

Отчет о прохождении внешнего курса

1 этап

Симонова Полина Игоревна

Содержание

1 Цель работы	5
2 Задание	6
3 Теоретическое введение	7
4 Выполнение лабораторной работы	8
5 Выводы	20

Список иллюстраций

4.1	Задание 1	8
4.2	Задание 2	9
4.3	Задание 3	9
4.4	Задание 4	10
4.5	Задание 5	10
4.6	Задание 6	11
4.7	Задание 7	11
4.8	Задание 8	12
4.9	Задание 9	12
4.10	Задание 10	13
4.11	Задание 11	13
4.12	Задание 12	14
4.13	Задание 13	14
4.14	Задание 14	15
4.15	Задание 15	15
4.16	Задание 16	16
4.17	Задание 17	16
4.18	Задание 18	17
4.19	Задание 19	17
4.20	Задание 20	18
4.21	Задание 21	18
4.22	Задание 22	19

Список таблиц

1 Цель работы

Пройти внешний курс «Основы кибербезопасности» на платформе Stepik.
Получить начальные знания в сфере кибербезопасности.

2 Задание

Пройти все обучающие материалы, на их основе выполнить задания и тесты.

3 Теоретическое введение

Сетевой протокол - это некая последовательность правил, по которым, во-первых, устанавливается соединение между устройствами сети, то есть между роутером, и другими устройствами сети.

4 Выполнение лабораторной работы

Я выполняла первый модуль курса Основы кибербезопасности на стеке.

HTTPS - протокол прикладного уровня, в то время как IP - сетевого уровня, а UDP и TCP - протоколы транспортного уровня. (рис. 1)

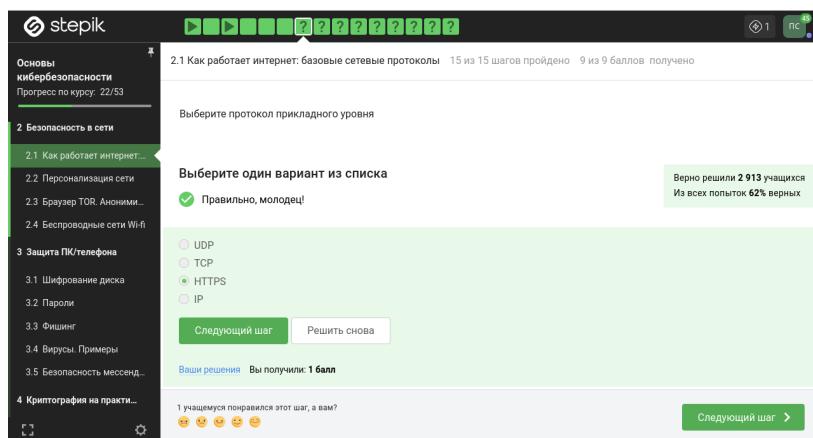


Рисунок 4.1: Задание 1

Как было замечено ранее, TCP - протокол транспортного уровня.(рис.2)

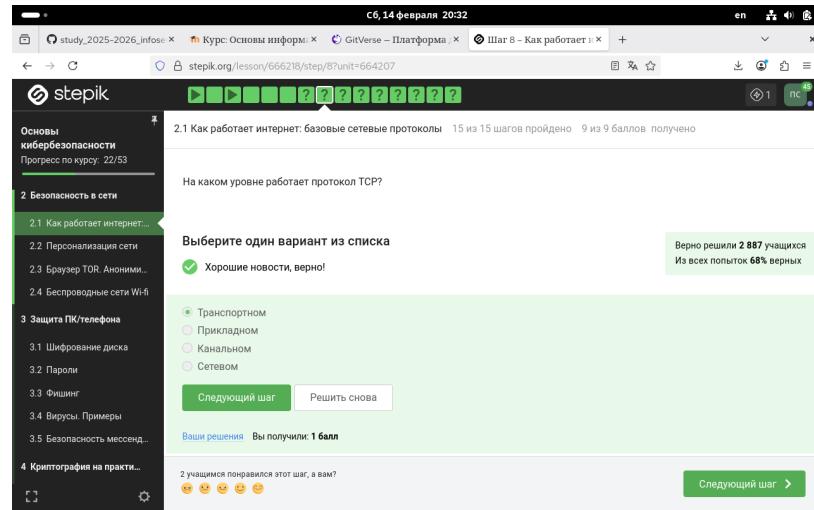


Рисунок 4.2: Задание 2

В стандарте IPv4 октеты не должны превышать 255. Нам подходят только 3 и 4 варианты ответаю (рис.3)

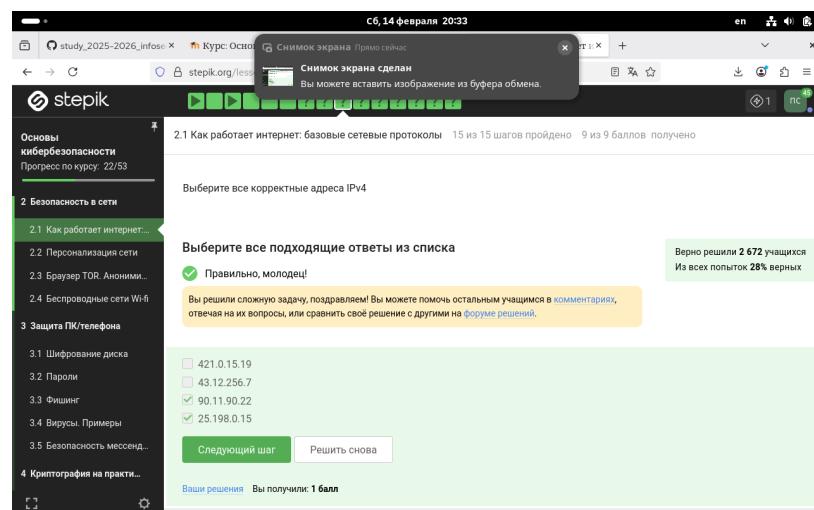


Рисунок 4.3: Задание 3

DNS используется для преобразования удобно читаемых доменных имен в айпи адреса. (рис.4)

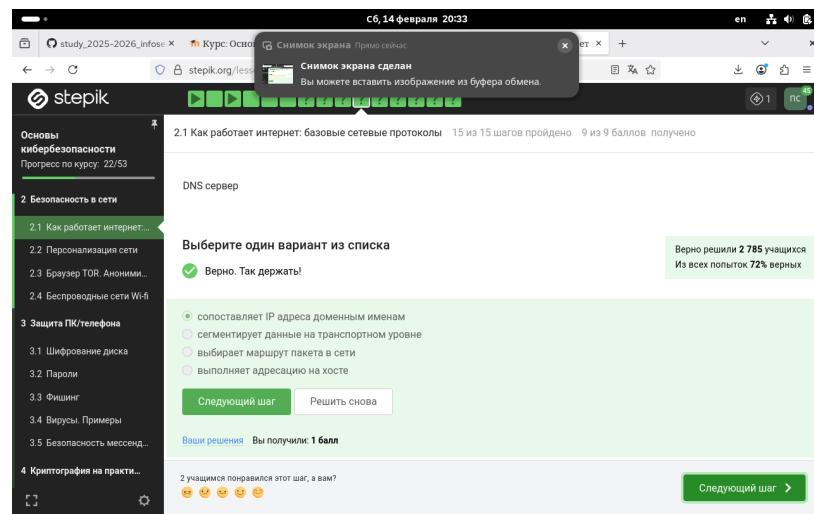


Рисунок 4.4: Задание 4

Правильная последовательность - прикладной, транспортный, сетевой, канальный. (рис. 5)

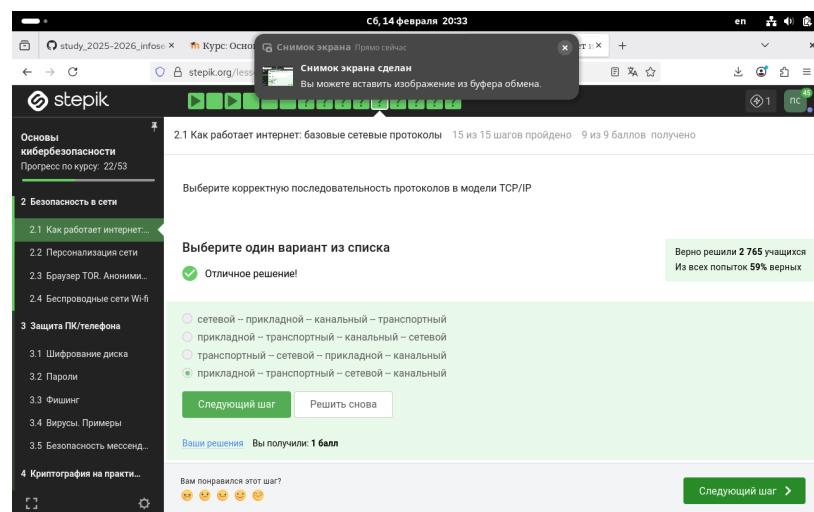


Рисунок 4.5: Задание 5

HTTP предполагает передачу данных в открытом виде, а HTTPS - использует шифрование. (рис.6)

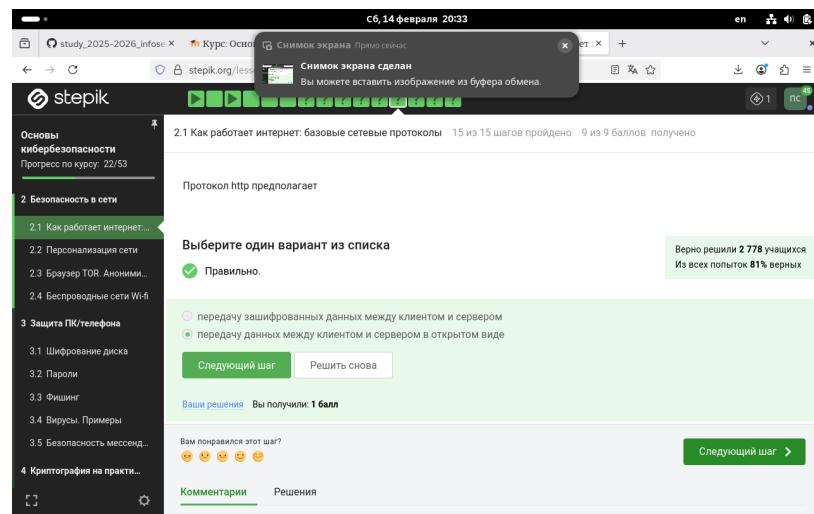


Рисунок 4.6: Задание 6

TLS работает поверх HTTPS, а в этом протоколе есть две фазы - рукопожатие и обмен данными (рис. 7)

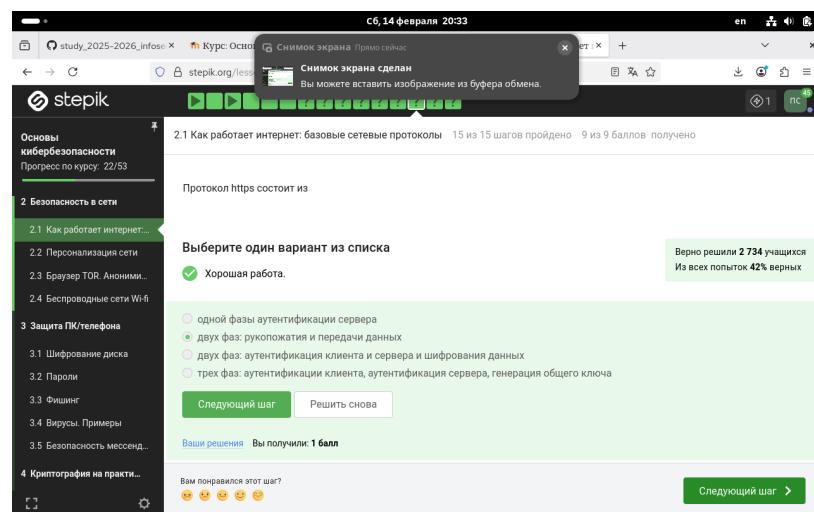


Рисунок 4.7: Задание 7

В TLS предлагаются несколько версий этого протокола, и в процессе переговоров выбирается наиболее удобная. (рис.8)

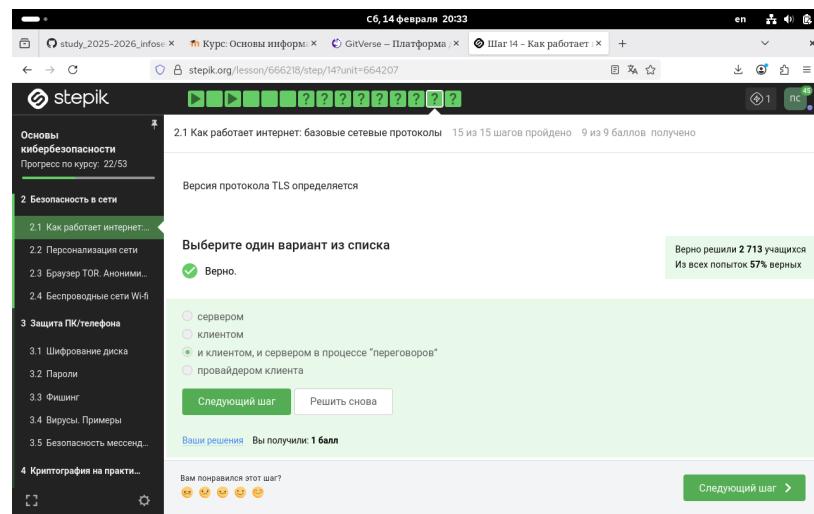


Рисунок 4.8: Задание 8

Шифрование в TLS предусмотрено уже после фазы рукопожатия, во время обмена анными непосредственно. (рис.9)

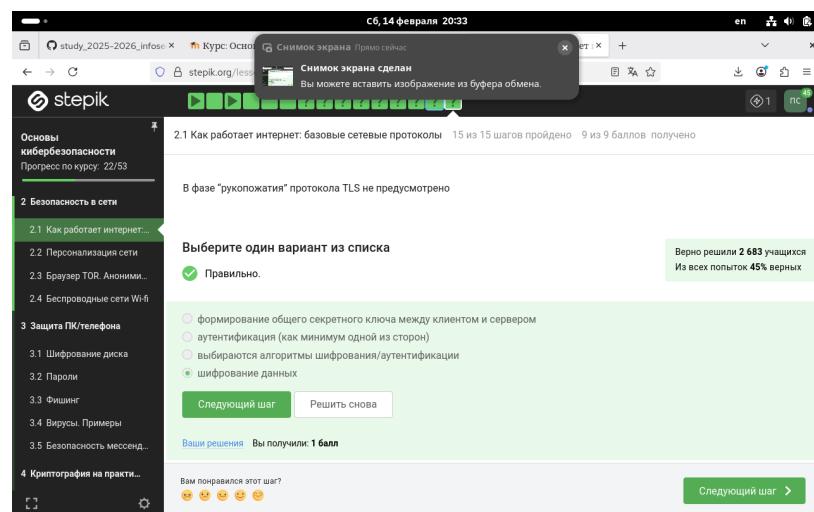


Рисунок 4.9: Задание 9

Куки не хранят ни пароль пользователя, ни его айпи адрес. (рис. 10)

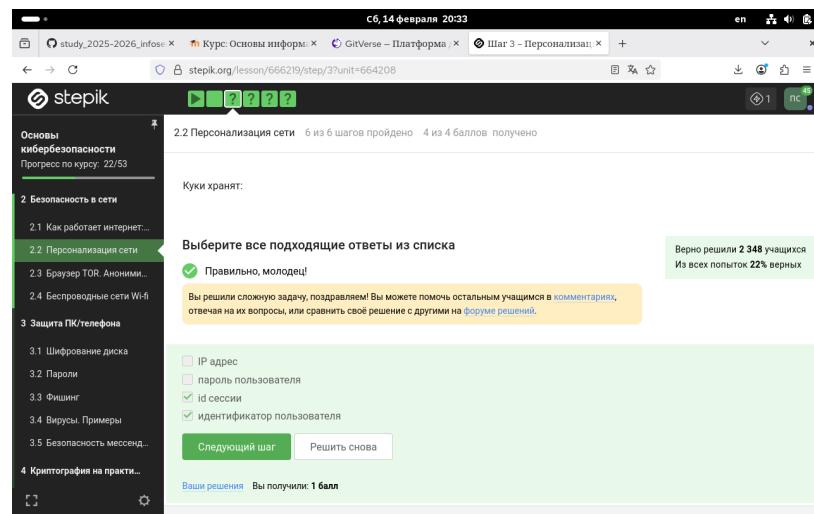


Рисунок 4.10: Задание 10

Куки используются в основном для персонализации сессий пользователя, но никак не для улучшения надежности соединения. (рис. 11)

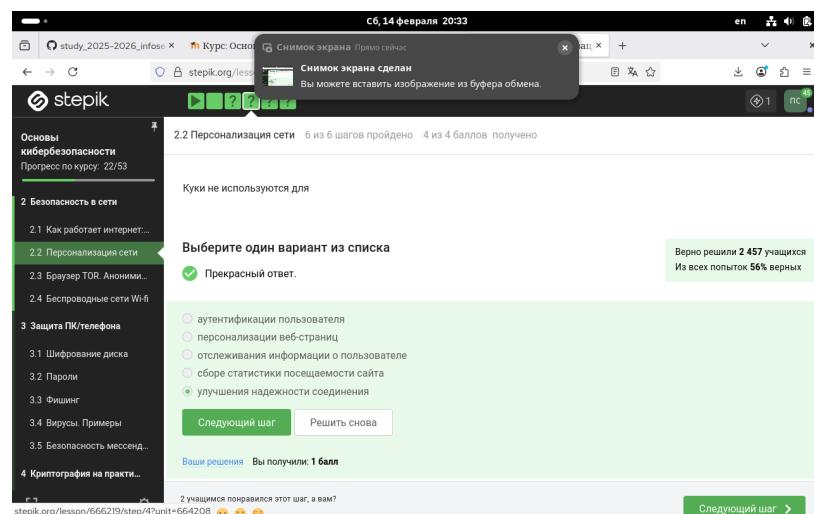


Рисунок 4.11: Задание 11

Куки (cookies) генерируются веб-сервером при посещении пользователем сайта и отправляются в браузер через HTTP-заголовок. (рис 12)

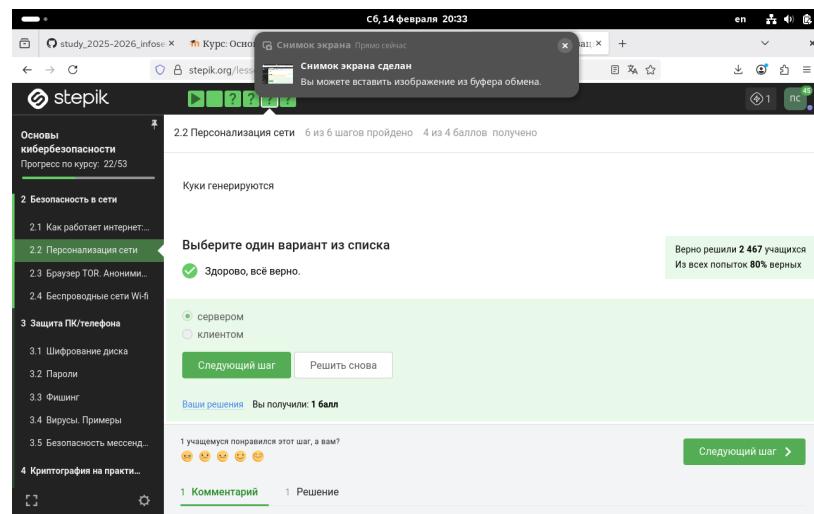


Рисунок 4.12: Задание 12

Сессионные куки используются для запоминания действий пользователя (авторизация, товары в корзине, заполнение форм) внутри одного посещения. (рис. 13)

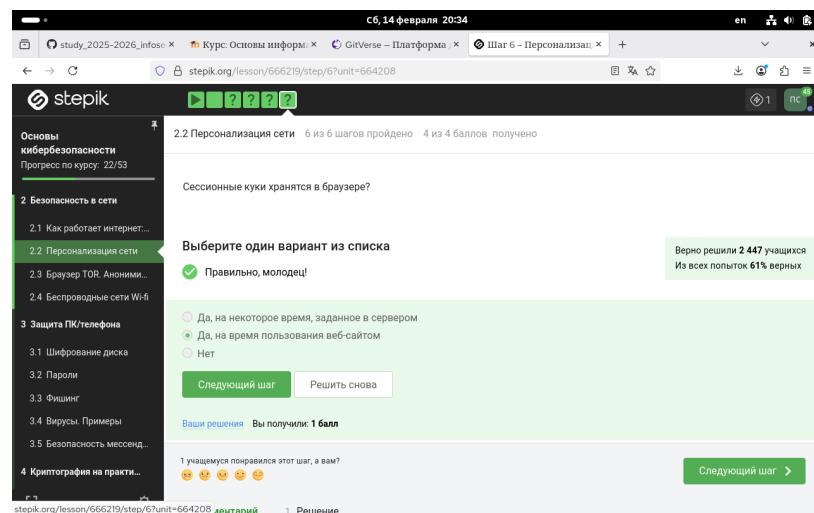


Рисунок 4.13: Задание 13

В стандартной цепочке Tor-сети используется три промежуточных узла (ретранслятора) для обеспечения анонимности: входной узел (Guard/Entry), средний узел (Middle) и выходной узел (Exit). (рис. 14)

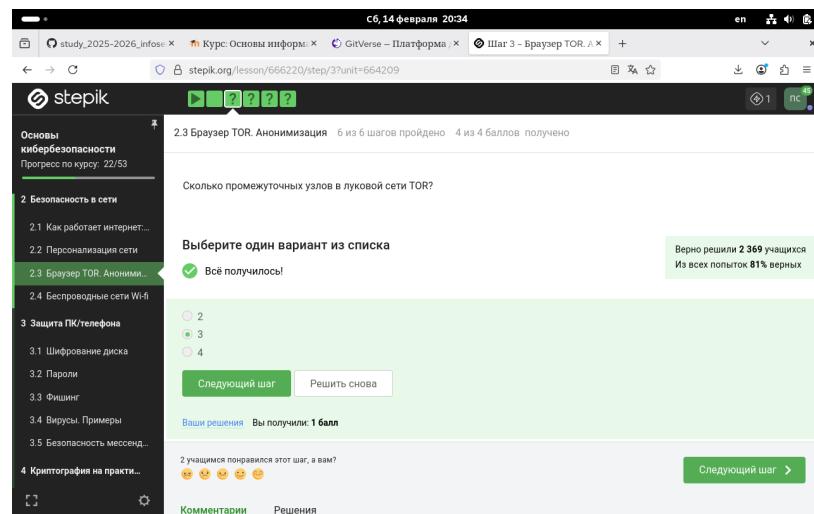


Рисунок 4.14: Задание 14

В браузере тор видно айпи выходного узла, и отправителя. (рис. 15)

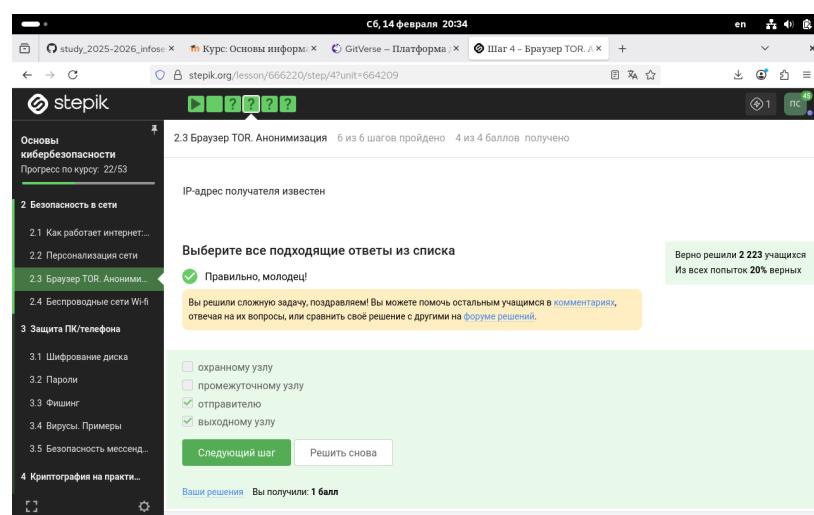


Рисунок 4.15: Задание 15

Общий секретный ключ генерируется со всеми узлами, через которые идет передача, то есть со всеми тремя. (рис. 16)

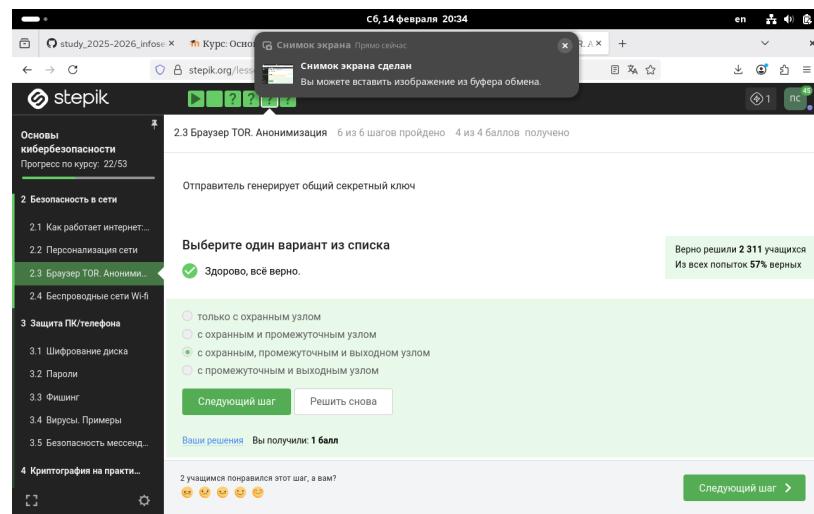


Рисунок 4.16: Задание 16

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

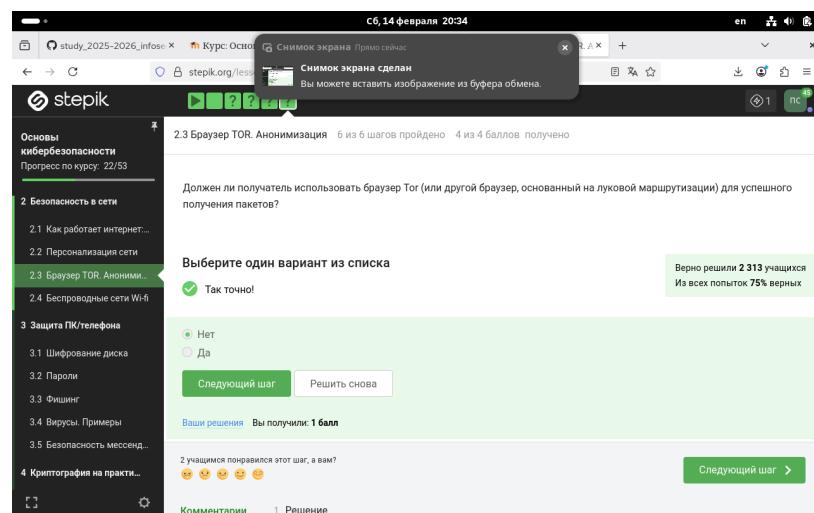


Рисунок 4.17: Задание 17

Самое базовое и полное определение вайфая. (рис. 18)

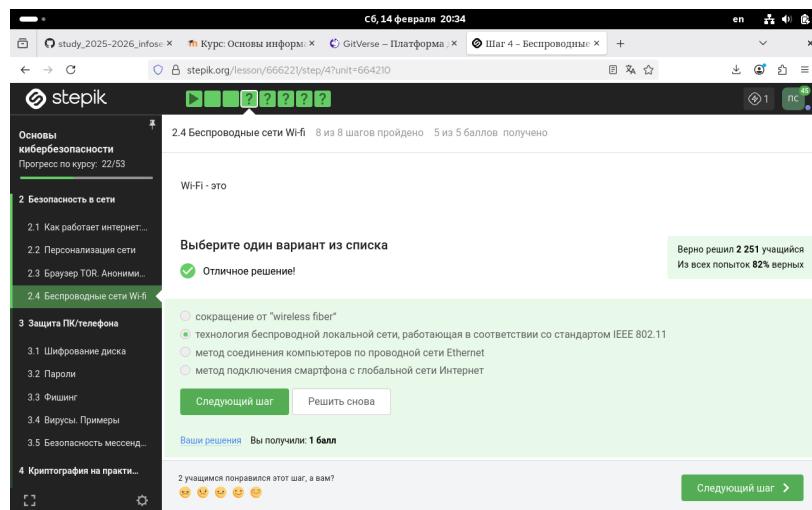


Рисунок 4.18: Задание 18

Для целей работы в Интернете Wi-Fi обычно располагается как канальный уровень (эквивалентный физическому и канальному уровням модели OSI) ниже интернет-уровня интернет-протокола. (рис. 19)

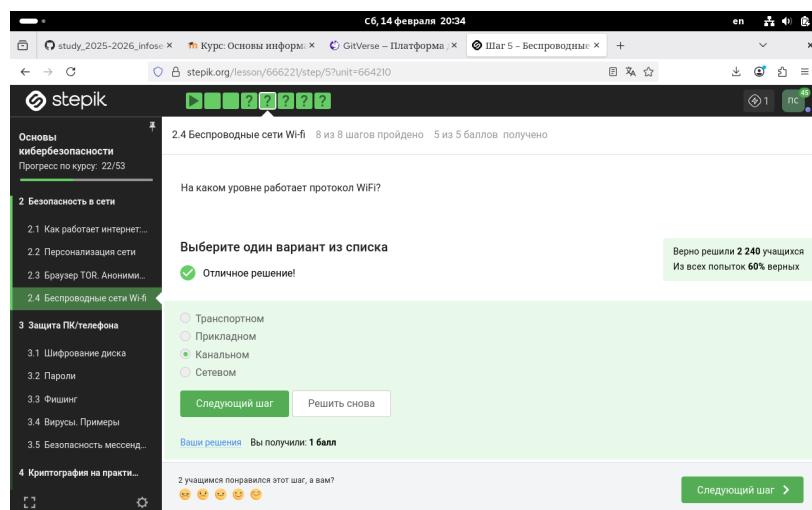


Рисунок 4.19: Задание 19

WEP - устаревший протокол безопасности сети, сейчас используются более защищенные протоколы семейства WPA/ (рис. 20)

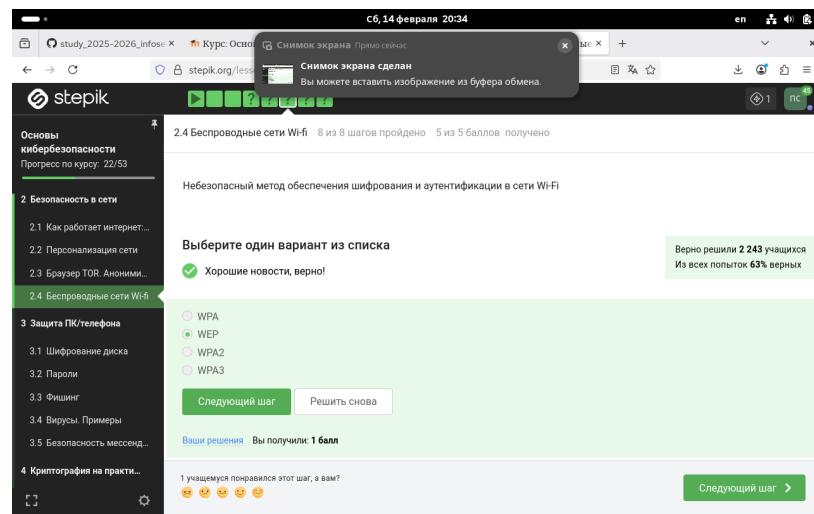


Рисунок 4.20: Задание 20

Сначала устройства аутентифицируются, затем уже передаются зашифрованные данные. (рис. 21)

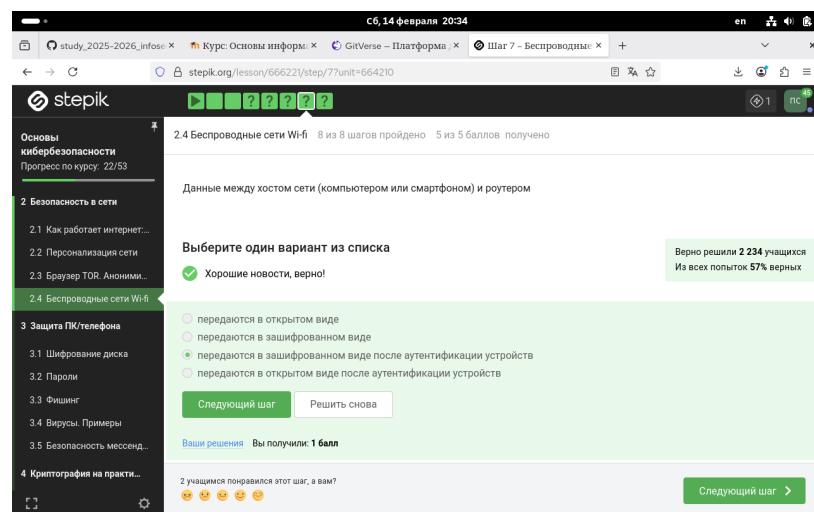


Рисунок 4.21: Задание 21

Используется метод Personal, Enterprise используется для предприятий. (рис. 22)

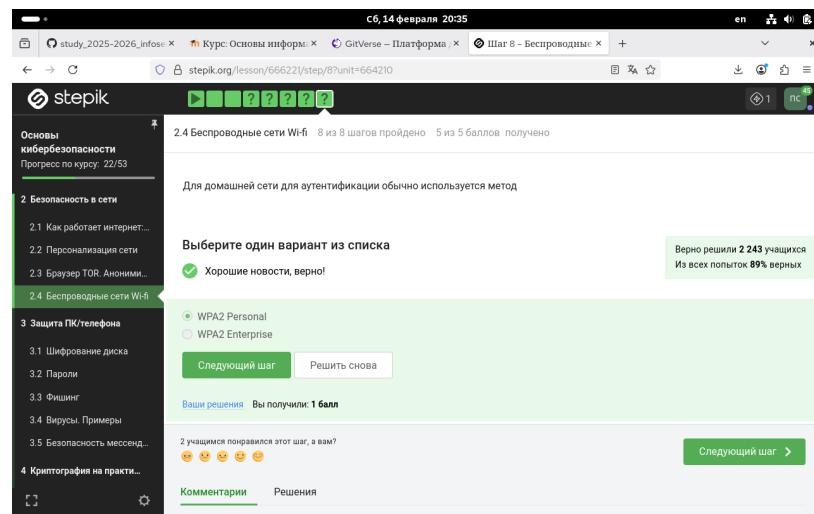


Рисунок 4.22: Задание 22

5 Выводы

Я выполнила все задания первого модуля курса и приобрела знания о протоколах связи, луковой маршрутизации и современных стандартах WI-FI.