ГАЗИНФОРМ СЕРВИС

Программный комплекс «Litoria DVCS»

Руководство администратора безопасности

Санкт-Петербург, 2021

Аннотация

В документе приводится руководство администратора безопасности программного комплекса «Litoria DVCS» (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) на котором функционирует комплекс.

В разделе «Настройка ПК «Litoria DVCS» описан порядок действий по установке и настройке комплекса.

В разделе «Использование ПК «Litoria DVCS» описан порядок работы с комплексом и действия, необходимые для обращения к основным функциям.

В разделе «Настройки конфигурационных файлов» описан порядок действий для изменения настроек, связанных с функционированием ПК «Litoria DVCS».

В разделе «Модуль REST API» описаны действия по выполнению автоматизированной отправке запросов и получению ответов участниками электронного взаимодействия.

Содержание

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 предоставляет пользователю возможность создания запросов на проверку, выполняет анализ этих запросов и формирует ответы, содержащие информацию о проведенных проверках.

Основные функциональные возможности ПК «Litoria DVCS»:

- подтверждение электронной подписи (ЭП) электронного документа;
- подтверждение действительности сертификата ключа подписи;
- удостоверение обладания информацией в указанный момент времени с предоставлением ее сервису;
- удостоверение обладания информацией без предоставления ее сервису;
- проверка данных, содержащихся в запросе;
- формирование и анализ DVC-квитанций в соответствии с рекомендациями RFC3029.

ПК «Litoria DVCS» включает следующие компоненты:

- **Служба DVCS** (полное описание протокола DVCS, на основании которого строится работа службы, приведено в RFC3029) предоставляет услуги проверки данных в запросе, полученном службой от пользователя, подтверждая действительность ЭП документа, срок действия сертификатов ключей проверки ЭП. А также свидетельствует о предоставлении ей данных и о факте обладания пользователем этими данными в указанный момент времени.

- **Служба штампов времени TSP** (полное описание протокола TSP, на основании которого строится работа службы, приведено в RFC3161) удостоверяет факт существования электронного документа на определённый момент времени. Служба выдает штампы времени – документы, подписанные электронной подписью службы.

- **Модуль REST API** выполняет автоматизированную отправку запросов и получение ответов участниками электронного взаимодействия.

- **Единый web-кабинет** участника электронного взаимодействия позволяет управлять настройками службы, получать услуги по проверке электронных документов в программном комплексе, а также вести журналирование и получать статистическую информацию о произведенных операциях.

2 Условия применения

2.1 Требования к техническим средствам

Минимальные требования к рабочей станции, на которую устанавливается ПК «Litoria DVCS», обусловлены применением используемых ОС.

2.2 Требования к программному обеспечению

ПК «Litoria DVCS» функционирует под управлением 64х-разрядных версий следующих ОС:

- Windows Server 2016R2;
- Windows Server 2019R2;
- ОС семейств Linux.

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).
- СУБД Jatoba 1.0 и выше или PosgreSQL 11 и выше.
- Internet Information Services (IIS).
- распространяемый пакет Microsoft Visual C++ 2015-2019 Redistributable.
- Обратный прокси-сервер, ретранслирующий запросы клиентов из внешней сети на один или несколько серверов, логически расположенных во внутренней сети (в ОС семейства Linux могут использоваться реверс-прокси Nginx или Apache).[1]

[1] Допускается работа с ПК «Litoria DVCS» без использования обратного прокси-сервера.

3 Настройка ПК «Litoria DVCS»

Перед началом использования ПК «Litoria DVCS» необходимо выполнить следующие настройки:

- установить СУБД «PostgreSQL» или СУБД «Jatoba» (при этом СУБД и службы ПК «Litoria DVCS» могут быть установлены на как одну рабочую станцию, так и на разные);
- установить и настроить «Веб-сервер (IIS)»;
- установить ПК «Litoria DVCS»;
- получить сертификаты служб;
- настроить web-кабинет участника электронного взаимодействия;
- активировать ПК «Litoria DVCS».

3.1 Добавление роли «Веб-сервер (IIS)»

Перед началом работы с ПК «Litoria DVCS» необходимо установить и настроить веб-сервер IIS. Для этого выполните следующие действия:

1. Перейдите в «***Диспетчер сервера»*** по кнопке «***Пуск***».
2. В открывшемся окне выберите ***«Добавить роли и характеристики»*** (рисунок 3.1).

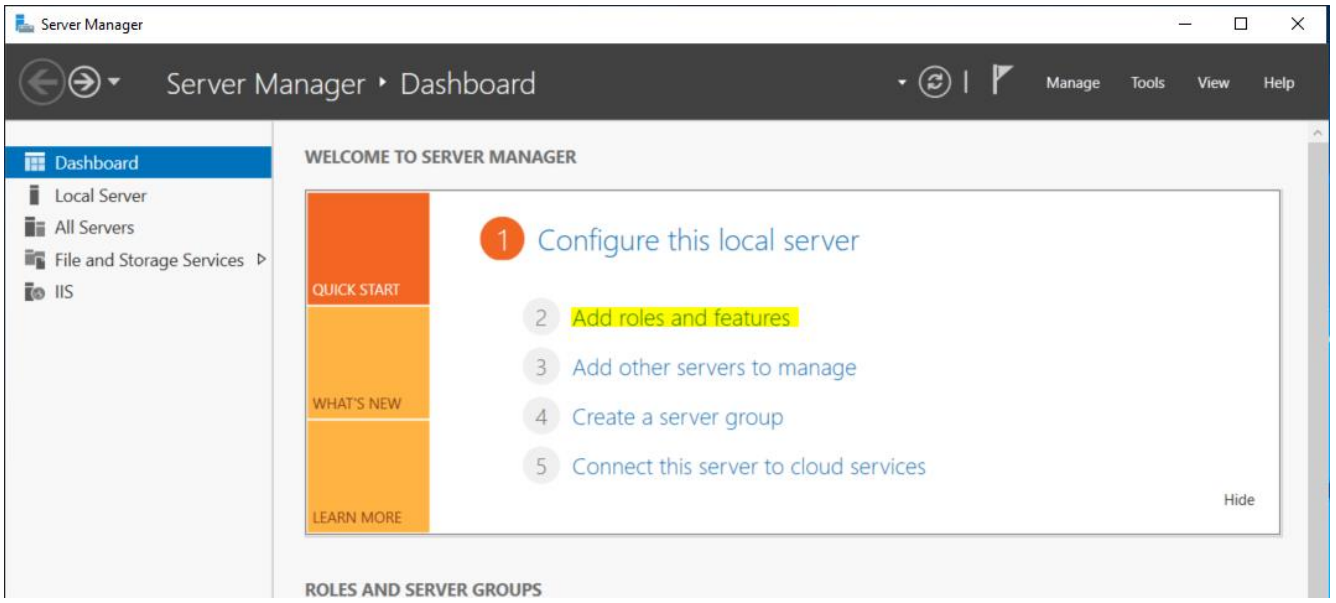

Рисунок 3.1 – Окно «Диспетчер сервера»

3. В окне приветствия нажмите на кнопку «***Далее***» (рисунок 3.2).

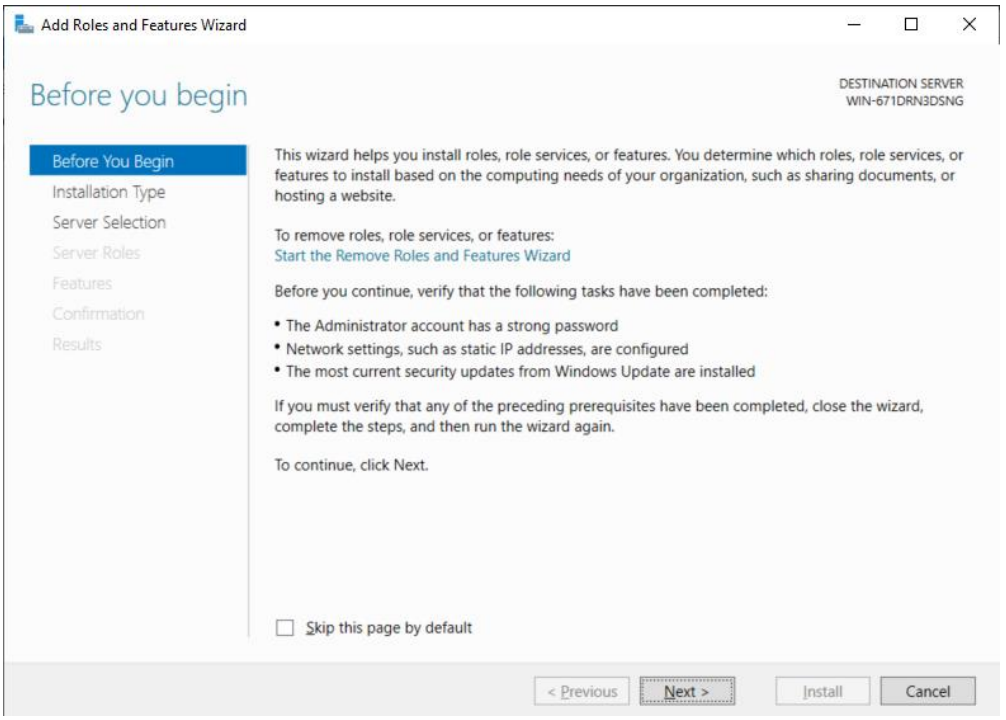

Рисунок 3.2 – Окно приветствия «Диспетчер сервера»

4. В окне ***«Тип установки»*** выберите ***«Установка ролей или компонентов»*** (рисунок 3.3) и нажмите ***«Далее»***.

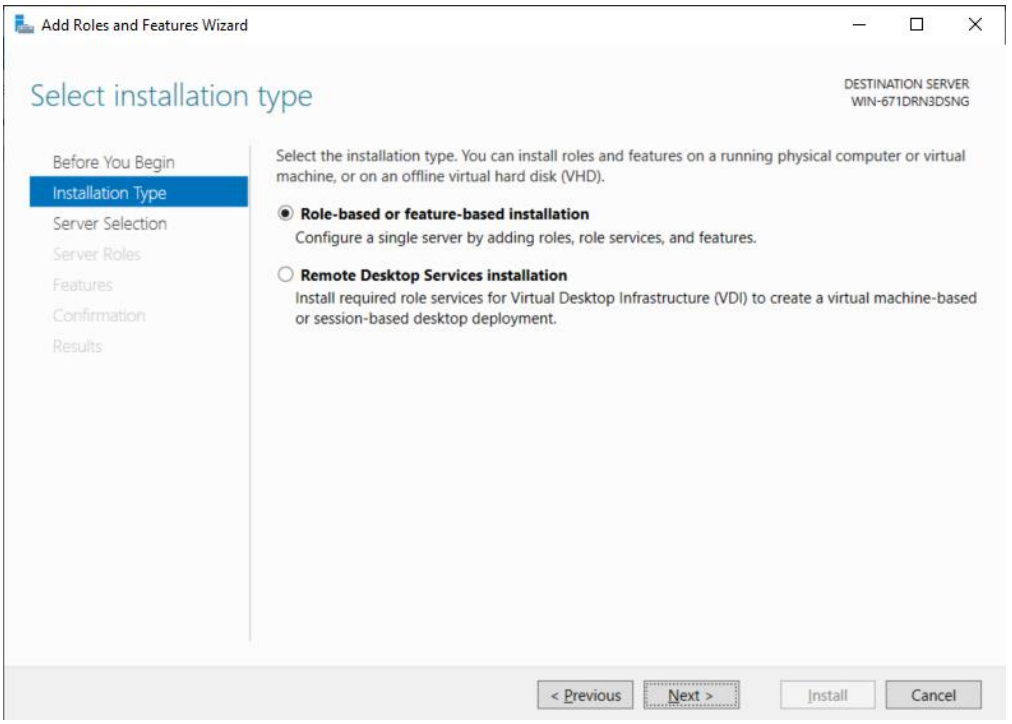

Рисунок 3.3 – Выбор типа установки

5. В окне ***«Выбор сервера»*** установите ***«Выберите сервер из пула серверов»***, выберите необходимый сервер из списка и нажмите на кнопку «***Далее***» (рисунок 3.4).

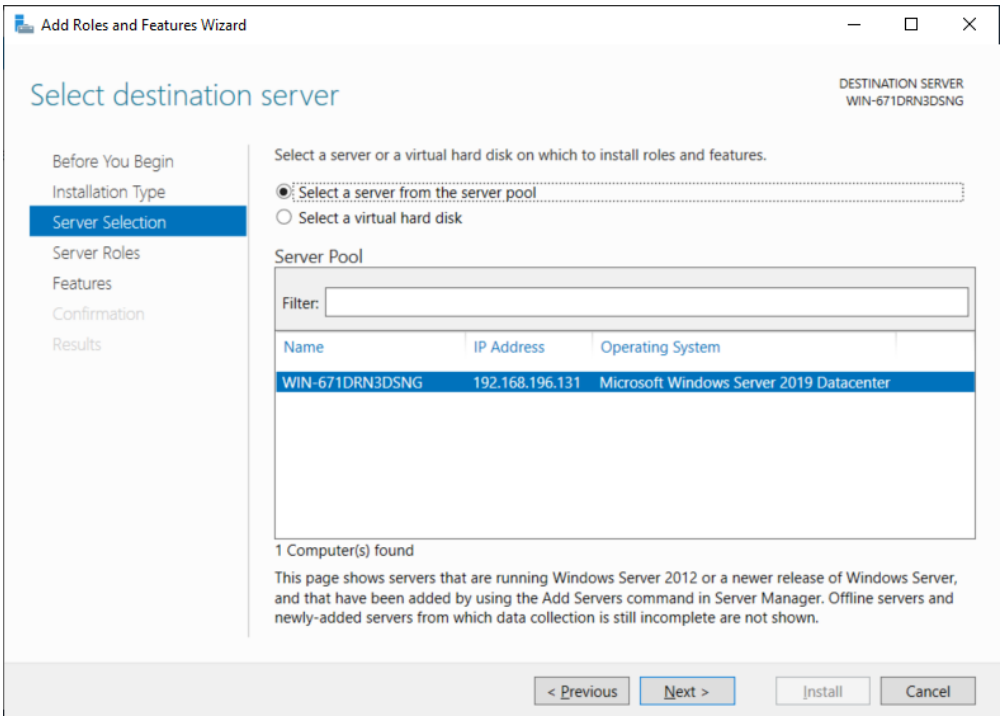

Рисунок 3.4 – Выбор сервера

6. В окне ***«Роли сервера»*** выберите ***«Веб-сервер (IIS)»*** и нажмите на кнопку ***«Далее»*** (рисунок 3.5).

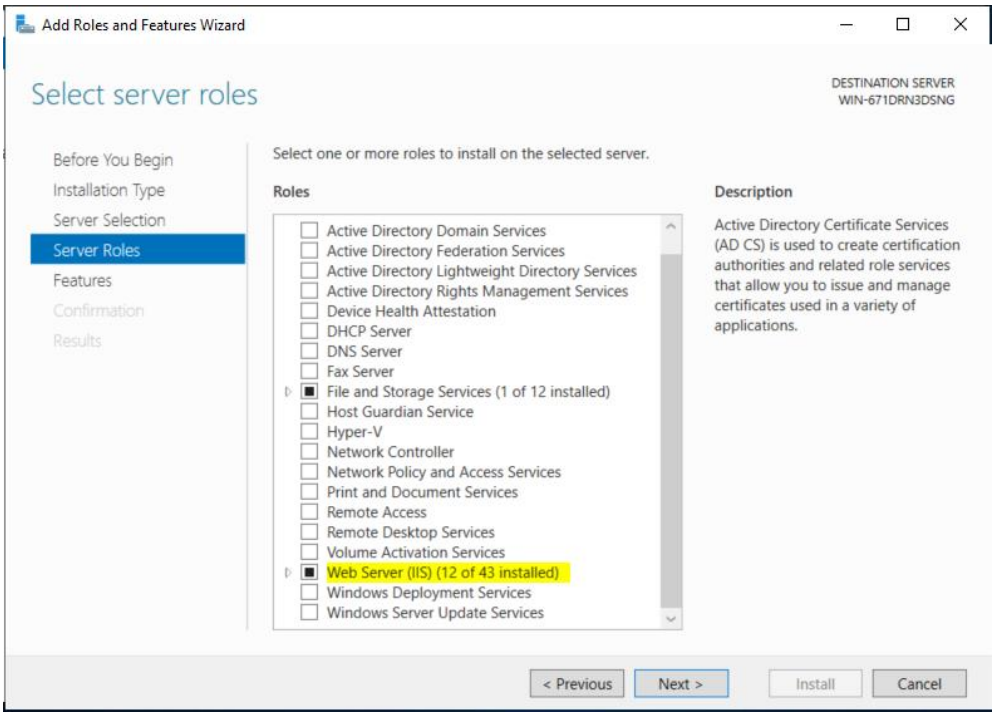

Рисунок 3.5 – Выбор роли сервера

7. В окне ***«Подтверждение»*** установите при необходимости параметр ***«Автоматический перезапуск конечного сервера»*** и нажмите ***«Установить»*** (рисунок 3.6).

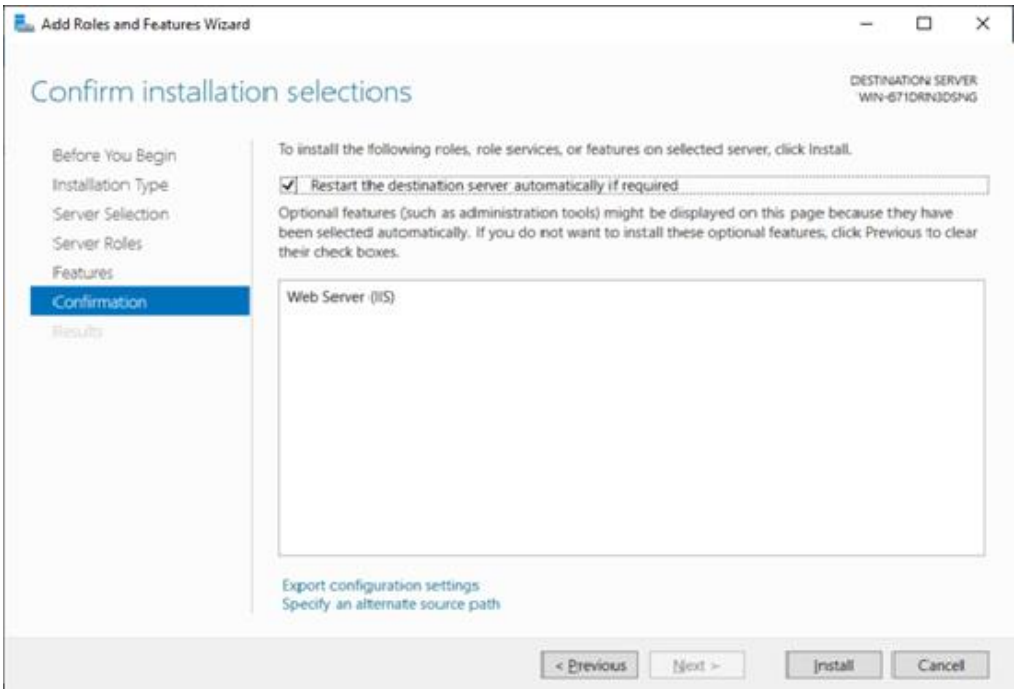

Рисунок 3.6 – Установка выбранных ролей и компонентов

3.2 Установка комплекса

Для установки ПК «Litoria DVCS» выполните следующие действия:

1. Запустите файл-инсталлятор «Litoria DVCS.msi» и в окне приветствия нажмите на кнопку «***Далее***» (рисунок 3.7).

Рисунок 3.7 – Установка ПК «Litoria DVCS

2. Выберите директорию установки и укажите параметры создаваемой базы данных (рисунок 3.8):

- ***Host*** – указывается IP-адрес или DNS-имя рабочей станции, на которой установлена СУБД «PostgreSQL» или СУБД «Jatoba» (при размещении СУБД и ПК на одной рабочей станции в поле ***Host*** можно оставить значение по умолчанию *localhost)*;
- ***Port*** – указывается значение TCP-порта, по которому осуществляется работа СУБД «PostgreSQL»/«Jatoba»;
- ***Database*** – указывается имя создаваемой базы данных;
- ***Username*** – имя учетной записи, обладающей полномочиями создания и редактирования в СУБД;
- ***Password*** – пароль указанной выше учетной записи.

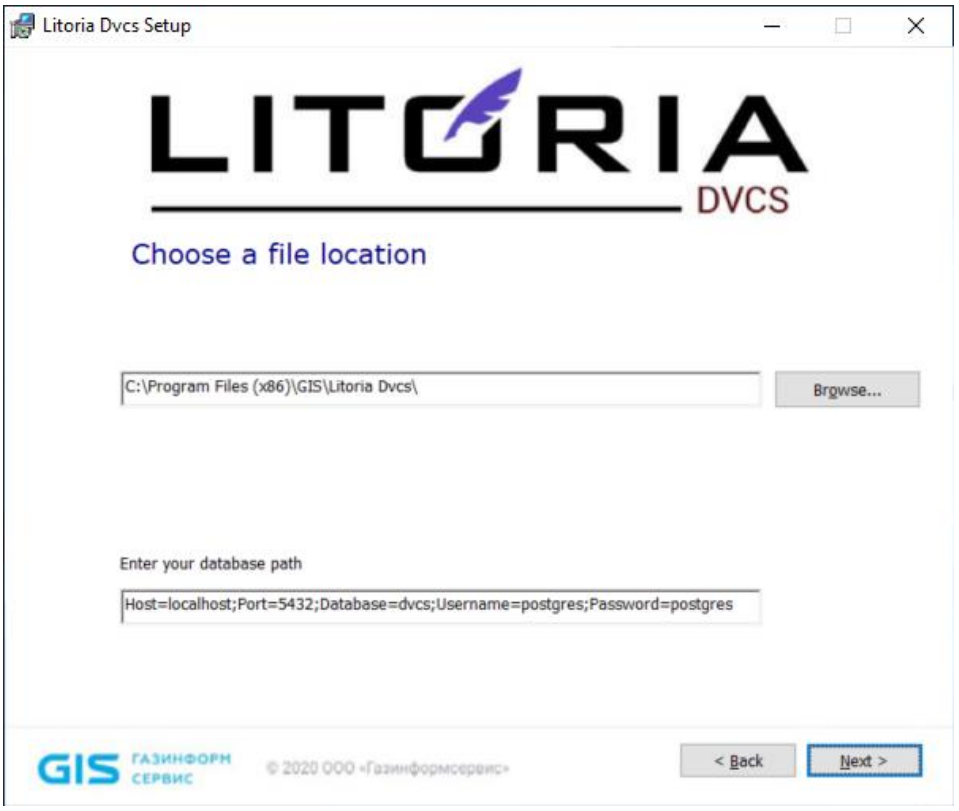

Рисунок 3.8 – Выбор директории установки и параметры БД

3. В появившемся окне подтвердите установку по кнопке «***Установить***» (рисунок 3.9).

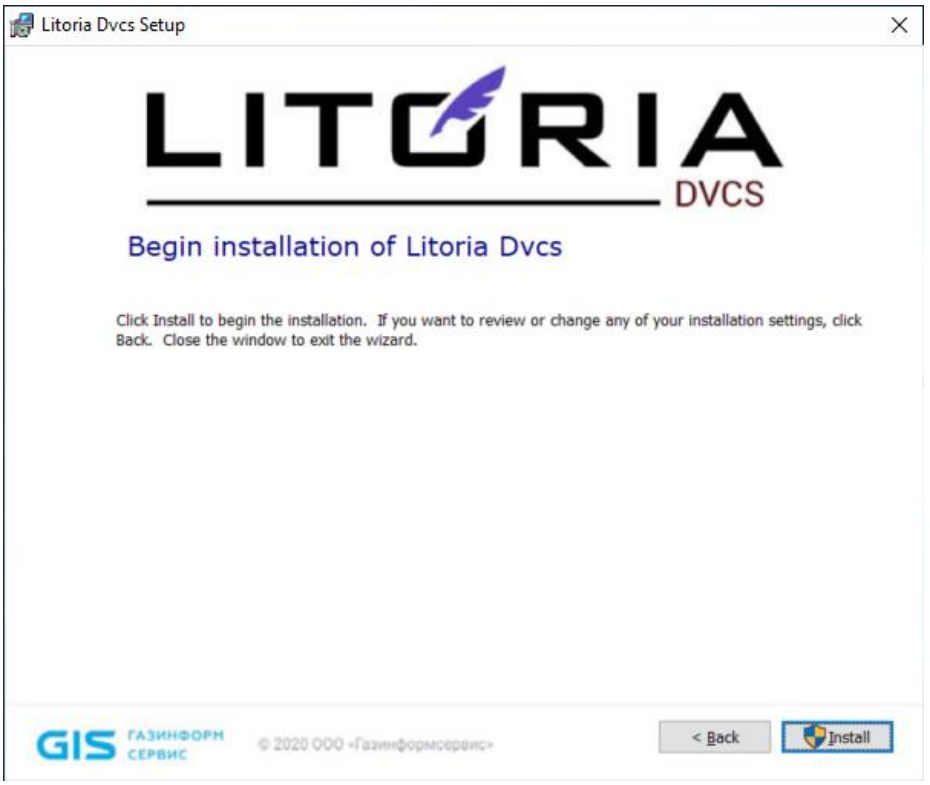

Рисунок 3.9 – Установка комплекса

4. На следующем этапе для выполнения установки распространяемого пакета Microsoft Visual C++ 2015-2019 Redistributable нажмите «***Установить***» (рисунок 3.10).

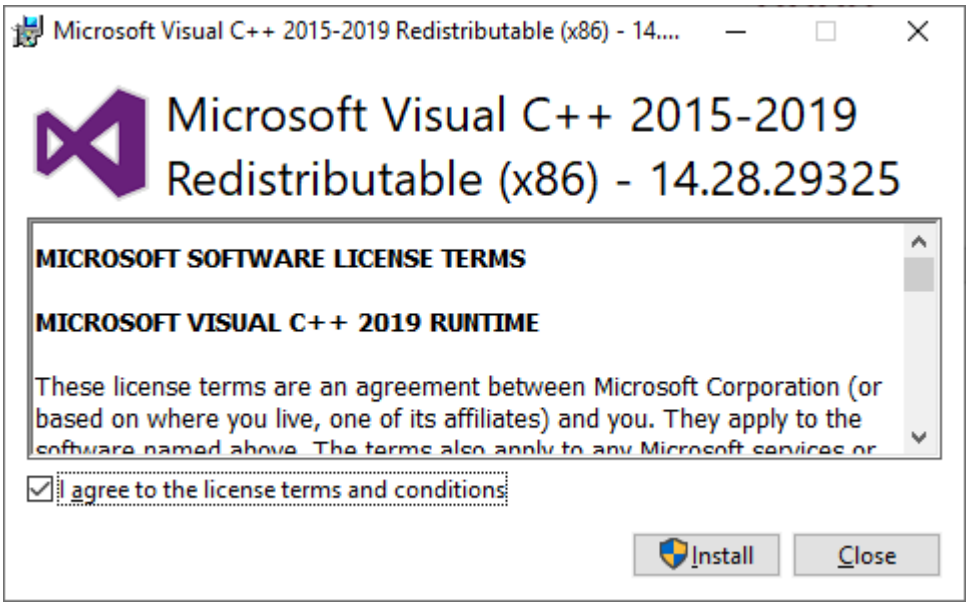

Рисунок 3.10 – Установка пакета Microsoft Visual C++ 2015-2019 Redistributable

5. На следующем этапе для выполнения установки пакета Windows Server Hosting для работы IIS нажмите «***Установить***» (рисунок 3.11).

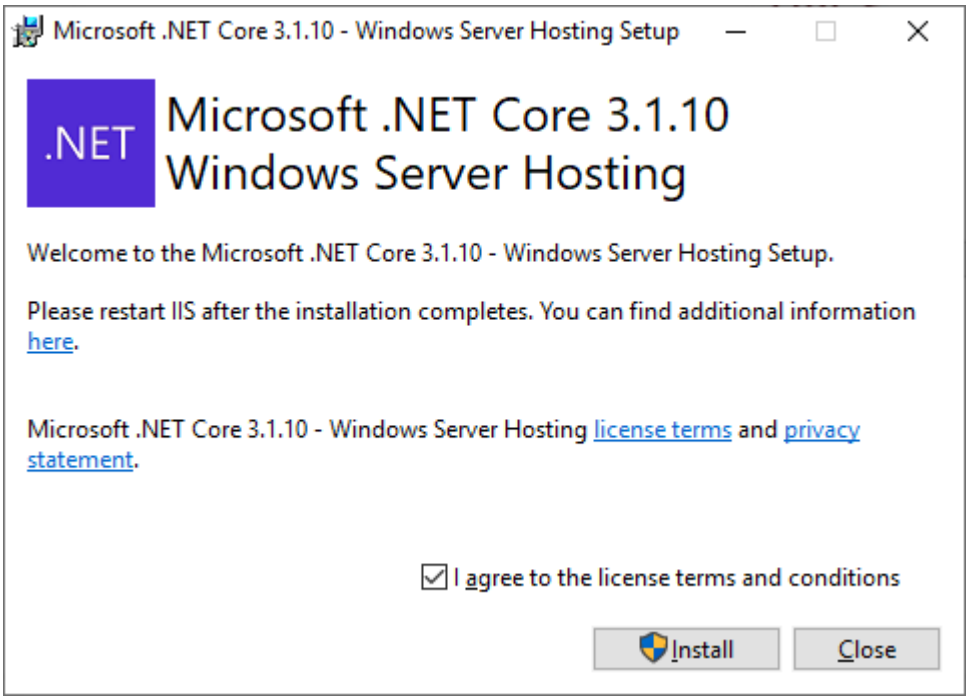

Рисунок 3.11 – Установка Windows Server Hosting пакет для работы IIS

6. По окончанию установки нажмите на кнопку «***Закрыть***» в окне завершения установки (рисунок 3.12).

Рисунок 3.12 – Успешное завершение установки

3.3 Получение сертификатов служб

Перед использованием ПК «Litoria DVCS» необходимо установить сертификаты служб DVCS и TSP[2]. Для этого необходимо выполнить следующие действия:

- создать запросы на выпуск сертификатов служб комплекса;
- отправить созданные файлы запроса в УЦ;
- получить сертификаты служб;
- установить корневые и промежуточные сертификаты в хранилище сертификатов.

3.3.1 Создание запроса на сертификат в УЦ

Создание запросов на сертификат выполняется с помощью средств СКЗИ, реализованного в соответствии с технологией Microsoft CSP (с описанием процедуры создания запросов можно ознакомиться в документации на используемое СКЗИ).

При создании запросов на сертификаты необходимо указать параметры сертификатов, приведенные в таблице 3.1.

[2] При использовании внешней службы TSP, сертификат службы TSP устанавливать не нужно.

Таблица 3.1 – Параметры сертификатов служб

№	Наименование сертификата	Параметры сертификата
1	Сертификат службы DVCS	Сертификат службы DVCS – сертификат, которым подписываются квитанции, выданные службой DVCS в ответ на запрос пользователя. Такой сертификат должен иметь следующие критичные значения параметров использования ключа: – подпись данных; – неотрекаемость; – подпись сертификатов; – подпись списков отзывов. Критичное значение назначения сертификата: – служба DVCS (согласно п. 6 RFC3029, OID 1.3.6.1.5.5.7.3.10).
2	Сертификат службы TSP	Сертификат службы TSP – сертификат, которым подписываются квитанции, выданные службой TSP. Такой сертификат должен иметь следующие критичные значения параметров использования ключа: – подпись данных; – неотрекаемость. Критичное значение назначения сертификата: – штамп времени подписи (согласно п. 2.3 RFC3161, OID 1.3.6.1.5.5.7.3.8).

На основе созданных запросов УЦ выдаст сертификаты, которые затем необходимо установить на рабочую станцию с установленным ПК «Litoria DVCS». Также необходимо установить сертификаты цепочки сертификации и списки отзыва для полученных сертификатов.

Если сертификат был выпущен без нужного OID, то система не примет как сертификат службы!

3.3.2 Установка корневых и промежуточных сертификатов и списков отзыва

Установка корневых и промежуточных сертификатов и списков отзыва должна осуществляться для учетной записи, от имени которой настроена работа пула приложений служб комплекса.

Посмотреть учетную запись, из-под которой настроена работа пула приложений служб, можно в диспетчере служб IIS (кнопка ***«Пуск»→«Все программы»→«Администрирование»→«Диспетчер служб IIS»***). Поле ***«Удостоверение»*** содержит информацию об учетной записи (рисунок 3.13).

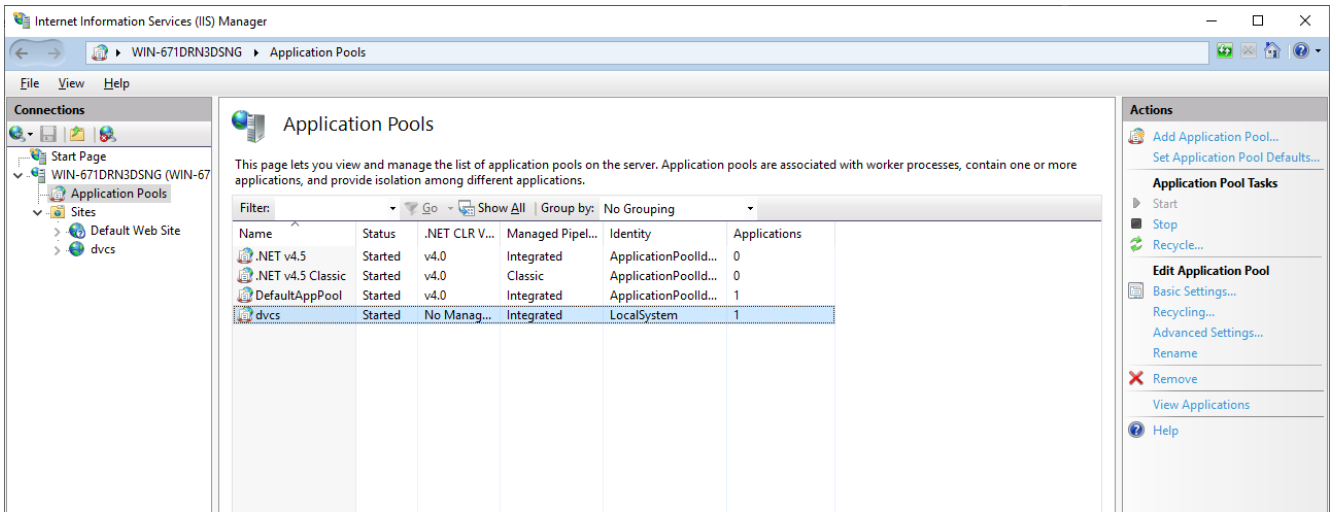

Рисунок 3.13 – Просмотр учетной записи в Диспетчере служб IIS

Для установки корневых и промежуточных сертификатов зайдите под нужной учетной записью в оснастку сертификатов ***«certmgr.msc»*** и установите корневые сертификаты в хранилище «Доверенные корневые центры сертификации».

3.4 Настройка единого web-кабинета

Для настройки единого web-кабинет участника электронного взаимодействия выполните следующие действия:

1. Откройте ***«IIS Manager»*** (***«Пуск»→«Все программы»→«Администрирование»→«Диспетчер служб IIS»***) и в открывшемся окне перейдите к пункту «Сайты» (рисунок 3.14).

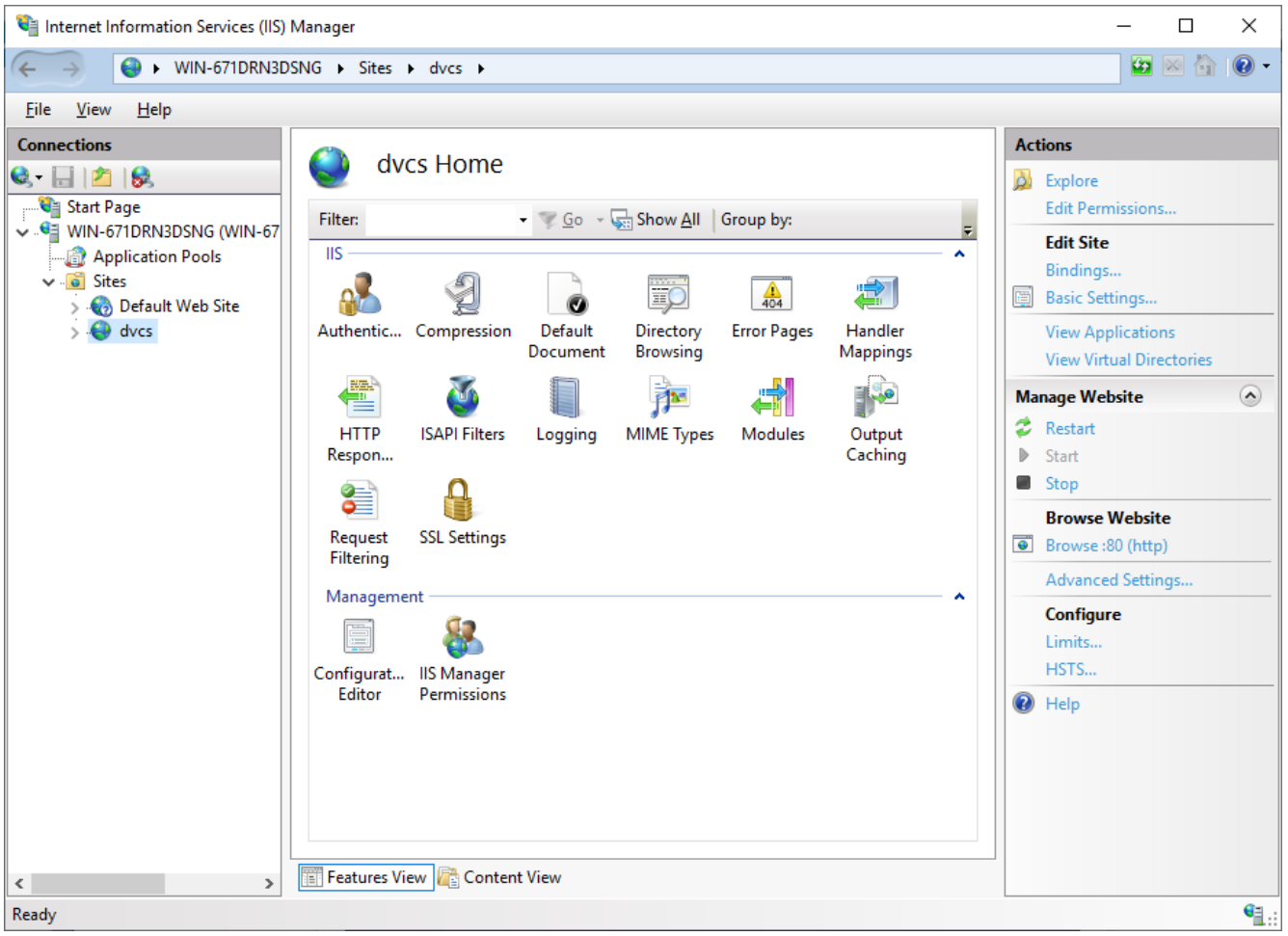

Рисунок 3.14 – Отображение сконфигурированного web-кабинета в IIS

2. В разделе «***Сайты***» отобразится «***DVCS***» – web-кабинет, позволяющий управлять настройками ПК «Litoria DVCS».

3. Для внешнего доступа к web-кабинету в окне «***Привязки сайта***» (рисунок 3.15) нажмите «***Добавить***», и в появившемся окне «***Добавление привязок сайта***» (рисунок 3.16):

- выберите тип «https»;
- введите IP-адрес рабочей станции и номер порта (по умолчанию 443);
- выберите SSL-сертификат, который ранее был установлен на данной рабочей станции.

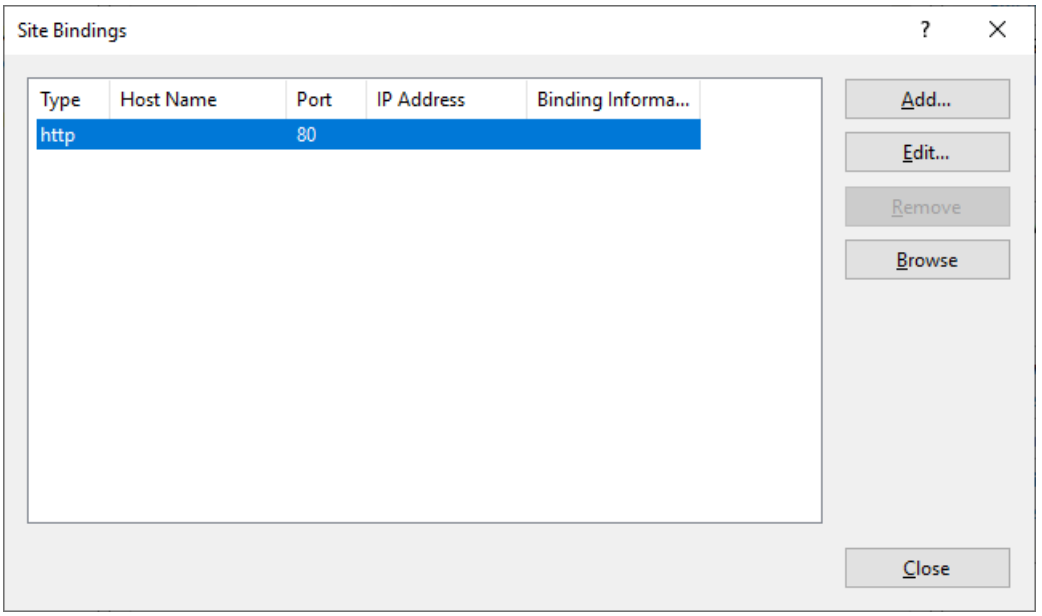

Рисунок 3.15 – Редактирование привязок

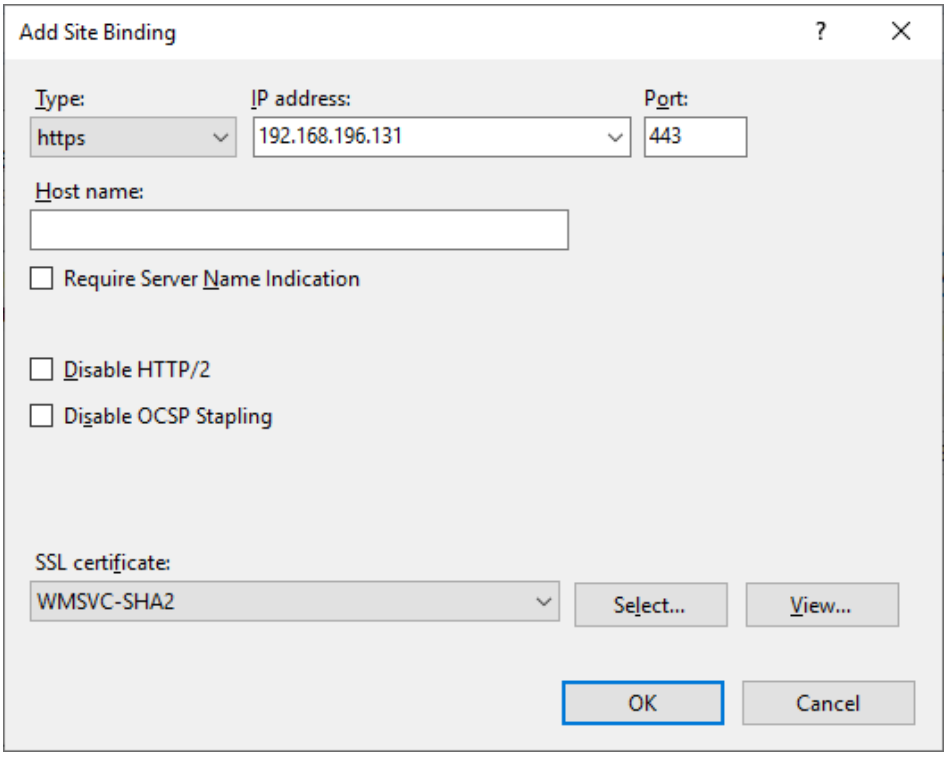

Рисунок 3.16 – Добавление привязки https

Если сайт не запущен (сайт отмечен значком), в области «***Управление сайтами***» необходимо нажать на кнопку ***«Начало»*** (рисунок 3.17). Если сайты запущены, то после внесения изменений необходимо перезапустить сайт ***«DVCS»***, нажав на кнопку ***«Перезапустить»***.

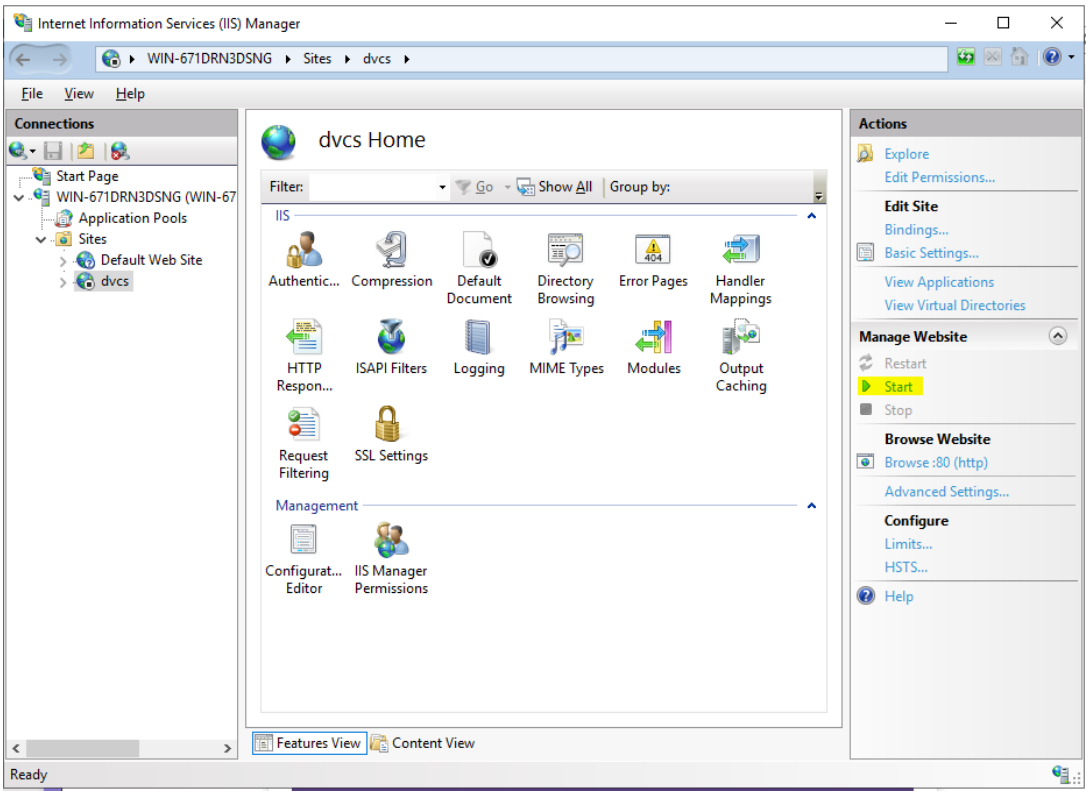

Рисунок 3.17 – Запуск сайта

4. Для перехода к главной странице web-кабинета перейдите к сайту ***«DVCS»*** и выберите действие ***«Обзор веб-сайта»*** (рисунок 3.18).

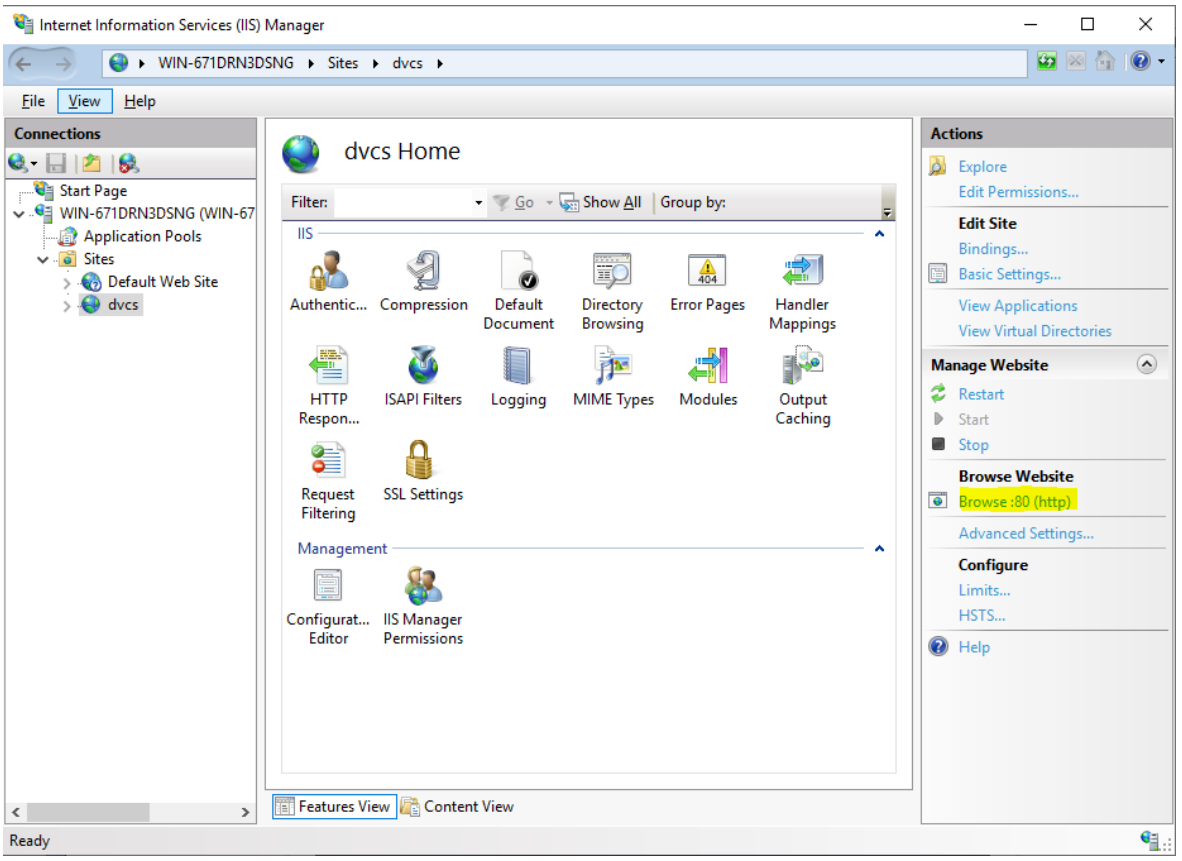

Рисунок 3.18 – Обзор web-сайта DVCS

5. Главная страница web-кабинета представлена на рисунке 3.19.

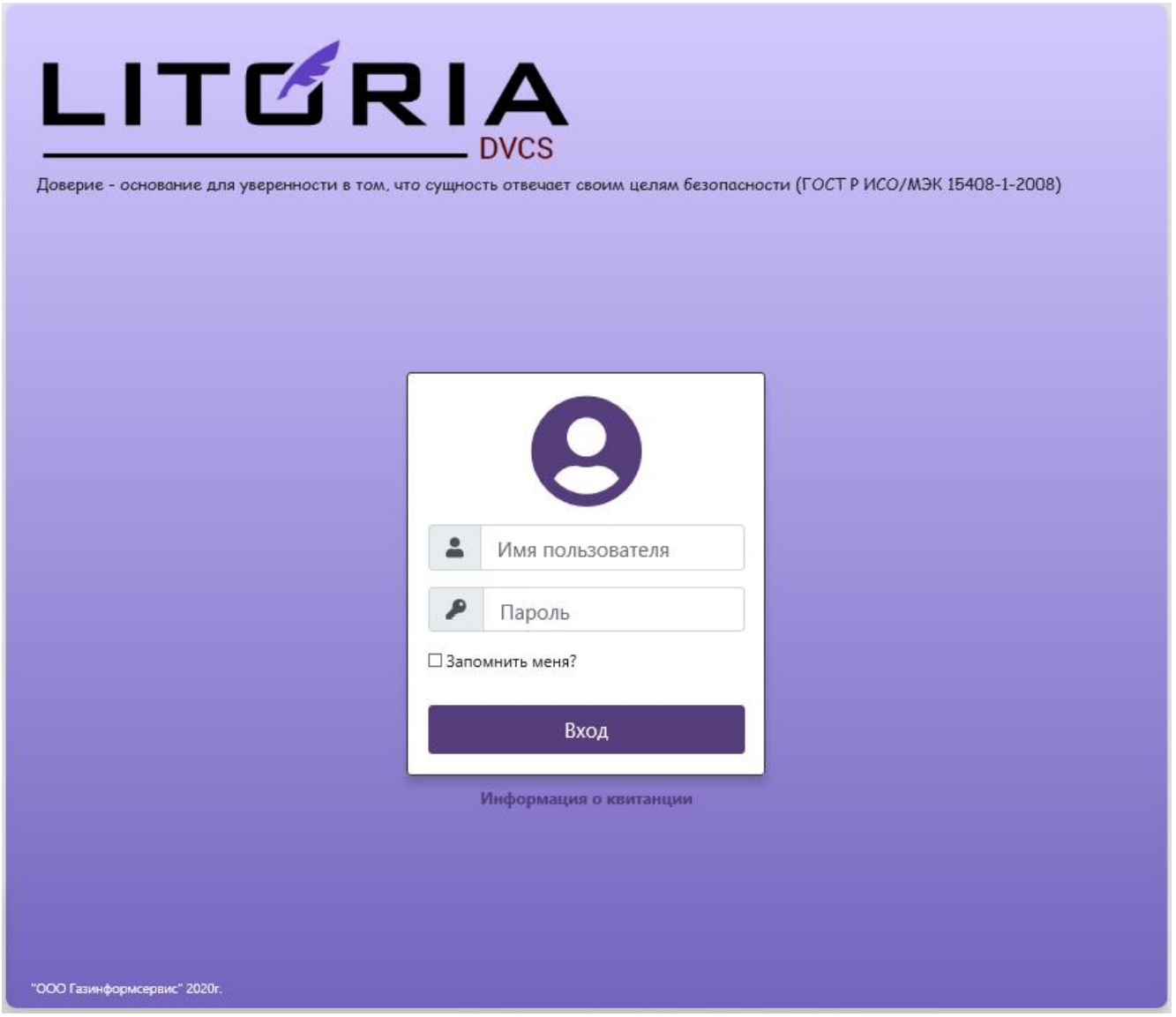

Рисунок 3.19 – Главная страница web-кабинета ПК «Litoria DVCS»

3.5 Активация комплекса

После установки, ПК «Litoria DVCS» работает в режиме пробной версии продукта, в котором доступна полная функциональность комплекса, за исключением того, что в web-кабинете и во всех выдаваемых квитанциях устанавливается значение статуса продукта «пробная версия».

Для выполнения активации выполните следующие действия:

1. Выполните вход в web-кабинет (см. п. 5.1 «Начало работы»).

2. Нажмите ссылку ***«О программе»*** в нижнем правом углу основного окна ПК «Litoria DVCS» (рисунок 3.20).

Рисунок 3.20 – Web-кабинет ПК «Litoria DVCS»

3. В появившемся окне (рисунок 3.21) отобразится информация об использовании пробной версии продукта.

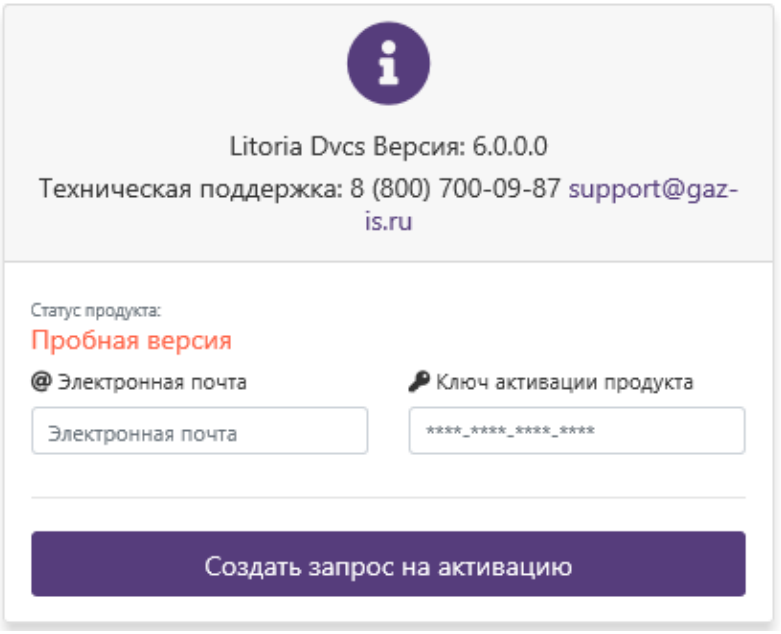

Рисунок 3.21 – Окно «О программе»

4. Для активации продукта введите ключ лицензии и адрес электронной почты, на который в дальнейшем придет сообщение, содержащее ключ активации, и нажмите «***Создать запрос на активацию***» (рисунок 3.22).

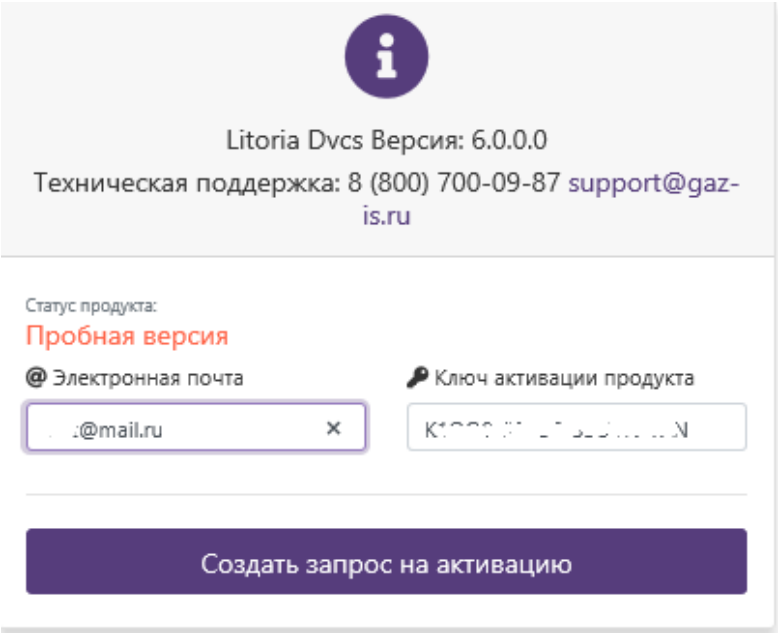

Рисунок 3.22 – Ввод ключа лицензии

5. В появившемся окне (рисунок 3.23) скопируйте в буфер обмена запрос для активации продукта по кнопке « » .

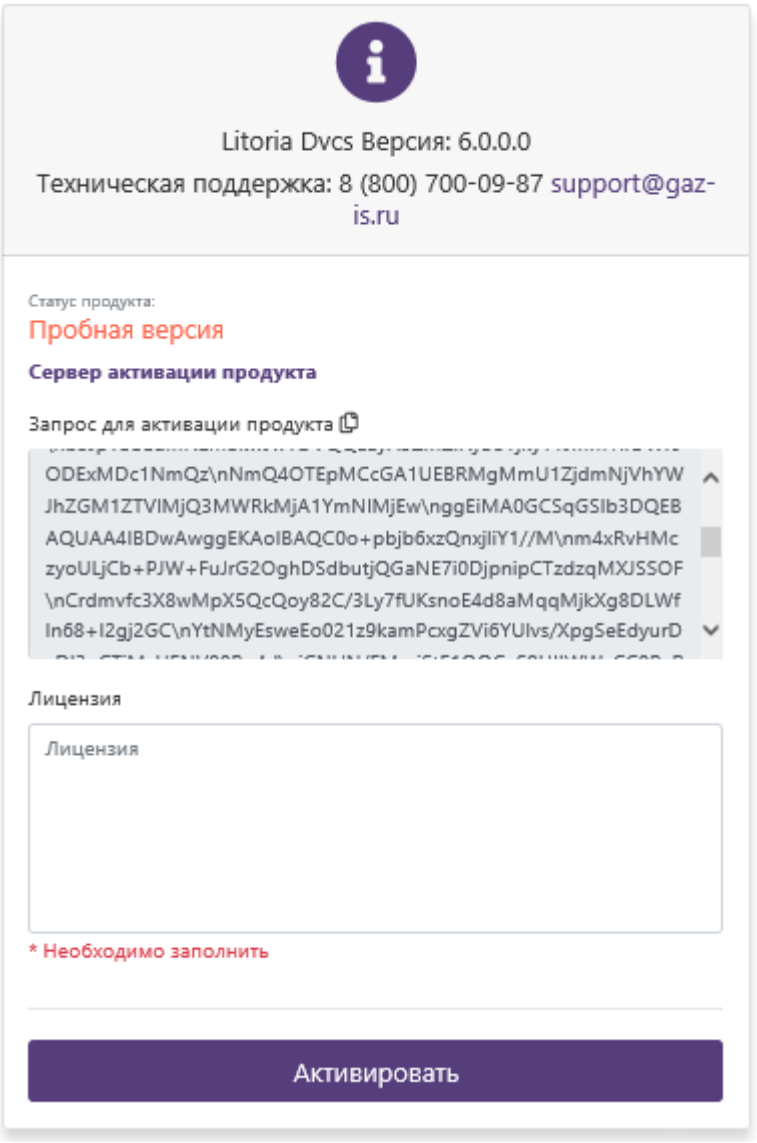

Рисунок 3.23 – Запрос для активации продукта

6. Перейдите на сайт активации продуктов ООО «Газинформсервис» по ссылке https://license.gaz-is.ru/offlineActivate.

При отсутствии подключения к сети Интернет на рабочей станции, на которой установлен ПК «Litoria DVCS», необходимо перейти по указанной ссылке на любой другой рабочей станции, с имеющимся подключением к сети Интернет.

7. В окне активации (рисунок 3.24) вставьте скопированную в буфер обмена информацию с помощью контекстного меню правой кнопки мыши и нажмите кнопку «***Активировать***».

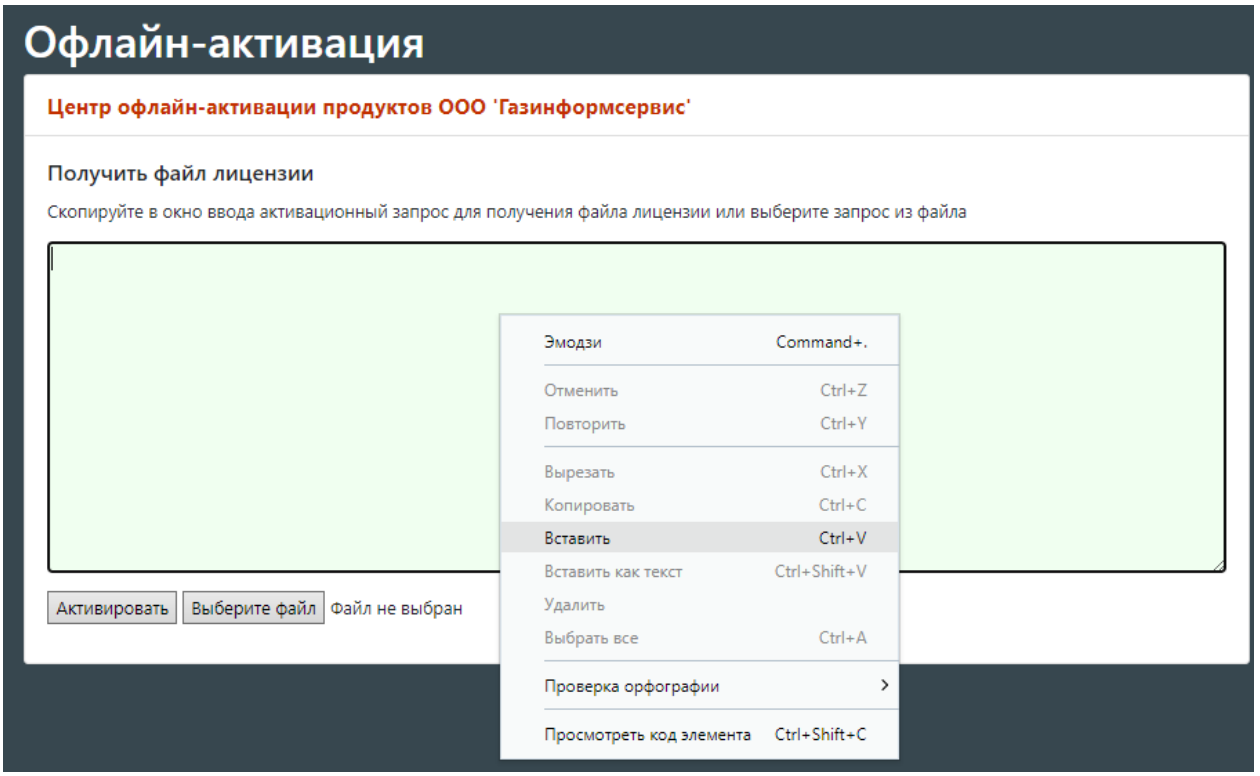

Рисунок 3.24 – Вставка активационного запроса

8. В появившемся окне (рисунок 3.25) введите ключ, полученный на указанный ранее адрес электронной почты, и нажмите кнопку «***Активировать***».

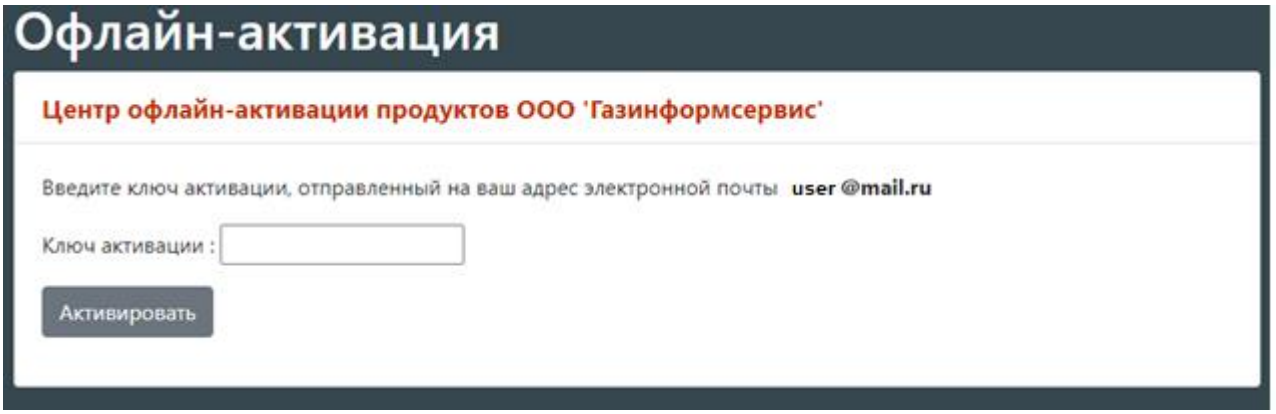

Рисунок 3.25 – Ввод ключа активации

9. В появившемся окне (рисунок 3.26) сохраните файл лицензии по кнопке ***«Скопировать в буфер обмена»***.

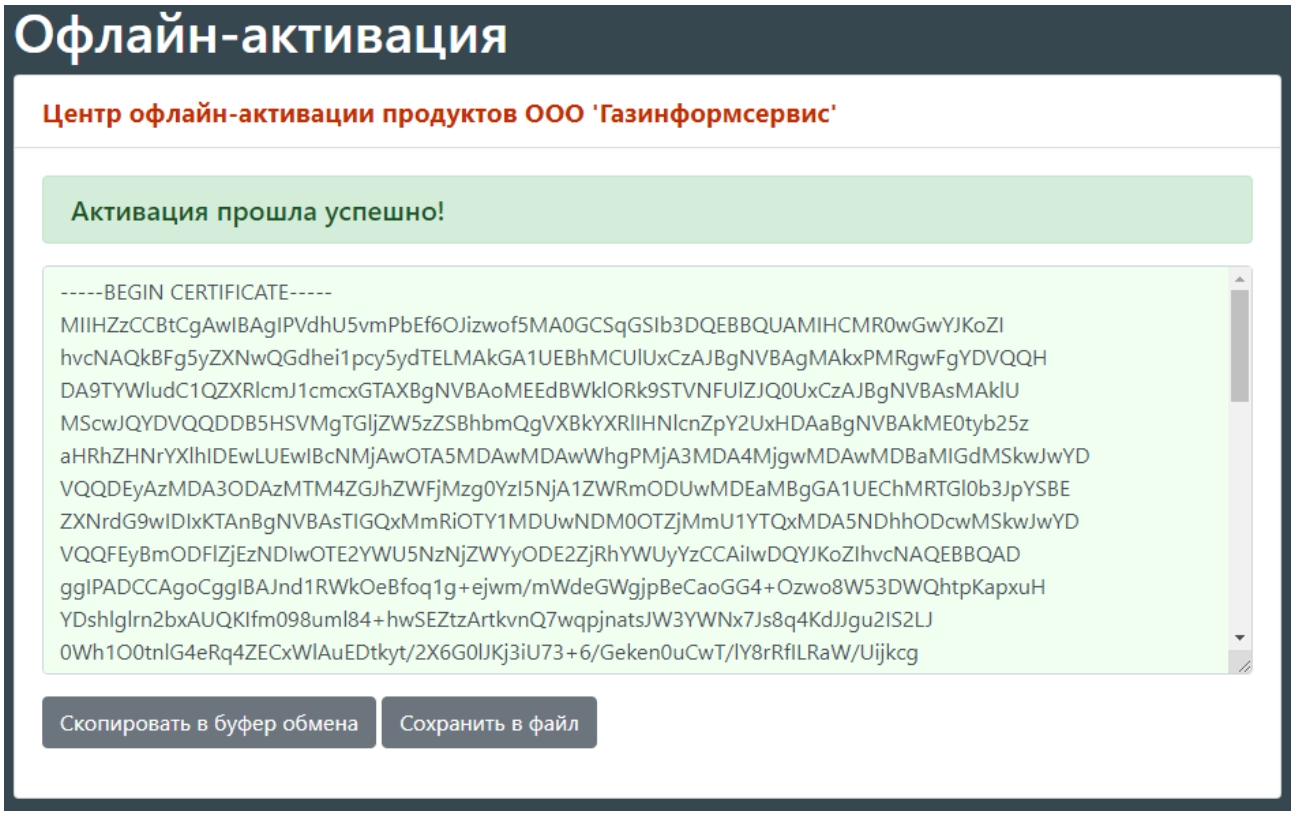

Рисунок 3.26 – Сохранение в буфер обмена файла лицензии

10. Вставьте скопированную информацию в окно «***Лицензия***» (рисунок 3.27) с помощью контекстного меню правой кнопки мыши и нажмите кнопку «***Активировать***».

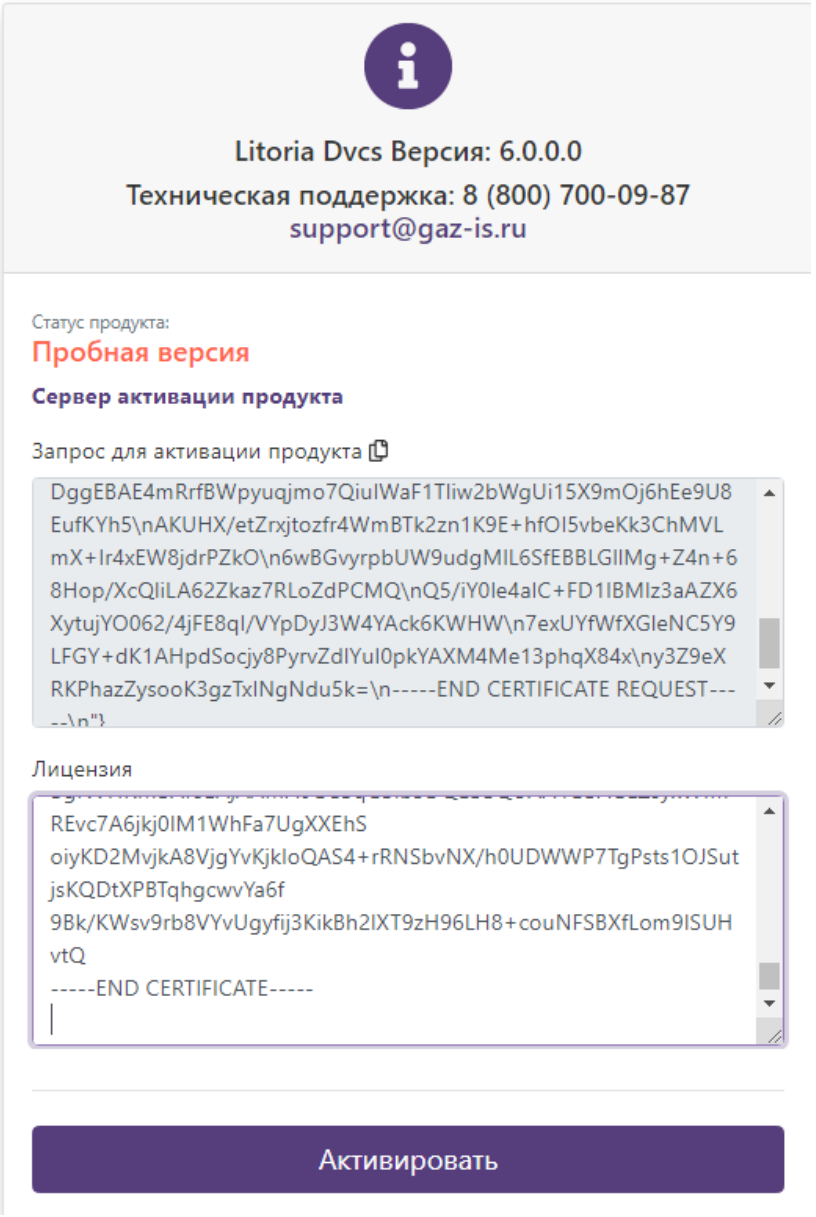

Рисунок 3.27 – Вставка файла лицензии

11. В результате успешно пройденной активации окно «О программе» примет вид, представленный на рисунке 3.28 с дополнительным сообщением об успешной установке лицензии. На указанный адрес электронной почты придет сообщение о завершении активации продукта.

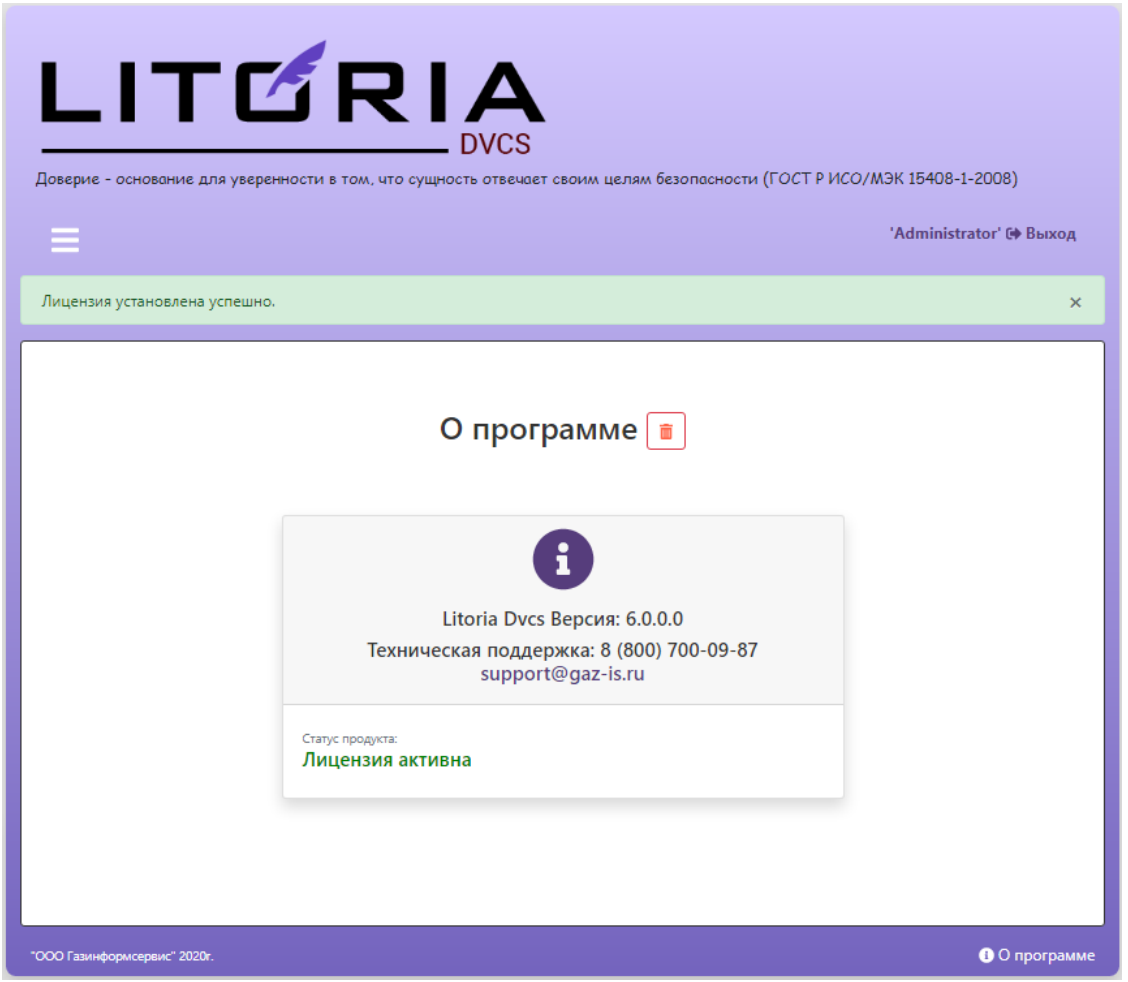

Рисунок 3.28 – Успешная активация продукта

4 Настройка ПК «Litoria DVCS» в ОС семейств Linux

Настройка ПК «Litoria DVCS» будет рассмотрена на примере ОС «ALT Linux». Ввиду того, что ОС семейства Linux могут значительно отличаться друг от друга в вопросе использования команд и их синтаксиса при настройке различных приложений.

Перед началом настройки ПК «Litoria DVCS» необходимо убедиться в выполнении требований к рабочей станции, на которую устанавливается ПК «Litoria DVCS», и установить дополнительное программное обеспечение (см. разделы 2.1 и 2.2).

Перед началом использования ПК «Litoria DVCS» необходимо выполнить следующие настройки:

- установить и настроить корректное соединение с СУБД «PostgreSQL» или СУБД «Jatoba»;
- установить и настроить обратный прокси-сервер;
- установить и настроить ПК «Litoria DVCS»;
- получить и выполнить установку сертификатов служб;
- настроить web-кабинет участника электронного взаимодействия;
- активировать ПК «Litoria DVCS».

4.1 Настройка обратного прокси на примере установки Apache2

Для подключения к web-части ПК «Litoria DVCS» с использованием обратного прокси-сервера необходимо выполнить следующие действия:

1. Установить пакет *Apache2* (в ОС «Alt Linux» используется команда *apt-get install apache2*).

2. Установить запуск веб-сервера при старте ОС.

3. Запустить *Apache2*.

4. Проверить работоспособность *Apache2*, перейдя в браузере по адресу *http://localhost*. В случае корректной работы появится сообщение *«Its Works!»*. (подробнее работа с *Apache2* в ОС «Alt Linux» изложена в материале *https://wiki.lblss.ru/Вебсервер_Apache2_на_ALT_Linux*).

5. Создать файл *dvcs.conf* по пути */etc/httpd2/conf/sites-available*.

6. Создать программную ссылку на указанный выше файл, с тем же именем в

/etc/httpd2/conf/sites-enabled.

Содержимое файла *dvcs.conf*:

```
<VirtualHost *:80>
ProxyPreserveHost On
ProxyPass / http://127.0.0.1:5000/
ProxyPassReverse / http:// 127.0.0.1:5000/
ErrorLog /var/log/httpd2/dvcs-error.log
CustomLog /var/log/httpd2/dvcs-access.log common
</VirtualHost>,
```

"VirtualHost"	Используемый порт для подключения
"ProxyPreserveHost"	включение режима реверс-прокси
"ErrorLog"	путь для сохранения файла лога ошибок
"CustomLog"	путь к общему файлу логу
"ProxyPas"	IP адрес публикуемого ресурса
"ProxyPassReverse"	URL-адрес, на который Apache должен перезаписать URL-адреса, которые будут перенаправлять на проксированный (скрытый) URL-адрес

Адрес *http://127.0.0.1:5000/* используется по умолчанию. При необходимости его изменить, достаточно в файл настроек службы ДТС *appsettings.json* (раздел 7) добавить дополнительный блок.

```
{
  "Kestrel": {
    "Endpoints": {
      "Http": {
        "Url": "http://<url:port>"
      },
      "Https": {
        "Url": "https:// <url:port1>"",
        "Certificate": {
          "Path": "",
          "Password":""
        }
      }
    }
  }
}
```

"Http"	Блок настроек подключения по протоколу HTT, URL – используемый адрес для подключения к сервису
"Https"	Блок настроек подключения по протоколу HTTPS, URL – используемый адрес для подключения к сервису
"Certificate"	Блок настроек использования сертификатов для защищённого подключения.
"Path"	Путь к файлу формата *.pfx
"Password"	Пароль для доступа к закрытому ключу

7. Добавить в конец файла */etc/httpd2/conf/httpd2.conf* строки, перечисляющие модули, необходимые для работы *Apache*:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
```

4.2 Установка и настройка ПК «Litoria DVCS»

Для установки и настройки ПК «Litoria DVCS» необходимо выполнить следующие действия:

1. Установить пакет *litoriadvcs-<версия>.rpm*. После установки каталог с исполняемыми файлами будет находиться в директории */opt/GIS/litoriadvcs*.

2. Задать параметры для подключения и работы с БД в файле настроек, расположенному по пути */opt/GIS/litoriadvcs/dvcs/appsettings.json* (описание файла приведено в разделе 7).

3. В каталоге */opt/GIS/litoriadvcs* после установки созданы скрипты для работы со службой ДТС:

- dvcs_enable.sh – разрешение запуска службы ДТС при запуске системы
- dvcs_disable.sh – прекращение запуска службы ДТС при запуске системы
- dvcs_start.sh – старт службы ДТС;
- dvcs_stop.sh – остановка службы ДТС
- update_enable.sh – разрешение запуска службы автопродления при запуске системы
- update_disable.sh - прекращение запуска службы автопродления при запуске системы
- update_start.sh - запуск службы автопродления при запуске системы
- update_stop.sh - остановка службы автопродления при запуске системы

4. Для запуска службы ДТС необходимо запустить скрипт *dvcs_start.sh* от имени и с правами суперпользователя.

5. Перейти в браузере на страницу ДТС используя адрес *http://<url>:port*, где:

url – адрес рабочей станции, на которой запущена служба ДТС;

port – порт, по которому происходит подключение.

4.3 Выпуск и установка сертификатов

Как и в случае работы ПК «Litoria DVCS» в ОС семейств Windows, в ОС семейств Linux для корректного функционирования системы необходимо, чтобы сертификаты для работы со службой ДТС были установлены в хранилище того пользователя, от имени которого происходит запуск службы.

Просмотреть учетную запись, которая производит запуск службы, можно в файле /etc/systemd/system/litoriadvcs.service

Дальнейшая настройка ПК «Litoria DVCS» аналогична настройкам для работы комплекса в ОС семейства Windows, приведенным в разделе 3 «Настройка ПК «Litoria DVCS».

5 Использование ПК «Litoria DVCS»

Основные функциональные возможности ПК «Litoria DVCS» по созданию запросов на проверку электронной подписи или действительности сертификата ключа проверки электронной подписи, анализ запросов и формирование ответов, содержащих информацию о проведенных проверках, управление настройками службы, учетными записями пользователей, журналирование и получение статистической информации о произведенных операциях доступны в едином web-кабинете участника электронного взаимодействия.

5.1 Начало работы

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 5.1). Функциональные возможности web-кабинета станут доступны после успешного прохождения аутентификации.

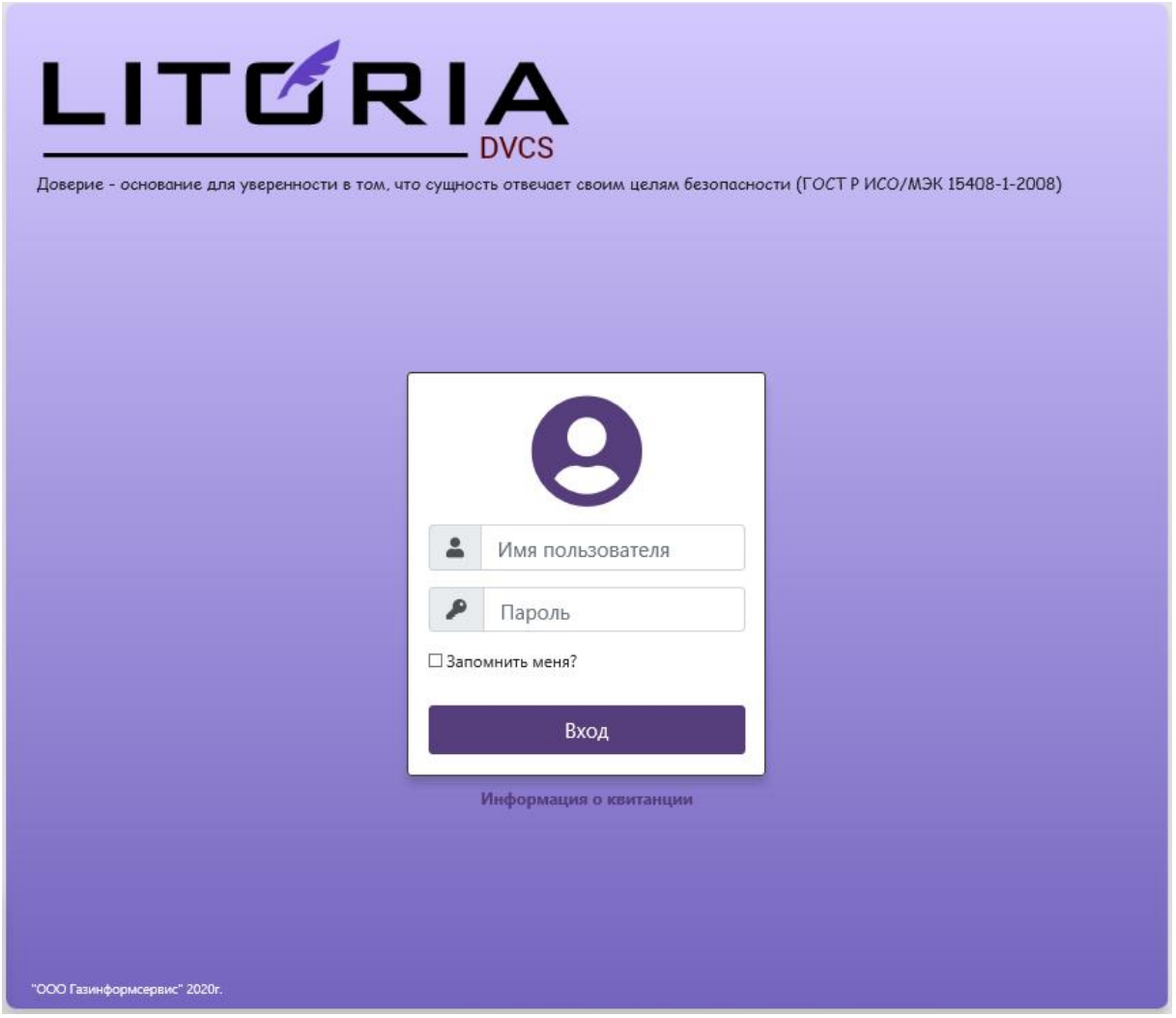

Рисунок 5.1 – Начальная страница web-кабинета ПК «СДТС «Litoria DVCS»

5.1.1 Первый вход администратора

Для первого входа в web-кабинет введите имя встроенного администратора сайта, его пароль и нажмите на кнопку ***«Вход»*** (рисунок 5.2). Учетная запись встроенного администратора создается при установке ПК «Litoria DVCS» и имеет следующие данные: имя пользователя – **Administrator**, пароль – **Admin123**@#.

Учетную запись встроенного администратора невозможно удалить из web-кабинета и изменить его роль.

В целях безопасности рекомендуется создать дополнительную учетную запись с правами администратора, а встроенную учетную запись Администратора заблокировать

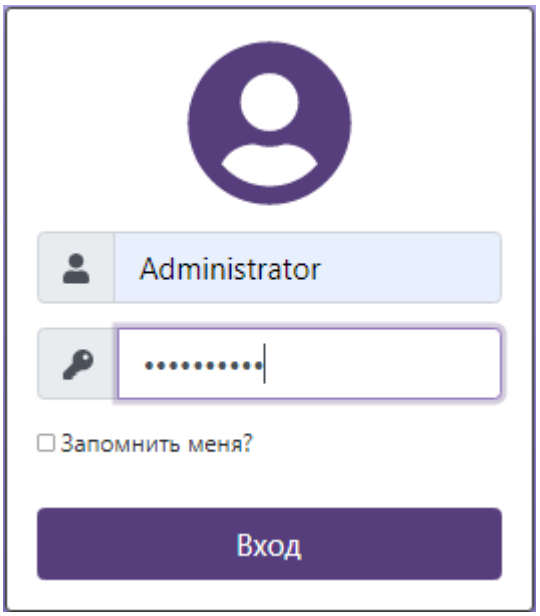

Рисунок 5.2 – Первый вход в web-кабинет

После успешной аутентификации администратора появится главное окно web-кабинета ПК «Litoria DVCS» (рисунок 5.3), в котором администратору безопасности доступно управление следующими функциями:

- управление учетными записями пользователей и администраторов;
- управление настройками служб DVCS и TSP (добавление сертификатов служб, добавление служб штампов времени);
- управление маршрутами;
- просмотр общих настроек ПК «Litoria DVCS» в формате дашборда;

- просмотр и отслеживание операций и квитанций всех пользователей (поиск квитанций для проверяемого документа, проверка соответствия документа квитанции);
- просмотр архива проводимых операций;
- формирование и просмотр статистических отчётов по операциям пользователей.

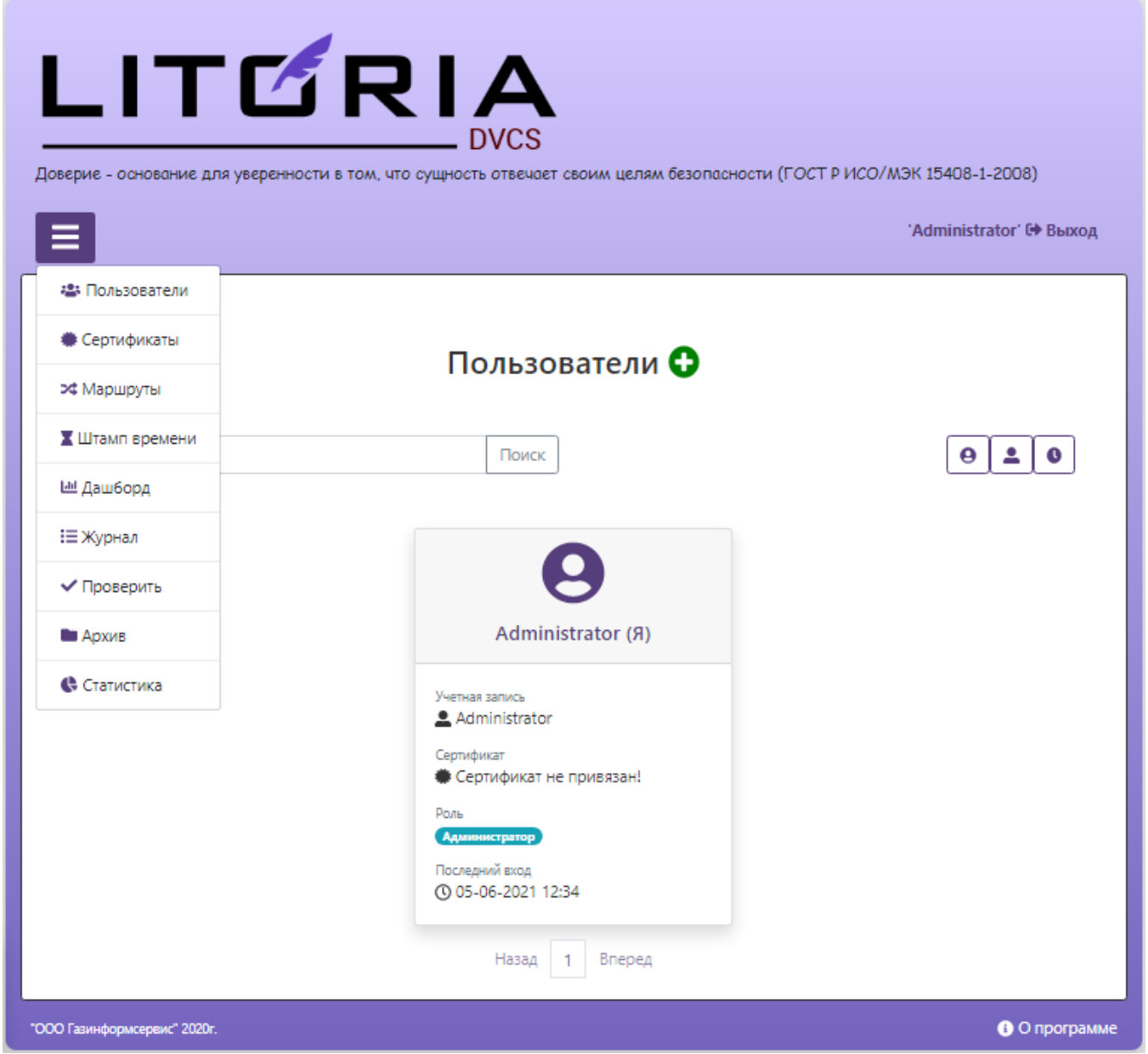

Рисунок 5.3 – Вид главной страницы web-кабинета после авторизации администратора

5.1.2 Смена пароля администратора

После первого входа в web-кабинет администратор должен сменить пароль для входа в соответствии со следующими требованиями:

- длина пароля не менее 8 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения;
- при смене пароля недопустимо использовать 5 последних паролей, использованных ранее;
- после третьего неверного ввода идентификационных данных учетная запись блокируется на 60 минут;
- период смены пароля - не реже одного раза в 180 дней.

Требования к парольной информации задаются в соответствии с политикой эксплуатирующей организации и могут быть изменены в соответствии с ней в конфигурационном файле *appsettings.json* (см. п. 6 «Настройки конфигурационных файлов»).

Для смены пароля выполните следующие действия:

1. Выберите пункт меню ***«Пользователи»,*** нажмите на ссылку ***«Администратор (Я)»*** и перейдите к редактированию выбранной учетной записи (рисунок 5.4).

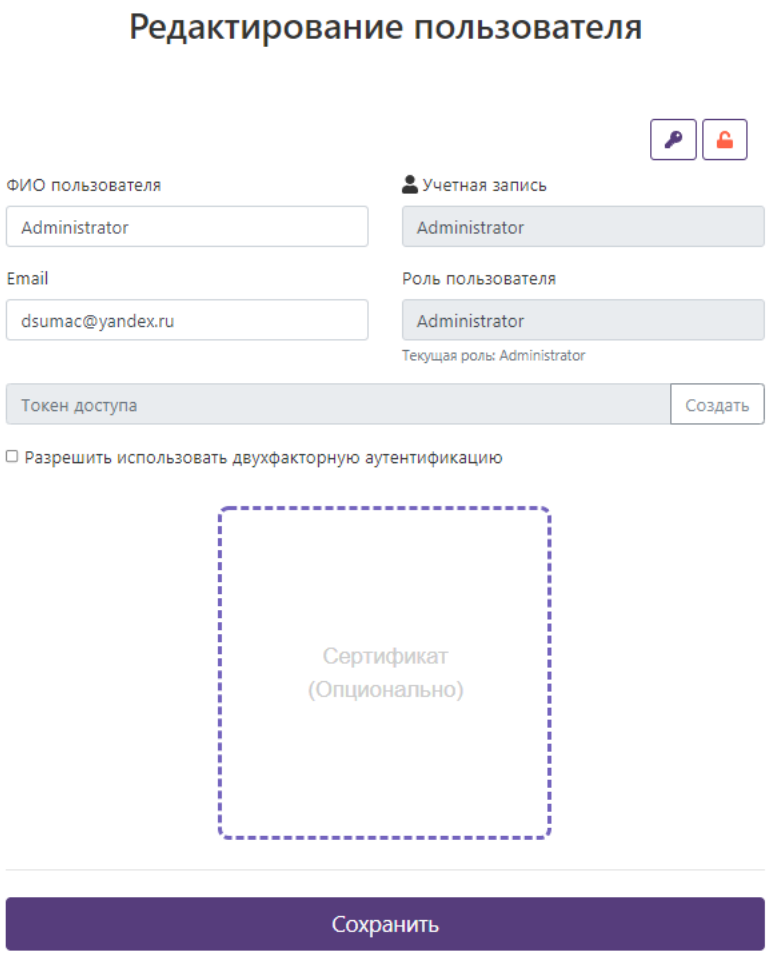

Рисунок 5.4 – Редактирование учетной записи администратора

2. По кнопке «  » перейдите в окно изменения пароля (рисунок 4.5), введите новый пароль в соответствии с предъявляемыми к нему требованиями и нажмите «***Сохранить***».

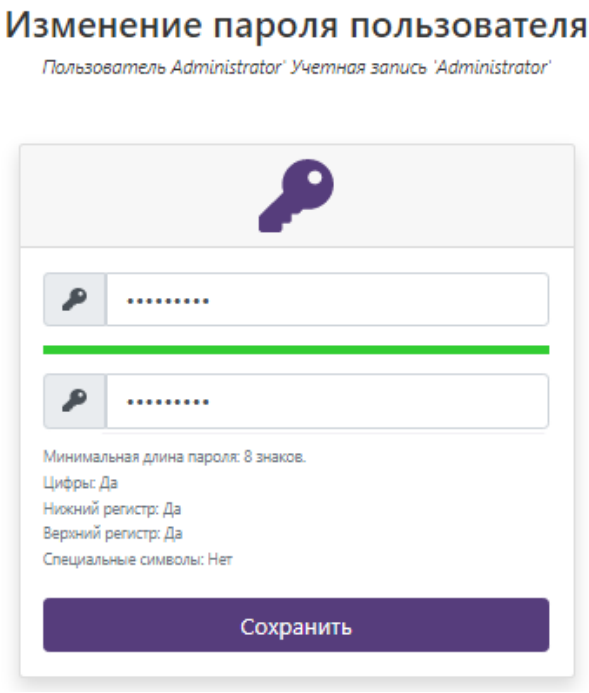

Рисунок 5.5 – Изменение пароля администратора

5.2 Управление учетными записями

Управление учетными записями доступно администратору в пункте меню ***«Пользователи»*** после успешного прохождения аутентификации в web-кабинете «ПК «Litoria DVCS».

В зависимости от предоставляемых полномочий, администратор может создать учетную запись:

- администратора (управление всеми функциональными возможностями web-кабинета «ПК «Litoria DVCS»).
- пользователя (управление собственной учетной записью, проверка документов, просмотр статистических отчётов и архива квитанций).

Функциональные возможности, доступные администратору:

- управление учетными записями пользователей и администраторов;
- добавление сертификатов служб DVCS и TSP;
- добавление маршрутов, по которым будет происходить разбор DVC-запроса;
- добавление адреса службы TSP по которому служба DVCS обращается к сервису TSP;
- просмотр всех настроек ПК «Litoria DVCS», используемых в работе служб DVCS и TSP;
- просмотр системного журнала;

- проверка электронных документов;
- просмотр архива квитанции, полученных в ответ на DVC-запросы всех пользователей;
- просмотр сводных данных по квитанциям;
- продление срока доверенного архивного хранения подписанных квитанций в автоматическом режиме с помощью службы продления квитанций.

Функциональные возможности, доступные пользователю:

- управление собственной учетной записью;
- проверка электронных документов (типы DVC-запросов: VSD, VPKC, CPD);
- просмотр архива квитанции, полученных в ответ на DVC-запросы, оправленных пользователем;
- просмотр сводных данных по квитанциям, оправленных пользователем.

5.2.1 Создание учетной записи пользователя/администратора

Для создания новой учетной записи выполните следующие действия:

1. Перейдите в пункт меню ***«Пользователи»*** и нажмите на кнопку « » (рисунок 5.6).

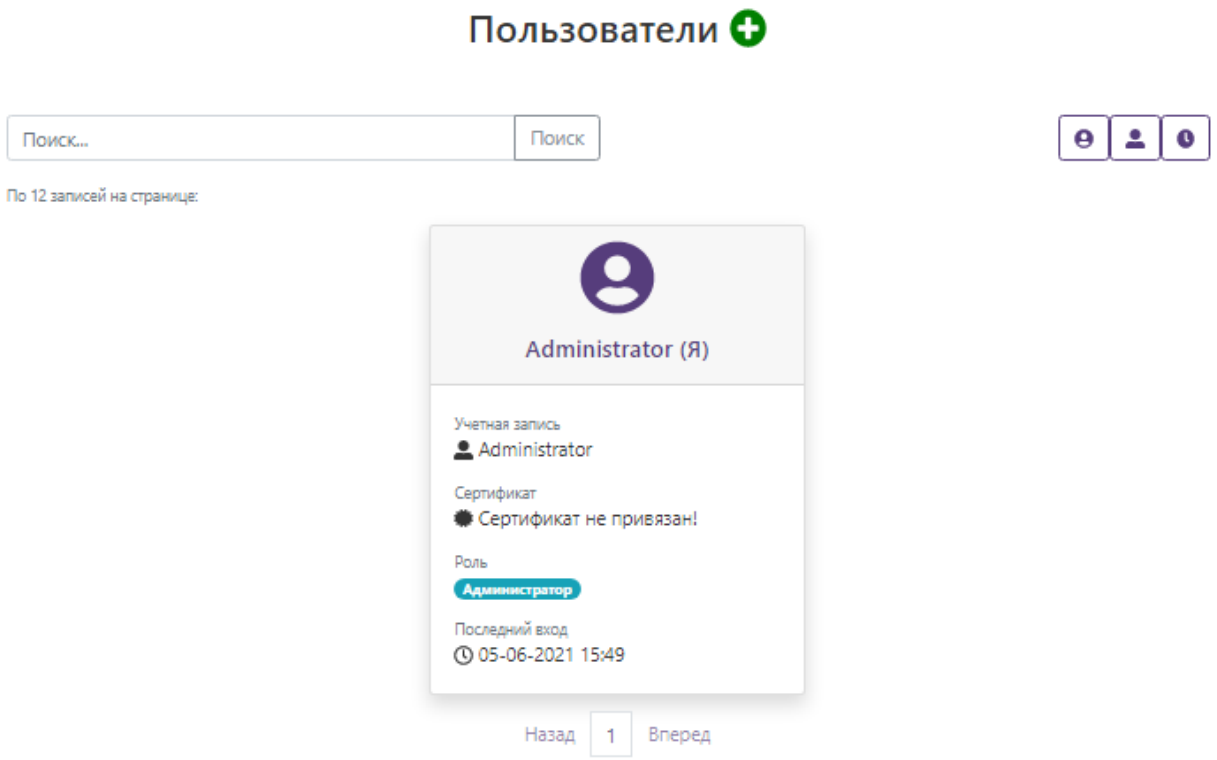

Рисунок 5.6 – Пункт меню «Пользователи»

2. В появившемся окне (рисунок 5.7) заполните данные о создаваемой учетной записи:

- ФИО пользователя;
- учетная запись пользователя;
- адрес электронной почты (при включенной двухфакторной аутентификации на заданный адрес электронной почты отправляется ключ подтверждения, который необходимо будет ввести в дополнительное окно при входе);
- пароль пользователя;
- роль пользователя (администратор или пользователь) в зависимости от предоставляемых ему полномочий;
- разрешение использования двухфакторной аутентификации (при включении двухфакторной аутентификации при каждом прохождении аутентификации пользователю на почту будет отправляться ключ, который необходимо ввести в дополнительное окно при входе);
- добавление сертификата аутентификации при отправке DVC-запроса.

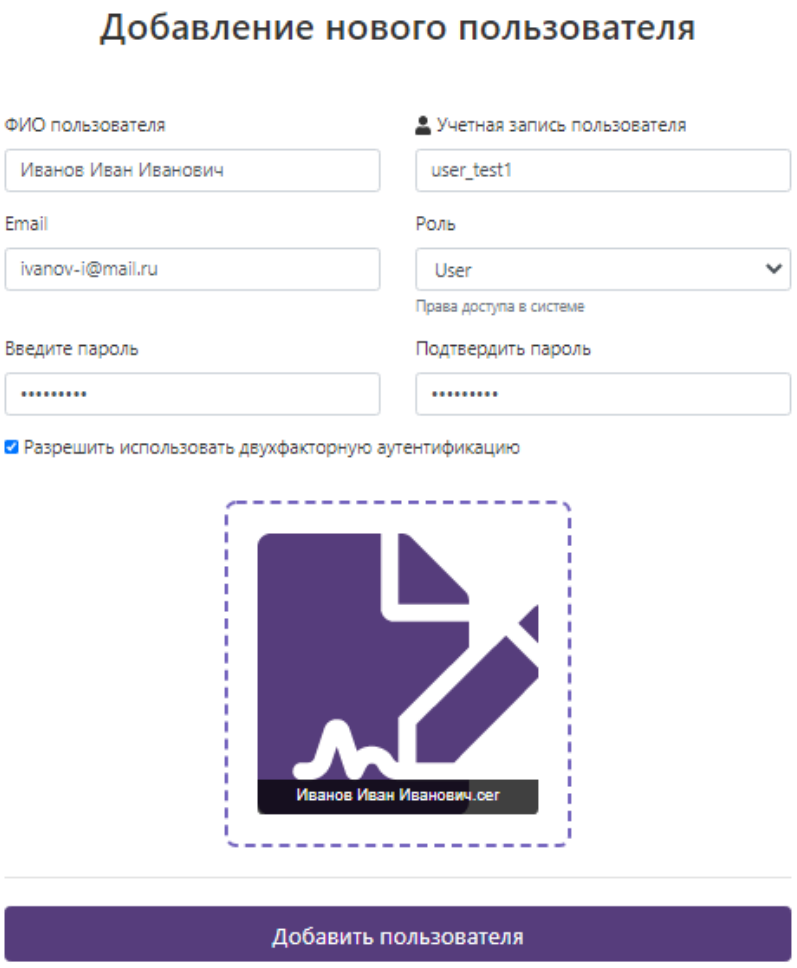

Рисунок 5.7 – Добавление нового пользователя

3. Нажмите на кнопку «***Добавить пользователя***» для завершения операции создания учетной записи.

4. При успешном завершении операции создания учетной записи появится сообщение *«Пользователь <ФИО пользователя> учетная запись <учетная запись пользователя> создан успешно»* и созданная учетная запись отобразится в списке пользователей (рисунок 5.8).

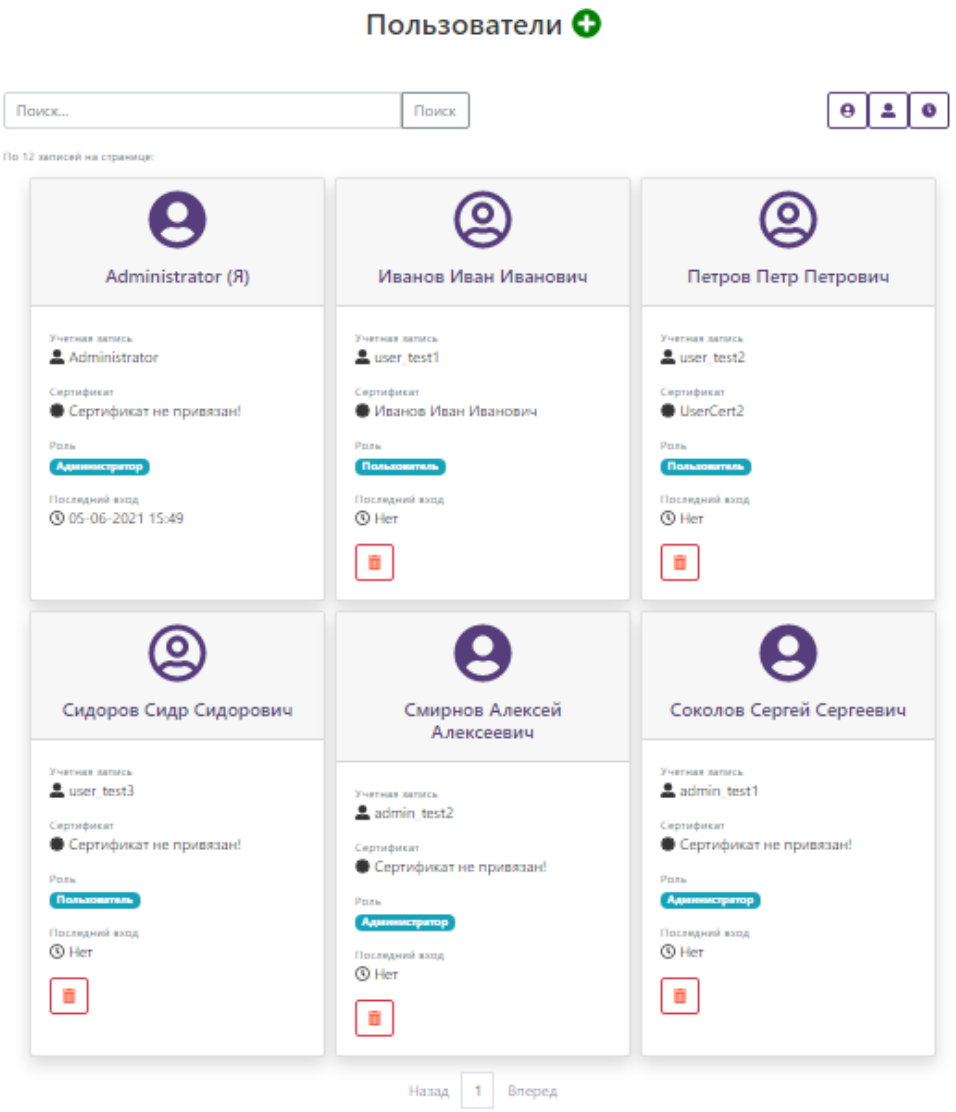

Рисунок 5.8 – Отображение добавленной учетной записи в списке пользователей

Список учетных записей в пункте меню «Пользователи» можно отсортировать по имени учетной записи (кнопка «»), по ФИО пользователя (кнопка «») или по времени последнего входа (кнопка «»).

Для быстрого поиска необходимой учетной записи в списке следует использовать функцию ***«Поиск»*** (рисунок 5.9).

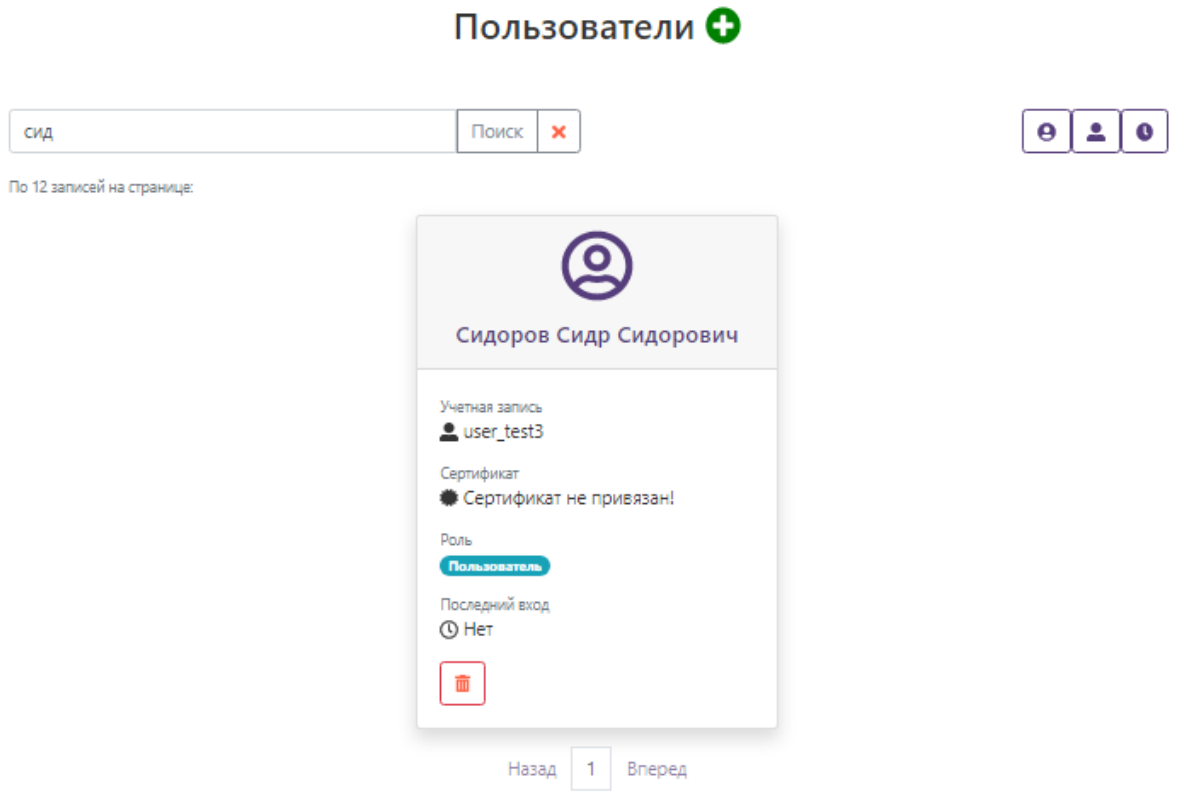

Рисунок 5.9 – Поиск учетной записи в списке пользователей

5.2.2 Просмотр и редактирование учетной записи

Для редактирования учетной записи выполните следующие действия:

1. В пункте меню ***«Пользователи»*** в списке добавленных пользователей (рисунок 4.8) щелкните по нужной учетной записи.

2. В открывшемся окне (рисунок 5.10) доступны для изменения следующие параметры учетной записи:

- изменение личных параметров учетной записи (ФИО пользователя, Email, роль пользователя);
- управление сертификатами учетной записи (добавление нового сертификата, просмотр/удаление имеющегося сертификата);
- генерация и добавление токена доступа (используется при отправке API-запросов, см. п. 8 «Модуль REST API»);
- разрешение использования двухфакторной аутентификации;
- изменение пароля учетной записи по кнопке « » ;
- блокировка учетной записи по кнопке « » (учетная запись пользователя блокируется до момента её разблокировки администратором).

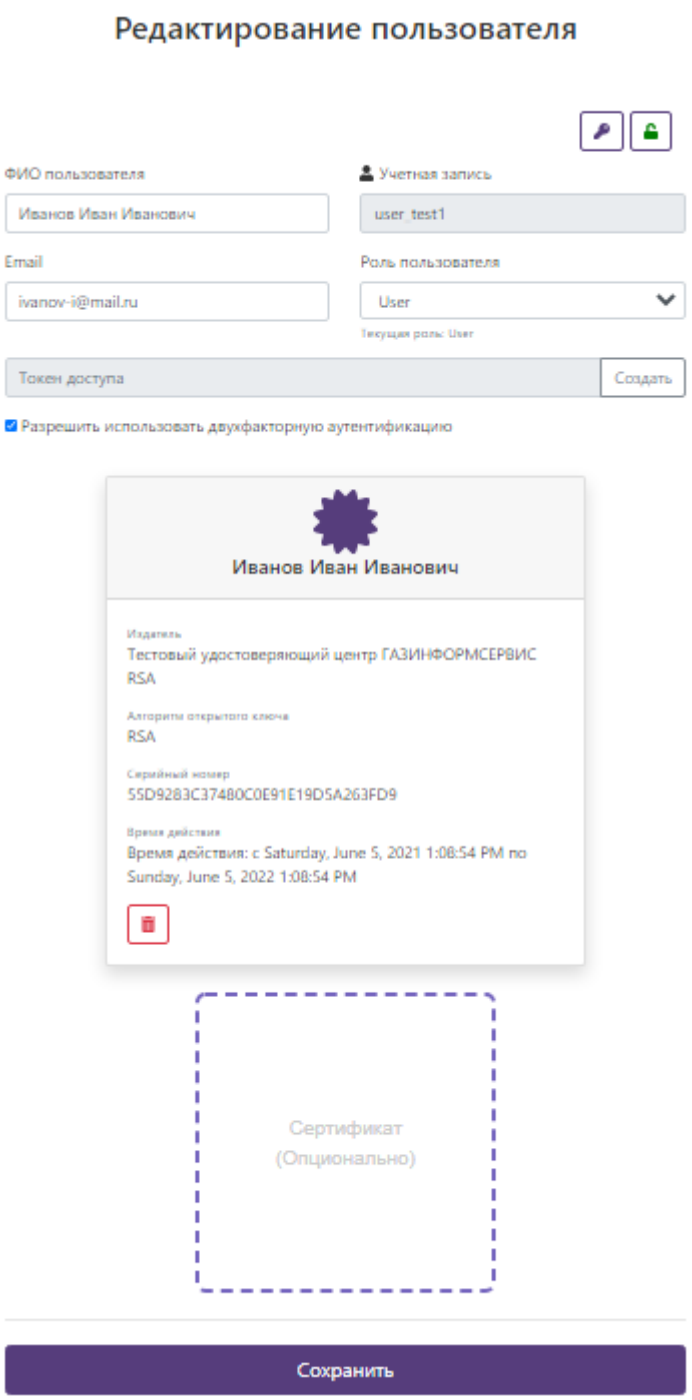

Рисунок 5.10 – Просмотр и редактирование учетной записи

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

5.2.3 Удаление учетной записи

Для удаления учетной записи из списка в пункте меню ***«Пользователи»*** в списке добавленных пользователей (рисунок 5.8) выберите нужную учетную запись и нажмите на кнопку « » .

При удалении учетной записи необходимо учитывать, что восстановление данной учетной записи невозможно! (рисунок 5.11)
Квитанции, созданные удаляемой учетной записью, также будут удалены.

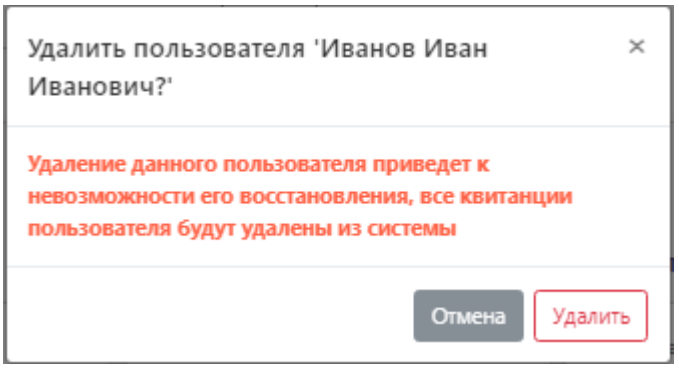

Рисунок 5.11 – Подтверждение удаления учетной записи

Учетную запись встроенного администратора невозможно удалить из web-кабинета.

5.3 Сертификаты

Пункт меню ***«Сертификаты»*** предназначен для добавления сертификатов служб DVCS и TSP, сертификатов-фильтров для определения конечных маршрутов. В том числе, сертификаты службы DVCS:

- для подписи квитанций;
- для подписи запроса при его трансляции на сервер другой службы DVCS;

Перечисленные сертификаты должны быть ранее установлены на рабочую станцию, на которой установлен ПК «Litoria DVCS».

Для добавления сертификата выполните следующие действия:

1. Перейдите в пункт меню ***«Сертификаты»*** и нажмите на кнопку « » (рисунок 5.12).

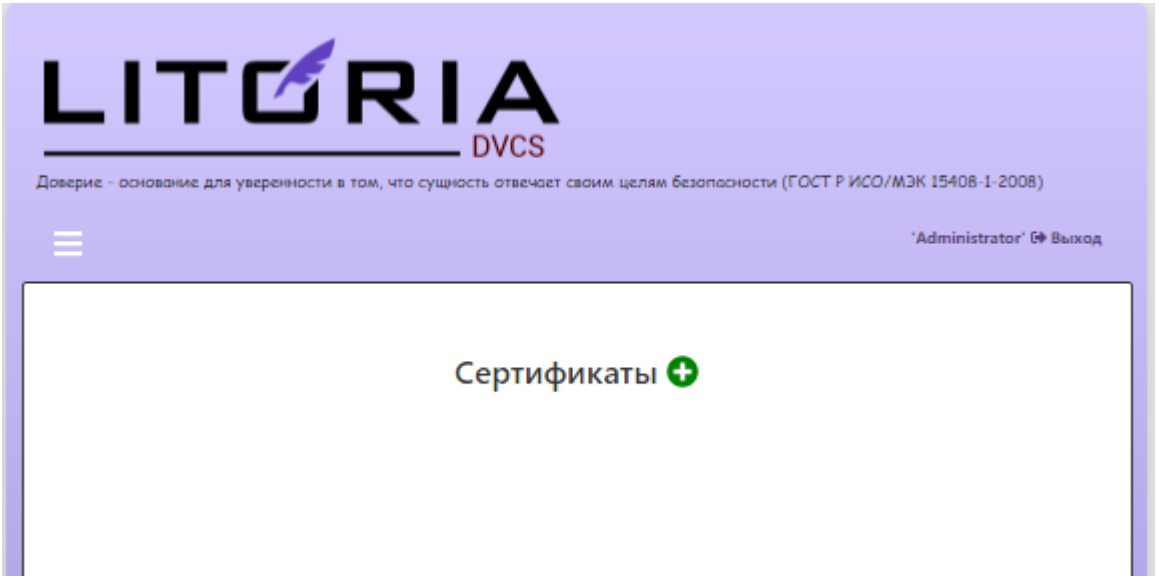

Рисунок 5.12 – Вкладка «Сертификаты»

2. В появившемся окне (рисунок 5.13):

- по щелчку на области ***«Сертификат»*** выберите месторасположение файла добавляемого сертификата службы;
- введите назначение добавляемого сертификата;
- введите пин-код доступа к закрытому ключу сертификата (если сертификат создан без пин-кода, поле допустимо не заполнять).

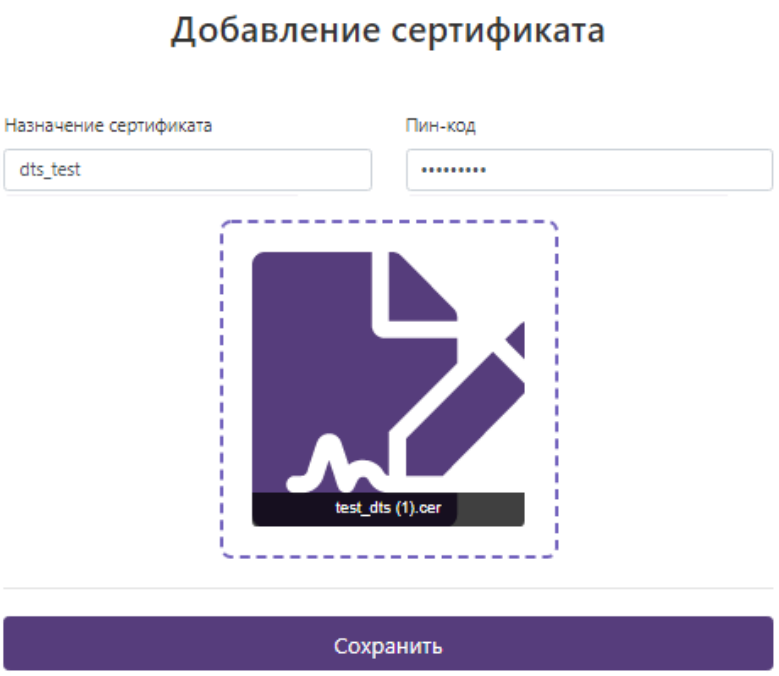

Рисунок 5.13 – Добавление сертификата

3. Нажмите на кнопку «***Сохранить***» для завершения операции добавления сертификата службы.

4. При успешном завершении операции добавления сертификата появится сообщение *«Сертификат <наименование сертификата> успешно добавлен»* и добавленный сертификат отобразится в списке сертификатов (рисунок 5.14).

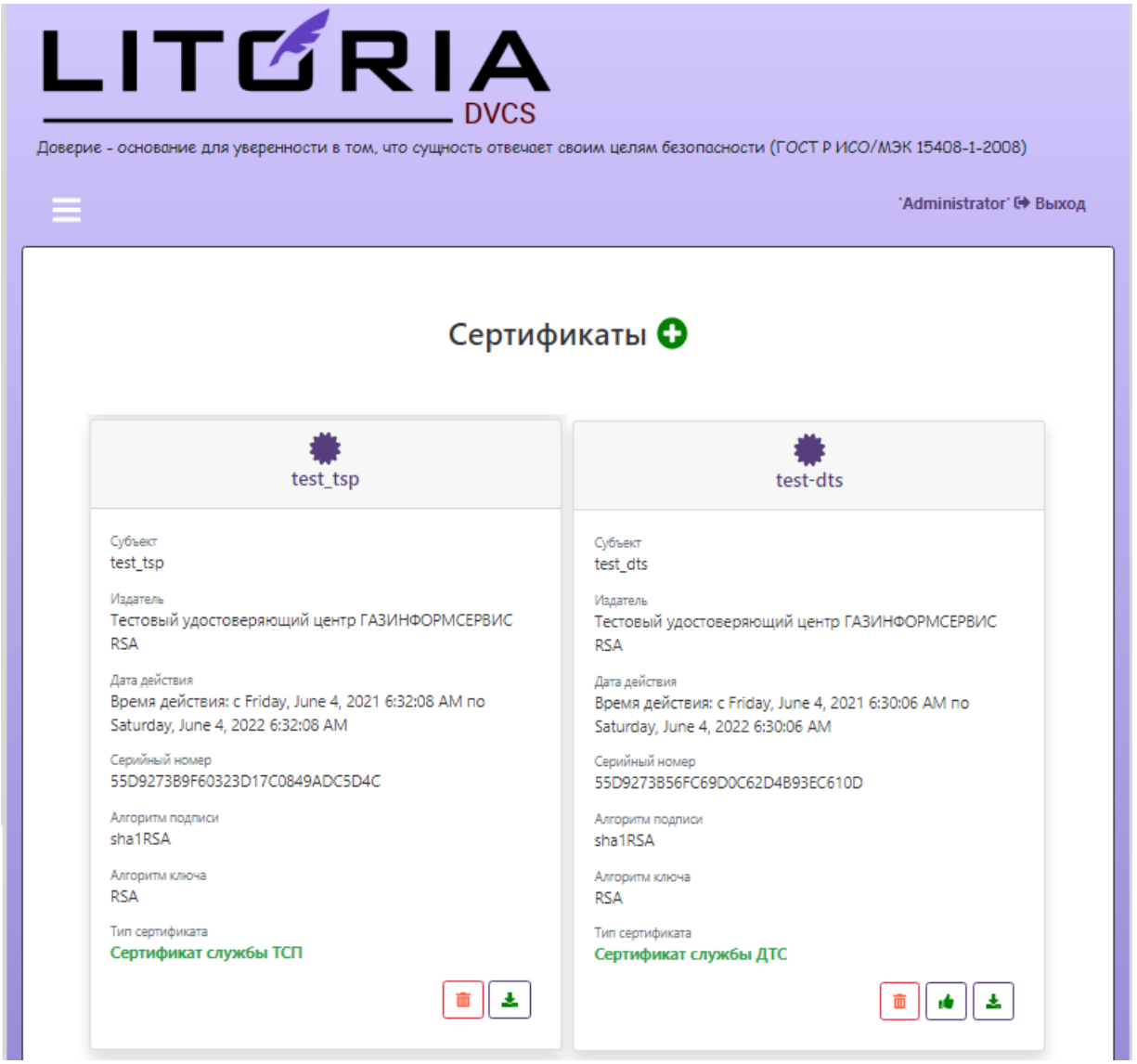

Рисунок 5.14 – Отображение добавленного сертификата

Для удаления сертификата из списка в пункте меню ***«Сертификаты»*** в списке добавленных сертификатов (рисунок 5.14) выберите нужный сертификат и нажмите на кнопку « » , в появившемся окне (рисунок 5.15) подтвердите удаление по кнопке ***«Удалить»***.

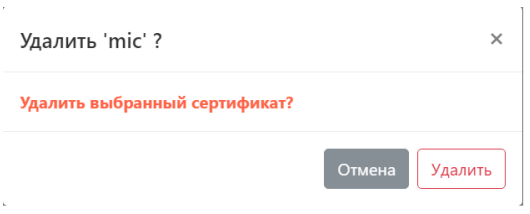

Рисунок 5.15 – Удаление сертификата

По кнопке « » необходимо назначить сертификат для подписи ответов с неопределённым состоянием. Если при проверке запроса служба DVCS не может определить, по какому маршруту следовать для определения сертификата подписи ответа, по умолчанию будет использован выбранный сертификат.

По кнопке « » возможно сохранить на рабочую станцию выбранный сертификат.

5.4 Добавление маршрутов

Маршруты необходимы при выполнении запросов для формирования пути и определения местоположения, где и какой службой DVCS будет выполнена проверка документа.

Маршруты могут быть внешними, определяющими взаимодействие между службами различных независимых систем ДТС, расположенных в других государствах, которые используют разные криптографические алгоритмы.

Внутренние маршруты определяют взаимодействие между службами различных систем ДТС, расположенных в одном регионе, которые используют одинаковый криптографический алгоритм.

Формирование маршрута, по которому будет происходить разбор DVC-запроса (проверка ЭП и выдача квитанции), происходит по алгоритму на рисунке 5.16.

Алгоритм построения маршрутов

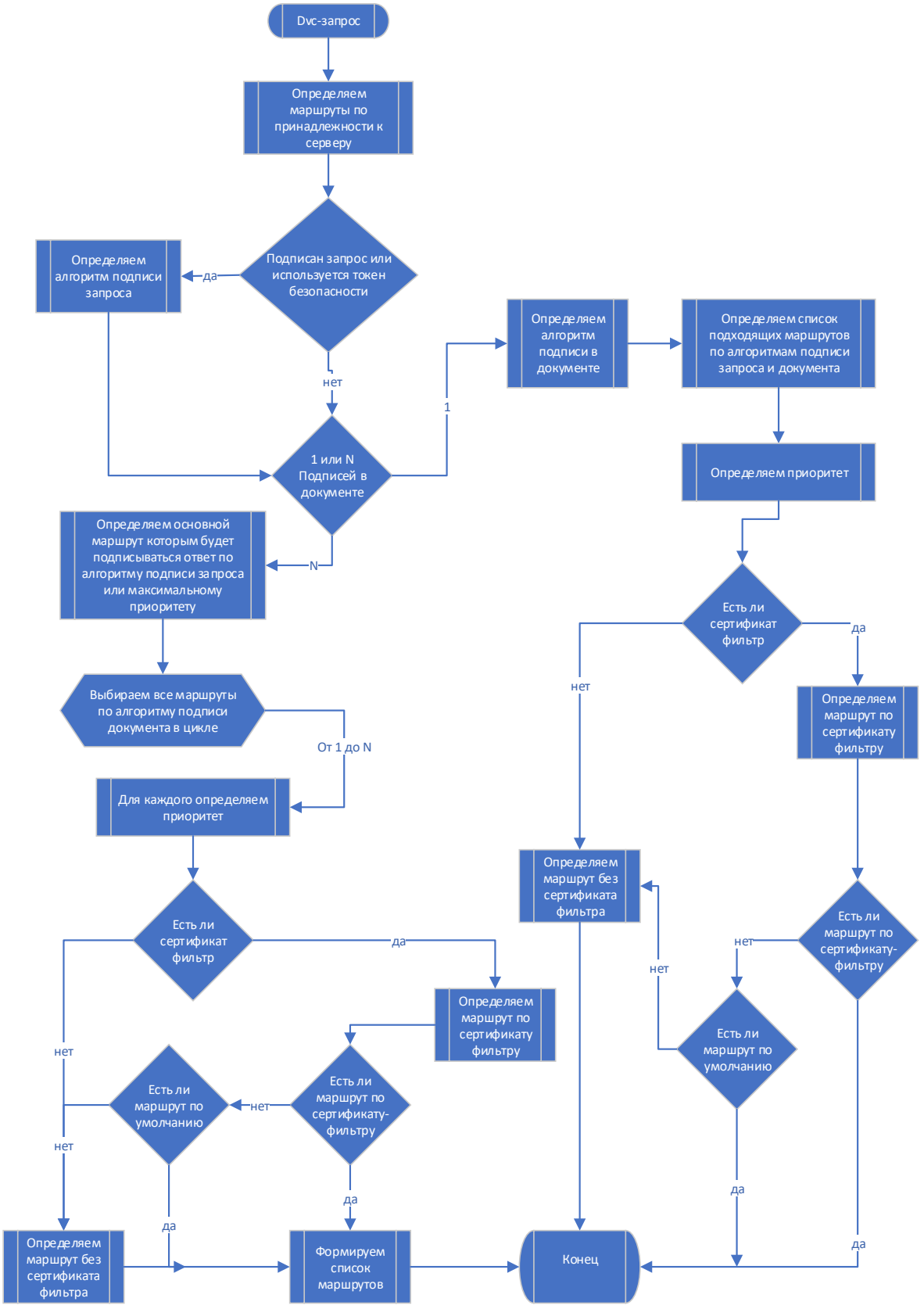

Рисунок 5.16 – Алгоритм построения маршрутов

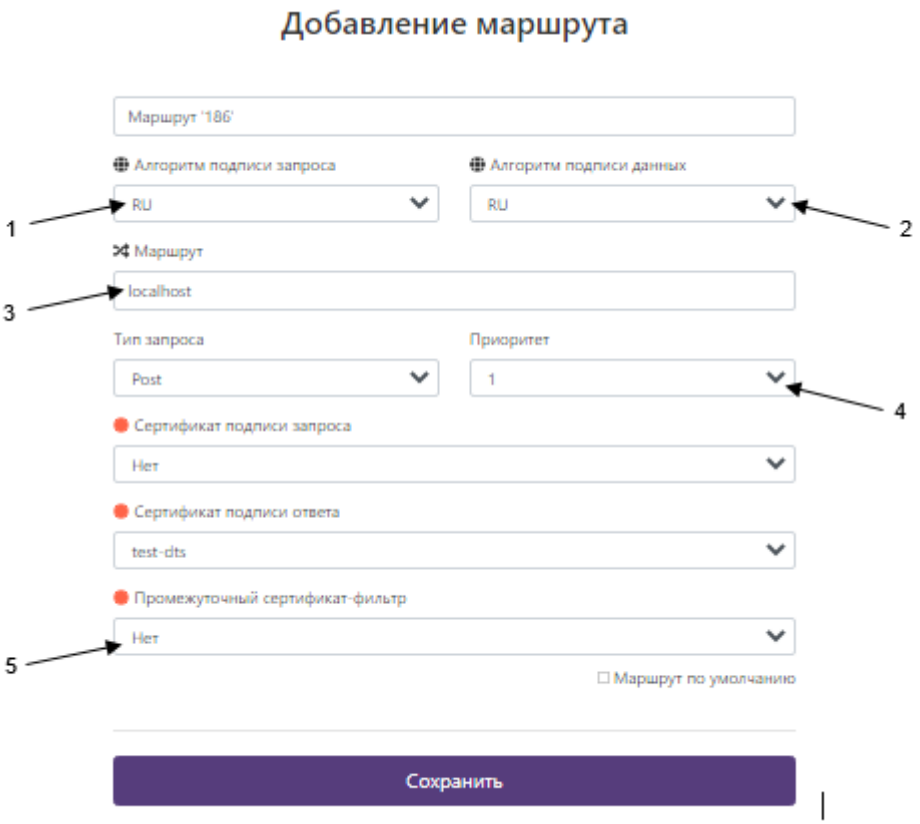

Рисунок 5.17 – Соответствие алгоритма построения маршрутов полям в пункте меню «*Маршруты*»

Соответствие алгоритма построения маршрутов полям в пункте меню «*Маршруты*» (рисунок 5.17):

1. Определяется алгоритм подписи запроса.
2. Определяется алгоритм подписи данных.
3. Определяется список подходящих маршрутов по алгоритмам подписи запроса и документа.
4. Определяется приоритет маршрута.
5. Определяется есть ли у подходящих маршрутов промежуточный сертификат-фильтр.

Управление маршрутами доступно администратору в пункте меню ***«Маршруты»*** после успешного прохождения аутентификации в web-кабинете «ПК «Litoria DVCS».

Для создания нового маршрута выполните следующие действия:

1. Перейдите в пункт меню ***«Маршруты»*** и нажмите на кнопку « » (рисунок 5.18).

Рисунок 5.18 – Вкладка «Маршруты»

2. В появившемся окне (рисунок 5.19) заполните данные о создаваемом маршруте:

- Наименование маршрута (задается по умолчанию, доступно к изменению).
- Алгоритм подписи запроса и алгоритм подписи данных, по которым будут происходить проверки по создаваемому маршруту:
  - «RU» –алгоритмы ГОСТ;
  - «EU» – европейские алгоритмы;
  - «KZ» – алгоритмы Республики Казахстан;
  - «RB» – алгоритмы Республики Беларусь.

Изменить перечень OID алгоритмов, относящихся к определенной группе, или создать новую группу алгоритмов можно в конфигурационном файле *«appsettings.json»* по пути: C:\Program Files (x86)\GIS\Litoria Dvcs\dvcs (см. п. 6 «Настройки конфигурационных файлов»).

- Маршрут – адрес службы DVCS, с которой необходимо настроить взаимодействие (при обращении к собственной службе DVCS, можно оставить значение по умолчанию *localhost,* при этом сервер не будет пытаться отправить запрос по сети);
- Тип запроса – формат передачи данных для удаленного сервера ДТС.
- Приоритет – порядковый номер маршрута в иерархии всех маршрутов, имеющихся в списке (числовое значение из диапазона чисел 1-25 определяет уникальность маршрута, два маршрута с одинаковым приоритетом создать невозможно);

- Сертификат подписи запроса – сертификат службы DVCS, которым подписывается запрос при перенаправлении запроса пользователя другой службе (в случае обращения к собственной службе DVCS (*localhost)* данное поле не заполняется);
- Сертификат подписи ответа – сертификат службы DVCS, которым подписывается ответ, направляемый пользователю;
- Промежуточный сертификат-фильтр – свойство маршрута, которое содержит сертификат издателя в подписанном документе, по которому будет определен конечный маршрут.

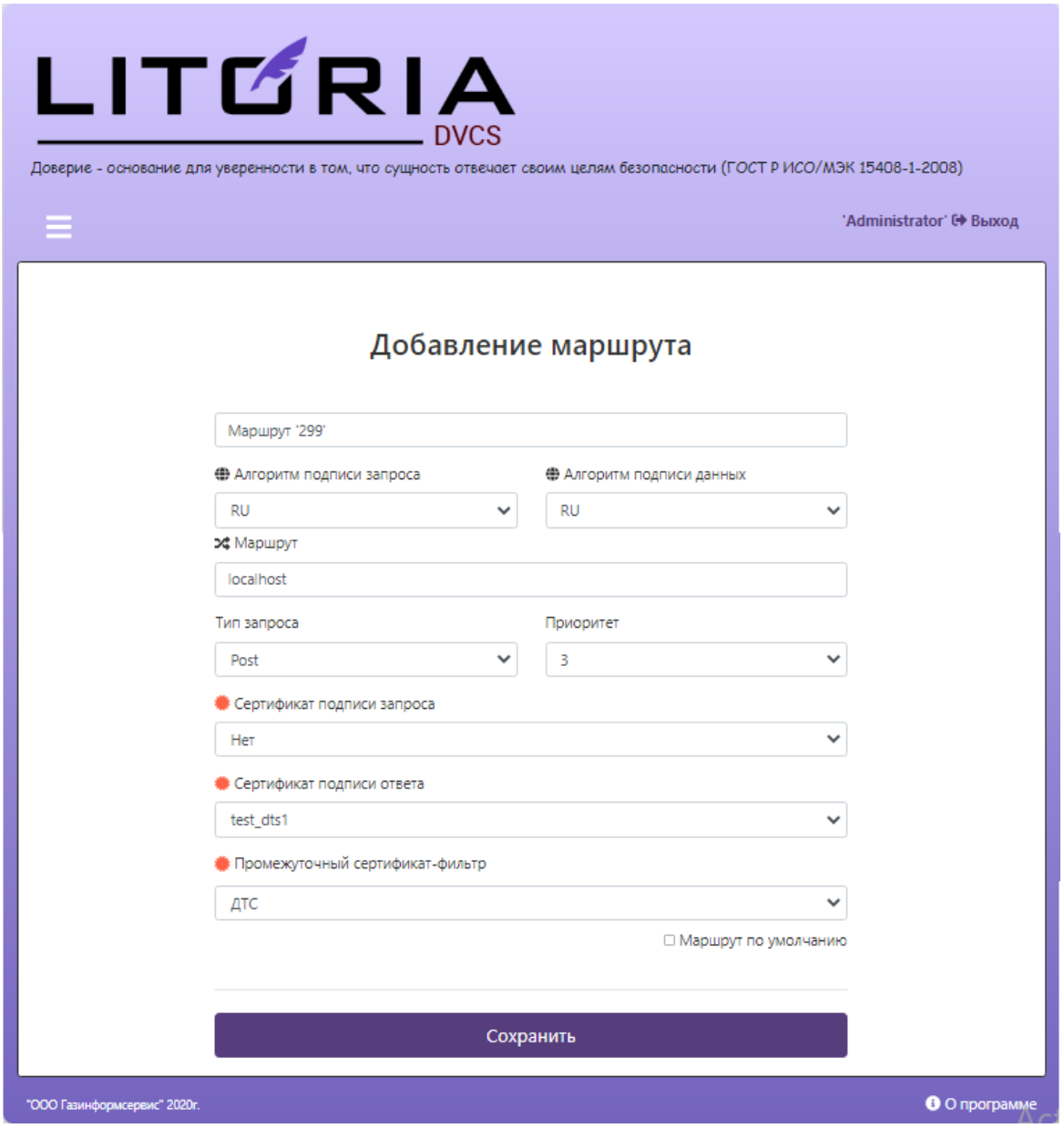

Рисунок 5.19 – Добавление нового маршрута

3. Нажмите на кнопку «***Сохранить***» для завершения операции создания маршрута.
4. При успешном завершении операции создания учетной записи появится

сообщение *«Маршрут <Наименование маршрута> добавлен в систему»* и созданный маршрут отобразится в списке маршрутов (рисунок 5.20).

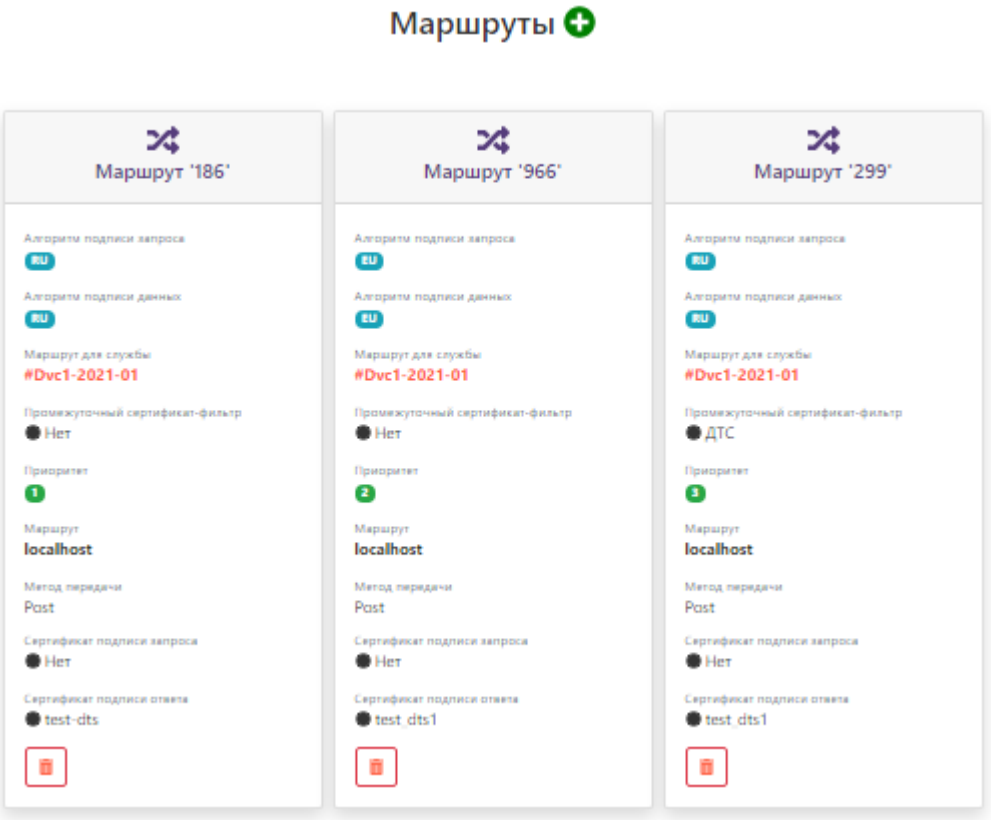

Рисунок 5.20 – Отображение добавленного маршрута в списке маршрутов

Для удаления маршрута из списка в пункте меню ***«Маршруты»*** в списке добавленных маршрутов (рисунок 5.20) выберите нужный маршрут и нажмите на кнопку « 🗑 ».

5.4.1 Настройка маршрутов трансграничности

Маршрутом трансграничности (внешним маршрутом) сервера проверки подлинности является взаимодействие между различными службами доверенной третьей стороны, находящимися как в одном регионе, так и в разных, и использующими как разную криптографию, так и одинаковую (например, служба ДТС, использующая европейскую криптографию и служба ДТС, использующая российскую).

Для пояснения механизма взаимодействия нескольких служб ДТС рассмотрены два случая работы – одностороннее взаимодействие и двухстороннее.

Одностороннее взаимодействие

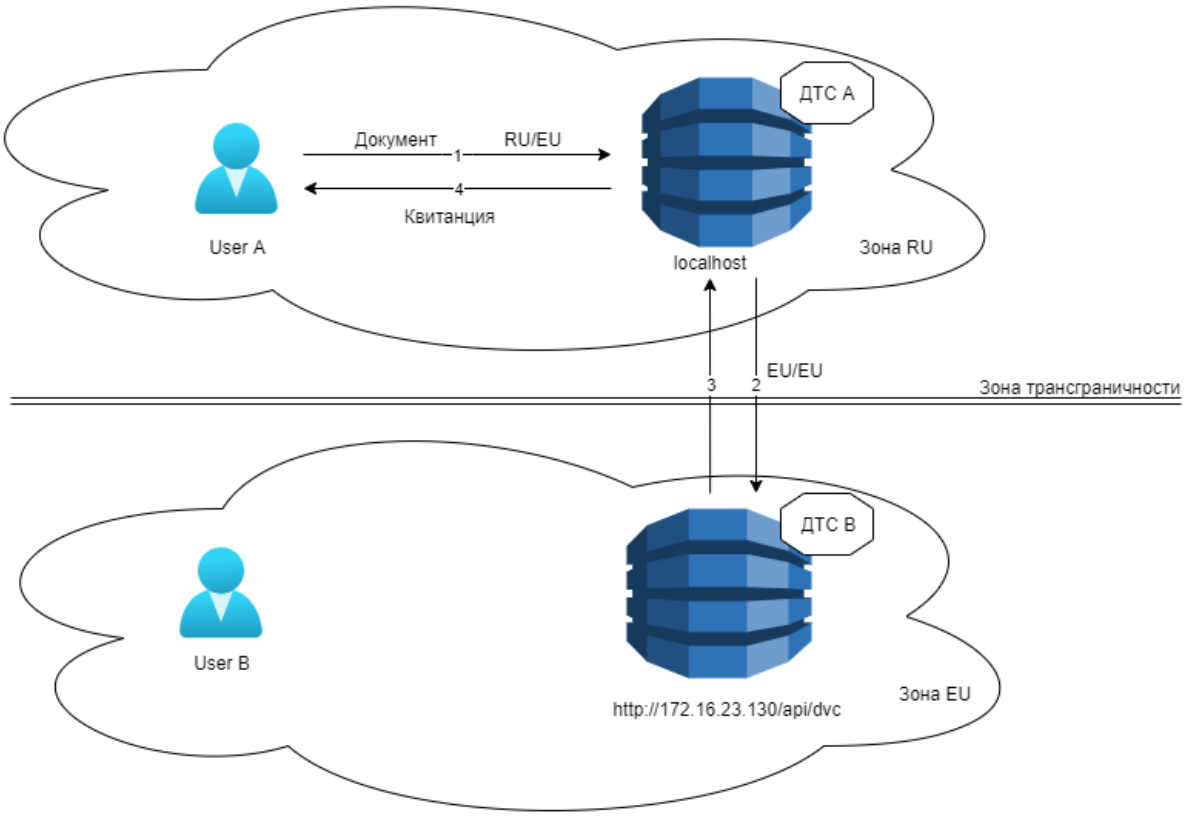

Рисунок 5.21 – Одностороннее взаимодействие двух ДТС

Пример одностороннего взаимодействия (рисунок 5.21): пользователь ***User A*** отправляет службе ***ДТС А*** на проверку документ, содержащий европейскую ЭП (EU), но запрос пользователя подписан на основе ГОСТ-алгоритма (RU).

Настройки службы ***ДТС А*** таковы, что в случае получения такого вида запроса (RU/EU), проверка будет осуществляться службой ***ДТС В*** (пример созданного маршрута см. на рисунке 5.22).

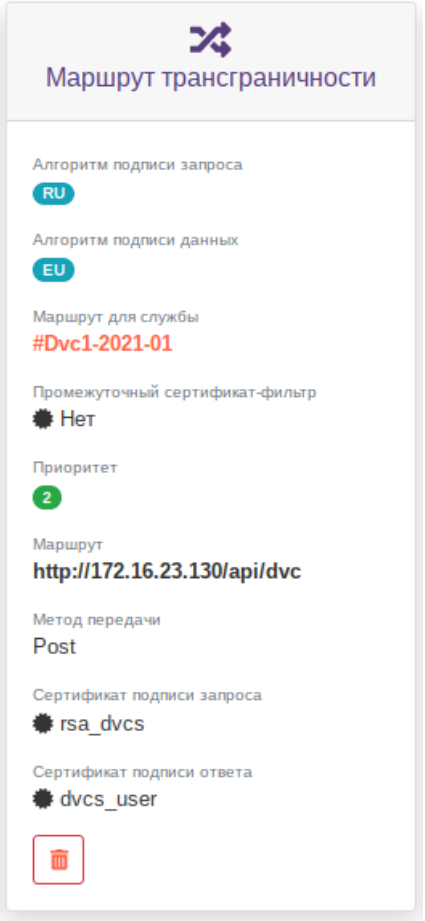

Рисунок 5.22 – Маршрут трансграничности службы ***ДТС А***

Механизм работы следующий:

1. Пользователь ***User A*** отправляет службе ***ДТС А*** запрос, подписанный при помощи национальной криптографии (RU), а внутри имеющий европейскую ЭП (EU).

2. Обработав запрос от пользователя и найдя подходящий маршрут, служба ***ДТС А*** подписывает запрос для отправки службе ***ДТС В*** (сертификат подписи запроса **rsa_dvcs**) и передаёт его, используя указанный в маршруте метод передачи. Адрес службы ДТС возможно узнать в разделе **5.6 «Дашборд»**.

> Для взаимодействия различных служб ДТС в зоне трансграничности рекомендуется использовать общие криптографические алгоритмы, например, RSA на обеих службах ДТС.

3. Служба ***ДТС В*** получает входящий запрос от службы ***ДТС А***, подписанный с использованием европейской криптографии (EU), внутри содержащий также европейскую ЭП (EU/EU), обрабатывает его, согласно имеющемуся у него маршруту (рисунок 5.23), подписывает ответ (сертификат подписи ответа **dvcs**) и отправляет на сторону службы ***ДТС А.***

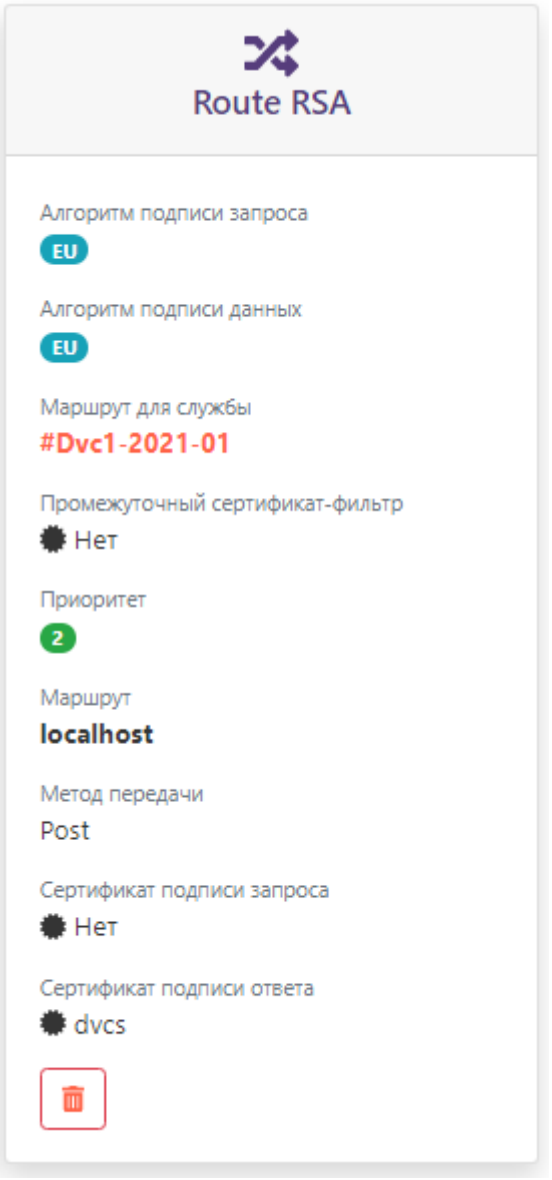

Рисунок 5.23 – Маршрут трансграничности на ***ДТС В***

Для проведения аутентификации и установления доверия между службами ДТС необходимо, чтобы на стороне ***ДТС В*** был создан пользователь с привязанным к нему сертификатом подписи запроса от ***ДТС А*** (в примере **rsa_dvcs**), и в хранилищах промежуточных сертификатов обеих служб ДТС были установлены промежуточные сертификаты из цепочки подписи отвечающей стороны.

4. Служба ***ДТС А***, получив ответ от службы ***ДТС В,*** снимает его подпись и подписывает с помощью своей ЭП (сертификат **dvcs_user**), затем отправляет пользователю ***User A*** квитанцию, подписанную на указанном в маршруте сертификате.

Двухстороннее взаимодействие

Двустороннее взаимодействие означает, что обработка запросов от служб ДТС происходит в обе стороны (рисунок 5.24).

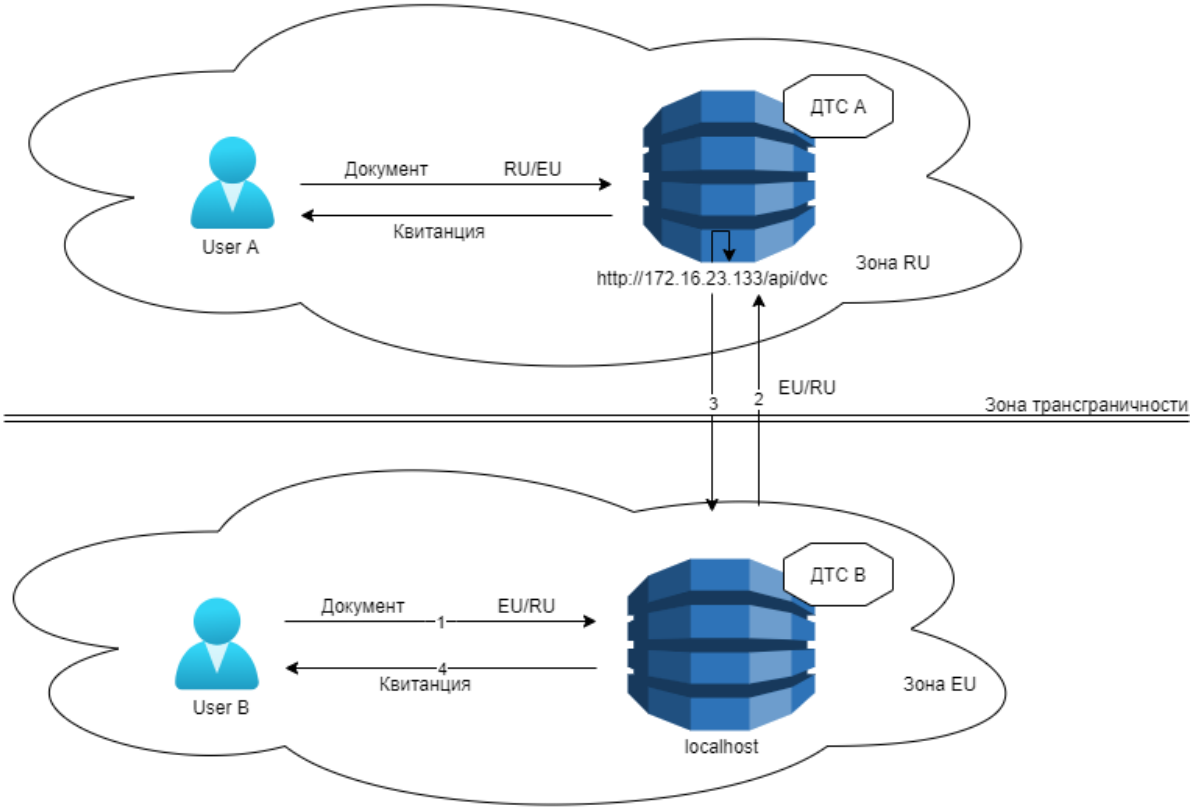

Рисунок 5.24 – Двухстороннее взаимодействие служб ДТС

Пример двустороннего взаимодействия: пользователь ***User B*** отправляет службе ***ДТС В*** на проверку документ, содержащий отечественную ЭП (RU), но запрос для обращения подписан с использованием европейской криптографии (EU). Настройки службы ***ДТС В*** таковы, что в случае получения такого вида запроса (EU/RU), проверка будет осуществляться службой ***ДТС А*** (пример маршрута см. на рисунке 5.25):

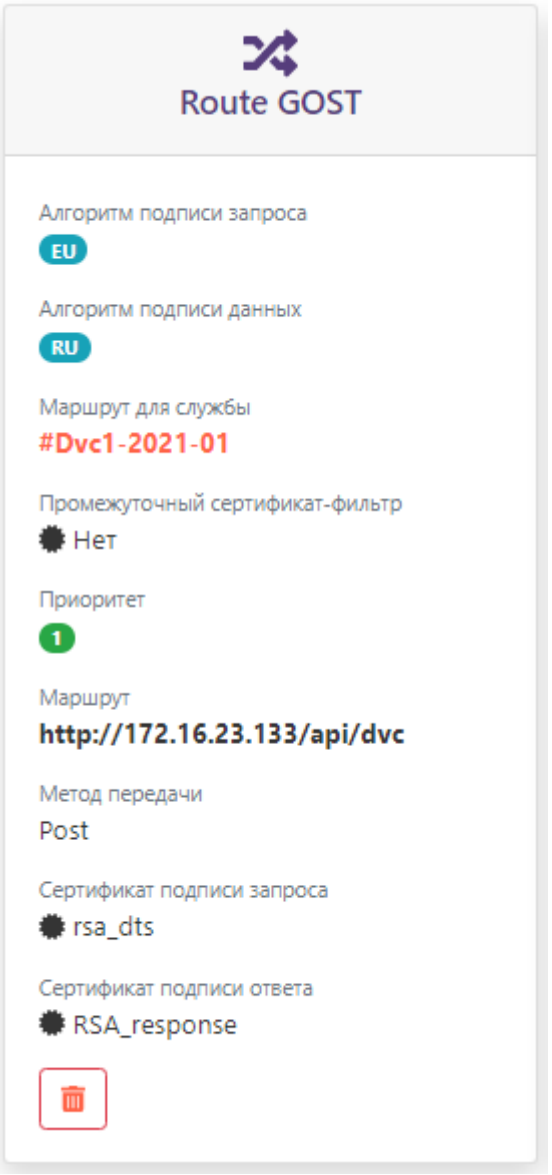

Рисунок 5.25 – Пример маршрута службы ***ДТС В*** для взаимодействия со службой ***ДТС А***

Механизм взаимодействия при указанных условиях будет следующий:

1. ***User B*** отправляет службе ***ДТС В*** запрос, подписанный с использованием европейской криптографии (EU), а внутри имеющий ЭП на основе ГОСТ-алгоритмов (RU).

2. Обработав запрос от пользователя и найдя подходящий маршрут, служба ***ДТС В*** подписывает запрос для отправки с использованием сертификата подписи запроса (в примере **rsa_dts**) и передаёт службе ***ДТС А***, используя указанный в маршруте метод передачи. Адрес службы ДТС возможно узнать в разделе **5.6 «Дашборд»**.

3. ***ДТС А*** получает входящий запрос от ***ДТС В***, подписанный с использованием европейской криптографии (EU), внутри содержащий ЭП на основе алгоритмов ГОСТ (RU), обрабатывает его согласно имеющемуся у него маршруту (рисунок 5.26, маршрут

трансграничности RSA), и отправляет подписанный ответ (сертификат **rsa_dvcs**) на сторону службы ***ДТС В***.

4. Служба ***ДТС В***, получив ответ от службы ***ДТС А***, снимает его подпись и подписывает с использованием сертификата ответа (**RSA_response**), согласно маршруту (рисунок 5.25), в завершении отправляет пользователю подписанную квитанцию.

В случае двухстороннего взаимодействия, описанного в примере, маршруты для обеих служб ДТС должны быть созданы как показано на рисунках 5.26 и 5.27.

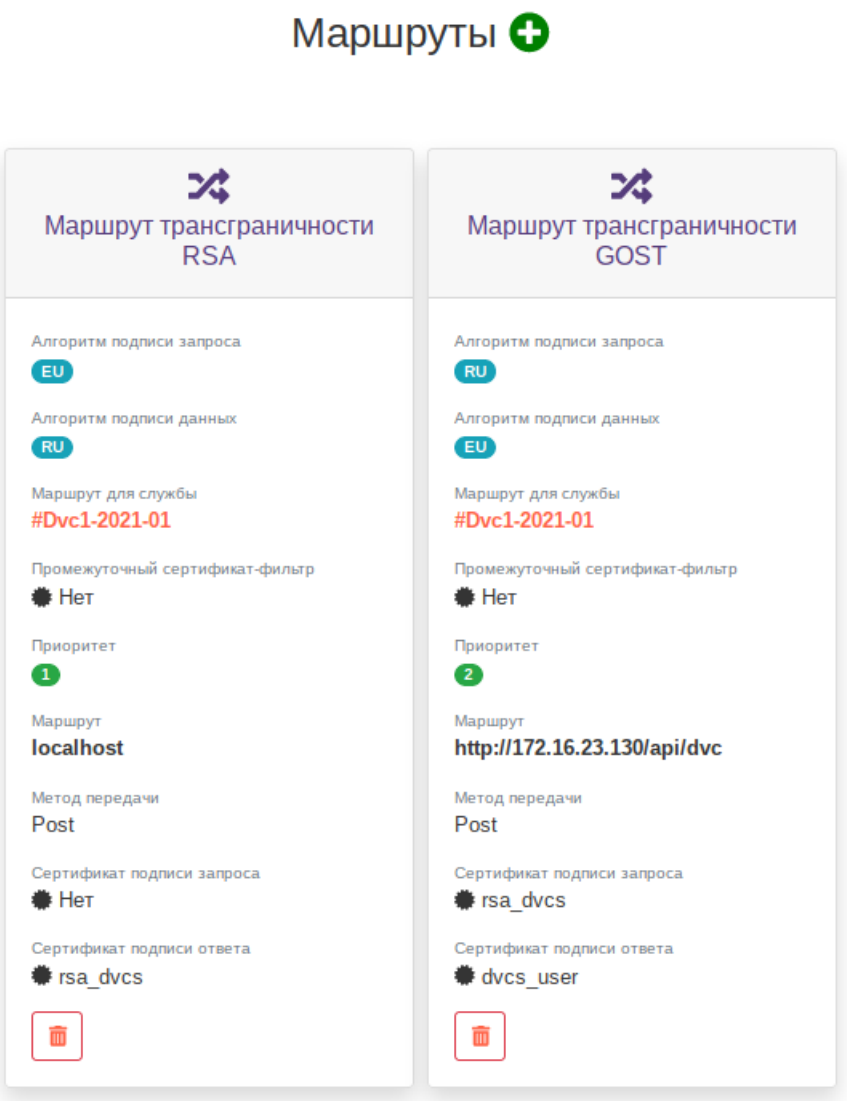

Рисунок 5.26 - Маршруты службы ***ДТС А*** при двустороннем взаимодействии

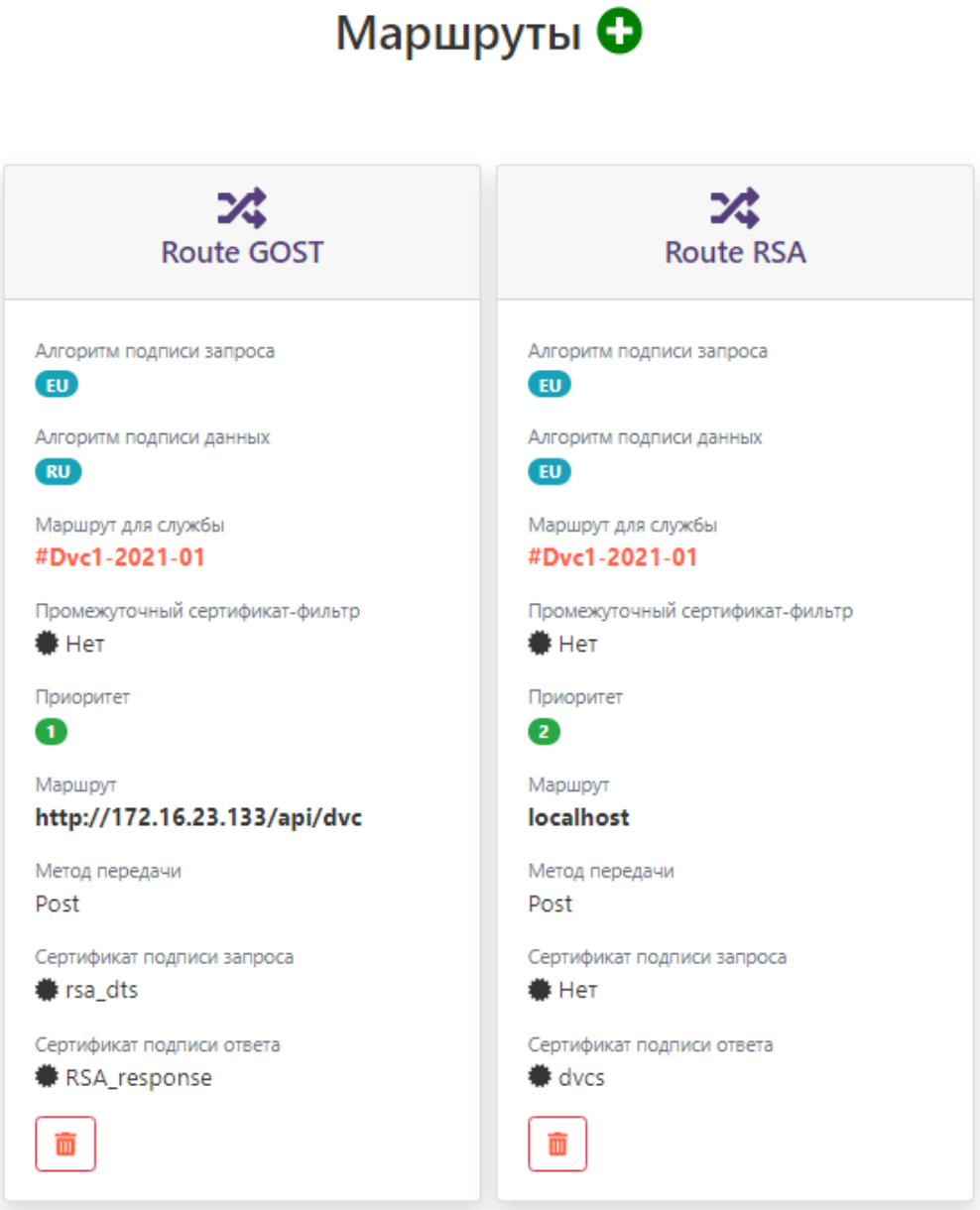

Рисунок 5.27 - Маршруты службы ***ДТС В*** при двустороннем взаимодействии

5.5 Штамп времени

Пункт меню ***«Штамп времени»*** предназначен для добавления адреса службы TSP по которому служба DVCS обращается к сервису TSP для получения штампа времени на квитанциях, создаваемых при проверке документа.

> Сертификат службы TSP должен быть ранее добавлен в список сертификатов во вкладке ***«Сертификаты»*** web-кабинета «ПК «Litoria DVCS».

Для добавления штампа времени выполните следующие действия:

1. Перейдите в пункт меню ***«Штамп времени»*** и нажмите на кнопку « » (рисунок

5.28).

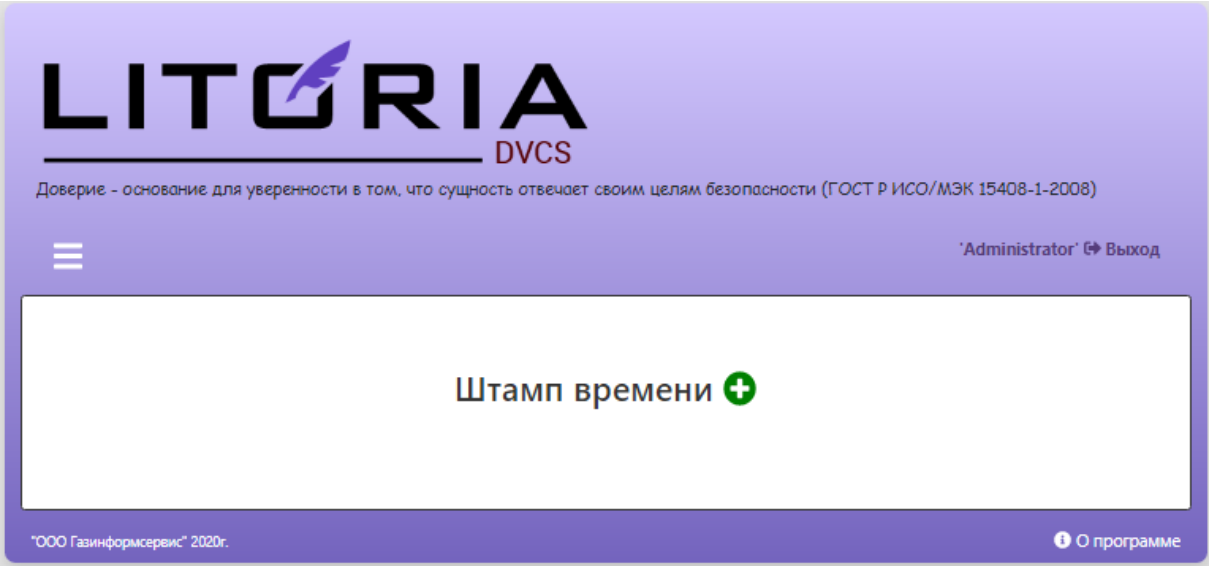

Рисунок 5.28 – Вкладка «Штамп времени»

2. В появившемся окне (рисунок 5.29):

- выберите сертификат подписи ответа штампа времени из списка добавленных сертификатов;
- при необходимости измените назначение добавляемого штампа времени и заголовок маршрута (введенный заголовок в дальнейшем будет использован в адресе службы штампов времени).

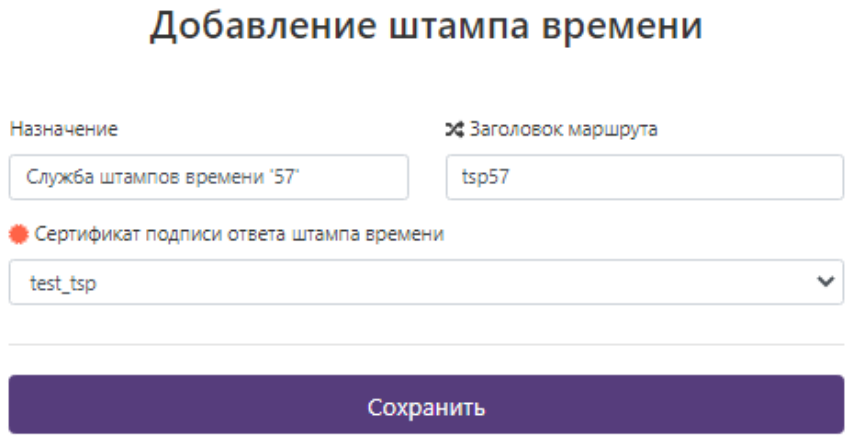

Рисунок 5.29 – Добавление штампа времени

Добавление штампа времени с одинаковым маршрутом недопустимо! Если при добавлении штампа времени используется маршрут, который уже имеется в заведенном ранее штампе времени, появится ошибка вида « Служба штампов времени с заданным маршрутом уже добавлена » и штамп добавлен не будет.

3. Нажмите на кнопку «***Сохранить***» для завершения операции добавления штампа

времени.

4. При успешном завершении операции добавления штампа времени появится сообщение *«Штамп времени <наименование службы штампа времени> добавлен в систему»* и добавленный штамп отобразится в списке штампов времени (рисунок 5.30).

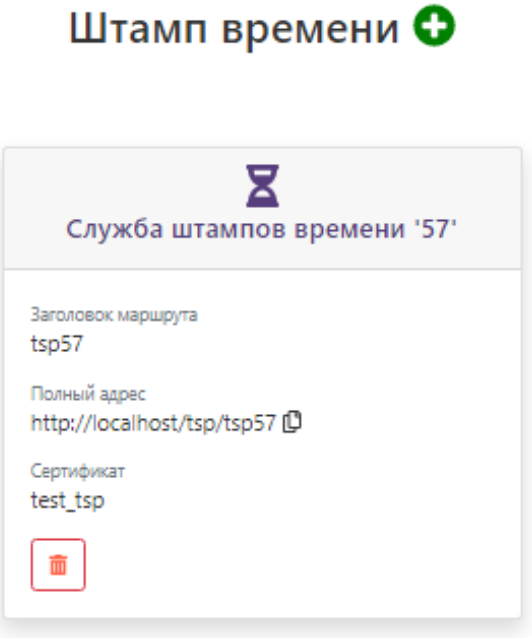

Рисунок 5.30 – Отображение добавленного штампа времени

Для удаления службы штампов времени из списка в пункте меню ***«Штамп времени»*** в списке добавленных штампов времени (рисунок 5.30) выберите нужный штамп и нажмите на кнопку « » .

По кнопке « » расположенной в строке с адресом службы штампов времени можно скопировать адрес службы в буфер обмена.

5.6 Дашборд

Пункт меню ***«Дашборд»*** (рисунок 5.31) предназначен для отображения всех настроек ПК «Litoria DVCS», используемых в работе служб DVCS и TSP, в том числе адреса службы DVCS.

Изменение настроек доступно в одноименных конфигурационных файлах ***«appsettings.json»***, расположенных в директории установки ПК «Litoria DVCS» по пути: *C:\Program Files (x86)\GIS\Litoria Dvcs\dvcs* и *C:\Program Files (x86)\GIS\Litoria Dvcs\updater* (см. п. **7 «Настройки конфигурационных файлов»**).

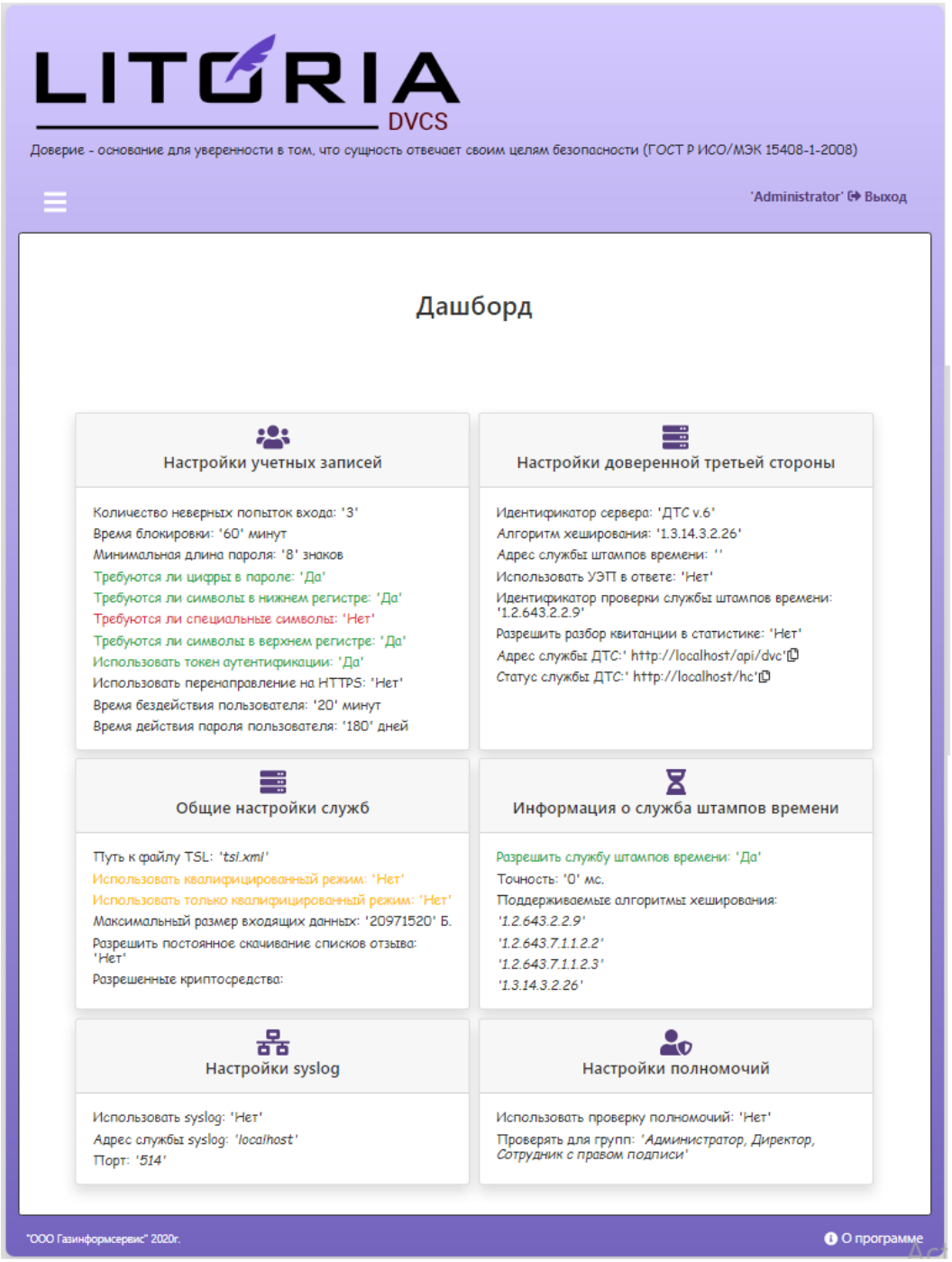

Рисунок 5.31 – Вкладка «Дашборд»

5.7 Системный журнал

В пункте меню ***«Журнал»*** фиксируются и отображаются все операции, выполненные в ПК «Litoria DVCS» (рисунок 5.32).

Журнал предназначен для фиксации, хранения и отображения информации о значимых событиях, которые меняют состояние настроек комплекса, а также о событиях, связанных с использованием функций, предоставляемых службами ПК «Litoria DVCS».

События комплекса, фиксируемые в журнале событий:

- Создание/удаление пользователей и администраторов.
- Вход/выход администраторов и пользователей в web-кабинет.
- Попытка входа с неверным паролем администратора/пользователя.
- Обновление настроек учетных записей администратора/пользователя.
- Изменение настроек служб DVCS и TSP.
- Факт получения запроса на проверку от пользователя или другой службы DVCS.
- Проверка документов с выдачей квитанций.
- Информация об ошибках, возникающий в процессе работы службы DVCS.
- Результат проверки работы службы DVCS и штампов времени, службы продления ЭП квитанций и скачивания трастед листа.

События, фиксируемые в журнале, возможно отфильтровать по типу события и/или по источнику события путем установки флага напротив нужного типа в соответствующих областях ***«Тип события»/«Источник события»*** (рисунок 5.32).

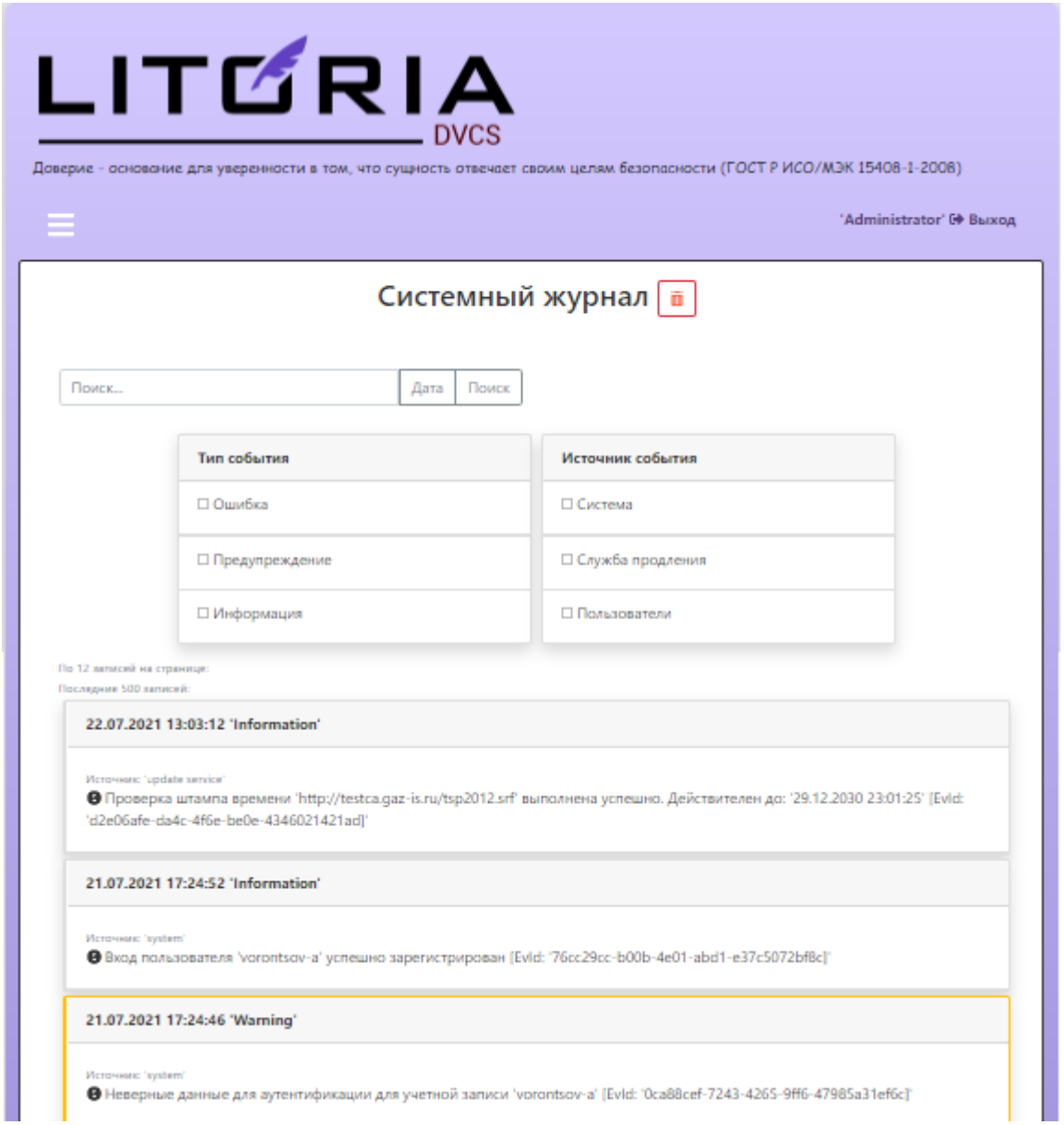

Рисунок 5.32 – Вкладка «Системный журнал»

В зависимости от типа события, сообщение в системном журнале выделяется цветом:

- – сообщение об ошибке;
- – сообщение – предупреждение;
- нет индикации – информативное сообщение.

При необходимости можно отфильтровать сообщения системного журнала по дате (по кнопке ***«Дата»***) или выполнить поиск по тексту сообщения, вводом необходимых для поиска символов в строку поиска.

Запись сообщений в системный журнал включена по умолчанию. Изменение данной настройки доступно в конфигурационном файле «*appsettings.json*» (см. п. **7 «Настройки конфигурационных файлов»**).

5.8 Проверка документа

Основное назначение ПК «Litoria DVCS» возможность проверки электронных документов, полученных от участника электронного взаимодействия.

Служба DVCS предоставляет следующие услуги проверки данных в запросе, полученном службой от пользователя:

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

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

5.8.1 Проверка документа

Для выполнения операции проверки документа:

1. Перейдите в пункт меню ***«Проверить»***, во вкладку ***«Проверить документ»*** и поместите документ, который необходимо проверить в область ***«Подписанный документ»*** (рисунок 5.33). Данную операцию можно выполнить несколькими способами:

- нажатием на ссылку ***«Подписанный документ»*** и выбором необходимого файла в открывшемся окне;
- перетаскиванием файла из окна Проводника в область ***«Подписанный документ»***.

Рисунок 5.33 – Проверка документа

2. При проверке отделенной подписи, выберите исходные данные для отделенной подписи в области «***Данные для отделенной подписи***».

При проверке конфиденциального документа, чтобы конфиденциальные данные не выходили за пределы рабочей станции пользователя, создайте запрос на проверку не самого файла, а его хеш-значения. При этом должен быть настроен параметр «*IsUseHash*» в конфигурационном файле *appsettings.json*. После его настройки, тип запроса будет определяться автоматически в зависимости от типа документа.

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

4. При успешном завершении проверки документа на экране отобразится ответная квитанция службы DVCS, содержащая информацию в проведенных проверках (рисунок 5.34).

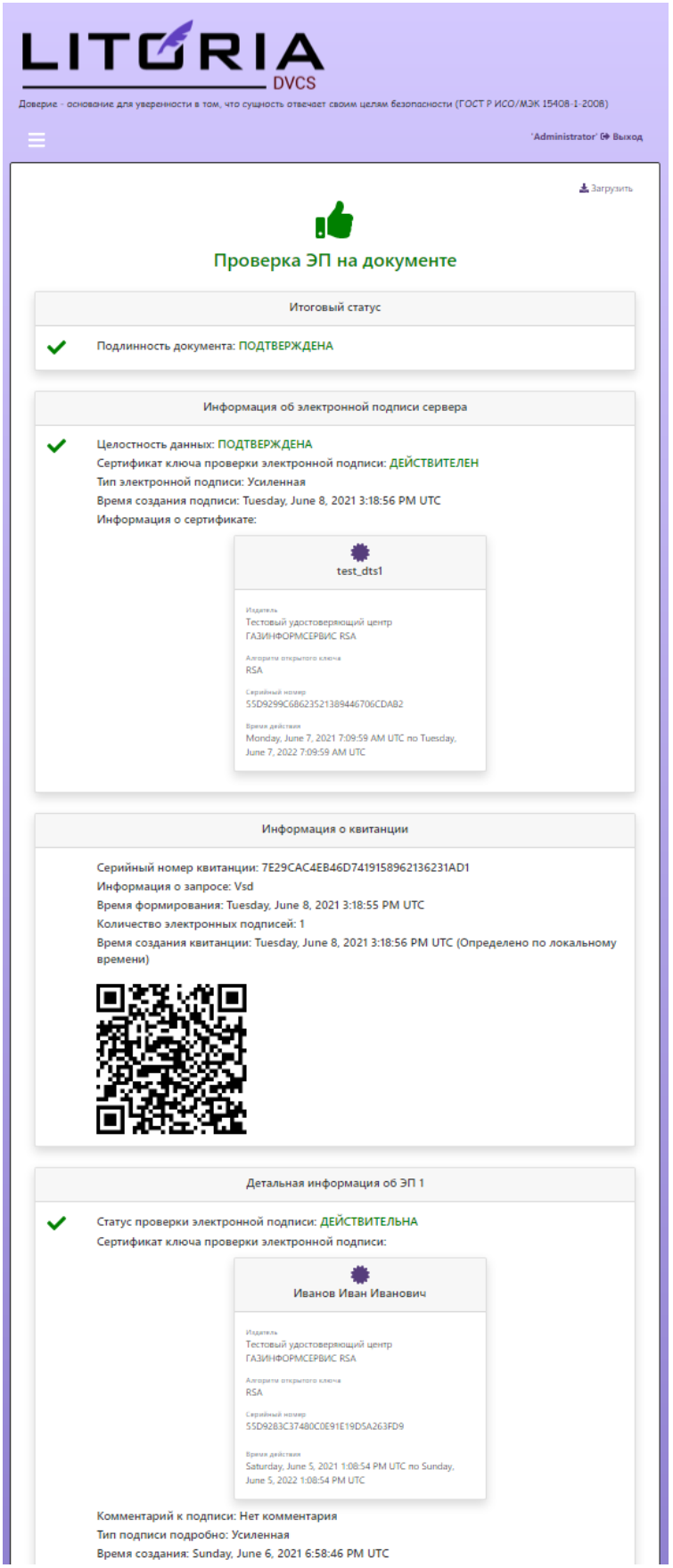

Рисунок 5.34 – Квитанция по отправленному запросу на проверку

Для загрузки квитанции нажмите на кнопку «Загрузить» (рисунок 5.34).

5.8.2 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 5.35).

Рисунок 5.35 – Просмотр квитанции

2. Нажмите на кнопку «***Разобрать***» для просмотра загруженной квитанции.

3. На экране отобразится содержание загруженной квитанции службы DVCS (рисунок 5.34).

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

5.8.3 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 5.36).

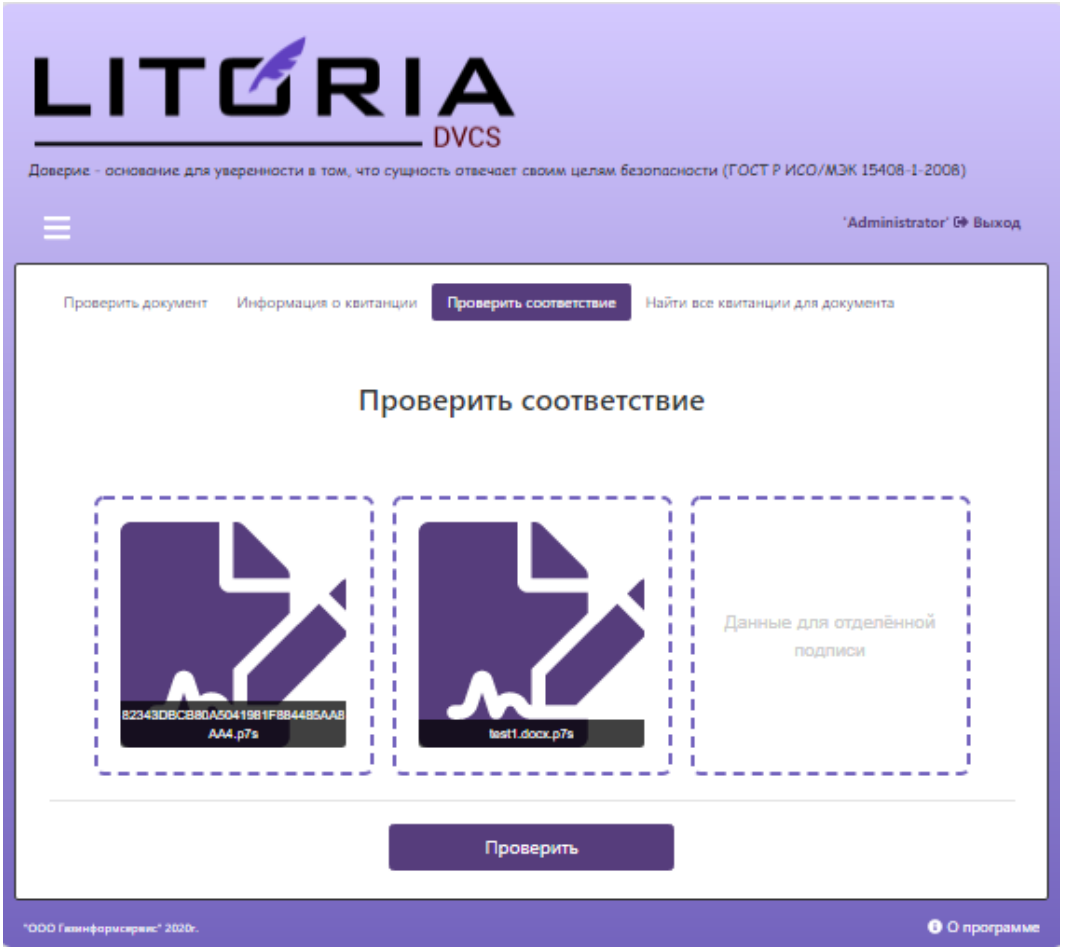

Рисунок 5.36 – Проверка соответствия квитанции и подписанного документа

2. При проверке отделенной подписи, добавьте исходные данные для отделенной подписи в область «***Данные для отделенной подпис***и».

3. Нажмите на кнопку «***Проверить***» для выполнения операции соответствия.

4. На экране отобразится информация о соответствии проверяемого документа добавленной квитанции (рисунок 5.37).

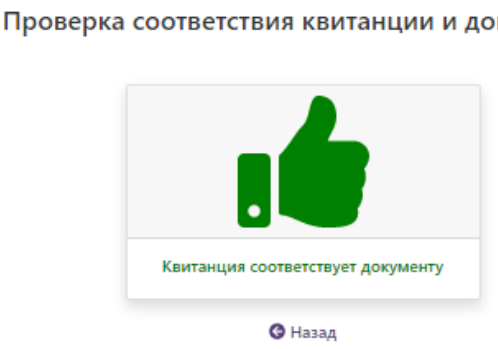

Рисунок 5.37 – Квитанция соответствует загруженному документу

5.8.4 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 5.38).

2. Если необходимо осуществить поиск для файла отделенной подписи, то также укажите исходные данные отделенной подписи в области ***«Данные для отделенной подписи»***.

Рисунок 5.38 – Поиск квитанций подписанного документа

3. Нажмите на кнопку «***Найти***» для выполнения поиска.

4. На экране отобразится список всех квитанций проверяемого документа (рисунок 5.39). Операции, доступные в журнале «***Архив***» описаны в п.5.9.

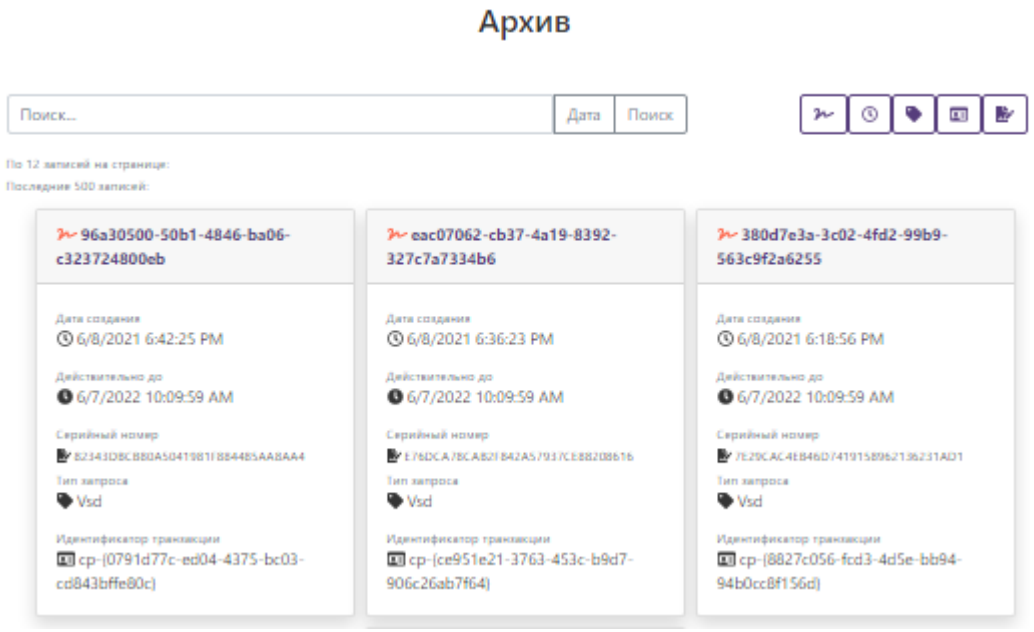

Рисунок 5.39 – Отображение квитанций искомого документа

Для просмотра квитанции необходимо в строке с нужной квитанцией нажать на ссылку с номером квитанции (рисунок 5.39).

5.9 Архив

В пункте меню ***«Архив»*** отображаются все квитанции, полученные при создании DVCS-запросов с использованием web-кабинета и другого программного обеспечения (рисунок 5.40).

Рисунок 5.40 – Архив квитанций ПК «Litoria DVCS»

В списке квитанций архива отображается следующая информация по квитанции:

- уникальный номер квитанции,
- серийный номер квитанции,
- идентификатор транзакции,
- дату 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 «»)

При необходимости можно выполнить поиск квитанции в архиве за выбранный период

времени (по кнопке ***«Дата»***) для конкретной учетной записи пользователя или для всех (рисунок 5.41).

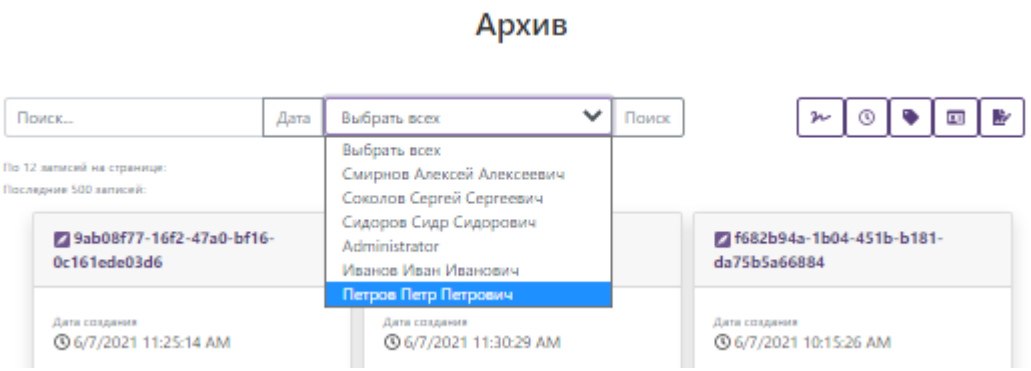

Рисунок 5.41 – Поиск квитанций пользователя

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 5.42).

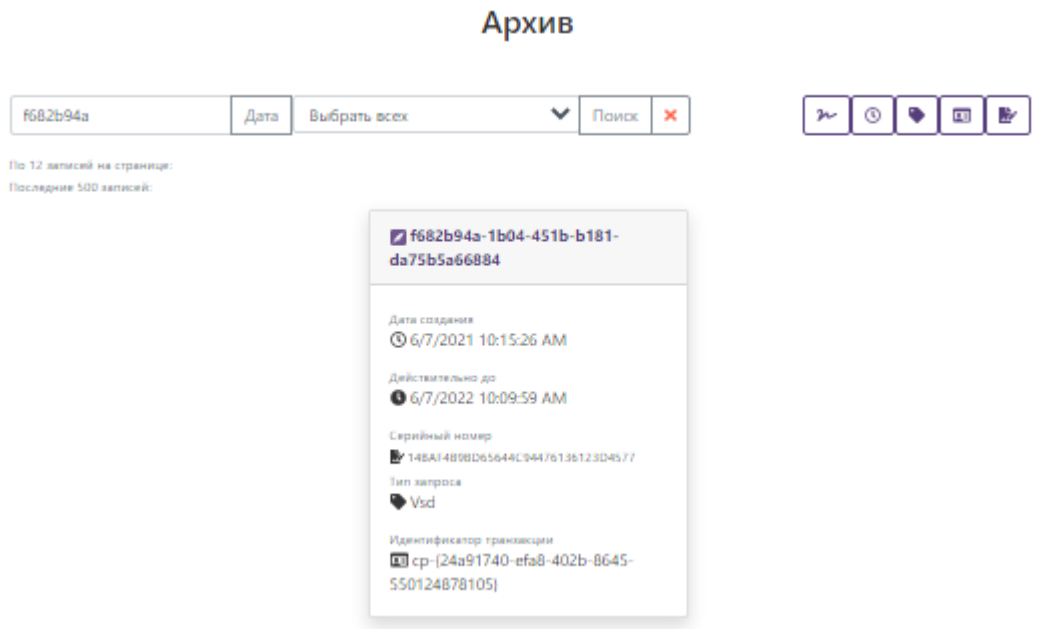

Рисунок 5.42 – Поиск квитанции по идентификатору квитанции

Для просмотра квитанции необходимо в строке с нужной квитанцией нажать на ссылку с номером квитанции (рисунок 5.43).

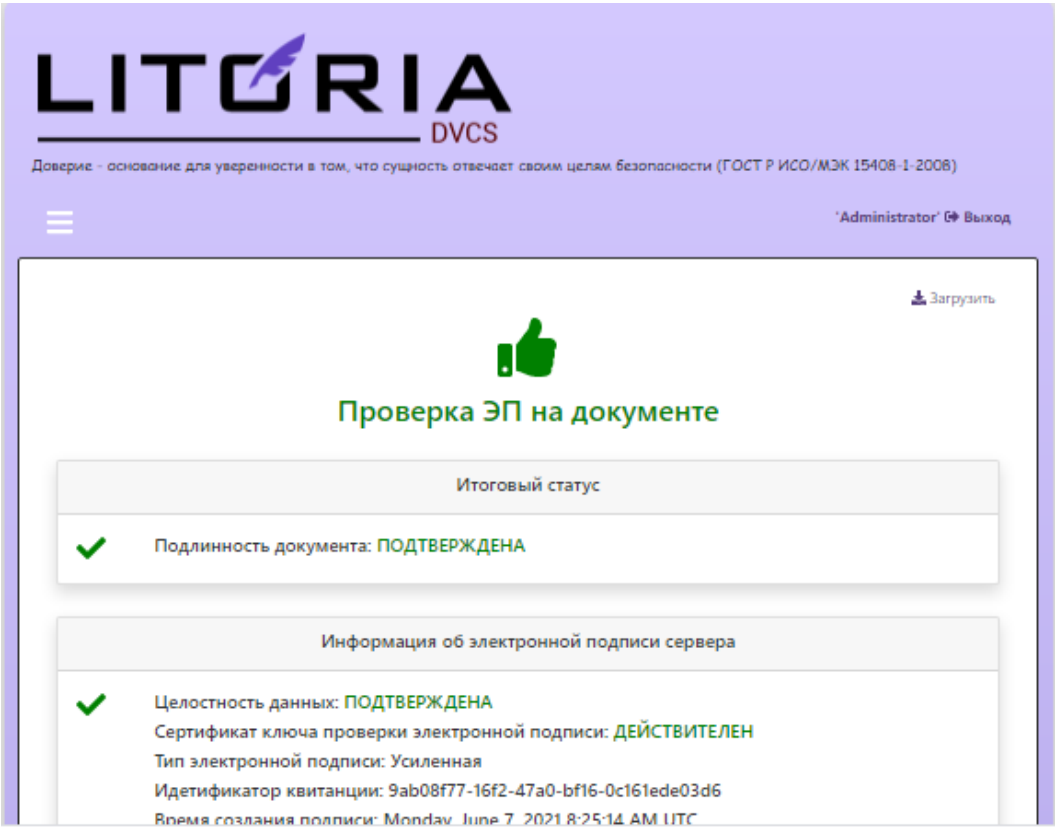

Рисунок 5.43 – Просмотр квитанции

Для загрузки квитанции на рабочую станцию откройте выбранную квитанцию на просмотр и нажмите на кнопку « Загрузить » (рисунок 5.43).

5.10 Статистика

В пункте меню ***«Статистика»*** отображаются сводные данные по квитанциям, полученным при создании DVCS-запросов с использованием web-кабинета и другого программного обеспечения (рисунок 5.44).

Данные в пункте меню ***«Статистика»*** отображаются в виде диаграмм по типу запроса и маршрутизации квитанций (рисунок 5.44) или более детально в виде перечня запросов по каждому пользователю (рисунок 5.45). 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 формирования сводных данных по квитанциям определенного пользователя, выберите его учетную запись в соответствующем поле.

Для загрузки всех квитанции за выбранный период нажмите на кнопку « Получить все квитанции за выбранный период » (рисунок 5.44). При загрузке квитанции на рабочую станцию сохраняется архив, содержащий в себе:

- квитанцию DVC в формате CMS в файле с расширением **.p7s*;
- краткое отображение квитанции в файлах с расширением **.pdf, *.html*;
- полный разбор квитанции и саму квитанцию в формате BASE64 в файле с расширением **.json*.

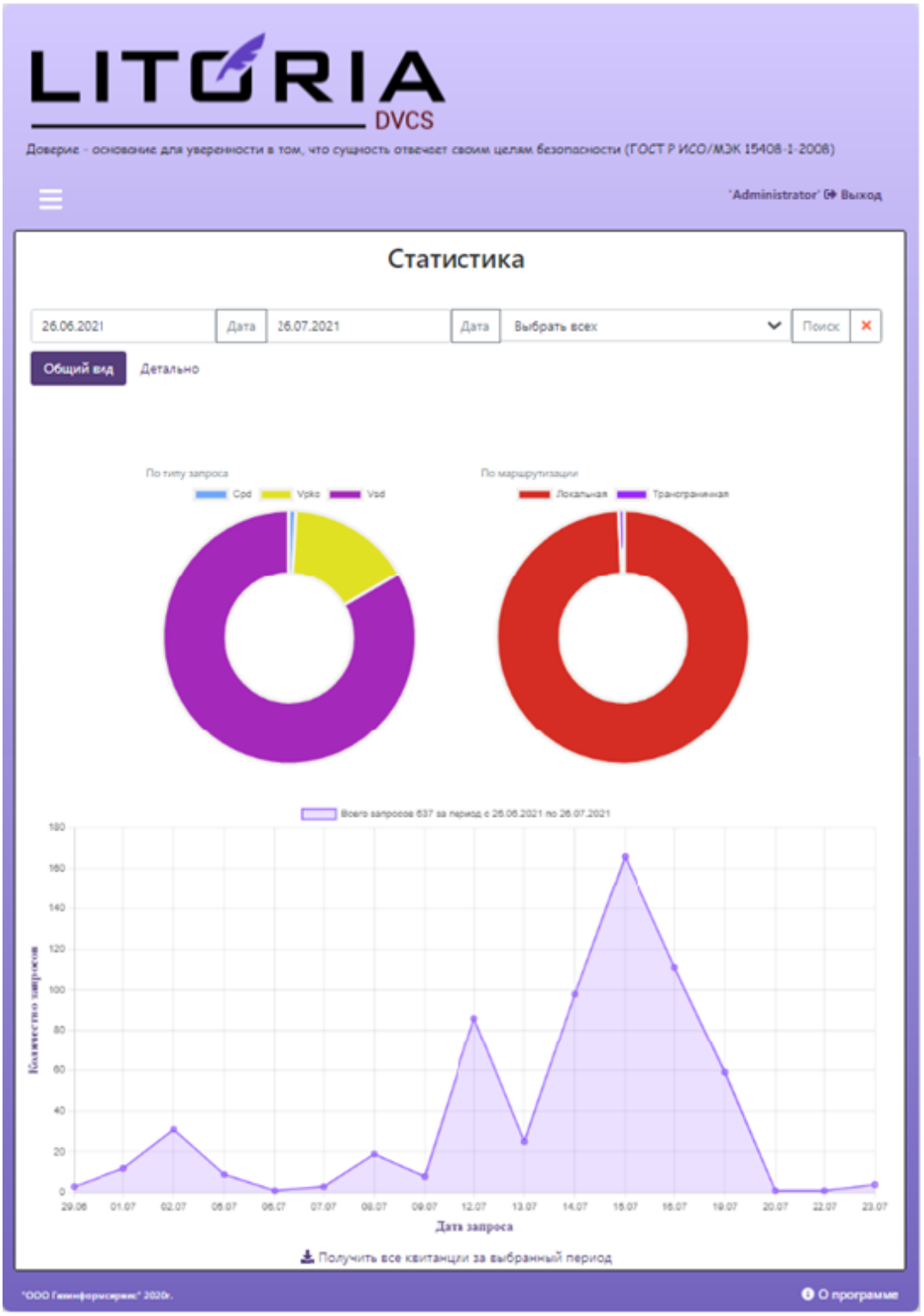

Рисунок 5.44 – Вкладка «Статистика» общий вид

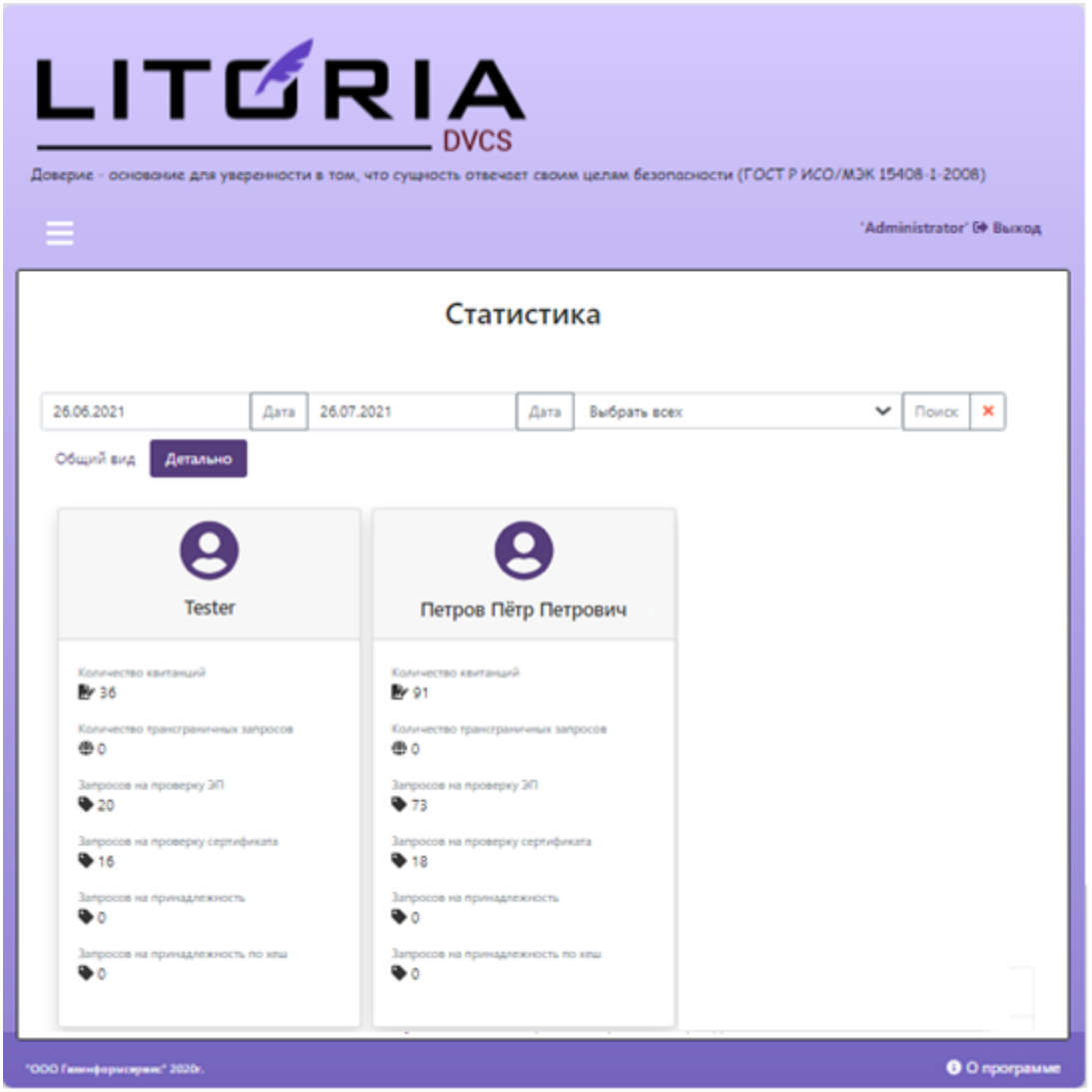

Рисунок 5.45 – Вкладка «Статистика» детальное отображение

6 Служба продления квитанций

Служба продления квитанций предназначена для автоматической пролонгации подписанных квитанций, хранящихся в базе данных сервиса доверенной третьей стороны.

При проверке служба продления квитанций выполняет следующие шаги:

1. Осуществляется проверка на действительность сертификата сервиса штампов времени, к которому обращается комплекс.

2. При положительном результате проверки сертификата сервиса штампов времени на действительность служба запускает процедуру пролонгации квитанций в зависимости от настроек, заданных в файле конфигурации службы *«appsettings.json»* по пути *C:\Program Files (x86)\GIS\Litoria Dvcs\updater* (содержание файла приведено в Приложении 1).

По умолчанию в файле конфигурации установлено, что ЭП квитанции будет продлеваться в случае, если до окончания ее действия осталось менее 90 дней. Изменение срока продления квитанции доступно в файле конфигурации *«appsettings.json»* по пути *C:\Program Files (x86)\GIS\Litoria Dvcs\updater*.

В случае, если срок действия подписи квитанции становится меньше указанного (параметр *"UpdateOffset"*), подпись автоматический продляется с использованием нового штампа времени (параметр *"UpdateTsp"*).

Второй функцией службы является автоматическая загрузка списка аккредитованных удостоверяющих центров для корректной работы в квалифицированном режиме (параметры *"QualifyFileUrl", "QualifyFilePath"*) и поддержка его в актуальном состоянии.

6.1 Особенности работы службы в ОС Linux

После установки пакета ПК «Litoria DVCS» в каталоге */opt/GIS/litoriadvcs* создаются скрипты для управления службой автопролонгации:

- *update_start.sh* – запуск службы;
- *update_stop.sh* – остановка службы;
- *update_enable.sh* – разрешение запуска службы при загрузке ОС;
- *update_disable.sh* – запрет запуска службы при загрузке ОС.

7 Конфигурационные файлы

Файлы конфигурации предназначены для хранения настроек, связанных с функционированием ПК «Litoria DVCS».

Изменение настроек доступно в одноименных конфигурационных файлах ***«appsettings.json»***, расположенных в директории установки ПК «Litoria DVCS» по пути: *C:\Program Files (x86)\GIS\Litoria Dvcs\dvcs* – для работы службы DVCS и *C:\Program Files (x86)\GIS\Litoria Dvcs\update* – для работы службы автопролонгации квитанций, хранимых в базе данных (примеры конфигурационных файлов приведены в Приложении 1).

После внесения изменений в конфигурационные файлы необходимо перезапустить работу пула приложений служб в диспетчере служб IIS: перейти к сайту *«DVCS»* и нажать на кнопку *«Перезапустить»* (рисунок 3.22).

7.1 Настройки лог-файла

Лог-файл необходим для выяснения причин неработоспособности служб комплекса. По умолчанию в комплексе выключено создание лог-файла. Для его включения необходимо перейти к набору параметров для настройки ведения лога, указать в параметре «*IsEnFileLog*» значение «true» и при необходимости изменить остальные параметры в соответствии с пояснениями к ним.

```
"FileLog": {
  //Вести файловый лог
  "IsEnFileLog": false,
  //Название файла лога
  "Path": "dvcs.txt",
  //Возможность добавления
  "Append": "True",
  //Максимальный размер файла лога байт
  "FileSizeLimitBytes": 0,
  //Ротация файлов лога по достижению максимального размера
  "MaxRollingFiles": 0
}
```

7.2 Настройки подключения к БД

Параметры подключения к БД задаются при установке ПК «Litoria DVCS». При необходимости их изменения перейдите к набору параметров для настройки подключения к базе данных и установите требуемые параметры в соответствии с пояснениями к ним, где:

- ***Host*** – IP-адрес или DNS-имя рабочей станции, на которой установлена СУБД;
- ***Port*** – значение TCP-порта, по которому осуществляется работа СУБД;
- ***Database*** – имя создаваемой базы данных;
- ***Username*** – имя учетной записи, обладающей полномочиями создания и редактирования СУБД;
- ***Password*** – пароль указанной выше учетной записи.

```
//Список разрешенных для подключения хостов
  "AllowedHosts": "*",
  "ConnectionStrings": {
    //Настройки подключения к базе данных
    "DefaultConnection":
"Host=localhost;Port=5432;Database=dvcs;Username=postgres;Password=postgres"
  },
```

7.3 Настройки учетных записей

По умолчанию установлены следующие настройки учетных записей пользователей и администраторов:

- длина пароля не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения;
- при смене пароля недопустимо использовать 5 последних паролей, использованных ранее;
- после третьего неверного ввода идентификационных данных учетная запись блокируется на 60 минут.
- период смены пароля не реже одного раза в 180 дней.

При необходимости изменения требований к парольной информации перейдите к набору параметров для настройки учетных записей пользователей и установите требуемые параметры в соответствии с пояснениями к ним.

```
"DvcsConfig": {
   "AccountOptions": {
     //Время на которое будет заблокирован пользователь (мин)
     "LockTime": 60,
     //Количество неудачных попыток после которых произойдет блокировка
     "LockCount": 3,
```

```
    //Блокировка последних N введенных паролей
    "LockLastPwdCount": 5,
    //Минимальная длина задаваемого пароля
    "RequiredLength": 8,
    //Неоходимость использования цифры в пароле
    "RequireDigit": true,
    //Необходимость использования в пароле символов в нижнем регистре
    "RequireLowercase": true,
    //Необходимость использования в пароле символов в верхнем регистре
    "RequireUppercase": true,
    //Необходимость использования в пароле специальных символов
    "RequireNonAlphanumeric": false,
    //Включение использования токена аутентификации
    "IsUseSecurityToken": true,
    //Включение использования перенаправления на https
    "IsUseHttpsRedirection": false,
    //Время бездействия пользователя по истечении которого происходит выход из системы (минут)
    "IdleTimeOut": 20,
    //Время действия пароля пользователя в (дней)
    "PwdChangeTimeout": 180,
    //Пароли запрещенные к использованию (можно изменить на свои)
    "BlockedPwd": [
      "qwerty",
      "123456",
      "qwertyuiop",
      "qwe123",
      "123456789",
      "111111",
      "klaster",
      "qweqwe",
      "1qaz2wsx",
      "1q2w3e4r",
      "qazwsx",
      "1234567890",
      "1234567",
      "7777777",
      "123321",
      "1q2w3e",
      "123qwe",
      "1q2w3e4r5t",
      "zxcvbnm",
```

```
      "123123"
    ]
  },
```

7.4 Настройки службы DVCS

При необходимости изменения настроек службы DVCS перейдите к набору параметров для настройки службы доверенной третьей стороны и установите требуемые параметры в соответствии с пояснениями к ним.

```
"Dvcs": {
    //Сохранять или нет квитанции в базе данных
    "IsSaveData": true,
    //Наименование идентификатора службы, которое будет отображаться в квитанции
    "DtsId": "ДТС v.6",
    //Используемое уникальное имя службы ДТС, для определения маршрута, принадлежащего данному серверу
    "DvcUniqueId": "#Dvc1-2021-01",
    //Используемый адрес службы штампов времени
    "TspAddress": null,
    //Включение использования усовершенствованной электронной подписи в ответе
    "IsUseCadesXLT": false,
    //Используемый алгоритм хеширования
    "HashOid": "1.3.14.3.2.26",
    //Включение разрешения разбора квитанции в статистике при скачивании архива
    "EnableParsedStatView": false,
   //Использовать режим хеширования запросов в браузере и API
    "IsUseClientHash": false,
    //Тип журналирования событий
    "Journal": "Both"
   },
```

7.4.1 Настройка сохранения квитанций

По умолчанию в комплексе будет производиться сохранение квитанций службы в базе данных. Для отмены сохранения необходимо указать в параметре *«IsSaveData»* значение «false».

7.4.2 Настройка идентификатора службы

По умолчанию в комплексе используется идентификатор службы DVCS *«ДТС v.6»*. Это наименование будет отображаться в квитанциях службы.

В случае, когда используется режим работы в кластере с более чем одной службой DVCS при обращении к одной БД, и требуется подписывать квитанции с помощью другой

ключевой пары сертификат – закрытый ключ, то необходимо использовать уникальные идентификаторы на каждой машине кластера. Уникальное имя службы задается в параметре «*DvcUniqueId*»

7.4.3 Использование усовершенствованной ЭП в ответе службы

По умолчанию в настройках комплекса не используется усовершенствованная ЭП в ответе службы (т.е. в подпись не включаются доказательства действительности сертификата на момент времени службы DVCS). Если необходимо использовать усовершенствованную ЭП в ответе службы DVCS, в параметре «*IsUseCadesXLT*» необходимо указать значение «true».

7.4.4 Настройка используемого алгоритма хеширования

Для обеспечения соответствия ответа службы DVCS полученному запросу необходимо указать и установить алгоритм хеширования. По умолчанию установлен алгоритм SHA-1, OID 1.3.14.3.2.26.

> В случае установки алгоритма хеширования ГОСТ необходимо убедиться, что удаленный сервер ДТС поддерживает криптографию ГОСТ. В противном случае он не сможет выполнить проверку документа.
>
> Рекомендуется оставить алгоритм SHA-1, OID 1.3.14.3.2.26.

Для изменения используемого алгоритма хеширования добавьте нужный OID в параметре «*HashOid*».

7.4.5 Настройка используемого идентификатора проверки службы TSP

Идентификатор, с помощью которого будут хешироваться данные и отправляться в службу TSP, определяется автоматически и не требует дополнительных настроек.

7.4.6 Настройка типа журналивания событий

По умолчанию включено ведение одновременно двух журналов (значение параметра *"Journal": "Both"*). Возможно использование и других значений:

"Db" – для записи только в базу данных;

"Syslog" – для ведения журнала только с использованием syslog.

7.5 Общие настройки

При необходимости изменения общих настроек перейдите к набору параметров для общих настроек службы и установите требуемые параметры в соответствии с пояснениями к ним.

```
"BaseService": {
    //Список разрешенных криптосредств
```

```
    "AllowedCsp": [],
    //Режим обработки квалифицированного статуса
    "Qualify": "No",
    //Максимально допустимый размер документа, отправляемого на проверку байт.
    "MaxRequestSizeBytes": 20971520,
    //Включение разрешения принудительного скачивания списка отзыва
    "InhibitCashingCrl": false
  },
```

7.5.1 Настройка списка разрешенных криптопровайдеров

Данная настройка предоставляет возможность ограничить список разрешенных криптопровайдеров. При наличии данного списка служба будет проверять только:

- запросы, созданные с использованием криптопровайдеров, указанных в этом списке;
- файлы, подписанные с использованием алгоритма криптопровайдеров, указанных в этом списке.

По умолчанию в параметре «*AllowedCsp*» не указаны разрешенные криптопровайдеры. Для добавления криптопровайдера в список, добавьте названия нужных криптопровайдеров в параметре «*AllowedCsp*», например:

"AllowedCsp": ["Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider"],

7.5.2 Настройка работы служб в квалифицированном режиме

По умолчанию службы DVCS и TSP работают в неквалифицированном режиме (т.е. при проверке подписей и сертификатов в квитанции всегда будет информация о том, что подпись/сертификат не квалифицированные). Для указания параметров работы служб в квалифицированном режиме необходимо установить следующие значения параметров, приведенных в таблице 7.1.

Таблица 7.1 – Настройки служб DVCS и TSP для работы в квалифицированном режиме

Параметр	Назначение параметра
"Qualify": " Label",	Использование квалифицированного режима (запрос проверяется на предмет квалифицированности, т.е. все сертификаты в цепочке должны быть выпущены аккредитованным УЦ): • *No* - не использовать квалифицированный режим; • *Label* – положительная квитанция с пометкой о квалифицированности; • *Error* – отрицательная квитанция, если статус не квалифицированный (если сертификат

Параметр	Назначение параметра
	неквалифицированный, то будет создаваться квитанция с ошибкой).
"QualifyFileUrl": "https://e-trust.gosuslugi.ru/CA/DownloadTSL?schemaVersion=0"	Указание URL адреса для скачивания списка аккредитованных УЦ (см. п. 6.10 «Настройка обновление списка квалифицированных средств ЭП и УЦ»). Данный параметр содержится в файле настроек службы автопролонгации (C:\Program Files (x86)\GIS\Litoria Dvcs\updater\appsettings.json)
"QualifyFilePath": "tsl.xml"	Указание пути к скаченному файлу списка аккредитованных УЦ (см. п. 6.10 «Настройка обновление списка квалифицированных средств ЭП и УЦ»). Дублируется из C:\Program Files (x86)\GIS\Litoria Dvcs\updater\appsettings.json.

При включенном квалифицированном режиме при каждом обращении к службам выполняется дополнительная проверка сертификатов служб на квалифицированность.

Настройки квалифицированности применяются для текущей службы ДТС. В случае переадресации документа другой службе ДТС (согласно маршруту) формирование квитанции происходит на удалённой стороне с использованием указанных там настроек.

7.5.3 Настройка ограничения размера документа, отправляемого на проверку

По умолчанию в комплексе максимально допустимый размер входящего запроса ограничен 20Мб:

"MaxRequestSizeBytes": 20971520,

Для изменения данного ограничения необходимо в параметре «*MaxRequestSizeBytes*» указать требуемое значение.

7.5.4 Настройка запрета/разрешения принудительного скачивания списков отзыва

По умолчанию принудительное скачивание список отзыва выключено. При таком режиме запрашиваемые списки отзыва, использующиеся для проверки сертификата, не сохраняются в локальном хранилище сертификатов.

Для разрешения принудительного скачивания списков отзыва на сервер службы DVCS необходимо указать в параметре «*InhibitCashingCrl*» значение «true».

7.6 Настройки работы со службой TSP

При необходимости изменения настроек службы TSP перейдите к набору параметров

для настройки работы со службы штампов времени и установите требуемые параметры в соответствии с пояснениями к ним.

```
Tsp": {
    //Список поддерживаемых алгоритмов хэширования
    "AllowedHashAlgs": [ "1.2.643.2.2.9", "1.2.643.7.1.1.2.2", "1.2.643.7.1.1.2.3", "1.3.14.3.2.26" ],
    //Точность времени (мс)
    "Accuracy": 0,
    //Включение разрешения работы службы штампов времени
    "IsUseTsp": true
  },
```

Значение параметра «*Accuracy*» (точность) указывается в микросекундах и должно содержать допустимое отклонение (погрешность) времени выдачи штампа.

Список поддерживаемых алгоритмов хеширования указывается в параметре «*AllowedHashAlgs*». По умолчанию служба TSP поддерживает алгоритмы:

- ГОСТ Р 34.11-94, OID 1.2.643.2.2.9;
- ГОСТ Р 34.11-12 с длиной 256, OID 1.2.643.7.1.1.2.2;
- ГОСТ Р 34.11-12 с длиной 512, OID 1.2.643.7.1.1.2.3.

Если требуется добавить алгоритм хеширования, который отсутствует в этом списке и необходим для работы службы TSP, в параметре «*AllowedHashAlgs*» укажите OID требуемого алгоритма.

7.7 Настройки групп алгоритмов в маршрутах

Маршруты необходимы при выполнении запросов для определения алгоритма подписи ответов службы DVCS и формирования пути проверки документов в зависимости от возможности службы DVCS обрабатывать различные алгоритмы

При необходимости изменения алгоритмов подписи, которые сможет проверять служба DVCS, допустимых для выбора при настройке маршрутов, перейдите к набору параметров для настройки маршрутов и установите требуемые параметры в соответствии с пояснениями к ним.

```
"RouteGroup": {
    "Route": {
     //Список разрешенных для использования отечественных алгоритмов
     "RU": [ "1.2.643.2.2.19", "1.2.643.7.1.1.1.1", "1.2.643.7.1.1.1.2" ],
     //Список разрешенных для использования европейских алгоритмов
     "EU": [ "1.2.840.113549.1.1.1", "1.2.840.113549.1.1.2", "1.2.840.113549.1.1.3", "1.2.840.113549.1.1.4", "1.2.840.113549.1.1.5" ],
     //Список разрешенных для использования казахстанских алгоритмов
```

```
    "KZ": [ "1.2.398.3.10.1.1.1.2", "1.2.398.3.10.1.3.1", "1.2.398.3.10.1.1.1.1" ],
    //Список разрешенных для использования белорусских алгоритмов
    "RB": [ "1.2.112.0.2.0.34.101.45.12", "1.2.112.0.2.0.34.101.45.2.1" ]
  }
 },
```

По умолчанию в группе параметров *"Route"* указан список алгоритмов подписи, с которыми может работать служба DVCS при настройке маршрутов.

Если требуется добавить алгоритм подписи, который отсутствует в этом списке, укажите OID требуемого алгоритма в соответствии с принадлежностью алгоритма.

7.8 Настройка работы со службой syslog

Набор параметров для настройки работы со службой syslog по умолчанию содержит настройки, при которых информационные сообщения сохраняются только в системном журнале web-кабинета (параметр «*IsDubSyslog*»):

```
"Syslog": {
    //Адрес службы syslog
    "Host": "localhost",
    //Порт для подключения к службе syslog
    "Port": 514,
 },
```

При необходимости изменения работы со службой syslog перейдите к набору параметров для настройки работы со службой и установите требуемые параметры в соответствии с пояснениями к ним.

7.9 Настройки продления квитанций

Продление квитанции используется в случае, когда срок действия квитанций подходит к концу.

Настройки продления квитанций, задаются в блоке настроек продления квитанций и обновления трастед листа.

```
"Update": {
        //Оставшийся период действия в днях до которого квитанции не будет продлеваться
    "UpdateOffset": 90,
    //Период обновления сервиса обновления в часах
    "UpdatePeriod": 24,
    //Используемый адрес службы штампов времени для обновления квитанций
    "UpdateTsp": null,
        //Сохранять или нет по заданному пути после скачивания
    "IsSaveTsl": true
```

},

По умолчанию в параметре «*UpdateOffset*» установлено значение «90», означающее, что квитанция будет продлеваться в случае, если до окончания ее действия осталось менее 90 дней.

В параметре «*UpdateTsp*» задается адрес службы TSP, используемый для обновления и продления квитанций.

7.10 Настройка обновления списка квалифицированных средств ЭП и УЦ

При включенном квалифицированном режиме работы, для проверки сертификатов служб на квалифицированность и для признания проверяемой ЭП квалифицированной ЭП, необходим список сертифицированных средств ЭП и УЦ. Список содержит наименования сертифицированных средств ЭП и УЦ, и реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным законодательством Российской Федерации.

Настройка обновления списка сертифицированных средств ЭП и УЦ, необходимая для работы при включенном квалифицированном режиме работы, задается в конфигурационном файле *«appsettings.json»* по пути *C:\Program Files (x86)\GIS\Litoria Dvcs\update* в блоке настроек продления квитанций и обновления трастед листа.

```
"Update": {
        //Путь к файлу трастед листа сохраненного ранее
    "QualifyFilePath": "tsl.xml",
    //Адрес для скачивания промежуточных сертификатов Мин.Связи
    "QualifyFileUrl": "https://e-trust.gosuslugi.ru/CA/DownloadTSL?schemaVersion=0",
        //Сохранять или нет по заданому пути после скачивания
    "IsSaveTsl": true
  },
```

Адрес для загрузки списка квалифицированных средств ЭП и УЦ задается в конфигурационном файле *«appsettings.json»* по пути *C:\Program Files (x86)\GIS\Litoria Dvcs\update* в параметре «*QualifyFileUrl*». По умолчанию скачивание списка квалифицированных средств ЭП и УЦ происходит с портала уполномоченного федерального органа в области использования электронной подписи (УФО).

Путь к скаченному файлу списка квалифицированных средств ЭП и УЦ задается в параметре «*QualifyFilePath*».

Необходимо убедится в том, что путь к загруженному файлу списка квалифицированных средств ЭП и УЦ в одноименных конфигурационных файлах ***«appsettings.json»***, расположенных в директории установки ПК «Litoria DVCS» по пути: C:\Program Files (x86)\GIS\Litoria Dvcs\dvcs и C:\Program Files (x86)\GIS\Litoria Dvcs\updater задан одинаково.

7.11 Настройки для проверки разграничений по полномочиям

Возможность проверки полномочий предназначена для регулирования доступа к проверяемым документам. OID, занесённые в список для определённый группы, сравниваются с данными в сертификате, и, если они совпадают, проверка разрешается.

При необходимости изменения настроек разграничений полномочий пользователей перейдите к набору параметров для настройки проверки разграничений по полномочиям и установите требуемые параметры в соответствии с пояснениями к ним.

```
"Policy": {
    //Включение использования проверки полномочий
    "IsUsePolicy": false,
    "PolicyName": {
     //Наименование группы и OID список
     "Директор": [ "1.3.6.1.5.5.7.3.55", "1.3.6.1.5.5.7.3.56" ],
     //Наименование группы и OID  список
     "Администратор": [ "1.2.643.2.2.34.7" ],
     //Наименование группы и OID  список
     "Сотрудник с правом подписи": [ "1.3.6.1.5.5.7.3.11" ]
    }
```

8 Модуль REST API

Модуль REST API позволяет выполнять автоматизированную отправку запросов и получение ответов участниками электронного взаимодействия, при этом позволяя внешней информационной системе не иметь криптографию.

Для отправки запросов с использованием модуля, учетной записи пользователя, который формирует запрос, должен быть назначен токен безопасности, для прохождения аутентификации при обращении в службе.

Назначение токена доступно после прохождения аутентификации в web-кабинете ПК «Litoria DVCS» в пункте меню ***«Пользователи»*** в окне редактирования учетной записи (рисунок 8.1) в поле ***«Токен доступа»*** по кнопке ***«Создать»***.

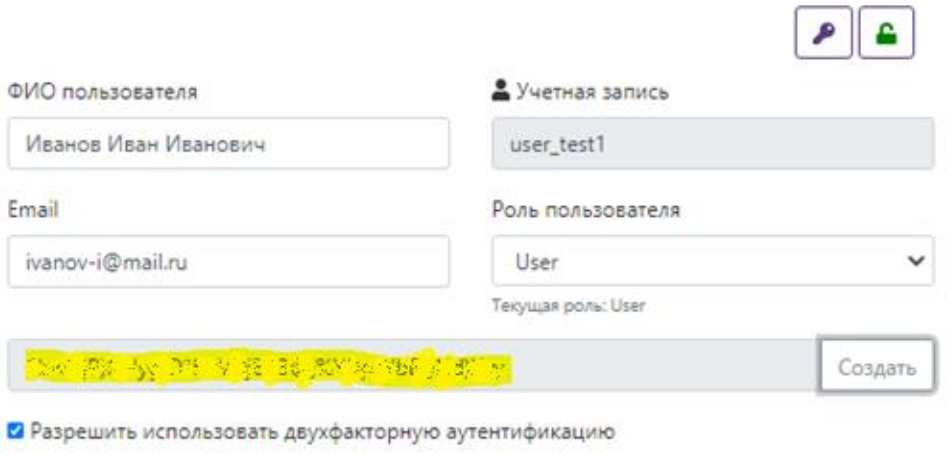

Рисунок 8.1 – Назначение пользователю токена для отправки запросов

1. Метод проверки жизнеспособности ДТС – ***hc.*** Метод позволяет определить работоспособность ДТС, к которой происходит обращение. В результате выполнения запроса запускаются следующие механизмы: проверка работоспособности службы ДТС, проверка соединения с БД, тестовая подпись данных с использованием маршрута с максимальным приоритетом.

Метод: *POST, GET*

URL: http://<ip_dvcs>/hc

Задаётся без параметров.

Результатом данного запроса станет ответ в формате Json, содержащий информацию о проверке службы DVCS, проверке соединения с БД, проверке на возможность подписи и подпись данных из маршрута с максимальным приоритетом. Пример ответа представлен ниже:

```
{
    "Status": "",
    "Duration": "",
    "Info": [
```

```
        {
            "Status": "",
            "IsActivated": bool,
            "Description": "",
            "Duration": "",
            "Key": ""
        }
    ],
    "Name": ""
```

"Status"	Состояние работоспособности ДТС. Принимает значение Healthy – в случае корректности работы, и Unhealthy – в случае возникновения ошибок
"Duration"	Время обработки запроса
"Info"	Блок, описывающий подробно результаты проверки работоспособности ДТС
"IsActivated"	Флаг, показывающий, активирован ли ПК, принимает значение *true* – если активирован, *false* – если нет
"Description"	Комментарий к параметру *IsActivated*
"Key"	Идентификатор проверки работоспособности
"Name"	Заголовок ответа

2. Метод проверки данных через сервис ДТС – ***GetDvcResponse***. Запрос отправляет документ (сертификат, хэш-значение) на проверку доверенной третьей стороне, аналогично проверке документа через web-кабинет. В качестве ответа возвращается квитанция в формате Json, содержащая в себе информацию о подписи и сертификатах в ней.

Метод: *POST*

URL: http://<ip_dvcs>/Api/GetDvcResponse

JSON:

```
{
  "File": "",
  "FileName": "",
  "Data": "",
  "DataName": "",
  "Token": "",
  "Policy":[""],
  "Ccpd": bool
}
```

"File"	Данные для проверки (подпись, сертификат, файл), представленные в бинарном виде (Base64)
"FileName"	Имя проверяемого файла. Используется только для отображения в квитанции, является опциональным. Передаётся в виде текста
"Data"	Данные для проверки отделённой подписи, представленные в бинарном виде (Base64). Параметр является опциональным, используется в случае работы с отделённой подписью.

"DataName"	Имя файла данных в случае, если подпись отделенная, является опциональным. Передаётся в виде текста
"Token"	Токен безопасности, используется для прохождения аутентификации, выпускается самостоятельно пользователем или администратором в web-кабинете. Передаётся в открытом виде. Обязательно использование https-соединения
"Policy"	Набор полномочий в виде объектных идентификаторов, массив. Является опциональным. Задаётся в формате 0.0.0.0.0.0.0.0.0
"Ccpd"	Параметр, включающий использование запроса типа CCPD. Принимает значение *true/false*

3. Метод получения всех квитанций по исходному файлу – ***GetTicketByFile.*** Данный запрос позволяет выполнить поиск и разбор квитанции по исходному документу. В качестве ответа возвращается разобранная квитанция в формате Json, содержащая развёрнутую информацию о подписи и сертификатах в ней.

Метод: *POST*

URL: http://<ip_dvcs>/Api/GetTicketByFile

JSON:

```
{
  "File": "",
  "Token": ""
}
```

"File"	Данные для проверки (подпись, сертификат, файл), представленные в бинарном виде (Base64)
"Token"	Токен безопасности, используется для прохождения аутентификации, выпускается самостоятельно пользователем или администратором в личном кабинете. Передаётся в открытом виде. Обязательно использование https-соединения

4. Метод получения квитанции по идентификационному или серийному номеру - ***GetTicketById.*** Запрос выполняет поиск квитанции или по её идентификационному номеру, или по серийному. Результатом выполнения операции является разобранная искомая квитанция в формате Json.

Метод: *POST*

URL: http://<ip_dvcs>/Api/GetTicketById

JSON:

```
{
  "TicketSn": "",
  "TicketId": "",
  "Token": "",
 "IsSigned": bool
}
```

"TicketSn"	Серийный номер искомой квитанции – в случае поиска по серийному номеру. Передаётся в открытом виде

"TicketId"	Идентификатор искомой квитанции – в случае поиска по идентификационному номеру. Передаётся в открытом виде
"Token"	Токен безопасности, используется для прохождения аутентификации, выпускается самостоятельно пользователем или администратором в личном кабинете. Передаётся в открытом виде. Обязательно использование https-соединения
"IsSigned"	Флаг, подтверждающий выдачу подписанной (состояние *true*) квитанции или не подписанной квитанции (состояние *false*) (влияет на производительность).

5. Метод получения всех квитанций по исходному документу – ***GetDVCByFile.*** Запрос выполняет поиск всех квитанций, связанных с документом в запросе. Результатом выполнения операции является массив неразобранных квитанций.

Метод: *POST*

URL: http://<ip_dvcs>/Api/GetDVCByFile

JSON:

```
{
  "File": "",
  "Data": "",
  "Token": ""
  }
```

"File"	Данные для проверки (подпись, сертификат, файл), представленные в бинарном виде (Base64)
"Data"	Данные для проверки отделённой подписи, является опциональным, используется в случае работы с отделённой подписью, представленные в бинарном виде (Base64)
"Token"	Токен безопасности, используется для прохождения аутентификации, выпускается самостоятельно пользователем или администратором в личном кабинете. Передаётся в открытом виде. Обязательно использование https-соединения

6. Метод получения Dvc-запроса на документ - ***GetDvcRequest.*** Результатом выполнения операции является сформированный запрос на обращение к ДТС в бинарном виде (base64).

Метод: *POST*

URL: http://<ip_dvcs>/Api/GetDvcRequest

JSON:

```
{
  "File": "",
  "FileName": "",
  "Data": "",
  "DataName": "",
  "Token": ""
}
```

"File"	Данные для проверки (подпись, сертификат, файл), представленные в бинарном виде (Base64)

"FileName"	Имя проверяемого файла. Используется только для отображения в квитанции, является опциональным. Передаётся в виде текста
"Data"	Данные для проверки отделённой подписи, является опциональным, используется в случае работы с отделённой подписью. представленные в бинарном виде (Base64)
"DataName"	Имя файла данных в случае, если подпись отделенная, является опциональным. Передаётся в виде текста
"Token"	Токен безопасности, используется для прохождения аутентификации, выпускается самостоятельно пользователем или администратором в личном кабинете. Передаётся в открытом виде. Обязательно использование https-соединения

7. Метод продления подписи - ***Update.*** Запрос предназначен для продления срока действия ЭП в документе путём включения в неё информации о времени создания подписи (TSP). Используемый адрес службы штампов времени задаётся в файле настроек – параметр *UpdateTsp.*

Метод: *POST*

URL: http:// <ip_dvcs>/Api/Update

JSON:

```
{
  "File": "",
  "Data": "",
  "Token": ""
}
```

"File"	Данные для проверки (подпись, сертификат, файл), представленные в бинарном виде (Base64)
"Data"	Данные для проверки отделённой подписи, является опциональным, используется в случае работы с отделённой подписью. представленные в бинарном виде (Base64)
"Token"	Токен безопасности, используется для прохождения аутентификации, выпускается самостоятельно пользователем или администратором в личном кабинете. Передаётся в открытом виде. Обязательно использование https-соединения

9 Нагрузочное тестирование

9.1 Исходные данные

В данном тесте использовались три типа электронной подписи:

- усиленная квалифицированная,
- усиленная квалифицированная со штампом времени,
- усовершенствованная квалифицированная подпись.

Размеры подписанных документов - 10кб, 100кб, 1мб.

Алгоритм подписи - ГОСТ 2012.

В связи с тем, что по структуре ЭП указанных типов различны, время, затраченное на их обработку в ходе тестирования, также будет отличаться.

Наиболее быстро проверяется усиленная квалифицированная подпись, т.к. она не содержит штампов времени или доказательств, которые требуют дополнительной проверки.

В данном исследовании использовались реальные ЭП с проверкой:

- через службу онлайн-проверки сертификатов аккредитованного удостоверяющего центра;
- через службу штампов времени аккредитованного УЦ.

Необходимо учитывать, что проверка ЭП всегда состоит из локальных вычислений и получения доказательств от источников в УЦ. Даже если время вычисления корректности ЭП будет минимальным, а получение списка отзыва и ответа службы онлайн-проверки сертификатов по сети максимальным, то общее время проверки будет равняться сумме этих значений. Поэтому необходимо анализировать затраты на сетевое взаимодействие между службой ДТС и УЦ.

Для достижения максимальной производительности при проверке ЭП необходимо:

- исключить сетевое взаимодействие,
- установить промежуточные сертификаты в локальное хранилище сертификатов,
- убедится, что в сертификате подписчика отсутствуют ссылки на службу онлайн-проверки сертификатов,
- убедится, что ЭП не содержит метки времени.

Аналогично учитывается количество промежуточных сертификатов в цепочке: чем больше сертификатов, тем дольше проверка ЭП, т.к. доказательства собираются для каждого сертификата.

В описываемом в данном отчете тесте цепочка состояла из:

- корневого сертификата Минкомсвязи России,
- промежуточного сертификата аккредитованного УЦ,
- сертификата подписчика.

Основным фактором увеличения скорости работы службы ДТС является производительность CPU, т.к. если сетевые задержки можно свести к минимальному времени, разместив УЦ в той же сети, то скорость хеширования, вычисление подписи и доступ к закрытому ключу прямо коррелируют с производительность CPU. Скоростные показатели жесткого диска, сетевой карты памяти не являются приоритетом, если они не критически устарели.

Стоит учитывать готовность службы ДТС к проверке в том случае, когда она находится в состоянии сна, т.е. первый запрос всегда обрабатывается медленнее, т.к. в момент обращения происходит инициализация криптографического ядра, загрузка промежуточных сертификатов и установка соединения с СУБД.

9.2 Этапы тестирования

Проводимое тестирование разбито на три этапа:

1. Первый набор теста проверяет ЭП и определяет нагрузку от внешней ИС через прямой POST-запрос в службу ДТС с аутентификацией по сертификату и выдачей неразобранной подписанной квитанции в бинарном формате.

2. Второй набор выполняет проверку ЭП и определяет нагрузку от внешней ИС через REST-запрос в службу ДТС с аутентификацией по токену безопасности с выдачей разобранной и подписанной квитанции в формате json. Данный метод работает медленнее, т.к. происходит разбор квитанции с выдачей всей информации по результатам проверки ЭП, но он не требует наличия криптографии на стороне ИС.

3. Третий набор выполняет продление ЭП из состояния CAdES-Bes в CAdES-XLT, и затем в CAdES-A, что означает модификацию усиленной квалифицированной ЭП до состояния усовершенствованной квалифицированной ЭП, и модификацию усовершенствованной квалифицированной ЭП до состояния архивной квалифицированной ЭП.

Производительности данного сервера недостаточно, и во всех многопоточных тестах нагрузка CPU она была равна 100%.

9.3 Описание оборудования

При проведении тестирования был использован стенд со следующими характеристиками:

- ОС – Windows Server 2016;
- Процессор - Intel Xeon CPU E5-2678V3 2.5 GHz;
- Оперативная память - 32 GB RAM DDR-4;
- Установлен КриптоПро версии 4.0.9971.

9.4 Результаты тестирования

Результаты тестирования после отправки DVC-запроса из ИС приведены в таблице 9.1.

Таблица 9.1 – Результаты тестирования после отправки DVC-запроса

Тип запроса /api/dvc						
№	**Тип подписи**	**Размер документа, Кбайт**	**Нагрузка**	**Время обработки (мин)**	**Кол-во запросов/сек**	**Кол-во запросов/мин**
1	Усиленная квалифицированная	10	20 потоков по 50 запросов	01:19	12	840
2	Усиленная квалифицированная	10	1 поток - 1000 запросов	09:56	1	104
3	Усиленная квалифицированная ЭП	100	20 потоков по 50 запросов	01:20	12	833
4	Усиленная квалифицированная ЭП	1024	20 потоков по 50 запросов	01:21	12	826
5	Усиленная квалифицированная ЭП со штампом времени	1024	20 потоков по 50 запросов	01:51	9	662
6	Усиленная квалифицированная ЭП со штампом времени	1024	20 потоков по 250 запросов	08:59	9	582
7	Усиленная квалифицированная ЭП	1024	20 потоков по 250 запросов	06:26	13	799
8	Усовершенствованная квалифицированная ЭП	1024	20 потоков по 250 запросов	07:59	10	659
9	Усиленная квалифицированная ЭП	1024	20 потоков по 2500 запросов	62:55	13	799

Результаты тестирования операции отправки запроса и разбора квитанции через REST с использованием токена безопасности приведены в таблице 9.2.

Таблица 9.2 – Результаты тестирования операции отправки запроса и разбора квитанции через REST

Тип запроса /api/GetDvcResponse						
№	**Тип подписи**	**Размер документа, Кбайт**	**Нагрузка**	**Время обработки (мин)**	**Кол-во запросов/сек**	**Кол-во запросов/мин**
1	Усиленная квалифицированная ЭП	10	20 потоков по 50 запросов	01:16	13	862
2	Усиленная квалифицированная ЭП	100	20 потоков по 50 запросов	01:16	13	862
3	Усиленная квалифицированная ЭП	1024	20 потоков по 50 запросов	01:18	12	847
4	Усиленная квалифицированная ЭП	1024	20 потоков по 250 запросов	06:22	13	803
5	Усиленная квалифицированная ЭП со штампом времени	1024	20 потоков по 250 запросов	11:38	7	439
6	Усовершенствованная квалифицированная ЭП	1024	20 потоков по 250 запросов	13:12	6	381

Результаты тестирования операции продления ЭП приведены в таблице 9.3.

Таблица 9.3 – Результаты тестирования операции продления ЭП

Продление ЭП до состояния усовершенствованная квалифицированная ЭП, /api/update						
№	**Тип подписи**	**Размер документа, Кбайт**	**Нагрузка**	**Время обработки (мин)**	**Кол-во запросов/сек**	**Кол-во запросов/мин**
1	Усиленная квалифицированная ЭП	100	20 потоков по 50 запросов	02:41	6	415
Продление ЭП до состояния архивной квалифицированной ЭП, /api/update						
2	Усиленная квалифицированная ЭП	100	20 потоков по 50 запросов	02:05	6	488

Приложение 1

Конфигурационный файл работы службы DVCS *«appsettings.json»*

```
{

  //Блок настроек логирования службы ДТС

  "Logging": {
    "LogLevel": {
      // Лог службы ДТС.
      "Default": "Trace",
      // Лог райнтайма
      "Microsoft": "Error"
    },
    //Набор параметров для настройки ведения лога

    "FileLog": {
      //Вести файловый лог
      "IsEnFileLog": true,
      //Название файла лога
      "Path": "dvcs.txt",
      //Возможность добавления
      "Append": "True",
      //Максимальный размер файла лога байт
      "FileSizeLimitBytes": 0,
      //Ротация файлов лога по достижению максимального размера
      "MaxRollingFiles": 0
    }
  },

  //Набор параметров для настройки подключения к базе данных

  //Список разрешенных для подключения хостов
  "AllowedHosts": "*",
  "ConnectionStrings": {
    //Настройки подключения к базе данных
    "DefaultConnection":
"Host=localhost;Port=5433;Database=dvcs;Username=postgres;Password=postgres"
  },

  //Набор параметров для настройки учетных записей пользователей


  "DvcsConfig": {
    "AccountOptions": {
      //Время на которое будет заблокирован пользователь (мин)
      "LockTime": 60,
      //Количество неудачных попыток после которых произойдет блокировка
      "LockCount": 3,
      //Блокировка последних N введенных паролей
      "LockLastPwdCount": 5,
      //Минимальная длина задаваемого пароля
      "RequiredLength": 8,
      //Необходимость использования цифры в пароле
      "RequireDigit": true,
```

```
      //Необходимость использования в пароле символов в нижнем регистре
      "RequireLowercase": true,
      //Необходимость использования в пароле символов в верхнем регистре
      "RequireUppercase": true,
      //Необходимость использования в пароле специальных символов
      "RequireNonAlphanumeric": false,
      //Включение использования токена аутентификации
      "IsUseSecurityToken": true,
      //Включение использования перенаправления на https
      "IsUseHttpsRedirection": false,
      //Время бездействия пользователя по истечении которого происходит выход из системы (минут)
      "IdleTimeOut": 20,
      //Время действия пароля пользователя в (дней)
      "PwdChangeTimeout": 180,
      //Пароли запрещенные к использованию (можно изменить на свои)
      "BlockedPwd": [
        "qwerty",
        "123456",
        "qwertyuiop",
        "qwe123",
        "123456789",
        "111111",
        "klaster",
        "qweqwe",
        "1qaz2wsx",
        "1q2w3e4r",
        "qazwsx",
        "1234567890",
        "1234567",
        "7777777",
        "123321",
        "1q2w3e",
        "123qwe",
        "1q2w3e4r5t",
        "zxcvbnm",
        "123123"
      ]
    },

    //Набор параметров для настройки отображения информации на страницах


    "ViewOptions": {
      //Количество отображаемых на странице элементов квитанции пользователи и т.д.
      "LinesPerPage": 12,
      //Подпись левого футера
      "Issuer": "\"ООО Газинформсервис\" 2020г.",
      //Основная подпись нас странице
      "MainLabel": "Доверие - основание для уверенности в том, что сущность отвечает своим целям
безопасности (ГОСТ Р ИСО/МЭК 15408-1-2008)",
      //Количество записей, выбираемых за запрос влияет на производительность
      "FetchLevel": 500
    },

    //Набор параметров для настройки службы доверенной третьей стороны

    "Dvcs": {
```

```
      //Сохранять или нет квитанции в базе данных
      "IsSaveData": true,
      //Наименование идентификатора службы, которое будет отображаться в квитанции
      "DtsId": "ДТС v.6",
      //Используемый уникальное имя службы ДТС, для определения маршрута, принадлежащего данному
серверу
      "DvcUniqueId": "#Dvc1-2021-01",
      //Используемый адрес службы штампов времени
      "TspAddress": "",
      //Включение использования усовершенствованной электронной подписи в ответе
      "IsUseCadesXLT": false,
      //Используемый алгоритм хеширования
      "HashOid": "1.3.14.3.2.26",
      //Включение разрешения разбора квитанции в статистике при скачивании архива
      "EnableParsedStatView": false,
      //Использовать режим хеширования запросов в браузере и API
      "IsUseClientHash": false,
      //Тип журналирования событий
      "Journal": "Both"
    },

    //Блок общих настроек службы


    "BaseService": {
      //Список разрешенных криптосредств
      "AllowedCsp": [],
      //Включение использования квалифицированного режима
      "IsUseQualify": false,
      //Включение использования только квалифицированного режима
      "IsOnlyQualified": false,
      //Максимально допустимый размер документа, отправляемого на проверку байт.
      "MaxRequestSizeBytes": 20971520,
      //Включение разрешения принудительного скачивания списка отзыва
      "InhibitCashingCrl": false
    },


    //Блок продления квитанций и обновления трастед листа
    "Update": {
      //Путь к файлу трастед листа, сохраненного ранее
      "QualifyFilePath": "tsl.xml",
      //Адрес для скачивания промежуточных сертификатов Мин.Связи
      "QualifyFileUrl": "https://e-trust.gosuslugi.ru/CA/DownloadTSL?schemaVersion=0",
      //Сохранять или нет по заданному пути после скачивания
      //Оставшийся период действия в днях до которого квитанции не будет продлеваться
      "UpdateOffset": 90,
      //Период обновления сервиса обновления в часах
      "UpdatePeriod": 24,
      //Используемый адрес службы штампов времени для обновления квитанций
      "UpdateTsp": "http://testca.gaz-is.ru/tsp/tsp2012.srf",
      //Сохранять или нет по заданному пути после скачивания
      "IsSaveTsl": true
    },

    //Набор параметров для настройки работы со службой штампа времени
```

```
    "Tsp": {
      //Список поддерживаемых алгоритмов хэширования
      "AllowedHashAlgs": [ "1.2.643.2.2.9", "1.2.643.7.1.1.2.2", "1.2.643.7.1.1.2.3",
"1.3.14.3.2.26" ],
      //Точность времени (мс)
      "Accuracy": 0,
      //Включение разрешения работы службы штампов времени
      "IsUseTsp": true
    },

    //Блок настроек маршрутов транграничности

    "RouteGroup": {
      "Route": {
        //Список разрешенных для использования отечественных алгоритмов
        "RU": [ "1.2.643.2.2.19", "1.2.643.7.1.1.1.1", "1.2.643.7.1.1.1.2" ],
        //Список разрешенных для использования европейских алгоритмов
        "EU": [ "1.2.840.113549.1.1.1", "1.2.840.113549.1.1.2", "1.2.840.113549.1.1.3",
"1.2.840.113549.1.1.4", "1.2.840.113549.1.1.5" ],
        //Список разрешенных для использования казахских алгоритмов
        "KZ": [ "1.2.398.3.10.1.1.1.2", "1.2.398.3.10.1.3.1", "1.2.398.3.10.1.1.1.1" ],
        //Список разрешенных для использования казахских алгоритмов
        "RB": [ "1.2.112.0.2.0.34.101.45.12", "1.2.112.0.2.0.34.101.45.2.1" ]
      }
    },

    /*Набор параметров для настройки активации приложения*/

    "Activation": {
      //Адрес сервера активации
      "Url": "https://license.gaz-is.ru/",
      //Адрес для проведения офлайн-активации
      "UrlOffline": "https://license.gaz-is.ru/offlineActivate"
    },

    //Набор параметров для настройки работы двухфакторной аутентификации


    "Mail": {
      //Адрес Smtp сервера
      "SmtpHost": null,
      //Порт Smtp сервера
      "SmtpPort": 587,
      //Имя пользователя
      "SmtpUser": null,
      //Пароль для подключения к серверу
      "SmtpPassword": null,
      //Использовать TLS при соединении
      "IsUseTls": true,
      // Адрес отправителя
      "From": null
    },

    //Набор параметров для настройки работы со службой syslog


    "Syslog": {
```

```
      //Адрес службы syslog
      "Host": "localhost",
      //Порт для подключения к службе syslog
      "Port": 514

    },

    //Блок настроек для проверки разграничений по полномочиям


    "Policy": {
      //Включение использования проверки полномочий
      "IsUsePolicy": false,
      "PolicyName": {
        //Наименование группы и OID список
        "Директор": [ "1.3.6.1.5.5.7.3.55", "1.3.6.1.5.5.7.3.56" ],
        //Наименование группы и OID список
        "Администратор": [ "1.2.643.2.2.34.7" ],
        //Наименование группы и OID список
        "Сотрудник с правом подписи": [ "1.3.6.1.5.5.7.3.11" ]
      }
    }


  }
}
```

Конфигурационный файл службы автопролонгации квитанций «appsettings.json»

```
{

  //Блок настроек логирования службы ДТС
  "Logging": {
    "LogLevel": {
      // Лог службы ДТС.
      "Default": "Debug",
      // Лог райнтайма
      "Microsoft": "Error"
    },
    //Набор параметров для настройки ведения лога

    "FileLog": {
      //Вести файловый лог
      "IsEnFileLog": true,
      //Название файла лога
      "Path": "update.txt",
      //Возможность добавления
      "Append": "True",
      //Максимальный размер файла лога байт
      "FileSizeLimitBytes": 0,
      //Ротация файлов лога по достижению максимального размера
      "MaxRollingFiles": 0
    }
  },
  //Список разрешенных для подключения хостов
  "AllowedHosts": "*",
  "ConnectionStrings": {
```

```
    //Настройки подключения к базе данных
    "DefaultConnection":
"Host=localhost;Port=5433;Database=dvcs;Username=postgres;Password=postgres"
  },
  "DvcsConfig": {
    //Набор параметров для проверки службы штампов времени
    "Dvcs": {
    //Тип журналирования событий
      "Journal": "Both"
    },

    //Блок продления квитанций и обновления трастед листа
    "Update": {
      //Путь к файлу трастед листа сохраненного ранее
      "QualifyFilePath": "tsl.xml",
      //Адрес для скачивания промежуточных сертификатов Мин.Связи
      "QualifyFileUrl": "https://e-trust.gosuslugi.ru/CA/DownloadTSL?schemaVersion=0",
      //Оставшийся период действия в днях до которого квитанции не будет продлеваться
      "UpdateOffset": 90,
      //Период обновления сервиса обновления в часах
      "UpdatePeriod": 24,
      //Используемый адрес службы штампов времени для обновления квитанций
      "UpdateTsp": "http://testca.gaz-is.ru/tsp/tsp2012.srf",
      //Сохранять или нет по заданному пути после скачивания
      "IsSaveTsl": true
    },

    "Syslog": {
      //Адрес службы syslog
      "Host": "localhost",
      //Порт для подключения к службе syslog
      "Port": 514

    }
  }
}
```

Перечень сокращений

API	–	Application Programming Interface
DNS	–	Domain Name System
IIS	–	Internet Information Services
IP	–	Internet Protocol
CMS	–	Cryptographic Message Syntax
CSP	–	Cryptographic Service Provider
DVC	–	Data Validation and Certification
DVCS	–	Data Validation and Certification Server
OID	–	Object Identifier
SSL	–	
TSP	–	Time-Stamp Protocol
VPKC	–	Validation of Public Key Certificates
VSD	–	Validation of digitally Signed Document
АРМ	–	Автоматизированное Рабочее Место
БД	–	База Данных
ДТС	–	Доверенная Третья Сторона
ОС	–	Операционная Система
ПК	–	Программный комплекс
СКЗИ	–	Средство Криптографической Защиты Информации
УФО	–	Уполномоченный Федеральный Орган
УЦ	–	Удостоверяющий Центр
ЭП	–	Электронная Подпись