**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 №5**

Инфраструктура открытых ключей.

Выполнил:

Студент группы КБ-211

Коренев Д.Н.

Принял:

Смакаев А.В.

Оглавление

[Задание 3](#_Toc183129580)

[Разработанная программа 4](#_Toc183129581)

[Тестирование производительности 5](#_Toc183129582)

[Вывод 7](#_Toc183129583)

[Приложения 9](#_Toc183129584)

*Цель работы:* ознакомиться с принципами работы инфраструктуры открытых ключей, методами ее работы, хранения ключей и форматом сертификатов X.509. Разработать консольное приложение, работающее со встроенным в операционную систему хранилищем сертификатов.

Задание

1. Сгенерировать самоподписанный сертификат CA. В качестве CN указываем 127.0.0.1, остальные данные можно указать вымышленные
   * вариант с openssl описан [в статье на habr](https://habr.com/ru/articles/671730/)
   * вариант с CA Smallstep описан [в статье на habr](https://habr.com/ru/articles/671730/)
2. Установить сертификат CA
   * перевести сертификат в формат PEM

openssl x509 -in root\_ca.crt -out root\_ca.pem -outform PEM

* установить сертификат CA
  + на [ubuntu](https://ubuntu.com/server/docs/install-a-root-ca-certificate-in-the-trust-store)
  + на [windows](https://learn.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate#adding-certificate-snap-ins)

1. Сгенерировать сертификат для сервера
   * вариант с openssl описан [в статье на habr](https://habr.com/ru/articles/671730/)
   * вариант с CA Smallstep описан [в статье на habr](https://habr.com/ru/articles/671730/)
2. Запустить сервер
   * Вариант с Node.js описан [в статье на habr](https://habr.com/ru/articles/671730/)
   * Вариант с Nginx описан [в gist на github](https://gist.github.com/RoobinGood/9eda5261fc532c878a21c667a8a568c7)
3. Обратиться к серверу

curl https://127.0.0.1:9443

1. Опционально можно выпустить [сертификат для localhost](https://gist.github.com/cecilemuller/9492b848eb8fe46d462abeb26656c4f8) и зайти на сервер через браузер, но всегда [надо помнить о MitM](https://letsencrypt.org/docs/certificates-for-localhost/)

*В отчёт обязательно надо включить описание хода работы и вывод openssl X509 --text для выпущенных сертификатов.*