Инструкция по настройке транспорта ПО ViPNet Client в рамках услуги «Информационная безопасность»

(для «Координатор КА61_Server02»)

Листов 13

ИнфоТеКС Интернет Траст
2021 г.

Оглавление

I. Введение

✓ Документ предназначен для пользователей, осуществляющих самостоятельную настройку транспорта ПО ViPNet Client.

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

✓ При несоблюдении данных рекомендаций АО «ИнфоТеКС Интернет Траст» не несет ответственности за корректную работу программы ViPNet Client;

✓ **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. Общие и обязательные рекомендации по настройке транспорта ViPNet Client

Для работы защищенного транспорта ViPNet Client (отправка/прием файлов и писем) необходимо:

1) Проверить подключен ли интернет, любым способом – интернет должен быть подключен и доступен.
2) Проверить следующие параметры:
   - ✓ Состояние брандмауэра Windows – должен быть включен.
   - ✓ Если в системе установлены сторонние файрволы (например, встроенные в некоторые антивирусные программы: **Kaspersky Internet Security, Dr.Web, ESET NOD32 Smart Security, и. др.)**, то необходимо:
     - Либо выключить встроенный в антивирусное ПО файрвол;
     - Либо настроить разрешения:
       - инициативные соединения по порту **UDP 55777**[1] – если установлен **ViPNet Monitor + «Деловая почта»;**
       - открыть порты **TCP/IP**[2] в диапазоне **от 5000 до 5003 –** если установлена **только «Деловая почта».**
   - ✓ Текущие: дата, время, часовой пояс, региональные параметры в операционной системе должны быть актуальными и соответствовали региону (Рисунок 1).

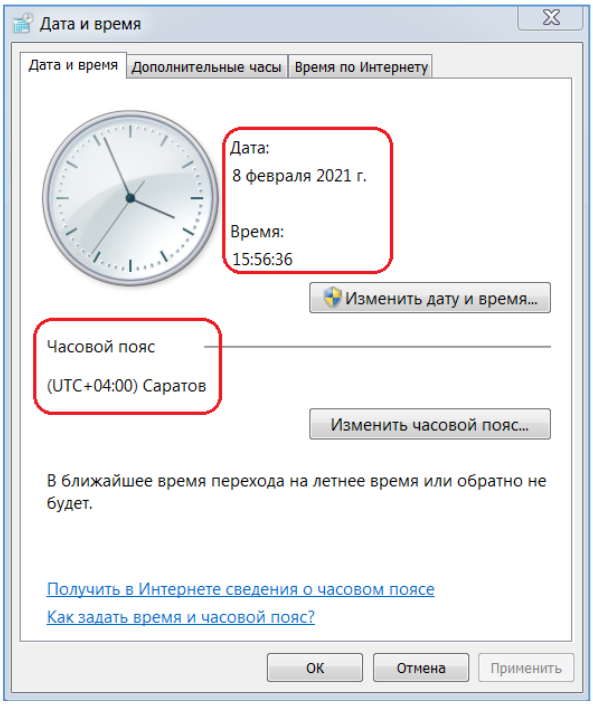

Рисунок 1

[1] Если Интернет в организации раздается локальным компьютерам через шлюз или прокси-сервер, то инициативные соединения по порту UDP 55777 также необходимо открыть на самом сервере в настройках NAT.

[2] Если Интернет в организации раздается локальным компьютерам через шлюз или прокси-сервер, то на них также необходимо разрешить оговоренные порты.

III. Настройки транспорта, если установлен ViPNet Client Monitor + «Деловая почта»

В случае если в систему был установлен программный комплекс ViPNet Client по типичной схеме (установлены модули Monitor + «Деловая почта»), то корректность настроек в ПО ViPNet Client Monitor следующая:

ViPNet Client Monitor должен быть выставлен за региональный координатор (сетевой узел – маршрутизатор), расположенный на площадке АО «ИнфоТеКС Интернет Траст». Для этого необходимо чтобы были выставлены следующие настройки в ViPNet Client Monitor:

Откройте - ***«Сервис»*** -> ***«Настройка приложения»*** (Рисунок 2).

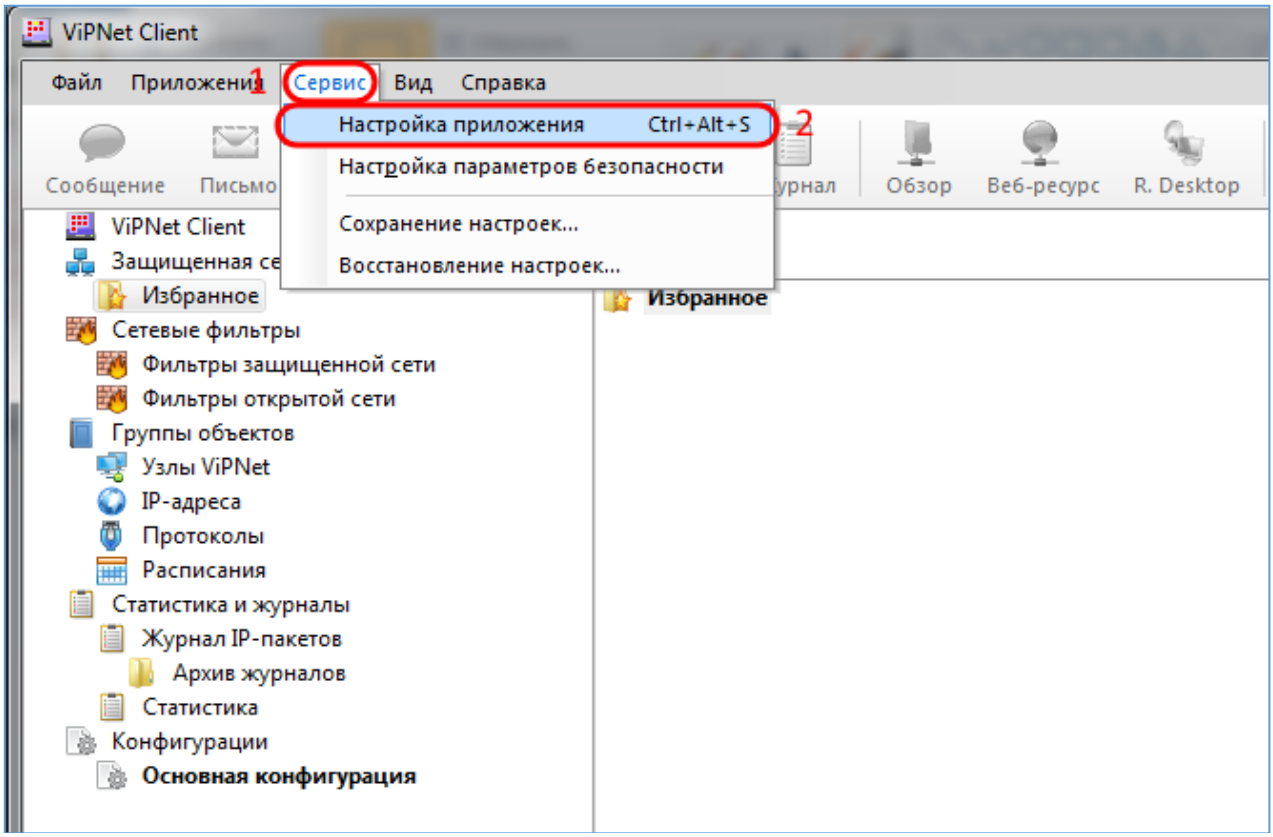

Рисунок 2

В открывшемся окне выбрать раздел ***«Защищенная сеть»*** (Рисунок 3, позиция 1), в поле ***«Сервер соединений:»*** должен быть выбран ***«Координатор КА61_Server02»*** (Рисунок 3, позиция 2). В поле ***«UDP-инкапсуляция»*** - галочка ***«Весь трафик направлять через сервер соединений»*** **не должна** быть установлена (Рисунок 3, позиция 3). В поле ***«Сервер IP-адресов:»*** должен быть выбран ***«Координатор КА61_Server02»*** (Рисунок 3, позиция 4).

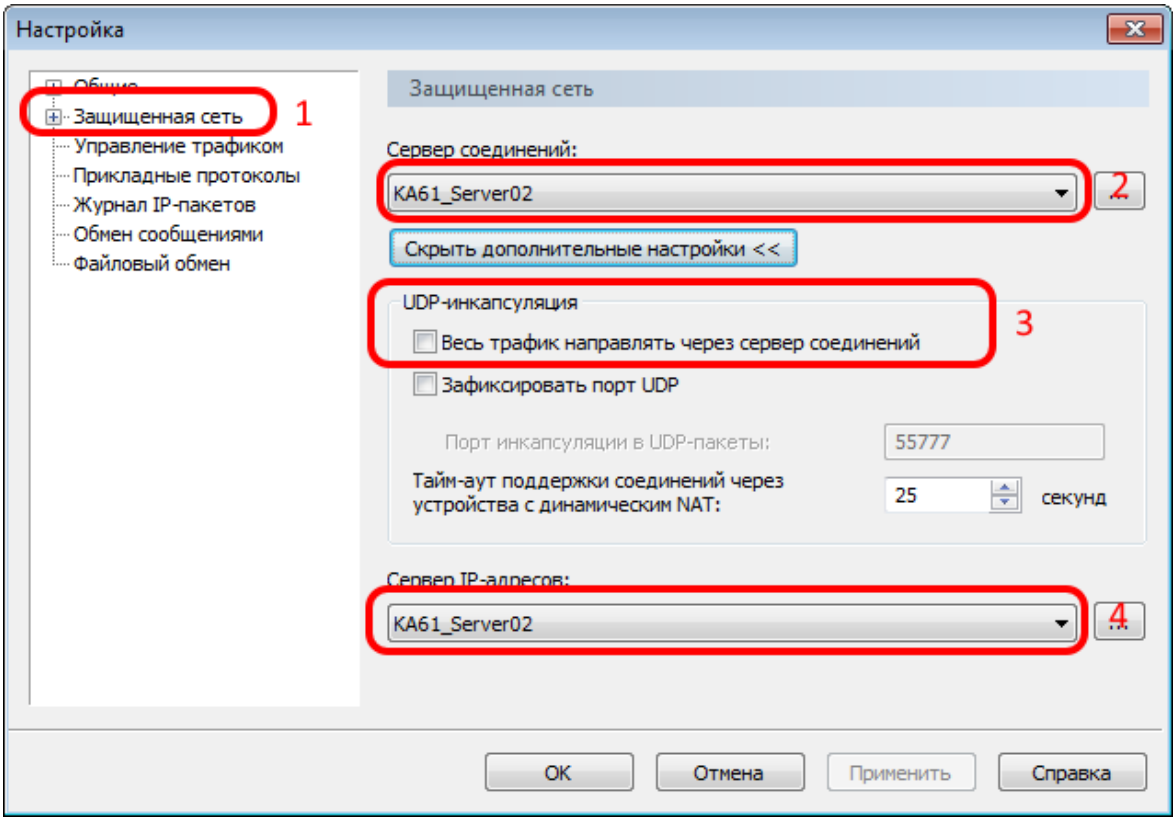

Рисунок 3

Т.е если у вас были выставлены иные настройки, то необходимо их привести в соответствие с рисунком 3.

В ViPNet Client Monitor, открыть раздел ***«Защищенная сеть»*** (Рисунок 4, позиция 1), выделить мышкой сетевой узел (координатор) за который заведен текущий абонентский пункт (Рисунок 4, позиция 2), нажать на клавиатуре клавишу ***«F5»***, таким образом запуститься проверка соединения с выделенным в защищенной сети сетевым узлом (Рисунок 5).

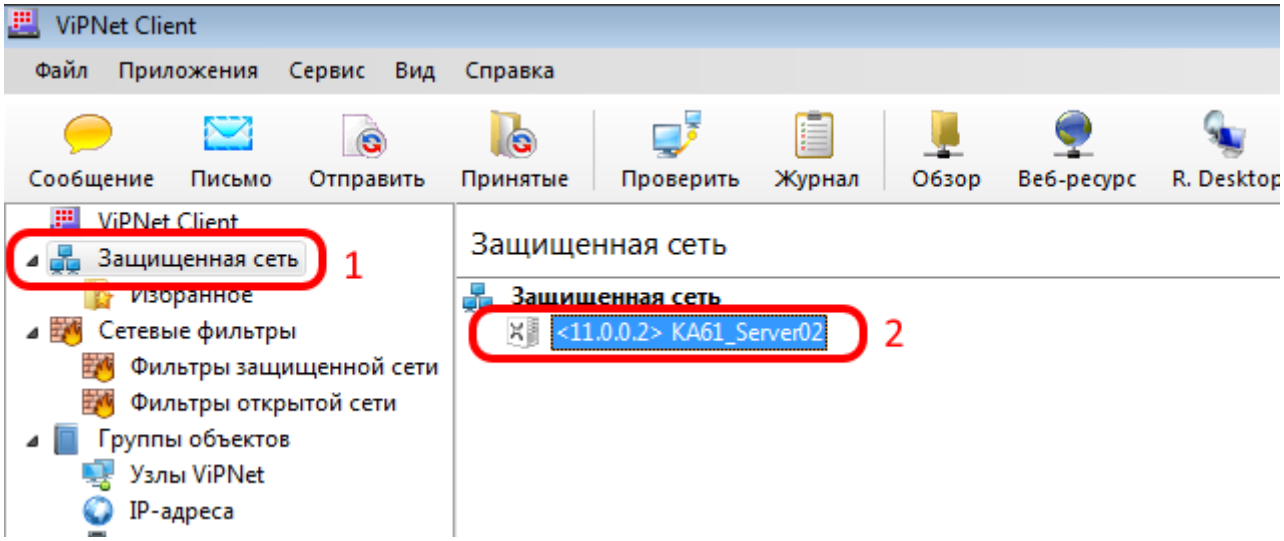

Рисунок 4

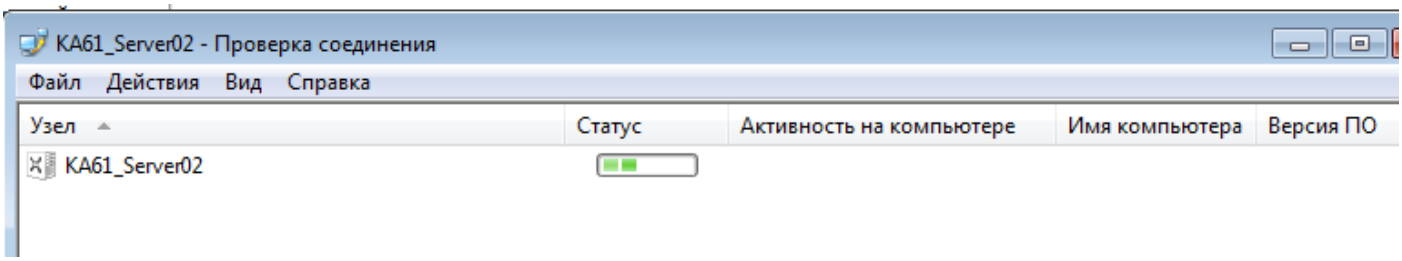

Рисунок 5

В случае если интернет доступен и инициативные соединения по порту **UDP 55777** ничем не ограничены для текущего компьютера, то высвечивается статус ***«Доступен»*** (Рисунок 6), при выполнении этих условий обмен (отправка/прием) файлов и писем со связанными защищенными узлами будет 100% выполняться.

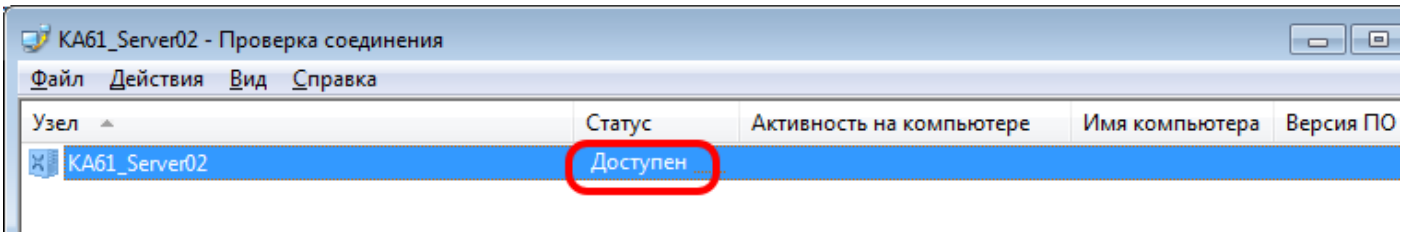

Рисунок 6

Если при проверке соединения с координатором соединение долгое время не устанавливается – статус высвечивается как ***«Недоступен»*** (Рисунок 7)

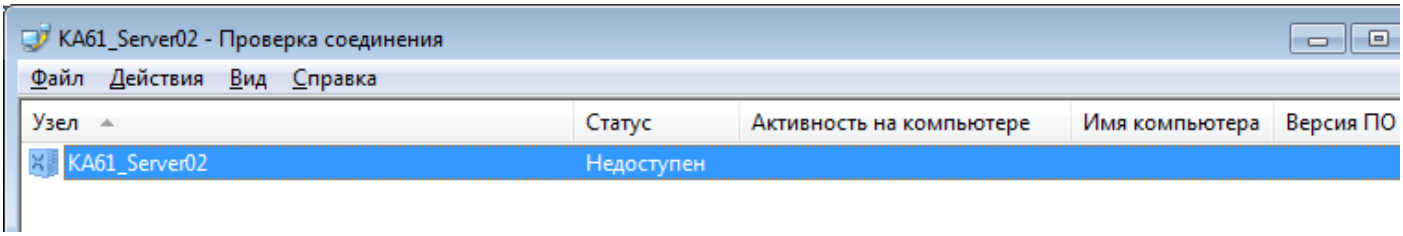

Рисунок 7

<u>В этом случае необходимо проверить:</u>

- Соблюдение всех рекомендаций, применимых к настройкам операционной системы, указанных на странице 4 данной инструкции;
- Проверить настройки правил доступа для координатора. Для этого щелкнуть двойным кликом левой кнопки мышки по строке ***«Координатор KA61_Server02»*** в разделе ***«Защищенная сеть»*** (Рисунок 4, позиция 1), в результате откроется окно ***«Свойства узла»*** (Рисунок 8);

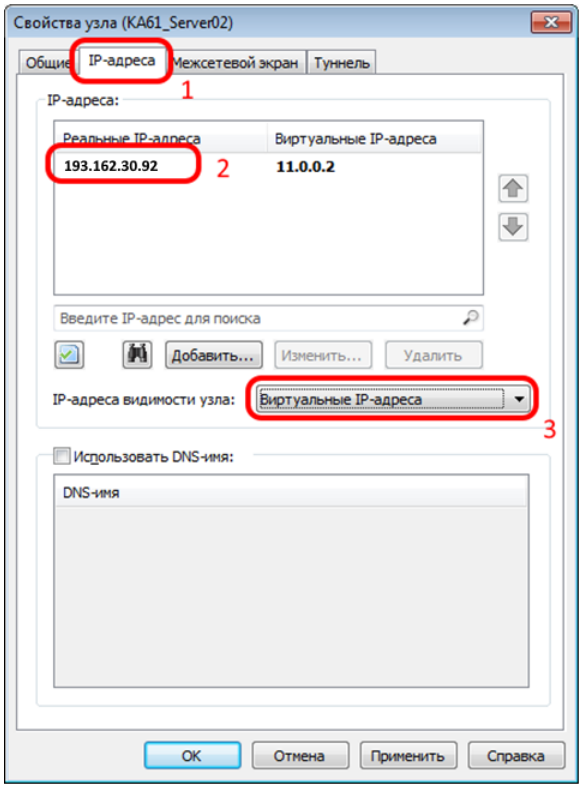

Рисунок 8

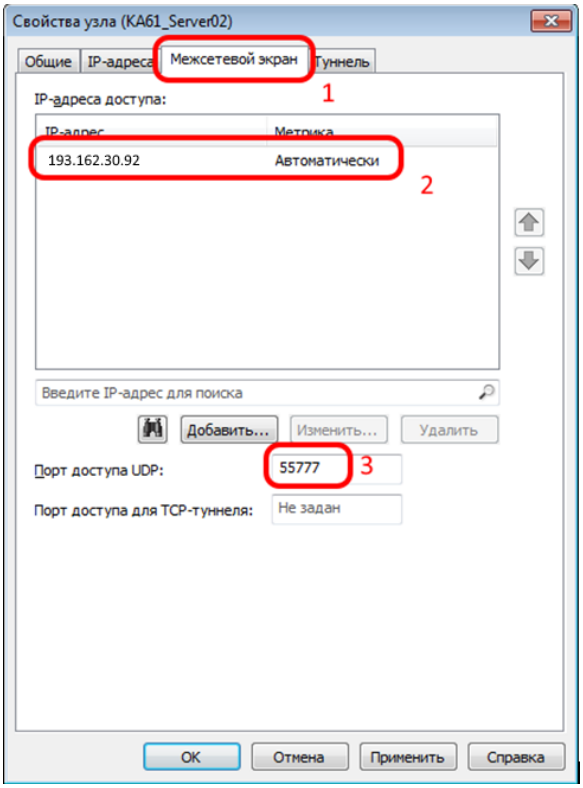

Рисунок 9

В окне ***«Свойства узла»***:

Откройте вкладку ***«IP адреса»*** (Рисунок 8, позиция 1), затем проверьте:

- Правильность IP адреса (Рисунок 8, позиция 2) указанного в поле ***«IP адреса»*** - должен присутствовать **193.162.30.92**;
- В поле ***«IP-адреса видимости узла:»*** - должен быть выбран пункт ***«Виртуальные IP-адреса»*** (Рисунок 8, позиция 3).

Откройте вкладку ***«Межсетевой экран»*** (Рисунок 9, позиция 1), затем проверьте:

В поле ***«IP-адреса доступа»*** - должен присутствовать **193.162.30.92** (Рисунок 9, позиция 2);

В поле ***«Порт доступа UDP:»*** - должен быть указан **55777** (Рисунок 9, позиция 3);

В случае если настройки отличаются от указанных в данной инструкции, необходимо исправить их на указанные. Ниже представлен пример изменения IP адреса координатора:

Изменение IP адреса во вкладке ***«IP-адреса»*** (Рисунок 10, позиция 1):

- Выделите старый IP адрес (Рисунок 10, позиция 2), и нажмите кнопку ***«Изменить»*** (Рисунок 10, позиция 3);
- Введите значение **193.162.30.92** (Рисунок 10, позиция 4), затем нажмите кнопку ***«ОК»*** (Рисунок 10, позиция 5).

Изменение IP адреса во вкладке ***«Межсетевой экран»*** (Рисунок 11, позиция 1):

- Выделите старый IP адрес (Рисунок 11, позиция 2), нажать кнопку ***«Изменить»*** (Рисунок 11, позиция 3);
- Ввести значение **193.162.30.92** (Рисунок 11, позиция 4), нажать кнопку ***«ОК»*** (Рисунок 11, позиция 5);
- Нажать кнопку ***«ОК»*** (Рисунок 11, позиция 6).

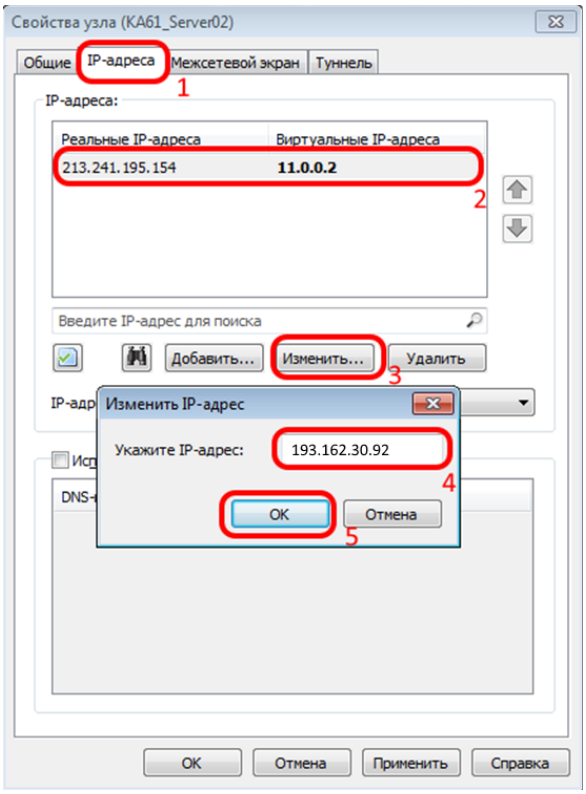

Рисунок 10

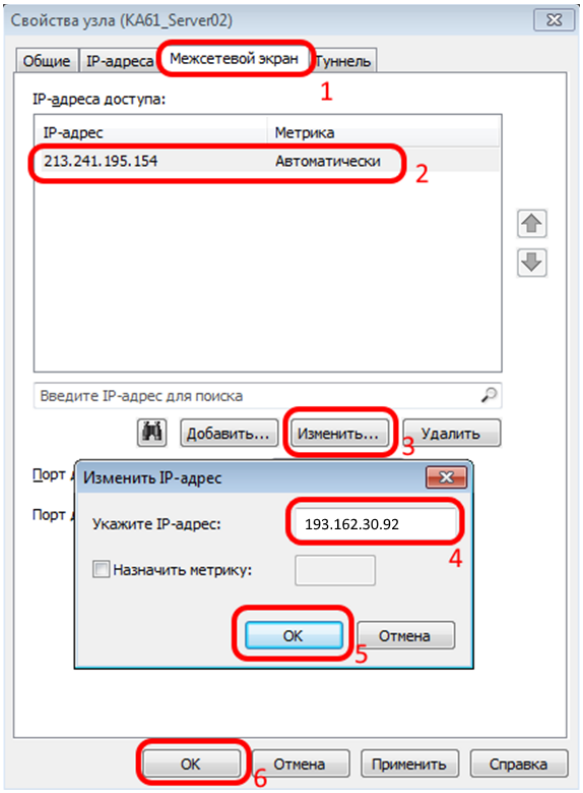

Рисунок 11

IV. Настройки транспорта, если установлена только «Деловая почта»

В случае если в систему был установлен программный комплекс ViPNet Client по выборочной схеме (установлен только модуль «Деловая почта»), то корректность настроек ViPNet «Деловая почта» следующая:

1) Открыть VipNet Client «Деловая почта», нажать кнопку ***«Отпр/Получ»*** (Рисунок 12).

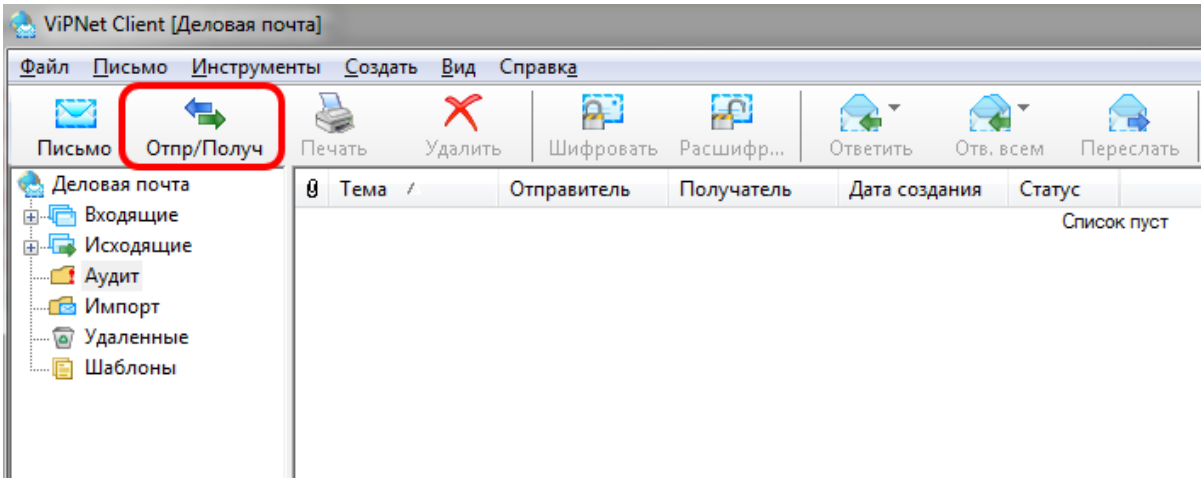

Рисунок 12

2) В открывшемся окне нажать кнопку ***«Настройки»*** (Рисунок 13).

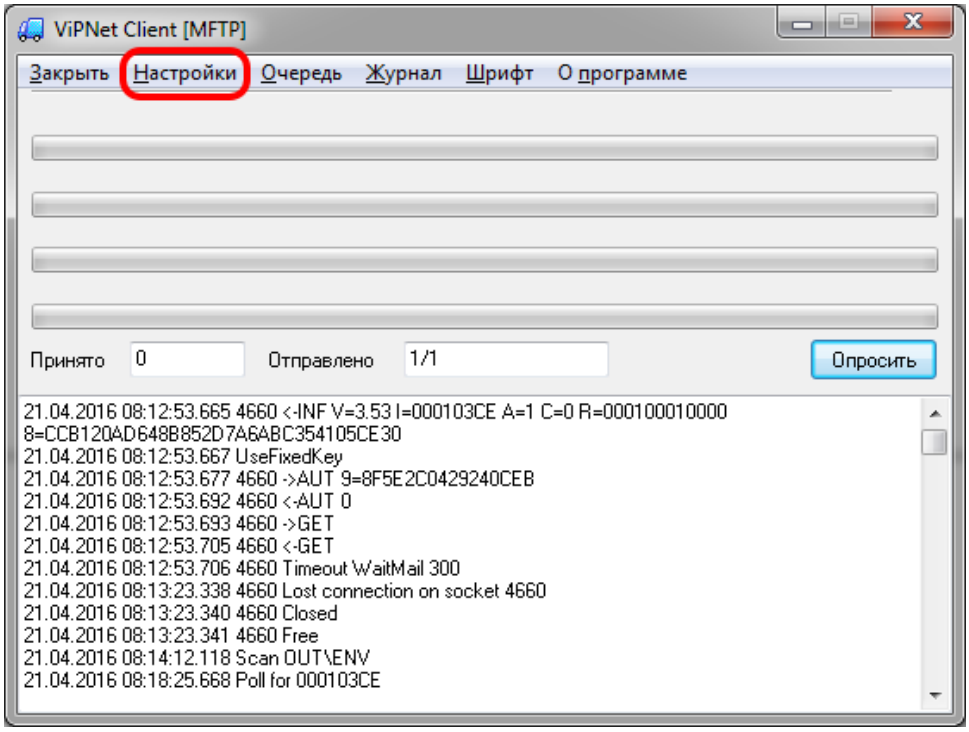

Рисунок 13

3) Во вкладке ***«Каналы»*** (Рисунок 14, позиция 1) сетевой узел ***«Координатор КА61_Server02»*** должен быть установлен с типом канала ***«MFTP»*** (Рисунок 14, позиция 2), IP адрес должен быть прописан: **193.162.30.92** (Рисунок 14, позиция 3).

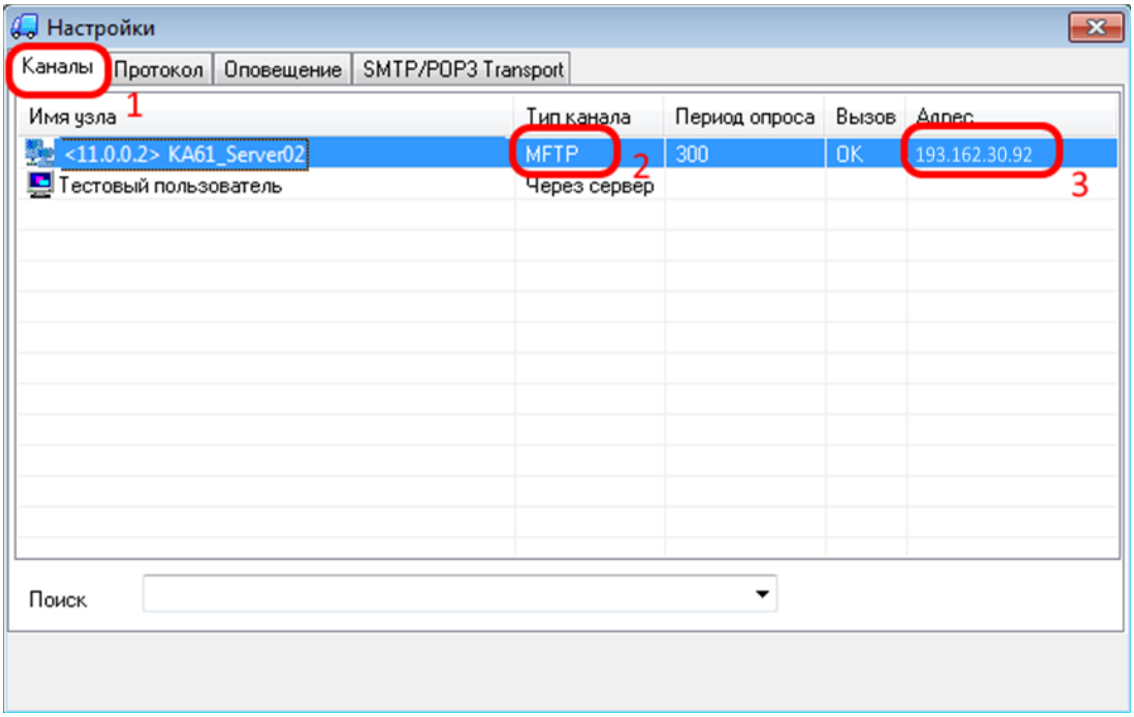

Рисунок 14

В случае если напротив ***«Координатор сети KA61_Server02»*** прописан иной IP адрес, то необходимо его исправить. Дважды кликните по нему. (Рисунок 15).

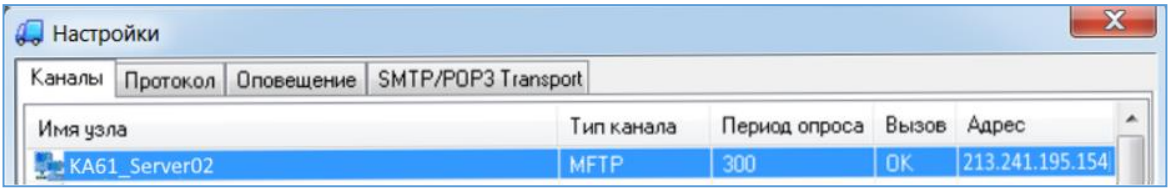

Рисунок 15

В строке ***«Адрес»*** задайте новый IP-адрес: **193.162.30.92** (Рисунок 16). Последовательно закройте все окна, нажав ***«ОК» -> «ОК»***;

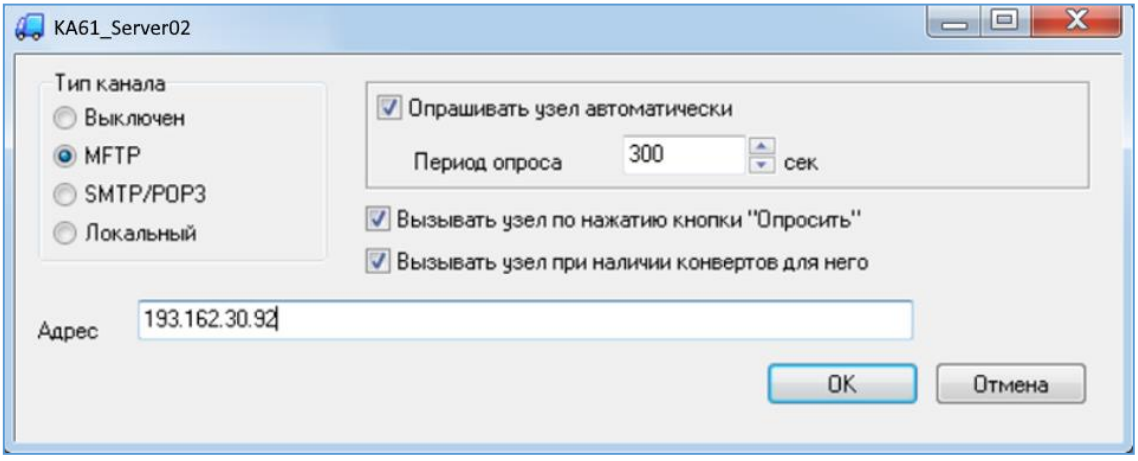

Рисунок 16

В настройках транспорта нажмите кнопку ***«Опросить»*** (Рисунок 17).

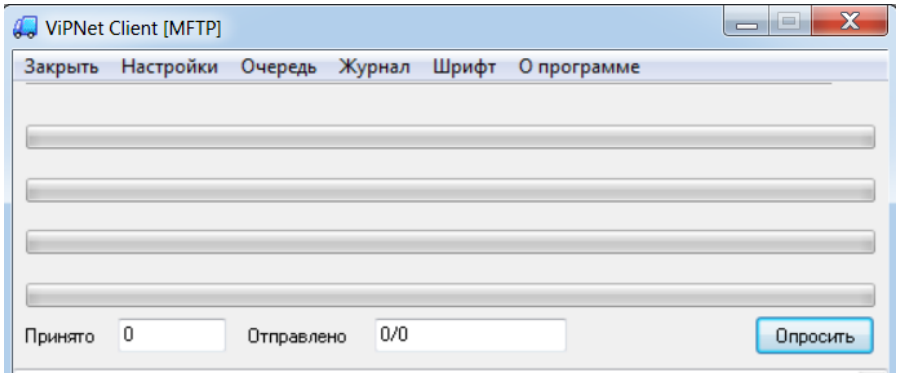

Рисунок 17

Если в окне состояния Вы видите строки *дата время Connection is already established with XXXXXXXX* – настройки успешно завершены.

Если настройки выше не помогли, откройте из каталога с установленным ПО ViPNet Деловая Почта файл ***fireaddr.doc*** с помощью стандартного текстового редактора ***«Блокнот»*** (Рисунок 18).

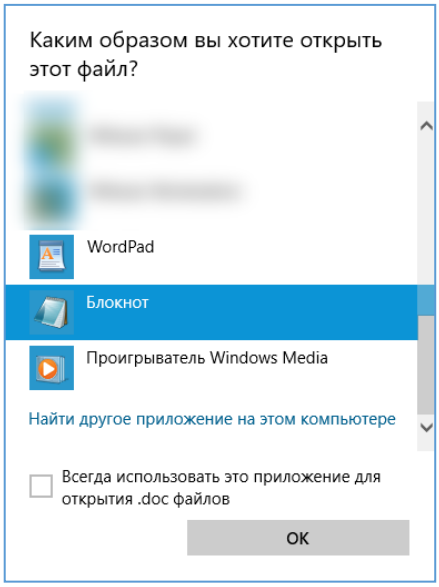

Рисунок 18

- В открывшемся файле будет прописан идентификатор сетевого узла – координатора, через который работает ViPNet Деловая Почта (**10F1001E**) и через пробел, заданный для его работы IP адрес (Рисунок 19).

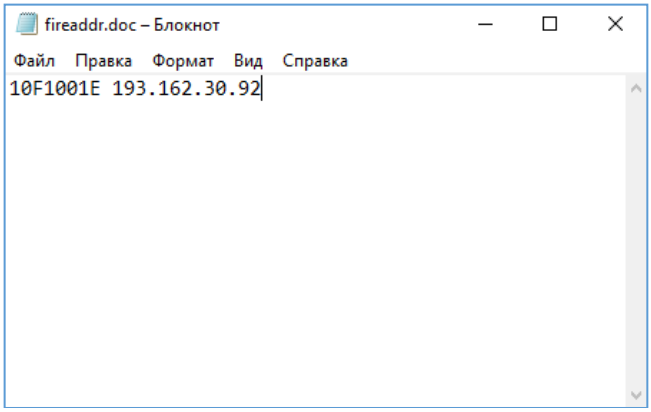

Рисунок 19

- В случае если компьютер, где установлена программа ViPNet Деловая почта, имеет прямое подключение к сети интернет, то напротив идентификатора координатора должен быть прописан реальный IP адрес: напротив, идентификатора **10F1001E** через пробел должен быть IP **193.162.30.92**. Если в открытом для редактирования файле fireaddr.doc прописан иной адрес, то его необходимо исправить и сохранить изменения при закрытии (Рисунок 20).

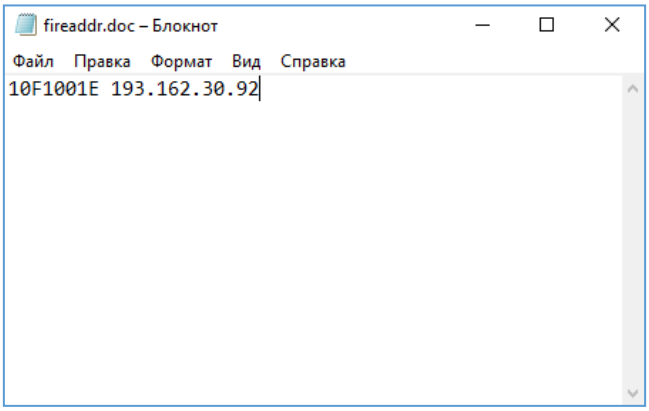

Рисунок 20

После чего, для проверки соединения необходимо отправить пустое письмо самим-себе (в получателях выбрать свой же узел) через ViPNet Деловая почта:

Если письмо пришло во ***«Входящие»*** - все настройки верны, соединение с координатором устанавливается, обмен (отправка/прием) файлов и писем со связанными защищенными узлами будет 100% выполняться.

Замечание!!! Если компьютер, где установлена программа ViPNet Client «Деловая почта» находится в сегменте локальной сети не имеющего прямого доступа в Интернет, т.е Интернет раздается прокси-сервером который при этом не поддерживает NAT, то транспорт для Деловой почты необходимо будет настроить через правила «переназначения портов».
