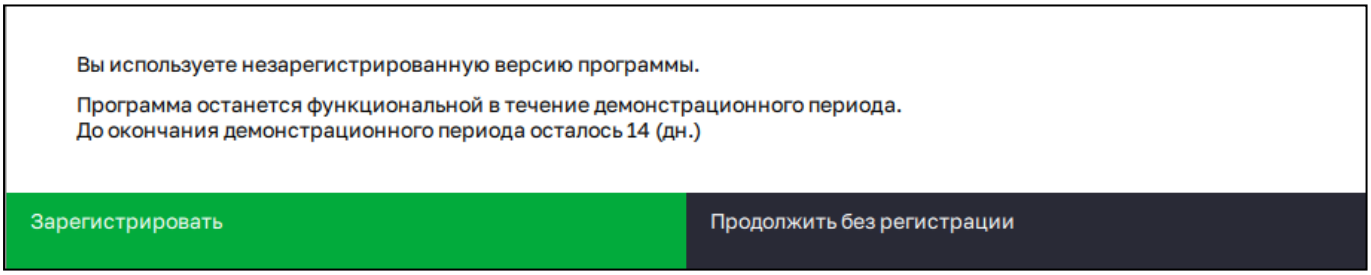
Континент ZTN Клиент
Запуск ПО Континент ZTN Клиент
Континент ZTN Клиент (режим администратора)
Запуск ПО Континент ZTN Клиент в режиме администратора
Регистрация – Континент ZTN Клиент
Регистрация ПО Континент ZTN Клиент на сервере регистрации компании "Код Безопасности"
Сбор диагностической информации – Континент ZTN Клиент
Экспорт отчета о состоянии работоспособности ПО Континент ZTN Клиент
Контроль целостности – Континент ZTN Клиент
• Контроль целостности дистрибутива и установленного на компьютере ПО • Пересчет контрольных сумм (в исполнениях, соответствующих классам КС1, КС2)
Контроль целостности (режим администратора) – Континент ZTN Клиент
• Контроль целостности дистрибутива и установленного на компьютере ПО • Пересчет контрольных сумм (в исполнении, соответсвующем классу КС3)

Регистрация

Сразу после установки Клиента начинается демонстрационный период, который составляет 14 дней. Количество дней, оставшихся до окончания демонстрационного периода, отображается в окне "О программе".

Примечание. Функции Клиента в демонстрационном периоде не ограничиваются.

Если в течение демонстрационного периода регистрация не будет выполнена, при каждом запуске Клиента на экране будет появляться окно с сообщением о необходимости регистрации ПО.

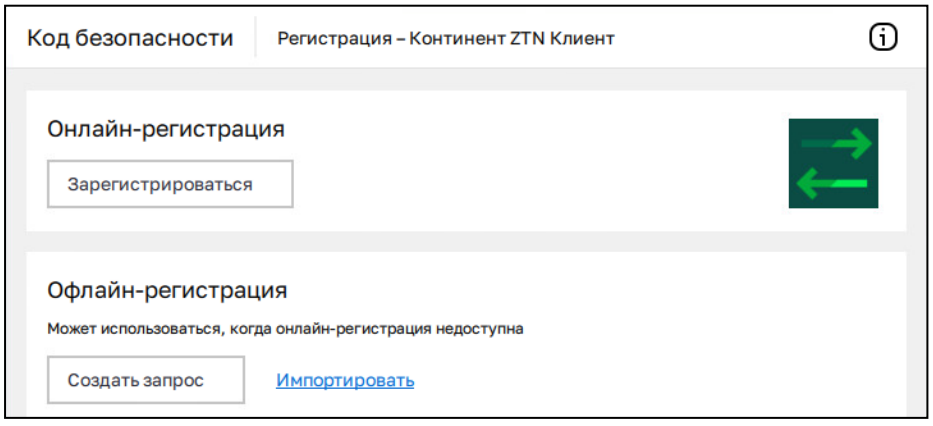


В случае отказа от регистрации по истечении демонстрационного периода работа Клиента будет невозможна до момента успешной регистрации.

Для онлайн-регистрации:

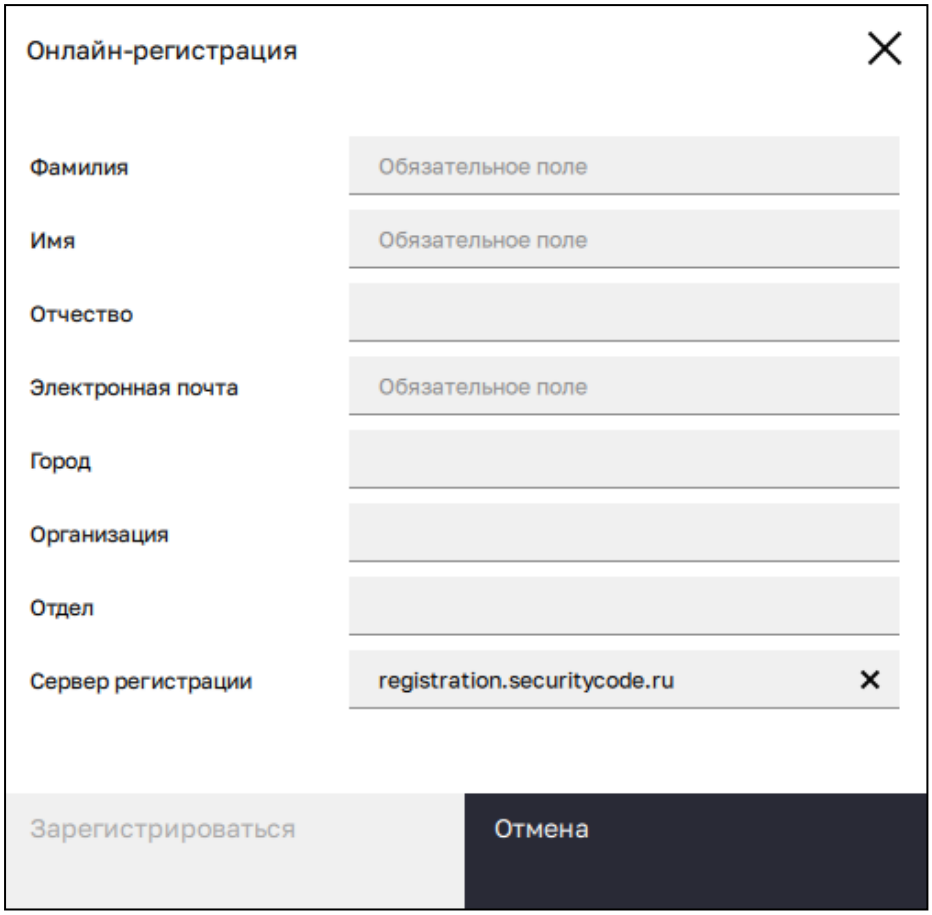
1. В окне сообщения о необходимости регистрации нажмите кнопку "Зарегистрировать" или в главном меню приложений ОС выберите пункт "Регистрация – Континент ZTN Клиент".

   На экране появится окно регистрации Клиента.



2. В области "Онлайн-регистрация" нажмите кнопку "Зарегистрироваться".

   На экране появится окно с формой регистрации.



3. Укажите требуемые значения и нажмите кнопку "Зарегистрироваться".

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

Для офлайн-регистрации:

1. В окне регистрации Клиента (см. стр. **13**) в области "Офлайн-регистрация" нажмите кнопку "Создать запрос".

   На экране появится окно с формой регистрации аналогично онлайн-регистрации (см. стр. **14**).

   Примечание. Данные, введенные ранее в форме для онлайн-регистрации, сохраняются и будут автоматически указаны в форме для офлайн-регистрации.

2. Укажите требуемые значения и нажмите кнопку "Сохранить".

   На экране появится стандартное окно сохранения файла.

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

4. После получения файла с серийным номером откройте окно регистрации Клиента и в области "Офлайн-регистрация" нажмите кнопку "Импортировать".

   На экране появится стандартное окно выбора файла.

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

   По завершении процесса регистрации на экране появится соответствующее сообщение.

После регистрации ПО Клиента в разделе "О программе" основного окна появится регистрационный номер программы.

Удаление

Внимание! Для удаления ПО Клиента необходимо обладать правами суперпользователя.

Предусмотрены следующие варианты удаления ПО Клиента:

- с помощью графического пакетного менеджера (если графический пакетный менеджер входит в состав операционной системы);
- с помощью командной строки:
  - для ОС, использующих менеджер пакетов rpm, выполните следующую команду:

    ```
    yum remove ztn
    ```

  - для ОС, использующих менеджер пакетов deb, и ОС Альт Линукс выполните следующую команду:

    ```
    apt-get purge ztn
    ```

Глава 3
Настройка и эксплуатация

Запуск

Континент ZTN Клиент по умолчанию автоматически запускается после входа в систему. Запуск ПО Клиента вручную осуществляется в главном меню приложений ОС или с помощью значка на рабочем столе.

В результате запуска основное окно Клиента (см. стр. **11**) по умолчанию сворачивается в системный трей, а на панели задач отображается значок программы (см. стр. **12**).

Вызов контекстного меню значка программы на панели задач позволяет осуществлять следующие действия:

- подключение с профилем по умолчанию;
- разрыв текущего соединения или установление соединения с использованием добавленных профилей;
- подключение к избранным ресурсам;
- сброс соединений;
- переход к меню настроек работы ПО;
- завершение работы ПО.

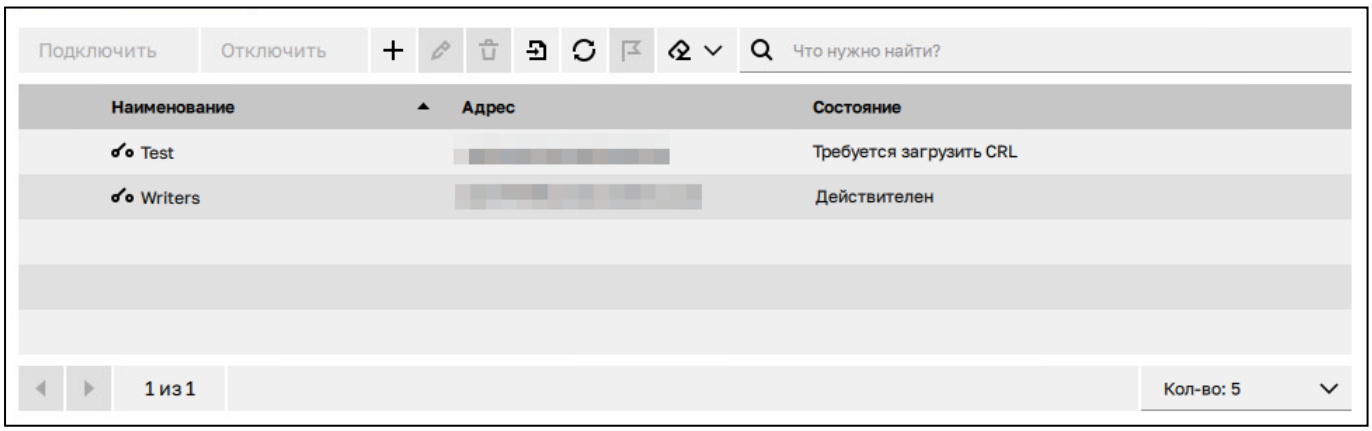
При двойном нажатии левой кнопкой мыши по значку программы на панели задач устанавливается или разрывается соединение с СД с использованием профиля по умолчанию.

Управление профилями подключения

Для подключения к серверам доступа комплекса "Континент" используются профили подключения, представляющие собой набор настраиваемых параметров. Добавление и настройка профилей подключения доступны как администраторам, так и пользователям (в исполнениях, соответствующих классам КС1, КС2).

Если к СД должны подключаться несколько зарегистрированных на компьютере пользователей, для каждого из них необходимо добавить отдельный профиль подключения. В списке профилей отображаются только профили пользователя, от имени которого осуществлен вход в систему.

Управление профилями подключения осуществляется в разделе "Профили" основного окна Клиента. Раздел "Профили" содержит список профилей, строку поиска и панель инструментов.



Панель инструментов раздела "Профили" содержит элементы, приведенные ниже.

Кнопка	Описание
Подключить	Установить соединение с СД, используя профиль, выбранный в списке
Отключить	Разорвать соединение с СД
+	Добавить профиль

Кнопка	Описание
	Редактировать параметры профиля
	Удалить профиль
	Импортировать профиль из файла конфигурации
	Обновить список профилей
	Использовать профиль для подключения по умолчанию
	Удалить сохраненные пароли из профиля либо все пароли

Параметры профиля подключения

Параметры профиля подключения приведены в таблице ниже.

Использовать по умолчанию
Профиль, с помощью которого соединение с СД после запуска Клиента устанавливается автоматически (если параметр включен, см. стр. **34**) или при двойном нажатии на значок Клиента в области уведомлений панели задач
Наименование
Имя профиля, отображаемое в списке используемых профилей
Версия протокола
Номер версии протокола соединения с СД
Тип аутентификации
Тип аутентификации пользователя — по сертификату или паре "логин–пароль"
Тип протокола
Тип используемого транспортного протокола — TCP
Сертификат
Имя выбранного сертификата пользователя из списка ранее импортированных сертификатов. Доступно для настройки только при выборе типа аутентификации по сертификату (см. выше)
Ключевой контейнер
Имя ключевого контейнера. Для выбора ключевого контейнера предназначена кнопка "Установить" (). При нажатии открывается окно выбора ключевого контейнера. Любая операция с ключевым контейнером требует подтверждения паролем доступа к этому контейнеру. Доступно для настройки только при выборе типа аутентификации по сертификату (см. выше)
Логин/Пароль
Учетные данные пользователя. Доступно для настройки только при выборе типа аутентификации по паре "логин–пароль" (см. выше)
Количество попыток подключения
Количество попыток подключения к СД, по исчерпании которых начнется установление соединения со следующим СД в списке (при наличии дополнительных адресов СД). Подключение выполняется до тех пор, пока не будет установлено соединение или исчерпается количество попыток для каждого адреса СД в списке. Значение по умолчанию — 5
Адреса серверов доступа
Перечень доступных для подключения СД. Панель инструментов, предназначенная для настройки списка адресов СД, становится доступна после добавления первого адреса СД

Адрес
IP-адрес или имя СД. Доступно для настройки при добавлении адреса СД или редактировании его параметров
Порт
Порт СД для установления соединения. Доступно для настройки при добавлении адреса СД или редактировании его параметров

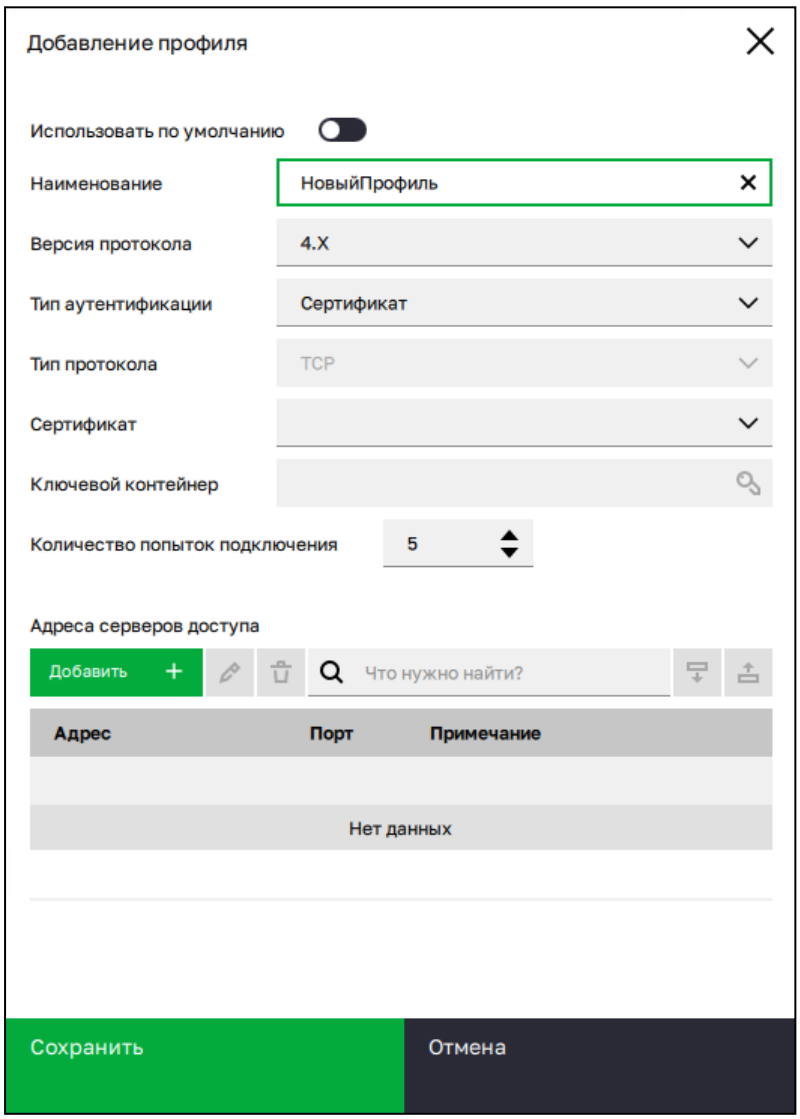
Создание, настройка и удаление профилей подключения

Перед созданием профиля необходимо подготовить файл сертификата пользователя, полученный от администратора СД, и внешний носитель с ключевым контейнером, если ключевой контейнер сохранен на нем, а не в системном хранилище локального компьютера. Файл сертификата можно сохранить на жестком диске или на внешнем носителе.

Для создания профиля подключения:

1. В основном окне Клиента в разделе "Профили" нажмите кнопку "Добавить" на панели инструментов (см. стр. **16**).

   В правой части основного окна появится список настроек профиля подключения.



Примечание. Если профиль для подключения планируется использовать по умолчанию, установите соответствующую отметку.

2. Укажите имя профиля в поле "Наименование".
3. Выберите в раскрывающемся списке версию протокола и в поле ниже укажите тип аутентификации.

4. В зависимости от указанного типа аутентификации выполните одно из следующих действий:
   - по сертификату — выберите из раскрывающегося списка сертификат пользователя. В поле "Ключевой контейнер" появится имя соответствующего ключевого контейнера;

     Примечание.
     - Если добавлен новый сертификат, поле "Ключевой контейнер" останется пустым. Для добавления ключевого контейнера нажмите кнопку "Установить", укажите в списке ключевой контейнер и нажмите кнопку "Выбрать".
     - Поле "Ключевой контейнер" заполнится автоматически только в том случае, если ранее на компьютере (даже для другого профиля) была сохранена пара "Сертификат" – "Ключевой контейнер".
   - по логину и паролю — введите в открывшиеся поля данные учетной записи пользователя.
5. Укажите количество попыток для подключения к СД.
6. Для настройки списка адресов СД выполните следующие действия:

   Внимание!
   - Соединение с СД устанавливается по первому адресу из списка в выбранном профиле. Если СД, указанный первым, будет недоступен, а количество попыток подключения — исчерпано, начнется установление соединения со следующим адресом СД.
   - Максимальное количество адресов СД для каждого профиля подключения — 10.

   - для добавления адреса СД нажмите кнопку "Добавить". В появившемся окне укажите адрес/имя СД и номер порта, если он должен отличаться от указанного автоматически. Нажмите кнопку "Добавить";

     Примечание.
     - В поле "Адрес" необходимо ввести значение, указанное в поле "CommonName" сертификата сервера.
     - При наличии дополнительных адресов СД в профиле они должны быть представлены DNS-именами. СД, имеющие одинаковые значения в полях "Адрес" и "Порт" или представленные IP-адресами, будут проигнорированы.
   - для настройки параметров адреса СД выберите адрес/имя и нажмите кнопку "Изменить". В появившемся окне внесите необходимые изменения и нажмите кнопку "Сохранить";
   - для удаления адреса СД выберите адрес/имя и нажмите кнопку "Удалить". Подтвердите выполнение операции;
   - для изменения порядка адресов СД выберите адрес/имя и используйте кнопки "Вверх" и "Вниз".
7. Нажмите кнопку "Сохранить".

   Профиль появится в списке. Для подключения к СД профиль должен иметь статус "Действителен".

Для редактирования настроек профиля подключения:

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

1. Выберите профиль и нажмите кнопку "Редактировать" на панели инструментов либо дважды нажмите левой кнопкой мыши по строке требуемого профиля.

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

   Изменения будут применены.

Для импорта профиля подключения:

1. Для импорта профиля нажмите кнопку "Импортировать" на панели инструментов.

   На экране появится стандартное окно открытия файла.
2. Выберите файл конфигурации и нажмите кнопку "Открыть".

   На экране появится окно ввода пароля доступа к файлу конфигурации.
3. Введите полученный от администратора пароль для файла конфигурации и нажмите "Продолжить".

   На экране появится окно ввода пароля доступа к ключевому контейнеру.
4. Введите полученный от администратора пароль к ключевому контейнеру и нажмите кнопку "ОК".

   Примечание. Максимальное количество попыток ввода пароля доступа к ключевому контейнеру — 5. После 5-й неудачной попытки выполнение операции будет прервано.

   На экране появится окно установления пароля.
5. Введите пароль в требуемых полях и нажмите кнопку "ОК".

   Примечание. Пароль должен содержать не менее 6 символов, прописные и строчные буквы латинского алфавита (A–Z, a–z), арабские цифры (0–9) и следующие символы: **? ! : ; ” ’ , . < > / { } [ ] ~ @ # $ % ^ & * - _ + = \ ` | № ( )**.

На экране появится окно выбора ключевого носителя для сохранения ключевого контейнера.

6. Выберите ключевой носитель и нажмите кнопку "Выбрать".

   На экране появится окно ввода имени профиля.

7. Укажите наименование профиля и нажмите кнопку "Продолжить".

   На экране появится сообщение о завершении импорта профиля.

8. Нажмите кнопку "Закрыть".

   Примечание. Если профиль импортирован без ключевого контейнера, на экране появится сообщение о необходимости выбора контейнера в настройках профиля. Для добавления ключевого контейнера в настройках профиля в соответствующем поле нажмите кнопку "Установить", укажите в списке контейнер и нажмите кнопку "Выбрать".

   На экране появится сообщение с предложением произвести пробное подключение с использованием импортированного профиля.

9. Для установления пробного подключения нажмите кнопку "Подключиться", для возврата в раздел "Профили" — кнопку "Пропустить".

   В случае установления подключения на экране появится информационное сообщение.

Для обновления списка профилей нажмите кнопку "Обновить" на панели инструментов.

Для выбора профиля по умолчанию укажите профиль и нажмите кнопку "Установить профиль по умолчанию" на панели инструментов (см. стр. **16**). Автоматическое подключение к СД будет осуществляться по выбранному профилю.

Для удаления профиля подключения:

Внимание! Удаление профиля, используемого для активного подключения, невозможно.

1. Выберите профиль и нажмите кнопку "Удалить" на панели инструментов.

   На экране появится окно запроса на подтверждение операции.

2. Нажмите кнопку "Удалить".

   Профиль будет удален из списка.

Для удаления сохраненных паролей:

1. Выберите профиль и нажмите кнопку "Удалить сохраненные пароли" на панели инструментов.
2. В появившемся раскрывающемся списке выберите один из следующих пунктов:
   - "Удалить пароль из профиля", если для выбранного профиля был сохранен пароль;
   - "Удалить все пароли" для всех профилей в списке.

   На экране появится запрос на подтверждение операции.
3. Нажмите кнопку "Удалить".

   Сохраненные пароли будут удалены.

Управление защищенными ресурсами

Управление защищенными ресурсами осуществляется в разделе "Ресурсы" основного окна Клиента. Раздел "Ресурсы" содержит список серверов и ресурсов, строку поиска и панель инструментов.

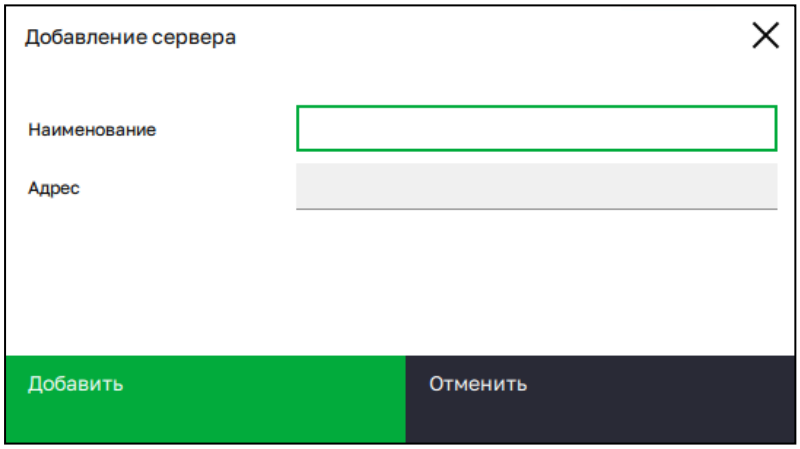
Панель инструментов раздела "Ресурсы" содержит элементы, приведенные ниже.

Кнопка	Описание
Добавить	Добавить сервер/ресурс
	Редактировать параметры сервера/ресурса
	Удалить сервер/ресурс
	Добавить ресурс в избранное
	Режим отображения серверов и ресурсов

Добавление, настройка и удаление защищенных ресурсов

Для добавления сервера:

1. В основном окне Клиента в разделе "Ресурсы" нажмите кнопку "Добавить" на панели инструментов (см. стр. **21**).
2. В появившемся раскрывающемся списке нажмите кнопку "Сервер".
   В правой части основного окна появится список настроек сервера.



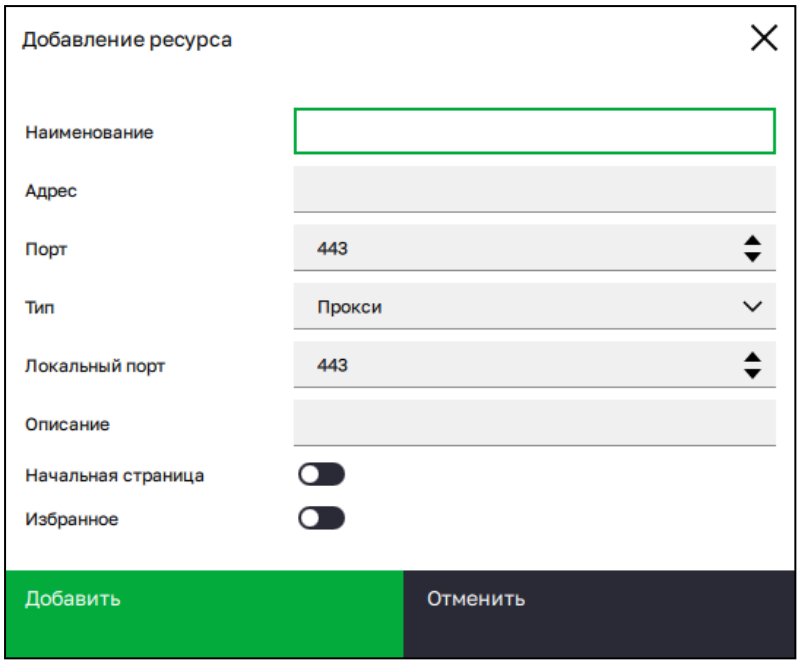
3. Введите название сервера для установления TLS-подключения в поле "Наименование".
4. Укажите сетевое имя или IP-адрес сервера в поле "Адрес".
5. Нажмите кнопку "Добавить".
   На экране появится сообщение о добавлении сервера.
6. Нажмите кнопку "Закрыть".
   Сервер появится в списке. На экране появится запрос на загрузку ресурсов.
7. Нажмите кнопку "Да".
   На экране появится окно выбора сертификата для доступа к серверу.
8. Выберите из списка требуемый сертификат.
   Ресурсы добавленного сервера будут загружены и появятся в списке.

Для добавления ресурса:

Примечание. Ресурс, загруженный ранее при добавлении сервера, добавить нельзя. В случае если сначала был добавлен ресурс, а затем — сервер с одноименным ресурсом, он будет перемещен в список ресурсов сервера.

1. В основном окне Клиента в разделе "Ресурсы" нажмите кнопку "Добавить" на панели инструментов.
2. В появившемся раскрывающемся списке нажмите кнопку "Ресурс".

В правой части основного окна появится список настроек ресурса.



3. Введите название ресурса для установления TLS-подключения в поле "Наименование".
4. Укажите сетевое имя или IP-адрес ресурса в поле "Адрес".
5. Выберите из раскрывающегося списка тип подключения и установите значения в полях "Порт" и "Локальный порт".
6. При необходимости заполните поле "Описание", а также установите отметки "Начальная страница" и "Избранное".

Примечание. Отметки "Начальная страница" и "Избранное" доступны в случае, если в поле "Тип" указано значение "Прокси".

7. Нажмите кнопку "Добавить".

   Ресурс появится в списке.

Для редактирования настроек сервера/ресурса:

Внимание! Редактирование настроек ресурса, сконфигурированного автоматически, невозможно.

1. Выберите сервер/ресурс и нажмите кнопку "Редактировать" на панели инструментов либо дважды нажмите левой кнопкой мыши по строке требуемого ресурса.

   В правой части основного окна появится список настроек сервера/ресурса.
2. Внесите изменения в доступные поля и нажмите кнопку "Сохранить".

   Изменения будут применены.

Для добавления ресурса в избранное выберите ресурс с типом "Прокси" и нажмите кнопку "Добавить в избранное" на панели инструментов. В строке с ресурсом появится значок ☆. Для отмены действия нажмите кнопку "Добавить в избранное" повторно либо удалите отметку в настройках ресурса.

Для изменения режима отображения перечня серверов/ресурсов нажмите кнопку "Список/дерево" на панели инструментов и выберите в раскрывающемся списке требуемый пункт. Перечень серверов/ресурсов примет необходимый вид.

Примечание. При переключении на режим отображения "Список" в списке будут отображены только ресурсы.

Для удаления сервера/ресурса:

Внимание! Удаление ресурса, сконфигурированного автоматически, невозможно.

1. Выберите сервер/ресурс и нажмите кнопку "Удалить" на панели инструментов.

   На экране появится окно запроса на подтверждение операции.
2. Нажмите кнопку "Удалить".

   Сервер/ресурс будет удален.

Настройка подключения

Перед установлением соединения с СД или защищенными ресурсами необходимо настроить параметры подключения.

Для настройки параметров подключения:

1. В основном окне Клиента нажмите кнопку "Настройки".

   На экране появится окно настройки общих параметров подключения (см. стр. **34**).
2. Настройте значения параметров на требуемых вкладках и нажмите кнопку "Сохранить".

Подключение к серверу доступа

Внимание!
- Подключение к СД возможно только в том случае, если вход в ОС выполнен одним пользователем. Если вход в ОС выполнен двумя и более пользователями, для подключения одного из них к СД необходимо, чтобы другие пользователи выполнили выход из системы.
- Подключение к СД возможно только с помощью профиля, имеющего статус "Действителен".
- Перед подключением к СД необходимо подключить к компьютеру ключевой носитель с закрытым ключом пользователя.

Континент ZTN Клиент позволяет подключиться к СД следующими способами:

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

При необходимости можно сохранить пароль для профиля подключения (в исполнениях, соответствующих классам КС1, КС2). Для этого требуется установить соответствующую отметку в окне подключения и 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.
- Если пароль не был сохранен, при установлении соединения с СД в зависимости от типа аутентификации, указанного в настройках профиля, на экране появится окно запроса пароля доступа к ключевому контейнеру или логина и пароля пользователя.
- Максимальное количество попыток ввода пароля доступа к ключевому контейнеру — 5. После 5-й неудачной попытки установление соединения с СД будет прервано.

После подключения к СД в строке с используемым профилем появится индикатор качества связи. При наведении курсора на индикатор качества связи на экране появится соответствующая всплывающая надпись.

Индикатор	Описание
	Хорошее качество связи
	Среднее качество связи
	Плохое качество связи

Автоматическое подключение с профилем по умолчанию

Для настройки подключения:

1. В основном окне Клиента нажмите кнопку "Настройки".

   На экране появится окно настройки общих параметров Клиента.
2. Установите отметку в поле "Автоматическое подключение к серверу доступа с профилем по умолчанию" (подробнее о настройках режима запуска см. на стр. **34**).
3. Если при создании или импорте профилей не был назначен профиль по умолчанию, выберите один из списка и установите в его настройках отметку "Использовать по умолчанию".

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

   Внимание! Если в настройках указано не разрывать соединение при выходе из программы, текущее подключение к СД останется активным в фоновом режиме.

В ОС без графического интерфейса пользователя для настройки автоматического подключения к СД при входе в систему необходимо средствами консольных команд утилиты cts настроить скрипт автоматического подключения к СД и 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 с профилем по умолчанию из панели задач ОС Linux:

Внимание! Если при создании или импорте профилей не был назначен профиль по умолчанию, предварительно выберите один профиль из списка и поставьте в его настройках отметку "Использовать по умолчанию" (подробнее о редактировании профиля см. на стр. 18).

1. Запустите Континент ZTN Клиент.
2. Наведите указатель на значок ПО в области панели задач и дважды нажмите левой кнопкой мыши.

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

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

1. Запустите Континент ZTN Клиент.
2. Наведите указатель на значок ПО в области панели задач и нажмите правую кнопку мыши.
3. В контекстном меню выберите пункт "Установить соединение", а затем — имя требуемого профиля.

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

Если соединение с СД установлено с помощью панели задач ОС Linux и произошел разрыв соединения, начнется переподключение к тому же СД. При исчерпании количества попыток подключения начнется установление соединения со следующим СД из списка в профиле.

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

1. Запустите Континент ZTN Клиент.
2. В основном окне Клиента выберите раздел "Профили".

   В области отображения информации появится список имеющихся профилей подключения.
3. Выберите профиль и нажмите кнопку "Подключить" на панели инструментов.

   Если для профиля указано несколько адресов СД, на экране появится окно выбора СД для подключения.
4. Выберите из раскрывающегося списка адрес СД и нажмите кнопку "Подключиться".

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

Если соединение с СД установлено из основного окна Клиента и произошел разрыв соединения, начнется переподключение к тому же СД. При исчерпании количества попыток подключения установление соединения с СД будет прервано.

Разрыв соединения с сервером доступа

Для разрыва соединения с СД из области уведомлений панели задач дважды нажмите левой кнопкой мыши по значку Клиента или вызовите контекстное меню и нажмите кнопку "Отключить "<имя_профиля>". Соединение с СД будет разорвано, а значок на панели задач станет серым.

Для разрыва соединения с СД из основного окна Клиента:

1. В основном окне Клиента перейдите в раздел "Профили".

   На экране появится список профилей подключения.
2. Выберите требуемый профиль и нажмите кнопку "Отключить" на панели инструментов.

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

Внимание!

- Если после установления соединения с СД выполнена блокировка пользователя ОС, соединение не разрывается.
- При смене пользователя в ОС во время активного подключения, у первого пользователя будет выполнен разрыв соединения.
- При одновременном входе двух и более пользователей в ОС соединение не сможет установить ни один из них.

Доступ к защищенным ресурсам

Для доступа к избранным ресурсам из панели задач ОС Linux:

Примечание. В список избранных ресурсов могут быть добавлены ресурсы только типа "Прокси".

1. Запустите Континент ZTN Клиент.
2. Наведите указатель на значок ПО в области панели задач и нажмите правую кнопку мыши.
3. В контекстном меню выберите пункт "Избранные ресурсы", а затем — имя требуемого ресурса.

   В веб-браузере откроется страница в соответствии с конфигурацией выбранного ресурса.

Для доступа к защищенному ресурсу с помощью веб-браузера:

Примечание.
- Для корректного подключения к защищенным веб-ресурсам по протоколу HTTPS необходимо импортировать в хранилище корневых сертификатов используемого веб-браузера сертификат "ContinentTLSClientRoot", который расположен в файле с именем "cert" в директории "etc/cts/cert/tlsca/0000". Перед импортом сертификата необходимо в название файла "cert" добавить расширение "cer".
- При повторной установке ПО Клиента необходимо заново импортировать сертификат "ContinentTLSClientRoot" в хранилище корневых сертификатов используемого веб-браузера.

1. Запустите веб-браузер и в адресной строке введите адрес ресурса.

   Внимание!
   - При установленном туннеле в веб-браузере необходимо указать протокол, который используется на защищенном веб-сервере.
   - В случае использования сетевого имени ресурса вместо его адреса необходимо осуществить соответствующую настройку DNS-сервера или файла "hosts". После внесения изменений в файл "hosts" требуется перезапустить Клиент.

   Если не установлен сертификат по умолчанию (см. стр. 34), на экране появится окно выбора сертификата пользователя из списка импортированных сертификатов.
2. Выберите сертификат пользователя и нажмите кнопку "OK".
3. Если на экране появится окно ввода пароля доступа к ключевому контейнеру, введите пароль и нажмите кнопку "OK".

   Примечание. Если требуется сохранить пароль доступа, установите отметку в соответствующем поле.

   Окно выбора сертификата закроется, и будет установлено защищенное соединение с указанным ресурсом.

   Если пользователь 5 раз подряд в течение 10 минут предъявил недействительный сертификат, доступ к серверу заблокируется на 10 минут (ограничение реализовано на стороне сервера, его параметры могут быть изменены).

   Примечание. Если на TLS-сервере включен режим работы без аутентификации пользователя, для доступа к защищенному ресурсу достаточно запустить веб-браузер и в адресной строке ввести адрес веб-ресурса.

Вход в режим администратора

Режим администратора предназначен для управления УКЦ и более тонкой настройки работы Клиента.

По умолчанию Континент ZTN Клиент запускается в обычном режиме. Для входа в режим администратора необходимо выбрать в списке главного меню приложений ОС программу "Континент ZTN Клиент" или ее утилиты, доступные в режиме администратора, и ввести пароль, подтверждающий права суперпользователя.

В режиме администратора доступны следующие операции:

- расширенные настройки работы Клиента:
  - 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.

Для запуска Клиента в режиме администратора:

1. Завершите работу приложения "Континент ZTN Клиент", если оно запущено.
2. Откройте главное меню приложений ОС (например, в разделе "Сеть") и выберите пункт "Континент ZTN Клиент (режим администратора)".

   На экране появится окно запроса пароля для подтверждения прав администратора.
3. Введите пароль и нажмите кнопку "Да".

   Континент ZTN Клиент будет запущен, на панели задач появится значок программы, и откроется основное окно интерфейса.
4. Для возврата в обычный режим перезапустите Континент ZTN Клиент, выбрав в главном меню приложений ОС пункт "Континент ZTN Клиент" без пометки "режим администратора".

Для запуска УКЦ в режиме администратора:

1. Откройте главное меню приложений ОС (например, в разделе "Сеть") и выберите пункт "Континент ZTN Клиент – Контроль целостности (режим администратора)".

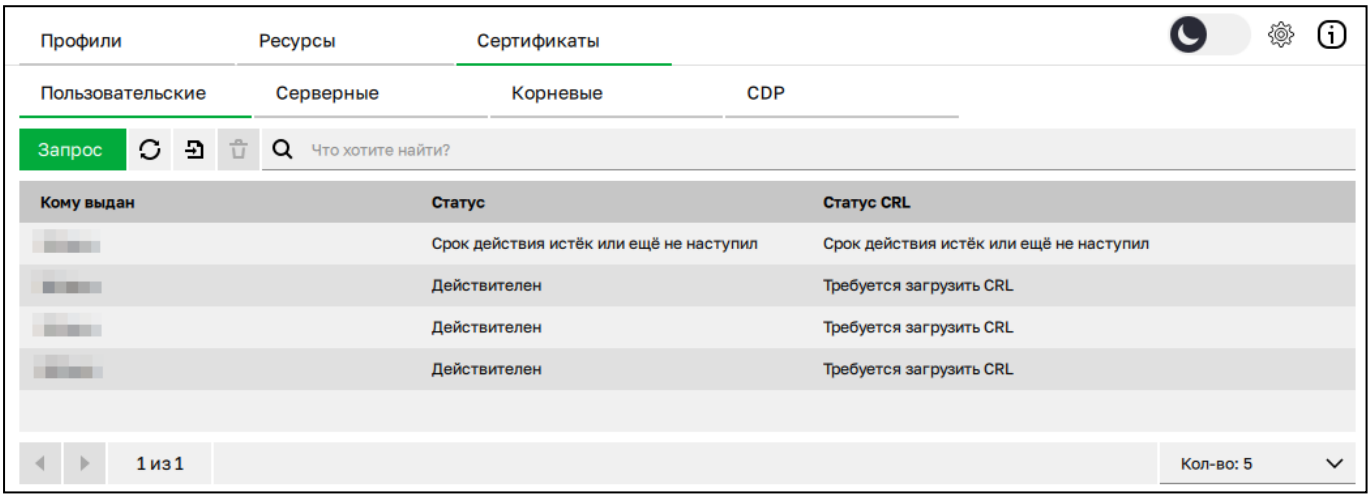
   На экране появится окно запроса пароля для подтверждения прав администратора.
2. Введите пароль и нажмите кнопку "Да".

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

Глава 4
Управление сертификатами

Континент ZTN Клиент позволяет добавлять сертификаты в хранилище, создавать запросы на получение сертификата пользователя и осуществлять запись закрытых ключей на съемный носитель или в Систему (хранилище на локальном компьютере пользователя).

Раздел "Сертификаты" содержит вкладки со списками пользовательских, серверных и корневых сертификатов, CDP, а также строку поиска и панель инструментов.



Панель инструментов раздела "Сертификаты", в зависимости от вкладки, содержит элементы, приведенные ниже.

Кнопка	Описание
Запрос	Создать запрос на сертификат
	Обновить список импортированных сертификатов/список CDP
	Импортировать сертификат/CRL
	Удалить сертификат/CDP, добавленный вручную
Добавить +	Добавить CDP вручную
	Редактировать параметры CDP, добавленного вручную
	Загрузить CRL из всех добавленных CDP

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

Примечание. Допускается использовать действительный уникальный сертификат пользователя, выпущенный УЦ ранее.

Для передачи сертификатов рекомендуется использовать отчуждаемый носитель.

Примечание. В качестве ключевых носителей могут использоваться USB-флеш-накопители, USB-ключи и смарт-карты, а также идентификаторы iButton (см. стр. **9**).

После получения всех сертификатов необходимо установить их в локальное хранилище компьютера средствами Клиента (см. стр. **31**).

Для отображения состояния сертификатов используются статусы, приведенные ниже.

Активен
Сертификат действителен и используется в профиле для подключения
Неактивен
Срок действия сертификата еще не наступил
Просрочен
Срок действия сертификата истек
Срок действия истекает через X дней
Переменная X обозначает количество дней до окончания срока действия сертификата. По умолчанию статус появляется за 14 дней до окончания срока действия сертификата
Не найден корневой сертификат
В пользовательском или серверном сертификате отсутствуют сведения о корневом сертификате
Ошибка проверки цепочки сертификатов
Не удалось построить цепочку от пользовательского сертификата до корневого
Нет CRL
Сертификат не прошел проверку по CRL, так как не импортирован необходимый CRL-файл
CRL просрочен
Срок действия CRL истек или еще не наступил
Отозван по CRL
Сертификат не прошел проверку по CRL

Создание запроса

Запрос на получение сертификата создается пользователем средствами Клиента по требованию администратора безопасности. Одновременно с запросом средствами криптопровайдера генерируется закрытый ключ пользователя.

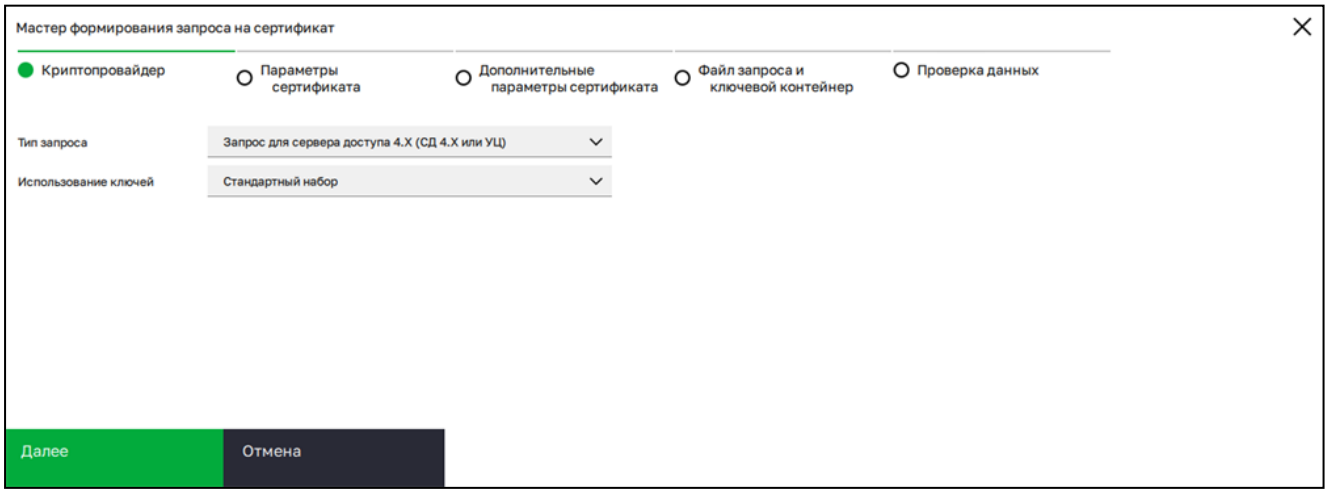
Запрос в виде файла сохраняется в указанную пользователем папку, ключевой контейнер с закрытым ключом сохраняется на ключевом носителе, указанном в настройках.

Примечание. Рекомендуется заранее подготовить отформатированный ключевой носитель для записи ключевого контейнера.

Для создания запроса на получение сертификата:

1. В основном окне Клиента в разделе "Сертификаты" перейдите на вкладку "Пользовательские сертификаты" и нажмите кнопку "Запрос" на панели инструментов (см. стр. **27**).

   На экране появится окно создания запроса на сертификат.



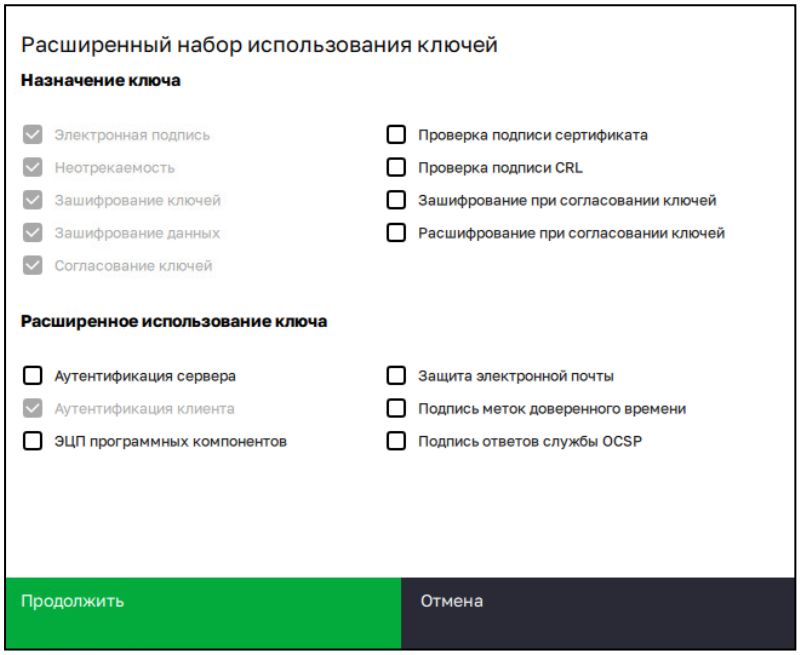
2. В раскрывающемся списке "Использование ключей" укажите набор использования ключей.

Стандартный набор
Минимально необходимые параметры для функционирования ключа шифрования
Расширенный набор
Выбор использования дополнительных параметров ключа шифрования, если это предусмотрено политикой информационной безопасности компании

3. Нажмите кнопку "Далее".

   Если указан стандартный набор параметров использования ключа, на экране появится окно для ввода имени ключевого контейнера и имени файла для запроса сертификата. Перейдите к п. **5**.

   Если указан расширенный набор параметров использования ключа, на экране появится окно выбора параметров ключа шифрования.



4. Укажите необходимые параметры ключа шифрования и нажмите кнопку "Продолжить".

   На экране появится диалог для ввода параметров запроса.

5. В раскрывающемся списке "Тип субъекта" укажите требуемое значение.

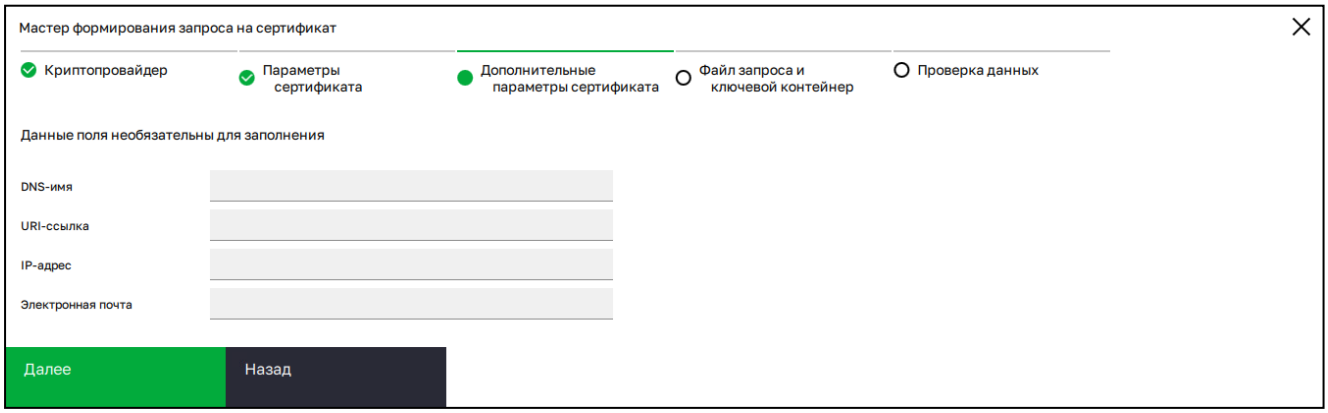
   Примечание. В зависимости от значения параметра "Тип субъекта" меняются параметры формы запроса.

6. Укажите сведения о субъекте в оставшихся полях.

   Внимание! Для продолжения настройки запроса необходимо указать значения для параметров с отметкой "Обязательной поле".

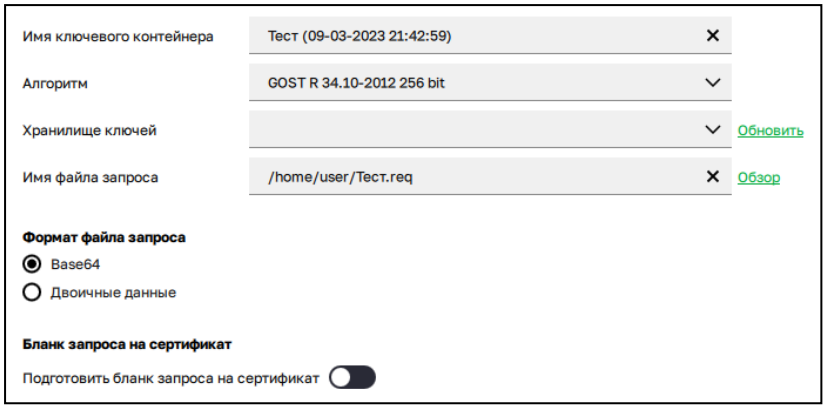
7. Нажмите кнопку "Далее".

   На экране появится окно для ввода дополнительной информации о владельце сертификата.



8. При необходимости заполните требуемые поля и нажмите кнопку "Далее".

   На экране появится окно настройки свойств файла запроса и ключевого носителя.



9. Укажите имя ключевого контейнера и имя файла запроса.

   Примечание.
   - По умолчанию запрос сохраняется в файле с расширением *.req и именем, содержащим имя пользователя, создающего запрос, а также текущие время и дату.
   - Для изменения расположения или имени файла запроса нажмите кнопку "Обзор". В открывшемся окне менеджера файлов ОС укажите диск (папку) для создания файла и имя файла запроса, а затем нажмите кнопку "Сохранить".

10. Выберите из раскрывающегося списка требуемый алгоритм.

11. Выберите из раскрывающегося списка "Хранилище ключей" тип ключевого носителя.

    Примечание. Для обновления списка доступных ключевых носителей нажмите кнопку "Обновить".

12. Выберите формат, в котором будет сохранен файл запроса.

13. Установите отметку в поле "Подготовить бланк запроса на сертификат", если необходимо сохранить версию запроса для печати.

    Примечание. Бланк запроса сохраняется в файле с расширением "html" с именем, аналогичным имени файла запроса.

14. Нажмите кнопку "Далее".

    На экране появится сообщение о завершении работы мастера запроса сертификата, и отобразятся параметры создаваемого запроса.

15. Нажмите кнопку "Создать".

    Начнется процедура создания закрытого ключа. 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.**17** .

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

    После завершения процедуры на экране появится окно ввода пароля доступа к ключевому контейнеру.

17. Введите и подтвердите пароль доступа к создаваемому ключевому контейнеру и нажмите кнопку "ОК".

    Примечание. Длина пароля должна быть не менее 6 символов.

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

    Внимание! Если используемый съемный носитель содержит файлы, имена которых совпадают с именами записываемых файлов:
    - файлы на USB-флеш-накопителе будут автоматически переименованы и сохранены;
    - файлы на Рутокен будут перезаписаны.

18. Нажмите кнопку "ОК" и извлеките носитель, если закрытый ключ был сохранен на нем.

    На экране появится сообщение о завершении создания запроса на сертификат.

19. Нажмите кнопку "Закрыть".

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

Импорт и удаление сертификатов

Для импорта сертификата пользователя:

Внимание! Возможен импорт сертификатов только с использованием алгоритма подписи ГОСТ Р 34.10-2012.

1. В основном окне Клиента в разделе "Сертификаты" перейдите на вкладку "Пользовательские".

   В области отображения информации появится список установленных сертификатов.
2. Нажмите кнопку "Импортировать" на панели инструментов.

   На экране появится окно импорта сертификата.
3. Нажмите кнопку "..." в строке поля "Сертификат".

   На экране появится стандартное окно открытия файла.
4. Выберите файл сертификата и нажмите кнопку "Открыть".

   Произойдет возврат в окно импорта сертификата.
5. Укажите в раскрывающемся списке "Расположение контейнера" место хранения ключевого контейнера.

   Внимание! При установленном значении "Файловая система" необходимо указать ключ в формате для ОС Windows.
6. В зависимости от указанного расположения контейнера выполните одно из следующих действий:
   - файловая система — нажмите кнопку "Установить" (). В появившемся окне для работы с файловой системой выберите файл ключевого контейнера и нажмите кнопку "Открыть";
   - хранилище — выберите из раскрывающегося списка "Хранилище" место хранения ключевого контейнера и укажите в раскрывающемся списке "Ключевой контейнер" требуемое наименование.
7. Нажмите кнопку "Импортировать".

   На экране появится окно ввода пароля доступа к ключевому контейнеру.
8. Введите пароль и нажмите кнопку "Продолжить".

   На экране появится экран набора энтропии.
9. Следуйте указаниям инструкции на экране и дождитесь завершения набора энтропии.

   Начнутся загрузка и установка сертификата. Если в папке, где хранится сертификат пользователя, будет обнаружен соответствующий корневой сертификат, откроется окно с предложением его импортировать.
10. Нажмите кнопку "Да".

    После успешного завершения операции на экране появится соответствующее сообщение.
11. Нажмите кнопку "Закрыть".

Для импорта серверного/корневого сертификата:

1. В основном окне Клиента в разделе "Сертификаты" перейдите на вкладку с требуемым видом сертификата и нажмите кнопку "Импортировать" на панели инструментов.

   На экране появится стандартное окно открытия файла.
2. Выберите файл сертификата и нажмите кнопку "Открыть".

   Сертификат появится в списке.

Для удаления сертификата пользователя:

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

1. В основном окне Клиента в разделе "Профили" выберите профиль, к которому привязан сертификат, и нажмите кнопку "Редактировать" на панели инструментов.

   На экране появится список настроек профиля.
2. Выберите другой возможный сертификат пользователя и нажмите кнопку "Сохранить".
3. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку "Пользовательские сертификаты".

   В области отображения информации появится список установленных сертификатов.
4. Выберите сертификат и нажмите кнопку "Удалить" на панели инструментов.
5. В окне подтверждения нажмите кнопку "Удалить".

   Сертификат будет удален из списка.

Для удаления корневого/серверного сертификата:

1. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку с требуемым видом сертификата.

   В области отображения информации появится список установленных сертификатов.
2. Выберите требуемый сертификат и нажмите кнопку "Удалить".
3. В окне подтверждения нажмите кнопку "Удалить".

   Сертификат будет удален из списка.

Просмотр сведений о сертификатах

Получить информацию об импортированных сертификатах можно с помощью средств Клиента.

Для просмотра сведений о сертификате:

1. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку с требуемым типом сертификатов.
2. Выберите сертификат в списке и дважды нажмите левой кнопкой мыши по строке с ним.

   На экране появится стандартное окно сведений о сертификате.
3. После просмотра информации о сертификате нажмите кнопку "Закрыть".

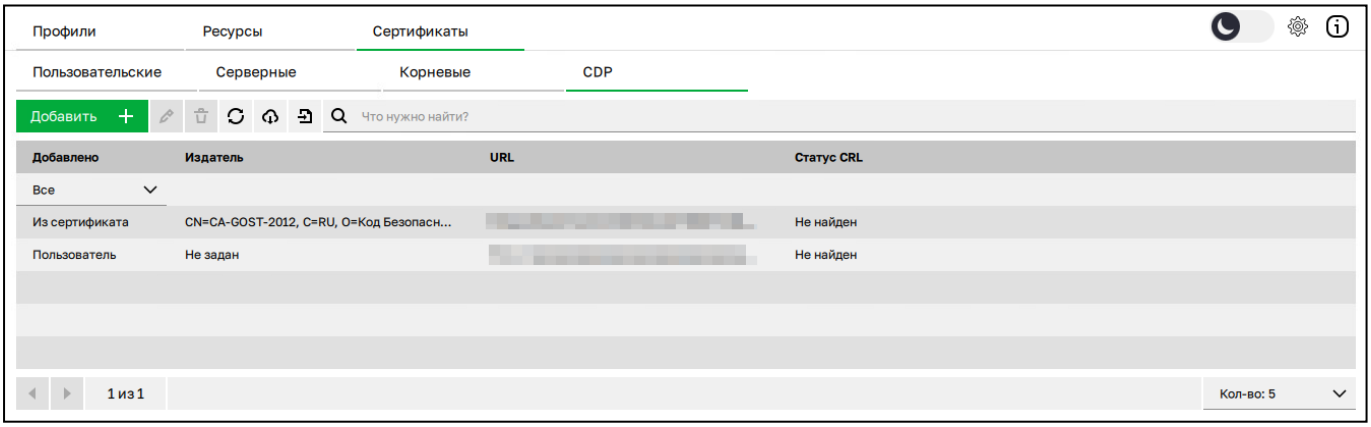
Управление CRL

Континент ZTN Клиент позволяет в автоматическом и ручном режимах получать CDP, а также скачивать CRL для проверки валидности используемых сертификатов.

Управление CRL осуществляется в разделе "Сертификаты" на вкладке "CDP" (см. стр. **27**).

Настройка CDP

Если используемые сертификаты содержат информацию о CDP, Континент ZTN Клиент получит ее при импорте сертификатов. Для автоматической загрузки CDP необходимо импортировать пользовательский, корневой или серверный сертификат (см. стр. **31**). При необходимости CDP можно добавить вручную.

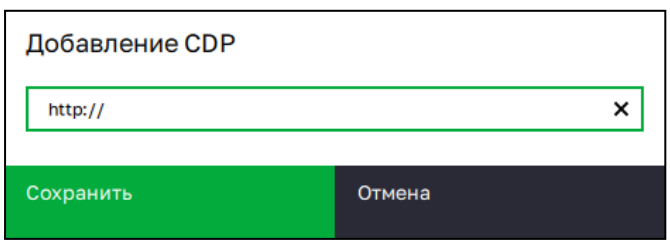


Для добавления CDP:

1. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку "CDP".

   В области отображения информации появится список используемых CDP.
2. Нажмите кнопку "Добавить" на панели инструментов (см. стр. **27**).

   На экране появится окно для ввода адреса CDP.



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

   CDP появится в списке.

Для редактирования и удаления CDP, а также обновления списка CDP необходимо использовать соответствующие кнопки на панели инструментов.

Примечание. Редактирование и удаление CDP, полученного из сертификата, невозможно.

Загрузка CRL

Автоматическая загрузка CRL происходит в результате добавления CDP после импорта сертификатов. CRL также может быть добавлен вручную с помощью кнопки "Загрузить".

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

Для обновления списка CRL выполните скачивание CRL вручную.

Для импорта файла CRL:

1. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку "CDP".

   В области отображения информации появится список имеющихся CDP.
2. Нажмите кнопку "Импортировать".

   На экране появится стандартное окно открытия файла.
3. Укажите требуемый CRL-файл и нажмите кнопку "Открыть".

   Начнется загрузка. После завершения операции на экране появится соответствующее сообщение.
4. Нажмите кнопку "Закрыть".

Для загрузки файлов CRL вручную:

1. В основном окне Клиента выберите раздел "Сертификаты" и перейдите на вкладку "CDP".

   В области отображения информации появится список CDP.

   Примечание. Если CDP не прописан в установленном сертификате или не добавлен пользователем ранее, необходимо добавить CDP вручную (см. стр. 32).
2. Нажмите кнопку "Загрузить" на панели инструментов.

   Начнется загрузка. После завершения операции на экране появится соответствующее сообщение.
3. Нажмите кнопку "Закрыть".

Глава 5
Управление работой ПО Клиента

Настройка параметров работы Клиента

Настройка параметров работы Клиента осуществляется в разделе "Настройки" основного окна (см. стр. **11**).

Общие настройки

Для настройки общих параметров Клиента:

1. В окне настроек перейдите на вкладку "Общие".
   В области отображения информации появится окно настройки общих параметров подключения.
2. Установите требуемые значения для параметров, приведенных ниже.

Параметр	Описание
Режим запуска	
При старте системы	При включенном параметре ПО Клиента запускается автоматически после загрузки ОС
Свернуть в системный трей при запуске	При включенном параметре Клиент запускается в свернутом виде, в области уведомлений панели задач появляется значок Клиента
Автоматическое подключение к серверу доступа с профилем по умолчанию	При включенном параметре осуществляется автоматическое подключение к СД с профилем по умолчанию. Если профиль по умолчанию не указан, в области уведомлений панели задач появится соответствующее сообщение
Режим завершения работы	
Разорвать все соединения	При включенном параметре активные соединения завершаются при завершении работы ПО Клиента. Если параметр выключен, при завершении работы ПО Клиента текущее соединение с СД останется активным в фоновом режиме, соединения с ресурсами прервутся
Подтверждение	
Подтверждать сброс соединений	При включенном параметре в случае разрыва соединения по инициативе пользователя на экране появится окно подтверждения
Отображение	
Отображать стабильность соединения	При включенном параметре после подключения к СД в строке с используемым профилем появится индикатор качества связи (подробнее см. на стр. **23**)

3. Нажмите кнопку "Сохранить".

Настройки сертификатов и CRL

Внимание! Для изменения настроек сертификатов и CRL необходимо запустить Континент ZTN Клиент в режиме администратора.

Для настройки параметров работы с сертификатами и CRL:

1. В окне настроек перейдите на вкладку "Сертификаты".
   На экране появится окно настройки параметров работы с сертификатами и CRL.
2. Установите требуемые значения для параметров, приведенных ниже.

Параметр	Описание
Пользовательские сертификаты	
Предупреждать об истечении срока действия	Начало периода оповещения пользователя об окончании срока действия сертификата. Принимает значения от 1 до 30 (в днях)

Параметр	Описание
Запрашивать добавление других серверных сертификатов	При включенном параметре во время первого подключения к СД для добавления сертификата в локальное хранилище запрашивается подтверждение пользователя. При отказе пользователя установление соединения будет прервано
Параметры CRL	
Проверять подлинность сертификатов	При включенном параметре во время установления соединения с СД и/или ресурсами осуществляется проверка подлинности сертификатов по CRL
Блокировать работу при истечении срока действия CRL	Период, в течение которого возможно осуществить подключение после истечения срока действия CRL. Принимает значения от 0 до 30 (в днях). Доступно для настройки только при включенном параметре "Проверять подлинность сертификатов"
Автоматическая загрузка CRL	При включенном параметре осуществляется автоматическое обновление CRL с периодичностью, указанной в параметре "Периодичность загрузки CRL"
Периодичность загрузки CRL	Периодичность, с которой осуществляется автоматическая загрузка CRL. Принимает значения от 1 до 48 (в часах). Параметр доступен для настройки только при включенном параметре "Автоматическая загрузка CRL"

3. Нажмите кнопку "Сохранить".

Настройки TLS-соединений

Внимание! Для изменения некоторых настроек установления TLS-подключения необходимо запустить Континент ZTN Клиент в режиме администратора.

Для настройки параметров работы режима TLS:

1. В окне настроек перейдите на вкладку "TLS".

В области отображения информации появится окно настройки параметров.

2. Установите требуемые значения для параметров, приведенных ниже.

Параметр	Описание
Пользовательские сертификаты	
Сертификат по умолчанию	Сертификат, который будет автоматически использоваться для подключения к ресурсам
Браузер	
Браузер по умолчанию	Браузер, используемый для установления соединения с ресурсами
Серверные сертификаты	
Проверять подлинность сертификатов	При включенном параметре во время установления соединения с СД и/или ресурсами осуществляется проверка подлинности сертификатов по CRL
Обновление списка ресурсов	
Проверить наличие обновлений	При нажатии кнопки, если доступно обновление списка ресурсов, на экране появится окно с соответствующим уведомлением. При нажатии кнопки "Да" осуществляется обновление списка ресурсов
Автоматически проверять наличие обновлений	При включенном параметре осуществляется автоматическая проверка обновлений списка ресурсов с периодичностью, указанной в параметре "Периодичность проверки", и временем ожидания, указанным в параметре "Время ожидания соединения"
Периодичность проверки	Период времени для автоматического обновления ресурсов (в часах). Принимает значения от 1 до 999. Значение по умолчанию — 1
Время ожидания соединения	Период времени ожидания сервера при обновлении списка ресурсов (в секундах). Принимает значения от 1 до 999. Значение по умолчанию — 120

Параметр	Описание
Подключение	
Протокол	Протоколы, используемые для TLS-соединений. Принимает значения: • TLS v1.0; • TLS v1.2; • TLS v1.0, v1.2
Режим упрощенного подключения	При включенном параметре возможно установление соединения при возникновении проблем с серверным сертификатом

3. Нажмите кнопку "Сохранить".

Настройки прокси-сервера

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

Для настройки подключения через внешний прокси-сервер:

1. В окне настроек перейдите на вкладку "Прокси".

   В области отображения информации появится окно настройки параметров работы с прокси-сервером.
2. Установите требуемые значения для параметров, приведенных ниже.

Параметр	Описание
Прокси	
Подключаться через внешний прокси-сервер	При включенном параметре доступна ручная настройка прокси-сервера для установления соединения с СД и ресурсами
Адрес	Адрес прокси-сервера (URL или IP-адрес)
Порт	Порт прокси-сервера. Принимает значения от 1 до 65535
Исключения	Адреса веб-ресурсов, для подключения к которым не используется внешний прокси-сервер
Аутентификация	
Метод аутентификации	Метод аутентификации на прокси-сервере. Принимает значения: • без аутентификации; • Basic; • NTLM
Использовать данные текущего пользователя системы	При включенном параметре аутентификация на прокси-сервере осуществляется с помощью учетных данных текущего пользователя ОС
Домен	Домен для аутентификации на прокси-сервере
Учетная запись	Имя учетной записи, принадлежащей указанному выше домену, для аутентификации на прокси-сервере
Пароль	Пароль для аутентификации на прокси-сервере
Сбросить сохраненный пароль	При нажатии осуществляется сброс пароля к внешнему прокси-серверу

3. Нажмите кнопку "Сохранить".

Импорт и экспорт конфигурации

На вкладке "Конфигурация" окна "Настройки" осуществляется импорт и экспорт конфигурации Клиента. Конфигурация сохраняется в виде файла с расширением "json".

Для экспорта конфигурации:

Примечание. Конфигурация содержит данные о профилях и ресурсах пользователя, от имени которого осуществлен вход в систему.

1. В окне настроек перейдите на вкладку "Конфигурация".
2. В группе параметров "Экспорт" в раскрывающемся списке укажите требуемый тип данных:
   - все данные;
   - только профили для подключения к СД;
   - только TLS-ресурсы.

3. Нажмите кнопку "Экспортировать".
   На экране появится стандартное окно для сохранения файла.
4. Укажите имя файла и его месторасположение.
5. Нажмите кнопку "Сохранить".
   Файл конфигурации будет сохранен в указанной директории.

Для импорта конфигурации:

1. В окне настроек перейдите на вкладку "Конфигурация".
2. В группе параметров "Импорт" нажмите кнопку "Импортировать".
   На экране появится стандартное окно выбора файла.
3. Выберите требуемый файл конфигурации с расширением "json" и нажмите кнопку "Открыть".
   Конфигурация будет импортирована. На экране появится соответствующее сообщение.

Просмотр событий

События, связанные с работой Клиента, а также установлением соединения с СД и защищенными ресурсами, регистрируются в журнале.

Примечание. Для Клиента в исполнении 3 только администратор имеет право на чтение файлов журналов.

Файлы журналов Клиента расположены в директории "/var/log" и имеют следующие имена:

- cts.log — события, связанные с работой Клиента в режиме VPN;
- ctstls.log — события, связанные с работой Клиента в режиме TLS.

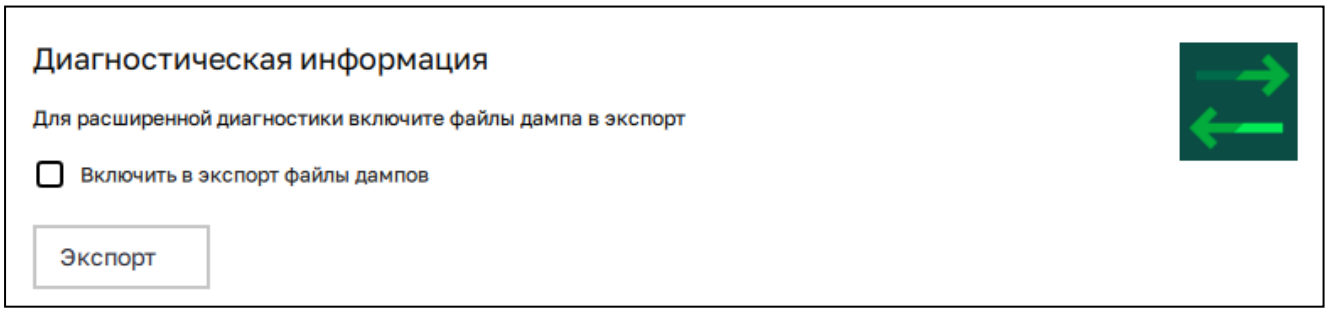
Для просмотра событий необходимо открыть требуемый файл в текстовом редакторе.

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 утилиту "Сбор диагностической информации – Континент ZTN Клиент".
   На экране появится окно утилиты сбора диагностической информации.



2. Для включения в сборку файлов дампов установите соответствующую отметку.

   Примечание. При включении файлов дампов в экспортный файл формирование отчета занимает более продолжительное время.
3. Нажмите кнопку "Экспорт".
   На экране появится стандартное окно сохранения файла.
4. Укажите имя архива и его месторасположение.
5. Нажмите кнопку "Сохранить".
   Архив с диагностической информацией будет сохранен в указанной директории. На экране появится соответствующее сообщение.
6. Нажмите кнопку "Закрыть".

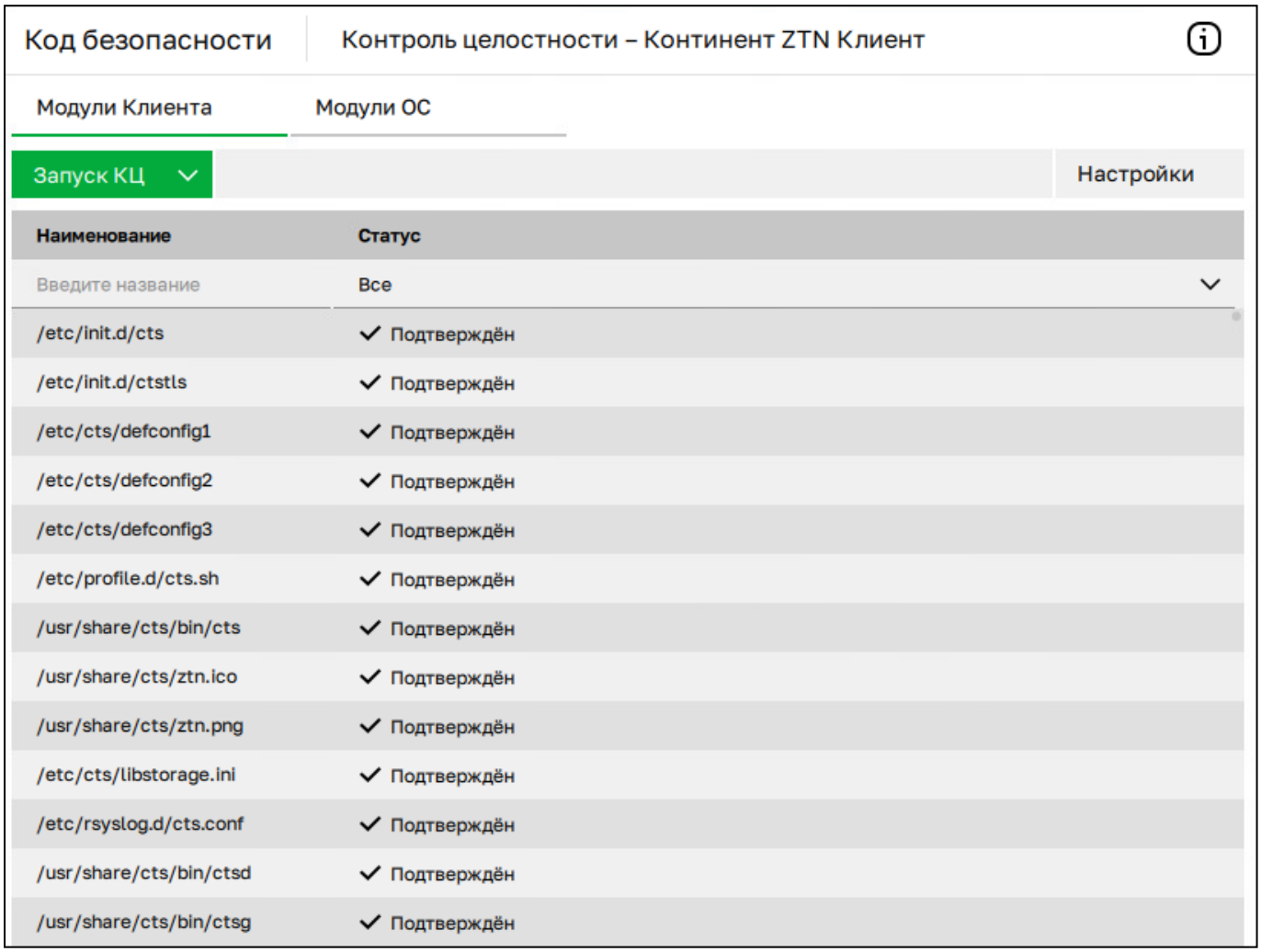
Контроль целостности

Контроль целостности осуществляется с помощью утилиты "Контроль целостности – Континент ZTN Клиент".

В список контролируемых файлов включаются:

- файлы ПО Клиента;
- файлы ОС, связанные с его функционированием;
- дополнительное ПО, отсутствие которого не позволит установить подключение с СД.

При запуске утилиты проверка КЦ начнется автоматически. По результатам проверки на экране появится соответствующее сообщение.



Для проверки целостности вручную:

1. Запустите утилиту "Контроль целостности – Континент ZTN Клиент".

   На экране появится основное окно УКЦ.
2. На панели инструментов нажмите кнопку "Запуск КЦ".
3. В раскрывающемся списке нажмите кнопку "Программа и операционная система".

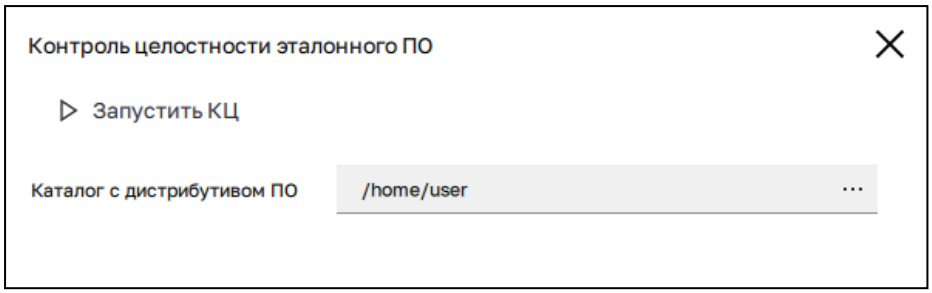
   Начнется процедура проверки целостности, по завершении которой на экране появится соответствующее сообщение.

Для проверки целостности эталонного ПО:

1. Запустите утилиту "Контроль целостности – Континент ZTN Клиент".

   На экране появится основное окно УКЦ.
2. На панели инструментов нажмите кнопку "Запуск КЦ".
3. В раскрывающемся списке нажмите кнопку "Эталонное ПО".

На экране появится окно для запуска процедуры проверки целостности эталонного ПО.



4. В поле "Каталог с дистрибутивом ПО" укажите месторасположение эталонного ПО.
5. Нажмите кнопку "Запустить КЦ".

   Начнется процедура проверки целостности эталонного ПО, в результате которой на экране появится таблица, содержащая названия проверенных файлов, их контрольные суммы и статусы КЦ.

Для пересчета контрольных сумм:

1. Запустите утилиту "Контроль целостности – Континент ZTN Клиент".

   Примечание. При работе с Клиентом в исполнении, соответствующем классу КС3, запустите УКЦ в режиме администратора.

   На экране появится основное окно УКЦ.
2. Перейдите на вкладку "Модули ОС" и на панели инструментов нажмите кнопку "Пересчет".

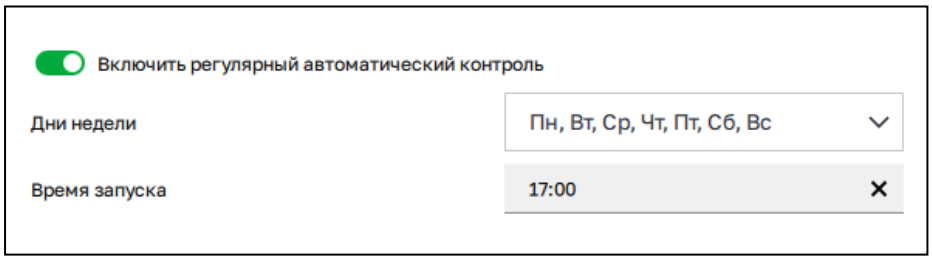
   Начнется процедура пересчета контрольных сумм, по завершении которой на экране появится соответствующее сообщение.

Для настройки проверки целостности по расписанию:

1. Запустите утилиту "Контроль целостности (режим администратора) – Континент ZTN Клиент".

   На экране появится основное окно УКЦ.
2. На панели инструментов нажмите кнопку "Настройки".

   На экране появится окно с настройками расписания автоматической проверки целостности.



3. Активируйте параметр "Включить регулярный автоматический контроль".

   Параметры "Дни недели" и "Время запуска" станут доступными для настройки.
4. В раскрывающемся списке "Дни недели" укажите требуемые значения.
5. В поле "Время запуска" укажите время для начала процедуры проверки целостности по расписанию.
6. Нажмите кнопку "Сохранить".

   Автоматическая проверка целостности будет осуществляться по указанному расписанию.

Приложение

Список поддерживаемых ОС семейства Linux

ОС	Версия
Astra Linux	Common Edition 2.12.43 x86_64 Desktop
	Common Edition 2.12.45.5 Desktop
	Special Edition 1.6 x86_64 Desktop
	Special Edition 1.7 x86_64 Desktop
	Special Edition 8.1 x86_64 Desktop
CentOS	7.2 x86_64 Server, Desktop
	7.3.1611 x86_64 Server, Desktop
	7.5.1804 x86_64 Server, Desktop
Debian	11 x86_64 Server, Desktop
RHEL	8.2 x86_64 Server, Desktop
Ubuntu	22.04.3 LTS x86_64 Server, Desktop
Альт	8 СП x86_64 Server, Desktop
	Рабочая станция 9.1 x86_64 Desktop
	Рабочая станция 9.2 x86_64 Desktop
	Рабочая станция К 9.2 x86_64 Desktop
РЕД ОС	7.3 x86_64 Server, Desktop

Управление Клиентом из командной строки

В данном разделе приведено описание специализированной утилиты **cts**, расположенной в каталоге /usr/share/cts/bin и используемой для управления Клиентом. В этом каталоге содержатся все исполняемые файлы Клиента.

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 Клиентом;
- ctsic — для контроля и расчета КЦ;
- ctsreg — для регистрации.

Утилита вызывается в следующем формате:

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

Для каждой команды имеется уникальный набор параметров. 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 Клиента
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
import initial-entropy	Импорт начальной энтропии из файла
events	Просмотр журнала событий
show profile	Просмотр параметров профиля
show certificate/cert	Просмотр данных сертификата
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 сертификата
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 config/parameter	Редактирование конфигурации пользователя
edit/modify settings proxy	Редактирование настроек прокси
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
generate-entropy	Генерация начальной энтропии

Команда connect

Команда осуществляет подключение к СД. Принимает на вход параметры, указанные ниже.

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

Команда disconnect

Команда осуществляет отключение от СД. Принимает на вход опциональный параметр -profile <NAME> для указания имени профиля.

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. Принимает на вход обязательный параметр -ras-version/-ras <number {3, 4}> для указания версии СД.

Команда import profile

Команда осуществляет импорт конфигурационного файла профиля. В ходе выполнения команды будет выполнен диалоговый скрипт. Принимает на вход параметры, указанные ниже.

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

Команда import initial-entropy

Команда предназначена для импорта начальной энтропии из файла. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Обязательный	
-file-path/-path	Путь к файлу
Опциональный	
-key-pass	Пароль доступа к файлу

Команда events

Команда предназначена для просмотра журнала событий. Принимает на вход параметры, указанные ниже.

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

Команда show profile

Команда предназначена для просмотра списка профилей. Принимает на вход параметры, указанные ниже.

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

Команда show certificate/cert

Команда предназначена для просмотра информации о сертификатах. Принимает на вход параметры, указанные ниже.

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

Команда show config/parameter

Команда предназначена для просмотра информации о конфигурации пользователя. Принимает на вход опциональный параметр -user <NAME> для указания имени пользователя.

Команда show stats

Команда предназначена для просмотра информации об активном подключении. Принимает на вход опциональный параметр -user <NAME> для указания имени пользователя.

Команда add profile

Команда предназначена для создания профиля подключения. Принимает на вход параметры, указанные ниже.

Параметр	Описание
Обязательный	
-name <NAME>	Имя профиля

Параметр	Описание
Опциональные	
-ras-version/-ras {3, 4}	Версия СД
-auth {login, cert}	Тип аутентификации
-cert-path	Путь к сертификату
-login	Логин пользователя
-server <HOST>	Адрес сервера
-port <number {0..65535}>	Порт сервера доступа
-proto/-protocol	Протокол соединения
-user <NAME>	Имя пользователя
-default	Использовать профиль по умолчанию
-select-cert	Выбрать сертификат
-select-key	Выбрать ключевой контейнер

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. Принимает на вход параметры, указанные ниже.

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

Команда add cert

Команда предназначена для добавления сертификатов. Принимает на вход параметры, указанные ниже.

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

Команда add cdp

Команда предназначена для ручного добавления адреса CDP. Принимает на вход обязательный параметр -url для указания ссылки на CDP.

Команда edit/modify profile

Команда предназначена для редактирования профиля пользователя. Принимает на вход параметры, указанные ниже.

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

Команда edit/modify connection

Команда предназначена для редактирования существующего подключения в профиле. Принимает на вход параметры, указанные ниже.

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

Команда edit/modify cdp

Команда предназначена для редактирования адреса CDP, введенного вручную. Принимает на вход параметры, указанные ниже.

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

Команда edit/modify config/parameter

Команда предназначена для редактирования конфигурации пользователя. Принимает на вход опциональный параметр -connection-try-count <number {0..99}> для указания количества попыток подключения.

Команда edit/modify settings proxy

Команда предназначена для настройки прокси соединения. Принимает на вход параметры, указанные ниже.

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

Команда edit/modify settings gui

Команда предназначена для изменения графических настроек приложения. Принимает на вход параметры, указанные ниже.

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

Команда delete/del profile

Команда предназначена для удаления профиля пользователя. Принимает на вход параметры, указанные ниже.

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

Команда delete/del connection

Команда предназначена для удаления существующего подключения в профиле. Принимает на вход параметры, указанные ниже.

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

Команда delete/del cdp

Команда предназначена для удаления адреса CDP, введенного вручную. Принимает на вход параметры, указанные ниже.

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

Команда delete/del cert

Команда предназначена для удаления сертификатов. Принимает на вход параметры, указанные ниже (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

Команда delete/del pass

Команда предназначена для удаления сохраненных паролей из профилей пользователя. Принимает на вход параметры, указанные ниже.

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

Команда update keypass

Команда предназначена для смены пароля ключевого контейнера пользовательского сертификата. Принимает на вход параметры, указанные ниже.

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

Файлы контроля целостности

Просмотр списка файлов, поставленных на контроль

Для просмотра списка файлов, поставленных на КЦ, 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. **40**) и выполните следующую команду:

```
ctsic check --print
```

Повторное создание списка файлов, подлежащих контролю

Список файлов, подлежащих КЦ, содержится в файле **/etc/cts/filelist.current**. В некоторых случаях, например, при обновлении ОС, 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 выполните следующую команду:

```
autoctsic
```

Перерасчет контрольных сумм

Для перерасчета контрольных сумм:

1. Повторно создайте список файлов, подлежащих контролю целостности (см. выше).
2. Рассчитайте их контрольные суммы, выполнив следующую команду:

   ```
   ctsic compute
   ```

Для проверки целостности дистрибутива "Континент ZTN Клиент" выполните следующую команду:

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

где **<path>** — путь до каталога, в котором находятся установочный пакет Клиента и файл, содержащий его контрольную сумму.

Для настройки расписания КЦ выполните следующую команду:

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

Внимание!

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

Сбор диагностической информации

Для сбора диагностической информации выполните 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
  ```

  где **-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 ZTN Клиент

Для каждой команды имеется уникальный набор параметров. Список команд и их описание приведены в таблице ниже.

Команда	Описание
-h/help/--help/-help/sos/?	Вызов инструкции по использованию утилиты
-o/online	Онлайн-регистрация через HOST
-r/request	Создание файла запроса на регистрацию
-i/import	Импорт лицензии из файла
-c/check	Проверка регистрации
-t/trial	Просмотр количества дней, оставшихся до окончания демонстрационного периода
-H/HID	Просмотр HID (идентификатора оборудования)

Команда -h/help/--help/-help/sos/?

Команда осуществляет вывод инструкции по использованию утилиты и перечня всех команд.

Команда -o/online

Примечание. Если выполнить ввод команды без указания параметров, на экране поочередно будут запрошены обязательные данные, требуемые для регистрации.

Команда предназначена для выполнения онлайн-регистрации. Принимает на вход параметры, приведенные ниже.

Параметр	Описание
Обязательные	
--first-name	Имя
--last-name	Фамилия
--email <user@host.domain>	Электронная почта
--security-class/protection {КС1, КС2, КС3}	Класс безопасности
Опциональные	
--host <HOST (default: registration.securitycode.ru)>	Сервер регистрации
--middle-name	Отчество
--city	Город проживания
--org/--organization	Организация
--dept/--department	Отдел

Команда -r/request

Команда предназначена для создания файла запроса на регистрацию (офлайн-регистрация). Принимает на вход параметры, приведенные ниже.

Параметр	Описание
Обязательные	
--path <FILE>	Путь к файлу для сохранения запроса
--first-name	Имя
--last-name	Фамилия
--email <user@host.domain>	Электронная почта
--security-class/protection {КС1, КС2, КС3}	Класс безопасности

Параметр	Описание
Опциональные	
--middle-name	Отчество
--city	Город проживания
--org/--organization	Организация
--dept/--department	Отдел

Команда -i/import

Команда предназначена для импорта лицензии из файла. Принимает на вход обязательный параметр --path <FILE> для указания пути к файлу для импорта лицензии.