Лабораторная работа № 7

«SSL – сертификат»

Цель работы

Ознакомиться с понятием и предназначением SSL – сертификата и создать его.

Задачи

1. Запустить прилагаемое к методичке приложение;
2. Удостовериться, что подключение небезопасно;
3. Включить службы IIS;
4. Сгенерировать новый SSL сертификат для localhost;
5. Привязать сертификат к серверу через диспетчер служб IIS;
6. Настроить IIS в качестве обратного прокси-сервера;
7. Провести проверку SSL - сертификата.

Необходимое ПО

* Node.js (если её нет, то установить актуальную версию с сайта: <https://nodejs.org/en/>)
* IIS (Internet Information Services)

Теория

SSL-сертификат – это цифровой сертификат, удостоверяющий подлинность веб-сайта и позволяющий использовать зашифрованное соединение. Аббревиатура SSL означает Secure Sockets Layer – протокол безопасности, создающий зашифрованное соединение между веб-сервером и веб-браузером.

Компаниям и организациям необходимо добавлять SSL-сертификаты на веб-сайты для защиты онлайн-транзакций и обеспечения конфиденциальности и безопасности клиентских данных.

SSL обеспечивает безопасность интернет-соединений и не позволяет злоумышленникам считывать или изменять информацию, передаваемую между двумя системами. Если в адресной строке рядом с веб-адресом отображается значок замка, значит этот веб-сайт защищен с помощью SSL

Так как современном мире защита данных имеет принципиальное значение. Поэтому внедрили HTTPS, который расшифровывается как протокол безопасного соединения. Принципом работы защищённого протокола HTTPS является обмен ключами шифрования. Прежде чем ответить на запрос от браузера, сервер предъявляет ключ — SSL-certificate. Браузер проверяет подлинность ключа в Центре сертификации. Если ключ «подошёл», браузер и сервер доверяют друг другу и договариваются о разовом шифре. Так происходит каждую сессию, то есть каждый раз при обмене запросами и ответами. Вот таким хитрым способом и обеспечивается сохранность данных и конфиденциальность при обмене информацией.

Чтобы сайт стал работать по протоколу безопасного соединения HТТPS, нужен SSL-сертификат. Это виртуальный документ, который содержит данные об организации, её владельце и подтверждает их существование. Позволяет узнать сервер и подтвердить безопасность сайта.

Использование сертификата безопасности для сайта гарантирует:

* Подлинность ресурса, к которому обращается пользователь. Это повышает у посетителей уровень доверия.
* Целостность передаваемой информации. При транспортировке от сервера к браузеру данные не изменятся и не потеряются.
* Конфиденциальность. 256-разрядное шифрование исключает доступ злоумышленников к информации.

SSL-сертификатов несколько видов. Во-первых, они отличаются по количеству доменов и субдоменов, для которых они могут использоваться. Во-вторых, по тому, как именно сайт будет проверяться, — тут есть три варианта:

Первый — DV (domain validation) SSL — подтверждает домен, а также шифрует и защищает данные при передаче с помощью протокола https. Установить его себе на сайт могут как физические лица, так и организации. Выпускается он, как правило, почти мгновенно (точно не дольше 3 часов), после чего на сайте появляется значок замочка (см. пункт 2) и сайт становится защищенным.

Второй — OV (organization validation) SSL — кроме защиты информации гарантируется принадлежность домена конкретной организации. Сертификат выдается только юридическим лицам с подтвержденным номером телефона (перед его выпуском в организацию звонят). На сайте с таким сертификатом пользователь может найти информацию об организации — владельце сайта, обычно просто щелкнув по иконке замка. Выпускается он в течение 3 дней.

Третий — EV (extended validation) — то же, что и OV, только проверяется уже и налоговая, и коммерческая деятельность компании, причем более детально. На сайте рядом с URL появляется название компании. Выпускается в течение 5 дней.

Самый простой способ узнать, есть ли у сайта SSL-сертификат – обратить внимание на следующие элементы в адресной строке браузера:

* Если веб-адрес начинается с HTTPS, а не с HTTP, значит он защищен с помощью SSL-сертификата.
* Для защищенных сайтов отображается значок закрытого замка, который можно щелкнуть и посмотреть сведения о безопасности. У самых надежных сайтов будут зеленые замки или адресные строки.
* Браузеры также показывают предупреждения, если соединение небезопасно, например красный замок, открытый замок, линию, пересекающую адрес веб-сайта, треугольник-предупреждение над значком замка.

Что дает SSL-сертификат для сайта кроме защиты данных? SSL-сертификат помогает в SEO-продвижении проекта — позволяет занять более высокую позицию в поисковой выдаче. Поисковые системы (Google, Яндекс и пр.) дорожат доверием аудитории и выше ранжируют сайты, которые работают через безопасное соединение.

Задание

1. Запустить прилагаемое к методичке приложение.

Для этого на вашем устройстве должна быть установлена актуальная версия Node.js, если её нет, то можно установить с сайта: <https://nodejs.org/en/>

Затем перейдите в командную строку и запустите сервер приложения из директории ‘ssl’ командой: *node index.js*

После запуска сервера перейдите в браузере по адресу: <http://localhost:456/>, на экране откроется страница (рис. 1).



Рисунок 1 – Страница приложения

1. Удостовериться, что подключение небезопасно.

Нажав на иконку ‘i’ в строке адреса открывается окно, показывающее, что подключение к сайту не защищено (рис. 2), собственно, чтобы установить безопасное соединение нужно создать SSL сертификат.

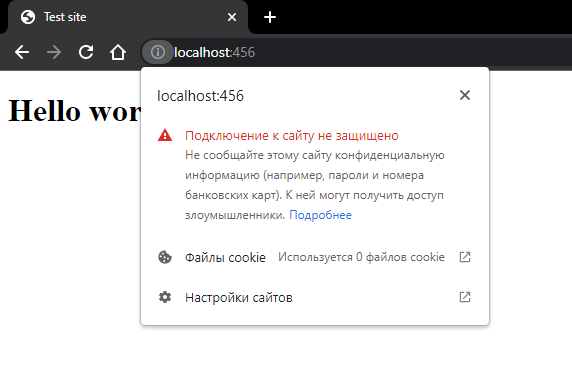


Рисунок 2 – Окно проверки подключения

1. Включение служб IIS

Первым делом вы должны включить службы IIS. Для этого в Панели управления необходимо выбрать раздел «Программы и компоненты» и в открывшемся окне в меню слева нажать на ссылку «Включение или отключение компонентов Windows». Далее в открывшемся окне нужно включить компонент «Службы IIS» (рис. 3).

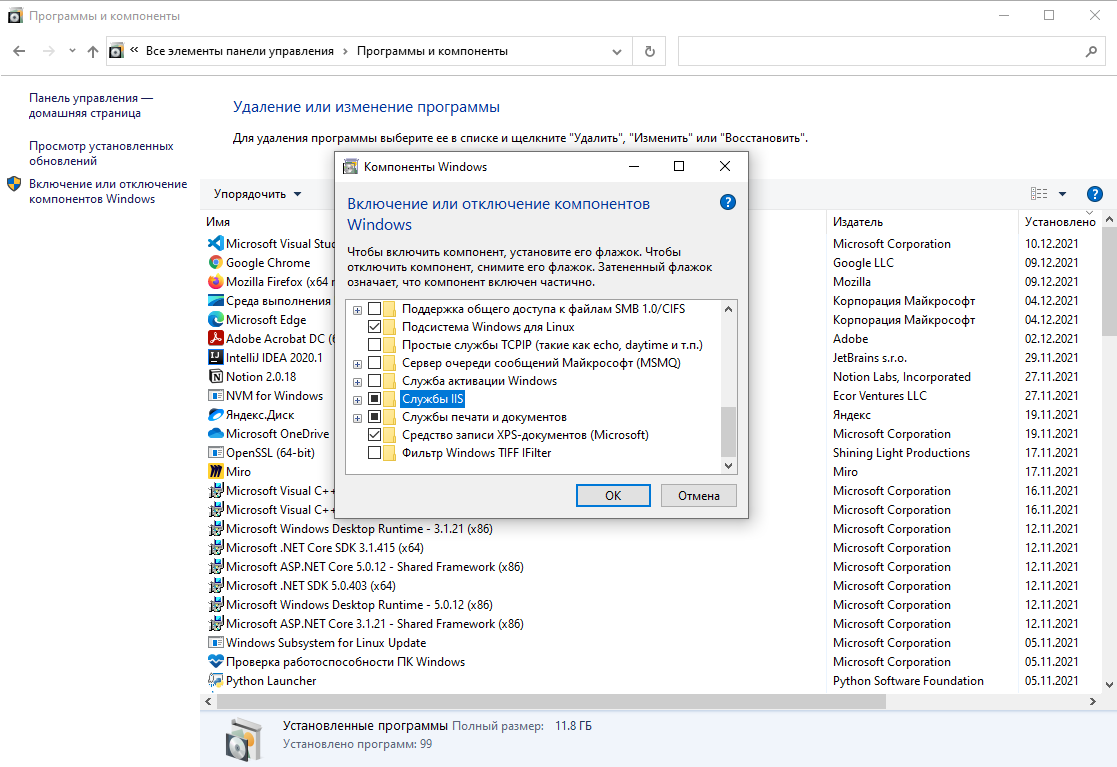


Рисунок 3 – Включение служб IIS

1. Сгенерировать новый SSL сертификат для localhost.

Запустить Windows PowerShell от имени администратора и ввести команду:

*New-SelfSignedCertificate -DnsName "localhost" -CertStoreLocation "cert:\LocalMachine\My"*

1. Установить сертификат в Trusted Root Certification Authorities.

Так как созданный сертификат не является надежным, нужно открыть Консоль управления (MMC) (рис. 4). Для этого с помощью клавиш «Win» + «R» вывести на экран окно «Выполнить», в котором нужно ввести команду *mmc.exe*.

Далее нужно перейти к:

Файл -> Добавить или удалить оснастку -> Сертификаты -> Добавить -> Учетная запись компьютера -> Локальный компьютер -> Нажмите кнопку Готово и затем в окне добавления и удаления оснасток нажмите ОК (рис. 5).

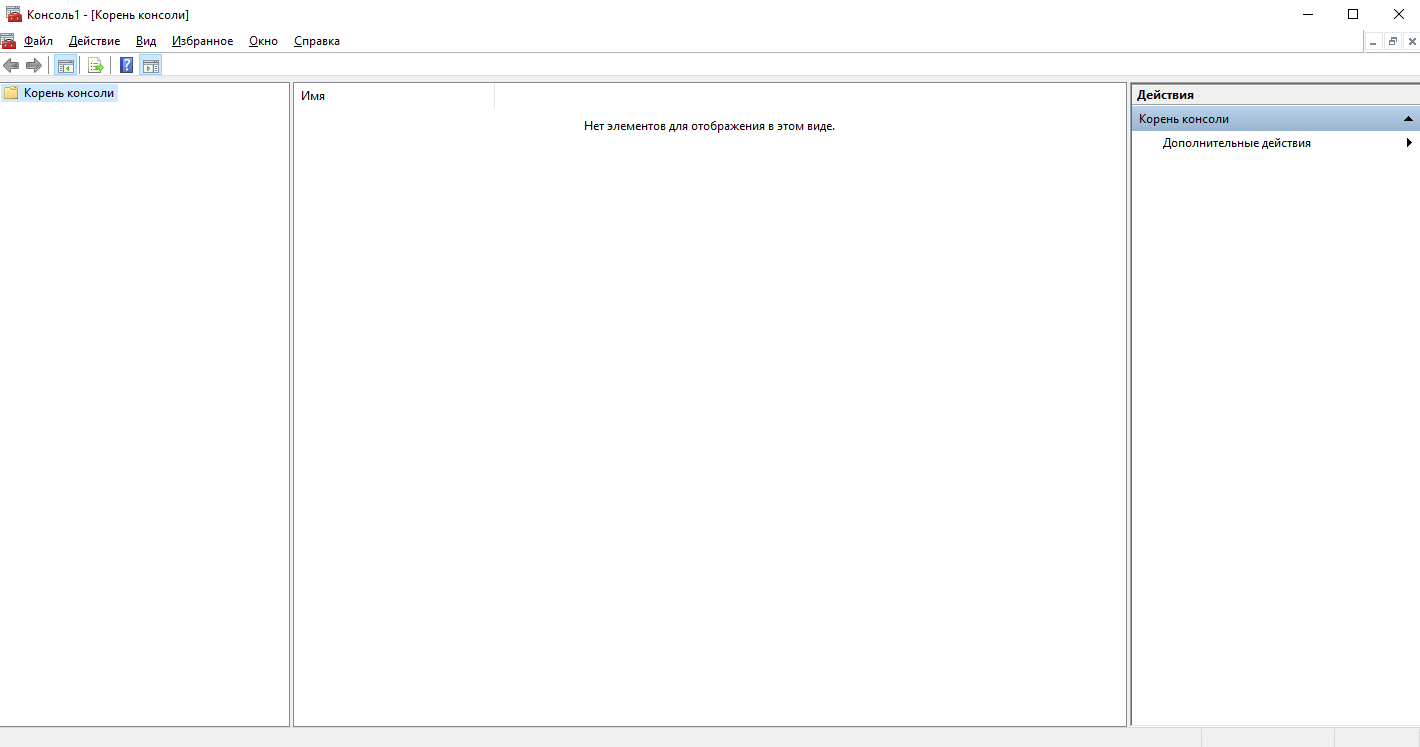


Рисунок 4 - Консоль управления (MMC)

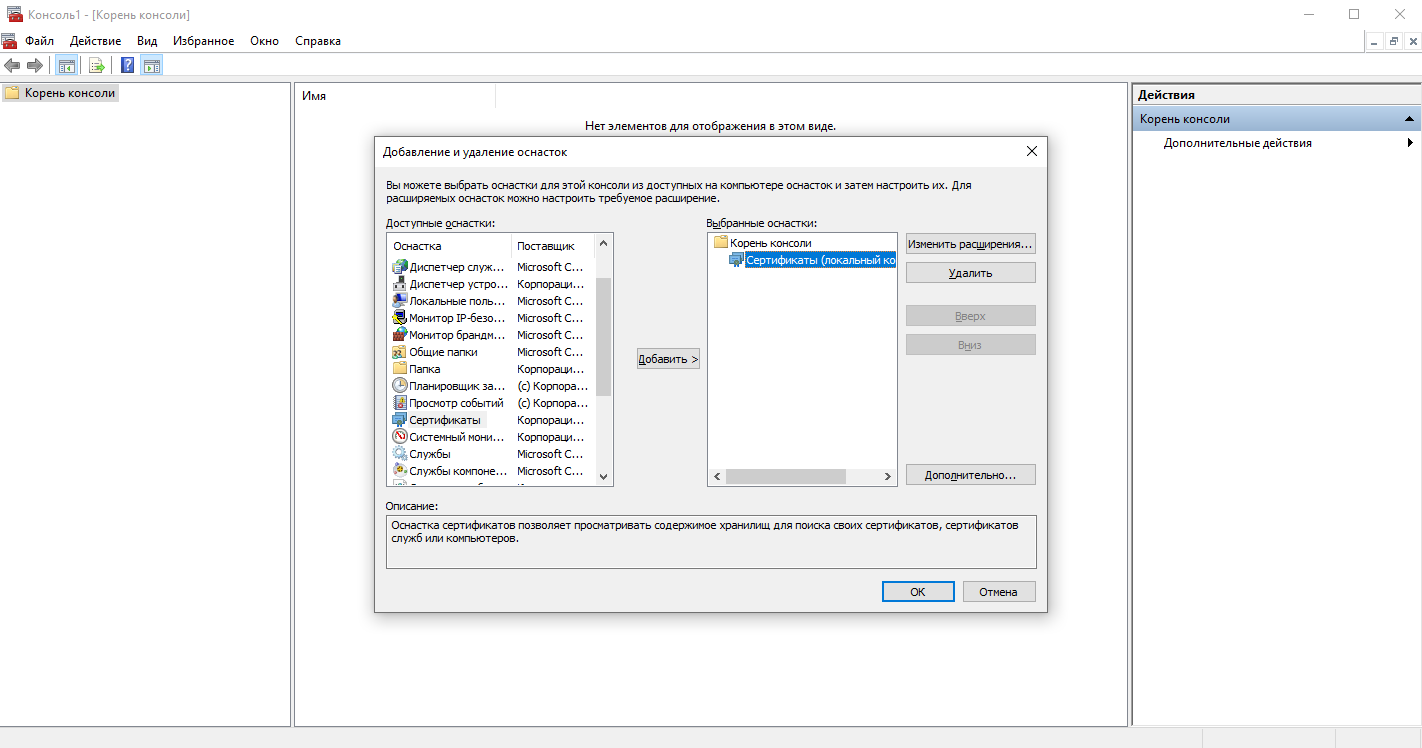


Рисунок 5 – Добавление оснасток

После чего в левом баре разверните 'Сертификаты', затем папку 'Личное' и внутри откройте папку 'Сертификаты', вы увидите свой сертификат localhost (рис. 6).

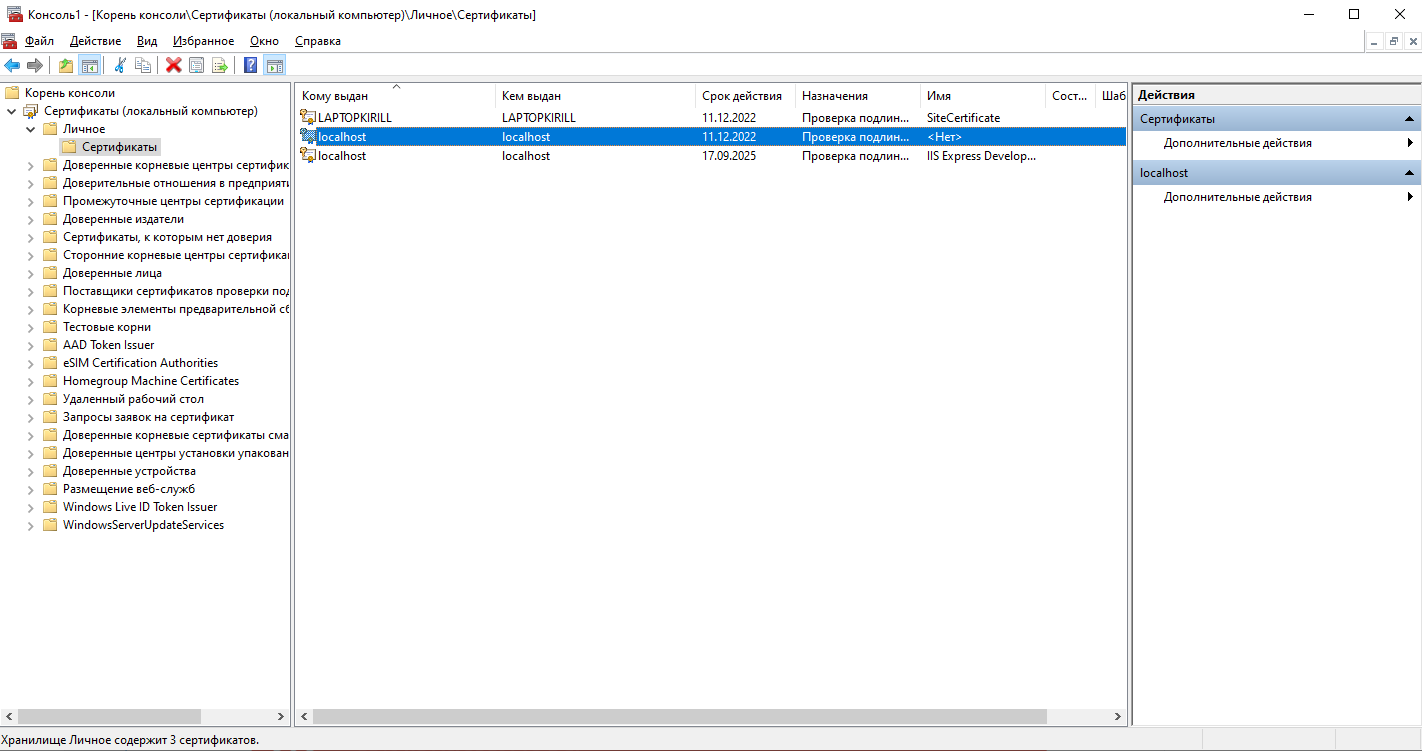


Рисунок 6 – Список сертификатов

Затем перейдите в папку ‘Доверенные корневые центры сертификации’ и скопируйте наш сертификат (localhost) во вложенную папку этой директории 'Сертификаты' (рис. 7). Тем самым вы сделали свой сертификат надежным.

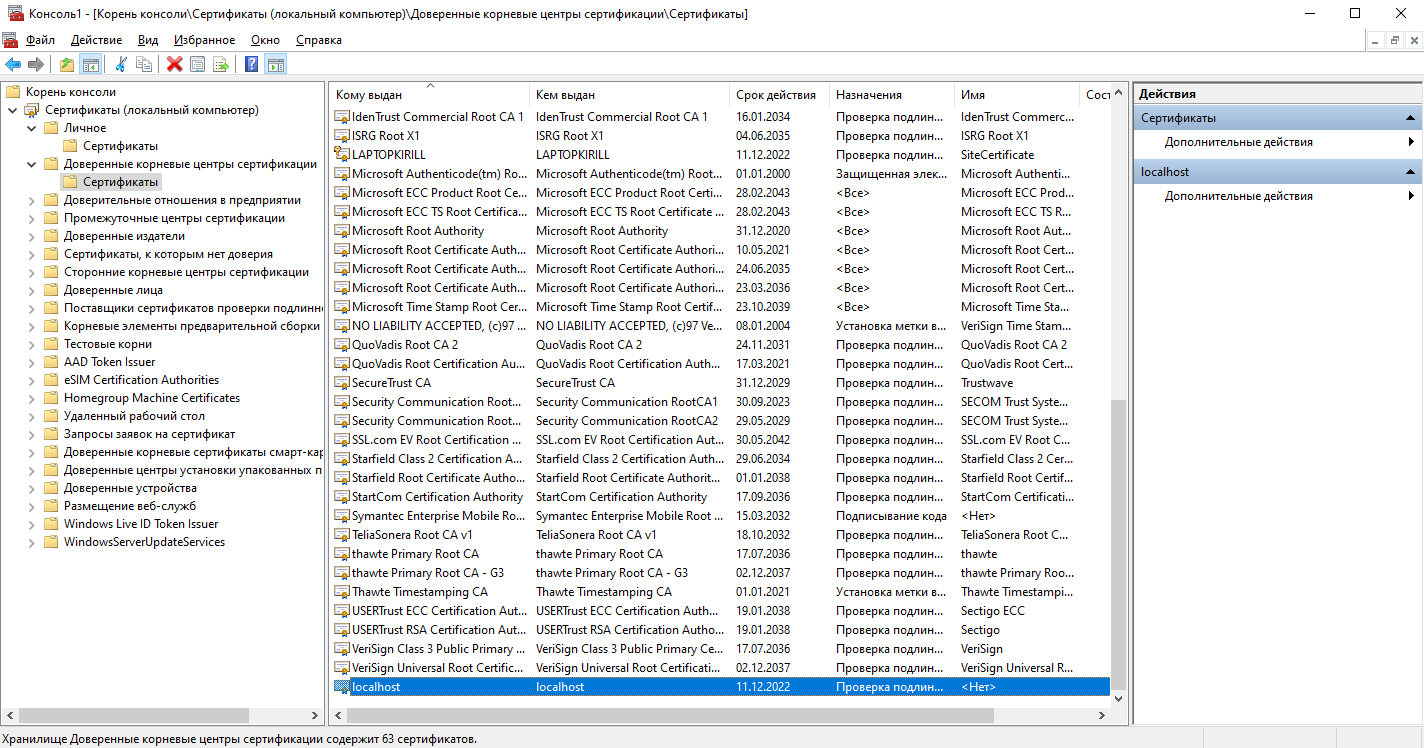


Рисунок 7 - Доверенные корневые центры сертификации

1. Привязать сертификат к серверу через диспетчер служб IIS.

Сначала вы должны открыть диспетчер служб IIS (рис. 8). Для этого с помощью клавиш «Win» + «R» вывести на экран окно «Выполнить», в котором нужно ввести команду *inetmgr.exe*.

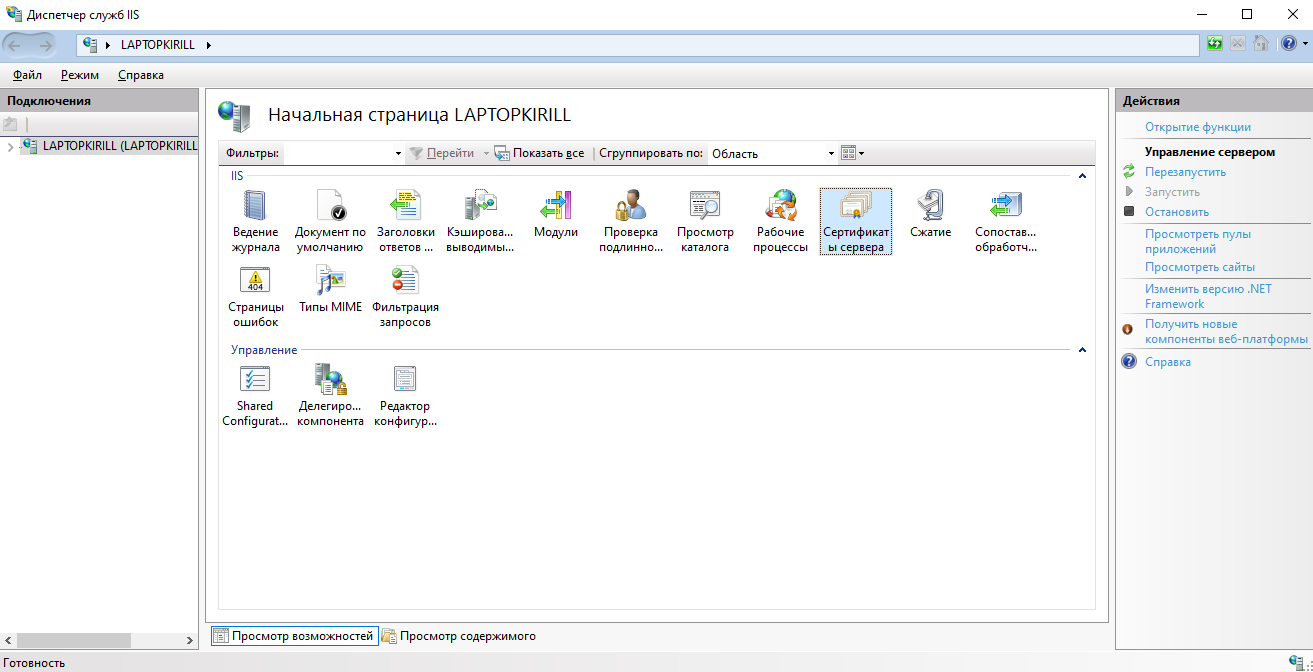


Рисунок 8 - Диспетчер служб IIS

В левом баре выберите сайт, к которому планируете привязать созданный сертификат и в столбце «Действия» нажмите на «Привязки…» (рис. 9).

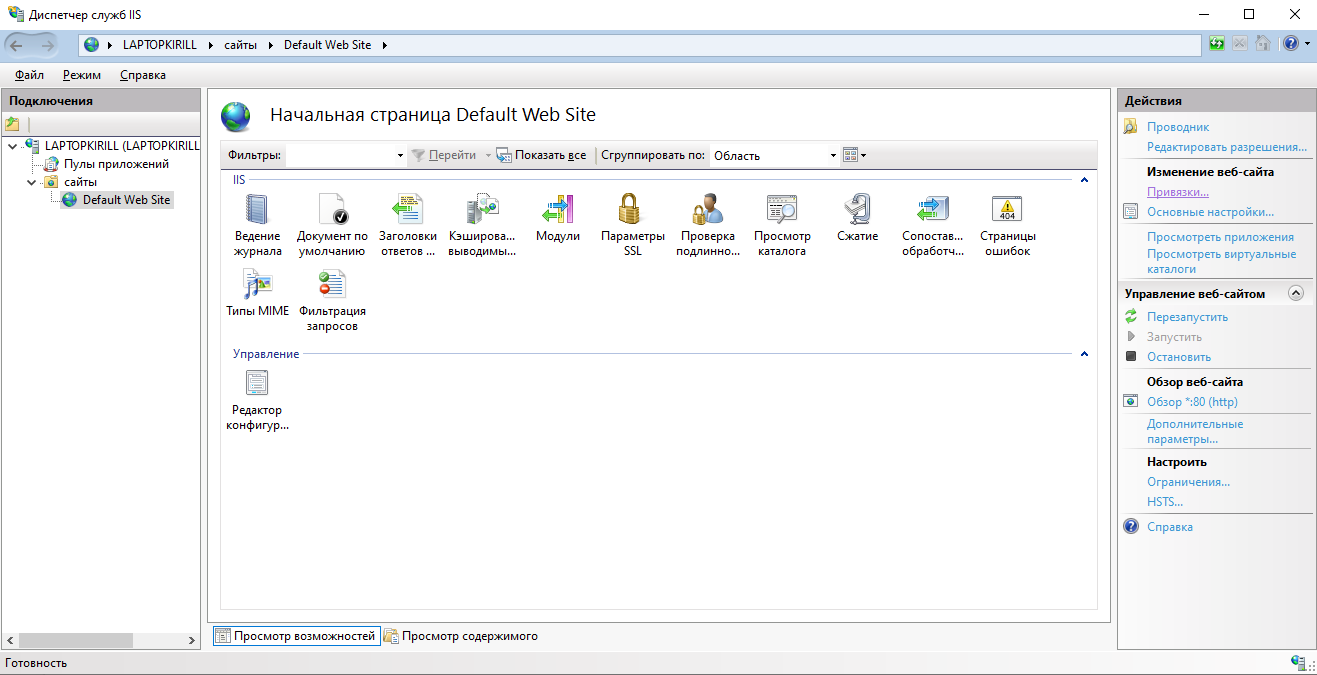


Рисунок 9 - Привязка к серверу

В открывшемся окне (рис. 10) добавляем привязку, указываем тип, порт и вам SSL-сертификат.

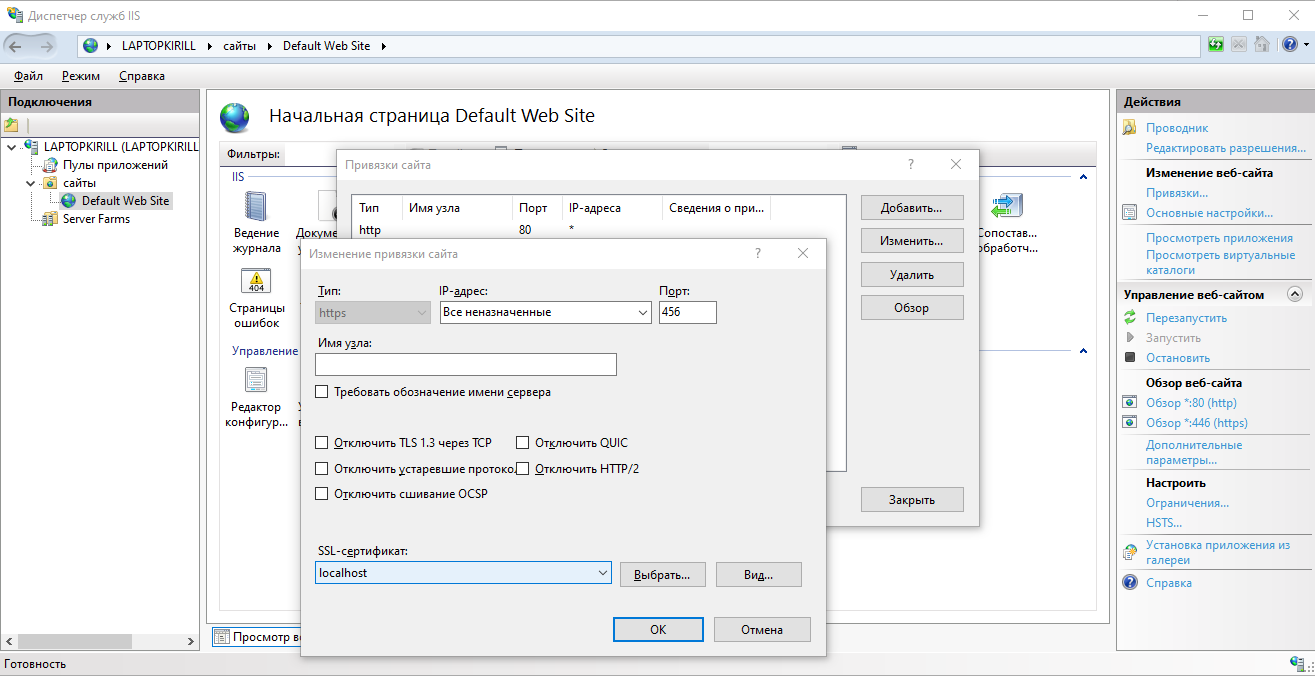


Рисунок 10 – Окно добавления привязки

Нажав на кнопку «Вид…» можно посмотреть ваш сертификат (рис. 11).

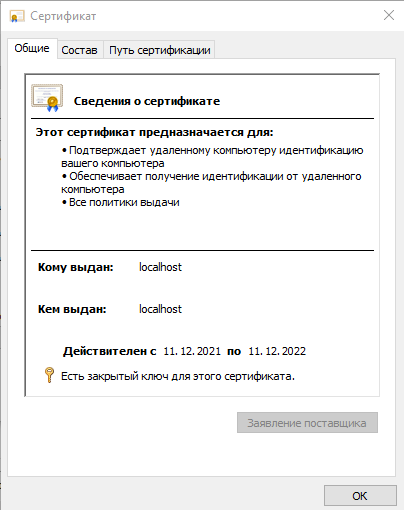


Рисунок 11 – Вид сертификата

1. Настроить IIS в качестве обратного прокси-сервера.

Чтобы настроить IIS в качестве обратного прокси-сервера, вам необходимо установить расширение [URL Rewrite extension](https://www.iis.net/downloads/microsoft/url-rewrite) и расширение [Application Request Routing extension](https://www.iis.net/downloads/microsoft/application-request-routing). Расширение URL Rewrite позволяет вам определять правила для включения URL-адресов, которые пользователям легче запоминать, а поисковым системам - находить. Расширение Application Request Routing обеспечивает функции масштабируемости: балансировку нагрузки, маршрутизацию на основе правил и многое другое.

Таким образом сервер, который на самом деле в прилагаемом приложении запущен на порту 3000, будет синхронизирован с IIS и расположен по адресу: <https://localhost:456/>.

Нужно перейти на сайт и выбрать опцию «Переопределение URL-адресов» и добавить новое правило (рис. 12).

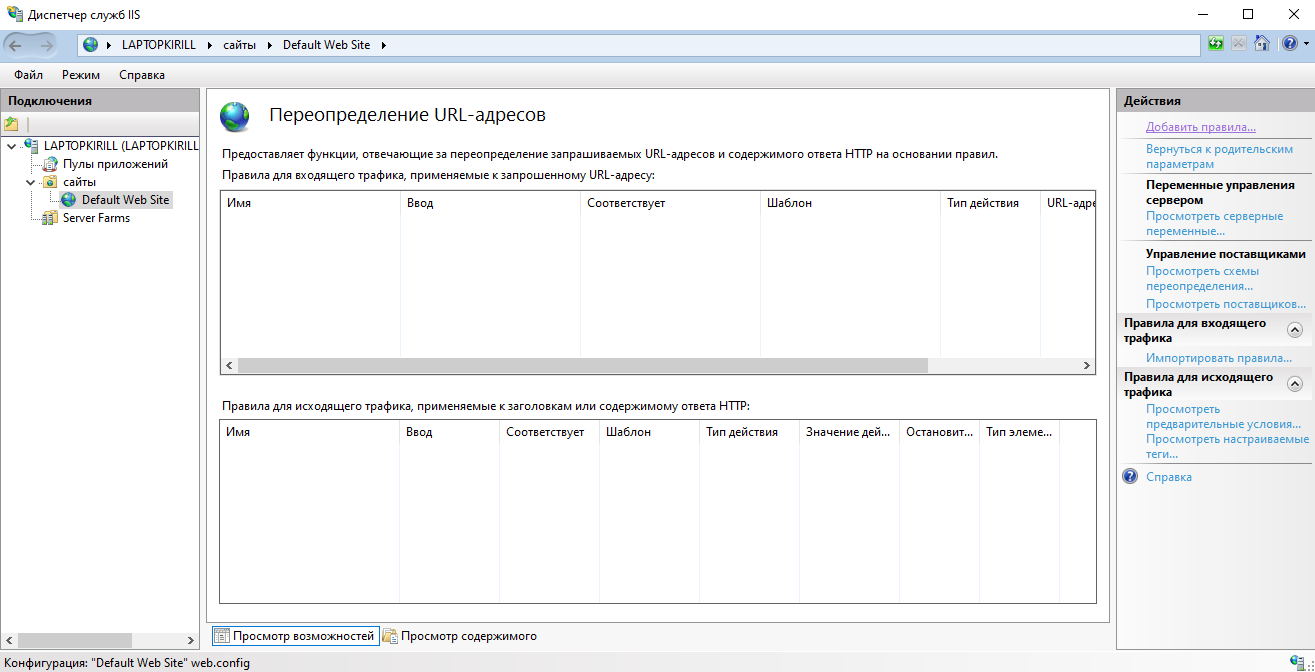


Рисунок 12 – Переопределение URL-адресов

В открывшемся окне добавления правила выбираем правила ддля входящего и исходящего трафика как обратный прокси-сервер (рис. 13).

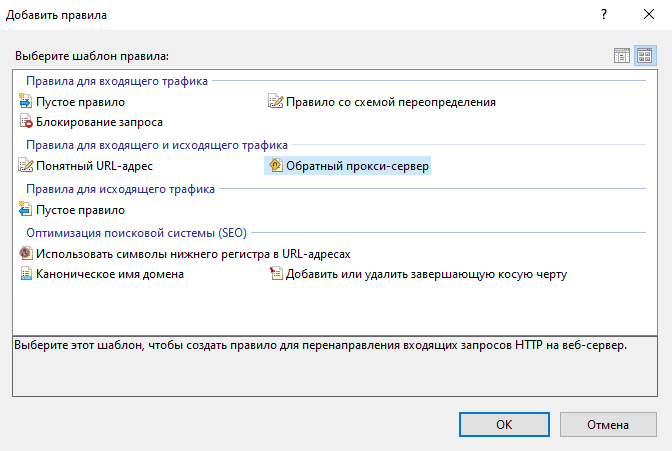


Рисунок 13 – Окно добавления правила

Затем прописываем на каком порту у нас находится наш Node.js сервер (рис. 14).

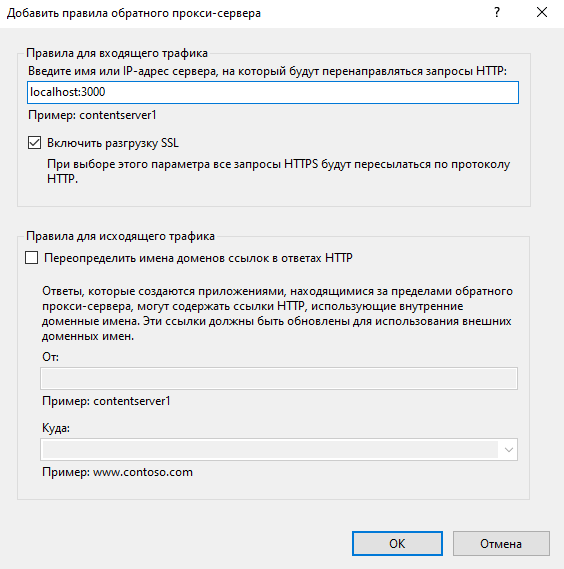


Рисунок 14 - Окно правила обратного прокси-сервера

1. Провести проверку SSL - сертификата.

Теперь вы можете перейти по адресу: <https://localhost:456/> и подключение будет считаться безопасным (рис. 15).

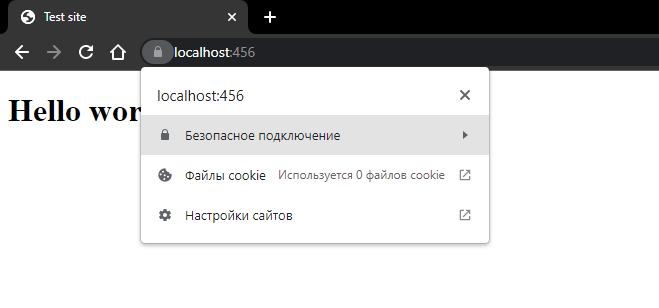


Рисунок 15 – Окно проверки подключения

Нажав на «Безопасное подключение» открывается окно (рис. 16), в котором можно посмотреть на наш сертификат (рис. 17).

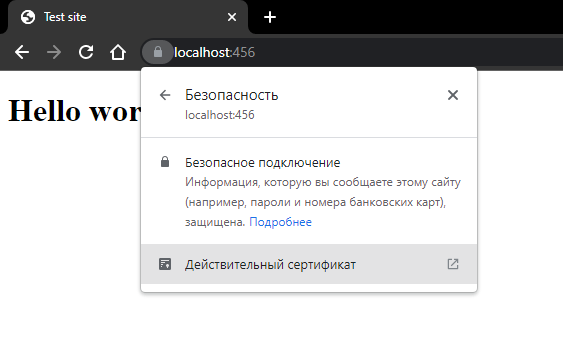


Рисунок 16 – Окно безопасного подключения

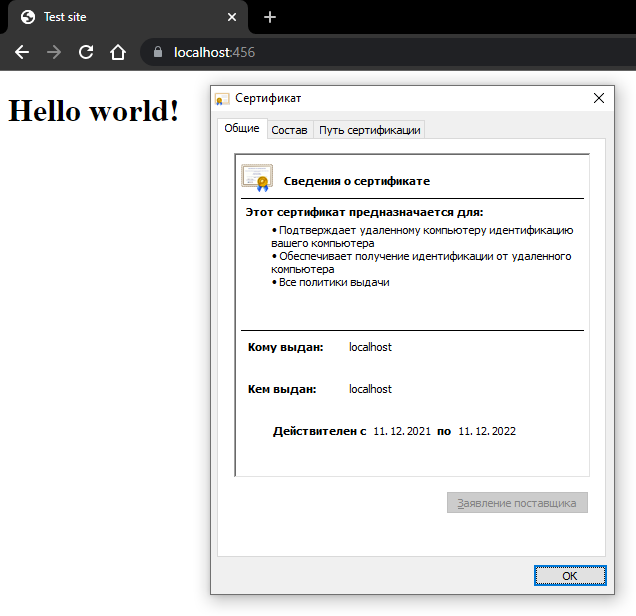


Рисунок 17 – Применённый сертификат