

### УТВЕРЖДАЮ Генеральный директор ООО «Кейсистемс» \_\_\_\_\_\_ А. А. Матросов «\_\_\_» \_\_\_\_\_ 2019 г.

# **ПРОГРАММНЫЙ КОМПЛЕКС «ПРОЕКТ–СМАРТ ПРО»** ВЕРСИЯ 18.0

Руководство пользователя

Настройка SSL на IIS

# ЛИСТ УТВЕРЖДЕНИЯ

СОГЛАСОВАНО

Заместитель генерального директора ООО «Кейсистемс»

\_\_\_\_\_ О. С. Семенов «\_\_\_» \_\_\_\_\_ 2019 г.

Руководитель ДПиАБ

\_\_\_\_\_ А. В. Никитин «\_\_\_» \_\_\_\_\_ 2019 г.

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

Подп и дата



# **ПРОГРАММНЫЙ КОМПЛЕКС «ПРОЕКТ–СМАРТ ПРО»** ВЕРСИЯ 18.0

# Руководство пользователя

Настройка SSL на IIS

Листов 17

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

#### АННОТАЦИЯ

Настоящий документ является частью руководства администратора программного комплекса «Проект-смарт ПРО» версии 18.0 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 «Проект-Смарт ПРО»

OOO «Кейсистемс» Адрес: 428000, Чебоксары, Главпочтамт, а/я 172 Телефон: (8352) 323-323 Факс: (8352) 571-033 <u>http://www.keysystems.ru</u> E-mail: <u>info@keysystems.ru</u>

### СОДЕРЖАНИЕ

Введение	4
1. Настройка SSL на IIS	5
1.1. Сертификаты для настройки нттрѕ сайта на IIS	. 5
1.2.         Генерация CSR запроса на ПS 7           1.2.1.         Создание запроса сертификата	. 6 . 7
1.2.2. Создание самозаверенного сертификата	10
1.3. Установка SSL в PFX 1	12
Глоссарий1	5
Перечень сокращений 1	6
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ 1	7

### 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.

#### словные 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></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 [1]	_	Ссылки на структурные элементы, рисунки, таблицы текущего документа. Ссылки на документы из перечня ссылочных документов.
	Уведомление Предупреждение Предостережение Замечание (Выполнить] <f1> «Чек» Статус Окна =&gt; навигатор n. 2.1.1 рисунок 5 [1]</f1>	Уведомление

## 1. HACTPOЙKA SSL HA 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*).

🍞 Проект-СМАР	РТ Про 18.41.32367.0	? <mark>×</mark>
ПР	OEKT-CMAP	Ккейсистемс Т ПРО
Регистрация	Сервер приложений:	Да 🛛 🗸 🗸
4	Сервер:	http://dwh_saas.keysystems.ru/dwh2ws_mrw/service.asmx
Соединение	Таймаут:	600 Секунд
Обновление	Сертификат:	
Внешний вид	Кэш:	Очистить 1,5 МБ П Работать в автономном режиме
Дополнительно	🗹 Прокси-сервер —	Использовать системные настройки прокси.
	Сервер:	0 🗘
	Имя:	
	Пароль:	
L		Войти Отмена

Рисунок 1. Вкладка «Соединение»

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

Для подключения через сервер приложений рекомендуется 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. Сертификаты 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. 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.

ПК «ПРОЕКТ–СМАРТ ПРО»

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. 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 2*).

	📕 Private_key_ssl.txt — Блокнот	
	Файл Правка Формат Вид Справка	
Certificate_ssl_reques.bxt — Блокнот	BEGIN PRIVATE KEY MIIEvQIBADANBGKqhkiG9w0BAQEFAASCBKcwgg5jAgEAAOIBAQDCHpYNzeoet VTmwEi86zwz8k6ntKoUvqwbdp6bYUJDXEY2//5kLkki6hmgdvz0GCPTKmwyCHS zjD09N8ximIPm38THH02yhJtMSufrIEMBDN7P161BdwgTebesfF61Lk2ZtDS: vbYjfc0Y50uumLA7ICE1BrLq1ep0/L8f9nqC/uzPejGC78dUQCZ1yNGIB9Cz K1YRiqYCd1JYeM+P0SX5sp/jbm63kAce4Tf1bUjHEwX2xr3ihL7gdnuCnYiD m1B5m4dgsqsYIK+q9jPiEh508I4T9es1e7mKEpKT4p36ecnaqxVQQ1sw/kdcC ILYY67XAQMBAAECgGEALSUrKR9qC7QUnOT123EqHrHvTbLy43CoS0VbS2 adRixE/j7Dgp7LqCbc6Nm3VvPI+vqMqNGS2L5jwsqkd1cv7M87Cn67VufcDEC djeGM56P7/4jpXtwSDbCSNjVFC485Skp6cprNyiB2dVeYSifS1JqJ3k470 Bu10MvE3zcRKy1Kk1qFB1SwNxnSv/DjC6Wi07LAHiVHSB/scMozV01jcUhjU YmRX2u16b1XauDF10s45GGu5103XQ60Ejdb/Art4DhvZxR/OwitjHxchSEVw qqndd4LdyV2m0ESRbe1uVkA+h2240hZqnkTedQwQKBgQDULSHRyptCs0pTb) SuTwB4qky81/LAzvosiG57P5328Cp/0k81las711iBwZjLg4egDqKs1xx1JwC WTTNZ1501hv/3dubJvUmieGL10FqXxQL4jKgTece1SbWPZB8N06XZIKUWJcc e+YqdfVqN6cs8yHmg4PX70KmyQR8gQDs1d+211bmCZR/cUmbFrFMPLZHqZGY MEfNhL0fqdz75ICSnR6a5baDPACT85SLD81ef/AchHwyAuhIBunXR88Wk/ Ap7R6rkMDN95eQj52D7NY5+0SEJv7ATXjX61SoghTMdBLrnJvf1g9LwHkunz 1099Npc71fKxL6+V#FLXp0KlRTDwE090Ywa90RvgeKacLUq+RQp/NNC7ERhkm hnVHwmjbjWf01z19hcZXgYvjG8eat+c01572ViVIuC6efem5B0RGx1URA0GA jj8VZN/WKt058Bm8ARc+KV0HfbKwA44DmcTIZIVGeY1R8BWC28JP2mHSu0AGZ m3hd2cCcFGj4Q1BJSYVBR70gKWNeSFwJ1kje1ZBm7B3DJR424D0FRWE1 unSw2TKK61g1YXG2Cd0Hx73WH0E2XGY4WH6KAA4DrTZIVUV24A2H0FRWE1 j08VZN/WKt058Bm8ARc+KV0HfbKwA44DmcTIZIVGEY1R8BW223PY2mHSU0AGZ m3hd2cCcFGj4Q1BJSYVBR70gKVHFbKAA4DmcTIZIVGEY1R8Wk23PY2mHSU0AGZ m3hd2cCcFGj4Q1BJSYVBR70gKWNESFwJ1kje1ZBm7B3DJTx242H0FRWE1 j0R3WRB9Zf008SINB2Q24008SINB2ACK4V0HfbKWA44DmcTIZIVGEY1R8Wk23PY2mHSU0AGZ m3hd2cCcFGj4Q1BJSYVBR70gKWNESFwJ1kje1ZBm7B3DJTx242H0FRWE1 j0R3WRB9Zf008SINB2ACK4V0HfbKWA44DmcTIZIVGEY1R8Wk23PY2mHSU0AGZ m3hd2cCcFG3AS1H24C40HX73WHfbKWA44DMcTIZIVGEY1R8Wk23PY2mHSU0AGZ m3hd2cCcFG4Q14JSVBR70gYJB2XDRJJUQPNPXLV1D446EcJ4BpHkFRI qapAsFe3WB18KWEaeYGdfQ= END PRIVATE KEY	A irck sab9 J+GE zYZI zYZI zYZI zZ3S GLO4 IVZL jW3J VZL tVZL vTA2 vD4C vD4C vD4C vD4C vD4C vD4WW 88PV sb01 sb01 sb01 vD4C vD4
×		~

Рисунок 2. Запрос и закрытый ключ

После того как пара ключей приватный/публичный сгенерированы, на основе публичного ключа формируется запрос на SSL-сертификат в Центр сертификации (*n. 1.2.1*).

Существует возможность создать такой сертификат, не обращаясь в Центр сертификации. Подписываются такие сертификаты этим же сертификатом, поэтому они называются «самоподписанными»/«самозаверенными» (self-signed) (*n. 1.2.2*).



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

### 1.2. Генерация CSR запроса 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 3*).

				Диспе	тчер служб	IIS				
🌒 Ha	чальная	страница	a KSDB16	5						
Фильтры:		- 💚 Пе	рейти 👻 🙀 Г	Токазать все	Сгруппирова	ть по: Обла	сть	-		
ASP.NET		_								^
<u> </u>	7		<b>*</b>		i n	<b>\$</b>		404	ab	
Глобализ .NET	Ключ машины	Компиляция .NET	Параметры приложения	Поставщики	Правила авторизац	Состояние сеанса	Страницы и элементы	Страницы ошибок	Строки подключе…	
Уровни	Электронная									
довер	10418 (SIVI									~
						2				
ASP	Ведение	Документ по	Заголовки	Кэширова	Модули	Ограниче	Проверка	Просмотр	Рабочие	
	журнала	С		выводимы		<b>W</b>	подлинно	каталога	процессы	
Сертифик сервера	Сжатие	Сопостав обработч	Страницы ошибок	Типы МІМЕ	Фильтрация запросов	Фильтры ISAPI				
Управлен З	апрос и обра	ботка сертифі	икатов для ве	б-сайтов, испо	ользующих SS	L				~
	¥=									
Делегиро	Общая	Редактор								
компонента	конфигур	конфигур								
Просмотр	возможносте	й / 🕼 Просма	тр содержим	ого						

Рисунок 3. Сертификаты сервера

# 1.2.1. Создание запроса сертификата

В открывшемся окне, в области «Действия», выберите опцию «Создать запрос сертификата» (*Рисунок 4*).

HACTPOЙKA SSL HA IIS

<b>V</b> i		Диспетчер служ	бIIS			_ <b>D</b> X
€ • KSDB16 •						😰 🛛 🟠 🔞 •
Файл Режим Справка						
Подключения	Consultane					Действия
🔍 - 📊 🖄  🏀	Сертификаты	сервера				Импортировать
Чачальная страница ▲ КSDB16 (KEYSYSTEMS\kotova КSDB16 (KEYSYSTEMS\kotova)	Используйте эту функцию для с веб-сайтами, где настроено	запроса и обработки сертификатов использование SSL.	ать	Создать запрос сертификата Запрос установки сертификатов		
— Пулы приложении ⊳ сайты	Фильтры:	🔹 🖤 Перейти 👒 🔙 Показать все	Сгруппировать	по:	-	Создать сертификат домена
	Имя	Получатель сертификата	Тоставщик	Дата окончания	Хэь	Создать самозаверенный сертификат
						Включить автоматическую повторную привязку обновленных сертификатов
	< Просмотр возможностей и	III Просмотр содержимого			>	Оправка
	Contraction of the second structure of the	E				€∃ .
ТОТОВНОСТЬ						1.:

Рисунок 4. Создание запроса сертификата

В окне параметров запроса заполните следующие поля (Рисунок 5):

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

ПК «ПРОЕКТ–СМАРТ ПРО»	ŀ

	Запросить сертификат	?	x
Свойства разли	нающегося имени		
Укажите данные, необходимы указаны полные официальны	е для сертификата. В полях "Область, край" и "Город" должны быть е названия без сокращений.		
Полное <u>и</u> мя:	сертификат		
Органи <u>з</u> ация:	Кейсистемс		
<u>П</u> одразделение:	ДПРСиБ		
Г <u>о</u> род	Чебоксары		
О <u>б</u> ласть, край:	Чувашия		
С <u>т</u> рана или регион:	RU V		
	Назад Далее Готово О	тмена	

Рисунок 5. Свойства имени сертификата

Далее выберите значение длины ключа - 2048 бит (Рисунок 6).

Запросить сертификат	?	x
Свойства поставщика служб шифрования		
Выберите поставщика служб шифрования и длину в битах. Длина ключа шифрования определяет стойкость шифрования сертификата. Чем больше длина, тем выше безопасность. Однако большая длина может снизить производительность. Поставщик служб шифрования:		
Microsoft RSA SChannel Cryptographic Provider		
Длина ключа (в битах): [2048]		
Назад Далее Готово О	тмена	

Рисунок 6. Свойства поставщика служб шифрования

Укажите место сохранения CSR запроса (это будет обычный текстовый файл \*.txt) (Рисунок 7).

ПК «ПРОЕКТ–СМАРТ	ПРО»				ΗA
		Запросить сертификат	?	)	c
		Имя файла			

Имя файла					
Укажите имя файла для запроса сертификата. Эти сведения могут быть отправлены в центр сертификации для подписи.					
Имя файла для запроса сертификата: C:\Certificate ssl reques.txt					
Назад Далее Готово Отмена					

Рисунок 7. Путь к месту сохранения CSR запроса

Полученный от центра сертификации сертификат, будет необходимо настроить под IIS, так как ему потребуется формат pfx.

## 1.2.2. Создание самозаверенного сертификата

В открывшемся окне, в области «Действия», выберите опцию «Создать самозаверенный сертификат» (*Рисунок 8*).

HACTPOЙKA SSL HA IIS

<b>8</b> ]		Диспетчер служ	6 IIS		_ <b>D</b> X
€ • KSDB16 →					🕶 🛛 🟠 🔞 🗸
Файл Режим Справка					
Подключения		6000000			Действия
😪 - 📊 🖄 😽	Сертификаты	сервера			Импортировать
<ul> <li>Начальная страница</li> <li>KSDB16 (KEYSYSTEMS\kotova</li> </ul>	Используйте эту функцию для с веб-сайтами, где настроено	Создать запрос сертификата Запрос установки сертификатов			
р <mark>©</mark> сайты	Фильтры:	🔹 🖤 Перейти 👒 🔙 Показать все	Сгруппировать по:	Ŧ	Создать сертификат домена
	Имя	Получатель сертификата Г	Поставщик Дата окончания	Хэг	Создать самозаверенный сертификат
					Включить автоматическую повторную привязку обновленных сертификатов
< III >	< Тёп Просмотр возможностей разможностей р	Ш		>	Справка
Готовность					• <u>•</u> :
					14.11

Рисунок 8. Создание запроса сертификата

В окне параметров запроса заполните следующие поля (Рисунок 9):

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

Создание самозаверенного сертификата			
Понятное имя			
Укажите имя файла для запроса сертификата. Следующие данные могут быть отосланы центру сертификации:			
Понятное имя сертификата:			
Сертификат			
Выбрать хранилище сертификатов для нового сертификата: Личный			
ОК О	тмена		

Рисунок 9. Свойства имени сертификата

По кнопке **[OK]** сертификат сразу отобразится в списке «Сертификаты сервера» (*Рисунок 10*).

8j	Диспетчер служб IIS	_ 🗆 X
€ SDB16 ►		😇 🖂 🟠 🔞 -
<u>Ф</u> айл <u>Р</u> ежим <u>С</u> правка		
Файл Режим Справка Подключения С С С С С С С С С С С С С С С С С С С	Уторования и поличатия и поличателя сертификата поставщик дата окончания и и поличателя сертификата поставщик дата окончания и и казы I сертификата и I поличателя и казы I сертификата и I поличателя и казы I сертификата и и каза I поставщик и поличателя и казы I сертификата и и каза I поставщик и поличателя и казы I сертификата и и каза I поставщик и поличателя и казы I сертификата и и поличателя и казы I сертификата и и каза I поставщик и поличателя и казы I сертификата и казы I сертификата и каза I поставщик и поличателя и казы I сертификата и сертификата и сертификата и казы I сертификата и казы I сертификата и сертификата и казы I сертификата и сертифи	<ul> <li>№ № № № №</li> <li>Асйствия</li> <li>Импортировать</li> <li>Создать запрос сертификата</li> <li>Запрос установки сертификатов</li> <li>Создать самозаверенный сертификат</li> <li>Вид</li> <li>Вид</li> <li>Удалить</li> <li>Включить затоматическую повторную привязку обновленных сертификатов</li> <li>Справка</li> </ul>
< Ш > Готовность	< III > Просмотр возможностей 🔊 Просмотр содержимого	କୁଥି::

Рисунок 10. Сертификаты сервера

### **1.3.** Установка SSL в PFX

Для дальнейшей работы необходимо импортировать нужный сертификат. Откройте диспетчер IIS и перейдите в окно «Сертификаты сервера» (см. *Рисунок 10*). В открывшемся окне, в области «Действия», выберите опцию «Импортировать». В режиме «Обзор» выберите pfx архив (*Рисунок 11*).

HACTPOЙKA SSL HA IIS

<b>V</b> _1		Диспетчер служб IIS	_ 🗆 X
€ ) • KSDB16 ►			😰 🖂 🏠 I 🔞 🗸
<u>Ф</u> айл <u>Р</u> ежим <u>С</u> правка			
Подключения ♥ • • • • • • • • • • • • • • • • • • •	Фринскаты сере Используйте эту функцию для запро с веб-сайтами, где настроено исполя Фильтры:	ера са и обработки сертификатов, которые веб-сервер может использовать зование SSL. 	Действия 1. Импортировать Создать запрос сертификата Запрос установки сертификатов Создать сертификат домена
	Имя Пол	чатель сертификата Поставщик Дата окончания Xэц	Создать самозаверенный сертификат
Импорт се	ертификата ? Х	Открытие Открытие	Rua
Файл сертификата (.pfx): Пароль: Выбрать хранилище сертифи Личный ✓ Разрешить экспортироват	2 катов: ь этот сертификат ОК Отмена <	<ul> <li> </li> <li></li></ul>	Поиск: Рабочий стол ♪ ВТ ↓ П @ bX bX ма *.pfx ↓ Открыть Отмена 

Рисунок 11. Подготовка к импорту сертификата

Пароль - укажите пароль;

**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 12).

Импорт сертификата	?	x
Файл сертификата (.pfx):		
C:\Users\kotova\Desktop\Certificate_api428637.pfx		
Пароль:		
••••••		
Выбрать хранилище сертификатов:		
Личный		~
<ul> <li>Разрешить экспортировать этот сертификат</li> </ul>		
ОК	мена	

Рисунок 12. Импорт сертификата

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 13*).



Рисунок 13. Настройка протокола https в IIS

Укажите для сайта (Рисунок 14):

- 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.

	Добавление прив	азки сайта	? X	іавить.
Тип:	ІР-адрес:	Порт:		енить.
https	• Все неназначенные	✓ 443		алить
Имя узла:				
				-
🖌 Требовать обо	означение имени сервера			
Требовать обс	означение имени сервера			
<ul> <li>Требовать обс</li> <li>SSL-сертификат:</li> </ul>	означение имени сервера			
<ul> <li>Требовать обс</li> <li>SSL-сертификат:</li> <li>Не выбрано</li> </ul>	означение имени сервера	♥ Выбрать	Вид	
<ul> <li>Требовать обо</li> <li>SSL-сертификат:</li> <li>Не выбрано</li> <li>Не выбрано</li> </ul>	означение имени сервера	• Выбрать	Вид	
<ul> <li>Требовать обс</li> <li>SSL-сертификат:</li> <li>Не выбрано</li> <li>Не выбрано</li> <li>Сертификат</li> </ul>	означение имени сервера	♥ Выбрать	Вид	

Рисунок 14. 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 14*).





## 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

# ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер версии	Примечание	Дата	ФИО исполнителя
01	Начальная версия	20.03.2019	Белоносов А.А.