**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 №4**

**Дисциплина: Информационная безопасность**

**Тема: Принцип работы SSL**

Выполнил: ст. группы ВТ-31

Подкопаев Антон Валерьевич

Проверил: ст. пр. ПОВТиАС

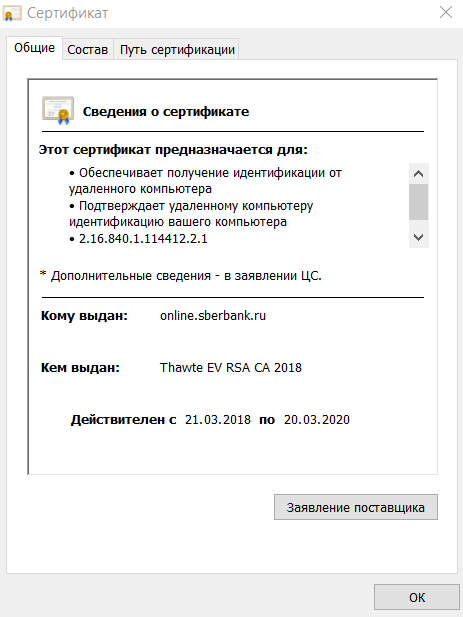
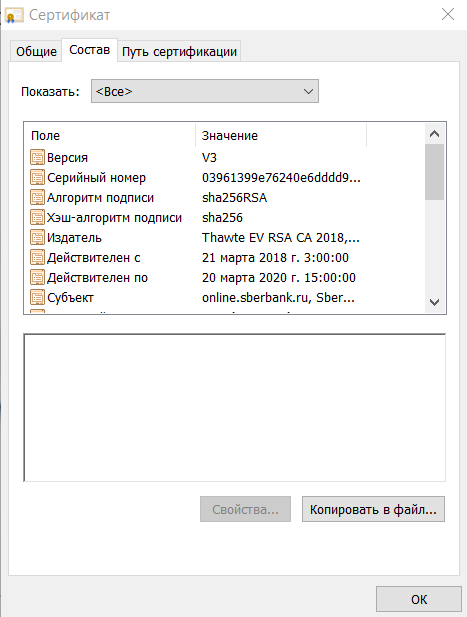
Гвоздевский Игорь Николаевич

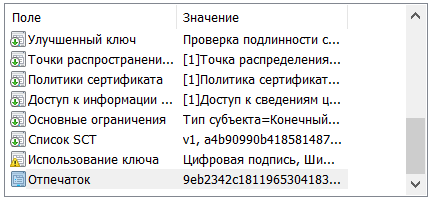
**Белгород 2019**

**Цель работы:** Получение и работа с SSL сертификатом.

**Ход работы**

1. Посмотрите параметры сертификата "электронной сберкассы" Сбербанка



1. Опишите, кем, на какой срок и для какого субъекта сертификат был выдан.



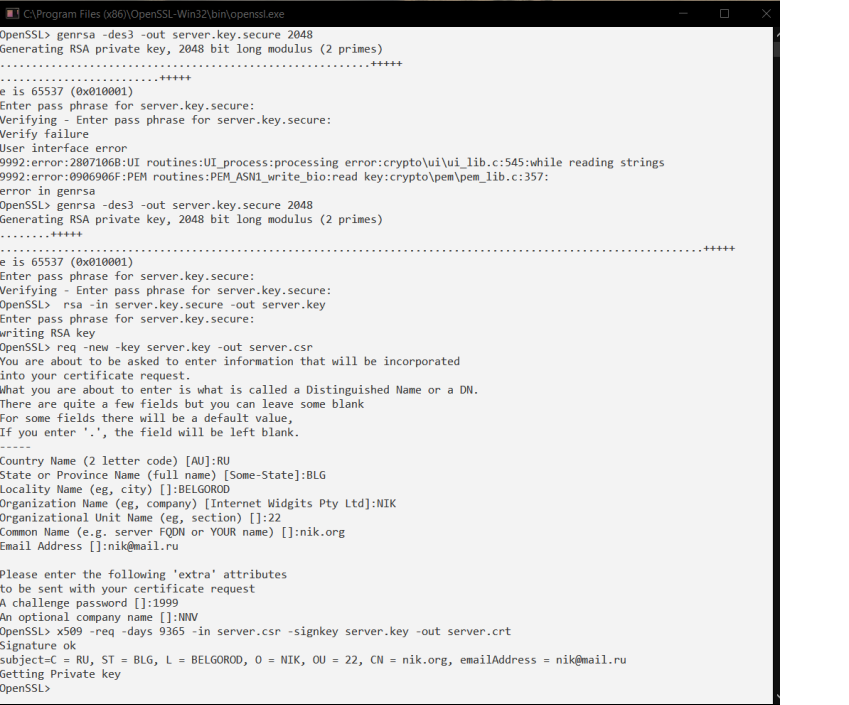




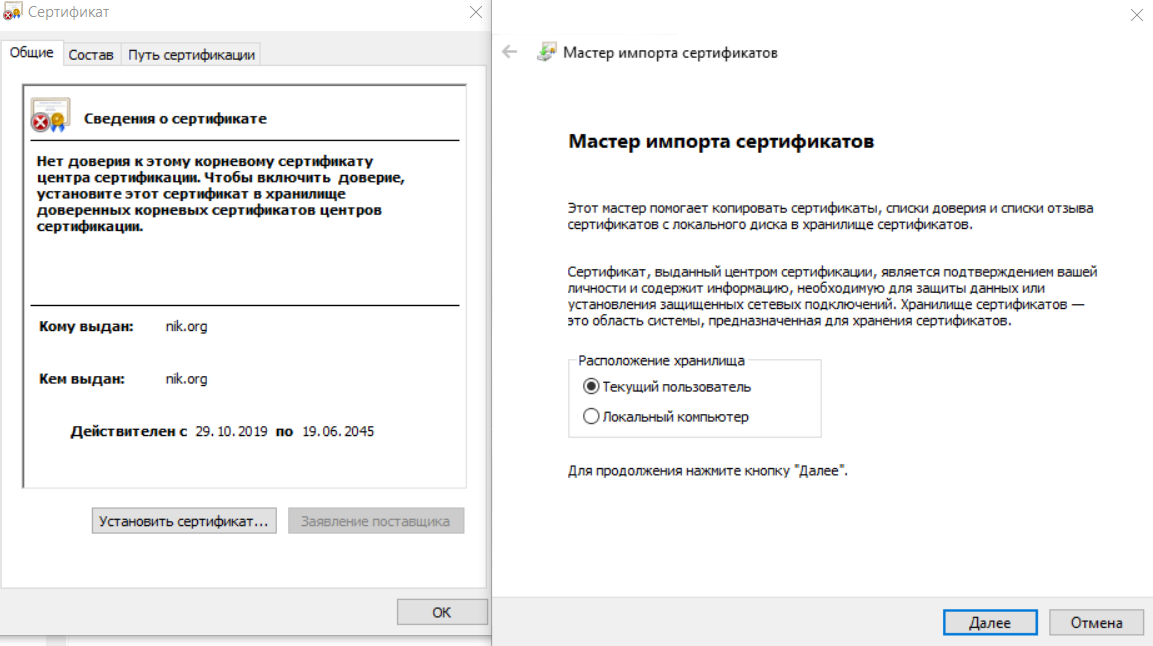
3-4. Выполните запрос личного сертификата, используя центр сертификации

Thawte свободно распространяемый (trial SSL)

Выполните настройку, запросите сертификат X.509 и получите личный сертификат пользователя



1. Убедитесь, что сертификат был опубликован в хранилищеСертификатов



1. Создайте две учетные записи пользователей, например, User1 и User 2.

7. Зарегистрируйтесь как Администратор всистеме. Работая под первой учетной записью, запросите сертификат (если он не был получен ранее), после чего зашифруйте папку с текстовым файлом, который не жалко потерять. Проверьте, что будет происходить при добавлении файлов (**файлы и папки тоже будут шифроватся**), переименовании папки(**ничего**), копировании ее на другой диск с файловой системой NTFS на том же компьютере(**ничего**), копировании папки на сетевой диск или диск с FAT(**ничего**).

**OpenSSL> des3 -in my\_cods.txt -out file.des3**

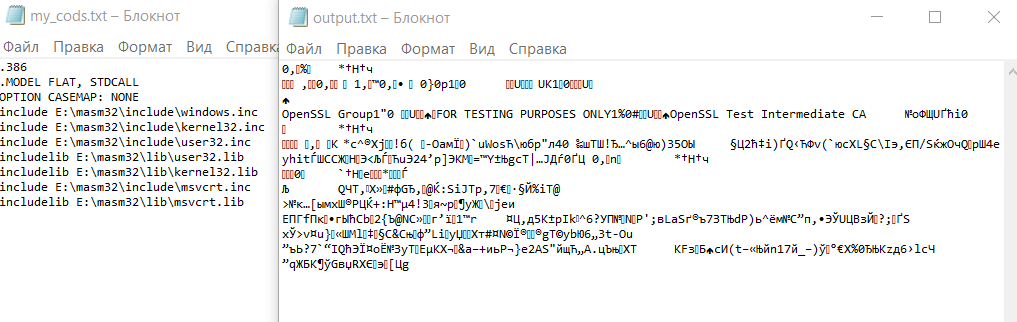
**enter des-ede3-cbc encryption password:**

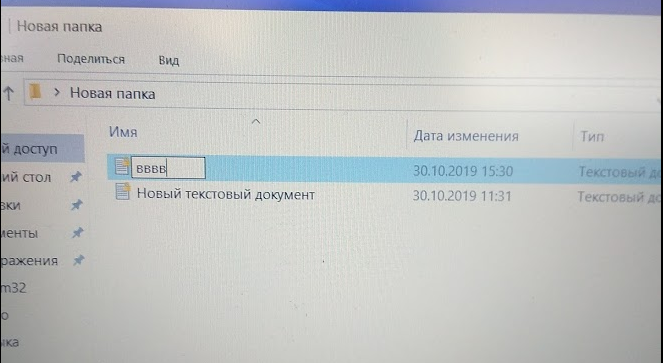
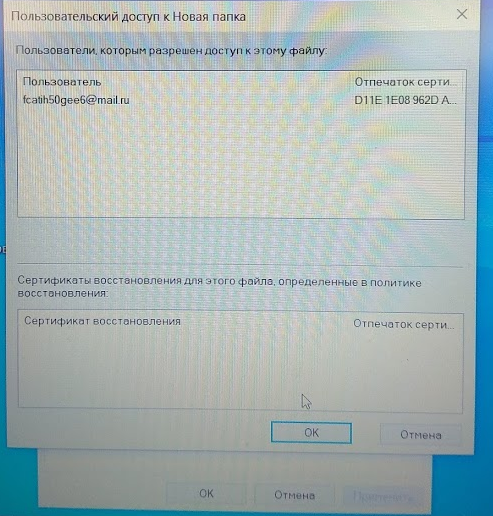
**Verifying - enter des-ede3-cbc encryption password:**

**\*\*\* WARNING : deprecated key derivation used.**

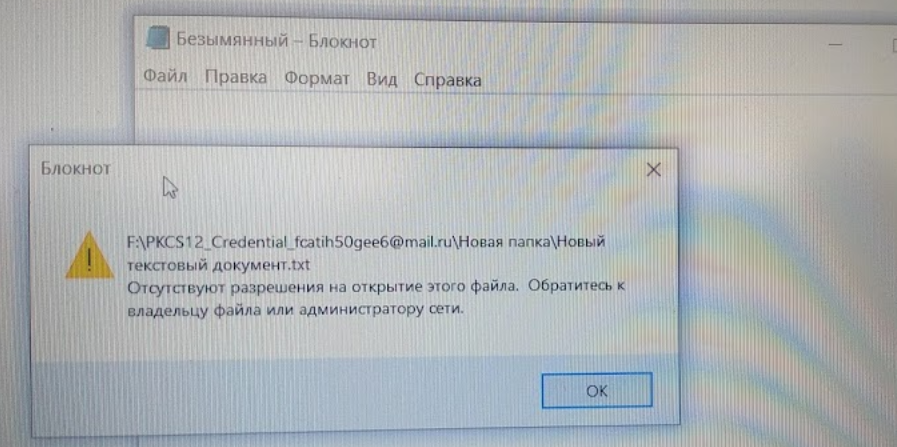
**Using -iter or -pbkdf2 would be better.**

****

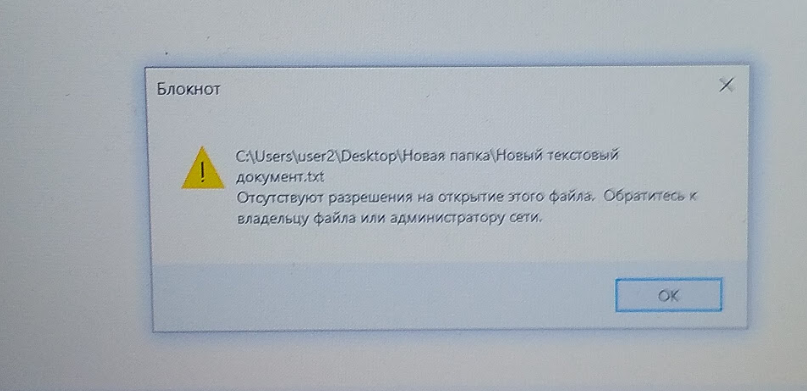
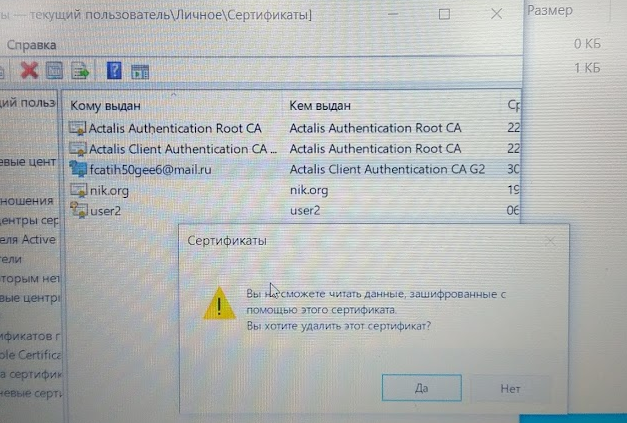
****

****

8. Убедитесь, что другой пользователь не сможет прочитать зашифрованный файл.

****

9. Снова зайдите под первой учетной записью. В оснастке Certificates, удалите сертификат пользователя (несмотря на выдаваемые системой предупреждения). Завершите сессию пользователя в системе и войдите заново. Попробуйте открыть зашифрованный файл.

****

Вывод: Научились получать и работать с SSL сертификатом.