Санкт – Петербургский Национальный Исследовательский

Университет Информационных Технологий, Механики и Оптики

Кафедра Программных систем

Отчет по лабораторной работе

Построение корпоративной VPN с помощью ПО «Infotecs VipNet»

Выполнил:

Антонов Е.П

Группа: К4120

Проверил: к.т.н. Ананченко И.В.

Санкт – Петербург

2017

Цель работы

Настроить корпоративную VPN при помощи ПО “Infotecs VipNet”.

Ход работы

Построение корпоративной VPN при помощи ПО “Infotecs VipNet” состоит в распределении ролей между участниками такой сети. Наиболее часто использующиеся узлы сети – это администратор, координатор и клиент.

VipNet «Администратор» состоит из двух глобальных частей:

- ЦУС – центр управления сетью
- УКЦ – удостоверяющий и ключевой центр

VipNet «Координатор» – аналог DHCP, DNS, межсетевое взаимодействие с другой сетью

VipNet «Клиент» – это пользователи сети, представляющие рабочее место.

Рабочее место настраивается при помощи следующих конфигурационных файлов:

- КН – ключевой набор
- КД – ключевая дискета
- Справочник
- Infotecs.re – файл сгенерированных специально для данного рабочего места

Настроим три виртуальные машины на основе общего материнского виртуального жёсткого диска. Это позволит ускорить запуск виртуальных машин. Одну виртуальную машину настроим под VipNet «Координатор», а две других будут играть роль VipNet «Клиент».

Начнём с установки приложения координатора.

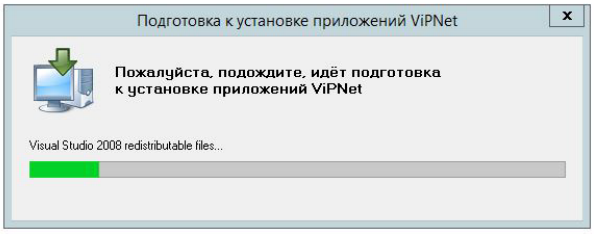

Рисунок 1 – Начало установки координатора

Примем условия лицензионного соглашения.

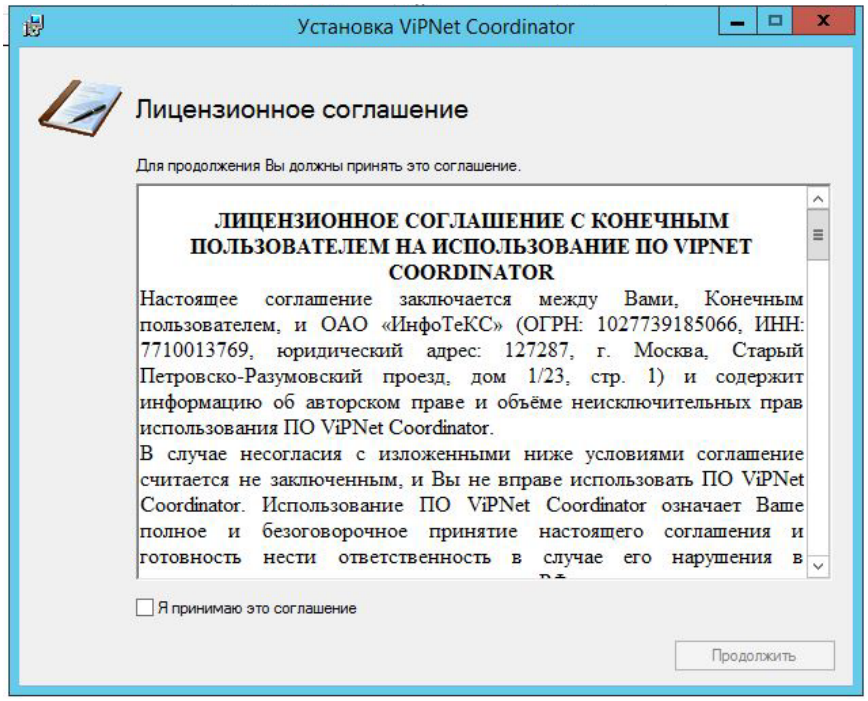

Рисунок 2 – Лицензионное соглашение

Начнём установку программного обеспечения

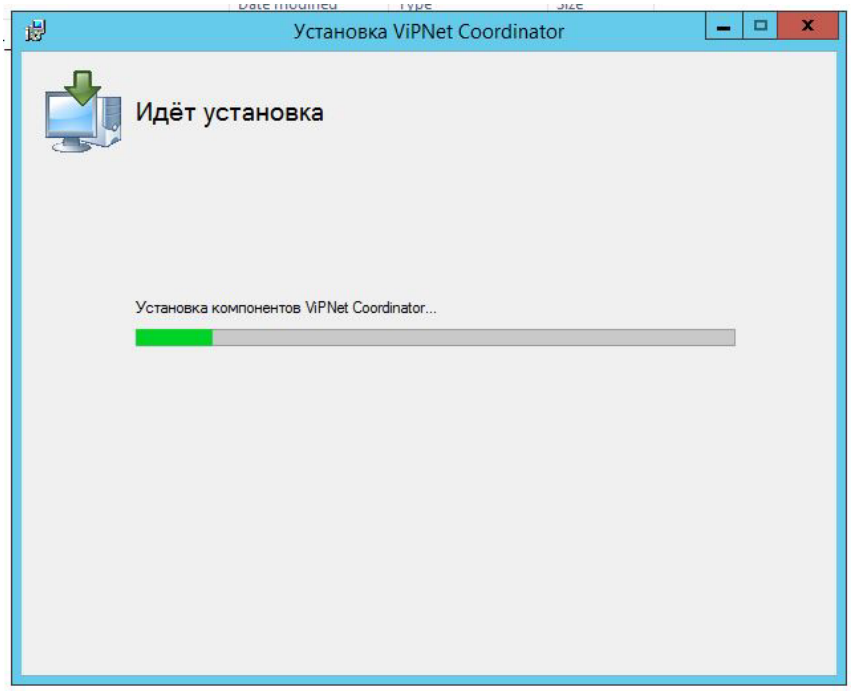

Рисунок 3 – Установка VipNet «Координатор»

Координатор успешно установлен.

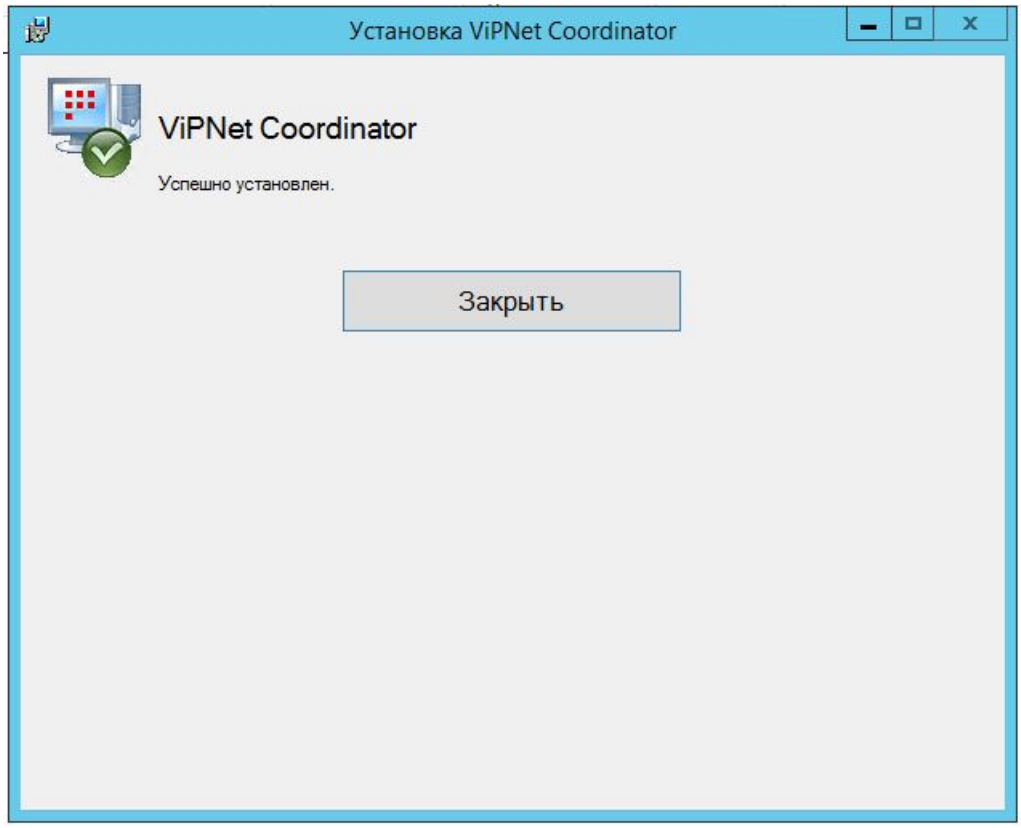

Рисунок 4 – Установка завершена

Установим ключи сети VipNet

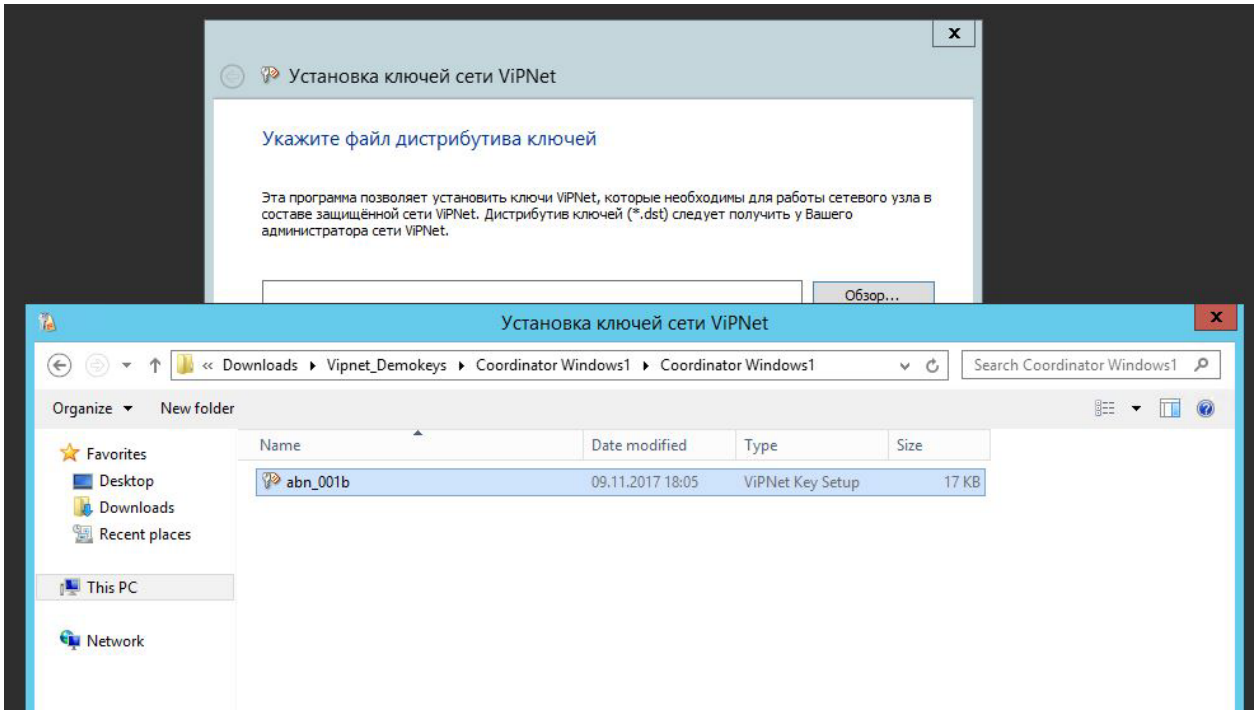

Рисунок 5 – Установка ключей сети для координатора

Ключи успешно установлены.

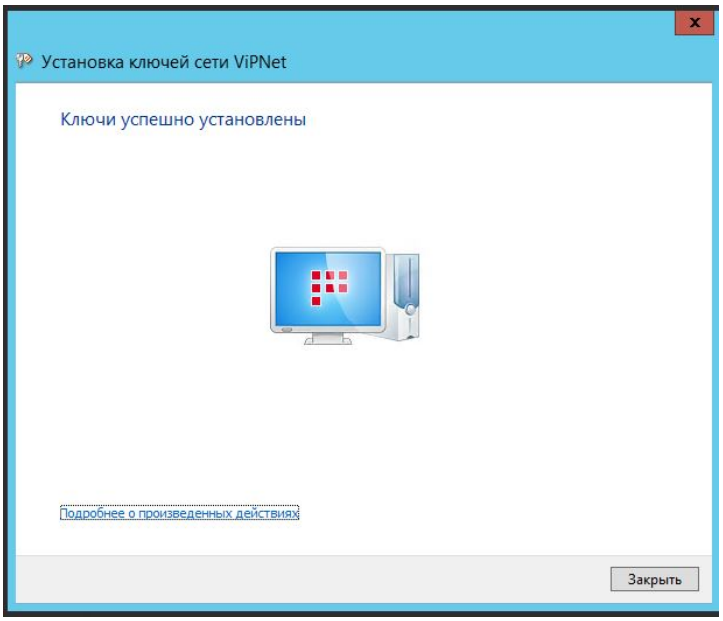

Рисунок 6 – Установка ключей завершена

Войдём в установленное приложение с учетными данными демо-версии.

- Имя пользователя: Coordinator Windows1
- Пароль: 11111111

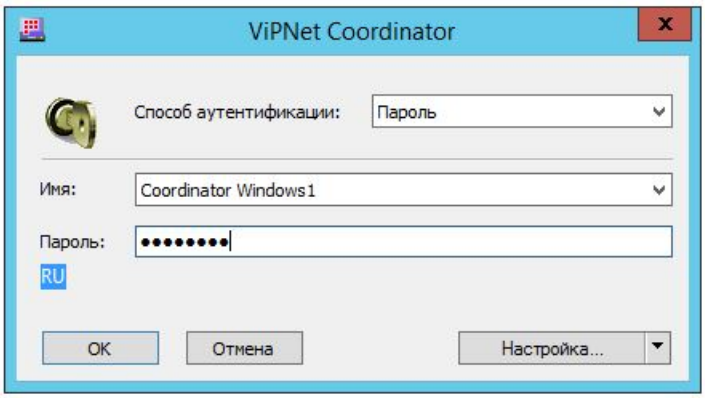

Рисунок 7 – Вход в VipNet Coordinator

Интерфейс приложения выглядит следующим образом:

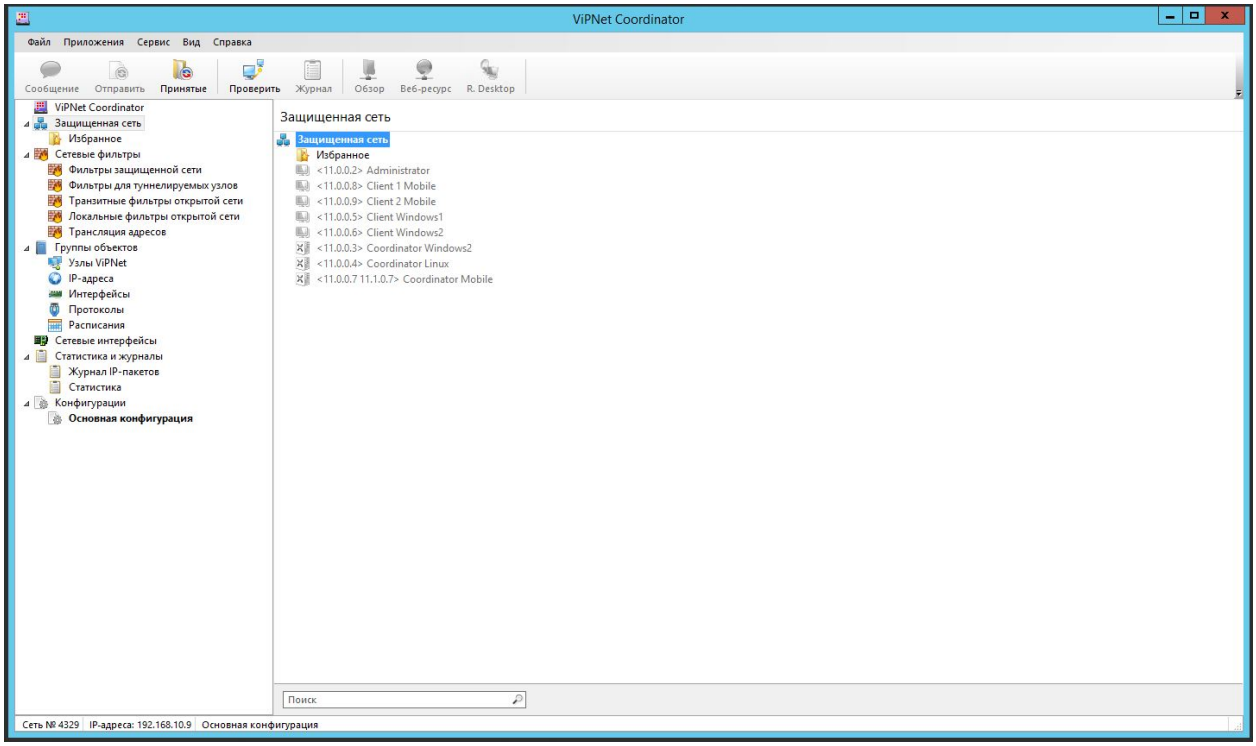

Рисунок 8 – Интерфейс координатора

Можно заметить, что сеть VipNet пока пустая, т.к. не было установлено ни одного клиента.

Установим два клиента на ранее подготовленные виртуальные машины.

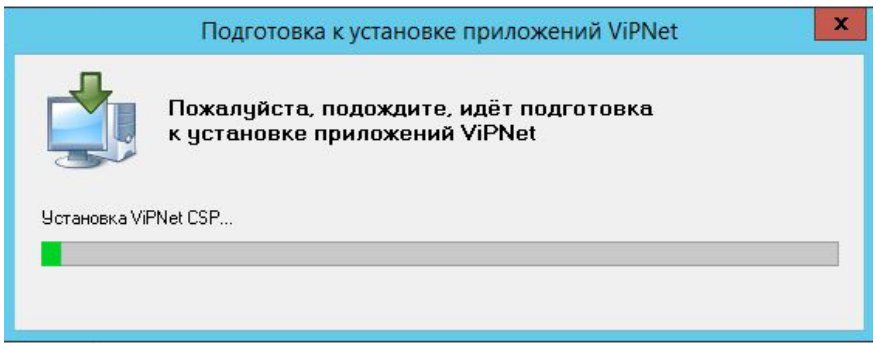

Рисунок 9 – Подготовка к установке клиента

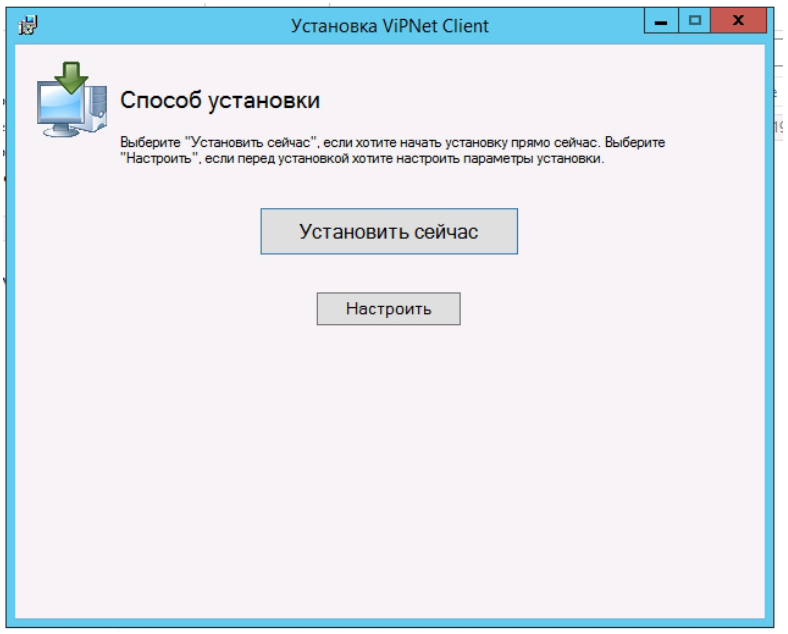

Рисунок 10 – Выбор настроек установки

Установка обоих клиентов практически идентична, за исключением установки ключей для каждого из клиентов

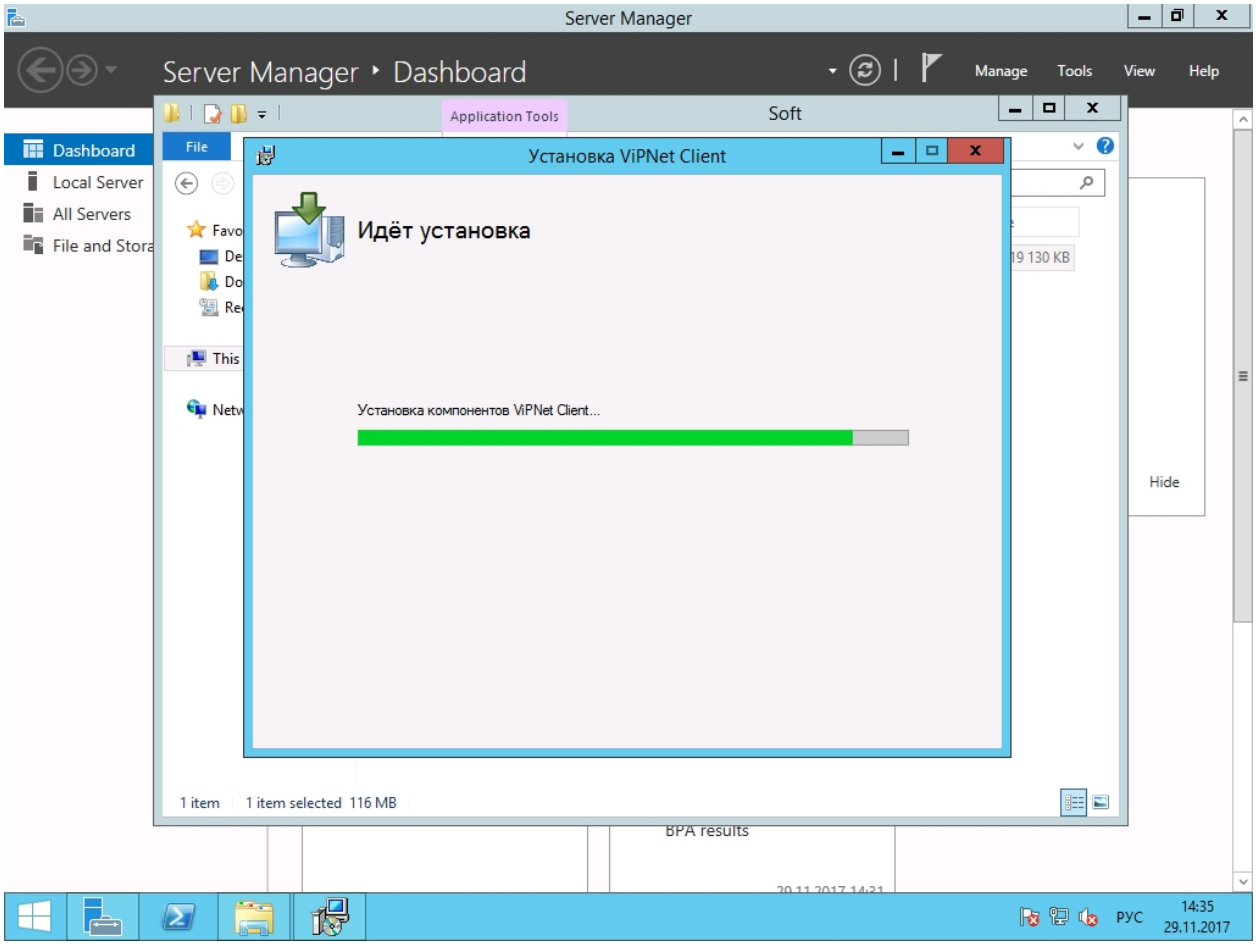

Рисунок 11 – Установка компонентов VipNet Client

Клиент успешно установлен

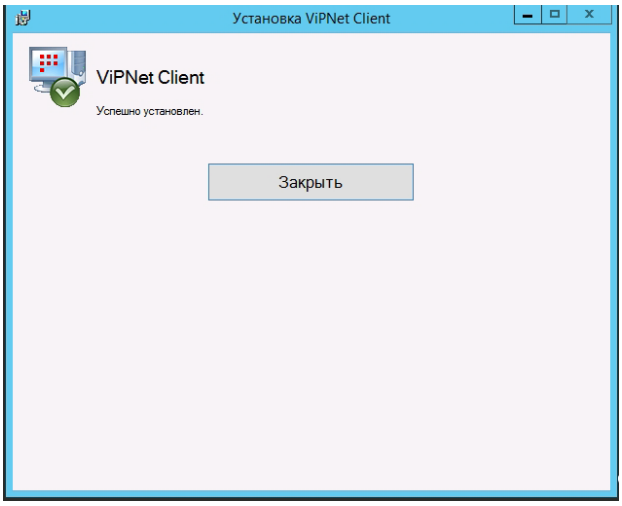

Рисунок 12 – VipNet клиент установлен

Установим ключи для каждого из клиентов.

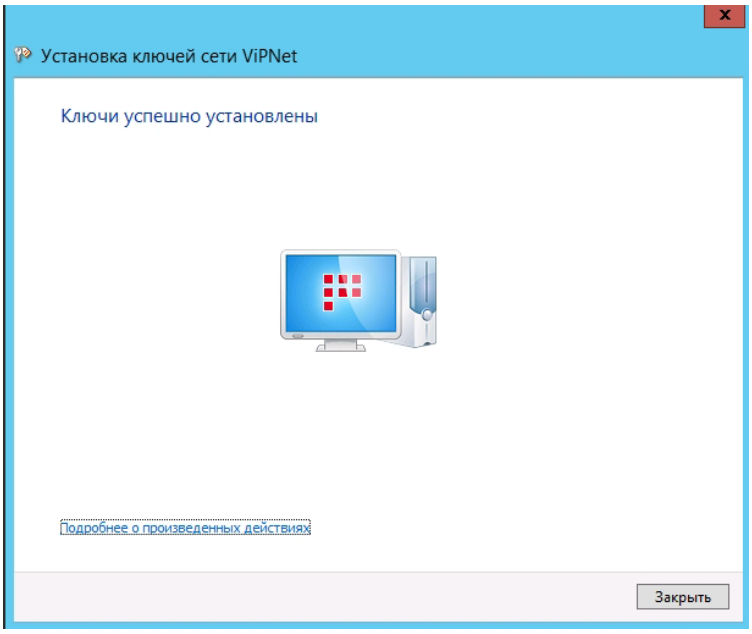

Рисунок 13 – Ключи успешно установлены

Теперь в защищенной сети для каждого из клиентов можно увидеть остальные узлы сети

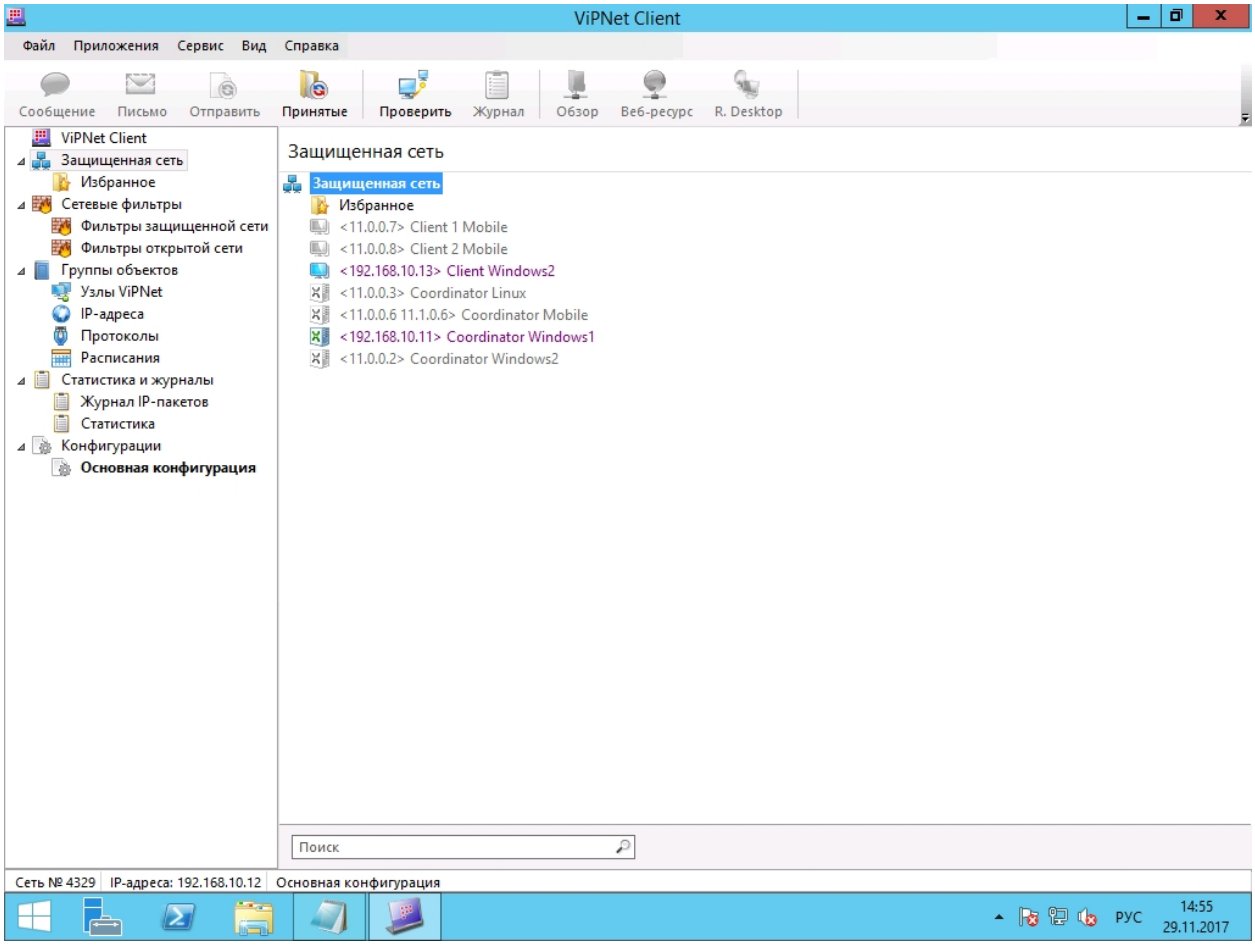

Рисунок 14 – Интерфейс «клиента 1»

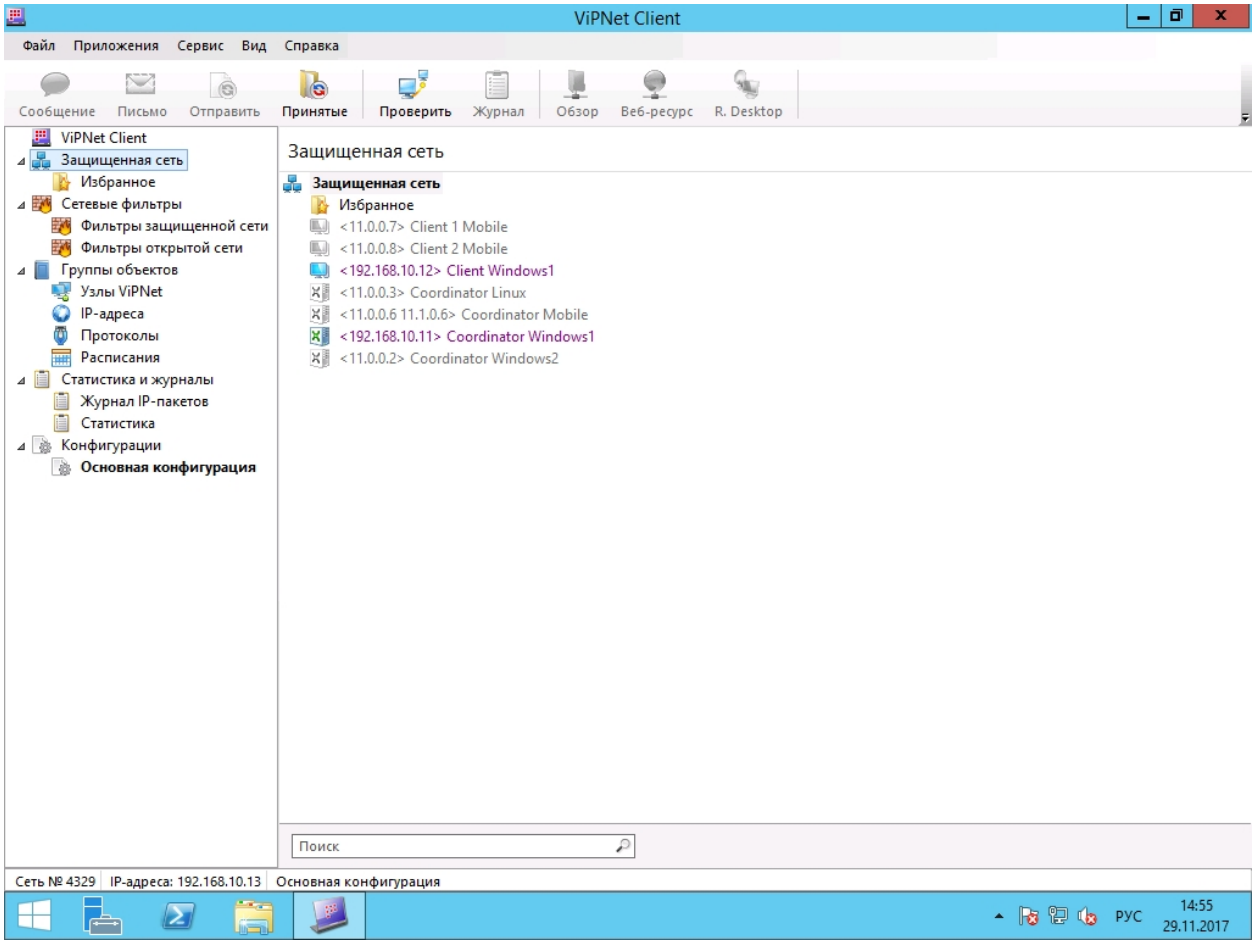

Рисунок 15 – Интерфейс «клиента 2»

VipNet обеспечивает полный контроль над сетевыми настройками компьютера.

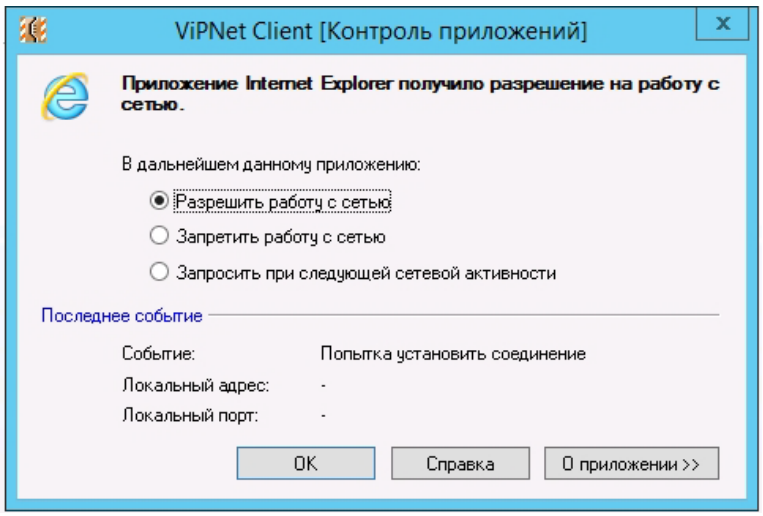

Рисунок 16 – Контроль приложений

Обращение клиента к координатору

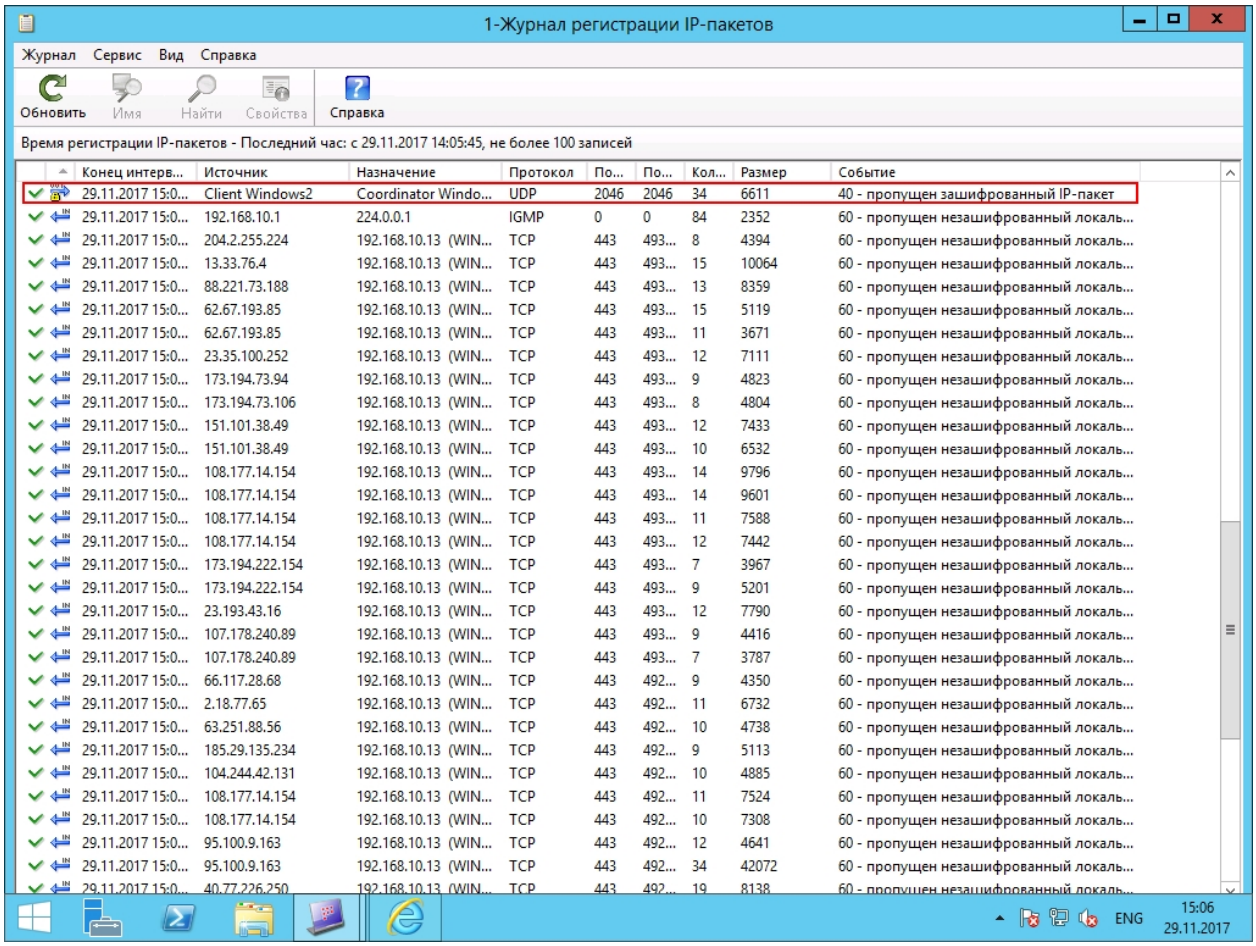

Рисунок 17 – Обращение клиента к координатору

С координатора можно посмотреть на работоспособность клиентов и последнюю активность на компьютере.

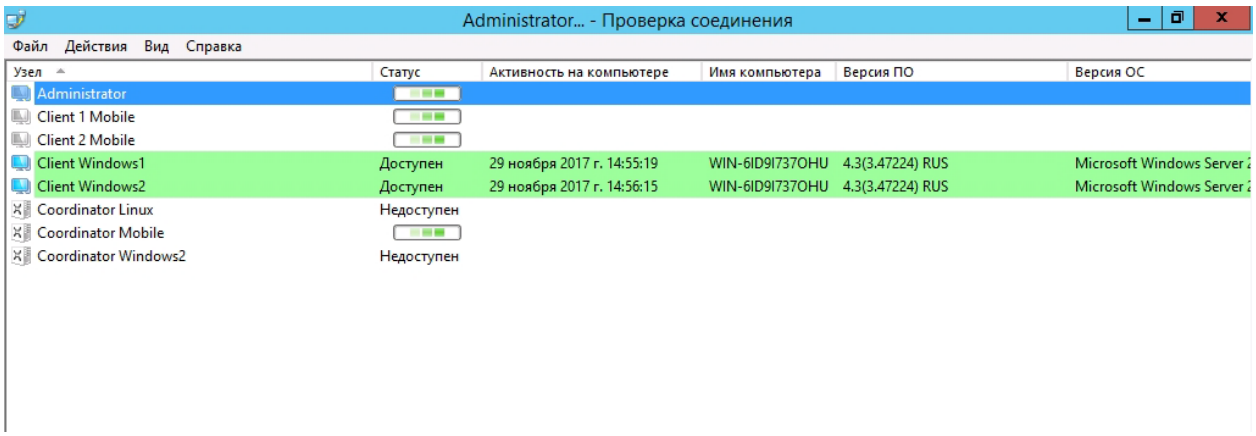

Рисунок 18 – Администрирование и контроль

Зашифрованные пакеты внутри VPN можно увидеть в журнале регистрации IP-пакетов

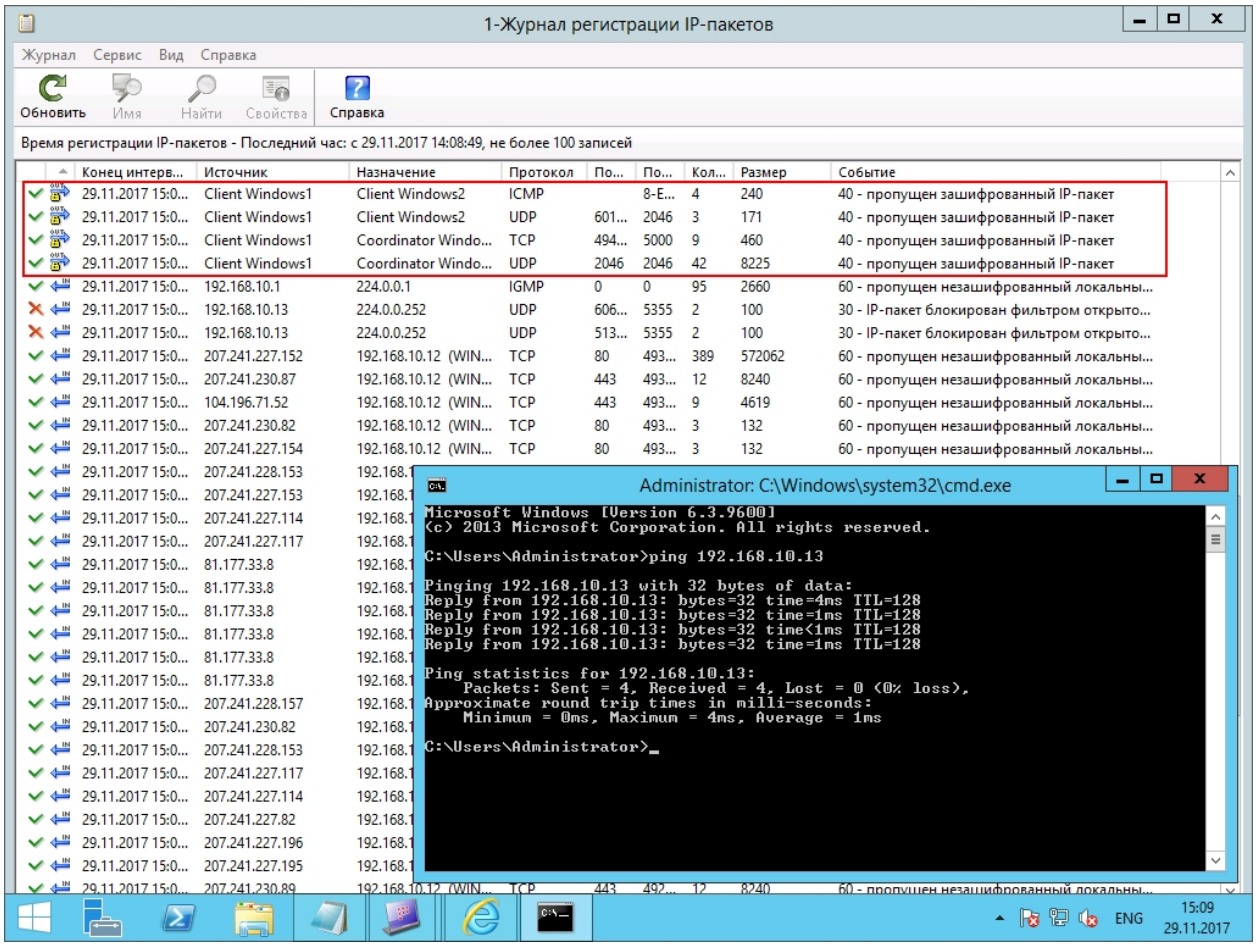

Рисунок 19 – Просмотр журнала пакетов

Отправим файл от одного компьютера к другому при помощи интерфейса приложения.

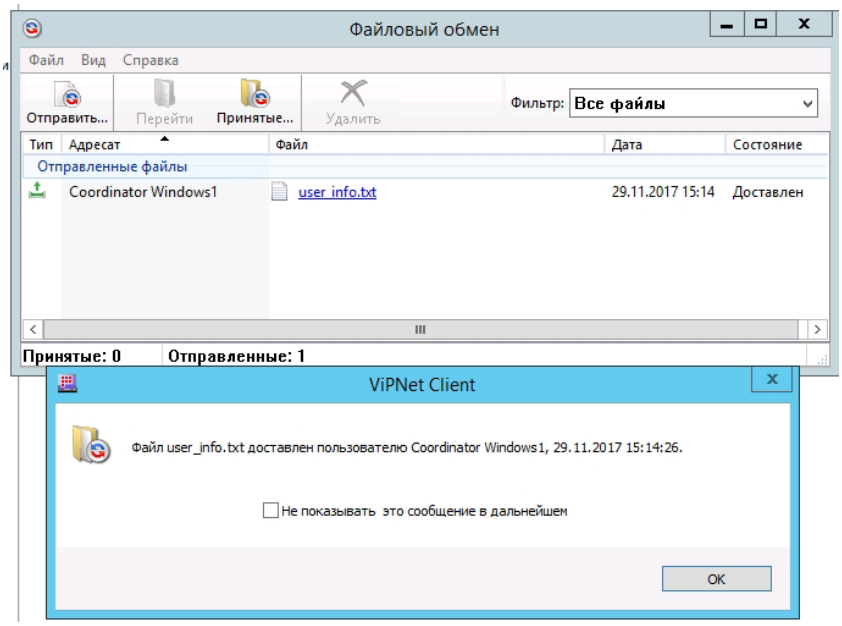

Рисунок 20 – Файл отправлен

Получим этот файл на другом компьютере

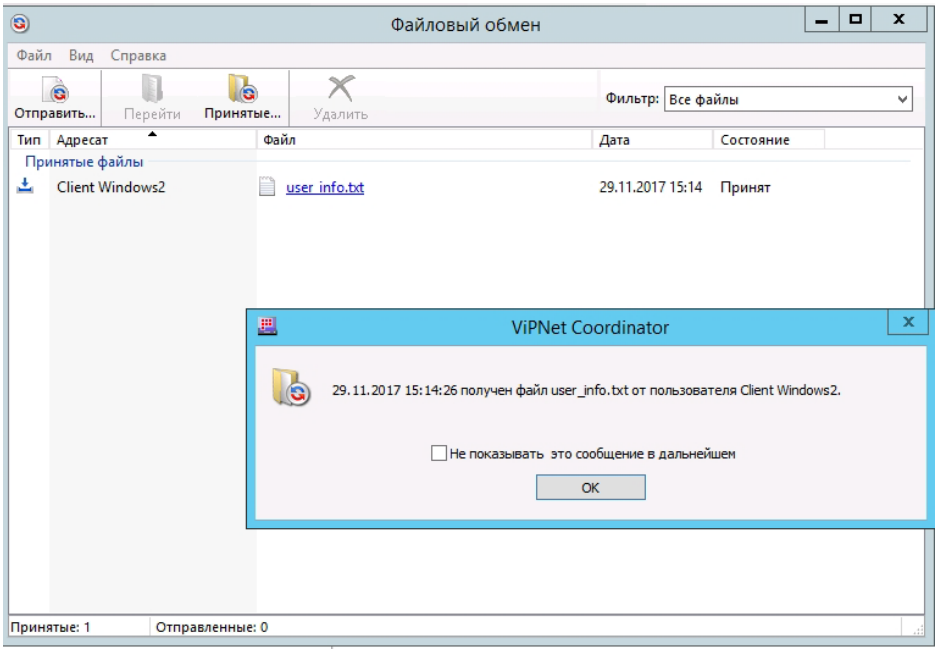

Рисунок 21 – Файл получен

Вывод:

В ходе лабораторной работы была настроена корпоративная VPN при помощи ПО “Infotecs VipNet”. Выбранная архитектура сети состоит из следующих узлов: два клиента и один координатор. Для них были установлены ключи регистрации в сети и настроены параметры взаимодействия.