Внешний курс. Блок 1: Безопасность в сети

Дисцеплина: Основы информационной безопасности

Неустроева Ирина Николаевна

Содержание

# 1 Цель работы

Выполненить контрольные задания первого блока “Безопасность в сети” внешнего курса “Основы кибербезопасности”.

# 2 Выполнение заданий блока “Основы Кибербезопасности”

## 2.1 Как работает интернет: базовые сетевые протоколы

Протокол HTTP(S) протокол прикладного уровня, ответ на вопрос 1 - HTTPS (рис. 1).

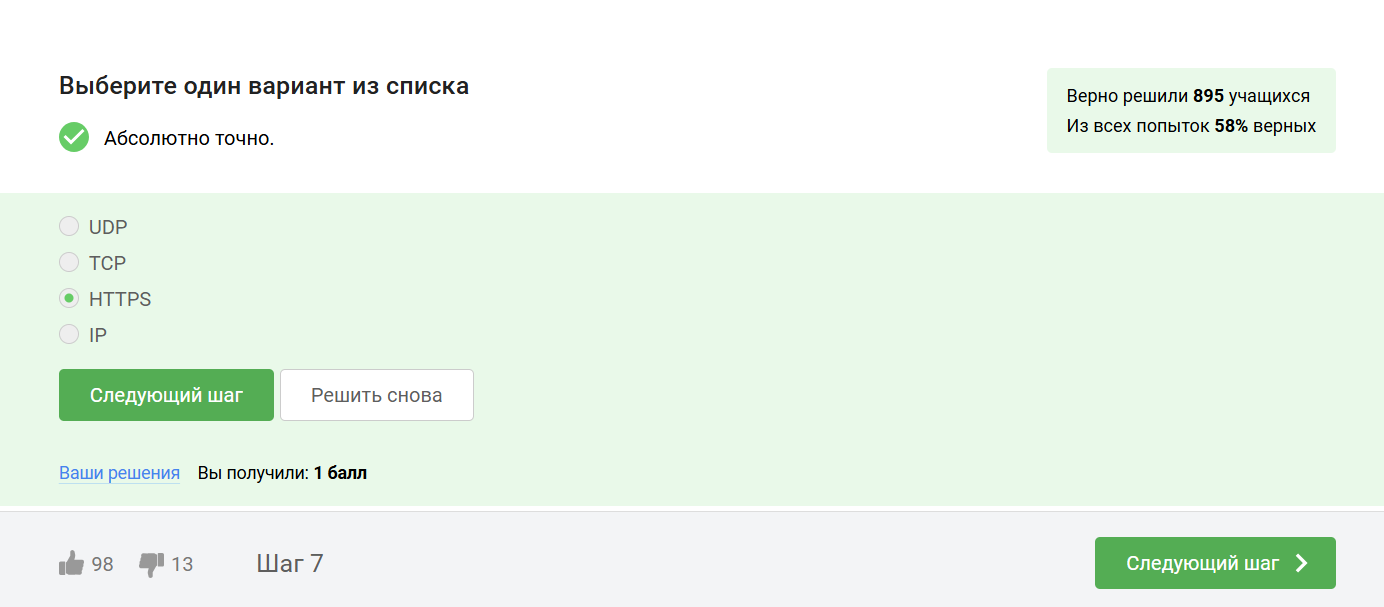


Рис. 1: Вопрос 2.1.1

На транспортном уровне существует два примера протокола: первый - это TCP, в честь которого названа модель. (рис. 2).

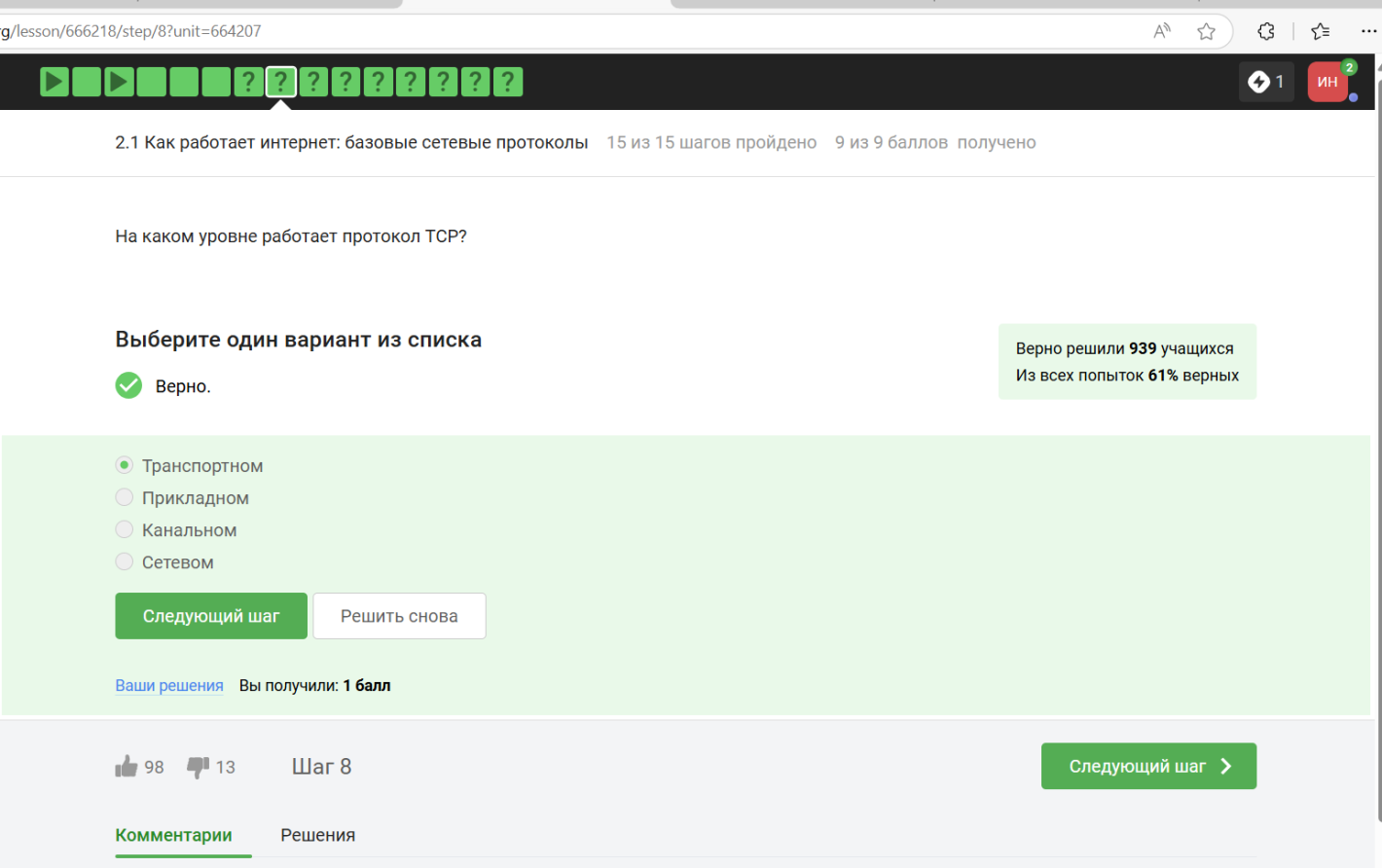


Рис. 2: Вопрос 2.1.2

Т.к адрес состоит из большего набора чисел, а именно это 4 или 6 цифер от 0 до 255. В двух вариантах встречаются цифры больше 255, что неверно(рис. 3).

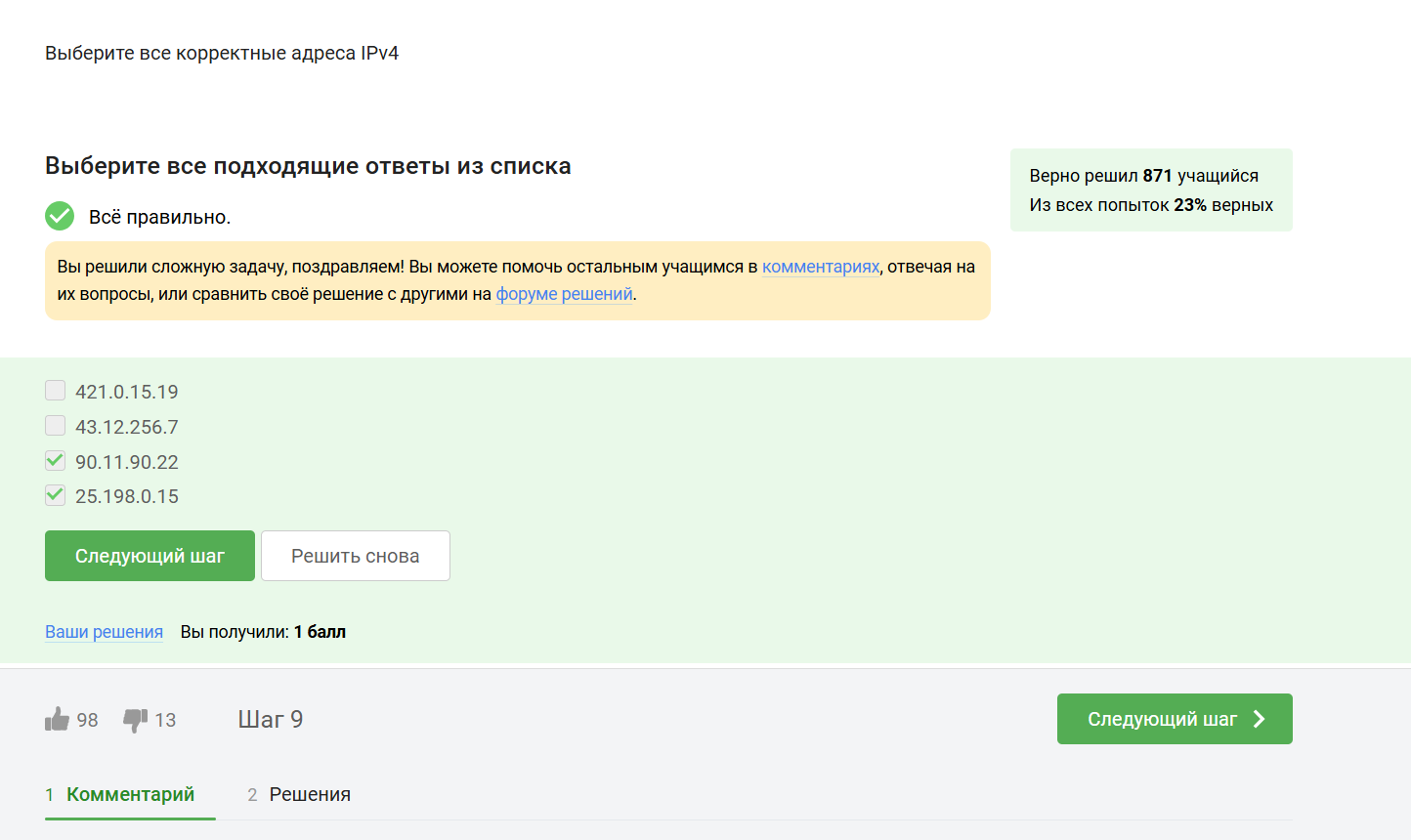


Рис. 3: Вопрос 2.1.3

Основная задача DNC это сопоставлять название ( доменное имя, с корекстым IP-адресом) с тем, где лежит этот сервер, этот сайт. (рис. 4).

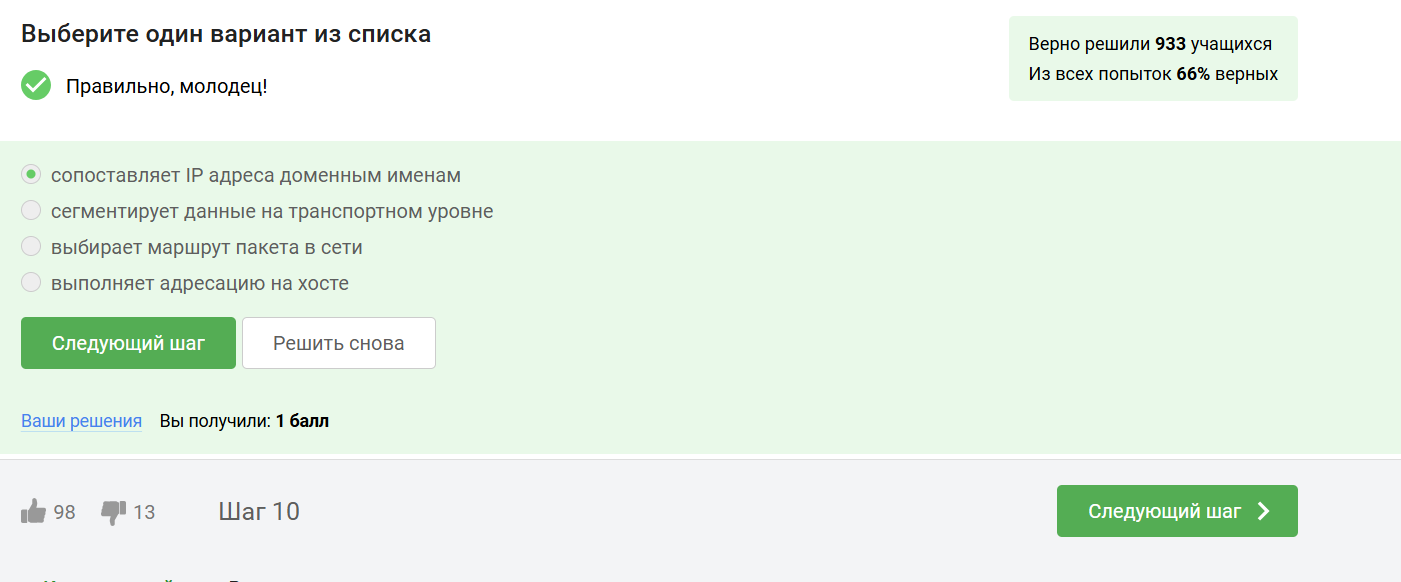


Рис. 4: Вопрос 2.1.4

Классификация протоколов в модели TCP/IP:

* Прикладной уровень: HTTP, RTSP, FTP, DNS.
* Транспортный уровень: TCP, UDP, SCTP, DCCP.
* Сетевой уровень: IP.
* Уровень сетевого доступа (Канальный) (Link Layer): Ethernet, IEEE 802.11, WLAN, SLIP, Token Ring, ATM и MPLS(рис. 5).

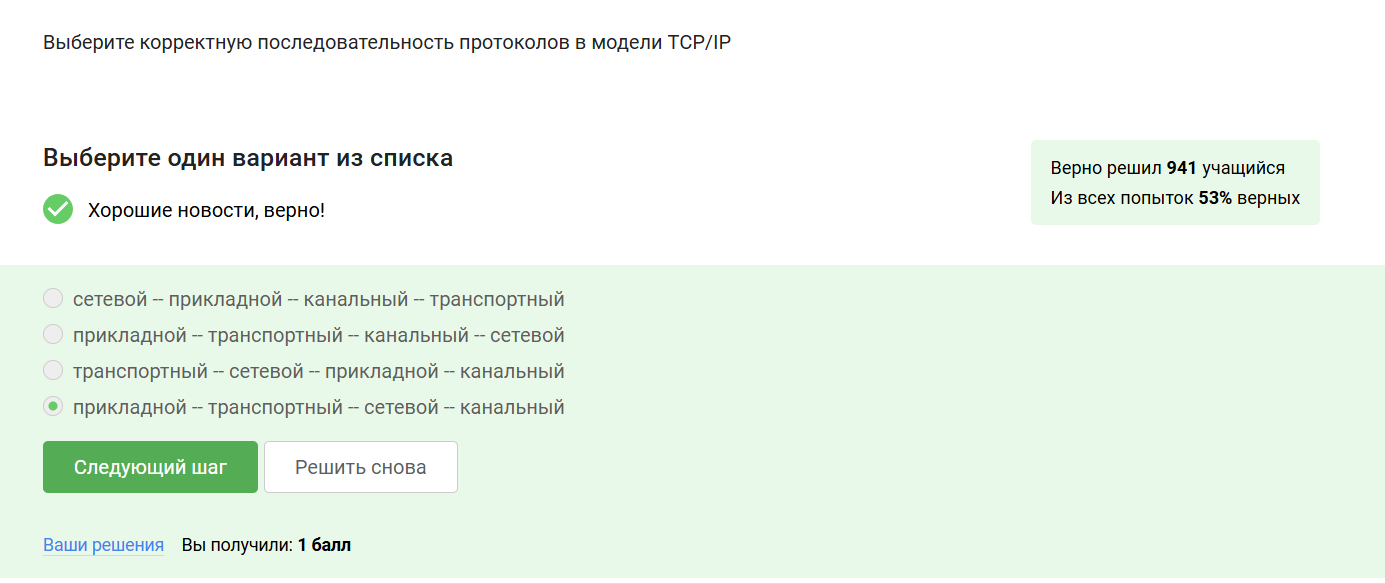


Рис. 5: Вопрос 2.1.5

Протокол http передает не зашифрованные данные, а протокол https уже будет передавать зашифрованные данные (рис. 6).

https передает зашифрованные данные, поэтому одна из фаз это передача данных, другая должна быть рукопожатием

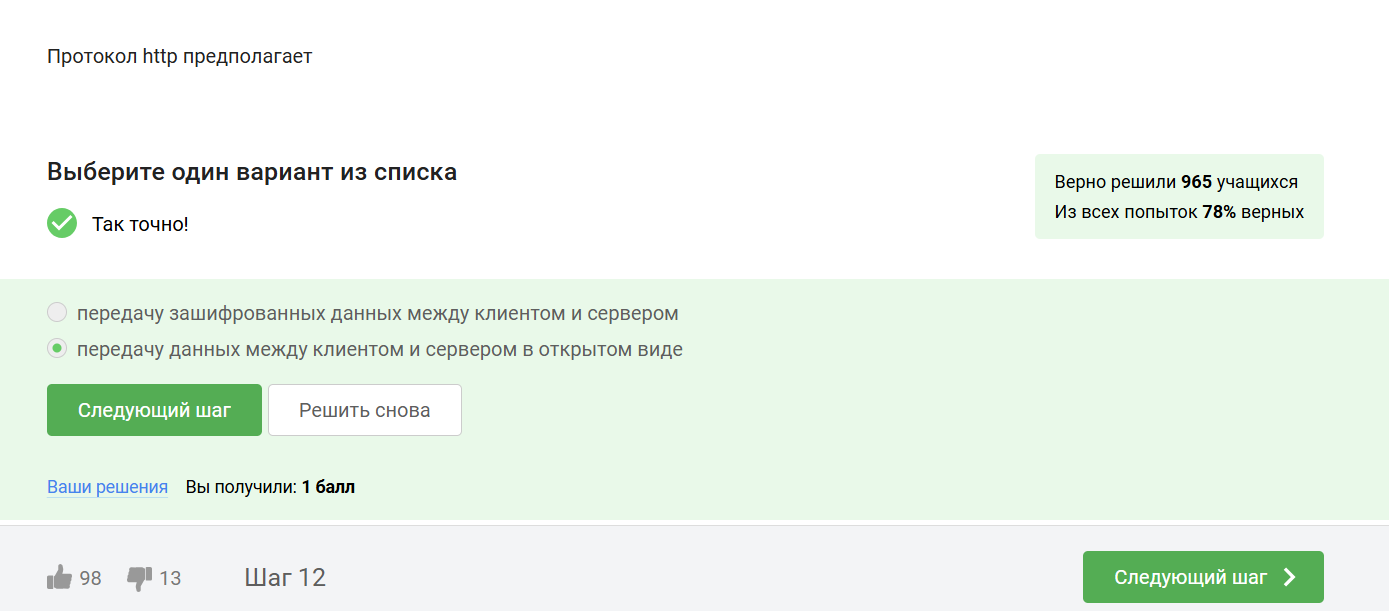


Рис. 6: Вопрос 2.1.6

TLS определяется и клиентом, и сервером, чтобы было возможно подключиться (рис. 7).

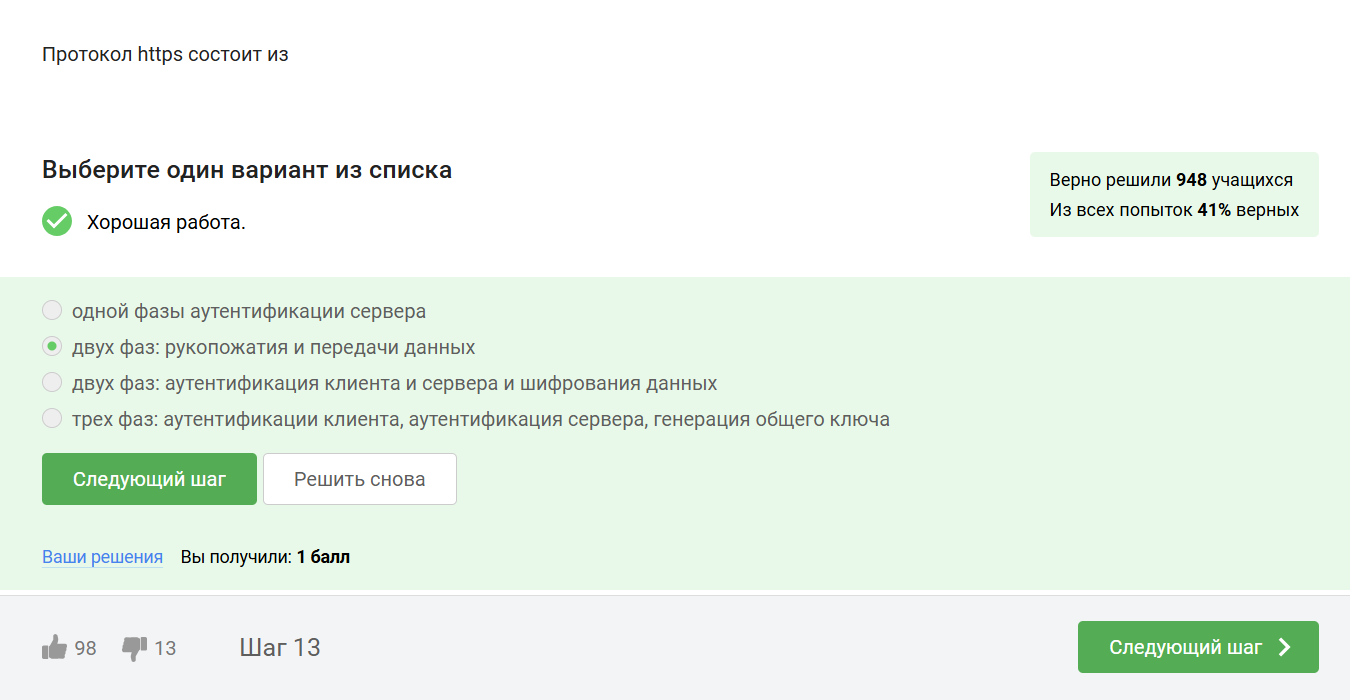


Рис. 7: Вопрос 2.1.7

TLS определяется клиентом и сервером, чтобы возможно было подключиться (рис. 8).

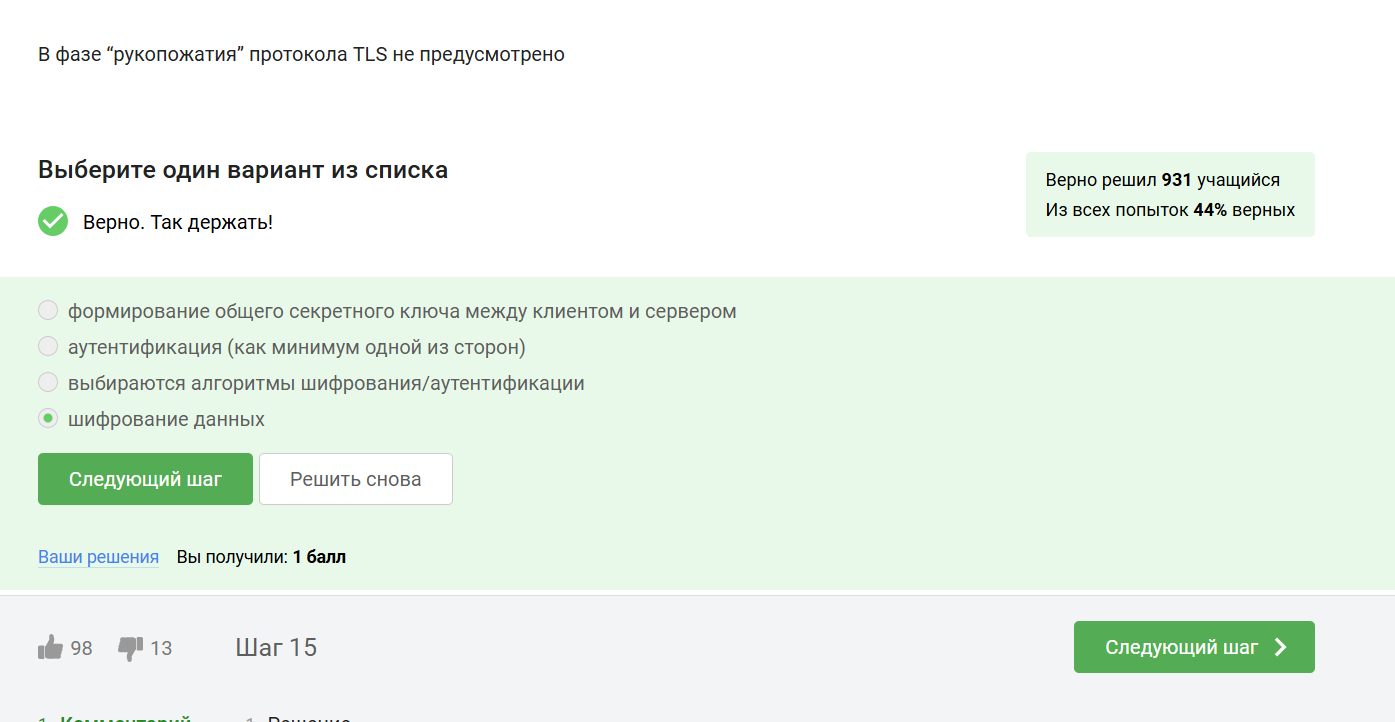


Рис. 8: Вопрос 2.1.8

Фаза рукопожатия вкючает в себя:

* выбор параметров, протоколов
* аутентификация (как минимум, сервера)
* формируется общий секретный ключ K

Следовательно вариант с шифрованием лишний (рис. 9).

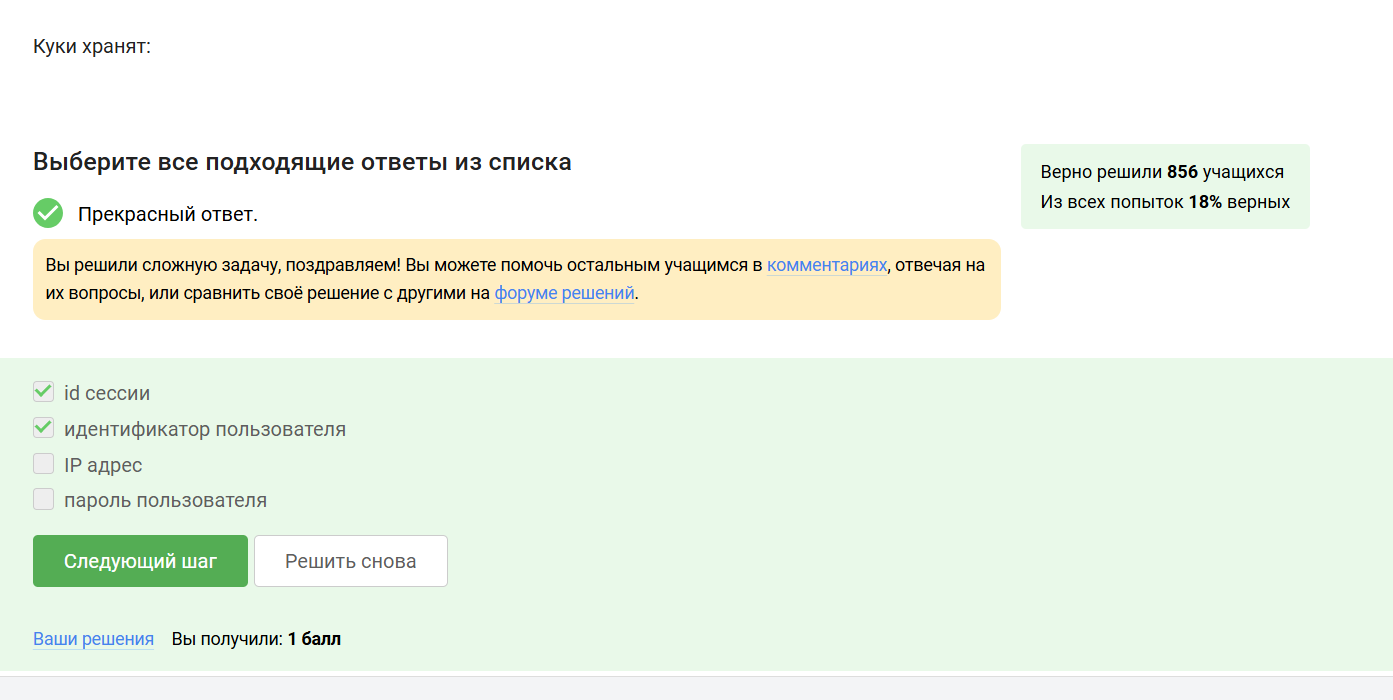


Рис. 9: Вопрос 2.1.9

## 2.2 Персонализация сети

Куки хранят в себе список параметров и их значений. Этими параметрами могут быть id пользователя, id сессии, тип браузера и некоторые действия пользователей(рис. 10).

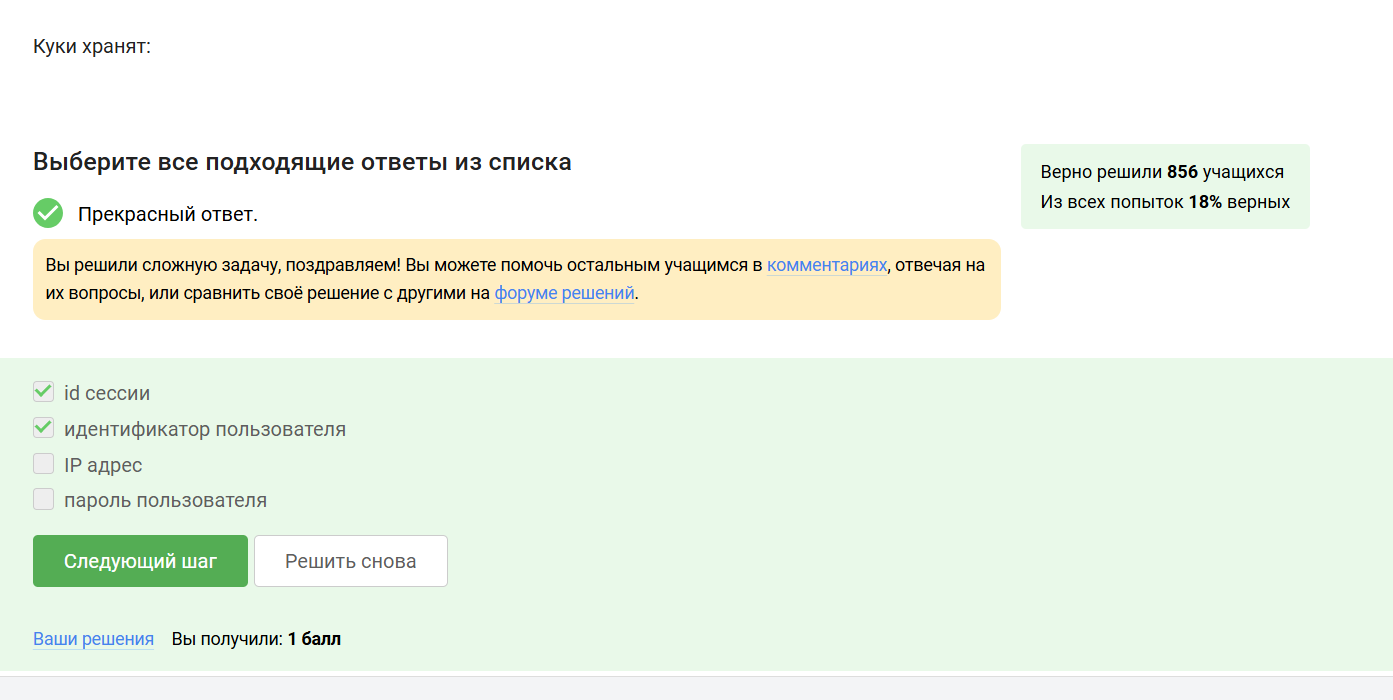


Рис. 10: Вопрос 2.2.1

Куки не делают соединение надежным (рис. 11).

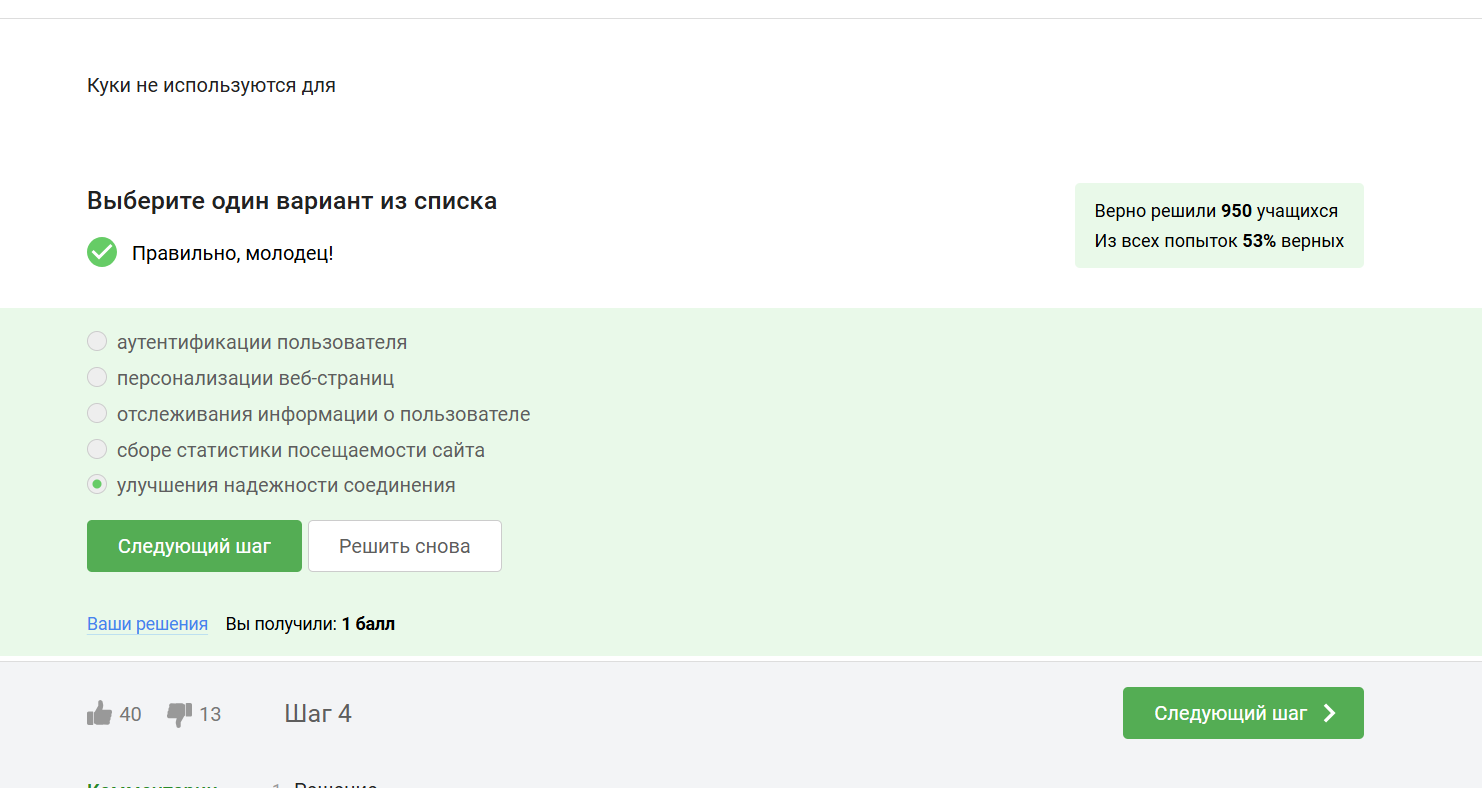


Рис. 11: Вопрос 2.2.2

Куки генерируются сервером(рис. 12).

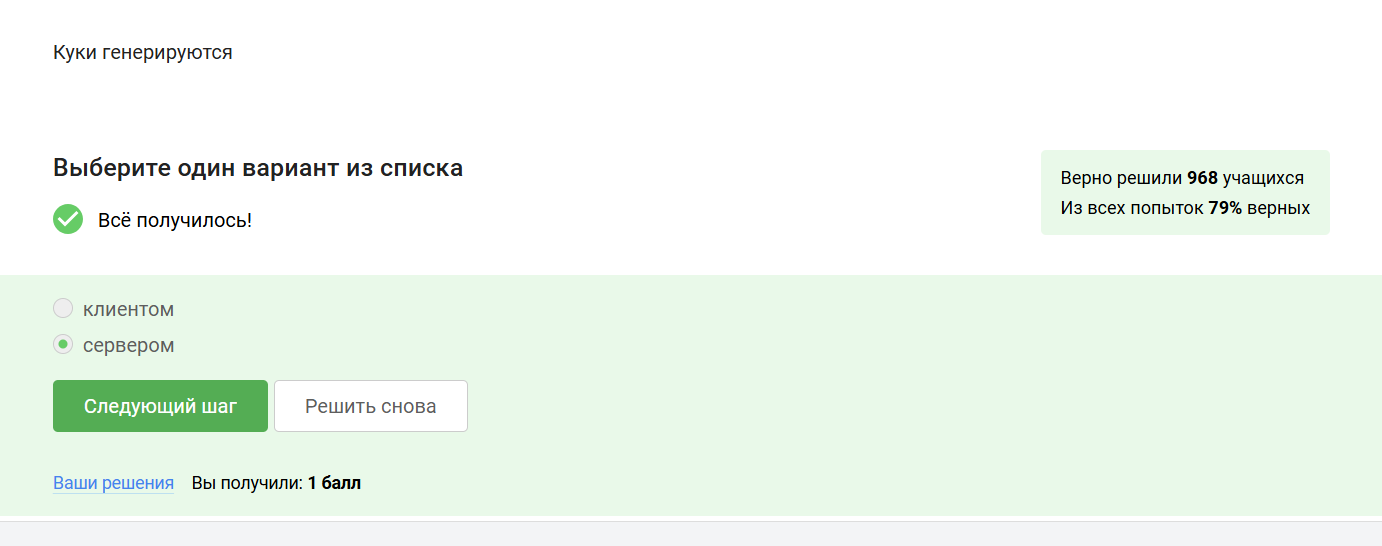


Рис. 12: Вопрос 2.2.3

Куки бывают сессионные, удаляются при закрытии окна браузера (рис. 13).

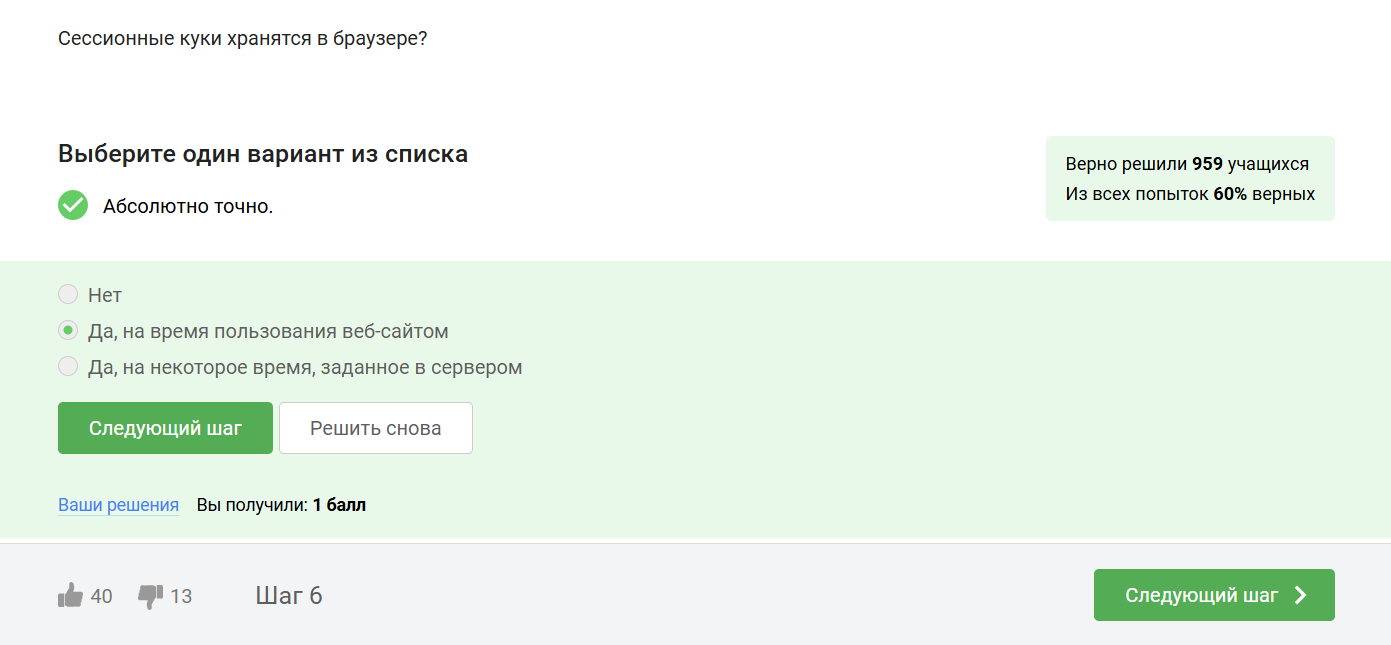


Рис. 13: Вопрос 2.2.4

## 2.3 Браузер TOR. Анонимизация

В луковой модели маршрутизации у нас тоже есть узлы. Они разделяются на охранный узел, промежуточный и выходной. В браузере Tor всегда есть три роутера, их не больше и не меньше (рис. 14).

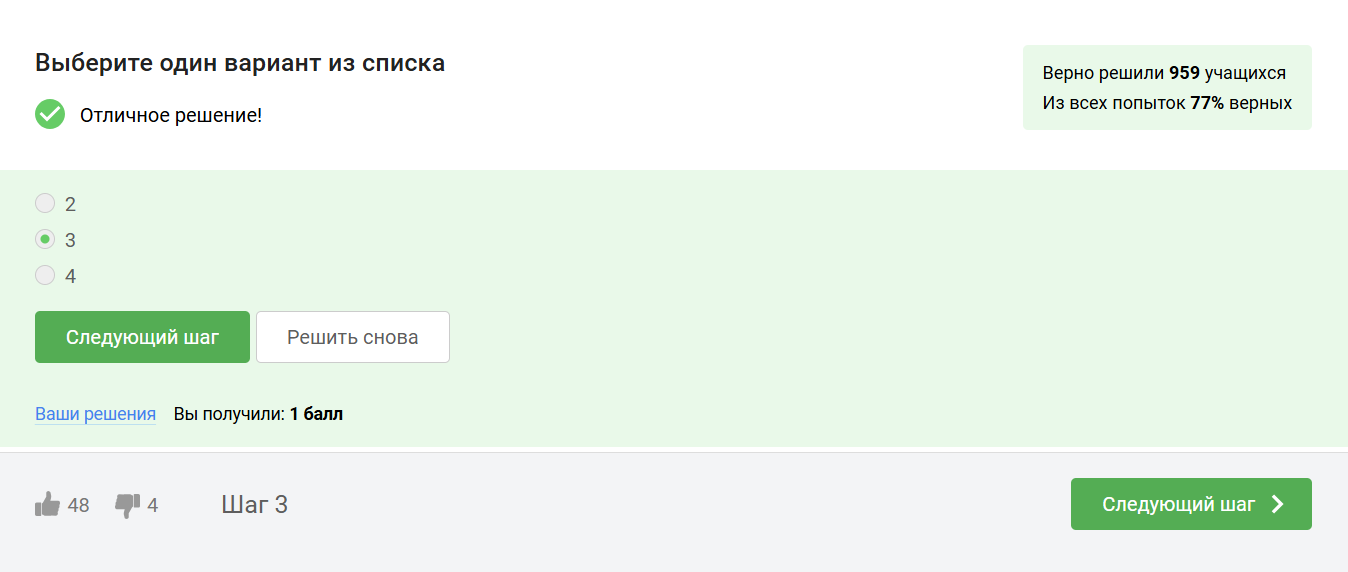


Рис. 14: Вопрос 2.3.1

IP-адрес не должен быть известен охранному и промежуточному узлам (рис. 15).

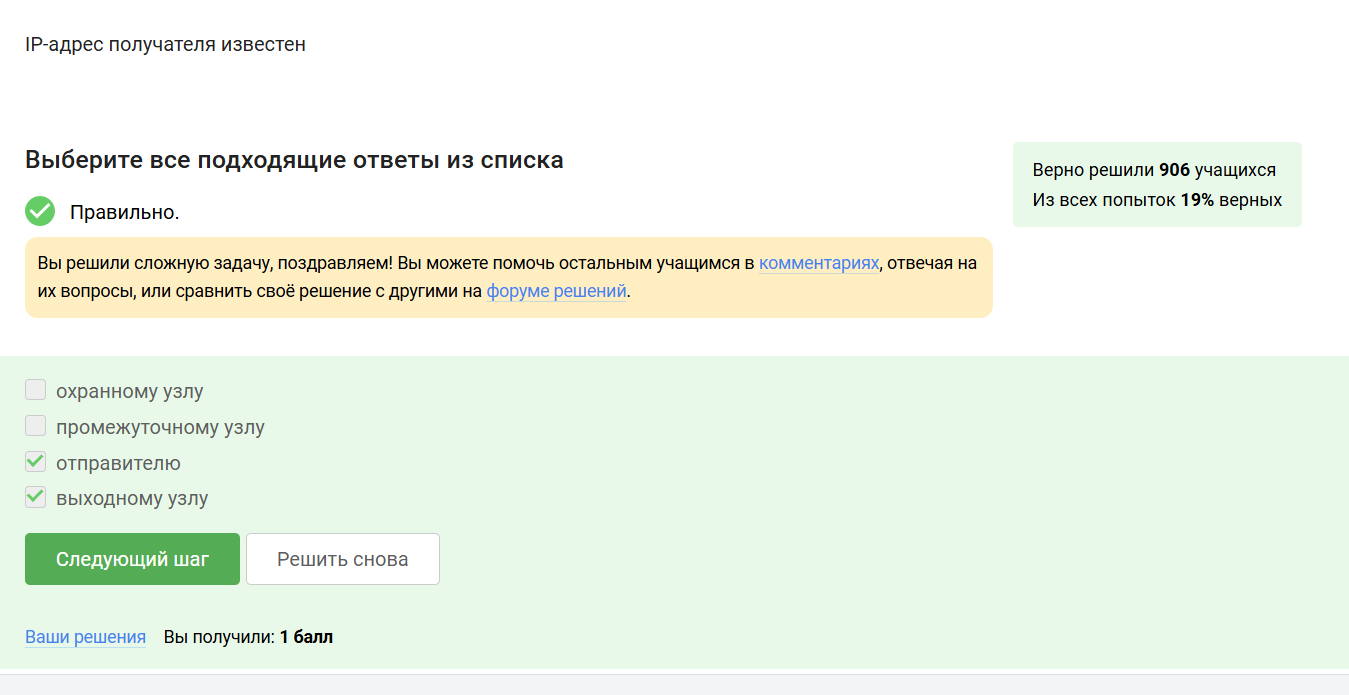


Рис. 15: Вопрос 2.3.2

В анонимных сетях, таких как Tor, общий секретный ключ для сквозного шифрования требует участия всех трех типов узлов: охранного, промежуточного и выходного. Охранный узел сам по себе не обеспечивает генерацию ключа. Каждый узел вносит свой вклад в криптографический протокол (например, Diffie-Hellman), обеспечивая анонимность и защиту от перехвата. (рис. 16).

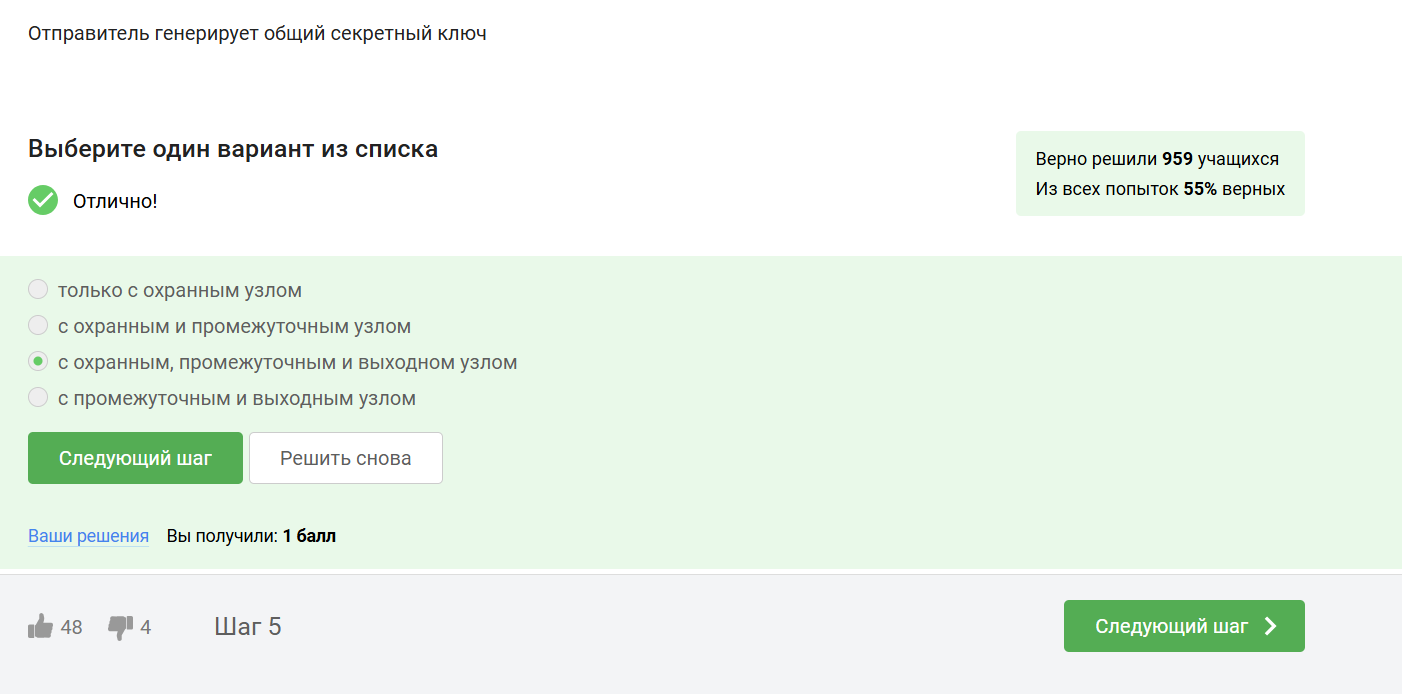


Рис. 16: Вопрос 2.3.3

Для получения пакетов не нужно использовать TOR. TOR — это технология, которая позволяет с некоторым успехом скрыть личность человека в интернете.(рис. 17).

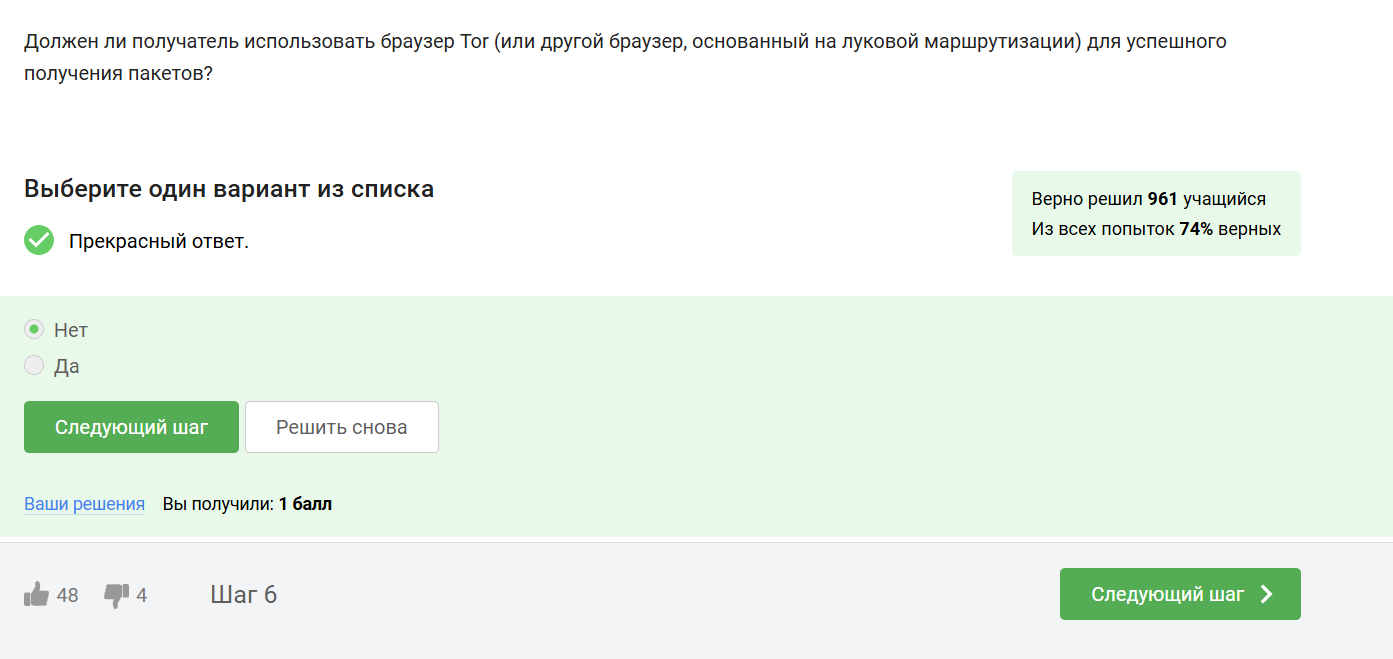


Рис. 17: Вопрос 2.3.4

## 2.4 Беспроводные сети Wi-fi

WiFi - это технология беспроводной локальной сети, она основана на стандарте IEEE 802.11 (рис. 18).

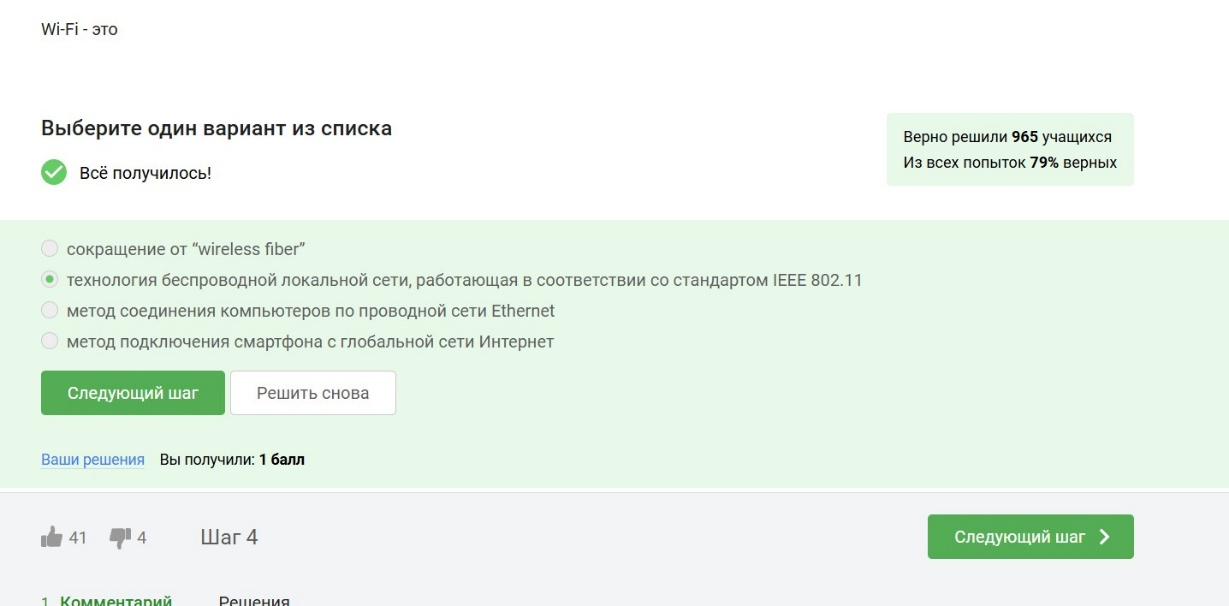


Рис. 18: Вопрос 2.4.1

WiFi работает на самом нижнем канальном уровне (рис. 19).

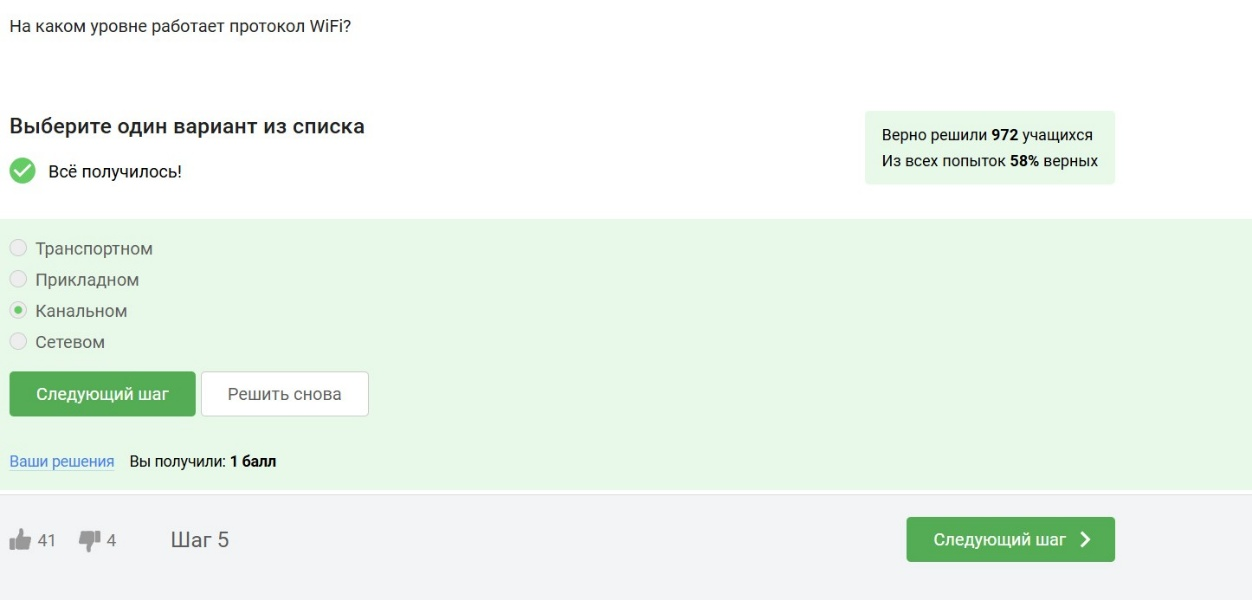


Рис. 19: Вопрос 2.4.2

WEP - устаревший и небезопасный метод шифрования WiFi из-за короткой длины ключа (40 бит), что делает его легко взламываемым. Использовать WEP категорически не рекомендуется.(рис. 20).

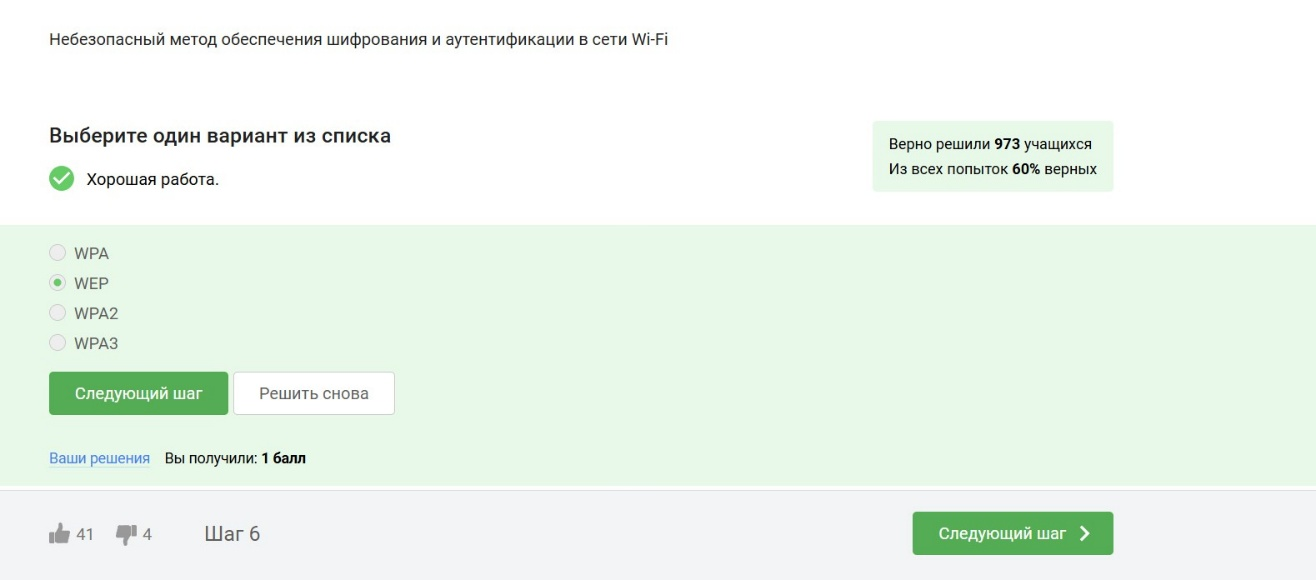


Рис. 20: Вопрос 2.4.3

Безопасность WiFi подразумевает защиту передачи данных между устройством (телефон, компьютер) и роутером (подключенным к интернету), осуществляемую с помощью шифрования и аутентификации.(рис. 21).

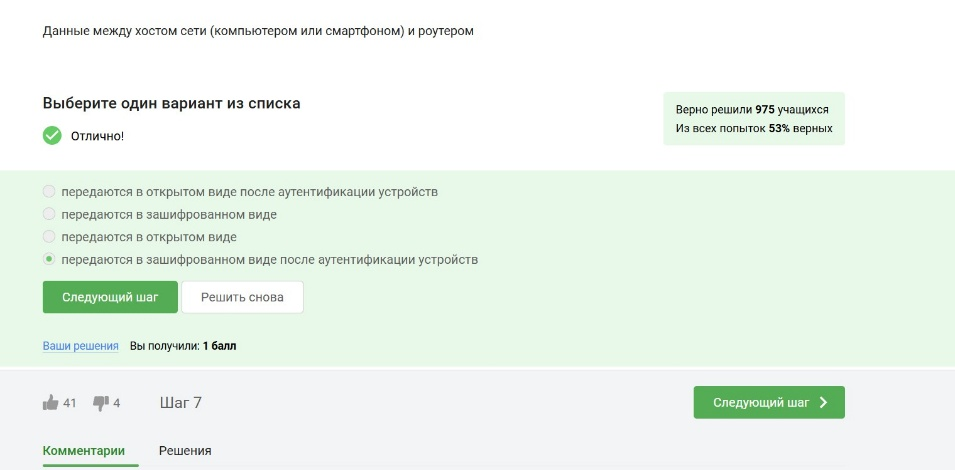


Рис. 21: Вопрос 2.4.4

WPA2 Personal предназначен для домашнего использования, а WPA2 Enterprise - для коммерческих организаций. (рис. 22).

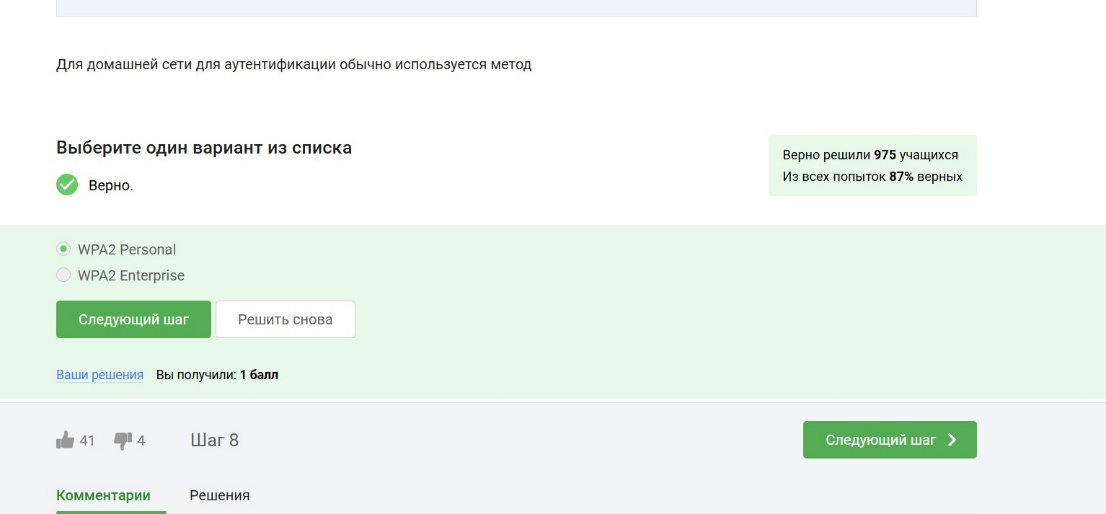


Рис. 22: Вопрос 2.4.5

# 3 Выводы

В результате выполнения блока “Безопасность в сети” я узнала, как работают сетевые пратаколы, куки-файлы, сети вайфай и для чего нужен браузер Tor.