

Подключение к конференции MS Lync.

**БУЗ ВО «МИАЦ»
Центр Обработки Данных
Салтаев Михаил Викторович**

Вологда,
2013 г.

Содержание

1. Общие сведения	3
2. Технические требования к аппаратному и программному обеспечению..	4
2.1. Требования к аппаратному обеспечению.....	4
2.2. Требования к программному обеспечению.....	4
3. Параметры учетной записи домена ЦОД	5
4. Включение рабочего места в сегмент корпоративной сети ЛПУ-ЦОД	7
4.1. Схема организации связи.....	7
5. Настройка маршрутизации для видеоконференцсвязи	9
5.1. Настройка маршрутизатора Mikrotik.....	9
5.2. Настройка сетевого интерфейса APM (для Windows XP)	10
6. Настройка VPN-соединения для видеоконференцсвязи	13
6.1. Создание VPN-соединения в Windows XP	13
6.2. Создание VPN-соединения в Windows 7/8	20
7. Установка корневого сертификата домена видеоконференцсвязи	30
7.1. Простая (первичная) установка сертификата	30
7.2. Расширенная установка сертификата.....	33
8. Подключение к конференции	47

1. Общие сведения

В настоящей статье рассмотрены основные последовательности действий, которые необходимо выполнить специалистам подразделений АСУ в лечебных учреждениях (ЛПУ) Вологодской области для возможности участия в видеоконференцсвязи на базе программного обеспечения Microsoft Lync.

Данная задача разбивается на несколько этапов:

- 1) Так как программное обеспечение разработано компанией Microsoft, важное значение имеют технические требования к аппаратному и программному обеспечению рабочего места.
- 2) Параметры учетной записи домена ЦОД (для видеоконференцсвязи).
- 3) Включение рабочего места в сегмент корпоративной сети ЛПУ-ЦОД.
- 4) Настройка маршрутизации для видеоконференцсвязи.
- 5) Настройка VPN-подключения.
- 6) Установка корневого сертификата домена видеоконференцсвязи.
- 7) Подключение к конференции.

2. Технические требования к аппаратному и программному обеспечению

2.1. Требования к аппаратному обеспечению

Для того, чтобы можно было принимать полноценное участие в конференциях на базе ПО MS Lync, необходимо:

- 1) Определить рабочее место, с которого будет производиться подключение к конференции. Указанное рабочее место на данном этапе может быть установлено в подразделении АСУ, либо в помещении, расположенном в непосредственной близости от маршрутизатора, который используется для стыка с ЦОД.
- 2) Рабочее место должно включать в себя:
 - персональный компьютер или ноутбук;
 - web-камера со встроенным микрофоном;
- 3) Рабочее место подключить программным или аппаратным способом к каналу связи ЛПУ-ЦОД (как это сделать будет сказано ниже).

а) Требования к персональному компьютеру или ноутбуку:
конкретных показателей мы устанавливать не будем, единственно укажу, что для работы в видеоконференцсвязи нужен все-таки компьютер, на котором минимум стабильно работает операционная система Windows XP.

б) Требования к Web-камере:

- наличие встроенного микрофона;
- разрешение не менее 640x480 пикселей;

Разрешается использовать встроенные в ноутбук web-камеры.

2.2. Требования к программному обеспечению

- а) Операционная система: Windows XP (не ниже Service Pack 3)/7 (не ниже Service Pack 1)/8;
- б) Офисный пакет: не ниже версии MS Office 2007 (иначе не удастся установить MS Lync);
- в) Для корректной работы в составе клиента MS Lync для Web-камеры должны быть установлены «родные» (от производителя) драйвера;
- г) Клиент MS Lync: Lync 2010 для компьютеров с ОС Windows XP, Lync 2013 для компьютеров с ОС Windows 7 (не ниже Service Pack 1)/8;

Просьба также учесть, что данным мануалом не рассматривается вопрос установки клиентского программного обеспечения MS Lync. Установка продукта достаточно простая, особых требований к ней нет. Сами дистрибутивы можно найти по следующим адресам:

MS Lync 2010 (32-разрядная)

<http://www.microsoft.com/ru-ru/download/details.aspx?id=5484>

MS Lync 2010 (64-разрядная)

<http://www.microsoft.com/ru-ru/download/details.aspx?id=10400>

MS Lync Basic 2013 (32-разрядная)

<http://www.microsoft.com/ru-ru/download/details.aspx?id=35451>

MS Lync Basic 2013 (64-разрядная)

<http://www.microsoft.com/ru-ru/download/details.aspx?id=35450>

3. Параметры учетной записи домена ЦОД

Для возможности подключения к конференции MS Lync на каждом клиентском месте потребуется вводить авторизационные данные (логин/пароль).

Архитектура системы такова, что для того, чтобы подключиться к конференции, клиент должен быть в составе домена, в котором работает сервер MS Lync.

Следовательно для реализации указанного требования потребуются следующие параметры:

Таблица 3.1.

№	Параметр	Значение
1	Домен	VOLOGDAMED
2	Имя пользователя	<логин, выданный для подключения к ftp-серверу с дампами МИС>
3	Пароль	<пароль, выданный для подключения к ftp-серверу с дампами МИС>

Как видно из таблицы 3.1, в качестве логина/пароля для доступа к конференции можно использовать те же авторизационные параметры, которые выдавались для доступа на ftp-сервер ЦОД (для проверки корректности передачи дампов МИС из ЛПУ в ЦОД).

Если Вами такие данные ранее не были получены, то их необходимо запросить по следующей форме:

Таблица 3.2

№	Запрос авторизационных данных для доступа к сервисам ЦОД	
1	Наименование учреждения	
2	IP-адрес сервера с МИС	<i>*IP-адрес, который установлен на сетевом интерфейсе сервера с МИС, «смотрящему» на VipNet-координатор</i>
3	ФИО сотрудника АСУ	
4	Контактный телефон	

Запрос необходимо отправлять на адреса электронной почты: msvv@yandex.ru, kabakovda@mail.ru, ra1qkb@gmail.com

* Примечание 1: здесь должен быть указан IP-адрес из подсети 10.0.xx.64/26, который, согласно инструкции «Подключение ЛПУ к ЦОД», устанавливается на сетевой интерфейс сервера с программным обеспечением МИС. Если у Вас МИС установлена на сервер с VipNet-координатором, то в данной табличке нужно указать IP-адрес сетевого интерфейса данного сервера, «смотрящему» на маршрутизатор.

В ответном письме будут высланы следующие параметры для настройки соединения:

Таблица 3.3

Параметры для доступа к сервисам ЦОД	
Сервис 1. FTP-архив дампов МИС	
IP-адрес FTP-сервера с дампами МИС	
Логин	
Пароль	
Сервис 2. Система видеоконференцсвязи ЦОД	
IP-адрес VPN-сервера (протокол PPTP)	10.35.1.1
IP-адрес сети видеоконференцсвязи	10.35.10.0/24
Домен сети видеоконференцсвязи	VOLOGDAMED

Логин	
Пароль	

Также, в ответном письме будет прикреплен файл – корневой сертификат домена видеоконференцсвязи. Данный файл необходимо скачать на тот компьютер, который будет использоваться для видеоконференцсвязи, и установить сертификат на него. Как это сделать, см. ниже.

4. Включение рабочего места в сегмент корпоративной сети ЛПУ-ЦОД

4.1. Схема организации связи

В рамках реализации подключения ЛПУ к ЦОД рассматривалась следующая схема организации связи (Рис. 4.1):

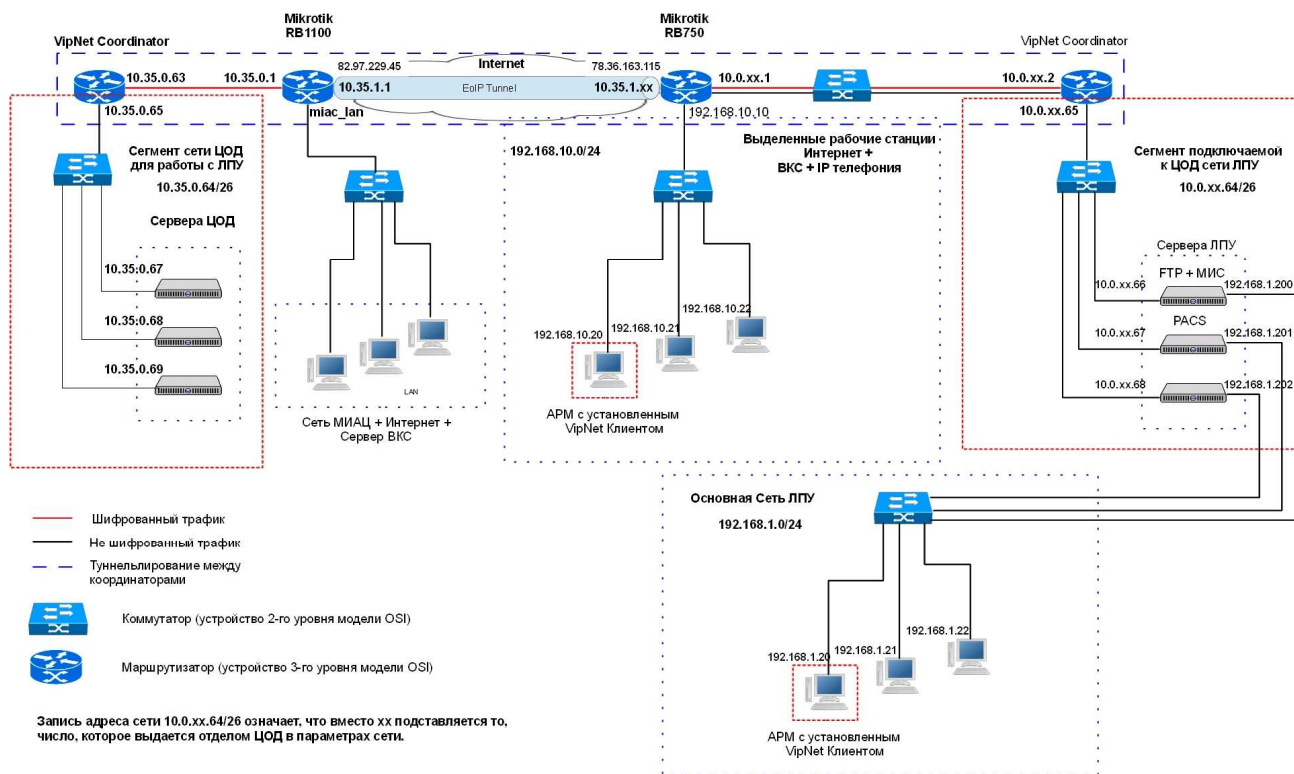


Рисунок 4.1 – Вариант схемы организации связи подключения оборудования ЛПУ к ЦОД

Здесь изображен один из вариантов, реализуемый через существующее подключение к сети Интернет.

В настоящем руководстве предполагается, что в лечебном учреждении данная схема организации реализована.

Посмотрим на сегмент сети на стороне ЛПУ – Рисунок 4.2.

Как видно из рисунка, между маршрутизатором и сервером с VipNet-координатором расположено еще устройство – коммутатор. Когда, данная схема приводилась в инструкции «Подключение ЛПУ к ЦОД», наличие коммутатора было не очевидно и возможно не понятно. Теперь использование устройства здесь прояснится, в данном случае возникает необходимость его использования: к указанному коммутатору нужно подключить рабочее место, с которого будет осуществляться подключение к видеоконференцсвязи.

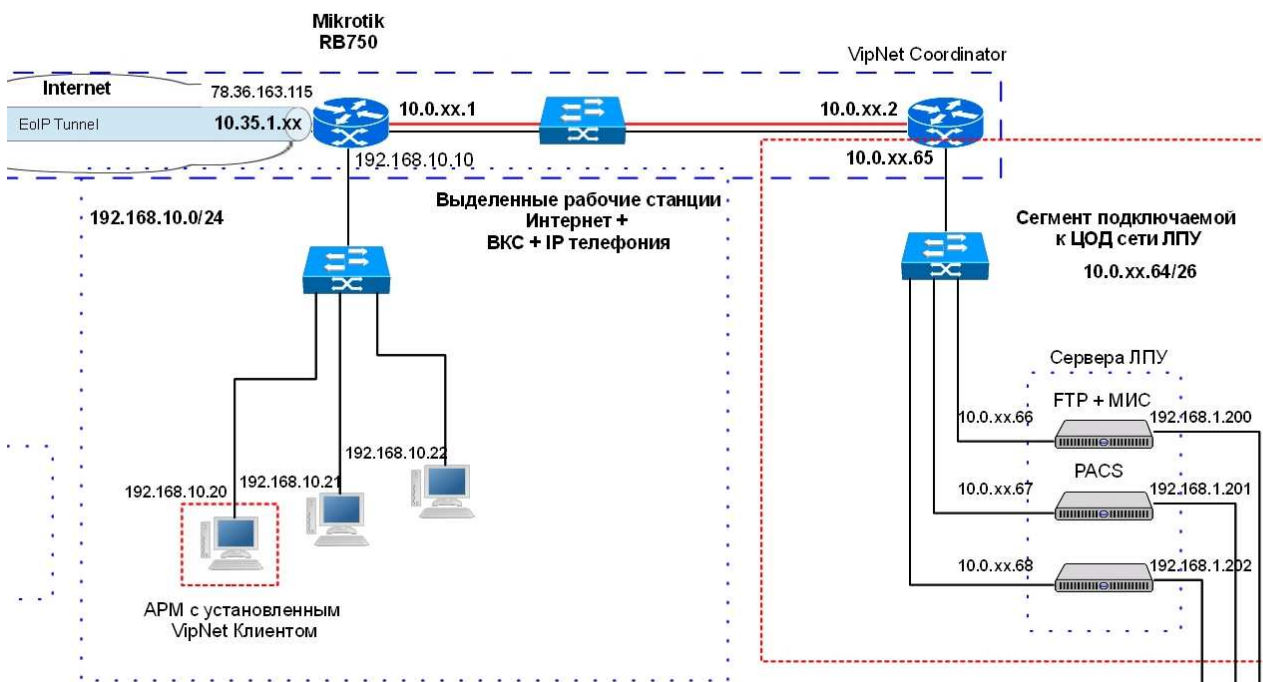


Рисунок 4.2 – Сегмент сети ЛПУ

После подключения рабочего места к коммутатору сегмент сети, приведенный на рисунке 4.2 изменится так:

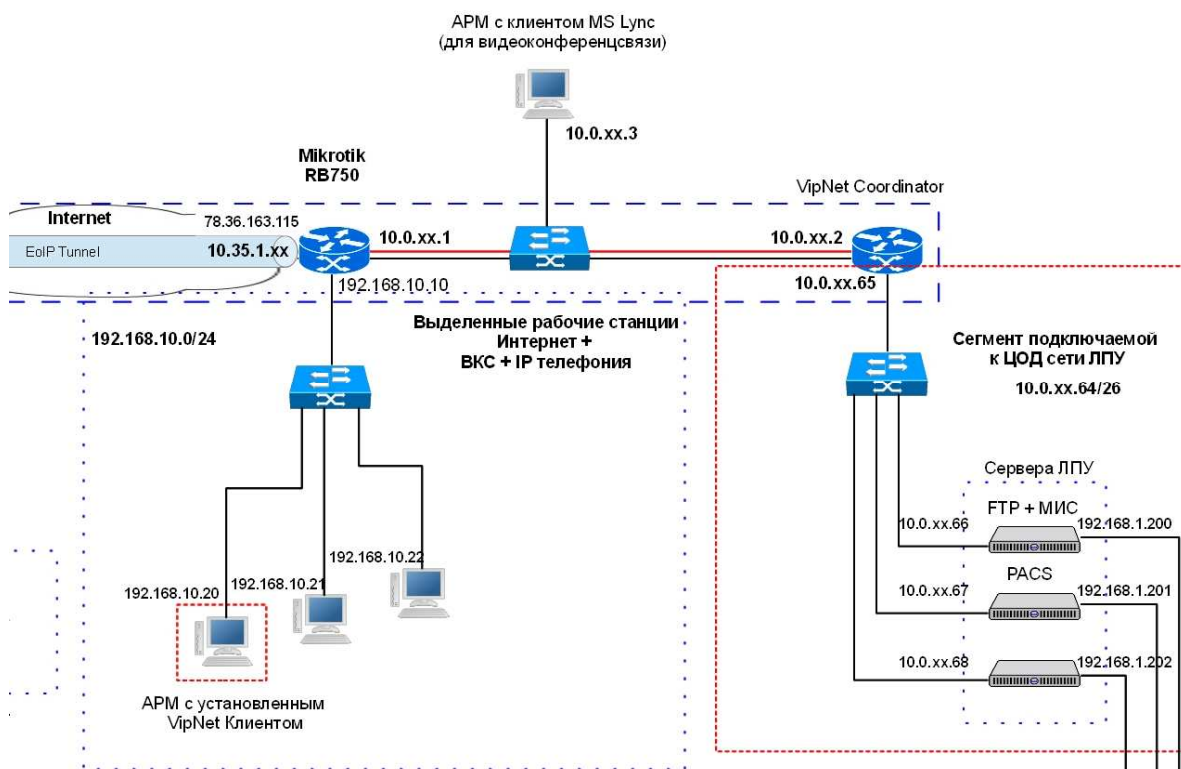


Рисунок 4.3 – Сегмент сети ЛПУ с АРМ для видеоконференцсвязи

Перечень настроек, которые должны быть выполнены на сетевом интерфейсе АРМ с клиентом MS Lync, ищите в следующем разделе ниже.

5. Настройка маршрутизации для видеоконференцсвязи

5.1. Настройка маршрутизатора Mikrotik

Следующим этапом конфигурирования сети будет настройка маршрутизации до серверов MS Lync.

Сервера видеоконференцсвязи MS Lync находятся в ЦОД в следующем сегменте сети: 10.35.10.0\24.

Так как на уровне сети лечебного учреждения об этой сети ничего неизвестно, следовательно на маршрутизаторе Mikrotik нужно добавить специальный маршрут.

а) Для этого в Winbox нужно зайти в раздел IP -> Routes. Откроется следующее окно:

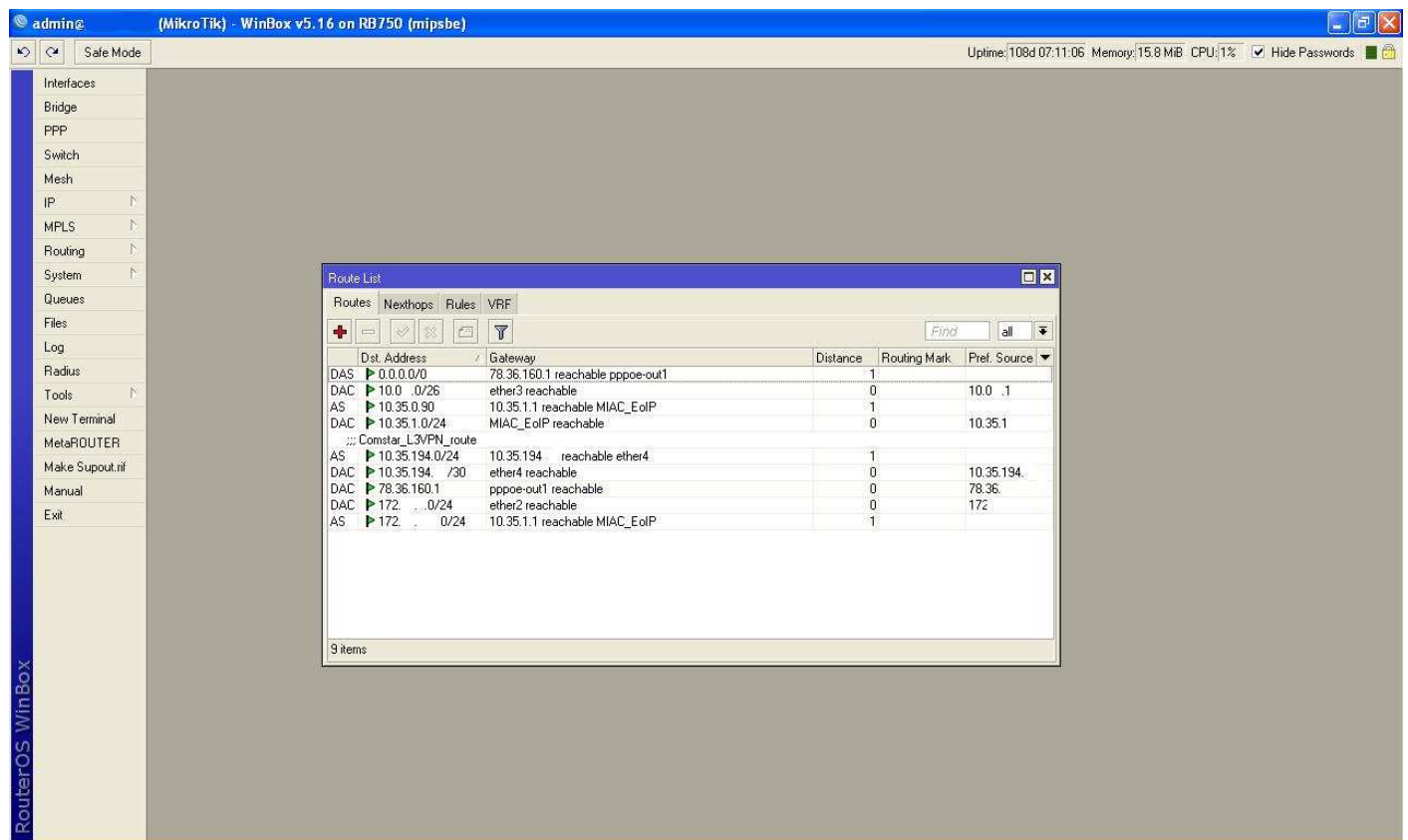


Рисунок 5.1 – Таблица маршрутизации Mikrotik

б) Здесь нажимаем кнопку «плюс» и в открывшемся окне прописываем маршрут до сети 10.35.10.0/24:

На данном скриншоте:

Dst. Address: 10.35.10.0/24 – адрес сети, до которой нам нужно сделать маршрут;

Gateway: 10.35.1.1 – адрес того маршрутизатора, который знает об этой сети и который известен нашему маршрутизатору.

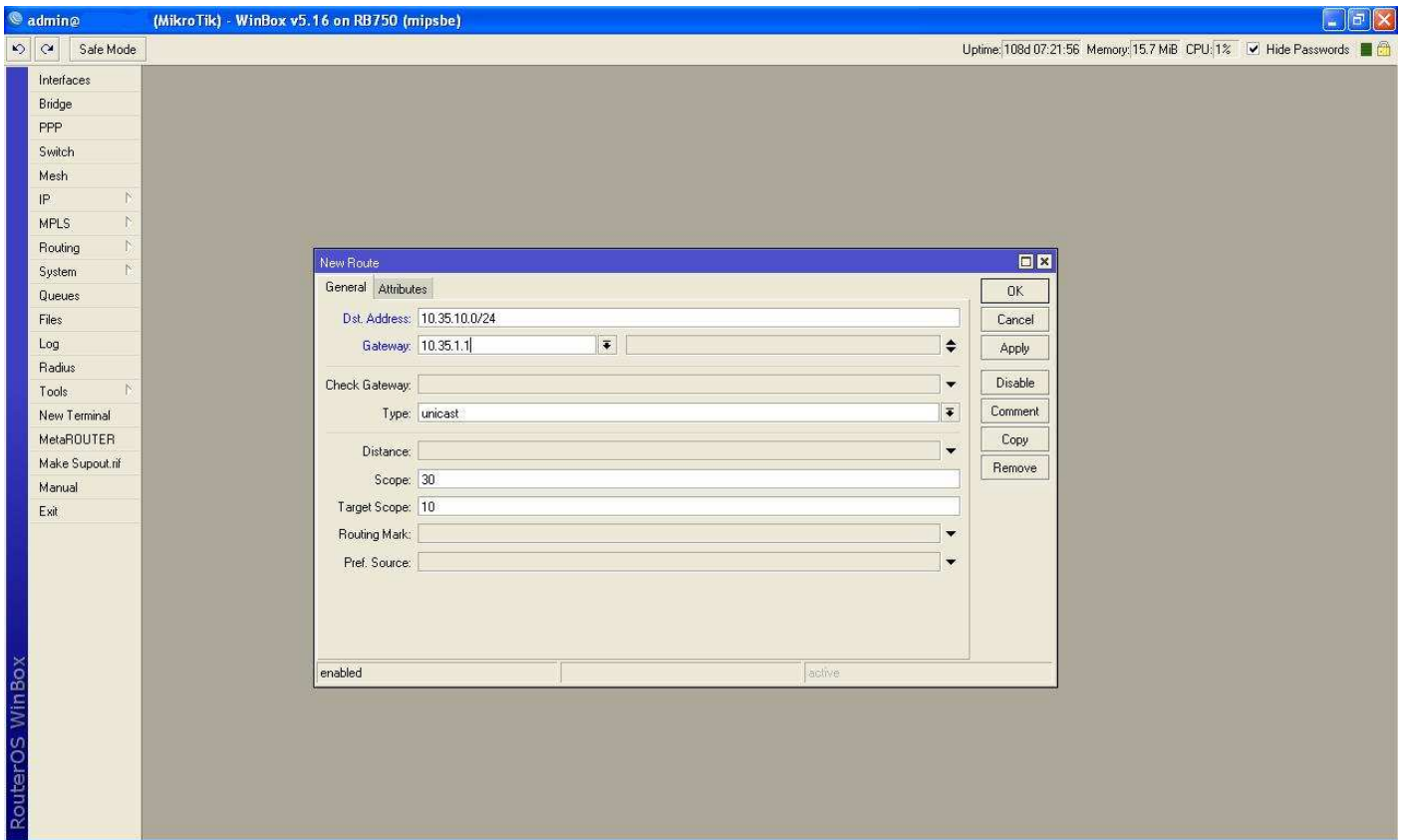


Рисунок 5.2 – Настройка маршрута до сети

Нажимаем ОК. Маршрут создан.

5.2. Настройка сетевого интерфейса АРМ (для Windows XP)

а) Открываем свойства сетевого интерфейса -> Протокол Интернета (TCP/IP) -> Свойства

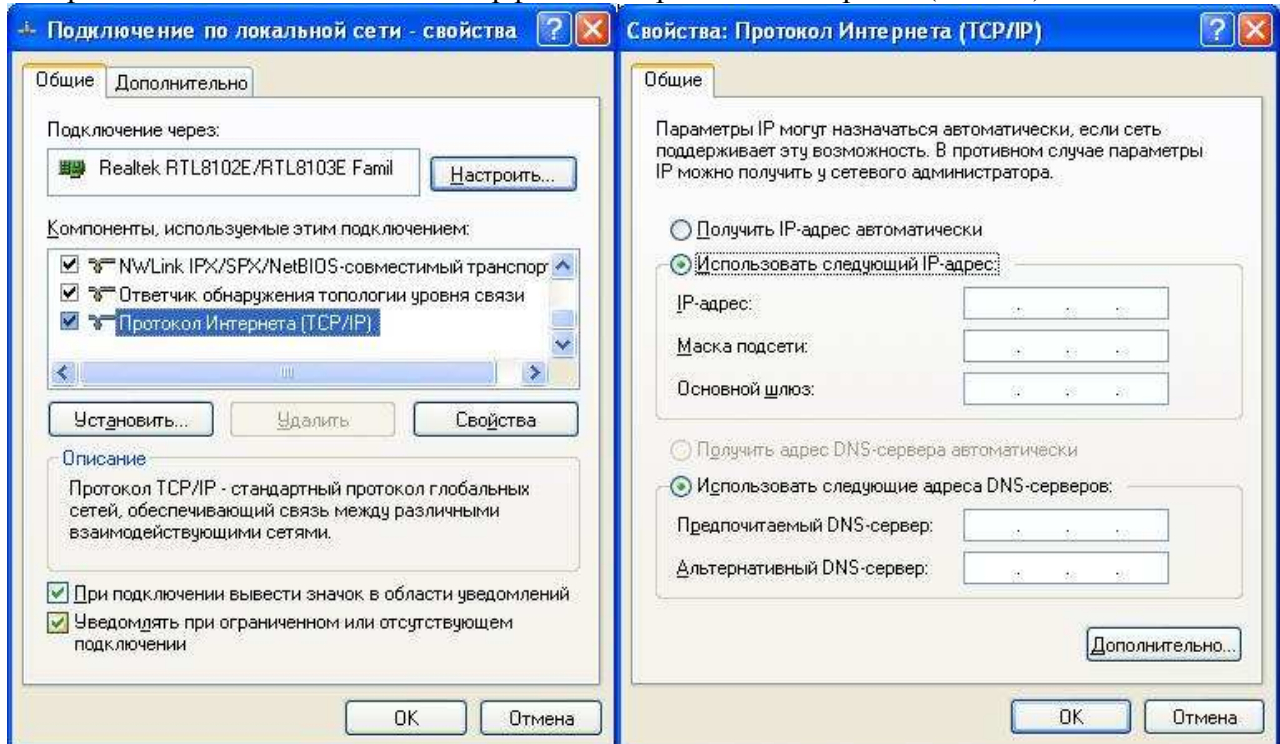


Рисунок 5.3 – Настройка сетевого интерфейса

б) В открывшемся окне заполняем соответствующие поля:

IP-адрес – согласно схеме, приведенной на рисунке 4.3 устанавливаем IP-адрес из выделенной вашей подсети. Он должен быть вида: 10.0.хх.3, где хх – номер вашей подсети, выдаваемый на стадии подключения ЛПУ к ЦОД.

Маска подсети - /26 или 255.255.255.192

Основной шлюз: здесь указывается IP-адрес, который висит на Микротике. Т.е.: 10.0.хх.1

Предпочитаемый DNS-сервер: 10.35.10.101

Т.е. должно получиться так:

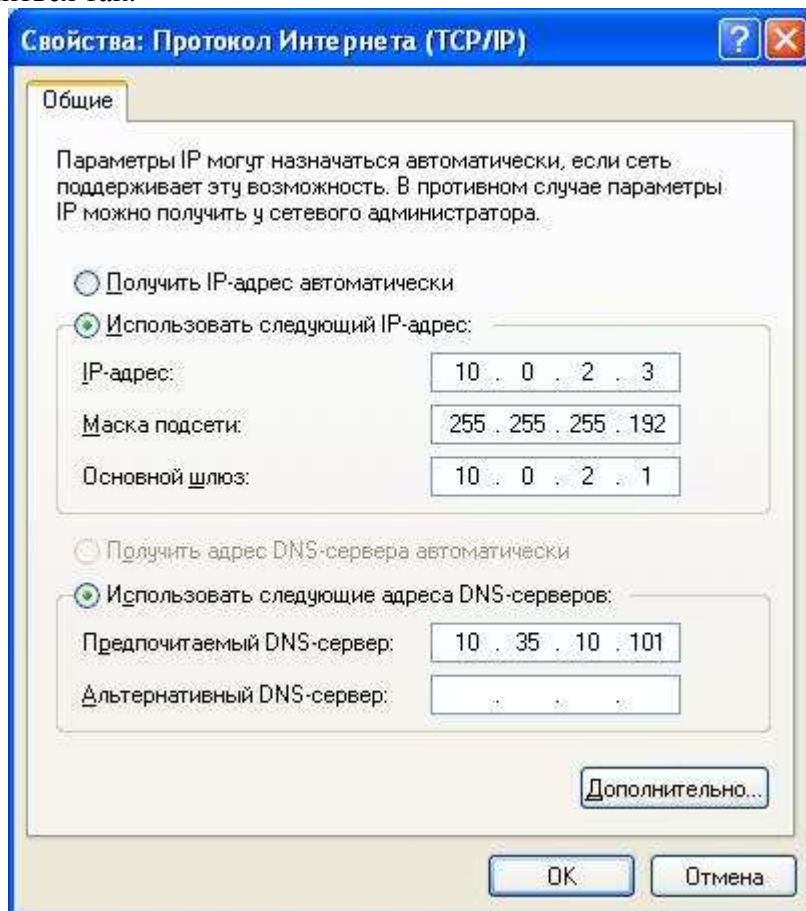


Рисунок 5.4 – Настройка сетевого интерфейса

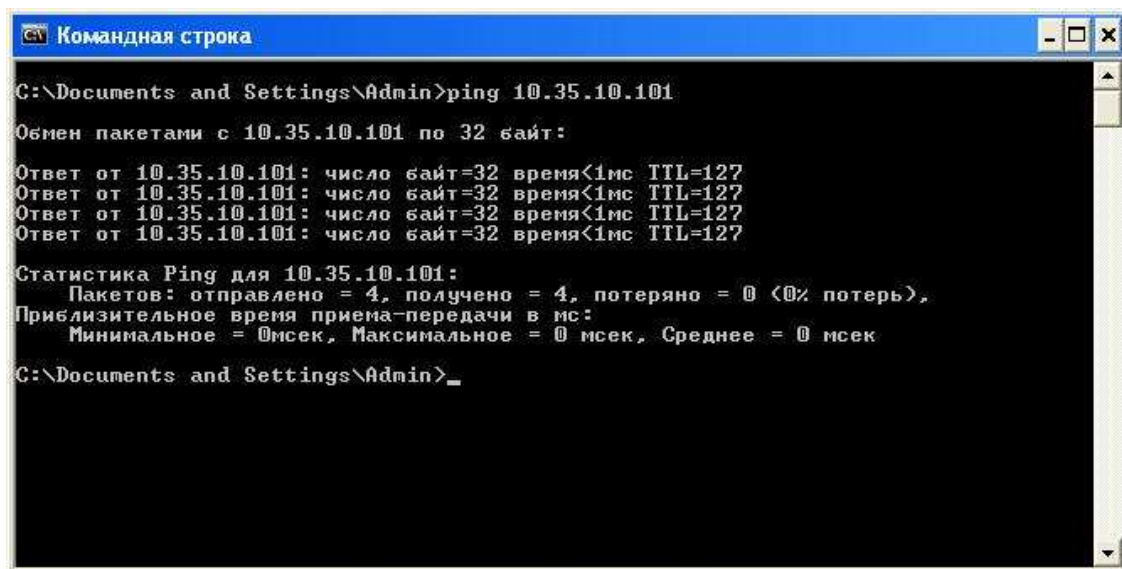
Жмем ОК во всех окнах. Настройка интерфейса завершена.

Выше приведена инструкция по настройке сетевого интерфейса в Windows XP. Для Windows 7/8 делается все точно также (расположение папки с сетевыми интерфейсами можно найти через «Центр управления сетями и общим доступом»).

в) Делаем проверку.

Для того, чтобы убедиться в том, что все сделано правильно, достаточно лишь пропинговать некоторые адреса:

- ping 10.35.10.101 (пингуем DNS-сервер сети видеоконференцсвязи)



```
Командная строка
C:\Documents and Settings\Admin>ping 10.35.10.101
Обмен пакетами с 10.35.10.101 по 32 байт:
Ответ от 10.35.10.101: число байт=32 время<1мс TTL=127
Ответ от 10.35.10.101: число байт=32 время<1мс TTL=127
Ответ от 10.35.10.101: число байт=32 время<1мс TTL=127
Ответ от 10.35.10.101: число байт=32 время<1мс TTL=127

Статистика Ping для 10.35.10.101:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Documents and Settings\Admin>_
```

Рисунок 5.5

Если тесты проходят и пакеты также идут – значит все ОК, можно двигаться дальше.

6. Настройка VPN-соединения для видеоконференцсвязи

После подключения рабочего места в необходимый сегмент сети нужно настроить VPN-подключение, с помощью которого будет осуществляться вход в домен видеоконференцсвязи. Здесь приводится инструкция для создания таких подключений для двух разных операционных систем – Windows XP и Windows 7/8.

6.1. Создание VPN-соединения в Windows XP

а) Заходим в папку Панель управления -> Сетевые подключения

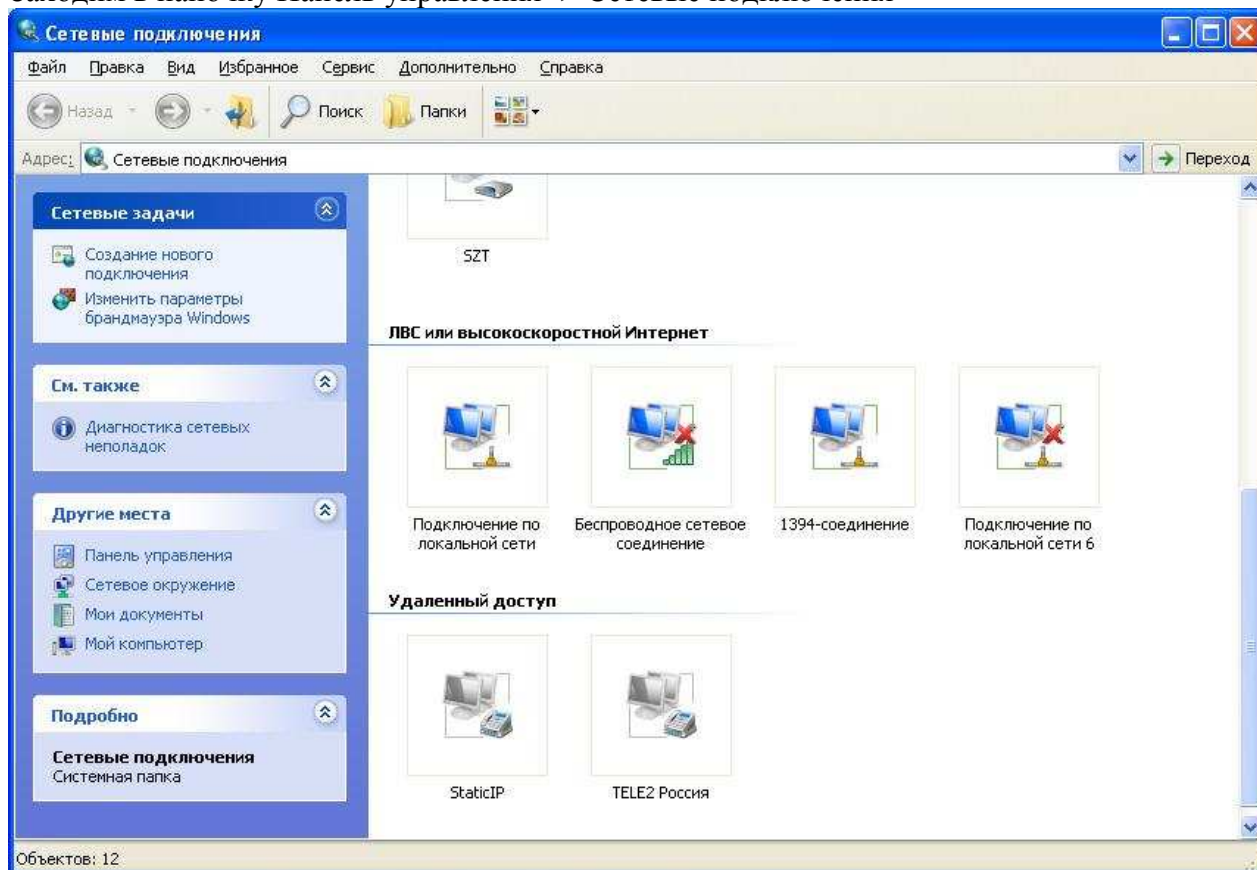


Рисунок 6.1 – Сетевые подключения в Windows XP

б) В боковом меню слева жмем на буквы «Создание нового подключения». Откроется следующее окно:

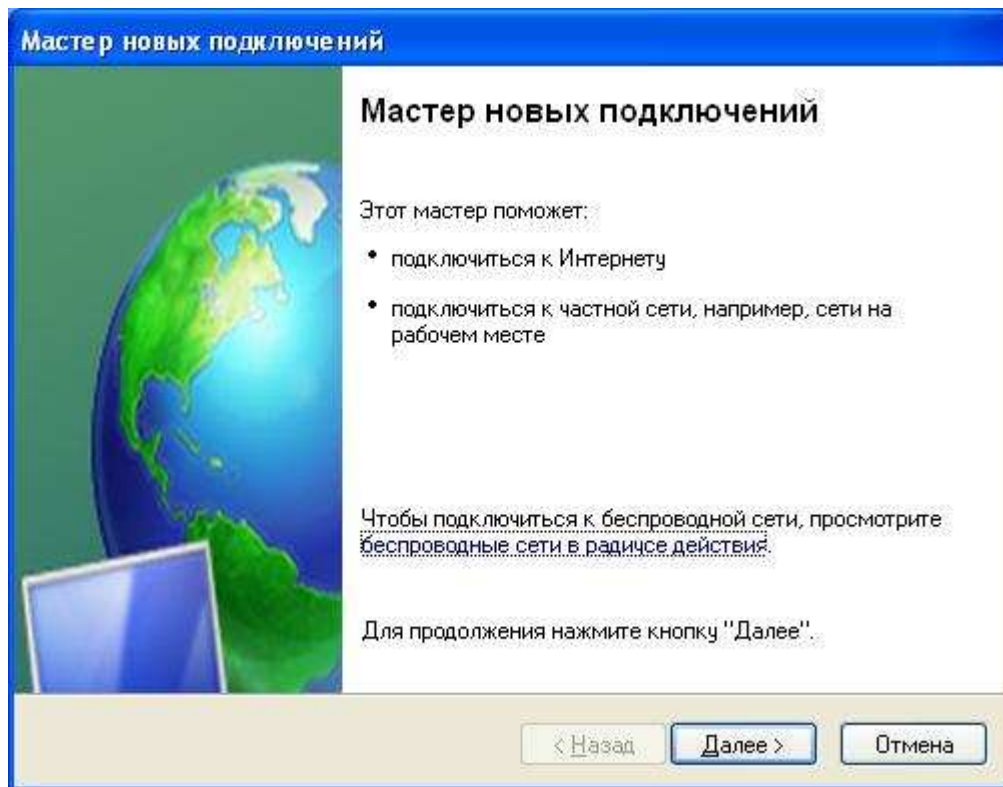


Рисунок 6.2 – Создание нового подключения в Windows XP

Здесь нажимаем «Далее».

в) На следующем окне выбираем пункт «Подключить к сети на рабочем месте».

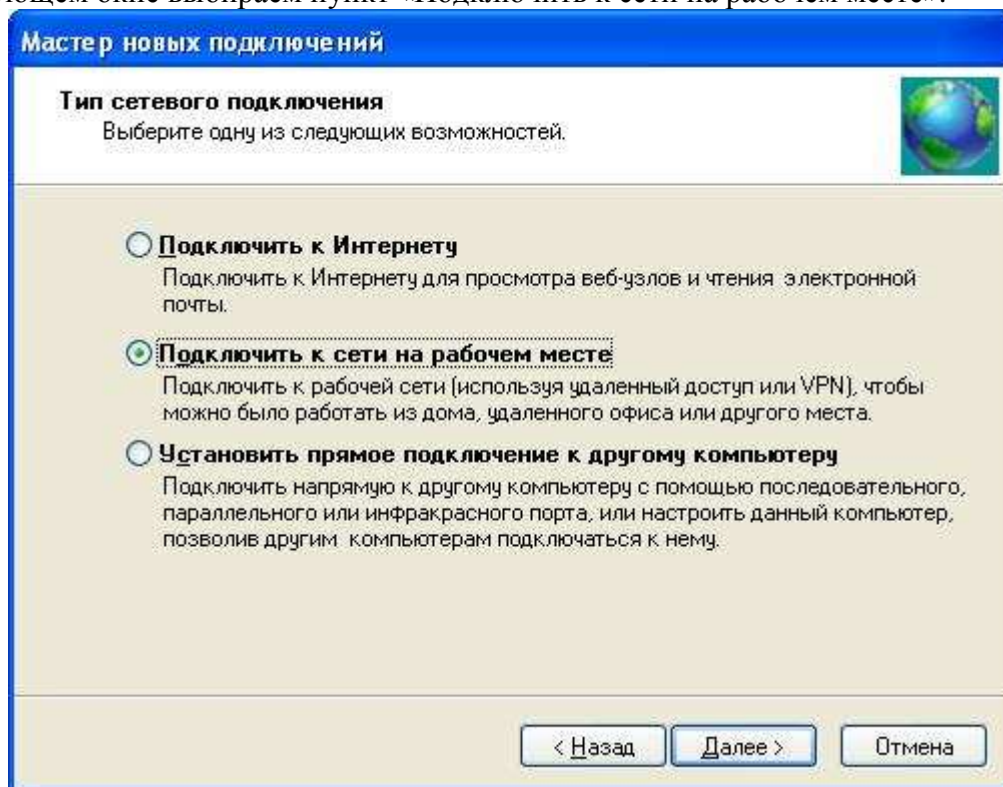


Рисунок 6.3 – Выбор типа подключения в Windows XP

Жмем «Далее».

г) На следующем окне выбираем пункт «Подключение к виртуальной частной сети».

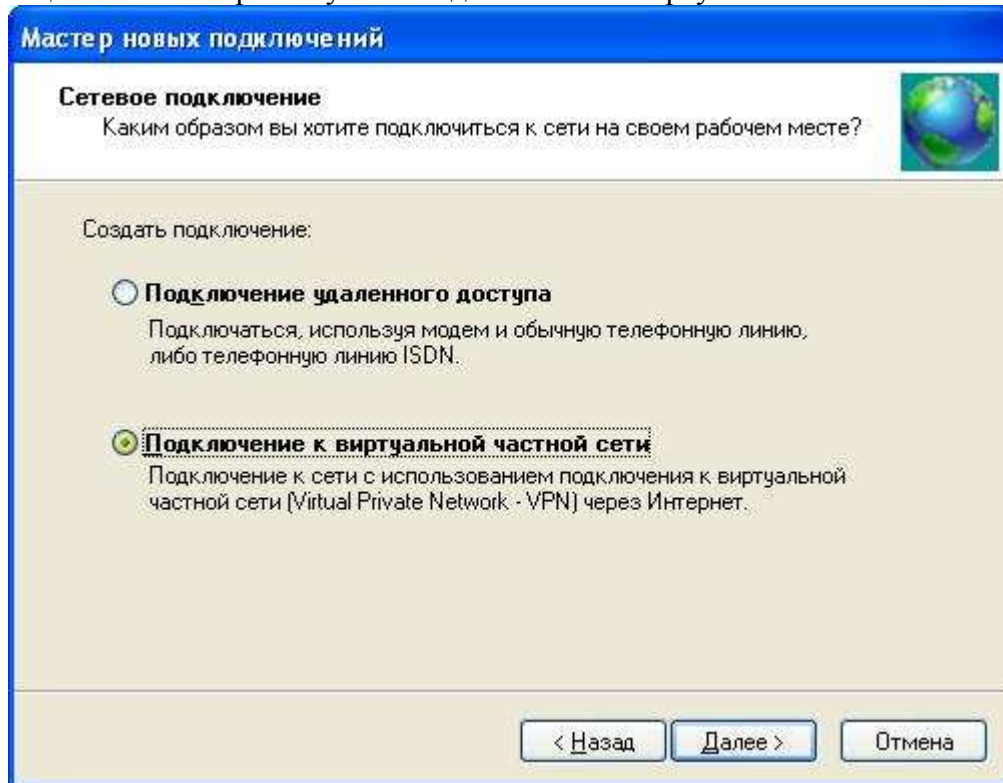


Рисунок 6.4 – Выбор типа подключения в Windows XP

Жмем опять «Далее».

д) На следующем окне вписываем произвольное имя подключения, но так, чтобы было понятно.

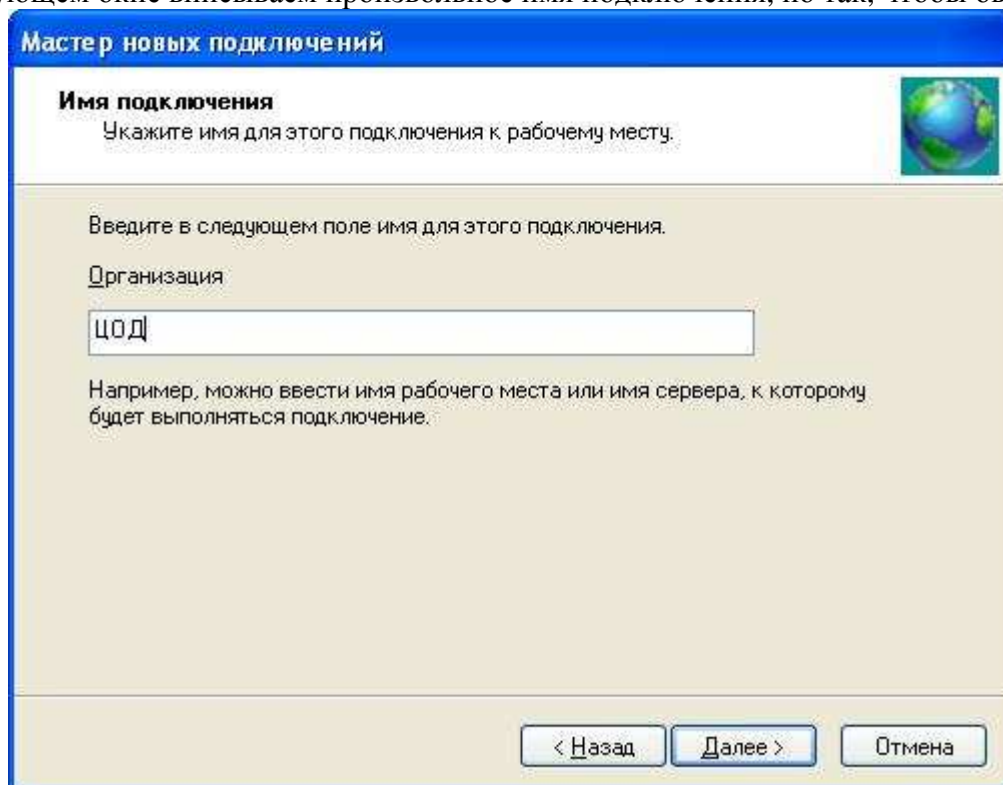


Рисунок 6.5 – Настройка VPN-подключения в Windows XP

е) На следующем окне выбираем пункт «Не набирать номер для предварительного подключения»

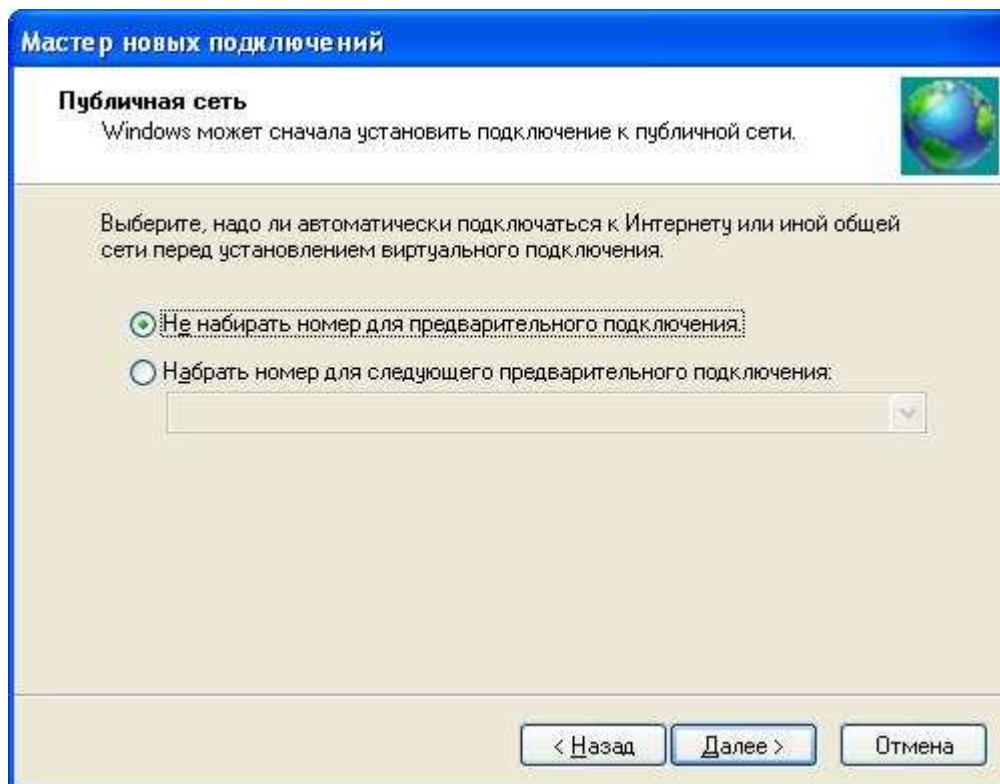


Рисунок 6.6 – Настройка VPN-подключения в Windows XP

ж) На следующем окне вбиваем адрес VPN-сервера, который был выдан в параметрах. Правда, на текущий момент для всех этот сервер един: 10.35.1.1

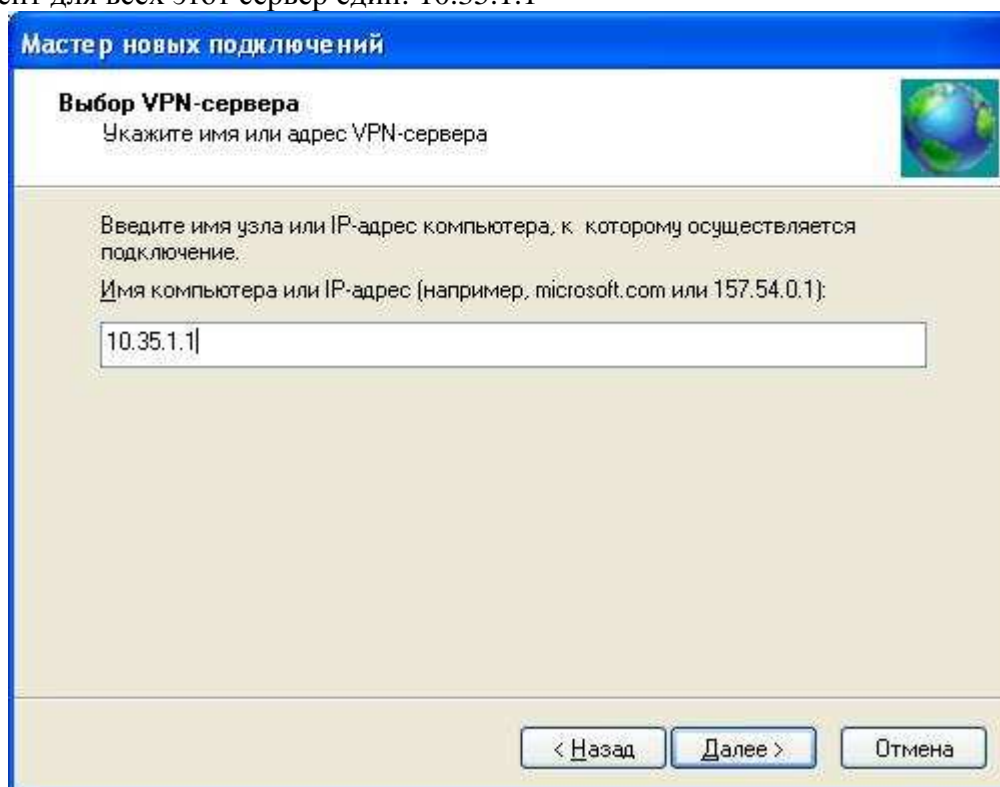


Рисунок 6.7 – Настройка VPN-подключения в Windows XP

з) На следующем окне обязательно(!) выбираем пункт «для всех пользователей» (иначе это подключение не высветится в экране приветствия Windows):

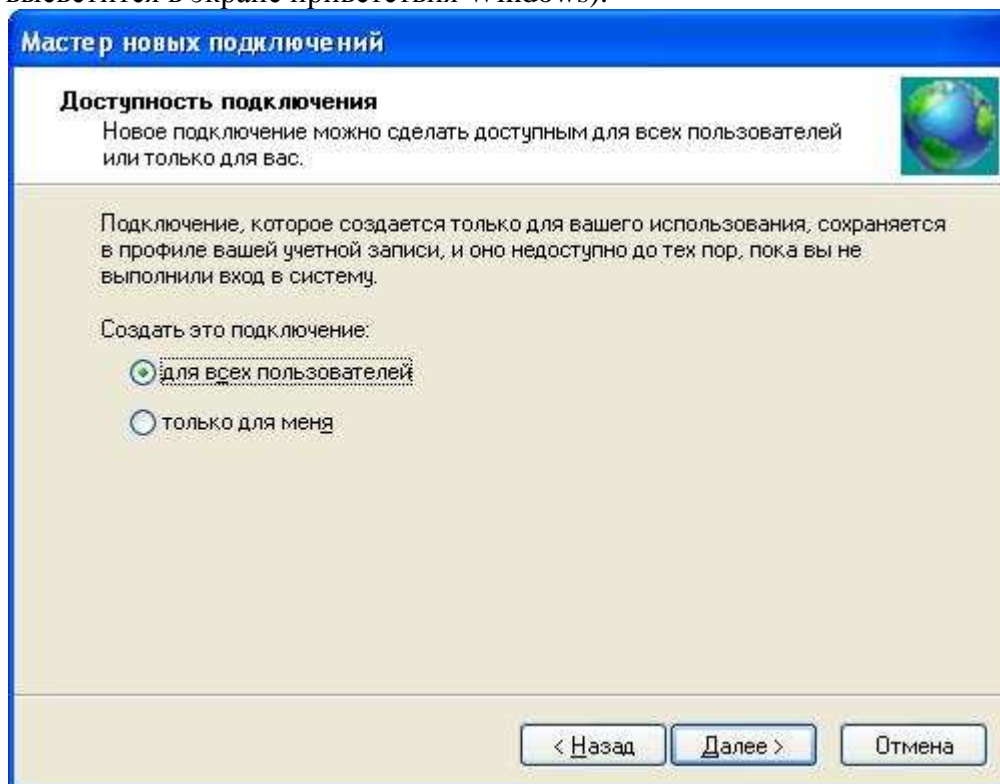


Рисунок 6.8 – Настройка VPN-подключения в Windows XP

и) На следующем окне нас система радостно извещает, что настройки выполнены и все ок. Жмем «Готово». После этого откроется окошко созданного VPN-подключения (см. рис 6.9). Нужно данное подключение дозаполнить:

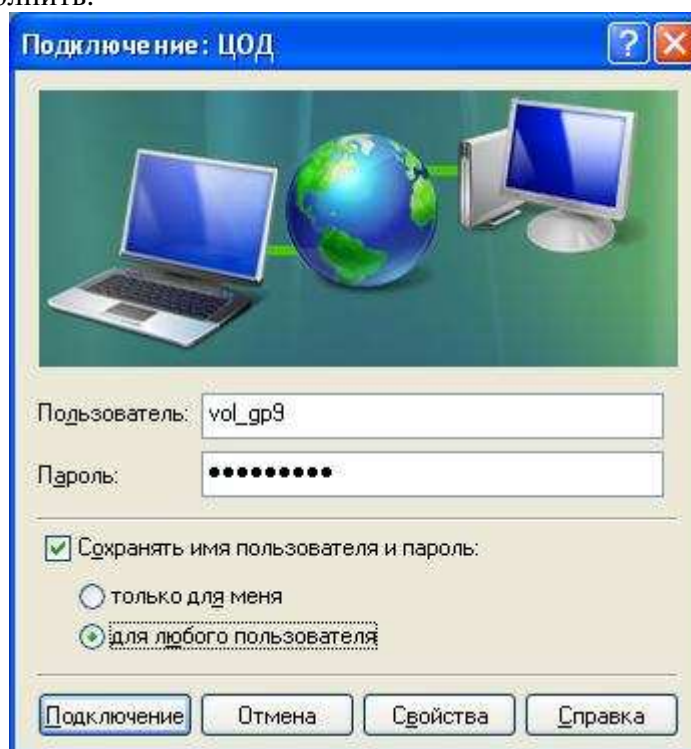


Рисунок 6.9 – Окно VPN-подключения

Необходимо ввести следующие данные:

Пользователь – здесь вводится логин, который был вам выдан в параметрах (см. таблицу 3.3)

Пароль – здесь вводится пароль, который также был вам выдан в параметрах (см. таблицу 3.3)

Также нужно поставить галочку «Сохранять имя пользователя и пароль», а также отметить «для любого пользователя».

После этого ждем на кнопку «Свойства».

к) Откроется окно со свойствами подключения. В нем нужно перейти на вкладку «Безопасность»:

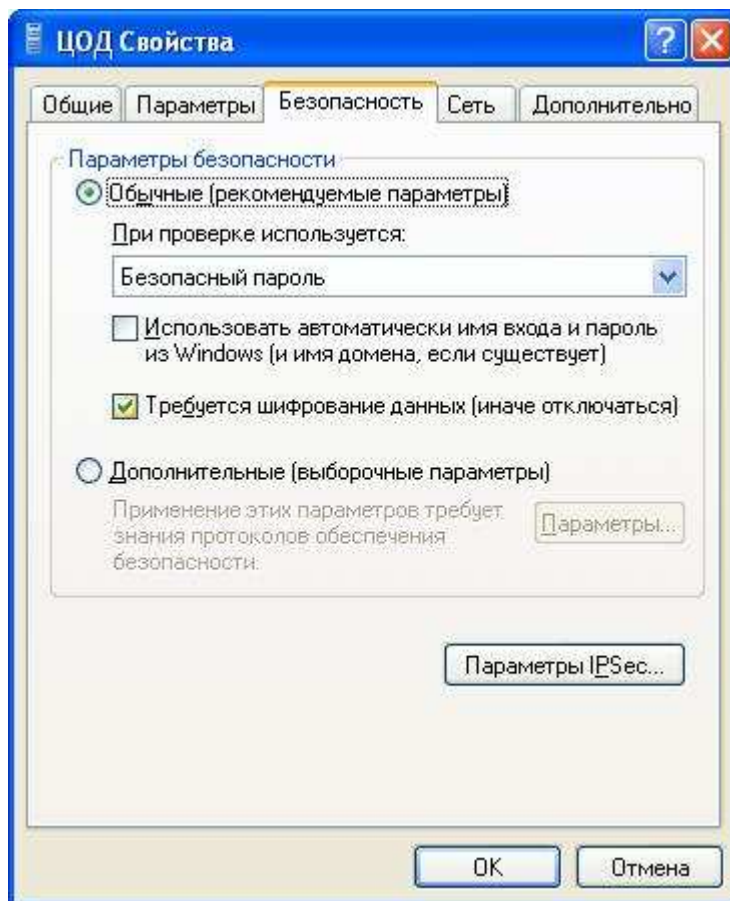


Рисунок 6.10 – Свойства VPN-подключения

В данном окне нужно выбрать пункт «Дополнительные (выборочные параметры)». После этого активируется кнопка «Параметры». Ждем на нее.

л) В открывшемся окне в поле «Шифрование данных» должен быть выбран пункт «необязательное (подключиться даже без шифрования)». Остальные параметры должны быть также как на рисунке ниже:

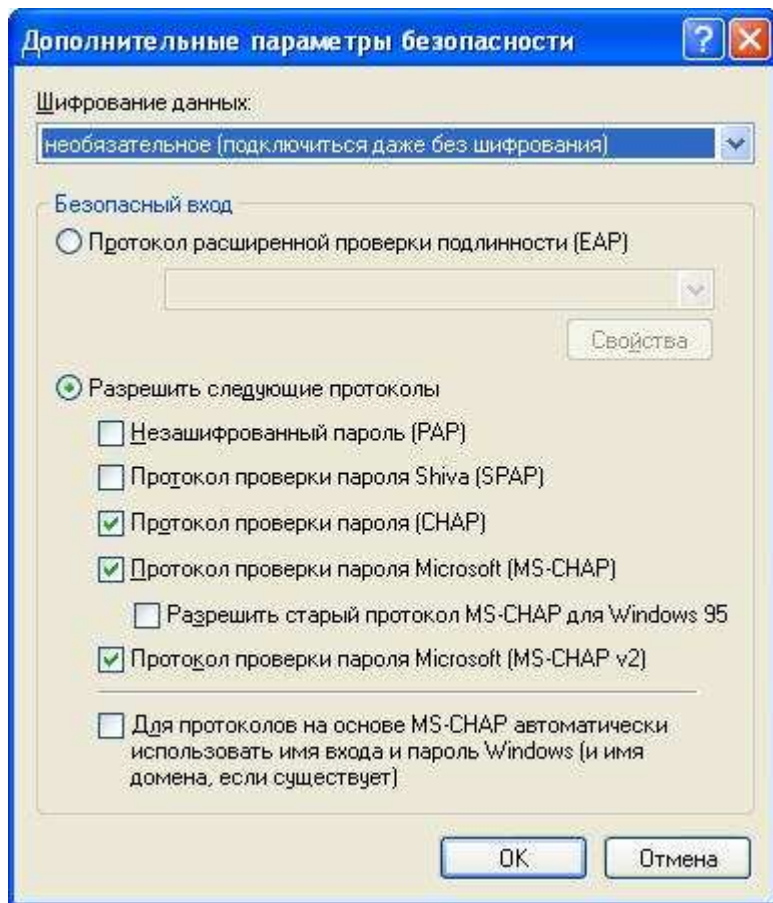


Рисунок 6.11 – Свойства VPN-подключения

Как только выполнили настройку везде жмем ОК.

м) Теперь нужно попробовать подключиться и проверить VPN-подключение. Для этого в главном окне VPN-подключения (рис. 6.9) жмем на кнопку «Подключение».

Если данные введены правильно, то сразу установится соединение:

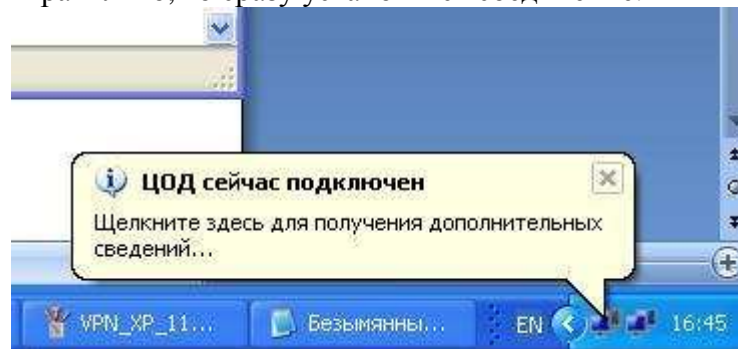
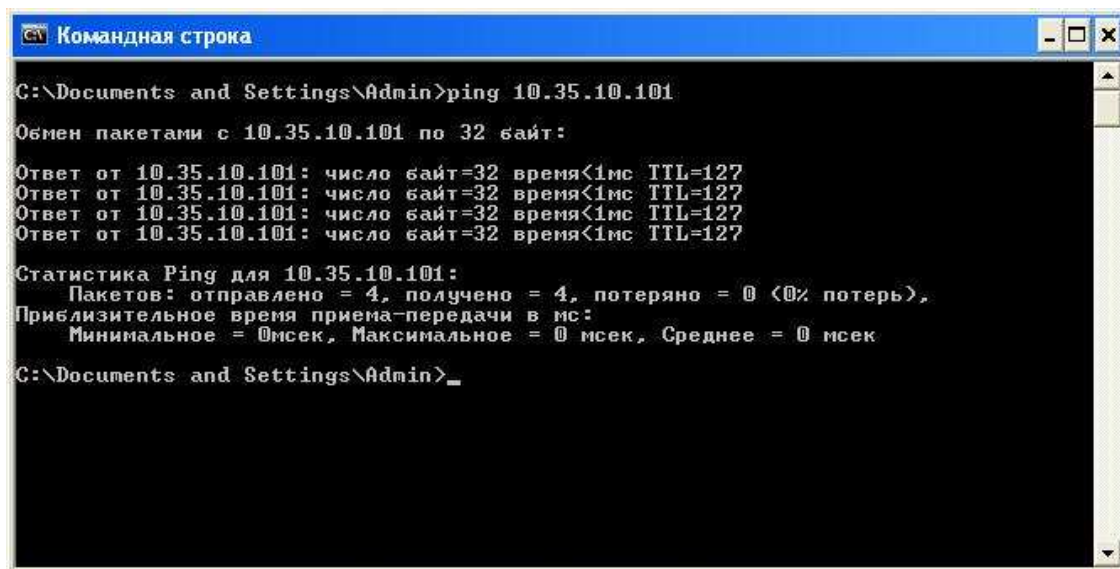


Рисунок 6.12 – Подключение по VPN

н) Делаем проверку.

Для того, чтобы убедиться в том, что все сделано правильно, достаточно лишь пропинговать некоторые адреса:

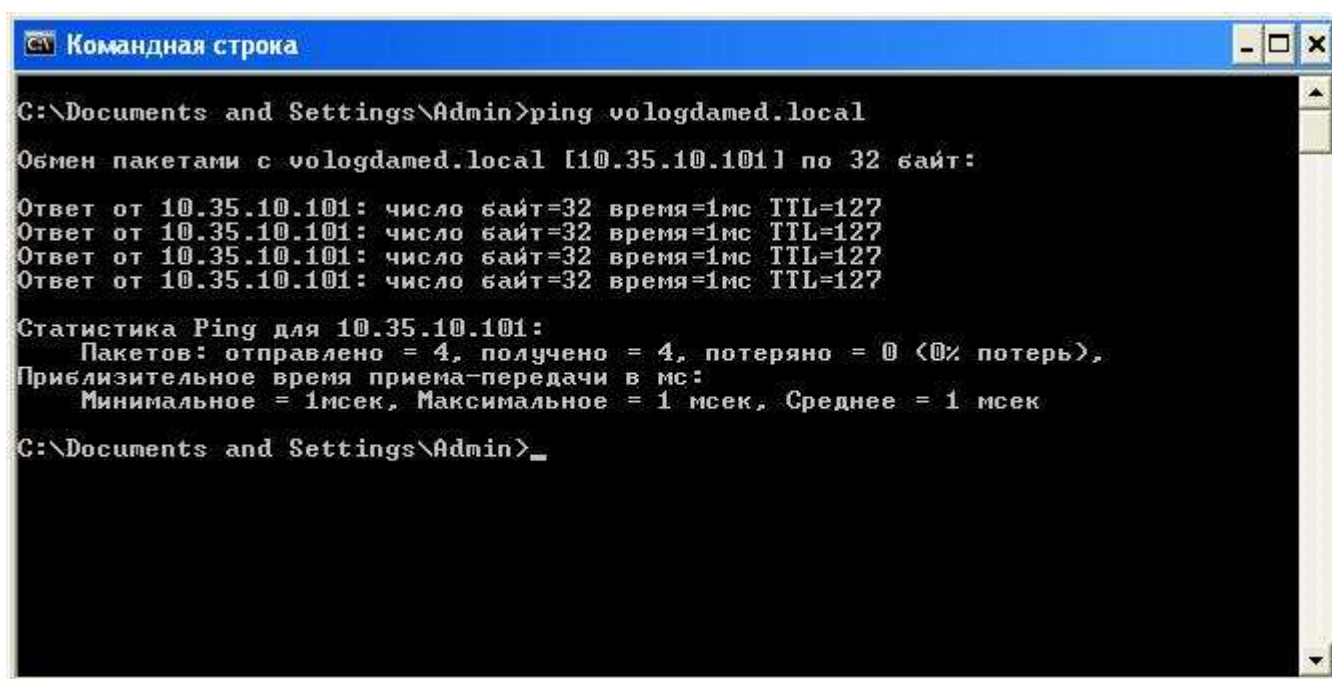
- ping 10.35.10.101 (пингуем DNS-сервер сети видеоконференцсвязи)



```
Командная строка
C:\Documents and Settings\Admin>ping 10.35.10.101
Обмен пакетами с 10.35.10.101 по 32 байт:
Ответ от 10.35.10.101: число байт=32 время<1мс TTL=127
Ответ от 10.35.10.101: число байт=32 время<1мс TTL=127
Ответ от 10.35.10.101: число байт=32 время<1мс TTL=127
Ответ от 10.35.10.101: число байт=32 время<1мс TTL=127
Статистика Ping для 10.35.10.101:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
  Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
C:\Documents and Settings\Admin>_
```

Рисунок 6.13

- ping VOLOGDAMED.LOCAL (пингуем домен сети видеоконференцсвязи)



```
Командная строка
C:\Documents and Settings\Admin>ping vologdamed.local
Обмен пакетами с vologdamed.local [10.35.10.101] по 32 байт:
Ответ от 10.35.10.101: число байт=32 время=1мс TTL=127
Ответ от 10.35.10.101: число байт=32 время=1мс TTL=127
Ответ от 10.35.10.101: число байт=32 время=1мс TTL=127
Ответ от 10.35.10.101: число байт=32 время=1мс TTL=127
Статистика Ping для 10.35.10.101:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
  Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек
C:\Documents and Settings\Admin>_
```

Рисунок 6.14

Если тесты проходят, домен «резолвится» в IP-адрес и пакеты также идут – значит все ОК, можно двигаться дальше.

НЕ отключаемся от VPN и переходим на параграф 7.

6.2. Создание VPN-соединения в Windows 7/8

а) Заходим в папку Панель управления -> Сеть и Интернет -> Центр управления сетями и общим доступом

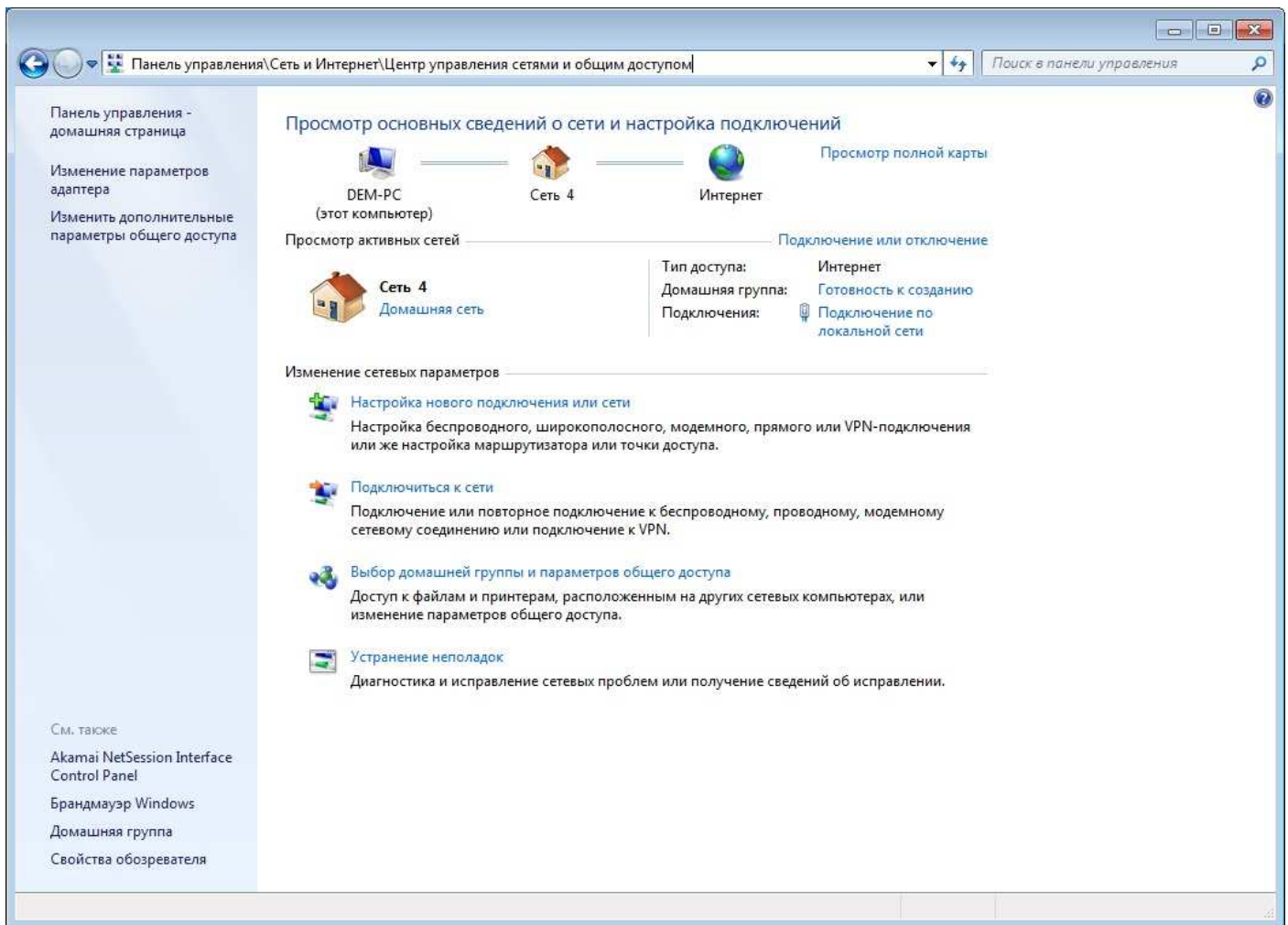


Рисунок 6.15 – Центр управления сетями и общим доступом в Windows 7/8

б) В разделе «Изменение сетевых параметров» выбираем пункт «Настройка нового подключения или сети». Откроется следующее окно:

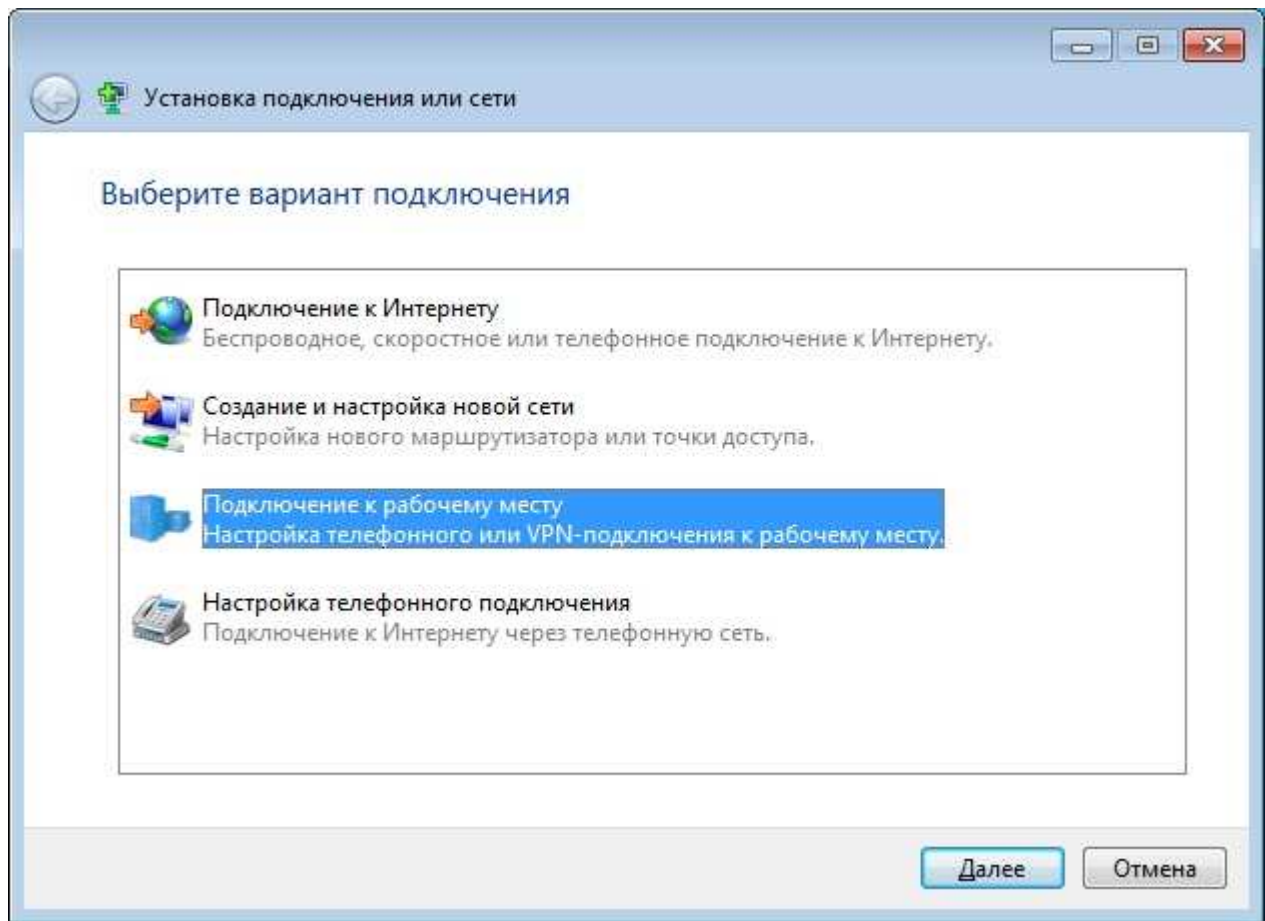


Рисунок 6.16 – Установка подключения или сети в Windows 7/8

Здесь выбираем пункт «Подключение к рабочему месту» и нажимаем «Далее».

в) На следующем окне выбираем пункт «Использовать мое подключение к Интернету (VPN)».

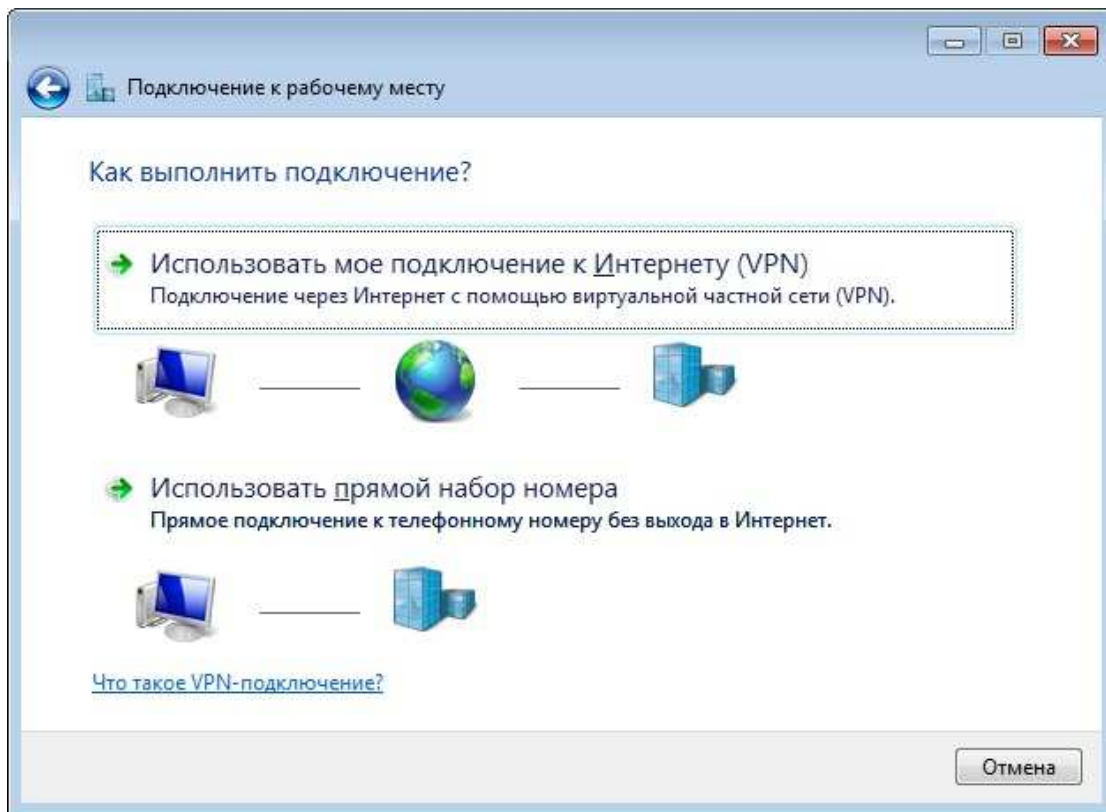


Рисунок 6.17 – Настройка подключения в Windows 7/8

г) На следующем окне вбиваем адрес VPN-сервера (10.35.1.1) и название подключения

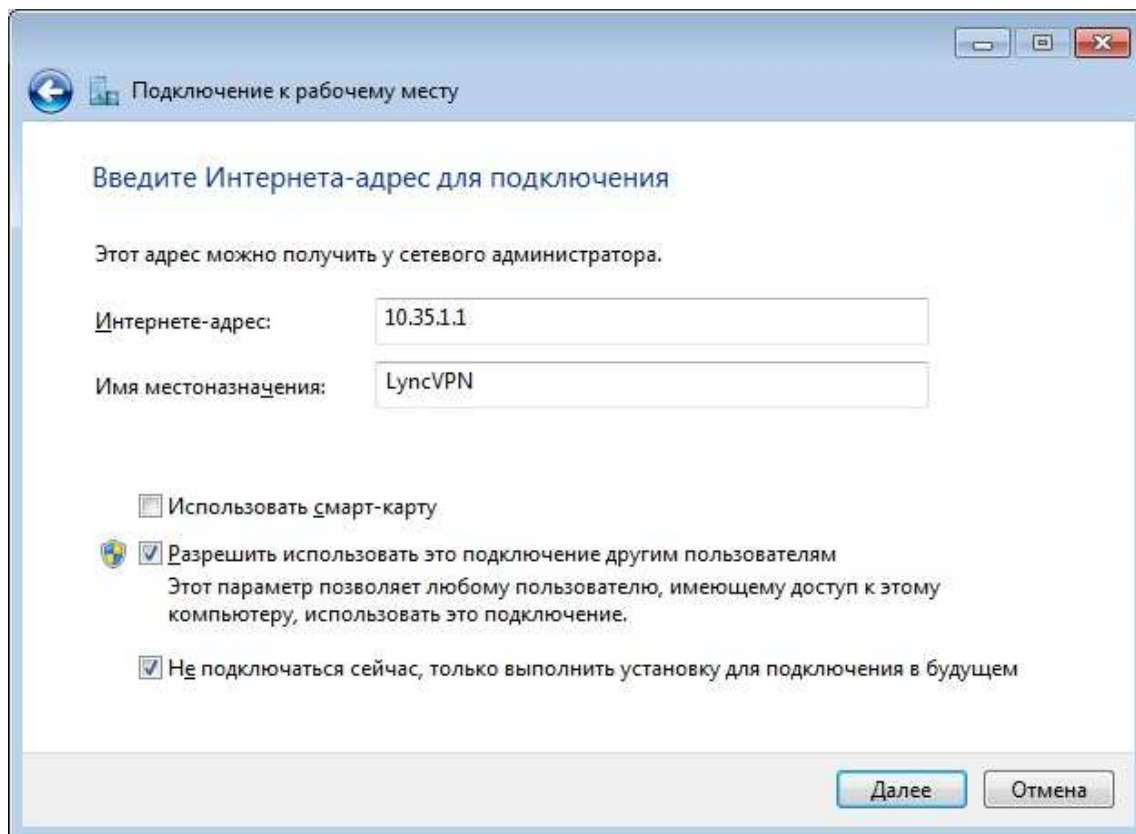


Рисунок 6.18 – Настройка подключения в Windows 7/8

Обязательно нужно поставить галочки на пунктах «Разрешить использовать это подключение другим пользователям» и «Не подключаться сейчас, только выполнить установку для подключения в будущем».

Жмем опять «Далее».

д) На следующем окне вбиваем авторизационные параметры.

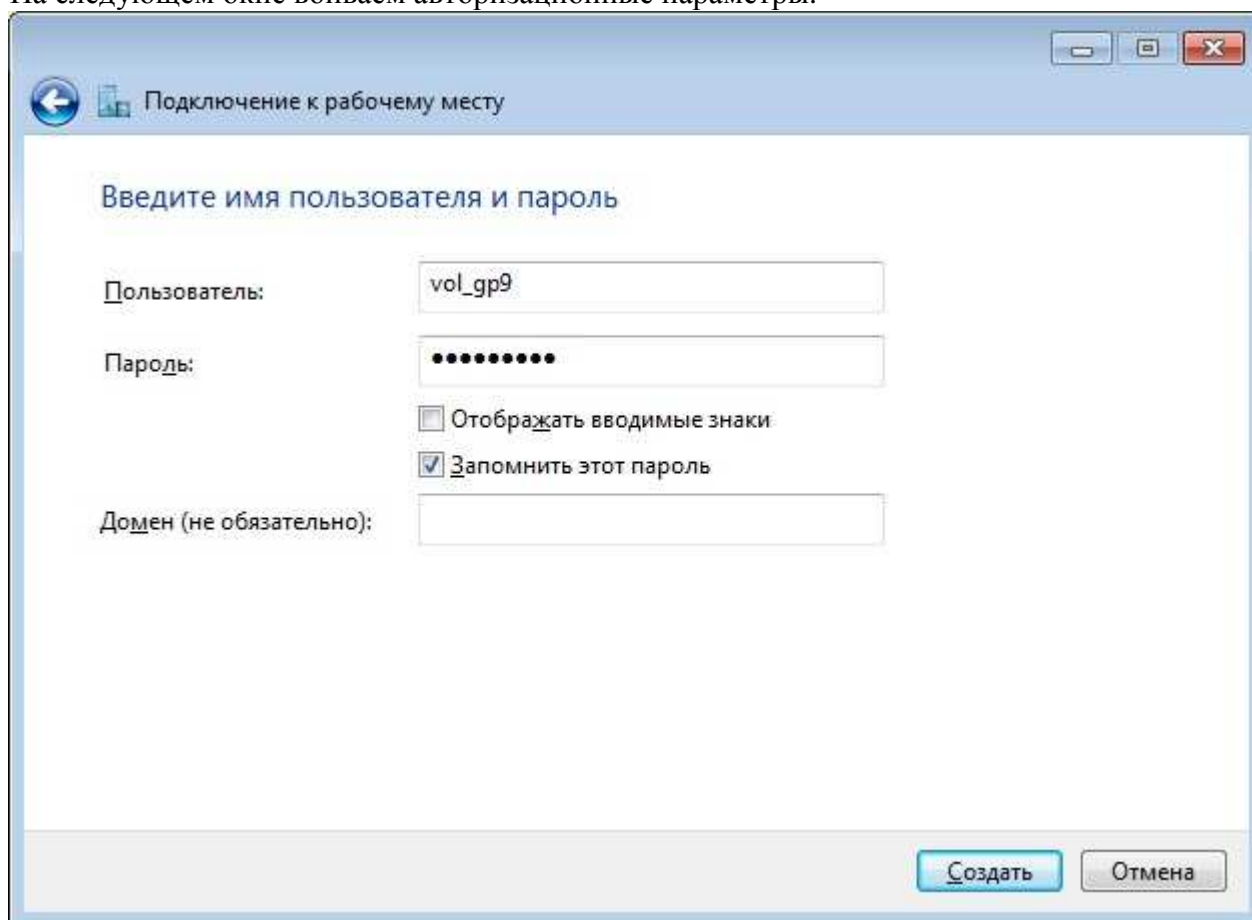


Рисунок 6.19 – Настройка подключения в Windows 7/8

Необходимо ввести следующие данные:

Пользователь – здесь вводится логин, который был вам выдан в параметрах (см. таблицу 3.3)

Пароль – здесь вводится пароль, который также был вам выдан в параметрах (см. таблицу 3.3)

Домен: VOLOGDAMED

Также ставим галочку «Запомнить этот пароль».

Жмем на кнопку «Создать».

е) На следующем окне жмем кнопку Закр~~ыть~~. Создание подключения выполнено.

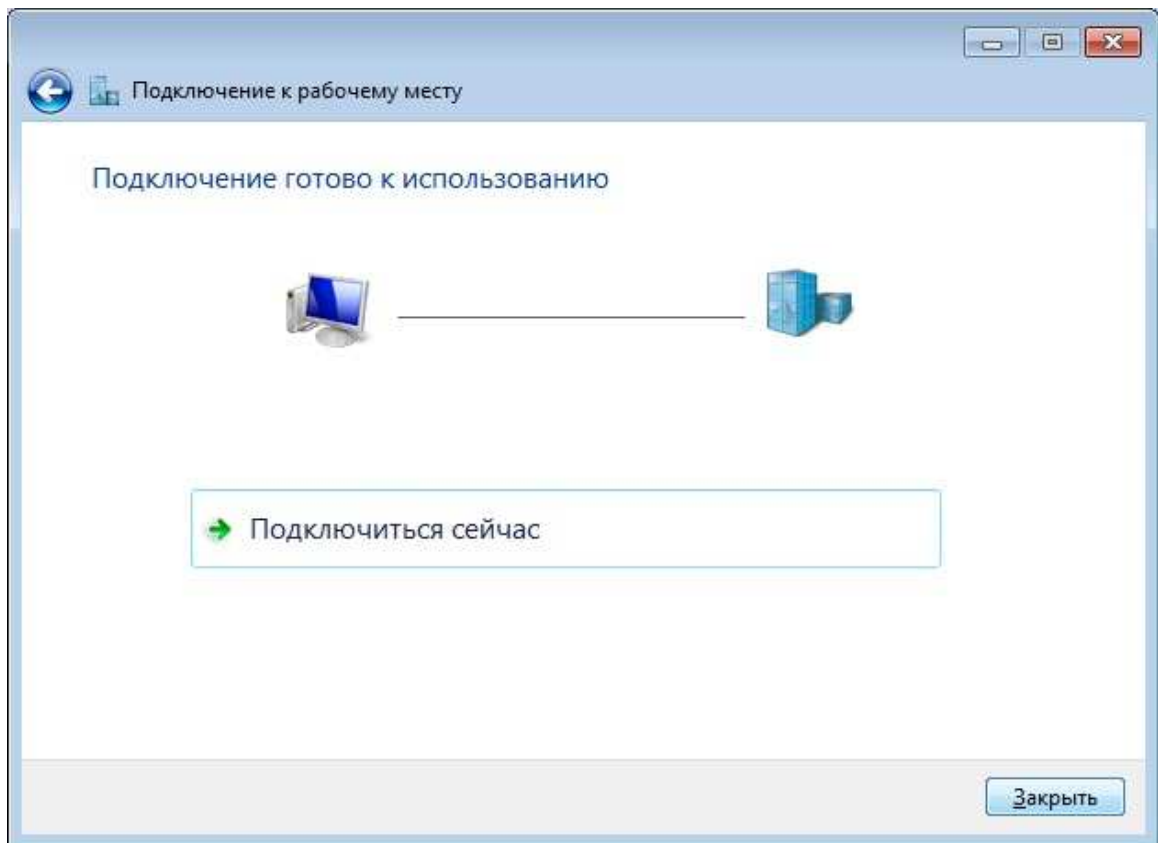


Рисунок 6.20 – Настройка подключения в Windows 7/8

ж) Теперь возвращаемся в Центр управления сетями и общим доступом (см. рис 6.15) и щелкаем в левом меню «Изменение параметров адаптера». В результате попадаем в папку «Сетевые подключения»:

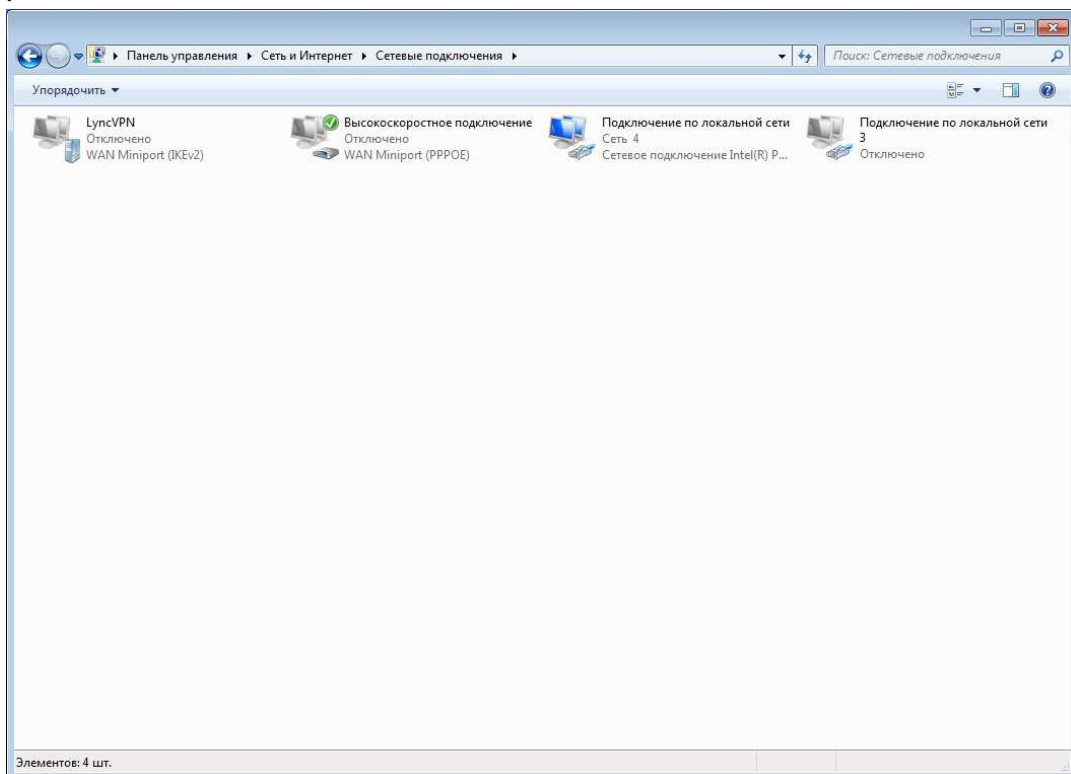


Рисунок 5.21 – Сетевые подключения в Windows 7/8

з) Щелкаем двойным щелчком по созданному VPN-подключению. В результате открывается окно:

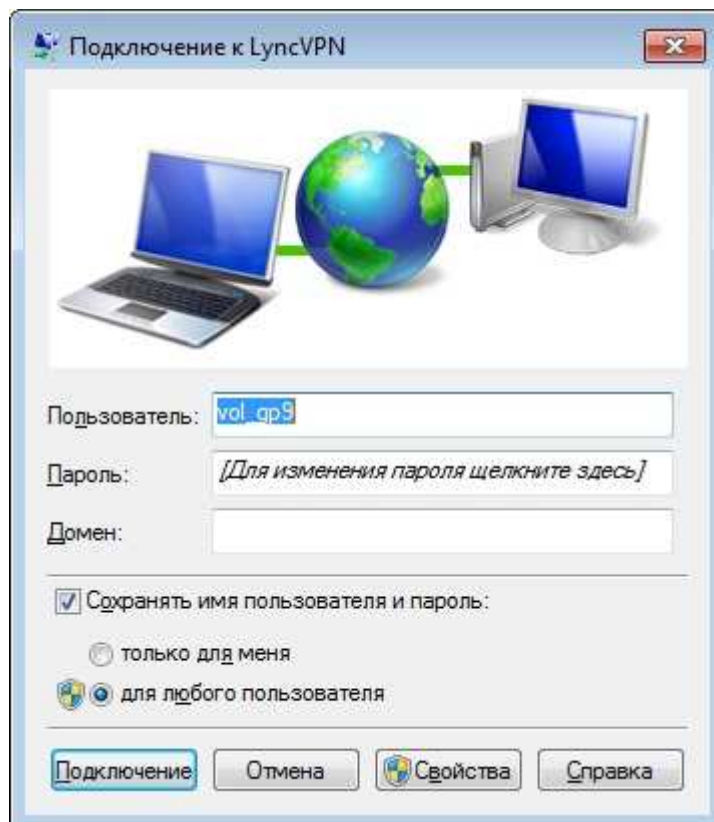


Рисунок 6.22 – Окно VPN-подключения в Windows 7/8

Поля Пользователь, Пароль, Домен должны быть заполнены данными, которые вы вводили ранее при создании подключения.

Также просьба обратить внимание: должна стоять галочка «Сохранять имя пользователя и пароль», а также «для любого пользователя».

и) Жмем в окошке на кнопку Свойства и в открывшемся диалоговом окне переходим на вкладку «Безопасность»:

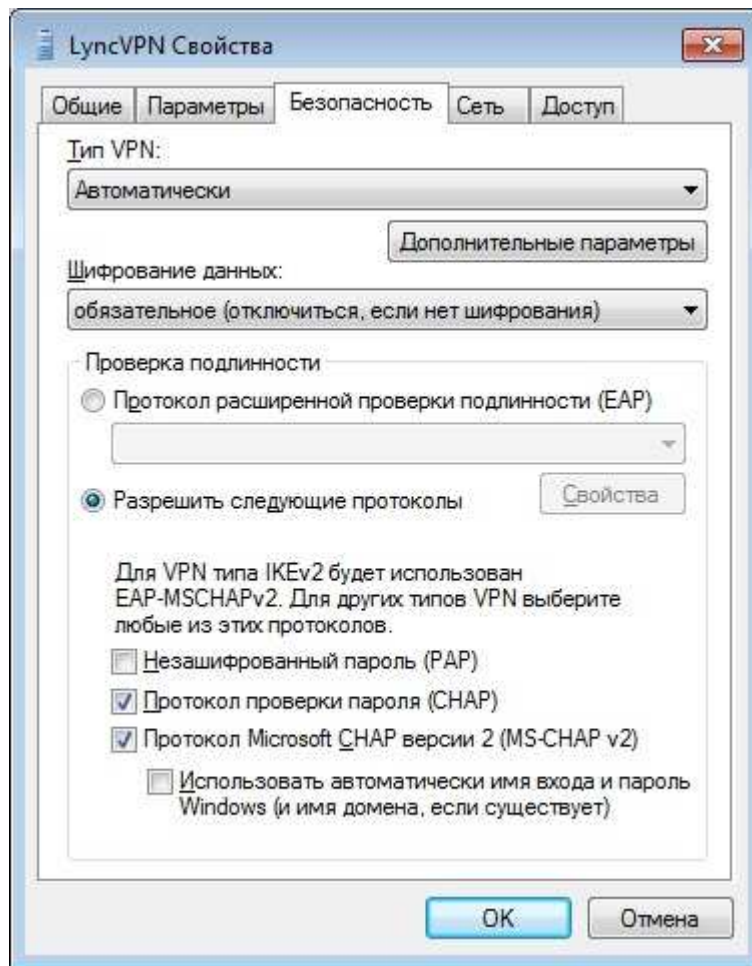


Рисунок 6.23 – Окно VPN-подключения в Windows 7/8

к) На вкладке «Безопасность» нужно выбрать в поле «Тип VPN» опцию «Туннельный протокол точка-точка», а в поле «Шифрование данных» опцию «необязательное, подключаться даже без шифрования»:

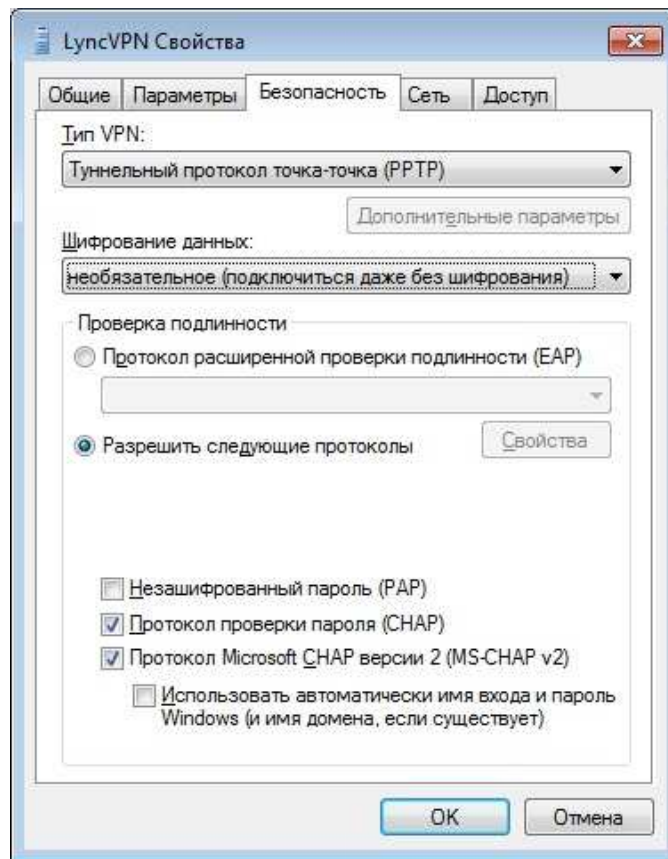


Рисунок 6.24 – Свойства VPN-подключения

После этого везде жмем ОК.

л) Теперь нужно попробовать подключиться и проверить VPN-подключение. Для этого в главном окне VPN-подключения (рис. 6.22) жмем на кнопку «Подключение».:.

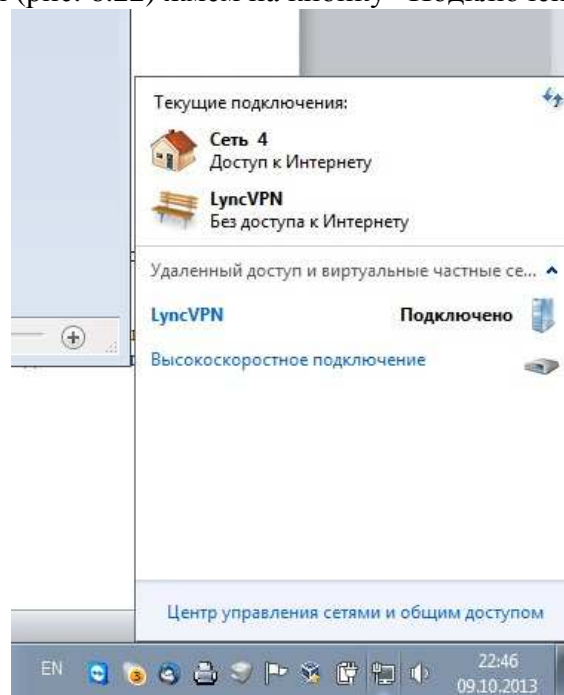


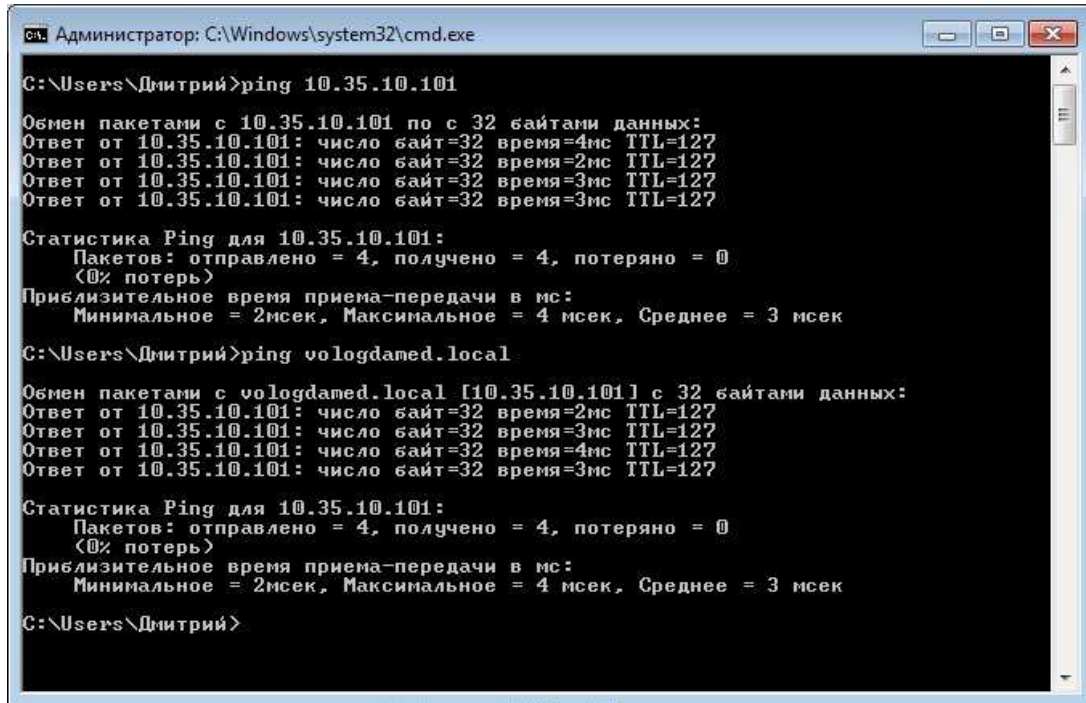
Рисунок 6.25 – Подключение по VPN

Как только выполнили настройку везде жмем ОК.

м) Делаем проверку.

Для того, чтобы убедиться в том, что все сделано правильно, достаточно лишь пропинговать некоторые адреса:

- ping 10.35.10.101 (пингует DNS-сервер сети видеоконференцсвязи)
- ping VOLOGDAMED.LOCAL (пингует домен сети видеоконференцсвязи)



```
Администратор: C:\Windows\system32\cmd.exe
C:\Users\Дмитрий>ping 10.35.10.101
Обмен пакетами с 10.35.10.101 по 32 байтами данных:
Ответ от 10.35.10.101: число байт=32 время=4мс TTL=127
Ответ от 10.35.10.101: число байт=32 время=2мс TTL=127
Ответ от 10.35.10.101: число байт=32 время=3мс TTL=127
Ответ от 10.35.10.101: число байт=32 время=3мс TTL=127

Статистика Ping для 10.35.10.101:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 4 мсек, Среднее = 3 мсек

C:\Users\Дмитрий>ping vologdamed.local
Обмен пакетами с vologdamed.local [10.35.10.101] с 32 байтами данных:
Ответ от 10.35.10.101: число байт=32 время=2мс TTL=127
Ответ от 10.35.10.101: число байт=32 время=3мс TTL=127
Ответ от 10.35.10.101: число байт=32 время=4мс TTL=127
Ответ от 10.35.10.101: число байт=32 время=3мс TTL=127

Статистика Ping для 10.35.10.101:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 4 мсек, Среднее = 3 мсек

C:\Users\Дмитрий>
```

Рисунок 6.26

Если тесты проходят, домен «резолвится» в IP-адрес и пакеты также идут – значит все ОК, можно двигаться дальше.

НЕ отключаемся от VPN и переходим на пункт 6.

7. Установка корневого сертификата домена видеоконференцсвязи

Теперь, когда компьютер (точнее – операционная система) видит сеть системы видеоконференцсвязи, на компьютере установлен клиент MS Lync, подключена Web-камера, необходимо установить корневой сертификат домена видеоконференцсвязи. Для этого нужно выполнить следующие шаги.

7.1. Простая (первичная) установка сертификата

В данном подразделе рассматривается самый простой способ установки сертификата. Если после его выполнения вам все равно не удастся войти в Lync, то переходите к пункту 7.2.

а) Начало установки сертификата

Так как файл сертификата вам должен быть прислан по электронной почте, то его необходимо скачать. Скачать можно в любую папку. В данном примере, сертификат скачан на рабочий стол:



Рисунок 7.1 – Корневой сертификат домена видеоконференцсвязи

Щелкаем по сертификату двойным щелчком левой кнопки мыши. Запустится следующее окно:

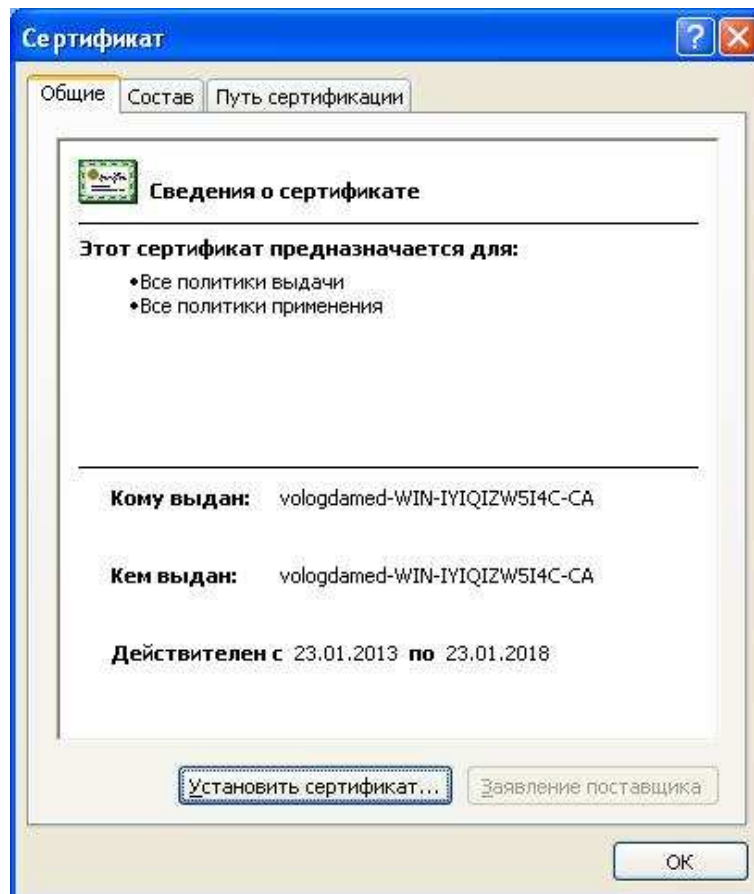


Рисунок 7.2 – Диалоговое окно сертификата

б) Жмем на кнопочку «Установить сертификат». Откроется «Мастер импорта сертификатов»

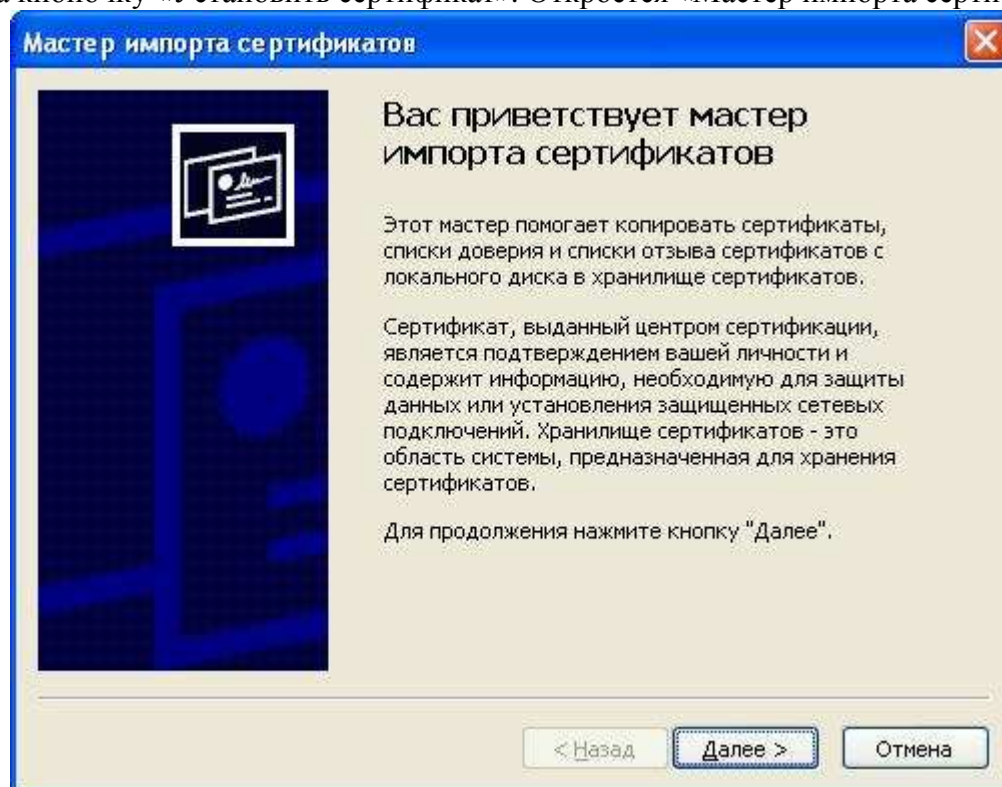


Рисунок 7.3 – Мастер импорта сертификатов

Жмем кнопку «Далее».

в) В открывшемся окне выбора хранилища сертификатов оставляем все по умолчанию:

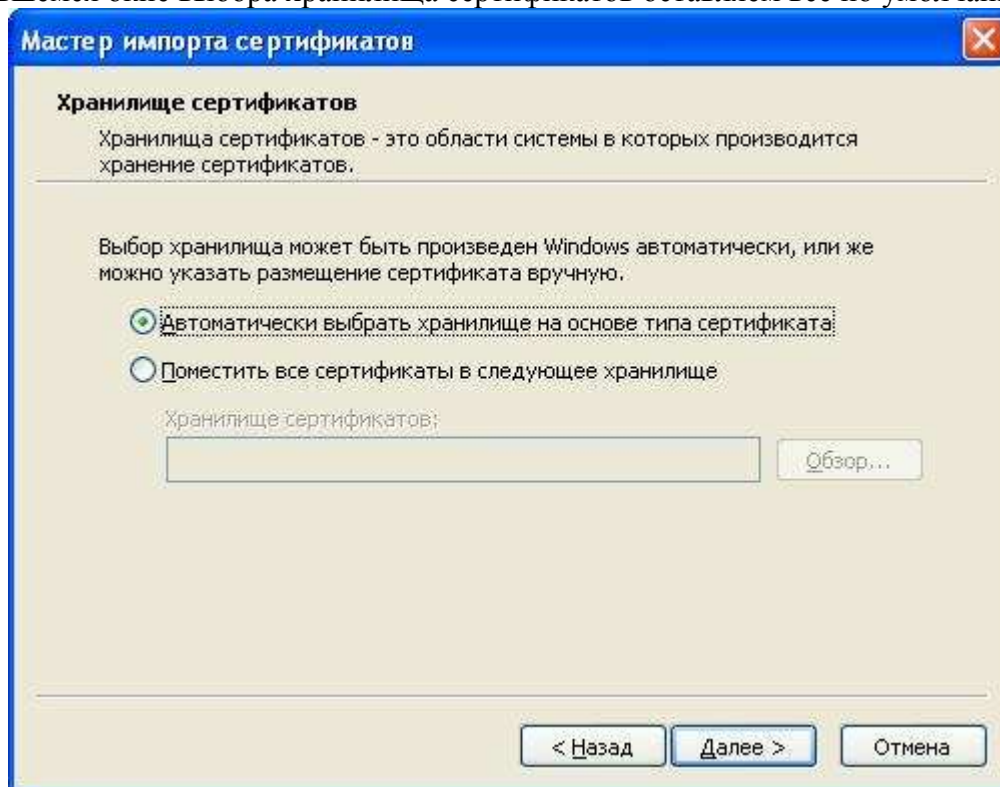


Рисунок 7.4 – Установка сертификата. Выбор хранилища сертификатов.

г) В следующем окне Мастер должен известить вас о завершении импорта сертификатов:

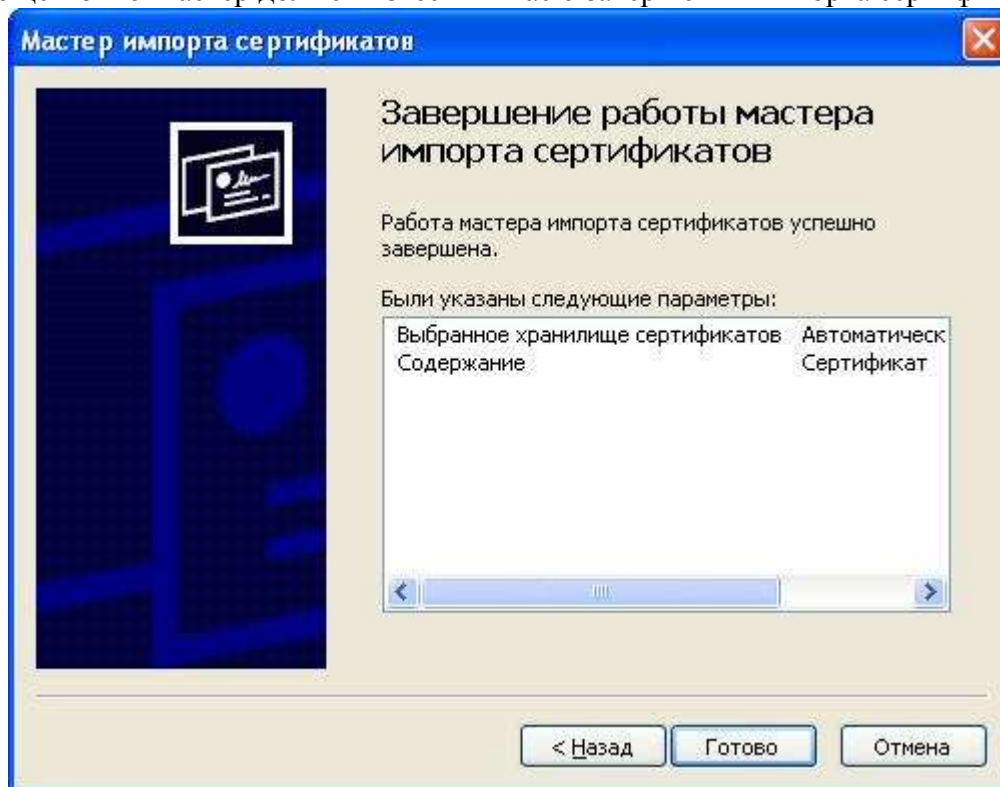


Рисунок 7.5 – Завершение работы мастера импорта сертификатов

Здесь жмем кнопку «Готово».

д) Если импорт прошел успешно, то выскочит такое сообщение:

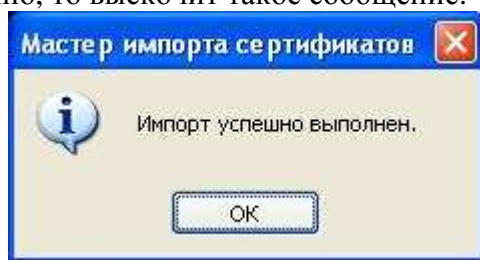


Рисунок 7.6 – Успешный импорт сертификатов

Жмем кнопку ОК и переходим к 8-ому параграфу. Если при выполнении всех инструкций по входу в Lync там выйдет ошибка, то проделываем последовательность шагов, приведенную в подразделе 7.2.

7.2. Расширенная установка сертификата

Внимание! Во избежание разночтений, действия данного подраздела просьба выполнять только после того, как были выполнены все шаги из подраздела 7.1.

а) Двойным щелчком снова кликаем по сертификату (как в подразделе 7.1, пункт а). Видим ошибку.

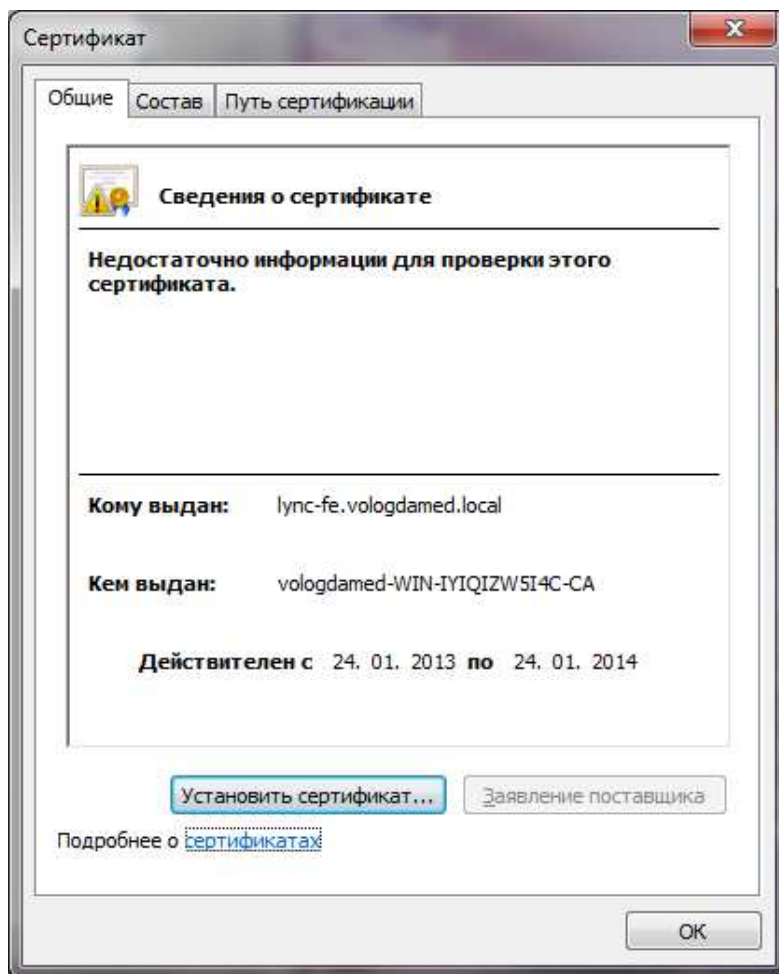


Рисунок 7.7 – Ошибка при установке сертификата

Переходим на вкладку «Путь сертификации» и видим, что сертификат установлен с ошибкой (желтый треугольник с восклицательным знаком).

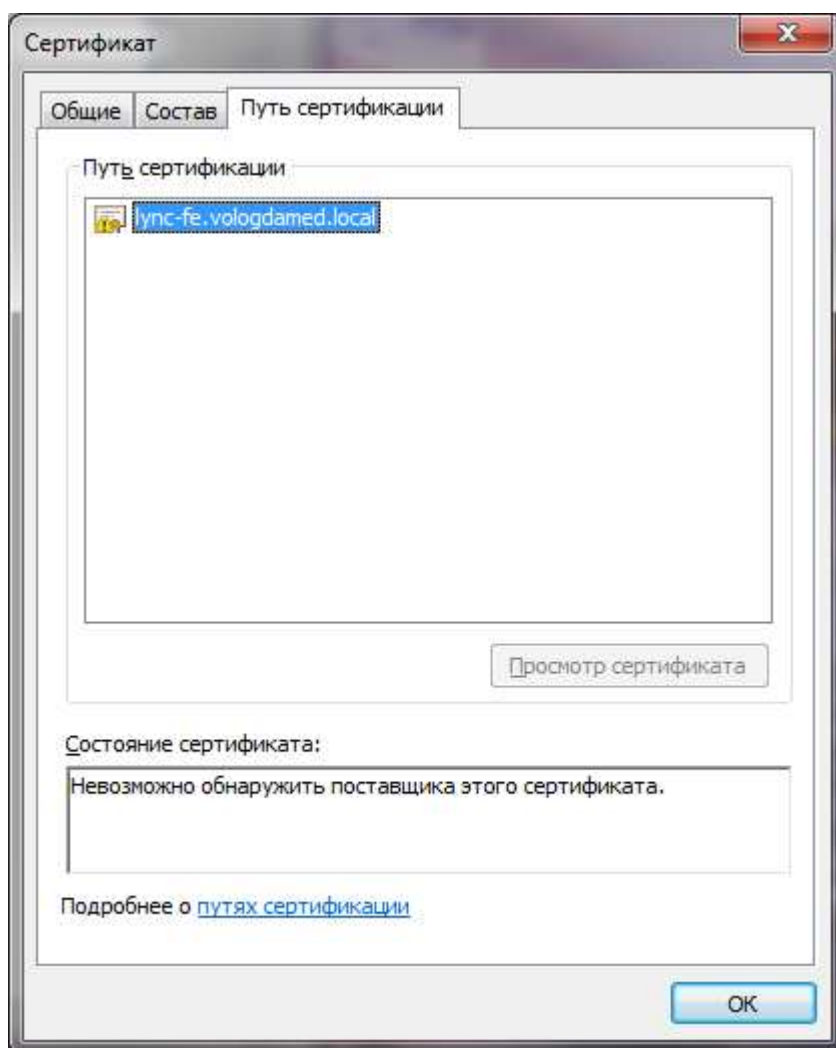


Рисунок 7.8 – Ошибка при установке сертификата

б) Заходим в Панель управления -> Сеть и Интернет -> Свойства обозревателя. В открывшемся диалоговом окне переходим на вкладку «Содержание» и там кликаем по кнопке «Сертификаты».

В окне «Сертификаты» переходим на вкладку «Другие пользователи» и видим следующее – наш сертификат почему-то установился в этот раздел (см. рис. 7.9).

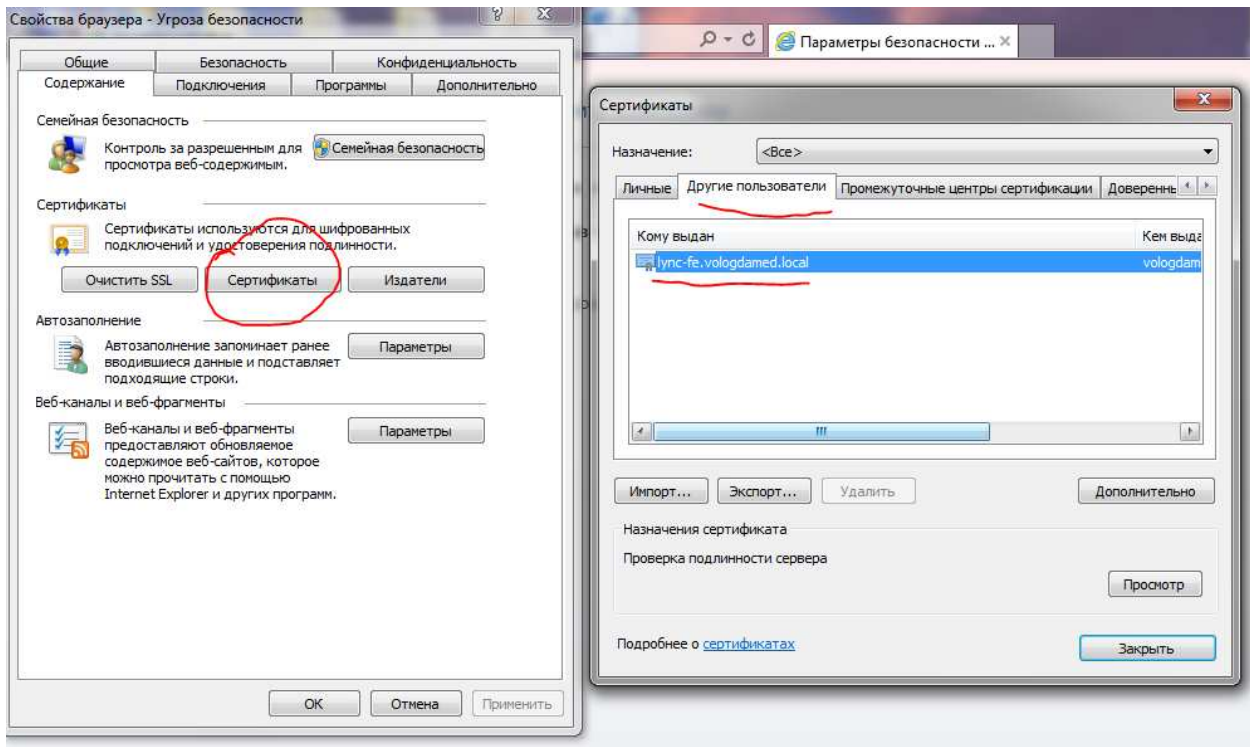


Рисунок 7.9 – Некорректное размещение сертификата

в) Начинаем процедуру импорта еще раз. Двойным щелчком щелкаем по сертификату и ждем на кнопку «Установить сертификат» (пункты а), б) подраздела 7.1).

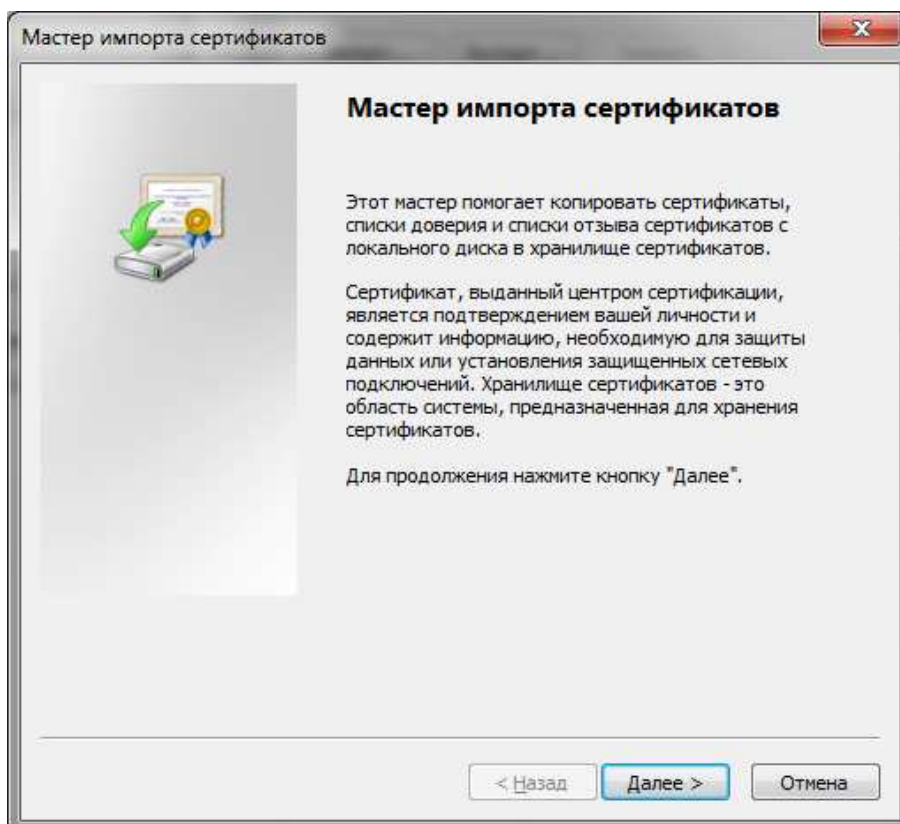


Рисунок 7.10 – Установка сертификата

Здесь ждем кнопку «Далее».

г) В следующем окне ставим галочку на пункте «Поместить все сертификаты в следующее хранилище» и ждем на кнопку «Обзор».

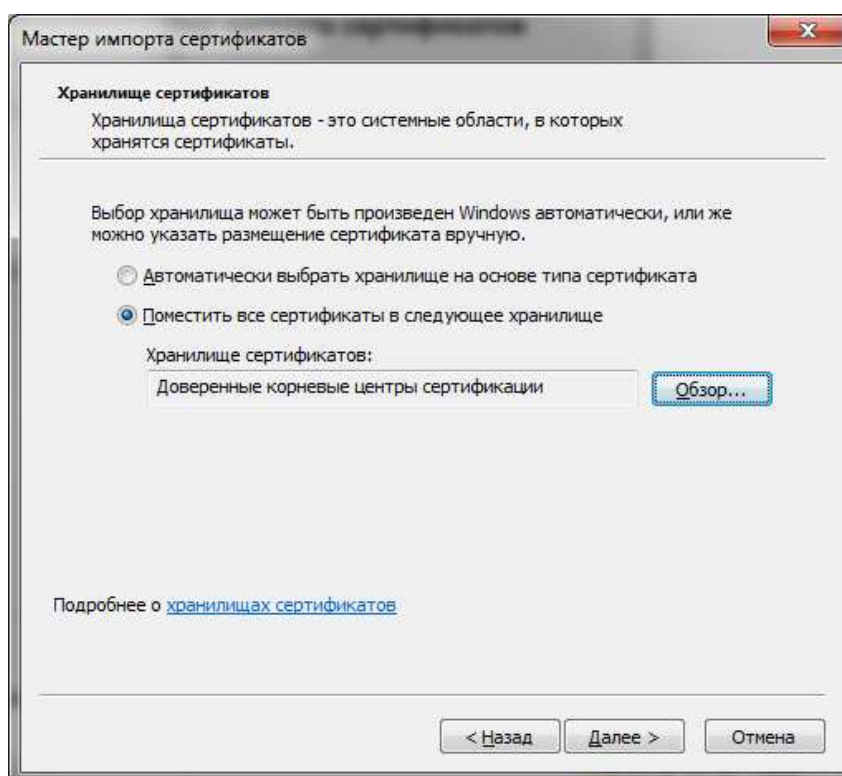


Рисунок 7.11 – Выбор хранилища сертификатов

д) В открывшемся диалоговом окне нужно выбрать «Доверенные корневые центры сертификации».

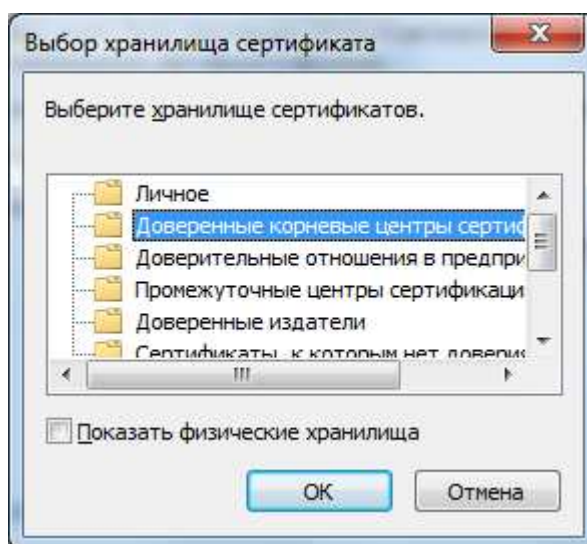


Рисунок 7.12 – Выбор хранилища сертификатов

Ждем здесь кнопку «ОК», а в окне «Мастер импорта сертификатов» проверяем поле «Хранилище сертификатов» (рис. 7.11) и, если все соответствует нашему выбору, ждем кнопку «Далее».

е) В открывшемся окне жмем кнопку «Готово».

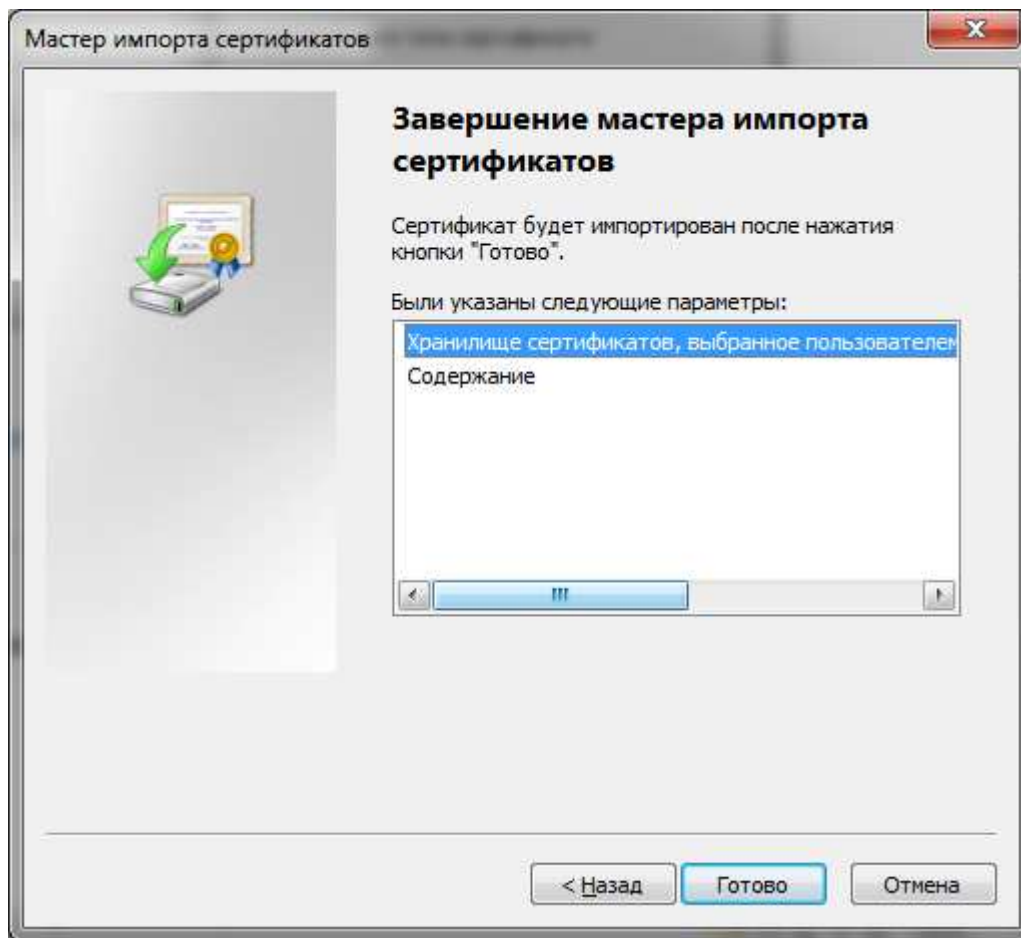


Рисунок 7.13 – Завершение Мастера импорта сертификатов

ж) В некоторых случаях может выскочить следующее предупреждение о безопасности.

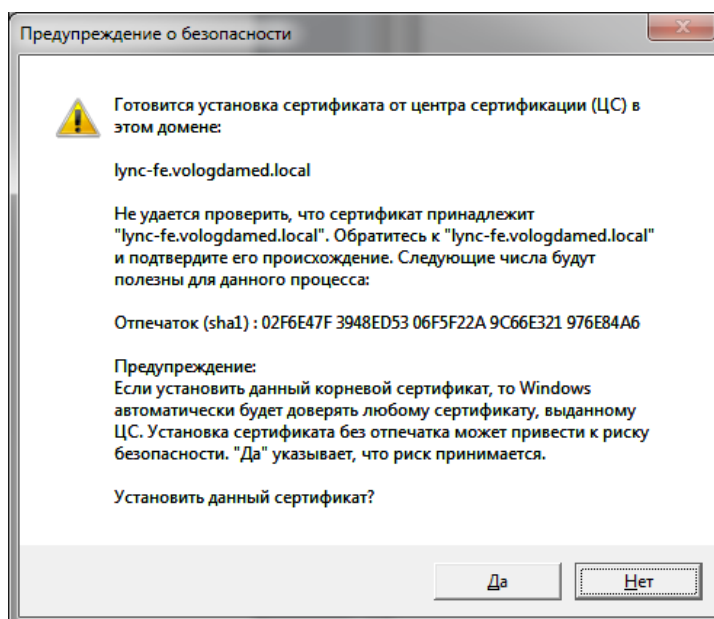


Рисунок 7.14 – Предупреждение о безопасности

В открывшемся окне жмем на «Да». После этого должно высветиться сообщение об успешном импорте сертификата.

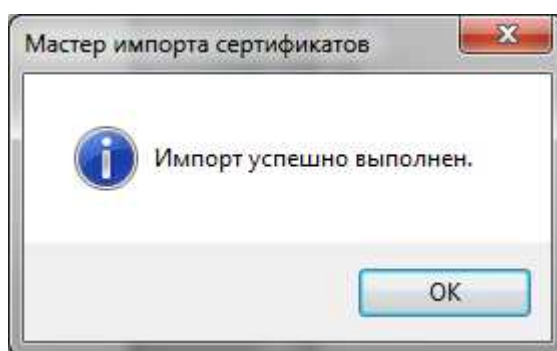


Рисунок 7.15 – Успешный импорт сертификата

з) Снова открываем сертификат на вкладке «Путь к сертификации» (пункт а) данного подраздела)

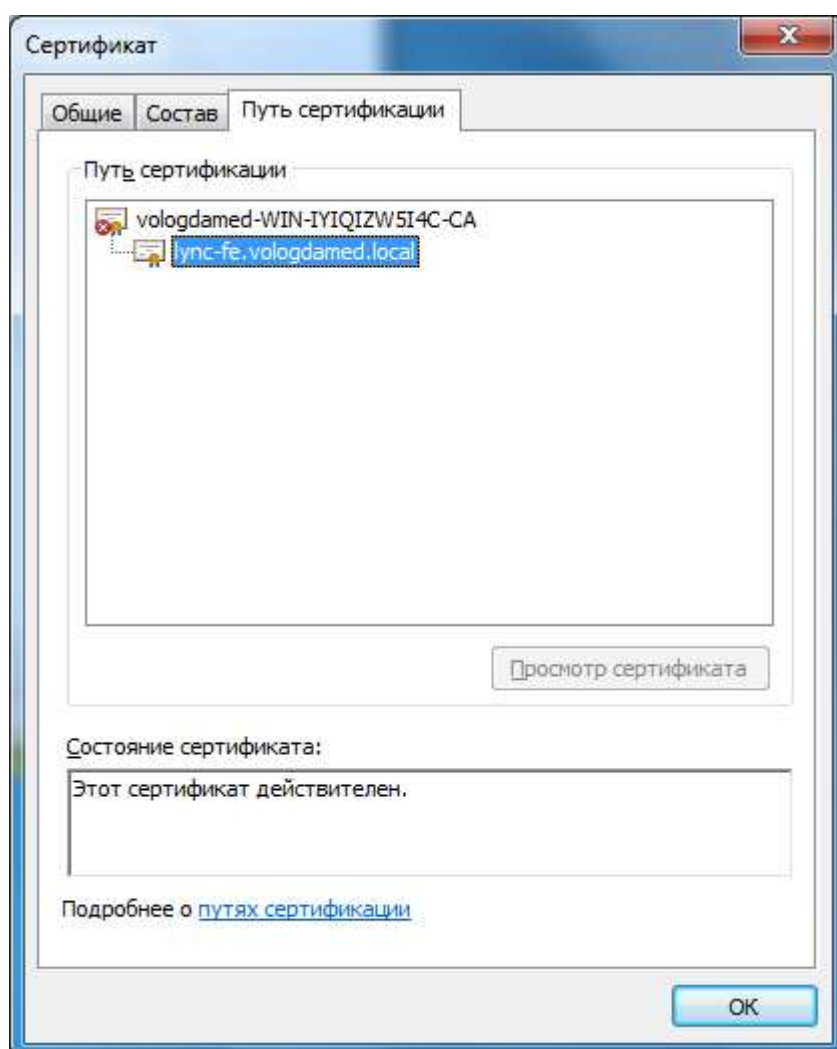


Рисунок 7.16 – Проблема с корневым сертификатом

Видимо, что не хватает корневого сертификата.

и) Заходим в Панель управления -> Сеть и Интернет -> Свойства обозревателя. В открывшемся диалоговом окне переходим на вкладку «Содержание» и там кликаем по кнопке «Сертификаты».

В окне «Сертификаты» переходим на вкладку «Промежуточные центры сертификации» и видим следующее – наш сертификат почему-то установился в этот раздел (см. рис. 7.17).

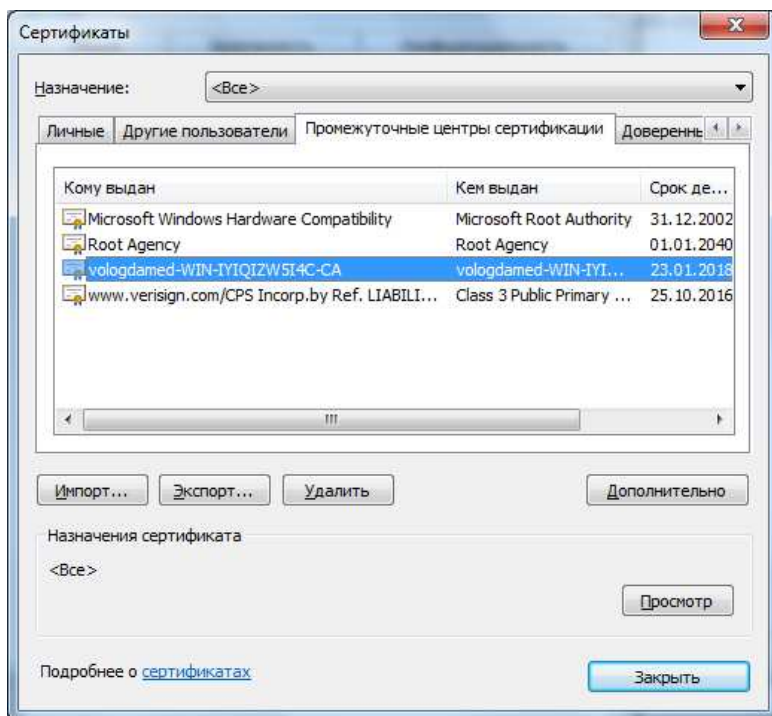


Рисунок 7.17 – Проблема с корневым сертификатом

к) Нам нужно перенести данный сертификат в Доверенные центры. Для этого, экспортируем данный сертификат. Допустим сделаем это на рабочий стол. Выделяем корневой сертификат (как на рис. 7.17) и ждем на кнопку «Экспорт...».

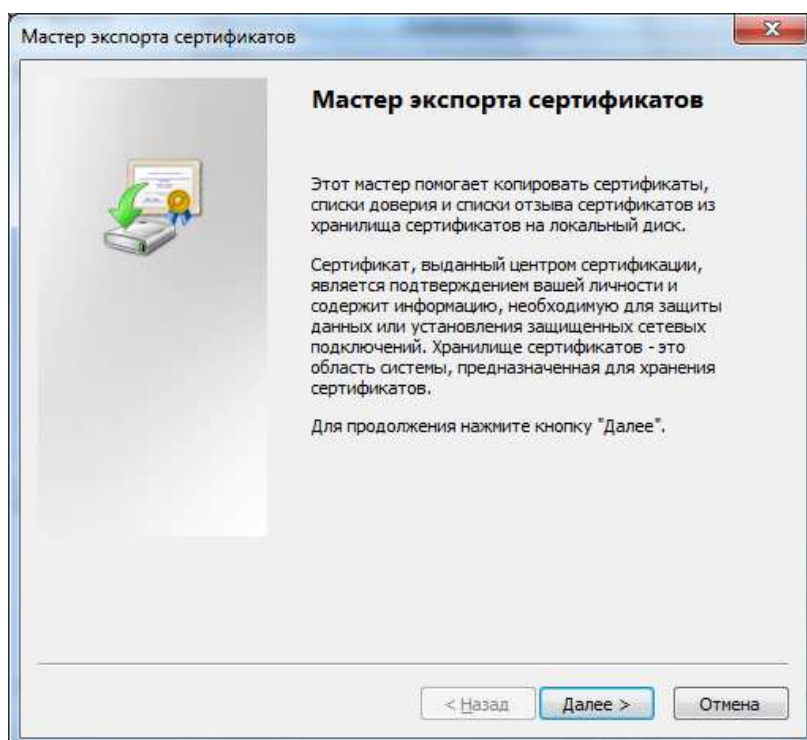


Рисунок 7.18 – Экспорт корневого сертификата

Жмем здесь кнопку «Далее».

л) В открывшемся окне выбираем пункт «Файлы X.509 (.CER) в кодировке DER».

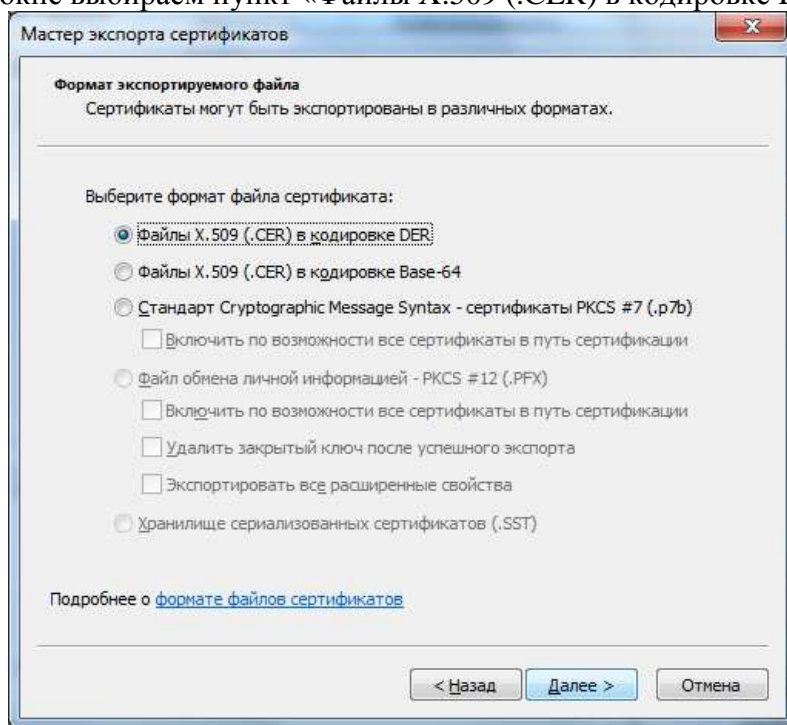


Рисунок 7.19 – Экспорт корневого сертификата

Жмем кнопку «Далее».

м) В открывшемся окне жмем на кнопочку обзор. Откроется окно, где выбираем место и имя экспортируемого сертификата. Например, назовем его 1.cer и положим на Рабочий стол.

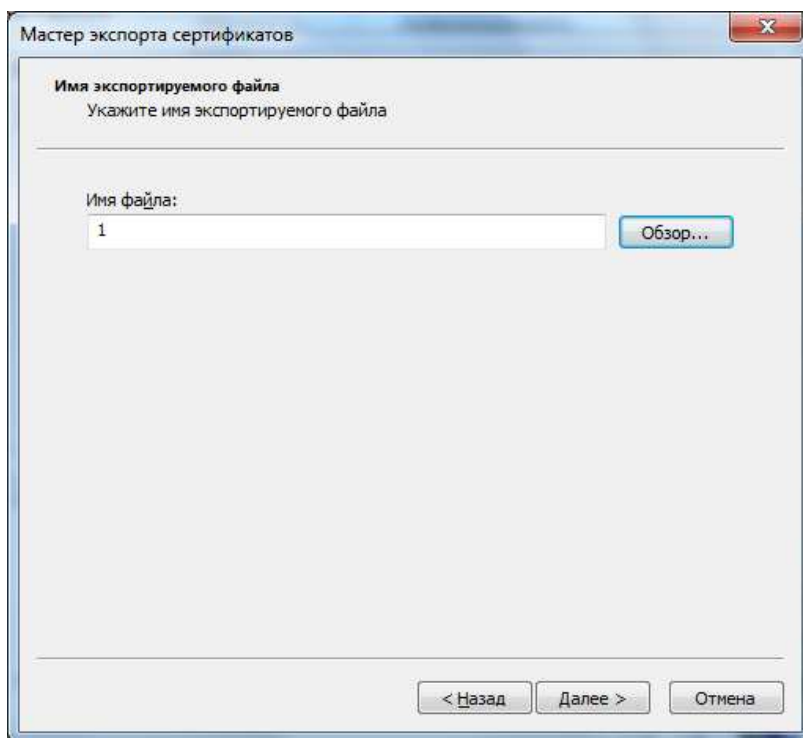


Рисунок 7.20 – Выбор места экспорта и имени файла

Выбираем название файла и место его сохранения.

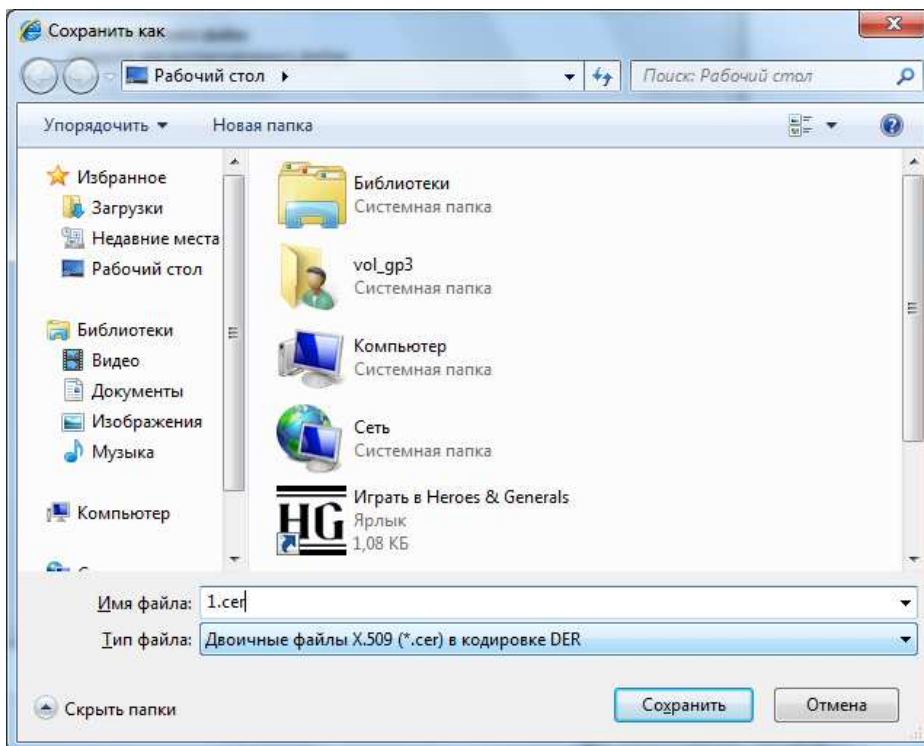


Рисунок 7.21 – Выбор места экспорта и имени файла

Жмем на кнопку «Сохранить» и кнопку «Далее» в окне Мастера экспорта сертификатов.

м) В следующем окне жмем на кнопку «Готово».

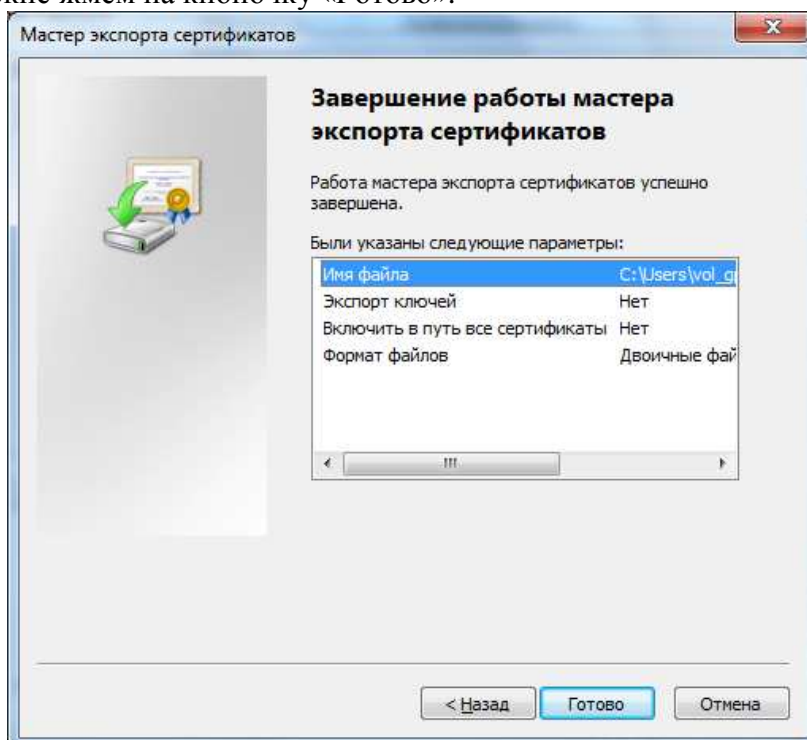


Рисунок 7.22 – Завершение Мастера экспорта сертификата

После нам сразу же должно выдаться сообщение об успешном экспорте сертификата.

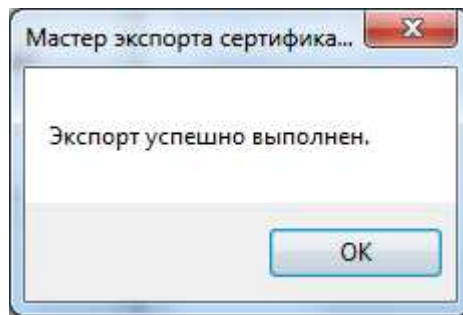


Рисунок 7.23 – Успешный экспорт сертификата

н) Далее двойным щелчком левой кнопки мыши открываем только что экспортированный сертификат.



Рисунок 7.24 – Установка корневого сертификата

о) Начинаем процедуру импорт, теперь уже корневого сертификата. Двойным щелчком щелкаем по сертификату и ждем на кнопку «Установить сертификат» (пункт в) данного подраздела).

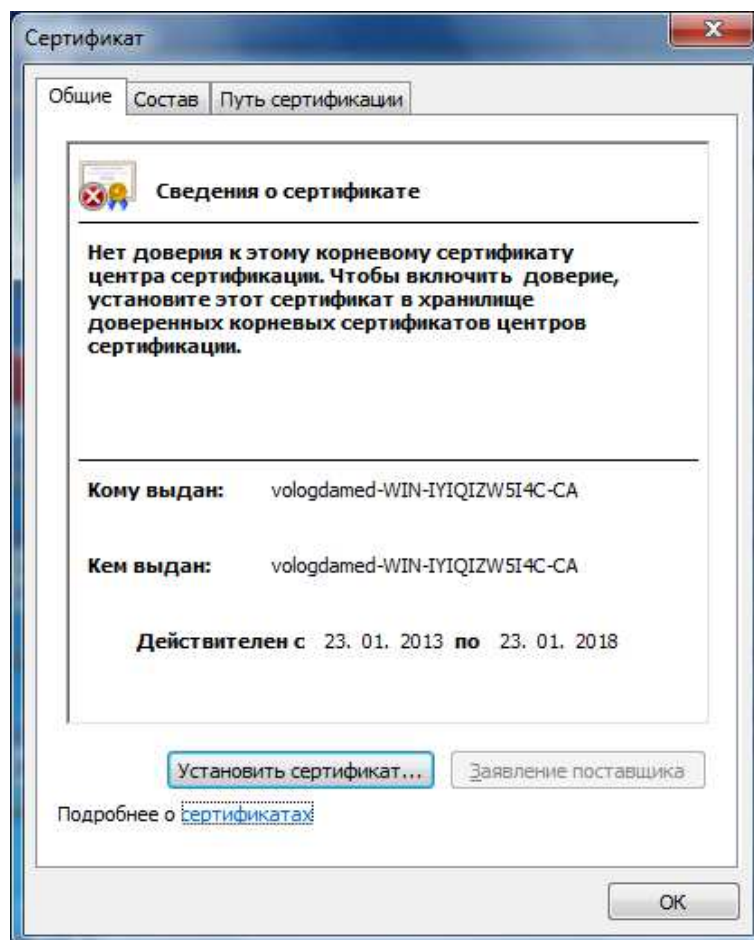


Рисунок 7.25 – Установка корневого сертификата

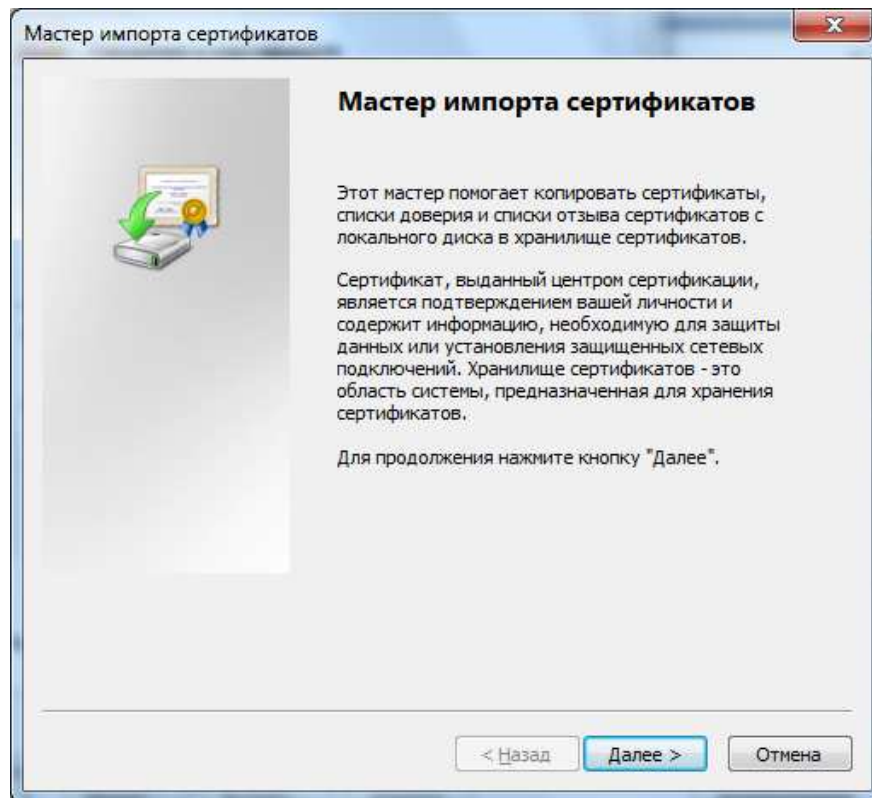


Рисунок 7.26 – Установка корневого сертификата

В открывшемся окне жмем на кнопку «Далее».

п) В следующем окне ставим галочку на пункте «Поместить все сертификаты в следующее хранилище» и жмем на кнопочку «Обзор».

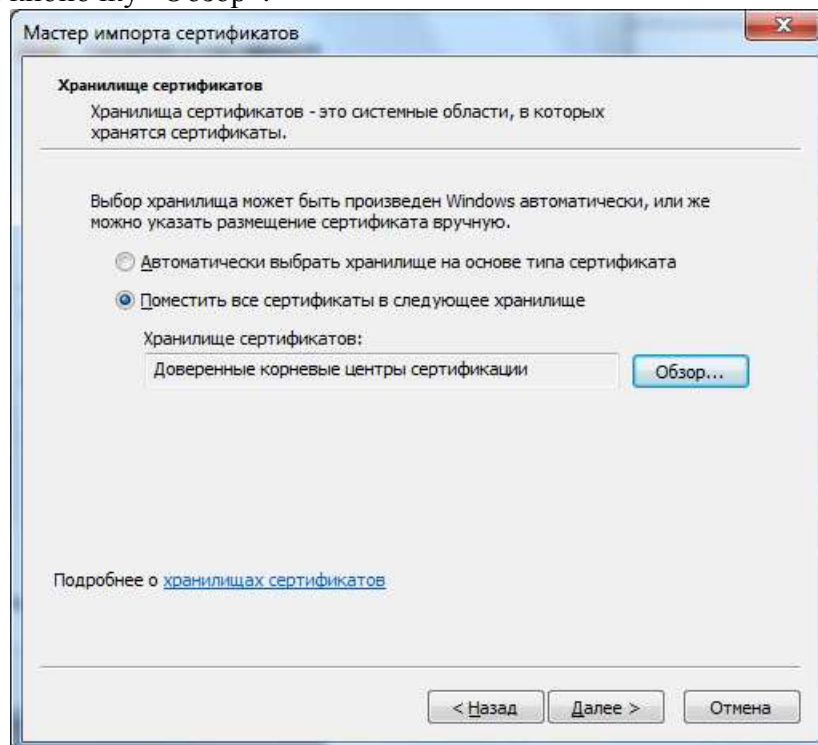


Рисунок 7.27 – Выбор хранилища сертификатов

р) В открывшемся диалоговом окне нужно выбрать «Доверенные корневые центры сертификации».

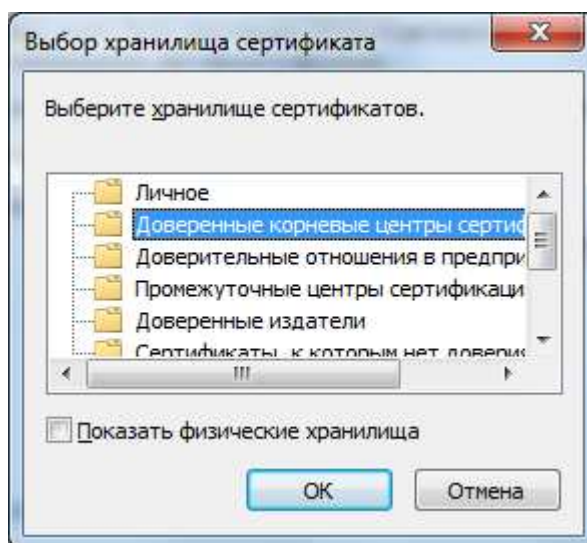


Рисунок 7.28 – Выбор хранилища сертификатов

Жмем здесь кнопку «ОК», а в окне «Мастер импорта сертификатов» проверяем поле «Хранилище сертификатов» (рис. 7.11) и, если все соответствует нашему выбору, жмем кнопку «Далее».

с) В открывшемся окне жмем кнопку «Готово».

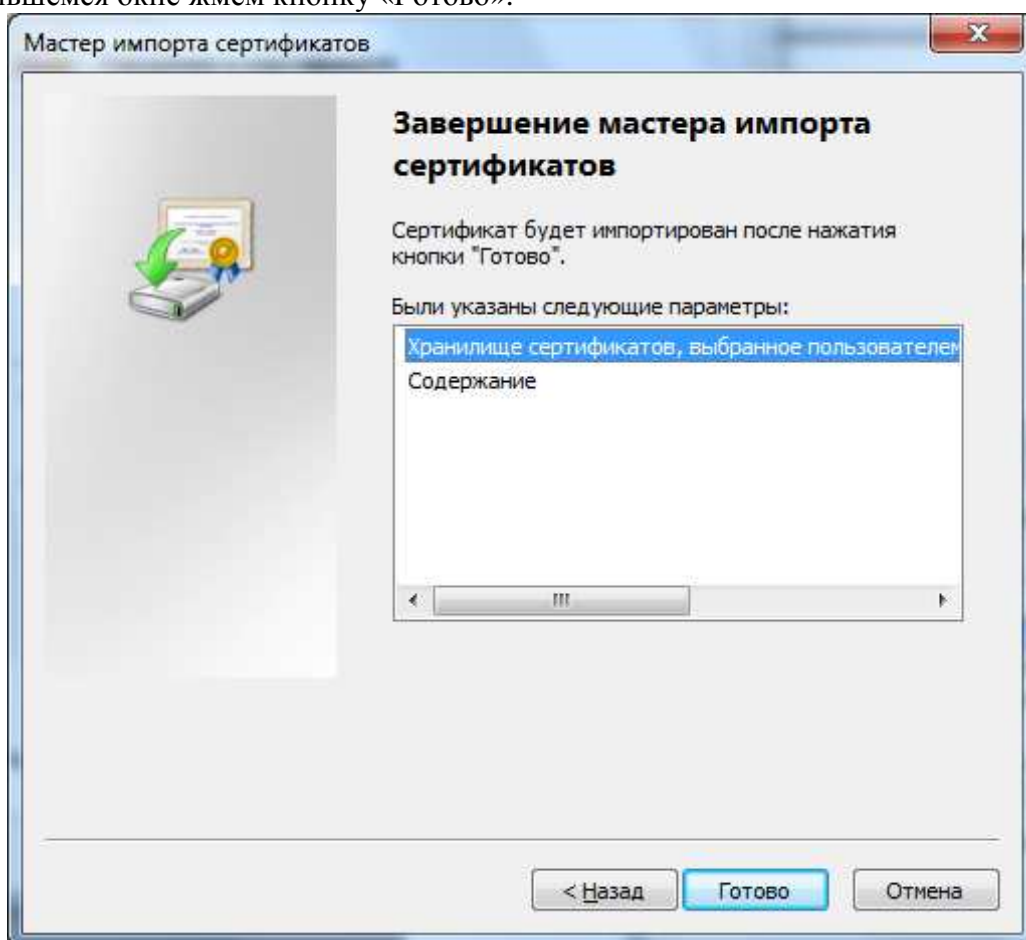


Рисунок 7.29 – Завершение работы Мастера импорта сертификатов

т) В некоторых случаях может выскочить следующее предупреждение о безопасности.

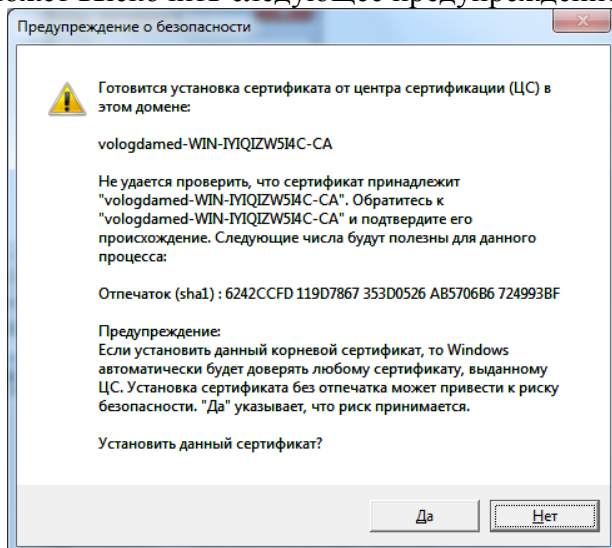


Рисунок 7.30 – Предупреждение о безопасности

Жмем на кнопочку Да и видим сообщение об успешном импорте сертификата.

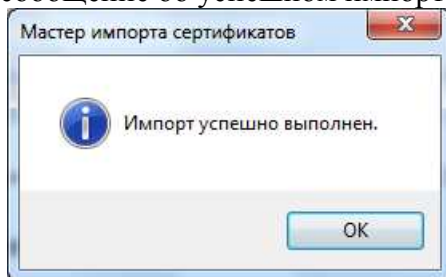


Рисунок 7.31 – Успешный импорт корневого сертификата

у) Проверим корректность установки сертификатов. Запускаем снова сертификат, который был получен из ЦОД (также см рис. 7.1). Сначала на вкладке «Общие».

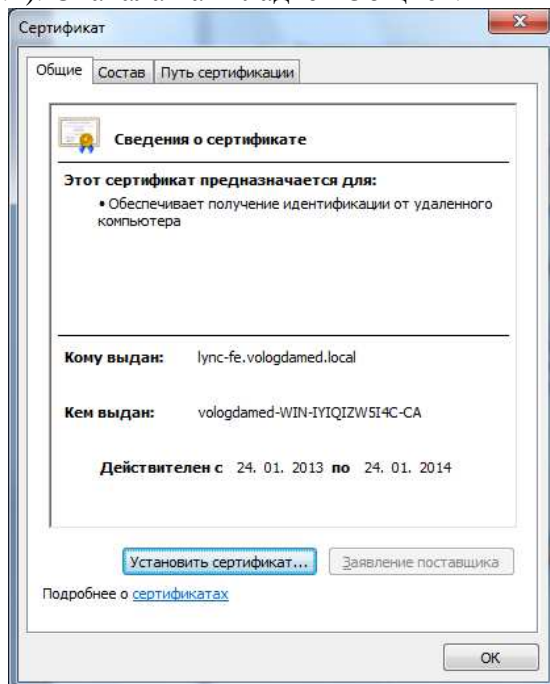


Рисунок 7.32 – Проверка сертификата

Затем переходим на вкладку «Путь сертификации» и видим, что никаких крестиков и знаков восклицания нет.

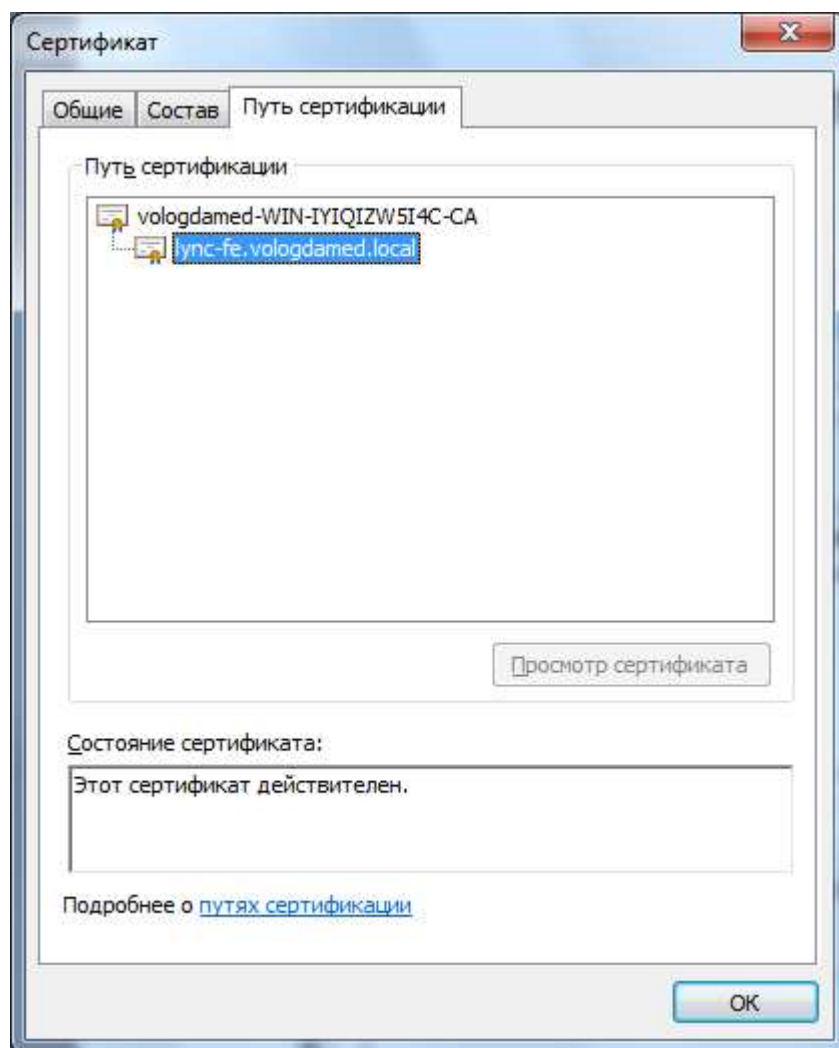


Рисунок 7.33 – Проверка сертификата

Если все так, то с чистой совестью снова переходим на раздел 8 и пытаемся зайти в Lync.

Не забываем также отправить тысячи лучей благодарности и счастья, за обнаружение данного глюка с установкой сертификатов и подготовку подраздела 7.2 данной инструкции, системному администратору из Вологодской Поликлиники №3 Сергею!

8. Подключение к конференции

Вообще после установки MS Lync должен загрузиться автоматически.

Если этого не произошло, нужно сделать следующее.

а) Найти MS Lync в установленных программах и запустить его

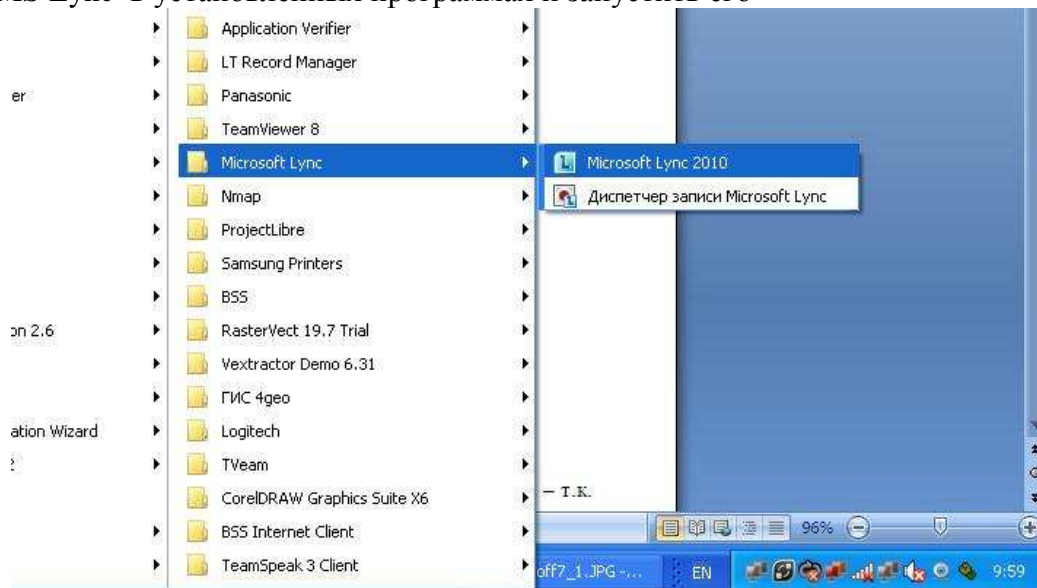


Рисунок 8.1 – Запуск MS Lync

б) Далее Lync загрузится и попытается подключиться к серверу, скорее всего у него это не получится сделать и будет выдано такое сообщение:

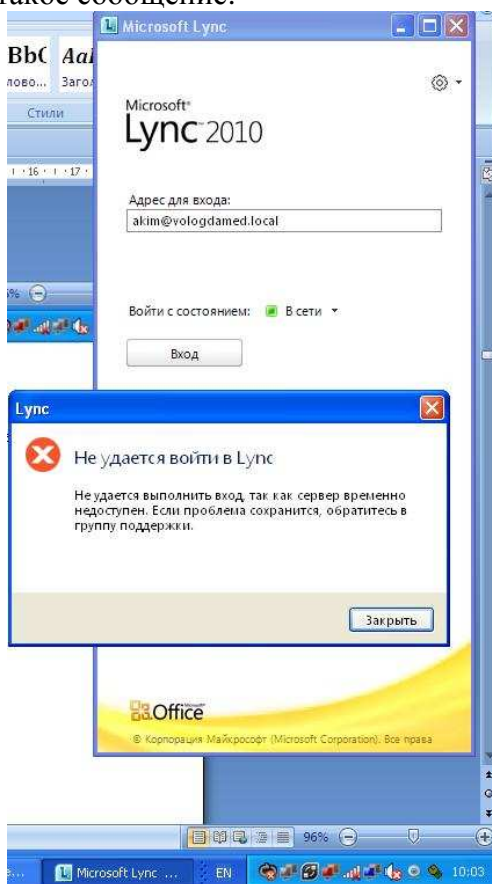


Рисунок 8.2 – Вход в MS Lync

Сообщение об ошибке может быть другим. Не обращаем на него внимание и закрываем его. Далее ждем на «шестеренку», располагающуюся в правом верхнем углу.

в) Настройка доступа к серверу конференций

После нажатия на «шестеренку» откроется окно параметров клиента. В нем надо перейти в раздел «Личные» (в меню слева).

Здесь указан адрес для входа. Он должен быть в следующем формате:

[Выданное имя пользователя@vologdamed.local](mailto:m.saltaev@vologdamed.local)

Если Вы видите что-то другое, то нужно внести изменения в эту строчку.

Затем нажимаем на кнопку Дополнительно, располагающуюся справа.

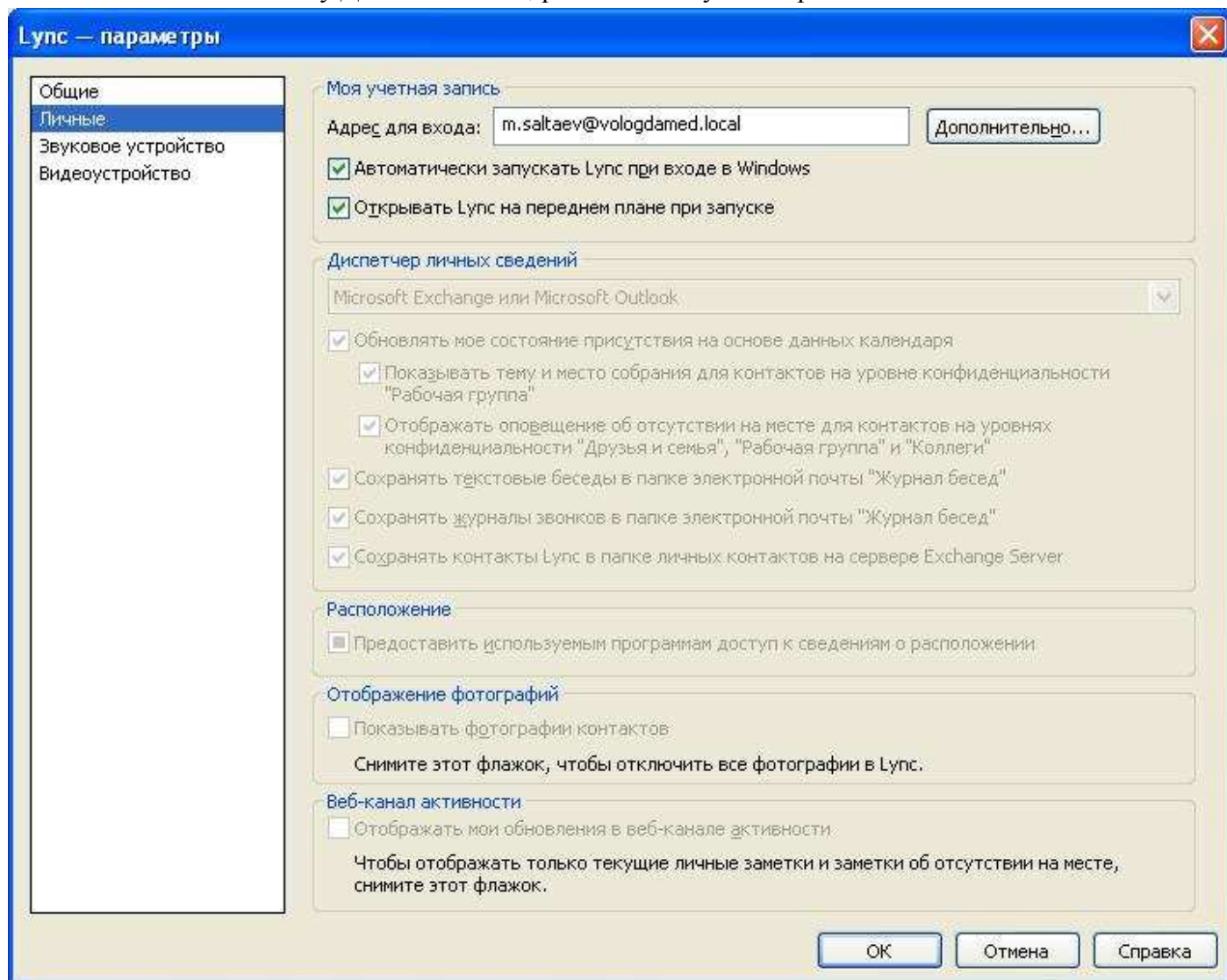


Рисунок 8.3 – Настройка параметров Lync

г) Настройка серверов видеоконференцсвязи

После нажатия на кнопку «Дополнительно» отобразится окно «Дополнительные параметры подключения»

Здесь нужно выбрать параметр «Настроить вручную» и ввести параметры, которые указаны на рисунку 8.4 ниже.

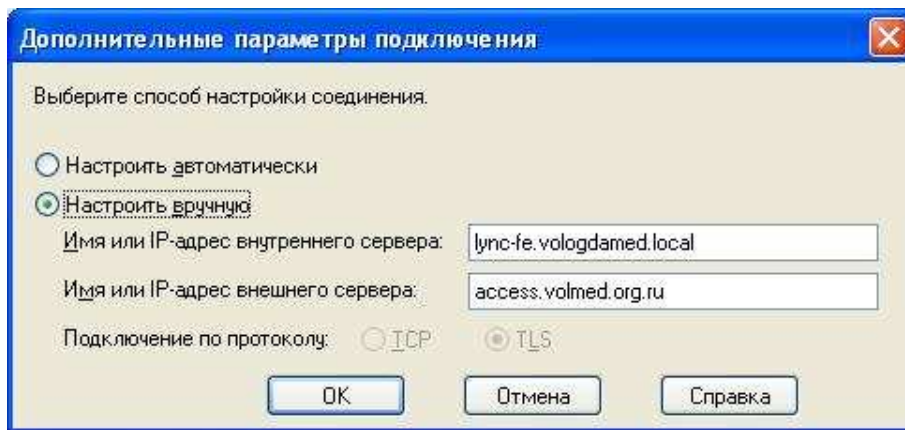


Рисунок 8.4 – Параметры подключения к серверам видеоконференцсвязи

После этого везде нажимаем ОК.

д) Вход в систему видеоконференцсвязи

После этого завершающий этап – вход в систему.

Для этого достаточно нажать на кнопку «Вход» в основном окне клиента.



Рисунок 8.5 – Вход в систему

Просьба обратить внимание на поля «Адрес для входа:» и «Войти с состоянием». В поле «Адрес для входа» должно стоять тоже самое значение, что вводилось в подпункте «в» данного параграфа.

В поле «Войти с состоянием» должно стоять значение «В сети».

е) При первоначальном входе в систему окно MS Lync изменится и появятся дополнительные параметры входа:

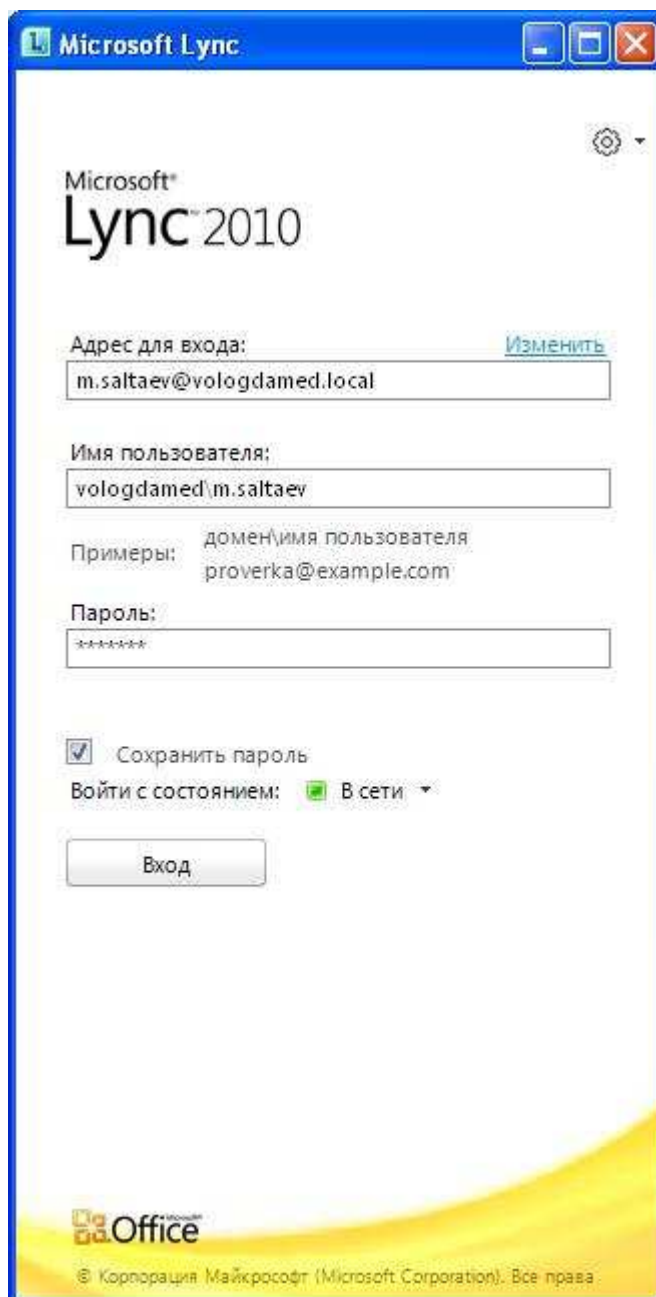


Рисунок 8.6 – Вход в систему

Заполняем вновь появившиеся поля следующим образом:

Имя пользователя: имя_домена\выданное_имя_пользователя

Пароль: выданный пароль

Жмем кнопку «Вход».

ж) Если все ввели правильно, то окно MS Lync будет выглядеть следующим образом:

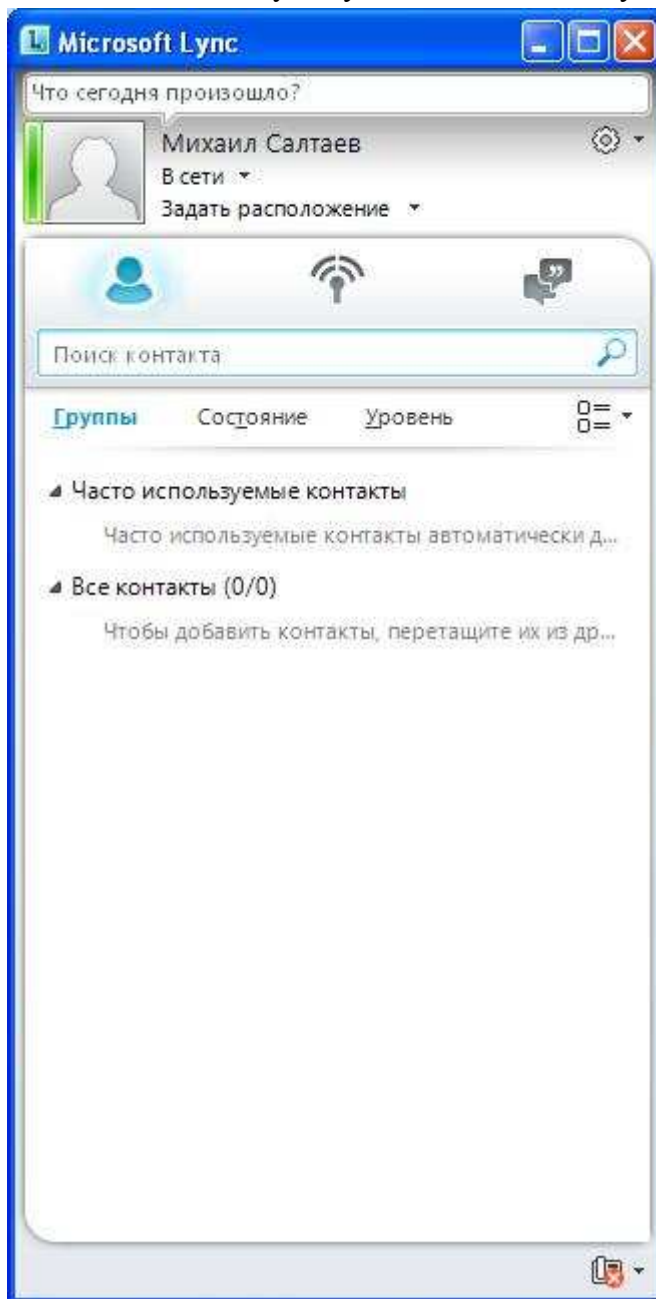


Рисунок 8.7 – Окно авторизованного пользователя в MS Lync

Далее, после авторизации, Вам нужно будет ожидать приглашение в конференцию, которое будет выглядеть в форме звонка (по аналогии, как в Skype).

В дальнейшем, в случае необходимости, мы сделаем дополнительную инструкцию по основным моментам работы с клиентом MS Lync.