



Средство криптографической защиты информации

Континент TLS-клиент

Версия 2

Руководство по эксплуатации



© Компания "Код Безопасности", 2021. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

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

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

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

Телефон: **8 495 982-30-20**

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

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

Оглавление

Введение	4
Общие сведения	5
Назначение и основные функции	5
Принципы функционирования	6
Сертификаты открытых ключей	6
Контроль целостности	7
Назначение ключевых носителей	8
Аудит	8
Установка, удаление, восстановление и обновление программного обеспечения	9
Установка программного обеспечения TLS-клиента	9
Установка дополнительного ПО	11
Удаление	11
Восстановление	11
Обновление ПО	11
Настройка и эксплуатация	13
Ввод в эксплуатацию	13
Подготовка к работе	13
Запуск TLS-клиента	13
Контекстное меню	14
Пользовательский интерфейс основного окна	14
Регистрация TLS-клиента	15
Управление сертификатами	17
Начальная настройка	17
Создание ключа и запроса на сертификат	17
Варианты использования криптопровайдера при формировании закрытого ключа пользователя	21
Импорт сертификата	25
Просмотр сведений о сертификате	27
Управление CRL	27
Настройка CDP	27
Загрузка CRL	28
Настройка соединений	29
Режим упрощенного подключения	30
Настройка параметров работы TLS-клиента	31
Основные настройки	32
Настройки прокси	34
Управление конфигурацией	36
Настройки обновления	37
Аудит	39
Внешний вид	40
Эксплуатация TLS-клиента	41
Доступ к защищенным ресурсам	41
Контроль целостности	42
Приложение	45
Требования к сертификатам	45
Структура и содержание серверного сертификата	45
Структура и содержание сертификата пользователя	46
Пример настроечного файла	47
Список регистрируемых событий	50

Введение

Руководство предназначено для пользователей и администраторов изделия "Средство криптографической защиты информации "Континент TLS-клиент". Версия 2" (далее — TLS-клиент). В нем содержатся сведения, необходимые для установки, настройки и эксплуатации TLS-клиента.

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 8-800-500-30-20 или по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании <https://www.securitycode.ru/company/education/training-courses/>.

Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Глава 1

Общие сведения

Назначение и основные функции

TLS-клиент предназначен для реализации защищенного доступа удаленных пользователей к веб-ресурсам корпоративной сети по каналам связи общих сетей передачи данных.

TLS-клиент выполняет следующие основные функции:

- реализация TLS-аутентификации (в том числе односторонней) на основе технологии открытых ключей (используются сертификаты открытых ключей стандарта X.509 версии 3);
- поддержка работы с ключевыми носителями, изданными в "КриптоПро УЦ" 1.5 и 2.0 (последний при условии активации модуля extendedcontainer);
- установление защищенного соединения с TLS-сервером на базе протокола HTTPS и обмен данными с ресурсами корпоративной сети;
- возможность работы с серверами, поддерживающими протокол TLS 1.0, 1.2;
- хранение ключевой информации в защищенном контейнере;
- проверка сертификатов ключей по списку отозванных сертификатов (CRL);
- регистрация событий, связанных с настройкой и функционированием TLS-клиента, в журнале операционной системы (ОС) Windows;
- контроль целостности программного обеспечения (ПО), передаваемой и хранимой информации;
- возможность автоматического обновления ПО и автоматической конфигурации перечня защищенных ресурсов;
- очистка сессионной, включая криптографическую, информации при разрыве соединения.

TLS-клиент функционирует совместно с изделиями "Средство криптографической защиты информации "Континент TLS VPN Сервер". Версия 1.2", "Средство криптографической защиты информации "Континент TLS-сервер". Версия 2" (далее — TLS-сервер).

TLS-клиент используется для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.

TLS-клиент реализуется в двух исполнениях:

- исполнение 1 соответствует требованиям ФСБ России к криптографическим средствам класса KC1;
- исполнение 2 соответствует требованиям ФСБ России к криптографическим средствам класса KC2, работает совместно с сертифицированным ФСБ России аппаратно-программным модулем доверенной загрузки "Программно-аппаратный комплекс "Соболь" (далее — ПАК "Соболь").

TLS-клиент устанавливается на компьютеры, удовлетворяющие следующим системным требованиям:

Элемент	Требование
Операционная система (должны быть установлены все обновления системы)	<ul style="list-style-type: none"> • Windows 10 (включая выпуски Starter и Home Edition); • Windows 8.1; • Windows 7 SP1; • Windows Server 2012 R2 x64; • Windows Server 2016 x64; • Windows Server 2019 x64
Процессор. Оперативная память	В соответствии с требованиями ОС, установленной на компьютер

Элемент	Требование
Жесткий диск (свободное место)	150 Мбайт
Порты (свободные)	1 x USB 2.0 — для использования USB-флеш-накопителя; 1 x слот PCI-E — для установки платы ПАК "Соболь" (для исполнения 2)
Привод	Привод DVD/CD-ROM
Дополнительное оборудование (для исполнения 2)	ПАК "Соболь"
Дополнительное ПО	Веб-браузер: <ul style="list-style-type: none"> • Google Chrome 48 или выше (для Windows 7, 8.1, 10, Windows Server 2012, 2016, 2019); • Mozilla Firefox 46 или выше (для Windows 7, 8.1, 10, Windows Server 2012, 2016, 2019); • Internet Explorer 8, 9, 10 (для Windows 7, Windows Server 2012, 2016, 2019); • Internet Explorer 11 (для Windows 7, 8.1, 10, Windows Server 2012, 2016, 2019); • Microsoft Edge (для Windows 10, Windows Server 2012, 2016, 2019)

Принципы функционирования

TLS-клиент представляет собой устанавливаемое на компьютер пользователя ПО, взаимодействующее с TLS-сервером.

Для подключения к защищаемым веб-ресурсам корпоративной сети удаленный пользователь должен в адресной строке веб-браузера ввести имя веб-ресурса. По указанному имени TLS-клиент посылает TLS-серверу запрос на создание защищенного соединения.

На основании принятого запроса TLS-сервер запускает процедуру аутентификации клиент-сервер. Аутентификация проводится на основе сертификатов открытых ключей.

После успешного завершения процедуры аутентификации выполняется генерация сеансового ключа, и между TLS-клиентом и TLS-сервером устанавливается защищенное соединение по протоколу TLS. Далее TLS-сервер направляет запрос TLS-клиента по указанному пользователем адресу веб-ресурса в защищаемую сеть. Полученный от веб-сервера ответ на запрос TLS-сервер возвращает TLS-клиенту в рамках защищенного соединения.

TLS-клиент поддерживает работу в режиме единого входа – Single Sign On (SSO) с помощью протоколов NTLM и Negotiate. Аутентификационные данные, введенные пользователем при входе в систему, не требуют повторного ввода при переходе с ресурса на ресурс на протяжении рабочей сессии.

В случае невыполнения по каким-либо причинам требований, предъявляемых к аутентификации TLS-клиента и TLS-сервера, защищенное соединение не устанавливается и доступ пользователя к веб-ресурсу блокируется.

TLS-клиент также может формировать безопасный туннель на основе протокола TLS (далее — TLS-туннель) по алгоритмам ГОСТ 28147-89, ГОСТ Р 34.12-2015 для обмена данными какого-либо приложения пользователя с защищаемым веб-ресурсом корпоративной сети. При этом обеспечивается криптографическая двусторонняя аутентификация отправителя и адресата, контроль целостности и шифрования данных информационного обмена.

Сертификаты открытых ключей

Для работы TLS-клиента требуются следующие сертификаты:

- сертификат издателя;

Пояснение. Сертификат издателя — это корневой сертификат удостоверяющего центра, издавшего сертификат TLS-сервера.

- сертификат пользователя;
- сертификат TLS-сервера.

Поддерживается работа с ключами форматов PKCS#15, с сертификатами X.509v3 форматов DER и PEM.

Предусмотрена проверка сертификатов TLS-сервера по списку отозванных сертификатов. При наличии прямого доступа компьютера к удостоверяющему центру загрузка CRL по протоколу HTTP осуществляется автоматически. При отсутствии прямого доступа CRL должны загружаться пользователем посредством ПО TLS-клиента в хранилище сертификатов OC Windows.

Контроль целостности

Функция контроля целостности (КЦ) предназначена для слежения за неизменностью содержимого ПО TLS-клиента, выполняется с помощью утилиты "Контроль целостности" (УКЦ), входящей в дистрибутив TLS-клиента.

Контролируются файлы и каталоги дистрибутива или установленного ПО TLS-клиента, а также файлы OC Windows.

В первом случае УКЦ выполняет КЦ эталонного ПО путем вычисления контрольных сумм (КС) файлов, содержащихся на диске из комплекта поставки TLS-клиента, и сравнения полученных значений со значениями, хранящимися в специальном файле дистрибутива TLS-клиента. Эти значения также приведены в формуляре TLS-клиента.

Во втором случае выполняется сравнение текущих значений КС контролируемых файлов и эталонных значений, рассчитанных в ходе установки TLS-клиента. Выполнение процедуры пересчета эталонных значений доступно пользователю с правами администратора OC Windows.

Список файлов TLS-клиента, подлежащих контролю, и значения КС для каждого из них хранятся в конфигурационном файле. Конфигурационный файл формируется при установке инсталляционного пакета.

КЦ установленного ПО осуществляется в начале работы TLS-клиента и в ходе регламентных проверок с периодичностью, заданной в настройках УКЦ. Настройка параметров КЦ разрешена только пользователям с правами администратора OC Windows (см. стр. 43).

Если в ходе проведения КЦ в начале работы будет обнаружено нарушение целостности файлов, ошибка, то TLS-клиент не будет запущен, а пользователь получит информационное сообщение о нарушении целостности.

Если в ходе проведения регламентной проверки будет обнаружено нарушение целостности и при этом приложение TLS-клиента будет активно, то:

- рабочие сессии с защищенными ресурсами будут продолжаться;
- создание новых защищенных сессий будет заблокировано;
- значок приложения на панели задач OC Windows будет дополнен предупреждающим элементом;
- пользователь получит информационное сообщение о нарушении целостности с одновременным предложением восстановить целостность ПО.

В случае обнаружения нарушения целостности при неактивном ПО TLS-клиента будет сделана соответствующая запись в журнале событий.

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

- при каждом запуске TLS-клиента;
- каждой попытке установления сессии с защищенным ресурсом (если нарушение целостности обнаружено в ходе регламентного контроля целостности при наличии активных сессий с защищенными ресурсами).

События, связанные с КЦ, регистрируются в журнале событий ОС Windows (см. стр. 50).

В состав УКЦ включена опция "Контроль установленного программного обеспечения". Она собирает информацию о наличии на компьютере пользователя ПО согласно заданным критериям. По умолчанию опция отключена. Включение проверки и определение ее критериев доступно только пользователю с правами администратора ОС Windows. В случае непрохождения проверки подключение TLS-клиента к TLS-серверу запрещается.

Назначение ключевых носителей

Персональный ключевой носитель, выдаваемый пользователю администратором, предназначен для хранения ключевой информации: контейнера с закрытым ключом и пароля к нему. Также на ключевом носителе могут быть переданы сертификат пользователя и удостоверяющий его корневой сертификат.

Необходимо учесть:

- рабочих ключевых носителей одновременно может быть больше одного;
- на одном ключевом носителе могут быть записаны ключи для разных серверов.

В качестве ключевых носителей могут использоваться аппаратные носители следующих типов:

- USB-флеш-накопители;
- USB-ключи — Рутокен, Рутокен Lite, Рутокен S (версии 2.0 и 3.0), Рутокен ЭЦП, JaCarta PKI, JaCarta ГОСТ, JaCarta PKI Flash, JaCarta ГОСТ Flash, eToken PRO (Java), Esmart USB Token, Esmart USB Token ГОСТ;
- смарт-карты — Рутокен ЭЦП, Рутокен Lite, JaCarta PKI, JaCarta ГОСТ, eToken PRO (Java), Esmart, Esmart ГОСТ;
- идентификаторы DS1995, DS1996.

Примечание. Для использования аппаратных носителей требуется установка их драйверов и сопутствующего ПО (см. стр. 11).

После предъявления ключевого носителя считанные ключ и сертификаты сохраняются в памяти программы. При отсутствии секретного ключа в памяти программы при двусторонней аутентификации он запрашивается с выводом на экран соответствующего сообщения.

Пользователь может отказаться от чтения ключевого контейнера при двусторонней аутентификации. В этом случае соединение с защищаемым сервером не устанавливается.

Аудит

Под аудитом (сбором диагностической информации) подразумевается контроль состояния работоспособности TLS-клиента. Аудит производится с помощью утилиты "Сбор диагностической информации", входящей в дистрибутив TLS-клиента. Оценка функционирования ПО осуществляется посредством анализа произошедших событий, зарегистрированных в ходе аудита.

В рамках аудита используются два типа ресурсов, хранящихся локально на TLS-клиенте:

- системный журнал;
- лог-файлы (доступен их экспорт).

В системном журнале хранятся события от узлов сети, служб TLS-клиента, а также любые другие системные события, удовлетворяющие минимальным требованиям к хранению их в журнале.

Лог-файлы содержат более полную информацию. Аудит этого типа ведется только при включенном расширенном логировании в настройках TLS-клиента (подробнее см. стр. 39).

Глава 2

Установка, удаление, восстановление и обновление программного обеспечения

Установка программного обеспечения TLS-клиента

Пользователь, устанавливающий ПО TLS-клиента, должен обладать правами администратора компьютера — входить в локальную группу администраторов.

Внимание! До начала инсталляции ПО TLS-клиента должны быть установлены последние обновления ОС Windows. Иначе в процессе установки TLS-клиента появится сообщение об ошибке и инсталляция будет прервана.

В процессе установки ПО инсталлятор анализирует установленные программные компоненты и при необходимости сообщает о недостающем ПО.

Для удобства работы с TLS-клиентом администратор безопасности вашей компании может предоставить вам файл с настройками работы ПО (настроечный файл). Сохраните файл на своем локальном компьютере и во время процедуры установки ПО укажите путь к нему.

Внимание! Корневой и серверный сертификаты, а также сертификат пользователя не импортируются с помощью настроечного файла. Их надо устанавливать отдельно.

В ходе установки также будет установлено или обновлено ПО криптопровайдера "Код Безопасности CSP".

TLS-клиент поддерживает работу со сторонними криптопровайдерами при соблюдении некоторых условий:


- сторонний криптопровайдер должен быть установлен перед инсталляцией TLS-клиента;
- для установки криптопровайдера должна быть выбрана версия на том же языке, на котором будет установлен TLS-клиент (в настоящее время доступна только русскоязычная версия ПО).

Если планируется использовать исключительно криптопровайдер "Код Безопасности CSP", уберите отметку о возможности совместной работы со сторонним криптопровайдером (установлена по умолчанию, см. рисунок ниже).

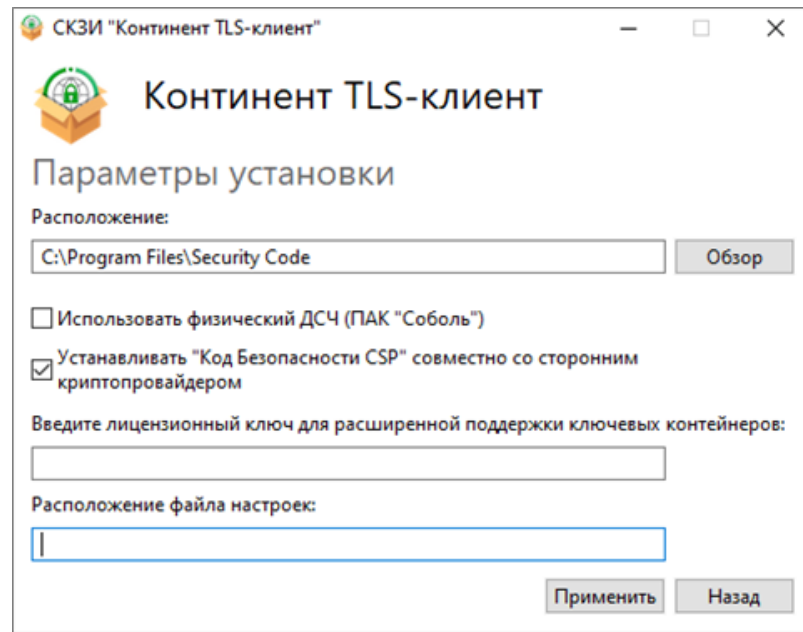
Внимание! Если на компьютере установлена старая версия "Код Безопасности CSP", удалите ее перед началом установки TLS-клиента.

Если после установки TLS-клиента сторонний криптопровайдер будет удален, необходимо заново установить "Код Безопасности CSP" с помощью одноименной утилиты, входящей в состав дистрибутива TLS-клиента.

Для установки ПО:

1. Для установки TLS-клиента поместите установочный компакт-диск в привод DVD/CD-ROM и запустите на исполнение файл  Континент TLS-клиент.exe. На экране появится окно установки TLS-клиента с текстом лицензионного соглашения.

Примечание. Если необходимо исключить совместную работу "Код Безопасности CSP" с другими криптопровайдерами, выбрать каталог установки файлов программы, отличный от выбора по умолчанию, ввести лицензионный ключ для расширенной поддержки ключевых контейнеров, выбрать физический датчик случайных чисел ПАК "Соболь" или указать адрес расположения настроечного файла, нажмите кнопку "Настройки" и следуйте инструкциям, появляющимся на экране.



2. Прочтите лицензионное соглашение и, если вы принимаете его условия, поставьте отметку в поле "Я принимаю условия лицензионного соглашения", затем нажмите кнопку "Далее".

Примечание. В случае появления окна системы безопасности ОС Windows о подтверждении установки ПО нажмите кнопку "Да" или "Установить".

Мастер установки выполнит диагностику системы и начнет установку ПО. После успешного завершения установки программы на экране появится сообщение о необходимости перезагрузки компьютера.

3. Нажмите кнопку "Перезагрузить" в окне сообщения.

Начнется перезагрузка компьютера.

После установки TLS-клиента на рабочем столе ОС Windows появится значок запуска графического приложения TLS-клиента, а в главном меню ОС Windows появится раздел "Код Безопасности".

В этом разделе доступны следующие приложения:

Название	Описание
Восстановление TLS-клиента	Восстановление ПО TLS-клиента из дистрибутива
Восстановление "Код Безопасности CSP"	Восстановление криптопровайдера "Код Безопасности CSP" из дистрибутива
Код Безопасности CSP	Запуск криптопровайдера "Код Безопасности CSP"
Континент TLS-клиент	Запуск ПО TLS-клиента
Контроль целостности TLS-клиента	Контроль целостности дистрибутива и установленного на компьютере ПО TLS-клиента
Регистрация TLS-клиента	Регистрация ПО "TLS-клиент" на сервере регистрации компании "Код Безопасности"
Сбор диагностической информации TLS-клиента	Экспорт отчета о состоянии работоспособности TLS-клиента

Установка дополнительного ПО

Если предполагается использовать СКЗИ "Континент TLS- клиент" с персональными ключевыми носителями, необходимо выполнить установку дополнительного ПО.

Для установки дополнительного ПО:

1. Если предполагается использовать персональные ключевые носители Ру-токен, необходимо скачать их драйверы и выполнить действия в соответствии с инструкцией по установке драйверов.
2. Если предполагается использовать персональные ключевые носители JaCarta PKI, JaCarta ГОСТ или eToken PRO (Java), необходимо установить единый клиент JaCarta.

Удаление

Удалить ПО "TLS-клиент" можно тремя способами, используя:

- средства удаления и изменения программ "Программы и компоненты" ОС Windows;

Примечание. При удалении TLS-клиента с помощью средств ОС Windows пользовательские настройки ПО на компьютере сохраняются и могут быть применены в дальнейшем, если на компьютер будет снова установлен TLS-клиент.

- утилиту восстановления ПО "TLS-клиент";
- MSI-пакет, находящийся на установочном диске.

Примечание. При удалении TLS-клиента с помощью утилиты восстановления или MSI-пакета доступна опция удаления пользовательских настроек ПО.

TLS- клиент и "Код Безопасности CSP" удаляются по отдельности в любом порядке.

Восстановление

Для восстановления ПО:

1. В главном меню ОС Windows в списке установленных программ найдите раздел "Код Безопасности" и активируйте приложение восстановления соответствующего ПО.

На экране появится окно установки ПО.

2. Нажмите кнопку "Далее".

На экране появится окно для восстановления или удаления ПО.

3. Выберите вариант "Восстановить", нажмите кнопку "Далее".

На экране появится итоговое окно.

4. Нажмите кнопку "Восстановить".

Начнется соответствующая операция, после завершения которой на экране появится окно об успешном завершении процесса.

5. Нажмите кнопку "Готово".

На экране появится сообщение о необходимости перезагрузки системы.

6. Нажмите кнопку "Перезагрузить".

Обновление ПО

Обновить установленное ПО TLS-клиента возможно как в автоматическом, так и в ручном режиме. Подробные сведения о настройках получения и установки обновлений см. стр. [37](#).

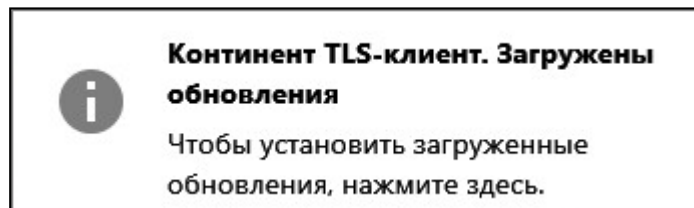
Внимание! При совместной работе с СКЗИ "Континент TLS VPN Сервер" версии 1.2 обновление посредством ПО TLS-клиента невозможно. В этом случае необходимо получить файл обновления от поставщика или с сервера обновлений ПО и установить его принудительно.

Для получения обновления ПО TLS-клиента:

1. Если в настройках TLS-клиента установлено автоматическое обновление ПО, при добавлении на TLS-сервер новых файлов обновлений на экране TLS-клиента появится информационное окно о наличии обновления. Перейдите к п. 5.

Внимание! Для управления обновлением ПО требуется запустить TLS-клиент от имени администратора.

2. Выберите в меню настроек TLS-клиента пункт "Обновления".
В области отображения информации основного окна откроется соответствующее подменю.
3. Введите адрес сервера обновлений ПО в соответствующее поле.
4. Нажмите кнопку "Проверить" в области принудительного обновления ПО.
Если адрес сервера обновлений не будет задан, на экране появится сообщение о необходимости ввести его.
На экране появится информационное окно о наличии обновления.
5. Нажмите на это окно.
Файлы обновлений будут загружены, и на экране появится информационное сообщение:



6. Нажмите на сообщение.
Будет произведена установка обновления, после чего на экране появится окно с требованием перезагрузки ОС.
7. Нажмите кнопку "Да".
Будет выполнена перезагрузка ОС Windows.

Глава 3

Настройка и эксплуатация

Ввод в эксплуатацию

Подготовка к работе

Ввод TLS-клиента в эксплуатацию состоит из следующих последовательных этапов:

1. Установка TLS-клиента (см. стр. 9).
2. Регистрация ПО (см. стр. 15).
3. Получение сертификатов (см. стр. 17).

Примечание. Алгоритмы формирования электронной подписи в используемых сертификатах должны совпадать.

4. Установка корневых и пользовательских сертификатов (см. стр. 25).
5. Установка CRL (если необходима проверка сертификатов по CRL, см. стр. 27).
6. Установка серверных сертификатов (если необходима соответствующая проверка, см. стр. 26).
7. Настройка параметров работы TLS-клиента (см. стр. 31).

Примечание. В случае использования прокси-сервера для доступа к интернет необходимо осуществить дополнительную настройку параметров работы TLS-клиента (см. стр. 34).

8. Настройка списка ресурсов (см. стр. 29).

Примечание. Для использования сетевых имен сервера или веб-ресурсов необходимо осуществить соответствующую настройку DNS-сервера или файла hosts. После внесения изменений в файл hosts необходимо перезапустить приложение TLS-клиента.

Запуск TLS-клиента

Для запуска TLS-клиента:

1. Дважды нажмите левой кнопкой мыши на значок "Континент TLS-клиент" на рабочем столе или войдите в меню "Пуск" и выберите в главном меню ОС Windows пункт "Код Безопасности | Континент TLS-клиент".

На экране откроется сообщение о накоплении энтропии для использования биологического датчика случайных чисел.

Внимание! Срок действия накопленной энтропии – 1 год. За две недели до окончания этого срока при каждом запуске TLS-клиента на экране начнет появляться запрос о наборе новой энтропии. Для накопления новой энтропии следуйте инструкциям на экране.

При отказе пользователь получит предупреждение о небезопасности использования устаревшей энтропии.

Если новая энтропия не будет набрана, то после окончания срока действия ранее накопленной энтропии работа TLS-клиента будет заблокирована и установление соединений станет невозможным.

2. Следуйте инструкциям на экране.

После завершения накопления энтропии появится сообщение о том, что программа не зарегистрирована, и предложение зарегистрировать "Континент TLS-клиент" на сервере регистрации компании "Код Безопасности".

3. Зарегистрируйте TLS-клиент на сервере регистрации (в случае необходимости выберите продолжение работы без регистрации). Подробнее о процессе регистрации см. стр. 15.

На экране появится основное окно программы, а в правом углу панели задач ОС Windows появится значок программы.

4. Если администратором безопасности вашей компании вам был предоставлен настроечный файл, импортируйте его (подробнее о настроечном файле и импорте/экспорте конфигурации см. стр. 36).

Контекстное меню



Вызов контекстного меню TLS-клиента с панели задач ОС Windows позволяет выполнить следующие команды:

- развернуть основное окно TLS-клиента ;
- сбросить текущие соединения;

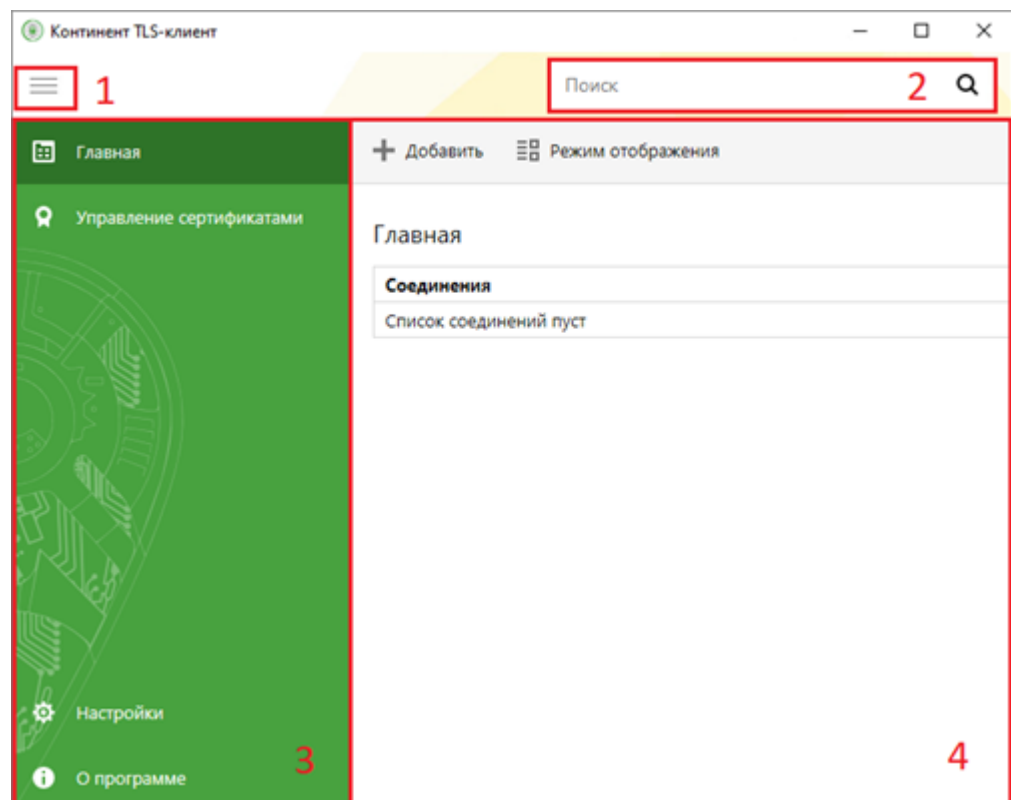
Внимание! Чтобы избежать случайного выполнения данной команды, в настройках TLS-клиента настройте подтверждение сброса соединений (см. стр. 33). После выполнения данной команды для установления новых соединений необходимо будет ввести учетные данные пользователя повторно.


- завершить работу ПО.

При двойном нажатии на значок программы TLS-клиента левой кнопкой мыши осуществляется раскрытие или скрытие основного окна.

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

Пользовательский интерфейс основного окна

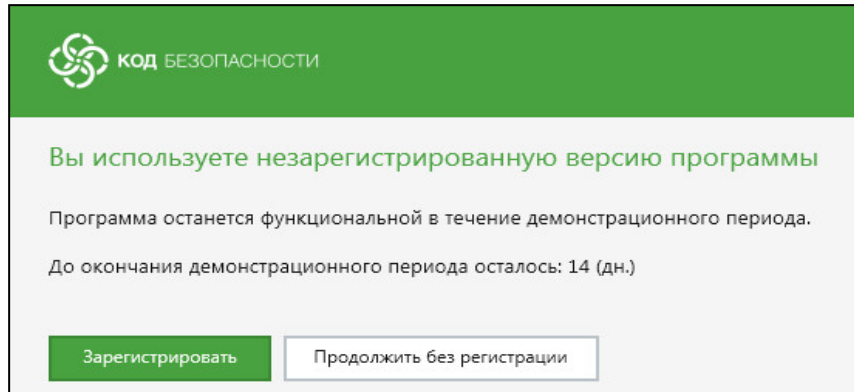


В верхней части основного окна расположена кнопка (1) переключения полного/сжатого вида главного меню  и строка (2) контекстного поиска.

В левой части основного окна расположен список разделов главного меню (3), а в правой — область отображения информации (4) активного раздела меню с панелью инструментов в верхней части.

Регистрация TLS-клиента

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



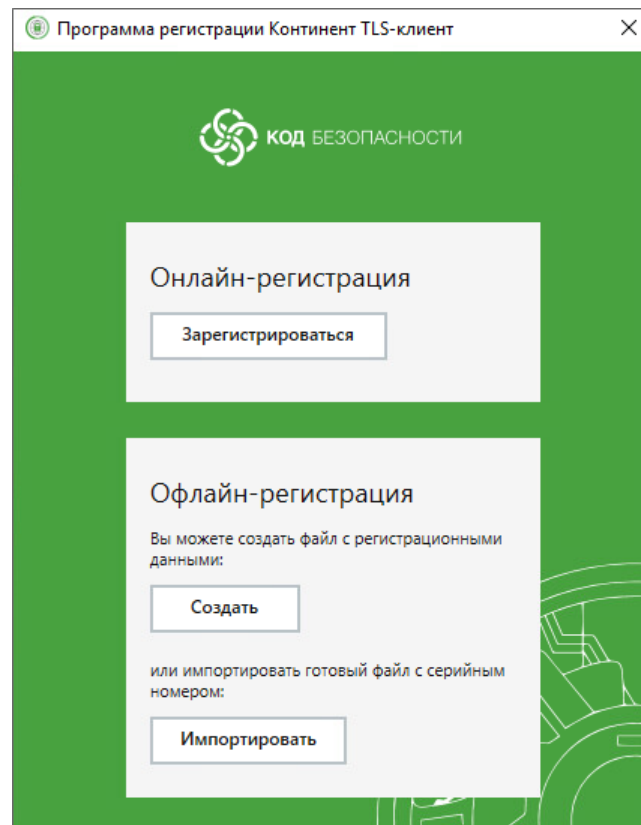
Срок работы без регистрации TLS-клиента ограничен и составляет 14 дней. Количество дней, оставшихся до окончания регистрации, отображается в разделе "О программе". Если в течение этого срока TLS-клиент не зарегистрировать, то при каждом следующем запуске на экране будет появляться предложение зарегистрировать ПО. В случае отказа работа СКЗИ "Континент TLS-клиент" будет прервана.

Внимание! Настройки системного прокси-сервера начинают работать в программе регистрации TLS-клиента после первого запуска TLS-клиента.

Для онлайн-регистрации TLS-клиента:

1. Нажмите кнопку "Зарегистрировать" в окне регистрации или выберите в главном меню ОС Windows пункт "Все приложения | Код Безопасности | TLS-клиент | Регистрация TLS-клиента".

Откроется окно регистрации.



2. Выберите пункт "Онлайн- регистрация" и нажмите кнопку "Зарегистрироваться".

На экране появится диалоговое окно регистрации.

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

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

После регистрации TLS-клиента в разделе "О программе" вместо текста "Программа не зарегистрирована" появится регистрационный номер программы.

Для офлайн-регистрации TLS-клиента:

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

На экране появится диалоговое окно регистрации.

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

2. Заполните требуемые параметры и нажмите кнопку "Готово".
На экране появится стандартное окно сохранения файла.
3. Сохраните файл с персональными данными и передайте его на сервер регистрации для получения файла с серийным номером.
4. После получения файла с серийным номером нажмите кнопку "Импортировать" в окне регистрации TLS-клиента.

На экране появится стандартное окно выбора файла.

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

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

Управление сертификатами

TLS-клиент позволяет устанавливать сертификаты в хранилище, создать криптографические контейнеры, запросы на издание сертификата пользователя, а также осуществлять их запись на съемный носитель или в реестр.

Начальная настройка

Для работы с TLS-клиентом необходимы корневые сертификаты, сертификаты пользователя и сертификаты сервера, получаемые в соответствии с общим порядком, установленным конкретным удостоверяющим центром. Процедура создания запроса на выдачу сертификата по алгоритму ГОСТ Р 34.10–2012 приводится на стр. 17.

TLS-клиент поддерживает сертификаты, выпущенные по алгоритму ГОСТ Р 34.10–2012 на основе использования эллиптических кривых Эдвардса с длиной ключа 256 и 512 бит.

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

TLS-клиент поддерживает совместную работу пары "сертификат пользователя – сертификат сервера", выпущенных по разным алгоритмам.

Для передачи сертификатов рекомендуется использовать отчуждаемый носитель.

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

- USB-флеш-накопители;
- USB-ключи — Рутокен, Рутокен Lite, Рутокен S (версии 2.0 и 3.0), Рутокен ЭЦП, JaCarta PKI, JaCarta ГОСТ, JaCarta PKI Flash, JaCarta ГОСТ Flash, eToken PRO (Java), Esmart USB Token, Esmart USB Token ГОСТ;
- смарт-карты — Рутокен ЭЦП, Рутокен Lite, JaCarta PKI, JaCarta ГОСТ, eToken PRO (Java), Esmart, Esmart ГОСТ;
- идентификаторы DS1995, DS1996.

После получения всех сертификатов пользователь TLS-клиента должен установить сертификаты в хранилище текущего пользователя средствами ПО TLS-клиента (см. стр. 25), ОС Windows

(см. [https://technet.microsoft.com/ru-ru/library/cc754841\(v=ws.11\).aspx#BKMK_addlocal](https://technet.microsoft.com/ru-ru/library/cc754841(v=ws.11).aspx#BKMK_addlocal)) или средствами стороннего криптопровайдера:

Сертификаты	Используемый криптопровайдер	
	Код Безопасности CSP	Сторонний
Корневые	Средствами ОС Windows или TLS-клиента	Средствами ОС Windows
Пользовательские	Средствами TLS-клиента	Средствами криптопровайдера
Серверные, CRL	Средствами TLS-клиента	Средствами TLS-клиента

Создание ключа и запроса на сертификат

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

Для создания запроса:

1. Выберите в главном меню TLS-клиента пункт "Управление сертификатами". В области отображения информации появится список установленных сертификатов.

Примечание. Для просмотра списка установленных сертификатов нажмите кнопку "Открыть хранилище" на панели инструментов.

2. На панели инструментов выберите вкладку пользовательских сертификатов и нажмите кнопку "Создать запрос".

На экране появится диалог выбора криптопровайдера и место хранения контейнера закрытого ключа сертификата.

3. Выберите нужные пункты меню:
 - в поле "Криптопровайдер" выберите в раскрывающемся списке нужное значение;
 - в поле "Хранилище сертификатов" выберите в раскрывающемся списке хранилище ключевого контейнера, в котором будет сохранен закрытый ключ сертификата пользователя:
 - Текущий пользователь;
 - Локальный компьютер;
 - в поле "Тип субъекта" выберите в раскрывающемся списке тип пользователя, создающего запрос:
 - Произвольный тип (по умолчанию);
 - Физическое лицо;
 - Физическое лицо с доверенностью от юридического;
 - Индивидуальный предприниматель;
 - Юридическое лицо;

- в поле "Использование ключей" выберите из раскрывающегося списка набор использования ключей:
 - Стандартный набор (минимально необходимые параметры для функционирования ключа шифрования);
 - Расширенный набор (выбор использования дополнительных параметров ключа шифрования, если это предусмотрено политикой информационной безопасности компании).
4. Нажмите кнопку "Далее".

На экране появится диалог для ввода параметров запроса.

Примечание. Каждому типу пользователя, создающего запрос, соответствует свой перечень параметров для заполнения. Ниже в качестве примера представлен диалог для ввода параметров запроса произвольного типа пользователя.

5. Заполните параметры диалога и нажмите кнопку "Далее".

Если был выбран расширенный набор параметров использования ключа (см. стр. 19), на экране появится диалог выбора параметров.

Примечание. Если был выбран стандартный набор параметров использования ключа, на экране появится диалог для ввода имени ключевого контейнера и имени файла для запроса сертификата. Перейдите к п. 7.

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

На экране появится диалог для ввода имени ключевого контейнера и имени файла для запроса сертификата.

7. Укажите:

- имя ключевого контейнера;

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

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

Примечание. По умолчанию запрос сохраняется в файле с расширением *.req и именем newreq.

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

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

8. Нажмите кнопку "Далее".

Появится сообщение о завершении работы мастера запроса сертификата.

9. Проверьте корректность введенных параметров и нажмите кнопку "Готово".

Криптопровайдер приступит к созданию закрытого ключа. Выполните следующие операции:

- сформируйте закрытый ключ с помощью датчика случайных чисел;
- выберите тип ключевого носителя для записи закрытого ключа;
- введите пароль для ограничения доступа к ключевому контейнеру.

Примечание. При наличии отметки в поле "Запомнить пароль" введенный пароль сохраняется в реестре компьютера. В дальнейшем при обращении к этому ключевому контейнеру запрос пароля на экран не выводится.

Порядок выполнения операций зависит от используемого криптопровайдера, датчика случайных чисел и ключевого носителя, выбранного для хранения ключевой информации. Следуйте указаниям, появляющимся на экране.

Более подробно о создании закрытого ключа см. стр. **21**.

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

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

Внимание! Если в качестве ключевого носителя был выбран системный реестр, после создания ключевой информации не рекомендуется выполнять действия, затрагивающие системное ПО данного компьютера.

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

Примечание. В случае пересылки содержимого файла запроса посредством веб-интерфейса стороннего криптопровайдера откройте файл запроса в любом текстовом редакторе.

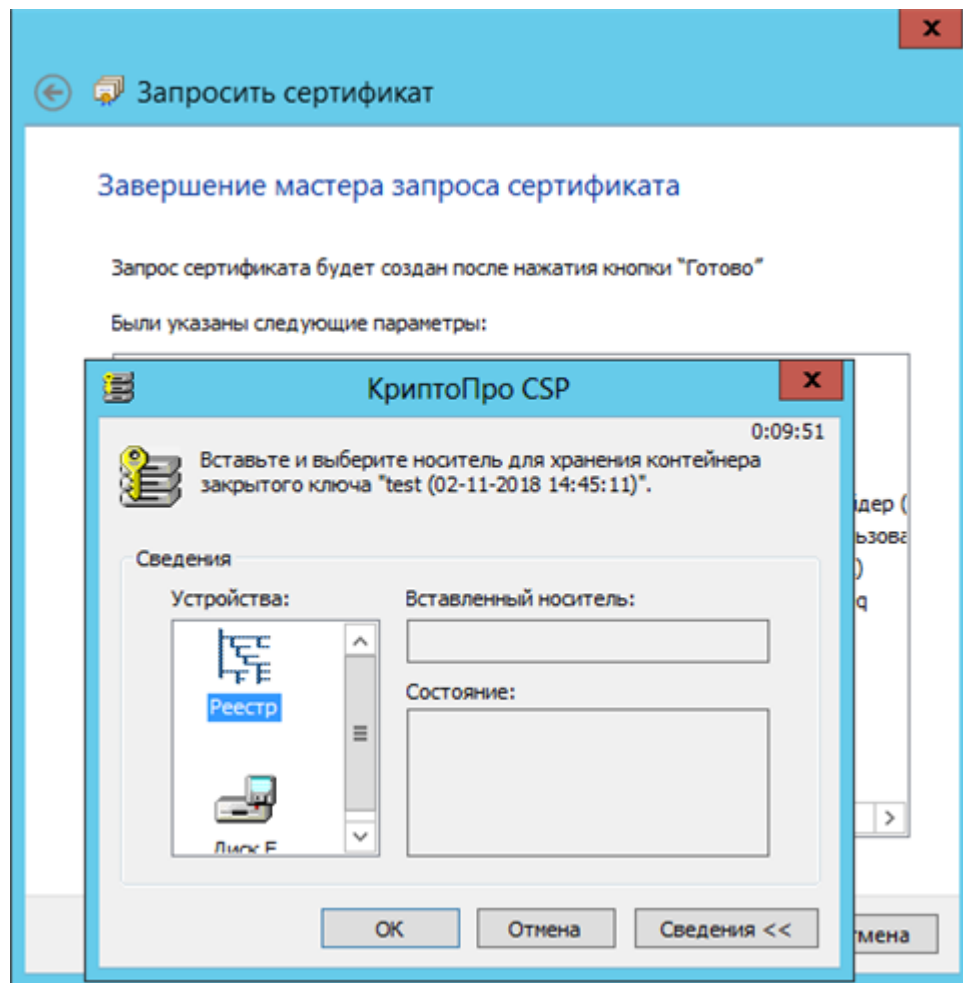
Варианты использования криптопровайдера при формировании закрытого ключа пользователя

Ниже приведены процедуры формирования закрытого ключа пользователя при создании запроса на получение сертификатов (см. стр. **17**). Представлены варианты использования криптопровайдеров "КриптоПро CSP" и "Код Безопасности CSP".

КриптоПро CSP

Для формирования закрытого ключа:

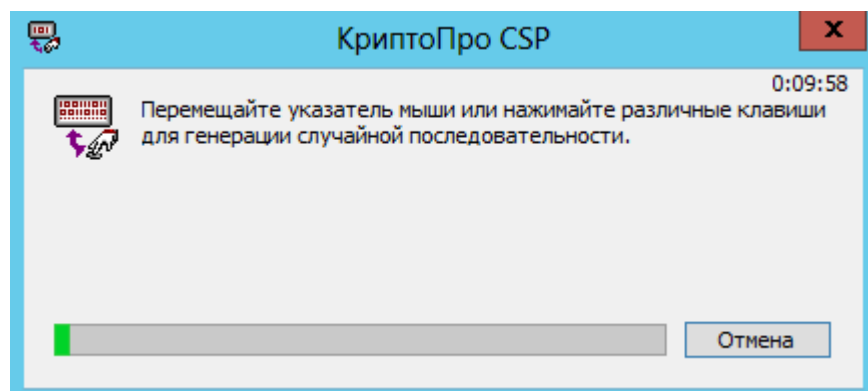
- 1.** После нажатия в окне завершения работы мастера запроса сертификата кнопки "Готово" на экране появится окно с указанием вставить чистый ключевой носитель.



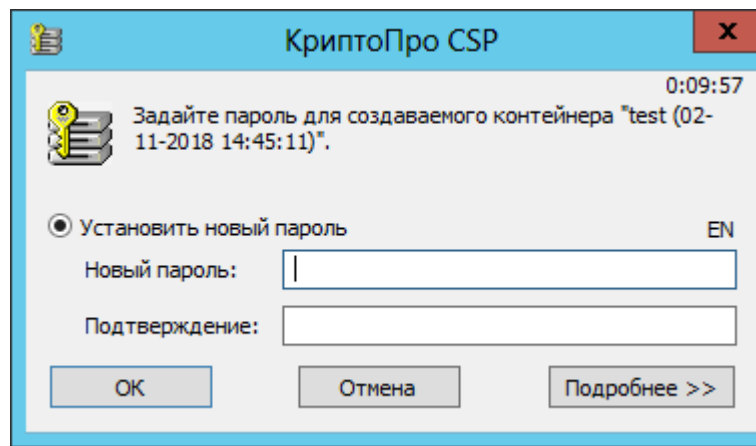
2. Вставьте носитель, нажмите кнопку "Сведения" и укажите устройство.
3. Нажмите кнопку "ОК".

На экране появится окно "Биологический датчик случайных чисел".

Примечание. Если в "КриптоПро CSP" настроен датчик случайных чисел ПАК "Соболь", на экране появится окно задания пароля для доступа к содержимому ключевого контейнера (см. п.4). Перейдите к выполнению п.5.



4. Следуйте инструкции на экране и дождитесь завершения создания ключа.
На экране появится окно задания пароля для доступа к содержимому ключевого контейнера.



5. Введите и подтвердите пароль на создаваемый ключевой контейнер и нажмите кнопку "ОК".

Начнется запись закрытого ключа пользователя на ключевой носитель, и после ее окончания на экране появится сообщение об успешном завершении создания запроса.

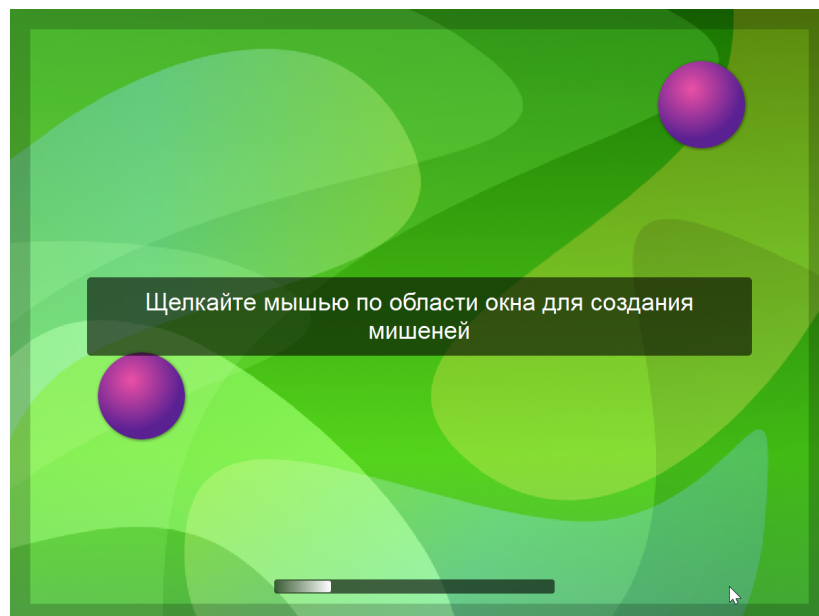
Код Безопасности CSP

Для формирования закрытого ключа:

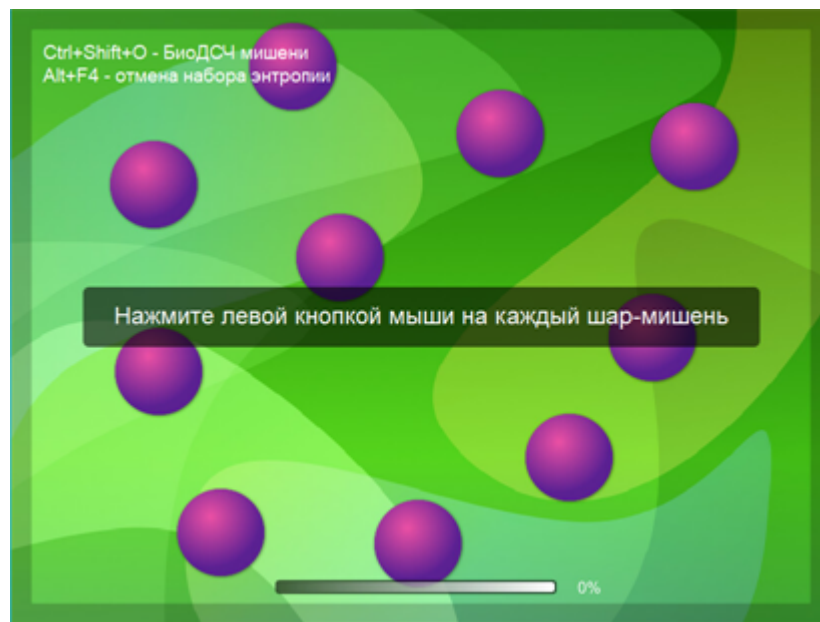
1. После нажатия в окне завершения работы мастера запроса сертификата кнопки "Готово" на экране появится окно накопления энтропии для биологического датчика случайных чисел.

Примечание. Если используется физический датчик случайных чисел ПАК "Соболь", набор энтропии выполняется автоматически и на экране не отображается. Вместо окна накопления энтропии появится окно задания пароля. Перейдите к п. 4.

2. Нажмите несколько раз в произвольном месте внутри открывшегося окна, чтобы появились шары-мишени.



3. Следуйте указаниям на экране и дождитесь завершения набора энтропии.

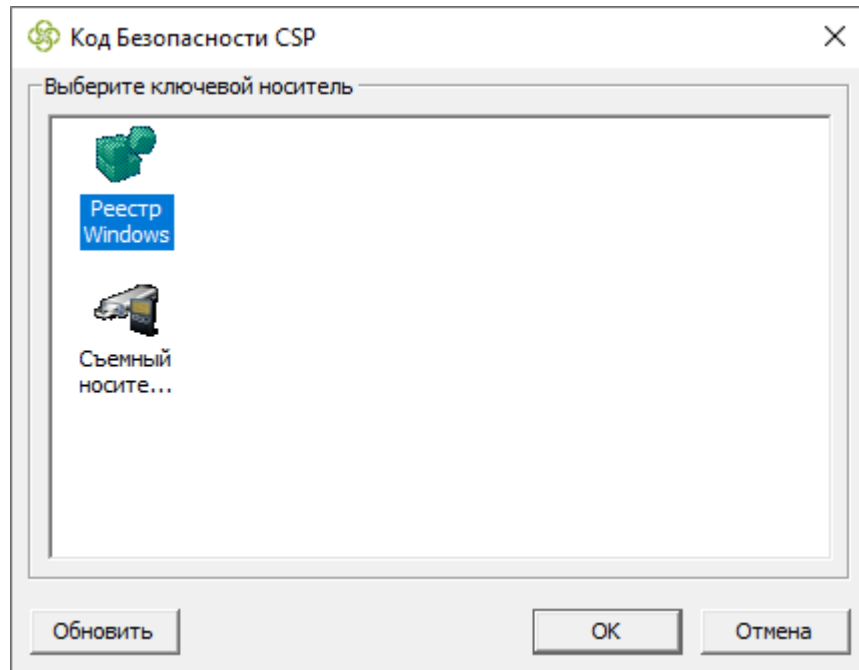


Примечание. Процесс накопления энтропии обозначается полосой прогресса внизу окна.

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

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

На экране появится окно выбора ключевого носителя.



5. Выберите нужный ключевой носитель и нажмите кнопку "ОК".

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

- файлы на USB-флеш-накопителе будут автоматически переименованы и сохранены;
- файлы на Рутокен будут перезаписаны с выводом запроса на выполнение операции.

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

6. Нажмите кнопку "ОК" и извлеките носитель.

Примечание. В случае пересылки содержимого файла запроса посредством веб-интерфейса стороннего криптопровайдера откройте файл запроса в любом текстовом редакторе.

Импорт сертификата

Для импорта корневого или пользовательского сертификата:

1. Выберите в главном меню TLS-клиента пункт "Управление сертификатами". В области отображения информации появится список установленных сертификатов.
2. На панели инструментов выберите пользовательский тип сертификатов и нажмите кнопку "Импортировать". На экране появится диалог настройки параметров импорта.

Имортируемый файл

Имя файла:

Обзор...

Замечание: сертификаты формата PKCS #7 (.p7b) могут содержать более одного сертификата.

Далее Отмена

Примечание. При использовании "КриптоПро CSP" на экране после нажатия кнопки "Имортировать" появится сообщение о необходимости воспользоваться сторонним криптопровайдером.

3. В поле "Имя файла" укажите полный путь и имя файла с расширением .cer или .p7b, содержащего нужный сертификат, и нажмите кнопку "Далее".

При импорте пользовательского сертификата появится окно запроса контейнера закрытого ключа сертификата. Выберите требуемый контейнер и нажмите кнопку "Далее".

На экране появится завершающий диалог мастера установки сертификата.

4. Проверьте корректность введенных параметров импорта и нажмите кнопку "Готово".

При импорте пользовательского сертификата появится окно запроса пароля к контейнеру закрытого ключа сертификата. Введите требуемый пароль и нажмите кнопку "ОК".

Начнется загрузка и установка сертификата в указанное хранилище. После успешного завершения операции на экране появится соответствующее информационное сообщение.

5. Нажмите кнопку "ОК".

Для импорта серверного сертификата:

1. Выберите в главном меню TLS-клиента пункт "Управление сертификатами".

В области отображения информации появится список установленных сертификатов.

2. На панели инструментов выберите нужную категорию и нажмите кнопку "Имортировать".

На экране появится стандартное окно открытия файла.

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

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

4. Нажмите кнопку "ОК".

Просмотр сведений о сертификате

Получить сведения о сертификате можно с помощью средств ОС Windows и СКЗИ "Континент TLS-клиент".

Для просмотра сертификата средствами ОС Windows и СКЗИ "Континент TLS-клиент":

1. Выберите в главном меню СКЗИ "Континент TLS- клиент" пункт "Сертификаты".
Откроется меню раздела "Сертификаты".
2. Нажмите кнопку "Открыть хранилище".
Откроется окно проводника ОС Windows со списком папок, в которых размещены сертификаты.
3. Откройте нужную папку и выберите сертификат.
4. Вызовите окно сведений о сертификате двойным щелчком левой кнопки мыши.
Откроется стандартное окно сведений о сертификате.

Для просмотра сертификата средствами СКЗИ "Континент TLS-клиент":

1. Выберите в главном меню СКЗИ "Континент TLS- клиент" пункт "Сертификаты", а затем вкладку с требуемым типом сертификатов на панели инструментов.
В области отображения информации появится список установленных сертификатов.
2. Вызовите окно сведений о сертификате двойным щелчком левой кнопки мыши по соответствующей строке списка установленных сертификатов.
Откроется стандартное окно сведений о сертификате.

Примечание. Экспорт сертификата можно выполнить средствами ОС Windows. Для этого перейдите в окне сведений о сертификате на вкладку "Состав" и нажмите кнопку "Копировать в файл..."

Управление CRL

Континент TLS-клиент позволяет в автоматическом или ручном режиме задавать CDP, при этом автоматически скачивая CRL для проверки валидности используемых сертификатов. Возможен и импорт CRL вручную.

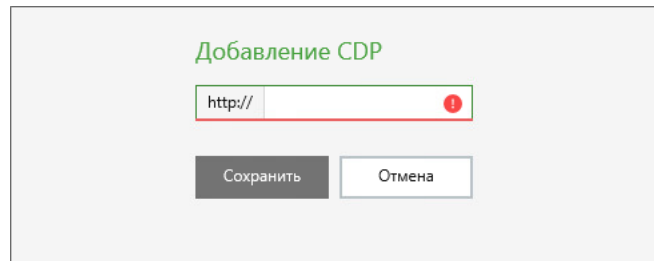
Настройка CDP

Если используемые сертификаты содержат информацию о CDP, СКЗИ "Континент TLS-клиент" получит ее при импорте сертификатов. Для автоматической загрузки CDP импортируйте корневой или серверный сертификат, как описано на стр. 26.

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

Для настройки списка CDP вручную:

1. Выберите в меню настроек СКЗИ "Континент TLS- клиент" пункт "Сертификаты", вкладку "CDP".
В области отображения информации основного окна появится список используемых CDP.
2. Нажмите кнопку "Добавить".
На экране появится окно для ввода URL CDP.



Добавление CDP

http:// !

Сохранить
Отмена

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

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

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

Загрузка CRL

Автоматическая загрузка CRL происходит следующими способами:

- в результате добавления CDP после импорта сертификатов;
- согласно расписанию, заданному в настройках ПО (см. стр. 31).

CRL может быть добавлен вручную следующими способами:

- импорт файла CRL;
- загрузка CRL из CDP (если он получен);
- импорт файла CRL с помощью средств ОС Windows.

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

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

Для импорта файла CRL:

1. Выберите в главном меню СКЗИ "Континент TLS-клиент" раздел "Управление сертификатами" и вкладку "CDP".

В области отображения информации появится список имеющихся CDP.

2. Нажмите кнопку "Импортировать CRL".

На экране появится стандартное окно открытия файла.

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

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

4. Нажмите кнопку "ОК".

Для загрузки файла CRL вручную:

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

В области отображения информации основного окна появится список CDP.

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

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

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

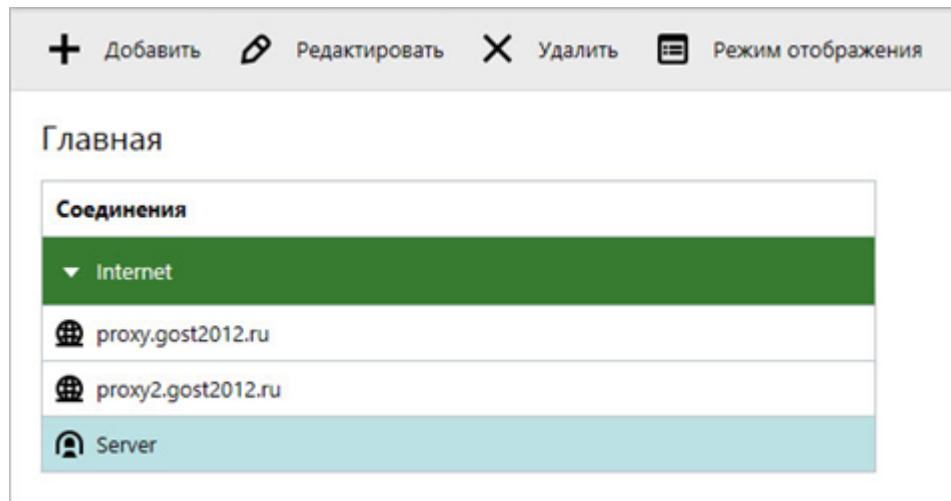
4. Нажмите кнопку "ОК".

Настройка соединений

В случае совместного использования с СКЗИ "Континент TLS VPN Сервер". Версия 1.2" необходимо создать и настроить соединение с ним и добавить доступные ресурсы (см. ниже).

В случае совместного использования с СКЗИ "Континент TLS- сервер". Версия 2" необходимо создать и настроить соединение с ним (см. ниже), получить или обновить список его ресурсов (см. стр. 30).

С помощью панели инструментов раздела пользователь может отредактировать или удалить ранее созданное соединение, а также выбрать вид отображения информации: список или таблица.



TLS-клиент осуществляет три типа соединений:

Тип	Обозначение	Класс
TLS-сервер	▶	Сервер
HTTPS-прокси	🌐	Ресурс
Туннель	👤	Ресурс

Для добавления нового соединения:

1. В основном меню TLS-клиента выберите пункт "Главная".
В области отображения информации откроется список имеющихся защищенных ресурсов и TLS-серверов (соединений).
2. Выберите закладку "+ Добавить" на панели инструментов, а затем нужный класс ("Сервер" или "Ресурс") в раскрывшемся списке.
В правой части области отображения информации основного окна появится соответствующий список настроек.
3. Введите необходимые параметры для настройки соединения и нажмите кнопку "Сохранить".

Внимание! Адреса серверов и ресурсов не могут быть заданы символами кириллицы.

4. Если необходимо добавить еще одно соединение, повторите пп. 2, 3.

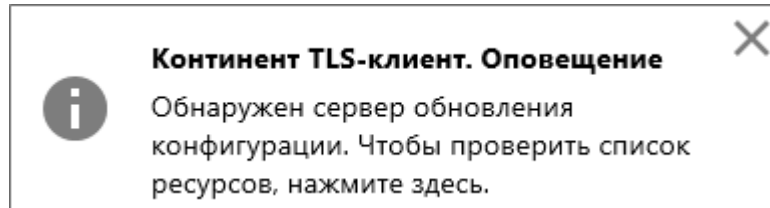
Для редактирования соединения:

1. Для внесения изменений в параметры соединения выберите его в списке соединений и нажмите кнопку "Редактировать" на панели инструментов.
В правой части области отображения информации основного окна появится список настроек соответствующего соединения.
2. Внесите необходимые изменения в параметры соединения и нажмите кнопку "Сохранить".

Для удаления соединения:

1. Для удаления соединения выберите его в списке соединений и нажмите кнопку "✕ Удалить" на панели инструментов.
2. Нажмите кнопку "Да" в появившемся окне подтверждения.

По умолчанию в настройках TLS-клиента установлено автоматическое обновление списка ресурсов сервера соединений (подробнее о настройках обновления ресурсов сервера см. стр. 37). Если в результате проверки список ресурсов сервера будет признан неактуальным, рядом с адресом сервера в списке соединений появится статус "список ресурсов неактуален". На экране появится информационное сообщение о наличии обновлений. Такое же сообщение появится при добавлении нового сервера в список соединений.

**Для получения или обновления списка ресурсов сервера:**

1. Нажмите на информационное сообщение в правом нижнем углу экрана.

Внимание! Если необходимо отменить обновление, нажмите ✕.

На экране появится окно выбора сертификата.

2. Выберите требуемый сертификат и нажмите кнопку "ОК".

На экране появится окно для ввода пароля для доступа к криптографическому контейнеру, если при создании контейнера не была выбрана опция "запомнить пароль".

3. Введите пароль и нажмите кнопку "ОК".

После удачного обновления на экране появится сообщение о том, что список ресурсов сервера обновлен. Посмотреть его можно, выбрав нужный сервер в списке соединений.

Режим упрощенного подключения

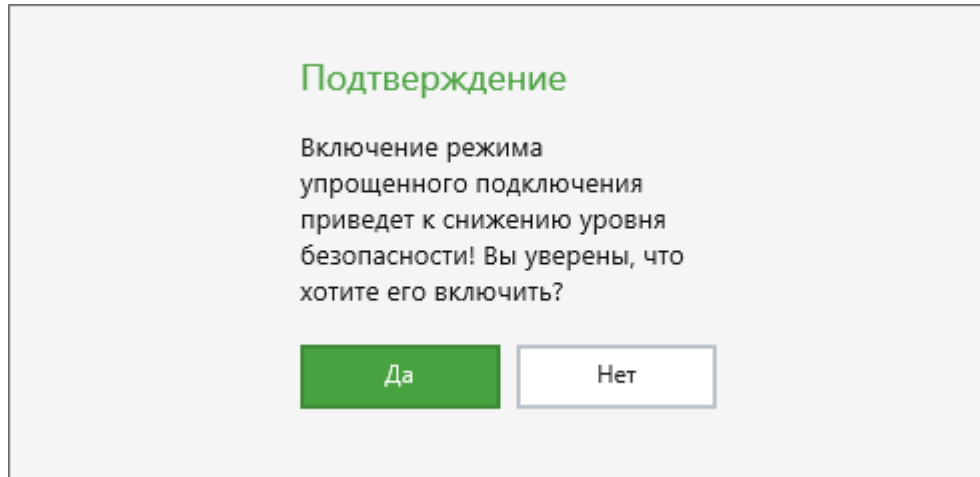
Режим упрощенного подключения позволяет пользователю устанавливать соединения с защищенными ресурсами при проблемах с серверными сертификатами (если включение данного режима допускает политика информационной безопасности компании).


По умолчанию режим упрощенного подключения отключен, а возможность его включения заблокирована. Возможность включения данного режима задается в основных настройках работы ПО TLS-клиента (см. стр. 32). При включении режима игнорируются настройки:

- "Запрашивать добавление других серверных сертификатов";
- "Проверять сертификаты по CRL";
- "Проверять подлинность сертификатов" (на странице сертификатов),

а также сроки действия сертификатов.

При попытке включения режима упрощенного подключения пользователь получит информационное сообщение о снижении уровня безопасности и запрос о подтверждении изменения режима работы.



После включения режима упрощенного подключения значок TLS-клиента на панели задач ОС Windows изменит вид на , предупреждая о том, что TLS-клиент работает в режиме упрощенного подключения

В обычном режиме работы TLS-клиент проверяет валидность серверных сертификатов. Если сертификат признан недействительным, соединение не устанавливается.

В режиме упрощенного подключения задача проверки на доверие получаемых серверных сертификатов возложена на пользователя.

При попытке подключения к защищенному ресурсу в режиме упрощенного подключения на экране появится окно с информацией о сертификате. TLS-клиент предложит пользователю **самостоятельно** определить степень доверия к сертификату. Если пользователь признает его доверенным, соединение с ресурсом будет установлено. Полученный сертификат будет добавлен в хранилище серверных сертификатов локального компьютера.

Для признания сертификата доверенным:

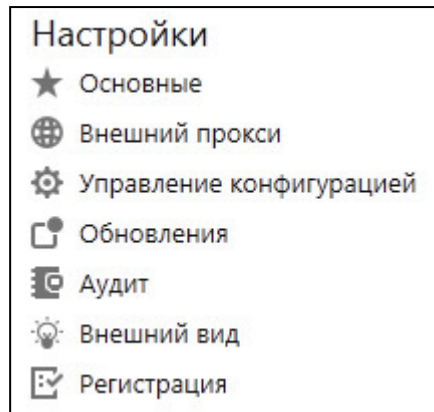
1. Включите режим упрощения соединения.
2. Начните попытку подключения к защищенному ресурсу. Если получаемый серверный сертификат невалиден, на экране появится сообщение с информацией о сертификате и предложение о признании его доверенным.
3. Если вы признаете сертификат доверенным, нажмите кнопку "Добавить".
Сертификат будет добавлен в хранилище серверных сертификатов, подключение будет установлено.
4. Если вы решите не доверять сертификату, нажмите кнопку "Отмена".
Установка подключения будет запрещена.

Настройка параметров работы TLS-клиента

ПО TLS-клиента позволяет:

- настраивать параметры работы ПО;
- осуществлять управление сертификатами;
- добавлять, редактировать и удалять соединения с ресурсами TLS-сервера.

Изменение параметров ПО TLS-клиента осуществляется через меню настроек, вызов которого происходит при выборе пункта "Настройки" в главном меню основного окна TLS-клиента.



Внимание! Для изменения настроек проксирования, обновлений и туннелируемых приложений TLS-клиент следует запускать от имени администратора (через контекстное меню).

Основные настройки

Для настройки TLS-клиента:

1. Выберите в меню настроек пункт "Основные".

В области отображения информации основного окна откроется соответствующее подменю.

Основные

Настройки сертификатов

Сертификат пользователя по умолчанию: ...

Предупреждать об истечении срока действия пользовательских сертификатов за дней

☒ Запрашивать добавление других серверных сертификатов

Настройки CRL

☒ Проверять сертификаты по CRL

Разрешить работу системы после истечения срока действия CRL в течение дней

☒ Скачивать CRL автоматически

Период скачивания CRL часов

Настройки проксирования

☒ Использовать непрозрачное проксирование

Порт:

☐ Самопроверка драйвера прозрачного проксирования

Настройки туннелируемых приложений

☐ Запускать туннелируемые приложения по ссылкам

☒ Уведомлять о запуске приложений

Режим запуска

☐ Запускать при старте системы

☐ При запуске свернуть в системный трей

Настройки работы приложения


☒ Подтверждать сброс соединений

Настройки подключения

Протокол TLS:

☐ Настроить параметры шифроработ

☐ Режим упрощенного подключения

2. Для автоматической аутентификации при подключении к TLS-серверу под определенным пользователем следует указать его сертификат, нажав кнопку . В противном случае переходите к п. 4.

Примечание. Если планируется подключение к ресурсам нескольких серверов, использовать данную настройку не рекомендуется.

На экране появится окно для выбора сертификата.

3. Укажите нужный сертификат и нажмите кнопку "ОК".

Примечание. Если сертификат пользователя, выбранный для подключения по умолчанию, станет недействительным, при попытке подключения появится сообщение о невозможности использования данного сертификата, а само подключение установлено не будет. Имя невалидного сертификата и его статус будут отображаться в разделе "Управление сертификатами", на вкладке "Пользовательские сертификаты". Для установления подключения выберите новый сертификат по умолчанию, как описано выше.

4. Выберите период для старта получения предупреждения об истечении срока действия сертификата пользователя.
5. Если политика информационной безопасности компании позволяет получение по сети серверных сертификатов информационных ресурсов, установите отметку в поле "Запрашивать добавление других серверных сертификатов".

Внимание! Настройка данного параметра игнорируется при работе в режиме упрощенного соединения.

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

Внимание! Настройка данного параметра игнорируется при работе в режиме упрощенного соединения.

7. Для настройки периода автоматического обновления сертификата CRL установите флажок "Скачивать CRL автоматически" и укажите нужный период в соответствующем поле.
8. В случае использования непрозрачного режима TLS-клиента установите отметку в поле "Использовать непрозрачное проксирование" и укажите выделяемый для этого порт (подробнее о настройках прокси см. стр. 34).
9. Для включения самотестирования прозрачного режима проксирования при старте TLS-клиента поставьте соответствующую отметку (по умолчанию процедура отключена).
10. Для разрешения автоматического запуска туннелируемых приложений по гиперссылкам установите соответствующую отметку.
11. Настройте режим запуска ПО TLS-клиента при старте системы (по умолчанию включено).
12. Выберите режим отображения ПО после запуска (по умолчанию выключено). В обычном режиме открывается основное окно TLS-клиента и появляется значок в панели задач ОС Windows. Если настройка активирована, главное окно интерфейса при запуске открываться не будет.
13. Для получения предупреждающего сообщения о сбросе всех установленных соединений установите отметку в поле "Подтверждать сброс соединений".

Примечание. В таком случае при выборе в контекстном меню TLS-клиента команды "Сброс соединений" на экране появится сообщение о необходимости подтверждения команды. Для сброса соединений нажмите кнопку "Да", для возврата к работе нажмите кнопку "Нет".

14. Для включения, в случае необходимости, режима упрощенного подключения поставьте отметку в соответствующее поле (подробнее о режиме подключенного соединения см. стр. 30). По умолчанию режим выключен, а настройка заблокирована.

Внимание! Для внесения изменений в данную настройку необходимо перезапустить TLS-клиент от имени администратора.

15. Для сохранения выполненных настроек нажмите кнопку "Сохранить".

Настройки прокси

Непрозрачное проксирование

Использование непрозрачного прокси-сервера дает возможность модифицировать запрос и/или ответы пользователя.

Если политика информационной безопасности вашей организации предусматривает непрозрачное проксирование, необходимо настроить параметры работы прокси-сервера в этом режиме.

Для использования непрозрачного копирования:

1. Запустите TLS-клиент от имени администратора и перейдите в раздел "Основные настройки".
2. Поставьте отметку в поле "Использовать непрозрачное проксирование"
3. Укажите выделяемый для этого порт.

Внимание! Порт непрозрачного режима — уникальный параметр, который необходимо вводить для каждого пользователя заново. При входе под учетной записью другого пользователя непрозрачный режим, несмотря на проставленную отметку, будет недоступен до тех пор, пока пользователь не укажет свой индивидуальный порт.

4. Перейдите в основное окно TLS-клиента и выберите нужное соединение из списка.

Откроется дополнительное окно настройки параметров соединения.

5. Если в качестве типа соединения с ресурсом выбран прокси, в настройках интернет-браузера укажите localhost в качестве адреса HTTP- и SSL-прокси-сервера, а также пропишите тот же порт.

Примечание. При использовании интернет-браузера Firefox для корректной работы в режиме непрозрачного проксирования необходимо импортировать корневой сертификат ContinentTLSClientRoot, находящийся в хранилище доверенных корневых центров сертификации, в хранилище сертификатов Firefox.

6. Если в качестве типа соединения с ресурсом выбран туннель, в адресной строке интернет-браузера укажите в качестве адреса 127.0.0.1 и номер локального порта (например, 127.0.0.1:2000). В случае подключения пользователя с помощью удаленного рабочего стола адрес необходимо вводить в адресную строку окна вызова удаленного рабочего стола.

Внимание! Номер локального порта при соединении в режиме туннеля — уникальный параметр, который необходимо вводить для каждого соединения отдельно.

Внешний прокси

Для настройки подключения к интернету через внешний прокси-сервер вручную:

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

В области отображения информации основного окна отобразится соответствующий список настроек.

Внешний прокси

☐ Настраивать автоматически
 ☒ Использовать внешний прокси-сервер

Адрес:

Порт:

Исключения (адреса разделяются ";"):

Аутентификация:

Автоматический выбор

☐ Использовать учетные данные текущего пользователя для авторизации

Сброс пароля

СБРОСИТЬ

2. Установите отметку в поле "Использовать внешний прокси-сервер".
3. В поле "Адрес" введите IP-адрес или имя прокси-сервера. В поле "Порт" — порт для подключения к прокси-серверу.
4. Выберите способ аутентификации и заполните соответствующие данные.
5. Разрешите, поставив отметку в соответствующем поле, использовать учетные данные текущего пользователя для авторизации (если это допускает политика информационной безопасности вашей компании).
6. При необходимости укажите список исключений (перечень IP-адресов или сетевых имен, разделенных символом ";").
7. Для завершения настройки и применения введенных или исправленных значений параметров нажмите кнопку "Сохранить".

Для автоматической настройки подключения к интернету через внешний прокси-сервер:

1. Выберите в меню настроек пункт "Внешний прокси".
В области отображения информации основного окна отобразится соответствующий список настроек.
2. Установите отметку в поле "Настраивать автоматически".

3. TLS-клиент применит для настройки параметров прокси-сервера существующие настройки браузера автоматически.

Примечание. Список ресурсов будет автоматически помещен в исключения в системных настройках браузера. В остальных полях графического интерфейса пользователя появятся значения, сохраненные в системных настройках.

4. Разрешите, поставив отметку в соответствующем поле, использовать учетные данные текущего пользователя для авторизации (если это допускает политика информационной безопасности вашей компании).
5. Для применения настройки нажмите кнопку "Сохранить".

В настройках внешнего прокси-сервера предусмотрена возможность сброса текущего пароля для доступа к прокси-серверу.

Для сброса пароля к прокси-серверу:

1. Нажмите кнопку "Сбросить".
2. Нажмите кнопку "Да" в появившемся окне подтверждения.

При следующем подключении к удаленным ресурсам прокси-сервер потребует ввода нового пароля, который пользователь предварительно должен будет получить от администратора.

Управление конфигурацией

Настройками TLS-клиента предусмотрена возможность импорта/экспорта конфигурации настроек в виде файла с расширением *.json (далее — настроечный файл).

Внимание! При импорте/экспорте конфигурации настроек корневые, серверные сертификаты и сертификат пользователя не переносятся. Их, при необходимости, нужно импортировать/экспортировать отдельно.

Настроечный файл содержит в себе параметры для настройки работы ПО. Он также может включать в себя регистрационные данные и список ресурсов для создания защищенного соединения.

Настройки, содержащиеся в файле, заменяют имеющиеся настройки работы TLS-клиента и вступают в действие немедленно после успешного импорта настроечного файла.

Внимание! Настройки, которые были определены пользователем, имеющим права администратора заменены не будут. Для применения всех настроек настроечного файла перед импортом конфигурации запустите TLS-клиент от имени администратора.

Мастер установки TLS-клиента предоставляет возможность использования настроечного файла для облегчения настройки работы ПО. Для этого получите от администратора безопасности настроечный файл, сохраните его на своем локальном компьютере и укажите в настройках мастера установки TLS-клиента путь к его месту расположения.

Внимание! Использование настроечного файла при установке ПО TLS-клиента возможно исключительно в рамках одной версии СКЗИ.

Начнется процесс установки и инициализации ПО. Настройки, указанные в настроечном файле, вступят в силу при первом запуске TLS-клиента.

Пример настроечного файла приведен в приложении на стр. [47](#).

Для экспорта конфигурации TLS-клиента:

1. Перейдите в меню настроек в раздел "Управление конфигурацией" и выберите опцию "Экспортировать конфигурацию".
Откроется окно проводника ОС Windows.
2. Укажите место хранения и название файла архива и нажмите кнопку "Сохранить".
Появится сообщение об успешном завершении экспорта.
3. Нажмите кнопку "ОК", чтобы вернуться в раздел "Управление конфигурацией".

Для импорта конфигурации TLS-клиента:

1. Перейдите в меню настроек в раздел "Управление конфигурацией" и выберите опцию "Импортировать конфигурацию".
Появится сообщение о том, что запуск импорта конфигурации приведет к изменению текущих настроек, и запрос подтверждения операции.
2. Для отмены импорта конфигурации и возврата в раздел "Управление конфигурацией" нажмите кнопку "Нет". В противном случае перейдите к п. 3.
3. Для продолжения импорта конфигурации нажмите кнопку "Да".
Откроется окно проводника ОС Windows.
4. Выберите нужный конфигурационный файл и нажмите кнопку "Открыть".
Появится сообщение об успешном завершении импорта.
5. Нажмите кнопку "ОК", чтобы вернуться в раздел "Управление конфигурацией".

Настройки обновления

Настройки обновления ПО

TLS-клиент позволяет автоматически проверять наличие обновлений ПО, хранящихся на TLS-сервере, а также скачивать и производить установку по запросу пользователя.

Внимание! Для управления настройками обновления и ручной проверки обновления требуется запустить TLS-клиент от имени администратора.

Для настройки обновления ПО:

1. Выберите в меню настроек TLS-клиента пункт "Обновления".
Откроется список настроек:

Обновления

☐ Автоматически проверять наличие актуальных обновлений ПО

☒ Автоматически проверять наличие обновлений списка ресурсов

Адрес сервера обновлений ПО

Ручное обновление ПО

ПРОВЕРИТЬ

Ручное обновление списка ресурсов

ПРОВЕРИТЬ

Дополнительные настройки

Интервал между проверками (час.):

1

Тайм-аут соединения (сек.):

120

Количество попыток загрузки:

3

Папка для загрузки обновлений:

C:\Users\Admin\AppData\Roam...

Сохранить

Отменить

2. Для настройки параметров обновления:

- Введите имя сервера обновлений.

Примечание. Наличие обновлений может проверить любой пользователь, для загрузки обновлений требуется аутентификация по сертификату, а для их установки — права локального администратора.

- Для принудительной проверки наличия обновлений нажмите кнопку "Проверить".
- При необходимости пропишите параметры автоматического обновления в подразделе дополнительных настроек.

3. Для завершения настройки нажмите кнопку "Сохранить".

Обновление списка ресурсов на TLS-серверах

TLS-клиент позволяет проверять наличие обновлений ресурсов сервера, с которым настроено соединение.

Для настройки обновления ресурсов сервера:

1. Выберите в меню настроек TLS-клиента пункт "Обновления".

Откроется список настроек. Отметка в поле "Автоматически проверять наличие обновлений списка ресурсов" установлена по умолчанию.


Примечание. Поиск наличия обновления проводится при каждом запуске графического интерфейса пользователя.

О порядке получения обновлений при автоматическом получении обновлений списка ресурсов сервера см. стр. 30.

2. При необходимости провести принудительную проверку нажмите кнопку "Проверить" для ручного обновления списка ресурсов.

Если обновления не были обнаружены, на экране появится соответствующее сообщение. При наличии обновлений появится сообщение о наличии обновлений конфигурации.

3. Нажмите на сообщение.

Внимание! Если необходимо отменить обновление, нажмите .

На экране появится окно выбора сертификата.

4. Выберите требуемый сертификат и нажмите кнопку "ОК".

Внимание! Если в списке соединений указан один сервер, для которого будут выполняться проверки списка ресурсов, то в основных настройках можно выбрать сертификат пользователя по умолчанию. Если в списке соединений несколько серверов и для каждого необходим индивидуальный сертификат, применять данную опцию не рекомендуется. При наличии обновлений следует выбирать из списка индивидуальный сертификат для каждого сервера.

На экране появится окно для ввода пароля для доступа к криптографическому контейнеру, если при создании контейнера не была выбрана опция "запомнить пароль".

5. Введите пароль и нажмите кнопку "ОК".

После удачного обновления на экране появится сообщение о том, что список ресурсов сервера обновлен. Посмотреть его можно, выбрав нужный сервер в списке соединений.

Аудит

Настройки аудита позволяют управлять порядком записи системных событий и лог-файлов, а также просматривать журналы событий — как сохраненные на локальном компьютере пользователя, так и экспортированные.

Внимание! Для активации возможности просмотра журнала событий требуется запуск TLS-клиента от имени администратора.

Для просмотра журнала событий:

1. Выберите в меню настроек в раздел "Аудит".
Откроется вкладка настроек параметров аудита.
2. Откройте "Журнал".
Откроется системный журнал ОС Windows.
3. Выберите нужный журнал.
На экране появится список событий.
4. Выберите нужную запись и в контекстном меню выбранной записи активируйте команду "Свойства".

На экране появится окно, в котором содержится информация о событии.

Сбор диагностической информации происходит с помощью соответствующей утилиты.

Для изменения параметров аудита:

1. Выберите в меню настроек раздел "Аудит".
Откроется вкладка настроек параметров аудита.
2. Установите режим работы расширенного логирования, поставив или убрав отметку в соответствующем поле.

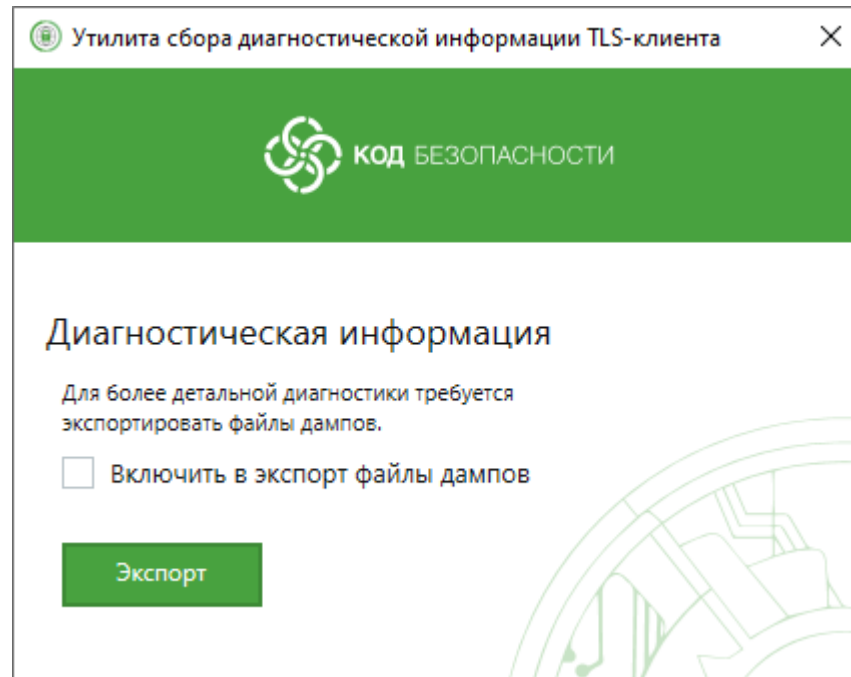
3. Установите режим записи логов рабочей сессии в системный журнал, поставив или убрав отметку в соответствующем поле.
4. Нажмите кнопку "Сохранить".

Примечание. После включения режима расширенного логирования потребуется перезагрузить TLS-клиент.

Для сбора диагностической информации:

1. Нажмите кнопку "Пуск" и выберите в главном меню ОС Windows пункт "Все приложения | Код Безопасности | TLS-клиент | Сбор диагностической информации".

Появится предложение об экспорте диагностической информации.



Примечание. Для включения в сборку файлов дампов поставьте отметку в соответствующее поле.

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

2. Нажмите кнопку "Экспорт".
На экране появится окно для работы с файловой системой.
3. Укажите место хранения и название файла архива и нажмите кнопку "Сохранить".
В случае успешного сохранения файла появится соответствующее сообщение.

Внешний вид

Для настройки вида интерфейса TLS-клиента:

1. Выберите в меню настроек пункт "Внешний вид".
В области отображения информации основного окна появится соответствующий список настроек.
2. Выберите тему оформления.

Эксплуатация TLS-клиента

Доступ к защищенным ресурсам

Для доступа к защищенному ресурсу:

Внимание! Если для доступа к защищенному ресурсу требуется аутентификация по сертификату, подключите внешний носитель с ключевой информацией.

1. Запустите веб-браузер (или консоль подключения к удаленному рабочему столу) и в адресной строке введите адрес защищенного ресурса.

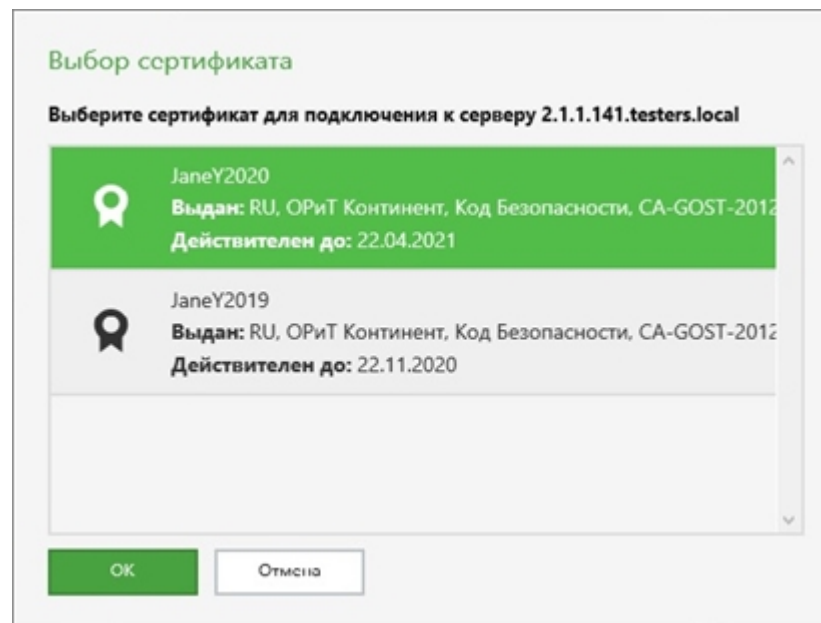
Для подключения к защищенным ресурсам в веб-браузере рекомендуется использовать протокол HTTP, но допустимо также использовать протокол HTTPS. Протокол, указанный в браузере, не влияет на защищенное соединение между TLS-клиентом и сервером.

Внимание! При установленном туннеле необходимо в веб-обозревателе задавать тот же протокол, который используется на защищенном веб-сервере.

Пример: `https://172.20.20.7` или `https://SRV` или `http://192.168.47.1:4444`.

Примечание. В случае использования сетевого имени ресурса вместо его адреса необходимо осуществить соответствующую настройку DNS-сервера или файла hosts. После внесения изменений в файл hosts необходимо перезапустить приложение TLS-клиента.

Если не установлен сертификат по умолчанию (см. п. 2 процедуры настройки параметров TLS-клиента на стр. 33), на экране появится окно выбора сертификата пользователя.



В диалоге отображается список установленных сертификатов.

2. Выберите сертификат пользователя и нажмите кнопку "OK".
3. Если на экране появится окно ввода пароля доступа к ключевому контейнеру — введите его и нажмите кнопку "OK".

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

Диалог выбора сертификата закрывается, и будет установлено защищенное соединение с указанным ресурсом.

Примечание. Во время сессии настройки ОС Windows или самого ресурса могут потребовать дополнительно ввести и логин пользователя для доступа в интернет. В случае появления на экране окна для введения логина и пароля действуйте в соответствии с политикой информационной безопасности вашей компании.

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

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

Контроль целостности

КЦ установленного ПО осуществляется в начале работы TLS-клиента, в ходе регламентных проверок с периодичностью, заданной в настройках УКЦ, а также вручную, с помощью УКЦ.

Внимание! Для изменения настроек контроля целостности требуется запуск TLS-клиента от имени администратора.

Для запуска УКЦ:

- Выберите в главном меню ОС Windows пункт "Все приложения | Код Безопасности | Контроль целостности TLS-клиента".

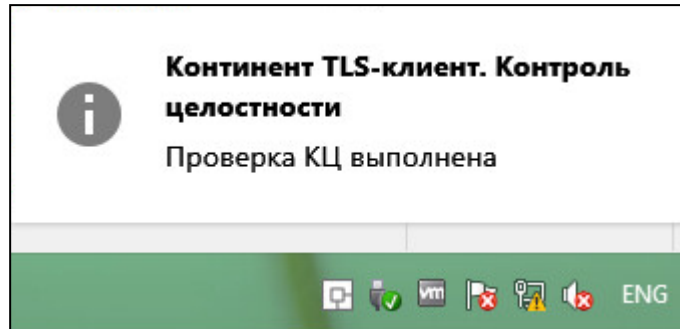
Проверка начнется автоматически, и на экране появится основное окно утилиты с результатом проверки.

Контроль целостности TLS-клиент	
☰	
<div> <div>🔍</div> <div>Выполнить КЦ</div> <div>🔍</div> <div>Выполнить КЦ эталонного ПО</div> <div>Σ</div> <div>Пересчитать контрольные суммы</div> </div>	
<div> <div>📄</div> <div>СПИСОК МОДУЛЕЙ TLS-КЛИЕНТА</div> <div>📄</div> <div>СПИСОК МОДУЛЕЙ ОС</div> </div>	
Название файла	статус
CspAssistTlsUI.dll	✓
CspCertTls.dll	✓
LogCollectorTlsClient.exe	✓
RegistrationTlsClient.exe	✓
TlsClient.exe	✓
GUIIntegrityController.exe	✓
IntegrityController.exe	✓
GostEngine.dll	✓
CertificateChainVerification.dll	✓
libssl-1_1-x64.dll	✓
libcrypto-1_1-x64.dll	✓
openssl.cnf	✓
scCertImRu.msc	✓
MobyDickTestClient.exe	✓
sciter.dll	✓
UpdateInstaller.exe	✓
MobyDickManager8.exe	✓

Для выполнения контроля целостности системных файлов ПО TLS-клиента:

- В основном окне УКЦ выберите на панели инструментов пункт "Выполнить КЦ".

Будет выполнена пофайловая процедура контроля целостности списка модулей TLS-клиента и ОС. В ходе ее выполнения проверенные файлы на экране будут отмечены знаком ✓. После успешного завершения процедуры на экране появится следующее информационное окно:




Если в ходе проверки будет обнаружена ошибка КЦ, неверный файл будет отмечен знаком !. Для исправления ошибки восстановите ПО из дистрибутива (см. стр. 11).

Для выполнения контроля целостности файлов дистрибутива ПО TLS-клиента:

1. В основном окне УКЦ выберите на панели инструментов команду "Выполнить КЦ эталонного ПО".

На экране появится окно открытия каталога дистрибутива.

2. Укажите путь к файлам дистрибутива, нажав кнопку .

Будет выполнена пофайловая процедура контроля целостности дистрибутива. После ее успешного завершения на экране появится соответствующее информационное окно.

Для пересчета контрольных сумм системных файлов ОС Windows:

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


На экране появится окно подтверждения действия.

2. Нажмите кнопку "Да".

Будет выполнен пофайловый пересчет контрольных сумм списка модулей СКЗИ "Континент TLS-клиент" и ОС. В ходе выполнения процедуры на экране будут отмечаться знаком ✓ соответствующие файлы. После ее успешного завершения на экране появится информационное окно.



Для настройки расписания регламентных проверок:

1. В основном окне УКЦ выберите в главном меню пункт вызова настроек .

Внимание! Для изменения расписания регламентных проверок требуется запуск УКЦ от имени администратора.

На экране появится текущее расписание регламентных проверок.

Расписание проверок контроля целостности


Начало в ч. мин.

Дни недели:

☐ Пн ☐ Вт ☐ Ср ☐ Чт ☐ Пт ☐ Сб ☒ Вс

2. Укажите время и дни, в которые нужно проводить регламентные проверки.
3. Нажмите кнопку "Сохранить".
Будет выполнено изменение настроек УКЦ, после чего на экране появится соответствующее информационное окно.
4. Нажмите кнопку "ОК".
5. По умолчанию функция контроля установленного на компьютере пользователя ПО отключена. Утилита активируется, если того требует политика информационной безопасности организации.

Для контроля установленного программного обеспечения:

1. В основном окне УКЦ выберите в главном меню пункт вызова подутилиты .

На экране появится окно настроек контроля установленного ПО.

Контроль целостности TLS-клиент

Контроль установленного программного обеспечения

☐ Производить контроль установленного программного обеспечения

Список программного обеспечения:

Программное обеспечение	Состояние	Проверка
Secret Net Studio версии 8.4 и новее	×	<input type="checkbox"/>
ПАК «Соболь» версии 3.0 и новее	×	<input type="checkbox"/>
Антивирусное ПО	×	<input type="checkbox"/>

2. Активируйте контроль установленного ПО, поставив отметку в соответствующем поле.
3. Отметьте в списке ПО, подлежащее проверке.

Внимание! Чтобы добавить ПО в список, укажите его в файле настроек УКЦ. Для добавления ПО необходимо запустить TLS-клиент от имени администратора. После добавления ПО в файл настроек оно появится в списке.

Приложение

Требования к сертификатам

Устанавливаемые серверный сертификат и сертификат пользователя должны иметь определенную структуру и отвечать ряду требований.

Структура и содержание серверного сертификата

Для получения серверного сертификата администратор должен сформировать запрос и отправить его в удостоверяющий центр. Параметры запрашиваемого сертификата предварительно настроены и подставляются автоматически при создании запроса.

Внимание! Проверкой актуальности серверного сертификата занимается клиент.

В таблице ниже приведены общие характеристики свойств серверного сертификата.

Табл.1 Структура и содержание серверного сертификата

№ п/п	Параметр	Описание	Значение
Базовые поля сертификата			
1.1	Version	Версия	V3
1.2	Serial Number	Серийный номер	Уникальный серийный номер сертификата
1.3	Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.10–2012
1.4	Issuer	Издатель сертификата, Поставщик	CN = Имя центра сертификации. O = Организация. C = Страна/Регион. E = Электронная почта
1.5	Valid from	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс GMT
1.6	Valid to	Срок действия сертификата	Действителен по: дд.мм.гггг чч:мм:сс GMT
1.7	Subject	Владелец сертификата	CN = Имя сервера. OU = Подразделение. O = Организация. C = Страна/Регион (задается двумя латинскими буквами). E = Электронная почта
1.8	Public Key	Открытый ключ	Открытый ключ в соответствии с алгоритмом ГОСТ Р 34.10–2012 (512 Bits)
Дополнения сертификата			
2.1	Basic Constraints	Основные ограничения	Тип субъекта=Конечный субъект. Ограничение на длину пути=отсутствует
2.2	Key Usage	Использование ключа	Согласование ключа или цифровая подпись
2.3	Extended Key Usage	Улучшенный ключ	Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
2.4	CRL Distribution Point	Точка распространения списка отозванных сертификатов	URL=http://www.test.ru/test.crl

Структура и содержание сертификата пользователя

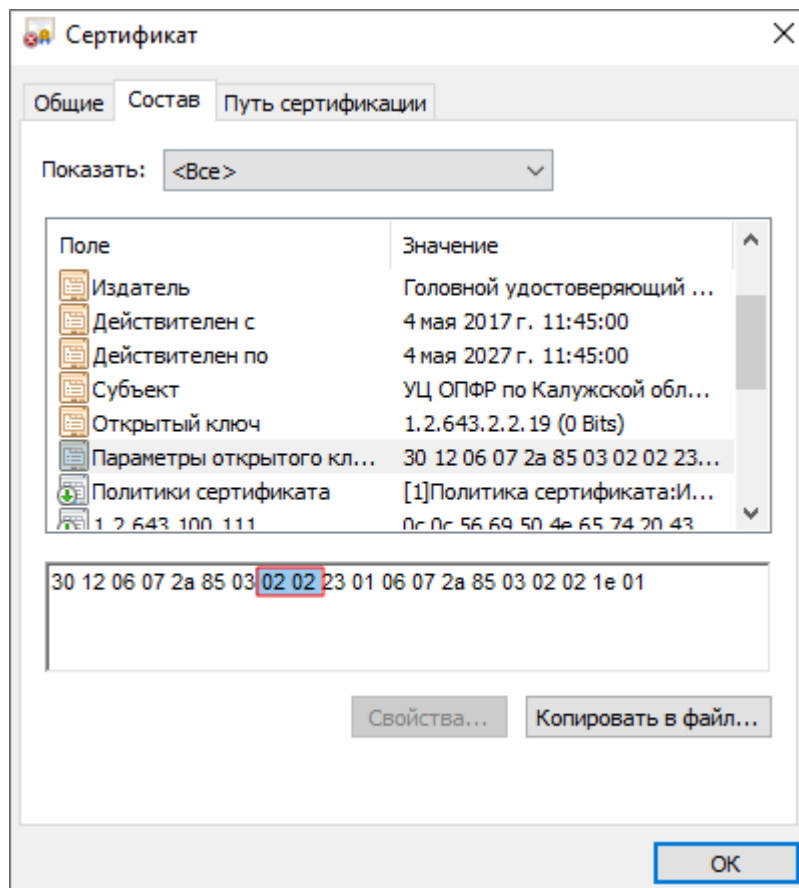
Валидность сертификата пользователя проверяется сервером.

В таблице ниже приведены общие характеристики свойств сертификата пользователя.

Табл.2 Структура и содержание сертификата пользователя

№ п/п	Параметр	Описание	Значение
Базовые поля сертификата			
1.1	Version	Версия	V3
1.2	Serial Number	Серийный номер	Уникальный серийный номер сертификата
1.3	Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.10–2012
1.4	Issuer	Издатель сертификата, Поставщик	CN = Имя центра сертификации. O = Организация. C = Страна/Регион. E = Электронная почта
1.5	Valid from	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс GMT
1.6	Valid to	Срок действия сертификата	Действителен по: дд.мм.гггг чч:мм:сс GMT
1.7	Subject	Владелец сертификата	CN = ФИО. OU = Подразделение. O = Организация. C = Страна/Регион (задается двумя латинскими буквами). E = Электронная почта
1.8	Public Key	Открытый ключ	Открытый ключ в соответствии с алгоритмом ГОСТ Р 34.10–2012 (512 Bits)
Дополнения сертификата			
2.1	Basic Constraints	Основные ограничения	Тип субъекта=Конечный субъект. Ограничение на длину пути=отсутствует
2.2	Key Usage	Использование ключа	Согласование ключа, или цифровая подпись, или зашифрование ключа
2.3	Extended Key Usage	Улучшенный ключ	Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
2.4	CRL Distribution Point	Точка распространения списка отозванных сертификатов	URL=http://www.test.ru/test.crl

При работе со сторонними провайдерами TLS-клиент поддерживает работу только с ключами, созданными с использованием параметров 1.2.643.2.2.35.1, 1.2.643.2.2.35.2, 1.2.643.2.2.35.3, 1.2.643.2.2.36.0, 1.2.643.2.2.36.1. Для проверки валидности сертификата откройте диалог просмотра свойств сертификата. Перейдите на вкладку "Состав" и выберите поле "Параметры открытого ключа". Убедитесь, что восьмой и девятый байты слева имеют значение "02".



Если значения не совпадают, создайте запрос на другой сертификат или получите новый сертификат из внешних источников.

Пример настроечного файла

```
{
  "GlobalConfig": {
    "configVersion": 1,
    "transparentMode": true,
    "tunnelingApplicationNotification": true,
    "updaterConfig": {
      "autoCheckConfigUpdates": true,
      "autoCheckSoftUpdates": false,
      "downloadTimeout": 120,
      "numberOfAttempts": 3,
      "updateDirectory":
        "C:\\Users\\User\\AppData\\Roaming\\ContinentTLSClient",
      "updateHost": "",
      "updatePeriod": 1
    }
  },
  "PublicConfig": {
    "configVersion": 1,
    "loggingConfig": {
      "fileLogMaxSize": 3145728,
      "fileLoggingDirectory":
        "C:\\Users\\Public\\ContinentTLSClient\\",
      "fileLoggingEnabled": true,
      "logLevel": 2,
      "sessionLogsEnabled": true
    }
  }
}
```

```

"servers": [
{
"host": "172.17.117.121",
"isConfigActual": true,
"name": "172.17.117.121",
"tlsServerId": 6
}
],
"tlsProtocolCode": "1_0_OR_1_2"
},
"RegistrationNumberConfig": {
"configVersion": 1,
"registrationNumber": ""
},
"RegistrationUserInfo": {
"city": "Москва",
"configVersion": 1,
"department": "Отдел",
"email": "primer@primer.ru",
"firstName": "Имя",
"host": "registration.securitycode.ru",
"lastName": "Фамилия",
"middleName": "Отчество",
"organization": "Код Безопасности",
"protectionClass": "kcl"
},
"RegistryConfig": {
"runAtStartup": false,
"uriRegistered": false
},
"UserConfig": {
"certWarnExpirationDays": 14,
"checkServerCertFingerprint": false,
"configVersion": 1,
"crlAutoUpdate": true,
"crlNextUpdateExpirationDays": 0,
"crlUpdatePeriod": 12,
"defaultCertificateSerial": "20 9f ec 1d 00 00 00 00 05 2b",
"defaultCertificateSubject": "user2-2012",
"externalProxyConfig": {
"authMethod": "Auto",
"exceptions": "",
"host": "proxy.ru",
"port": 5555,
"useProxy": false,
"useWinSessionCredentials": false
},
"importCertRequested": true,
"lowSecurityMode": false,
"performMobyDickTest": false,
"proxyPort": 15197,
"resources": [
{
"host": "tls.srv.testers.local",
"hostForHandshake": "tls.srv.testers.local",
"id": 8,
"isStartPage": false,
"name": "tls.srv.testers.local",
"tlsServerId": 0
}
],

```



```

{
  "host": "reg.2012.testers.local",
  "hostForHandshake": "reg.2012.testers.local",
  "id": 12,
  "isStartPage": false,
  "name": "reg.2012.testers.local",
  "tlsServerId": 0
},
{
  "host": "192.168.100.199",
  "hostForHandshake": "192.168.100.199",
  "id": 18,
  "isStartPage": false,
  "name": "192.168.100.199",
  "tlsServerId": 0
},
{
  "host": "c.2012.testers.local",
  "hostForHandshake": "c.2012.testers.local",
  "id": 19,
  "isStartPage": false,
  "name": "c.2012.testers.local",
  "tlsServerId": 6
},
{
  "host": "a.2012.testers.local",
  "hostForHandshake": "a.2012.testers.local",
  "id": 20,
  "isStartPage": false,
  "name": "a.2012.testers.local",
  "tlsServerId": 6
},
{
  "host": "192.168.100.119",
  "hostForHandshake": "192.168.100.119",
  "id": 21,
  "isStartPage": false,
  "name": "192.168.100.119",
  "tlsServerId": 6
},
{
  "host": "172.17.116.176",
  "hostForHandshake": "172.17.116.176",
  "id": 22,
  "isStartPage": false,
  "name": "172.17.116.176",
  "tlsServerId": 6
},
{
  "host": "startpage.2012.testers.local",
  "hostForHandshake": "startpage.2012.testers.local",
  "id": 23,
  "isStartPage": false,
  "name": "startpage.2012.testers.local",
  "tlsServerId": 6
}
],
"tunnels": [
{
  "host": "t1.tun.testers.local",

```

```

"hostForHandshake": "t1.tun.testers.local",
"id": 1,
"isStartPage": false,
"localPort": 2000,
"name": "t1.tun.testers.local",
"remotePort": 3389,
"tlsServerId": 6
},
{
"host": "t2.tun.testers.local",
"hostForHandshake": "t2.tun.testers.local",
"id": 2,
"isStartPage": false,
"localPort": 2001,
"name": "t2.tun.testers.local",
"remotePort": 3390,
"tlsServerId": 6
},
{
"host": "t3.tun.testers.local",
"hostForHandshake": "t3.tun.testers.local",
"id": 3,
"isStartPage": false,
"localPort": 2002,
"name": "t3.tun.testers.local",
"remotePort": 3391,
"tlsServerId": 6
}
],
"uiConfig": {
"runMinimized": false,
"uiTheme": "light-theme"
},
"updateUserInfo": [
{
"hashConfig": "39c747ac1d6abcee0798c3e93b194bd7d50ed490",
"tlsServerId": 6,
"updateCertName": "user2-2012"
}
],
"useAutoProxyIEConfig": false,
"useCrl": true
}
}

```

Список регистрируемых событий

Ниже приведен список событий, связанных с работой TLS-клиента и регистрируемых в журнале ОС Windows. Для просмотра зарегистрированных событий пользователь должен входить в группу локальных администраторов компьютера.

Событие
Продукт: Континент TLS-клиент -- Установка завершена успешно
Продукт: Континент TLS-клиент -- Удаление завершено успешно
Осуществлен запуск TLS-клиента
TLS-клиент остановлен
Произошла системная ошибка: %сообщение%

*Установлено соединение с защищенным ресурсом: %имя ресурса%
*Разорвано соединение с защищенным ресурсом: %имя ресурса%
Защищенный сервер не прошел аутентификацию. Причина %причина%
Сервер отказал в аутентификации
Сервер разорвал соединение на этапе аутентификации
Инициализация процедуры проверки целостности файлов выполнена успешно. Количество контролируемых файлов: %число%
Ошибка инициализации процедуры проверки целостности файлов. Требуется переустановка TLS-клиента
Проверка целостности файлов выполнена успешно
Нарушена целостность файлов. Создание новых сессий запрещено
Выполнен перерасчет контрольной суммы файла %имя_файла%
Сертификат сервера добавлен в хранилище. Кем выдан: %имя%. Кому выдан: %имя%. Серийный номер: %номер%
Сертификат сервера был удален. Кем выдан: %имя%. Кому выдан: %имя%. Серийный номер: %номер%
Добавление защищенного ресурса: %имя%
Удаление защищенного ресурса: %имя%
CRL импортирован в систему. Издатель: %имя%

Примечание. События с символом * регистрируются только при включенной опции "Записывать логи сессии в системный журнал" в настройках аудита.