**Лабораторная работа № 8.**

Сетевая безопасность.

1.Постановка задачи: Продемонстрировать и объяснить поля цифрового сертификата на SSL-соединении

Результат выполненной работы:

SSL-сертификат – это своего рода уникальная цифровая подпись вашего сайта. Такой сертификат нужен, в первую очередь, банкам, платежным системам и другим организациям, работающим с персональными данными, – для защиты транзакций и предотвращения несанкционированного доступа к информации.

SSL-сертификат содержит следующую информацию:

\* доменное имя, на которое оформлен SSL-сертификат;

\* юридическое лицо, которое владеет сертификатом;

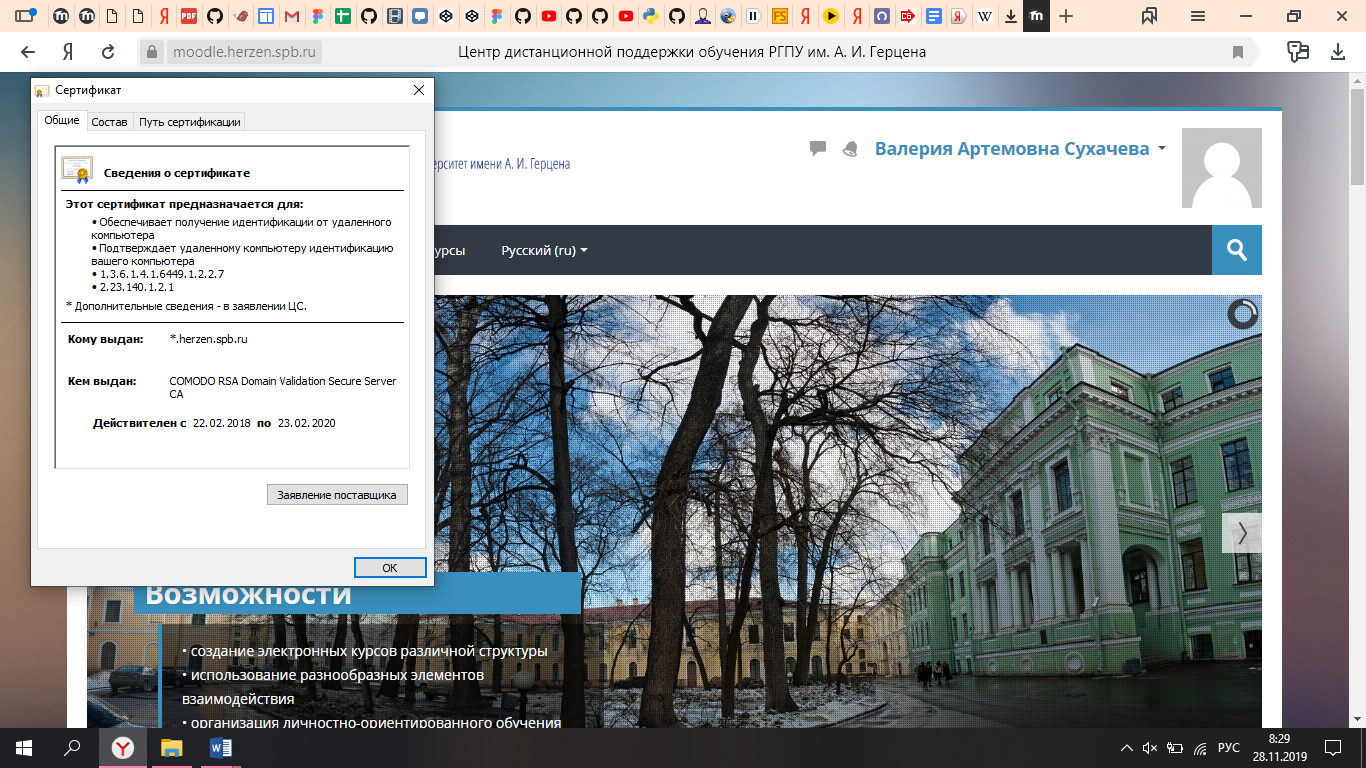
\* физическое местонахождение владельца сертификата (город, страна);

\* срок действия сертификата;

\* реквизиты компании-поставщика SSL-сертификата.

Чтобы посмотреть данные о SSL-сертификате перейдём на сайт, адрес которого начинается с https:// (!). К примеру, на сайт https://moodle.herzen.spb.ru/

4



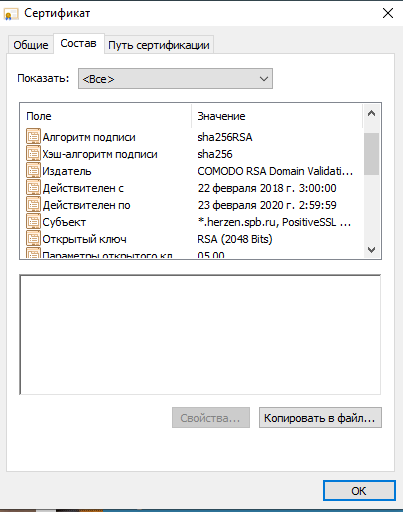
В сертификате:

Кому выдан – домен, на который распространяется сертивикат

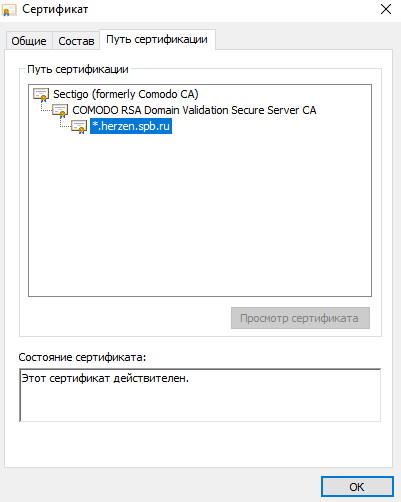
Кем выдан – организация, которая выдала сертификат

Действителен – срок действия лицензии

На что распространяется:

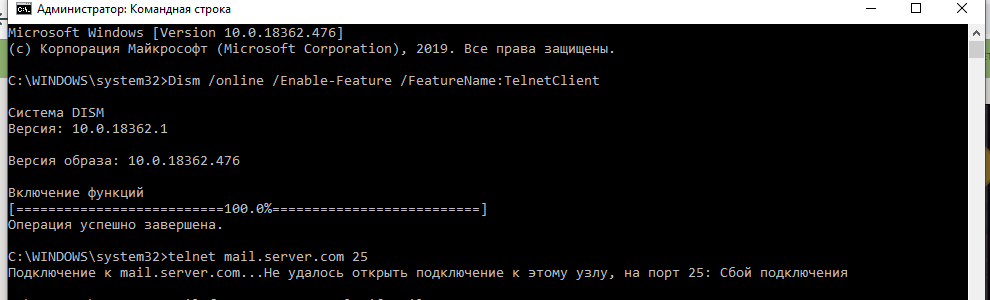


Иерархия:

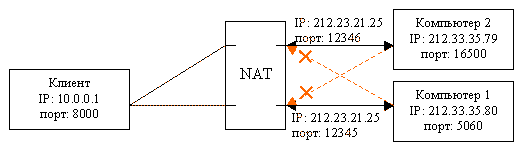


2.Постановка задачи: Продемонстрировать отправку сообщения по электронной почте через telnet

Результат выполненной работы:



Настроить сетевую трансляцию адресов (SNAT) для общего доступа в интернет



При исходящем коннекте от клиента к серверу в интернете PF открывает канал между исходящим портом клиента и принимающим портом сервера.

По каналу пакеты будут идти в обе стороны только между исходящим портом клиента и принимающим портом сервера.

Инициатором соединения всегда останется локальный компьютер. Любые соединения, инициированные из вне будут блокированы.

То есть проще говоря PF будет разрешать только ответы внешних серверов на запросы локальных машин.