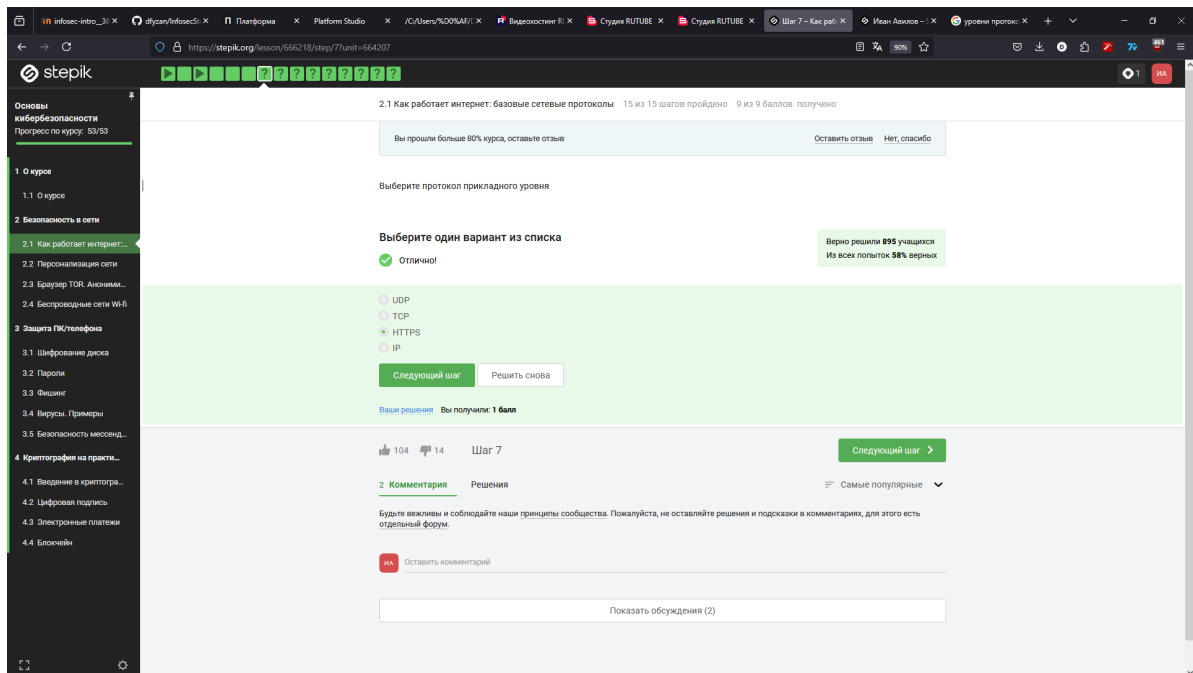
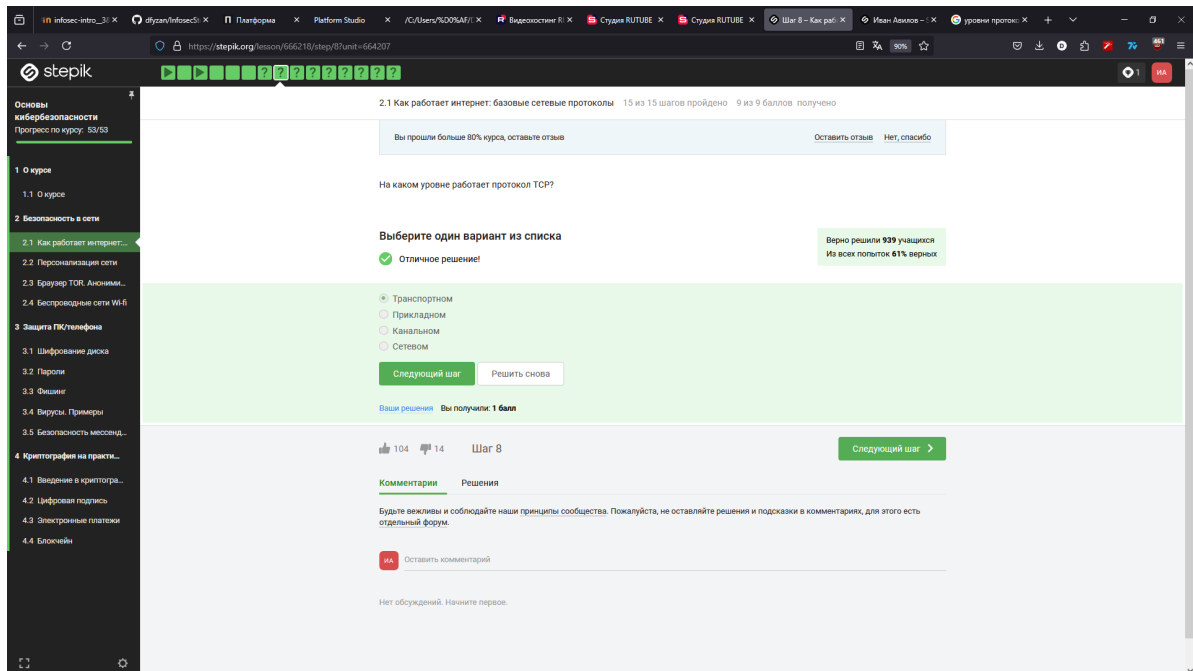


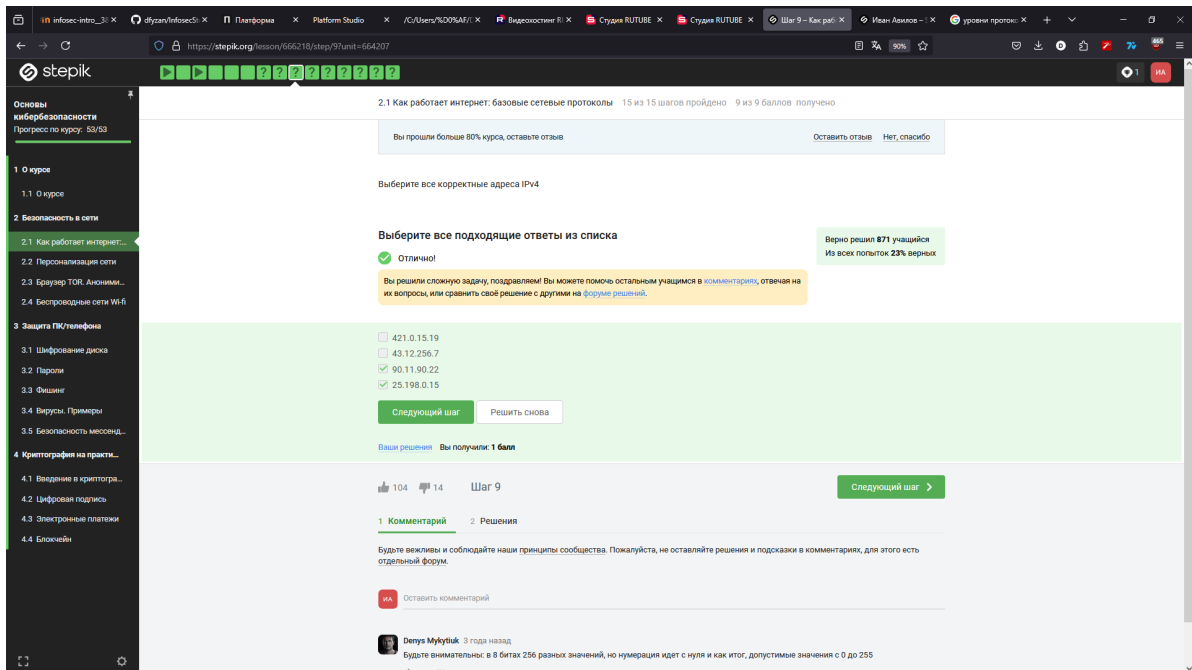
# Задание



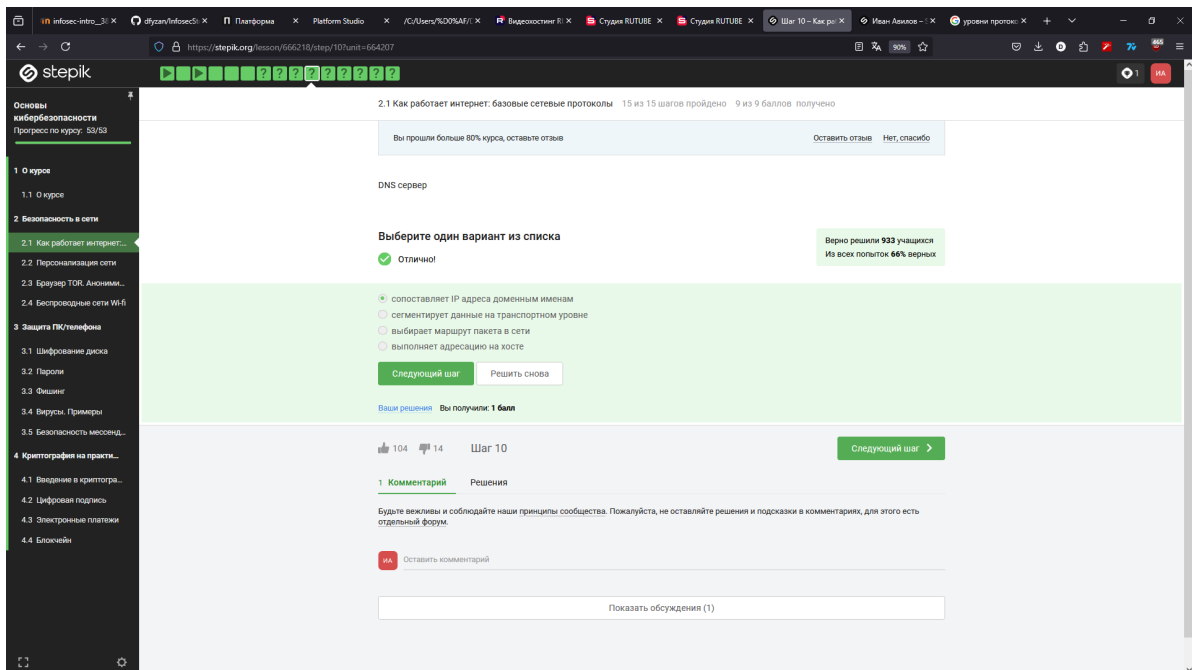
Только HTTPS является протоколом прикладного уровня



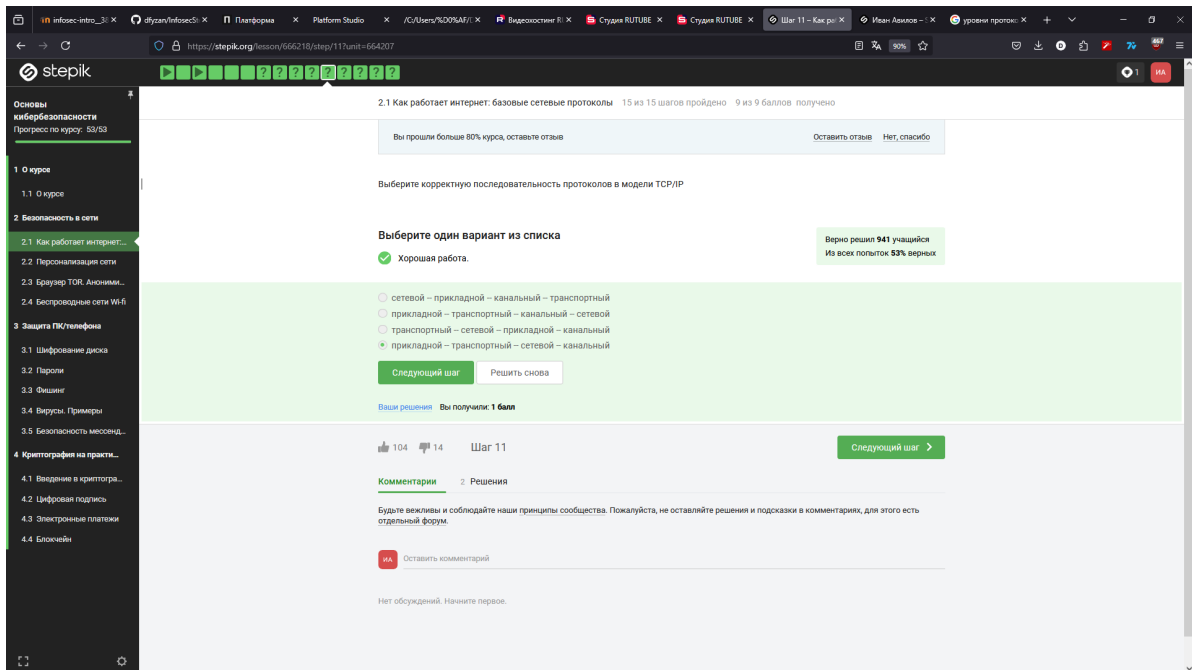
TCP является протоколом транспортного уровня



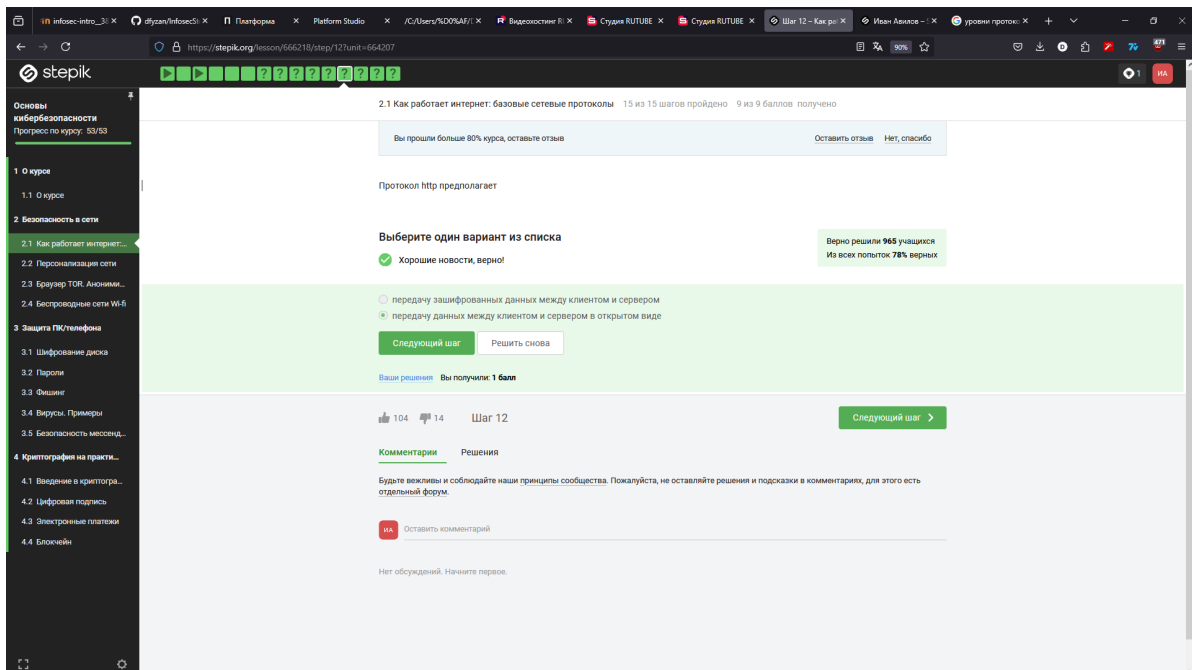
Адреса, в которых есть числа больше 255 - некорректны



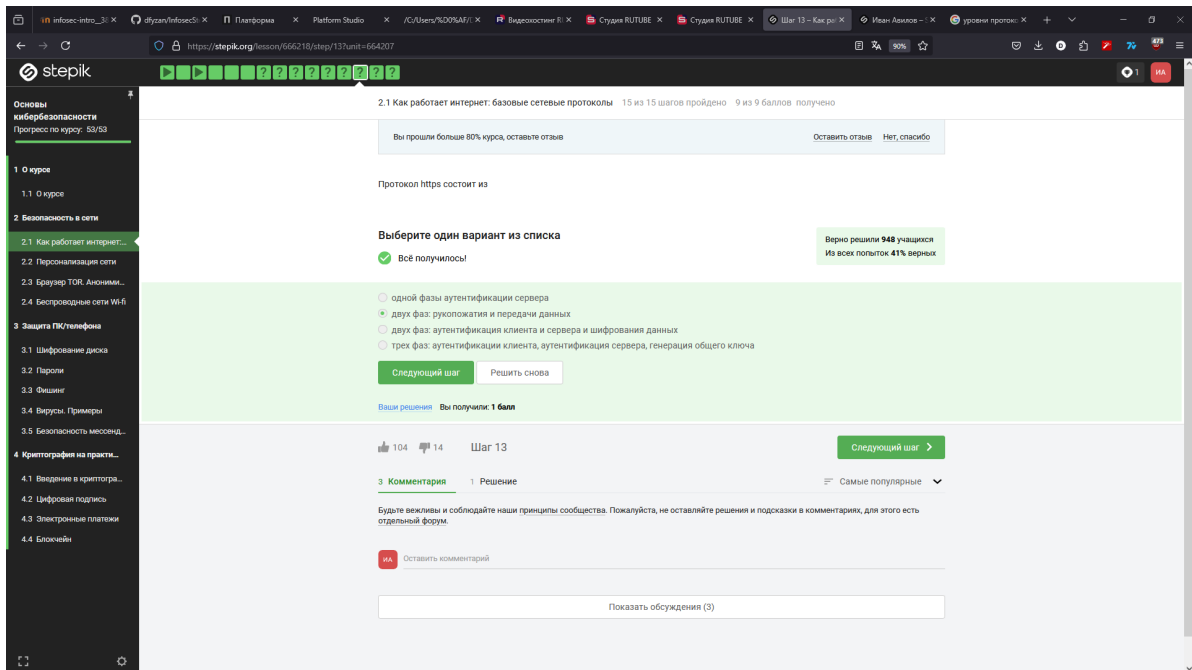
DNS сервера действительно сопоставляют доменное имя с его IP адресом



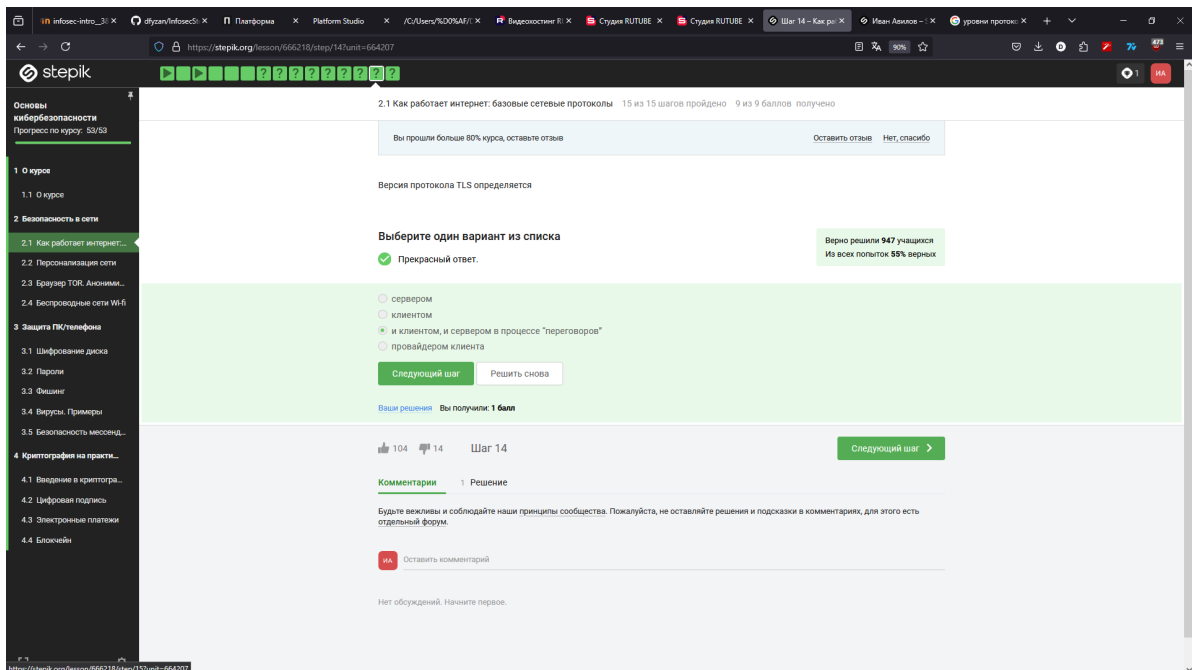
В верной последовательности протоколы отсортированы от верхнего к нижнему



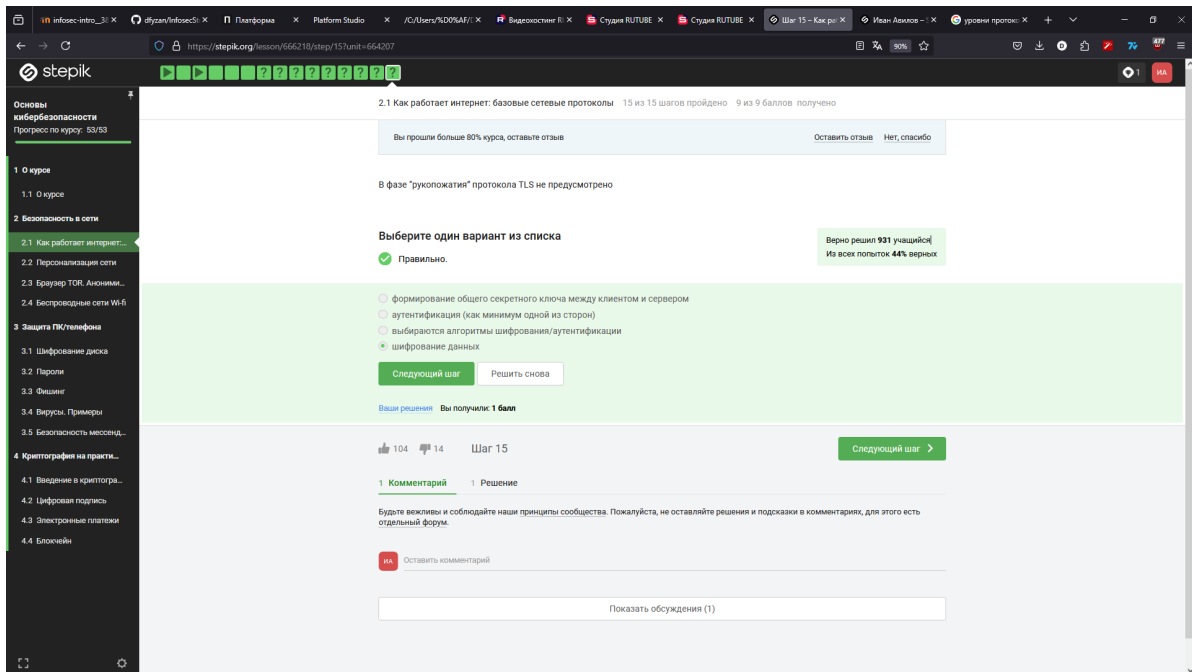
http, в отличие от https не предполагает шифрования



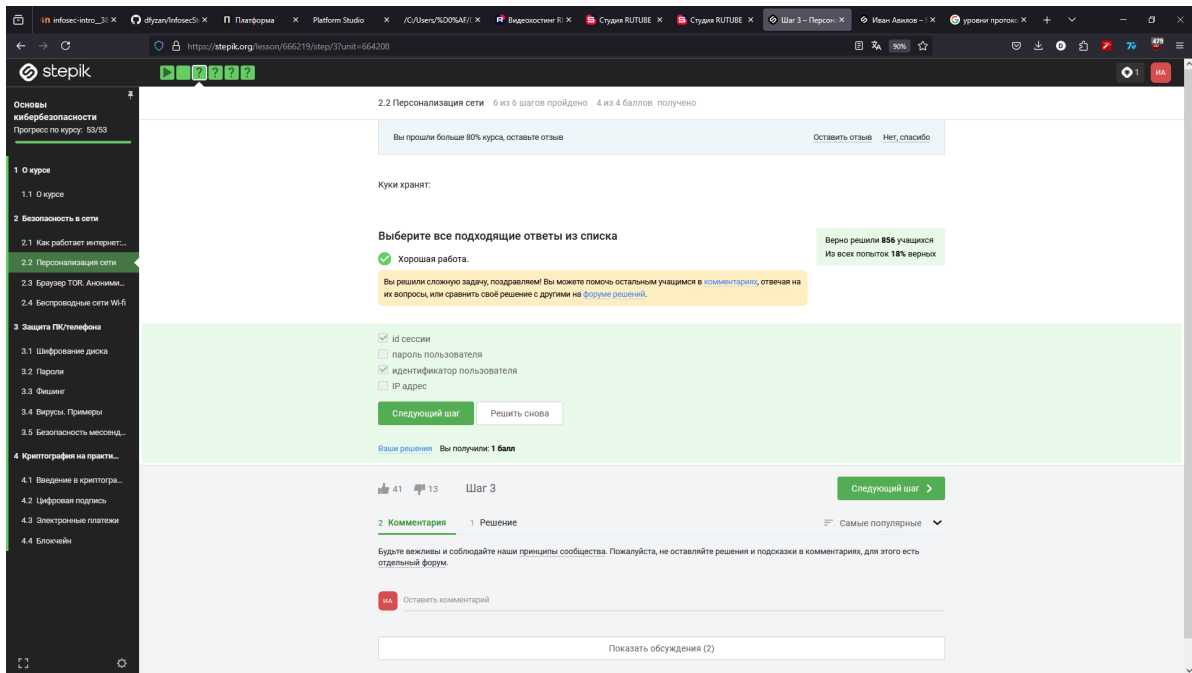
Правильный ответ - 2 фазы, рукопожатие и передача данных



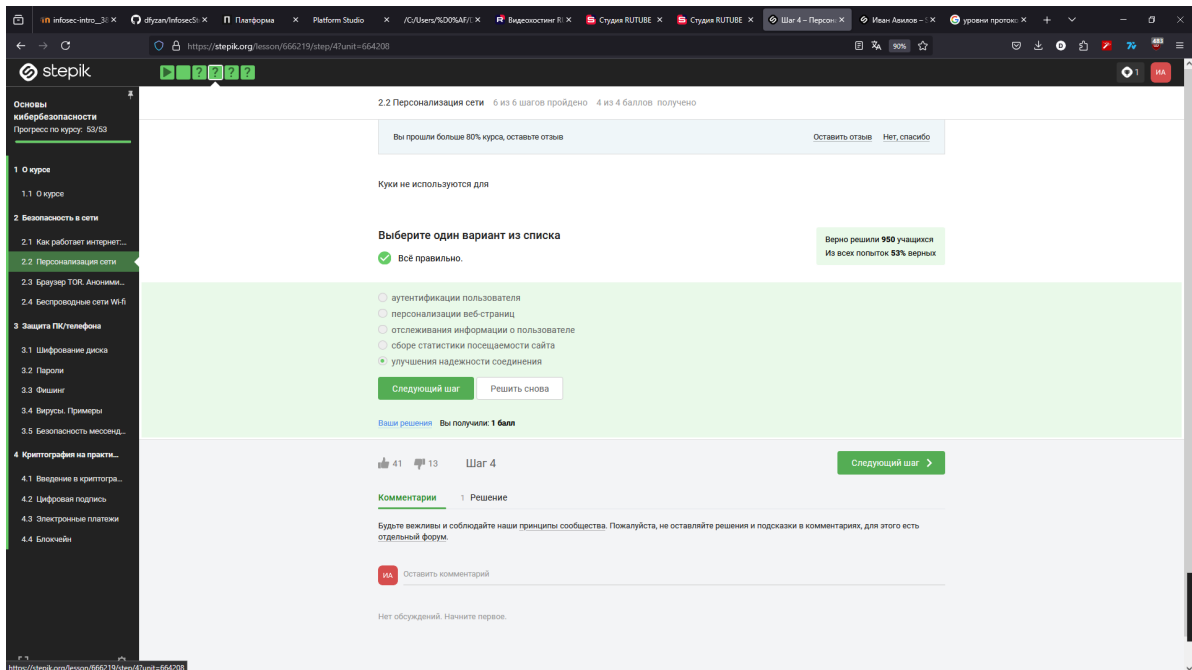
Если у какой-то стороны нету поддержки определённой версии, они договариваются использовать прошлую версию, которая есть у обеих сторон.



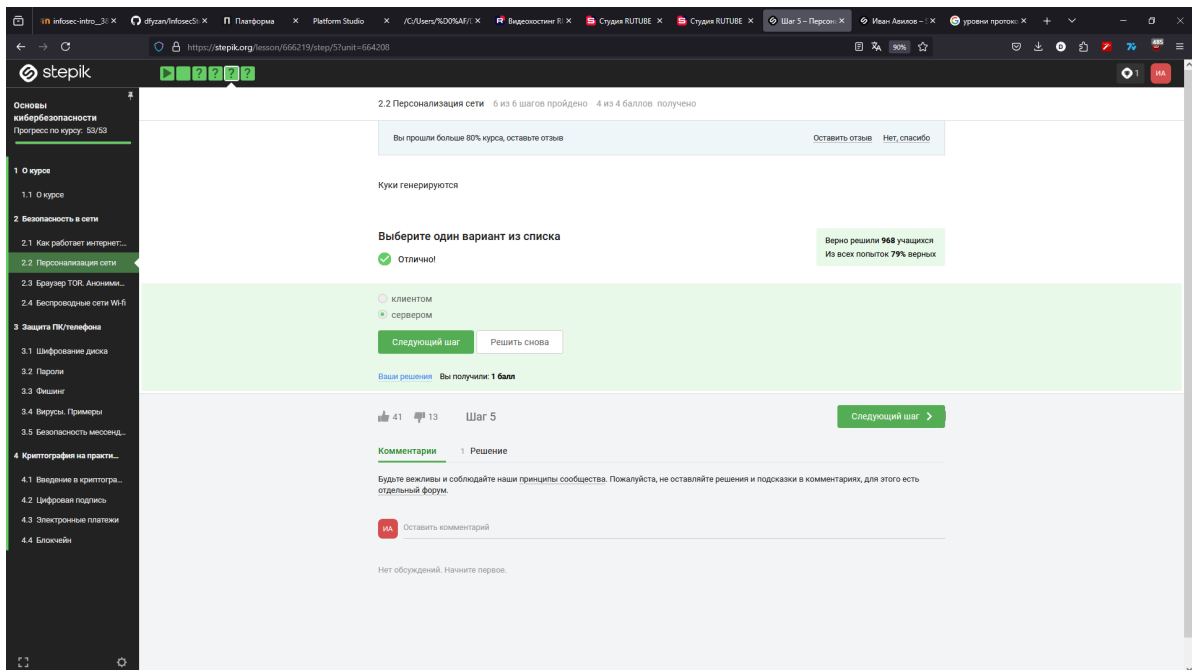
Фаза рукопожатия предполагает лишь обмен информацией о способах шифрования: ключах, алгоритмах и т.д. Шифрование данных не выполняется



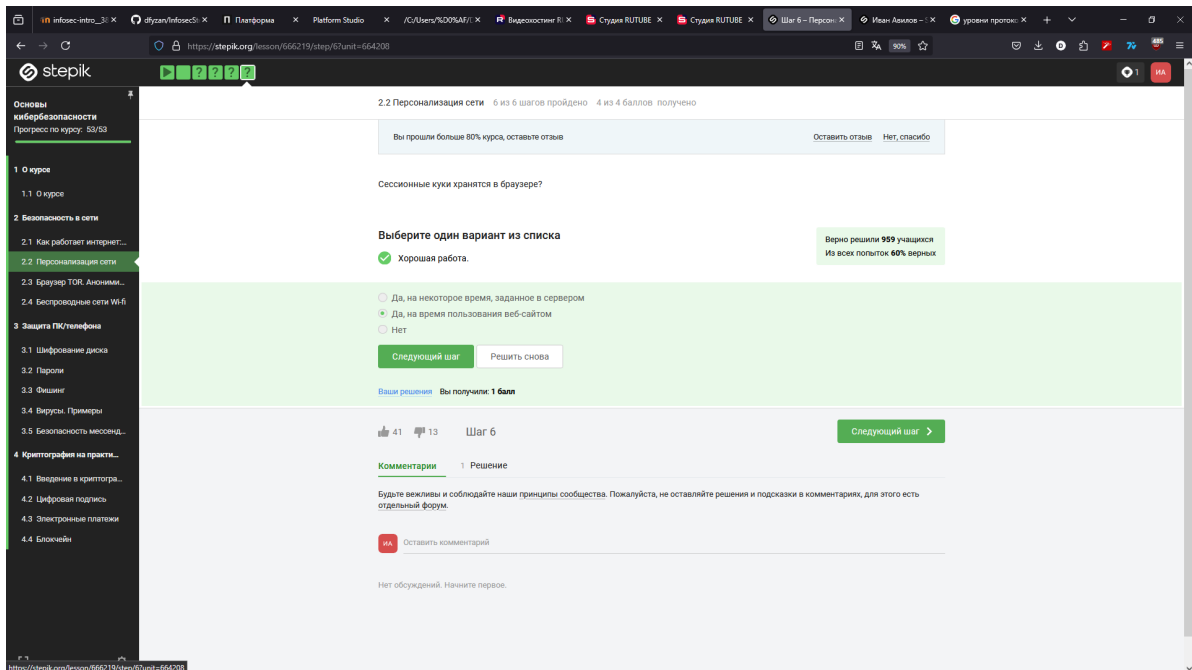
Куки файлы позволяют идентифицировать пользователя, не открывая его персональные данные



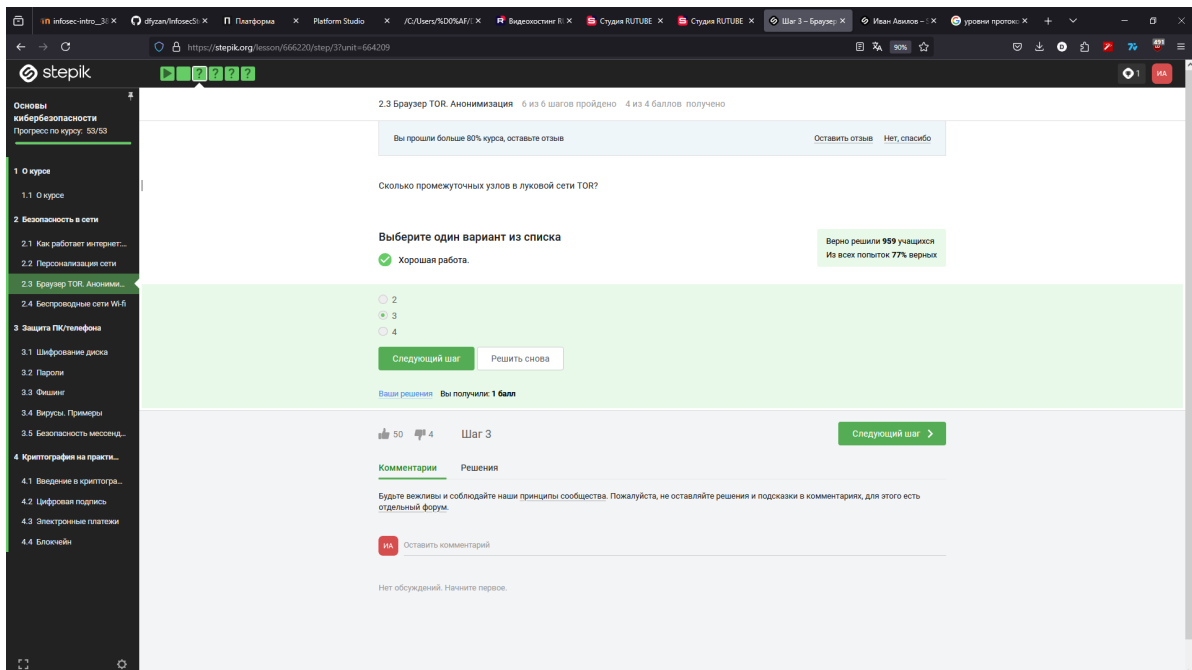
Надёжность соединения - не зона ответственности владельца сайта



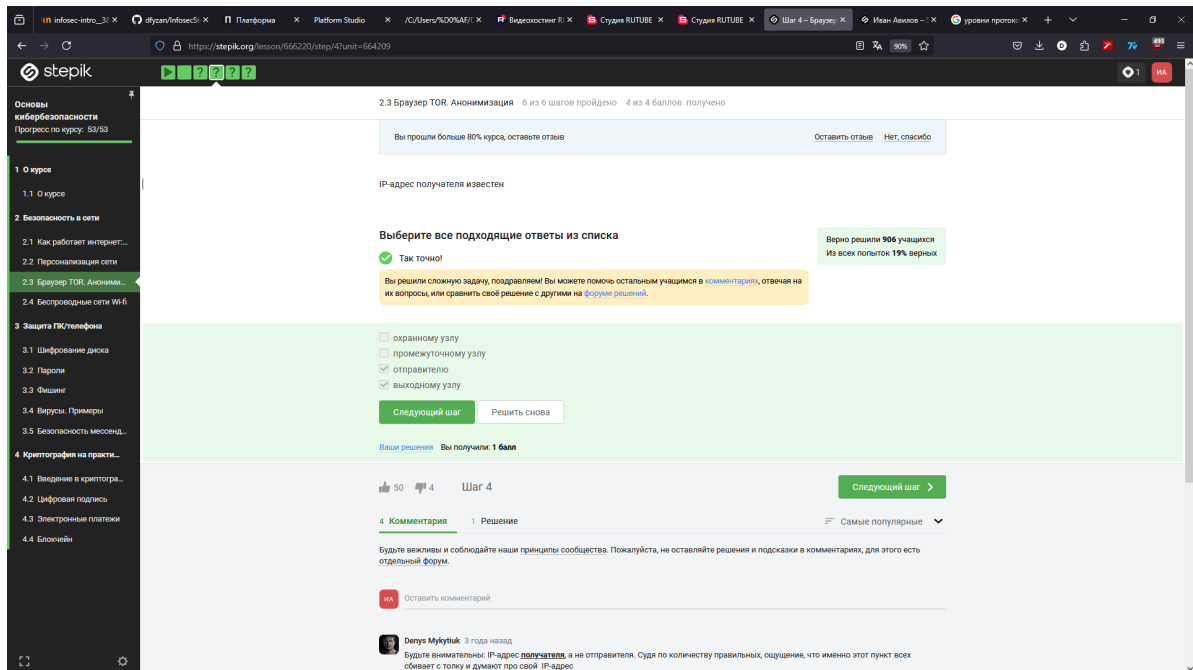
Куки файлы используются и генерируются сервером



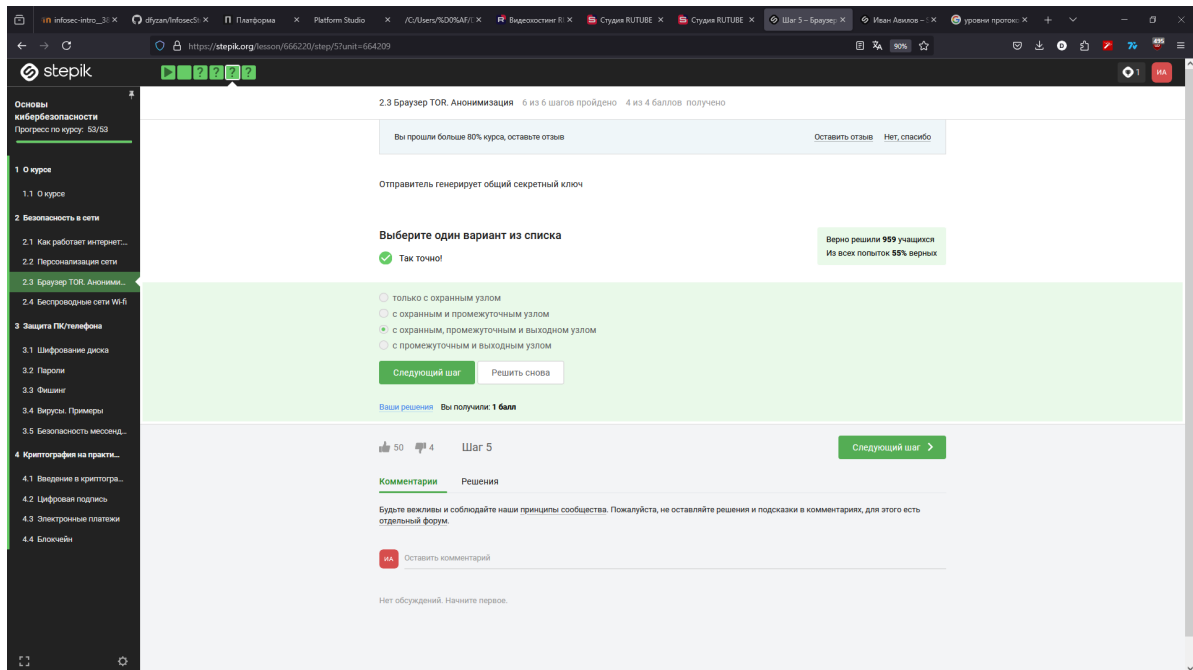
Куки файлы хранятся в браузере на время пользования сайтом



Промежуточных узлов в сети TOR - 3

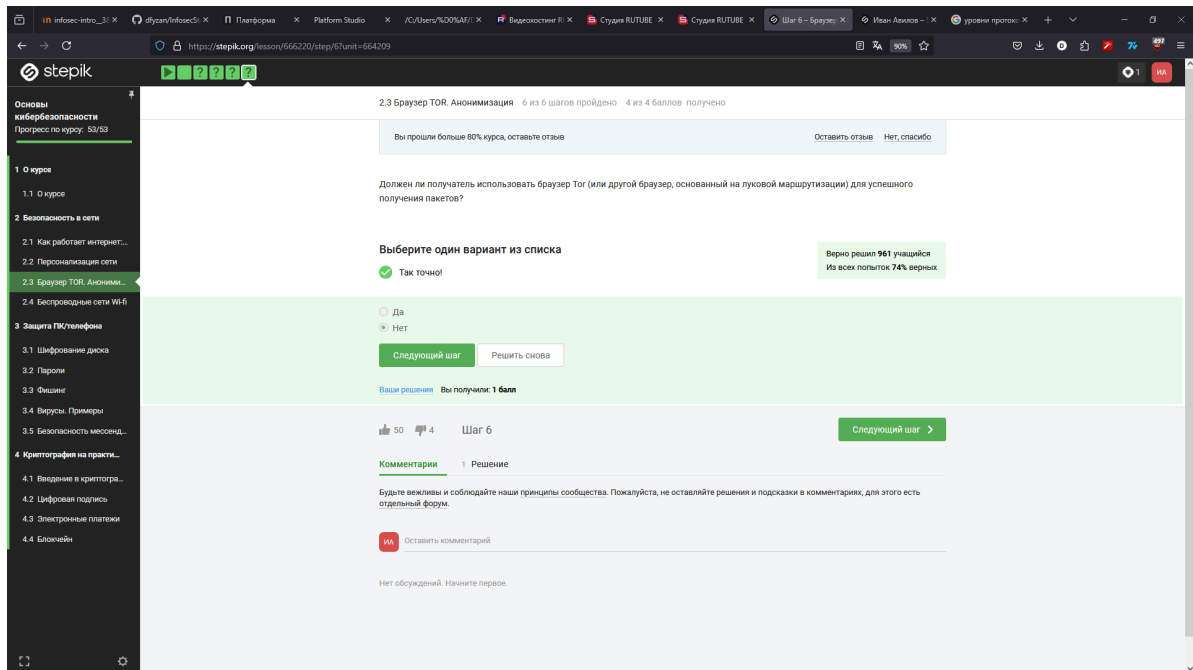


Отправитель должен знать адрес получателя, иначе он не сможет передать его выходному узлу. Выходной узел должен знать адрес получателя, иначе он не будет знать, куда направить пакеты.

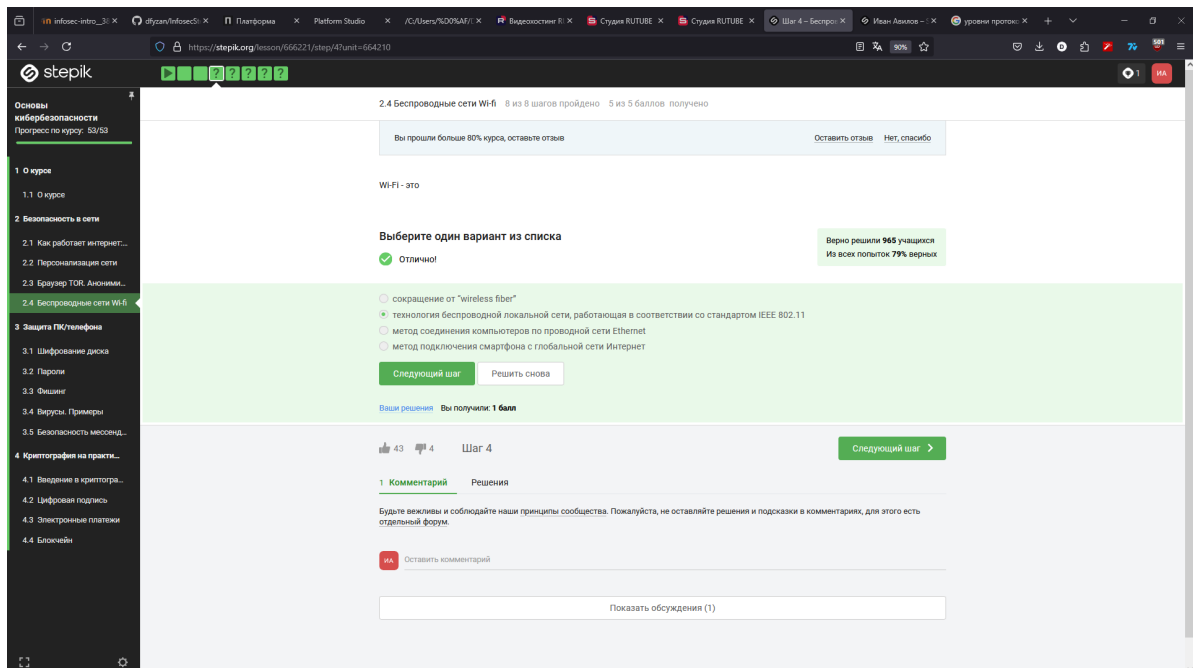


Каждый узел знает только свой ключ, которым узел снимает один слой "луковицы"

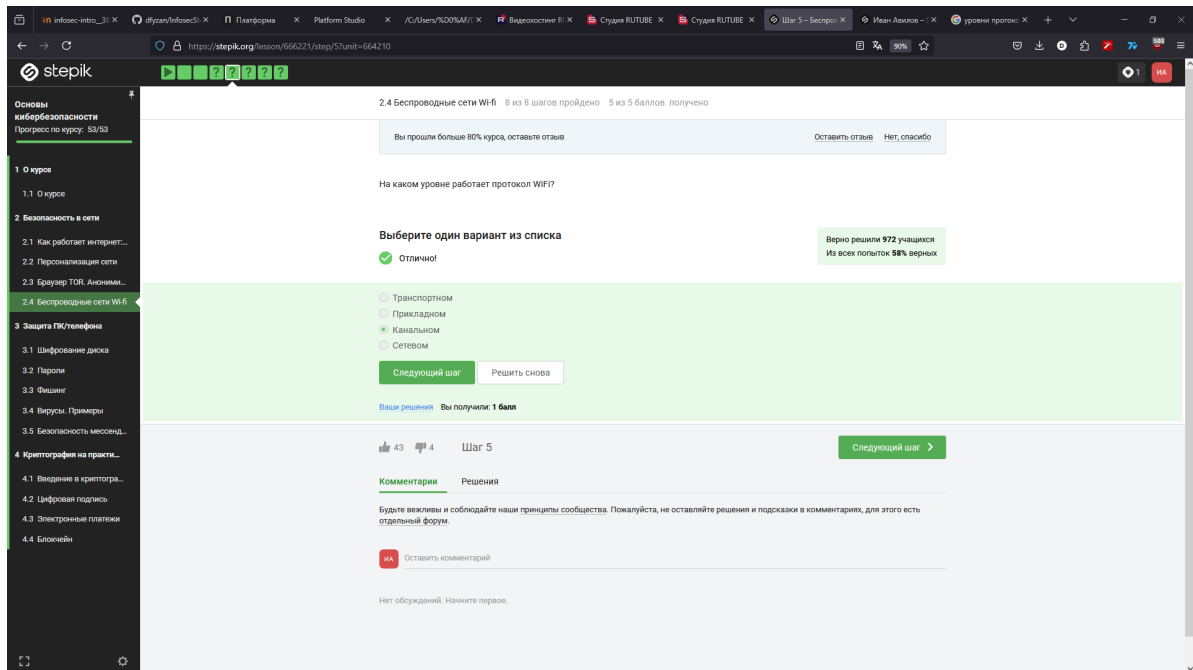




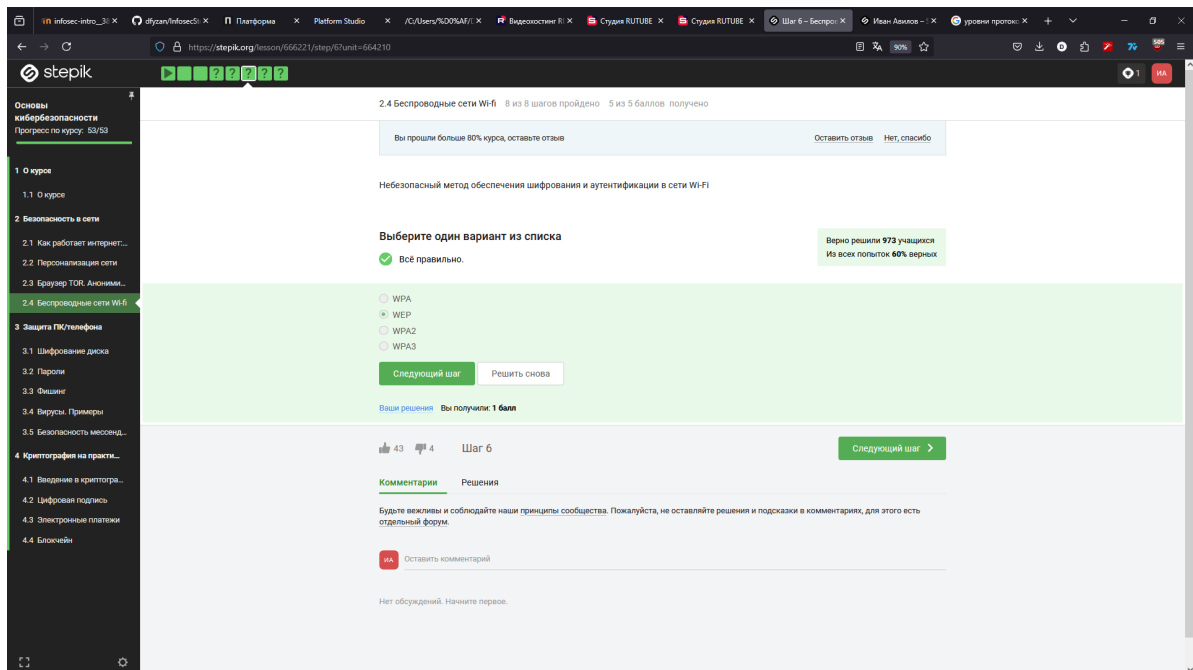
Нет, так как выходной узел играет роль виртуального пользователя.



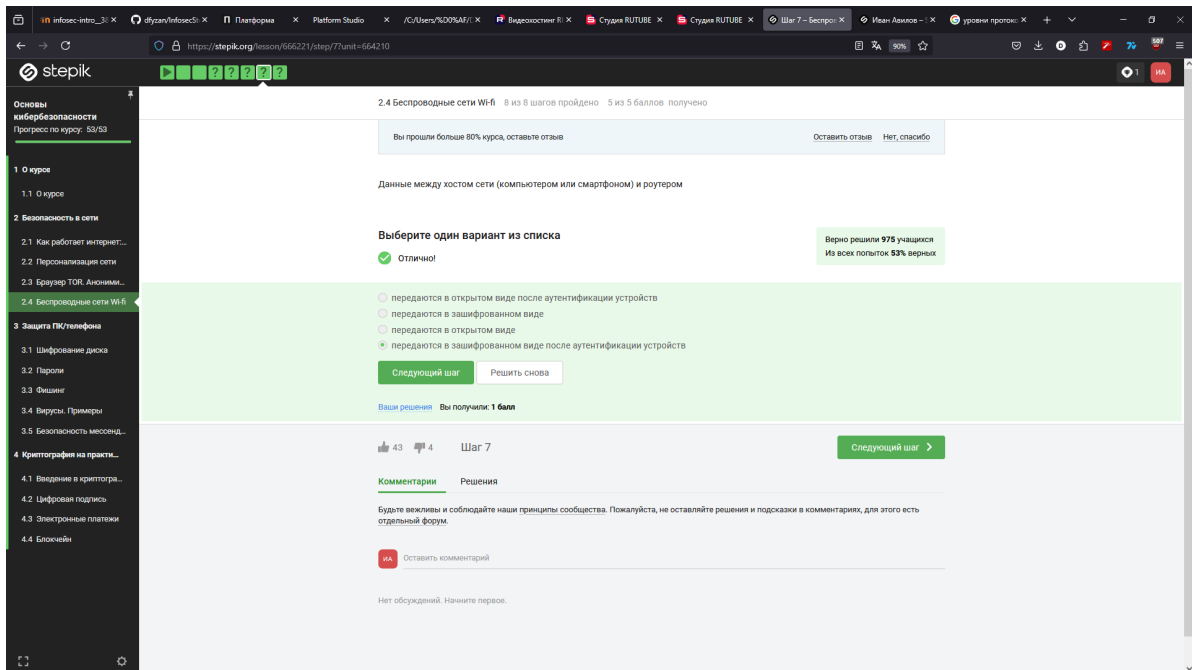
Wi-Fi - технология беспроводной передачи данных в локальной сети



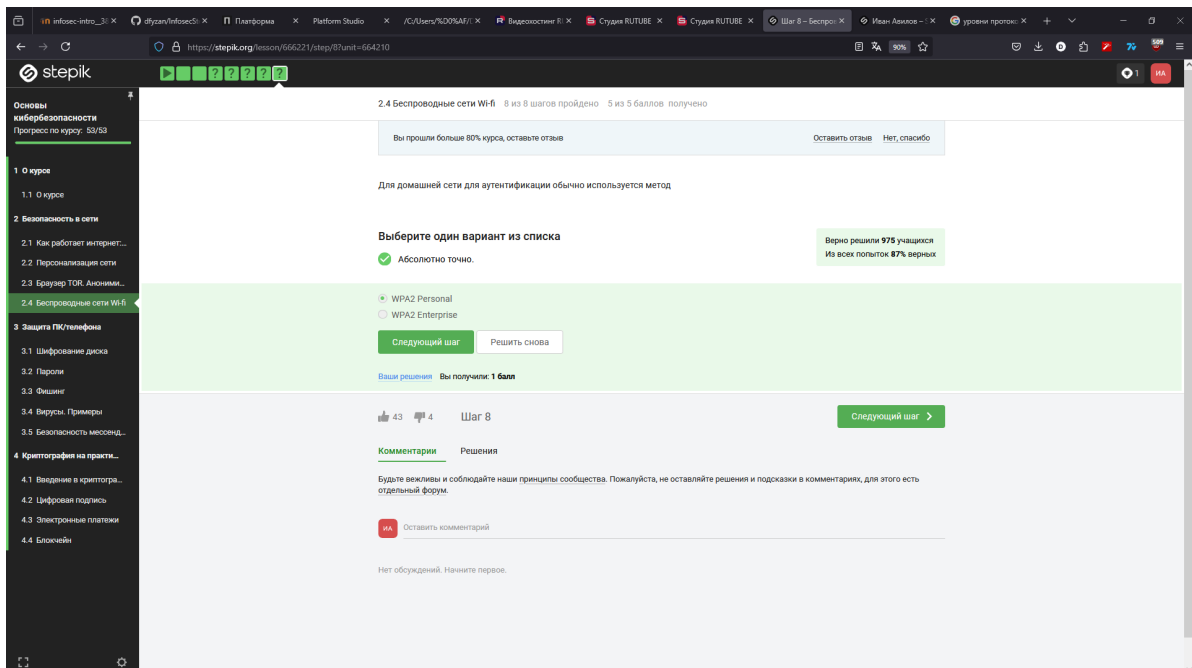
Wi-fi работает на канальном уровне



Самый уязвимый метод - WEP



Шифрование начинается после аутентификации устройств



Personal - для личного пользования. Enterprise - для бизнеса