ГАЗИНФОРМ СЕРВИС

Программный комплекс «Litoria Desktop 2»
Руководство администратора

Санкт-Петербург, 2018

Аннотация

В документе приводится руководство администратора программного комплекса «Litoria Desktop 2» (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 средствам автоматизированного рабочего места (АРМ).

В разделе «Настройка комплекса» описаны действия, необходимые для выполнения настройки основных функций комплекса, тиражирования настроек и приведены примеры создания пользовательских профилей настроек.

Содержание

1 Назначение ПК «Litoria Desktop 2»

1.1 Назначение

Основным назначением ПК «Litoria Desktop 2» является создание, добавление, заверение и проверка электронной подписи (ЭП), а также шифрование и извлечение 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; установки сертификата на устройство; установки сертификата из устройства в реестр; просмотра установленных криптопровайдеров и их параметров; использования службы DVCS для проверки ЭП и действительности сертификата ключа проверки подписи, в том числе для электронных документов длительного архивного хранения.

Интеграция в различные системы документооборота, порталы и на серверы приложений с использованием российских и иностранных криптографических алгоритмов с возможностью трансграничного взаимодействия возможна с помощью криптографической платформы «Litoria Crypto Platform».

1.2 Функции

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

- создание нового запроса на сертификат;
- создание запроса на основе имеющегося сертификата;
- установка сертификата на устройство;
- 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 COC и по протоколу OCSP в реальном времени;
- просмотр списка криптопровайдеров;
- удаление контейнера ключа ЭП;
- управление настройками комплекса.

Для работы с ЭП комплекс обеспечивает выполнение следующих функций:

- создание ЭП для файлов произвольного типа;

- добавление ЭП для подписанных файлов;
- заверение ЭП для подписанных файлов;
- создание, добавление, заверение ЭП для файлов PDF в формате CAdES/PAdES;
- проверка ЭП для подписанных файлов с возможностью получения исходного документа;
- использование службы DVCS для проверки ЭП и действительности сертификата ключа проверки подписи;
- 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.

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 удостоверяющего центра (УЦ), 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 имя выходного файла, криптопровайдер, имя ключевого контейнера, 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.

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 имя выходного файла, криптопровайдер, имя ключевого контейнера 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 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 сертификации удостоверяющего центра с локального диска в хранилище сертификатов.

Экспорт – это копирование сертификатов и списков сертификации удостоверяющего центра из хранилища сертификатов на локальный диск.

С помощью ПК «Litoria Desktop 2» можно выполнить операции установки корневого сертификата и сертификатов других пользователей.

Также с помощью функции *Импорт* можно установить личный сертификат из файла, полученного от УЦ в ответ на отправленный запрос, в хранилище сертификатов «Личное».

1.2.6 Просмотр списка криптопровайдеров

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

1.2.7 Удаление контейнера ключа ЭП

ПК «Litoria Desktop 2» позволяет удалить контейнер 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 сертификат подписчика, указать параметры создания и проверки ЭП, выбрать сертификаты получателей и другое.

Благодаря таким настройкам возможна автоматизация всех операций – выполнение любой операции за один клик мыши.

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 вложенным внутренним штампом времени;
- создание усовершенствованной ЭП.

Процесс создания усовершенствованной ЭП делится на следующие этапы:

- создание ЭП;
- получение штампа времени на значение ЭП;
- сбор доказательств действительности сертификата ключа проверки подписи и присоединение этих доказательств и их хэш-кодов к подписанному документу;
- получение штампа 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.

Заверению ЭП возможна лишь для подписанных ранее файлов.

1.2.12 Проверка ЭП

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

- принадлежности электронной подписи в электронном документе владельцу сертификата ключа проверки подписи;
- отсутствия искажений в подписанном данной электронной подписью электронном документе;
- 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 усовершенствованной ЭП файла с отделенной подписью – проверка корректности самого файла подписи.

1.2.13 Использование службы DVCS для проверки ЭП и действительности сертификата ключа проверки ЭП

ПК «Litoria Desktop» позволяет получать подтверждение корректности ЭП электронного документа (Validation of Digitally Signed Document – VSD) и подтверждение действительности сертификата ключа проверки подписи (Validation of Public Key Certificates – VPKC) от службы DVCS.

Для обращения к службе необходимо наличие личного сертификата ключа проверки ЭП, зарегистрированного ранее на сервере ДТС. Подписанный указанным личным сертификатом DVCS-запрос отправляется для проверки на сервер службы ДТС. В ответ сервер присылает информацию о действительности ЭП документа или сроке действия сертификата ключа проверки ЭП.

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

Использование службы DVCS для проверки ЭП и действительности сертификата ключа проверки подписи позволяет пользователю не устанавливать списки отзывов сертификатов на локальный компьютер. Проверка ЭП и действительности сертификата ключа проверки 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 DVCS для проверки ЭП и действительности сертификата ключа проверки ЭП осуществляется пользователем с правами администратора. Более подробное описание настройки смотрите в документе «ПК «Litoria Desktop». Руководство администратора».

1.2.14 Поддержка электронных документов длительного архивного хранения

Необходимым условием архивного хранения электронных документов является использование усовершенствованной ЭП (УЭП). Формат усовершенствованной электронной подписи предусматривает обязательное включение в реквизиты подписанного документа доказательства момента создания подписи (штамп 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 УЭП, к подписи добавляется архивный штамп времени, повышая значимость подписи до формата CAdES-A.

В ПК «Litoria Desktop 2» реализована поддержка электронных документов длительного архивного хранения включая доказательство момента подписи документа и действительность сертификата ключа подписи 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

Программный 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 пользователя.

1.2.18 Универсальная операция извлечения файла и проверки ЭП

Функциональность проверки идентична отдельным проверкам – 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 Интеграция криптоплатформы в системы документооборота

Криптографическая платформа «Litoria Crypto Platform» является ядром усовершенствованной электронной подписи (УЭП) и предназначена для интеграции в различные системы документооборота, порталы и на серверы приложений с использованием российских и иностранных криптографических алгоритмов с возможностью трансграничного взаимодействия.

При использовании криптографической платформы «Litoria Crypto Platform» разработчику доступны следующие возможности:

- создание, добавление, заверение и проверка электронной подписи (ЭП) различного типа (простая, усовершенствованная, отделенная);
- создание и добавление ЭП документа без предоставления данных (подпись хеша документа);
- шифрование, расшифровывание, гарантированное удаление файлов;
- работа с ключевой информацией и сертификатами (создание сертификата; установка сертификата в заданное хранилище; получение сертификата из хранилища; получение информации о сертификате; проверка статуса сертификата по спискам отзыва сертификатов (COC) и по Online Certificate Status Protocol (OCSP);
- управление списками отзыва сертификатов: создание, импорт, экспорт, удаление, детальный просмотр;
- применение для работы с ЭП различных криптопровайдеров, как программных (Base CSP, КриптоПро CSP, ViPNet CSP, ВАЛИДАТА CSP, Avest CSP и др.), так и аппаратных (JaCarta, eToken ГОСТ, РУТОКЕН ЭЦП);
- реализация функций службы актуальных статусов сертификатов согласно RFC2560 «Online Certificate Status Protocol (OCSP)»;

- реализация функций службы штампов времени согласно RFC3161 «Time-Stamp Protocol (TSP)»;
- формирование и проверка ЭП электронных сообщений в соответствии со спецификацией RFC3029 «Data Validation and Certification Server Protocol (DVCS)»;
- интеграция сервисов пролонгации;
- интеграция в системы электронного документооборота, включая SharePoint, Citrix, веб-сервер MS IIS (Internet Information Servies);
- предоставление интерфейсов (Com, Java, C#, SilverLight, ASP.net) для встраивания в различные среды и системы.

2 Условия применения комплекса

2.1 Требования к программному обеспечению

ПК «Litoria Desktop 2» функционирует под управлением следующих ОС:

- Windows 7 с пакетом обновления 1 (SP1) (32 бит/64 бит);
- Windows Server 2012 (64 бит);
- Windows Server 2012 R2 (64 бит);
- Windows 10 (32 бит/64 бит).

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 драйвера для аппаратных СКЗИ – «Криптотокен» в составе изделия «eToken ГОСТ» или «РУТОКЕН ЭЦП».

2.2 Требования к техническим средствам

Требования к рабочей станции, на которую устанавливается ПК «Litoria Desktop 2», обусловлены применением ОС.

Рекомендуется на рабочей станции, на которую устанавливается ПК «Litoria Desktop 2» использование монитора с разрешением экрана не менее 1280x800

2.1.1 Системные требования ОС Windows 7

Необходимые условия для запуска Windows 7 на компьютере:

- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 ГГц или выше;
- 1 ГБ (для 32-разрядной системы) или 2 ГБ (для 64-разрядной системы) оперативной памяти;
- 16 ГБ (для 32-разрядной системы) или 20 ГБ (для 64-разрядной системы) свободного места на жестком диске;
- графическое устройство DirectX 9 с драйвером WDDM версии 1.0 или выше.

2.1.2 Системные требования ОС Windows 10

Необходимые условия для запуска Windows 10 на компьютере:

- процессор с тактовой частотой не менее 1 ГГц или SoC;
- оперативная память:
  - для новых устройств: 2 ГБ для 32-разрядных и 64-разрядных систем;
  - при обновлении: 1 ГБ (для 32-разрядной системы) или 2 ГБ (для 64-разрядной

системы);

- 16 ГБ (для 32-разрядной системы) или 20 ГБ (для 64-разрядной системы) свободного места на жестком диске;
- графическое устройство Microsoft DirectX версии 9 или выше с драйвером WDDM 1.0.

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.

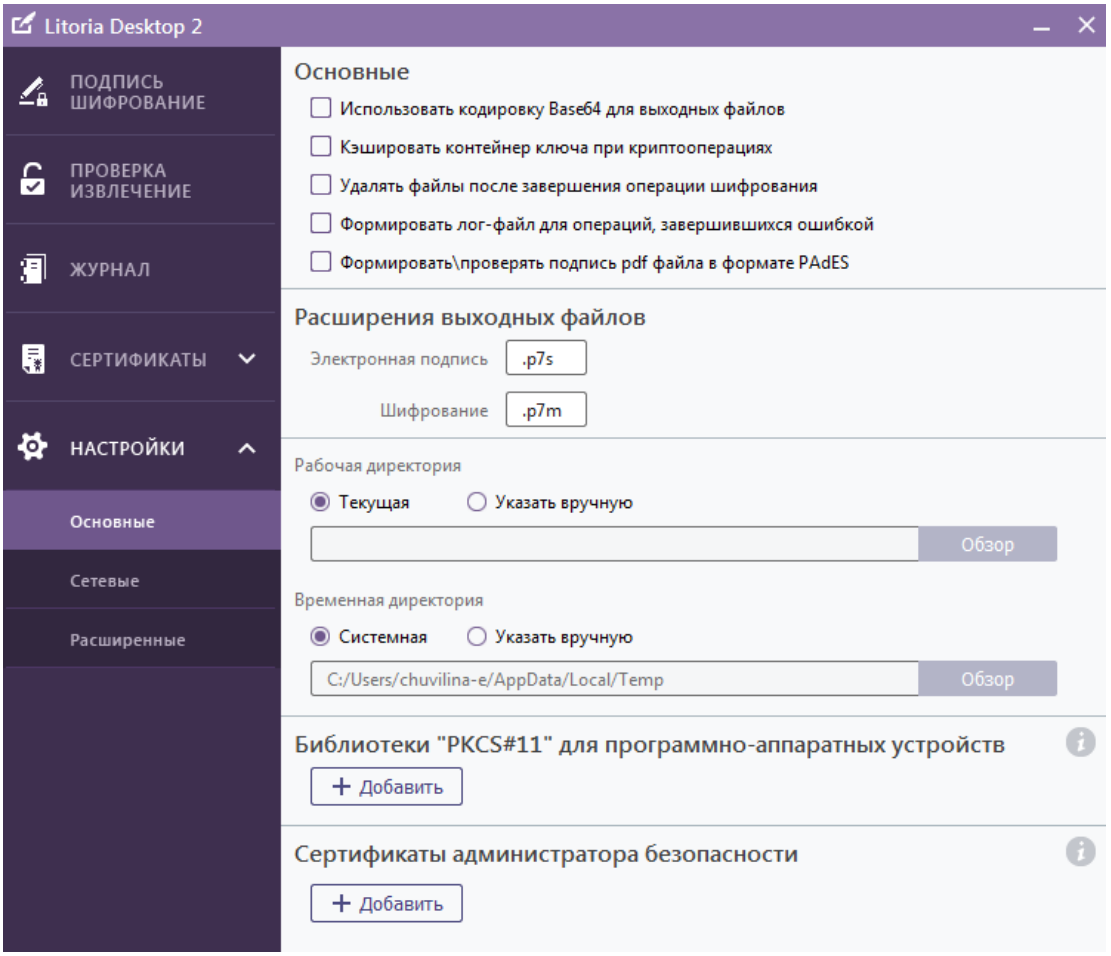

Рисунок 3.1 – Пункт меню «Настройки»

3.1 Основные настройки

Вкладка «*Основные настройки*» позволяет выполнять настройку:

- кодировки для выходных файлов;
- кэширования контейнера;
- удаления файлов после шифрования;
- лог-файла для операций, завершившихся ошибкой;
- подписи pdf файла в формате PAdES;
- расширений выходных файлов;
- рабочих и временных директорий;
- библиотек PKCS#11;
- сертификатов администратора безопасности.

3.1.1 Настройки кодировки для выходных файлов

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

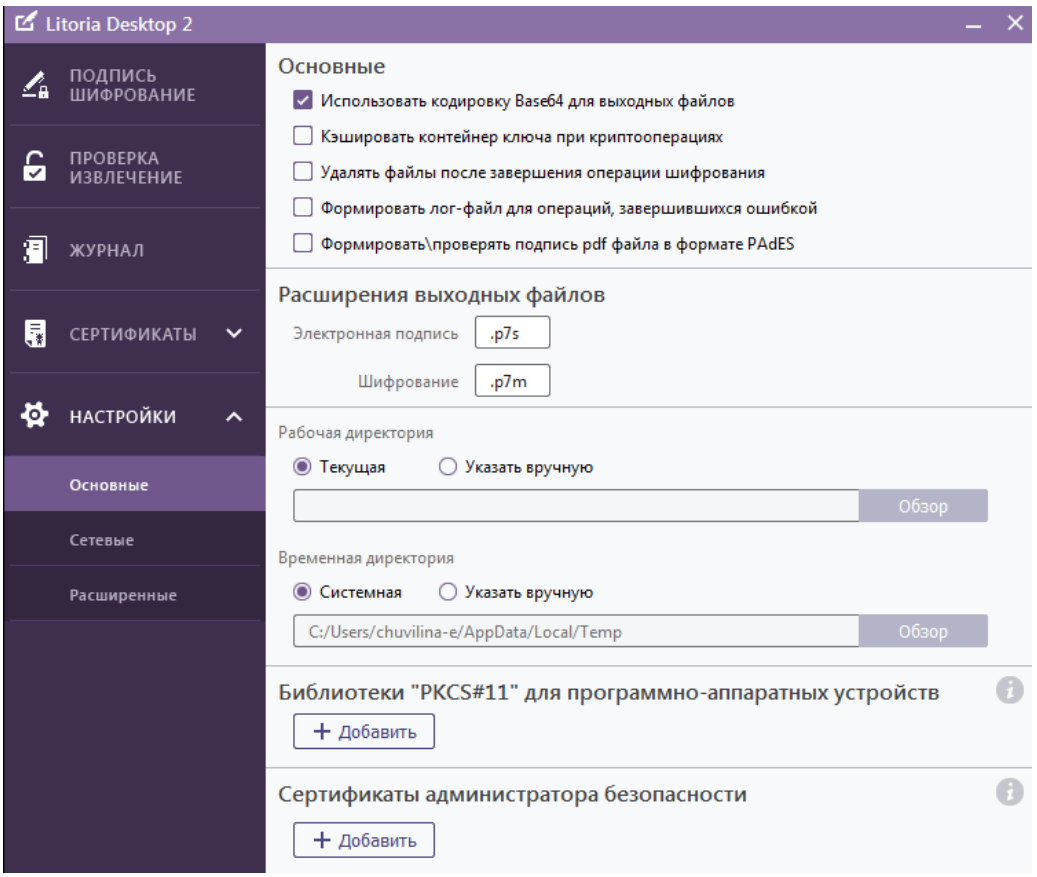

Рисунок 3.2 – Настройка кодировки выходных файлов

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:

– для 32-битной ОС – HKEY_LOCAL_MACHINE\SOFTWARE\GIS\Litoria Desktop 2;
– для 64-битной версии ОС – HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GIS\Litoria Desktop 2.

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 Формирование лог-файла для операций, завершившихся ошибкой

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

По умолчанию лог-файл не формируется. Для формирования файла установите флаг напротив пункта «*Формирование лог-файла для операций, завершившихся ошибкой*» (рисунок 3.3).

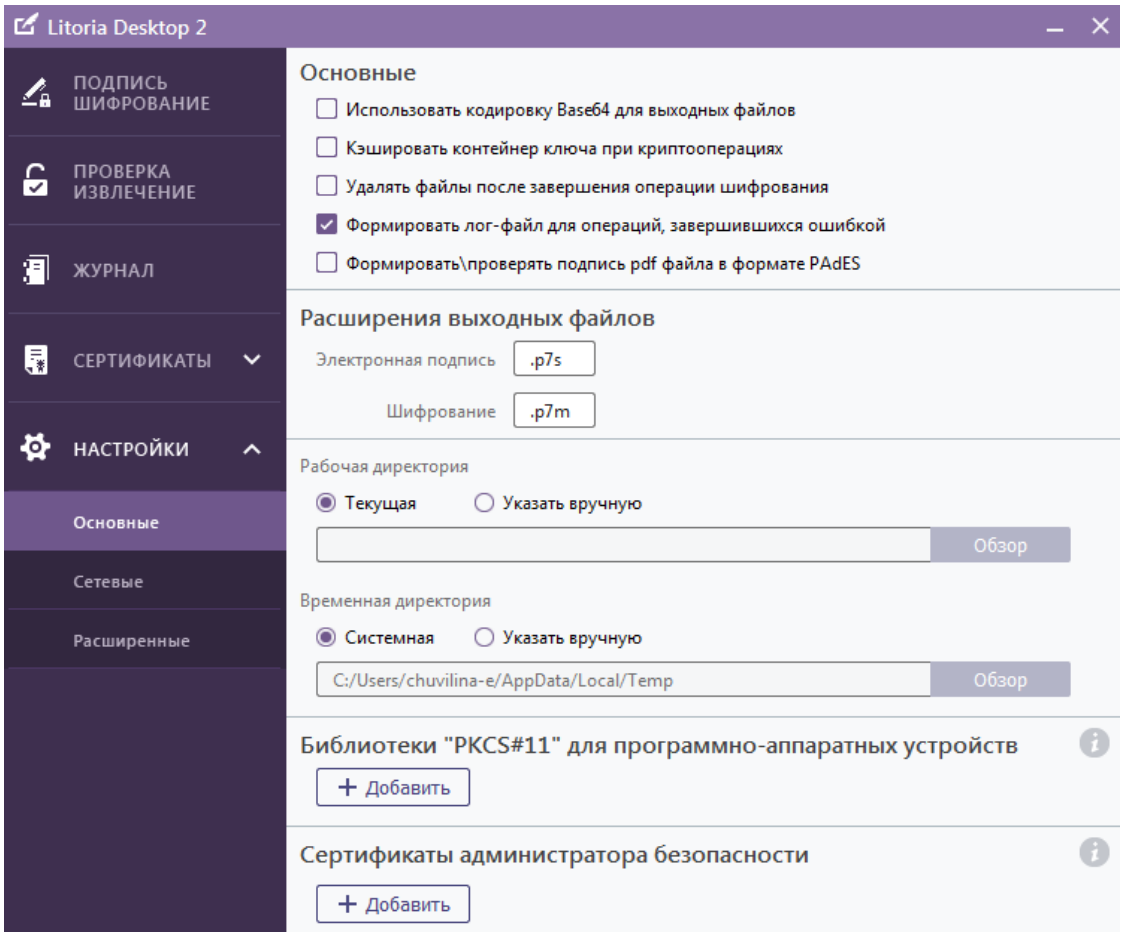

Рисунок 3.3 – Настройка формирования лог-файла

3.1.5 Формирование/проверка подписи pdf-файла в формате PAdES

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

По умолчанию формирование ЭП файла формата PDF осуществляется в формате CAdES, при этом расширение файла не изменится (рисунок 3.4).

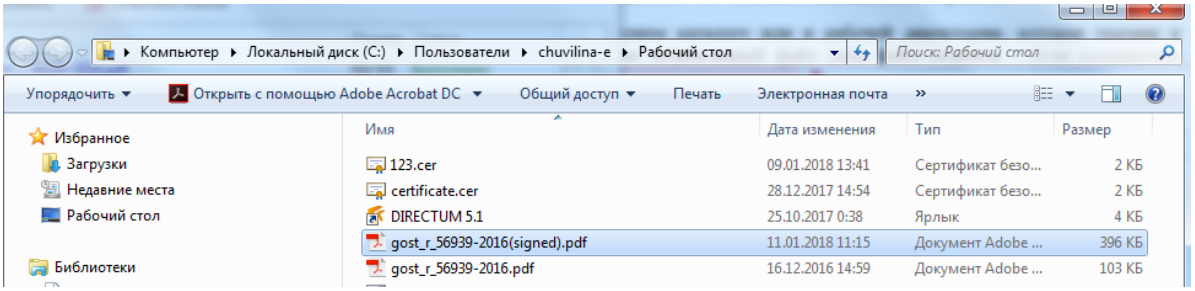

Рисунок 3.4 – Результат подписи pdf-файла в формате CAdES

Pdf-файлы, со сформированной ЭП в формате CAdES, могут добавляться и проверяться в более ранних версиях ПК «Litoria Desktop 2» без внесения в них изменений.

Для изменения формата подписи pdf-файлов на PAdES, необходимо установить флаг *«Формировать\проверять подпись pdf файла в формате PAdES»*.

> Параметры создания подписи для pdf-файлов в формате PAdES описываются в библиотеке «PdfSignature.dll», расположенной по пути установки комплекса (по умолчанию C:\Program Files (x86)\GIS\Litoria Desktop 2).

3.1.6 Расширения выходных файлов

В основных настройках, в области «*Расширения выходных файлов*» указаны расширения, используемые по умолчанию (рисунок 3.5):

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

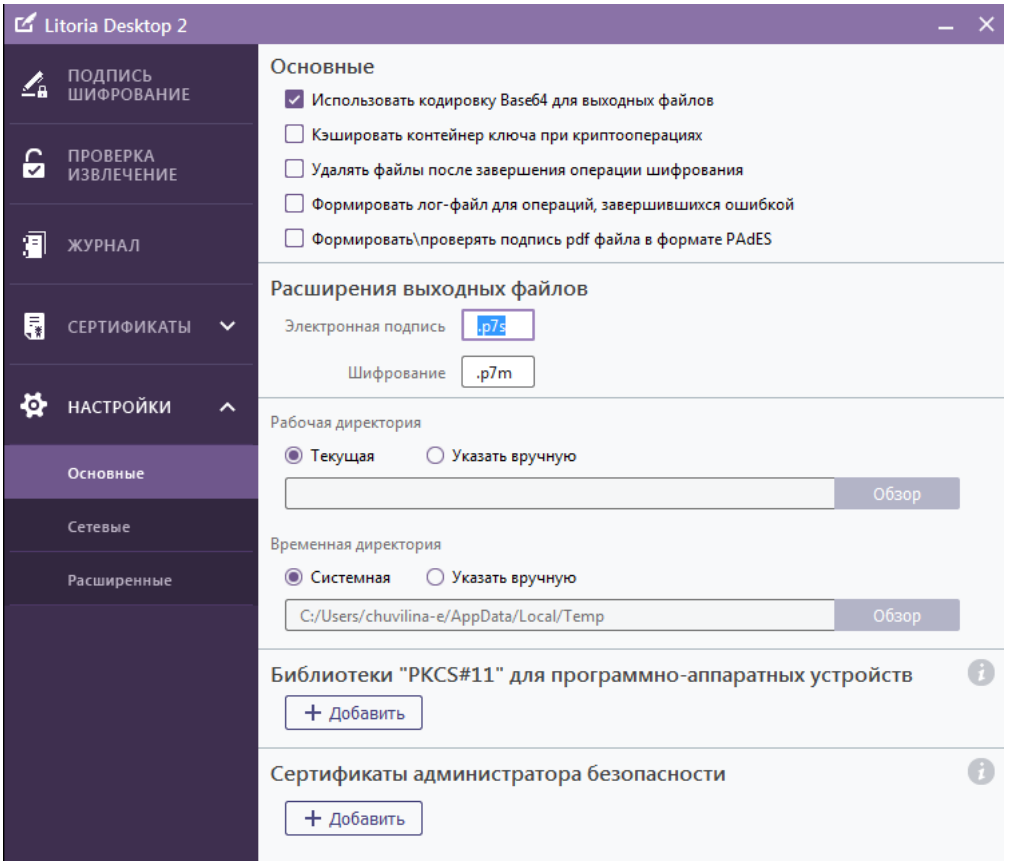

Рисунок 3.5 – Настройки расширений выходных файлов

Данные расширения хранятся в ветке реестра:

– для 32-битной ОС – HKEY_LOCAL_MACHINE\SOFTWARE\GIS\Litoria Desktop 2\Extensions;
– для 64-битной версии ОС – HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GIS\Litoria Desktop 2\Extensions.

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 выходных файлов сохраняются для всех пользователей компьютера.

3.1.7 Установка директорий

Указание рабочей директории, в которую будут записываться выходные файлы всех основных операций, осуществляется в области «*Рабочая директория*» пункта «*Основные настройки*» (рисунок 3.6). 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*».

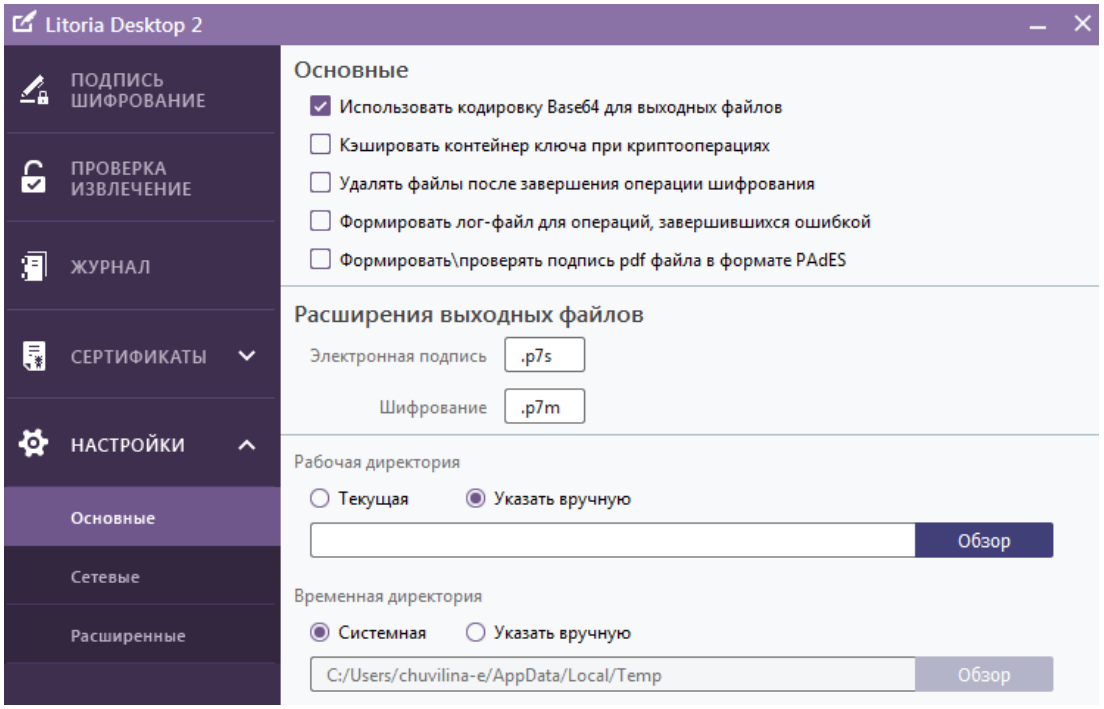

Рисунок 3.6 – Настройки директорий

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.

3.1.8 Добавление библиотек PKCS#11

Перед началом работы с отчуждаемыми носителями, необходимо добавить библиотеки PKCS#11. Добавление библиотек осуществляется в области «*Библиотеки «PKCS#11» для программно-аппаратных устройств*» пункта «*Основные настройки*».

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\rtpkcs11.dll) (рисунок 3.7).

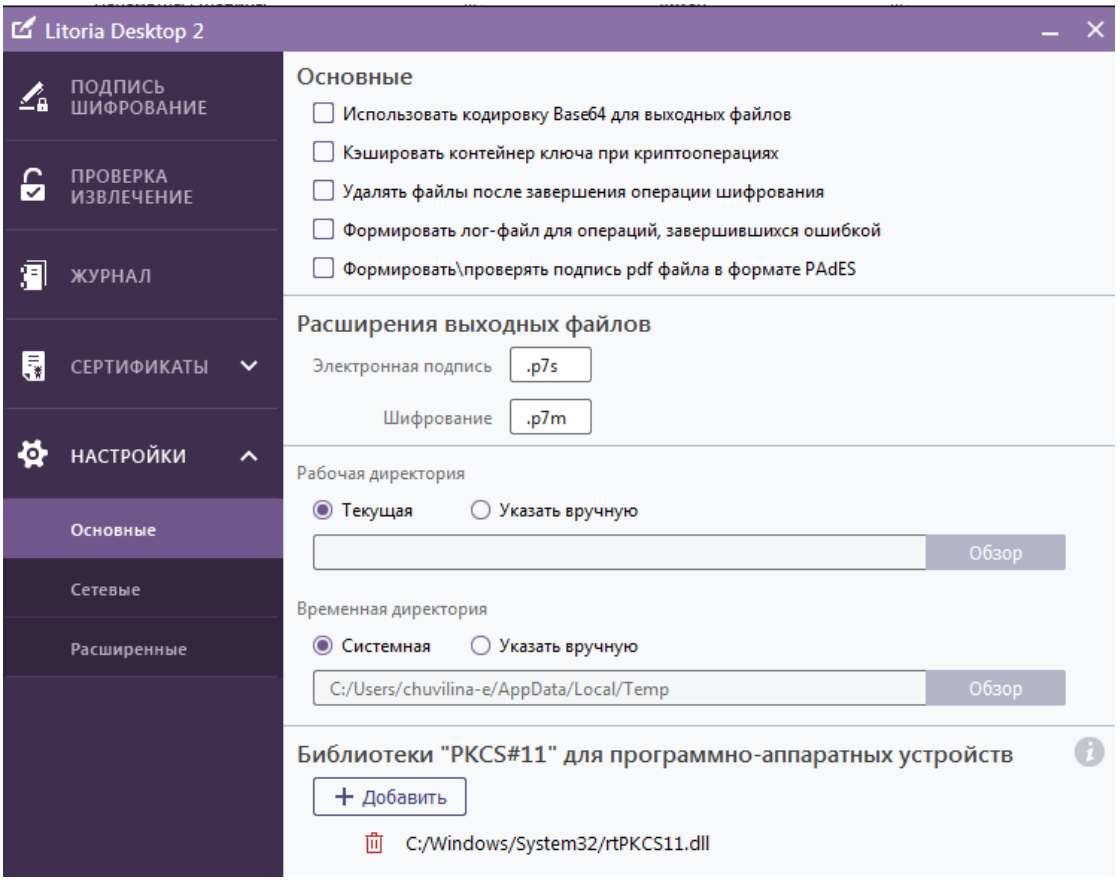

Рисунок 3.7 – Добавление библиотеки PKCS#11

3.1.9 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 3.8).

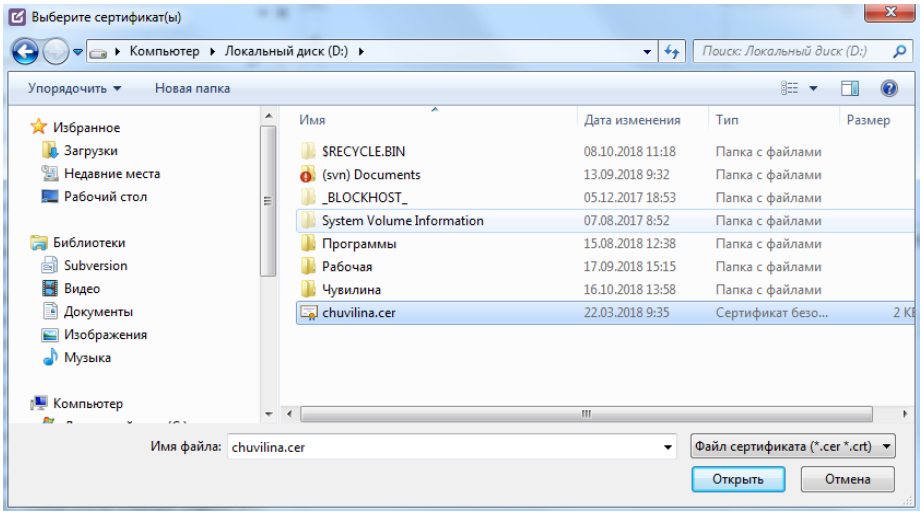

Рисунок 3.8 – Выбор сертификата администратора безопасности

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 3.9).

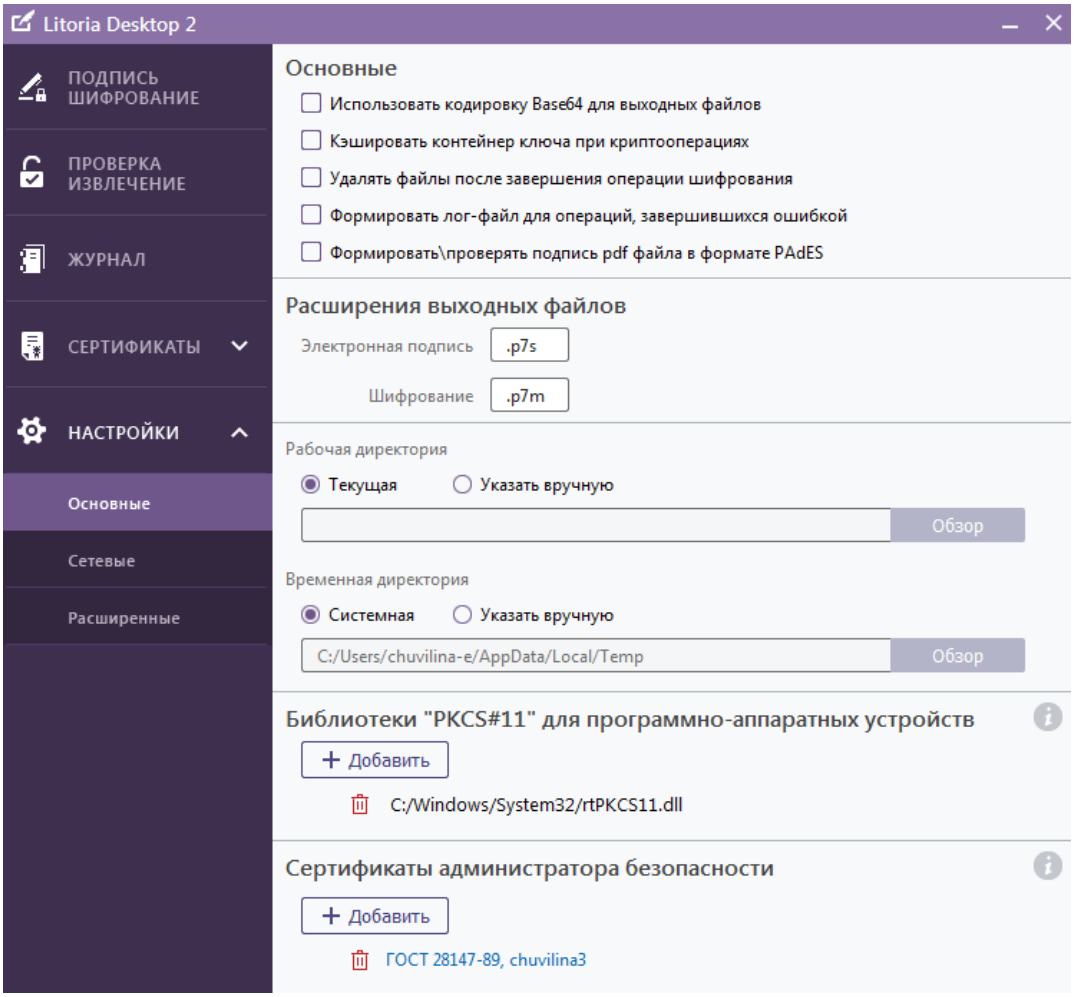

Рисунок 3.9 – Отображение выбранного сертификата администратора безопасности

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

3.2 Сетевые настройки

Вкладка «*Сетевые настройки*» позволяет выполнять настройки:

- адреса используемой службы штампов времени;
- службы DVCS;
- 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 3.10).

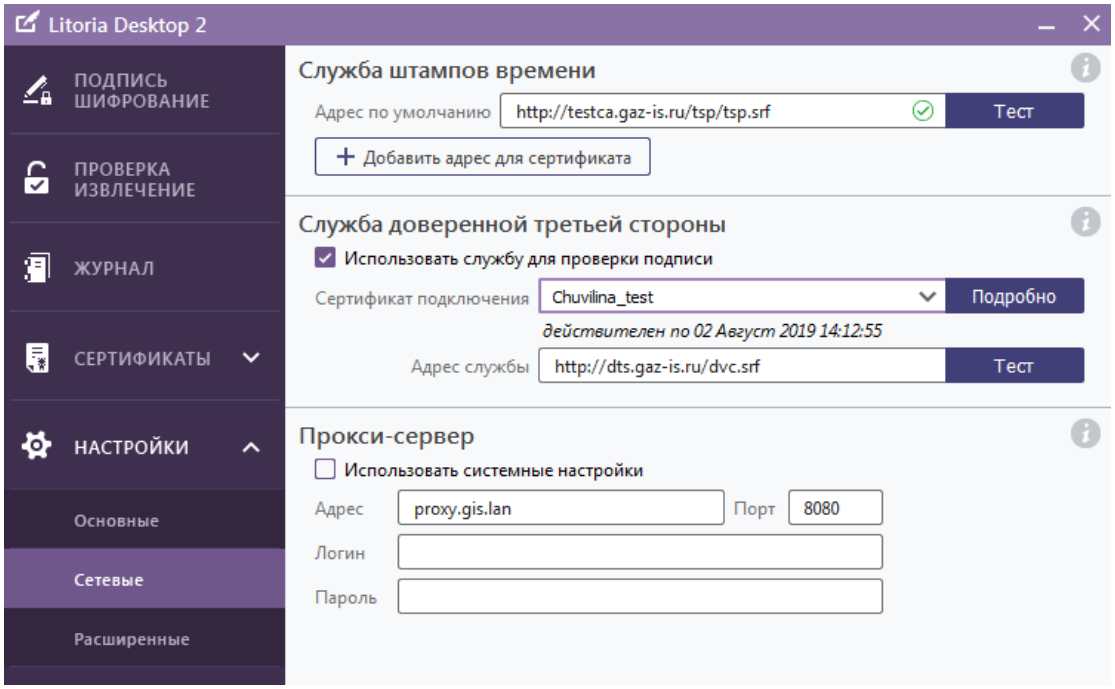

Рисунок 3.10 – Настройка адреса службы штампов времени

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 3.11). 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.

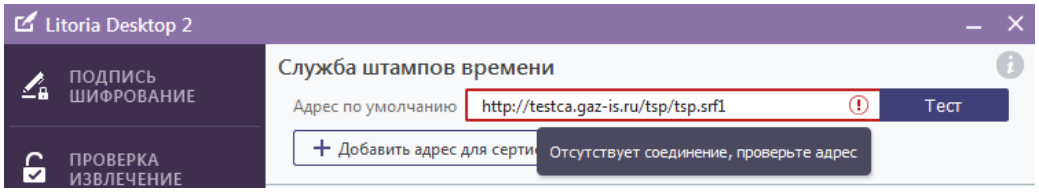

Рисунок 3.11 – Сообщение об ошибке «Отсутствует соединение»

В случае сообщения об ошибке «Нет доверия к сертификату службы» (рисунок 3.12), необходимо нажать на ссылку с сообщением, для получения детальной информации о сертификате службы, с дальнейшей возможностью разрешения проблемы доверия.

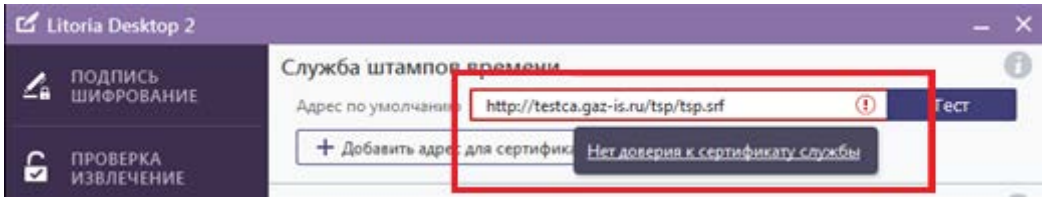

Рисунок 3.12 – Сообщение об ошибке «Нет доверия к службе»

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 3.13).

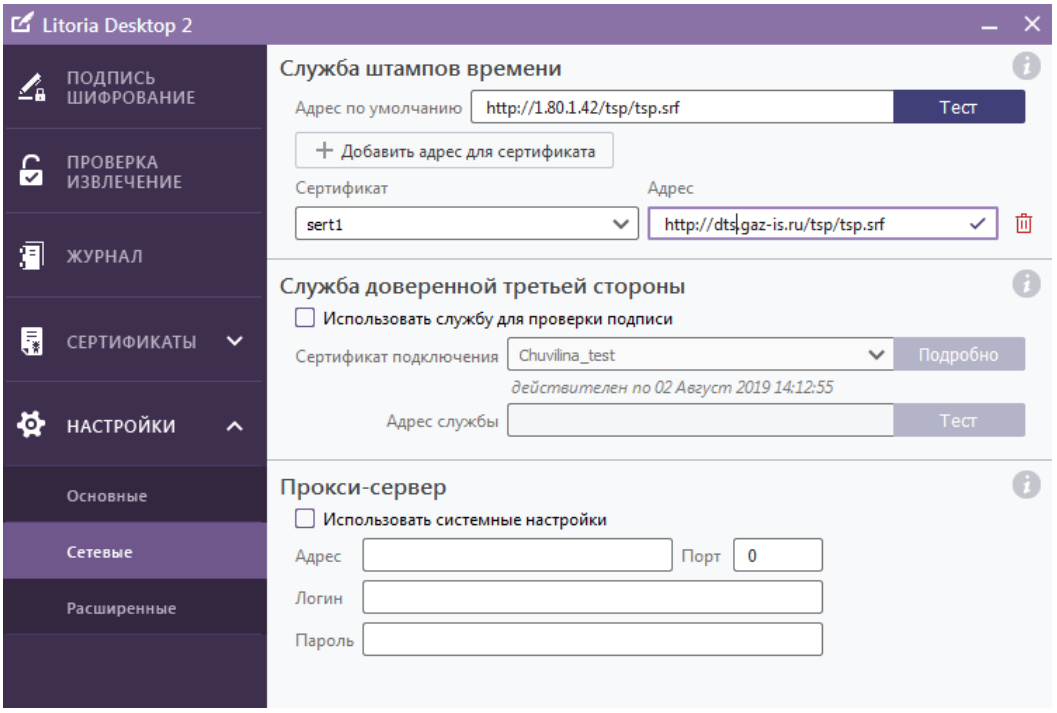

Рисунок 3.13 – Добавление адреса службы штампов времени для сертификата

3.2.2 Настройки службы доверенной третьей стороны

Для проверки подписи с использованием службы доверенной третьей стороны, необходимо установить флаг «*Использовать службу доверенной третьей стороны для проверки подписи*» в области «*Служба доверенной третьей стороны*» (рисунок 3.14). При этом станут доступными для заполнения поля «*Сертификат подключения*» и «*Адрес службы*».

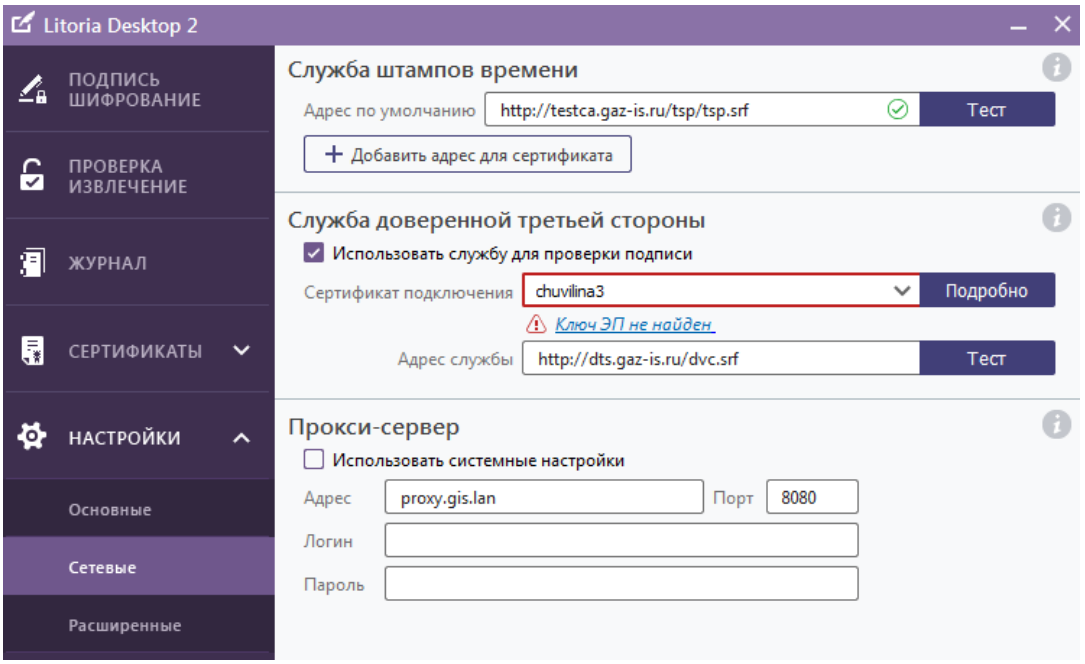

Рисунок 3.14 – Настройки службы доверенной третьей стороны

Для указания сертификата для подключения к службе доверенной третьей стороны в поле «*Сертификат подключения*» выберите из списка свой личный сертификат, который ранее был зарегистрирован на сервере ДТС.

Если ключ ЭП выбранного сертификата не будет обнаружен в реестре, то внизу поля появится сообщение «*Ключ ЭП не найден*» (рисунок 3.14).

Для ввода пин-кода, нажмите на ссылку «*Ключ ЭП не найден*» и в появившемся окне укажите в соответствующем поле пин-код к контейнеру (рисунок 3.15) и нажмите на кнопку «*Проверить*».

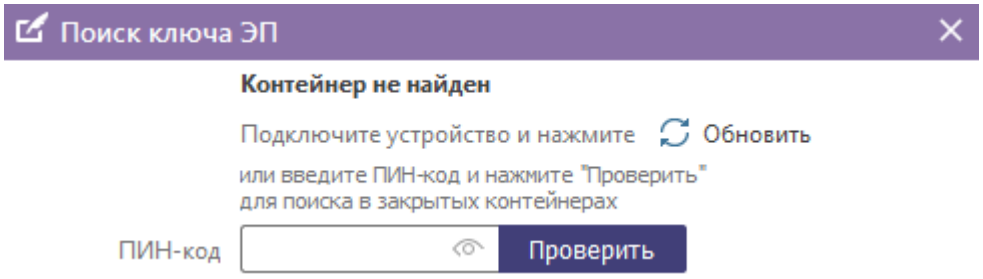

Рисунок 3.15 – Поиск ключа ЭП

Если пин-код к контейнеру не был найден, проверьте наличие физического отчуждаемого носителя в нужном разъеме (при его использовании) и нажмите кнопку «*Обновить*» (рисунок 3.15).

Если данные указаны верно, внизу поля с сертификатом появится сообщение о сроке действия сертификата (рисунок 3.16). Сертификат готов к использованию.

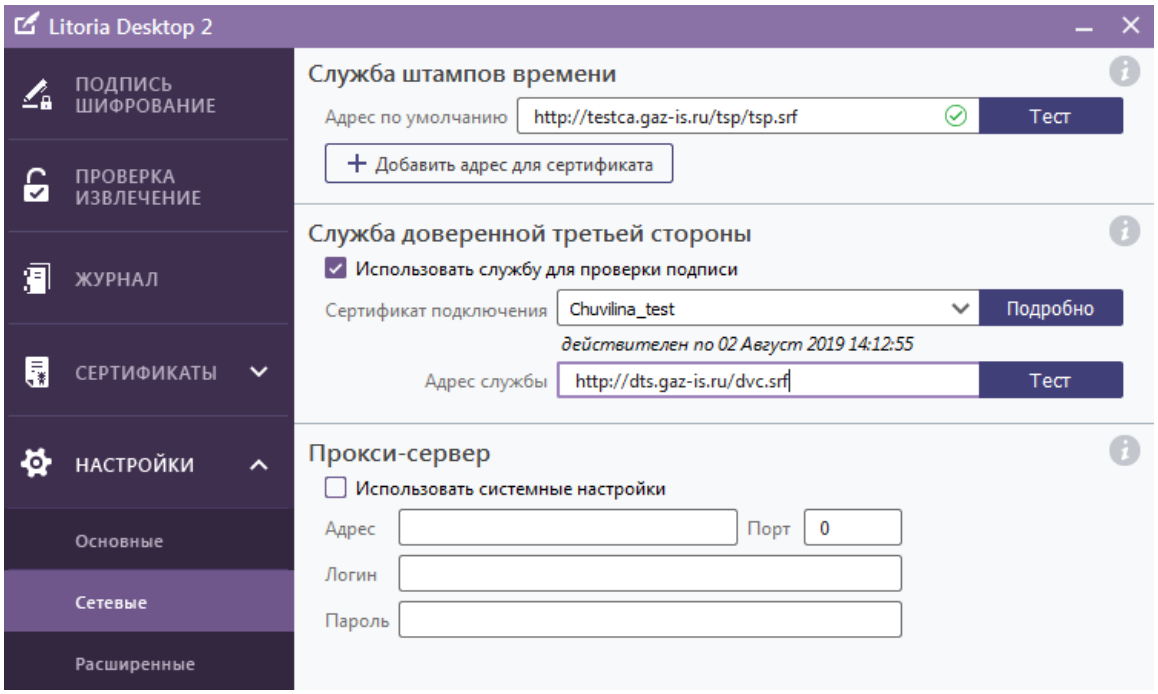

Рисунок 3.16 – Готовность сертификата к использованию

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 3.17), 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).

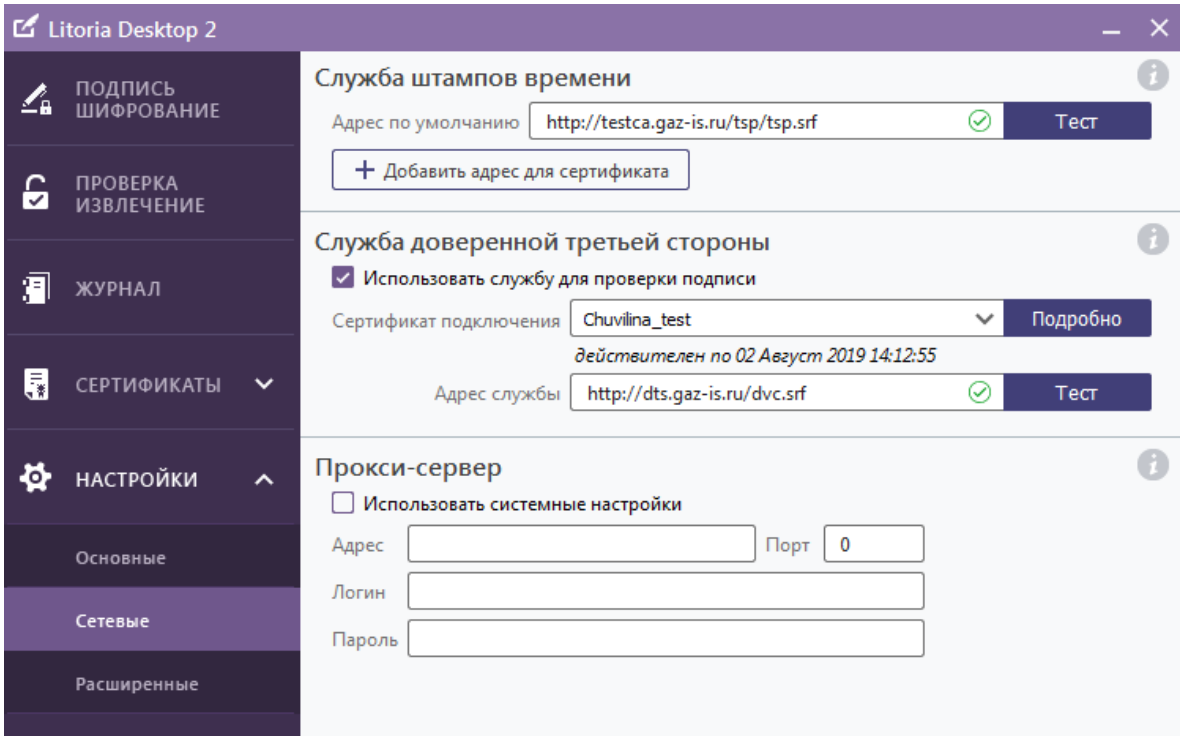

Рисунок 3.17 – Проверка работоспособности службы доверенной третьей стороны

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 3.18).

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.

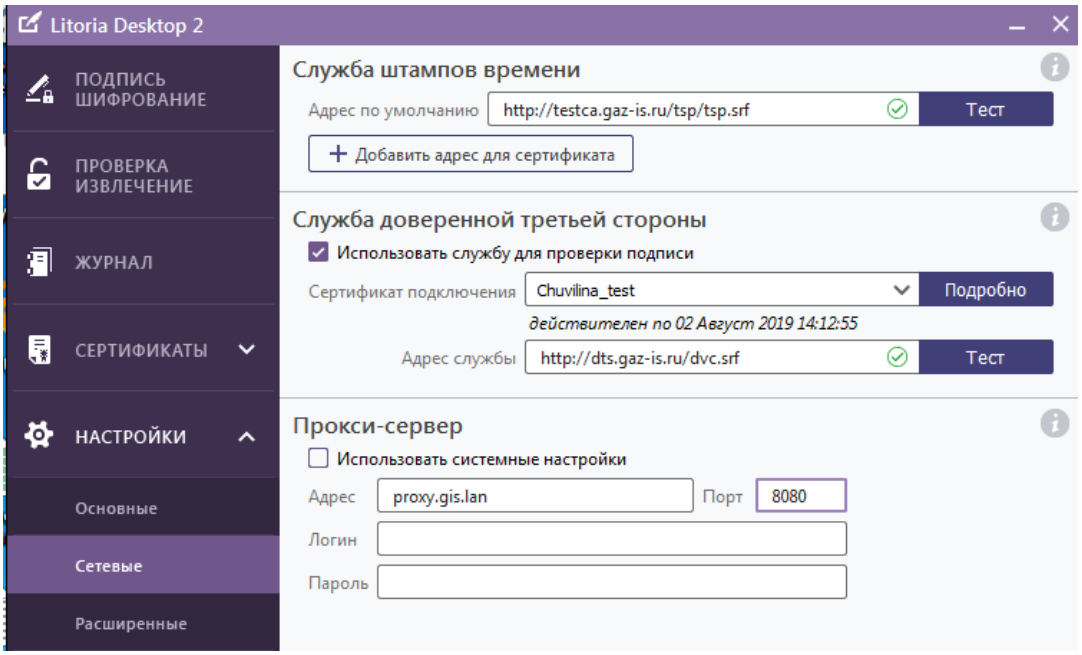

Рисунок 3.18 – Настройки прокси-сервера

3.3 Расширенные настройки

Вкладка «*Расширенные настройки*» позволяет выполнять настройки использования квалифицированного режима и настроить ограничения использования сертификата.

3.3.1 Квалифицированный режим

При использовании квалифицированного 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 **http://e-trust.gosuslugi.ru/MainCA**.

Для использования квалифицированного режима, необходимо зайти в пункт меню «*Настройки*» вкладка «*Расширенные*» и в области «*Квалифицированный режим*» установить флаг «*Включить режим квалифицированной подписи*» (рисунок 3.19).

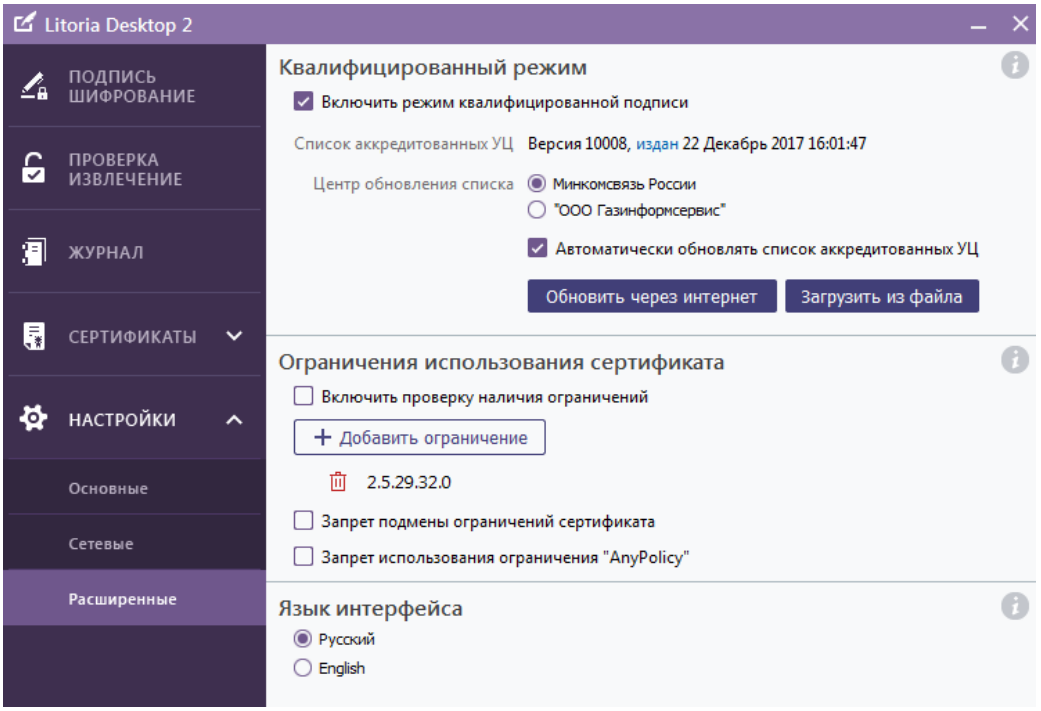

Рисунок 3.19 – Настройка использования квалифицированного режима

Установка флага возможна только при наличии актуального списка аккредитованных УЦ. При отсутствии списка, включение режима квалифицированной подписи недоступно (рисунок 3.20).

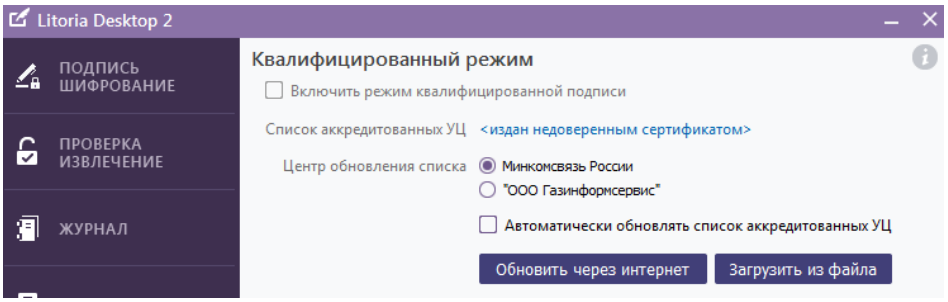

Рисунок 3.20 – Список аккредитованных УЦ, изданный недоверенным сертификатом

Скачать актуальный список аккредитованных УЦ можно через интернет с сайта Минкомсвязи РФ или с Центра обновлений GIS или загрузить из ранее скаченного файла.

По ссылке «*издан*» (рисунок 3.19) возможно просмотреть и проверить на действительность сертификат, выпустивший список аккредитованных УЦ (рисунок 3.21).

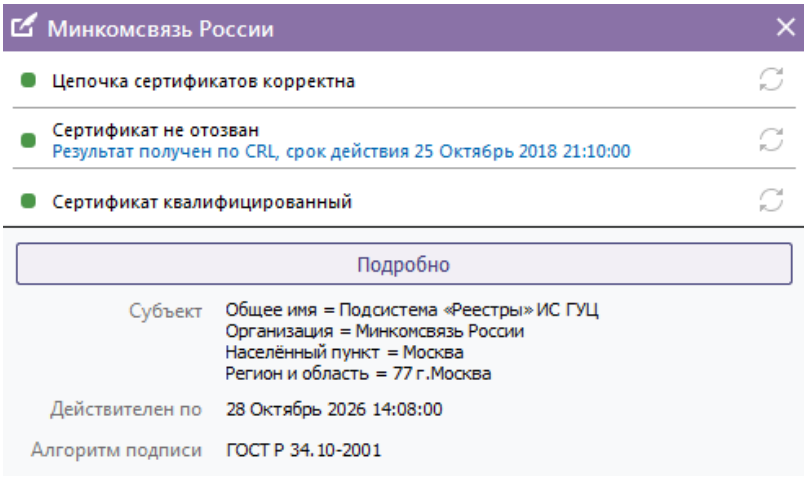

Рисунок 3.21 – Просмотр сертификата Минкомсвязи России

Для выбора места скачивания списка аккредитованных УЦ установите переключатель на выбранную позицию в поле «*Центр обновления списка*».

При необходимости, установите флаг в поле «*Автоматически обновлять список аккредитованных УЦ*».

При нажатии кнопки «*Обновить через интернет*», поиск актуального списка аккредитованных УЦ будет осуществляться на сайте по выбранному выше местоположению.

При выборе «*Загрузить из файла*» откроется окно «*Выберите файл TSL*» в котором необходимо выбрать файл, содержащий список аккредитованных УЦ, и нажать на кнопку «*Открыть*» (рисунок 3.22).

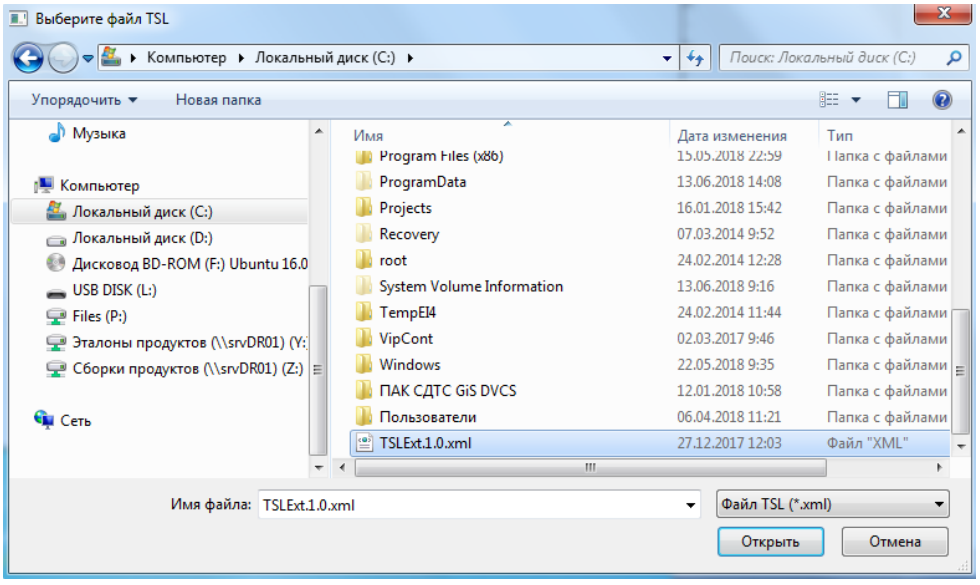

Рисунок 3.22 – Окно выбора TSL файла

3.3.2 Ограничения использования сертификата

Для указания политик сертификата, определяющих правила его использования, выберите 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 3.23).

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

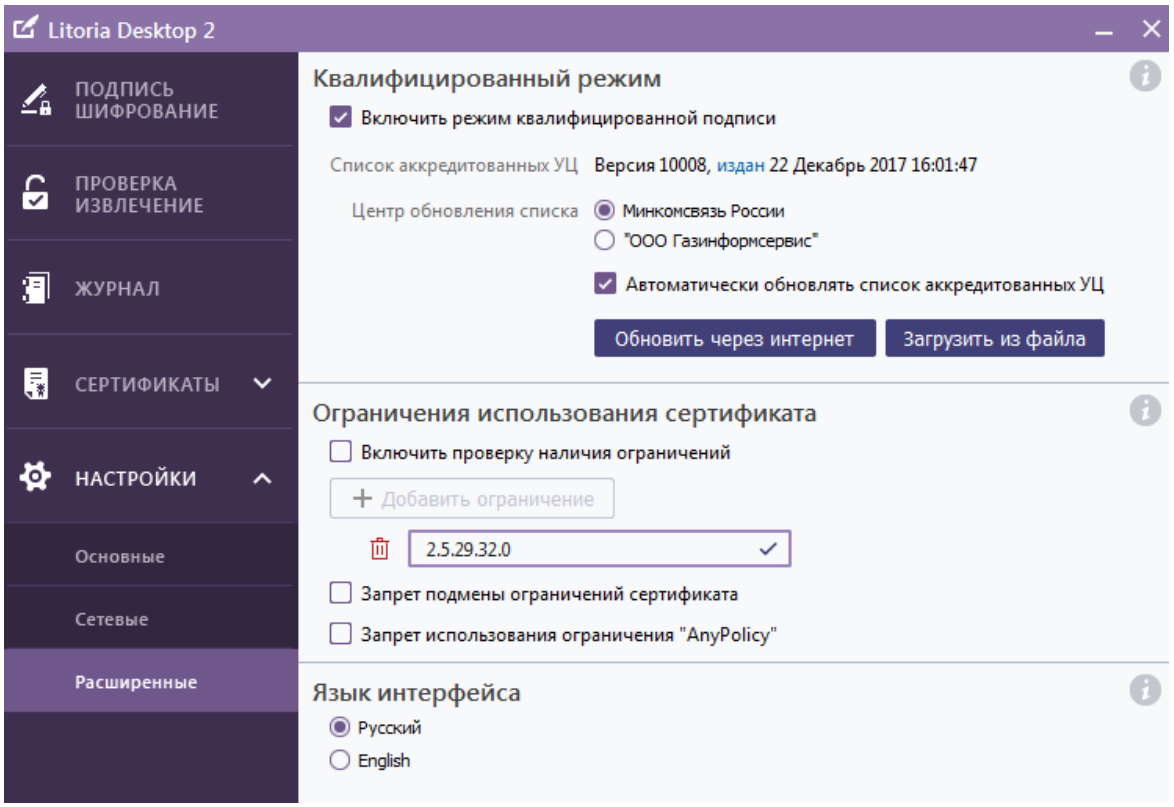

Рисунок 3.23 – Добавление пользовательской политики

Установите флаги:

- «*Включить проверку наличия ограничений*» – если необходимо, чтобы сертификат имел расширения, указанные ниже в поле ввода добавления ограничения (рисунок 3.20);
- «*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 Язык интерфейса ПК «Litoria Desktop 2»

По умолчанию интерфейс ПК «Litoria Desktop 2» русскоязычный.

Для смены языка интерфейса во вкладке «*Расширенные*» в области «*Язык интрефейса*» установите переключатель в нужную позицию (рисунок 3.24). Изменения вступят в силу после перезагрузки ПК «Litoria Desktop 2».

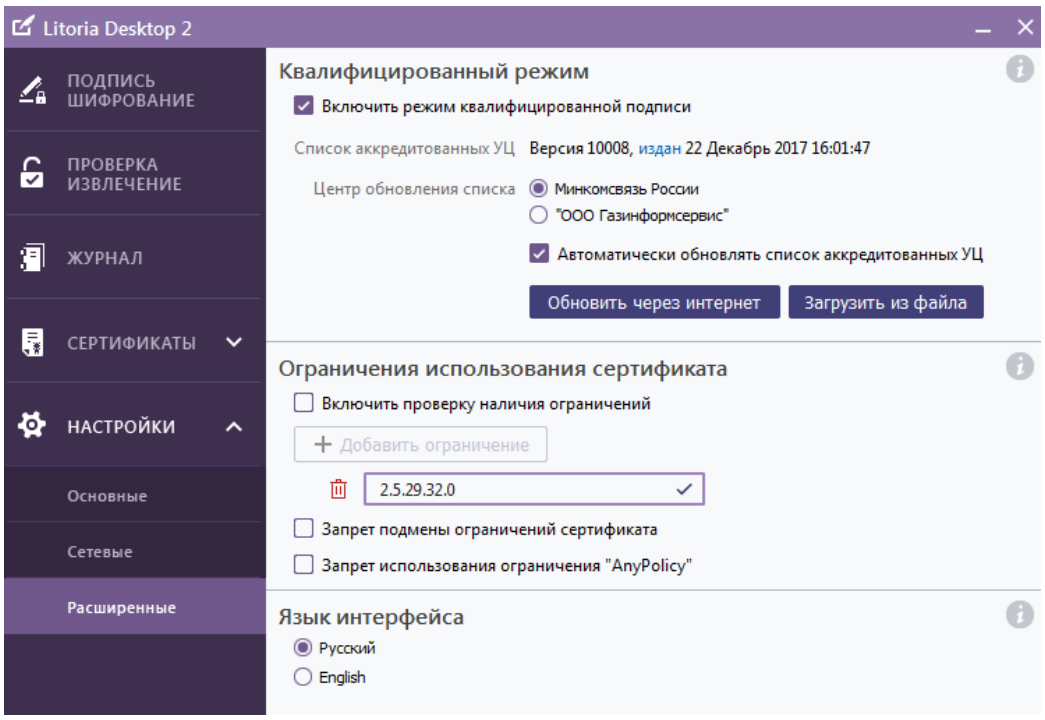

Рисунок 3.24 – Смена языка интерфейса

4 Журнал событий

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

Во вкладке «*Журнал*» (рисунок 4.1) отображаются операции создания, добавления, заверения и проверки ЭП, шифрования и извлечения файлов. А также результаты успешности произведенных операций.

По каждой операции указывается дата и время совершения события, тип события и статус выполнения.

В нижней части журнала отображается информация о выбранном событии:

– пользователь, выполнивший операцию;
– файлы, над которыми производилась операция;
– сертификат;
– лог ошибки – файл, содержащий информацию об ошибке.

Формирование лог-файла осуществляется, если установлен соответствующий флаг в меню «*Настройки*» –> «*Основные*». Установка флага описана в п.3.1.4.

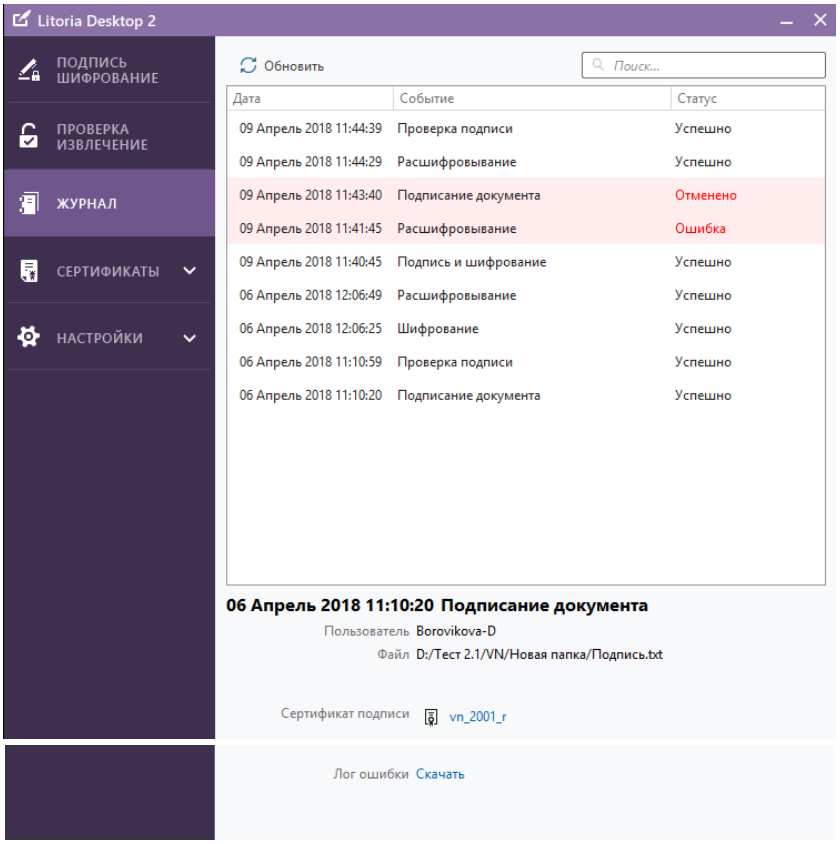

Рисунок 4.1 – Журнал событий

При необходимости можно отфильтровать события по дате, типу события или статусу. Для этого необходимо ввести требуемые значения в поле «*Поиск*».