

127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
<https://CryptoPro.ru>
E-mail: info@CryptoPro.ru



Средство

Криптографической

Защиты

Информации

КриптоПро CSP

Версия 5.0 R2 KC1

Исполнение 1-Base

Инструкция по использованию JavaTLS

ЖТЯИ.00101-02 92 05
Листов 14

© ООО «КРИПТО-ПРО», 2000-2021. Все права защищены.

Авторские права на средство криптографической защиты информации КриптоПро CSP и эксплуатационную документацию к нему зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент). Документ входит в комплект поставки программного обеспечения СКЗИ КриптоПро CSP версии 5.0 R2 КС1; на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО «КРИПТО-ПРО» документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

Содержание

Список сокращений 4

1 Установка КриптоПро JavaTLS 6

 1.1 Ввод серийного номера лицензии 8

2 Контрольная панель 10

 2.1 Закладка «Сервер JTLS» 10

 2.2 Закладка «Настройки TLS» 11

3 Настройка параметров провайдера с помощью Preferences 13

Список определений и сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск (Hard Disk Drive)
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
Регистрация	Присвоение определенных атрибутов (адреса, номера ключа, прав использования и т.п.) абоненту
Регламент	Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах
СВТ	Средства вычислительной техники
Сертификат	Электронный документ, подтверждающий принадлежность открытого ключа или ключа проверки электронной подписи и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата открытого ключа или ключа проверки электронной подписи абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей и ключей проверки электронной подписи. Сетевой справочник
СФК	Среда функционирования комплекса
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ЭД	Электронный документ
ЭП	Электронная подпись

Аннотация

Настоящая Инструкция содержит описание процесса установки, настройки и использования КриптоПро JavaTLS (JTLS), входящего в состав средства криптографической защиты информации «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base.

Модуль КриптоПро JavaTLS предоставляет доступ к реализациям протоколов SSL и TLS в соответствии с российскими криптографическими алгоритмами и функционирует под управлением виртуальной Java-машины.

Основные функции, реализуемые КриптоПро JavaTLS:

- две схемы аутентификации с использованием обмена ключей по схеме Диффи-Хэллмана и хэширования в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 — односторонняя (анонимный клиент, аутентифицируемый сервер) и двухсторонняя (аутентифицируемые клиент и сервер);
- в случае аутентификации клиента на ключе подписи применяются алгоритмы выработки и проверки электронной подписи в соответствии с ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012;
- шифрование соединения в соответствии с ГОСТ 28147-89;
- имитозащита передаваемых данных в соответствии с ГОСТ 28147-89.

1 Установка КриптоПро JavaTLS

В случае использования Java-машин версии 10 и выше:

Установка модуля КриптоПро JavaTLS не требуется, функционал провайдера будет доступен после добавления модуля в classpath.

Эксплуатация осуществляется путем добавления провайдера в список java.security:

```
security.provider.<N>=JTLS
```

В случае использования Java-машин версии 1.7 или 1.8:

Для установки КриптоПро JavaTLS на ПЭВМ с установленной Java-машиной версии 1.7 или 1.8 следуйте описанной ниже инструкции.

Перед тем, как приступить к установке КриптоПро JavaTLS, необходимо установить криптопровайдер КриптоПро JavaCSP, включая модули шифрования.

Установка модуля КриптоПро JavaTLS может быть выполнена с помощью графического (setup.exe, setup_gui.sh) или консольного (setup_console.bat, setup_console.sh) инсталляторов.

Установка модуля КриптоПро JavaTLS с помощью командной строки возможна в интерактивном (с участием пользователя) и тихом (без взаимодействия с пользователем) режимах. Для запуска установки в интерактивном режиме необходимо выполнить следующую команду с правами администратора из папки с инсталлятором: `setup_console.bat <путь_к_JRE>`

В процессе установки пользователем пошагово указываются необходимые данные. Для установки модуля КриптоПро JavaTLS в окне установщика на этапе выбора продуктов необходимо указать «TLS провайдер».

Для установки в тихом режиме используются дополнительные параметры командной строки, например (setup_console.bat -help):

1) установка JCP (с модулем шифрования) и модуля JTLS (cpSSL) в C:\Program Files\Java\jre7:

```
setup_console.bat "C:\Program Files\Java\jre7" -force -ru -install -jre "C:\Program Files\Java\jre7" -jcp -jcryptop -cpssl
```

2) дополнительная установка к уже установленному JCP модуля JTLS в JRE по умолчанию (текущая исполняемая JRE) с указанием серийного номера для JTLS:

```
setup_console.bat "C:\Program Files\Java\jre7" -force -ru -install -cpssl -sslserial  
XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

Установка модуля КриптоПро JavaTLS также может быть выполнена с помощью графического установщика setup.exe. Процесс установки КриптоПро JavaTLS аналогичен процессу установки КриптоПро JCP или КриптоПро JavaCSP с единственным уточнением — для установки модуля JTLS в окне выбора продуктов инсталлятора необходимо установить флаг в поле TLS провайдер (см. [рис. 1](#)).

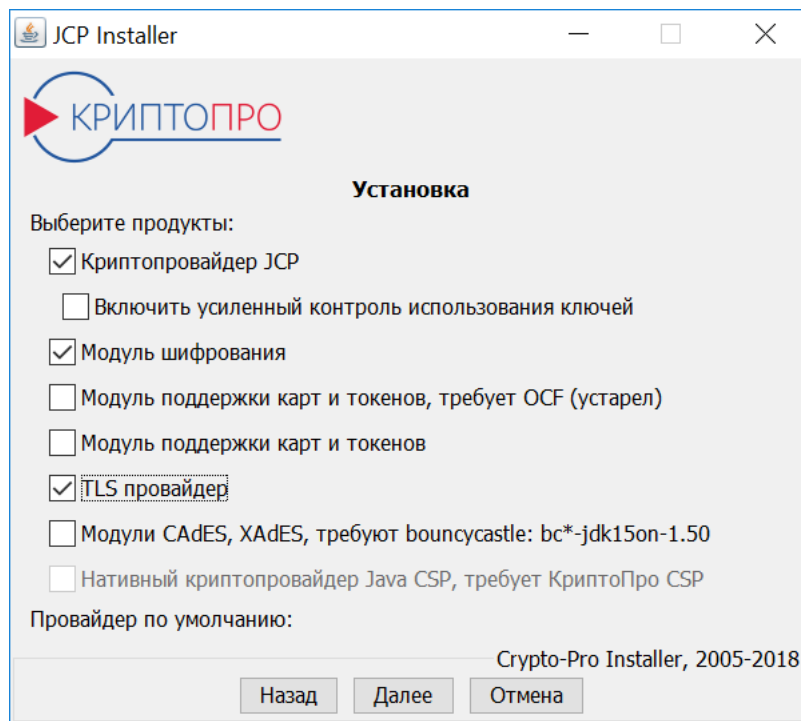


Рисунок 1. Установка модуля КриптоПро JavaTLS

На следующем этапе установки будет предложено ввести номер лицензии для КриптоПро JavaTLS в соответствующее поле (см. [рис. 2](#)).

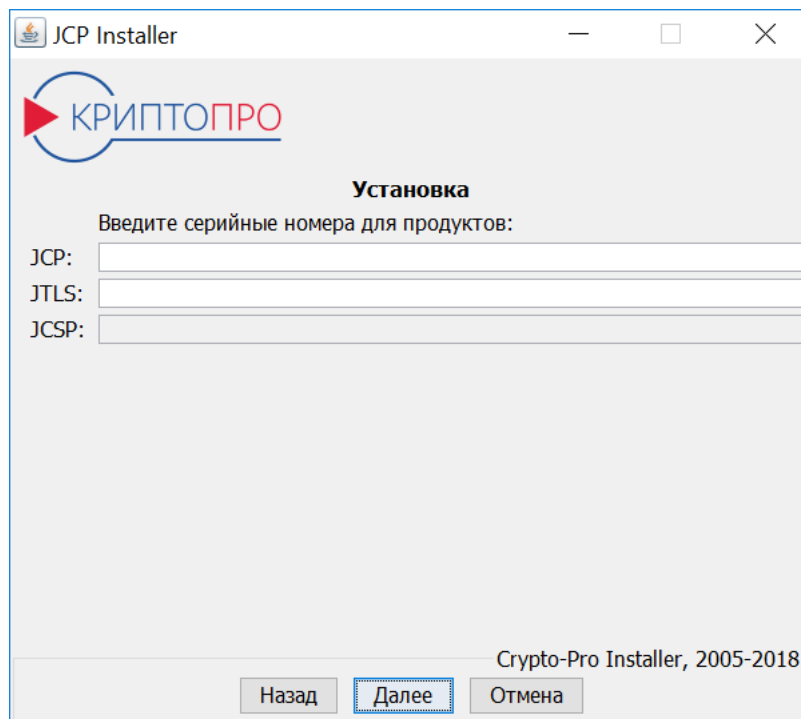


Рисунок 2. Ввод лицензии КриптоПро JavaTLS

Если номер лицензии не указан на этапе установки, то будут использованы серийные номера по умолчанию сроком действия 3 месяца. Номер лицензии также можно ввести после установки с помощью контрольной панели или командной строки (см. [разд. 1.1](#)).

Установка может осуществляться через вызов программы Java. Для запуска программы установки необходимо вызвать Java с именем jar-файла, например:

```
<JRE>/bin/java -jar cpSSL.jar
```

Также возможна установка с вводом серийного номера с помощью класса ru.CryptoPro.ssl.JTLSInstall:

```
<JRE>/bin/java -cp cpSSL.jar ru.CryptoPro.ssl.JTLSInstall -install -verbose -sslserial  
XXXXXX-XXXXX-XXXXX-XXXXX-XXXXX -sslcompany "My Company"
```



Примечание. Процесс установки КриптоПро JavaTLS во многом совпадает с процессом установки модуля КриптоПро JavaCSP. Для получения подробной информации по видам установки, описания дополнительных параметров инсталлятора и пошагового процесса установки продуктов см. инструкцию по использованию КриптоПро JCP или КриптоПро JavaCSP, входящую в комплект эксплуатационной документации на СКЗИ.

1.1 Ввод серийного номера лицензии

Для работы с лицензией КриптоПро JavaTLS можно использовать контрольную панель (закладка **Сервер JTLS**) или командную строку (класс ru.CryptoPro.ssl.ServerLicense).

Минимальные требования к лицензии для данной системы указаны на контрольной панели, также их можно узнать из командной строки:

```
ru.CryptoPro.ssl.ServerLicense -required
```

Ввод лицензии осуществляется вызовом класса ru.CryptoPro.JCSP.JCSPLicense с параметрами:

```
ru.CryptoPro.ssl.ServerLicense -serial "serial_number" -company "company_name" -store
```

Также можно проверить заданную лицензию без ее установки:

```
ru.CryptoPro.ssl.ServerLicense -serial "serial_number" -company "company_name"
```

Вызов класса ru.CryptoPro.ssl.ServerLicense без параметров проверит установленную лицензию.

Дату первой установки можно узнать с помощью команды:

```
ru.CryptoPro.ssl.ServerLicense -first
```

Для вывода справки используйте команду:

```
ru.CryptoPro.ssl.ServerLicense ?
```

Для ввода лицензии КриптоПро JavaTLS с помощью контрольной панели откройте закладку **Сервер JTLS** и нажмите кнопку **Ввод лицензии**. В открывшемся окне введите имя пользователя, название организации и серийный номер продукта (см. [рис. 3](#)).

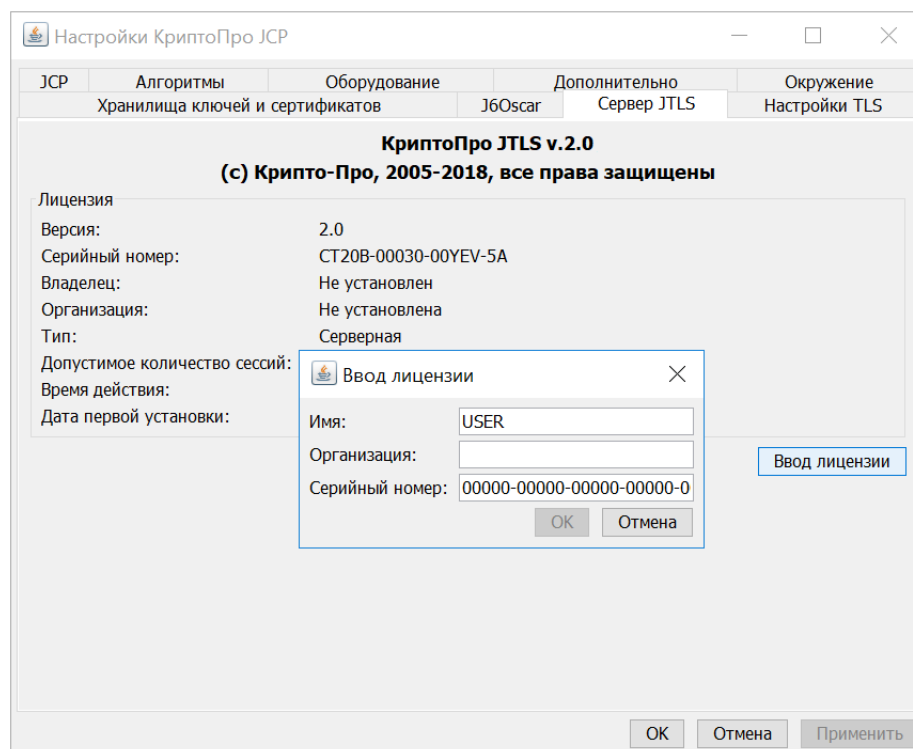


Рисунок 3. Ввод лицензии КриптоПро JavaTLS с помощью контрольной панели

2 Контрольная панель

Основной набор закладок контрольной панели описан в Инструкции по использованию КриптоПро JCP. Дополнительные закладки, устанавливаемые КриптоПро JavaCSP, описаны в ЖТЯИ.00101-02 92 05. КриптоПро CSP. Инструкции по использованию JavaCSP.

После установки модуля КриптоПро JavaTLS на контрольной панели появятся закладки:

- Сервер JTLS;
- Настройки TLS.

2.1 Закладка «Сервер JTLS»

Закладка «Сервер JTLS» (см. [рис. 4](#)) предназначена для просмотра информации о текущей лицензии на использование продукта КриптоПро JavaTLS, а также для установки новой лицензии.

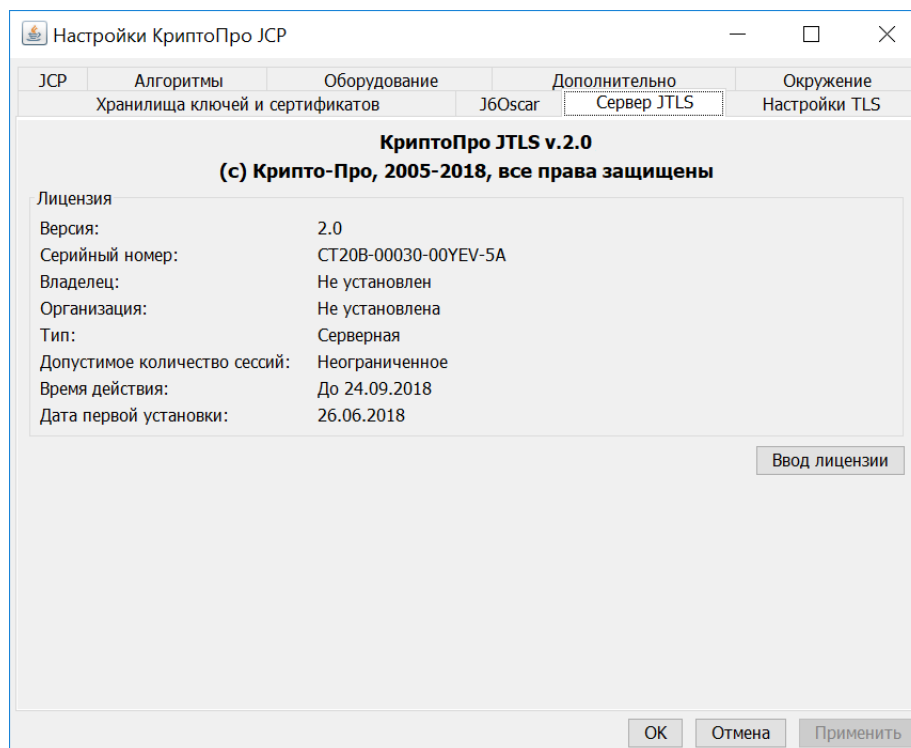


Рисунок 4. Закладка «Сервер JTLS»

При установке модуля КриптоПро JavaTLS без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования КриптоПро JavaTLS после окончания этого срока пользователь должен ввести серийный номер с бланка Лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (дилера). Для ввода лицензии нажмите кнопку Ввод лицензии и заполните соответствующее поле в открывшемся окне (подробнее [разд. 1.1](#)).

Внимание! Лицензия будет сохранена только после нажатия кнопок «ОК» или «Применить».

В случае использования JTLS (срSSL) совместно с JavaCSP на сервере помимо серверной лицензии для срSSL потребуется также серверная лицензия JavaCSP и серверная лицензия CSP.

Закладка «Сервер JTLS» содержит следующую информацию:

- версия КриптоПро JavaTLS;

- серийный номер лицензии на использование КриптоПро JavaTLS;
- имя владельца лицензии;
- организация, к которой относится владелец;
- тип лицензии;
- допустимое число сессий для данной лицензии;
- время действия лицензии;
- дата первой установки.

2.2 Закладка «Настройки TLS»

Закладка «Настройки TLS» (см. [рис. 5](#)) предназначена для просмотра и изменения настроек протокола TLS, реализуемого модулем КриптоПро JavaTLS.

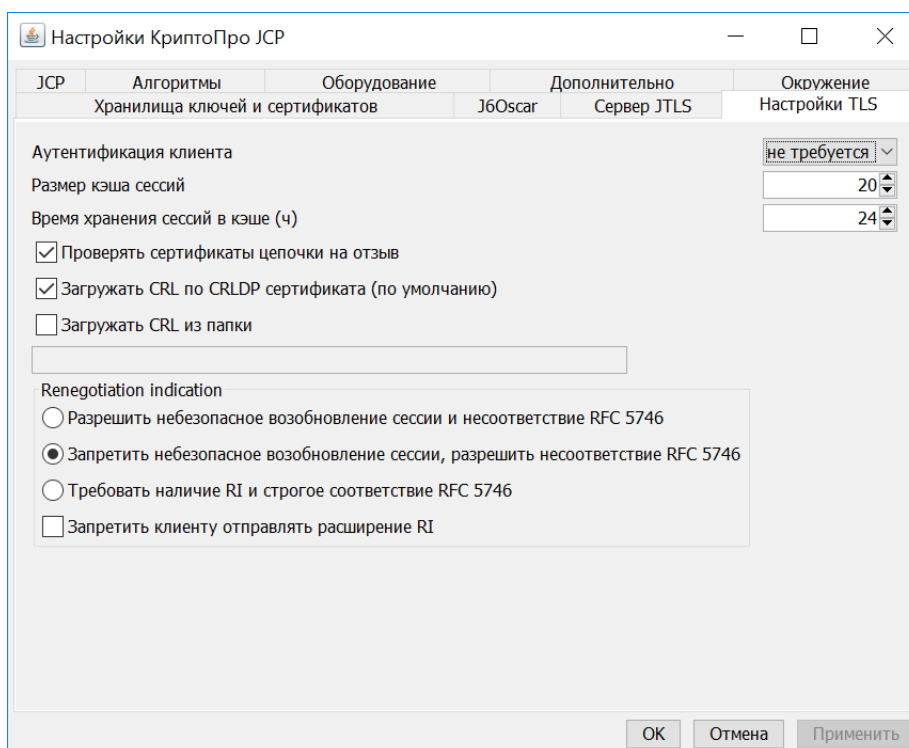


Рисунок 5. Закладка «Настройки TLS»

С помощью закладки устанавливаются следующие настройки сервера:

- необходимость аутентификации клиента (по умолчанию не требуется);
- размер кэша сессий (количество сессий; по умолчанию 0 — неограниченное);
- время хранения сессий в кэше (по умолчанию 24 часа; если размер кэша сессий не задан (=0), то старые сессии удаляться не будут);
- возможность полного отключения проверки цепочки сертификатов на отзыв, включение проверки с условием загрузки СОС из сети по CRLDP сертификата, включение проверки с условием загрузки СОС из папки (задается абсолютный путь к папке с СОС);
- отключение, включение и требование поддержки расширения Renegotiation Indication (RFC 5746). Задание данных настроек с помощью параметров `Dru.CryptoPro.ssl.allowUnsafeRenegotiation=<value>` и `Dru.CryptoPro.ssl.allowLegacyHelloMessages=<value>` в приложении имеет более высокий приоритет и переопределяет настройки JTLS. Пары указанных свойств образуют следующие группы (см. [табл. 1](#));
- возможность отправки клиентом расширения Renegotiation Indication (по умолчанию разрешено).

Таблица 1. Режимы поддержки Renegotiation Indication (RFC 5746)

Режим	Allow Legacy Hello Messages	Allow Unsafe Renegotiation	Аналогия с КриптоПро CSP TLS
Строгий (strict)	false	false	Требуем RFC 5746: наличие RI обязательно, проверка выполняется
Безопасный (interoperable)	true (SUN/Oracle default)	false	Поддерживаем RFC 5746 (по умолчанию в КриптоПро CSP версий 4.0, 5.0): наличие RI необязательно, проверка может выполняться
Небезопасный (insecure)	true	true	Не поддерживаем RFC 5746 (по умолчанию в КриптоПро CSP версий 4.0, 5.0): наличие RI необязательно, проверка не выполняется

3 Настройка параметров провайдера с помощью Preferences

В некоторых случаях может потребоваться настройка КриптоПро JavaTLS путем редактирования параметров провайдера, хранящихся в Preferences.

Доступ к ним преимущественно можно получить тремя способами:

- программно, с помощью `Preferences.systemRoot()` или `Preferences.userRoot()`, перечисления путей к узлам и задания новых значений;
- вручную, редактируя параметры в соответствующих разделах (`SOFTWARE\JavaSoft\Prefs\ru` или `SOFTWARE\Wow6432Node\JavaSoft\Prefs\ru` компьютера `HKEY_LOCAL_MACHINE` или пользователя `HKEY_CURRENT_USER`) реестра ОС Windows или файлы вида `prefs.xml` в соответствующих папках `.systemPrefs/ru` (например, `/etc/.java/.systemPrefs/ru`) или `.userPrefs (/home/user/.userPrefs/ru)` ОС *nix;

- с помощью класса `ru.CryptoPro.JCP.Util.SetPrefs`, находящегося в модуле JCP и предоставляющего возможности для добавления и редактирования, например:

```
java ru.CryptoPro.JCP.Util.SetPrefs -user -node ru/CryptoPro/ssl -key cpSSL_any_param
-value any_value
```

```
java ru.CryptoPro.JCP.Util.SetPrefs -system -node ru/CryptoPro/ssl -key cpSSL_any_param
-value any_value
```

Таблица 2. Основные параметры КриптоПро JavaTLS

Описание	Путь	Ключ	Соответствует
Путь к папке CRL	ru/CryptoPro/ssl	CRL_location_default	Закладка «Настройки TLS», загрузка CRL из папки
Аутентификация клиента, число (0-2)	ru/CryptoPro/ssl	Client_auth_default	Закладка «Настройки TLS», аутентификация клиента
Проверка цепочки сертификатов на отзыв, true или false	ru/CryptoPro/ssl	Enable_revocation_default	Закладка «Настройки TLS», проверка цепочки сертификатов на отзыв
Проверка цепочки сертификатов на отзыв, true или false	ru/CryptoPro/ssl	Enable_CRL_revocation_online_default	Закладка «Настройки TLS», проверка цепочки сертификатов на отзыв путем обращения в сеть
Проверка цепочки сертификатов на отзыв, true или false	ru/CryptoPro/ssl	Enable_CRL_revocation_offline_default	Закладка «Настройки TLS», проверка цепочки сертификатов на отзыв путем обращения к папке
Запрет для клиента отправлять расширение Renegotiation Indication, true или false	ru/CryptoPro/ssl	disable_client_ri	Закладка «Настройки TLS», запрет для клиента отправлять расширение Renegotiation Indication

Размер кеша сессий, число	ru/CryptoPro/ssl	Session_cache_size_default	Закладка «Настройки TLS», размер кеша сессий
Время хранения сессий в кеше, часы	ru/CryptoPro/ssl	Session_time_default	Закладка «Настройки TLS», время хранения сессий в кеше
Алгоритм работы с Renegotiation Indication, число (0-2)	ru/CryptoPro/ssl	RI_support	Закладка «Настройки TLS», Renegotiation Indication
Разрешение использовать сертификат другой стороны для выработки сессионного ключа. По умолчанию отключено.	ru/CryptoPro/ssl	tls_client_fixed_dh_allowed	Нет параметра в панели JCP
Добавление длины подписи в сообщение CertificateVerify. По умолчанию включено.	ru/CryptoPro/ssl	tls_client_strict_certificate_verify	Нет параметра в панели JCP
Запрет на отключение ряда проверок, которые выполняются при установлении соединения. Данный параметр включен по умолчанию и контролирует: 1) не отключена ли проверка соответствия CN/AlternativeName в сертификате (сервера) и ip-адреса/имени хоста, к которому производится подключение; 2) не отключена ли проверка цепочки сертификатов другой стороны; 3) входит ли для cрSSL провайдер подписи/шифрования по умолчанию в список допустимых провайдеров - JCP, Crypto или JCSP 4) все ли открытые ключи в цепочке сертификатов другой стороны имеют ГОСТ алгоритм.	ru/CryptoPro/ssl	tls_prohibit_disabled_validation	Нет параметра в панели JCP