

Инструкция
по настройке ПО ViPNet Client 4.x (КСЗ) для
подключения к сети 2936 ФГИС
Росаккредитации

версия документа 2019 г.

ОГЛАВЛЕНИЕ

I. ВВЕДЕНИЕ	3
II. НЕОБХОДИМЫЕ КОМПОНЕНТЫ.....	4
III. ТРЕБУЕМЫЙ СОСТАВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АРМ.....	5
IV. РУКОВОДСТВО ПО ПОЛУЧЕНИЮ КН	6
V. РАСШИФРОВАНИЕ ПОЛУЧЕННОГО КН	7
VI. УСТАНОВКА И ИНИЦИАЛИЗАЦИЯ ПО VIPNET CLIENT 4.X.....	8
VII. ПРОВЕРКА КОНФИГУРАЦИИ ПО VIPNET CLIENT 4.X.....	14
VIII. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ	18

I. Введение

Документ предназначен для пользователей, осуществляющих самостоятельную установку программного обеспечения (далее – ПО) ViPNet Client 4.x, необходимого для подключения к сети 2936 ФГИС Росаккредитации. Для правильной работы необходимо выполнить все пункты данного руководства в указанной последовательности.

Сокращения и обозначения:

АП – Абонентский пункт

АРМ – Автоматизированное рабочее место

ЕСИА – Единая система идентификации и аутентификации

КН – Ключевой набор

КСКП – Квалифицированный сертификат ключа проверки электронной подписи

ОС – Операционная Система

ПО – Программное обеспечение

СКЗИ – Средство криптографической защиты информации

УЦ – Удостоверяющий центр

ЭП – Электронная подпись

II. Необходимые компоненты

Для успешного развертывания ПО ViPNet Client на Вашем рабочем месте необходим минимальный набор компонентов, приведенный в таблице 1.

Таблица 1

№ п/п	Компонент	Описание	Где получить
1.	Сертифицированная версия ПО ViPNet Client 4.x (КСЗ) на оптическом носителе	Диск с дистрибутивом ПО ViPNet Client 4.x (КСЗ), включающий также комплект эксплуатационной документации, формуляр и копию сертификата соответствия.	Необходимо обращаться к любому из партнеров ОАО «ИнфоТеКС». Перечень партнеров доступен по ссылке https://infotecs.ru/partners/list/
2.	Лицензия на право пользования ПО ViPNet Client версии 4.x (КСЗ)	Документ на бумажном носителе с серийным номером, подтверждающий право законного приобретения сертифицированной версии ПО. Лицензия является одним из документов, необходимых для получения ключевого набора (см. п.3 настоящей таблицы)	
3.	Ключевой набор (КН) - файл первичной инициализации с расширением *.dst	Файл, содержащий в себе информацию о защищенной сети, необходим для «активации» ПО ViPNet Client. Передается конечному пользователю Росаккредитацией по электронной почте в зашифрованном виде. Представляет собой архив вида ARM-00000.zip.enc	КН необходимо получить непосредственно в Росаккредитации, согласно порядка получения, приведенному на официальном сайте http://fsa.gov.ru/index/statisticview/id/124/ Запросы принимаются на почту fgis@fsa.gov.ru

III. Требуемый состав программного обеспечения АРМ

Для подключения к ресурсам ФГИС Росаккредитации на АРМ пользователя должно быть установлено и настроено следующее ПО:

- Квалифицированная электронная подпись на любом ключевом носителе или без такового;
- Установленный драйвер последней версии для работы с соответствующим ключевым носителем (например, eToken PRO), загруженный с сайта производителя;
- Установленное ПО криптопровайдера. Допускается использование любого сертифицированного криптопровайдера, совместимого с Вашей ЭП (за рекомендациями обратитесь в УЦ, где была получена данная ЭП), например, ViPNet CSP или КриптоПро CSP;
- Дистрибутив ПО КриптоАРМ или любое аналогичное по функционалу ПО;
- Дистрибутив ПО ViPNet Client 4.x (KC3): ознакомьтесь с системными требованиями, указанными в документации на данное ПО. Документация идет в комплекте с дистрибутивом на диске, а также доступна по ссылке <https://infotecs.ru/product/vipnet-client-.html>;
- КН, необходимый для первичной инициализации ПО ViPNet Client, полученный от Росаккредитации в зашифрованном архиве **ARM-00000.zip.enc**. В архиве содержится файл первичной инициализации с расширением ***.dst**, необходимый для «активации» ПО, и текстовый файл с паролем, имеющий расширение ***.xps**.

IV. Руководство по получению КН

Для получения КН необходимо отправить на адрес электронной почты fgis@fsa.gov.ru запрос на бланке организации заявителя по форме, представленной на официальном сайте Росаккредитации:

http://fsa.gov.ru/public/uploads/usr/Zapros_connect_FGIS.docx

п. 4.5 [Порядка получения доступа информационным ресурсам ФГИС Росаккредитации.](#)

К запросу необходимо приложить открытую часть квалифицированной электронной подписи – это файл сертификата с расширением ***.cer**, полученный пользователем в УЦ, и скан лицензии на право пользования ПО ViPNet Client 4.x (КСЗ).

В письме необходимо указать информацию о количестве рабочих мест, на которых будет устанавливаться приобретённое ПО ViPNet Client 4.x (КСЗ).

В ответ на отправленное письмо пользователь получит архив, зашифрованный на предоставленном сертификате, имеющий вид **ARM-00000.zip.enc**.

V. Расшифрование полученного КН

Зашифрованный архив **ARM-00000.zip.enc** содержит в себе файлы (*.dst и *.xps), которые необходимы для первичной инициализации «активации» ПО ViPNet Client 4.x.

Для расшифрования полученного от Росаккредитации архива рекомендуется использовать бесплатное ПО, приведенное в таблице 2, или любое другое, аналогичное по функционалу ПО.

Таблица 2

Криптопровайдер	ПО для расшифрования и документация к нему
КриптоПро CSP	КриптоАРМ http://www.trusted.ru/products/cryptoarm/about/
ViPNet CSP	ViPNet PKI Client (демо-версия) https://infotecs.ru/product/vipnet-pki-client.html

Расшифрование архива необходимо произвести согласно документации к программному обеспечению.

Перед расшифрованием архива, содержащего КН, у пользователя на АРМ должна быть корректно развернута квалифицированная электронная подпись. При возникновении проблем с развертыванием квалифицированной электронной подписи необходимо обратиться в УЦ, выдавшего данную электронную подпись.

VI. Установка и инициализация ПО ViPNet Client

Для подключения АРМ пользователей к ФГИС Росаккредитации используется ПО ViPNet Client 4.x (КСЗ).

Перед установкой ПО ViPNet Client убедитесь, что на компьютере выполнены стандартные сетевые настройки, доступна работа в сети Интернет, а также правильно заданы часовой пояс, дата и время. Проконсультируйтесь с Вашим системным администратором и убедитесь, что открыт сетевой порт UDP 55777 до адреса 5.143.238.24 в оба направления, на всех сетевых устройствах (прокси-сервере, межсетевом экране и т.д.). **В ОС Windows 10, если не установлено антивирусное ПО, может потребоваться активировать встроенное средство антивирусной защиты Defender.**

Для установки ViPNet Client необходимо выполнить следующие действия:

- Запустите файл **setup.exe**, расположенный на диске с дистрибутивом;
- Выполните установку ViPNet Client, следуя инструкциям мастера установки;
- В появившемся окне поставьте галочку о принятии лицензионного соглашения и нажмите «Продолжить».

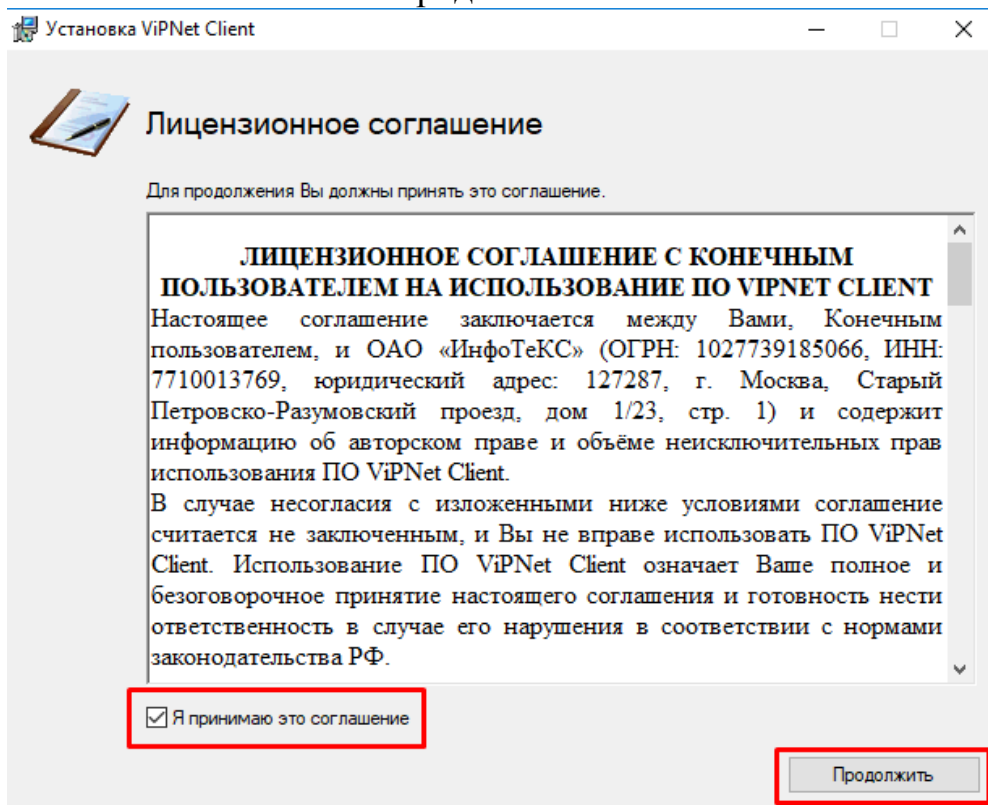


Рисунок 1

- Продолжите установку, нажав «Установить сейчас», рисунок 2;

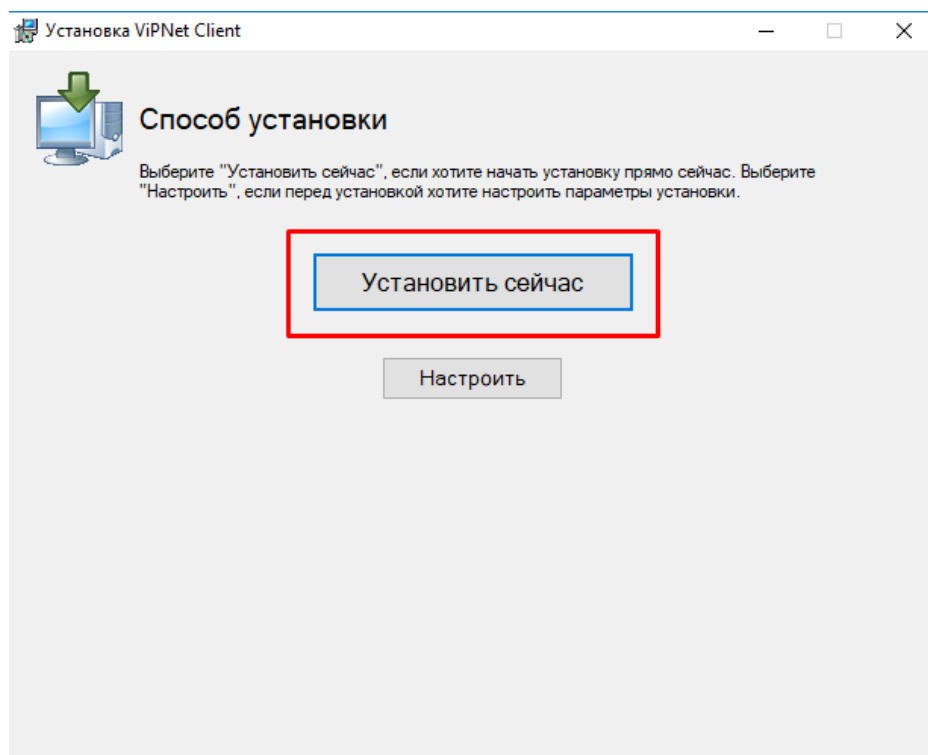


Рисунок 2

- После окончания установки появится сообщение об успешном завершении установки, нажмите «**Заккрыть**»;

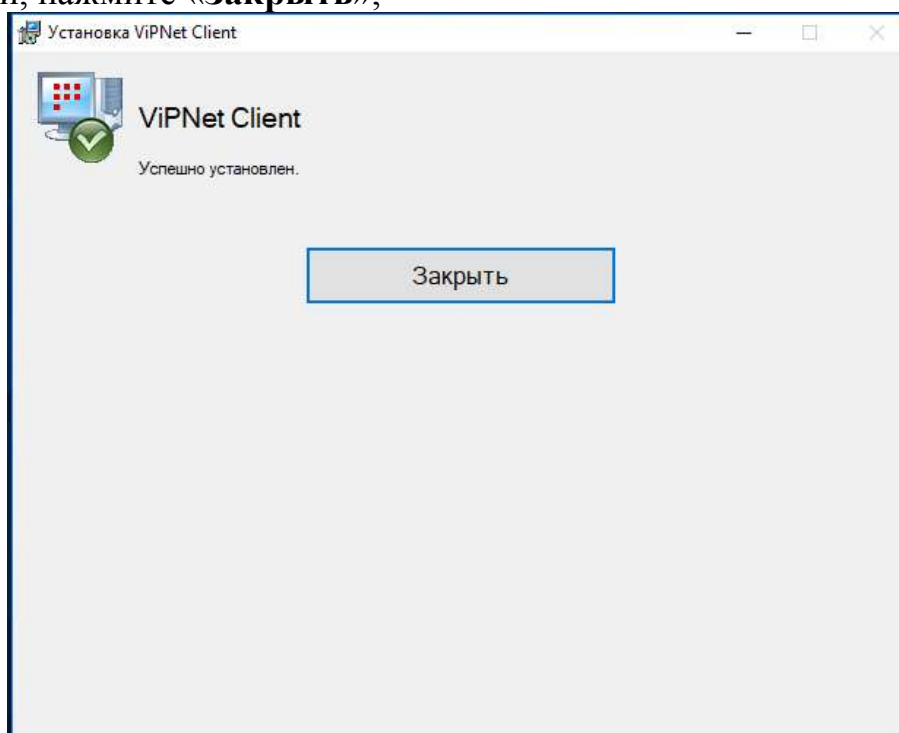


Рисунок 3

- По завершении установки ViPNet Client мастер установки предложит установить ключи, нажмите «**Нет**», как изображено на рисунке 4.

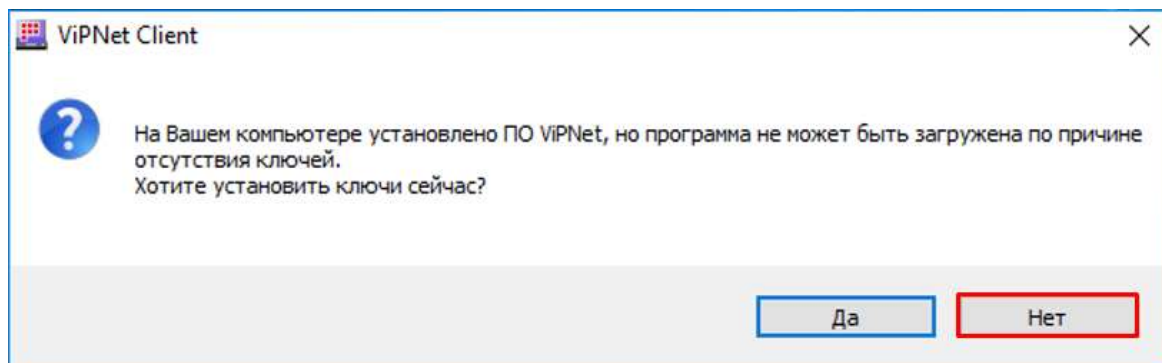


Рисунок 4

- Расшифрованный ключевой набор (см. п.п. V. **Расшифрование полученного КН**), полученный от Росаккредитации, имеющий расширение ***.dst**, кликнуть двойным щелчком мыши, у Вас откроется окно «Установка ключей сети ViPNet».

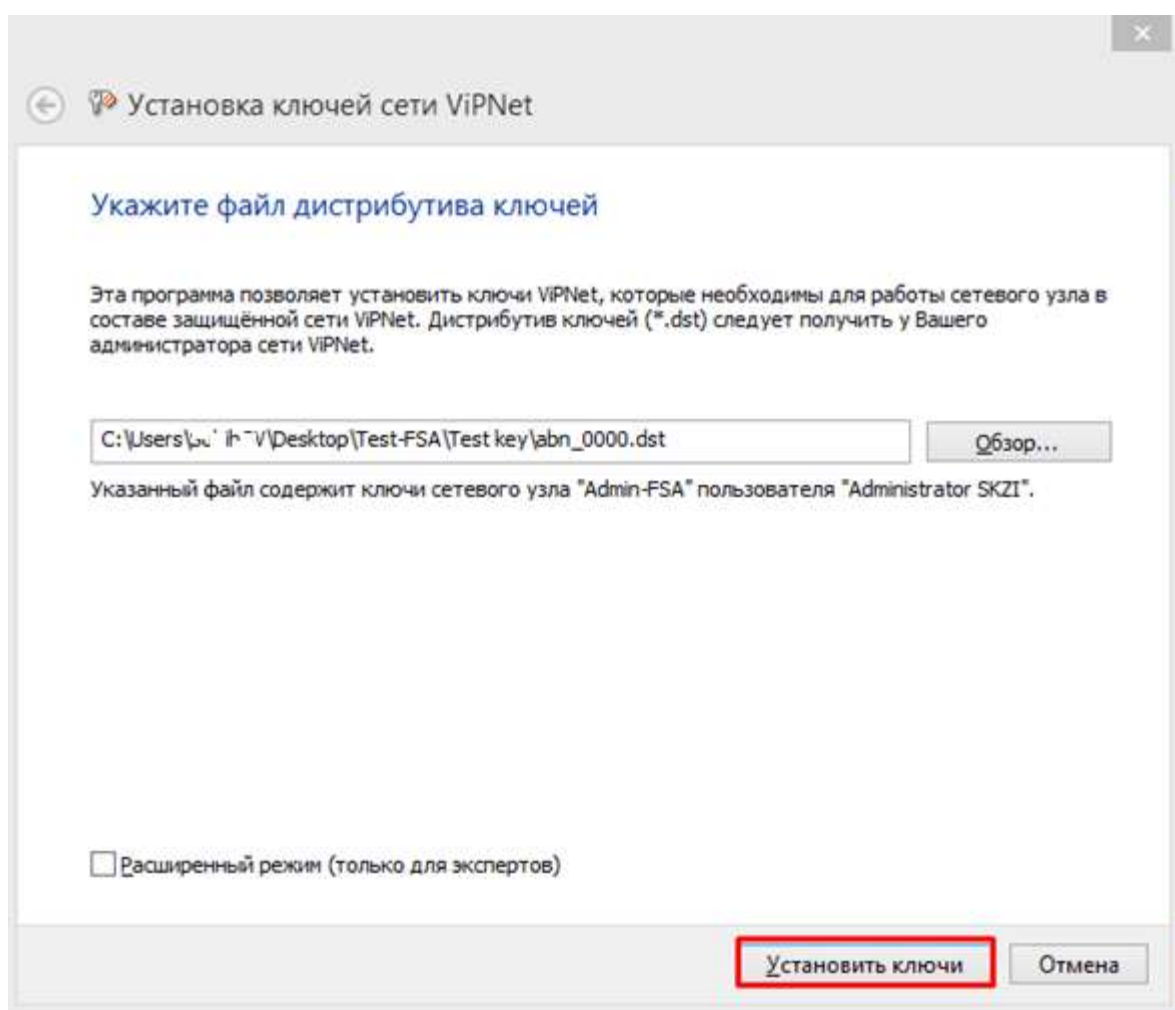


Рисунок 5

- Нажмите кнопку «Установить ключи».

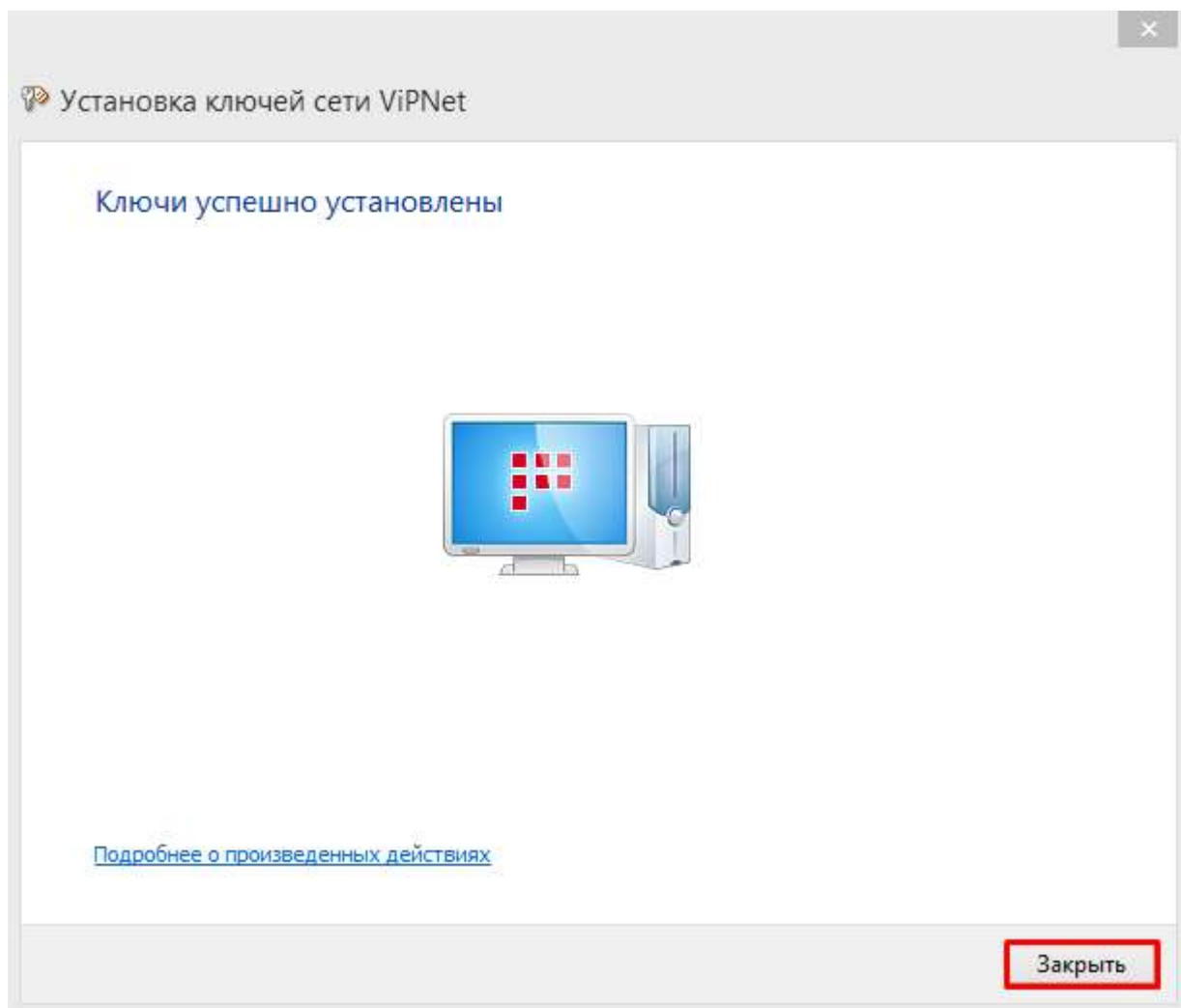


Рисунок 6

- Первичная инициализация выполняется **один раз** при установке программы ViPNet Client и в дальнейшем для запуска программы не требуется. Файл *.dst и текстовый файл с паролем (00000000NazvanieOrganizacii.xps, где 00000000 – это ИНН организации заявителя) необходимо сохранить, так как они понадобятся Вам в случае, если потребуется переустановить программу.
- В поиске операционной системы необходимо ввести «Монитор» и запустить ПО. Запустите ПО ViPNet Client 4.x кликом мыши, см. рисунок 7. Также для удобства можно вынести ярлык на рабочий стол.

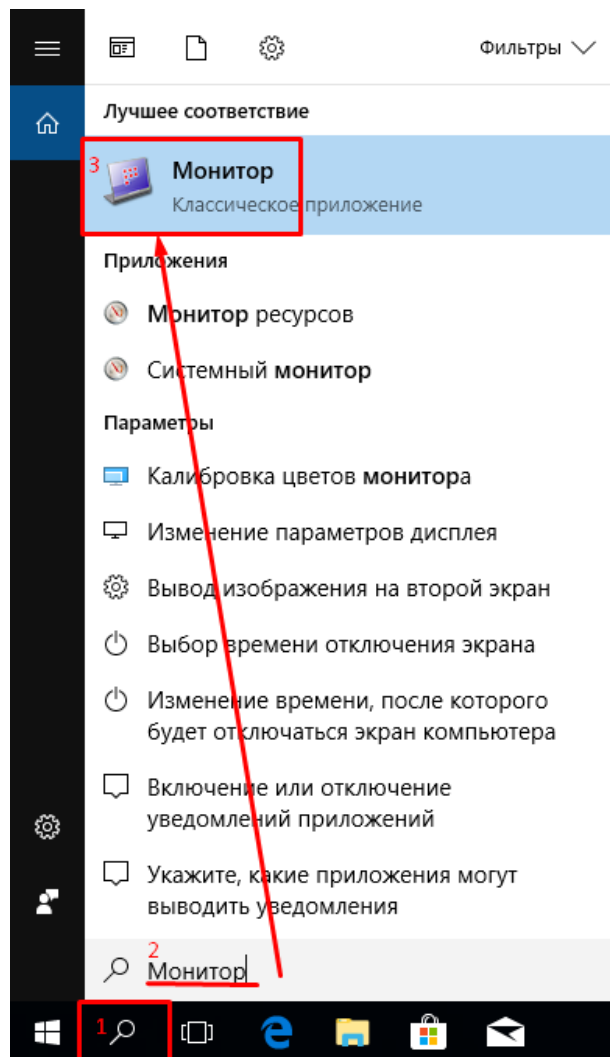


Рисунок 7

- Запустив приложение Монитор, необходимо ввести пароль, указанный в *.xps файле, в форму авторизации, см. рисунок 8.

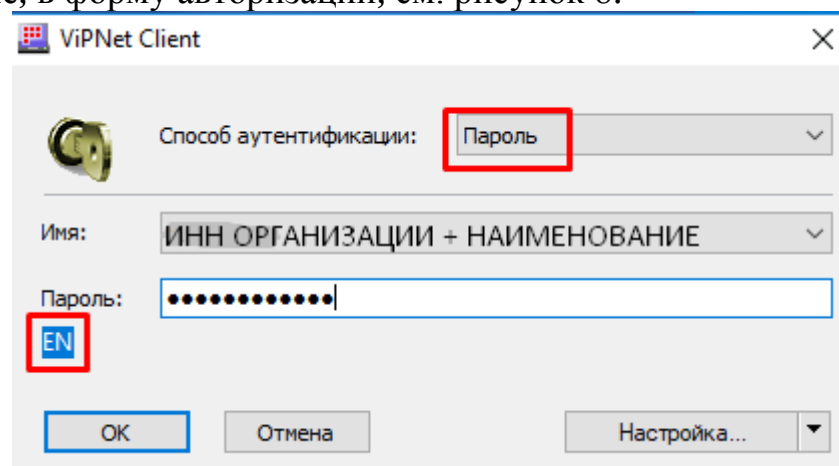


Рисунок 8

- Пароль необходимо запомнить по парольной фразе, указанной в текстовом документе с паролем. Пароль включает первые три буквы каждого слова парольной фразы без пробелов. Вводя пароль, нажимайте русские буквы на клавиатуре, при этом клавиатура должна быть в режиме английской раскладки. **Пример:** Если парольная фраза «Какая смешная парольная фраза», то пароль будет иметь вид rfrcvtgfhahf.

- После проведения первичной инициализации и запуска программы необходимо проверить соединение с узлом «hw5000-Moscow1», являющимся координатором. Для этого в окне программы ViPNet Client [Монитор] щелкните правой клавишей мыши по узлу «hw5000-Moscow1» и в контекстном меню выберите пункт «Проверить соединение», как изображено на рисунке 9.

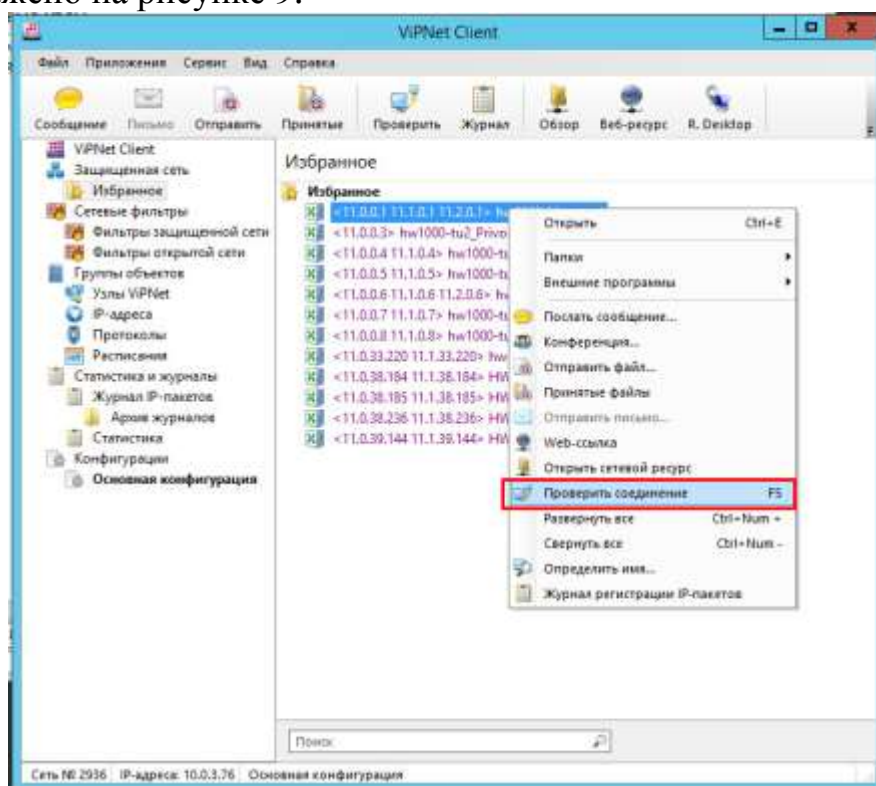


Рисунок 9

Если координатор **hw5000-Moscow1** имеет статус «Доступен», как на рисунке 10, то ПО настроено корректно и подключение прошло успешно.

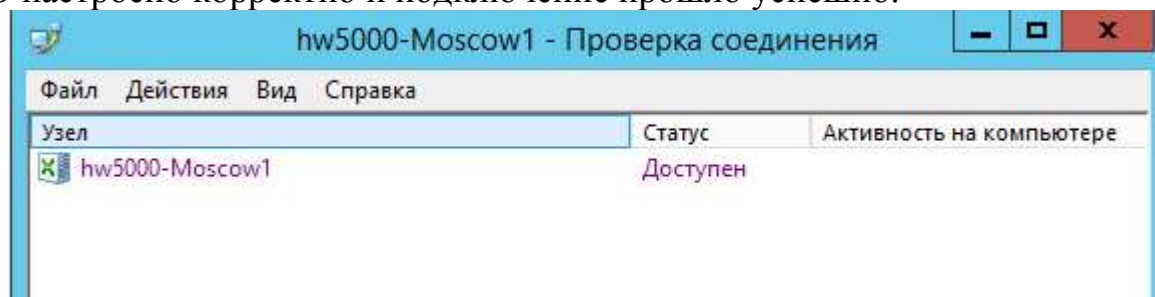


Рисунок 10

С этого момент можно подключиться к защищенным ресурсам на адреса <http://10.250.74.17/> и <http://10.250.4.13/>.

ВНИМАНИЕ! Если адреса <http://10.250.74.17/> и <http://10.250.4.13/> не открываются в браузере, но координатор **hw5000-Moscow1** имеет статус «Доступен» и данные ip-адреса пингуются с Вашего АРМ, необходимо выполнить действия, приведённые в п. VII. Проверка конфигурации ПО ViPNet Client 4.x.

Настоятельно рекомендуется не менять конфигурации ViPNet Client, чтобы не нарушить работоспособность ПО.

VII. Проверка конфигурации ПО ViPNet Client 4.x

При необходимости проверить настройки ViPNet Client [Монитор], в окне ViPNet Client [Монитор] откройте вкладку «Защищенная сеть» и в списке узлов выберите «hw5000-Moscow1», дважды щелкните по нему левой клавишей мыши. В появившемся окне «Свойства узла (hw5000-Moscow1)», во вкладке «Туннель» проверьте, снята ли галочка в пункте «Использовать виртуальные IP – адреса». Если необходимо, снимите ее и подтвердите действие кнопкой «Применить». Также проверьте, есть ли узлы в списке реальных IP-адресов для ФГИС 1.0: 10.250.4.12, 10.250.4.13, 10.250.4.18 и для ФГИС 2.0: 10.250.74.12, 10.250.74.17, 10.250.74.20, 10.250.74.23. Пример на рисунке 11.

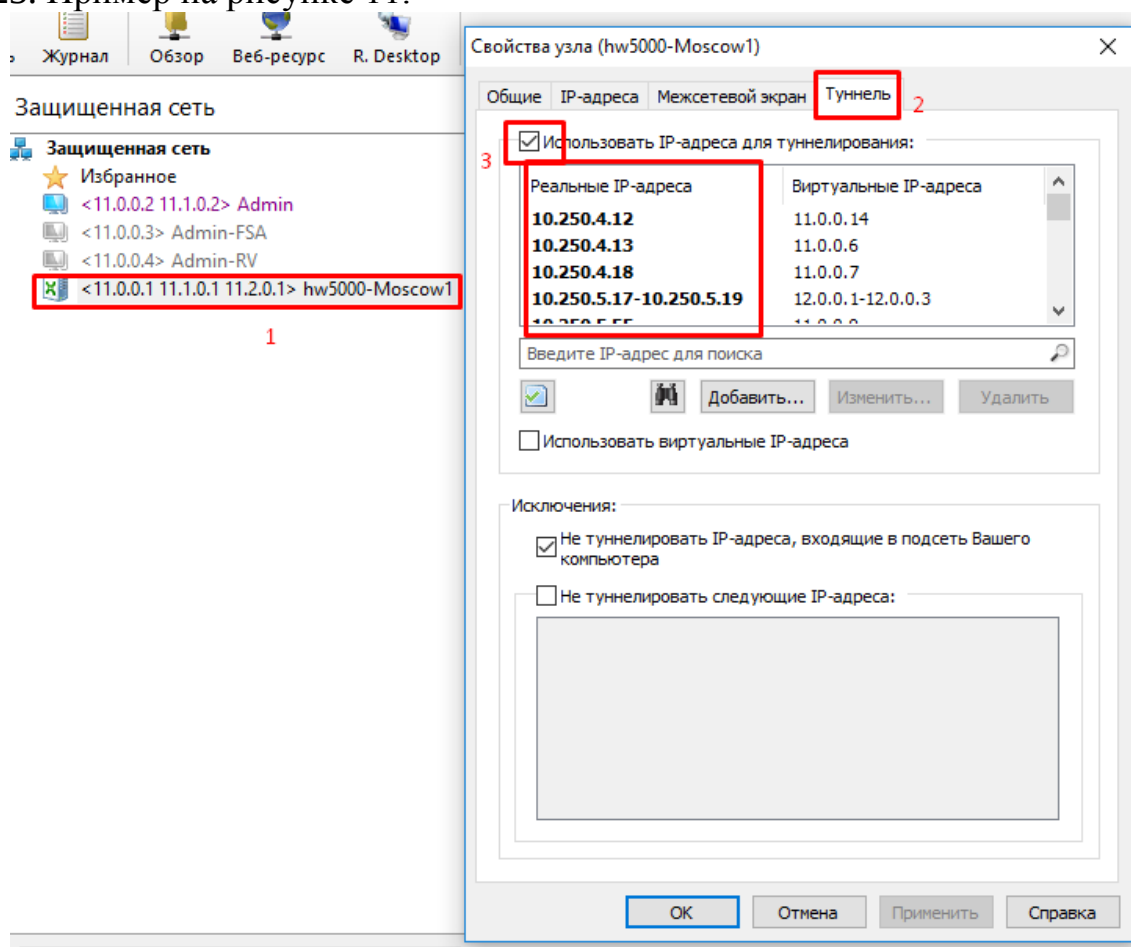


Рисунок 11

Далее необходимо проверить, отключен ли режим работы «Весь трафик направлять через сервер соединений». Для этого откройте пункт меню «Сервис» в окне программы ViPNet Client [Монитор] и выберите пункт «Настройка приложения» рисунок 12.

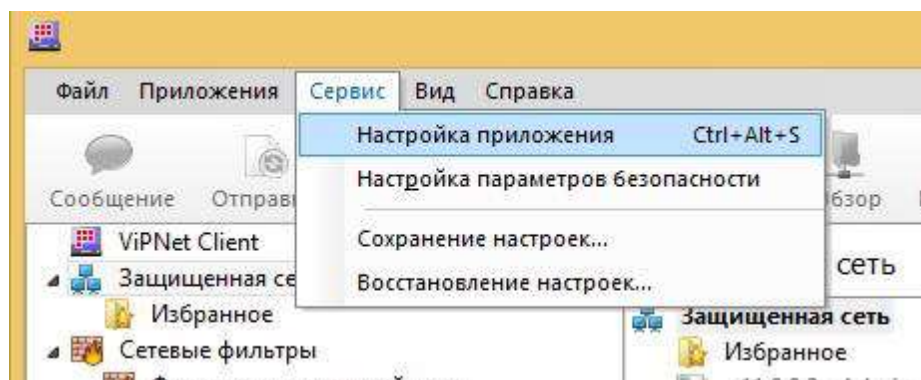


Рисунок 12

В открывшемся окне «Настройки» нажмите вкладку «Показать дополнительные настройки», галочка в пункте «Весь трафик направлять через сервер соединений» должна быть снята, см. рисунок 13.

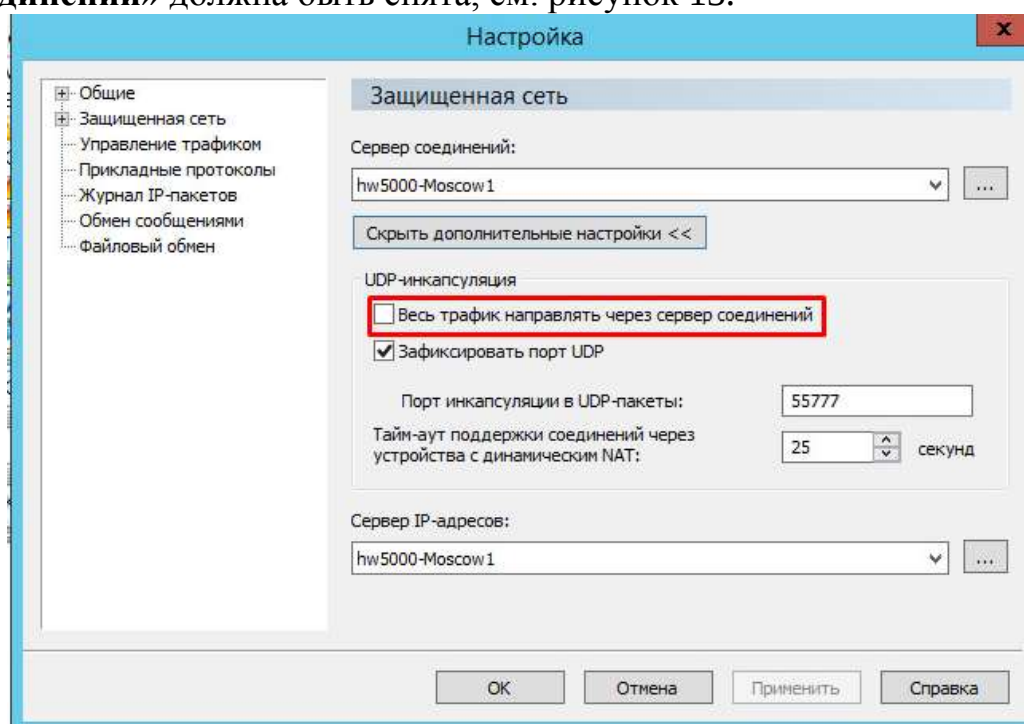


Рисунок 13

Поставьте галочку в пункте «**Зафиксировать порт UDP**» и прописать «**Порт инкапсуляции в UDP-пакеты**» 55777 как показано на Рисунке 13.

Нажмите кнопку «**Применить**», «**ОК**».

После настройки ПО VipNet Client проверьте функционирование защищенного канала связи для подключения к ФГИС Росаккредитации. (Программа VipNet Client Монитор должна быть запущена, и узел HW5000-Moscow1 должен быть доступен, как на рисунке 10.)

Для ФГИС 1.0 (рекомендуется Mozilla) по ссылке <http://10.250.4.13> откроется сайт, изображенный на рисунке 14.

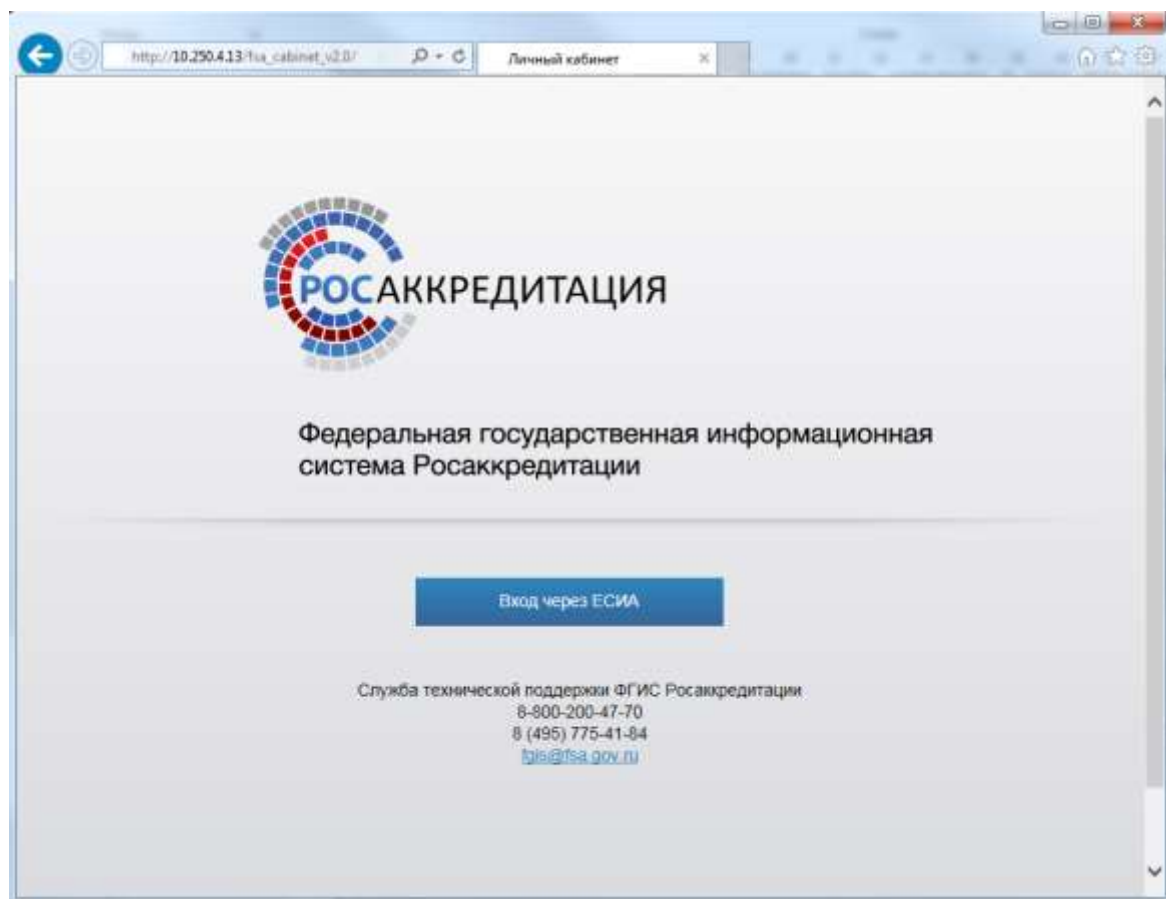


Рисунок 14

Для ФГИС2.0 (рекомендуется Яндекс.Браузер) по адресу <http://10.250.74.17/> откроется сайт, изображенный на рисунке 15.

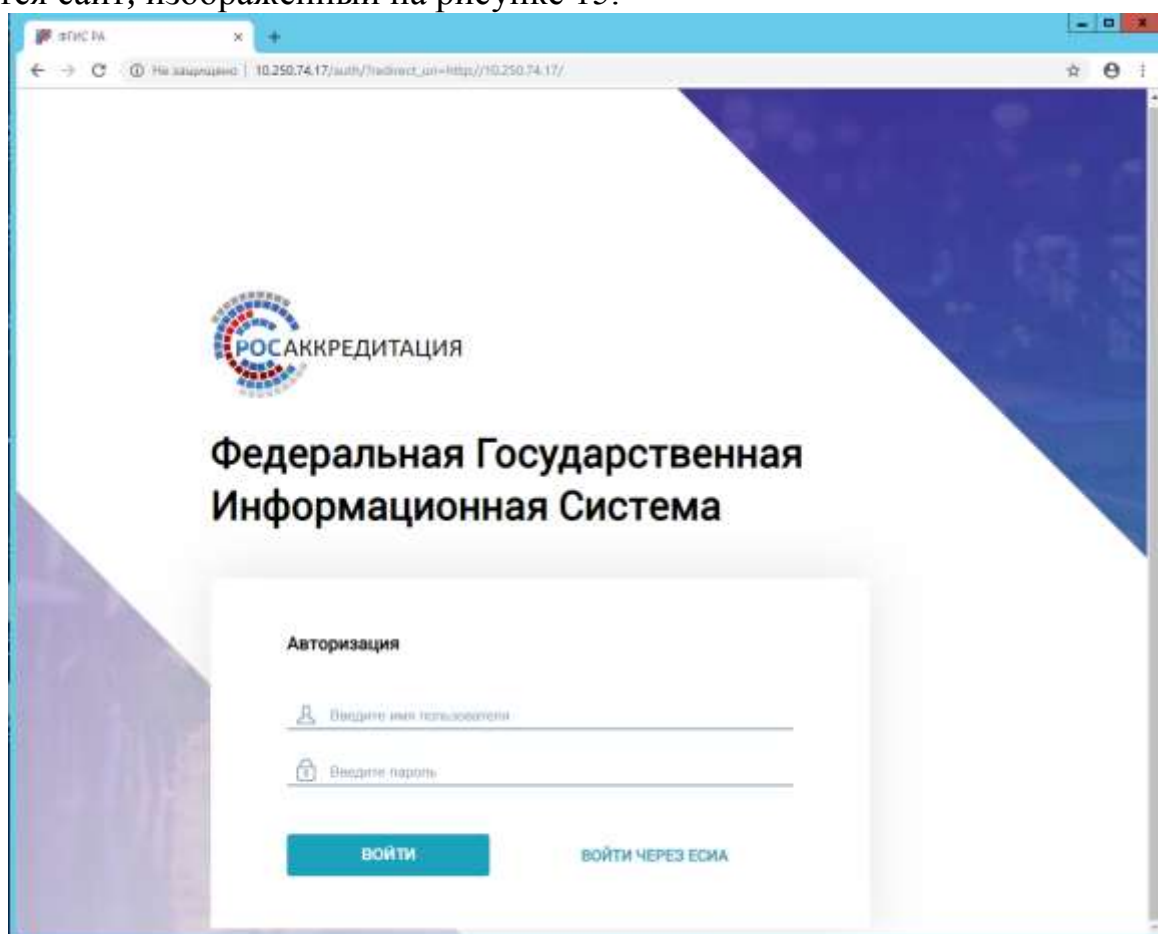


Рисунок 15

При необходимости дополнительных настроек ViPNet Client, отвечающих за функционирование абонентского пункта в сети «2936 ФСА», используйте документ «ViPNet Client [Монитор]. Руководство пользователя» (ViPNet_Client_Monitor_Ru.pdf), входящий в состав эксплуатационной документации ViPNet.

ВНИМАНИЕ!!! Подробную информацию по регистрации в ЕСИА, а также по работе на портале и установке плагина для работы с порталом, можно получить на сайте www.gosuslugi.ru или в Росаккредитации (fgis@fsa.gov.ru). Телефон службы технической поддержки ФГИС Росаккредитации 8-800-200-47-70 доступен в режиме 24 на 7.

VIII. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

ВНИМАНИЕ!!! Официальная поддержка операционной системы Windows XP была прекращена в 2014 г. При любых неполадках ПО, развернутом на данной ОС, техническая консультация не оказывается.

Вопрос: У нас установлен ViPNet CSP. После установки ViPNet Client перестала работать подпись на портале Госуслуг и не проходит авторизация по сертификату в ЕСИА.

Ответ:

Необходимо переустановить ViPNet CSP.

Вопрос: ПО КриптоАРМ при попытке расшифровать присланный файл ключевого набора *.zip.enc выдаёт ошибку. Что делать?

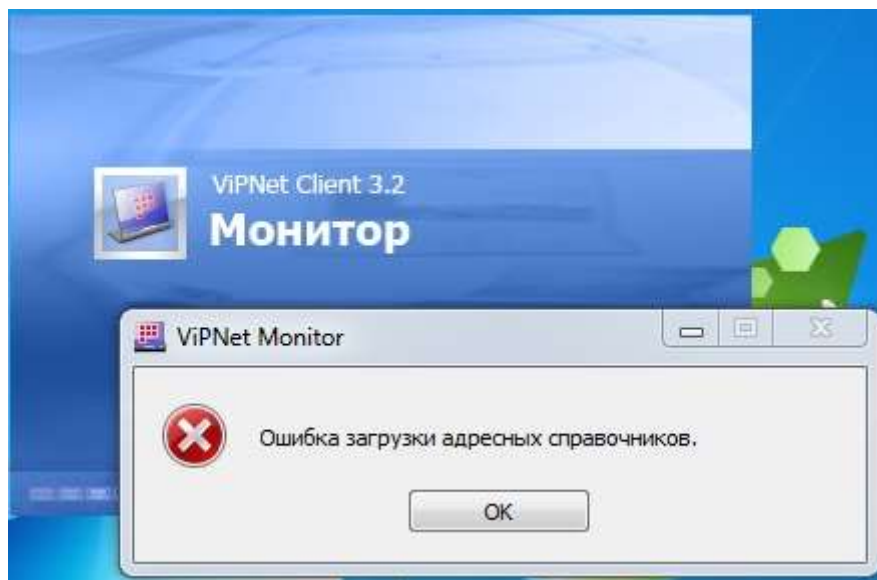
Ответ:

- 1) Причины возникновения ошибки расшифрования КН могут быть следующие:
 - некорректно установлен и настроен криптопровайдер и сертификат ЭП. Необходимо установить и настроить криптопровайдер и сертификат ЭП в соответствии с инструкциями УЦ, где была приобретена электронная подпись;
 - не связаны сертификат ЭП с контейнером ключа ЭП. Связать контейнер с носителем ключа ЭП через криптопровайдер в соответствии с инструкциями УЦ;
 - установлены несколько криптопровайдеров. На рабочем месте должен быть установлен и настроен только один криптопровайдер, указанный в качестве средства ЭП пользователя в распечатке сертификата ключа ЭП;
 - убедиться, что для расшифрования КН используется тот же сертификат ЭП, что и присланный ранее в заявке на получение доступа к ФГИС.
 - 2) Рекомендуются обратиться в УЦ, выдавшего квалифицированную электронную подпись.
-

Вопрос: ViPNet Client 4.x не устанавливается, ошибка 0xD.

Ответ: Удалите антивирусное обеспечение с Вашего ПК и проведите установку ПО ViPNet Client, после чего установите антивирус. Для Windows 10 в панели управления включите встроенное антивирусное ПО Defender.

Вопрос: ViPNet Client 4.x при запуске выдает ошибку, «Ошибка загрузки адресных справочников».



Ответ:

- 1) Скорее всего Вы не провели первичную инициализацию или сделали это с ошибкой, повторите проведение процедуры первичной инициализации согласно Главы VI данной инструкции.
- 2) Попробуйте переустановить ПО ViPNet Client с обязательным удалением папки установки вручную. Если проблема не решена, обратитесь в службу тех. поддержки Росаккредитации или по контактам, указанным в Сертификате на техническое сопровождение ViPNet (при его наличии).
- 3) Направьте скриншот ошибки в техническую поддержку по адресу fgis@fsa.gov.ru. Вам вышлют инструкцию по устранению ошибки.

Вопрос: При запуске ПО ViPNet Client выдает ошибку: "Обнаружены несанкционированно измененные или проверенные с ошибкой файлы журнала событий. ses. crg"

Ответ: Вам необходимо переустановить ViPNet Client. Не забудьте сохранить Ваши файлы ключевого набора для первичной инициализации ***.dst и *.xps!** Сначала удалите ViPNet стандартными средствами Windows (Пуск>Панель управления>Программы и компоненты), затем удалите папку с установленным ViPNet Client. По умолчанию ПО устанавливается в C:\Program Files\InfoTeCS. Перезагрузите компьютер, выполните установку ViPNet Client и его первичную инициализацию согласно Главы VI Настоящего руководства.

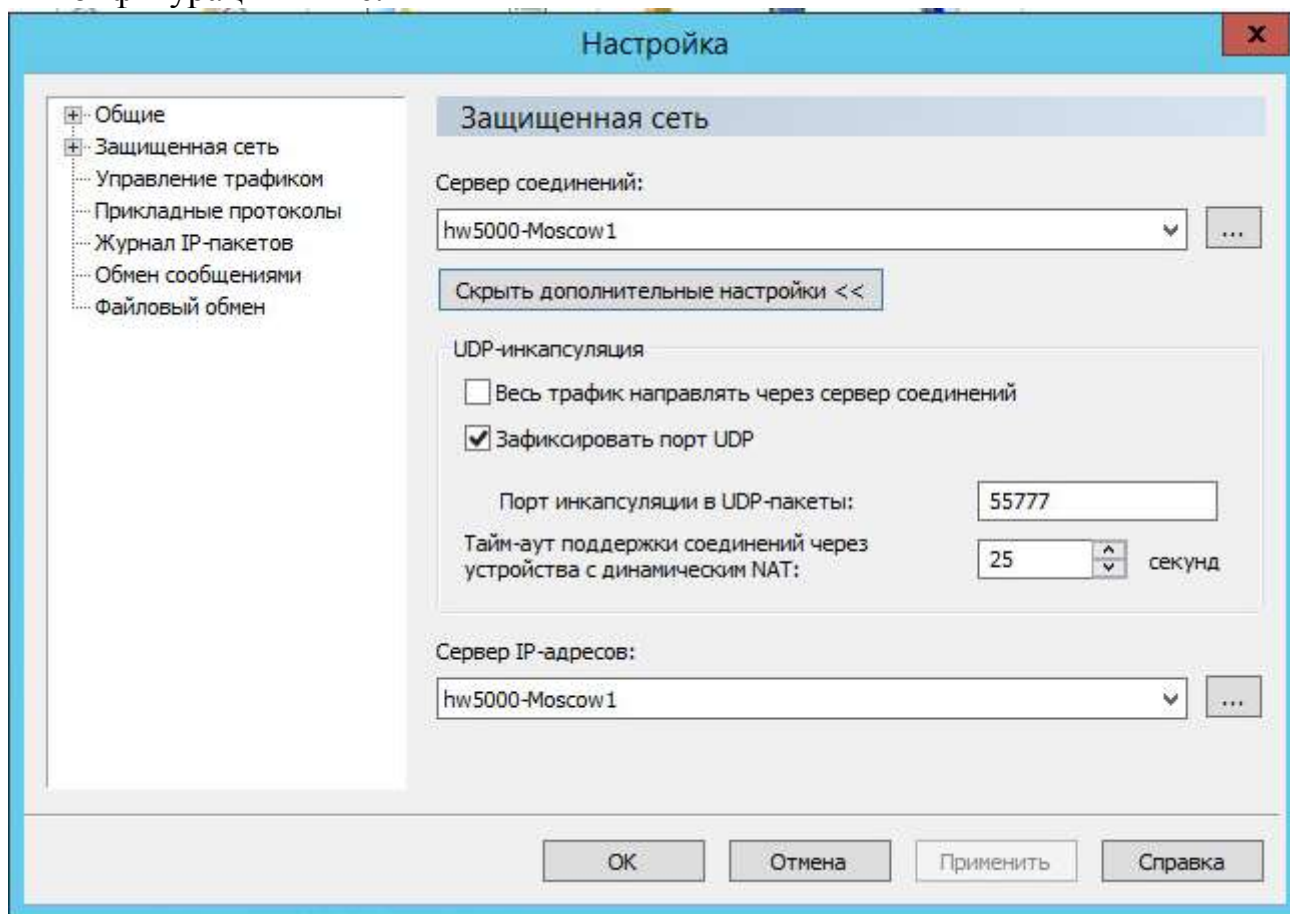
Вопрос: Как правильно переустановить ViPNet Client?

Ответ: Не забудьте сохранить Ваши файлы ключевого набора для первичной инициализации (*.dst и *.xps с паролем). Сначала удалите ПО ViPNet Client стандартными средствами Windows (Пуск > Панель управления > Программы и компоненты), затем следует удалить папку с установленным ViPNet Client, по умолчанию ПО устанавливается в C:\Program Files\InfoTeCS. Перезагрузите компьютер, выполните установку ViPNet Client и его первичную инициализацию, предварительно удалив антивирус. Для Windows 10 в панели управления включите встроенное антивирусное ПО Defender.

Вопрос: В ПО ViPNet Client Монитор узел hw5000-Moscow1 координатора недоступен, что делать?

Ответ:

- 1) Проверьте настройки даты, времени и часового пояса на Вашем ПК. Время и дата должны быть настроены точно, для Вашего региона +/- 5 минут.
- 2) Проконсультируйтесь с Вашим системным администратором и убедитесь, что открыт на вход и на выход порт UDP 55777 на всех сетевых устройствах (прокси-сервере, маршрутизаторе и т.д).
- 3) Проверьте настройки программы ViPNet Client. Образец правильной конфигурации ниже.



В ПО ViPNet Client сверху, слева в шапке окна программы нажать пункт меню Сервис/Настройка/Защищенная сеть. Должен быть прописан порт 55777, для «Сервер соединений» и «Сервер IP-адресов» выбран узел hw5000-Moscow1.

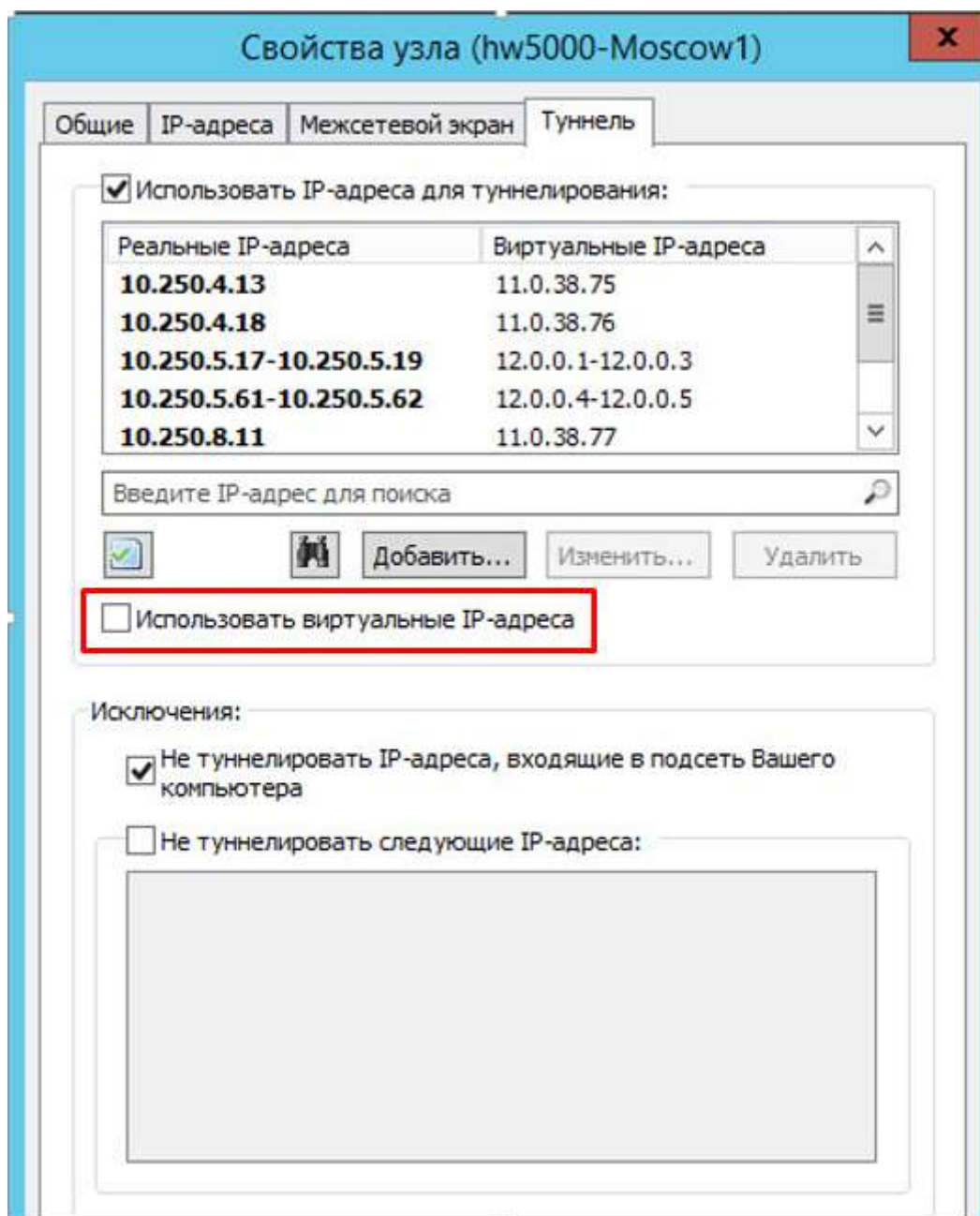
- 4) Также некоторые антивирусы с собственными межсетевыми экранами мешают корректной установке ПО ViPNet Client, из-за чего связь с координатором отсутствует. Рекомендуется удалить антивирус и переустановить ПО ViPNet Client с обязательным удалением папки установки вручную.
- 5) Если устранить ошибку не получается, просим направить информацию на электронный адрес fgis@fsa.gov.ru:
 - Скриншоты всех настроек клиента согласно высланной инструкции;
 - Скриншот версии ОС и ПО ViPNet Client;

- Скриншот результата выполнения команды ping 5.143.238.24;
 - Скриншот результата выполнения команды ping 10.250.74.17;
 - Скриншот журнала пакетов связи с hw5000-Moscow1: в ПО ViPNet Monitor выбрать узел hw5000-Moscow1, правой кнопкой вызвать контекстное меню и выбрать пункт «Журнал регистрации IP-пакетов», далее в открывшемся меню нажать Поиск;
 - Номер Вашего АРМ. Посмотреть его можно в ПО ViPNet Monitor: откройте программу, выделите слева папку «Защищенная сеть», справа отобразится содержимое папки. Номер имеет вид АРМ-XXXX (четыре цифры).
-

Вопрос: Координатор hw5000-Moscow1 доступен, но недоступен (невозможно зайти) в ЕСИА по адресу <http://10.250.4.13/> и <http://10.250.74.17>

Ответ:

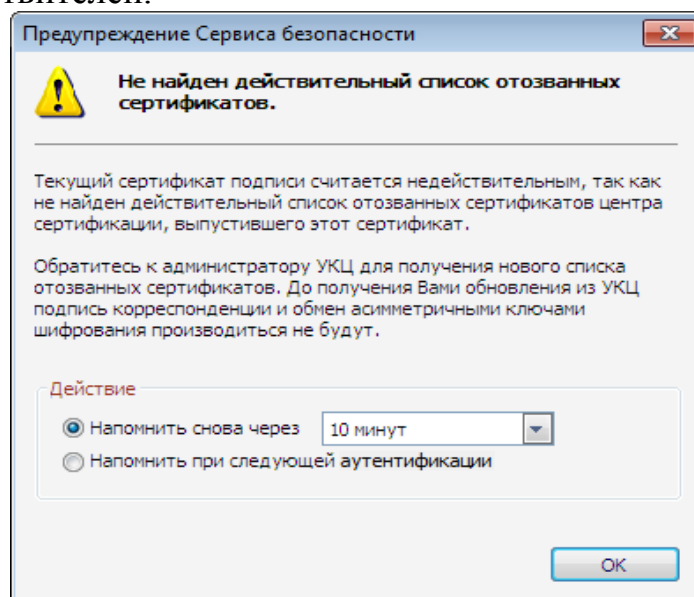
- 1) Проверьте в свойствах узла координатора hw5000-Moscow1 вкладку «Туннель», добавлен ли там реальный IP адрес 10.250.4.13 и 10.250.4.18, если нет, добавьте их. Для этого дважды кликните на узел hw5000-Moscow1 и перейдите во вкладку «Туннель». В поле «Использовать виртуальные IP-адреса» не должно быть галки. Жирным шрифтом должны быть выделены реальные IP-адреса.



- 2) Проверьте остальные настройки ViPNet Client согласно инструкции.
- 3) Возможно, проблема в Вашем антивирусе (прокси-сервере, маршрутизаторе, свитчах и т.д.). Попробуйте полностью отключить антивирус и зайти на адрес <http://10.250.4.13/> Если узел станет доступен, добавьте его в исключения антивируса. Также разрешите входящие и исходящие соединения для данного узла на Вашем прокси-сервере, маршрутизаторе, свитчах и т.д., если это необходимо.
- 4) Если устранить ошибку не получается, просим направить информацию на электронный адрес fgis@fsa.gov.ru:
 - Скриншоты всех настроек клиента согласно высланной инструкции;
 - Скриншот версии ОС и ПО ViPNet Client;
 - Скриншот результата выполнения команды ping 5.143.238.24;
 - Скриншот результата выполнения команды ping 10.250.4.13;
 - Скриншот результата выполнения команды ping 10.250.74.17;

- Номер Вашего АРМ. Посмотреть его можно в ПО ViPNet Monitor: откройте программу, выделите слева папку «Защищенная сеть», справа отобразится содержимое папки. Номер имеет вид АРМ-XXXX (четыре цифры).

Вопрос: Ошибка! Устарел список отозванных сертификатов СОС. Сертификат ПО ViPNet Client не действителен.

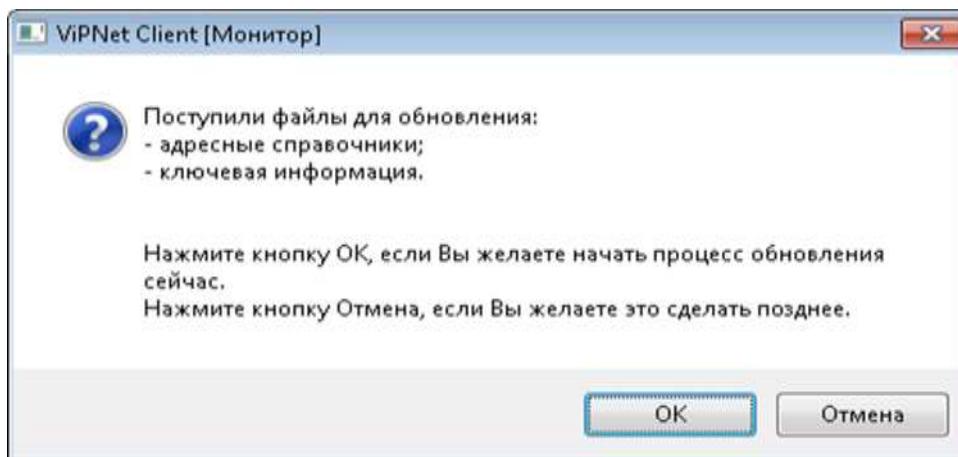


Ответ: Для начала необходимо проверить доступность координатора hw5000-Moscow1. Если координатор недоступен, см. вопрос о недоступности координатора. Предупреждение о том, что действительный список отозванных сертификатов не найден, появляется, если список отозванных сертификатов не обнаружен в хранилище пользователя или срок его действия истек. Такое сообщение также может появиться, если Вы не приняли последние обновления для программы ViPNet Client. *Данная ошибка не влияет на работу в личных кабинетах ФГИС Росаккредитации. Так как функционал подписи ПО ViPNet Client не используется в сети 2936 ФСА.*

Для закрытия окна и продолжения работы выберите одно из предложенных действий:

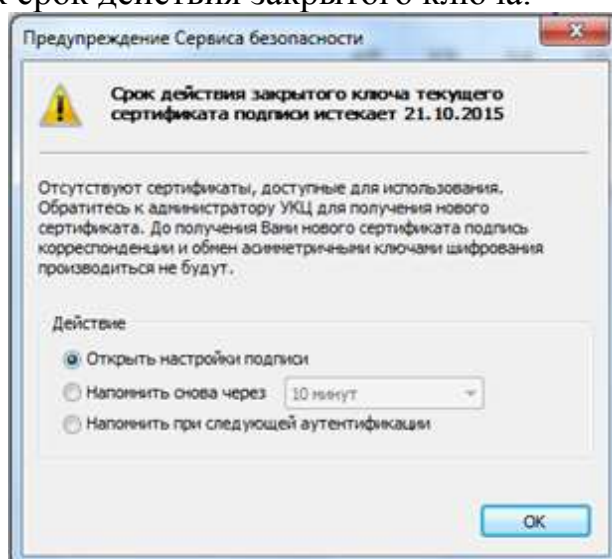
- 1) напомнить снова через — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя);
- 2) напомнить при следующей аутентификации — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Client;
- 3) нажмите кнопку «ОК».

Все обновления для программы ViPNet Client 4.x приходят через Интернет по внутреннему каналу самой программы. При получении программой обновлений появится окно ViPNet Client «Монитор».



В данном окне необходимо нажать кнопку «ОК», для того чтобы принять обновления. В случае если по каким-то причинам обновление не было установлено, необходимо дождаться нового (обновления будут приходить периодически по мере их выхода, и их НЕОБХОДИМО устанавливать.)

Вопрос: Ошибка! Истек срок действия закрытого ключа.



Ответ: Если координатор – узел hw5000-moscow1 доступен и данное сообщение касается закрытого ключа ПО ViPNet Client, то это ни коим образом не влияет на работу с порталом Росаккредитации.

Данный функционал больше не используется, для исправления Вам необходимо перевыпустить Ваш КН.

http://fsa.gov.ru/public/uploads/usr/Zapros_connect_FGIS.docx п. 4.5 Порядка получения доступа информационным ресурсам ФГИС Росаккредитации. В письме также необходимо указать информацию о номере Вашего АРМ.

Посмотреть его можно в ПО ViPNet Monitor: откройте программу, выделите слева папку «Защищенная сеть», справа отобразится содержимое папки. Номер имеет вид АРМ-XXXX (четыре цифры).

Если сообщение касается Вашего личного сертификата ЭП, обратитесь в Ваш УЦ для обновления ЭП.