

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

версия документа 2018 г.

## ОГЛАВЛЕНИЕ

<b>I. ВВЕДЕНИЕ .....</b>	<b>3</b>
<b>II. ТРЕБУЕМЫЙ СОСТАВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АРМ .....</b>	<b>4</b>
<b>III. ПОЛУЧЕНИЕ И УСТАНОВКА ПО VIPNET CRYPTOFILE.....</b>	<b>6</b>
<b>IV. УСТАНОВКА И ИНИЦИАЛИЗАЦИЯ ПО VIPNET CLIENT.....</b>	<b>9</b>
<b>V. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ .....</b>	<b>19</b>

## **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

**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. Требуемый состав программного обеспечения АРМ

Для установки и настройки ПО ViPNet Client 4.x 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».

**ВНИМАНИЕ!** Не устанавливайте VipNet CSP если у вас уже установлен «КриптоПро CSP», это приведет к конфликту программ и нарушению их работоспособности. Подробнее см. Главу V данного руководства.

- Дистрибутив ПО ViPNet CryptoFile (или аналогичное по функционалу ПО, например, КриптоАРМ);

**ВНИМАНИЕ!!!** Программа ViPNet CryptoFile может использоваться бесплатно совместно с программным обеспечением ViPNet (ViPNet CSP, ViPNet Client) только в случае, если данное ПО уже установлено и зарегистрировано, а в случае ПО ViPNet Client - проведена первичная инициализация. До проведения первичной инициализации ПО ViPNet Client программа ViPNet CryptoFile не может быть зарегистрирована бесплатно! Если вы используете криптопровайдер стороннего производителя, тогда рекомендуется устанавливать ПО КриптоАРМ непосредственно перед расшифровкой файла первичной инициализации.

- Дистрибутив ПО ViPNet Client (ознакомьтесь с системными требованиями на вашу версию ПО ViPNet Client указанными в документации на данное ПО). Документация идет в комплекте с дистрибутивом;

- Ключевой набор для подключения АП к сети «2936 ФСА» необходимый для первичной инициализации ПО ViPNet Client имеющий формат \*.zip.enc являющийся зашифрованным архивом, содержащий файл первичной инициализации (\*.dst) и текстовый файл с паролем на доступ к сети (ARM-xxxx.txt, где xxxx – номер АП).

**ВНИМАНИЕ!!!** Для получения файла первичной инициализации АП необходимо полученный в УЦ файл сертификата квалифицированной электронной подписи (файл с расширением \*.cer) заархивировать (формат \*.zip или \*.rar) и отправить на адрес электронной почты [fgis@fsa.gov.ru](mailto: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](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 также необходимо указать информацию о количестве рабочих мест, на которых будет устанавливаться приобретённое ПО «ViPNet Client 4.x (КСЗ)». В ответ на отправленное письмо пользователь должен получить зашифрованный на его сертификате файл(ы) первичной инициализации АП (\*.dst) в сети «2936 ФСА» и текстовый файл с паролем на доступ к сети (ARM-xxxx.txt или .xps, где xxxx – номер АП. Файлы будут находиться в зашифрованном архиве \*.zip.enc).

### III. Получение и установка ПО ViPNet CryptoFile.

**ВНИМАНИЕ!!!** Полученный из Росаккредитации зашифрованный файл (\*.zip.enc) является файлом первичной инициализации АП в сети «2936 ФСА» и содержит архив с вложенными файлами (\*.dst и \*.txt или .xps), который потребуется для первичной инициализации ПО ViPNet Client.

Для расшифрования полученного от Росаккредитации файла первичной инициализации абонентского пункта в сети «2936 ФСА» (\*.zip.enc) рекомендуется использовать бесплатное ПО ViPNet CryptoFile или КриптоАРМ.

**ВНИМАНИЕ!!!** Программа ViPNet CryptoFile может использоваться бесплатно совместно с программным обеспечением ViPNet (ViPNet CSP, ViPNet Client) только в случае, если данное ПО уже установлено и зарегистрировано, а в случае ПО ViPNet Client - проведена первичная инициализация. До проведения первичной инициализации ПО ViPNet Client программа ViPNet CryptoFile не может быть зарегистрирована бесплатно! Если вы используете криптопровайдер стороннего производителя, тогда рекомендуется устанавливать ПО КриптоАРМ непосредственно перед расшифровкой файла первичной инициализации.

Скачать ПО ViPNet CryptoFile можно скачать самостоятельно с сайта производителя по ссылке - <http://infotecs.ru/product/vipnet-cryptofile.html> нажав кнопку «Загрузить» и выбрать дистрибутив, соответствующий разрядности вашей операционной системы x86 или x64. Для установки ПО ViPNet CryptoFile:

- Запустите установку ПО ViPNet CryptoFile из файла setup\_x86.msi или setup\_x64.msi для установки на 32-х или 64-х разрядную ОС Windows соответственно;
- Следуйте инструкциям мастера установки;
- После успешной установки ПО запустите его с рабочего стола или из меню «Пуск»;
- Добавьте полученный от ФГИС Росаккредитации файл ключевого набора (\*.zip.enc) в список ViPNet CryptoFile (Рисунок 1)

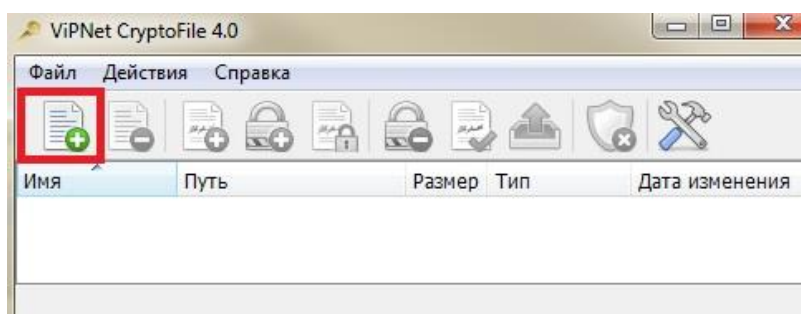
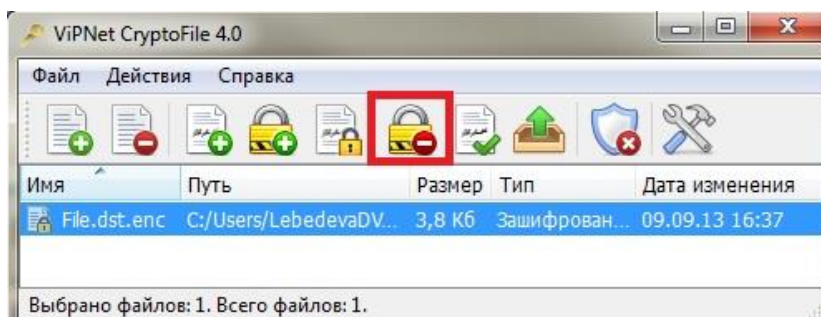


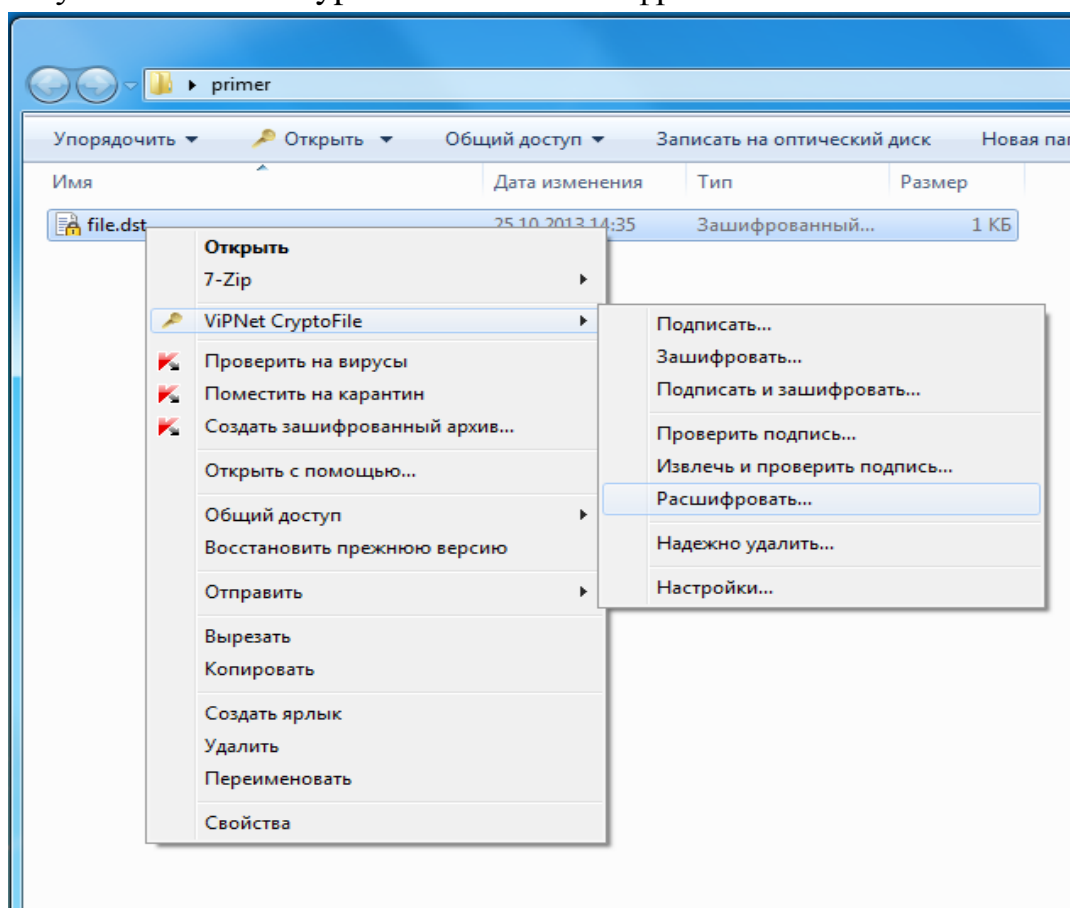
Рисунок 1

Выделите данный файл в списке и нажмите «Расшифровать» (Рисунок 2)



**Рисунок 2**

- Введите ПИН-код от носителя контейнера ЭП.
- Убедитесь в успешном завершении операции и нажмите «Закрыть». Расшифрованный файл будет сохранен в той же папке, что и зашифрованный файл и будет иметь такое же имя, что и зашифрованный, только с расширением .zip. Также можно расшифровать файл \*.zip.enc, щелкнув по нему правой клавишей мыши и выбрав в контекстном меню пункт «ViPNet CryptoFile» -> «Расшифровать...» см. Рис. 3



**Рисунок 3**

Далее расшифрованный архив (\*.zip) с ключевым набором необходимо разархивировать либо встроенным в операционную систему архиватором, либо иной установленной в систему программой архивирования.

**Внимание!** При возникновении проблем и ошибок с расшифровкой файла \*.zip.enc см. Главу V данного руководства.



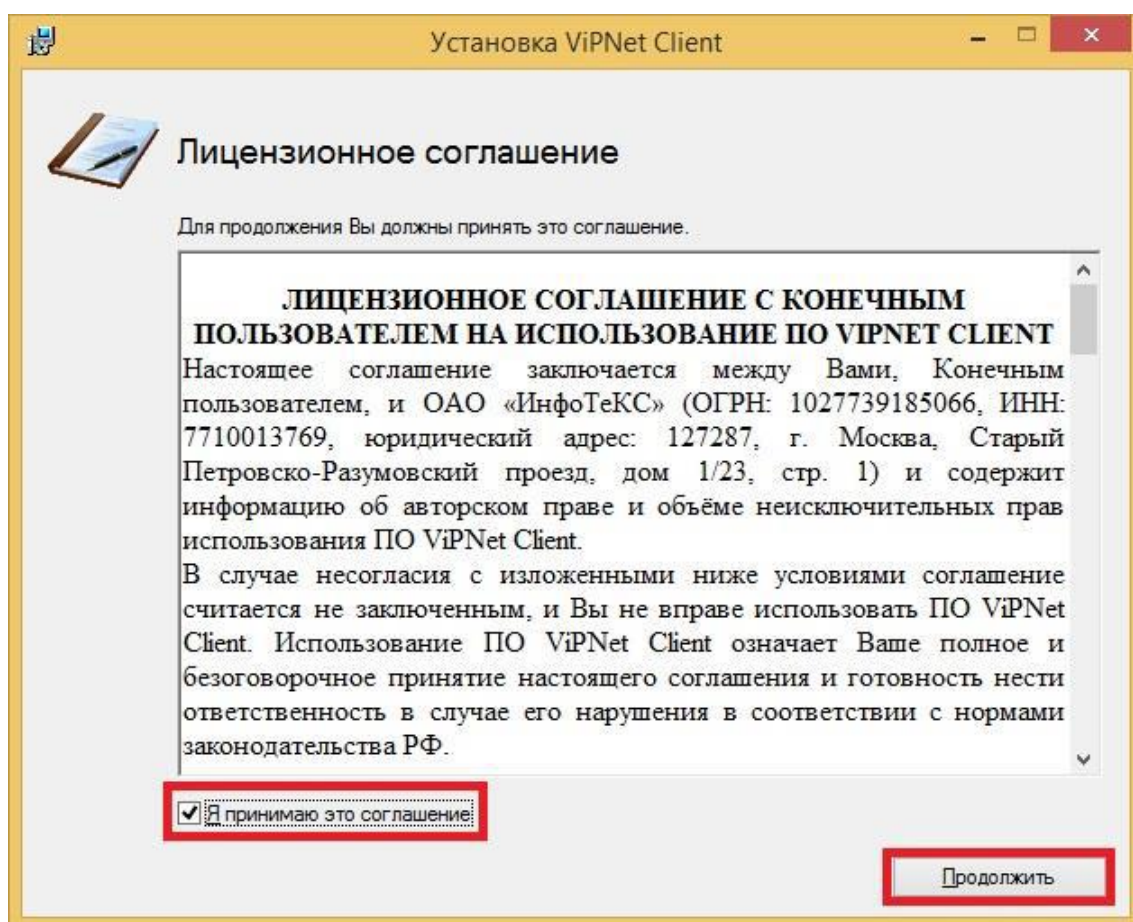
#### IV. Установка и инициализация ПО ViPNet Client

По вопросу приобретения дистрибутива ПО ViPNet Client на CD-диске, включая комплект эксплуатационной документации, формуляр и копию сертификата соответствия, необходимо обращаться к региональным партнерам в реестре ОАО «ИнфоТеКС» <http://infotecs.ru/partners/list>. Для подключения АРМ пользователей к ФГИС Росаккредитации используется ПО «ViPNet Client 4.x (КС3)».

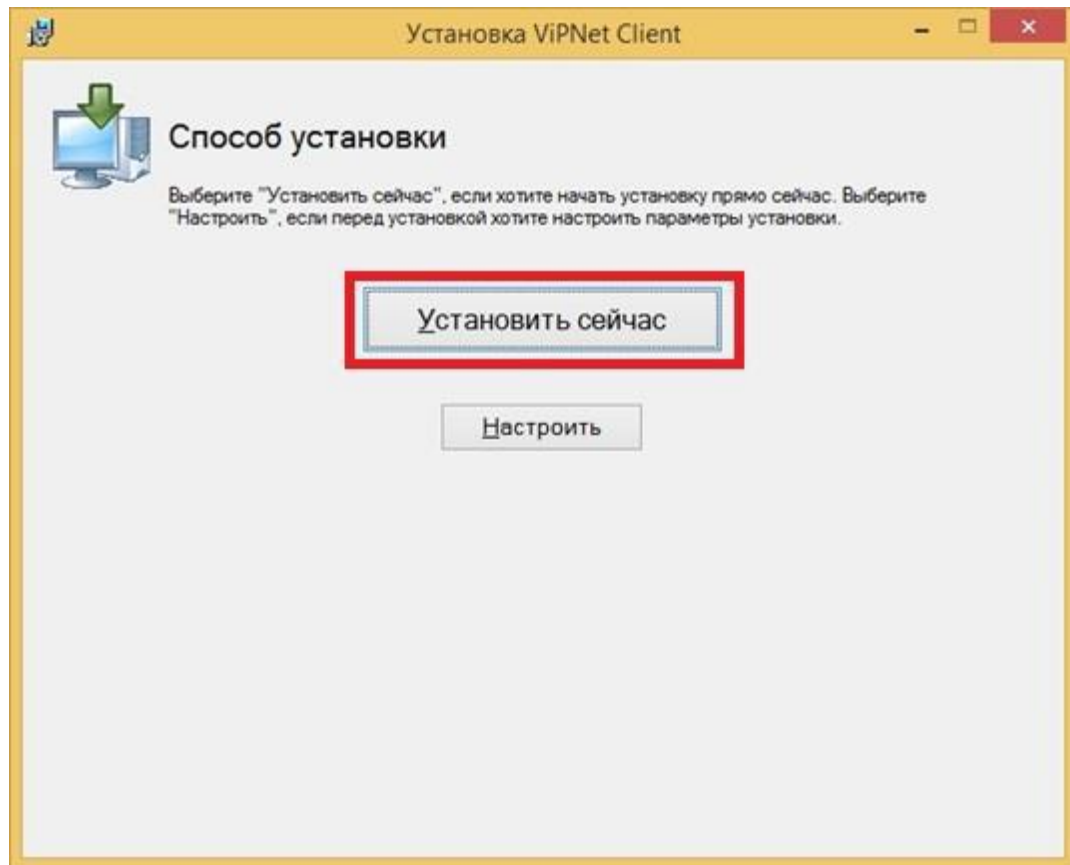
Перед установкой ПО ViPNet Client убедитесь, что на компьютере выполнены стандартные сетевые настройки, доступна работа в сети Интернет, а также правильно заданы часовой пояс, дата и время. Проконсультируйтесь с Вашим системным администратором и убедитесь, что открыт на вход и на выход порт UDP 55777 на всех сетевых устройствах (прокси-сервере, маршрутизаторе и т.д.). В ОС Windows 10 включите стандартное средство антивирусной защиты Defender.

Для установки ViPNet Client необходимо выполнить следующие действия:

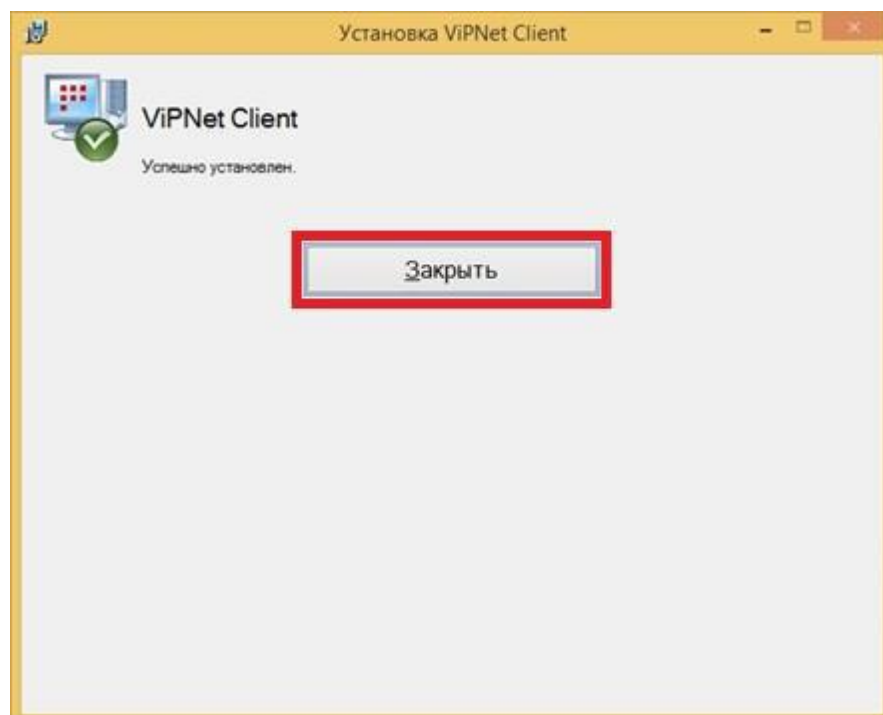
- Запустите файл setup.exe;
- Выполните установку ViPNet Client, следуя инструкциям мастера установки;
- В появившемся окне поставьте галочку о принятии лицензионного соглашения и нажмите «Продолжить».



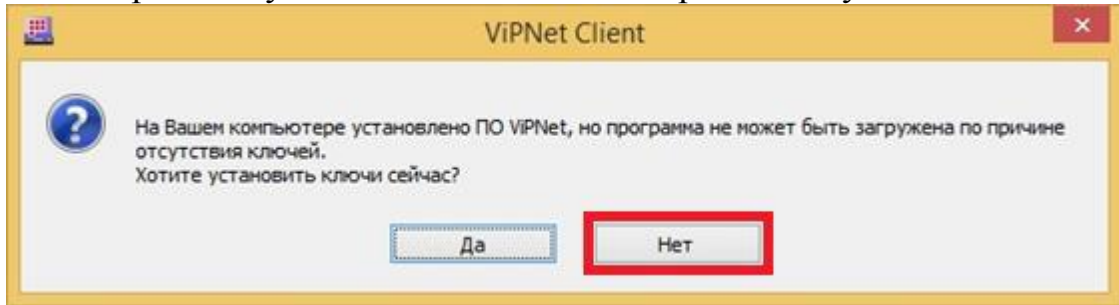
- Продолжите установку, нажав «**Установить сейчас**»;



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



- По завершении установки ViPNet Client предложит установить ключи

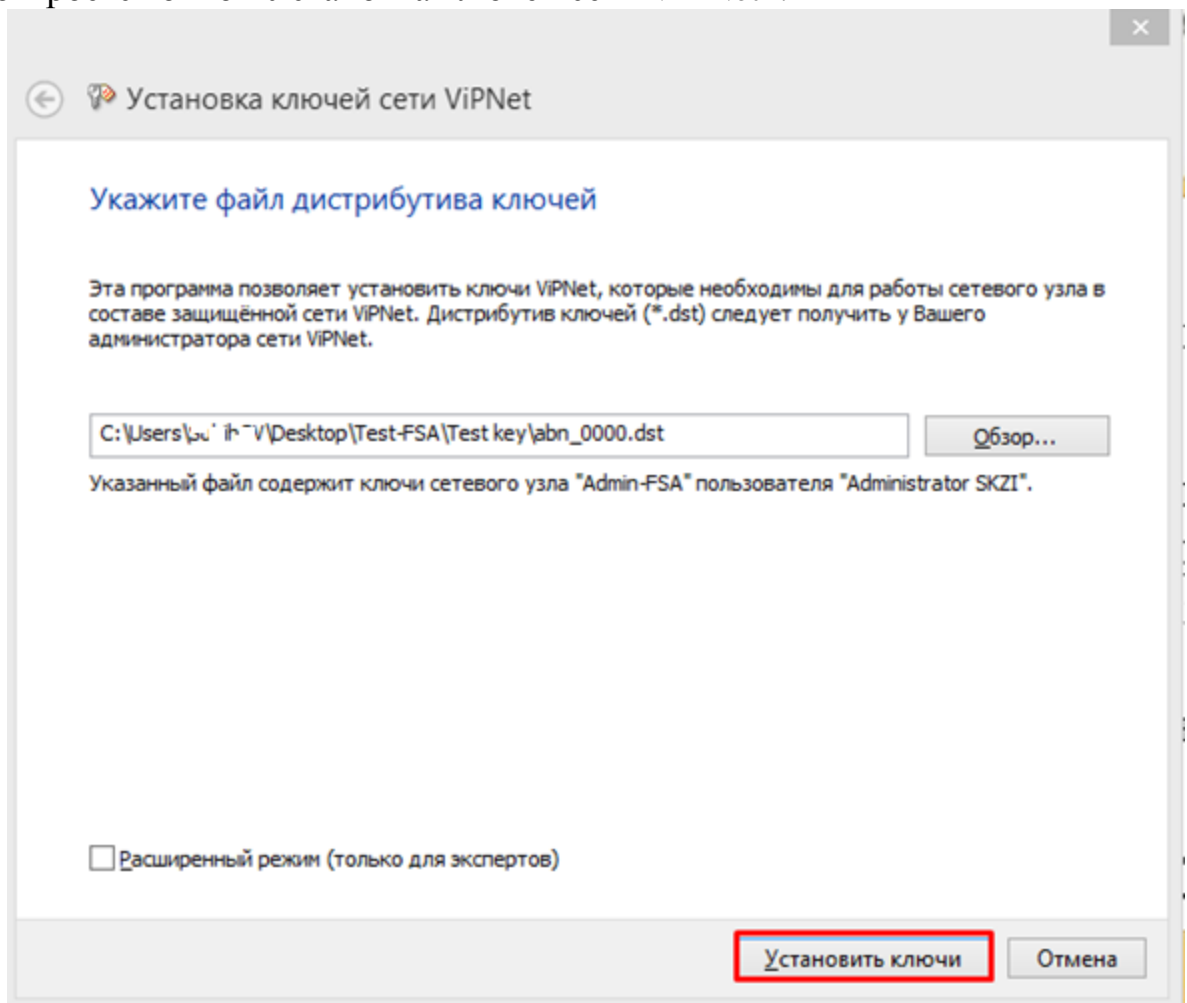


**Рисунок 6**

нажмите «**Нет**» как изображено на рисунке 6.

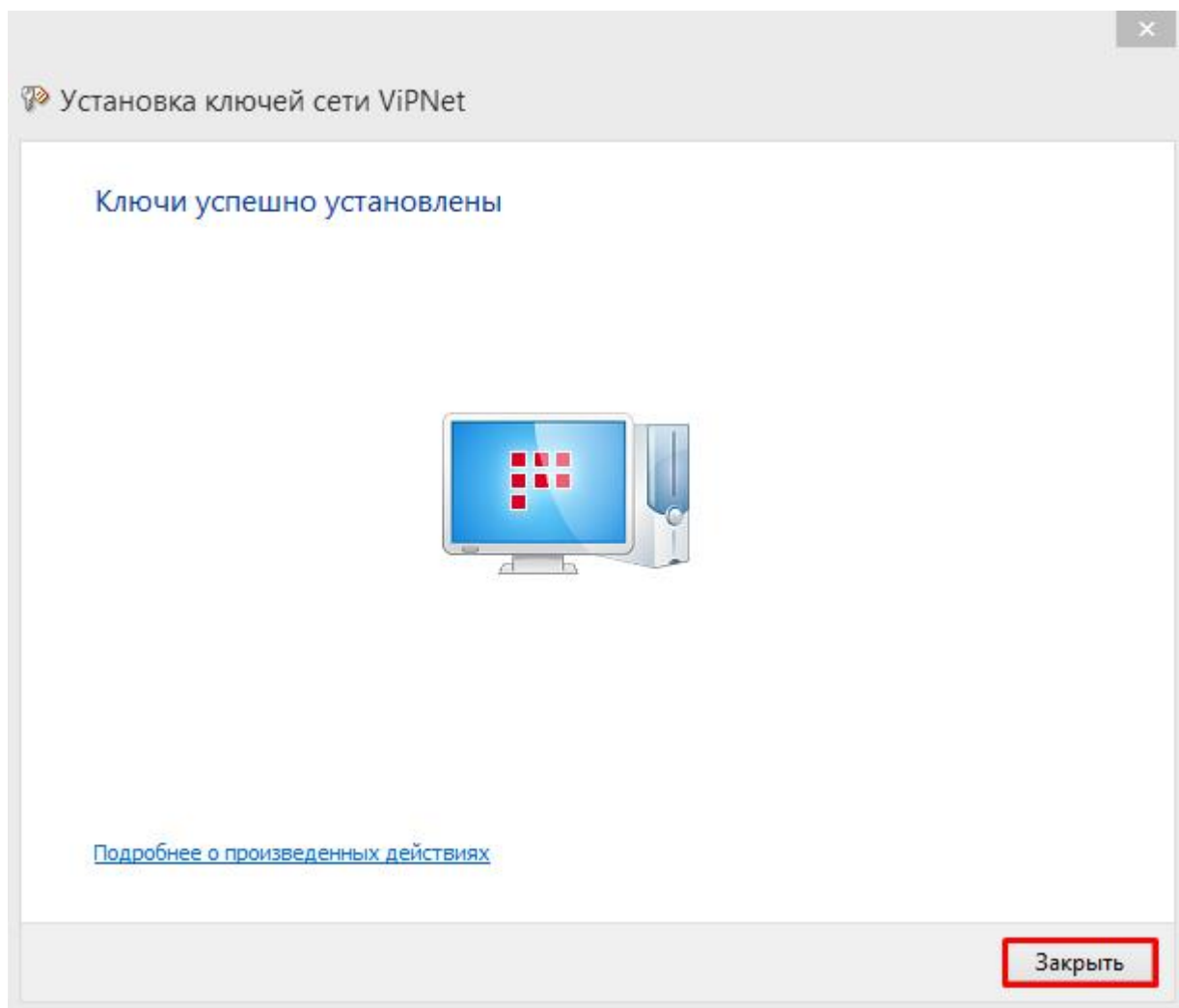
После установки ПО ViPNet Client Монитор необходимо перезагрузить компьютер. После перезагрузки, АРМ еще не готов к работе, поскольку не установлен ключевой набор (dst-файл). Для первичной инициализации ключевого набора выполните следующее:

- Расшифрованный ключевой набор (файл с расширением. dst), полученный от ФСА Росаккредитации, кликнуть двойным щелчком мыши, у Вас откроется окно «Установка ключей сети ViPNet».



**Рисунок 7**

- Нажмите кнопку «Установить ключи», см. Рисунок 7.



**Рисунок 8**

- Завершение успешной инициализации ключей, показано на рисунке 8, нажмите «Заккрыть».
- После первичной инициализации для запуска программы, Вам необходимо только ввести пароль из текстового файла (ARM-xxxx. txt или xps, где xxxx – номер АП).

Первичная инициализация выполняется **один раз** при установке программы ViPNet Client и более не требуется для запуска программы. Файл \*.dst и текстовый файл с паролем (ARM-xxxx.txt или .xps, где xxxx – номер АП) необходимо сохранить, так как они понадобятся Вам в случае, если потребуется переустановить программу. Пароль необходимо запомнить по парольной фразе, указанной в текстовом документе с паролем. Для этого необходимо набрать первые три буквы каждого слова парольной фразы русскими буквами, переключившись на английскую раскладку клавиатуры.

**Пример:** Если парольная фраза «Какая смешная парольная фраза», то пароль будет rfrcvtgfhahf.

- Теперь можно включить ПО ViPNet Client Монитор, двойным кликом мыши



нажмите на ярлык

- После запуска ViPNet Client [Монитор] мастер установки предложит установить сертификат УКЦ, нажмите «ОК» см. Рисунок 10.

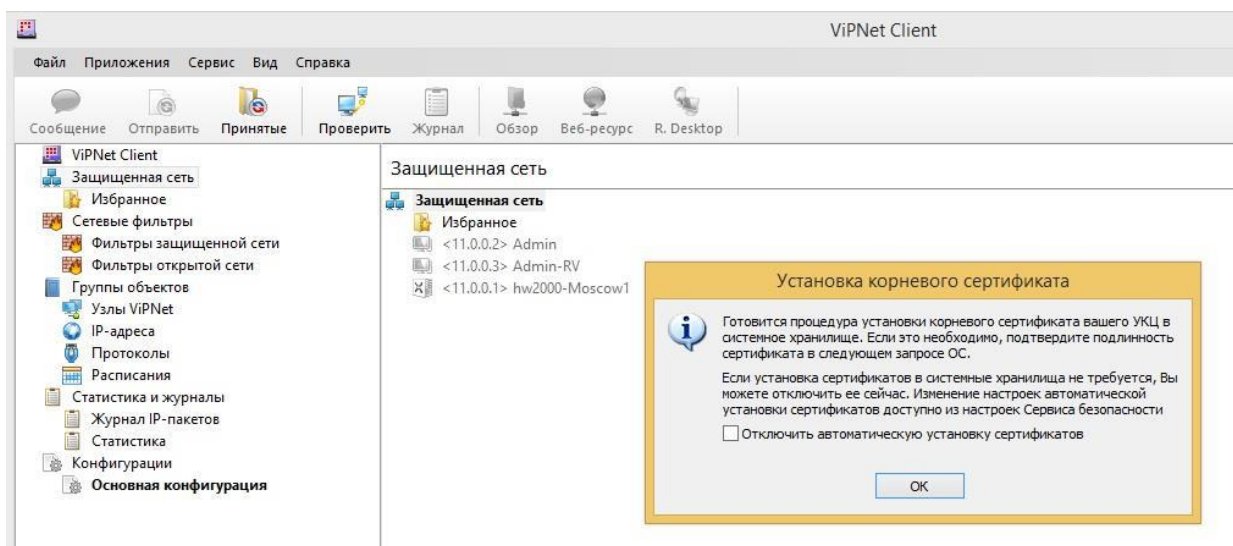


Рисунок 10

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**». См. Рис. 11. Координатор должен быть доступен. См. рис. 12. В случае если узел «**hw5000-Moscow1**» недоступен, см. Главу V данного руководства.

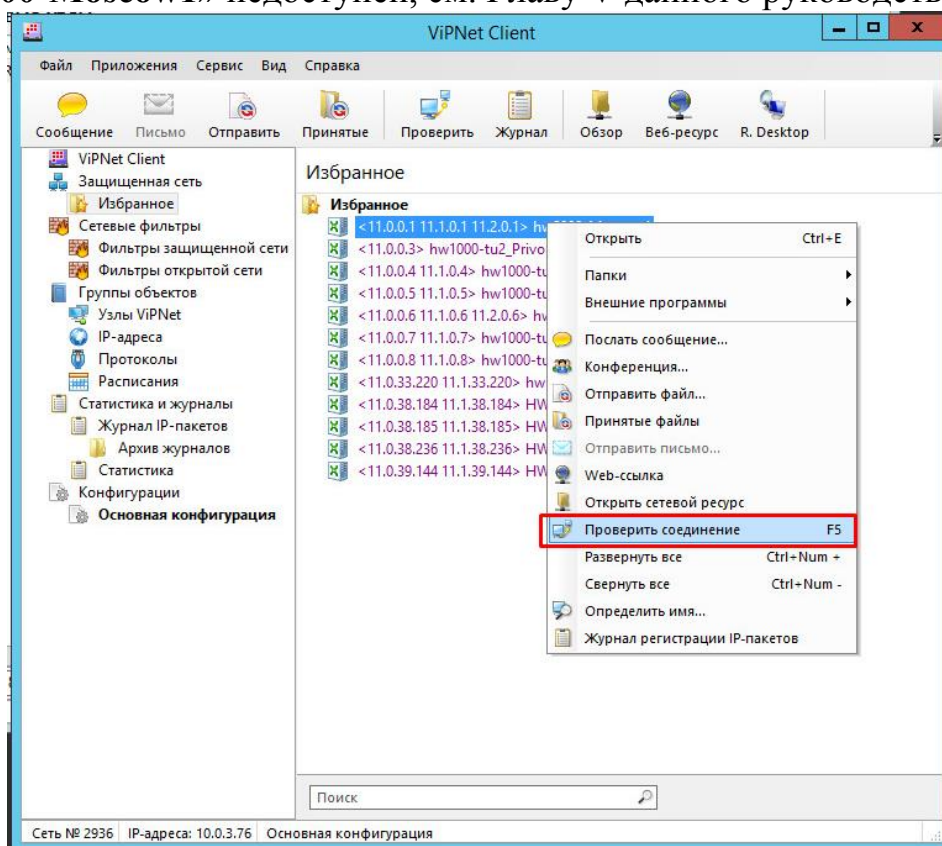


Рисунок 11



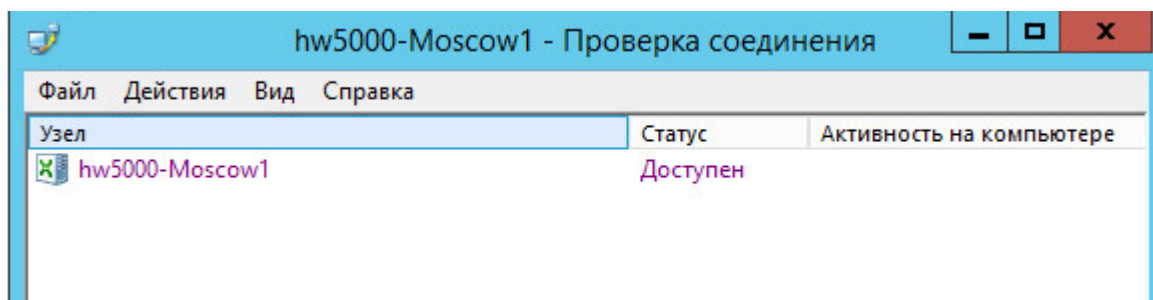


Рисунок 12

Далее необходимо проверить настройки **ViPNet Client [Монитор]**. Для этого в окне **ViPNet Client [Монитор]** откройте вкладку «**Защищенная сеть**» и в списке узлов выберите «**hw5000-Moscow1**», дважды щелкнув 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**» см. Рисунок 13. Если необходимо, снимите ее. Нажмите кнопку «**Применить**». Также проверьте, есть ли узлы 10.250.4.12, 10.250.4.13, 10.250.4.18 в списке реальных IP-адресов для **ФГИС 1.0**; 10.250.74.12, 10.250.74.17, 10.250.74.20, 10.250.74.23 в списке реальных IP-адресов для **ФГИС 2.0**

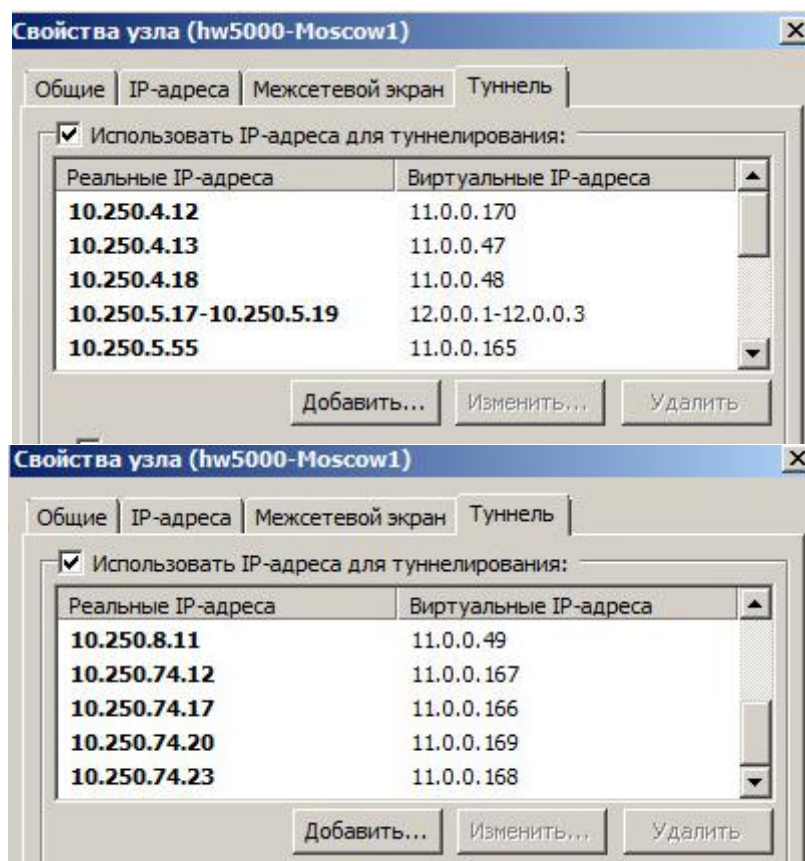
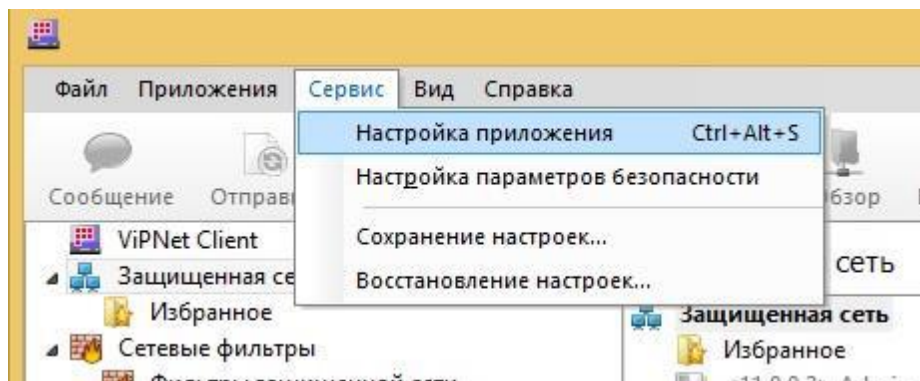


Рисунок 13

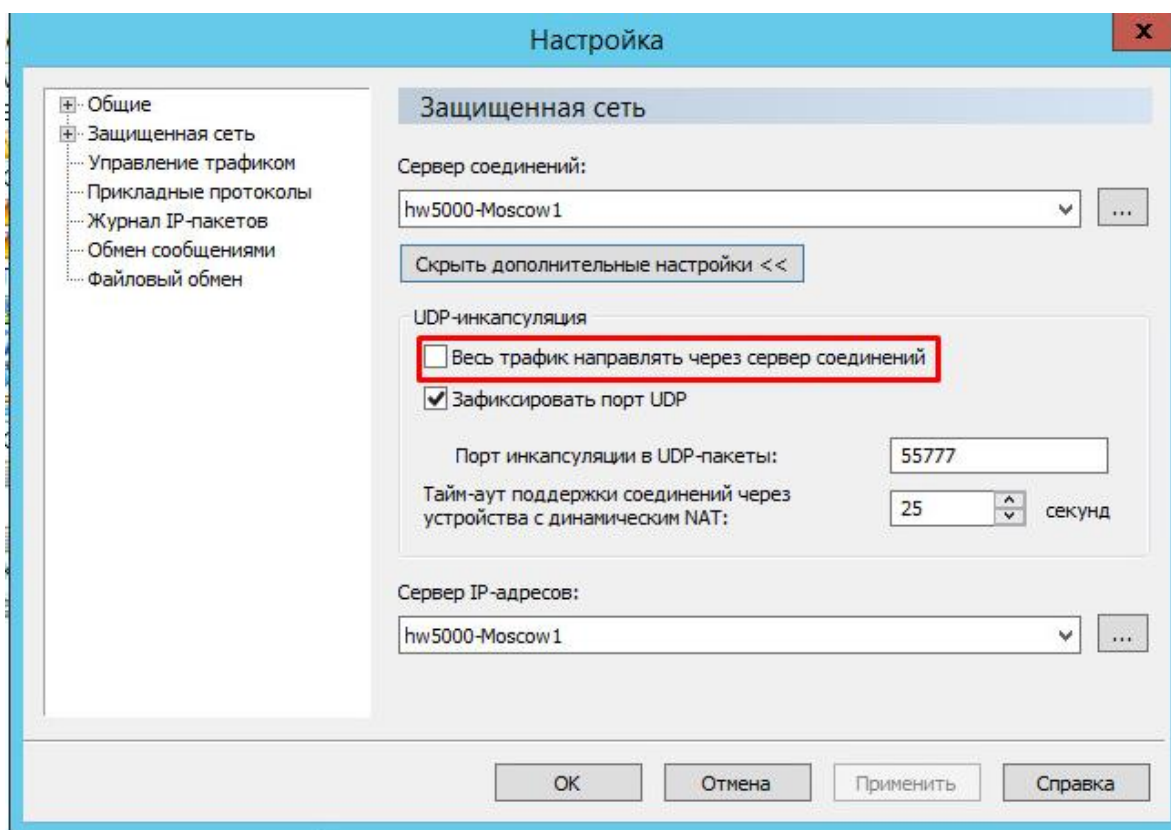
Далее необходимо проверить, отключен ли режим работы «**Весь трафик направлять через сервер соединений**». Для этого откройте пункт меню «**Сервис**» в

окне программы **ViPNet Client [Монитор]** и выберите пункт **«Настройка приложения»** см. Рисунок 14.



**Рисунок 14**

В открывшемся окне **«Настройки»** нажмите вкладку **«Показать дополнительные настройки»**, галочка в пункте **«Весь трафик направлять через сервер соединений»** должна быть снята, как показано на Рисунке 15.



**Рисунок 15**

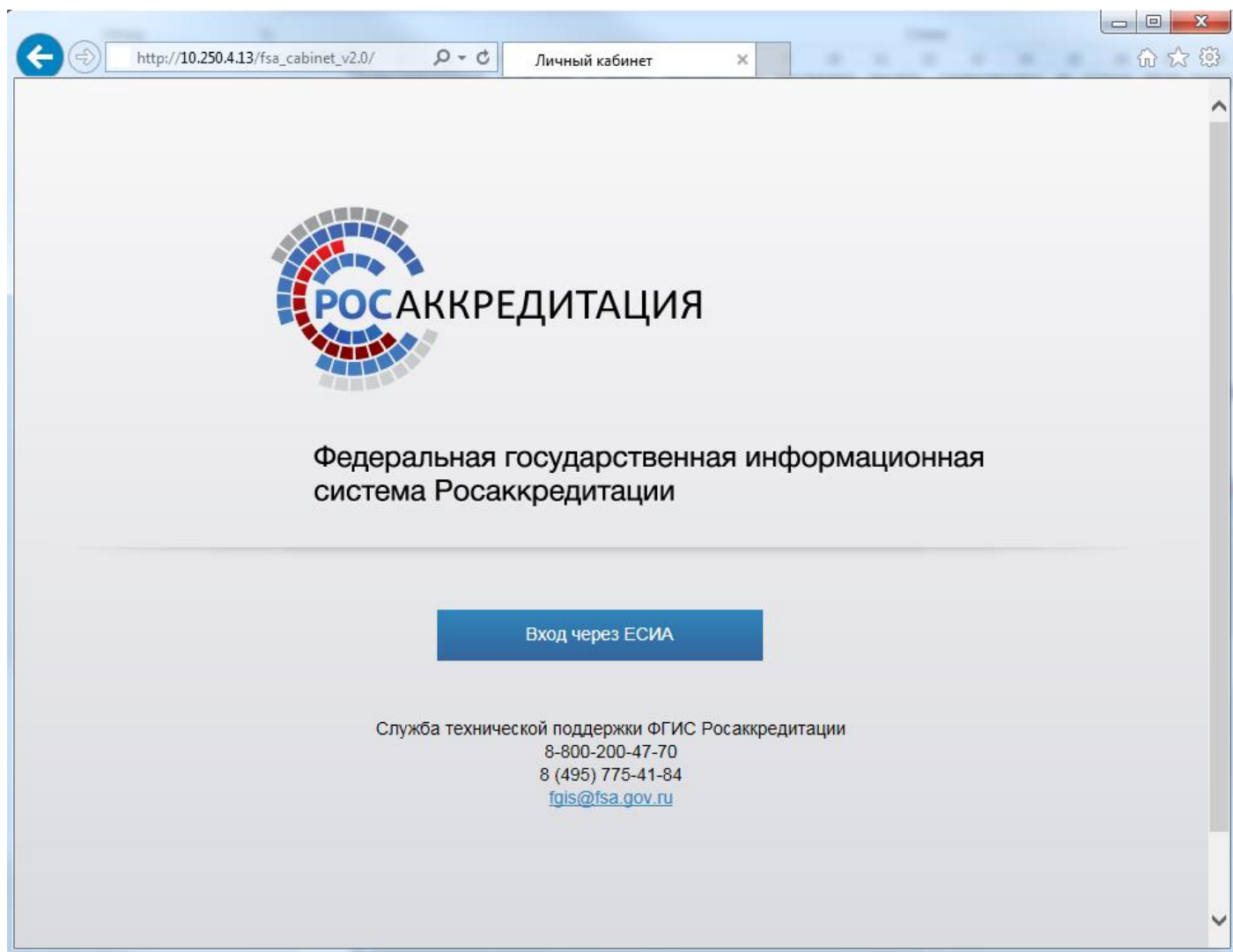
Поставьте галочку в пункте **«Зафиксировать порт UDP»** и пропишите **«Порт инкапсуляции в UDP-пакеты» 55777** как показано на Рисунке 15.

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.)

## ФГИС 1.0:

Для этого в Интернет-обозревателе (рекомендуется Mozilla Firefox) введите адрес: <http://10.250.4.13/>. Страница (Рисунок 16) должна быть доступна (открыться). Если страница недоступна, см. Главу V данного руководства.



**Рисунок 16**

## ФГИС 2.0:

Для этого в Интернет-обозревателе (рекомендуется Яндекс.Браузер последней версии) введите адрес: <http://10.250.74.17/>. Страница (Рисунок 17) должна быть доступна (открыться). Если страница недоступна, см. Главу V данного руководства.



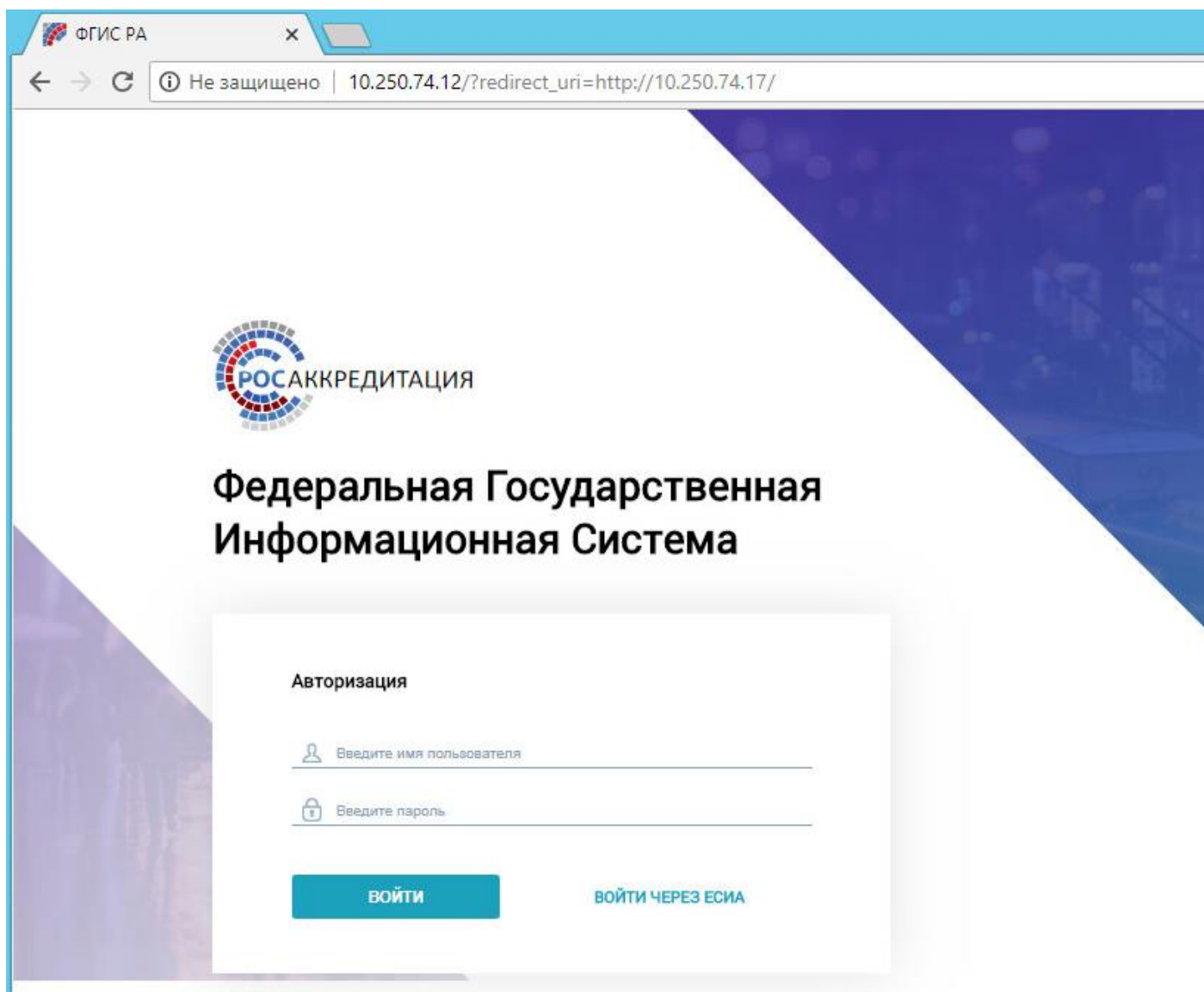


Рисунок 17

При необходимости дополнительных настроек ViPNet Client, отвечающих за функционирование абонентского пункта в сети «2936 ФСА» используйте «**ViPNet Client [Монитор]. Руководство пользователя**» (**ViPNet\_Client\_Monitor\_Ru.pdf**), входящей 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](http://www.gosuslugi.ru) или в Росаккредитации ([fgis@fsa.gov.ru](mailto:fgis@fsa.gov.ru)). Телефон службы технической поддержки ФГИС Росаккредитации 8-800-200-47-70 доступен в режиме 24 на 7.

### Получение обновлений ПО VipNet Client 4.x

При получении обновлений появится окно см. рисунок 18

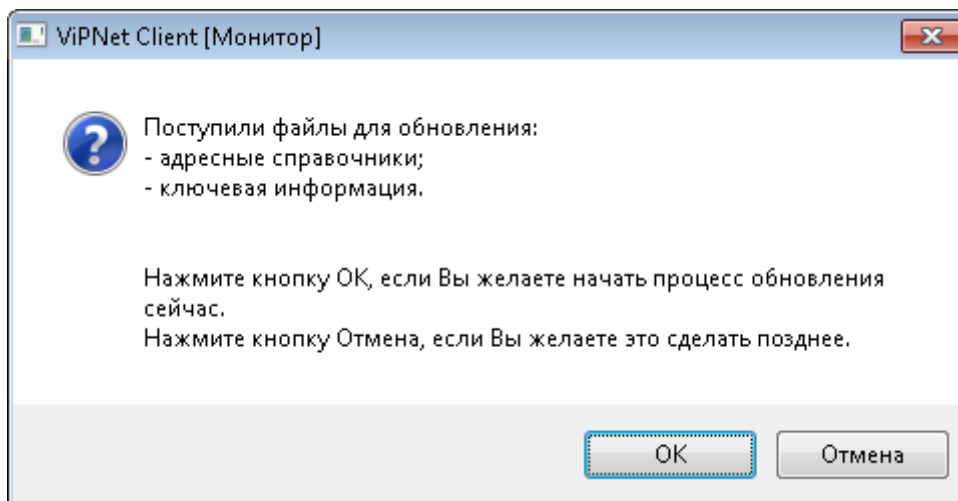


Рисунок 18

Их необходимо принять, нажав кнопку «ОК». 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.) Так же в случае если вы не приняли обновление, возможна ошибка «**Не найден действительный список отозванных сертификатов**» см. Главу V данного руководства.

## V. 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:** ViPNet Cryptofile просит зарегистрироваться (истек пробный период 14 дней). Как расшифровать ключевой набор?

**Ответ:**

Установите аналогичное ПО, например, КриптоАРМ. Также можно установить ViPNet Cryptofile или КриптоАРМ на другой компьютер, расшифровать файл \*.dst и перенести на АРМ с развернутым ПО ViPNet Client.

-----

**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:** ViPNet Cryptofile при попытке расшифровать присланный файл ключевого набора \*.zip.enc выдаёт ошибку. Что делать?

**Ответ:**

- 1) Если Вы используете криптопровайдер КриптоПРО CSP, рекомендуется использовать ПО КриптоАРМ.
- 2) 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.

3) Направьте скриншот ошибки в техническую поддержку по адресу [fgis@fsa.gov.ru](mailto:fgis@fsa.gov.ru). Вам вышлют инструкцию по устранению ошибки.

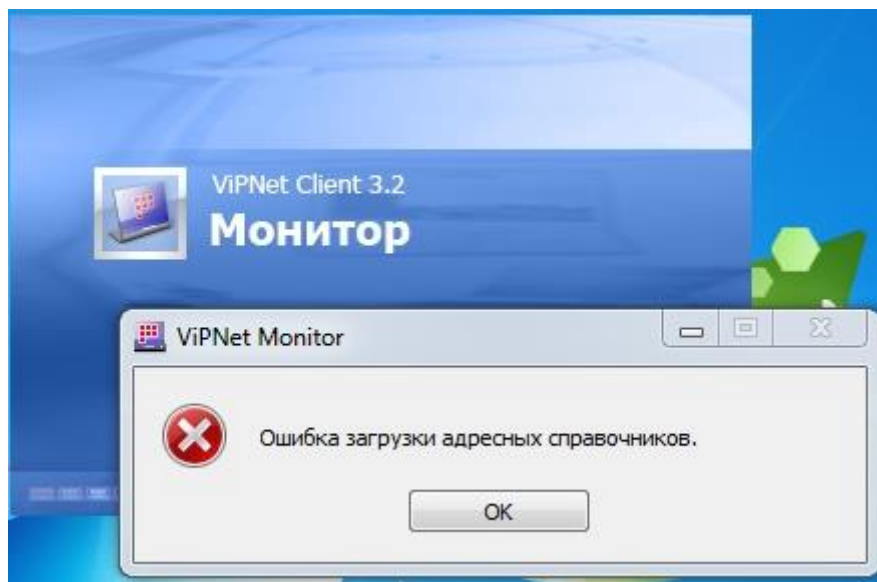
---

**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 данной инструкции.
- 2) Попробуйте переустановить ПО ViPNet Client с обязательным удалением папки установки вручную. Если проблема не решена обратитесь в службу тех. поддержки вашего поставщика ПО ViPNet Client.

- 3) Направьте скриншот ошибки в техническую поддержку по адресу [fgis@fsa.gov.ru](mailto:fgis@fsa.gov.ru). Вам вышлют инструкцию по устранению ошибки
- 

**Вопрос:** Ошибка 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 \*.txt или \*.xps с паролем)! Сначала удалите VipNet стандартными средствами Windows (Пуск>Панель управления>Программы и компоненты), затем удалите папку с установленным ViPNet Client. По умолчанию он устанавливается в C:\Program Files\InfoTeCS. Перезагрузите компьютер, выполните установку VipNet Client и его первичную инициализацию.

---

**Вопрос:** Как правильно переустановить ViPNet Client?

**Ответ:** Не забудьте сохранить ваши файлы ключевого набора для первичной инициализации (\*.dst и \*.txt или \*.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 он 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.

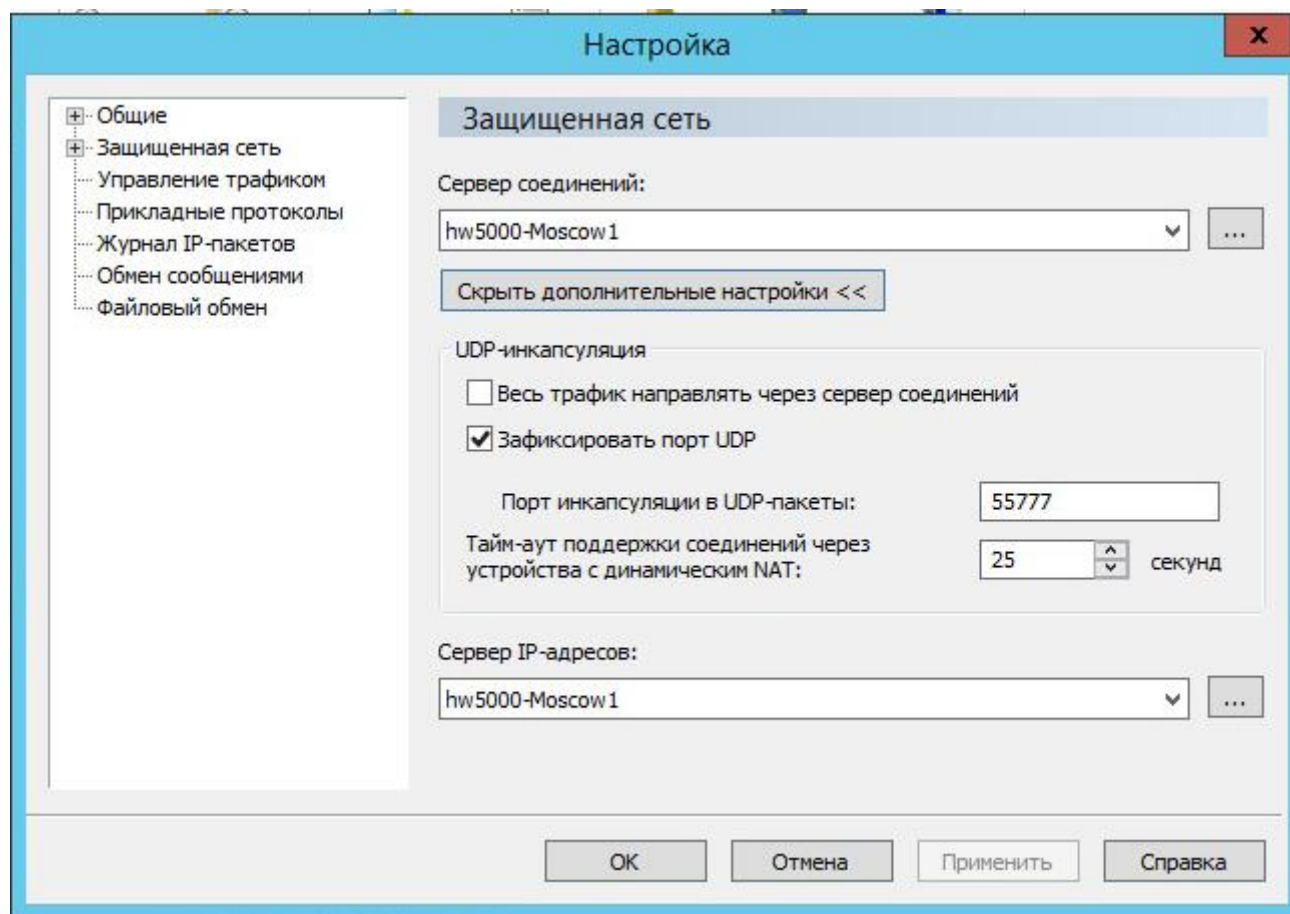
---

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

**Ответ:**

- 1) Проверьте настройки даты и времени 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 не редки случаи, когда используемые настройки не корректны. 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, «Сервер соединений» и «Сервер IP-адресов» выбран узел hw5000-Moscow1.

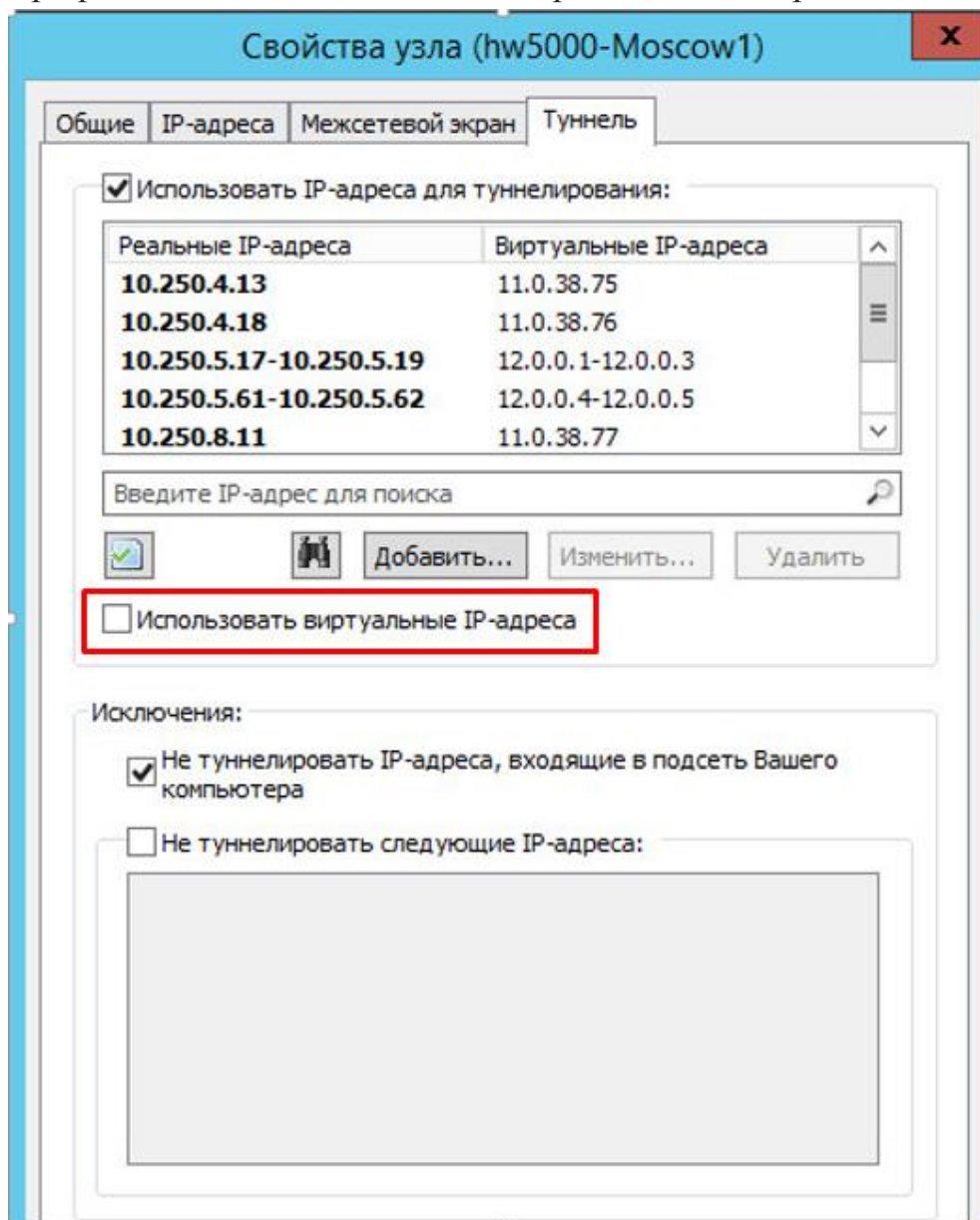
- 4) Так же некоторые антивирусы с собственными межсетевыми экранами мешают корректной установке ПО ViPNet Client из-за чего связь с координатором отсутствует. Рекомендуется удалить антивирус и переустановить ПО ViPNet Client с обязательным удалением папки установки вручную.
- 5) Если устранить ошибку не получается, просим направить информацию на электронный адрес [fgis@fsa.gov.ru](mailto: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`;
  - Скриншот журнала пакетов связи с hw5000-Moscow1: в ПО ViPNet Monitor выберите 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:** ViPNet Client координатор hw5000-Moscow1 доступен, но недоступен (невозможно зайти) в ЕСИА по адресу <http://10.250.4.13/> или <http://10.250.74.17/>

**Ответ:**

- 1) Проверьте в свойствах узла координатора hw5000-Moscow1 вкладку «Туннель» добавлен ли там реальный IP адреса, указанные на рис.13, 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.

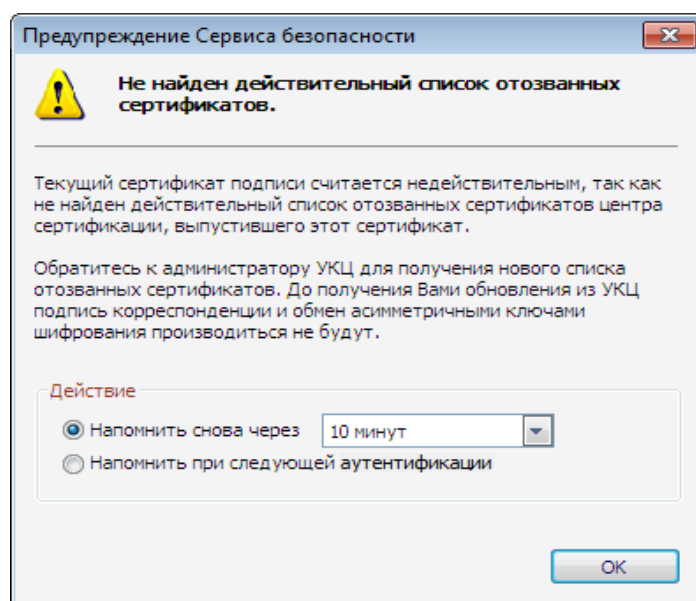


- 2) Проверьте остальные настройки ViPNet Client согласно инструкции.



- 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/>, <http://10.250.74.17/>. 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](mailto: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, так же может появиться если Вы не приняли последних обновлений для программы ViPNet Client. *Данная*



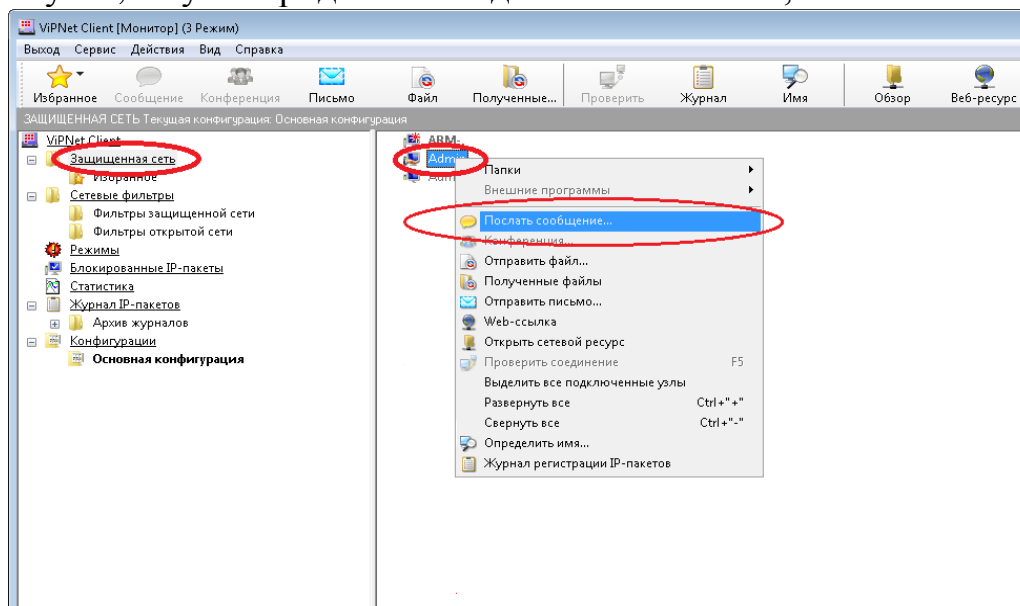
ошибка не влияет на работу в личных кабинетах ФГИС Росаккредитации. Так как функционал подписи ПО ViPNet Client не используется в сети 2936 ФСА.

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

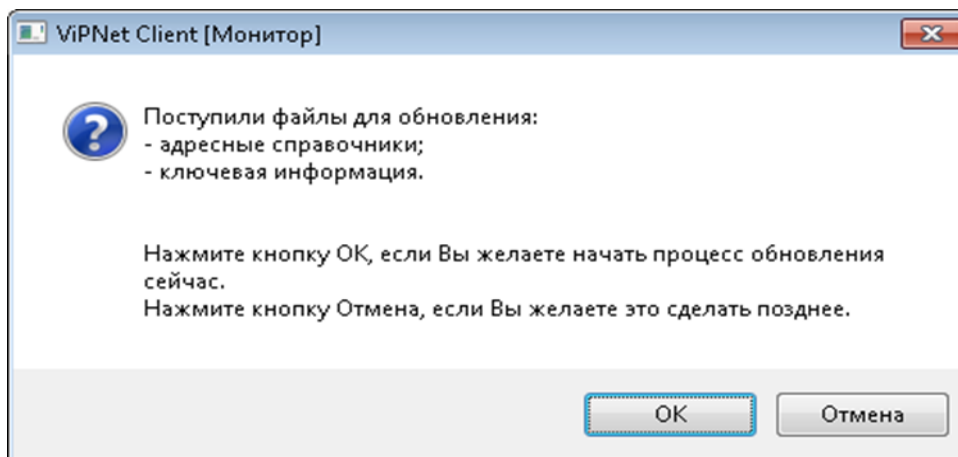
- 1) напомнить снова через — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя);
- 2) напомнить при следующей аутентификации — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Client;
- 3)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

Для устранения данного сообщения в будущем Вам необходимо обратиться к администратору сети ViPNet с целью отправки обновлений, включающих список отозванных сертификатов (COC).

Для этого откройте программу ViPNet Client «Монитор», выберите вкладку «Защищенная сеть» в основном окне программы, выберите узел «Admin», нажмите на него правой кнопкой мыши и в контекстном меню выберите пункт «Послать сообщение» как на рисунке ниже. В сообщении укажите название ошибки, после чего в течение суток, на узел придет необходимое обновление, и ошибка исчезнет.



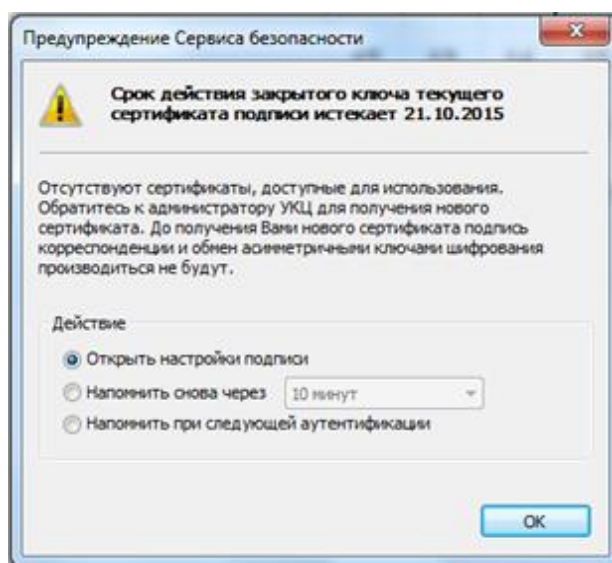
Все обновления для программы ViPNet Client 4.x приходят через интернет по внутреннему каналу самой программы. При получении программой обновлений появится окно ViPNet Client «Монитор»



В данном окне необходимо нажать кнопку «ОК» для того что бы 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 никоим 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](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.

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).

Если сообщение касается вашего личного сертификата ЭП обратитесь в ваш УЦ для обновления ЭП.