127 018, Москва, Сущевский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро JTLS

Версия 2.0

Инструкция по использованию

ЖТЯИ.00091-01 91 02

Листов 7

2016 г.

Оглавление

1. Введение

«КриптоПро JTLS» версия 2.0 является программным комплексом защиты информации, разработанным на основе «КриптоПро JCP» версия 2.0 и реализующим протоколы SSL и TLS в соответствии с российскими криптографическими алгоритмами.

Основные функции, реализуемые «КриптоПро JTLS» версия 2.0:

- Две схемы аутентификации с использованием обмена ключей по алгоритму Диффи-Хэллмана и хэширования в соответствии с ГОСТ Р 34.11-94.
  - односторонняя - анонимный клиент, аутентифицируемый сервер;
  - двухсторонняя - аутентифицируемые клиент и сервер.

  В случае аутентификации клиента на ключе подписи применяются алгоритмы выработки электронной подписи в соответствии с ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012 и проверки 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.

2. Контрольная панель

Основной набор закладок контрольной панели «КриптоПро JCP» версия 2.0 описан в «Руководстве администратора». После установки модуля «КриптоПро JTLS» версия 2.0 на контрольной панели появятся соответствующие закладки.

2.1.Закладка "Сервер JTLS"

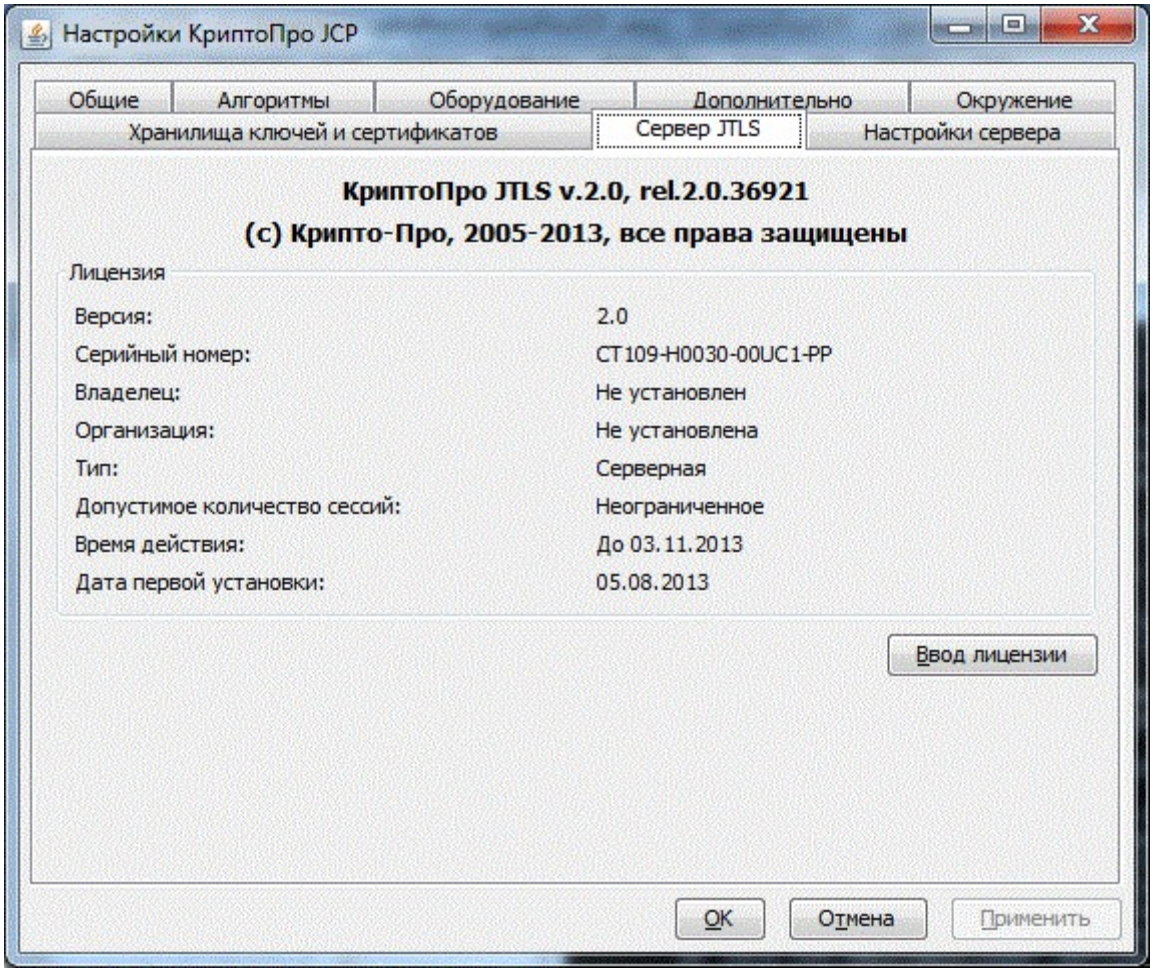

Рисунок 1. Внешний вид панели "Лицензия" (временная лицензия)

Данная панель содержит информацию о серверной лицензии «КриптоПро JTLS» версия 2.0. Работа с данной панелью аналогична работе с закладкой "Общие" (панель "Лицензия").

2.2.Закладка "Настройки сервера"

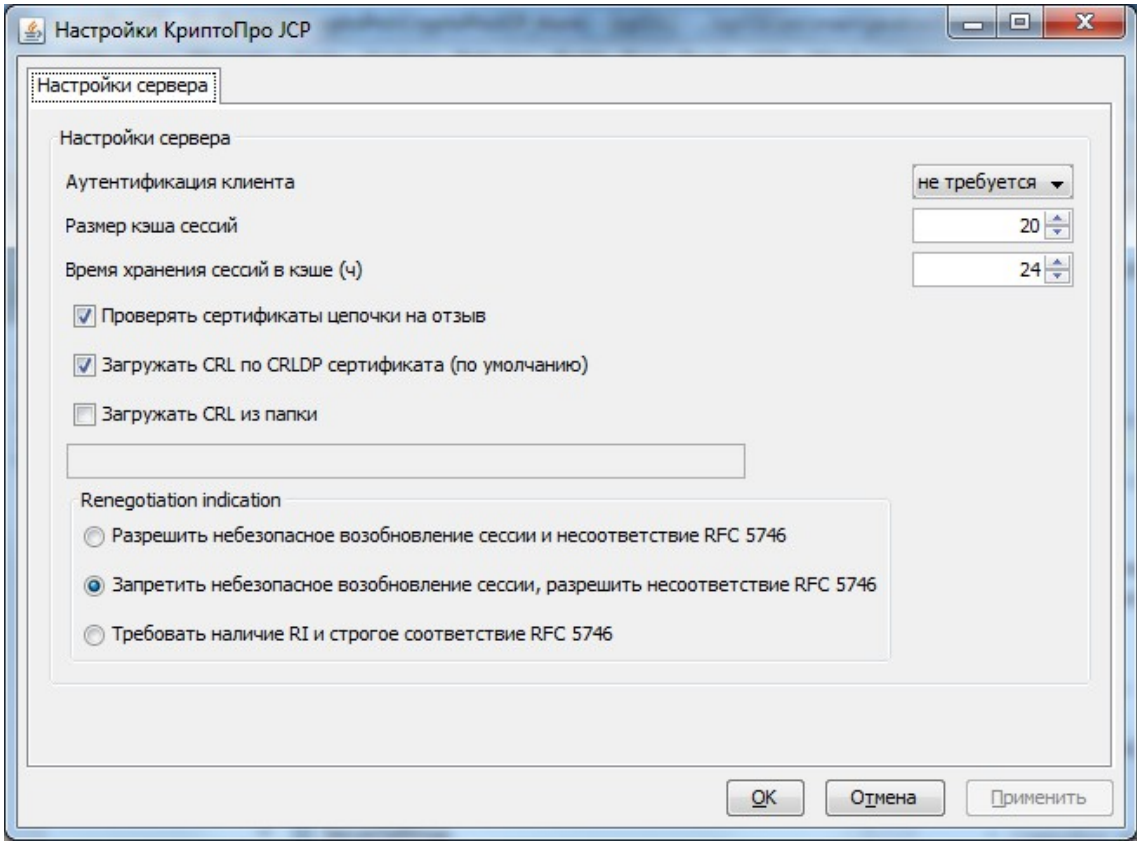

Рисунок 2. Внешний вид панели "Настройки сервера"

Данная панель содержит настройки сервера:

- Аутентификация клиента:
  - не требуется (по умолчанию)
  - желательна
  - 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 COC из сети по CRLDP сертификата, включение проверки с условием загрузки COC из папки (задается абсолютный путь к папке с COC).
- Отключение, включение и требование поддержки расширения Renegotiation Indication (RFC 5746). Задание данных настроек с помощью параметров *-Dru.CryptoPro.ssl.allowUnsafeRenegotiation=<value>* *-Dru.CryptoPro.ssl.allowLegacyHelloMessages=<value>* в приложении имеет приоритет выше и переопределяет настройки JTLS. Пары указанных свойств образуют следующие группы:

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

(insecure)			CryptoPro CSP): наличие RI необязательно, проверка не выполняется