

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ «БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
(БГТУ им. В.Г.Шухова)**

Лабораторная работа №5
дисциплина «Информационная безопасность»
по теме «Инфраструктура с открытыми ключами (PKI)»

Выполнил: студент группы ВТ-31
Проверил:

Макаров Д.С.
Гвоздевский И.Н.

Белгород 2019

Лабораторная работа №5

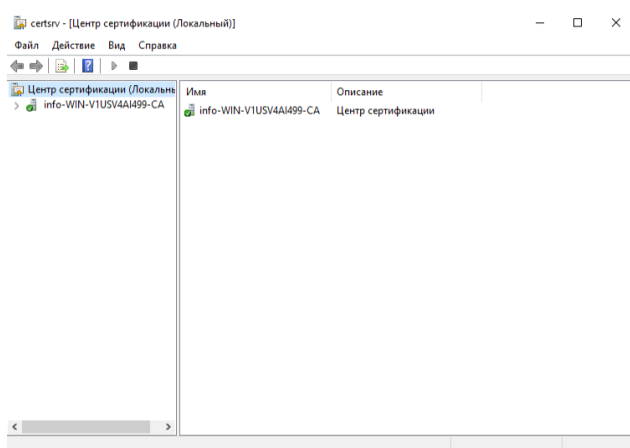
«Инфраструктура с открытыми ключами (PKI)»

Практическое задание:

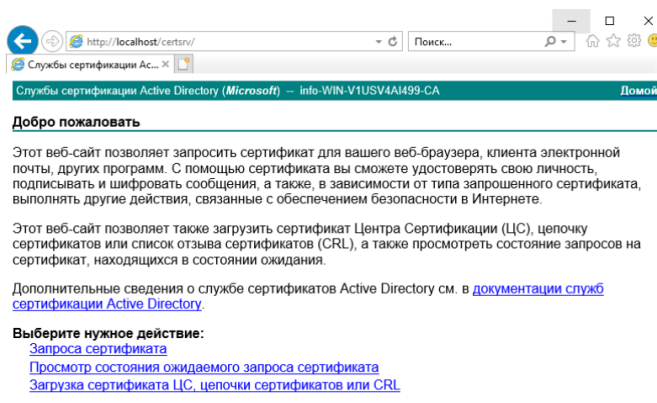
1. Развернуть структуру PKI на базе сервера Windows;
2. Произвести настройку центра сертификации;
3. Установить сгенерированный корневой сертификат в хранилище сертификатов;
4. Сгенерировать новый сертификат для локального ПК, либо виртуальной клиентской машины;
5. Сгенерировать различные сертификаты для клиентских приложений.

Ход работы

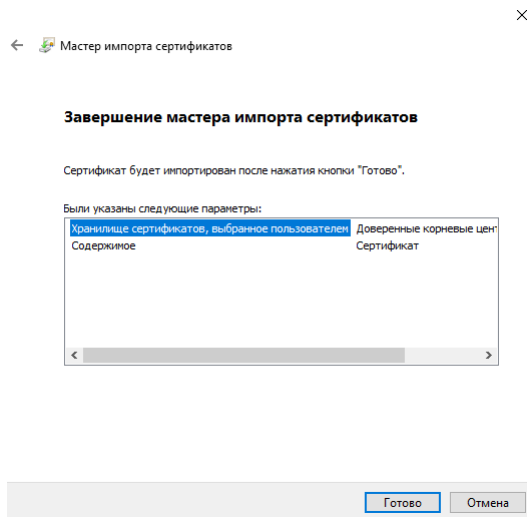
1. Добавлена роль центра сертификации.



2. HTTP страница службы сертификации AD.



3. Получен и установлен сертификат центра сертификации.



4. Окно расширенного запроса пользовательского сертификата.

Расширенный запрос сертификата

Шаблон сертификата:

Пользователь ▼

Параметры ключа:

☒ Создать новый набор ключей ☐ Использовать существующий набор ключей

CSP: Microsoft Enhanced Cryptographic Provider v1.0 ▼

Использование ключей: ☒ Exchange

Размер ключа: 2048 Минимальный: 384 Максимальный: 16384 (стандартные размеры ключей: 812 1024 2048 4096 8192 16384)

☒ Автоматическое имя контейнера ключа ☐ Заданное пользователем имя контейнера ключа

☒ Пометить ключ как экспортируемый

☐ Включить усиленную защиту закрытого ключа

Дополнительные параметры:

Формат запроса: ☐ CMC ☒ PKCS10

Алгоритм хеширования: md5 ▼

Используется только для подписания запроса.

☐ Сохранить запрос

Атрибуты: < >

Понятное имя:

Выдать >