Внешний курс. Блок 1: Безопасность в сети

Дисциплина: Основы информационной безопасности

Ибатулина Дарья Эдуардовна, НКАбд-01-22

Содержание

Список иллюстраций

Список таблиц

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) является примером протокола прикладного уровня, по которому передаются веб-страницы, поэтому ответ на вопрос 1 - HTTPS (рис. [2.1]).

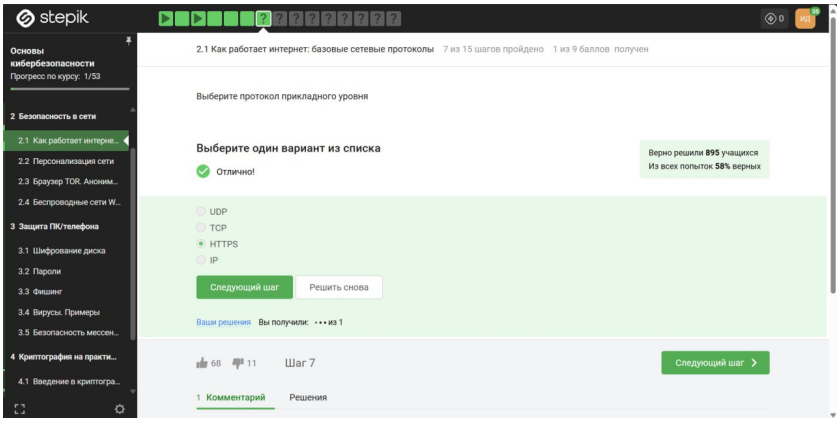

Рис. 2.1: Вопрос 2.1.1

На транспортном уровне существует два примера протокола: первый - это TCP, в честь которого названа модель. Этот протокол, в отличие от второго примера – UDP, обеспечивает надежную передачу пакетов. Ответ на вопрос - транспортный (рис. [2.2]).

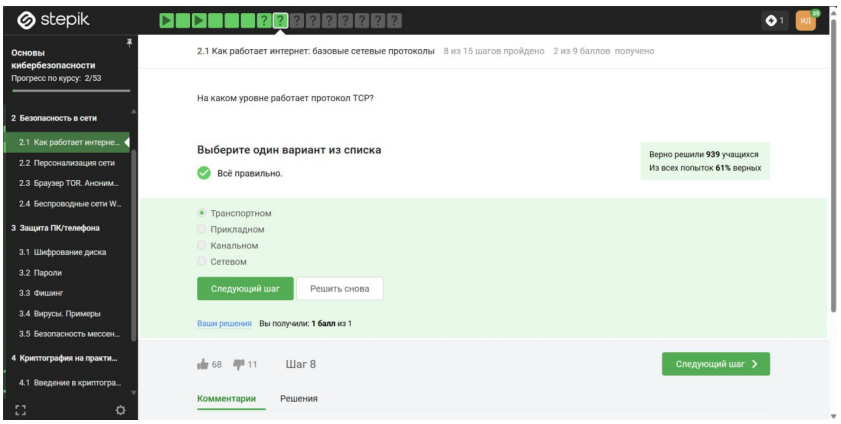

Рис. 2.2: Вопрос 2.1.2

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. В других двух вариантах встречаются числа большие 255, что неверно для IPv4 (рис. [2.3]).

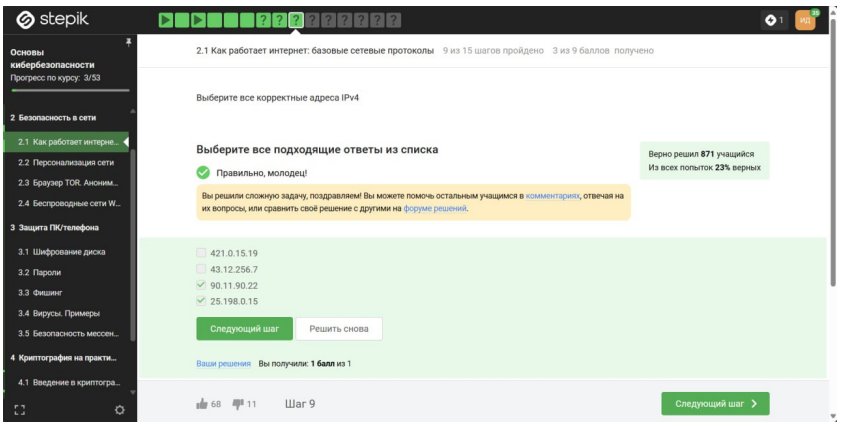

Рис. 2.3: Вопрос 2.1.3

Основная задача DNS-сервера - это сопоставить название, то есть доменное имя, с корректным IP-адресом, с тем, где лежит этот сервер, этот сайт (рис. [2.4]).

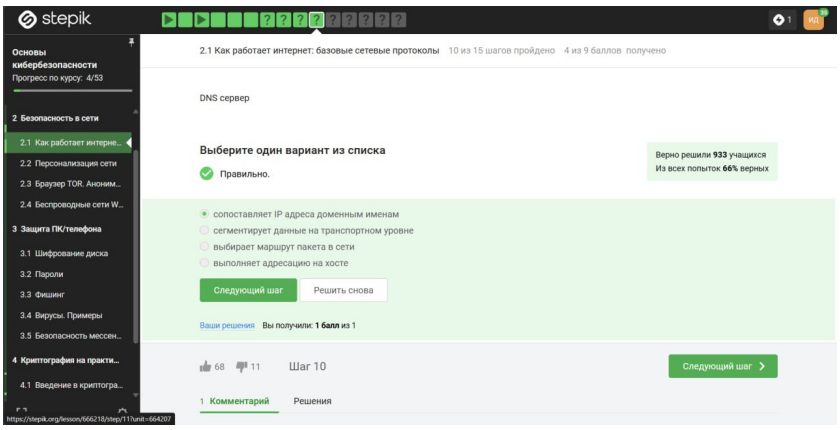

Рис. 2.4: Вопрос 2.1.4

Классификация протоколов в модели TCP/IP:

- Прикладной уровень (Application Layer): HTTP, RTSP, FTP, DNS.
- Транспортный уровень (Transport Layer): TCP, UDP, SCTP, DCCP.
- Сетевой (Межсетевой) уровень (Network Layer): IP.
- Уровень сетевого доступа (Канальный) (Link Layer): Ethernet, IEEE 802.11, WLAN, SLIP, Token Ring, ATM и MPLS (рис. [2.5]).

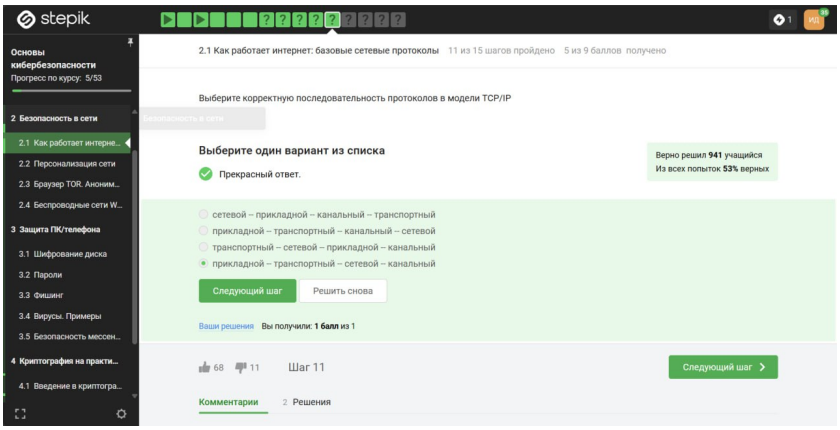

Рис. 2.5: Вопрос 2.1.5

Протокол http передает не зашифрованные данные, а протокол https уже будет передавать зашифрованные данные (рис. [2.6]).

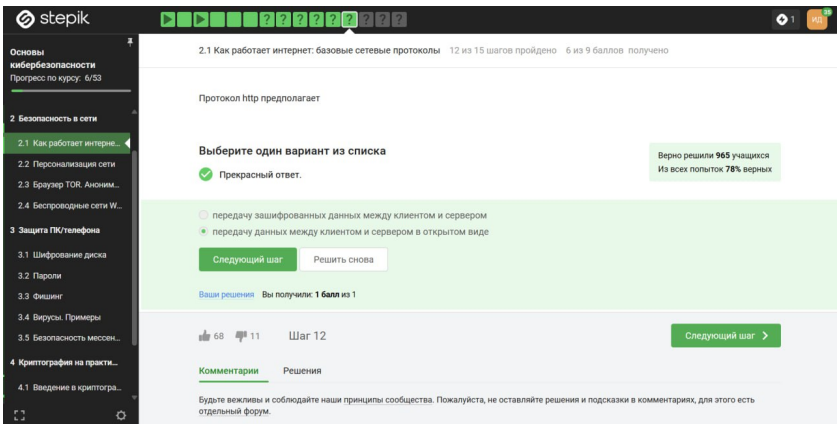

Рис. 2.6: Вопрос 2.1.6

Во-первых, https передает зашифрованные данные, а следовательно, одна из фаз - передача данных, другая должна быть рукопожатием (рис. [2.7]).

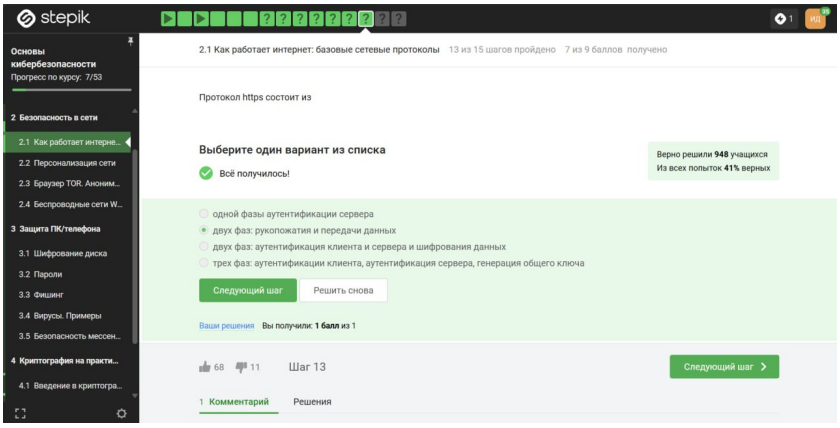

Рис. 2.7: Вопрос 2.1.7

TLS определяется и клиентом, и сервером, чтобы было возможно подключиться (рис. [2.8]).

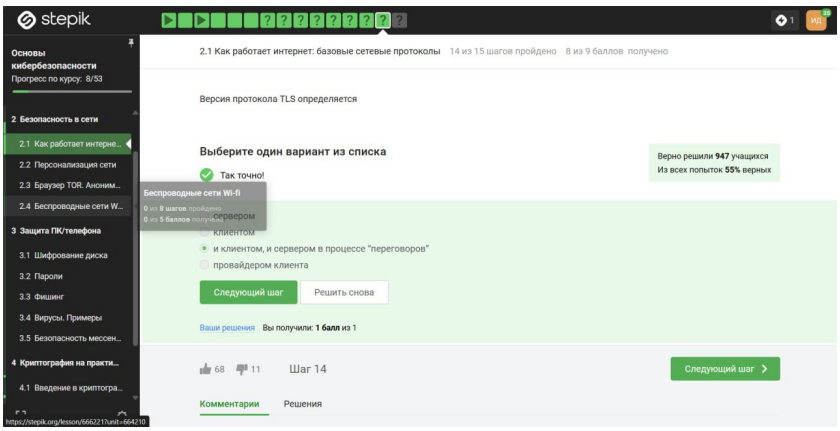

Рис. 2.8: Вопрос 2.1.8

В ходе TLS-рукопожатия клиент и сервер вместе выполняют следующие действия:

- Указывают, какую версию TLS (TLS 1.0, 1.2, 1.3 и т. д.) они будут использовать
- Решают, какие наборы шифров (см. ниже) они будут использовать
- Проверяют подлинность сервера с помощью открытого ключа сервера и цифровой подписи центра сертификации SSL.
- Генерируют сеансовые ключи, чтобы использовать симметричное шифрование после завершения рукопожатия Следовательно, вариант *шифрование* выбираем, он лишний (рис. [2.9]).

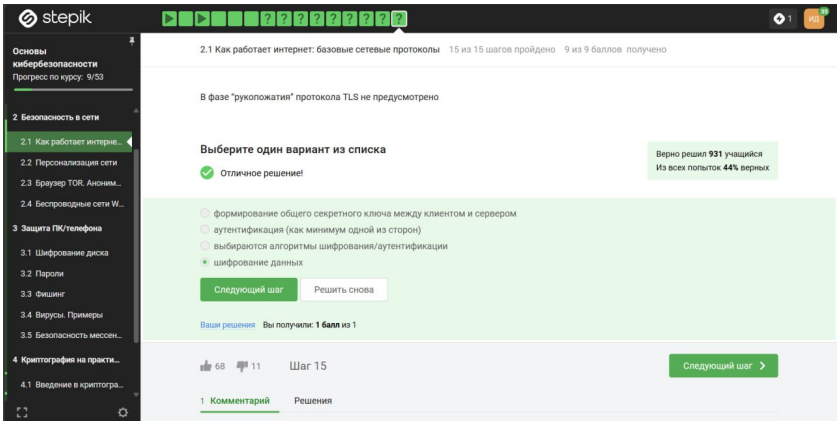

Рис. 2.9: Вопрос 2.1.9

2.2 Персонализация сети

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 (рис. [2.10]).

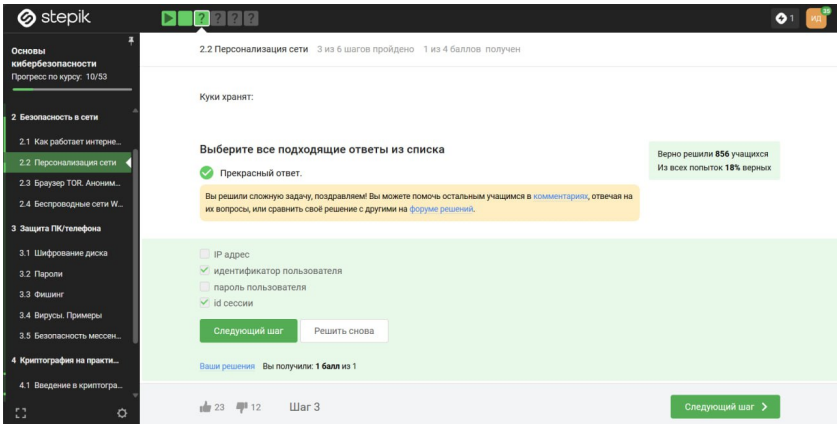

Рис. 2.10: Вопрос 2.2.1

Куки не делают соединение более надежным (рис. [2.11]).

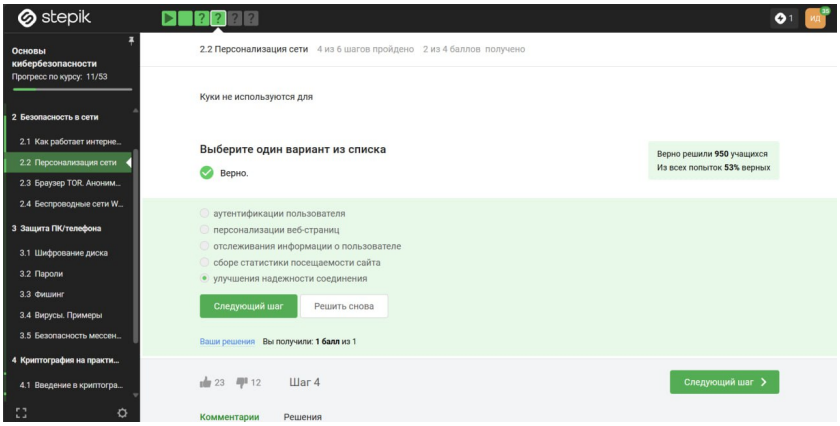

Рис. 2.11: Вопрос 2.2.2

Конечно же, куки генерируются сервером (рис. [2.12]).

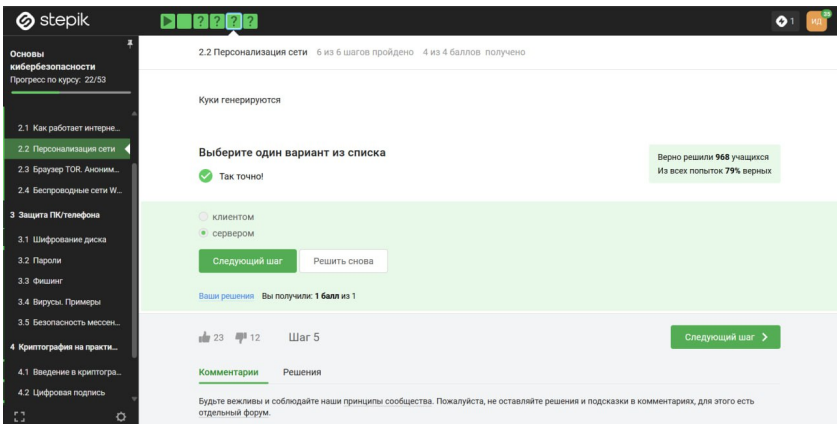

Рис. 2.12: Вопрос 2.2.3

Куки бывают сессионные; как правило, эти cookies используются при навигации на сайте и удаляются при закрытии окна браузера (рис. [2.13]).

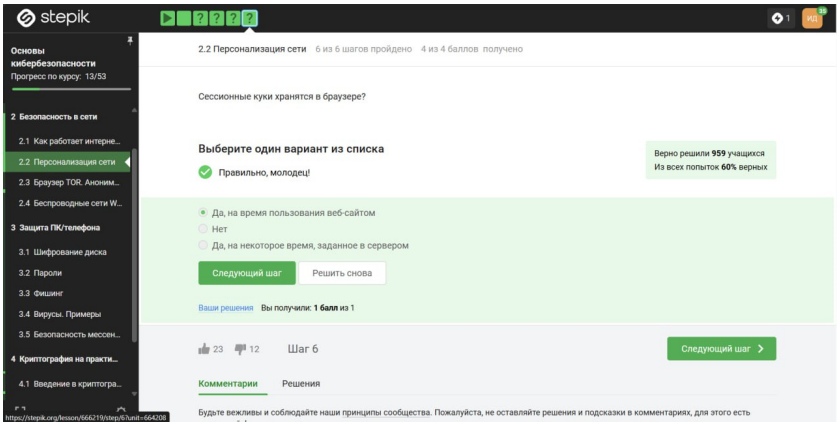

Рис. 2.13: Вопрос 2.2.4

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. [2.14]).

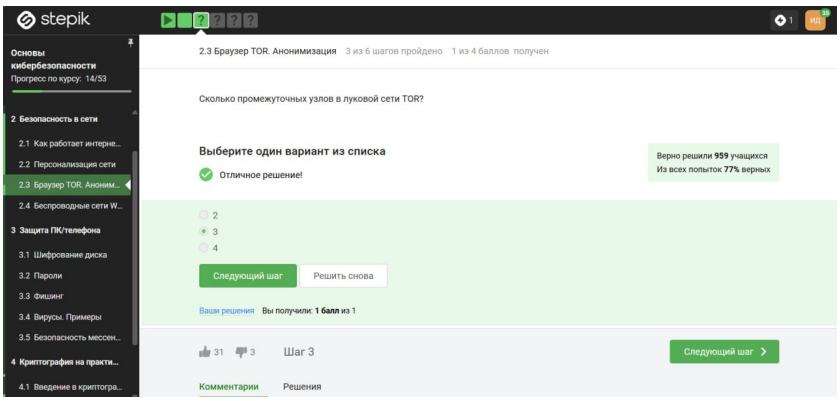

Рис. 2.14: Вопрос 2.3.1

IP-адрес не должен быть известен охранному и промежуточному узлам (рис. [2.15]).

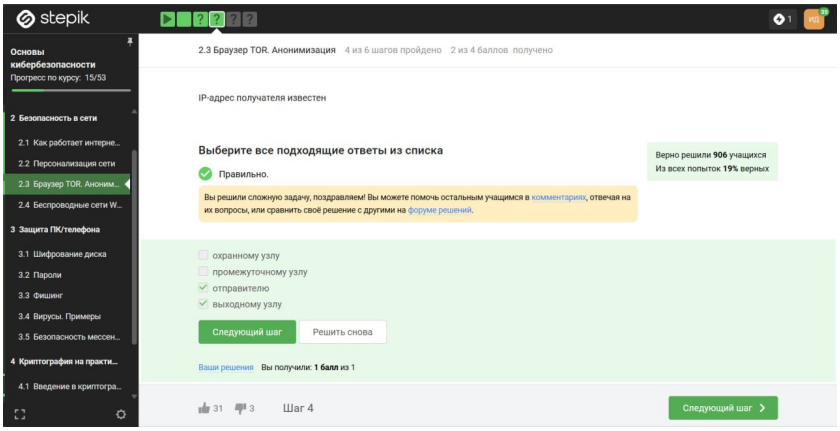

Рис. 2.15: Вопрос 2.3.2

Далее отправитель генерирует общие ключи с помощью определенного криптографического алгоритма, того же самого, который используется в TLS-протоколе. Он генерирует общие ключи последовательно с охранным узлом A, далее с промежуточным узлом B, а потом и с выходным узлом C (рис. [2.16]).

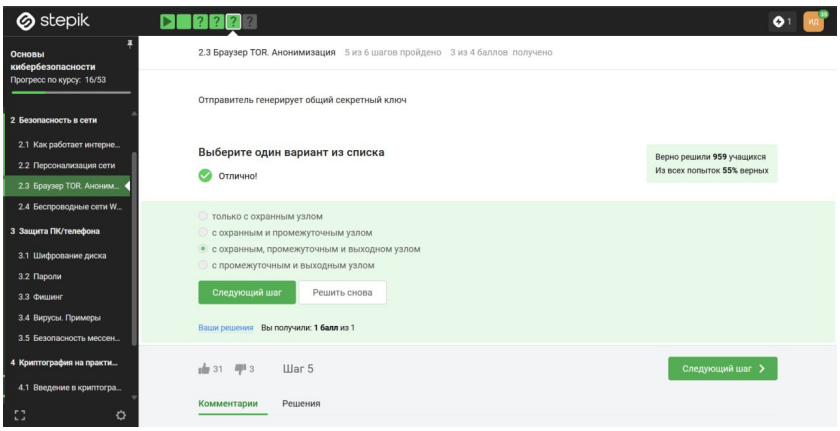

Рис. 2.16: Вопрос 2.3.3

Для получения пакетов не нужно использовать TOR. TOR — это технология, которая позволяет с некоторым успехом скрыть личность человека в интернете. Ну и напоследок, наверное, стоит отметить, что, конечно, у браузера Tor есть как и поклонники, которые пользуются им, так и люди, которые считают, что такая версия анонимизации не очень хорошая по разным причинам, например, потому, что так можно общаться не только с хорошими людьми, но и с плохими. Тут уже каждый выбирает сам для себя, насколько это хорошая идея - иметь такую анонимную сеть или нет (рис. [2.17]).

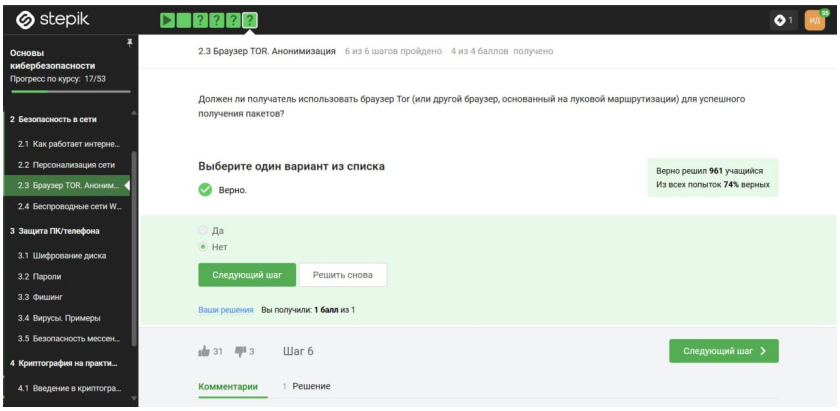

Рис. 2.17: Вопрос 2.3.4

2.4 Беспроводные сети Wi-fi

WiFi - это технология беспроводной локальной сети, она основана на стандарте IEEE 802.11 (рис. [2.18]).

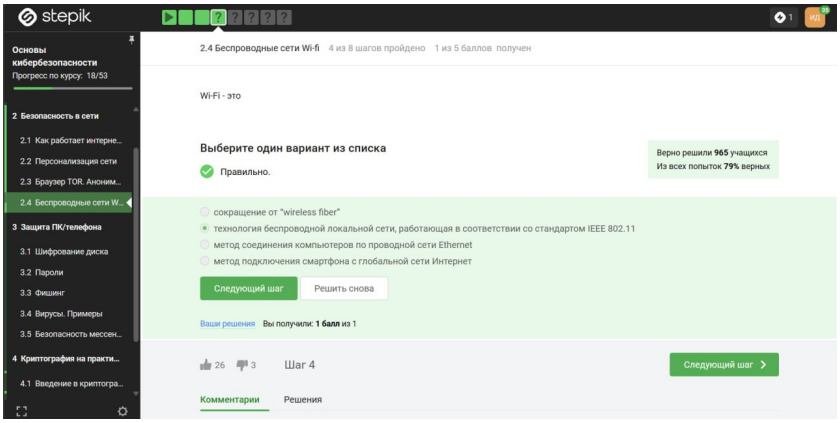

Рис. 2.18: Вопрос 2.4.1

WiFi работает на самом нижнем канальном уровне (рис. [2.19]).

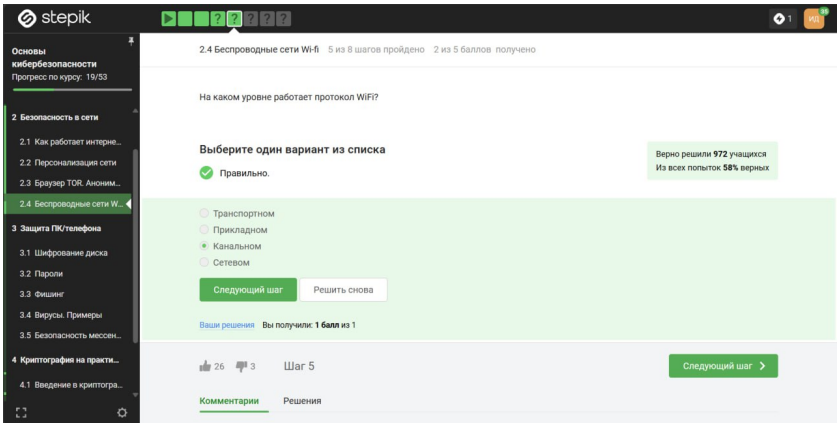

Рис. 2.19: Вопрос 2.4.2

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 (рис. [2.20]).

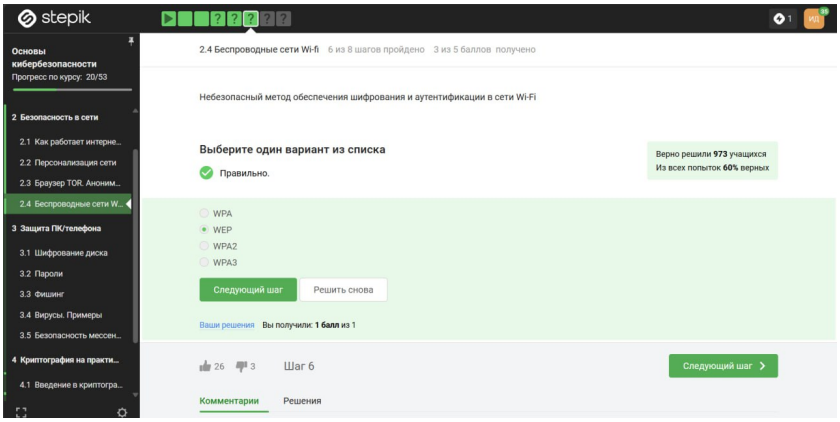

Рис. 2.20: Вопрос 2.4.3

Лектор говорит: Поговорим все-таки о безопасности в сетях WiFi. Что я имею в виду под безопасностью? Я имею в виду передачу данных от устройства, будь это мобильный телефон или компьютер, к роутеру, к тому прибору, который подключен непосредственно к глобальной сети Интернет с помощью провода, и безопасность осуществляется на этом уровне с помощью шифрования и аутентификации (рис. [2.21]).

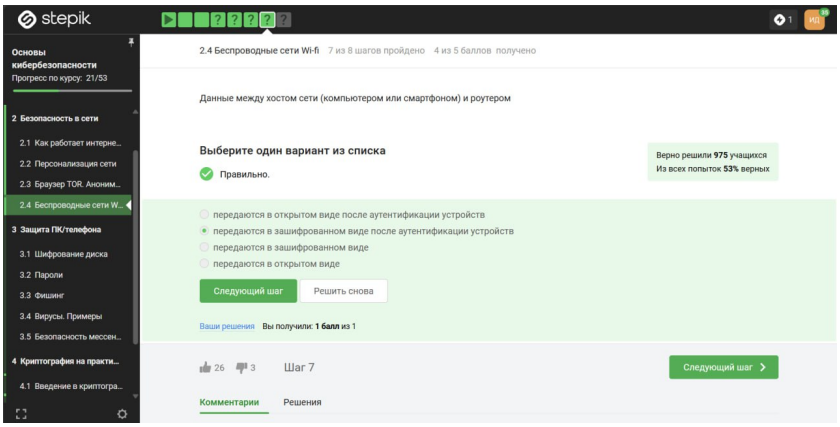

Рис. 2.21: Вопрос 2.4.4

Судя по названию, WPA2 Personal для личного использования, как раз для домашней сети, enterprise - для использования в коммерческих организациях

(рис. [2.22]).

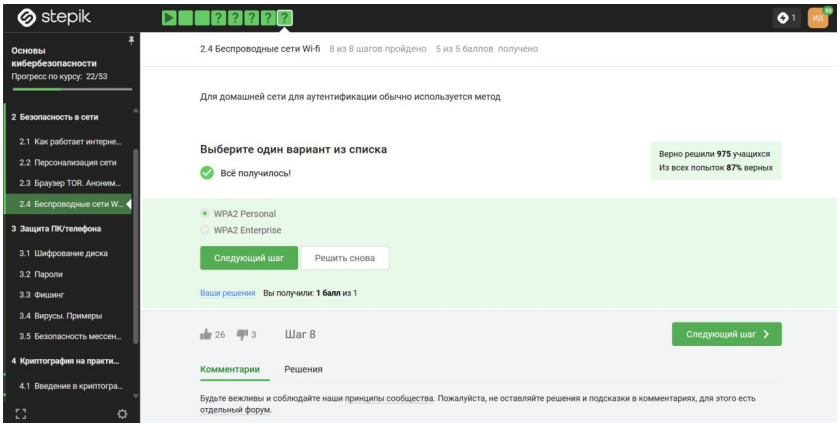

Рис. 2.22: Вопрос 2.4.5

3 Выводы

В результате выполнения блока “Безопасность в сети” я узнала, как работают базовые сетевые протоколы, куки-файлы, сети Wi-Fi и для чего предназначен браузер TOR.