МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южный федеральный университет»
Институт компьютерных технологий и информационной безопасности
Кафедра информационной безопасности телекоммуникационных систем

Лабораторная работа №13
дисциплина «Администрирование операционных систем»
на тему: «Настройка службы сертификации»

Таганрог, 2021 г.

Цель работы: изучение принципов установки и настройки службы сертификации в операционных системах семейства Windows.

Оборудование: персональный компьютер.

Программное обеспечение: программный продукт виртуализации (VirtualBox, VMware Workstation), виртуальная машина с операционной системой Windows 10 актуальной версии, виртуальная машина с операционной системой Windows Server 2019 актуальной версии, виртуальная машина с операционной системой Windows Server 2019 актуальной версии без графического интерфейса.

Внимание! Для решения задач рекомендуется использовать результаты выполнения лабораторной работы №12.

Задачи:

1. Установить службы сертификации;

2. Настроить доменный корневой сервер сертификации;

3. Настроить шаблон выдаваемого сертификата для клиентских компьютеров;

4. Настроить шаблон выдаваемого сертификата для группы IT;

5. Оформить отчёт по работе.

Домашнее задание:

1. Внимательно изучить методические указания к выполнению лабораторной работы;

2. Подготовить необходимое программное обеспечение.

Порядок выполнения работы

1 Установить службы сертификации

- На машине DC установить роль «Службы сертификатов Active Directory». На этапе выбора компонентов и служб ролей всё оставить без изменений;

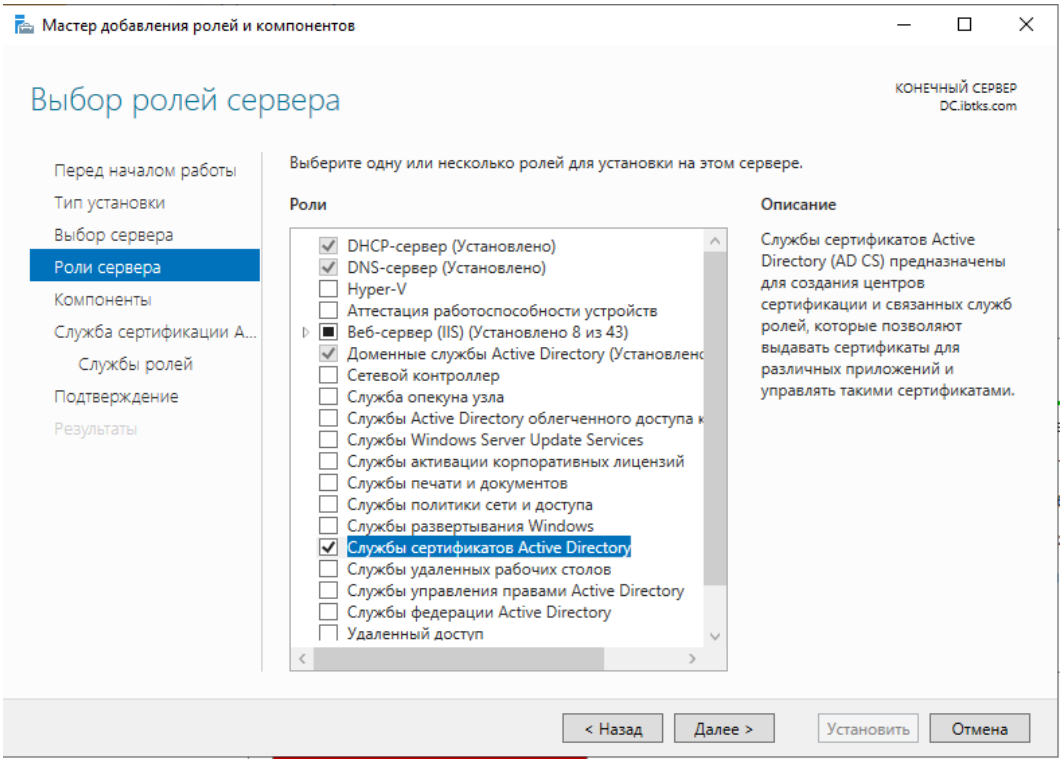

Рисунок 1 – Выбор ролей сервера

- На этапе «Службы сертификатов Active Directory» внимательно ознакомиться с представленной информацией. Далее, при выборе служб ролей установить галочку напротив пункта «Центр сертификации».

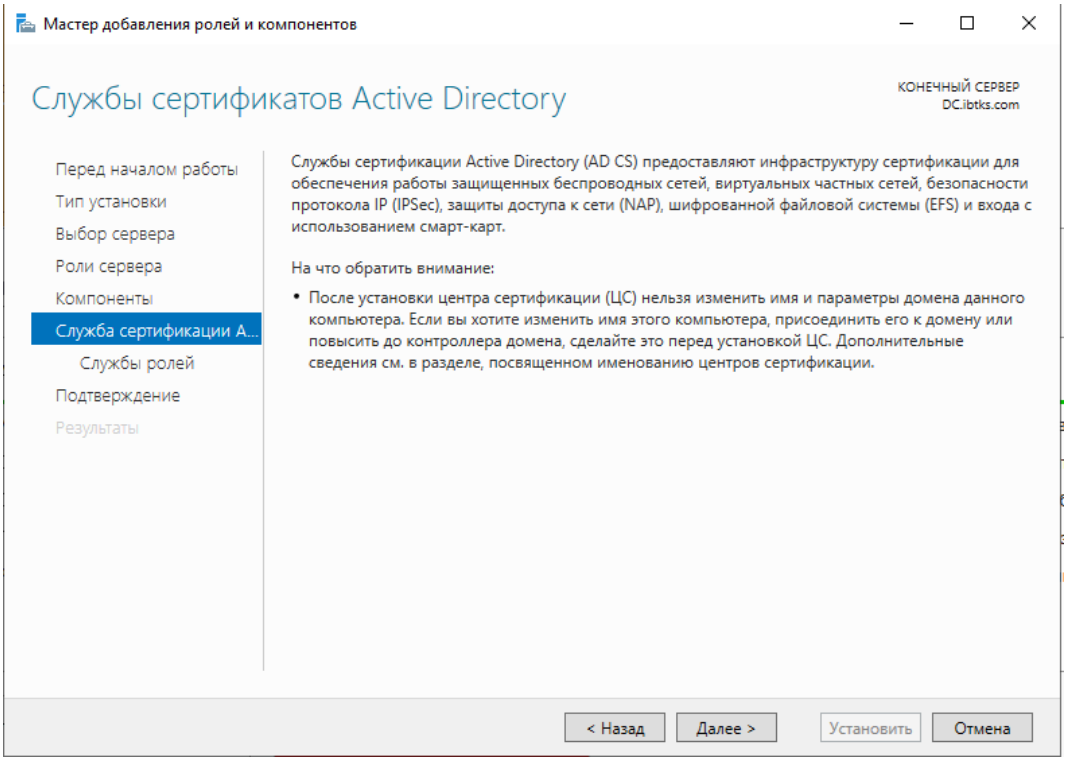

Рисунок 2 – Службы сертификатов Active Directory

2 Настроить доменный корневой сервер сертификации

- На машине DC в диспетчере серверов открыть «Службы сертификации Active Directory». Щёлкнуть по восклицательному знаку, затем нажать на ссылку «Настроить службы сертификатов Active Directory». На этапе выбора служб ролей для настройки поставить галочку напротив пункта «Центр сертификации» и нажать «Далее». На следующем этапе выбрать «ЦС предприятия». В качестве типа центра сертификации указать корневой ЦС. При выборе типа закрытого ключа установить маркер напротив пункта «Создать новый закрытый ключ» и нажать «Далее». Алгоритм и длину ключа оставить без изменений;

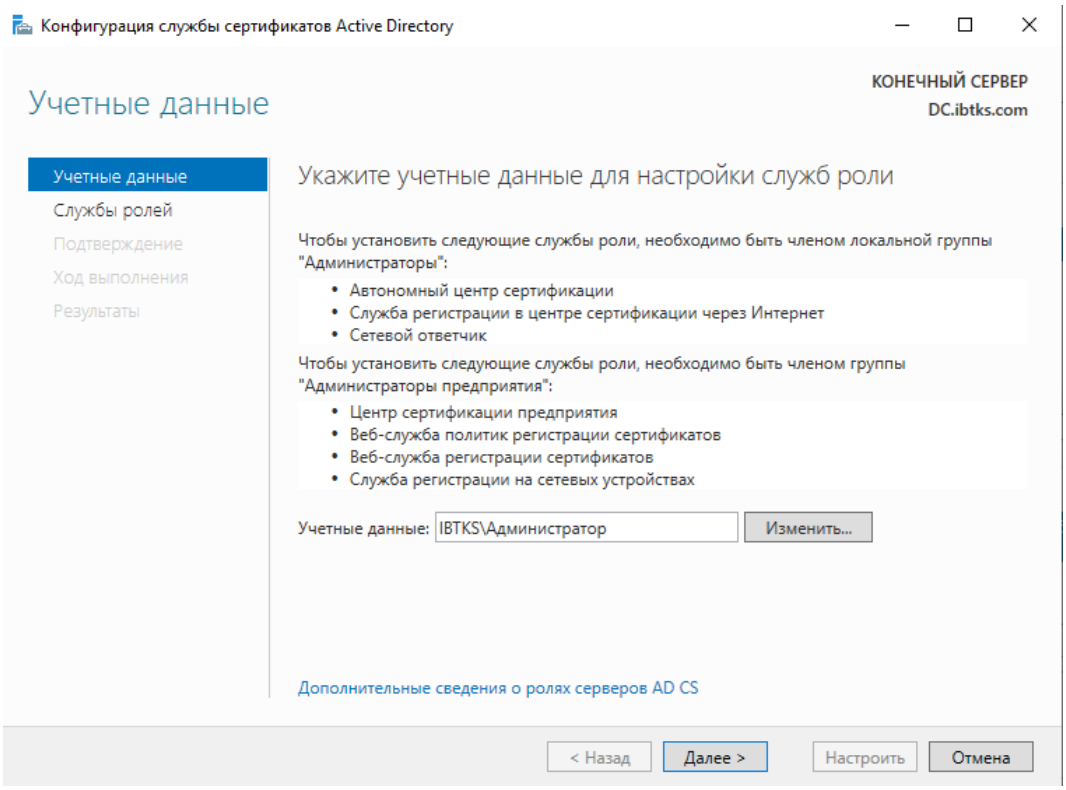

Рисунок 3 – Конфигурация службы сертификатов Active Directory

- На этапе настройки имени ЦС в качестве общего имени указать «IBTKS-CA». Установить период действия сертификата – 20 лет и нажать «Далее». Расположение баз данных оставить без изменений. На завершающем этапе внимательно проверить параметры настраиваемой службы сертификации и нажать «Настроить».

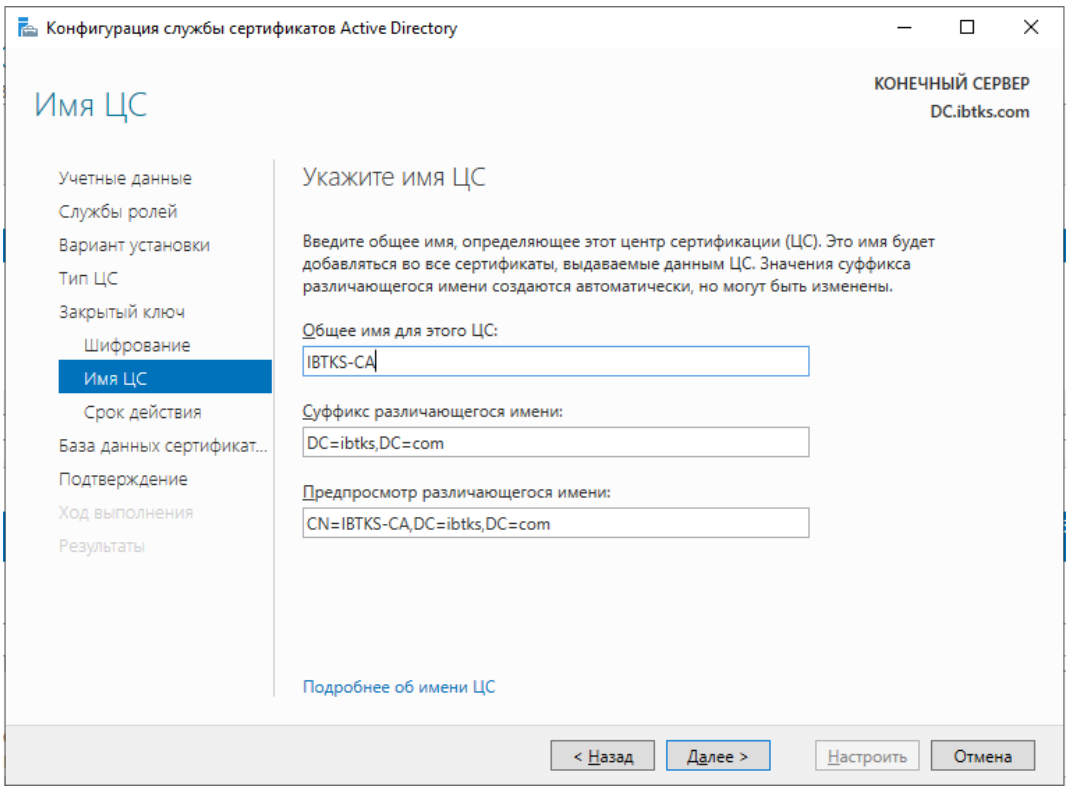

Рисунок 4 – Имя ЦС

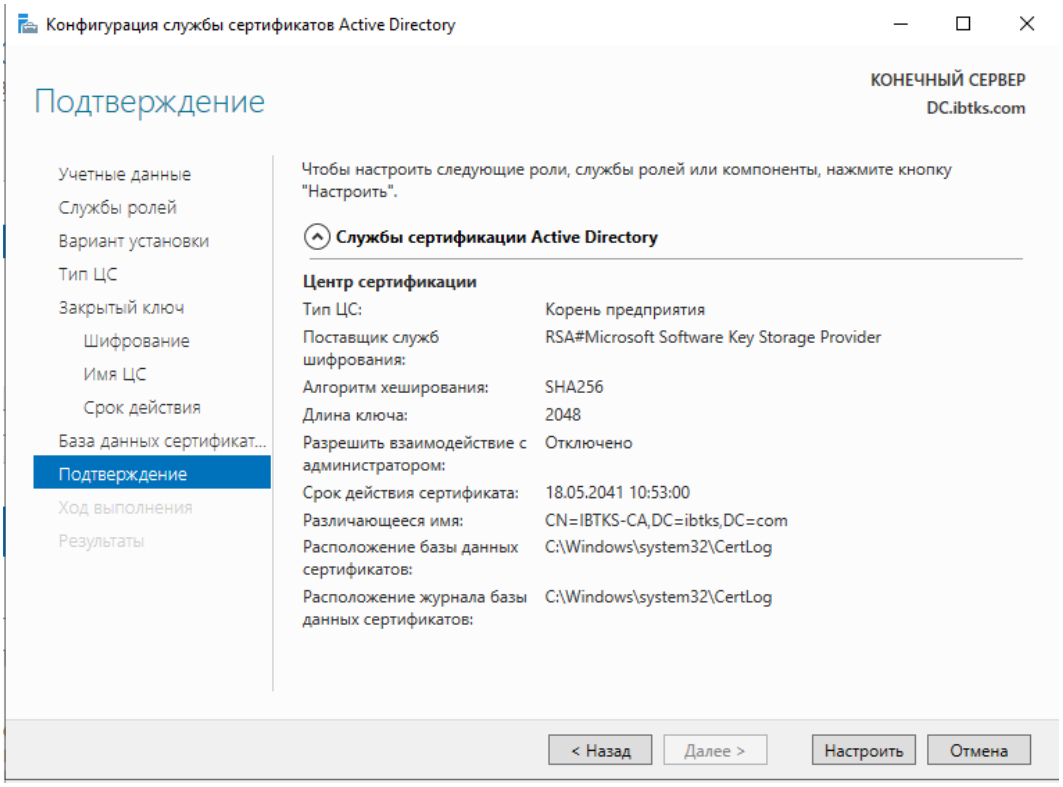

Рисунок 5 – Подтверждение

3 Настроить шаблон выдаваемого сертификата для клиентских компьютеров

- На машине DC в диспетчере серверов перейти в «Служба сертификации Active Directory», нажать правой кнопкой мыши на сервер DC и выбрать «Центр сертификации». Открыть созданный центр и перейти в папку «Шаблоны сертификатов»;

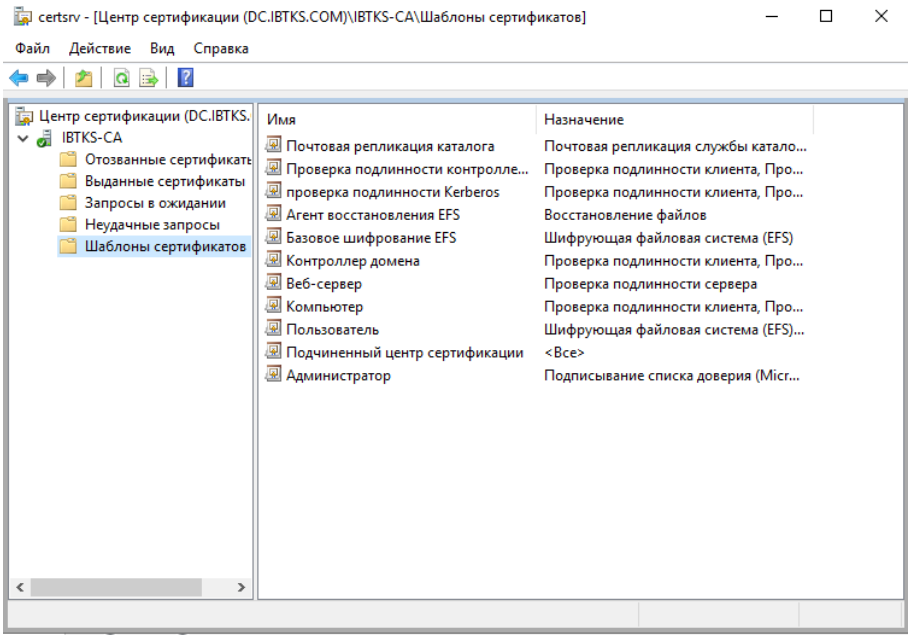

Рисунок 6 – Центр сертификации

- Нажать правой кнопкой мыши на папку «Шаблоны сертификатов» и выбрать «Управление». Найти в списке имя «Компьютер», нажать на него правой кнопкой мыши и выбрать «Скопировать шаблон». В окне «Свойства нового шаблона» во вкладке «Совместимость» всё оставить без изменений. Во вкладке «Общие» в качестве имени указать «Компьютер IBTKS», установить период действия 2 года, период обновления – 2 недели. Установить галочку напротив пункта «Опубликовать сертификат в Active Directory». Далее во вкладке «Безопасность» для групп и пользователей, прошедших проверку разрешить заявки и автоматическую подачу заявок.

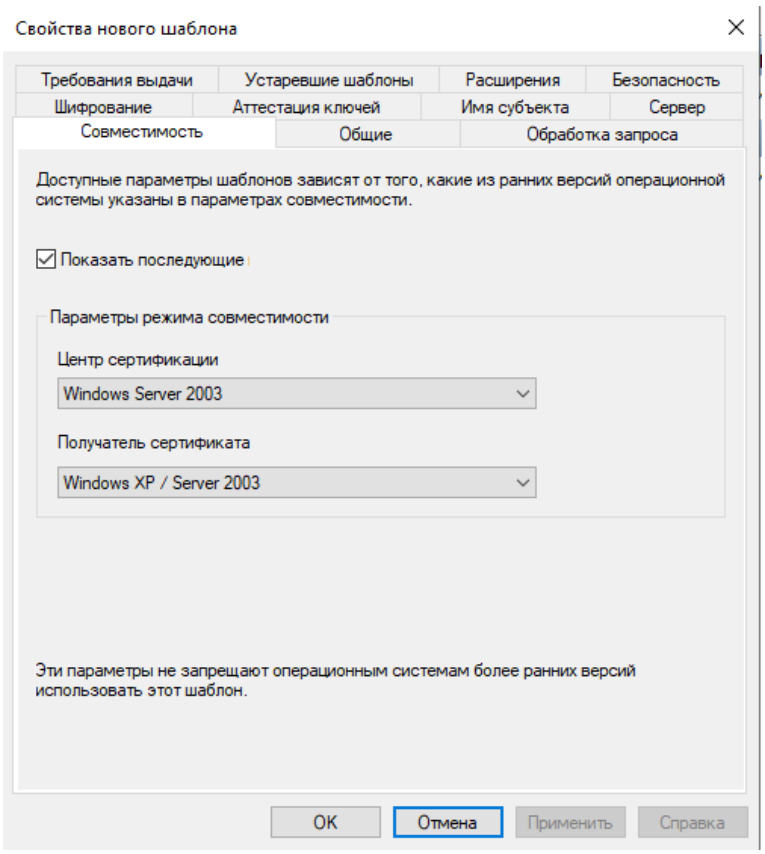

Рисунок 7 – Свойства нового шаблона

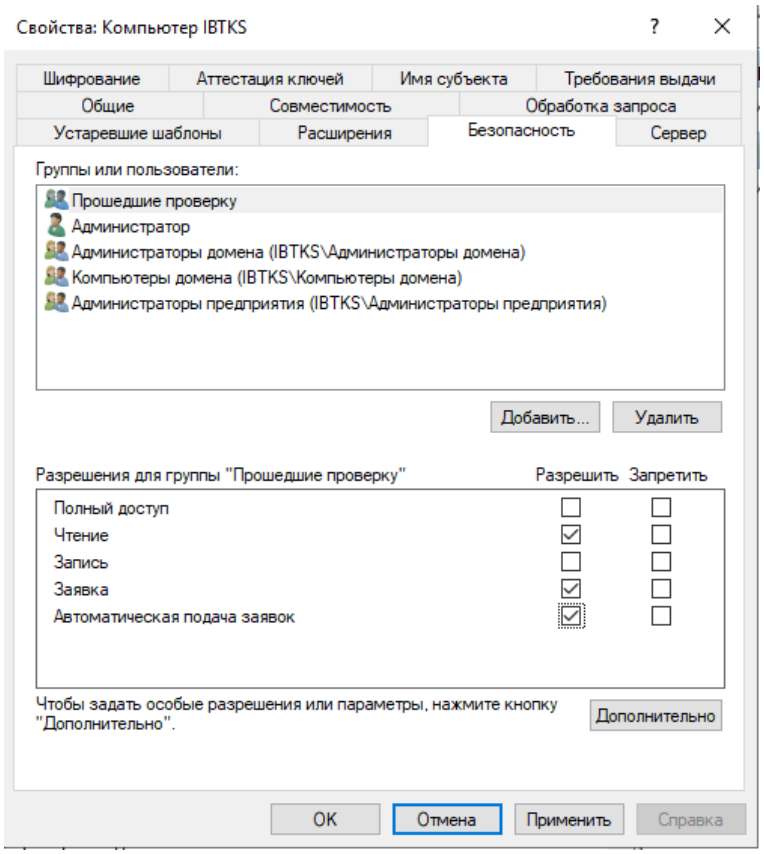

Рисунок 8 – Безопасность

4 Настроить шаблон выдаваемого сертификата для группы IT

- На машине DC в центре сертификации нажать правой кнопкой мыши на папку «Шаблоны сертификатов» и выбрать «Управление». Найти в списке имя «Пользователь» нажать на него правой кнопкой мыши и выбрать «Скопировать шаблон». В окне «Свойства нового шаблона» во вкладке «Совместимость» всё оставить без изменений. Во вкладке «Общие» в качестве имени указать «IT-IBTKS», установить период действия 3 года, а период обновления – 2 недели. Установить галочку напротив пункта «Опубликовать сертификат в Active Directory». Далее во вкладке «Безопасность» добавить группу «IT» и разрешить пользователям этой группы заявки и автоматическую подачу заявок;

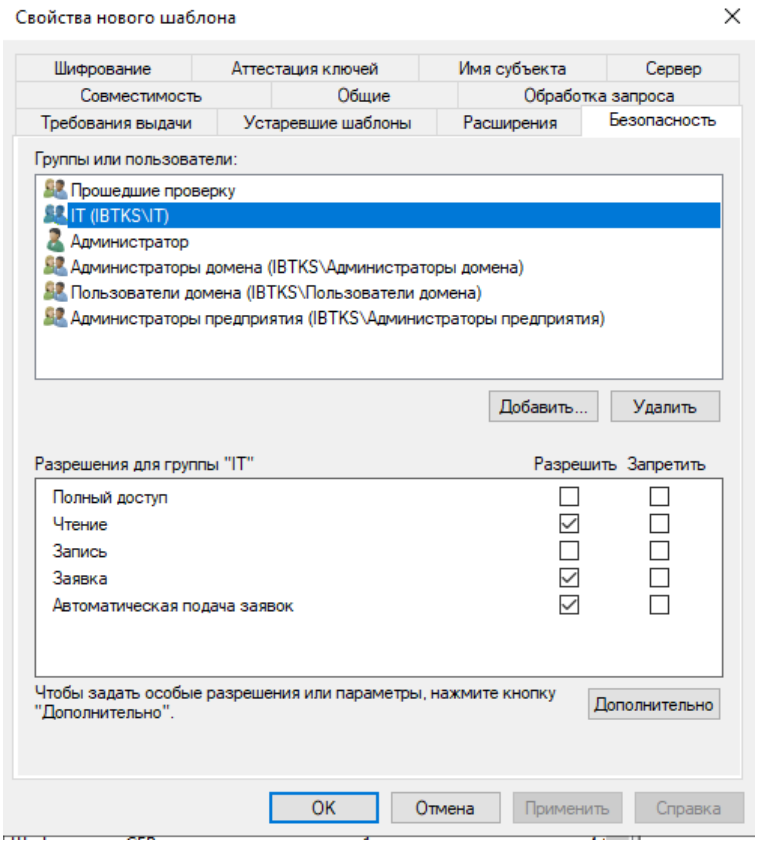

Рисунок 9 – Безопасность

- Перейти в окно центра сертификации, нажать правой кнопкой мыши по папке «Шаблоны сертификатов», выбрать пункт «Создать» и подпункт «Выдаваемый шаблон сертификата». В окне «Включение шаблонов сертификатов» выбрать шаблон «Агент регистрации», затем удерживая клавишу «Ctrl» выбрать шаблоны «Компьютер IBTKS» и «IT-IBTKS», затем нажать «ОК».

5. Оформить отчёт по работе

Отчет по лабораторной работе должен содержать:

- Титульный лист;
- Цель работы;
- Список задач;
- Ход работы;
- Вывод.

Отчёт должен содержать скриншоты, подтверждающие выполнение задач.

В процессе защиты лабораторной работы необходимо продемонстрировать работоспособность виртуальных машин, подтверждающую выполнение задач.