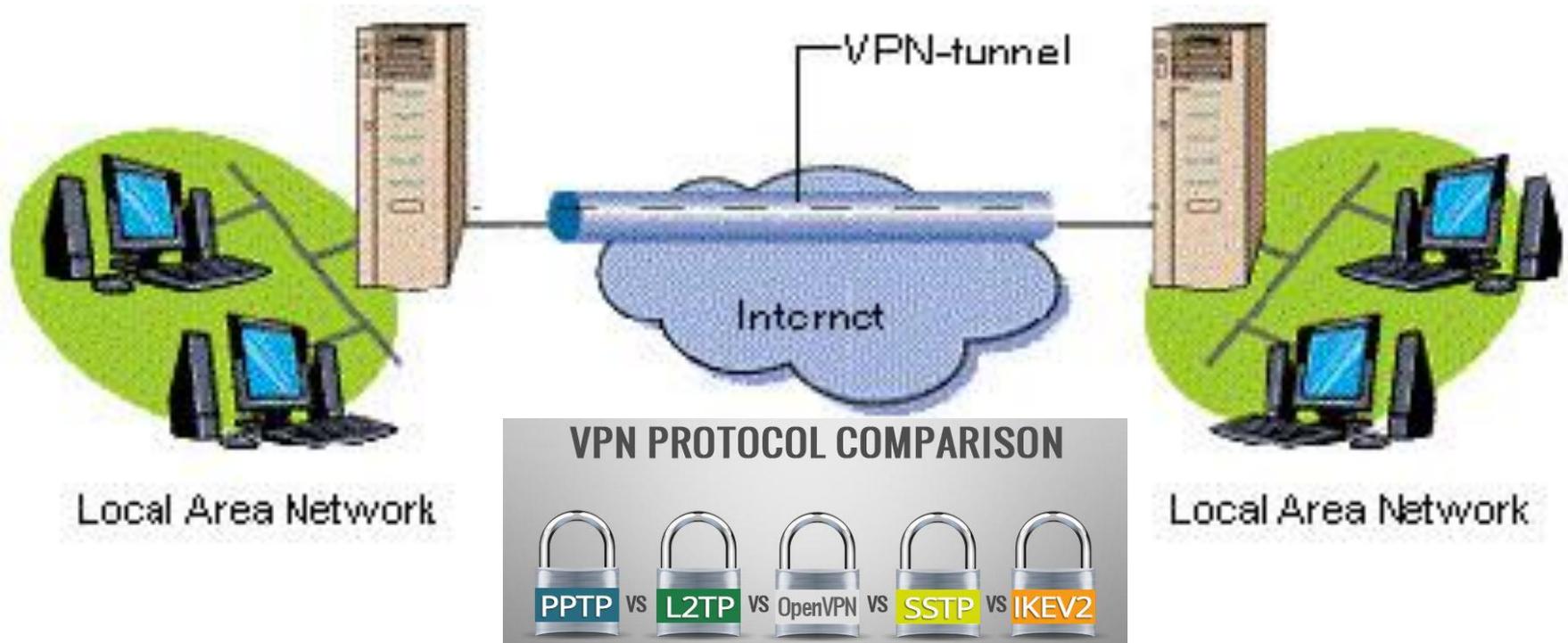


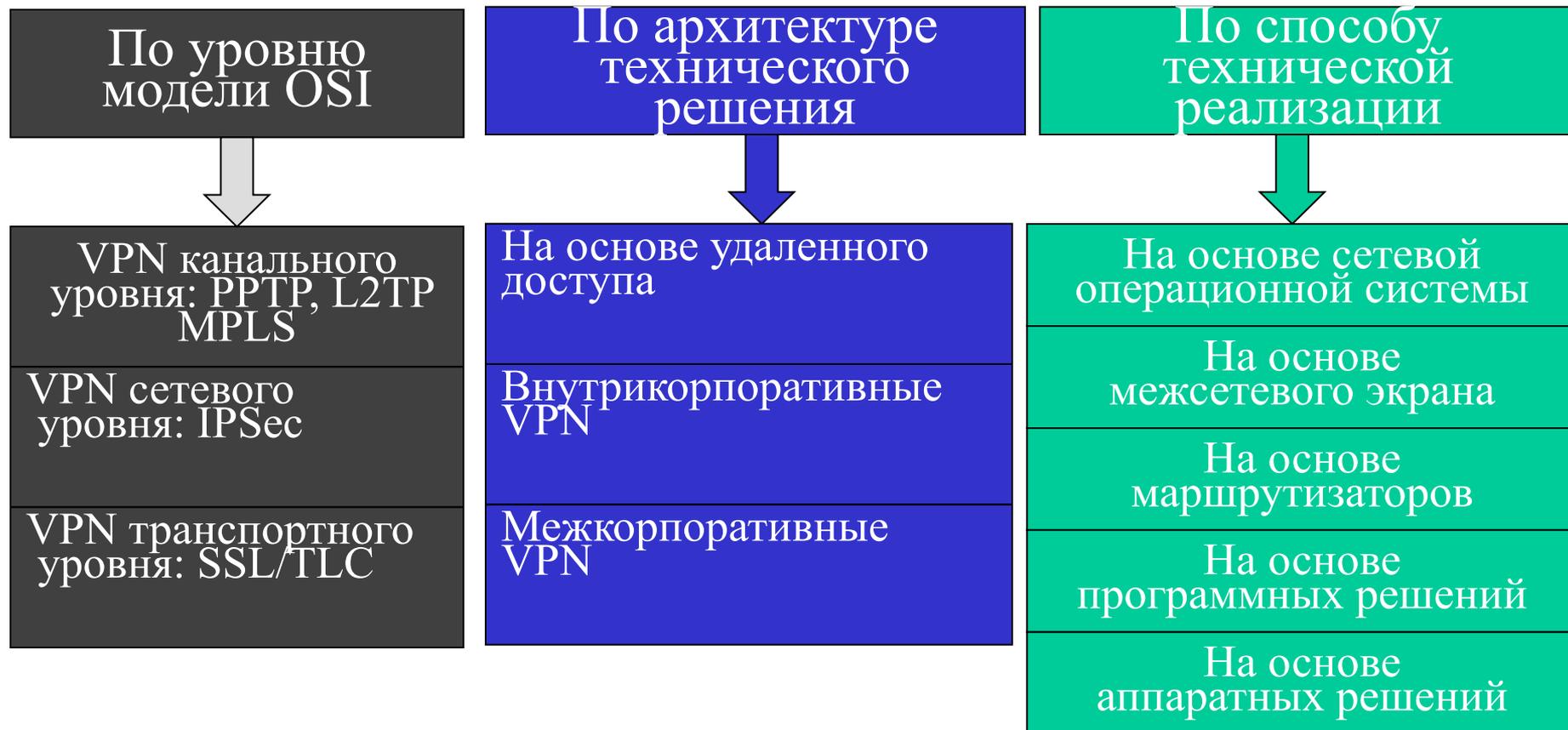


Протоколы

# Виртуальные частные сети - VPN



# Классификация VPN



# Поддержка VPN на различных уровнях модели OSI

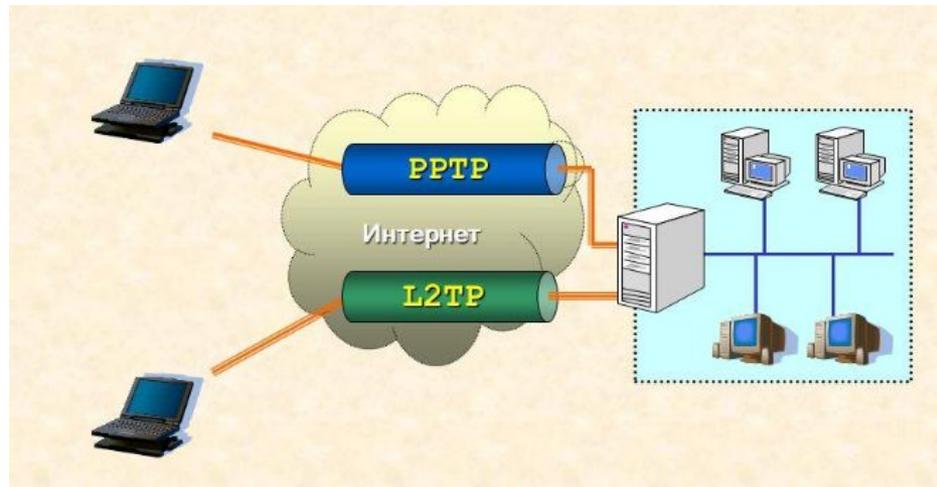
- Канальный уровень:
  - L2TP, PPTP (авторизация и аутентификация)
  - Технология MPLS (установление туннеля)
- Транспортный уровень:
  - SSL/TLS (поддержка шифрования и аутентификации, реализован только для поддержки TCP-трафика)

Прикладной	HTTP/S, S/MIME	Непрозрачны для приложений, не зависят от транспортной инфраструктуры
Презентационный	SSL	
Сеансовый		
Транспортный		
Сетевой	IPSec, SKIP	Прозрачны для приложений, зависят от транспортной инфраструктуры
Канальный	PPTP	
Физический		

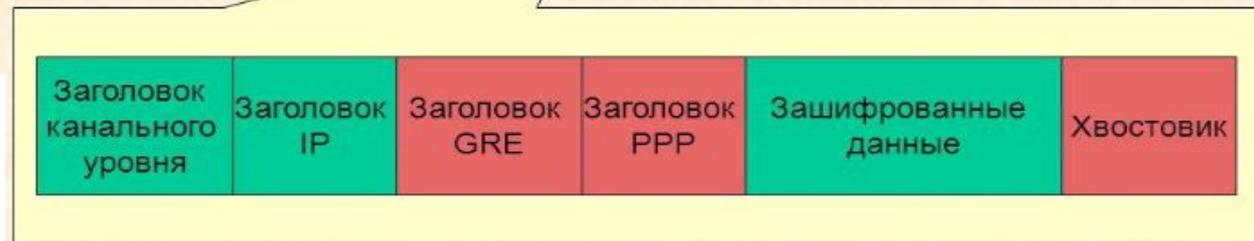
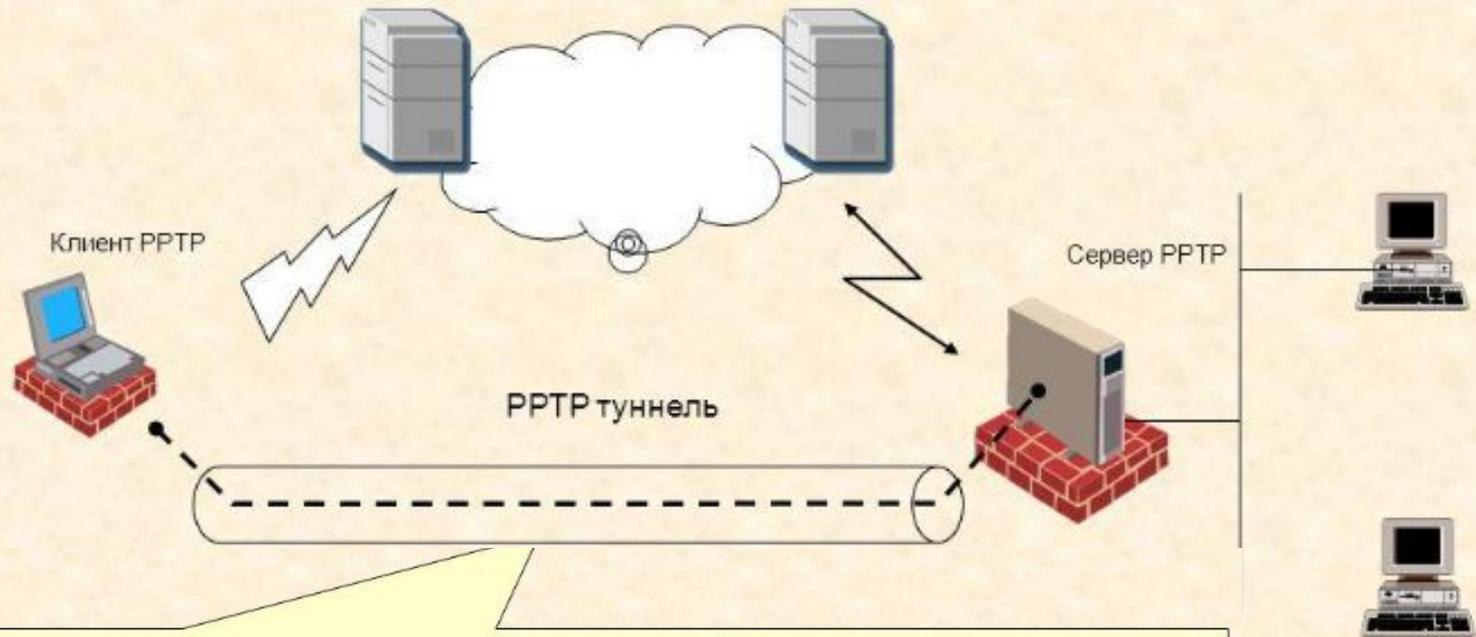
# Протоколы канального уровня:

**PPTP** (Point-to-Point Tunneling Protocol). Шифрует кадры PPP и инкапсулирует их в IP пакеты

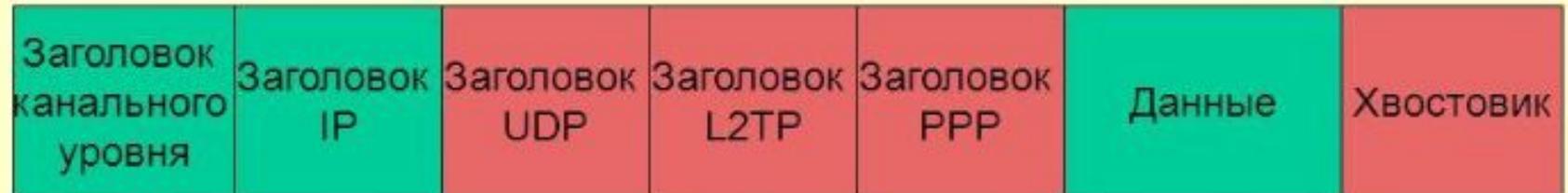
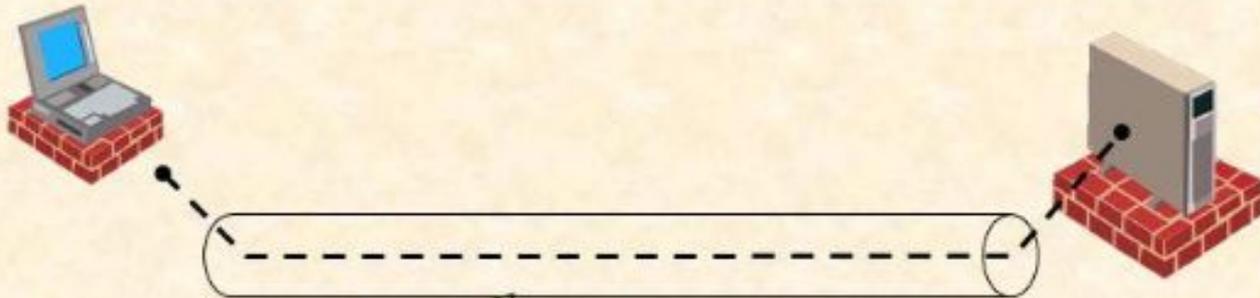
**L2TP** (Layer to Tunneling Protocol). Инкапсулирует кадры PPP в протокол сетевого уровня, предварительно проведя аутентификацию пользователя



# Протокол PPTP



# Протокол L2TP



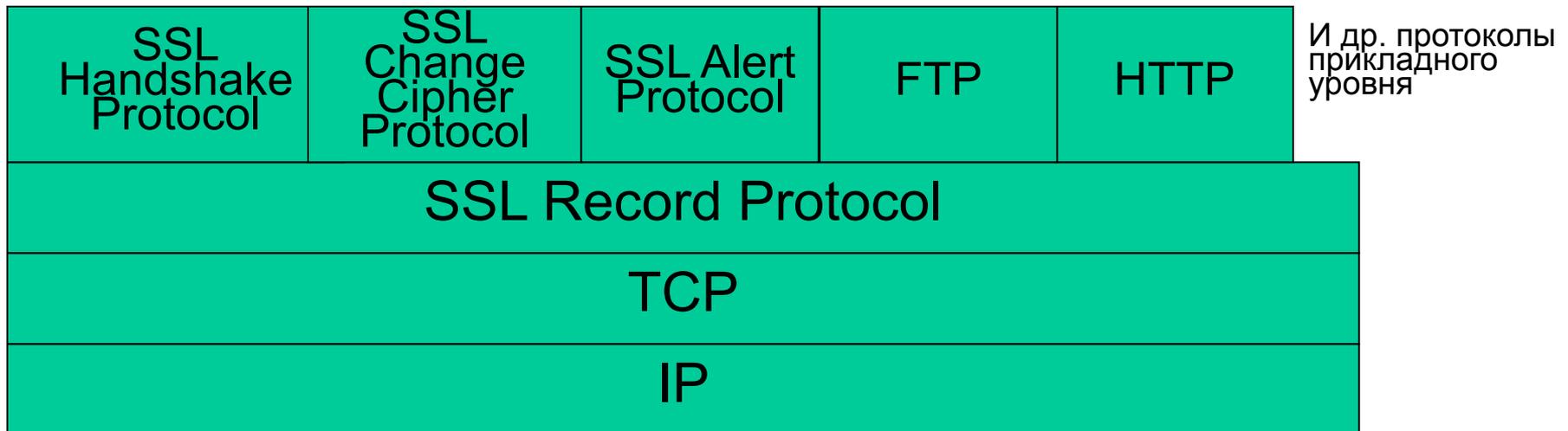
# Протоколы транспортного уровня

**SSL** – (Secure Sockets Layer) уровень защищенных сокетов.

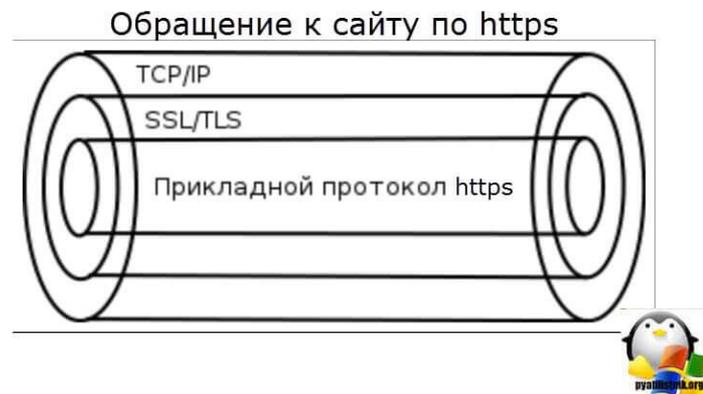
**TLS** – (Transport Layer Security) безопасность транспортного уровня.

В настоящее время объединены в общий стек протоколов SSL/TLS (по сути это одно и то же)

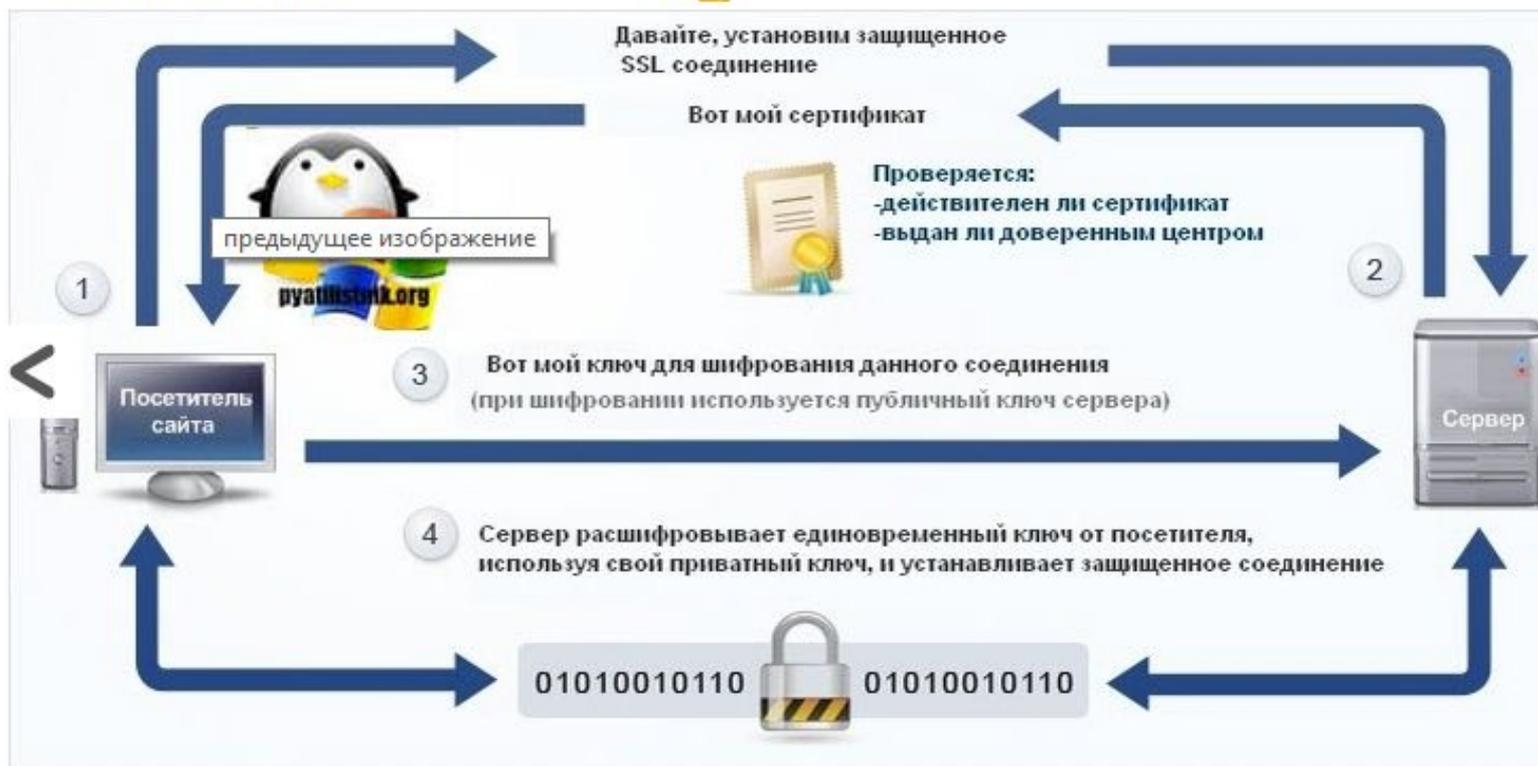
## Стек протоколов SSL/TLS



- SSL/TLS реализован поверх TCP (надёжность доставки, квитирование), между транспортным и прикладным уровнем.
- Стек протоколов SSL/TLS:
  - SSL Record Protocol: защита передаваемых данных
  - SSL Handshake Protocol: установление сессии (соглашение о используемых алгоритмах, параметры безопасности)
  - SSL Change Cipher Protocol (смена шифра)
  - SSL Alert Protocol (сообщения об ошибках)



Этап 1: установка защищенного соединения



# Последовательность обмена сообщениями протоколов TLS/SSL

## Протокол рукопожатия

