

Внешний курс. Этап 1: Введение в Linux

Скворцова Анастасия Дмитриевна

Содержание

| | | |
|---|------------------|---|
| 1 | Цель работы..... | 2 |
|---|------------------|---|

| | | |
|-----|---|----|
| 2 | Выполнение заданий блока “Основы Кибербезопасности” | 3 |
| 2.1 | Как работает интернет: базовые сетевые протоколы..... | 3 |
| 2.2 | Персонализация сети | 7 |
| 2.3 | Браузер TOR. Анонимизация | 9 |
| 2.4 | Беспроводные сети Wi-fi..... | 12 |
| 3 | Выводы..... | 14 |

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. 1).

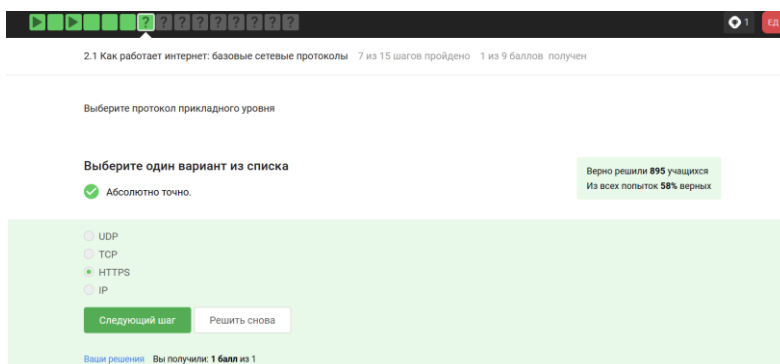


Рис. 1: Вопрос 2.1.1

Ранее было упомянуто, что протокол TCP - transmission control protocol - работает на транспортном уровне (рис. 2).

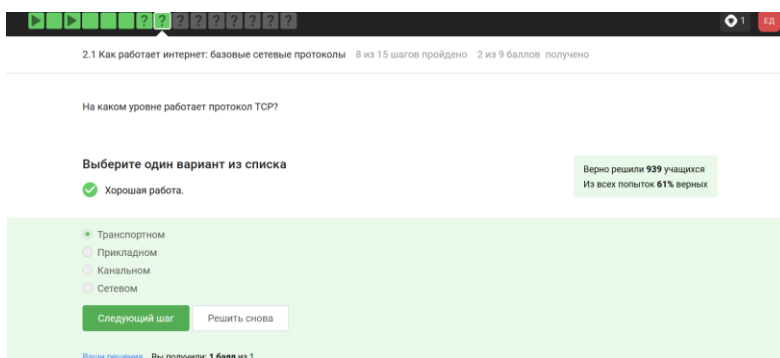


Рис. 2: Вопрос 2.1.2

В адресе типа IPv4 не может быть чисел больше 255, поэтому первые два варианта не подходят (рис. 3).

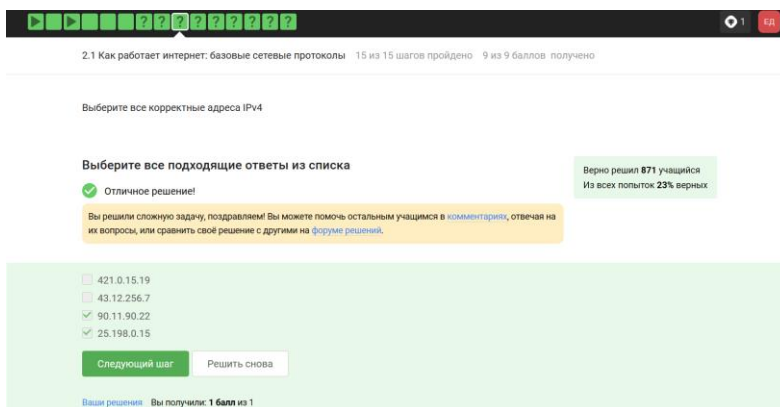


Рис. 3: Вопрос 2.1.3

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. 4).

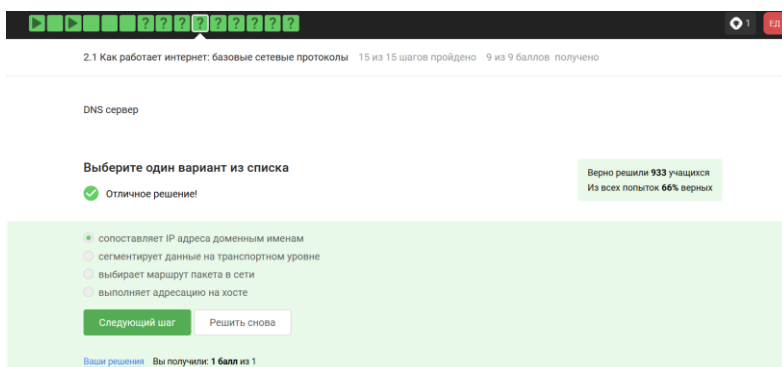


Рис. 4: Вопрос 2.1.4

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. 5).

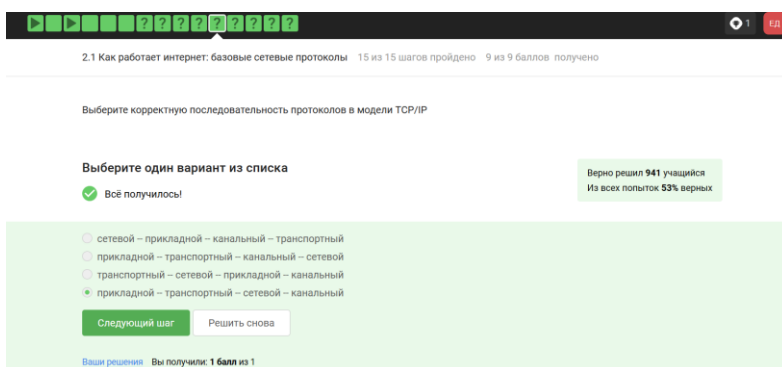


Рис. 5: Вопрос 2.1.5

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

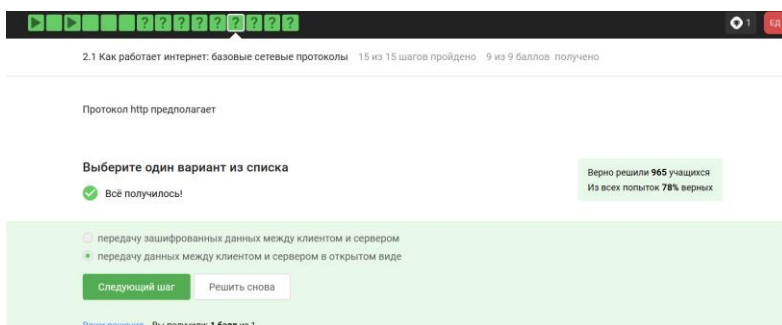
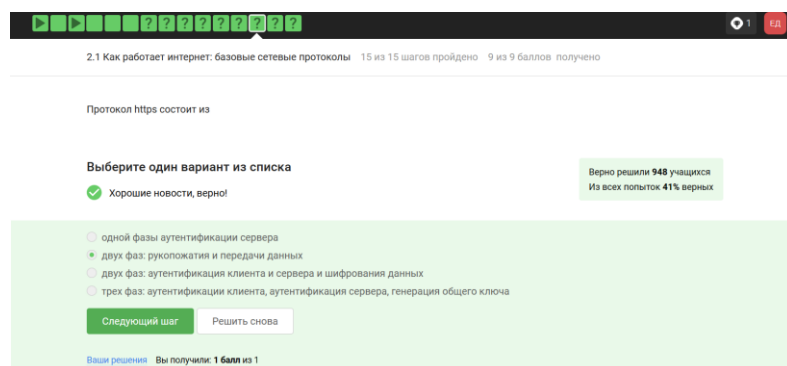


Рис. 6: Вопрос 2.1.6

https передает зашифрованные данные, одна из фаз - передача данных, другая должна быть рукопожатием (рис. 7).



2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено 9 из 9 баллов получено

Протокол https состоит из

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 948 учащихся
Из всех попыток 41% верных

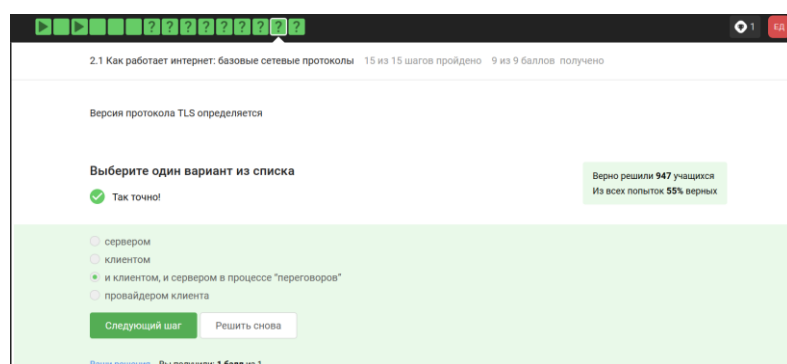
- ☐ одной фазы аутентификации сервера
- ☒ двух фаз: рукопожатия и передачи данных
- ☐ двух фаз: аутентификация клиента и сервера и шифрования данных
- ☐ трех фаз: аутентификация клиента, аутентификация сервера, генерации общего ключа

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 7: Вопрос 2.1.7

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



2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено 9 из 9 баллов получено

Версия протокола TLS определяется

Выберите один вариант из списка

✓ Так точно!

Верно решили 947 учащихся
Из всех попыток 55% верных

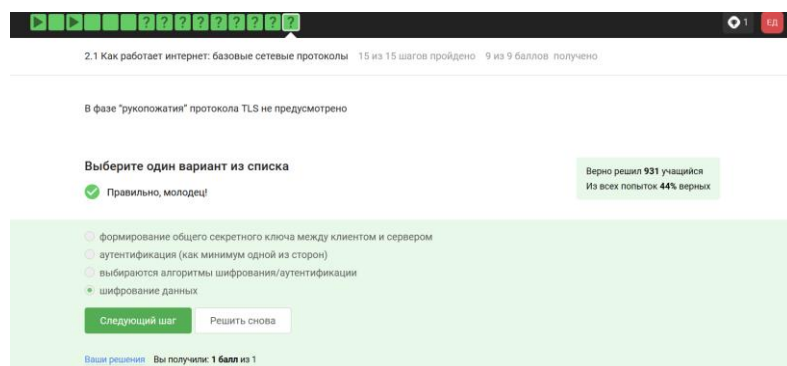
- ☐ сервером
- ☐ клиентом
- ☒ и клиентом, и сервером в процессе "переговоров"
- ☐ провайдером клиента

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 8: Вопрос 2.1.8

Ответ на изображении, остальные варианты в протоколе предусмотрены (рис. 9).



2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено 9 из 9 баллов получено

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решил 931 учащихся
Из всех попыток 44% верных

- ☐ формирование общего секретного ключа между клиентом и сервером
- ☐ аутентификация (как минимум одной из сторон)
- ☐ выбираются алгоритмы шифрования/аутентификации
- ☒ шифрование данных

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 9: Вопрос 2.1.9

2.2 Персонализация сети

Куки точно не хранят пароли и IP-адреса, а id сессии и идентификатор хранят (рис. 10).

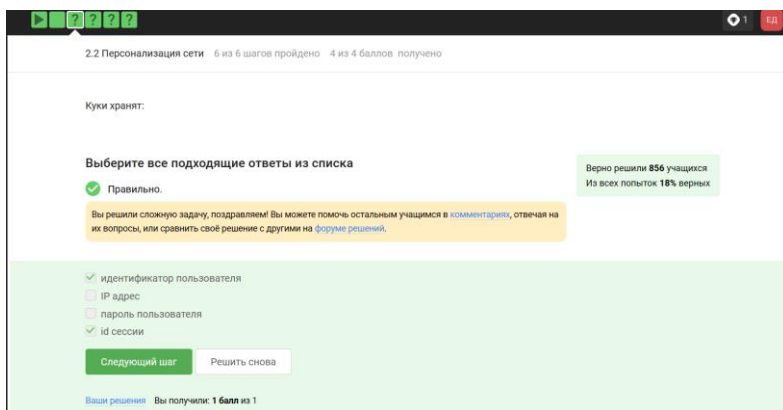


Рис. 10: Вопрос 2.2.1

Конечно же, куки не делают соединение более надежным (рис. 11).

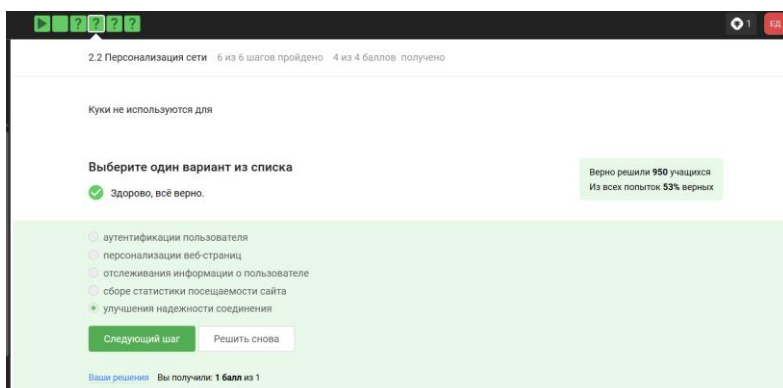


Рис. 11: Вопрос 2.2.2

Ответ на изображении (рис. 12).

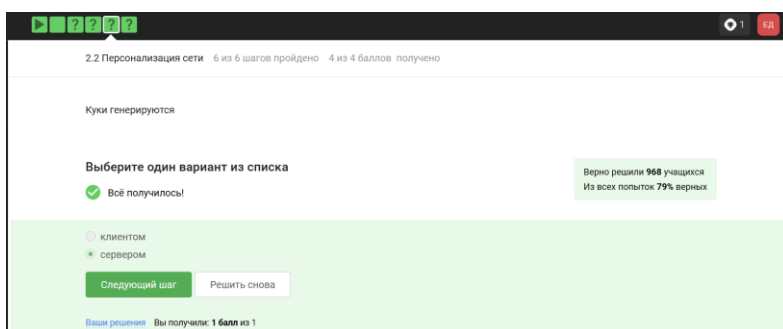


Рис. 12: Вопрос 2.2.3

Сессионные куки хранятся в течение сессии, то есть пока используется веб-сайт (рис. 13).

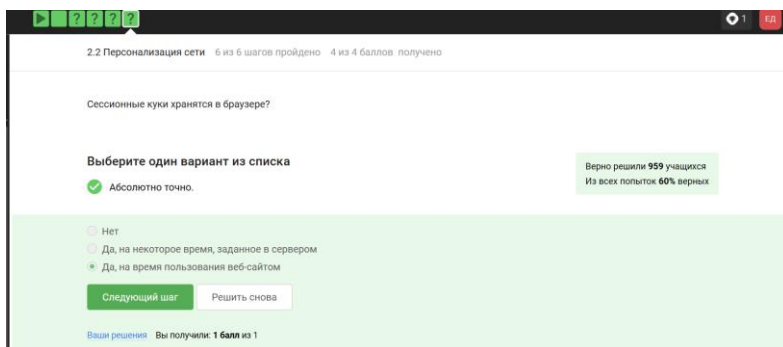
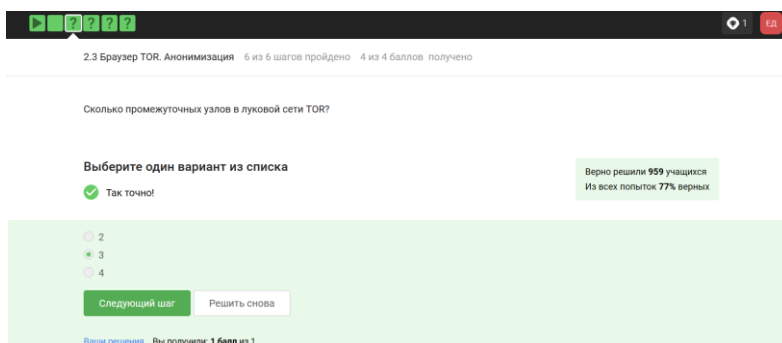


Рис. 13: Вопрос 2.2.4

2.3 Браузер TOR. Анонимизация

Необходимо три узла - входной, промежуточный и выходной (рис. 14).



2.3 Браузер TOR. Анонимизация 6 из 6 шагов пройдено 4 из 4 баллов получено

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

✓ Так точно!

Верно решили 959 учащихся
Из всех попыток 77% верных

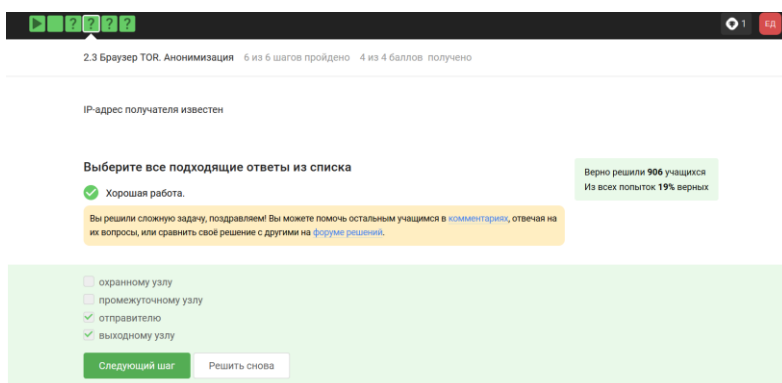
☐ 2
☒ 3
☐ 4

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл из 1

Рис. 14: Вопрос 2.3.1

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



2.3 Браузер TOR. Анонимизация 6 из 6 шагов пройдено 4 из 4 баллов получено

IP-адрес получателя известен

Выберите все подходящие ответы из списка

✓ Хорошая работа.

Верно решили 906 учащихся
Из всех попыток 19% верных

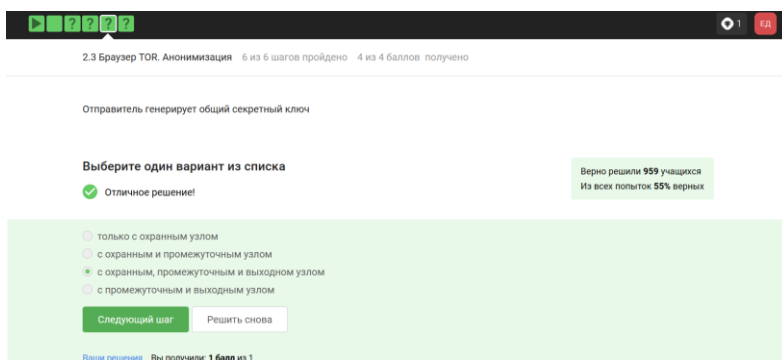
Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить своё решение с другими на форуме решений.

☐ охранному узлу
☐ промежуточному узлу
☒ отправителю
☒ выходному узлу

Следующий шаг Решить снова

Рис. 15: Вопрос 2.3.2

Отправитель генерирует общий секретный ключ со узлами, через которые идет передача, то есть со всеми (рис. 16).



2.3 Браузер TOR. Анонимизация 6 из 6 шагов пройдено 4 из 4 баллов получено

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

✓ Отличное решение!

Верно решили 959 учащихся
Из всех попыток 55% верных

☐ только с охраным узлом
☐ с охраным и промежуточным узлом
☒ с охраным, промежуточным и выходным узлом
☐ с промежуточным и выходным узлом

Следующий шаг Решить снова

Ваше решение Вы получили: 1 балл из 1

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).

1

1/4

2.3 Браузер TOR. Анонимизация 6 из 6 шагов пройдено 4 из 4 баллов получено

Должен ли получатель использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов?

Выберите один вариант из списка

Да

Нет

Верно решил 961 учащийся
Из всех попыток 74% верных

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл из 1

Рис. 17: Вопрос 2.3.4

2.4 Беспроводные сети Wi-fi

Действительно, это определение Wi-Fi (рис. 18).

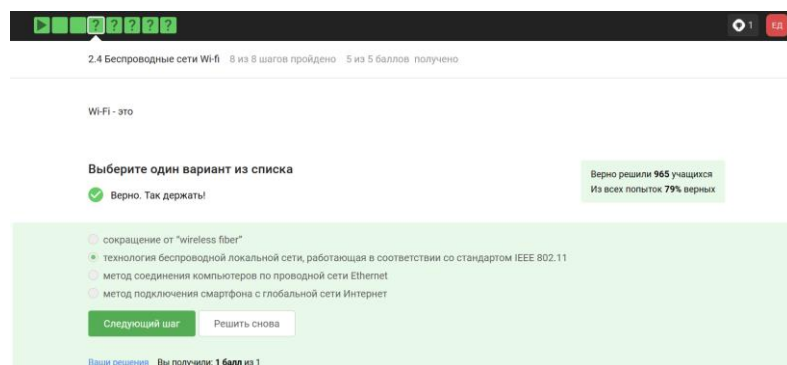


Рис. 18: Вопрос 2.4.1

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. 19).

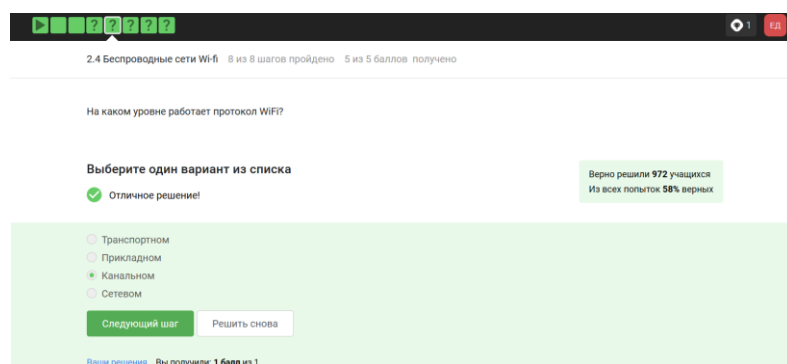


Рис. 19: Вопрос 2.4.2

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. 20).

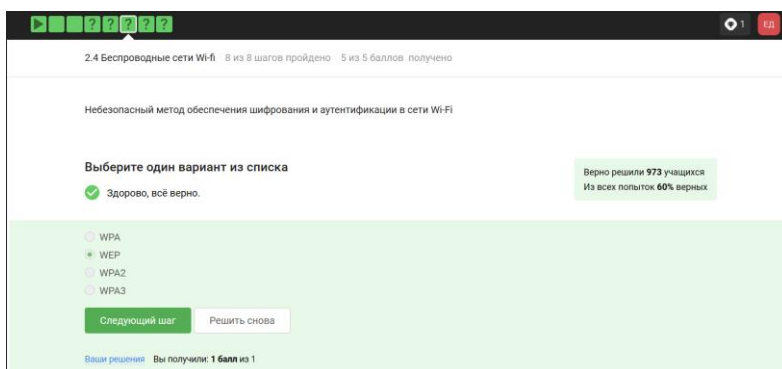


Рис. 20: Вопрос 2.4.3

Нужно аутентифицировать устройства и позже передаются зашифрованные данные (рис. 21).

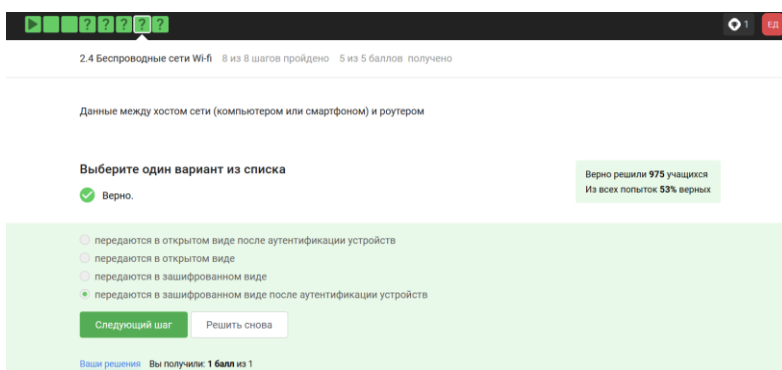


Рис. 21: Вопрос 2.4.4

В целом, понятно по названию, что WPA2 Personal для личного использования, то есть для домашней сети, enterprise - для предприятий (рис. 22).

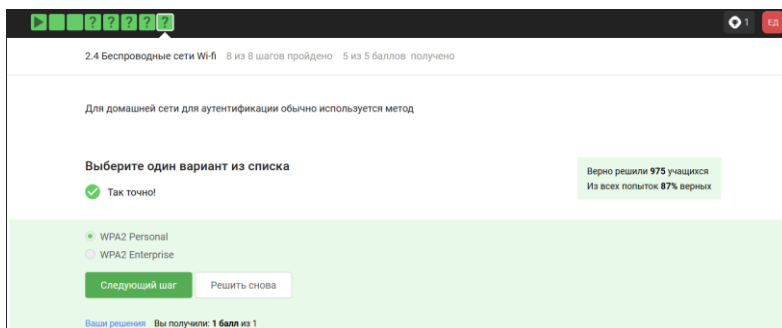


Рис. 22: Вопрос 2.4.5

3 Выводы

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