Инструкция пользователю
по настройке персонального компьютера для работы с электронной подписью УЦ ФНС России

Москва
2024

Содержание

Вход в личный кабинет УЦ ФНС России

Для работы с удостоверяющим центром ФНС России необходимо перейти по следующей ссылке в браузере вашего персонального компьютера: https://ucfns.tax.gov.ru/manual

Откроется следующее окно, в котором необходимо пройти процедуру аутентификации и авторизации для доступа к ресурсу, а именно ввести персональные логин и пароль.

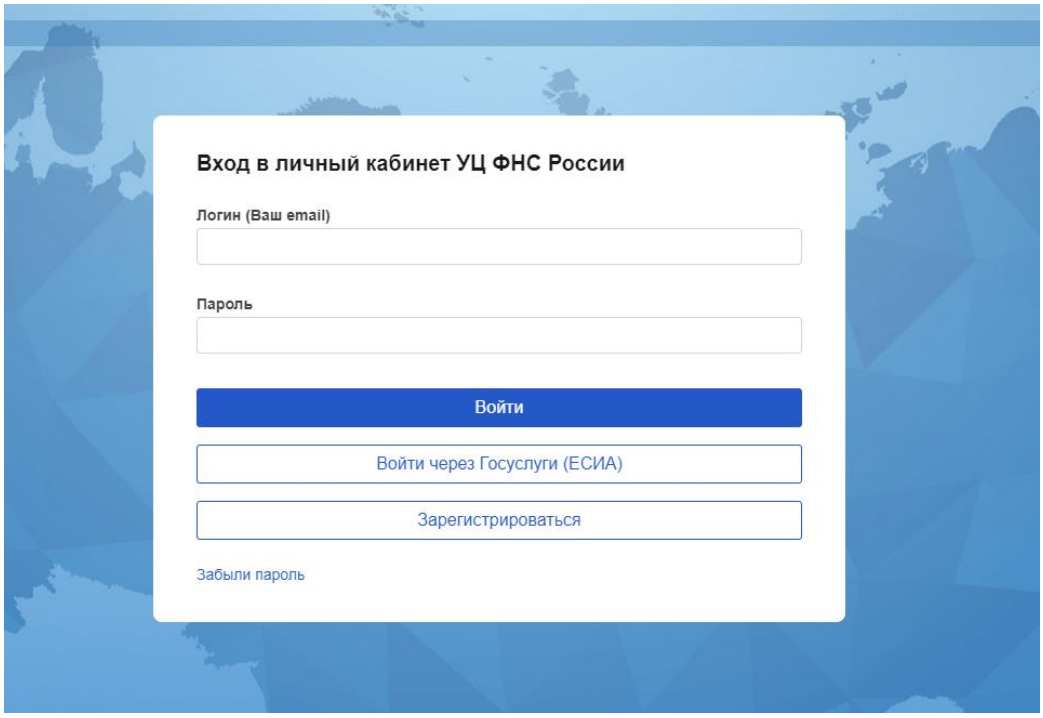

Рисунок 1 – Окно аутентификации и авторизации

Также в случае установленной неподдерживаемой версии браузера на экране появится следующее информационное сообщение.

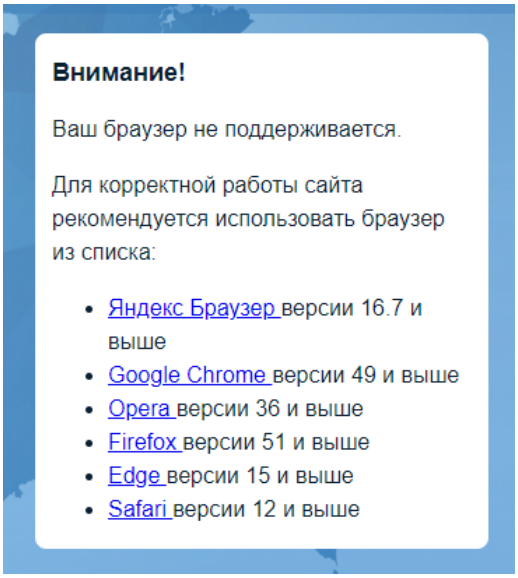

Рисунок 2 – Информационное сообщение

В данном случае рекомендуется обновить или установить подходящую версию браузера из представленных в информационном сообщении.

После успешного прохождения процедур аутентификации и авторизации в браузере откроется следующее окно.

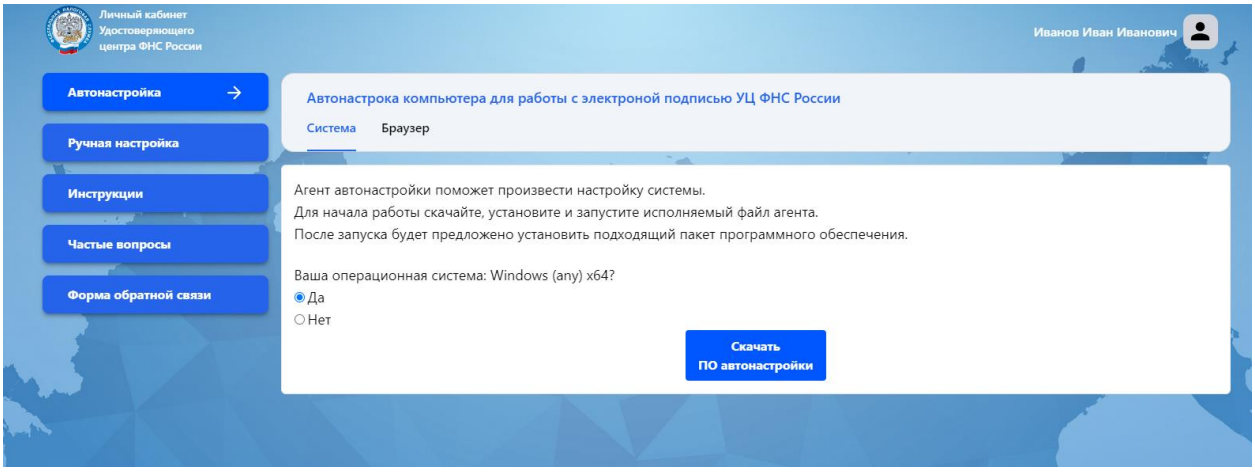

Рисунок 3 – Окно автонастройки

Далее для работы с электронной подписью УЦ ФНС России требуется установить дополнительное программное обеспечение на компьютер.

Возможны два варианта настройки компьютера для работы с электронной подписью УЦ ФНС России.

Автонастройка компьютера для работы с электронной подписью УЦ ФНС России

Для автонастройки компьютера необходимо перейти в вкладку «Автонастройка».

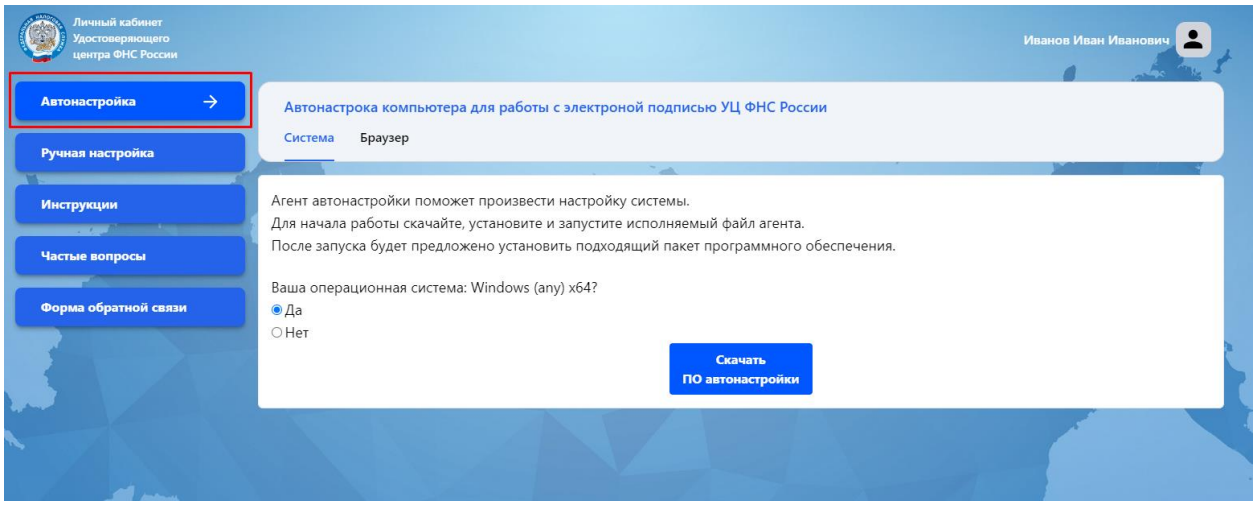

Рисунок 4 – Вкладка «Автонастройка»

Затем необходимо указать операционную систему вашего компьютера. В случае, если на компьютере установлена операционная система Windows x64 указывается вариант «Да». Далее необходимо скачать файл автонастройки, нажав на кнопку «Скачать ПО автонастройки».

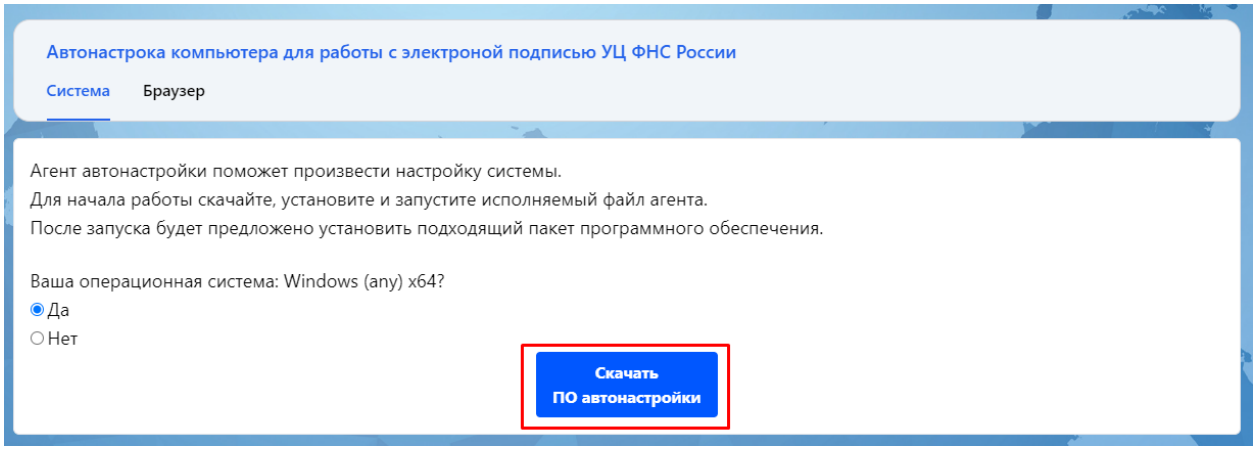

Рисунок 5 – Выбор операционной системы компьютера

Если на компьютере установлена другая операционная система указывается вариант «Нет» и появляется возможность выбора подходящего установщика. Скачивание установщика начнется после нажатия кнопки .

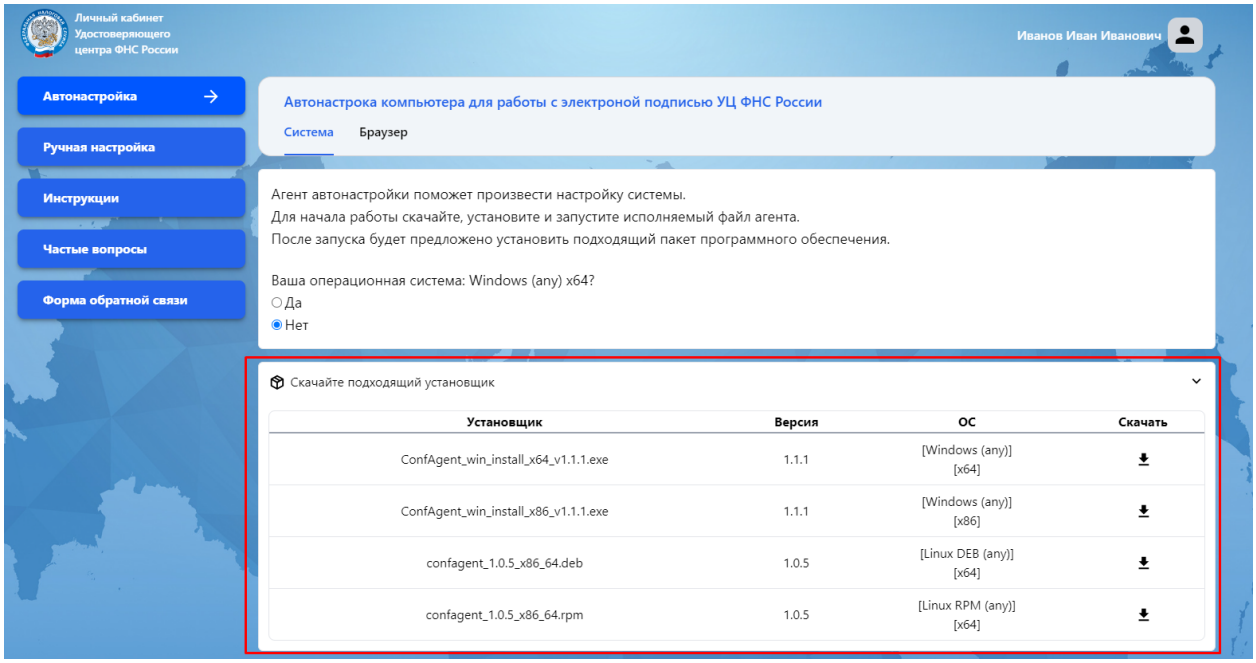

Рисунок 6 – Выбор операционной системы компьютера

После скачивания необходимо открыть файл установщика. Появится окно автонастройки. После нажатия «Установить» начнется процесс установки Агента автонастройки.

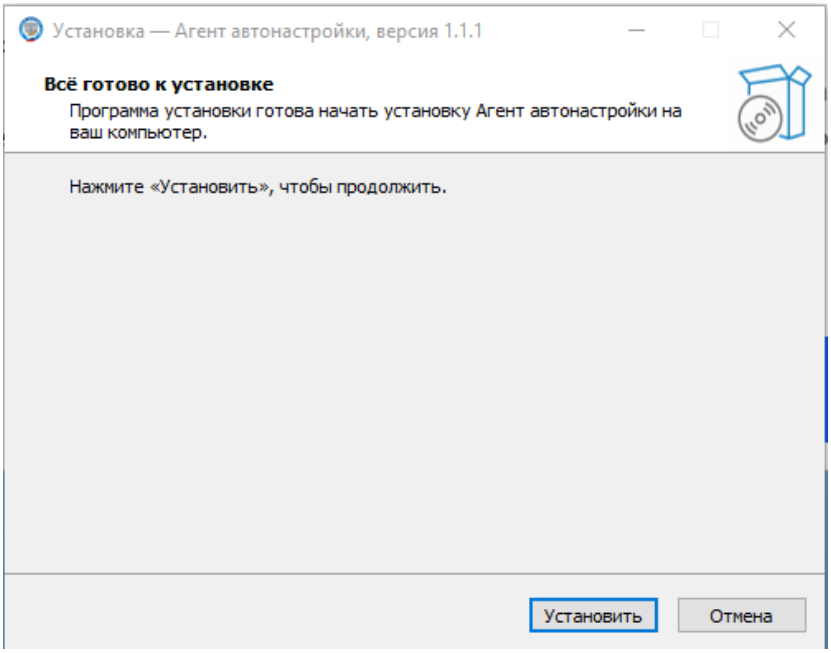

Рисунок 7 – Окно установки Агента автонастройки

После завершения установки Агента автонастройки необходимо отметить галочкой пункт «Запустить ConfAgent_win.exe» (или другое название файла, если используется иная операционная система) и нажать кнопку «Завершить».

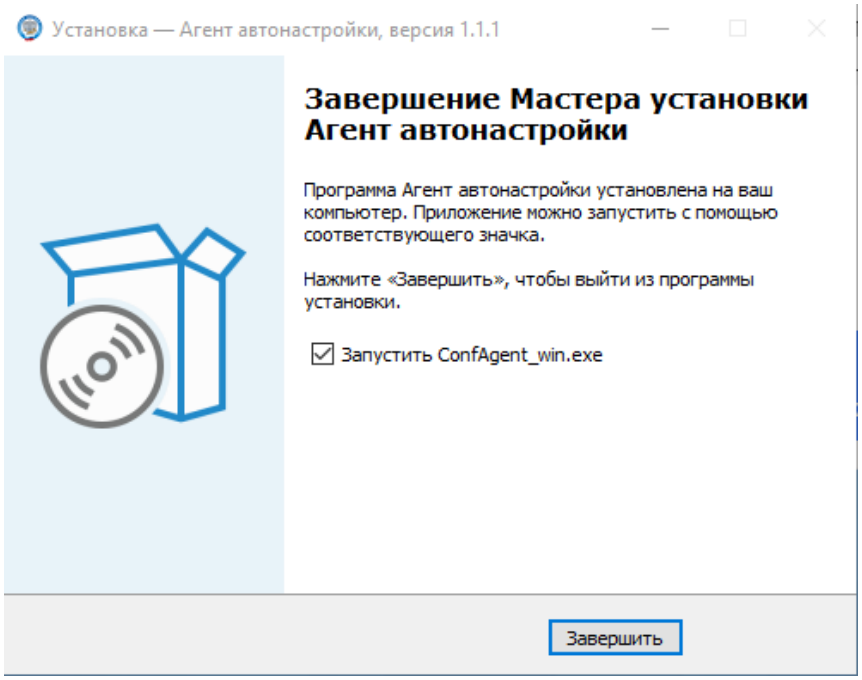

Рисунок 8 – Окно завершения установки Агента автонастройки

Затем на компьютере откроется окно Агента автонастройки, где будет отображаться информации об используемой версии браузера, операционной системы компьютера, программных пакетах СКЗИ, корневых сертификатах и промежуточных сертификатах. Необходимо дождаться успешного соединения с Web-сервисом настройки (Рисунок 9).

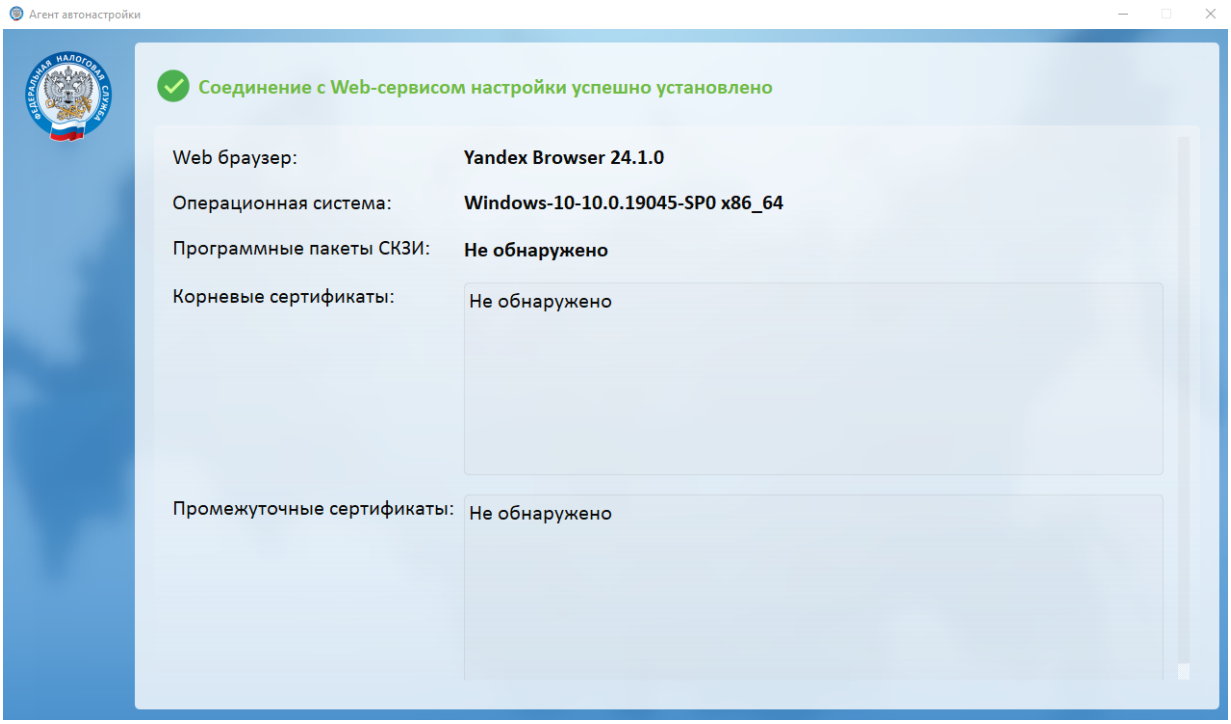

Рисунок 9 – Окно Агента автонастройки

Далее необходимо вернуться в браузер во вкладку «Автонастройка». После запуска Агента автонастройки появится сообщение «Подключено к агенту автонастройки» (Рисунок 10).

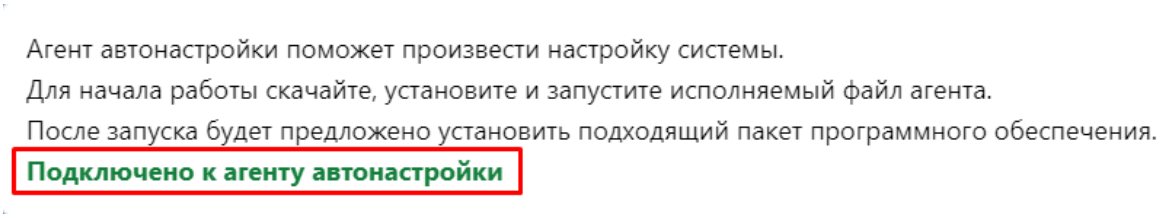

Рисунок 10 – Сообщение «Подключено к агенту автонастройки» в браузере

Также появится доступ к статусу установки необходимого программного обеспечения и возможность проведения повторного сканирования, выбору криптопровайдера для установки, установке сертификатов и драйверов устройств (Рисунок 11).

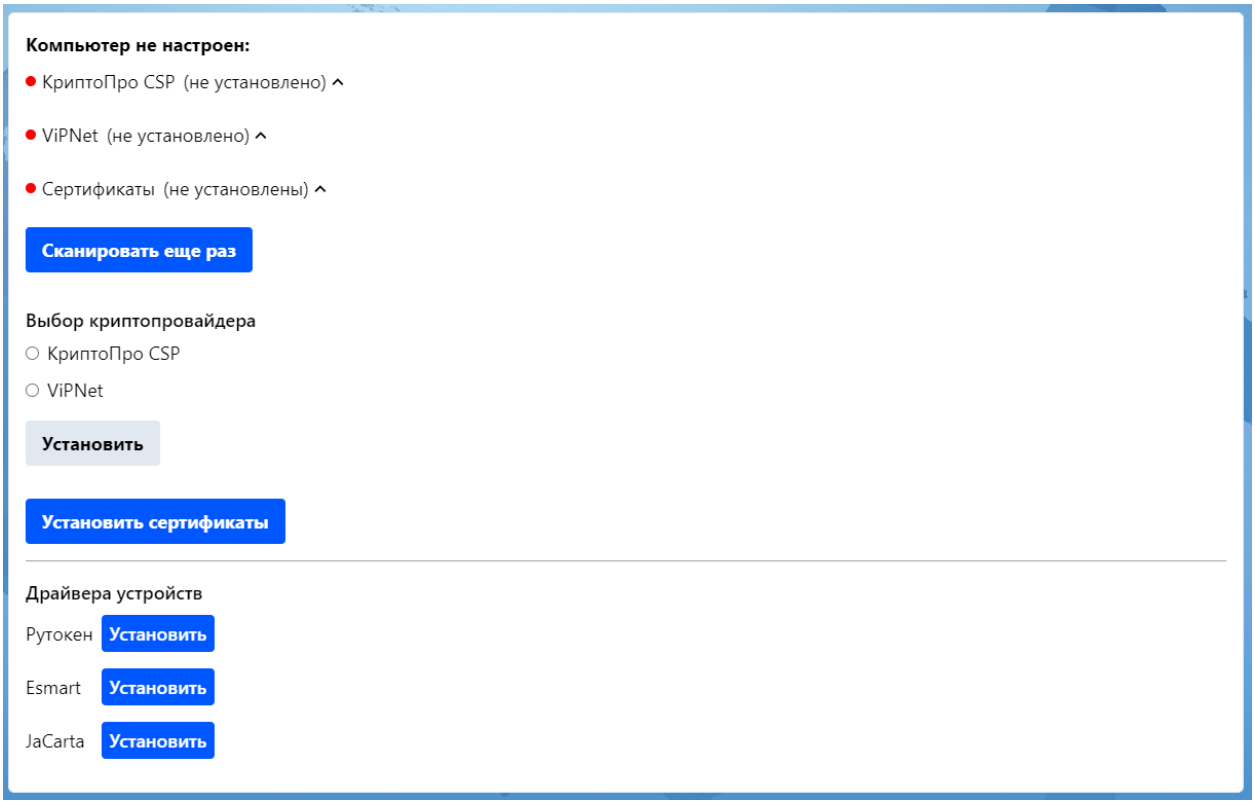

Рисунок 11 – Окно установки программного обеспечения в браузере

Выбрав криптопровайдера, необходимо нажать кнопку «Установить», после чего начнется установка требуемого программного обеспечения и соответствующее сообщение о начале установки появится в браузере (Рисунок 12).

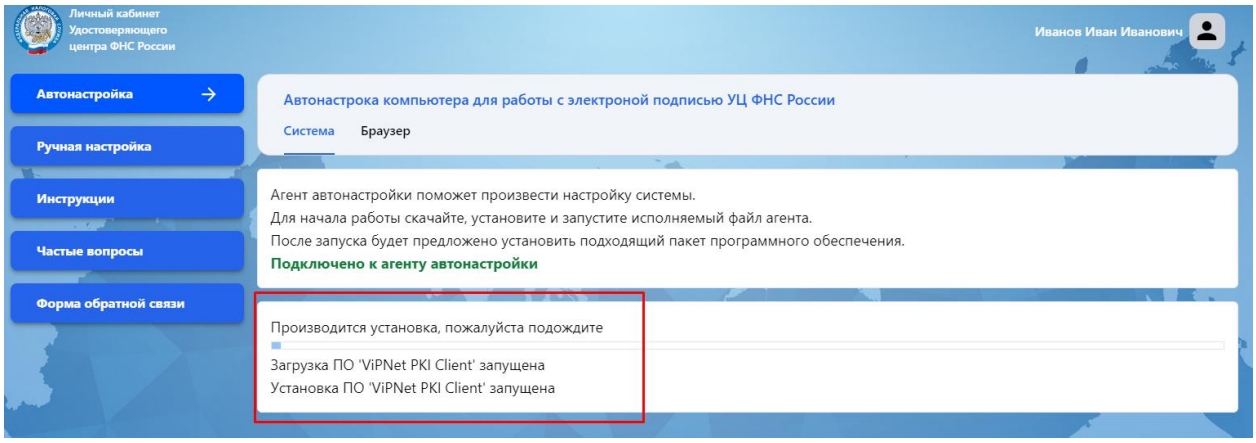

Рисунок 12 – Процесс установки ПО

Вместе с тем на компьютере откроется окно установки выбранного криптопровайдера.

Установка VipNet PKI Client

После того, как на компьютере появится окно установки VipNet PKI Client необходимо принять условия лицензионного соглашения и нажать «Далее».

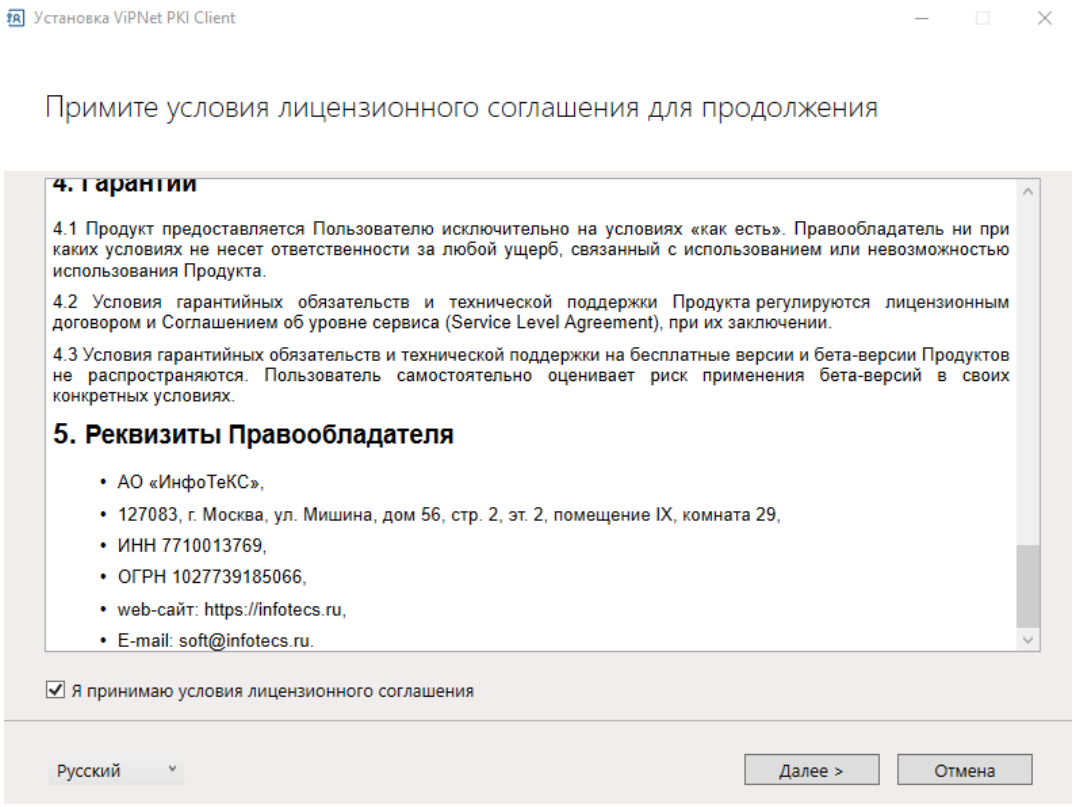

Рисунок 13 – Окно установки VipNet PKI Client

На следующем этапе требуется выбрать путь установки программного обеспечения (Рисунок 14) и нажать «Установить».

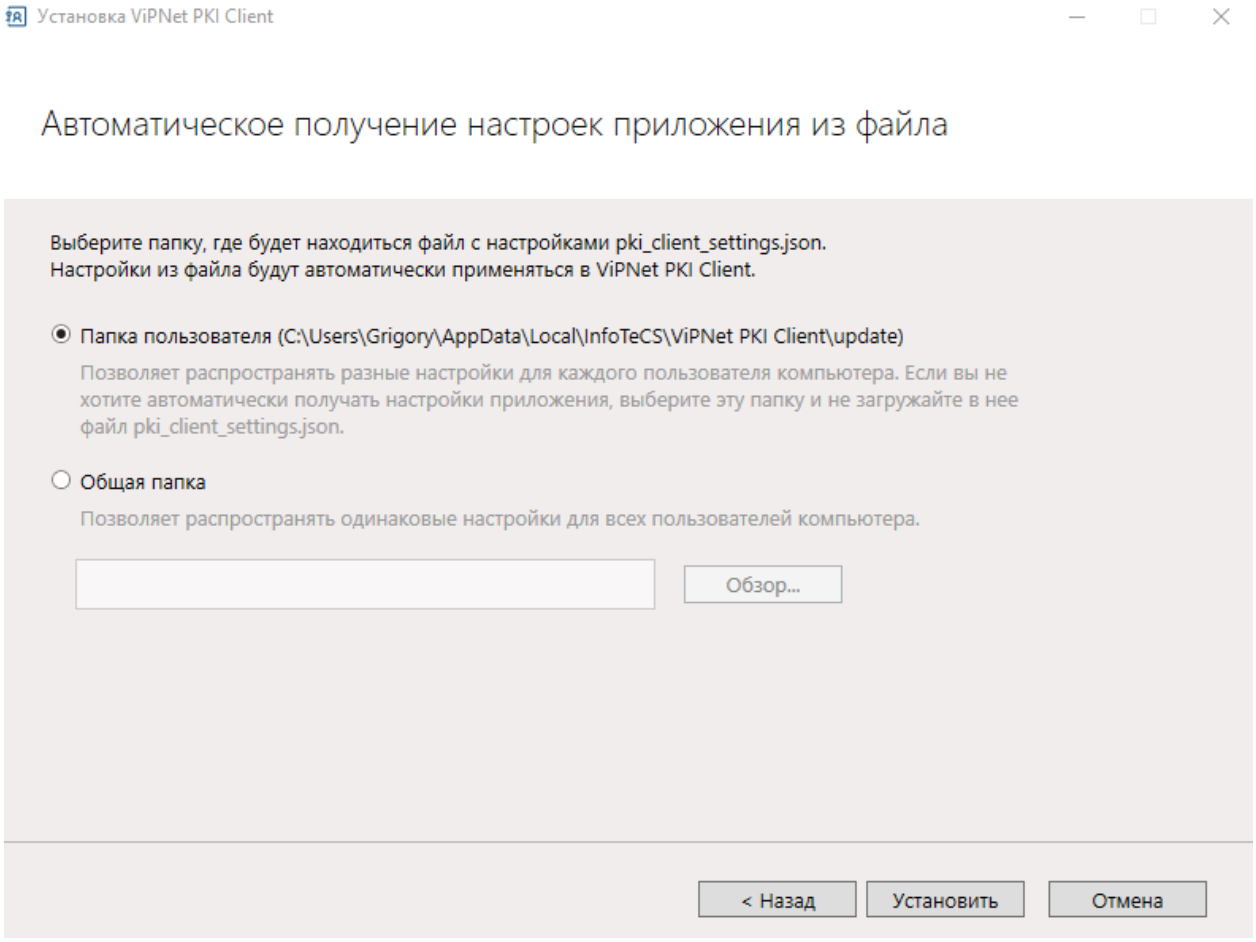

Рисунок 14 – Выбор места установки VipNet PKI Client

По завершению установки необходимо перезагрузить компьютер.

После перезагрузки необходимо запустить Агент автонастройки, а также в браузере перейти на вкладку «Автонастройка» для установки необходимых сертификатов, нажав «Установить сертификаты» (Рисунок 15).

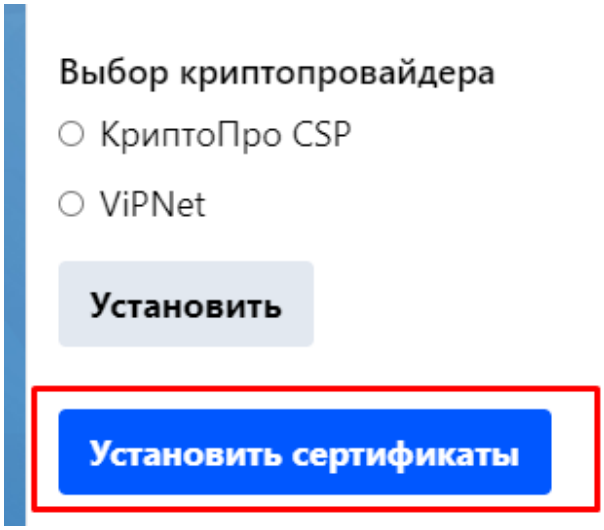

Рисунок 15 – Процесс установки сертификатов

После данных действий начнется установка сертификатов, статус которой будет отображаться в Агенте автонастройки. В результате в браузере появится информация об установленных сертификатах (Рисунок 16).

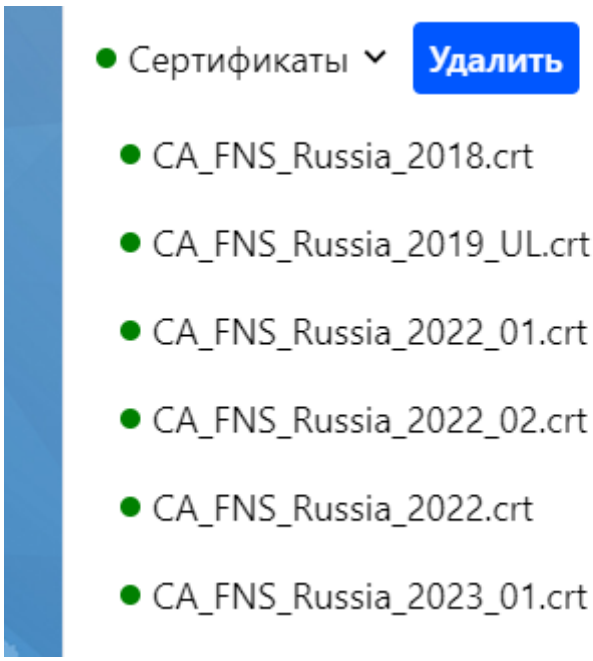

Рисунок 16 – Информационное окно об установленных сертификатах

После установки всех требуемых сертификатов необходимо открыть установленную ранее программу «Настройки PKI Client» и перейти к активации лицензии. Вы можете активировать лицензию с использованием файла лицензии или через ViPNet TLS Gateway.

При использовании файла лицензии:

1. Загрузите лицензию в ViPNet PKI Client.

2. Если лицензия не была активирована сразу (например, из-за отсутствия интернет-соединения), активируйте ее вручную.

Загрузка лицензии

1. Перейдите в настройки ViPNet PKI Client.
2. В разделе Лицензия нажмите «Выбрать способ > С использованием файла лицензии».
3. Выберите файл лицензии и в окне Загрузка лицензии нажмите «Загрузить».

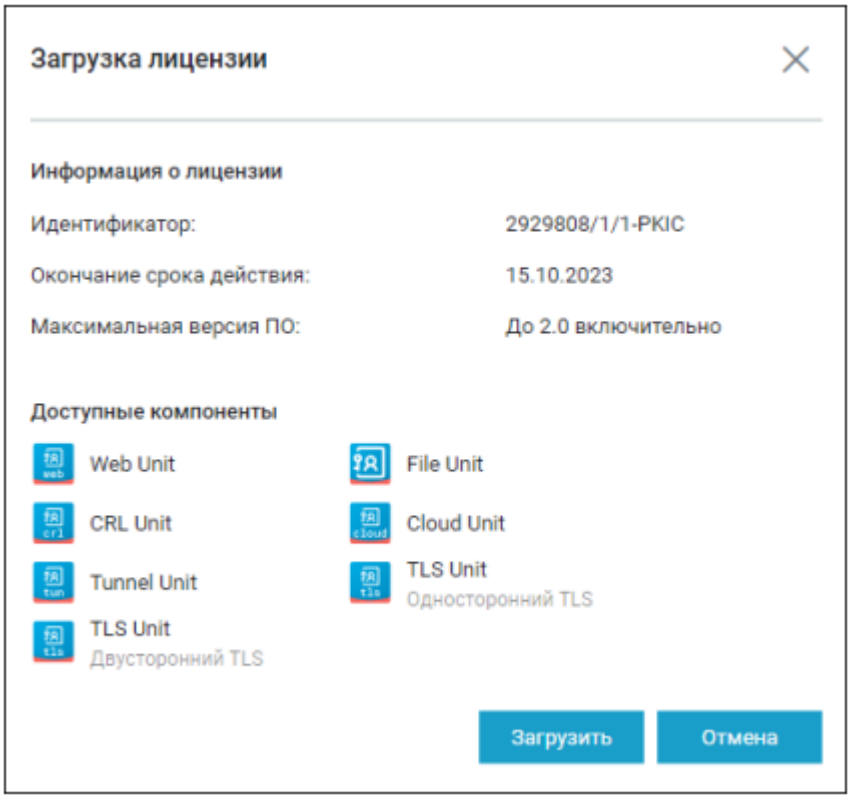

Рисунок 17 – Просмотри информации о лицензии

Если связь с сервером регистрации ИнфоТеКС установлена, лицензия будет активирована автоматически. Если лицензия не была активирована, активируйте ее вручную.

Активация лицензии с использованием файла

1. Перейдите в настройки ViPNet PKI Client.
2. В разделе Лицензия нажмите «Активировать».

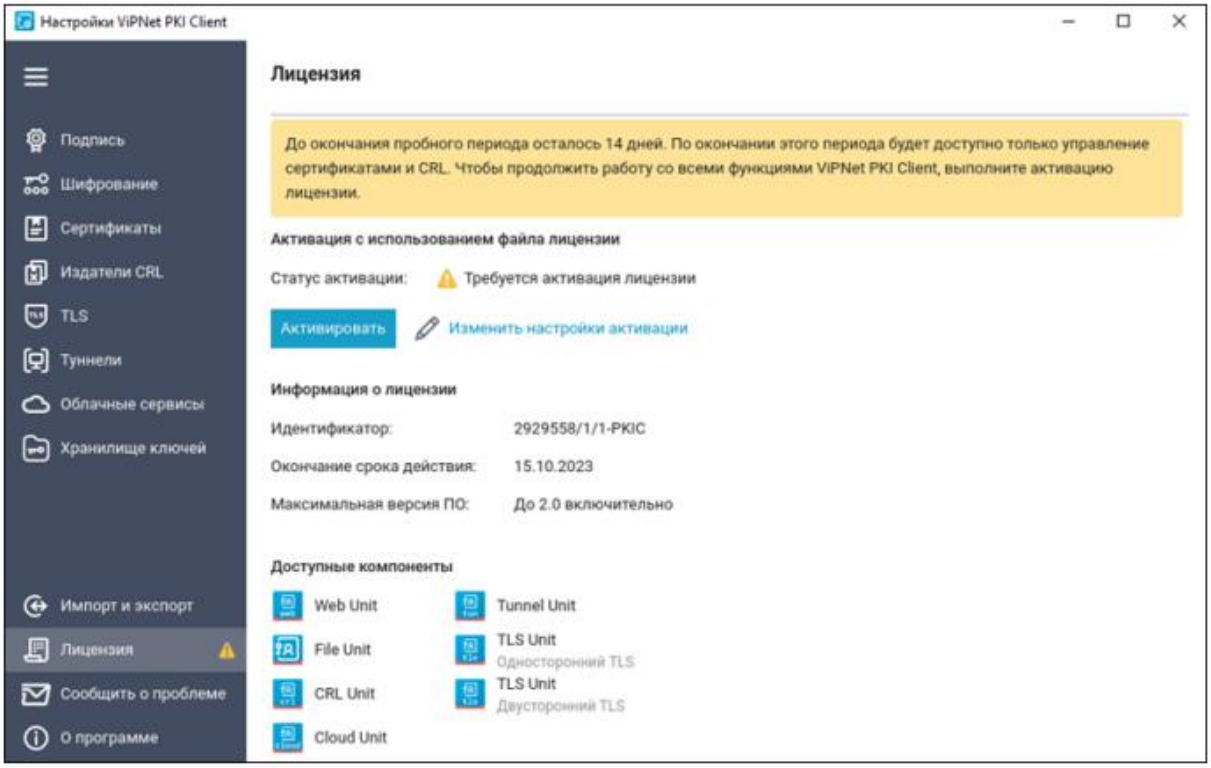

Рисунок 18 – Просмотр информации о лицензии

3. Нажмите «Сохранить запрос».
4. Укажите имя и путь для сохранения файла запроса.
5. Отправьте файл запроса на электронную почту reg@infotecs.ru. Тема и оформление письма могут быть любыми.
6. Дождитесь ответного письма, в котором будут указаны данные для активации.
7. В поле «Код регистрации, полученный в ответном письме» введите регистрационный код и нажмите «Активировать».

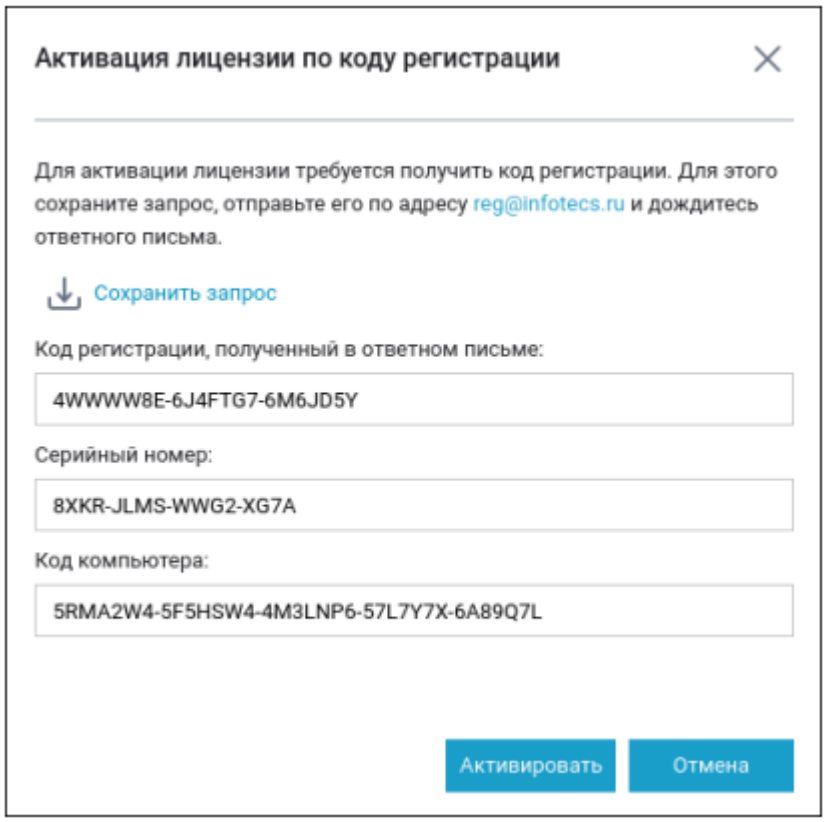

Рисунок 19 - Ввод данных для активации ViPNet PKI Client

Активация лицензии через ViPNet TLS Gateway

Перед активацией лицензии:

1. Получите у администратора ViPNet TLS Gateway:

   - Адрес и порт для лицензирования.
   - Цепочку сертификатов транспортного сертификата ViPNet TLS Gateway, используемого для подключения к каналу лицензирования.

2. Установите в ViPNet PKI Client на компьютере пользователя:

   - Личный сертификат с ключом ЭП для подключения к ViPNet TLS Gateway, доверие к которому установлено в ViPNet TLS Gateway.

   Сертификат должен соответствовать требованиям:

   - сертификат действителен;
   - ЭП сертификата верна;

- сертификат в поле Расширенное использование ключа содержит назначение Проверка подлинности клиента;
- сертификат в поле Использование ключа содержит назначение Цифровая подпись и (или) Согласование ключей.

Корневой сертификат УЦ, в котором издан сертификат пользователя для подключения к ViPNet TLS Gateway, а также все сертификаты цепочки и соответствующие CRL.

Цепочку сертификатов транспортного сертификата ViPNet TLS Gateway, используемого для подключения к каналу лицензирования.

Для активации лицензии на компьютере пользователя:

1. Перейдите в настройки ViPNet PKI Client.
2. В разделе «Лицензия» нажмите Выбрать способ > Через ViPNet TLS Gateway.
3. Введите полученные адрес и порт.
4. Выберите установленный сертификат для подключения.

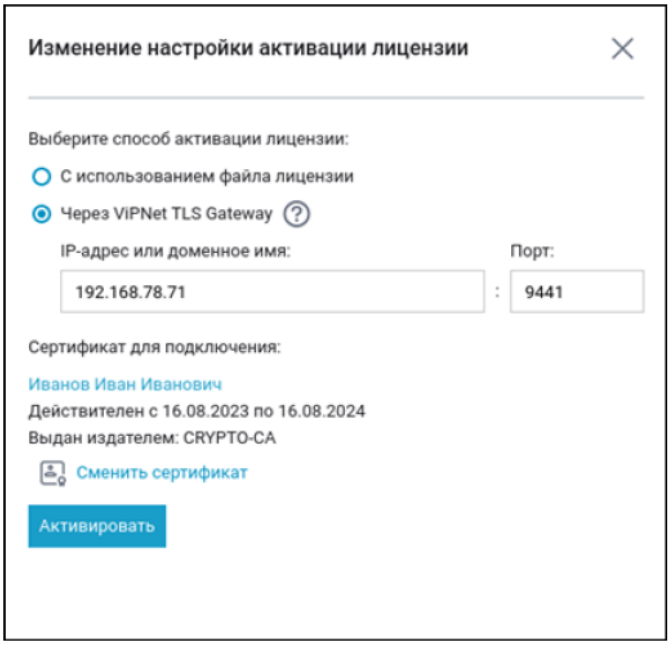

Рисунок 20 - Активация через ViPNet TLS Gateway

5. Нажмите Активировать.
6. В зависимости от места хранения контейнера ключей:
   - Хранилище ViPNet PKI Client — введите пароль хранилища ViPNet PKI Client и нажмите Продолжить.

- Токен — введите ПИН.

7. ViPNet PKI Client отправит запрос на активацию на ViPNet TLS Gateway. После успешной обработки запроса ViPNet PKI Client перейдет в состояние Лицензия активирована.
8. В случае неуспешной активации ознакомьтесь с причиной и следуйте указаниям.

Подписание файла с помощью ViPNet PKI Client

1. Запустите File Unit и выполните одно из действий:
   - Перетащите файлы в главное окно File Unit.
   - Нажмите «Выбрать файлы» и выберите один или несколько файлов.
2. Справа выберите «Подписать сертификатом». Станут доступны настройки параметров ЭП.

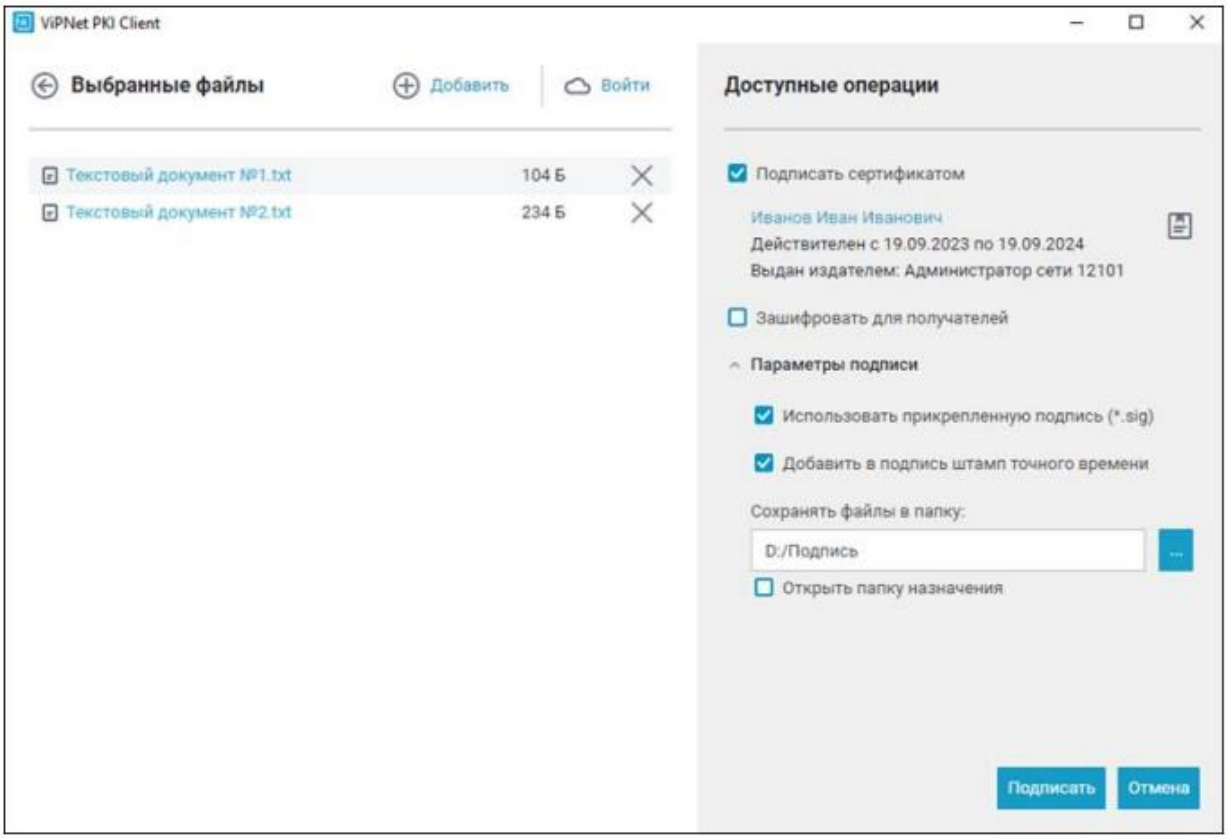

Рисунок 21 - Подписание файла

3. Если необходимо, выберите другой сертификат с помощью, включите зашифрование и измените параметры ЭП.
4. Нажмите «Подписать».
5. В зависимости от места хранения контейнера ключей:
   - Хранилище ViPNet PKI Client — введите пароль хранилища ViPNet PKI Client и нажмите «Продолжить».
   - Токен — введите ПИН.

   В выбранную папку будут помещены файлы:

   - *.sig, если вы выбрали прикрепленную ЭП;
   - *.detached.sig, если вы выбрали откреплённую ЭП.

Установка криптопровайдера КриптоПро CSP

После того, как на компьютере появится окно установки КриптоПро CSP необходимо принять условия лицензионного соглашения и нажать «Далее» (Рисунок 22).

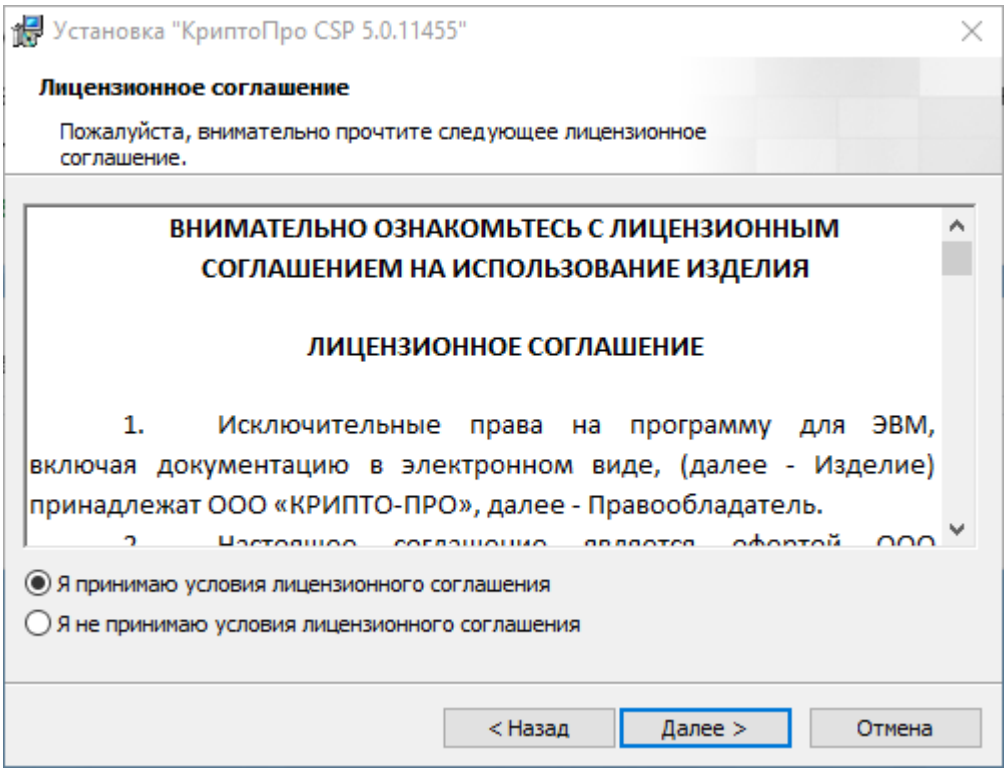

Рисунок 22 – Лицензионное соглашение

Затем необходимо ввести имя пользователя и наименование организации (Рисунок 23). Серийный номер вводить **не требуется,** так как лицензия будет автоматически применена на все время действия сертификата со встроенной лицензией. Далее необходимо выбрать вид установки «Обычная» (Рисунок 24) и после этого нажать «Установить».

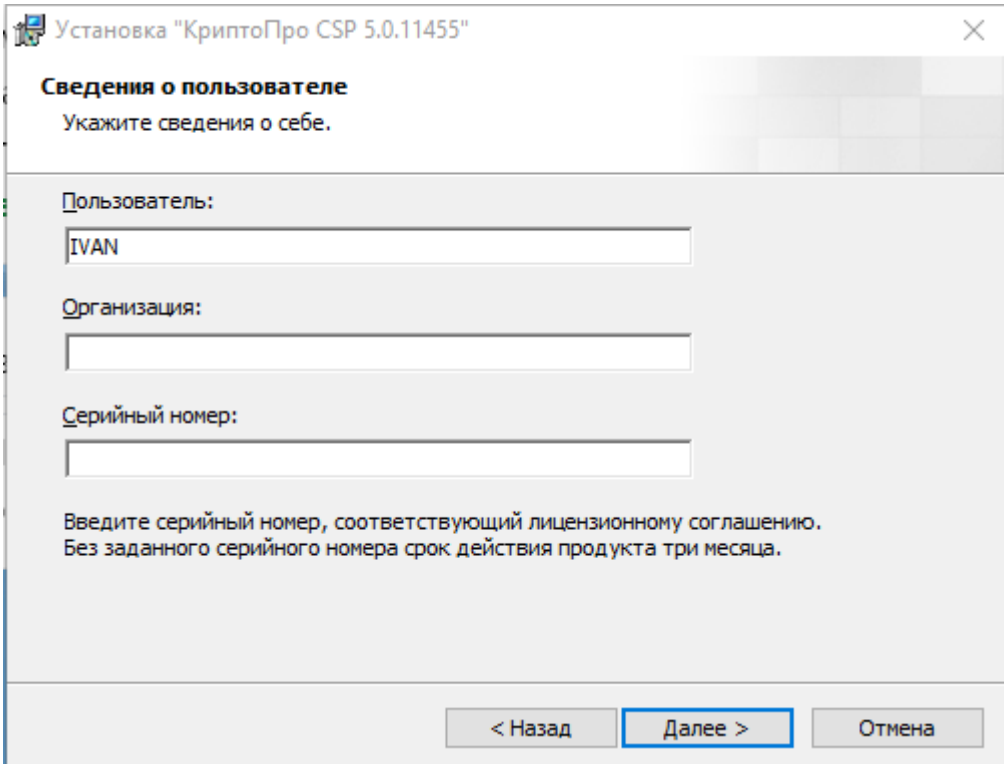

Рисунок 23 – Сведения о пользователе

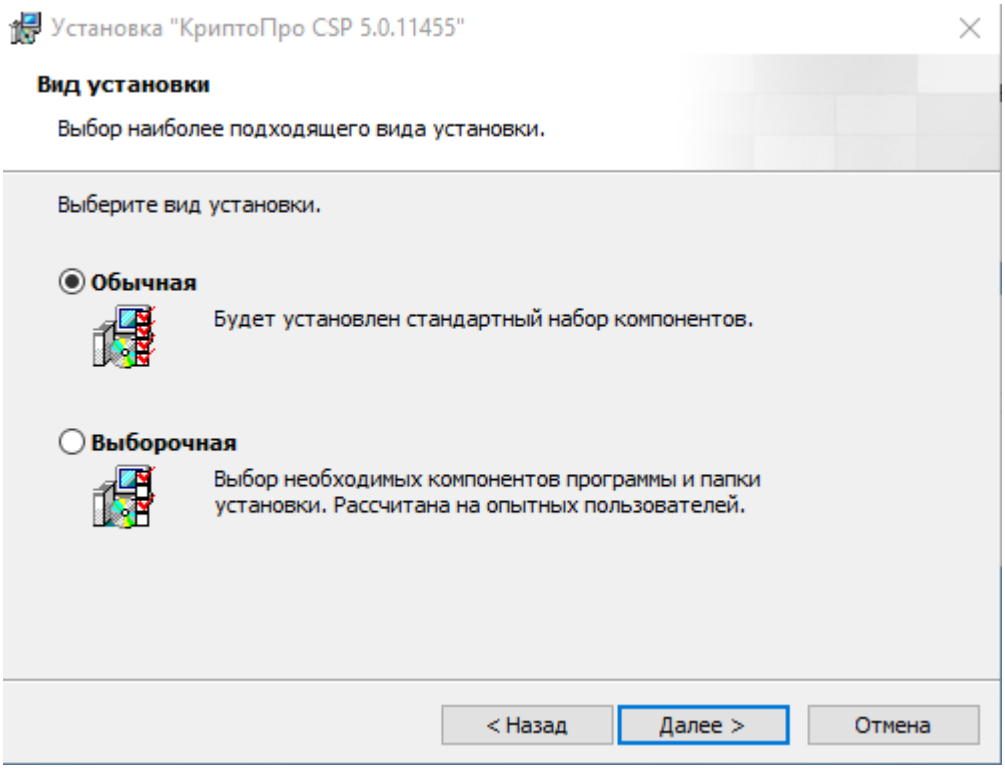

Рисунок 24 – Выбор вида установки

Далее начнется установка КриптоПро Browser plug-in (Рисунок 25). По завершению установки необходимо перезагрузить компьютер.

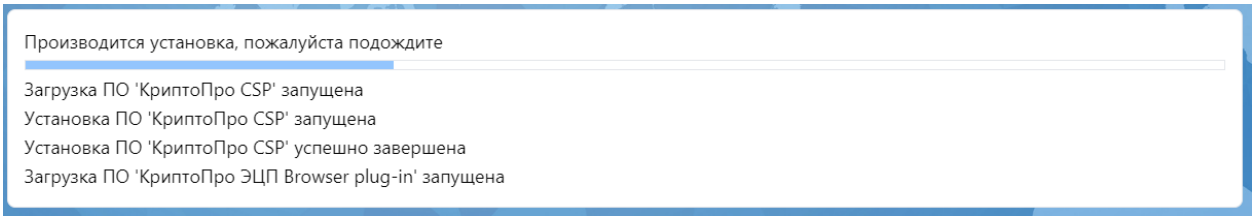

Рисунок 25 – Установка КриптоПро Browser plug-in

После перезагрузки необходимо запустить Агент автонастройки, а также в браузере перейти на вкладку «Автонастройка» для установки необходимых сертификатов, нажав «Установить сертификаты» (Рисунок 26).

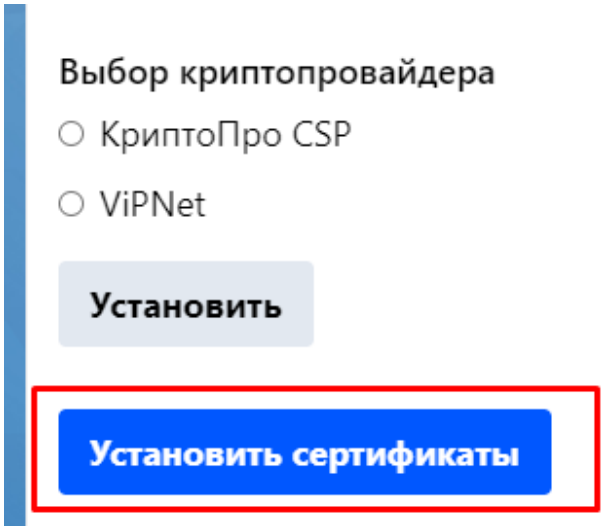

Рисунок 26 – Установка сертификатов

После данных действий начнется установка сертификатов, статус которой будет отображаться в Агенте автонастройки. В результате в браузере появится информация об установленных сертификатах (Рисунок 27).

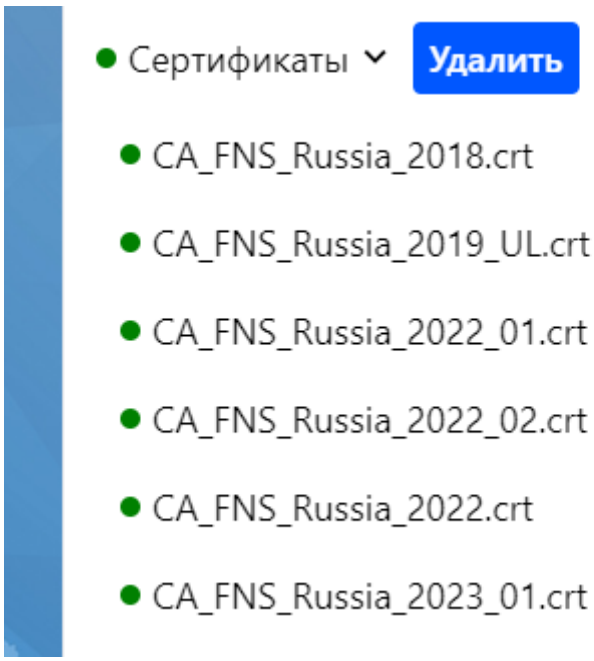

Рисунок 27 – Информация об установленных сертификатах

Подписание файла с помощью КриптоПро CSP

Далее необходимо открыть установившееся программное обеспечение «Инструменты КриптоПро» и выбрать раздел «Создание подписи», после чего выбрать файл для подписи, сертификат из списка и нажать «Подписать».

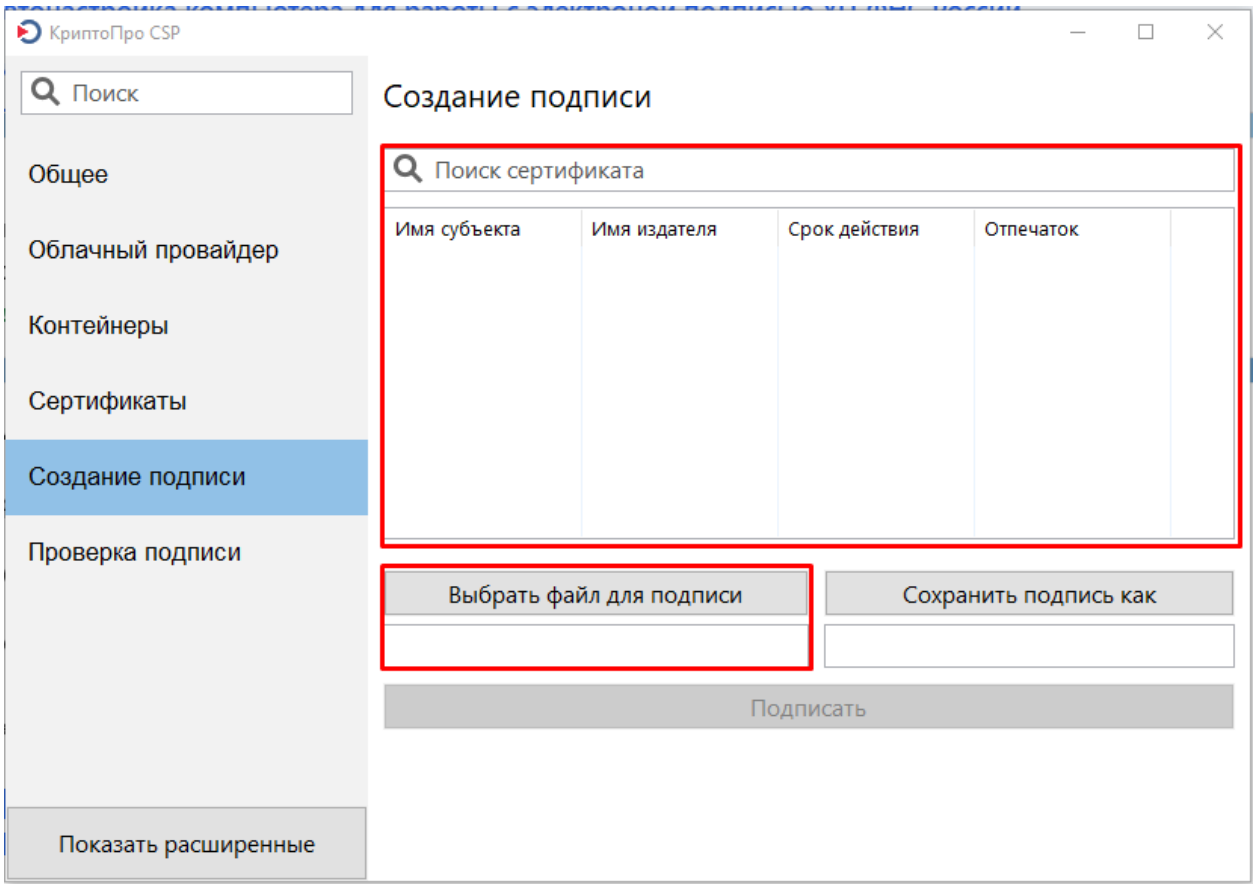

Рисунок 28 – Выбор файла для подписи и сертификата