ГАЗИНФОРМ СЕРВИС

Программный комплекс «Litoria Desktop 2»
Руководство администратора

Санкт-Петербург, 2022

Аннотация

В документе приводится руководство администратора программного комплекса «Litoria Desktop 2» версия 2.8.7-1 (в дальнейшем ПК «Litoria Desktop 2» или комплекс).

В разделе «Назначение, функции и состав комплекса» приводятся сведения о назначении комплекса.

В разделе «Условия применения комплекса» указаны условия, необходимые для использования комплекса, требования к аппаратным и программным средствам автоматизированного рабочего места (АРМ).

В разделе «Настройка комплекса» описаны действия, необходимые для выполнения настройки основных функций комплекса.

В разделе «Создание шаблонов для запросов на сертификаты» описан порядок действий по созданию пользовательского шаблона, отличного от базового набора шаблонов запросов на сертификаты, имеющегося в ПК «Litoria Desktop 2».

В разделе «Журнал событий» приведен перечень событий, фиксируемых в ПК «Litoria Desktop 2» при работе пользователей с комплексом.

Содержание

1 Назначение, функции и состав комплекса

1.1 Назначение комплекса

Основным назначением ПК «Litoria Desktop 2» является создание, добавление, заверение и проверка электронной подписи (ЭП), а также шифрование и извлечение зашифрованных файлов. В ПК «Litoria Desktop 2» реализована возможность выполнения одновременных операций создания ЭП и шифрования, извлечения и проверки ЭП.

Кроме того, продукт позволяет выполнить функции просмотра хранилища сертификатов; создания запроса на выпуск и перевыпуск сертификата, в т.ч. запроса, подписанного актуальной ЭП; установки сертификата на устройство; установки сертификата из устройства в реестр; просмотра установленных криптопровайдеров и их параметров; продления срока доверенного архивного хранения подписанных электронных документов, использования службы доверенной третьей стороны (ДТС) для проверки ЭП.

ПК «Litoria Desktop 2» поддерживает работу с USB-токенами, представленными в таблице 1.1.

Таблица 1.1 – Поддержка работы с носителями в зависимости от ОС, в которой функционирует ПК «Litoria Desktop 2»

Операционные системы	Носитель
Windows	Рутокен S, Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен Lite; JaCarta PKI, JaCarta ГОСТ, JaCarta LT; eToken NG-FLASH (Java), eToken PRO, eToken PRO (Java), eToken ГОСТ; ESMART Token USB 64K
Linux	ruToken S, ruToken ЭЦП, ruToken ЭЦП 2.0, ruToken Lite

ПК «Litoria Desktop 2» поддерживает обращение к функциональным ключевым носителям через интерфейс PKCS#11[1].

1.2 Функциональные возможности

Для подготовки АРМ к работе с ЭП ПК «Litoria Desktop 2» предоставляет пользователю возможность выполнить следующие функции:

- создание нового запроса на сертификат, в т.ч. подписанного актуальной ЭП;
- создание запроса на основе имеющегося сертификата;
- установка сертификата на устройство;

[1] Корректная работа с интерфейсом PKCS#11 в ПК «Litoria Desktop 2» осуществляется только для ruToken ЭЦП и ruToken ЭЦП 2.0.

– просмотр сертификатов в контейнерах;
– установка сертификата из устройства в хранилище «Личное»;
– управление сертификатами:
  - импорт;
  - экспорт;
  - удаление;
  - детальный просмотр;
  - проверка статуса по локальному и/или удаленному списку отзыва сертификатов (COC) и по протоколу OCSP в реальном времени;
– просмотр списка криптопровайдеров;
– управление контейнерами (импорт сертификатов в контейнер, экспорт сертификатов из контейнера, в том числе с экспортированием ключей);
– управление настройками комплекса.

Для работы с ЭП комплекс обеспечивает выполнение следующих функций:

– создание, добавление, заверение ЭП для файлов произвольного типа;
– создание, добавление, заверение ЭП для pdf документов в соответствии со стандартами CAdES (согласно RFC 5126) и PAdES (согласно ETSI as TS 102 778);[2]
– создание, добавление, заверение ЭП для xml документов в соответствии со стандартами CAdES (согласно RFC 5126) и XAdES (согласно ETSI as TS 101 903);
– проверка ЭП для подписанных файлов с возможностью получения исходного документа;
– использование службы ДТС для проверки ЭП;
– шифрование файла произвольного типа;
– извлечение файла;
– универсальные операции:
  - создание ЭП и шифрование файла произвольного типа;
  - извлечение файла и проверка ЭП с возможностью получения исходного документа;
– поддержка электронных документов длительного архивного хранения.

Для проверки целостности и достоверности при передаче данных заказчику комплекс обеспечивает возможность хеширования файлов по алгоритмам ГОСТ.

1.2.1 Создание нового запроса на сертификат

Для выполнения операций создания/добавления/заверения ЭП необходимо иметь личный сертификат ключа проверки ЭП.

Сертификат ключа проверки ЭП содержит уникальный номер сертификата ключа проверки ЭП, даты начала и окончания срока действия сертификата, идентификационную информацию о пользователе (в том числе его имя), уникальный ключ проверки ЭП, наименование используемого средства ЭП и наименование

[2] Операции заверения для pdf документов по стандарту PAdES недоступны.

удостоверяющего центра, который выдал сертификат ключа проверки ЭП.

Ключ ЭП, соответствующий ключу проверки ЭП должен находиться в контейнере на отчуждаемом носителе. В качестве отчуждаемого носителя может использоваться любой носитель (например, сменный носитель с интерфейсом USB и др.).

С помощью ПК «Litoria Desktop 2» можно создать запрос на новый личный сертификат. Для этого надо указать криптопровайдер, имя ключевого контейнера и ПИН-код к контейнеру, личную идентификационную информацию пользователя и информацию о создаваемом сертификате, такую как использование ключа и назначение сертификата. При выполнении операции создания запроса осуществляется так же создание ключевой пары: ключ ЭП – ключ проверки ЭП. Созданный запрос отправляется на рассмотрение в УЦ и на основе него УЦ выпустит сертификат ключа проверки ЭП.

Также ПК «Litoria Desktop 2» позволяет создать запрос на сертификат на основе предустановленного шаблона и возможность подписи создаваемого запроса имеющейся актуальной ЭП.

1.2.2 Создание запроса на основе имеющегося сертификата

ПК «Litoria Desktop 2» позволяет создать запрос на новый сертификат на основе имеющегося сертификата, у которого истекает или уже истек срок действия.

Для создания запроса на сертификат на основе имеющегося необходимо указать криптопровайдер, имя ключевого контейнера и ПИН-код к контейнеру, и выбрать сертификат, на основе которого надо создать запрос на новый сертификат.

1.2.3 Установка сертификата на устройство

ПК «Litoria Desktop 2» позволяет выполнить установку сертификата ключа проверки подписи на устройство, которое ранее использовалось для создания запроса и содержит контейнер с парой: ключ ЭП – ключ проверки ЭП к этому сертификату.

1.2.4 Просмотр сертификатов в контейнерах

С помощью ПК «Litoria Desktop 2» можно выполнить просмотр сертификатов, созданных на основе различных криптопровайдеров, во всех имеющихся контейнерах. И установить выбранный сертификат в хранилище «Личное».

1.2.5 Управление сертификатами

ПК «Litoria Desktop 2» позволяет работать с системными и пользовательскими хранилищами сертификатов. Существуют возможности импорта, экспорта и удаления сертификатов, а также просмотра хранилища сертификатов.

Хранилище сертификатов – это область системы, предназначенная для хранения сертификатов.

Импорт – это копирование сертификатов и списков отозванных сертификатов с локального диска в хранилище сертификатов.

Экспорт – это копирование сертификатов и списков отозванных сертификатов из

хранилища сертификатов на локальный диск.

С помощью функции *Импорт* можно установить сертификаты или списки отзыва (с расширениями *.cer, *.crl, *.crt, *.p7b) и сертификаты из файлов обмена ключевой информации (*.pfx):

1) сертификаты доверенных корневых центров сертификации и промежуточных центров сертификации в хранилища *«Доверенные корневые центры сертификации»* и *«Промежуточные центры сертификации»* соответственно;

2) списки отозванных сертификатов в хранилище сертификатов «*Списки отозванных сертификатов*»;

3) личные сертификаты из файлов, полученных от УЦ в ответ на отправленный запрос, в хранилище сертификатов *«Личные сертификаты»*;

4) личные сертификаты из pfx-контейнеров в хранилище сертификатов *«Личные сертификаты»*, при этом создается контейнер с необходимыми ключами.

1.2.6 Просмотр списка криптопровайдеров

С помощью ПК «Litoria Desktop 2» можно выполнить просмотр установленных на компьютере криптопровайдеров и информацию о них.

ПК «Litoria Desktop 2» поддерживает работу с криптографическими алгоритмами, приведенными в таблице 1.2.

Таблица 1.2 – Криптографические алгоритмы, поддерживаемые ПК «Litoria Desktop 2»

Алгоритм	Длина ключа	ОС
КриптоПро ГОСТ Р 34.10-2012	512, 1024	Windows/Linux
КриптоПро ГОСТ Р 34.10-2001	512	Windows/Linux
RSA	384-16384	Windows/Linux
CNG RSA	512-4096	Windows
CNG ECDSA_P256	256	Windows
CNG ECDSA_P384	384	Windows
CNG ECDSA_P521	521	Windows

1.2.7 Управление контейнерами

ПК «Litoria Desktop 2» предоставляет возможность импортировать сертификаты в контейнеры, экспортировать сертификаты из контейнеров в заданный файл (в том числе с экспортированием ключевой информации), а также удалять контейнеры ключа ЭП с ключевого отчуждаемого носителя.

1.2.8 Управление настройками комплекса

ПК «Litoria Desktop 2» предоставляет возможность создать настройки для типовых операций: установить кодировку выходных файлов операций, указать информацию для

подключения к прокси-серверу, установить адрес службы штампов времени, указать имя рабочей директории, выбрать стандарт PAdES при создании и проверке подписи pdf-документов и другое.

Более подробное описание создания и изменения настроек смотрите в разделе 3 данного документа.

1.2.9 Создание ЭП

ЭП – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки и полученный в результате криптографического преобразования информации с использованием ключа ЭП. С помощью ЭП можно идентифицировать владельца сертификата ключа проверки подписи, а также установить отсутствие искажения информации в электронном документе.

Для создания ЭП должен быть осуществлен выбор сертификата ключа проверки подписи и параметров создания ЭП.

К параметрам создания ЭП относятся:

– создание отделенной или совмещенной ЭП;
– создание ЭП с меткой доверенного времени на значение ЭП;
– создание ЭП с доказательством действительности сертификата.

Процесс создания ЭП с доказательством действительности сертификата делится на следующие этапы:

– создание ЭП;
– получение метки доверенного времени на значение ЭП;
– сбор доказательств действительности сертификата ключа проверки подписи и присоединение этих доказательств и их хеш-кодов к подписанному документу;
– получение метки доверенного времени на сформированные доказательства действительности сертификата ключа проверки ЭП.

1.2.10 Добавление ЭП

В случае, когда в подписании документа участвует несколько лиц, и каждый должен поставить в нем свою подпись (например, в листе согласования), используется операция добавления ЭП. В отличие от операции создания ЭП, добавление ЭП производится в уже подписанный ранее документ.

В ПК «Litoria Desktop 2» существует возможность добавления подписи, созданной на криптографическом алгоритме, отличном от ГОСТ, например, RSA.

1.2.11 Заверение ЭП

ПК «Litoria Desktop 2» позволяет формировать заверяющую ЭП. С помощью этого типа подписи можно заверить ЭП другого пользователя, сформировав ЭП на значении ЭП другого пользователя, тем самым косвенно подписывая сами данные.

Перед созданием заверяющей подписи производится проверка ЭП, чтобы было

достоверно известно, какие подписи уже существуют в документе, и их статус.

Дальнейшая операция по заверению подписи аналогична созданию ЭП.

Заверение ЭП возможно лишь для подписанных ранее файлов.

1.2.12 Проверка ЭП

Проверка ЭП подразумевает подтверждение подлинности электронной подписи в электронном документе, то есть:

– принадлежность ЭП в электронном документе владельцу сертификата ключа проверки подписи;
– отсутствие искажений в электронном документе, который подписан данной ЭП;
– подтверждение момента подписи;
– подтверждение действительности сертификата ключа проверки подписи на момент проверки либо на момент создания ЭП при наличии в подписи доказательств, определяющих этот момент.

Проверка ЭП с доказательством действительности сертификата файла с отделенной подписью – проверка корректности самого файла подписи.

1.2.13 Использование службы ДТС для проверки ЭП

ПК «Litoria Desktop 2» позволяет получать подтверждение корректности ЭП электронного документа (Validation of Digitally Signed Document – VSD) от службы ДТС.

Для обращения к службе необходимо наличие сертификата ключа проверки ЭП, зарегистрированного ранее на сервере ДТС. Подписанный указанным сертификатом DVCS-запрос отправляется для проверки на сервер службы ДТС. При этом, если найден подходящий криптопровайдер, используется хеширование подписанного файла. В ответ сервер присылает информацию о действительности ЭП документа.

Формирование запросов к службе ДТС происходит в прозрачном для пользователя режиме. При этом отображение результатов проверок пользователю как с использованием службы ДТС, так и без нее, осуществляется в обычном режиме.

Использование службы ДТС для проверки ЭП позволяет пользователю не устанавливать списки отзывов сертификатов на локальный компьютер. Проверка ЭП осуществляется на сервере ДТС с выдачей доказательств действительности в виде квитанции. Таким образом, пользователи осуществляют перечисленные проверки в единой точке, контролируемой администратором безопасности, с сохранением всех результатов операций и статистических выборок.

Настройка включения/выключения режима использования службы ДТС для проверки ЭП и действительности сертификата ключа проверки ЭП осуществляется пользователем с правами администратора. Более подробное описание настройки смотрите в п.3.2.2.

1.2.14 Поддержка электронных документов длительного архивного хранения

Необходимым условием архивного хранения электронных документов является

использование ЭП с доказательством действительности сертификата. Такой формат подписи предусматривает обязательное включение в реквизиты подписанного документа доказательства момента создания подписи (метку доверенного времени) и действительности сертификата в момент создания подписи. Такую подпись можно успешно проверять в течение срока действия ключа проверки подписи службы штампов времени.

При истечении срока действия ключа проверки подписи службы штампа времени, для длительного архивного хранения электронных документов, подписанных ЭП с доказательством действительности сертификата, к подписи добавляется архивная метка времени, повышая значимость подписи до стандарта CAdES-A. [3]

В ПК «Litoria Desktop 2» реализована поддержка электронных документов длительного архивного хранения включая доказательство момента подписи документа при создании ЭП и проверке ее корректности и возможность доказательства корректности подписи и целостности файла после истечения срока действия сертификата подписи.

1.2.15 Шифрование файла

Шифрование производится с использованием ключа проверки ЭП, содержащегося в сертификате получателя. Ключ ЭП есть только у владельца использованного сертификата ключа проверки ЭП. Таким образом, при шифровании файла никто, кроме владельца ключа ЭП, не сможет расшифровать файл.

ПК «Litoria Desktop 2» может производить шифрование файла сразу для нескольких будущих получателей файла, при этом их сертификаты должны быть созданы с помощью криптографического алгоритма, относящегося к стандарту (например, ГОСТ или RSA), единому для всех участников операции. Для каждого сертификата получателей пользователь может просмотреть статус, чтобы на его основании сделать вывод о пригодности данного сертификата к шифрованию.

1.2.16 Извлечение файла

При получении зашифрованного документа извлечение пройдет успешно при условии наличия ключа ЭП, связанного с одним из ключей проверки ЭП, на которых производилось шифрование файла. Если существует несколько ключей ЭП, которым соответствуют несколько ключей проверки ЭП, участвующих при шифровании, то расшифровывание произойдет на первом из ключей ЭП. После извлечения можно получить информацию о том, на каком сертификате была произведена операция расшифровывания.

1.2.17 Универсальная операция создания ЭП и шифрования файла

Комплекс предоставляет возможность одновременного создания ЭП и шифрования. Все действия, выполняемые при этом аналогичны одиночным операциям создания ЭП и шифрования. Таким образом достигается универсальность в интерфейсе и удобство для

[3] Архивное хранение pdf документа по стандарту PAdES не осуществляется.

пользователя.

1.2.18 Универсальная операция извлечения файла и проверки ЭП

Данная операция выполняется в два этапа: вначале выполняется извлечение, потом проверка ЭП.

После выполнения операции пользователю становится доступна следующая информация:

– для извлечения – сертификат ключа проверки ЭП, на связанном с которым ключе ЭП файл был расшифрован;
– для проверки ЭП – все сертификаты, их статусы.

1.2.19 Вычисление контрольных сумм файлов

С помощью ПК «Litoria Desktop 2» возможно вычисление хеш-суммы для любого файла по алгоритмам хеширования ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 с длиной хеш-кода 256 бит и ГОСТ Р 34.11-2012 с длиной хеш-кода 512 бит.

Расчет хеш-сумм файлов необходим для проверки целостности и достоверности при передаче данных заказчику.

2 Условия применения комплекса

2.1 Требования к среде функционирования

ПК «Litoria Desktop 2» функционирует под управлением следующих операционных систем (ОС) Microsoft Windows:

– Windows 7 (32 бит/64 бит) 4;
– Windows 8/8.1 (32 бит/64 бит);
– Windows 10 (32 бит/64 бит).
– Windows Server 2008 R2;
– Windows Server 2012/2012R2/2016/2019 (64 бит).

и ОС семейств Linux, поддерживающих системную библиотеку GNU C Library (Glibc) версии не ниже 2.22.

Гарантирована работа ПК «Litoria Desktop 2» на следующих ОС семейств Linux:

– AltLinux версии 8.2 или выше (64 бит);
– Ubuntu версии 16 или выше (64 бит);
– RedOS версии 7.1 или выше (64 бит);
– Astra Linux Special Edition версии 1.6 (64 бит);
– Astra Linux Common Edition версии 2.12.42 или выше (64 бит).

2.2 Требования к аппаратному и программному обеспечению

Минимальные требования к производительности рабочей станции, на которую устанавливается ПК «Litoria Desktop 2», обусловлены требованиями используемых ОС.

При использовании аппаратных идентификаторов необходимо наличие на рабочей станции USB-порта.

Для корректного отображения ПК «Litoria Desktop 2» рекомендуется использовать разрешение экрана монитора не менее 1280x960 пикселей.

Дополнительно должно быть установлено следующее программное обеспечение:

– Средство криптографической защиты информации, реализованное в соответствии с технологией Microsoft CSP. Например: либо программные СКЗИ – «ViPNet CSP», «ВАЛИДАТА CSP», «Крипто-Ком», «КриптоПро CSP» или ПК «ЛИССИ-CSP»; либо драйверы для аппаратных СКЗИ – «Криптотокен» в составе изделия «eToken ГОСТ» или «РУТОКЕН ЭЦП».

[4] Срок эксплуатации ОС определяется сроками выпуска обновлений критических уязвимостей.

3 Настройка комплекса

Настройка комплекса осуществляется пользователем с правами администратора. Вкладка «*Настройки*» (рисунок 3.1) содержит разделенные по вкладкам основные, сетевые и расширенные настройки комплекса.

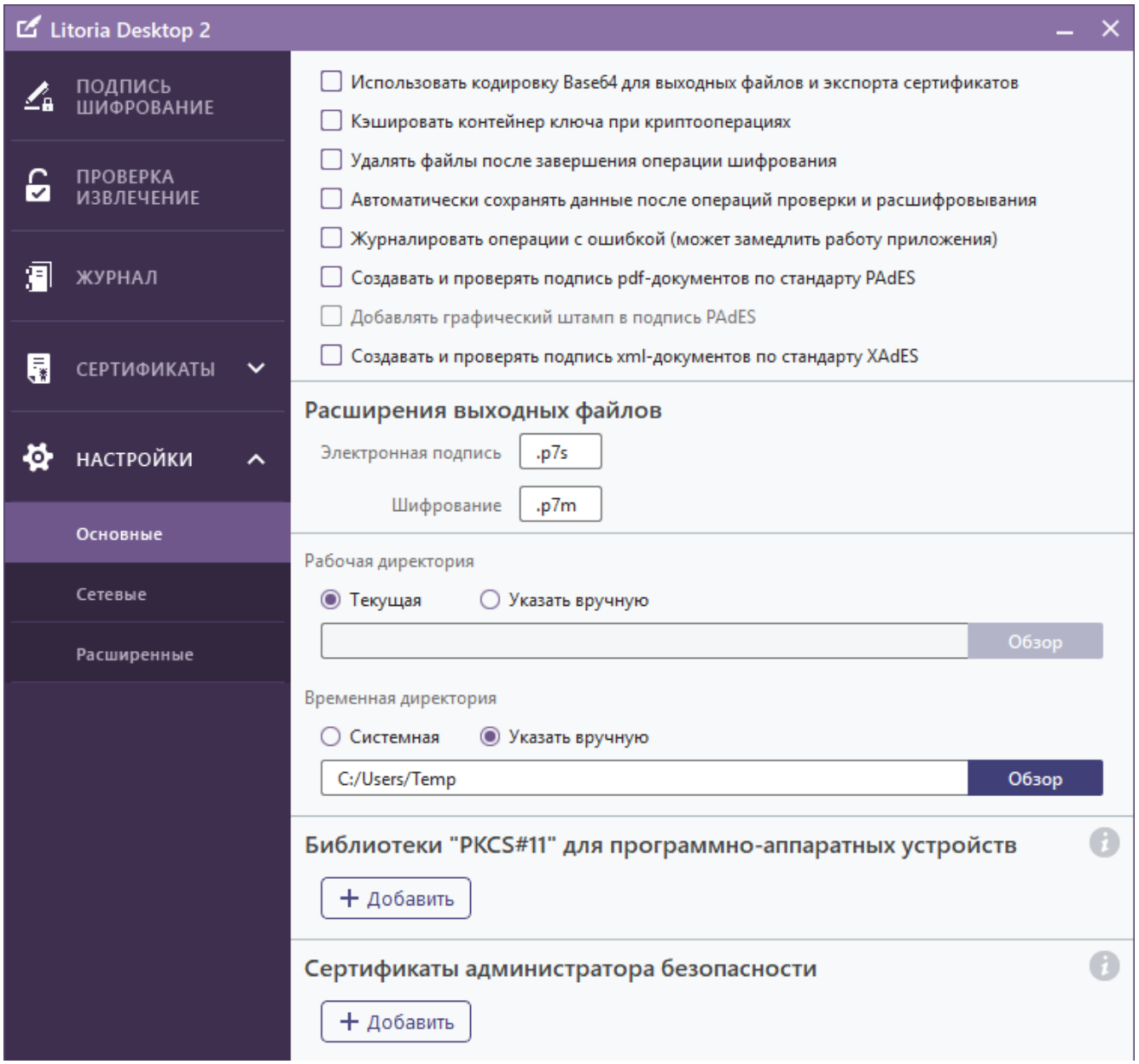


Рисунок 3.1 – Пункт меню «Настройки»

3.1 Основные настройки

Вкладка «*Основные настройки*» позволяет выполнять настройку:

– кодировки для выходных файлов и экспорта сертификатов;
– кэширования контейнера;

– удаления файлов после шифрования;
– автоматического сохранения данных после операций проверки и расшифровывания;
– журналирования операций, завершившихся ошибкой;
– создания и проверки подписи pdf документов по стандарту PAdES;
– добавления графического штампа в подписи PAdES;
– создания и проверки подписи xml-документов по стандарту XAdES;
– расширений выходных файлов;
– рабочих и временных директорий;
– используемых криптопровайдеров[5];
– библиотек PKCS#11 для программно-аппаратных устройств;
– сертификатов администратора безопасности.

3.1.1 Настройки кодировки для выходных файлов и экспорта сертификатов

По умолчанию используется DER-кодировка выходных файлов и экспорта сертификатов. Для изменения кодировки выходных файлов основных операций поставьте флаг «*Использовать кодировку Base64 для выходных файлов и экспорта сертификатов*» в пункте меню «*Настройки*» вкладка «*Основные*» (рисунок 3.2).

[5] Настройка доступна при работе ПК «Litoria Desktop 2» в ОС семейств Linux.

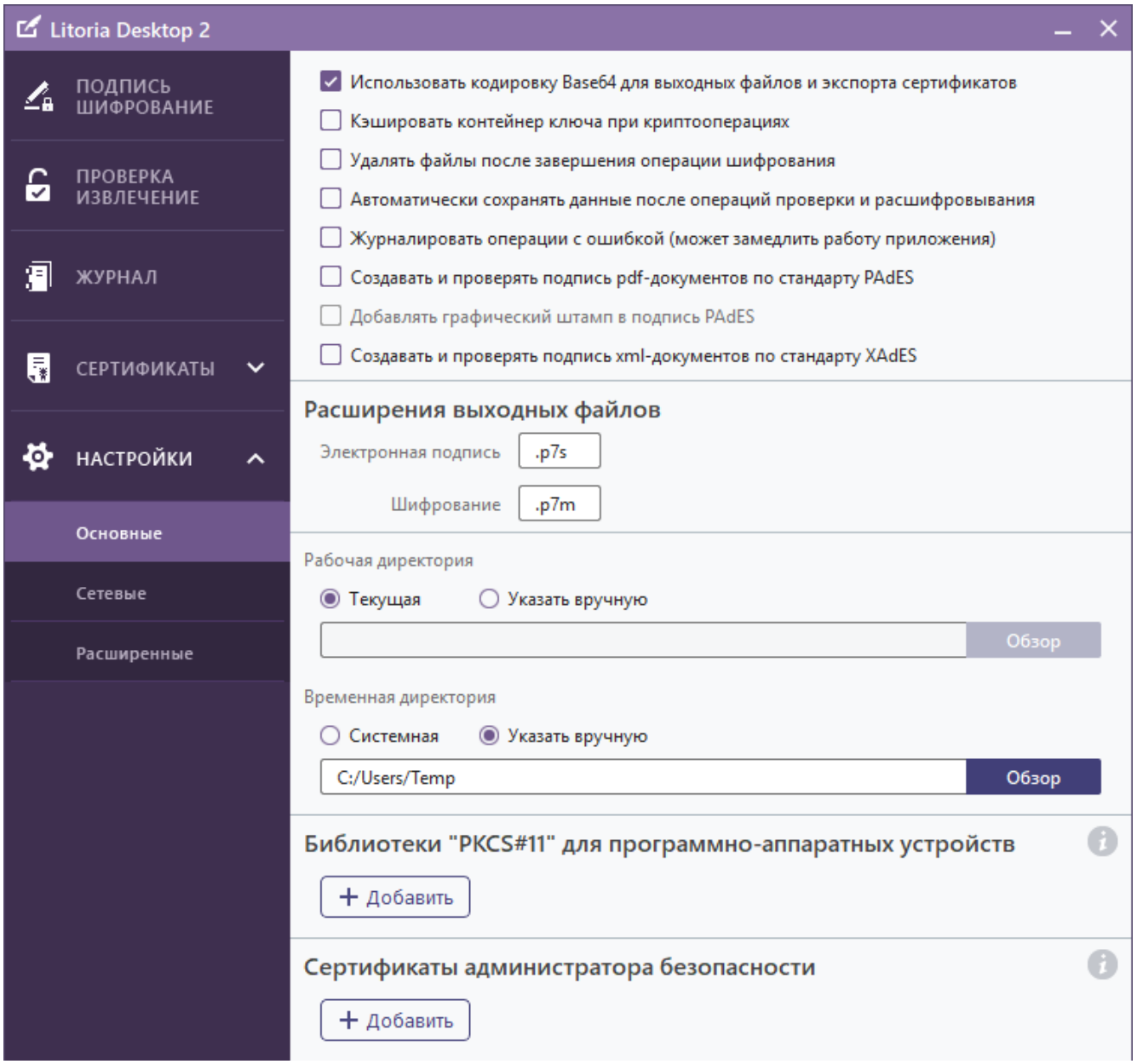


Рисунок 3.2 – Настройка кодировки выходных файлов

3.1.2 Настройка кэширования контейнера

В основных настройках возможно установить флаг «*Кэшировать контейнер ключа при криптооперациях*». Включение такого режима работы ПК «Litoria Desktop 2» означает увеличение скорости выполнения основных функций комплекса с большим количеством файлов.

Увеличение скорости происходит за счет того, что при первом обращении к контейнеру ключа ЭП и после ввода пользователем ПИН-кода к ключевому носителю, содержащему этот контейнер, создается дубликат контейнера, открытый на доступ на протяжении выполнения всей операции, которая требует несколько обращений к контейнеру ключа ЭП.

После завершения операции с большим количеством файлов созданный дубликат контейнера удаляется.

Значение настройки криптопровайдера хранится в ветке реестра HKEY_LOCAL_MACHINE\SOFTWARE\GIS\litoria.

3.1.3 Настройки удаления файлов после шифрования

При необходимости удалять файлы после завершения операции шифрования установите флаг напротив пункта «*Удалять файлы после завершения операции шифрования*». По умолчанию файлы не удаляются.

3.1.4 Настройка автоматического сохранения данных после операций проверки и расшифровывания

При необходимости автоматического сохранения исходных данных файла после выполнения операций проверки и расшифровывания установите флаг напротив пункта «*Автоматически сохранять данные после операций проверки и расшифровывания*».

В случае установки флага исходные данные проверяемого файла будут сохранены в рабочей директории (п. 3.1.9 «*Установка директории*»). По умолчанию в качестве рабочей директории используется текущая – та директория, в которой расположен исходный файл.

3.1.5 Настройка журналирования операций с ошибкой

Для операций создания, добавления, заверения и проверки ЭП, шифрования и извлечения файлов, завершившихся ошибкой, возможно журналирование. В случае выявления ошибки в операции, следует открыть сформированный файл и просмотреть содержащиеся в нем сообщения.

По умолчанию журналирование операций с ошибкой не осуществляется. Для осуществления журналирования установите флаг напротив пункта «*Журналировать операции с ошибкой (может замедлить работу приложения)*» (рисунок 3.3).

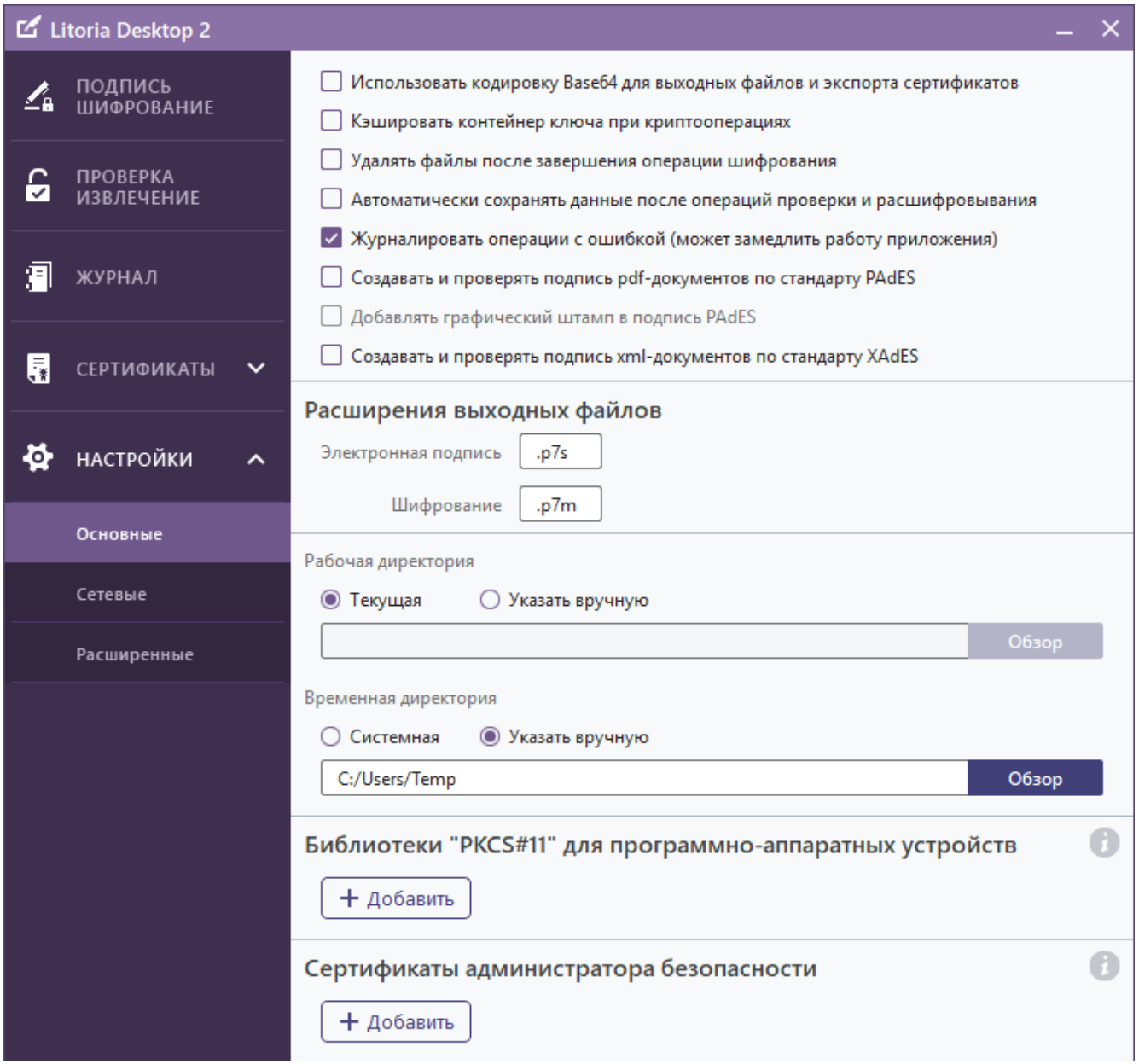


Рисунок 3.3 – Настройка журналирования операций с ошибкой

3.1.6 Настройка создания и проверки подписи pdf документов по стандарту PAdES

По умолчанию создание и проверка ЭП pdf документа осуществляется по стандарту CAdES, при этом расширение документа не изменится, и будет иметь вид расширения, заданного в настройках параметра «*Электронная подпись*» в области «*Расширения выходных файлов*». По умолчанию «.p7s» (рисунок 3.4).

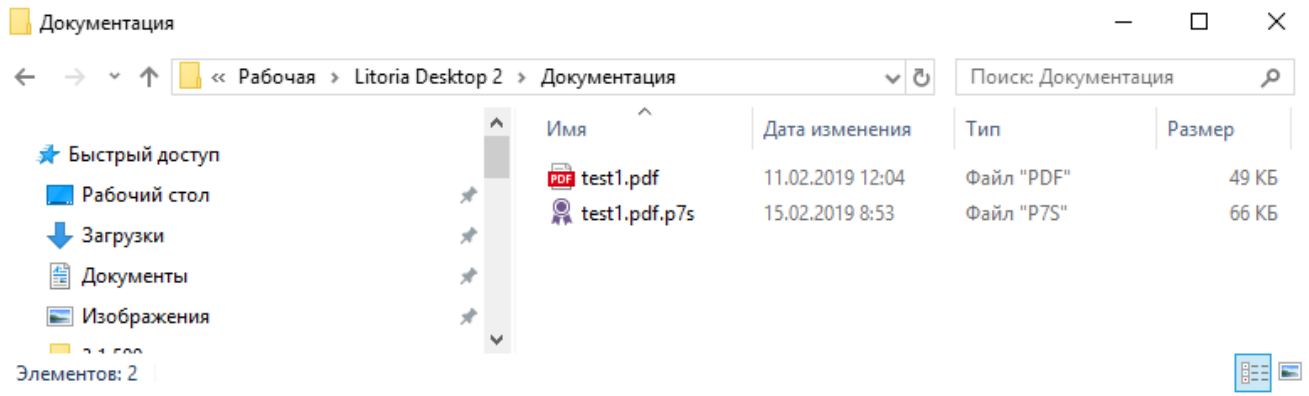


Рисунок 3.4 – Результат подписи pdf документа по стандарту CAdES

Pdf документы со сформированной ЭП по стандарту CAdES могут добавляться и проверяться в более ранних версиях ПК «Litoria Desktop 2» без внесения в них изменений.

Для изменения стандарта подписи pdf документов на PAdES необходимо установить флаг «*Создавать и проверять подпись pdf документов по стандарту PAdES*». При этом подписанный документ будет иметь вид, представленный на рисунке 3.5.

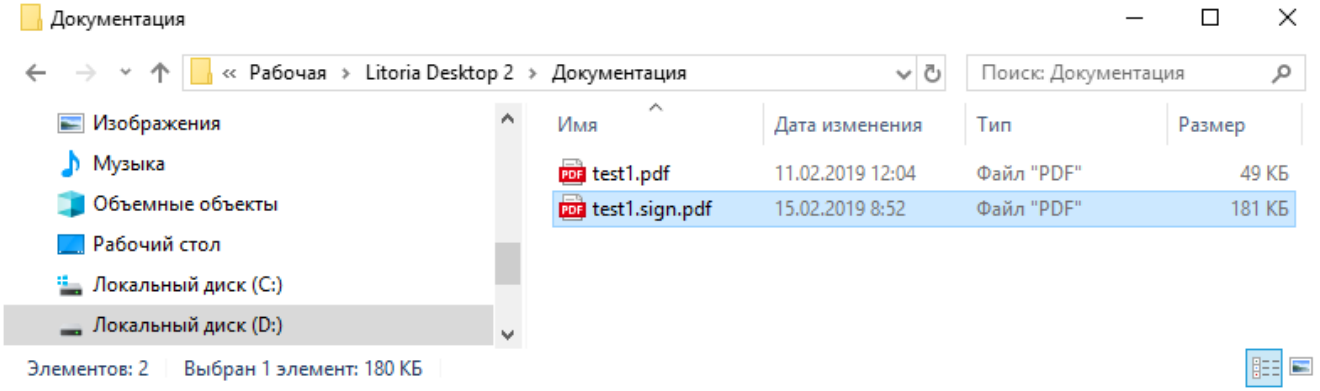


Рисунок 3.5 – Результат подписи pdf документа по стандарту PAdES

При подписи pdf документов по стандарту PAdES используется кодировка «adbe.pkcs7.detached».

3.1.7 Добавление графического штампа в подпись PAdES

При установке создания и проверки ЭП pdf документа по стандарту PAdES (пункт 3.1.6 «Настройка создания и проверки подписи pdf документов по стандарту PAdES») возможно формирование графического штампа вида, представленного на рисунке 3.6.

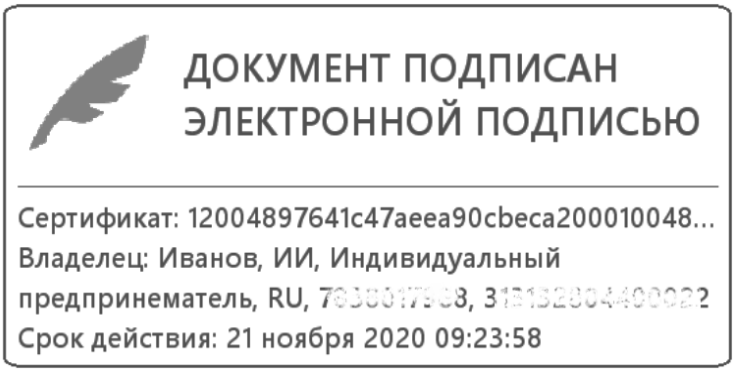


Рисунок 3.6 – Пример графического штампа pdf документа

Для добавления графического штампа в подпись pdf документа по стандарту PAdES, необходимо установить флаг *«Добавлять графический штамп в подпись PAdES»*.

Необходимо учитывать, что графический штамп добавляется в правый нижний угол последней страницы подписываемого документа. Убедитесь в том, что добавляемый графический штамп не заходит на текст документа.

При наличии нескольких подписей в документе, графический штамп первой подписи добавляется в правый нижний угол, а все последующие подписи левее в порядке подписания.

3.1.8 Настройка создания и проверки подписи xml-документов по стандарту XAdES

По умолчанию создание и проверка ЭП xml-документа осуществляется по стандарту CAdES, при этом расширение документа не изменится, и будет иметь вид расширения, заданного в настройках параметра «*Электронная подпись*» в области «*Расширения выходных файлов*». По умолчанию «.p7s» (рисунок 3.7).

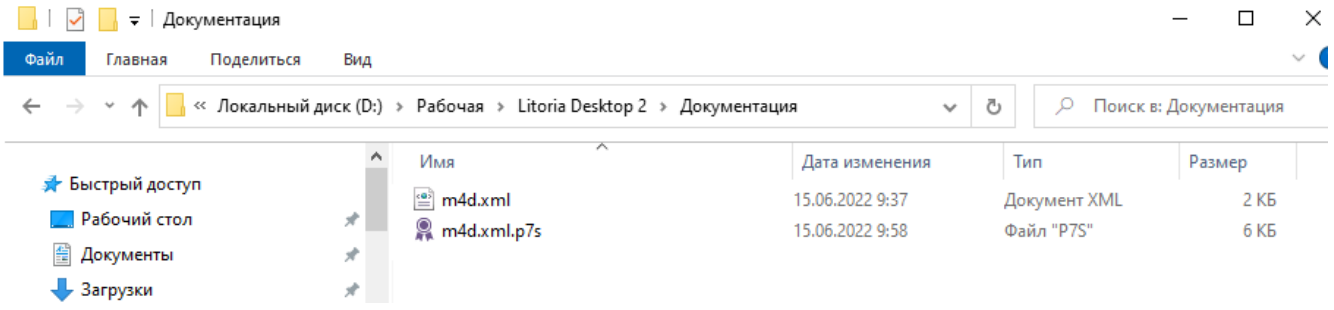


Рисунок 3.7 – Результат подписи xml-документа по стандарту CAdES

Xml-документы со сформированной ЭП по стандарту CAdES могут добавляться и проверяться в более ранних версиях ПК «Litoria Desktop 2» без внесения в них изменений.

Для изменения стандарта подписи xml-документов на XAdES необходимо установить флаг «*Создавать и проверять подпись xml-документов по стандарту XAdES*». При этом подписанный документ будет иметь вид, представленный на рисунке 3.8.

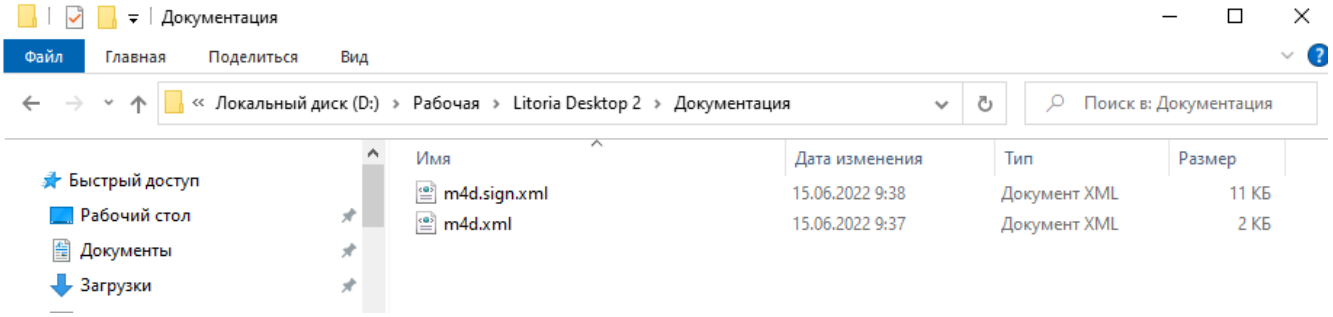


Рисунок 3.8 – Результат подписи xml-документа по стандарту XAdES

3.1.9 Расширения выходных файлов

В основных настройках, в области «*Расширения выходных файлов*» указаны расширения, используемые по умолчанию (рисунок 3.9)[6]:

– для функций, связанных с ЭП – «.p7s»;
– для функции шифрования – «.p7m».

[6] При функционировании ПК «Litoria Desktop 2» под управлением ОС семейств Linux, расширения выходных файлов заданы по умолчанию и недоступны для редактирования.

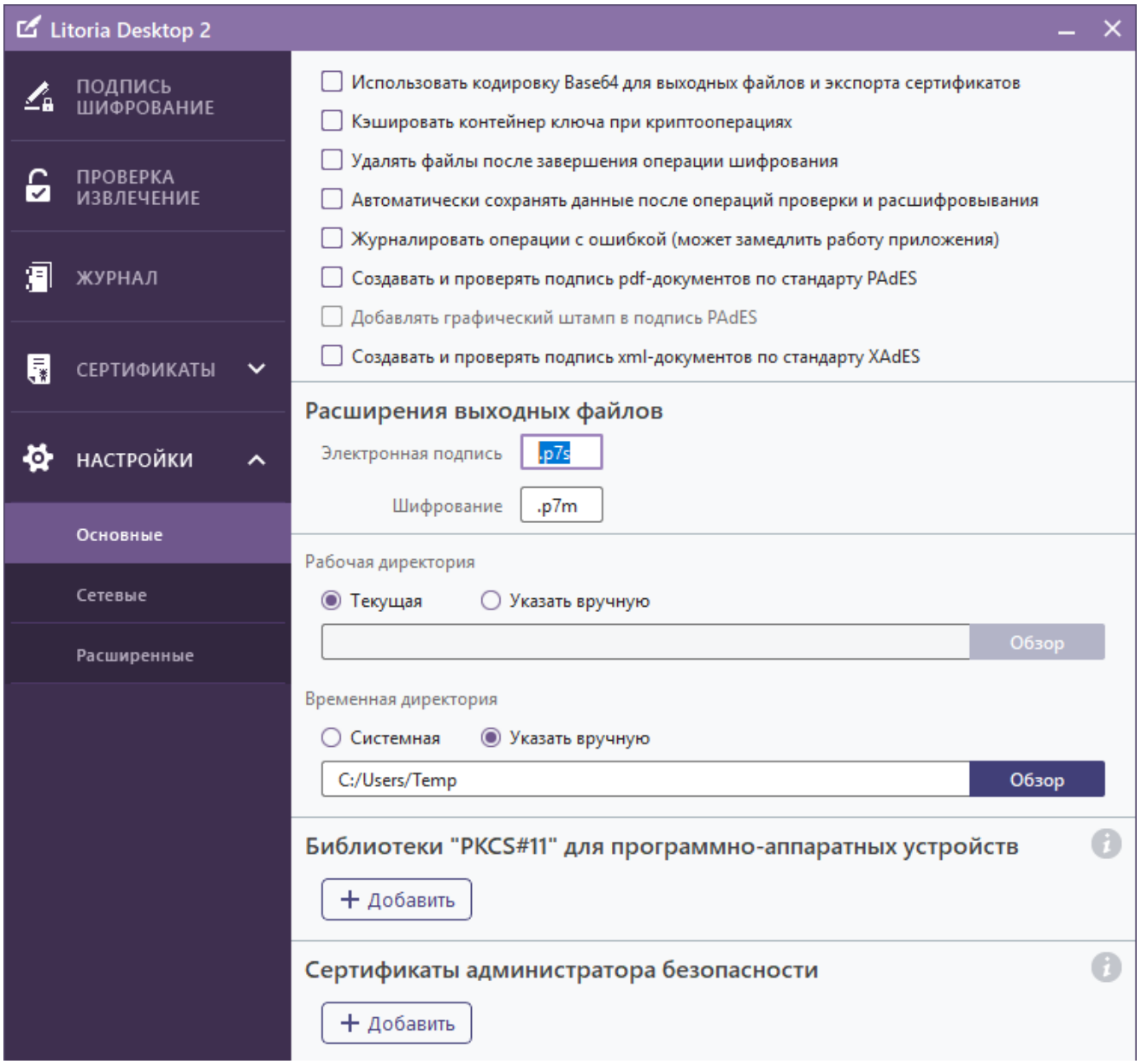


Рисунок 3.9 – Настройки расширений выходных файлов

Данные расширения хранятся в ветке реестра HKEY_LOCAL_MACHINE\SOFTWARE\GIS\litoria\Extensions. [7]

Для изменения расширений выходных файлов операций, связанных с ЭП, введите нужное расширение (например, *sign*) в поле «*Электронная подпись*».

Для изменения расширения выходных файлов операции шифрования введите нужное расширение (например, *pem*) в поле «*Шифрование*».

Сохранение измененных расширений происходит автоматически. Новые расширения

[7] Расширения сохранятся в указанной ветке реестра только после внесения изменений в данную настройку.

выходных файлов сохраняются для всех пользователей компьютера.

3.1.10 Установка директорий

Указание рабочей директории, в которую будут записываться выходные файлы всех основных операций, осуществляется в области «*Рабочая директория*» пункта «*Основные настройки*» (рисунок 3.10).

По умолчанию в качестве рабочей директории используется текущая – та директория, в которой расположен исходный файл. Для указания другой директории установите переключатель в позицию «*Указать вручную*» и нажмите на кнопку «*Обзор*».

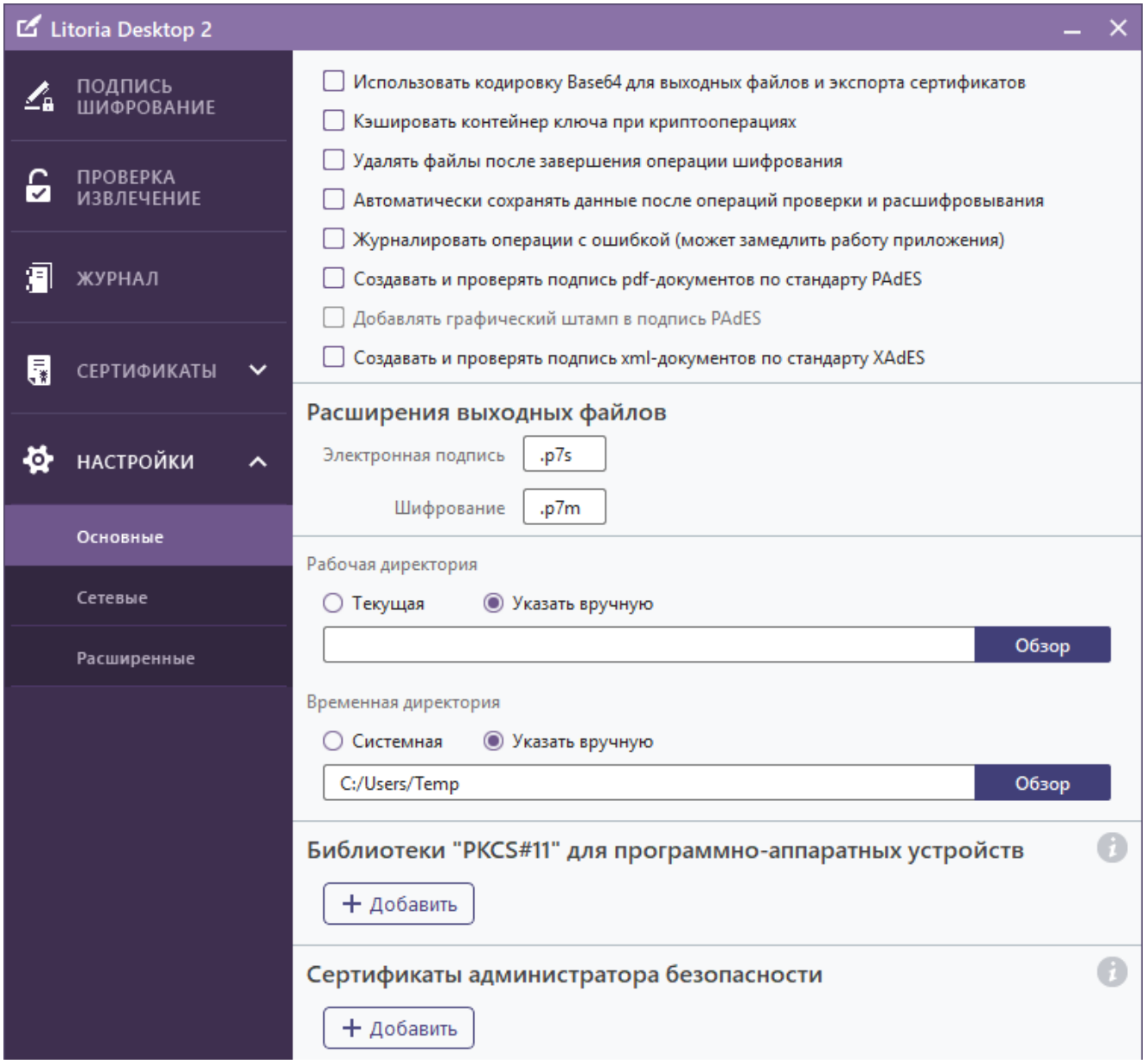


Рисунок 3.10 – Настройки директорий

В появившемся окне укажите нужную директорию и нажмите на кнопку «*Выбор папки*».

Для хранения временных файлов ПК «Litoria Desktop 2» по умолчанию используется

системная директория, и в области «*Временная директория*» установлен переключатель в позиции «*Системная*».

Для изменения директории, отличной от системной, установите переключатель в позицию «*Указать вручную*». Затем нажмите на кнопку «*Обзор*» и в открывшемся окне укажите необходимую директорию.

3.1.11 Используемый криптопровайдер[8]

При установке ПК «Litoria Desktop» выполняется определение криптопровайдера, установленного на компьютере, и в области «*Используемый криптопровайдер*» пункта «*Основные настройки*» будет отображено наименование криптопровайдера в соответствии с криптопровайдером, обнаруженным на рабочей станции (рисунок 3.11).

При установке ПК «Litoria Desktop» на lite-версии ОС Linux настройки используемого криптопровайдера не отображаются.

Если ПК «Litoria Desktop» был установлен на компьютер под управлением lite-версии ОС Linux и на рабочей станции на момент установки не было установленных программных криптопровайдеров, то после установки криптопровайдера необходимо выполнить команду *sudo litoria config*.

[8] Настройка доступна при работе ПК «Litoria Desktop 2» в ОС семейств Linux.

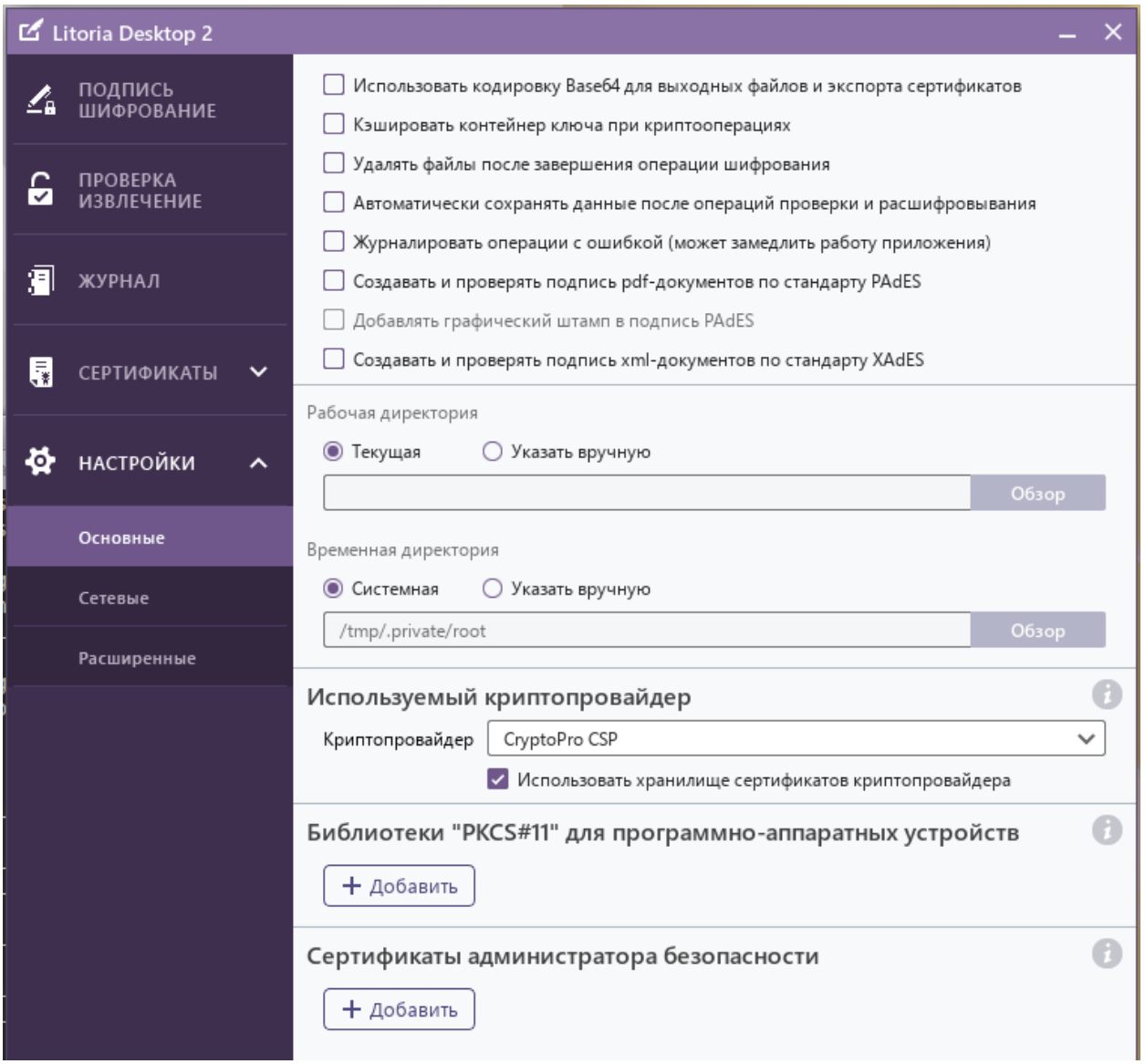


Рисунок 3.11 – Используемый криптопровайдер

Если на рабочей станции нет установленных программных криптопровайдеров, можно для работы с функциональными носителями использовать интерфейс PKCS#11 (рисунок 3.12).

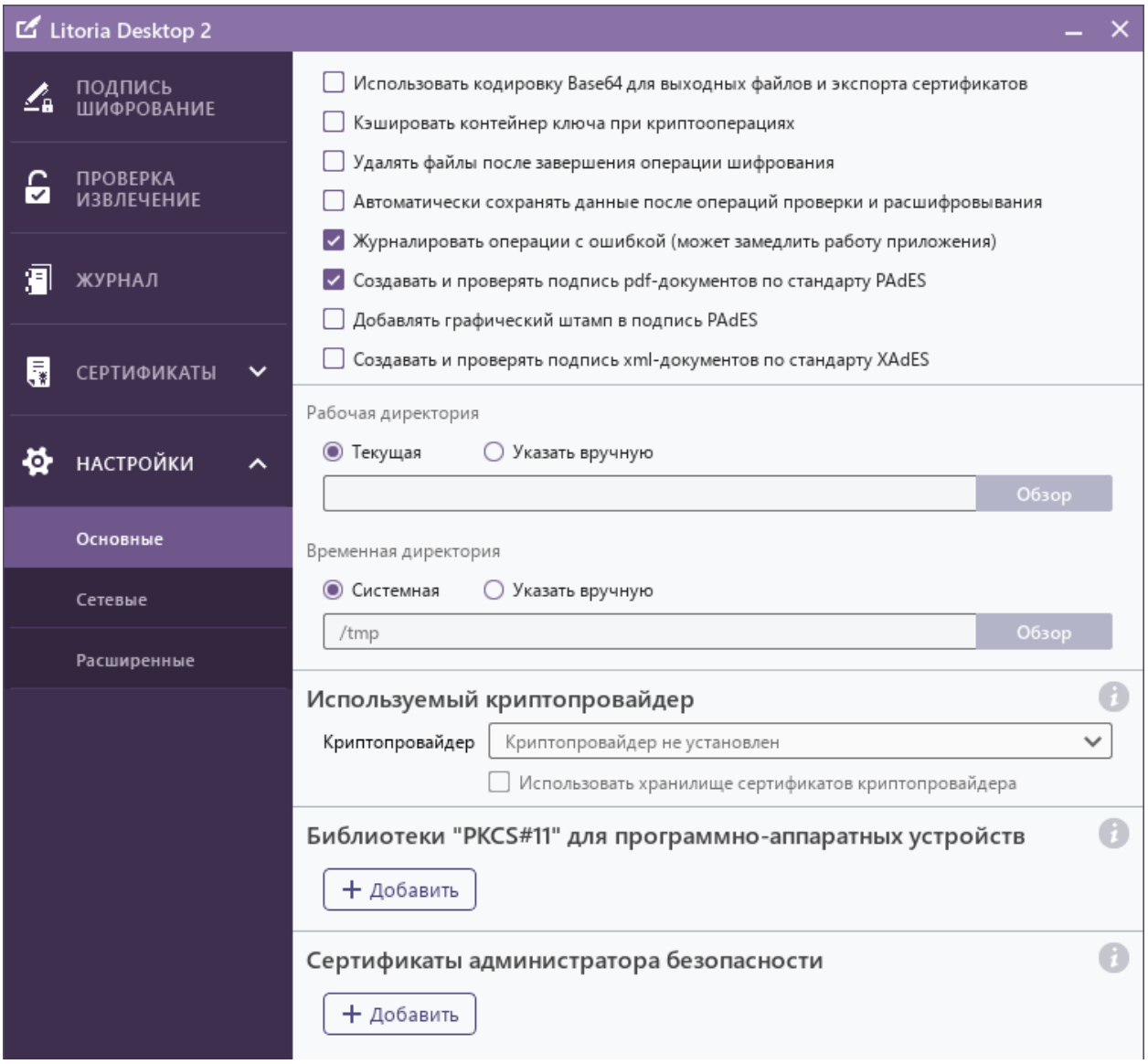


Рисунок 3.12 – Криптопровайдеры отсутствуют

Если на рабочей станции установлены и СКЗИ «КриптоПро CSP», и СКЗИ «ViPNet CSP», по умолчанию будет выбран криптопровайдер СКЗИ «КриптоПро CSP» (рисунок 3.13). При необходимости изменения значения, заданного по умолчанию, измените криптопровайдер и подтвердите перезапуск ПК «Litoria Desktop» в появившемся окне (рисунок 3.14).

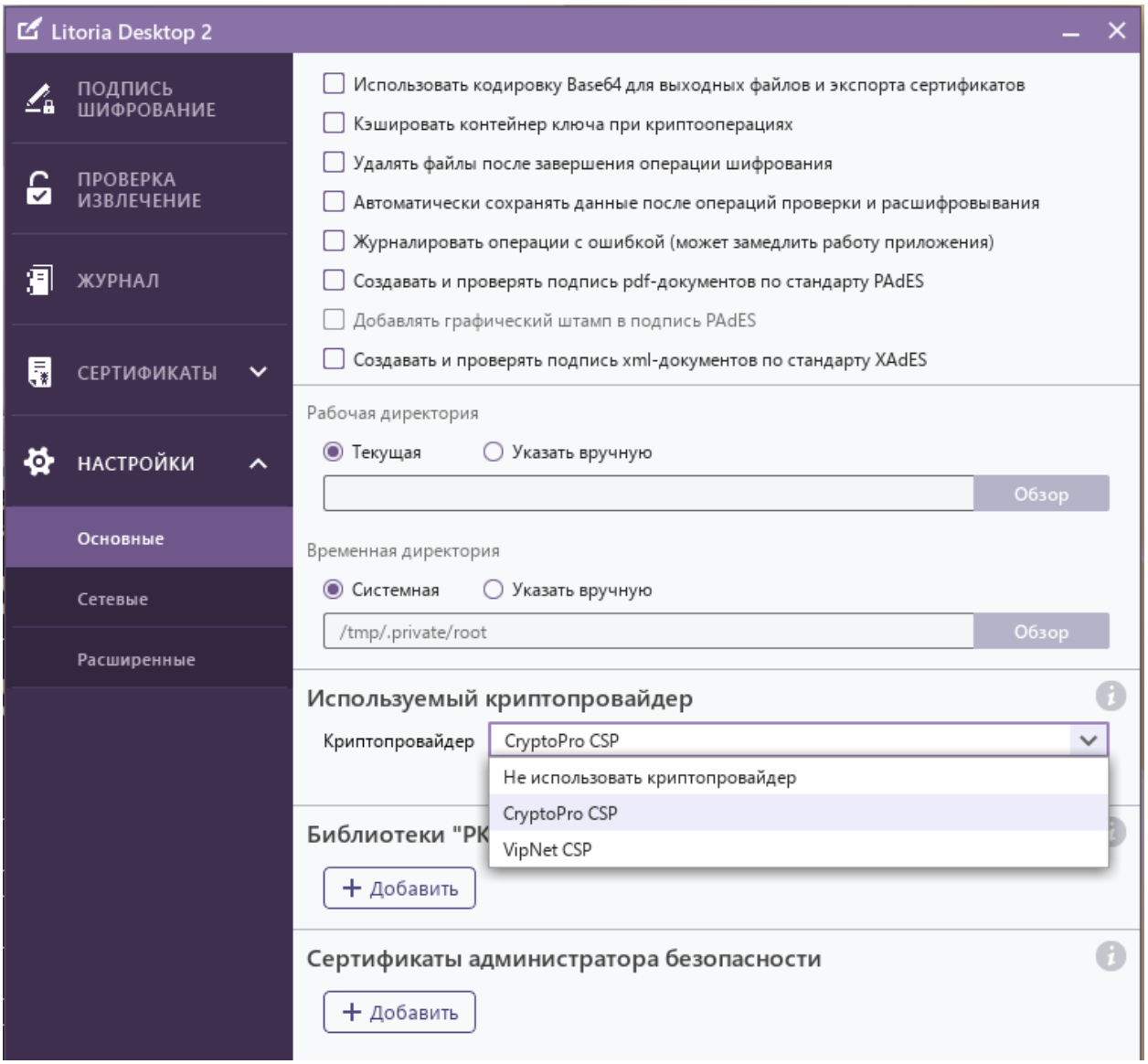


Рисунок 3.13 – Установлено несколько криптопровайдеров

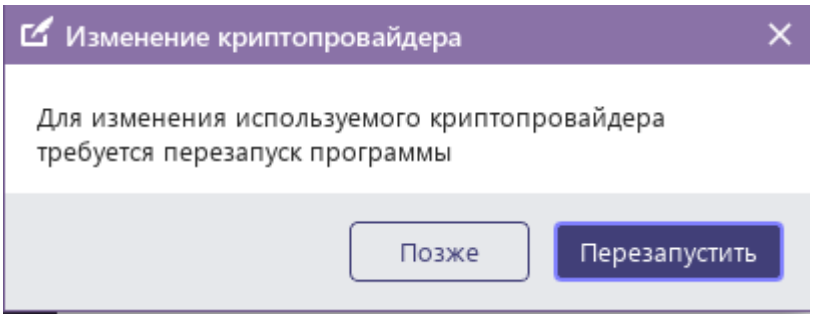


Рисунок 3.14 – Смена используемого криптопровайдера

Флаг «Использовать хранилище сертификатов криптопровайдера» (рисунок 3.13) позволяет хранить добавляемые сертификаты в хранилище установленного криптопровайдера. Если флаг не установлен, сертификаты хранятся в хранилище ПК «Litoria Desktop 2».

3.1.12 Добавление библиотек PKCS#11

Библиотеки PKCS#11 необходимо добавить перед началом работы с функциональными носителями (интерфейс PKCS#11).

Для добавления в список библиотеки, реализующей взаимодействие с необходимым аппаратным криптопровайдером, в области «*Библиотеки «PKCS#11» для программно-аппаратных устройств*» нажмите на кнопку «*Добавить*». В открывшемся окне выберите расположение необходимой библиотеки (как правило, она устанавливается при установке драйверов к устройству и расположена, например, по следующему пути: C:\windows\system32\rtpkcs11ecp.dll) (рисунок 3.15).

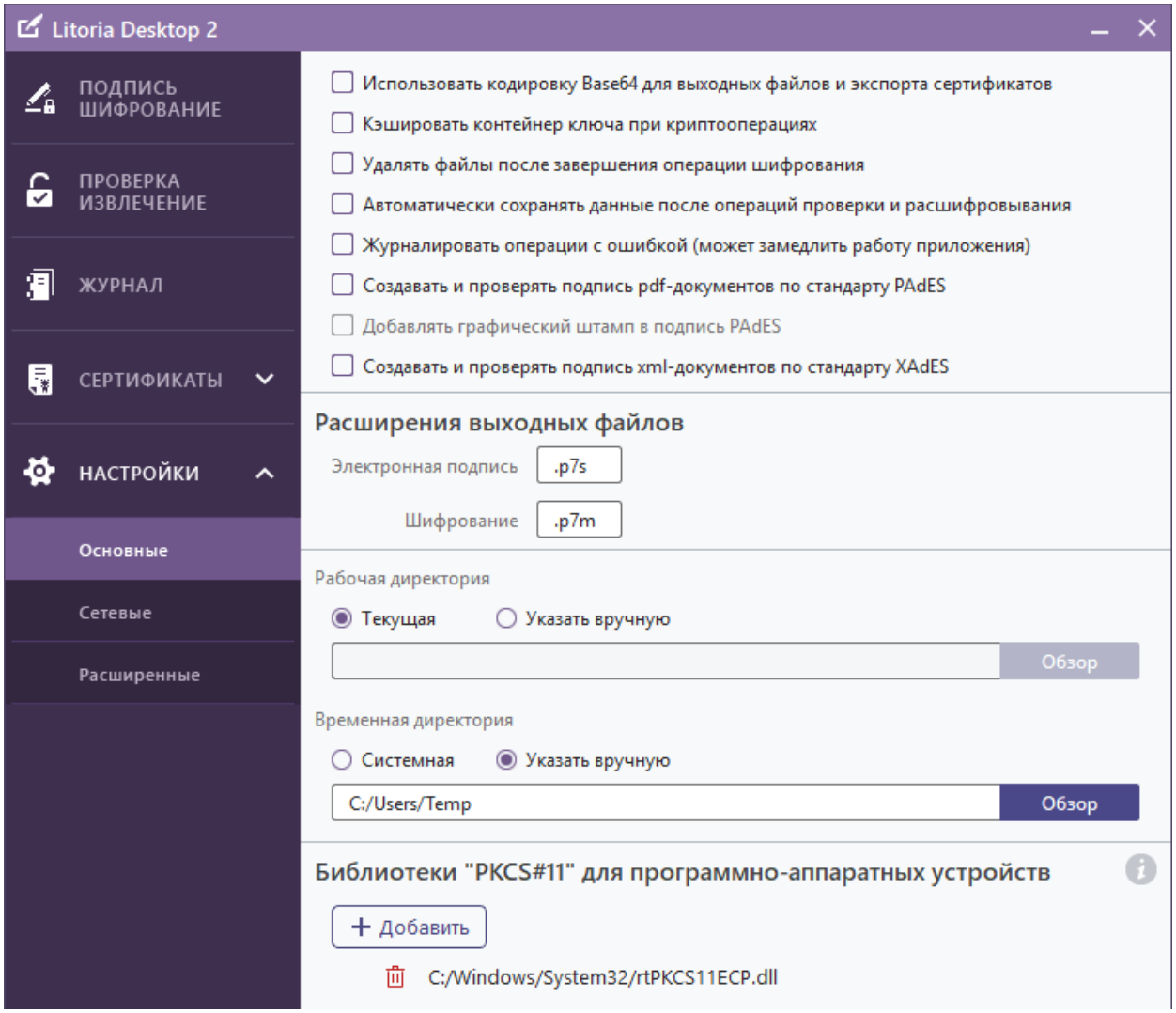


Рисунок 3.15 – Добавление библиотеки PKCS#11

3.1.13 Сертификаты администратора безопасности

В данной настройке указывается сертификат, который будет всегда добавляться в список получателей операции шифрования. При выполнении операции шифрования сертификат администратора безопасности не будет отображаться в списке получателей, но шифрование любого файла будет производиться и для этого сертификата.

Если получатель потеряет ключевой носитель с ключом ЭП, то файл сможет расшифровать владелец сертификата, указанного в данной настройке.

Добавление сертификата осуществляется с помощью кнопки «*Добавить*» в области «*Сертификаты администратора безопасности*» основных настроек.

1) При нажатии на кнопку появится окно «*Выберите сертификат(ы)*» (рисунок 3.16).

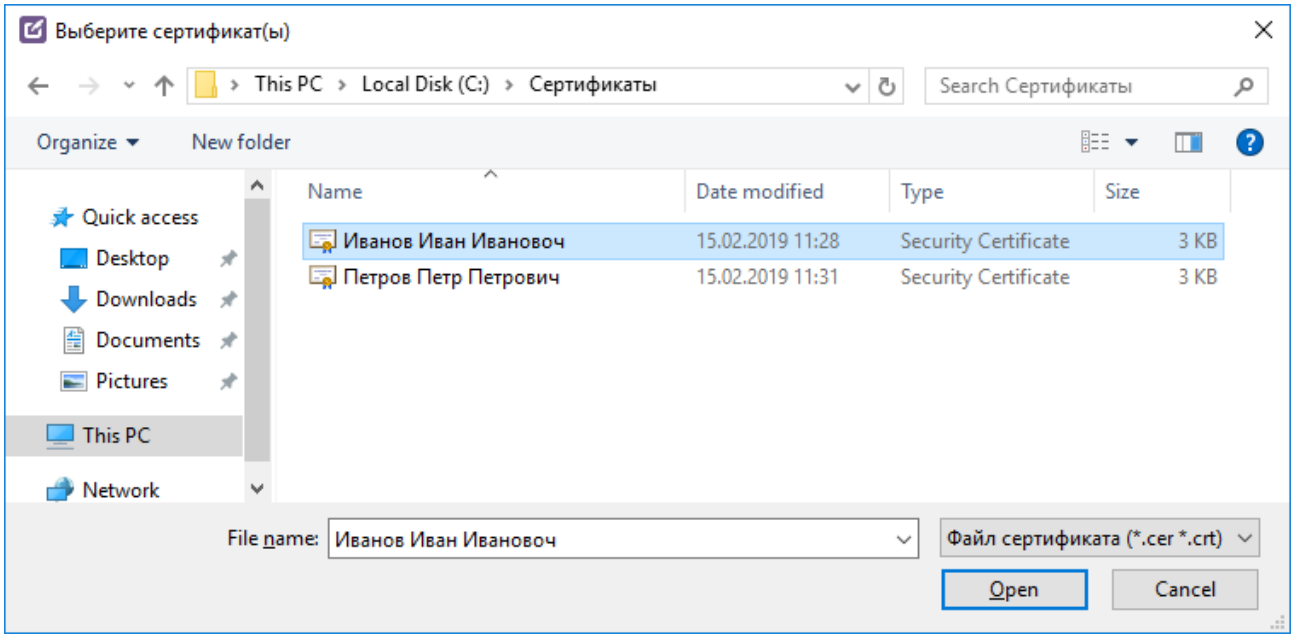


Рисунок 3.16 – Выбор сертификата администратора безопасности

2) В появившемся окне укажите файл сертификата и нажмите на кнопку «Открыть».

3) В окне основных настроек в области «Сертификаты администратора безопасности» будет отображено общее имя выбранного сертификата (рисунок 3.17).

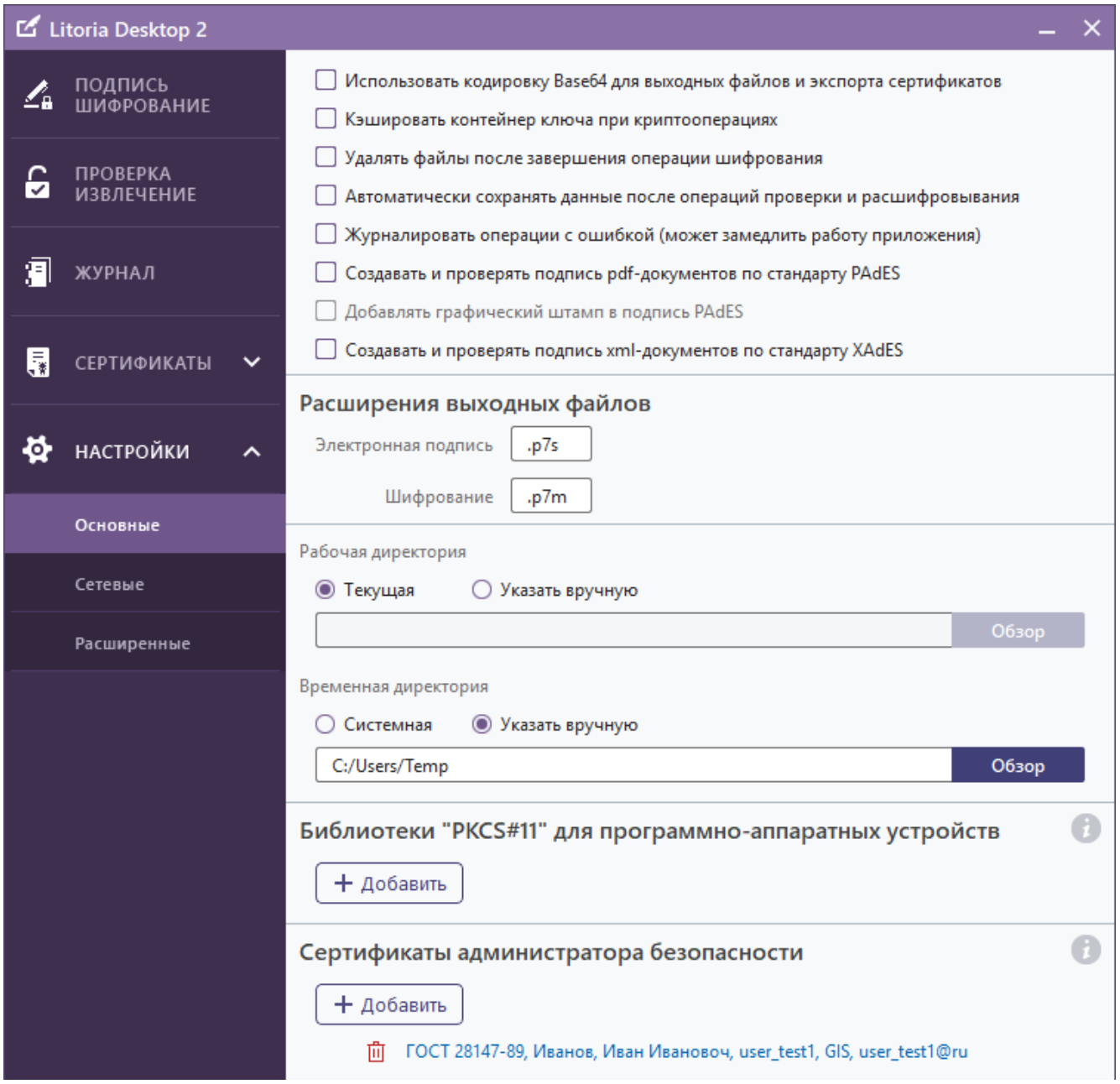


Рисунок 3.17 – Отображение выбранного сертификата администратора безопасности

Установленный сертификат администратора безопасности сохранится для всех пользователей компьютера и будет участвовать во всех операциях шифрования, выполненных любым пользователем данного компьютера, для соответствующих криптографических алгоритмов.

3.2 Сетевые настройки

Вкладка «*Сетевые настройки*» позволяет выполнять настройки:

– адреса используемой службы штампов времени;
– службы доверенной третьей стороны;

– прокси-сервера.

3.2.1 Настройки службы штампов времени

Для указания используемого адреса службы штампов времени в пункте меню «*Настройки*» вкладка «*Сетевые*» в области «*Служба штампов времени*» введите адрес, который будете использовать, в поле «*Адрес по умолчанию*» (рисунок 3.18).

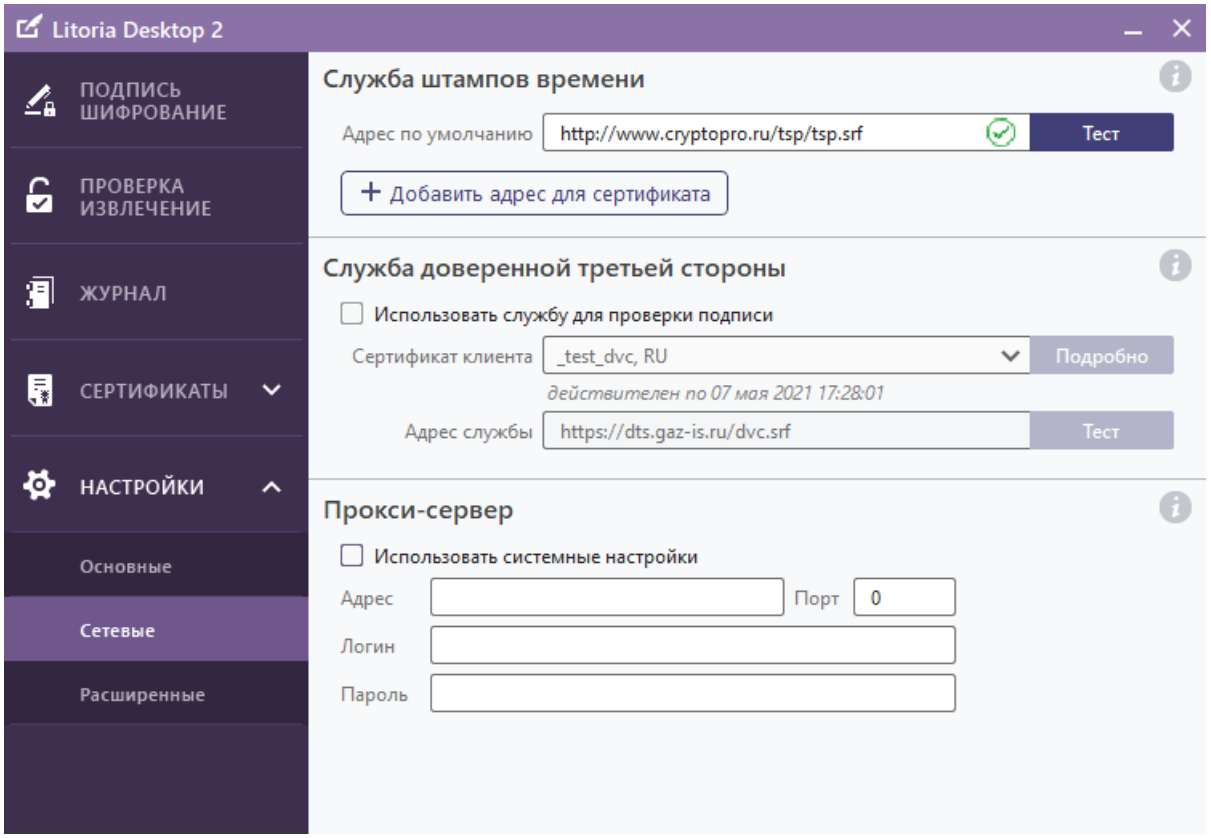


Рисунок 3.18 – Настройка адреса службы штампов времени

Для проверки работоспособности адреса службы штампов времени нажмите на кнопку «*Тест*».

При успешном соединении со службой, в поле с адресом появится значок « », указывающий на корректность введенного адреса службы штампов времени и готовность ее к использованию.

В случае возникновения ошибки (возможные варианты ошибок описаны ниже), в поле с адресом службы появится значок « » (рисунок 3.19). Подробная информация о выявленной ошибке выводится в сообщении при нажатии на значок.

Перечень возможных сообщений об ошибках:

– Формат запроса некорректный.
– Формат ответа некорректный.
– Отсутствует соединение, проверьте адрес.
– Ошибка аутентификации, проверьте сертификат.

– Нет доверия к сертификату службы.

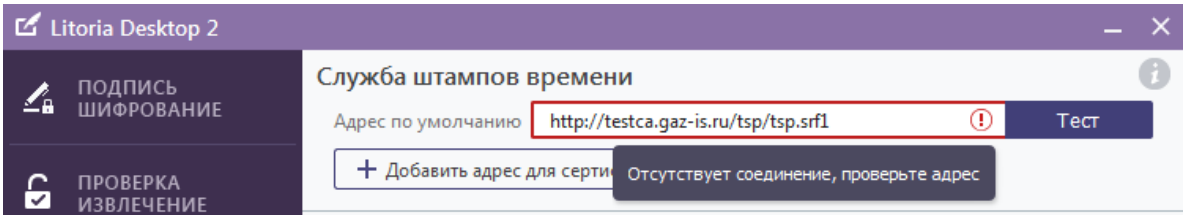


Рисунок 3.19 – Сообщение об ошибке «Отсутствует соединение»

В случае сообщения об ошибке «*Нет доверия к сертификату службы*» (рисунок 3.20), необходимо нажать на ссылку с сообщением, для получения детальной информации о сертификате службы, с дальнейшей возможностью разрешения проблемы доверия.

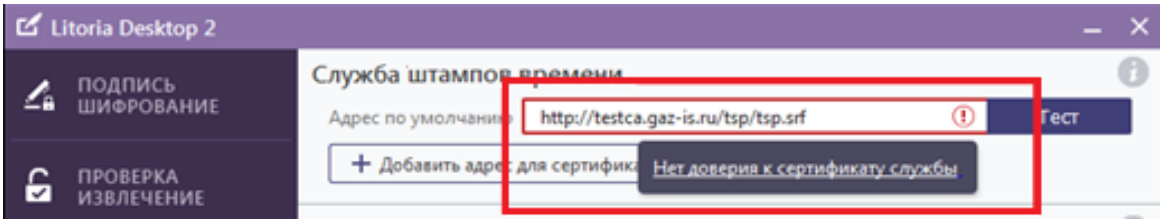


Рисунок 3.20 – Сообщение об ошибке «Нет доверия к службе»

При необходимости использовать разные адреса службы штампов времени для сертификатов, выпущенных различными УЦ, в области «*Служба штампов времени*» нажмите на кнопку «*Добавить адрес для сертификата*». Указанный адрес будет использоваться для всех сертификатов, изданных УЦ, которым был выпущен выбранный сертификат (рисунок 3.21).

Кнопка «*Добавить адрес для сертификата*» доступна при наличии в хранилище «*Личные сертификаты*» сертификатов, относящихся к разным корневым сертификатам (выпущенных разными УЦ).

Если кнопка «*Добавить адрес для сертификата*» недоступна, необходимо проверить наличие таких сертификатов в хранилище «*Личные сертификаты*», и, в случае их отсутствия, выполнить установку сертификатов. После этого ПК «Litoria Desktop 2» необходимо перезапустить.

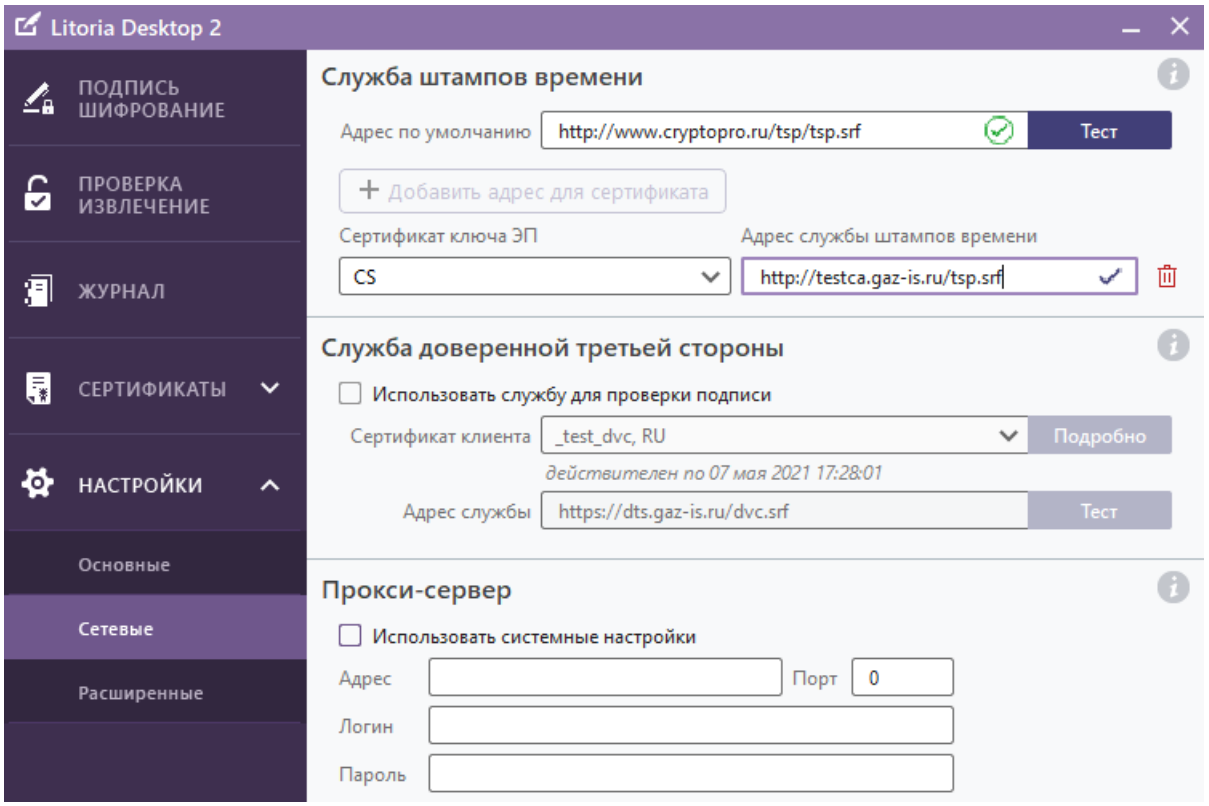


Рисунок 3.21 – Добавление адреса службы штампов времени для сертификата

3.2.2 Настройки службы доверенной третьей стороны

Для проверки подписи с использованием службы ДТС необходимо установить флаг «*Использовать службу для проверки подписи*» в области «*Служба доверенной третьей стороны*» (рисунок 3.22). При этом станут доступными для заполнения поля «*Сертификат клиента*» и «*Адрес службы*».

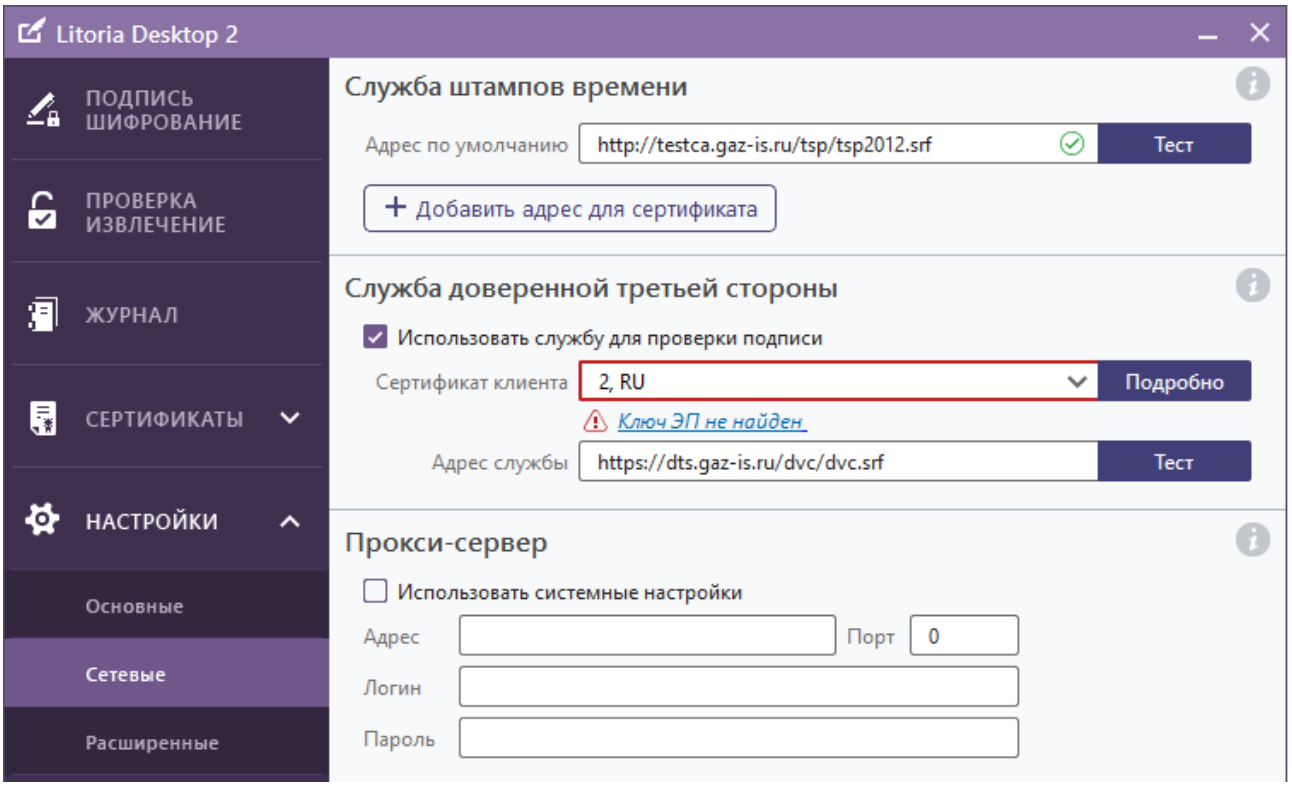


Рисунок 3.22 – Настройки службы доверенной третьей стороны

Для указания сертификата для подключения к службе ДТС в поле «*Сертификат клиента*» выберите из списка сертификат, который ранее был установлен в хранилище сертификатов *«Личные сертификаты»* и зарегистрирован на сервере ДТС.

Если ключ ЭП выбранного сертификата не будет обнаружен в доступных контейнерах, то внизу поля появится сообщение «*Ключ ЭП не найден*» (рисунок 3.22).

Для ввода ПИН-кода нажмите на ссылку «*Ключ ЭП не найден*» и в появившемся окне укажите в соответствующем поле ПИН-код к контейнеру (рисунок 3.23) и нажмите на кнопку «*Проверить*».

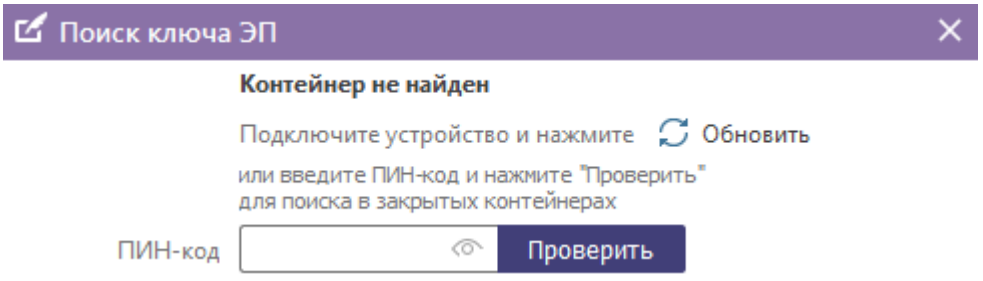


Рисунок 3.23 – Поиск ключа ЭП

Если ПИН-код к контейнеру не был найден, проверьте наличие физического отчуждаемого носителя в нужном разъеме (при его использовании) и нажмите кнопку «*Обновить*» (рисунок 3.23).

Если данные указаны верно, внизу поля с сертификатом появится сообщение о сроке действия сертификата (рисунок 3.24). Сертификат готов к использованию.

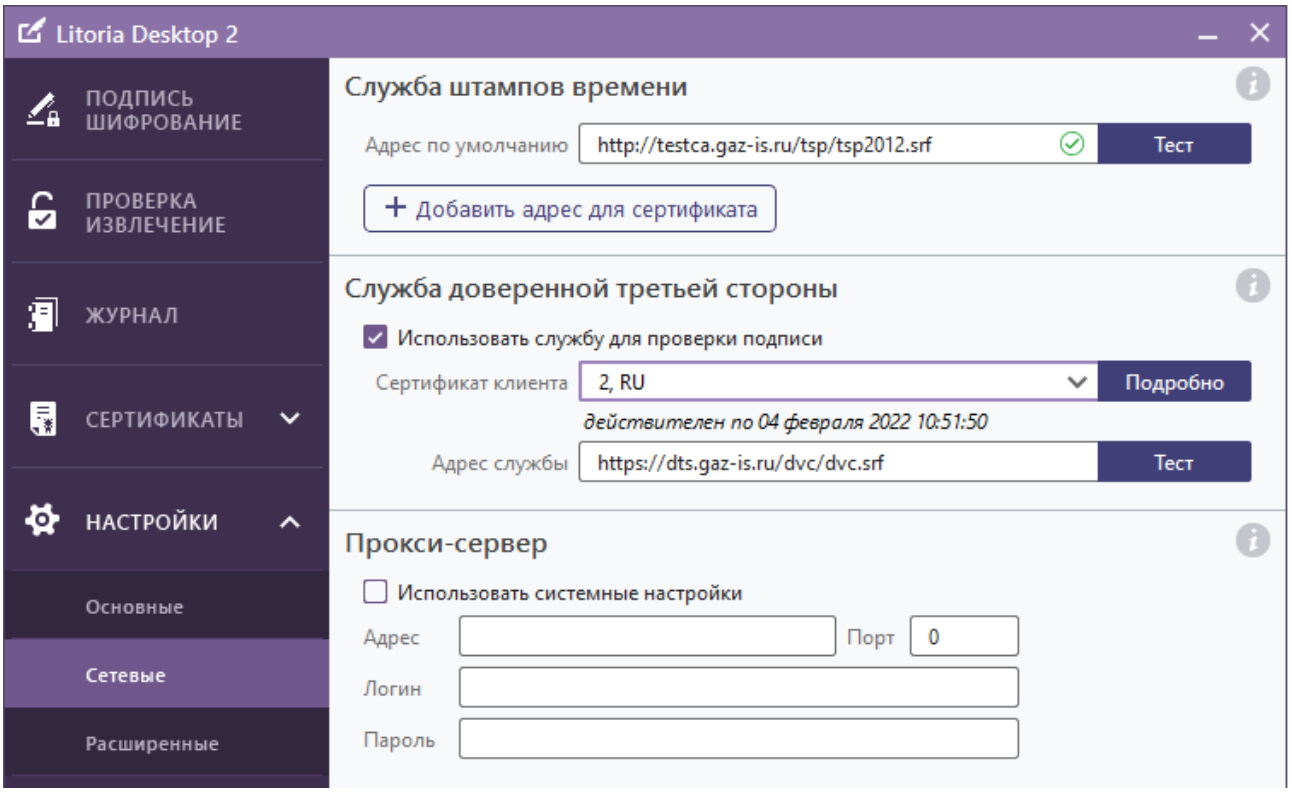


Рисунок 3.24 – Готовность сертификата к использованию

В поле «*Адрес службы*» введите адрес клиента ДТС, который будет использоваться по умолчанию и проверьте его работоспособность по нажатию кнопки «*Тест*».

При успешном соединении со службой в поле с адресом появится значок « » (рисунок 3.25), указывающий на корректность введенного адреса службы доверенной третьей стороны и готовность ее к использованию.

В случае возникновения ошибки, в поле с адресом службы появится значок « ». Подробная информация о выявленной ошибке выводится в сообщении при нажатии на значок (возможные варианты ошибок описаны в п.3.2.1).

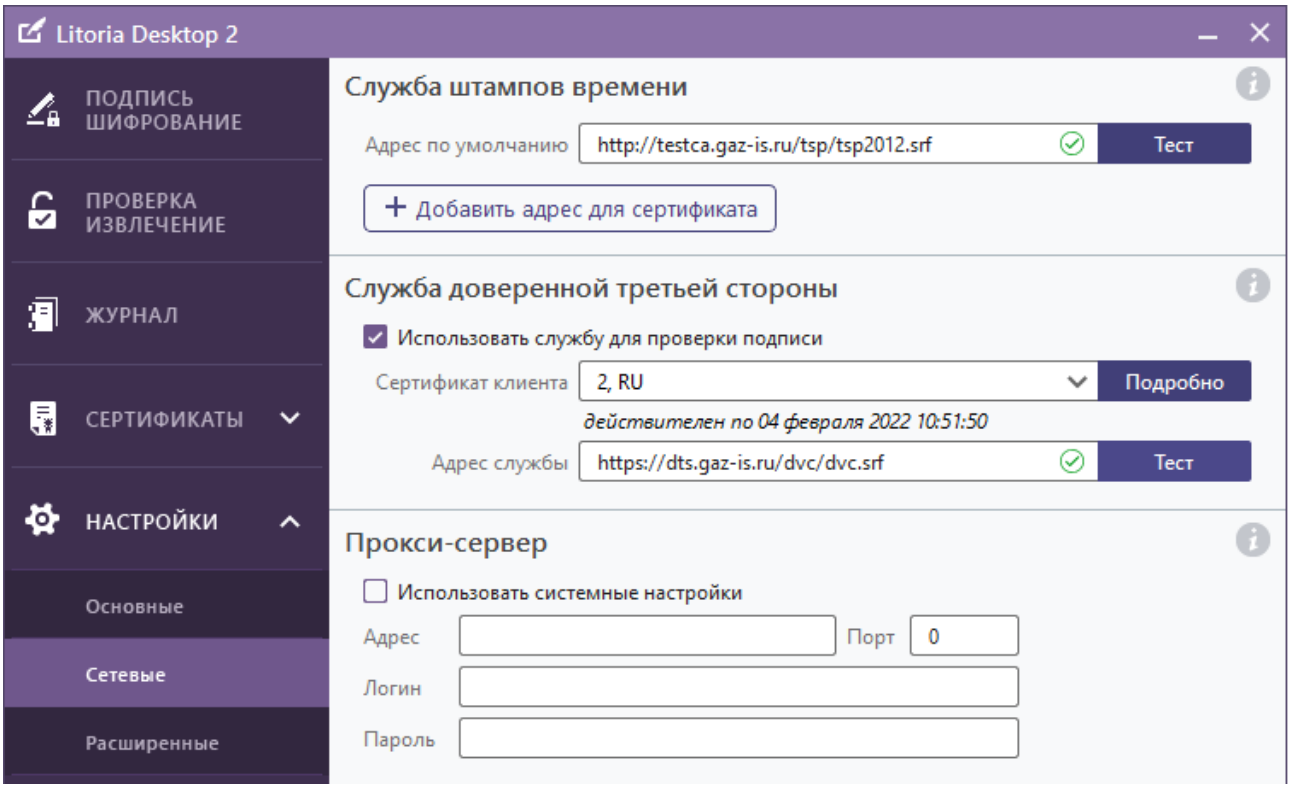


Рисунок 3.25 – Проверка работоспособности службы доверенной третьей стороны

Сертификат клиента службы ДТС необходимо ввести до тестирования работоспособности службы по кнопке «*Тест*».

При внесении изменений в настройки подключения к службе ДТС (изменение сертификата подключения или адреса службы) необходима проверка работоспособности службы по кнопке «*Тест*».

В случае, если при проверке подписи с использованием службы ДТС (в настройках установлен флаг «*Использовать службу для проверки подписи*»), в строке проверяемого файла отображается статус «*Ошибка настроек*» (рисунок 3.26), необходимо перейти в настройки службы ДТС и убедиться в работоспособности службы (наличие в поле с адресом службы значка « »).

Отсутствие значка « » в поле с адресом службы может означать, что были внесены изменения в настройки подключения к службе ДТС, при этом проверка работоспособности службы по кнопке «*Тест*» не была произведена.

Подтвердите корректность адреса службы и сертификата подключения и нажмите кнопку «*Тест*» для проверки.

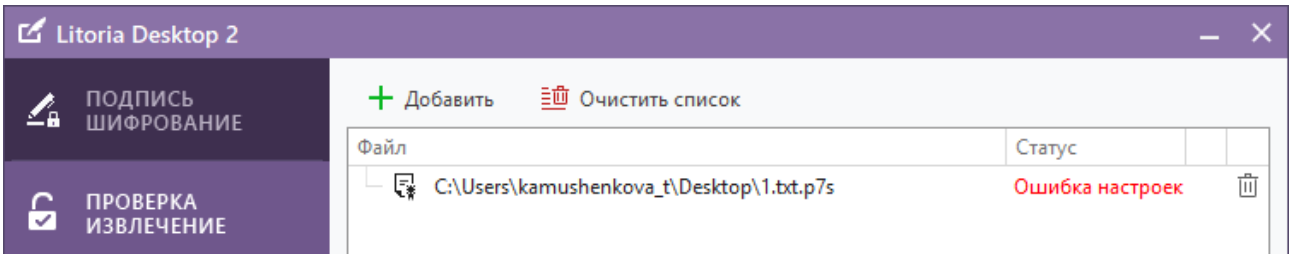


Рисунок 3.26 – Необходимость в настройке параметров службы ДТС

3.2.3 Настройки сети

Для настройки аутентификации на прокси-сервере в пункте меню «*Настройки*», во вкладке «*Сетевые*» в области «*Прокси-сервер*» установите флаг «*Использовать системные настройки*». Укажите в соответствующих полях имя пользователя и пароль. В полях «*Адрес*» и «*Порт*» отображаются значения, ранее указанные в настройках сети интернет-браузера (рисунок 3.27).

Отсутствие значений в полях «*Адрес*» и «*Порт*» в настройках сети комплекса означает, что на рабочей станции для подключения к прокси-серверу используется автоматическая настройка и ПК «Litoria Desktop 2» не сможет выполнить подключение к прокси-серверу. Чтобы комплекс мог выполнить подключение к прокси-серверу и использовать системную прокси-аутентификацию, следует изменить настройки сети интернет-браузера, если это возможно. В настройках сети браузера следует установить флаг «*Использовать прокси-сервер для локальных подключений (…)*» и указать адрес и порт прокси-сервера.

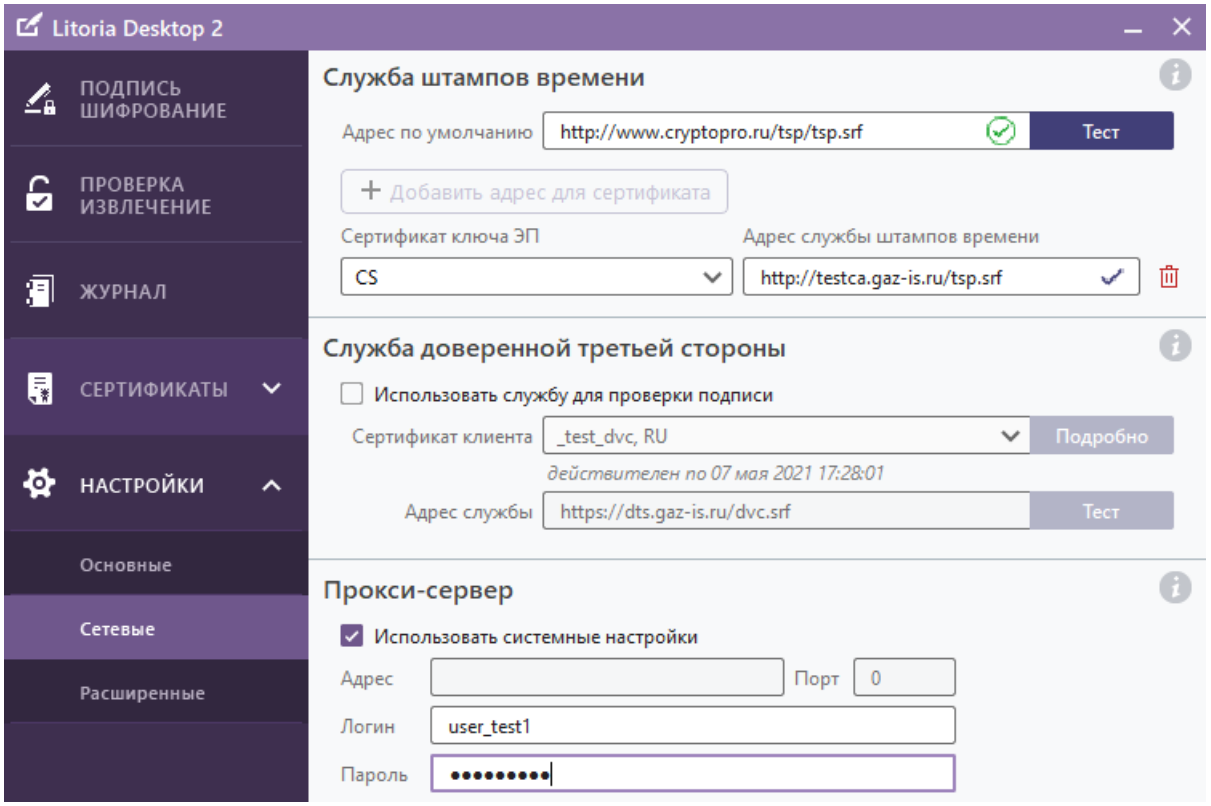


Рисунок 3.27 – Настройки прокси-сервера

3.3 Расширенные настройки

Вкладка «*Расширенные настройки*» позволяет выполнять настройки использования квалифицированного режима, настраивать ограничения использования сертификата, добавлять возможность продления срока действия ЭП и устанавливать язык интерфейса ПК «Litoria Desktop 2».

3.3.1 Квалифицированный режим

Для использования квалифицированного режима, необходимо зайти в пункт меню «*Настройки*» вкладка «*Расширенные*» и в области «*Квалифицированный режим*» установить флаг «*Включить режим квалифицированной подписи*» (рисунок 3.28).

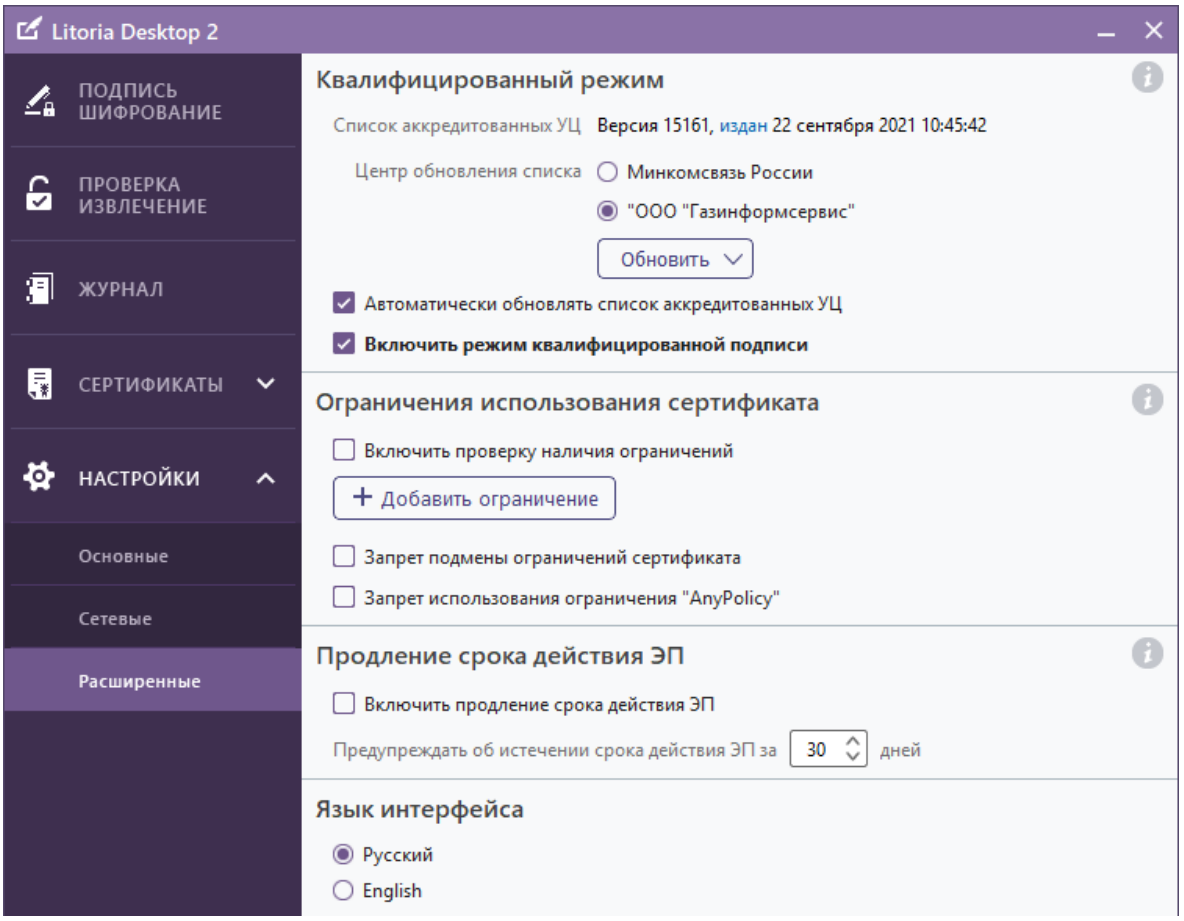


Рисунок 3.28 – Настройка использования квалифицированного режима

3.3.1.1 Предварительные настройки для работы в квалифицированном режиме

Для использования квалифицированного режима работы необходимо, чтобы были выполнены следующие условия:

1. Квалифицированный режим может использоваться только при наличии актуального списка аккредитованных УЦ (tsl-списка). При отсутствии списка или запрете доступа к нему, включение режима квалифицированной подписи недоступно (рисунок Рисунок 3.29).

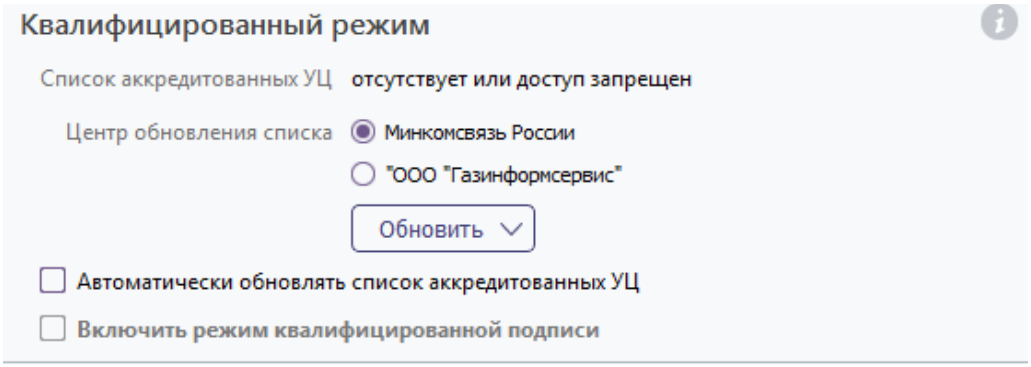


Рисунок 3.29 – Список аккредитованных УЦ отсутствует или доступ запрещен

2. Перед использованием квалицированного режима необходимо установить цепочку сертификатов (доверенный корневой сертификат и списки отзыва сертификатов) в хранилище сертификатов с сайта Минкомсвязи РФ. Скачать актуальную цепочку сертификатов можно по ссылке ***https://e-trust.gosuslugi.ru/#/portal/mainca***.

3. Перед загрузкой tsl-списка в ОС семейств Windows необходимо предварительно установить в хранилище локального компьютера «Доверенные корневые центры сертификации» сертификат "Russian Trusted Root CA" к ssl-сертификату сайта, с которого скачивается tsl-список (рисунок 3.30).

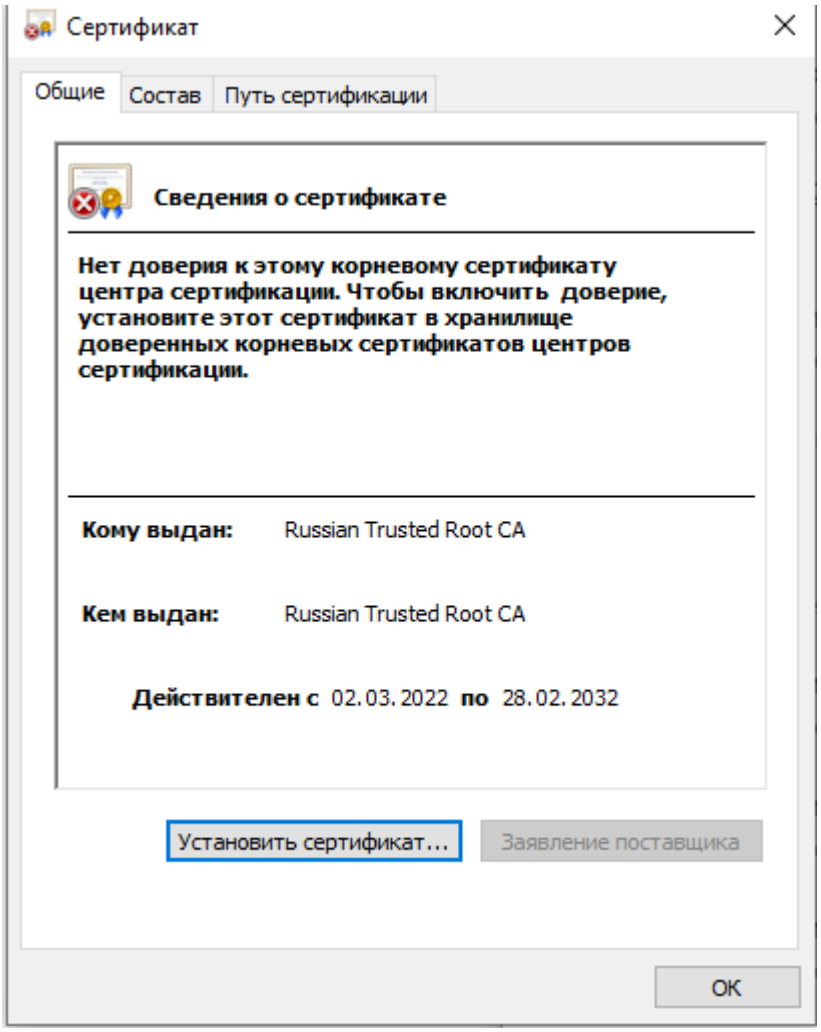


Рисунок 3.30 – Установка корневого сертификата

4. Перед загрузкой tsl-списка в ОС семейств Linux необходимо предварительно выполнить установку корневого сертификата "Russian Trusted Root CA" к ssl-сертификату сайта, с которого скачивается tsl-список:

– в ОС «Astra linux 1.6» необходимо положить сертификат (в base64 с тегами) в */usr/local/share/ca-certificates/*, затем из-под пользователя root зайти в каталог */usr/sbin* и выполнить команду:

./update-ca-certificates –fresh

– в ОС «Redos 7.3.1» необходимо выполнить команду:

su -

dnf install ca-certificates-ru

(источник https://redos.red-soft.ru/base/arm/arm-other/russian-ssl-sert/)

– в ОС «Alt 10» необходимо поместить файл сертификата в */etc/pki/ca-trust/source/anchors/* и обновить общесистемный список доверенных центров сертификации командой:

 # update-ca-trust

(источник https://www.altlinux.org/%D0%A3%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B0_%D0%BA%D0%BE%D1%80%D0%BD%D0%B5%D0%B2%D0%BE%D0%B3%D0%BE_%D1%81%D0%B5%D1%80%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%82%D0%B0)

5. Перед загрузкой tsl-списка необходимо убедиться в правильности адреса скачивания. Для этого в реестре ОС перейдите в раздел «HKEY_LOCAL_MACHINE\SOFTWARE\GIS\litoria»[9] и убедитесь, что поле «MKS_TSL_Source» содержит значение «***https://e-trust.gosuslugi.ru/app/scc/portal/api/v1/portal/ca/getxml***». Если значение соответствует указанному, но список аккредитованных УЦ не загружается, необходимо обратиться в техническую поддержку ПК для уточнения адреса скачивания списка.

6. Если при очередной загрузке списка аккредитованных УЦ сертификат, которым подписывается список аккредитованных УЦ, был изменен, то в поле «Список аккредитованных УЦ» появится сообщение о том, что список выпущен сторонним сертификатом (рисунок 3.31).

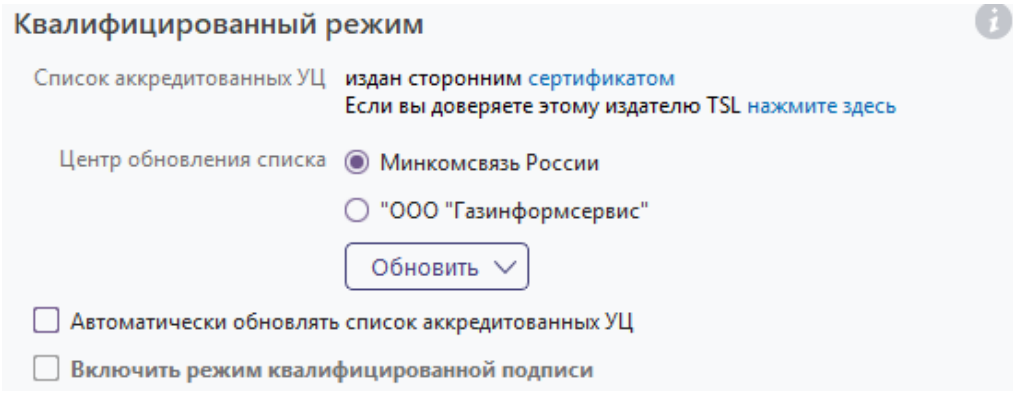


Рисунок 3.31 – Список аккредитованных УЦ выпущен сторонним сертификатом

Для изменения эталонного сертификата издателя списка аккредитованных УЦ нажмите на ссылку «*нажмите здесь*». Сертификат издателя, хранящийся в BASE64 кодировке в реестре ОС в разделе: «HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\GIS\litoria\TSL_Certificate», будет изменен на сертификат, которым подписан загруженный список. В поле *«Список аккредитованных УЦ»* будет отображена новая версия сертификата (рисунок 3.28).

[9] Если разрядность версии ОС Windows и ПК «Litoria Desktop 2» не совпадают в разделе реестра ОС "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\GIS\litoria".

3.3.1.2 Настройка работы со списком аккредитованных УЦ

Актуальный список аккредитованных УЦ возможно загрузить:

– автоматически;

– вручную (при этом доступна загрузка списка онлайн или локально из выбранного файла).

Для автоматической загрузки списка аккредитованных УЦ необходимо установить флаг «*Автоматически обновлять список аккредитованных УЦ*» (по умолчанию флаг установлен) и выбрать центр обновления списка (Минкомсвязь России или ООО «Газинформсервис»), установив переключатель в нужную позицию (рисунок 3.32).

Для обновления списка аккредитованных УЦ вручную с сайта Минкомсвязи России или ООО «Газинформсервис» необходимо выбрать центр обновления списка, установив переключатель в нужную позицию, нажать кнопку «*Обновить*» и выбрать «*Онлайн*» (рисунок 3.33).

Для обновления списка аккредитованных УЦ локально из выбранного файла необходимо нажать кнопку «*Обновить*», выбрать «*Файл*» (рисунок 3.32) и в появившемся окне «*Выберите файл TSL*» указать файл, содержащий список аккредитованных УЦ (рисунок 3.34).

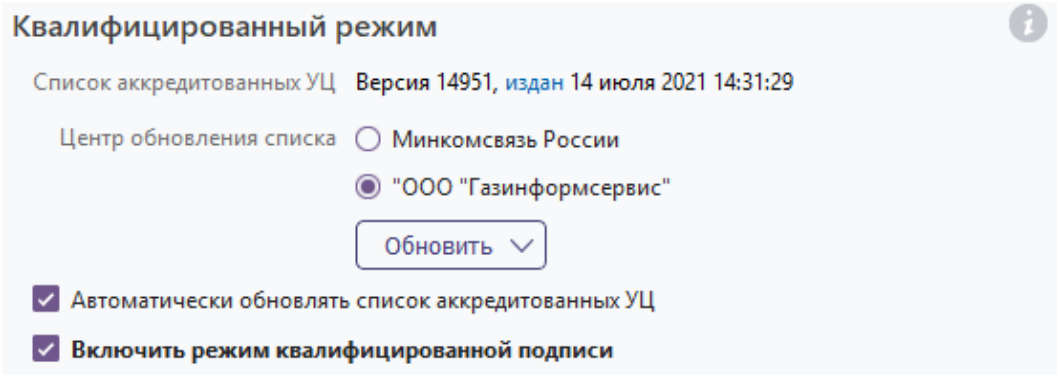


Рисунок 3.32 – Автоматическое обновление списка аккредитованных УЦ

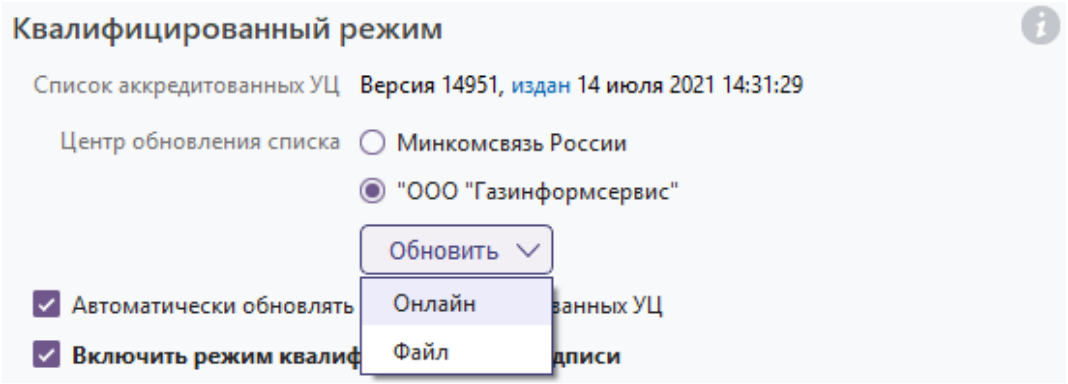


Рисунок 3.33 – Обновление списка аккредитованных УЦ онлайн

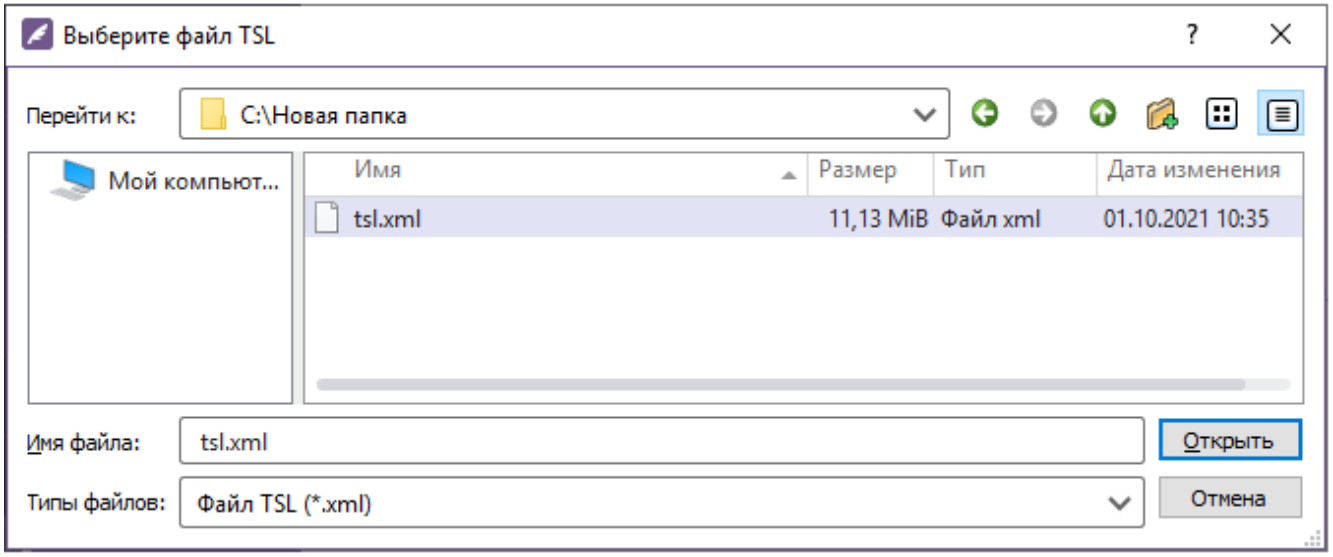


Рисунок 3.34 – Выбор файла со списком аккредитованных УЦ

По ссылке «*издан*» (рисунок 3.32) возможно просмотреть и проверить на действительность сертификат, выпустивший список аккредитованных УЦ (рисунок 3.35).

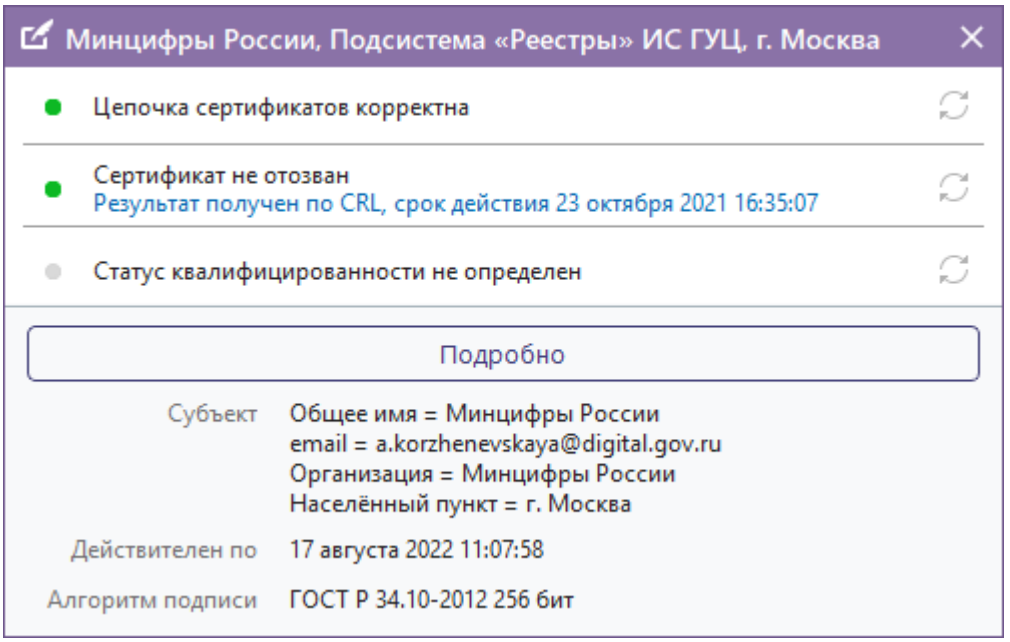


Рисунок 3.35 – Просмотр сертификата Минкомсвязи России

3.3.2 Ограничения использования сертификата

Для указания политик сертификата, определяющих правила его использования, во вкладке «*Расширенные*» в области «*Ограничения использования сертификата*» нажмите «*Добавить ограничение*», в появившемся поле введите значение требуемого идентификатора (например, 2.5.29.32.0) и нажмите на «✓» (рисунок 3.36).

Добавленный идентификатор отобразится в области «*Ограничения использования сертификата*».

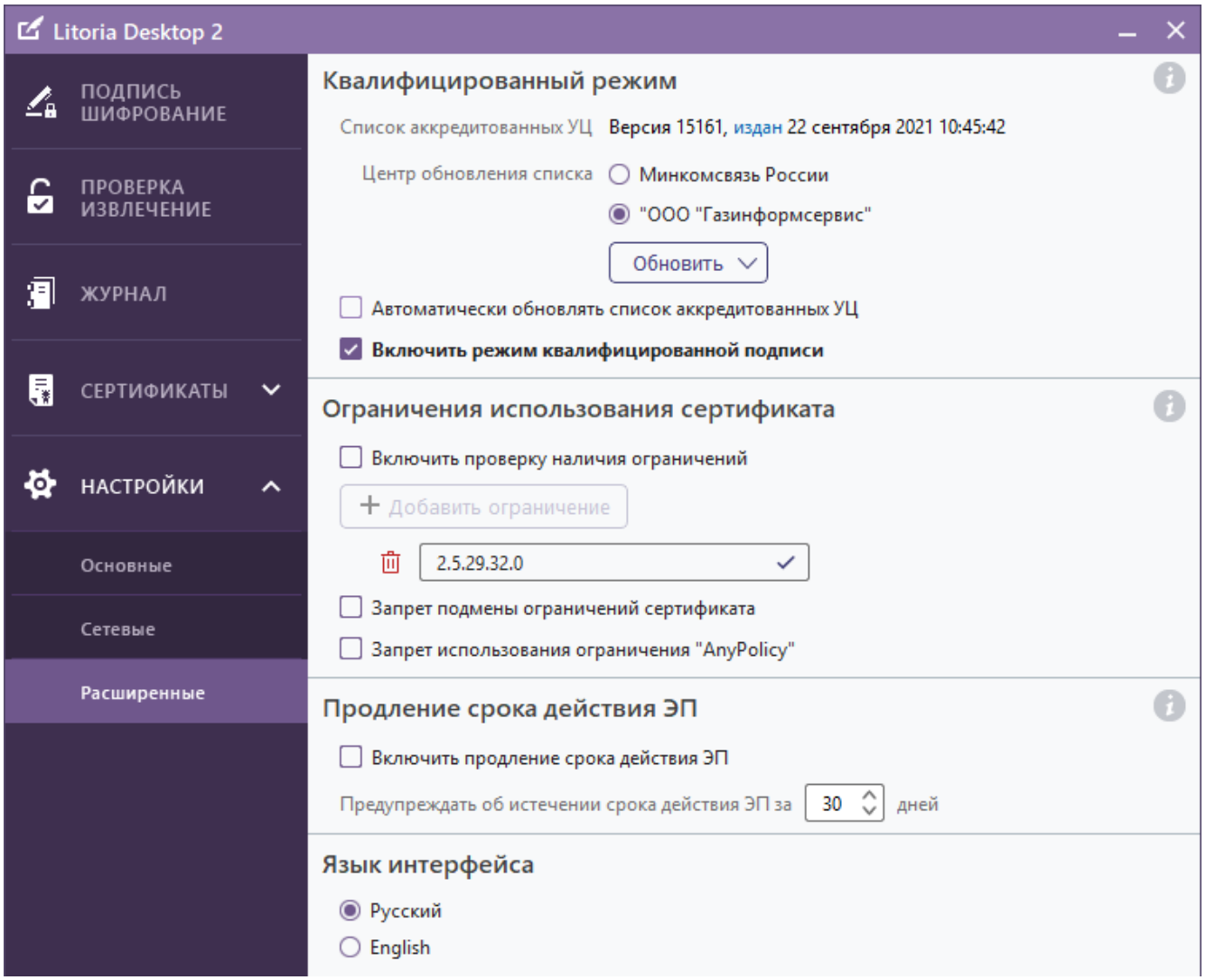


Рисунок 3.36 – Добавление пользовательской политики

Назначение флагов, доступных к установке в области *«Ограничения использования сертификата»,* описано ниже:

– «*Включить проверку наличия ограничений*» – если необходимо, чтобы выполнялась проверка наличия у сертификатов политик, указанных в расширениях (рисунок 3.36);

– «*Запрет подмены ограничений сертификата*» – если необходимо запретить использование отображения политик при построении цепочки сертификации и проверке его статуса;

– «*Запрет использования ограничения «AnyPolicy*» – если необходимо запретить использование сертификатов, в которых указана политика применения AnyPolicy (идентификатор 2.5.29.32.0).

3.3.3 Продление срока действия ЭП

Для включения продления срока действия ЭП необходимо зайти в пункт меню

«*Настройки*» вкладка «*Расширенные*», в области «*Продление срока действия ЭП*» установить флаг «*Включить продление срока действия ЭП*» (рисунок 3.37).

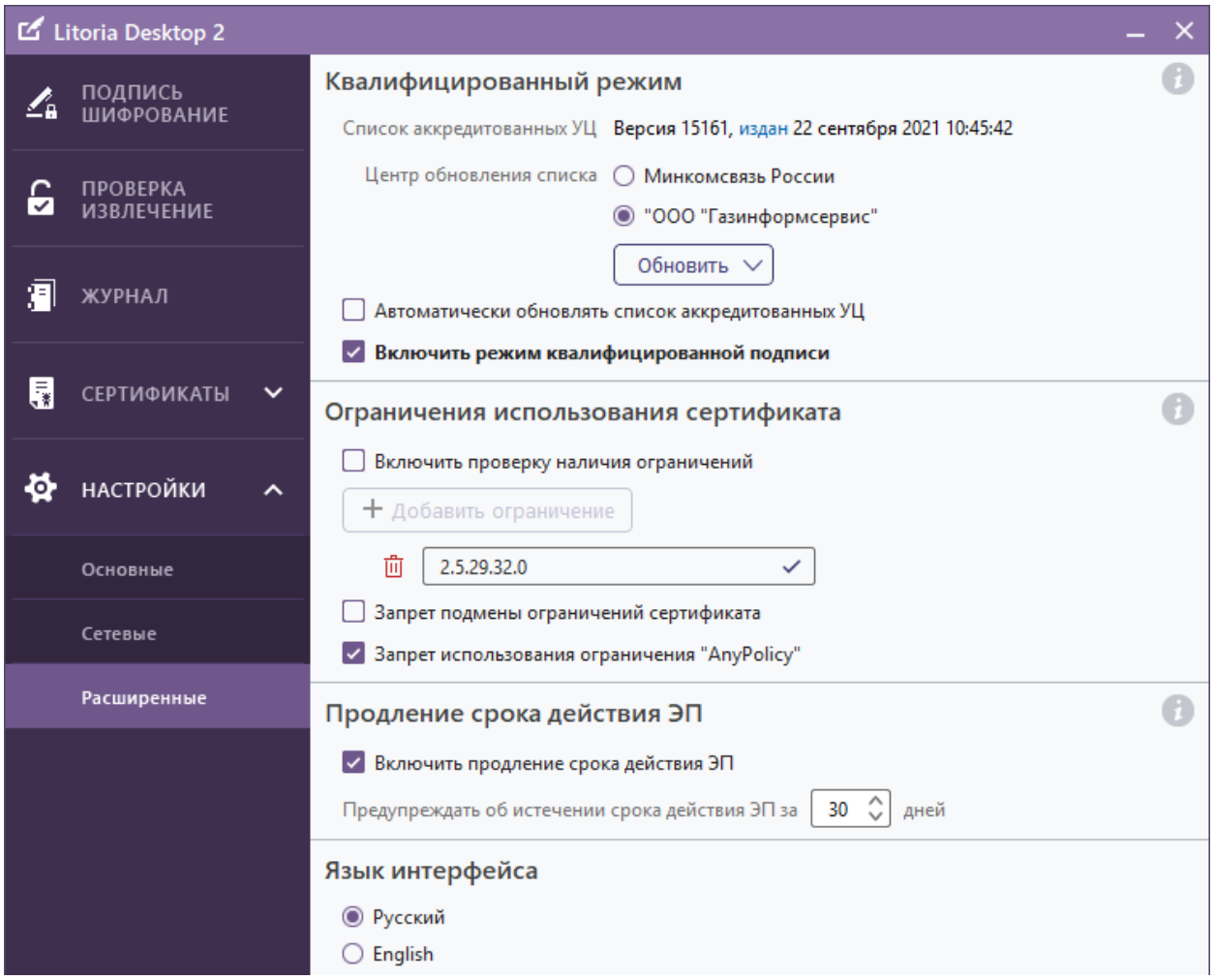


Рисунок 3.37 – Включение продления срока действия ЭП

Включение данной настройки позволяет продлевать ЭП, срок действия которых истекает в соответствии с установленным количеством дней, за которое выдается предупреждение об истечении (рисунок 3.38).

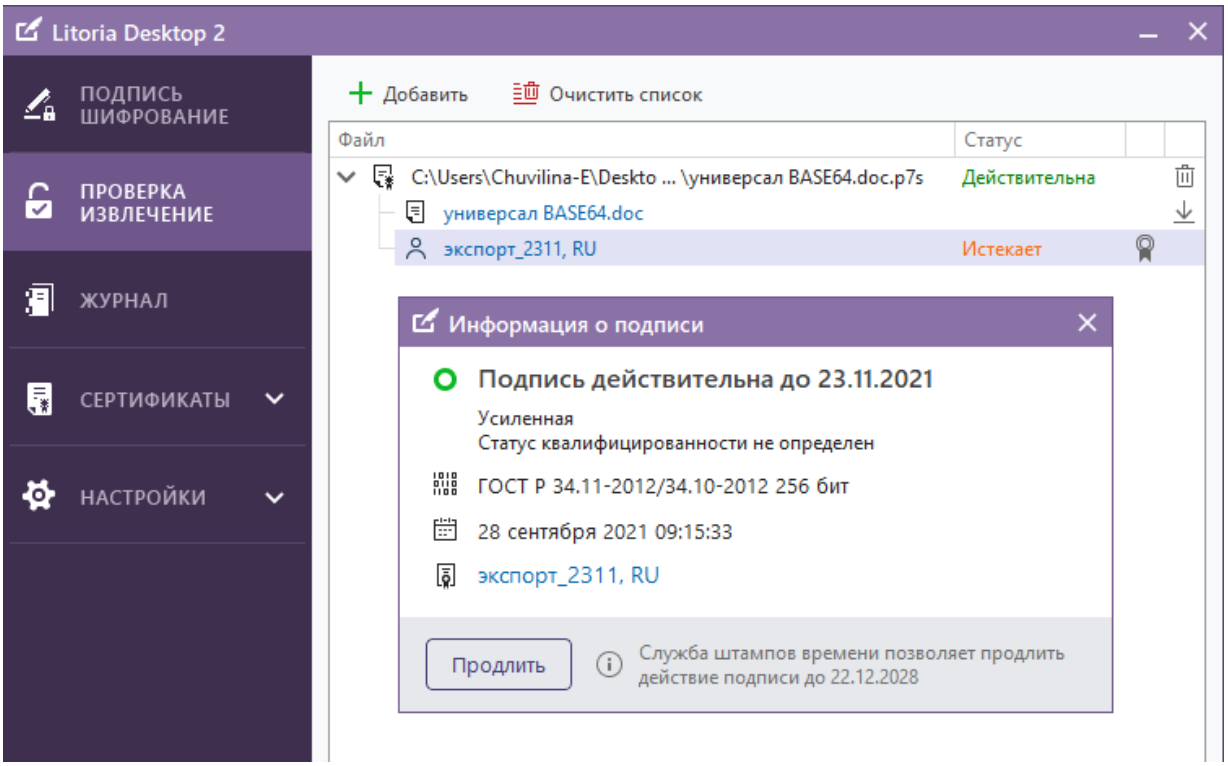


Рисунок 3.38 – Продление срока действия истекающей ЭП

По умолчанию продление срока действия ЭП выключено, кнопка продления не отображается, предупреждение об истечении срока действия ЭП (рисунок 3.39) выдается за 30 дней до истечения.

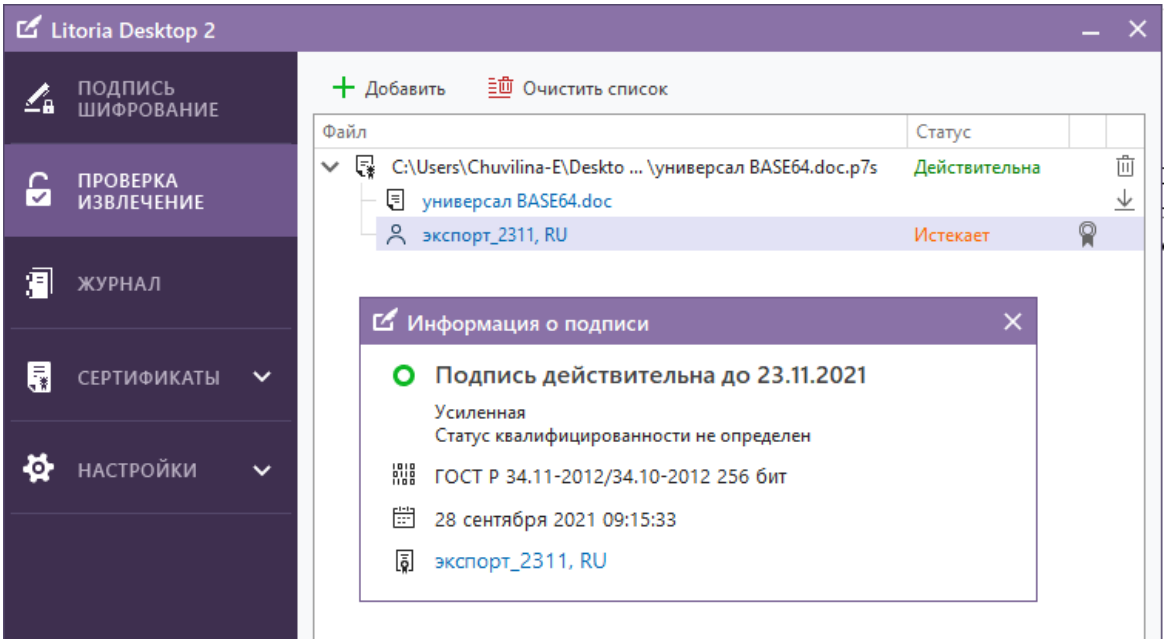


Рисунок 3.39 – Предупреждение об истечении срока действия ЭП

3.3.4 Язык интерфейса ПК «Litoria Desktop 2»

По умолчанию язык интерфейса ПК «Litoria Desktop 2» устанавливается в соответствии с языком используемой ОС.

Для смены языка интерфейса во вкладке «*Расширенные*» в области «*Язык интерфейса*» установите переключатель в нужную позицию и в появившемся окне выберите перезапуск программы в данный момент или вручную позже (рисунок 3.40). Изменения вступят в силу после перезагрузки ПК «Litoria Desktop 2».

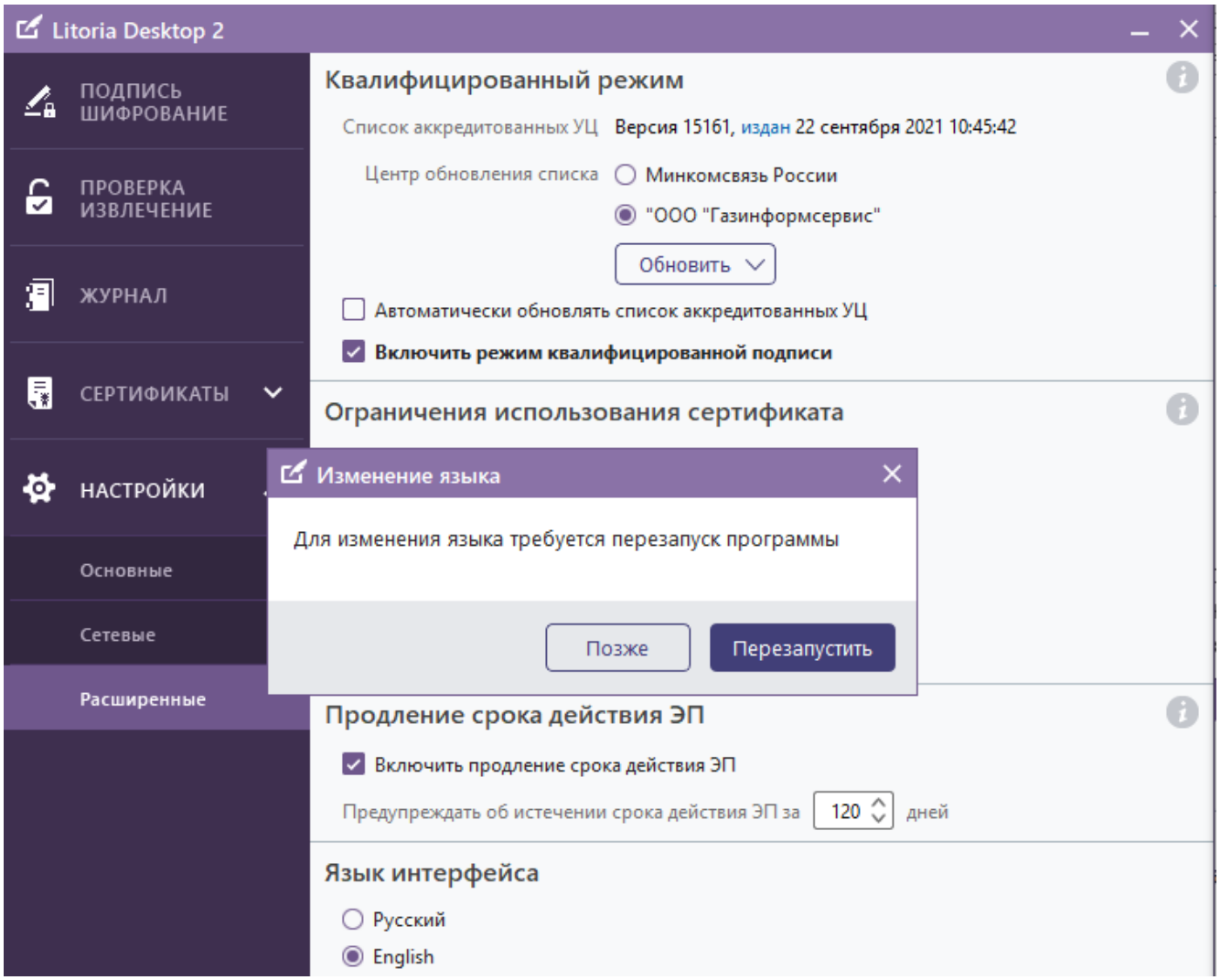


Рисунок 3.40 – Смена языка интерфейса

4 Создание шаблонов для запросов на сертификаты

Программный комплекс «Litoria Desktop 2» позволяет пользователю создавать запросы на сертификаты с использованием шаблонов. ПК «Litoria Desktop 2» содержит базовый набор шаблонов, включающий в себя перечень различных комбинаций параметров сертификата, достаточный для создания большинства запросов на сертификат, используемых пользователем.

При потребности создания пользовательского шаблона, отличного от базового набора шаблонов, необходимо добавить вновь создаваемый шаблон в файл *templates.xml*, расположенный по пути: *C:\Program Files\GIS\Litoria Desktop 2* (Приложение 1. Содержание файла templates.xml).

Пример секции с создаваемым пользовательским шаблоном и описание его параметров приведено ниже.

```
{
  "templates": [
    {
      "title": {
        "default": "ФЛ",
        "ru": "Квалифицированный сертификат физического лица",
        "en": "Qualified certificate of an individual"
      },
      "userInfo": {
        "requirement": [
          "2.5.4.3",
          "2.5.4.4",
          "2.5.4.42",
          "1.2.643.3.131.1.1",
          "1.2.643.100.3",
        ],
        "optional": [
          "2.5.4.10",
          "2.5.4.12",
```

```
        "1.2.840.113549.1.9.1",
        "2.5.4.8",
        "2.5.4.7",
        "2.5.4.9"
        "2.5.4.6"
      ]
    },
    "extensions": {
      "eku": {
        "critical": false,
        "value": [
          "1.3.6.1.5.5.7.3.2",
          "1.3.6.1.5.5.7.3.4"
        ]
      },
      "ku": {
        "critical": false,
        "value": 240
      }
    }
  }
```


Описание файла *templates.xml*:

"Templates"	Массив шаблонов сертификатов
"Title"	Название шаблона
"Default"	Название шаблона по умолчанию
"Ru"	Название шаблона для русскоязычной версии
"En"	Название шаблона для английской версии
"UserInfo"	Информация о владельце сертификата
"Requirement"	Массив OID обязательных полей сертификатов
"Optional"	Массив OID опциональных полей сертификатов
"Extensions":	Расширения сертификата
"Eku"	Расширения типа «Extended key usage»
"Critical"	Критичность значений (true/false)

"Value"	Массив OID'ов расширений сертификатов
"Ku"	Расширения типа «Key usage»
"Critical"	Критичность значений (true/false)
"Value"	Битовая конкатенация флагов расширений

Список часто используемых объектных идентификаторов (OID) полей сертификата:

Поле сертификата	**OID**
CN	2.5.4.3
SN	2.5.4.4
G	2.5.4.42
I	2.5.4.43
E	1.2.840.113549.1.9.1
INN	1.2.643.3.131.1.1
INNLE	1.2.643.100.4
ОГРН	1.2.643.100.1
ОГРНИП	1.2.643.100.5
СНИЛС	1.2.643.100.3
C	2.5.4.6
S	2.5.4.8
L	2.5.4.7
Street	2.5.4.9
O	2.5.4.10
OU	2.5.4.11
T	2.5.4.12

Расширения сертификата типа «*Extended key usage*»:

Сертификат проверки подлинности сервера	1.3.6.1.5.5.7.3.1
Сертификат проверки подлинности клиента	1.3.6.1.5.5.7.3.2
Сертификат цифровой подписи	1.3.6.1.5.5.7.3.3
Сертификат защиты электронной почты	1.3.6.1.5.5.7.3.4
Сертификат штампа времени подписи	1.3.6.1.5.5.7.3.8
Сертификат для работы с OCSP	1.3.6.1.5.5.7.3.9
Сертификат IKE-посредника IP-безопасности	1.3.6.1.5.5.8.2.2
Сертификат службы ДТС	1.3.6.1.5.5.7.3.10
Временный доступ к Центру Регистрации	1.2.643.2.2.34.2
Пользователь Центра Регистрации, HTTP, TLS клиент	1.2.643.2.2.34.6
Вход со смарт-картой	1.3.6.1.4.1.311.20.2.2

Расширения сертификата типа «*Key usage*»:

Подпись данных	128
Неотрекаемость	64
Шифрование ключа	32

Шифрование данных	16
Согласование ключей	8
Подпись сертификатов	4
Подпись списка отзывов	2
Только шифрование	9
Только расшифровывание	2176

Для вычисления значения расширения сертификата типа «*Key usage*» необходимо просуммировать значения расширений, которые требуется включить в шаблон пользовательского сертификата, и записать полученный результат в соответствующее поле «*Value*».

5 Настройка списка криптопровайдеров

Настройка списка криптопровайдеров осуществляется пользователем с правами администратора.

Во вкладке «*Контейнеры*» содержится список криптопровайдеров, которые администратор может разрешить или запретить для пользователя, все контейнеры, относящиеся к установленным криптопровайдерам, и имеющиеся на ключевом отчуждаемом носителе.

Для настройки списка криптопровайдеров, доступных пользователю, необходимо перейти в меню «*Сертификаты*» → «*Контейнеры*» и установить переключатель в строке криптосредства в положение для разрешения или в положение для запрета (рисунок 5.1).

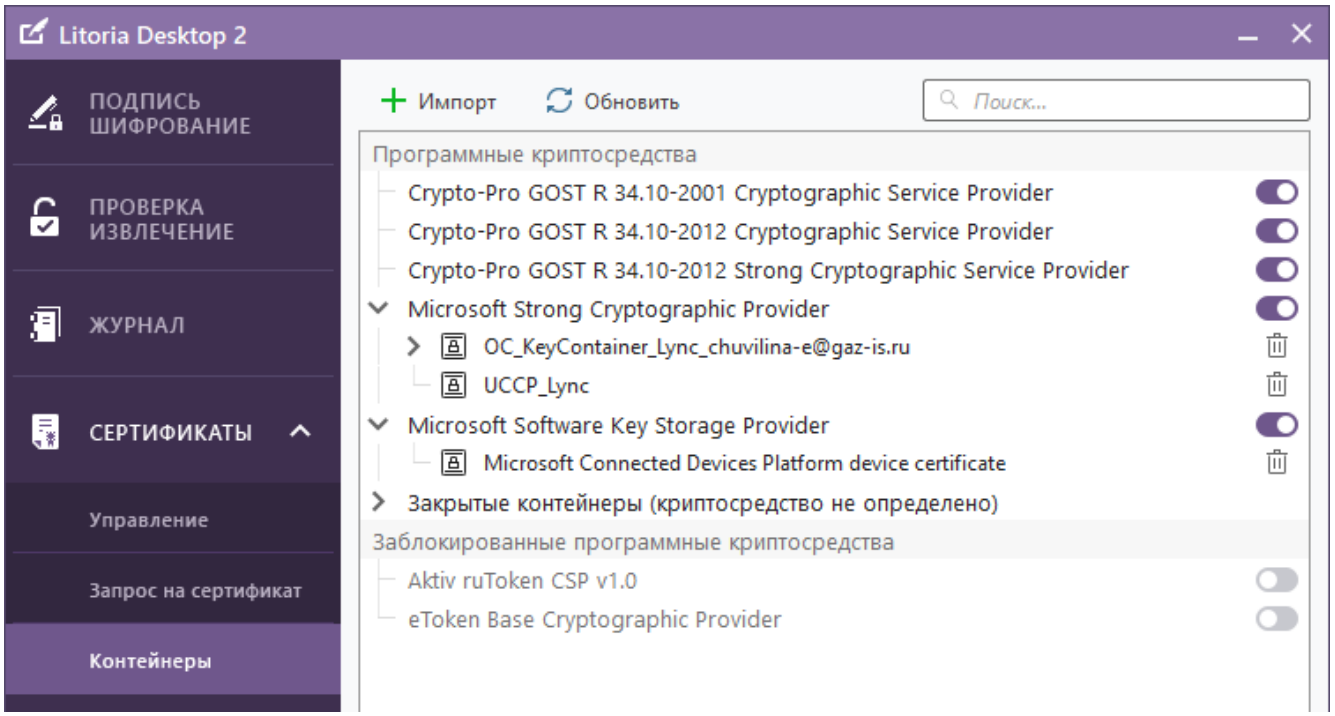


Рисунок 5.1 – Список установленных криптопровайдеров

После внесения изменений в список разрешенных/запрещенных криптопровайдеров потребуется перезапуск ПК «Litoria Desktop 2» (рисунок 5.2).

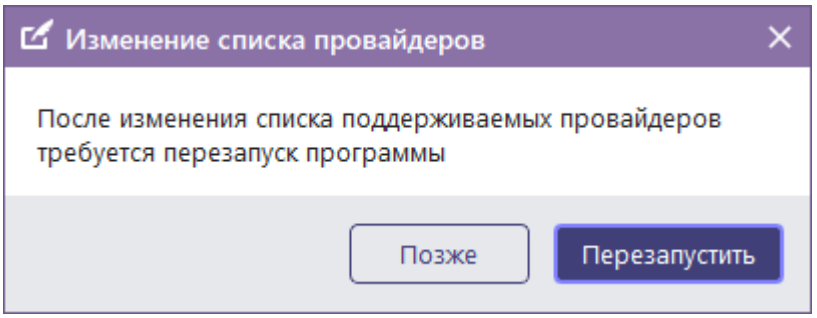


Рисунок 5.2 – Требование перезапуска комплекса для изменения списка криптопровайдеров

При отказе от немедленного перезапуска комплекса и выборе пункта «*Позже*» кнопка «*Перезапустить*» будет продублирована в верхнем меню вкладки «*Контейнеры*» до момента перезагрузки ПК «Litoria Desktop 2 (рисунок 5.3).

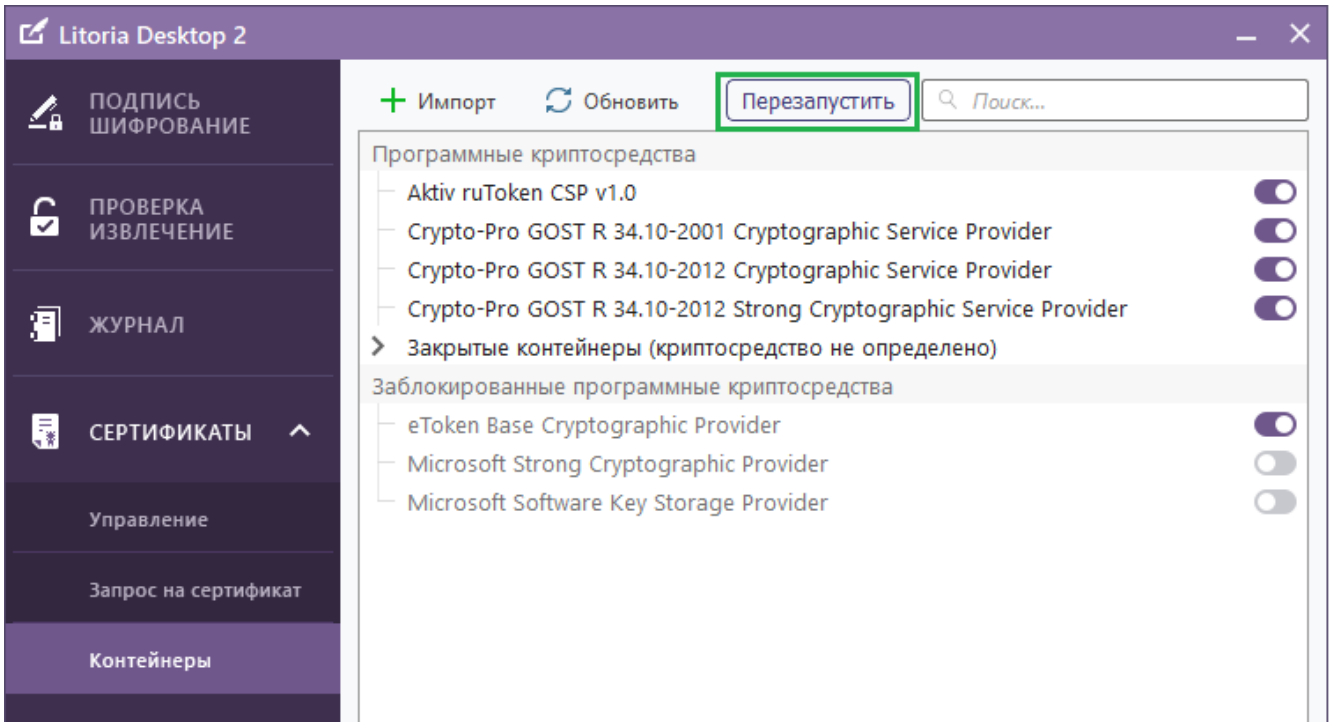


Рисунок 5.3 – Отображение кнопки «*Перезапустить*» в верхнем меню вкладки

6 Журнал событий

Журнал предназначен для фиксации, хранения и отображения информации о событиях, производимых пользователем в ПК «Litoria Desktop 2».

Список событий журнала (рисунок 6.1) содержит:

- дату и время совершенного события;
- наименование типа события;
- объект, в отношении которого производилась операция;
- пиктограмму успешности произведенной операции.

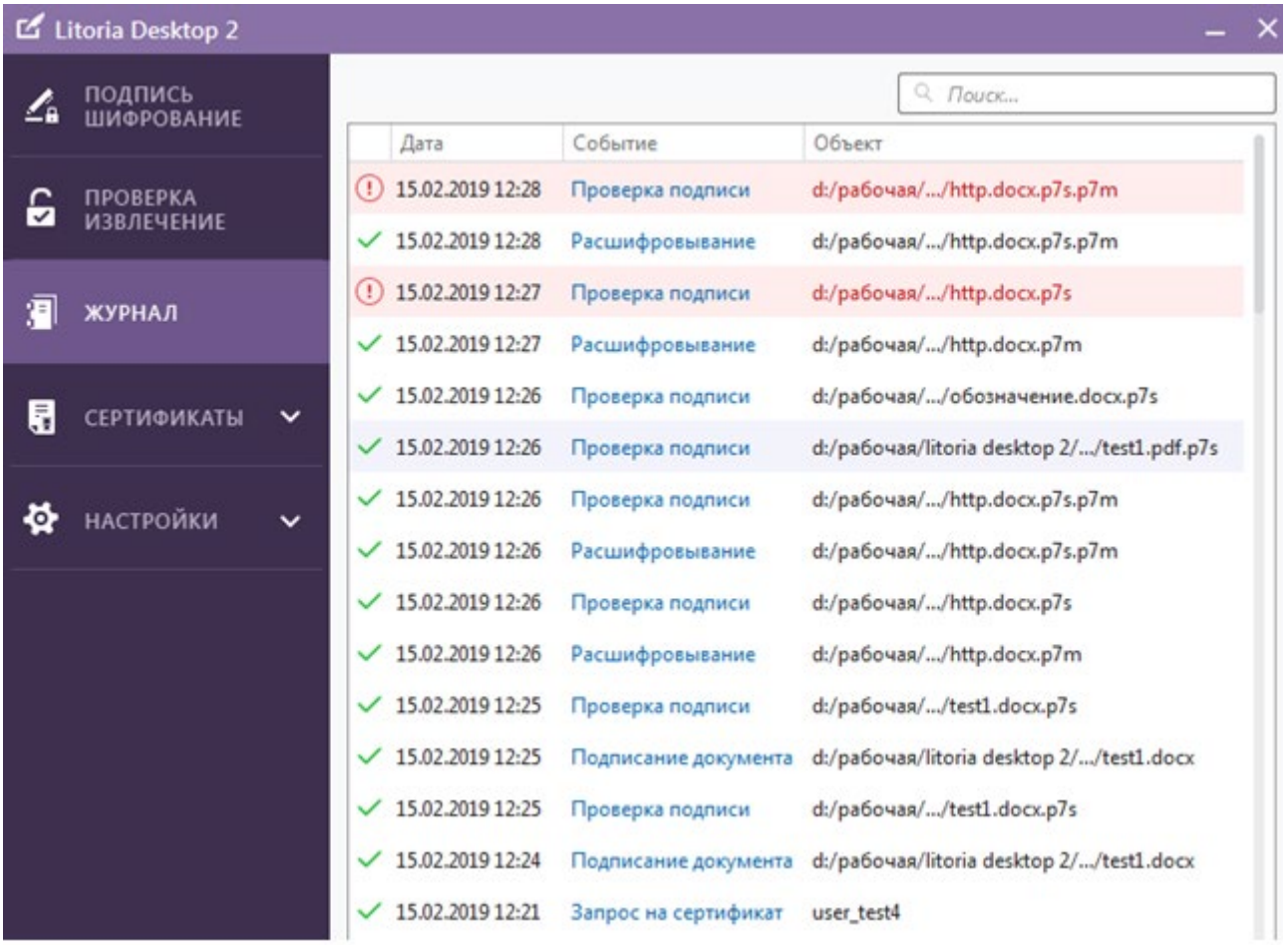


Рисунок 6.1 – Журнал событий

Список событий, регистрируемых в журнале событий (рисунок 6.1), приведен в таблице 6.1.

Таблица 6.1 – Список событий журнала

№	Событие	Успех/Ошибка	Пиктограмма
1	Подписание документа	Успех	✓
		Ошибка	!
		Отмена	×
2	Добавление подписи	Успех	✓
		Ошибка	!
		Отмена	×
3	Шифрование	Успех	✓
		Ошибка	!
		Отмена	×
4	Проверка подписи	Успех	✓
		Ошибка	!
		Отмена	×
5	Расшифровывание	Успех	✓
		Ошибка	!
		Отмена	×
6	Подпись и шифрование	Успех	✓
		Ошибка	!
		Отмена	×
7	Запрос на сертификат	Успех	✓
		Ошибка	!
		Отмена	×
8	Удаление контейнера	Успех	✓
		Ошибка	!
		Отмена	×
9	Проверка ДТС	Успех	✓
		Ошибка	!
		Отмена	×
10	Экспорт контейнера	Успех	✓
		Ошибка	!
		Отмена	×
11	Импорт pfx	Успех	✓
		Ошибка	!
		Отмена	×
12	Заверение подписи	Успех	✓
		Ошибка	!
		Отмена	×

№	Событие	Успех/Ошибка	Пиктограмма
13	Продление подписи	Успех	✓
		Ошибка	!
		Отмена	×
14	Выпуск сертификата	Успех	✓
		Ошибка	!
		Отмена	×

Подробная информация по каждому событию доступна по щелчку на событии в списке событий (рисунок 6.2). Для каждого события отображается информация:

– наименование события;

– дата и время события;

– успешность операции;

– файлы, над которыми производилась операция;

– возможность просмотра сформированного отчета в формате pdf при выполнении операции проверки подписи (рисунок 6.3);

– сертификат;

– файл, содержащий информацию об ошибке *«Техническая информация об ошибке»* (при установленном флаге «*Журналировать операции с ошибкой*» в меню «*Настройки*» –> «*Основные*», установка флага описана в п.3.1.4);

– дополнительная информация в зависимости от события (например, техническая информация о сертификате службы ДТС и ответная квитанция о проведенной проверке в событии *«Проверка ДТС»*);

– кнопки перехода к предыдущей и следующей записи журнала.

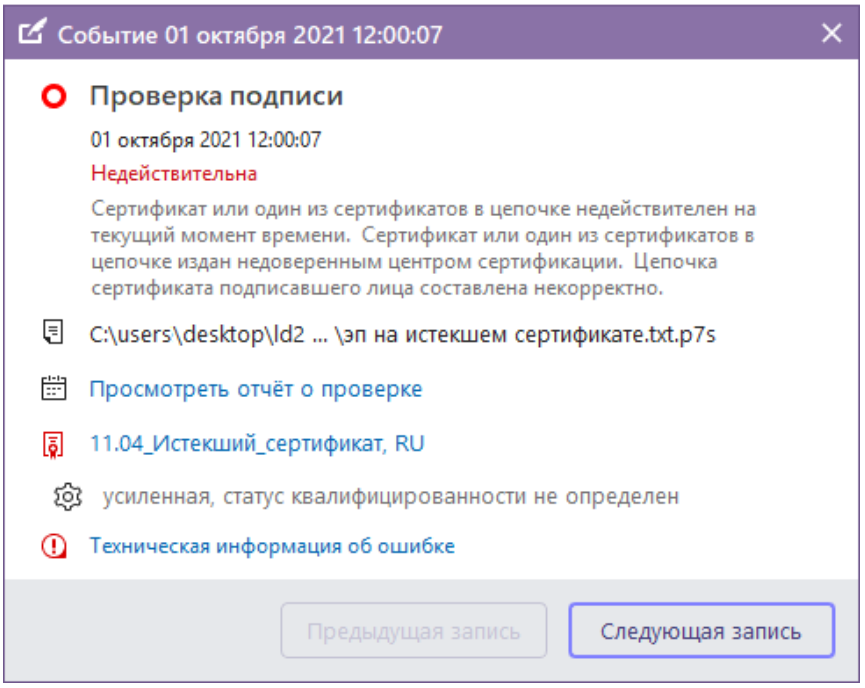
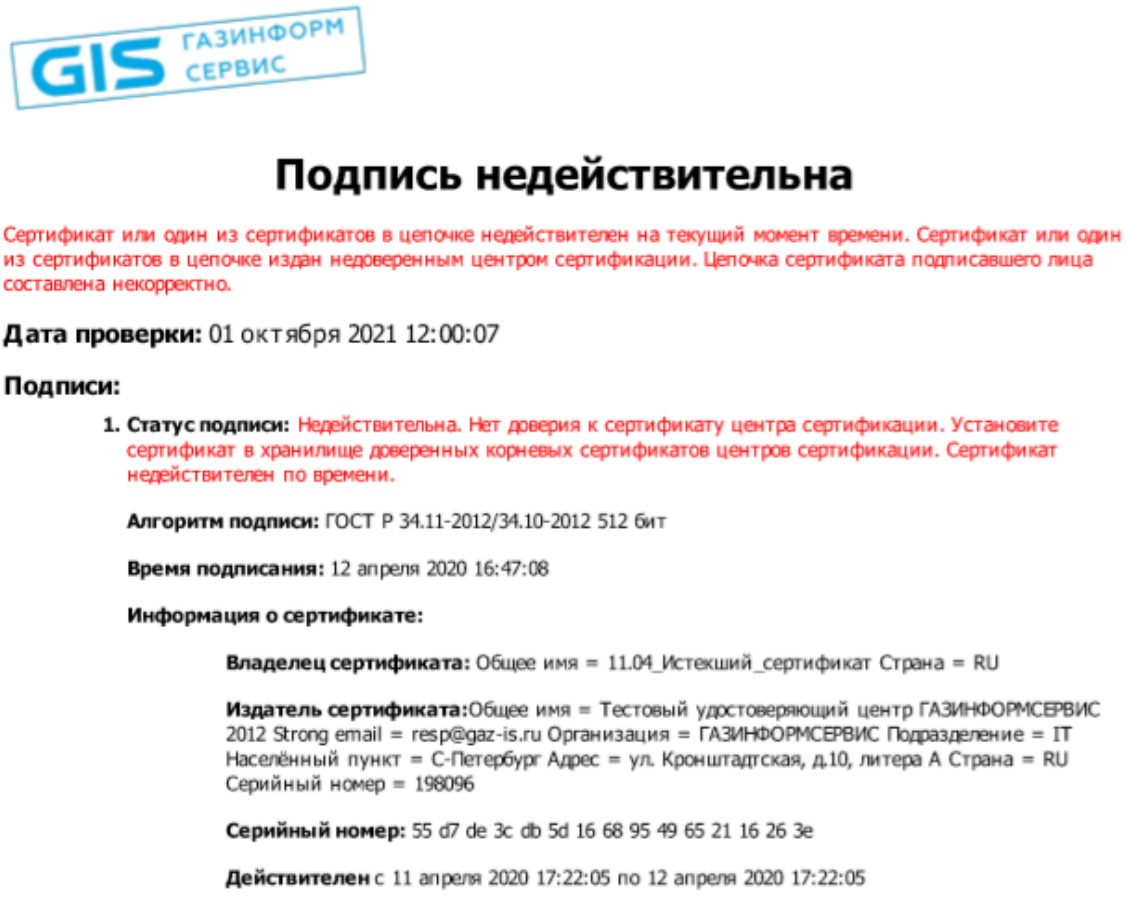


Рисунок 6.2 – Описание события



Подпись недействительна

Сертификат или один из сертификатов в цепочке недействителен на текущий момент времени. Сертификат или один из сертификатов в цепочке издан недоверенным центром сертификации. Цепочка сертификата подписавшего лица составлена некорректно.

Дата проверки: 01 октября 2021 12:00:07

Подписи:

1. **Статус подписи:** Недействительна. Нет доверия к сертификату центра сертификации. Установите сертификат в хранилище доверенных корневых сертификатов центров сертификации. Сертификат недействителен по времени.

   Алгоритм подписи: ГОСТ Р 34.11-2012/34.10-2012 512 бит

   Время подписания: 12 апреля 2020 16:47:08

   Информация о сертификате:

   Владелец сертификата: Общее имя = 11.04_Истекший_сертификат Страна = RU

   Издатель сертификата:Общее имя = Тестовый удостоверяющий центр ГАЗИНФОРМСЕРВИС 2012 Strong email = resp@gaz-is.ru Организация = ГАЗИНФОРМСЕРВИС Подразделение = IT Населённый пункт = С-Петербург Адрес = ул. Кронштадтская, д.10, литера А Страна = RU Серийный номер = 198096

   Серийный номер: 55 d7 de 3c db 5d 16 68 95 49 65 21 16 26 3e

   Действителен с 11 апреля 2020 17:22:05 по 12 апреля 2020 17:22:05

Рисунок 6.3 – Отчет о проверке

При необходимости можно отфильтровать события по дате, типу события или объекту. Для этого необходимо ввести требуемые значения в поле «*Поиск*» (рисунок 6.1).

Приложение 1

Содержание файла templates.xml

{
"templates": [
{
"title": {
"default": "Пустой",
"ru": "Пустой",
"en": "Empty"
},
"userInfo": {
"requirement": [
],
"optional": [
"2.5.4.3",
"2.5.4.4",
"2.5.4.42",
"2.5.4.43",
"1.2.840.113549.1.9.1",
"1.2.643.3.131.1.1",
"1.2.643.100.1",
"1.2.643.100.3",
"1.2.643.100.4",
"1.2.643.100.5",
"2.5.4.6",
"2.5.4.7",
"2.5.4.8",
"2.5.4.9",
"2.5.4.10",

"2.5.4.11",
"2.5.4.12",
"2.5.4.5",
"0.9.2342.19200300.100.1.25"
]
}
},
{
"title": {
"default": "ФЛ",
"ru": "Квалифицированный сертификат физического лица",
"en": "Qualified certificate of an individual"
},
"userInfo": {
"requirement": [
"2.5.4.3",
"2.5.4.4",
"2.5.4.42",
"1.2.643.3.131.1.1",
"1.2.643.100.3"
],
"optional": [
"2.5.4.10",
"2.5.4.12",
"1.2.840.113549.1.9.1",
"2.5.4.8",
"2.5.4.7",
"2.5.4.9",
"2.5.4.6"
]
},

"extensions": {
"eku": {
"critical": false,
"value": [
"1.3.6.1.5.5.7.3.2",
"1.3.6.1.5.5.7.3.4"
]
},
"ku": {
"critical": false,
"value": 240
}
}
},
{
"title": {
"default": "ИП",
"ru": "Квалифицированный сертификат индивидуального предпринимателя",
"en": "Individual entrepreneur"
},
"userInfo": {
"requirement": [
"2.5.4.3",
"2.5.4.4",
"2.5.4.42",
"1.2.643.3.131.1.1",
"1.2.643.100.5",
"1.2.643.100.3"
],
"optional": [
"2.5.4.10",

"2.5.4.12",
"1.2.840.113549.1.9.1",
"2.5.4.8",
"2.5.4.7",
"2.5.4.9",
"2.5.4.6"
]
},
"extensions": {
"eku": {
"critical": false,
"value": [
"1.3.6.1.5.5.7.3.2",
"1.3.6.1.5.5.7.3.4"
]
},
"ku": {
"critical": false,
"value": 240
}
}
},
{
"title": {
"default": "ЮЛ",
"ru": "Квалифицированный сертификат юридического лица",
"en": "Qualified legal entity certificate"
},
"userInfo": {
"requirement": [
"2.5.4.3",

"1.2.643.100.4",
"1.2.643.100.1",
"2.5.4.6",
"2.5.4.8",
"2.5.4.7",
"1.2.643.3.131.1.1",
"2.5.4.9",
"2.5.4.4",
"2.5.4.42",
"1.2.643.100.3"
],
"optional": [
"1.2.840.113549.1.9.1",
"2.5.4.12",
"2.5.4.10"
]
},
"extensions": {
"eku": {
"critical": false,
"value": [
"1.3.6.1.5.5.7.3.2",
"1.3.6.1.5.5.7.3.4"
]
},
"ku": {
"critical": false,
"value": 240
}
}
},

{
"title": {
"default": "ЮЛ(АС)",
"ru": "Квалифицированный сертификат информационной системы",
"en": "Qualified legal entity certificate (Information system)"
},
"userInfo": {
"requirement": [
"2.5.4.3",
"1.2.643.100.4",
"1.2.643.100.1",
"2.5.4.6",
"2.5.4.7",
"2.5.4.8",
"2.5.4.9"
],
"optional": [
"2.5.4.10"
]
},
"extensions": {
"eku": {
"critical": false,
"value": [
"1.3.6.1.5.5.7.3.2",
"1.3.6.1.5.5.7.3.4"
]
},
"ku": {
"critical": false,
"value": 240

}
}
},
{
"title": {
"default": "DVCS",
"ru": "Сертификат службы валидации (DVC)",
"en": "DVC service certificate"
},
"userInfo": {
"requirement": [
"2.5.4.3",
"1.2.643.100.4",
"1.2.643.100.1",
"2.5.4.6",
"2.5.4.7",
"2.5.4.8",
"2.5.4.9"
],
"optional": [
"2.5.4.10"
]
},
"extensions": {
"eku": {
"critical": true,
"value": [
"1.3.6.1.5.5.7.3.10"
]
},
"ku": {

"critical": true,
"value":198
}
}
},
{
"title": {
"default": "TSP",
"ru": "Сертификат службы штампов времени (TSP)",
"en": "TSP service certificate"
},
"userInfo": {
"requirement": [
"2.5.4.3",
"1.2.643.100.4",
"1.2.643.100.1",
"2.5.4.6",
"2.5.4.7",
"2.5.4.8",
"2.5.4.9"
],
"optional": [
"2.5.4.10"
]
},
"extensions": {
"eku": {
"critical": true,
"value": [
"1.3.6.1.5.5.7.3.8"
]

},
"ku": {
"critical": true,
"value":192
}
}
},
{
"title": {
"default": "OCSP",
"ru": "Сертификат сервиса онлайн проверки статуса (OCSP)",
"en": "OCSP service certificate"
},
"userInfo": {
"requirement": [
"2.5.4.3",
"1.2.643.100.4",
"1.2.643.100.1",
"2.5.4.6",
"2.5.4.7",
"2.5.4.8",
"2.5.4.9"
],
"optional": [
"2.5.4.10"
]
},
"extensions": {
"eku": {
"critical": true,
"value": [

"1.3.6.1.5.5.7.3.9"
]
},
"ku": {
"critical": true,
"value":192
}
}
},
{
"title": {
"default": "Web server",
"ru": "Web-сервер",
"en": "Web server"
},
"userInfo": {
"requirement": [
"2.5.4.3"
],
"optional": [
"1.2.840.113549.1.9.1",
"2.5.4.6",
"2.5.4.7",
"2.5.4.8",
"2.5.4.10"
]
},
"extensions": {
"ku": {
"critical": true,
"value":218

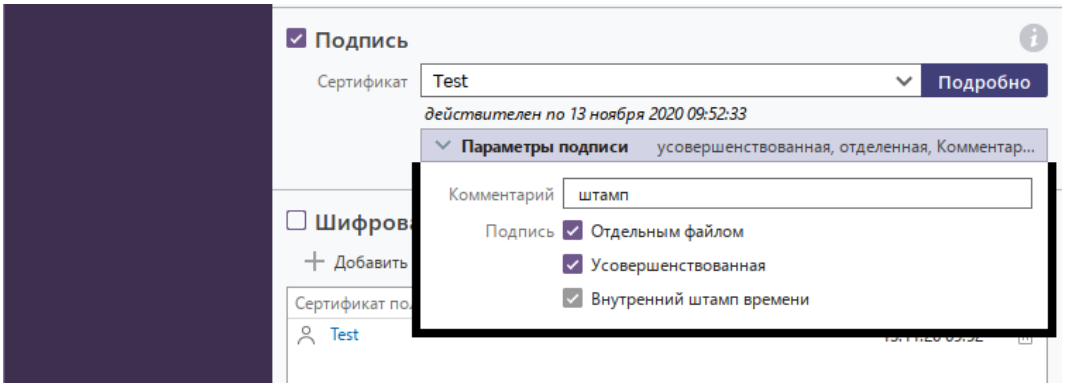
}
}
},

{
"title": {
"default": "Шаблон на основе сертификата",
"ru": "Шаблон на основе сертификата",
"en": "Template bases on certificate"
},
"dynamic": true
}
]
}

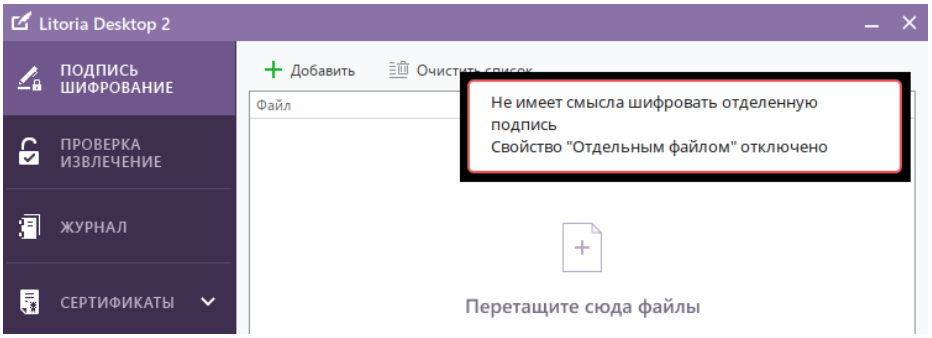
Приложение 2

Особенности отображение окон ПК «Litoria Desktop 2» в ОС Astra Linux Special Edition (Smolensk) v. 1.6

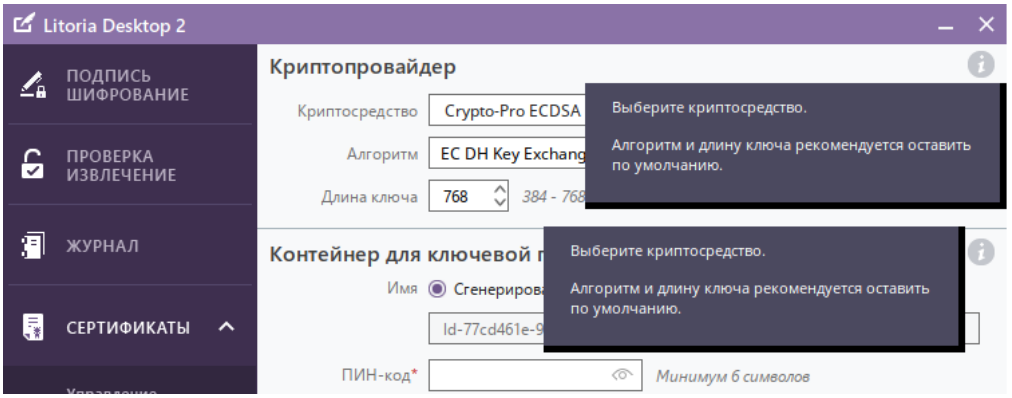
В ОС Astra Linux (Smolensk) v. 1.6 в ПК «Litoria Desktop 2» возможно появление черного обрамления вокруг некоторых дополнительных окон (рисунки П2.1 а, б, в).



а)



б)



в)

Рисунок П2.1 – Отображение дополнительных окон ПК «Litoria Desktop 2»

Появление черного обрамления дополнительных окон связано с отключением настроек

графики с целью повышения эффективности работы ОС.

Для включения настроек и корректного отображения дополнительных окон ПК «Litoria Desktop 2» необходимо:

1) В меню кнопки «*Пуск*» перейти в «*Панель управления*» и выбрать «*Оформление Fly*» (рисунок П2.2).

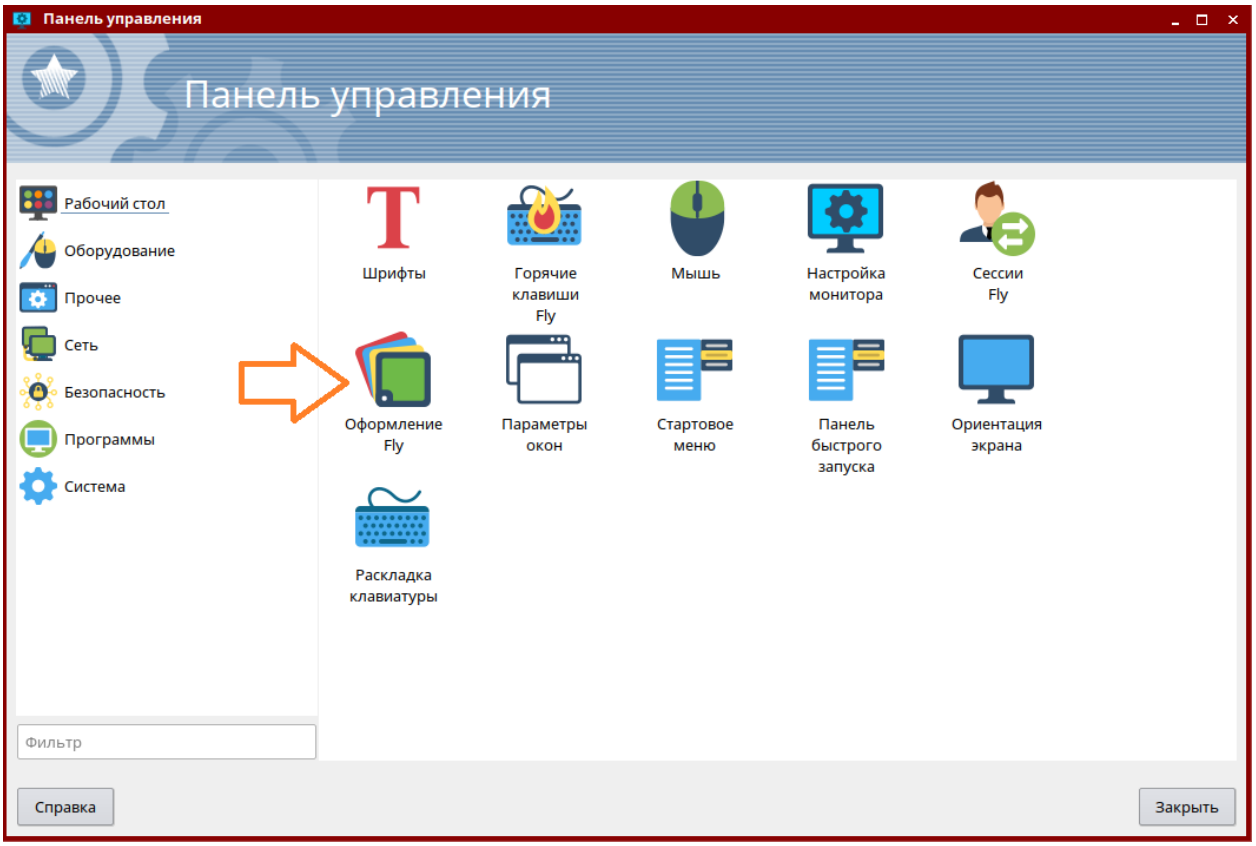


Рисунок П2.2 – Панель управления ОС Astra Linux (Smolensk) v. 1.6

2) В окне «*Оформление Fly*» выбрать «*Эффекты*» (рисунок П2.3).

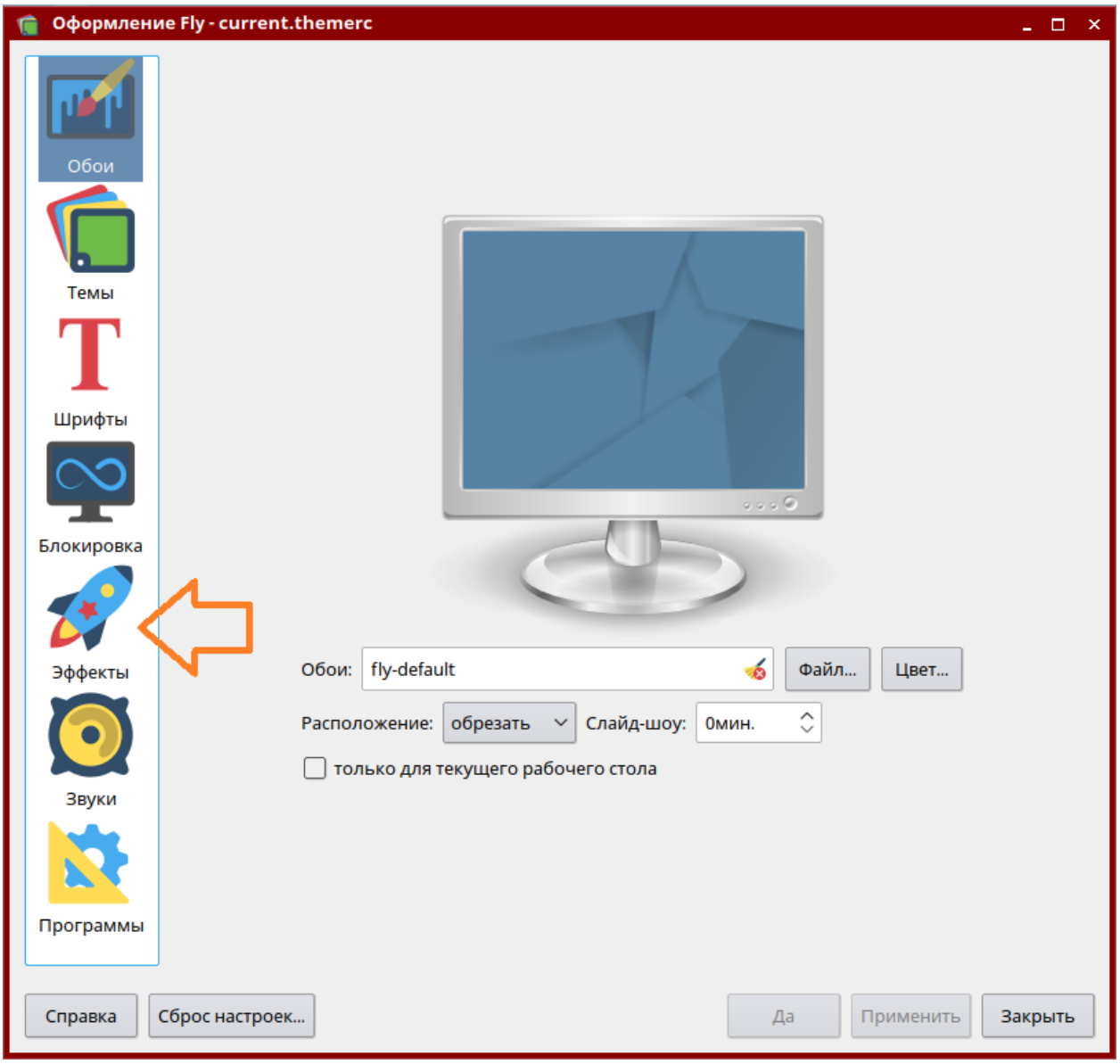


Рисунок П2.3 – Переход к настройке эффектов

3) В открывшемся окне перейти во вкладку «*Для окон*» (рисунок П2.4).

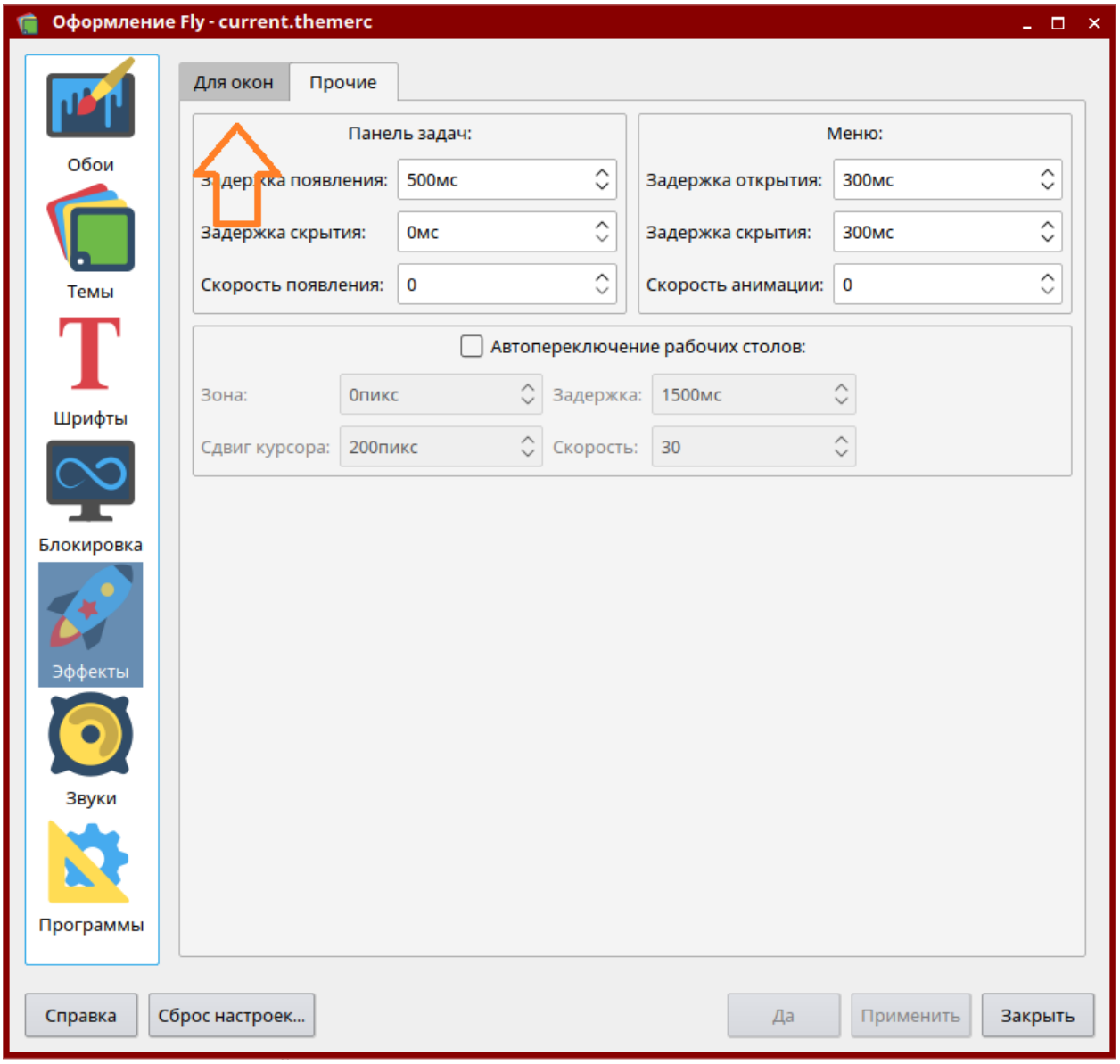


Рисунок П2.4 – Переход к вкладке «*Для окон*»

4) В открывшейся вкладке в области «*Композитинг*» установить флаг «*Композит-менеджер*» (рисунок П2.5).

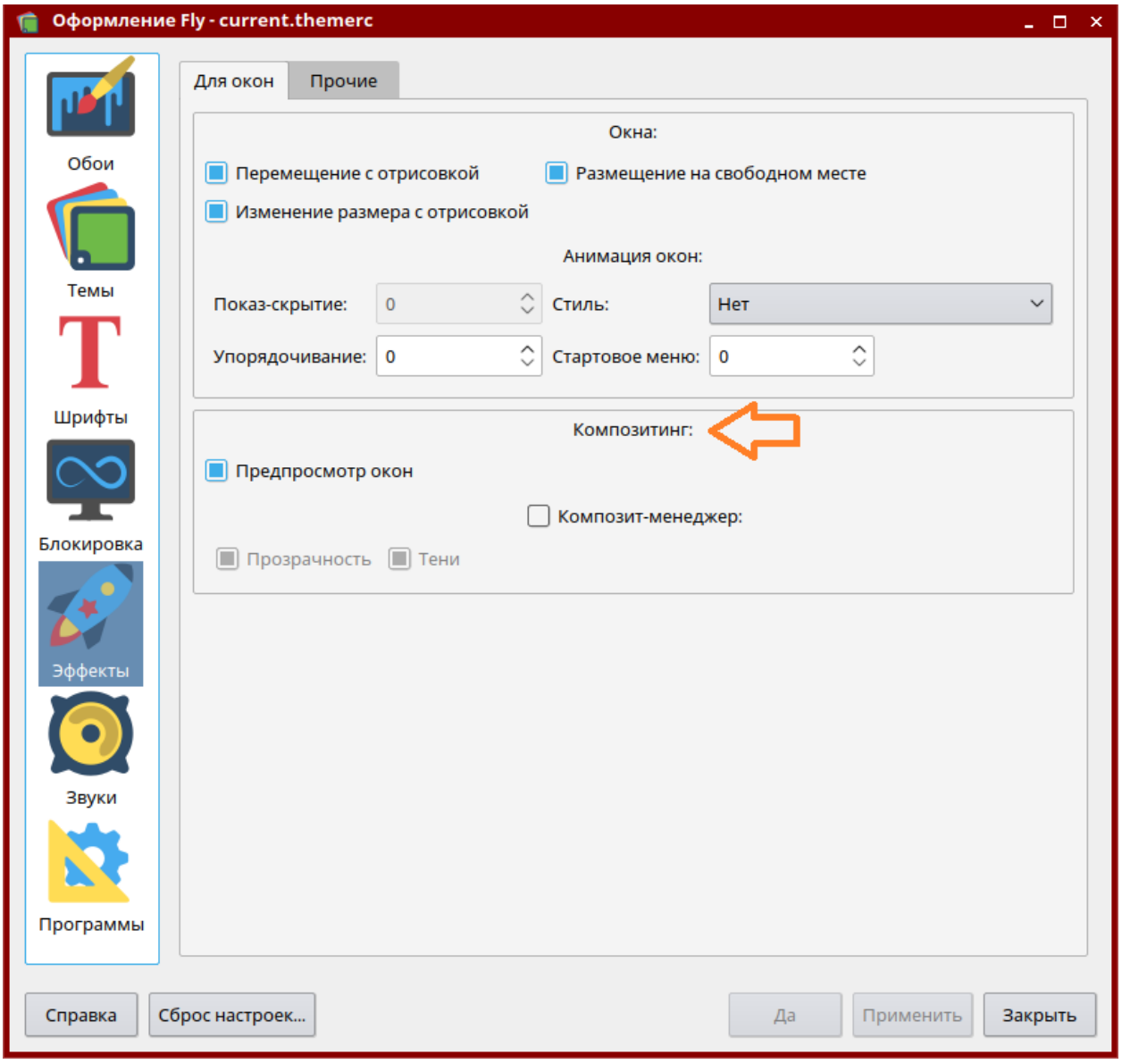


Рисунок П2.5 – Установка флага «*Композит-менеджер*»

5) Для сохранения установленных настроек, нажмите кнопку «*Применить*».

Выполненные настройки позволят отображать дополнительные окна в ПК «Litoria Desktop 2» корректно, без черного обрамления (рисунок П2.6).

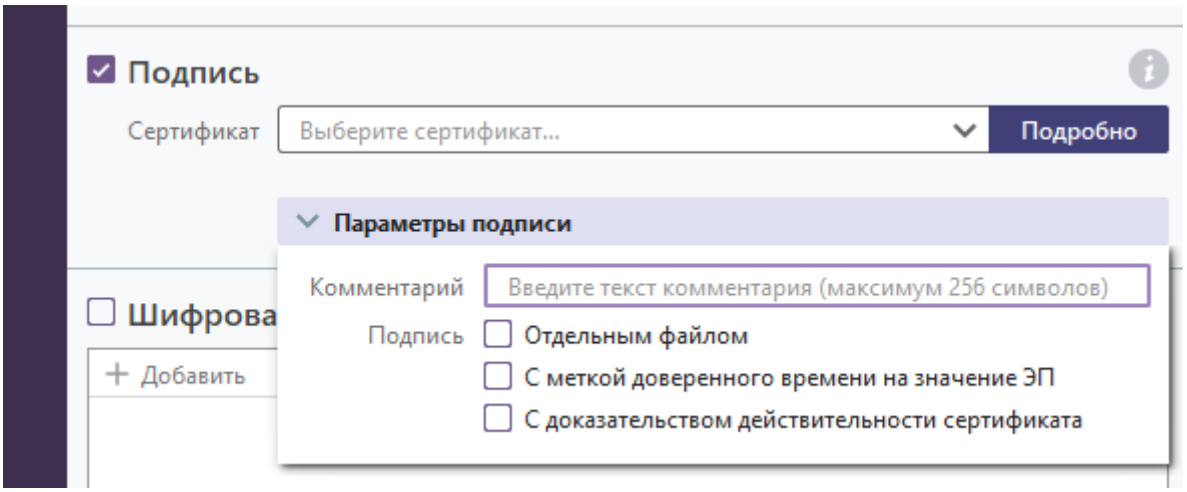


Рисунок П2.6 – Корректное отображение дополнительных окон

Перечень сокращений

АРМ – Автоматизированное Рабочее Место

ГОСТ – ГОсударственный СТандарт

ДТС – Доверенная Третья Сторона

ОС – Операционная Система

ПИН – Персональный Идентификационный Номер

ПК – Программный Комплекс

СКЗИ – Средство Криптографической Защиты Информации

СОС – Список Отзыва Сертификата

УЦ – Удостоверяющий Центр

ЭП – Электронная Подпись

DVCS – Data Validation and Certification Server (сервер проверки достоверности данных и сертификации)

OSCP – Online Certificate Status Protocol (протокол для проверки статуса сертификата электронной подписи)

PDF – Portable Document Format (межплатформенный открытый формат электронных документов)

PKCS – Public Key Cryptography Standards (криптографические стандарты открытого ключа)

RSA – Аббревиатура от фамилий Rivest, Shamir и Adleman (криптографический алгоритм с открытым ключом)

TSP – Time-Stamp Protocol (протокол штампа времени)

VSD – Validation of Digitally Signed Document (подтверждение корректности ЭП электронного документа)

Термины и определения

CAdES – Стандарт ЭП, являющийся расширенной версией стандарта CMS.
CMS (Cryptographic Message Syntax) утвержден в RFC5652 вместо устаревшего стандарта RSAPKCS#7. Синтаксис CMS описывает способы формирования криптографических сообщений, в результате чего сообщение становится полностью самодостаточным для его открытия и выполнения всех необходимых операций.
Стандарт CAdES сохраняет существующую структуру ЭП формата CMS, добавляя только подписываемые или не подписываемые атрибуты. ЭП с доказательством действительности сертификата предоставляет возможность осуществления:
  - множественной подписи (данные могут быть подписаны несколькими сторонами);
  - подписания не только данных, но и некоторых атрибутов сообщения (хеша сообщения, времени подписи, значения другой подписи).

Формат CAdES определен в RFC5126 «CMS Advanced Electronic Signatures (CAdES)».

DVCS-запрос – Электронный документ, подписанный ЭП пользователя (сертификат ЭП должен быть зарегистрирован в службе DVCS), содержащий сведения, зависящие от типа запроса, который направляется для проверки на сервер проверки подлинности.

PAdES – Стандарт ЭП, представляющий собой набор ограничений и расширений для PDF и ISO 32000-1. ЭП на основе PAdES, имеет статус передовой электронной подписи. Это означает, что:
  - подпись однозначно связана с подписавшим;
  - способность идентифицировать подписавшего;
  - только подписавшая сторона контролирует данные, используемые для создания подписи;
  - возможность идентификации, если данные, прикрепленные к подписи, были изменены после подписания.

Формат PAdES определен в ETSI TS 102 778-1 V1.1.1 (2009-07) «PDF Advanced Electronic Signatures (PAdES)».

XAdES – Стандарт ЭП, основанный на стандарте XML DSig. XML DSig является основой для цифровой подписи документов и рекомендован консорциумом W3C. Фактически XML DSig решает те же задачи, что и PKCS#7 (т.е. утверждает целостность информации и неотрекаемость обладателя ЭП), но областью применения XML DSig являются веб-приложения и веб-сервисы.

Ключ ЭП – Уникальная последовательность символов, предназначенная для создания ЭП.

Ключ проверки ЭП – Уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП.

Простая ЭП – По Федеральному закону №63-ФЗ, простая ЭП получена посредством использования кодов, паролей или иных средств, и подтверждает факт формирования электронной подписи определенным лицом.

Сертификат ключа проверки ЭП – Электронный документ или документ на бумажном носителе, выданные УЦ либо доверенным лицом УЦ и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП.

Служба штампов времени – Доверенный субъект инфраструктуры открытых ключей, обладающий точным и надежным источником времени и оказывающий услуги по созданию меток доверенного времени.

Список отозванных сертификатов, список отзыва (COC, CRL) – Электронный документ с электронной подписью уполномоченного лица удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были аннулированы (отозваны) или действие которых было приостановлено.

Удостоверяющий центр – Юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки ЭП, а также иные функции, предусмотренные

Федеральным законом №63-ФЗ от 06.04.2011 г. «Об электронной подписи».

Усиленная квалифицированная ЭП

– По Федеральному закону №63-ФЗ, усиленная квалифицированная ЭП включает в себя все признаки усиленной неквалифицированной ЭП и дополнена следующими параметрами:
  – ключ проверки электронной подписи указан в квалифицированном сертификате;
  – для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом №63-ФЗ.

Усиленная неквалифицированная ЭП

– По Федеральному закону №63-ФЗ:
  – получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
  – позволяет определить лицо, подписавшее электронный документ;
  – позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
  – создается с использованием средств электронной подписи.

ЭП с доказательством действительности сертификата

– Предусматривает включение в электронную подпись информации о времени создания подписи (TSP) и о статусе сертификата электронной подписи (OCSP) в момент подписания (действителен или отозван).

Хеш-функция

– Алгоритм, конвертирующий строку произвольной длины (сообщение) в битовую строку фиксированной длины, называемой *хеш-кодом*, проверочной суммой или цифровым отпечатком.

Метка доверенного времени

– Достоверная информация в электронной форме о дате и времени подписания электронного документа электронной подписью, создаваемая службой штампов времени и полученная в момент подписания электронного документа электронной подписью.

Электронная подпись

– Информация в электронной форме, которая присоединена к другой информации в электронной

форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.