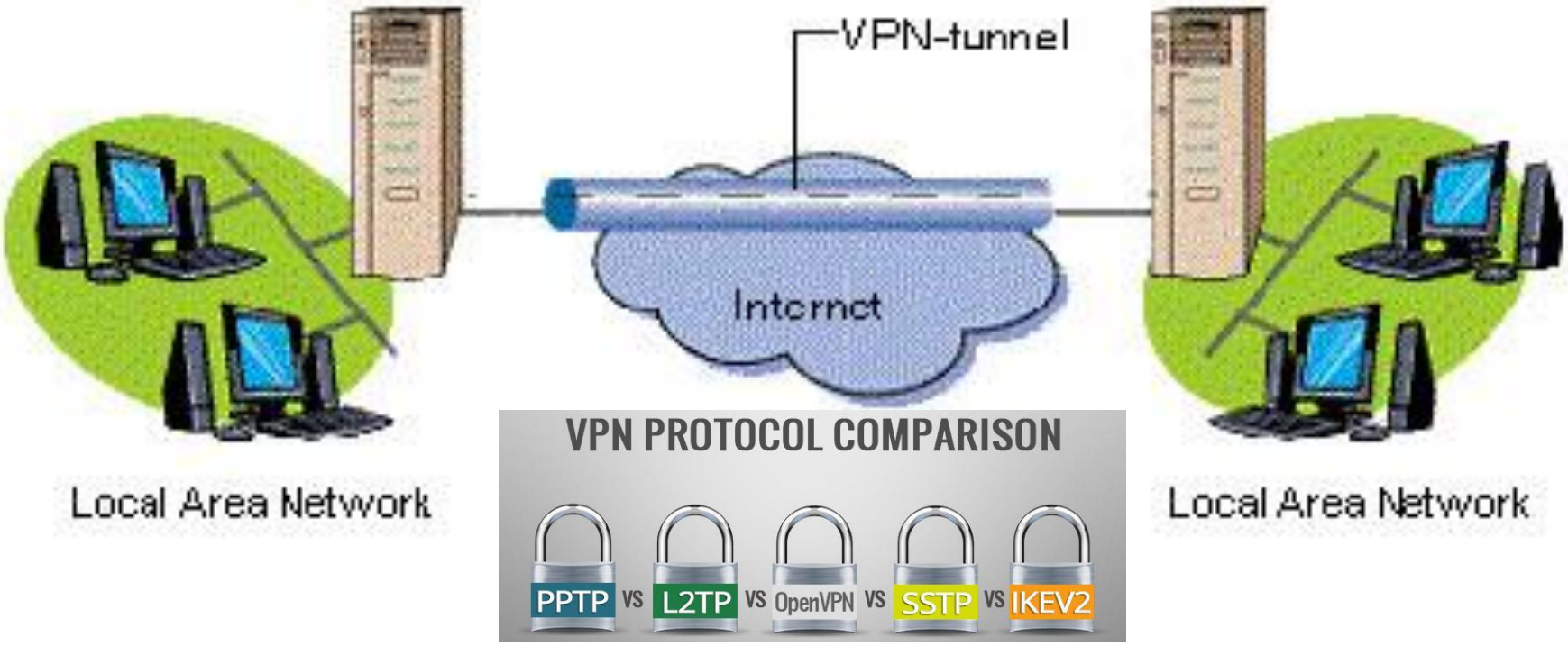
Протоколы

Виртуальные частные сети - VPN



Классификация VPN

По уровню модели OSI

- VPN канального уровня: PPTP, L2TP MPLS
- VPN сетевого уровня: IPSec
- VPN транспортного уровня: SSL/TLC

По архитектуре технического решения

- На основе удаленного доступа
- Внутрикорпоративные VPN
- Межкорпоративные VPN

По способу технической реализации

- На основе сетевой операционной системы
- На основе межсетевого экрана
- На основе маршрутизаторов
- На основе программных решений
- На основе аппаратных решений

Поддержка VPN на различных уровнях модели OSI

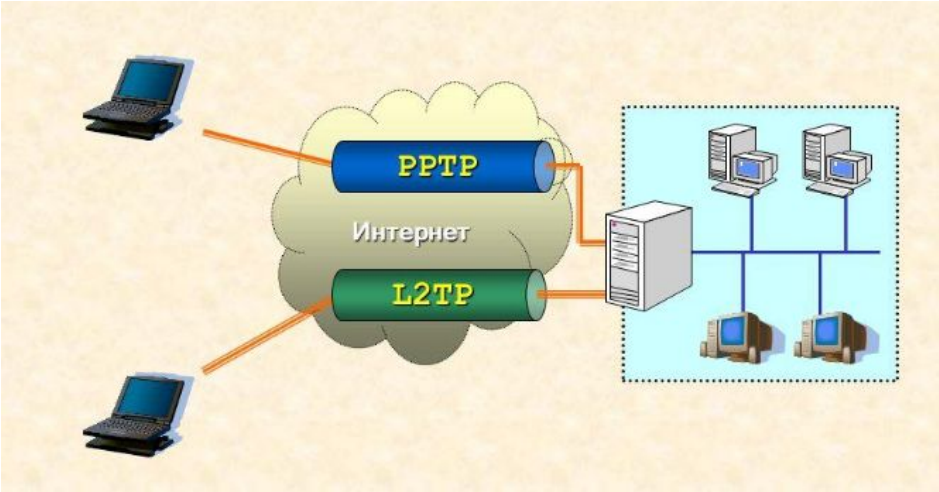
- <u>Канальный уровень:</u>
  - L2TP, PPTP (авторизация и аутентификация)
  - Технология MPLS (установление туннеля)
- <u>Транспортный уровень:</u>
  - SSL/TLS (поддержка шифрования и аутентификации, реализован только для поддержки TCP-трафика)

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		

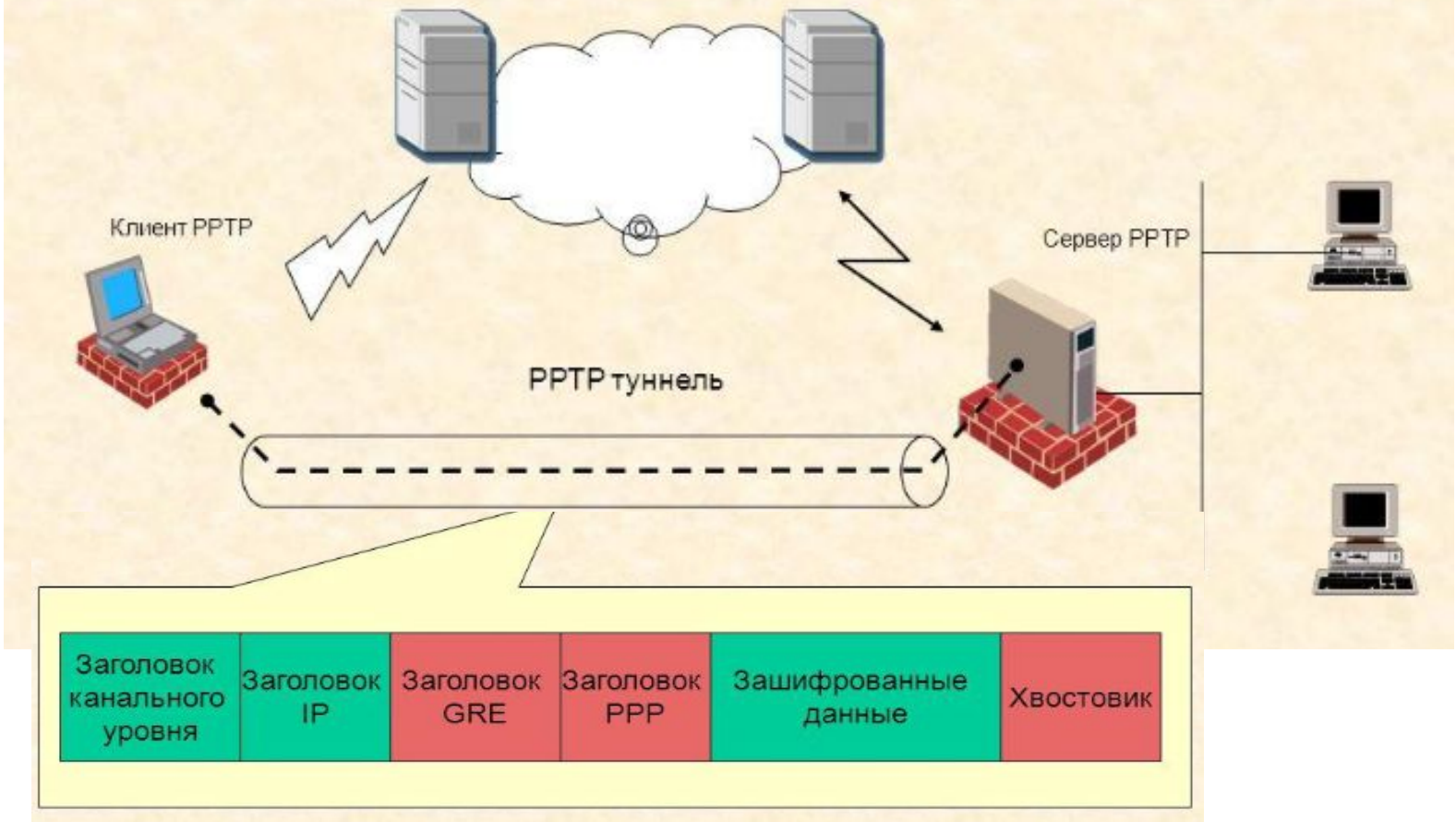
Протоколы канального уровня:

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

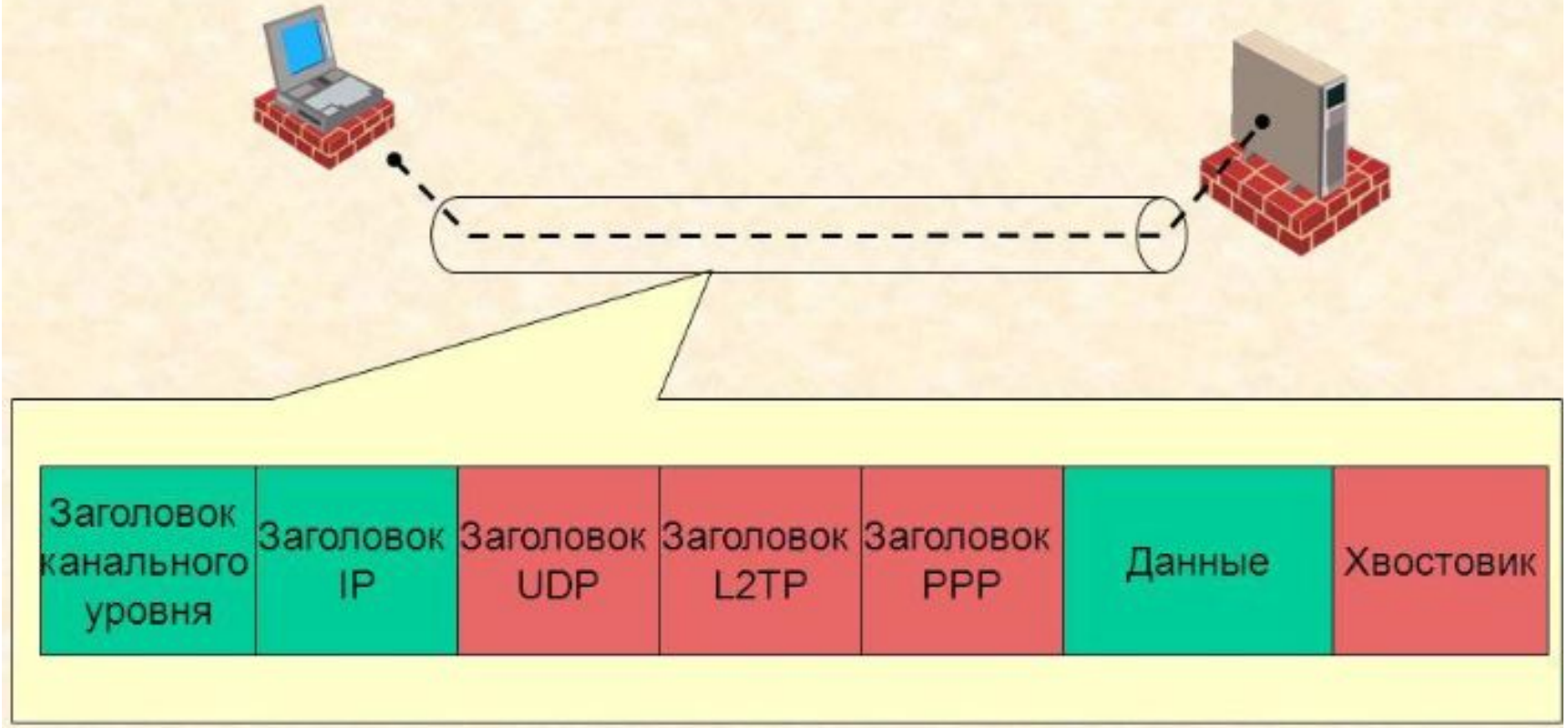
L2TP (Layer to Tunneling Protocol). Инкапсулирует кадры PPP в протокол сетевого уровня, предварительно проведя аутентификацию пользователя



Протокол PPTP



Протокол L2TP



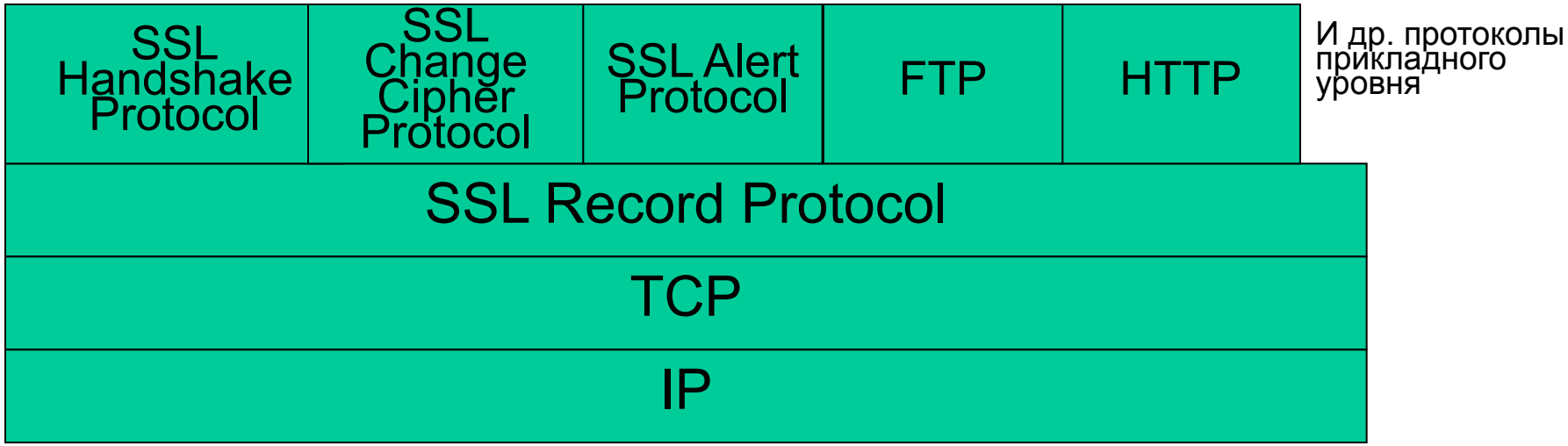
Протоколы транспортного уровня

SSL – (Secure Sockets Layer) уровень защищенных сокетов.

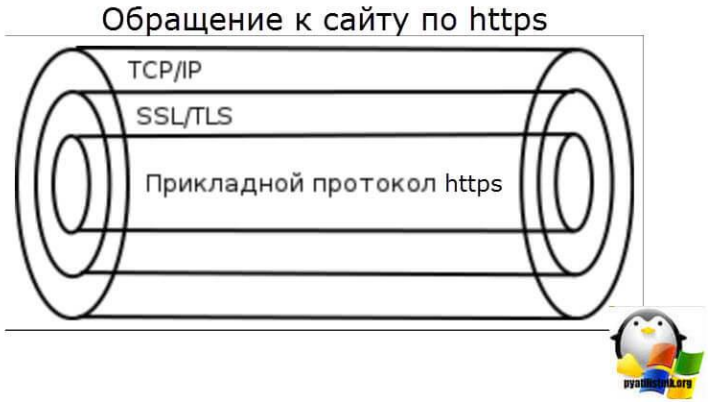
TLS – (Transport Layer Security) безопасность транспортного уровня.

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

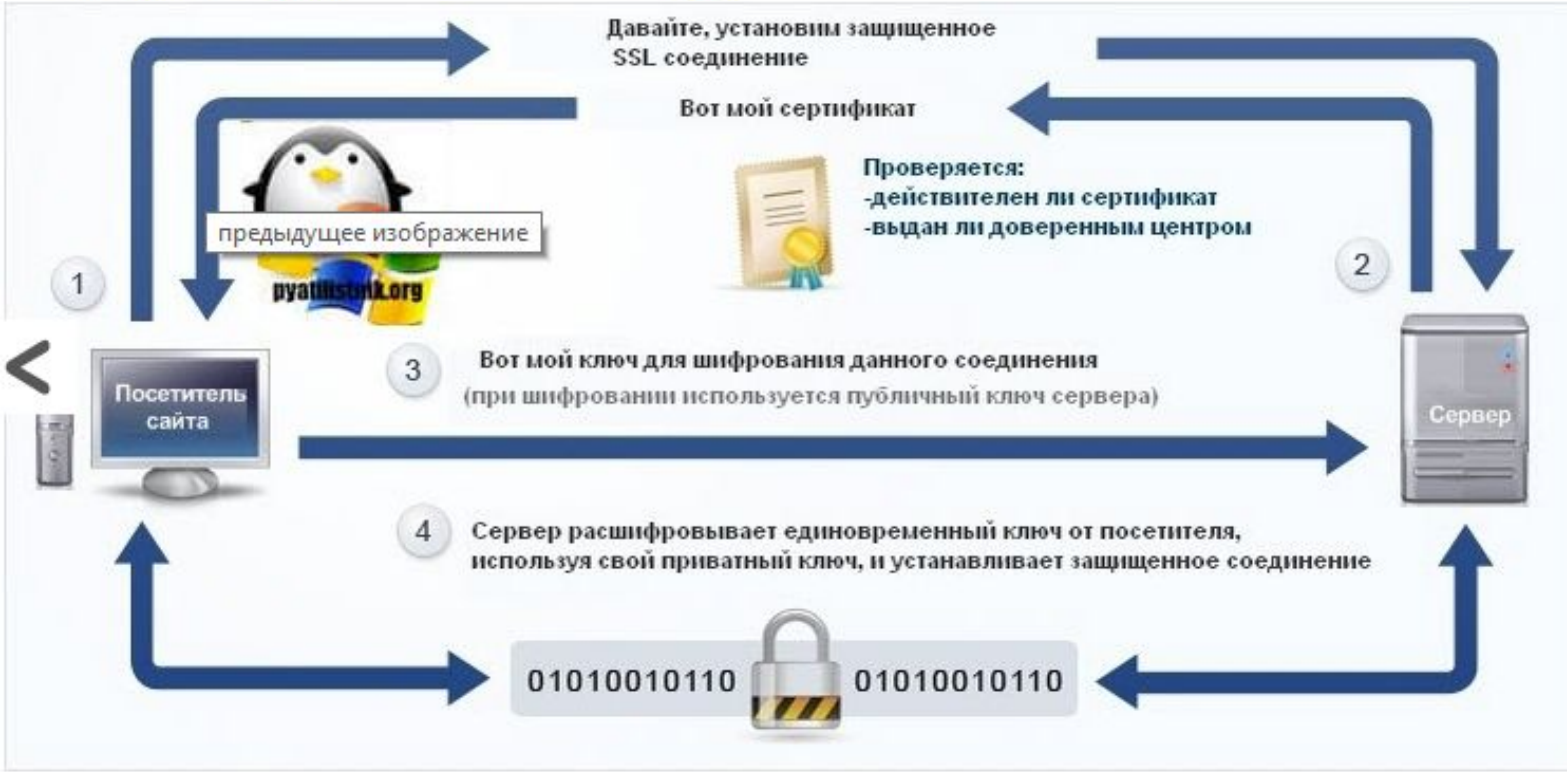
Стек протоколов SSL/TLS

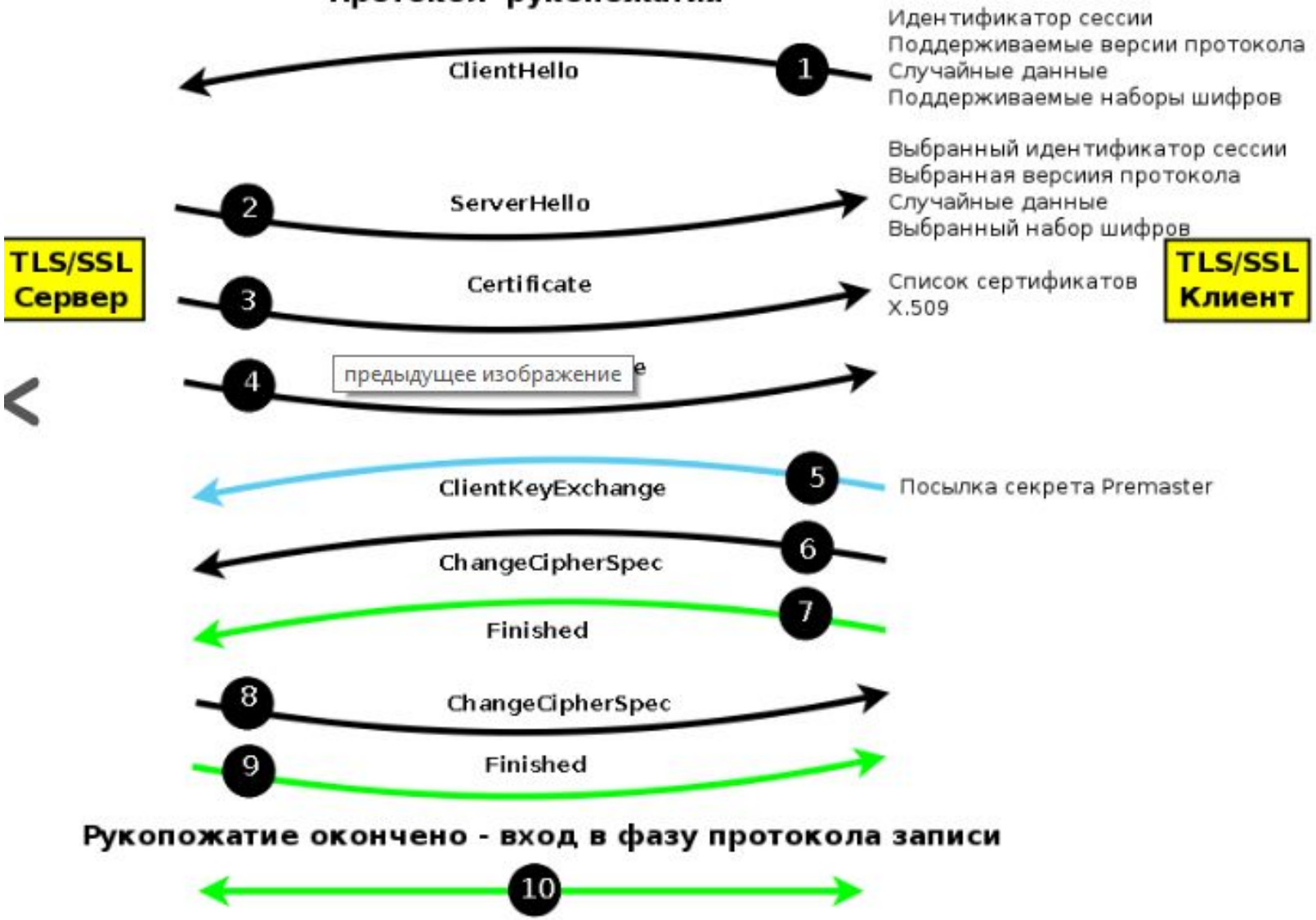


- SSL/TLS реализован поверх TCP (надежность доставки, квитирование), между транспортным и прикладным уровнем.
- <u>Стек протоколов SSL/TLS:</u>
  - SSL Record Protocol: защита передаваемых данных
  - SSL Handshake Protocol: установление сессии (соглашение о используемых алгоритмах, параметры безопасности)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



Этап1: установка защищенного соединения
Этап 2: выдача и проверка сертификата
ИНТЕРНЕТ
Клиент
Сервер (ИКС)
Этап 3: клиент использует открытый ключ
Этап 4: сервер расшифровывает ключ
защищенное соединение установлено,
идет передача данных


Давайте, установим защищенное
SSL соединение
Вот мой сертификат
Проверяется:
-действителен ли сертификат
-выдан ли доверенным центром
предыдущее изображение
1
2
3
Посетитель сайта
Вот мой ключ для шифрования данного соединения
(при шифровании используется публичный ключ сервера)
Сервер
4
Сервер расшифровывает единовременный ключ от посетителя,
используя свой приватный ключ, и устанавливает защищенное соединение
01010010110
01010010110

Последовательность обмена сообщениями протоколов TLS/SSL

Протокол рукопожатия