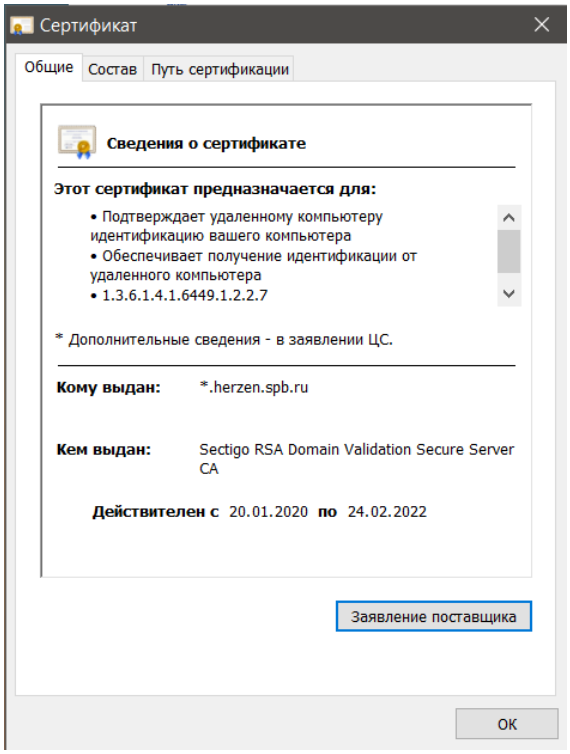
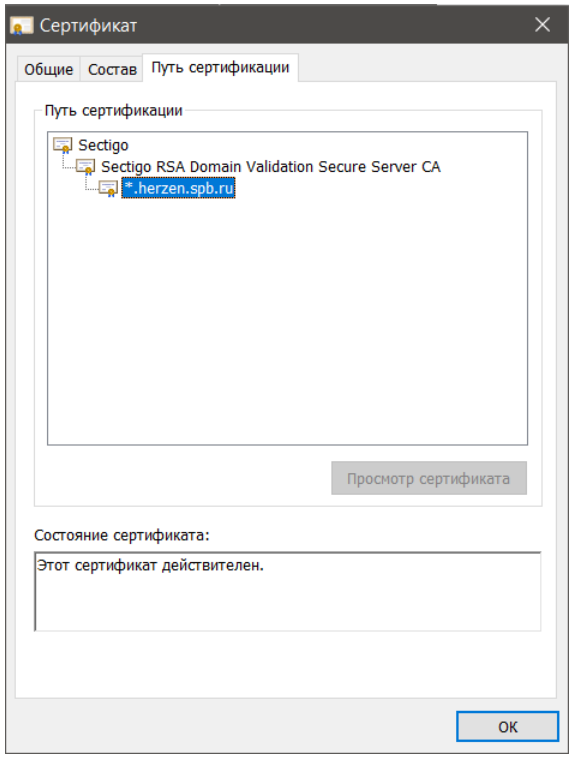
Лабораторная работа №8

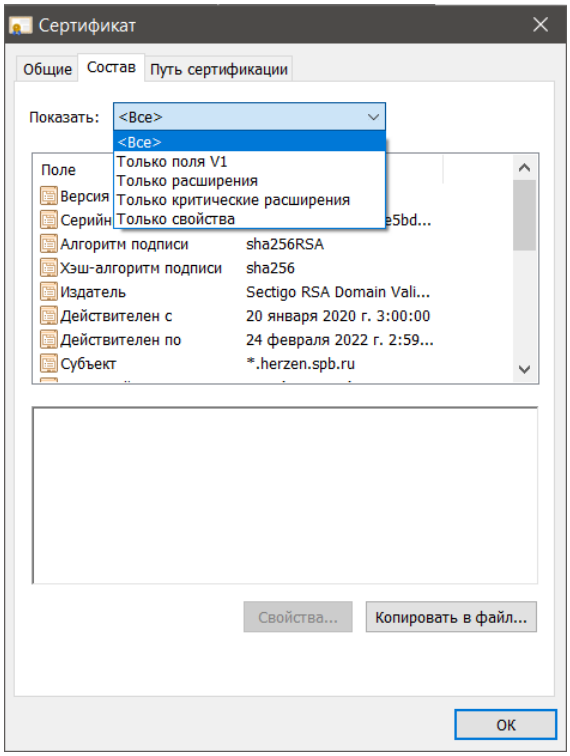
Сетевая безопасность

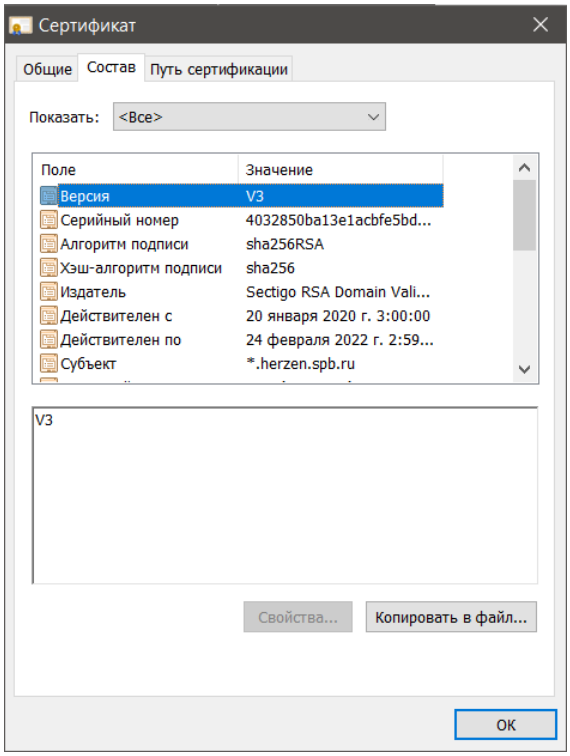
1. Продемонстрировать и объяснить поля цифрового сертификата на SSL-соединении

Ниже приведен пример SSL-сертификата сайта Moodle Герценовского университета в нескольких вкладках.









Что нам говорит данный сертификат?

На вкладке «Общее» не сложно догадаться, что есть общая информация о том, для чего выдан сертификат, какому домену, кем и на какой срок.

На вкладке «Путь сертификации» показана цепочка данного сертификата. Цепочки сертификатов полезны для того, чтобы распределить нагрузку между разными центрами сертификации и сделать систему удостоверения сертификатов более надёжной.

На самой объемной вкладке «Состав» мы можем увидеть много характеристик сертификата. Они делятся на группы:

- поля V1 — это поля с базовой информацией о сертификате, соответствующей первой версии стандарта (X.509, version 1); эта группа полей поддерживается для обратной совместимости сертификатов с разными браузерами;
- расширения — поля, не входящие группу полей V1;
- критические расширения — поля, ошибка в которых приведён к признанию SSL-сертификата недействительным;
- свойства — цифровая подпись сертификата и её алгоритм.

В окне снизу показывается текст того, что написано в одной из характеристик.