GIS ГАЗИНФОРМ СЕРВИС

Программный комплекс «Litoria DVCS»

Руководство пользователя

Санкт-Петербург, 2026

Аннотация

В документе приводится руководство пользователя программного комплекса «Litoria DVCS» версия 6.14.0-4 (далее – ПК «Litoria DVCS», ПК или комплекс).

В разделе «Назначение, функции и состав комплекса» приводятся сведения о назначении ПК «Litoria DVCS» и перечислены его основные функциональные возможности.

В разделе «Условия применения» указаны условия, необходимые для использования комплекса, требования к аппаратным и программным средствам автоматизированного рабочего места (АРМ) пользователя, а также приведен перечень программного обеспечения, с помощью которого пользователь может обращаться к ПК.

В разделе «Использование ПК «Litoria DVCS» описаны действия, необходимые для начала работы с ПК «Litoria DVCS», перечислены возможности пользователя и доступные ему настройки личного кабинета.

Содержание

1 Назначение, функции и состав комплекса 4
1.1 Назначение единого web-кабинета пользователя 6
2 Условия применения 7
2.1 Требования к техническим средствам 7
2.2 Требования к программному обеспечению 7
2.3 Программное обеспечение для обращения к комплексу 7
3 Использование ПК «Litoria DVCS» 8
3.1 Начало работы 8
3.1.1 Вход в web-кабинет 9
3.2 Аутентификация в web-кабинете «ПК «Litoria DVCS» 13
3.2.1 Аутентификация по сертификату 14
3.2.2 Аутентификация по протоколу LDAP 14
3.2.3 SSO-аутентификация 15
3.2.4 Восстановление пароля учетной записи пользователя 16
3.3 Редактирование личной информации пользователя 18
3.4 Проверка документа 21
3.4.1 Проверка документа 23
3.4.2 Проверка сертификата 26
3.4.3 Проверка подписанного документа 30
3.4.4 Постановка запроса в очередь 44
3.4.5 Информация о квитанции 48
3.4.6 Проверка соответствия подписанного документа и квитанции 49
3.4.7 Поиск квитанций по документу 51
3.4.8 Загрузка квитанции 53
3.5 Продление электронной подписи 53
3.5.1 Архив продлений 60
3.6 Задачи 62
3.7 Архив 64
3.8 Статистика 67
3.9 Изменение языка интерфейса 71
4 Лицензия и техподдержка 74
Перечень сокращений 75

1 Назначение, функции и состав комплекса

ПК «Litoria DVCS» предназначен для проверки электронной подписи или действительности сертификата ключа проверки электронной подписи, а также для подтверждения обладания информацией в указанный момент времени с предоставлением ее сервису или без предоставления, и продления срока действия ЭП.

ПК реализует функции сервиса доверенной третьей стороны (ДТС) и предоставляет пользователю возможность создания запросов на проверку, выполняет анализ этих запросов и формирует ответы, содержащие информацию о проведенных проверках, внутри страны/региона и при трансграничном электронном документообороте.

ПК «Litoria DVCS» может использоваться на предприятии в качестве сервиса, предоставляющего услуги по:

- проверке действительности ЭП и сертификатов на определенный момент времени;
- проверке полномочий владельцев сертификатов ЭП;
- выдаче квитанций с результатами проверки квалифицированной ЭП;
- хранению данных и журналированию всех выполняемых ДТС операций;

в том числе с использованием REST API (при этом внешняя информационная система может не иметь криптографию).

ПК «Litoria DVCS» разработан в соответствии с требованиями следующих нормативных документов:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ (в ред. от 6 апреля 2011 г.) «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- Приказ ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи»;
- Приказ ФСБ России от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;
- Приказ ФСБ России от 04.12.2020 г. № 556 «Об утверждении требований к средствам доверенной третьей стороны, включая требования к используемым доверенной третьей стороной средствам электронной подписи».

Основные функциональные возможности ПК «Litoria DVCS»:

- подтверждение электронной подписи (ЭП) электронного документа (Validation of Digitally Signed Document – VSD);
- подтверждение действительности сертификата ключа подписи (Validation of Public Key Certificates – VPKC);

– удостоверение обладания информацией в указанный момент времени с предоставлением ее сервису (Certification of Possession of Data – CPD);
– удостоверение обладания информацией без предоставления ее сервису (по хеш) (Certification of Claim of Possession of Data – CCPD);
– проверка данных, содержащихся в запросе;
– формирование и анализ DVC-квитанций в соответствии с рекомендациями RFC3029;
– поддержка электронных документов длительного архивного хранения;
– возможность просмотра информации о машиночитаемой доверенности;
– возможность взаимодействия с облачным хранилищем ПК «Litoria Nova».

ПК «Litoria DVCS» предназначен для проверки электронной подписи стандартов CAdES (согласно RFC 5126), PAdES (согласно ETSI as TS 102 778), XAdES (согласно ETSI as TS 101 903). Гарантирована проверка электронной подписи в следующих форматах:

Стандарт	Формат
CAdES	CAdES-BES/EPES, CAdES-T, CAdES-X Long Type 2, CAdES-A (v.2), CAdES-B-LTA, CAdES-E-A (v.3)
PAdES	PAdES-BES/EPES, PAdES-T, PAdES-LT
XAdES	XAdES-BES/EPES, XAdES-T, XAdES-XL, XAdES-A

ПК «Litoria DVCS» включает следующие компоненты:

1) **Служба DVCS** реализует протоколы DVCS (RFC 3029):
   – проверки электронной подписи в электронном документе, с предоставлением сервису подписанного электронного документа (протокол VSD) и без предоставления сервису подписанного документа, только по значению хеш-функции и сведений об электронной подписи (протокол VSD+);
   – проверки цепочки сертификатов (протокол VPKC);
   – выдачи свидетельств о предоставлении пользователем данных в заданный момент времени (протокол CPD);
   – выдачи свидетельств о факте обладания пользователем данными в заданный момент времени (протокол CCPD).
2) **Служба штампов времени TSP** (согласно RFC3161) удостоверяет факт существования электронного документа на определённый момент времени. Служба выдает штампы времени – документы, подписанные электронной подписью службы.
3) **Модуль REST API** выполняет автоматизированную отправку запросов и получение ответов участниками электронного взаимодействия.
4) **Единый web-кабинет** участника электронного взаимодействия (администратора/пользователя) позволяет обращаться к программному комплексу и предоставлять управление следующими функциями в зависимости от роли администратора или пользователя:

– управление настройками комплекса;
– управление учетными записями пользователей и администраторов;
– управление сертификатами служб;
– управление маршрутами;
– просмотр журнала произведенных операций;
– просмотр архива квитанций;
– проверка электронных документов.

1.1 Назначение единого web-кабинета пользователя

Единый web-кабинет позволяет пользователю осуществлять следующие операции:

1) Формирование DVCS-запросов следующих типов (в соответствии с рекомендациями RFC3029):
   – подтверждение электронной подписи (ЭП) электронного документа (Validation of Digitally Signed Document – VSD);
   – подтверждение действительности сертификата ключа подписи (Validation of Public Key Certificates – VPKC);
   – удостоверение обладания информацией в указанный момент времени с предоставлением ее сервису (Certification of Possession of Data – CPD);
   – удостоверение обладания информацией без предоставления ее сервису (по хеш) (Certification of Claim of Possession of Data – CCPD).
2) Поиск квитанций на ранее сделанный DVCS-запрос.
3) Редактирование данных профиля пользователя.
4) Отправку запроса в службу поддержки.

Кроме того, для пользователей с полномочиями администратора предусмотрены следующие дополнительные возможности:

1) добавление учетных записей пользователей в систему и разделение пользовательских полномочий;
2) просмотр квитанций других пользователей.

Полномочия администратора для пользователей присваиваются администратором пользователей в соответствии с документом «ПК «Litoria DVCS». Руководство администратора безопасности».

2 Условия применения

2.1 Требования к техническим средствам

Минимальные аппаратные требования к рабочей станции, с которой пользователь будет обращаться к ПК «Litoria DVCS», обусловлены применением используемых ОС.

2.2 Требования к программному обеспечению

Минимальные требования к составу программных средств рабочей станции, с которой пользователь будет обращаться к ПК «Litoria DVCS»:

- ОС Microsoft Windows 7/8/8.1/10;
- ОС семейств Linux[1].

Дополнительно должно быть установлено следующее программное обеспечение:

- Средство криптографической защиты информации, реализованное в соответствии с технологией Microsoft CSP (при работе с отечественной криптографией необходимо использовать соответствующие СКЗИ)[2].
- СКЗИ «КриптоПро CSP» с поддержкой графического представления или СКЗИ «ViPNet CSP».[3]

Поддерживаются веб-браузеры:

- Google Chrome не ниже версии 97.0.4692.71;
- Chromium-Gost не ниже версии 97.0.4692.71;
- Яндекс.Браузер не ниже версии 22.1.0;
- Microsoft Edge не ниже версии 97.0.1072.55.

2.3 Программное обеспечение для обращения к комплексу

Для обращения к ПК «Litoria DVCS» пользователь может использовать различное программное обеспечение разработанное на основе средств, предоставляемых ПК «Litoria DVCS».

[1] Гарантирована работа ПК «Litoria DVCS» на ОС Astra Linux Смоленск версии 1.7.5 и РЕД ОС версии 7.3.4.

[2] При функционировании ПК на ОС семейства Windows.

[3] При функционировании ПК на ОС семейства Linux.

3 Использование ПК «Litoria DVCS»

Основные функциональные возможности ПК «Litoria DVCS» доступны в едином web-кабинете пользователя.

3.1 Начало работы

Перед началом работы с личным кабинетом при аутентификации по паролю пользователь должен обратиться к администратору ПК «Litoria DVCS» для получения идентификационных данных (логина и временного/первичного пароля) для регистрации в службе DVCS.

Если пользователь будет создавать DVCS-запросы в службу проверки подлинности не через единый web-кабинет пользователя, а с помощью ПО, перечисленного в подразделе «Программное обеспечение для обращения к комплексу», то он также должен обратиться в удостоверяющий центр для получения личного сертификата ключа проверки ЭП (потребуется предъявить документы, удостоверяющие личность).

Для начала работы с ПК «Litoria DVCS» в строке web-браузера наберите адрес web-кабинета ПК «Litoria DVCS». На экране появится начальная страница сайта (рисунок 1). Функциональные возможности web-кабинета станут доступны после успешного прохождения аутентификации.

Рисунок 1 – Начальная страница web-кабинета ПК «СДТС «Litoria DVCS»

3.1.1 Вход в web-кабинет

При первом входе пользователя в веб-кабинет появится приглашение к смене пароля (рисунок 2).

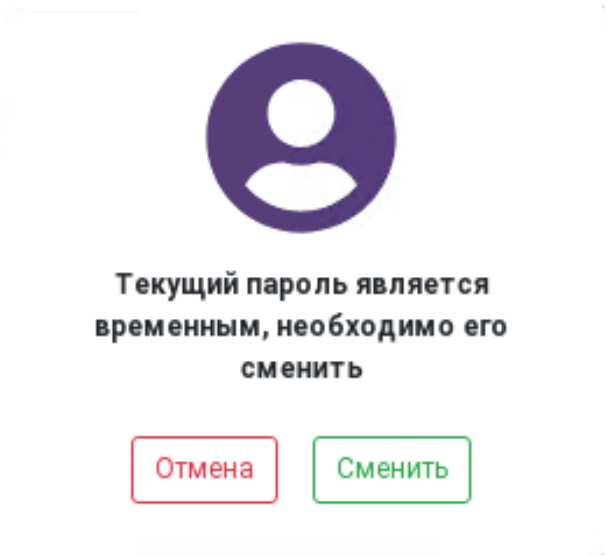


Рисунок 2 – Первый вход в web-кабинет по временному паролю

По нажатию на кнопку ***«Сменить»*** откроется интерфейс для замены временного пароля на постоянный (рисунок 3).

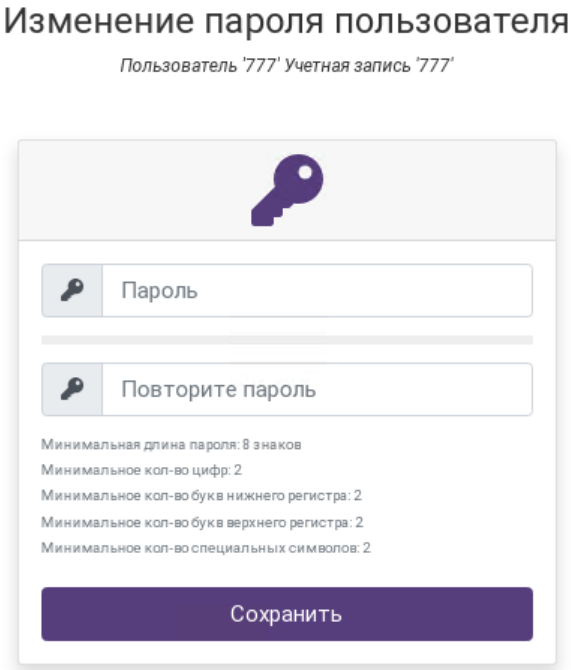


Рисунок 3 – Смена временного пароля на постоянный

Длительность действия временного пароля определяется администратором при настройке ПК «Litoria DVCS».

Последующий вход пользователя в веб-кабинет осуществляется по постоянному паролю. Для входа в web-кабинет необходимо заполнить поля «Имя пользователя» и «Пароль», и нажать на кнопку ***«Вход»*** (рисунок 4).

Для автоматического заполнения учетных данных при последующих входах предусмотрен флаг ***«Запомнить меня»***.

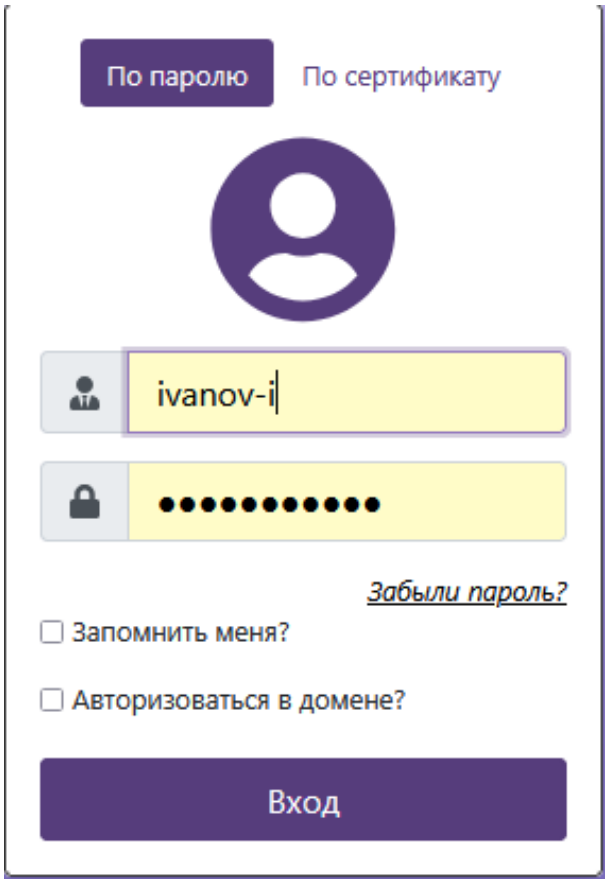


Рисунок 4 – Вход в web-кабинет

Пароль для входа в веб-кабинет пользователя создается в соответствии с политикой эксплуатирующей организации и включает следующие требования:

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры, спецсимволы;
– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения;
– при смене пароля недопустимо использовать пароли, использованные ранее.

Требования к предъявляемому паролю пользователя отображаются при изменении пароля пользователя (рисунок 5).

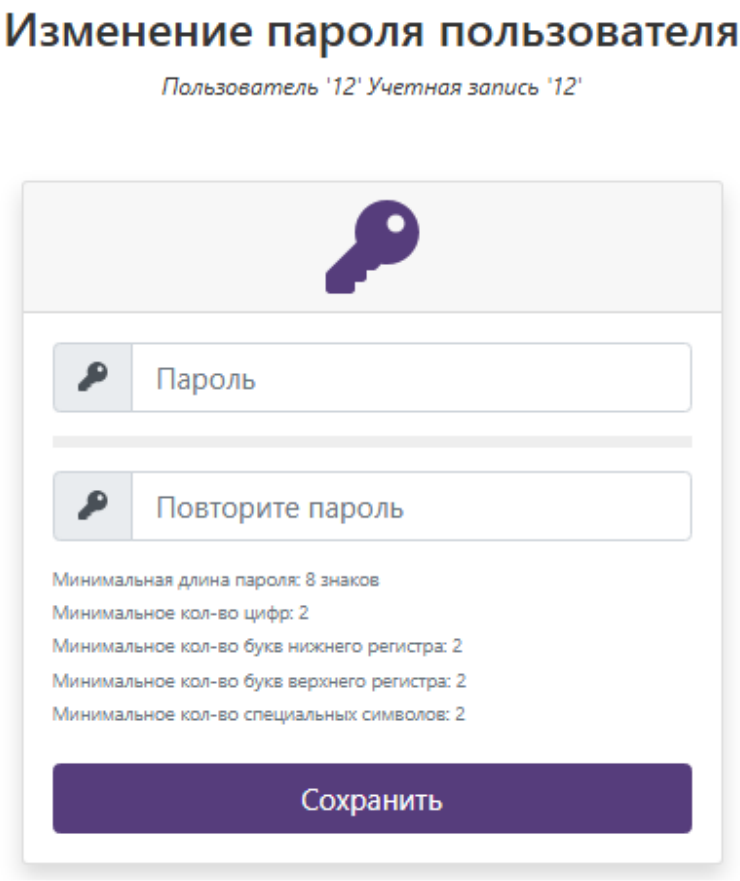


Рисунок 5 – Требования к паролю пользователя

При аутентификации в web-кабинете необходимо учитывать следующие ограничения:

- смена пароля должна производиться не реже одного раза в 180 дней;
- пользователь может самостоятельно сменить пароль до истечения срока действия пароля в карточке пользователя;
- по истечении времени действия пароля пользователя доступ в web-кабинет будет ограничен, пользователю после аутентификации в web-кабинете будет предложено сменить пароль;
- при превышении установленного количества неверного ввода идентификационных данных учетная запись будет заблокирована на установленное время блокировки или до момента разблокировки администратором системы.

Примечание. Если при вводе имени или пароля была неправильно нажата какая-либо клавиша, скорректируйте ошибочно набранные символы в строке и заново повторите ввод символов.

После успешной аутентификации пользователя появится главное окно web-кабинета ПК «Litoria DVCS» (рисунок 6), в котором пользователю доступно управление следующими функциями:

– управление собственной учетной записью пользователя;
– проверка электронных документов;
– просмотр продления срока доверенного архивного хранения подписанных квитанций в автоматическом режиме с помощью службы продления квитанций с отображением информации о продлении в системном журнале;
– просмотр асинхронного режима обработки запросов;
– просмотр и отслеживание архива квитанций пользователя (поиск квитанций для проверяемого документа, проверка соответствия документа квитанции);
– формирование и просмотр статистических отчётов по операциям пользователя;
– изменение языка интерфейса ПК «Litoria DVCS».

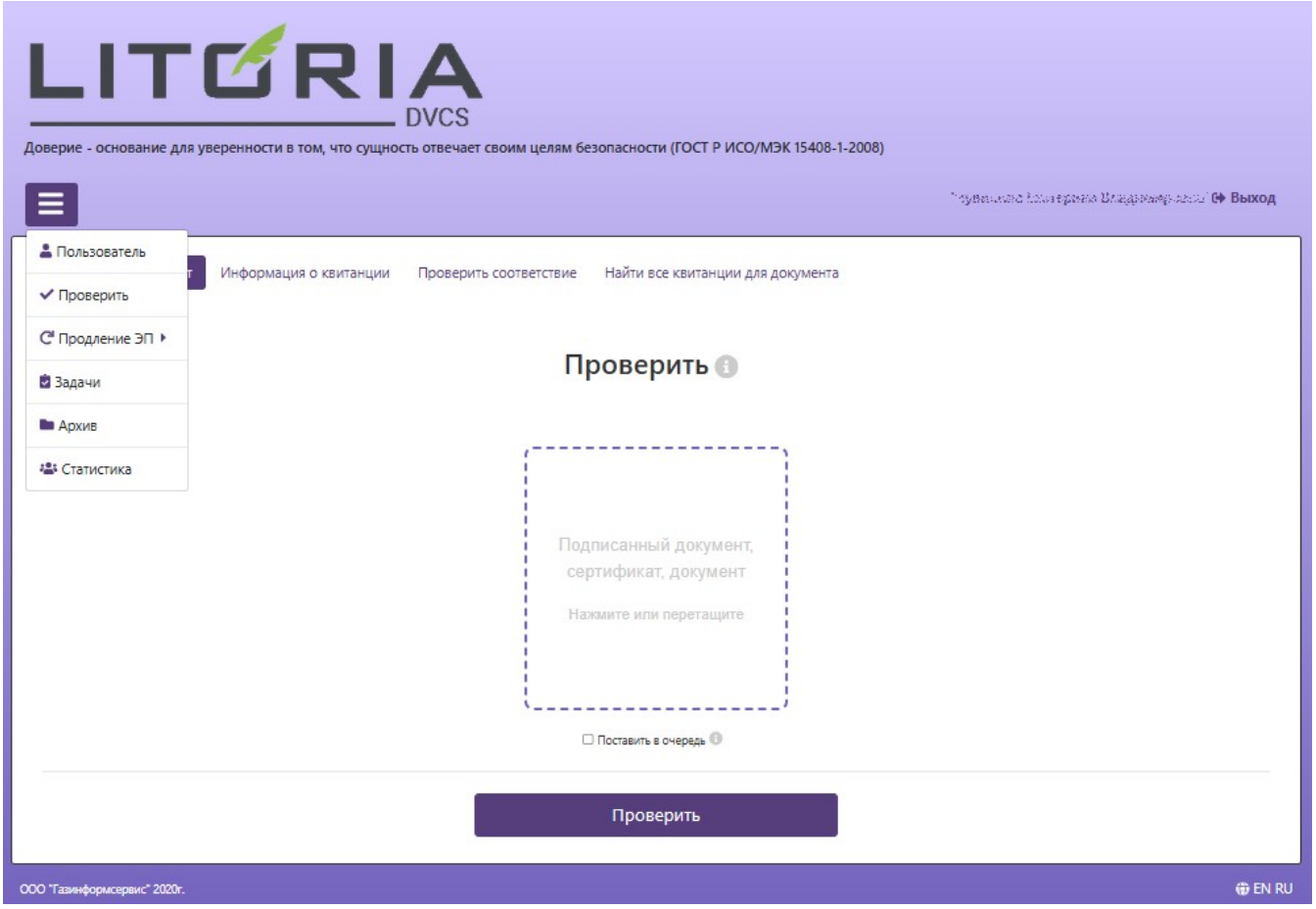


Рисунок 6 – Вид главной страницы web-кабинета после авторизации пользователя

3.2 Аутентификация в web-кабинете «ПК «Litoria DVCS»

При обращении к в web-кабинету «ПК «Litoria DVCS» пользователя возможны следующие виды аутентификации:

– вход по паролю – аутентификация с предъявлением имени учетной записи и пароля, соответствующего введенному имени учетной записи;
– двухфакторная аутентификация с использованием ключа подтверждения – при прохождении аутентификации пользователю на заданный адрес электронной

почты отправляется ключ подтверждения, который необходимо будет ввести в дополнительное окно при входе;

– вход по сертификату – двухфакторная аутентификация с помощью СКЗИ с использованием цифрового сертификата;
– аутентификация в домене по протоколу LDAP – аутентификация в ПК «Litoria DVCS» с указанием доменных учетных данных пользователя (рисунок 7).
– SSO-аутентификация – аутентификация в ПК «Litoria DVCS» с использованием внешнего сервера аутентификации.

3.2.1 Аутентификация по сертификату

Если администратором безопасности установлено разрешение аутентификации с использованием сертификата, а также установлен и запущен модуль «Litoria Auth», то на странице аутентификации в зависимости от установленных администратором безопасности настроек появится или окно с аутентификацией по сертификату или окно с вариантами аутентификации и по паролю, и по сертификату, в котором необходимо перейти на вкладку «По сертификату» (рисунок 1).

После выбора сертификата пользователю необходимо нажать кнопку ***«Вход»***.

Необходимость ввода пароля в интерфейсе аутентификации СКЗИ настраивается администратором безопасности.

3.2.2 Аутентификация по протоколу LDAP

Если администратором безопасности установлено разрешение аутентификации в домене при входе пользователя, на странице аутентификации, появится дополнительный параметр «Авторизоваться в '<имя_домена >'?». Пользователю нужно выбрать домен, указать свои доменные учетные данные и нажать кнопку «***Вход»***.

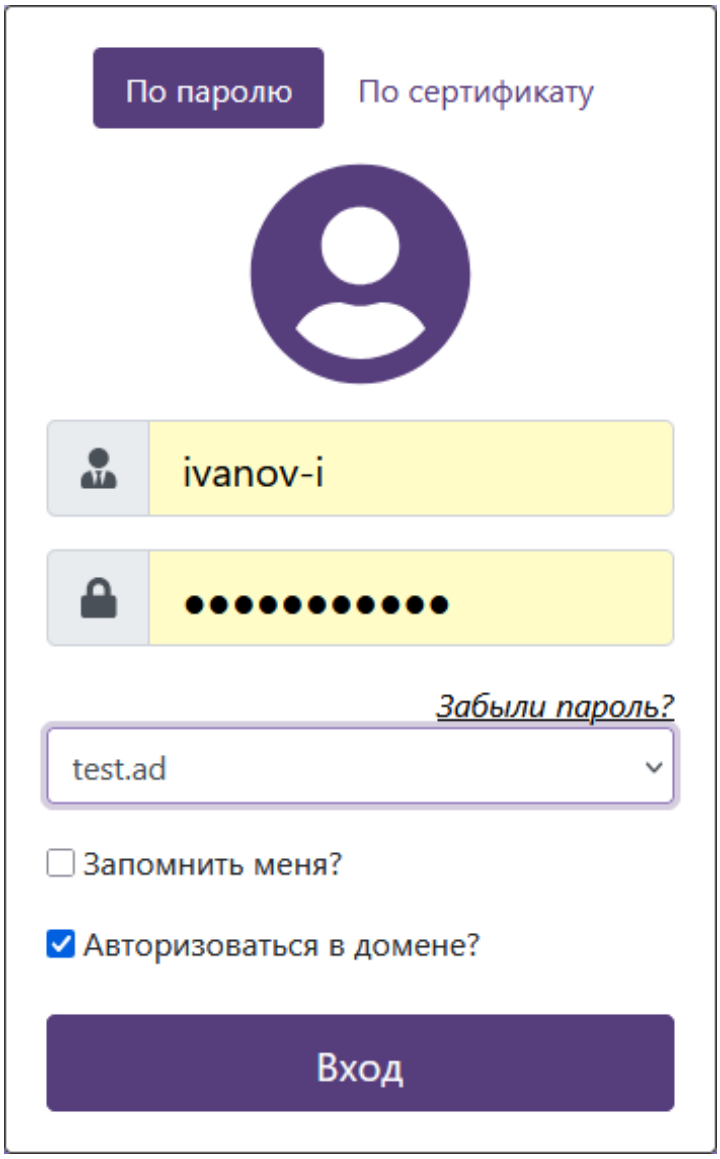


Рисунок 7 – Аутентификация по протоколу LDAP

Вид аутентификации пользователя определяется администратором безопасности в соответствии с документом «Руководство администратора безопасности».

3.2.3 SSO-аутентификация

Если администратором безопасности установлено разрешение на SSO-аутентификацию (Single Sign-On) с использованием внешнего сервера аутентификации, то на странице аутентификации в зависимости от установленных администратором безопасности настроек появится окно, в котором необходимо выполнить следующие действия:

1) На начальной странице веб-кабинета ПК «Litoria DVCS» перейти на вкладку ***«По SSO»*** (рисунок 8).

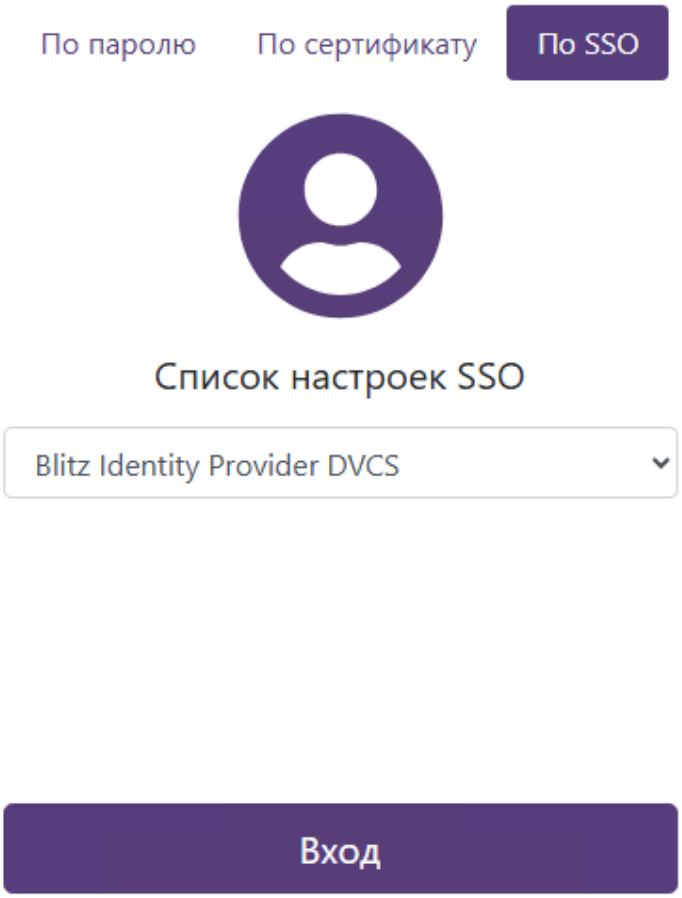


Рисунок 8 – Вкладка «Вход SSO»

2) Выбрать из выпадающего списка доступный внешний сервер аутентификации и нажать на кнопку ***Вход***.
3) По кнопке ***Вход*** происходит перенаправление на выбранный внешний сервер аутентификации для ввода логина и пароля пользователя SSO.
4) После успешного подтверждения логина и пароля пользователя SSO ПК «Litoria DVCS» аутентифицирует или регистрирует пользователя, автоматически перенаправляя его на главную страницу ПК «Litoria DVCS» с соответствующими правами (рисунок 6).

3.2.4 Восстановление пароля учетной записи пользователя

Процедура восстановления пароля пользователя доступна по ссылке *«Забыли пароль?»* в окне аутентификации (рисунок 7).

При нажатии на ссылку, на электронную почту, указанную в профиле учетной записи пользователя, придет письмо, содержащее код восстановления доступа в web-кабинет ПК «Litoria DVCS», который необходимо ввести в форму восстановления пароля (рисунок 9). Также необходимо ввести новый пароль учетной записи пользователя в соответствии с указанными требованиями к паролю.

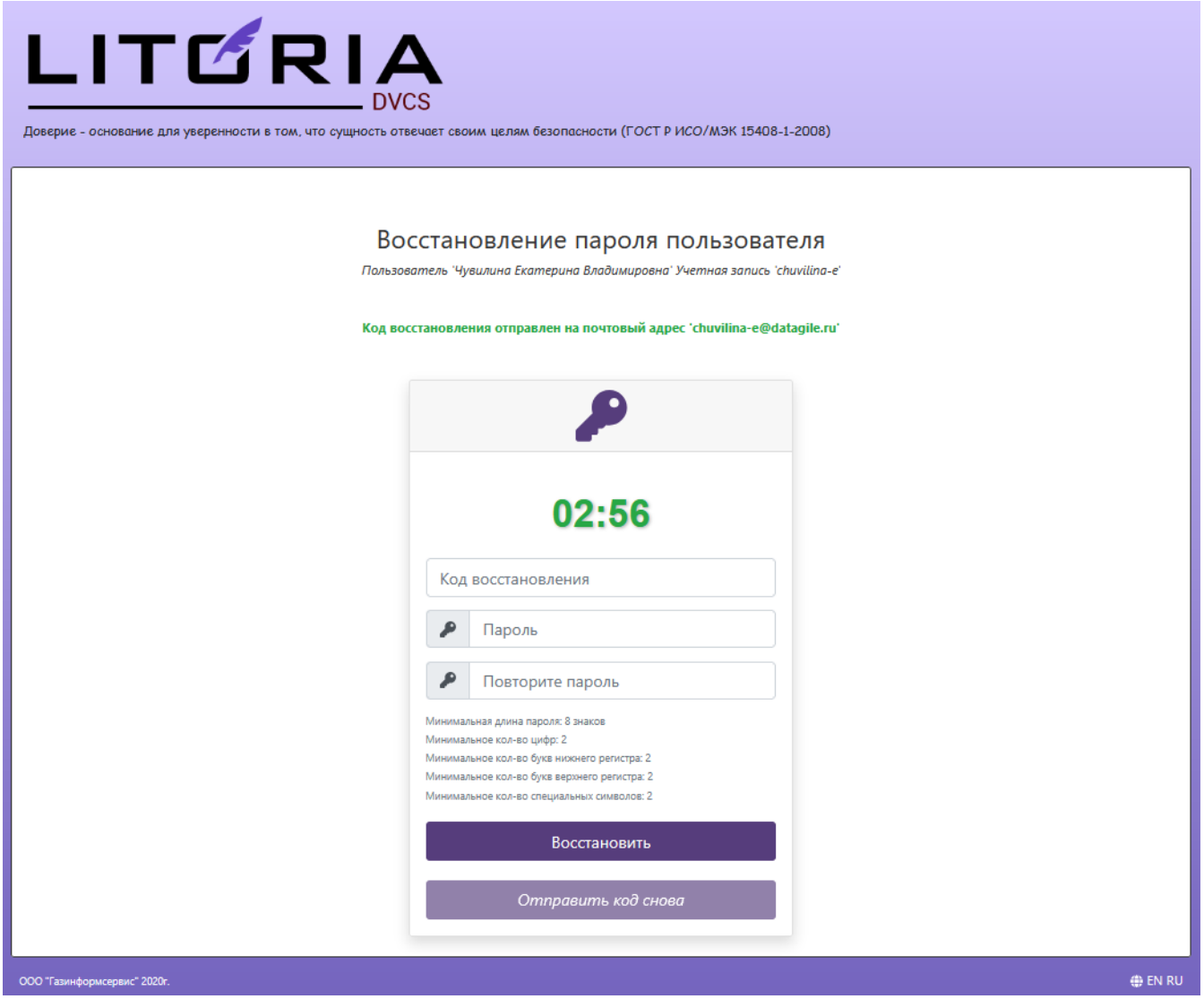


Рисунок 9 – Форма восстановления пароля

Заполнение полей в форме восстановления пароля доступно в течение срока действия таймера. В случае окончания таймера доступно повторное получение кода из окна восстановления пароля по кнопке *«Отправить пароль снова»* (рисунок 10).

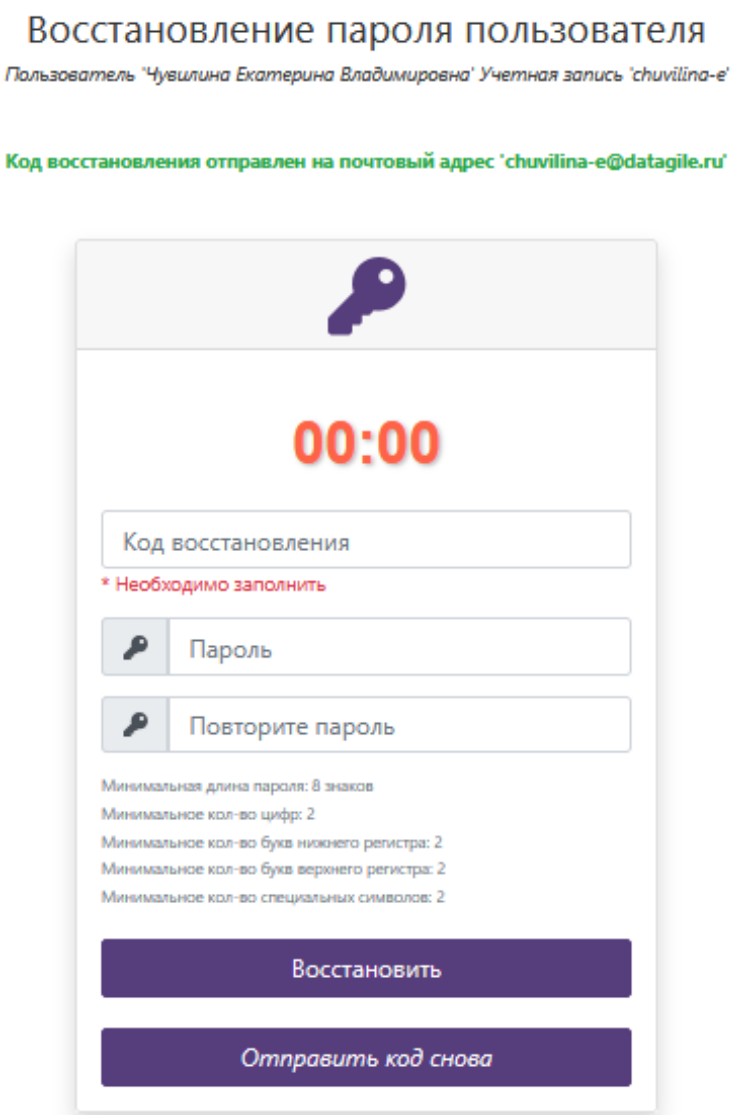


Рисунок 10 – Повторная отправка кода для восстановления пароля

При превышении неудачных попыток ввода возможность восстановления/сброса пароля учетной записи пользователя будет недоступна в течение времени, заданного администратором.

3.3 Редактирование личной информации пользователя

Редактирование личной информации доступно пользователю в пункте меню ***«Пользователь»*** после успешного прохождения аутентификации в web-кабинете «ПК «Litoria DVCS».

Для редактирования личной информации выполните следующие действия:

1) Перейдите в пункт меню ***«Пользователь»*** (рисунок 11).

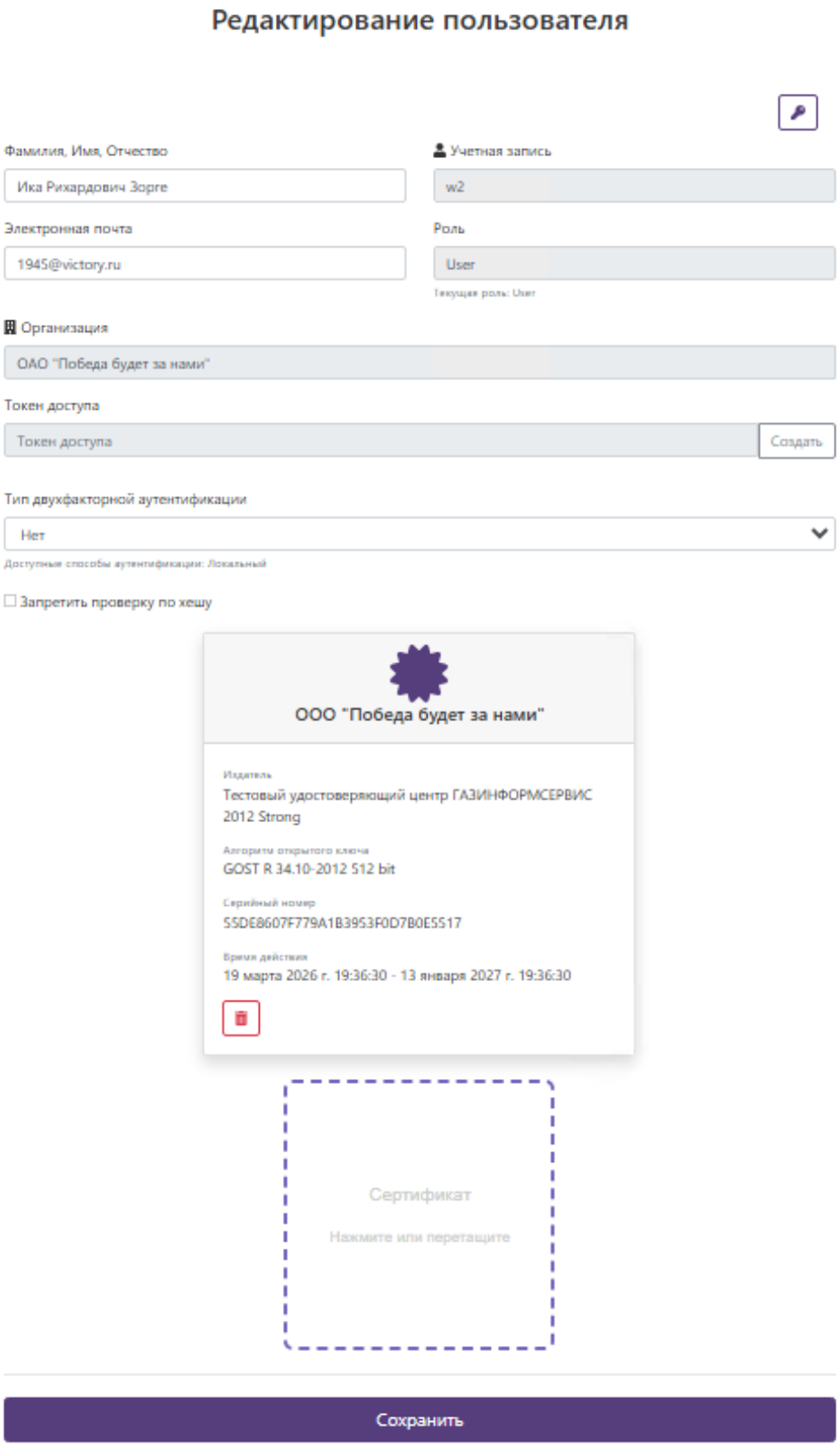


Рисунок 11 – Пункт меню «Пользователь»

2) В открывшемся окне отображаются следующие параметры учетной записи:

– личные параметры учетной записи (доступны для изменения ФИО пользователя, адрес электронной почты);
– организация, в которую входит пользователь (отображается только в случае привязки пользователя к какой-либо организации, доступно для редактирования администратору комплекса);
– сертификаты учетной записи (добавление нового сертификата, просмотр/удаление имеющегося сертификата);
– генерация и добавление токена доступа (используется при отправке API-запросов, см. документ «Руководство администратора безопасности. Модуль REST API»);
– изменение типа двухфакторной аутентификации (по умолчанию двухфакторная аутентификация выключена):
  а. аутентификация на основе почты (при каждом прохождении аутентификации пользователю на почту будет отправляться ключ, который необходимо ввести в дополнительное окно при входе);
  б. аутентификация через Google Authentificator (необходимо сканировать QR-код с помощью приложения Google Authentificator и далее, при каждом прохождении аутентификации, пользователю после ввода логина и пароля будет отправляться одноразовый пароль для входа);
– запрещение проверки по хешу (опция отключена по умолчанию - проверки по хешу разрешены, позволяет блокировать VSD-проверки по хешу, в том числе и при трансграничном взаимодействии);
– изменение пароля учетной записи по кнопке « 🔑 »;

3) Нажмите на кнопку «***Сохранить***» для завершения операции редактирования учетной записи.

В карточке редактирования пользователя также указываются доступные способы аутентификации пользователя (рисунок 12):

– если пользователь создан с помощью web-кабинета ПК «Litoria DVCS», ему будет доступна только локальная аутентификация (тип входа «Локальный»);
– если пользователь создан при аутентификации по LDAP, ему будет доступна аутентификация с доменным паролем по LDAP (тип входа «Доменный (LDAP)»);
– если пользователь создан при аутентификации по LDAP, а потом сменил пароль с помощью web-кабинета ПК «Litoria DVCS», пользователь сможет аутентифицироваться с доменным паролем по LDAP, а также с новым паролем локально (тип входа «Доменный (LDAP) | Локальный»).

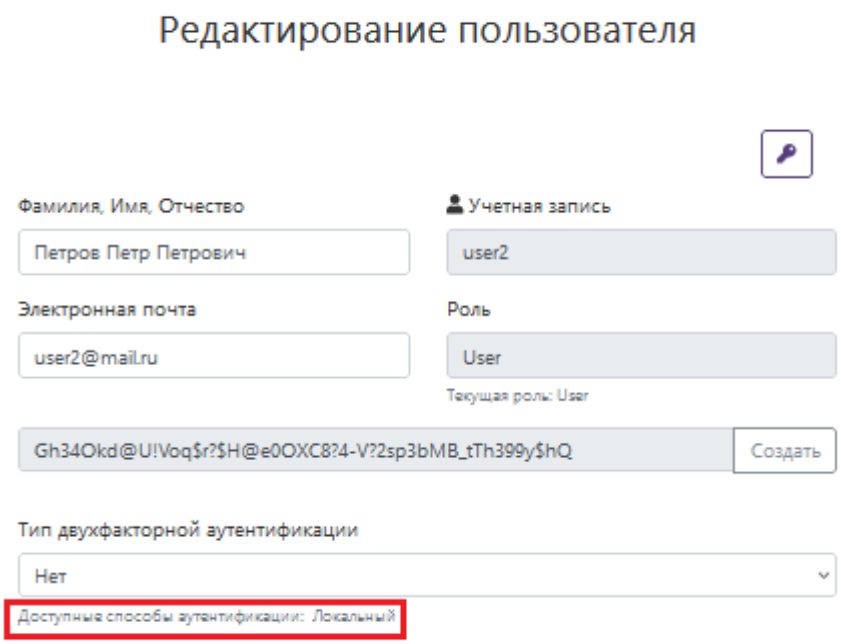


Рисунок 12 – Доступные способы аутентификации пользователя

3.4 Проверка документа

Основное назначение ПК «Litoria DVCS» возможность проверки электронных документов, полученных от участника электронного взаимодействия, и выдача квитанций с результатами проверки.

Служба DVCS предоставляет следующие услуги проверки данных в запросе пользователя:

- подтверждение действительности ЭП документа (VSD) (см. пункт «Проверка подписанного документа»);
- проверка срока действия сертификатов ключей проверки ЭП (VPKC) (см. пункт «Проверка сертификата»);
- удостоверение о предоставлении службе данных и о факте обладания пользователем этими данными в указанный момент времени (CPD) (см. пункт «Проверка документа»).

Операции проверки доступны администратору или пользователям в пункте меню ***«Проверить»*** после успешного прохождения аутентификации в web-кабинете «ПК «Litoria DVCS» (рисунок 13).

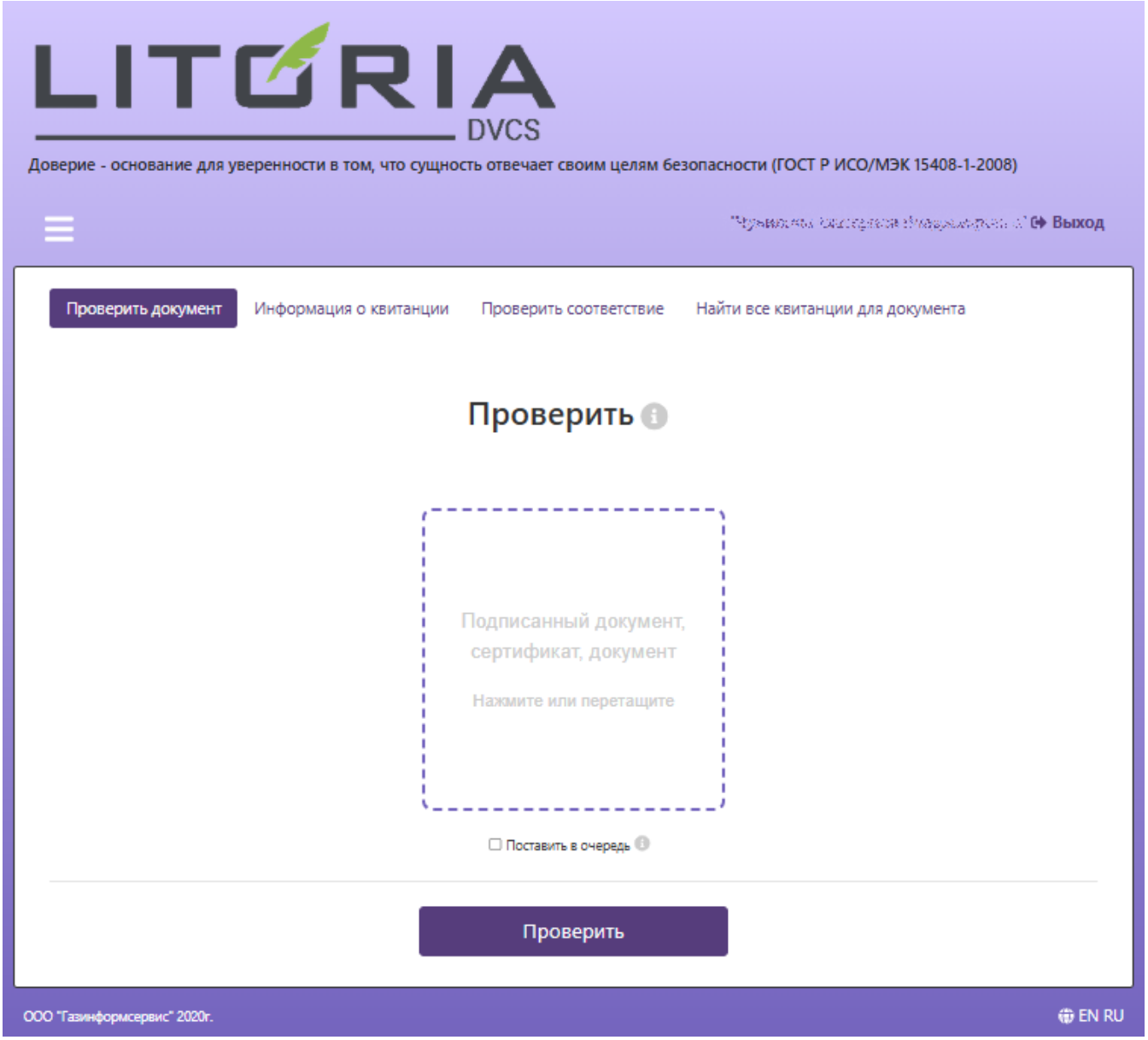


Рисунок 13 – Проверка подписанного документа, сертификата или документа

Для проверки возможно добавить следующие виды данных:

- документ;
- сертификат;
- подписанный документ (любая не отделенная подпись в DER-кодировке, в BASE64-кодировке);
- подписанный документ с отделенной подписью (любая отделенная подпись в DER-кодировке, в BASE64-кодировке);
- документ в формате PDF;
- подписанный PDF-документ;
- зашифрованный документ;
- подписанный XAdES-документ, в том числе подписанные отдельные секции XAdES-документа.

Примечание. По умолчанию максимально допустимый размер документа, отправляемого на проверку, равен 20Мб. Для увеличения максимально допустимого размера документа в запросе, необходимо обратиться к администратору безопасности.

3.4.1 Проверка документа

Для подтверждения обладания информацией в указанный момент времени с предоставлением ее сервису или без предоставления:

1) Перейдите в пункт меню ***«Проверить»,*** во вкладку ***«Проверить документ»*** (рисунок 13) и поместите документ, который необходимо проверить в область ***«Подписанный документ, сертификат, документ»*** (рисунок 14). Данную операцию можно выполнить несколькими способами:
   – нажатием на ссылку ***«Подписанный документ, сертификат, документ»*** и выбором необходимого файла в открывшемся окне;
   – перетаскиванием файла из окна Проводника в область ***«Подписанный документ, сертификат, документ».***

Примечание. При добавлении неподписанного документа для подтверждения обладания информацией, в области ***«Подписанный документ, сертификат, документ»***, указывается его тип – «*Документ*» и формат (рисунок 14).

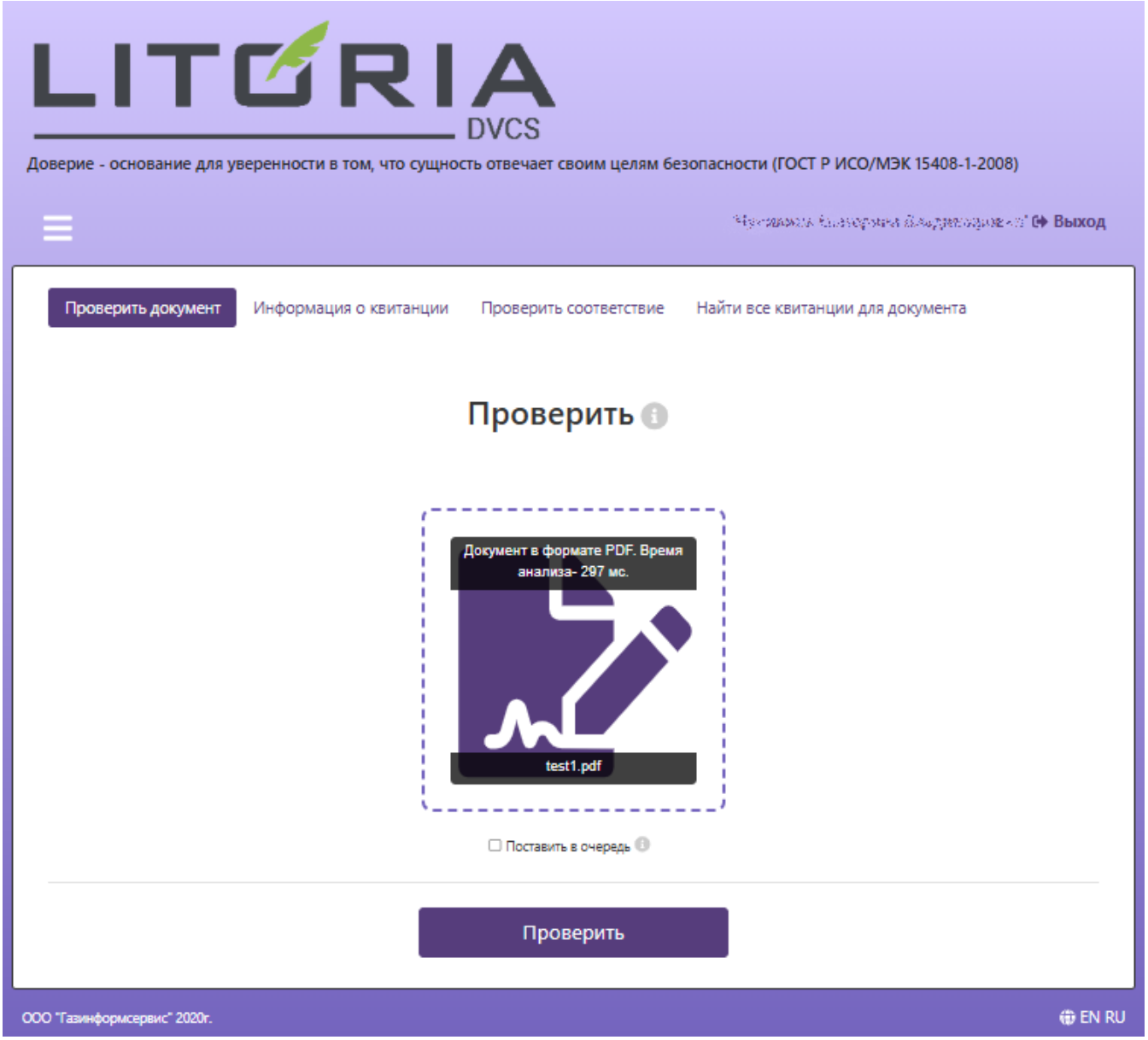


Рисунок 14 – Подтверждение обладания информацией в указанный момент времени

2) Нажмите на кнопку «***Проверить***» для отправки документа на проверку.
3) При успешном завершении проверки документа на экране отобразится ответная квитанция службы DVCS, содержащая информацию в проведенных проверках (рисунок 15).

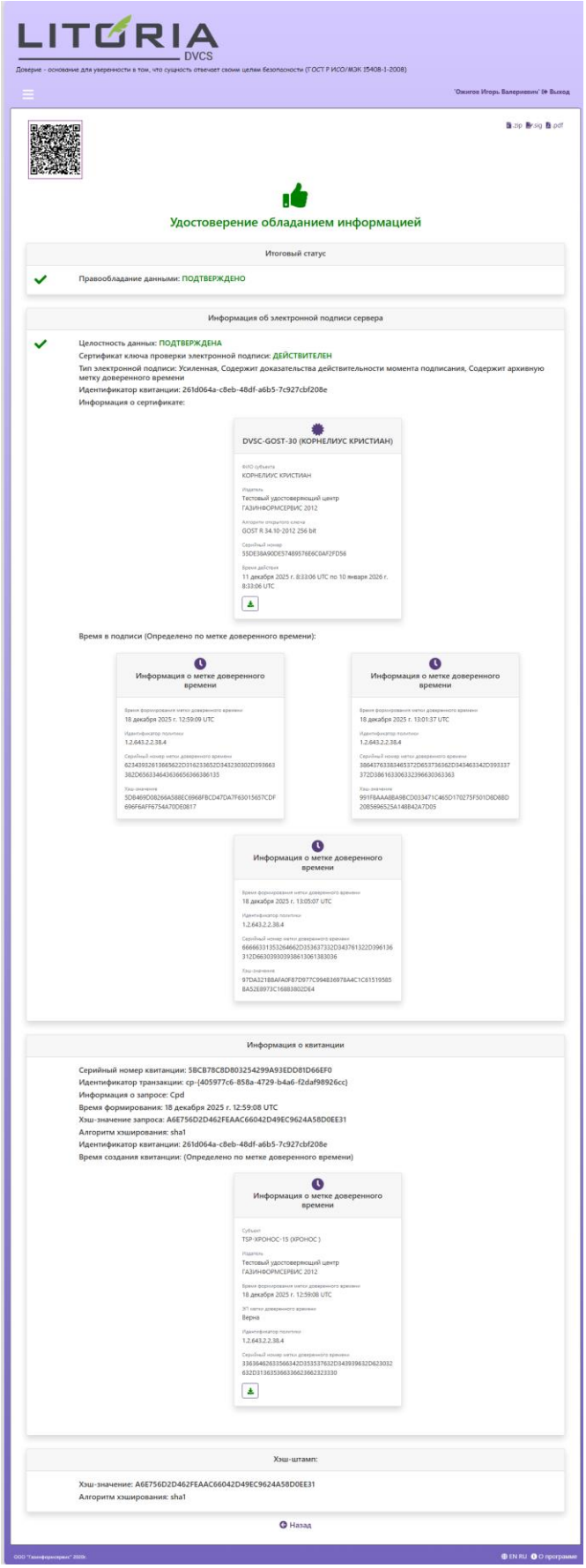


Рисунок 15 – Квитанция по отправленному запросу на проверку

Загрузка квитанции доступна по нажатию на ссылку с нужным форматом в правом верхнем углу « .zip .sig .pdf » (см. пункт 3.4.8).

При наличии МЧД сертификата службы DVCS в квитанции будут отражены следующие данные (рисунок 16):

– серийный номер доверенности;
– ссылка на местонахождение доверенности;
– ИНН доверителя;
– ИНН представителя.

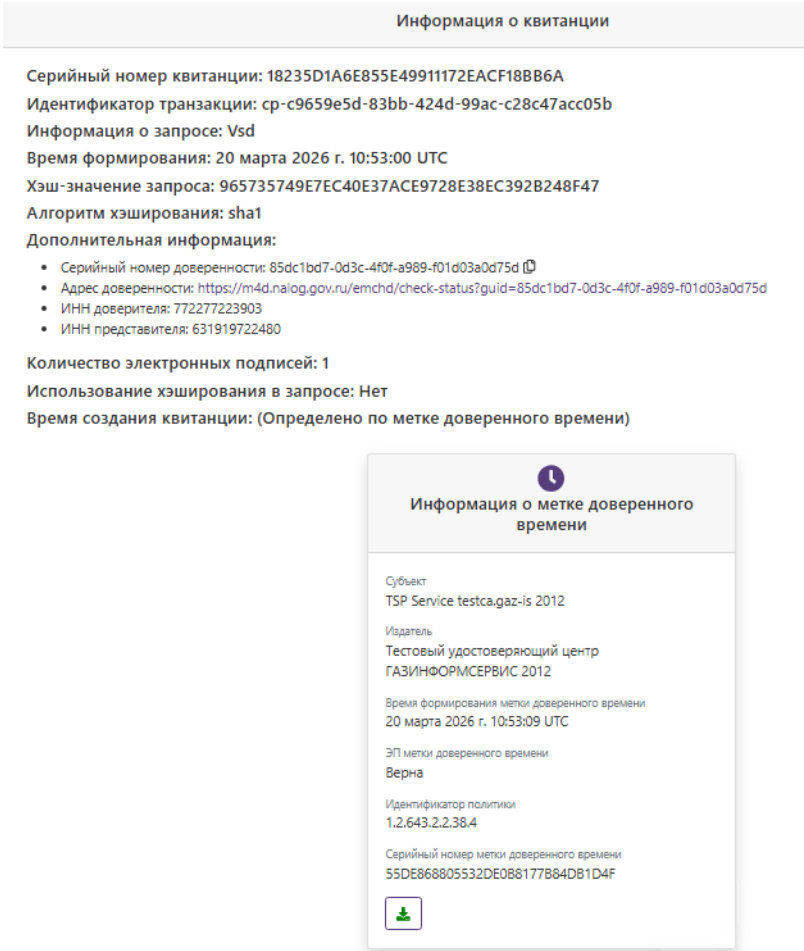


Рисунок 16 – Отображение в информации о квитанции МЧД сертификата службы DVCS

3.4.2 Проверка сертификата

Для проверки срока действия сертификатов ключей проверки:

1) Перейдите в пункт меню ***«Проверить»,*** во вкладку ***«Проверить документ»*** (рисунок 13) и поместите сертификат, который необходимо проверить в область ***«Подписанный документ, сертификат, документ»*** (рисунок 17). Данную операцию можно выполнить несколькими способами:
   – нажатием на ссылку ***«Подписанный документ, сертификат, документ»*** и выбором необходимого файла в открывшемся окне;

– перетаскиванием файла из окна Проводника в область ***«Подписанный документ, сертификат, документ».***

Примечание. При добавлении сертификата для проверки срока действия, в области ***«Подписанный документ, сертификат, документ»***, указывается его тип – «*Сертификат*» (рисунок 17).

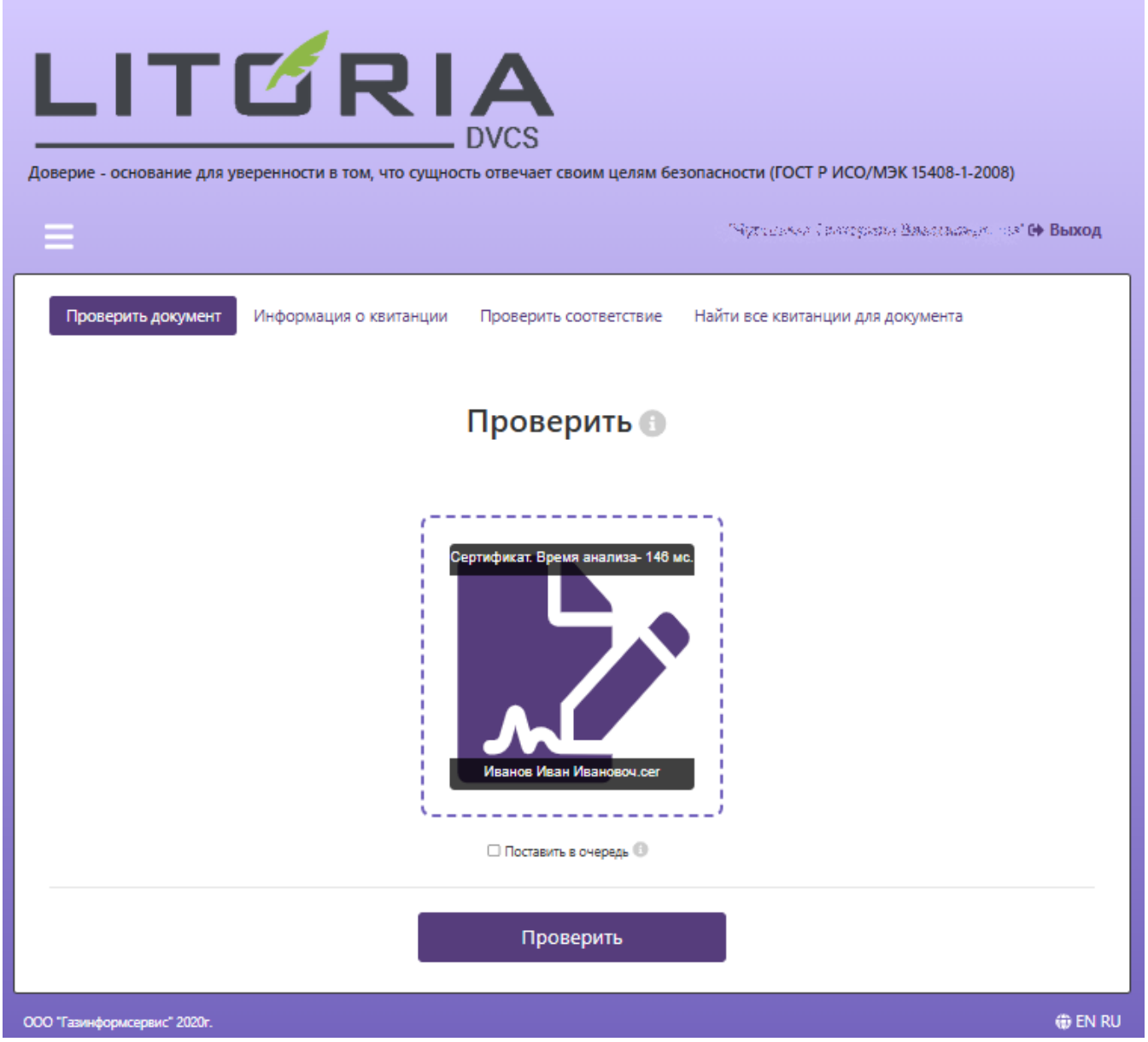


Рисунок 17 – Проверка срока действия сертификатов ключей проверки

2) Нажмите на кнопку «***Проверить***» для отправки сертификата на проверку.
3) При успешном завершении проверки сертификата на экране отобразится ответная квитанция службы DVCS, содержащая информацию в проведенных проверках (рисунки 18, 19).

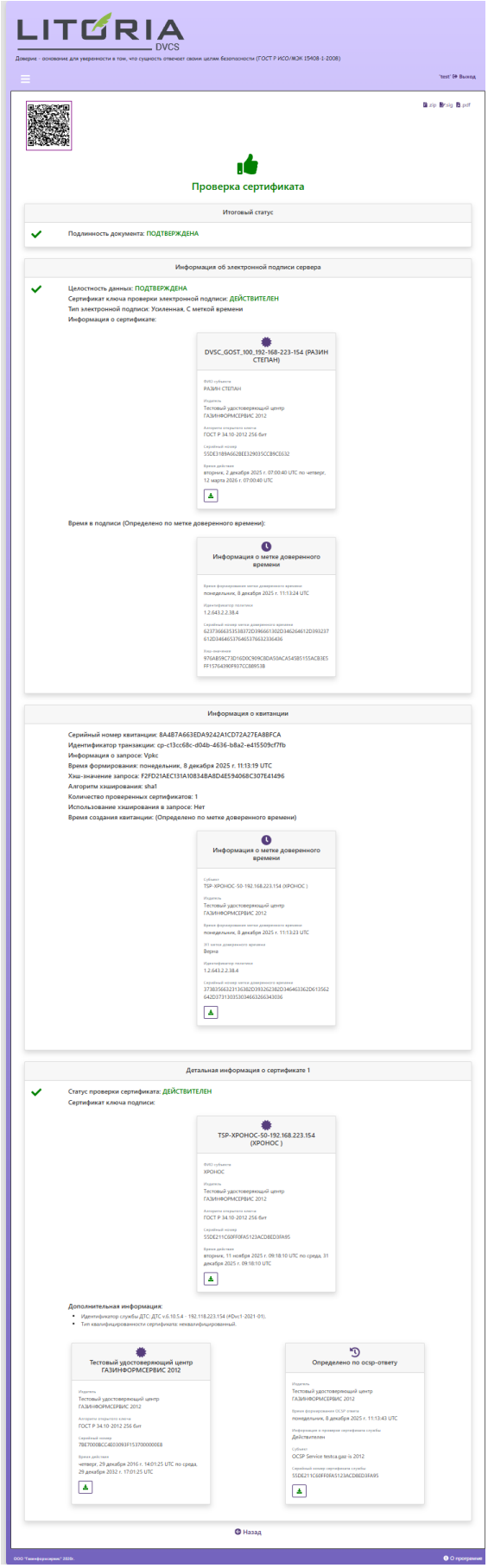


Рисунок 18 – Квитанция по отправленному запросу на проверку положительная

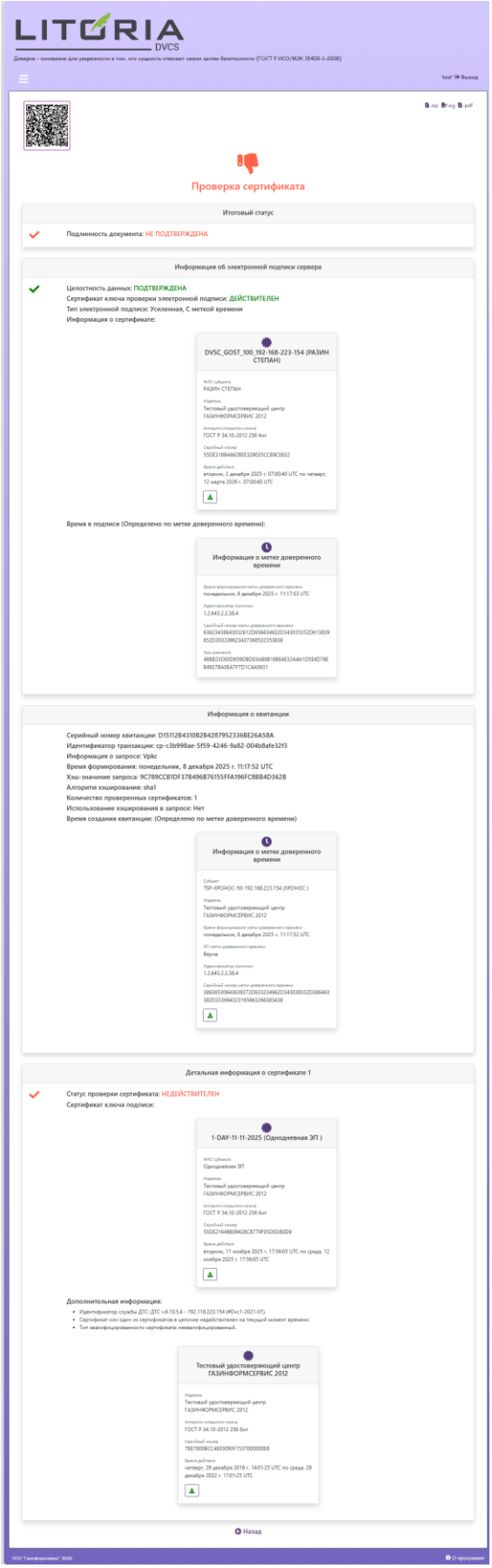


Рисунок 19 – Квитанция по отправленному запросу на проверку отрицательная

Загрузка квитанции доступна по нажатию на ссылку с нужным форматом в правом верхнем углу « .zip .sig .pdf » (см. пункт 3.4.8).

3.4.3 Проверка подписанного документа

Для подтверждения действительности ЭП документа:

1) Перейдите в пункт меню ***«Проверить»,*** во вкладку ***«Проверить документ»*** (рисунок 13) и поместите документ, который необходимо проверить в область ***«Подписанный документ, сертификат, документ»*** (рисунок 20). Данную операцию можно выполнить несколькими способами:
   – нажатием на ссылку ***«Подписанный документ, сертификат, документ»*** и выбором необходимого файла в открывшемся окне;
   – перетаскиванием файла из окна Проводника в область ***«Подписанный документ, сертификат, документ».***

Примечание. При добавлении подписанного документа для подтверждения действительности ЭП документа, в области ***«Подписанный документ, сертификат, документ»***, указывается его тип – «*Подписанный документ*», а также формат, в случае добавления подписанного PDF и XAdES (рисунок 20).

Рисунок 20 – Проверка действительности ЭП документа

2) При проверке отделенной подписи появится дополнительная область для ввода исходных данных отделенной подписи «***Исходный документ (для отделенной подписи)».***

Примечание. В области ***«Подписанный документ, сертификат, документ»*** дополнительно указывается информация о том, что подпись «Отделенная» (рисунок 21).

При проверке отделенной подписи вместо исходного файла можно добавлять его хеш-значение. Для этого после добавления данных на проверку раскройте ссылку ***Дополнительные параметры*** и введите хеш-значение исходного файл в формате HEX (рисунок 21).

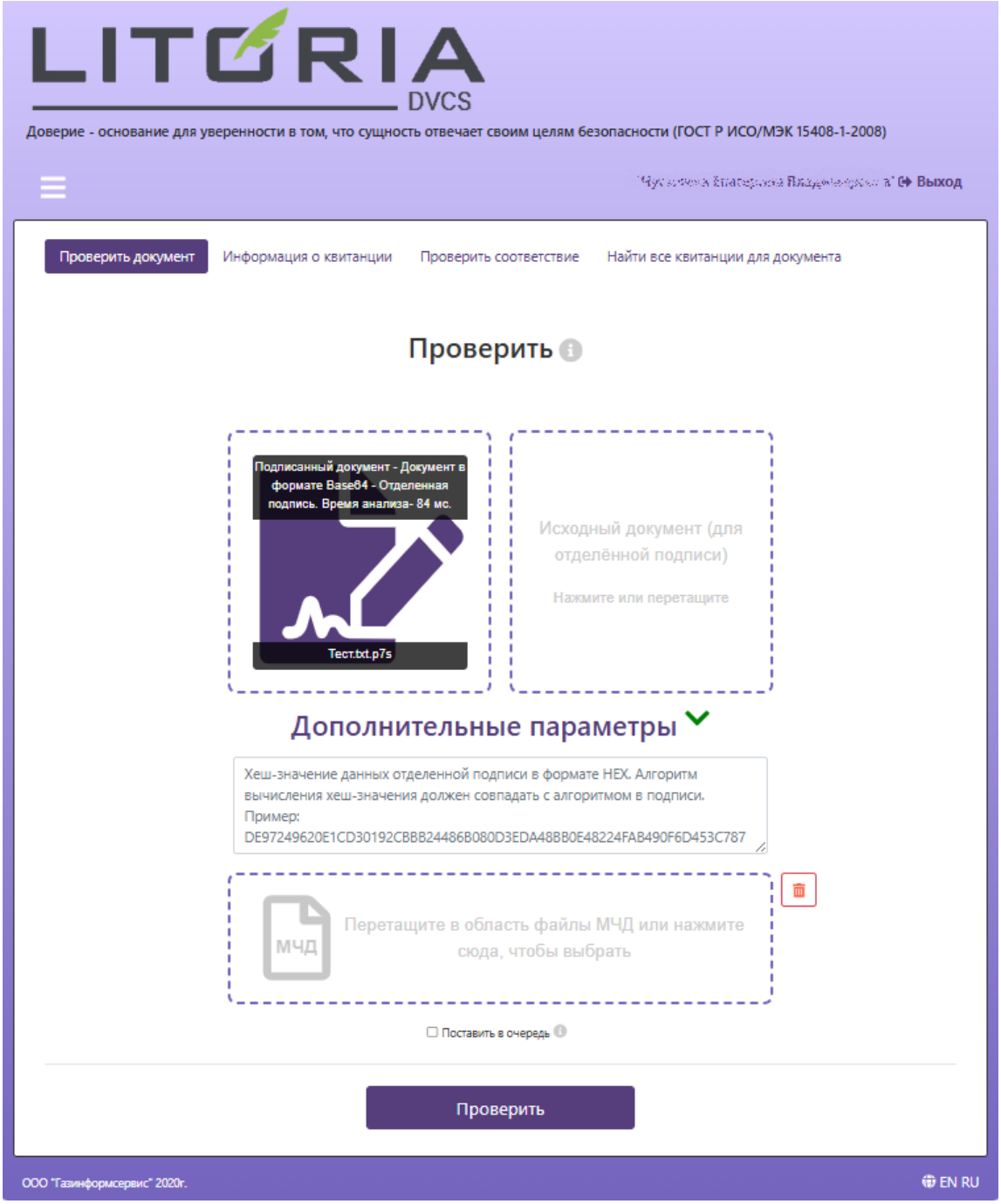


Рисунок 21 – Проверка отделенной подписи с хеш-значением исходного файла

3) Нажмите на кнопку «***Проверить***» для отправки документа на проверку.
4) При успешном завершении проверки подписи документа на экране отобразится ответная квитанция службы DVCS, содержащая информацию в проведенных проверках (рисунки 22, 23).

Рисунок 22 – Квитанция по отправленному запросу на проверку положительная

Рисунок 23 – Квитанция по отправленному запросу на проверку отрицательная

Загрузка квитанции доступна по нажатию на ссылку с нужным форматом в правом верхнем углу « .zip .sig .pdf » (см. пункт 3.4.8).

3.4.3.1 Проверка документа на соответствие полномочиям, определенным МЧД

Возможность проверки полномочий предназначена для регулирования доступа к проверяемым документам. Проверка полномочий участников электронного взаимодействия выполняется путем анализа МЧД.

МЧД – доверенность, созданная в электронной форме и подписанная электронной подписью лица, уполномоченного на действия от имени участника информационного обмена без доверенности. В МЧД указываются именно те полномочия, которые руководитель доверяет конкретному представителю.

При наличии машиночитаемой доверенности осуществляется проверка соответствия полномочий, определенных МЧД, в соответствии с требованиями Федерального закона № 63-ФЗ и соответствующих подзаконных актов.

ПК «Litoria DVCS» поддерживает следующие форматы МЧД:

– Формат 002;
– Формат 003 (EMCHD_1);
– Формат ФНС 5.01.

Для выполнения операции проверки документа на соответствие полномочиям, определенным МЧД:

1) Перейдите в пункт меню ***«Проверить»*** во вкладку ***«Проверить документ».***
2) Поместите документ, который необходимо проверить, в область ***«Подписанный документ»*** и добавьте машиночитаемую доверенность в область «***МЧД***» (рисунок 24).

Примечание. В «ПК «Litoria DVCS» возможна проверка множественной ЭП с МЧД. Для добавления нескольких МЧД необходимо выделить все МЧД, для которых будет выполняться проверка, и нажать кнопку «*Открыть*». В области «***МЧД***» отобразятся все добавленные машиночитаемые доверенности (рисунки 25, 27).

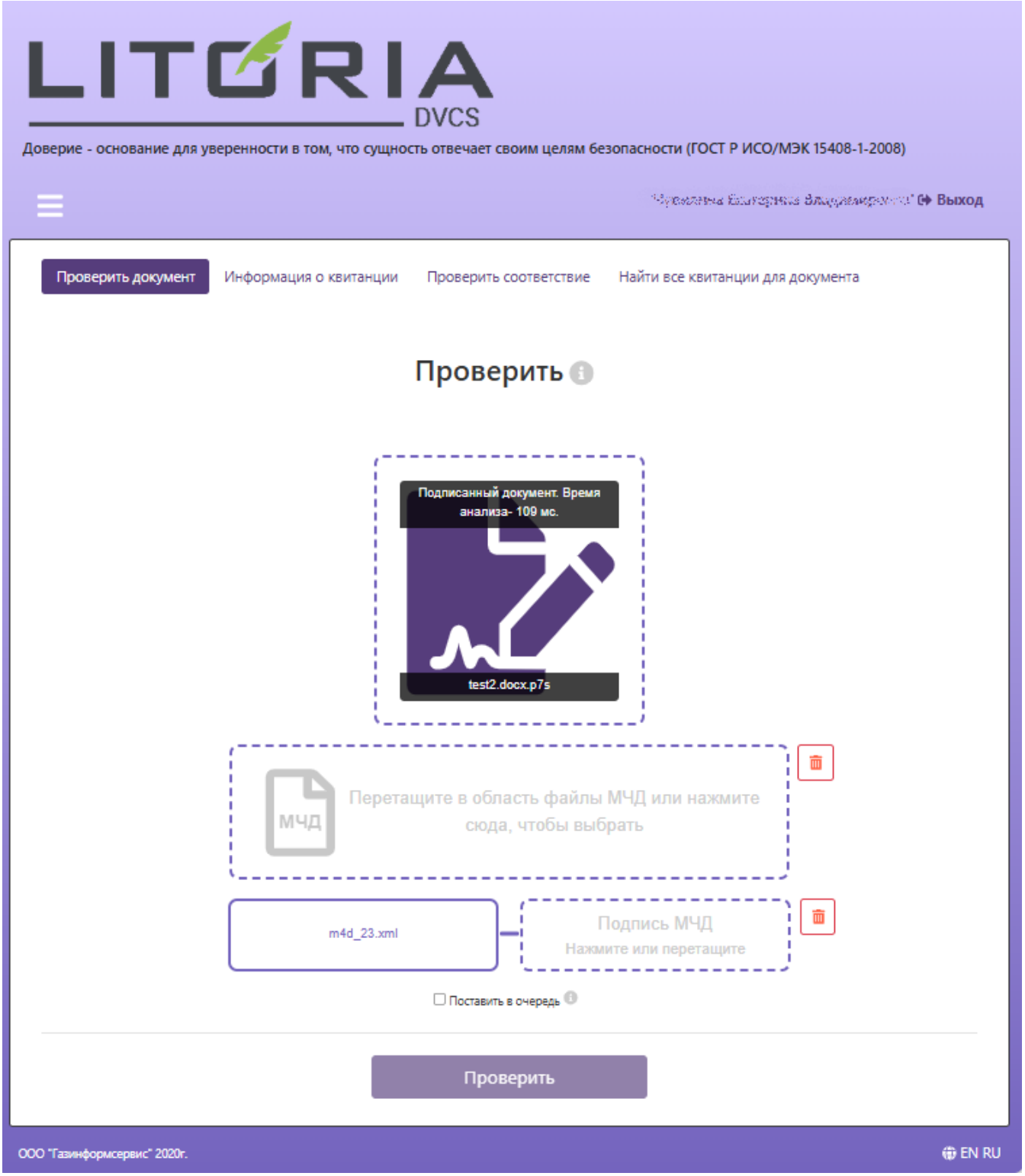


Рисунок 24 – Проверка документа с МЧД

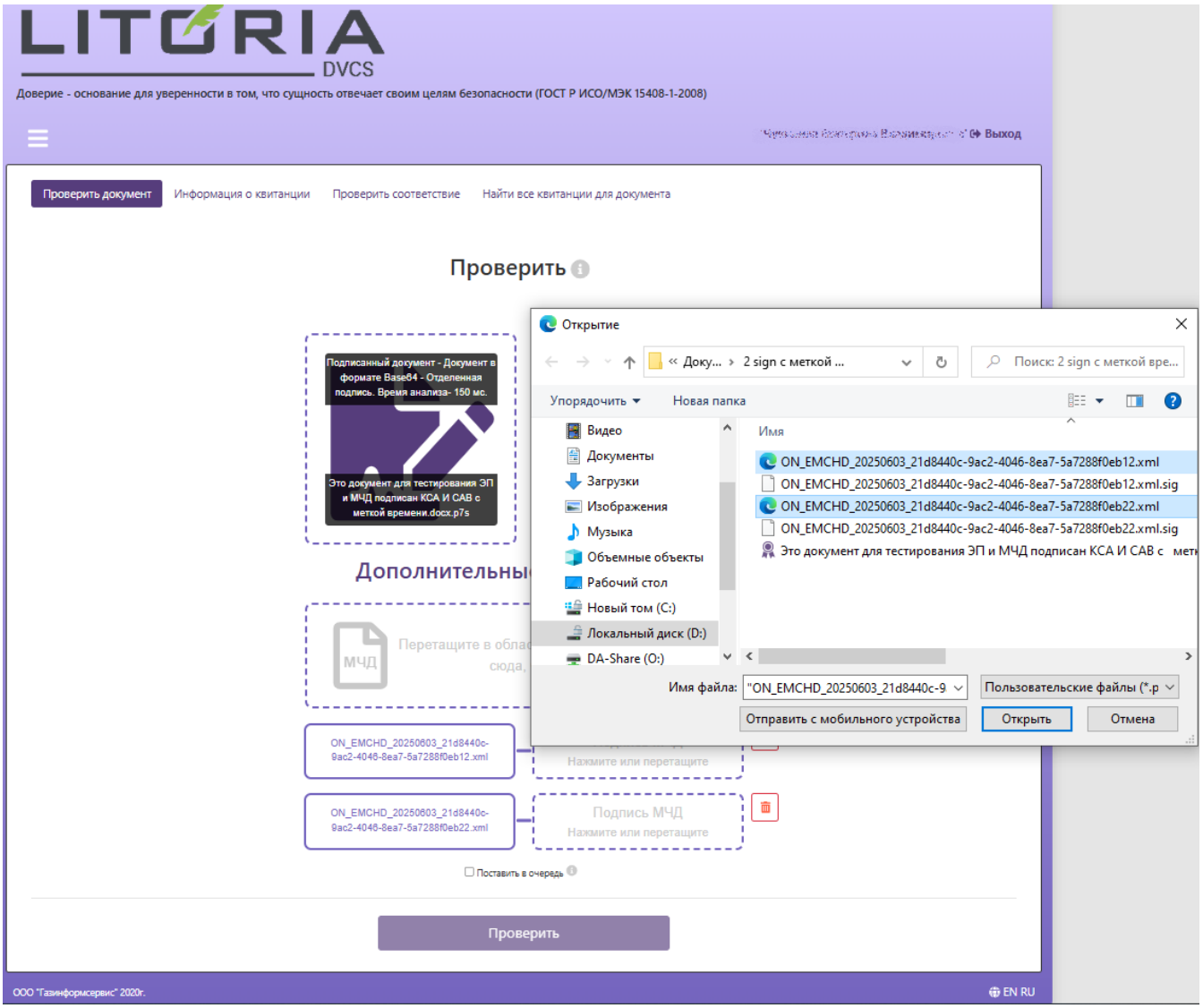


Рисунок 25 – Проверка документа с несколькими МЧД

3) Проверка документа на соответствие полномочиям, определенным МЧД, может выполняться также для МЧД, подписанной отделенной подписью в формате CAdES. Для проверки необходимо в соответствующие поля добавить подписанный файл, МЧД в формате xml и исходные данные для отделенной подписи МЧД в области «*Отделенная подпись МЧД*» (рисунок 26).

Рисунок 26 – Проверка документа с отделенной подписью МЧД

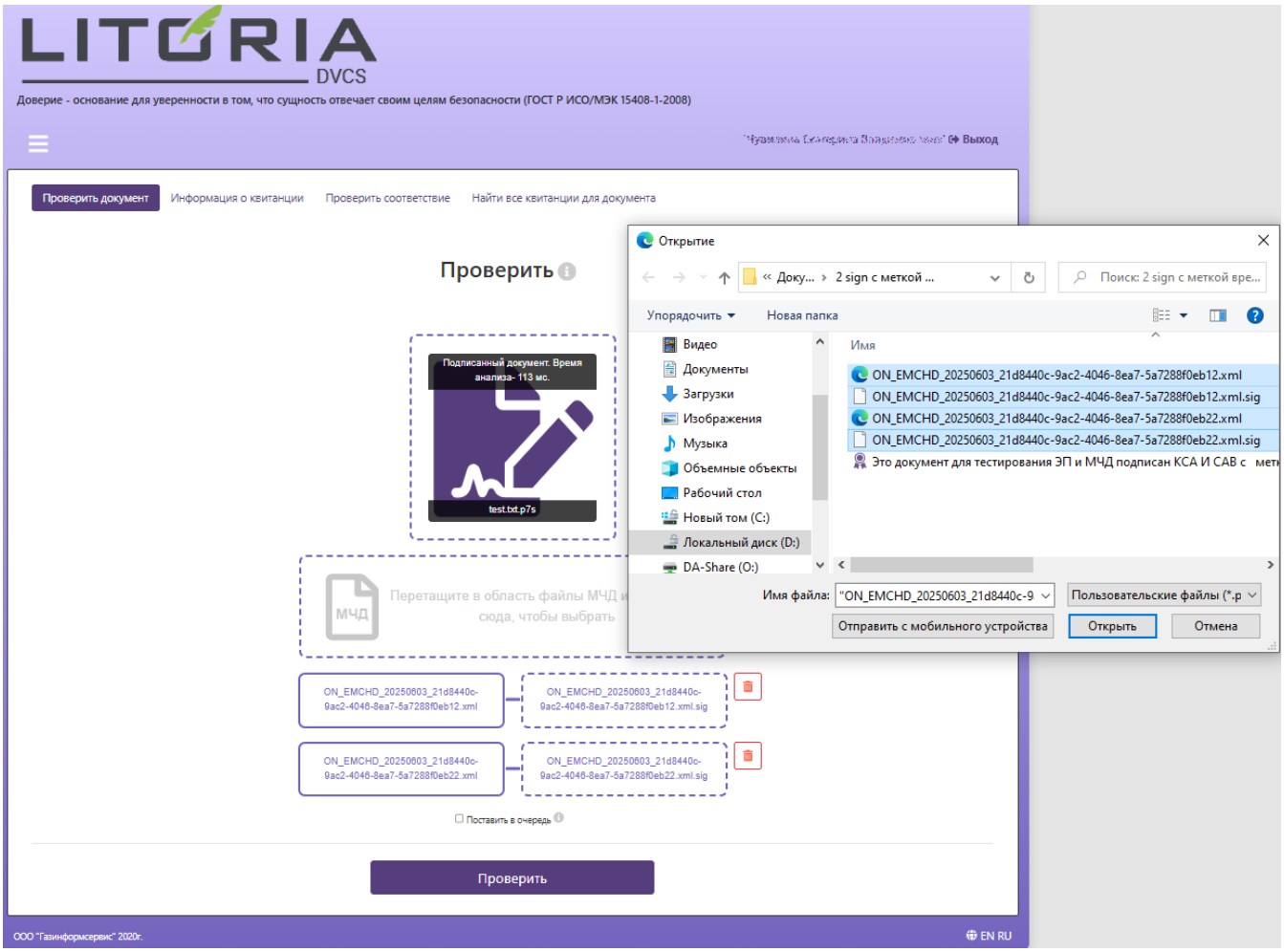


Рисунок 27 – Проверка документа с несколькими МЧД с отделенной подписью

4) Нажмите на кнопку «***Проверить***» для отправки документа на проверку.

При проверке документа на соответствие полномочиям, определенным МЧД, в квитанции добавляется область «*Информация о машиночитаемой доверенности*», в которой отображается статус проверки доверенности, сведения о доверенном лице и доверителе, дата выпуска и дата окончания действия МЧД, статус регистрации МЧД в реестре ФНС, статус отзыва МЧД и список полномочий (рисунки 28, 29).

Отображение списка полномочий будет различаться в зависимости от выбранных параметров в процессе создания МЧД: полномочия из справочника (рисунок 28) или полномочия в свободной форме (рисунок 29).

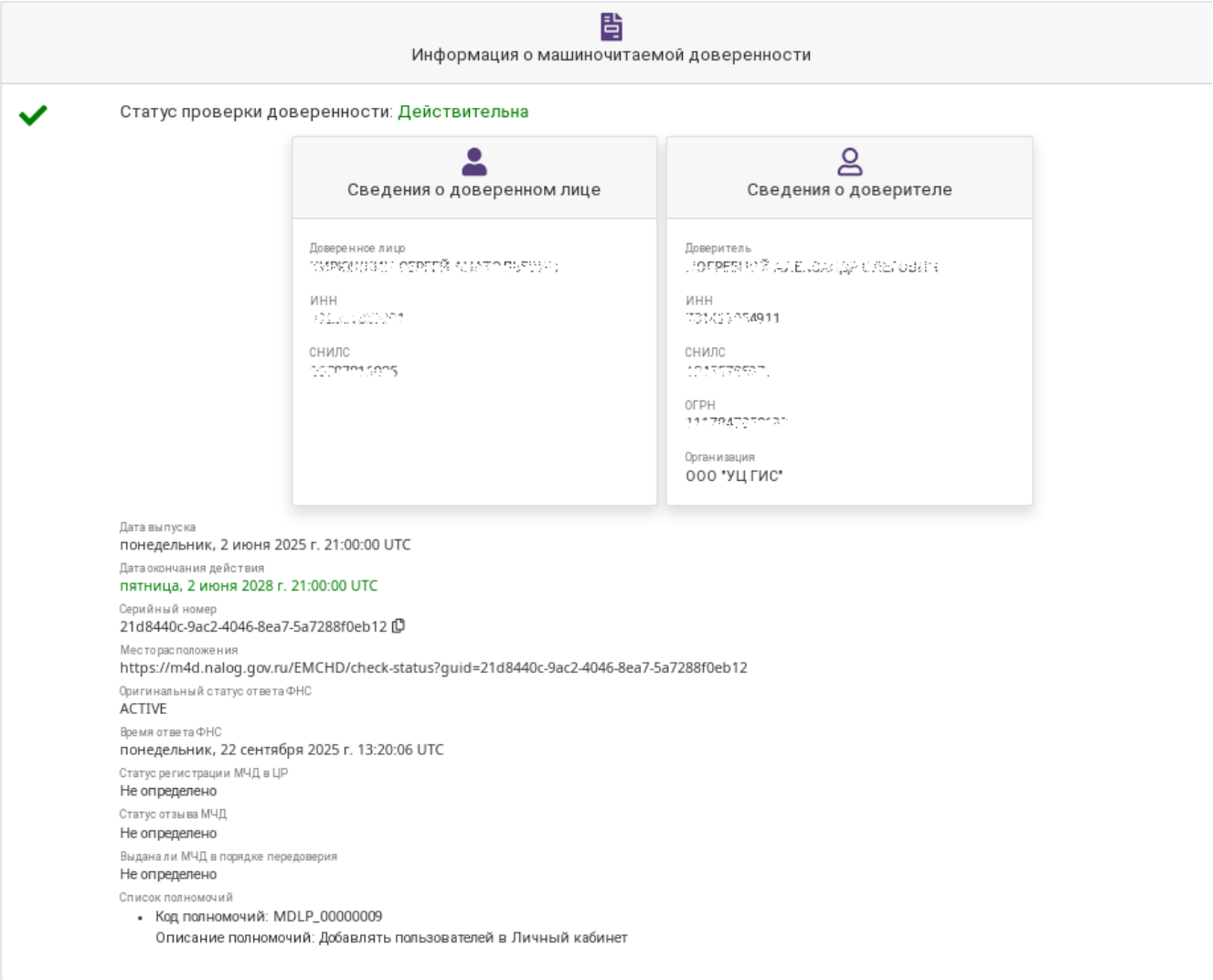


Рисунок 28 – Проверка документа на соответствие полномочиям, определенным МЧД

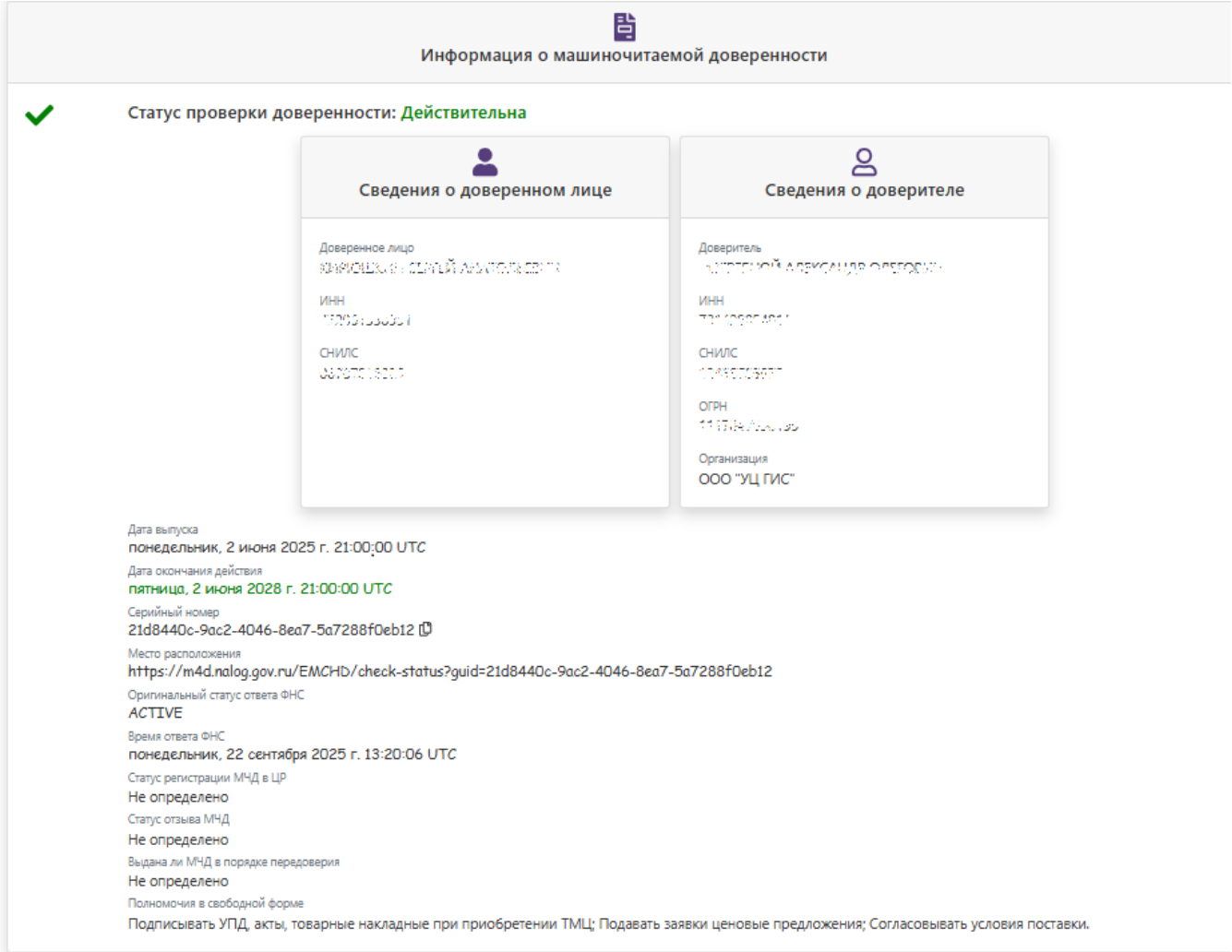


Рисунок 29 – Проверка документа на соответствие полномочиям, определенным МЧД

Принимаемый статус проверки доверенности:

- «Действительна»;
- «Ошибка разбора xml документа»;
- «Ошибка разбора структуры МЧД»;
- «Подписанты отсутствуют»;
- «Несколько подписантов»;
- «Не получилось провести проверку подписи»;
- «Ошибка проверки математической корректности документа»;
- «Ошибка валидации сертификата»;
- «МЧД выдана на другое лицо»;
- «Сертификат подписанта МЧД не соответствует тому, с которым МЧД зарегистрирована в узле ФНС».

3.4.3.2 Проверка МЧД в распределенном реестре ФНС

При проверке документа на соответствие полномочиям, определенным МЧД, может выполняться дополнительная проверка МЧД в распределенном реестре ФНС.

Для выполнения проверки МЧД в реестре ФНС необходимо обратиться к администратору безопасности для выполнения настроек в конфигурационном файле службы DVCS ***«appsettings.json»***.

Если в конфигурационном файле настройки подключения к реестру ФНС заданы, то при проверке МЧД служба DVCS по указанным аутентификационным данным пользователя попытается обратиться по заданному адресу в реестр ФНС, и по серийному номеру доверенности запросит в реестре ФНС информацию о данной доверенности.

Служба DVCS запрашивает наличие доверенности в реестре ФНС и, при ее наличии, в каком состоянии находится доверенность: отозвана или действительна.

Запрашиваемые данные отображаются в квитанции (рисунок 30):

– в поле «*Статус регистрации МЧД в ЦР*» – наличие доверенности в реестре ФНС;
– в поле «*Статус отзыва МЧД*» – состояние доверенности.

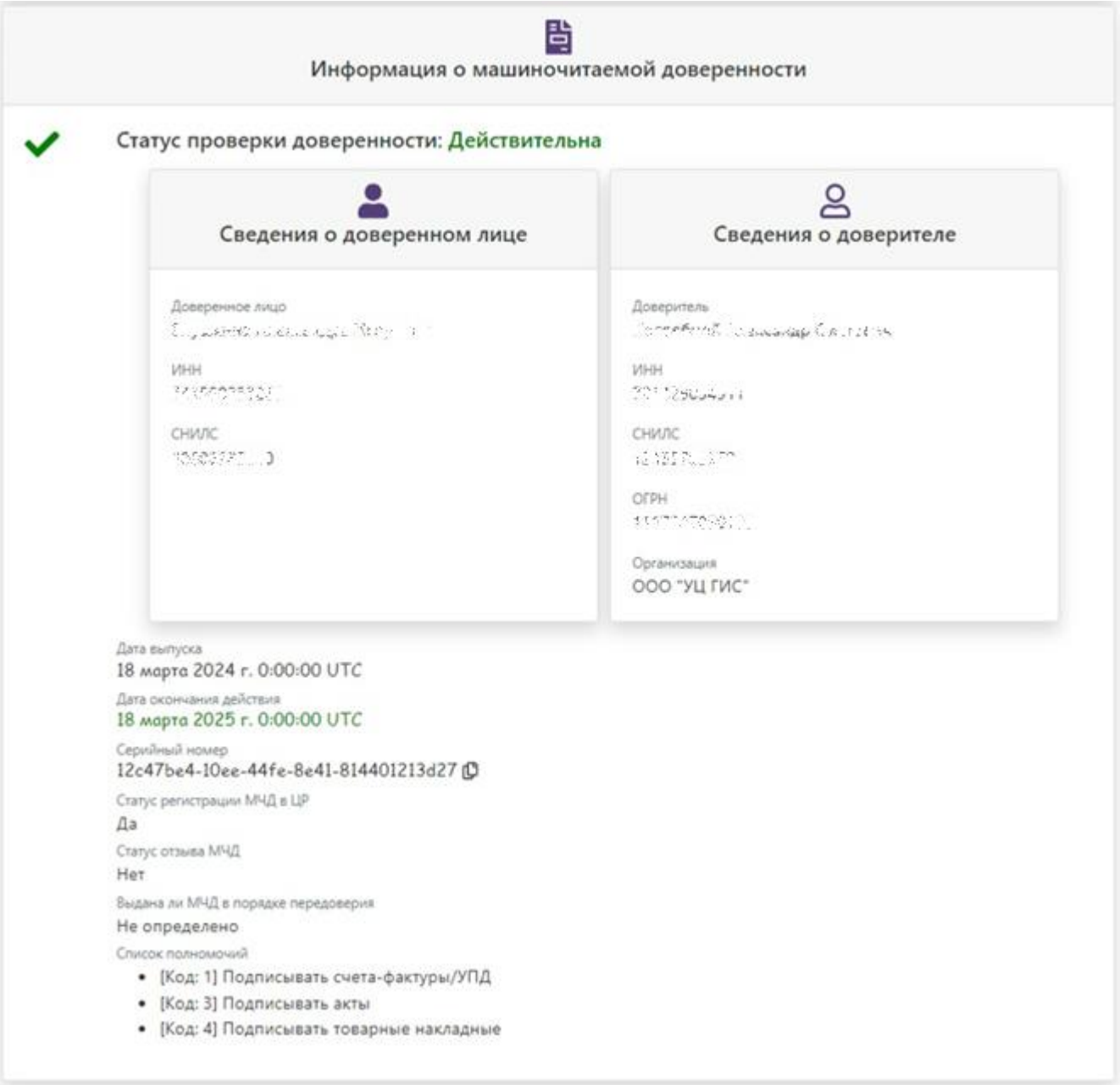


Рисунок 30 – Проверка МЧД в реестре ФНС

Если МЧД по заданному серийному номеру не найдена в реестре ФНС, состояние доверенности в поле «*Статус отзыва МЧД*» будет не определено (рисунок 31).

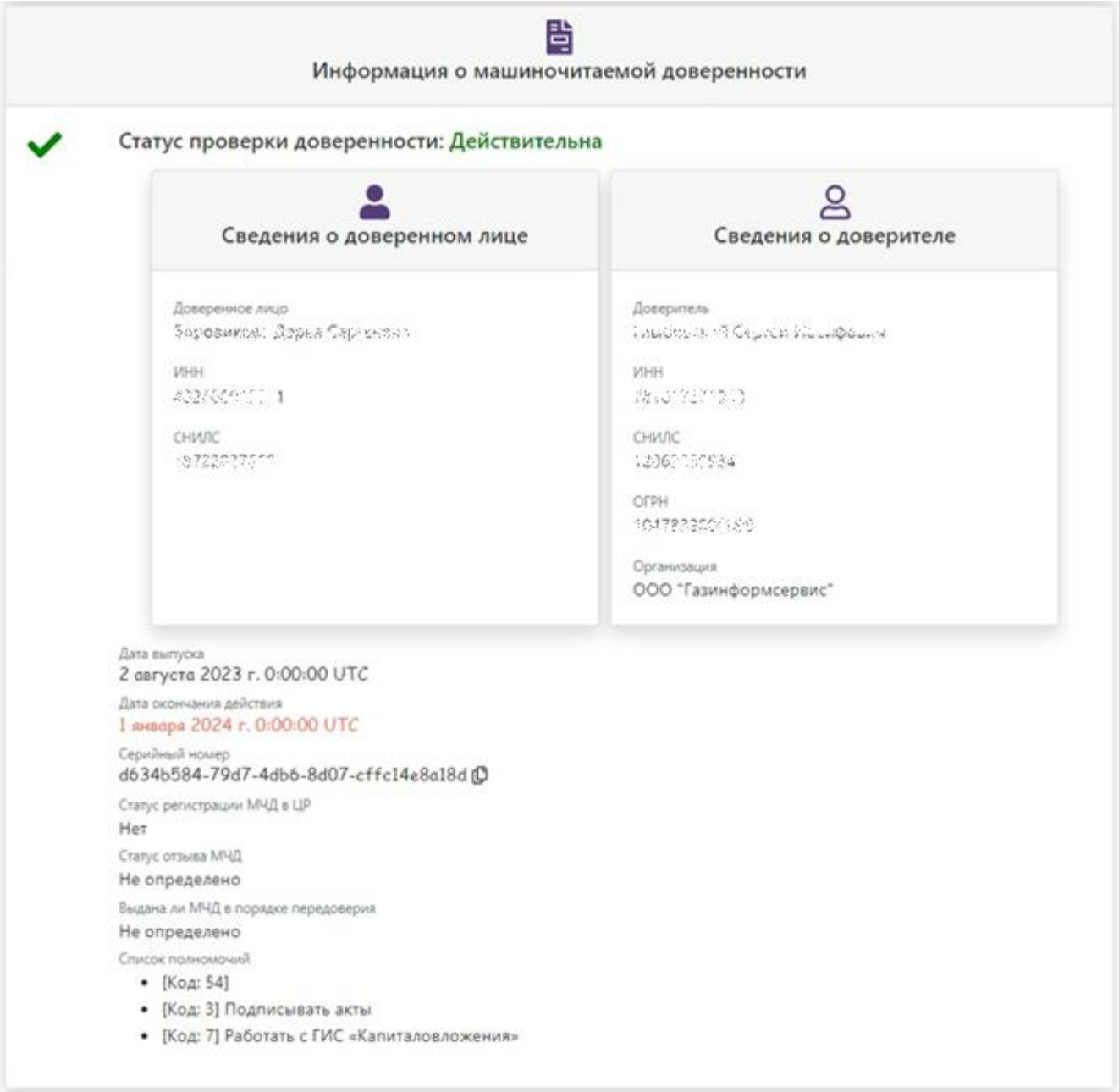


Рисунок 31 – МЧД не найдена в реестре ФНС

3.4.4 Постановка запроса в очередь

Для постановки запроса в очередь:

1) Перейдите в пункт меню ***«Проверить»,*** во вкладку ***«Проверить документ»*** (рисунок 13) и поместите документ, который необходимо проверить в область ***«Подписанный документ, сертификат, документ»*** (рисунок 14). Данную операцию можно выполнить несколькими способами:
   – нажатием на ссылку ***«Подписанный документ, сертификат, документ»*** и выбором необходимого файла в открывшемся окне;
   – перетаскиванием файла из окна Проводника в область ***«Подписанный документ, сертификат, документ».***
2) Установите флаг ***«Поставить в очередь»*** (рисунок 32).

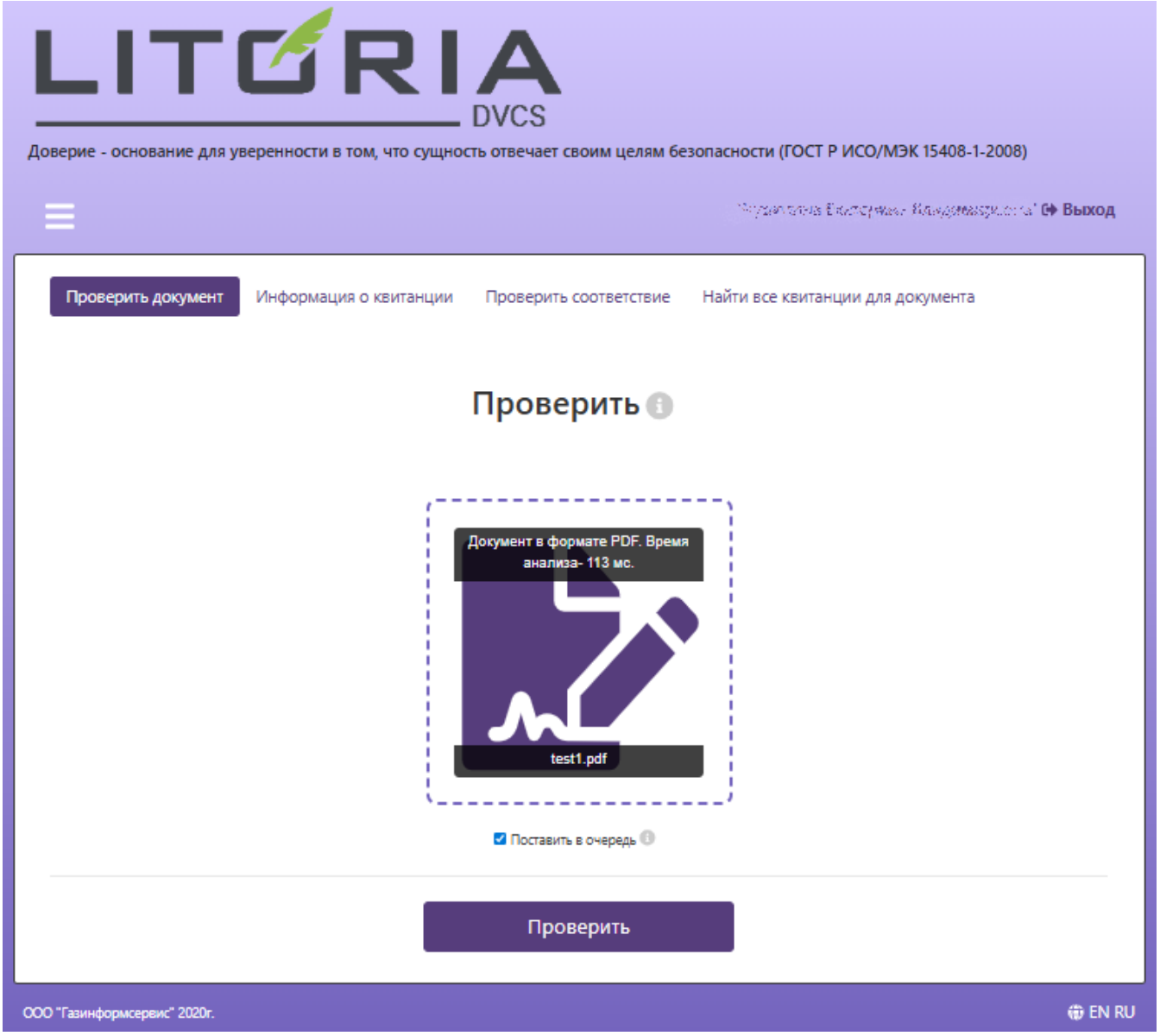


Рисунок 32 – Постановка запроса в очередь

Примечание. При использовании ПК «Litoria DVCS» в режиме пробной версии продукта данная функциональная возможность будет недоступна.

3) Нажмите на кнопку «***Проверить***» для отправки документа на проверку.
4) Произойдет перенаправление на вкладку ***«Задачи»*** (рисунок 33).

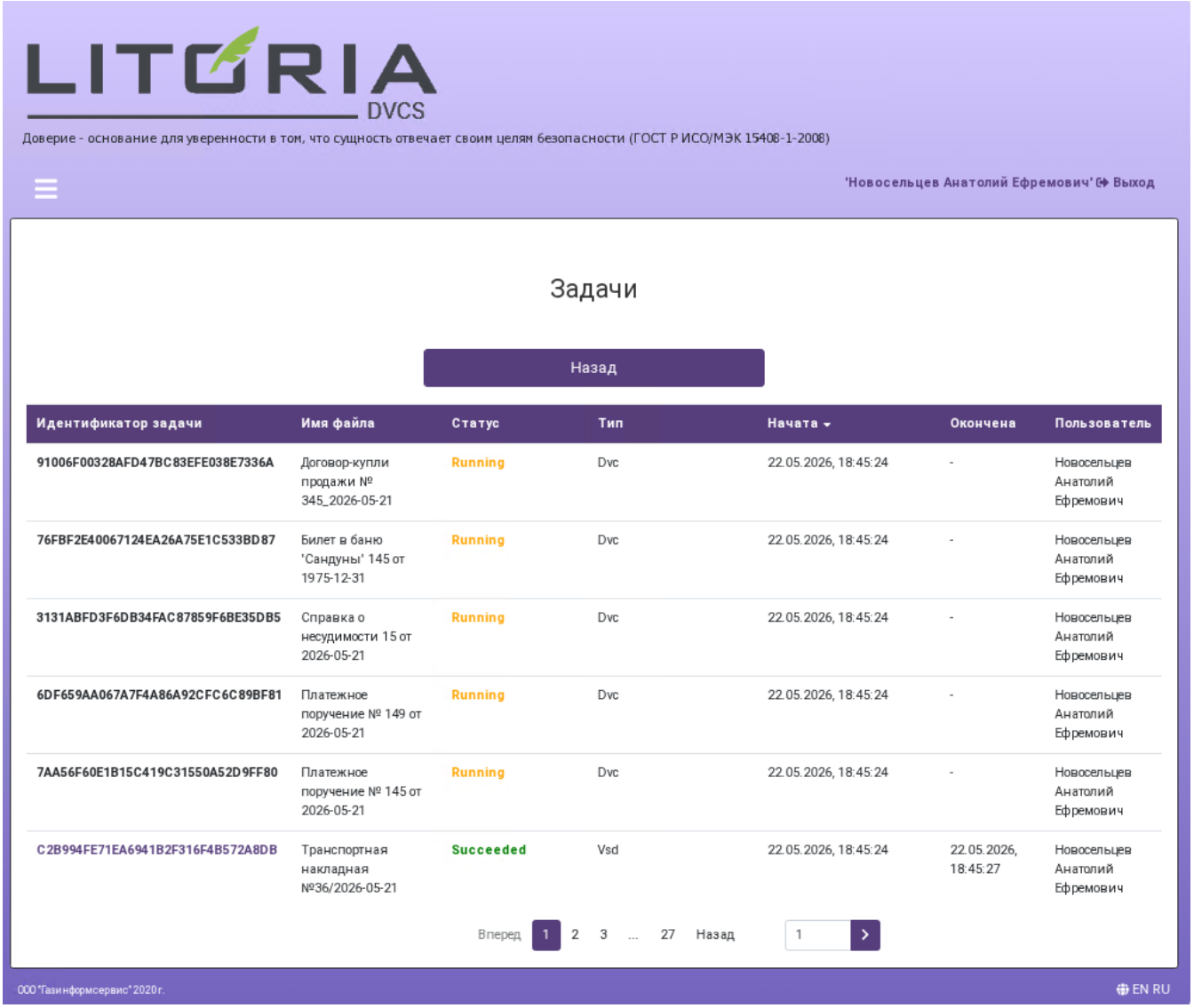


Рисунок 33 – Вкладка «Задачи»

5) Отслеживайте статус выполнения задачи на вкладке ***«Задачи»*** – он обновляется автоматически (рисунок 34).

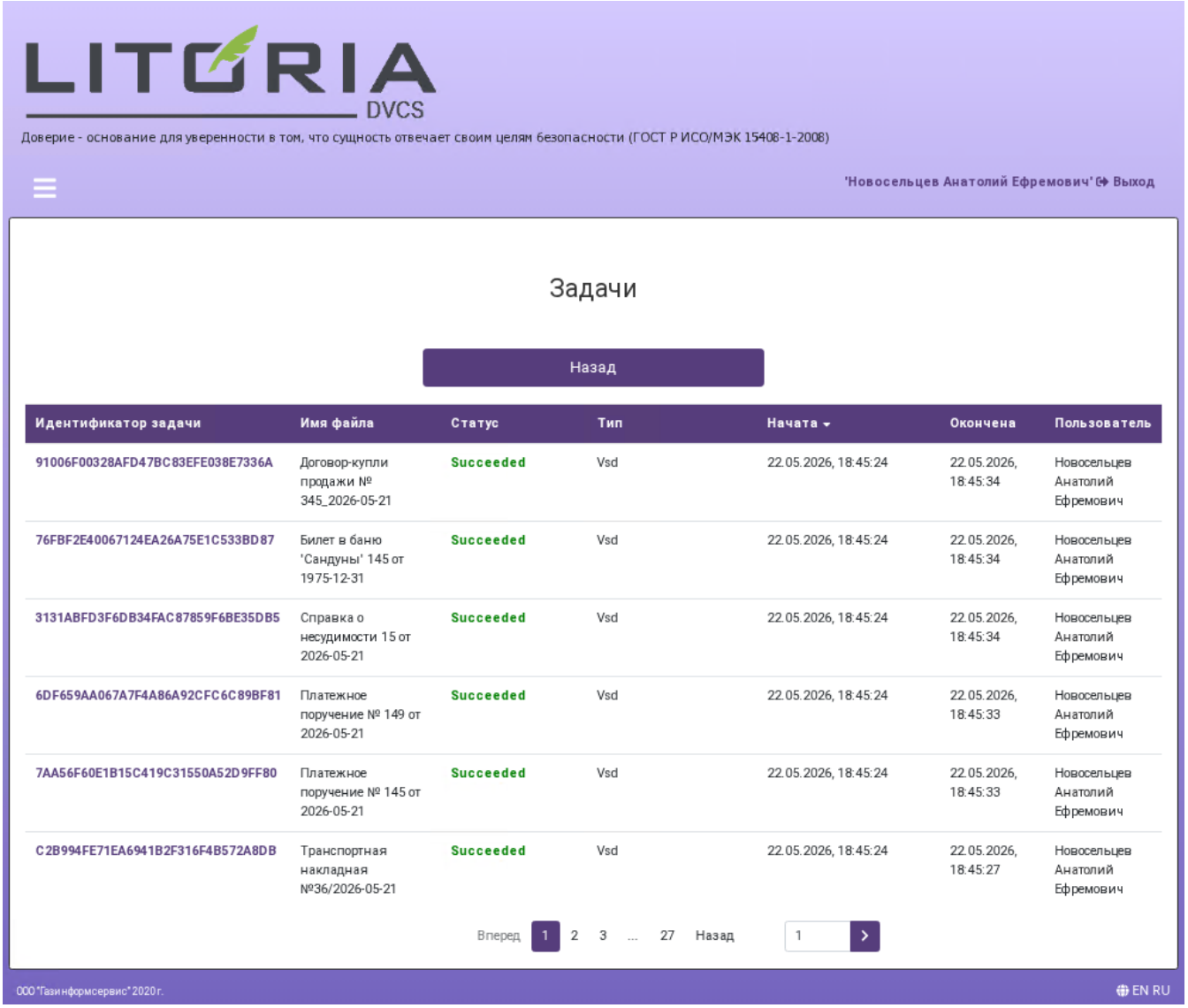


Рисунок 34 – Обновление статуса задачи

6) После завершения обработки задачи (статус `succeeded` или `failed`) перейдите по ссылке в столбце **«Идентификатор задачи»** (рисунок 34):
   – при статусе `succeeded` – для получения квитанции (рисунок 15);
   – при статусе `failed` – для получения ошибки в виде JSON-файла (рисунок 35).

Результат задачи


```
1 {
2   "ErrorTag": {
3     "ValB": false,
4     "Dsc": "Документ",
5     "Val": "Загруженный документ не может быть пустым"
6   },
7   "TransactionId": {
8     "Dsc": "Идентификатор транзакции",
9     "Val": "da967fd7-12c2-4f8b-9a3d-fbc7d5b721ca"
10  },
11  "VerifyType": 0,
12  "RequestLabel": "Ошибка операции"
13 }
```


Рисунок 35 – Ошибка в виде JSON-файла

Примечание. При успешном создании квитанции идентификатор задачи становится её серийным номером. Идентификатор задачи отображается в формате, соответствующем формату идентификатора квитанции.

Примечание. Описание статусов задач и порядок получения квитанции по идентификатору задачи см. в подразделе 3.6.

3.4.5 Информация о квитанции

Для просмотра информации о квитанции:

1) Перейдите в пункт меню ***«Проверить»,*** во вкладку ***«Информация о квитанции»*** и поместите квитанцию, которую необходимо просмотреть в область ***«Квитанция»*** (рисунок 36).

Рисунок 36 – Просмотр квитанции

2) Нажмите на кнопку «***Разобрать***» для просмотра загруженной квитанции.
3) На экране отобразится содержание загруженной квитанции службы DVCS (рисунок 15). Загрузка квитанции доступна по нажатию на ссылку с нужным форматом в правом верхнем углу « .zip .sig .pdf » (см. пункт 3.4.8).

Примечание. Возможен просмотр любой квитанции, сформированной в соответствии с требованиями RFC3029.

3.4.6 Проверка соответствия подписанного документа и квитанции

Для проверки соответствия подписанного документа и квитанции:

1) Перейдите в пункт меню ***«Проверить»,*** во вкладку ***«Проверить соответствие»*** и поместите подписанный документ и квитанцию, соответствие которых необходимо проверить в область ***«Подписанный документ»*** и ***«Квитанция»*** соответственно (рисунок 37).

Рисунок 37 – Проверка соответствия квитанции и подписанного документа

2) При проверке отделенной подписи, добавьте исходные данные для отделенной подписи в область «***Исходный документ (для отделенной подписи)***».

Примечание. В области ***«Подписанный документ»*** дополнительно указывается информация о том, что подпись «Отделенная» (рисунок 37).

---

3) Нажмите на кнопку «***Проверить***» для выполнения операции соответствия.
4) На экране отобразится информация о соответствии проверяемого документа добавленной квитанции (рисунок 38).

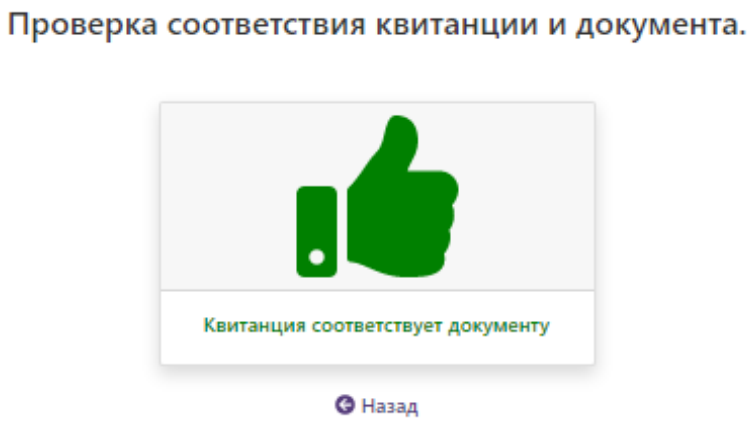


Рисунок 38 – Квитанция соответствует загруженному документу

3.4.7 Поиск квитанций по документу

Поиск квитанции можно осуществить для:

- подписанного документа;
- файла сертификата;
- любого файла, для которого выполнялся запрос типа CPD.
- файла отделенной подписи (с указанием исходных данных, для которых создавалась отделенная подпись).

Для поиска квитанций по документу:

1) Перейдите в пункт меню ***«Проверить»,*** во вкладку ***«Найти все квитанции для документа»*** и поместите документ, квитанции которого необходимо найти в область ***«Подписанный документ»*** (рисунок 39).
2) Если необходимо осуществить поиск для файла отделенной подписи, то также укажите исходные данные отделенной подписи в области ***«Исходный документ (для отделенной подписи)».***

Примечание. В области ***«Подписанный документ, сертификат, документ»*** дополнительно указывается информация о том, что подпись «Отделенная» (рисунок 39).

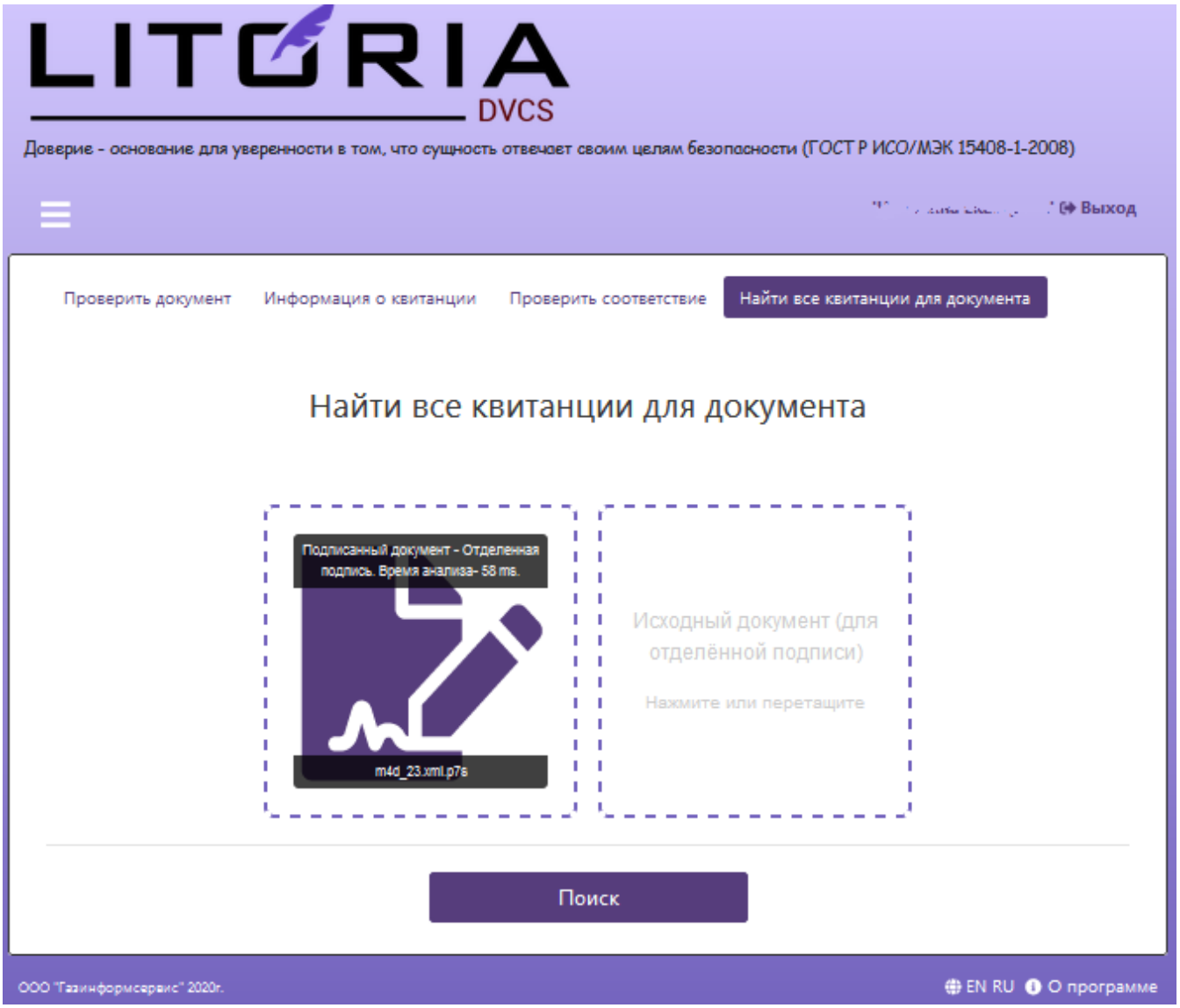


Рисунок 39 – Поиск квитанций подписанного документа

3) Нажмите на кнопку «***Поиск***» для выполнения поиска.
4) На экране отобразится список всех квитанций проверяемого документа (рисунок 40). Операции, доступные в журнале «***Архив***» описаны в подразделе «Архив».

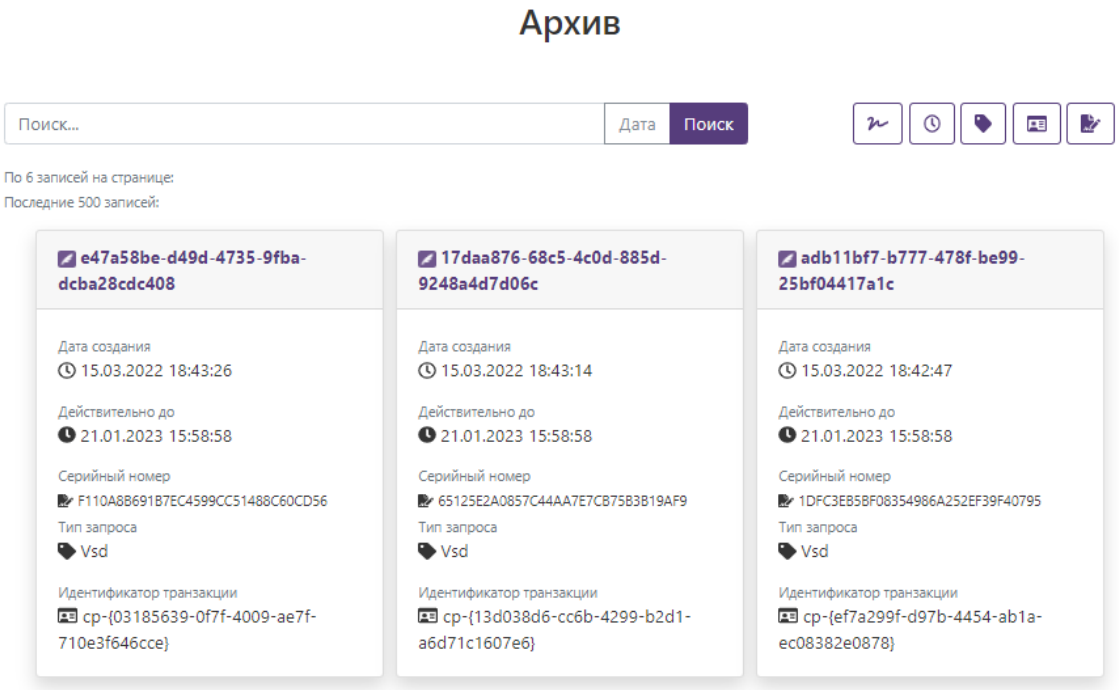


Рисунок 40 – Отображение квитанций искомого документа

Для просмотра квитанции необходимо в карточке нужной квитанции нажать на ссылку с ее номером (рисунок 40).

3.4.8 Загрузка квитанции

Для загрузки квитанции нажмите на ссылку с нужным форматом « .zip .sig .pdf » (рисунок 15). Тип расширения квитанции DVC и отделенной подписи в формате CMS устанавливается администратором комплекса (по умолчанию установлен тип расширения *«sig»)*.

При загрузке квитанции на рабочую станцию в формате *.zip*, сохраняется архив, содержащий в себе:

- квитанцию DVC в формате CMS в файле с расширением **.sig*;
- краткое отображение квитанции в файле с расширением **.pdf;*
- отделенную подпись в формате CMS с расширением **.sig*;
- краткое отображение квитанции в файле с расширением **.html*;
- полный разбор квитанции и саму квитанцию в формате BASE64 в файле с расширением **.json*.

3.5 Продление электронной подписи

Основное назначение функции продления ЭП – увеличение срока действия электронной подписи в документе путем включения в нее информации о времени создания подписи (штампа времени TSP).

Операции продления доступны администратору или пользователям в пункте меню ***«Продление ЭП»*** после успешного прохождения аутентификации в web-кабинете ПК «Litoria DVCS» (рисунок 41).

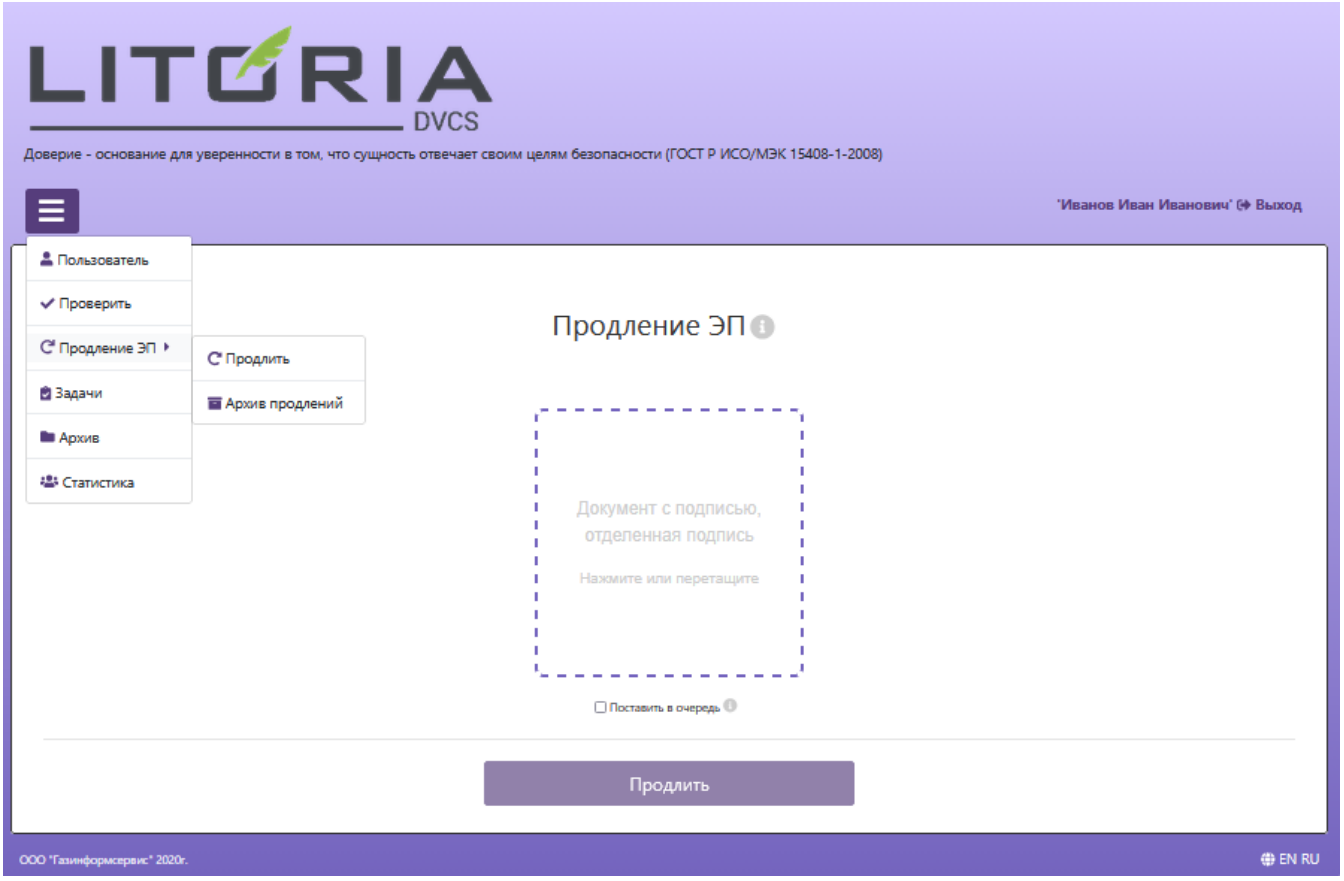


Рисунок 41 – Продление электронной подписи

Продление электронной подписи возможно в следующих режимах:

1) **Синхронное продление** – выполняется с удержанием активного сетевого соединения. После завершения операции происходит автоматическое скачивание файла с продленной подписью. Результат операции сохраняется в архиве продлений.
2) **Асинхронное продление** – выполняется с постановкой задачи в очередь без удержания сетевого соединения. Результат становится доступен для скачивания на странице «Задачи» после завершения обработки.

Для продления ЭП в синхронном режиме:

1) Перейдите в пункт меню ***«Продление ЭП»*** → ***«Продлить»*** (рисунок 42).

Рисунок 42 – Пункт меню «Продлить»

2) Поместите документ с ЭП в область загрузки файла. Добавление файла можно выполнить несколькими способами (рисунок 43):
   – нажатием на поле загрузки и выбором необходимого файла в открывшемся окне;
   – перетаскиванием файла из окна Проводника в область загрузки.

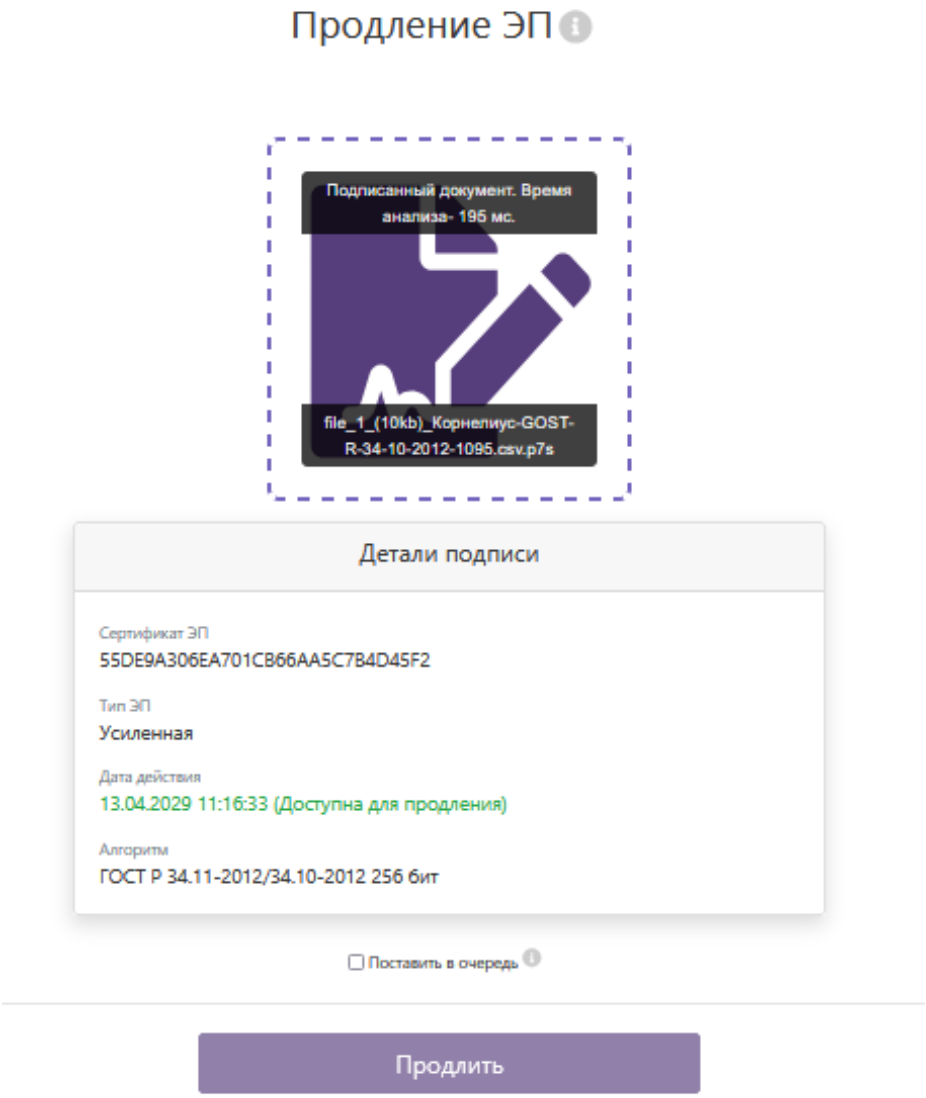


Рисунок 43 – Добавление документа с ЭП для продления

Примечание. При необходимости добавьте данные отделенной подписи в дополнительное поле ввода файла (рисунок 44).

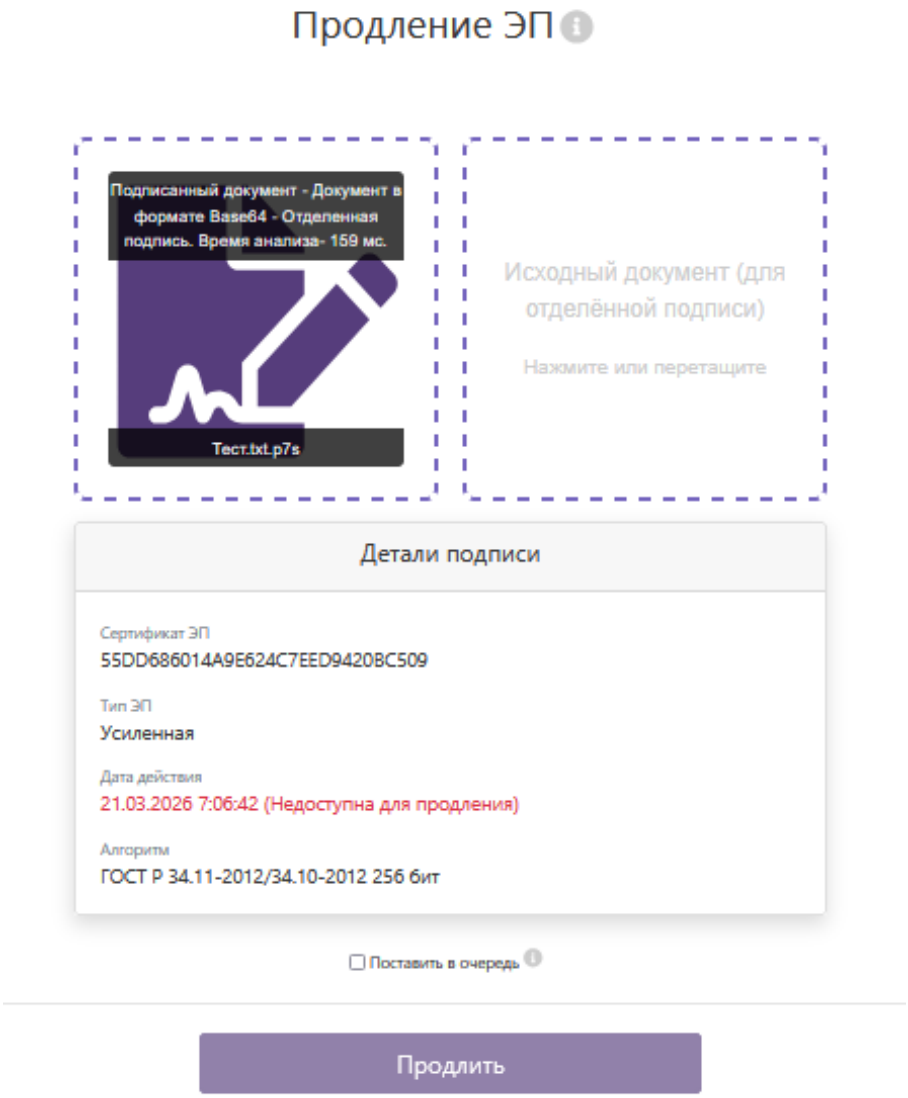


Рисунок 44 – Добавление документа с отделенной подписью

3) После загрузки файла ПК «Litoria DVCS» проанализирует подпись и выведет краткую информацию о подписи и возможности ее продления:
   – если подпись просроченная (рисунок 44) или не является CAdES (рисунок 45), продление невозможно;
   – если подпись действительна и соответствует требованиям, продление доступно (рисунок 43).

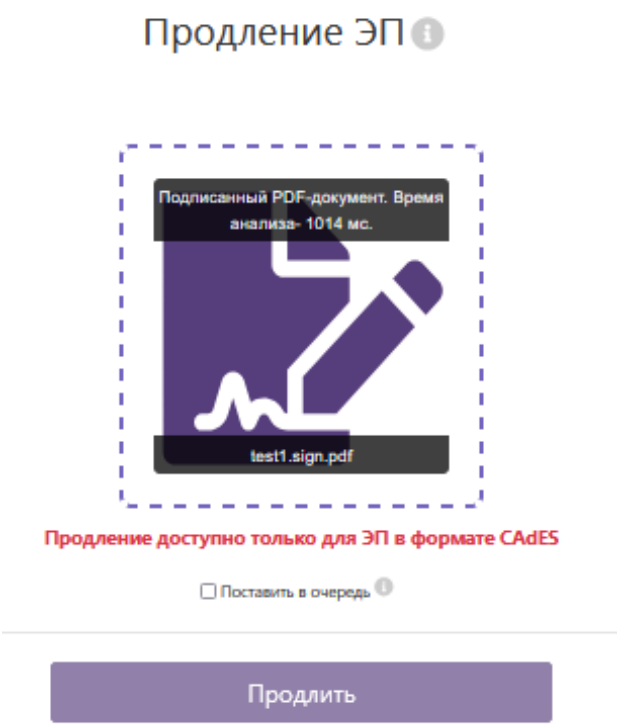


Рисунок 45 – Добавление документа с ЭП не в формате CAdES

4) Нажмите кнопку ***«Продлить»*** для выполнения операции.
5) После нажатия кнопки произойдет автоматический переход на страницу ***«Архив продлений»*** (рисунок 46). Перейти в архив вручную можно из пункта меню ***«Продление ЭП»*** → ***«Архив продлений».***

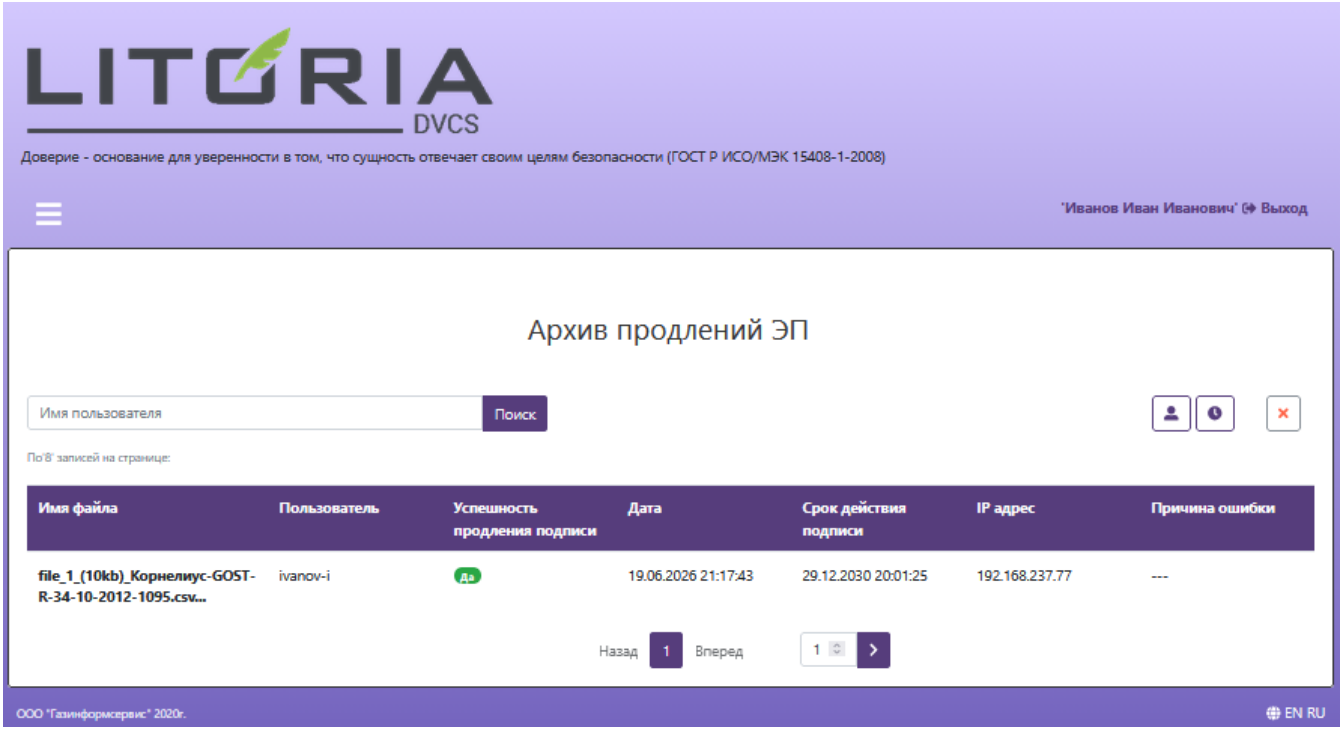


Рисунок 46 – Переход в архив продлений

6) При успешном продлении начинается скачивание файла с обновленной подписью. В случае ошибки в архиве отображается причина ошибки в столбце **«Причина ошибки»** (рисунок 46).

Продление в асинхронном режиме доступно при установке флага **«Поставить в очередь»** (рисунок 47).

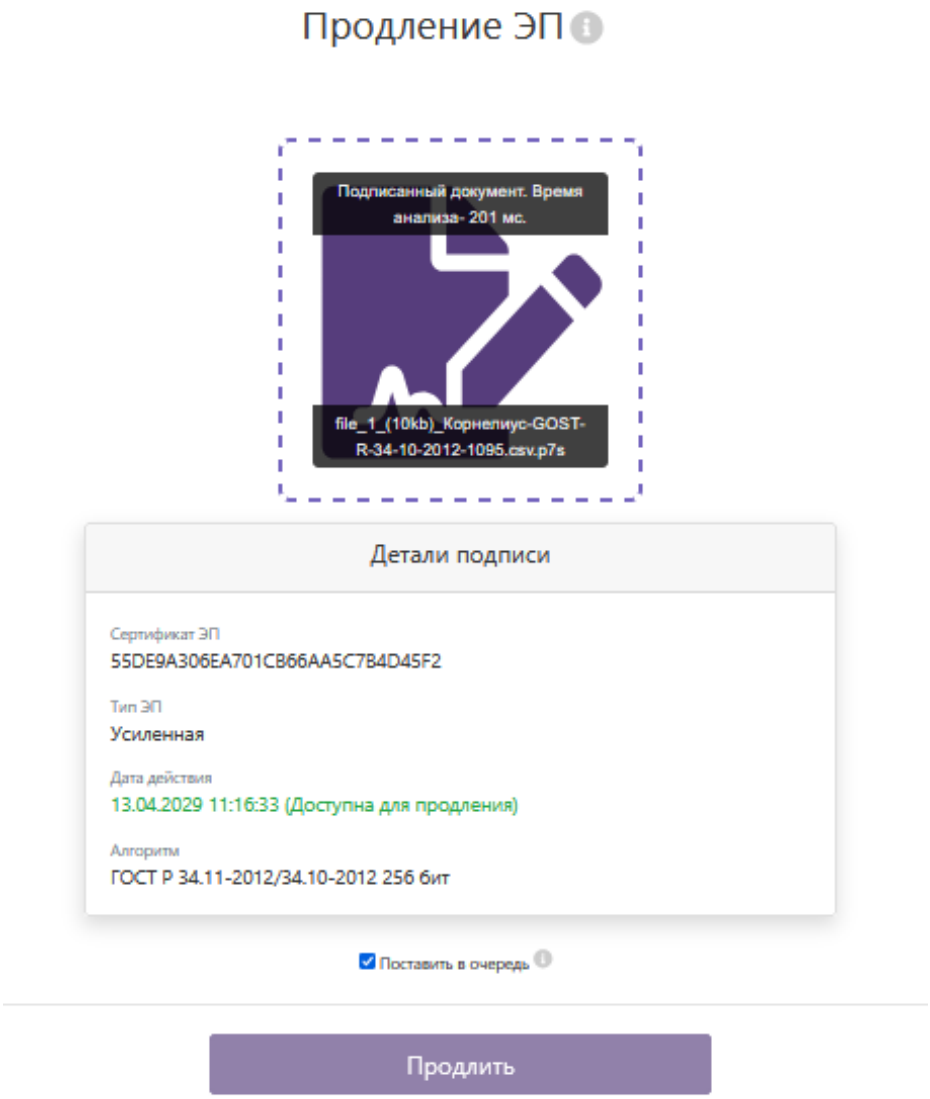


Рисунок 47 – Продление электронной подписи в асинхронном режиме

Шаги по продлению аналогичны синхронному режиму. Отличия:

– скачивание файла после нажатия кнопки ***«Продлить»*** не происходит;
– пользователь автоматически перенаправляется на страницу ***«Задачи»*** (рисунок 48);
– документ с продленной ЭП становится доступен в результатах задачи (по ссылке на идентификаторе задачи) – внутри JSON-ответа в поле `UpdateData` (рисунок 49);

– для скачивания `UpdateData` в виде файла предусмотрена кнопка « » (отображается только в случае успешного продления).

Рисунок 48 – Переход в задачи

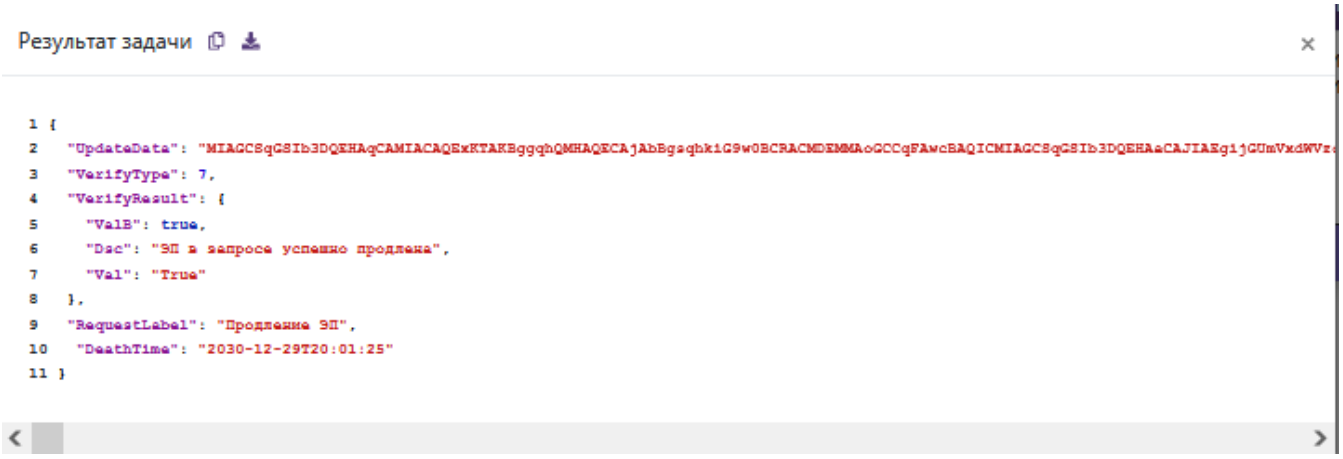


Рисунок 49 – Отображение результата задачи

Примечание. Описание статусов задач и порядок получения результата по идентификатору задачи см. в подразделе 3.6.

3.5.1 Архив продлений

Раздел **«Архив продлений»** предназначен для хранения и просмотра информации о всех выполненных операциях продления электронной подписи (рисунок 50).

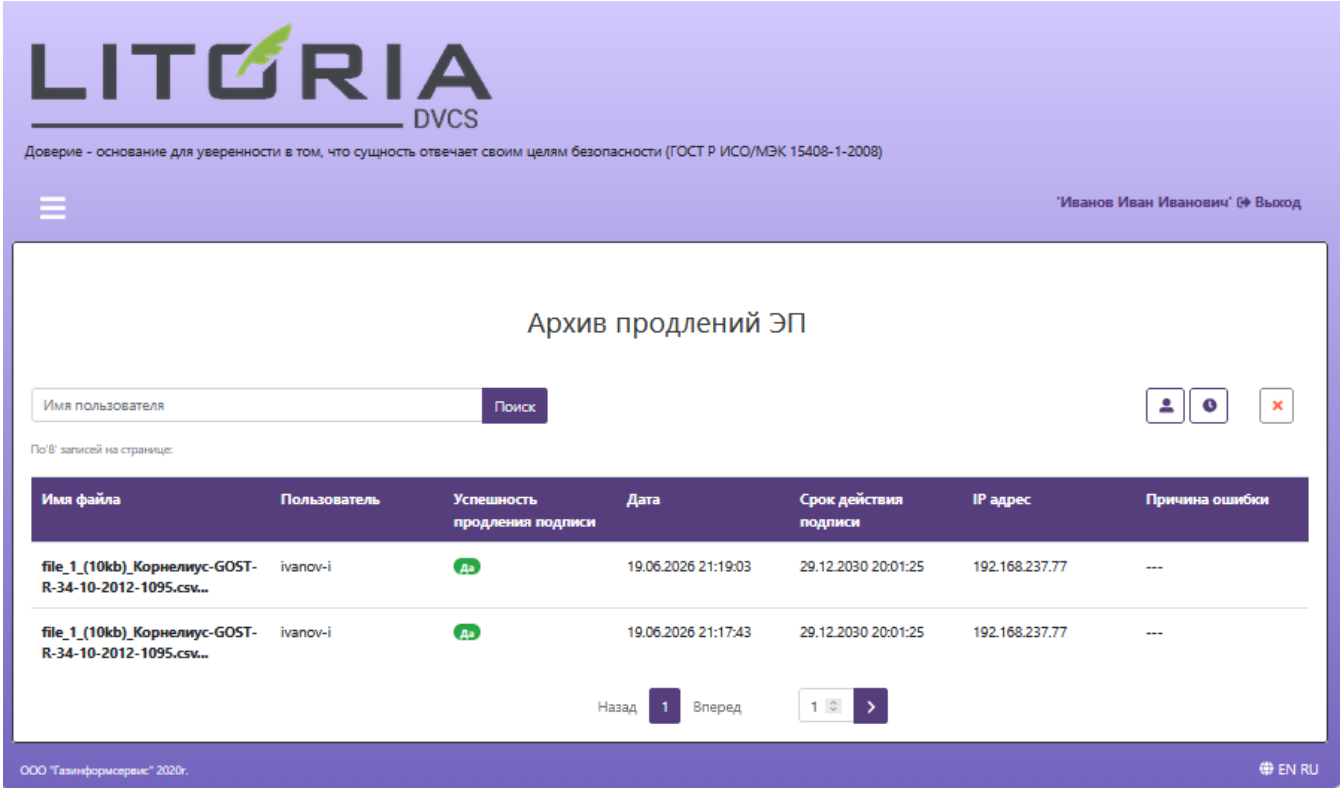


Рисунок 50 – Архив продлений

Переход в архив осуществляется:

- автоматически после выполнения синхронного продления;
- вручную через пункт меню ***«Продление ЭП»*** → ***«Архив продлений».***

В архиве содержится общая информация о факте операции продления:

- Имя файла;
- Пользователь, выполнивший продление;
- Успешность продления подписи (успешно/ошибка);
- Дата и время выполнения операции;
- Срок действия подписи;
- IP-адрес пользователя;
- Причина ошибки (при наличии).

Примечание. Архив не хранит сам документ с продленной ЭП, а только информацию о выполненной операции.

В архиве доступны следующие возможности:

- **Сортировка** – по учетной записи пользователей по кнопке « » и сроку действия ЭП по кнопке « ».
- **Поиск** – по имени пользователя.

3.6 Задачи

В пункте меню ***«Задачи»*** отображаются все запросы пользователя, поставленные в очередь на асинхронную обработку (рисунок 51).

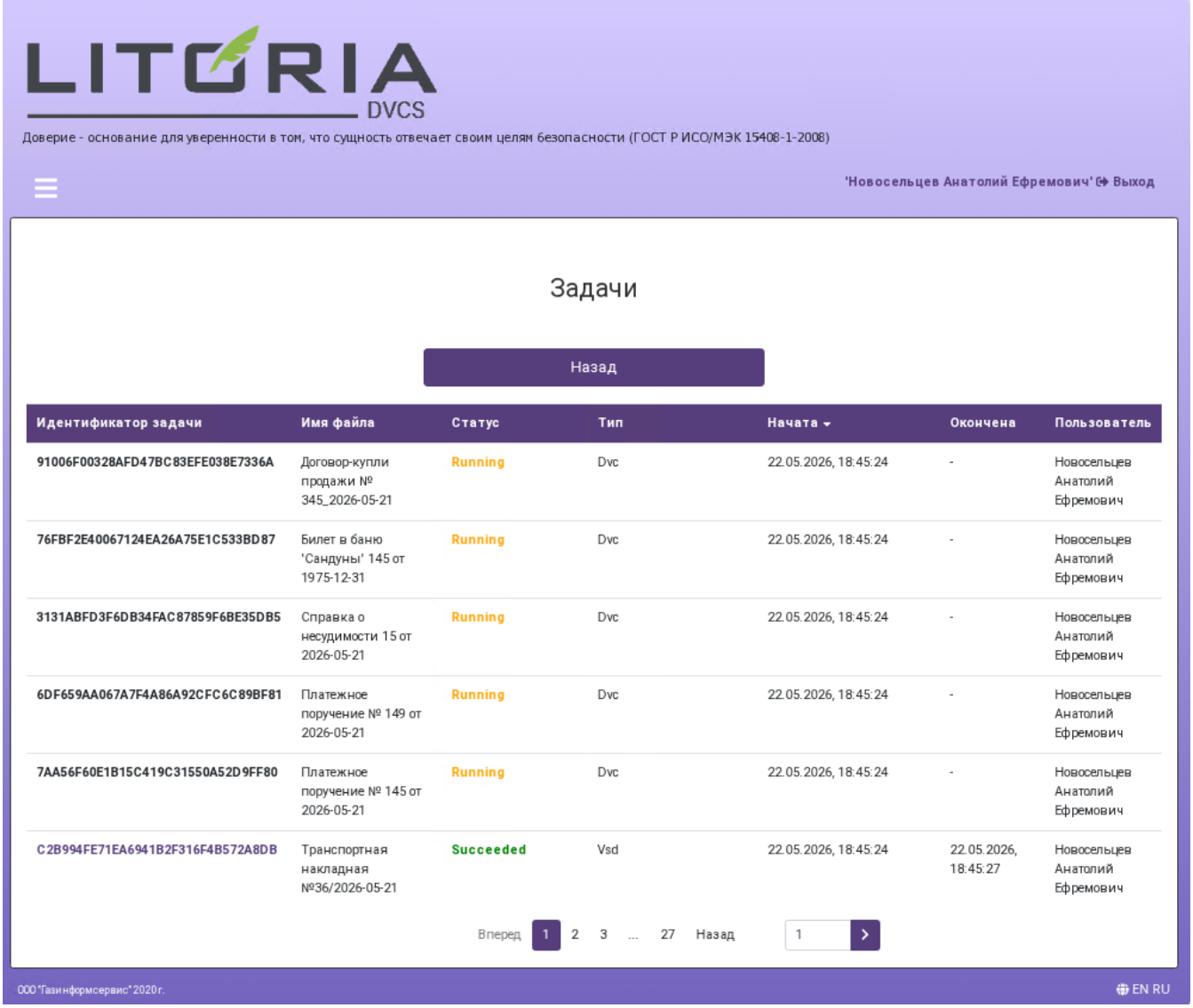


Рисунок 51 – Вкладка «Задачи»

Примечание. При использовании ПК «Litoria DVCS» в режиме пробной версии продукта вкладка **«Задачи»** будет недоступна.

Раздел предназначен для отслеживания статуса выполнения задач, запущенных с установленным флагом **«Поставить в очередь»**. При переходе на вкладку задачи отображаются в виде таблицы со следующими сведениями:

- **Идентификатор задачи** – уникальный номер, присваиваемый задаче при постановке в очередь;
- **Наименование файла** – имя загруженного документа, переданного на проверку;

- **Статус выполнения** – текущее состояние обработки задачи (см. таблицу статусов ниже);
- **Тип запроса** – вид операции, определяемый в момент проверки;
- **Начата** – время начала обработки задачи. Отсчёт начинается с момента попадания задачи в очередь (установка статуса `pending`), а не с момента начала выполнения (`running`);
- **Окончена** – время завершения обработки задачи (статус `succeeded` или `failed`);
- **Пользователь** – учётная запись пользователя или администратора, создавшего запрос.

Примечание. Параметры обработки задач задаются администратором в конфигурационном файле *«appsettings.json»*.

Статусы задач отображаются в соответствии с текущим состоянием обработки и приведены в таблице 1.

Таблица 1 – Статусы задач в соответствии с текущим состоянием обработки

Статус	Описание
`pending`	Задача ожидает в очереди
`running`	Задача выполняется
`succeeded`	Выполнено успешно
`failed`	Выполнено с ошибкой

Данные в пункте меню ***«Задачи»*** обновляются автоматически (динамически) без необходимости перезагрузки страницы.

Определение типа запроса происходит в момент проверки. По этой причине для задач со статусами `pending` и `running` тип отображается как *dvc*. После успешной обработки или возникновения ошибки тип становится детальным (например, VSD, VPKC, CPD, CCPD), если его удалось определить при проверке документа.

При успешном создании квитанции идентификатор задачи становится её серийным номером. Идентификатор задачи отображается в формате, соответствующем формату идентификатора квитанции, для удобства дальнейшего использования.

После завершения обработки задачи (статус `succeeded` или `failed`) перейдите по ссылке в столбце **«Идентификатор задачи»** (рисунок 51):

- при статусе `succeeded` – для получения квитанции (рисунок 15);
- при статусе `failed` – для получения ошибки в виде JSON-файла (рисунок 35).

3.7 Архив

В пункте меню ***«Архив»*** отображаются все квитанции пользователя, полученные при создании DVCS-запросов с использованием web-кабинета и другого программного обеспечения (рисунок 52).

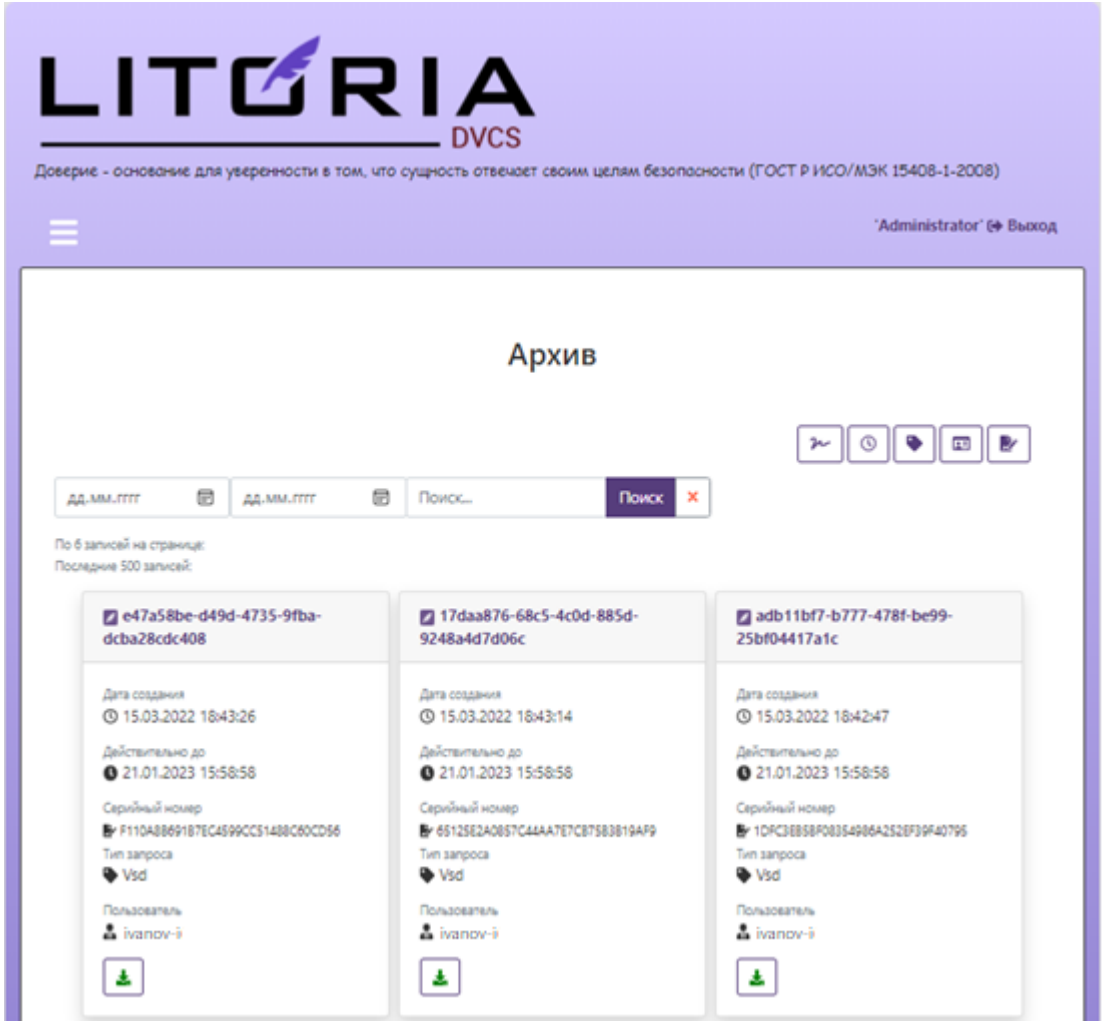


Рисунок 52 – Архив квитанций ПК «Litoria DVCS»

В карточках квитанций архива отображается следующая информация по квитанции:

- уникальный номер квитанции,
- серийный номер квитанции,
- идентификатор транзакции,
- дата создания квитанции,
- срок действия квитанции
- тип запроса.

Квитанции в архиве можно отсортировать по идентификатору квитанции (кнопка « »), по дате создания запроса (кнопка « »), по типу запроса (кнопка « »), по идентификатору транзакции (кнопка « ») или по серийному номеру квитанции (кнопка « »).

По кнопке « » можно изменить отображение квитанций в архиве на список, представленный в виде таблицы (рисунок 53).

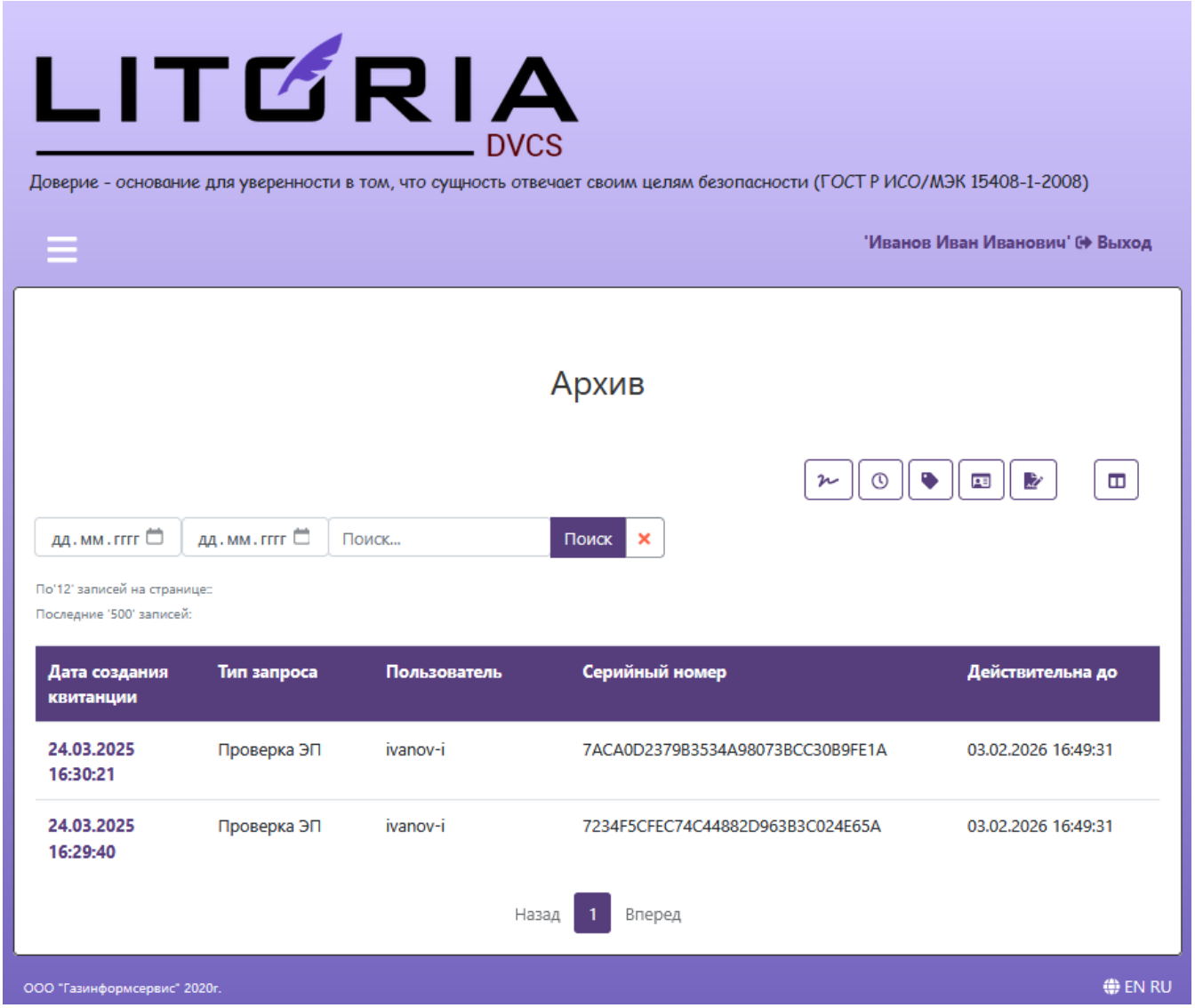


Рисунок 53 – Отображение квитанций в архиве в табличном виде

При необходимости можно выполнить поиск квитанции в архиве за выбранный период времени.

Во вкладке ***«Архив»*** доступен поиск квитанций по идентификатору квитанции, серийному номеру квитанции и идентификатору транзакции. Для этого в поле поиска укажите полностью или введите часть символов серийного номера квитанции, ее идентификатора или идентификатора транзакции (рисунок 54).

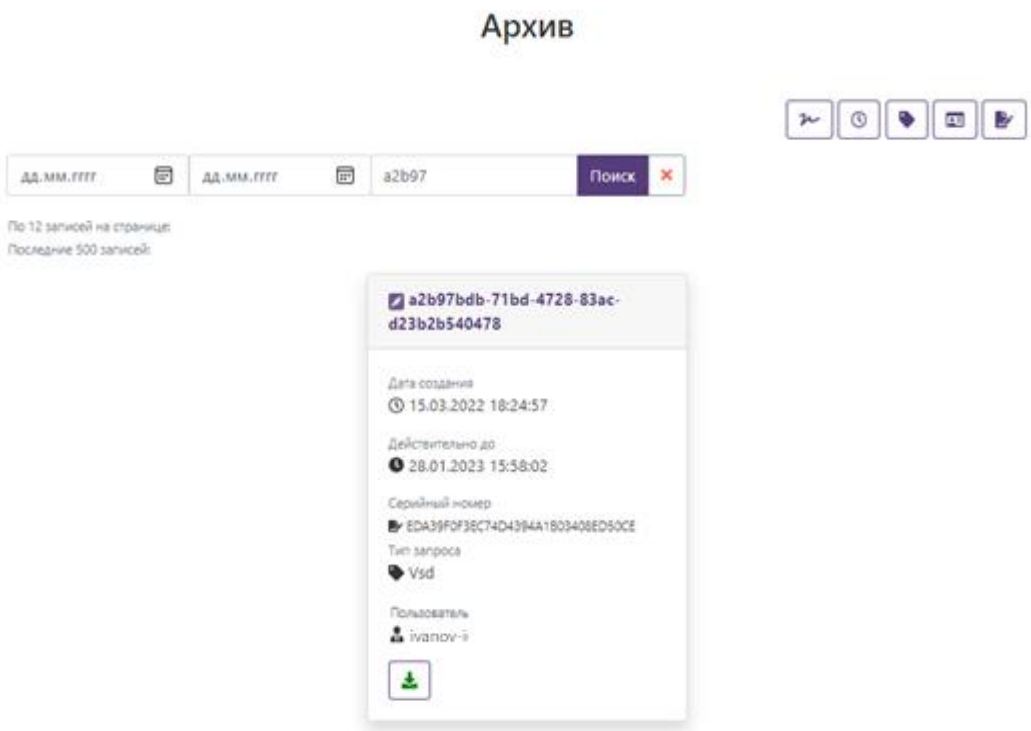


Рисунок 54 – Поиск квитанции по идентификатору квитанции

Для просмотра квитанции необходимо в карточке нужной квитанции нажать на ссылку с ее номером (рисунок 54). На экране отобразится ответная квитанция службы DVCS, содержащая информацию о проведенных проверках (рисунок 55).

Загрузка квитанции доступна по нажатию на ссылку с нужным форматом в правом верхнем углу « .zip .sig .pdf » (см. пункт 3.4.8).

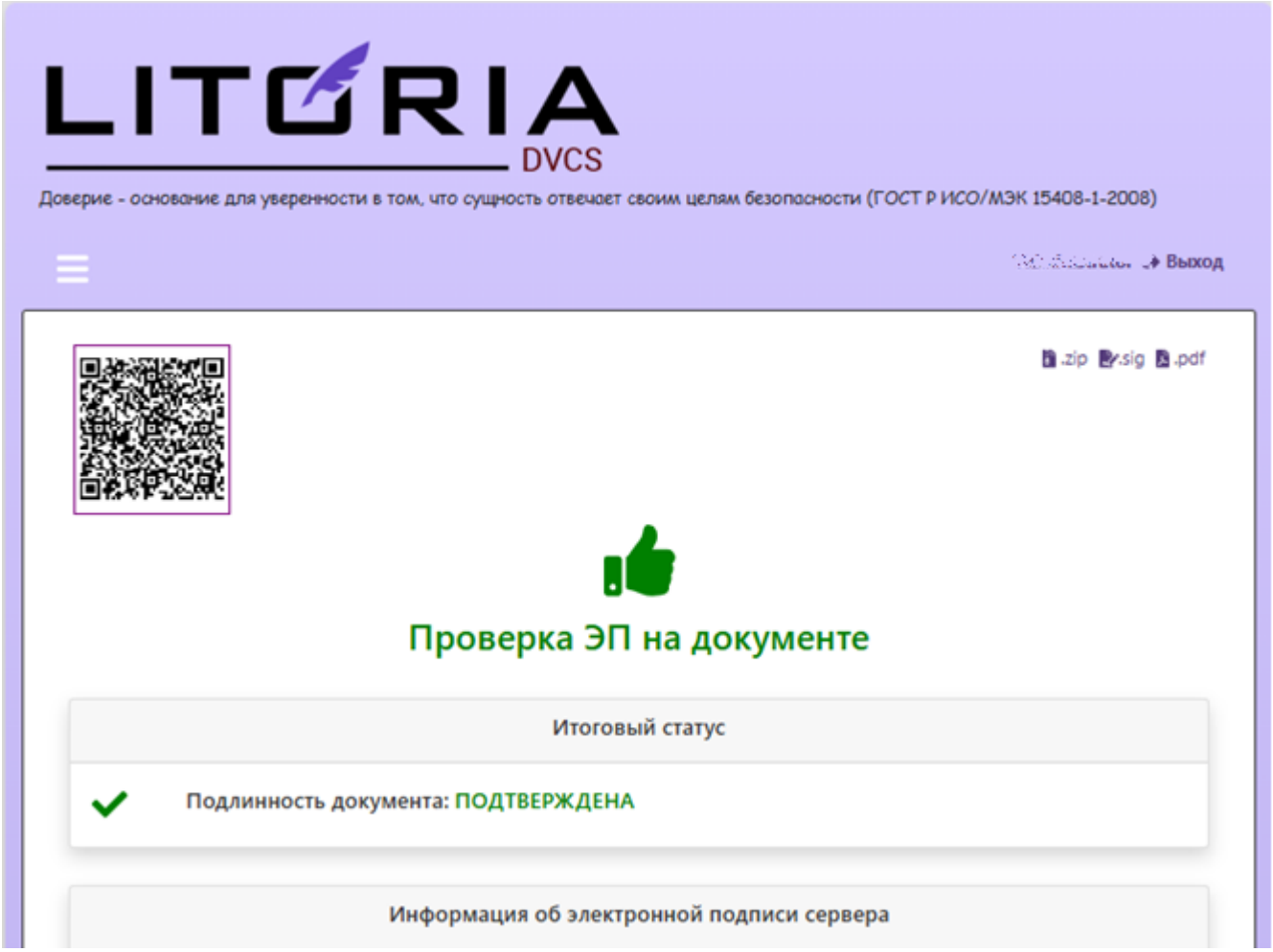


Рисунок 55 – Просмотр квитанции

3.8 Статистика

В пункте меню ***«Статистика»*** отображаются сводные данные по квитанциям, полученным при создании DVCS-запросов с использованием web-кабинета и другого программного обеспечения, и по запросам на продление ЭП (рисунок 57).

Данные в пункте меню ***«Статистика»*** отображаются в виде диаграмм (рисунок 57):

- по типу запроса (проверка принадлежности, проверка сертификата, проверка ЭП, проверка принадлежности по хеш, продление ЭП);
- по маршрутизации квитанций (локальная, трансграничная);
- по статусу результата проверки (успешен, неуспешен, неизвестен);
- по статусу результата запроса на продление ЭП (успешен, неуспешен);
- по стоимости запроса (обычная стоимость, повышенная стоимость);
- по направлению проверки (по всем направлениям, RU – российские алгоритмы ГОСТ, EU – европейские алгоритмы, KZ – алгоритмы Республики Казахстан, RB – алгоритмы Республики Беларусь);

или более детально в виде перечня запросов пользователя (рисунок 58).

Переключение между общим видом статистических данных по квитанциям и их детальным отображением доступно на кнопкам ***«Общий вид»/«Детально»***.

Сводные данные формируются за определенный промежуток времени, для выбора периода формирования статистики укажите дату начала и дату окончания периода.

Для загрузки всех квитанции за выбранный период нажмите на кнопку « Получить все квитанции за выбранный период » (рисунок 57). На рабочую станцию сохраняется архив, содержащий в себе:

– квитанцию DVC в формате CMS в файле с расширением **.sig*[4];
– полный разбор квитанции и саму квитанцию в файле с расширением **.dvc*.

Для получения отчета за выбранный период нажмите на кнопку « Получить отчет за выбранный период » (рисунок 57), предварительно выбрав формат выгрузки отчета .html или .xls в выпадающем списке (рисунок 56).

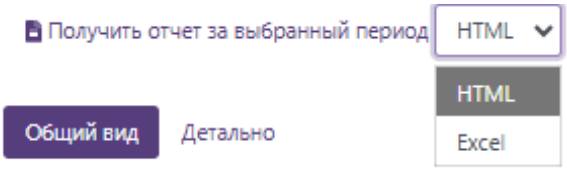


Рисунок 56 – Выбор формата отчета

На рабочую станцию сохраняется файл с расширением **.html* (рисунок 59) или **.xls* (рисунок 60), содержащий информацию о всех квитанциях пользователя в виде таблицы, отображающей :

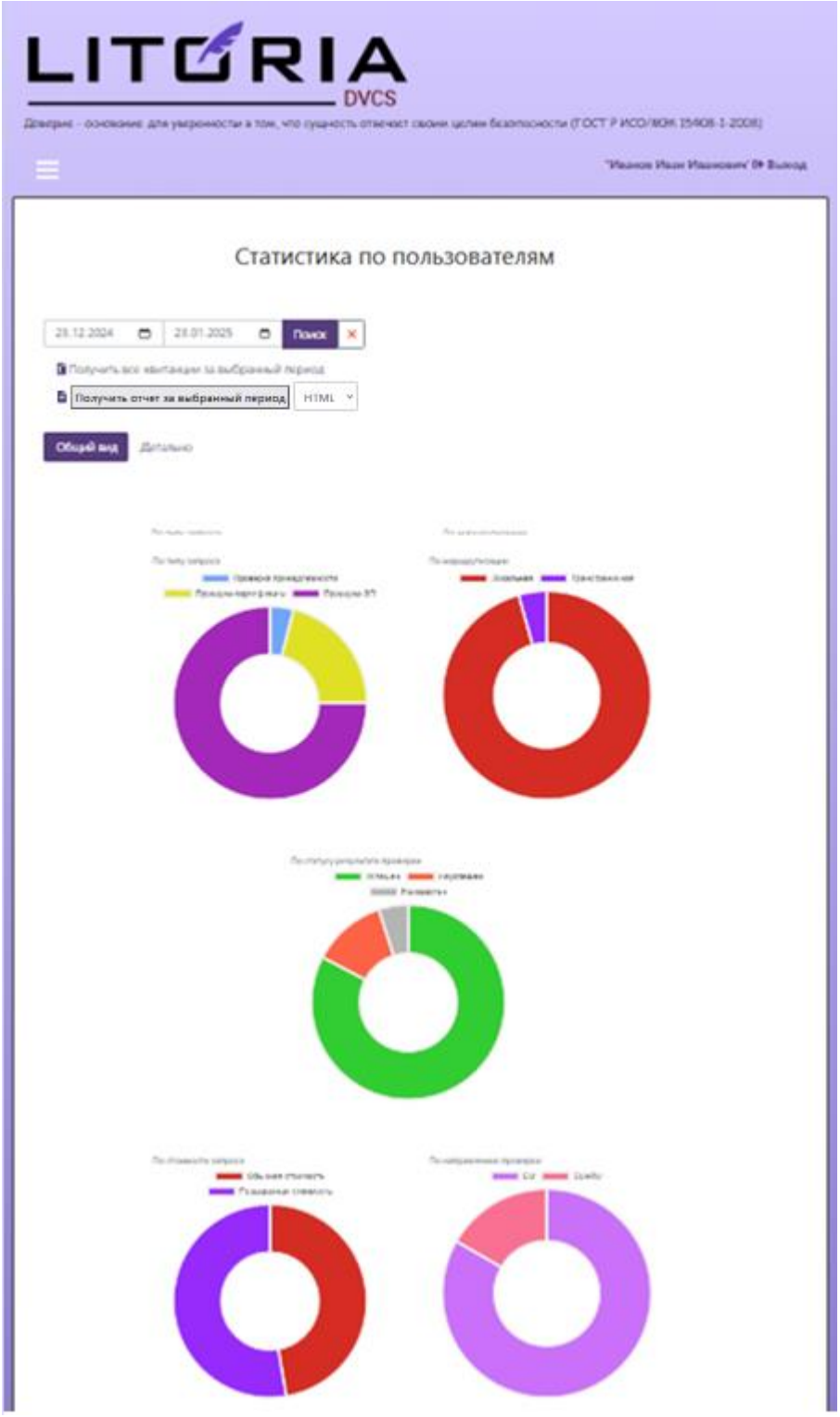
– общую информацию – время формирования отчета, общее количество квитанций, количество пользователей в отчете, общее количество организаций в отчете, количество успешных/неопределенных/неуспешных результатов проверки, количество успешных/неуспешных продлений;
– для локальной и трансграничной проверок – серийный номер квитанции, дату поступления запроса, дату создания, время обработки запроса, тип запроса, хеш запроса, IP-адрес, результат проверки, стоимость и организацию пользователя, направление проверки (только для трансграничных проверок);
– для продления ЭП – серийный номер сертификата (будет отсутствовать в случае, если сертификат не удалось определить), дату выполнения запроса, дату окончания действительности подписи после продления (будет отсутствовать в случае, если подпись не была продлена), размер документа в байтах, размер отделенной подписи (принимает значение «0» в случае, если подпись не отделенная), IP-адрес и результат выполнения запроса и организацию пользователя.

В столбце «Результат проверки» данные отображаются согласно следующих правилам:

[4] Тип расширения квитанции DVC в формате CMS устанавливается администратором комплекса (по умолчанию установлен тип расширения *«sig»)*.

– для локальной проверки и продления ЭП результат может быть «Успешен» или «Неуспешен»;
– для трансграничной проверки результат всегда «Неизвестен».

Примечание. Если в проверяемом документе несколько подписей и хотя бы для одной из них проводилась трансграничная проверка, результат в отчете будет «Неизвестен».



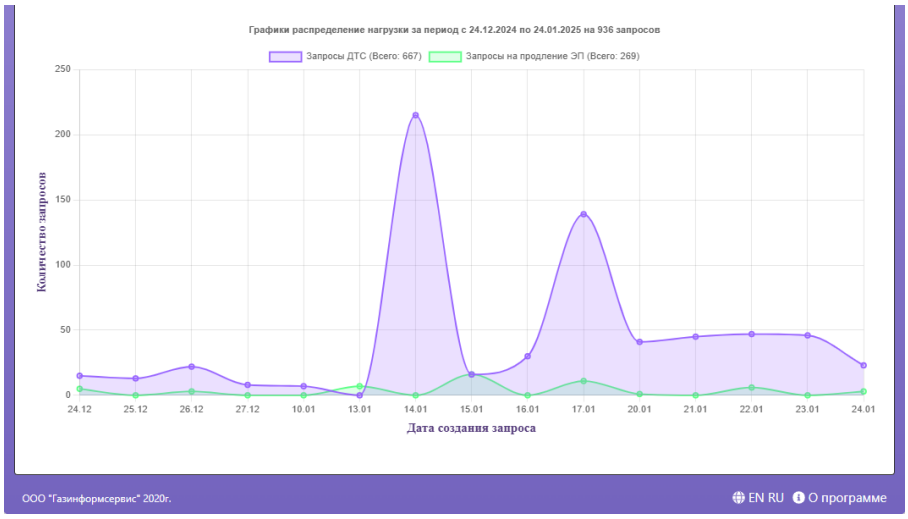


Рисунок 57 – Вкладка «Статистика» общий вид

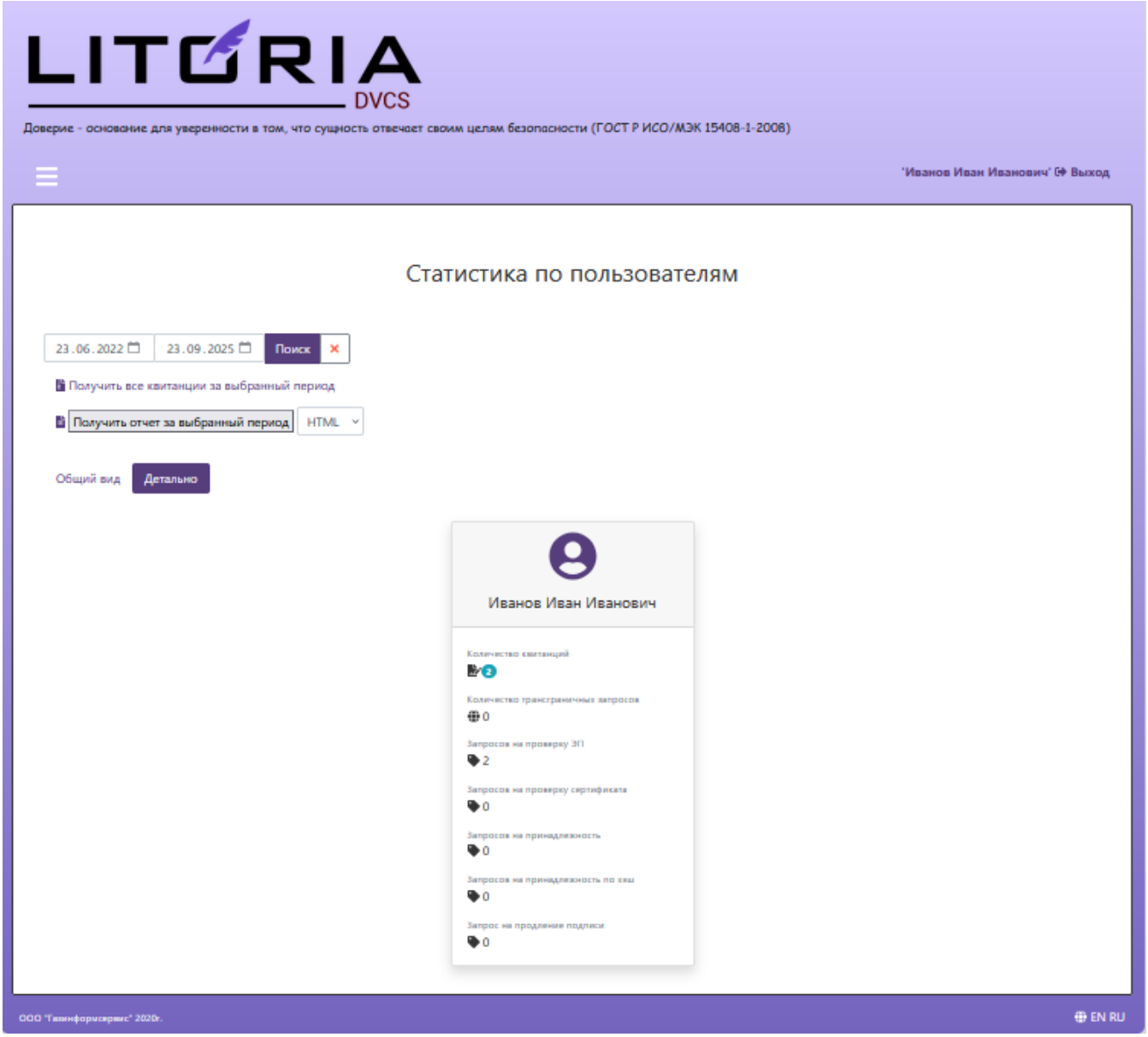


Рисунок 58 – Вкладка «Статистика» детальное отображение

Статистика за период с 06-04-2026 00:00 до 06-05-2026 12:51

Время формирования отчета: 06-05-2026 12:51
Количество пользователей в отчете: 1
Общее количество квитанций: 2
Успешных результатов проверки: 1
Неопределенных результатов проверки: 1
Неуспешных результатов проверки: 0
Успешных продлений 0
Неуспешных продлений 0

TEST111
ооо "Победа"
TEST@TEST.RU

Локальная проверка
Число проверок: 1

№	Серийный номер	Дата поступления запроса	Дата создания квитанции	Время обработки запроса	Тип запроса	Хэш запроса	Ip адрес	Результат проверки	Стоимость
1	DEF3877353FEA948A99AE781C3420510	06.05.2026 12:25:34	06.05.2026 12:25:36	1767 мс	Проверка сертификата	7100C98D4D0F2AC04EB3064DE23383062F129243	::1	Успешен	Обычная

Трансграничная проверка
Число проверок: 1

№	Серийный номер	Дата поступления запроса	Дата создания квитанции	Время обработки запроса	Тип запроса	Хэш запроса	Ip адрес	Результат проверки	Стоимость	Направление
1	EA9A1BD7707A8047BCF6B6CBBE3A04F8	06.05.2026 12:24:35	06.05.2026 12:25:11	35905 мс	Проверка сертификата	0D85DF2DB3B863AB68BEB36F9705A9F1A80AB457	::1	---	Обычная	EU

Рисунок 59 – Отображение отчета за выбранный период в формате html

Отчет за период с 23-06-2022 00:00 по 23-09-2025 23:59

Время формирования отчета:	23.09.2025 10:53
Общее количество квитанций:	2
Общее количество организаций в отчете:	1
Количество пользователей в отчете:	1
Успешных результатов проверки:	0
Неопределенных результатов проверки:	0
Неуспешных результатов проверки:	2
Успешных продлений	0
Неуспешных продлений	0

Данные отчета

№	Пользователь	Тип данных	Количество запросов
1	Иванов Иван Иванович	Локальная проверка	2
		Всего	2

Рисунок 60 – Отображение отчета за выбранный период в формате xls

3.9 Изменение языка интерфейса

По умолчанию в интерфейсе единого web-кабинета ПК «Litoria DVCS» и в сформированных по отправленным на проверку запросам (VSD, VPKC, CPD) квитанциях устанавливается русский язык.

Смена языка доступна в правом нижнем углу главного окна web-кабинета (рисунок 61).

Рисунок 61 – Изменение языка интерфейса

Для изменения русского языка на английский нажмите на ссылку EN, для возврата к русскому языку, нажмите RU.

При смене языка квитанции по отправленным на проверку запросам также будут сформированы на английском языке (рисунок 62).

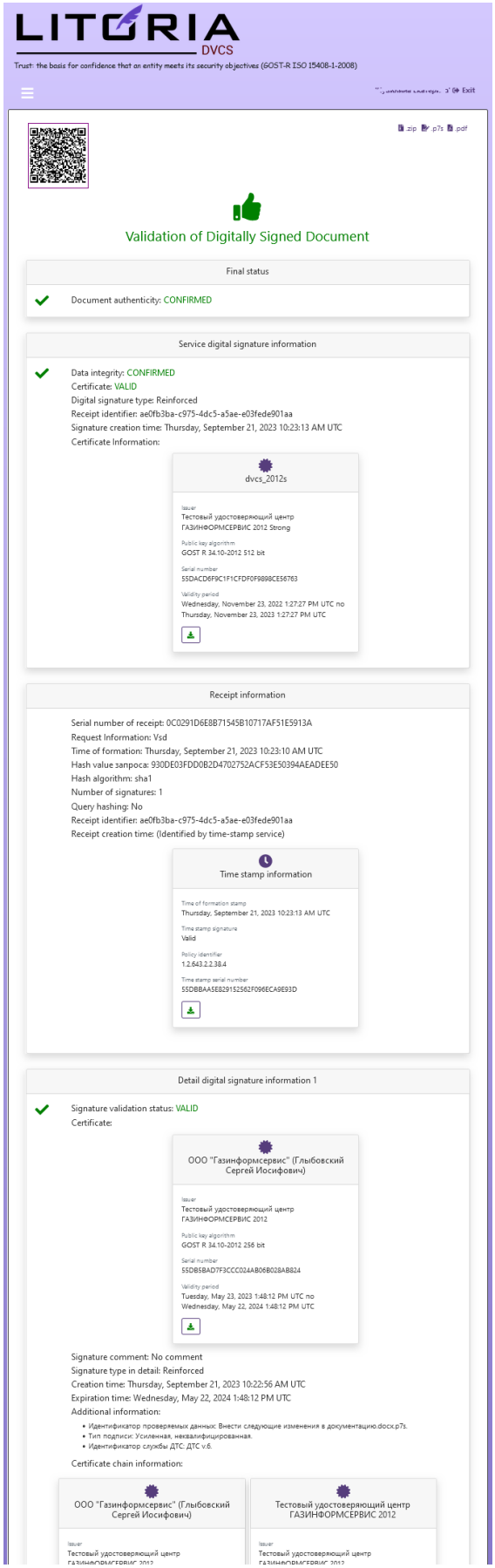


Рисунок 62 – Квитанция на английском языке

4 Лицензия и техподдержка

Информация о текущей лицензии ПК «Litoria DVCS» и техподдержке доступна только администратору комплекса.

Если ПК «Litoria DVCS» не активирован или в случае возникновения проблем с лицензией ПК «Litoria DVCS» в нижнем левом углу основного окна появится отображения, что ПК «Litoria DVCS» работает в режиме пробной версии продукта (рисунок 63).

Примечание. При возникновении проблем с активацией продукта рекомендуется обратиться к администратору комплекса.

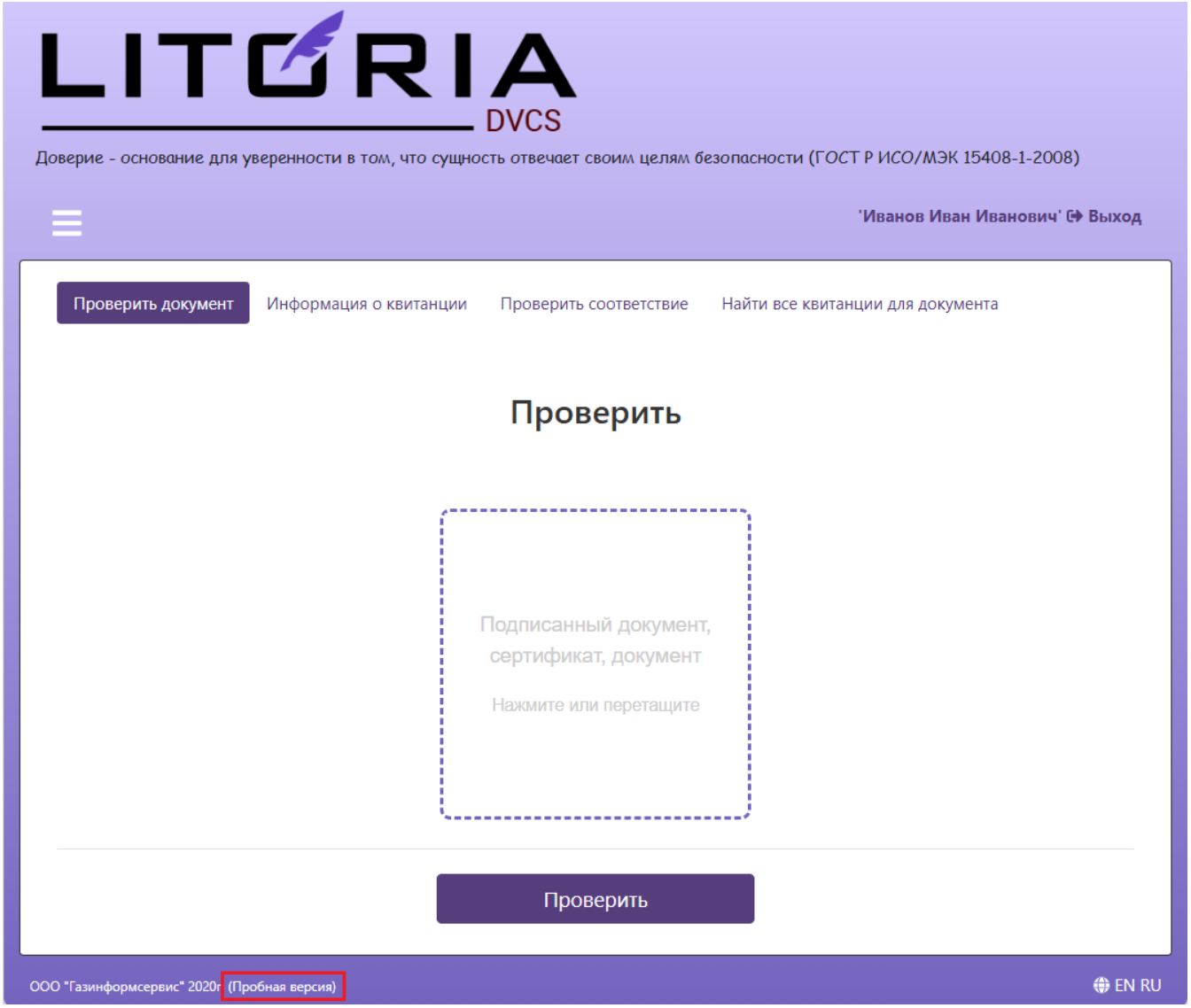


Рисунок 63 – Режим пробной версии продукта

Перечень сокращений

API – Application Programming Interface
CCPD – Certification of Claim of Possession of Data (удостоверение обладания информацией без предоставления ее сервису (по хеш))
CPD – Certification of Possession of Data (удостоверение обладания информацией в указанный момент времени с предоставлением ее сервису)
CMS – Cryptographic Message Syntax
CSP – Cryptographic Service Provider
DVC – Data Validation and Certification
DVCS – Data Validation and Certification Server
IP – Internet Protocol
ISO – International Organization for Standardization
PDF – Portable Document Format
RFC – Request for comments (рабочее предложение – документ, содержащий технические спецификации, применяемые в сети)
TSP – Time-Stamp Protocol
VPKC – Validation of Public Key Certificates
VSD – Validation of digitally Signed Document
XML – Extensible markup language (расширяемый язык разметки)
АРМ – Автоматизированное Рабочее Место
ДТС – Доверенная Третья Сторона
МЧД – Машиночитаемая Доверенность
ОС – Операционная Система
ПК – Программный Комплекс
СКЗИ – Средство Криптографической Защиты Информации
ФЗ – Федеральный закон
ФСБ – Федеральная служба безопасности Российской Федерации
ЭП – Электронная Подпись