

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

(для «Координатор ТФОМС РО»)

Листов 8

Оглавление

I. Введение	3
II. Общие и обязательные рекомендации по настройке транспорта ViPNet Client.....	4
III. Настройка транспорта	5

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 некорректную работу программы ViPNet Client;
- ✓ Необходимо обращать особое внимание на примечания помеченные знаком ➡.

➡ **Внимание! Вид окон может отличаться в зависимости от используемой операционной системы.**

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 55778¹** – если установлен **ViPNet Monitor + «Деловая почта»**;
 - открыть порты **TCP/IP²** 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).

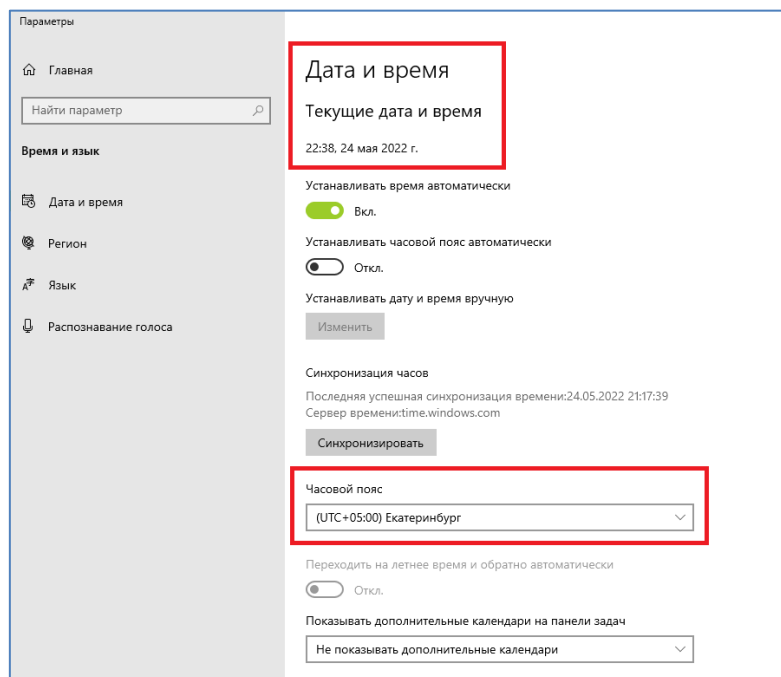


Рисунок 1

¹ Если Интернет в организации раздается локальным компьютерам через шлюз или прокси-сервер, то инициативные соединения по порту UDP 55778 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. Настройка транспорта

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

ViPNet Client Monitor должен быть выставлен за **«Координатор ТФОМС РО»**. Для этого необходимо чтобы были выставлены следующие настройки в ViPNet Client Monitor:

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

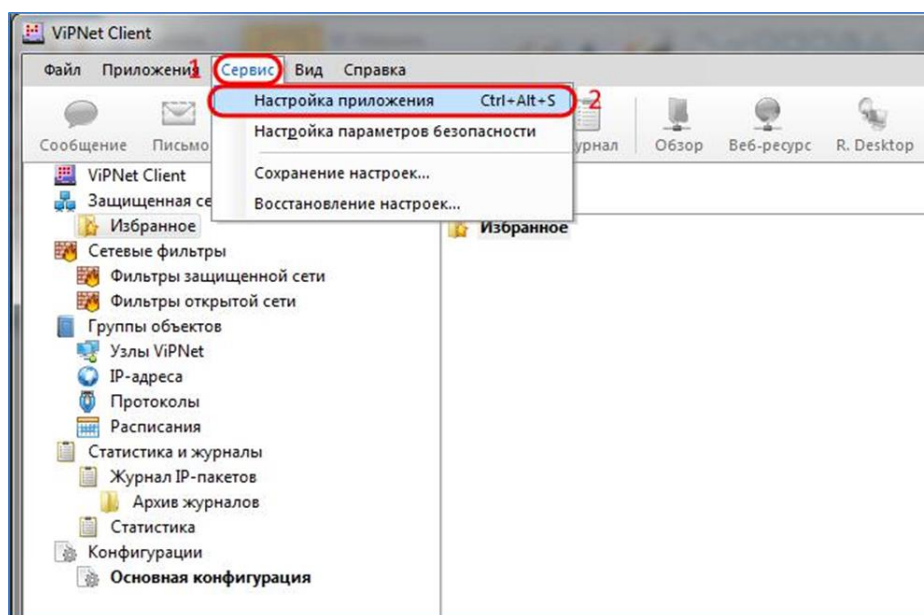


Рисунок 2

В открывшемся окне выберите раздел **«Защищенная сеть»** (Рисунок 3, позиция 1), в поле **«Сервер соединений»** должен быть выбран **«Координатор ТФОМС РО»** (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 ТФОМС РО»** (Рисунок 3, позиция 4).

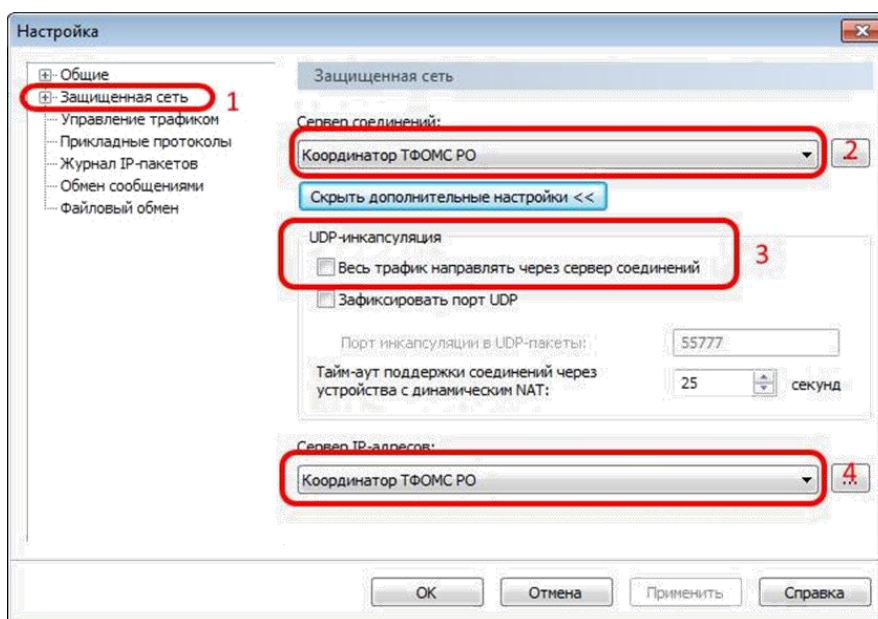


Рисунок 3

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

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

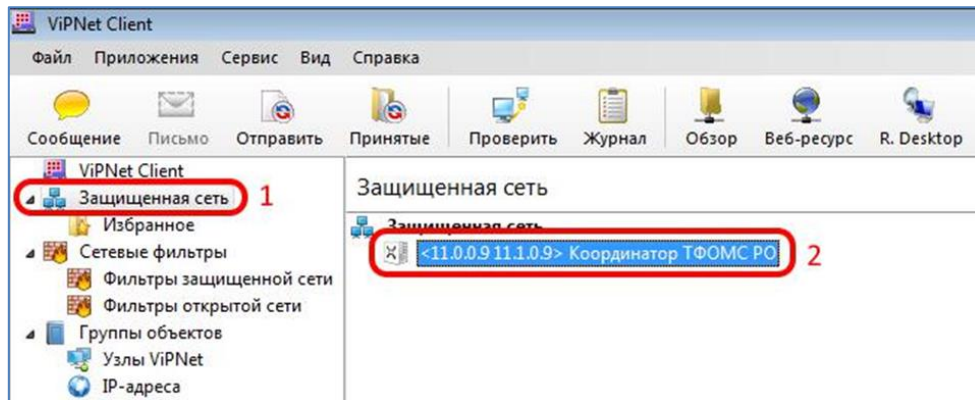


Рисунок 4

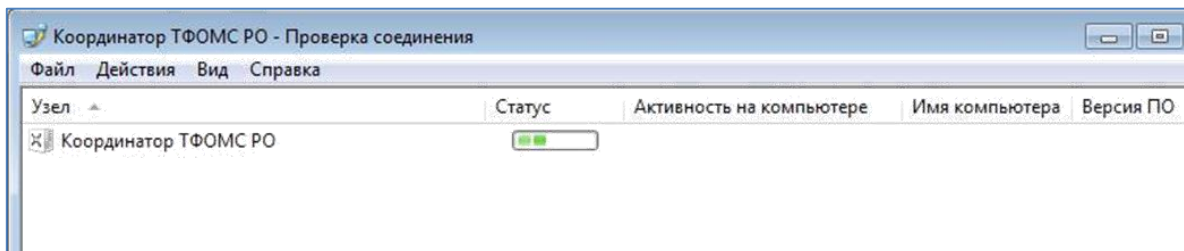


Рисунок 5

В случае если интернет доступен и инициативные соединения по порту **UDP 55778** 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 выполняться.

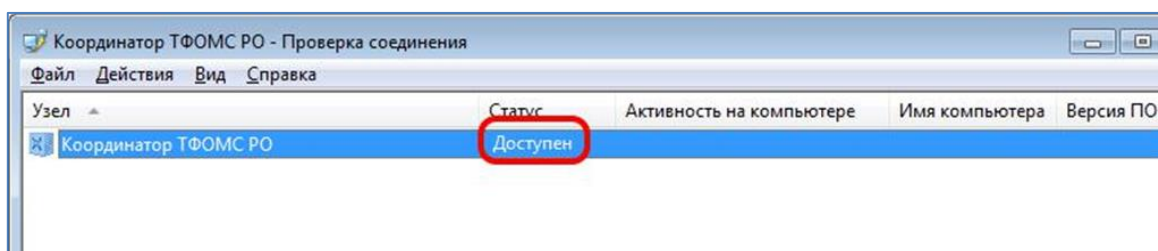


Рисунок 6

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

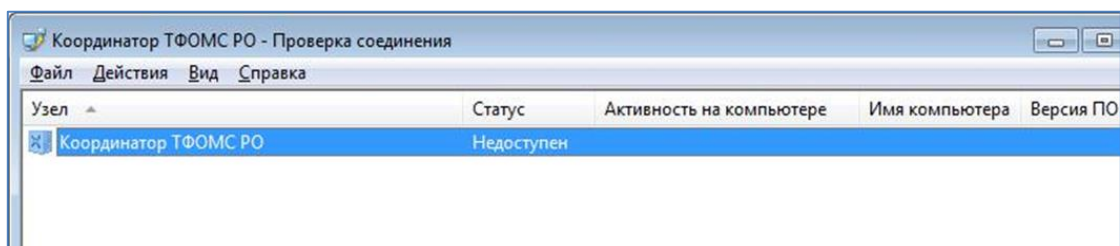


Рисунок 7

В этом случае необходимо проверить:

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

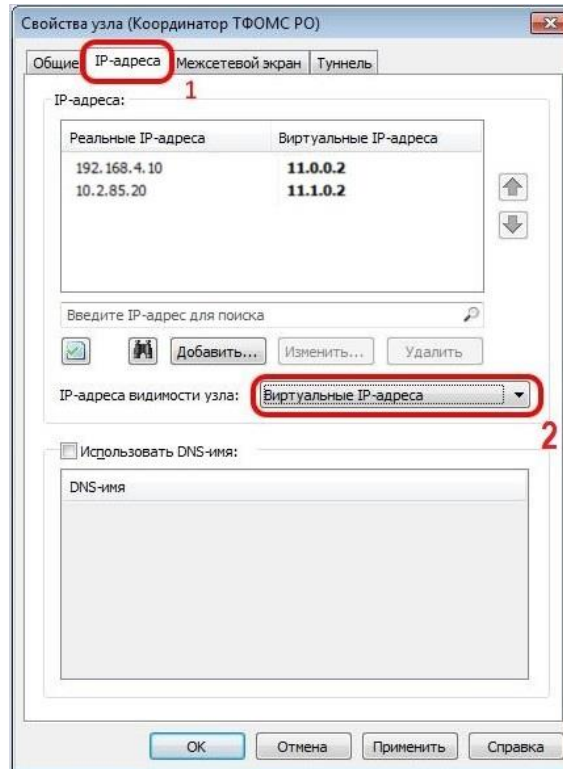


Рисунок 8

- ✓ В окне **«Свойства узла»**:
 - Откройте вкладку **«IP адреса»** (Рисунок 8, позиция 1). В поле **«IP-адреса видимости узла»** должен быть выбран пункт **«Виртуальные IP-адреса»** (Рисунок 8, позиция 2).
 - Откройте вкладку **«Межсетевой экран»** (Рисунок 9, позиция 1), затем проверьте:
 - В поле **«IP-адреса доступа»** должен присутствовать **93.178.96.202** (Рисунок 9, позиция 2);
 - В поле **«Порт доступа UDP»** должен быть указано **55778** (Рисунок 9, позиция 3);
 - Откройте вкладку **«Туннель»** (Рисунок 10, позиция 1), затем проверьте:
 - В пункте **«Использовать IP-адреса для туннелирования»** должна стоять галочка (Рисунок 10, позиция 2);
 - Правильность IP-адресов (Рисунок 10, позиция 3), указанных в поле **«Реальные IP-адреса»** - должны присутствовать **192.168.4.19** и **192.168.0.101**;
 - В пункте **«Использовать виртуальные IP-адреса»** должна стоять галочка (Рисунок 10, позиция 5);
 - В пункте **«Не туннелировать IP-адреса, входящие в подсеть Вашего компьютера»** должна стоять галочка (Рисунок 10, позиция 6);

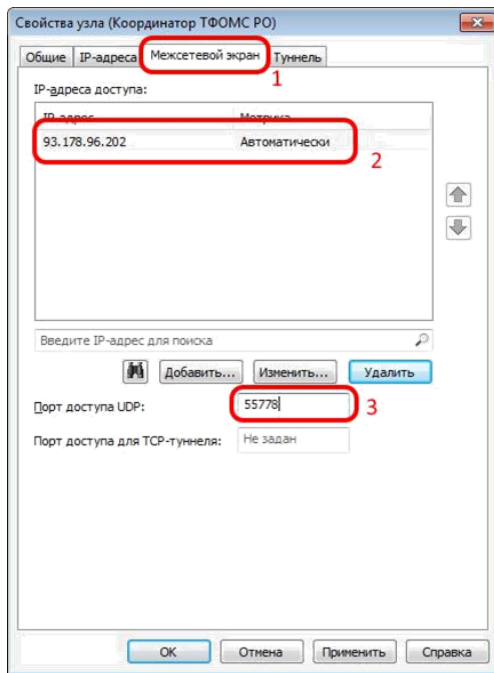


Рисунок 9

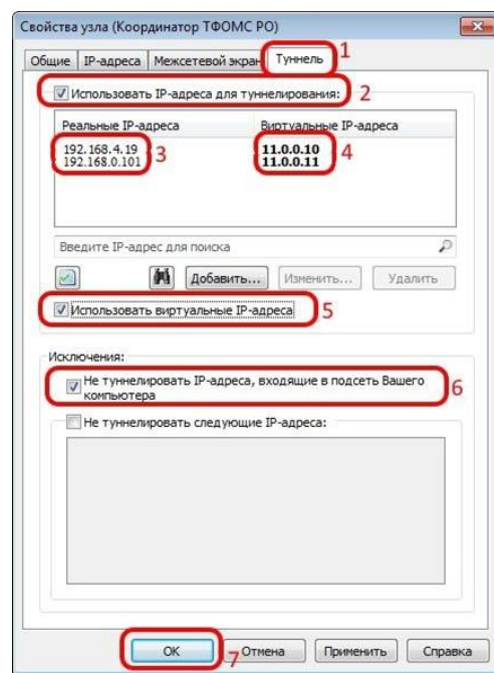


Рисунок 10

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

После проведения данных настроек у каждой организации появится индивидуальный IP-адрес доступа к portalу **11.0.0.XXX** – виртуальный IP-адрес доступа организации к portalу, индивидуальный для каждой организации, формируемый программой ViPNet Client Monitor.

Запустите браузер и введите адрес:

- для **регионального информационного ресурса (РИР)** виртуальный IP-адрес, соответствующий реальному IP-адресу **192.168.4.19** (Рисунок 10, позиция 4) в формате - <http://11.0.0.XXX/FomsInsurance>
- для **портала сервисов прикрепленного населения** виртуальный IP-адрес, соответствующий реальному IP-адресу **192.168.0.101** (Рисунок 10, позиция 4) в формате - <http://11.0.0.XXX:443>

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

➡ **Внимание! Если производите установку впервые, то доступ к portalу будет отсутствовать. Для получения доступа необходимо обратиться в ТФОМС РО**