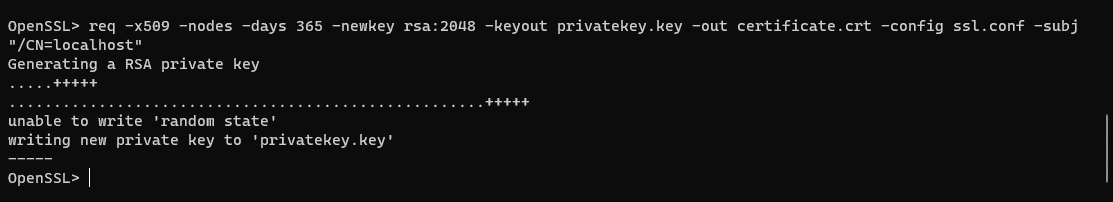
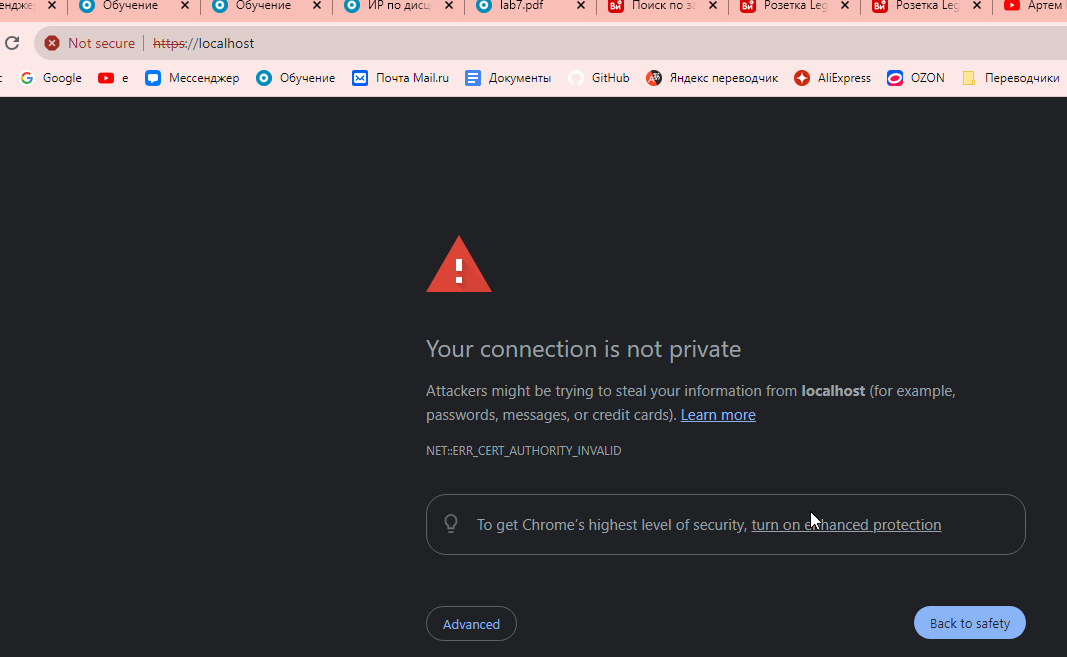
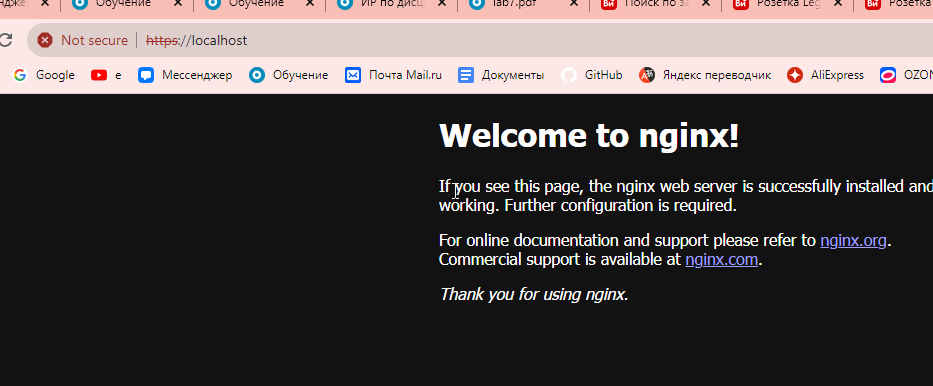
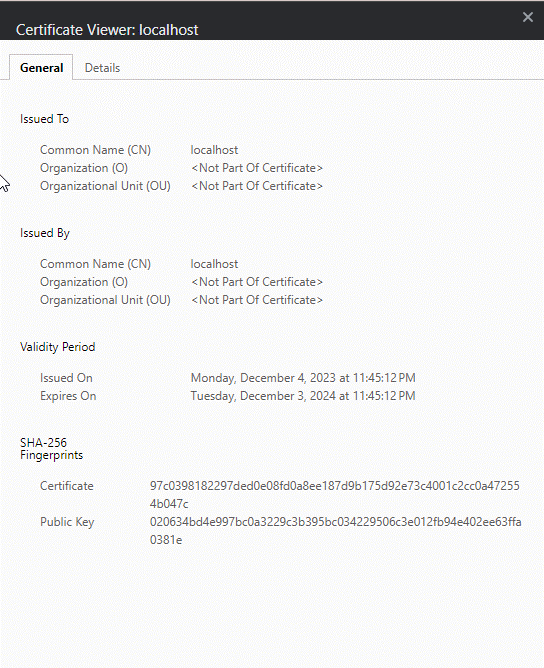
## **Отчет к лабораторной работе №5**

**Задание №1**









## **Контрольные вопросы**

**1. Недостатки HTTPS по сравнению с HTTP включают в себя:**

* Дополнительные вычислительные нагрузки и задержки из-за процесса установления безопасного соединения
* Необходимость в обновлении и управлении сертификатами для поддержания безопасности
* HTTPS может замедлить скорость загрузки веб-страниц из-за дополнительных шагов шифрования и дешифрования

2. Атака, в которой злоумышленник "подсовывает" свой TLS сертификат клиенту вместо ожидаемого сертификата от сервера, называется Man-in-the-Middle (MitM) атакой. Для борьбы с этой атакой можно использовать методы аутентификации сервера с помощью цифровых сертификатов, а также использование системы отзыва сертификатов (CRL) или Online Certificate Status Protocol (OCSP) для проверки действительности сертификата.

3. В протоколе TLS используется симметричное шифрование для эффективной защиты данных, так как симметричное шифрование гораздо быстрее ассиметричного шифрования. Однако ассиметричное шифрование используется для обмена ключами для симметричного шифрования и аутентификации сторон. Использование ассиметричного шифрования для всех сообщений было бы слишком накладно в вычислительном плане из-за больших затрат на ресурсы.