УТВЕРЖДАЮ
Генеральный директор
ООО «Кейсистемс»
_____ А. А. Матросов
«___» _____ 2020 г.

ПРОГРАММНЫЙ КОМПЛЕКС «БЮДЖЕТ-СМАРТ»

ВЕРСИЯ 20.01

Руководство администратора

Работа с оправдательными документами

ЛИСТ УТВЕРЖДЕНИЯ

Р.КС.02120-02 32 08-ЛУ

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

СОГЛАСОВАНО
Заместитель генерального директора
ООО «Кейсистемс»
_____ Е. В. Федоров
«___» _____ 2020 г.

Руководитель ДПиРСИБ

_____ Д. В. Галкин
«___» _____ 2020 г.

2020

Литера А

информационные технологии КЕЙСИСТЕМС

ПРОГРАММНЫЙ КОМПЛЕКС «БЮДЖЕТ-СМАРТ»

ВЕРСИЯ 20.01

Руководство программиста

Работа с оправдательными документами

Р.КС.02120-02 32 08

Листов 42

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

2020

Литера А

АННОТАЦИЯ

Настоящий документ является частью руководства администратора программного комплекса «Бюджет-СМАРТ» (далее – «программный комплекс») версии 20.01 по автоматизации процесса проектирования, исполнения и анализа бюджетов субъектов Российской Федерации, закрытых автономно-территориальных образований и муниципальных образований.

Документ содержит описание сервиса первичных документов – вспомогательной службы, обеспечивающей дополнительную проверку подлинности документов с помощью прикрепленных к ним оправдательных документов.

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

Порядок выпуска обновлений руководства

Выход новой версии программного комплекса сопровождается обновлением руководства только при наличии в версии значительных изменений режимов, описанных в руководстве, разработки новых режимов или изменении общей схемы работы. Если таких изменений версия не содержит, то остается актуальным руководство от предыдущей версии, дополненное информацией об изменениях, содержащихся в новых версиях.

Перечень изменений новых версий программного комплекса содержится в сопроводительных документах к версиям. Информация об изменениях руководства программиста 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 пользователя содержит описание работы с сервисом оправдательных документов, применяющимся для прикрепления к документам файлов произвольных форматов (так называемых оправдательных документов, являющихся основанием и подтверждением соответствующих электронных документов), а так же для работы в режиме «Сохраненные отчеты» в финансовых органах, органах государственной и муниципальной власти, государственных и муниципальных учреждениях.

Функциональные возможности

Сервис по работе с ОД позволяет сохранить в БД первичные документы путем сканирования и электронного приема. При этом сервис поддерживает следующие функции:

- возможность прикрепления к электронным документам отсканированных копий первичных документов;
- сохранение документов произвольного формата;
- возможность быстрого отображения в специализированном интерфейсе сервиса первичных документов
- поддержка работы с электронной подписью (далее – ЭП), в том числе возможность наложения нескольких ЭП разного уровня на один документ.

Уровень подготовки пользователя

Для успешного освоения материала, изложенного в руководстве пользователя, 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 (Linux) на уровне квалифицированного пользователя;
- умение свободно осуществлять базовые операции в стандартных приложениях Windows (Linux).

Перечень эксплуатационной документации

В *таблице 1* представлен список пользовательской документации в части описания блока задач «Администрирование».

Таблица 1. Перечень эксплуатационной документации

№ п/п	Код документа	Наименование документа
1	2	3
1	Р.КС.02120-02 32 01	Администрирование комплекса (ссылка на сайт)
2	Р.КС.02120-02 32 02	Установка Бюджет-СМАРТ (ссылка на сайт)
3	Р.КС.02120-02 32 03	Установка сервисов Бюджет-СМАРТ на ОС WINDOWS (ссылка на сайт)
4	Р.КС.02120-02 32 04	Управление сервисами СМАРТ/WEB (ссылка на сайт)

№ п/п	Код документа	Наименование документа
1	2	3
5	Р.КС.02120-02 32 05	Настройка SSL на IIS (ссылка на сайт)
6	Р.КС.02120-02 32 06	Единый Центр контроля (ссылка на сайт)
7	Р.КС.02120-02 32 07	Электронный обмен документами с применением электронно-цифровой подписи (ссылка на сайт)
8*	Р.КС.02120-02 32 08	Работа с оправдательными документами
* 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. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

1.1. Назначение сервиса ОД

Сервис ОД предназначен для прикрепления к электронным документам, участвующим в бизнес-процессах автоматизированных систем, файлов произвольных форматов (так называемых оправдательных документов, являющихся основанием и подтверждением соответствующих электронных документов), а так же для работы в режиме «Сохраненные отчеты».

1.2. Условия применения сервиса ОД

Сервис применяется в финансовых органах, органах государственной и муниципальной власти, государственных и муниципальных учреждениях.

2. УСТАНОВКА СЕРВИСА ОД

2.1. Порядок установки

ПК «Бюджет-СМАРТ» взаимодействует с различными сервисами, в том числе и с сервисом оправдательных документов (UploadService), который используется:

- для работы с ОД,
- для проверки ЭП документов и файлов,
- для применения в режиме «Сохраненные отчеты».

Сервис ОД может располагаться в любом сегменте сети при условии наличия доступа со стороны клиентских мест по порту 80. Сервис оправдательных документов (ОД) устанавливается как на сервере IIS, так и на отдельном сервисе.

Для обеспечения удаленных подключений к БД ПК «Бюджет-СМАРТ» и сервису ОД также предоставляется доступ со стороны Web-сервера с «тонким клиентом». Web-сервис устанавливается на компьютер, на который ранее был установлен диспетчер служб IIS. На той же машине должен быть установлено программное обеспечение Криптопровайдера, обеспечивающее работу с ЭП по алгоритмам ГОСТ РФ.

К сервису ОД обращается клиентское приложение, установленное на компьютере пользователя, либо Web-сервис (при удаленном подключении). Для сервиса ОД рекомендуется создать отдельный пул приложений.

Чтобы установить «Сервис оправдательных документов» запустите пакет установщика Keysystems.UploadWebService_ X.X.XXXX.msi сервиса ОД Убедитесь, что все необходимые перечисленные в окне компоненты установлены на компьютере. Нажмите кнопку **[Далее]** (*Рисунок 1*)

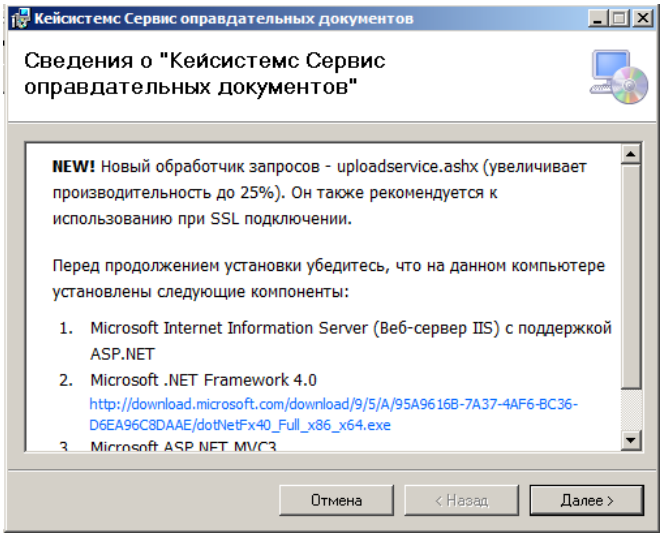

Рисунок 1. Мастер установки сервиса оправдательных документов

Ознакомьтесь с условиями лицензионного соглашения и отметьте опцию **[Принимаю]** Нажмите кнопку **[Далее]** (*Рисунок* 2).

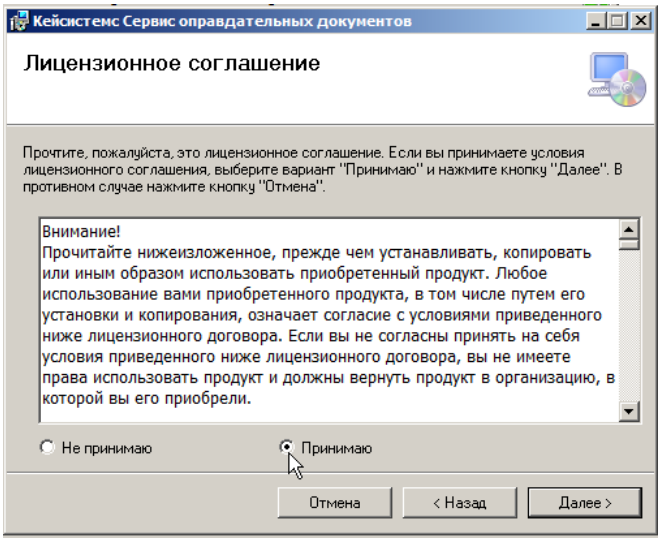

Рисунок 2. Лицензионное соглашение

В окне выбора папки для установки будет указан путь к каталогу по умолчанию. При необходимости данное расположение можно изменить по кнопке **[Обзор]** (*Рисунок 3*).

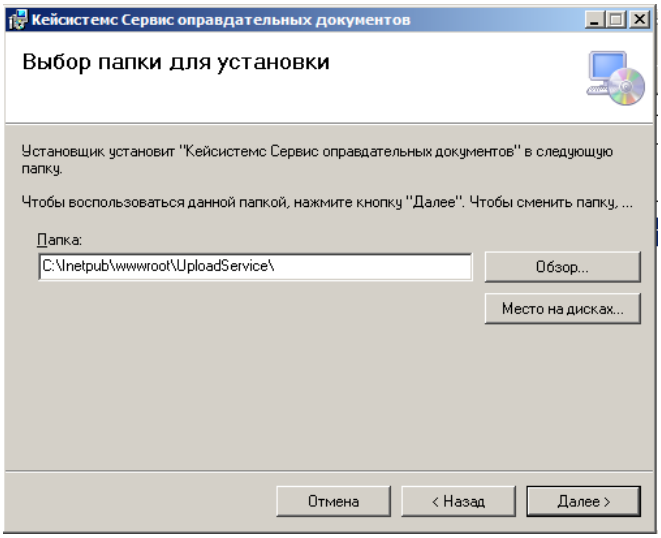

Рисунок 3. Выбор папки для установки

При выборе каталога по кнопке **[Место на дисках]** доступна опция оценки свободного места на дисках компьютера (*Рисунок 4*).

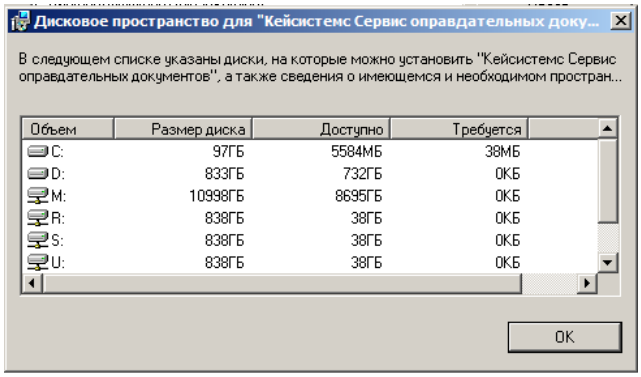

Рисунок 4. Проверка дискового пространства

Установка осуществляется на выбранный диск. (*Рисунок 5*).

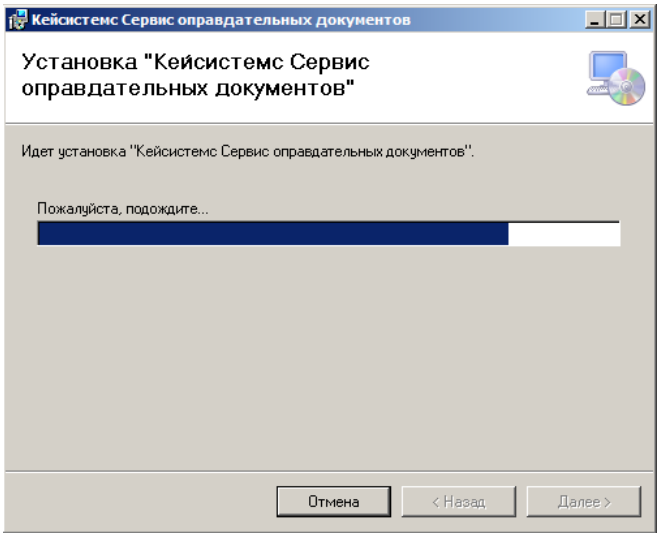

Рисунок 5. Ход установки

Далее выбираются параметры виртуального каталога UploadService.

В открывшемся окне **«Контроль данных»** нажмите кнопку **[Да]**.

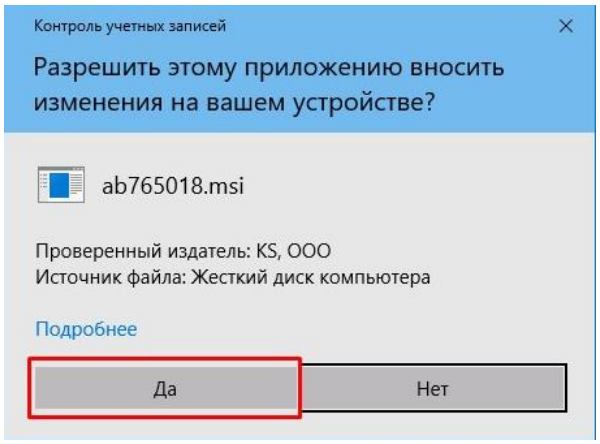

Рисунок 6. Контроль учетных записей

В окне **«Создание веб приложения»** указаны следующие значения по умолчанию (их необходимо оставить без изменений): в поле **Веб-узел** указано «Default Web Site», в поле **Виртуальный каталог** - название каталога «UploadServise». В поле **Пул приложений** указан ранее созданный пул «UploadServise». Нажмите кнопку **[Далее]** (*Рисунок 7*).

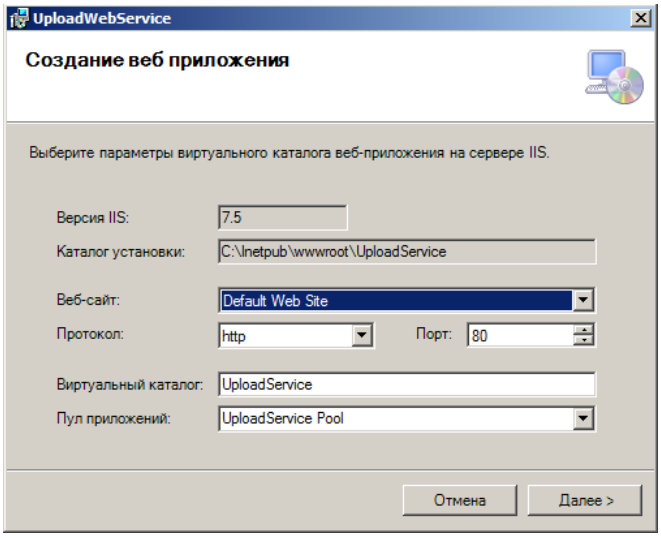

Рисунок 7. Создание веб приложения

В окне **«Расположение файлов»** заполните следующие поля (*Рисунок 8*):

Выберите в поле **Тип хранилища** значение «FileSystem», в поле **Путь** укажите сетевой путь или каталог (для случая, когда каталог размещается на том же компьютере, что и сервис ОД, по умолчанию – «App_Data\Uploade»). Если каталог ОД и сервис ОД размещены на разных серверах, то в группе полей «**Учетные данные для доступа к сетевому пути»** укажите имя пользователя и пароль доступа к каталогу ОД. Нажмите кнопку **[Далее]**.

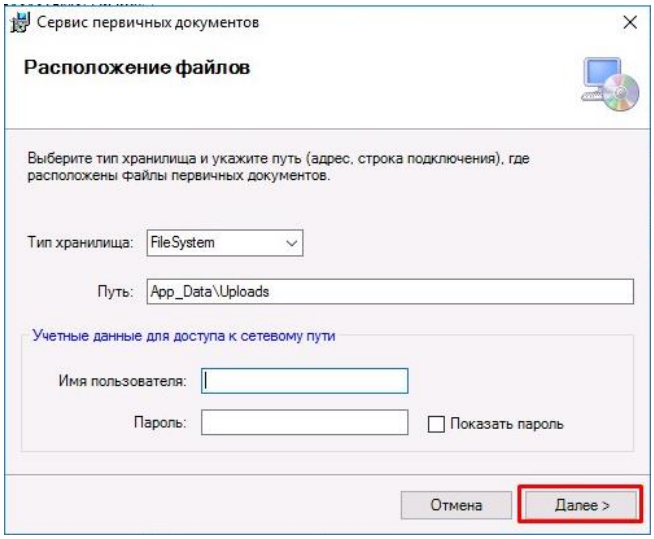

Рисунок 8. Расположение файлов

В окне **«Параметры авторизации»** заполните имя и пароль учетной записи (*Рисунок 9*). Нажмите кнопку **[Далее]**.

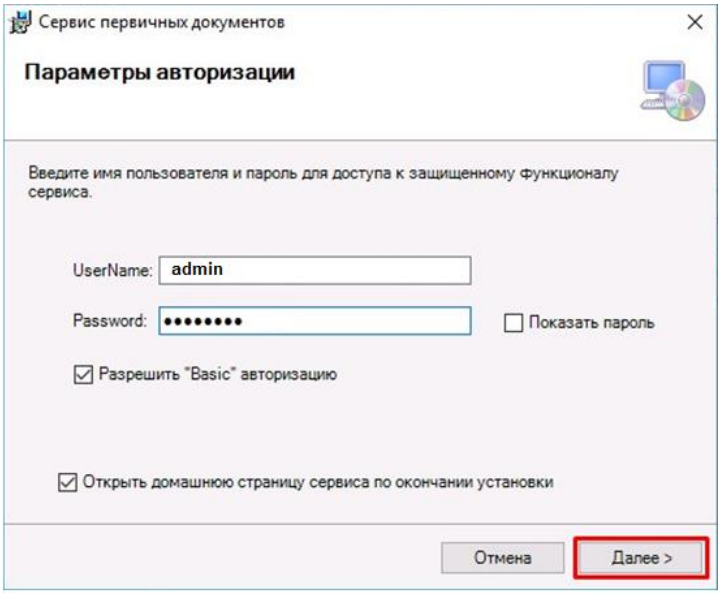

Рисунок 9. Параметры авторизации

В окне завершения установки нажмите **[Завершить]**. (*Рисунок 10*)

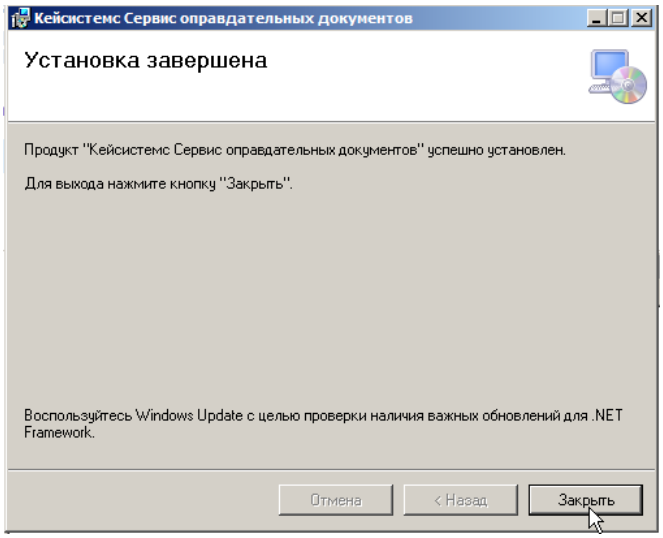

Рисунок 10. Установка завершена

По завершении установки автоматически открывается окно домашней страницы сервиса, что означает, что установка была выполнена корректно.

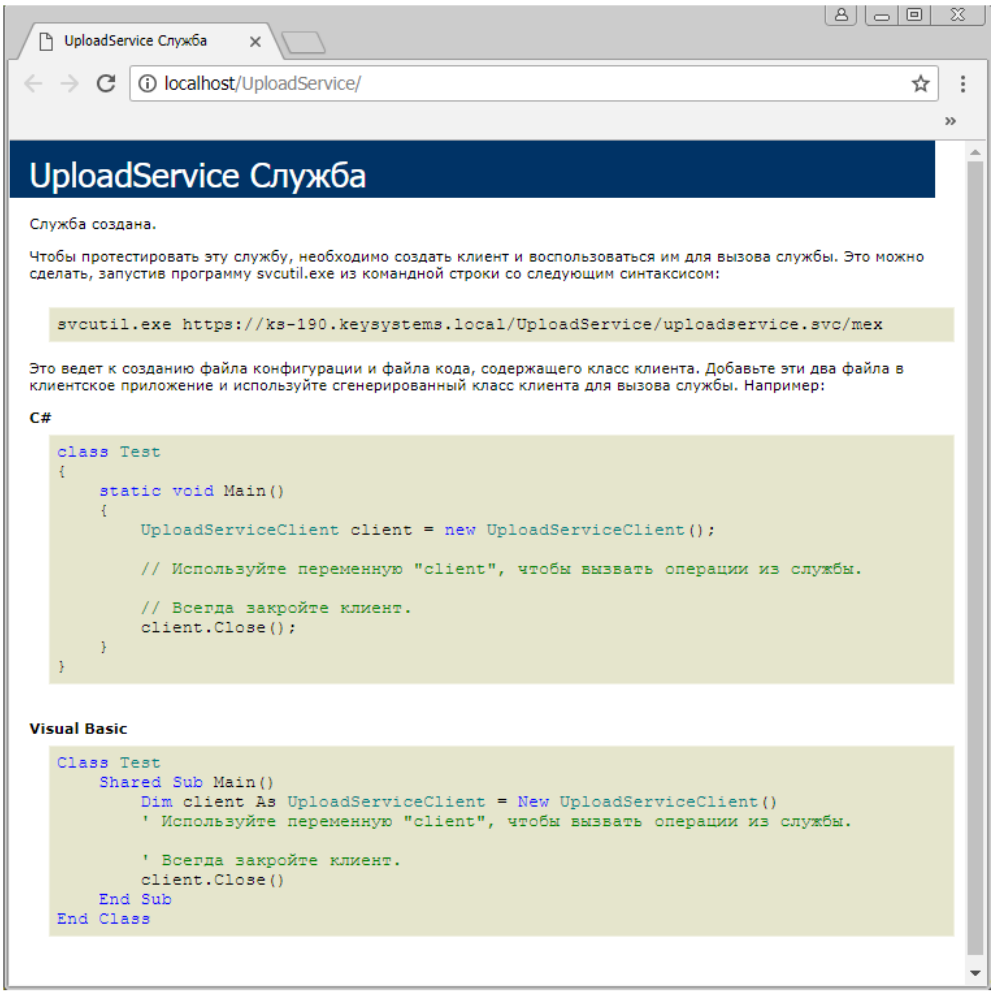

Рисунок 11. Проверка работоспособности

Аналогичным способом проверяются все установленные веб-сервисы. В адресной строке набирается соответствующий адрес, например: https://localhost/updateservice/ или https://localhost/budgetsmart - веб-сервис ПК «Бюджет-СМАРТ».

После установки сервиса необходимо убедиться, что пользователю IIS, от имени которого выполняется пул UploadService, предоставлены полные права на папку uploads\. Пользователя по умолчанию можно сменить в web.config в разделе <system.web> , поле <identity userName =...>. Пользователь по умолчанию - IIS_IUSRS - это встроенная группа, используемая службами IIS для Win7 и выше (для более ранних - это пользователь IIS_WPG).

Если в свойствах пула приложений сервиса ОД (при наличии у него персонального пула приложений) указать учетную запись LocalSystem, то у сервиса ОД будут права на чтение/запись по любому локальному пути (в пределах сети, в которой расположен компьютер IIS).

При возникновении ситуации, когда ОД прикрепляются к документам, но не открываются для просмотра, рекомендуется убедиться, что в настройках IIS расширения этих файлов входят в список типов MIME

3. ОПИСАНИЕ ОПЕРАЦИЙ

В данном разделе описывается работа с сервисом ОД в ПК «Бюджет-СМАРТ».

3.1. Настройки в ПК «Бюджет-СМАРТ»

Группа настроек, определяющих месторасположение хранилища для первичных (оправдательных) документов (ОД), прилагаемых к документам комплекса (сканы, текстовые документы и т.д.), в т.ч. при электронном приеме, а так же для хранения отчетов и произвольных документов размещена в каталоге **«Первичные документы»**. Все настройки данной группы устанавливаются как глобально, так и индивидуально, для выбранной учетной записи пользователя (*Рисунок 12*).

МЕНЮ НАСТРОЙКИ =>НАСТРОЙКИ => ПЕРВИЧНЫЕ ДОКУМЕНТЫ

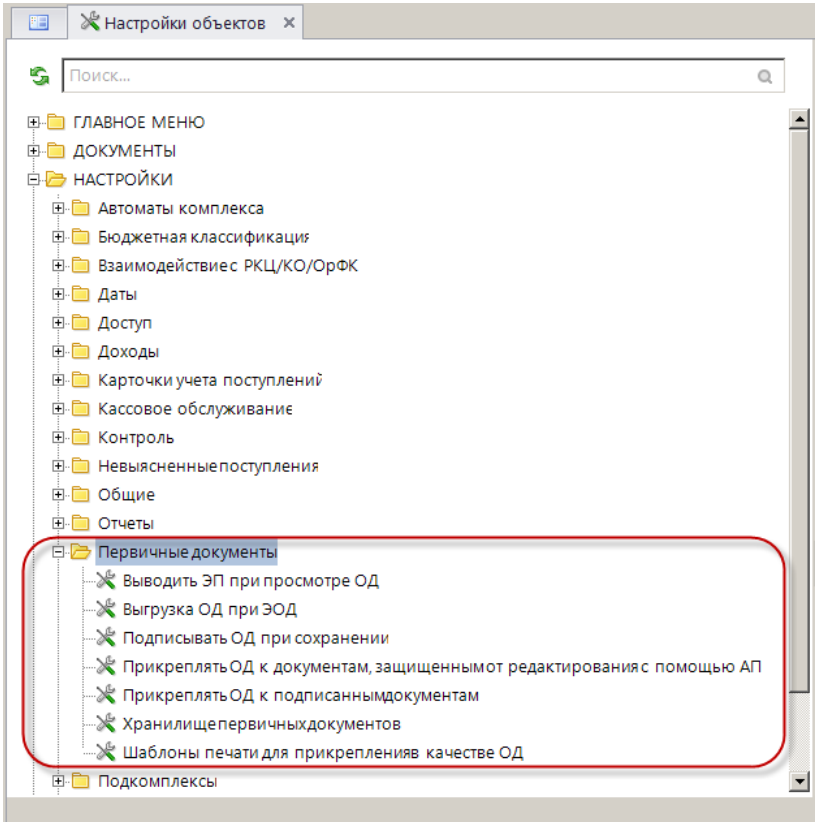

Рисунок 12. Настройки для обработки первичных документов

- **Выводить ЭП при просмотре ОД** - настройка определяет отображение ЭП при просмотре ОД;
- **Выгрузка ОД при ЭОД** - настройка позволяет отметить условия, при выполнении которых с документами при ЭОД будут выгружены и прикрепленные ОД, доступны следующие опции для отбора:
  - Из текущего документа;
  - Из заявок, по которым сформированы п/п;
  - Из действующего на дату платежа БО;
  - Из всех БО для текущего платежа;
  - Из действующего на дату платежа ДО;
  - Из всех ДО для текущего платежа;

  - Запрет повторной выгрузки;
  - Из реестров соглашений для БО;
- **Подписывать ОД при сохранении** - настройка позволяет автоматически накладывать ЭП на сохраняемые оправдательные документы;
- **Прикреплять ОД к документам, защищенным от редактирования с помощью АП** – настройка определяет возможность прикрепления ОД к документам, на которых установлен аналитический признак, запрещающий редактирование;
- **Прикреплять ОД к подписанным документам** - настройка определяет возможность манипулирования ОД при наличии ЭП на самом документе. При значении «нет» запрещено снимать ЭП с ОД, удалять ОД, добавлять ОД (при наличии ЭП на самом документе);
- **Хранилище первичных документов** - группа настроек для указания способа и места размещения файлов первичных документов (сканы, текстовые документы и т.п.), а так же отчетов (режим «Сохраненные отчеты») (*п. 3.2*).
- **Шаблоны печати для прикрепления в качестве ОД** – шаблоны печати, хранящиеся на сервере, также доступны для прикрепления в качестве ОД. Для отбора таких шаблонов в данной настройке отметьте нужные файлы в окне списка шаблонов (*Рисунок 13*).

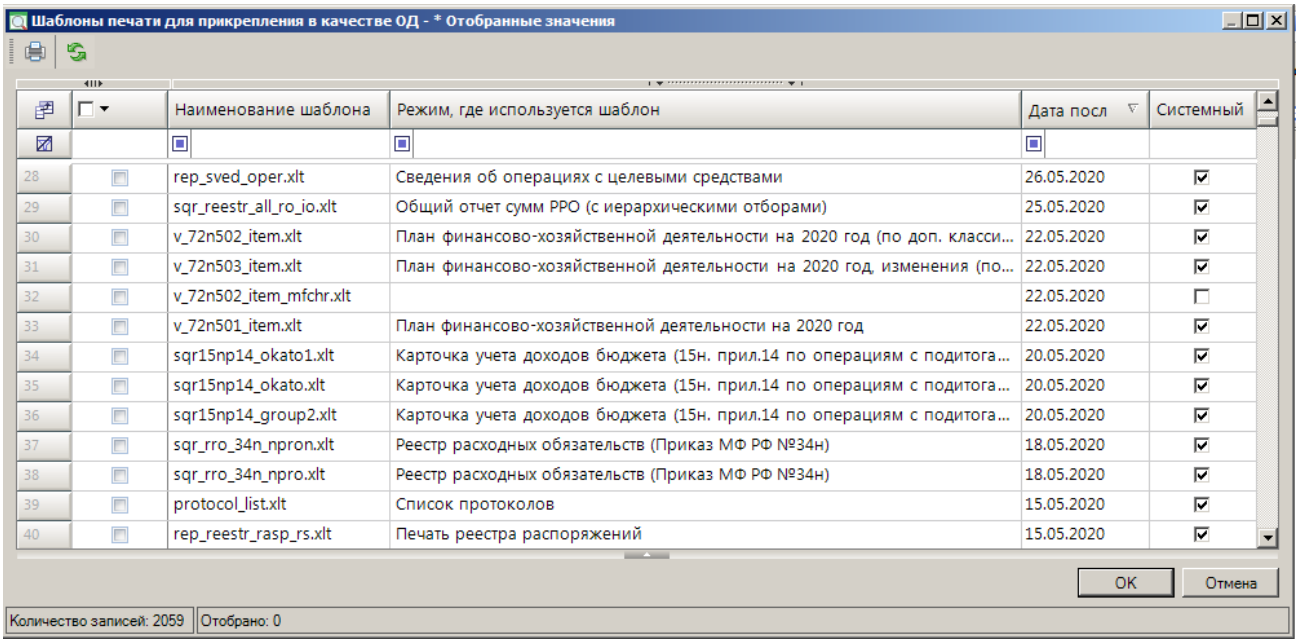

Рисунок 13. Шаблоны печати, прикрепляемые в качестве ОД

3.2. Хранилище первичных документов

Прикрепление ОД осуществляется в режиме списка документов по кнопке «Оправдательные документы», либо ОД принимаются электронно, одновременно с платежными поручениями. Хранение первичных документов задается рядом настроек «Хранилище первичных документов» (*Рисунок 14*).

ГЛАВНОЕ МЕНЮ => НАСТРОЙКИ => НАСТРОЙКИ => ПЕРВИЧНЫЕ ДОКУМЕНТЫ => ХРАНИЛИЩЕ ПЕРВИЧНЫХ ДОКУМЕНТОВ

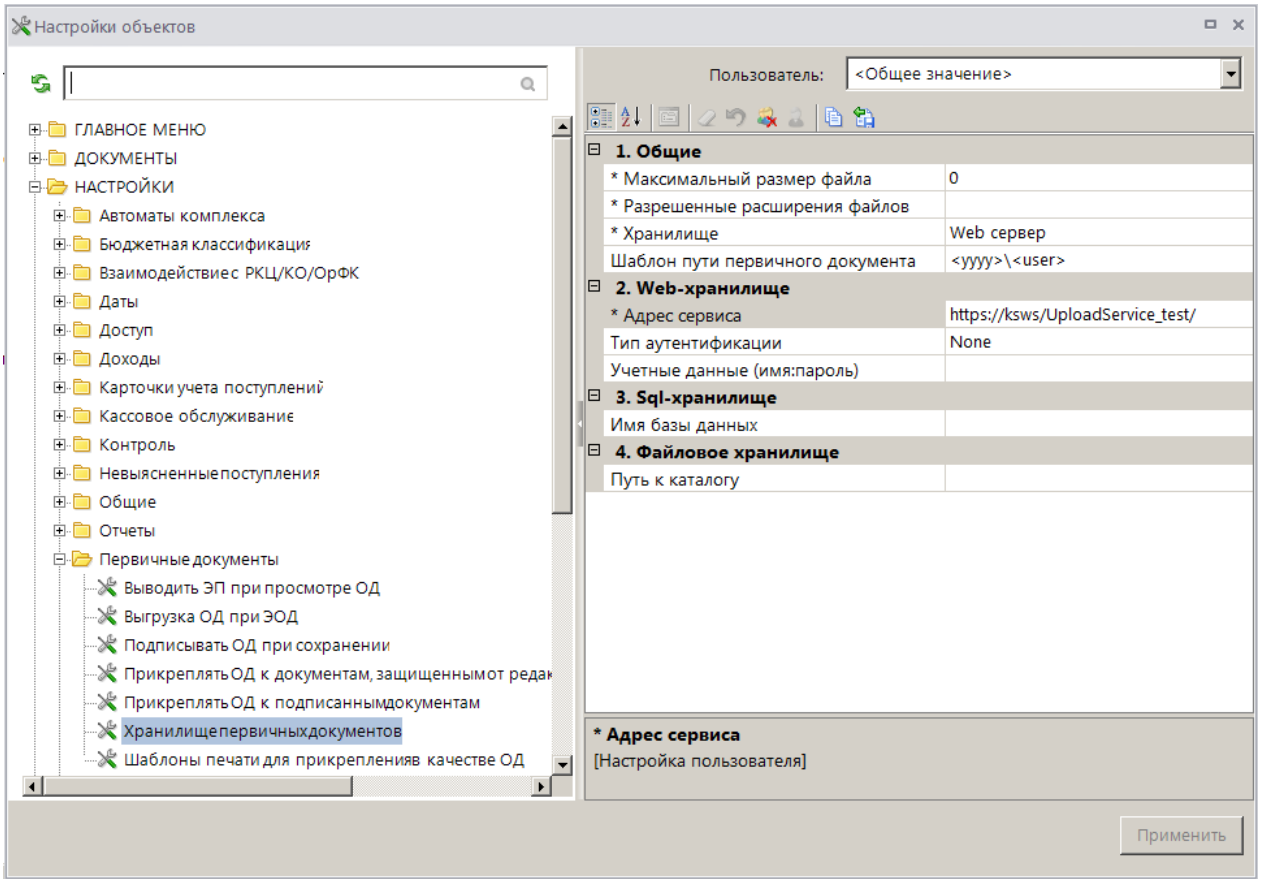

Рисунок 14. Настройки хранения первичных документов

Группа настроек «Общие»

- **Максимальный размер файла** - ограничение на размер файлов ОД, в байтах. Значение «0» или пусто означает «без ограничений». Пример значения: 10485760 - ограничение в 10 МБ
- **Разрешенные расширения файлов** – перечень расширений, указывается через запятую или точку с запятой, масок разрешенных расширений файлов ОД. Значение «*» или пусто означает «без ограничений» (любое расширение). Для каждого расширения через двоеточие можно указать максимальный размер в байтах. Пример значения: pdf,jp*,bmp:2097152,png - разрешены файлы вида *.pdf, *.jpg, *.jpeg, *.bmp, *.png , причем для bmp установлено ограничение в 2МБ
- **Хранилище** - место хранения ОД. Возможные значения:
  - **Не используется** - хранение ОД не применяется, кнопка работы с ОД в списке документов неактивна, режим «Сохранённые отчеты» не работает.
  - **WEB сервер** - хранилище управляется специализированным сервисом первичных/оправдательных документов (сервис ОД), развернутым на сервере IIS. Адрес сервиса задается в настройке «Адрес сервиса» (*см. далее*). При включении настройки *«Проверять ЭЦП на Сервисе первичных документов»* проверка ЭП как документов так и ОД осуществляется средствами сервиса ОД, что увеличивает производительность системы.
  - **SQL сервер** - хранилище организовано в отдельной базе данных. Имя базы задается в настройке «Имя базы данных» (*см. далее*).

– **Файл сервер** - хранилище организовано на сетевом диске в заданной папке. Путь задается в настройке «Путь к каталогу» (*см. далее*). Данное хранилище применимо только для локальных пользователей комплекса.

– **Шаблон пути первичного документа** - путь хранения прикрепляемых оправдательных документов относительно хранилища. В результате применения настройки файлы в хранилище первичных документов будут располагаться по пути: {uploads}\{шаблон}\<дата в формате yyyymmdd>\<имя файла ОД>, где {uploads} - папка uploads\ сервиса ОД; {шаблон} - значение данной настройки. В настройке указывается строка, которая содержит элементы, разделенные символом '\'. Элемент может быть как обычным именем папки, так и выражением в угловых скобках <> вида:

  – <database> - имя базы,

  – <user> - имя пользователя

  – <yyyymmdd> - текущая дата в заданном формате. Содержит в любой комбинации буквы 'y', 'm', 'd' и символ '.' (точка). Здесь формат: yyyy - 4 цифры года, mm - 2 цифры месяца, dd - 2 цифры числа. Другой вариант использования: <dd.mm.yyyy> или <yyyy> и т.д. Так же в качестве разделителя кроме символа «.» (точка) можно использовать «-» (тире) и «_» (подчеркивание).

  – Значение настройки по умолчанию: <yyyy>\<user>. Если настройка не задана, то используется имя пользователя <user>.

Группа настроек «WEB-хранилище»

– **Адрес сервиса (на пользователя)** - путь к сервису первичных/оправдательных документов (сервис ОД). Требуется установленный сервис оправдательных документов. При этом общее значение настройки должно указывать путь к хранилищу первичных документов (сервису ОД) в локальной сети - по нему будет обращаться к первичным документам сервер ключей (при отключенной настройке *«Проверять ЭЦП на Сервисе первичных документов»*). Внешний адрес (путь) указывается для удаленных пользователей индивидуально. В случае применения нескольких каналов (адресов) подключения к IIS (основной и резервный), рекомендуем применять параметр UseAppServiceHost в файле конфигурации сервиса приложений. Пример значения для внешних пользователей: https://mf.chuv.ru/UploadService/UploadService.svc. Пример значения для локальных пользователей к тому же сервису ОД: https://serveriis/UploadService/UploadService.svc, где «serveriis» - имя компьютера, на котором развернут сервис ОД.

– **Тип аутентификации** - способ проверки подлинности пользователя при подключении к сервису ОД (определяется настройками IIS).

– **Учетные данные (имя:пароль)** - логин и пароль УЗ для подключения к сервису ОД (если требуется).

Группа настроек «SQL хранилище»

– **Имя базы данных** - база данных SQL, в которой будут храниться ОД. Формат значения: <имя_SQL_сервер>.<имя_базы>. Имя SQL сервера может содержать символ «\». База должна иметь определенную структуру, для ее создания применяется специальный скрипт. Пример значения настройки: xandra\2016.fstorage_jpg , где «xandra\2016» - имя SQL сервера, «fstorage_jpg» - имя базы данных. При прописывании базы в данной настройке к ней получают доступ все активные (не помеченные красным фоном) пользователи рабочей БД. Если новая учетная запись пользователя добавлена

уже после заполнения данной настройки, в период отсутствия/недоступности базы ОД, то после восстановления (появления) базы ОД такие УЗ следует пересохранить для получения прав на подключение к базе ОД.

Группа настроек «Файловое хранилище»

– **Путь к каталогу** – в настройке указывается путь (как правило, сетевой) к каталогу хранения ОД. Путь не должен содержать символов «пробел». Пример значения настройки: \\xenix\bks\jpg_pp\.

3.3. Работа с оправдательными документами

Оправдательные документы прикрепляются к электронным документам, сохраненным в БД в режиме **«Работа с оправдательными документами»**, который вызывается по кнопке **Оправдательные документы** панели инструментов в списках документов (*Рисунок 15*). При этом для платежных поручений, заявок на кассовый расход - сразу показываются ОД для связанных документов БО.

НАВИГАТОР => ДОКУМЕНТЫ => ДОКУМЕНТ

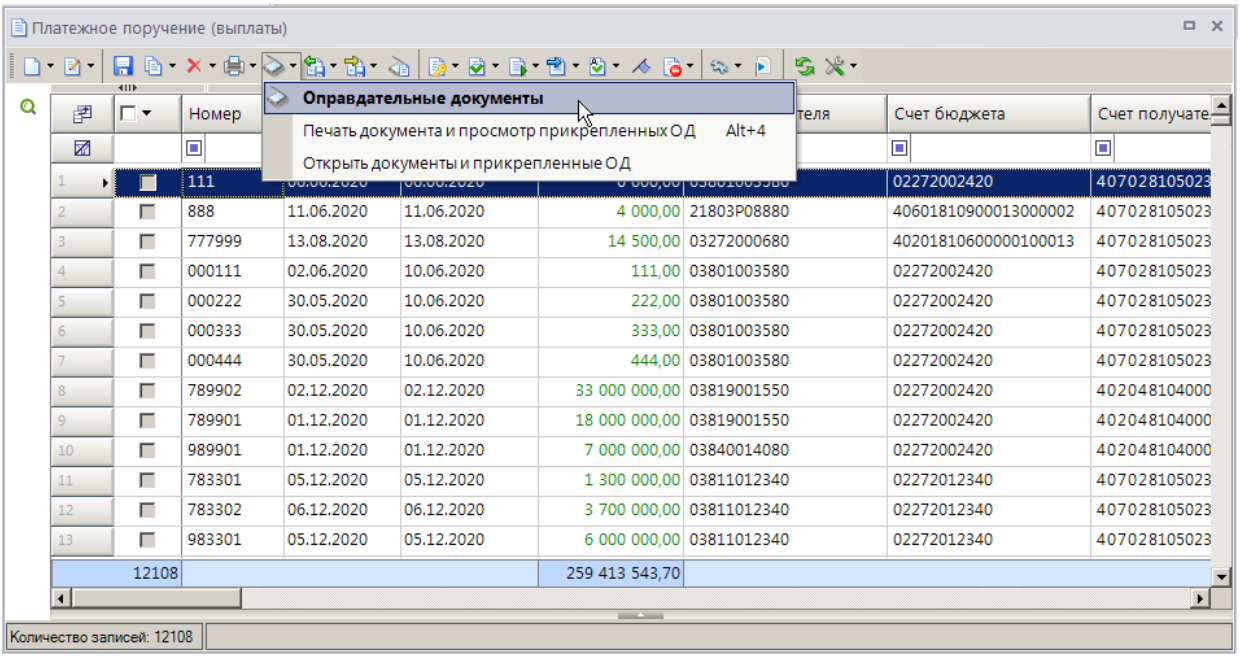

Рисунок 15. Переход в режим работы с ОД

В открывшемся окне режима работы с оправдательными документами нажмите кнопку **Добавить** и выберите файл ОД допустимого формата (*настройка «Разрешенные расширения файлов», см. пп. 3.2*) для загрузки (*Рисунок 16*).

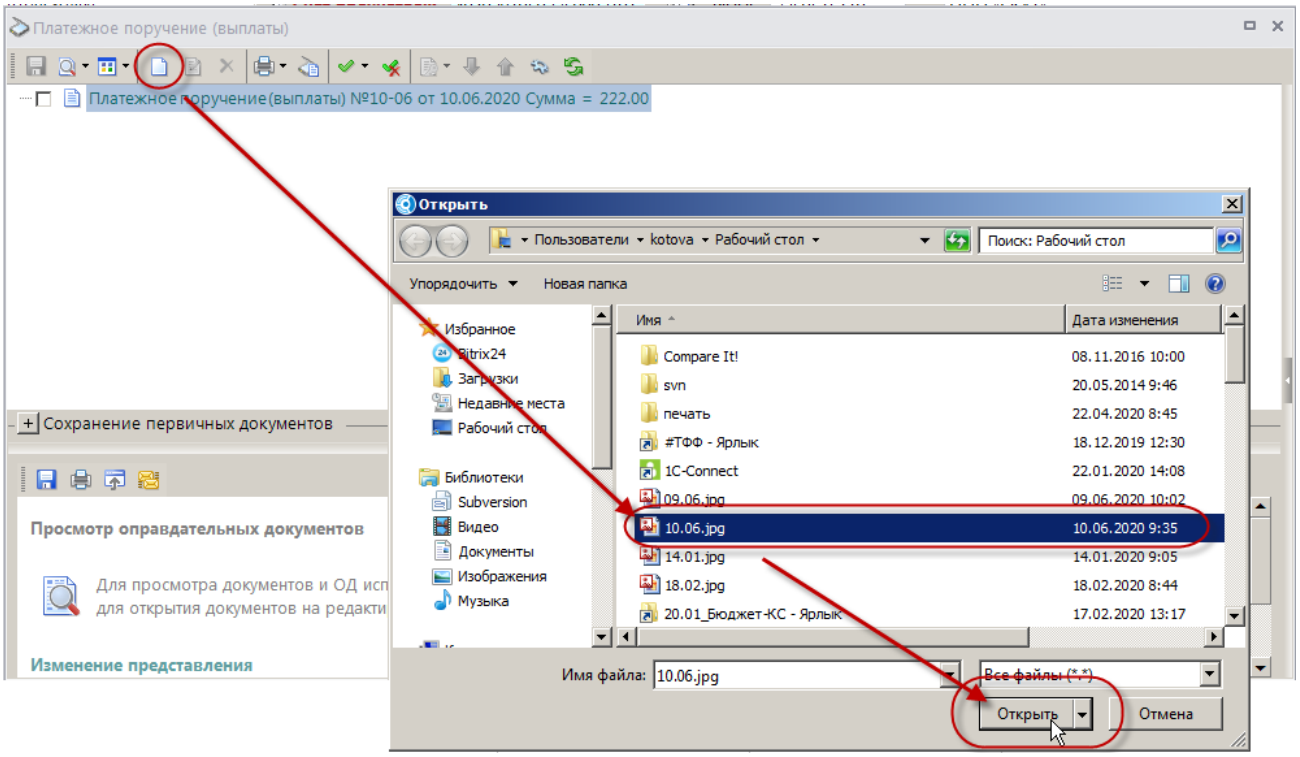

Рисунок 16. Прикрепление оправдательного документа

По кнопке **[Открыть]** файл будет загружен, затем его следует передать на сервер по кнопке **Передать документ на сервер** (*Рисунок 17*).

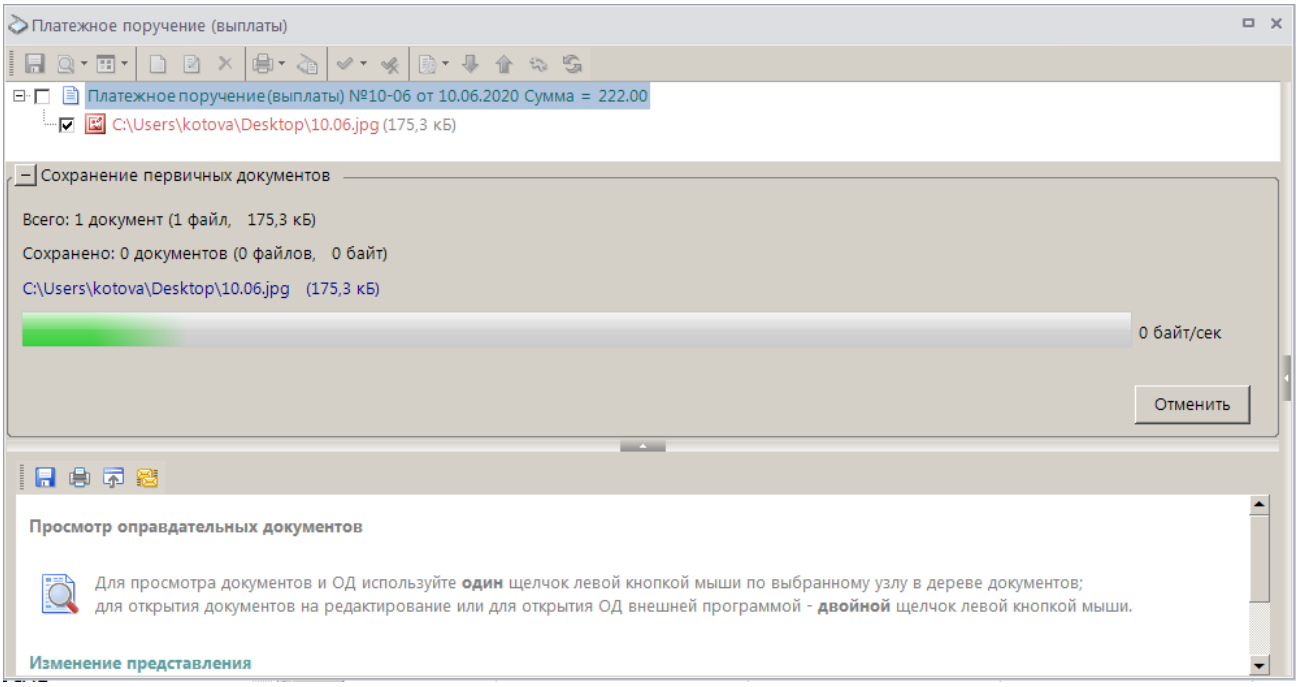

Рисунок 17. Передача ОД на сервер

При подключении к ПК оборудования для сканирования документов, доступно прикрепление ОД, полученных путем сканирования по кнопке **Сканировать**.

Для прикрепленных ОД доступен ряд действий, представленных на панели инструментов окна просмотра ОД (*Рисунок 18*).

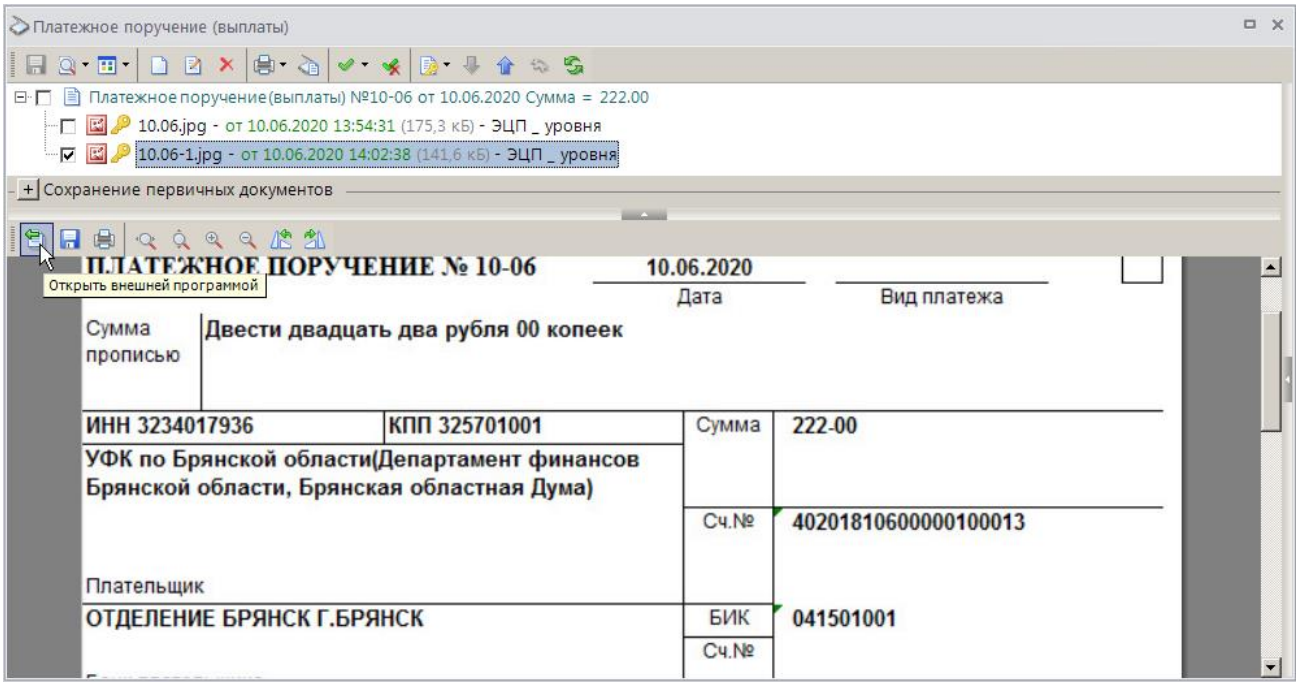

Рисунок 18. Панель управления прикрепленными ОД

- **Открыть внешней программой** – открытие документа в стороннем приложении, установленном на компьютере пользователя и предназначенном для открытия файлов с расширением, аналогичным расширению данного ОД;
- **Сохранить как** – сохранение ОД из БД в каталог на компьютере пользователя;
- **Печать** – вывод документа на печать.
- Также доступны инструменты для обработки изображений в текущем окне: выравнивание по ширине и высоте страницы, изменение масштаба и ориентации.

4. РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ СОЕДИНЕНИЯ

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 19*).

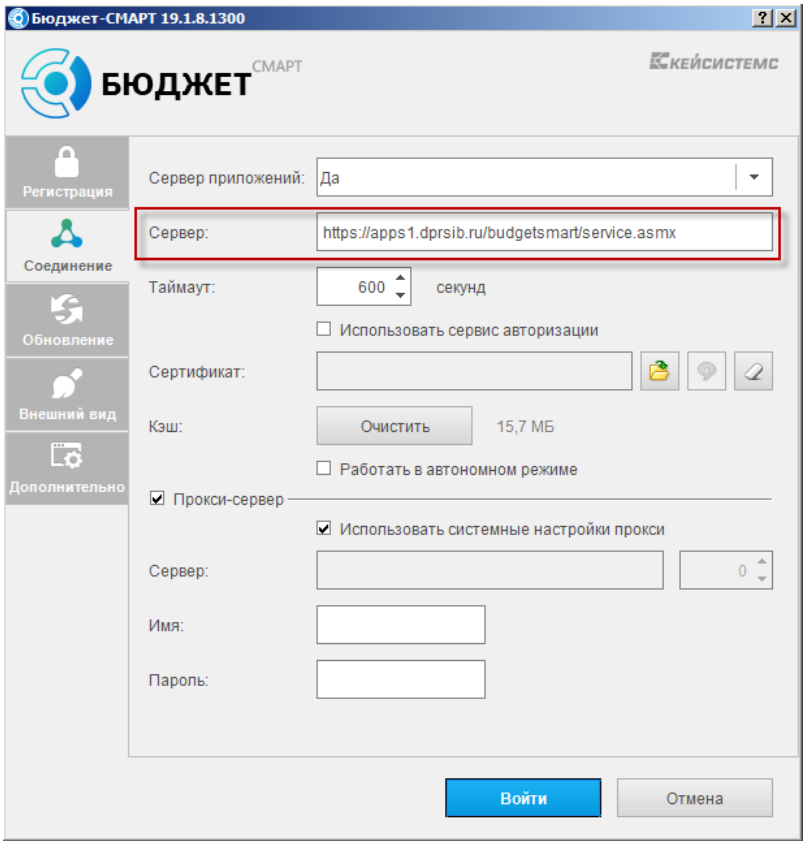

Рисунок 19. Вкладка «Соединение»

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.

4.1. 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. 4.2.2*).

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. 4.2.1*).

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

4.2. 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 20*).

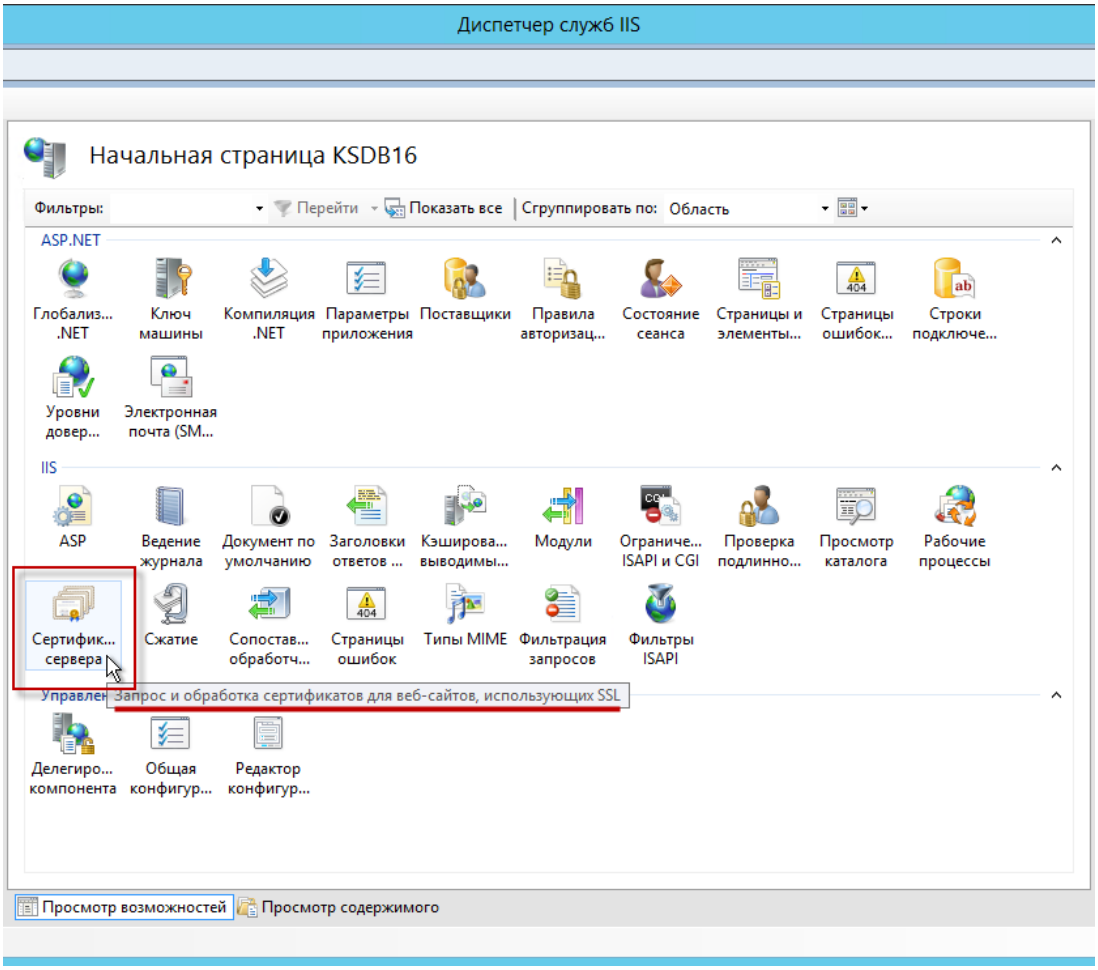

Рисунок 20. Сертификаты сервера

4.2.1. Создание самозаверенного сертификата

В открывшемся окне, в области **«Действия»**, выберите опцию **«Создать самозаверенный сертификат»** (*Рисунок 21*).

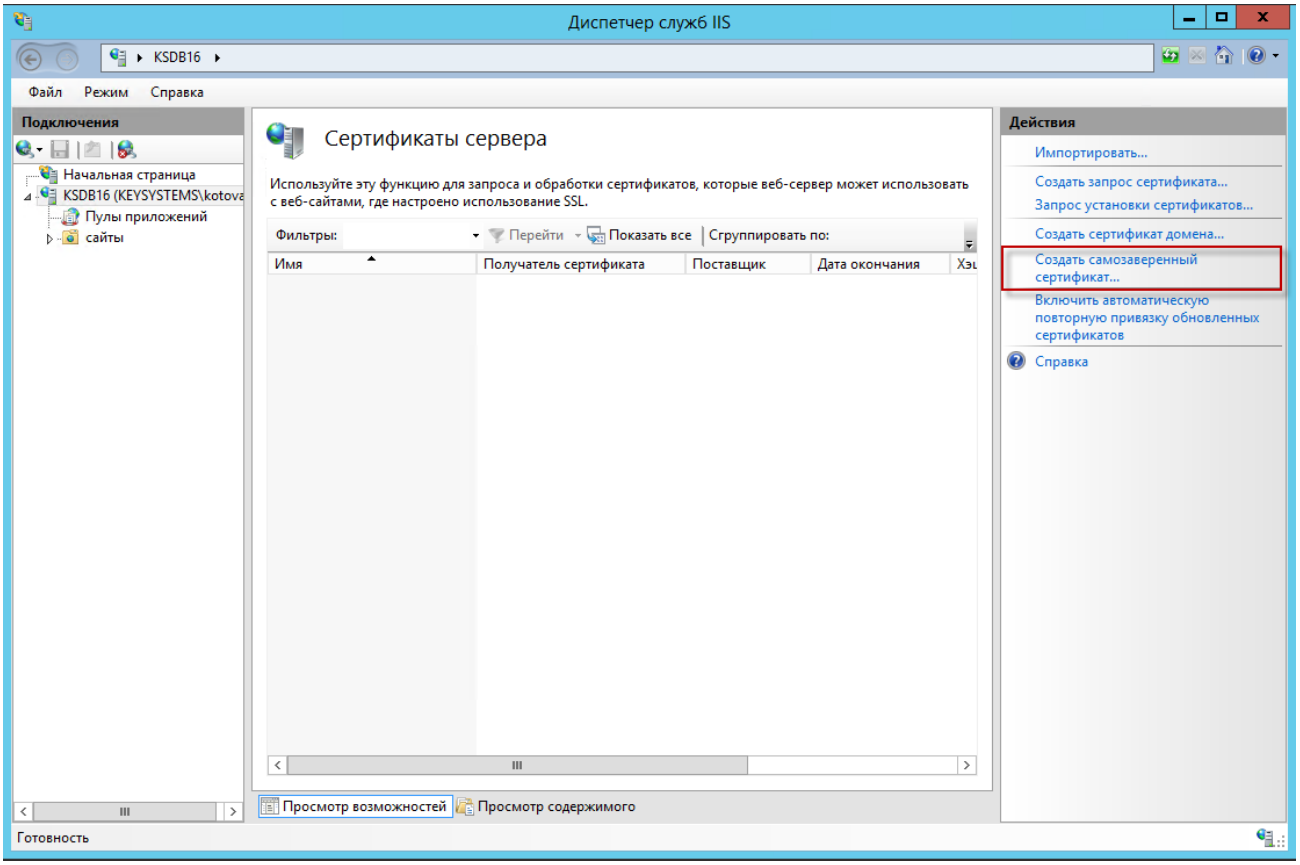

Рисунок 21. Создание запроса сертификата

В окне параметров запроса заполните следующие поля (*Рисунок 22*):

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

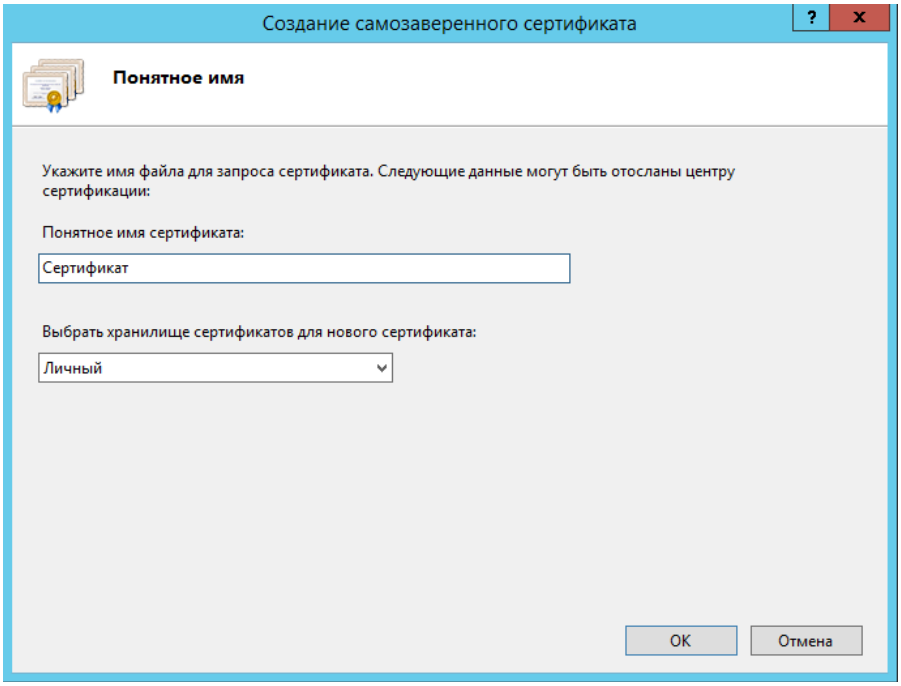

Рисунок 22. Свойства имени сертификата

По кнопке **[OK]** сертификат сразу отобразится в списке «Сертификаты сервера» (*Рисунок 23*).

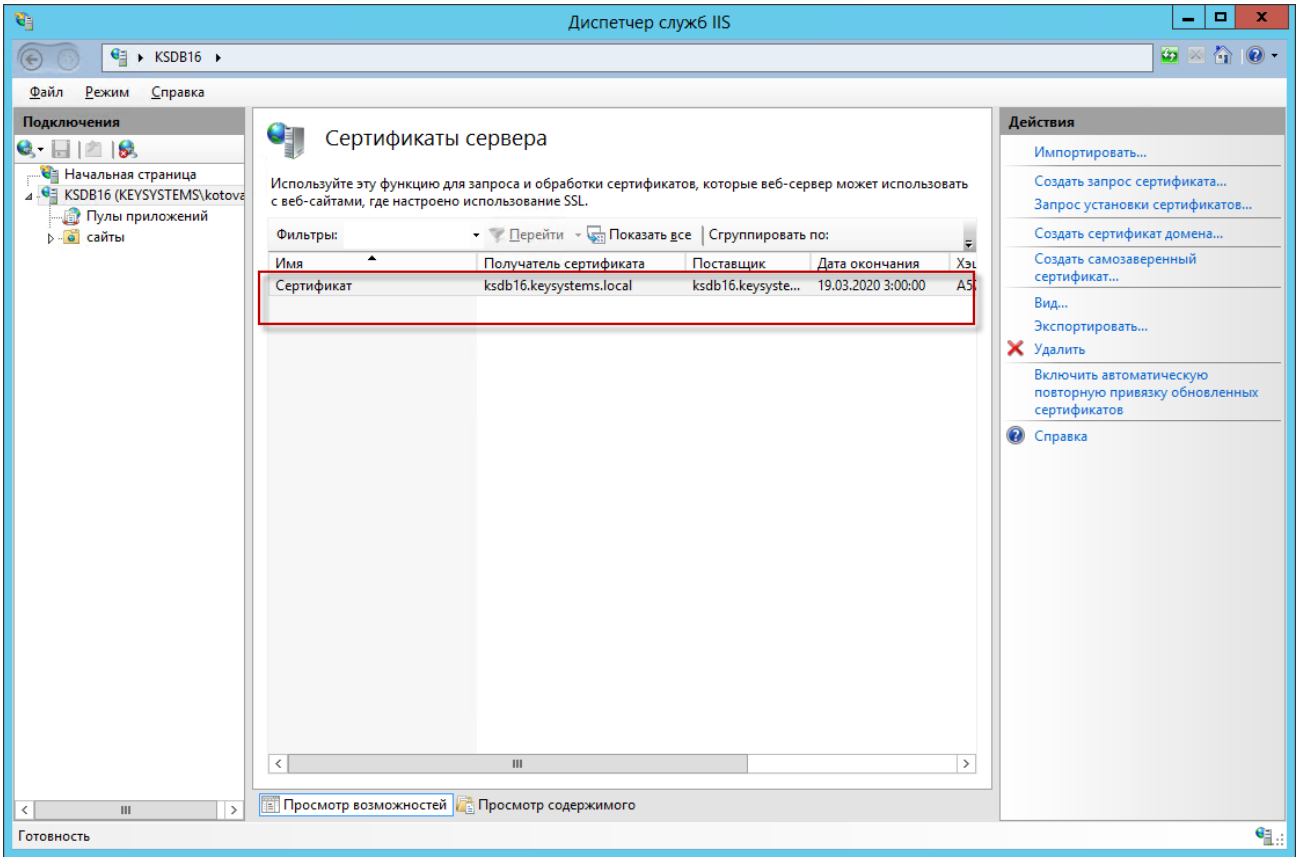

Рисунок 23. Сертификаты сервера

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

4.2.2. Генерация CSR запроса сертификата на IIS 7

В открывшемся окне, в области **«Действия»**, выберите опцию **«Создать запрос сертификата»** (*Рисунок 24*).

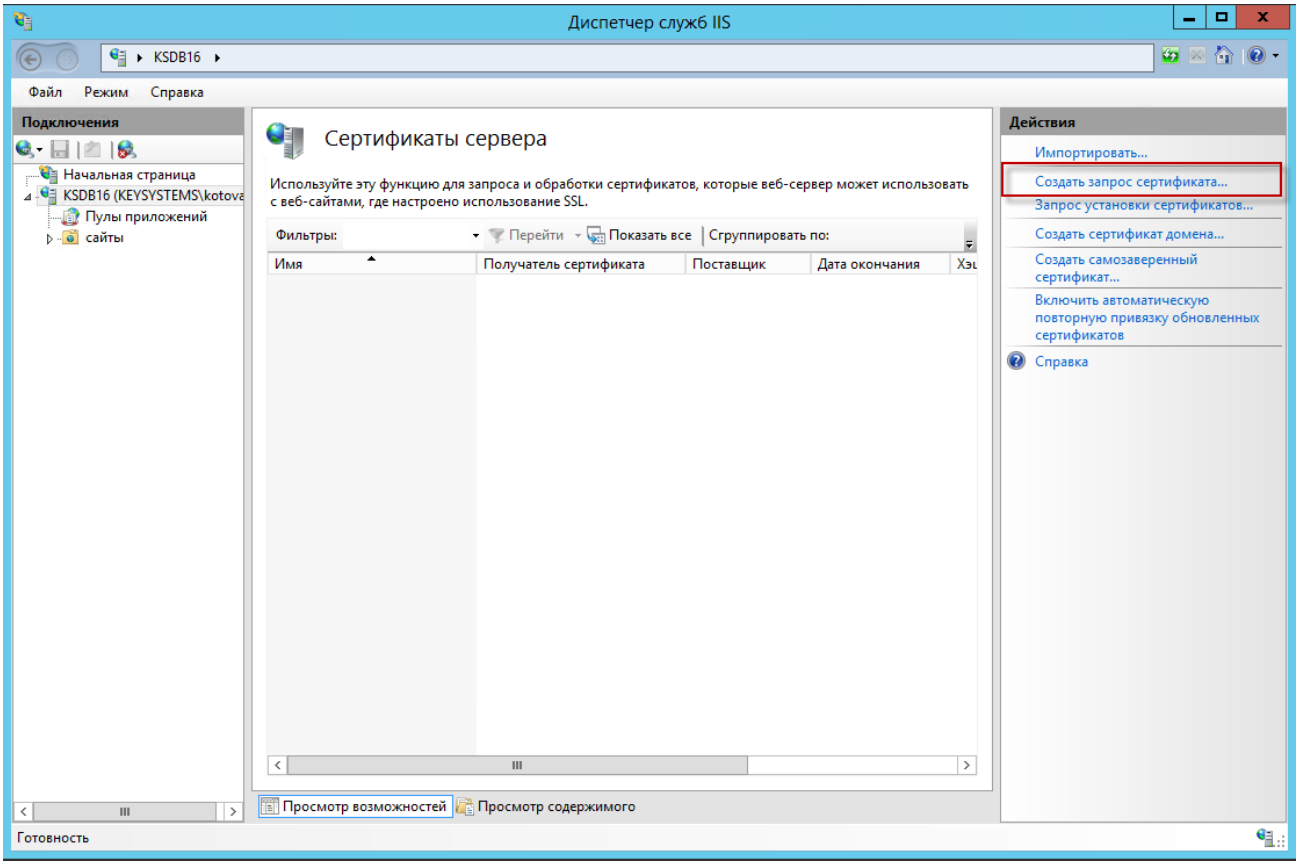

Рисунок 24. Создание запроса сертификата

В окне параметров запроса заполните следующие поля (*Рисунок 25*):

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

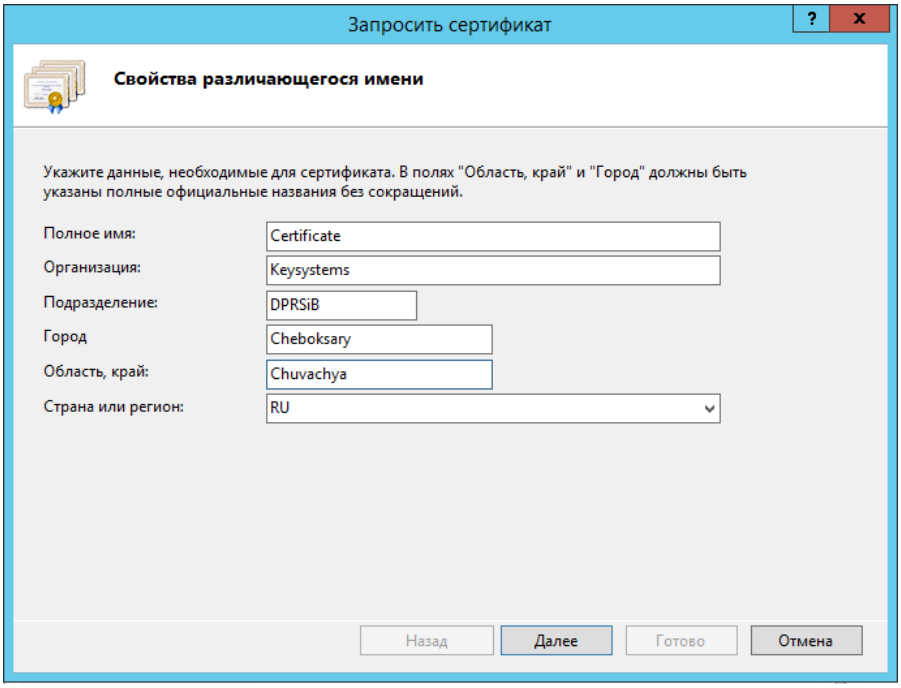

Рисунок 25. Свойства имени сертификата

Далее выберите значение длины ключа - 2048 бит (*Рисунок 26*).

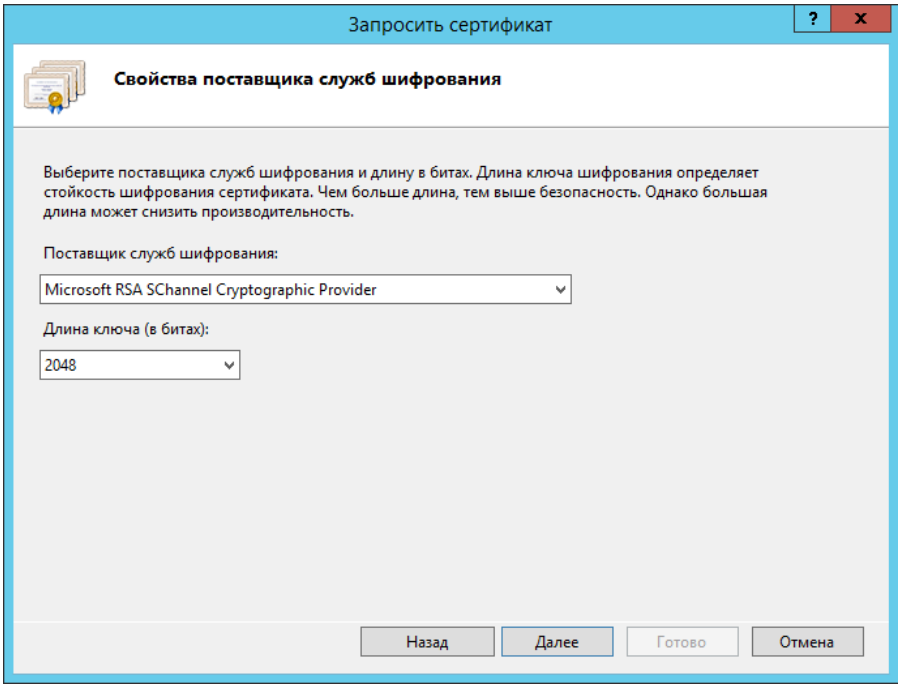

Рисунок 26. Свойства поставщика служб шифрования

Укажите место сохранения CSR запроса (это будет обычный текстовый файл *.txt) (*Рисунок 27*).

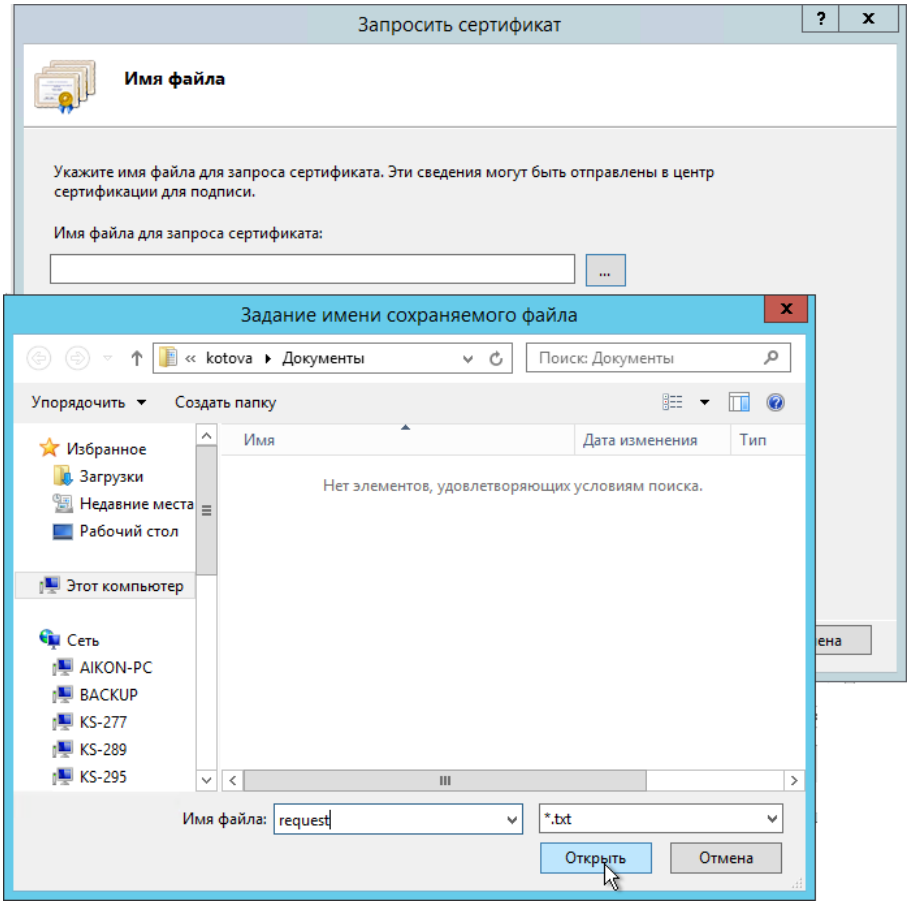

Рисунок 27. Путь к месту сохранения CSR запроса

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 28*).

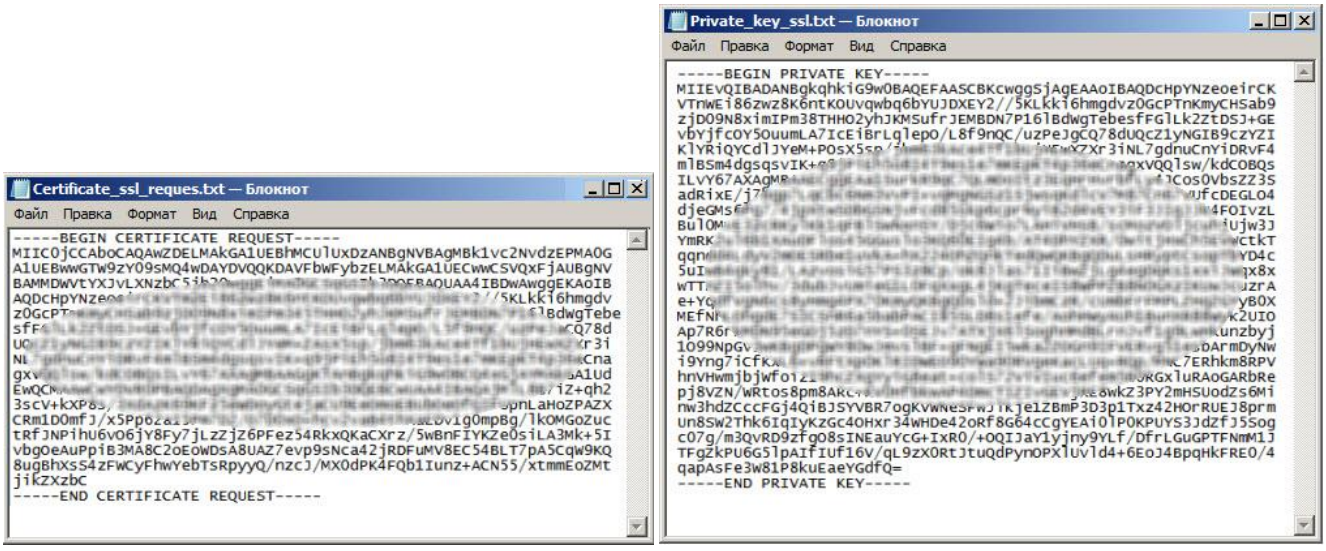

Рисунок 28. Запрос и закрытый ключ

После того как пара ключей приватный/публичный сгенерированы, на основе публичного ключа формируется запрос на SSL-сертификат в Центр сертификации (*Рисунок 29*). Перед этим измените расширение файла с *.txt на *.p10.

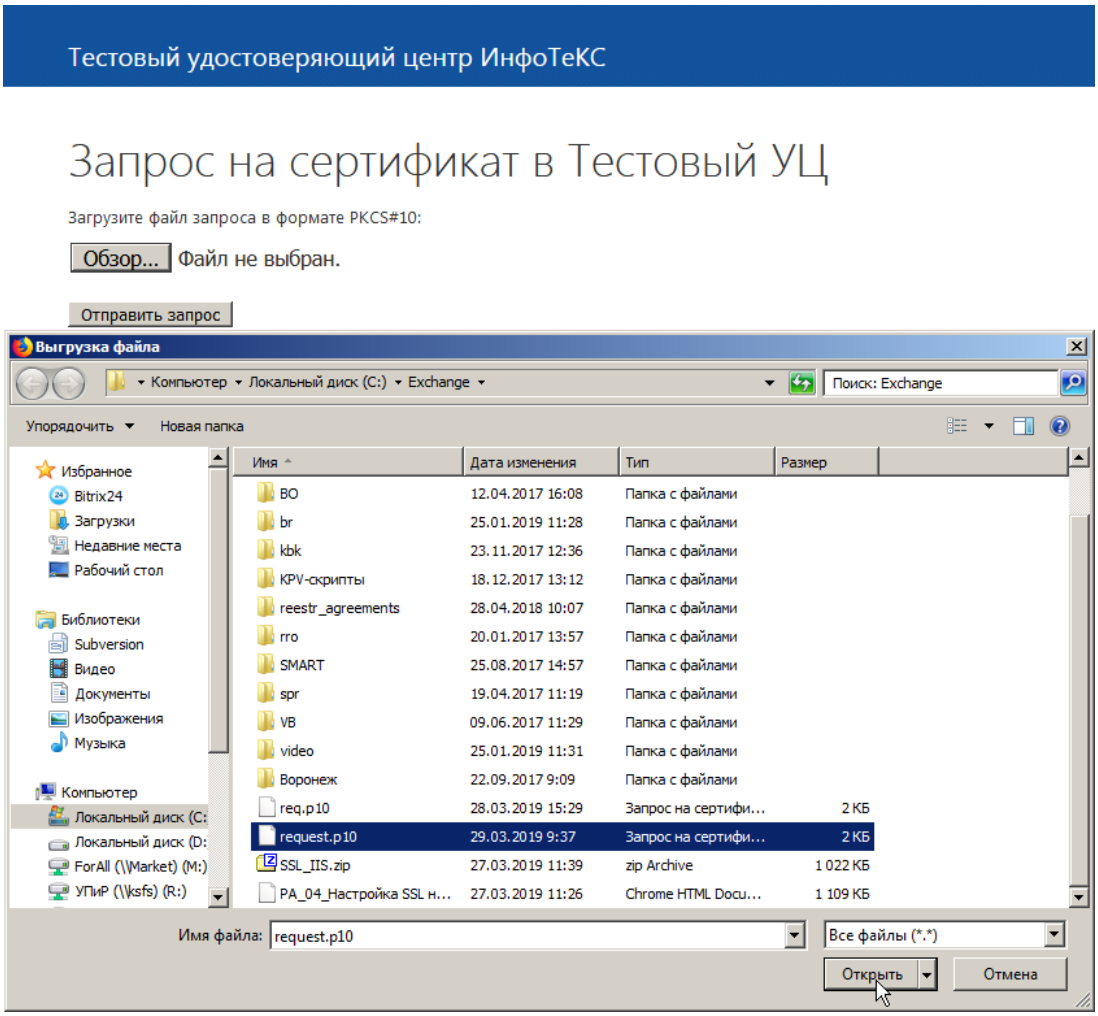

Рисунок 29. Передача запроса в удостоверяющий центр

Скачайте полученный сертификат (*Рисунок 30*).

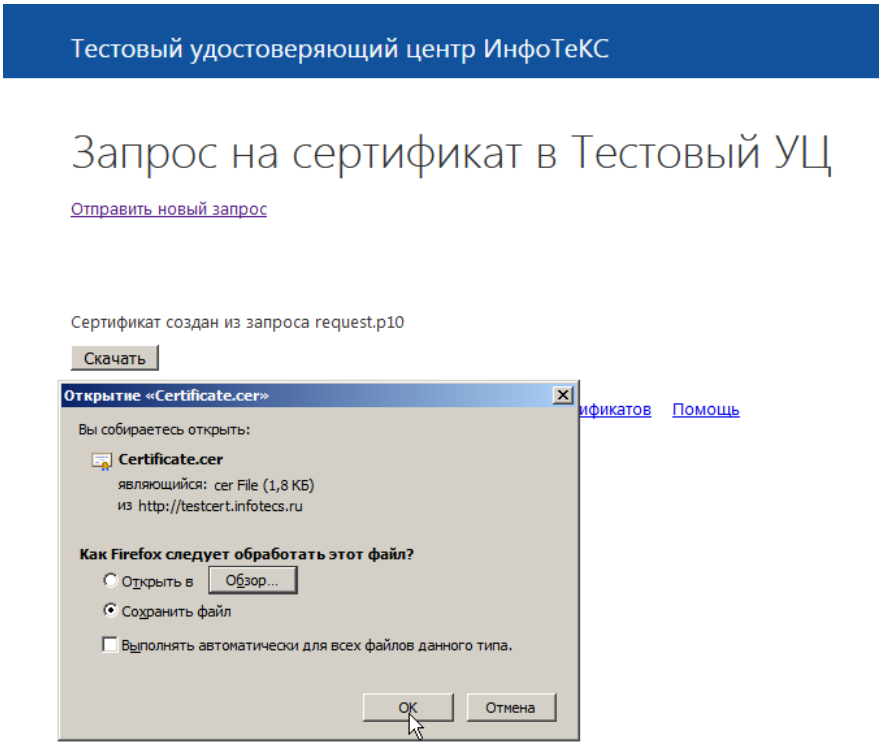

Рисунок 30. Сохранение сертификата, полученного от УЦ

Для установки на сервер полученного от УЦ сертификата воспользуйтесь опцией **«Запрос установки сертификатов»** в меню **«Действия»** (*Рисунок 31*).

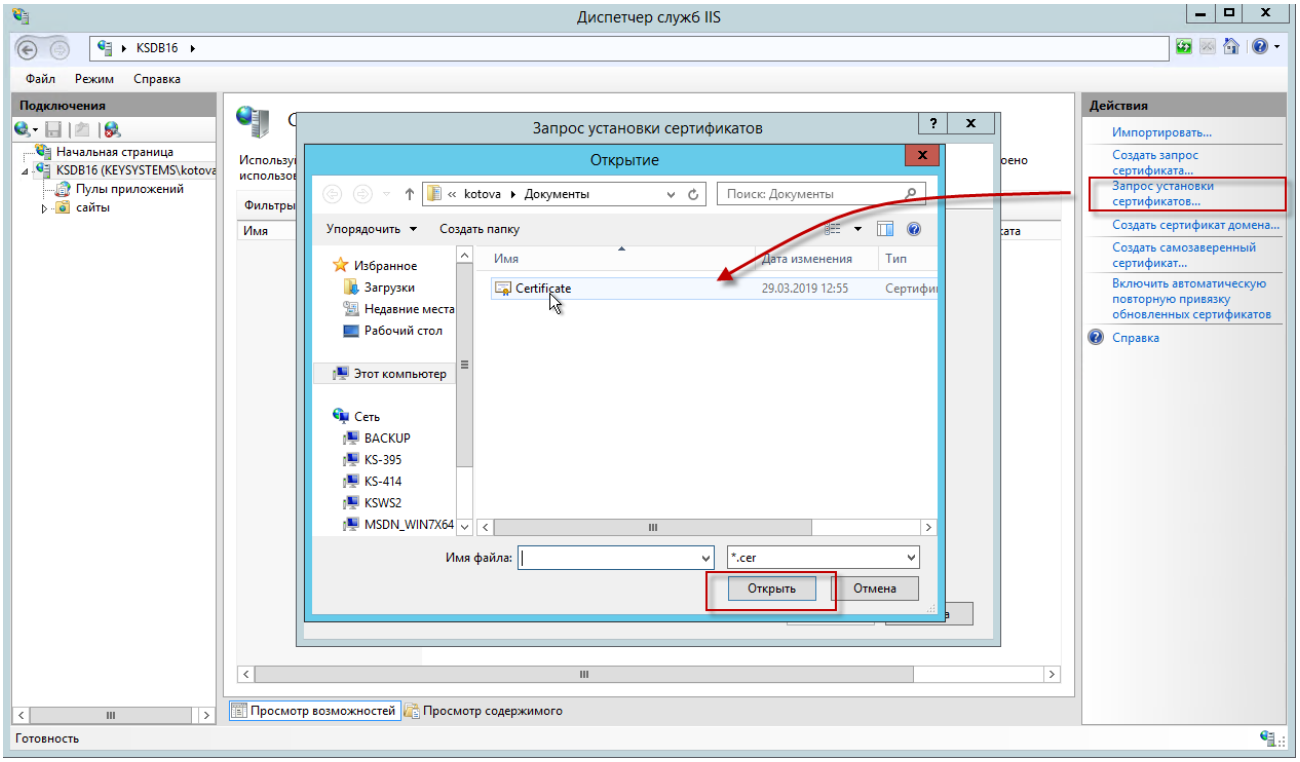

Рисунок 31. Установка сертификата, полученного от УЦ

В окне параметров запроса заполните следующие поля (*Рисунок 32*):

– **Понятное имя** – идентификатор сертификата;

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

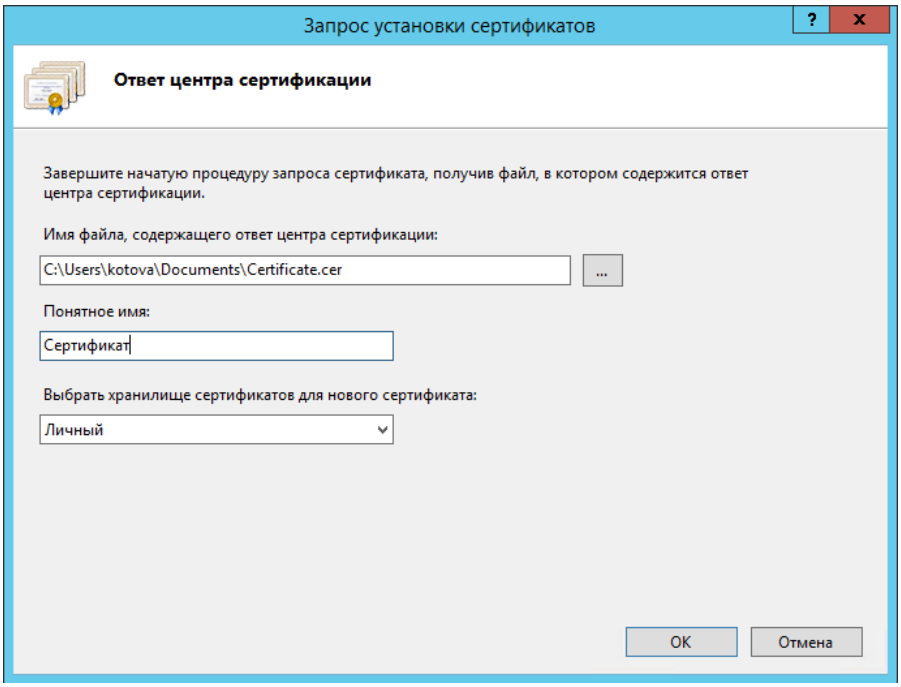

Рисунок 32. Запрос установки сертификатов

По кнопке **[OK]** сертификат сразу отобразится в списке **«Сертификаты сервера»** (*Рисунок 33*).

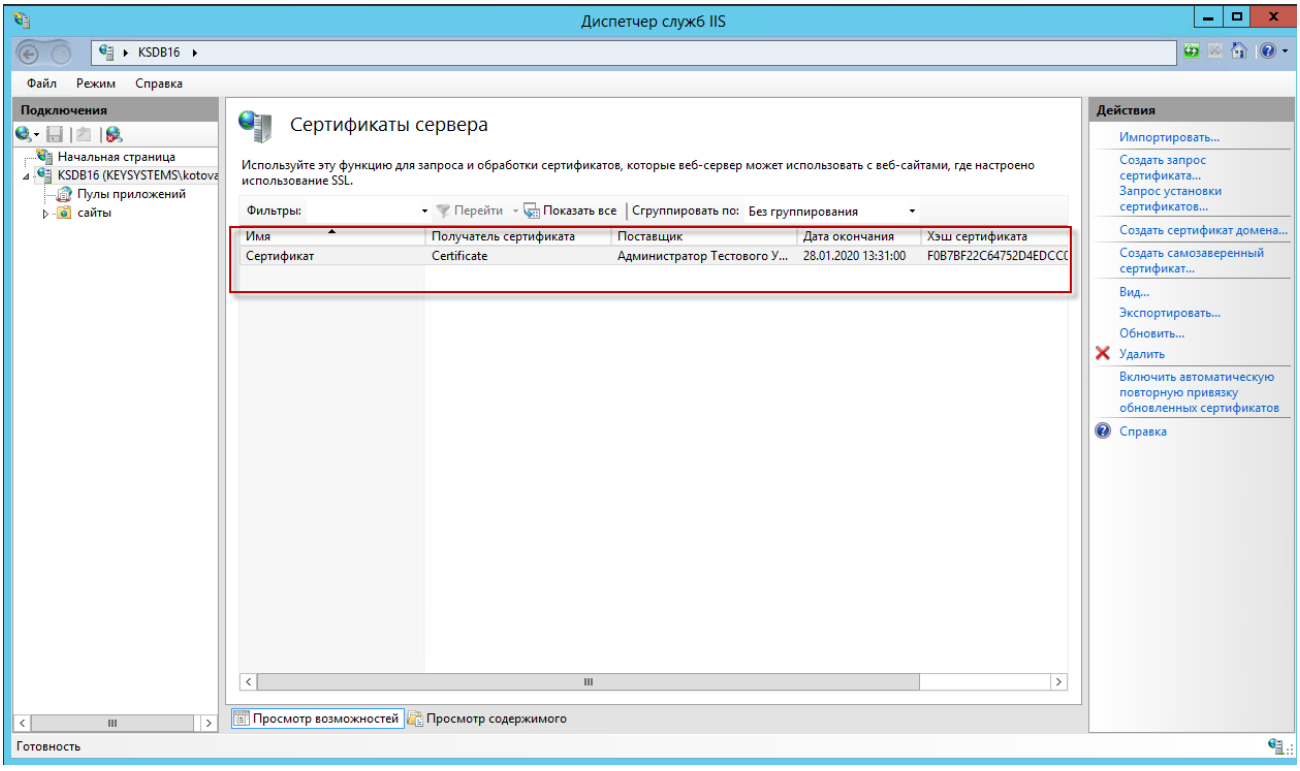

Рисунок 33. Сертификаты сервера

4.2.3. 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 29*).

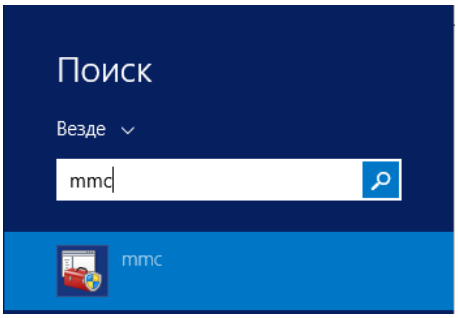

Рисунок 34. Вызов оснастки

Далее необходимо через меню «Файл» добавить новую оснастку (*Рисунок 35*).

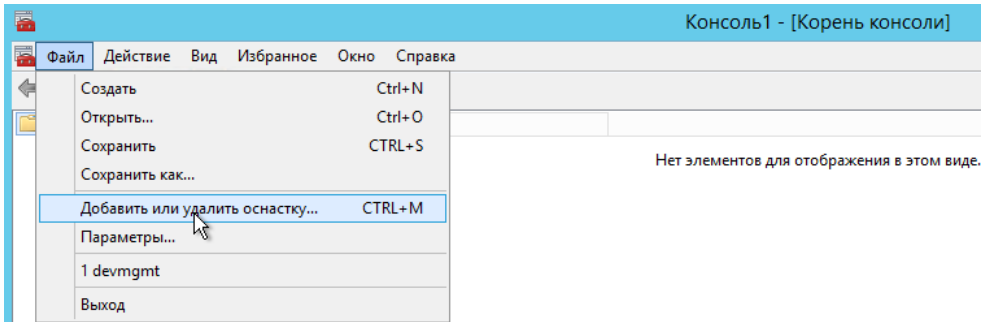

Рисунок 35.

Найдите сертификаты и нажмите кнопку **[Добавить]** (*Рисунок 36*).

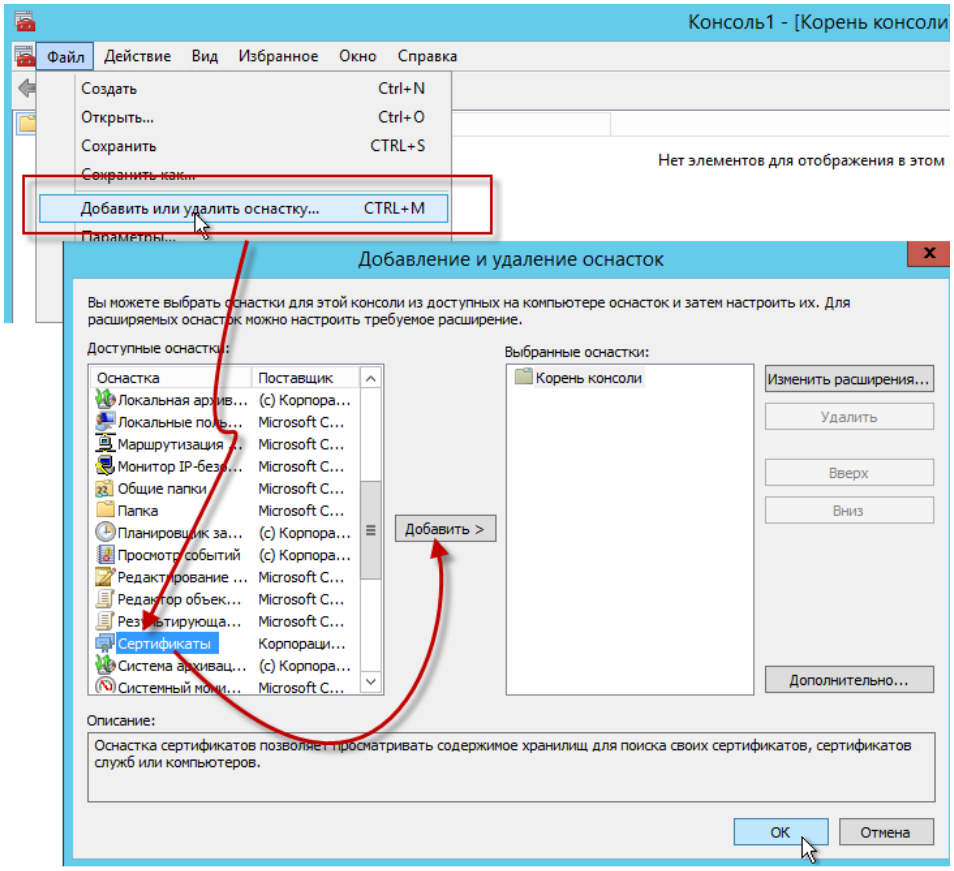

Рисунок 36. Добавление сертификата

В следующем окне выберите способ управления сертификатами: для «учетной записи компьютера» (*Рисунок 37*).

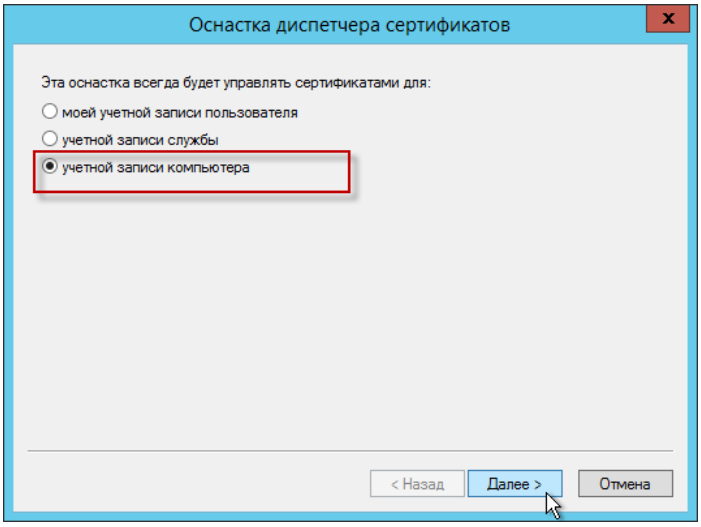

Рисунок 37. Способ управления сертификатами

Подтвердите, что будет осуществляться управление именно локальным компьютером (*Рисунок 38*).

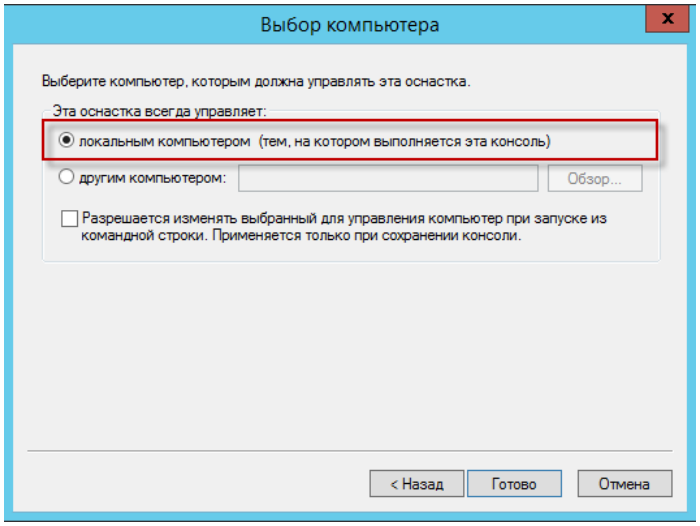

Рисунок 38. Выбор компьютера

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 39*).

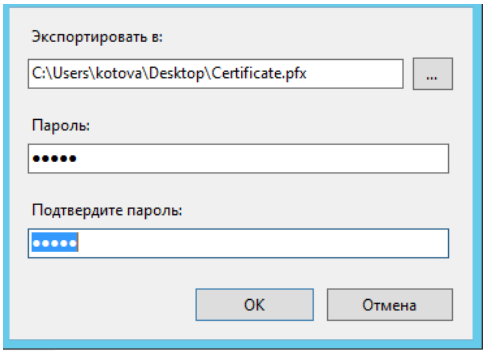

Рисунок 39. Экспорт сертификата

4.2.4. Экспорт сертификата с другого сервера

При переносе с другого сервера сертификат сначала необходимо выгрузить с данного сервера, чтобы потом импортировать на новый сервер (*Рисунок 40*).

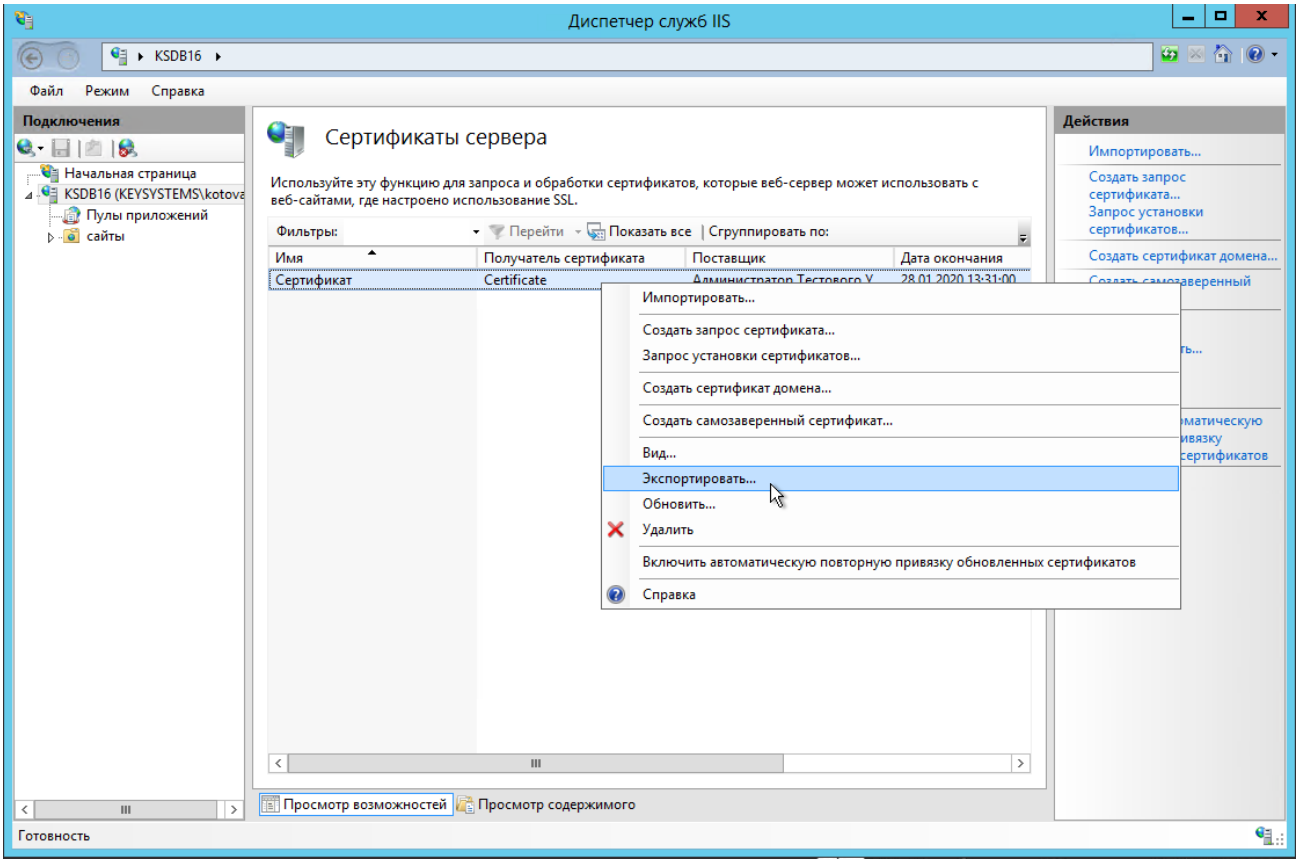

Рисунок 40. Экспорт сертификата

Аналогично описанию предыдущего пункта данного документа укажите путь выгрузки, а также придумайте и подтвердите пароль для данного сертификата (*Рисунок 41*).

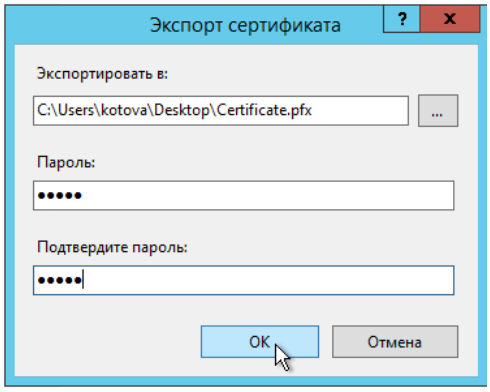

Рисунок 41. Задание пароля и пути выгрузки сертификата

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

4.2.5. Импорт сертификата на сервер

Для дальнейшей работы необходимо импортировать нужный сертификат. Откройте диспетчер IIS и перейдите в окно «Сертификаты сервера» (см. *Рисунок 23*). В открывшемся окне, в

области **«Действия»**, выберите опцию **«Импортировать»**. В режиме «Обзор» выберите pfx архив (*Рисунок 42*).

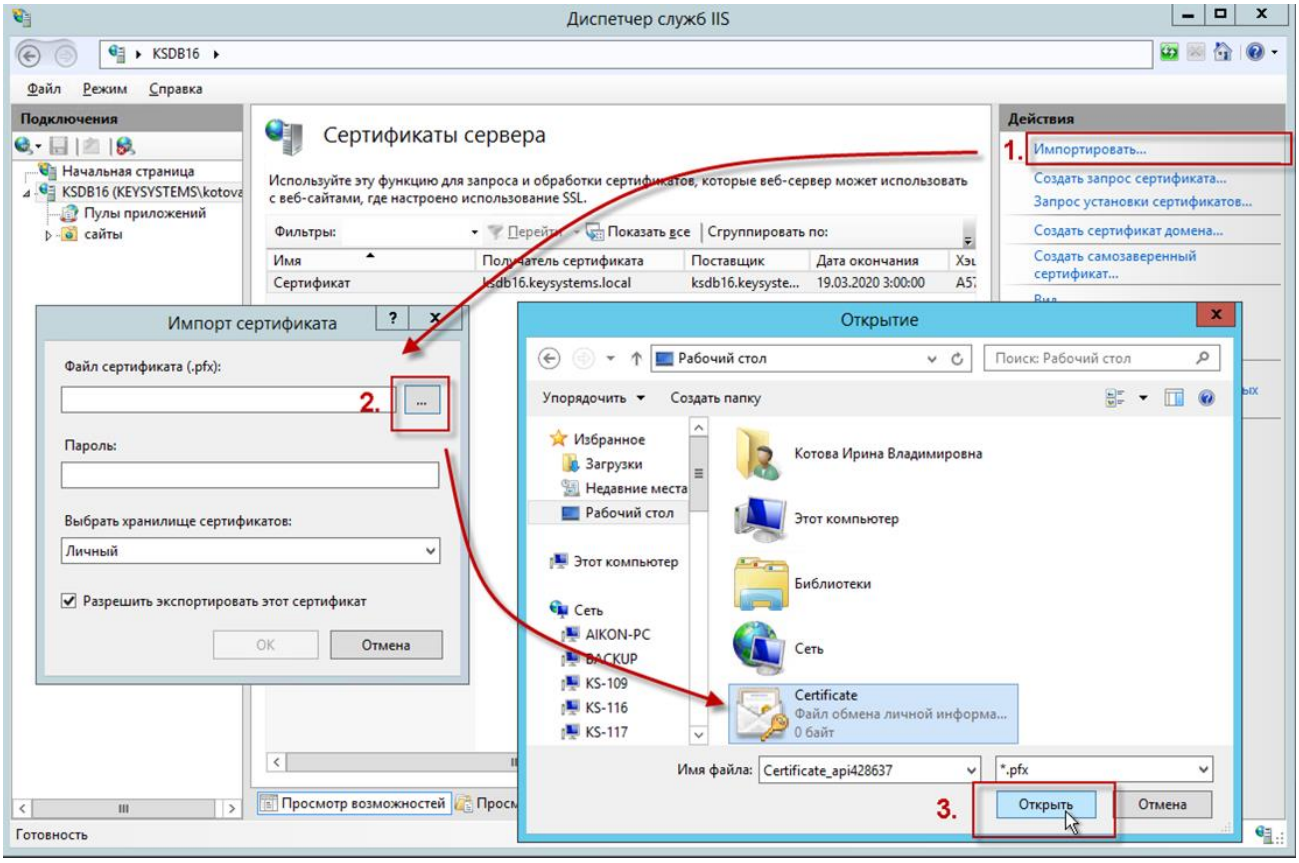

Рисунок 42. Подготовка к импорту сертификата

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 43*).

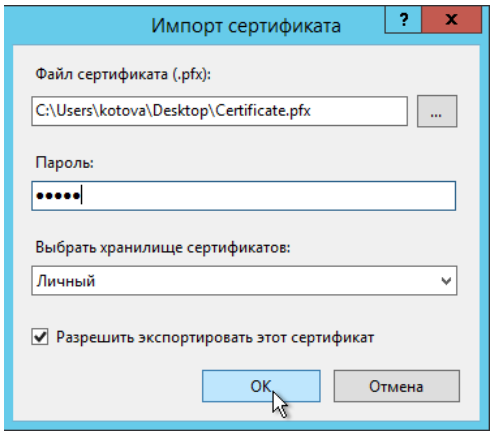

Рисунок 43. Импорт сертификата

4.3. 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 44*).

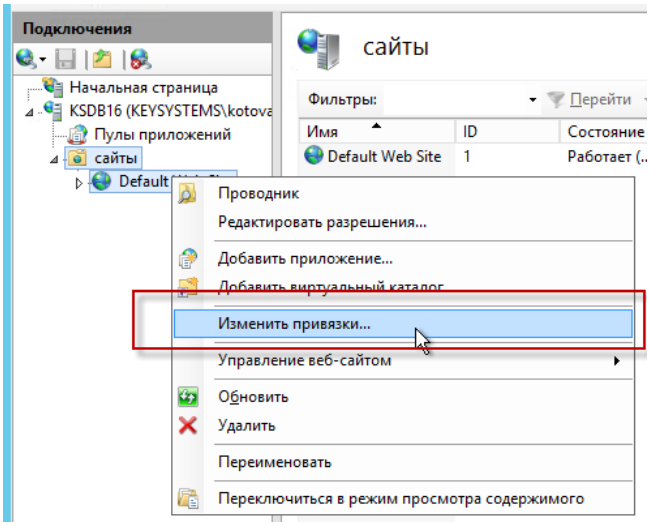

Рисунок 44. Настройка протокола https в IIS

Укажите для сайта (*Рисунок 45*):

- **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.

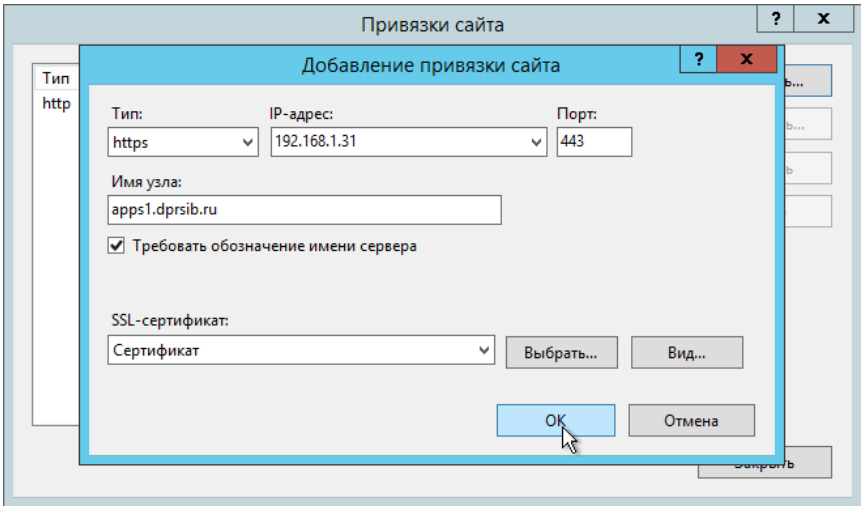

Рисунок 45. Добавление привязки сайта

В завершение проверьте сайт по протоколу HTTPS: в адресной строке должен отобразиться закрытый замочек. Это означает, что ssl сертификат установлен в IIS правильно (*Рисунок 46*).

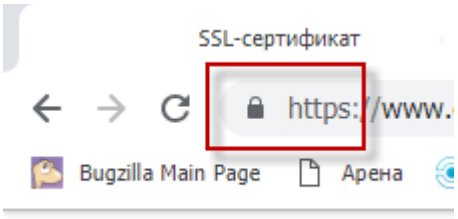

Рисунок 46. Проверка корректности установки сертификата

5. НЕСТАНДАРТНЫЕ СИТУАЦИИ

5.1. Ошибки при установке сервиса ОД

Возможны случаи, когда при установке сервиса оправдательных документов возникают ошибки. В данном разделе разберем наиболее часто встречающиеся ошибки.

Ошибка

«Невозможно создать файл, так как он уже существует. (Exception from HRESULT: 0x800700B7)» (*Рисунок 47*).

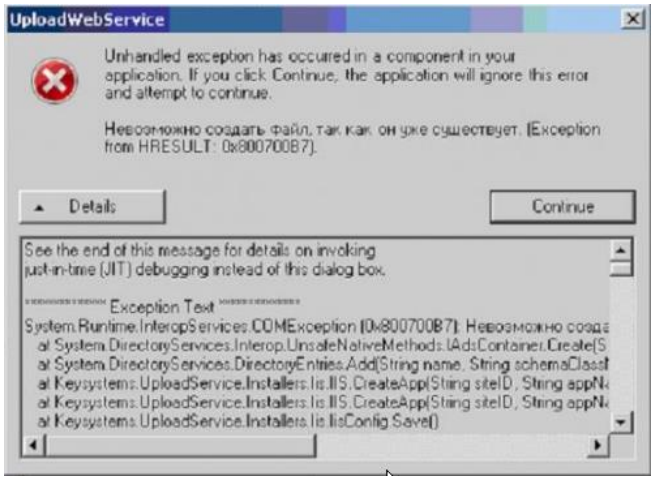

Рисунок 47. Сообщение об ошибке при установке сервиса ОД

Причина

На компьютере уже была установлена предыдущая версия Сервиса ОД, и ее либо забыли удалить, либо она была удалена некорректно.

Решение

Перейдите в каталог

```
C:\Windows\System32\inetsrv\config
```

Сделайте копию файла applicationHost.config (на случай повреждения файла в процессе редактирования).

Откройте файл applicationHost.config с помощью приложения «Блокнот». Это xml файл.

Найдите и удалите все строки, в которых встречается значение «UploadService», начиная от открывающего тэга и заканчивая закрывающим тэгом (и всю информацию между ними)

Например, необходимо удалить следующие строки:

```
<key path="LM/W3SVC/1/ROOT/UploadService">
...
</key>
```

Аналогичным образом удалите в файле любые тэги, в которых присутствует значение «UploadService» (могут быть различные, не только такие, как в примере). После чего повторите процесс установки (*см. п. 2*).

Если файл «applicationHost.config» был поврежден в процессе редактирования, воспользуйтесь его резервной копией, созданной перед началом редактирования.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Термин
1	2
БД	База данных
ОД	Оправдательные (первичные) документы
ОС	Операционная система
ПК	Программный комплекс
УЗ	Учетная запись (пользователя)
ЭП	Электронная подпись
ЭОД	Электронный обмен документами

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер версии	Примечание	Дата	ФИО исполнителя
01	Начальная версия	14.06.2018	Котова И.В.
02	Документ актуализирован, обновлены все разделы, добавлен раздел «Нестандартные ситуации», добавлены новые настройки работы с ОД в ПК «Бюджет-СМАРТ». Изменена структура и форматирование документа	10.06.2020	Котова И.В.