Ознакомиться с работой протокола TLS v1.2. Определить перечень проверок, которые совершаются на стороне клиента браузером при проверке сертификата сервера и записать в виде списка.

Список проверок:

1. **Проверка целостности и подлинности цифровой подписи сертификата. (**Клиент проверяет, что сертификат подписан одним из доверенных Удостоверяющих Центров**)**

2. **Построение и проверка цепочки сертификатов (Certificate Chain).**

3. **Проверка срока действия сертификата.**

4. **Проверка доменного имени (Subject Alternative Name).**

**5. Проверка отозванного статуса сертификата (CRL / OCSP).**

**6. Проверка расширений и назначения сертификата (Key Usage & Extended Key Usage).**

**7. Проверка алгоритмов и их стойкости.**

**8. Проверка базовых ограничений УЦ (Basic Constraints).**

**9. Проверка наличия самого сертификата и его формата.**