Инструкция по настройке автоматизированного рабочего места для работы в информационной системе ФГИС Росаккредитации

Листов 25

ИнфоТеКС Интернет Траст
2017

Оглавление

I. Введение

✓ Документ предназначен для пользователей, осуществляющих самостоятельную установку средства криптографической защиты информации (СКЗИ) ViPNet CSP и настройку автоматизированного рабочего места для работы с электронной подписью (ЭП) на портале ФГИС Росаккредитация.

✓ В удостоверяющем центре ОАО "ИнфоТеКС Интернет Траст" (далее – УЦ ИИТ) срок действия ключей и сертификата ЭП установлен равным 1 году. При необходимости произвести плановую (скорое истечение срока действия ЭП) или внеплановую (изменение учетных данных владельца ЭП, потеря доступа к ключевому носителю, потеря ключевого носителя и т.д.) смену ЭП необходимо повторно прибыть в УЦ «ИИТ» по согласованию с менеджером «ИИТ».

✓ Для правильной работы СКЗИ ViPNet CSP необходимо выполнить все пункты данного руководства в указанной последовательности.

✓ Для корректной работы с электронной подписью (ЭП) на различных интернет-порталах (электронные торговые площадки, порталы контролирующих органов, различные федеральные информационные ресурсы и т.д.) в качестве интернет-обозревателя рекомендуется использовать ***Microsoft Internet Explorer 11.0 и выше***, либо ***Mozilla Firefox 51 или ESR***.

✓ **Необходимо обращать особое внимание на примечания помеченные знаком .**

Внимание! Вид окон может отличаться в зависимости от используемой операционной системы. В примерах использовалась операционная система Windows 7.

Всю необходимую документацию по услугам нашей компании вы можете загрузить на нашем сайте www.iitrust.ru раздел «Поддержка», кнопка «Пользовательская документация»

II. Состав программного обеспечения АРМ

Для настройки АРМ пользователя необходим следующий состав программного обеспечения:

- ✓ Квалифицированная электронная подпись на защищённом носителе (eToken).
- ✓ Драйвер для работы с соответствующим ключевым носителем.
- ✓ ПО ViPNet CSP[1].
- ✓ ПО ViPNet CryptoFile[2].
- ✓ ПО ViPNet Client и файл первичной инициализации абонентского пункта (*.dst) в сети «2936 ФСА»[3].
- ✓ Специальное ПО (далее – плагин), обеспечивающее работу интернет-обозревателя с Единой системой идентификации и аутентификации (далее – ЕСИА).

III. Получение и установка ViPNet CSP

1. Для получения ViPNet CSP необходимо перейти на официальный сайт разработчика:
   - Если Вы работаете на операционной системе **Windows**: **7/8/8.1/Server 2008 / Server 2008 R2** (только x64)/**Server 2012** (только x64)/ **Server 2012R2** (только x64)/. Вам необходимо перейти по адресу http://www.infotecs.ru/downloads/besplatnye-produkty/vipnet-csp-4-2.html?show_form=Y для загрузки и регистрации ViPNet CSP поддерживаемой данными ОС.
   - Если Вы работаете на операционной системе **Windows 10**[4].Вам необходимо перейти по адресу http://www.infotecs.ru/downloads/beta-versii/vipnet-csp-4-2-5-windows-rus.html?show_form=Y для загрузки и регистрации ViPNet CSP поддерживаемой данной ОС с ограничениями работы протокола TLS.
   - Если вы работаете на операционной системе **Windows XP SP3 x32** разрядной. Вам необходимо перейти по адресу http://www.infotecs.ru/downloads/besplatnye-produkty/vipnet-csp-4-windows-x32-rus.html?show_form=Y для загрузки и регистрации ViPNet CSP поддерживаемой данной ОС.
2. Пройдите установленную процедуру регистрации, согласившись с условиями лицензионного соглашения (EULA) и заполнив обязательные поля.
3. Перейдите по полученной ссылке для скачивания продукта и сохраните указанный серийный номер[5]. Сохраните загруженный архив с дистрибутивом на своем компьютере, распакуйте архив, затем запустите установку ViPNet CSP файлом ***«Setup.exe»***.
4. Выполните установку ViPNet CSP, следуя инструкциям мастера установки.
5. После перезагрузки компьютера запустите настройку ViPNet CSP из панели ***«Пуск».***

   ✓ Выберите пункт ***«Зарегистрировать ViPNet CSP»*** и нажмите кнопку ***«Далее»*** (Рисунок 1)[6].

---

[1] Допускается использование иного сертифицированного криптопровайдера, например, «КриптоПро CSP». Процедуры по установке и настройке ПО Крипто-про описаны в Инструкции по настройке рабочего места для работы с ЭП (КриптоПро и eToken).

[2] Допускается использование другого средства электронной подписи, например, «КриптоАРМ». Процедуры по установке и настройке ПО Крипто-про описаны в Инструкции по установке и настройке КриптоАРМ.

[3] По вопросу получения дистрибутива ViPNet Client на CD-диске, включая комплект эксплуатационной документации, формуляр, копию сертификата соответствия, необходимо обращаться в ООО «Комлоджик» (email: 2936@comlogic.ru, тел. +7 (499) 922 2488.

[4] Для операционной системы Windows 10 действует ограничение - если производить установку ViPNet CSP по умолчанию то не будет установлена компонента поддержки протокола TLS/SSL. Если электронная подпись Вам необходима для применения на информационных системах работающих по протоколу TLS/SSL: «Электронные сервисы портала NALOG.RU», «Портал Росфинмониторинг», «Портал государственных закупок» - в начале процесса установки ViPNet CSP нажмите кнопку «Настроить», затем во вкладке «Выбор компонентов» раскройте плюсик напротив строки «Поддержка работы ViPNet CSP через Microsoft Crypto API», там, напротив строки «Поддержка протокола TLS/SSL» нажмите стрелку и выберите «Компонент будет установлен на локальный жесткий диск». Затем продолжите установку нажав «Установить сейчас»

[5] Дополнительно ссылка для скачивания продукта и серийный номер будут отправлены на указанный Вами адрес электронной почты при регистрации.

[6] Без регистрации ViPNet CSP будет функционировать в течение 14 дней и не сможет обеспечить юридической значимости электронной подписи.

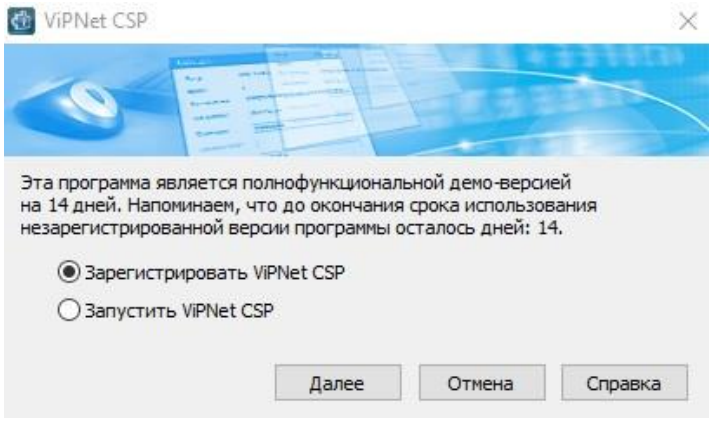

Рисунок 1

✓ Выберите пункт ***«Запрос на регистрацию (получить код регистрации)»*** и нажмите кнопку ***«Далее»*** (Рисунок 2).

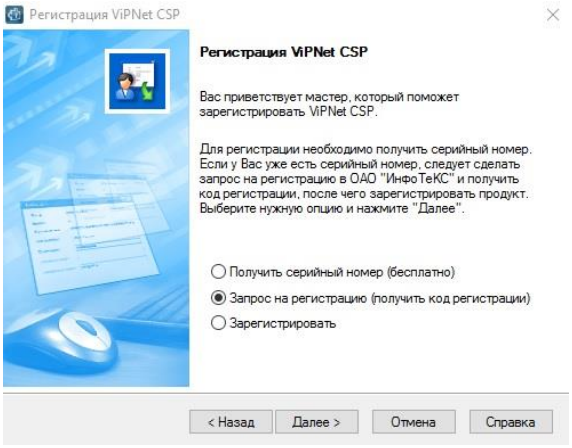

Рисунок 2

Выберите пункт ***«Через Интернет (online)»*** и нажмите кнопку ***«Далее»*** (Рисунок 3)

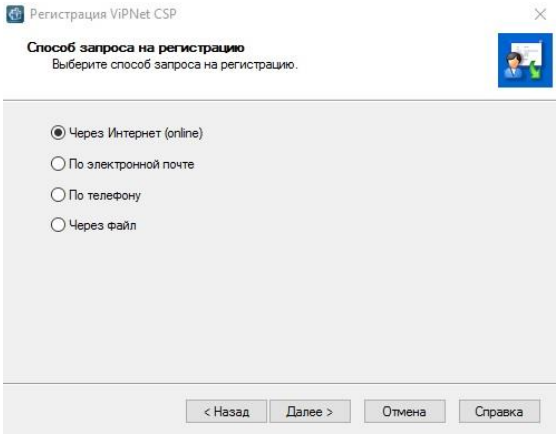

Рисунок 3

✓ Заполните форму своими регистрационными данными, включая ***«Серийный номер»*** ViPNet CSP, полученный при регистрации на Ваш E-mail и нажмите кнопку ***«Далее»*** (Рисунок 4).

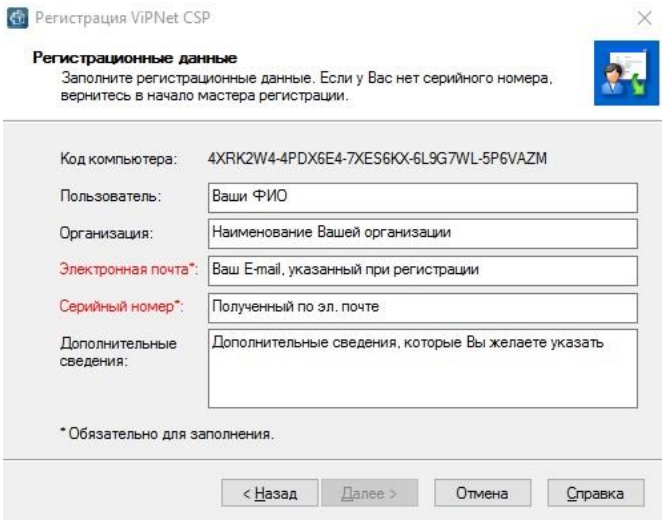

Рисунок 4

✓ После завершения процесса регистрации нажмите кнопку ***«Готово»*** (Рисунок 5).

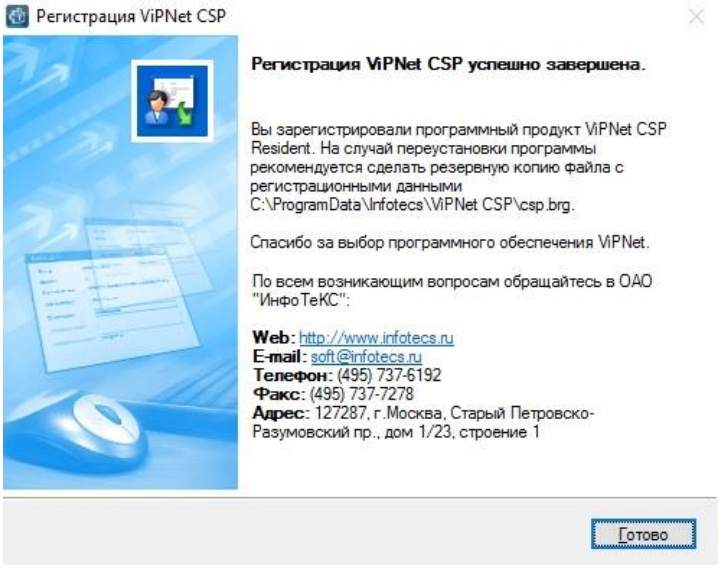

Рисунок 5

✓ На вопрос ***«Запустить ViPNet CSP сейчас?»*** нажмите кнопку ***«Да»*** или запустите ViPNet CSP позже из панели ***«Пуск».***

IV. Установка драйверов для ключевого носителя ETOKEN

Для корректной работы ключевого носителя eToken под управлением операционной системы Microsoft Windows необходимо установить программное обеспечение компании Аладдин РД ***«eToken PKI Client»*** актуальной версии.

1. Для получения ***«eToken PKI Client»*** актуальной версии необходимо загрузить дистрибутив с официального сайта разработчика https://aladdin-rd.ru/support/downloads/1b09ef64-acf2-4a8f-990d-d54ea9d1ba6b/get либо зайти самостоятельно на страницу ***eToken PKI Client 5.1 SP1 для Microsoft Windows XP, Vista, 7, Server 2003, Server 2008*** https://aladdin-rd.ru/support/downloads/6b23e20a-c832-4846-8581-b8b11319e1a9 и нажать на кнопку ***«Скачать файл»*** (Рисунок 6)

Рисунок 6

2. Загрузите архив с дистрибутивом в любое место компьютера и запустите установку ***«eToken PKI Client»*** файлом *PKIClient_x32_xx_xxx.msi (или PKIClient_x64_xx_xxx.msi)*[7] из папки архива. Выполните установку **«eToken PKI Client»** следуя инструкциям мастера установки. Установите пакет обновлений ***«eToken PKI Client»*** из файла *PKIClient-x32-x-x-SP1.msp (или PKIClient-x64-x-x-SP1.msp)*, содержащегося в том же архиве.

V. Настройка ViPNet CSP для работы с электронной подписью

Внимание! Убедитесь, что ключевой носитель eToken находится в USB-порте Вашего компьютера

1. Запустите ViPNet CSP и убедитесь, что в разделе ***«Дополнительно»*** включена опция ***«Поддержка работы ViPNet CSP через Microsoft CryptoAPI»*** (Рисунок 7).

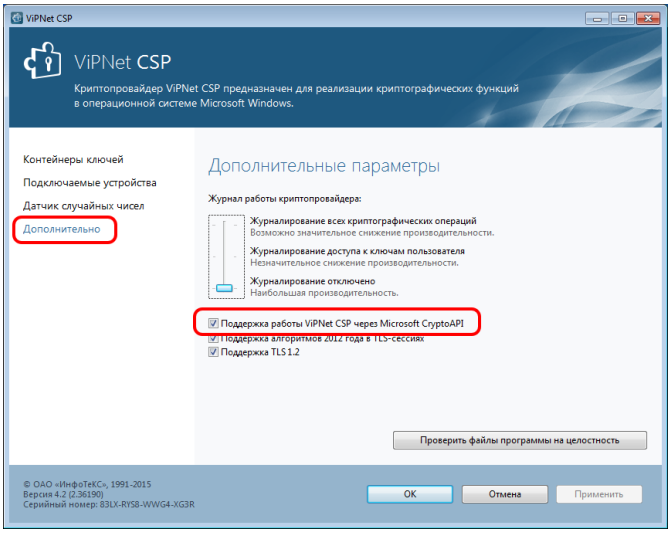

Рисунок 7

2. Перейдите в раздел ***«Контейнеры ключей»*** (рисунок 8, позиция 1)**.** В выпадающем списке (рисунок 8, позиция 2) выберите ***«eToken Aladdin(…)»*** (рисунок 8, позиция 3), а в разделе ***«Имя***

[7] **PKIClient_x32_xx_xxx.msi** – для установки на 32-х разрядную операционную систему Windows или **PKIClient_x64_xx_xxx.msi** – для установки на 64-х разрядную операционную систему Windows

контейнера» – контейнер ключей ***«XXX-XXXX-XXXX-XXXX-XXXX»*** (рисунок 8, позиция 4). Затем нажмите кнопку ***«Свойства»*** (Рисунок 8, позиция 5).

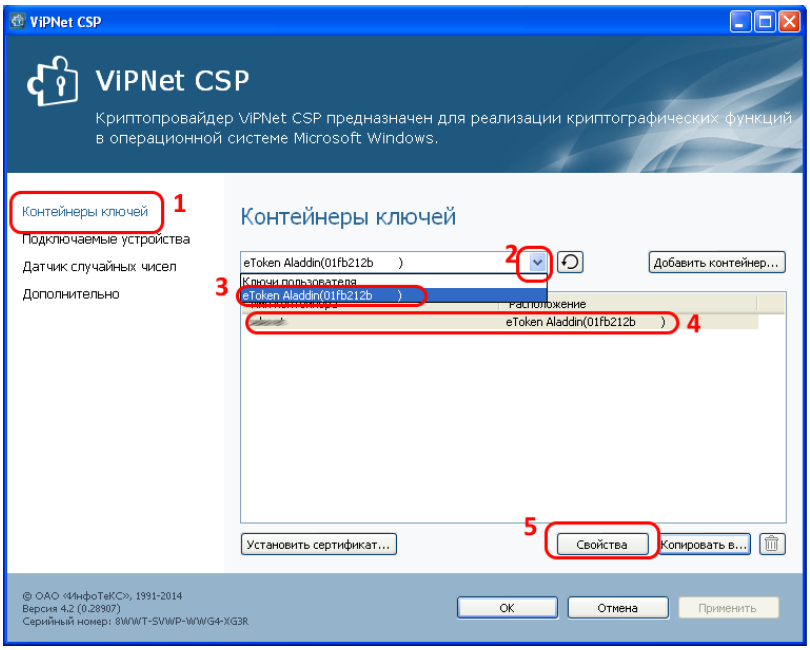

Рисунок 8

3. В окне свойств контейнера ключей (Рисунок 9) в разделе ***«Закрытый ключ, находящийся в контейнере»*** нажмите кнопку ***«Открыть»***.

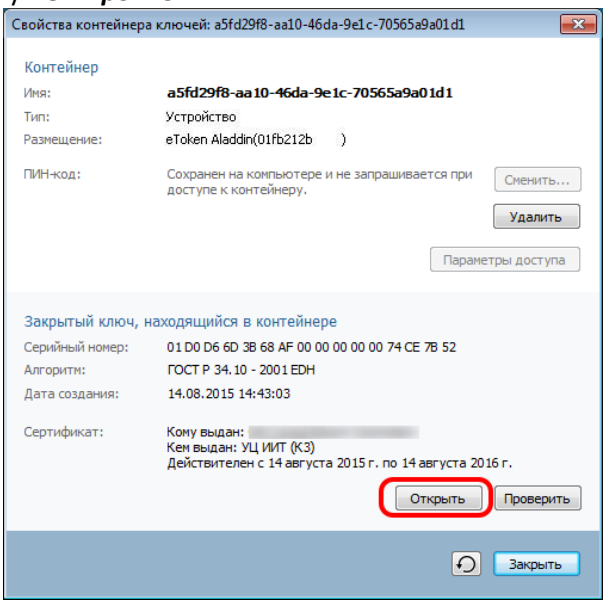

Рисунок 9

4. Убедитесь, что выбран именно тот сертификат, который необходимо использовать, и нажмите кнопку ***«Установить сертификат»*** (Рисунок 10).

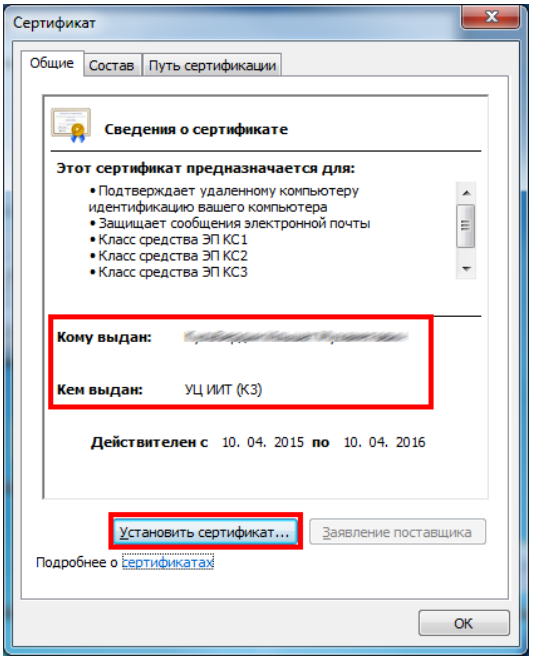

Рисунок 10

5. Далее следуйте указаниям Мастера установки сертификатов. В ходе установки сертификата обращайте внимание на выбранные опции, которые должны соответствовать рисункам 11-12.
6. В появившемся на очередном шаге окне (Рисунок 12) введите PIN-код к устройству[8].

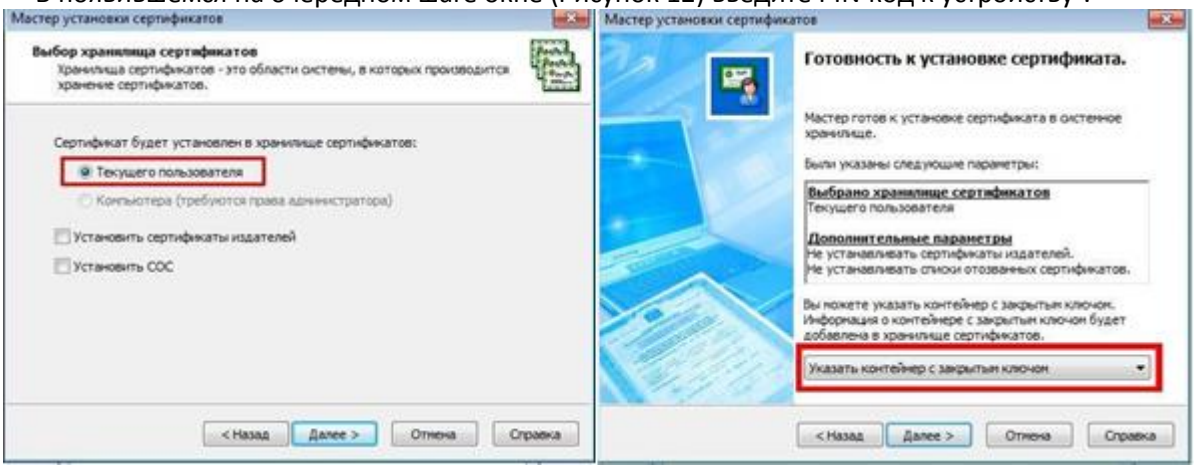

Рисунок 11

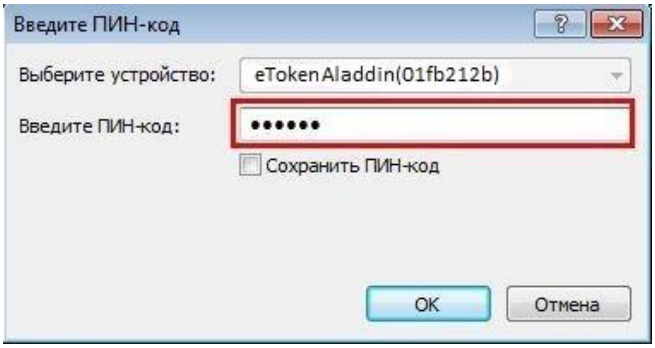

Рисунок 12

7. На этом работа Мастера установки сертификата завершается (Рисунок 13) нажмите кнопку ***«Готово»*** и переходите к следующему пункту инструкции.

[8] По умолчанию PIN-код на устройство eToken: **1eToken**

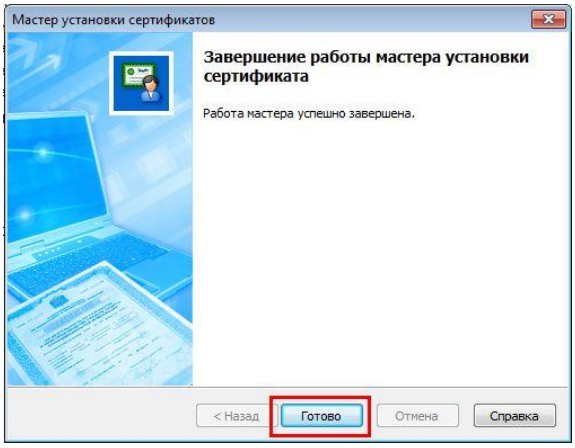

Рисунок 13

По умолчанию PIN-код на eToken: 1eToken. Рекомендуется сменить PIN-код доступа к eToken со стандартного на более устойчивый, который будете знать только Вы.

VI. Построение цепочки сертификатов до головного удостоверяющего центра Министерства связи и массовых коммуникаций

Установка сертификата головного удостоверяющего центра

1. Для того, чтобы загрузить головной сертификат удостоверяющего центра Министерства связи и массовых коммуникаций (далее по тексту - Головной УЦ) перейдите по ссылке https://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=8CAE88BBFD404A7A53630864F9033606E1DC45E2
2. Откройте загруженный сертификат и нажмите ***«Установить сертификат»*** (рисунок 14).
3. Запустится мастер импорта сертификатов, нажмите ***«Далее»***.
4. При установке корневого сертификата Головного УЦ в окне выбора хранилища, необходимо хранилище указать вручную, для этого выбрать ***«Поместить все сертификаты в следующее хранилище»*** (рисунок 15, позиция А), нажать ***«Обзор»*** (рисунок 15, позиция Б), выбрать ***«Доверенные корневые центры сертификации»*** (рисунок 15, позиция В), нажать ***«Далее»*** (рисунок 15, позиция Г).

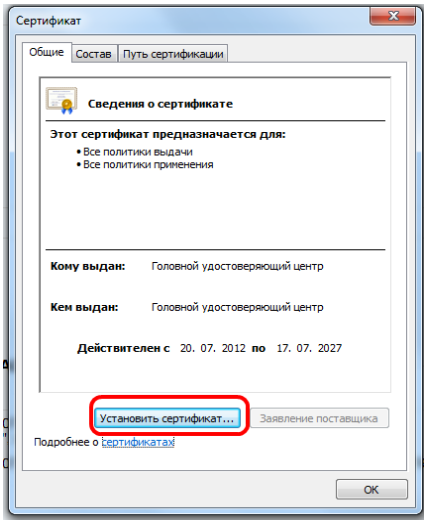

Рисунок 14

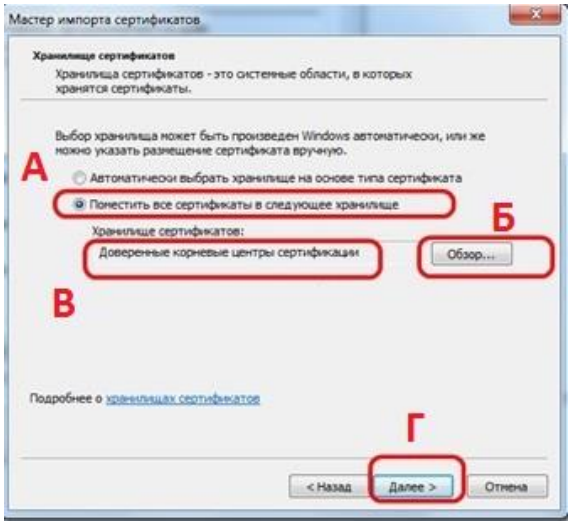

Рисунок 15

5. Далее на все запросы мастера импорта сертификатов об установке сертификата ***«Далее»/«Да»/«ОК»*** - соглашаетесь.

VII. Регистрация в ЕСИА

Вход пользователей в личные кабинеты ФГИС Росаккредитации осуществляется с использованием Единой системы идентификации и аутентификации (ЕСИА).

Для получения учетной записи юридического лица (организации) необходимо выполнить процедуру регистрации в ЕСИА (http://esia.gosuslugi.ru/registration).

Процедура регистрации юридического лица в ЕСИА предусматривает:

1. Получение руководителем организации средства электронной подписи. В качестве владельца сертификата проверки ключа электронной подписи должно быть указано лицо, имеющее право действовать без доверенности от имени юридического лица (руководитель юридического лица).

2. Регистрация руководителя юридического лица в ЕСИА как физического лица с подтвержденной учетной записью: данные о пользователе проверяются в государственных ведомствах (проверка СНИЛС и персональных данных в Пенсионном Фонде, проверка данных документа, удостоверяющего личность, в Федеральной миграционной службе) и личность пользователя подтверждена с помощью электронной подписи.

3. Авторизация в профиле физического лица, зарегистрированного в соответствии с пунктом 2, и создание учетной записи юридического лица (вкладка «Организации»).

Каждый сотрудник должен иметь зарегистрированную и подтвержденную учетную запись физического лица в ЕСИА.

> ***Внимание! Перед началом работы с порталом ЕСИА необходимо обязательно установить плагина для работы с порталом государственных услуг, для скачивания перейдите по ссылке*** https://ds-plugin.gosuslugi.ru/plugin/upload/Index.spr

A. Регистрация физического лица

1. Форма регистрации на Едином портале государственных услуг доступна по ссылке http://esia.gosuslugi.ru/registration (Рисунок 16). Заполните поля: ***«Фамилия»***; ***«Имя»; «Мобильный телефон»***. При отсутствии мобильного телефона заполните поле ***«Адрес электронной почты».*** После чего нажмите кнопку ***«Зарегистрироваться»***.

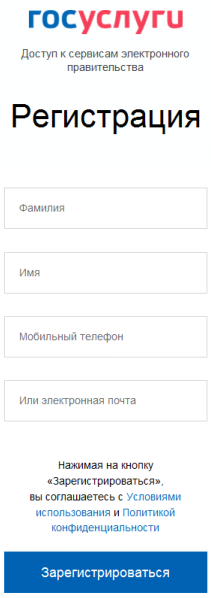

Рисунок 16

2. Если вы ввели мобильный телефон, то система отправляет код подтверждения на номер мобильного телефона, указанный при регистрации и отображается форма для подтверждения номера мобильного телефона (Рисунок 17). Введите полученный код подтверждения в поле ***«Код подтверждения»*** и нажмите кнопку ***«Подтвердить».***

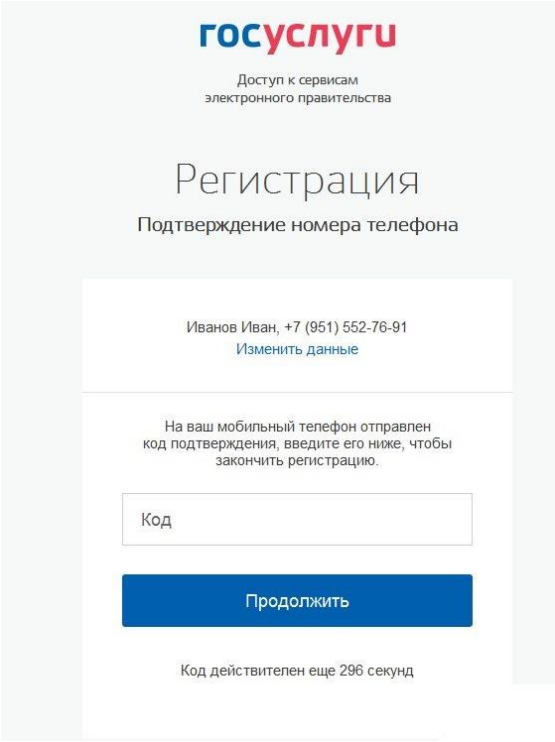

Рисунок 17

Код подтверждения можно ввести в течение 5 минут. При истечении отведенного времени можно запросить новый код подтверждения. Для этого необходимо нажать кнопку «Получить новый код подтверждения».

3. Если Вы ввели адрес электронной почты, то отобразится страница подтверждения адреса электронной почты для создаваемой учетной записи (Рисунок 18). На адрес электронной почты, указанный при регистрации, система отправляет письмо для подтверждения адреса электронной почты. Необходимо открыть полученное письмо и перейти по гиперссылке для подтверждения адреса электронной почты. Время действия полученной гиперссылки составляет 3 дня.

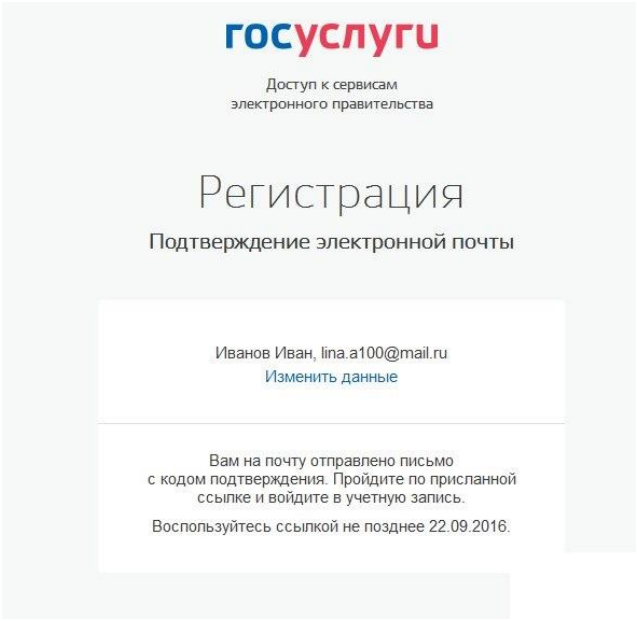

Рисунок 18

4. При нажатии кнопки ***«Подтвердить»*** (Рисунок 19) или при переходе по гиперссылке в письме для подтверждения адреса электронной почты, отобразится форма создания пароля (Рисунок 19). Пароль будет использоваться для входа в Систему. Введите пароль в поле ***«Пароль»***. Подтвердите создаваемый пароль его повторным вводом в поле ***«Подтвердите пароль»***. Нажмите на кнопку ***«Сохранить»***.

Пароль должен содержать не менее 8 символов и состоять из строчных и заглавных букв, а также содержать цифры.

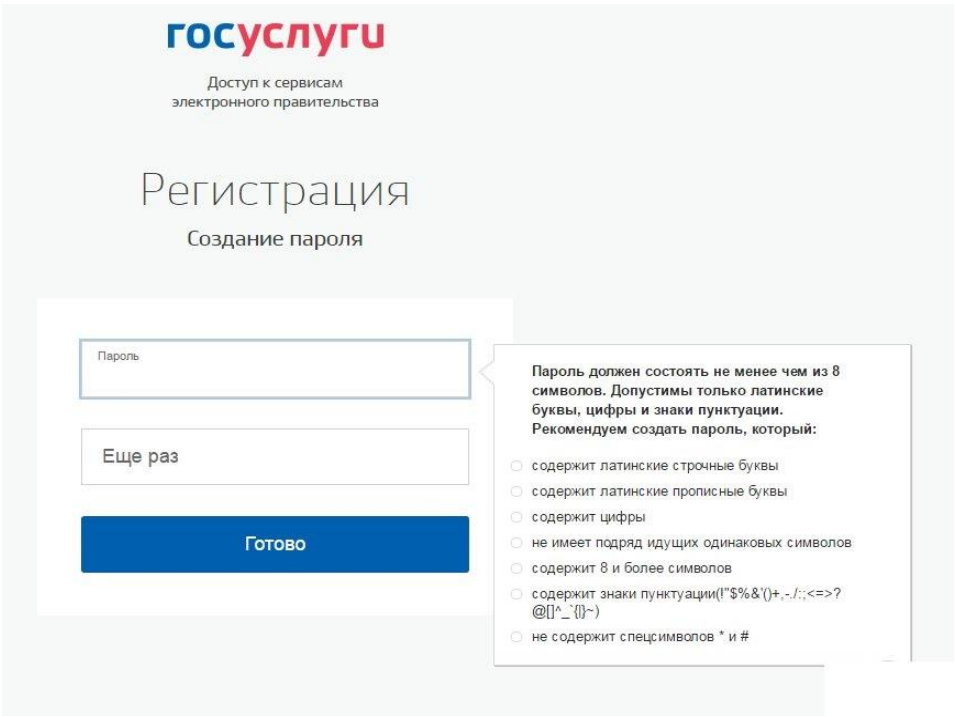

Рисунок 19

5. После выполнения проверки корректности введенных данных. Если указанные данные корректны, то отобразится окно с сообщением об успешной регистрации (Рисунок 20). Через 3 секунды Вас переадресует на окно основной информации в профиль пользователя.

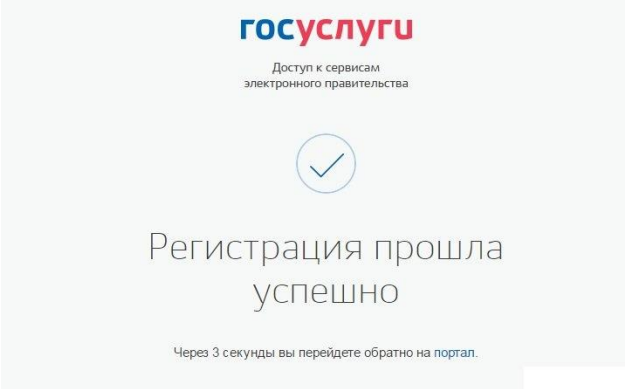

Рисунок 20

Б. Подтверждение учетной записи

1. Для подтверждения учетной записи необходимо заполнить личные данные в окне «Основная информация» профиля пользователя (Рисунок 21).

В случае если регистрируется руководитель юридического лица для последующей регистрации самого юридического лица в ЕСИА, рекомендуется сразу использовать способ подтверждения личности «с помощью средства электронной подписи».

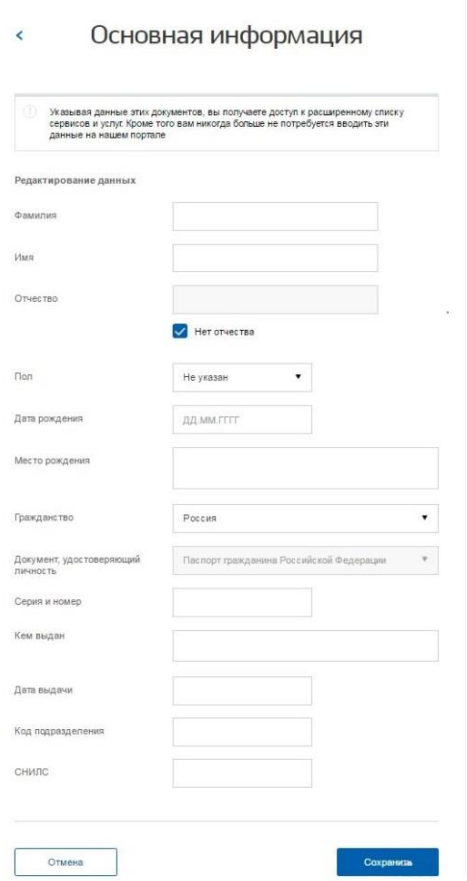

Рисунок 21

2. После заполнения личных данных нажмите кнопку ***«Сохранить»*** для перехода к автоматической проверке личных данных (Рисунок 22)

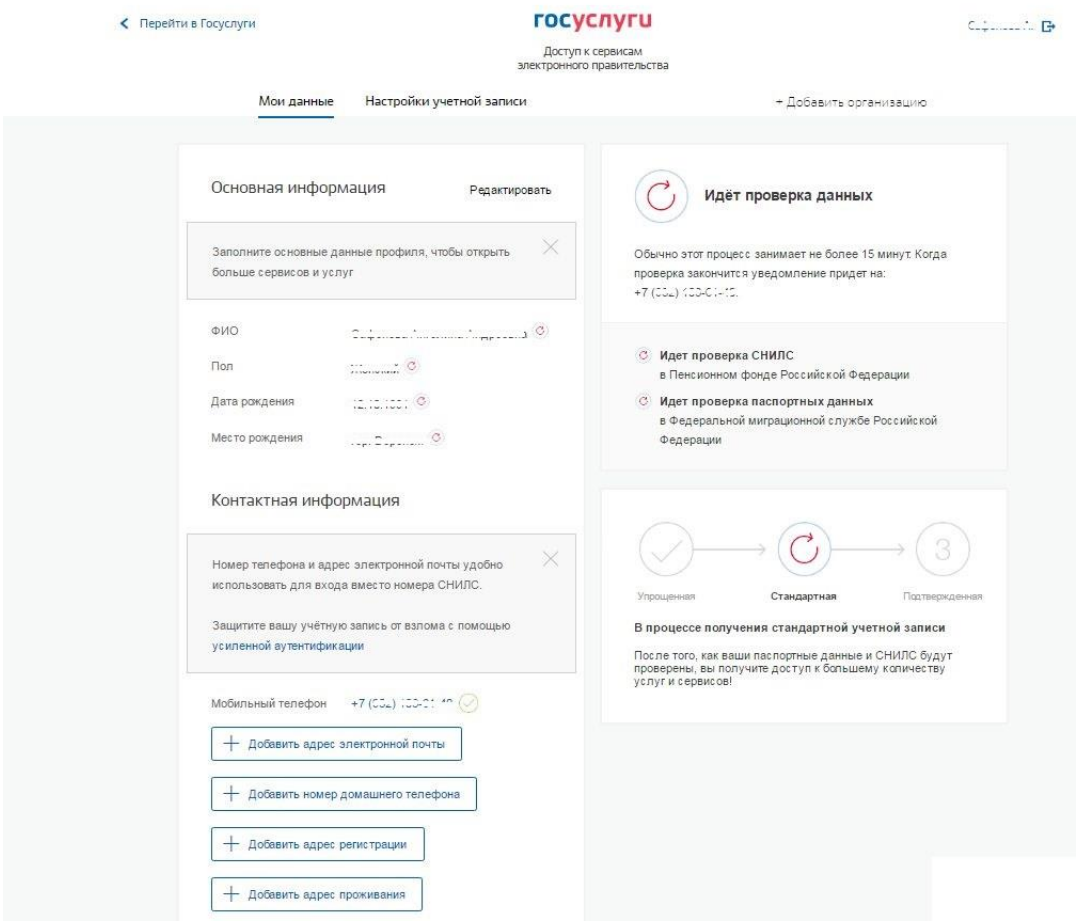

Рисунок 22

3. Проверка личных данных выполнена успешно, если в правой части окна появится запись «Проверка ваших документов успешно завершена» и кнопка ***«Подтвердить»*** – активна (Рисунок 23).

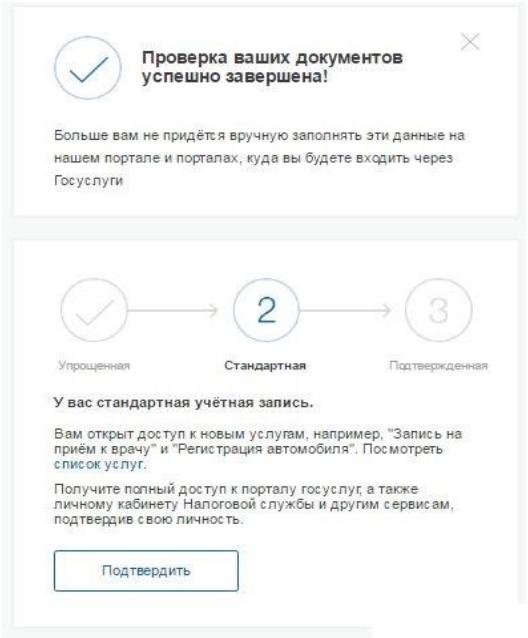

Рисунок 23

4. Нажмите кнопку ***«Подтвердить»*** для перехода к следующему этапу подтверждения учетной записи. Выберите способ подтверждения ***«Электронной подписью или УЭК»***, подключите средство

электронной подписи или УЭК, нажмите на кнопку ***«Готово»*** (Рисунок 24).

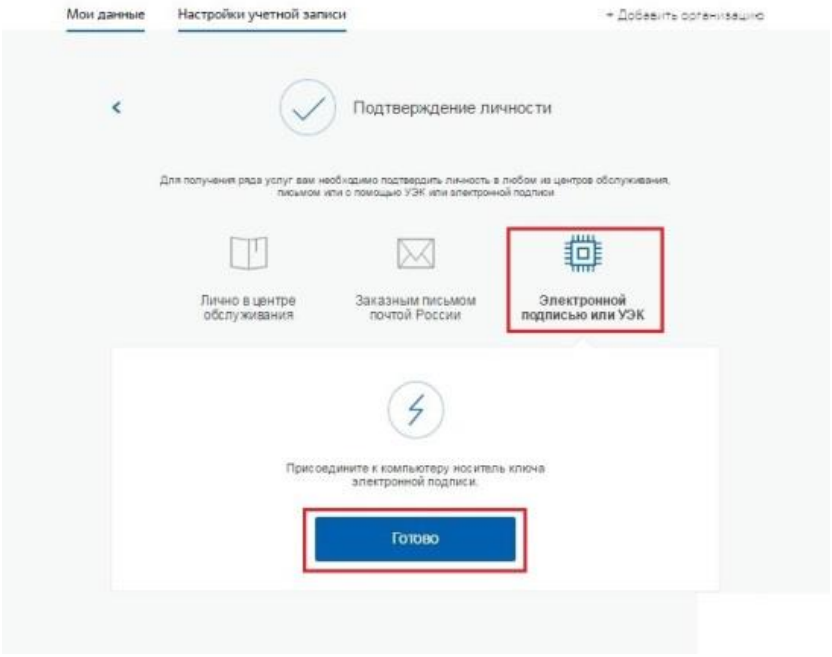

Рисунок 24

5. При нажатии кнопки ***«Готово»*** выполняется проверка электронной подписи или карты УЭК. При успешно выполненном подтверждении личности в правой части окна появится запись «У вас подтвержденная учетная запись» (Рисунок 25).

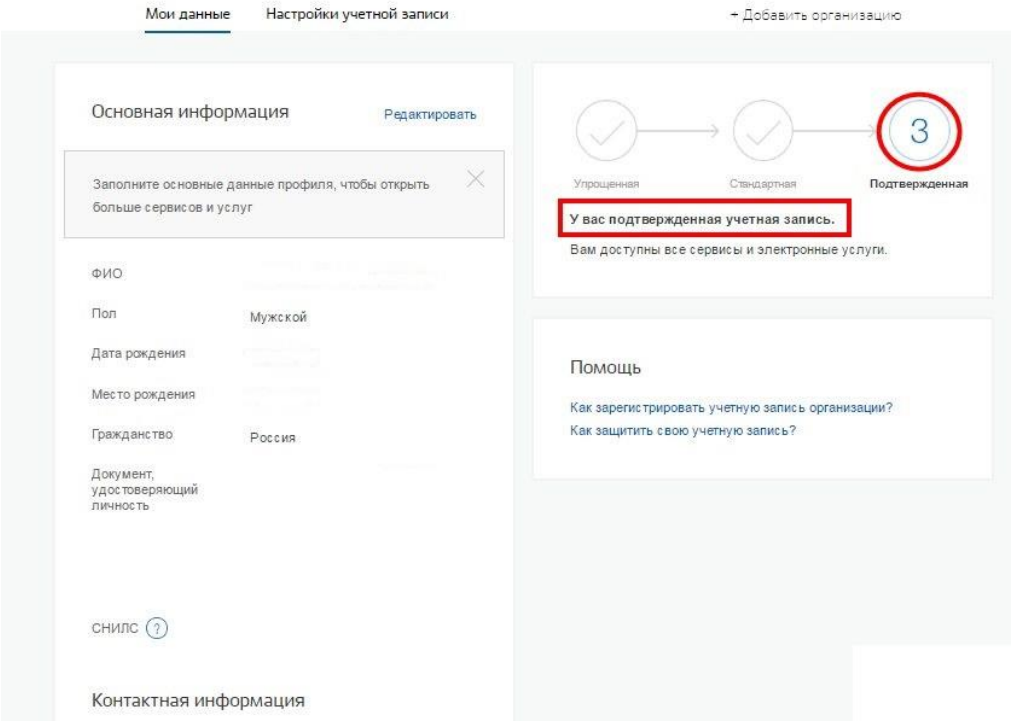

Рисунок 25

B. Регистрация юридического лица

Для создания учетной записи организации необходимо:

- ✓ наличие подтвержденной учетной записи физического лица в ЕСИА (см. Раздел А) для руководителя юридического лица или представителя юридического лица, имеющего право действовать от имени организации без доверенности (далее – руководитель организации);
- ✓ наличие средства электронной подписи, содержащего действующий квалифицированный сертификат ключа проверки электронной подписи (СКП), выданный руководителю организации, одним из УЦ, аккредитованных Минкомсвязи России.

Подключите носитель ключа электронной подписи, выданный на имя руководителя организации, к компьютеру. Не извлекайте носитель до завершения процедуры регистрации.

1. Для создания учетной записи организации на странице регистрации в ЕСИА http://www.esia.gosuslugi.ru/registration руководитель организации должен выполнить вход в профиль физического лица. Если учетная запись подтвержденная, в правом верхнем углу появится кнопка ***«Добавить организацию»*** (Рисунок 26).

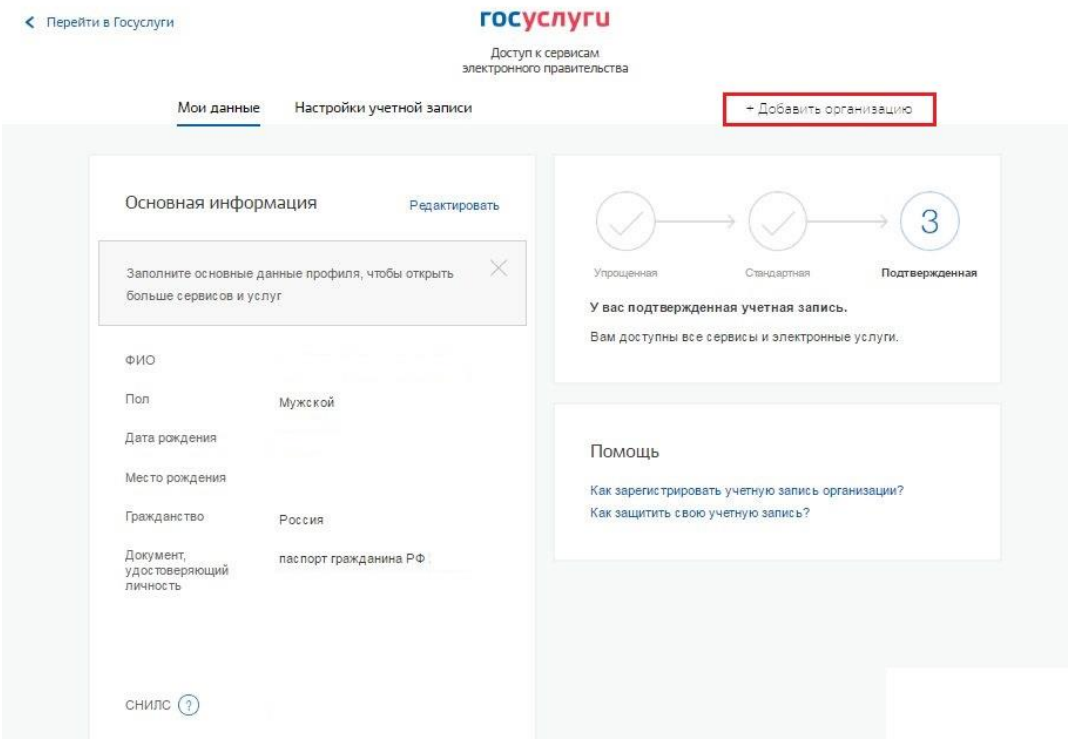

Рисунок 26

2. Во всплывающем окне ***«Добавление организации»***, необходимо выбрать тип создаваемой организации (Рисунок 27).

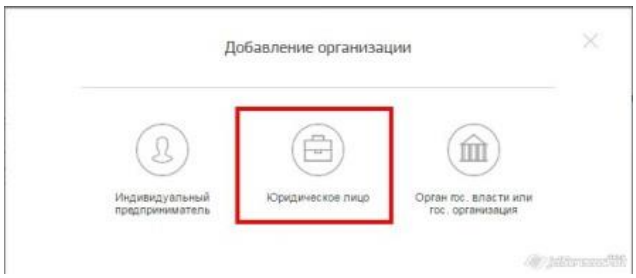

Рисунок 27

3. В окне с информацией по созданию учетной записи организации (Рисунок 28) нажмите кнопку ***«Продолжить»*** для перехода к шагу ввода данных организации и личных данных.

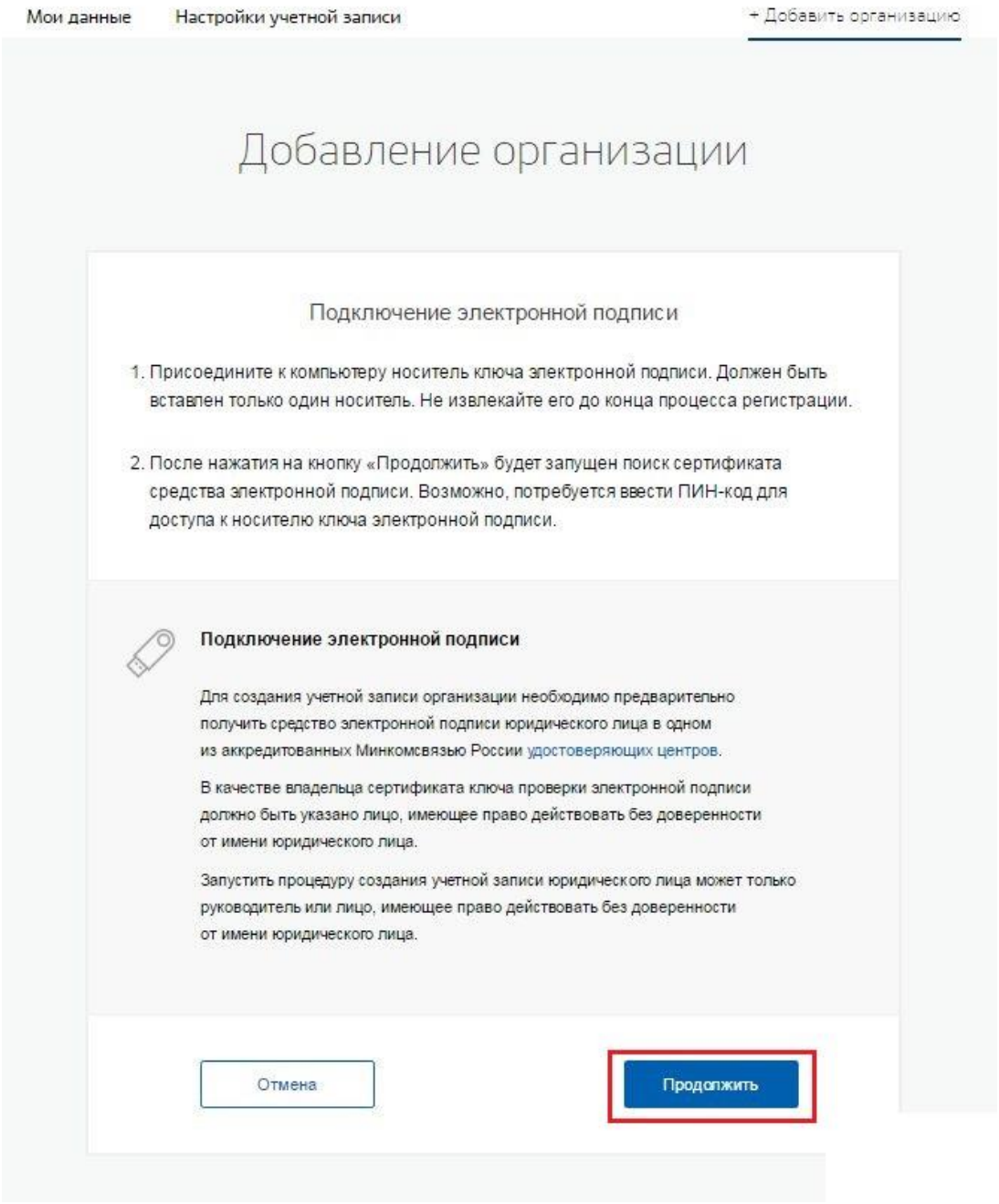

Рисунок 28

4. В форме для ввода данных об организации (Рисунок 29), часть сведений будет автоматически заполнена данными, загружаемыми из сертификата ключа проверки электронной подписи. Заполните оставшиеся поля формы ***«Организационно-правовая форма»*** и ***«Адрес электронной почты организации».*** Если в личных данных не был указан ИНН, то в поле ***«ИНН»*** следует указать ИНН пользователя как физического лица. После чего перейдите к шагу по автоматической проверке данных, нажав кнопку ***«Продолжить»*** (Рисунок 29).

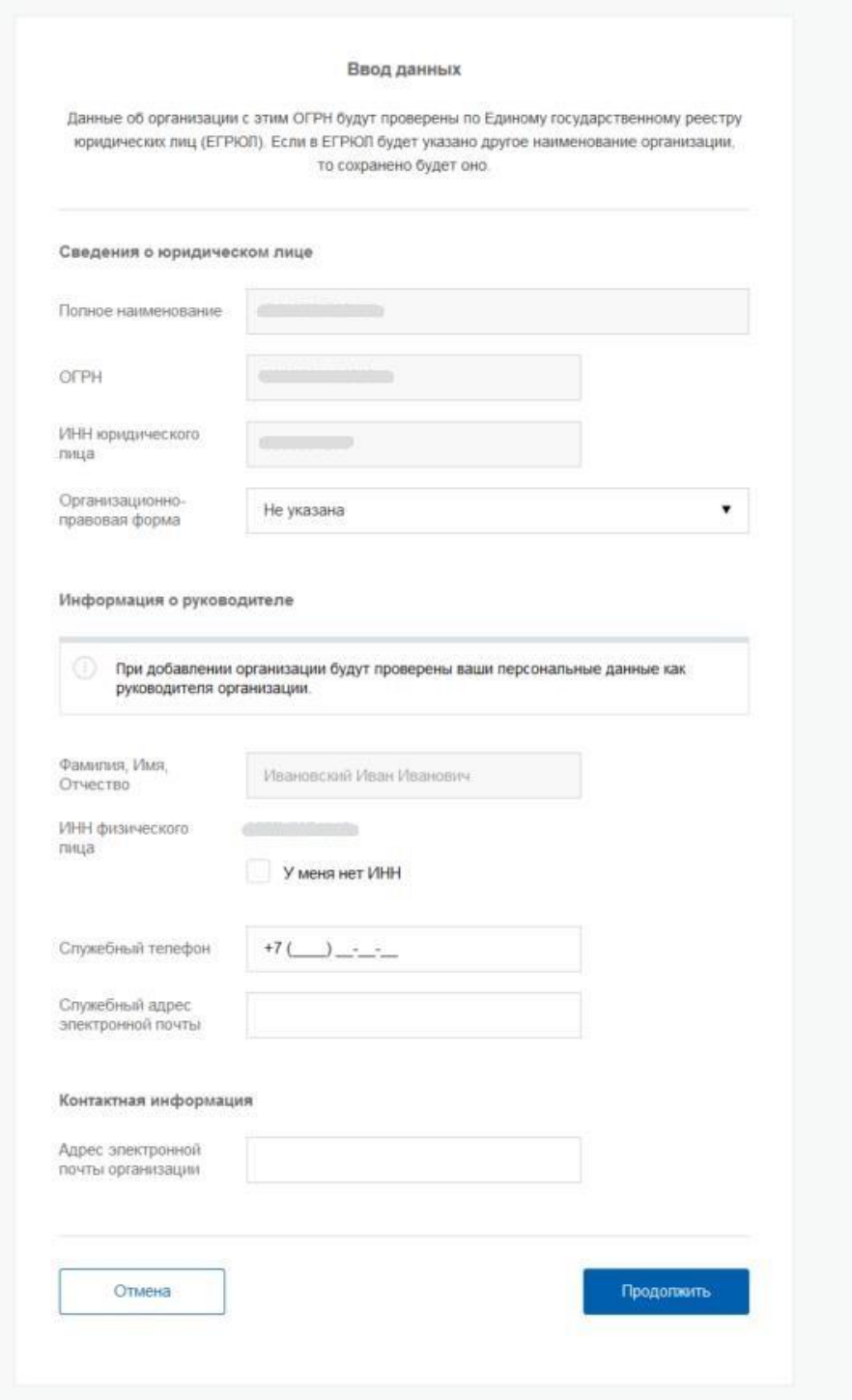

Рисунок 29

5. Проверка данных выполнена успешно, если в правой части окна для каждой из выполненных проверок отображается значок «» (Рисунок 30).

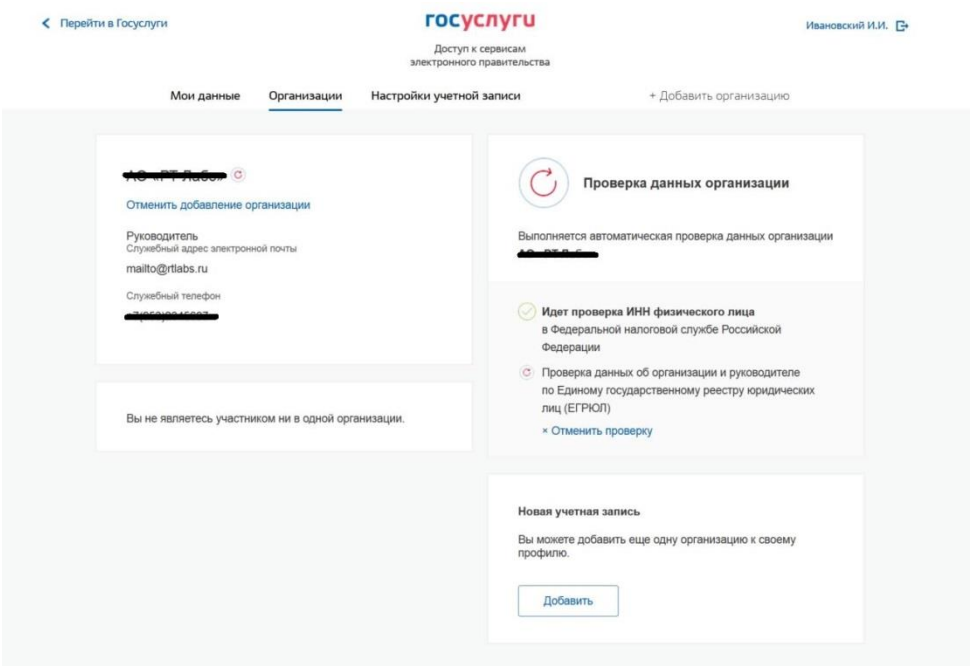

Рисунок 30

6. При успешно выполненной проверке данных выполняется регистрация юридического лица в ЕСИА, запись вносится в регистр ЮЛ. Руководитель организации, осуществлявший регистрацию ЮЛ, автоматически получает роль должностного лица данного ЮЛ и права руководителя. Зарегистрированная организация отображается на вкладке ***«Организации»*** в личном профиле подтвержденной учетной записи физического лица (Рисунок 31).

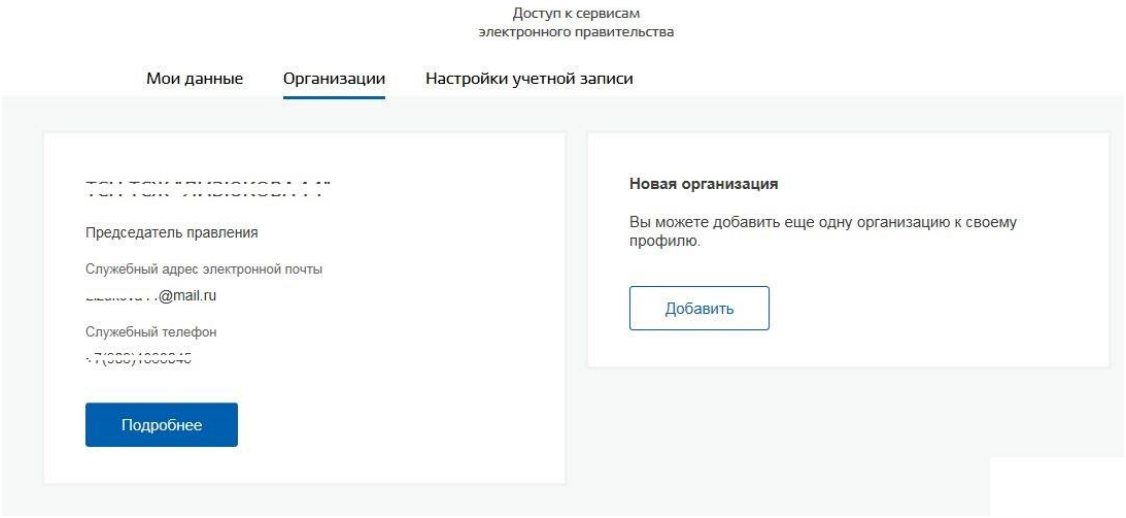

Рисунок 31

7. После регистрации учетной записи у руководителя организации появляется возможность приглашать сотрудников, регулировать их доступ к информационным системам.

VIII. Экспорт сертификата электронной подписи и передача его во ФГИС Росаккредитации

1. Для экспорта сертификата электронной подписи во ФГИС Росаккредитации запустите ViPNet CSP и перейдите в раздел ***«Контейнеры ключей»,*** выберете соответствующий контейнер и нажмите кнопку ***«Свойства»*** (Рисунок 32).

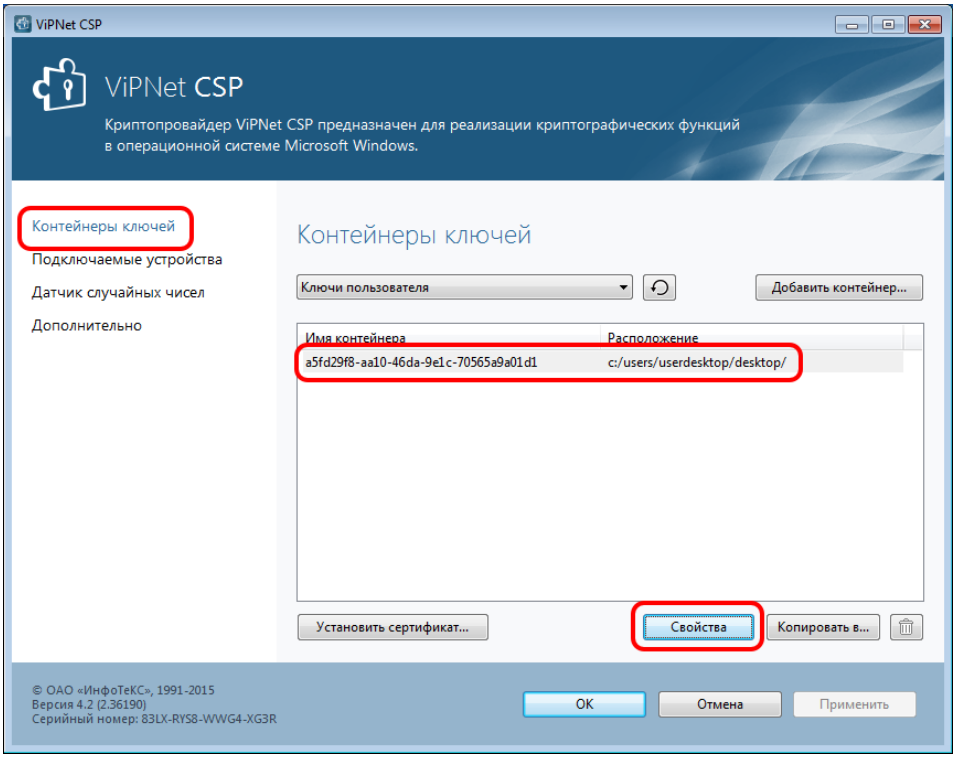

Рисунок 32

2. В окне свойств контейнера ключей (Рисунок 33) в разделе ***«Закрытый ключ, находящийся в контейнере»*** нажмите кнопку ***«Открыть»***.

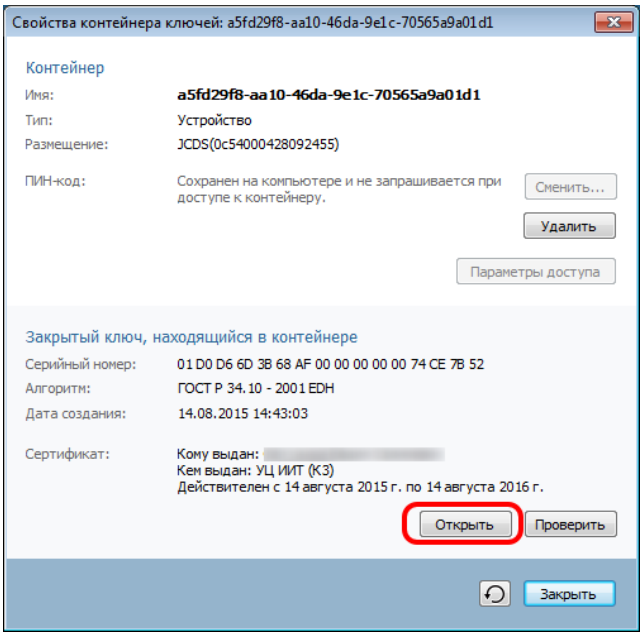

Рисунок 33

3. В окне просмотра сертификата перейдите на вкладку ***«Состав»*** и нажмите кнопку ***«Копировать в файл»*** (Рисунок 34).

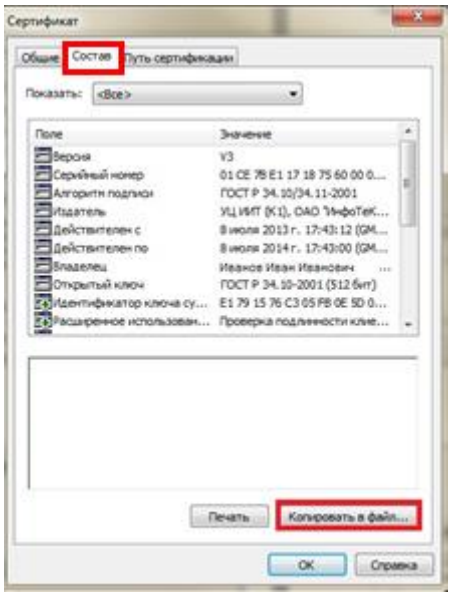

Рисунок 34

4. Следуйте инструкциям мастера экспорта сертификатов и сохраните файл сертификата в папку на диске компьютера.

Внимание! Полученный файл сертификата квалифицированной электронной подписи (файл с расширением *.cer) необходимо заархивировать (формат *.zip или *.rar).

5. Отправьте его на адрес электронной почты fgis@fsa.gov.ru. Название темы письма должно содержать номер аттестата аккредитации и словосочетание «*сертификат ЭП*». Содержание письма, отправляемого на указанный адрес электронной почты, должно соответствовать заполняемым полям формы запросов http://fsa.gov.ru/public/uploads/usr/Zapros_connect_FGIS.docx, указанных в п. 4.5 Порядка получения доступа информационным ресурсам ФГИС Росаккредитации. В письме так же необходимо указать информацию о количестве рабочих мест, на которых будет устанавливаться легально приобретённое ПО «ViPNet Client 3.x (КС3)».

6. В ответ на отправленное письмо пользователь должен получить зашифрованный на его сертификате файл(ы) первичной инициализации абонентского пункта (*.dst) в сети «2936 ФСА».

IX. Получение и установка ViPNet CryptoFile

Для расшифрования полученного от Росаккредитации файла первичной инициализации абонентского пункта (*.dst) в сети «2936 ФСА» рекомендуется использовать ПО ViPNet CryptoFile.

1. Загрузите дистрибутив ПО ViPNet CryptoFile по ссылке http://files.iitrust.ru/Cryptofile/4.0_(1.30030)/CryptoFile_4.0.1.30030.exe

2. Запустите установку ViPNet CryptoFile и следуйте инструкциям мастера установки.

3. После успешной установки ПО ViPNet CryptoFile запустите его с 

ярлыка на рабочем столе или из меню ***«Пуск».***

Внимание! При установленном криптопровайдере ViPNet CSP, ПО ViPNet CryptoFile не требует регистрации, если Вы используете другой криптопровайдер, то для получения серийного номера Вам необходимо обратиться в техническую поддержку ОАО «ИнфоТеКС Интернет Траст» по т. +7 (495) 737-33-69 или по бесплатному номеру 8-800-250-0-260 (кроме звонков из Москвы).

4. Добавьте полученный от ФГИС Росаккредитации файл в список ViPNet CryptoFile нажав кнопку ***«Добавить»*** (Рисунок 35).

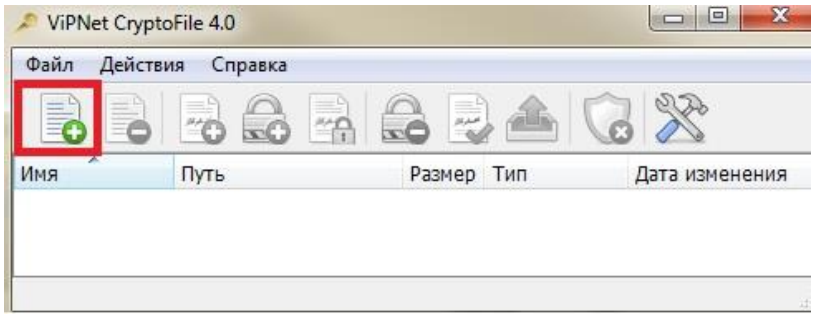

Рисунок 35

5. Выделите данный файл в списке и нажмите кнопку ***«Расшифровать»*** (Рисунок 36).

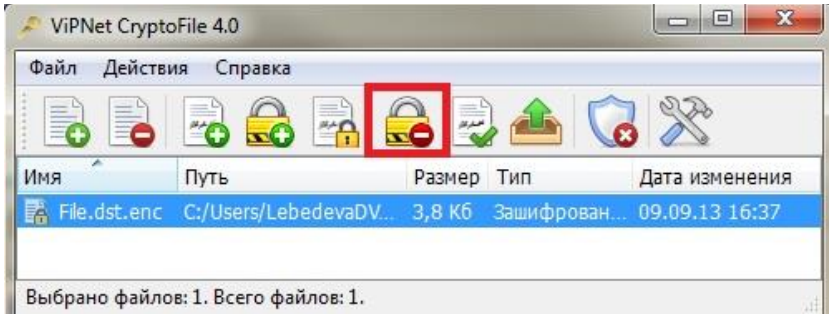

Рисунок 36

6. При необходимости введите пин-код[9] к ключевому носителю и убедитесь в успешном завершении операции, после чего нажмите кнопку ***«Закрыть»***.
7. Расшифрованный файл будет сохранен в той же папке, что и зашифрованный файл.

X. Установка и инициализация ViPNet Client

Для получения доступа к защищенному ресурсу ФГИС Росаккредитации и установке защищенного соединения используется ПО «ViPNet Client 3.x (КС3)»[10].

1. Для установки ViPNet Client необходимо запустить файл ***setup.exe*** из полученного дистрибутива ViPNet Client на CD-диске.
2. Выполните установку ViPNet Client, следуя инструкциям мастера установки.
3. В окне выбора ***«Типа установки»*** выберите пункт ***«Типичная»***.
4. Если во время установки Вам будет предложено отключить брандмауэр Windows, то соглашайтесь, нажав кнопку ***«Да»*** (Рисунок 37).

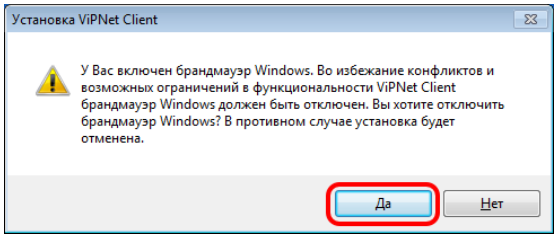

Рисунок 37

[9] По умолчанию PIN-код на устройство eToken: **1eToken**

[10] По вопросу получения дистрибутива ViPNet Client на CD-диске, включая комплект эксплуатационной документации, формуляр, копию сертификата соответствия необходимо обращаться в ООО «Комлоджик» (email: 2936@comlogic.ru, тел. +7 (499) 922 2488)

5. После окончания установки появится необходимо ***ОБЯЗАТЕЛЬНО***! перезагрузить компьютер.

6. После перезагрузки компьютера ViPNet Монитор еще не готов к работе, поскольку еще не установлен набор ключей (dst-файл). Для инициализации ключей выполните следующие действия:

- ✓ Запустите ViPNet Монитор, с ярлыка на рабочем столе или из меню ***«Пуск».***
- ✓ В окне ввода пароля в выпадающем списке меню ***«Настройка…»*** выберите пункт ***«Первичная инициализация»*** (Рисунок 38).

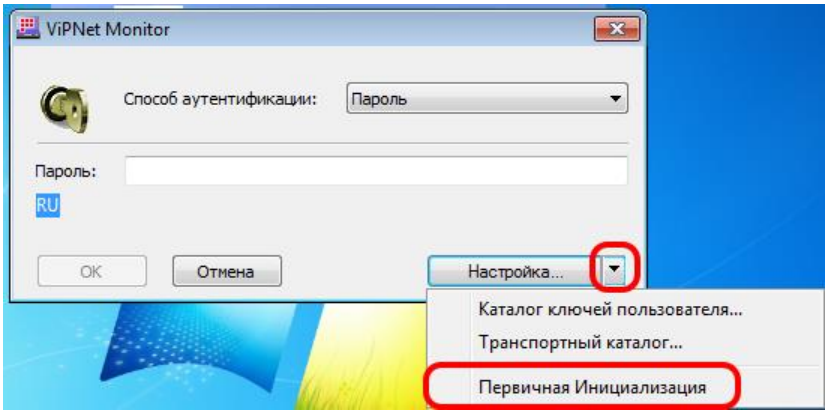

Рисунок 38

- ✓ В окне выбора местонахождения дистрибутива ключей нажмите кнопку ***«Обзор…»*** и укажите путь к файлу ключевой информации (*.dst).
- ✓ Далее следуйте инструкциям мастера установки.

После установки и инициализации ViPNet Client проверьте функционирование защищенного канала связи для подключения к ФГИС Росаккредитации.

Для этого в Интернет-обозревателе введите адрес: http://10.250.4.13/ (Рисунок 39). Страница должна быть доступна.

Если страница недоступна, необходимо обратиться **в службу технической поддержки ООО «Комлоджик»** для получения дальнейших инструкций (email: 2936@comlogic.ru, тел. +7 (499) 922 2488).

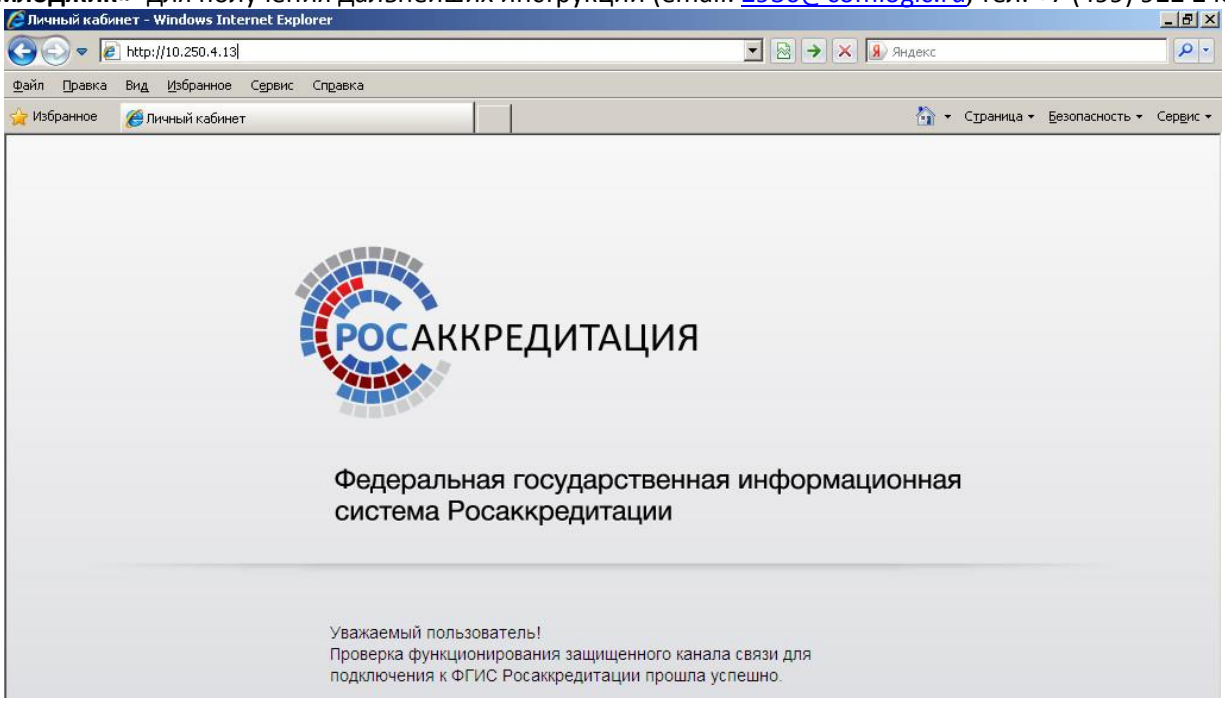

Рисунок 39

Для более подробной информации об установке и настройке ViPNet Client воспользуйтесь «Инструкцией по установке, запуску и первоначальной настройке ПО ViPNet Client», входящей в состав эксплуатационной документации ViPNet, а также размещенной по адресу http://iitrust.ru/upload/medialibrary/1f4/quickstart_client_ru.pdf.

При необходимости дополнительных настроек ViPNet Client, отвечающих за функционирование абонентского пункта в сети «2936 ФСА» используйте «ViPNet Client [Монитор]. Руководство пользователя», входящей в состав эксплуатационной документации ViPNet, а также размещенной по адресу http://iitrust.ru/upload/medialibrary/c30/vipnet_client_monitor_ru.pdf.

На этом настройка автоматизированного рабочего места для работы в информационной системе ФГИС Росаккредитации с использованием электронной подписи завершена.