Отчет по прохождению внешнего курса.

Раздел 1. Безопасность в сети.

Рогожина Надежда Александровна

Содержание

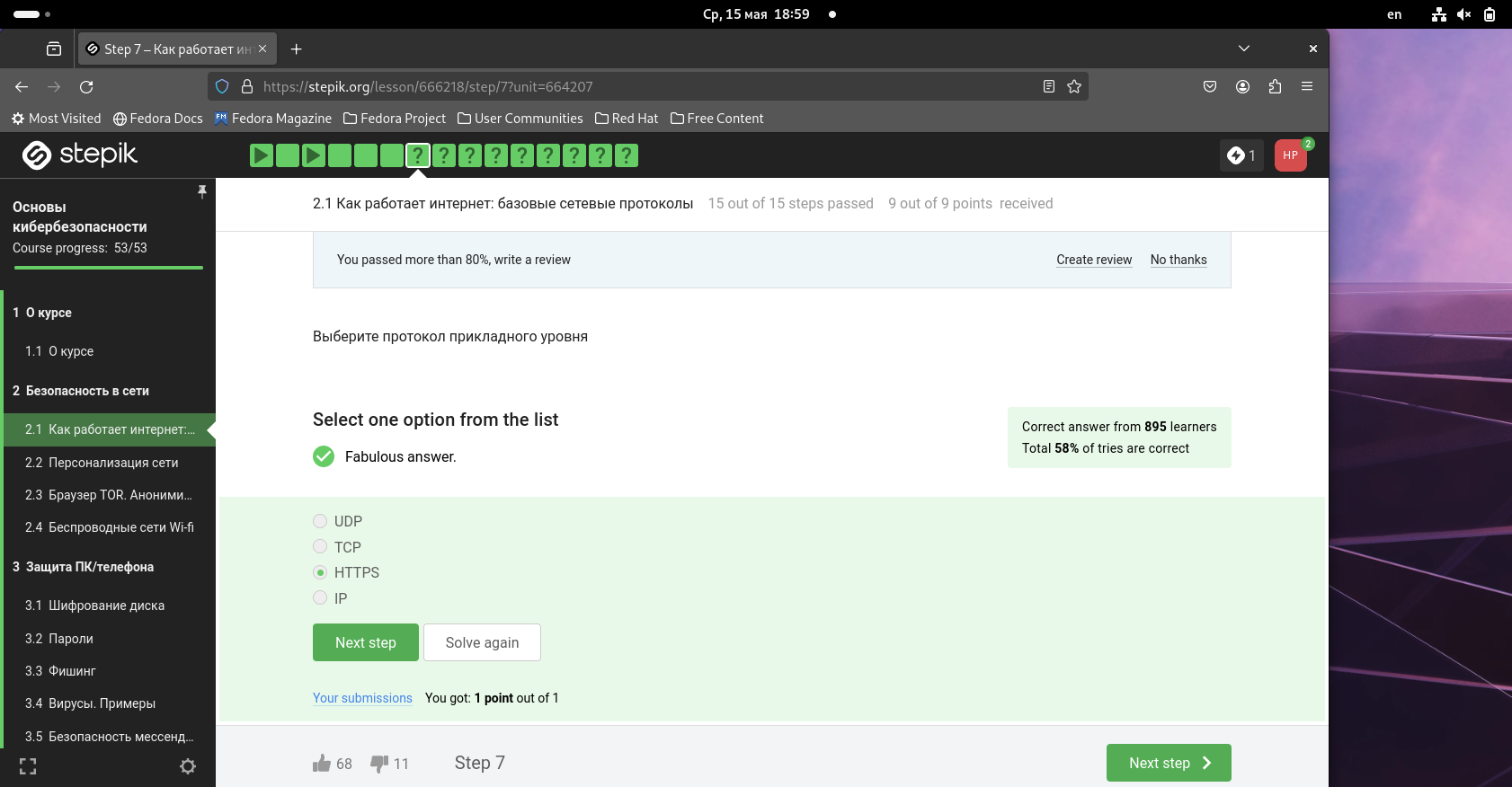
# 1 Цель работы

Цель данного курса - узнать, как обеспечивается безопасность интернет-трафика, какие пароли нужно выбирать и как их хранить, познакомиться с методами защиты сообщений в мессенджерах (WhatsApp, Telegram), понять, как работают механизмы аунтефикации в электронных платежах, а также зачем нас иногда просят выбрать квадраты, где изображены светофоры.

# 2 Выполнение

## 2.1 Как работает интернет: базовые сетевые протоколы

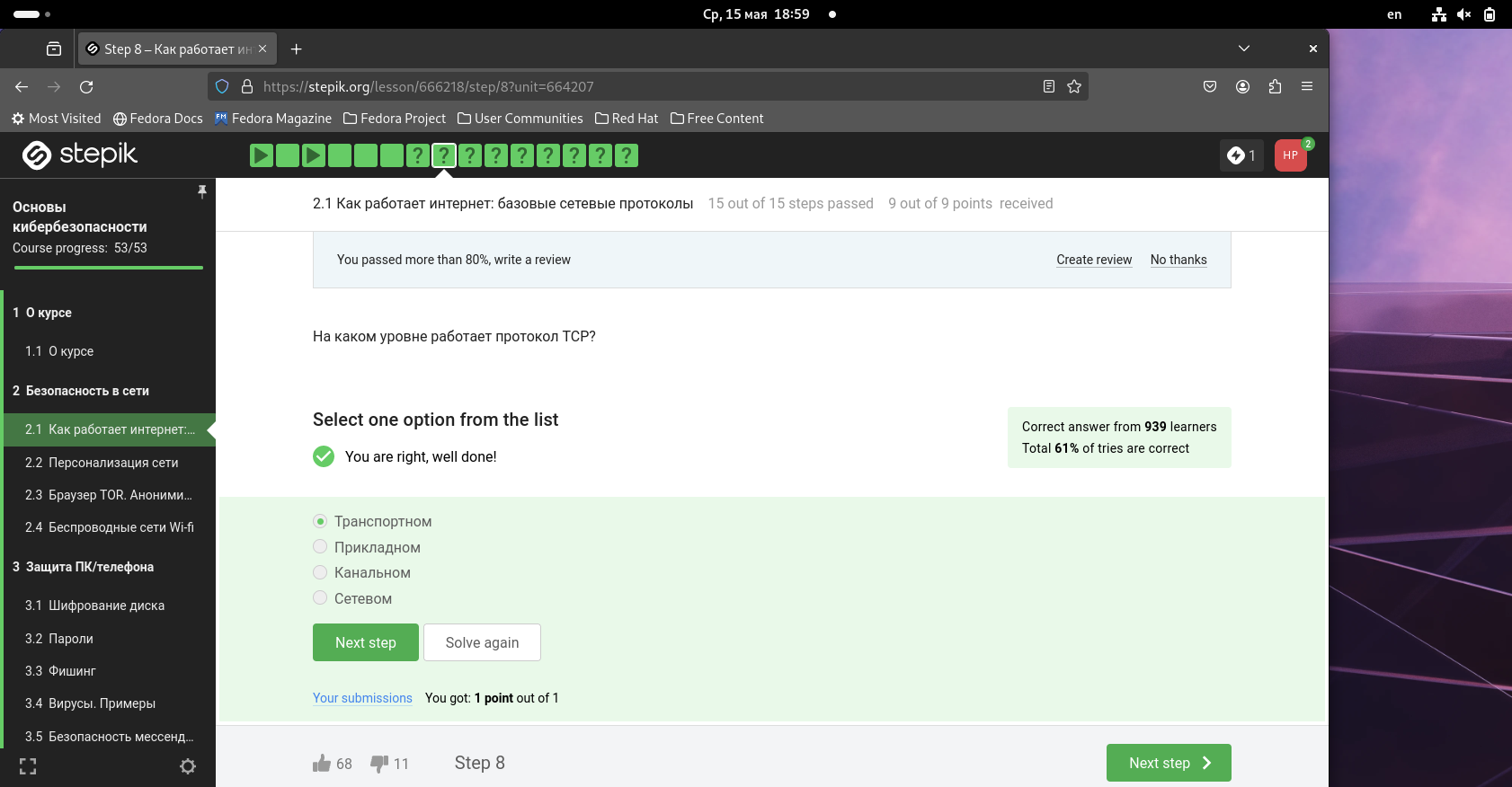
1. Выберите протокол прикладного уровня (рис. [??]):



HTTPS

Среди всех представленных TCP, UDP - протоколы транспортного уровня, а IP - сетевого. Протокол прикладного уровня здесь только один - HTTPS.

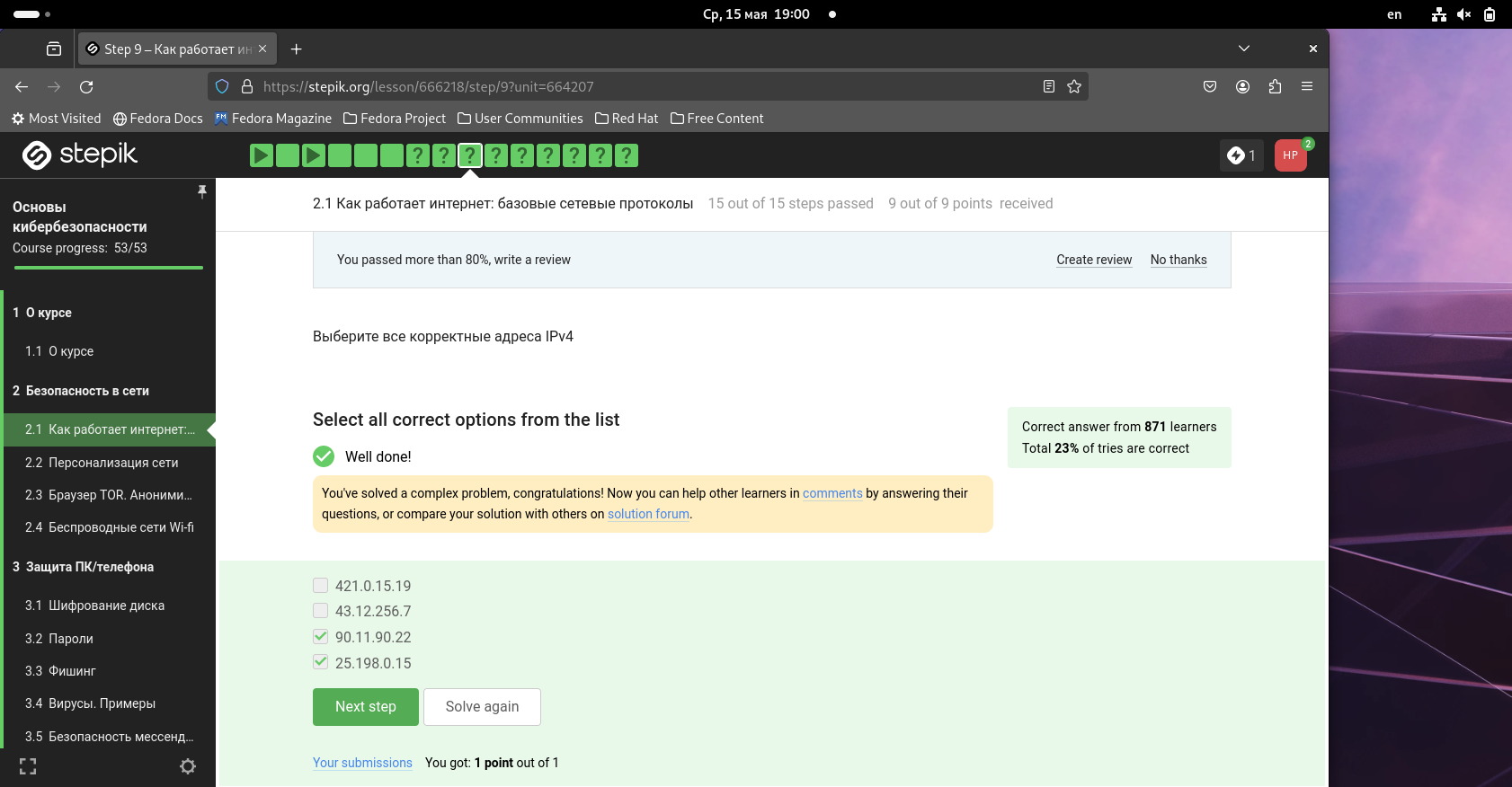
1. На каком уровне работает протокол TCP (рис. [??]):



Ответ

Протокол TCP работает на *транспортном* уровне.

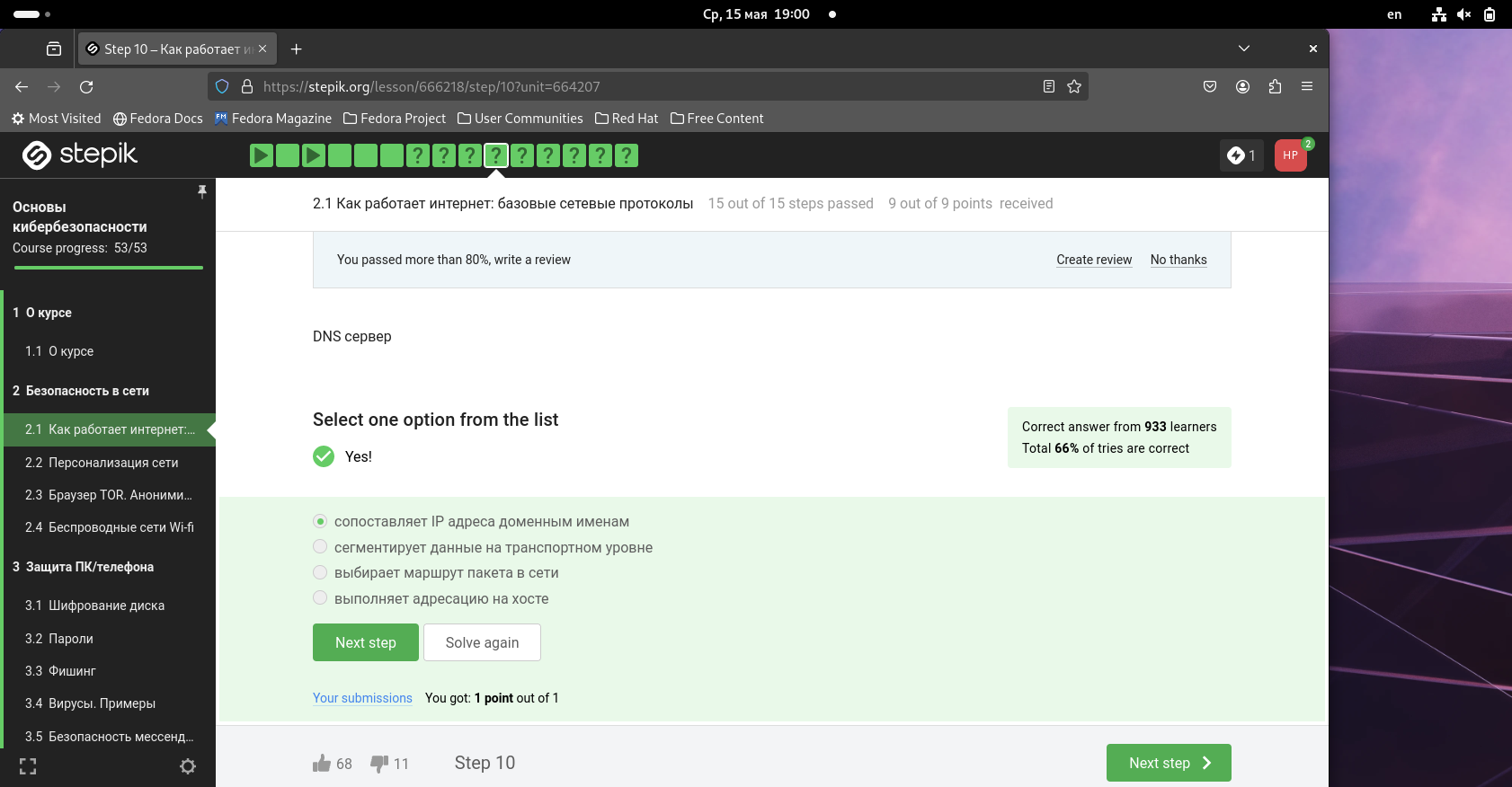
1. Выберите все корректные адреса IPv4 (рис. [??]):



Адреса

Существуют две версии адресации в протоколе IP. Популярный на сегодняшний день - это версия 4 адресации (IPv4), и этот адрес состоит из большего набора чисел, нежели порт в TCP протоколе, а именно это 4 числа от 0 до 255. Например, адрес IPv4 может выглядеть вот так: 192.168.1.4. Соответсвенно, все числа, которые >255 не подходят.

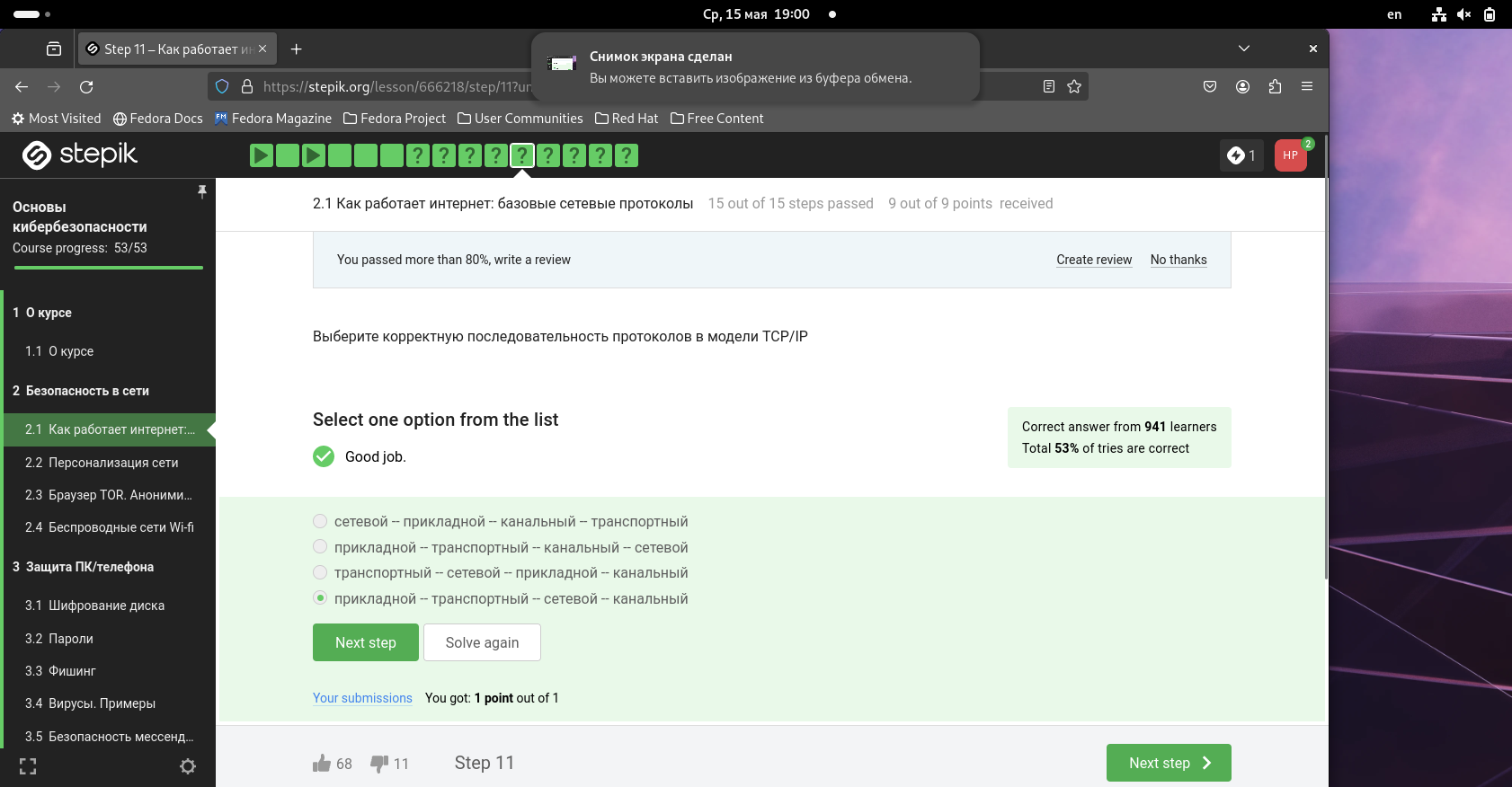
1. Что делает DNS сервер (рис. [??]):



DNS

Oсновная задача DNS-сервера - это сопоставить название, то есть доменное имя, с корректным IP-адресом, с тем, где лежит этот сервер, этот сайт. Когда это сопоставление прошло (то есть я знаю, что yandex.ru находится по такому IP-адресу), дальше в сети сегмент моих данных передается по транзитным узлам или маршрутизаторам.

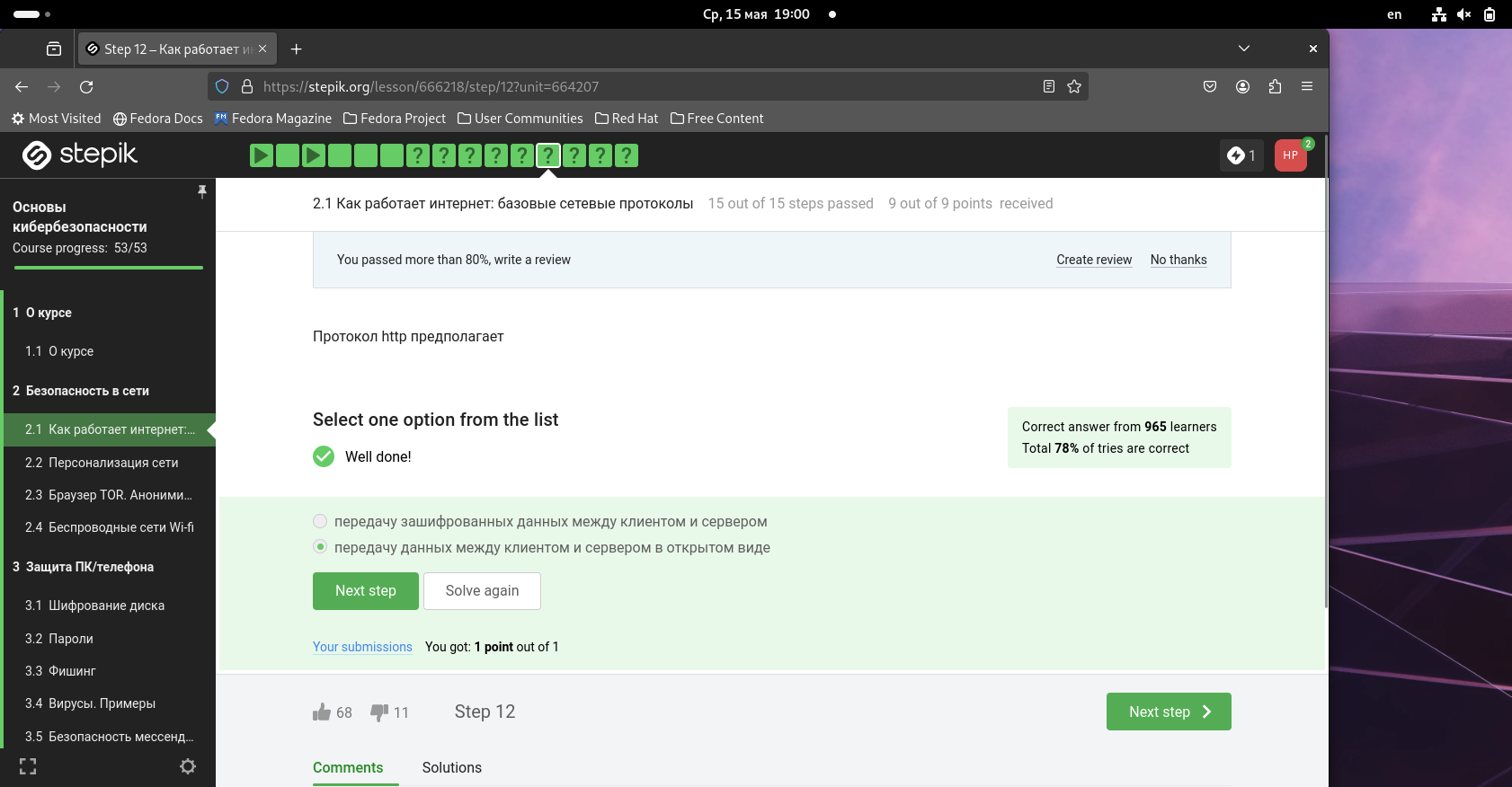
1. Выберите корректную последовательность протоколов модели TCP/IP (рис. [??]):



TCP/IP

В модели TCP/IP существует несколько уровней, а именно 4. На самом верхнем уровне, прикладном работают пользовательские программы, и задача прикладного уровня - обеспечить доступ для этих пользовательских программ к услугам Интернет. Все эти протоколы прикладного уровня работают над транспортным уровнем, это следующий уровень в модели TCP/IP. Транспортный уровень обеспечивает передачу данных между процессами на одной машине или хосте (host). Хост - это устройство, которое подключено к интернету. Это может быть компьютер, смартфон. И транспортный уровень отвечает за корректное распределение пакетов между программами. Транспортный уровень работает над следующим уровнем модели TCP, так называемым сетевым или межсетевым уровнем. В этом уровне принимает участие не только программа, не только наша машина, но уже наш роутер, то есть то устройство, к которому мы подключаемся, чтобы получить интернет. Сетевой уровень ответственен за передачу данных между различными физическими сетями. Сетевой уровень работает над так называемым канальным уровнем или самым низким уровнем модели TCP/IP. И в этой модели работает уже физика. Здесь происходит физическая передача данных. И здесь мы уже будем говорить о пропускной способности канала, об обеспечении помехоустойчивости, и основные примеры протоколов канального уровня непосредственно связаны с тем, как мы передаем данные.

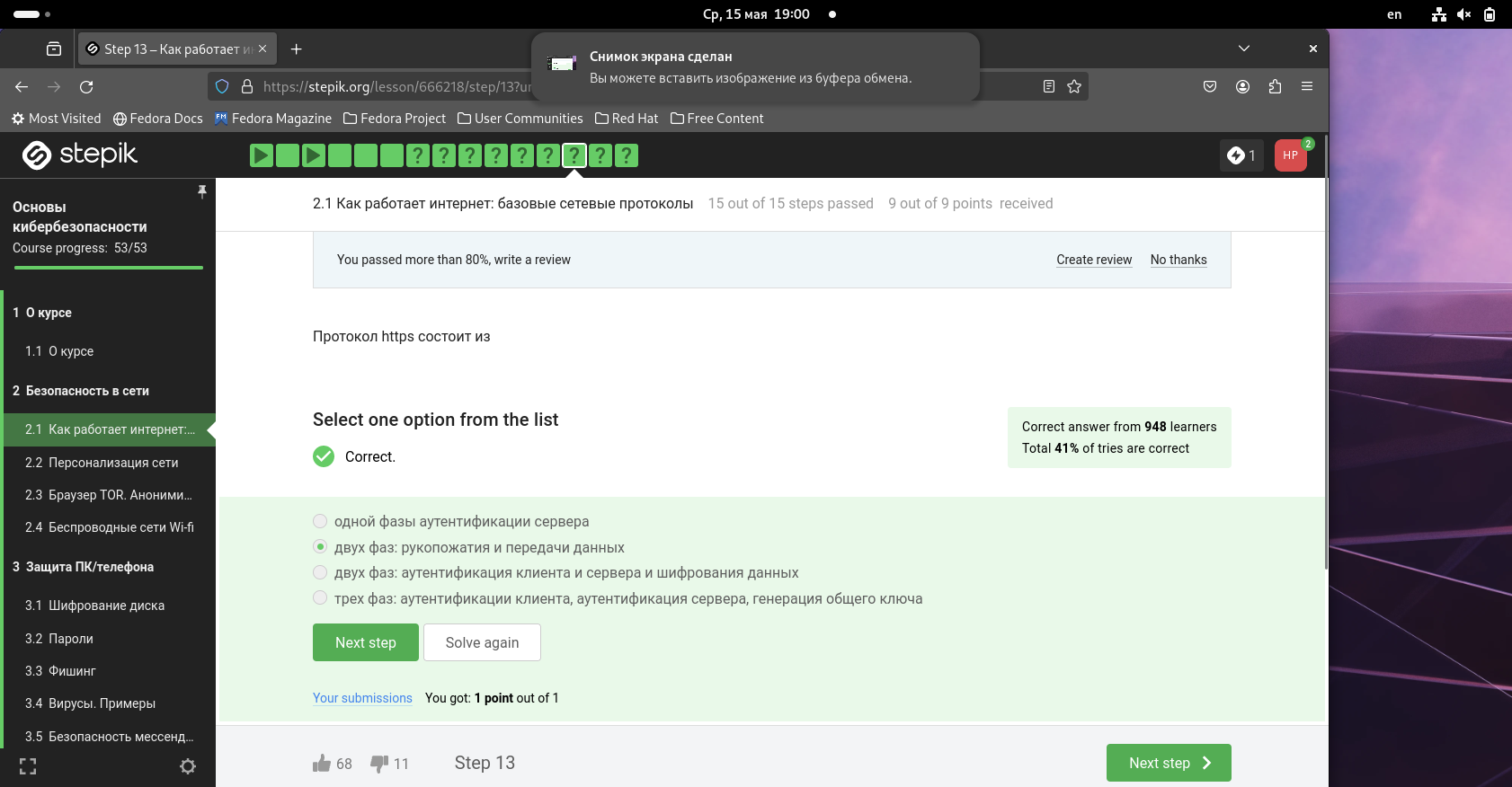
1. Протокол http предполагает (рис. [??]):



HTTP

HTTP-сообщения представляют собой обычный текст, поэтому неавторизованные лица могут легко получить к ним доступ и прочитать их через Интернет. Напротив, HTTPS передает все данные в зашифрованном виде.

1. Протокол https состоит из (рис. [??]):



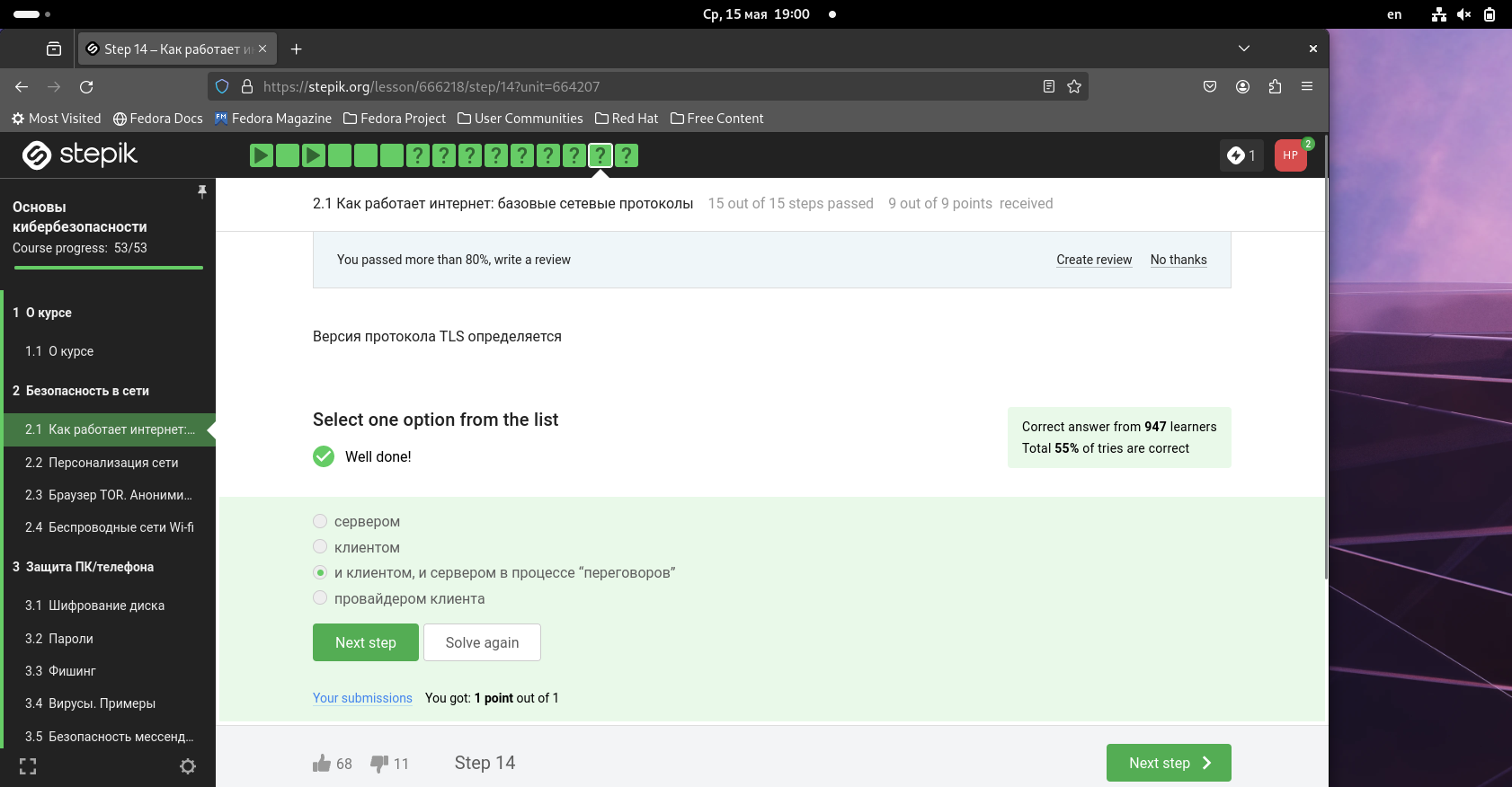
HTTPS

Протокол https состоит из 2 фаз: фазы рукопожатия и фазы данных. Во время фазы рукопожатия происходит:

* выбор параметров, протоколов
* аунтефикация
* формируется общий ключ К

В то время как во время фазы передачи данных происходит непосредственно шифрование трафика с помощью ключа К.

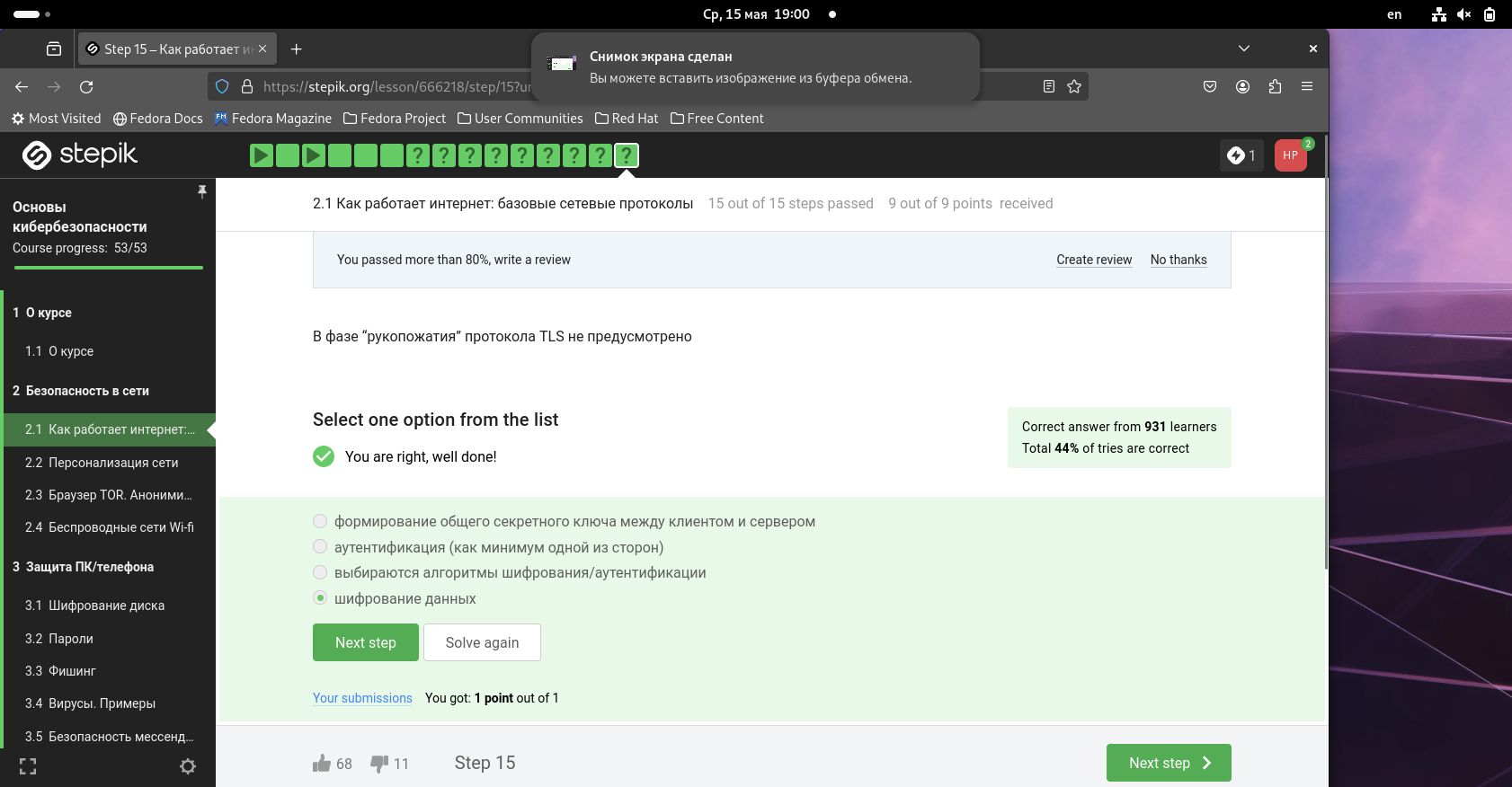
1. Версия протокола TLS определяется (рис. [??]):



TLS

Версия протокола выбирается в фазе рукопожатия при выборе параметров совместно.

1. В фазе “рукопожатия” протокола TLS не предусмотрено (рис. [??]):

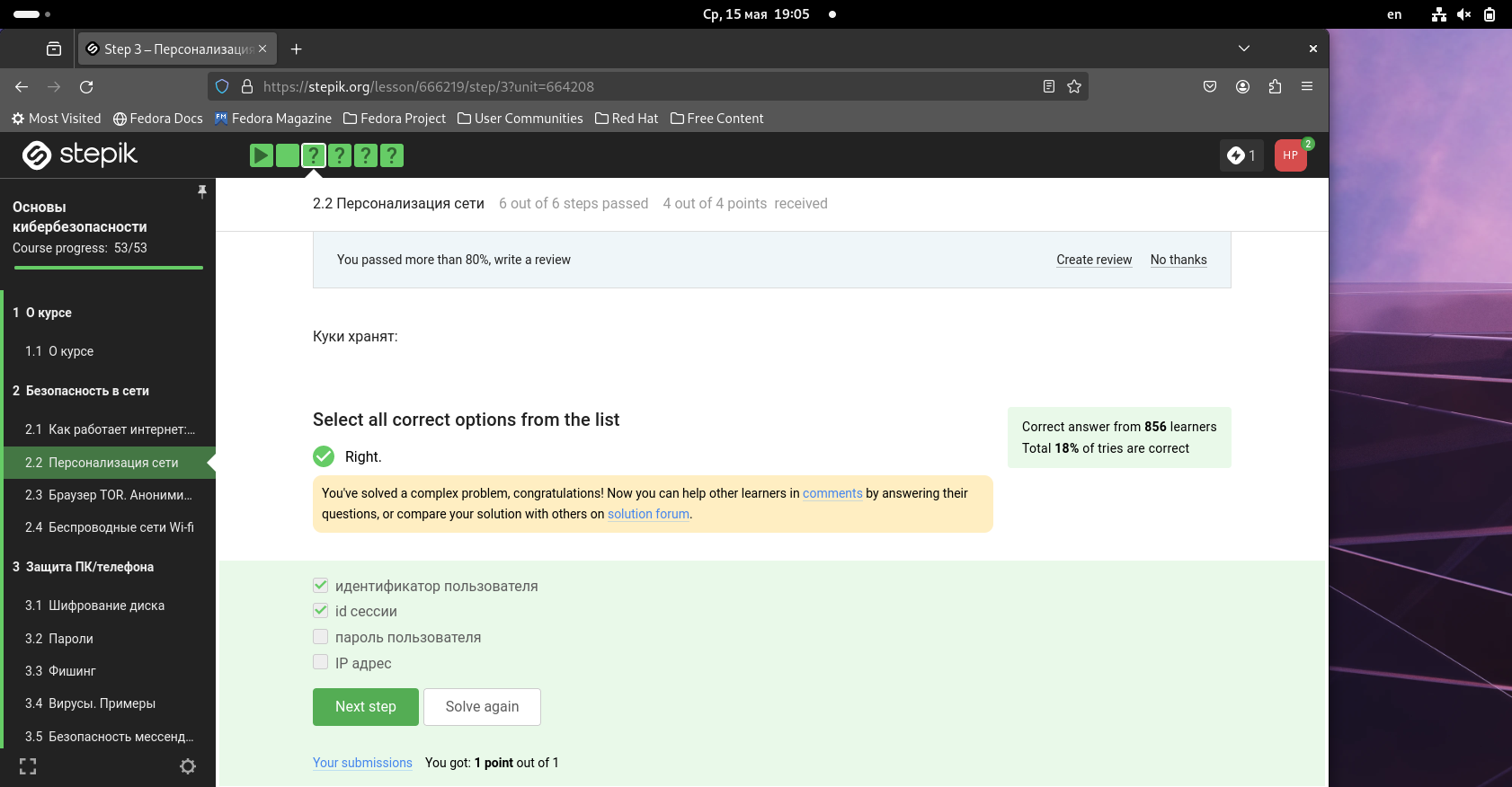


TLS

Шифрование данных происходит в фазе передачи данных.

## 2.2 Персонализация сети

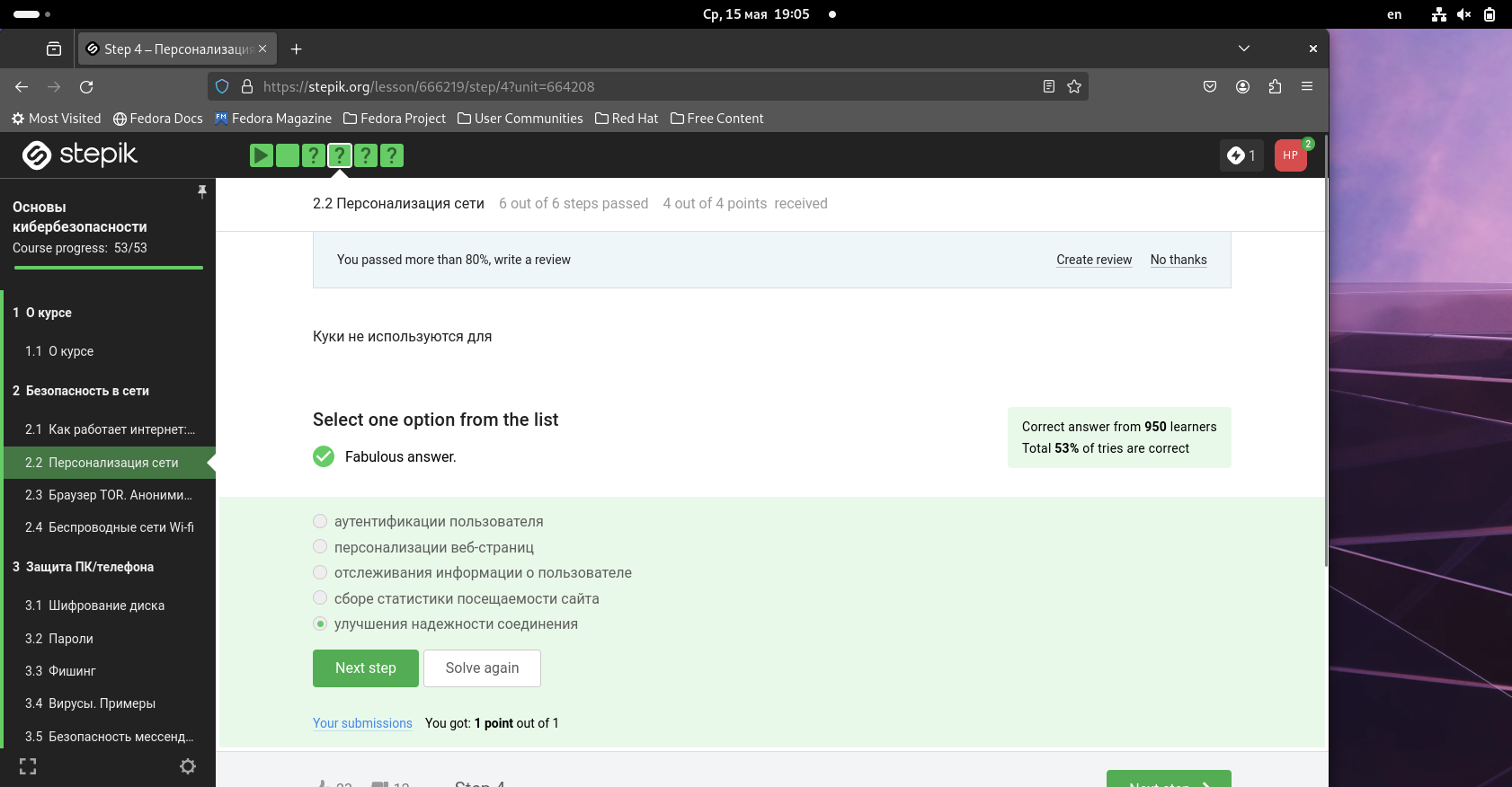
1. Куки хранят (рис. [??]):



cokkie

Куки, как правило, хранят в себе список параметров и их значений. Этими параметрами могут быть id пользователя, id сессии, иногда описан тип браузера и время запросов и некоторые действия пользователей. Опять же, если это интернет-магазин, то в куки может храниться то, что мы просматривали, какие страницы мы посещали. В куки никогда не хранятся пароли или хэш от паролей пользователя, куки для этого не предназначены и не должны хранить наши пароли.

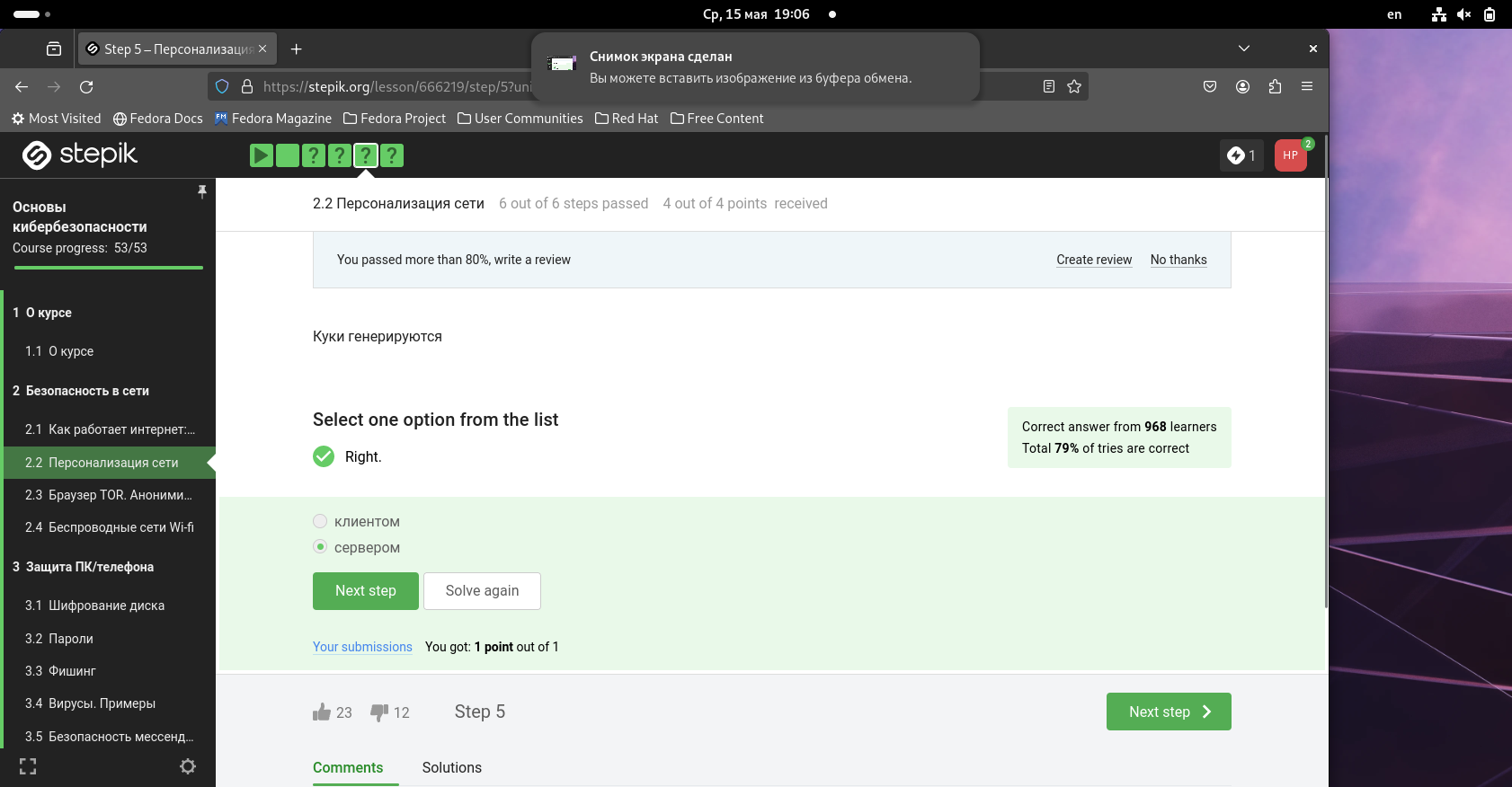
1. Куки не используются для (рис. [??]):



cokkie

Куки - это данные, которые передаются от сервера клиенту для его идентификации. Так, например, они сохраняют сессионную информацию. Примером является тот факт, что, когда вы, например, заходите на какой-то интернет-магазин, наполняете корзину каким-то покупками, но не завершайте покупку, а закрываете эту страницу, а потом открываете её когда-нибудь снова, часто получается так, что содержимое корзины запоминается. Кроме этого, куки позволяют персонализировать страницы: например, смена языка страницы, или когда браузер спрашивает, нужно ли перевести эту страницу на русский язык. А если вы попадаете на страницу с финским языком, и вы не часто или почти никогда не смотрите страницы на финском языке, то вас спрашивают, стоит изменить язык на какой-то другой. Кроме того, куки помогают отслеживать действия пользователей в сети. Этим часто пользуются рекламщики. Тоже, наверное, кто-то из вас встречался с такой ситуацией, когда вы покупаете что-то в интернет-магазине или смотрите какой-то товар в магазине, например, лыжи. Вы купили лыжи где-то или хотели купить, смотрели на них, и потом, заходя уже на страницы абсолютно других сайтов, никак не связанных с лыжами, в рекламе, рекламных разделах страницы вы вдруг увидите эти самые лыжи по несколько раз. Это происходит потому, что на первом сайте, где вы смотрели или купили товар, вы получили от этого сайта куки, которые записали ваши пожелания себе. Для разных сайтов эти куки выглядят по-разному, как правило, они содержат сессионный токен, который часто содержит имя пользователя, ну и ещё какие-то данные, которые позволяют этому конкретному серверу авторизовать этот браузер, этого клиента в эту конкретную сессию. Всегда, когда мы обновляем нашу страницу или переходим по каким-то ссылкам, браузер отправляет полученные заранее с этого сайта при первой авторизации куки, и наш браузер ответственен за хранение и управление куки, они у вас на вашей машине лежат. Естественно, куки - это удобно. А представьте себе, если бы каждый раз при нажатии на какую-то ссылку в Сбербанк Онлайн, вы бы заново проходили их двухфакторную аутентификацию. Конечно, это было бы неудобно, и мы делаем это исключительно благодаря тому, что при самой первой аутентификации нам прислал их сервер какие-то cookie.

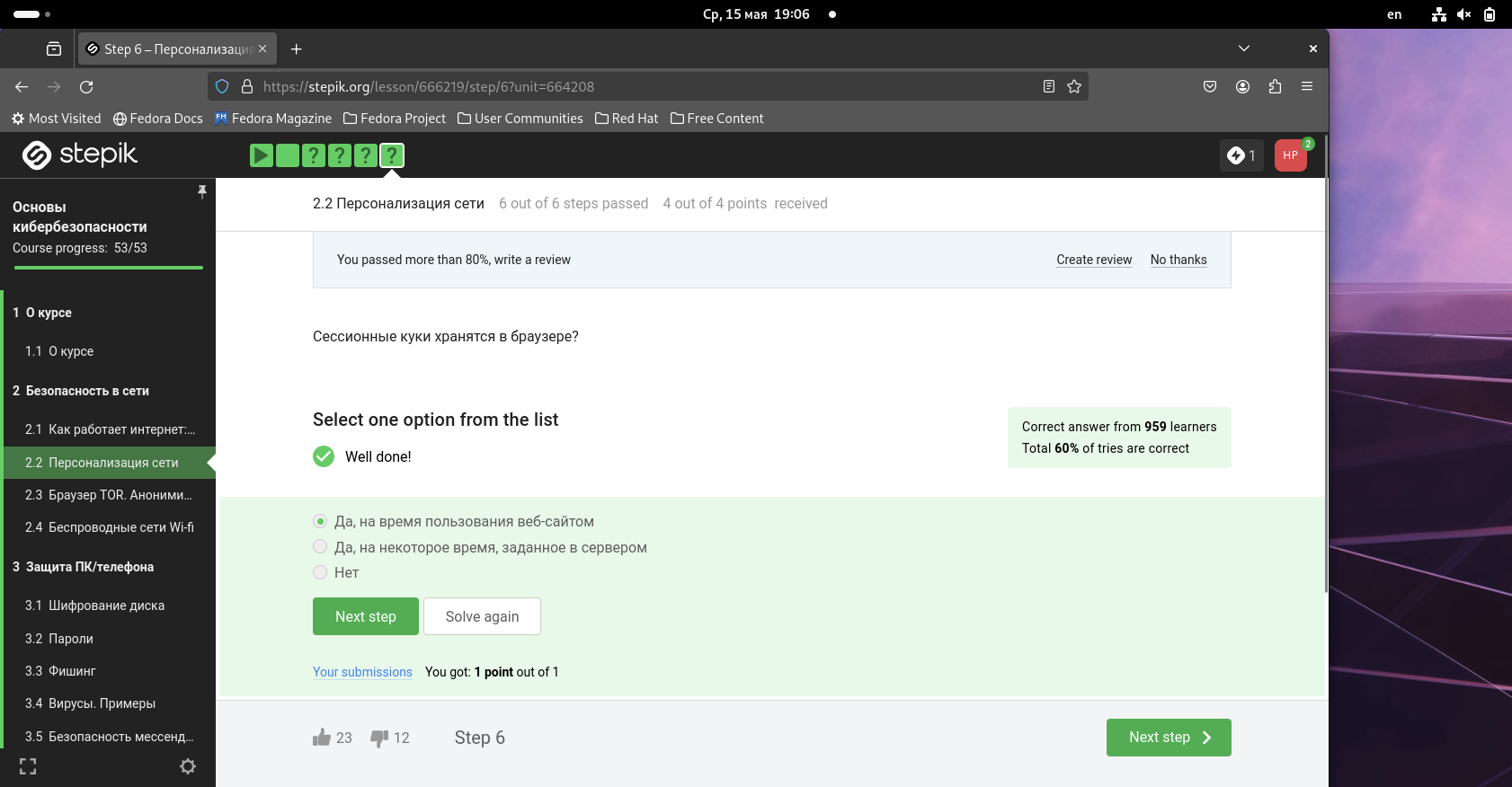
1. Куки генерируются (рис. [??]):



cokkie

Как видно из предыдущего пояснения, куки генерируются при входе на сайт самим сервером и сохраняются на компьютере пользователя.

1. Сессионные куки хранятся в браузере (рис. [??]):

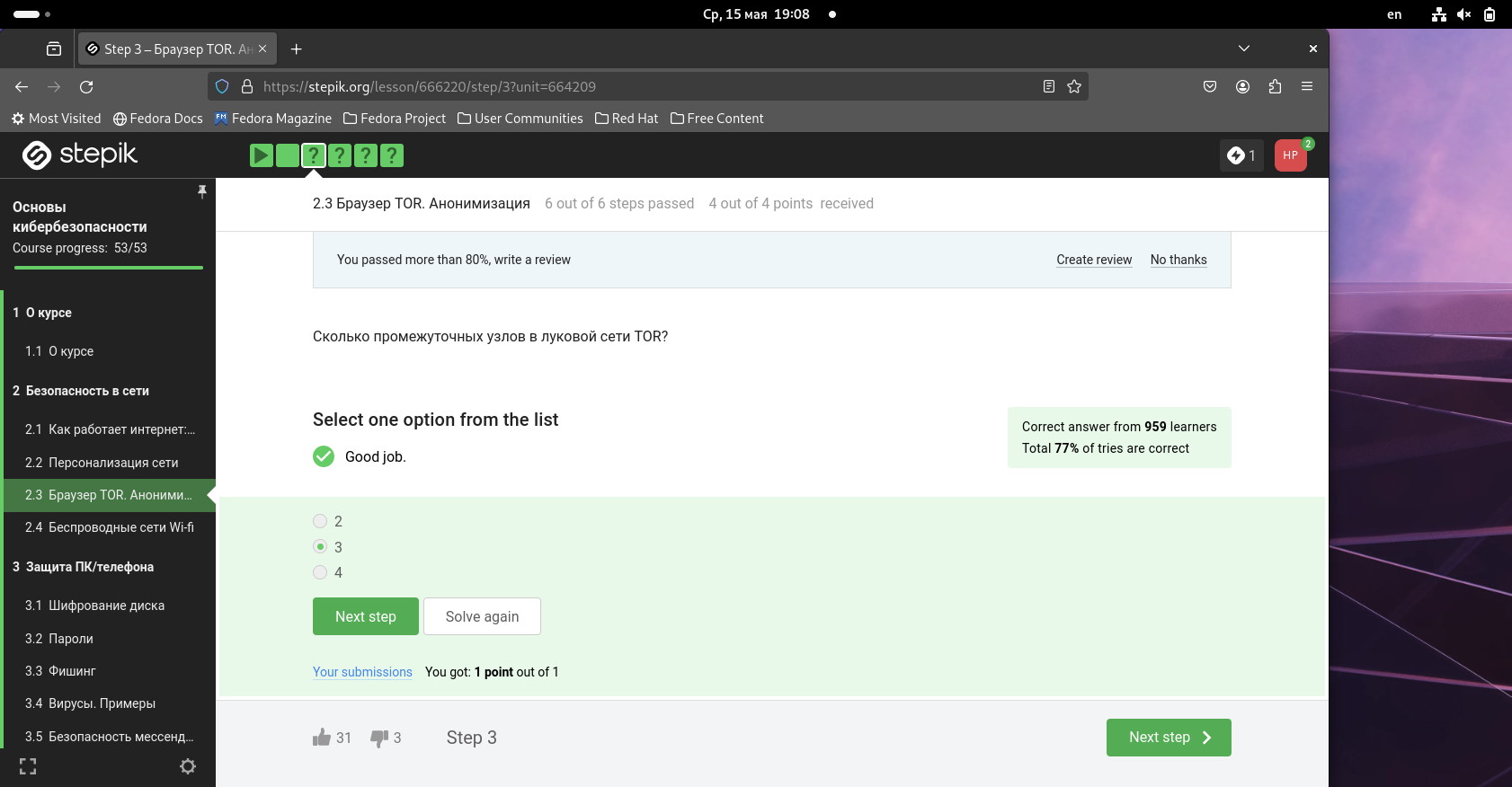


cokkie

Куки бывают сессионные; как правило, эти cookies используются при навигации на сайте и удаляются при закрытии окна браузера. То есть мы закрыли какое-то окно, интернет-магазин открыли заново - корзина пуста. Это означает, что в этом сайте, на этом сервере cookies куки сессионные. Ещё они бывают постоянные, как правило, они используются при аутентификации. Постоянные cookies применяются для сбора информации, для статистики посещаемости сайта. Откуда, например, известно, сколько раз вы посетили какой-то сайт - это записывается в куках. Хотя они и называются постоянными, как правило, у всех кук есть срок жизни, и он также записан в ещё одном значении в куках.

## 2.3 Браузер TOR. Анонимизация

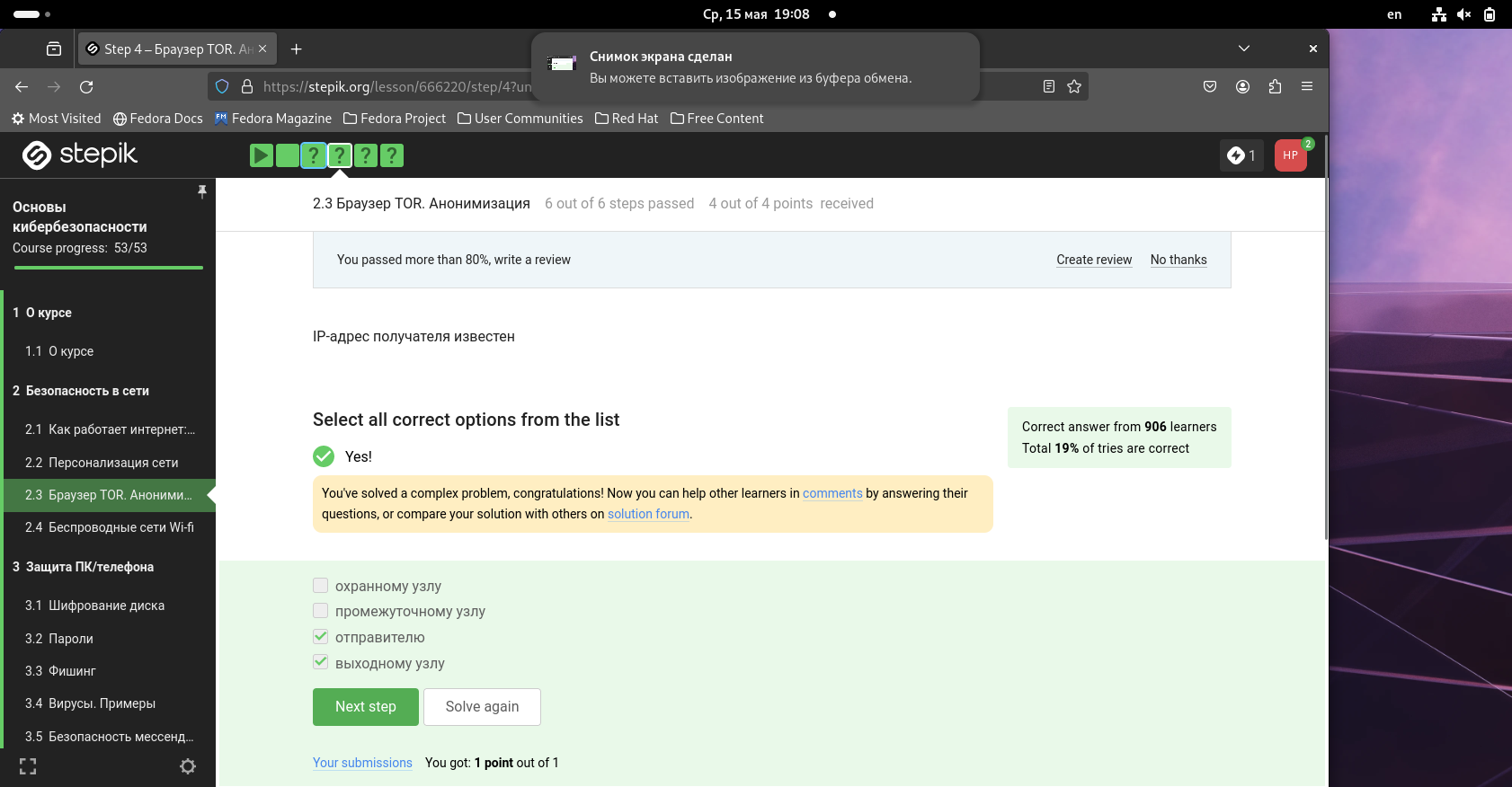
1. Сколько промежуточных узлов в луковой сети TOR (рис. [??]):



TOR

Узлы разделяются на охранный узел, промежуточный и выходной. Соответственно выходной узел, поскольку он является узлом перед получателем, знает, кому направлен пакет. Охранный узел знает, от кого пришёл пакет, поскольку он непосредственно является следующим узлом после отправителя, в то время как промежуточный узел не знает ни от кого этот пакет, ни кому он предназначен. В браузере Tor всегда есть три роутера, их не больше и не меньше. Их не меньше потому, что меньшего числа узлов не хватает для анонимизации, а большее число узлов не дает большую анонимизацию, поэтому выбирается всегда 3 луковых роутера.

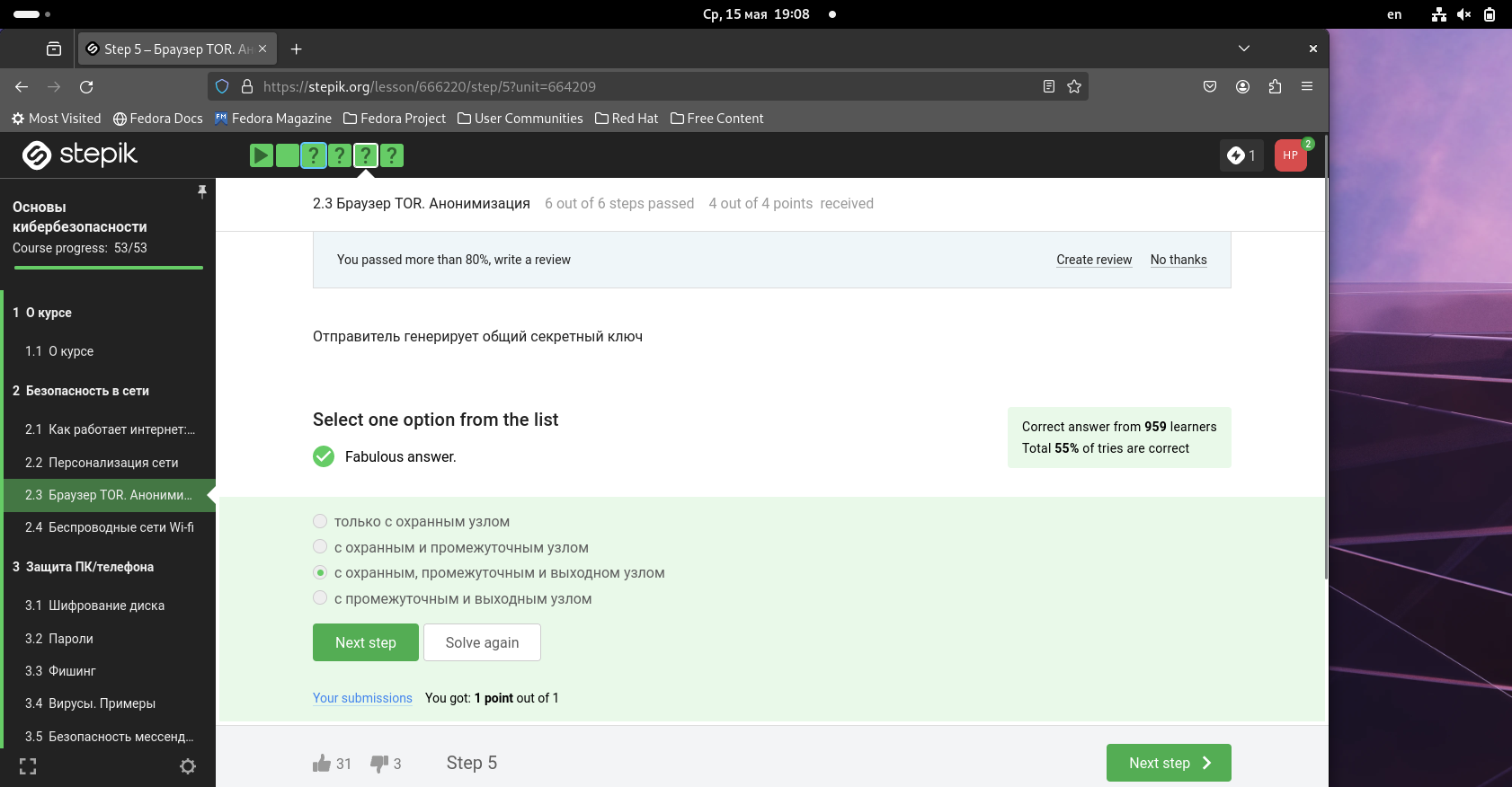
1. IP-адрес получателя известен (рис. [??]):



IP

Для того, чтобы передать некий пакет данных с помощью луковой маршрутизации, отправитель шифрует пакет и ip-получателя, генерирует 3 ключа, и постепенно расшифровывая данные, получается так, что ip-получателя знает только отправитель и выходной узел, который непосредственно передает пакет данных получателю.

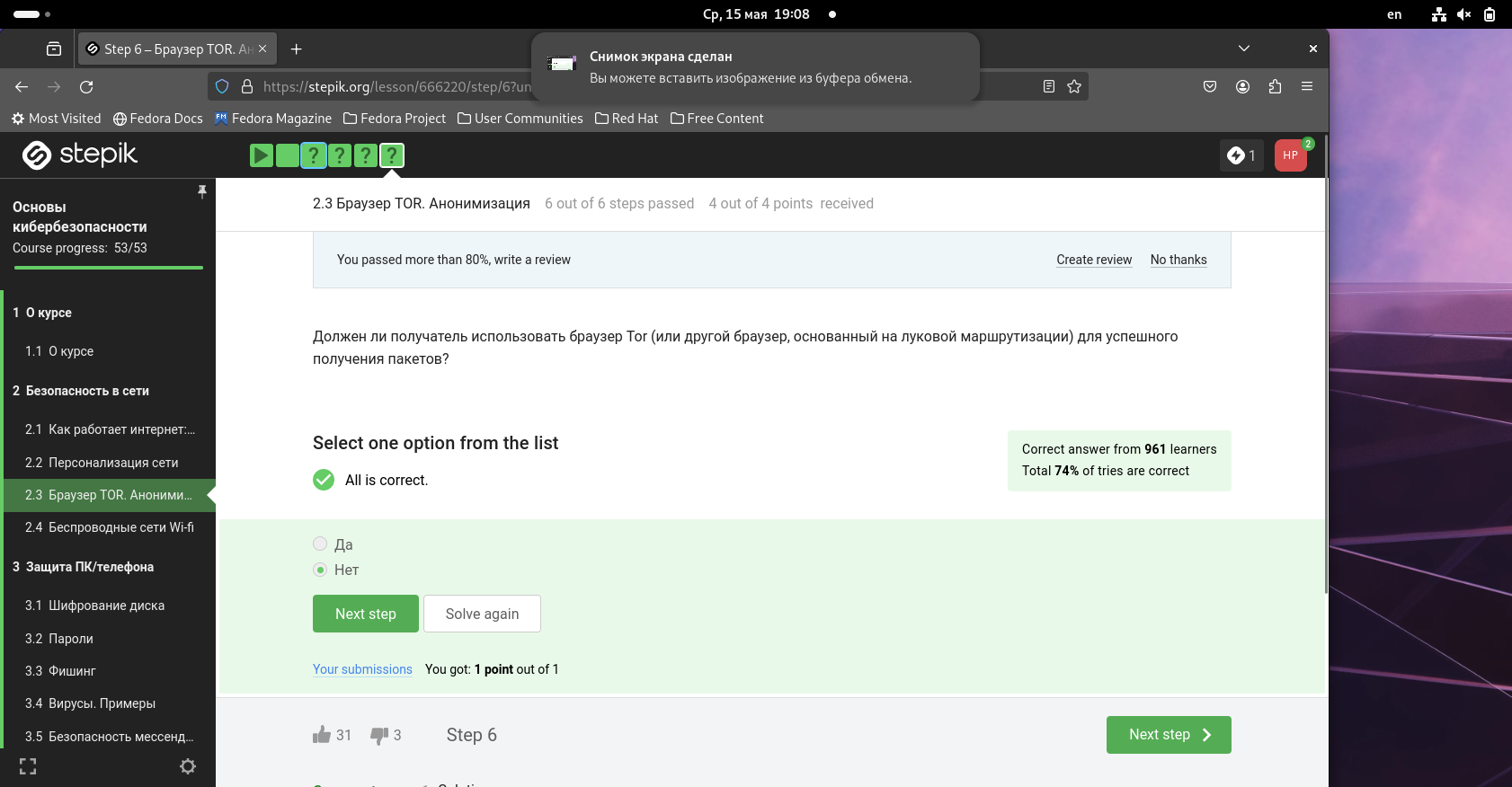
1. Отправитель генерирует общий секретный ключ (рис. [??]):



ключ

Отправитель генерирует общие ключи с тремя промежуточным узлами. Далее он шифрует свои данные под каждым из этих ключей. В начале он шифрует данные для выходного узла, сверху он шифрует зашифрованные уже данные с помощью ключа промежуточного узла, и наконец он шифрует данные с помощью ключа с охранным узлом и отправляет это тройное шифрование в сеть.

1. Должен ли получатель использовать браузер TOR (или другой браузер, основанные на луковой маршрутизации) для успешного получения пакетов (рис. [??]):



TOR

Нет, это не обязательно. Для получения пакетов использование луковой маршрутизации не обязательно.

## 2.4 Беспроводные сети Wi-fi

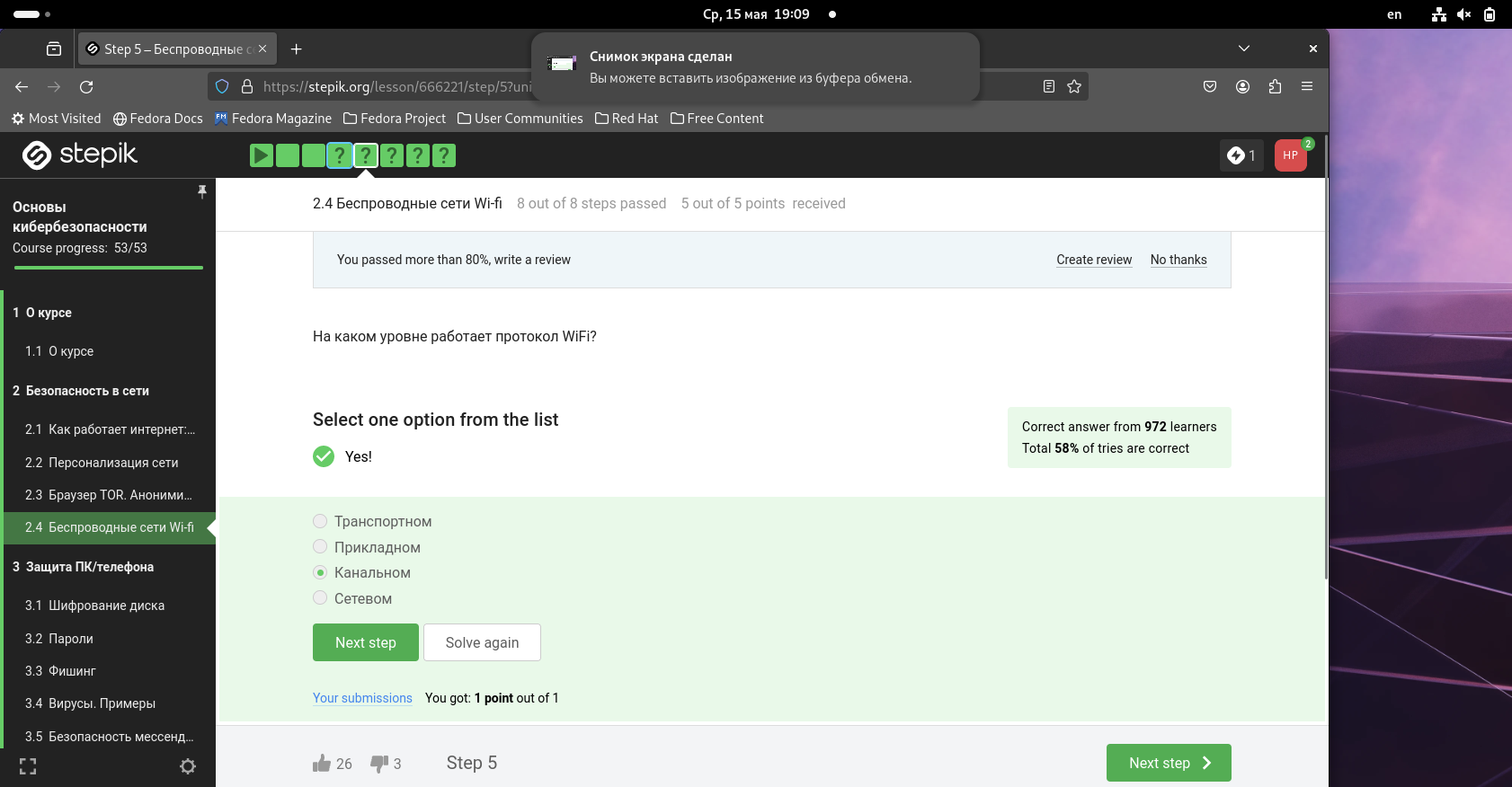
1. Wi-fi это (рис. [??]):



Wi-fi

WiFi - это технология беспроводной локальной сети, она основана на стандарте IEEE 802.11. IEEE – это организация, которая описывает вообще любые стандарты того, как работает интернет. В частности, она описывает, как должен работать беспроводной интернет, и номер этого стандарта 802.11, и все последующие модификации (этот стандарт модифицируется с течением времени) носят название 802.11 и далее какие-то буквы.

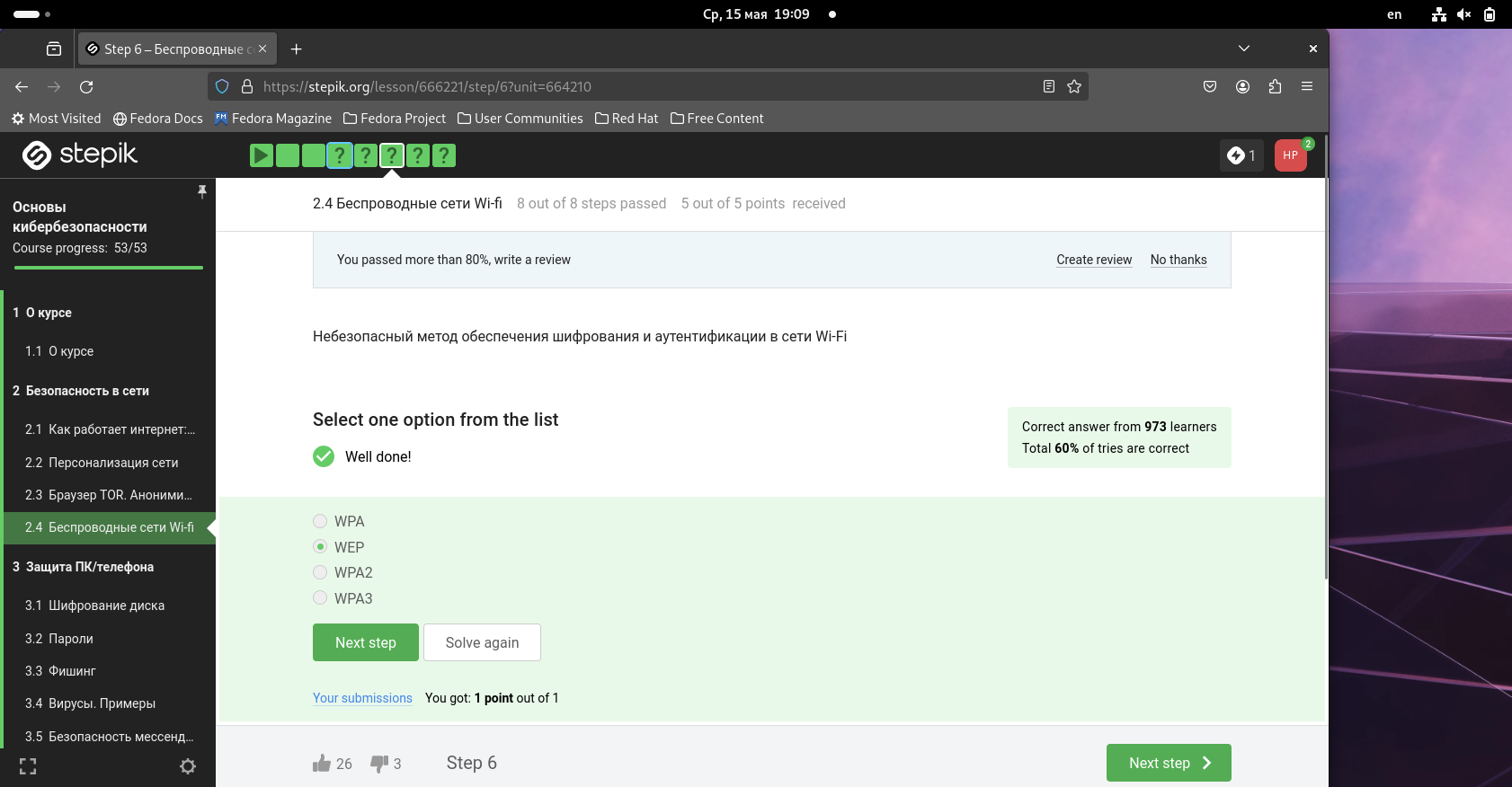
1. На каком уровне работает протокол Wi-fi (рис. [??]):



Wi-fi

Канальный уровень (англ. Link layer) описывает способ кодирования данных для передачи пакета данных на физическом уровне (то есть специальные последовательности бит, определяющих начало и конец пакета данных, а также обеспечивающие помехоустойчивость). Ethernet, например, в полях заголовка пакета содержит указание того, какой машине или машинам в сети предназначен этот пакет. Примеры протоколов канального уровня — Ethernet, IEEE 802.11 WLAN, SLIP, Token Ring, ATM и MPLS.

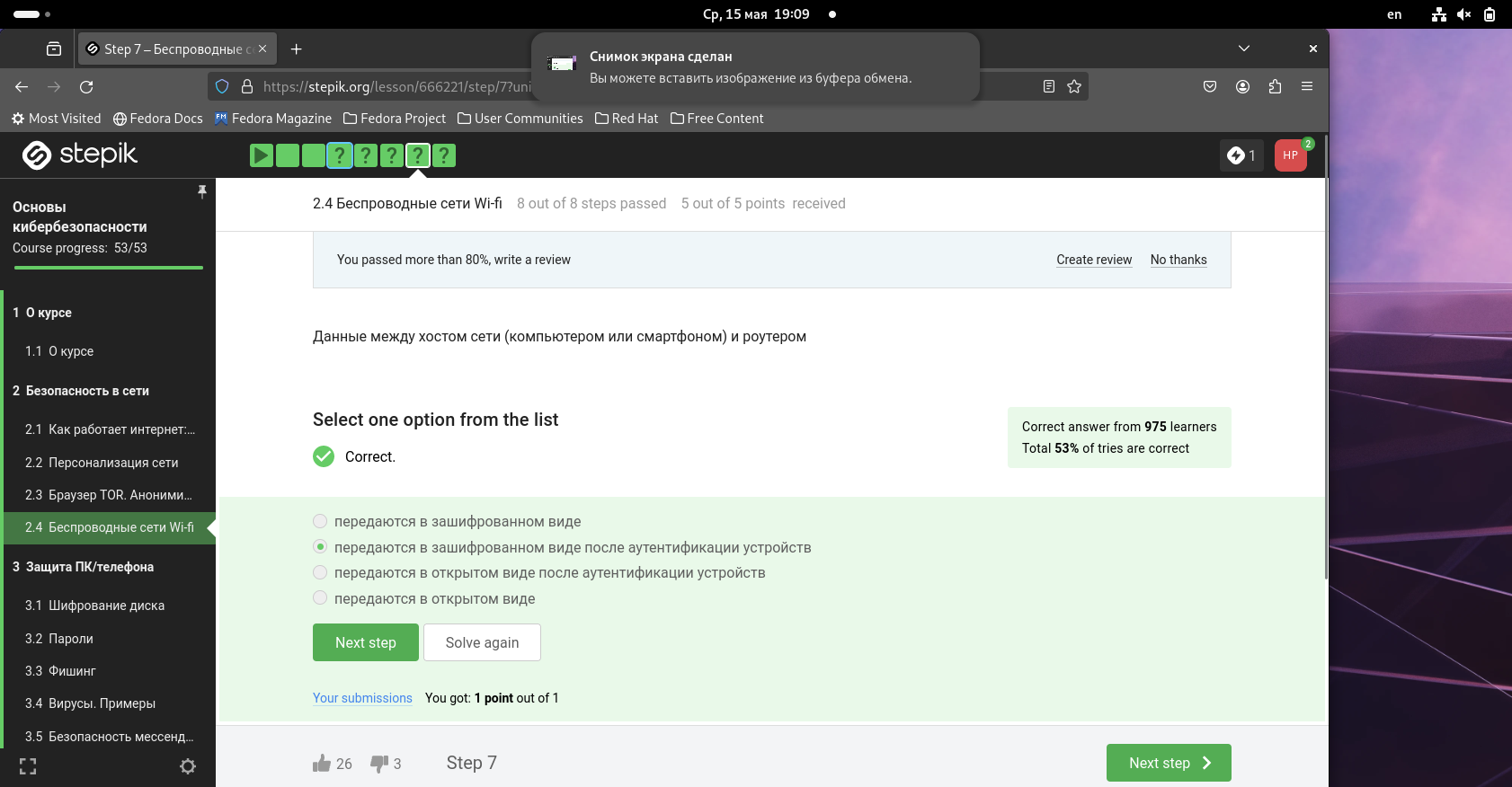
1. Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi (рис. [??]):



Wi-fi

Самый ранний и на сегодняшний день небезопасный метод шифрования данных WiFi называется WEP. Он устарел и уже категорически не рекомендуется к использованию. Он устарел, в частности, потому, что использовал малую длину ключа: так, например, он использовал длину ключа в 40 бит, это довольно мало на сегодняшний день, он может быть легко взломан.

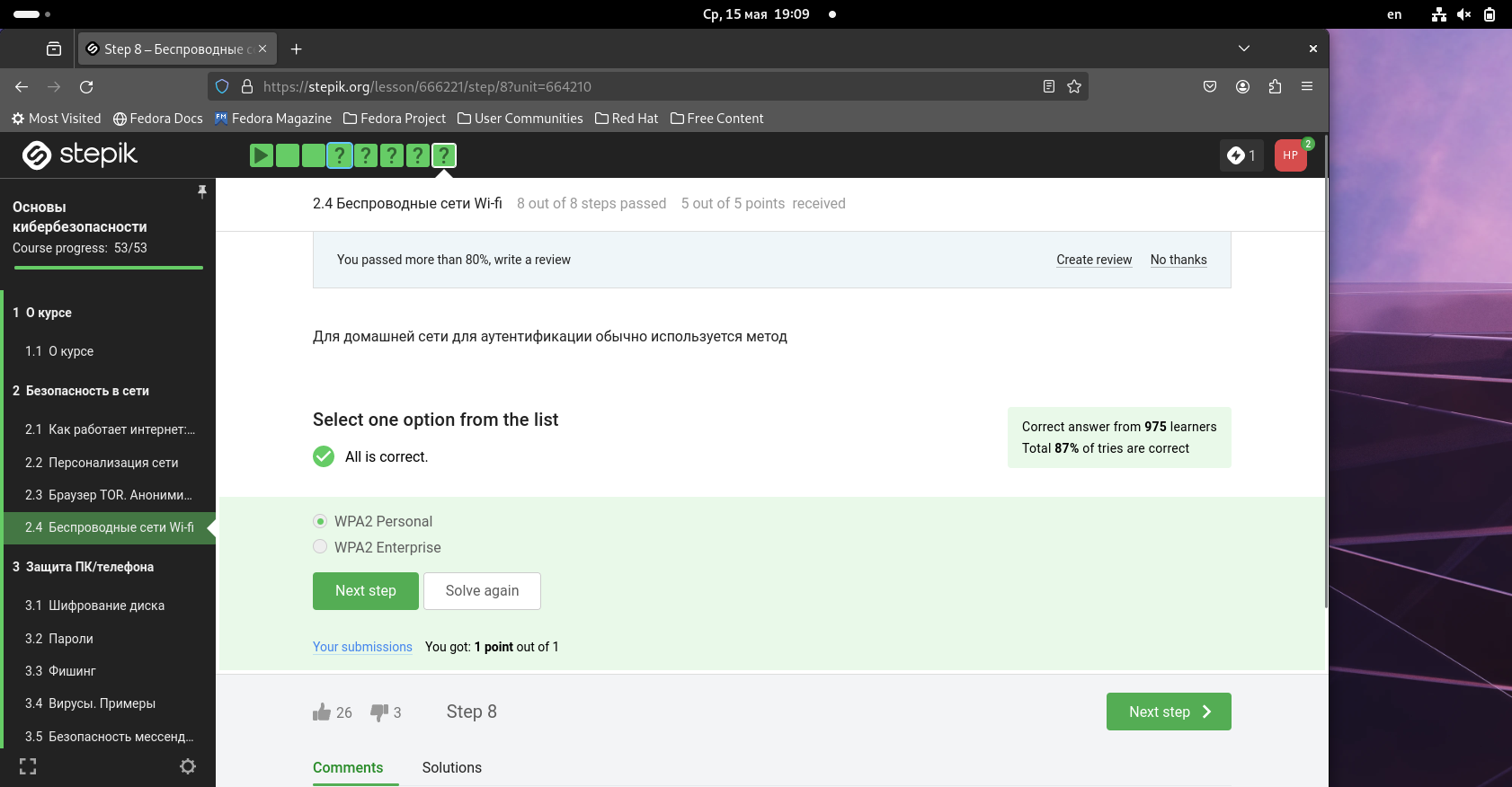
1. Данные между хостом сети (компьютером или смартфоном) и роутером (рис. [??]):



Данные

Когда мы с вами соединяемся к роутеру, мы шифруем наши данные, и до того, как начать шифрование, мы аутентифицируем себя, свое устройство этому самому роутеру.

1. Для домашней сети для аутентификации обычно используется метод (рис. [??]):



Домашняя сеть

Аутентификация в современных алгоритмах WPA, WPA2 может осуществляться в двух разных режимах: WPA Personal - это классическая аутентификация по паролю, как правило, такой алгоритм используется в домашних сетях или в небольших корпоративных сетях; более сложный метод аутентификации называется WPA Enterprise - это когда у нас существует база данных всех зарегистрированных пользователей, и когда человек подключается к сети WiFi, по этой базе данных проверяется, есть ли он в базе или нет, и как правило, сама эта база данных со списком разрешенных пользователей находится на специальных серверах. Это довольно сложное устройство аутентификации, которое, скорее всего, не нужно для маленьких домашних сетей.

# 3 Выводы

В ходе работы мы изучили, как работают интернет протоколы, что такое персонализация сети, как работает анонимизирование в интернете, что такое луковая маршрутизация и как работают беспроводные сети Wi-fi.

# Список литературы