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

Листов 18

ИнфоТеКС Интернет Траст
2021 г.

Оглавление

I. Введение

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

✓ В удостоверяющем центре АО «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 АО «ИнфоТеКС Интернет Траст».

✓ 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 **Mozilla FireFox, Google Chrome или Yandex браузер**.

✓ **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.
- ✓ Драйвер для работы с соответствующим ключевым носителем.
- ✓ ГОСТ СКЗИ
- ✓ ПО ViPNet CryptoFile[1].
- ✓ ПО ViPNet Client и файл первичной инициализации абонентского пункта (*.dst) в сети «2936 ФСА»[2].
- ✓ Специальное ПО (далее – плагины), обеспечивающие работу интернет-обозревателя с Единой системой идентификации и аутентификации (далее – ЕСИА) и порталом ФГИС Росаккредитация.

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

[2] По вопросу получения дистрибутива ViPNet Client на CD-диске, включая комплект эксплуатационной документации, формуляр, копию сертификата соответствия, необходимо обращаться к партнерам АО «ИнфоТеКС».

Внимание! Крайне не рекомендуется устанавливать СКЗИ ViPNet CSP на компьютер, где уже установлено СКЗИ «КриптоПро CSP». В случае использовании двух СКЗИ на одном рабочем месте не гарантируется работа одного из них, вплоть до выхода операционной системы из строя. АО «ИнфоТеКС Интернет Траст» не несет ответственности за корректную работу СКЗИ ViPNet CSP при несоблюдении пользователем данного условия.

III. Получение и установка ГОСТ СКЗИ

В зависимости от того какое у Вас используется средство криптографической защиты информации (СКЗИ) для работы с электронной подписью (ViPNet CSP или КриптоПРО CSP), воспользуйтесь одной из инструкций, опубликованных на **Официальном сайте АО ИнфоТеКС Интернет Траст**. Их можно загрузить в разделе **«Поддержка» > «Пользовательская документация»** (Рисунок 1).

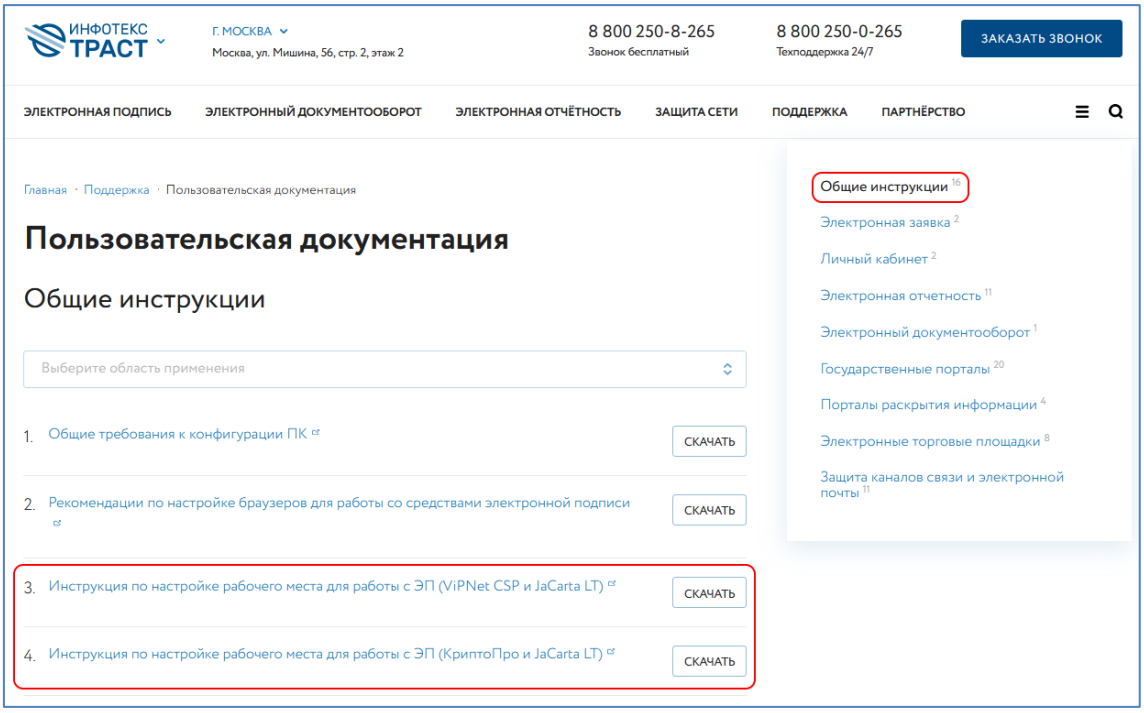

Рисунок 1

IV. Установка плагинов и настройка браузера

А. Установка плагина для работы с порталом государственных услуг

Для авторизации с помощью электронных средств на рабочем месте должен быть установлен Плагин пользователя портала государственных услуг. Для его получения необходимо перейти по ссылке https://ds-plugin.gosuslugi.ru/plugin/upload/Index.spr и выбрать версию плагина для Вашей версии операционной системы, её разрядности и расширение для браузера, если используется Chrome (Рисунок 2).

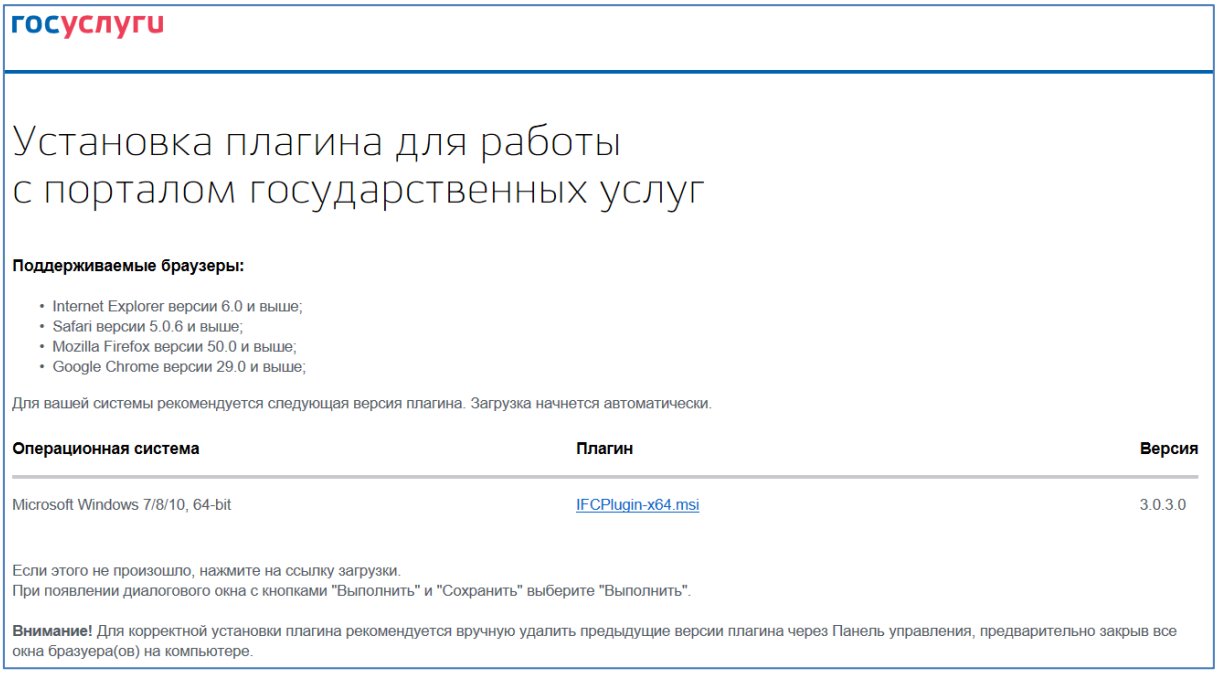

Рисунок 2

1. Выйдет окно предупреждения системы безопасности. Нажмите кнопку ***«Выполнить»*** (Рисунок 3).

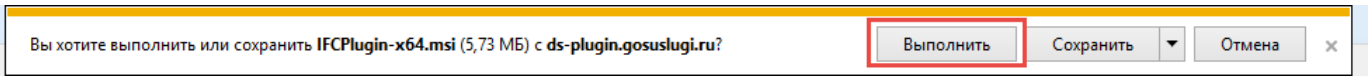

Рисунок 3

2. Начнется установка ПО ***«Плагин пользователя портала гос. услуг»*** Нажмите кнопку ***«Далее»*** (Рисунок 4).

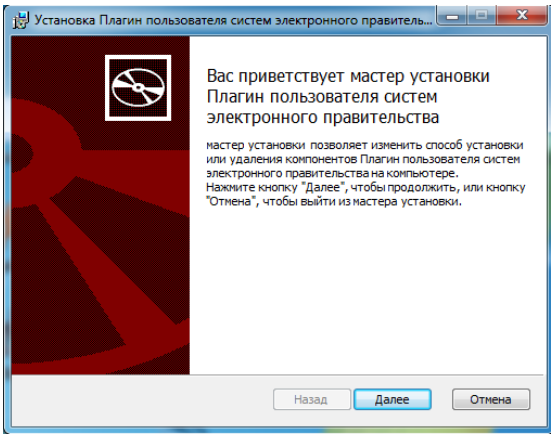

Рисунок 4

3. Дождитесь окончания установки и нажмите кнопку ***«Готово».*** После установки необходимо перезапустить браузер.

Б. Установка криптоплагина «Крипто компонента» и расширения ESEP Crypto Extension для подписания декларации

Для подписания сведений о регистрируемой декларации с помощью электронных средств на рабочем месте должен быть установлен криптоплагин ***«Крипто компонента»***, ссылка для загрузки http://esep.fsa.gov.ru/ESEP-WebApp/npcryco_esep.exe. После установки криптоплагина необходимо установить расширение ***«ESEP Crypto Extension»*** для браузера Google Chrome. Для его получения необходимо перейти по ссылке и нажать на кнопки **установить –> установить расширение**.

Для проверки корректности работы электронной подписи необходимо выполните следующие действия:

1. Перейдите по адресу http://esep.fsa.gov.ru/Esep-ExternalSystem/Sign/;
2. Выберите и загрузите любой документ с локального компьютера, нажав на кнопки ***«Выбрать файлы»***, затем ***«Загрузить»***;
3. Выполните подписание документа нажав на кнопку ***«Подписать документы»***.

V. 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 (https://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.

Регистрация физического лица, подтверждение учетной записи, регистрация юридического лица описаны в разделе IV инструкции (https://iitrust.ru/downloads/manual/uc/Manual_ESIA_ARM.pdf).

VI. Экспорт сертификата электронной подписи

1. Откройте свойства браузера, введя в поисковую строку ***«Свойства браузера»*** (Рисунок 5).

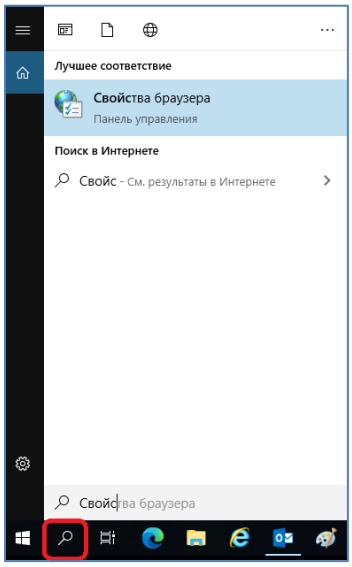

Рисунок 5

2. Перейти на вкладку ***«Содержание»***, нажать на кнопку ***«Сертификаты»***. В окне ***«Сертификаты»*** откройте вкладку ***«Личные»***, выделите требуемый для проверки подлинности сертификат и нажмите кнопку ***«Экспорт»*** (Рисунок 6):

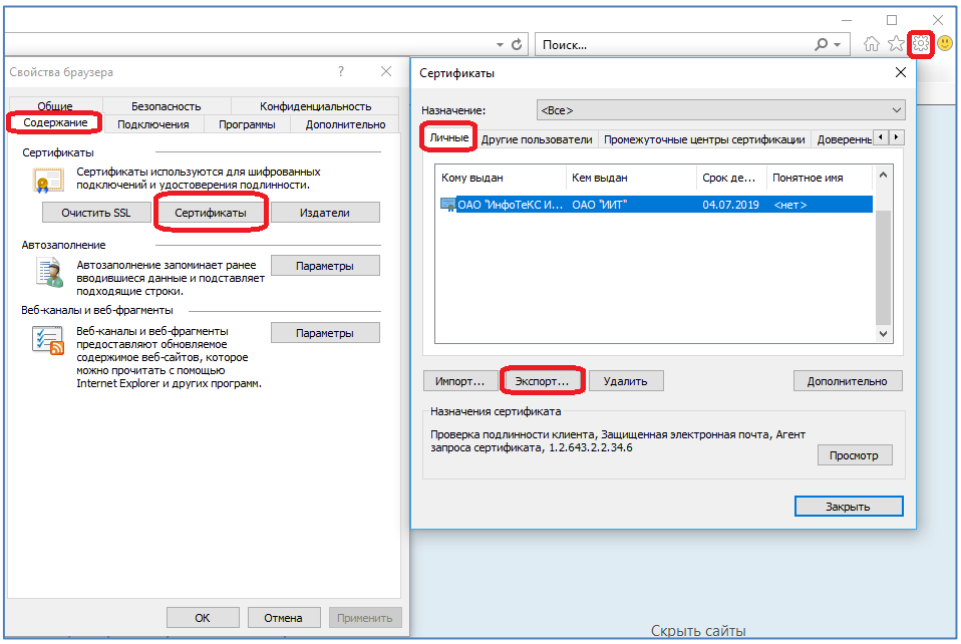

Рисунок 6

3. Откроется мастер экспорта сертификатов, нажмите ***«Далее»***.

4. Выберите ***«Нет, не экспортировать закрытый ключ»***, нажмите ***«Далее»***. В следующем окне укажите формат, который вы хотите использовать ***«Файлы X.509 (.CER) в кодировке DER»*** (Рисунок 7).

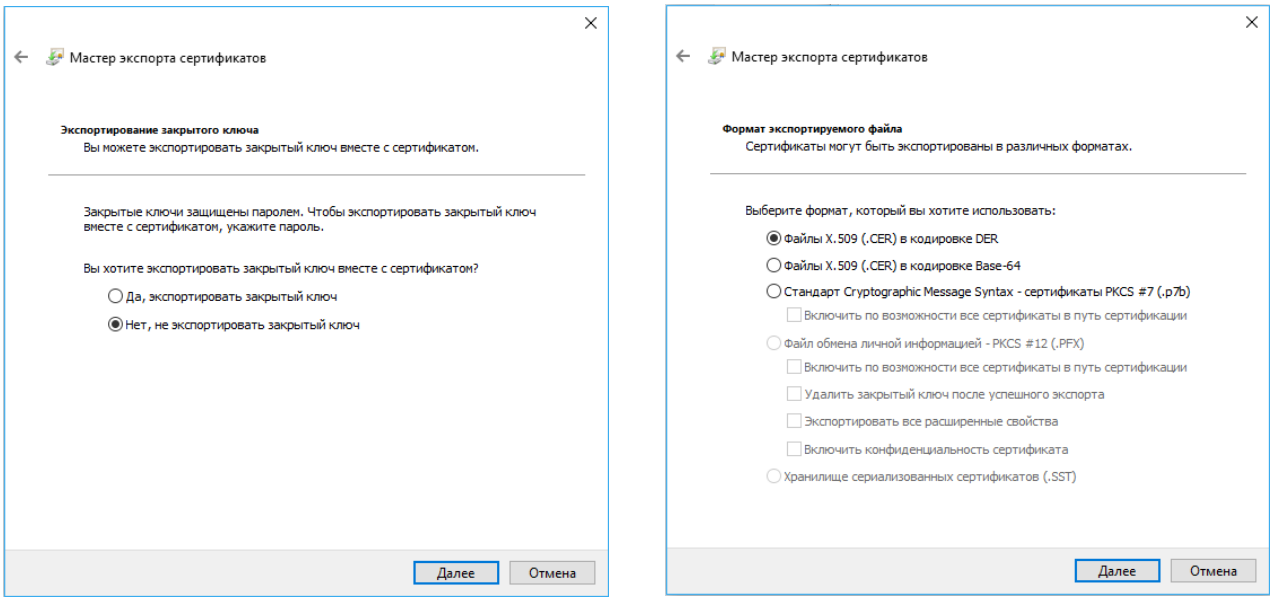

Рисунок 7

5. Нажмите ***«Обзор»*** и укажите каталог, куда вы хотите сохранить сертификат, на примере мы сохраняем сертификат на рабочем столе, задав ему имя. (Рисунок 8).

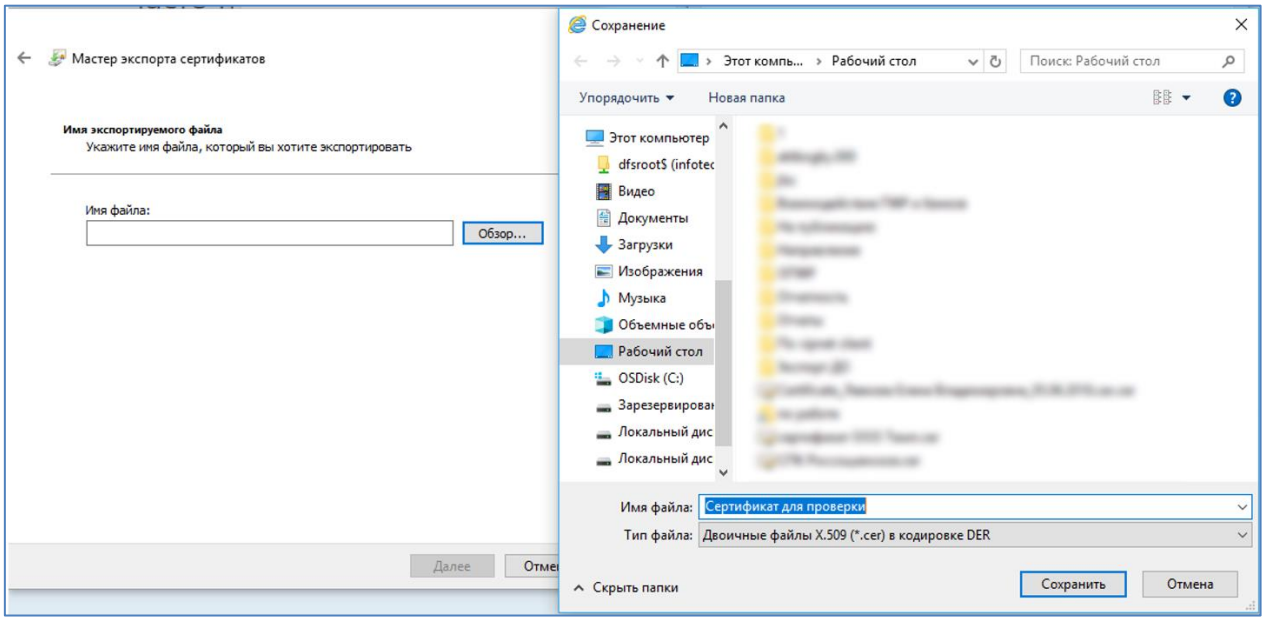

Рисунок 8

6. Нажмите ***«Далее»***, затем ***«Готово»*** (Рисунок 9).

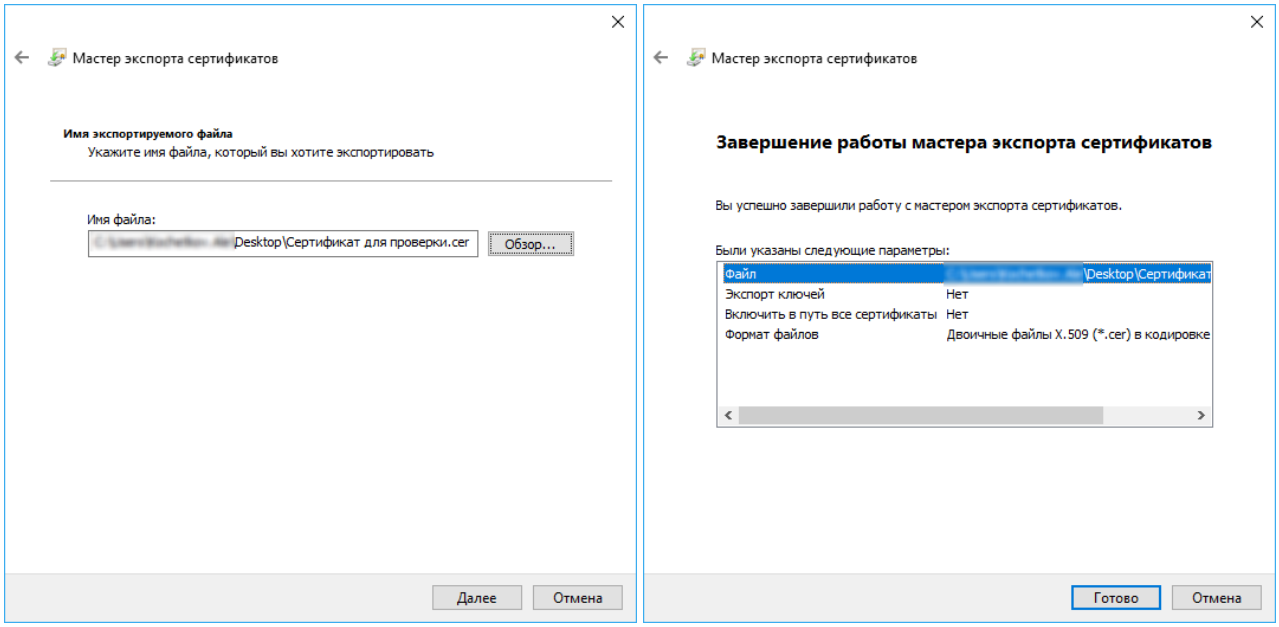

Рисунок 9

7. В результате Ваш сертификат (файл с расширением *.cer) будет сохранен в указанном каталоге.

VII. Доступ к ФГИС Росаккредитации

Для получения доступа к ФГИС Росаккредитации необходимо:

А. Отправить заявку на подключение нового пользователя

Б. Отправить заявку на получение ключевого набора для ViPNet Client

Опишем каждый из них подробнее, при необходимости выполнить **каждый пункт**.

А. Заявка на подключение нового пользователя

1. Для отправки заявки на подключение нового пользователя перейдите на сайт ФГИС Росаккредитации в раздел «Интерактивный помощник» по ссылке: https://support.fsa.gov.ru/. Откройте стандартизированную форму для подключения пользователя последовательно нажав кнопки: ***Доступ к ФГИС Росаккредитации*** / ***Подключение к ФГИС*** / ***Подключение нового пользователя*** / ***«Отправить заявку на подключение нового пользователя»*** (Рисунок 10, позиции А, Б, В, Г).

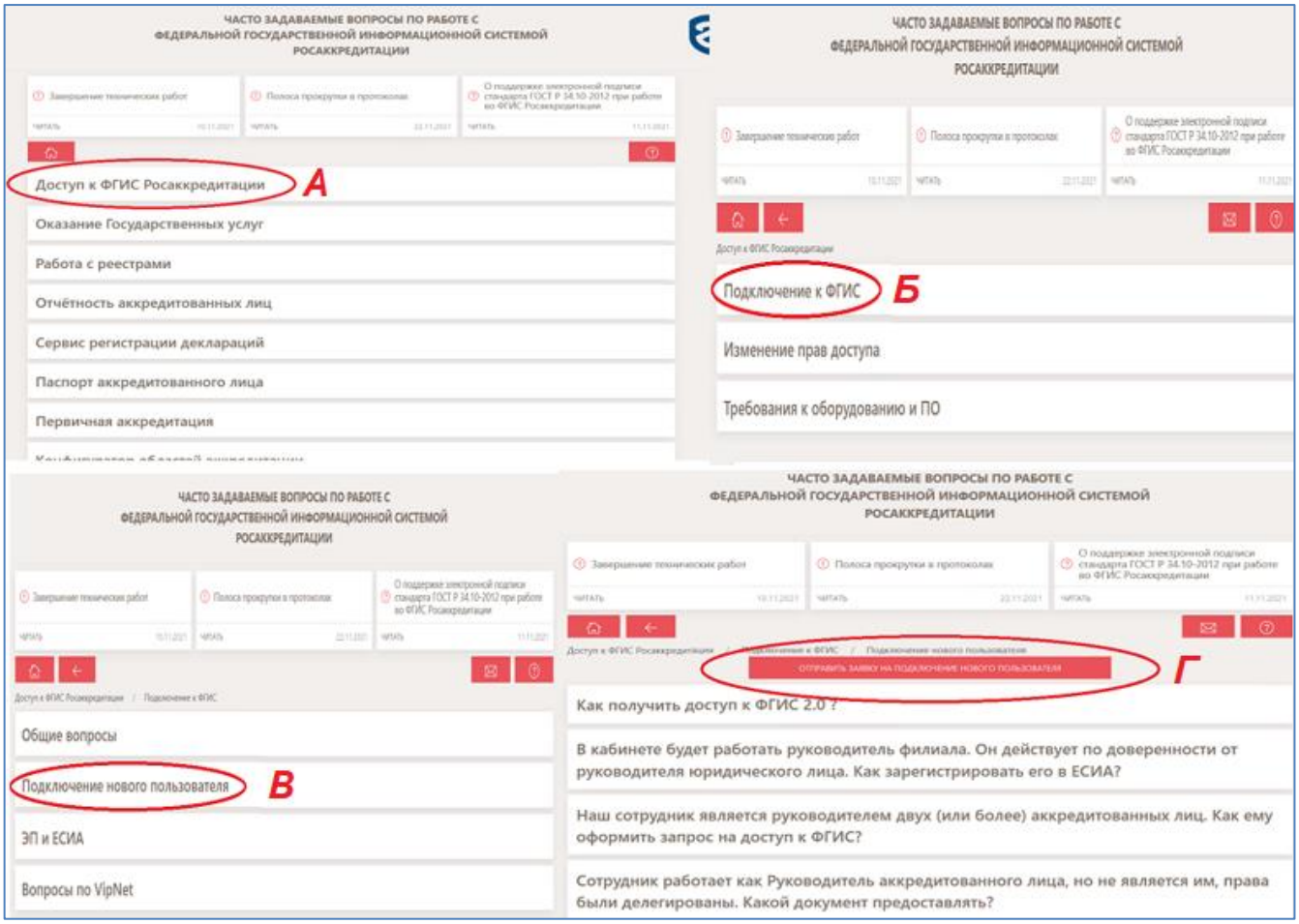

Рисунок 10

2. Заполните страницу заявки для подключения пользователя (Рисунок 11). Загрузите шаблон формы запроса в формате .docx (Рисунок 11, позиция А). Заполните его и загрузите скан-копию во вложения (Рисунок 11, позиция Б). Нажмите кнопку ***«Отправить»***.

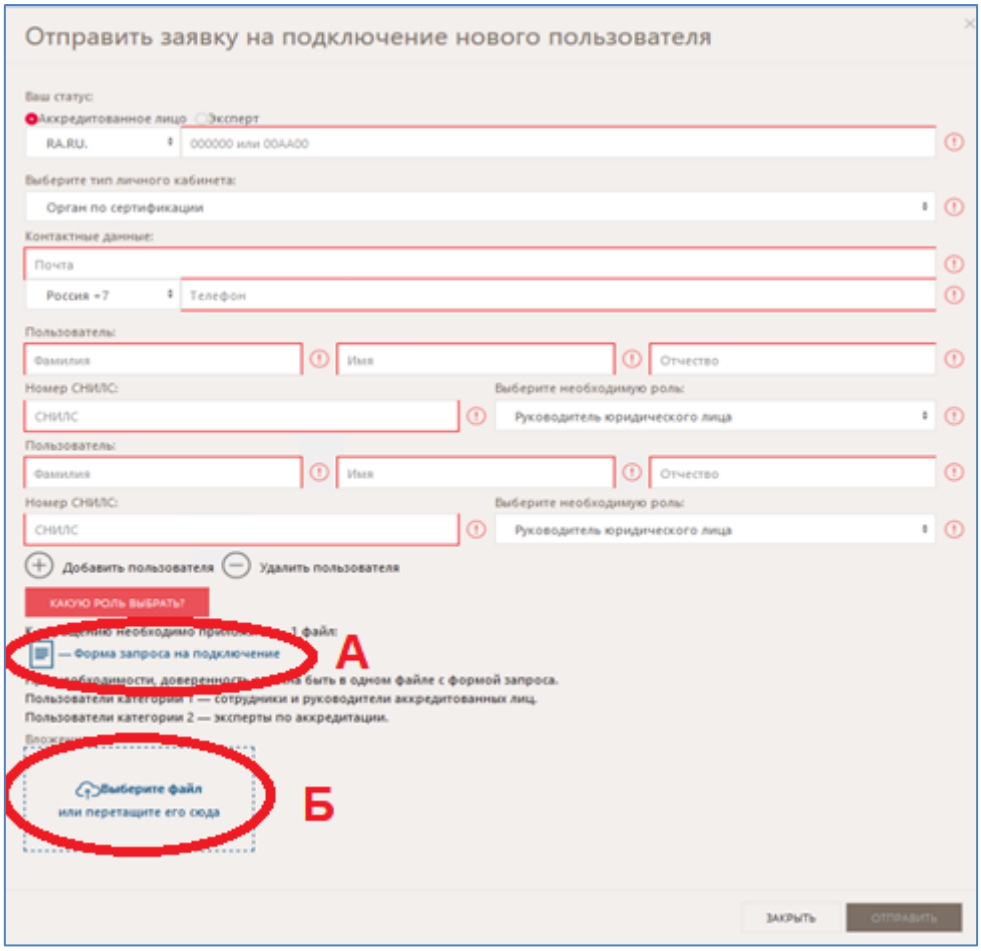

Рисунок 11

Б. Заявка на получение ключевого набора для ViPNet Client

1. Для отправки заявки на получение ключевого набора для ViPNet Client перейдите на сайт ФГИС Росаккредитации в раздел «Интерактивный помощник» по ссылке: https://support.fsa.gov.ru/. Откройте стандартизированную форму для получения ключевого набора последовательно нажав кнопки: ***Доступ к ФГИС Росаккредитации*** / ***Подключение к ФГИС*** / ***Вопросы по ViPNet*** / ***Получить/перевыпустить ключевой набор для ViPNet»*** (Рисунок 12, позиции А, Б, В, Г).

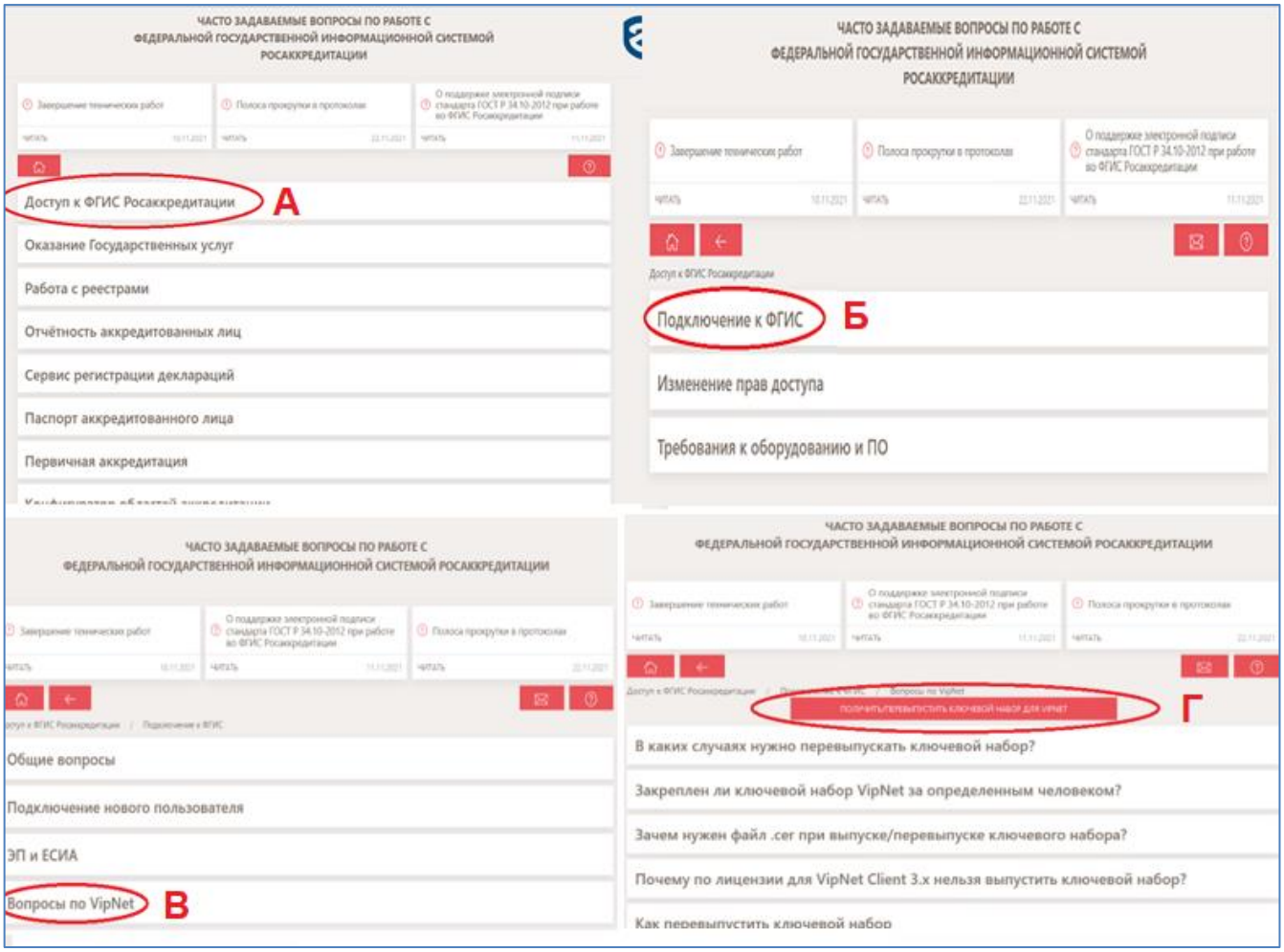

Рисунок 12

2. Заполните страницу заявки на получение ключевого набора для ViPNet Client (Рисунок 13). Загрузите шаблон формы запроса ключевого набора в формате .docx и заполните его (Рисунок 13, позиция А). Далее необходимо загрузить 3 файла во вложения (Рисунок 13, позиция Б): ***Лицензию на ViPNet Client***, заполненную ***форму запроса в формате .docx*** и ***файл сертификата с расширением .cer***, полученный в разделе VI, пункт 7[3]. Нажмите кнопку ***«Отправить»***.

3. По электронной почте пользователь должен получить зашифрованный на его сертификат файл(ы) первичной инициализации абонентского пункта (*.dst) в сети «2936 ФСА».

3 Способ выгрузки сертификата из КриптоПро CSP и ViPNet CSP также описан во встроенной подсказке, кнопка **Как получить файл сертификата ЭП «.CER»**

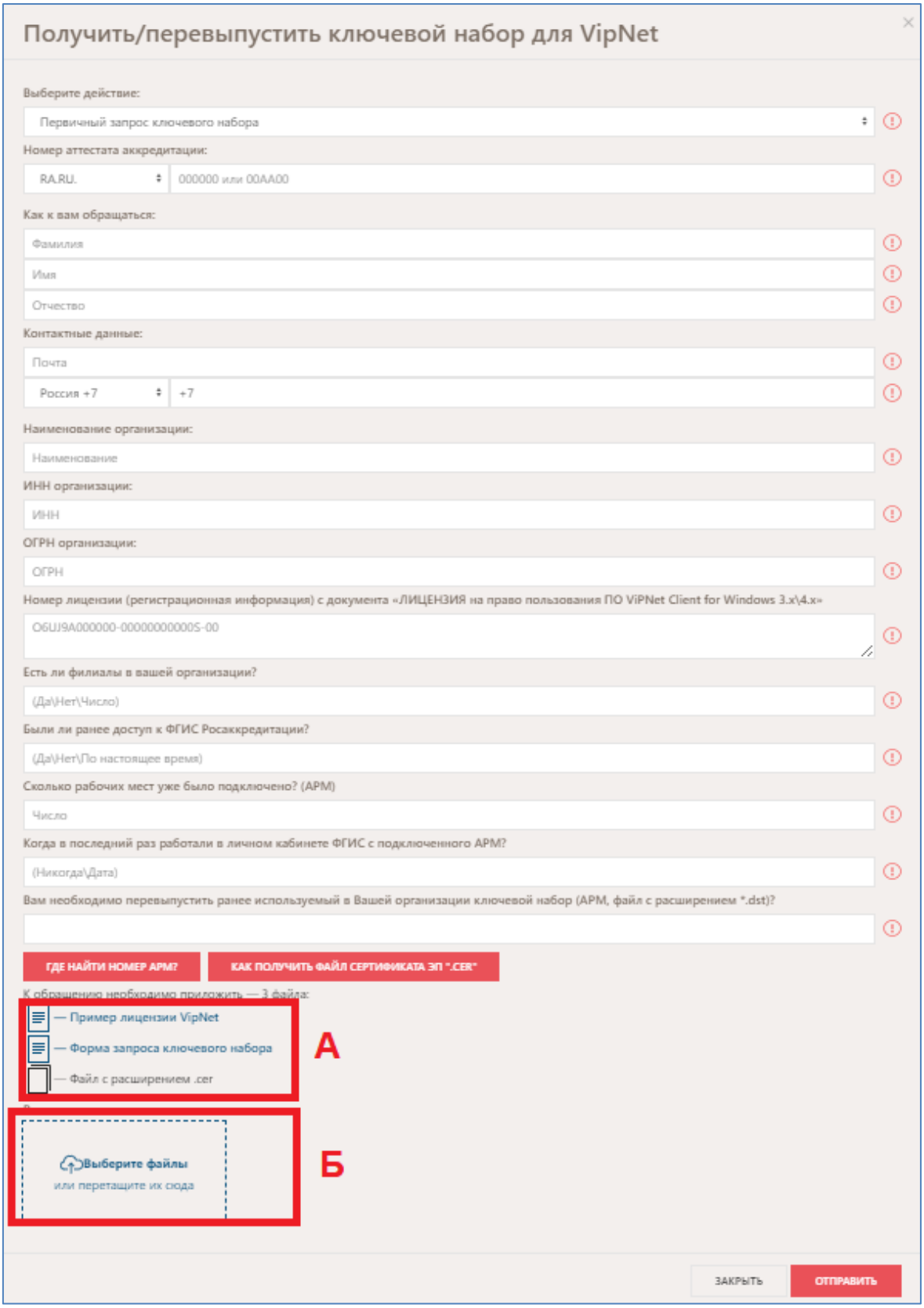
Получить/перевыпустить ключевой набор для VipNet
Выберите действие:
Первичный запрос ключевого набора
Номер аттестата аккредитации:
RA.RU.
000000 или 00AA00
Как к вам обращаться:
Фамилия
Имя
Отчество
Контактные данные:
Почта
Россия +7
+7
Наименование организации:
Наименование
ИНН организации:
ИНН
ОГРН организации:
ОГРН
Номер лицензии (регистрационная информация) с документа «ЛИЦЕНЗИЯ на право пользования ПО ViPNet Client for Windows 3.x\4.x»
O6UJ9A000000-000000000000S-00
Есть ли филиалы в вашей организации?
(Да\Нет\Число)
Были ли ранее доступ к ФГИС Росаккредитации?
(Да\Нет\По настоящее время)
Сколько рабочих мест уже было подключено? (АРМ)
Число
Когда в последний раз работали в личном кабинете ФГИС с подключенного АРМ?
(Никогда\Дата)
Вам необходимо перевыпустить ранее используемый в Вашей организации ключевой набор (АРМ, файл с расширением *.dst)?
ГДЕ НАЙТИ НОМЕР АРМ?
КАК ПОЛУЧИТЬ ФАЙЛ СЕРТИФИКАТА ЭП ".CER"
К обращению необходимо приложить — 3 файла:
— Пример лицензии ViPNet
— Форма запроса ключевого набора
— Файл с расширением .cer
А
Выберите файлы
или перетащите их сюда
Б
ЗАКРЫТЬ
ОТПРАВИТЬ

Рисунок 13

VIII. 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 https://iitrust.ru/downloads/cryptofile/vipnet_cryptofile.zip
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 АО «ИнфоТеКС Интернет Траст» по т. +7 (495) 137-70-47 или по бесплатному номеру 8-800-250-0-265 (кроме звонков из Москвы).

4. Добавьте полученный от ФГИС Росаккредитации файл в список ViPNet CryptoFile нажав кнопку ***«Добавить»*** (Рисунок 14).

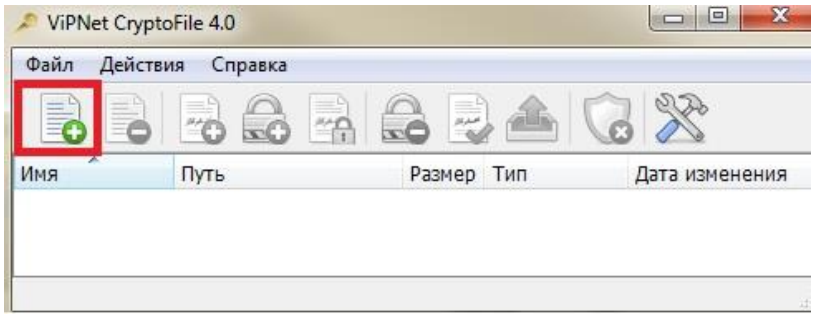

Рисунок 14

5. Выделите данный файл в списке и нажмите кнопку ***«Расшифровать»*** (Рисунок 15).

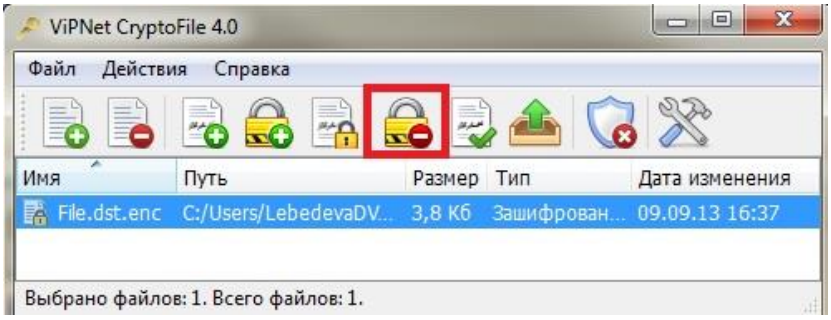

Рисунок 15

6. При необходимости введите пин-код[4] 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.

[4] По умолчанию PIN-код на устройство JaCarta LT:

- если носитель получен до 15.01.2019: **1eToken**
- с 15.01.19 года PIN -код устанавливается **1234567890**

IX. Установка и инициализация ViPNet Client

Для получения доступа к защищенному ресурсу ФГИС Росаккредитации и установке защищенного соединения используется ПО «ViPNet Client 4.x (КС3)»[5].

Перед установкой ПО ViPNet Client убедитесь, что на компьютере выполнены стандартные сетевые настройки, а также правильно заданы часовой пояс, дата и время. На компьютере не должны быть установлены сторонние межсетевые экраны (firewall). Установку должен выполнять пользователь, обладающий правами администратора в ОС Windows.

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. Примите условия лицензионного соглашения и нажмите кнопку «Установить» (Рисунок 16). При необходимости можно добавить/убрать компоненты программы, изменить каталог установки, нажав на «Компоненты и параметры».

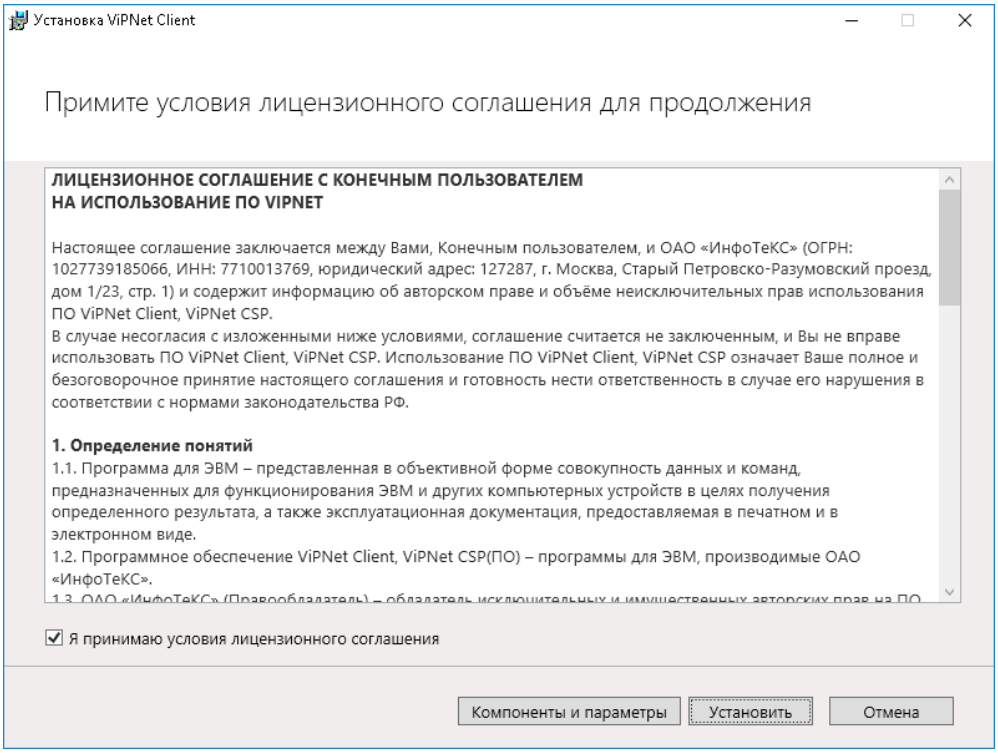

Рисунок 16

4. После окончания установки перезагрузите компьютер.
5. 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 программу установки ключей сети ViPNet, дважды щелкнув файл дистрибутива ключей (*abn_XXXX.dst*).
   - ✓ Убедитесь, что выбран дистрибутив ключей, предназначенный именно для текущего сетевого узла. Имя сетевого узла и имя пользователя отображаются ниже поля для указания пути к файлу дистрибутива. Нажмите кнопку «Установить» (Рисунок 17).

[5] По вопросу получения дистрибутива ViPNet Client на CD-диске, включая комплект эксплуатационной документации, формуляр, копию сертификата соответствия необходимо обращаться к партнерам АО «ИнфоТеКС».

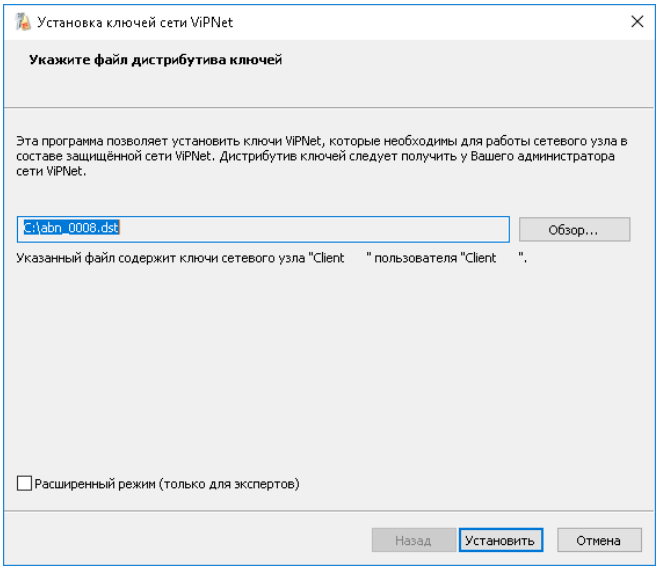

Рисунок 17

- ✓ После успешной установки ключей можно запустить ПО ViPNet Client. В дальнейшем программа будет запускаться автоматически, аутентификацию в ViPNet Client необходимо выполнять перед входом в операционную систему.

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

Для этого в Интернет-обозревателе введите адрес: http://10.250.74.17/ для новой версии портала, либо если Вам необходимо работать в старой версии портала http://10.250.4.13 (Рисунок 18). Страница должна быть доступна.

Если страница недоступна, необходимо обратиться в службу технической поддержки компании, у которой приобретали ПО ViPNet Client и сертификат технической поддержки, для получения дальнейших инструкций.

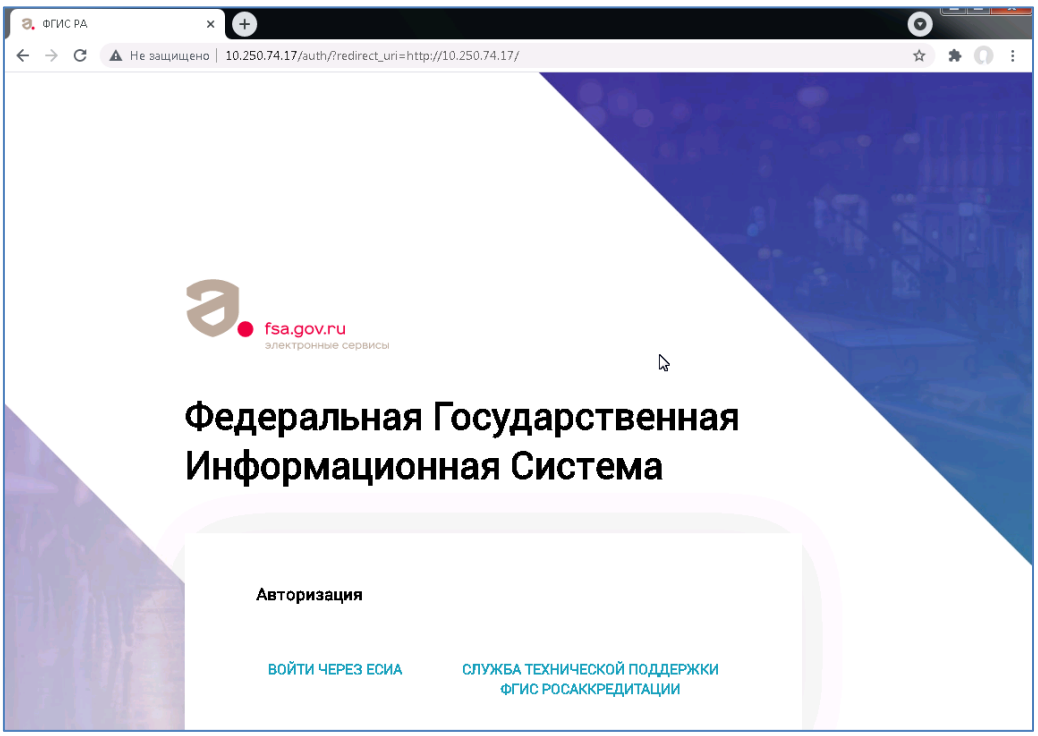

Рисунок 18

Для более подробной информации об установке и настройке ViPNet Client воспользуйтесь инструкцией «ViPNet Client 4. Быстрый старт», входящей в состав эксплуатационной документации ViPNet, а также размещенной по адресу https://files.infotecs.ru/_dl/sess/vipnet_client_4/docs/vipnet_client_4x_doc_rus.zip

При необходимости дополнительных настроек ViPNet Client, отвечающих за функционирование абонентского пункта в сети «2936 ФСА» используйте «ViPNet Client 4. Руководство пользователя», входящей в состав эксплуатационной документации ViPNet, а также размещенной по адресу https://files.infotecs.ru/_dl/sess/vipnet_client_4/docs/vipnet_client_4x_doc_rus.zip.

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