Руководство пользователя

по настройке автоматической синхронизации пользователей из внешних источников в базу данных «Системы тестирования INDIGO»

Версия программы: 3.0

Версия руководства: 1.7 (28.05.2020)

www.indigotech.ru

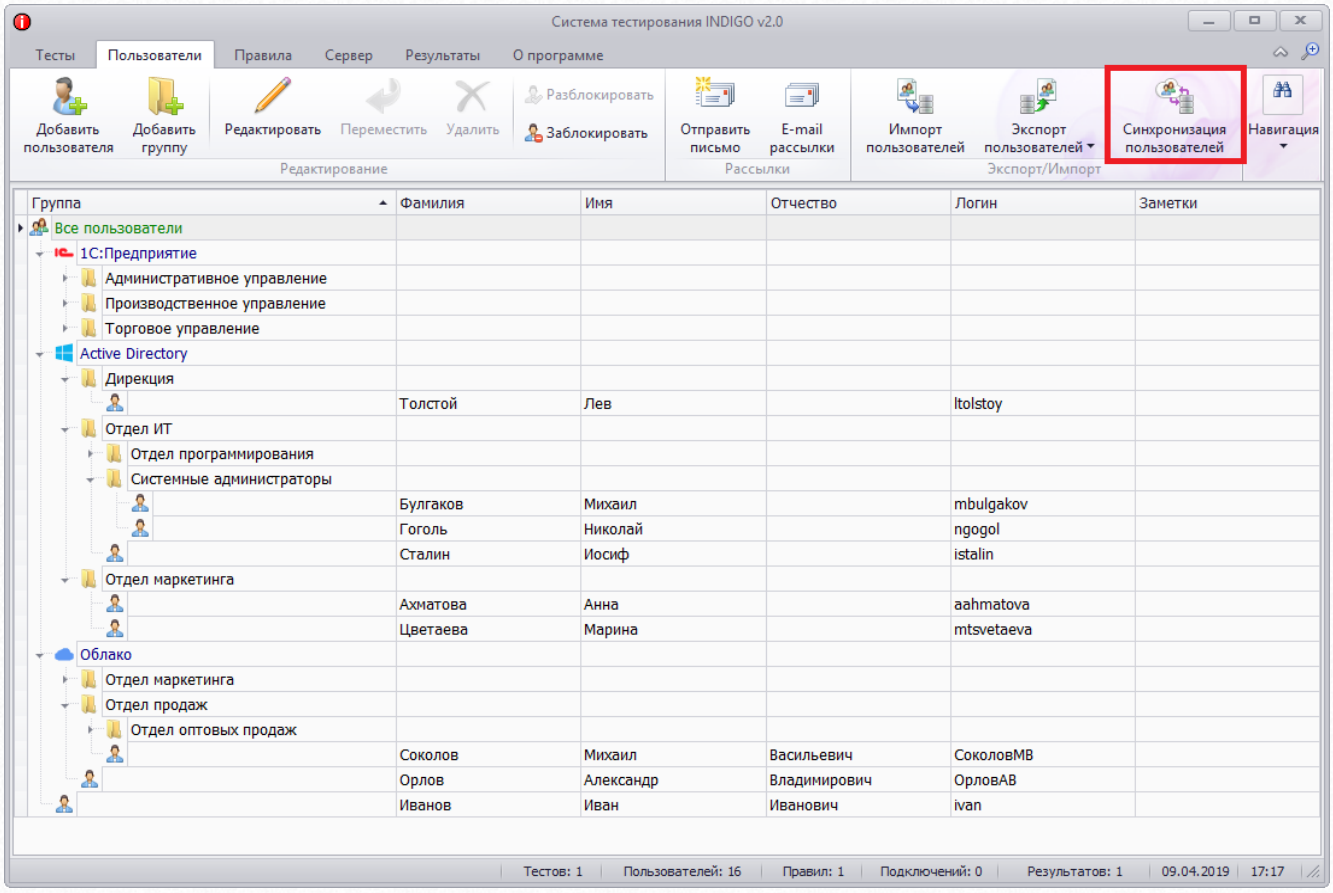
Содержание

Введение

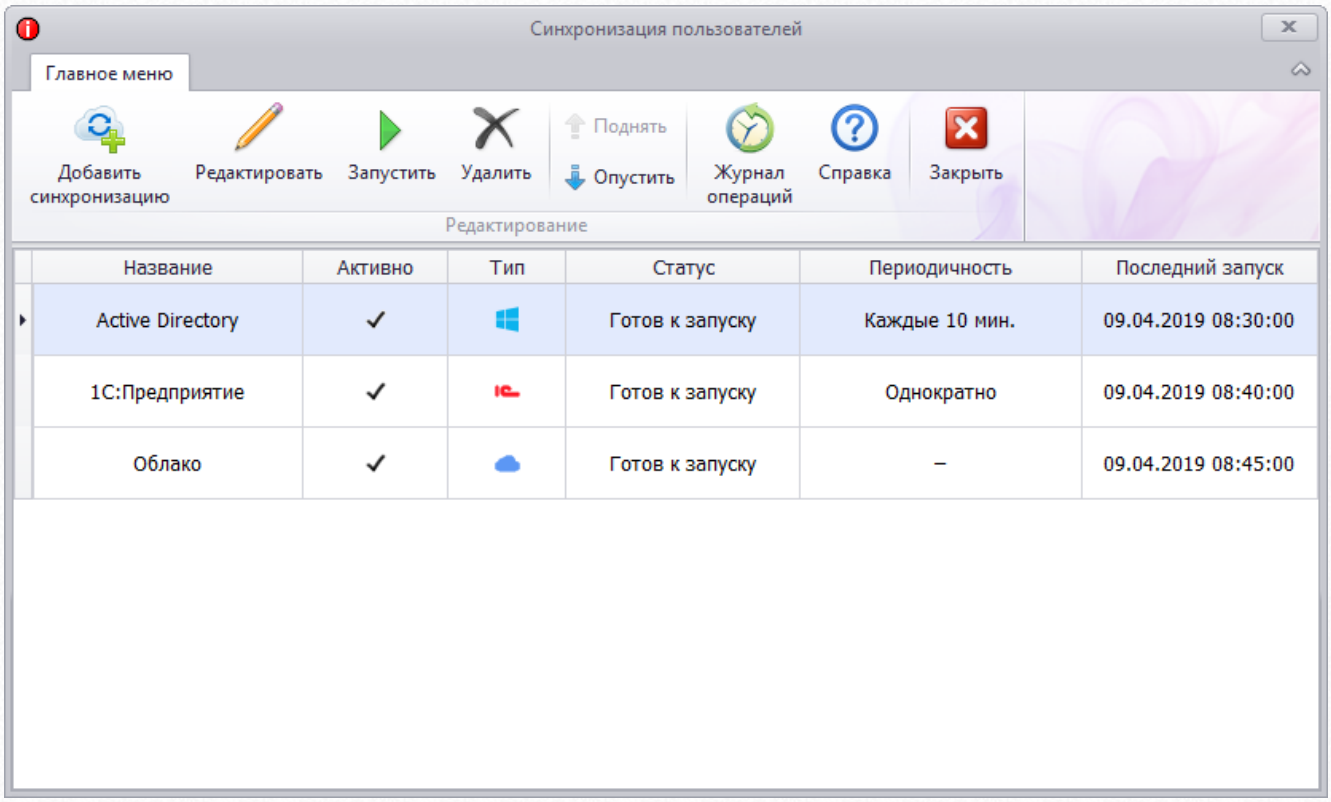
Система тестирования «INDIGO» имеет возможность синхронизации данных о пользователях и группах пользователей с внешними источниками. Если в вашей организации уже существует система, в которой ведется учет данных о пользователях, то администратор может настроить автоматическую синхронизацию пользователей из этой системы. Данная функциональная возможность упрощает администрирование программы INDIGO, избавляя администратора от необходимости выполнения дополнительной работы по поддержанию базы пользователей INDIGO в актуальном состоянии. Кроме этого, уменьшается вероятность возникновения ошибок несоответствия данных, т.к. INDIGO будет автоматически поддерживает актуальность данных в полном соответствии с внешним источником. Функция синхронизации также позволяет использовать сторонний сервис аутентификации, благодаря чему пользователям не нужно создавать отдельный пароль, а можно использовать данные авторизации из внешней системы, что повышает удобство работы пользователей, т.к. используется единый логин/пароль. Система тестирования INDIGO имеет возможность автоматически синхронизировать данные о пользователях из службы каталогов Active Directory, программных продуктов на базе платформы 1С:Предприятие, а также имеет универсальный функционал для синхронизации с любой другой сторонней системой.

1. Настройка синхронизации пользователей

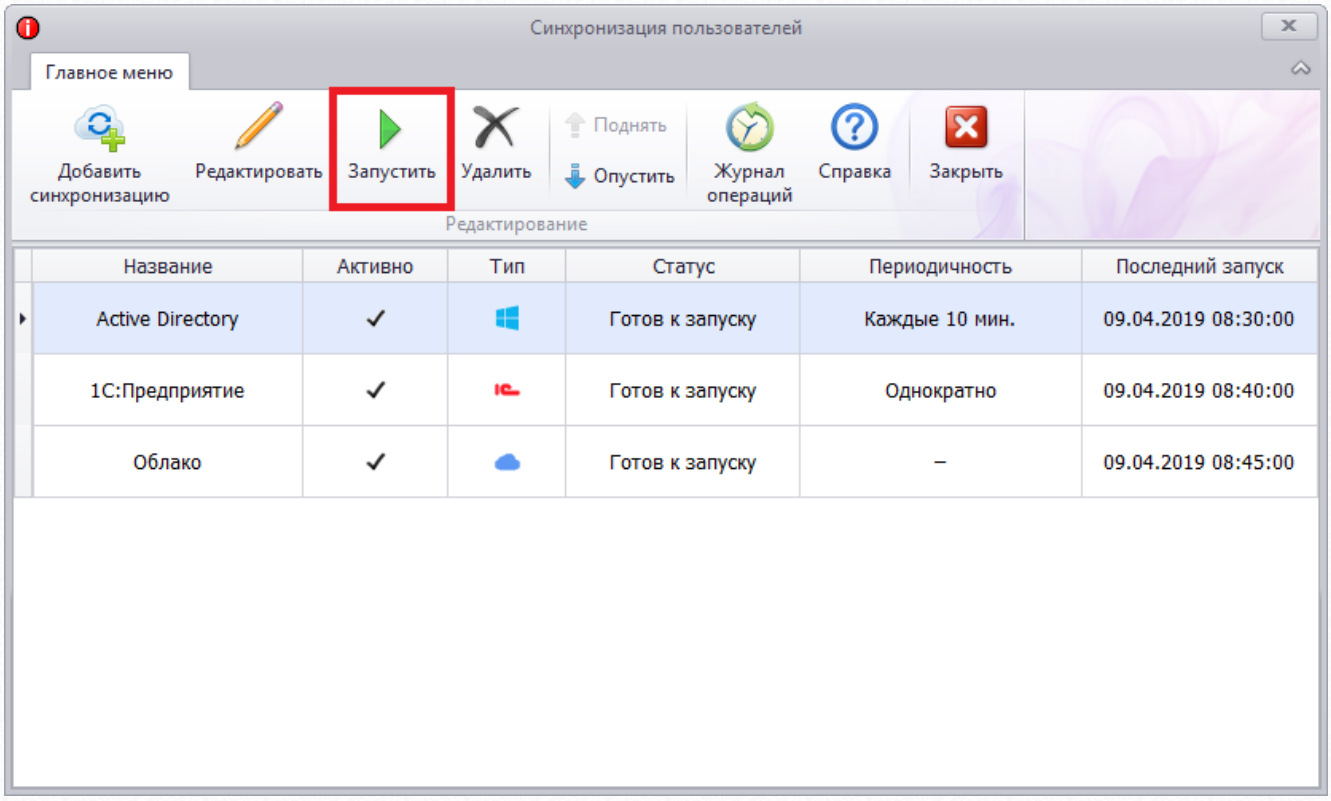
1. Откройте систему тестирования и перейдите на вкладку «Пользователи» и нажмите кнопку «Синхронизация пользователей».



2. В открывшемся окне «Синхронизация пользователей» отображается информация о ранее созданных синхронизациях. С помощью главного меню окна можно добавить новую синхронизацию и управлять уже имеющимися.



3. Если в параметрах была указана периодичность синхронизации, то процесс будет инициирован периодически через указанное количество минут в фоновом режиме. Но независимо от настроек имеется возможность принудительно инициировать процесс нажав на кнопку «Запустить сейчас» в главном меню окна.

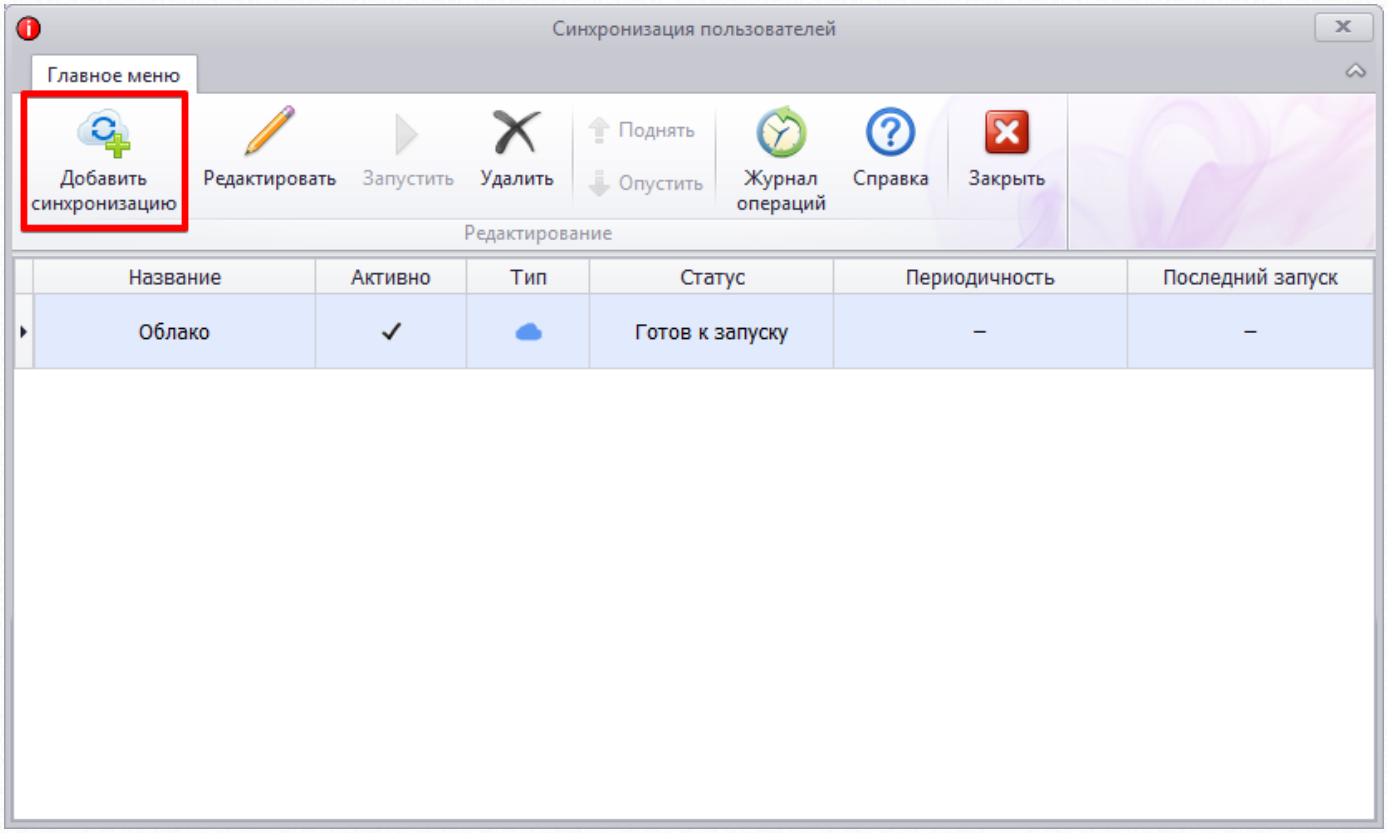


4. Если процесс синхронизации прошел успешно, то на вкладке «Пользователи» в главном окне системы тестирования «INDIGO» мы увидим созданную группу, которая содержит синхронизированные объекты и ту дополнительную информацию по ним, которая была получена из стороннего источника. Иконка группы указывает на тип источника синхронизации, а название группы совпадает с наименованием самой синхронизации.
5. После успешной синхронизации пользователи могут авторизоваться в системе с помощью логина и пароля, которые они используют для входа в стороннюю систему. Если в настройках синхронизации включена бесшовная авторизация (SSO), то пользователи могут авторизоваться кликом по ссылке «Авторизация через Active Directory».

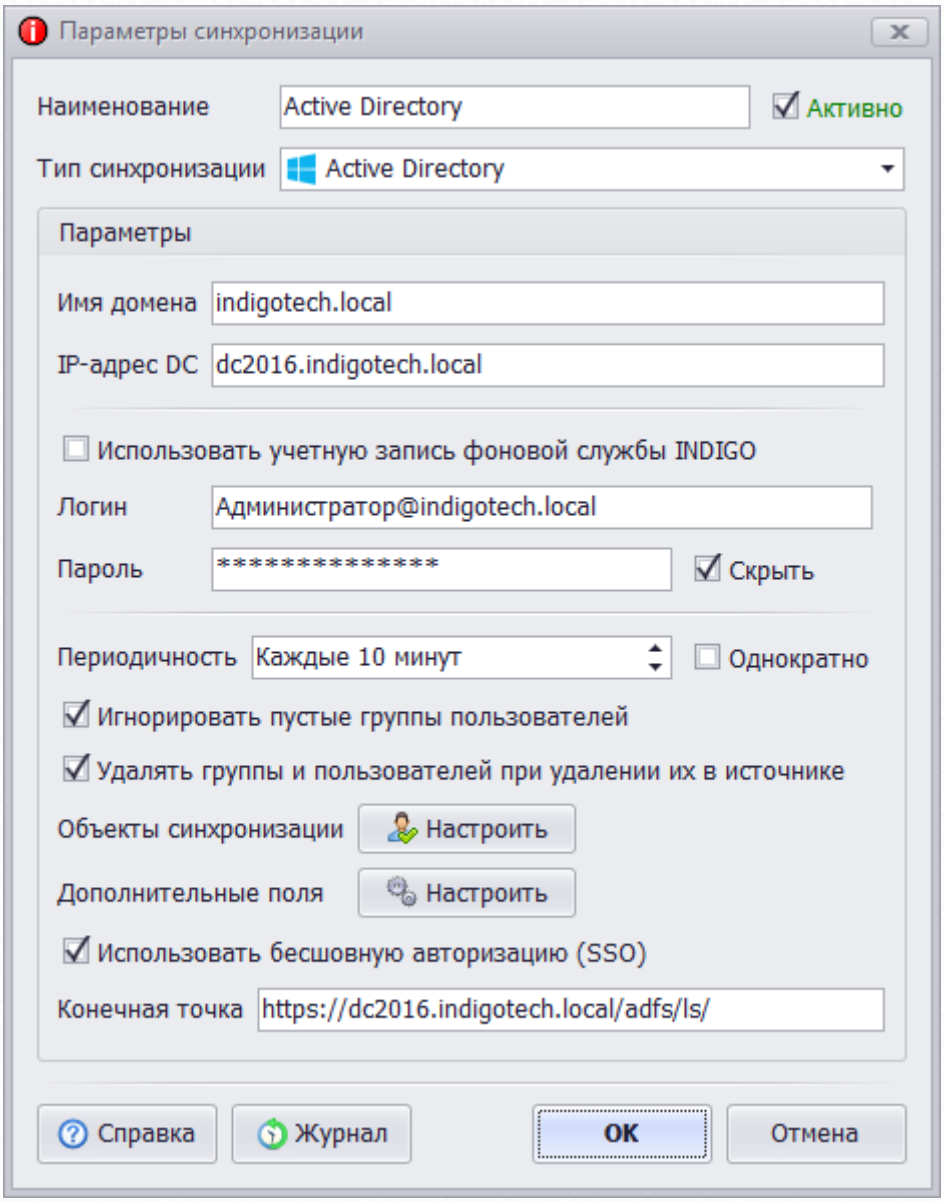
1.1. Настройка синхронизации пользователей с Active Directory

Синхронизация пользователей системы тестирования INDIGO с пользователями домена Active Directory осуществляется в фоновом режиме. Регулярно через заданный промежуток времени сервер системы тестирования опрашивает контроллер домена об изменениях в учетных записях пользователей и при необходимости актуализирует информацию в своей базе данных. Во время авторизации пользователя в веб-интерфейсе происходит проверка введенного логина и пароля на контролере домена. Имеется поддержка бесшовной авторизации пользователей SSO (пользователи автоматически авторизуются в INDIGO под своей учетной записью ОС без ввода логина и пароля в браузере).

1. В главном меню окна «Синхронизация пользователей» нажмите на кнопку «Добавить синхронизацию».



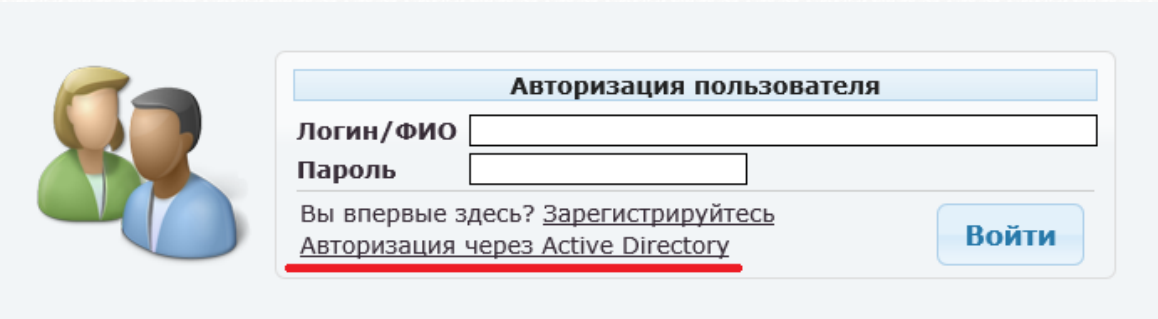
2. Откроется диалог «Параметры синхронизации»:



- **Наименование** - Название синхронизации. Значение этого параметра также будет использоваться в качестве названия для корневой группы синхронизации на вкладке Пользователи.
- **Тип синхронизации** - В данном случае рассматривается синхронизация пользователей с Active Directory, поэтому необходимо выбрать этот пункт.
- **Имя домена** - Необходимо ввести имя домена, с которым будет производится синхронизация.
- **IP-адрес DC** - Необходимо ввести IP-адрес или DNS-имя сервера, который является контроллером данного домена.
- **Использовать учетную запись фоновой службы INDIGO** - Если флаг установлен, то для доступа к каталогам AD будет использоваться аккаунт, от которого запущена служба системы тестирования IndigoController.exe. Система INDIGO не вносит никаких изменений в AD, поэтому в целях безопасности

достаточно создать специальную учетную запись с правами только на чтение данных о подразделениях и пользователях из AD. Если Вы хотите использовать отдельную учетную запись, то необходимо снять данный флаг и ввести логин и пароль пользователя домена, под которым система тестирования будет авторизовываться для чтения данных из Active Directory. В поле «Логин» необходимо ввести полное имя доменной учетной записи в формате: <имя_пользователя>@<имя_домена> или <ДОМЕН>\<логин>.

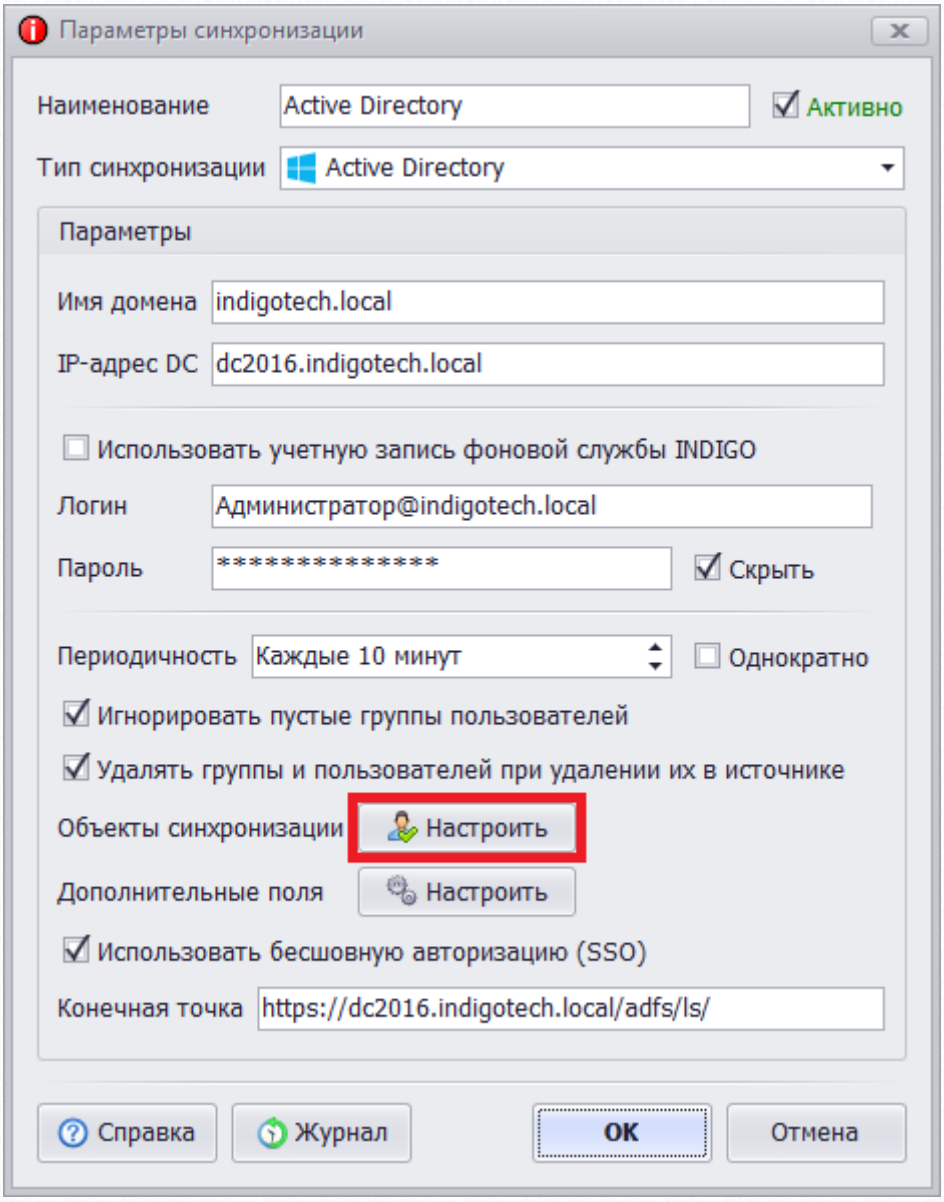
- **Периодичность** - Синхронизация пользователей может происходить однократно или регулярно через заданный период времени.
- **Игнорировать пустые группы пользователей** – При установке данного флага, группы пользователей, в которых нет ни одного пользователя, будут игнорироваться.
- **Удалять группы и пользователей при удалении их в источнике** - При установке данного флага, если в период между процессами синхронизаций в AD пользователи или подразделения будут удалены, то в системе тестирования объекты также будут удалены.
- **Использовать бесшовную авторизацию (SSO)** - Если в домене настроена служба Active Directory Federation Services, то есть возможность использовать бесшовную авторизацию пользователей без ввода логина и пароля. Для настройки необходимо ввести адрес конечной точки WS-Federation в поле «Конечная точка». Если данный флаг установлен, то в веб-интерфейсе на странице с формой авторизации появится ссылка «Авторизация через Active Directory», перейдя по которой пользователь попадет в учетную запись минуя ввод логина и пароля.



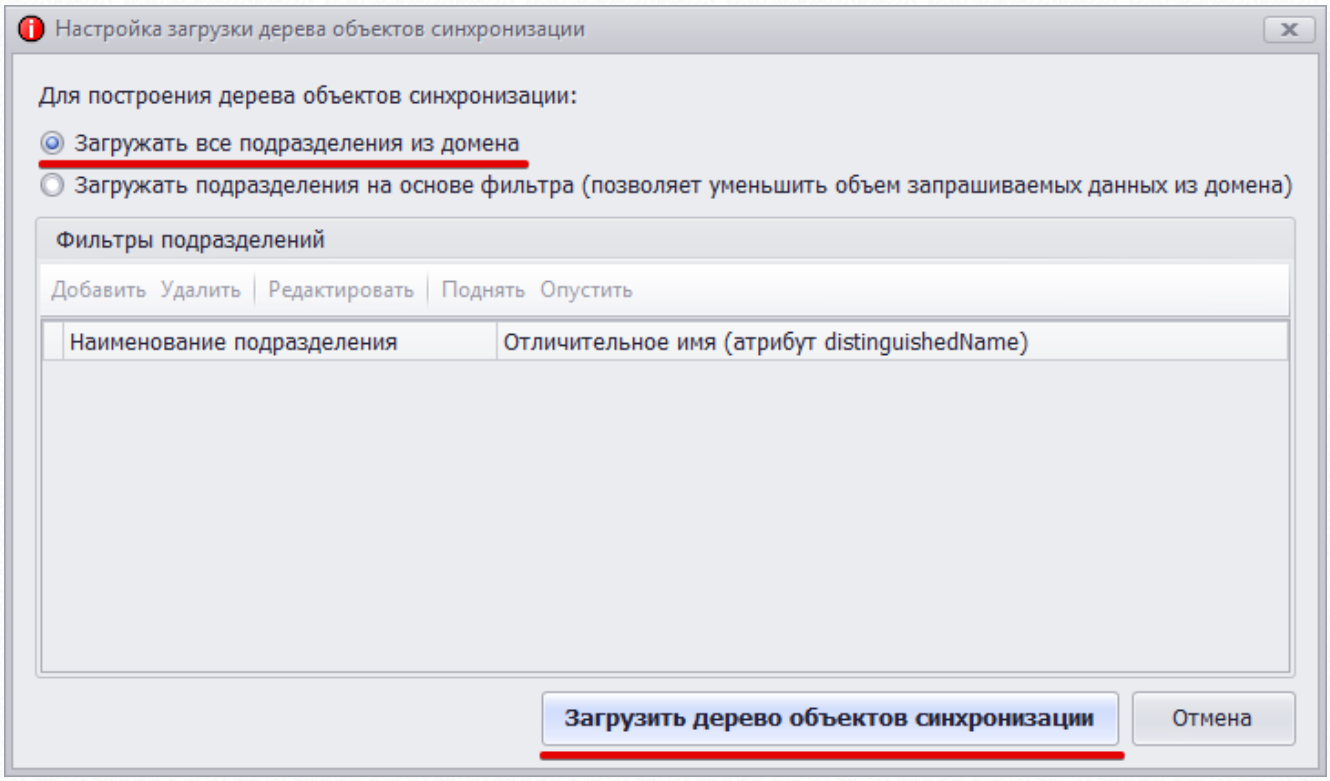
При необходимости можно организовать точку входа в виде ярлыка на рабочем столе пользователя или в виде кнопки на сайте организации, в которых будет указана ссылка на систему тестирования с добавлением в конце адреса «/ad» (https://url-системы-тестирования/ad), что позволит авторизовываться в системе тестирования сразу после перехода по данной ссылке без посещения страницы авторизации.

Подробнее про настройку бесшовной авторизации можно прочесть в разделе «2.2. Настройка бесшовной авторизации пользователей на базе служб федерации Active Directory».

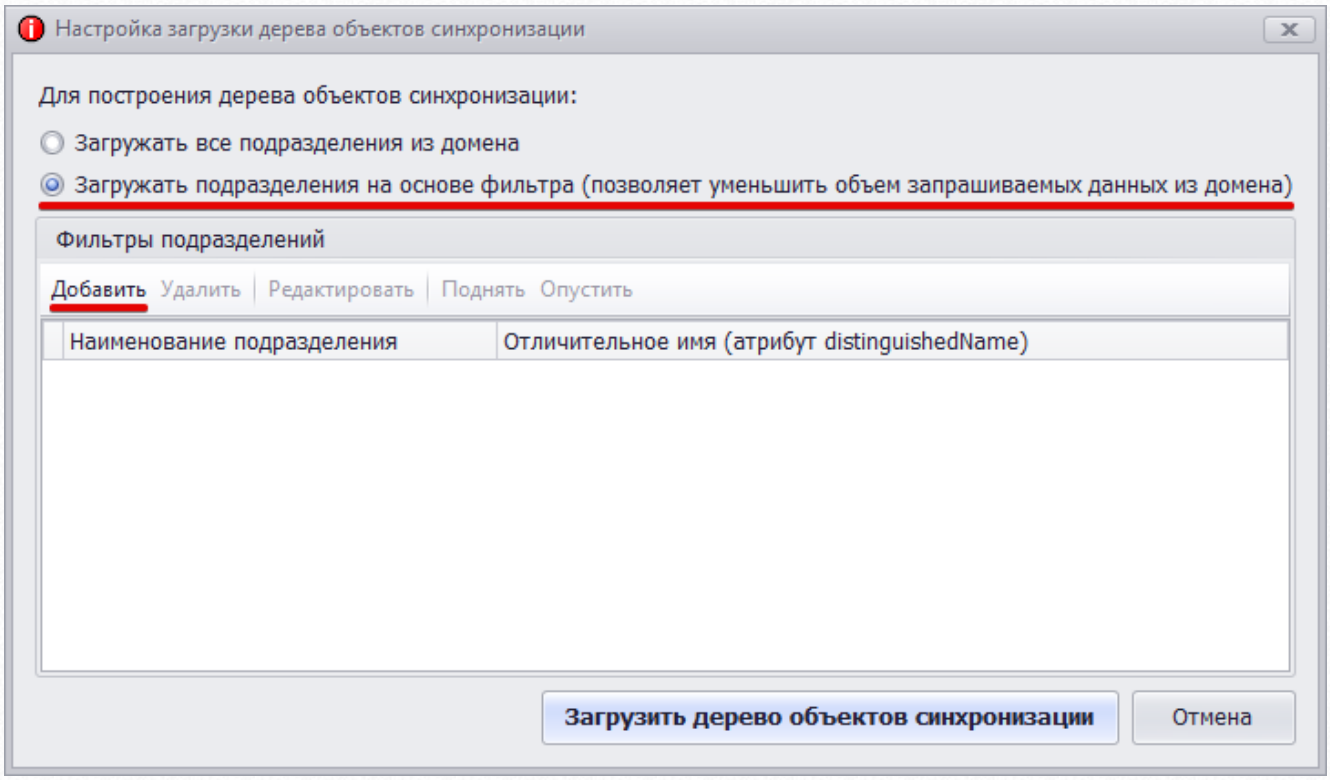
3. После установки параметров нажмите на кнопку «Настроить» в пункте «Объекты синхронизации».



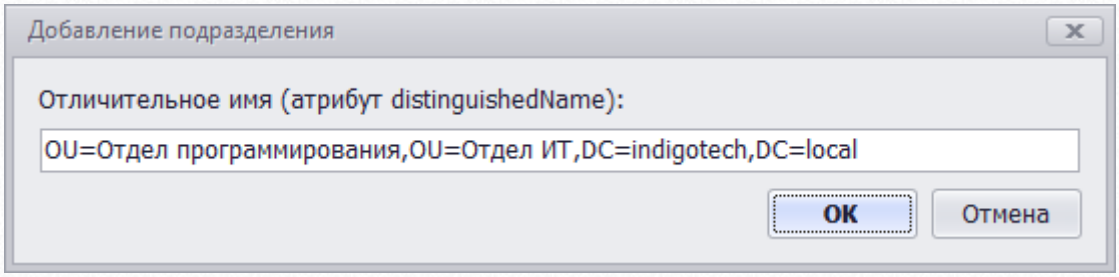
4. В появившемся окне «Настройка загрузки дерева объектов синхронизации» необходимо выбрать источник данных. По умолчанию установлена опция «Загружать все подразделения из домена» (в большинстве случаев процесс проходит корректно и настраивать фильтры для загрузки данных из конкретных подразделений нет необходимости). Для продолжения нажмите на кнопку «Загрузить дерево объектов синхронизации».



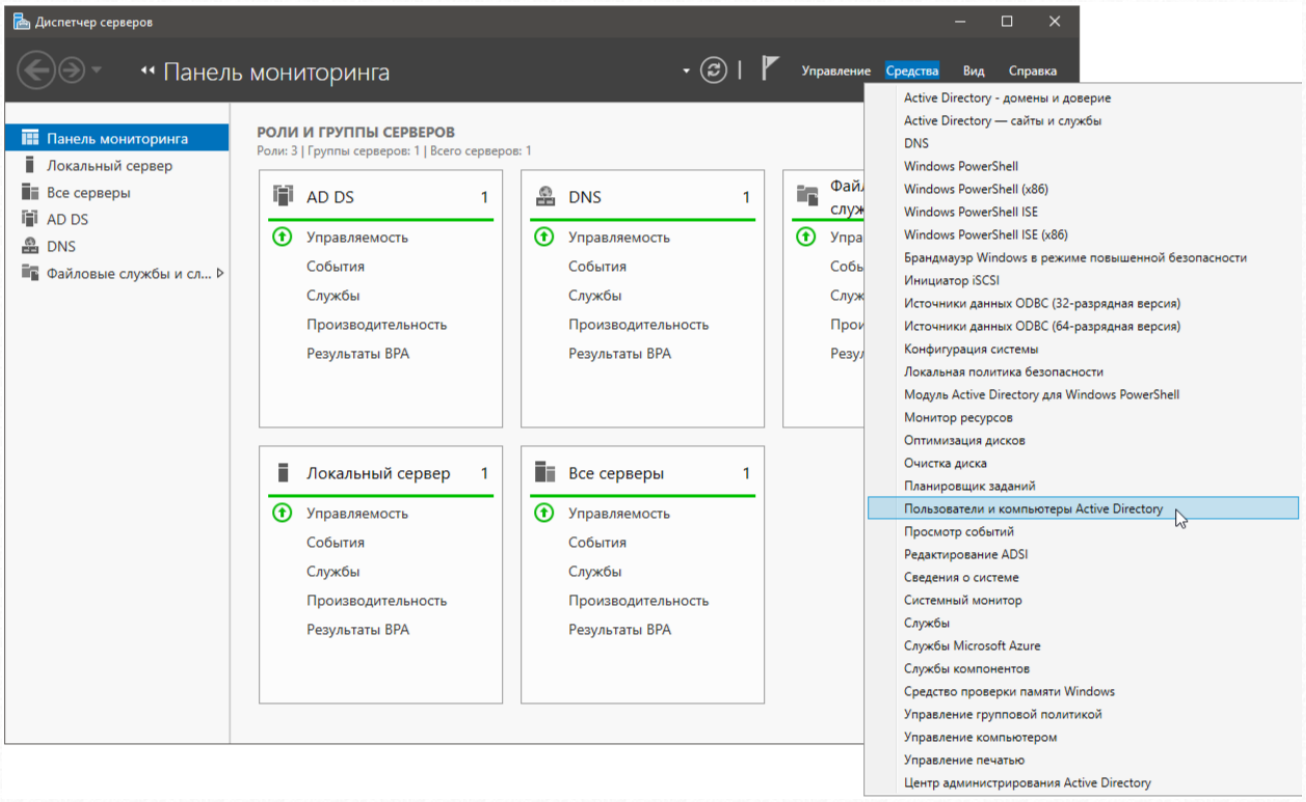
В некоторых случаях может возникнуть необходимость загружать данные только из конкретных подразделений. Например, если в домене большое количество пользователей и процесс получения данных занимает длительное время, либо пользователь, от имени которого происходит подключение к Active Directory, не будет иметь права на загрузку всех подразделений домена. В этих случаях необходимо выбрать опцию «Загружать подразделения на основе фильтра (позволяет уменьшить объем запрашиваемых данных из домена)» и добавить в таблицу только те подразделения, которые будут участвовать в синхронизации. Для добавления подразделений нажмите на кнопку «Добавить» в меню над таблицей.



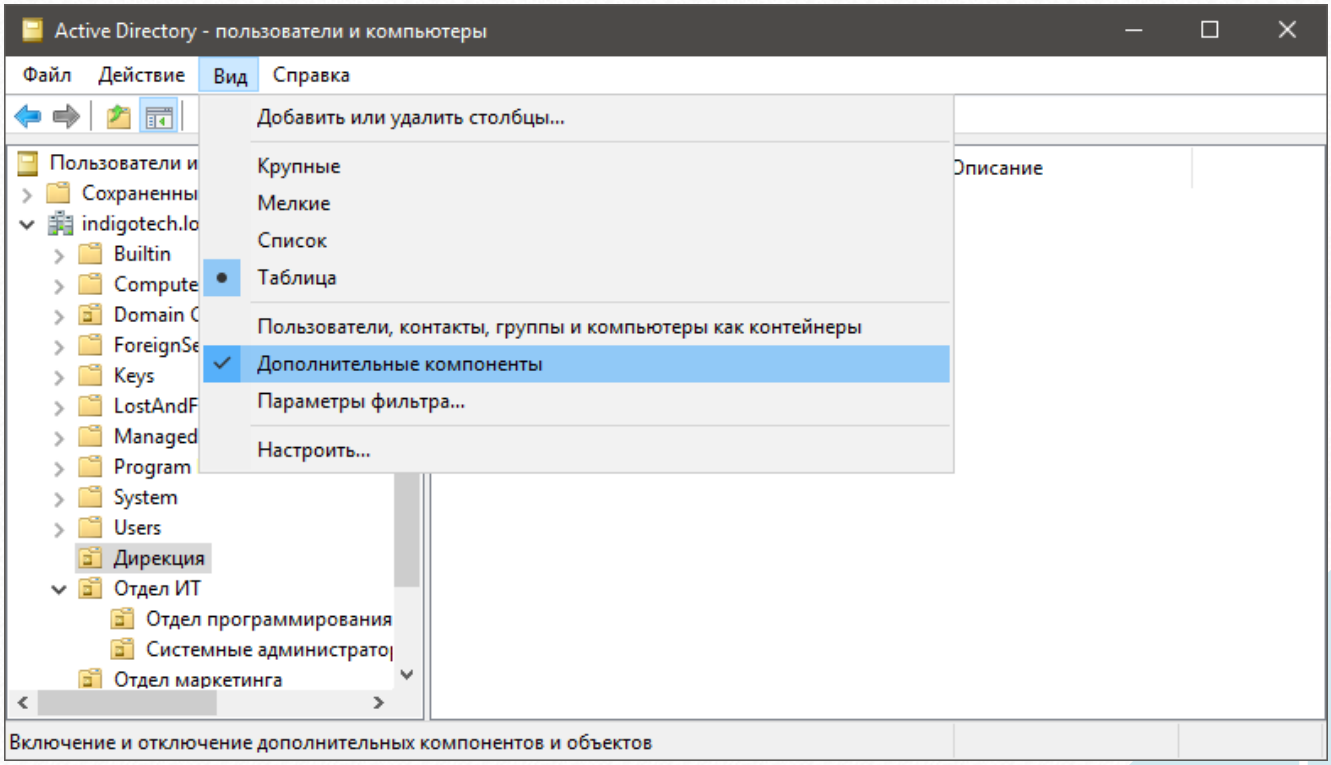
В появившемся окне «Добавление подразделения» в поле для ввода необходимо вписать атрибут Active Directory «distinguishedName» того подразделения, которое будет участвовать в синхронизации.



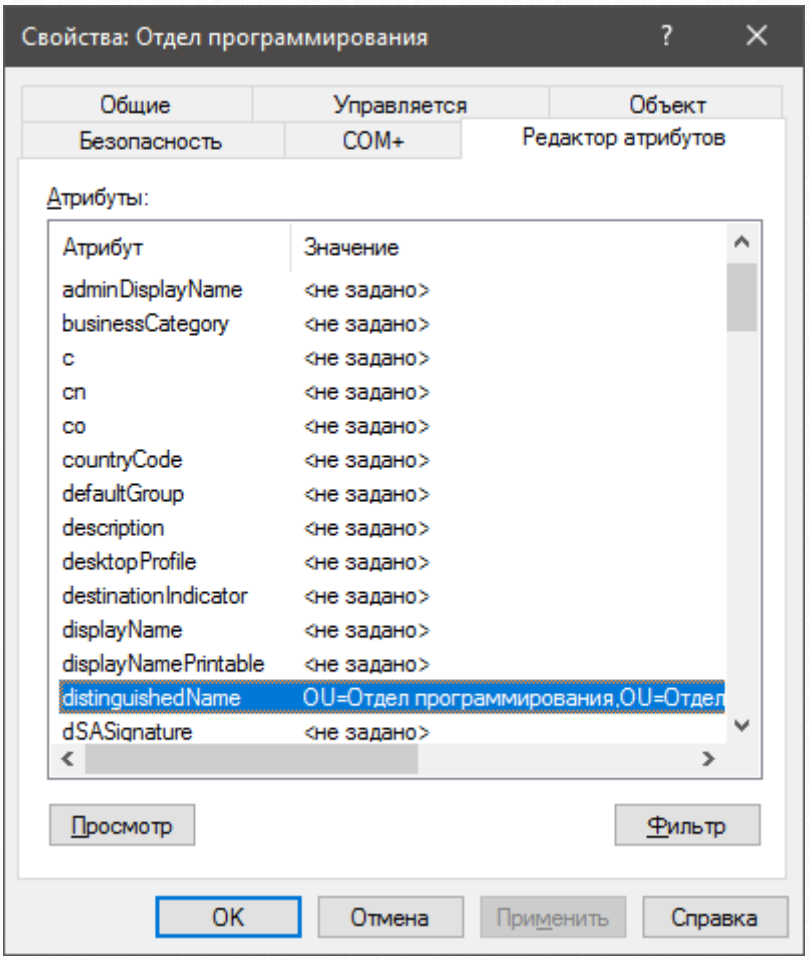
Для того чтобы узнать значение атрибута «distinguishedName» у конкретного подразделения необходимо в окне «Диспетчер серверов» выбирать пункт «Средства» → «Пользователи и компьютеры Active Directory».



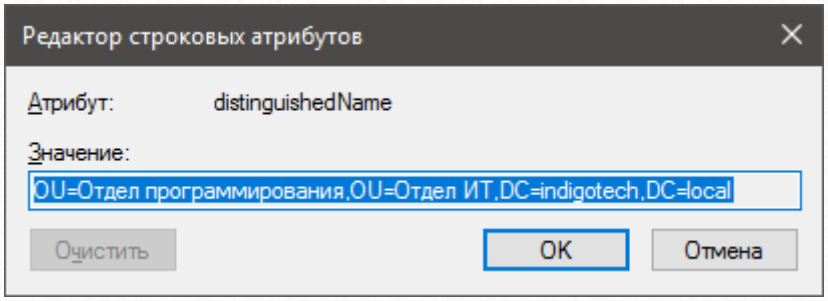
В открывшемся окне убедитесь, что включен флаг «Вид» → «Дополнительные компоненты».



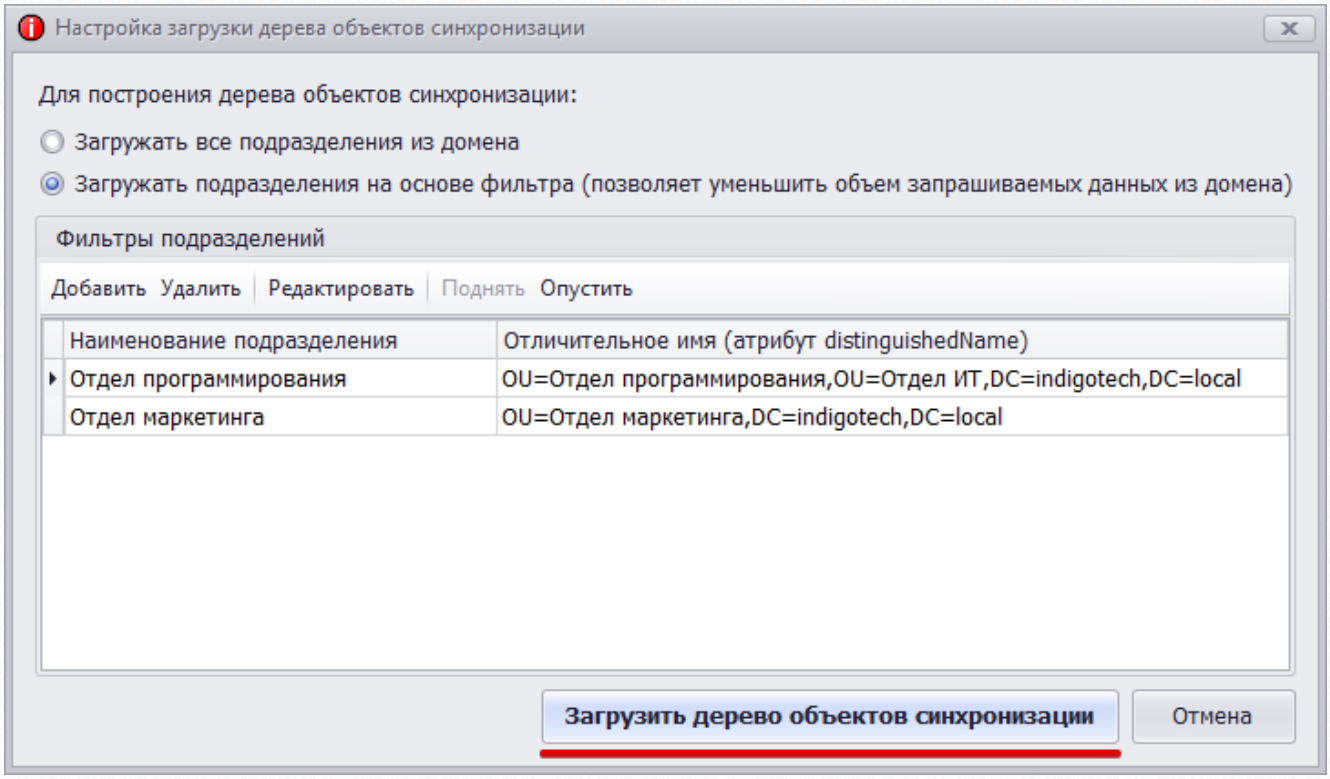
В дереве слева выберите подразделение и кликнете по нему правой кнопкой мыши. В выпадающем меню выберите пункт «Свойства». В появившемся окне перейдите на вкладку «Редактор атрибутов» и в списке атрибутов найдите «distinguishedName».



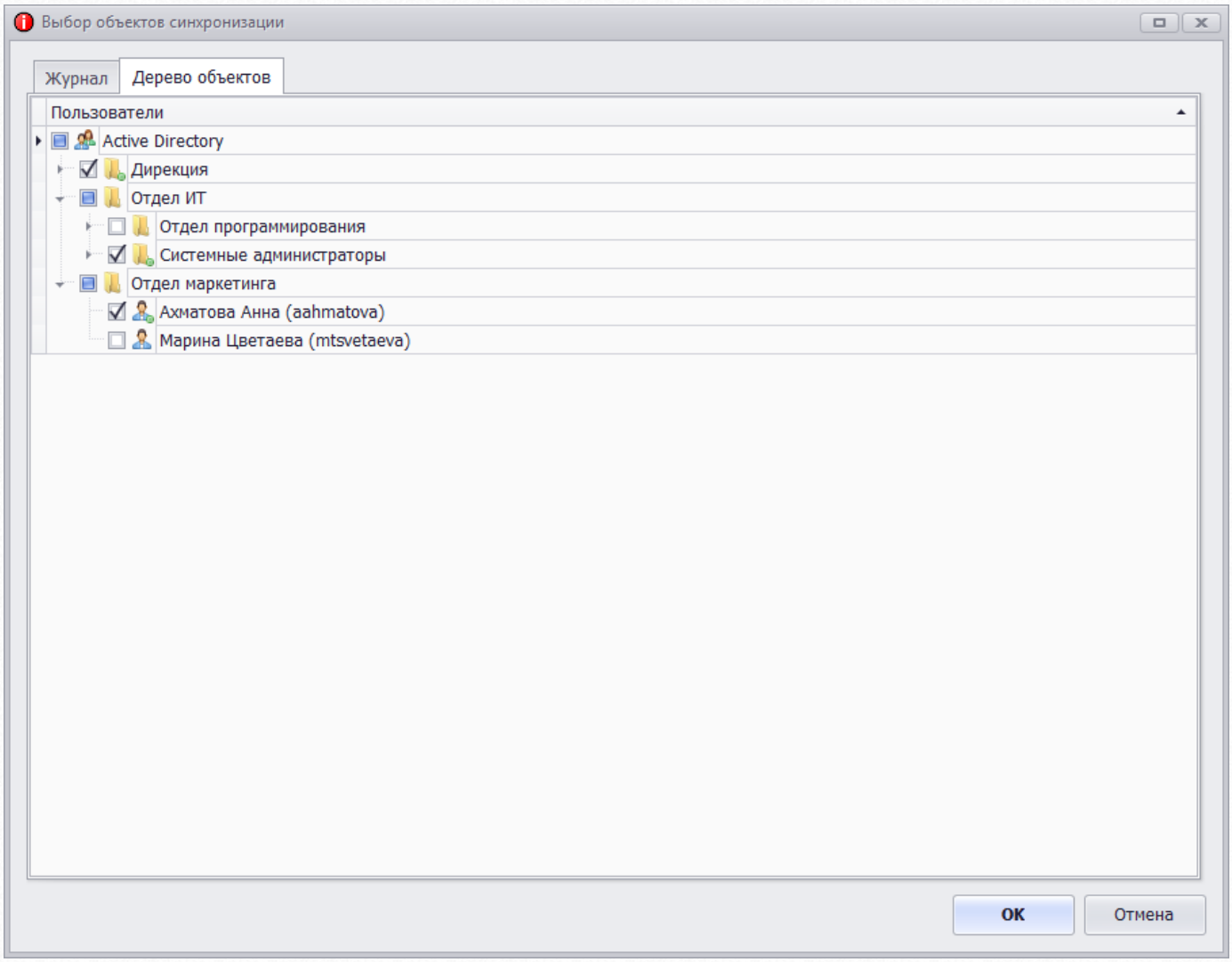
Дважды кликнув по элементу списка откроется окно «Редактор строковых атрибутов» откуда можно скопировать значение атрибута в буфер обмена и вставить в поле «Отличительное имя (атрибут distinguishedName)» в системе тестирования.



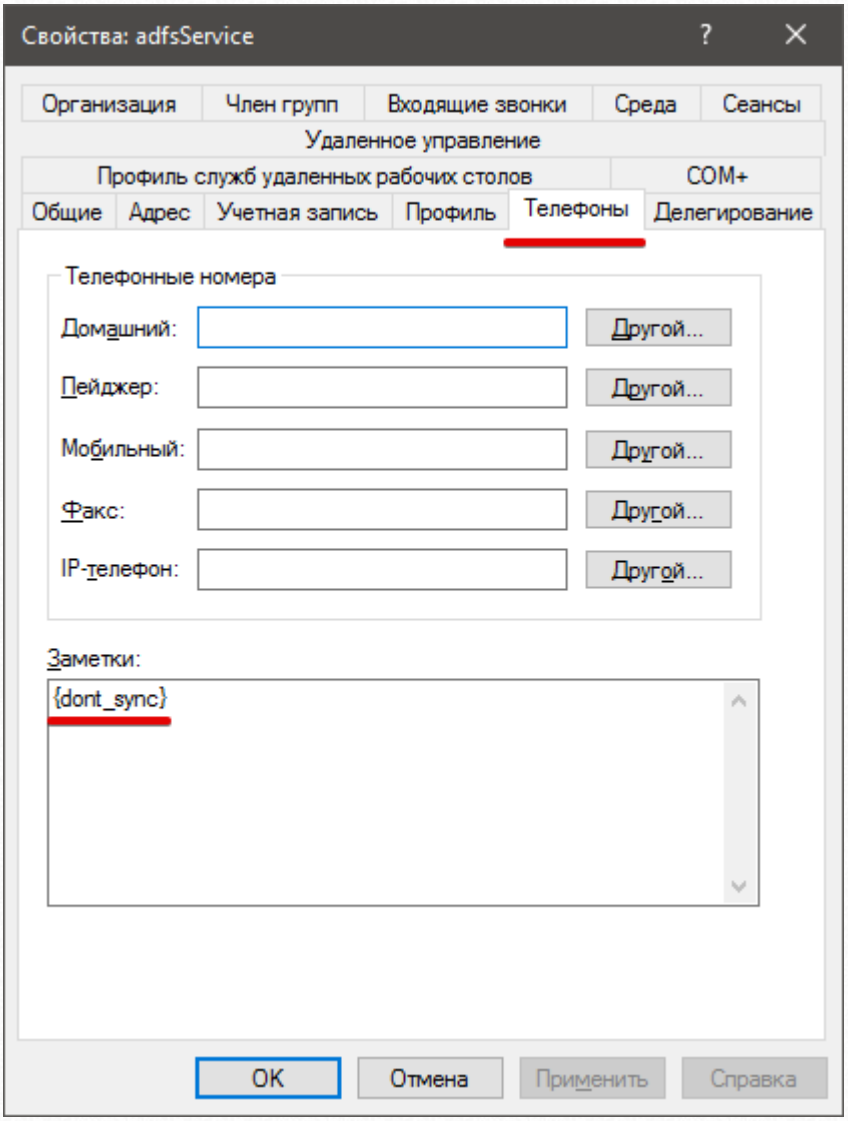
После того, как Вы добавили все необходимые подразделения нажмите на кнопку «Загрузить дерево объектов синхронизации».



5. Система тестирования подключится по указанным данным к контроллеру домена и получит информацию о группах и пользователях, которые возможно синхронизировать. В диалоге «Выбор объектов синхронизации» в процессе получения информации о пользователях на вкладке «Журнал» будет отображаться текущий этап операции. После получения необходимых данных вкладка «Дерево объектов» автоматически станет активной. В появившемся дереве необходимо отметить те группы или отдельных пользователей, которых необходимо синхронизировать. При выборе группы будут синхронизированы все группы и пользователи, которые в нее входят. Также при появлении в ней новых групп или пользователей они будут синхронизированы автоматически. После выбора нужных объектов нажмите на кнопку «ОК».

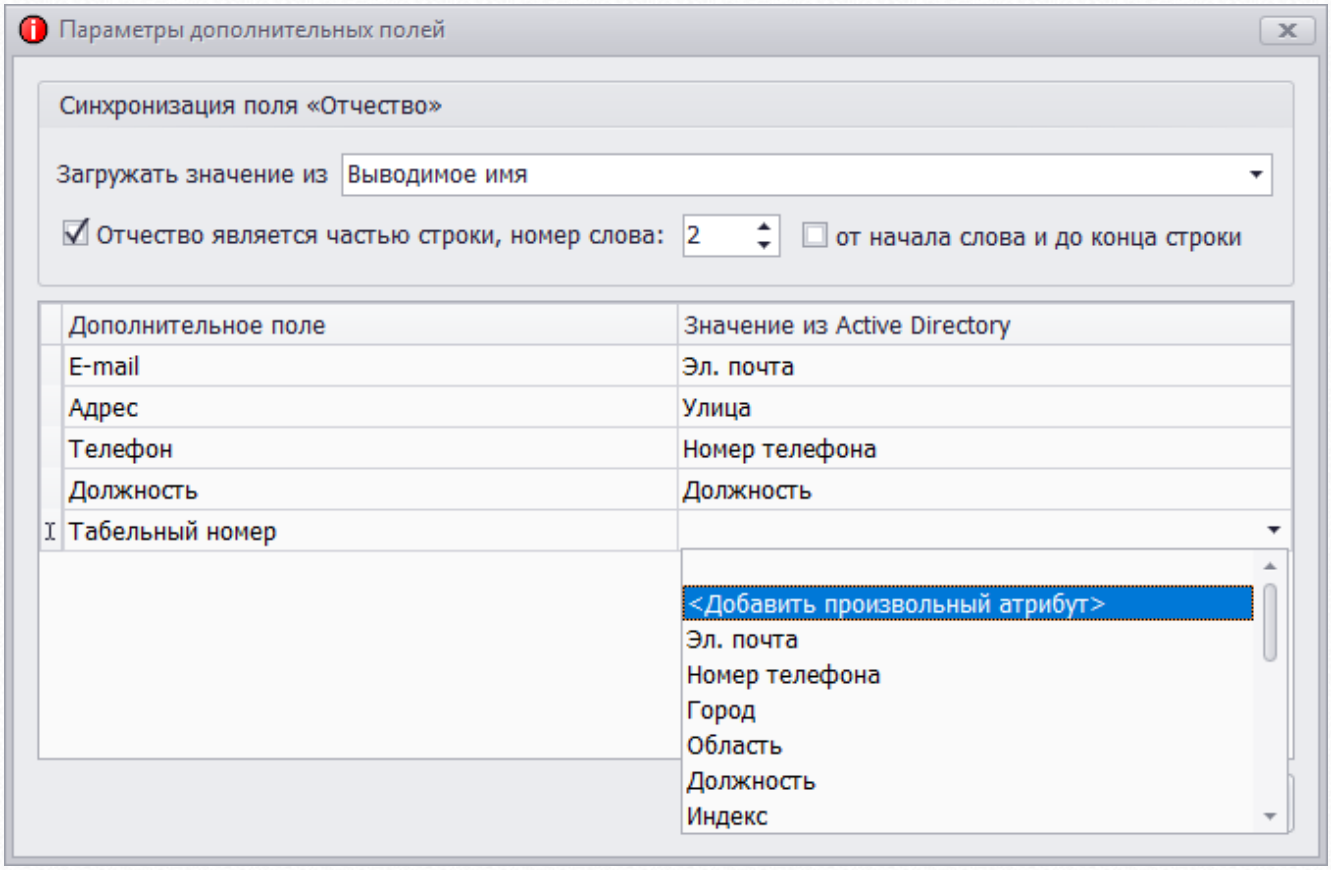


Если в домене имеются пользователи, которых необходимо исключить из синхронизации (например, учетные записи для запуска служб или любые другие служебные записи), то Вы можете добавить специальный маркер «`{dont_sync}`» в поле пользователя «Заметки» и данный пользователь перестанет добавляться в список синхронизации. Для этого зайдите на контролере домена откройте окно «Active Directory – пользователи и компьютеры» и отредактируйте нужного пользователя как показано на рисунке ниже.

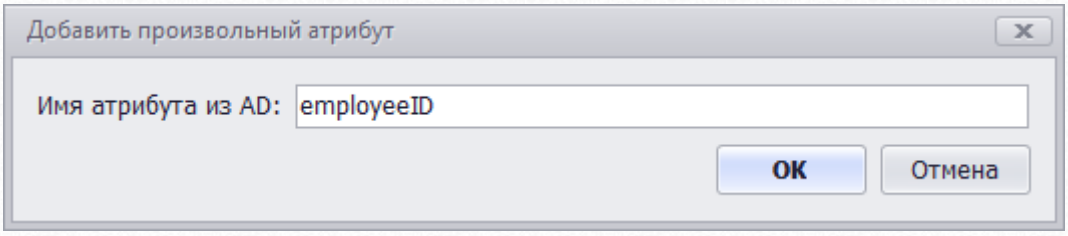


Поле «Заметки» не обязательно должно быть строго равно этому маркеру, а может его включать в своем тексте. Например, если у Вас заметки уже используются под какие-то данные, то для исключения пользователя из списка синхронизации можно дописать маркер «`{dont_sync}`» в конце текста заметок.

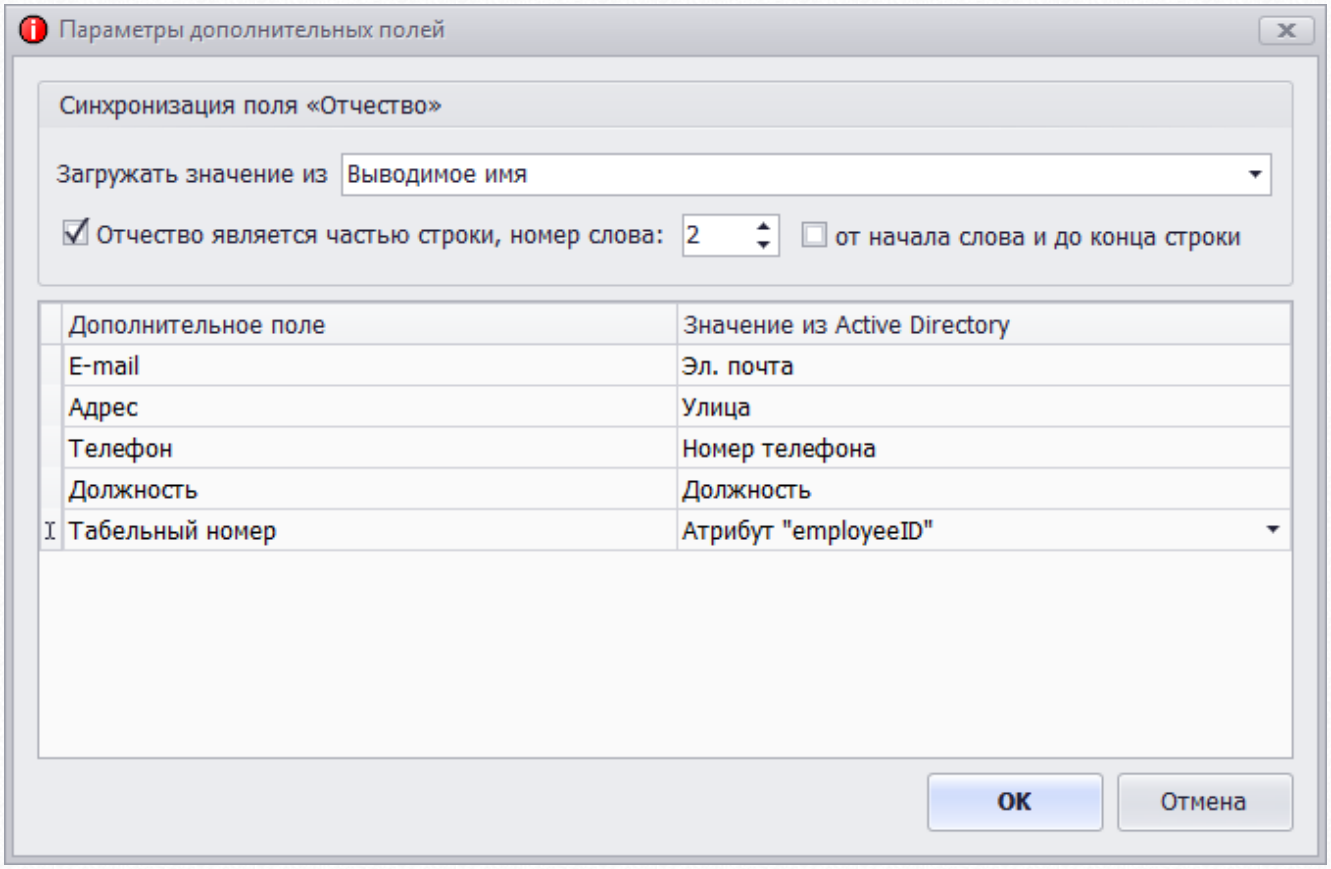
6. Если в системе тестирования используются дополнительные поля, то имеется возможность получить дополнительную информацию из AD по каждому пользователю и сохранить ее в соответствующих дополнительных полях системы тестирования INDIGO. Для этого нажмите на кнопку «Дополнительные поля». В карточке пользователя Active Directory не предусмотрено поле для хранения отчества пользователя, но если Вы храните его в каком-то атрибуте AD, то в этом окне возможно настроить его загрузку. Для этого в открывшемся диалоге «Параметры дополнительных полей» в области "Синхронизация поля «Отчество»" выберите атрибут, в котором хранится отчество пользователя. Если отчество является частью значения атрибута, например, вторым или третьем по счету словом, либо частью строки от какого-то слова и до ее конца, то Вы можете настроить его загрузку. В колонке «Дополнительное поле» находится список полей INDIGO, а в колонке «Значение из Active Directory» можно определить соответствующее значение из набора данных AD. Если в выпадающем списке нет того атрибута, значение которого Вам необходимо выгружать в систему тестирования, то имеется возможность добавить его в список атрибутов по его наименованию. Для этого выберите в выпадающем списке пункт «<Добавить произвольный атрибут>».



В открывшемся окне впишите наименование атрибута в поле «Имя атрибута из AD» и нажмите кнопку «ОК».



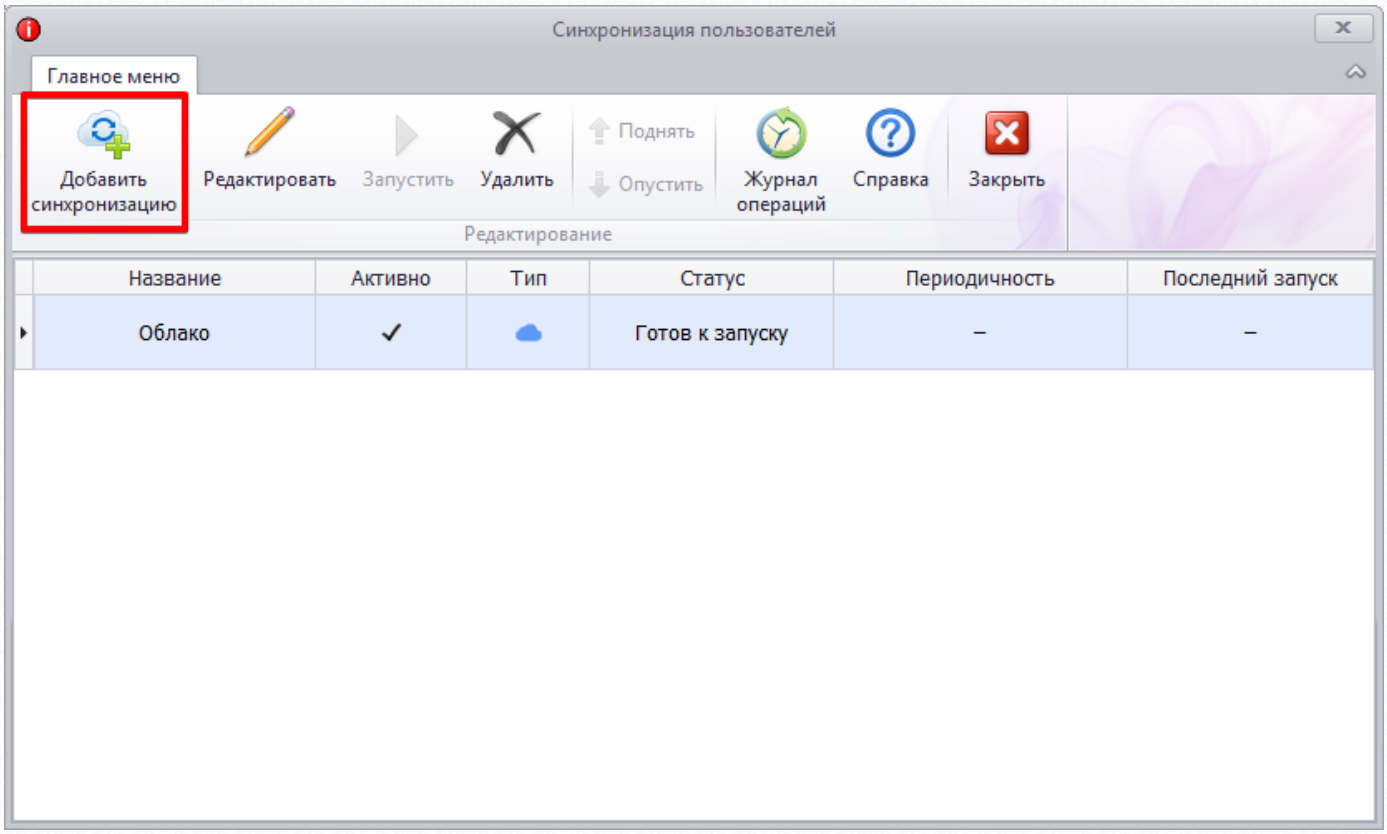
После выставления в окне «Параметры дополнительных полей» всех необходимых настроек и соответствий нажмите на кнопку «ОК».



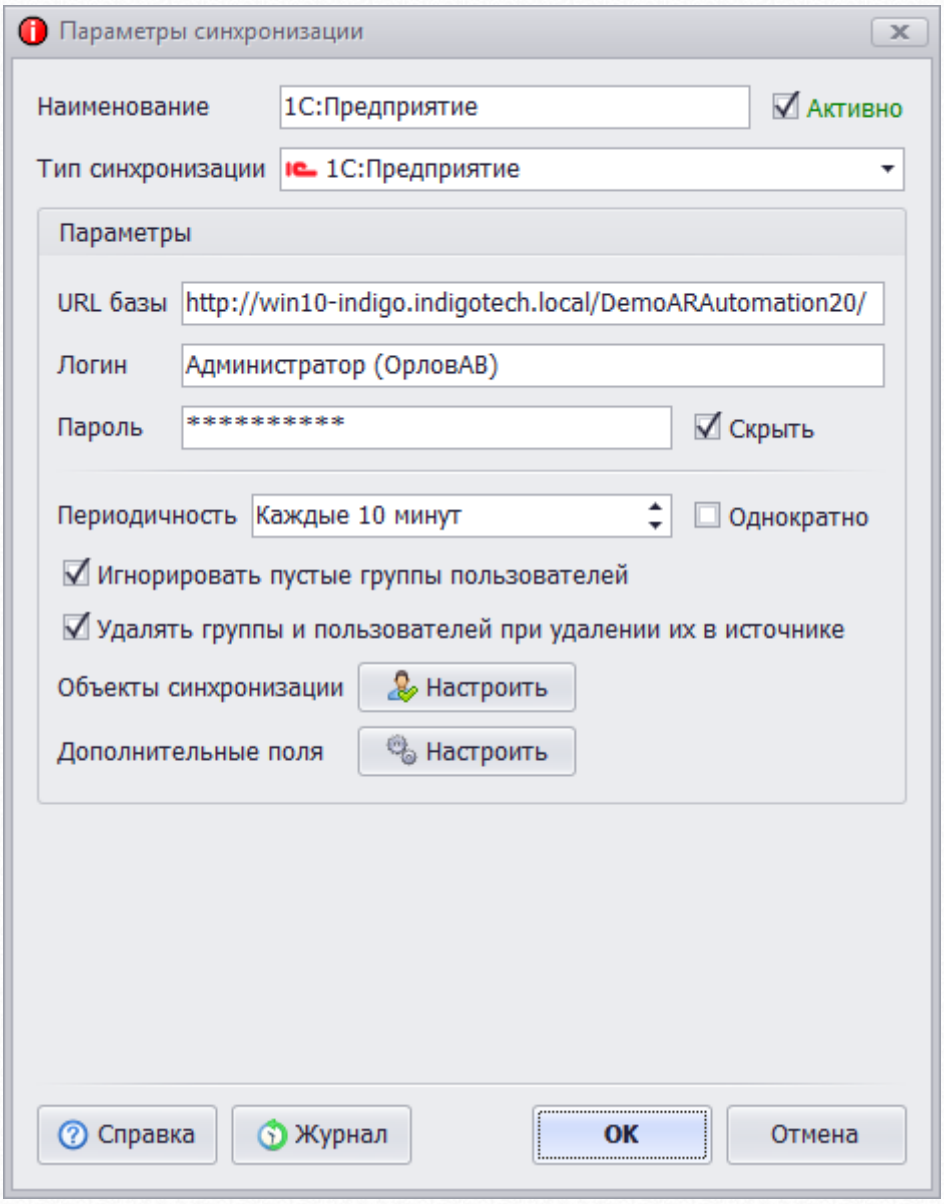
1.2. Настройка синхронизации пользователей с платформой 1С:Предприятие

Синхронизация пользователей системы тестирования INDIGO с пользователями платформы 1С:Предприятие осуществляется с помощью объекта конфигурации «HTTP-сервис». Благодаря механизму расширения конфигурации к базе 1С можно добавить HTTP-сервис без изменений в Вашей основной конфигурации. После публикации базы 1С на веб-сервере фоновая служба системы тестирования с указанной регулярностью будет запрашивать информацию по группам и пользователям с помощью HTTP-запроса. Для аутентификации пользователей используется штатная возможность платформы 1С выступать в качестве OpenID-провайдера.

1. В главном меню окна «Синхронизация пользователей» нажмите на кнопку «Добавить синхронизацию».



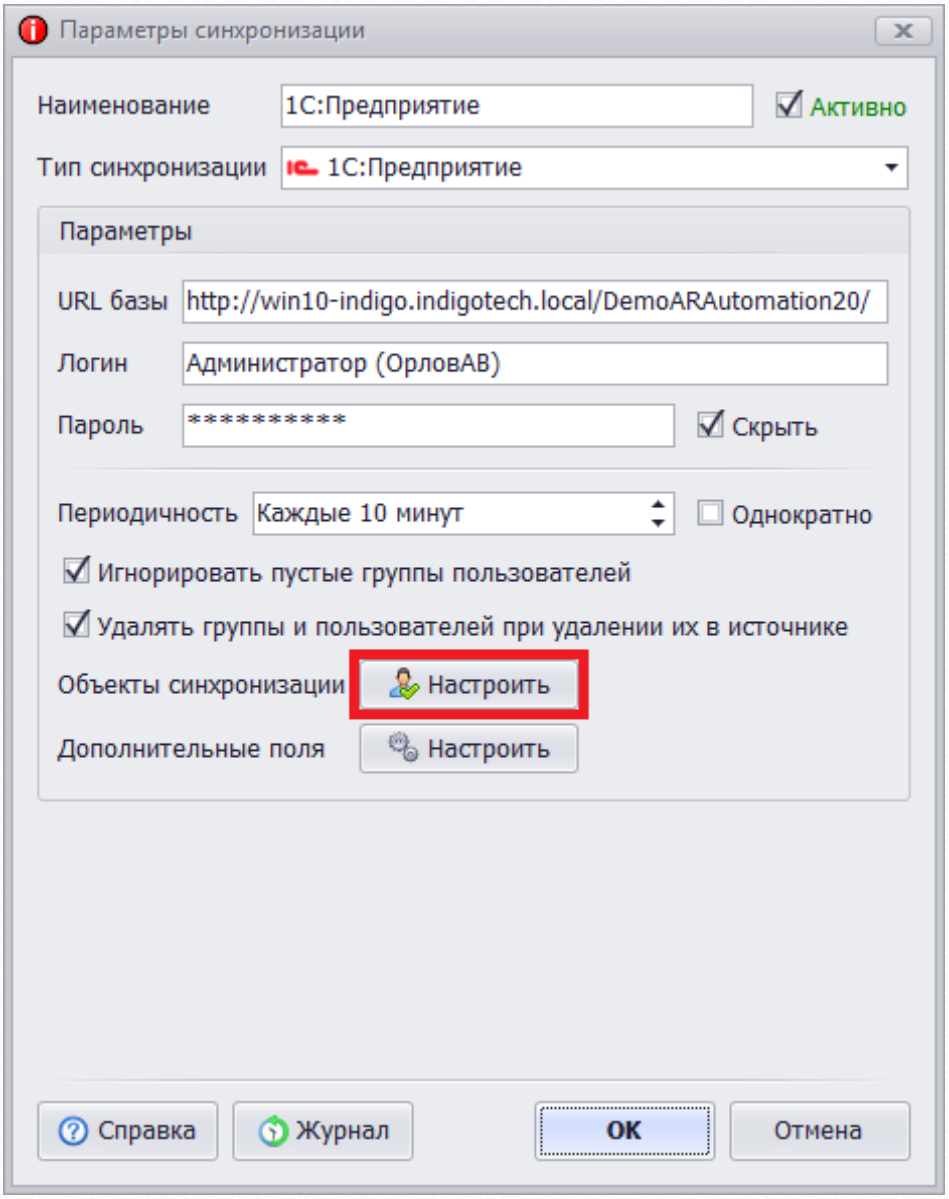
2. Откроется диалог «Параметры синхронизации»:



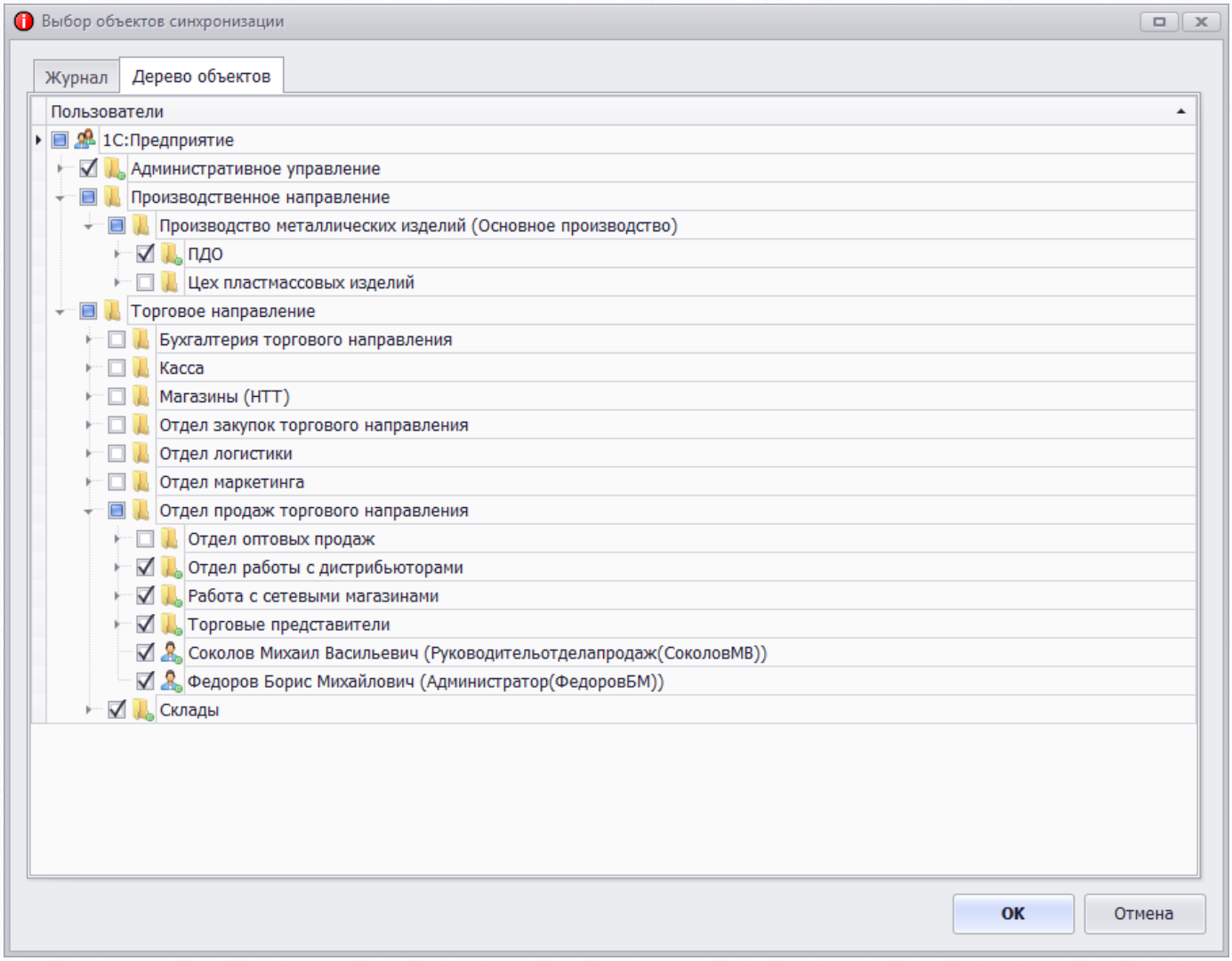
- **Наименование** - Название синхронизации. Значение этого параметра также будет использоваться в качестве названия для корневой группы синхронизации на вкладке Пользователи.
- **Тип синхронизации** - В данном случае рассматривается синхронизация пользователей с 1С:Предприятие, поэтому необходимо выбрать этот пункт.
- **URL базы** - URL-адрес базы 1С опубликованной на веб-сервере.
- **Логин** и **Пароль** - Данные об учетной записи администратора базы 1С.
- **Периодичность** - Синхронизация пользователей может происходить однократно или регулярно через заданный период времени.
- **Игнорировать пустые группы пользователей** - При установке данного флага, группы пользователей, в которых нет ни одного пользователя, будут игнорироваться.
- **Удалять группы и пользователей при удалении их в источнике** - При установке данного флага, если в период между процессами синхронизаций в 1С

пользователи или подразделения будут удалены, то в системе тестирования объекты также будут удалены.

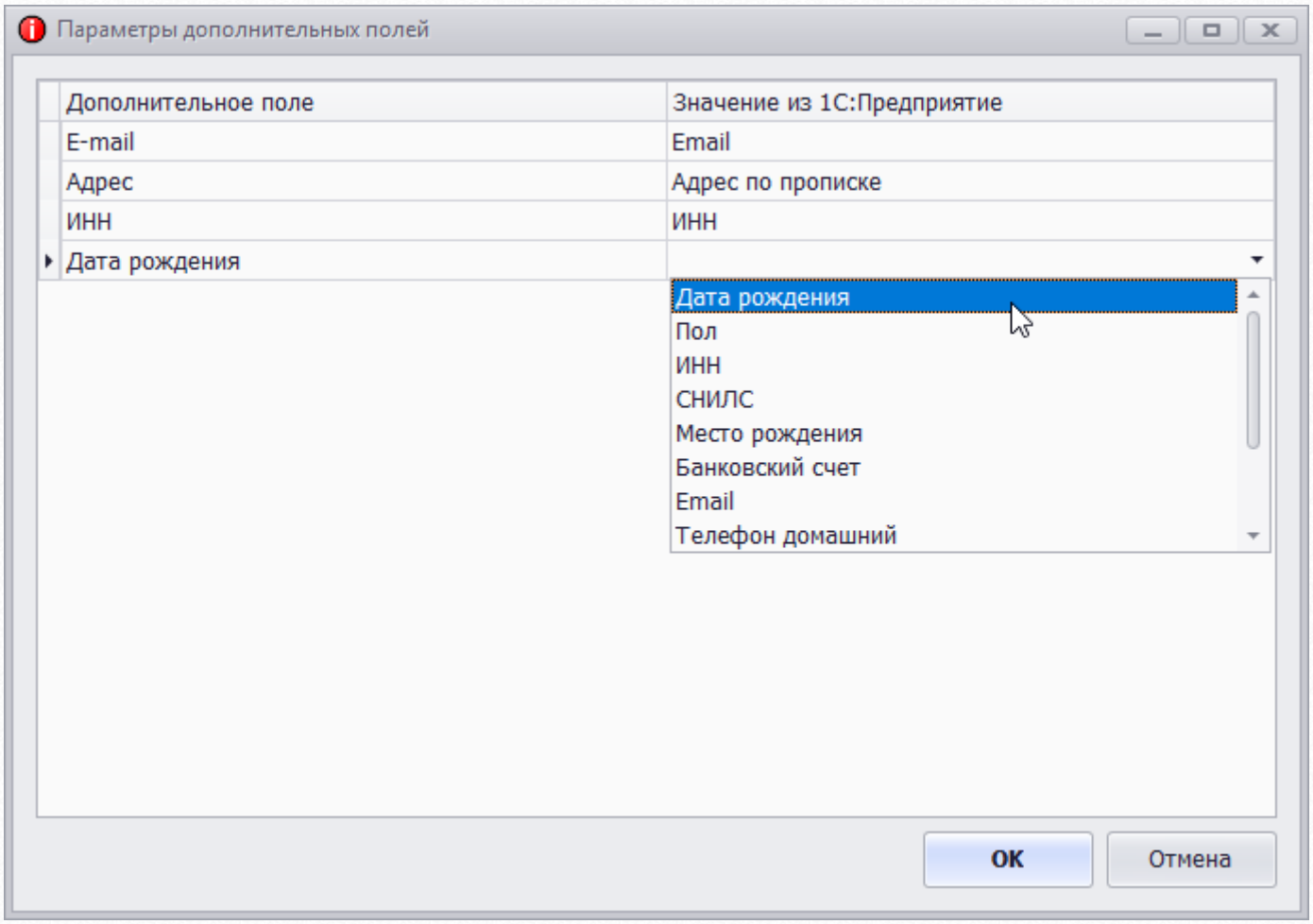
3. После установки параметров нажмите на кнопку «Настроить» в пункте «Объекты синхронизации». Система тестирования подключится по указанным данным к базе 1С и получит информацию о группах и пользователях, которые возможно синхронизировать.



В диалоге «Выбор объектов синхронизации» в процессе получения информации о пользователях на вкладке «Журнал» будет отображаться текущий этап операции. После получения необходимых данных вкладка «Дерево объектов» автоматически станет активной. В появившемся дереве необходимо отметить те группы или отдельных пользователей, которые необходимо синхронизировать. При выборе группы будут синхронизированы все группы и пользователи, которые в нее входят. Также при появлении в ней новых групп или пользователей они будут синхронизированы автоматически. После выбора нужных объектов нажмите на кнопку «ОК».



4. Если в системе тестирования используются дополнительные поля, то имеется возможность также получить дополнительную информацию из 1С по каждому пользователю и сохранить ее в соответствующих полях. Нажмите на кнопку «Дополнительные поля», чтобы установить соответствия. В открывшемся диалоге «Параметры дополнительных полей» в колонке «Дополнительное поле» находится список настроенных доп. полей пользователей. В колонке «Значение из Active Directory» можно определить соответствующее значение из набора данных, который может быть получен из 1С. После выставления всех необходимых соответствий нажмите на кнопку «ОК».



1.3. Настройка синхронизации пользователей со сторонней системой

Универсальный алгоритм работы синхронизации пользователей со сторонней системой состоит из двух этапов:

1. Формирование списка групп и пользователей в специальном формате.
2. Запись этого списка в базу данных системы тестирования с помощью SQL-запроса.

После записи автоматически инициируется процесс, считывающий список и обновляющий информацию в системе.

Для настройки синхронизации перейдите на вкладку «Пользователи» в главном окне программы и нажмите на кнопку «Синхронизация пользователей». В открывшемся окне нажмите на кнопку «Добавить синхронизацию», выберите тип синхронизации «Сторонние системы».

Список объектов представляет собой текст в кодировке UTF-8. Каждый атрибут объекта начинается с новой строки и имеет вид:

```
«Имя атрибута» = «Значение»
```

Между собой объекты отделяются пустой строкой.

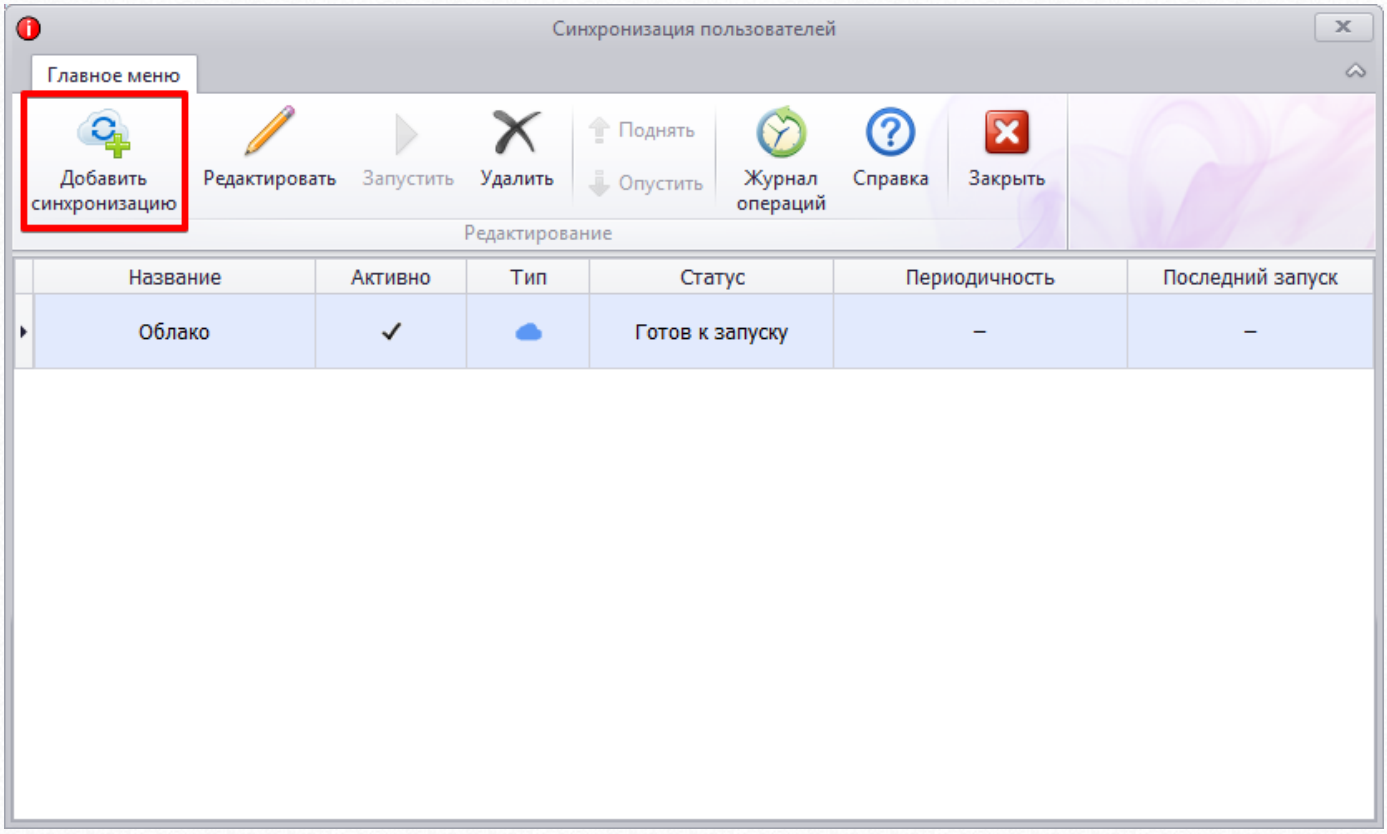
Имя атрибута	Описание
is_group	Является ли объект группой пользователей. Значение ноль 0 – объект является пользователем, другие значения – группой
id	Уникальная строка, однозначно определяющая объект в списке
parent_id	Уникальная строка, однозначно определяющая родительскую группу в списке. У корневого объекта параметр должен быть пустой
name	Наименование группы, либо имя пользователя
surname	Фамилия
middle_name	Отчество
login	Логин
password	Пароль
note	Заметки
custom_fieldN	Дополнительное поле, где N - ID дополнительного поля

Параметры `is_group`, `id`, `parent_id`, `name`, `note` являются общими для групп и пользователей, остальные параметры используются только для описания пользователей. Отсутствие в описании объекта какого-либо параметра допустимо, в этом случае значение приравнивается к пустой строке.

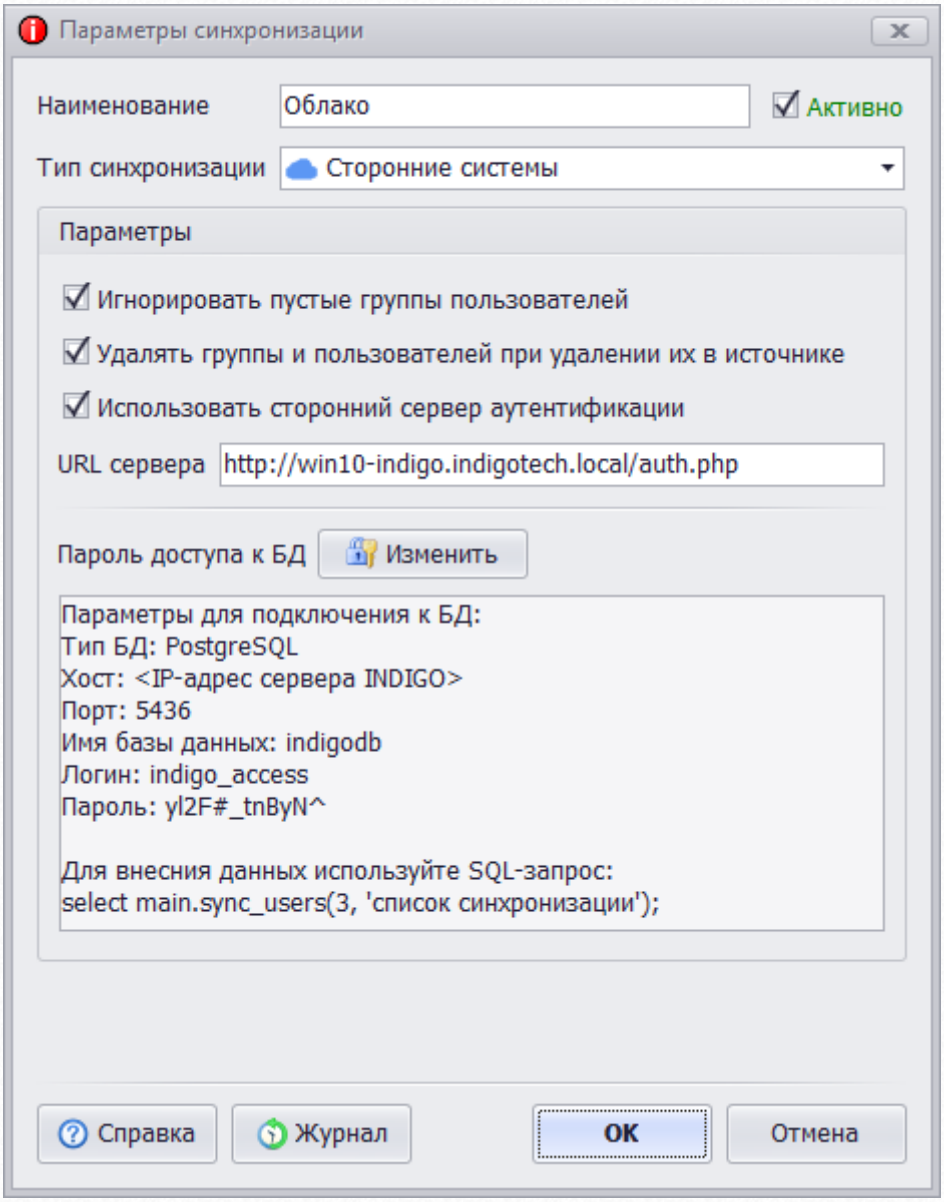
Для примера рассмотрим структуру организации, представленную на рисунке:

Группа	Фамилия	Имя	Отчество	Логин	Заметки
Отдел маркетинга					
	Шевченко	Ольга	Викторовна	ШевченкоОВ	
Отдел продаж					
Отдел оптовых продаж					
	Гладилина	Вера	Михайловна	ГладилинаВМ	
	Кислов	Артем	Сергеевич	КисловАС	Испытательный срок до 10.11.2018
	Соколов	Михаил	Васильевич	СоколовМВ	
	Орлов	Александр	Владимирович	ОрловАВ	

1. В главном меню окна «Синхронизация пользователей» нажмите на кнопку «Добавить синхронизацию».



2. Откроется диалог «Параметры синхронизации»:



- **Наименование** – Название синхронизации. Значение этого параметра также будет использоваться в качестве названия для корневой группы синхронизации на вкладке Пользователи.
- **Тип синхронизации** - В данном случае рассматривается синхронизация пользователей со сторонней системой, поэтому выбрать пункт «Сторонние системы».
- **Игнорировать пустые группы пользователей** - При установке данного флага, группы пользователей, в которых нет ни одного пользователя, будут игнорироваться.
- **Удалять группы и пользователей при удалении их в источнике** - При установке данного флага, если в списке синхронизации не будут переданы какие-либо объекты, которые ранее уже были синхронизированы, то в системе тестирования эти объекты будут удалены.
- **Использовать сторонний сервер аутентификации** - При установке флага необходимо будет указать URL сервера проверки введенных учетных данных.

- При нажатии на кнопку «Изменить» будет сгенерирован новый пароль для сервисной ученой записи. Важно учитывать, что пароль будет изменен и подключения со старым паролем перестанут работать.

3. В окне параметров синхронизации в текстовом поле отображаются все необходимые актуальные данные для подключения к СУБД и записи списка синхронизации в базу данных. Подключение должно осуществляться с помощью сервисной учетной записи «indigo_access». Запись списка производится с помощью вызова SQL-функции main.sync_users() принимающей 2 аргумента:

1. Число – идентификатор синхронизации.
2. Строка – список синхронизации (текст указывается в одинарных кавычках).

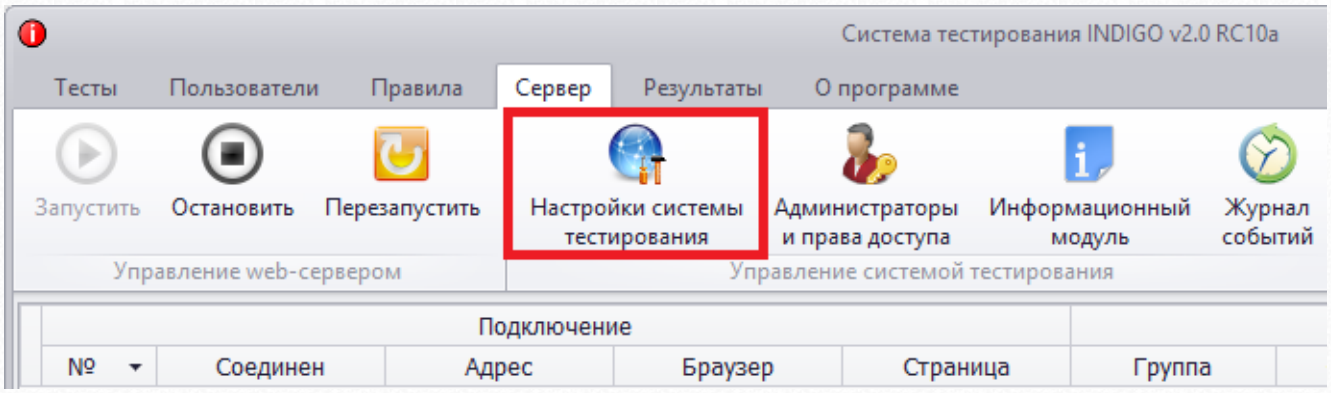
В примере в качестве идентификаторов объектов будут использованы натуральные числа, но стоит отметить, что это могут быть любые строки, в том числе GUID или UUID, единственное требование – это уникальность каждого значения во всем списке. Пользователь с логином «ОрловАВ» и группы «Отдел маркетинга», «Отдел продаж» находятся в корне иерархии, поэтому у этих объектов будет отсутствовать атрибут `parent_id`. Для приведенного примера список синхронизации будет иметь следующий вид:

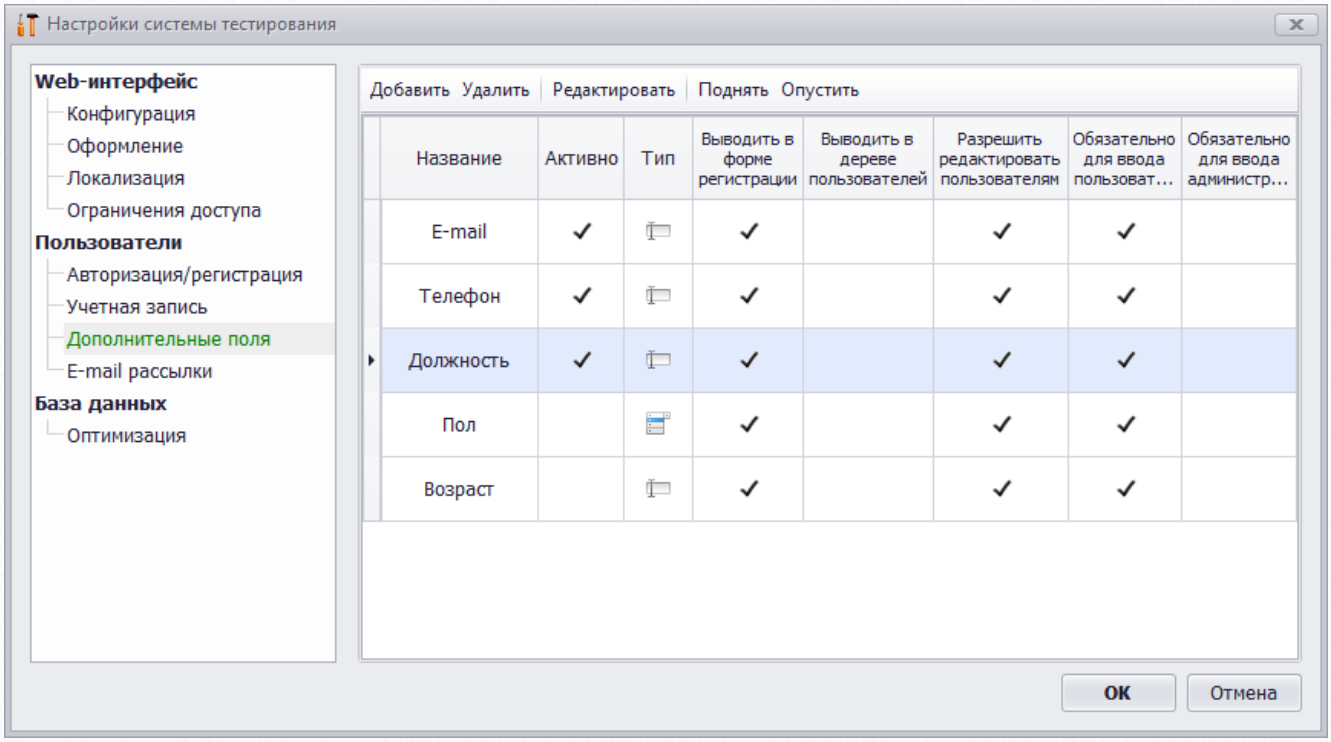
```
is_group=1
id=1
name=Отдел продаж

is_group=1
id=2
parent_id=1
name=Отдел оптовых продаж

is_group=0
id=3
parent_id=2
login=ГладилинаВМ
password=12345
name=Вера
surname=Гладилина
middle_name=Михайловна

is_group=0
id=4
parent_id=2
login=КисловАС
password=12345
name=Артем
surname=Кислов
middle_name=Сергеевич
```

```
note=Испытательный срок до 10.11.2019

is_group=1
id=5
name=Отдел маркетинга

is_group=0
id=6
parent_id=5
login=ШевченкоОВ
password=12345
name=Ольга
surname=Шевченко
middle_name=Викторовна

is_group=0
id=7
parent_id=1
login=СоколовМВ
password=12345
name=Михаил
surname=Соколов
middle_name=Васильевич

is_group=0
id=8
login=ОрловАВ
password=12345
name=Александр
surname=Орлов
middle_name=Владимирович
```

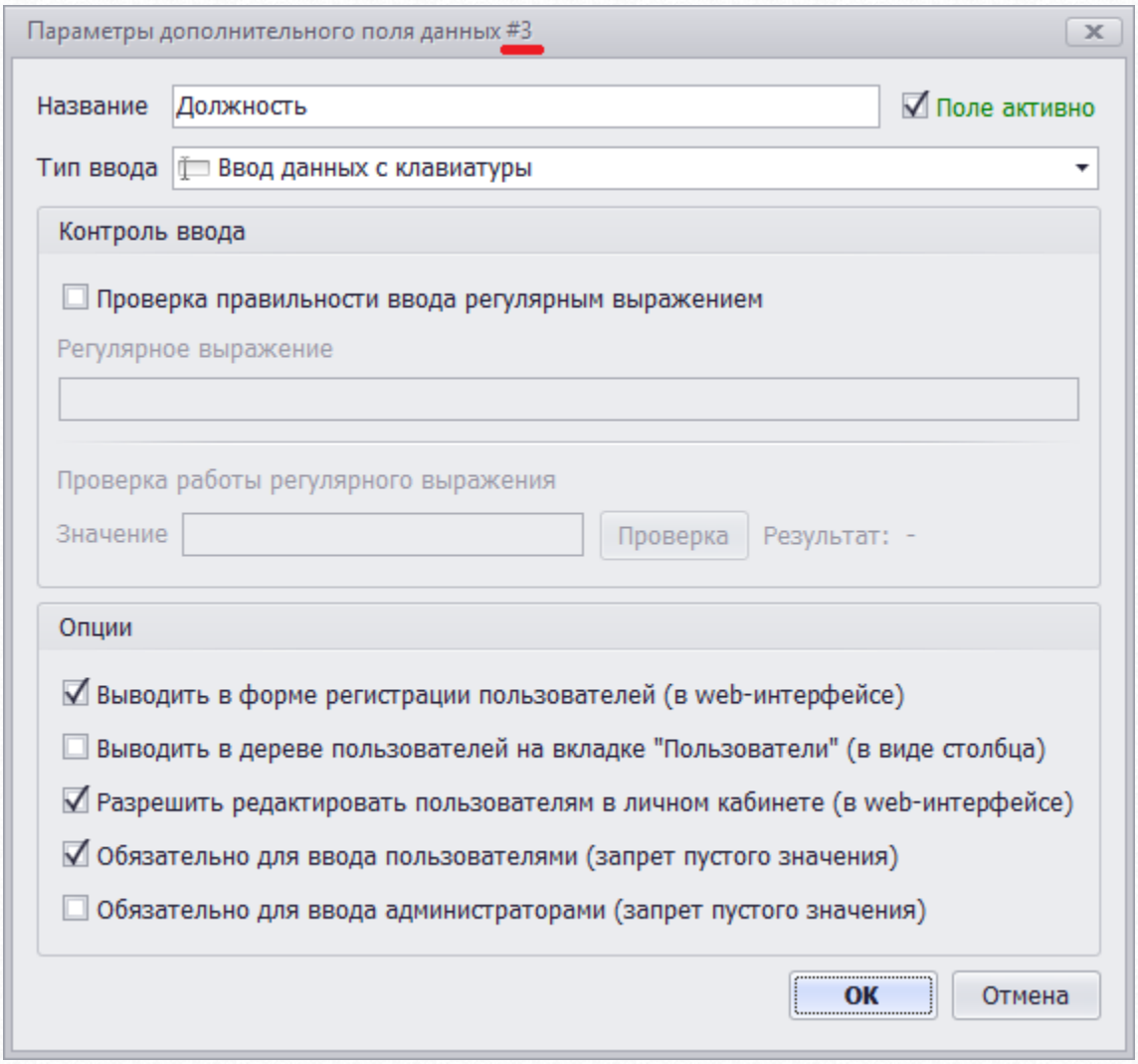
Скачать файл с примером можно по ссылке:
https://indigotech.ru/downloads/files/SyncUsersExample.txt

Для синхронизации значений дополнительных полей необходимо узнать идентификаторы каждого поля, для этого в главном меню системы тестирования перейдите на вкладку «Сервер» и нажмите на кнопку «Настройки системы тестирования». В открывшемся окне «Настройки системы тестирования» в списке слева выберите пункт «Дополнительные поля» и появившейся таблице справа выберите интересующее поле и нажмите на кнопку «Редактировать» в меню над таблицей.





В заголовке открывшегося окна «Параметры дополнительного поля данных» отображается идентификатор поля. На рисунке ID поля равен трем:



Например, если в нашем предыдущем примере пользователю с логином «ОрловАВ» необходимо указать должность «Менеджер», то его код должен выглядеть так:

```
is_group=0
id=8
login=ОрловАВ
password=12345
name=Александр
surname=Орлов
middle_name=Владимирович
custom_field3=Менеджер
```

Если для аутентификации будет использоваться внешний веб-сервис, то в списке пользователей атрибут `password` передавать не нужно. При настройке синхронизации необходимо установить флаг «Использовать сторонний сервер аутентификации» и указать URL этого сервиса в поле «URL сервера аутентификации». В момент авторизации в системе будет создан HTTP-запрос по указанному URL с двумя POST параметрами `login` и `password`. Сервис должен ответить на запрос строкой `true`, если логин и пароль верны, иначе должен ответить `false`. Пример кода на языке PHP, который может выступать в качестве сервиса аутентификации (auth.php):

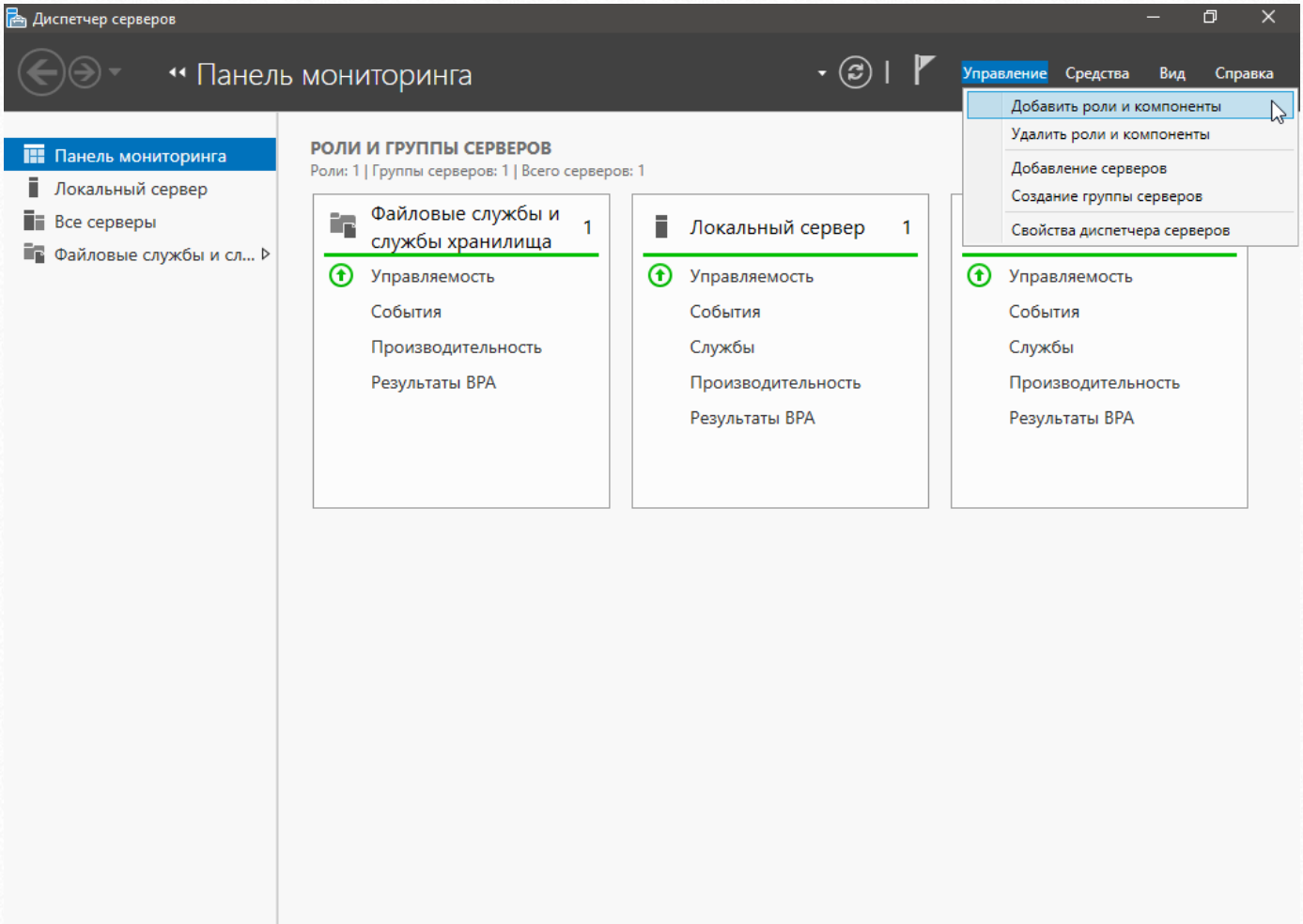
```
<?php

 if(!isset($_POST['login']) || !isset($_POST['password']))
 {
     exit('error');
 }

 if($_POST['login'] == 'ОрловАВ' && $_POST['password'] == '12345')
 {
     echo 'true';
 }
 else
 {
     echo 'false';
 }

?>
```

В реальном коде нужно будет провести проверку соответствия пары логин/пароль с внешней базой данных и аналогичным образом вернуть результат `true/false`.

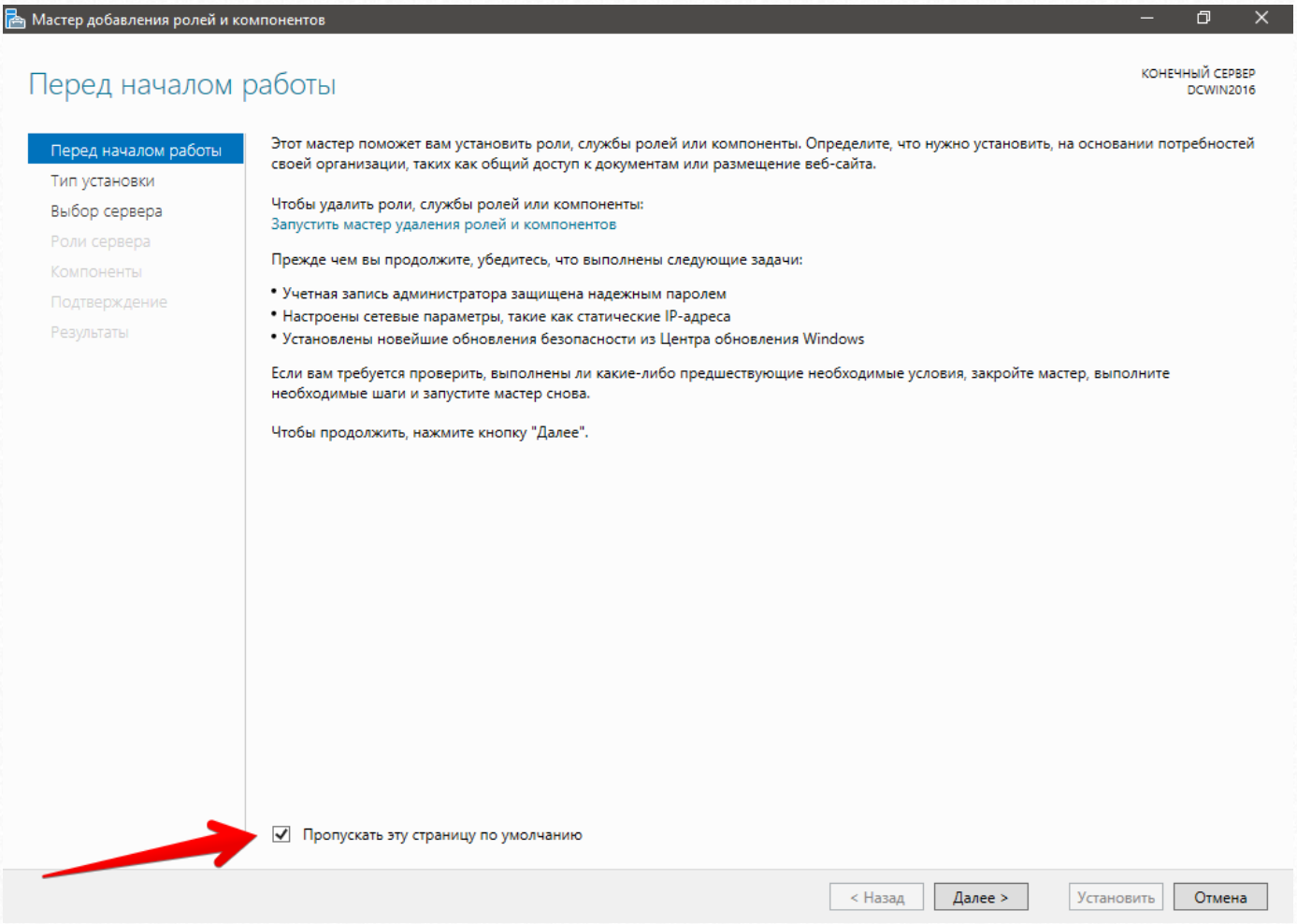
2. Настройка доменных служб Active Directory для синхронизации пользователей

2.1. Установка доменных служб Active Directory

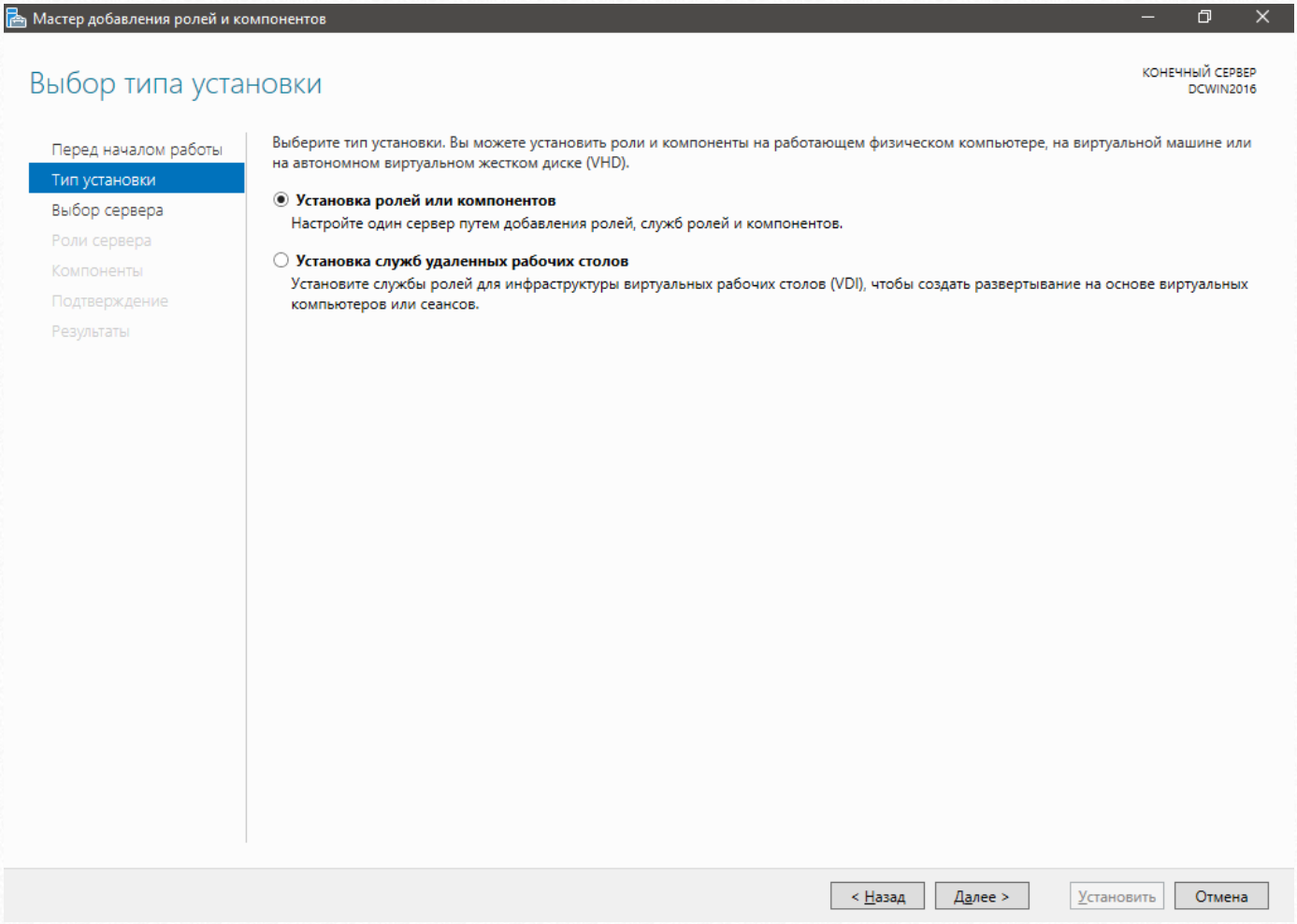
1. Открываем диспетчер серверов и в меню выбираем пункты «Управление» → «Добавить роли и компоненты».



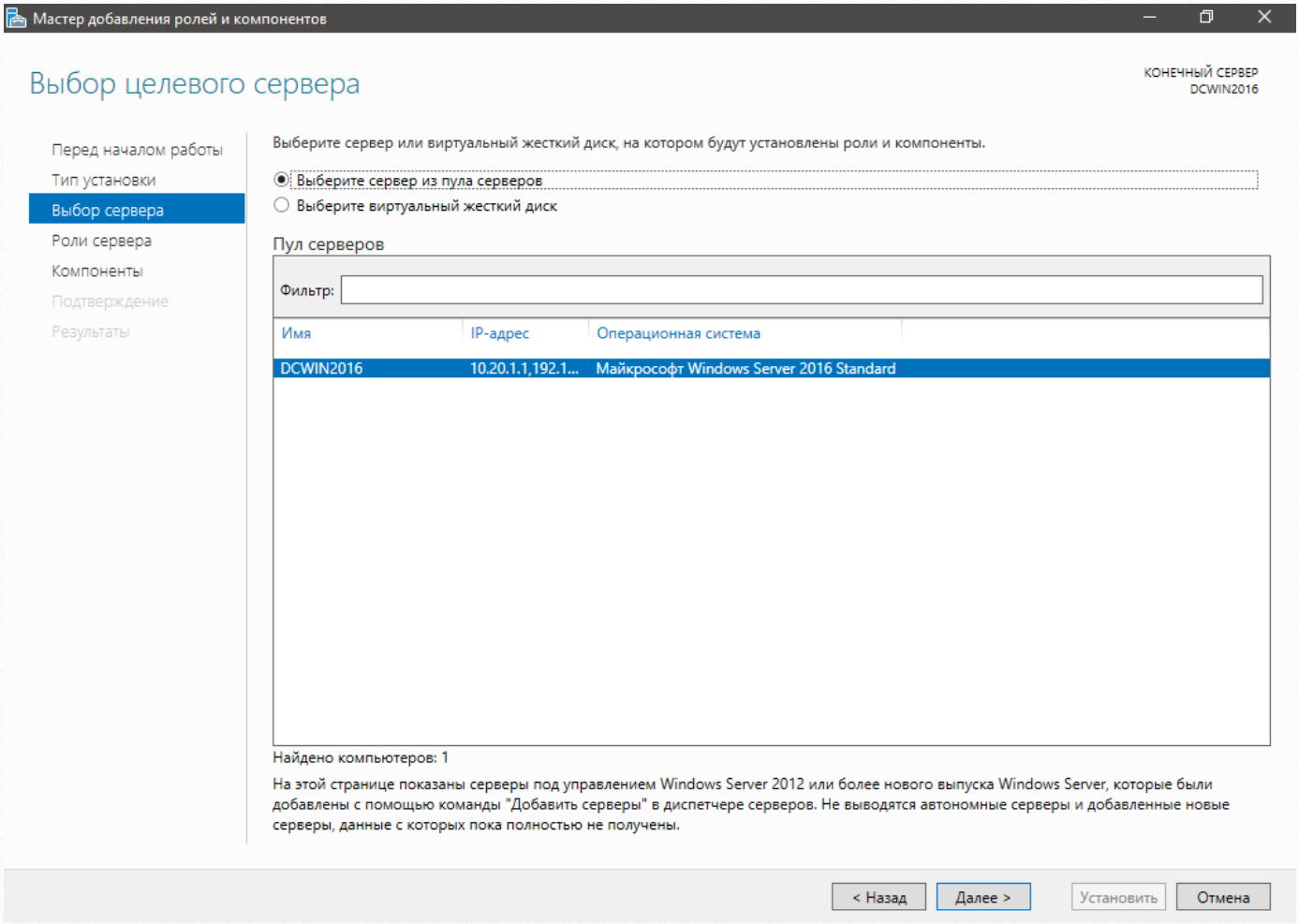
2. Откроется окно «Мастер добавления ролей и компонентов». Если мастер открывается впервые, то будет открыта вкладка «Перед началом работы». Если отметить пункт «Пропускать эту страницу по умолчанию», то данная вкладка далее появляться не будет. Нажимаем кнопку «Далее» для продолжения процесса добавления роли.



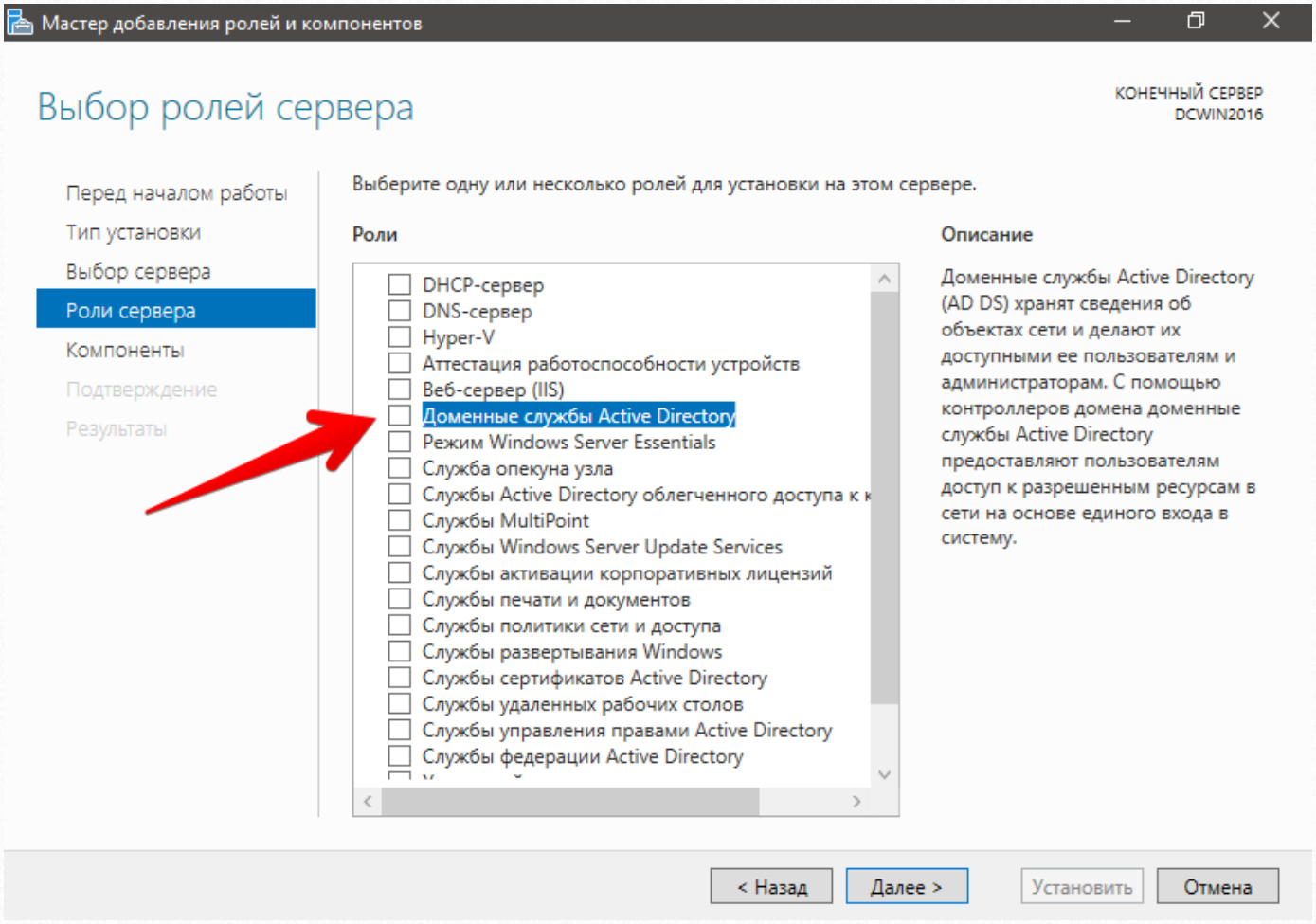
3. На вкладке «Тип установки» выбираем пункт «Установка ролей или компонентов» и нажимаем кнопку «Далее».



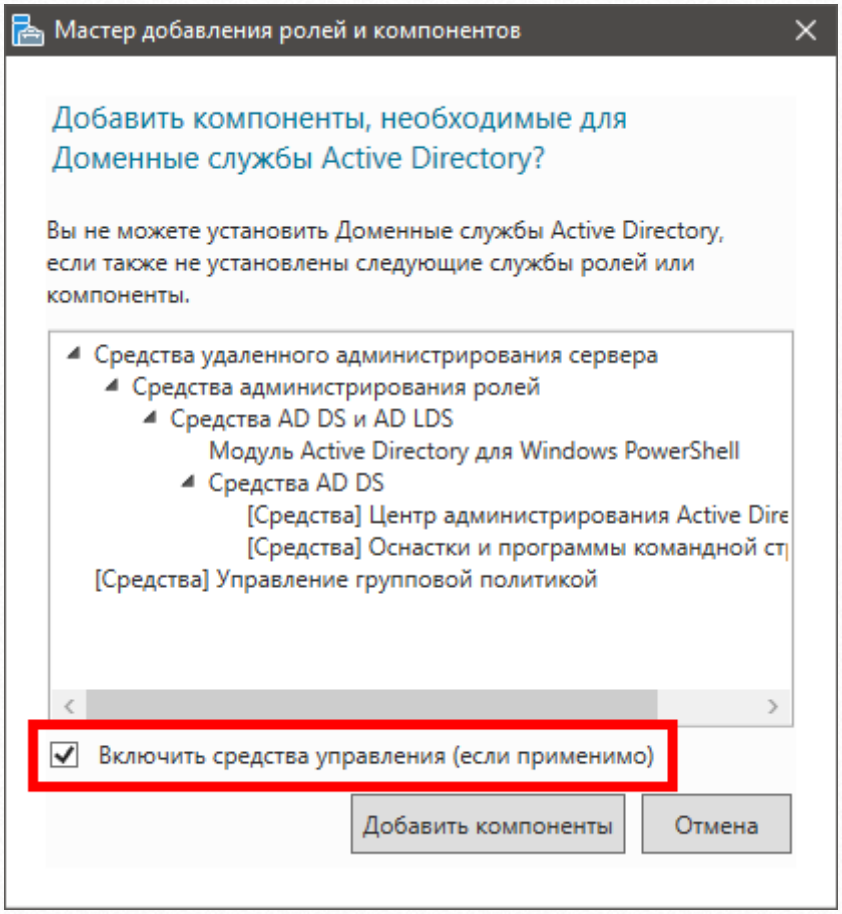
4. На вкладке «Выбор сервера» убедитесь, что выбран вариант «Выберите сервер из пула серверов» и в списке «Пул серверов» выбран тот сервер, которому необходимо установить роль контроллера домена.



5. На вкладке «Роли сервера» устанавливаем галочку в пункте «Доменные службы Active Directory».

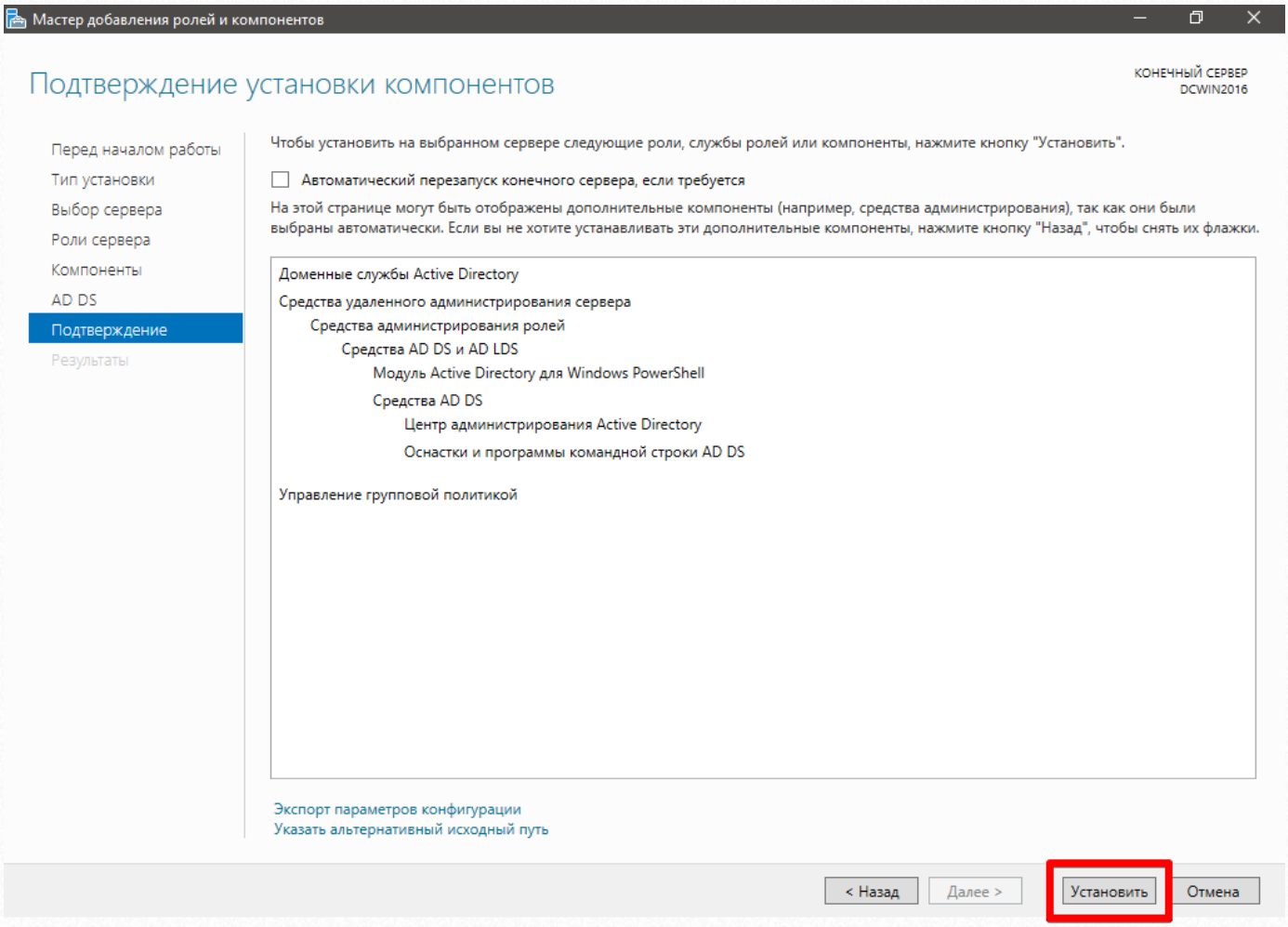


6. После установки флажка появится окно, информирующее о том, что для установки выбранной роли необходимо добавить несколько компонентов. Убедитесь, что галочка «Включить средства управления (если применимо)» установлена и нажмите кнопку «Добавить компоненты». Окно «Мастер добавления ролей и компонентов» закроется. Нажмите кнопку «Далее».

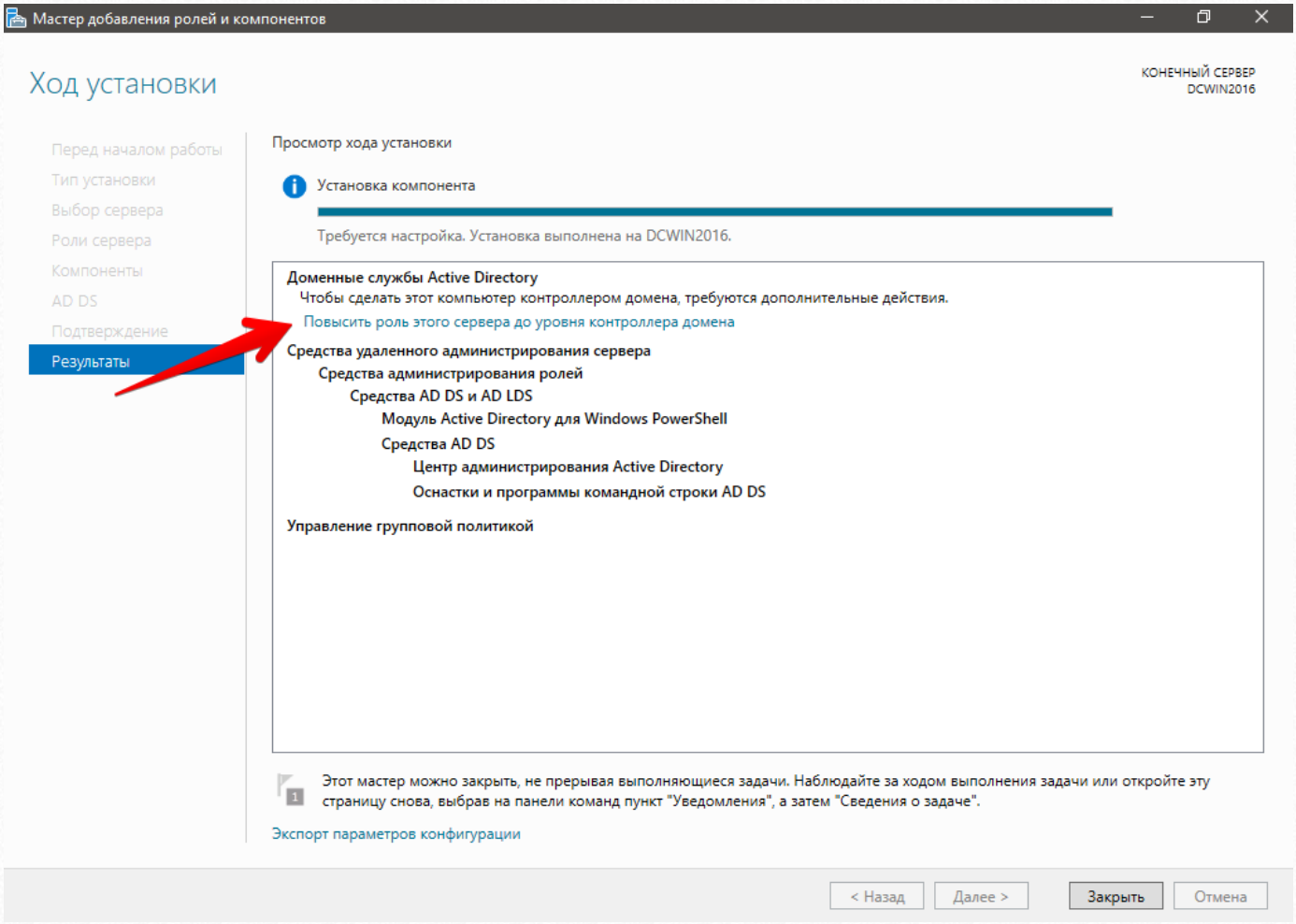


7. На вкладке «Компоненты» просто нажимаем кнопку «Далее».
8. На вкладке «AD DS» также нажимаем на кнопку «Далее».

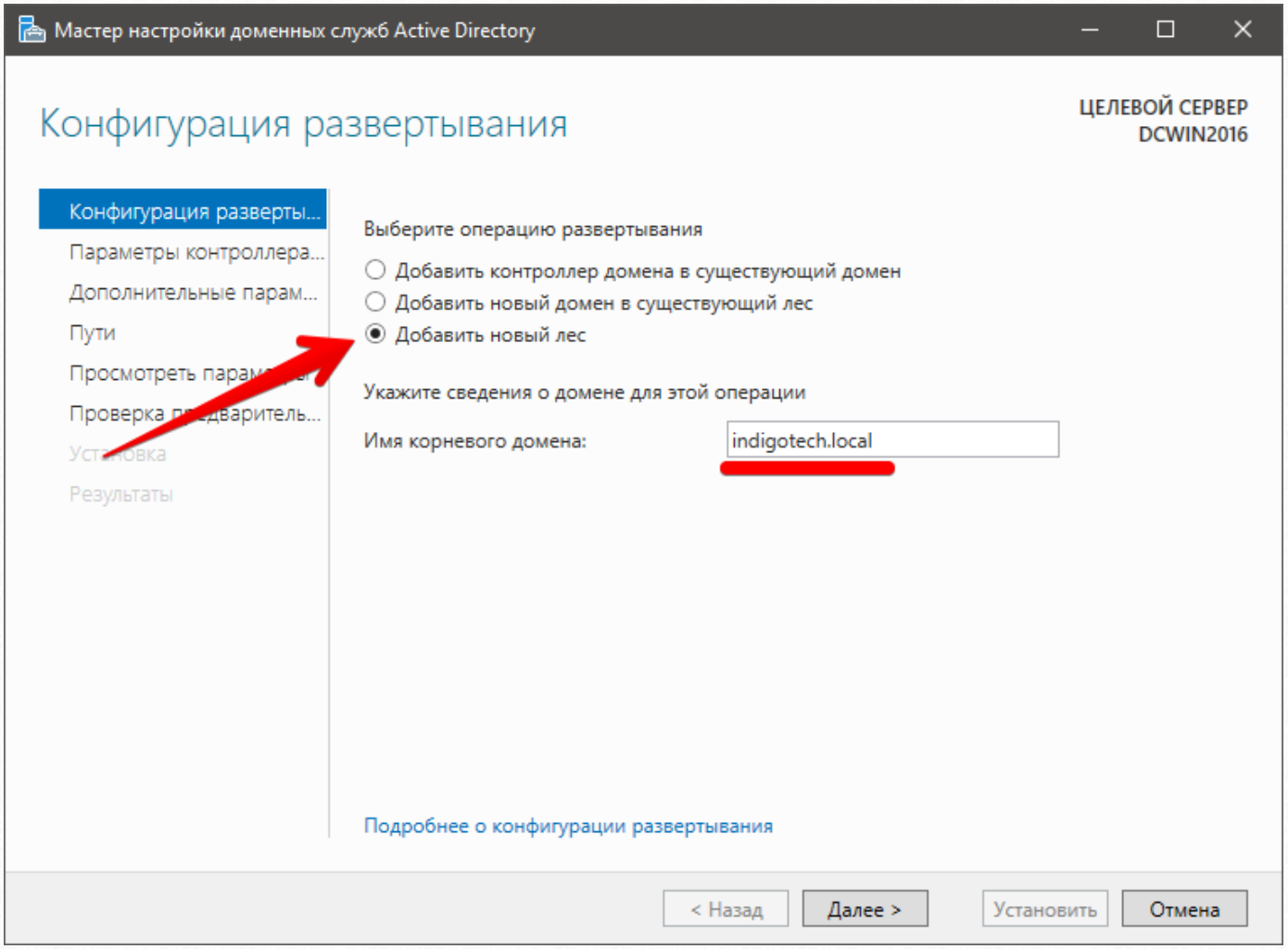
9. На вкладке «Подтверждение» жмем кнопку «Установить».



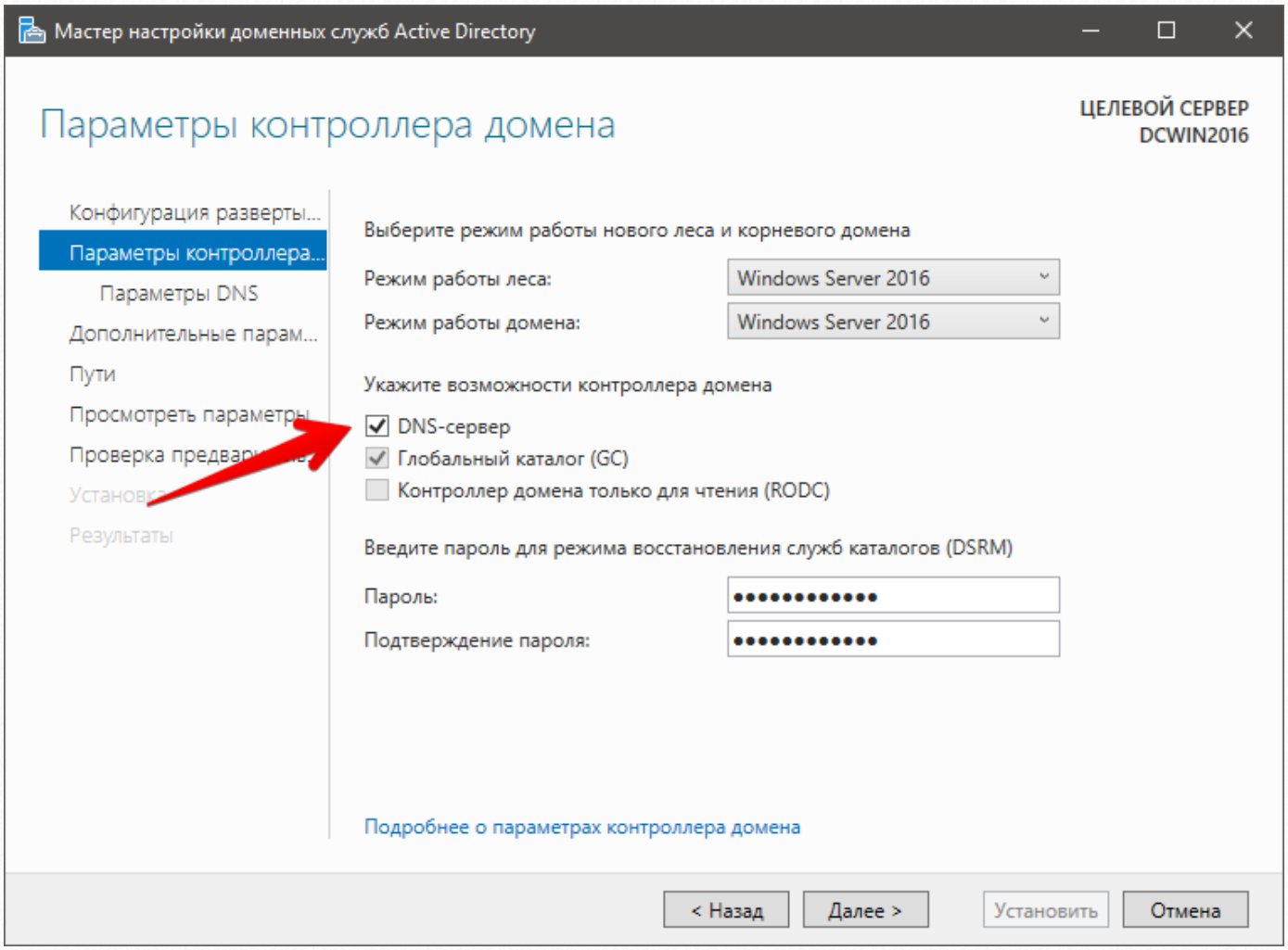
10. Когда установка будет выполнена нажмите на ссылку «Повысить роль этого сервера до уровня контроллера домена».



11. Откроется «Мастер настройки доменных служб Active Directory». На первой вкладке «Конфигурация развертывания» выбираем «Добавить новый лес» и указываем желаемое имя домена (в примере indigotech.local). Нажимаем на кнопку «Далее».

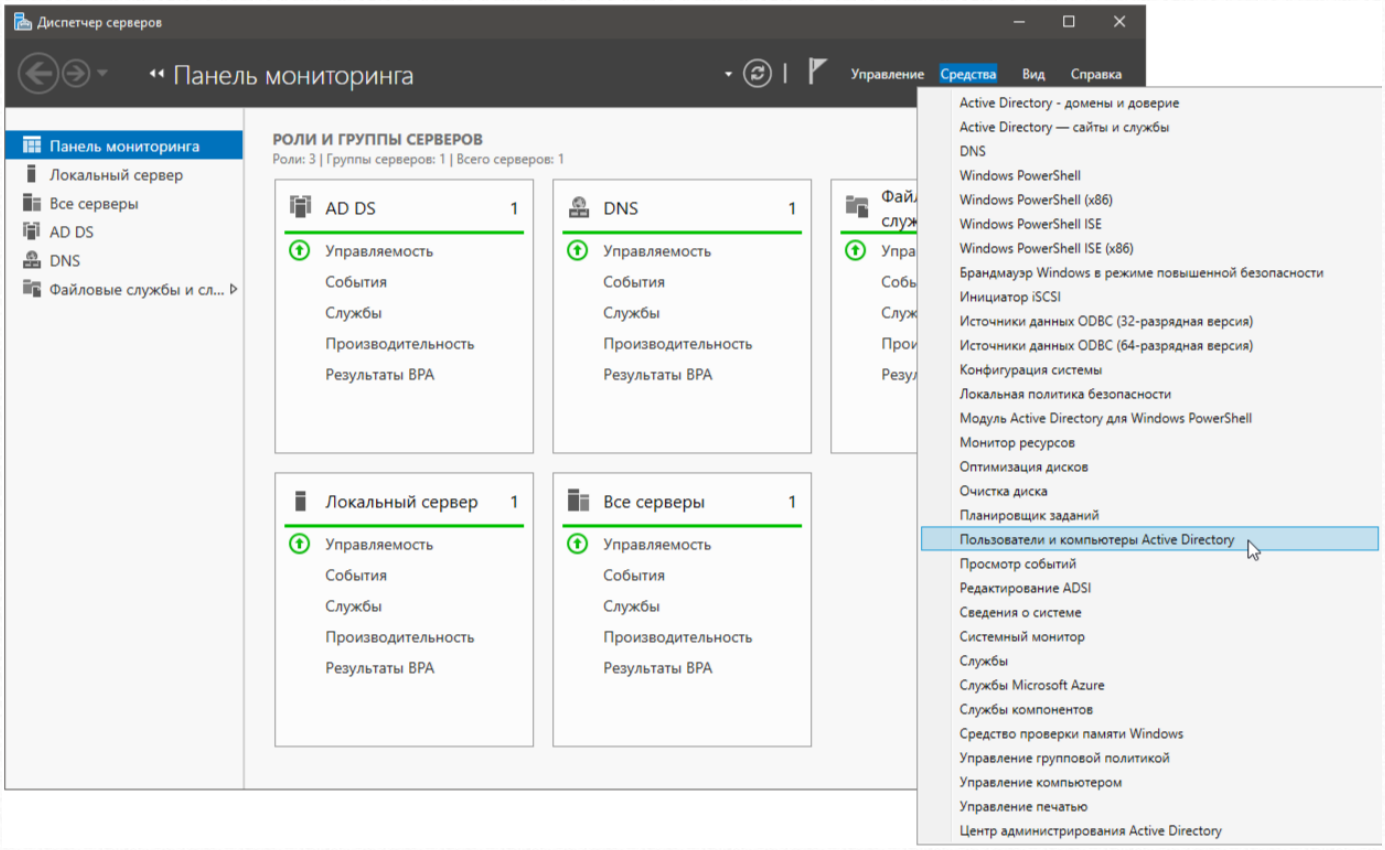


12. На вкладке «Параметры контроллера домена» проверяем, что галочка «DNS-сервер» установлена. Также вводим пароль для режима восстановления служб каталогов (DSRM). Он должен соответствовать установленным политикам безопасности. Нажимаем кнопку «Далее».

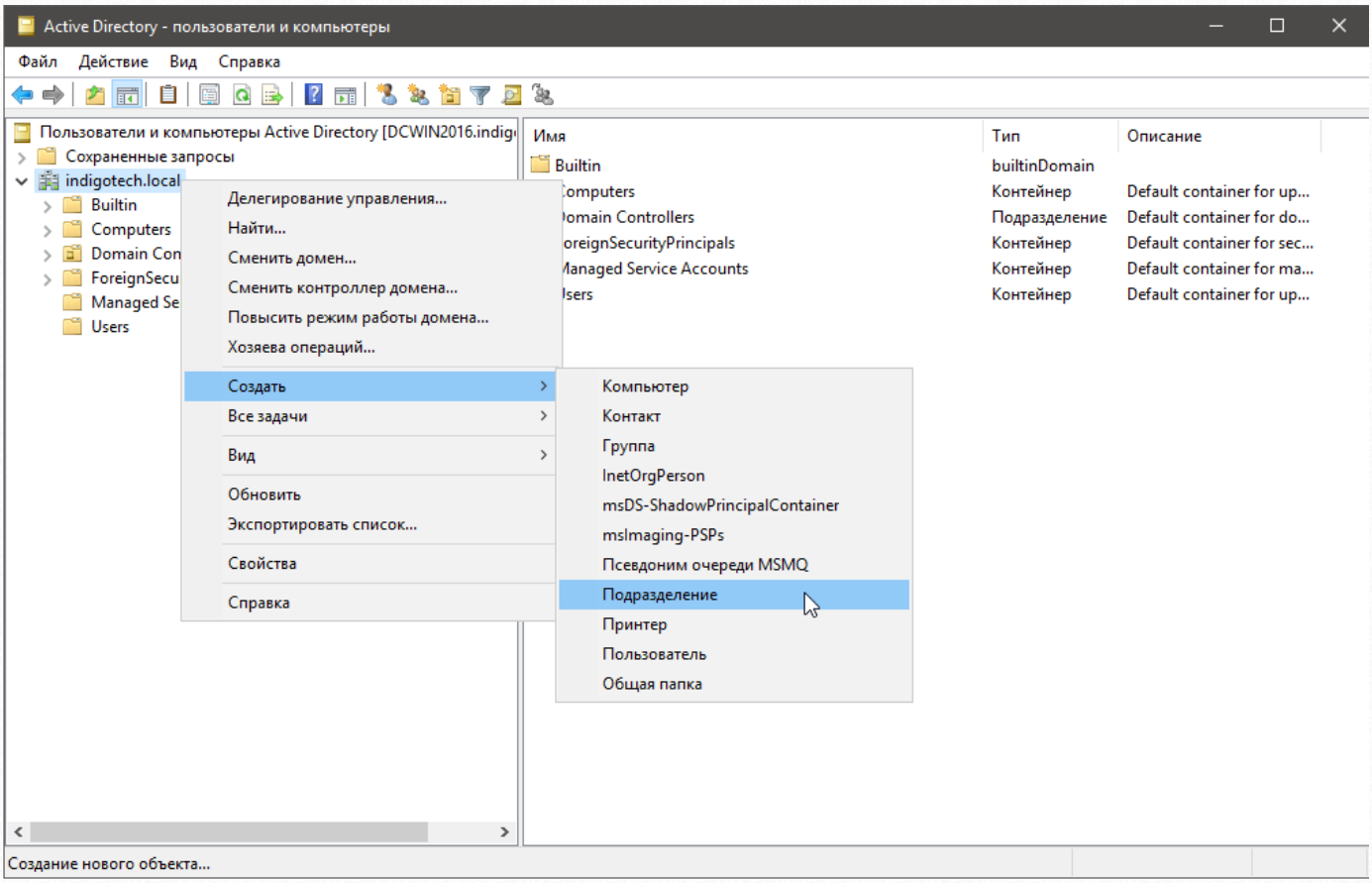


13. На вкладке «Параметры DNS» жмем «Далее», т.к. создаваемый DNS сервер единственный в нашей сети.
14. На вкладке «Дополнительные параметры» также жмем «Далее».
15. На вкладке «Пути» также жмем «Далее».
16. На вкладке «Просмотреть параметры» также жмем «Далее».
17. На вкладке «Проверка предварительных требований» нажимаем кнопку «Установить».
18. После установки будет произведена автоматическая перезагрузка сервера.

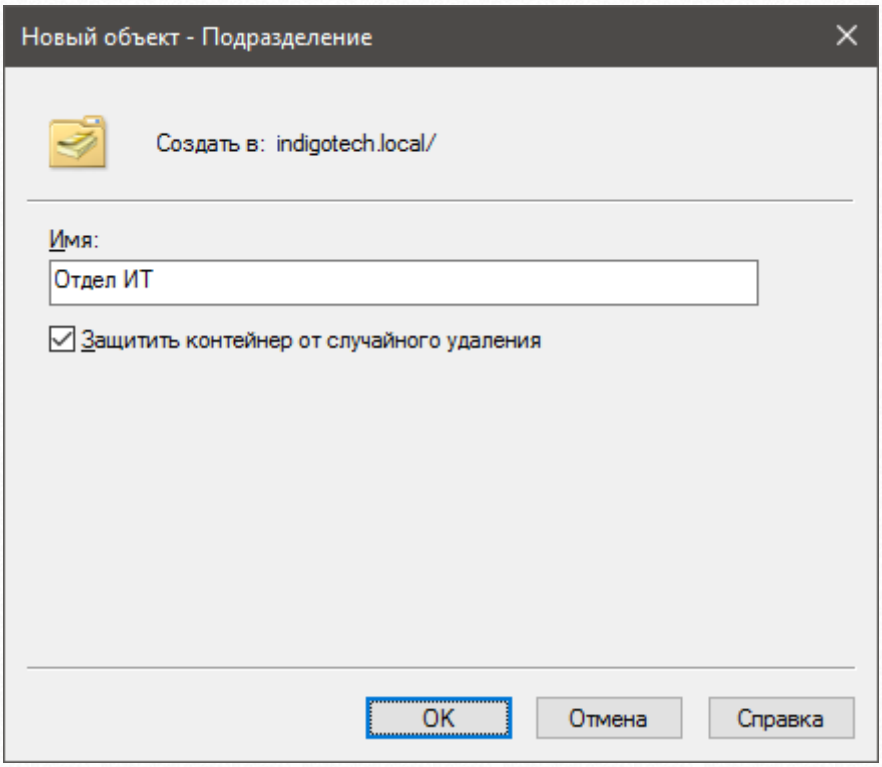
19. После перезагрузки в окне «Диспетчер серверов» в меню выбираем пункты «Средства» → «Пользователи и компьютеры Active Directory».



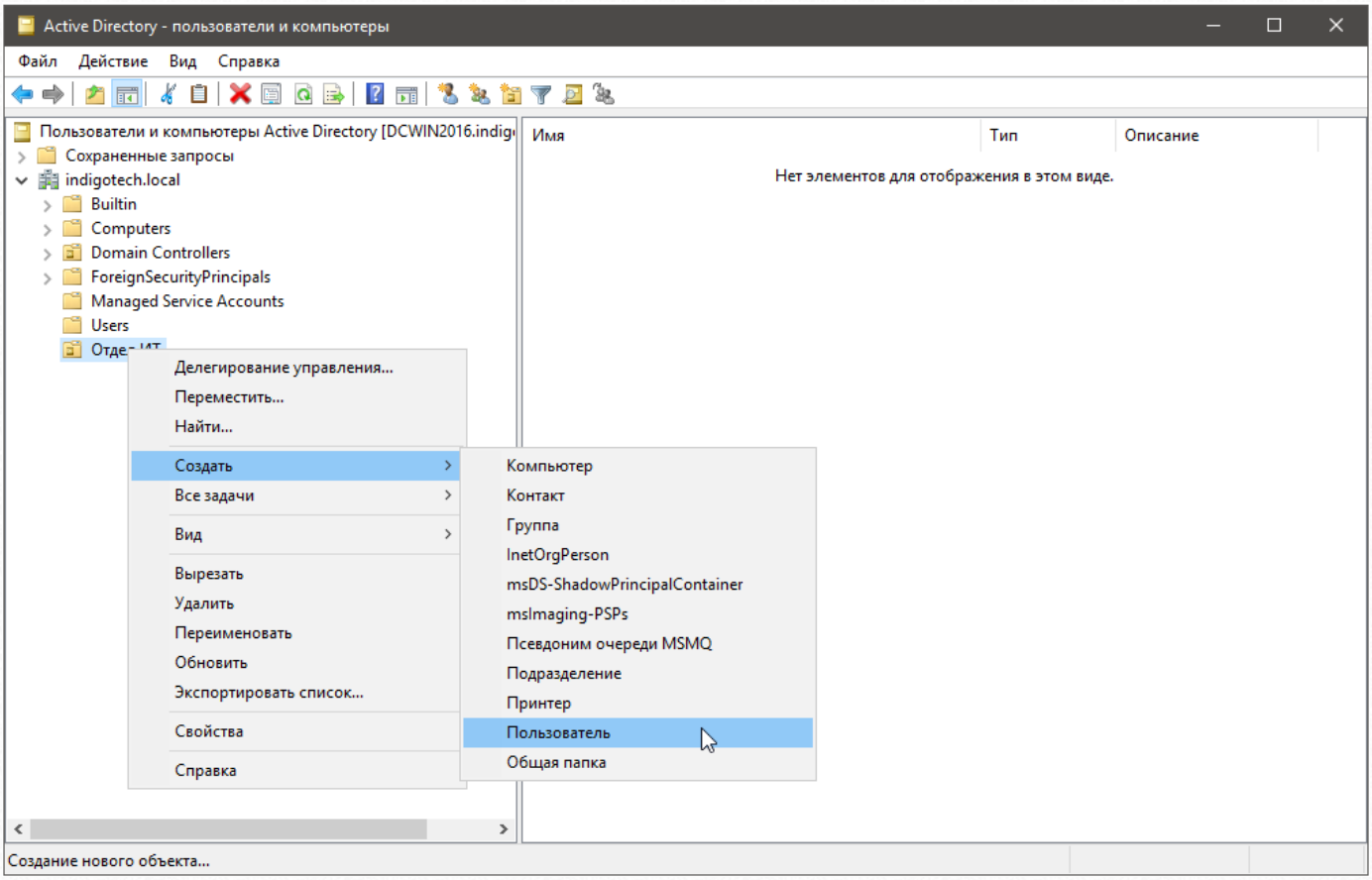
20. В открывшемся окне «Active Directory – пользователи и компьютеры» в списке слева выделите созданный домен и нажмите по нему правой кнопкой мыши. В открывшемся меню выберите пункт «Создать» → «Подразделение».



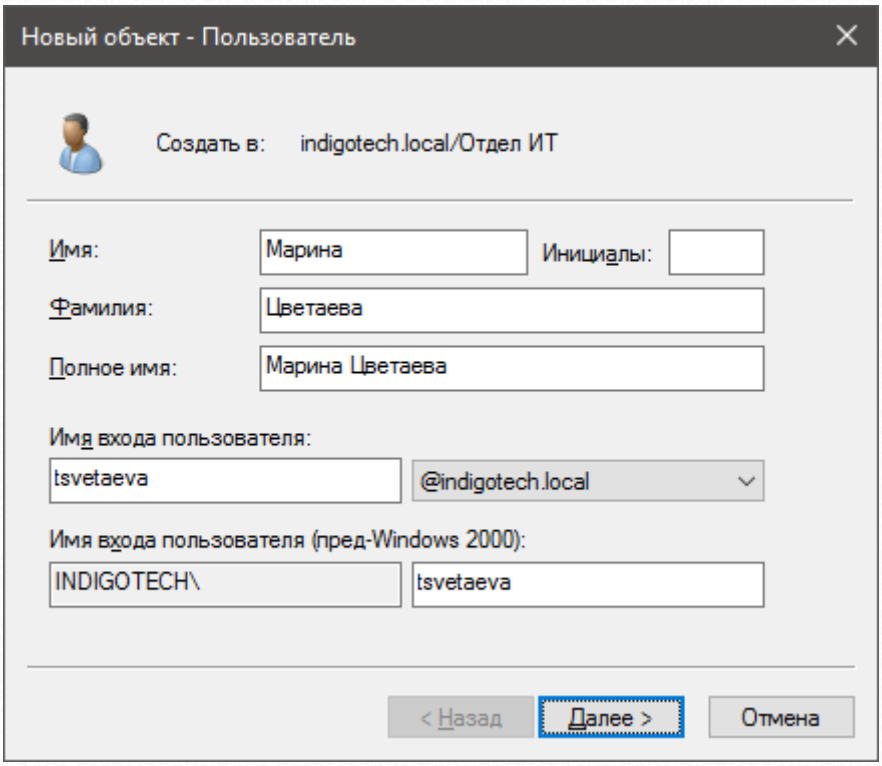
21. В появившемся окне «Новый объект - Подразделение» в поле «Имя» введите название подразделения организации. Если флаг «Защитить контейнер от случайного удаления» будет установлен, то для удаления данного подразделения будет необходимо зайти в его свойства и снять этот флаг. Это позволяет избежать случайного удаления. В процессе синхронизации пользователей с системой тестирования INDIGO подразделения являются группами, с помощью которых строится иерархический список пользователей. После ввода наименования подразделения и нажмите кнопку «ОК».



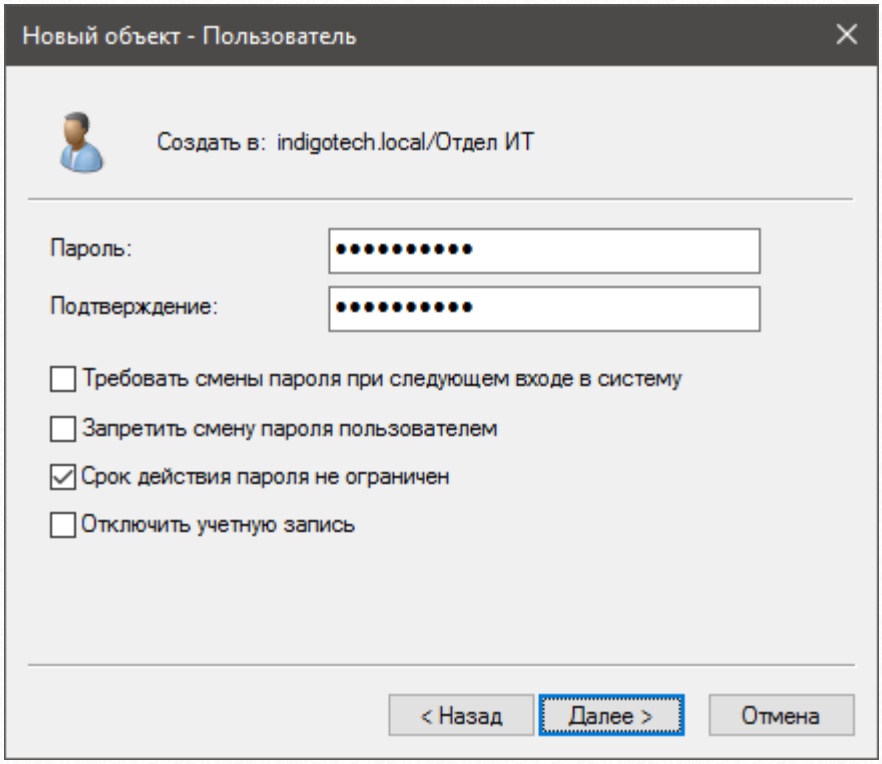
22. Для того чтобы добавить пользователя в подразделение выделите его в списке слева и нажмите по нему правой кнопкой мыши. В появившемся меню выберите пункт «Создать» → «Пользователь».



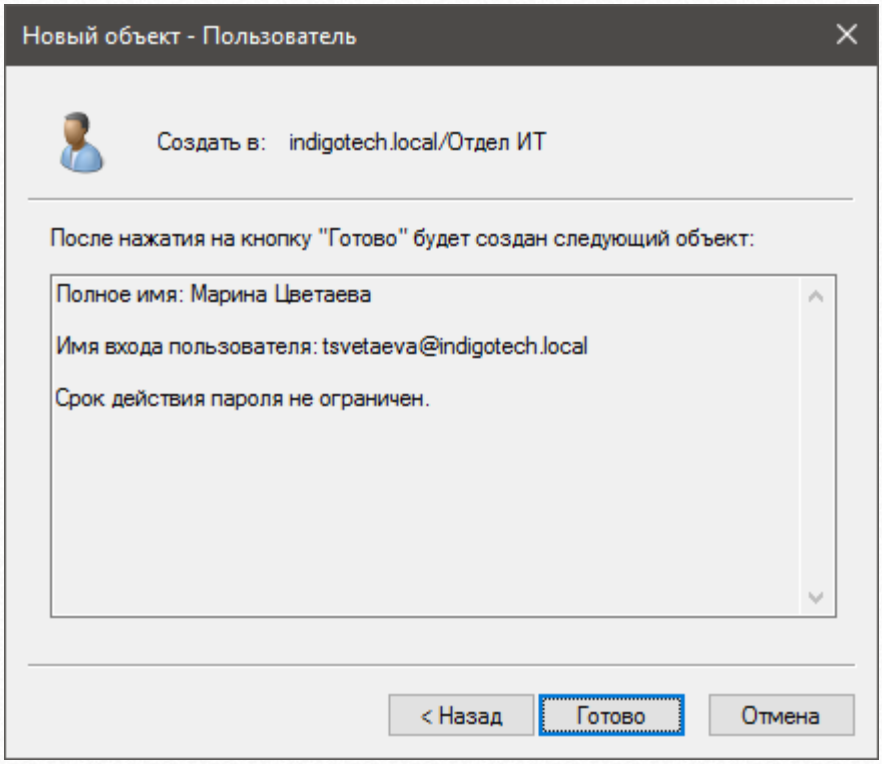
23. Заполните поля в появившемся окне «Новый объект - Пользователь» и нажмите кнопку «Далее».



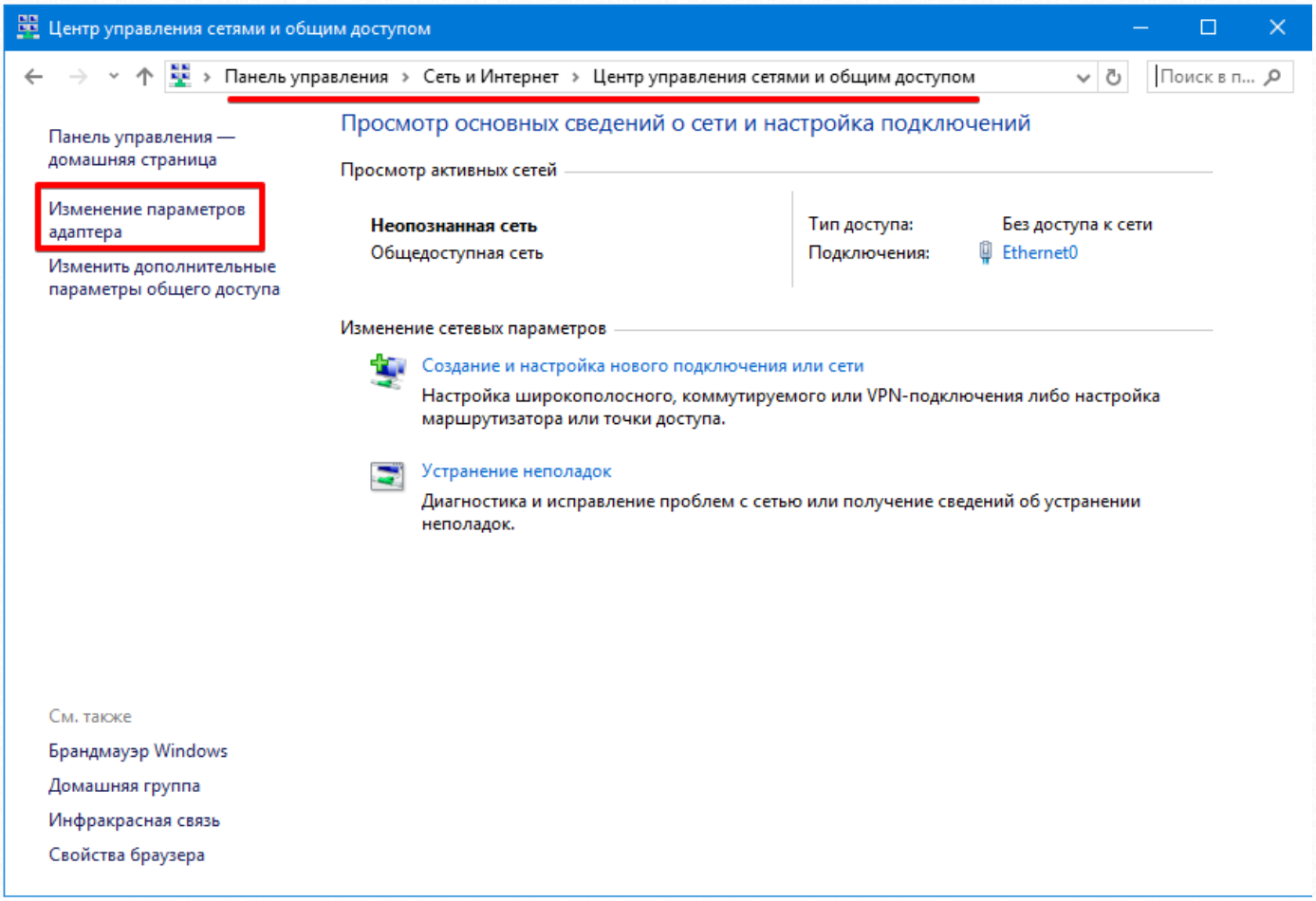
24. На следующем шаге в поля «Пароль» и «Подтверждение» введите пароль для создаваемого пользователя. Также дополнительно можете установить необходимые настройки с помощью флагов под полями, затем нажмите кнопку «Далее».



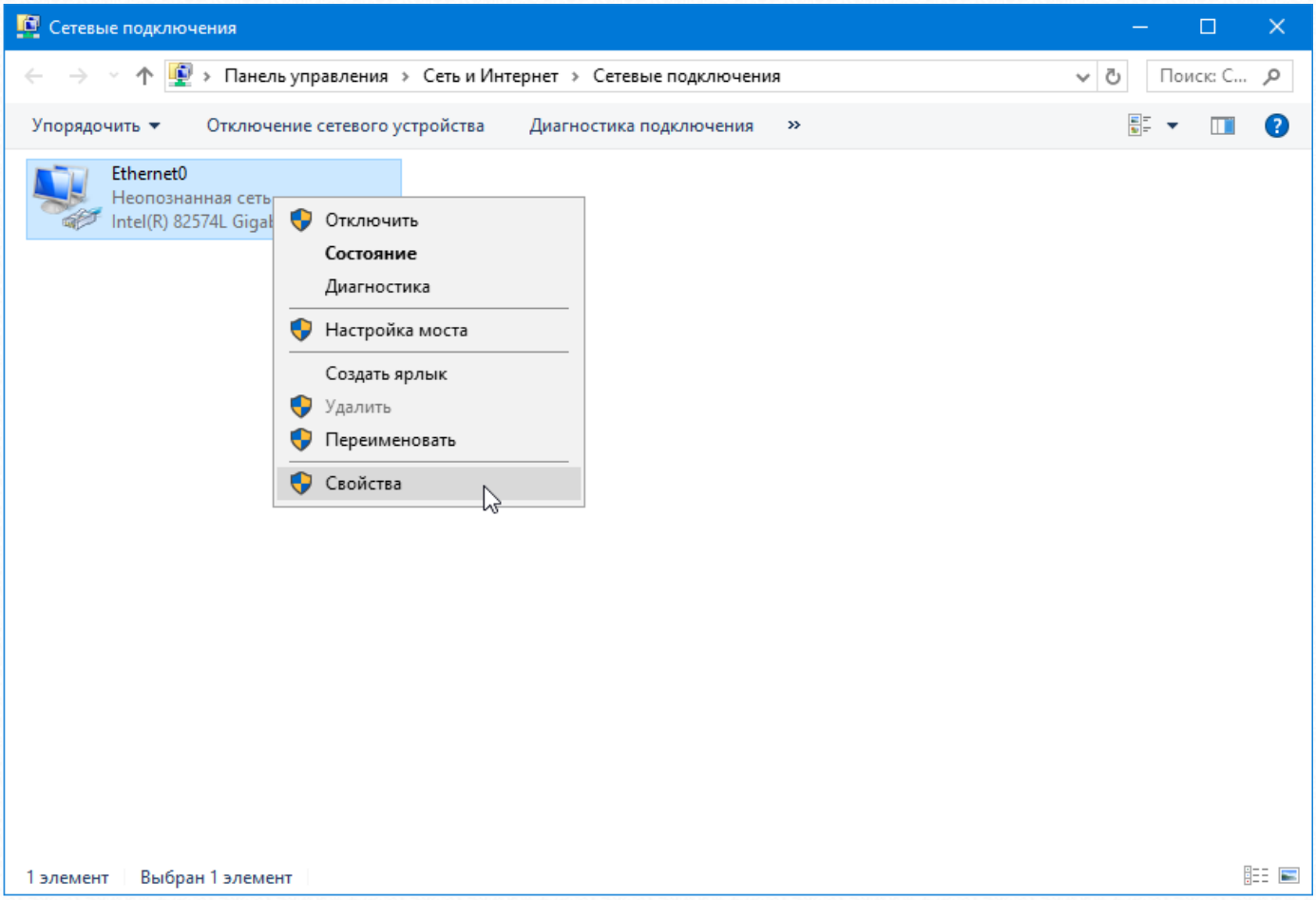
25. На следующем шаге нажмите кнопку «Готово».



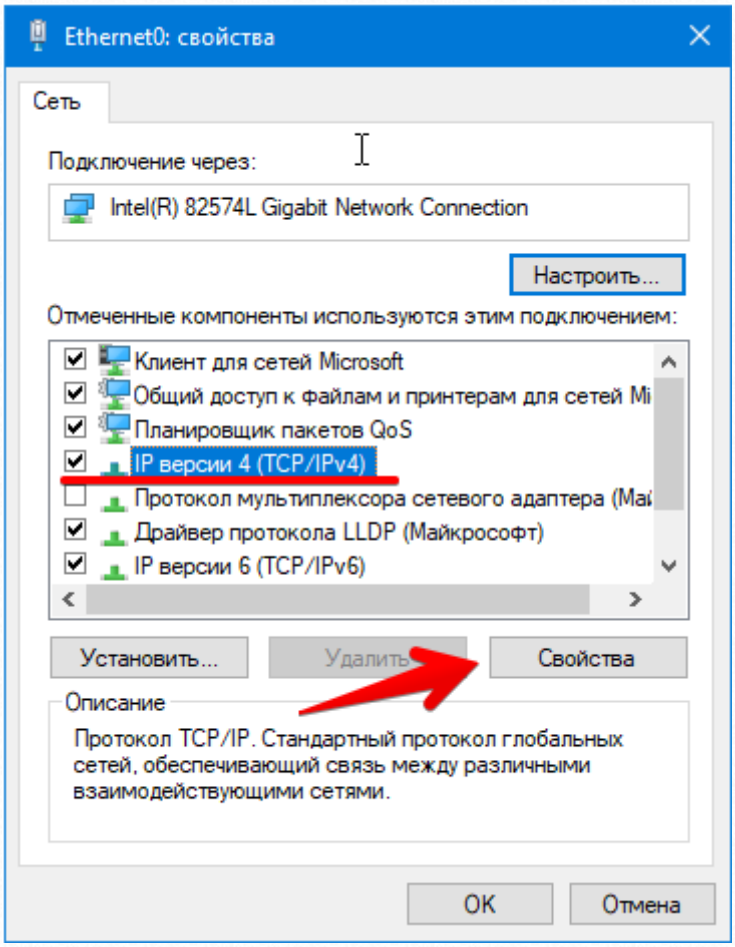
26. После создания пользователей введем в домен рабочую станцию на которую будем устанавливать систему тестирования. Для начала убедимся, что в настройках сети качестве DNS сервера указан наш контроллер домена. Для этого откройте панели управления и выберите пункты «Сеть и Интернет» → «Центр управления сетями и общим доступом». В открывшемся окне «Центр управления сетями и общим доступом» нажмите на ссылку «Изменение параметров адаптера».



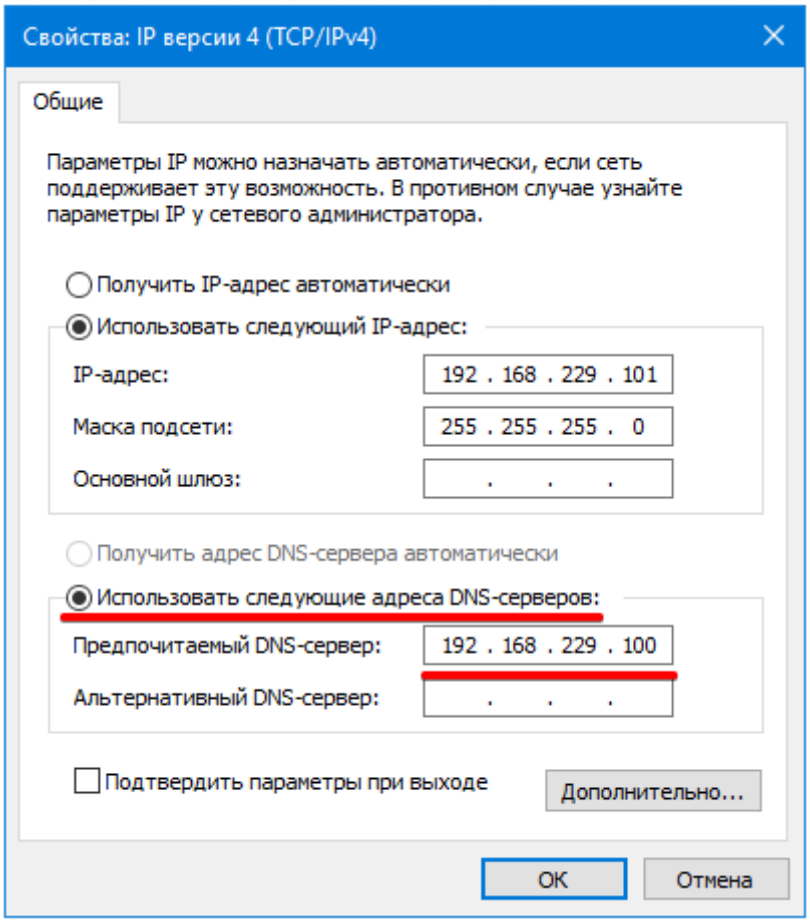
27. В Открывшемся окне нажмите правой кнопкой на сетевом устройстве и в выпадающем меню выберите пункт «Свойства».



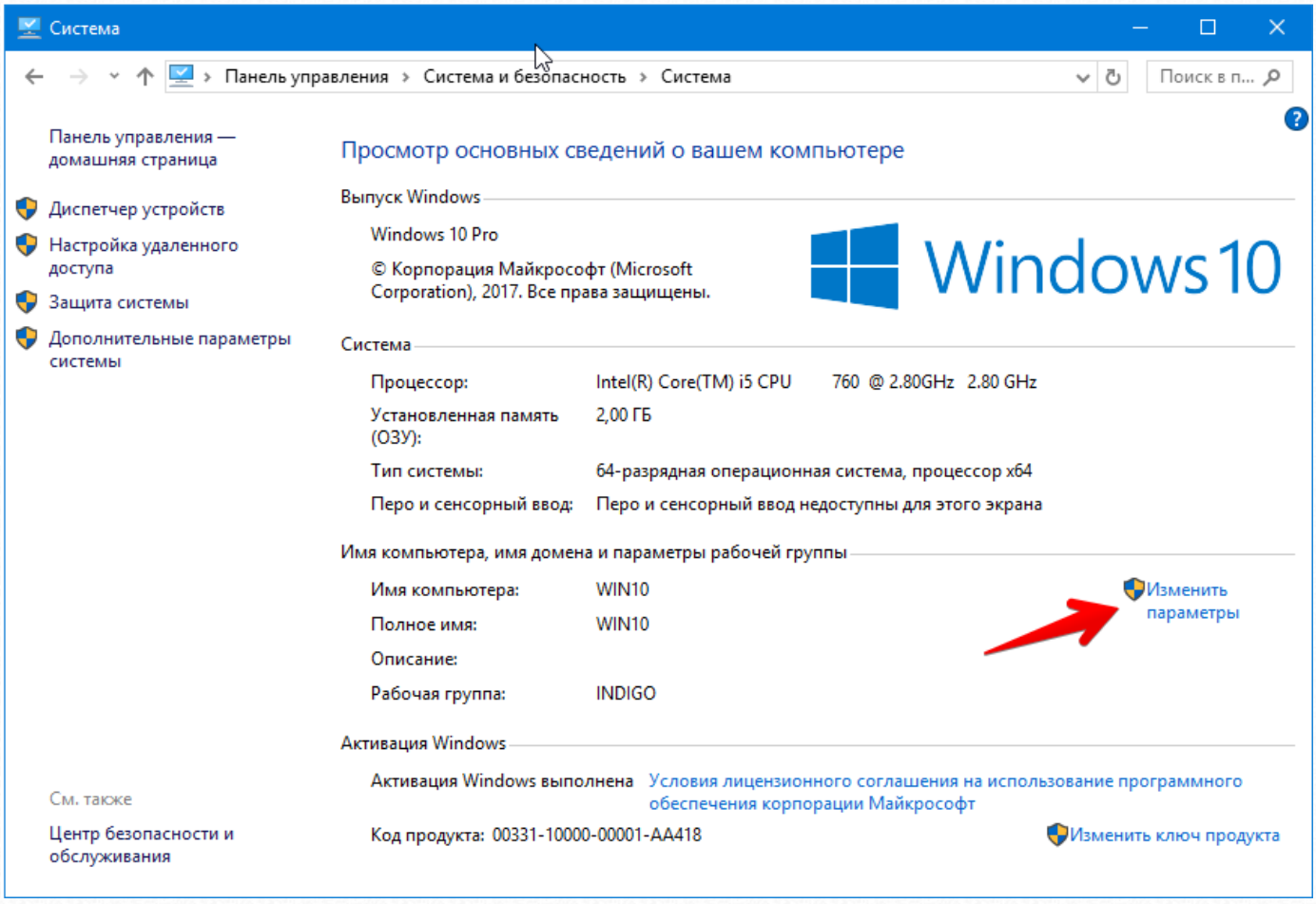
28. В открывшемся окне «Свойства» в списке компонентов выберите «IP версии 4(TCP/IPv4)» и нажмите кнопку «Свойства».



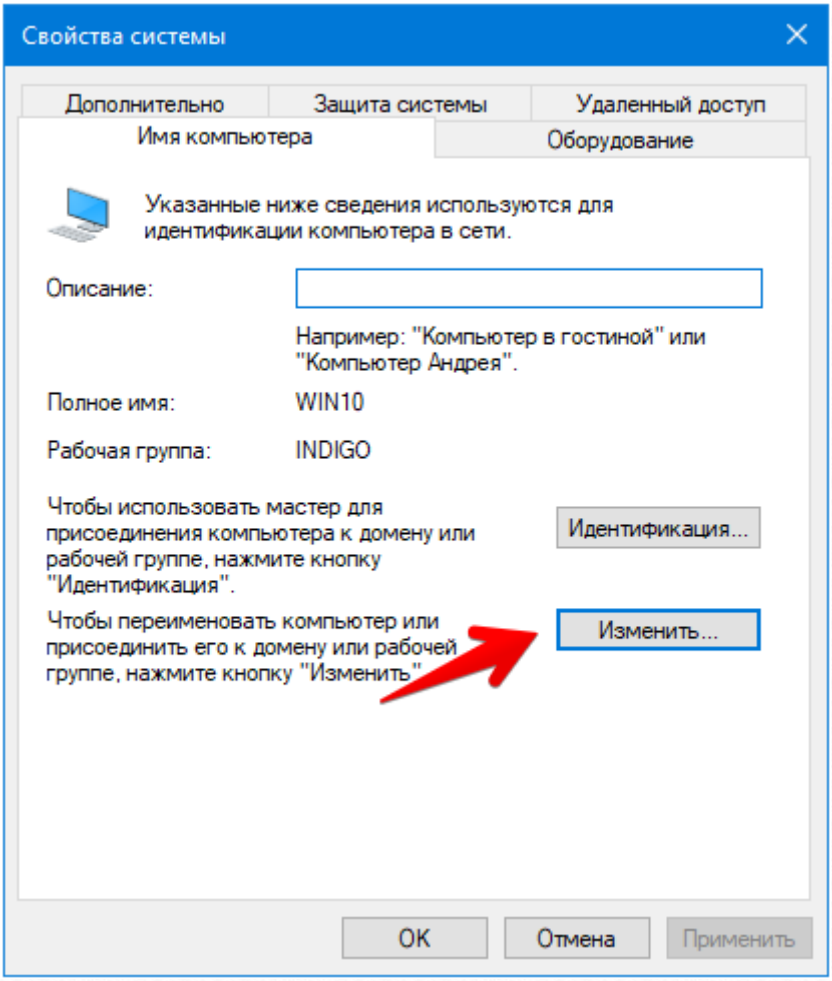
29. В открывшемся окне «Свойства: IP версии 4 (TCP/IPv4)» установите переключатель в положение «Использовать следующие адреса DNS-серверов» и в поле «Предпочитаемый DNS-сервер» введите IP-адрес контроллера домена, в нашем случае 192.168.229.100. После этого нажмите кнопку «ОК» и в окне свойств сетевого устройства также нажмите «ОК».



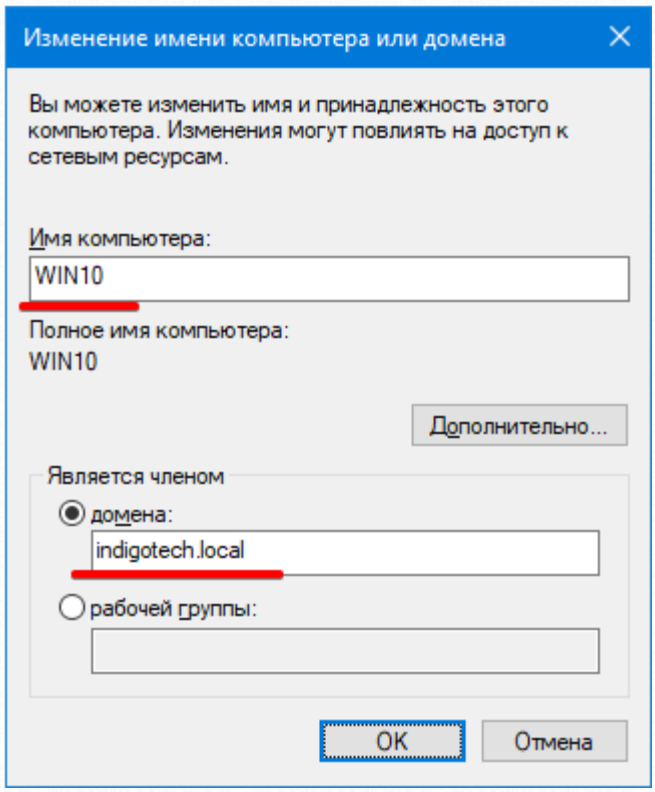
30. После настройки сети можно ввести компьютер в созданный домен. Для этого откройте «Панель управления» и выберите пункты «Система и безопасность» → «Система». В открывшемся окне «Система» кликните по ссылке «Изменить параметры».



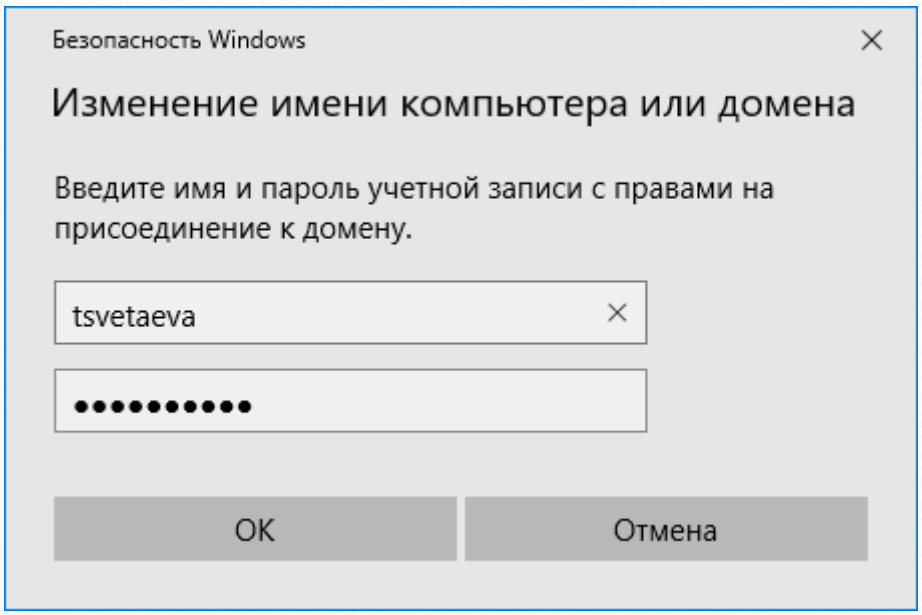
31. В открывшемся окне «Свойства системы» на вкладке «Имя компьютера» нажмите кнопку «Изменить...»



32. В открывшемся окне «Изменение имени компьютера или домена» установите выбор на пункт «Является членом домена» и впишите имя созданного домена «indigotech.local». Также можно задать имя компьютера, в нашем случае имя компьютера будет установлено «WIN10».



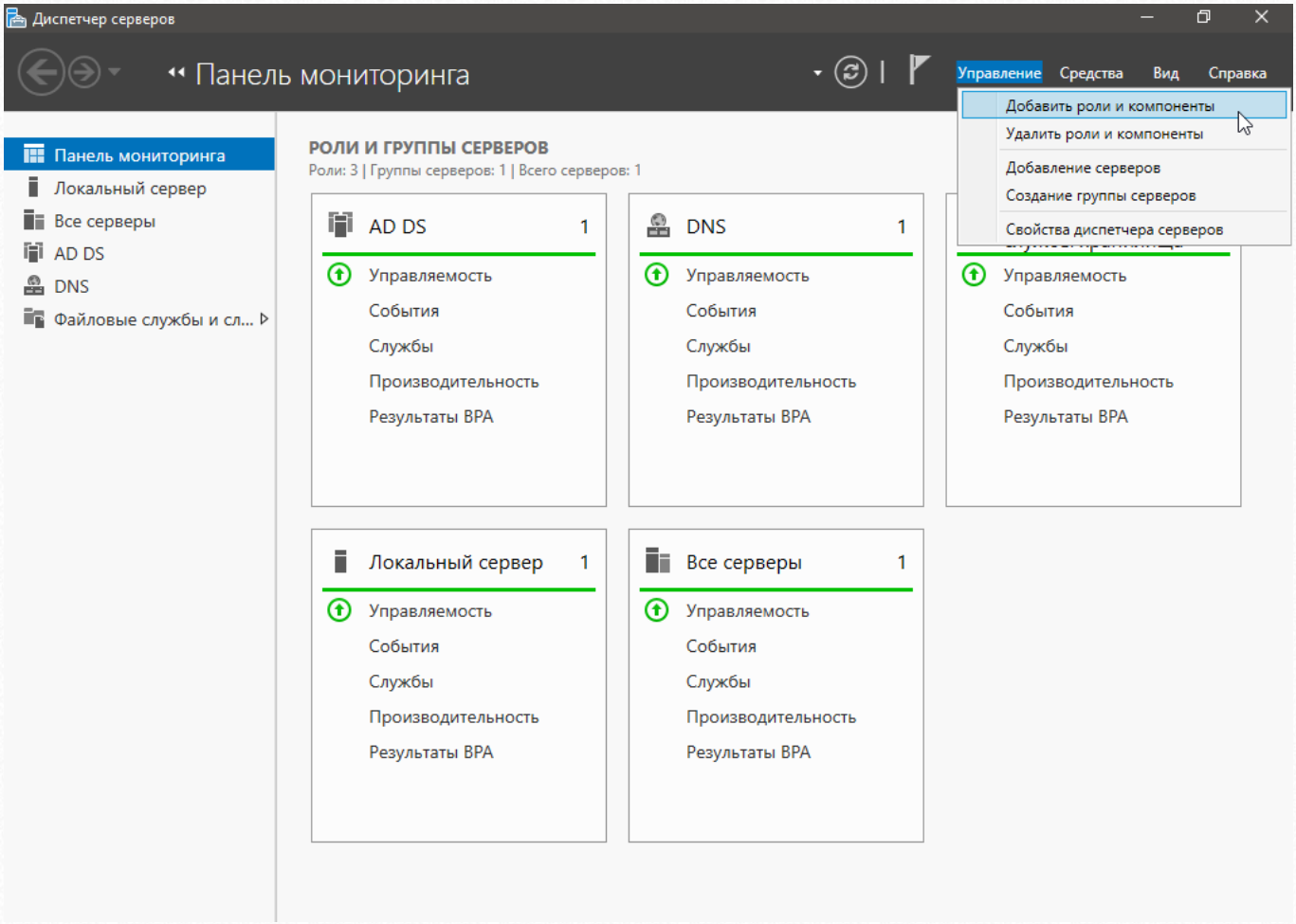
33. По окончании нажмите кнопку «ОК», после чего вам необходимо ввести имя пользователя и пароль пользователя, который ранее был создан в домене. После этого необходимо перезагрузить компьютер и на этом настройка окончена.



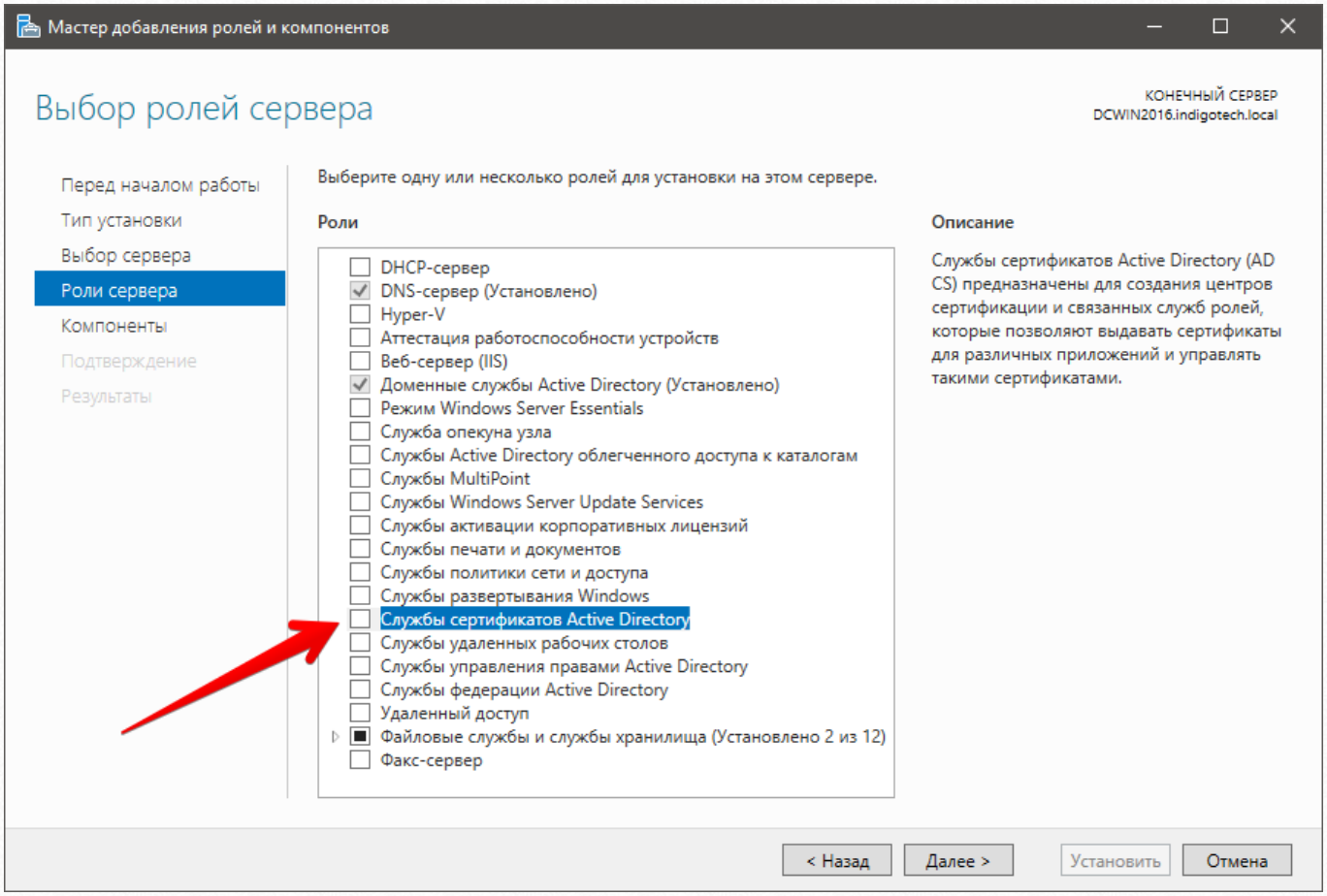
2.2. Настройка бесшовной авторизации пользователей на базе служб федерации Active Directory

2.2.1. Установка Центра Сертификации Active Directory

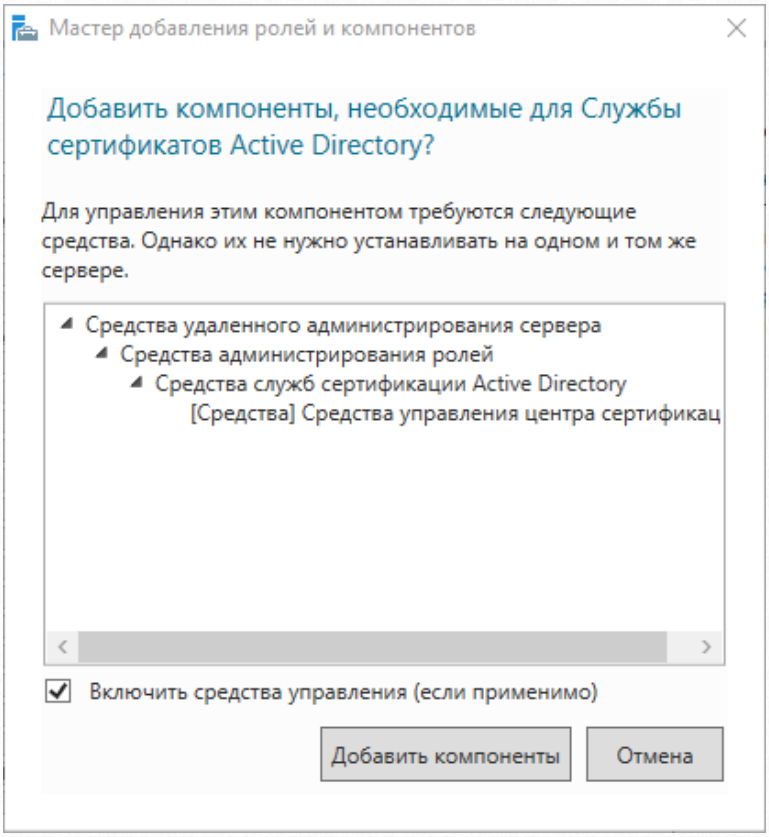
1. Предполагается, что синхронизация пользователей системы тестирования с AD уже корректно настроена. Чтобы настроить бесшовную авторизацию нужно одному из серверов в домене добавить роль службы федерации Active Directory (AD FS). Для работы AD FS необходим установленный центр сертификации AD. Для его установки нажмите «Управление» → «Добавить роли и компоненты» в окне «Диспетчер серверов».



2. На вкладке «Тип установки» выбираем «Установка ролей и компонентов». Жмем «Далее».
3. На вкладке «Выбор сервера» ставим выбор на «Выберите сервер из пула серверов» и убедитесь, что в списке «Пул серверов» выбран нужный сервер. Жмем «Далее».
4. На вкладке «Роли сервера» выбираем роль «Службы сертификатов Active Directory».

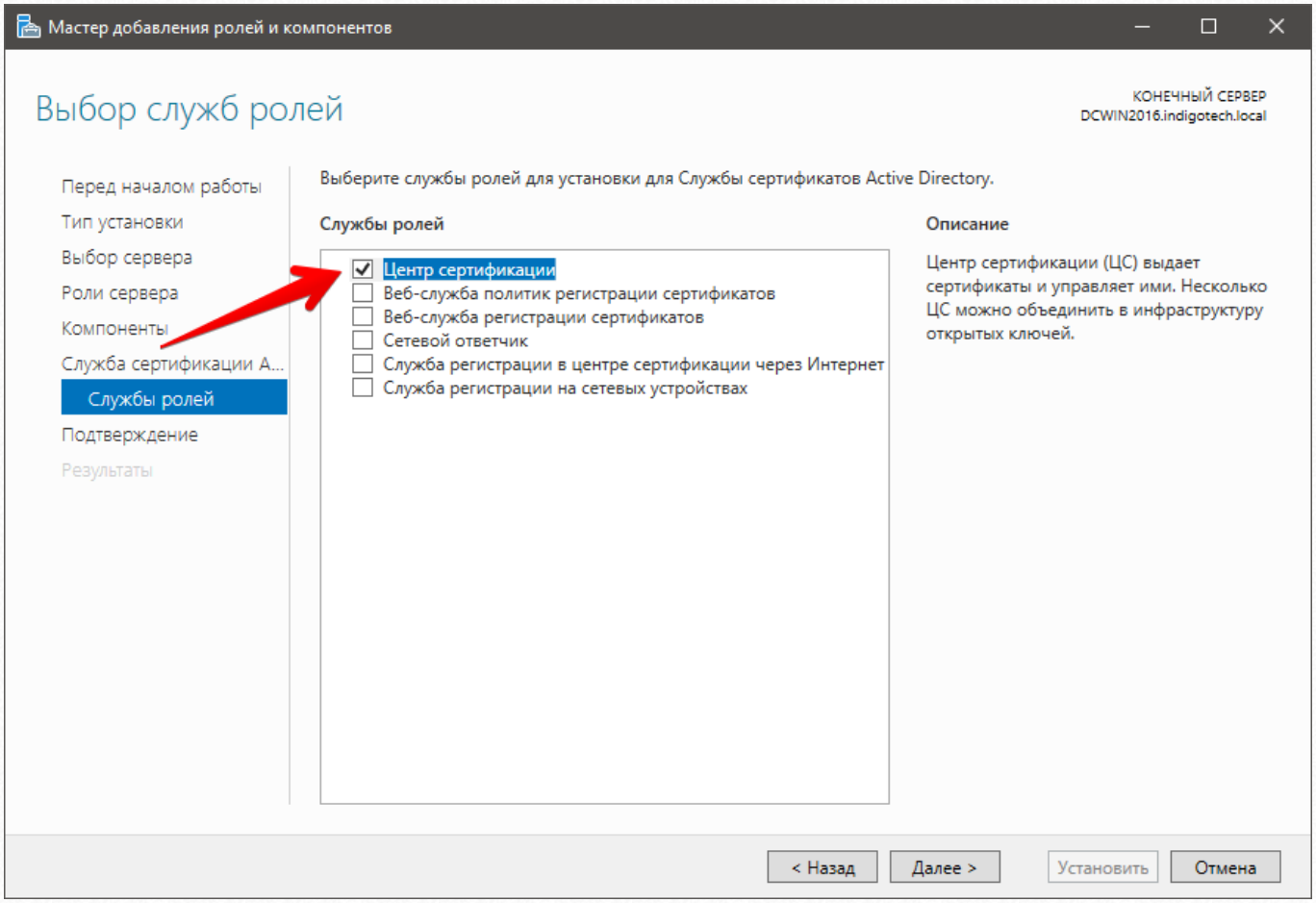

Мастер добавления ролей и компонентов
Выбор ролей сервера
КОНЕЧНЫЙ СЕРВЕР
DCWIN2016.indigotech.local
Перед началом работы
Тип установки
Выбор сервера
Роли сервера
Компоненты
Подтверждение
Результаты
Выберите одну или несколько ролей для установки на этом сервере.
Роли
DHCP-сервер
DNS-сервер (Установлено)
Hyper-V
Аттестация работоспособности устройств
Веб-сервер (IIS)
Доменные службы Active Directory (Установлено)
Режим Windows Server Essentials
Служба опекуна узла
Службы Active Directory облегченного доступа к каталогам
Службы MultiPoint
Службы Windows Server Update Services
Службы активации корпоративных лицензий
Службы печати и документов
Службы политики сети и доступа
Службы развертывания Windows
Службы сертификатов Active Directory
Службы удаленных рабочих столов
Службы управления правами Active Directory
Службы федерации Active Directory
Удаленный доступ
Файловые службы и службы хранилища (Установлено 2 из 12)
Факс-сервер
Описание
Службы сертификатов Active Directory (AD CS) предназначены для создания центров сертификации и связанных служб ролей, которые позволяют выдавать сертификаты для различных приложений и управлять такими сертификатами.
< Назад
Далее >
Установить
Отмена

5. Во всплывающем окне «Мастер добавления ролей и компонентов» убеждаемся, что включена галочка «Включить средства управления (если применимо)» и жмем кнопку «Добавить компоненты». И на вкладке «Роли сервера» жмем кнопку «Далее».

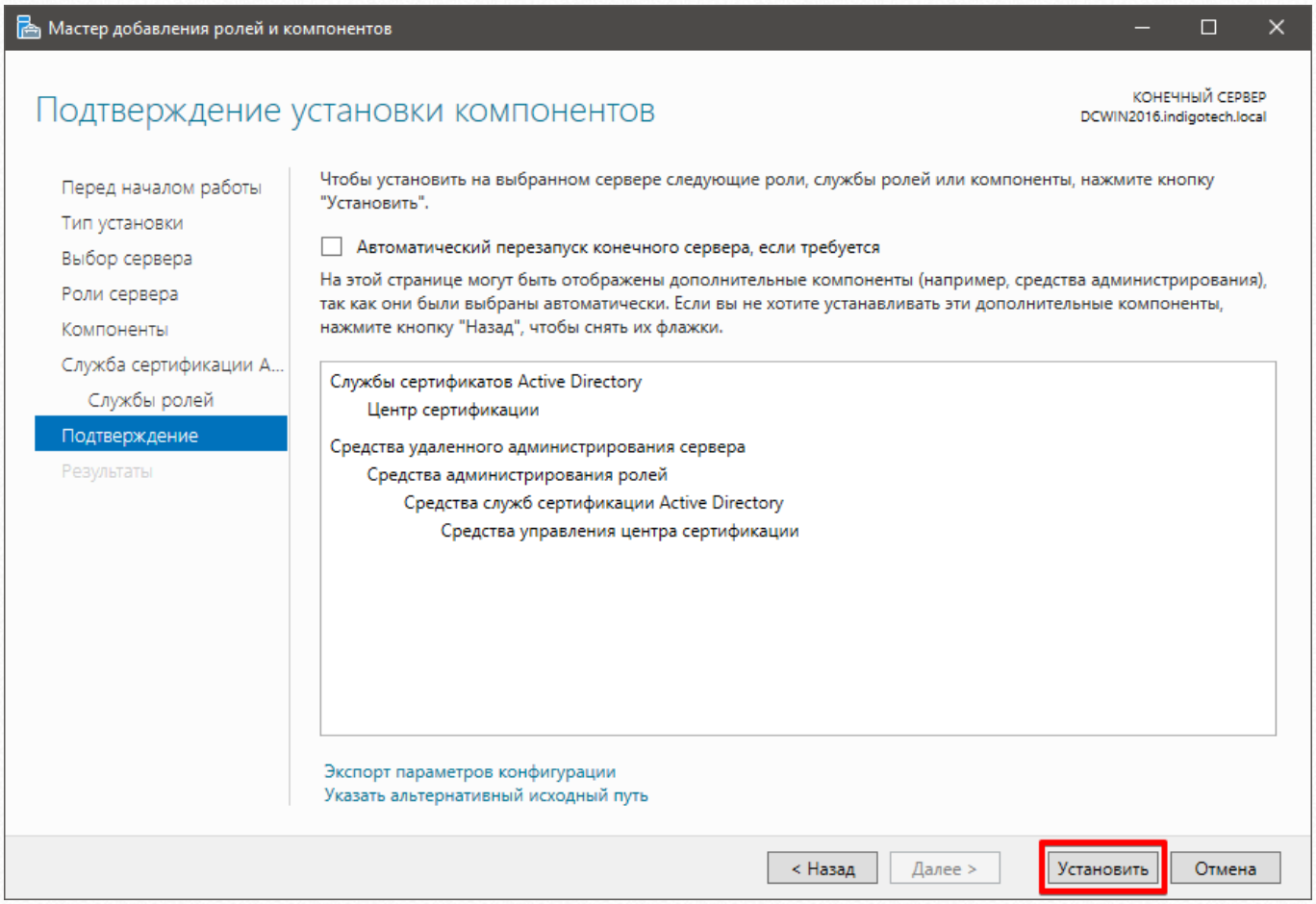


6. На вкладке компоненты жмем кнопку «Далее».
7. На вкладке «Службы сертификатов Active Directory» жмем кнопку «Далее».

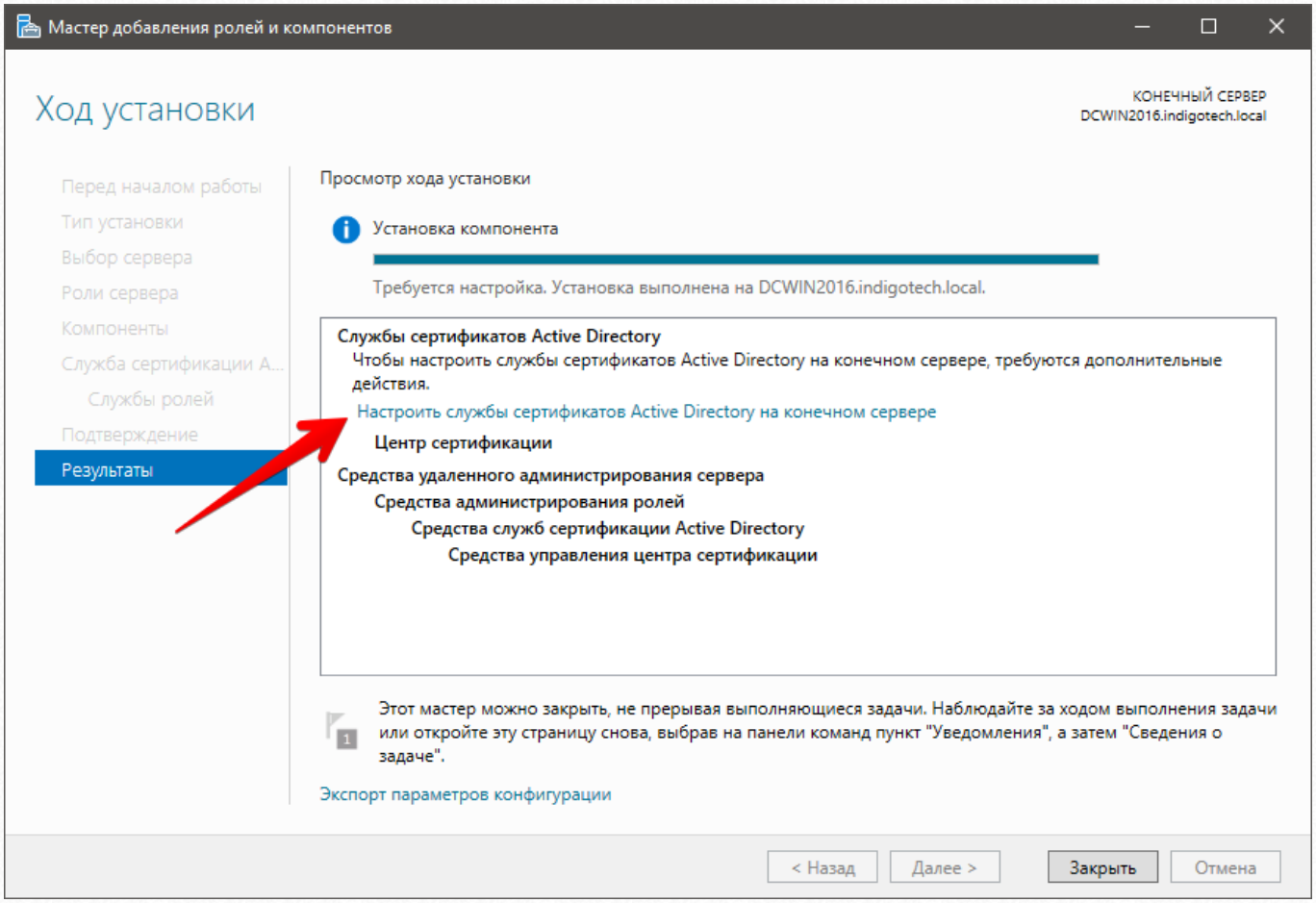
8. На вкладке «Службы ролей» убеждаемся, что отмечен флажок «Центр сертификации» и жмем «Далее».



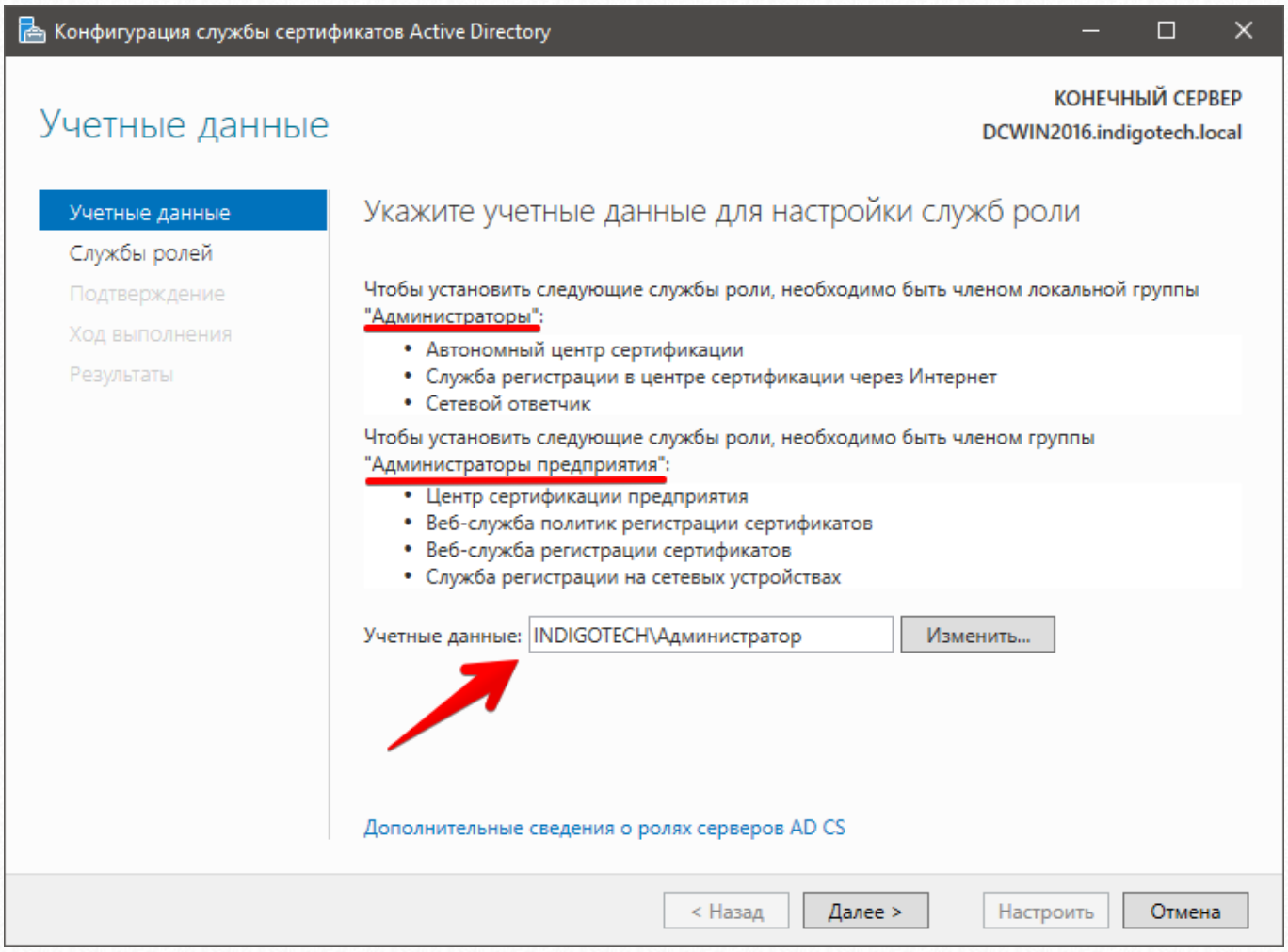
9. На вкладке «Подтверждение установки компонентов» жмем кнопку «Установить».



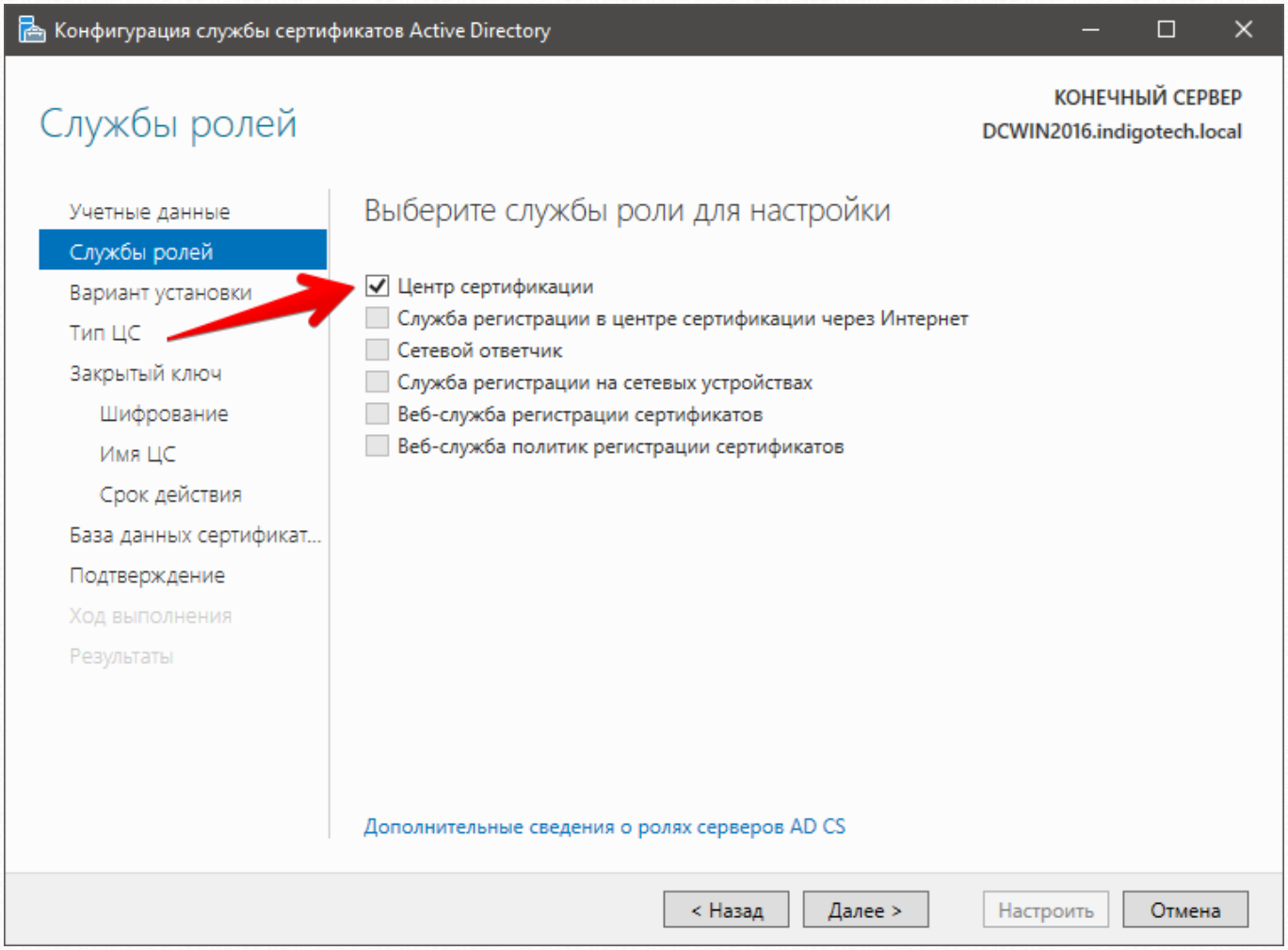
10. По завершению установки на вкладке «Результаты» появится ссылка «Настроить службы сертификатов Active Directory на конечном сервере», нажимаем на нее.



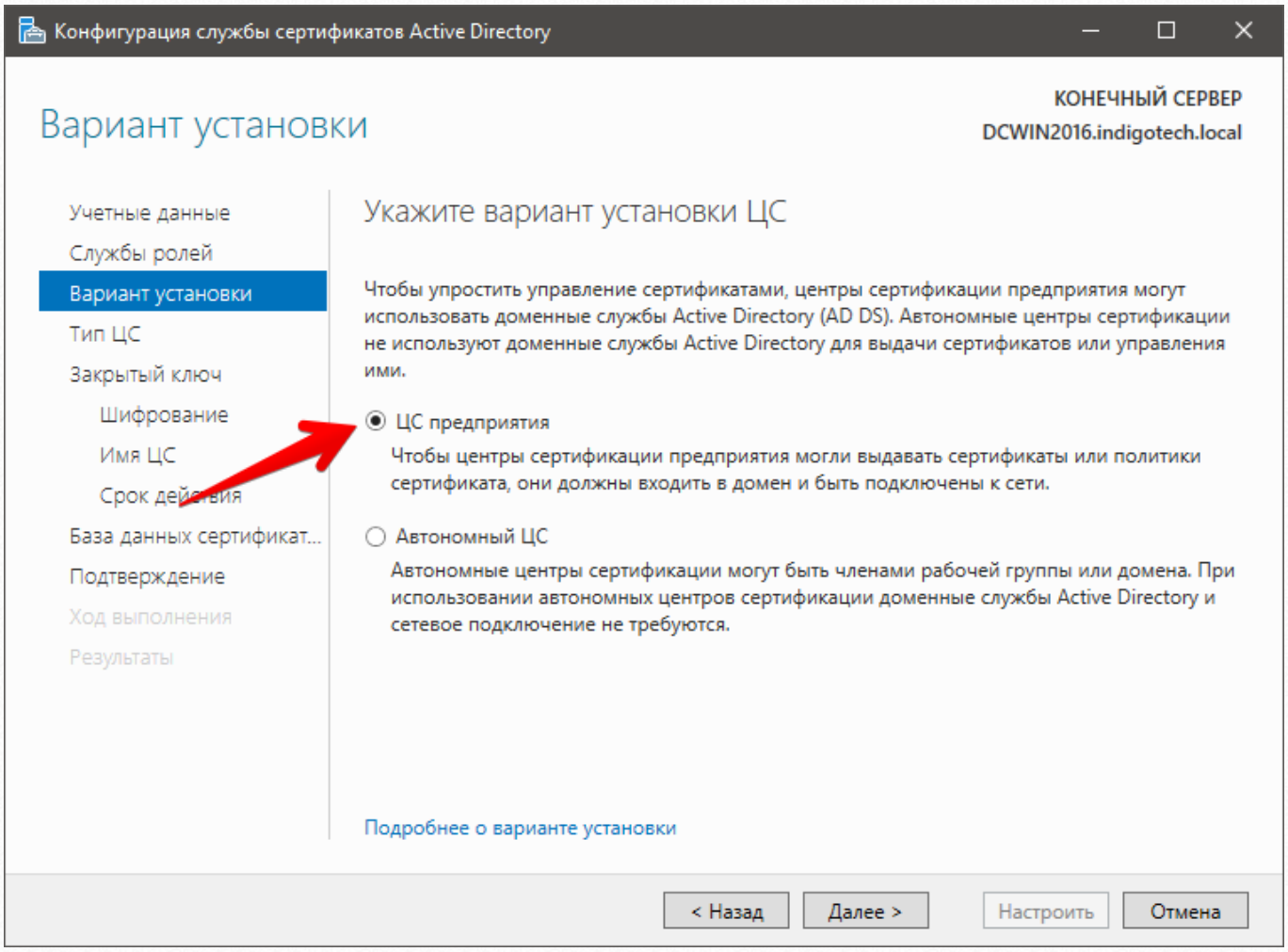
11. В открывшемся окне «Конфигурация службы сертификатов Active Directory» на вкладке «Учетные данные» убедитесь, что в поле «Учетные данные» выбран аккаунт пользователя, который входит в группы «Администраторы» и «Администраторы предприятия». Жмем кнопку «Далее».



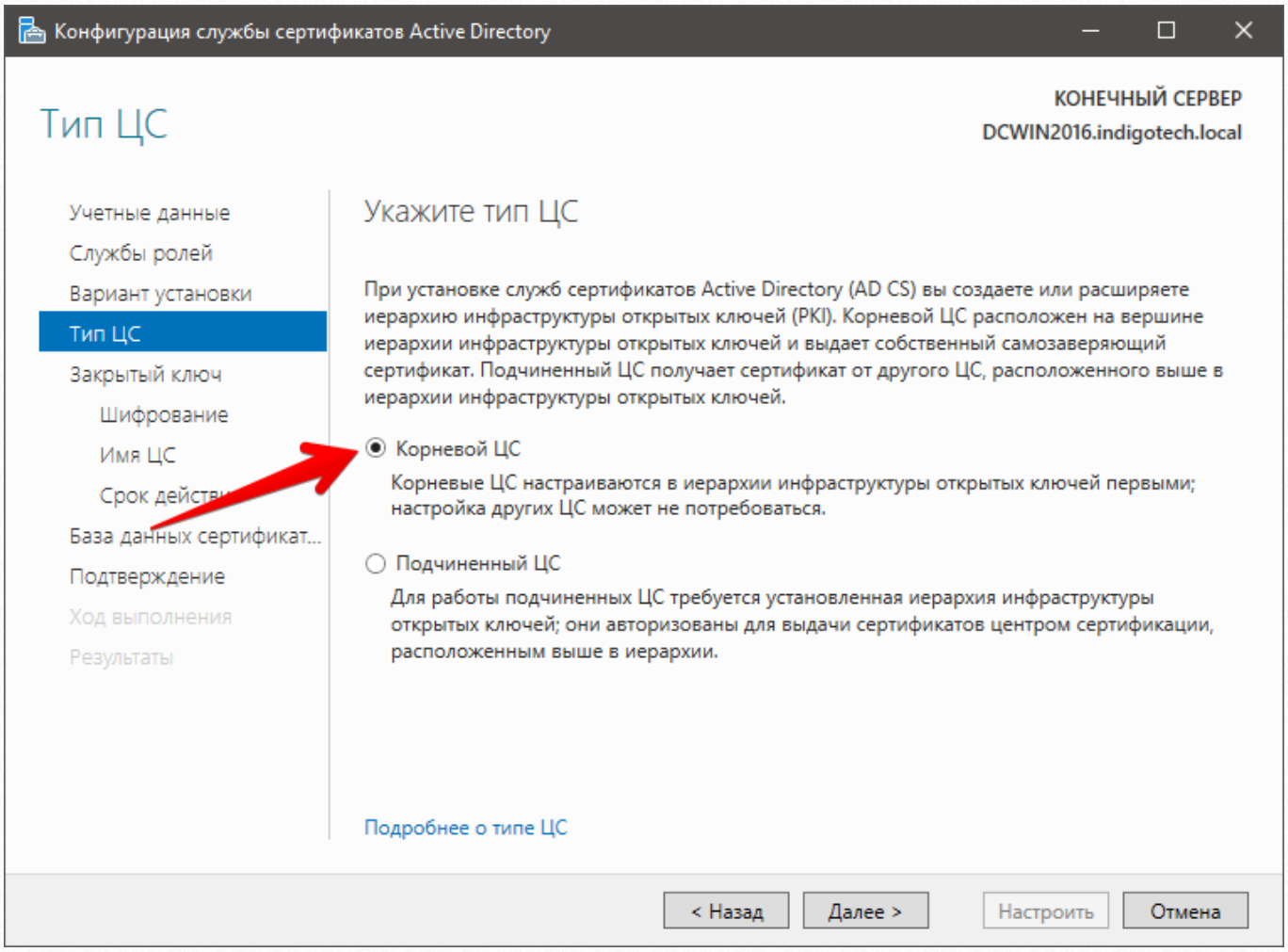
12. На вкладке «Службы ролей» ставим флажок на пункте «Центр сертификации» и нажимаем «Далее».



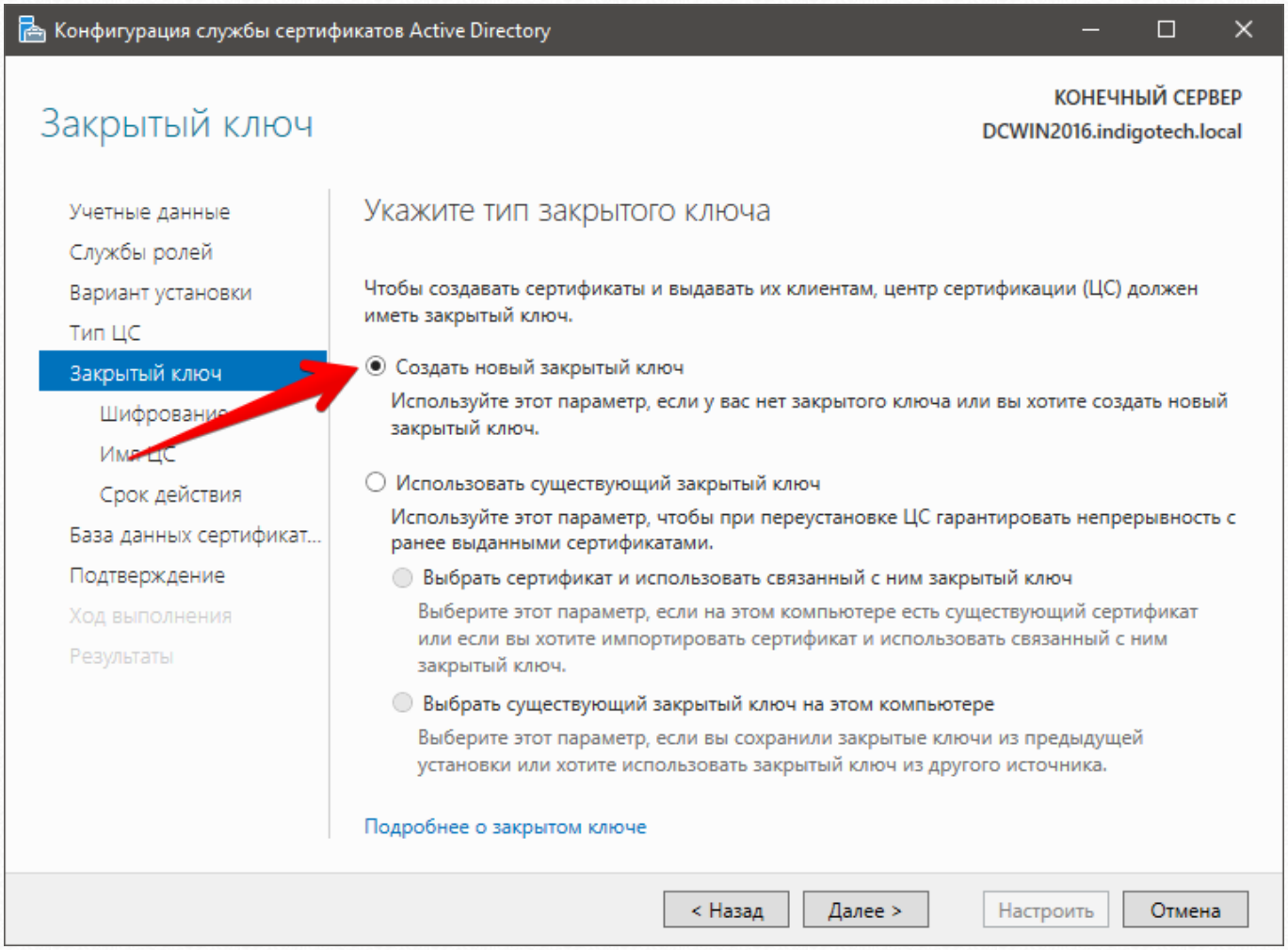
13. На вкладке «Вариант установки» выбираем «ЦС предприятия» и жмем «Далее».



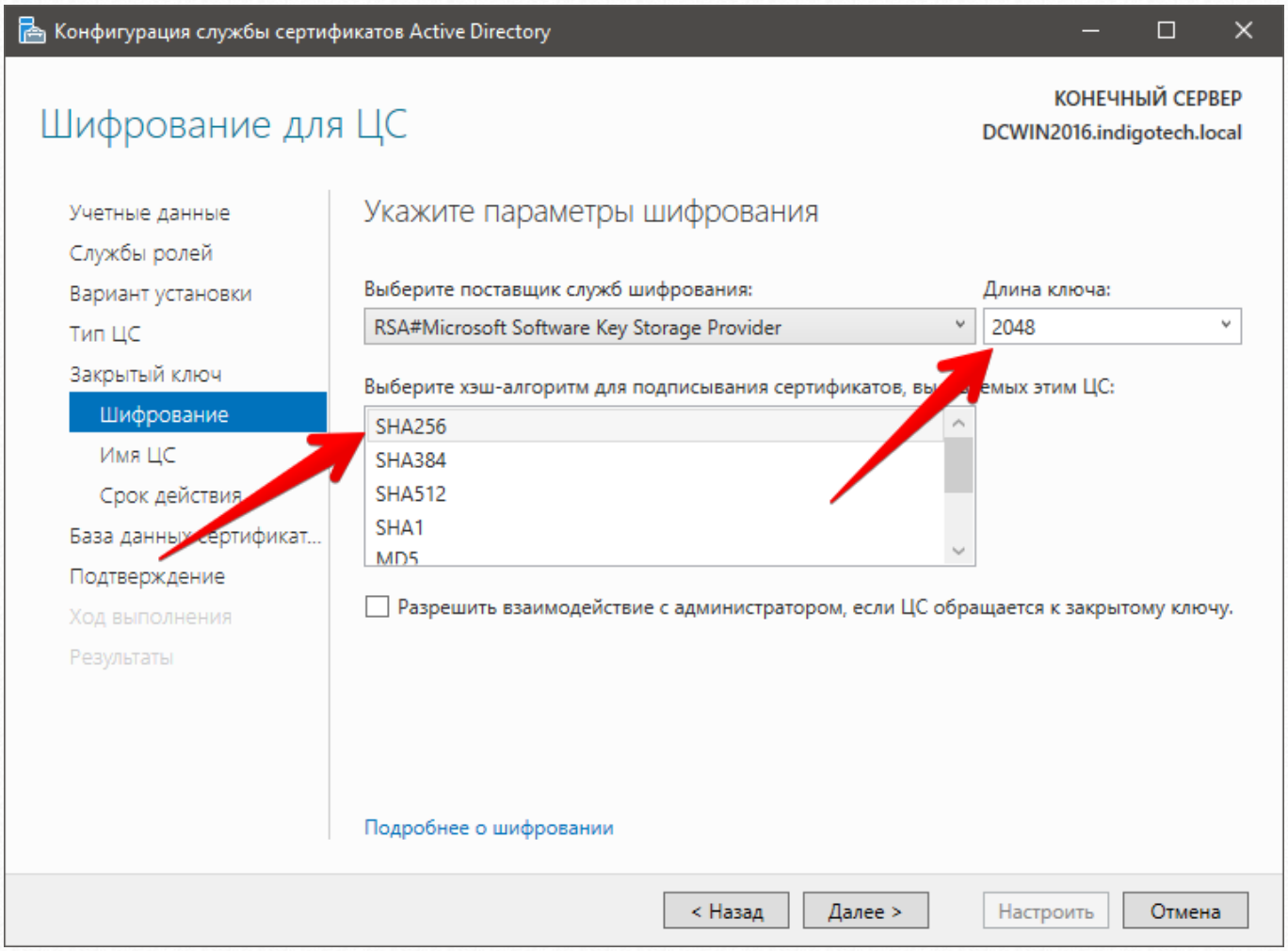
14. На вкладке «Тип ЦС» выбераем «Корневой ЦС» и жмем «Далее».



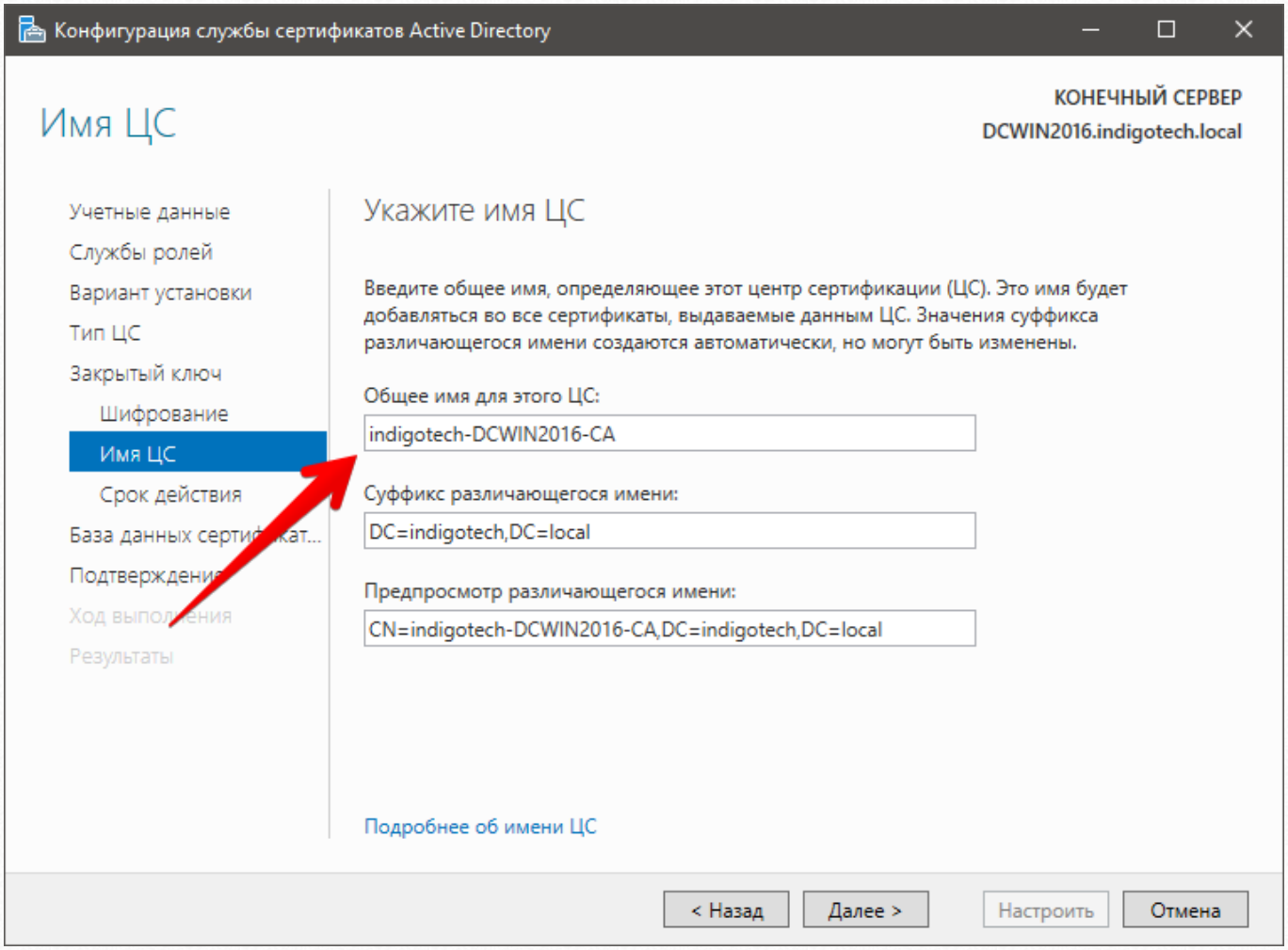
15. На вкладке «Закрытый ключ» выбираем «Создать новый закрытый ключ» и жмем «Далее».



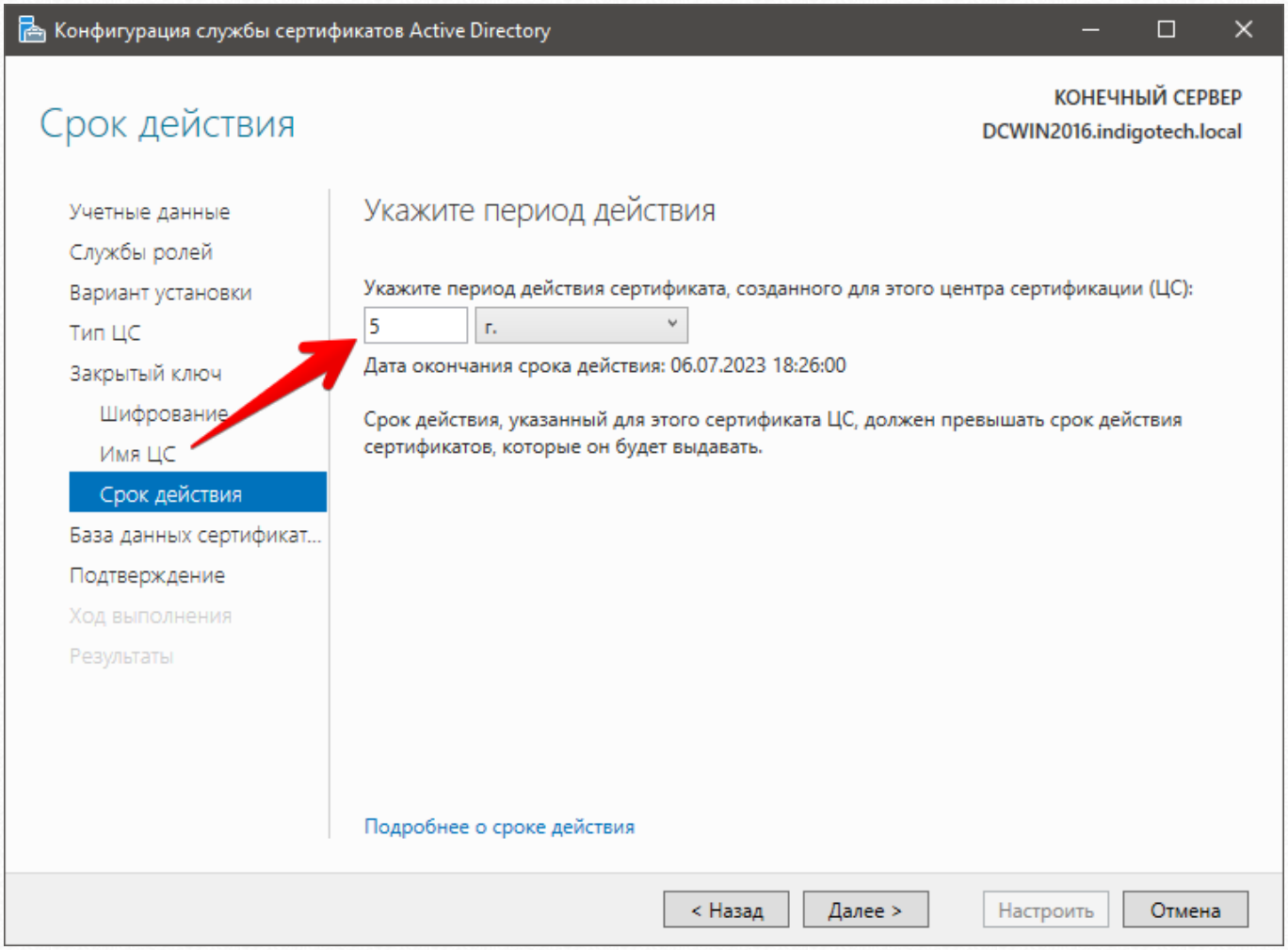
16. На вкладке «Шифрование для ЦС» обратите внимание, чтобы в графе «Длина ключа» было выбрано значение «2048», а в списке «Выберите хэш-алгоритм для подписывания сертификатов, выдаваемых этим ЦС» было выбрано значение «SHA-256».



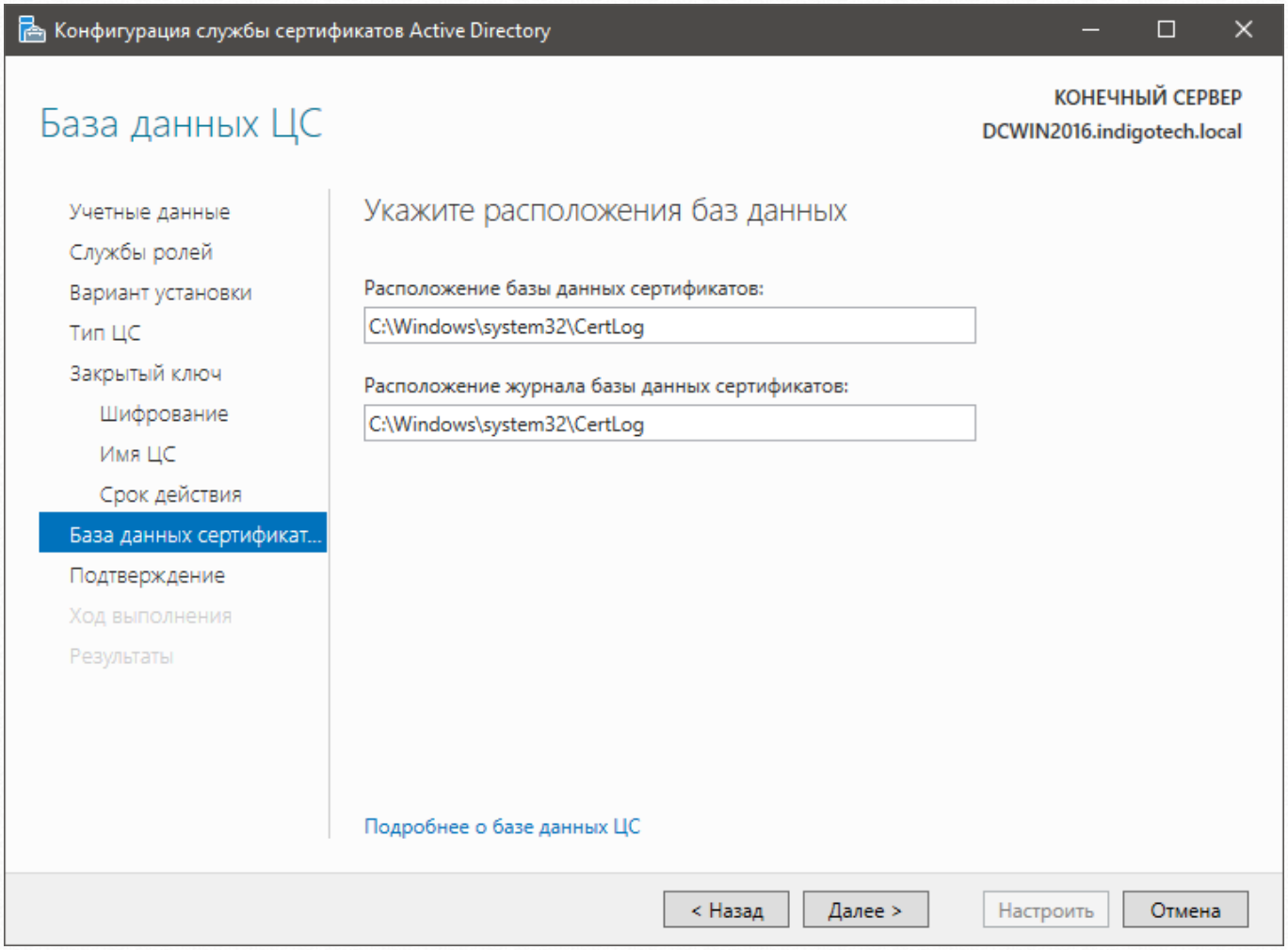
17. На вкладке «Имя ЦС» измените общее имя для ЦС или оставьте предложенное и нажмите «Далее».



18. На вкладке «Срок действия» укажите период действия сертификата (по умолчанию 5 лет) и нажмите «Далее».



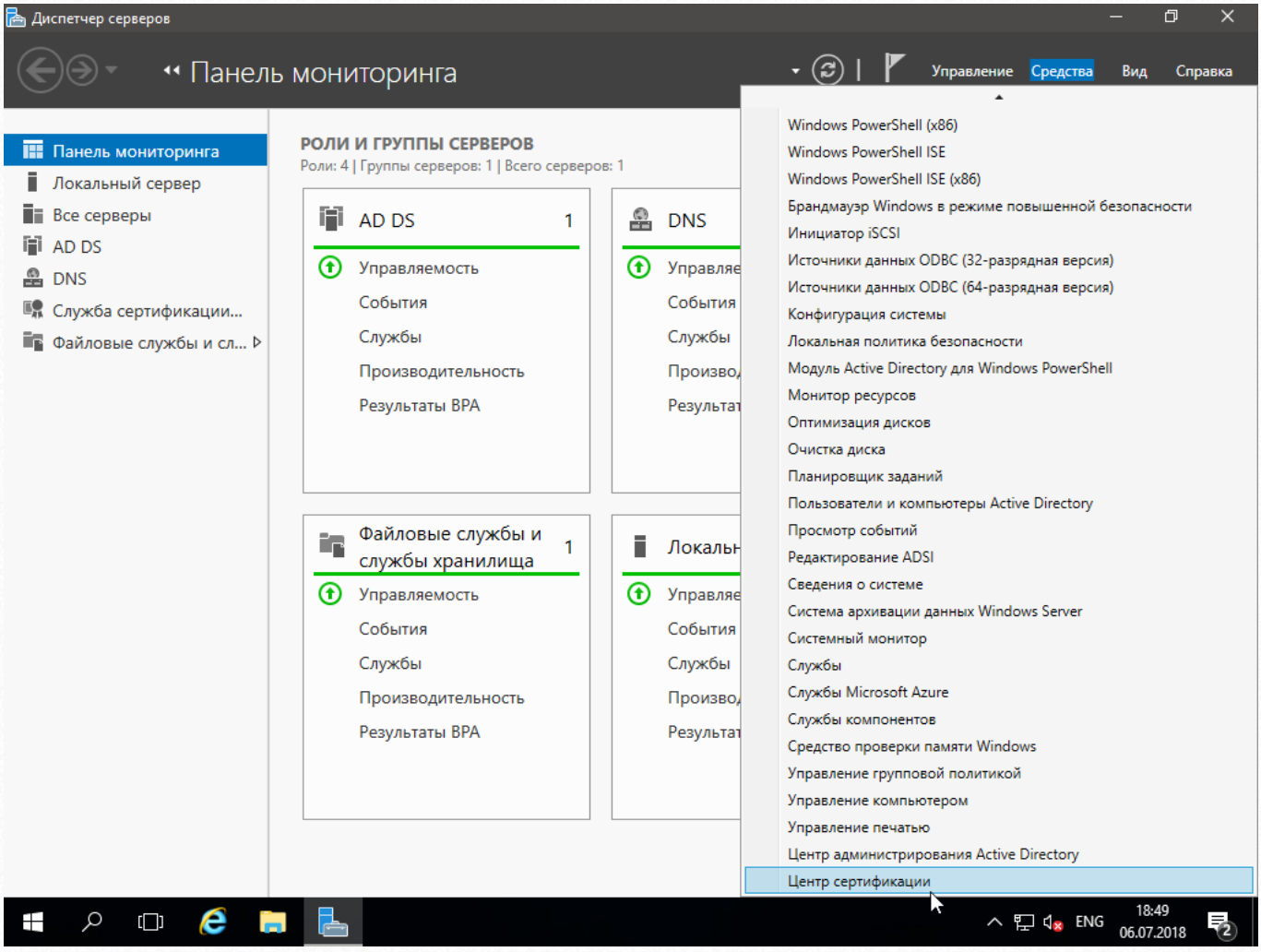
19. На вкладке «База данных ЦС» укажите каталоги расположения базы данных сертификатов и журнала базы данных сертификатов или оставьте значения по умолчанию и нажмите «Далее».



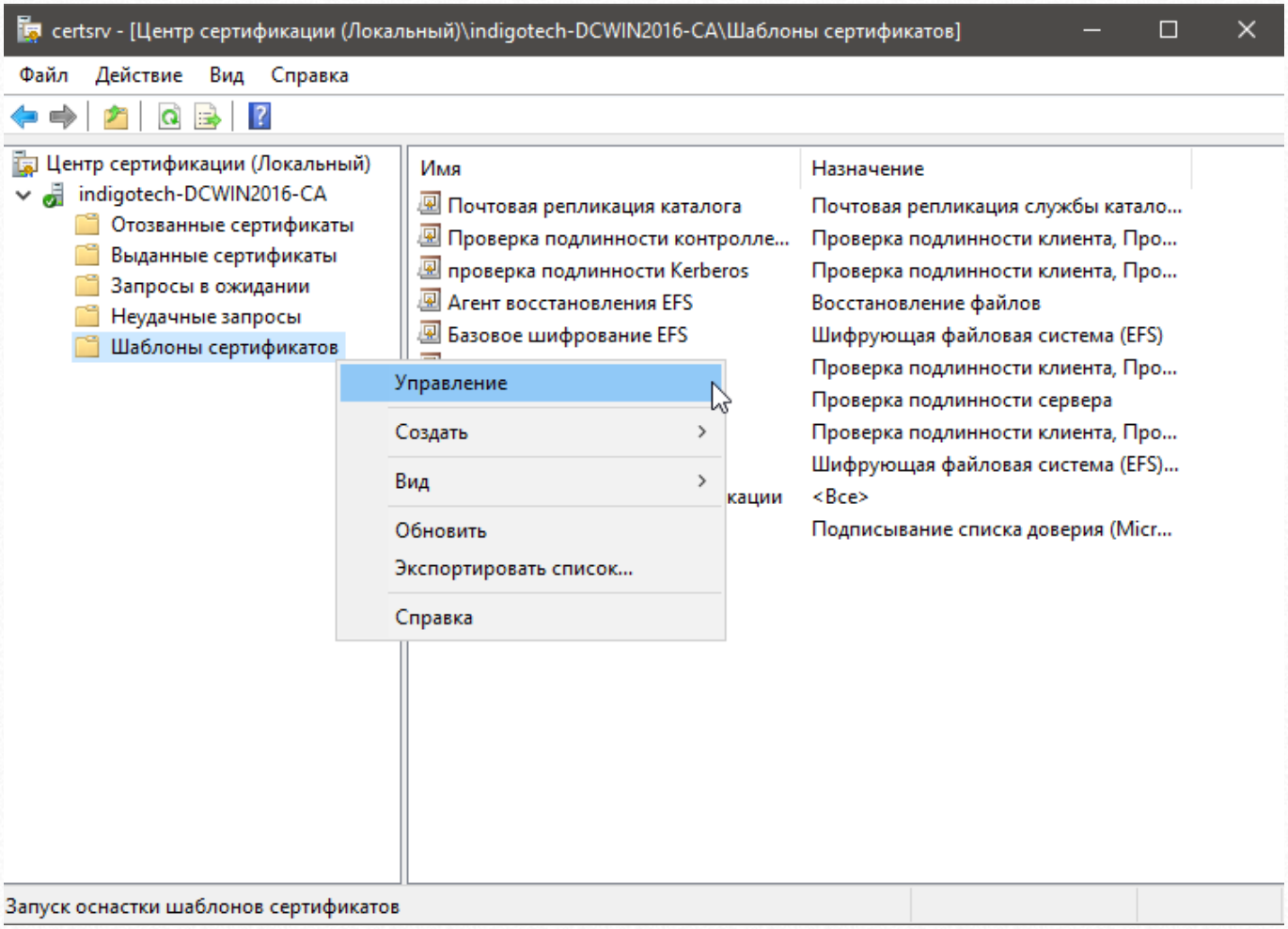
20. На вкладке «Подтверждение» нажмите кнопку «Настроить». А после настройки на вкладке «Результаты» кнопку «Закрыть». И вернувшись в окно «Мастер добавления ролей и компонентов» также нажимаем кнопку «Закрыть».

2.2.2. Генерация необходимых сертификатов

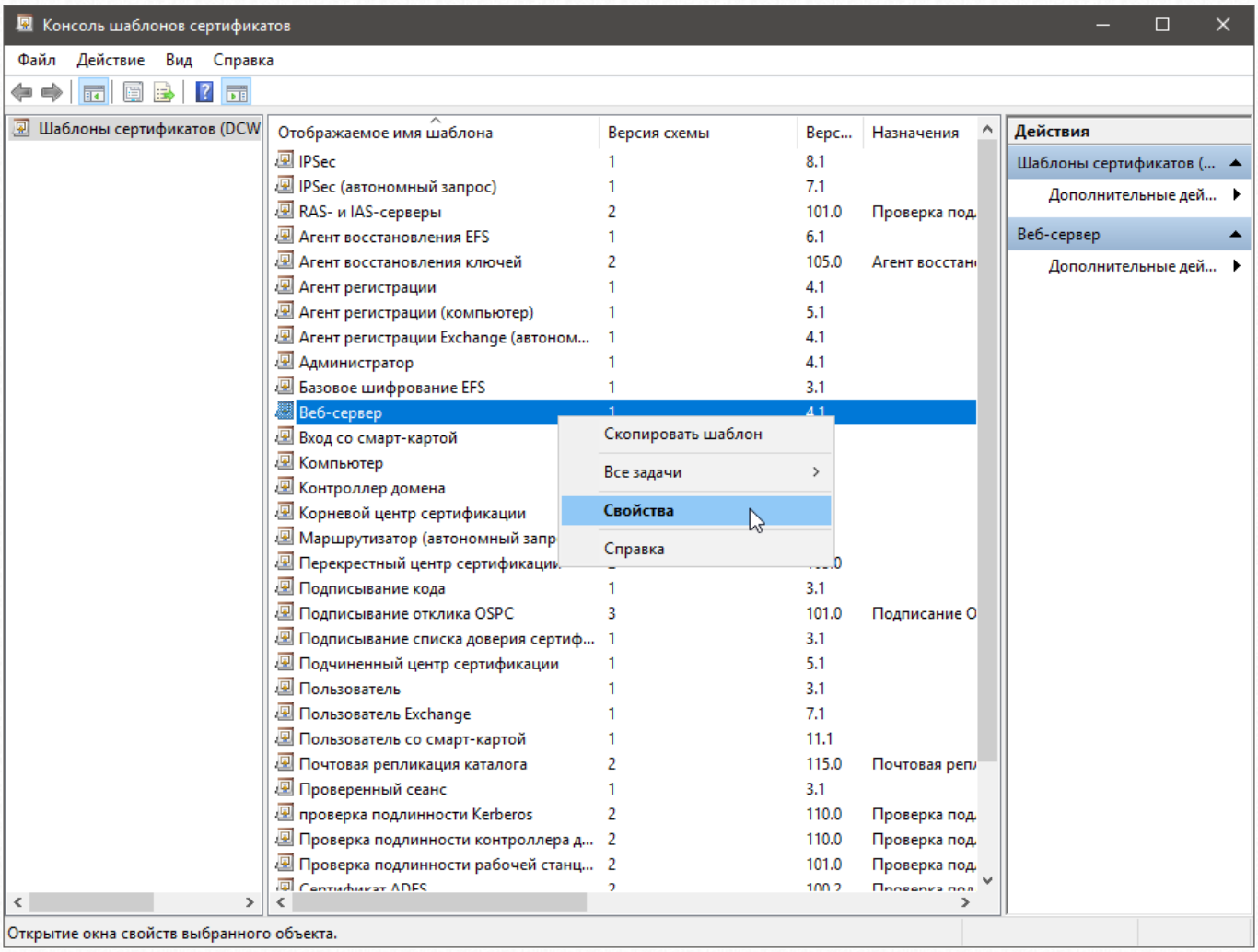
1. После установки центра сертификации необходимо создать сертификат для службы федерации AD, для этого в окне «Диспетчер серверов» нажимаем в меню «Средства» → «Центр сертификации».



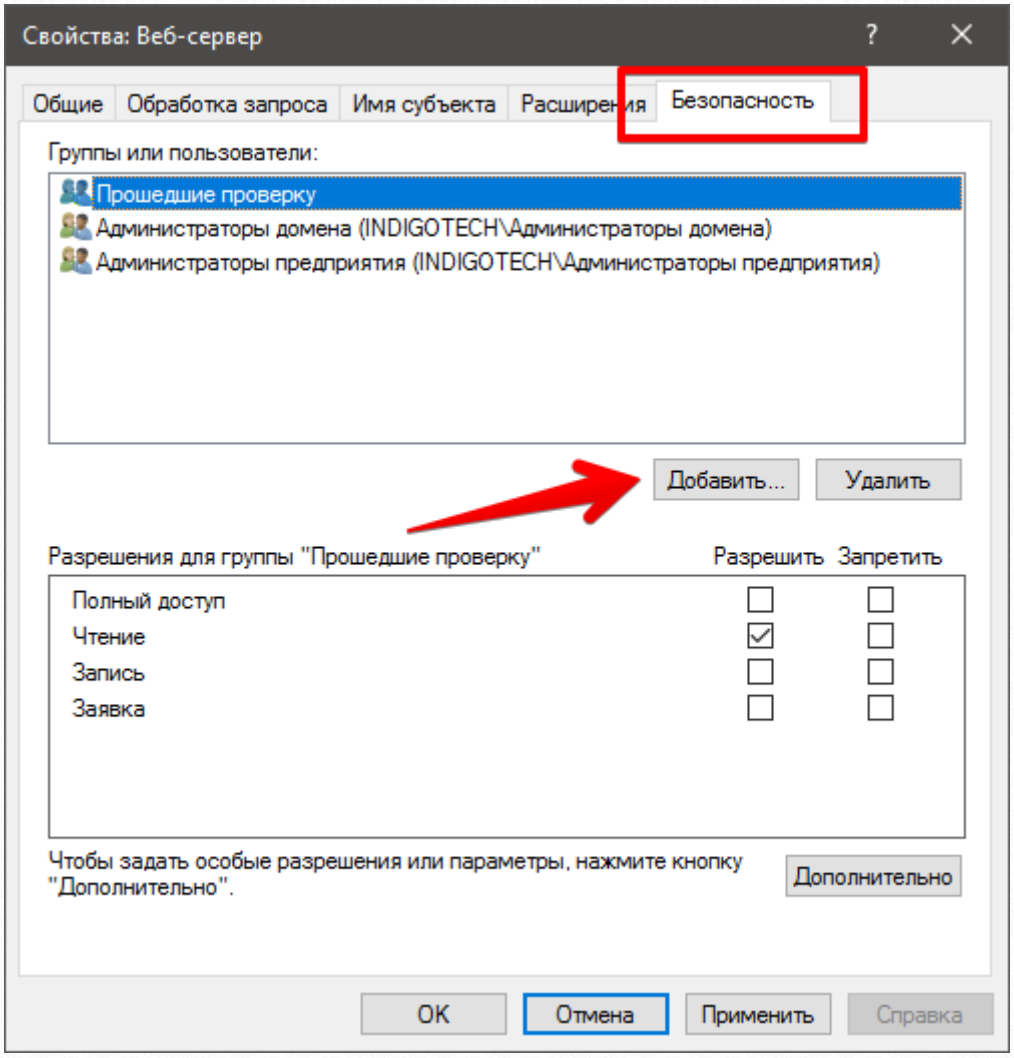
2. В открывшемся окне «Центр сертификации» слева раскрываем установленный центр сертификации и кликаем правой кнопкой мыши по разделу «Шаблоны сертификатов» и в выпадающем меню выбираем пункт «Управление».



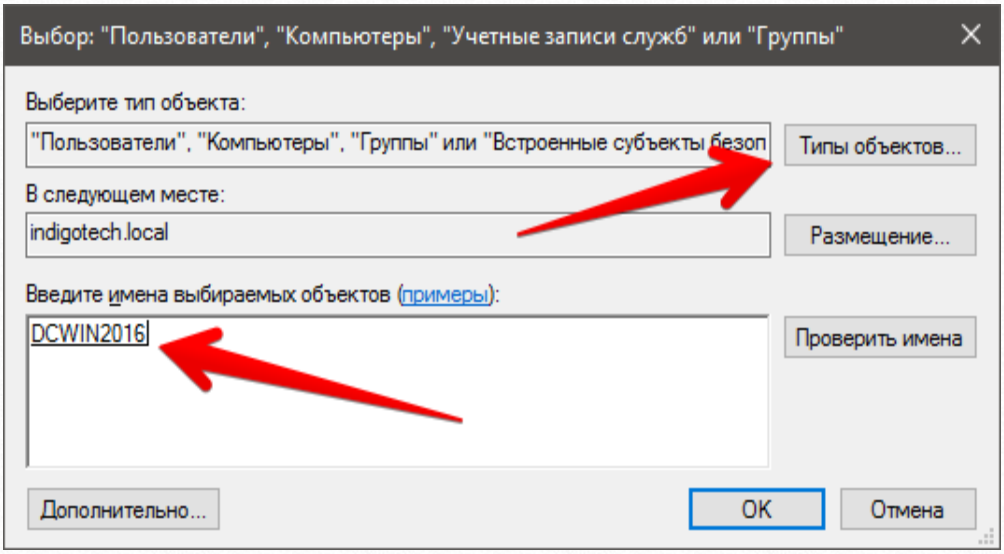
3. Нам необходимо разрешить этому серверу выдавать сертификаты по шаблону «Веб-сервер», а также на его основе создать новый шаблон сертификатов. Для этого выберите из списка шаблон «Веб-сервер», кликните по нему правой кнопкой мыши и выберите пункт «Свойства».

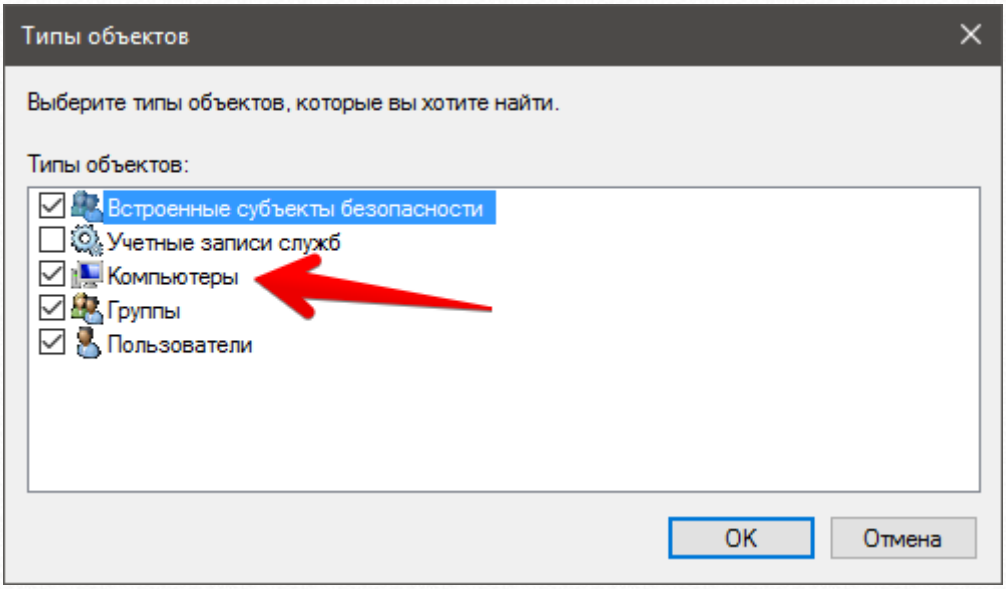


4. В окне «Свойства: Веб-сервер» перейдите на вкладку безопасность и нажмите кнопку «Добавить».

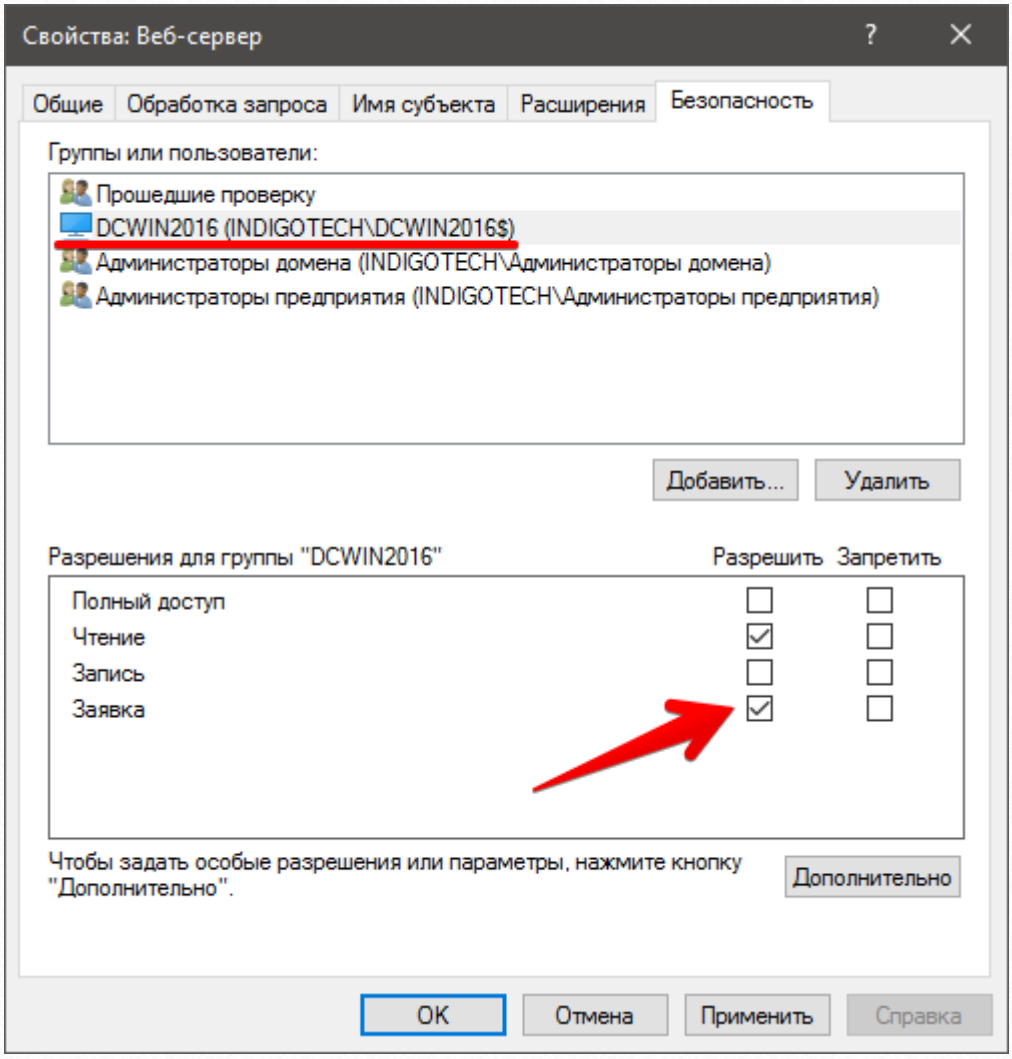


5. В появившемся окне нажмите кнопку «Типы объектов...» и поставьте флажок на пункте «Компьютеры». Затем впишите имя этого компьютера в поле «Введите имена выбираемых объектов» и нажмите «ОК».

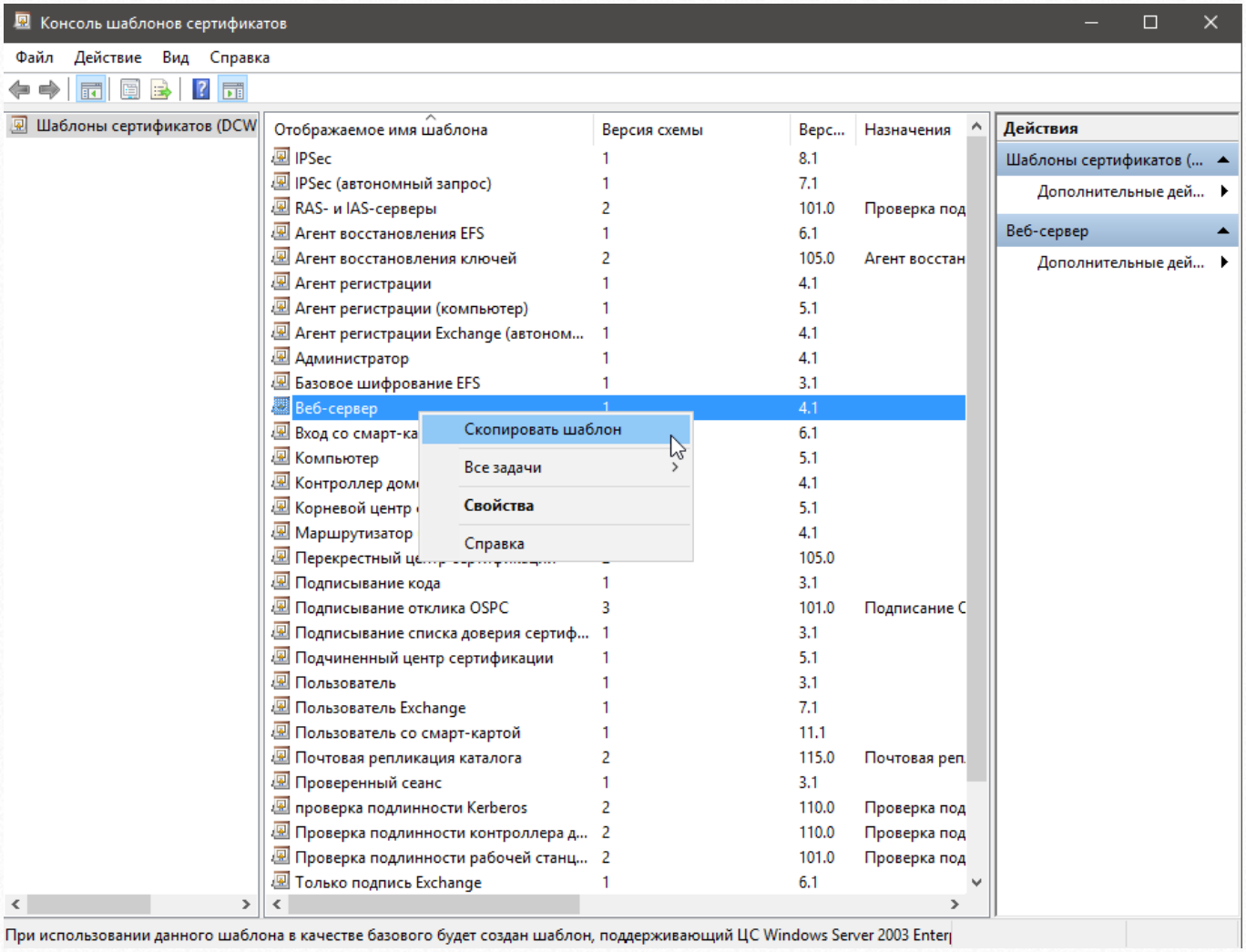




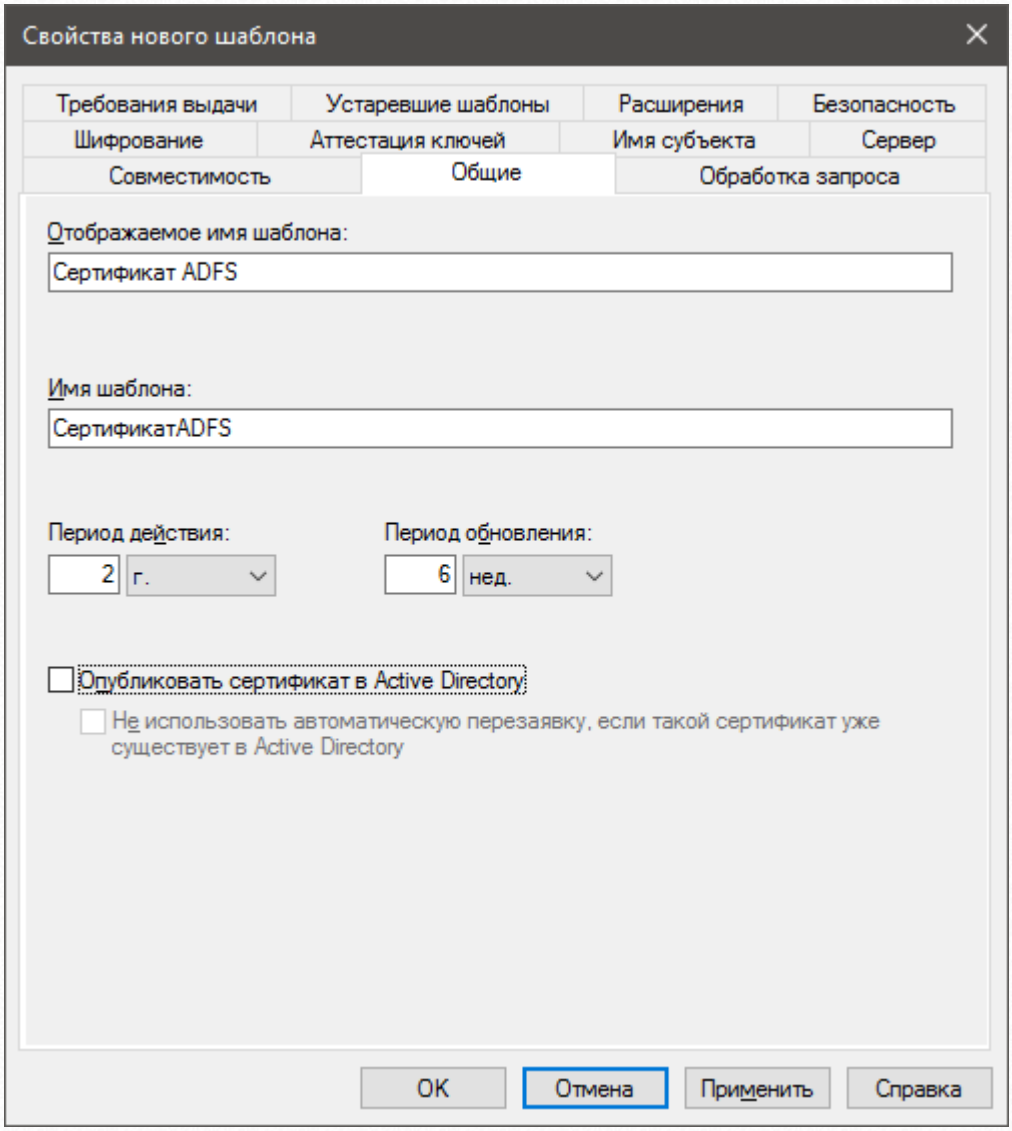
6. Вернувшись на вкладку «Безопасность» выберите в списке «Группы или пользователи» добавленный компьютер и в списке «Разрешение для группы» поставьте флажок в столбце «Разрешить» напротив пункта «Заявка». И нажимаем кнопку «ОК».



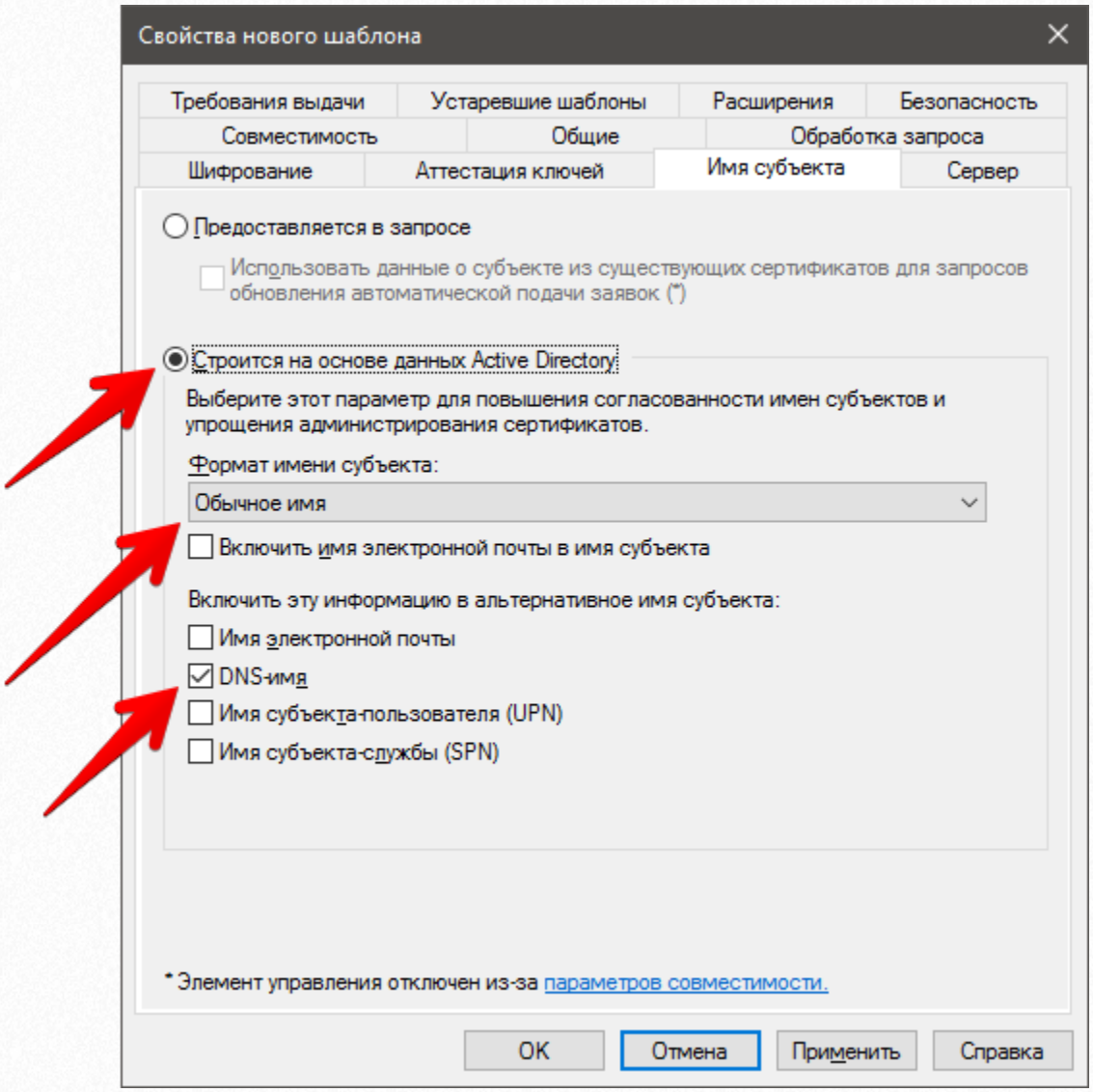
7. Теперь необходимо создать новый шаблон сертификатов, для этого кликаем на шаблоне «Веб-сервер» правой кнопкой мыши и выбираем пункт «Скопировать шаблон».



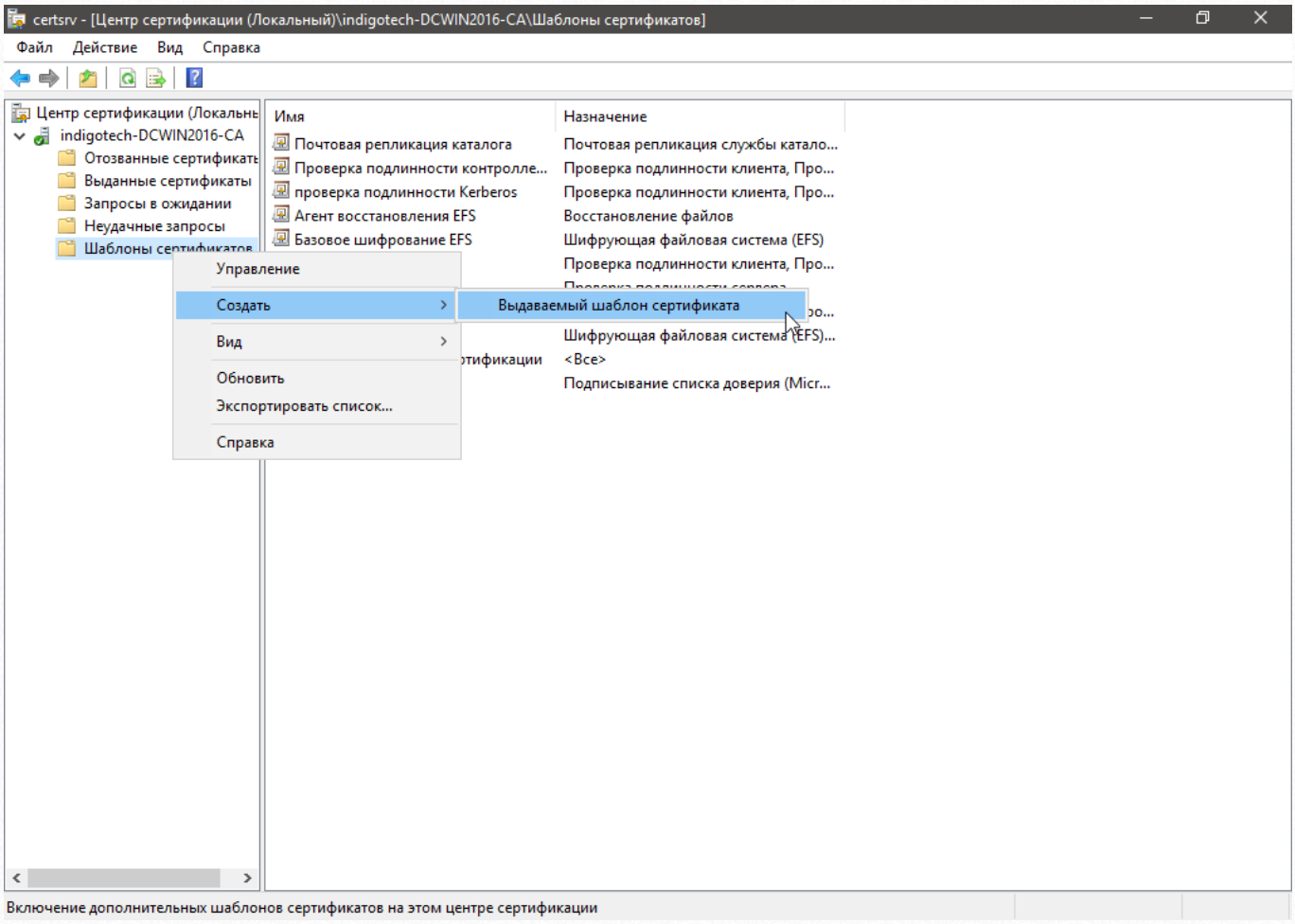
8. В открывшемся окне «Свойства нового шаблона» на вкладке «Общие» задаем «Отображаемое имя шаблона», например, «Сертификат ADFS».



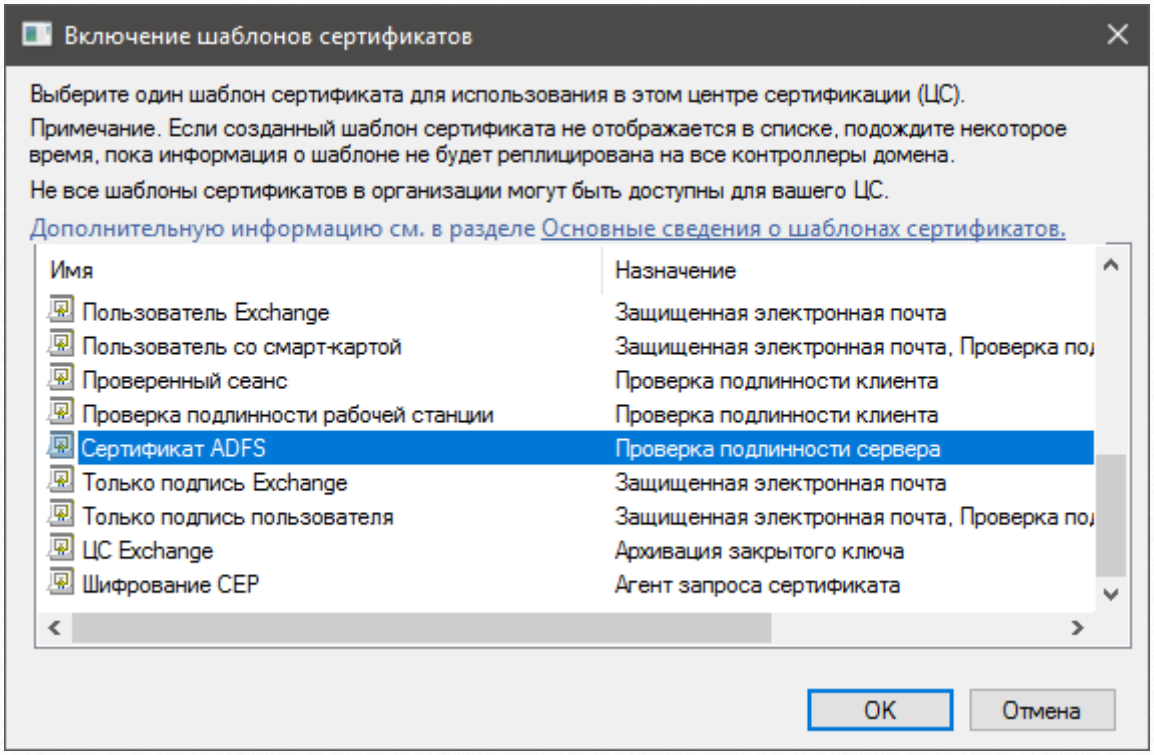
9. На вкладке «Имя субъекта» ставим выбор на пункте «Строится на основе данных Active Directory» и в графе «Формат имени субъекта» выбираем пункт «Обычное имя», а в списке «Включить эту информацию в альтернативное имя субъекта» оставляем только DNS-имя и нажимаем «ОК».



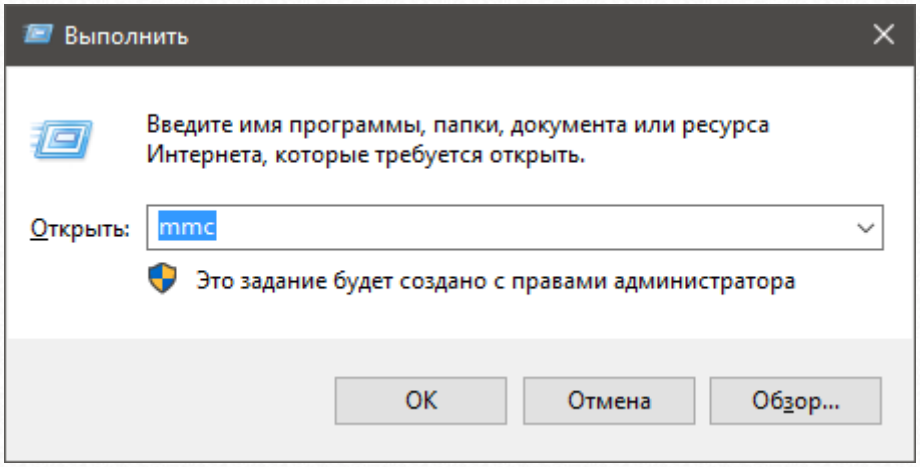
10. Вернувшись в окно «Центр сертификации» кликните правой кнопкой мыши по группе «Шаблоны сертификатов» и выберите пункт «Создать» → «Выдаваемый шаблон сертификата».



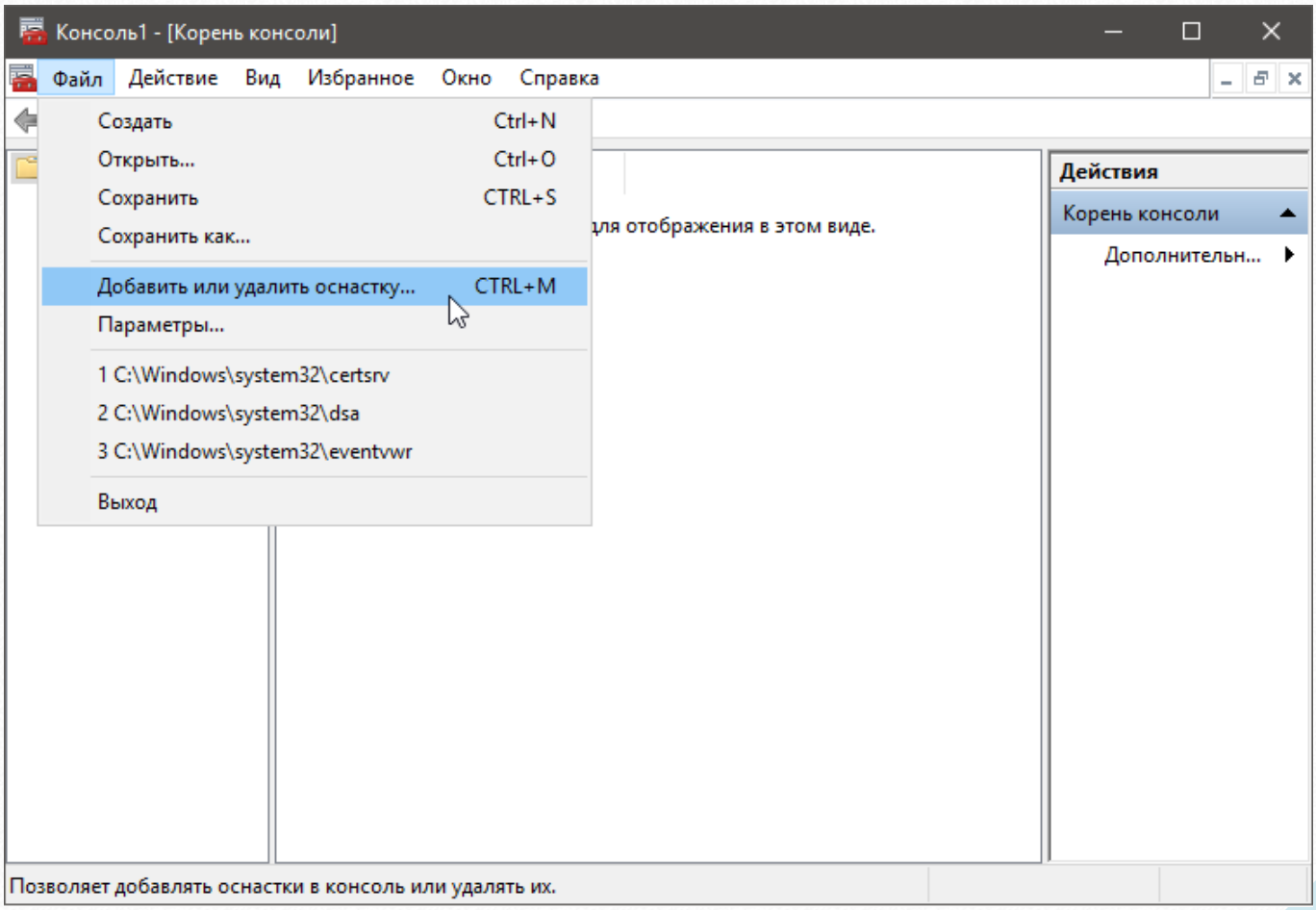
11. В окне «Включение шаблонов сертификатов» выбираем из списка созданный нами шаблон «Сертификат ADFS» и нажимаем кнопку «ОК». И закрываем окно «Центр сертификации».



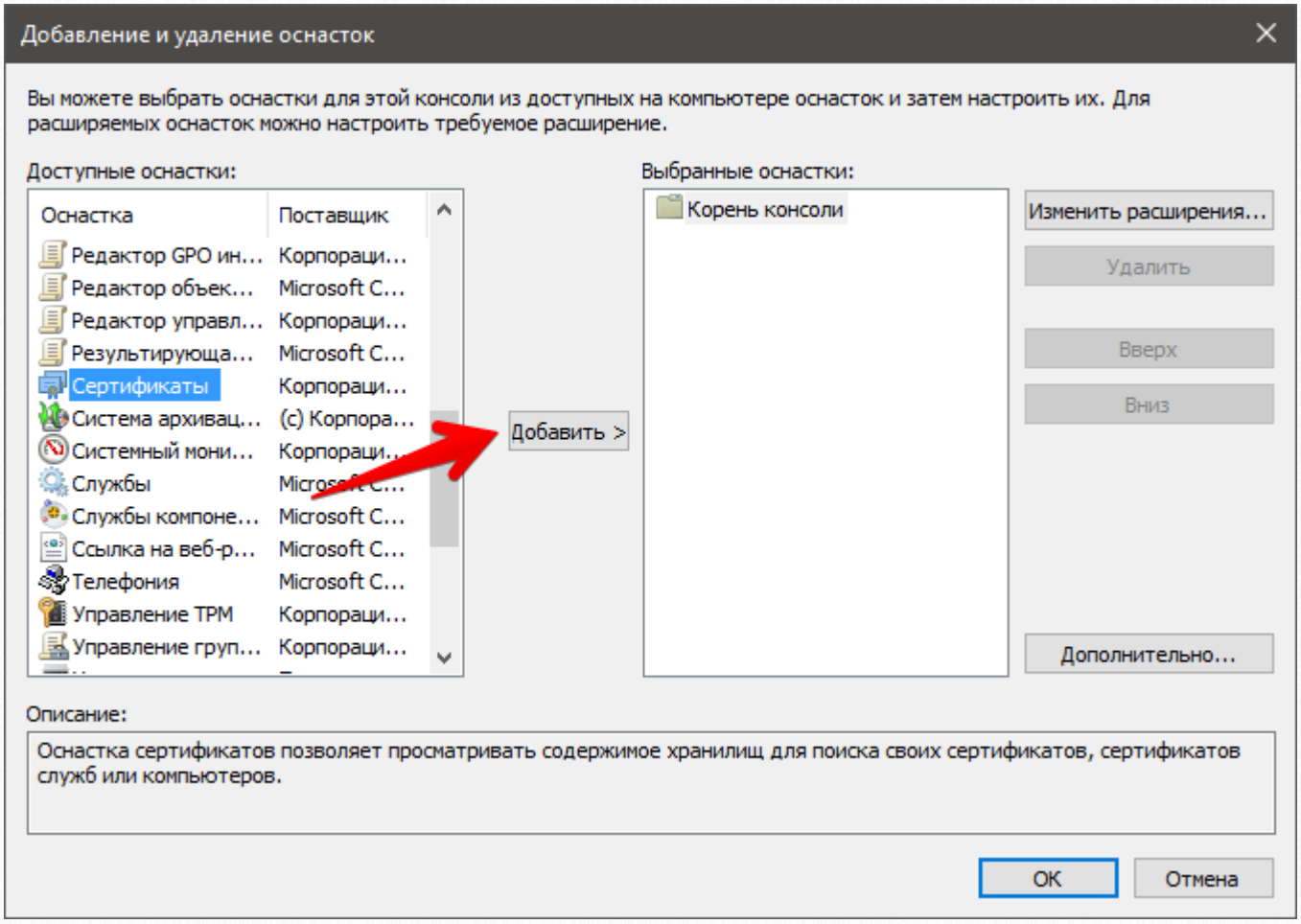
12. Откройте диалог «Выполнить» через меню «Пуск» или нажав сочетание клавиш ⊞+R. В поле «Открыть» введите «mmc» и нажмите кнопку «ОК».



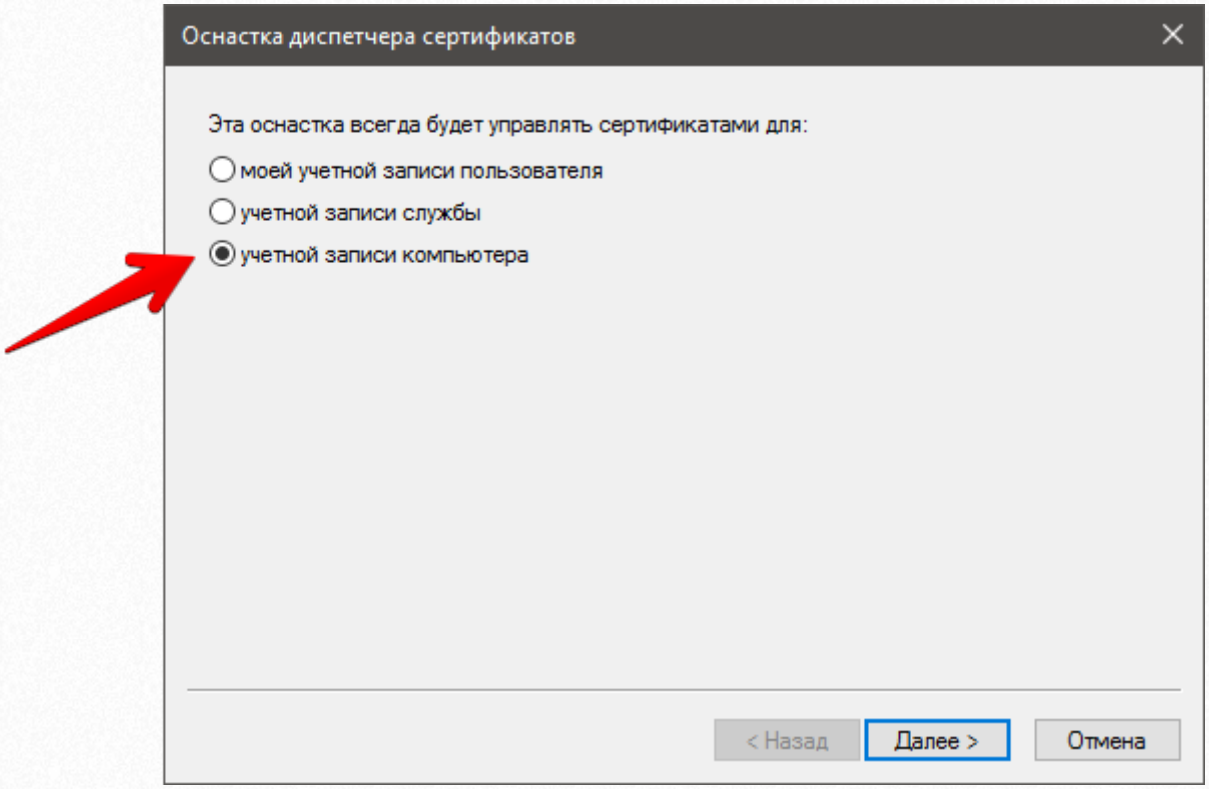
13. Выберите в главном меню «Файл» → «Добавить или удалить оснастку...».



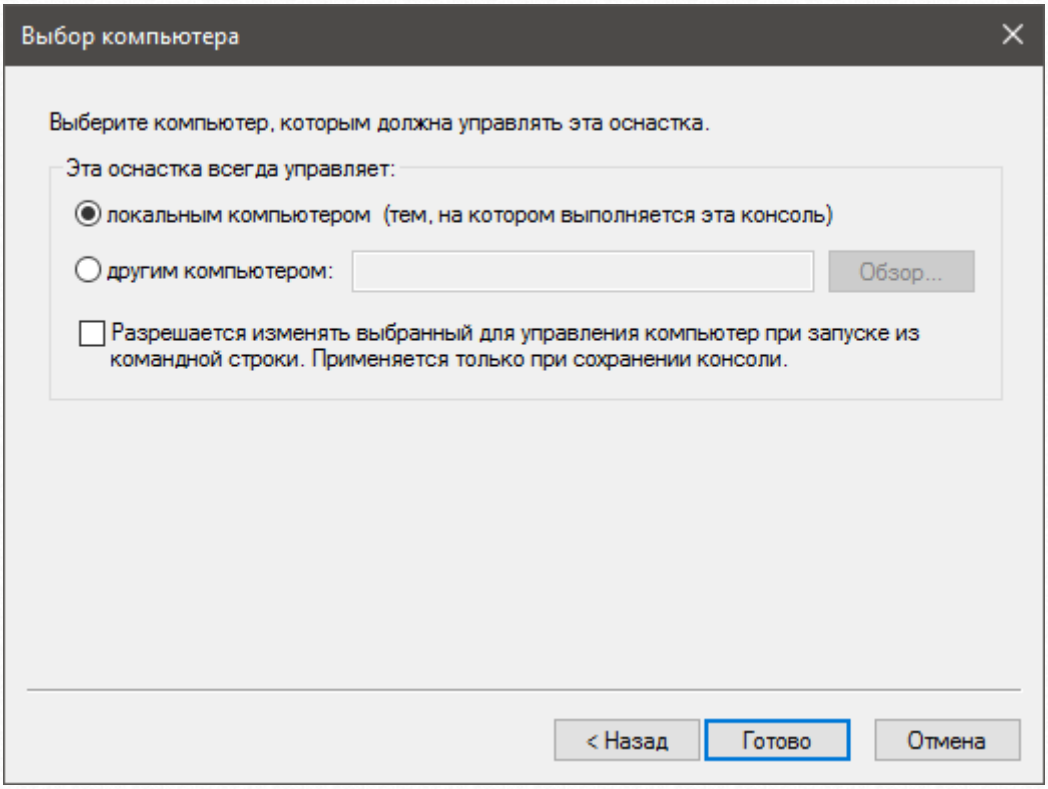
14. В окне «Добавление и удаление оснасток» в списке «Доступные оснастки» выберите «Сертификаты» и нажмите кнопку добавить.



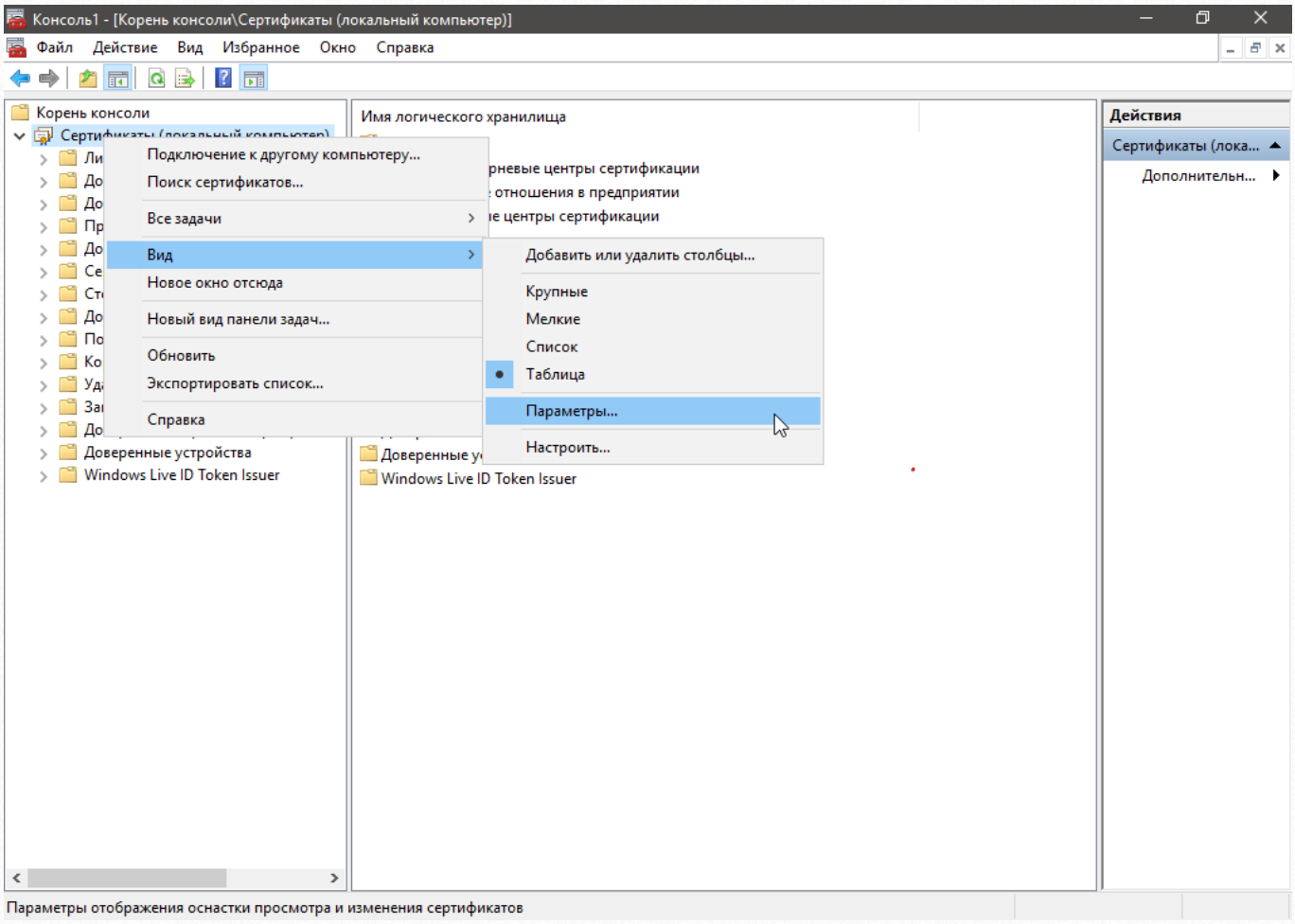
15. В окне «Оснастка диспетчера сертификатов» выберите тип «учетной записи компьютера» и нажмите кнопку «Далее».



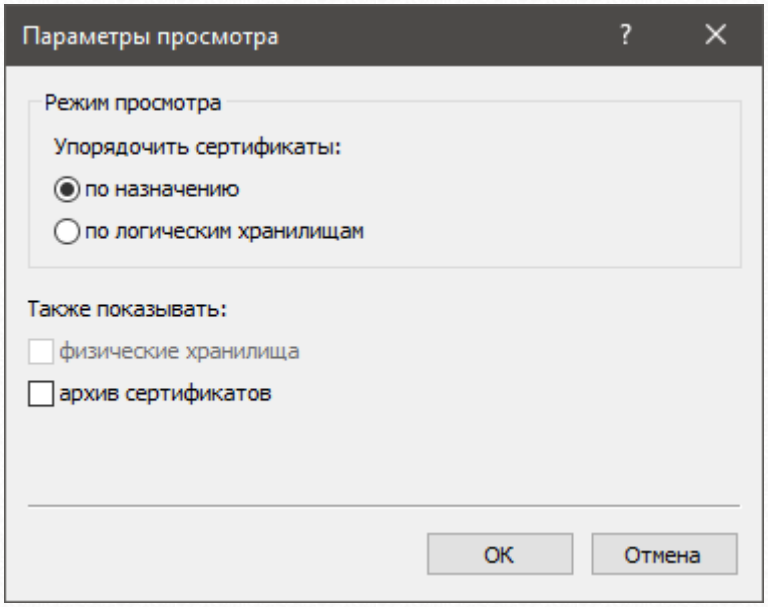
16. В окне «Выбор компьютера» выбираем пункт «локальным компьютером (тем, на котором выполняется консоль)» и нажимаем кнопку «Готово», а затем нажимаем «ОК» в окне «Добавление и удаление оснасток».



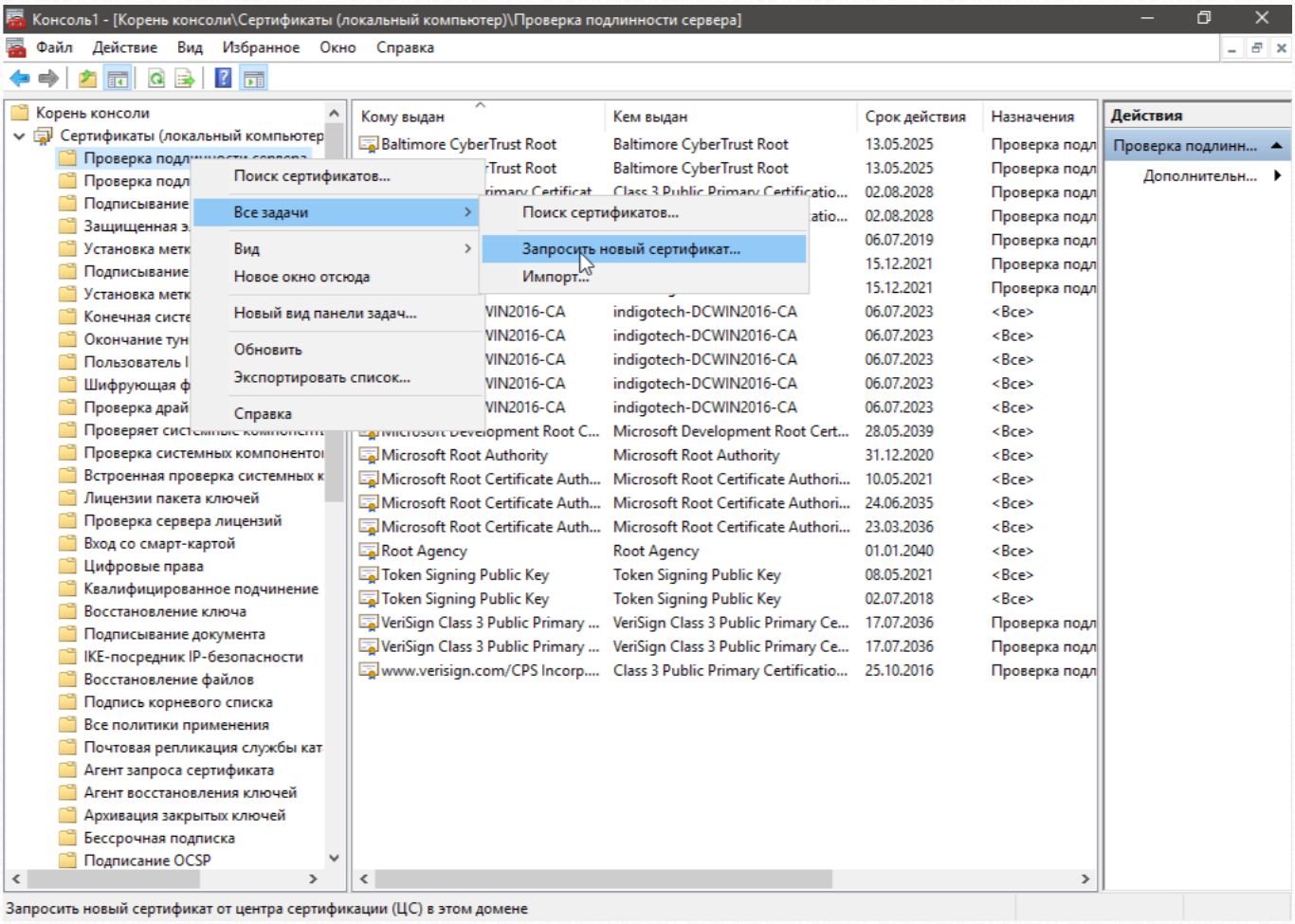
17. В корень консоли добавится группа «Сертификаты (локальный компьютер)». Нажмите по ней левой кнопкой мыши, чтобы она стала активной, затем правой кнопкой мыши и в меню выберите «Вид» → «Параметры».



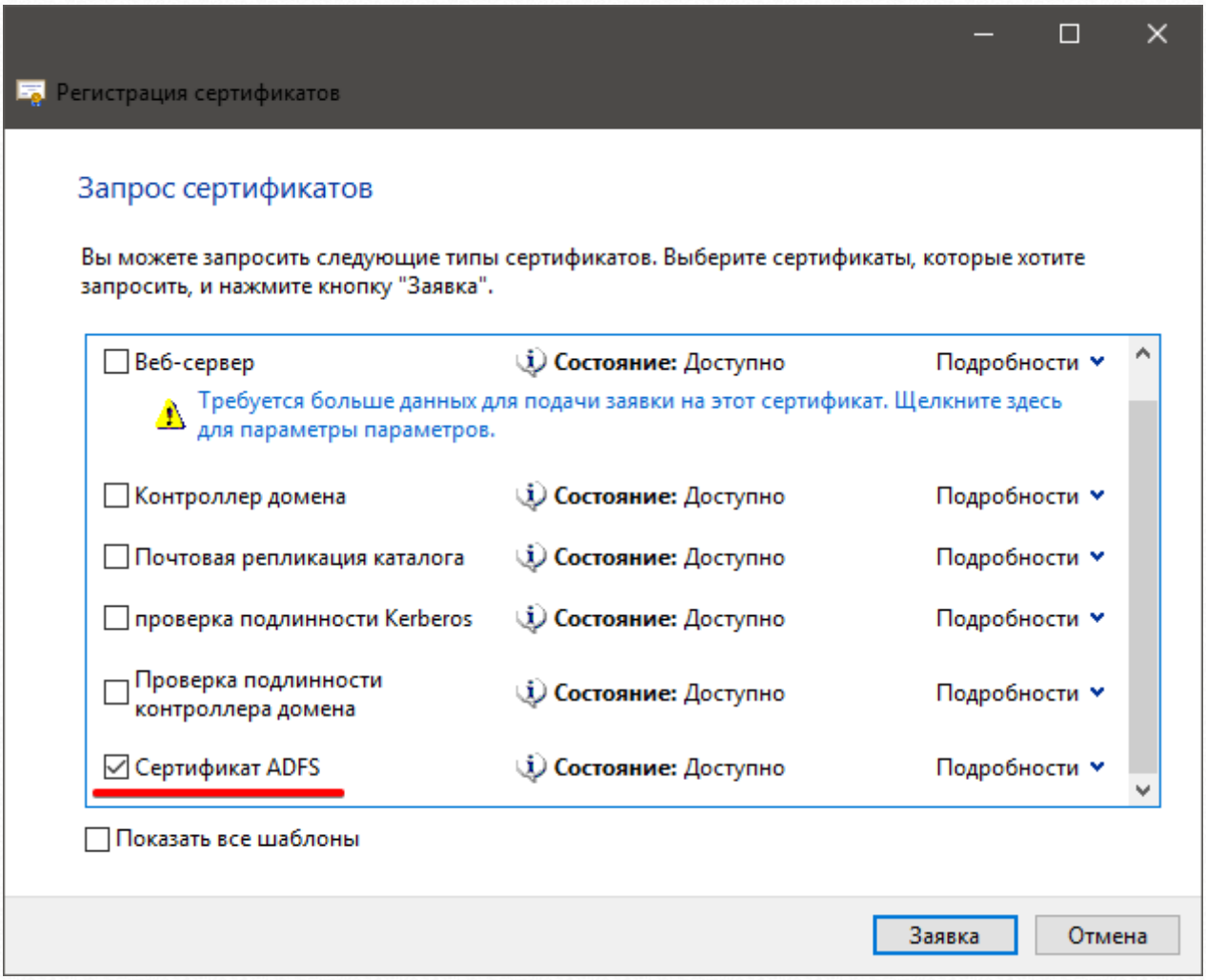
18. В окне «Параметры просмотра» в области «Режим просмотра» выберите пункт «по назначению» и нажмите кнопку «ОК».



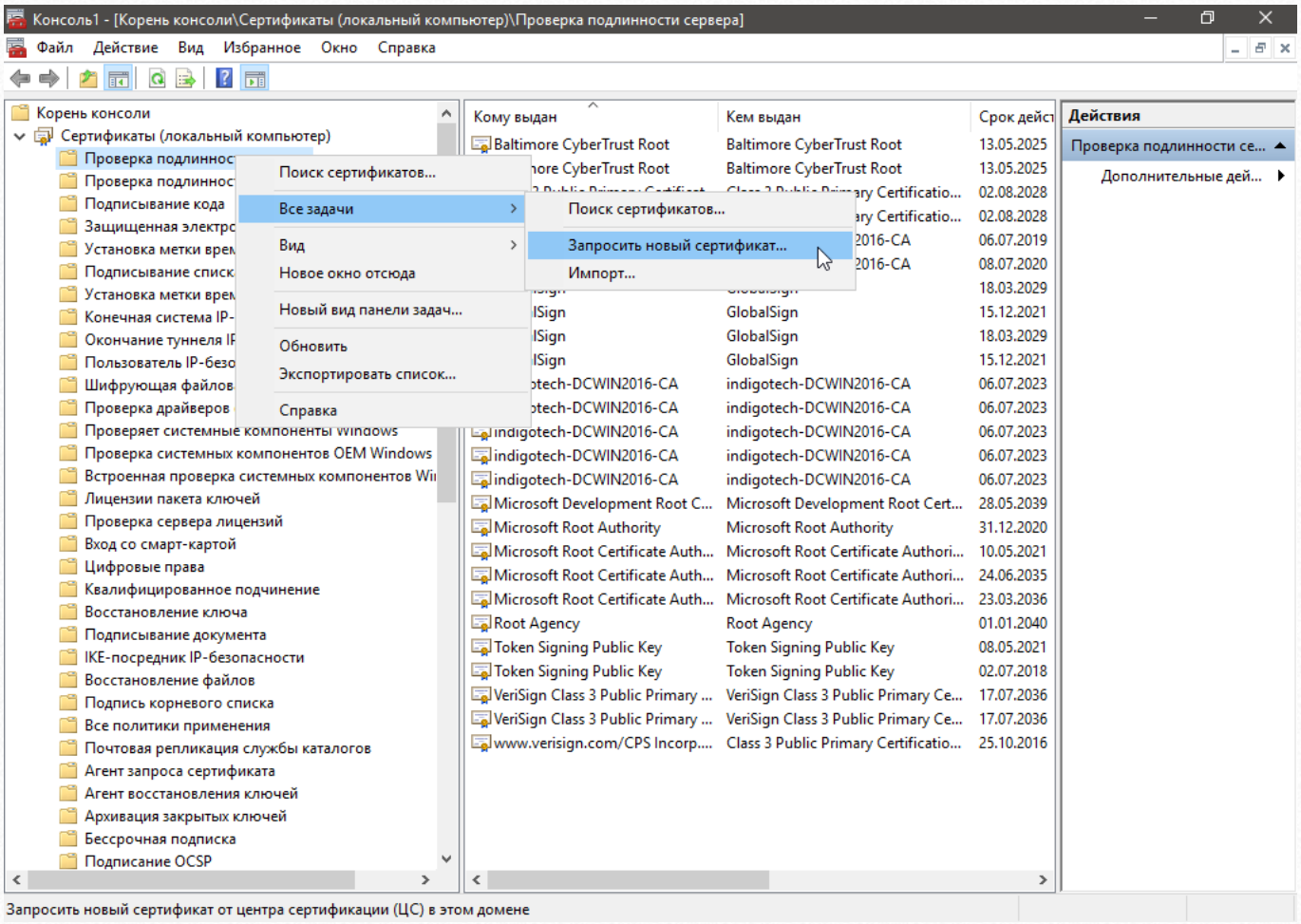
19. В дереве кликните правой кнопкой мыши по группе «Проверка подлинности сервера» и выберите пункт «Все задачи» → «Запросить новый сертификат...».



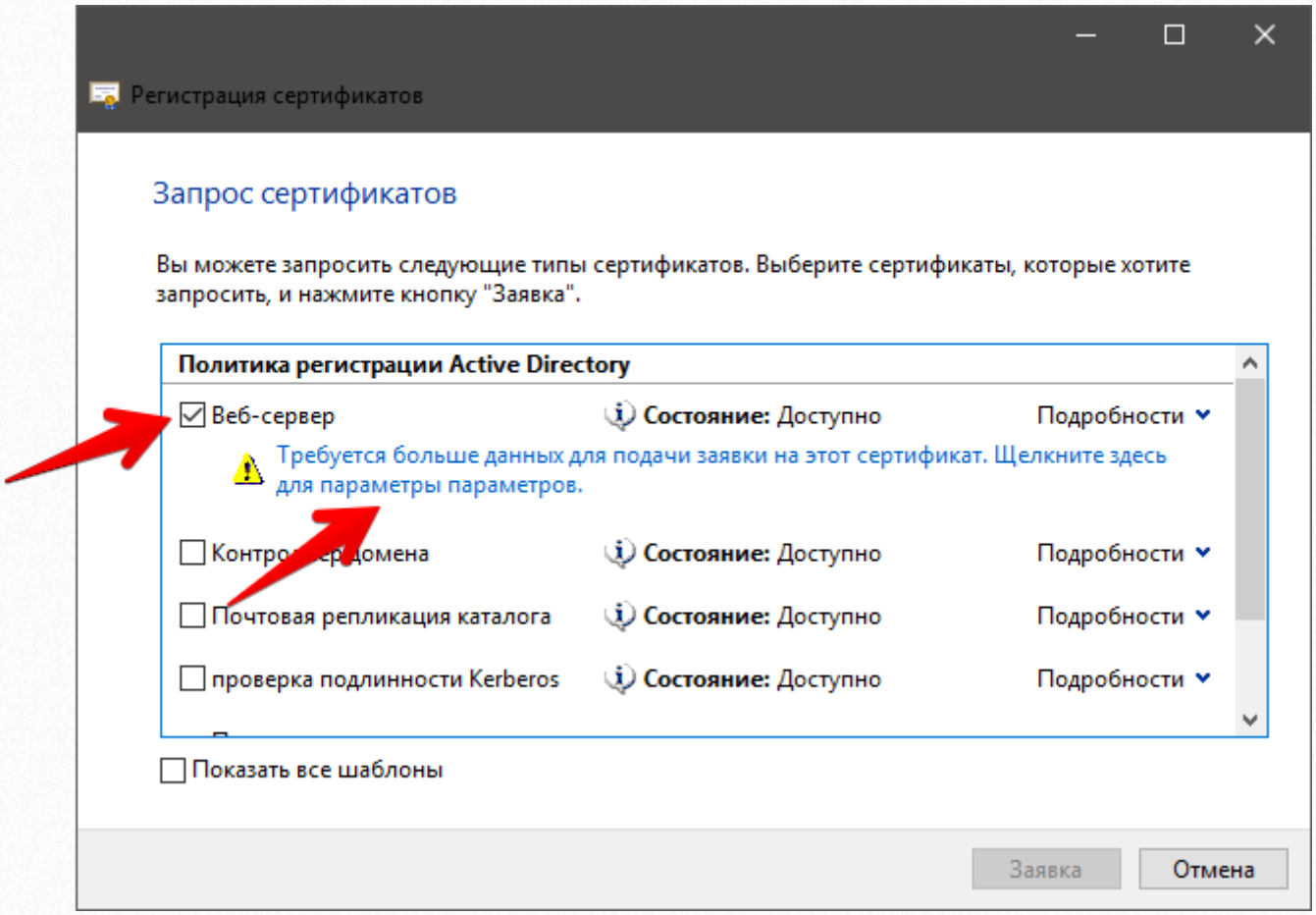
20. В окне «Регистрация сертификатов» на первом шаге «Перед началом работы» нажимаем «Далее».
21. На следующем шаге «Выбор политики регистрации сертификатов» также нажимаем кнопку «Далее».
22. На шаге «Запрос сертификатов» в списке «Политика регистрации Active Directory» отмечаем флажком, созданный ранее шаблон «Сертификат ADFS». И нажимаем кнопку «Заявка».



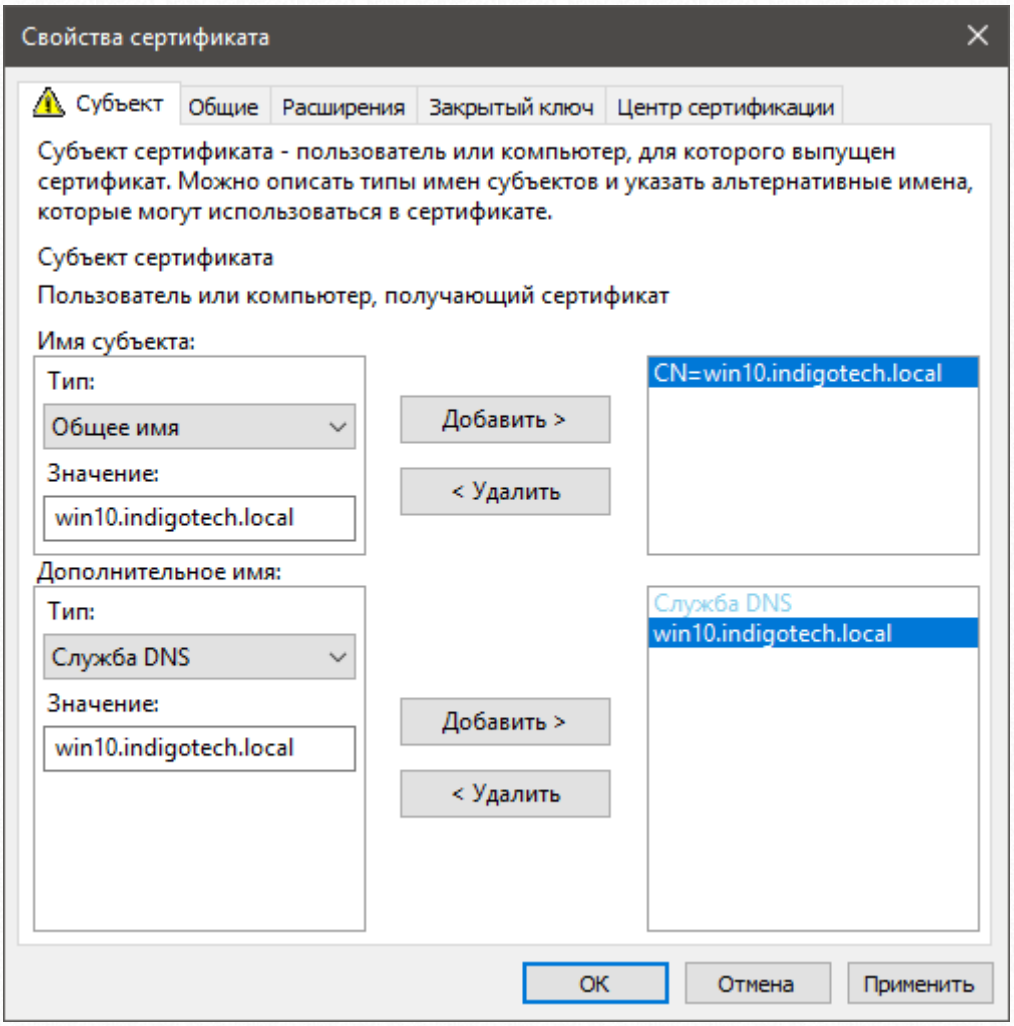
23. Для работы бесшовной авторизации необходимо, чтобы веб-приложение работало по защищенному протоколу (HTTPS). Для этого необходимо создать сертификат для веб-сервера системы тестирования «INDIGO». Вернемся в консоль управления сертификатами и кликнем правой кнопкой мыши по группе «Проверка подлинности сервера» и в меню выберите «Все задачи» → «Запросить новый сертификат...»



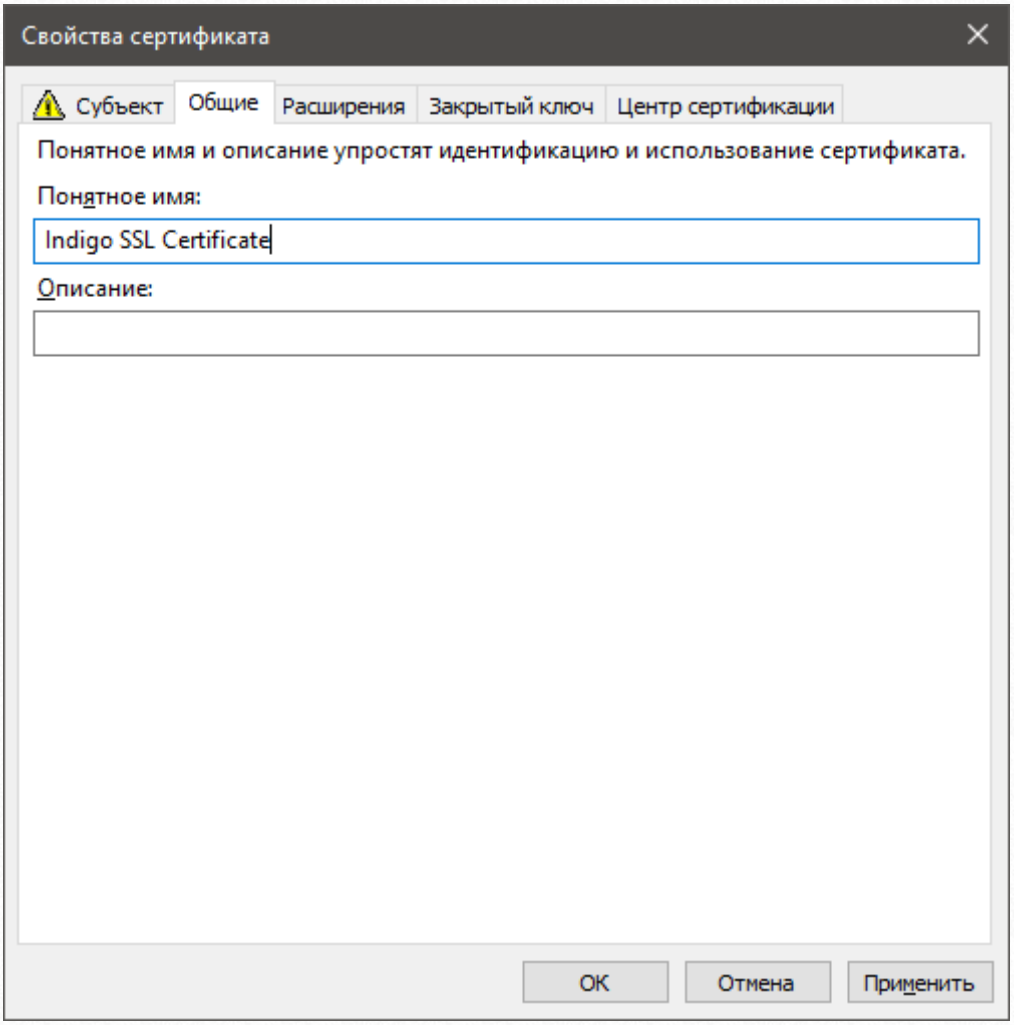
24. В окне «Регистрация сертификатов» на первой вкладке «Перед началом работы» нажмите «Далее».
25. На следующем шаге «Выбор политики регистрации сертификатов» нажмите «Далее».
26. На шаге «Запрос сертификатов» поставьте флажок на пункте «Веб-сервер» и кликните по ссылке «Требуется больше данных для подачи заявки на этот сертификат».



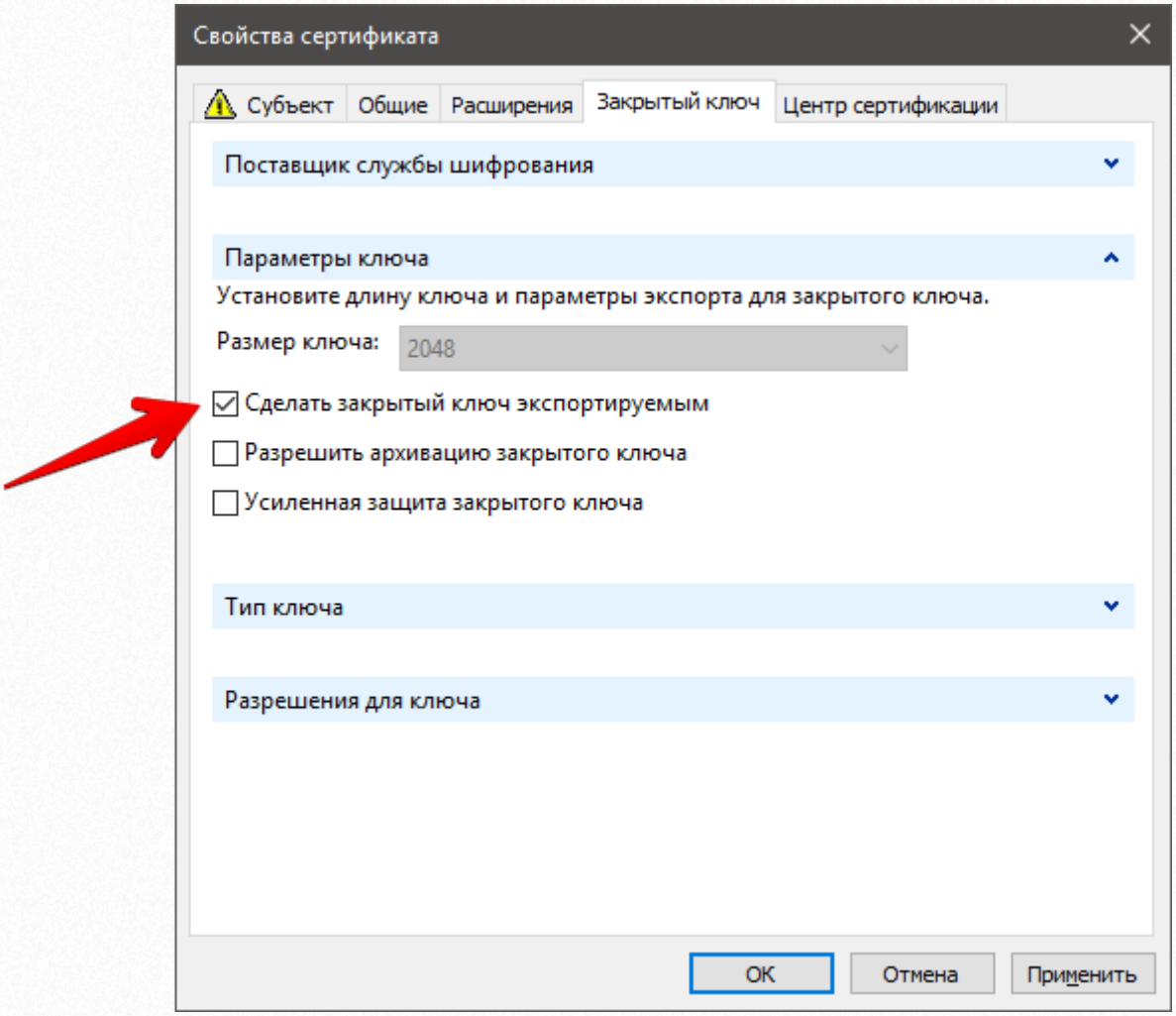
27. В окне «Свойства сертификата» на вкладке «Субъект» в поле «Имя субъекта» выберите из списка тип «Общее имя» и в поле значение напишите полное имя компьютера, на котором установлена система тестирования (с указанием домена), например, в нашем случае win10.indigotech.local и нажмите кнопку «Добавить». В поле «Дополнительное имя» в списке тип выберите «Служба DNS» и в поле значение также впишите полное имя сервера и нажмите «Добавить».



28. На вкладке «Общие» введите в поле «Понятное имя», наименование сертификата для удобства, например, Indigo SSL Certificate.

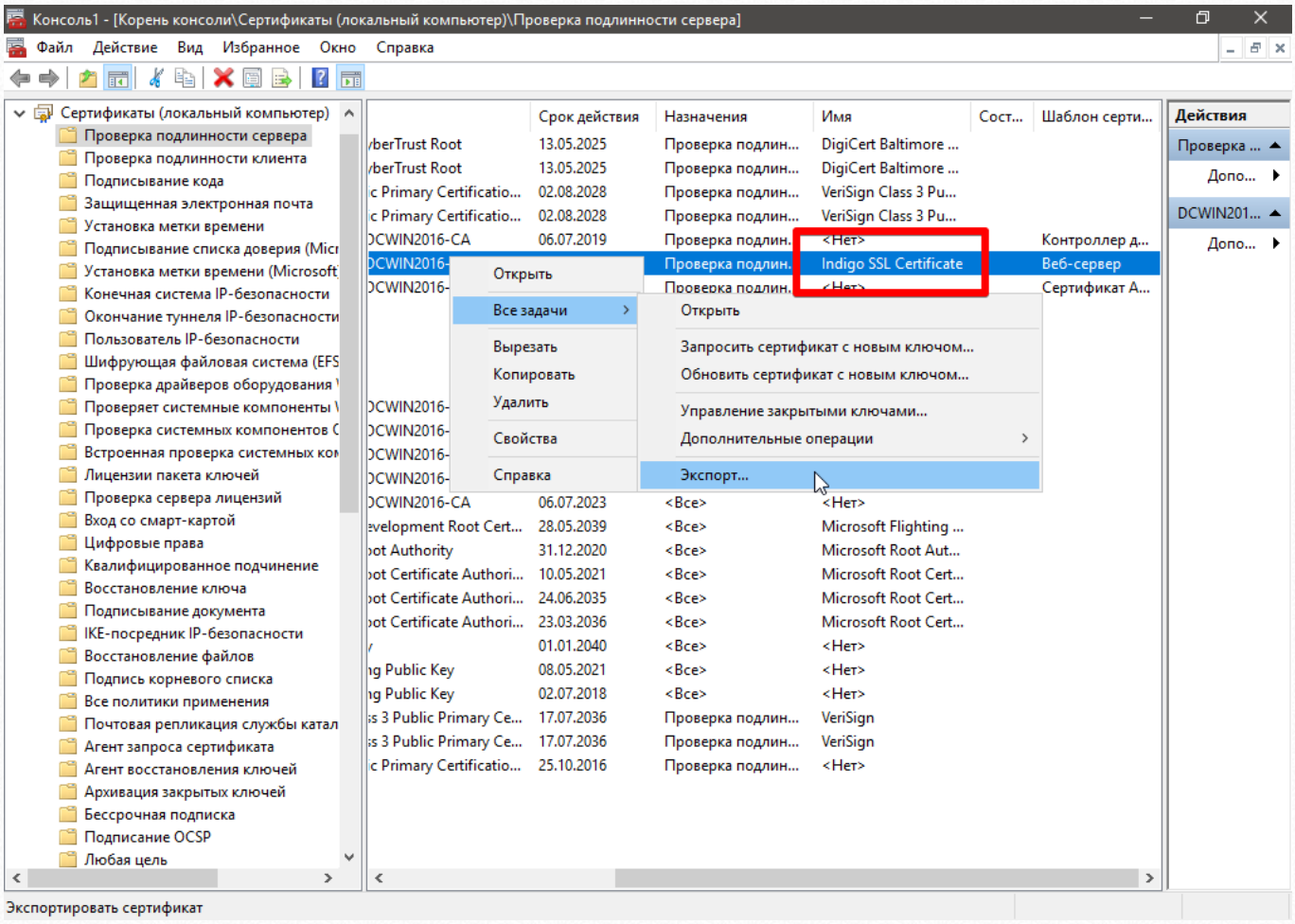


29. На вкладке «Закрытый ключ» в области «Параметры ключа» поставьте галочку «Сделать закрытый ключ экспортируемым». И нажмите «ОК».

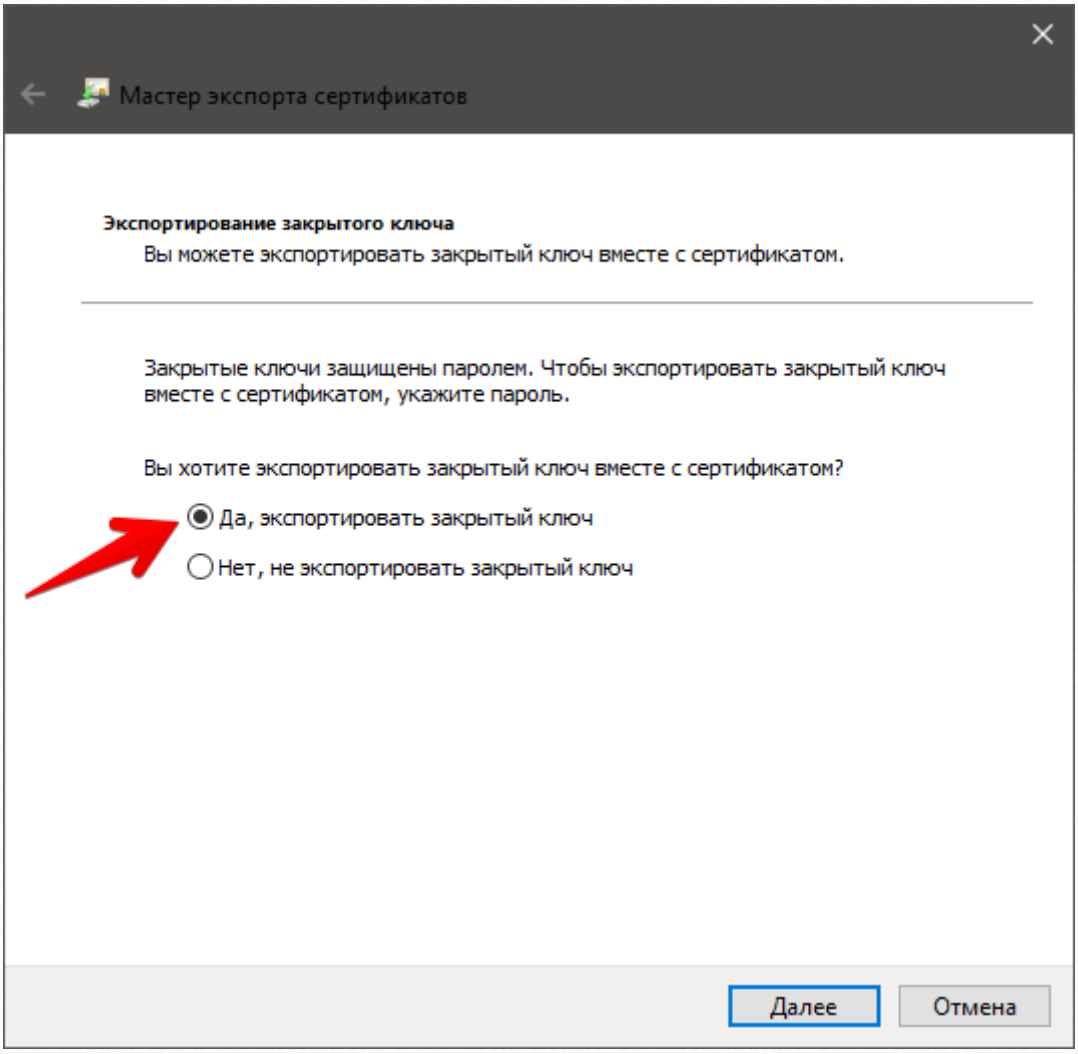


30. Вернувшись в окно «Регистрация сертификатов» нажмите кнопку «Заявка». И далее в окне «Результаты установки сертификатов» нажмите «Готово».

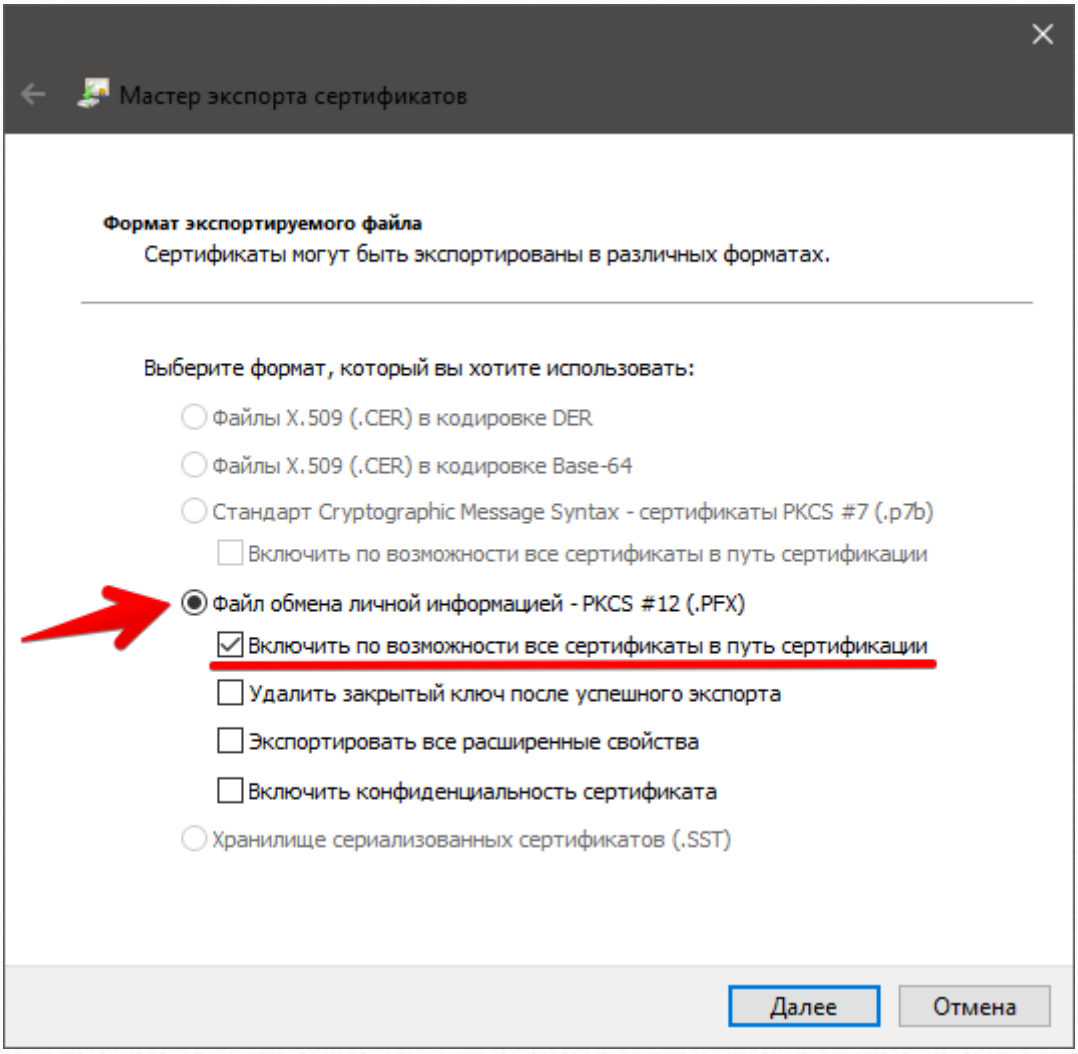
31. Теперь в консоли сертификатов в группе «Проверка подлинности сервера» появится созданный сертификат. Выберите его из списка и нажмите по нему правой кнопкой мыши, а затем в меню выберите пункт «Все задачи» → «Экспорт...»



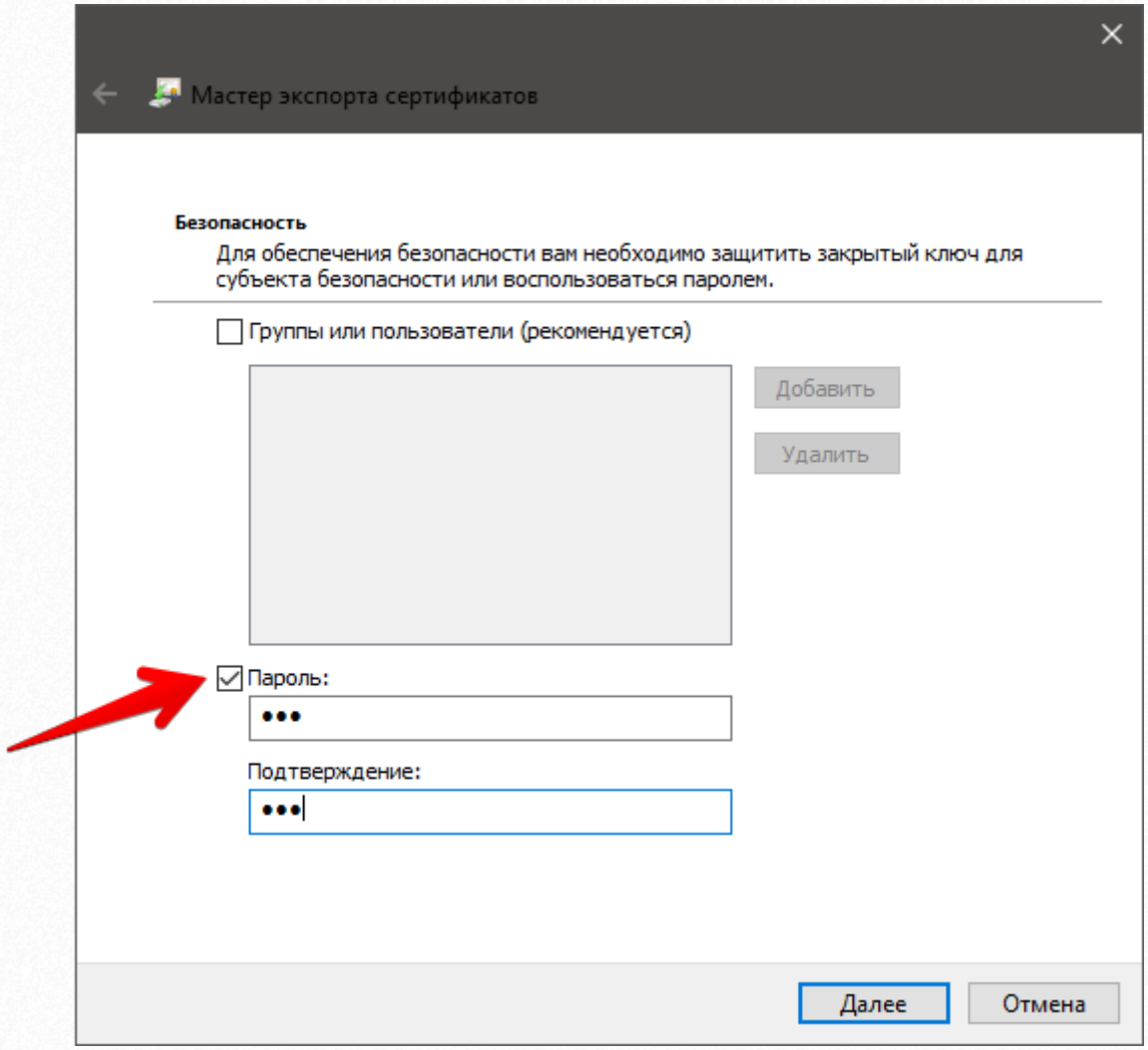
32. В открывшемся окне «Мастер экспорта сертификатов» нажимаем кнопку «Далее».
33. В шаге «Экспортирование закрытого ключа» делаем выбор на пункте «Да, экспортировать закрытый ключ» и нажимаем «Далее».



34. В шаге «Формат экспортируемого файла» выбираем «Файл обмена личной информацией – PKCS #12 (.PFX)» и поставьте флаг «Включить по возможности все сертификаты в путь сертификации» и нажимаем кнопку «Далее».



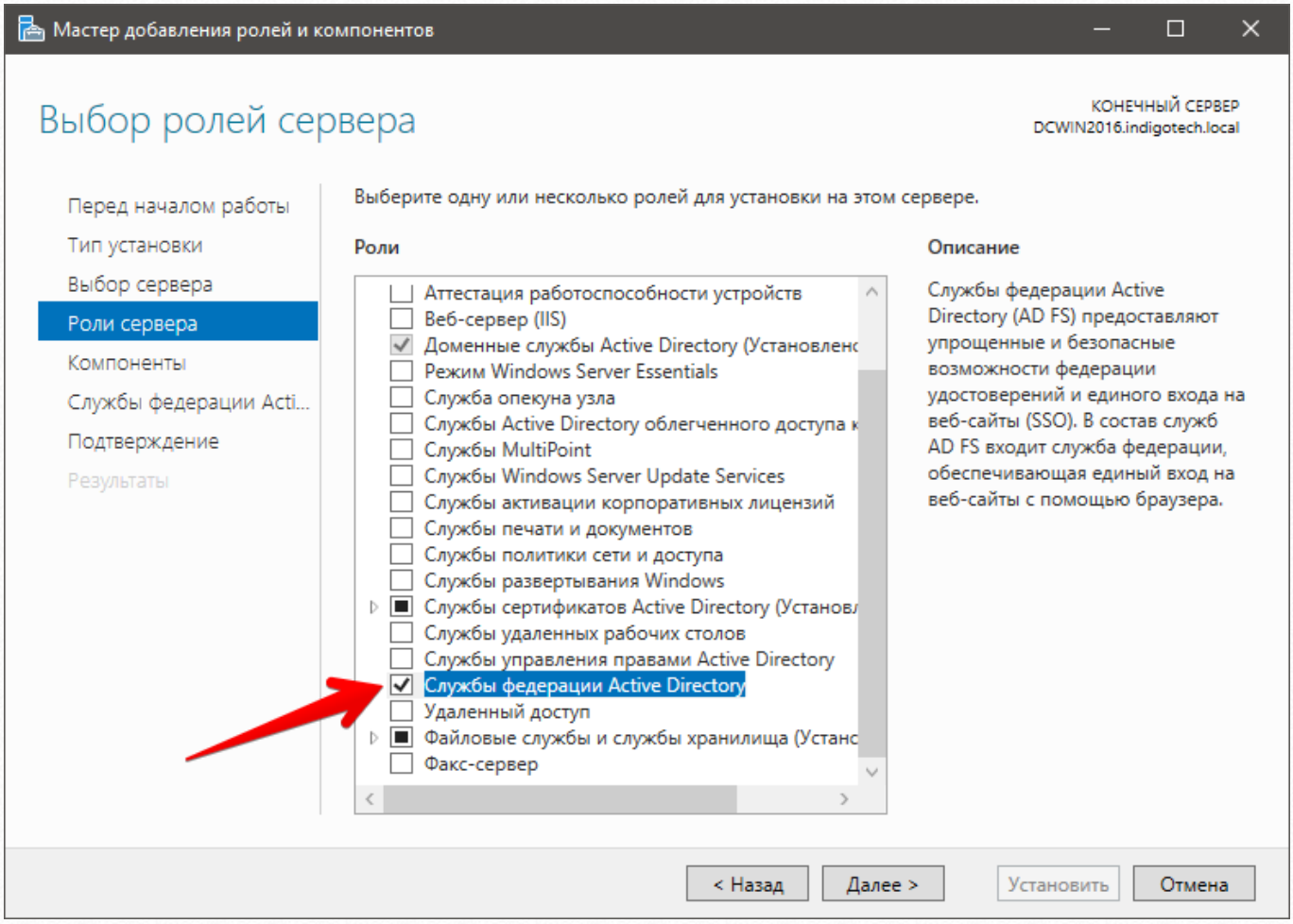
35. На шаге «Безопасность» ставим галочку на пункте «Пароль» и вводим простой пароль в поля «Пароль» и «Подтверждение», например, «123» и нажимаем «Далее».



36. Далее на шаге «Имя экспортируемого файла» укажите путь, куда будет сохранён файл сертификата и нажмите «Далее». И на завершающем шаге нажмите «Готово».

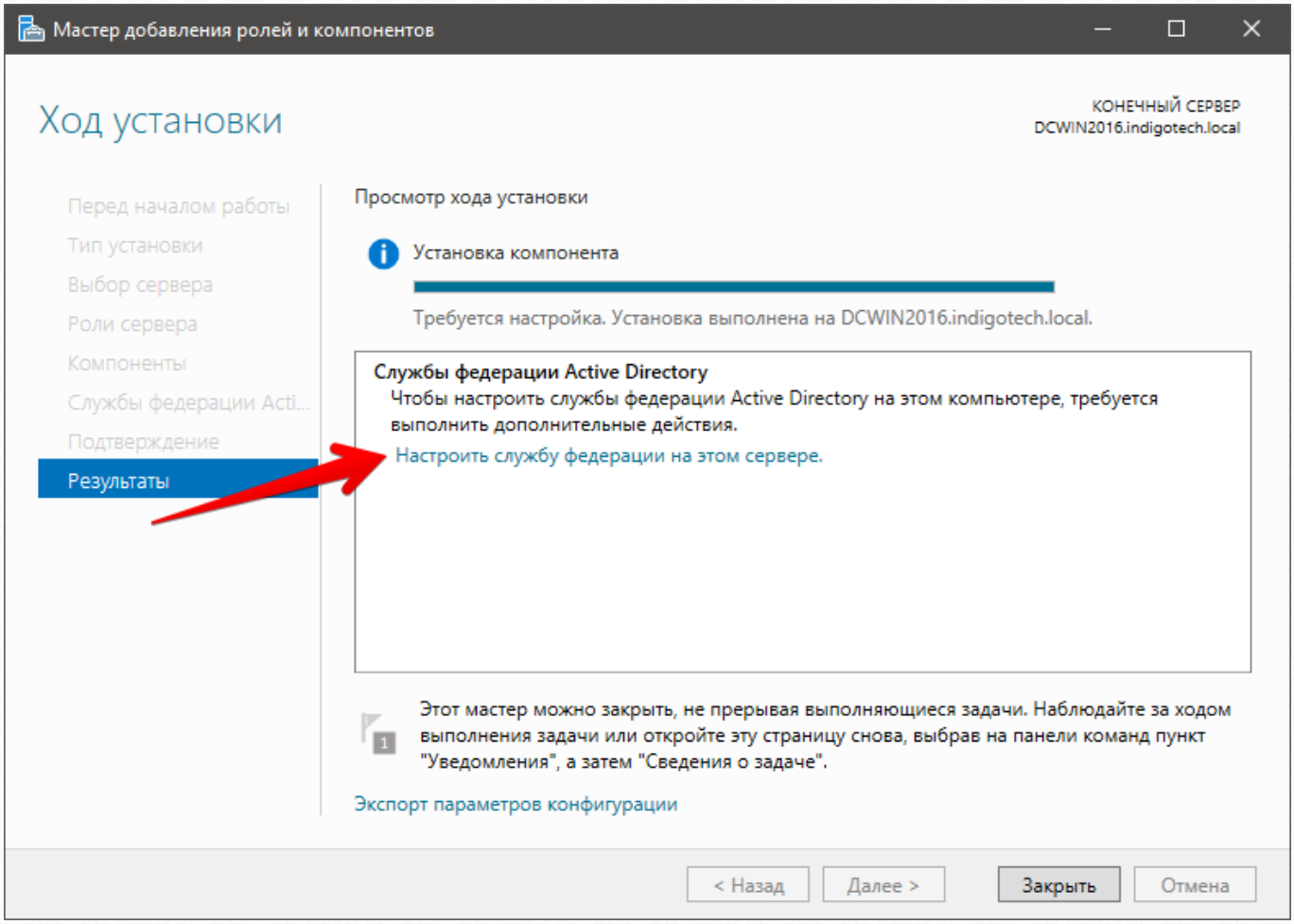
2.2.3. Установка служб федерации Active Directory

1. После создания сертификата можно приступить к добавлению роли «Службы федерации Active Directory» для этого в окне «Диспетчер серверов» выбираем пункт меню «Управление» → «Добавить роли и компоненты».
2. На вкладке «Тип установки» как и ранее выбираем «Установка ролей или компонентов» и жмем кнопку «Далее».
3. На вкладке «Выбор сервера» выбираем наш сервер и жмем кнопку «Далее».
4. На вкладке «Роли сервера» в списке «Роли» установите флажок на пункте «Службы федерации Active Directory».

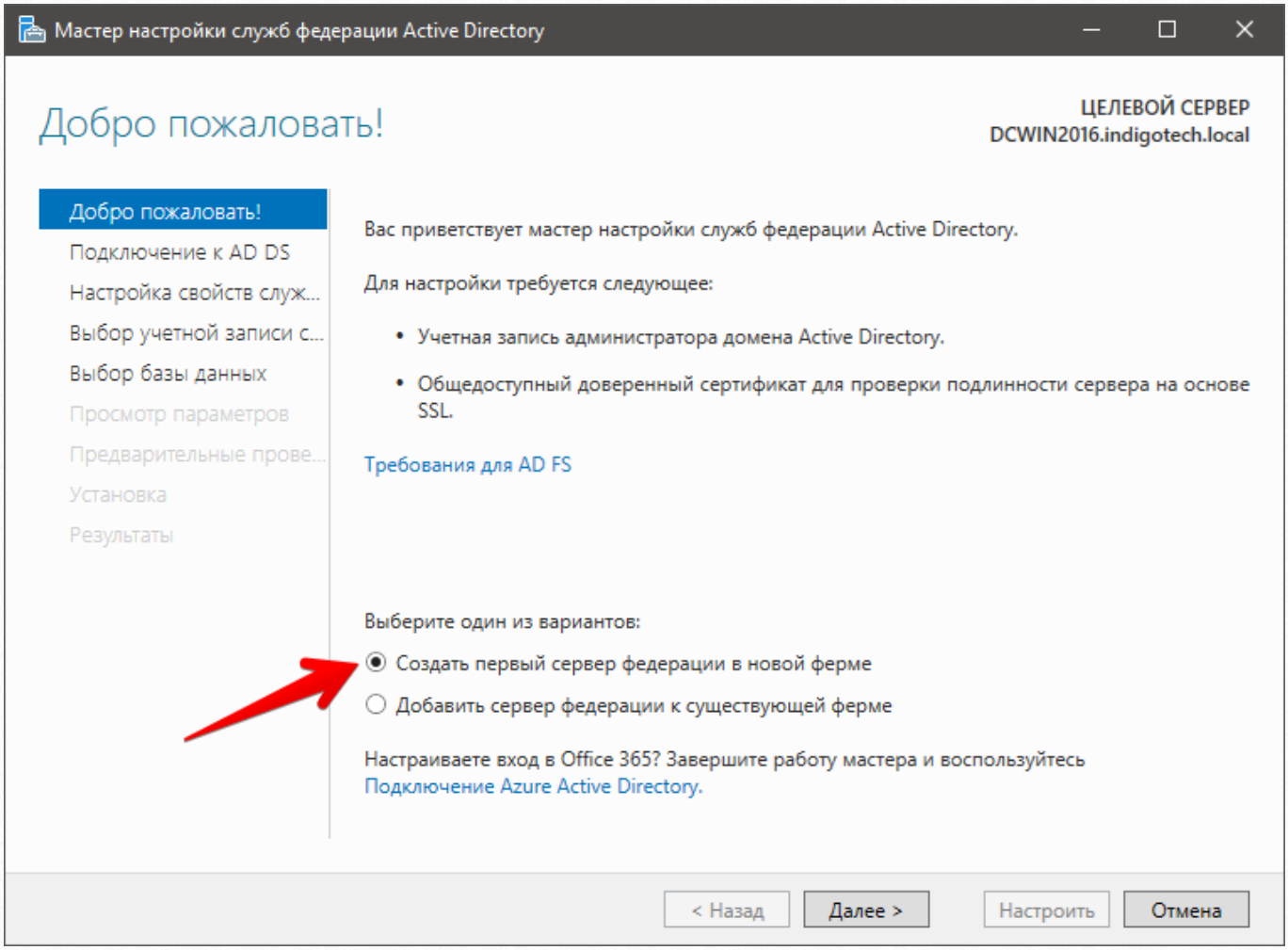


5. На вкладке «Компоненты» жмем кнопку «Далее».
6. На вкладке «Службы федерации Active Directory (AD FS)» также жмем кнопку «Далее».
7. На вкладке «Подтверждение» нажимаем кнопку «Установить».

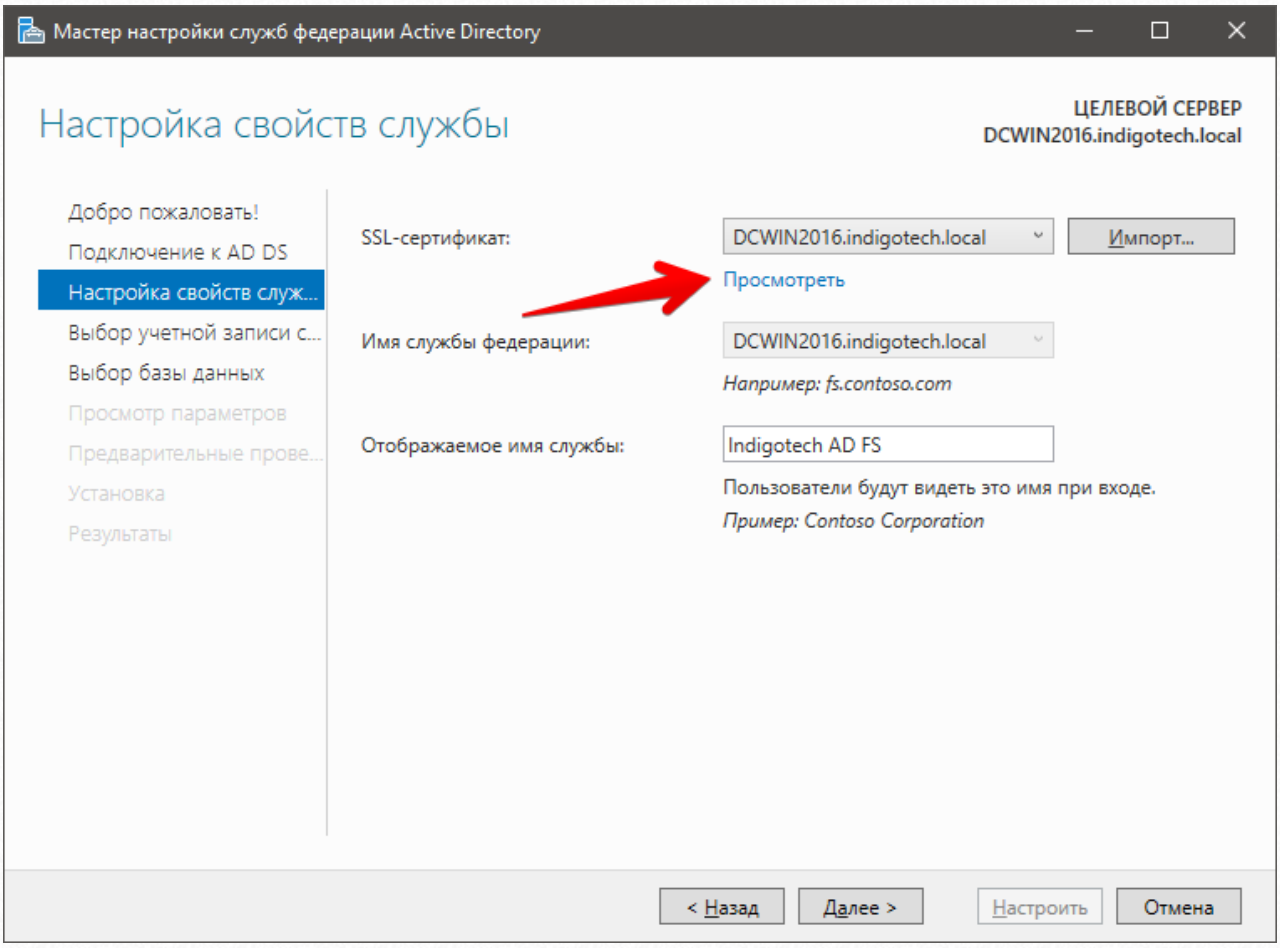
8. После успешной установки нажмите на ссылку «Настроить службу федерации на этом сервере».

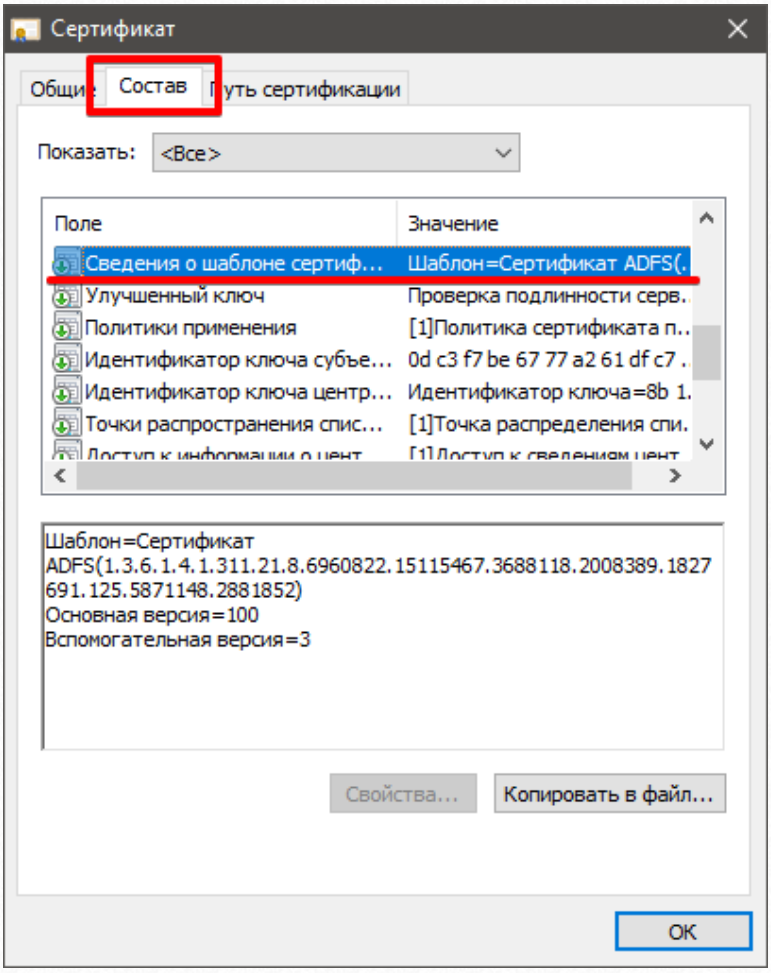


9. На первой вкладке «Добро пожаловать!» в окне «Мастер настройки служб федерации Active Directory» выбираем пункт «Создать первый сервер федерации в новой ферме» и нажимаем кнопку «Далее».



10. На вкладке «Подключение к AD DS» укажите учетную запись с разрешениями администратора домена. Если Вы выполняете установку от администратора, то текущий пользователь выберется автоматически. Нажмите кнопку «Далее».
11. На вкладке «Настройка свойств службы» из выпадающего списка «SSL-сертификат» выберите созданный заранее сертификат, а в поле «Отображаемое имя службы» впишите наименование вашей организации, например. В нашем случае это наименование нигде отображаться не будет.
12. Важно убедиться, что был выбран правильный сертификат. Для этого нажмите на ссылку «Просмотреть» и в окне «Сертификат» на вкладке «Состав» найдите поле «Сведения о шаблоне сертификата» и убедитесь, что в значении присутствует название шаблона «Сертификат ADFS».

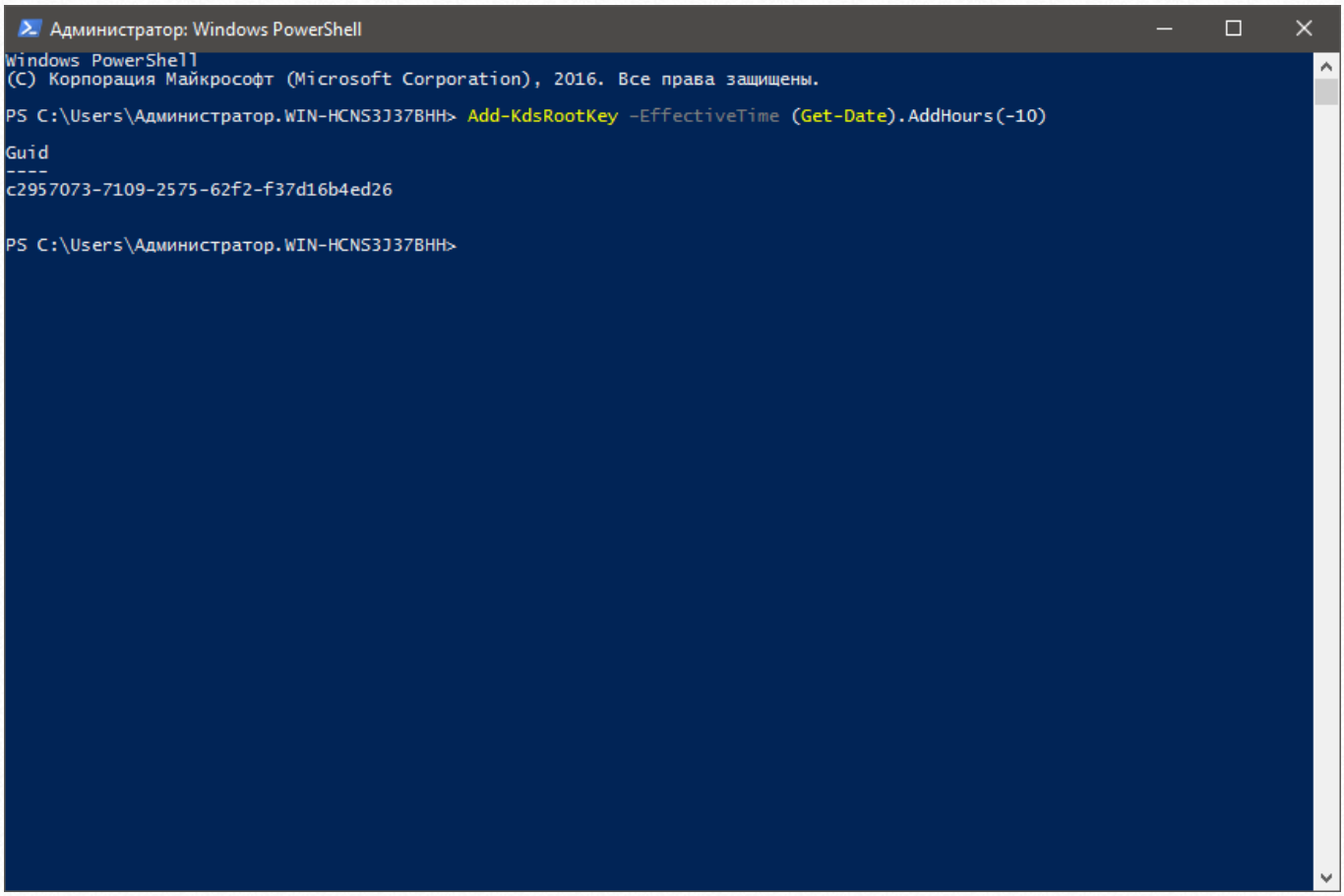




13. На следующей вкладке «Выбор учетной записи службы» необходимо выбрать пользователя, от имени которого будет запускаться служба федерации, поэтому необходимо создать нового пользователя. Для этого с помощью меню «Пуск» запустите Windows Power Shell.

14. Контроллеру домена необходим корневой ключ для создания паролей групповой управляемой учетной записи. Контроллеры домена будут ожидать до 10 часов с момента создания, чтобы все второстепенные контроллеры, выполнили слияние своих репликаций AD перед тем, как выдать разрешение на создание групповой управляемой учетной записи. 10 часов — это мера безопасности для предотвращения ситуации, когда генерация паролей началась прежде, чем все контроллеры домена в среде смогут ответить на запросы групповой управляемой учетной записи. В средах с одним контроллером домена можно создать корневой ключ KDS и установить начальную дату в прошлом, чтобы избежать периода ожидания для генерирования ключа. Для этого выполните команду:

```
Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)
```



15. Создадим нового пользователя с логином adfsService выполнив команду:

```
New-ADUser -Name adfsService
```

Затем зададим ему пароль командой:

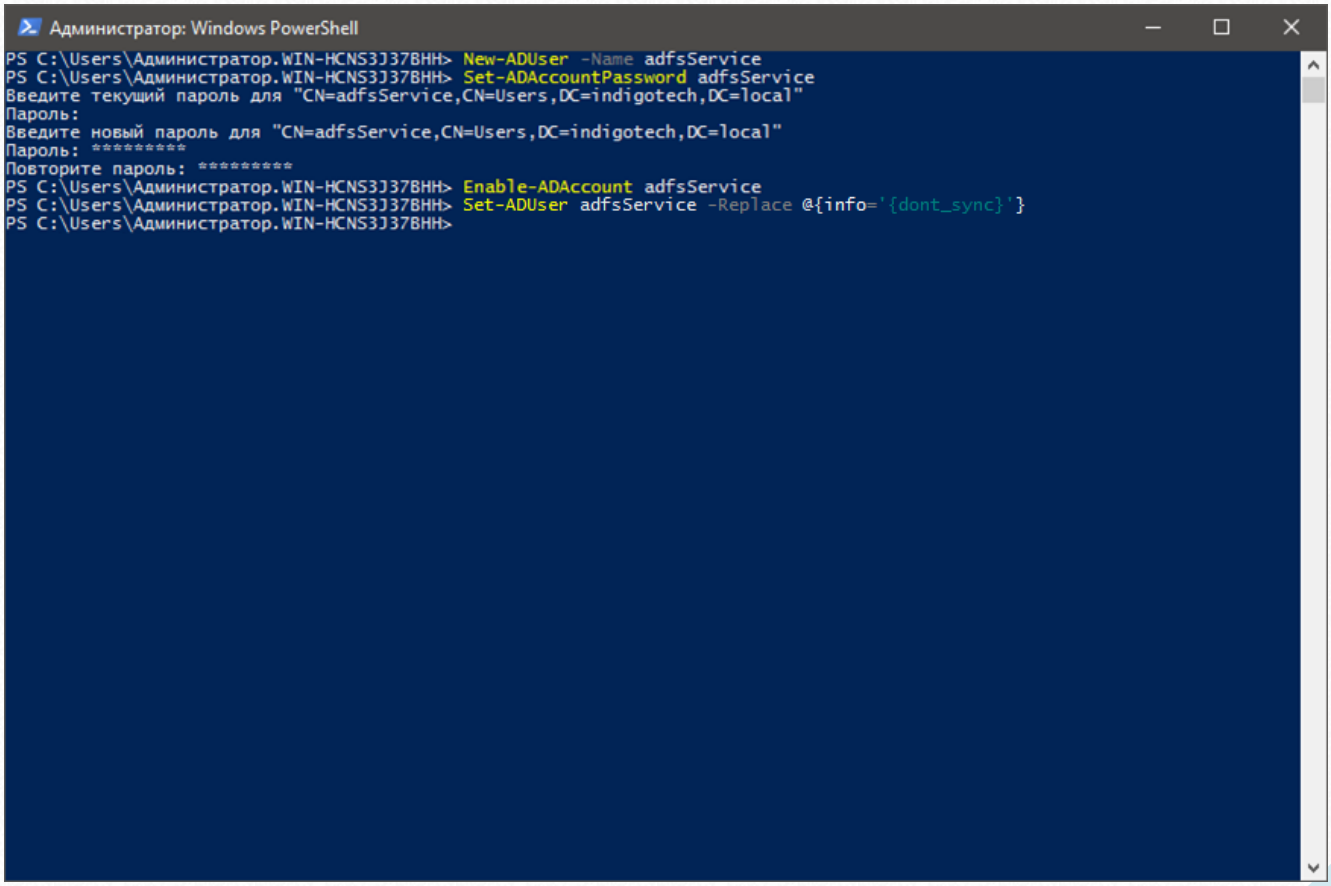
```
Set-ADAccountPassword adfsService
```

На первый запрос «Введите текущий пароль» просто нажимаем «Enter», т.к. мы только что создали этого пользователя и пароля не существует, а затем необходимо ввести пароль дважды, причем пароль должен соответствовать той сложности, которая указана в групповых политиках безопасности. После установки нужно активировать аккаунт выполнив команду:

```
Enable-ADAccount adfsService
```

Для того чтобы созданный пользователь не попал в список синхронизации необходимо добавить специальный маркер «`{dont_sync}`» в его поле «Заметки». Это можно сделать в настройках свойств пользователя в графическом интерфейсе или выполнить команду:

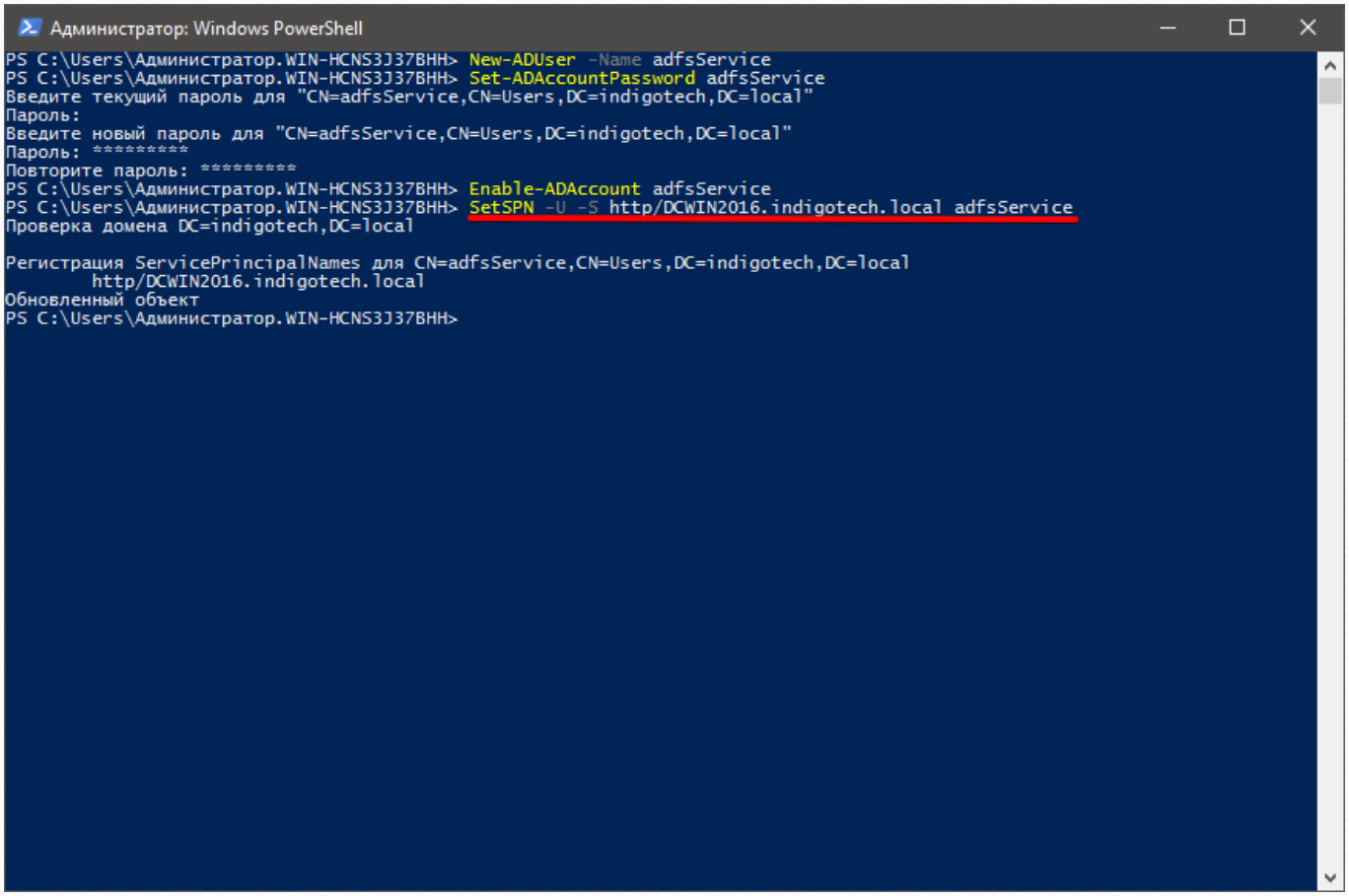
```
Set-ADUser adfsService -Replace @{info='{dont_sync}'}
```



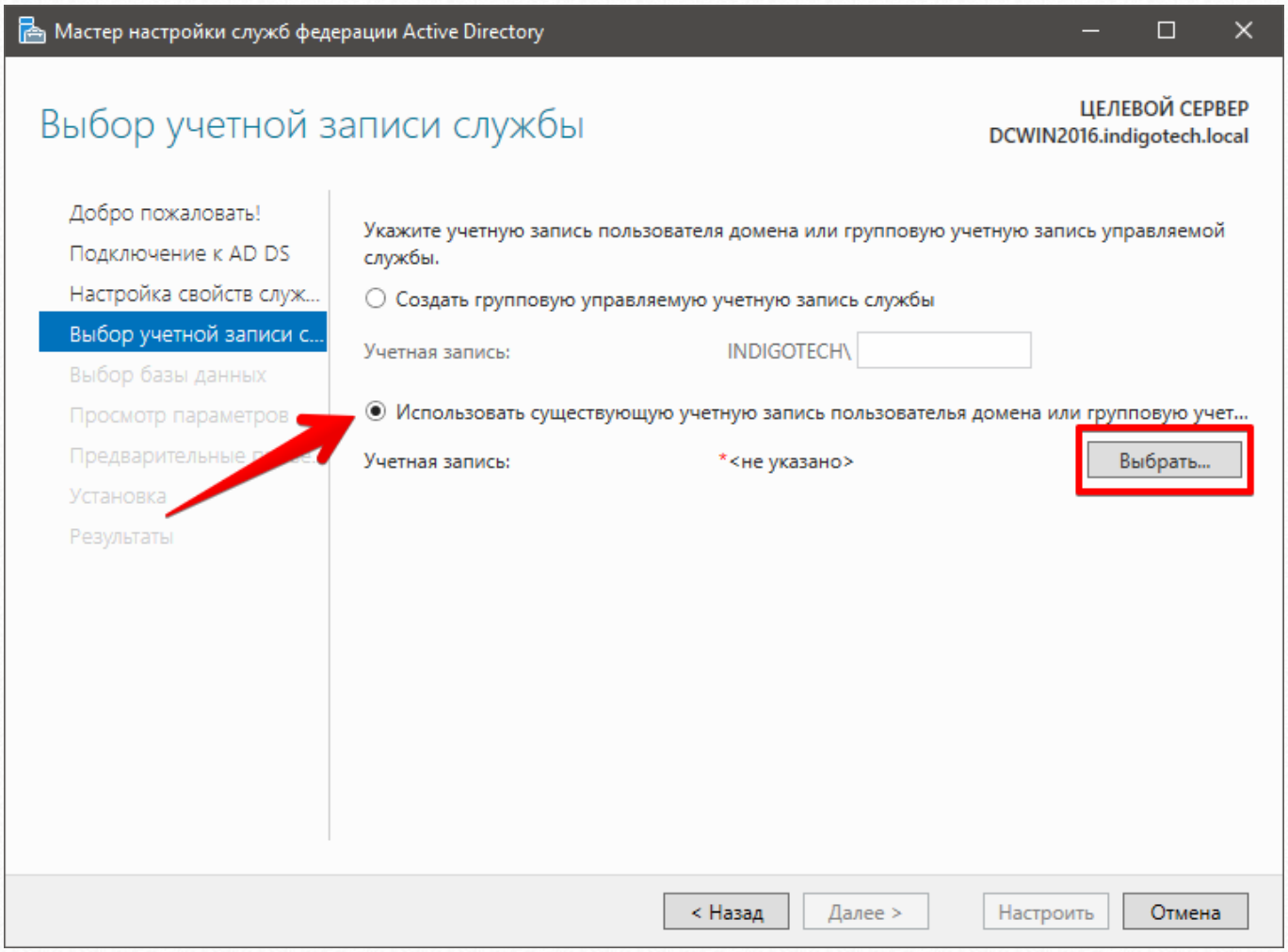
16. Также для корректной работы интегрированной аутентификации Windows необходимо установить Service Principal Name(SPN) для созданной учетной записи. Для этого выполним команду:

```
SetSPN -U -S http/dcwin2016.indigotech.local adfsService
```

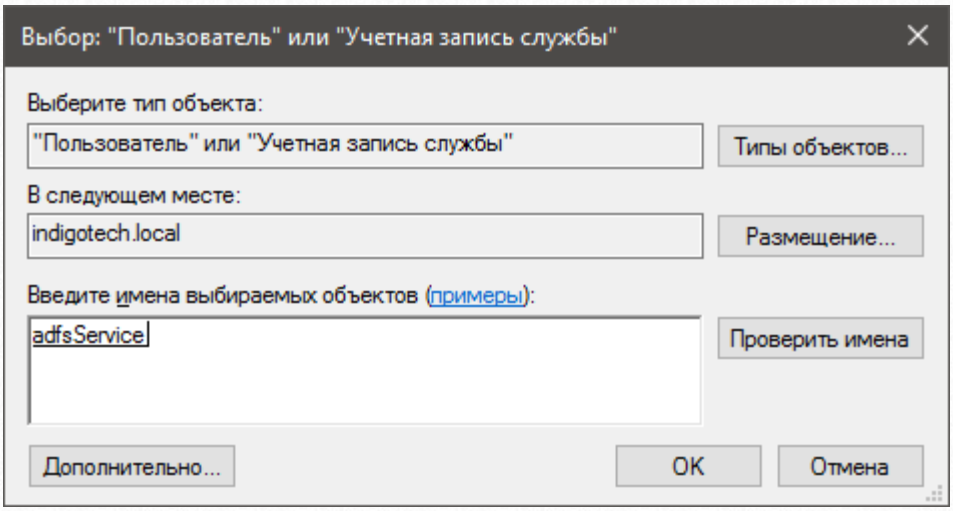
где dcwin2016.indigotech.local – полное имя компьютера, на который была установлена служба федерации Active Directory.



17. На этом настройка учетной записи закончена, вернемся к окну «Мастер настройки служб федерации Active Directory» и поставим выбор на пункт «Использовать существующую учетную запись домена или групповую учетную запись управляемой службы» и нажмем кнопку «Выбрать...»



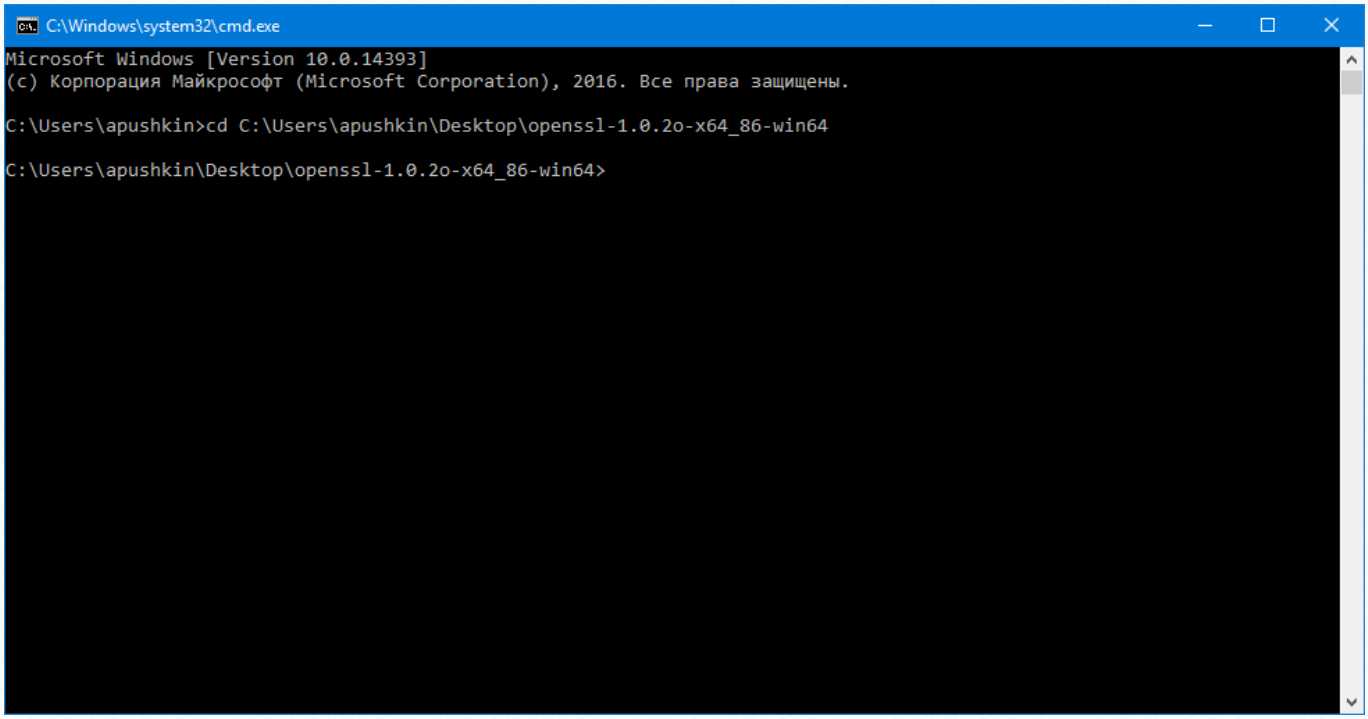
18. В открывшемся окне «Выбор» введите имя созданной учетной записи «adfsService» в поле «Введите имена выбираемых объектов» и нажмите кнопку «Проверить имена». Если все введено правильно, то шрифт в поле станет подчеркнутым. После этого нажмите «ОК».



19. В окне «Мастер настройки служб федерации Active Directory» появится поле «Пароль учетной записи», в которое необходимо ввести пароль, указанный при создании пользователя adfsService. Затем нажмите «Далее».
20. На вкладке «Выбор базы данных конфигурации» выберите «Создать на этом сервере базу данных на основе внутренней базы данных Windows» и нажмите кнопку «Далее».
21. На вкладке «Просмотрите параметры» нажмите «Далее».
22. На вкладке «Предварительные проверки» нажмите кнопку «Настроить».
23. После завершения настройки нажмите кнопу «Закрыть».

2.2.4. Установка сертификатов безопасности в систему тестирования и включение HTTPS протокола

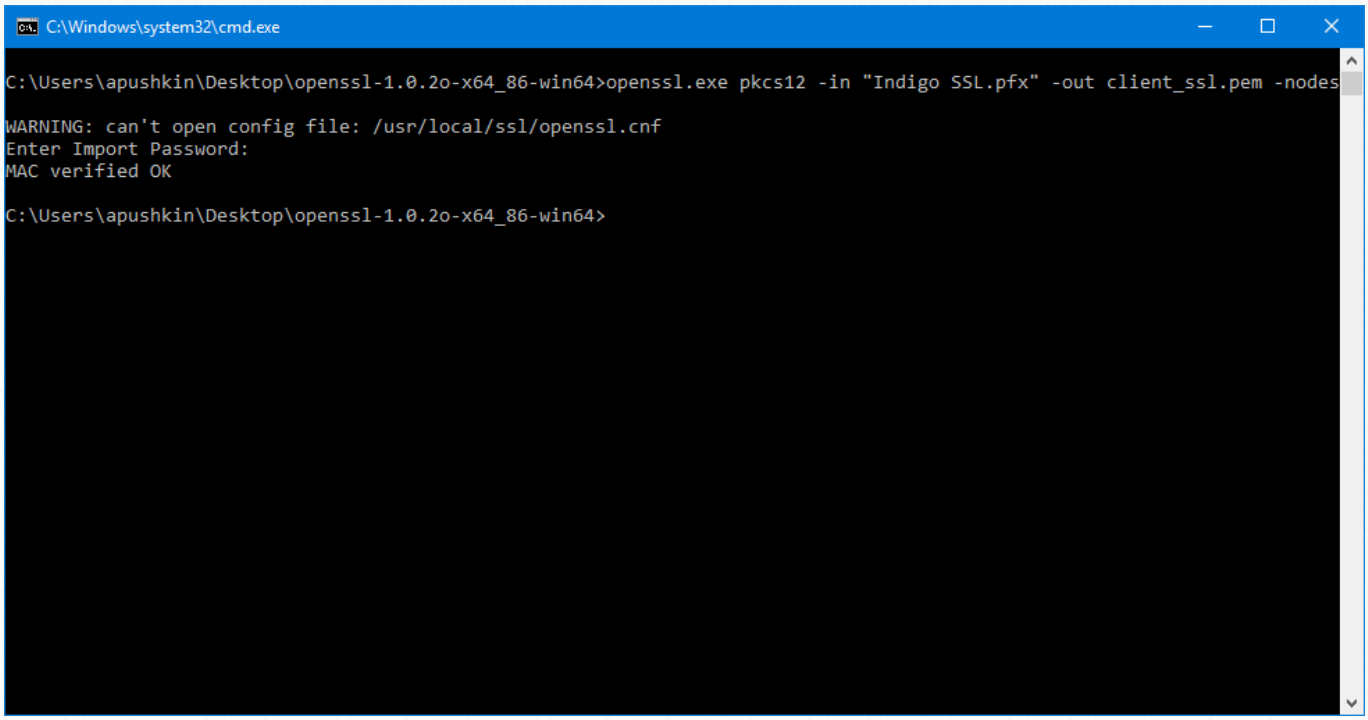
1. На компьютер, где установлена система тестирования «INDIGO», скачайте и распакуйте архив https://indigotech.ru/downloads/files/OpenSSLv1.1.0i.zip и скопируйте в эту папку экспортированный файл сертификата.
2. Откройте командную строку и смените текущий каталог на папку с сертификатом выполнив команду: «cd путь_до_папки».



3. Введите команду

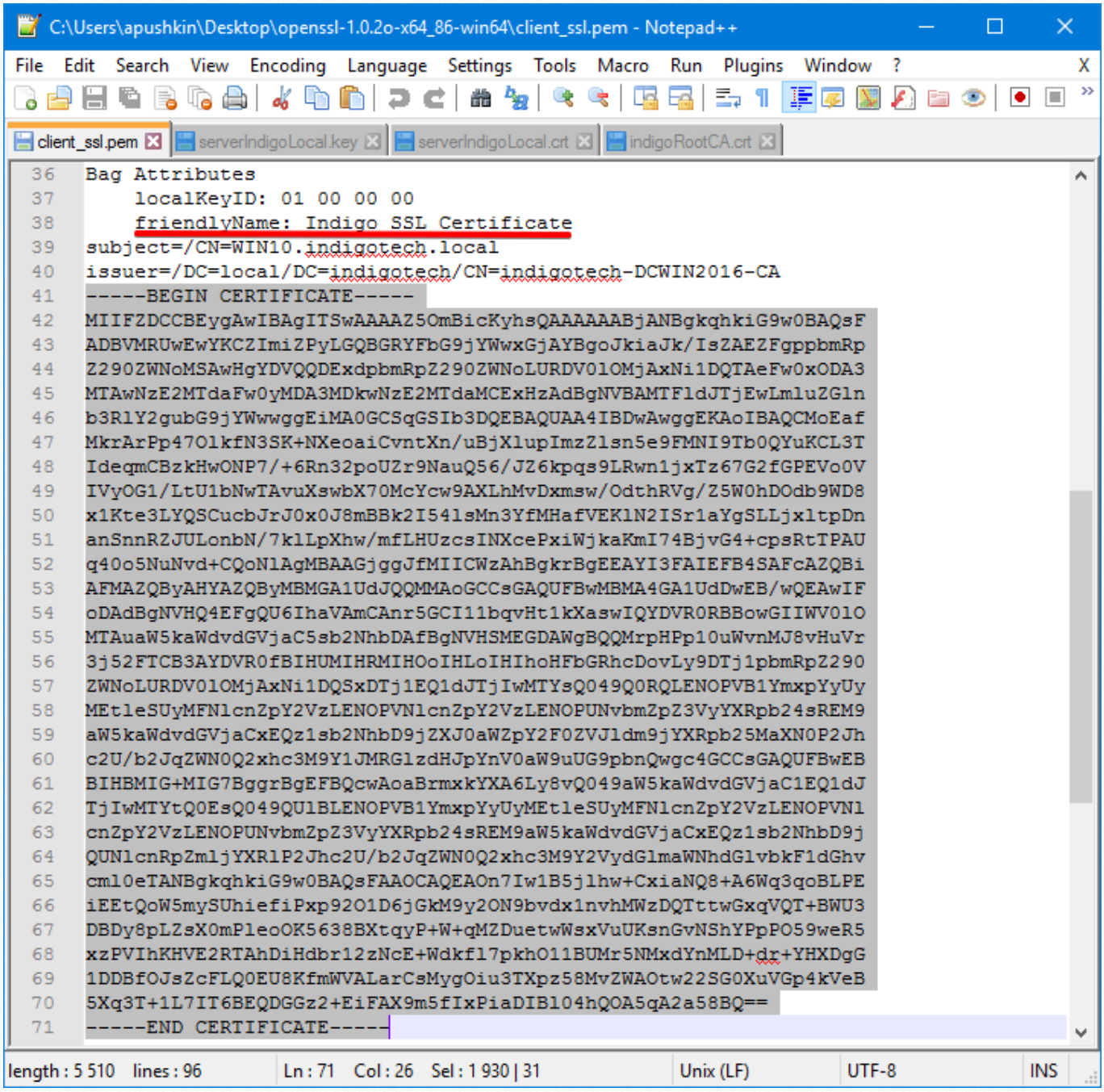
```
openssl.exe pkcs12 -in "имя_файла.pfx" -out client_ssl.pem –nodes
```

и нажмите Enter. На запрос «Enter Import Password:» введите пароль, который Вы вводили во время экспорта закрытого ключа, в нашем случае «123» и нажмите Enter.

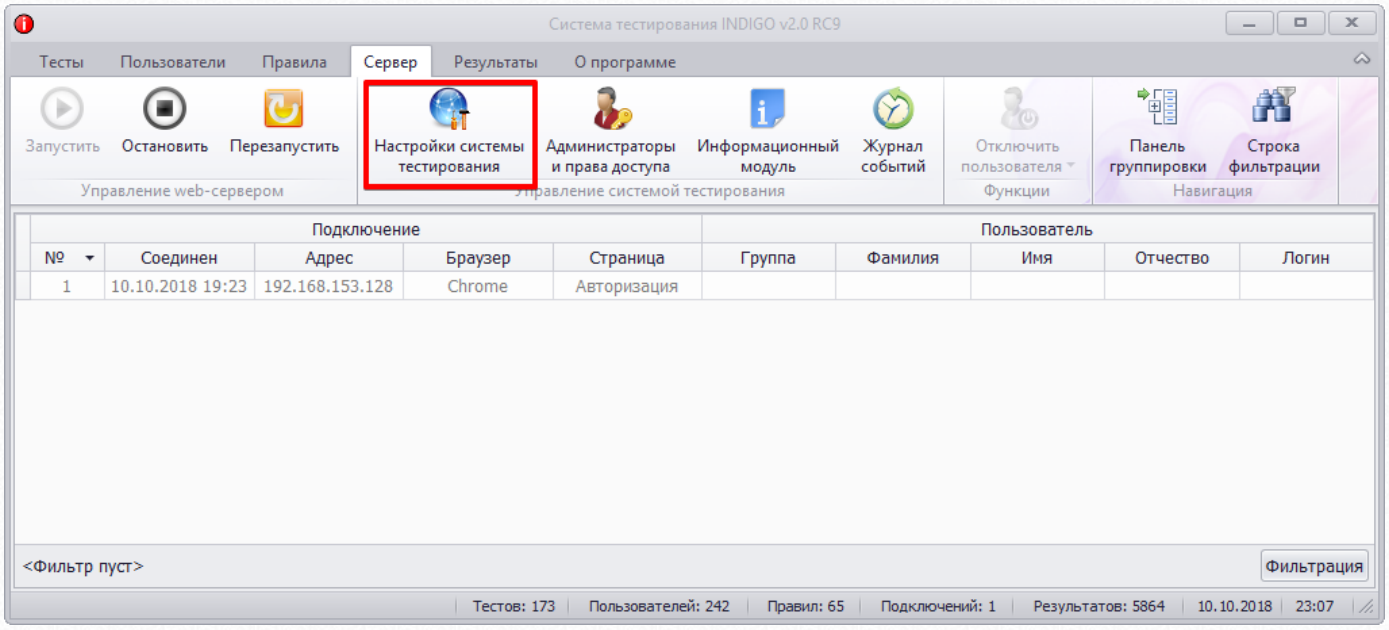


4. В папке с файлом PFX появится файл client_ssl.pem. Откройте его любым текстовым редактором.
5. Необходимо разделить файл на 3 отдельных, для этого скопируйте секцию, начиная с -----BEGIN PRIVATE KEY----- по -----END PRIVATE KEY----- и сохраните файл с названием, например, serverIndigoLocal.key. Это закрытый ключ созданного нами сертификата для веб-сервера системы тестирования.

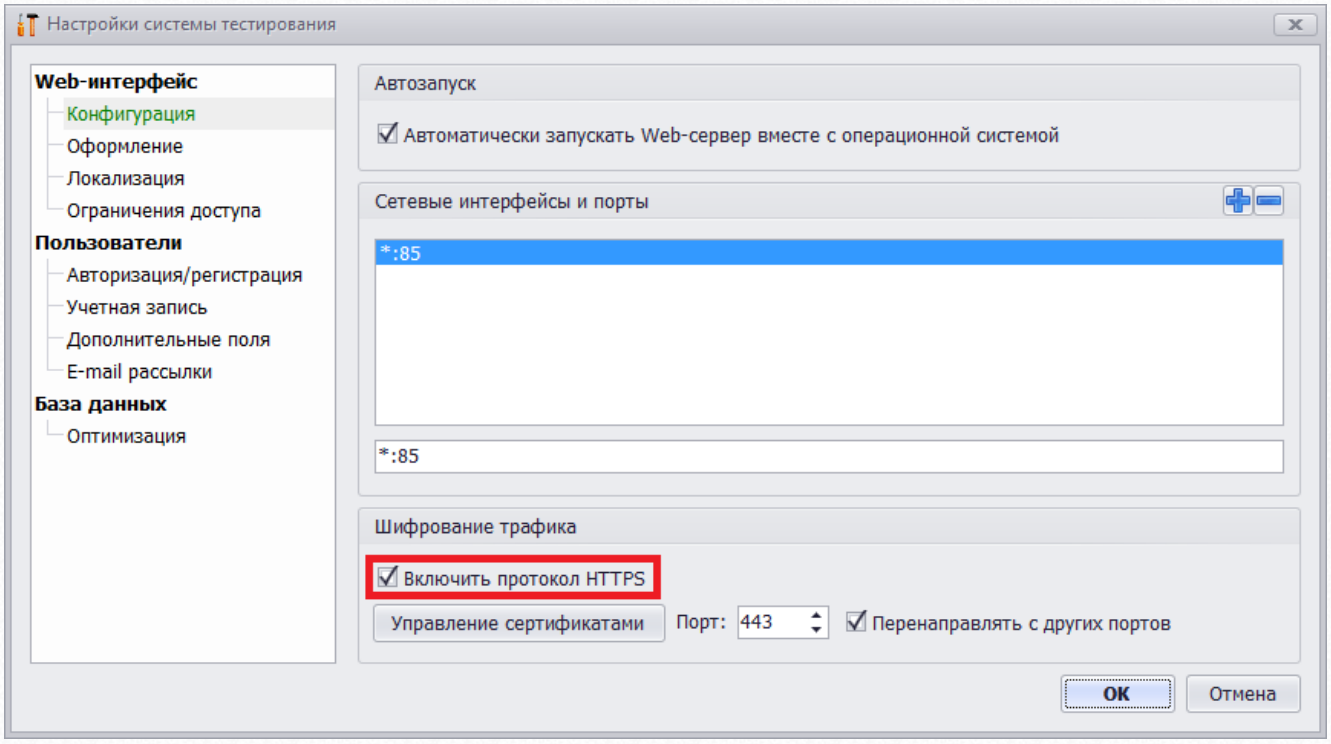
6. Далее две секции помечены одинаково с -----BEGIN CERTIFICATE----- по -----END CERTIFICATE-----. Но у первой в начале описан атрибут «friendlyName» и его значение «Indigo SSL Certificate» - это значит, что эта секция содержит открытый ключ созданного нами сертификата для веб-сервера системы тестирования. Копируем в новый файл и сохраняем с именем serverIndigoLocal.crt



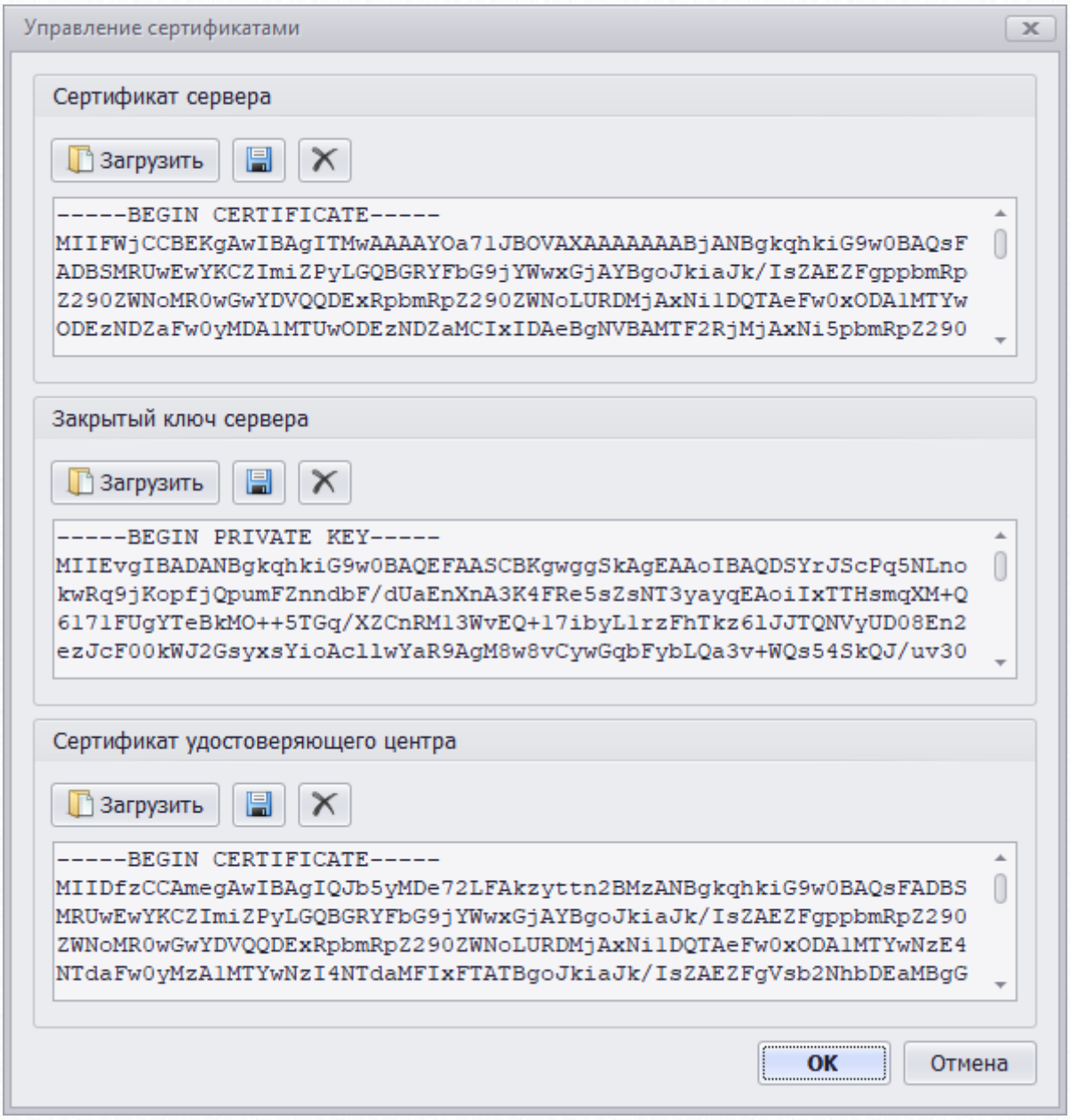
7. И третья секция содержит открытый ключ сертификата центра сертификации. Копируем ее в новый файл и сохраняем с именем indigoRootCA.crt
8. Теперь необходимо включить HTTPS протокол в системе тестирования, для этого в главном окне программы перейдём на вкладку «Сервер» и нажмем кнопку «Настройки системы тестирования».



9. В открывшемся окне «Настройки системы тестирования» установите флажок на пункте «Включить протокол HTTPS», а затем нажмите на кнопку «Управление сертификатами».



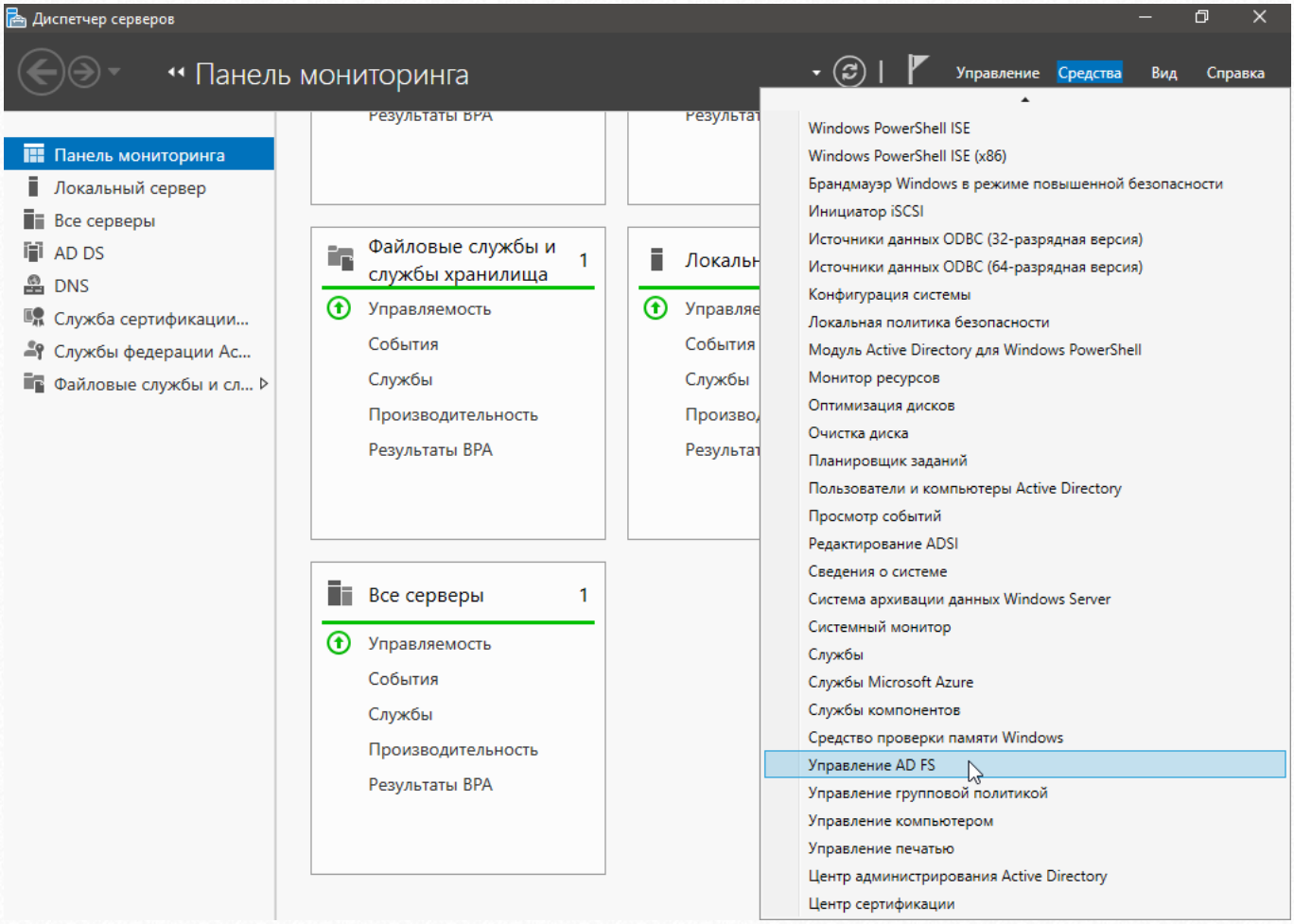
10. В открывшемся окне «Управление сертификатами» в поле «Сертификат сервера» с помощью кнопки «Загрузить» загрузите файл serverIndigoLocal.crt, в поле «Закрытый ключ сервера» загрузите файл serverIndigoLocal.key, а в поле «Сертификат удостоверяющего центра» загрузите файл indigoRootCA.crt и нажмите кнопку «ОК».



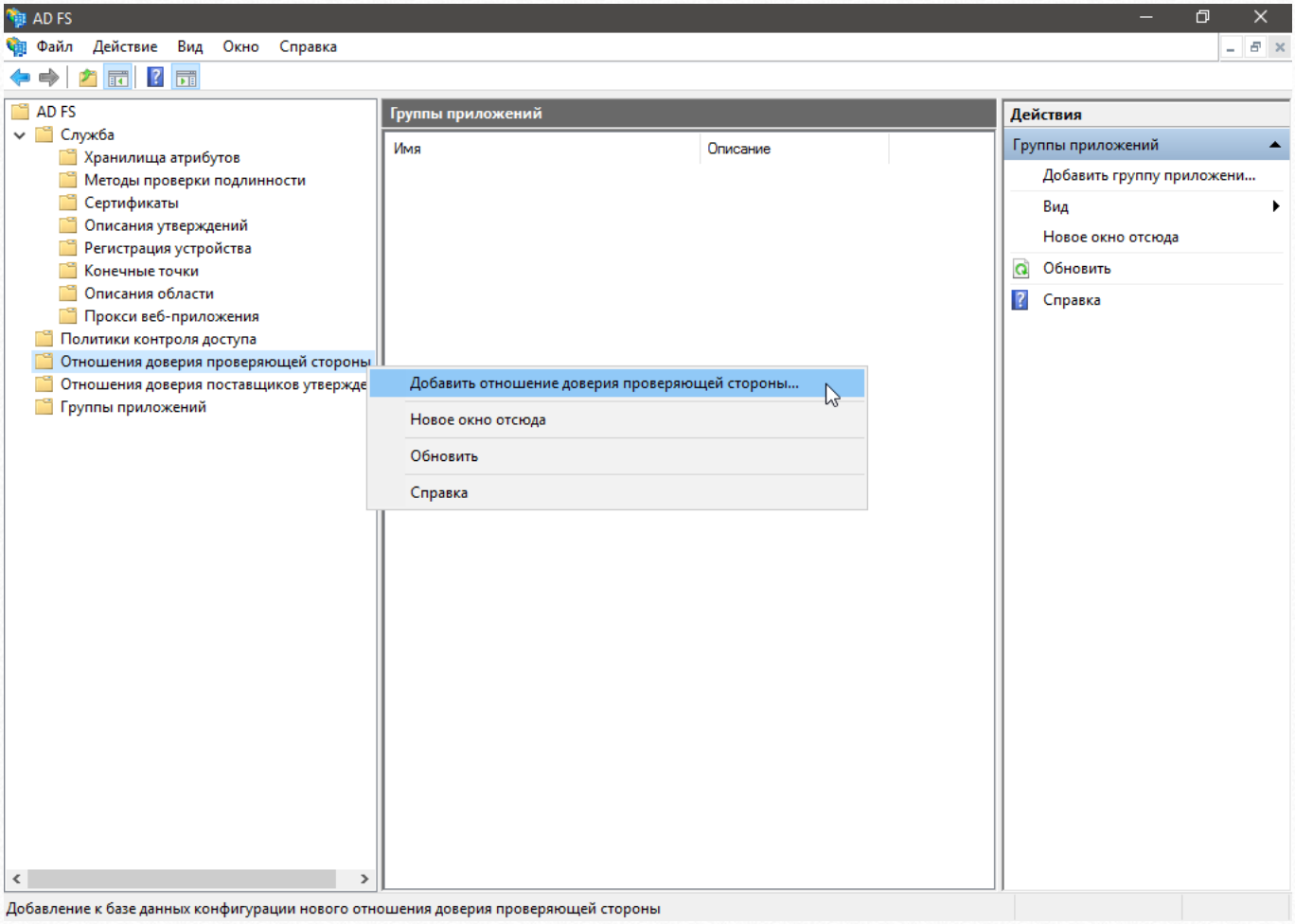
11. Вернувшись в окно «Настройки системы тестирования» тоже нажмите кнопку «ОК». На предупреждение о том, что сервер тестирования будет перезапущен необходимо ответить «Да».

2.2.5. Добавление отношения доверия проверяющей стороны в AD FS

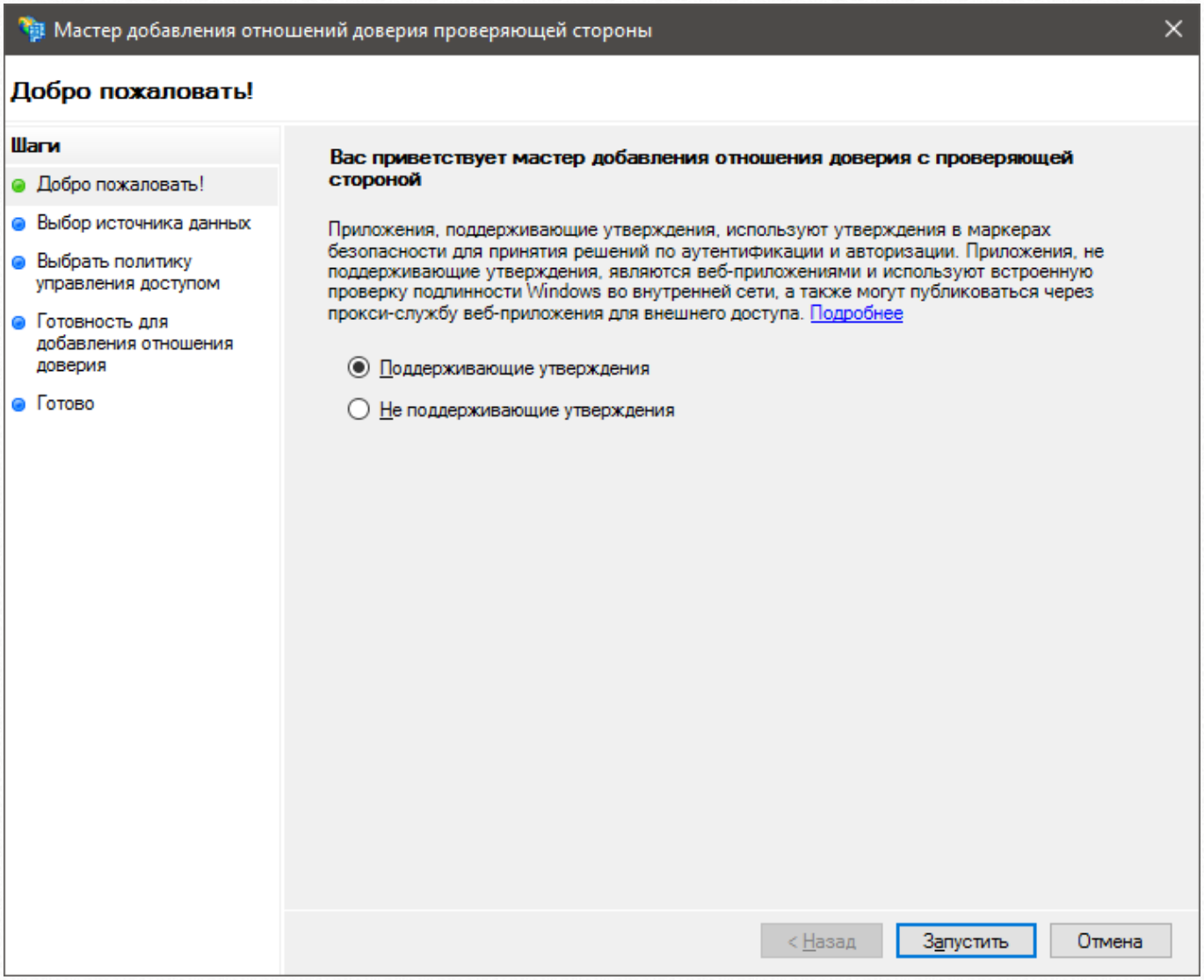
1. Теперь необходимо добавить отношение доверия проверяющей стороны в службе федерации AD. Для этого вернемся на сервер и в меню окна «Диспетчер серверов» выберем пункт «Средства» → «Управление AD FS».



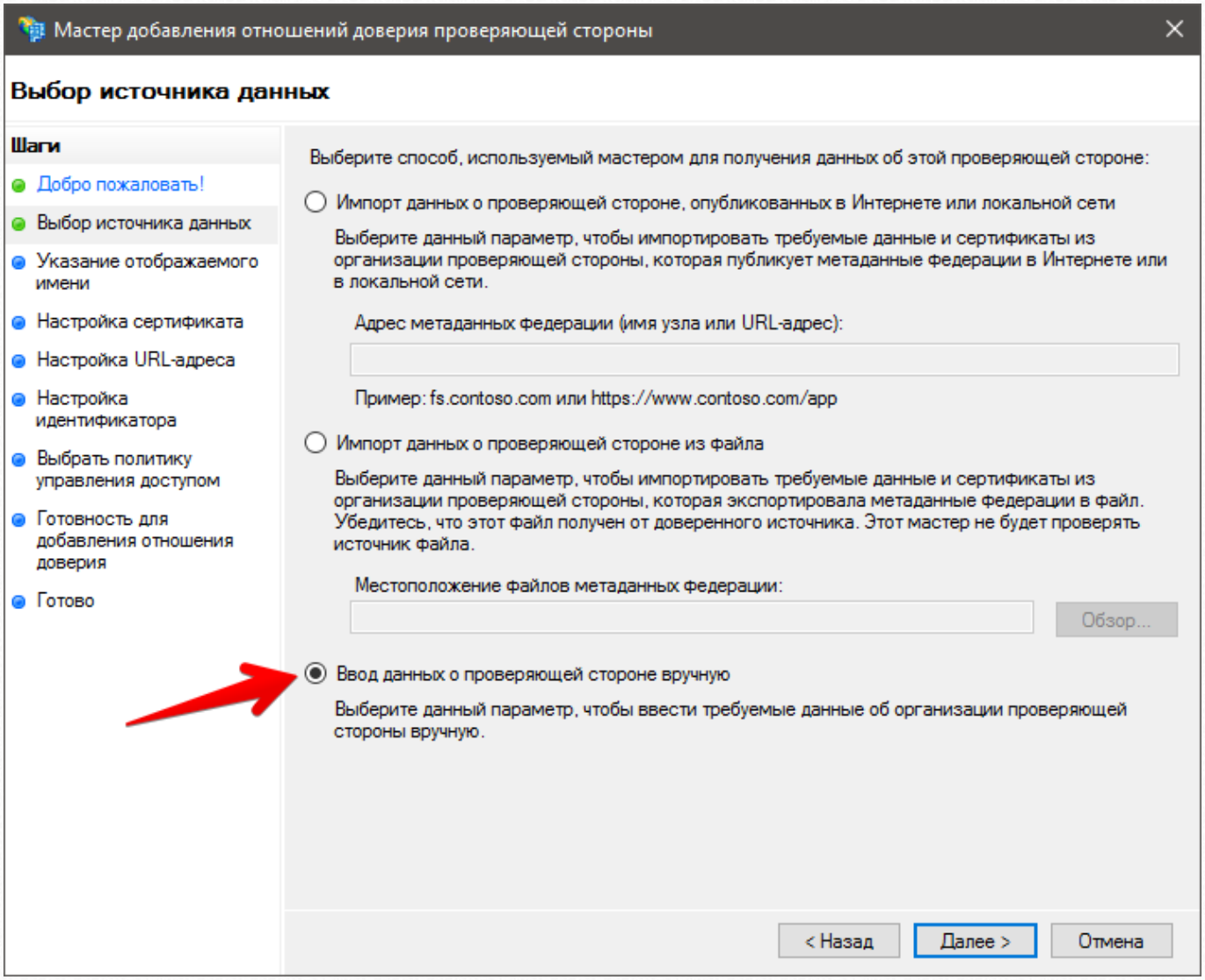
2. В открывшемся окне «AD FS» в списке слева нажмите правой кнопкой мыши по пункту «Отношения доверия проверяющей стороны» и выберите пункт «Добавить отношение доверия проверяющей стороны…».



3. В открывшемся окне «Мастер добавления отношений доверия проверяющей стороны» на шаге «Добро пожаловать» оставляем выбор на пункте «Поддерживающие утверждения» и нажимаем кнопку «Запустить».

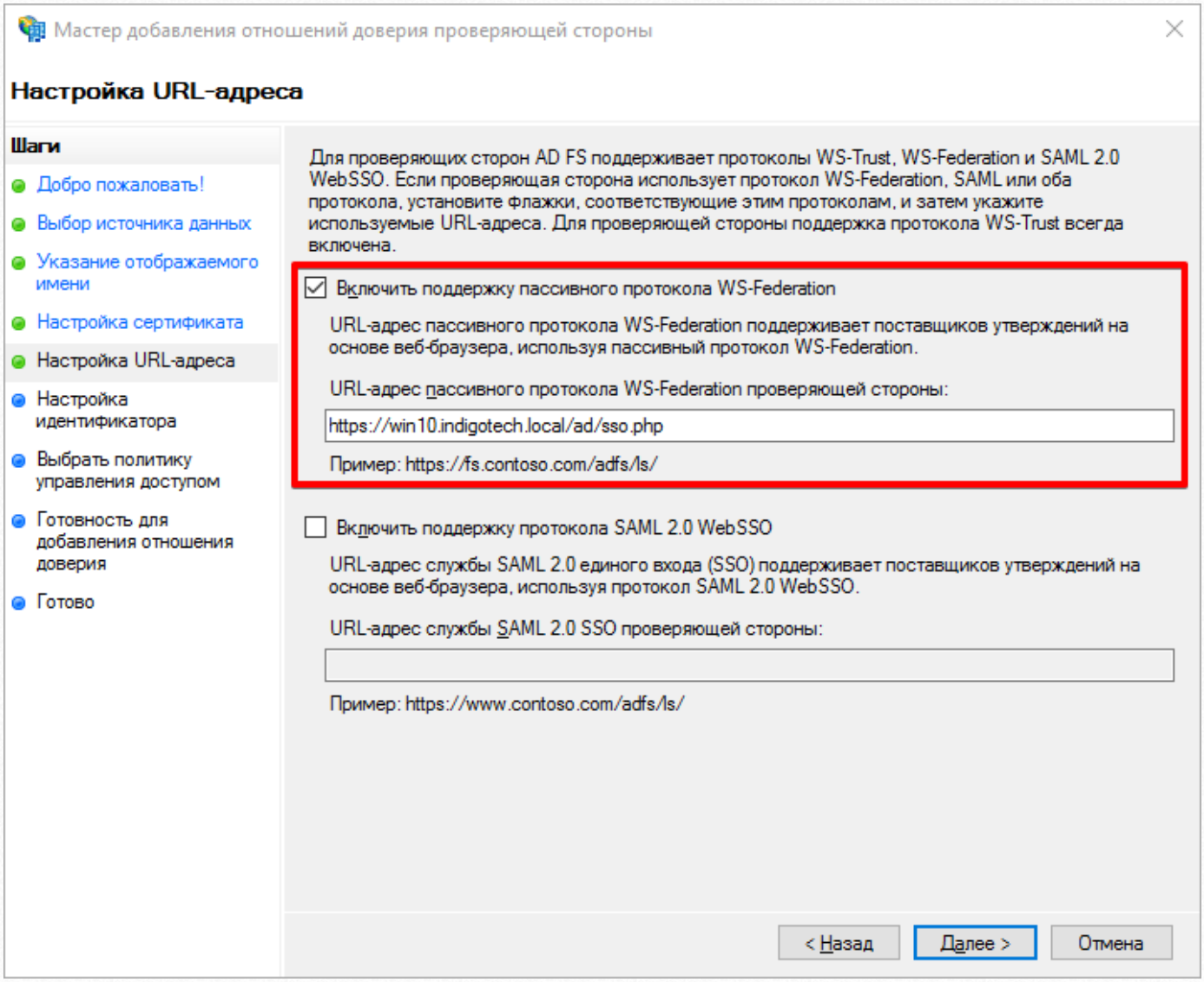


4. На следующем шаге «Выбор источника данных» выберите пункт «Ввод данных о проверяющей стороне вручную» и нажмите кнопку «Далее».

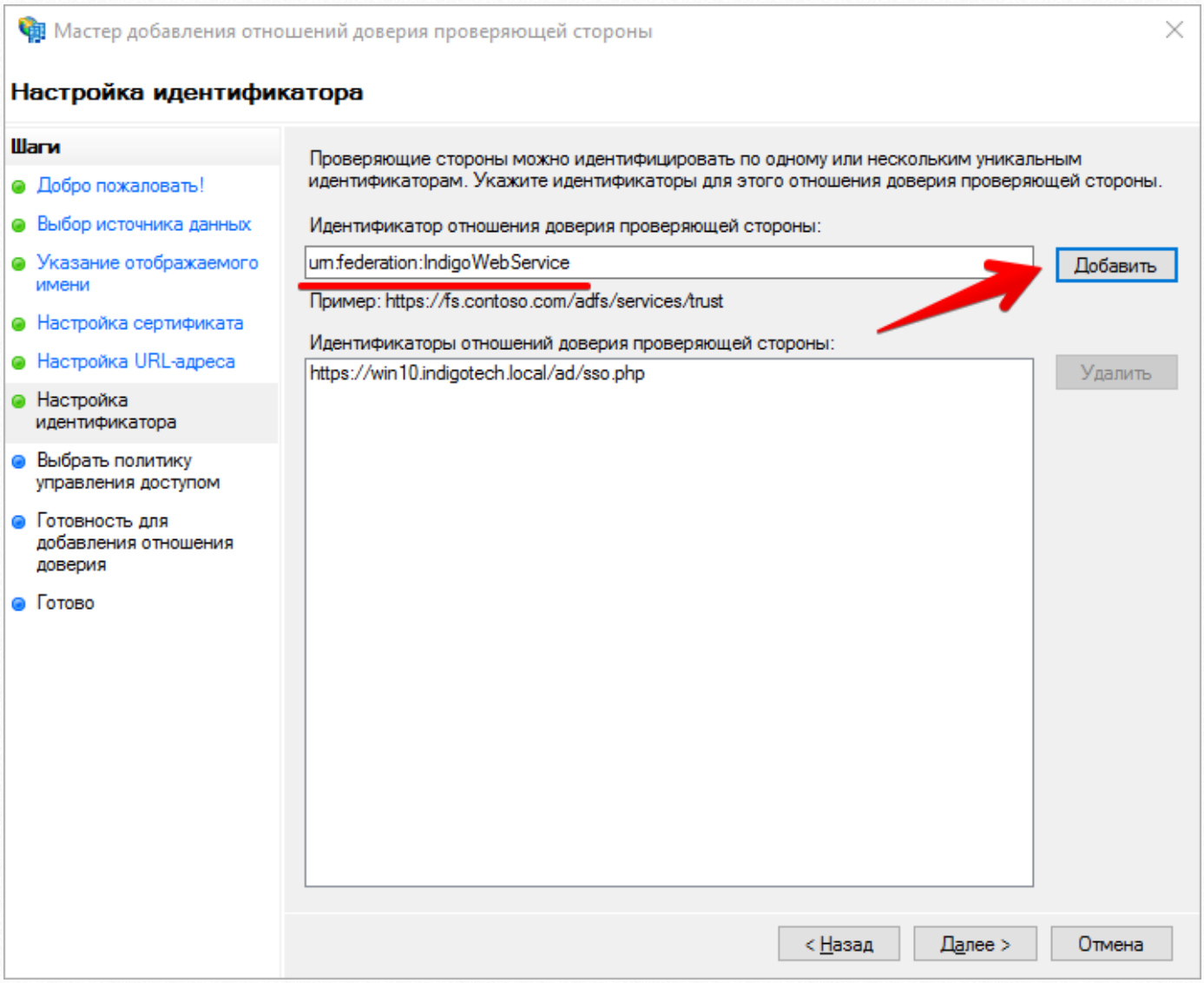


5. На шаге «Указание отображаемого имени» в поле «Отображаемое имя» введите наименование, например, «Indigo SSO» и нажмите «Далее».
6. На шаге «Настройка сертификата» нажмите «Далее».

7. На шаге «Настройка URL-адреса» поставьте галочку на пункте «Включить поддержку пассивного протокола WS-Federation» и в поле «URL-адрес пассивного протокола WS-Federation проверяющей стороны» введите URL: «https://win10.indigotech.local/ad/sso.php», где win10.indigotech.local – полное имя компьютера, на котором установлена система тестирования. Нажимаем кнопку «Далее».

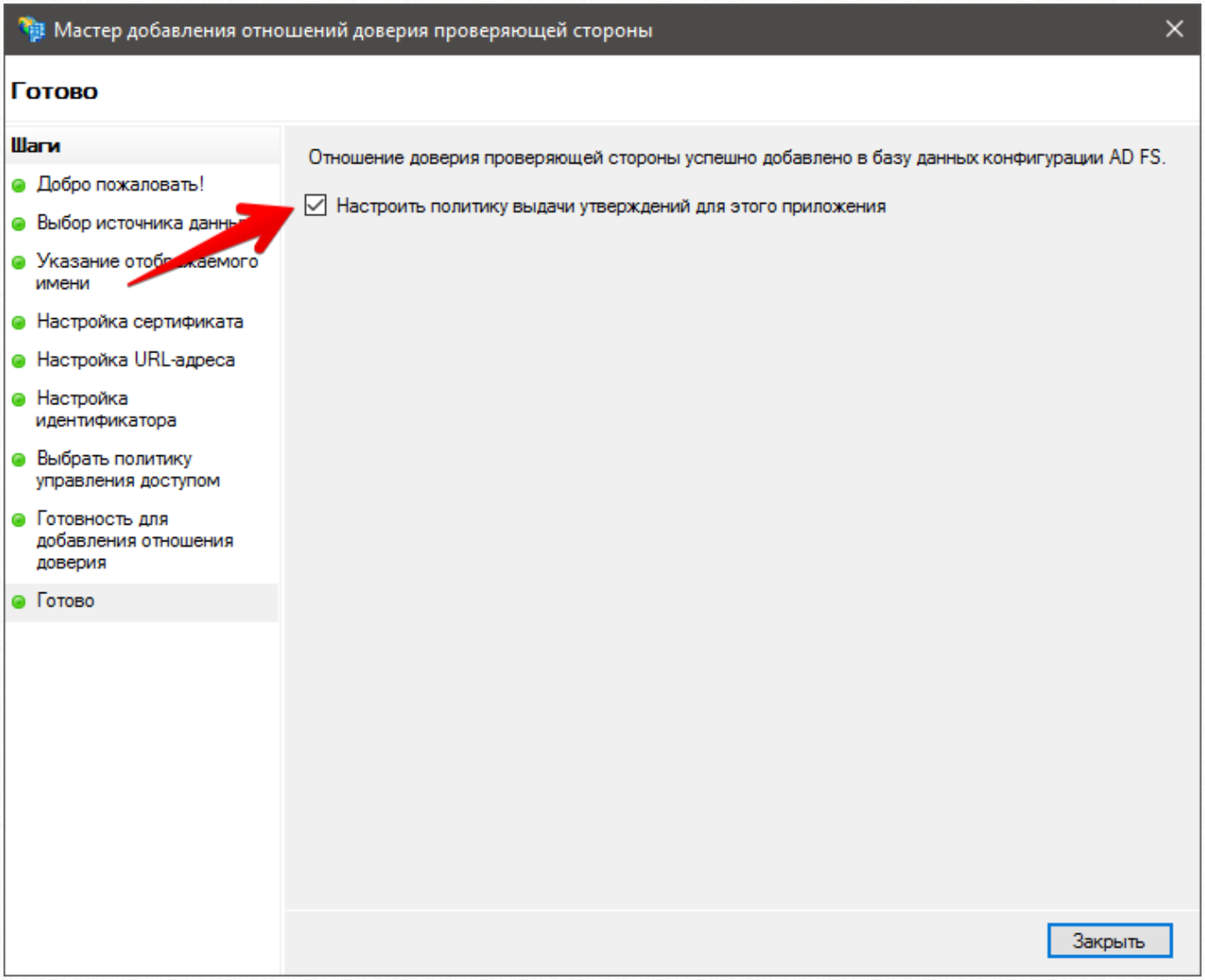


8. На шаге «Настройка идентификатора» в поле «Идентификатор отношения доверия проверяющей стороны» введите строку «urn:federation:IndigoWebService» и нажмите кнопку «Добавить». Нажимаем кнопку «Далее».

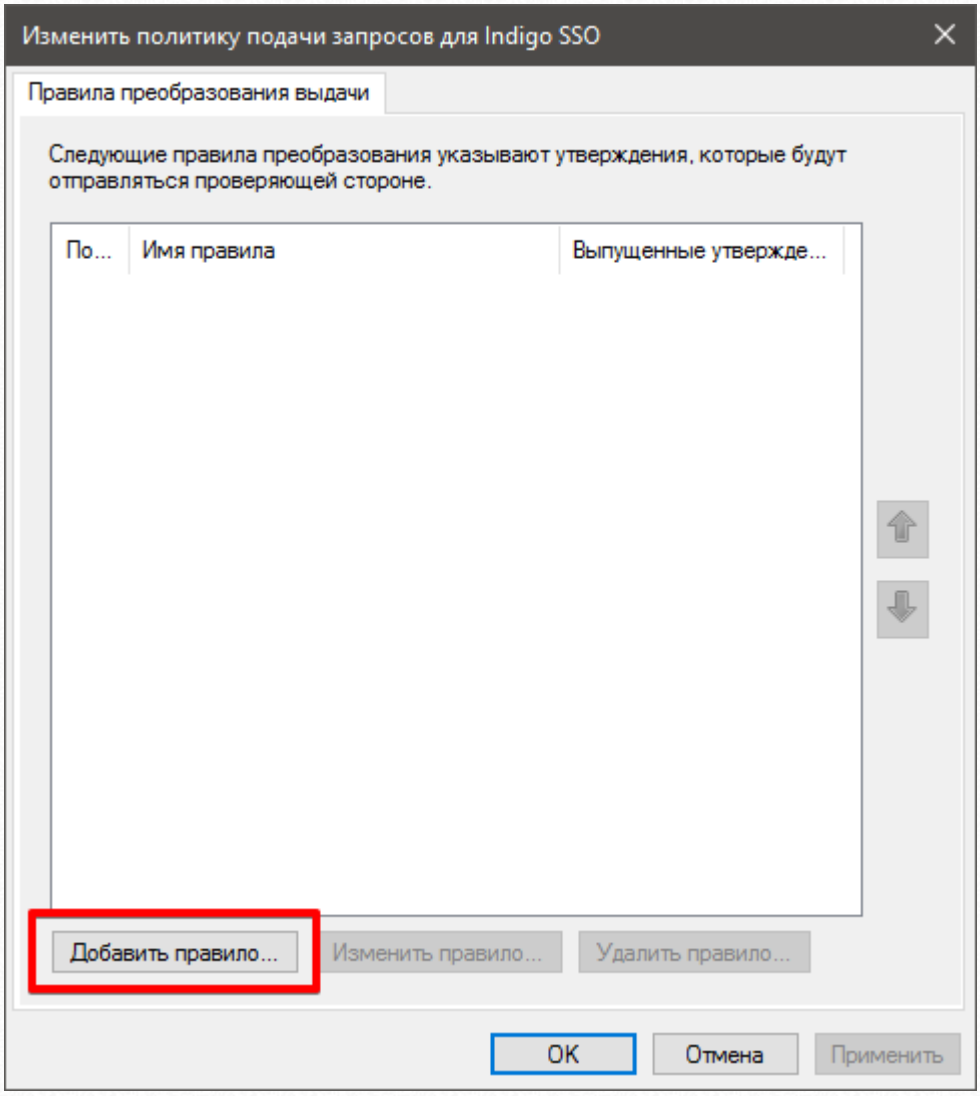


9. На шаге «Выбрать политику управления доступом» оставляем политику «Разрешение для каждого» и нажимаем кнопку «Далее».
10. На шаге «Готовность для добавления отношения доверия» нажимаем «Далее».

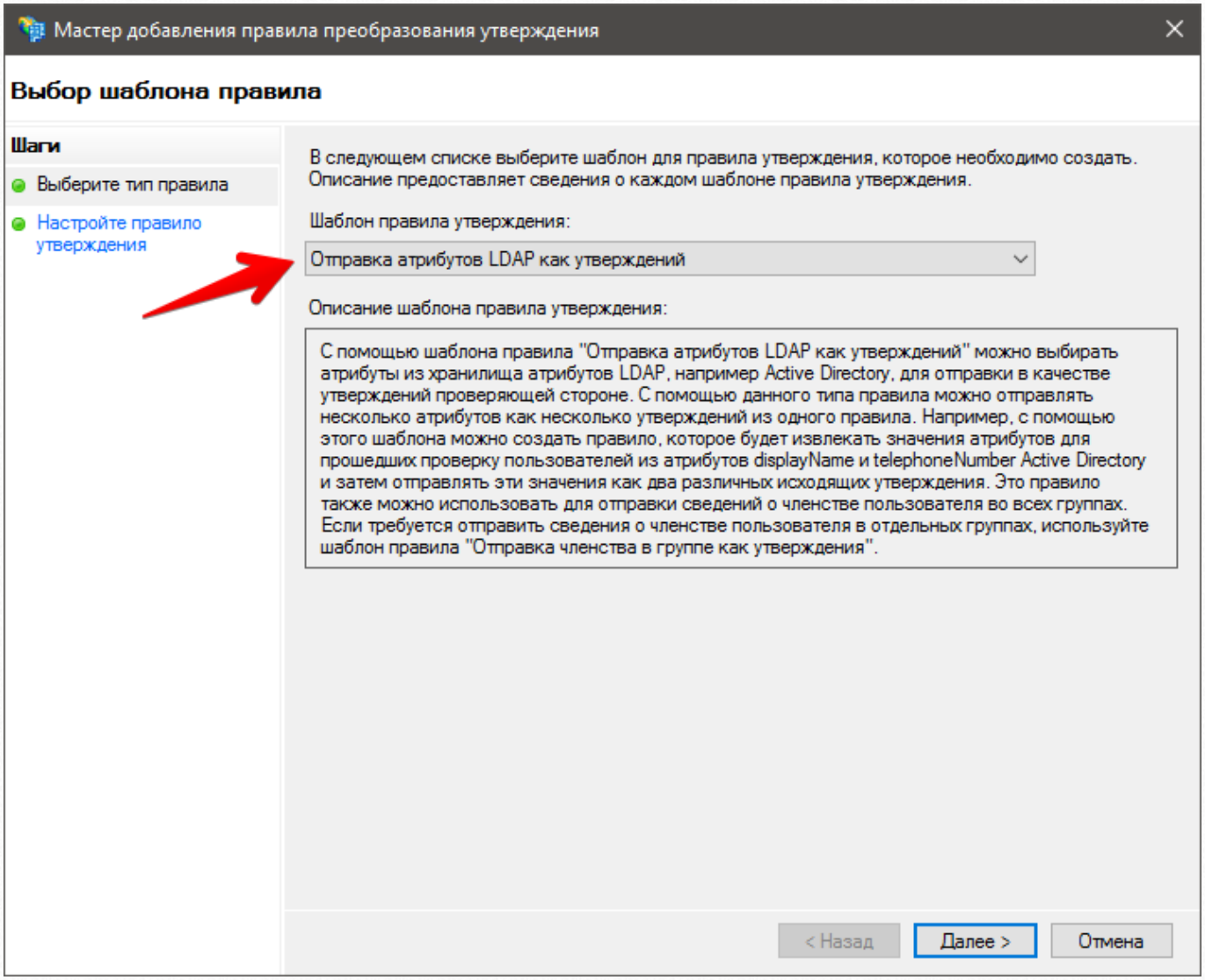
11. На заключительном шаге удостоверьтесь, что галочка «Настроить политику выдачи утверждений для этого приложения» установлена и нажмите «Закрыть».



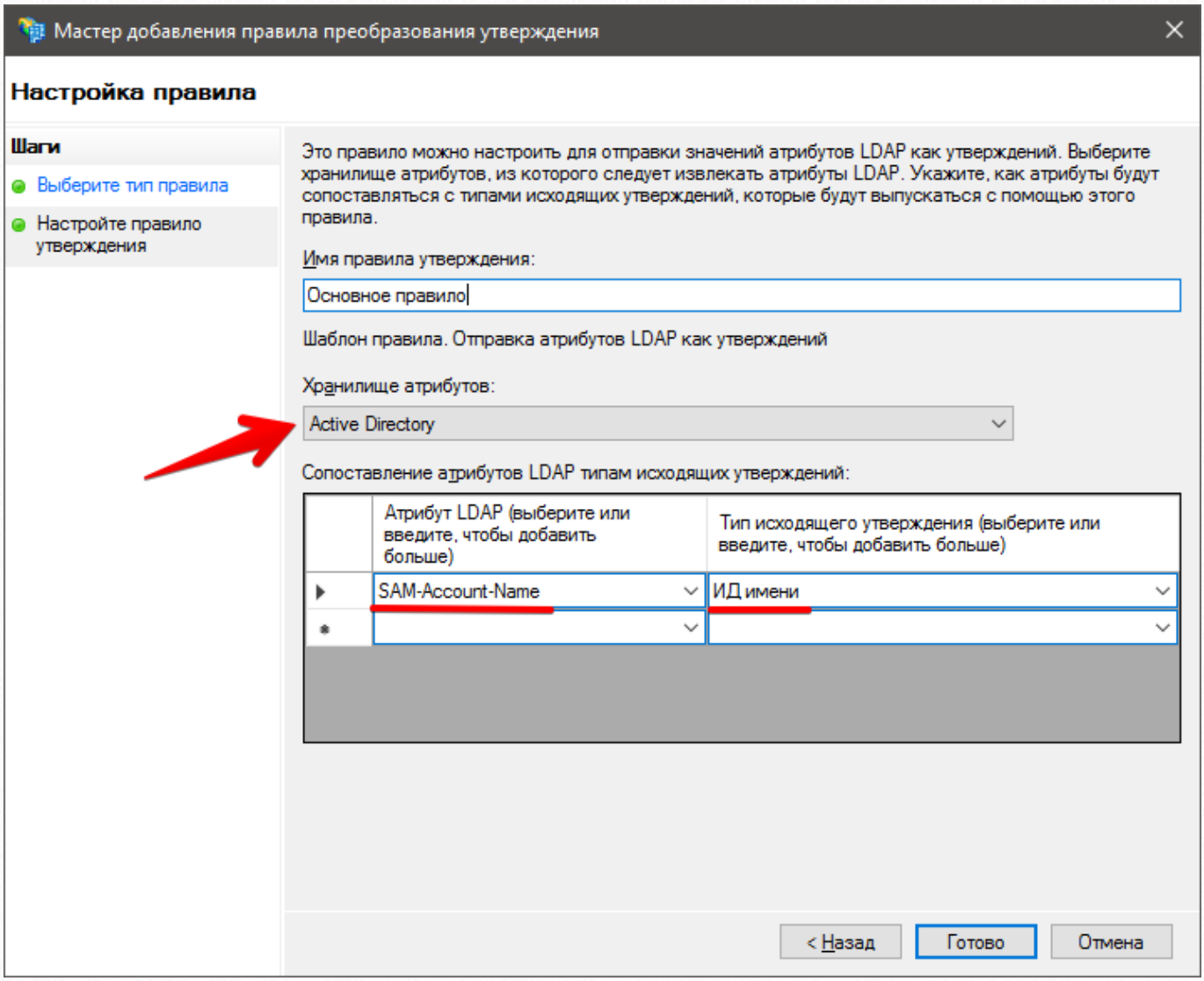
12. В открывшемся диалоге «Изменить политику подачи запросов для Indigo SSO» нажмите кнопку «Добавить правило...»



13. В открывшемся окне «Мастер добавления правила преобразования утверждения» в списке «Шаблон правила утверждения» выбираем «Отправка атрибутов LDAP как утверждений» и нажимаем «Далее».

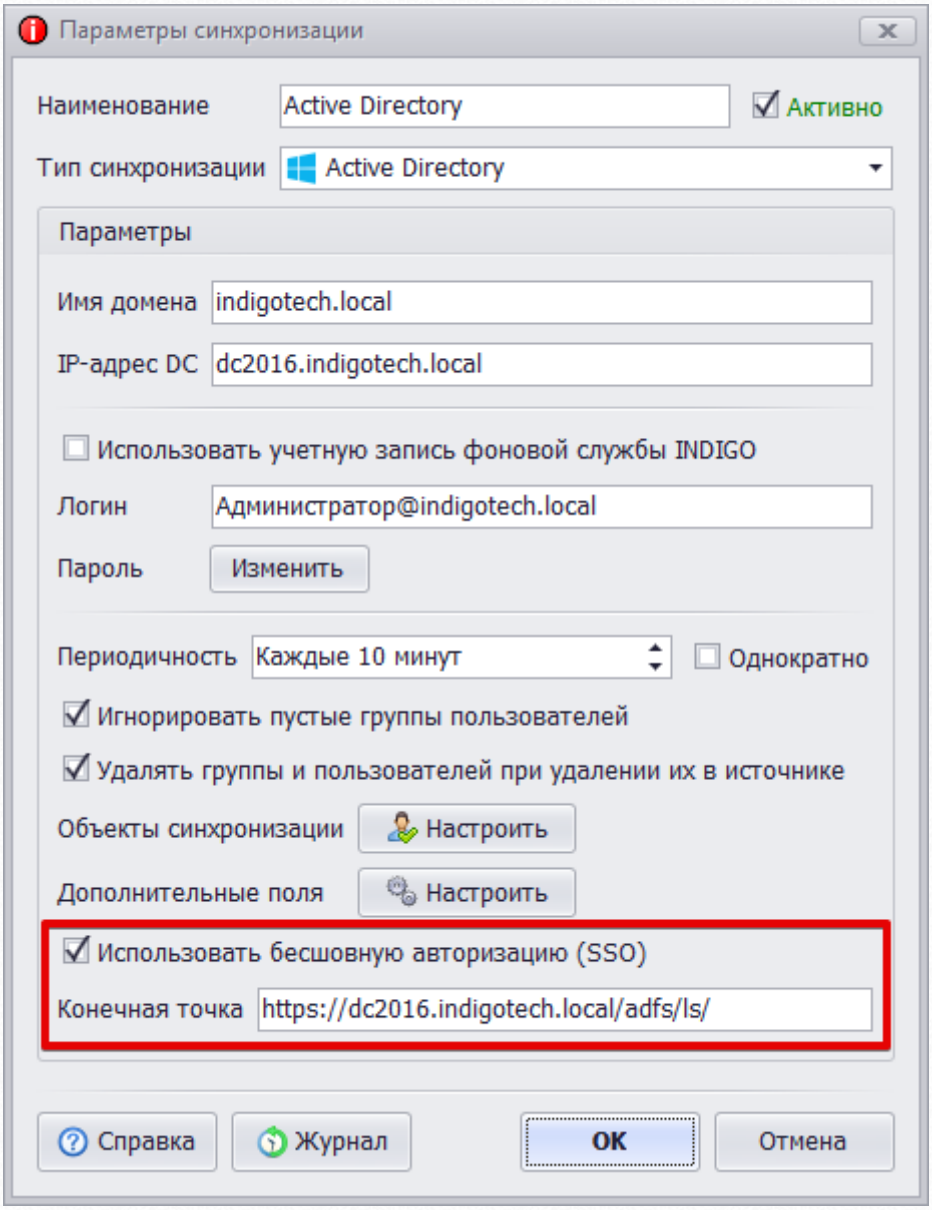


14. На шаге «Настройка правила» введите в поле «Имя правила утверждения» название для правила, например, «Основное правило». В списке «Хранилище атрибутов» выберите «Active Directory». В таблице «Сопоставление атрибутов LDAP типам исходящих утверждений» в колонке «Атрибут LDAP» выберите из выпадающего списка пункт «SAM-Account-Name», а в колонке «Тип исходящего утверждения» пункт «ИД имени». После нажмите «Готово».



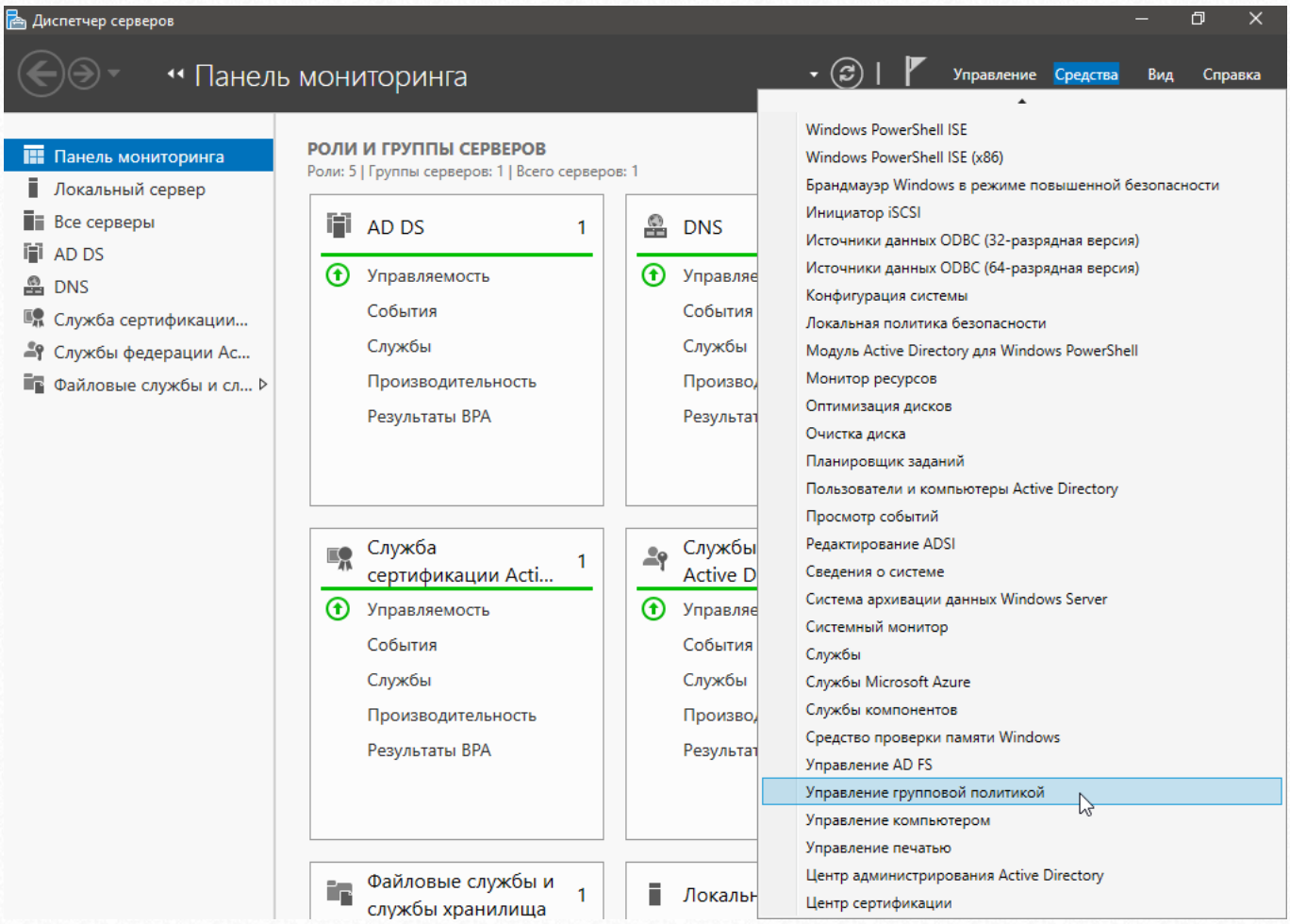
15. В окне «Изменить политику подачи запросов для Indigo SSO» нажмите «ОК».

16. Для того чтобы активировать бесшовную авторизацию зайдите в настройки синхронизации и установите флажок «Использовать бесшовную авторизацию Active Directory Federation Services». В поле «Конечная точка WS-Federation» введите адрес конечной точки, в нашем случае «https://dcwin2016.indigotech.local/adfs/ls/» и нажмите «ОК».

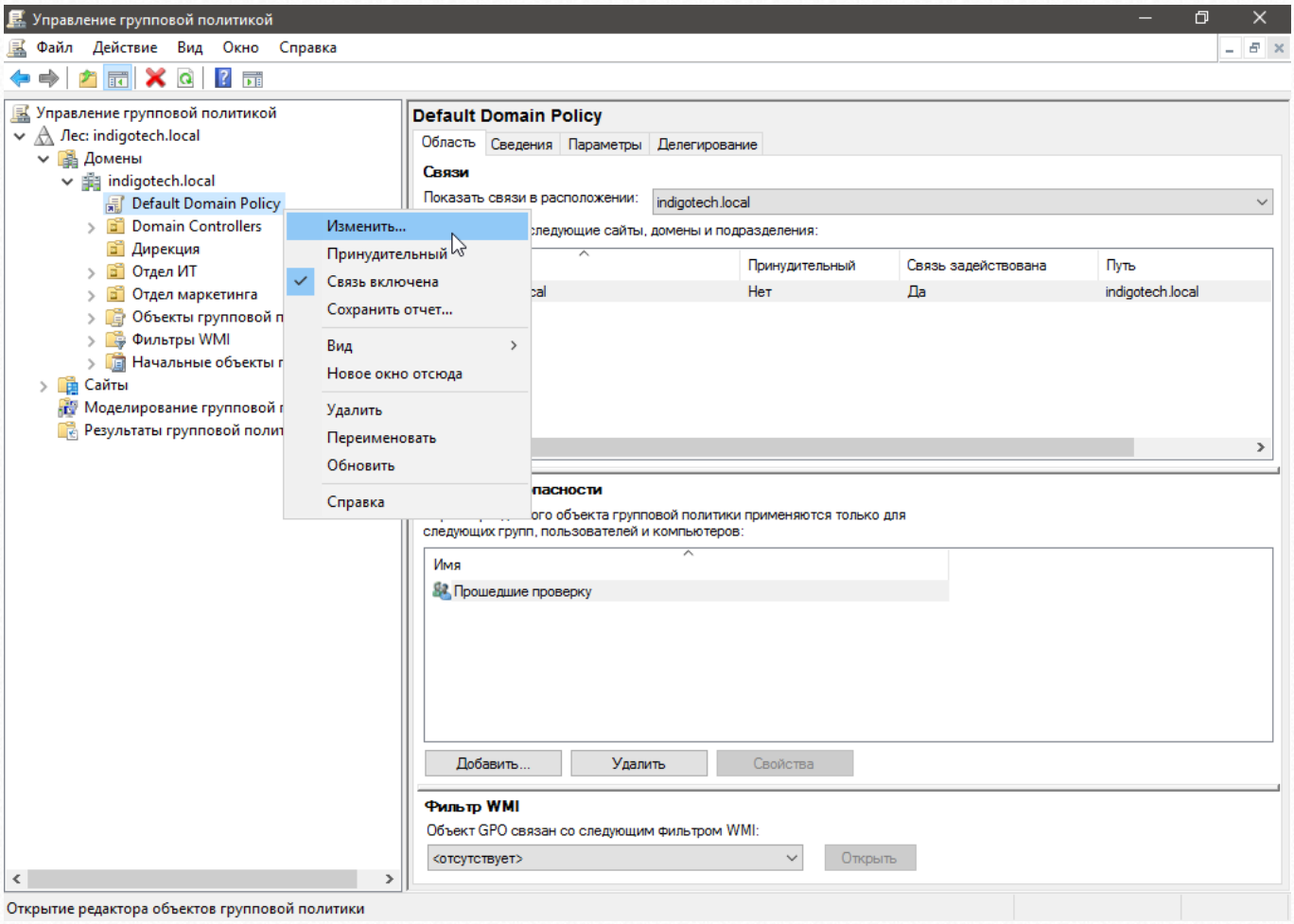


2.2.6. Настройка групповой политики

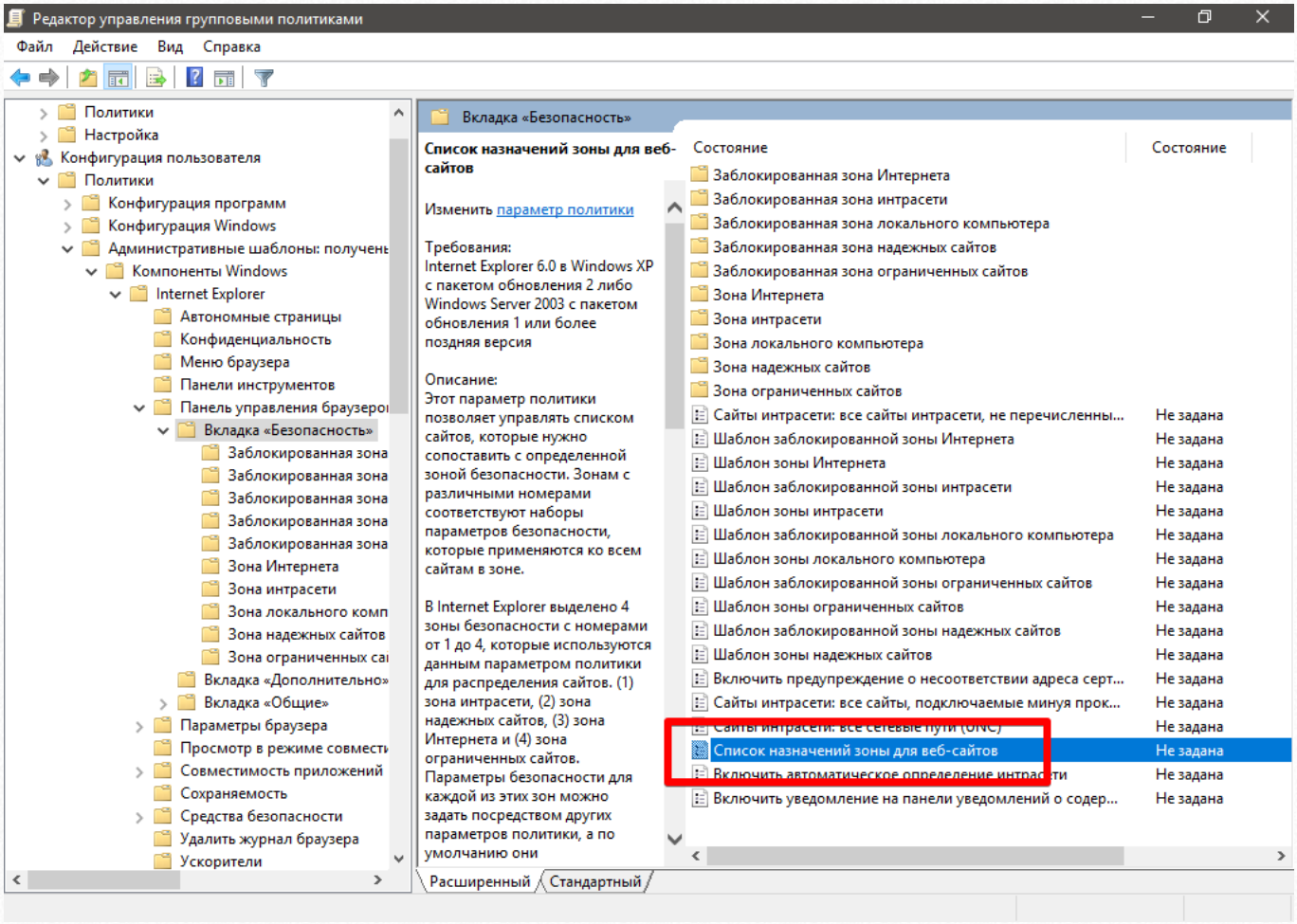
1. Для того чтобы бесшовная авторизация корректно работала необходимо адрес сервера, на котором установлена служба федерации Active Directory, добавить в зону «Местная интрасеть» в браузерах клиентов. Это можно сделать глобально с помощью настроек групповой политики. Для этого в окне «Диспетчер серверов» выбираем пункт меню «Средства» → «Управление групповой политикой».



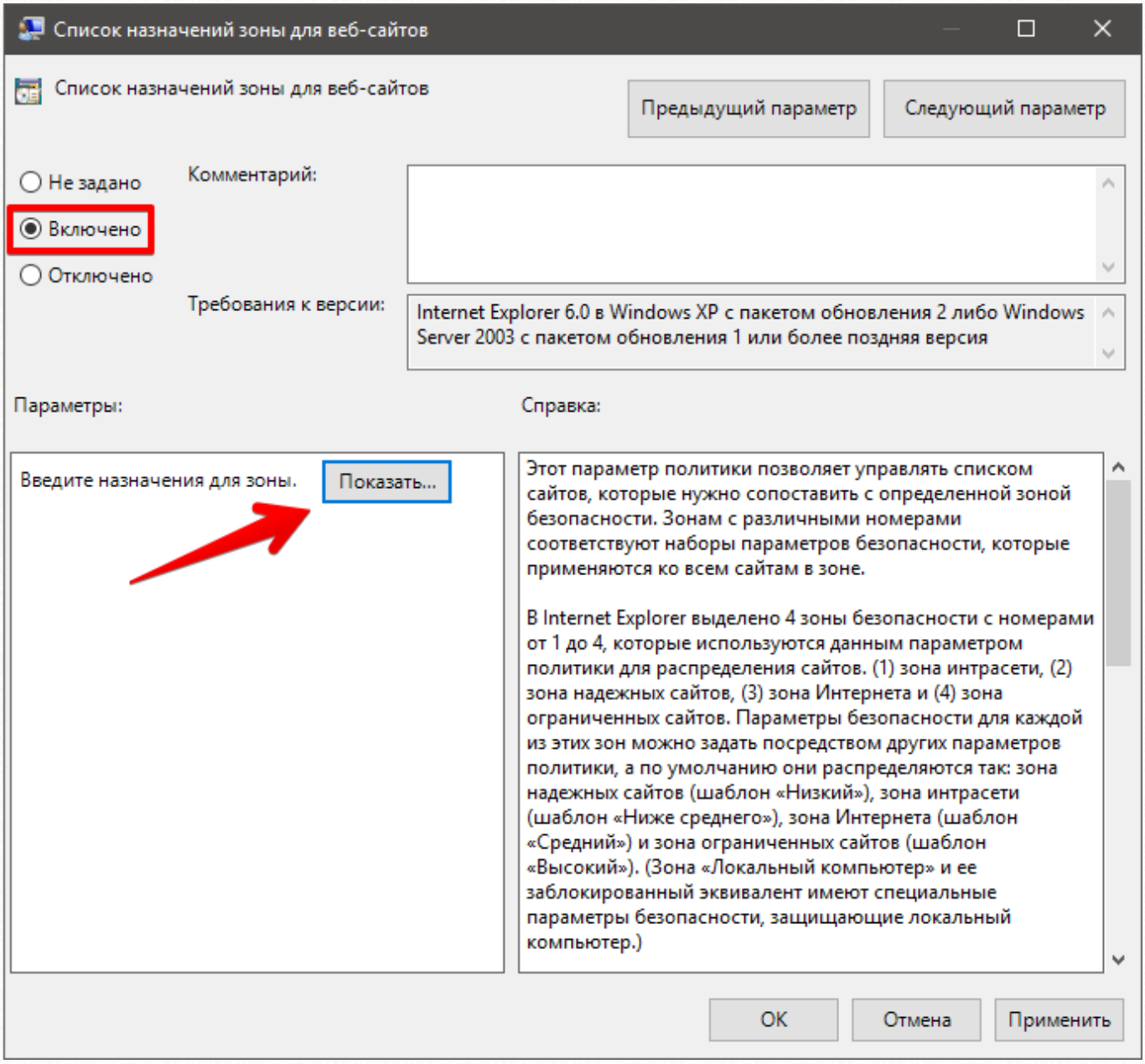
2. В открывшемся окне «Управление групповой политикой» в списке слева выберите политику, которая применяется к синхронизируемым пользователям в домене (в нашем случае будем изменять политику домена по умолчанию), нажмите на ней правой кнопкой мыши и выберите пункт меню «Изменить».



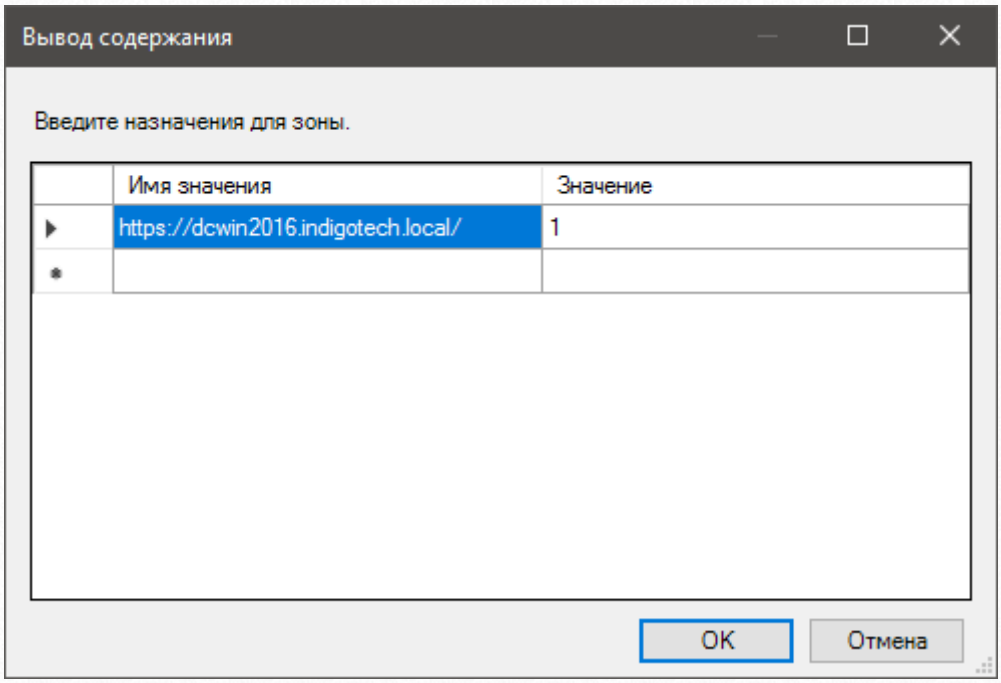
3. В открывшемся окне «Редактор управления групповыми политиками» в списке слева выберите группу «Конфигурация пользователя» → «Политики» → «Административные шаблоны» → «Компоненты Windows» → «Internet Explorer» → «Панель управления браузером» → «Вкладка Безопасность». В появившемся списке справа дважды кликните по пункту «Список назначений зоны для веб-сайтов».



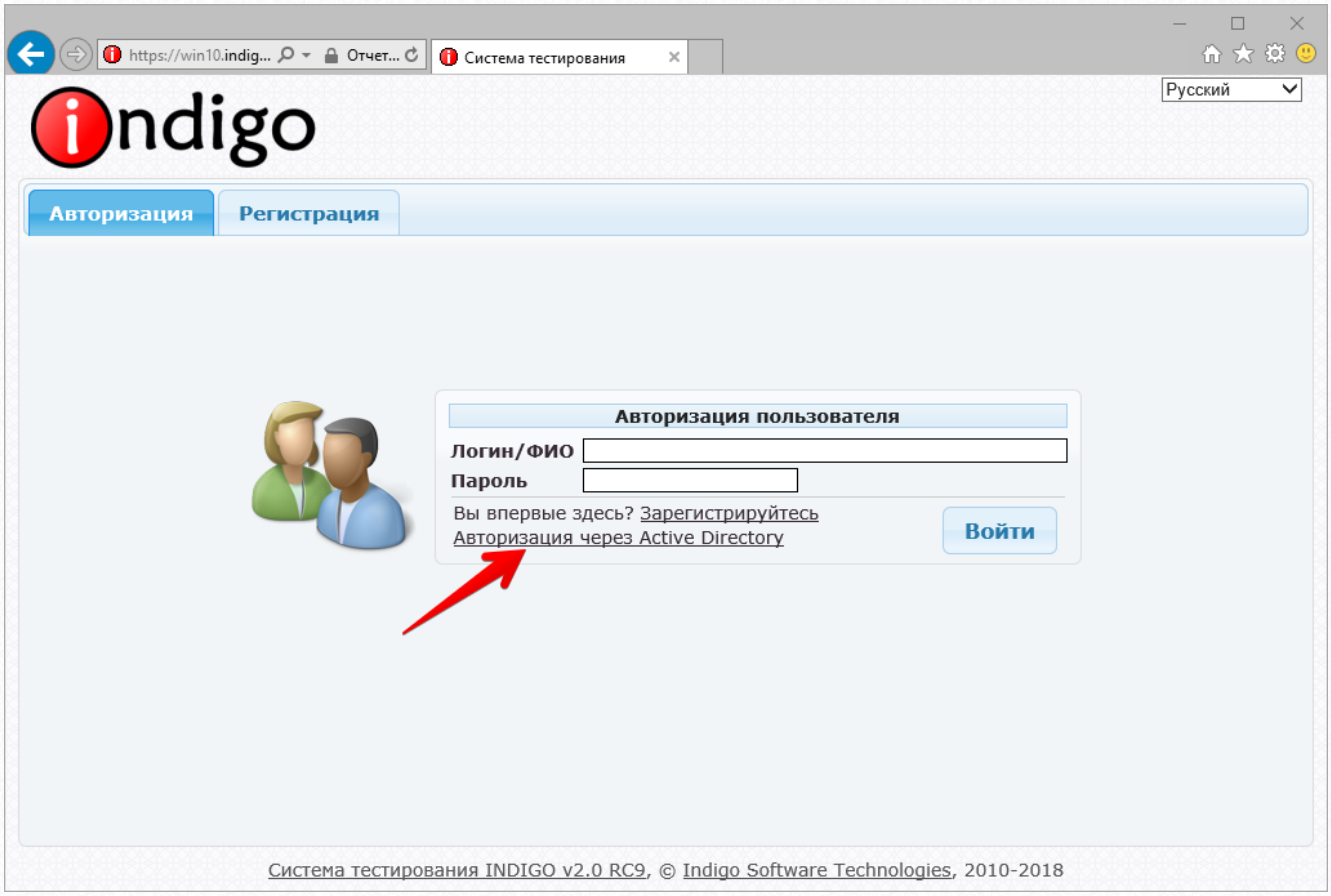
4. В окне «Список назначений зоны для веб-сайтов» установите выбор на пункт «Включено» и нажмите кнопку «Показать...».



5. В окне «Вывод содержания» в колонке «Имя значения» введите URL к серверу, на котором установлена служба федерации AD, в нашем случае «https://dcwin2016.indigotech.local/», а в колонке «Значение» введите «1». И нажмите «ОК». В окне «Список назначений зоны для веб-сайтов» также нажмите «ОК». Теперь у пользователей, к которым применена это политика, адрес нашего сервера федераций будет в зоне интрасети и бесшовная авторизация будет работать.



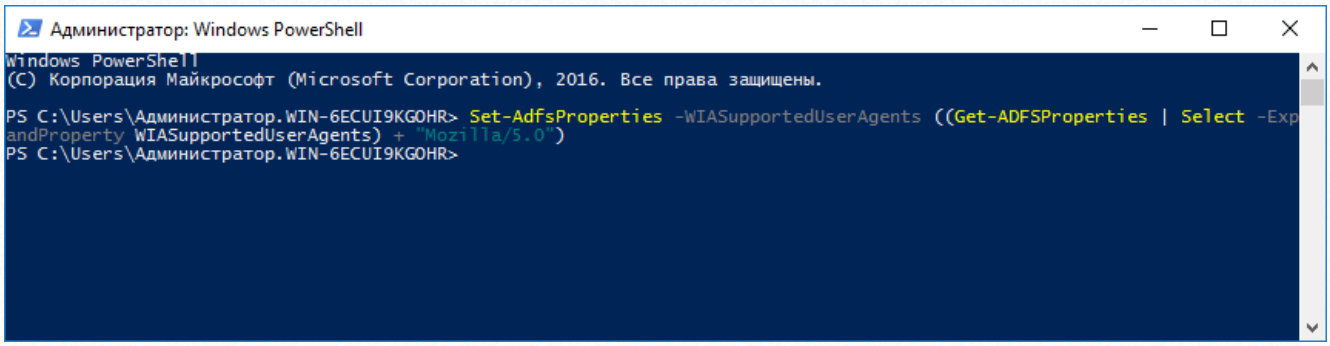
6. Теперь если открыть веб-интерфейс системы тестирования, то мы увидим, что появилась возможность авторизации через Active Directory. Если Вы пройдете по ссылке, то автоматически авторизуетесь под учетной записью, с помощью которой был выполнен вход в ОС.



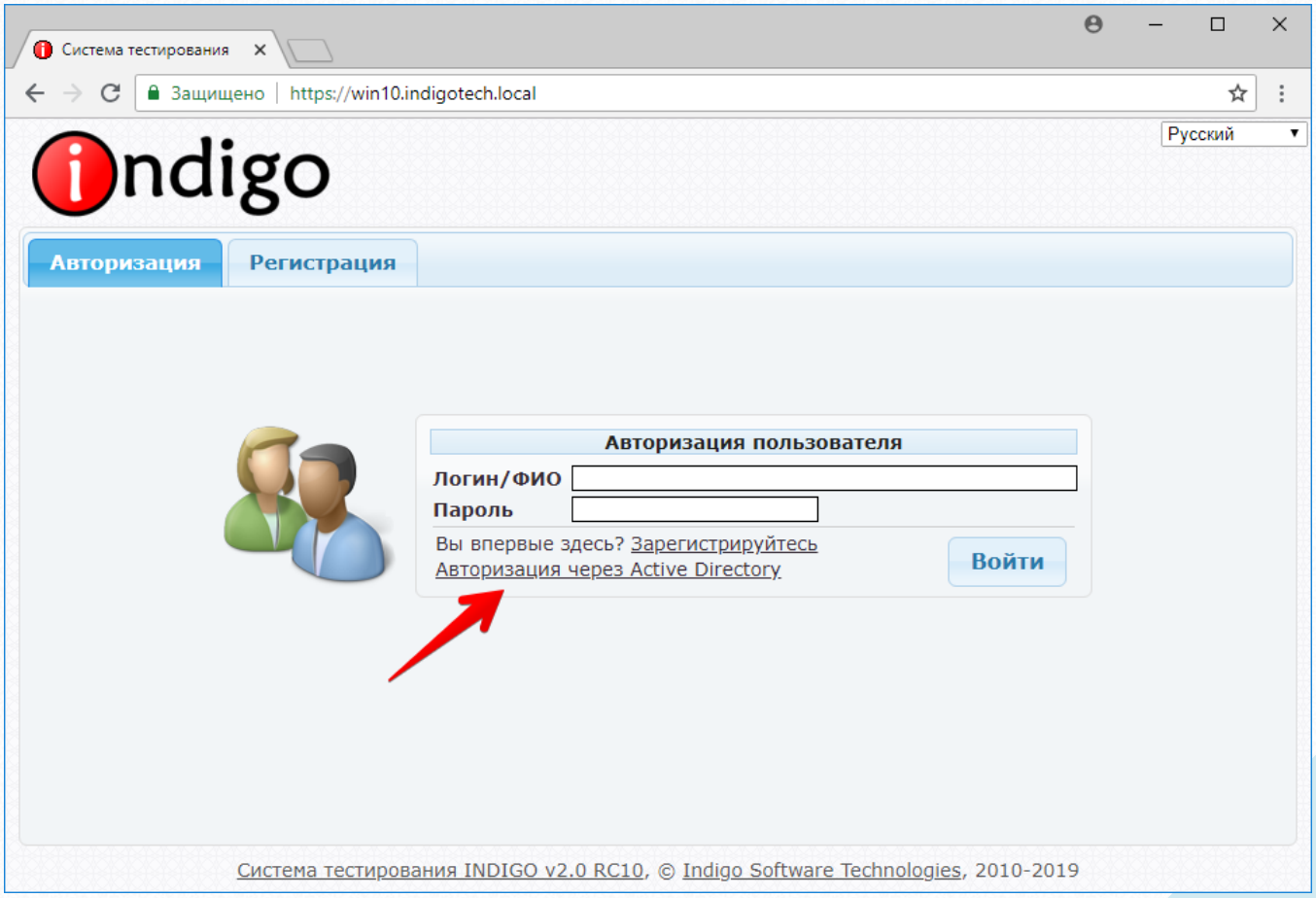
2.2.7. Настройка бесшовной авторизации для Google Chrome, Mozilla Firefox и других браузеров

Для того, чтобы бесшовная авторизация работала в браузерах Google Chrome, Mozilla Firefox и ряде других браузеров, необходимо добавить соответствующий «user-agent» в список поддерживаемых. Для этого с помощью меню «Пуск» запустите Windows Power Shell и выполните команду:

```
Set-AdfsProperties -WIASupportedUserAgents ((Get-ADFSProperties |
Select -ExpandProperty WIASupportedUserAgents) + "Mozilla/5.0")
```



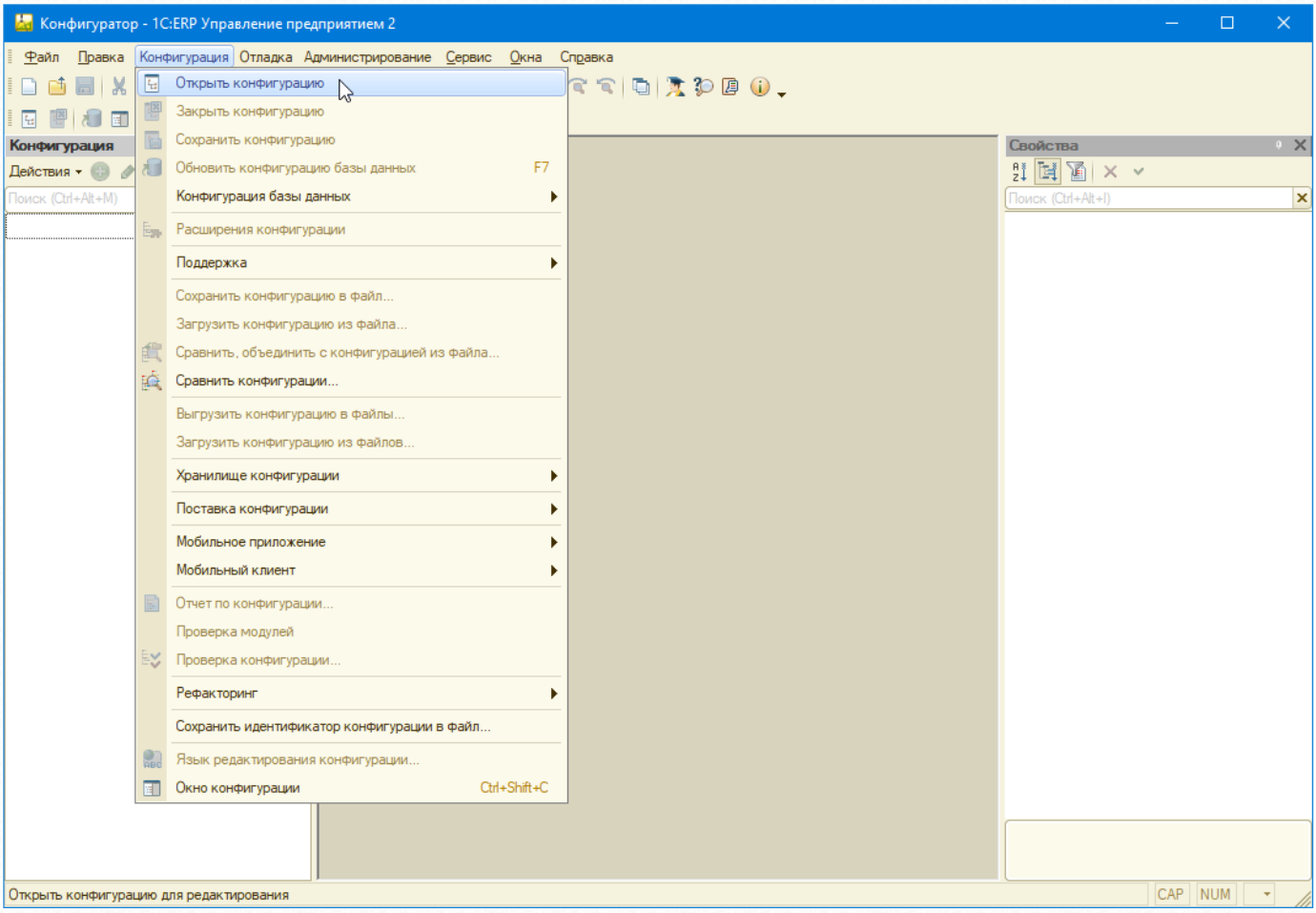
Теперь автоматическая авторизация будет работать в других браузерах:



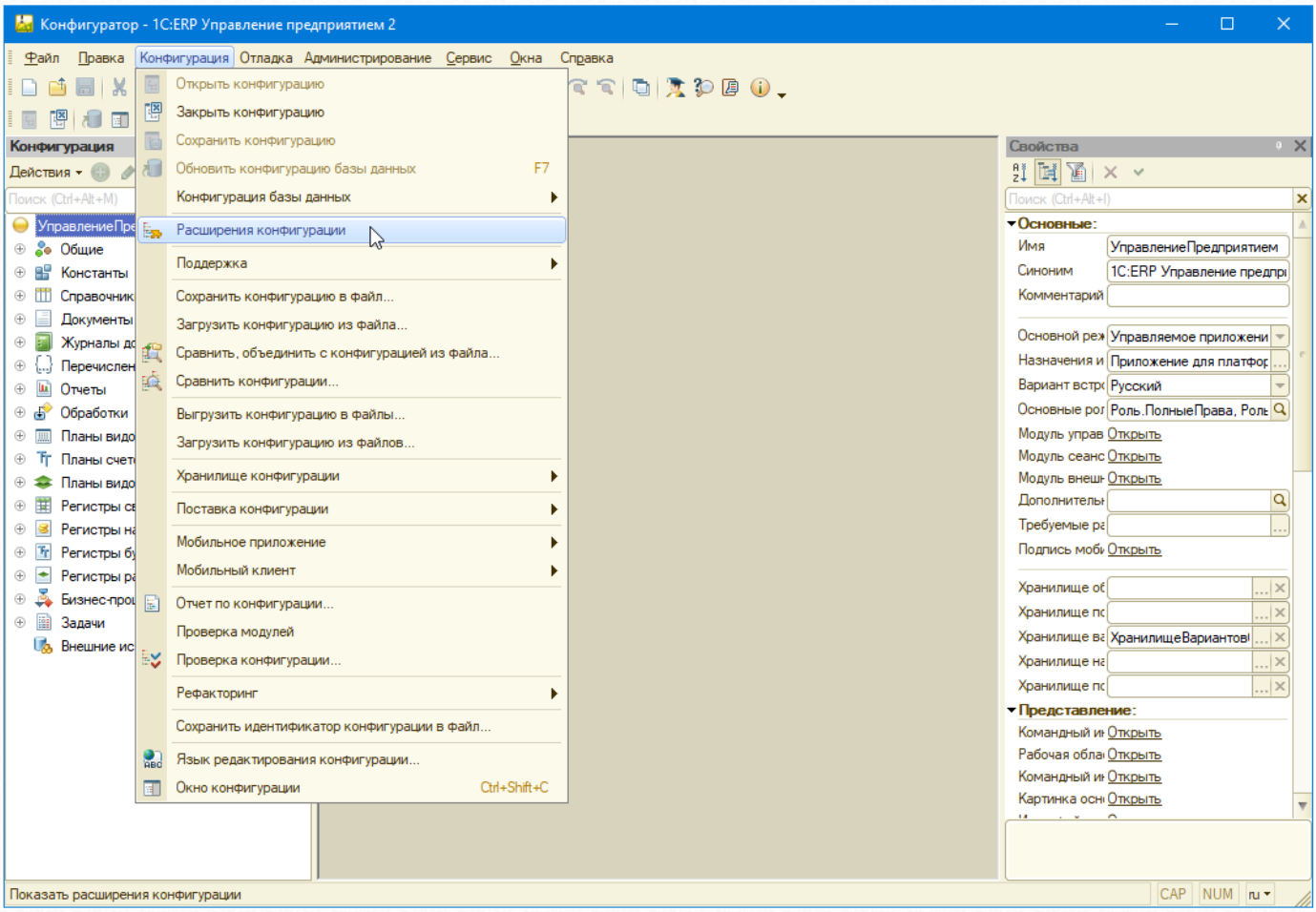
3. Настройка платформы 1С:Предприятие для синхронизации пользователей

3.1. Установка расширения конфигурации

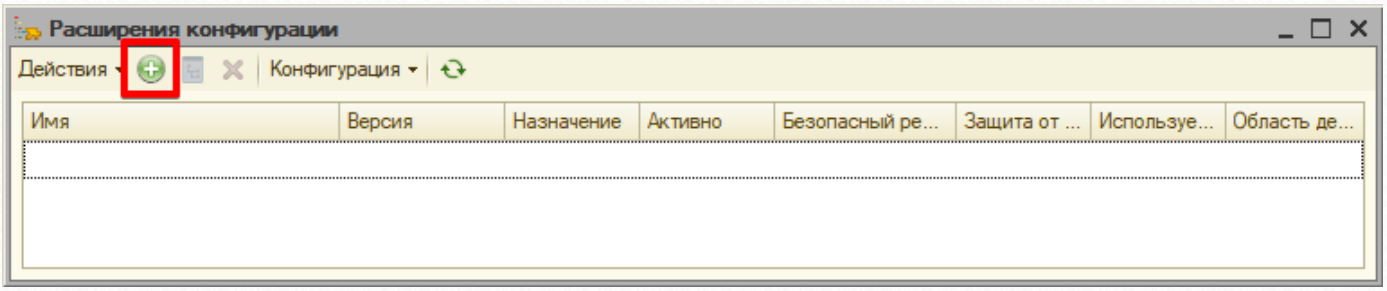
Для осуществления обмена информацией между системой тестирования INDIGO и базой 1С необходимо добавить новый объект конфигурации «HTTP-сервис». Чтобы не вносить изменения в текущую конфигурацию базы, HTTP-сервис добавляется в качестве расширения конфигурации. Для добавления расширения откройте платформу 1С в режиме конфигуратора и в главном меню выберите пункт «Конфигурация» → «Открыть конфигурацию».



После открытия конфигурации выберете в главном меню пункт «Конфигурация» → «Расширения конфигурации».

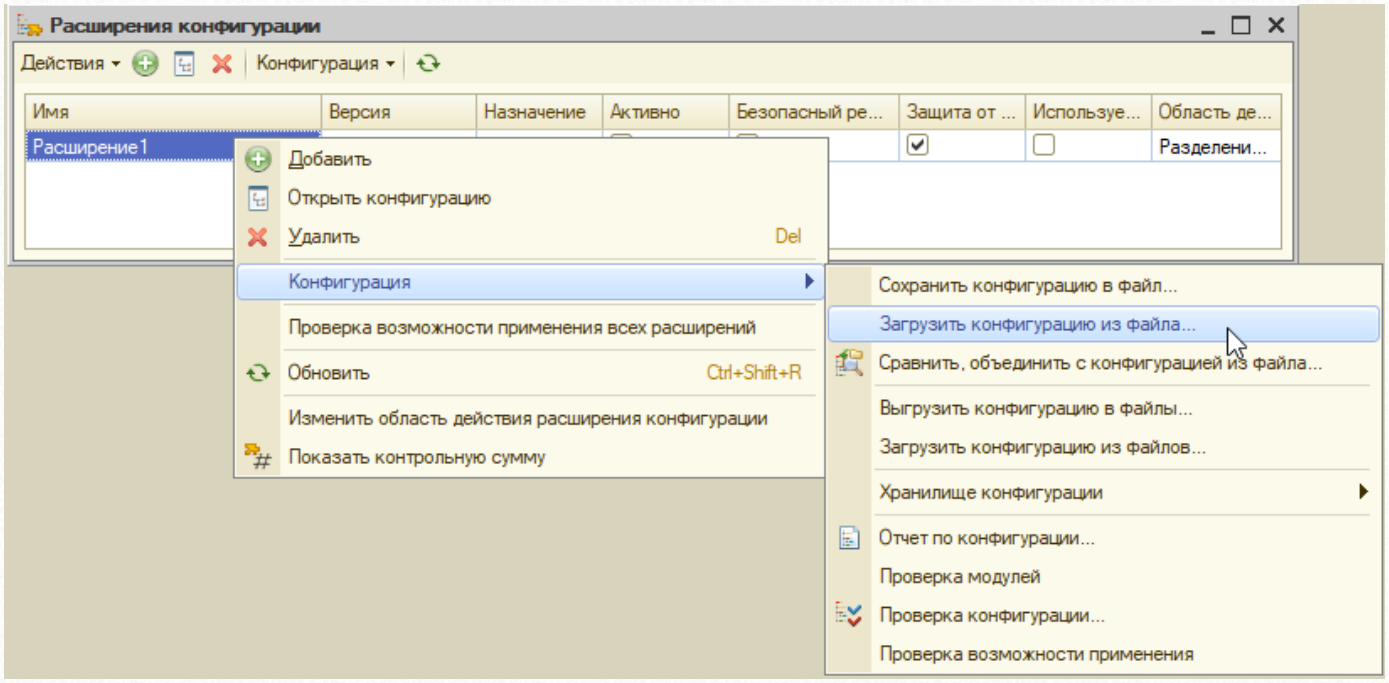


В открывшемся окне «Расширения конфигурации» нажмите кнопку «Добавить».

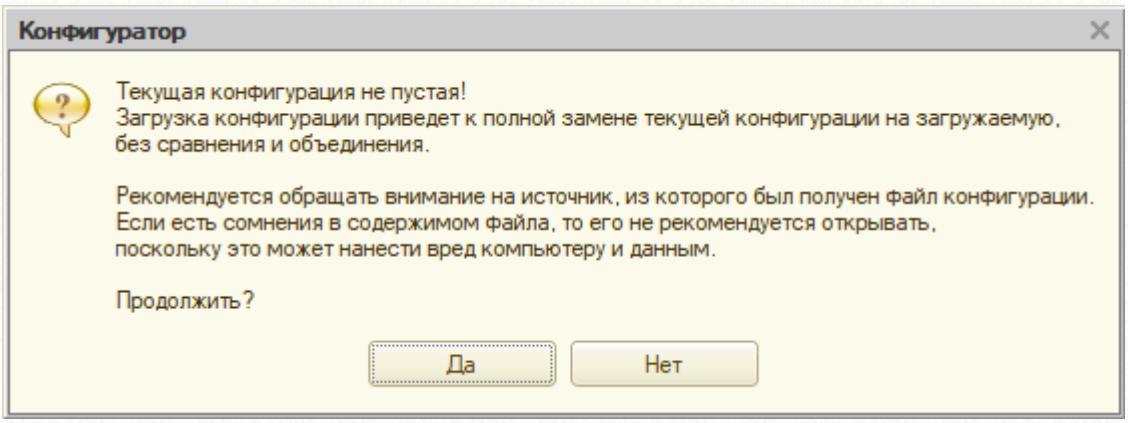


В открывшемся окне «Новое расширение конфигурации» оставьте все поля заполненными по умолчанию и нажмите кнопку «ОК».

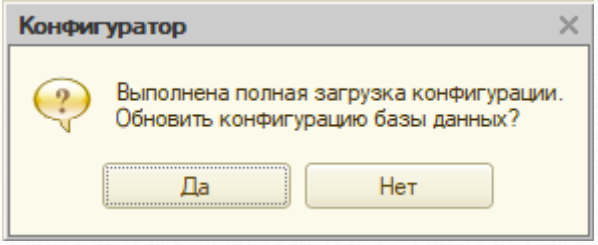
Нажмите правой кнопкой мыши по добавленной строке и в выпадающем меню выберите пункт «Конфигурация» → «Загрузить конфигурацию из файла...» и в диалоге укажите путь к файлу https://indigotech.ru/downloads/files/INDIGO.cfe.



В появившемся предупреждении нажмите кнопку «Да», чтобы продолжить.

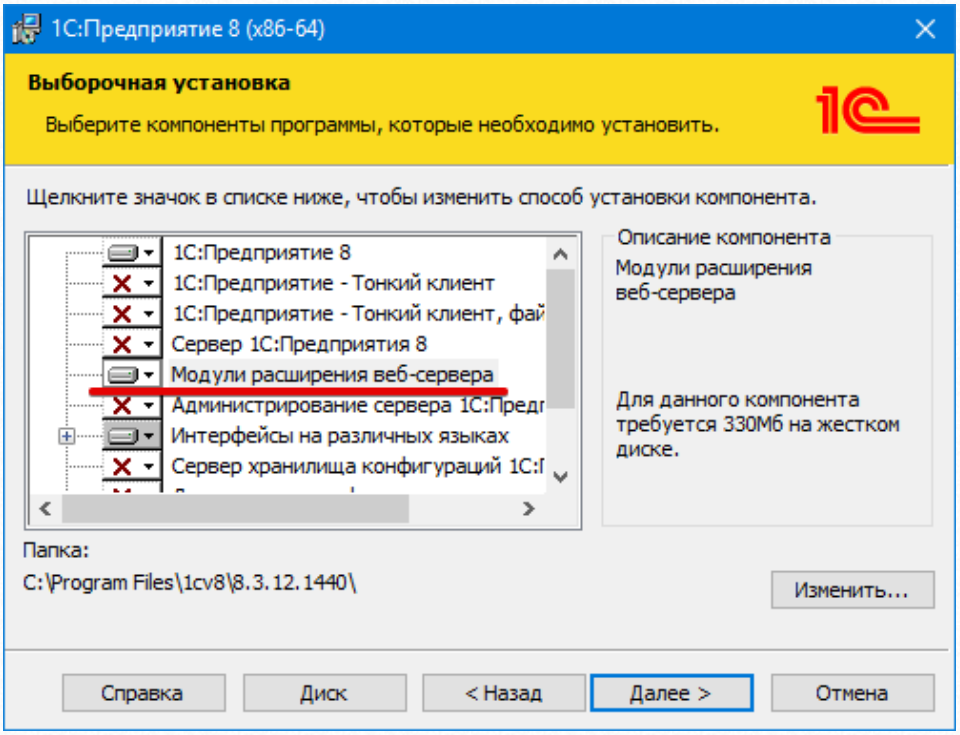


Затем, чтобы обновить конфигурацию нажмите также кнопку «Да» в следующем предупреждении.

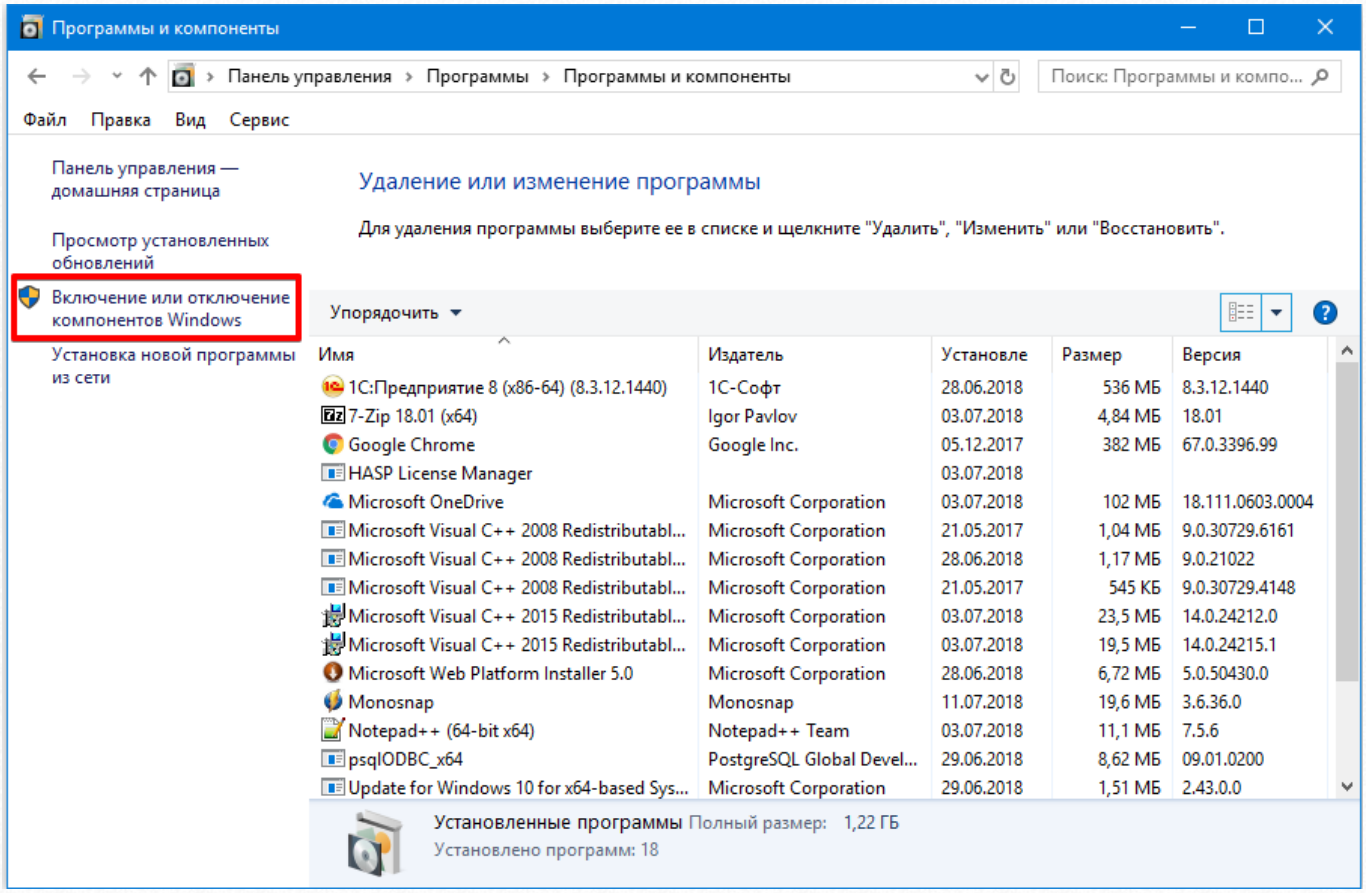


3.2. Публикация базы и настройка платформы в качестве OpenID-провайдера

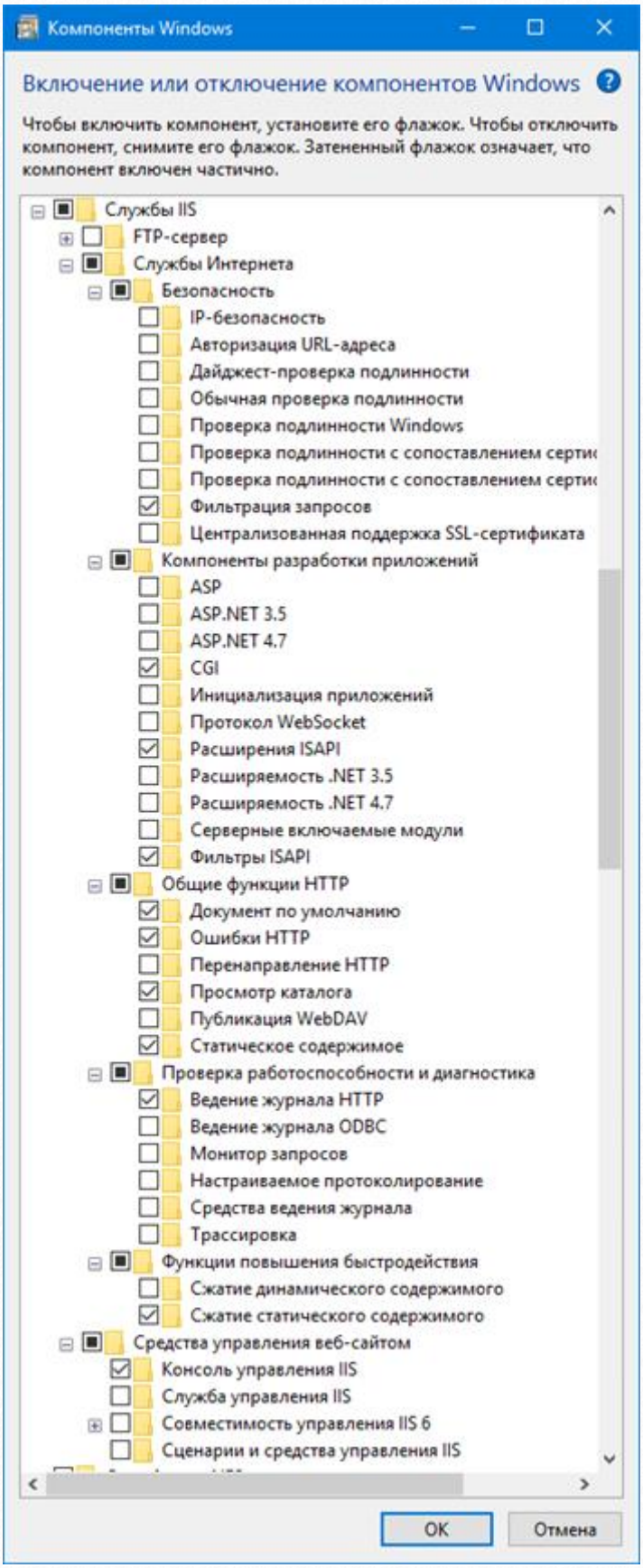
Для того, чтобы добавленный HTTP-сервис заработал необходимо опубликовать базу 1С. Для этого необходимо, чтобы был установлен компонент платформы «Модули расширения веб-сервера». Если он не был установлен запустите установщик платформы и добавьте нужный компонент.



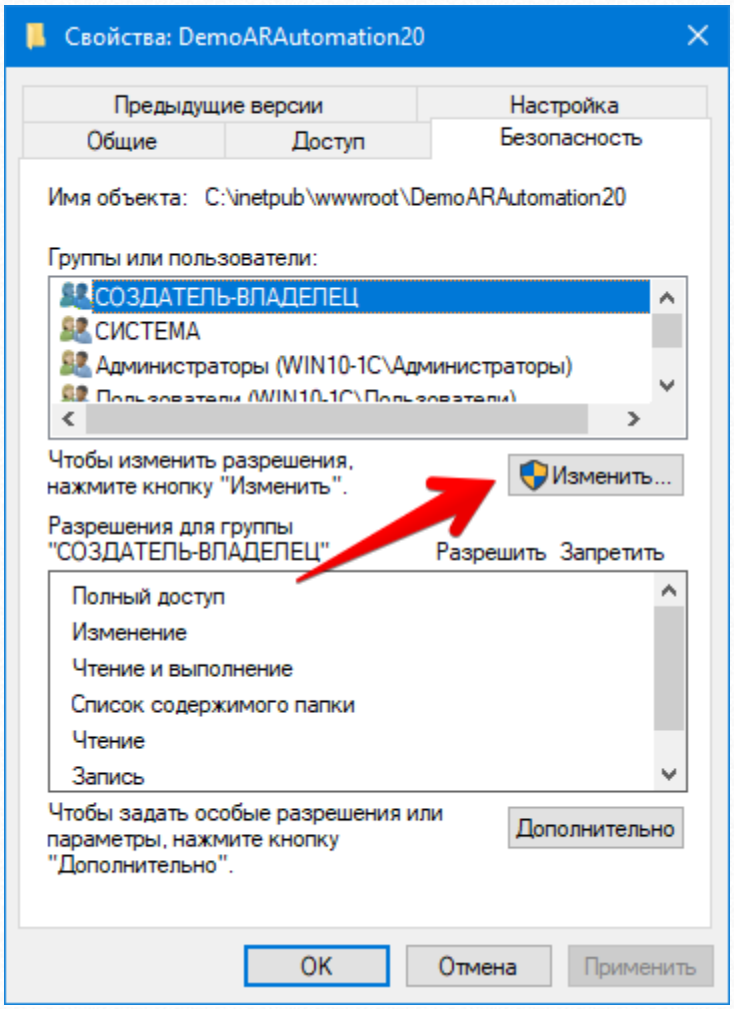
Также необходимо установить и настроить веб-сервер. В данном примере рассмотрим установку Internet Information Services (IIS) на ОС Windows 10. Его установка происходит штатными средствами ОС. Для этого откройте «Панель управления» → «Программы» → «Программы и компоненты» и нажмите на пункт в меню слева «Включение и отключение компонентов Windows»:



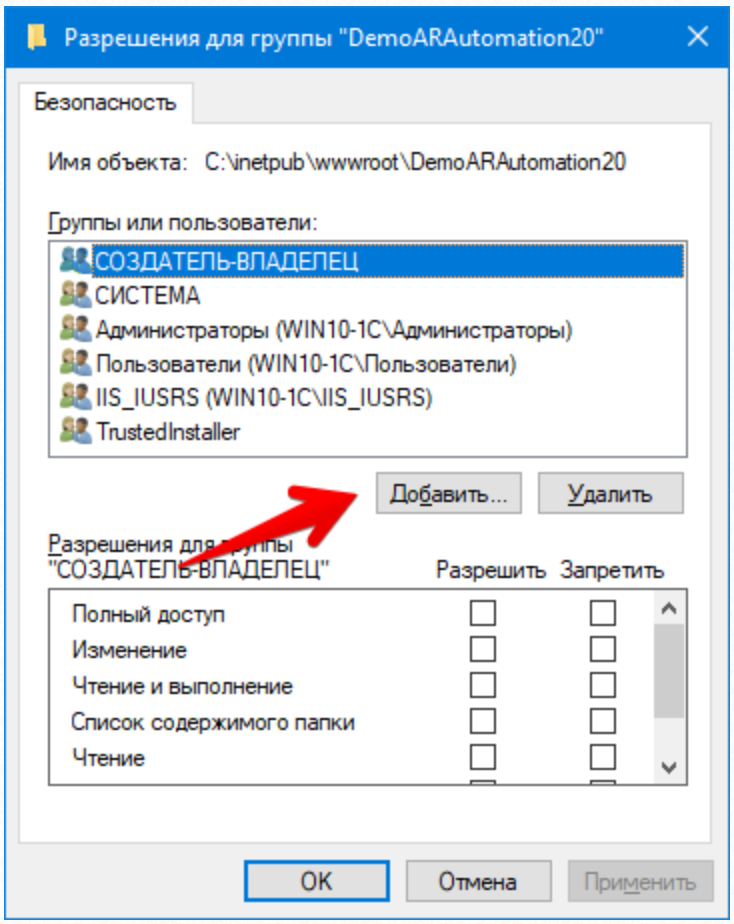
Необходимый набор компонентов указан на скриншоте. Отметив флажками недостающие компоненты нажмите «ОК».



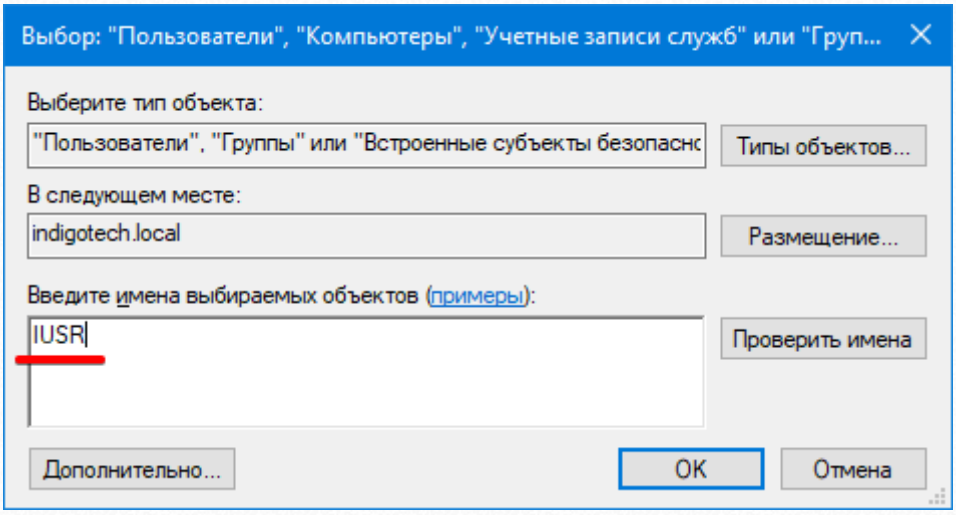
После установки компонентов перейдите к каталогу, в котором находится база 1С:Предприятие, из которой будет настраиваться синхронизация пользователей. Кликните по нему правой кнопкой мыши и выберите пункт «Свойства». Перейдите к вкладке «Безопасность» и нажмите кнопку «Изменить...».



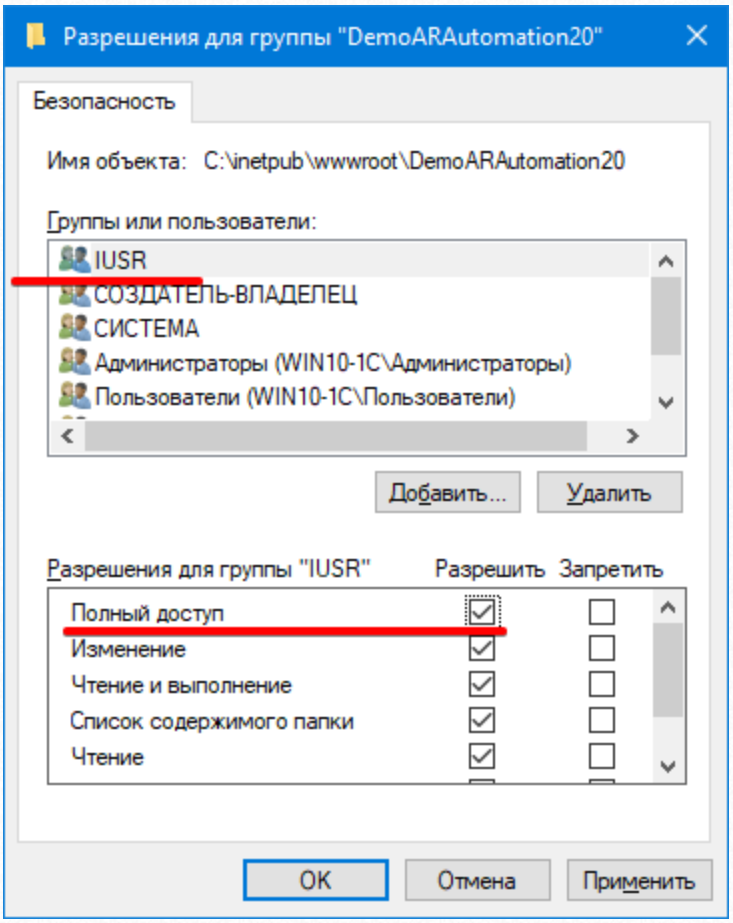
В окне «Разрешения для группы» нажмите на кнопку «Добавить...».



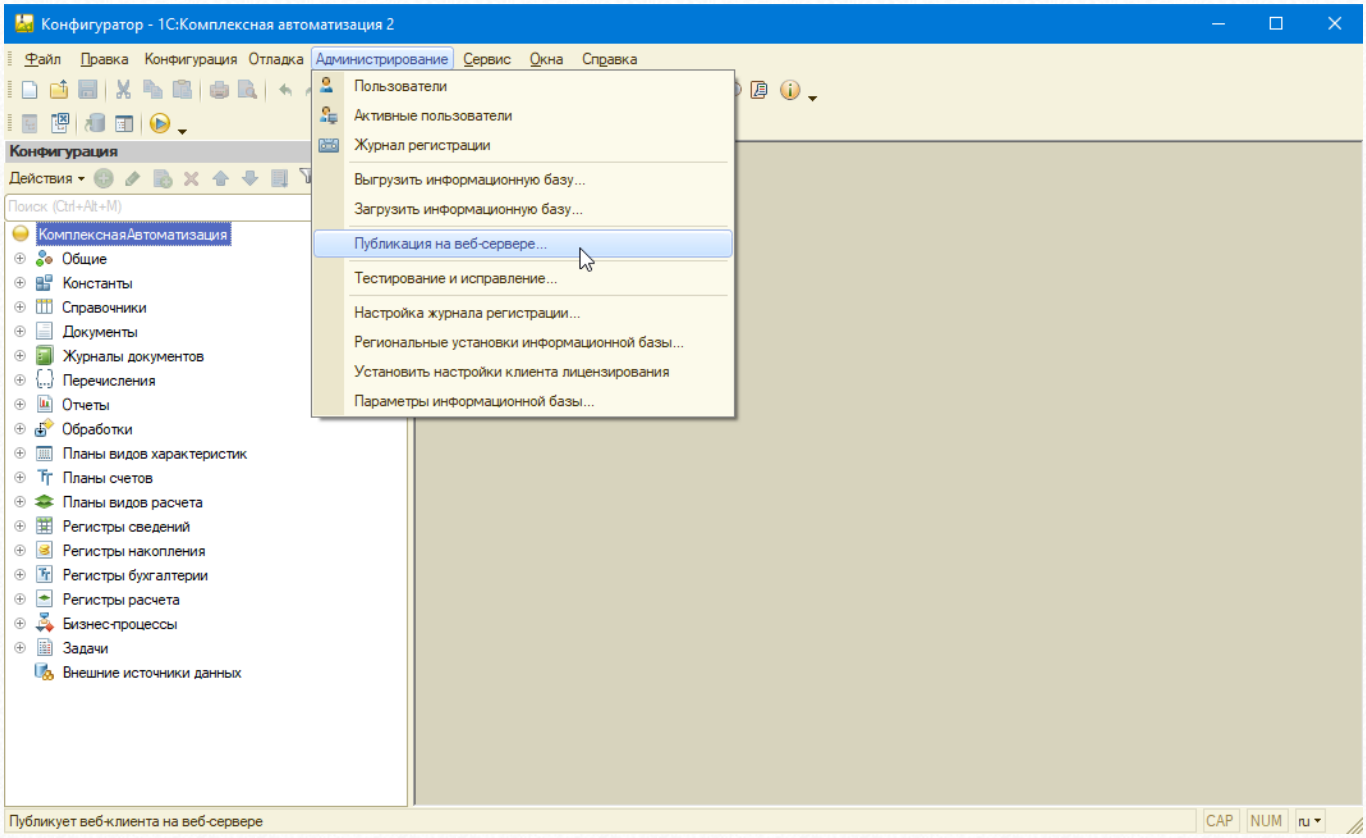
В окне «Выбор: Пользователи или Группы» в поле «Введите имена выбираемых объектов» введите IUSR и нажмите кнопку «ОК».



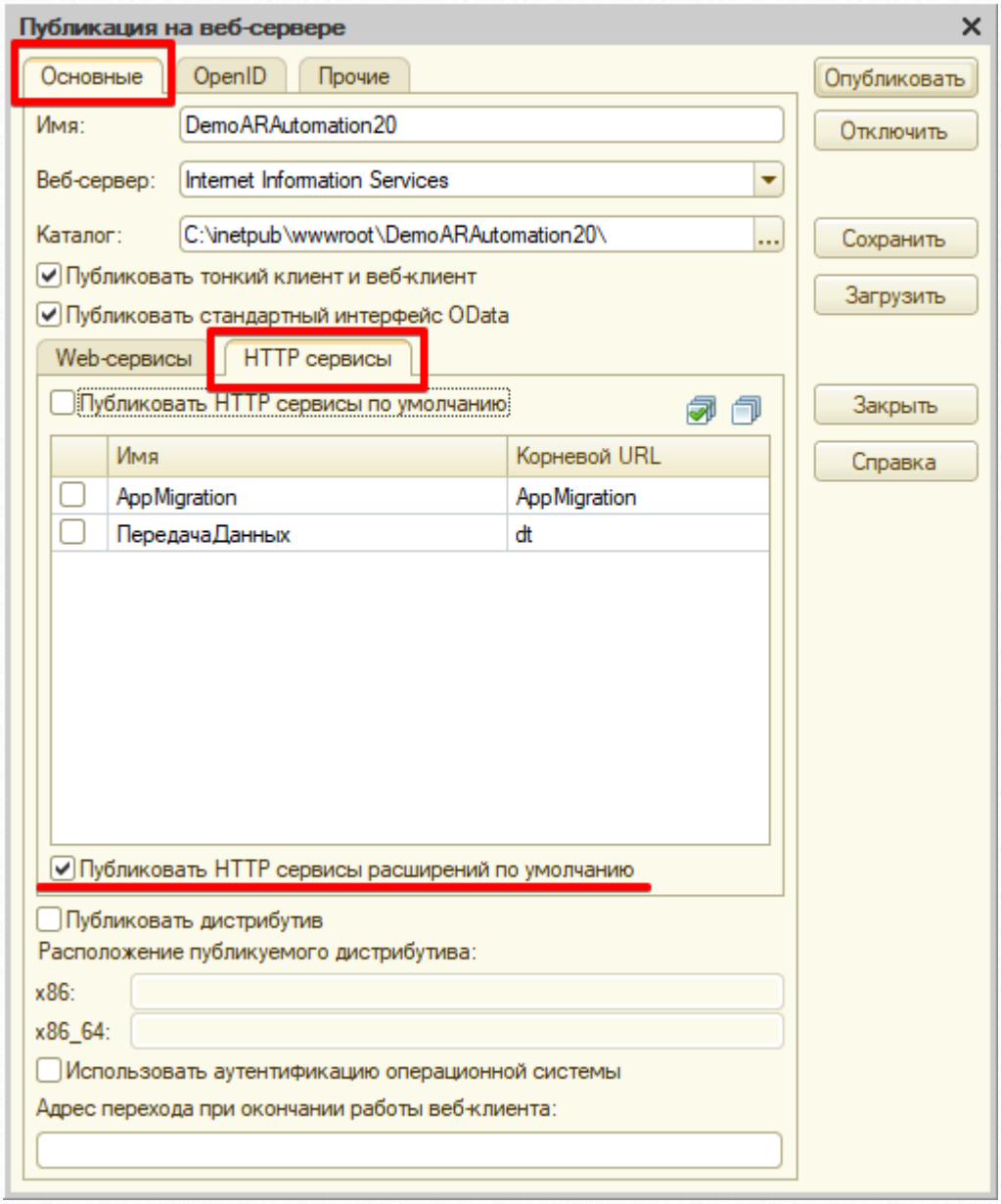
Вернувшись в окно «Разрешения для группы» разрешите пользователю IUSR полный доступ и нажмите «ОК».



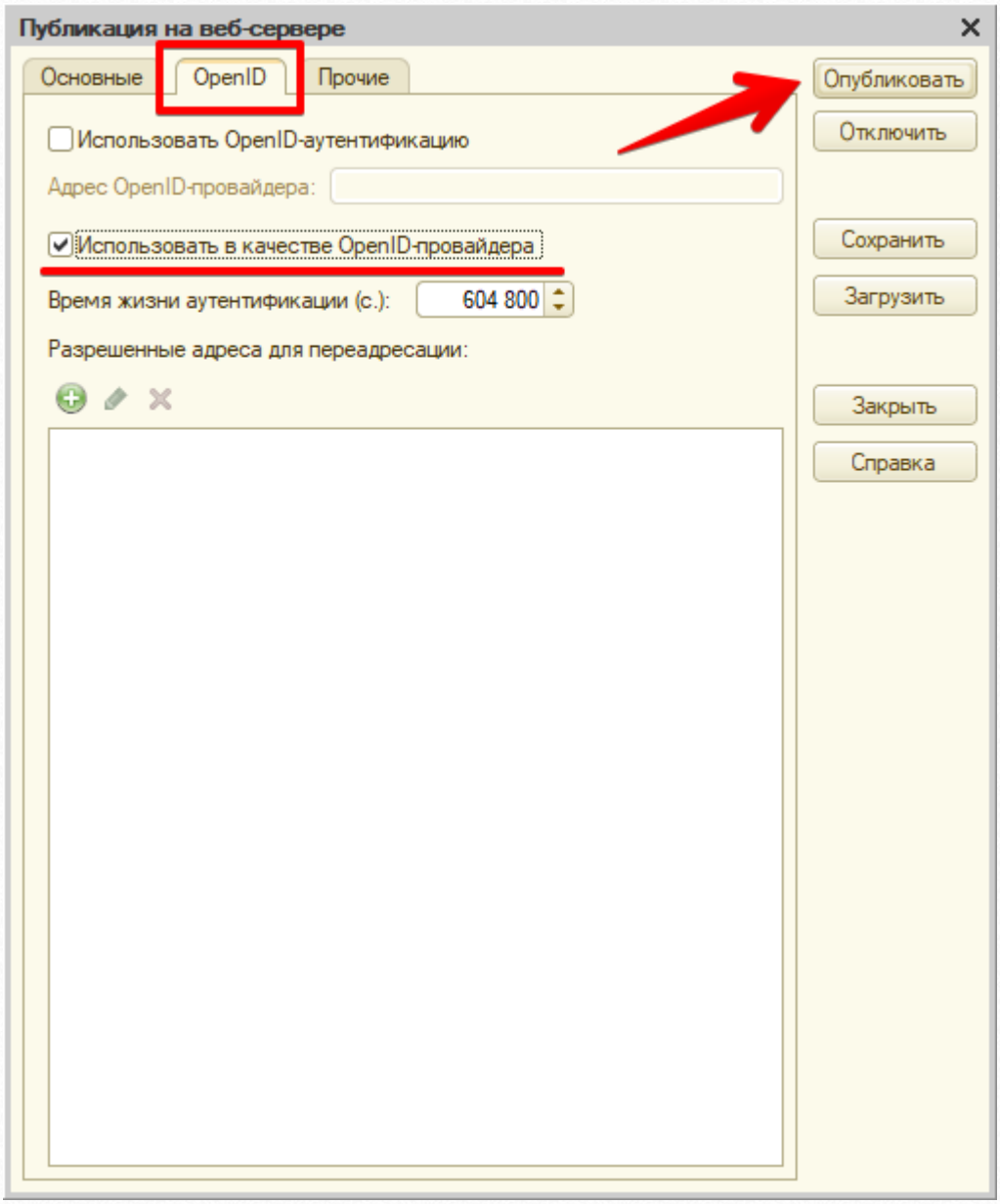
Для публикации базы на веб-сервере откройте 1С:Предприятие **с правами администратора** в режиме конфигуратора и в главном меню выберите пункт «Администрирование» → «Публикация на веб-сервере...».



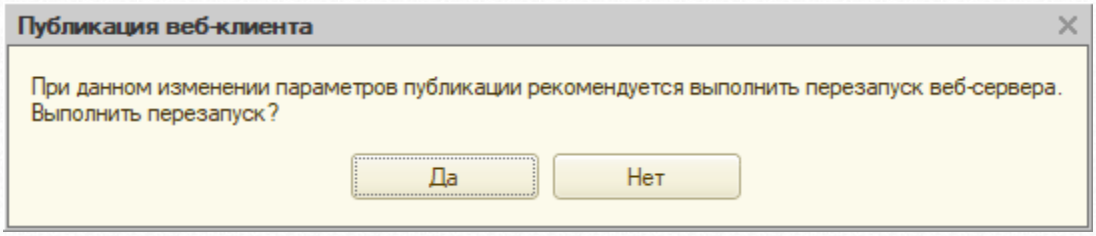
В открывшемся диалоге «Публикация на веб-сервере» перейдите на вкладку «Основные», а в ней на вкладку «HTTP сервисы» и установите флажок на пункте «Публиковать HTTP сервисы расширений по умолчанию».



Далее перейдите на вкладку «OpenID» и установите флажок на пункте «Использовать в качестве OpenID-провайдера». После этого нажмите на «Опубликовать».



После публикации будет предложено выполнить перезапуск веб-сервера. Нажмите «Да» и служба IIS перезапустится.



После публикации базы 1С можно будет настроить синхронизацию пользователей в системе тестирования INDIGO.