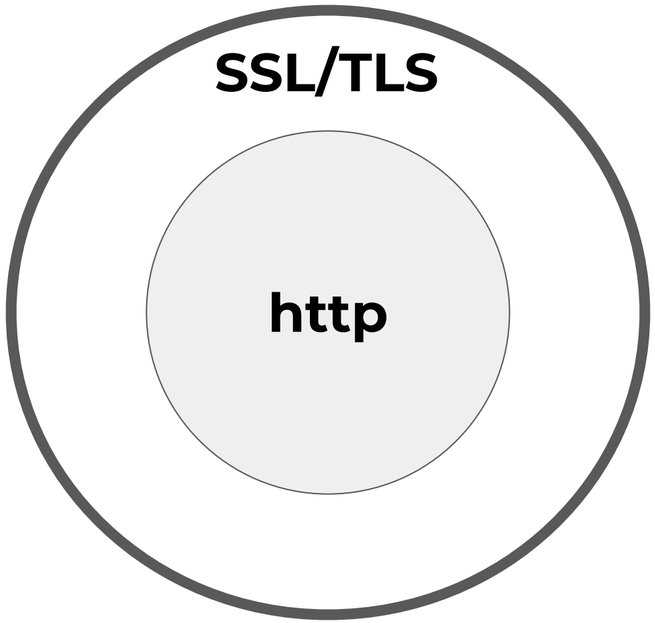
Skillbox

# SSL-сертификаты и настройка HTTPS

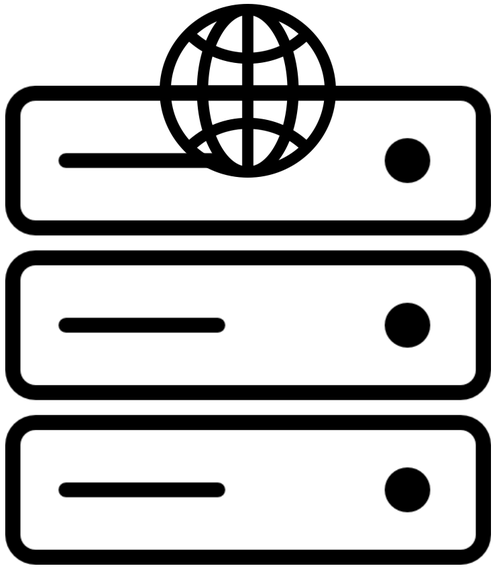
**Виктория Маркова**
Lead DevOps
«Валарм»

# HTTPS



# Handshake. Приветствие

Привет, я поддерживаю
версии SSL: ...
алгоритмы шифрования ...

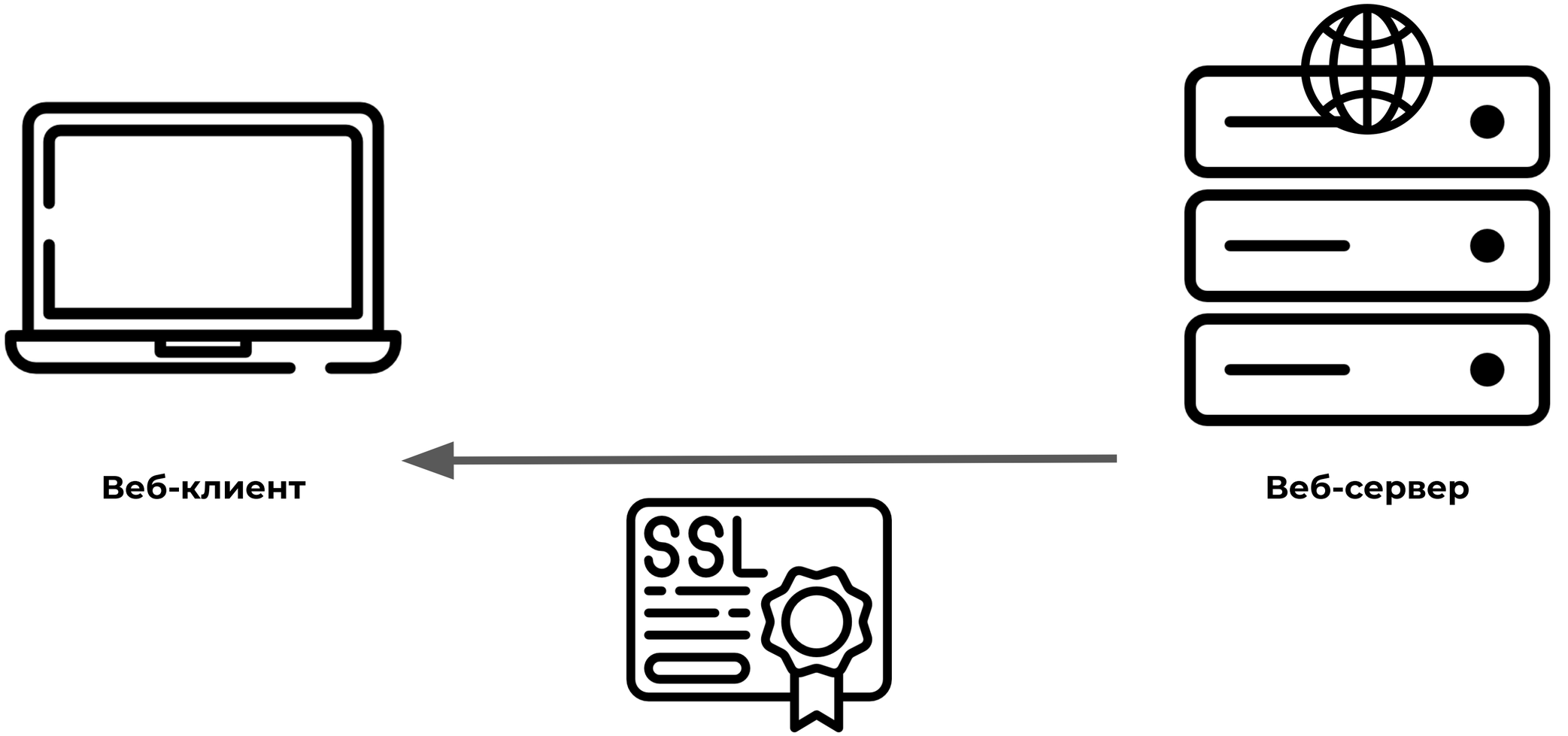


**Веб-клиент**

Привет, давай использовать
версию SSL: ...
алгоритм шифрования ...

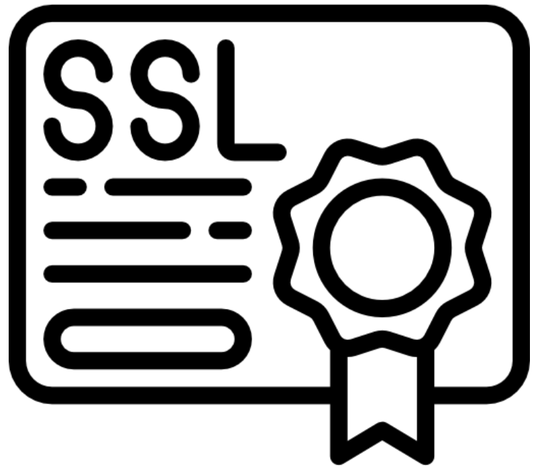
**Веб-сервер**

# Handshake. Сертификат сервера

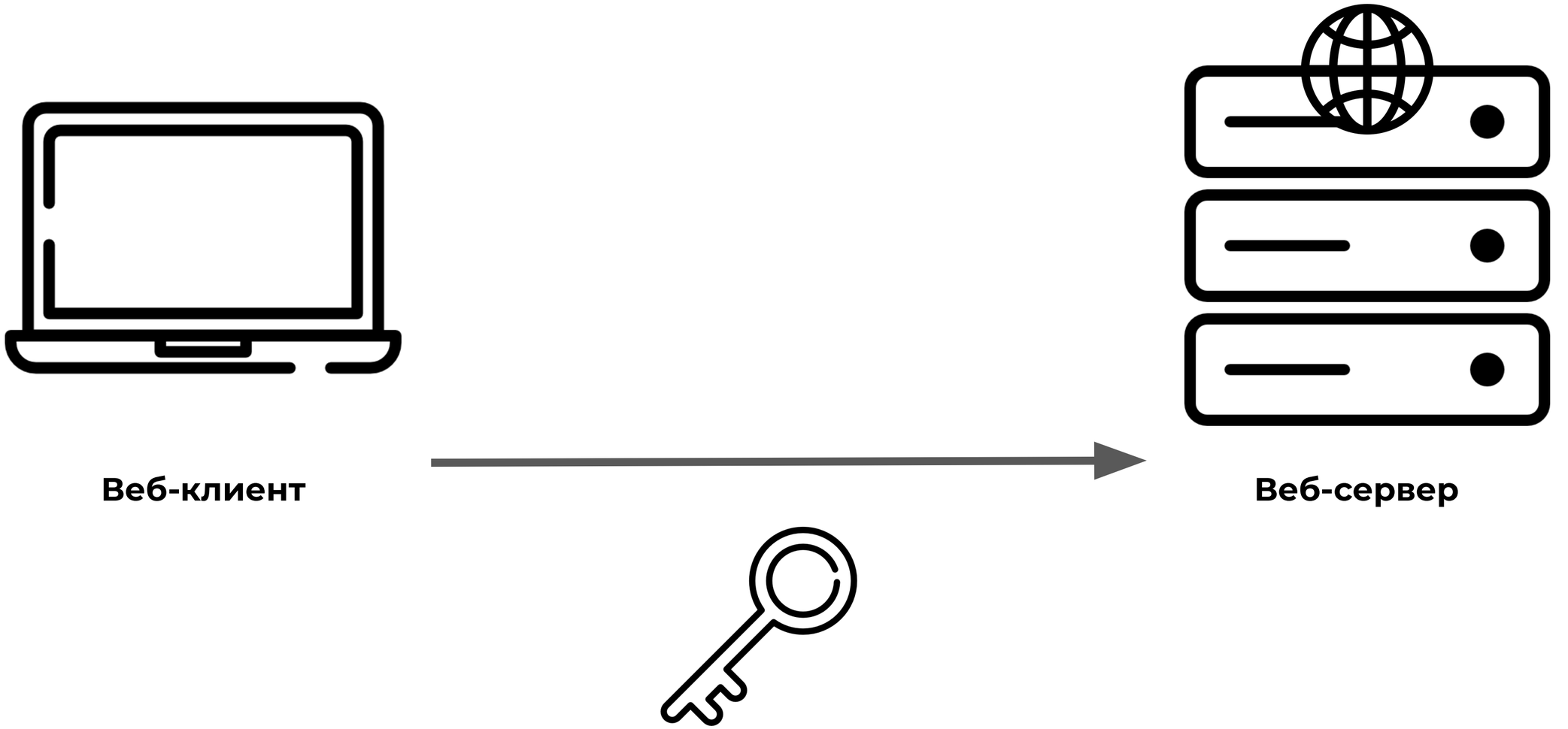


# SSL-сертификат

- открытый ключ
- информация о домене и организации
- электронно-цифровая подпись Удостоверяющего Центра



# Handshake. Обмен ключами



# openssl

- Генерация приватного ключа
  openssl genrsa -out server.key 4096
- Генерация CSR
  openssl req -new -key server.key  –out server.csr
- Создание сертификата
  openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
- Вывод информации о сертификате
  openssl x509 -noout -text -in server.crt
- Вывод модуля сертификата
  openssl x509 -noout -modulus -in ssl_certificate.crt | openssl md5
- Вывод модуля приватного ключа
  openssl rsa -noout -modulus -in private.key | openssl md5

Skillbox

# Домашнее задание

# Спасибо за внимание!