**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ**

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ **«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. В. Г. ШУХОВА»**

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

**ЛАБОРАТОРНАЯ РАБОТА №5**

**Дисциплина: Информационная безопасность**

**Тема: Инфраструктура с открытыми ключами**

Выполнил: ст. группы ВТ-31

Подкопаев Антон Валерьевич

Проверил: ст. пр. ПОВТиАС

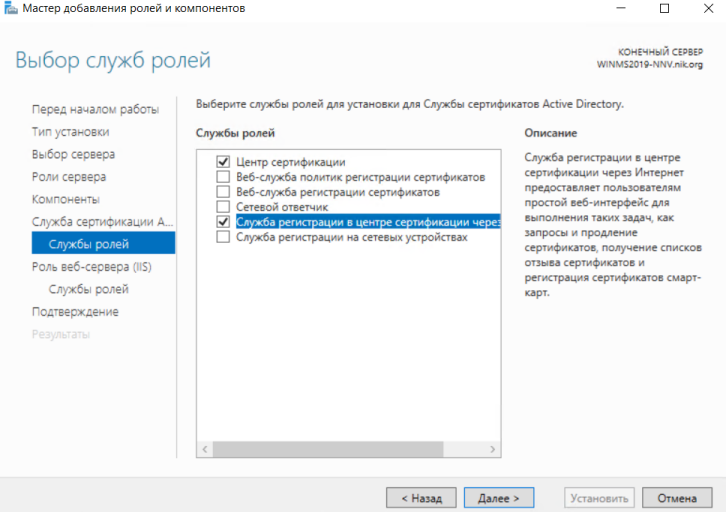
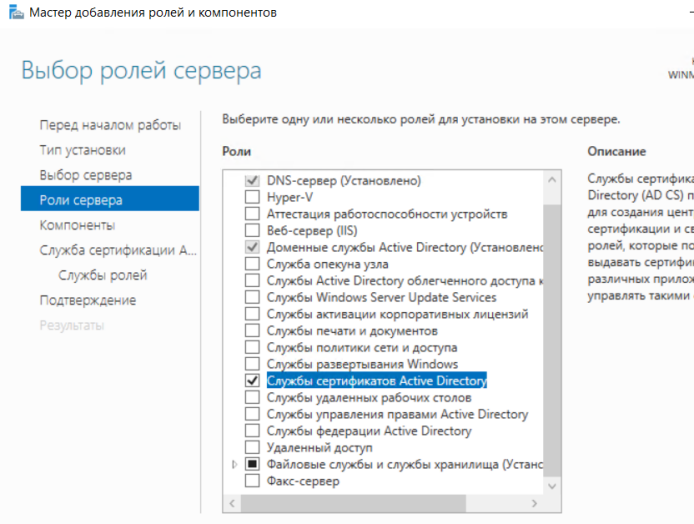
Гвоздевский Игорь Николаевич

**Белгород 2019**

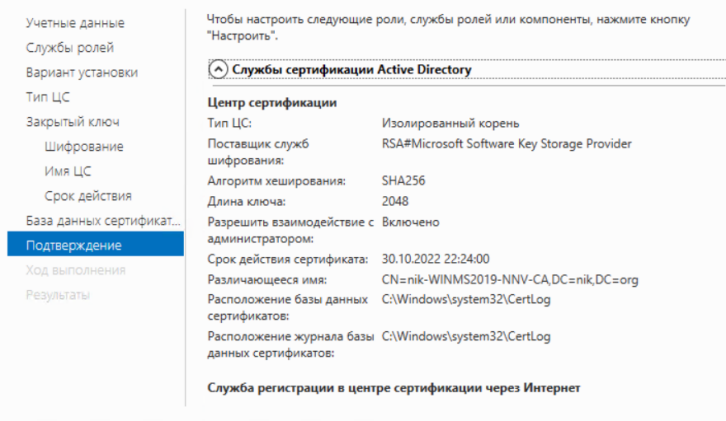
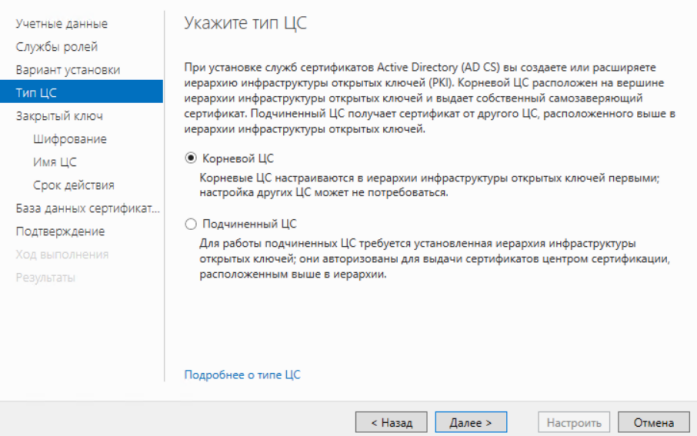
**Цель работы:** изучить методы работы инфраструктуры с открытыми ключами (PKI)

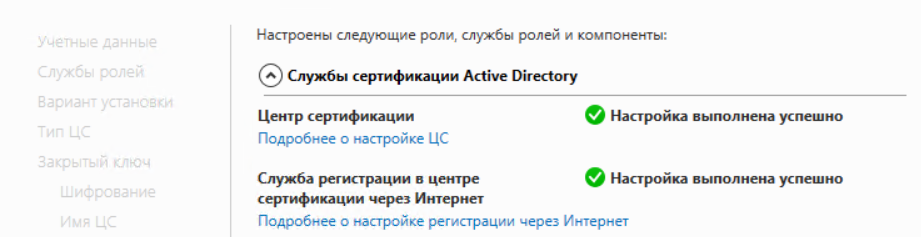
**Ход работы**:

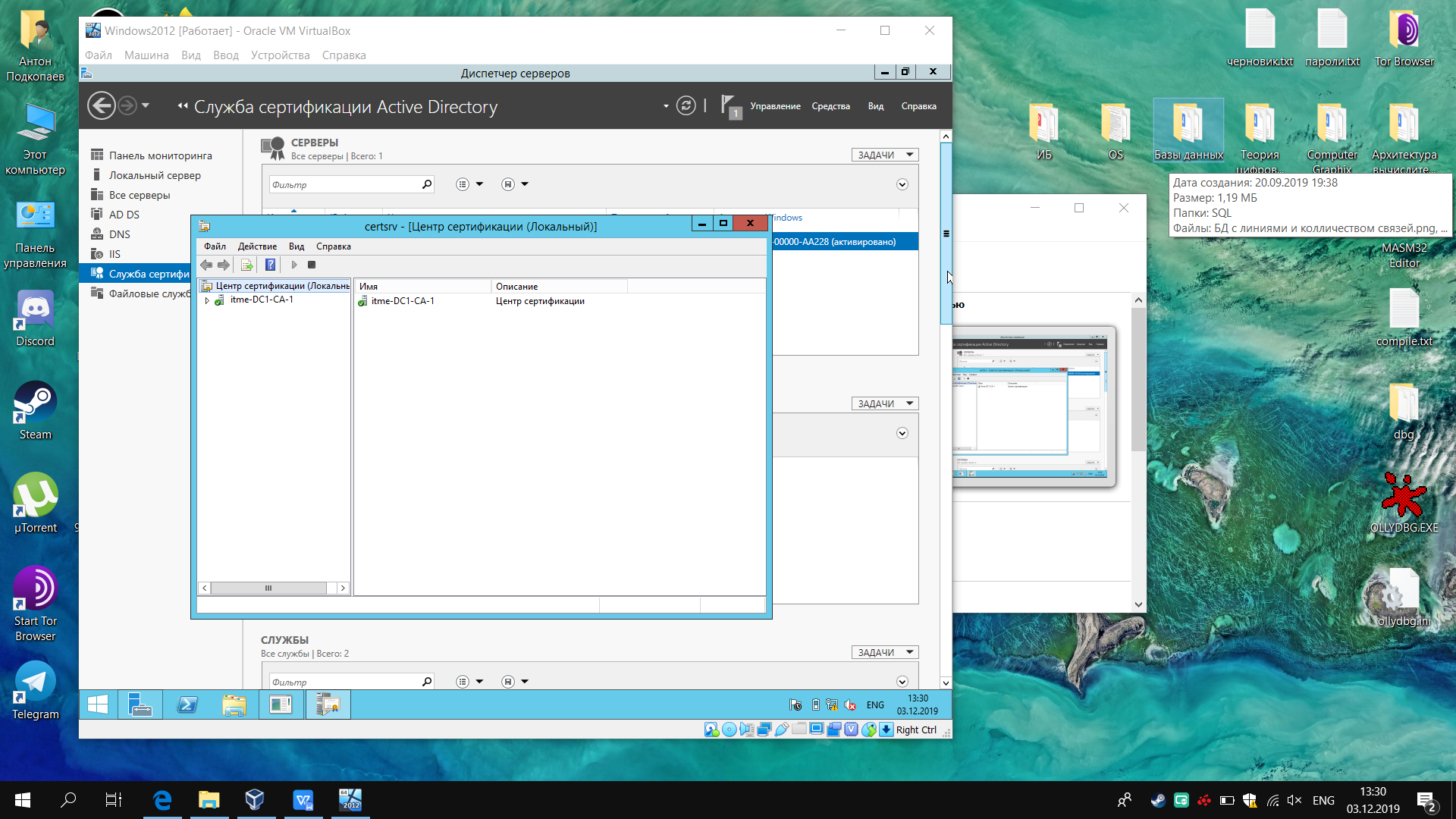
**1** **Развернуть структуру PKI на базе сервера Windows**;



**2** **Произвести настройку центра сертификации**;

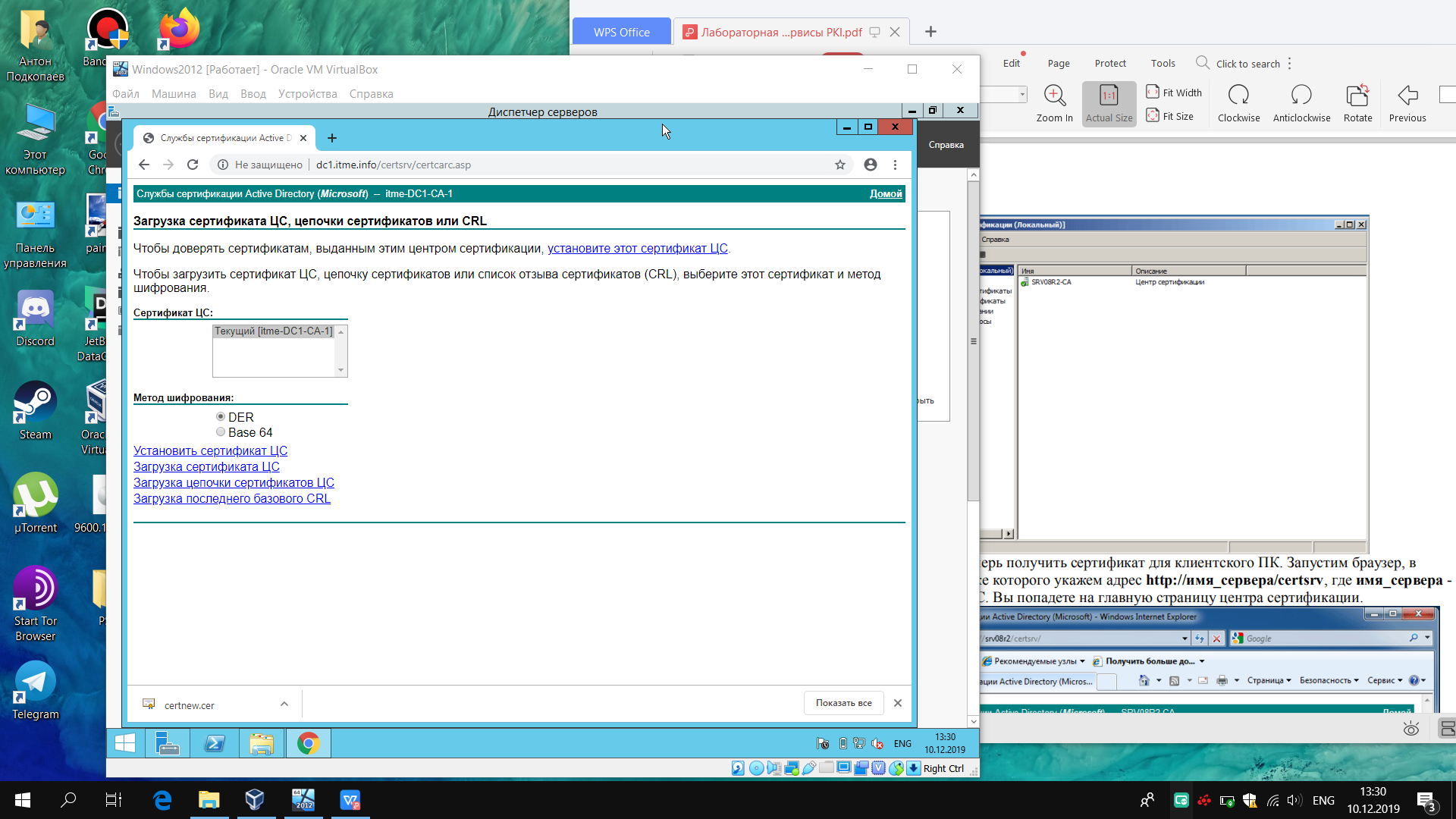


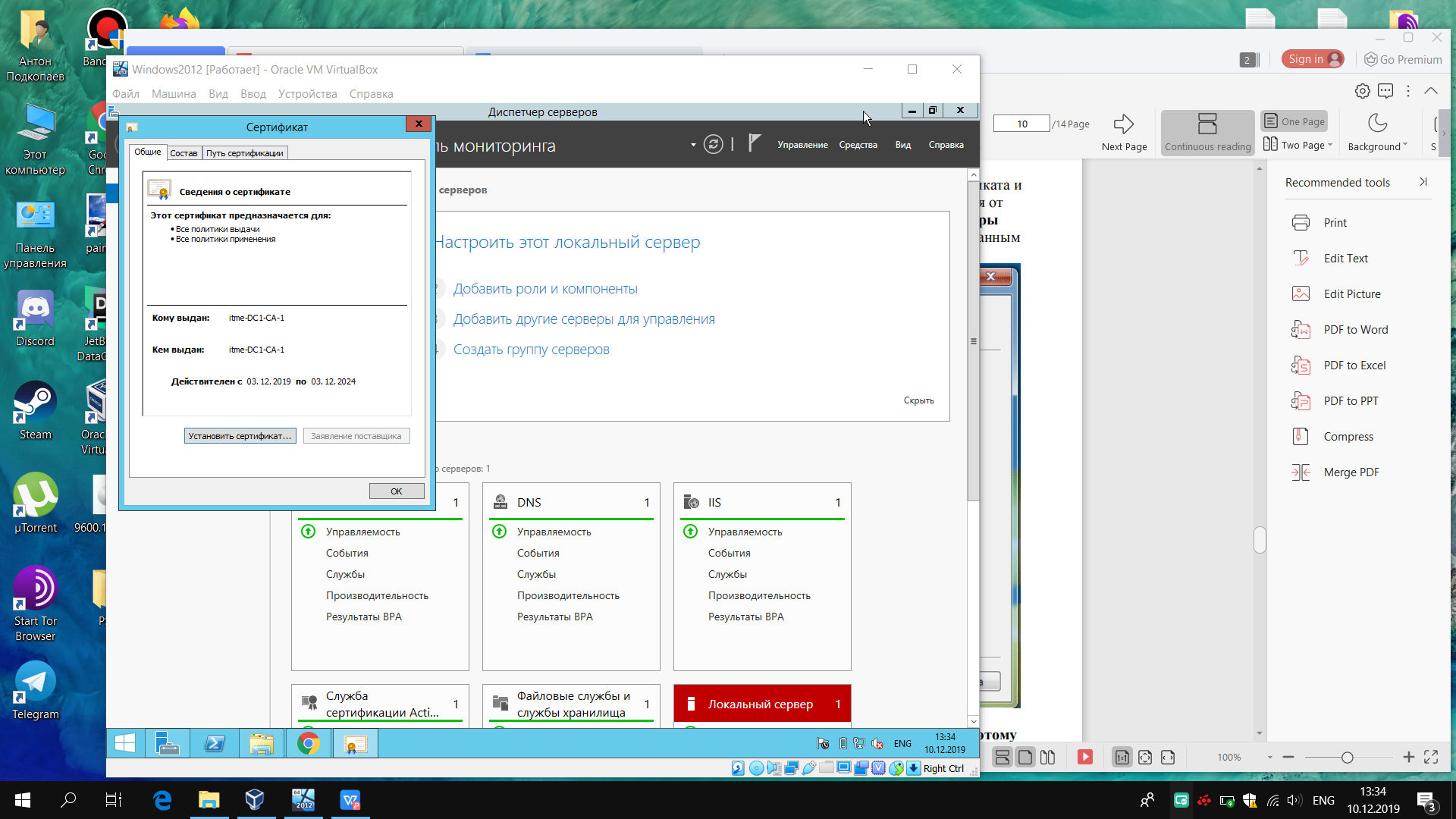




**3** **Установить сгенерированный корневой сертификат в хранилище сертификатов**;

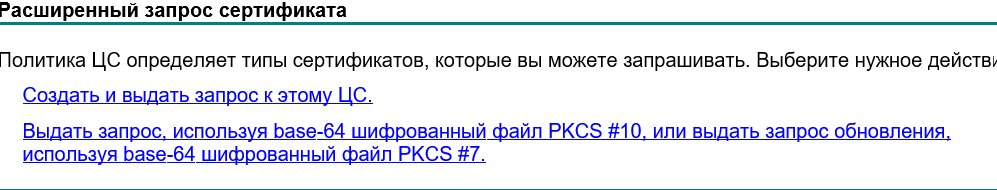


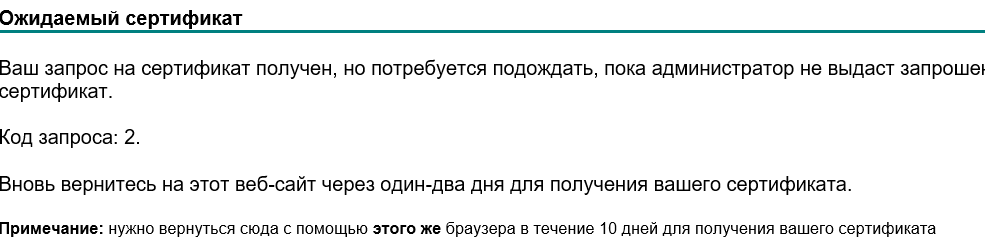


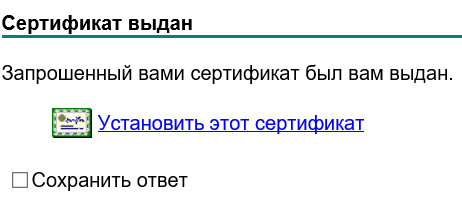
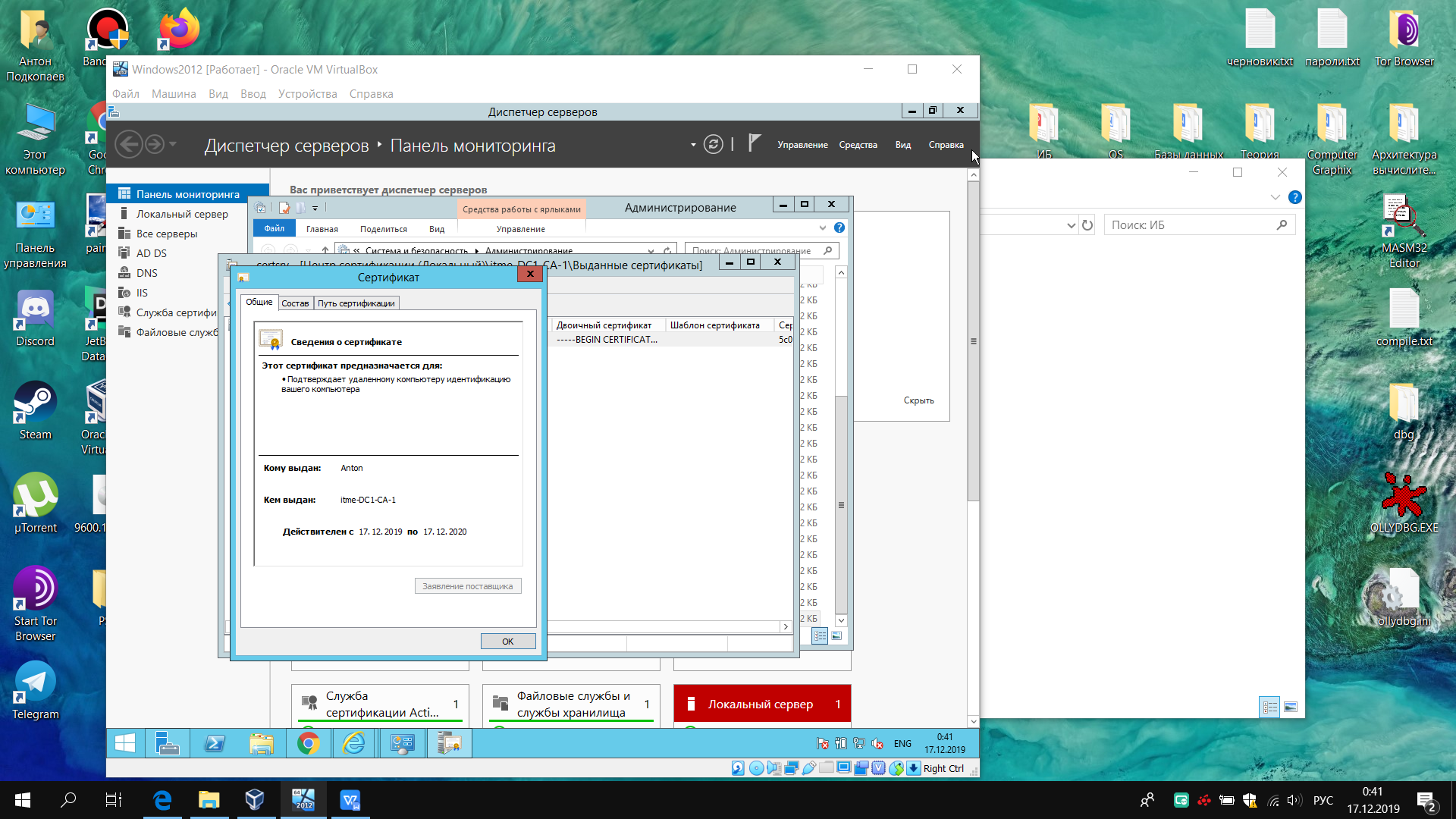


**4** **Сгенерировать новый сертификат для локального ПК, либо виртуальной клиентской**

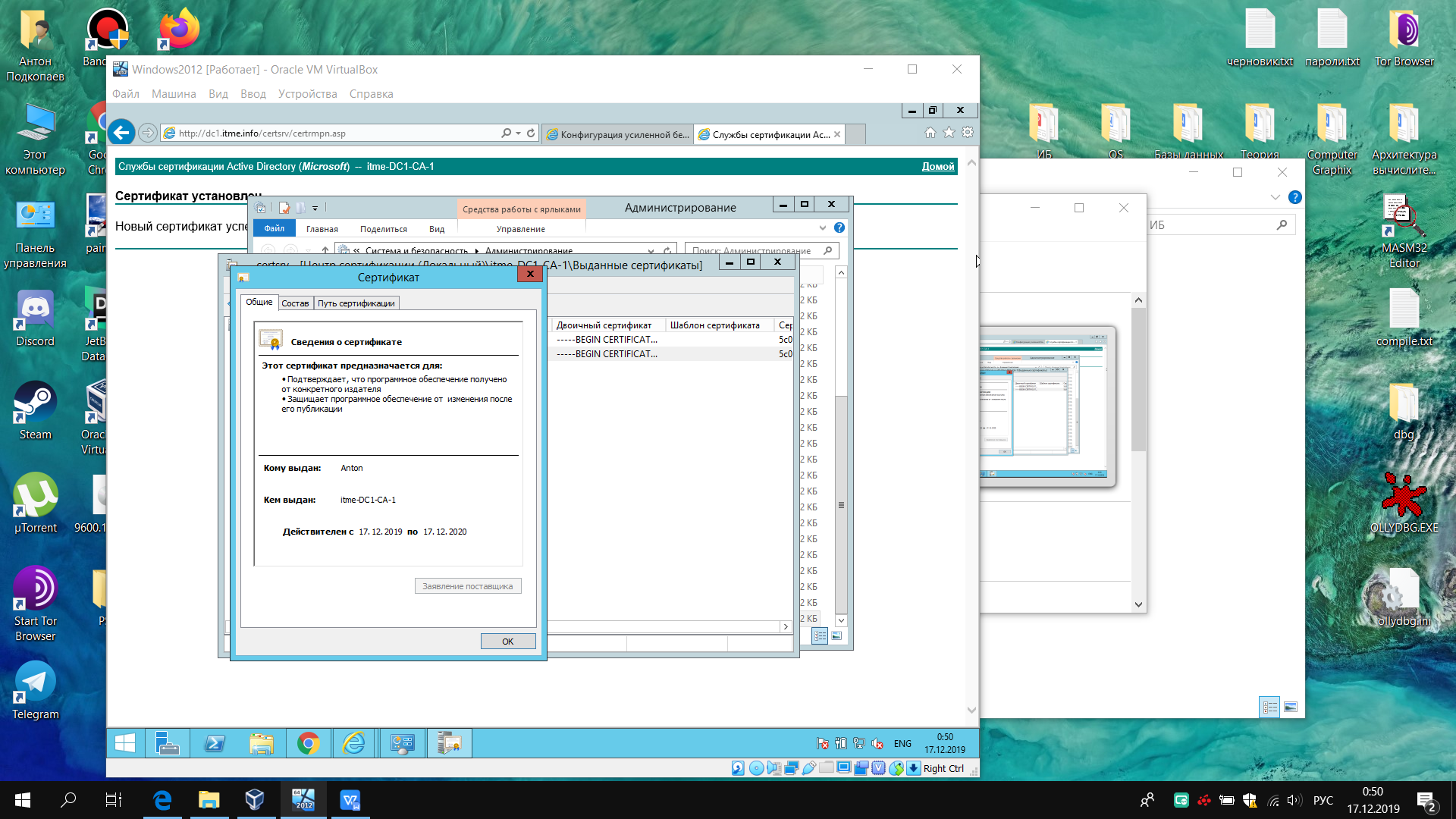
**машины**;





**5** **Сгенерировать различные сертификаты для клиентских приложений**.



Вывод: научились разворачивать и работать с PKI,установливать сгенерированный корневой сертификат в хранилище сертификатов и генерировать различные сертификаты для клиентских приложений.

Контрольные вопросы:

1 Как выглядит процедура получения сертификата при использовании web-страницы

формирования запроса?

2 Каким образом используется сертификат пользователя при шифровании в EFS? Каким

требованиям он должен удовлетворять?

3 Какой формат позволяет экспортировать сертификат вместе с путем сертфиикации?

4 По каким причинам необходимо разделение ключевых пар, используемых для подписи и

шифрования?

5 Используется ли в S/MIME технология «цифрового конверта»?

6 В чем отличие расширений сертификата Key Usage и Extended Key Usage? Для чего они

используются?

7 Каким образом осуществляется проверка статуса сертификатов? Каким образом

пользователи могут узнать источник информации о статусе данного сертификата?