Внешний курс. Блок 1: Безопасность в сети

Основы информационной безопасности

Швецов Михаил Романович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Выполнение контрольных заданий первого блока внешнего курса “Основы Кибербезопасности”

2 Выполнение заданий блока “Основы Кибербезопасности”

2.1 Как работает интернет: базовые сетевые протоколы

UDP - протокол сетевого уровня TCP - протокол транспортного уровня HTTPS - протокол прикладного уровня IP - протокол сетевого уровня, поэтому ответ HTTPS (рис. 2.1).

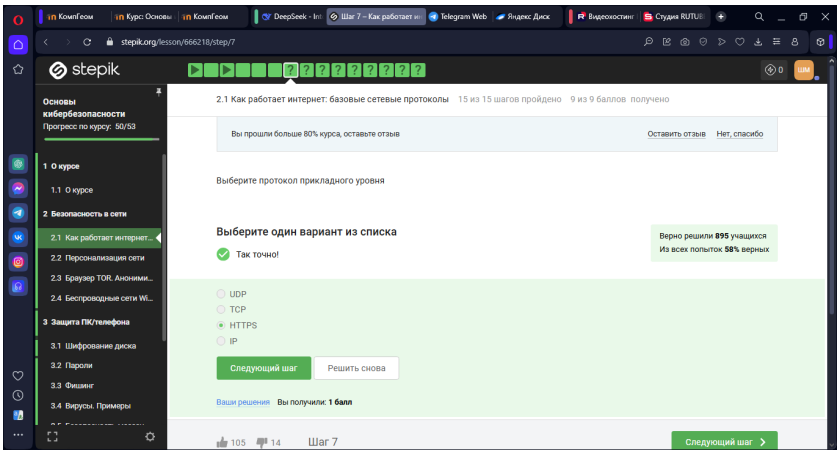

Рис. 2.1: Вопрос 2.1.1

Ранее было упомянуто, что протокол TCP - transmission control protocol - работает на транспортном уровне (рис. 2.2).

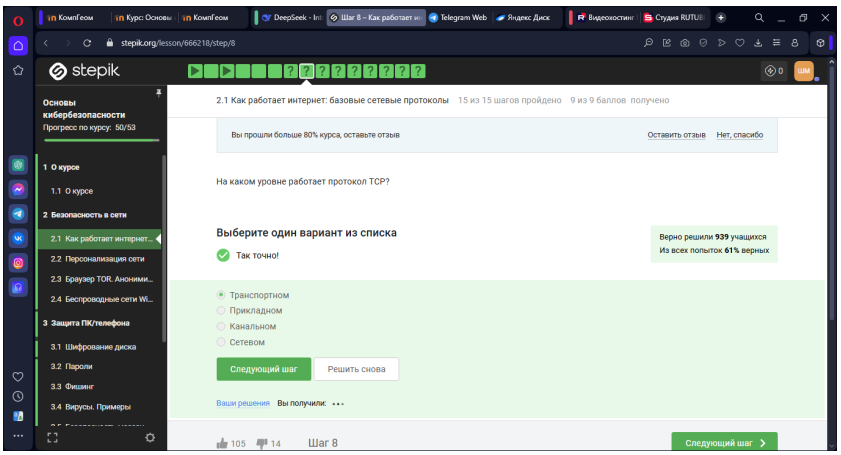

Рис. 2.2: Вопрос 2.1.2

В адресе типа IPv4 не может быть чисел больше 255, поэтому первые два варианта не подходят (рис. 2.3).

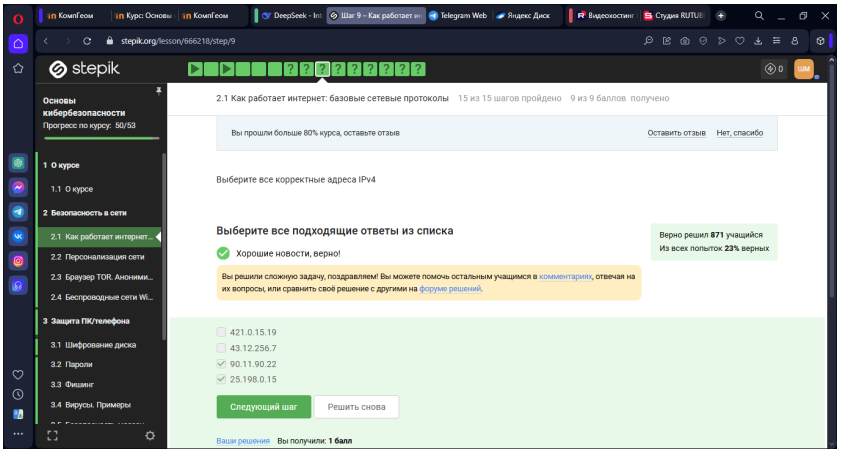

Рис. 2.3: Вопрос 2.1.3

DNS-сервер, Domain name server — приложение, предназначенное для ответов на DNS-запросы по соответствующему протоколу Обязательное условие – Сопоставление сервером доменных имен доменного имени с IP-адресом называется разрешением имени и адреса (рис. 2.4).

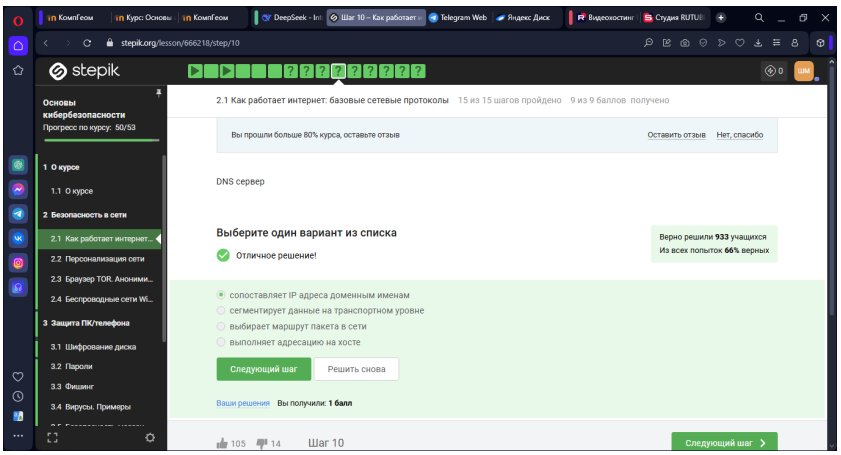

Рис. 2.4: Вопрос 2.1.4

Распределение 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).

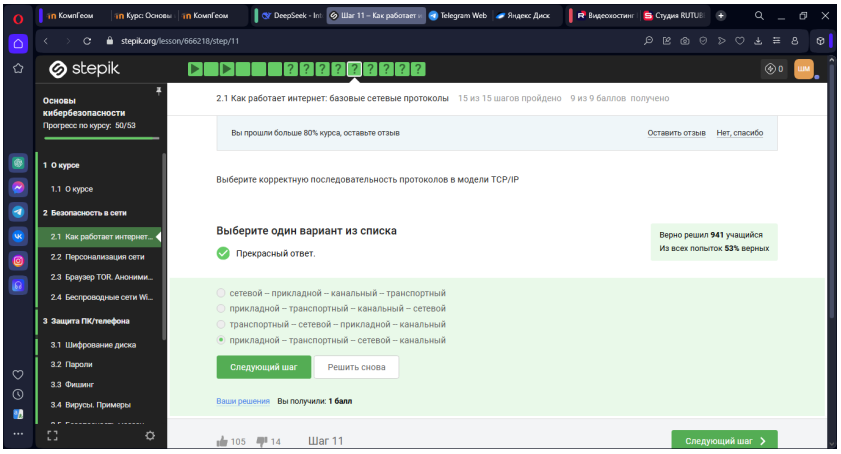

Рис. 2.5: Вопрос 2.1.5

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

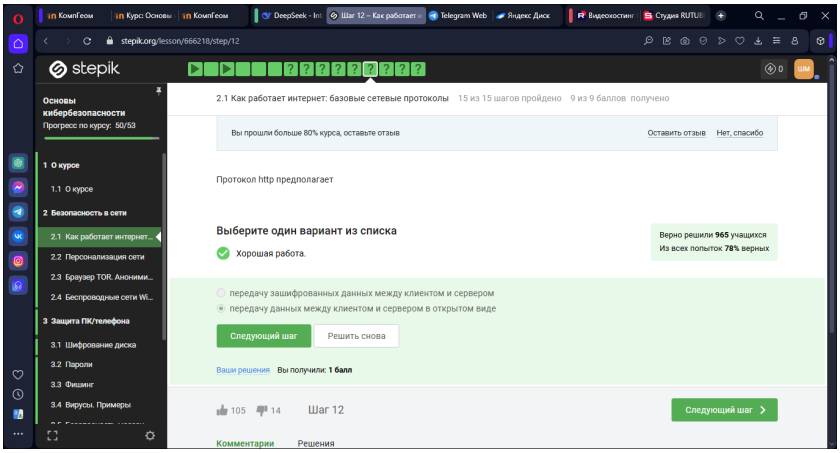

Рис. 2.6: Вопрос 2.1.6

https передает зашифрованные данные, одна из фаз - передача данных, другая должна быть рукопожатием (рис. 2.7).

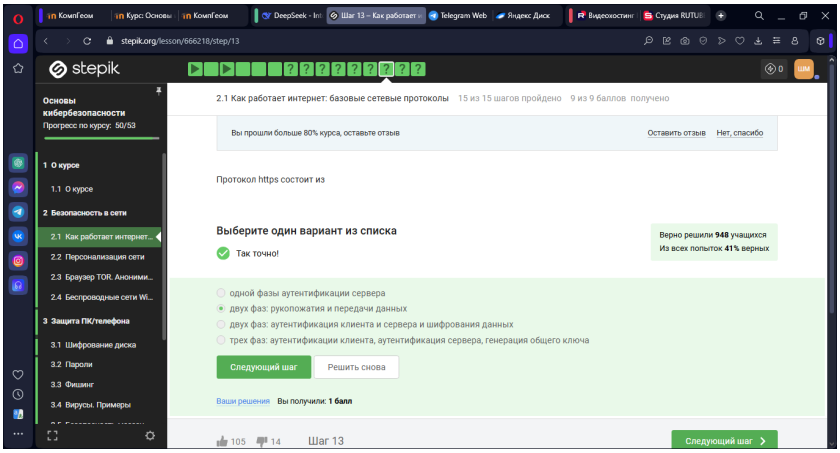

Рис. 2.7: Вопрос 2.1.7

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

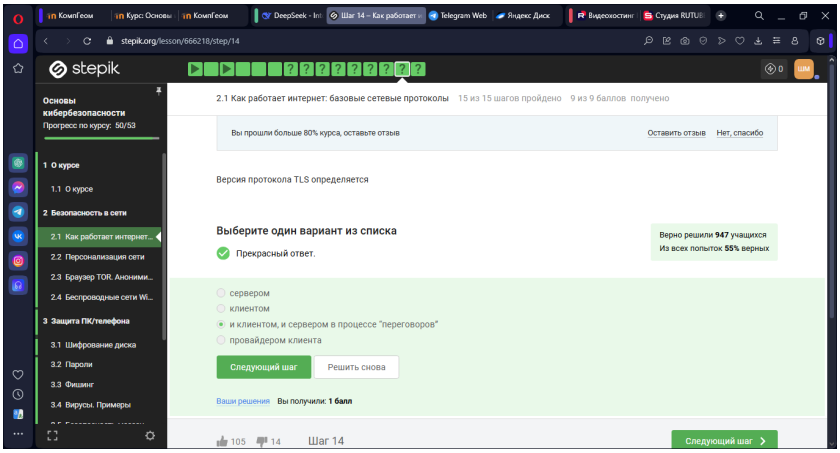

Рис. 2.8: Вопрос 2.1.8

Ответ на изобрадении, остальные варианты в протоколе предусмотрены (рис. **??**).

Вопрос 2.1.9

2.2 Персонализация сети

Куки точно не хранят пароли и IP-адреса, а id сессии и идентификатор хранят (рис. 2.9).

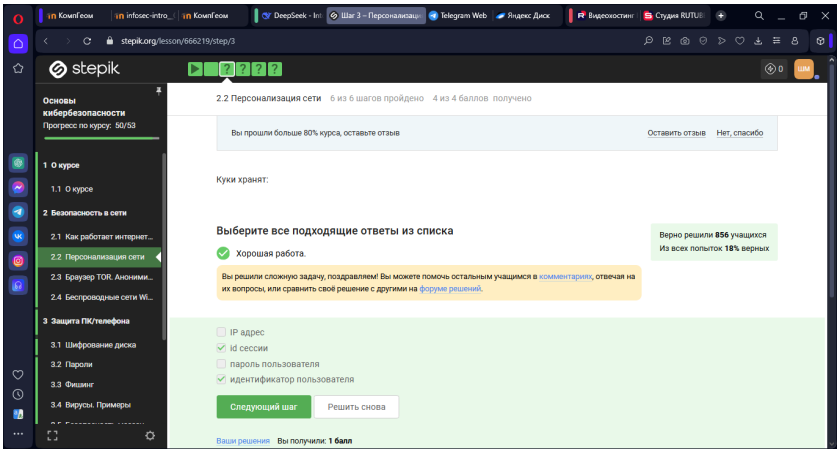

Рис. 2.9: Вопрос 2.2.1

Конечно же, куки не делают соединение более надежным (рис. 2.10).

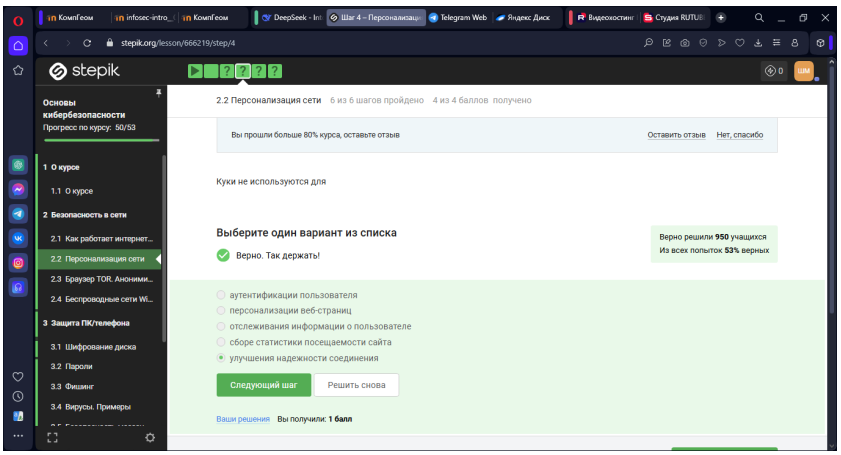

Рис. 2.10: Вопрос 2.2.2

Ответ на изображении (рис. 2.11).

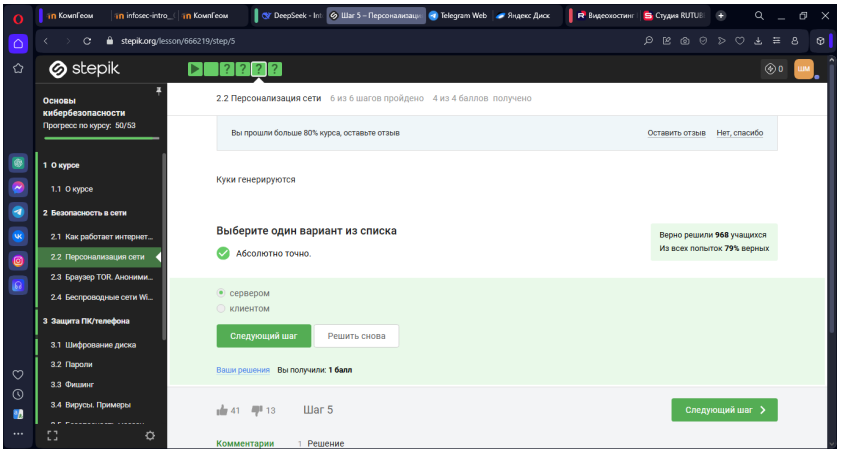

Рис. 2.11: Вопрос 2.2.3

Сессионные куки хранятся в течение сессии, то есть пока используется веб-сайт (рис. 2.12).

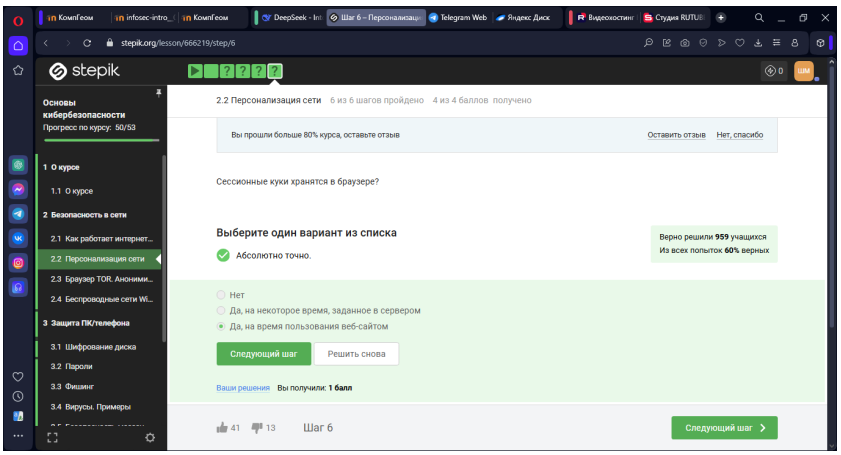

Рис. 2.12: Вопрос 2.2.4

2.3 Браузер TOR. Анонимизация

Необходимо три узла - входной, промежуточный и выходной (рис. 2.13).

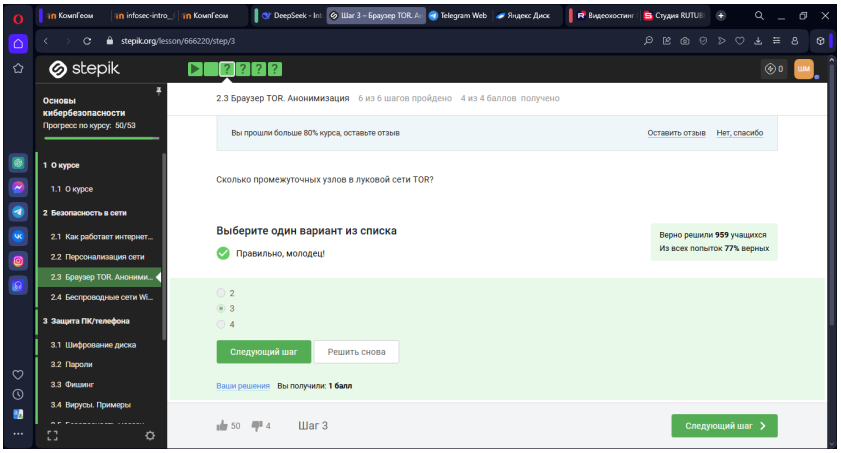

Рис. 2.13: Вопрос 2.3.1

IP-адрес не должен быть известен охранному и промежуточному узлам (рис. 2.14).

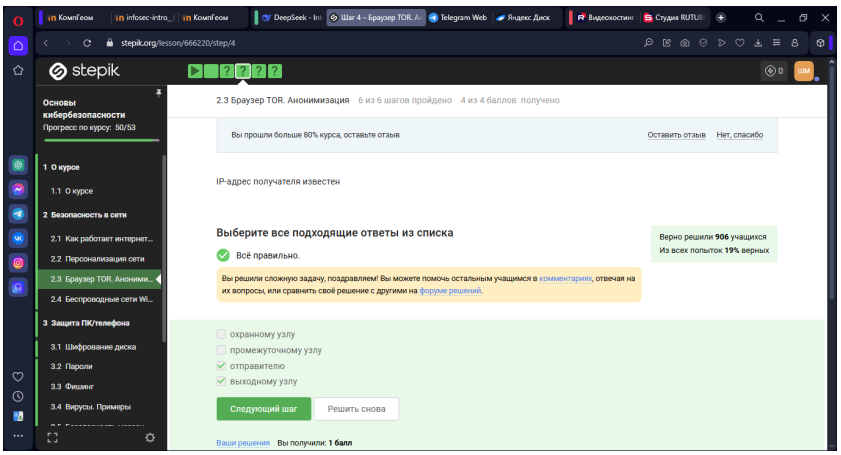

Рис. 2.14: Вопрос 2.3.2

Отправитель генерирует общий секретный ключ со узлами, через которые идет передача, то есть со всеми (рис. 2.15).

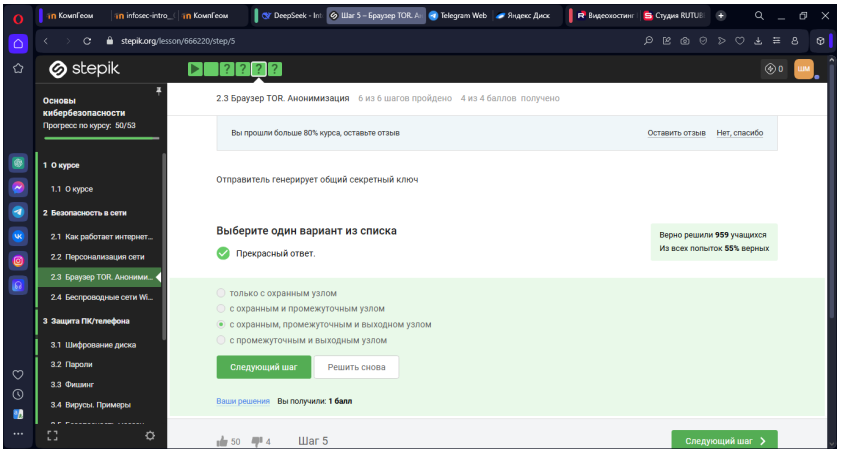

Рис. 2.15: Вопрос 2.3.3

Для получаения пакетов не нужно использовать TOR. TOR — это технология, которая позволяет с некоторым успехом скрыть личность человека в интернете (рис. 2.16).

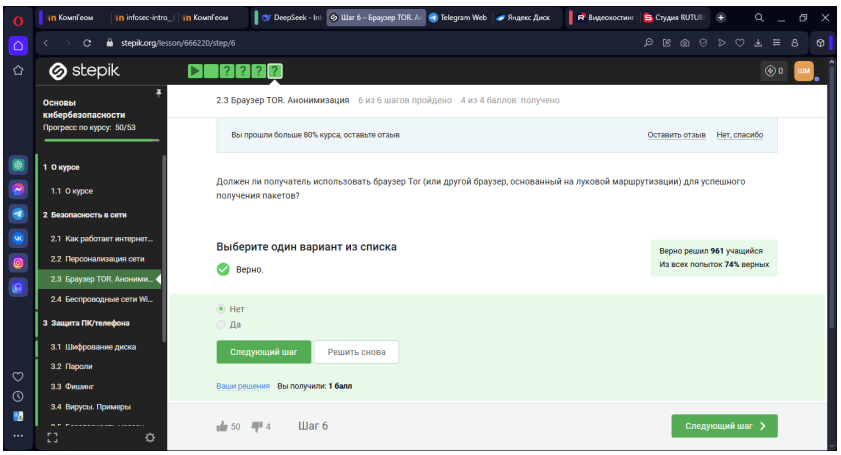

Рис. 2.16: Вопрос 2.3.4

2.4 Беспроводные сети Wi-fi

Действительно, это определение Wi-Fi (рис. 2.17).

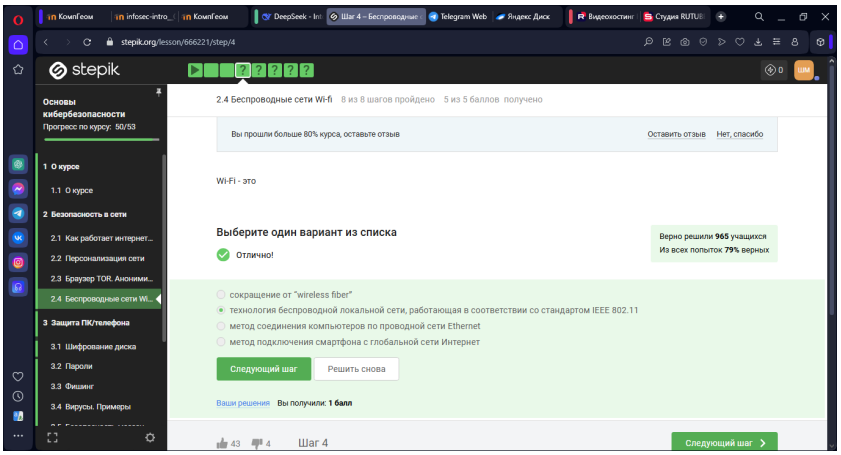

Рис. 2.17: Вопрос 2.4.1

Для целей работы в Интернете Wi-Fi обычно располагается как канальный уровень (эквивалентный физическому и канальному уровням модели OSI) ниже интернет-уровня интернет-протокола. Это означает, что узлы имеют связанный интернет-адрес, и при подходящем подключении это обеспечивает полный доступ в Интернет. (рис. 2.18).

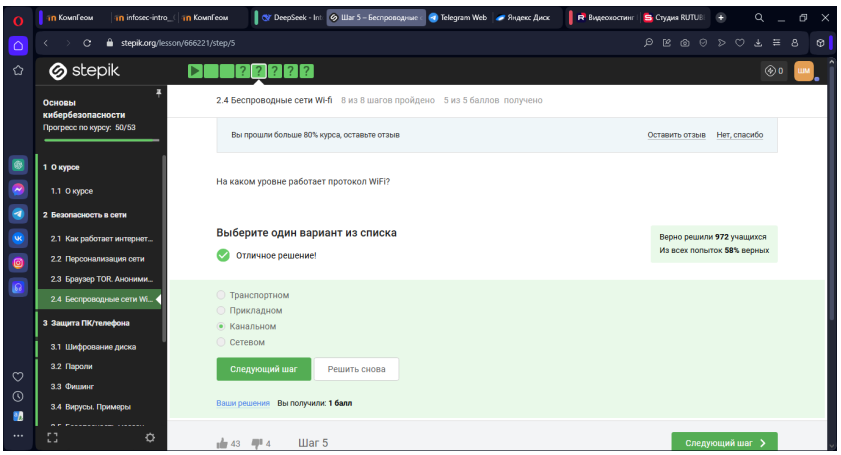

Рис. 2.18: Вопрос 2.4.2

WEP (Wired Equivalent Privacy) – устаревший и небезопасный метод проверки подлинности. Это первый и не очень удачный метод защиты. Злоумышленники без проблем получают доступ к беспроводным сетям, которые защищены с помощью WEP, был заменен остальными представленными (рис. 2.19).

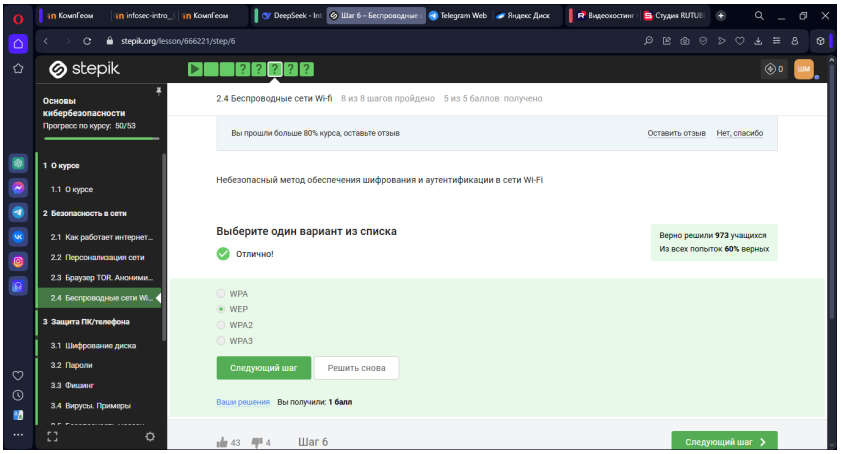

Рис. 2.19: Вопрос 2.4.3

Нужно аутентифицировать устройства и позже передаются зашифрованные данные (рис. 2.20).

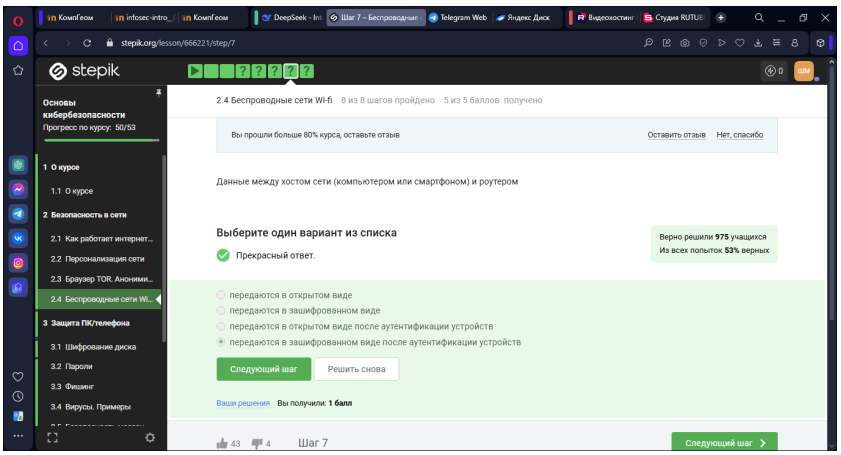

Рис. 2.20: Вопрос 2.4.4

В целом, понятно по названию, что WPA2 Personal для личного использования, то есть для домашней сети, enterprise - для предпиятий (рис. 2.21).

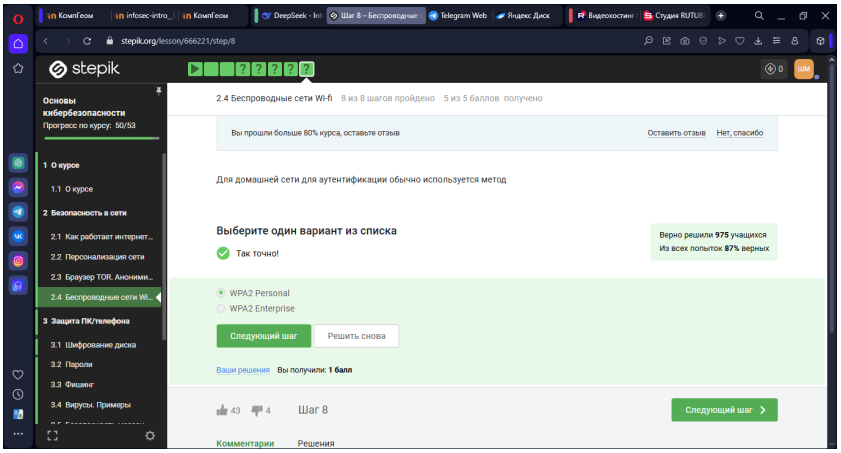

Рис. 2.21: Вопрос 2.4.5

3 Выводы

В ходе выполнения блока “Безопасность в сети” узнала о работе базовых сетевых протоколов, куки сетей Wi-Fi и браузера TOR.