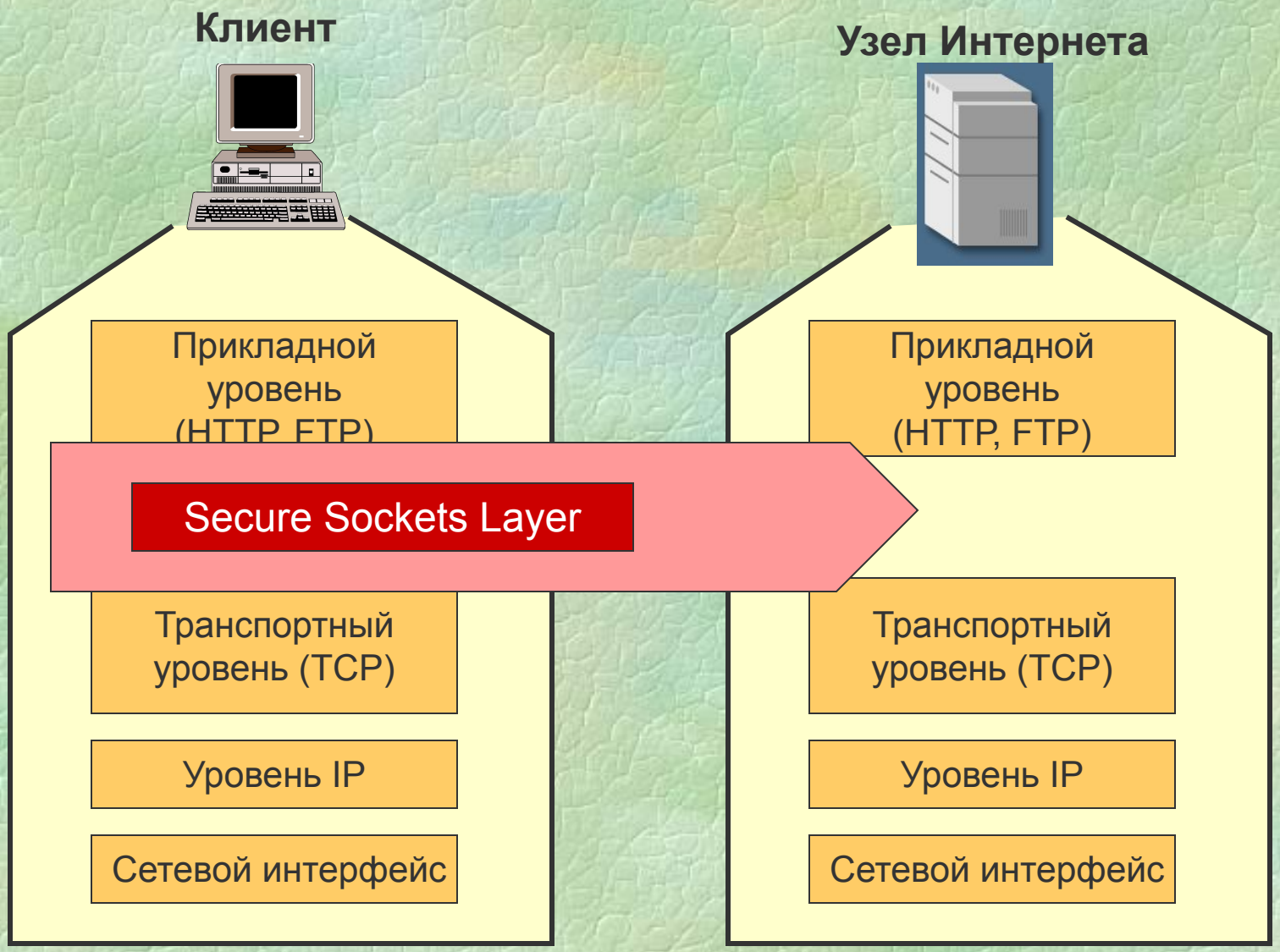
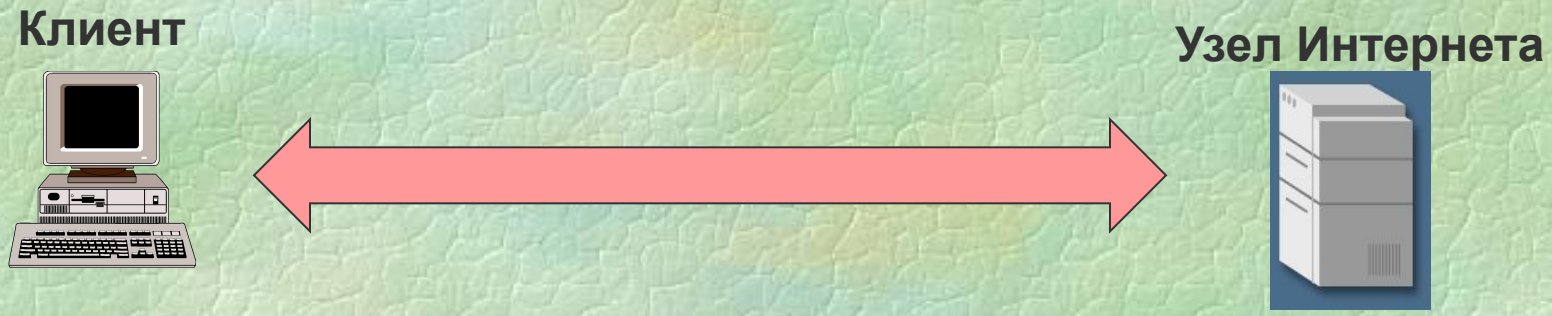
Протокол
Secure Sockets Layer

Архитектура SSL



Архитектура SSL



- **Защищенный канал передачи данных**

  Симметричное шифрование (DES, RC4)

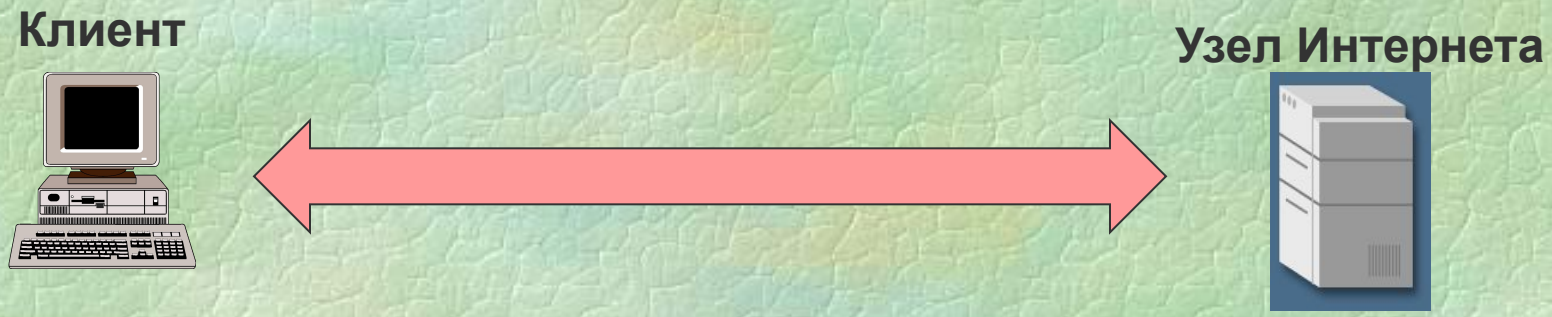
- **Аутентификация сервера**

  Асимметричное шифрование (D-H, RSA)

- **Контроль целостности передаваемых данных**

  Код аутентификации сообщения (MAC)

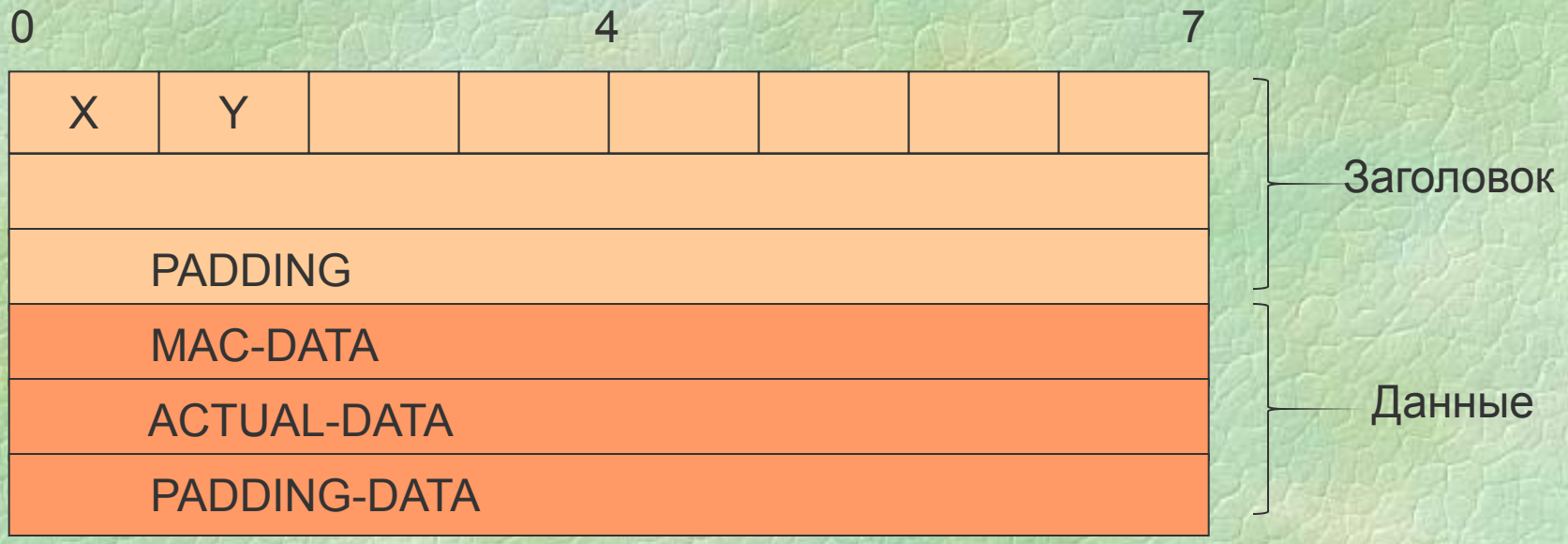
Архитектура SSL



SSL Handshake Protocol ← Установление связи

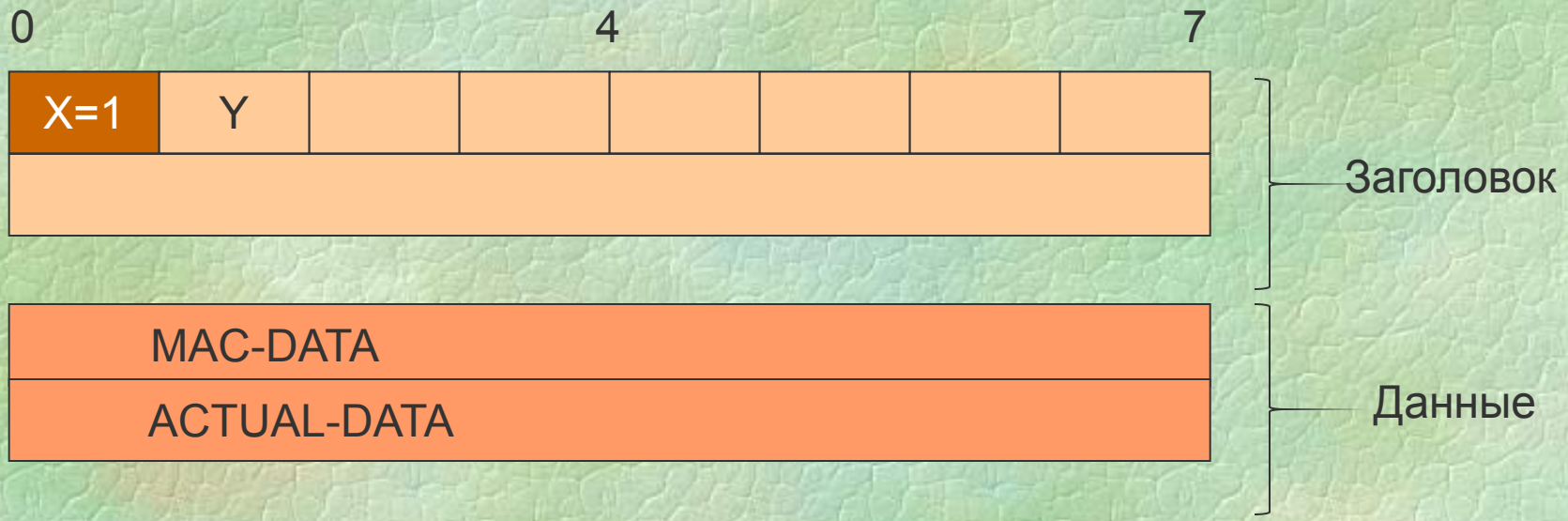
SSL Record Protocol ← Обмен данными

SSL Record Protocol



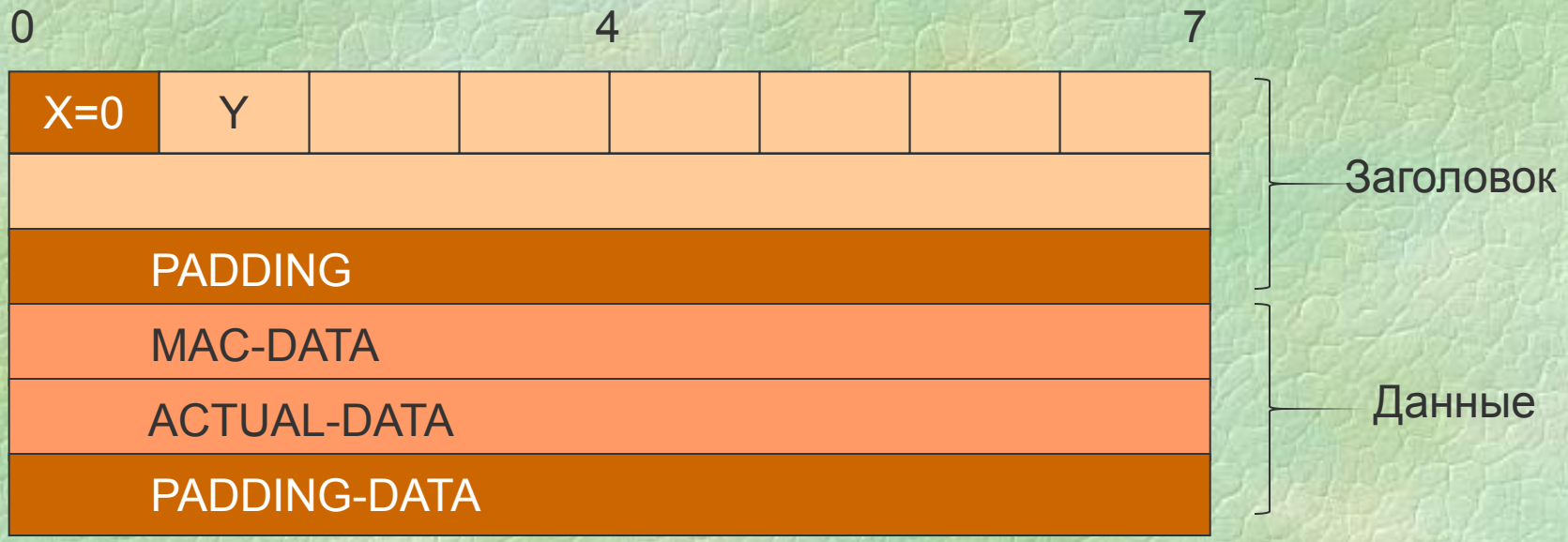
Формат пакета

SSL Record Protocol



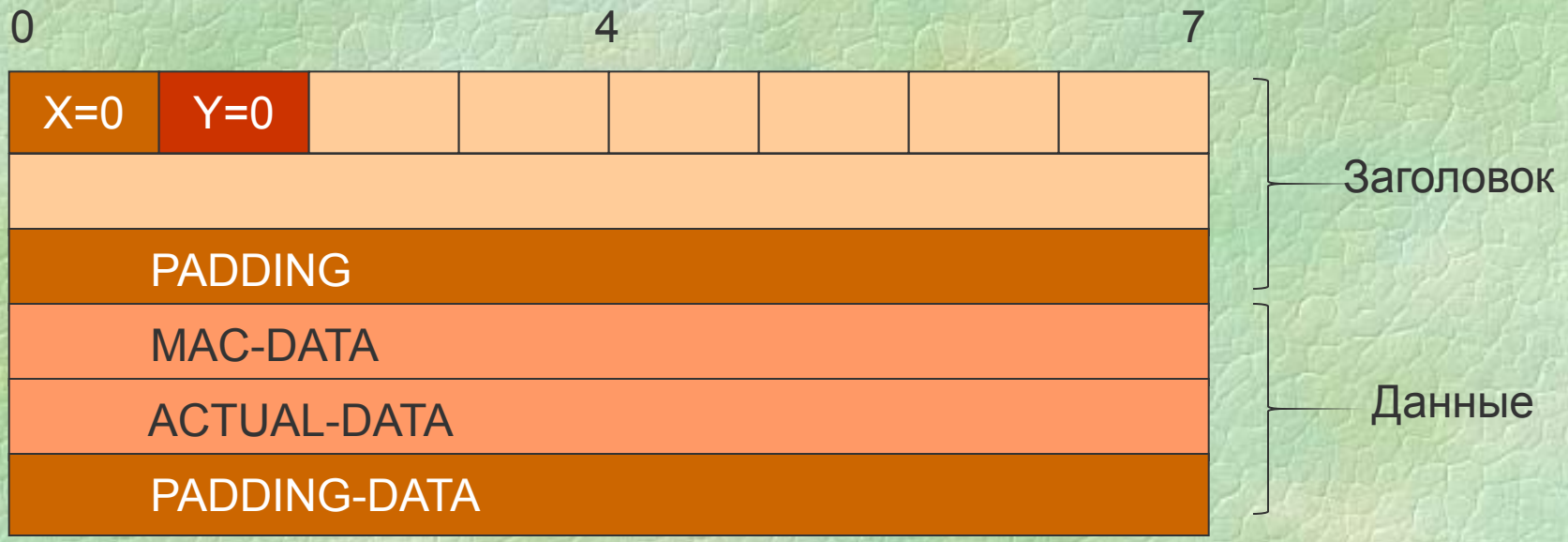
Формат пакета

SSL Record Protocol



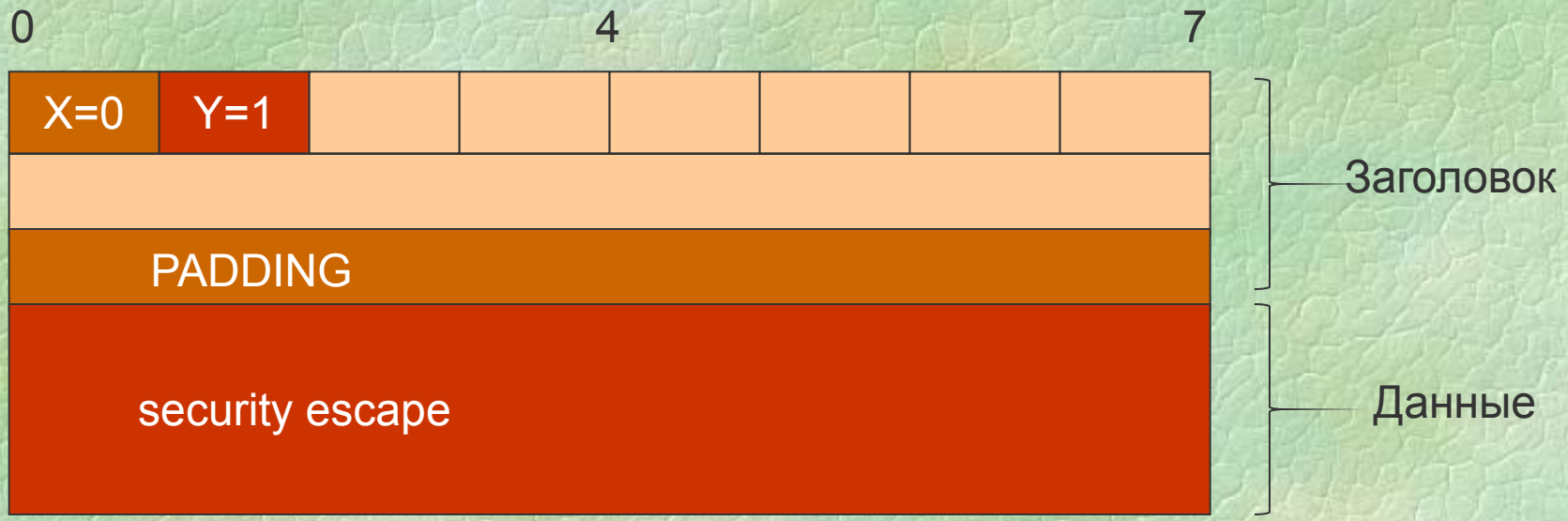
Формат пакета

SSL Record Protocol



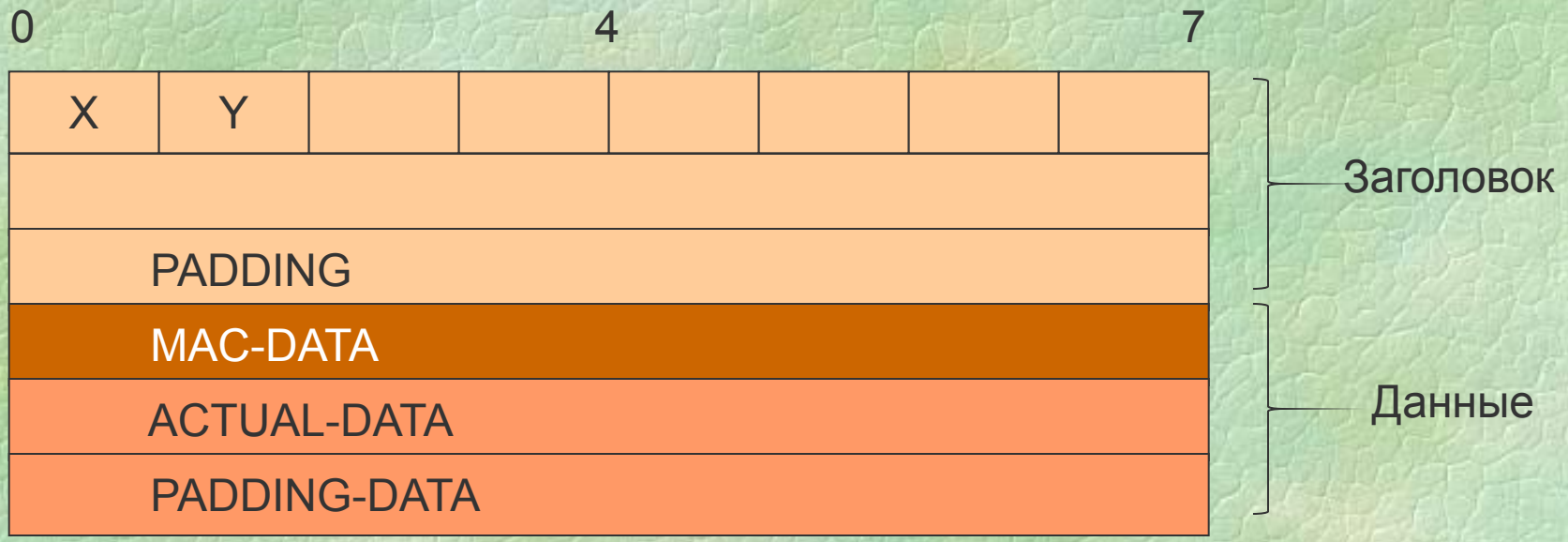
Формат пакета

SSL Record Protocol



Формат пакета

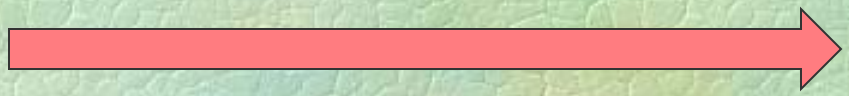
SSL Record Protocol



MAC-DATA=ХЭШ(SECRET, ACTUAL DATA,
PADDING DATA, SEQUENCE NUMBER)

SSL Record Protocol

Клиент



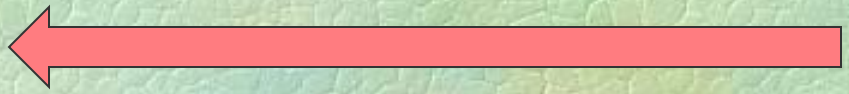
Узел Интернета

MAC-DATA=ХЭШ(**SECRET**, ACTUAL DATA,
PADDING DATA, SEQUENCE NUMBER)

SECRET - Закрытый ключ клиента

SSL Record Protocol

Клиент

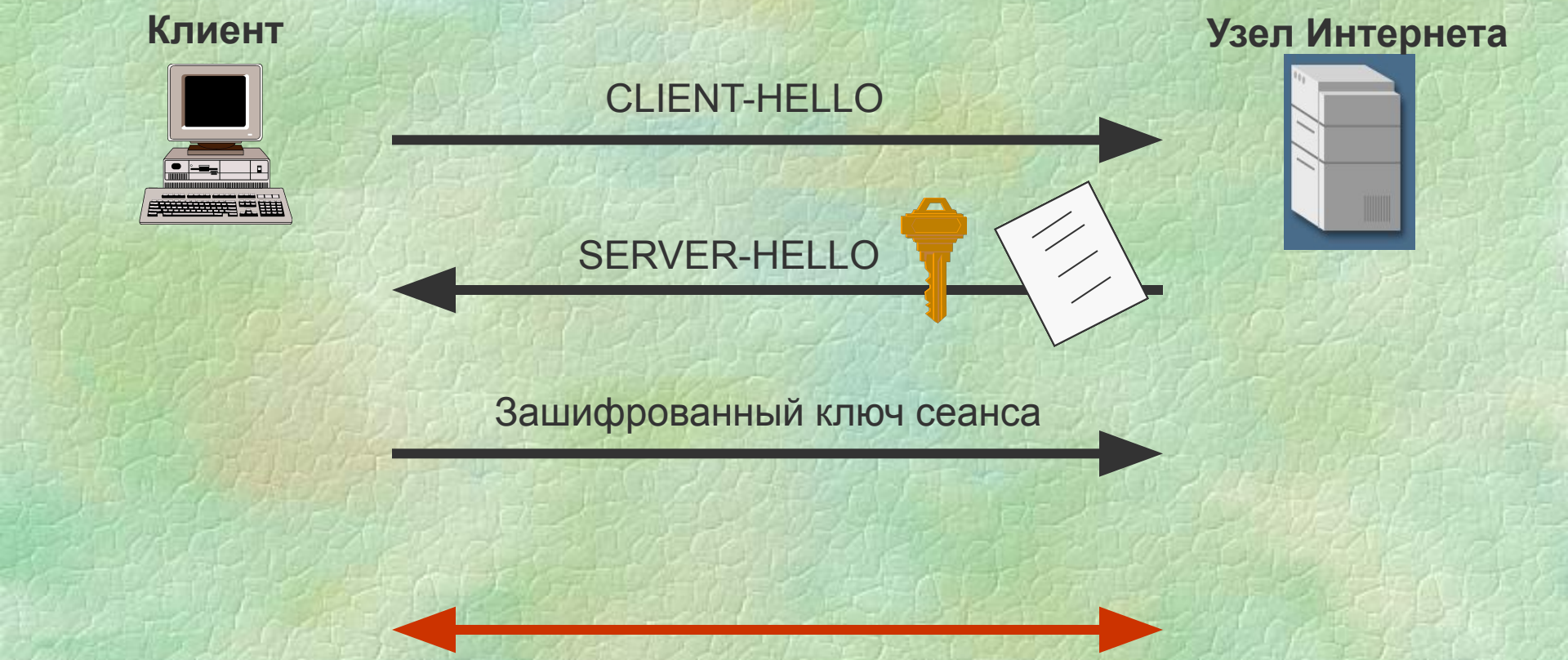


Узел Интернета

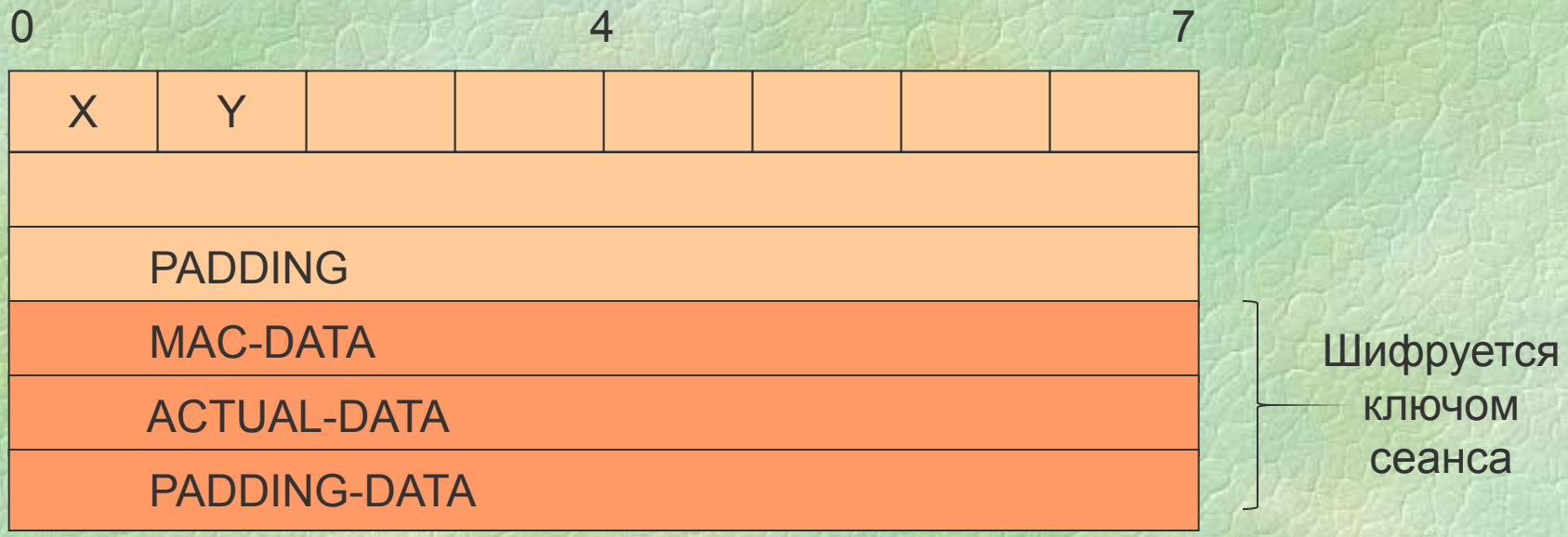
MAC-DATA=ХЭШ(**SECRET**, ACTUAL DATA,
PADDING DATA, SEQUENCE NUMBER)

SECRET - Открытый ключ клиента

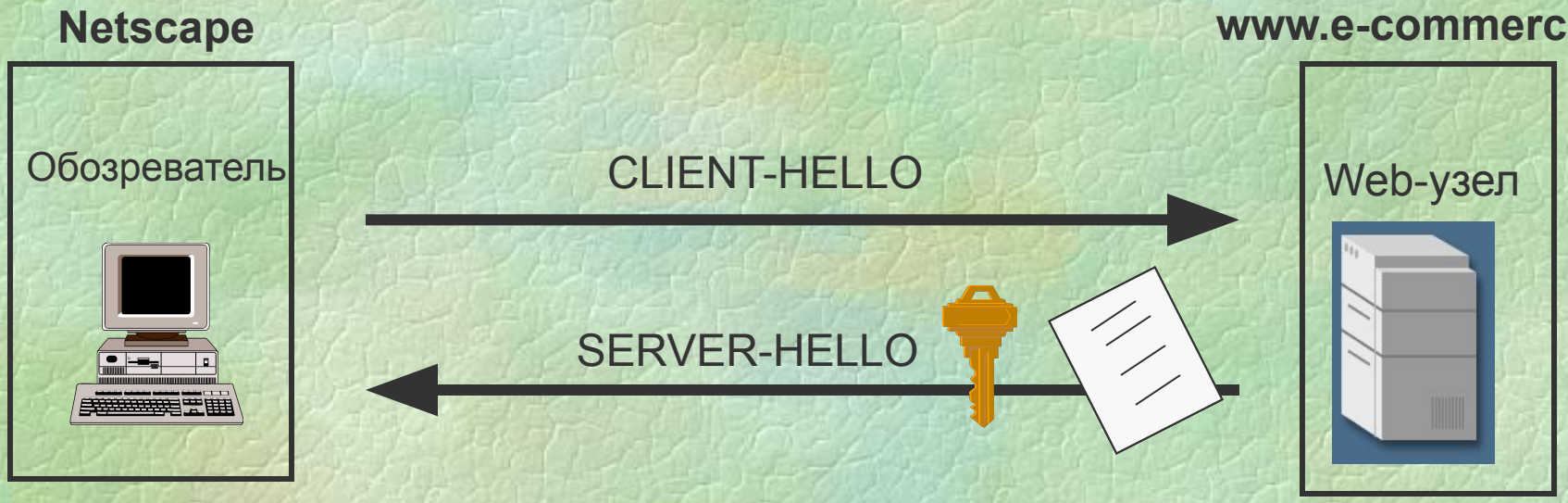
SSL Handshake Protocol



Шифрование данных



0шибка реализации SSL в Netscape



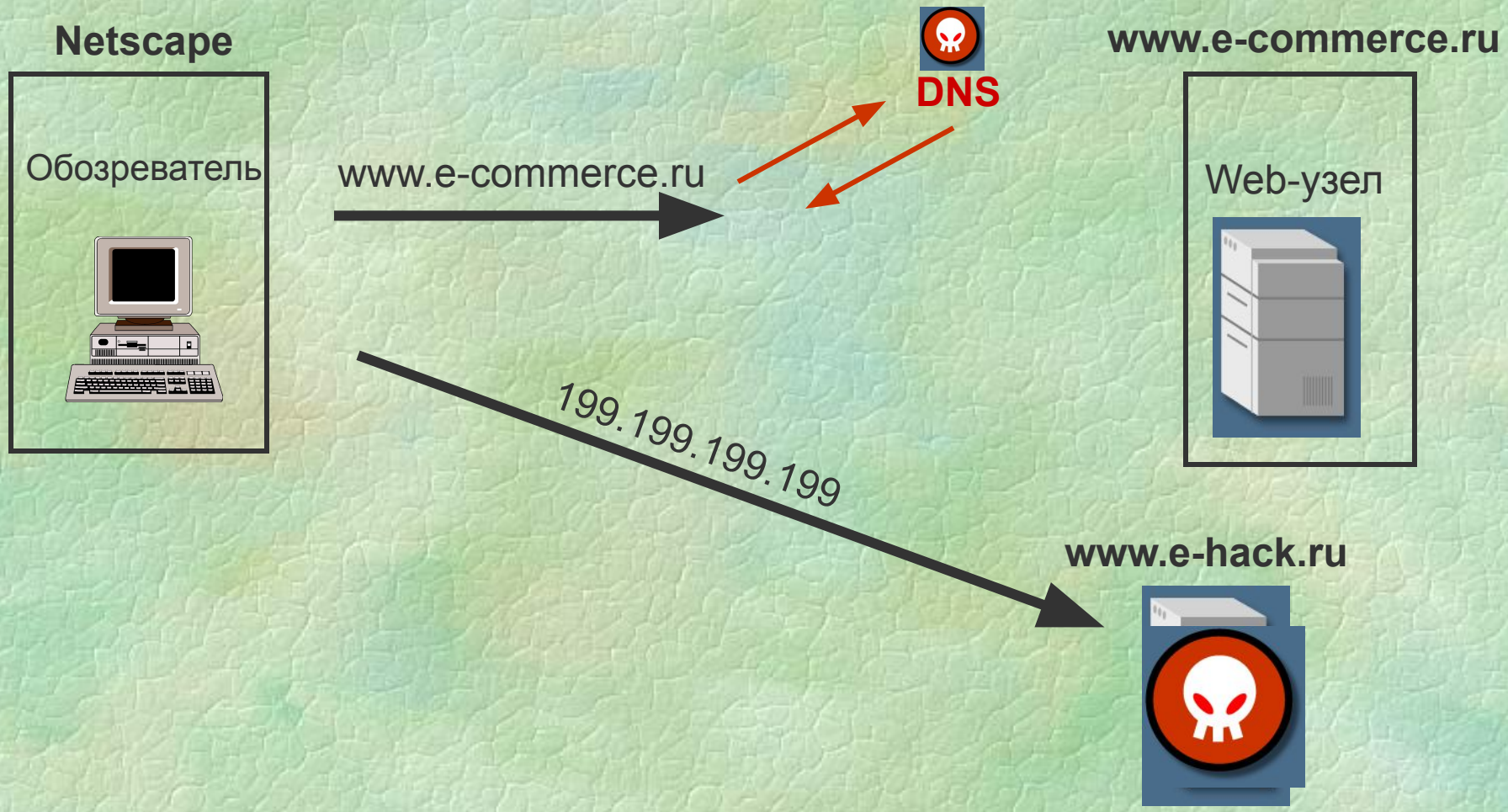
Сертификат выдан организацией, которая есть в доверительном списке у клиента

Сертификат не просрочен

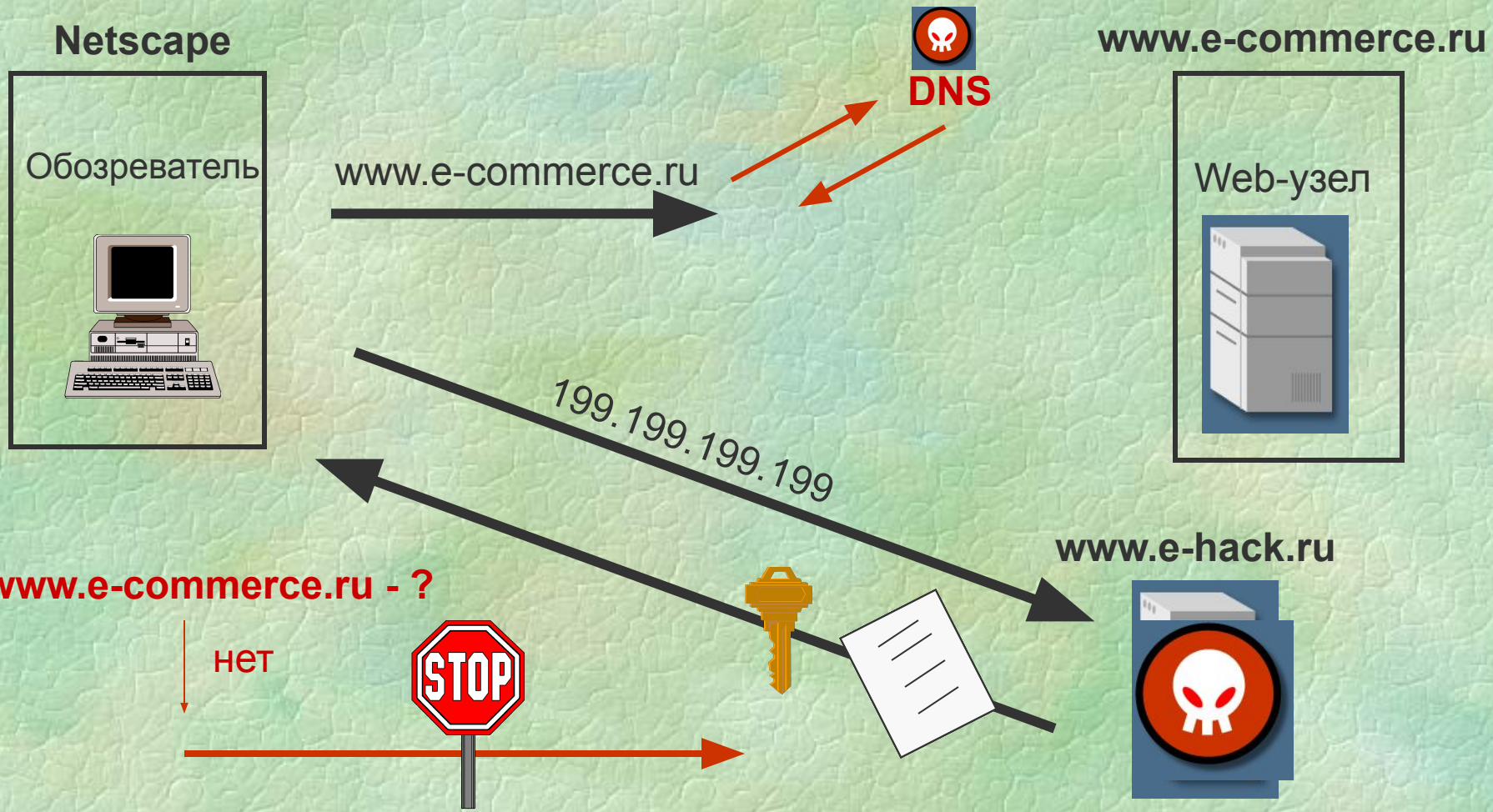
Сертификат содержит имя сервера, с которым клиент устанавливает соединение

Установление соединения без SSL

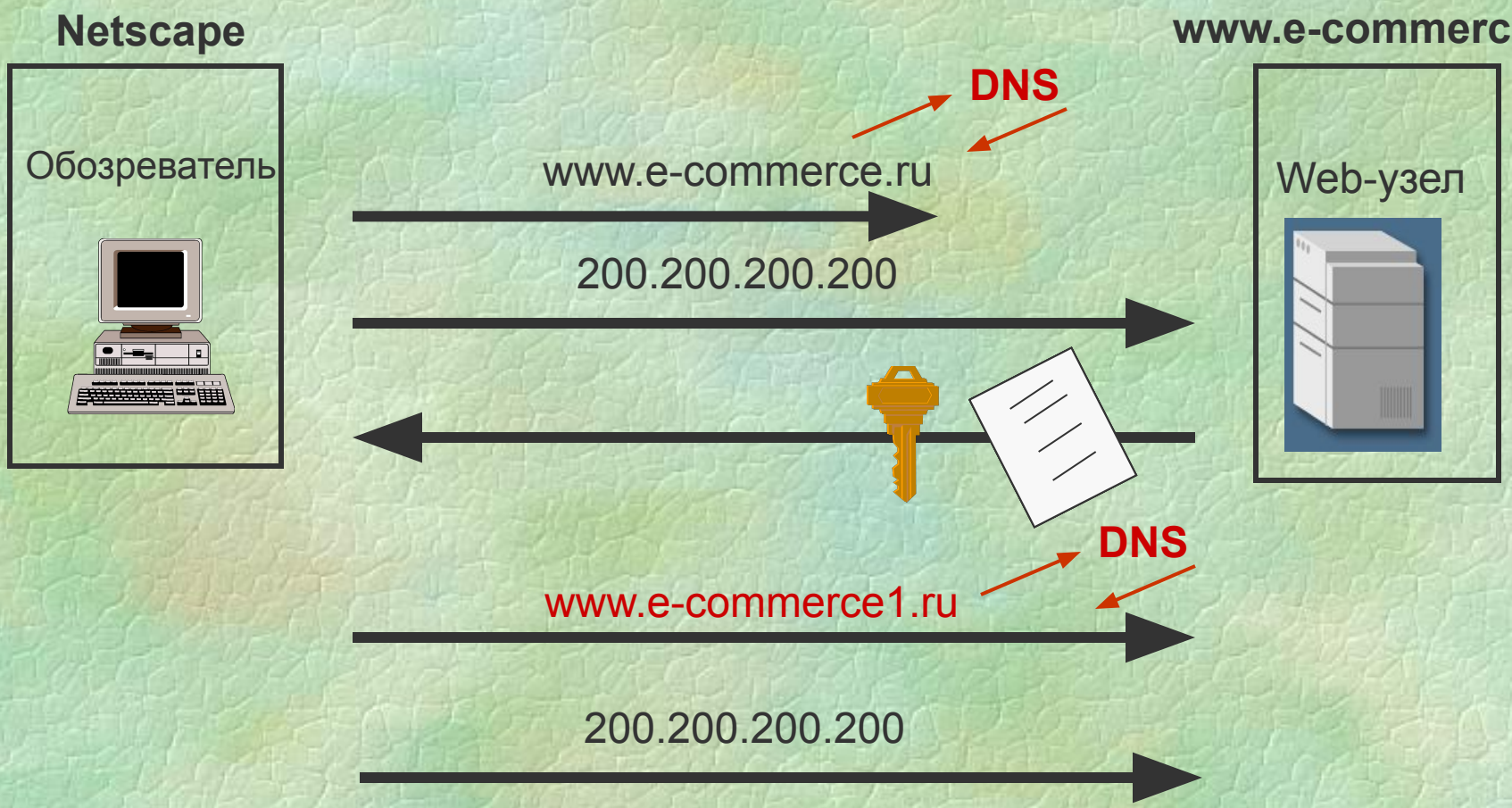
Установление соединения без SSL



Установление соединения с использованием SSL



0шибка реализации SSL в Netscape



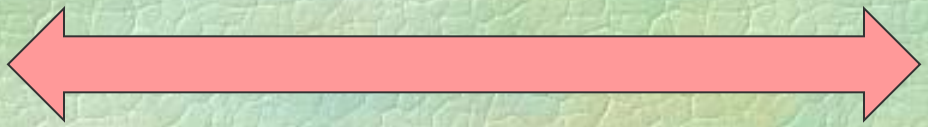
Netscape 4.72, 4.61, 4.07

Netscape 4.73

Протокол SSH

Возможности SSH

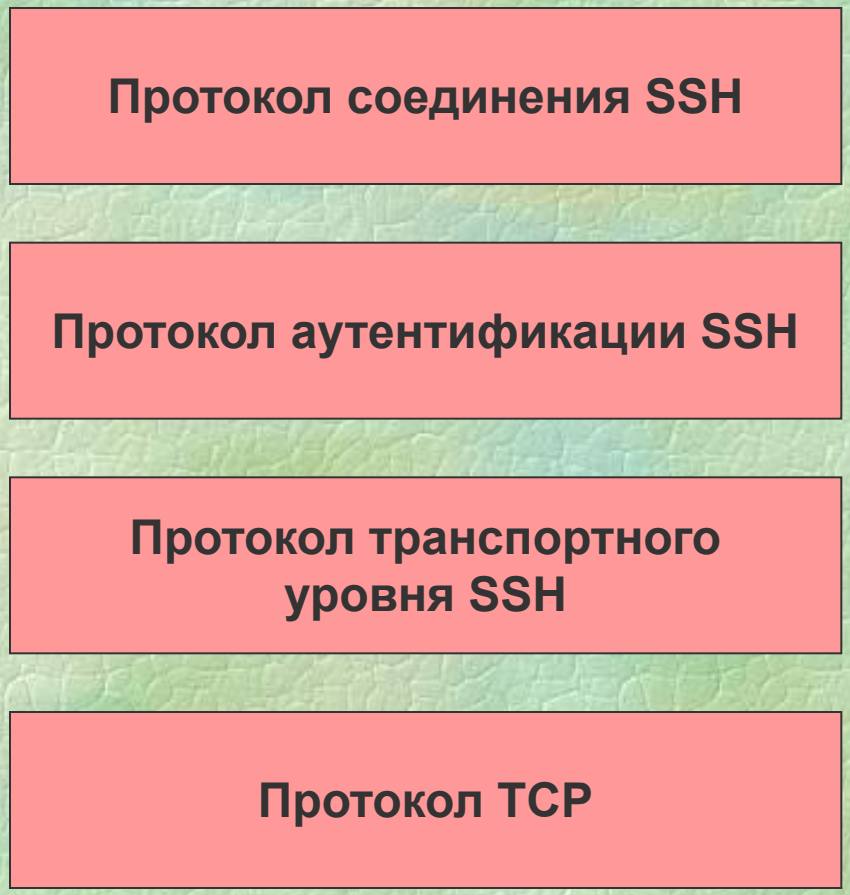
Клиент



Сервер

- Безопасная работа с TELNET
- Безопасная замена r - команд

Архитектура SSH



Ключи SSH

Клиент

Сервер

Ключ узла

Ключ пользователя

SSHD

Ключ демона

Ключ сервера

Сервер

Ключ узла - сервера

Клиент

Имя узла1 - Открытый ключ узла 1
Имя узла2 - Открытый ключ узла 2
.
.
.

Ключ сервера

Сервер

Ключ узла - сервера

Клиент

Сертификационный агент - Открытый ключ

Сертификационный агент

Имя узла1 - Открытый ключ узла 1
Имя узла2 - Открытый ключ узла 2
.
.
.

Установление соединения

Практическая работа 15

Работа с протоколом SSH