УТВЕРЖДАЮ
Генеральный директор
ООО «Кейсистемс»
_____ А. А. Матросов
«___» _____ 2019 г.

ПРОГРАММНЫЙ КОМПЛЕКС «БЮДЖЕТ-СМАРТ»

ВЕРСИЯ 19.01

Руководство пользователя

Настройка SSL на IIS

ЛИСТ УТВЕРЖДЕНИЯ

Р.КС.02120-01 32 04-ЛУ

Подп и дата	
Инв.N дубл	
Взам.инв.N	
Подп и дата	
Инв.N подл	

СОГЛАСОВАНО
Заместитель генерального директора
ООО «Кейсистемс»
_____ Е. В. Фёдоров
«___» _____ 2019 г.
Руководитель ДПиРСИБ

_____ Д. В. Галкин
«___» _____ 2019 г.

2019

Литера А

УТВЕРЖДЕНО
Р.КС.02120-01 32 04-ЛУ

информационные технологии
КЕЙСИСТЕМС

ПРОГРАММНЫЙ КОМПЛЕКС «БЮДЖЕТ-СМАРТ»

ВЕРСИЯ 19.01

Руководство пользователя

Настройка SSL на IIS

Р.КС.02120-01 32 04

Листов 25

Подп и дата	
Инв.N дубл	
Взам.инв.N	
Подп и дата	
Инв.N подл	

2019

Литера А

АННОТАЦИЯ

Настоящий документ является частью руководства администратора программного комплекса «Бюджет-СМАРТ» по автоматизации процесса проектирования, исполнения и анализа бюджетов субъектов Российской Федерации, закрытых автономно-территориальных образований и муниципальных образований версии 19.01 и содержит описание операций по созданию и настройке сертификатов SSL на IIS в ОС «WINDOWS».

Руководство актуально для указанной версии и для последующих версий вплоть до выпуска обновления руководства.

Порядок выпуска обновлений руководства

Выход новой версии программного комплекса сопровождается обновлением руководства только в случае наличия в версии значительных изменений режимов, описанных в руководстве, добавления новых режимов или изменения общей схемы работы. Если таких изменений версия не содержит, то остается актуальным руководство пользователя от предыдущей версии с учетом изменений, содержащихся в новой версии.

Перечень изменений версии программного комплекса содержится в сопроводительных документах к версии. Информация об изменениях руководства пользователя публикуется на сайте разработчика в разделе «Документация».

Информация о разработчике ПК «Бюджет-СМАРТ»

ООО «Кейсистемс»

Адрес: 428000, Чебоксары, Главпочтамт, а/я 172

Телефон: (8352) 323-323

Факс: (8352) 571-033

http://www.keysystems.ru

E-mail: info@keysystems.ru

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Настоящее руководство содержит описание операций по установке web-сервисов для работы программного комплекса на ОС «WINDOWS».

Уровень подготовки пользователя

Для успешного освоения материала, изложенного в руководстве, и формирования навыков работы в программном комплексе с описанными режимами к пользователю предъявляются следующие требования:

- наличие опыта работы с персональным компьютером на базе операционных систем Windows на уровне квалифицированного пользователя;
- умение свободно осуществлять базовые операции в стандартных приложениях Windows.

Перечень эксплуатационной документации

В *таблице 1* представлен список документации в части описания задач администрирования ПК «Бюджет-СМАРТ».

Таблица 1. Перечень эксплуатационной документации

№ п/п	Код документа	Наименование документа
1	2	3
1	Р.КС.02120-XX 32 -1	Установка Бюджет-СМАРТ
2	Р.КС.02120-XX 32 -2	Установка сервисов СМАРТ на ОС WINDOWS
3	Р.КС.02120-XX 34 -22	Описание интерфейса
4	Р.КС.02120-XX 34 -18-1	Администрирование комплекса
5	Р.КС.02120-XX 32 -3	Управление сервисами СМАРТ/WEB
6*	Р.КС.02120-XX 32 -4	Настройка SSL на IIS
* настоящее руководство		

Условные обозначения

В документе используются следующие условные обозначения:

Уведомление _ Важные сведения о влиянии текущих действий пользователя на выполнение других функций, задач программного комплекса.

Предупреждение _ Важные сведения о возможных негативных последствиях действий пользователя.

Предостережение _ Критически важные сведения, пренебрежение которыми может привести к ошибкам.

Замечание _ Полезные дополнительные сведения, советы, общеизвестные факты и выводы.

[Выполнить] _ Функциональные экранные кнопки.

<F1> _ Клавиши клавиатуры.

«Чек» _ Наименования объектов обработки (режимов).

Статус _ Названия элементов пользовательского интерфейса.

ОКНА => НАВИГАТОР _ Навигация по пунктам меню и режимам.

п. 2.1.1
рисунок 5 _ Ссылки на структурные элементы, рисунки, таблицы текущего документа.
[1] _ Ссылки на документы из перечня ссылочных документов.

1. НАСТРОЙКА SSL НА IIS

Подключение к базе данных может осуществляться как напрямую, так и с использованием сервера приложений. Выбор варианта подключения осуществляется в окне авторизации пользователей на вкладке **«Соединение»** (*Рисунок 1*).

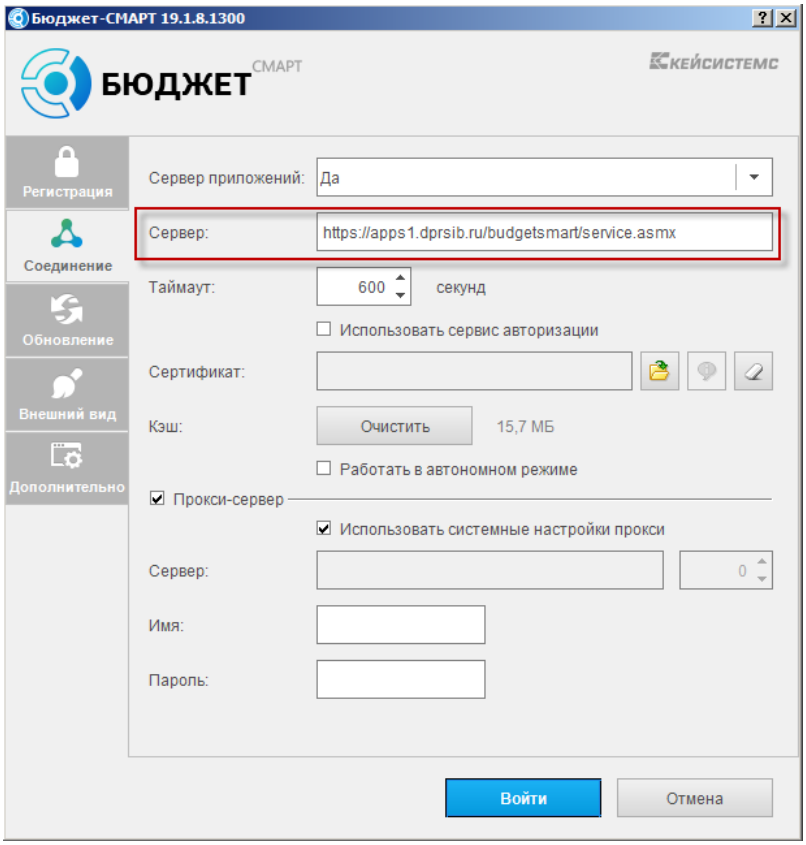

Рисунок 1. Вкладка «Соединение»

При использовании сервера приложений требуется выбрать в поле **Сервер приложений** опцию «Да» и ввести адрес сервера в поле **Сервер** окна настройки соединения.

Для подключения через сервер приложений необходимо использовать https сервер с SSL, т.е. расширение протокола http, поддерживающее шифрование.

Протокол SSL (Secure Sockets Layer – уровень защищенных сокетов) используется для защиты данных в сети Интернет. Он гарантирует безопасное соединение между компьютером пользователя и сервером. При использовании SSL-протокола информация передается в закодированном виде по https и расшифровать ее можно только с помощью специального ключа (в отличие от протокола http). Для работы SSL-протокола требуется, чтобы на сервере был установлен SSL-сертификат.

Для выполнения настройки SSL на Windows Server, начиная от 2008 R2 и выше, должен быть установлен веб сервер IIS.

1.1. Виды сертификатов для настройки https сайта на IIS

Чтобы подготовить веб-сервер для обработки HTTPS-соединений, администратор должен получить и установить в систему сертификат для этого веб-сервера.

Ключ выдается Центром сертификации на основании направленного туда запроса на SSL-сертификат (*п. 1.2.2*).

Такой сертификат состоит из двух частей (двух ключей) – public и private. Public-часть сертификата используется для шифрования трафика от клиента к серверу в защищенном соединении; private-часть – для расшифровывания полученного от клиента зашифрованного трафика на сервере.

Необходимо прописать все DNS записи и сгенерировать Certificate Signing Reques (CSR) запрос - запрос на получение сертификата, который представляет собой текстовый файл, содержащий в закодированном виде информацию об администраторе домена и открытый ключ.

Существует возможность создать такой сертификат, не обращаясь в Центр сертификации. Подписываются такие сертификаты этим же сертификатом, поэтому они называются «самоподписанными»/«самозаверенными» (self-signed) (*п. 1.2.1*).

При отсутствии дополнительных рекомендаций и требований к сертификату, рекомендуется использование опции «Создать самозаверенный сертификат».

1.2. Режим работы с сертификатами на IIS 7

Откройте консоль управления IIS. Для создания сайтов на протоколе https прежде всего необходимо создать и импортировать нужный сертификат. Для этого откройте диспетчер IIS и перейдите в пункт **«Сертификаты сервера»** (*Рисунок 2*).

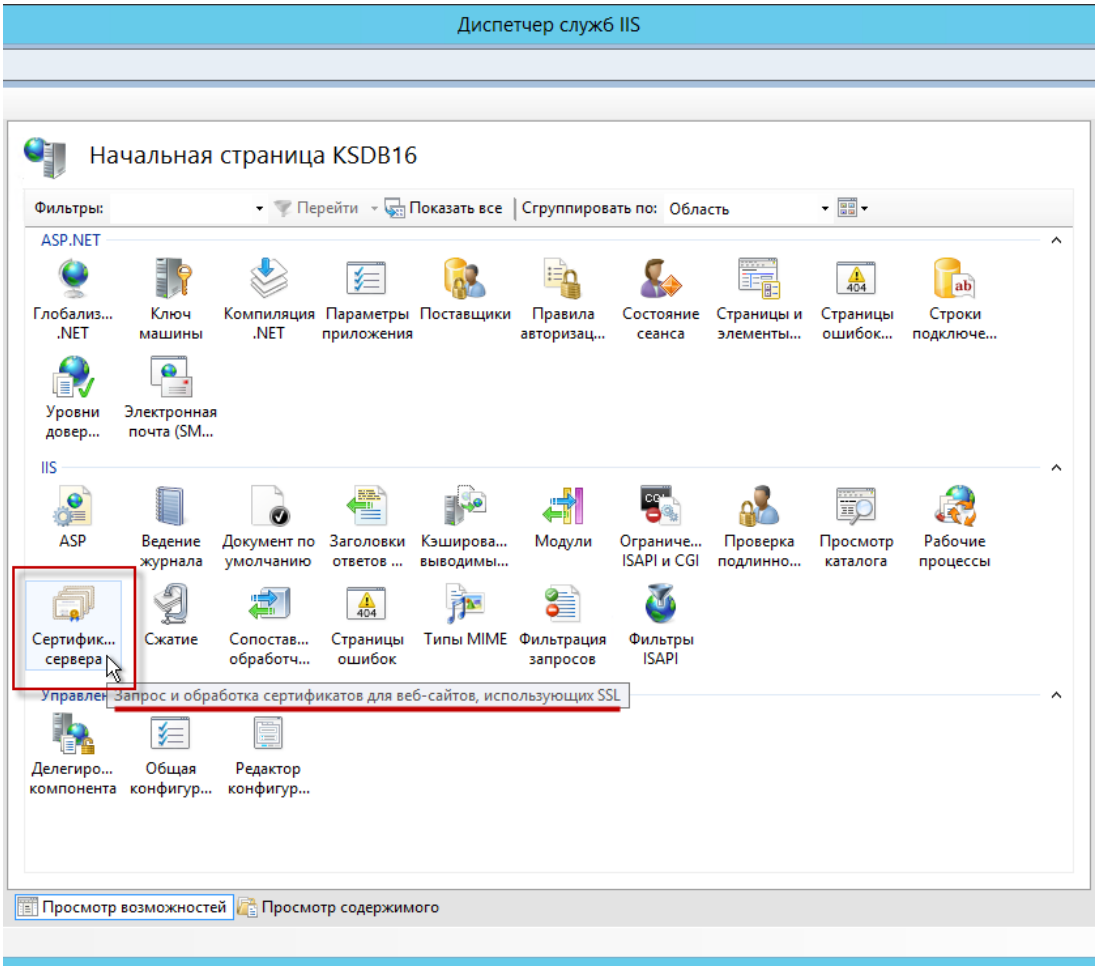

Рисунок 2. Сертификаты сервера

1.2.1. Создание самозаверенного сертификата

В открывшемся окне, в области **«Действия»**, выберите опцию **«Создать самозаверенный сертификат»** (*Рисунок 3*).

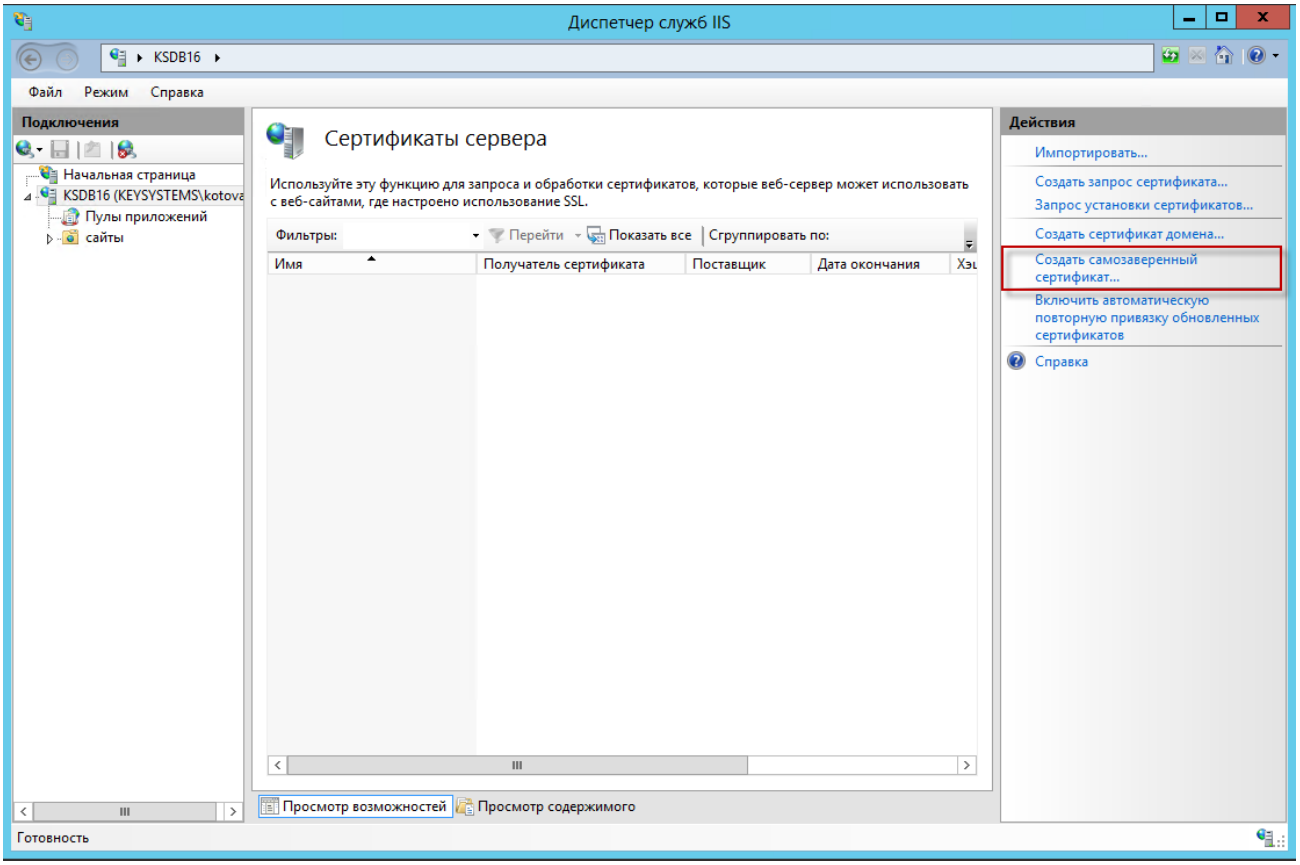

Рисунок 3. Создание запроса сертификата

В окне параметров запроса заполните следующие поля (*Рисунок 4*):

- **Понятное имя** – идентификатор сертификата;
- **Выбрать хранилище сертификатов** - укажите значение «Личный», оно подойдет для стандартного размещения (значение «Размещение веб-служб» используется для SNI технологии).

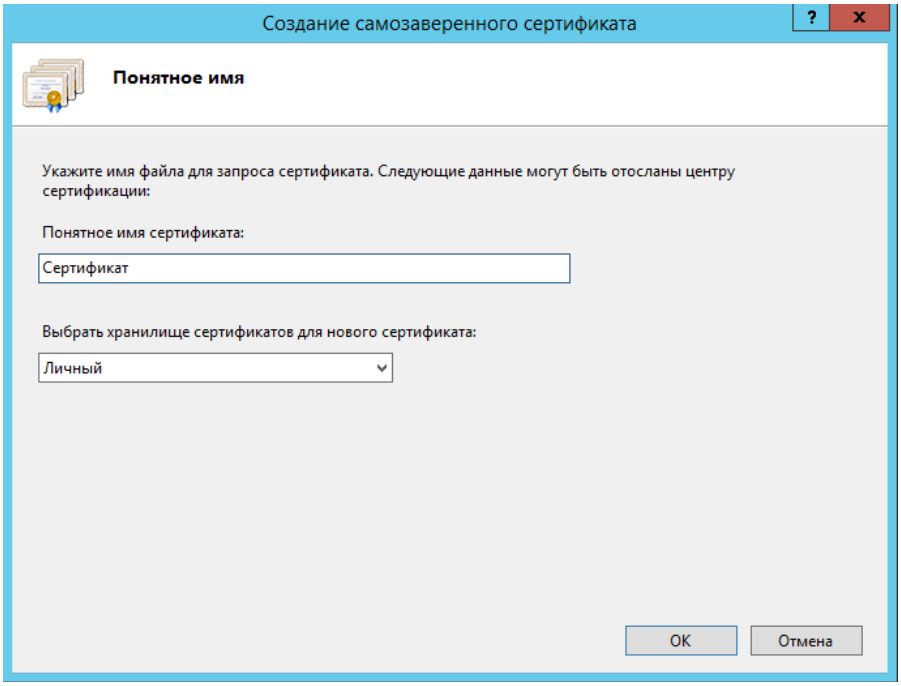

Рисунок 4. Свойства имени сертификата

По кнопке **[OK]** сертификат сразу отобразится в списке «Сертификаты сервера» (*Рисунок 5*).

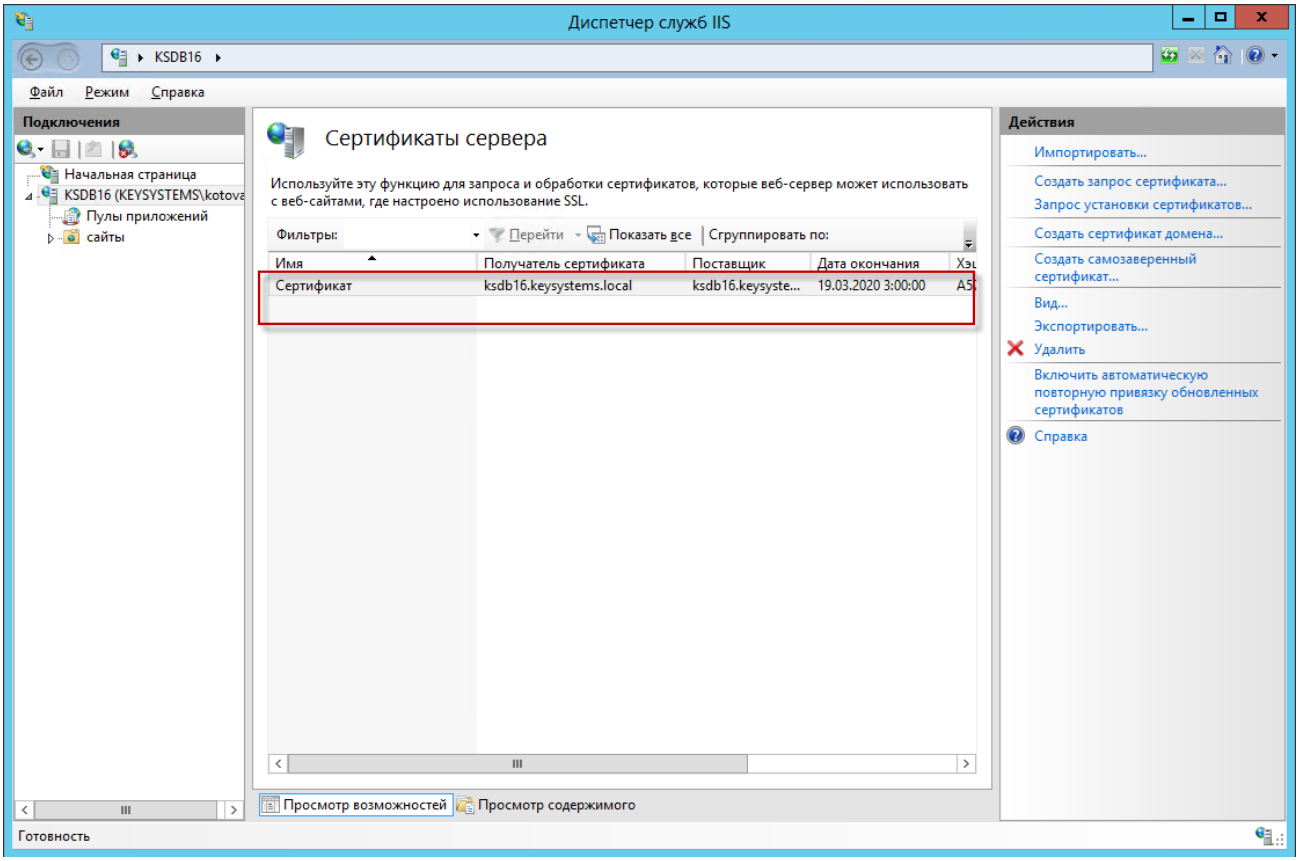

Рисунок 5. Сертификаты сервера

Такой сертификат уже содержит закрытый ключ, а также имеет требуемый для IIS формат *.pfx.

1.2.2. Генерация CSR запроса сертификата на IIS 7

В открывшемся окне, в области **«Действия»**, выберите опцию **«Создать запрос сертификата»** (*Рисунок 6*).

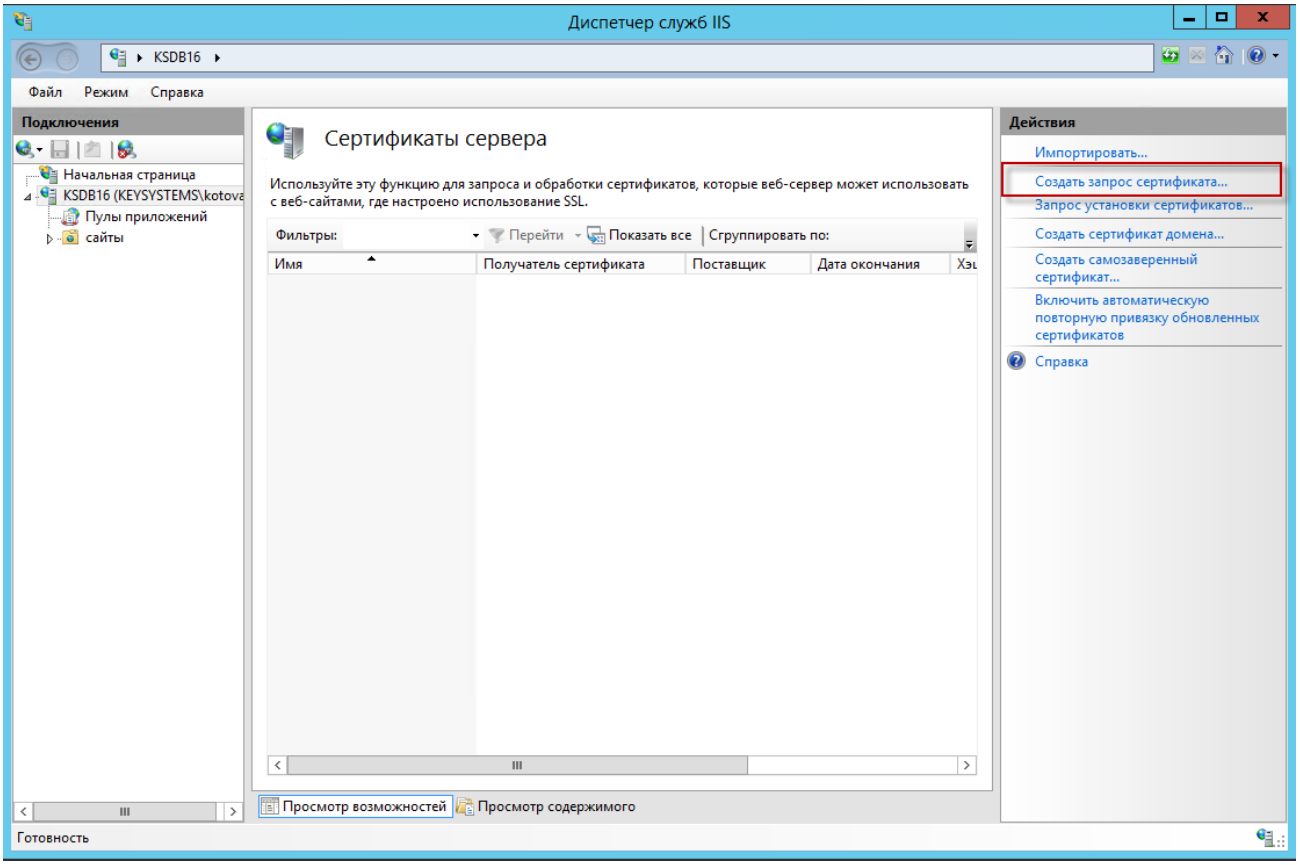

Рисунок 6. Создание запроса сертификата

В окне параметров запроса заполните следующие поля (*Рисунок 7*):

- **Полное имя** - адрес ресурса;
- **Организация**;
- **Подразделение** – не является обязательным для заполнения;
- **Город**;
- **Область**;
- **Страна или регион** - обозначение страны (на латинице);

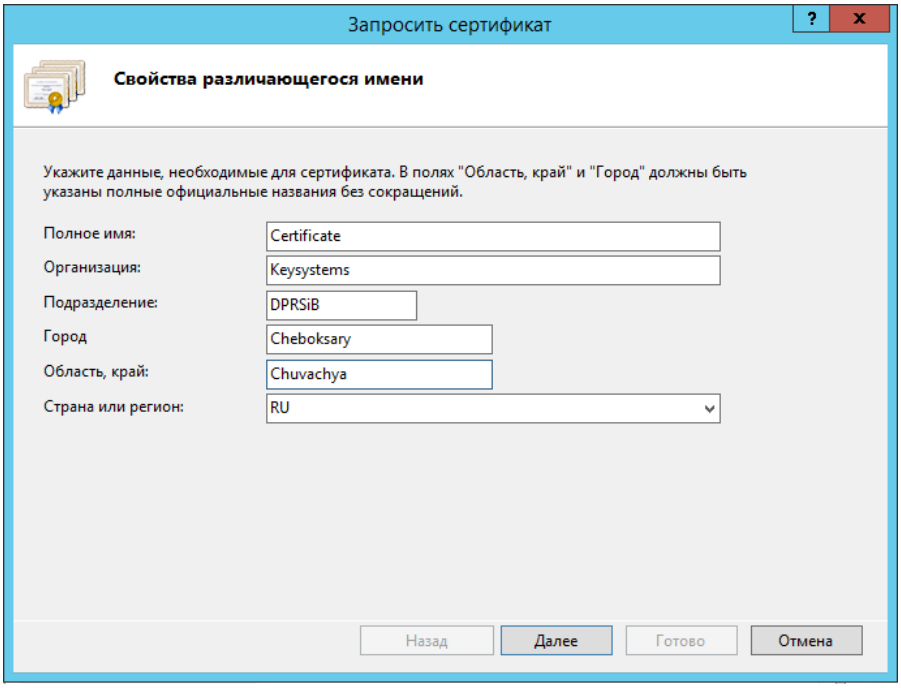

Рисунок 7. Свойства имени сертификата

Далее выберите значение длины ключа - 2048 бит (*Рисунок 8*).

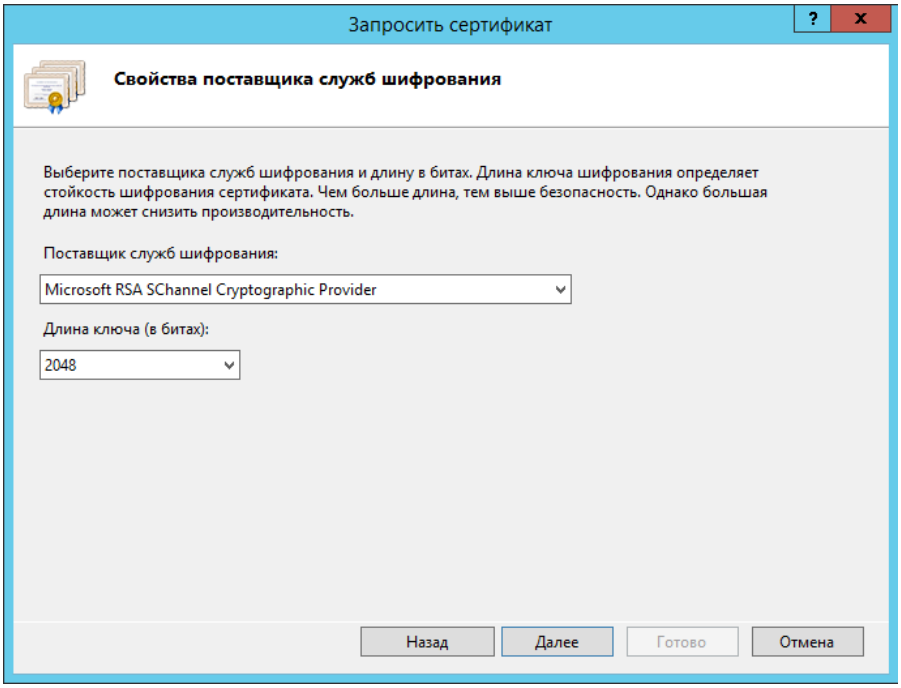

Рисунок 8. Свойства поставщика служб шифрования

Укажите место сохранения CSR запроса (это будет обычный текстовый файл *.txt) (*Рисунок 9*).

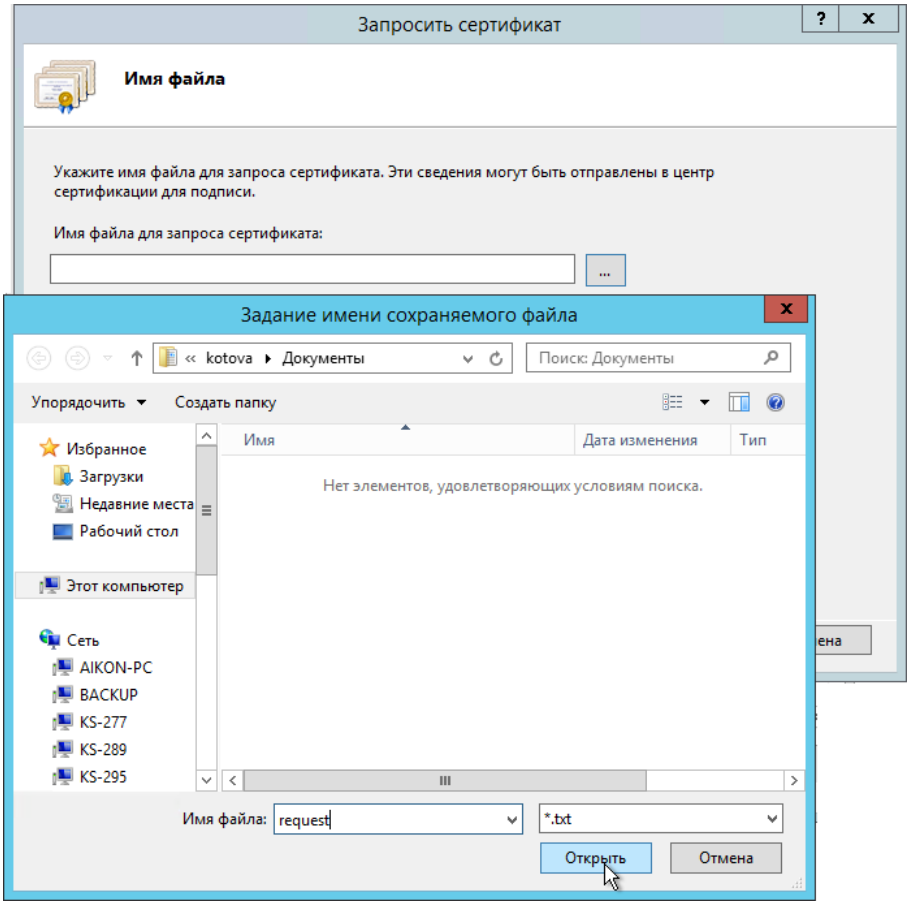

Рисунок 9. Путь к месту сохранения CSR запроса

CSR можно сгенерировать в процессе заказа SSL-сертификата или на стороне веб-сервера на выпуск сертификата. Задачей CSR является подготовка специального файла, в составе которого будет содержаться необходимая информация о домене, на который планируется выпустить SSL сертификат и информация об организации, всё это будет зашифровано. Вместе с CSR будет сгенерирован закрытый ключ (private key), которым сервер или сервис будет расшифровывать трафик между ним и клиентом (*Рисунок 10*).

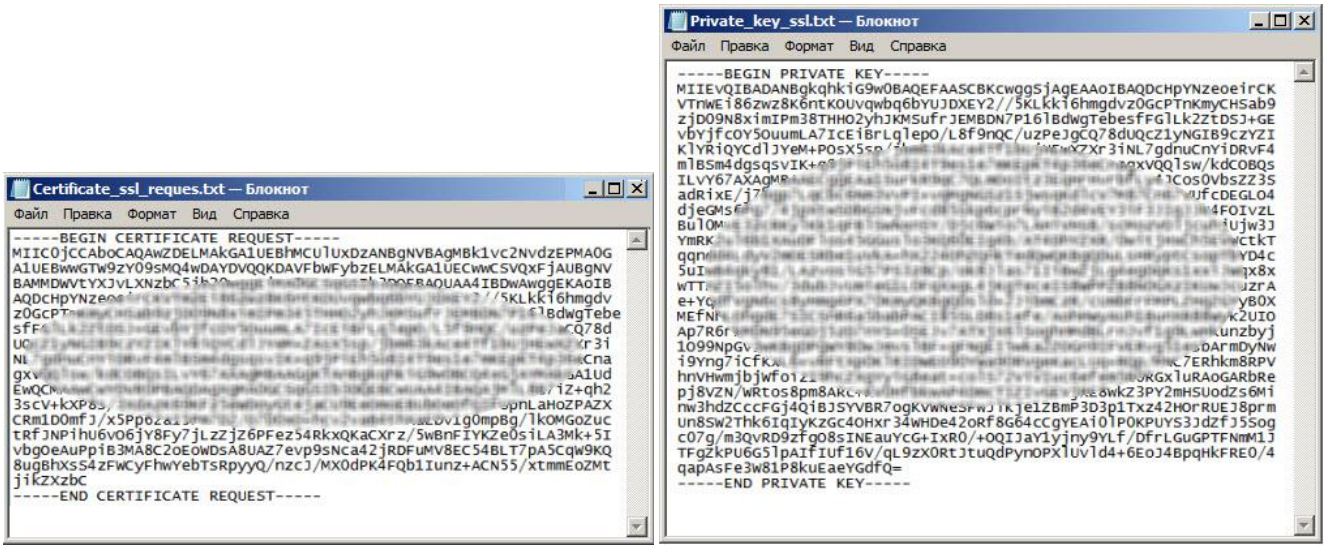

Рисунок 10. Запрос и закрытый ключ

После того как пара ключей приватный/публичный сгенерированы, на основе публичного ключа формируется запрос на SSL-сертификат в Центр сертификации (*Рисунок 11*). Перед этим измените расширение файла с *.txt на *.p10.

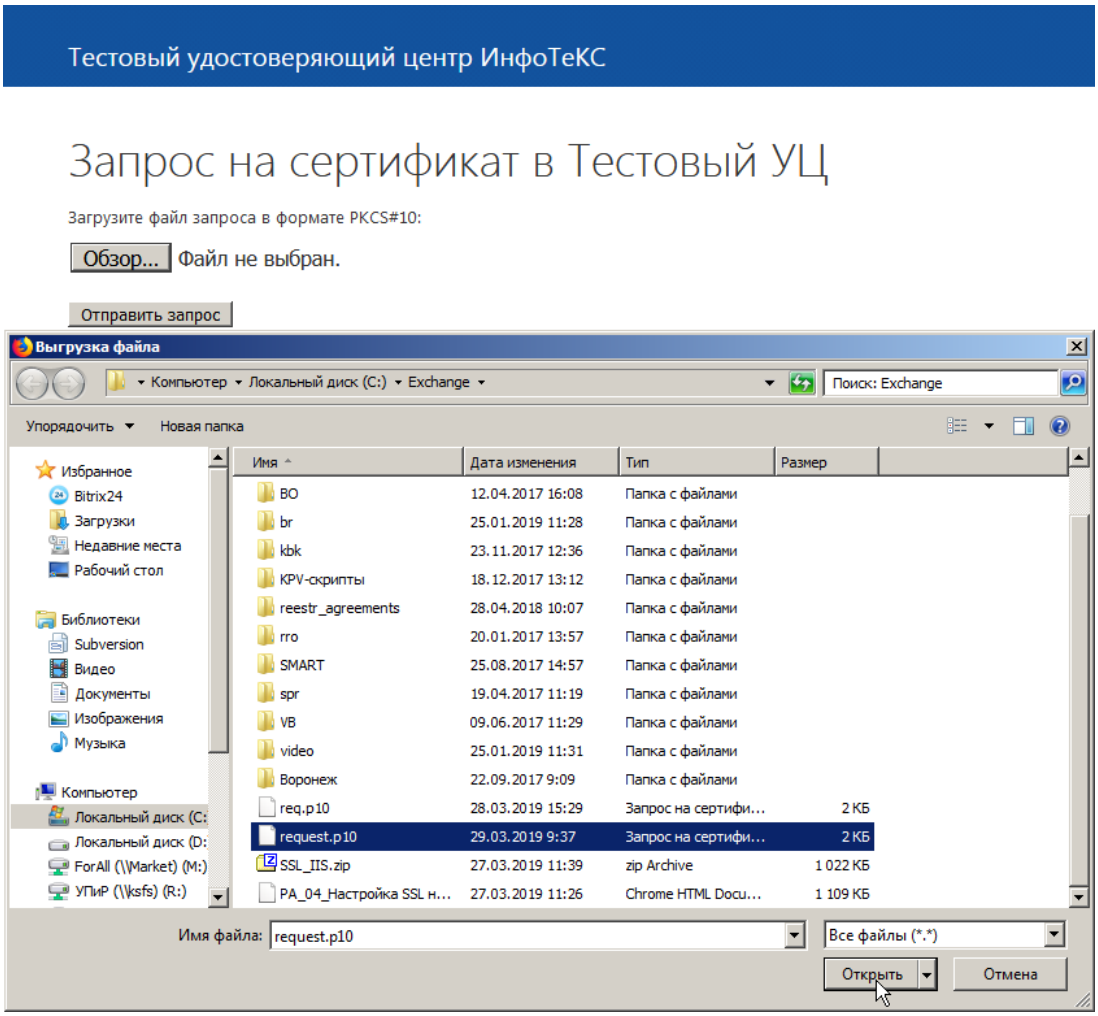

Рисунок 11. Передача запроса в удостоверяющий центр

Скачайте полученный сертификат (*Рисунок 12*).

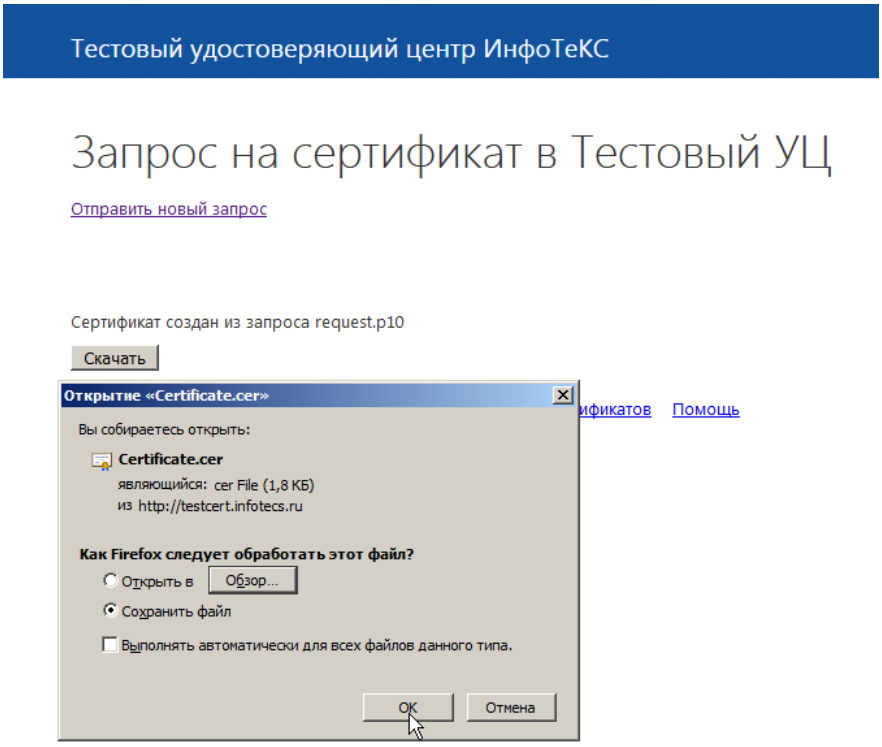

Рисунок 12. Сохранение сертификата, полученного от УЦ

Для установки на сервер полученного от УЦ сертификата воспользуйтесь опцией **«Запрос установки сертификатов»** в меню **«Действия»** (*Рисунок 13*).

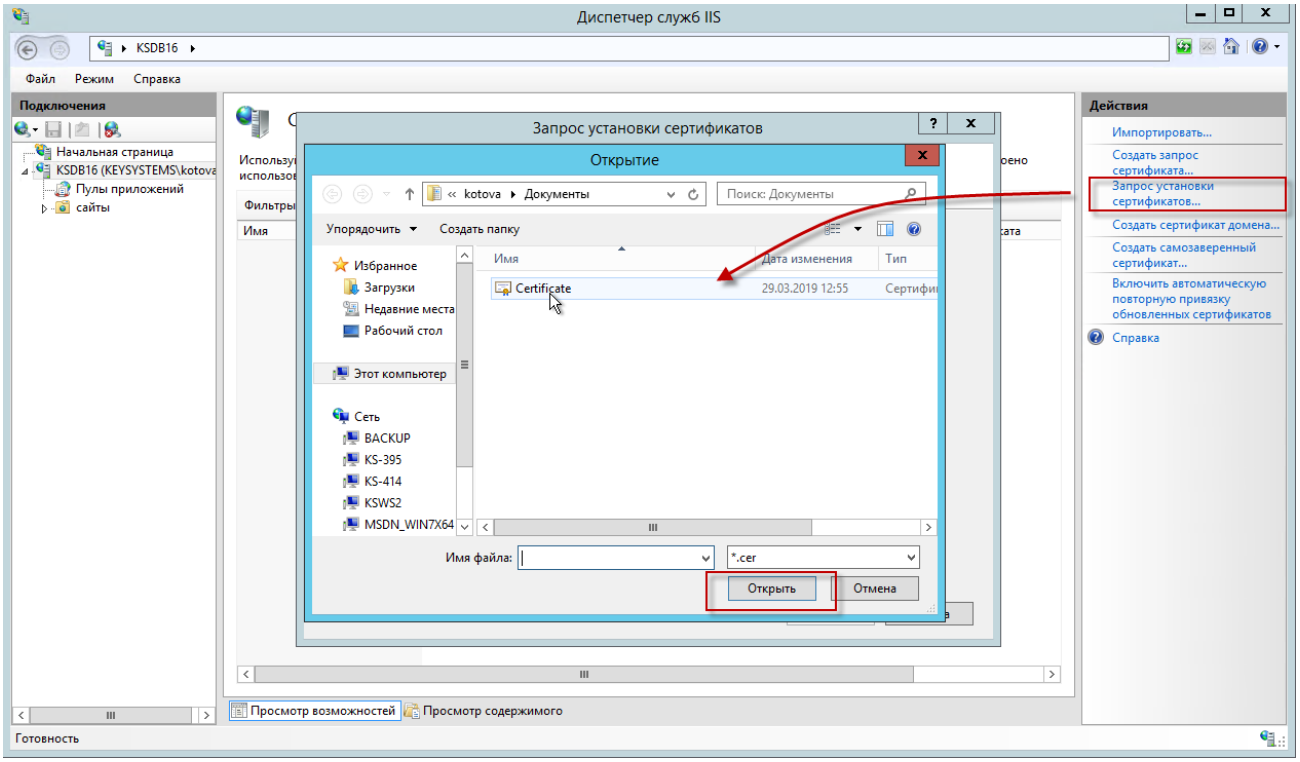

Рисунок 13. Установка сертификата, полученного от УЦ

В окне параметров запроса заполните следующие поля (*Рисунок 14*):

– **Понятное имя** – идентификатор сертификата;

– **Выбрать хранилище сертификатов** - укажите значение «Личный», оно подойдет для стандартного размещения (значение «Размещение веб-служб» используется для SNI технологии).

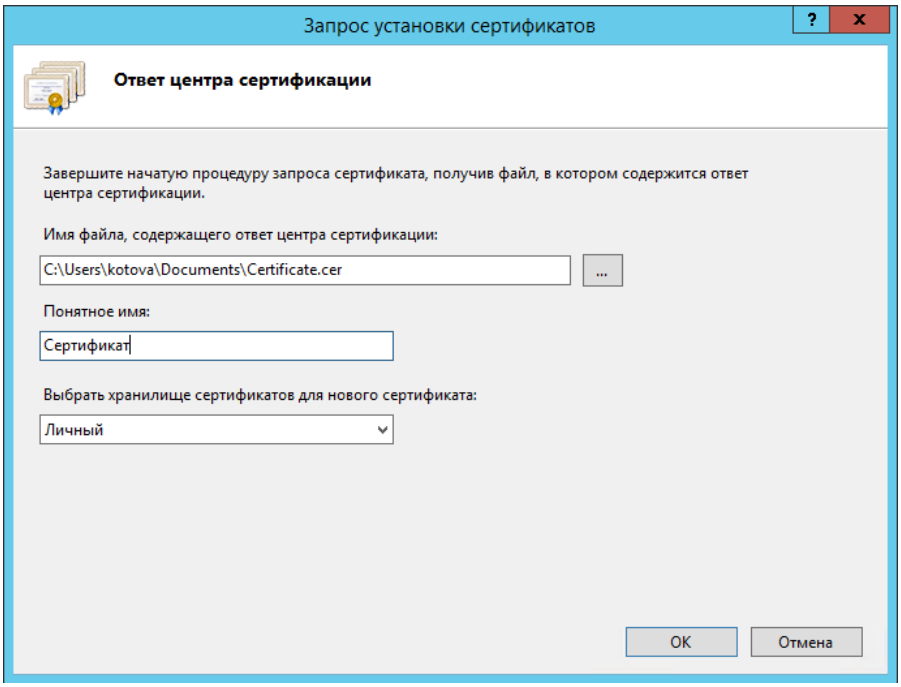

Рисунок 14. Запрос установки сертификатов

По кнопке **[OK]** сертификат сразу отобразится в списке **«Сертификаты сервера»** (*Рисунок 15*).

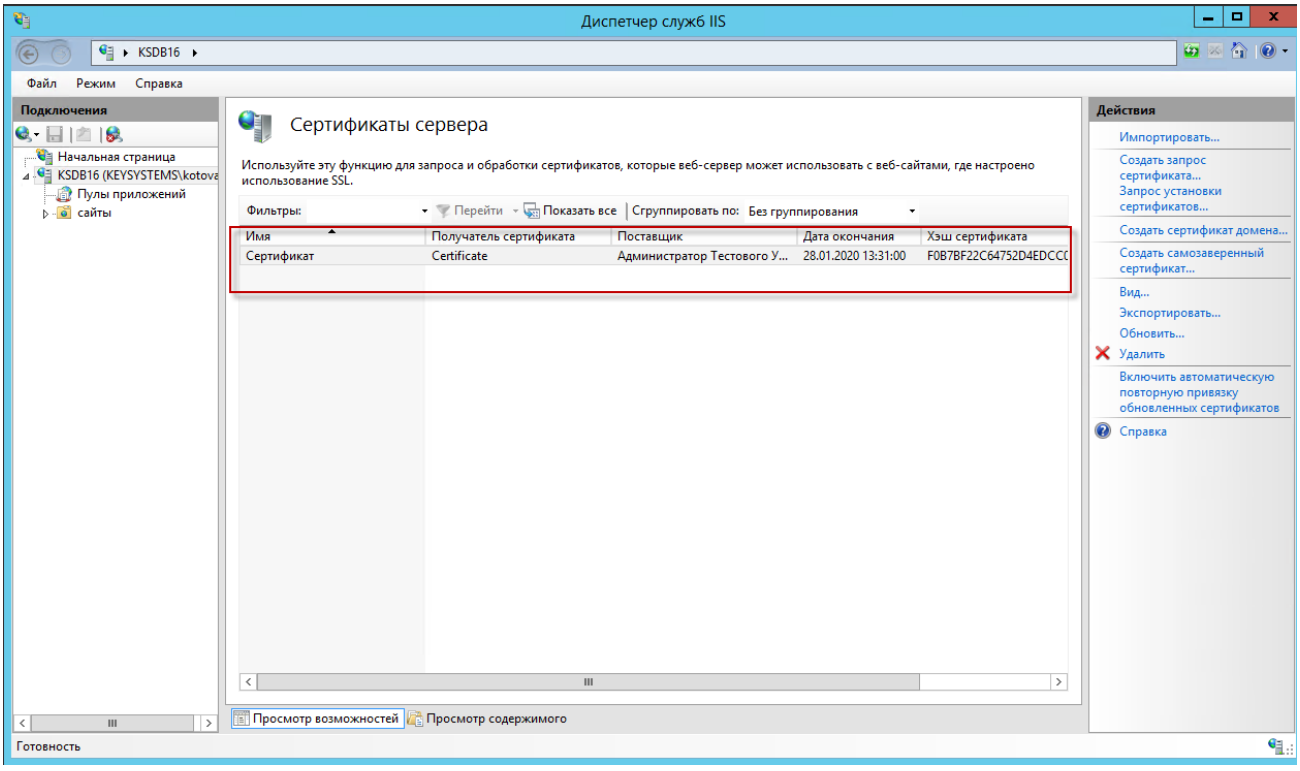

Рисунок 15. Сертификаты сервера

1.2.3. Преобразование сертификатов

В том случае, когда полученный от Центра сертификации сертификат имеет формат *.crt, его необходимо настроить под IIS, то есть получить требуемый формат *.pfx.

Нажмите сочетание клавиш **<WIN+R>** и вводим «mmc», для вызова оснастки (*Рисунок 11*).

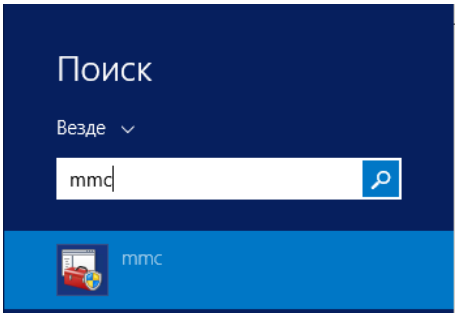

Рисунок 16. Вызов оснастки

Далее необходимо через меню «Файл» добавить новую оснастку (*Рисунок 17*).

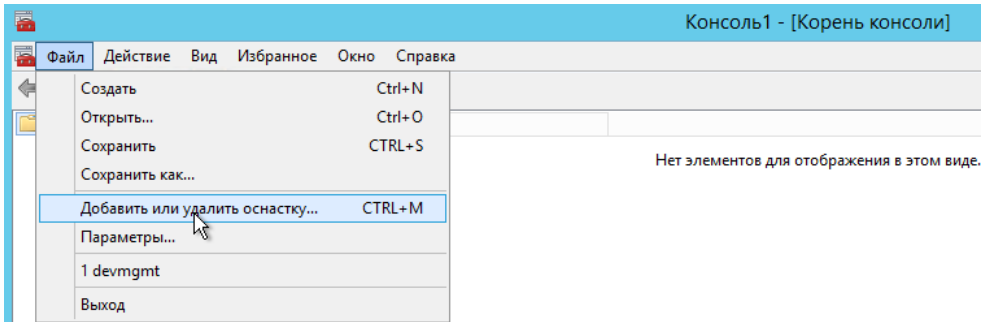

Рисунок 17.

Найдите сертификаты и нажмите кнопку **[Добавить]** (*Рисунок 18*).

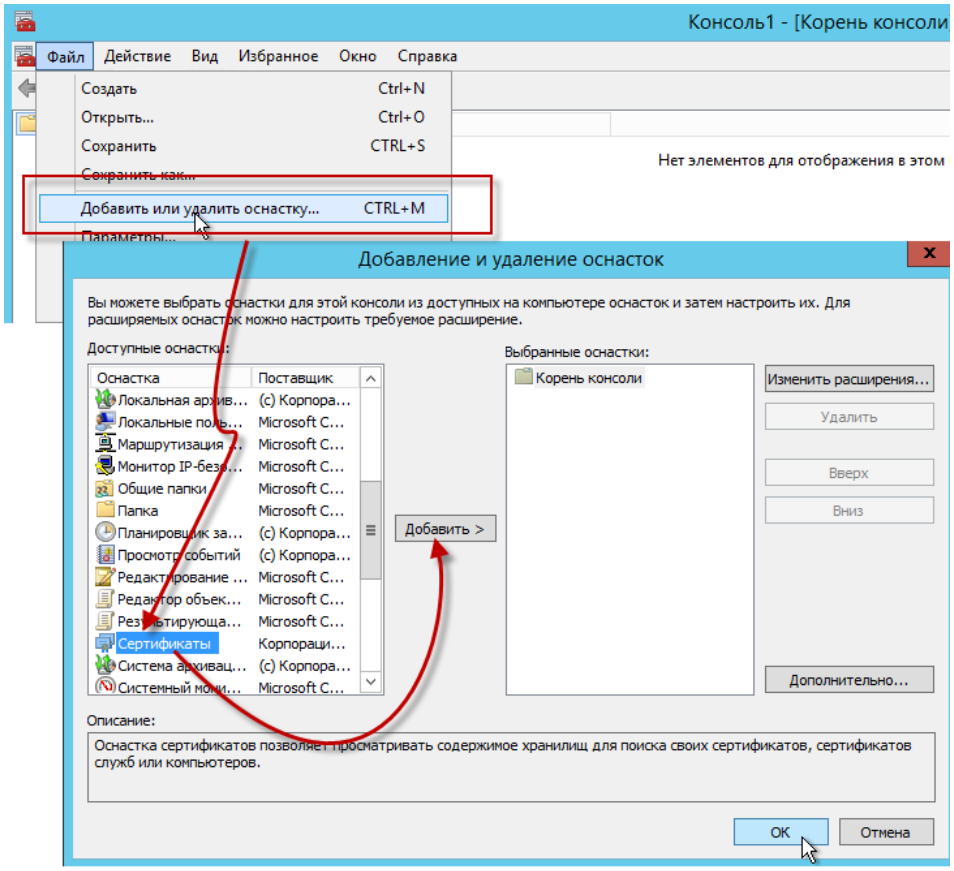

Рисунок 18. Добавление сертификата

В следующем окне выберите способ управления сертификатами: для «учетной записи компьютера» (*Рисунок 19*).

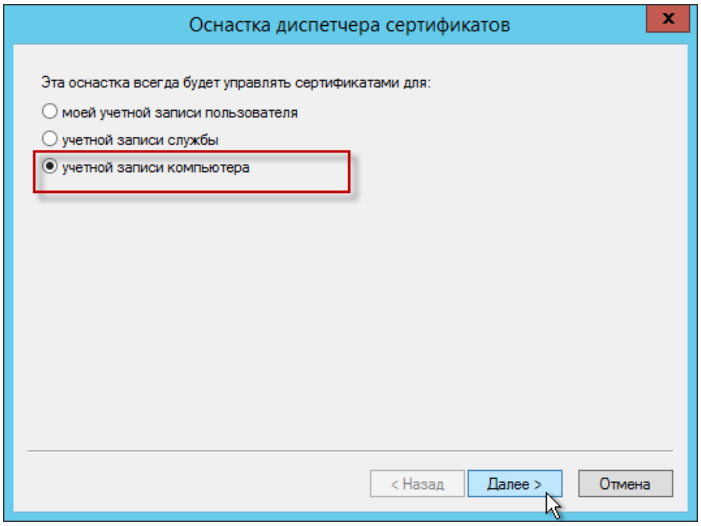

Рисунок 19. Способ управления сертификатами

Подтвердите, что будет осуществляться управление именно локальным компьютером (*Рисунок 20*).

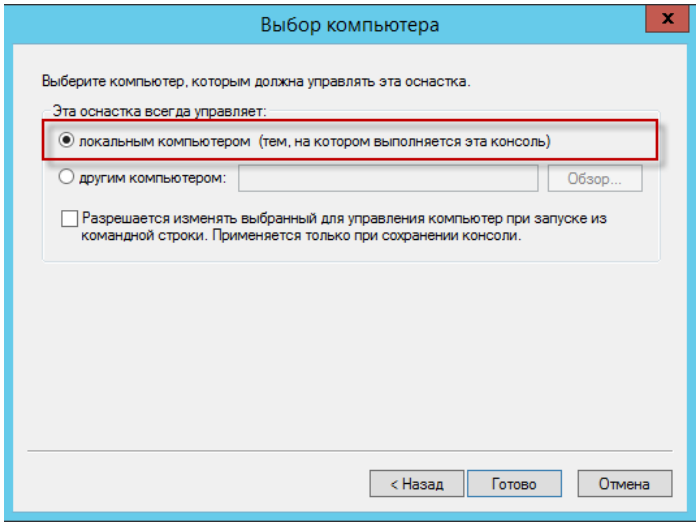

Рисунок 20. Выбор компьютера

Далее выберите пункт **«Запросы заявок на сертификат»**, найдите ваш запрос и выполните экспорт по правой клавише мыши.

В открывшемся окне мастера экспорта сертификатов выберите опцию «Да, экспортировать закрытый ключ». Отметьте флажком опцию **«Включить по возможности все сертификаты в путь сертификации»** и выполните экспорт *.pfx архива. В процессе экспорта необходимо указать путь выгрузки, а также придумать и подтвердить пароль в окне мастера (*Рисунок 21*).

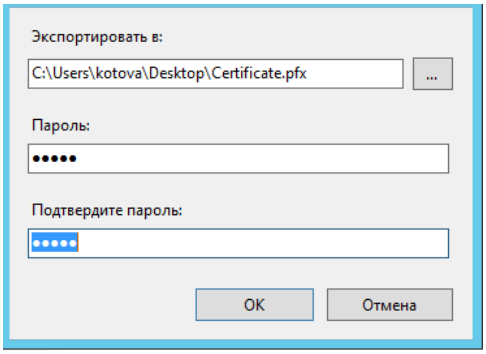

Рисунок 21. Экспорт сертификата

1.2.4. Экспорт сертификата с другого сервера

При переносе с другого сервера сертификат сначала необходимо выгрузить с данного сервера, чтобы потом импортировать на новый сервер (*Рисунок 22*).

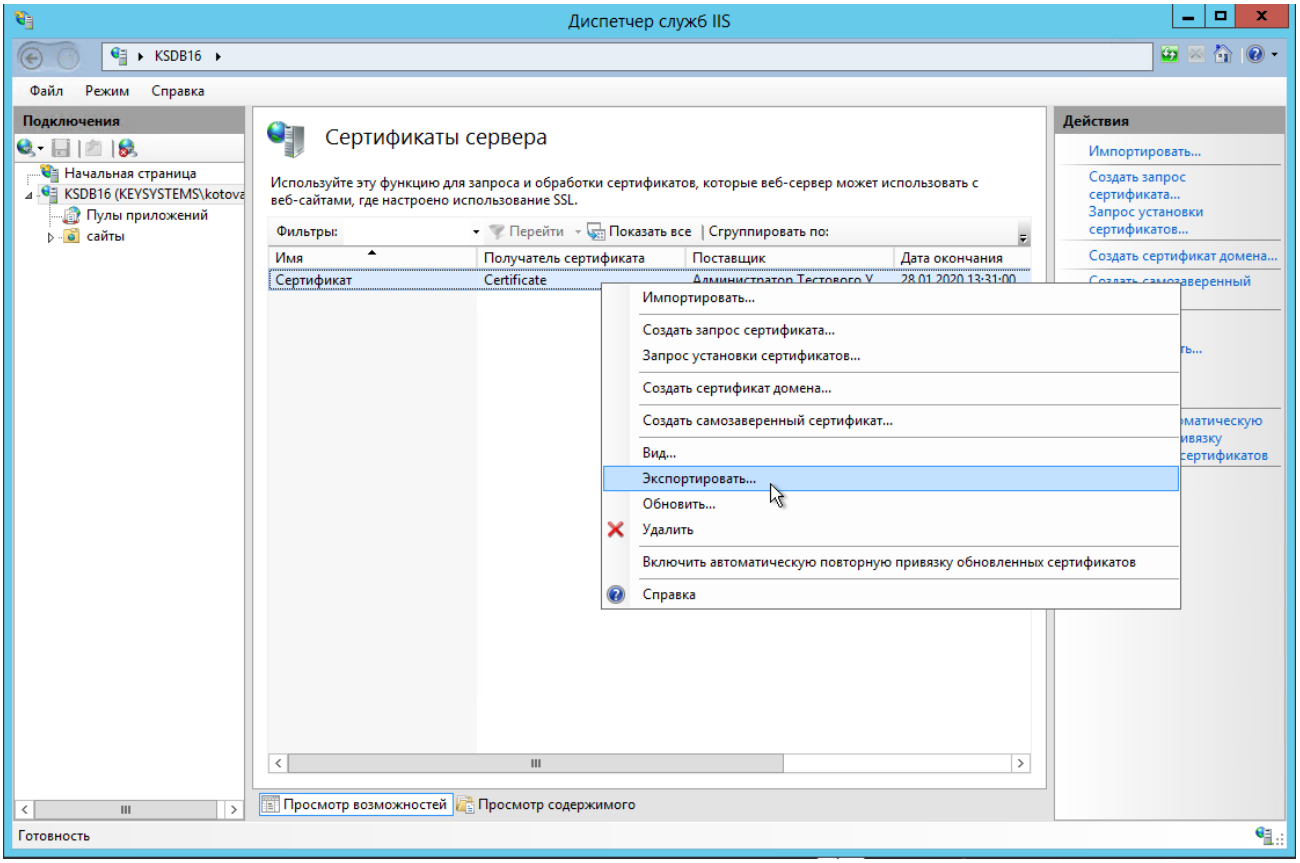

Рисунок 22. Экспорт сертификата

Аналогично описанию предыдущего пункта данного документа укажите путь выгрузки, а также придумайте и подтвердите пароль для данного сертификата (*Рисунок 23*).

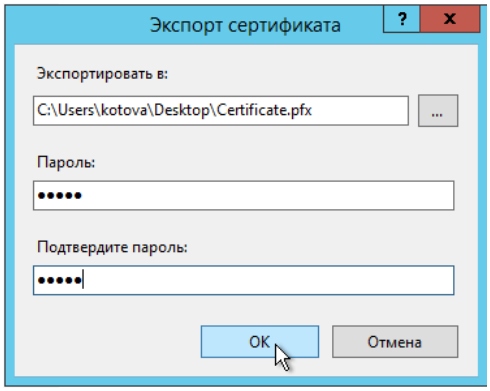

Рисунок 23. Задание пароля и пути выгрузки сертификата

Выгруженный сертификат отобразится в каталоге размещения (с соответствующим значком) и будет готов к последующему импорту.

1.2.5. Импорт сертификата на сервер

Для дальнейшей работы необходимо импортировать нужный сертификат. Откройте диспетчер IIS и перейдите в окно «Сертификаты сервера» (см. *Рисунок 5*). В открывшемся окне, в области **«Действия»**, выберите опцию **«Импортировать»**. В режиме «Обзор» выберите pfx архив (*Рисунок 24*).

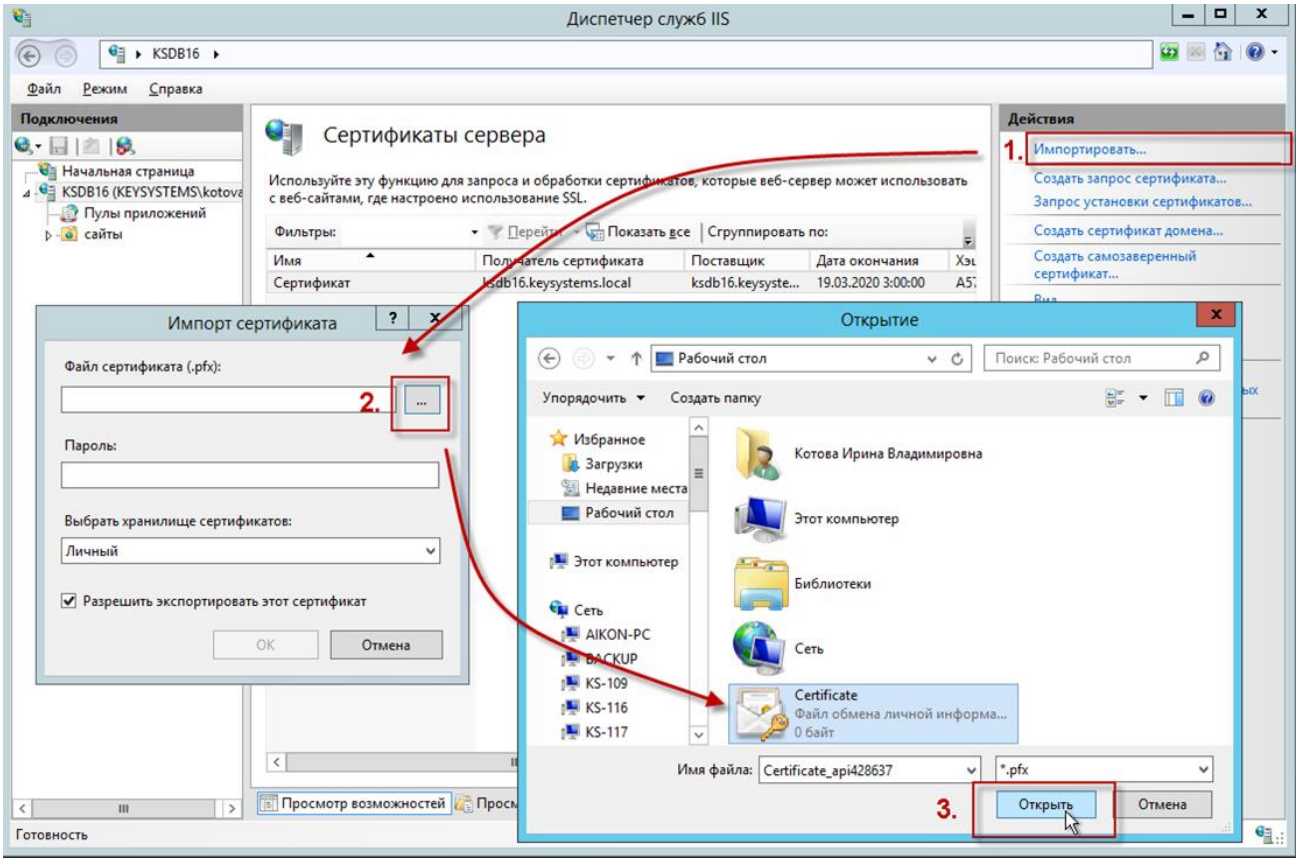

Рисунок 24. Подготовка к импорту сертификата

Пароль - укажите пароль (установленный при выгрузке);

Выбрать хранилище сертификатов - укажите значение «Личный», оно подойдет для стандартного размещения (значение «Размещение веб-служб» используется для SNI технологии).

Импорт будет выполнен по кнопке **[OK]** (*Рисунок 25*).

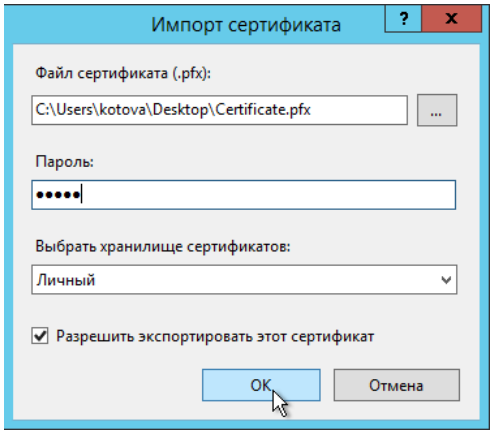

Рисунок 25. Импорт сертификата

1.3. Изменение привязки сайта

Далее выберите каталог «сайты» и по щелчку правой кнопкой мыши по соответствующей строке выберите в контекстном меню пункт «Изменить привязки» для настройки протокола https в IIS (*Рисунок 26*).

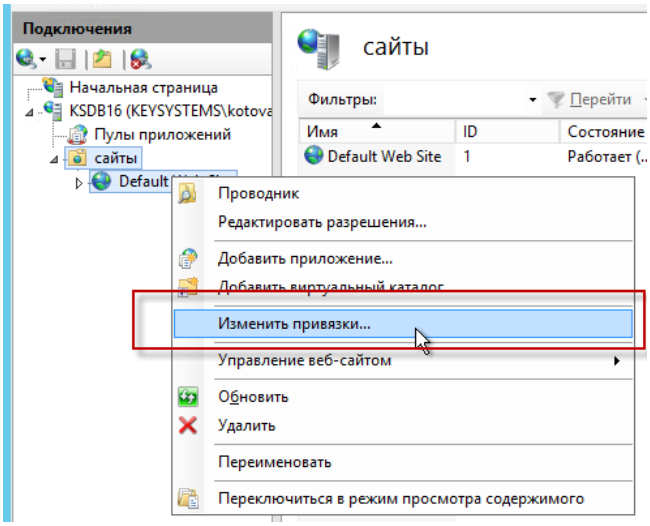

Рисунок 26. Настройка протокола https в IIS

Укажите для сайта (*Рисунок 27*):

- **Тип** - https и номер порта, по умолчанию, это порт 443 (убедитесь, что он открыт в брандмауэре);
- **Имя узла** - укажите полное название сайта;
- **SSL-сертификат** - выберите импортированный сертификат и сохраните настройки.

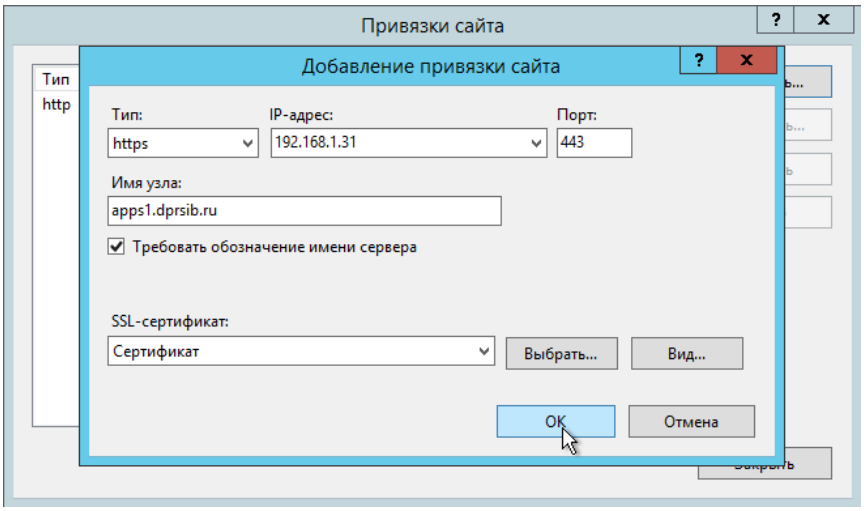

Рисунок 27. Добавление привязки сайта

В завершение проверьте сайт по протоколу HTTPS: в адресной строке должен отобразиться закрытый замочек. Это означает, что ssl сертификат установлен в IIS правильно (*Рисунок 27*).

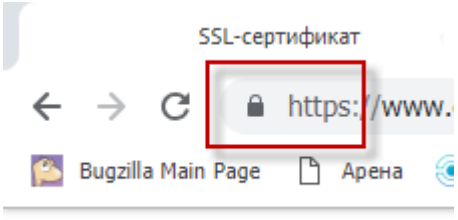

Рисунок 28. Проверка корректности установки сертификата

ГЛОССАРИЙ

Certificate Signing Reques (CSR) запрос - запрос на получение сертификата, который представляет собой текстовый файл, содержащий в закодированном виде информацию об администраторе домена и открытый ключ.

Secure Sockets Layer (SSL) - сертификат – уровень защищенных сокетов – уникальная цифровая подпись сайта. Такой сертификат нужен любым организациям, работающим с персональными данными для предотвращения несанкционированного доступа к информации.

HTTPS (HyperText Transfer Protocol Secure) – это расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTP, «упаковываются» в криптографический протокол SSL или TLS. По умолчанию HTTPS использует 443 TCP-порт (для незащищенного HTTP используется порт 80).

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Термин
1	2
ПК	Программный комплекс
CSR	Certificate Signing Reques, запрос на получение сертификата
SSL	Secure Sockets Layer, уровень защищенных сокетов
PFX	Формат, предназначенный для хранения ключевой пары, который распознается и используется браузерами и почтовыми агентами
УЦ	Удостоверяющий центр

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер версии	Примечание	Дата	ФИО исполнителя
01	Начальная версия	20.03.2019	Котова И.В.
02	Документ доработан по вопросам пользователей (добавлено описание импорта, преобразования сертификатов). Изменена структура документа	04.04.2019	Котова И.В.