ГАЗИНФОРМ СЕРВИС

Программный комплекс «Litoria Desktop 2»
Руководство пользователя

Санкт-Петербург, 2022

Аннотация

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

В разделе «Назначение ПК «Litoria Desktop 2» приводятся сведения о назначении и возможностях комплекса.

В разделе «Условия применения ПК «Litoria Desktop 2» указаны условия, необходимые для использования комплекса, требования к аппаратным средствам автоматизированного рабочего места (АРМ).

В разделе «Использование ПК «Litoria Desktop 2» описаны действия, необходимые для выполнения основных функций комплекса из интерфейса.

В разделе «Применение сертификатов, отличных от стандарта ГОСТ» описана поддержка ПК «Litoria Desktop 2» сертификатов ключа проверки подписи, созданных на основе алгоритмов, отличных от ГОСТ.

В разделе «Журнал событий» описываются действия пользователя, которые сохраняются в журнале событий ПК «Litoria Desktop 2».

В разделе «Вычисление контрольных сумм файлов» описываются действия пользователя по расчету хеш-сумм файлов для проверки целостности и достоверности данных.

Содержание

1 Назначение ПК «Litoria Desktop 2»

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

2 Условия применения ПК «Litoria Desktop 2»

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

– Windows 7 (32 бит/64 бит) [2];
– 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).

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», которое используется для формирования электронной подписи и шифрования электронных документов.

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

3 Использование ПК «Litoria Desktop 2»

3.1 Интерфейс комплекса

В интерфейсе пользователю доступны следующие функции ПК «Litoria Desktop 2»:

- создание нового запроса на сертификат, в т.ч. подписанного актуальной ЭП;
- 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 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;
- создание, добавление, заверение ЭП для файлов произвольного типа;
- создание, добавление, заверение ЭП для pdf документов по стандартам CAdES/PAdES; [3]
- создание, добавление, заверение ЭП для xml документов по стандартам CAdES/XAdES;
- 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;
- вычисление контрольных сумм файлов по алгоритмам ГОСТ.

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

Вид главного окна интерфейса комплекса представлен на рисунке 3.1.

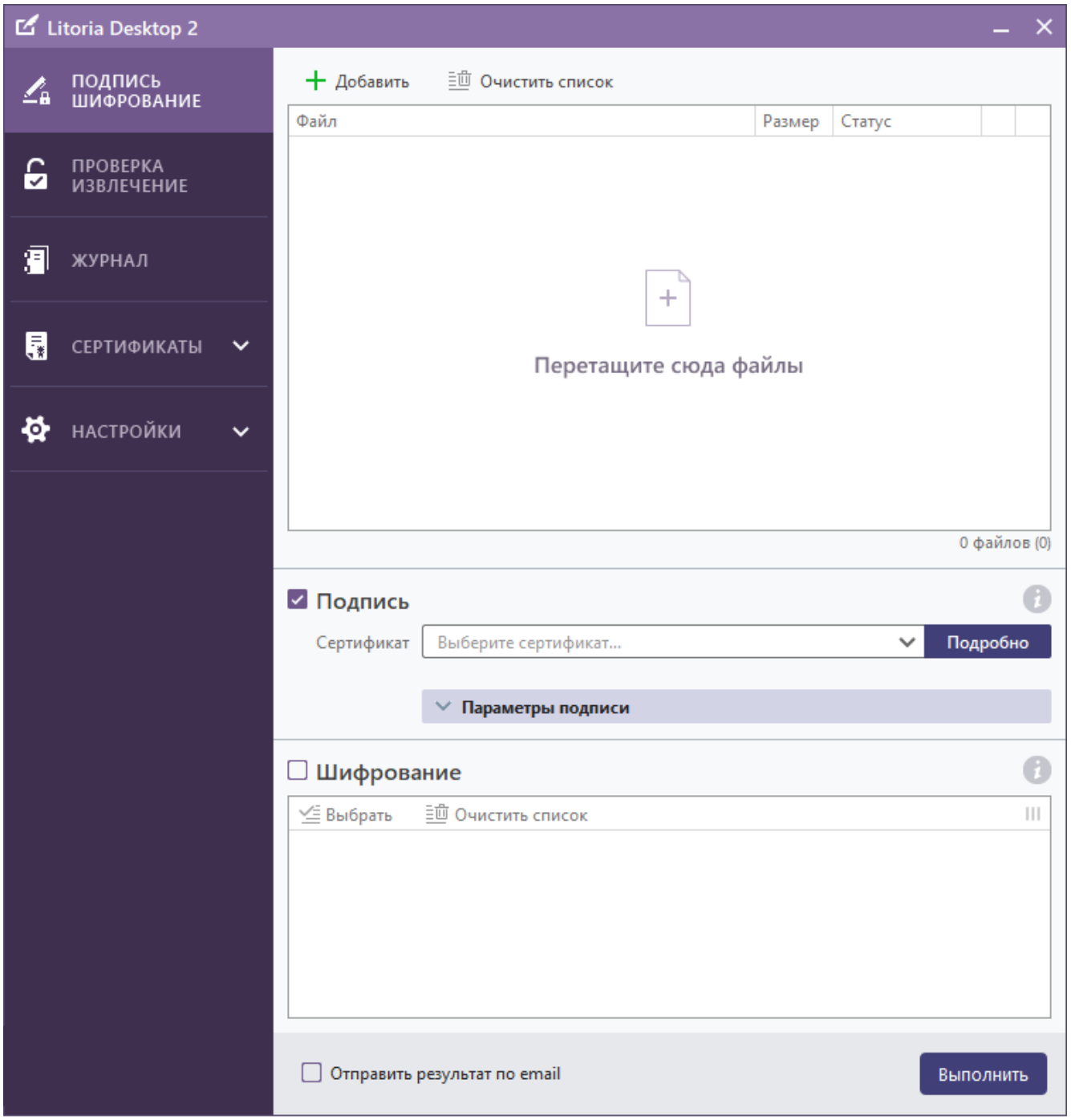


Рисунок 3.1 – Главное окно интерфейса комплекса

3.2 Получение личного сертификата и ключевой информации к нему

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 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 необходимо отправить на рассмотрение в УЦ и на основе него УЦ выпустит сертификат ключа проверки ЭП.

Необходимые действия для выполнения этих операций с помощью ПК «Litoria Desktop 2» описаны ниже в соответствующих разделах.

3.2.1 Создание нового запроса на сертификат

1 Откройте интерфейс ПК «Litoria Desktop 2».
2 Раскройте пункт меню «*Сертификаты*».
3 Выберите операцию «*Запрос на сертификат*» (рисунок 3.2).

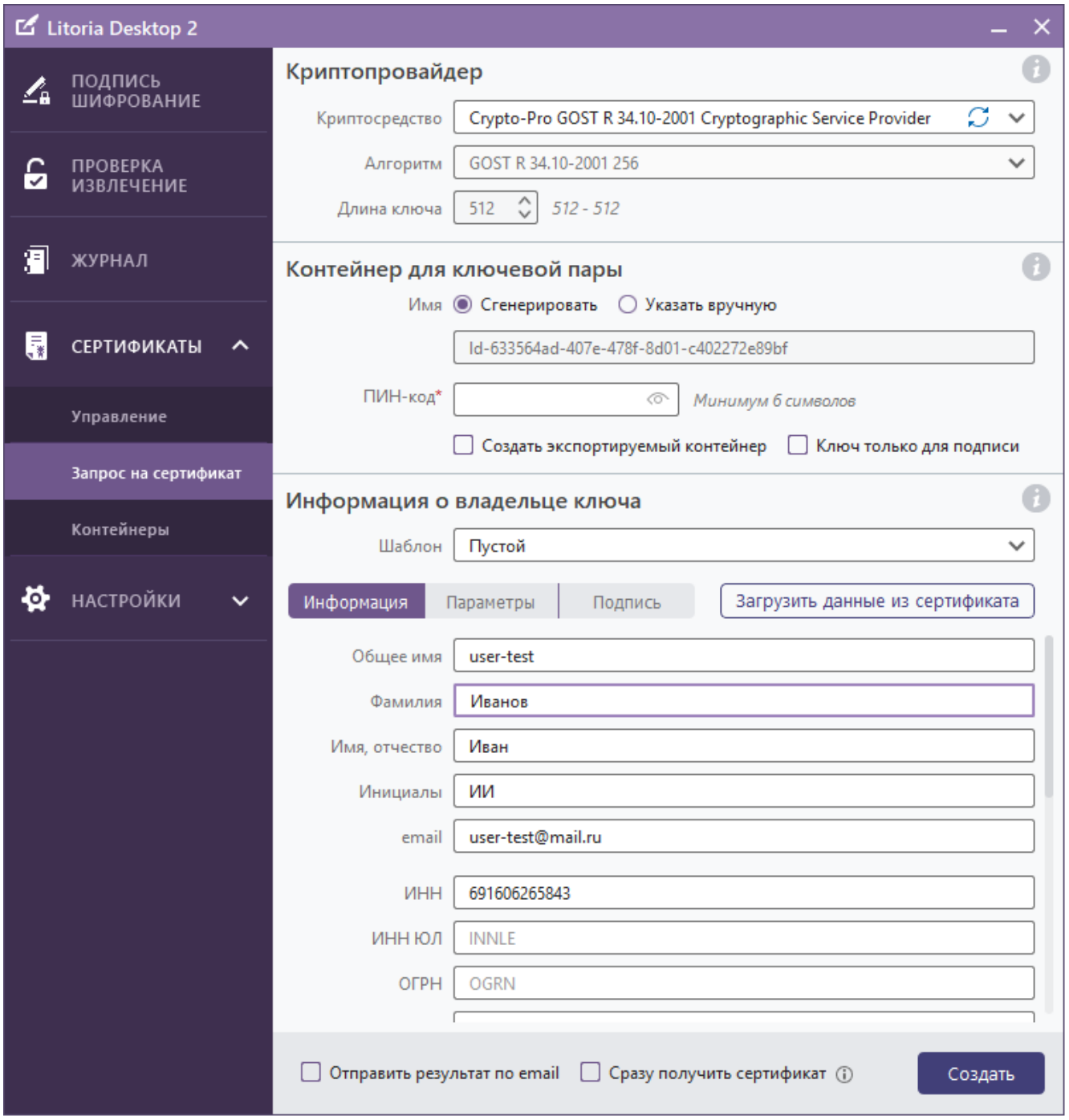


Рисунок 3.2 – Создание запроса на сертификат

Запрос на сертификат можно создавать на основе предустановленного шаблона: в области «*Информация о владельце ключа*» в поле «*Шаблон*» необходимо выбрать название шаблона, на основе которого будет создан запрос на сертификат.

При необходимости создания пользовательского шаблона, отличного от уже заведенного в комплексе базового набора шаблонов, необходимо обратиться к администратору комплекса, для создания шаблона с требующимися настройками в файле *templates.xml*.

4 При использовании физического отчуждаемого носителя вставьте его в нужный разъем.

5 В области «*Криптопровайдер*» (перечень криптографических алгоритмов, поддерживаемых ПК «Litoria Desktop 2» приведен в таблице 3.1) укажите следующую информацию:

- криптосредство, которое будет использовано при создании сертификата;
- алгоритм;
- длина ключа (рядом с полем указаны минимальное и максимальное значения длины, в битах);

Таблица 3.1 – 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

6 В области «*Контейнер для ключевой пары*» укажите информацию о ключевом контейнере:

- вид генерации имени ключевого контейнера:
  - при установке переключателя «*Сгенерировать*» имя будет создано автоматически;
  - при установке переключателя «*Указать вручную*» – в соответствующем текстовом поле укажите имя контейнера.
- ПИН-код к контейнеру (длина пароля должна быть не менее 6 символов);
- возможность сделать ключ ЭП экспортируемым – установка флага «*Создать экспортируемый контейнер*»;
- возможность создания пары ключей только для подписи данных – установка флага *«Ключ только для подписи»*.

7 В области «*Информация о владельце ключа*» введите личную идентификационную информацию, при необходимости выберите сертификат или шаблон для

запрашиваемого сертификата, и подпишите запрос (более подробно заполнение данной области описано в подпунктах 3.2.1.2 – 3.2.1.4).

8 Нажмите на кнопку «*Создать*».

9 Далее выполните действия, указанные в появившемся окне и во всех появляющихся в дальнейшем. Вид появляющихся окон зависит от выбранного для создания запроса криптопровайдера.

10 Если вы все сделали правильно, то появится окно, содержащее запрос на сертификат (рисунок 3.3).

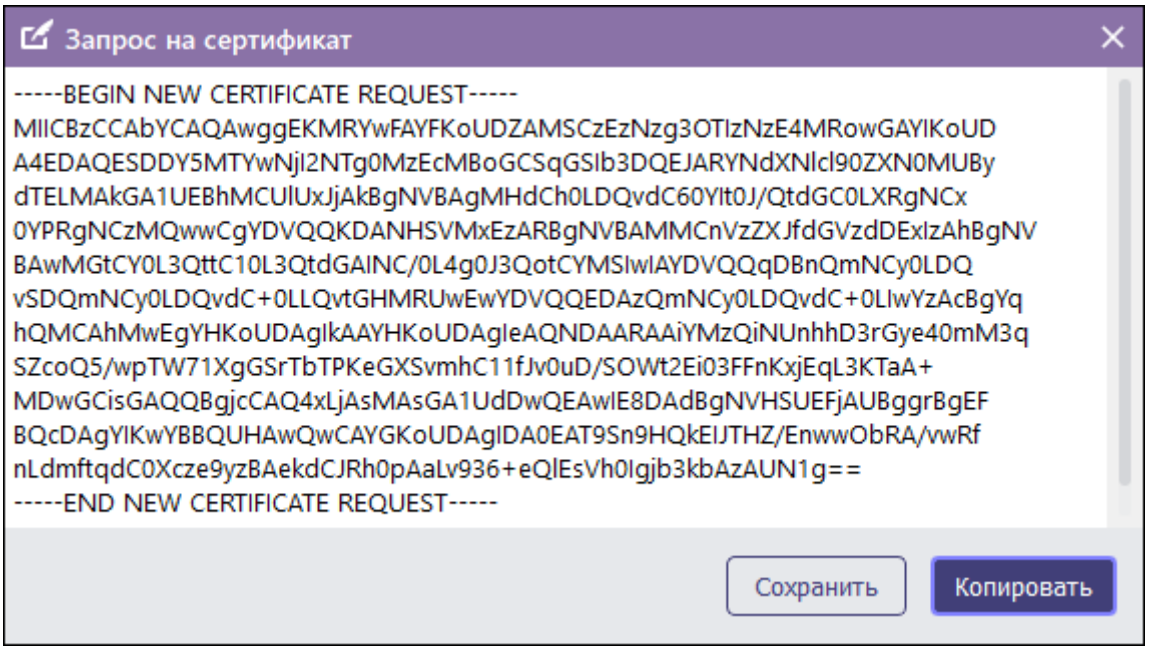


Рисунок 3.3 – Успешное создание запроса на сертификат

11 Для сохранения запроса на сертификат нажмите на кнопку «*Сохранить*» (рисунок 3.4).

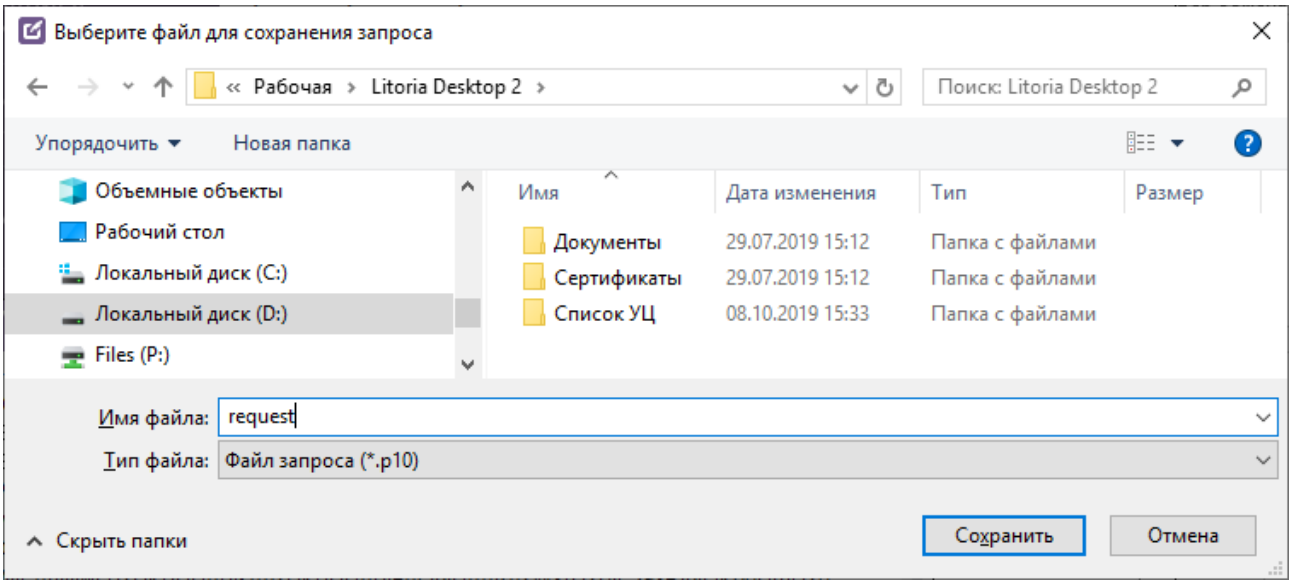


Рисунок 3.4 – Сохранение запроса на сертификат

12 Укажите имя файла для сохранения запроса на сертификат (например, request), его месторасположение, и нажмите на кнопку «*Сохранить*».

Результат: файл запроса, расположенный по пути и с именем, указанным выше, с расширением .p10, а на указанном ключевом носителе создан контейнер для будущего сертификата.

Файл запроса необходимо отправить в УЦ для создания на его основе вашего личного сертификата

13 При нажатии на кнопку «*Копировать*» (рисунок 3.3), текст запроса копируется в буфер памяти и скопированное сообщение можно самостоятельно вставить в поле запроса для отправки готового запроса PKCS#10 или PKCS#7 в кодировке Base64 на сайте УЦ.

3.2.1.1 *Создание самоподписанного сертификата*

Для создания самоподписанного сертификата необходимо последовательно выполнить пункты 1-7 раздела **3.2.1 «Создание нового запроса на сертификат»** при этом установив флаг *«Сразу получить сертификат»* (рисунок 3.5).

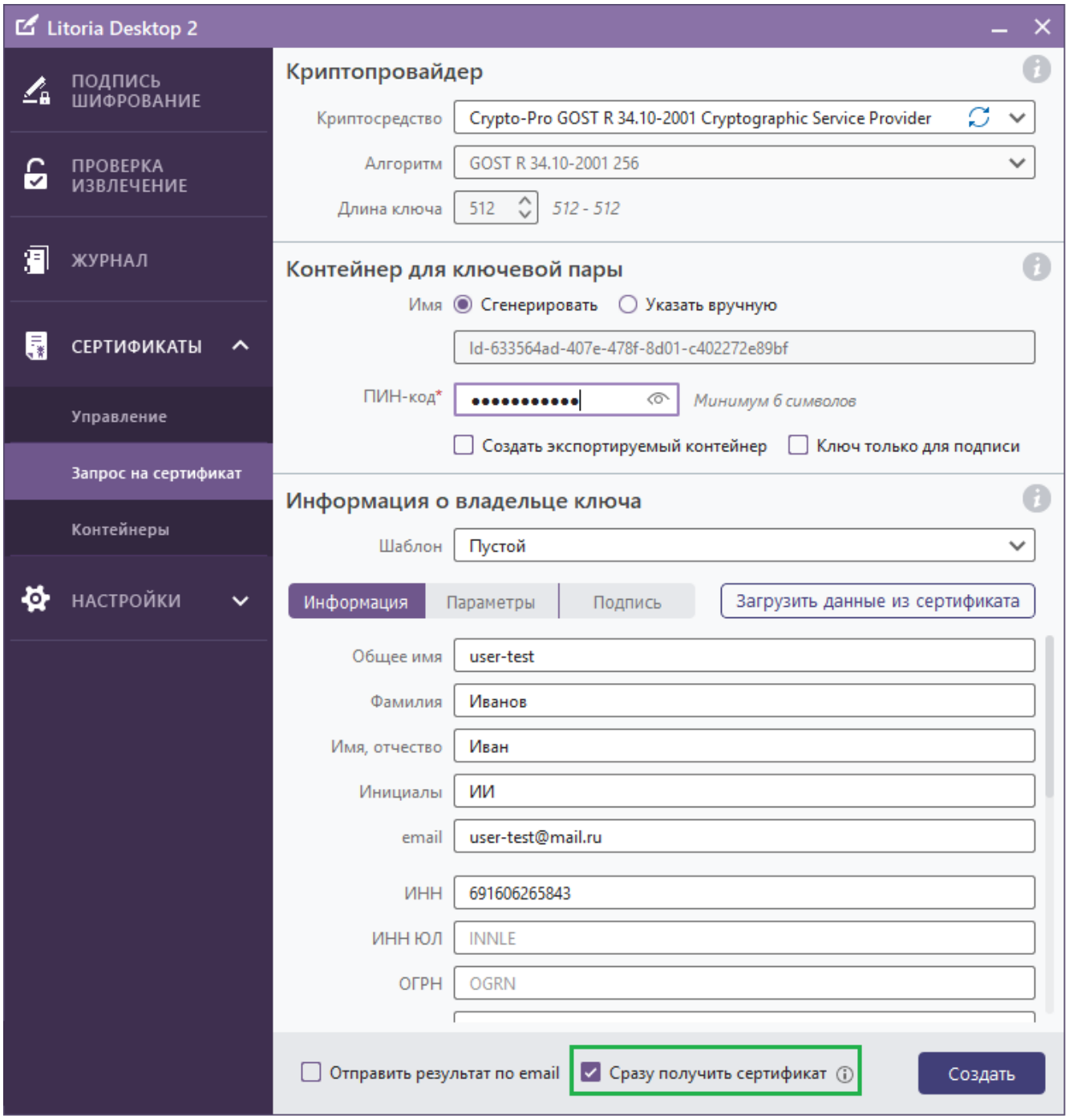


Рисунок 3.5 – Создание самоподписанного сертификата

После нажатия на кнопку *«Создать»* появится окно, содержащее самоподписанный сертификат (рисунок 3.6).

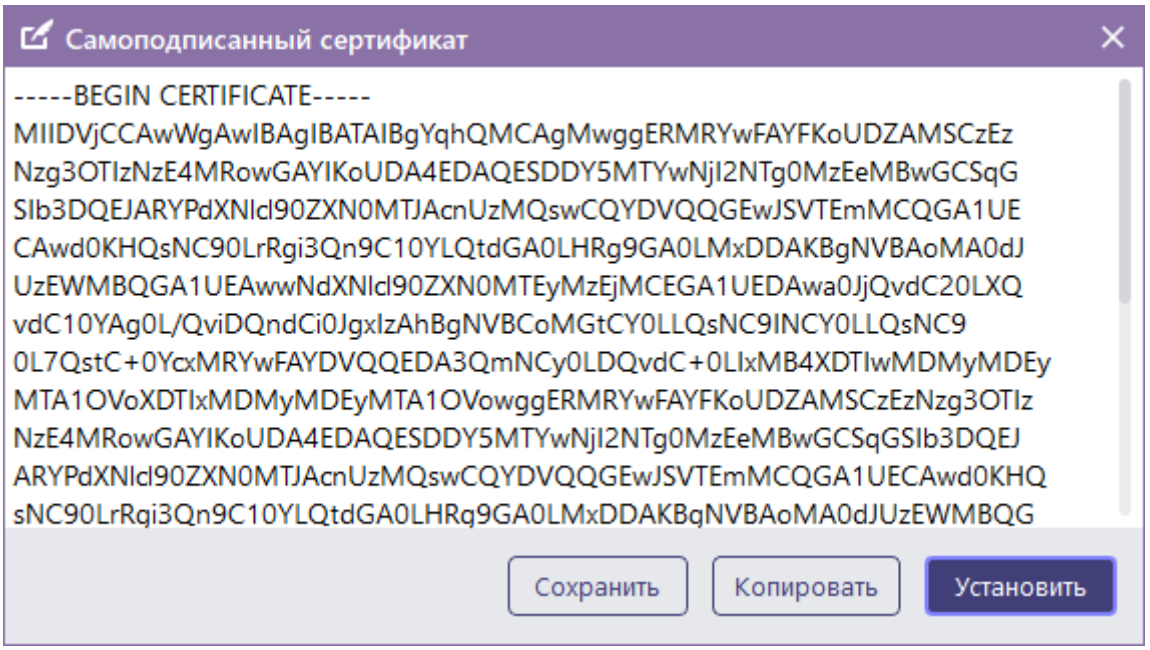


Рисунок 3.6 – Создание запроса на самоподписанный сертификат

Для установки самоподписанного сертификата на устройство или в хранилище сертификатов *«Личные сертификаты»,* в зависимости от выбранного криптопровайдера, нажмите кнопку «*Установить*».

3.2.1.2 Использование шаблонов при создании запроса на сертификат

В области «*Информация о владельце ключа*» вводится личная идентификационная информация о владельце сертификата.

Информация о создаваемом сертификате вводится на основании установленных параметров шаблона, выбранного в поле «*Шаблон*» (рисунок 3.2):

1 При выборе одного из предустановленных шаблонов:
- во вкладке «*Информация*» появятся обязательные к заполнению поля, обозначенные «*», заполнение которых задано в шаблоне (состав полей вкладки также будет меняться в зависимости от установок шаблона);
- установленные значения вкладки «*Параметры*» задаются шаблоном и недоступны для изменения (рисунок 3.7).

2 При выборе пустого шаблона:
- во вкладке «*Информация*» будут отображены все поля сертификата, возможные к заполнению, при этом их заполнение не обязательно;
- значения вкладки «*Параметры*» изменяемы и задаются вручную.

3 При выборе шаблона на основе сертификата:
- все поля вкладки «*Информация*» заполняются данными из выбранного сертификата, при этом значения можно менять;
- значения вкладки «*Параметры*» заполняются данными из выбранного

сертификата и не доступны для изменения.

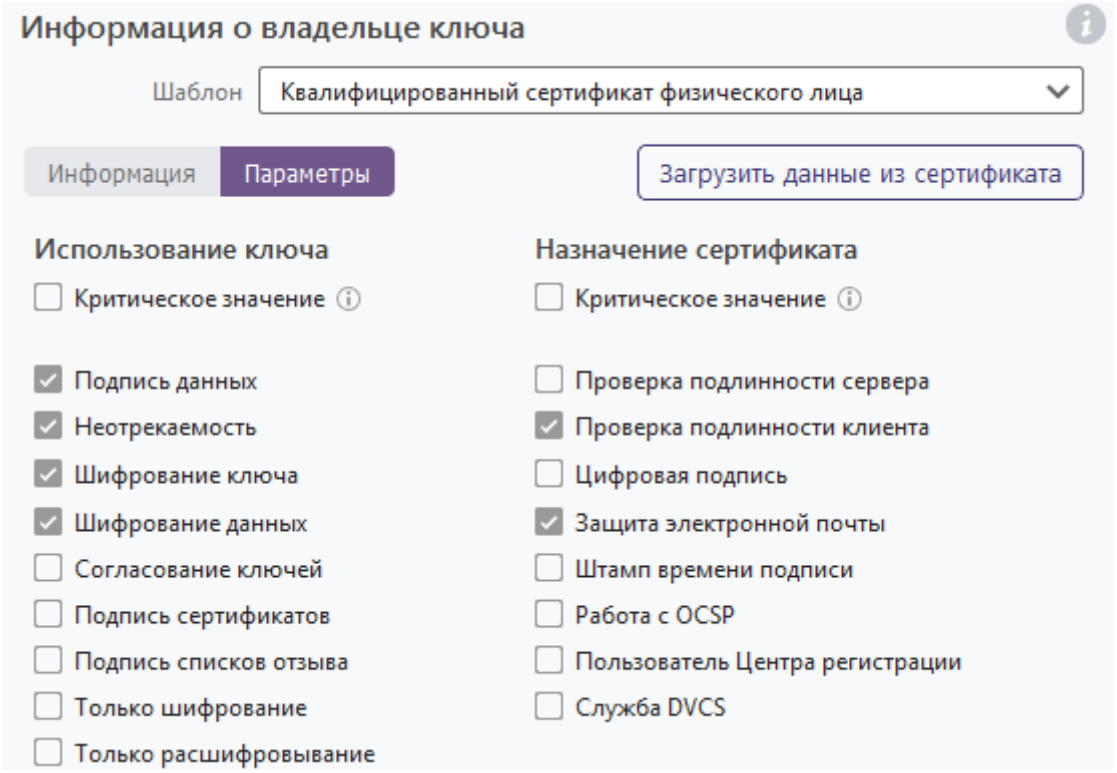


Рисунок 3.7 – Вкладка «*Параметры*»

3.2.1.3 Создание запроса на основе имеющегося сертификата

1 Для создания запроса на основании данных уже имеющегося сертификата, в области «*Информация о владельце ключа*» нажмите кнопку «*Загрузить данные из сертификата*» (рисунок 3.2).

2 В появившемся окне (рисунок 3.8) выберите необходимый файл сертификата и нажмите на кнопку «*Открыть*».

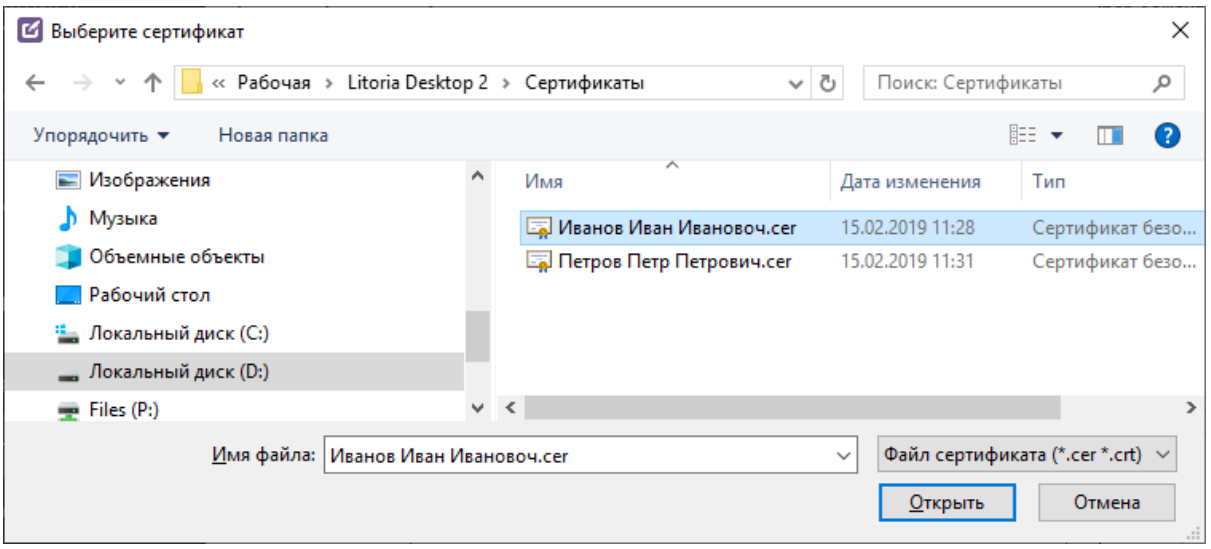
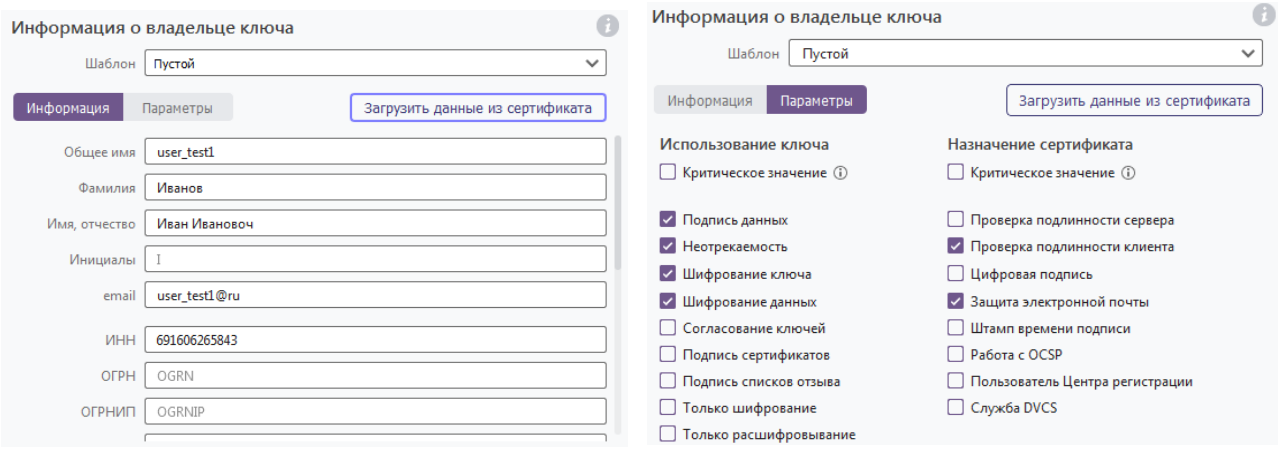


Рисунок 3.8 – Выбор сертификата

3 Информация, содержащаяся в выбранном сертификате, отобразится ниже, во вкладках «*Информация*» и «*Параметры*» (рисунок 3.9 а, б).



а) б)

Рисунок 3.9 – Отображение данных из выбранного сертификата

3.2.1.4 Подписание запроса на сертификат

С помощью ПК «Litoria Desktop 2» можно отправить запрос на новый сертификат при наличии еще действующего сертификата. В этом случае запрос на сертификат необходимо подписать действующим сертификатом.

Для подписания запроса на сертификат необходимо последовательно выполнить пункты 1-7 раздела **3.2.1 «Создание нового запроса на сертификат»**. В области «*Информация о владельце ключа*» перейти на вкладку «*Подпись*» и добавить действующий сертификат в соответствующее поле (рисунок 3.10).

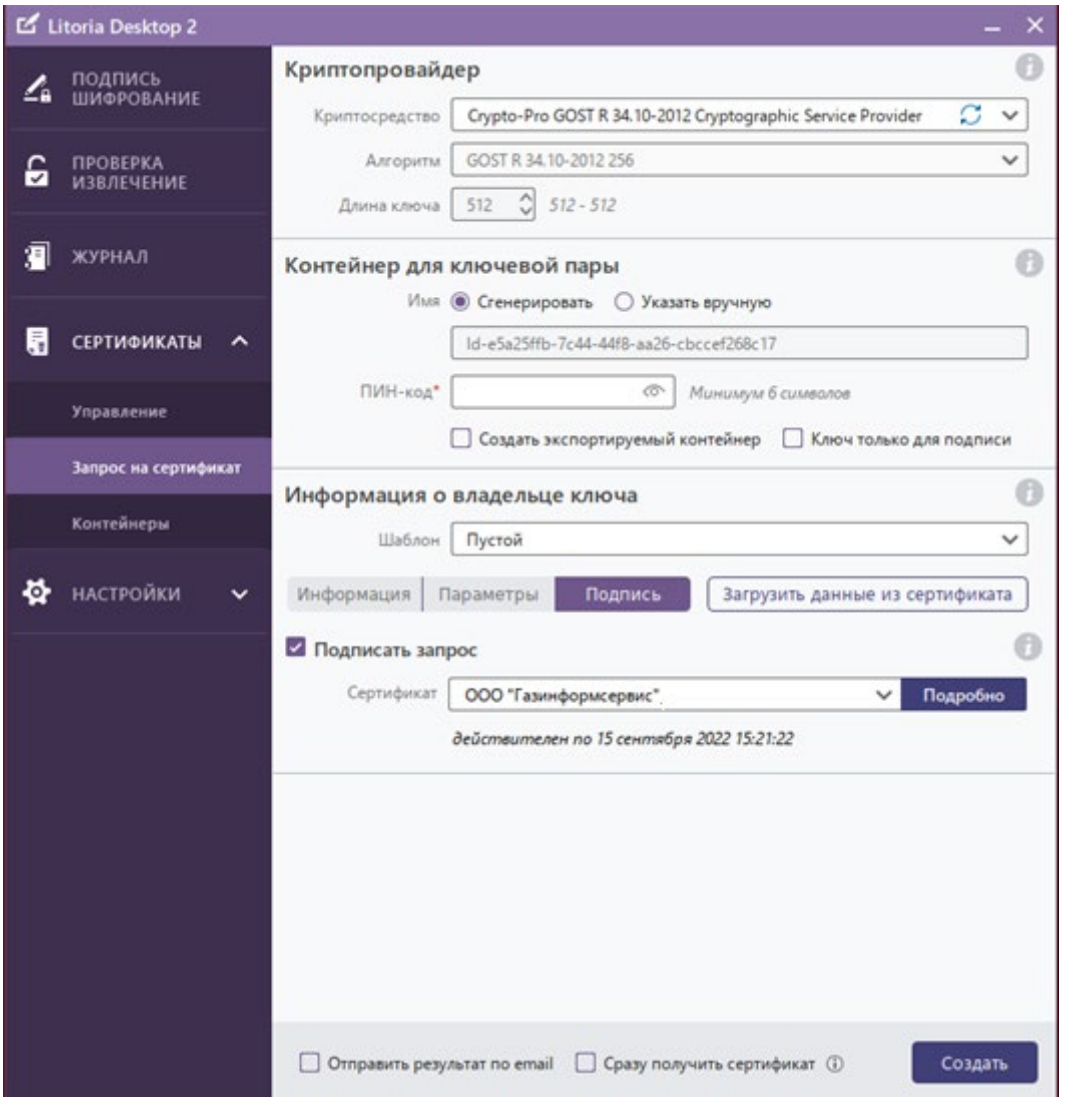


Рисунок 3.10 – Подпись запроса на сертификат

В сертификате, полученном с помощью подписанного запроса, в расширении «Тип идентификации заявителя» будет отображена информация о том, что выдача сертификата ключа проверки ЭП проводилась без личного присутствуя получателя с использованием квалифицированной ЭП при наличии действующего квалифицированного сертификата.

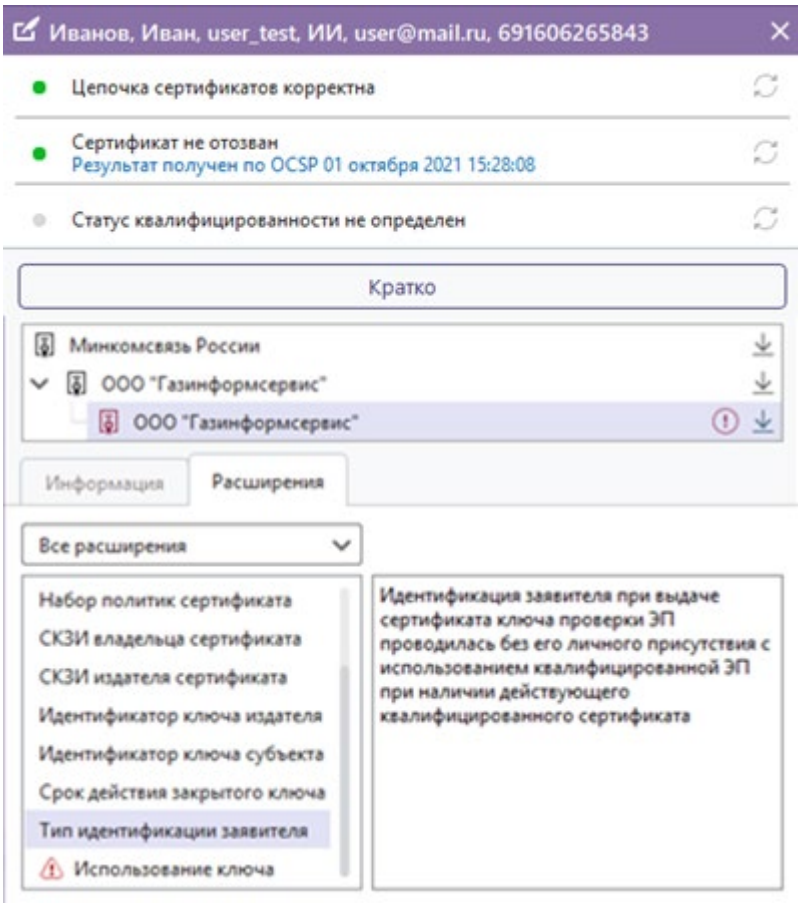


Рисунок 3.11 – Расширение сертификата «Тип идентификации заявителя»

3.2.2 Установка сертификата из файла на устройство

1 Откройте интерфейс ПК «Litoria Desktop 2».
2 Раскройте меню «*Сертификаты*».
3 Выберите пункт «*Контейнеры*» (рисунок 3.12).

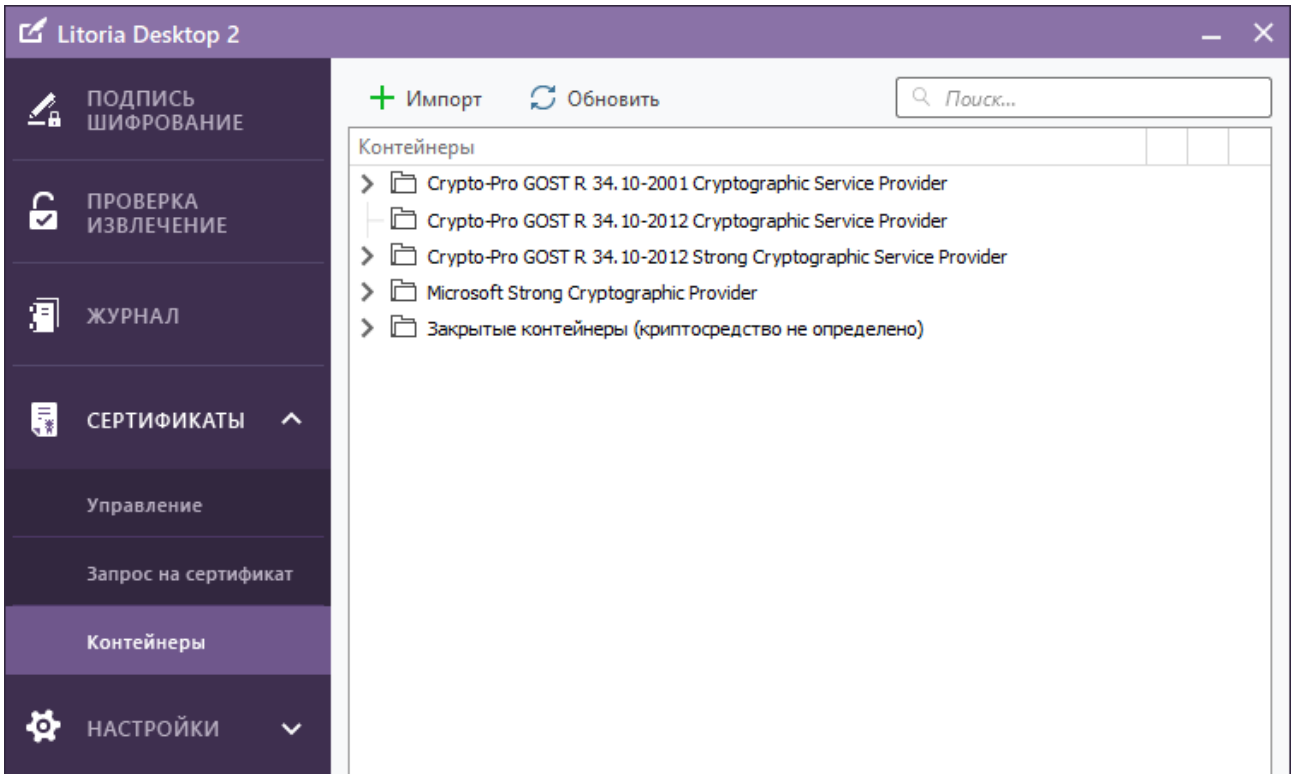


Рисунок 3.12 – Установка сертификата на устройство

4 При использовании физического отчуждаемого носителя вставьте его в нужный разъем и нажмите кнопку «*Обновить*» на вкладке «*Контейнеры*» (рисунок 3.12).

5 Для указания файла сертификата, полученного из УЦ, нажмите на кнопку «*Импорт*» (рисунок 3.13).

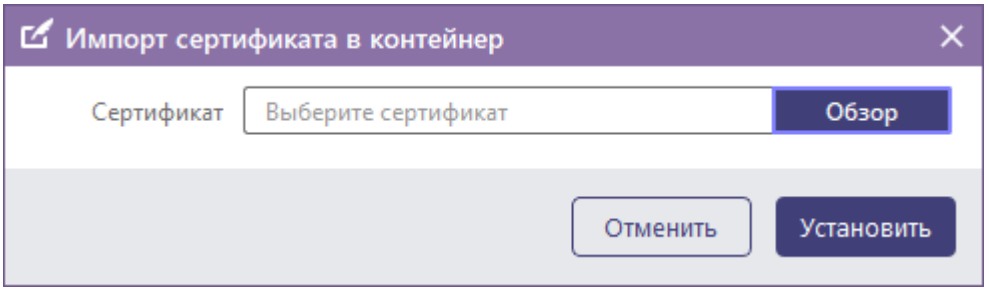


Рисунок 3.13 – Импорт сертификата

6 В появившемся окне нажмите кнопку «*Обзор*» и укажите файл сертификата (рисунок 3.14).

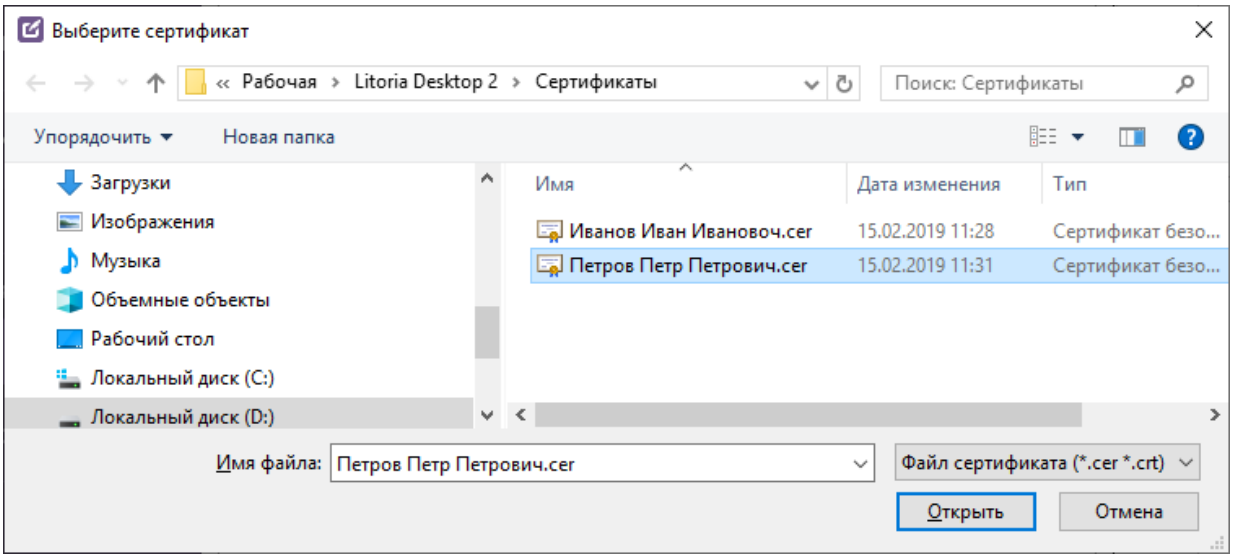


Рисунок 3.14 – Указание файла сертификата

7 Нажмите кнопку «*Открыть*».

8 В окне «*Импорт сертификата в контейнер*» автоматически отобразится информация об используемом устройстве (рисунок 3.15).

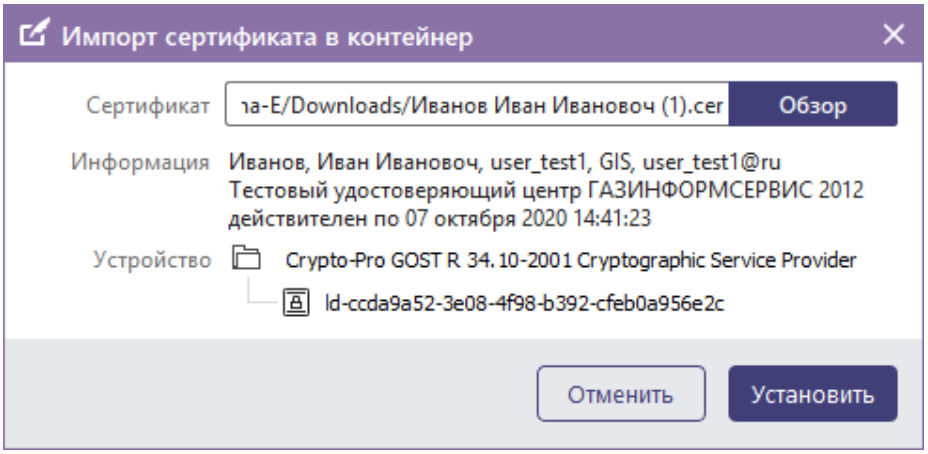


Рисунок 3.15 – Информация об импортируемом сертификате

Если для доступа к контейнеру требуется ПИН-код, введите его в соответствующем поле.

9 Нажмите на кнопку «*Установить*».

Если ранее не был сохранен ПИН-код к ключевому носителю, то контейнер будет расположен в группе «Закрытые контейнеры (криптосредство не определено)» и будет недоступен для просмотра. В строке напротив выбранного контейнера отобразиться « ». Для ввода ПИН-кода нажмите на кнопку « » в строке с нужным контейнером и в появившемся окне введите ПИН-код и нажмите на кнопку «ОК».

10 В результате выбранный сертификат установлен на устройство.

11 Для установки выбранного сертификата в хранилище *«Личные сертификаты»* нажмите на кнопку « » напротив поля с выбранным сертификатом (рисунок 3.16).

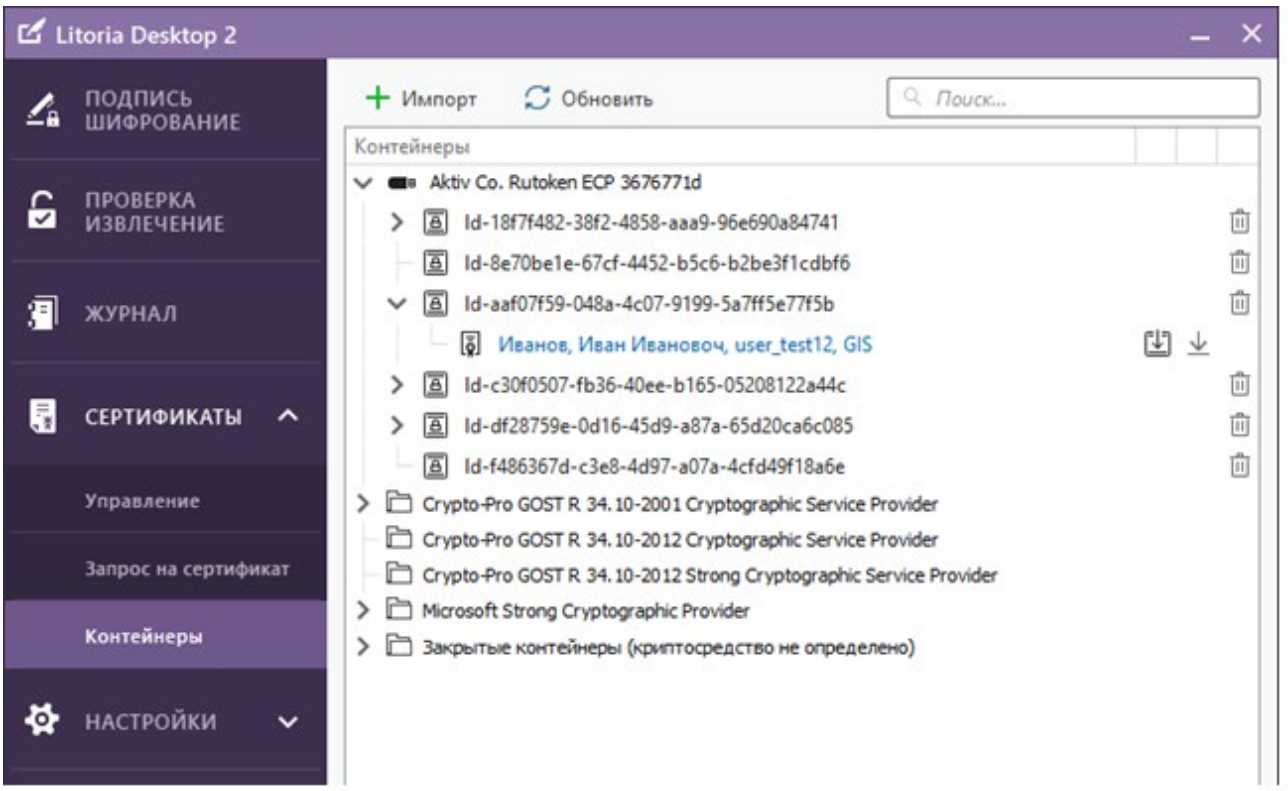


Рисунок 3.16 – Просмотр установленного сертификата в контейнере

3.2.3 Установка личного сертификата из контейнера

1 При установке сертификата из контейнера, расположенного на отчуждаемом носителе, вставьте этот носитель в нужный разъем.

2 Раскройте меню «*Сертификаты*».

3 Выберите пункт «*Контейнеры*» (рисунок 3.12).

4 Раскройте щелчком мыши нужный криптопровайдер и контейнер, в котором находится личный сертификат, необходимый к установке в хранилище (рисунок 3.17).

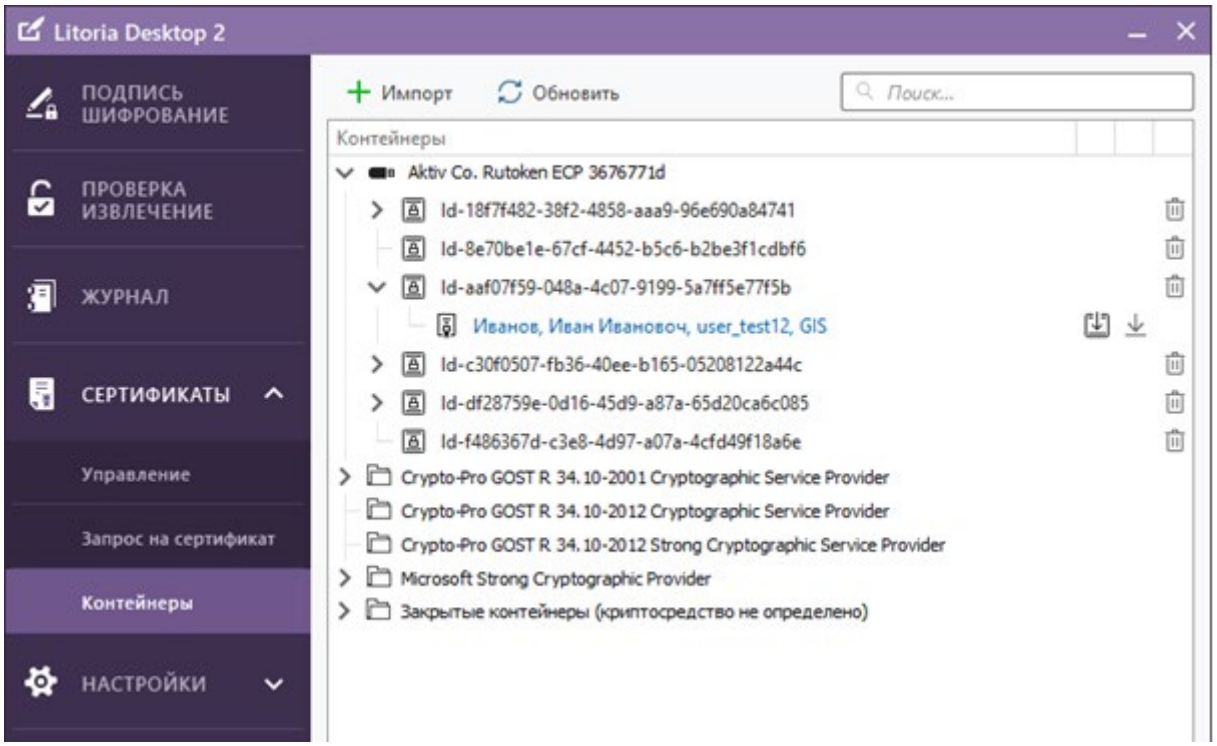


Рисунок 3.17 – Поиск необходимого к установке сертификата

Если ранее не был сохранен ПИН-код к ключевому носителю, то контейнер будет расположен в группе «Закрытые контейнеры (криптосредство не определено)» и будет недоступен для просмотра. В строке напротив выбранного контейнера отобразиться « ». Для ввода ПИН-кода нажмите на кнопку « » в строке с нужным контейнером и в появившемся окне введите ПИН-код и нажмите на кнопку «ОК».

5 Детальный просмотр сертификата, который расположен в выбранном контейнере, доступен по щелчку мыши на сертификате (рисунок 3.18).

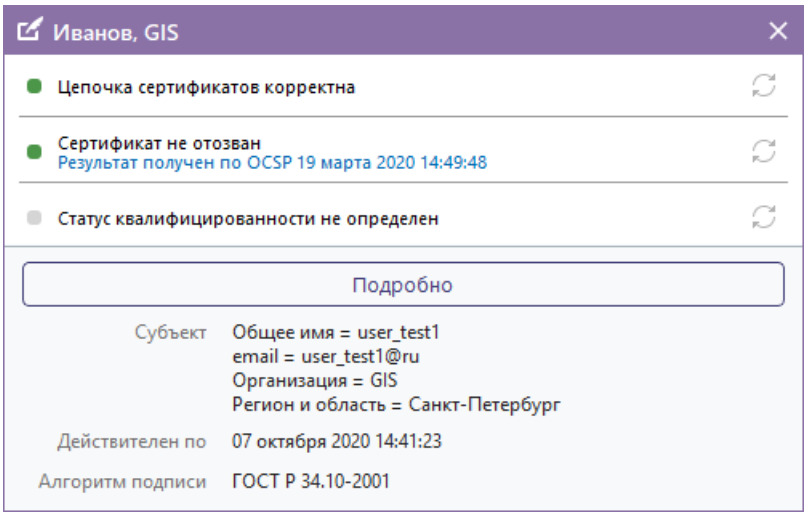


Рисунок 3.18 – Детальный просмотр сертификата

6 Для установки выбранного сертификата в хранилище *«Личные сертификаты»* нажмите на кнопку «⬇» напротив поля с выбранным сертификатом.

Отсутствия значка «⬇» напротив поля с выбранным сертификатом, означает, что выбранный сертификат уже установлен в хранилище сертификатов *«Личные сертификаты»*.

Результат: выбранный сертификат установлен в хранилище сертификатов *«Личные сертификаты»*.

3.3 Управление сертификатами

Для работы с ЭП помимо личного сертификата необходимо установить сертификаты доверенных корневых центров сертификации, промежуточных центров сертификации, при необходимости, и актуальные списки отзыва сертификатов, а также сертификаты других пользователей.

3.3.1 Управление сертификатами в хранилищах

Управление сертификатами осуществляется в меню «*Сертификаты*», пункт «*Управление*» через обращение к системным и пользовательским хранилищам сертификатов в которых они установлены (рисунок 3.19).

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

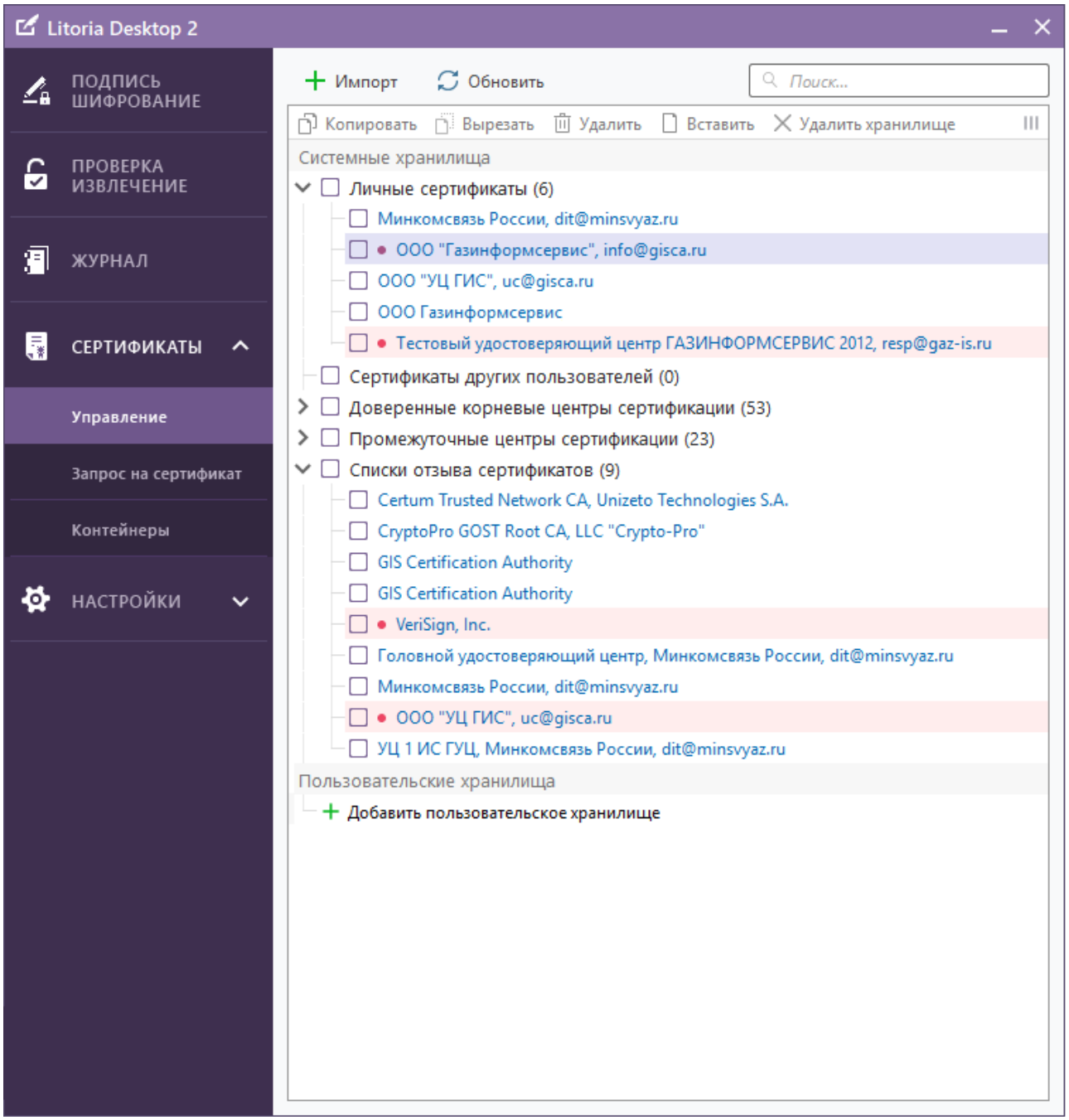


Рисунок 3.19 – Управление сертификатами в хранилищах

Во вкладке предоставляется возможность управления:

– Сертификатами, находящимися в системных хранилищах:
  - Личные сертификаты;
  - Сертификаты других пользователей;
  - Доверенные корневые центры сертификации;
  - Промежуточные центры сертификации.
– Списками отзыва сертификатов.
– Сертификатами, находящимися в пользовательских хранилищах.

Пользовательские хранилища предназначены для упрощения работы с сертификатами и объединения сертификатов в некоторые группы, для выполнения действий над всеми сертификатами в группе. Пользовательские хранилища можно добавлять Добавить пользовательское хранилище и удалять Удалить хранилище.

Системные хранилища нельзя добавить или удалить.

По кнопке Обновить доступной в контекстном меню выбранного хранилища или в основном меню вкладки, происходит перестроение цепочек сертификации выбранного хранилища/всех хранилищ соответственно.

Для сертификатов в системных и пользовательских хранилищах возможны следующие операции:

- просмотр и проверка сертификатов (см п.3.3.5);
- экспорт сертификатов (см. п. 3.3.4);
- копирование/перемещение сертификатов из одного хранилища в другое;
- удаление сертификатов из хранилища.

Над элементами системного хранилища «Списки отзыва сертификатов» недоступны операции копирования и перемещения.

Для выполнения операций копирования/перемещения/удаления сертификатов из/в хранилища выполните следующие действия:

1 Раскройте хранилище сертификатов.
2 Отметьте сертификаты, над которыми нужно произвести операции копирования/перемещения/удаления.
3 Выполните операцию копирования/перемещения/удаления (рисунок 3.20) с помощью основного меню вкладки, расположенного в верхней части окна. Операции копирования/перемещения также можно выполнить перетаскиванием нужного сертификата из одного хранилища в другое.

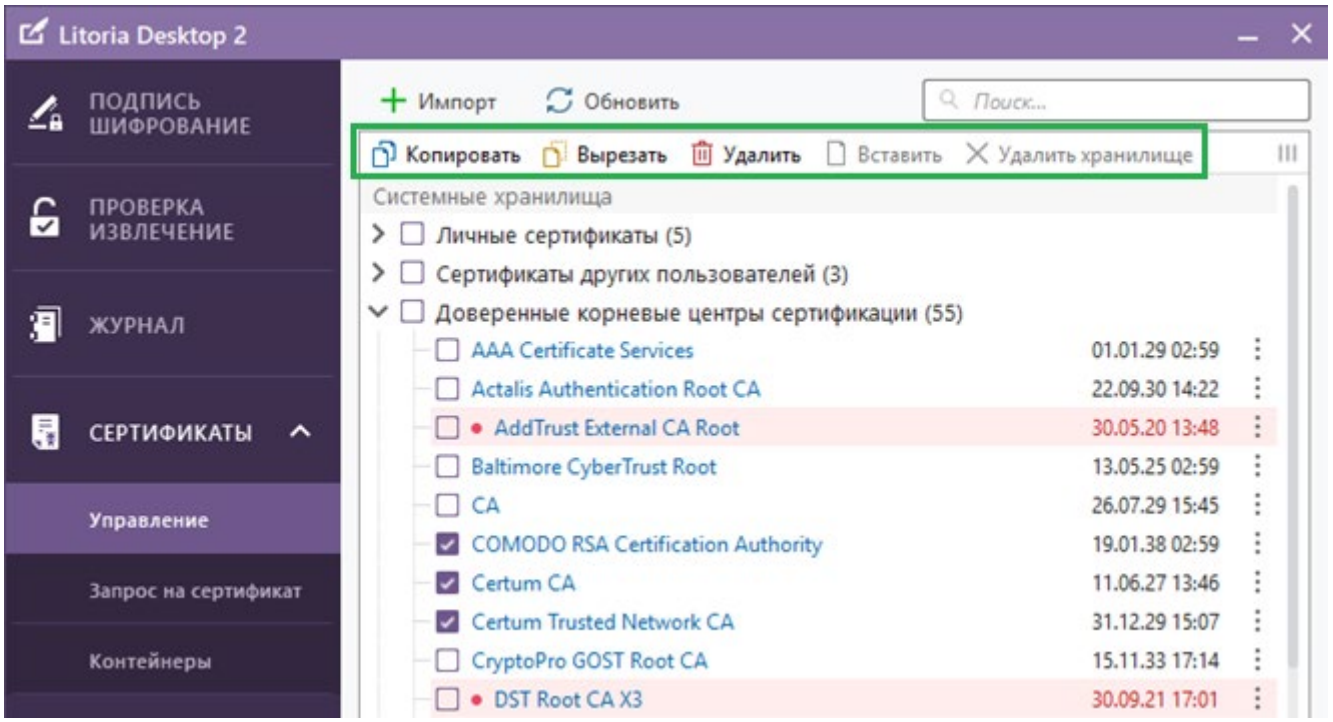


Рисунок 3.20 – Операции над сертификатами в хранилищах

Операции копирования/перемещения/удаления контекстного меню (рисунок 3.21) доступны только для одного выделенного элемента.

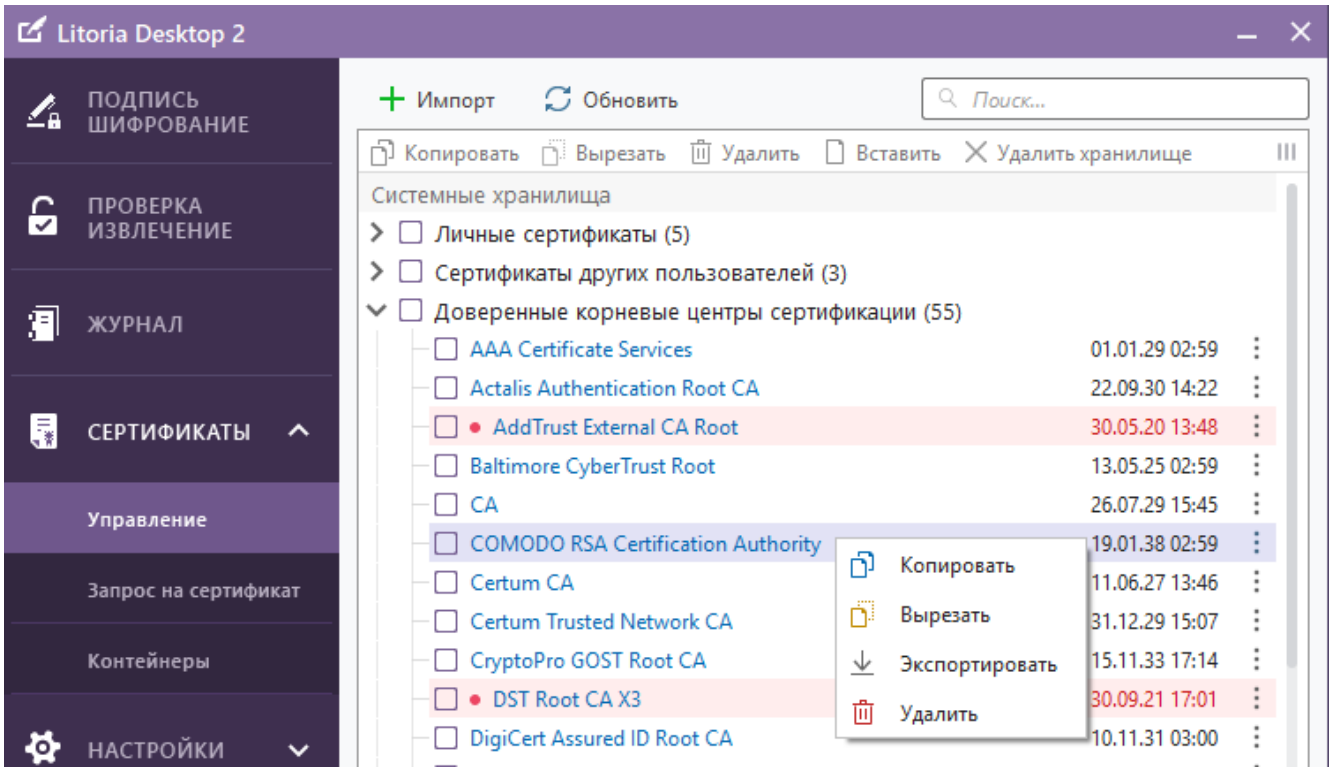


Рисунок 3.21 – Операции контекстного меню

3.3.2 Фильтрация сертификатов

Для фильтрации сертификатов во вкладке управления сертификатами в хранилищах необходимо нажать на кнопку « ||| » основного меню вкладки, расположенного в верхней части окна (рисунок 3.22).

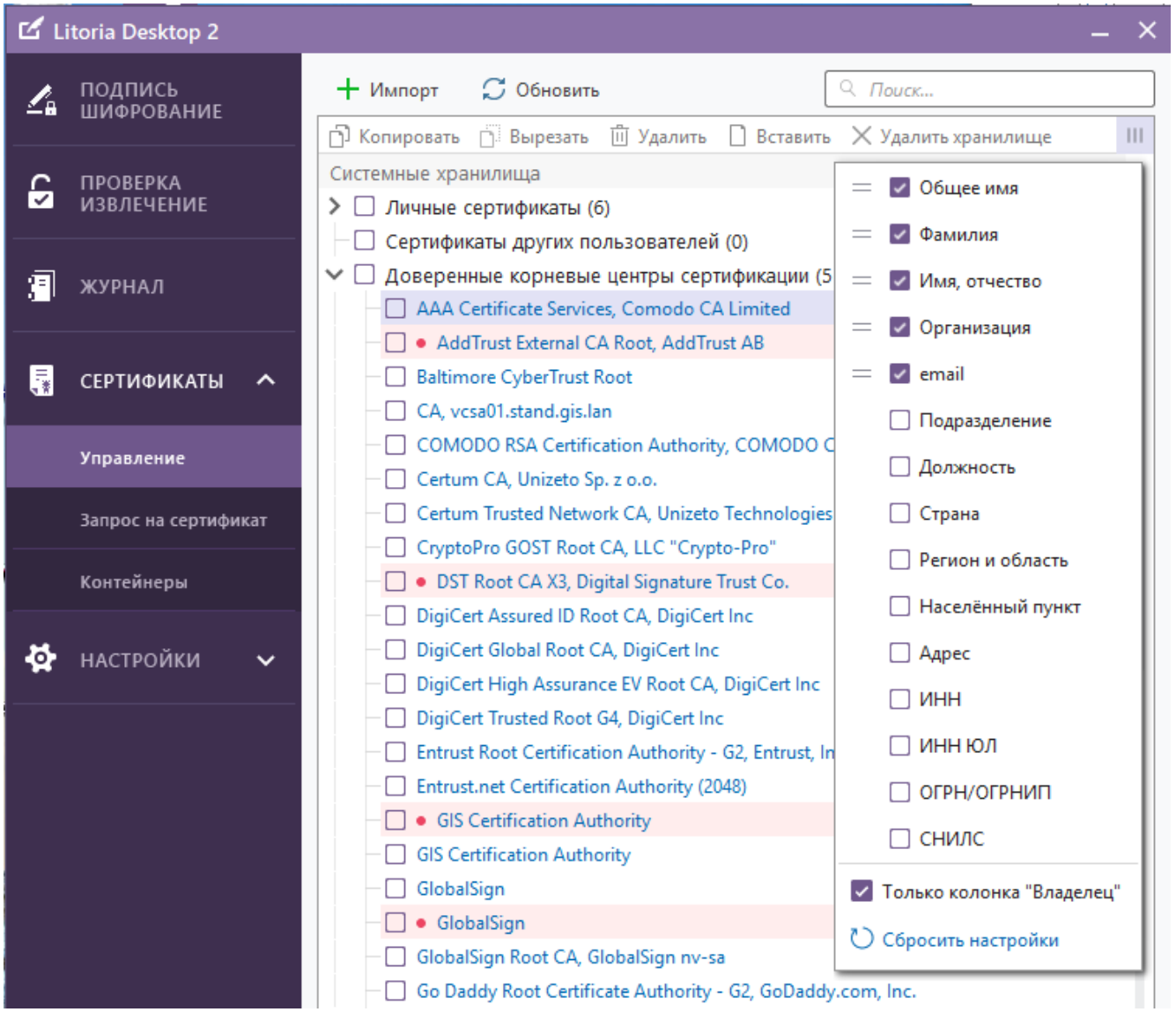


Рисунок 3.22 – Фильтрация сертификатов

Фильтрация позволяет изменить отображение сертификата в списке по информации о субъекте, содержащейся в сертификате (*Общее имя, ФИО, Организация, Подразделение* и т.д). При этом возможно изменить порядок следования информации в строке путем перетаскивания полей (рисунок 3.23).

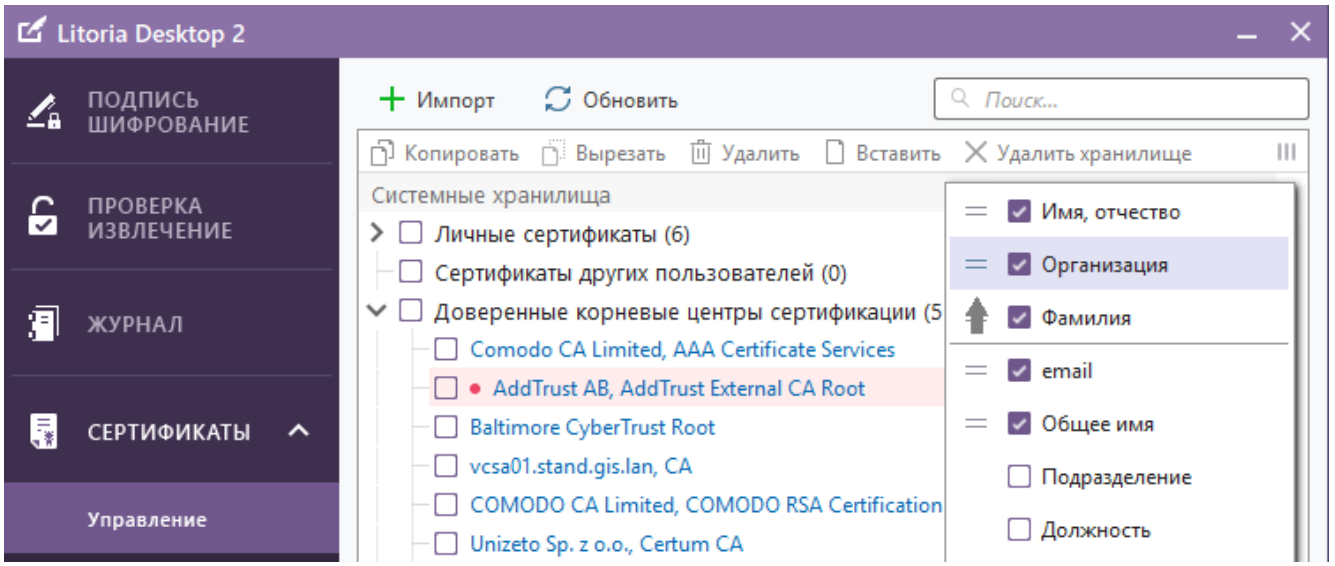


Рисунок 3.23 – Изменение порядка следования полей сертификатов

Установка флага *«Только колонка «Владелец»»* позволяет отображать в списке только информацию о сертификате. Остальные колонки, которые выводятся во вкладке «Управление», содержащие дату действительности сертификата и операции над сертификатами (рисунок 3.21), отображены не будут.

Выбранные во вкладке параметры фильтрации будут также применены в окне импорта сертификатов в хранилище (рисунок 3.26).

3.3.3 Импорт сертификатов

С помощью функции *Импорт* можно установить сертификаты или списки отзыва (с расширениями *.cer, *.crl, *.crt, *.p7b) в соответствующие хранилища 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;

Корневой сертификат необходимо заранее запросить в удостоверяющем центре, который выдал сертификат пользователя

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 (см. пункт 3.3.3.1).

Для выполнения функции *Импорт* необходимо выполнить следующие действия:

1 Импортировать сертификат в хранилище сертификатов можно несколькими способами:

– выбором в контекстном меню файла сертификата *«Litoria Desktop 2»* → *«Установить в хранилище»* (рисунок 3.24);

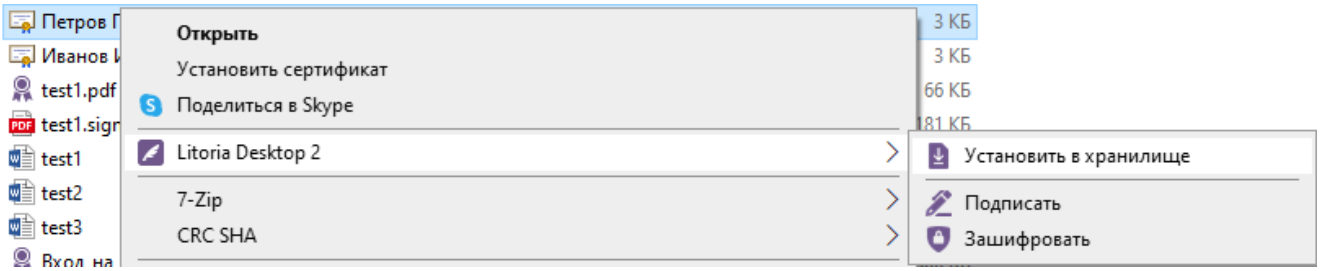


Рисунок 3.24 – Импорт сертификата через контекстное меню

– с помощью интерфейса ПК «Litoria Desktop 2»: меню «*Сертификаты*» → пункт «*Управление*» → кнопка «*Импорт*» (рисунок 3.25);

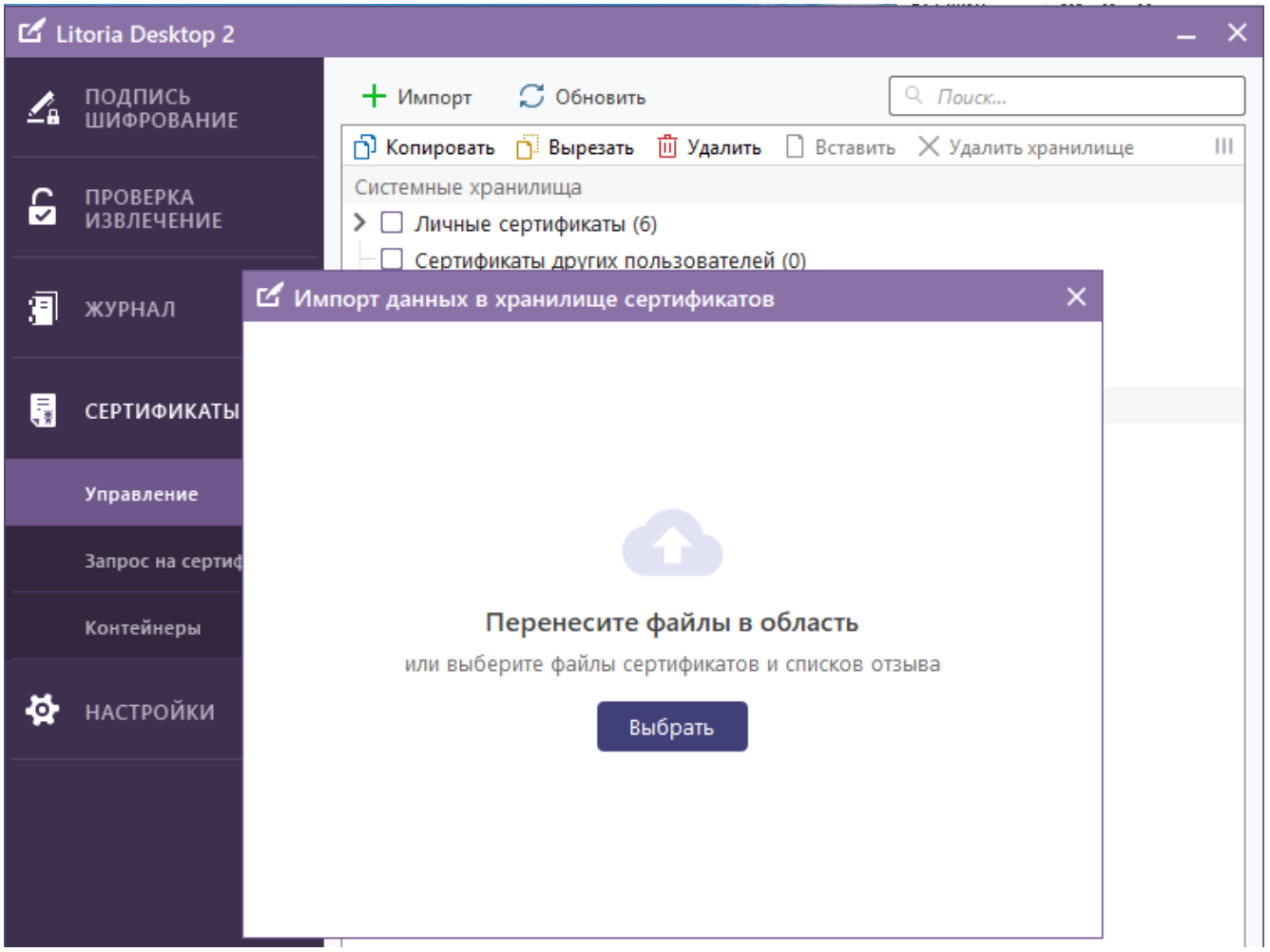


Рисунок 3.25 – Управление сертификатами

– перетаскиванием файла сертификата из окна Проводника в область списка

сертификатов пункта «*Управление*».

2 В открывшемся окне «*Импорт данных в хранилище сертификатов*» (рисунок 3.26) отобразятся системные и пользовательские хранилища, и добавленные в них сертификаты.

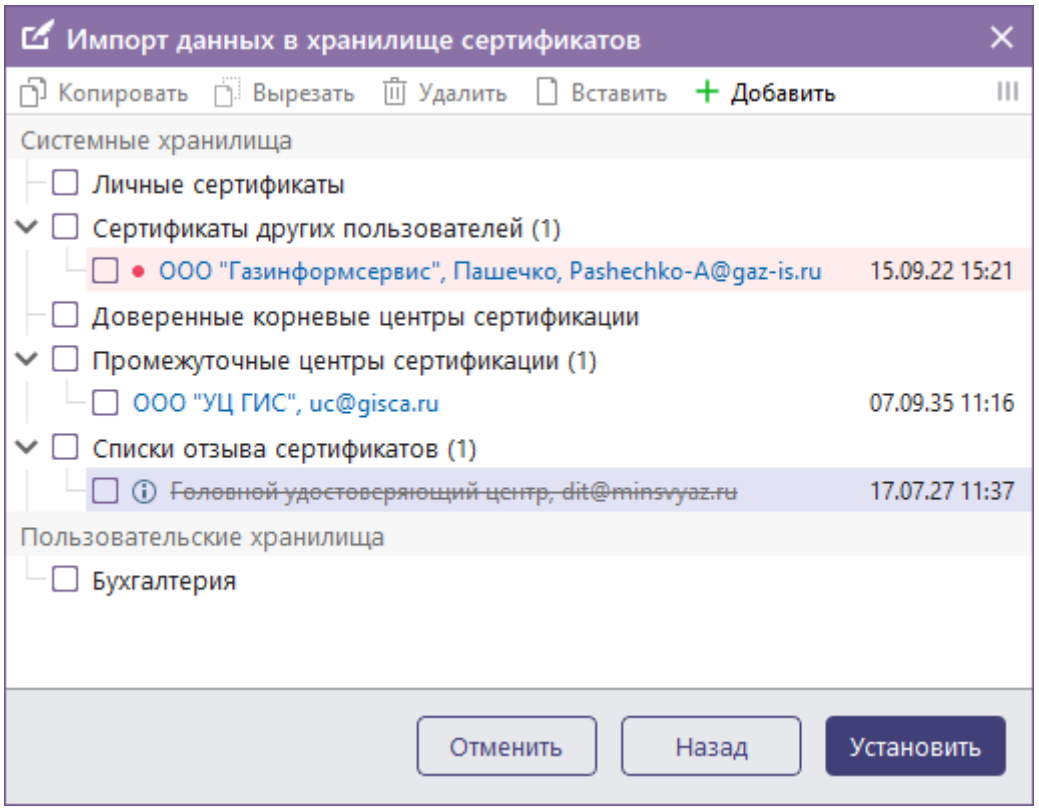


Рисунок 3.26 – Импорт данных в хранилище

3 В окне *«Импорт данных в хранилище сертификатов»* доступны все операции над сертификатами, описанные в п. 3.3.1 и 3.3.2 (копирование/перемещение/ удаление/фильтрация). Также в окне *«Импорт данных в хранилище сертификатов»* по кнопке + Добавить можно добавлять файлы сертификатов (кроме сертификатов из pfx-контейнеров) и списков отзыва.

Если добавляемый сертификат уже был импортирован в выбранное хранилище ранее, установка сертификата не будет осуществлена. В окне импорта сертификат будет перечеркнут (рисунок 3.27).

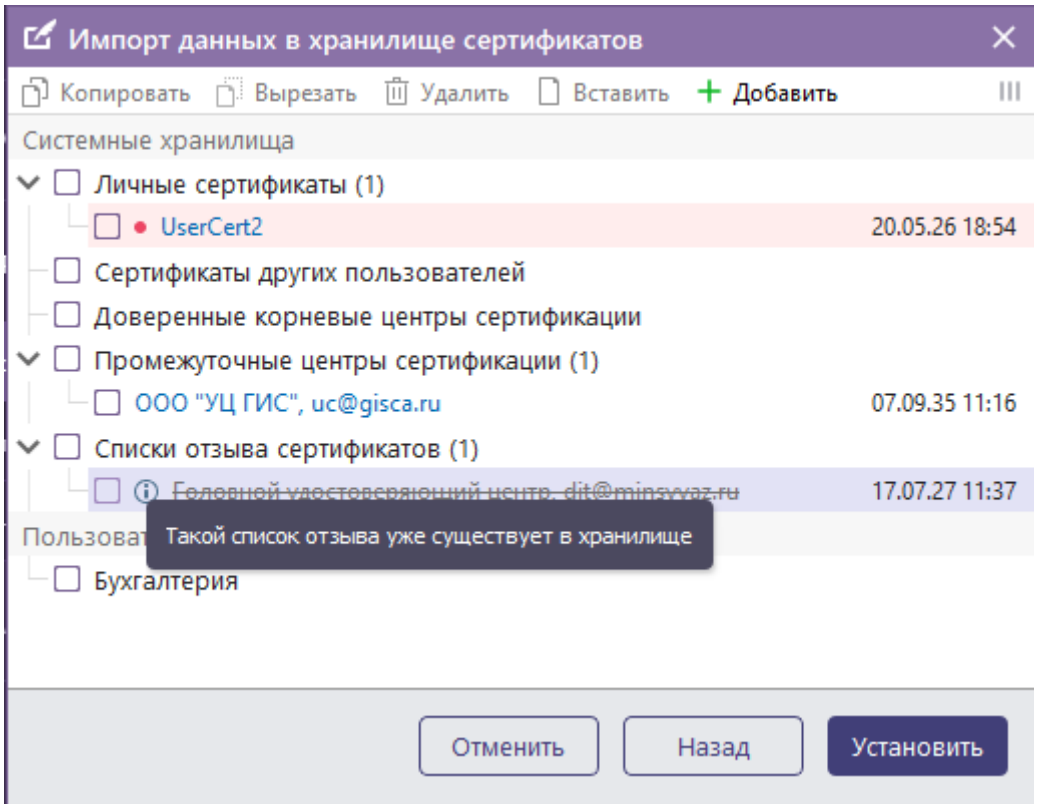


Рисунок 3.27 – Ошибка при импорте элемента, существующего в хранилище

4 Нажмите на кнопку «*Установить*».

5 При импорте корневого сертификата появится окно с запросом подтверждения установки данного корневого сертификата (рисунок 3.28).

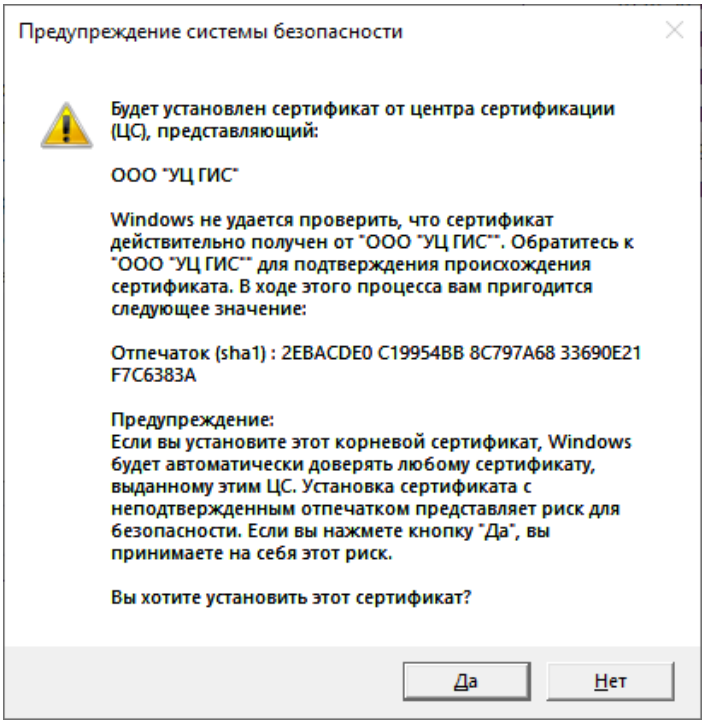


Рисунок 3.28 – Предупреждение системы безопасности

6 Нажмите кнопку «*Да*».

Результат: добавленные сертификаты импортированы в выбранные хранилища сертификатов.

3.3.3.1 Импорт сертификата из pfx-контейнера

1 Способы импорта сертификата из файла pfx-контейнера в хранилище сертификатов аналогичны описанным в п. 3.3.3:

> Необходимо учитывать, что при добавлении в окно импорта файла pfx-контейнера, добавление сертификатов с расширениями *.cer, *.crl, *.crt, *.p7b будет недоступно. Импорт сертификатов осуществляется отдельно от импорта файлов обмена ключевой информации.

– выбором в контекстном меню файла pfx-контейнера *«Litoria Desktop 2»* → *«Установить в хранилище»* (рисунок 3.24).
– с помощью интерфейса ПК «Litoria Desktop 2»: меню «*Сертификаты*» → пункт «*Управление*» → кнопка «*Импорт*» (рисунок 3.25);
– перетаскиванием файла pfx-контейнера из окна Проводника в область списка сертификатов пункта «*Управление*».

2 В появившемся окне «*Установка файла обмена личной информации*» (рисунок 3.29) введите ПИН-код к контейнеру и нажмите на кнопку «*Установить*» для продолжения импорта.

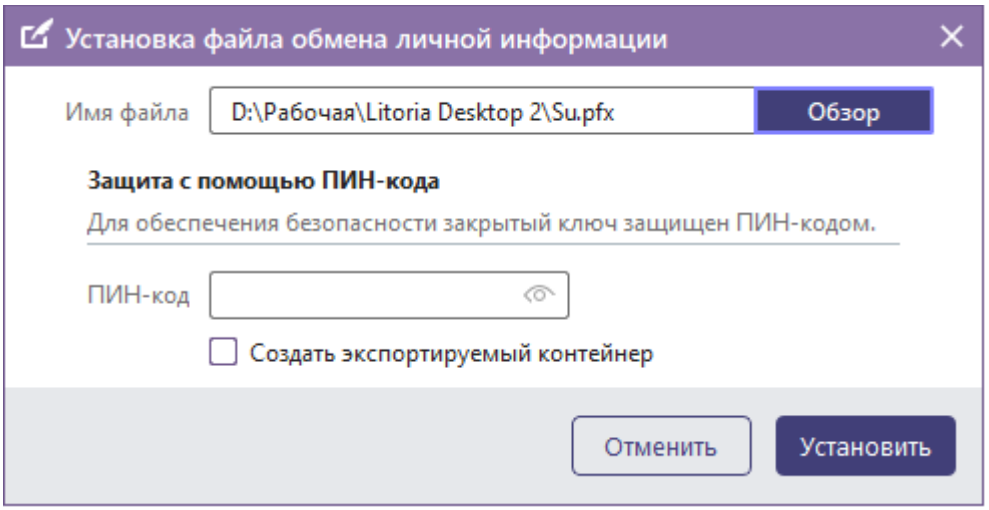


Рисунок 3.29 – Установка файла обмена личной информации

Результат: выбранный сертификат из файла обмена личной информации импортирован в хранилище сертификатов «*Личные сертификаты*».

3.3.4 Экспорт сертификата

Для выполнения операции экспорта сертификатов выполните следующие действия:

1 Раскройте хранилище сертификатов в котором находится сертификат для экспорта.

2 Выполните операцию экспорта с помощью контекстного меню выбранного сертификата (рисунок 3.21).

3 В появившемся окне *«Выберите файл для экспорта сертификата»* (рисунок 3.30) укажите месторасположение и имя экспортируемого сертификата и нажмите на кнопку «*Сохранить*»

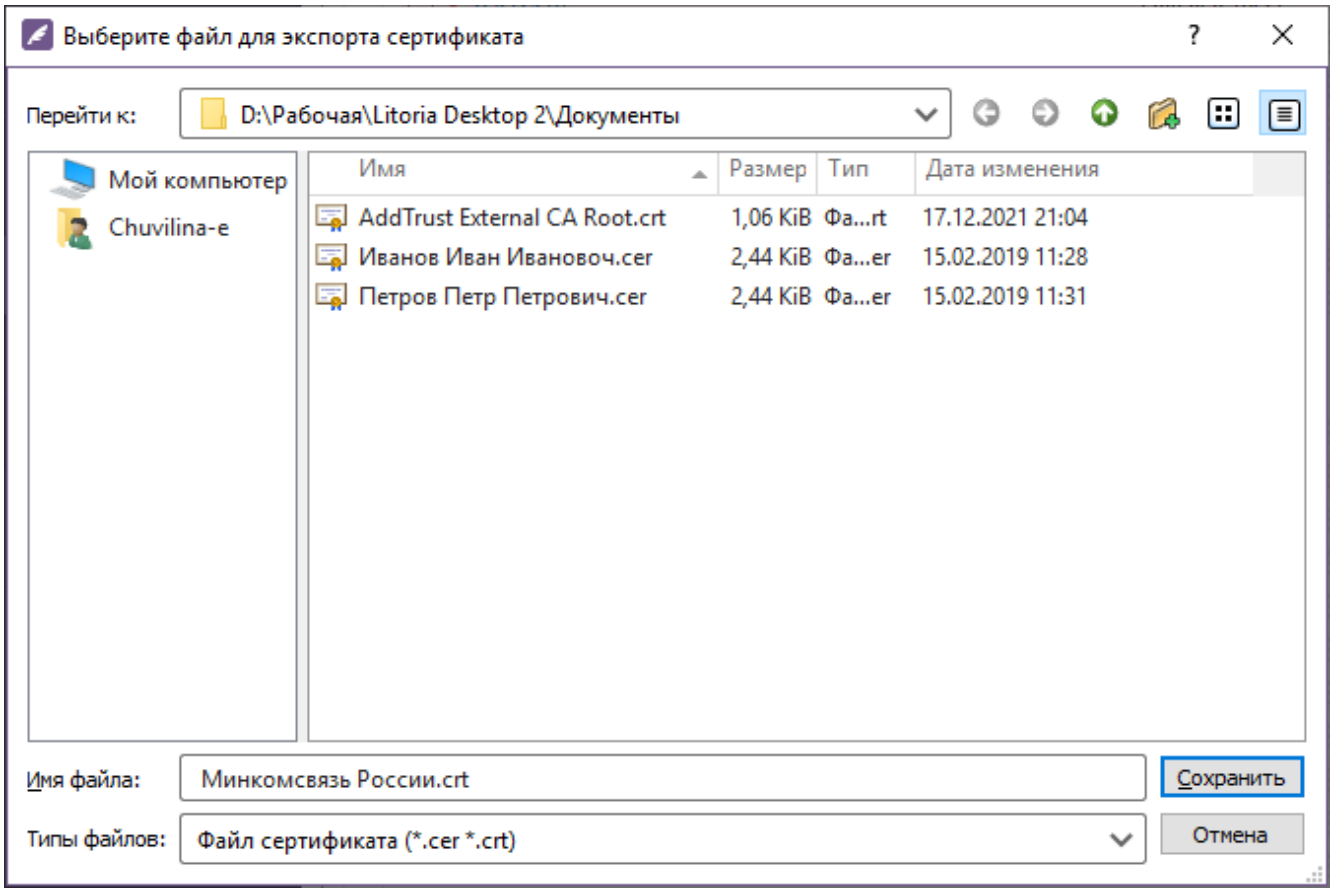


Рисунок 3.30 – Экспорт сертификата

Результат: выбранный сертификат сохранен в файл по указанному месторасположению.

3.3.5 Просмотр и проверка сертификата

Для просмотра сведений сертификата выполните следующие действия:

1 Раскройте хранилище сертификатов в котором находится интересующий вас сертификат.

2 В списке сертификатов выберите тот, который хотите просмотреть и по щелчку мыши раскройте его содержимое.

3 Появится окно (рисунок 3.31), в котором отображается информация о выбранном сертификате.

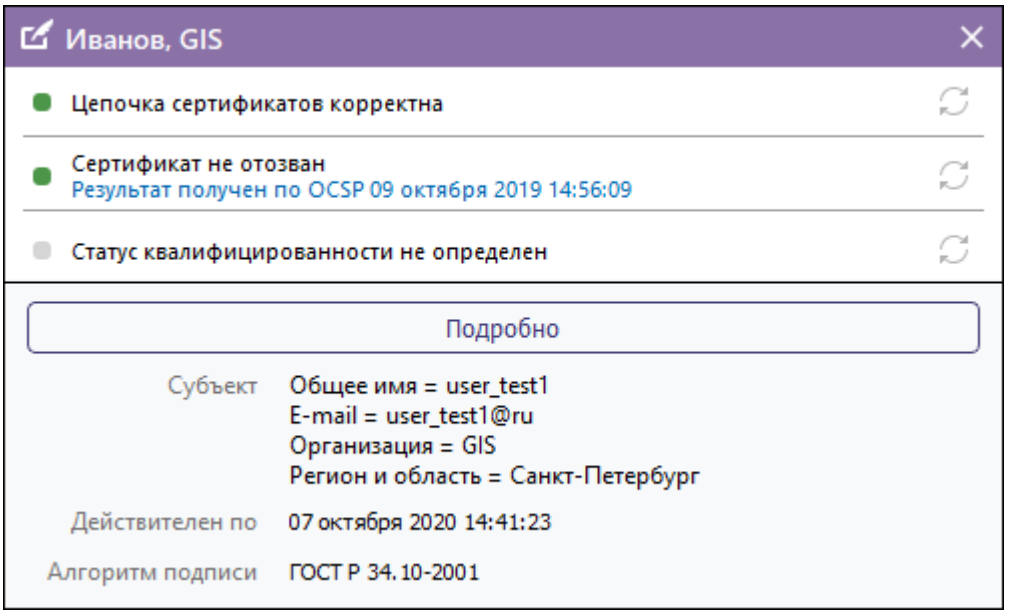


Рисунок 3.31 – Детальная информация о сертификате

3.3.5.1 Просмотр сертификата

В открывшемся окне отображается информация о субъекте, сроке действия сертификата и его алгоритме подписи (рисунок 3.31).

Более полную информацию о сертификате можно получить, раскрыв содержание сертификата по кнопке «*Подробно*».

Информация о сертификате расположена на двух вкладках:

- «*Информация*», где отображается полная информация о субъекте, издателе, сроке действия сертификата, его серийном номере, алгоритме ключа проверки ЭП и подписи сертификата (рисунок 3.32).
- «*Расширения*», где (в зависимости от вида сертификата) отображается информация об идентификаторах ключа издателя/субъекта, использовании ключа, основных ограничениях и др. (рисунок 3.33).

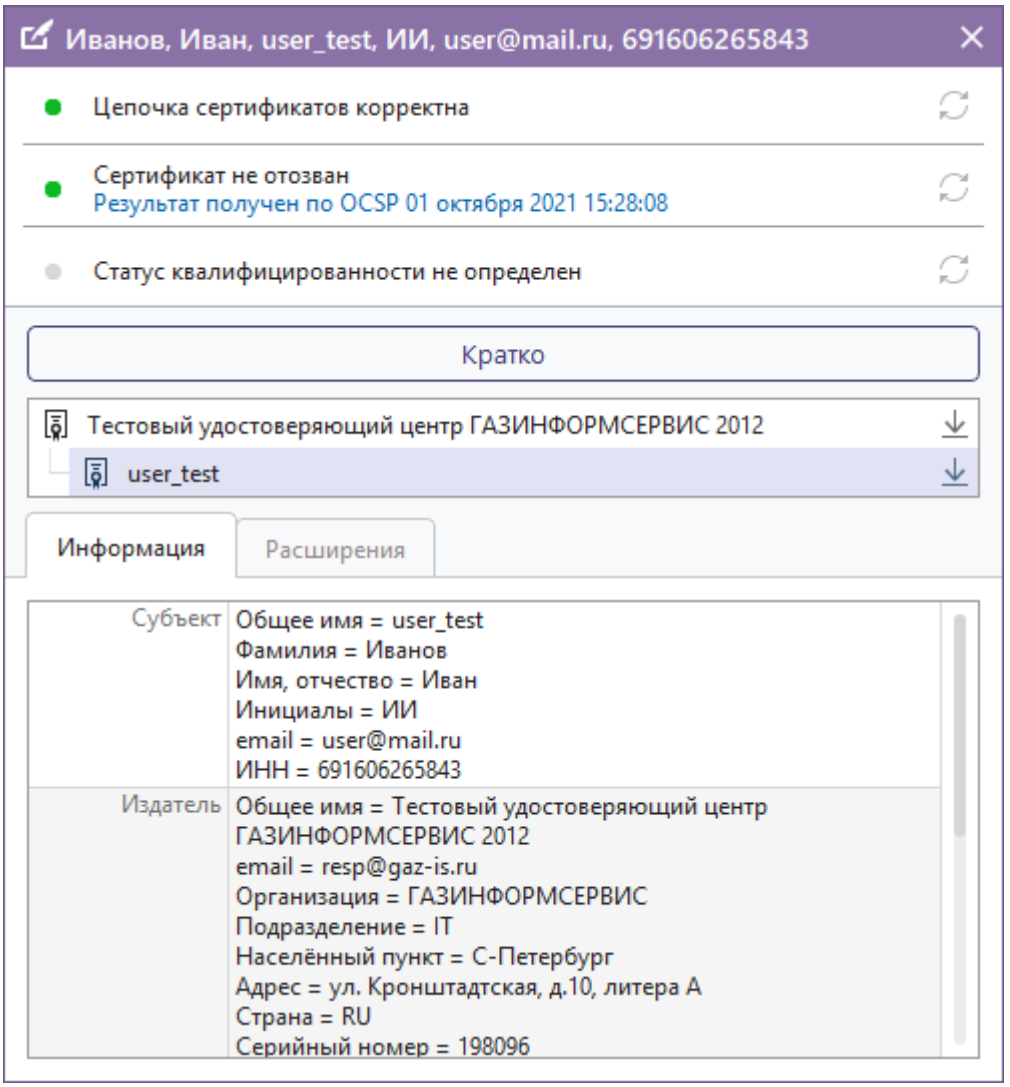


Рисунок 3.32 – Вкладка «*Информация*»

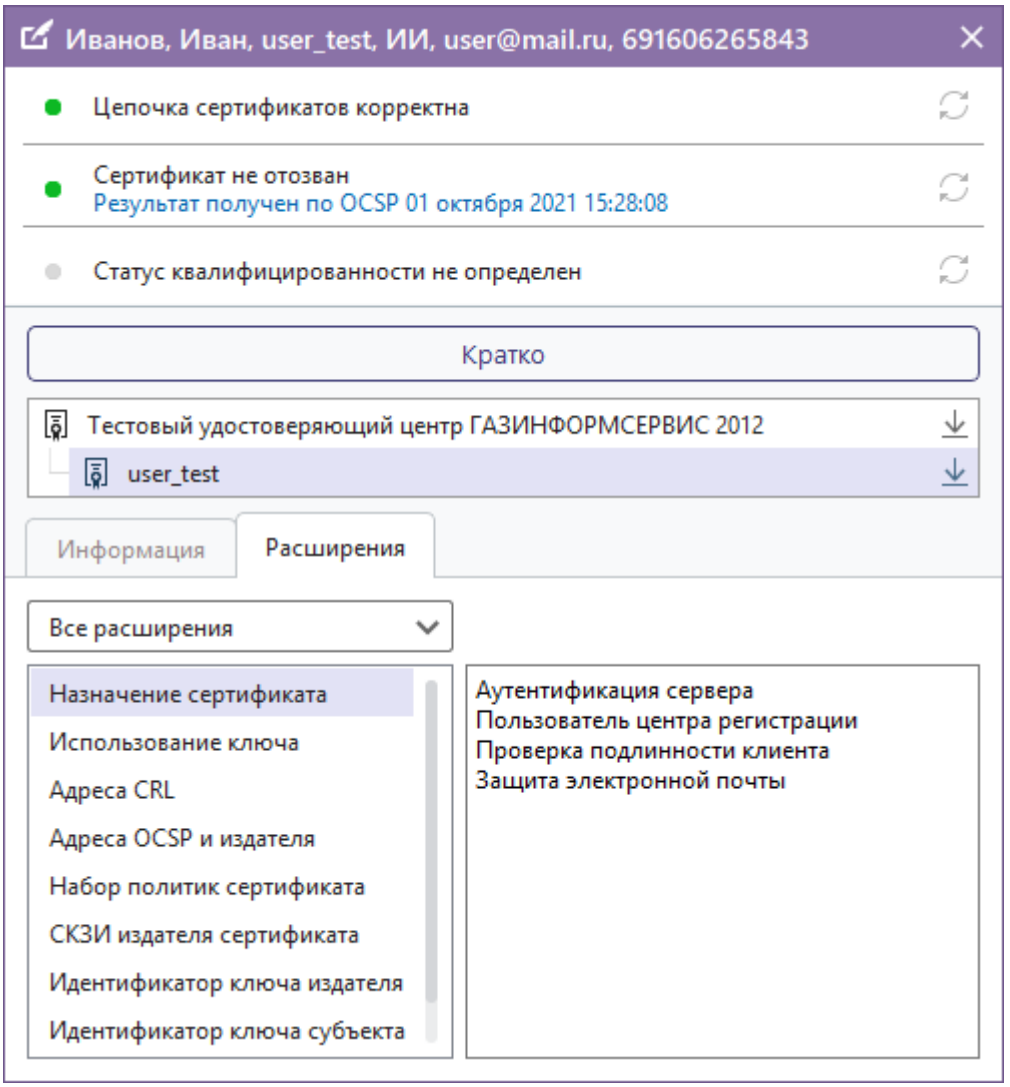


Рисунок 3.33 – Вкладка «*Расширения*»

3.3.5.2 Проверка статуса сертификата

ПК «Litoria Desktop 2» позволяет провести следующие проверки статуса сертификата:

– по спискам отзыва сертификатов (CRL);
– по протоколу OCSP (в реальном времени).

При проверке по CRL сертификат проверяется на наличие его в локальном CRL, который был ранее установлен на компьютер. Если локальный CRL не актуален, то выполняется проверка по удаленному CRL, который скачивается и устанавливается на компьютер во время проверки, при этом обновляя ранее установленный CRL.

В локальном списке отзыва сертификатов может содержаться указание наличия разностных списков отзывов (delta CRL[4]) – списков отзыва, которые выпускаются между базовыми (полными) списками отзывов и содержат информацию об отмененных сертификатах за промежуток времени, прошедший с момента выпуска базового CRL или последнего разностного списка.

В этом случае сертификат также будет проверен на наличие в разностном списке.

При проверке по протоколу OCSP в режиме реального времени статус сертификата запрашивается в службе OCSP, указанной в сертификате.

При отсутствии доступа к сети (нет подключения к сети Интернет или закрыт доступ к внутренним ресурсам сети) проверку по протоколу OCSP проводить не имеет смысла. В таком случае необходимо либо получить доступ к внутренним ресурсам сети или сети Интернет, либо получить на физическом носителе новый CRL и установить его на компьютер.

Проверка статуса сертификата по протоколу OCSP происходит в автоматическом режиме. Если необходима внеочередная проверка сертификата по протоколу OCSP или статус сертификата не определен, нажмите на кнопку «».

Результаты проверки можно посмотреть по ссылке в области информации о проверке сертификата (рисунок 3.31).

Пример результата проверки сертификата по OCSP и по протоколу CRL приведены на рисунке 3.34.

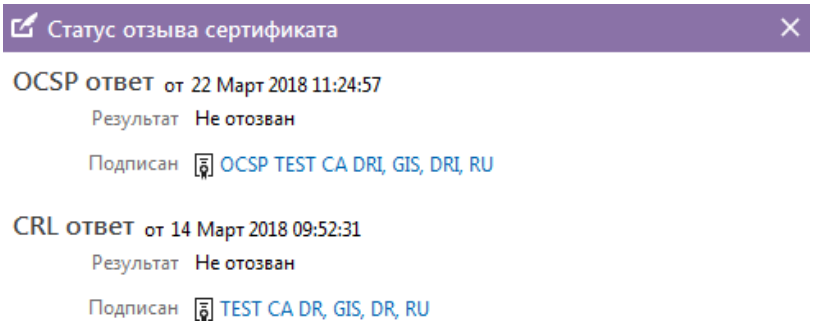


Рисунок 3.34 – Результат проверки по OCSP и CRL

[4]Описание delta CRL и базовых CRL приведено в RFC5280 «Certificate and Certificate Revocation List (CRL) Profile».

Если администратором установлен режим квалифицированной подписи (см. п.3.4.3 «Расширенные настройки»), все сертификаты проходят проверку по актуальному списку аккредитованных УЦ.

При возникновении ошибок в строке статуса квалифицированности отобразится пиктограмма по нажатию на которую можно увидеть перечень ошибок квалифицированности сертификата (рисунок 3.35).

В перечне отображается только три последние ошибки, чтобы увидеть полный перечень ошибок, необходимо скопировать перечень по ссылке «скопировать все в буфер обмена» и вставить информацию в текстовый файл.

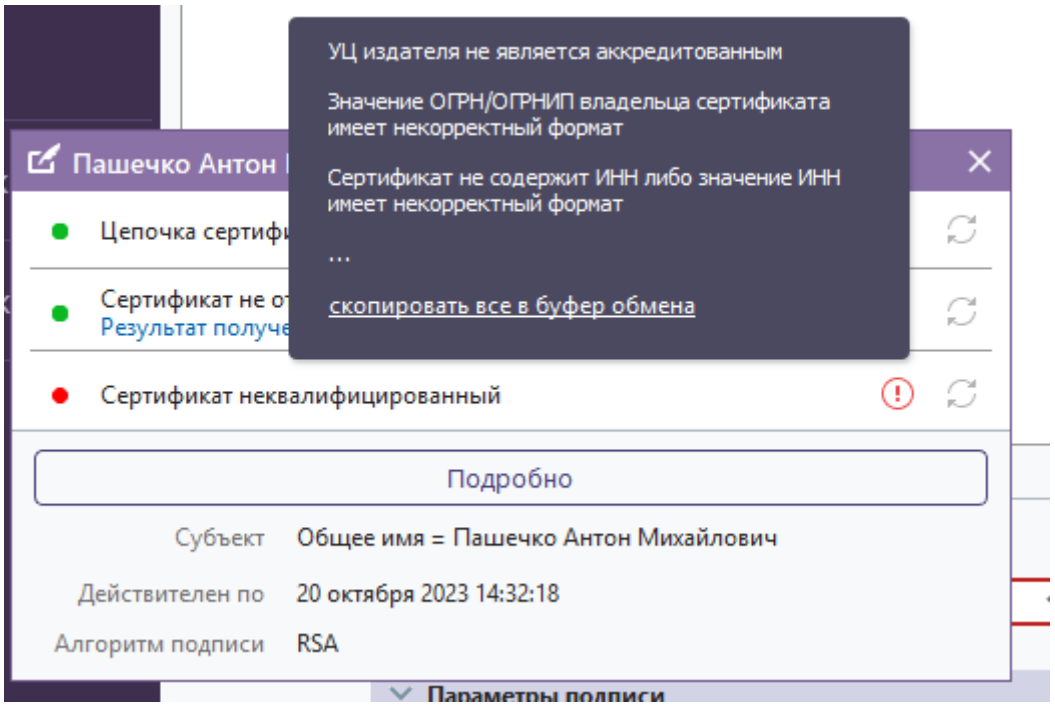


Рисунок 3.35 – Ошибки при проверке сертификата на квалифицированность

3.4 Настройка комплекса

Настройка комплекса осуществляется пользователем в меню «*Настройки*» (рисунок 3.36), состоящее из пунктов: основные, сетевые и расширенные настройки комплекса.

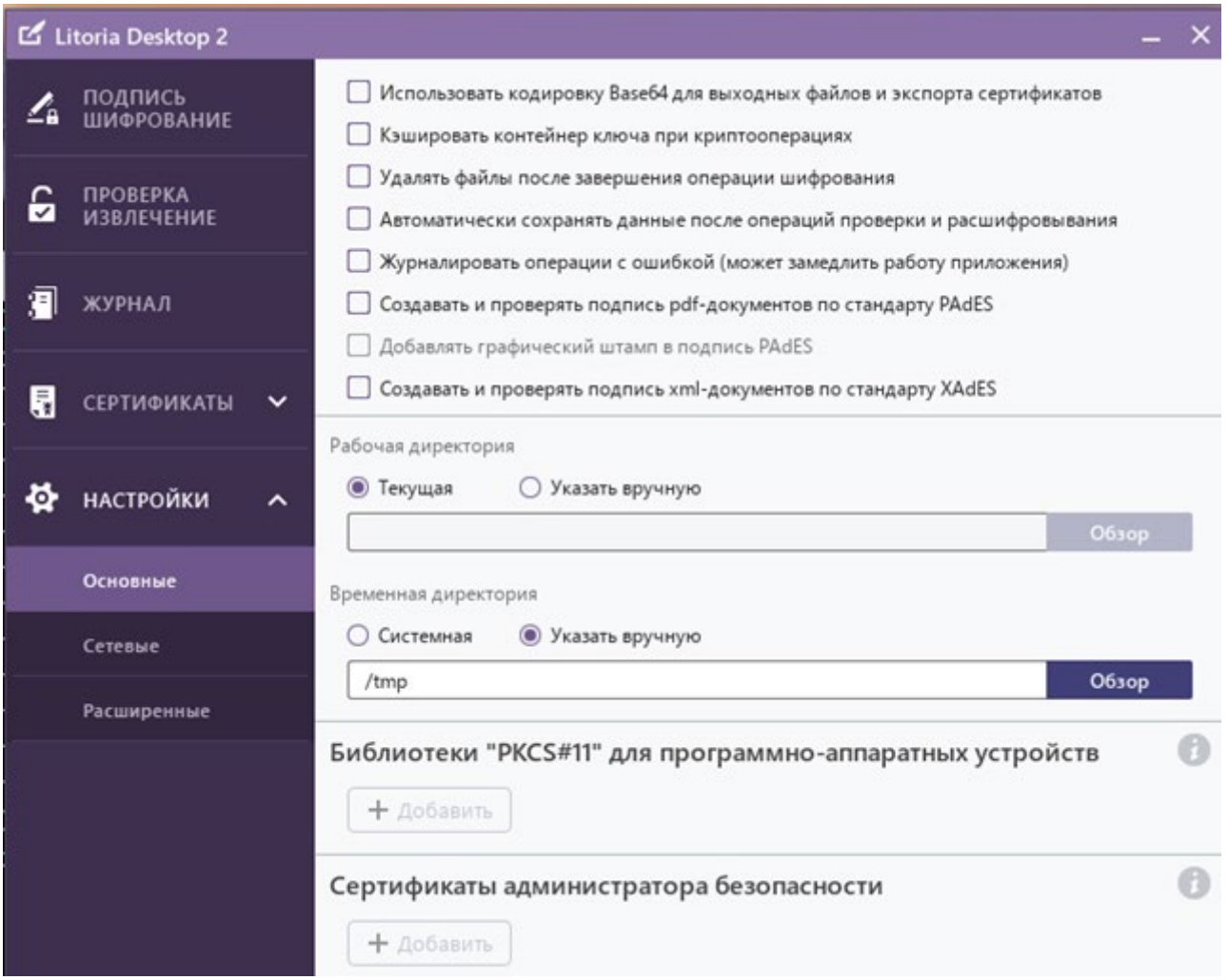


Рисунок 3.36 – Пункт меню «*Настройки*»

Пользователю доступны следующие настройки:

– Во вкладке «*Основные*»:
  - настройка кодировки для выходных файлов и экспорта сертификатов;
  - настройка кэширования контейнера ключа при криптооперациях;
  - настройка удаления файлов после шифрования;
  - настройка автоматического сохранения данных после операций проверки и расшифровывания;
  - настройка журналирования операций, завершившихся ошибкой;
  - настройка подписи pdf документа по стандарту PAdES;
  - настройка добавления графического штампа в подписи PAdES;

- настройка подписи xml-документов по стандарту XAdES;
- настройка рабочих и временных директорий.

– Во вкладке «*Сетевые*»:
- настройка адреса используемой службы штампов времени;
- настройка использования службы доверенной третьей стороны;
- настройка прокси-сервера.

– Во вкладке «*Расширенные*»:
- настройка языка интерфейса ПК «Litoria Desktop 2».

3.4.1 Основные настройки

3.4.1.1 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 меню «*Настройки*» пункт «*Основные*» (рисунок 3.37).

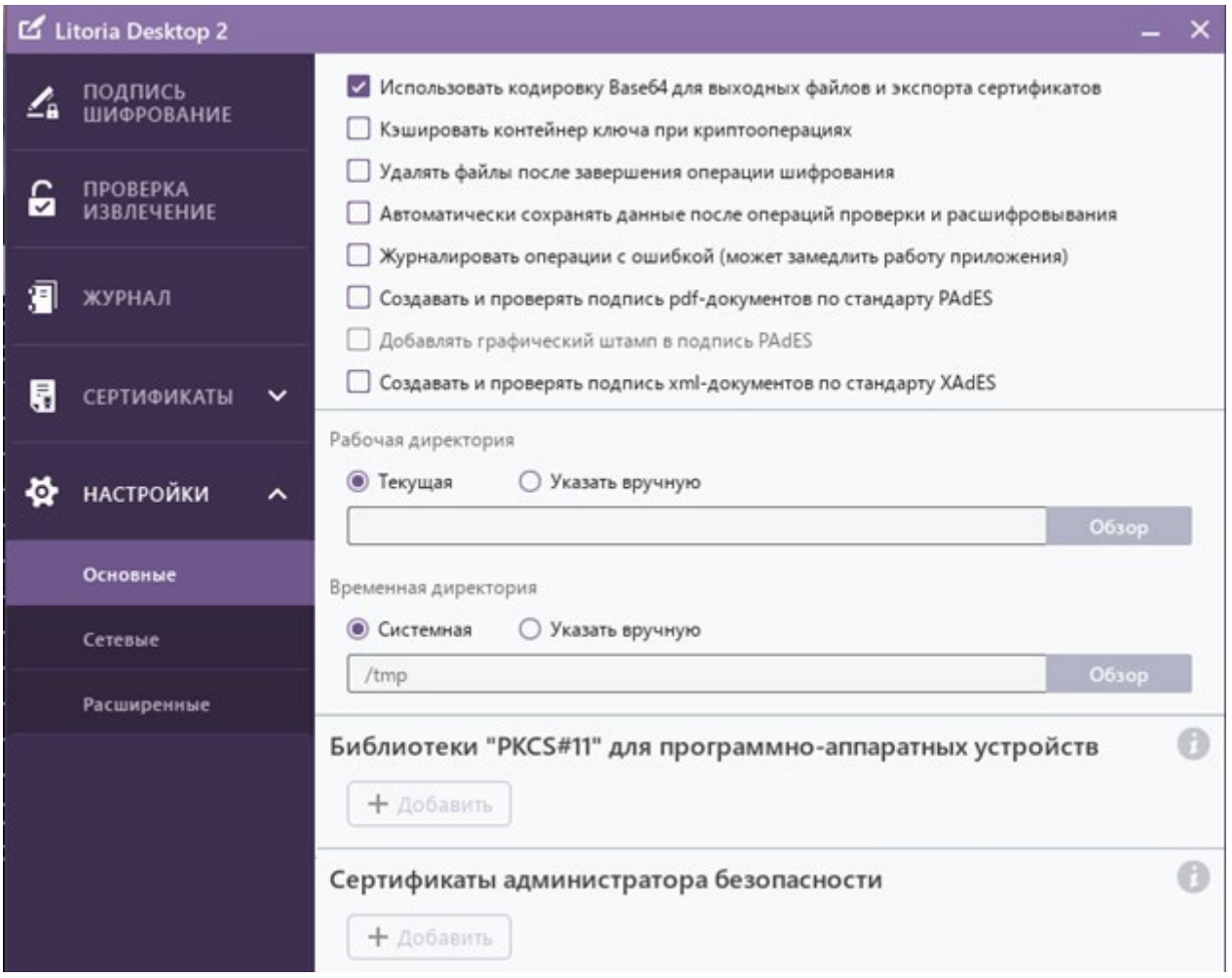


Рисунок 3.37 – Настройка кодировки выходных файлов

3.4.1.2 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.

3.4.1.3 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.

3.4.1.4 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. 3.4.1.8 *«Установка директории»*). По умолчанию в качестве рабочей директории используется текущая – та директория, в которой расположен исходный файл.

3.4.1.5 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 3.38).

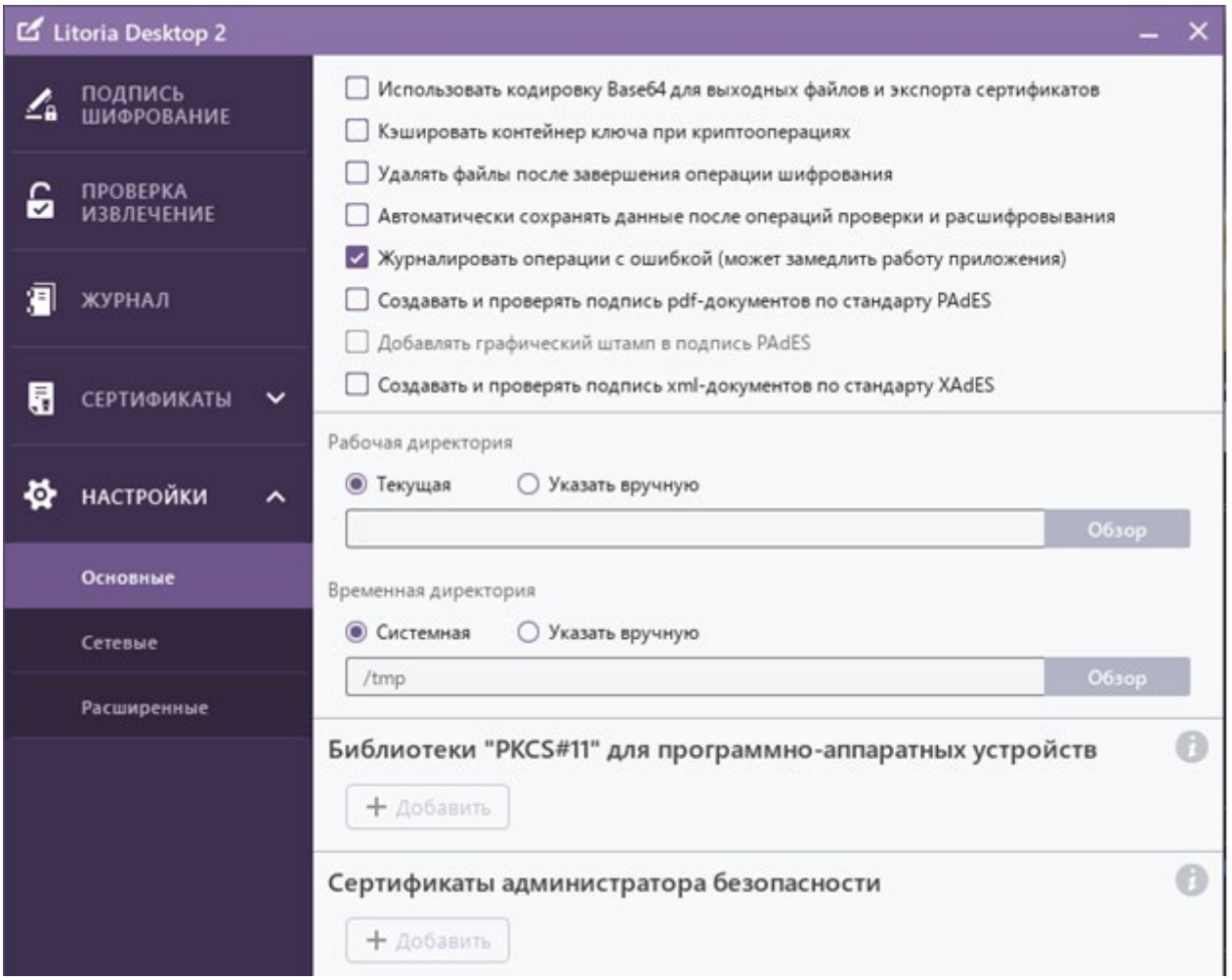


Рисунок 3.38 – Настройка журналирования операций с ошибкой

3.4.1.6 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 3.39).

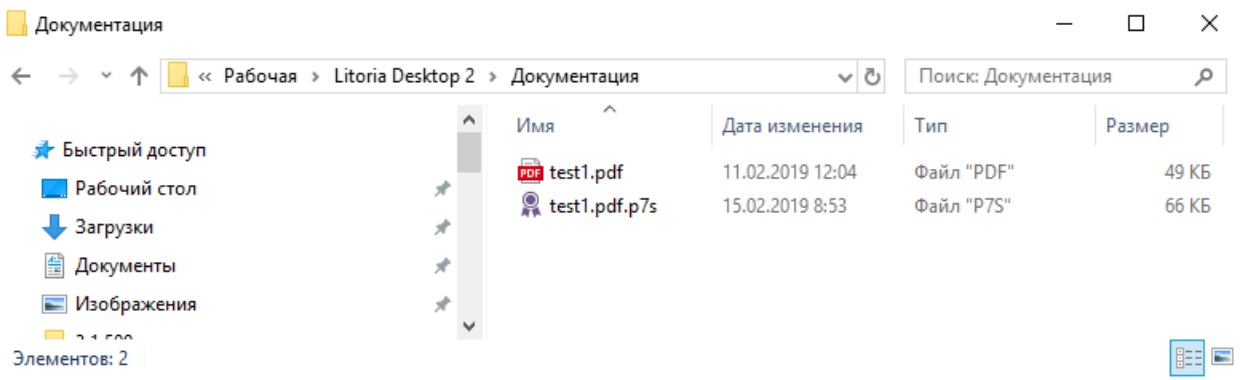


Рисунок 3.39 – Результат подписи pdf документа по стандарту CAdES

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 3.40.

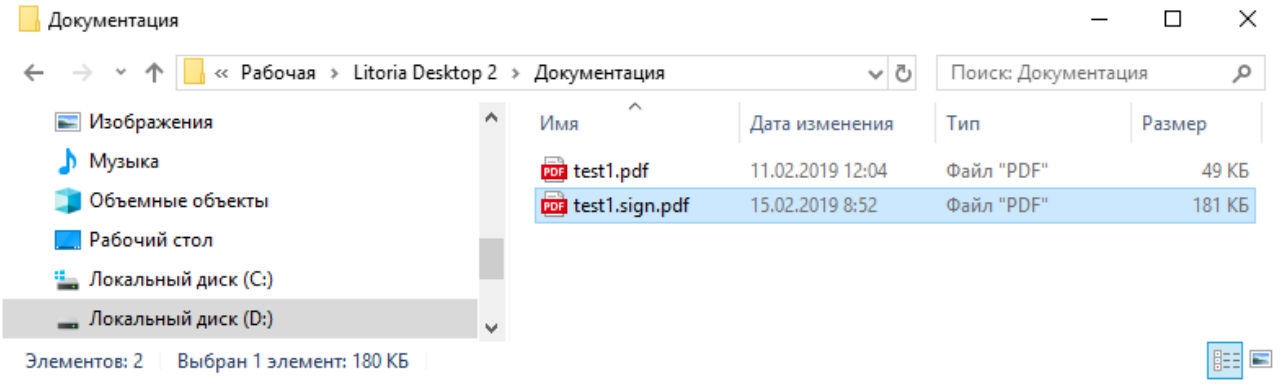


Рисунок 3.40 – Результат подписи pdf документа по стандарту PAdES

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

3.4.1.7 Добавление графического штампа в подпись PAdES

При установке создания и проверки ЭП pdf документа по стандарту PAdES (пункт 3.4.1.6 «Настройка создания и проверки подписи pdf документов по стандарту PAdES»), возможно формирование графического штампа вида, представленного на рисунке 3.41.

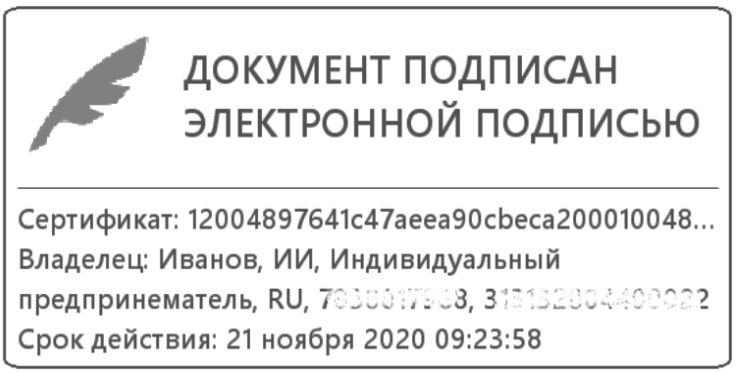


Рисунок 3.41 – Пример графического штампа pdf документа

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.

3.4.1.8 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 3.42).

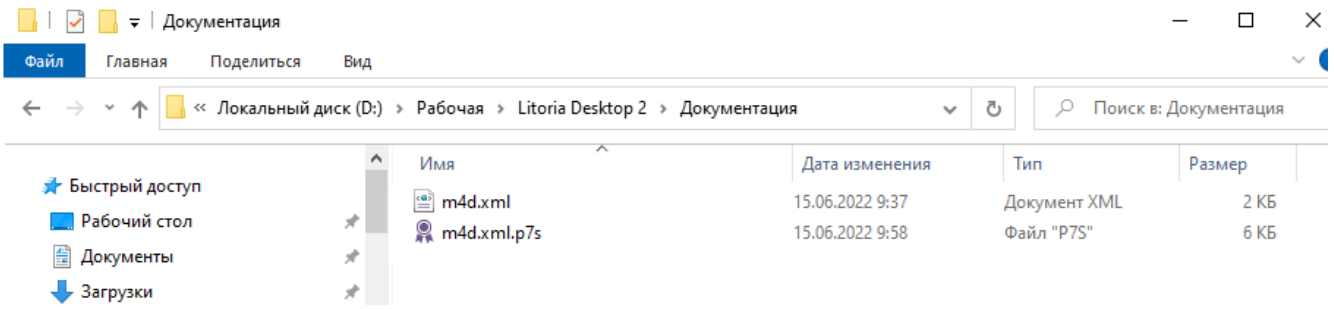


Рисунок 3.42 – Результат подписи xml-документа по стандарту CAdES

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 3.43.

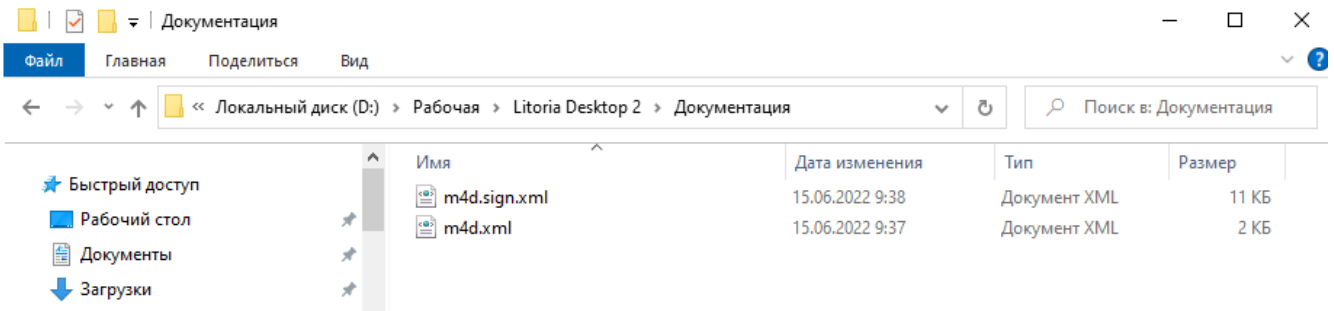


Рисунок 3.43 – Результат подписи xml-документа по стандарту XAdES

3.4.1.9 Установка директорий

Указание рабочей директории, в которую будут записываться выходные файлы всех основных операций, осуществляется в области «*Рабочая директория*» пункта «*Основные настройки*» (рисунок 3.44).

По умолчанию в качестве рабочей директории используется текущая – та директория, в которой расположен исходный файл.

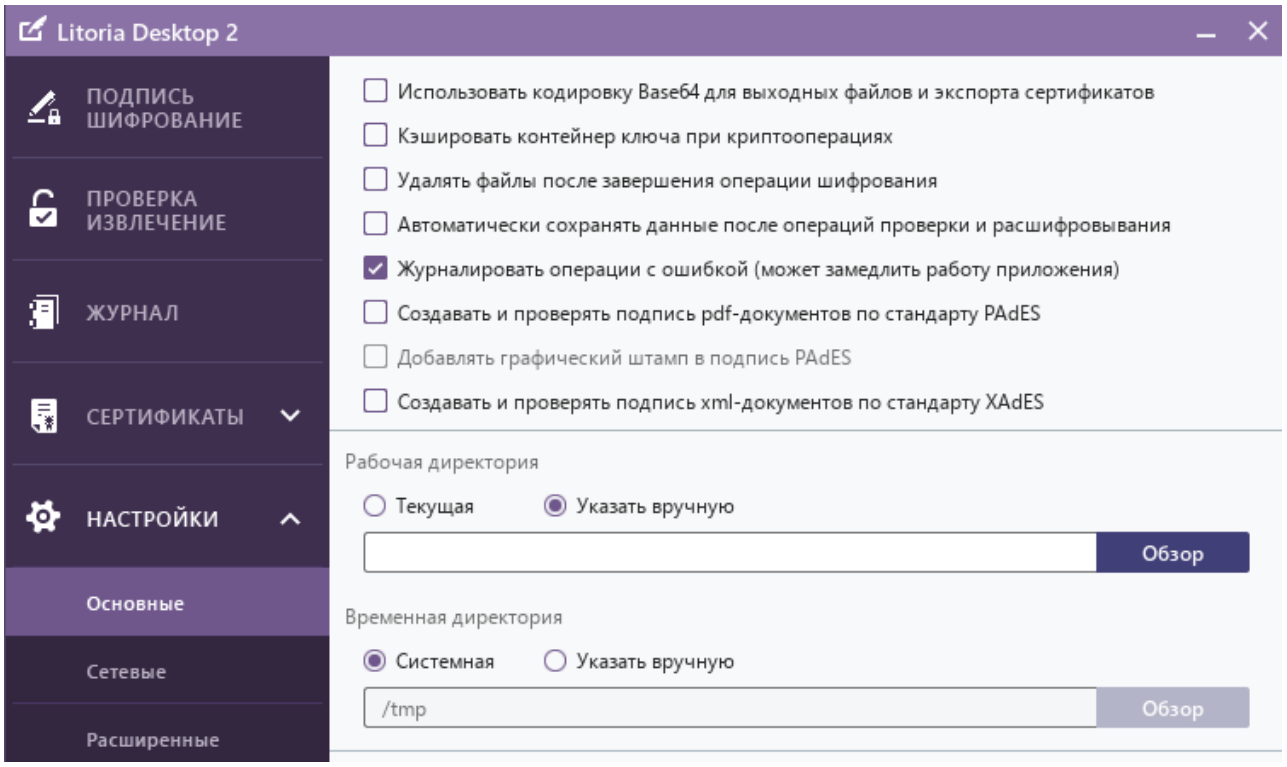


Рисунок 3.44 – Настройки директорий

Для указания другой директории установите переключатель в позицию «*Указать вручную*» и нажмите на кнопку «*Обзор*». 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.

3.4.2 Сетевые настройки

3.4.2.1 Настройка службы штампов времени

Для указания используемого адреса службы штампов времени в меню «*Настройки*»

пункт «*Сетевые*» в области «*Служба штампов времени*» введите адрес, который будет использоваться, в поле «*Адрес по умолчанию*» (рисунок 3.45).

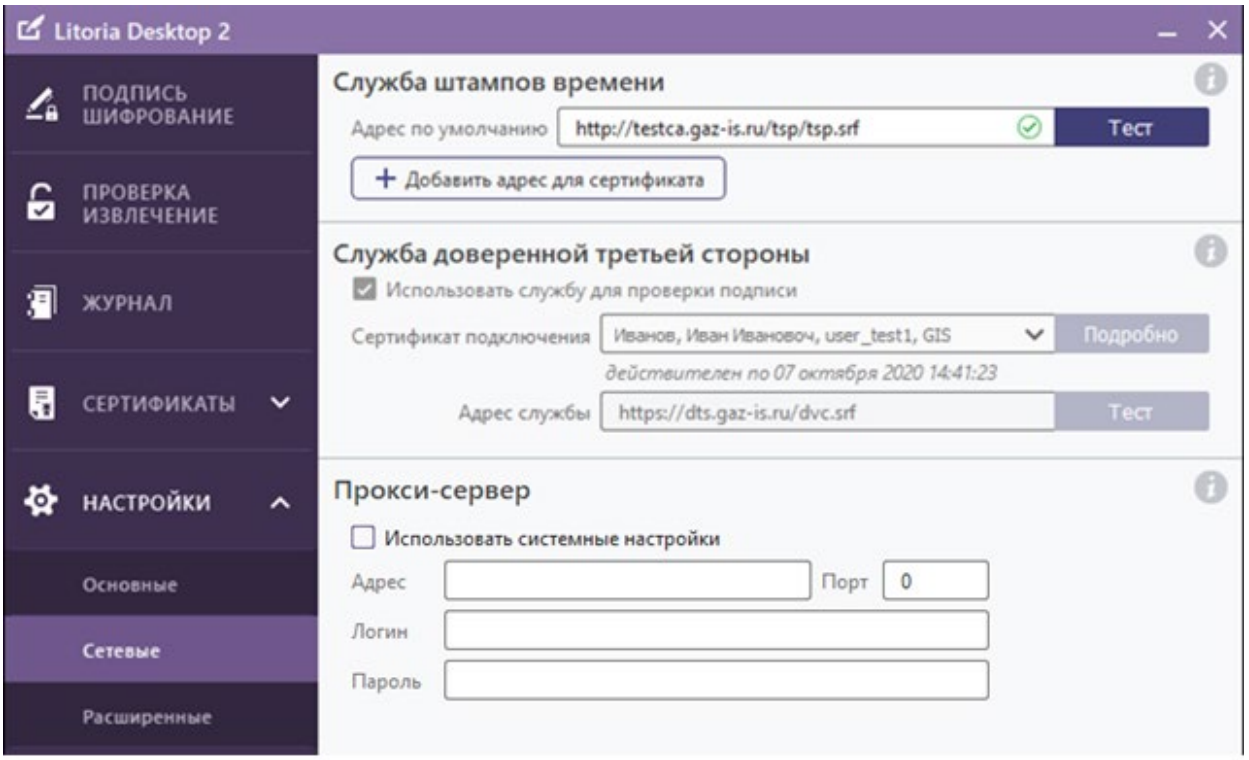


Рисунок 3.45 – Настройка адреса службы штампов времени

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 3.46). 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.

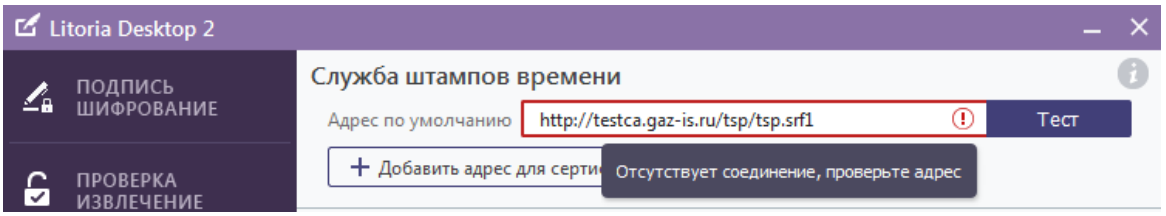


Рисунок 3.46 – Сообщение об ошибке «Отсутствует соединение»

В случае сообщения об ошибке «*Нет доверия к сертификату службы*» (рисунок 3.47) необходимо нажать на ссылку с сообщением для получения детальной информации о сертификате службы с дальнейшей возможностью разрешения проблемы доверия.

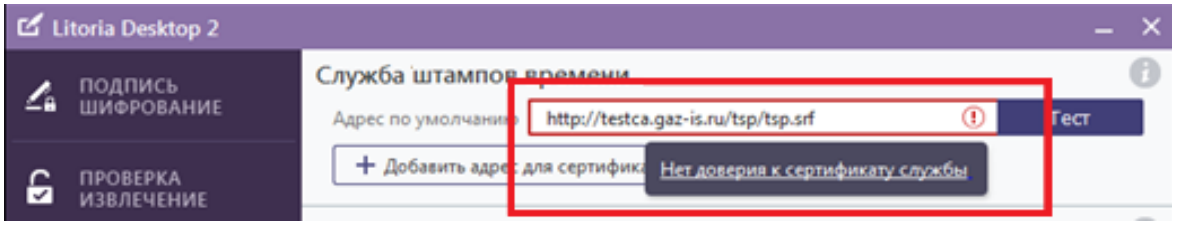


Рисунок 3.47 – Сообщение об ошибке «Нет доверия к сертификату службы»

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.

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.

3.4.2.2 Настройки службы доверенной третьей стороны

Если администратором комплекса установлен флаг «*Использовать службу для проверки подписи*» в области «*Служба доверенной третьей стороны*» (рисунок 3.48), пользователю станут доступными для заполнения поля «*Сертификат клиента*» и «*Адрес службы*».

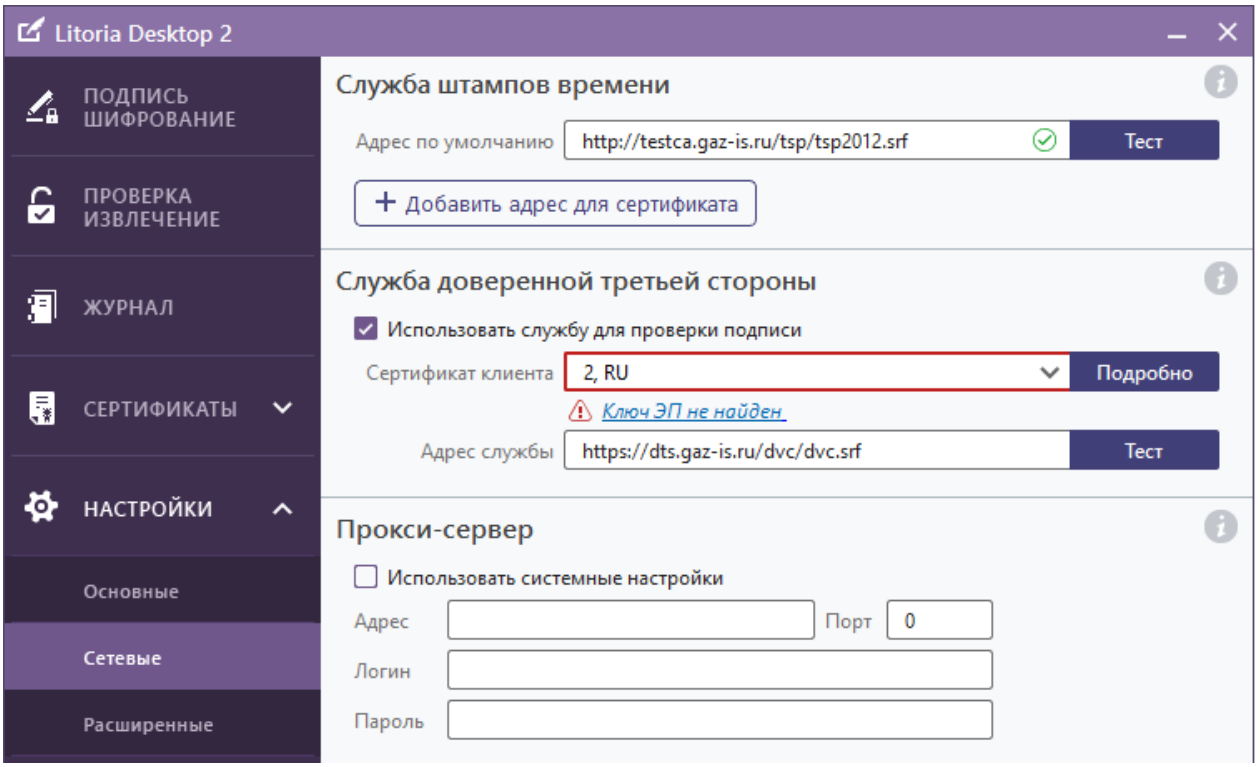


Рисунок 3.48 – Настройки службы доверенной третьей стороны

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 3.49).

Для ввода ПИН-кода нажмите на ссылку «*Ключ ЭП не найден»* и в появившемся окне укажите в соответствующем поле ПИН-код к контейнеру (рисунок 3.49) и нажмите на кнопку «*Проверить*».

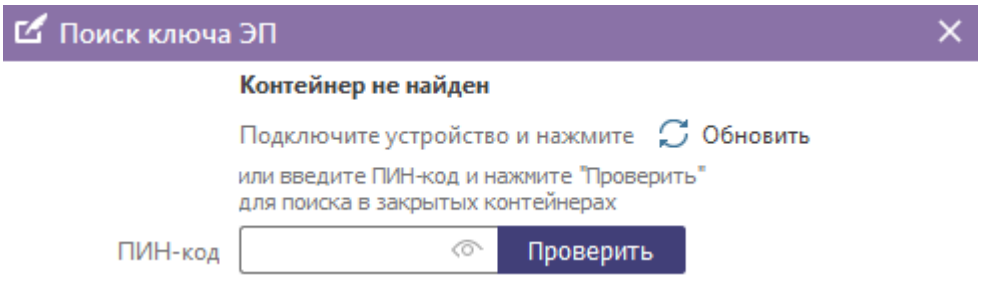


Рисунок 3.49 – Поиск ключа ЭП

Если ПИН-код к контейнеру не был найден, проверьте наличие физического отчуждаемого носителя в нужном разъеме (при его использовании) и нажмите кнопку «Обновить» (рисунок 3.49).

Если данные указаны верно, внизу поля с сертификатом появится сообщение о сроке действия сертификата (рисунок 3.50). Сертификат готов к использованию.

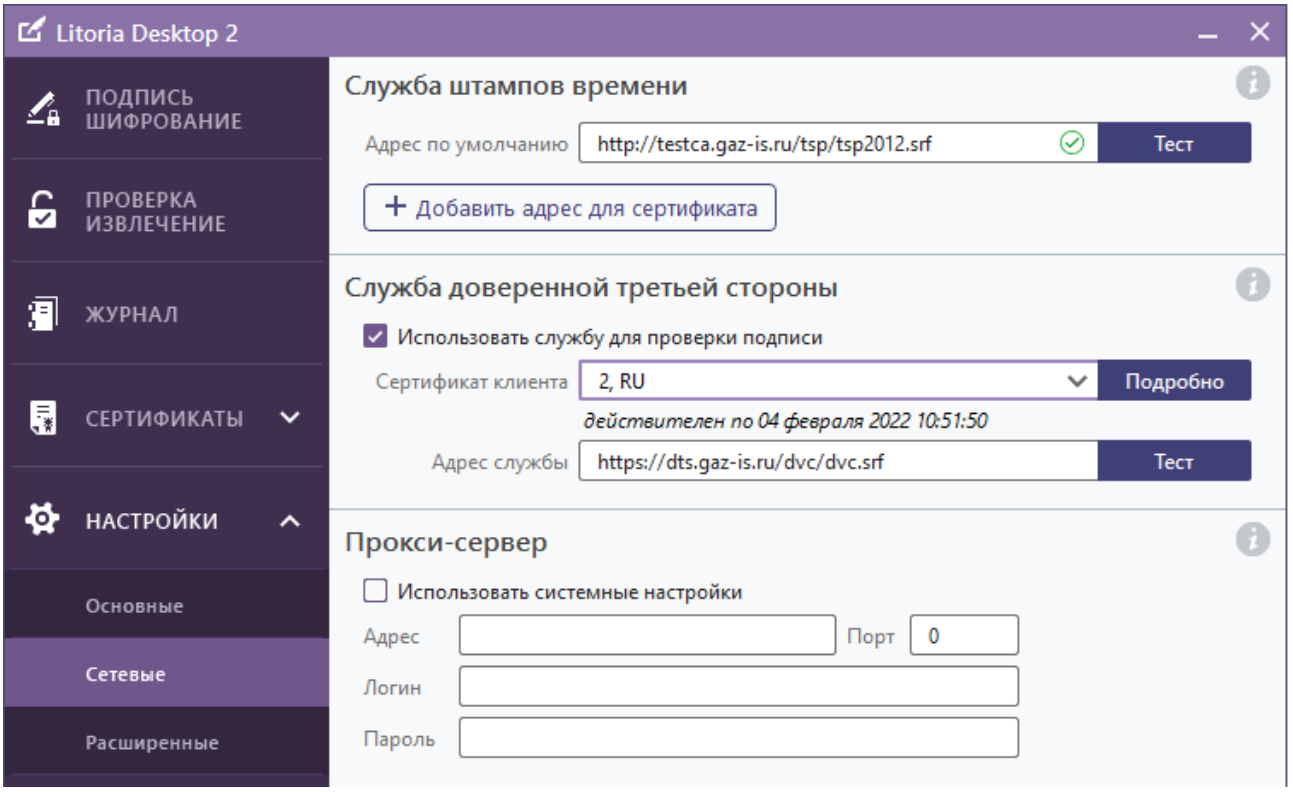


Рисунок 3.50 – Готовность сертификата к использованию

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 3.51), 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.3.4.2.1).

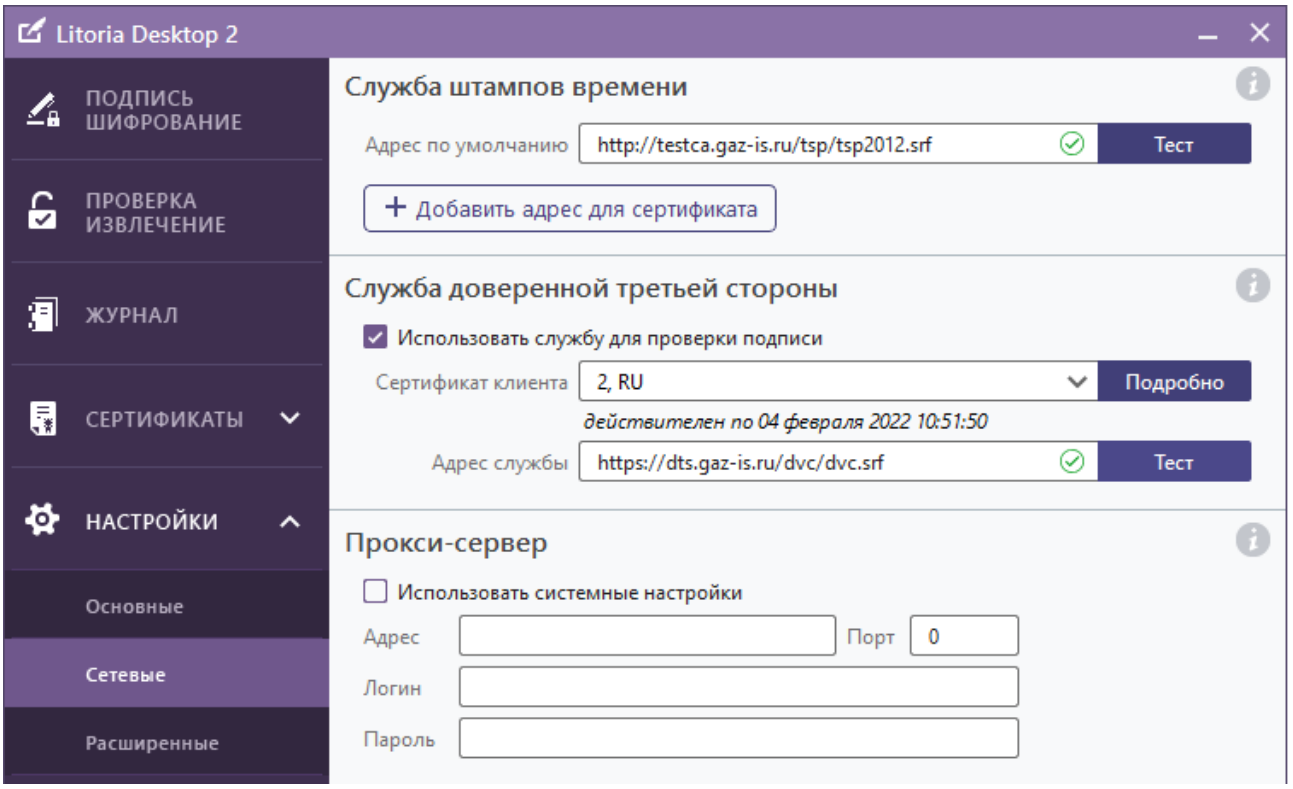


Рисунок 3.51 – Проверка работоспособности службы доверенной третьей стороны

Сертификат подключения 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 3.52), 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.

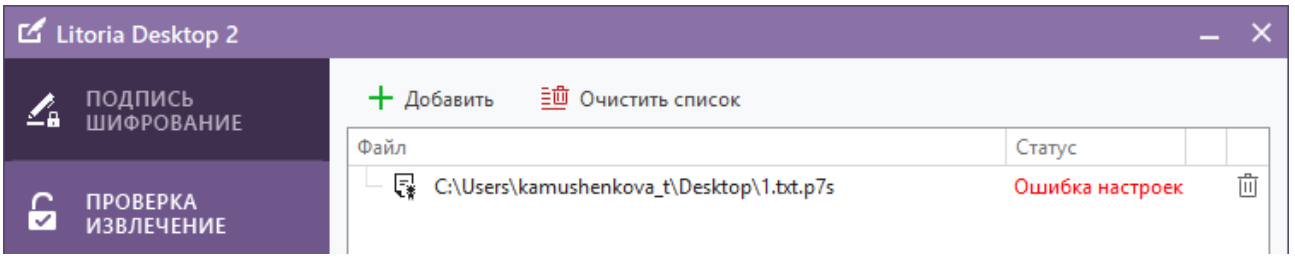


Рисунок 3.52 – Необходимость в настройке параметров службы ДТС

3.4.2.3 Настройка сети

Для настройки аутентификации на прокси-сервере в меню «*Настройки*» пункт «*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 3.53).

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.

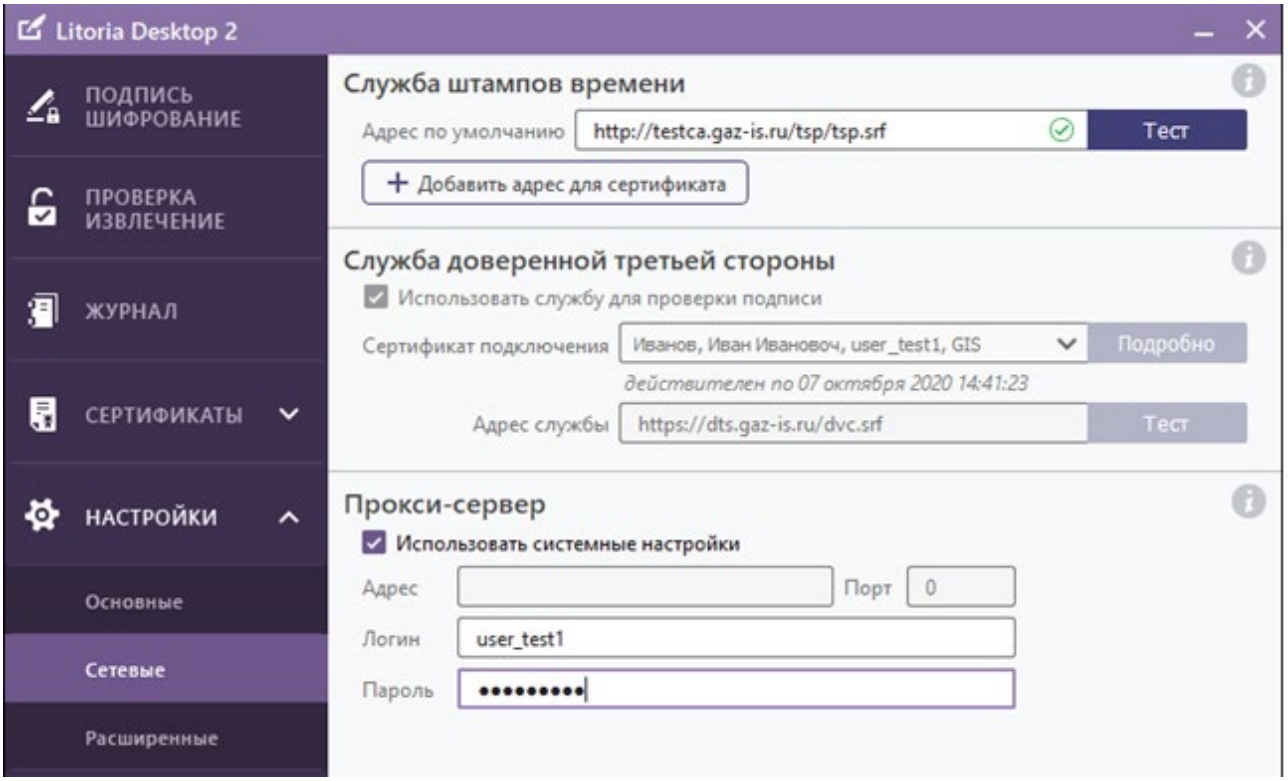


Рисунок 3.53 – Настройки прокси-сервера

3.4.3 Расширенные настройки

3.4.3.1 Настройка языка интерфейса

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 3.54). Изменения вступят в силу после перезагрузки ПК «Litoria Desktop 2».

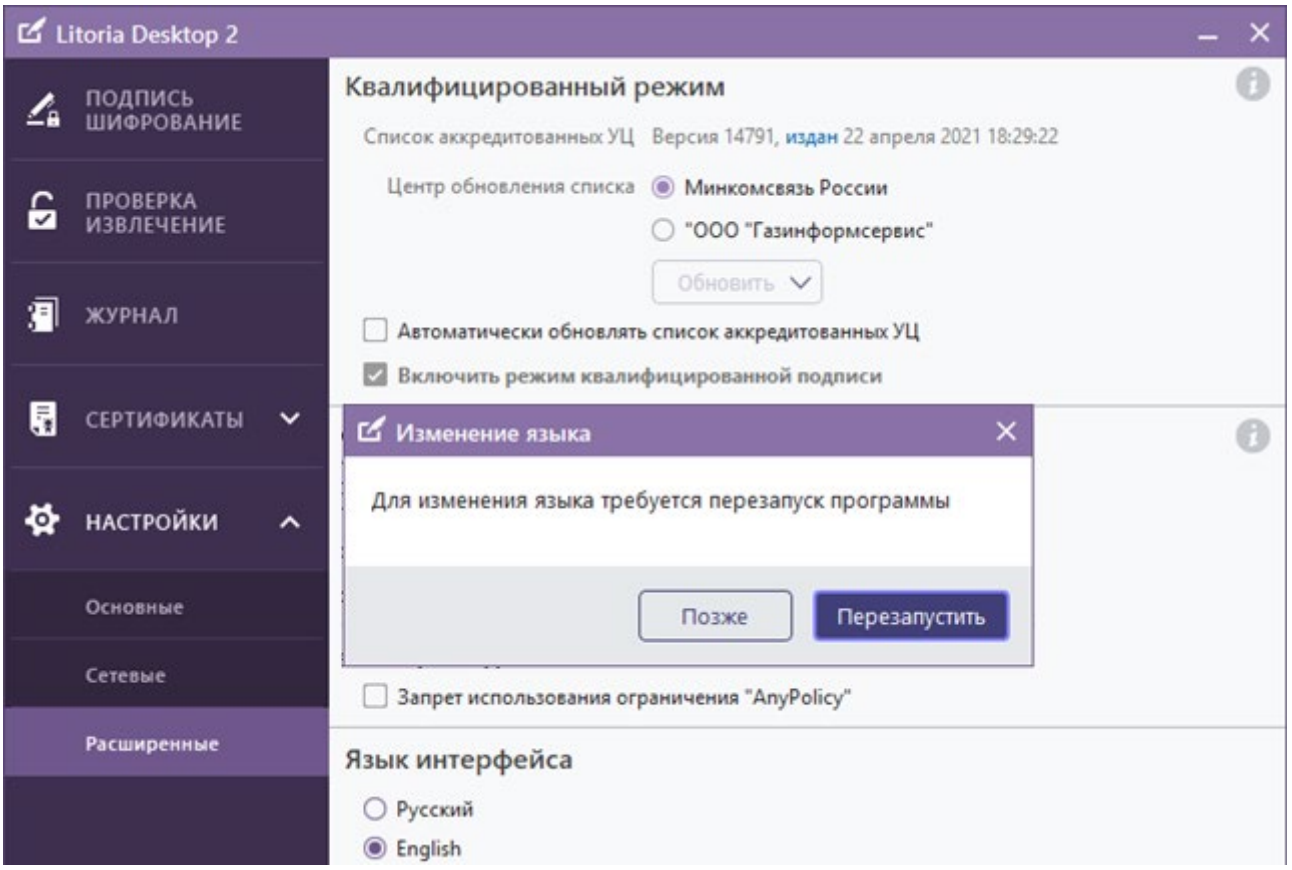


Рисунок 3.54 – Изменение языка интерфейса

3.5 Управление контейнерами

ПК «Litoria Desktop 2» позволяет просмотреть список криптопровайдеров, которые администратора указал как разрешенные для пользователя, все контейнеры, относящиеся к установленным криптопровайдерам, и имеющиеся на ключевом отчуждаемом носителе. Также в ПК «Litoria Desktop 2» осуществляется работа с контейнерами: импорт сертификата в контейнер, экспортирование сертификата с закрытым ключом и без него, удаление контейнера.

3.5.1 Просмотр списка контейнеров

1 Откройте интерфейс ПК «Litoria Desktop 2».
2 Раскройте меню «*Сертификаты*».
3 Для просмотра списка доступных пользователю криптопровайдеров выберите пункт «*Контейнеры*».
4 Появится окно со списком криптопровайдеров, доступных пользователю (рисунок 3.55).

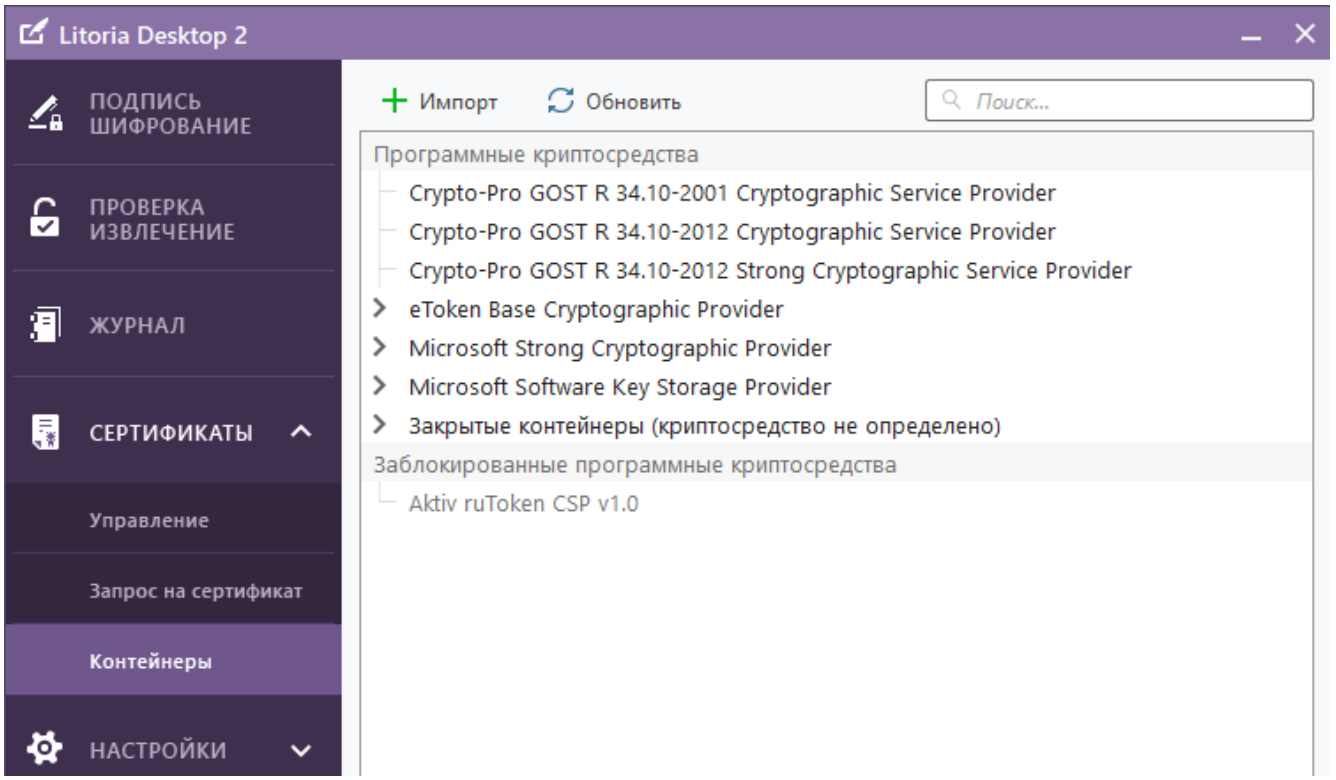


Рисунок 3.55 – Список установленных криптопровайдеров

5 Для просмотра списка контейнеров на выбранном криптопровайдере, раскройте щелчком мыши нужный криптопровайдер (рисунок 3.56).

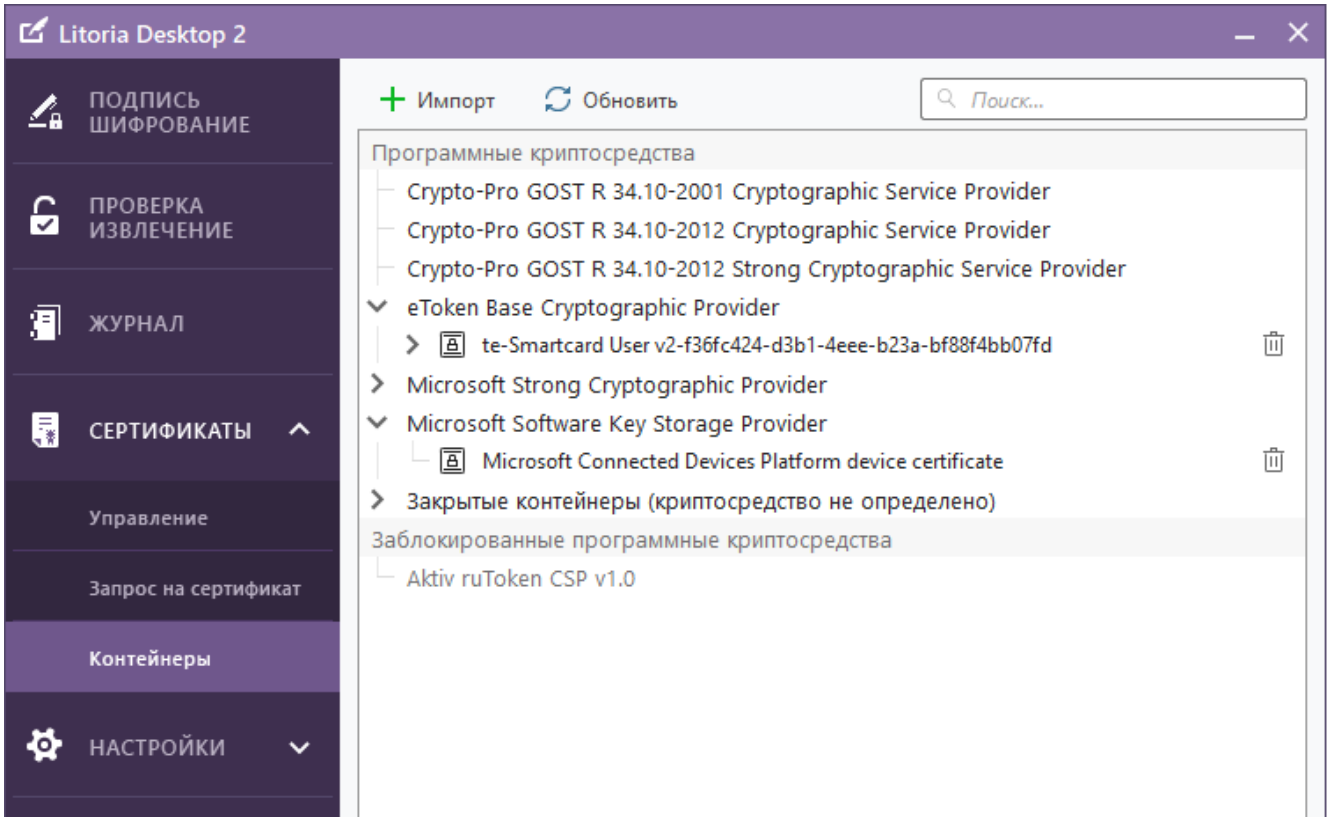


Рисунок 3.56 – Список контейнеров на криптопровайдерах

6 Если контейнер находится на отчуждаемом носителе, вставьте этот носитель в соответствующий разъем и нажмите кнопку «*Обновить*».

3.5.2 Импорт сертификата в контейнер

1 Откройте интерфейс ПК «Litoria Desktop 2».
2 Раскройте меню «*Сертификаты*».
3 Выберите пункт «*Контейнеры*» (рисунок 3.55).
4 Нажмите на кнопку «*Импорт*».
5 В появившемся окне «*Импорт сертификата в контейнер*» (рисунок 3.57) для выбора импортируемого сертификата нажмите на кнопку «*Обзор*».

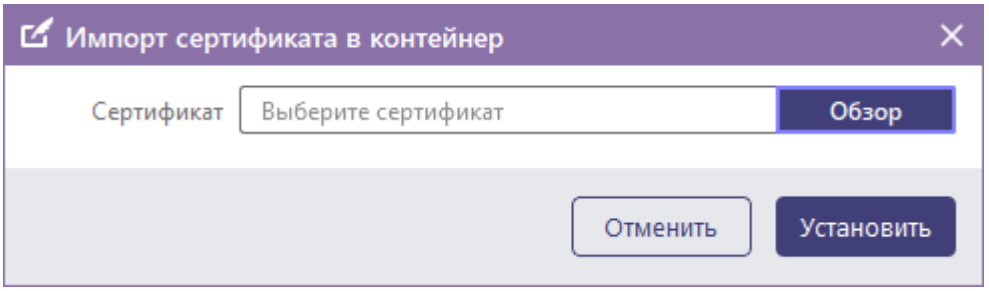


Рисунок 3.57 – Импорт сертификата в контейнер

6 В появившемся окне укажите файл сертификата (обычно имеет расширение .cer или .crt) и нажмите на кнопку «*Открыть*».
7 Контейнер для импорта сертификата определится автоматически (рисунок 3.58). Для продолжения установки нажмите на кнопку «*Установить*».

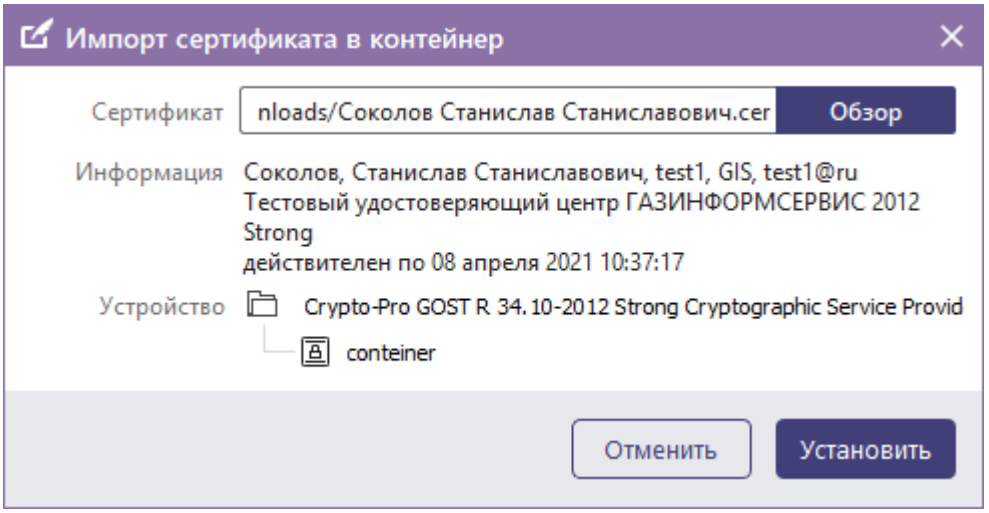


Рисунок 3.58 – Отображение устройства при выборе сертификата для импорта

Результат: выбранный сертификат импортирован на устройство.

3.5.3 Экспорт сертификата из контейнера

1 Откройте интерфейс ПК «Litoria Desktop 2».
2 Раскройте меню «*Сертификаты*».
3 Выберите пункт «*Контейнеры*» (рисунок 3.55).

4 Выберите контейнер и сертификат, который необходимо экспортировать.

5 Нажмите на кнопку « » в строке, напротив выбранного сертификата.

6 Появится окно «Выберите файл для экспорта сертификата» (рисунок 3.59).

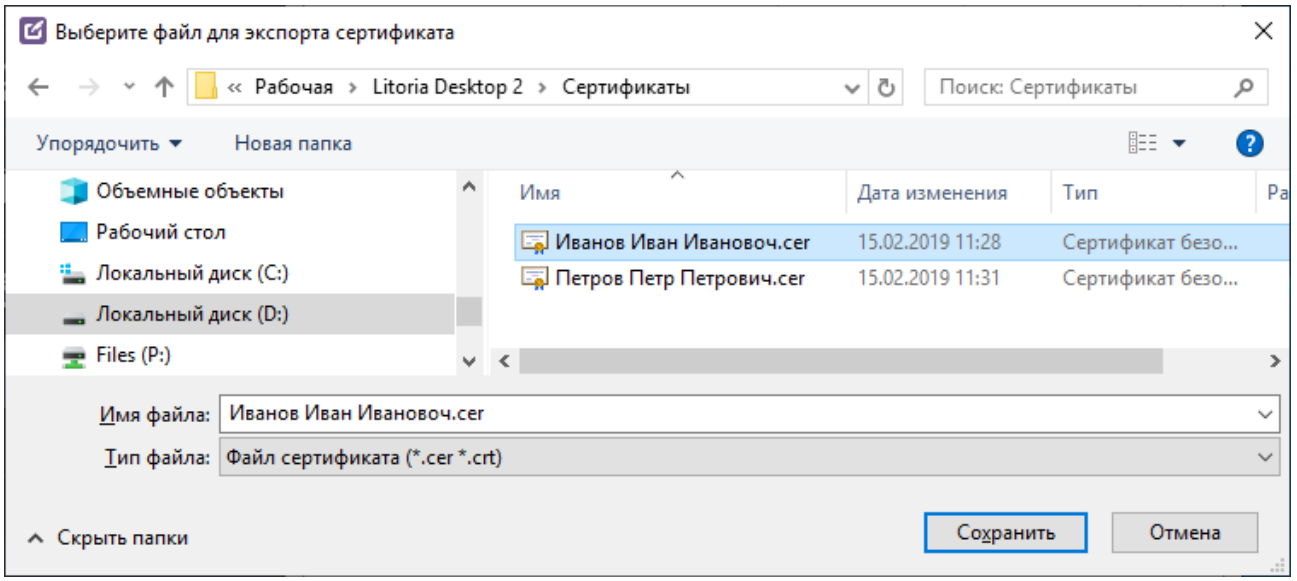


Рисунок 3.59 – Экспорт сертификата

7 Для указания месторасположения и имени экспортируемого сертификата укажите каталог и имя файла, затем нажмите на кнопку «*Сохранить*».

Результат: выбранный сертификат сохранен в файл по указанному месторасположению.

3.5.4 Экспорт сертификата с закрытым ключом

1 Откройте интерфейс ПК «Litoria Desktop 2».

2 Раскройте меню «*Сертификаты*».

3 Выберите пункт «*Контейнеры*» (рисунок 3.55).

4 Выберите контейнер и сертификат, который необходимо экспортировать.

5 Нажмите на кнопку « » в строке, напротив выбранного сертификата.

6 В случае, если экспортируется сертификат с закрытым ключом, при нажатии на кнопку « » появится окно «*Экспортирование закрытого ключа*» (рисунок 3.60).

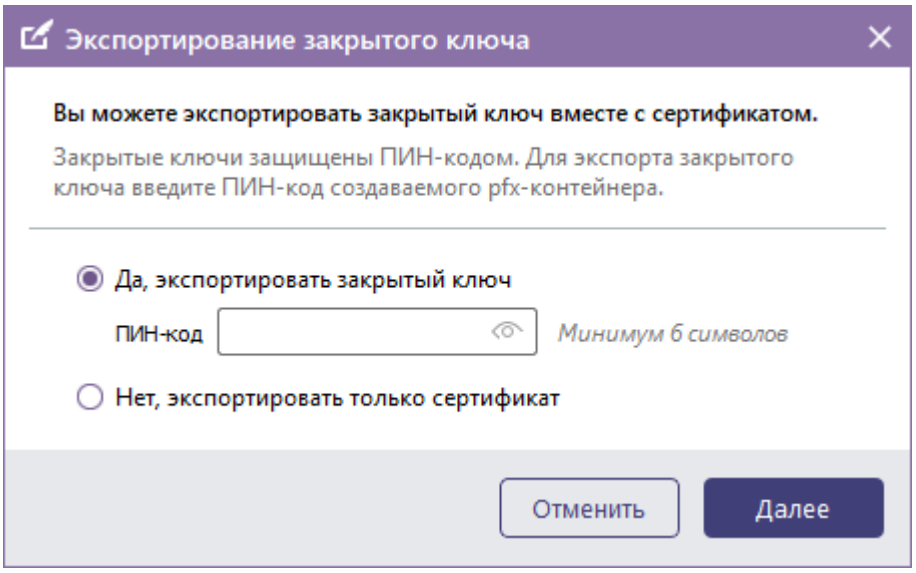


Рисунок 3.60 – Экспортирование сертификата с закрытым ключом

7 При выборе экспортирования сертификата без ключа «*Нет, экспортировать только сертификат*» после нажатия на кнопку «*Далее*» появится окно «*Выберите файл для экспорта сертификата*» (рисунок 3.60), в котором необходимо выбрать месторасположение и указать имя создаваемого файла по аналогии с действиями, описанными в пункте **3.5.3 «Экспорт сертификата из контейнера»**.

8 При выборе экспортирования закрытого ключа вместе с сертификатом, установив «*Да, экспортировать закрытый ключ*», введите ПИН-код в соответствующее поле и нажмите «*Далее*».

9 Введите ПИН-код к контейнеру в появившемся окне.

10 Далее в окне «*Выберите файл для экспорта контейнера*» (рисунок 3.61) введите имя экспортируемого контейнера и задайте его месторасположение, затем нажмите на кнопку «*Сохранить*».

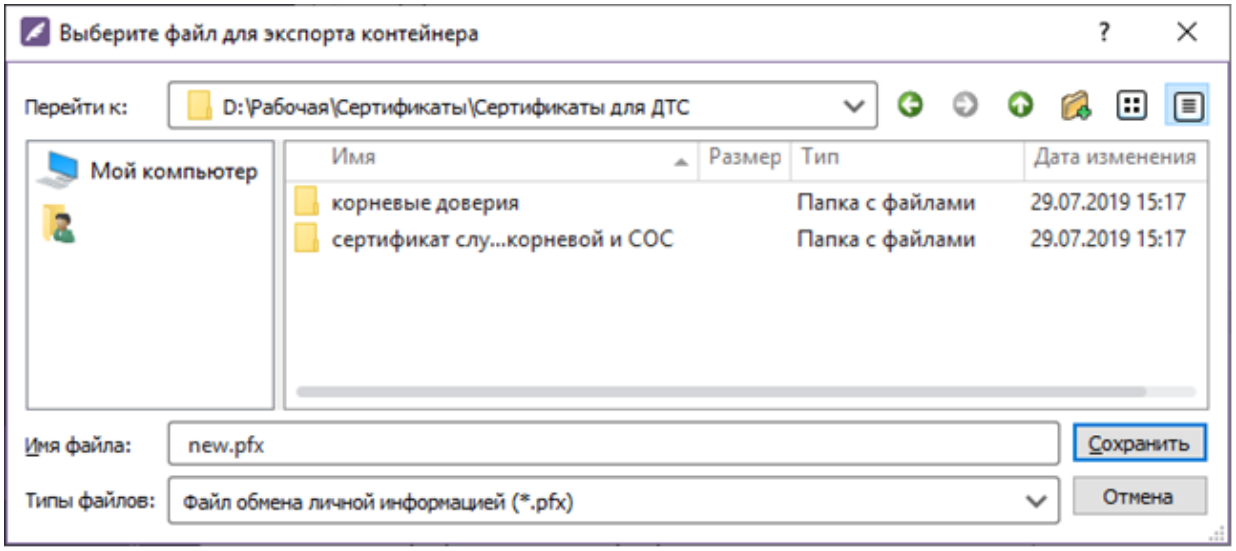


Рисунок 3.61 – Ввод имени экспортируемого контейнера

Результат: выбранный сертификат с закрытым ключом сохранен в контейнер по указанному месторасположению.

3.5.5 Удаление контейнера

1 Откройте интерфейс ПК «Litoria Desktop 2».
2 Раскройте меню «*Сертификаты*».
3 Выберите пункт «*Контейнеры*».
4 Появится окно, в котором отображен список криптопровайдеров, установленных на компьютере (рисунок 3.55).
5 Для удаления контейнера раскройте щелчком мыши криптопровайдер, с помощью которого он был создан, и, если контейнер находится на отчуждаемом носителе, вставьте этот носитель в соответствующий разъем.
6 В списке доступных контейнеров выберите тот, который хотите удалить, и нажмите на кнопку «» в соответствующей строке (рисунок 3.56).
7 Если в удаляемом контейнере содержится действующий сертификат, при нажатии на кнопку «» появится предупреждающее сообщение, что сертификат из контейнера будет невозможно использовать для подписания и расшифровывания после удаления контейнера (рисунок 3.62).

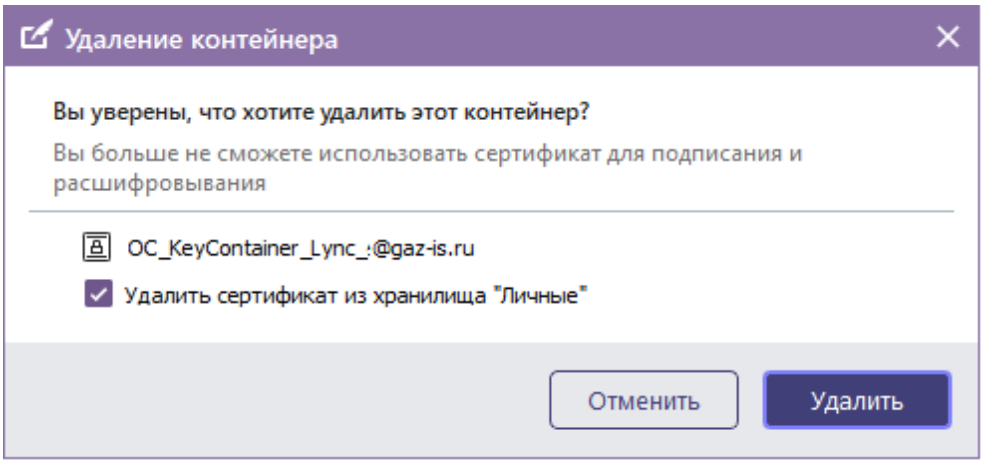


Рисунок 3.62 – Подтверждение удаления контейнера

8 Для удаления контейнера нажмите на кнопку «*Удалить*».

Результат: выбранный контейнер удален.

3.6 Подпись электронного документа

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 личного 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.

Для создания ЭП выполните следующие действия:

1 Откройте интерфейс ПК «Litoria Desktop 2».
2 Выберите меню «*Подпись Шифрование*» (рисунок 3.63).

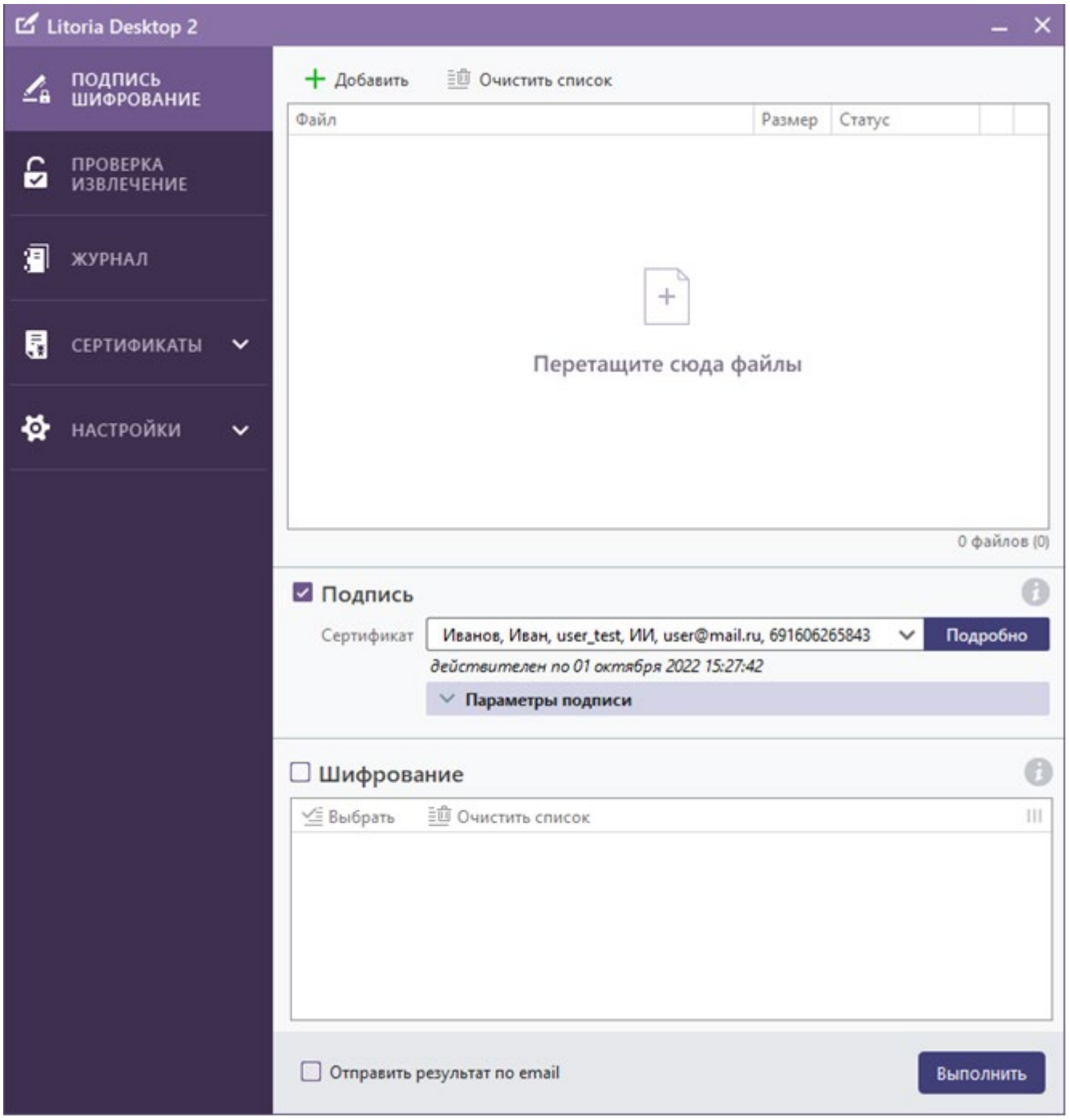


Рисунок 3.63 – Подпись документов

3 Поместите файлы, которые хотите подписать, в список файлов. Данную операцию можно выполнить несколькими способами:

– нажатием на кнопку «*Добавить*» и выбором необходимого файла в открывшемся окне;
– перетаскиванием файла или папки из окна Проводника в область списка файлов;
– выбором в контекстном меню нужного файла *«Litoria Desktop 2»* → *«Подписать»* (рисунок 3.64).

При добавлении файлов на выполнение операции через контекстное меню рекомендуется выбирать не более 400 файлов одновременно. При необходимости добавления большего количества файлов используйте другой способ добавления файлов.

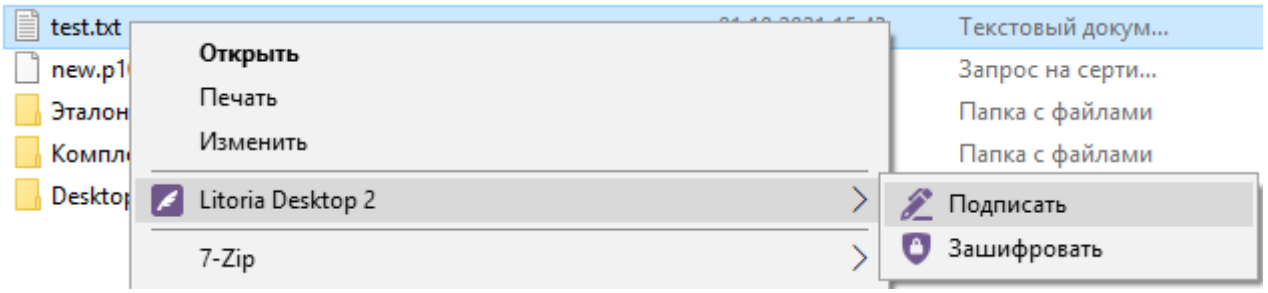


Рисунок 3.64 – Подпись документов через контекстное меню

При необходимости перед подписью добавленных файлов просмотрите их содержимое по щелчку мыши на имени файла в списке добавленных файлов.

4 Для создания ЭП необходимо поставить флаг «*Подпись*».

5 При использовании физического отчуждаемого носителя вставьте его в нужный разъем.

6 Для указания сертификата, которым вы хотите подписать файл, выберите сертификат из списка с вашими личными сертификатами в соответствующей области в поле «*Сертификат*» (рисунок 3.65).

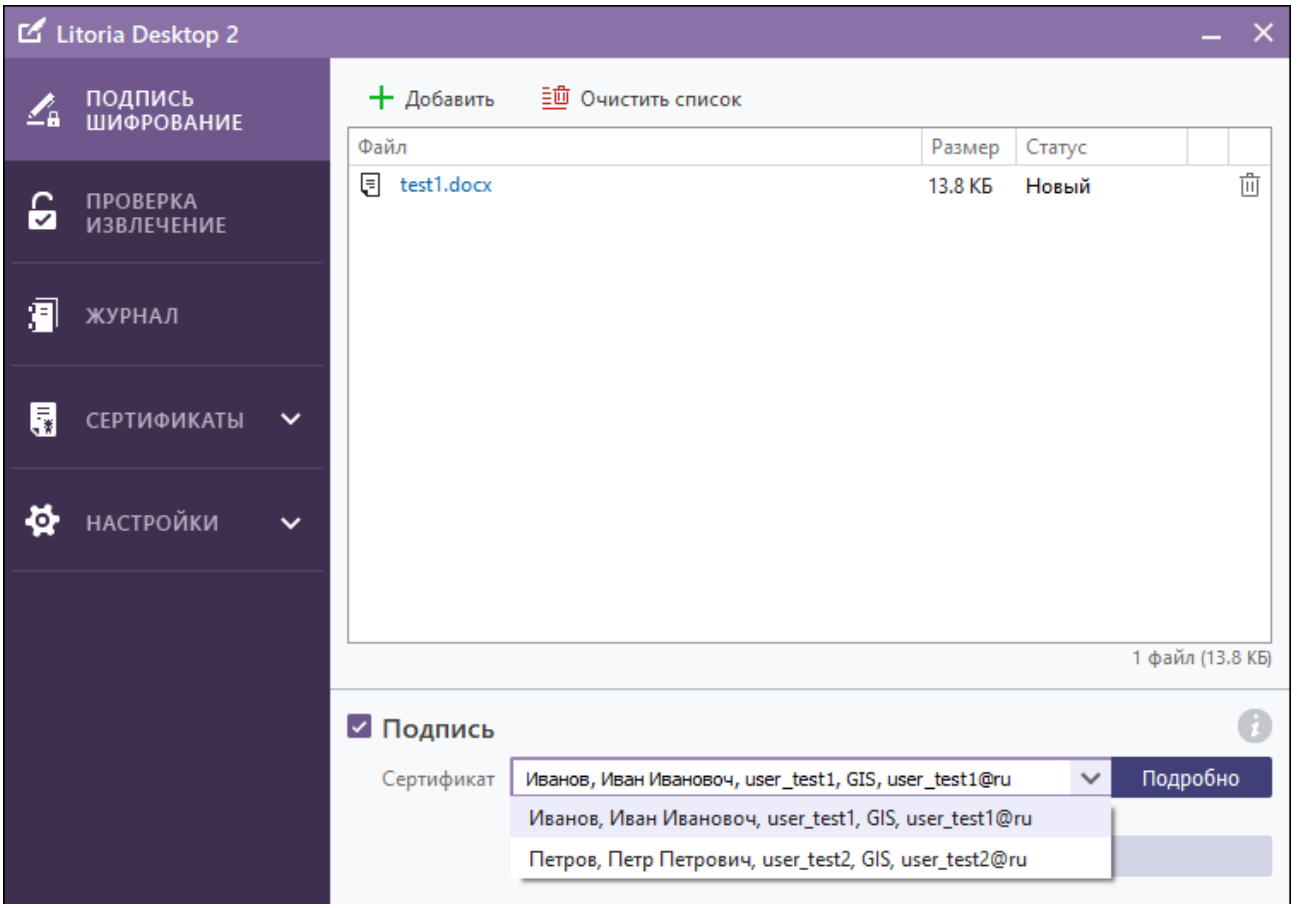


Рисунок 3.65 – Список сертификатов

7 Если данные указаны верно, внизу поля с выбранным сертификатом появится сообщение о сроке действия выбранного сертификата (рисунок 3.66). Сертификат готов к использованию.

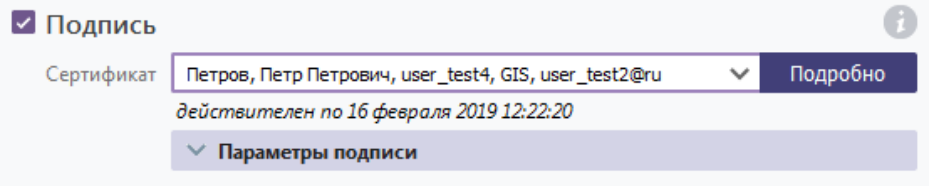


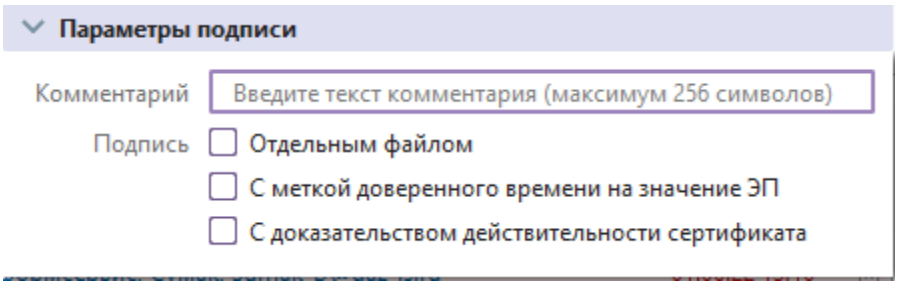
Рисунок 3.66 – Ключ ЭП найден

8 Установите параметры подписи (рисунок 3.67). В таблице 3.1 указаны типы подписи и параметры, установка которых необходима для их создания.

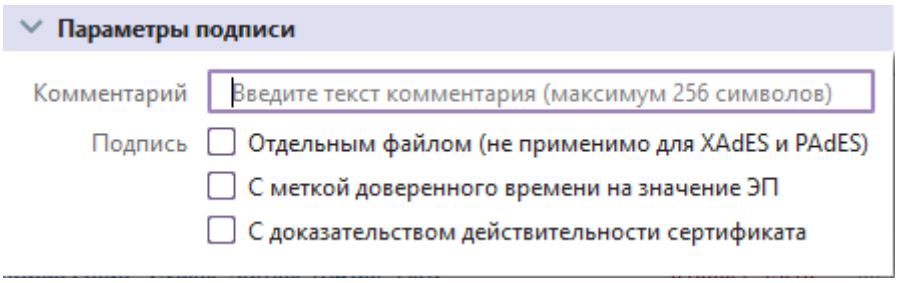
Таблица 3.1 – Типы и параметры подписи

Тип подписи	Параметры подписи в ПК «Litoria Desktop 2»	Примечание
Обычная совмещенная	–	Никакие флаги не надо устанавливать

Тип подписи	Параметры подписи в ПК «Litoria Desktop 2»	Примечание
Обычная отделенная	Отдельным файлом[5]	
Обычная совмещенная с меткой доверенного времени на значение ЭП	С меткой доверенного времени на значение ЭП	
Обычная отделенная с меткой доверенного времени на значение ЭП	Отдельным файлом; С меткой доверенного времени на значение ЭП	
С доказательством действительности сертификата совмещенная	С доказательством действительности сертификата	Флаг «С меткой доверенного времени на значение ЭП» установится автоматически
С доказательством действительности сертификата отделенная	Отдельным файлом; С доказательством действительности сертификата	Флаг «С меткой доверенного времени на значение ЭП» установится автоматически



а)



б)

Рисунок 3.67 – Параметры подписи

[5] Создание подписи отдельным файлом для pdf-документов по стандарту PAdES и xml-документов по стандарту XAdES недоступно. Если в «Основных настройках» установлена одна или обе опции «Создавать и проверять подпись pdf-документов по стандарту PAdES» и «Создавать и проверять подпись xml-документов по стандарту XAdES», в поле подпись «отдельным файлом» появится пояснение, что операция не применима для XAdES и PAdES (рисунок 3.67 б).

При создании ЭП с меткой доверенного времени или с доказательством действительности сертификата необходимо, чтобы в настройках ПК «Litoria Desktop 2» был задан корректный адрес службы штампов времени. Если на момент создания ЭП адрес не задан, появится сообщение с возможностью перехода к настройкам адреса службы штампов времени (рисунок 3.68).

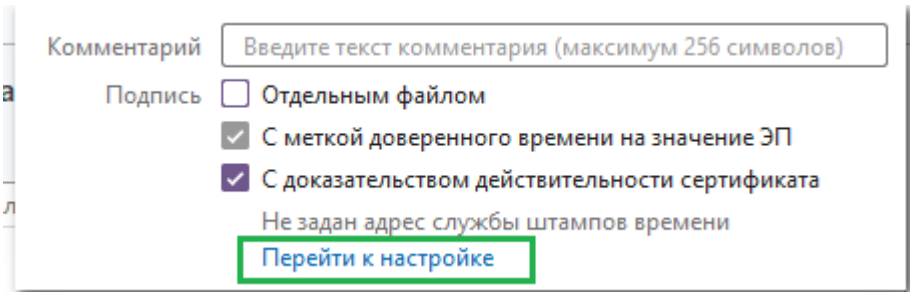


Рисунок 3.68 – Переход к вводу адреса службы штампов времени

9 При необходимости напишите комментарий к подписи в соответствующем поле.

10 Поставьте флаг «*Отправить результат по email*» при необходимости отправки подписанного документа на почту.

11 Для подписи документа необходимо нажать на кнопку «*Выполнить*».

12 Если операция выполнилась успешно, статус документа в списке поменяется на «*Выполнено*» (рисунок 3.69).

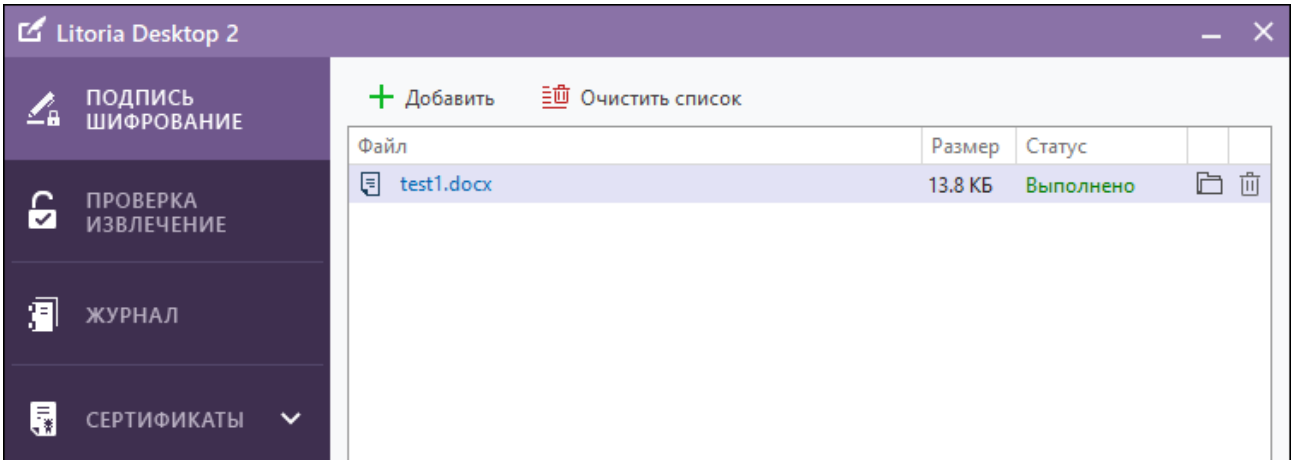


Рисунок 3.69 – Успешное выполнение операции

Результат: в текущем каталоге или в рабочей директории, которая указана в настройках, будет создан подписанный файл (или файл подписи – если создавалась отделенная подпись), обозначенный значком .

13 Просмотреть содержание подписанного файла можно по щелчку мыши на наименовании файла в списке добавляемых файлов (рисунок 3.69).

14 Просмотреть созданный подписанный файл (или файл подписи – если создавалась

отделенная подпись) в текущем каталоге или в рабочей директории, указанной в настройках, можно по кнопке « ».

При подписании pdf документа по стандарту PAdES (п.3.4.1.6) подпись встраивается в сам файл. Результатом подписи в текущем каталоге или в рабочей директории, которая указана в настройках, является файл вида, представленного на рисунке 3.70.

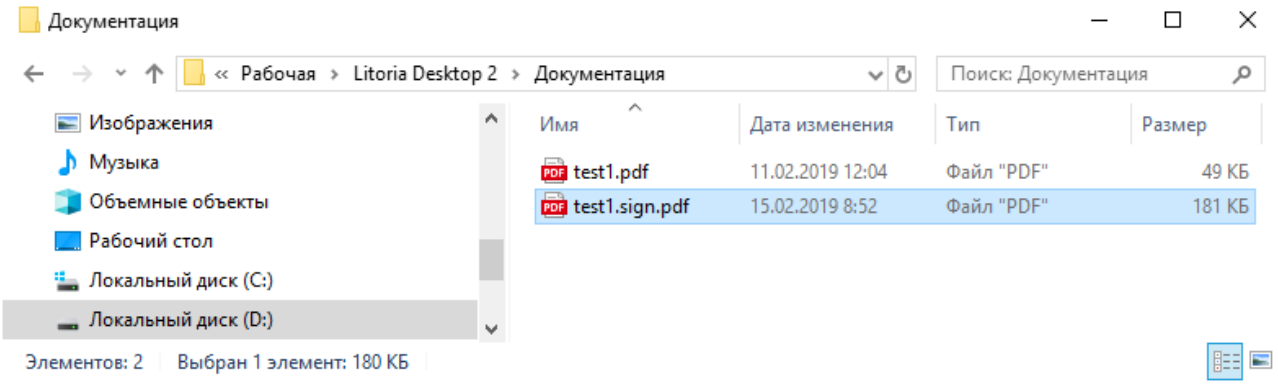


Рисунок 3.70 – Результат создания подписи pdf документа по стандарту PAdES

3.6.1 Возможные сообщения об ошибках при подписи документа

3.6.1.1 Сертификат не предназначен для подписи документа

Если в сертификате установлен флаг *«Критическое значение»* для расширений *«Использование ключа»* (рисунок 3.7), то подпись документов возможна только при наличии расширения *«Подпись данных»*. Если критическое расширение *«Подпись данных»* отсутствует, то в строке с выбранным сертификатом появится сообщение о невозможности использования данного сертификата для подписи (рисунок 3.6).

При отсутствии установленного флага «*Критическое значение*» для расширений *«Использование ключа»*, проверка наличия расширения *«Подпись данных»* не осуществляется.

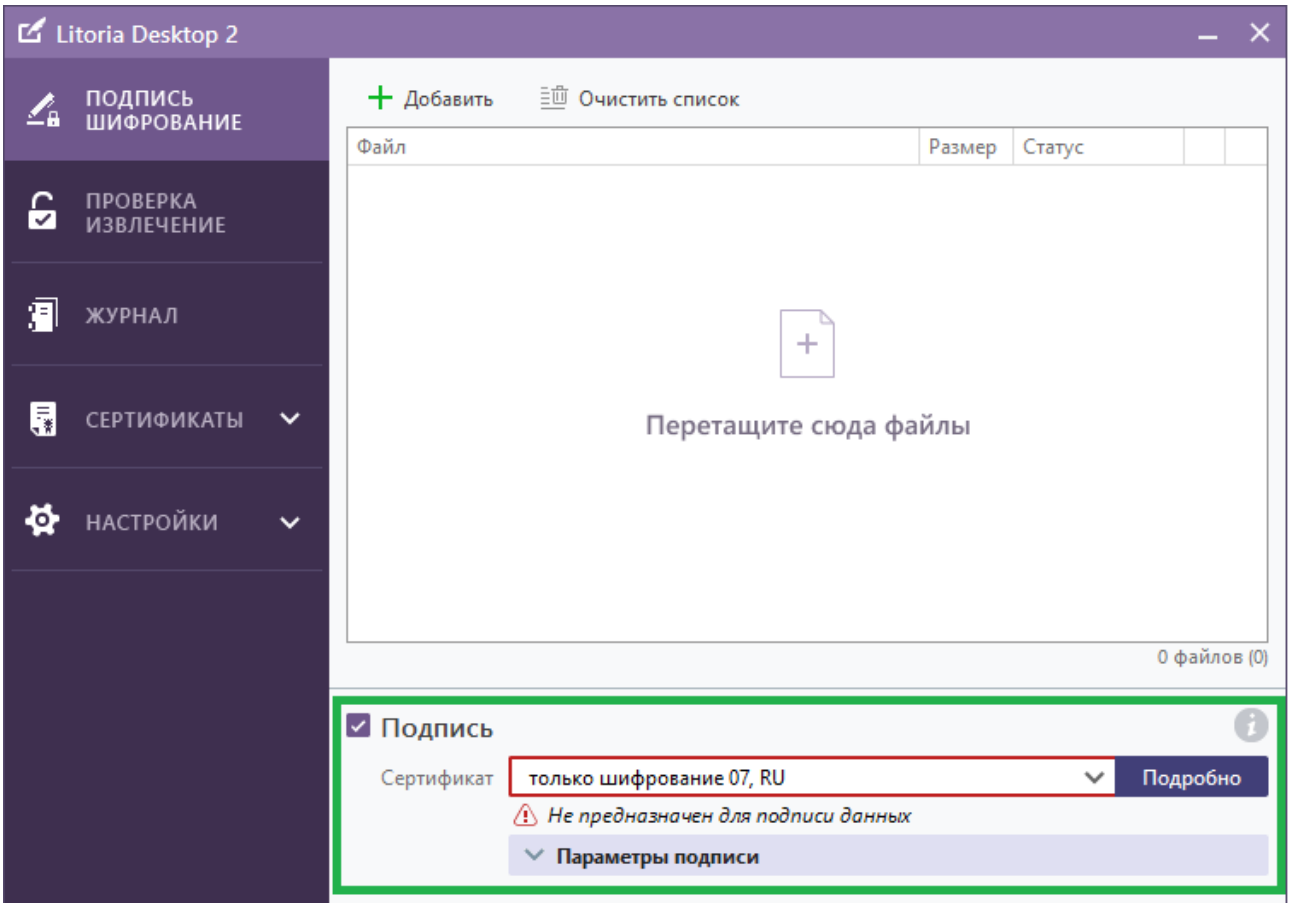


Рисунок 3.71 – Сертификат не предназначен для подписи

3.6.1.2 Ключ ЭП не обнаружен в доступных контейнерах

Если ключ ЭП выбранного сертификата не будет обнаружен в доступных конейнерах, внизу строки с выбранным сертификатом появится сообщение «*Ключ ЭП не найден*» (рисунок 3.72).

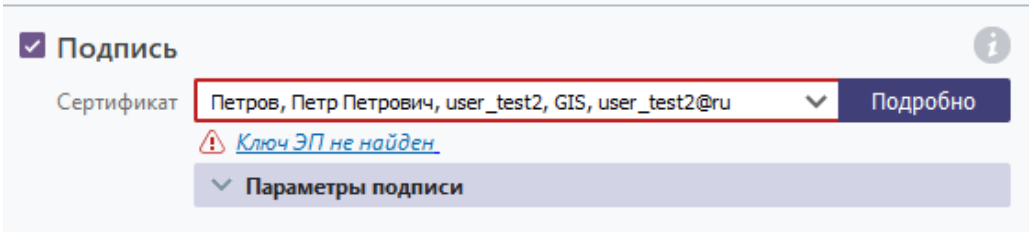


Рисунок 3.72 – Ключ ЭП не найден

По нажатию на ссылку «*Ключ ЭП не найден*» в появившемся окне (рисунок 3.72) введите ПИН-код к контейнеру в соответствующем поле, а затем нажмите на кнопку «*Проверить*».

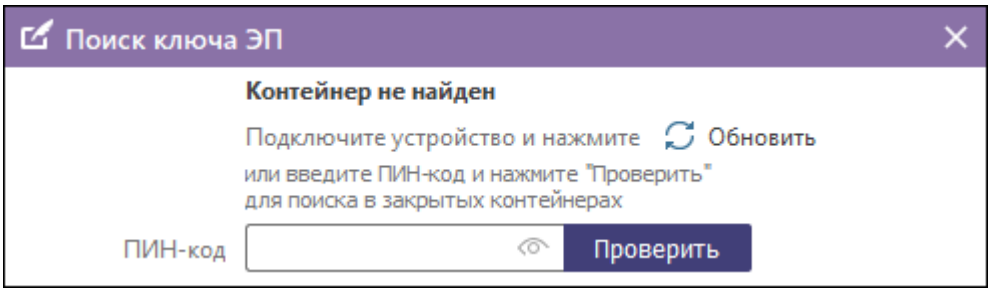


Рисунок 3.73 – Окно ввода ПИН-кода

Если ПИН-код к контейнеру не был найден, проверьте наличие физического отчуждаемого носителя в нужном разъеме (при его использовании) и нажмите кнопку «*Обновить*» (рисунок 3.73).

3.6.1.3 Истечение срока действия сертификата

Если у выбранного сертификата истек срок действия, внизу строки с выбранным сертификатом появится сообщение об истечении сертификата с указанием даты окончания срока действия сертификата (рисунок 3.74).

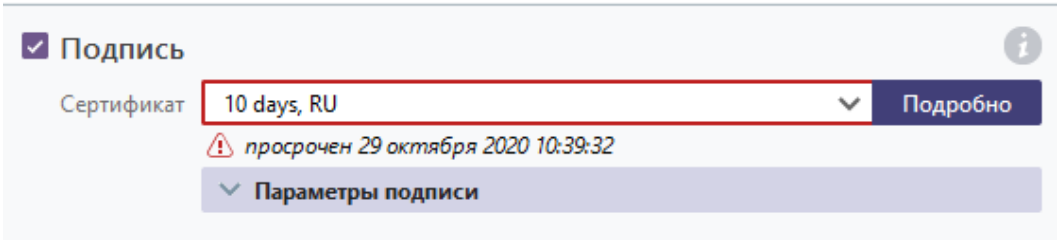


Рисунок 3.74 – Сертификат просрочен

3.6.1.4 Ошибка построения цепочки сертификата

Если при построении цепочки выбранного сертификата обнаружены ошибки (выполняются проверки на отозванность, искаженность сертификата, проверка доверия сертификата УЦ, срок списка отзыва сертификатов, искаженность списка отзыва), внизу строки с выбранным сертификатом появится сообщение об ошибке построения цепочки сертификатов (рисунок 3.75).

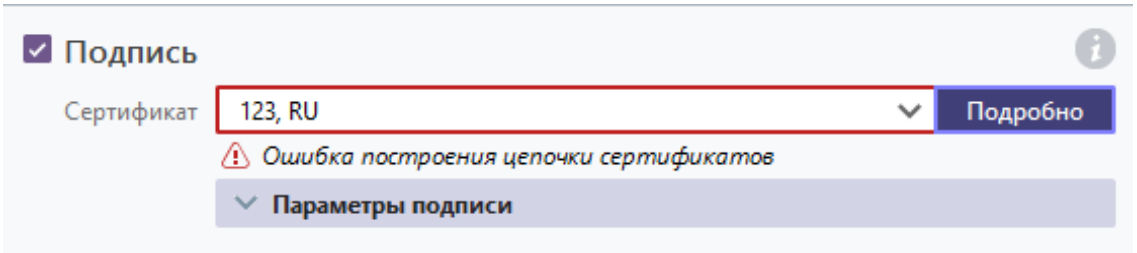


Рисунок 3.75 – Ошибка построения цепочки сертификатов

3.7 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 (рисунок 3.76).

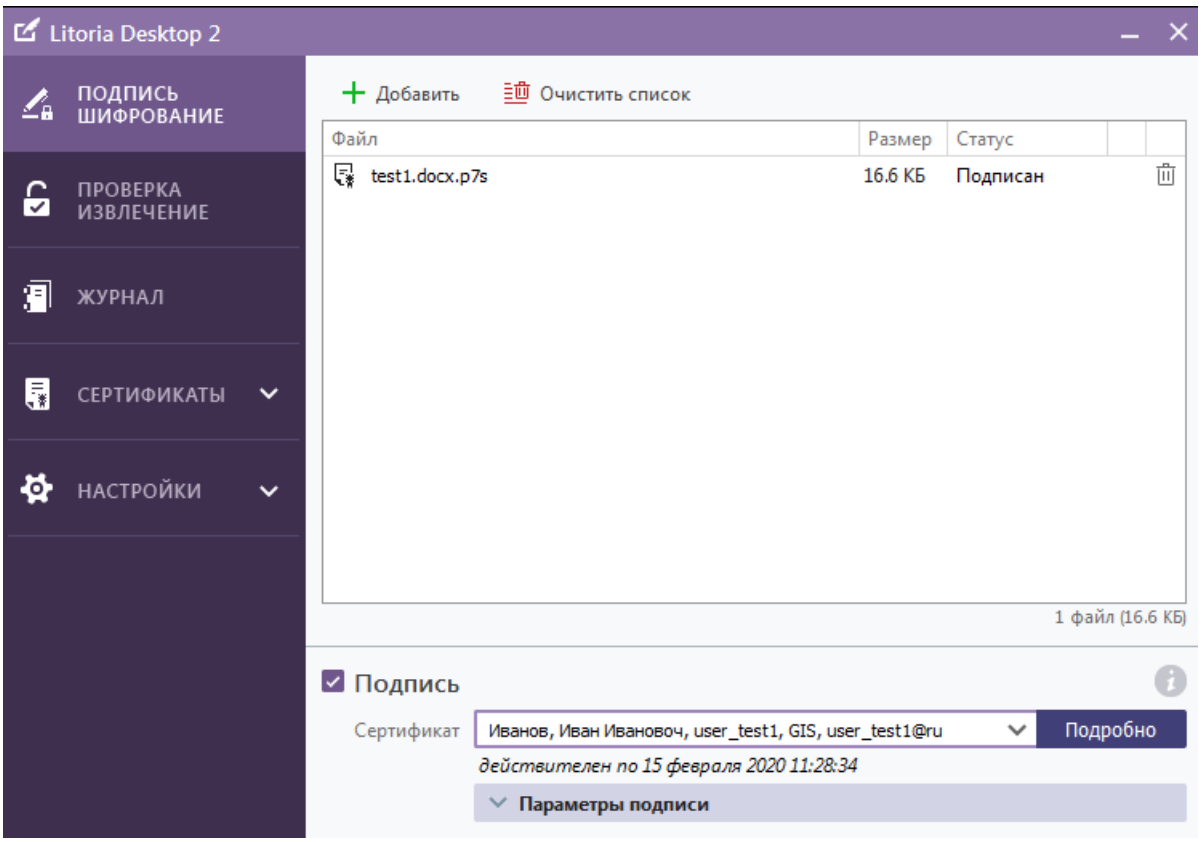


Рисунок 3.76 – Добавление подписи

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

Для добавления ЭП в документ необходимо выполнить действия для раннее подписанных файлов описанные в подразделе 3.6.

При операции добавления ЭП вид добавляемой подписи (отделенная или присоединенная подпись) определяется комплексом автоматически.

При добавлении ЭП с меткой доверенного времени или с доказательством действительности сертификата необходимо, чтобы в настройках ПК был задан корректный адрес службы штампов времени. Если на момент создания ЭП адрес не задан, появится сообщение с возможностью перехода к настройкам адреса службы штампов времени (рисунок 3.66).

Результат: в текущем каталоге или в рабочей директории, которая указана в настройках, будет создан файл, содержащий добавленную подпись и обозначенный значком .

При добавлении подписи в pdf документ по стандарту PAdES (п.3.4.1.6) подпись встраивается в сам файл. Результатом добавления подписи в pdf документ по стандарту PAdES в текущем каталоге или в рабочей директории, которая указана в настройках, будет файл, содержащий добавленные подписи (рисунок 3.77).

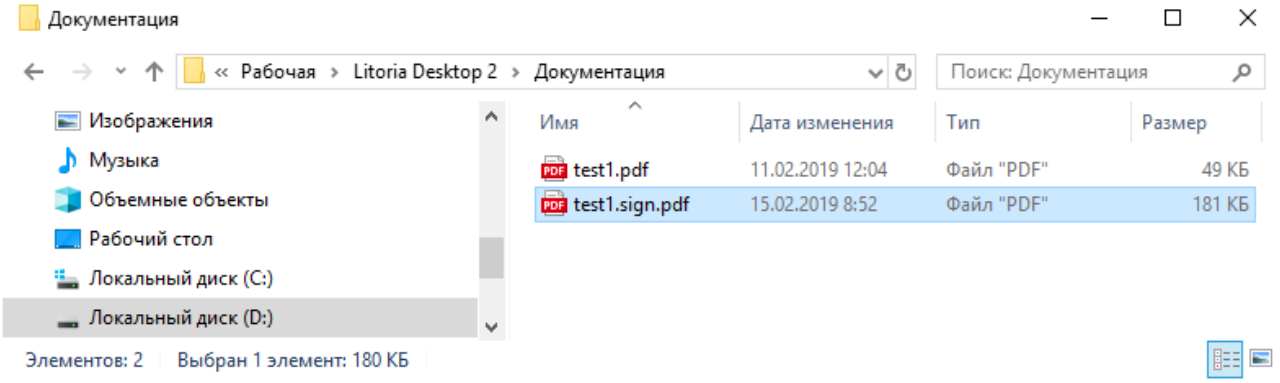


Рисунок 3.77 – Результат добавления подписи в pdf документ по стандарту PAdES

Возможные сообщения об ошибках при выполнении операции добавления подписи описаны в пункте **3.6.1 «Возможные сообщения об ошибках при подписи документа»**.

3.8 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, после шифрования 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 получателя пользователь может просмотреть статус, чтобы на его основании сделать вывод о пригодности данного сертификата.

Для шифрования файла выполните следующие действия:

1 Откройте интерфейс ПК «Litoria Desktop 2».
2 Выберите меню «*Подпись Шифрование*» (рисунок 3.63).
3 Поместите файлы, которые вы хотите зашифровать, в список файлов. Данную операцию можно выполнить несколькими способами:
   – нажатием на кнопку «*Добавить*» и выбором необходимого файла в открывшемся окне;
   – перетаскиванием файла или папки из окна Проводника в область списка файлов.
   – выбором в контекстном меню нужного файла *«Litoria Desktop 2»* → *«Зашифровать»* (рисунок 3.78).

Рисунок 3.78 – Шифрование файла через контекстное меню

При необходимости перед шифрованием добавленных файлов просмотрите их содержимое по щелчку мыши на имени файла в списке добавленных файлов.

4 Для шифрования файла необходимо поставить флаг «*Шифрование*».
5 Для выбора сертификатов получателей нажмите на кнопку Выбрать в области «*Шифрование*».
6 Появится окно «*Выбор сертификатов получателей*» (рисунок 3.79) в котором будут отображены сертификаты хранилища «Сертификаты других пользователей» и сертификаты пользовательских хранилищ.
7 По щелчку мыши на наименовании выбранного сертификата, можно просмотреть его содержимое, путь сертификации и провести проверку сертификата (см. пункт 3.3.5).

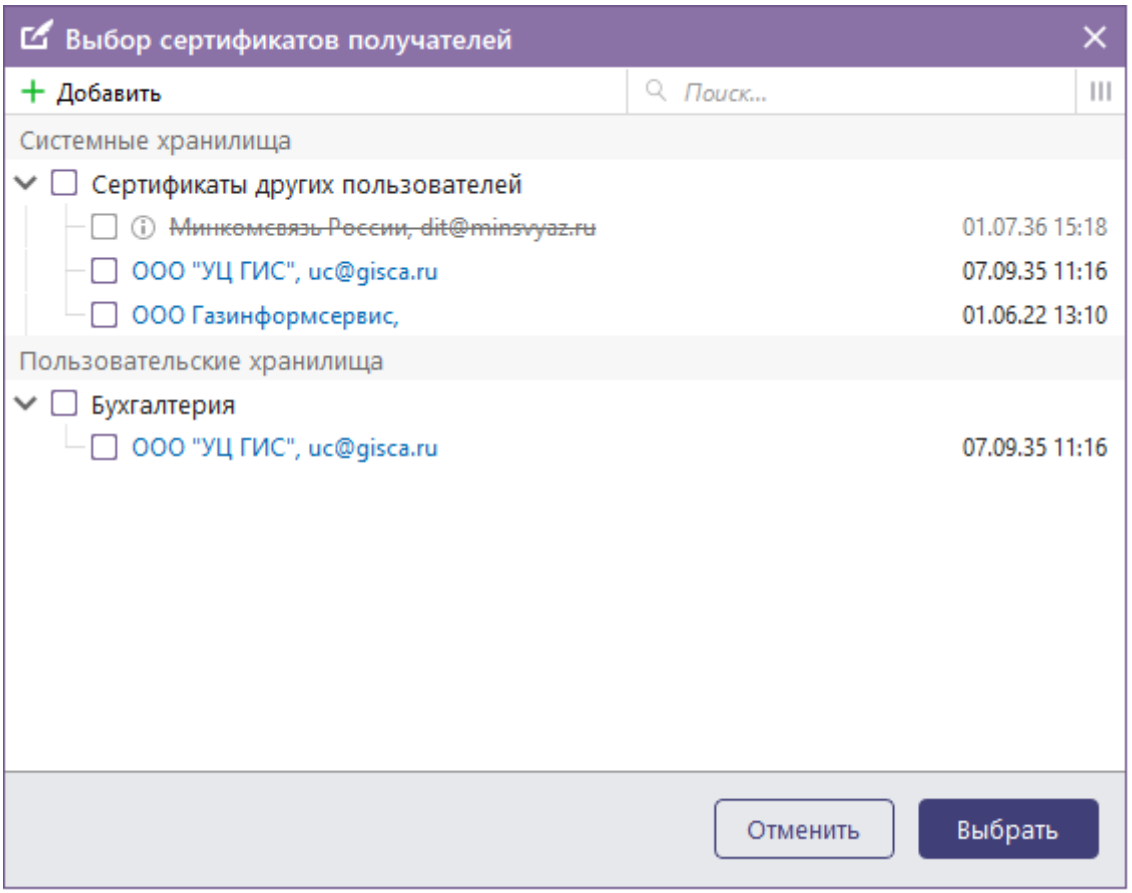


Рисунок 3.79 – Список сертификатов получателей

8 Если сертификата получателя нет в списке, нажмите на кнопку Добавить и в открывшемся окне укажите файл сертификата получателя, который необходимо добавить, нажмите на кнопку «*Открыть*».

9 Проверьте статус добавленного сертификата и при необходимости выполните его проверку.

10 Отметьте все сертификаты получателей, для которых хотите зашифровать файл, и нажмите на кнопку «*Выбрать*». В области «*Шифрование*» отобразится список сертификатов получателей (рисунок 3.80).

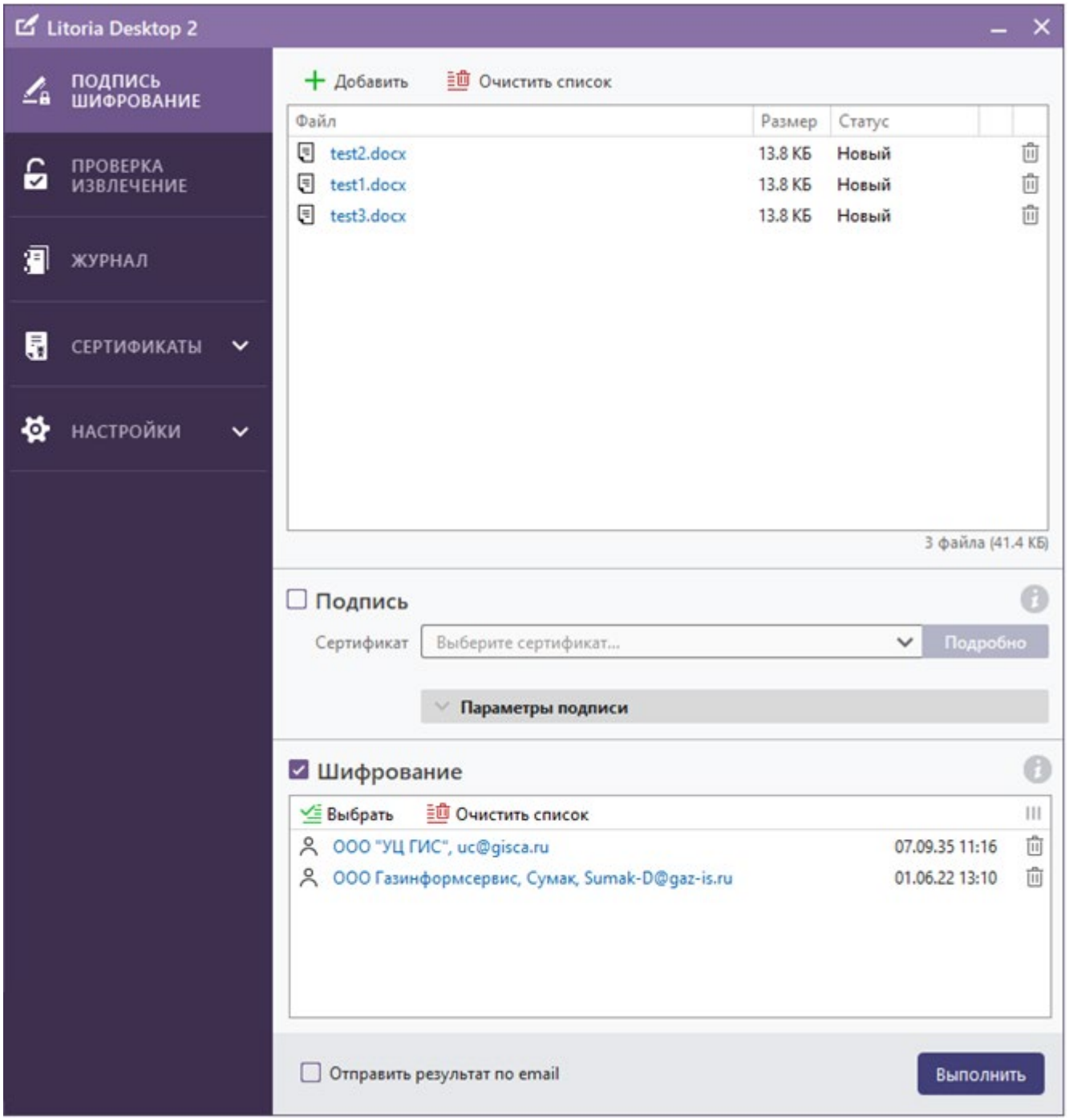


Рисунок 3.80 – Отображение сертификатов получателей в области «Шифрование»

11 Для удаления исходных файлов после выполнения операции установите в настройках флаг «*Удалять файлы после завершения операции шифрования*».

12 Нажмите на кнопку «*Выполнить*».

13 Если операция выполнилась успешно, статус документа в списке файлов поменяется на «*Выполнено*».

Результат: в текущем каталоге или в рабочей директории, которая указана в настройках, будет создан зашифрованный файл, обозначенный значком .

14 Просмотреть созданный зашифрованный файл в текущем каталоге или в рабочей директории, указанной в настройках, можно по кнопке « ».

3.8.1 Возможные сообщения об ошибках при шифровании документа

3.8.1.1 Сертификат не предназначен для шифрования документа

Если в сертификате установлен флаг «*Критическое значение*» для расширений «*Использование ключа*» (рисунок 3.7), то шифрование документов возможно только при наличии расширения *«Шифрование данных»*. Если критическое расширение *«Шифрование данных»* отсутствует, то сертификат в списке сертификатов получателей будет перечеркнут, при наведении курсора на пиктограмму появится сообщение о том, что данный сертификат не предназначен для шифрования данных (рисунок 3.81).

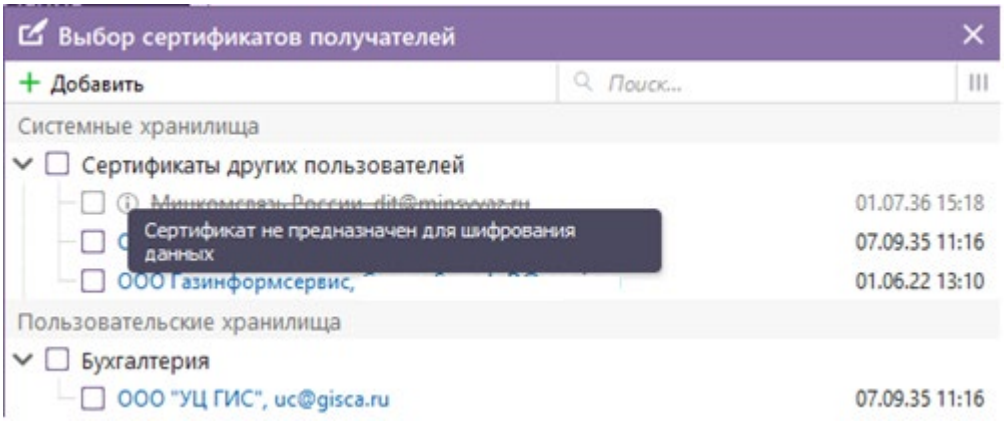


Рисунок 3.81 – Сертификат не предназначен для шифрования

При отсутствии установленного флага «*Критическое значение*» для расширений «*Использование ключа*», проверка наличия расширения *«Шифрование данных»* не осуществляется.

3.9 Подпись и шифрование файла

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

Для одновременного создания ЭП и шифрования файла выполните следующие действия:

1 Откройте интерфейс ПК «Litoria Desktop 2».
2 Выберите меню «*Подпись Шифрование*» (рисунок 3.63).
3 Поместите файлы, которые вы хотите подписать и зашифровать одновременно, в список файлов. Данную операцию можно выполнить несколькими способами:
– нажатием на кнопку «*Добавить*» и выбором необходимого файла в открывшемся

окне;

– перетаскиванием файла или папки из окна Проводника в область списка файлов;
– выбором в контекстном меню нужного файла *«Litoria Desktop 2»* → *«Подписать»* или *«Зашифровать»* (рисунки 3.64, 3.78).

При необходимости перед подписью и шифрованием добавленных файлов просмотрите их содержимое по щелчку мыши на имени файла в списке добавленных файлов.

4 Для одновременного создания ЭП и шифрования поставьте флаги «*Подпись*» и «*Шифрование*».

5 При использовании физического отчуждаемого носителя вставьте его в нужный разъем.

6 Для указания сертификата, которым вы хотите подписать файл, выберите сертификат из списка с вашими личными сертификатами в области «*Подпись*» в поле «*Сертификат*» (рисунок 3.82).

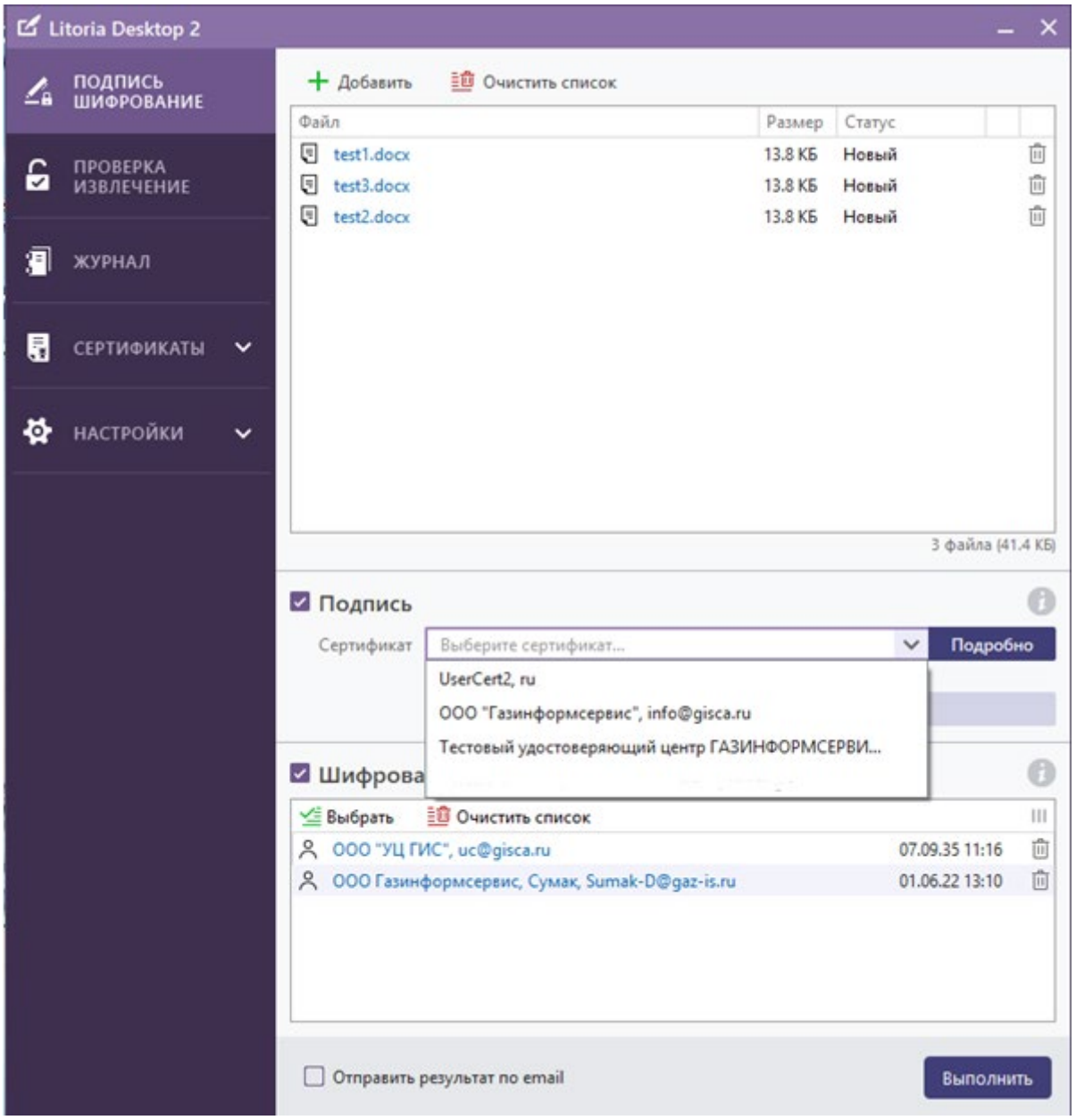


Рисунок 3.82 – Список сертификатов

7 Если данные указаны верно, внизу поля с выбранным сертификатом появится сообщение о сроке действия сертификата (рисунок 3.83). Сертификат готов к использованию.

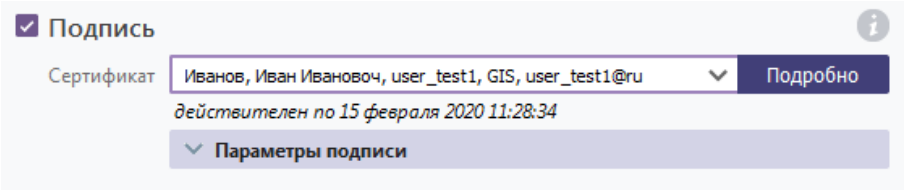


Рисунок 3.83 – Ключ ЭП найден

8 Установите параметры подписи. В таблице 3.2 указаны типы подписи и параметры,

установка которых необходима для их создания.

Таблица 3.2 – Типы и параметры подписи

Тип подписи	Параметры подписи в ПК «Litoria Desktop 2»	Примечание
Обычная совмещенная	–	Никакие флаги не надо устанавливать
Обычная совмещенная с меткой доверенного времени на значение ЭП	С меткой доверенного времени на значение ЭП	
С доказательством действительности сертификата совмещенная	С доказательством действительности сертификата	Флаг «С меткой доверенного времени на значение ЭП» установится автоматически

При одновременной операции подписи и шифрования документов нельзя создать отделенную подпись, поэтому параметр «*Создать отделенную подпись*» выключен.

В операции подписи и шифрования при создании ЭП с меткой доверенного времени или с доказательством действительности сертификата необходимо, чтобы в настройках ПК «Litoria Desktop 2» был задан корректный адрес службы штампов времени. Если на момент создания ЭП адрес не задан, появится сообщение с возможностью перехода к настройкам адреса службы штампов времени (рисунок 3.68).

9 Для выбора сертификата получателя нажмите на кнопку «*Выбрать*» в области «*Шифрование*».

10 Появится окно «*Выбор сертификатов получателей*» (рисунок 3.84) в котором будут отображены сертификаты хранилища «Сертификаты других пользователей» и сертификаты пользовательских хранилищ.

11 По щелчку мыши на наименовании выбранного сертификата, можно просмотреть его содержимое, путь сертификации и провести проверку сертификата (см. пункт 3.3.5).

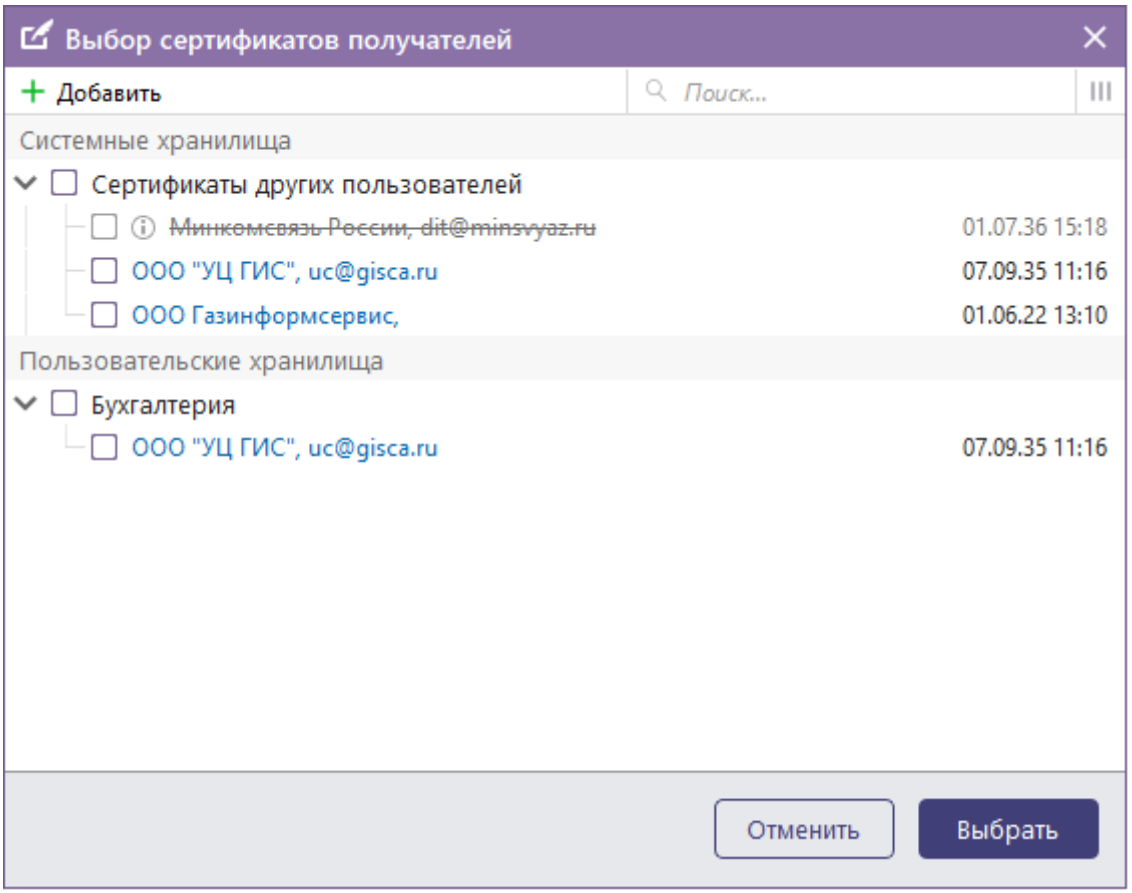


Рисунок 3.84 – Список сертификатов получателей

12 Если сертификата получателя нет в списке, нажмите на кнопку + Добавить и в открывшемся окне укажите файл сертификата получателя, который необходимо добавить, нажмите на кнопку «*Открыть*».

13 Проверьте статус добавленного сертификата и при необходимости выполните его проверку.

14 Отметьте все сертификаты получателей, для которых хотите зашифровать файл, и нажмите на кнопку «*Выбрать*». В области «*Шифрование*» отобразится список сертификатов получателей (рисунок 3.85).

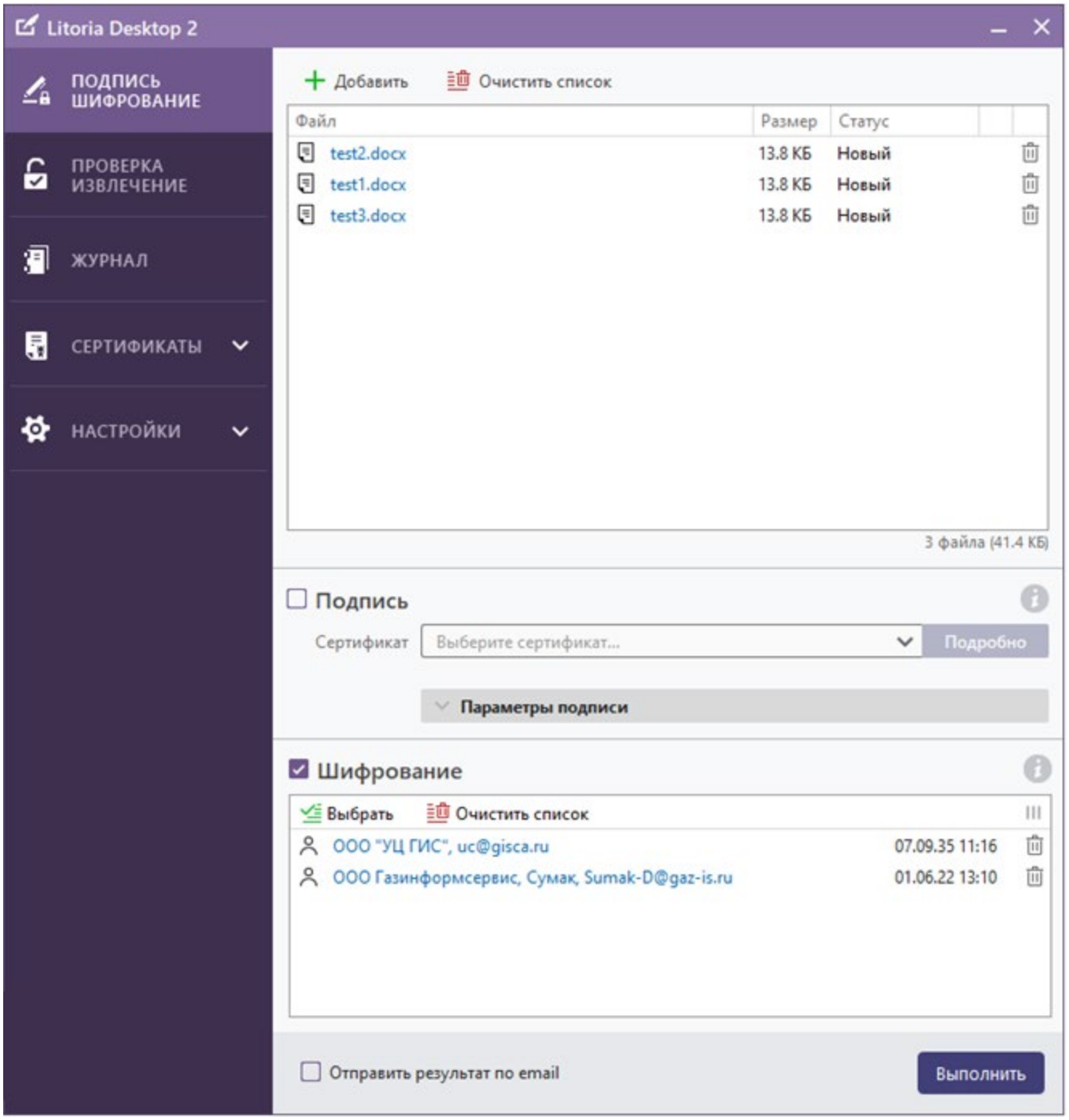


Рисунок 3.85 – Отображение сертификатов получателей в области «*Шифрование*»

15 Для удаления исходных файлов после выполнения операции установите в настройках флаг «*Удалять файлы после завершения операции шифрования*».

16 Нажмите на кнопку «*Выполнить*».

17 Если операция выполнилась успешно, статус документа в списке файлов поменяется на «*Выполнено*».

Результат: в текущем каталоге или в рабочей директории, которая указана в настройках, будет создан подписанный и зашифрованный файл, обозначенный значком .

Просмотреть созданный зашифрованный файл в текущем каталоге или в рабочей директории, указанной в настройках, можно по кнопке « ».

Возможные сообщения об ошибках при выполнении комплексной операции подписи и шифрования файла описаны в разделах **3.6.1 «Возможные сообщения об ошибках при подписи документа»** и **3.8.1 «Возможные сообщения об ошибках при шифровании документа».**

3.10 Проверка ЭП

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

- принадлежность электронной подписи 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 или создания ЭП при наличии в ЭП доказательств, определяющих этот момент.

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

ПК «Litoria Desktop 2» позволяет использовать службу доверенной третьей стороны для проверки ЭП в электронном документе. Настройка службы доверенной третьей стороны доступна пользователю только после включения администратором дополнительных параметров безопасности и установки флага *«Использовать службу для проверки подписи»* в области *«Служба доверенной третьей стороны»* (пункт **3.4.2.2 «Настройки службы доверенной третьей стороны»)**.

Для проверки ЭП выполните следующие действия:

1 Откройте интерфейс ПК «Litoria Desktop 2»
2 Выберите меню «*Проверка Извлечение*» (рисунок 3.86).

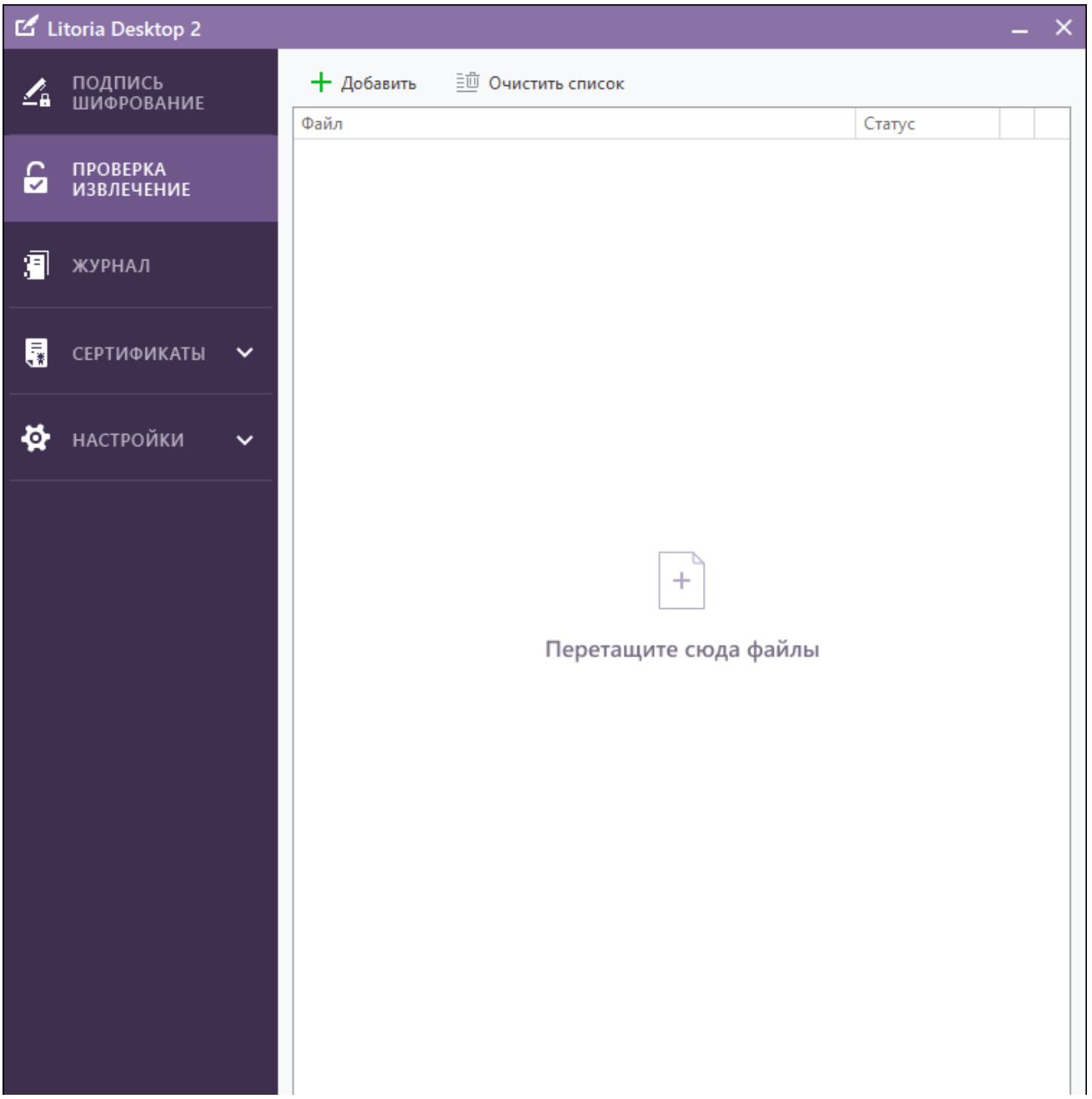


Рисунок 3.86 – Проверка подписи документов

3 Поместите ранее подписанные файлы, которые вы хотите проверить, в список файлов. Данную операцию можно выполнить несколькими способами:

– нажатием на кнопку «*Добавить*» и выбором необходимого файла в открывшемся окне;
– перетаскиванием файла или папки из окна Проводника в область списка файлов;
– выбором в контекстном меню нужного файла *«Litoria Desktop 2»* → *«Проверить подпись»* (рисунок 3.87).

Рисунок 3.87 – Проверка подписи документов через контекстное меню

4 Проверка файла осуществляется автоматически при добавлении файла в список.

5 Если операция выполнилась успешно, статус документа в списке поменяется на «*Действительна/Недействительна*» в зависимости от результатов проверки (рисунок 3.88).

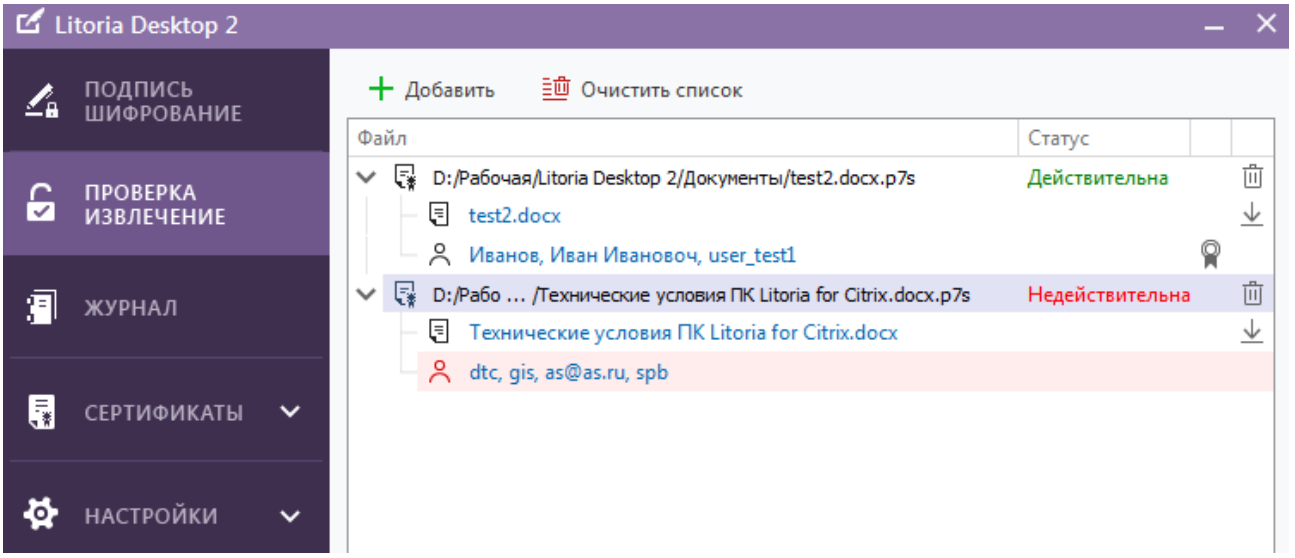


Рисунок 3.88 – Успешное выполнение операции

6 Просмотреть содержимое исходного файла можно по щелчку мыши на наименовании файла в списке добавляемых файлов.

7 Для сохранения исходного файла (для совмещенной подписи) нажмите на кнопку «⭳».

8 В открывшемся окне «*Выберите файл для сохранения данных*» (рисунок 3.89) укажите путь и имя файла и нажмите на кнопку «*Сохранить*».

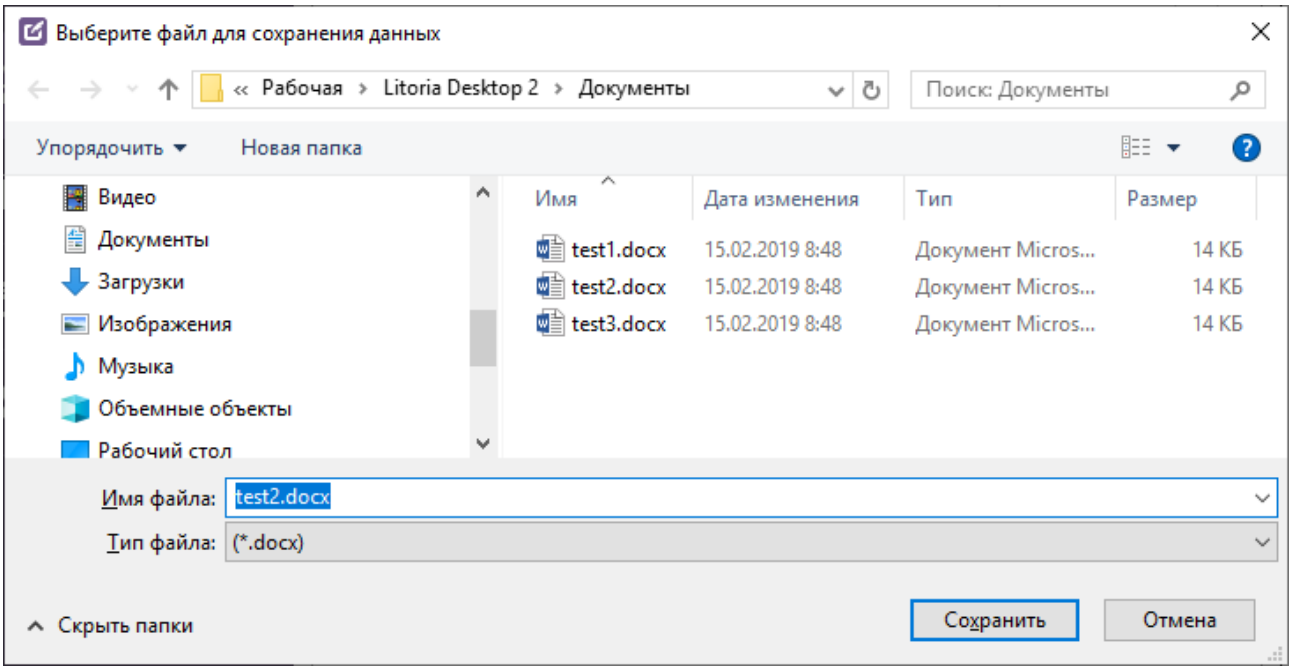


Рисунок 3.89 – Сохранение исходного файла

9 В указанном каталоге появится исходный файл.

10 Список подписей, содержащихся в проверяемом файле, доступен для просмотра в списке проверяемых файлов (рисунок 3.88).

3.10.1 Возможные сообщения об ошибках при проверке подписи

3.10.1.1 Сертификат не предназначен для цифровой подписи

При попытке выполнить проверку документа, который был подписан с помощью сертификата, не предназначенного для подписи, в строке статуса проверяемого файла отобразится статус «Недействительна» (рисунок 3.90).

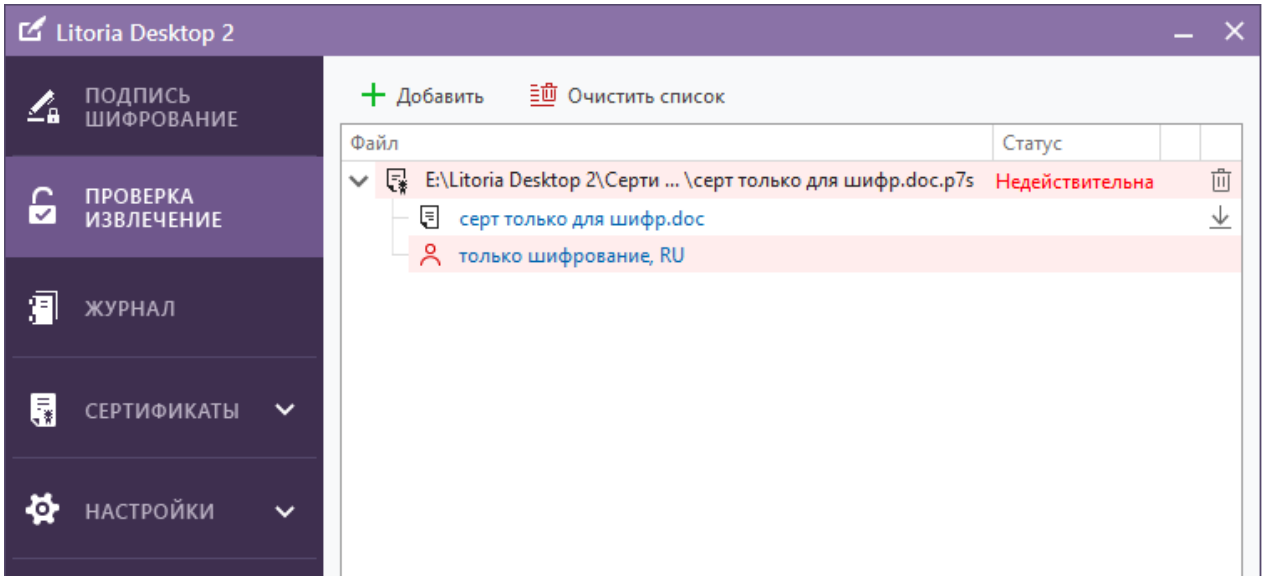


Рисунок 3.90 – Результат проверки подписи «Недействительна»

По щелчку мыши на имя сертификата можно посмотреть по какой причине подпись является недействительной. В случае если сертификат не предназначен для подписи, в окне отображается «Сертификат не предназначен для подписи данных» (рисунок 3.91)

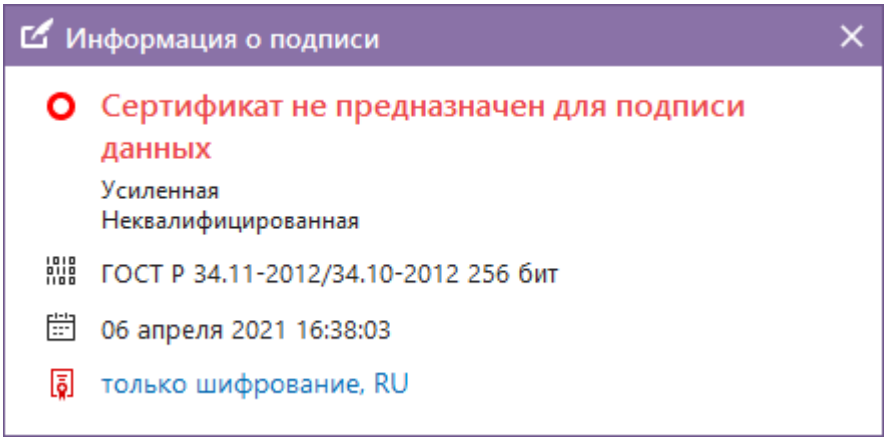


Рисунок 3.91 – Просмотр статуса проверенной подписи

3.10.1.2 Ошибка при добавлении файла на проверку

Ошибка вида *«Файлы не добавлены, так как они не подписаны и не зашифрованы»* (рисунок 3.92), отображается при попытке добавить на проверку документ в неверном формате:

- pdf-документ, добавляемый на проверку, имеет в расширении файла «*pdf*» пробелы или другие дополнительные символы;

- добавляемый документ действительно не содержит ЭП и/или не является зашифрованным файлом;

- на проверку добавляется подписанный pdf-документ, но при этом в основных настройках отсутствует разрешение проверки подписи pdf-документа по стандарту PAdES (не установлен флаг *«Создавать и проверять подпись pdf документов по стандарту PAdES»*).

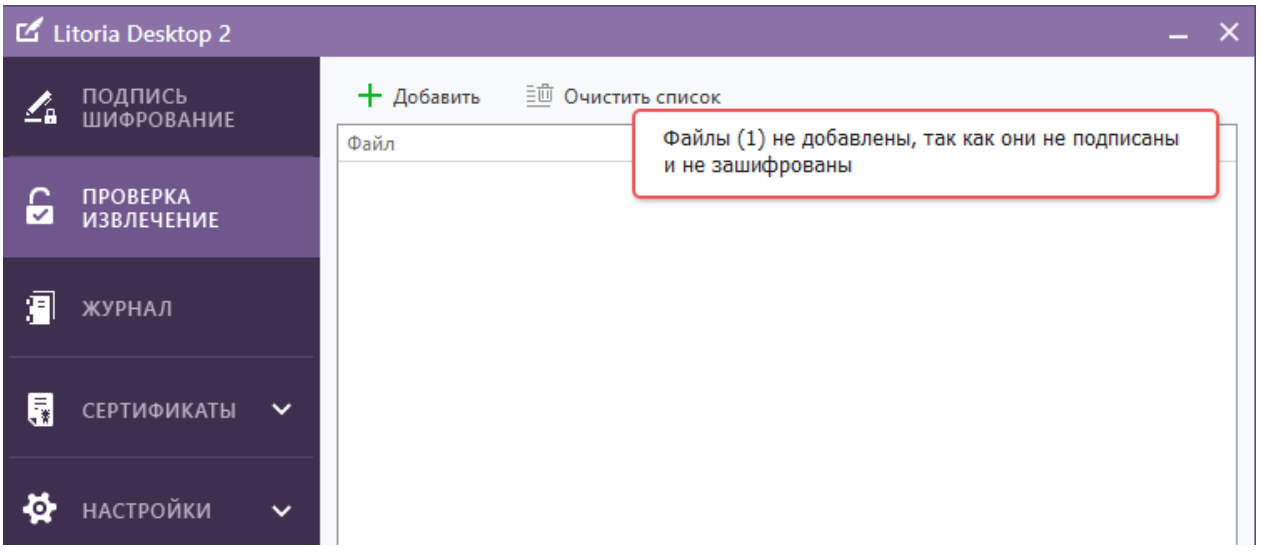


Рисунок 3.92 – Ошибка при добавлении файлов на проверку

3.10.1.3 Отсутствие прав доступа к файлу

При попытке добавления на проверку файла, в свойствах которого установлен запрет на доступ для конкретного пользователя или для группы, в которую входит пользователь, файл не будет добавлен в список проверяемых и отобразится ошибка вида «*Файлы не добавлены, так как к ним отсутствует доступ*» (рисунок 3.93).

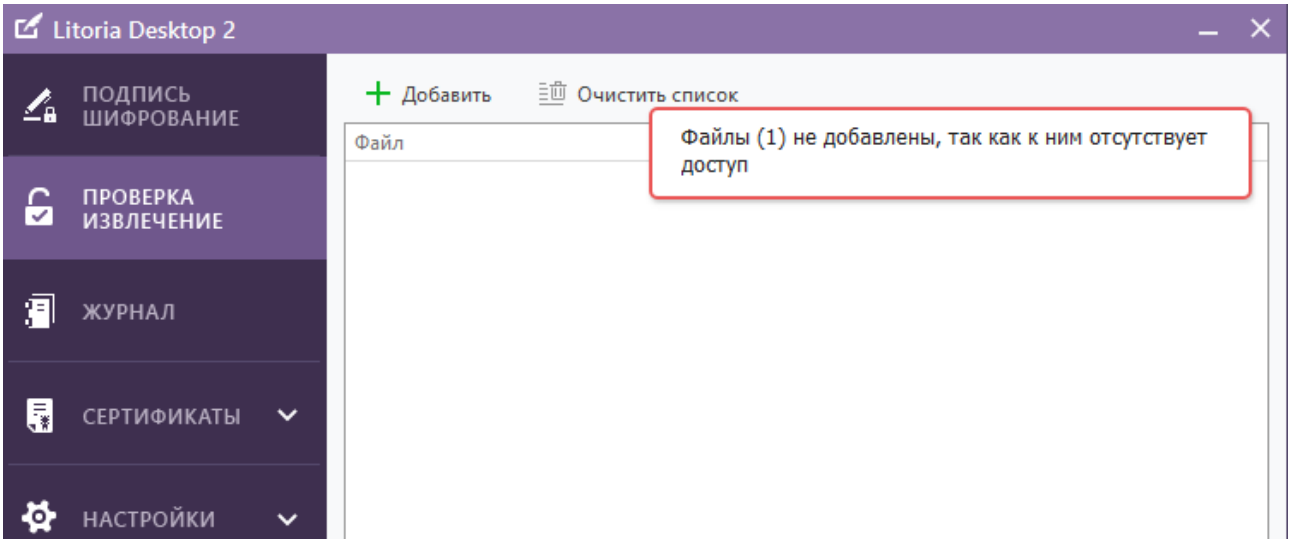


Рисунок 3.93 – Отсутствие прав доступа к файлу

3.11 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.

Для заверения своей подписью ранее подписанного документа выполните следующие действия:

1 Откройте интерфейс ПК «Litoria Desktop 2»
2 Выберите меню «*Проверка Извлечение*» (рисунок 3.86).
3 Поместите ранее подписанные файлы, которые вы хотите проверить, в список файлов. Данную операцию можно выполнить несколькими способами:
   – нажатием на кнопку «*Добавить*» и выбором необходимого файла в открывшемся окне;
   – перетаскиванием файла или папки из окна Проводника в область списка файлов;
   – выбором в контекстном меню нужного файла *«Litoria Desktop 2»* → *«Проверить подпись»* (рисунок 3.87).
4 Проверка и извлечение файла осуществляется автоматически при добавлении файла в список.
5 Если операция выполнилась успешно, статус документа в списке поменяется на «*Действительна/Недействительна*» в зависимости от результатов проверки (рисунок 3.88).
6 Добавление заверяющей подписи возможно только в документ со статусом «*Действительна*».
7 При использовании физического отчуждаемого носителя вставьте его в нужный разъем.
8 Нажмите на кнопку « » в строке с подписью, которую необходимо заверить.
9 Появится окно «*Заверение подписи*» (рисунок 3.94). В появившемся окне выберите сертификат из списка с вашими личными сертификатами в поле «*Сертификат*». Просмотреть статус сертификата, его содержимое, путь сертификации, провести его проверку (см. пункт 3.3.5) можно по кнопке «*Подробно*».

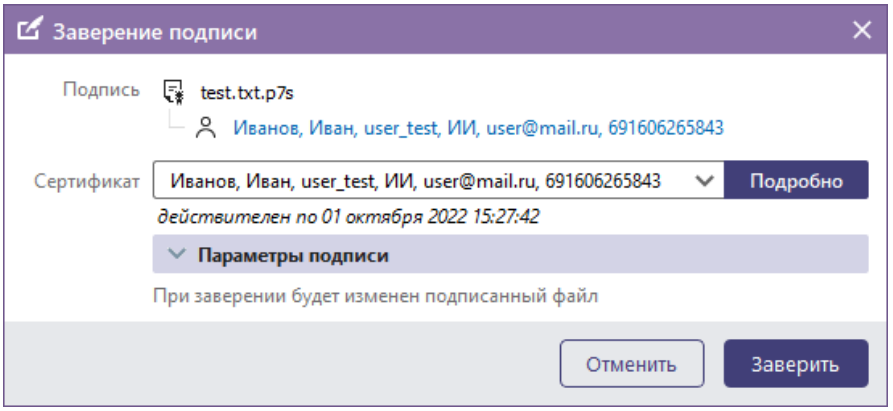


Рисунок 3.94 – Выбор сертификата для заверения подписи

10 Если данные указаны верно, внизу поля с выбранным сертификатом появится сообщение о сроке действия сертификата (рисунок 3.63). Сертификат готов к использованию.

11 После выбора сертификата установите параметры подписи (таблица 3.1) и при необходимости напишите комментарий к заверяющей подписи в соответствующем поле.

Нельзя установить параметр *«Отдельным файлом»*, поскольку комплекс определяет автоматически параметр заверения отделенной или присоединенной подписи (на основе вида подписей, созданных ранее).

При заверении ЭП с меткой доверенного времени или с доказательством действительности сертификата необходимо, чтобы в настройках ПК «Litoria Desktop 2» был задан корректный адрес службы штампов времени. Если на момент операции заверения ЭП адрес не задан, появится сообщение с возможностью перехода к настройкам адреса службы штампов времени (рисунок 3.95).

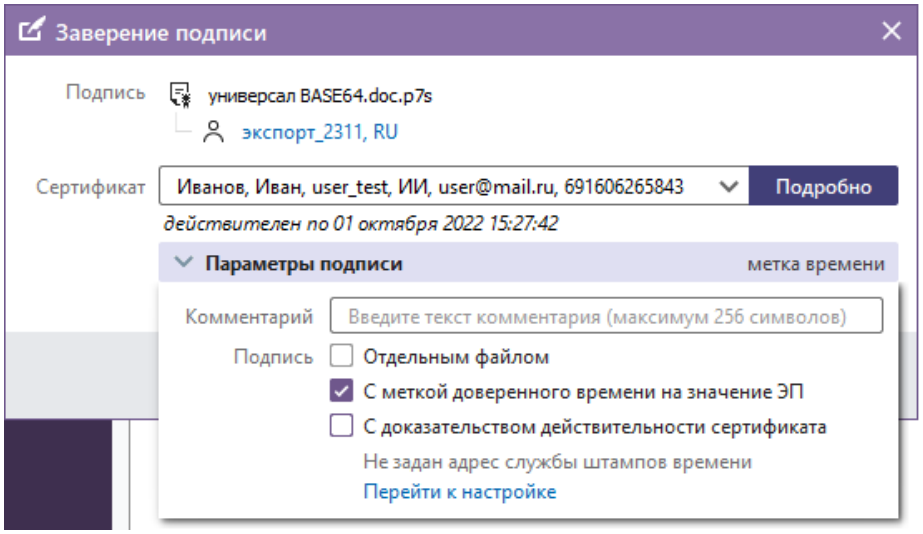


Рисунок 3.95 – Переход к настройке адреса службы штампов времени

12 Нажмите на кнопку «*Заверить*».

13 Если операция выполнилась успешно, то в списке проверяемых файлов появится заверяющая подпись к существующей подписи у соответствующего файла (рисунок 3.96).

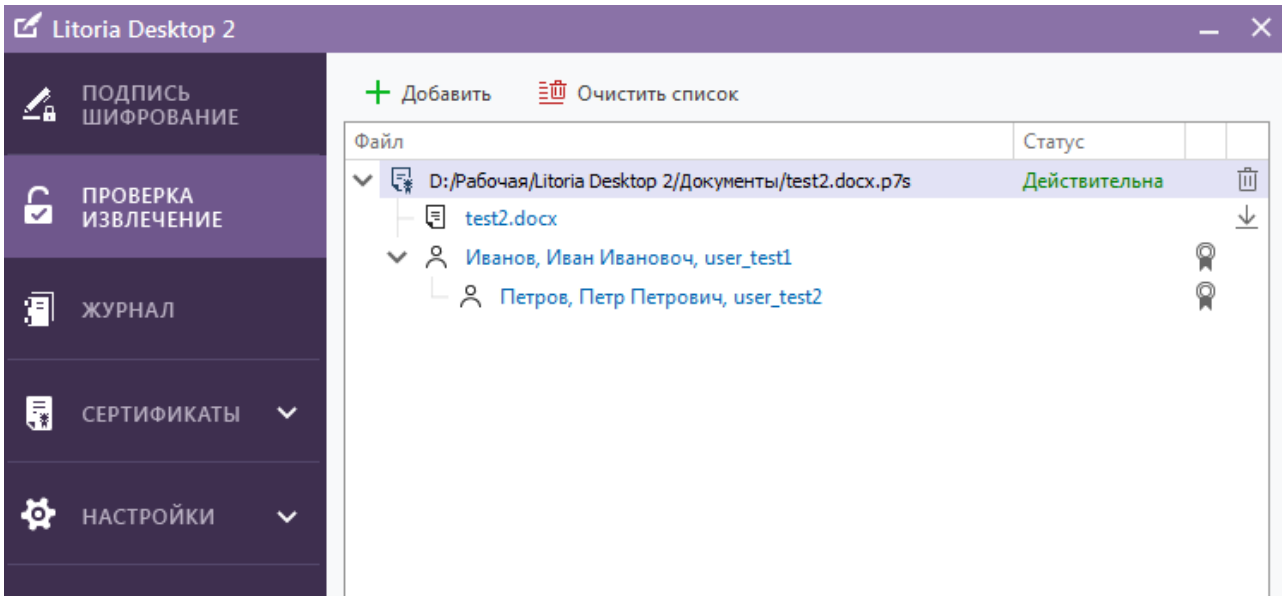


Рисунок 3.96 – Просмотр заверяющей подписи

14 Для заверения еще одной подписи в этом файле выполните действия, описанные в п. 15.

15 Для заверения подписи в другом проверяемом файле выполните действия, указанные в п.1 – п.13.

Результат: в текущем каталоге или в рабочей директории, которая указана в настройках, будет создан файл, содержащий заверенные подписи и обозначенный значком .

Заверение pdf-документов стандарта PAdES не осуществляется

Возможные сообщения об ошибках при выполнении операции заверения подписи описаны в пункте **3.6.1 «Возможные сообщения об ошибках при подписи документа».**

3.12 Извлечение файла

При получении зашифрованного документа извлечение пройдет успешно при наличии 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.

Для извлечения файла выполните следующие действия:

1 Откройте интерфейс ПК «Litoria Desktop 2».

2 Выберите меню «*Проверка Извлечение*» (рисунок 3.85).

3 Поместите файлы, которые вы хотите расшифровать, в список файлов. Данную операцию можно выполнить несколькими способами:

– нажатием на кнопку «*Добавить*» и выбором необходимого файла в открывшемся окне;

– перетаскиванием файла или папки из окна Проводника в область списка файлов;

– выбором в контекстном меню нужного файла *«Litoria Desktop 2»* → *«Расшифровать»* (рисунок 3.97).

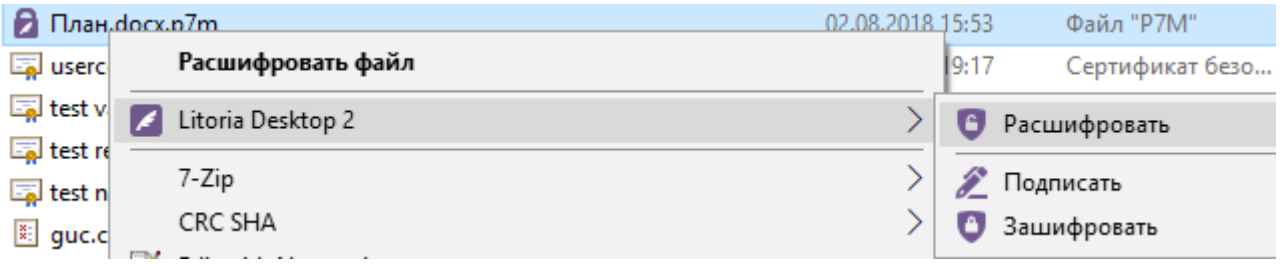


Рисунок 3.97 – Извлечение файла через контекстное меню

4 При использовании физического отчуждаемого носителя для извлечения вставьте его в нужный разъем.

5 При необходимости ввода ключа, нажмите на кнопку «🔗» в строке с извлекаемым файлом (рисунок 3.98).

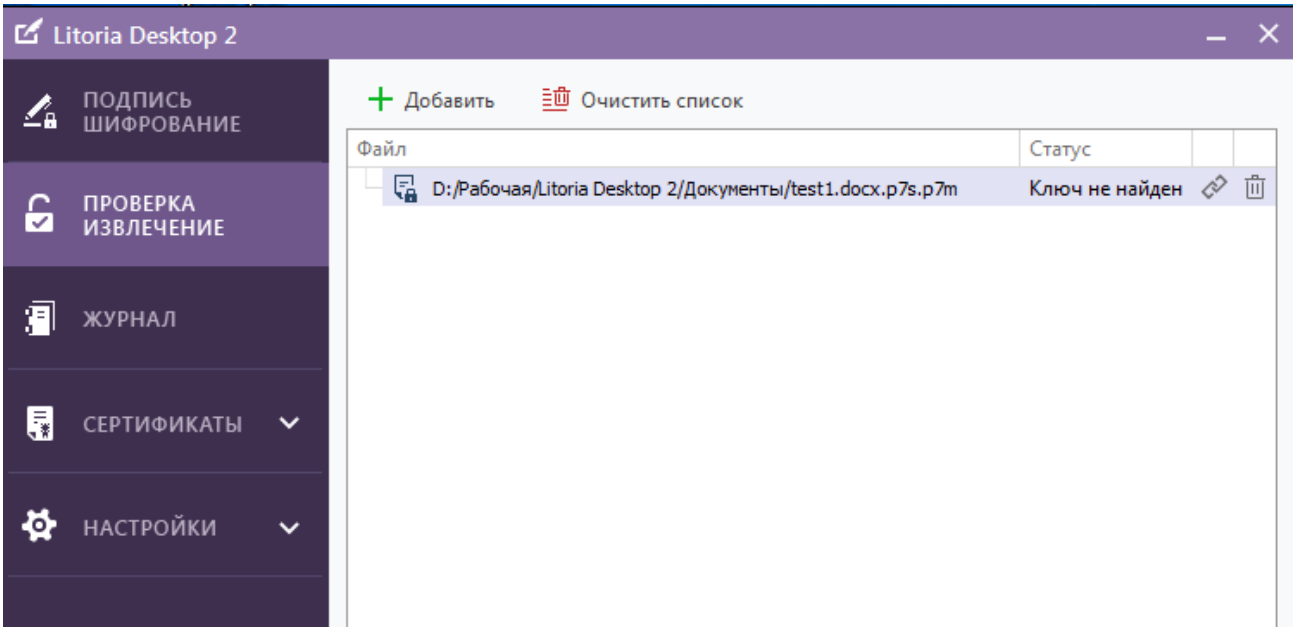


Рисунок 3.98 – Извлечение файла

6 Появится окно (рисунок 3.99) со списком сертификатов, содержащихся в зашифрованном файле.

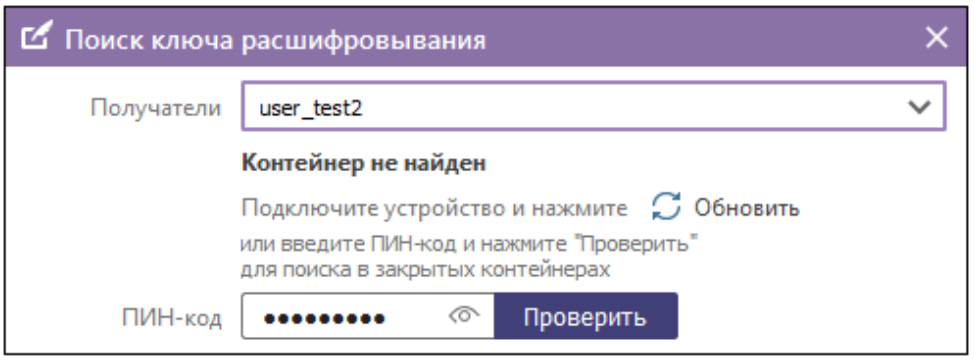


Рисунок 3.99 – Сертификаты в зашифрованном файле

7 Выберите сертификат, на котором выполняется операция извлечения файла в поле «*Получатели*» и в поле «*ПИН-код*» введите ПИН-код для контейнера, в котором содержится ключ ЭП к сертификату. Нажмите на кнопку «*Проверить*».

8 Если операция выполнилась успешно, то статус в списке извлекаемых файлов поменяется на «*Расшифрован*» (рисунок 3.100).

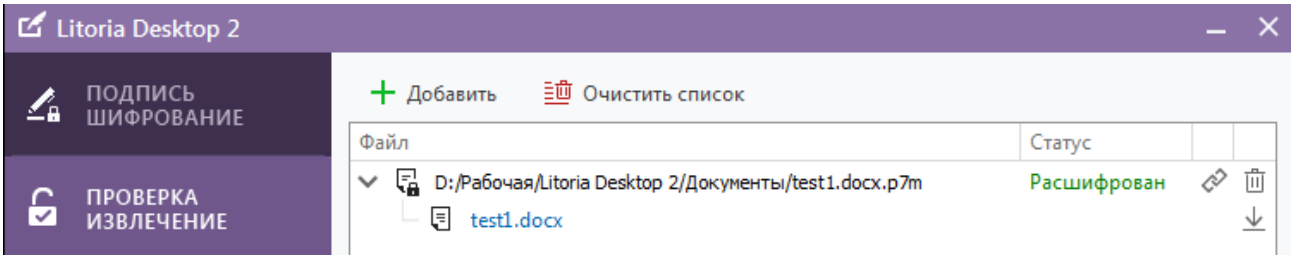


Рисунок 3.100 – Успешное выполнение извлечения файла

9 Просмотреть содержимое расшифрованного файла можно по щелчку мыши на наименовании файла в списке извлекаемых файлов.

10 Для сохранения файла нажмите на кнопку «».

11 В открывшемся окне «*Выберите файл для сохранения данных*» (рисунок 3.101) укажите путь и имя файла и нажмите на кнопку «*Сохранить*».

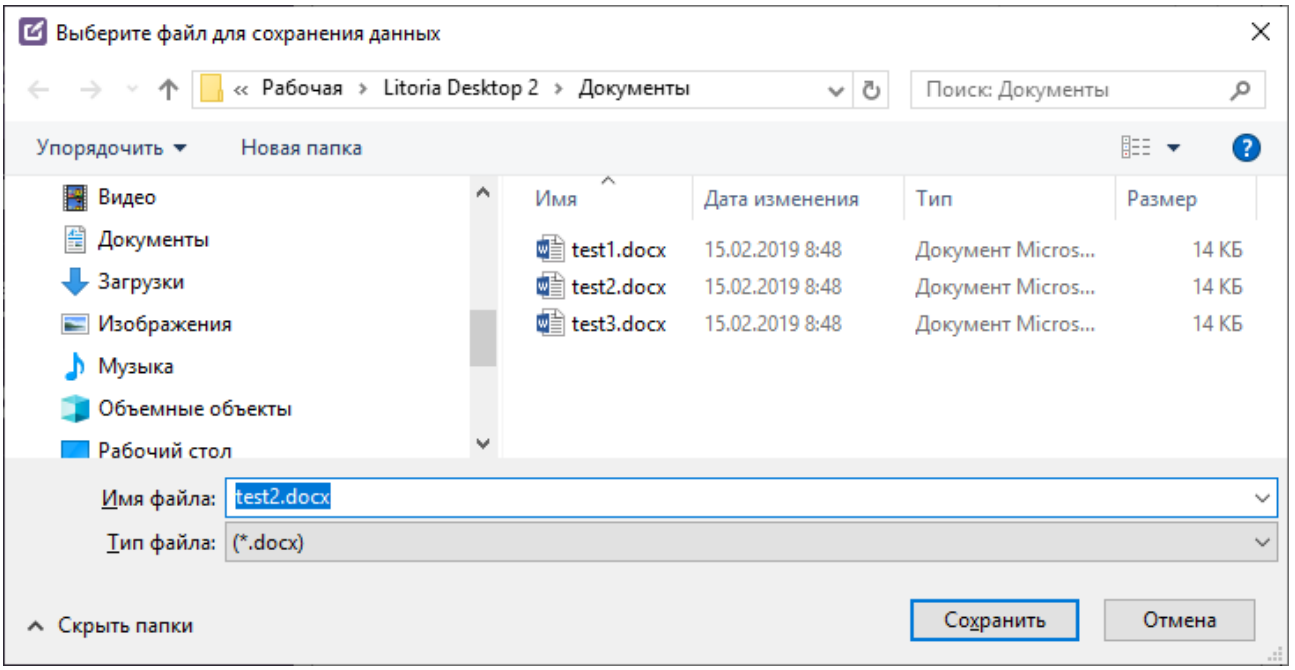


Рисунок 3.101 – Сохранение исходного файла

12 В указанном каталоге появится извлеченный файл.

3.12.1 Возможные сообщения об ошибках при извлечении файла

3.12.1.1 Сертификат не предназначен для расшифровывания документа

Если в сертификате установлен флаг «*Критическое значение*» для расширений «*Использование ключа*» (рисунок 3.7), то расшифровывание документов возможно только при наличии расширения *«Шифрование данных»*.

При попытке расшифровать документ, с помощью сертификата, не предназначенного для расшифровывания (рисунок 3.97), и нажатии на кнопку «🔗» для ввода ключа в строке с извлекаемым файлом появится предупреждение о невозможности использования данного сертификата для расшифровывания (рисунок 3.102).

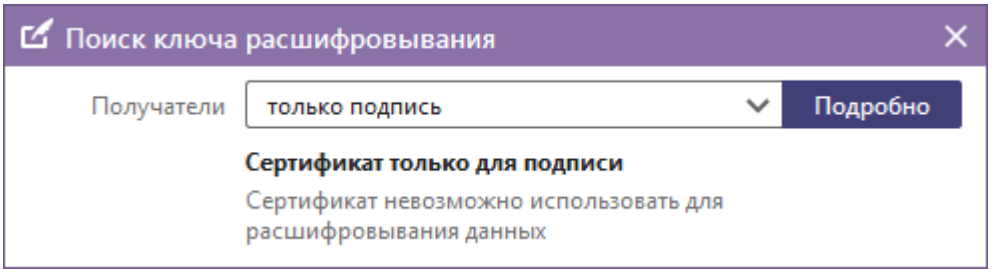


Рисунок 3.102 – Сертификат не предназначен для расшифровывания

3.13 Извлечение файла и проверка ЭП

Данная операция выполняется в два этапа: вначале выполняется извлечение, потом

проверка ЭП.

После извлечения файла и проверки ЭП 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.

Для одновременного извлечения файла и проверки ЭП выполните следующие действия:

1 Откройте интерфейс ПК «Litoria Desktop 2».
2 Выберите меню «*Проверка Извлечение*» (рисунок 3.103).

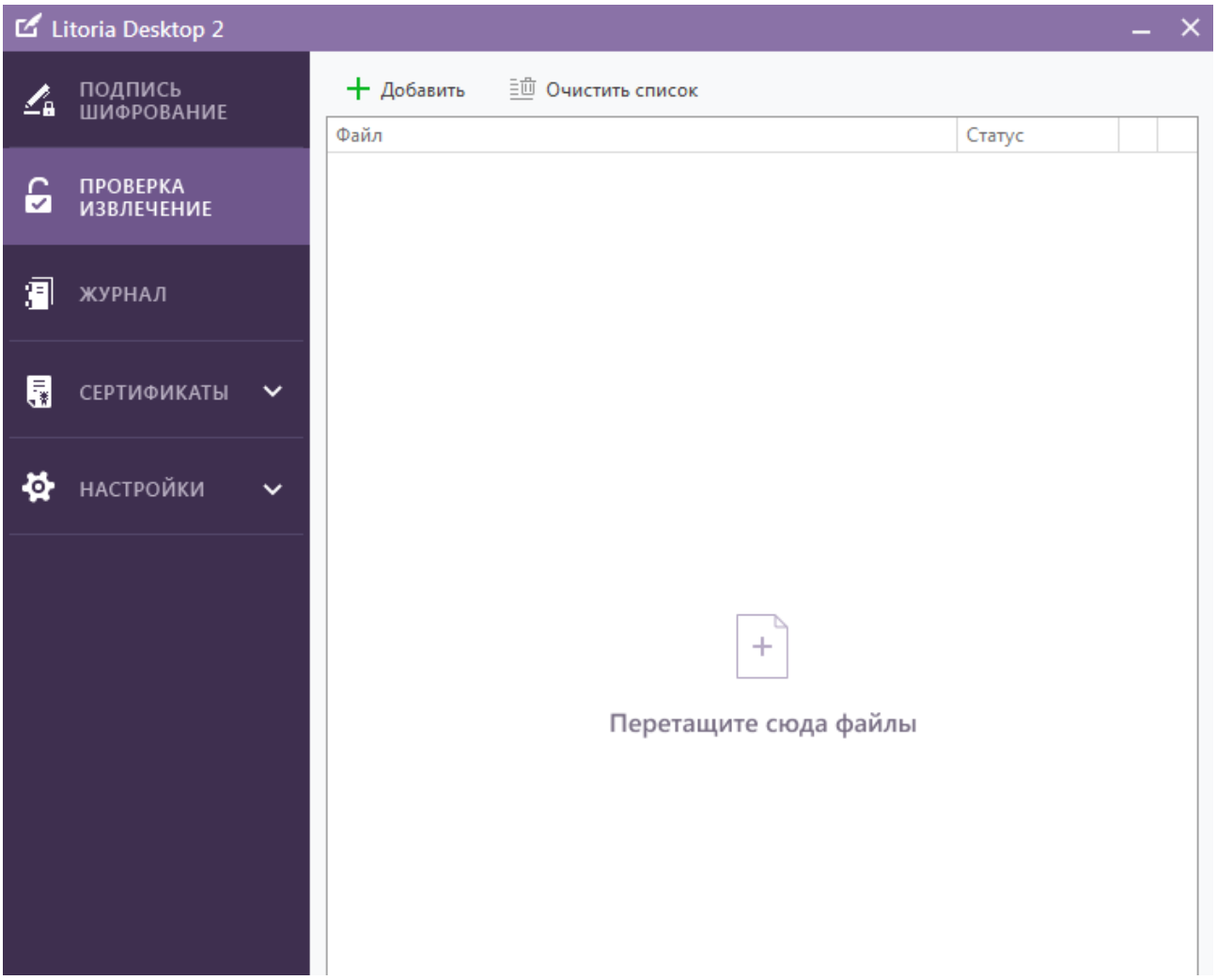


Рисунок 3.103 – Проверка подписи документов

3 Поместите файлы, которые вы хотите расшифровать и проверить их подпись одновременно, в список файлов. Данную операцию можно выполнить несколькими способами:
   – нажатием на кнопку «*Добавить*» и выбором необходимого файла в открывшемся окне;

– перетаскиванием файла или папки из окна Проводника в область списка файлов;
– выбором в контекстном меню нужного файла *«Litoria Desktop 2»* → *«Проверить подпись»* или *«Расшифровать»* (рисунки 3.87, 3.97)

4 При использовании физического отчуждаемого носителя для расшифровывания вставьте его в нужный разъем.

5 При необходимости ввода ключа, нажмите на кнопку «🔗» в строке с извлекаемым файлом (рисунок 3.104).

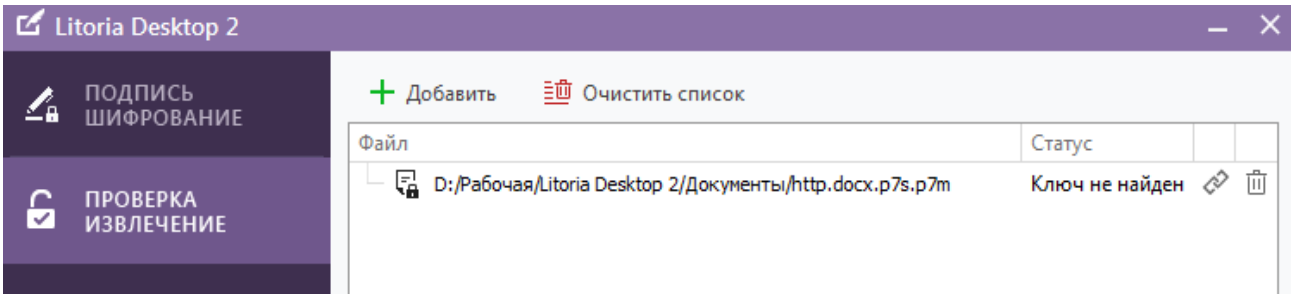


Рисунок 3.104 – Извлечение и проверка ЭП файла

6 Появится окно (рисунок 3.105) со списком сертификатов, содержащихся в зашифрованном файле.

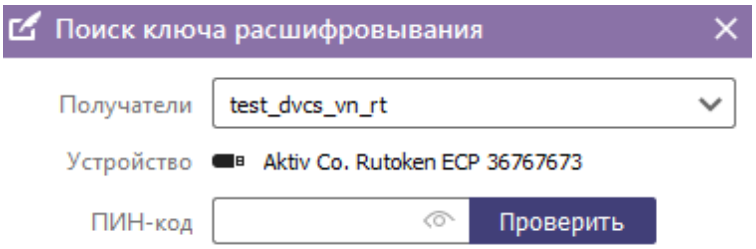


Рисунок 3.105 – Сертификаты в зашифрованном файле

7 Выберите сертификат, на котором выполняется операция извлечения файла в поле «*Получатели*», и в поле «*ПИН-код*» введите ПИН-код для контейнера, в котором содержится ключ ЭП к сертификату. Нажмите на кнопку «*Проверить*».

8 Если операция выполнилась успешно, то статус в списке извлекаемых файлов поменяется на «*Расшифрован*» и «*Действительна/Недействительна*» в зависимости от результатов проверки (рисунок 3.106).

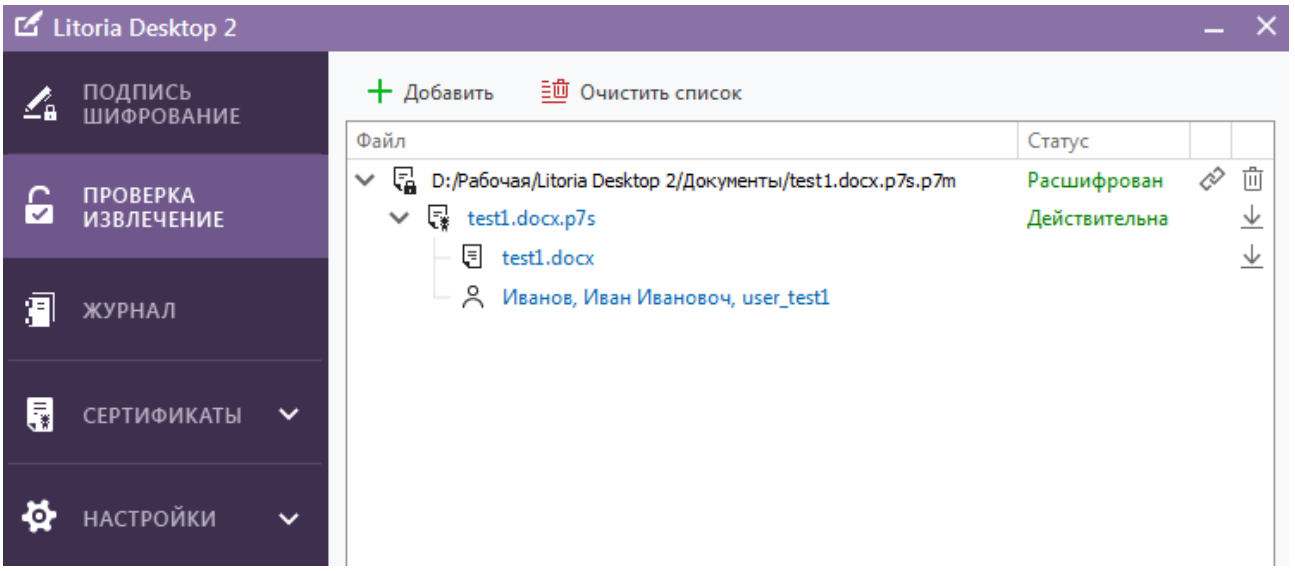


Рисунок 3.106 – Извлеченные и проверенные файлы

9 Просмотреть содержимое расшифрованного файла можно по щелчку мыши на наименовании файла в списке извлекаемых файлов.

10 Для сохранения файла нажмите на кнопку «».

11 В открывшемся окне «*Выберите файл для сохранения данных*» укажите путь и имя файла и нажмите на кнопку «*Сохранить*». В указанном каталоге появится извлеченный файл.

12 Список подписей, содержащихся в проверяемом файле, доступен для просмотра в списке извлеченных и проверенных файлов (рисунок 3.106).

3.14 Продление подписи электронного документа

Если срок действия подписи в проверяемом файле подходит к концу, статус подписи в списке проверяемых файлов примет значение «*Истекает*» (рисунок 3.107). Количество дней, за которое выдается предупреждение об истечении срока действия подписи задается администратором в настройках ПК. По умолчанию предупреждение об истечении срока действия ЭП выдается за 30 дней до ее истечения.

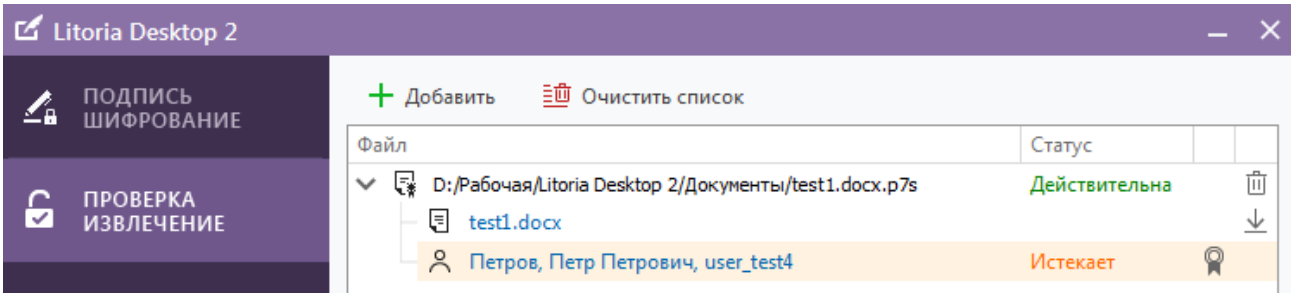


Рисунок 3.107 – Подпись со статусом «*Истекает*»

Если администратором установлен флаг «*Включить продление срока действия ЭП*» в

настройках комплекса, пользователю станет доступно продление срока действия ЭП. Подробнее описано в документе «ПК «Litoria Desktop 2. Руководство администратора».

Для продления подписи необходимо раскрыть информацию о подписи и выполнить следующие действия:

1 Для просмотра информации о подписи раскройте ее щелчком мыши.

2 В появившемся окне (рисунок 3.108) отображается информация о подписи: имя владельца и другие данные о владельце, комментарий к подписи, время создания, тип подписи, наличие данных в подписи, наличие метки доверенного времени и информация о ней, оттиск подписи и результат проверки этой подписи. Если в файле находится несколько подписей, то для каждой из них можно просмотреть информацию. Нажав на ссылку с именем владельца подписи, можно просмотреть дополнительную информацию, такую как статус сертификата подписчика и все сведения об этом сертификате.

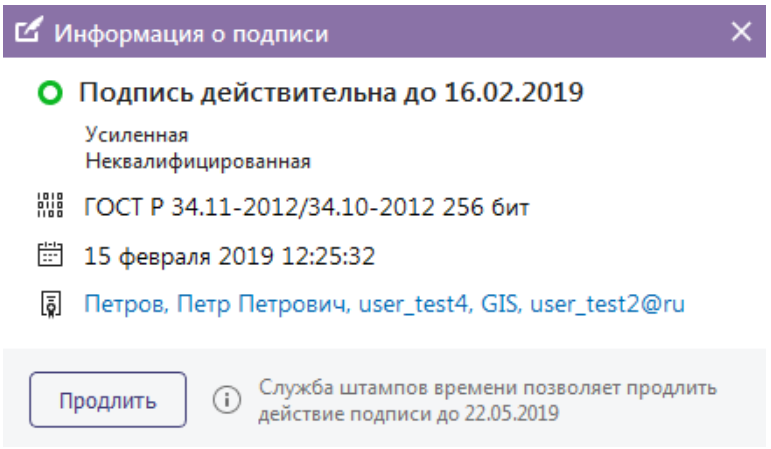


Рисунок 3.108 – Просмотр подписи

3 В окне просмотра подписи (рисунок 3.108) отображается информация о сроке действия подписи с возможностью его продления по кнопке «*Продлить*».

Продление подписи электронного документа при использовании аппаратного криптопровайдера pkcs#11 возможно только при наличии установленного средства криптографической защиты информации «КриптоПро CSP».

Время продления действия подписи рассчитывается в зависимости от используемой в подписанном файле ЭП:

– при подписи документа обычной подписью, т.е. в подпись не включены доказательства действительности сертификата, время действия подписи при продлении увеличивается до срока действия сертификата штампа времени;

– при подписи документа ЭП с доказательством действительности сертификата (в

подпись включены доказательства действительности сертификата и информация о времени создания подписи), время действия подписи увеличивается до срока действия сертификата архивной метки доверенного времени.

3.15 Недостаточно места для работы комплекса

Если при выполнении операций создания/добавления ЭП или шифровании документа недостаточно места на компьютере при нажатии на кнопку «Выполнить» появится сообщение об ошибке (рисунок 3.109).

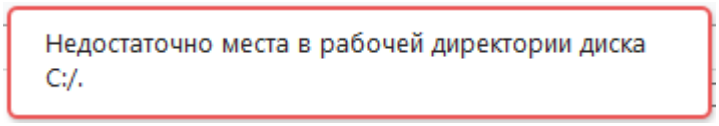
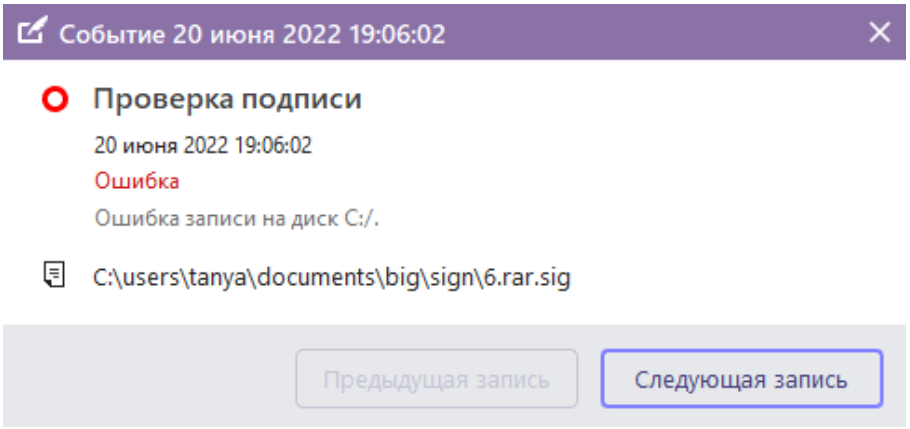
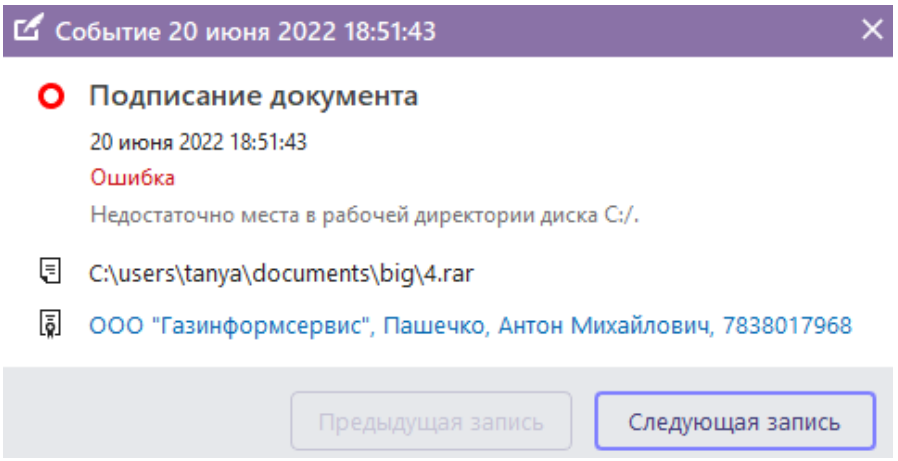


Рисунок 3.109 – Недостаточно места в рабочей директории

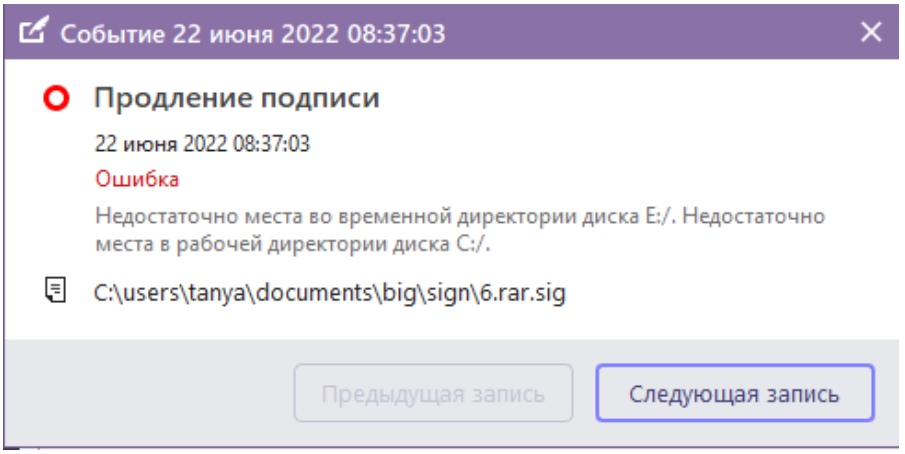
Если место на компьютере закончилось во время выполнения операций (создания/добавления ЭП, шифрования/проверки документа или продления подписи), то в строке напротив файла отобразится статус «Ошибка» и в журнале по щелчку на событии будет доступна подробная информация по событию (рисунок 3.110 а, б, в).



а)



б)



в)

Рисунок 3.110 – Ошибки при недостатке места на компьютере

Если нехватка места для корректной работы комплекса была обнаружена до запуска ПК «Litoria Desktop 2», при запуске комплекса появится сообщение об ошибке (рисунок 3.111). Данное сообщение будет появляться раз в минуту до момента закрытия комплекса и решения описанной проблемы.

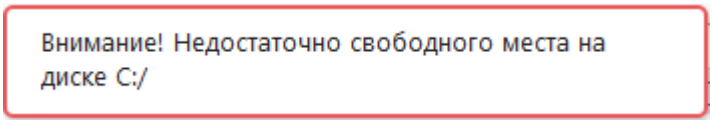


Рисунок 3.111 – Недостаточно места на диске C:/ для работы комплекса

Если при добавлении файлов на выполнении операций создания/добавления ЭП или шифровании документа недостаточно места в рабочей директории, определённой в основных настройках, внизу области добавления файлов появится сообщение об ошибке с возможностью перехода по ссылке *«Перейти к настройке»* для изменения рабочей директории (рисунок 3.112).

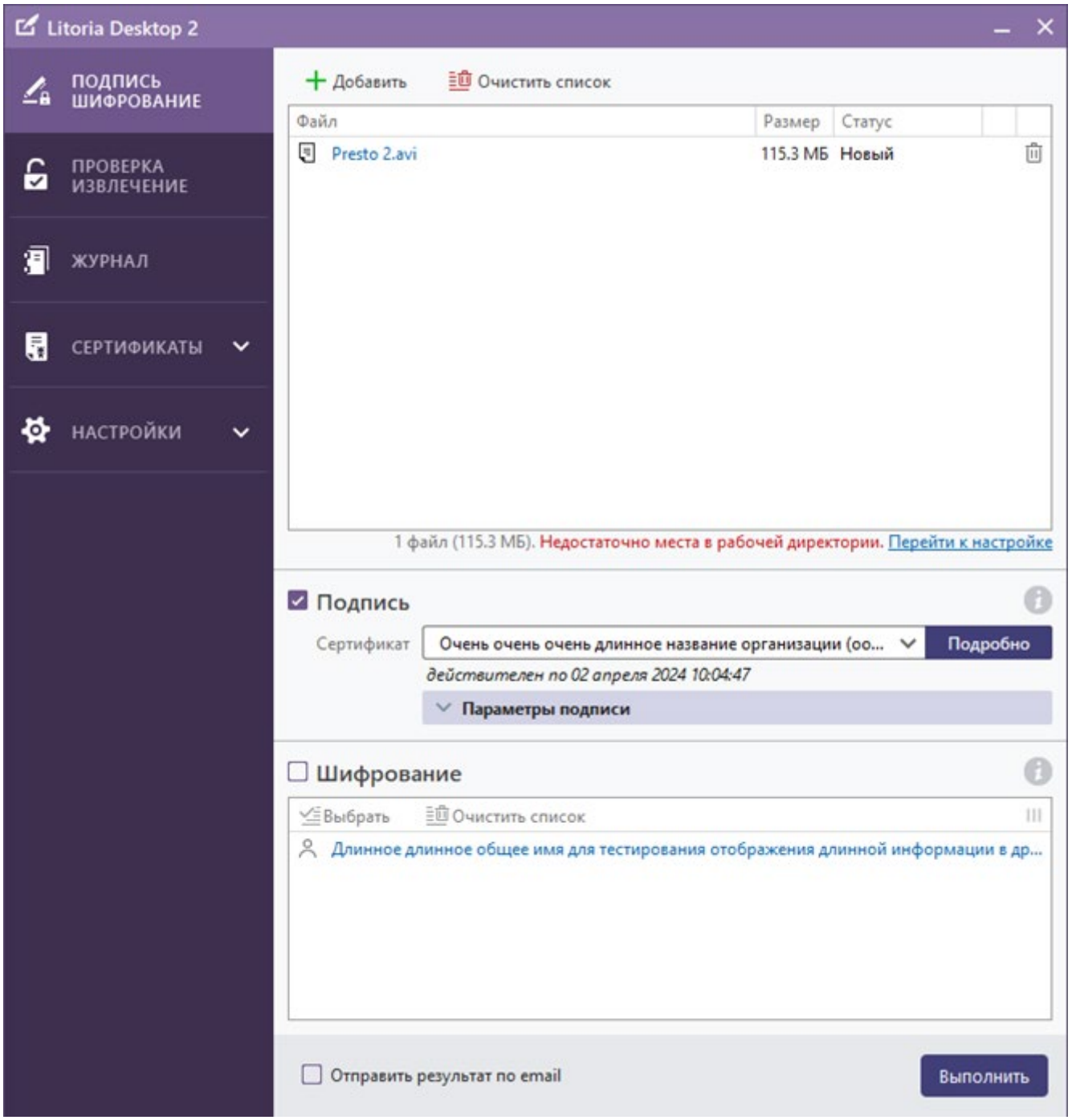


Рисунок 3.112 – Недостаточно места в рабочей директории

4 Вычисление контрольных сумм файлов

С помощью ПК «Litoria Desktop 2» возможно вычисление хеш-суммы (контрольной 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.

Для вычисления хеш-суммы файла необходимо запустить исполняемый файл *litoria.exe* из командной строки с дополнительными параметрами, описанными ниже (рисунки 4.1, 4.2):

litoria.exe hash --alg gost-3411 --dir "C:/1" --file "C:/1.txt" --pdf --out "C:/1.pdf"

где:

alg gost-3411 – алгоритм хеширования, по которому будет вычислена хеш-сумма, возможные значения gost-3411, gost-3411.12.256, gost-3411.12.512 (по умолчанию, если алгоритм в дополнительных параметрах не задан, хеш-сумма вычисляется по алгоритму ГОСТ Р 34.11-94);

dir "C:/1" – наименование каталога, для которого выполняется хеширование (при выборе каталога хеширование будет выполнено для всех файлов и подкаталогов, включенных в выбранный каталог);

file "C:/1.txt" – наименование файла, для которого выполняется хеширование;

pdf – формат вывода итогового отчета с КС файлов, возможные значения pdf, txt (по умолчанию, если формат в дополнительных параметрах не задан, отчет выводится в формате html);

out "C:/1.pdf" – путь для сохранения итогового отчета с КС (по умолчанию, если путь в дополнительных параметрах не задан, отчет сохраняется в директории *C:\Users\<имя пользователя>\AppData\Roaming\GIS\litoria\reports* в ОС Windows, */home/<имя пользователя>/.config/GIS/litoria/user_reports* в ОС Linux).

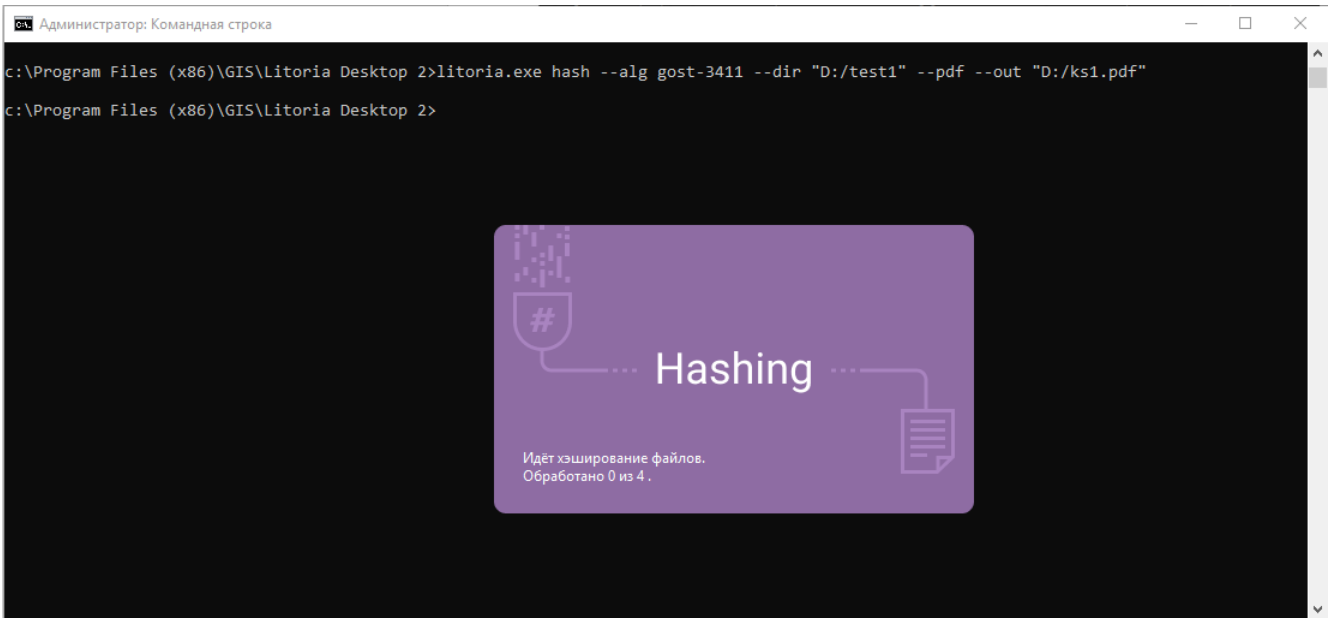


Рисунок 4.1 – Вычисление хеш-суммы файлов в ОС Windows

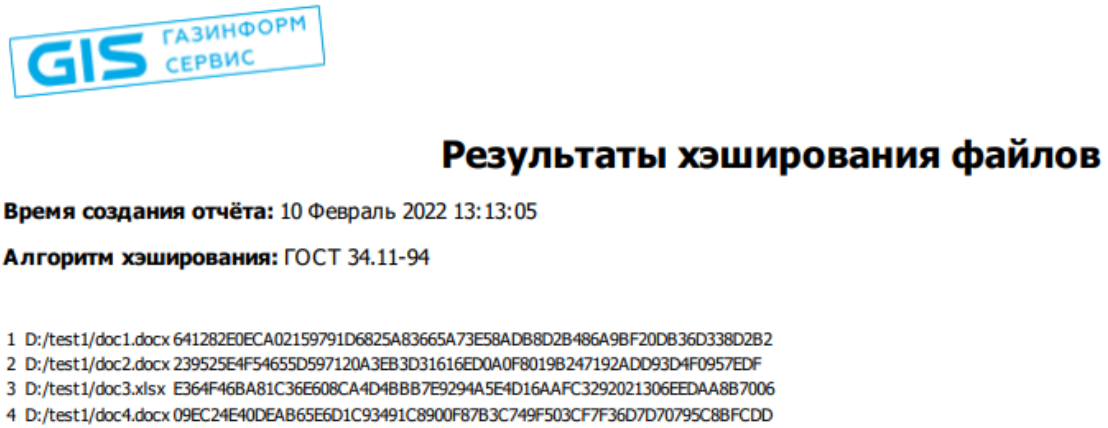


Рисунок 4.2 – Вывод итогового отчета с результатами хеширования в формате pdf

4.1 Вычисление КС файлов в ОС Windows с помощью контекстного меню

Вычисление хеш-суммы файла в ОС Windows возможно с помощью контекстного меню (рисунки 4.3, 4.4). При этом используются параметры хеширования, установленные по умолчанию:

– алгоритм хеширования *ГОСТ Р 34.11-94*,

– формат вывода итогового отчета с результатами хеширования *html*,
– имя отчета *hash_report*,
– директория сохранения отчета *C:\Users\<имя пользователя>\AppData\Roaming\GIS\litoria\reports*.

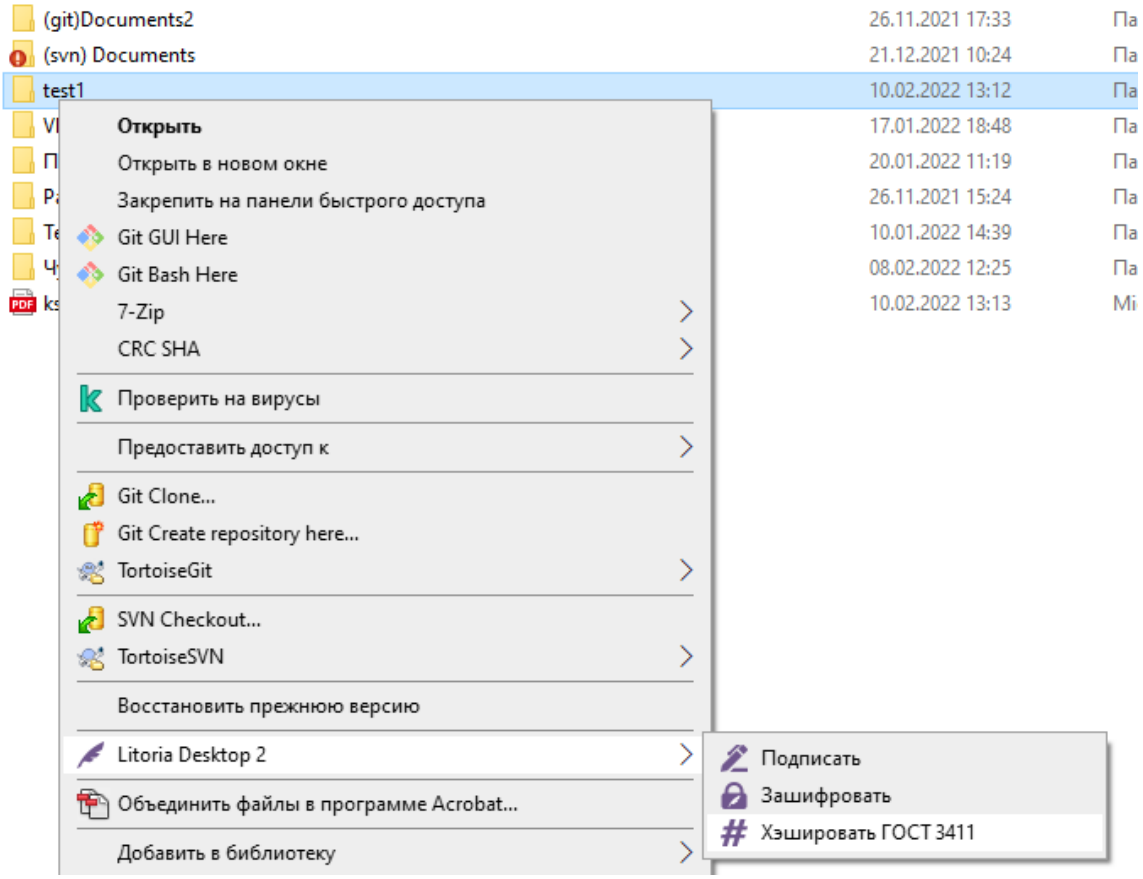


Рисунок 4.3 – Вычисление КС файлов с помощью контекстного меню

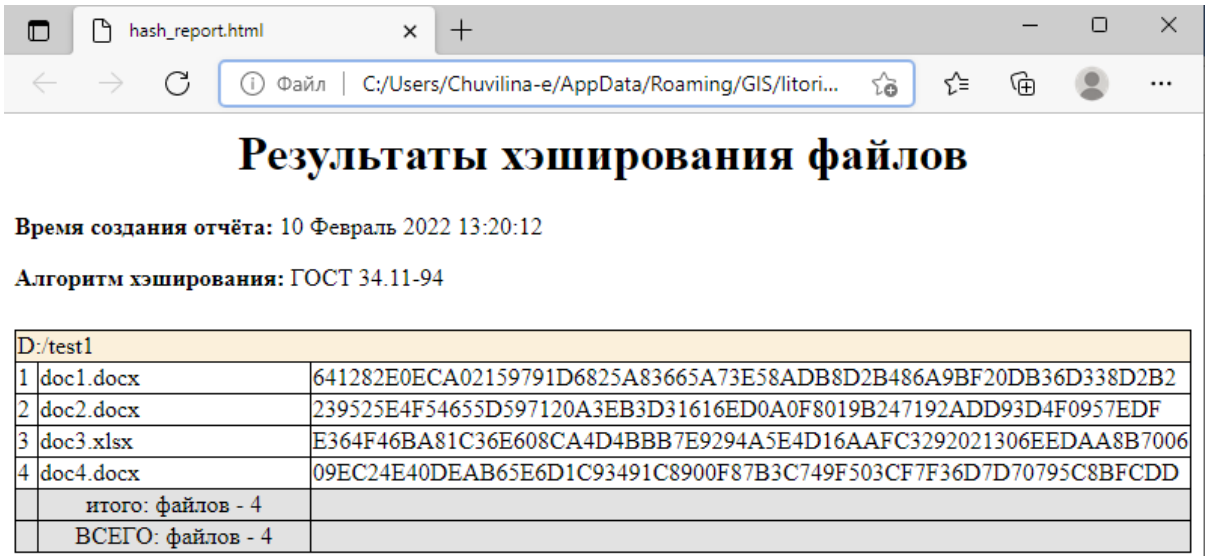


Рисунок 4.4 – Вывод итогового отчета с результатами хеширования в формате html

Возможные сообщения об ошибках при выполнении комплексной операции извлечения и проверки ЭП файла описаны в разделах **3.10.1 «Возможные сообщения об ошибках при проверке подписи»** и **3.12.1 «Возможные сообщения об ошибках при извлечении файла»**.

5 Применение сертификатов, отличных от стандарта ГОСТ

ПК «Litoria Desktop 2» поддерживает работу с сертификатами ключа проверки подписи, созданными на основе алгоритмов RSA, CNG RSA, CNG ECDSA_P256, CNG ECDSA_P384, CNG ECDSA_P521.

В ПК «Litoria Desktop 2» пользователь может использовать все функции, приведенные в данном документе, с сертификатами ключа проверки подписи, созданными на основе вышеперечисленных алгоритмов[6].

Все действия для выполнения функций идентичны действиям пользователя, описанным в разделах выше.

5.1 Совместное использование сертификатов, различных алгоритмов

Для функций добавления и заверения ЭП комплекс предоставляет возможность совместного использования сертификатов, относящихся к различным алгоритмам (ГОСТ и RSA), то есть создание так называемой «множественной» подписи.

При работе с сертификатами различных алгоритмов имеется единственное ограничение: нельзя выполнить функцию шифрования для получателей, сертификаты которых созданы на различных алгоритмах.

[6] Для сертификатов, на основе алгоритмов CNG RSA, CNG ECDSA_P256, CNG ECDSA_P384, CNG ECDSA_P521 не реализованы операции шифрования и извлечения.

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.

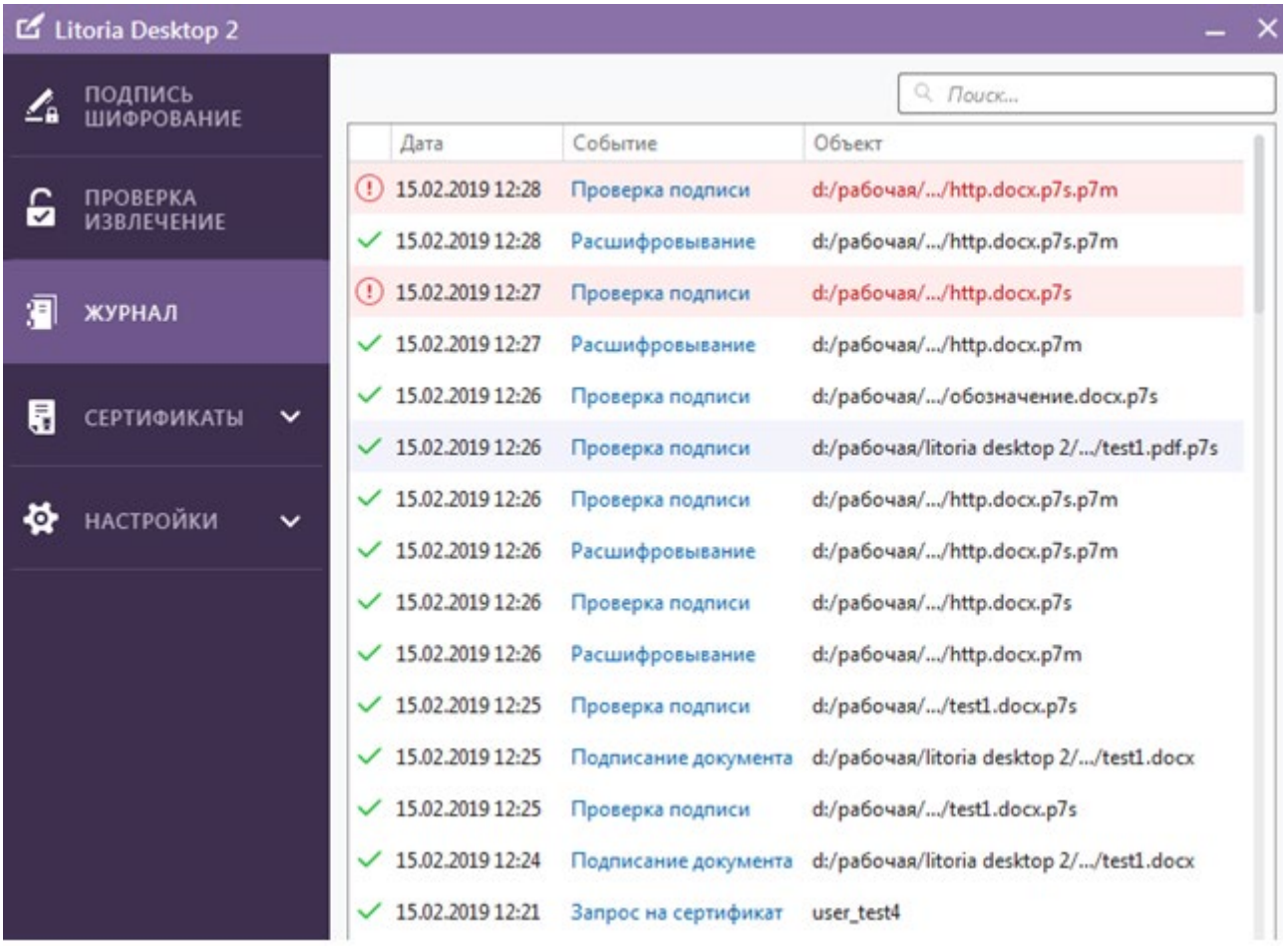


Рисунок 6.1 – Журнал событий

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	×
2	Шифрование	Успех	✓
		Ошибка	!
		Отмена	×
3	Проверка подписи	Успех	✓
		Ошибка	!
		Отмена	×
4	Расшифровывание	Успех	✓
		Ошибка	!
		Отмена	×
5	Подпись и шифрование	Успех	✓
		Ошибка	!
		Отмена	×
6	Запрос на сертификат	Успех	✓
		Ошибка	!
		Отмена	×
7	Удаление контейнера	Успех	✓
		Ошибка	!
		Отмена	×
8	Проверка ДТС	Успех	✓
		Ошибка	!
		Отмена	×
9	Экспорт контейнера	Успех	✓
		Ошибка	!
		Отмена	×
10	Импорт pfx	Успех	✓
		Ошибка	!
		Отмена	×
11	Заверение подписи	Успех	✓
		Ошибка	!
		Отмена	×
12	Продление подписи	Успех	✓

№	Событие	Успех/Ошибка	Пиктограмма
		Ошибка	
		Отмена	
13	Выпуск сертификата	Успех	
		Ошибка	
		Отмена	

Подробная информация по каждому событию доступна по щелчку на событии в списке событий (рисунок 6.2).

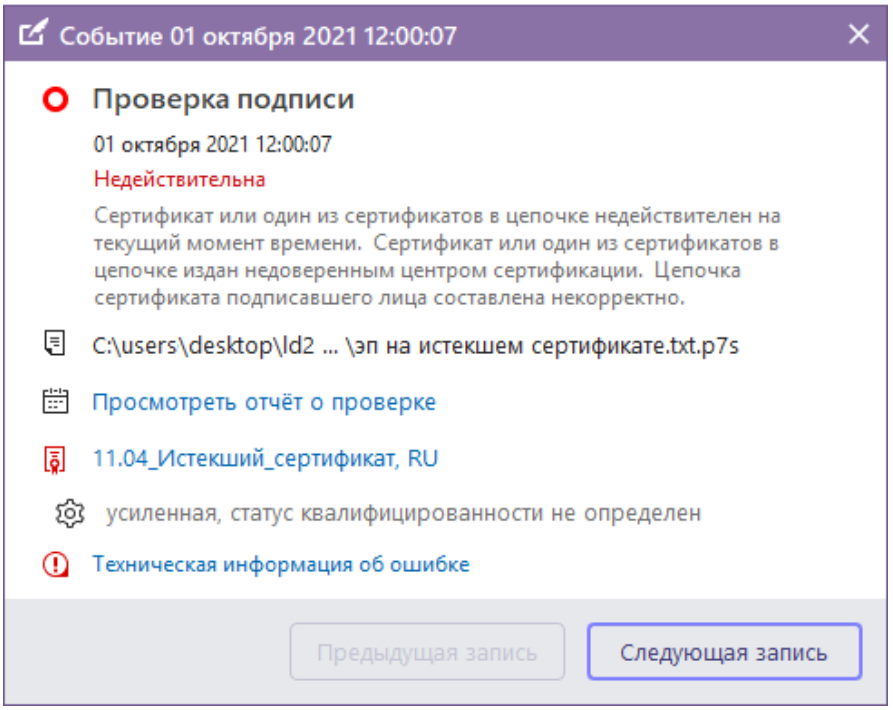


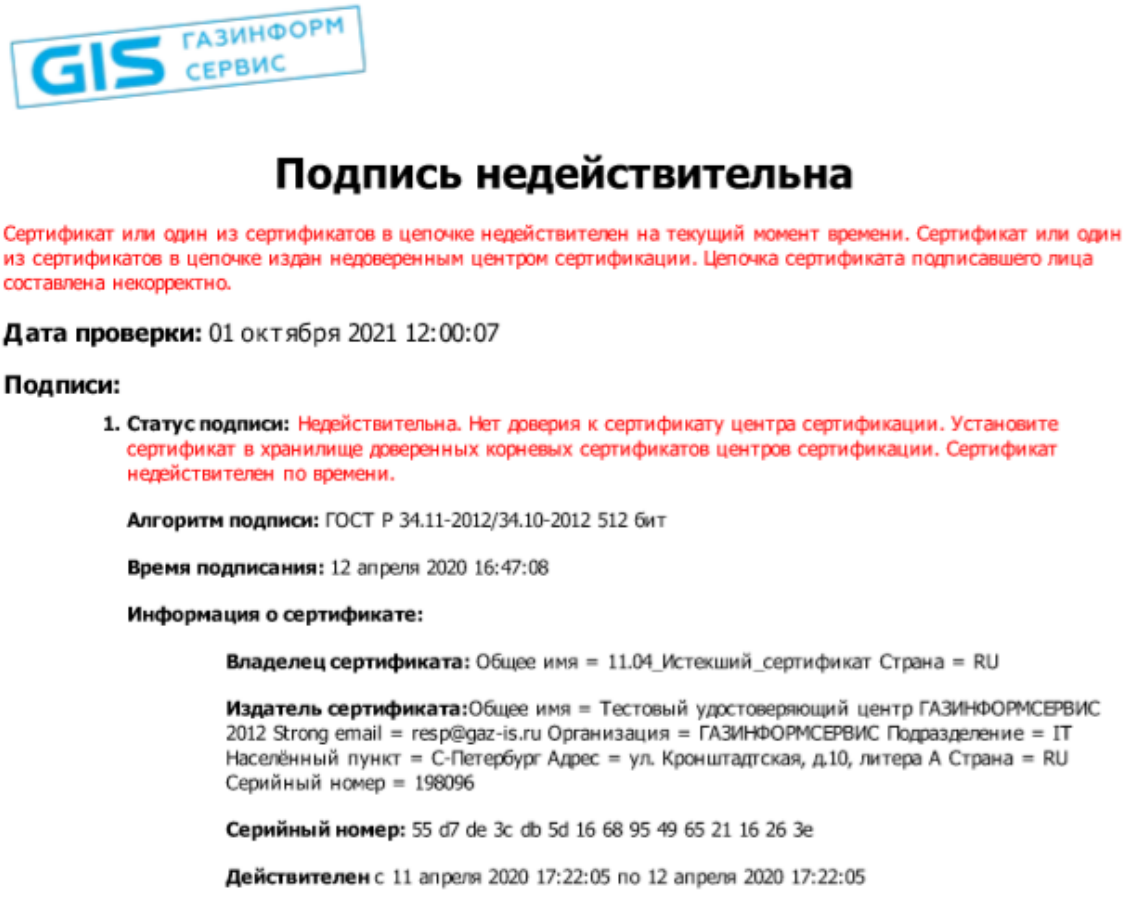
Рисунок 6.2 – Описание события

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.3.4.1);
- 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.



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).

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
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)

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)».

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».

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.