Практическая работа №5.

Цель работы: научится выдавать самоподписанные сертификаты с помощью OpenSSL.

Ход работы:

Шаг 1. Проверка сетевой связности.

1. На виртуальной машине сервера подключили второй адаптер, переведя его в режим NAT. Первый адаптер оставьте включенным, проверили, что в неразборчивом режиме стоит пункт «Разрешить всё».

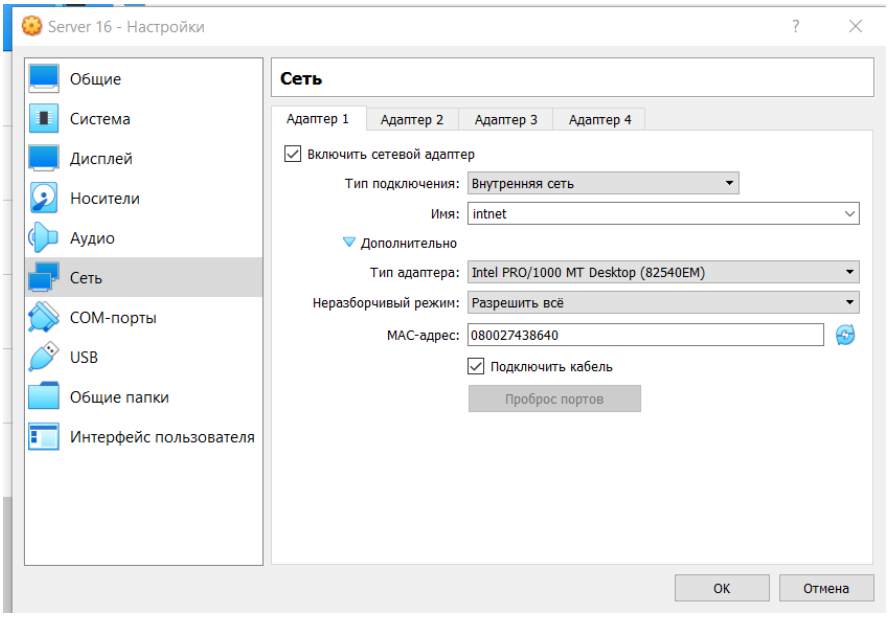

Рисунок 1 - Первый адаптер

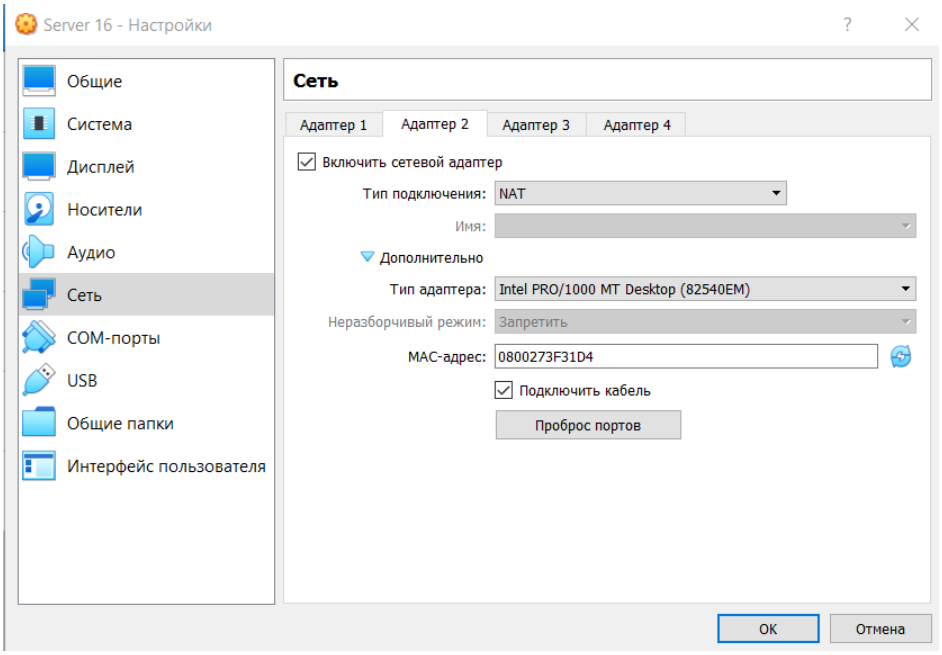

Рисунок 2 - Второй адаптер

2. В консоли отправили пинг-запрос на адрес 8.8.8.8 (DNS-сервер Google), ответ получен успешно.

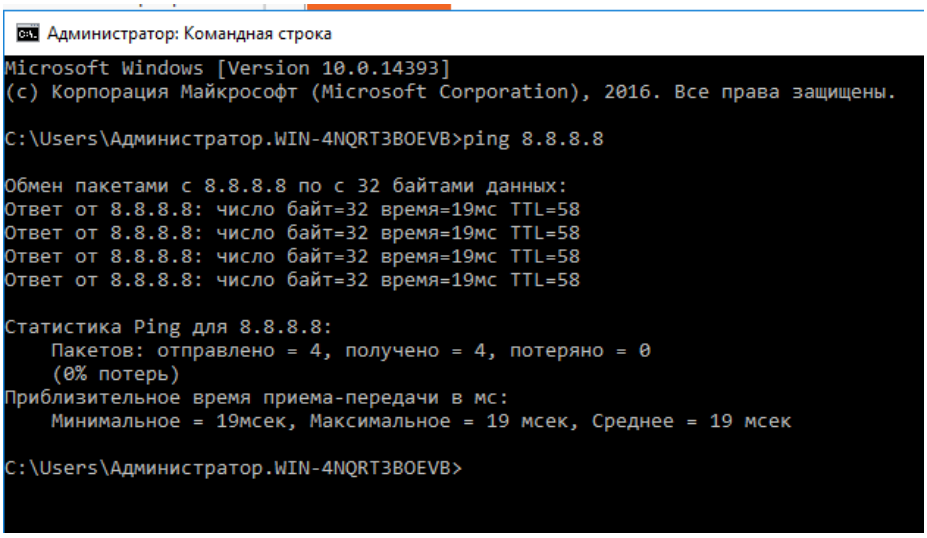

Рисунок 3 - Успешный пинг

Шаг 2. Установка OpenSSL.

3. Убедились, что отключены все параметры усиленной защиты Internet Explorer. Перейдите на сайт https://slproweb.com/products/Win32OpenSSL.html), где нужно скачать любую подходящую версию в сборке Light для разрядности системы. Скачали и запустили установщик OpenSSL.

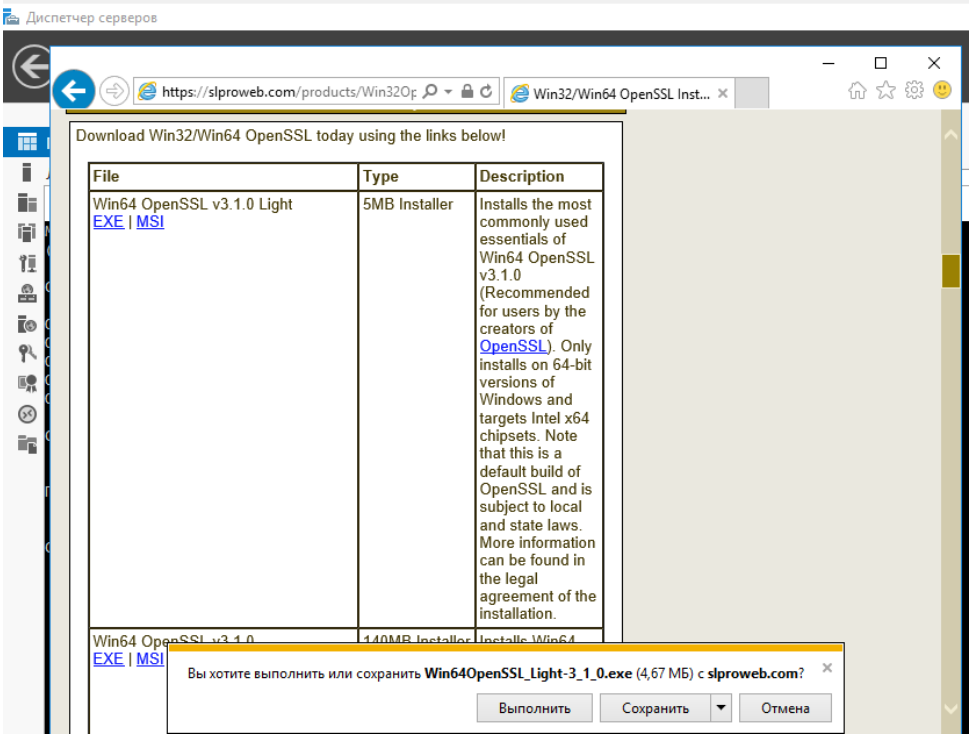

Рисунок 4 - Нужная версия OpenSSL

4. Для работы OpenSSL так же необходим компонент Microsoft Visual C++ 2019, согласились с установкой компонента, весь процесс будет идти через браузер.

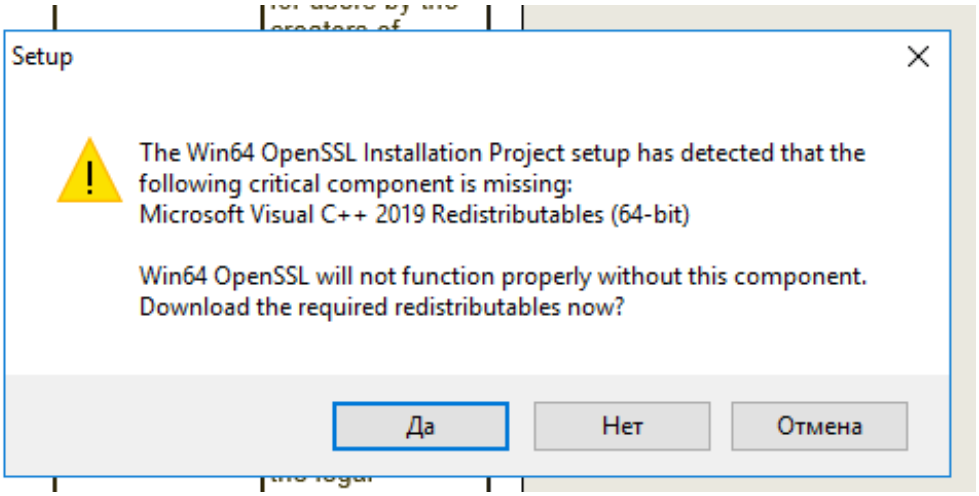

Рисунок 5 - Окно предупреждения

5. В ожидании скачивания компонента установили OpenSSL, где от нас зависит только один параметр: место копирования DLL, выбирали системную директорию ОС.

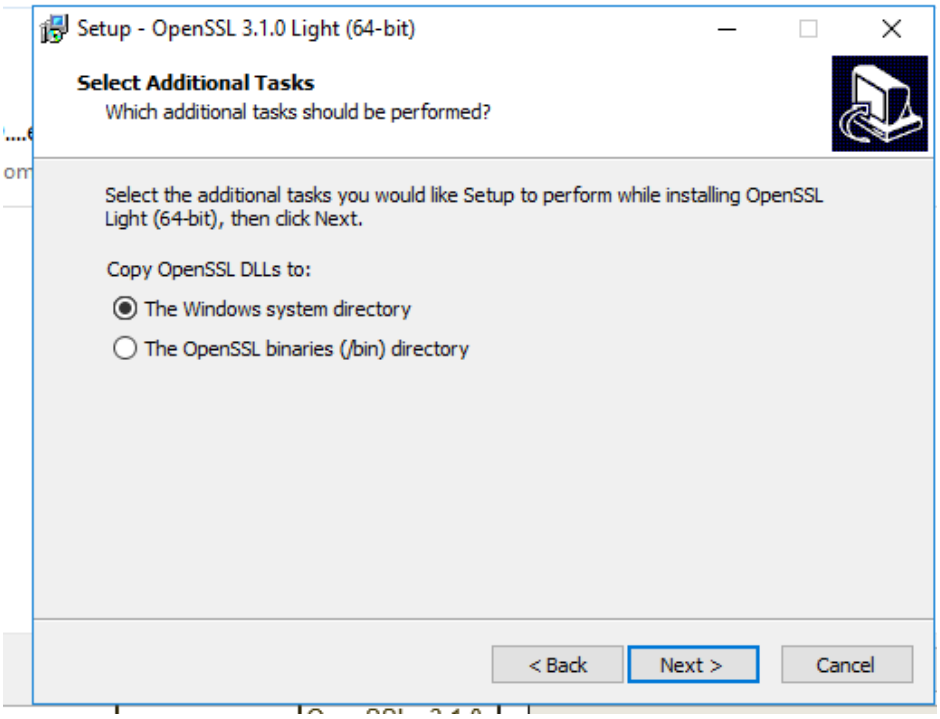

Рисунок 6 - Выбор копирования

6. По окончанию установки компонента дождались сообщения об успешном завершении и закрыли окно.

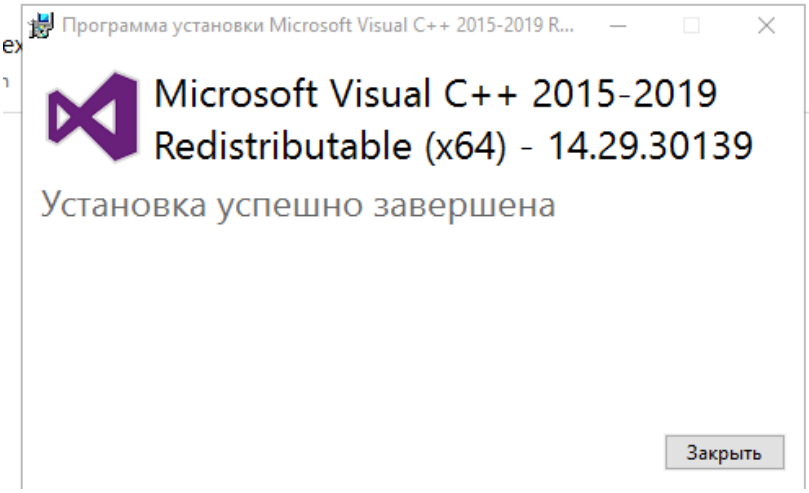

Рисунок 7 - Успешная установка MV C++

7. Далее, на диске С создали папку, в которой будем помещать сертификаты. На всякий случай, дали полный доступ системе и администратору, открыли общий доступ по сетевому пути.

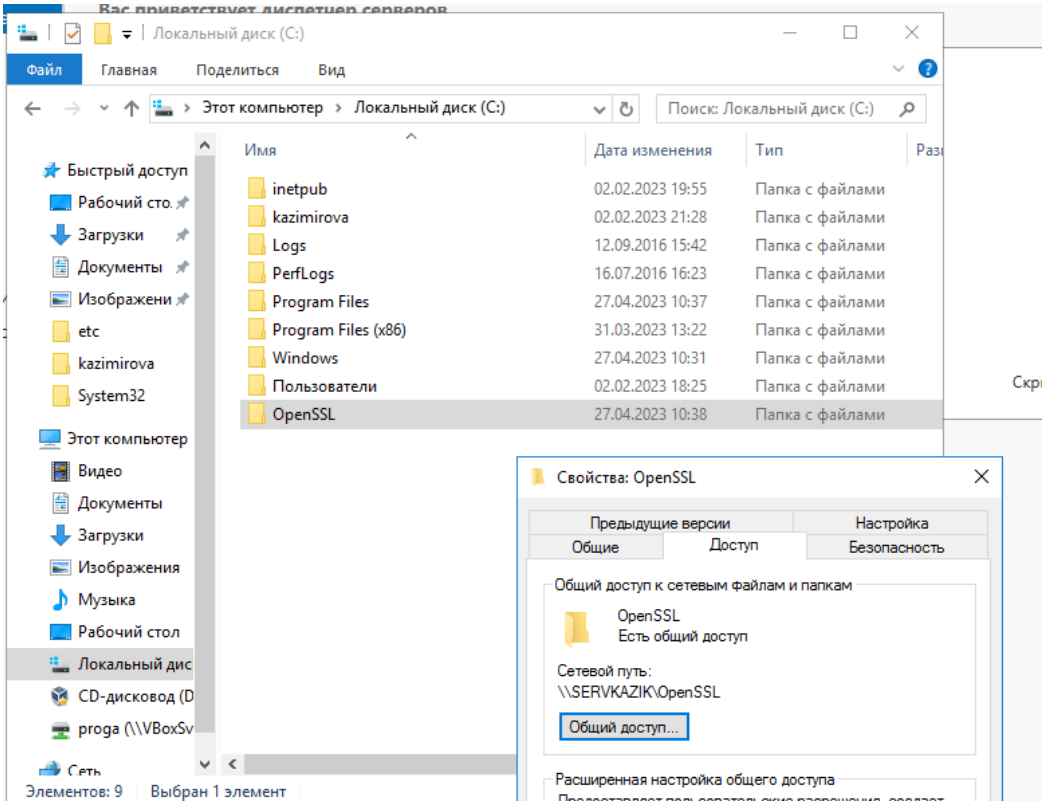

Рисунок 8 - Создание папки

8. Запускаем командную строку для OpenSSL.

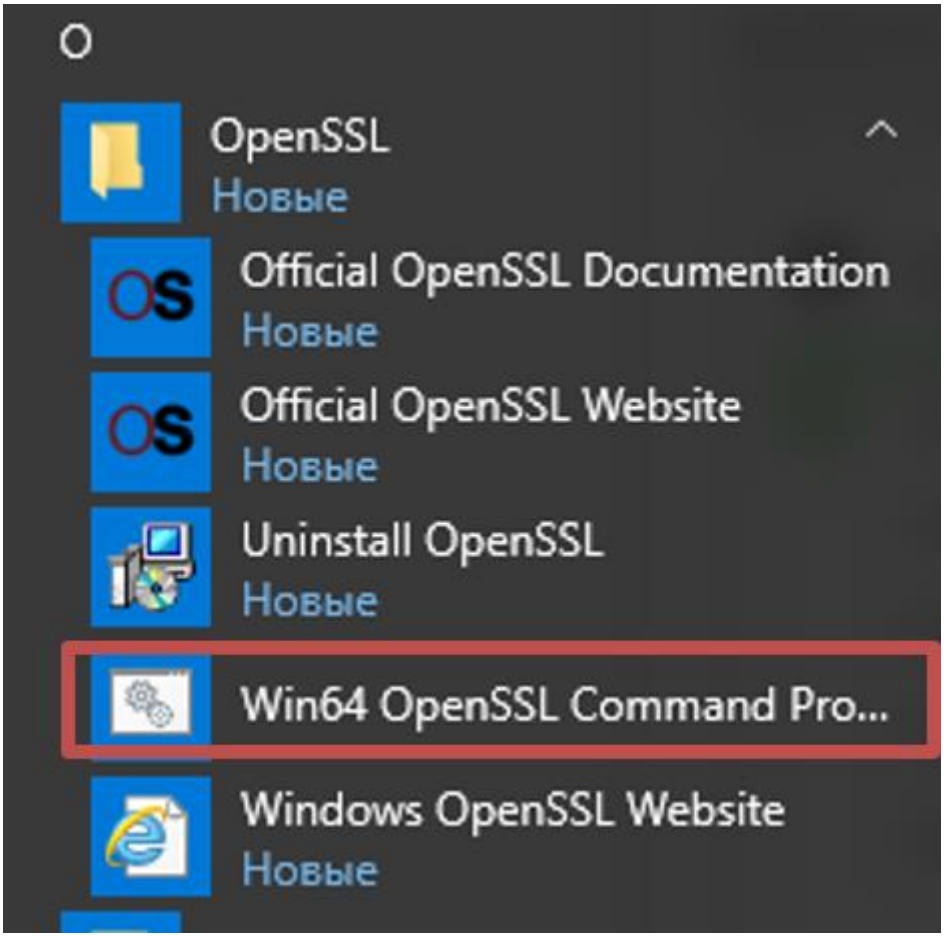

Рисунок 9 - Командная строка openssl

Шаг 3. Создание ключей и выдача сертификата.

9. В консоли перешли в созданную папку.

```
C:\Users\Администратор.WIN-4NQRT3BOEVB>cd /d c:\OpenSSL
```

Рисунок 10 - Переход в папку

10. Прописываем команду, в которой создаем новый ключ с указанной длинной.

```
c:\OpenSSL>openssl genrsa -out server.key 2048

c:\OpenSSL>
```

Рисунок 11 - создание ключа

11. Далее, создали шаблон запроса и сертификата. Отличие шаблона запроса от сертификата в том, что для сертификата в команде мы указываем ключ -x509, который говорит о создании само подписанного сертификата и ключ -days, где в днях можно обозначить срок действия.

```
c:\OpenSSL>openssl req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MPT_kazimirova
Organizational Unit Name (eg, section) []:MPT_site7
Common Name (e.g. server FQDN or YOUR name) []:Kazimirova.A.D
Email Address []:bi50_a.v.kazimirova@mpt.ru

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Kazik1964
An optional company name []:MPT_kazimirova

c:\OpenSSL>
```

Рисунок 12 - Создание шаблона запроса

```
c:\OpenSSL>openssl req -new -x509 -days 365 -key server.key -out server.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MPT_kazimirova
Organizational Unit Name (eg, section) []:MPT_site7
Common Name (e.g. server FQDN or YOUR name) []:Kazimirova.A.D
Email Address []:bi50_a.v.kazimirova@mpt.ru

c:\OpenSSL>
```

Рисунок 13 - Создание сертификата

12. Для повышения уровня безопасности сертификата, назначили пароль на импорт\экспорт.

```
c:\OpenSSL>openssl pkcs12 -inkey server.key -in server.crt -export -out server.pfx
Enter Export Password:
Verifying - Enter Export Password:

c:\OpenSSL>
```

Рисунок 14 - Назначение пароля

13. Теперь, прописали в «Выполнить» mmc.exe для того, чтобы открыть оснастку сертификатов.

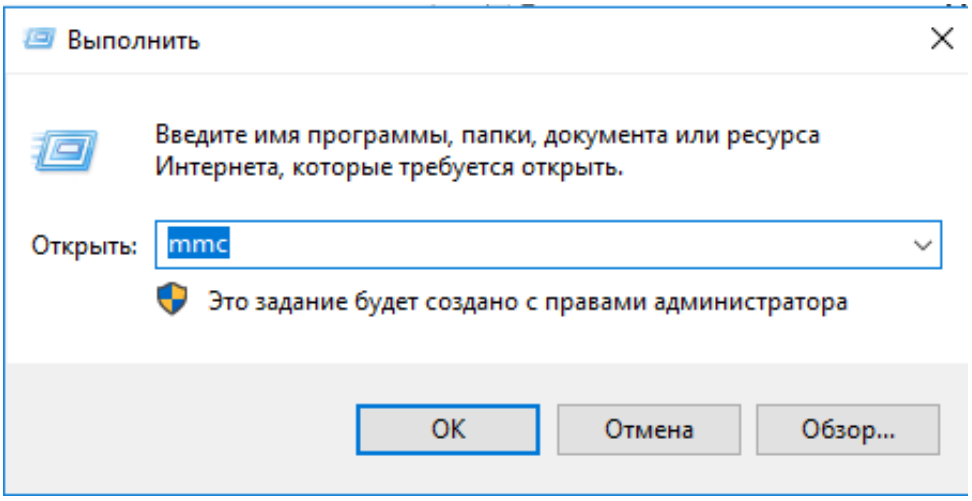

Рисунок 15 - Открытие консоли

14. В консоли выбрали добавление оснасток, там нашли «Сертификаты» с параметрами «локальный компьютер», добавляем и сохраняем.

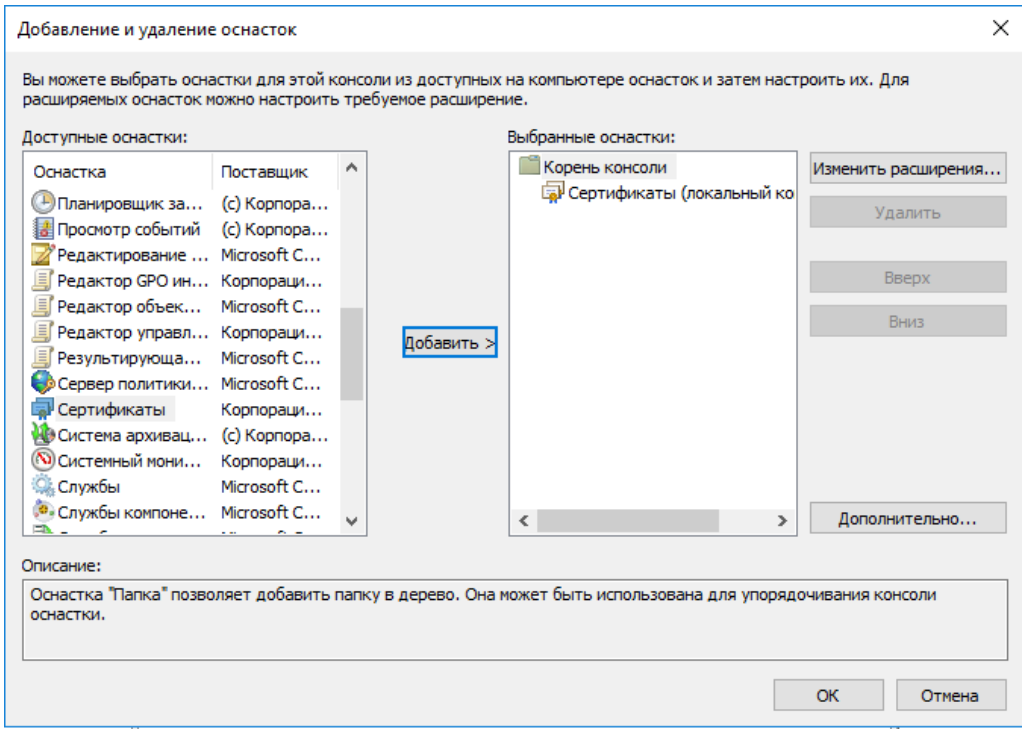

Рисунок 16 - Добавление оснастки

15.В оснастке нашли «Доверенные корневые центры сертификации» → Все задачи → Импорт.

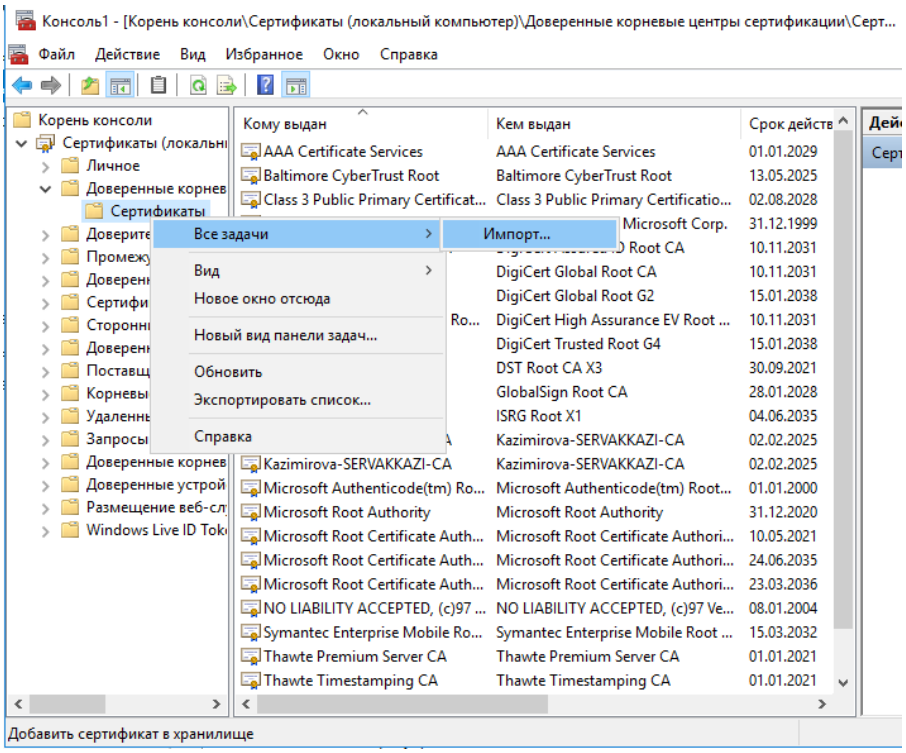

Рисунок 17 - Импорт сертификата

16.Выбрали по пути в папке созданный нами сертификат и добавили.

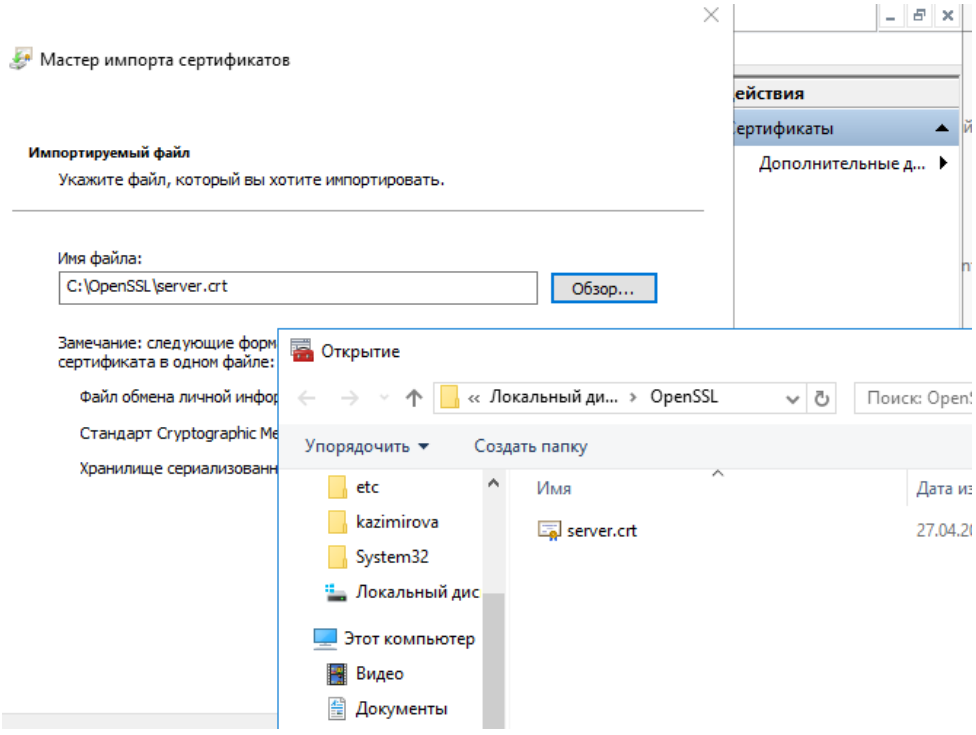

Рисунок 18 - Выбор пути до сертификата

17.В результате завершения в окне отобразился путь до файла с сертификатом, и высветилась информация об успешном импорте.

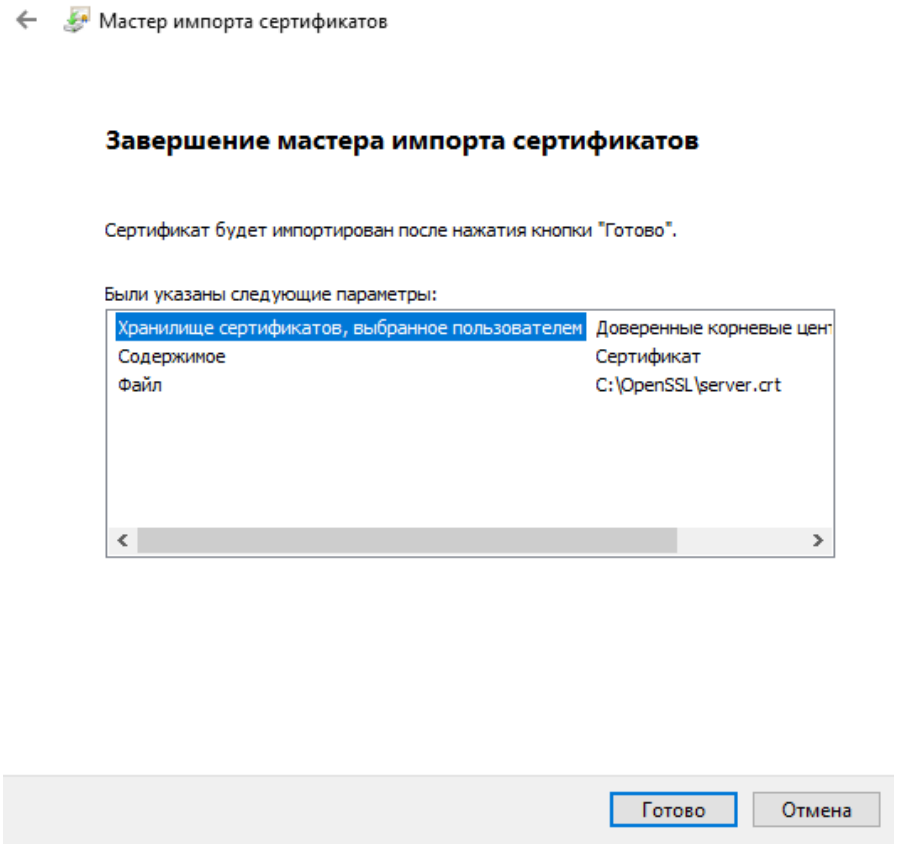

Рисунок 19 - Итог для мастера импорта сертификатов

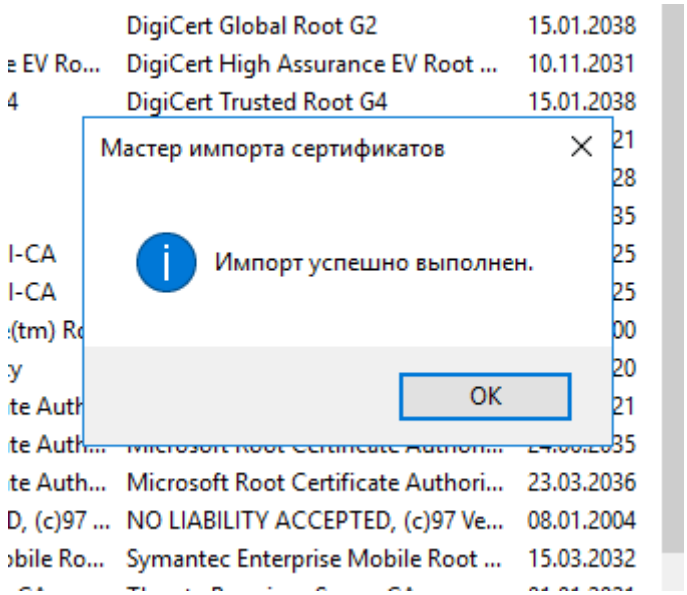

Рисунок 20 - Успешный импорт

Шаг 4. Выдача сертификата IIS-серверу.

18. На IIS-сервере в начальной странице нашли параметр «Сертификаты сервера».

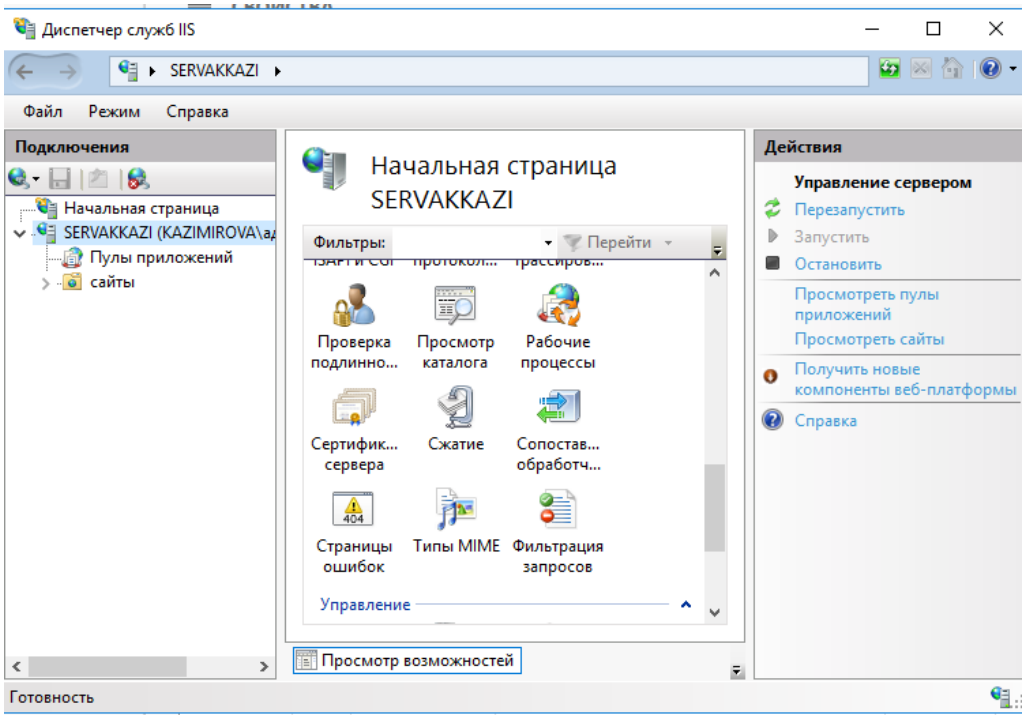

Рисунок 21 - Сертификаты сервера

19. Там выбрали пункт «Импорт сертификата», указали путь до него в папке, и ввели пароль, который ранее мы написали для импорта\экспорта. Хранилище указали как «Размещение веб-служб» .

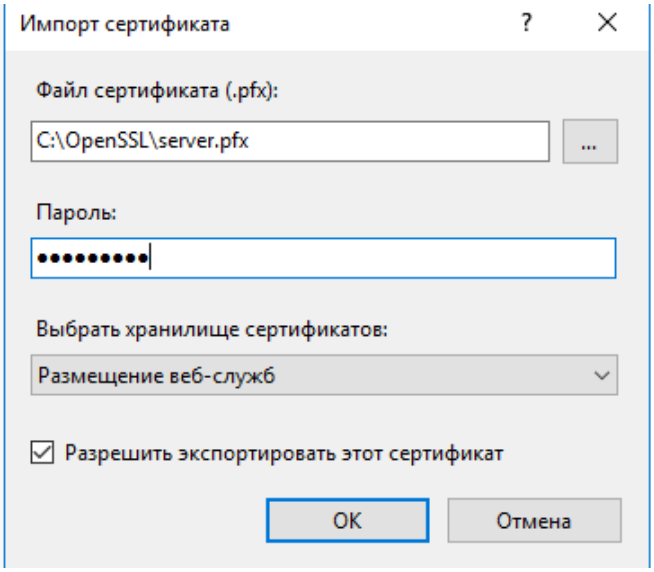

Рисунок 22 - Импорт сертификата

20. Перешли к созданию веб-страницы. Добавили веб-сайт с индивидуальным именем сайта и узла, указываем физический путь до каталога, через кнопку «Подкл. как», где вводим данные Администратора. После этого нажимаем «Тест настроек», и там мы наблюдали две зеленые галочки. В привязке указываем https и в списке сертификатов ищем тот, который создали и выдали себе ранее.

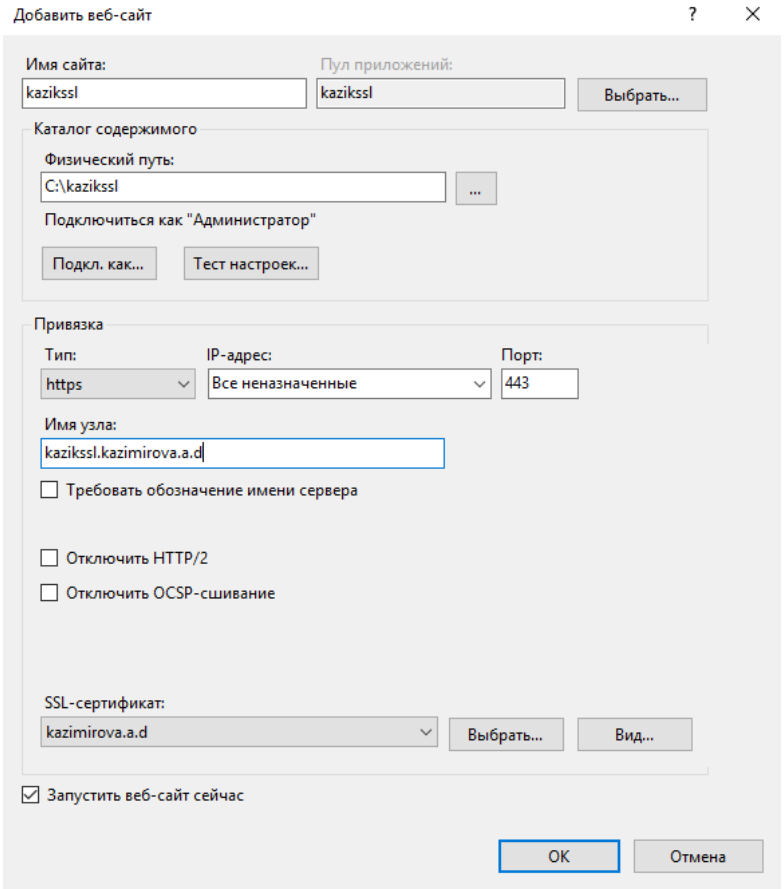

Рисунок 23 - Форма создания веб-сайта

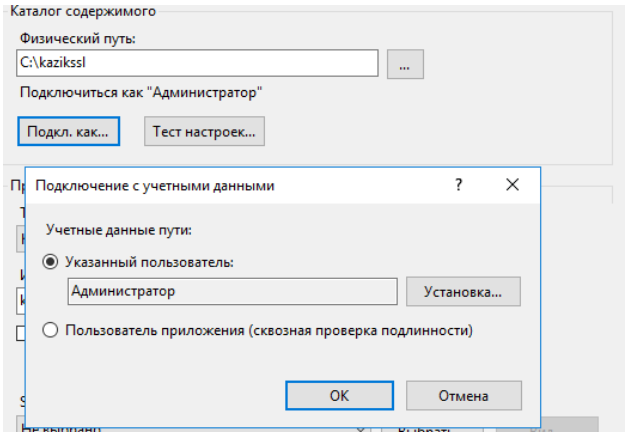

Рисунок 24 - Путь и учётные данные администратора

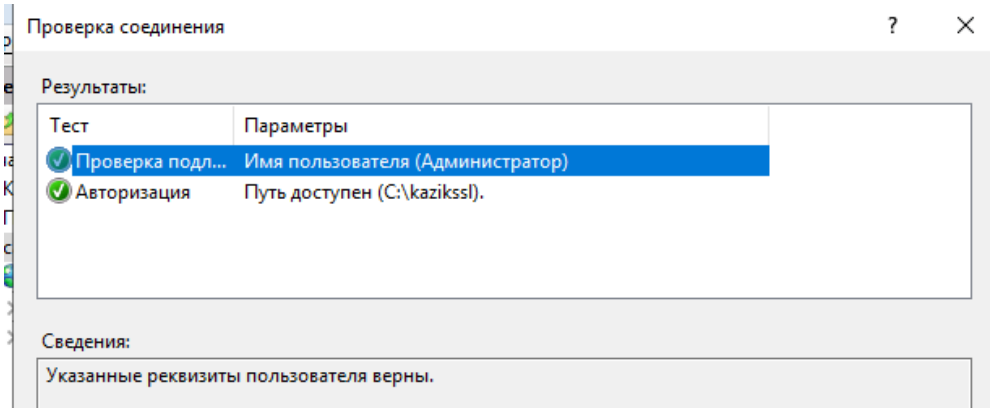

Рисунок 25 -Успешная проверка соединения

21. На всякий случай, выдали папке с сайтом права доступа для группы IIS_IUSRS на полный доступ.

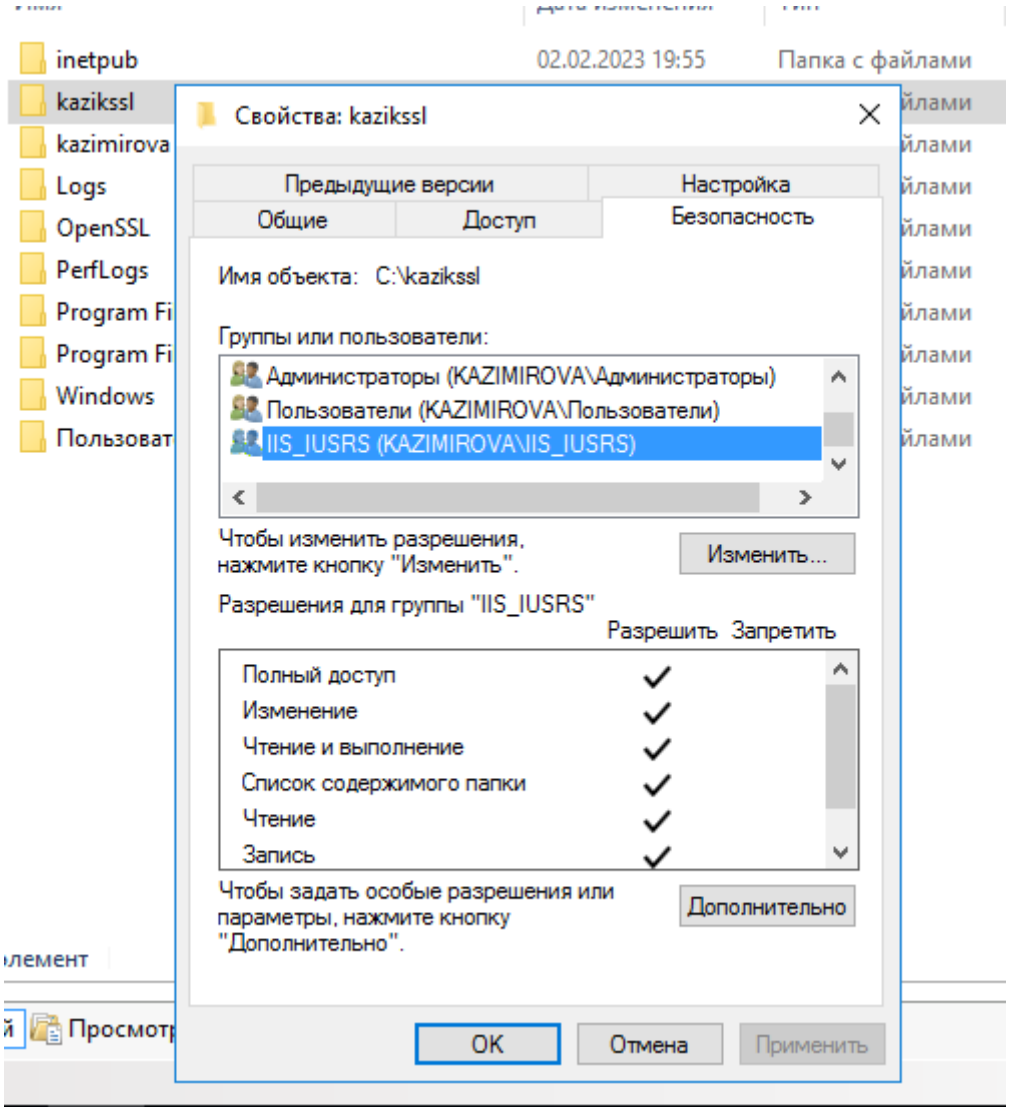

Рисунок 26 - Выдача полных прав

22. В параметрах для сайта нашли параметр «Просмотр каталога» и включили его в правом меню.

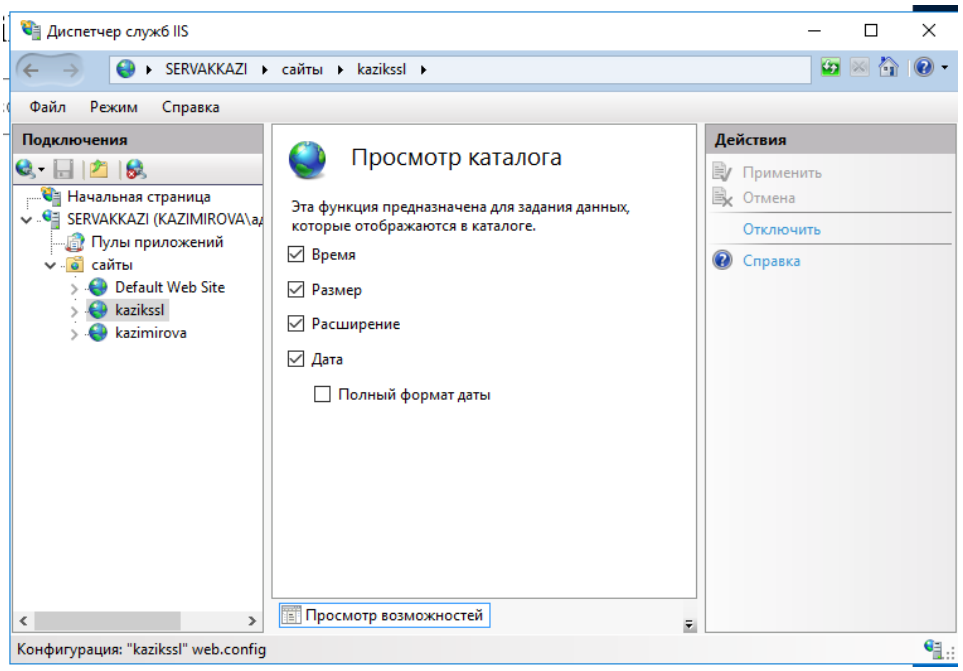

Рисунок 27 - Включение каталога

23. Для того, чтобы сайт был доступен по доменному имени внутри домена, сделали новую запись в DNS в зонах как прямого, так и обратного просмотра.

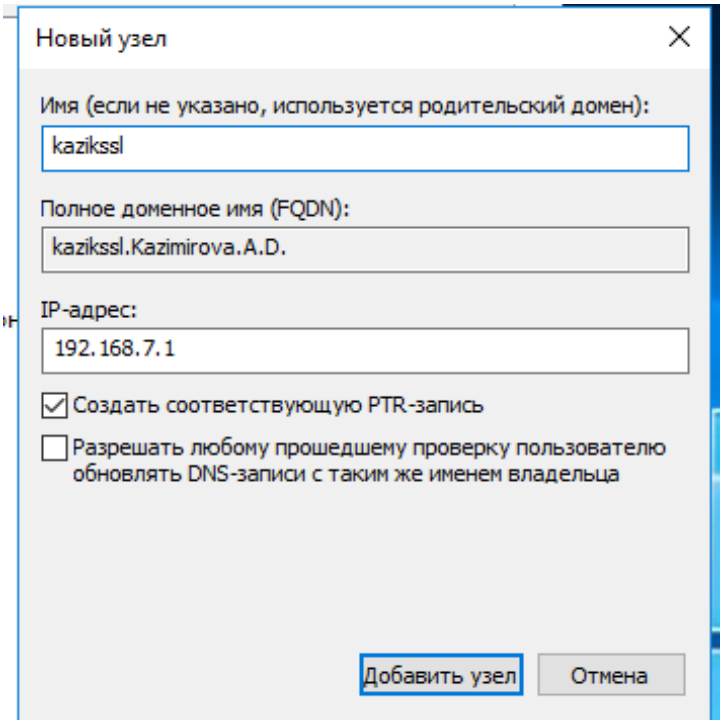

Рисунок 28 - Новая запись узла в прямой зоне

Шаг 5. Проверка работоспособности.

24. Перешли в браузер, ввели доменное имя нашего сайта через https, где нас встретило уведомление о том, что веб-сайт не защищен. Выбрали «Перейти на веб-страницу».

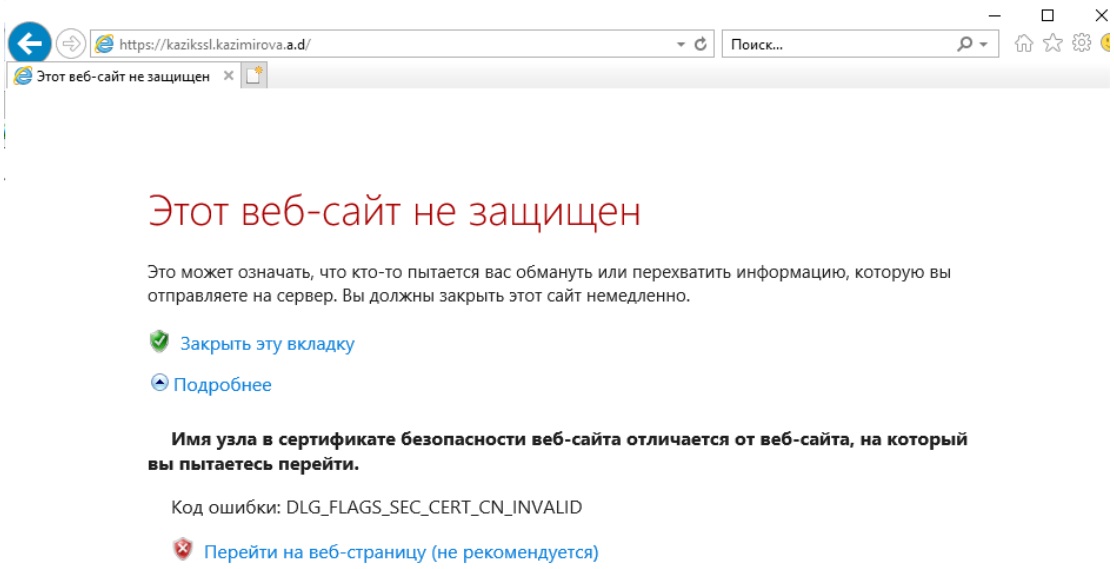

Рисунок 29 - Уведомление о том, что сайт не защищен

25. У меня нет файла index.html, поэтому в моем случае открылась корневая директория. Но вверху видно, что имеется ошибка наличия сертификата – он не является доверенным для системы, что и сопутствует само подписанному сертификату.

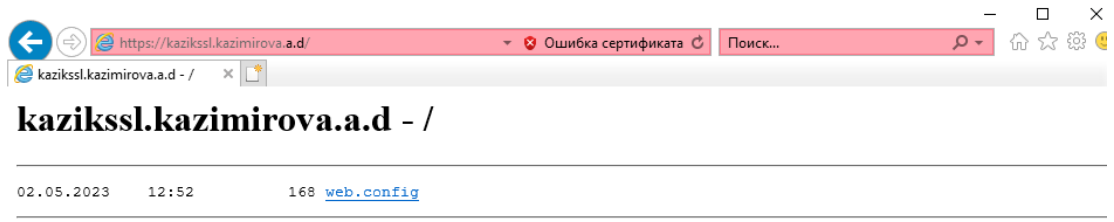

Рисунок 30 - Успешный вход на страницу

26. Теперь, зашли на клиентскую машину, открыли браузер, ввели доменное имя страницы, открываем ее, просматриваем свойства сертификатов → «Издатель». Данный скриншот, должен завершать вашу работу: вы демонстрируете, что сертификат действителен внутри домена, сайт доступен по доменному имени внутри сети.

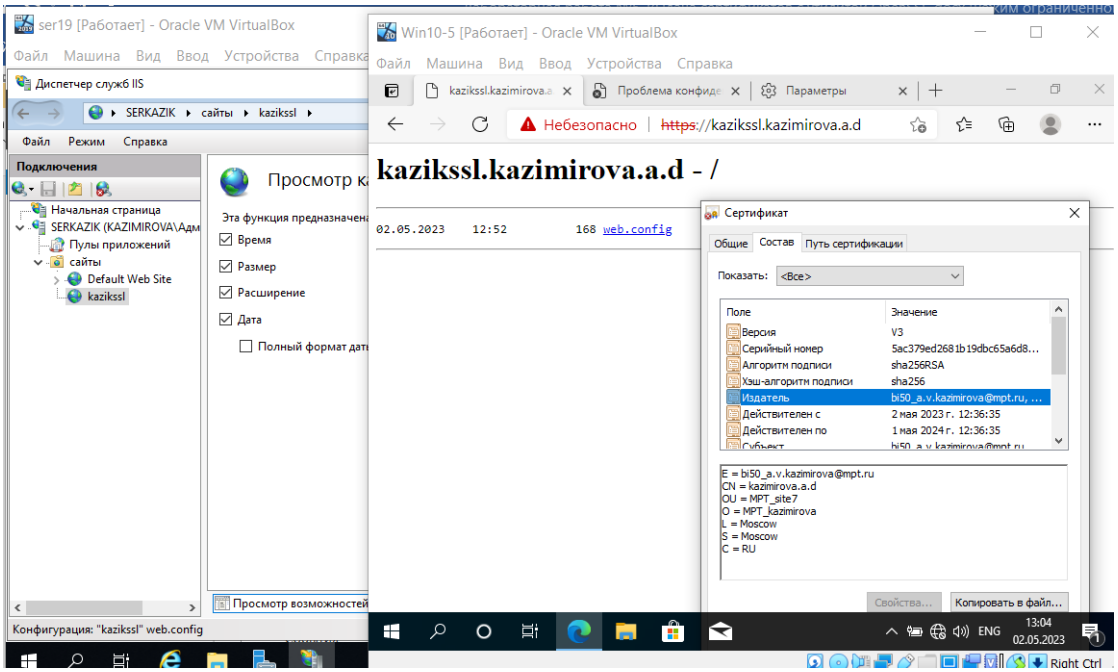

Рисунок 31 - Успешное подключение с клиента

Вывод: в процессе выполнения практической работы был освоен навык выдачи самоподписанных сертификатов с помощью утилиты OpenSSL.