

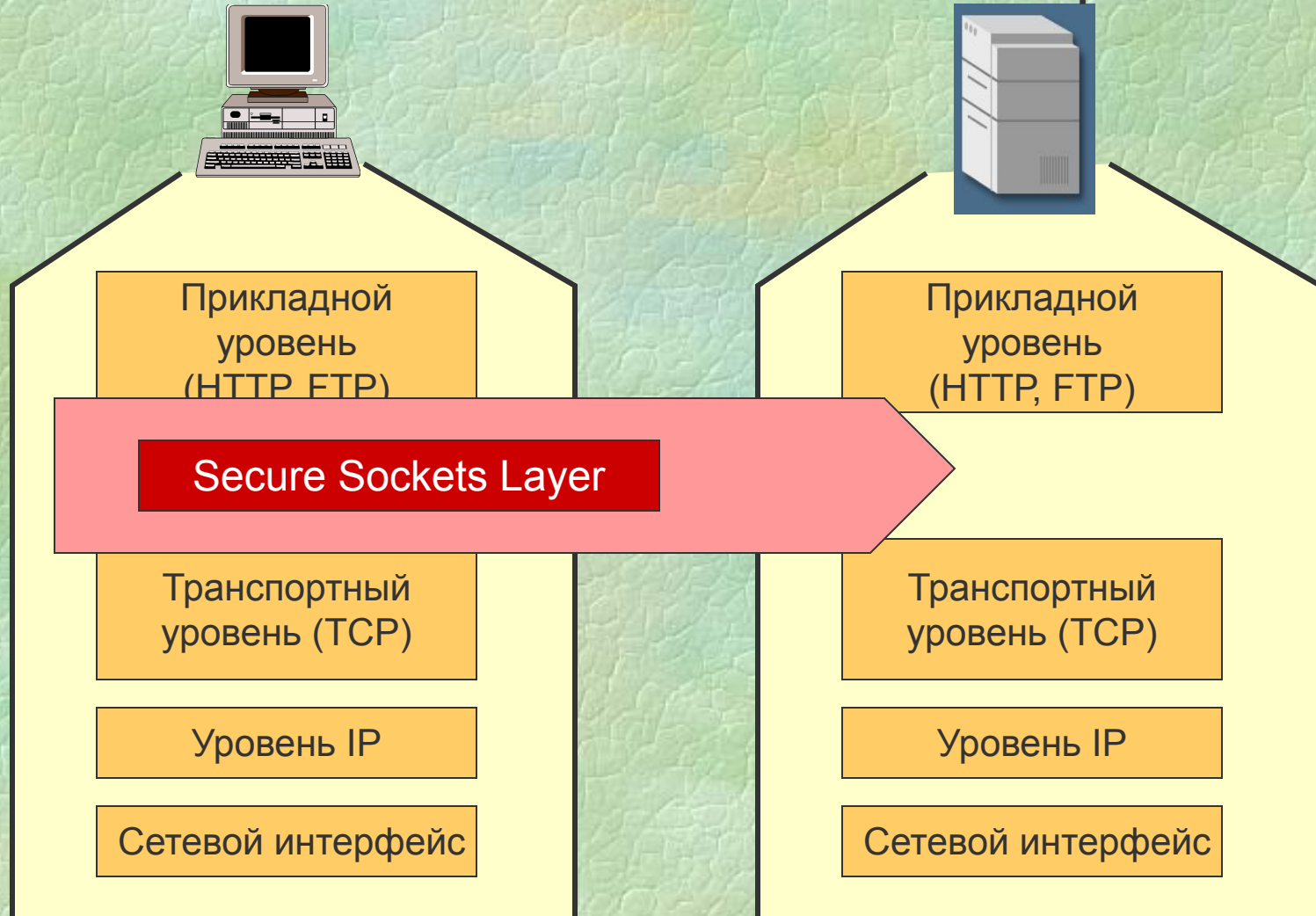
Протокол Secure Sockets Layer

Архитектура SSL

Клиент



Узел Интернета

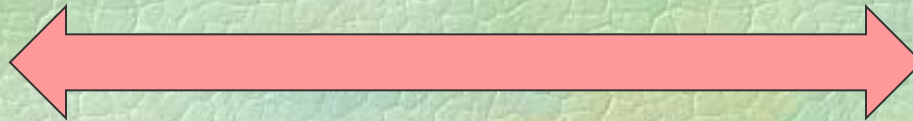


Архитектура SSL

Клиент



Узел Интернета



Защищенный канал передачи данных

Симметричное шифрование (DES, RC4)



Аутентификация сервера

Асимметричное шифрование (D-H, RSA)



Контроль целостности передаваемых данных

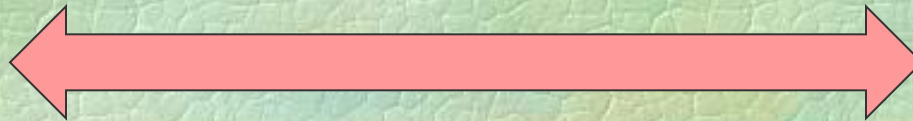
Код аутентификации сообщения (MAC)

Архитектура SSL

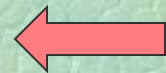
Клиент



Узел Интернета

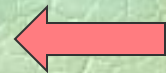


SSL Handshake Protocol

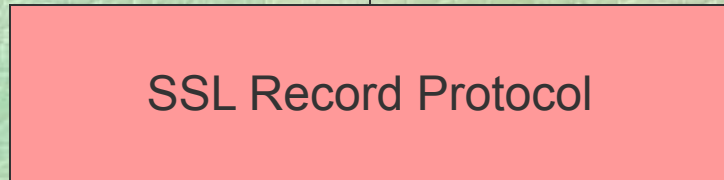
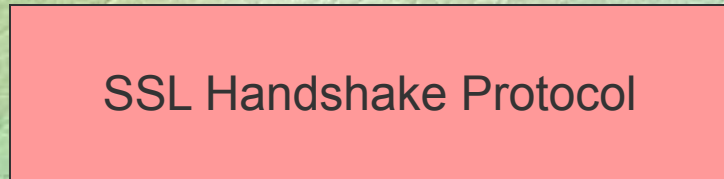


Установление связи

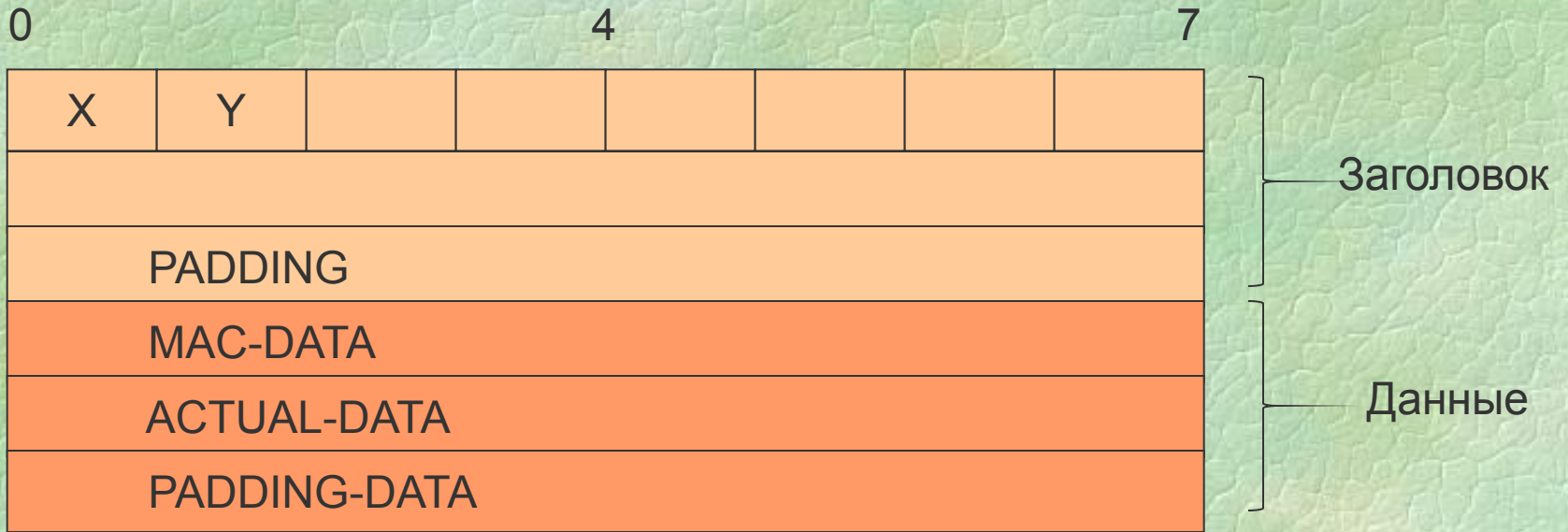
SSL Record Protocol



Обмен данными

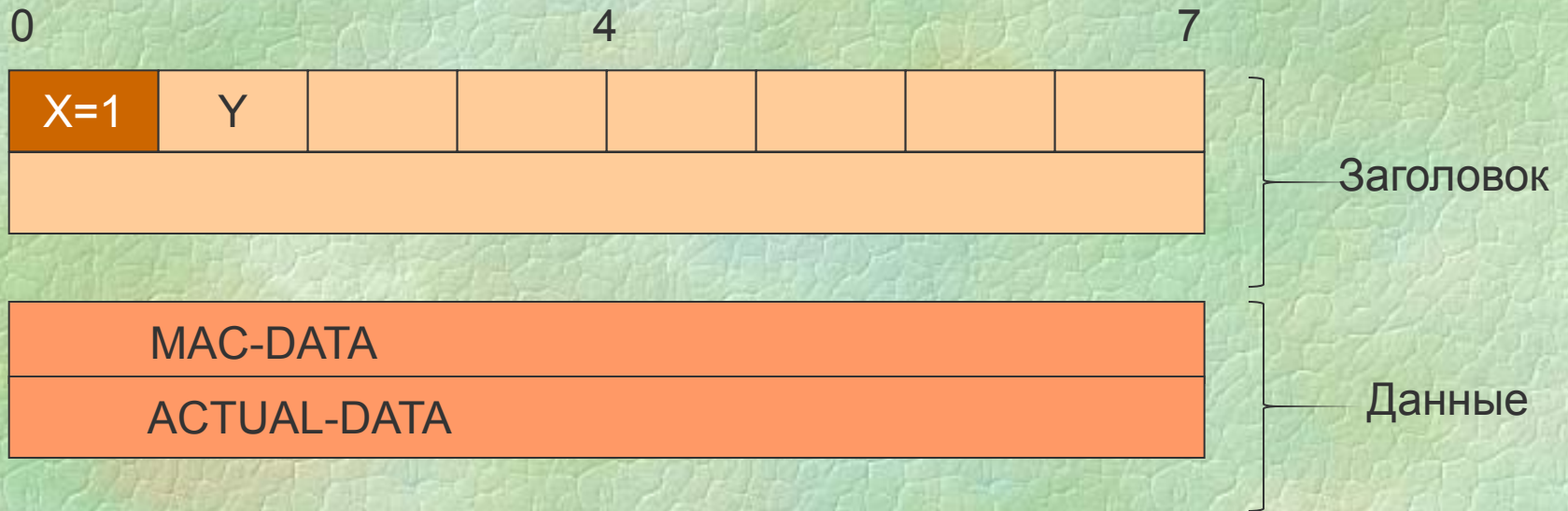


SSL Record Protocol



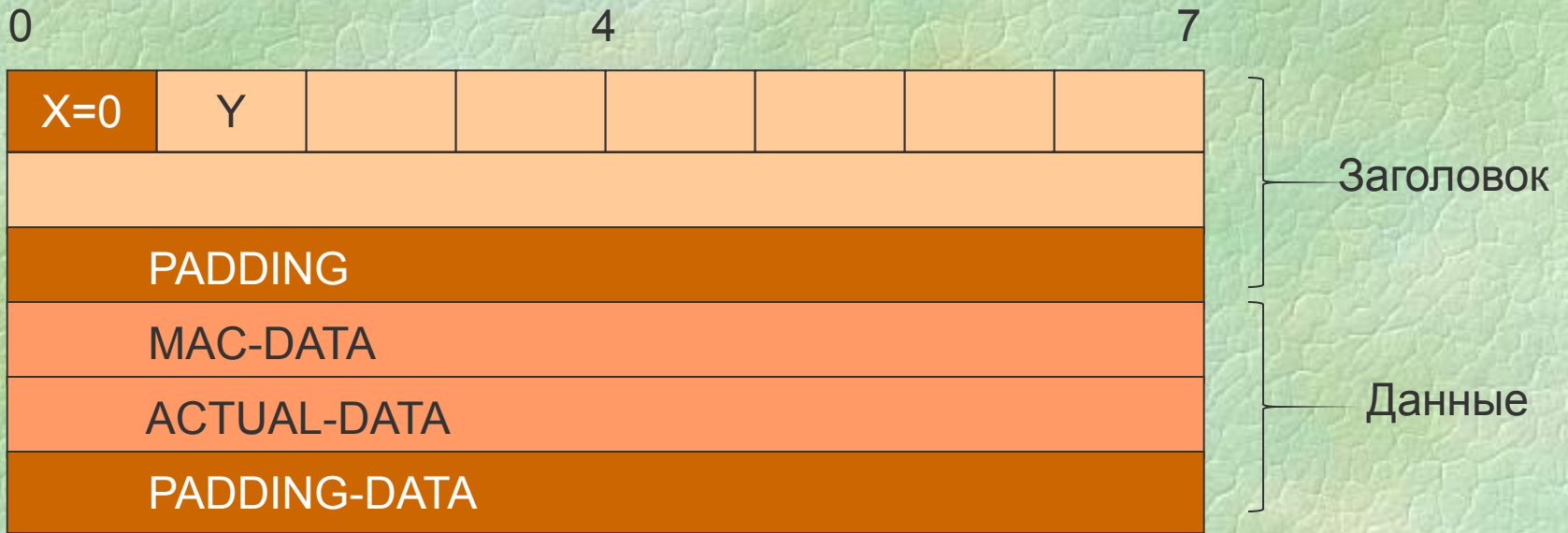
Формат пакета

SSL Record Protocol



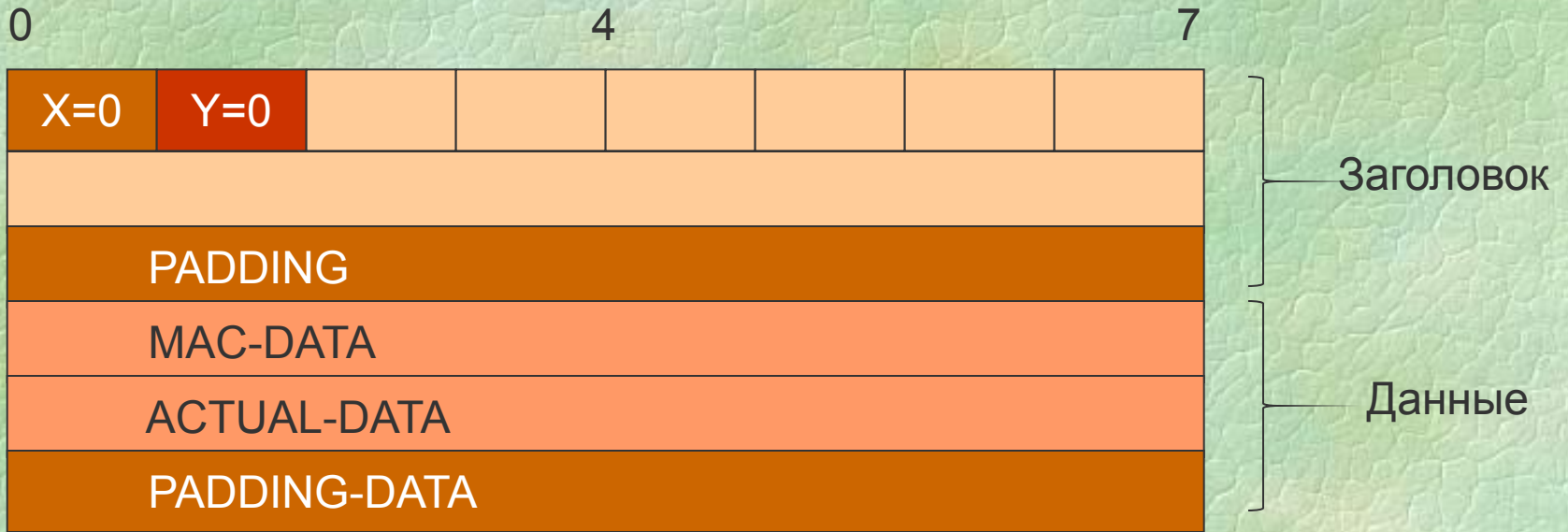
Формат пакета

SSL Record Protocol



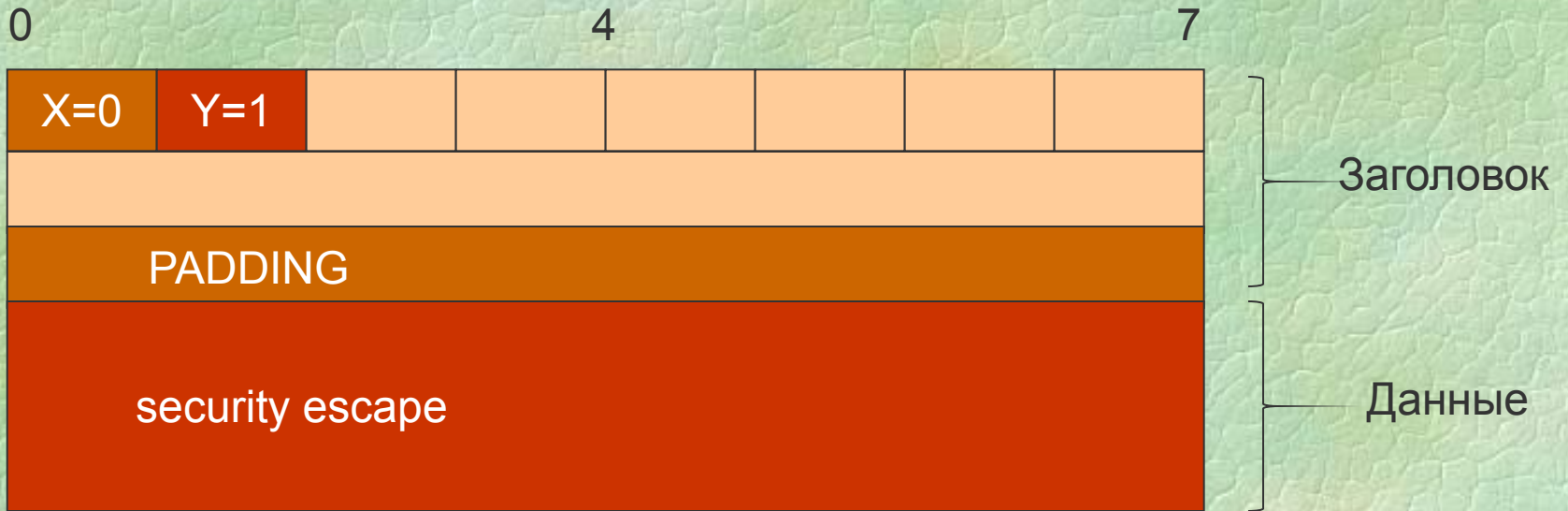
Формат пакета

SSL Record Protocol



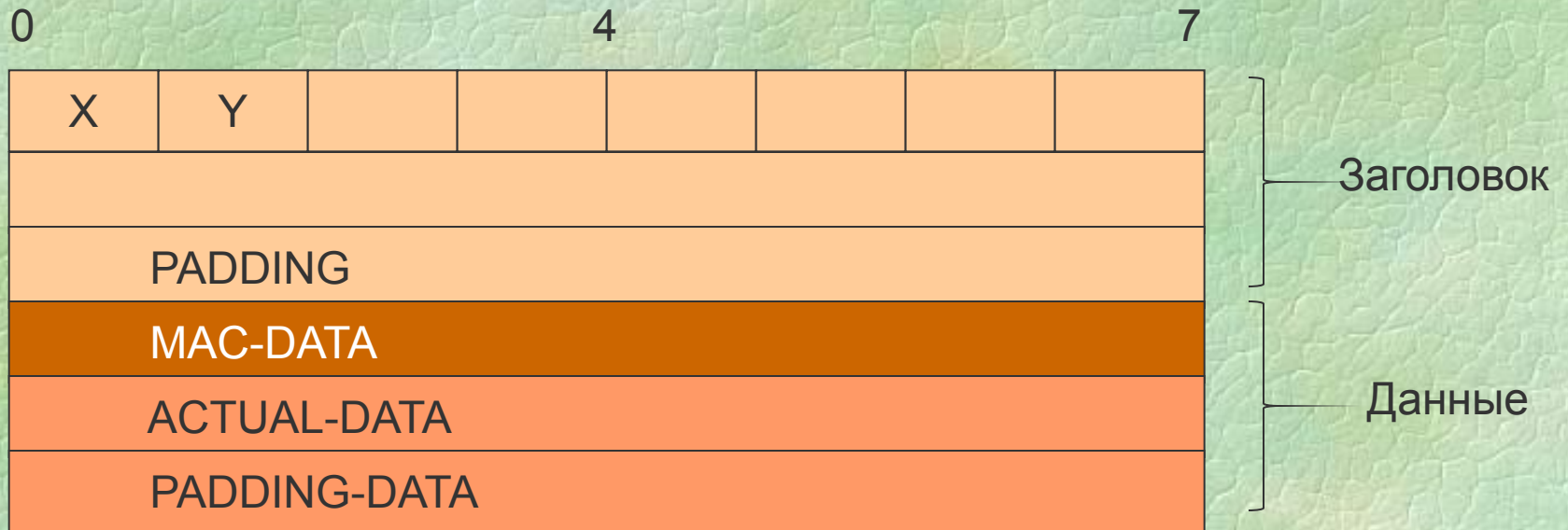
Формат пакета

SSL Record Protocol



Формат пакета

SSL Record Protocol



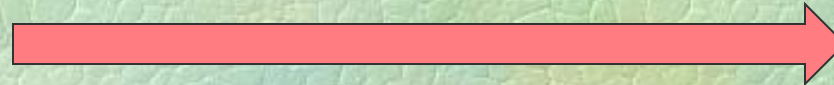
$MAC-DATA = XЭШ(SECRET, ACTUAL DATA, PADDING DATA, SEQUENCE NUMBER)$

SSL Record Protocol

Клиент



Узел Интернета



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

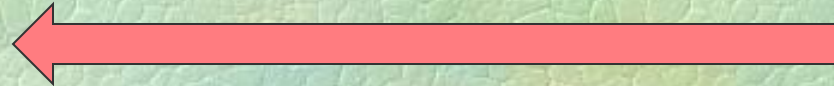
SECRET - Закрытый ключ клиента

SSL Record Protocol

Клиент



Узел Интернета



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

SECRET - Открытый ключ клиента

SSL Handshake Protocol

Клиент



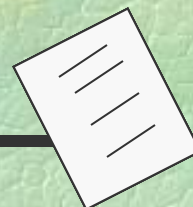
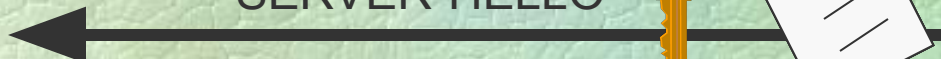
Узел Интернета



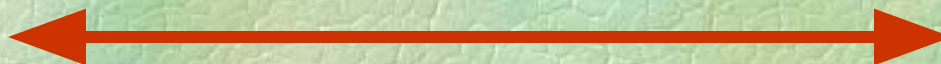
CLIENT-HELLO



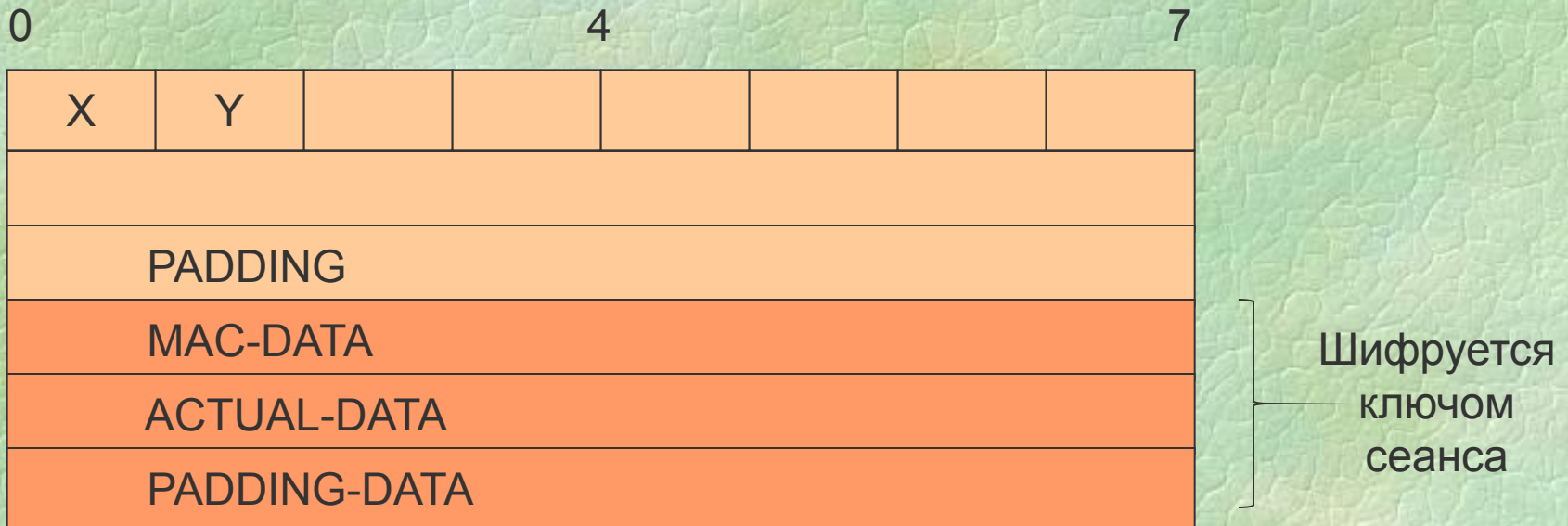
SERVER-HELLO



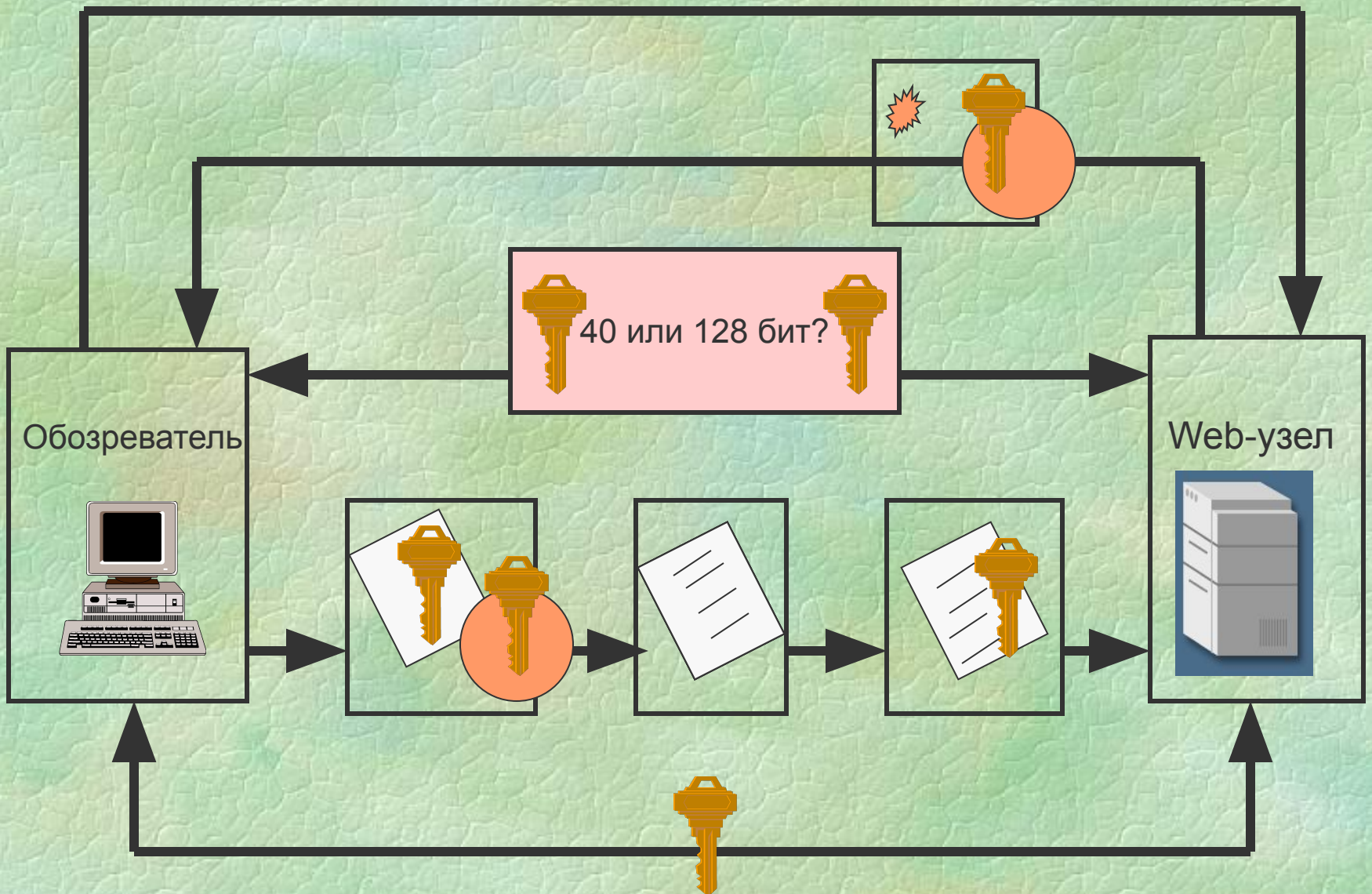
Зашифрованный ключ сеанса



Шифрование данных



Сеанс SSL в IIS 4.0



Ошибка реализации SSL в Netscape



Сертификат выдан организацией, которая есть в доверительном списке у клиента

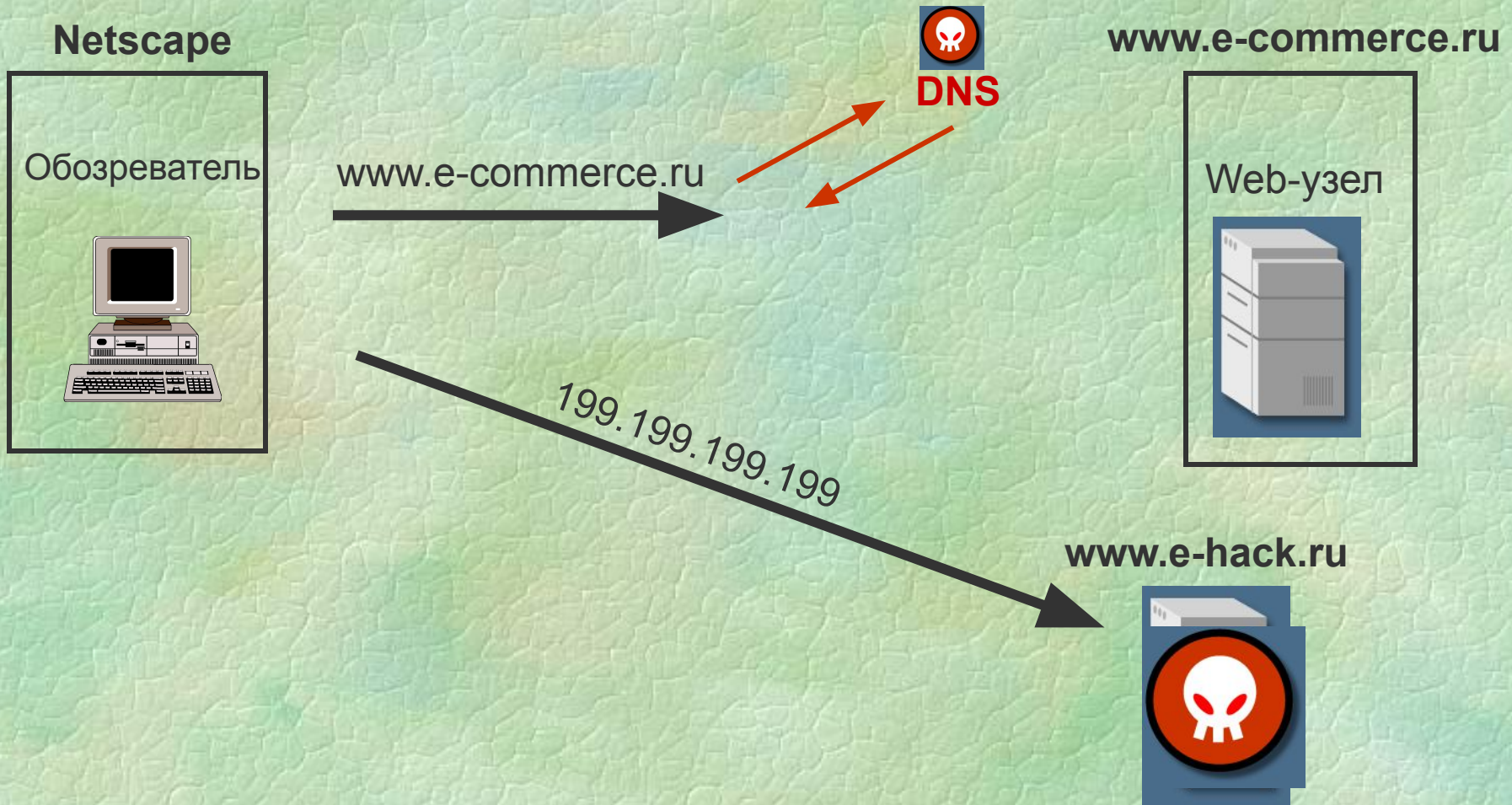
Сертификат не просрочен

Сертификат содержит имя сервера, с которым клиент устанавливает соединение

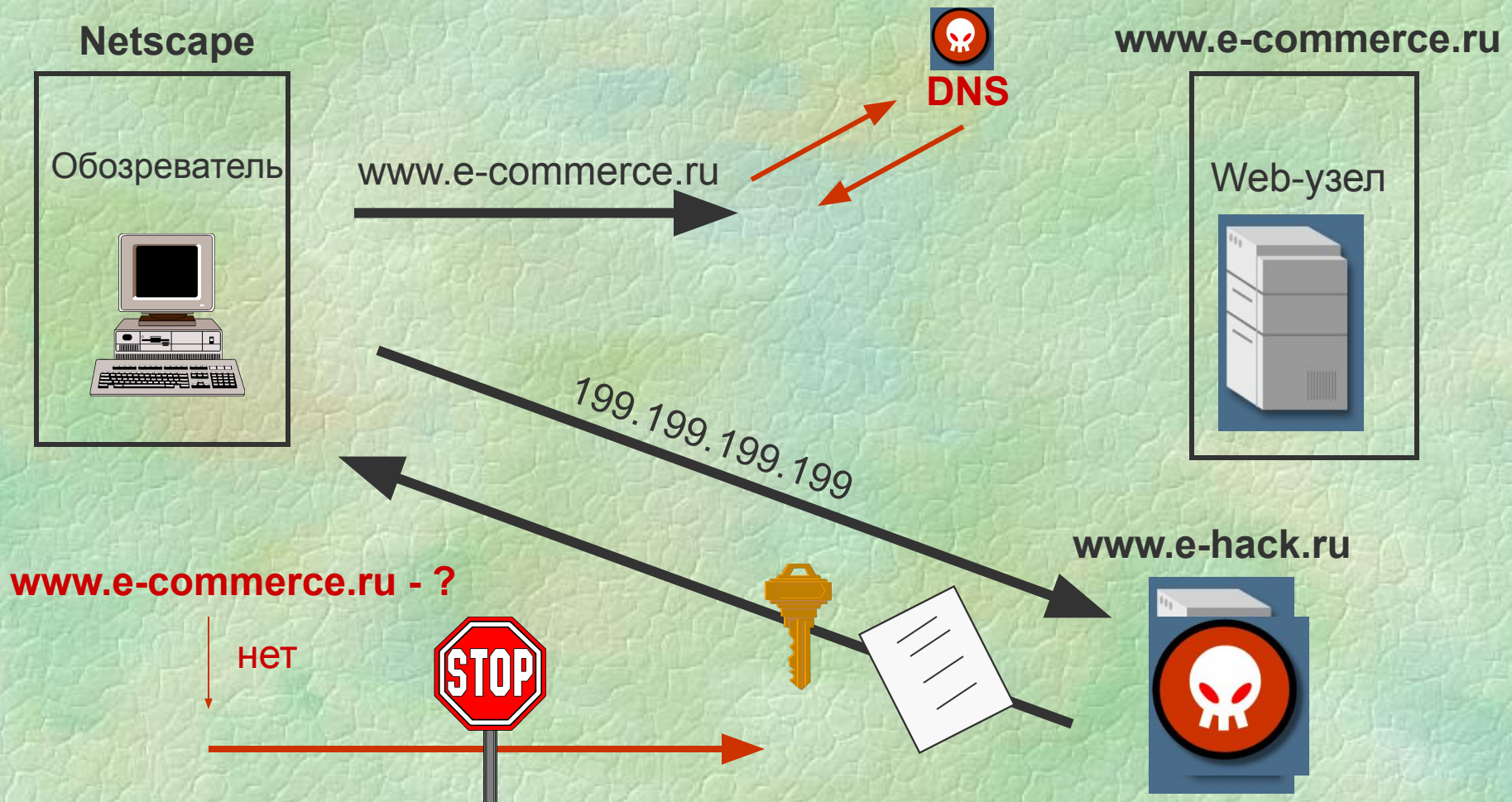
Установка соединения без SSL



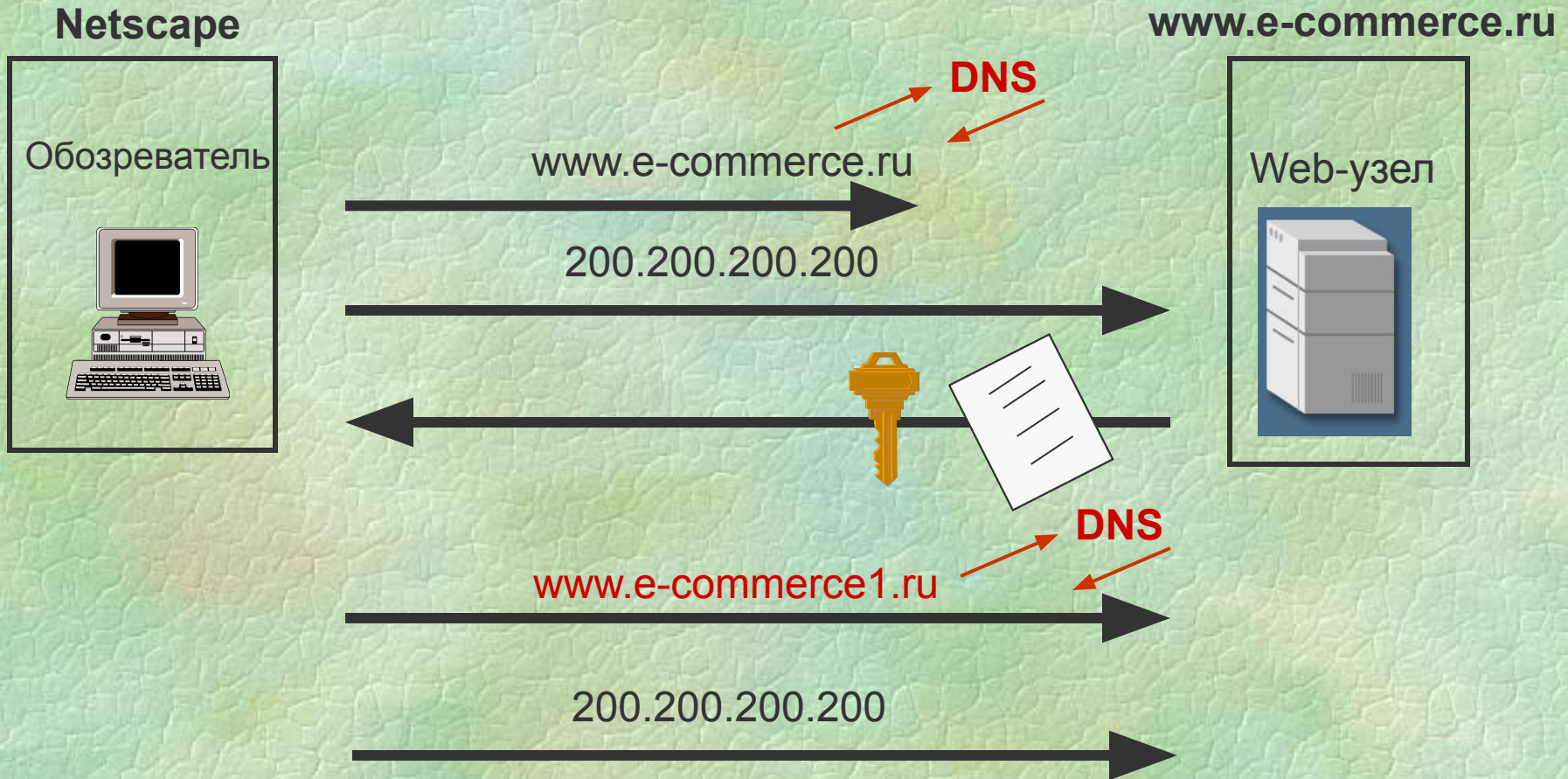
Установка соединения без SSL



Установление соединения с использованием SSL



Ошибка реализации SSL в Netscape



Netscape 4.72, 4.61, 4.07

Netscape 4.73