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

(для «Фонда перспективных исследований»)

Листов 13

АО «ИнфоТеКС Интернет Траст»
2023 г.

Оглавление

1. 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).

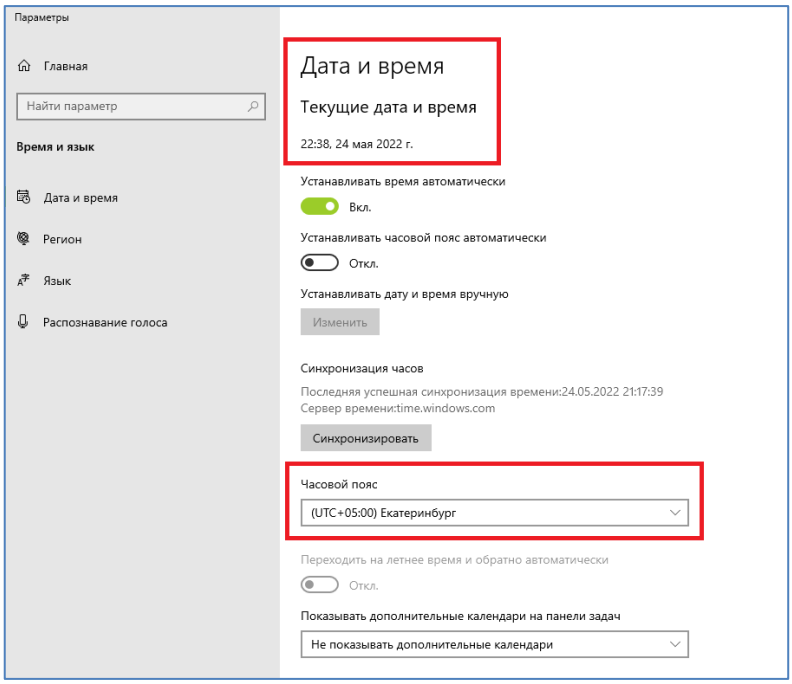

Рисунок 1

[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.

2. Настройки транспорта ViPNet Client

В случае если в систему был установлен программный комплекс ViPNet Client (модуль Monitor в версии 4.3), то корректность настроек в ПО ViPNet Client (Monitor) следующая, в зависимости от сервера маршрутизатора (СМ) за которым работает ваш абонентский пункт (АП):

А. Настройка транспорта для АП, работающих за СМ «Координатор сети УЦ ИИТ [4337] [01]»

Б. Настройка транспорта для АП, работающих за СМ « Server Coordinator IIT»

А. Настройка транспорта для АП, работающих за СМ «Координатор сети УЦ ИИТ [4337] [01]»

ViPNet Client должен быть выставлен за региональный координатор (сетевой узел – маршрутизатор) ***«Координатор сети УЦ ИИТ [4337] [01]»***, расположенный на площадке АО «ИнфоТеКС Интернет Траст». Для этого необходимо чтобы были выставлены следующие настройки в ViPNet Client:

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

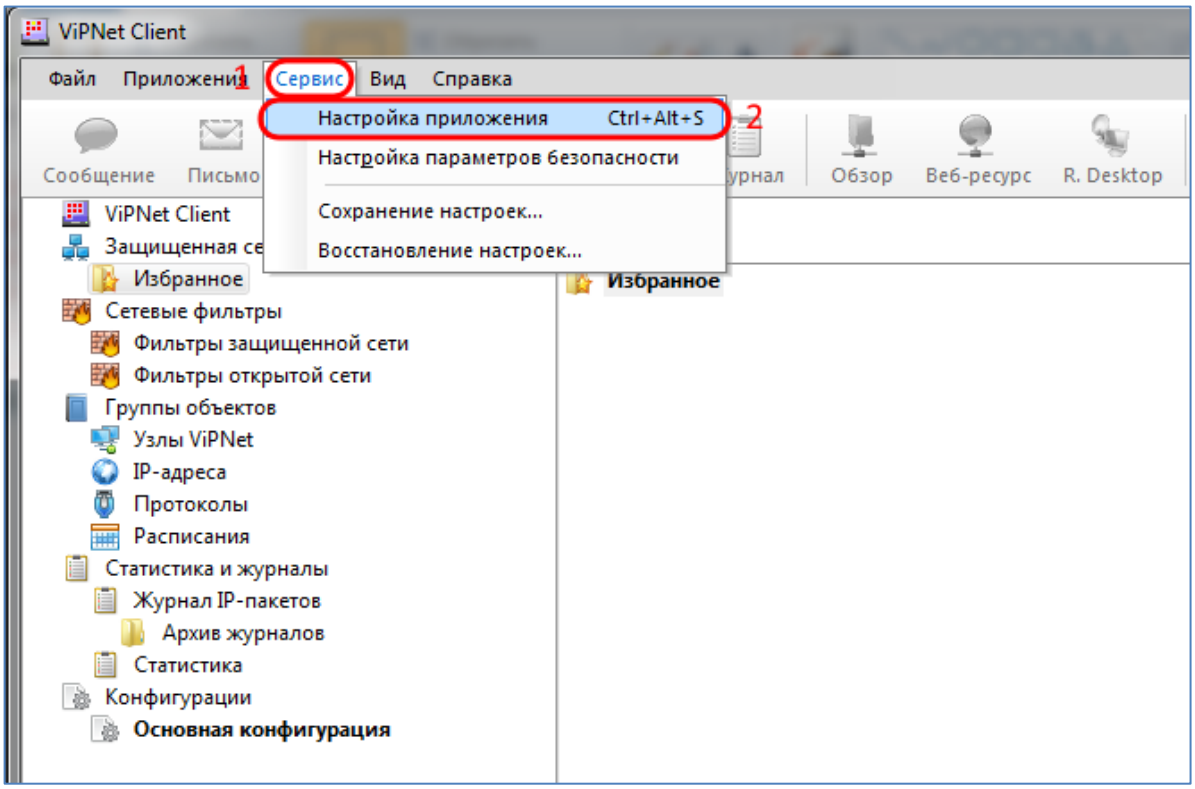

Рисунок 2

В открывшемся окне выберите раздел ***«Защищенная сеть»*** (Рисунок 3, позиция 1), в поле ***«Сервер соединений:»*** должен быть выбран ***«Координатор сети УЦ ИИТ [4337] [01]»*** (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 сети УЦ ИИТ [4337] [01]»*** (Рисунок 3, позиция 4).

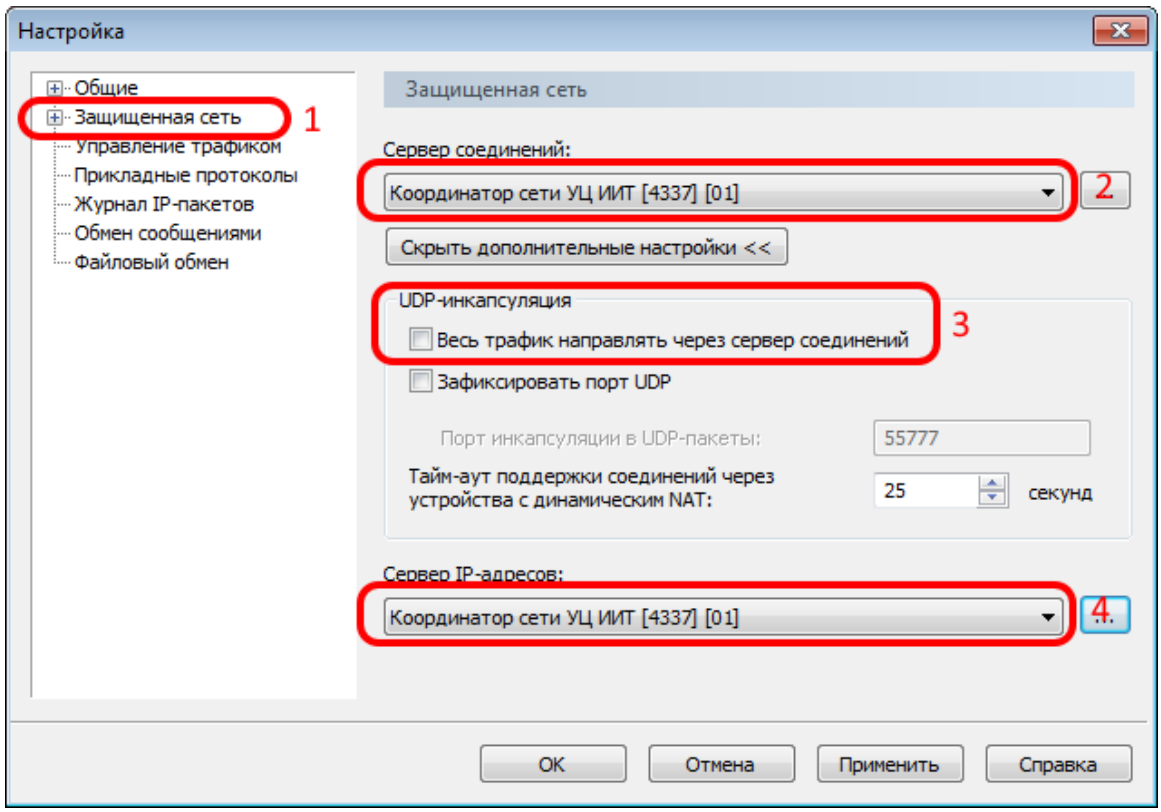

Рисунок 3

Если у вас были выставлены иные настройки, то необходимо их привести в соответствие с Рисунок 3.

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

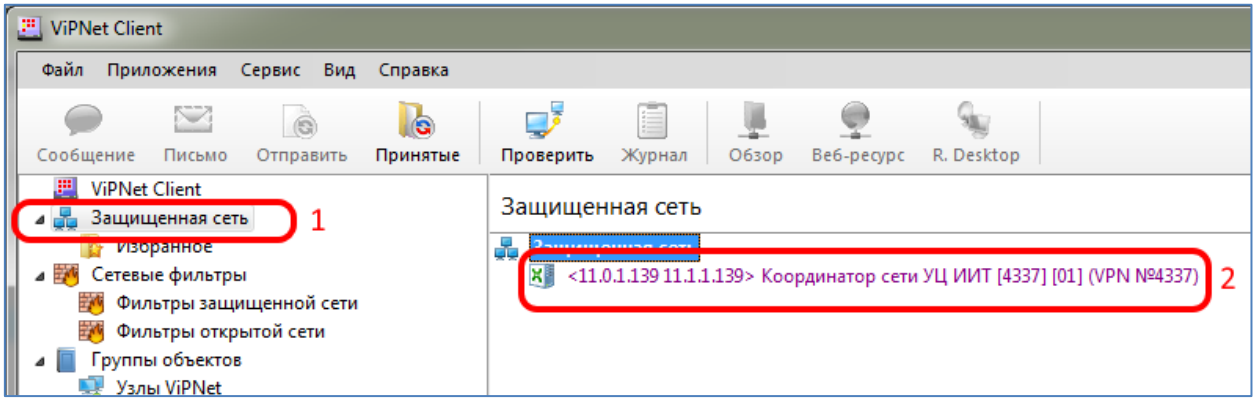

Рисунок 4

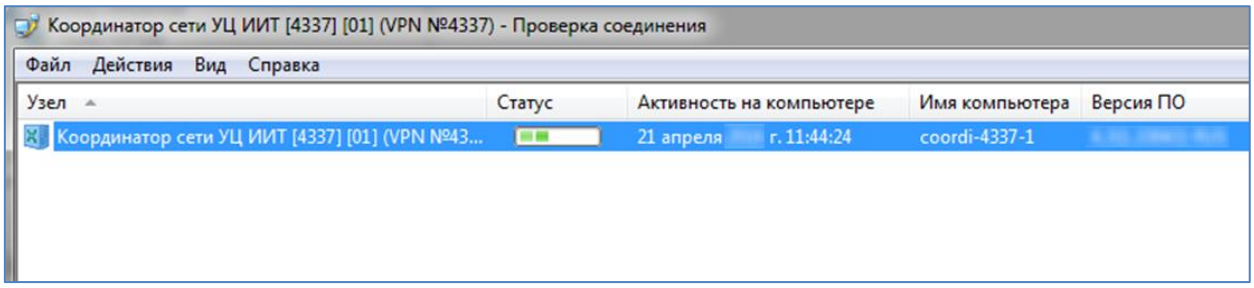

Рисунок 5

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

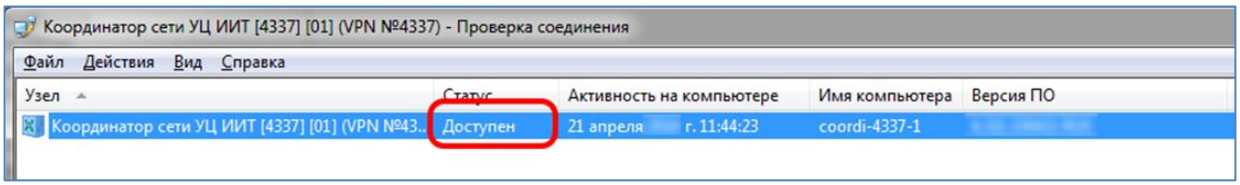

Рисунок 6

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

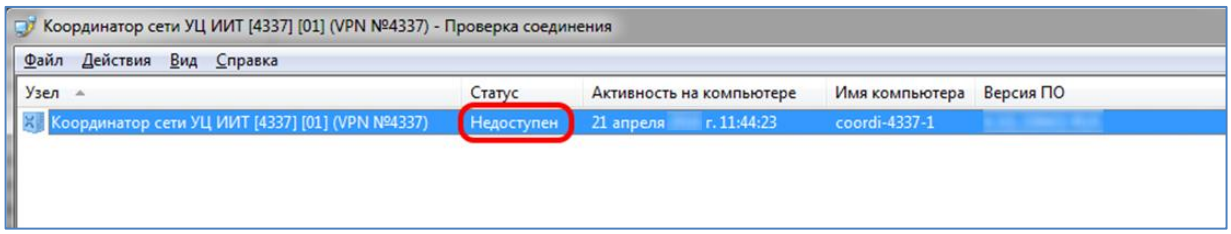

Рисунок 7

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

- Соблюдение всех рекомендаций, применимых к настройкам операционной системы, указанных на странице 3 данной инструкции;
- Проверить настройки правил доступа для координатора. Для этого щелкните двойным кликом левой кнопки мышки по строке ***«Координатор сети УЦ ИИТ [4337] [01]»*** в разделе ***«Защищенная сеть»*** (Рисунок 4, позиция 1), в результате откроется окно ***«Свойства узла»*** (Рисунок 8);

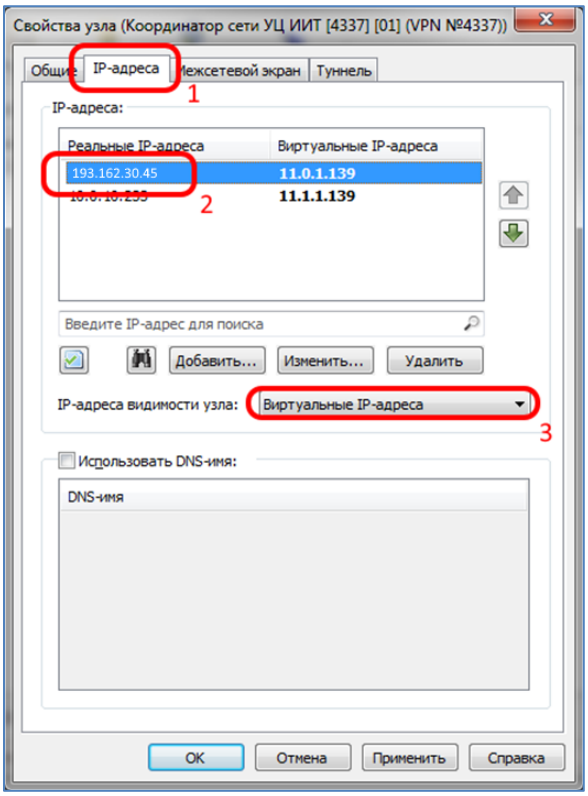

Рисунок 8

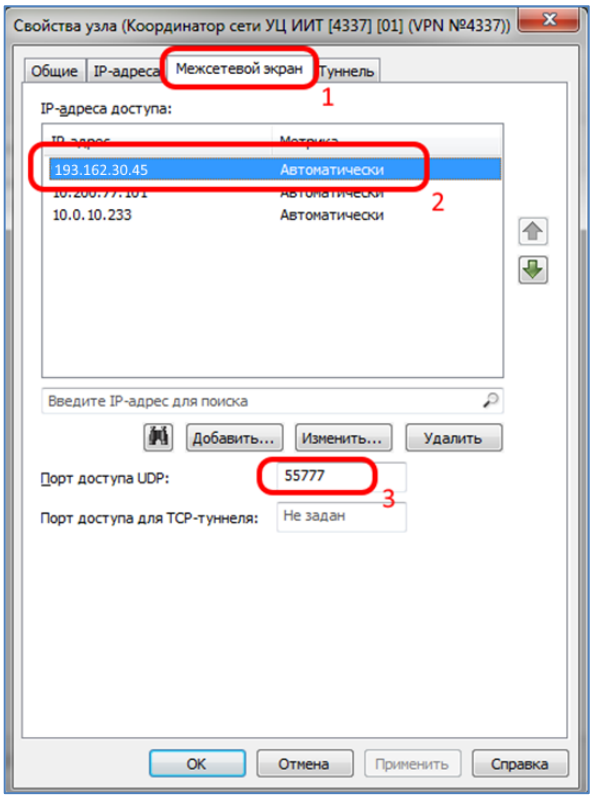

Рисунок 9

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 **193.162.30.45**;
- 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 **193.162.30.45** (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 **193.162.30.45** (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 **193.162.30.45** (Рисунок 11, позиция 4), нажать кнопку ***«ОК»*** (Рисунок 11, позиция 5);
- Нажать кнопку ***«ОК»*** (Рисунок 11, позиция 6).

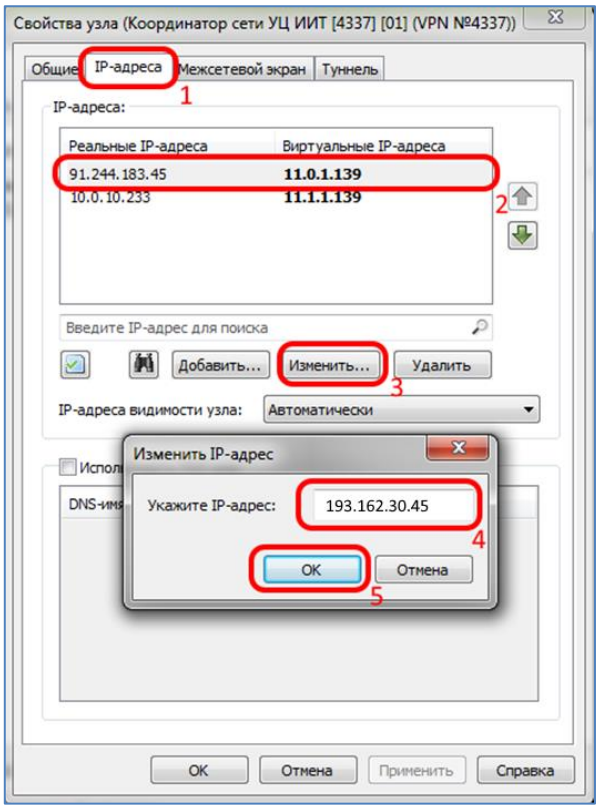

Рисунок 10

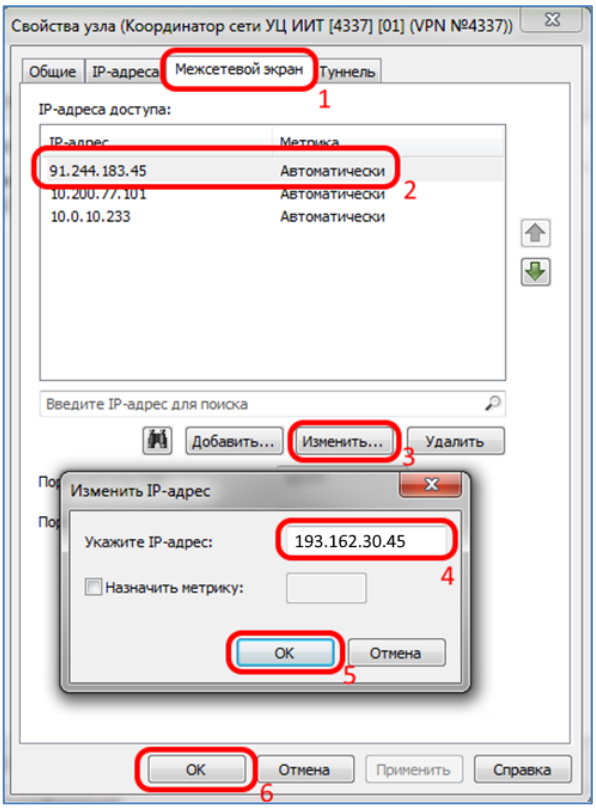

Рисунок 11

Б. Настройка транспорта для АП, работающих за СМ «_Server_Coordinator_IIT»

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

Откройте - ***«Сервис»*** -> ***«Настройка приложения»*** (Рисунок 12).

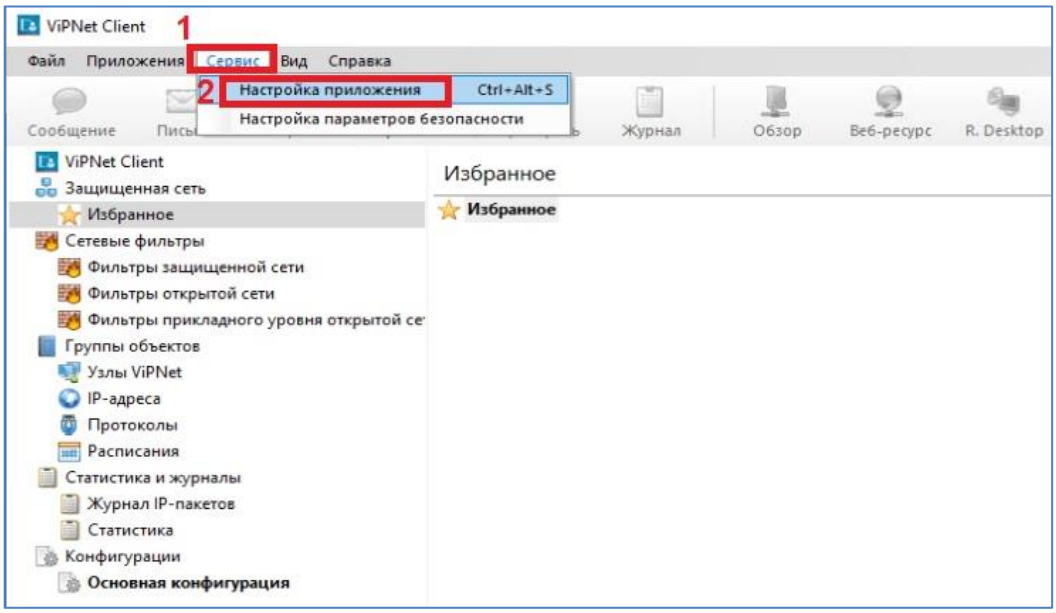

Рисунок 12

В открывшемся окне выберите раздел ***«Защищенная сеть»*** (Рисунок 13, позиция 1), в поле ***«Сервер соединений:»*** должен быть выбран ***«_Server_Coordinator_IIT»*** (Рисунок 13, позиция 2). В поле ***«UDP-инкапсуляция»*** - галочка ***«Весь трафик направлять через сервер***

соединений» **не должна** быть установлена (Рисунок 13, позиция 3). В поле ***«Сервер IP-адресов:»*** должен быть выбран ***«_Server_Coordinator_IIT»*** (Рисунок 13, позиция 4).

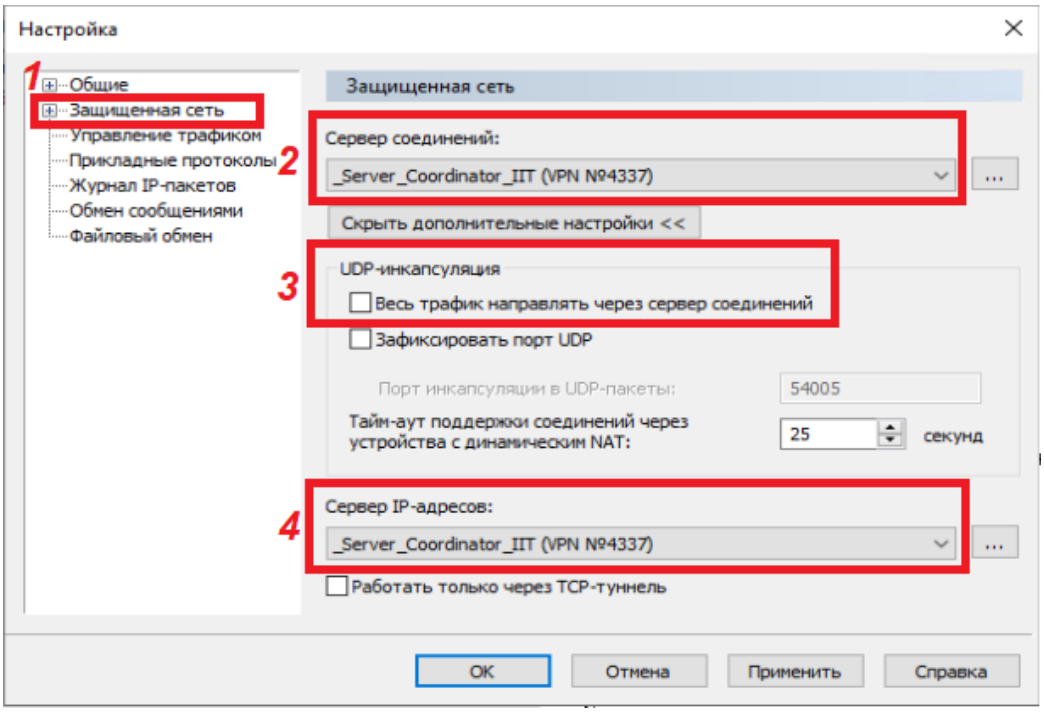

Рисунок 13

Если у вас были выставлены иные настройки, то необходимо их привести в соответствие с Рисунок 13.

В ViPNet Client, откройте раздел ***«Защищенная сеть»*** (Рисунок 14, позиция 1), выделите мышкой сетевой узел (координатор) за который заведен текущий абонентский пункт (Рисунок 14, позиция 2), затем нажмите на клавиатуре клавишу ***«F5»***, таким образом запустится проверка соединения с выделенным в защищенной сети сетевым узлом (Рисунок 15).

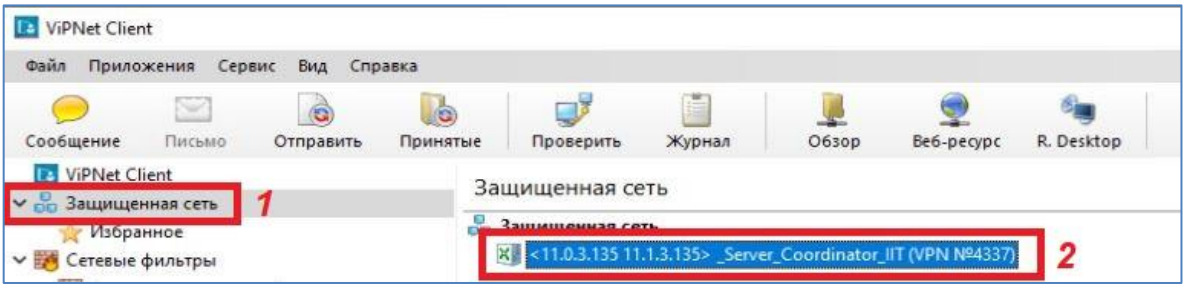

Рисунок 14

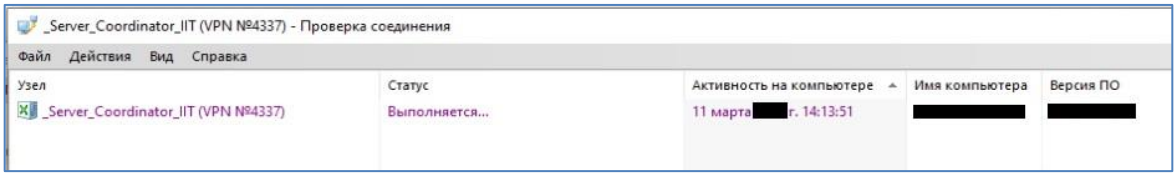

Рисунок 15

В случае если интернет доступен и инициативные соединения по порту **UDP 55777** ничем не ограничены для текущего компьютера, то отобразится статус ***«Доступен»*** (Рисунок 16), при выполнении этих условий обмен (отправка/прием) файлов и писем со связанными защищенными узлами будет 100% выполняться.

Рисунок 16

Если при проверке соединения с координатором соединение долгое время не устанавливается – статус отобразится как ***«Недоступен»*** (Рисунок 17).

Рисунок 17

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

- Соблюдение всех рекомендаций, применимых к настройкам операционной системы, указанных на странице 3 данной инструкции;
- Проверить настройки правил доступа для координатора. Для этого щелкните двойным кликом левой кнопки мышки по строке ***«_Server_Coordinator_IIT»*** в разделе ***«Защищенная сеть»*** (Рисунок 14, позиция 1), в результате откроется окно ***«Свойства узла»*** (Рисунок 18);

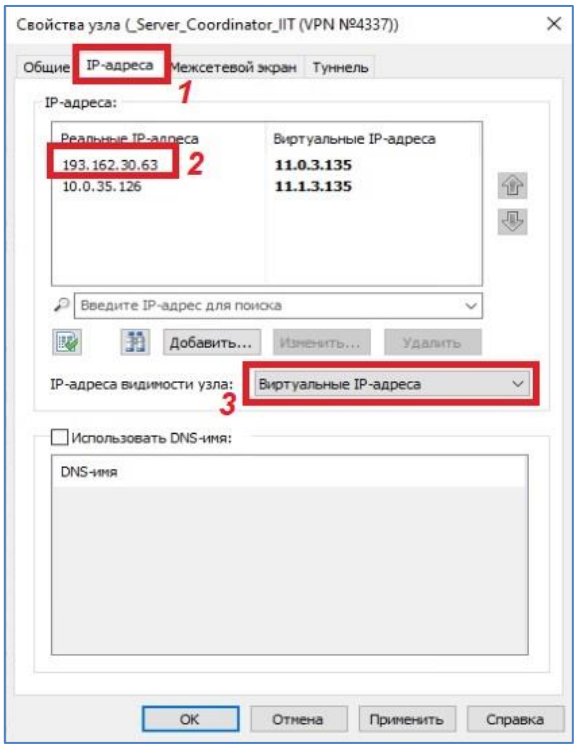

Рисунок 18

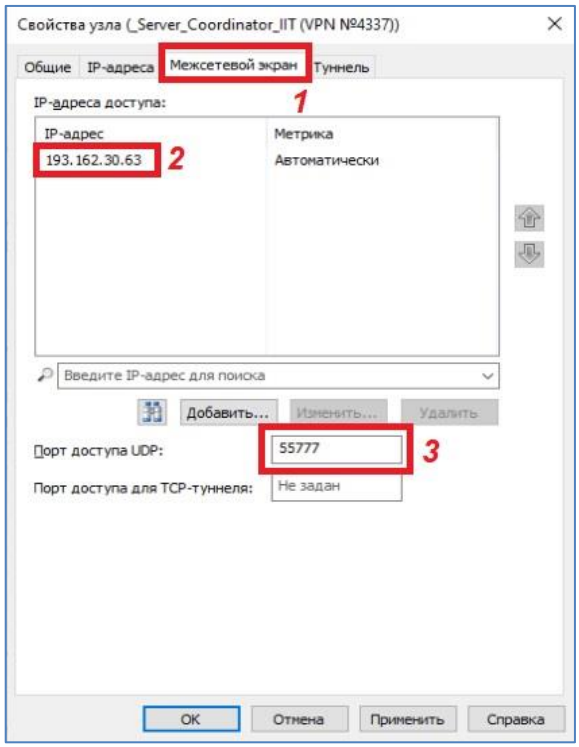

Рисунок 19

В окне ***«Свойства узла»***:

Откройте вкладку ***«IP адреса»*** (Рисунок 18, позиция 1), затем проверьте:

- Правильность IP адреса (Рисунок 18, позиция 2) указанного в поле ***«IP адреса»*** - должен присутствовать **193.162.30.63**;

- В поле ***«IP-адреса видимости узла:»*** - должен быть выбран пункт ***«Виртуальные IP-адреса»*** (Рисунок 18, позиция 3).

Откройте вкладку ***«Межсетевой экран»*** (Рисунок 19, позиция 1), затем проверьте:
В поле ***«IP-адреса доступа»*** - должен присутствовать **193.162.30.63** (Рисунок 19, позиция 2);
В поле ***«Порт доступа UDP:»*** - должен быть указан **55777** (Рисунок 19, 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 20, позиция 1):

- Выделите старый IP адрес (Рисунок 20, позиция 2), и нажмите кнопку ***«Изменить»*** (Рисунок 20, позиция 3);
- Введите значение **193.162.30.63** (Рисунок 20, позиция 4), затем нажмите кнопку ***«ОК»*** (Рисунок 20, позиция 5).

Изменение IP адреса во вкладке ***«Межсетевой экран»*** (Рисунок 21, позиция 1):

- Выделите старый IP адрес (Рисунок 21, позиция 2), нажать кнопку ***«Изменить»*** (Рисунок 21, позиция 3);
- Ввести значение **193.162.30.63** (Рисунок 21, позиция 4), нажать кнопку ***«ОК»*** (Рисунок 21, позиция 5);
- Нажать кнопку ***«ОК»*** (Рисунок 21, позиция 6).

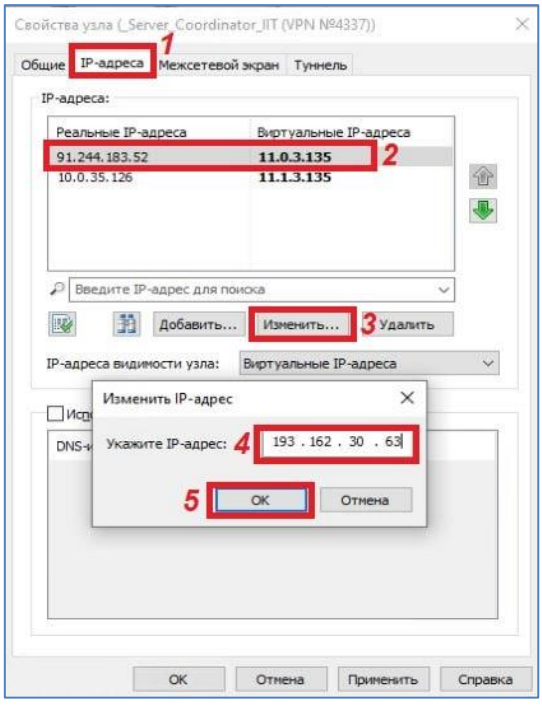

Рисунок 20

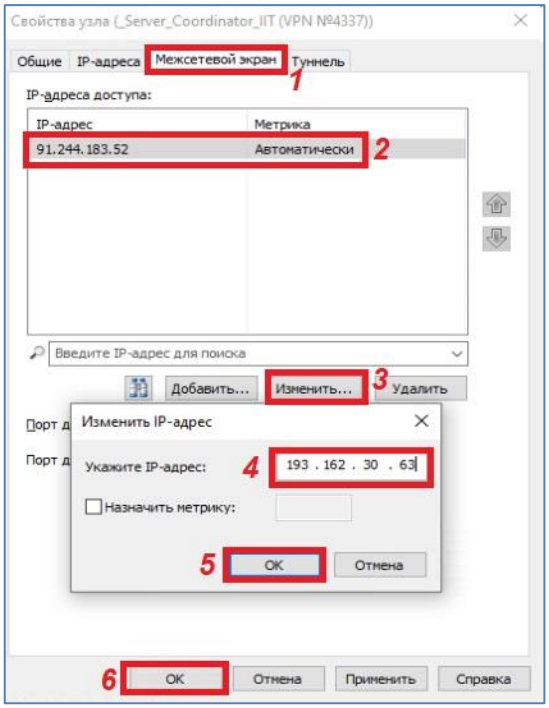

Рисунок 21

3. Настройки подключения к ФПИ

В ViPNet Client открыть раздел ***«Защищенная сеть»*** (Рисунок 22

, позиция 1), выделить мышкой сетевой узел (координатор) **«СК (VPN №3745)»** (Рисунок 22

, позиция 2), нажать на клавиатуре клавишу ***«F5»***, таким образом запустится проверка соединения с выделенным в защищенной сети сетевым узлом.

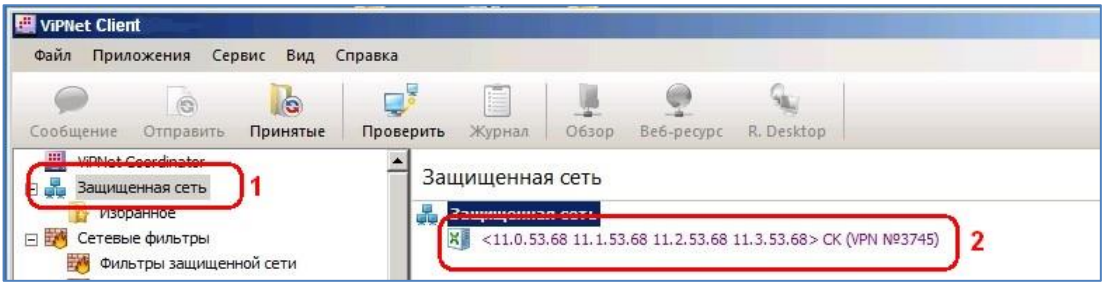

Рисунок 22

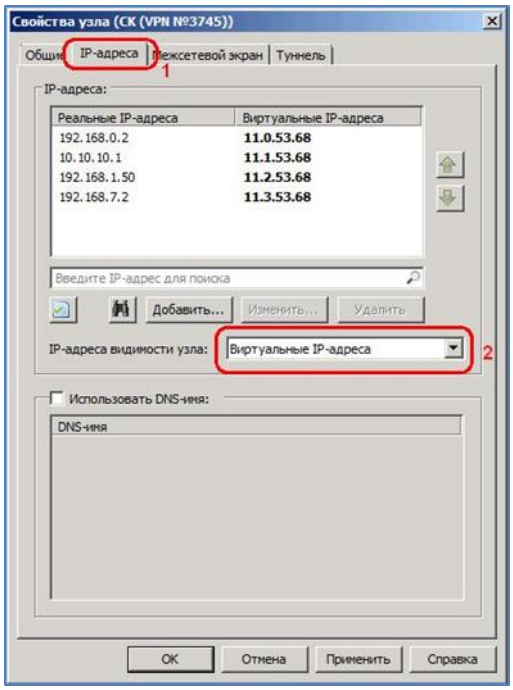

Рисунок 23

Проверить настройки правил доступа для сетевого узла (координатора). Для этого щелкните двойным кликом левой кнопки мышки по строке **«СК (VPN №3745)»** в разделе ***«Защищенная сеть»*** (Рисунок 22, позиция 2), в результате откроется окно ***«Свойства узла»*** (Рисунок 23);

В окне ***«Свойства узла»***:

Открыть вкладку ***«IP адреса»*** (Рисунок 23, позиция 1). В поле ***«IP-адреса видимости узла»*** должен быть выбран пункт ***«Виртуальные IP-адреса»*** (Рисунок 23, позиция 2).
Открыть вкладку ***«Межсетевой экран»*** (Рисунок 24, позиция 1), проверить:

- В поле ***«IP-адреса доступа»*** должен присутствовать **79.98.209.228** (Рисунок 24, позиция 2);
- В поле ***«Порт доступа UDP»*** должен быть указано **55777** (Рисунок 24, позиция 3);

Открыть вкладку ***«Туннель»*** (Рисунок 25, позиция 1), проверить:

- В пункте «***Использовать IP-адреса для туннелирования»*** должна стоять галочка (Рисунок 25, позиция 2);
- Правильность IP-адреса (Рисунок 25, позиция 3), указанного в поле ***«Реальные IP-адреса»*** - должен присутствовать **192.168.1.40**;
- В пункте «***Использовать виртуальные IP-адреса»*** должна стоять галочка (Рисунок 25, позиция 5);
- В пункте «***Не туннелировать IP-адреса, входящие в подсеть Вашего компьютера»*** должна стоять галочка (Рисунок 25, позиция 6);

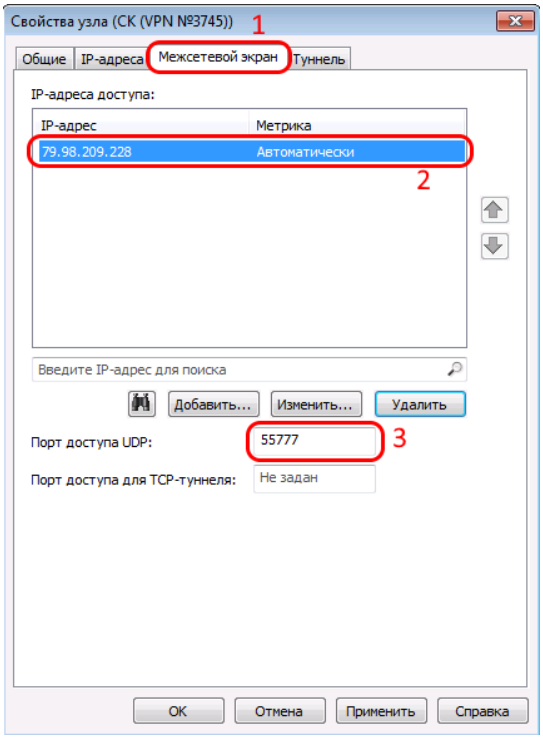

Рисунок 24

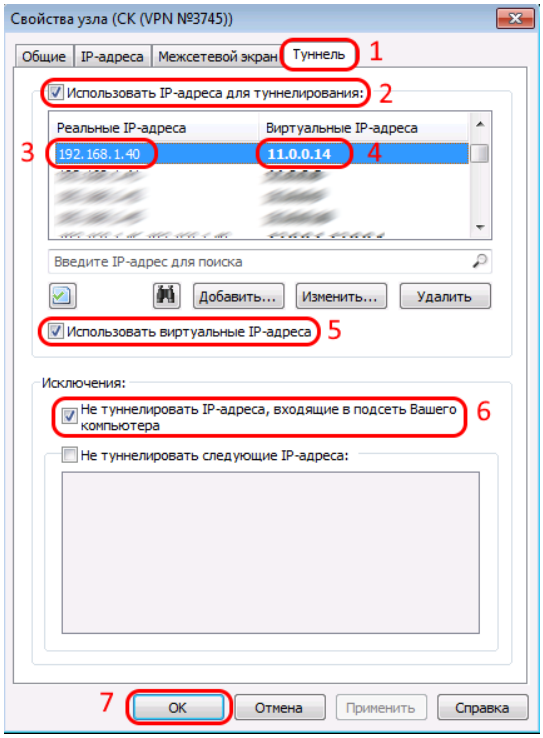

Рисунок 25

В случае если настройки отличались от указанных в данной инструкции, необходимо исправить их, затем нажать кнопку ***«Применить»***.

1) После проведения данных настроек у каждой организации появится индивидуальный IP-адрес доступа к порталу (Рисунок 25, позиция 4), **11.0.0.XXX** – виртуальный IP-адрес доступа организации к порталу, индивидуальный для каждой организации формируемый программой ViPNet Client.

2) Запустите браузер и введите адрес **http://11.0.0.XXX:8080**

3) Если в организации используется прокси-сервер, то адрес доступа к порталу необходимо внести в исключения (чтобы для этого адреса не использовался прокси-сервер).

4) Если связь с координатором ФПИ проверяется, а вход на портал не возможен, то в пункте «***Не туннелировать IP-адреса, входящие в подсеть Вашего компьютера»*** можно снять галочку (Рисунок 25, позиция 6) и проверить доступ к сайту.

v4