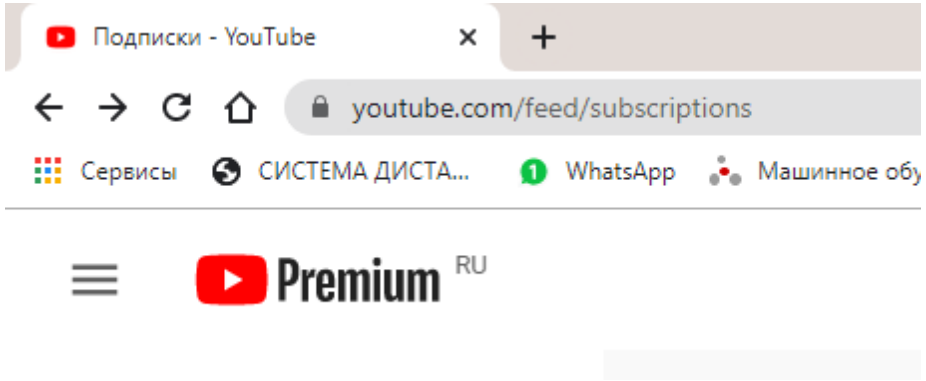
Протокол HTTPS

Компьютерные сети

Протокол HTTPS

HTTPS - Hypertext Transfer Protocol Secure

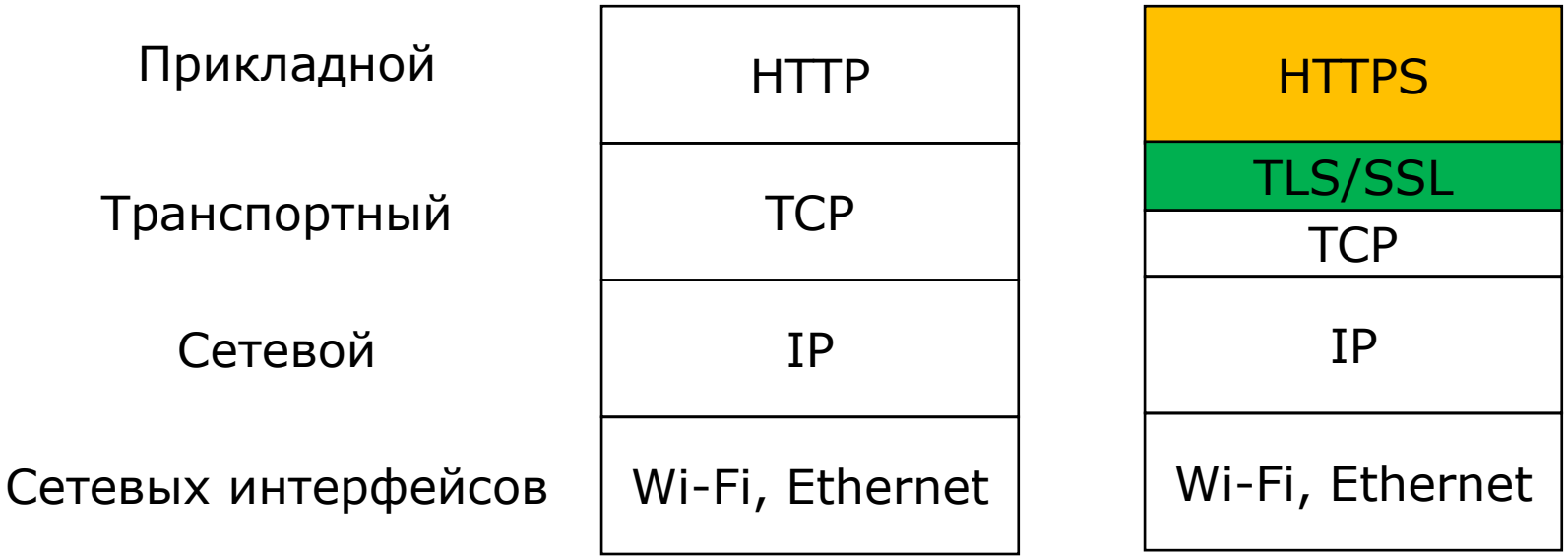
- Протокол безопасной передачи гипертекста
- Использует TLS/SSL для защиты данных



RFC 2818, 2000 год

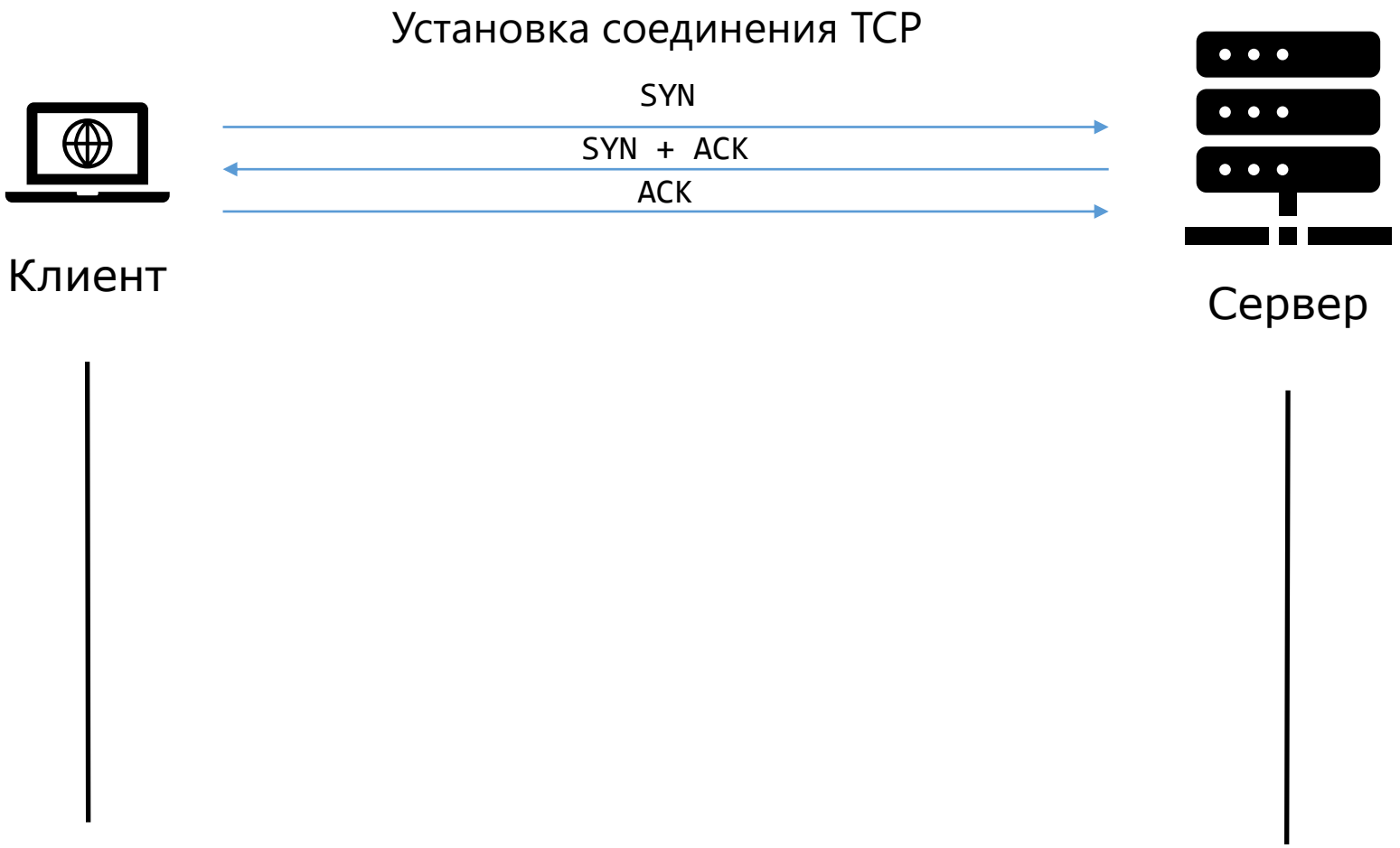
- «HTTP Over TLS»
- Нет изменений в протоколе HTTP

Место в модели TCP/IP

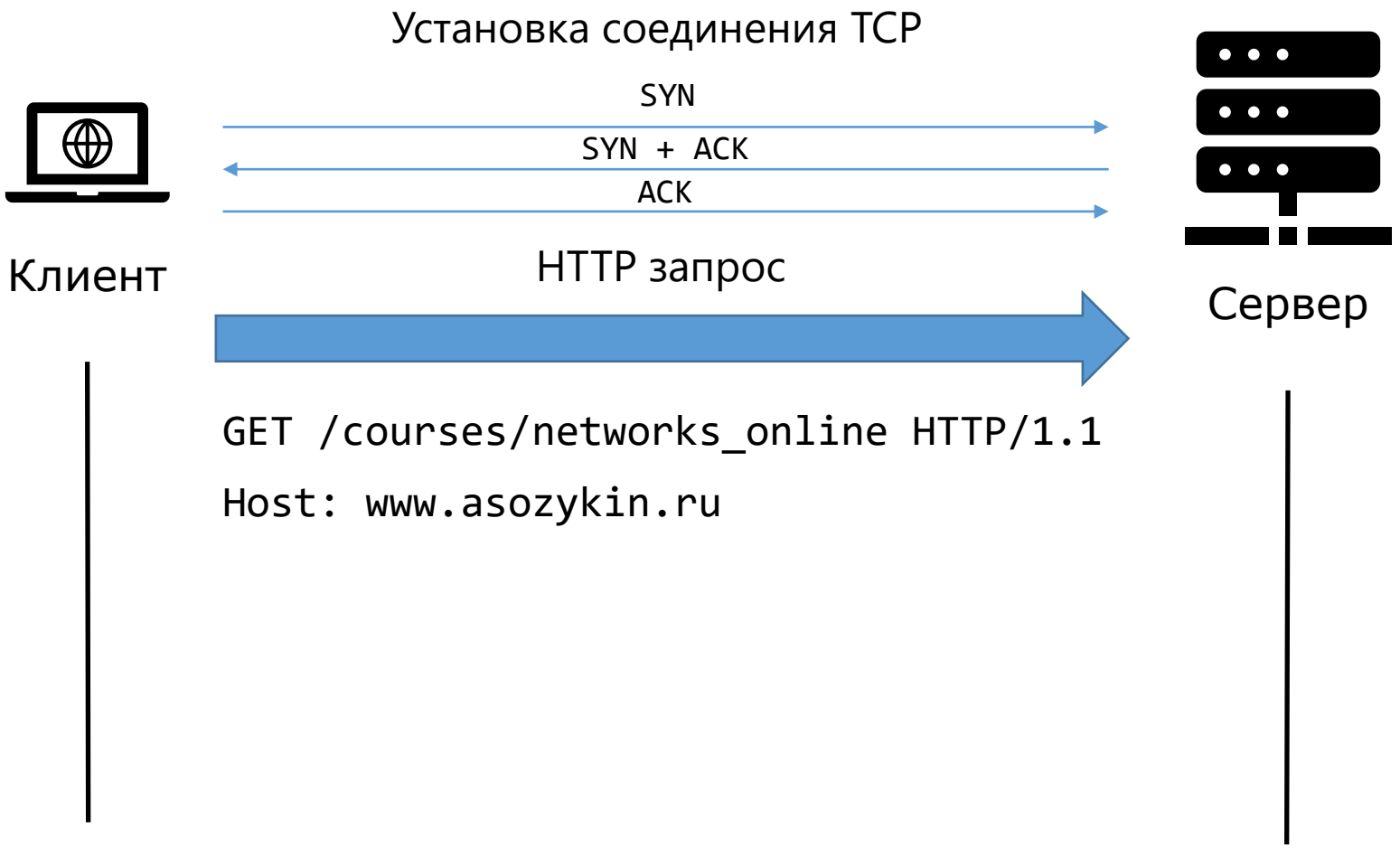


Уровни модели TCP/IP

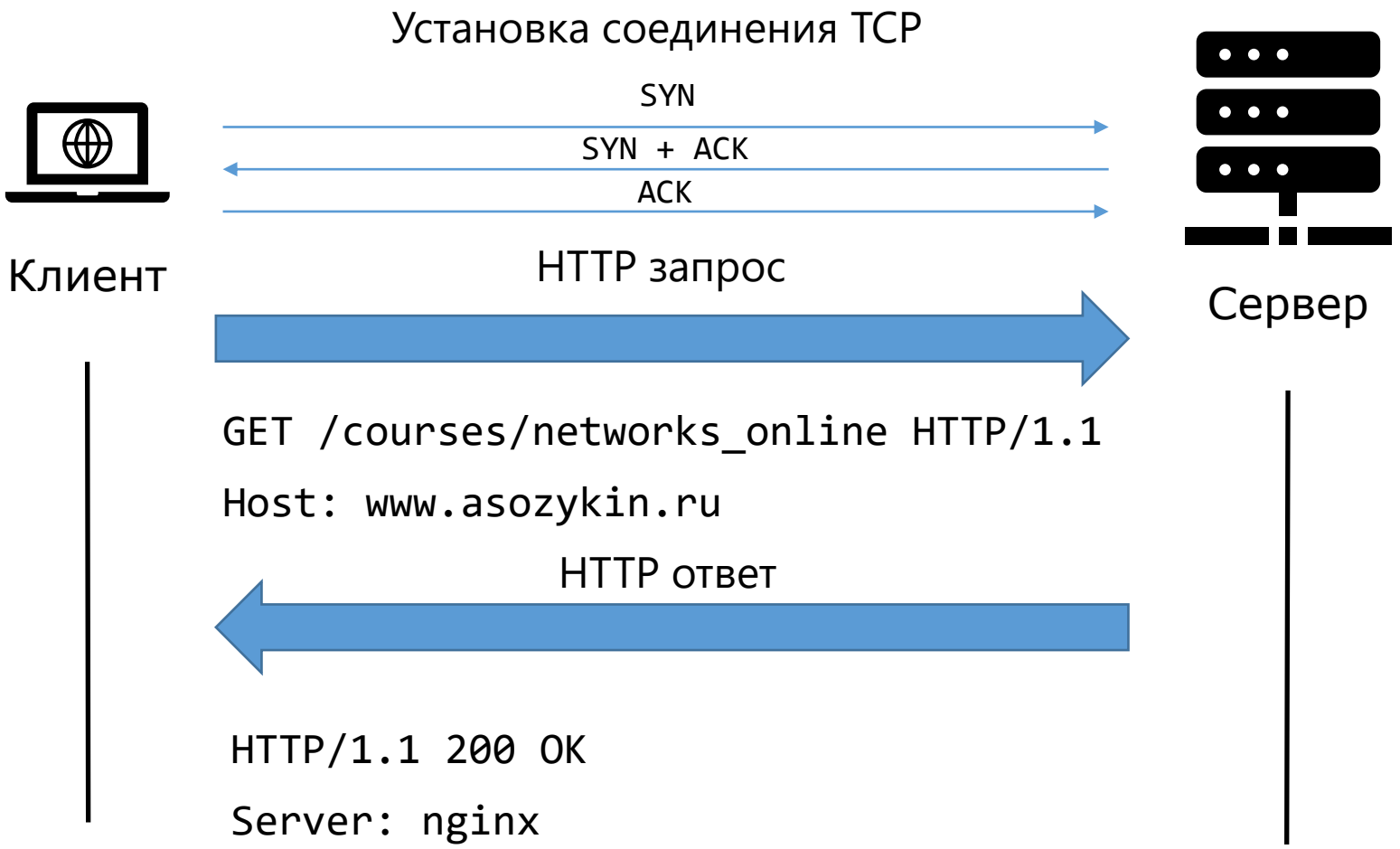
Работа протокола HTTP



Работа протокола HTTP



Работа протокола HTTP



Работа протокола HTTPS

Работа протокола HTTP поверх TLS

Номера портов сервера

- HTTP – 80
- HTTPS – 443

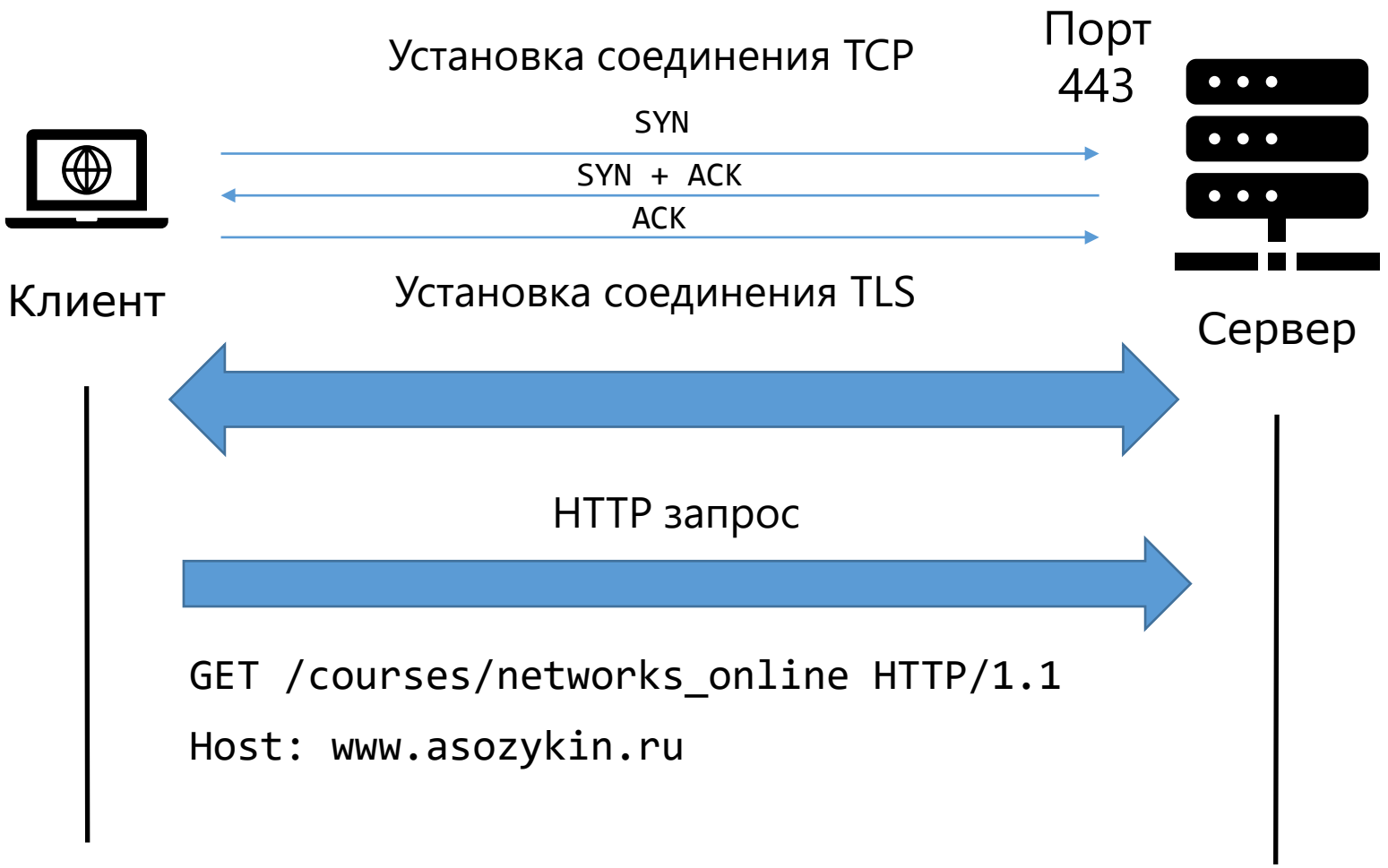
Порядок работы HTTPS

- Установка TCP соединения
- Установка TLS соединения
- Передача данных HTTP с помощью протокола передачи данных TLS (Application Data Protocol)

Формат URI (Uniform Resource Identifier)

- https://www.asozykin.ru:443/courses/networks_online

Работа протокола HTTPS



Альтернативные варианты обеспечения безопасности HTTP

RFC 2817, 2000 г., Upgrading to TLS Within HTTP/1.1

```
GET http://example.bank.com/acct_stat.html?749394889300 HTTP/1.1
Host: example.bank.com
Upgrade: TLS/1.0
Connection: Upgrade
```

RFC 2660, 1999, The Secure HyperText Transfer Protocol

- Протокол S-HTTP
- Не использует TLS/SSL, собственные алгоритмы обеспечения безопасности
- Идентификатор протокола shttp, порт 80
- Для выбора протокола его нужно явно указать в строке запроса

```
GET /prize.html HTTP/1.0
Security-Scheme: S-HTTP/1.4
```

Итоги

HTTPS - Hypertext Transfer Protocol Secure:

- Безопасный протокол передачи гипертекста
- Для безопасности используется TLS/SSL
- RFC 2818, 2000 г., HTTP Over TLS

Особенности HTTPS:

- Данные HTTP передаются в зашифрованном виде с помощью Application Data Protocol TLS/SSL
- Номер порта сервера 443
- Идентификатор протокола https

Нет изменений в протоколе HTTP:

- Текстовый режим работы
- Модель запрос/ответ