

# **Внешний курс раздел 1**

**Безопасность в сети**

Александр Андреевич Шуплецов

# Содержание

1	Цель работы	5
2	Выполнение работы	6
3	Выводы	18
4	Список литературы	19

## Список иллюстраций

2.1	первое задание . . . . .	6
2.2	второе задание . . . . .	7
2.3	третье задание . . . . .	7
2.4	четвертое задание . . . . .	8
2.5	пятое задание . . . . .	8
2.6	шестое задание . . . . .	9
2.7	седьмое задание . . . . .	9
2.8	восьмое задание . . . . .	10
2.9	девятое задание . . . . .	10
2.10	десятое задание . . . . .	11
2.11	одиннадцатое задание . . . . .	11
2.12	двенадцатое задание . . . . .	12
2.13	тринадцатое задание . . . . .	12
2.14	четырнадцатое задание . . . . .	13
2.15	пятнадцатое задание . . . . .	13
2.16	шестнадцатое задание . . . . .	14
2.17	семнадцатое задание . . . . .	14
2.18	восемнадцатое задание . . . . .	15
2.19	девятнадцатое задание . . . . .	15
2.20	двадцатое задание . . . . .	16
2.21	двадцать первое задание . . . . .	16
2.22	двадцать второе задание . . . . .	17

## Список таблиц

# 1 Цель работы

Изучить основы безопасности в сети.

## 2 Выполнение работы

1. Единственным протоколом прикладного уровня из списка является протокол HTTPS.

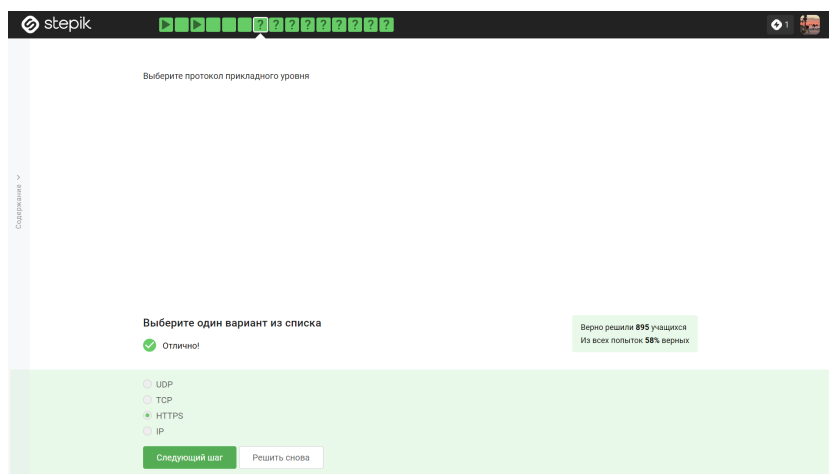


Рис. 2.1: первое задание

2. Протокол TCP работает на транспортном уровне.

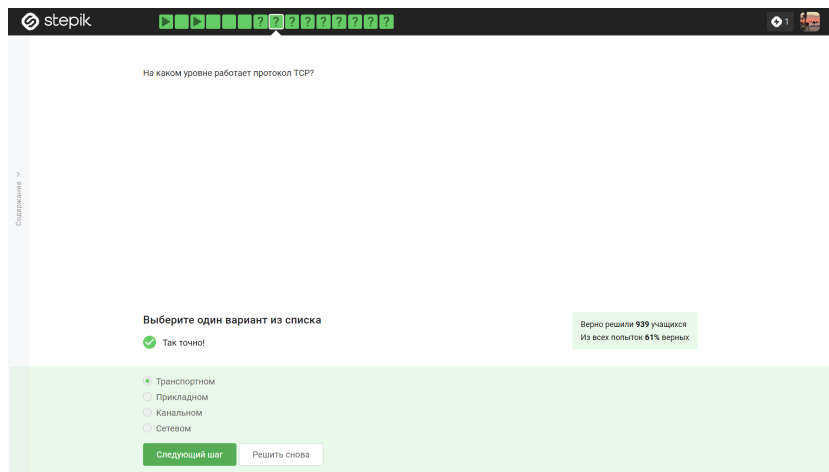


Рис. 2.2: второе задание

3. В 8 битах 256 разных значений, но нумерация идет с нуля и как итог, допустимые значения в IP адресе - с 0 до 255.

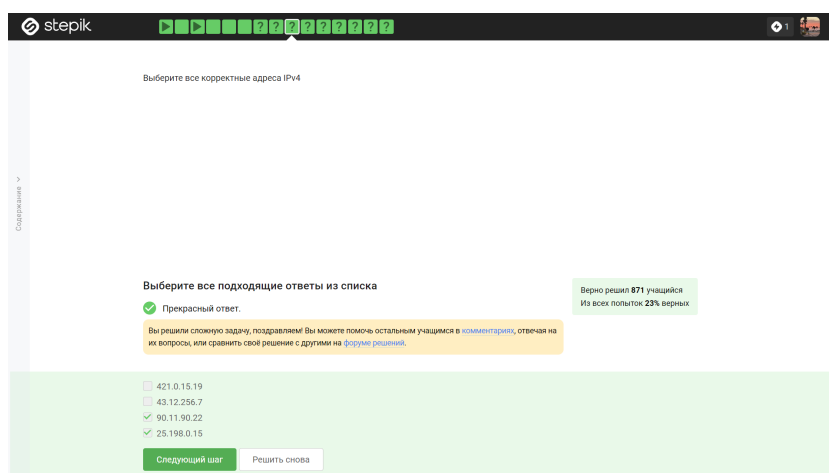


Рис. 2.3: третье задание

4. Основная задача DNS-сервера - это сопоставить название, то есть доменное имя, с корректным IP-адресом, с тем, где лежит этот сервер, этот сайт.

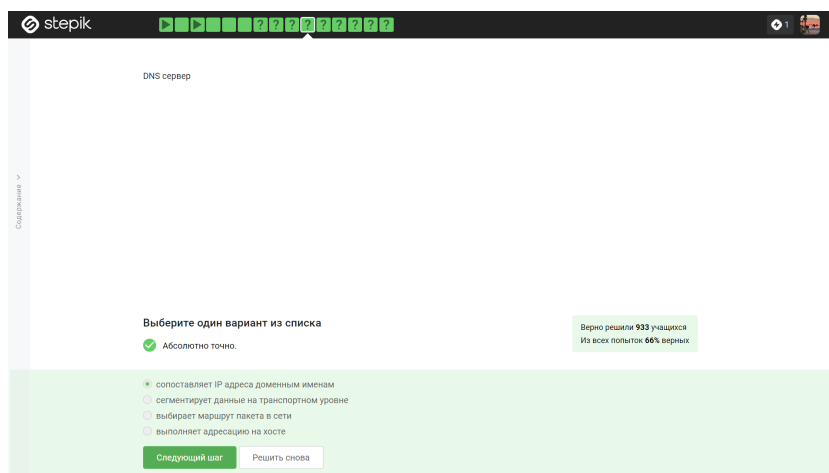


Рис. 2.4: четвертое задание

5. Корректная последовательность протоколов в модели TCP/IP: прикладной-транспортный-сетевой-канальный.

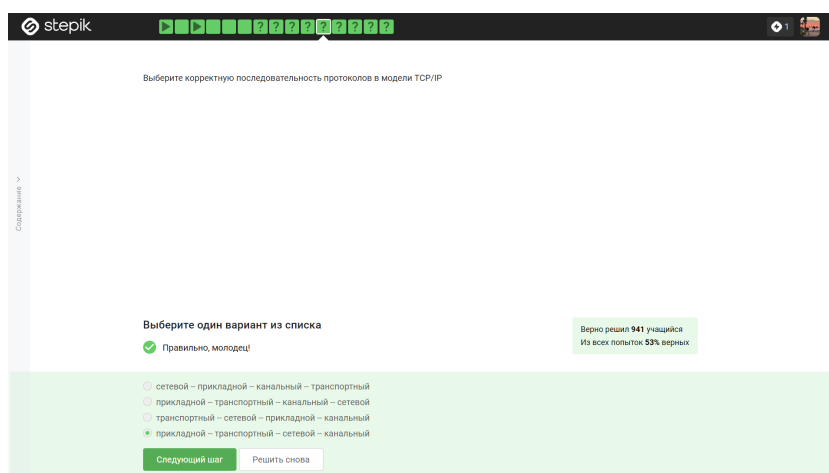


Рис. 2.5: пятое задание

6. Протокол http, в отличие от протокола https, предполагает передачу данных между клиентом и сервером в открытом виде.



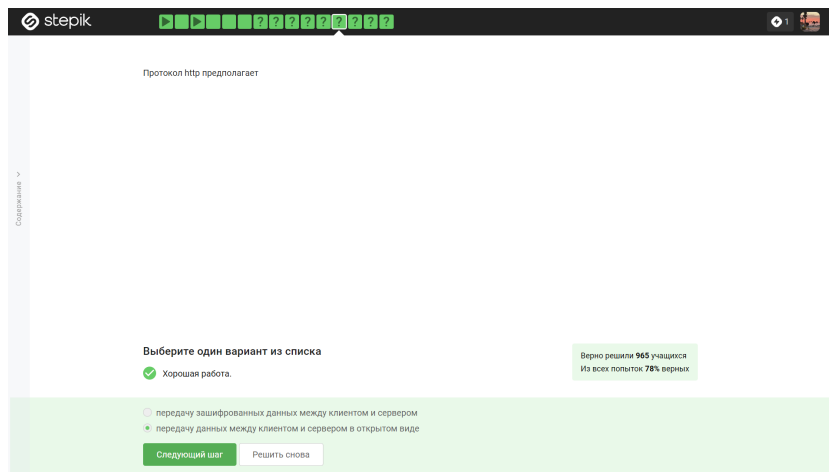


Рис. 2.6: шестое задание

7. Протокол https состоит из двух фаз: рукопожатия (handshake) и передачи данных.

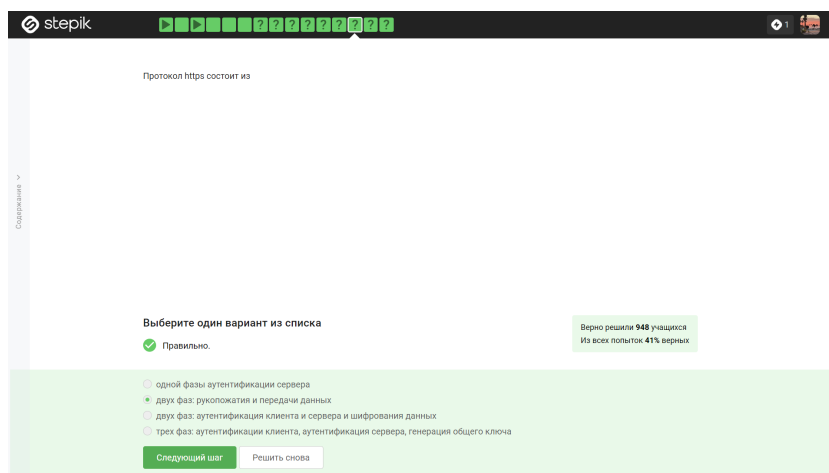


Рис. 2.7: седьмое задание

8. Версия протокола TLS определяется и клиентом, и сервером в процессе “переговоров”.

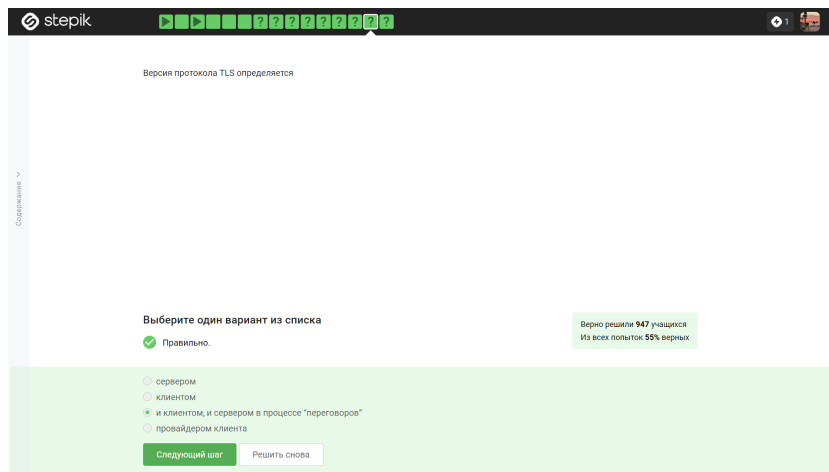


Рис. 2.8: восьмое задание

9. В фазе рукопожатия не предусмотрено шифрование данных, так как эта фаза является вводной перед защищенной передачей данных.

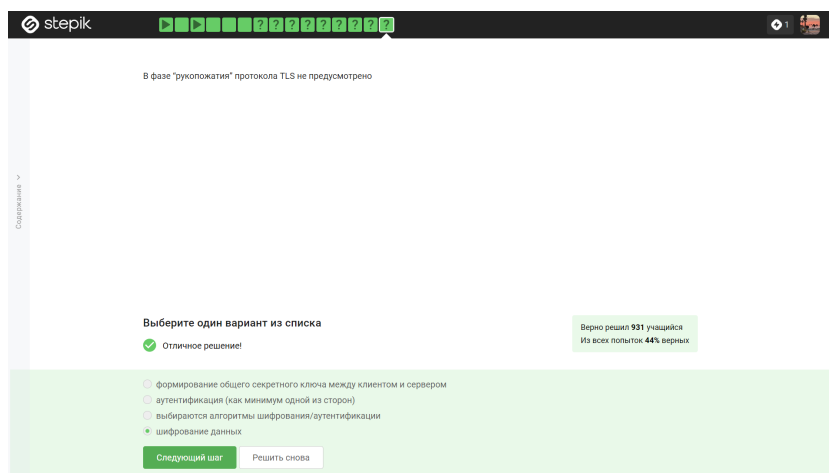


Рис. 2.9: девятое задание

10. Куки хранят id сессии, идентификатор пользователя, пароль и IP адрес они не хранят.

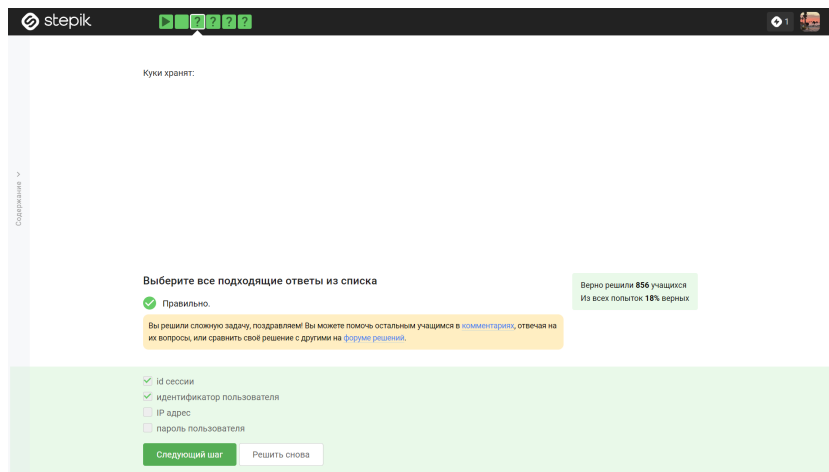


Рис. 2.10: десятое задание

11. Куки не используются для улучшения надежности соединения, они с соединением пользователя никак не связаны.

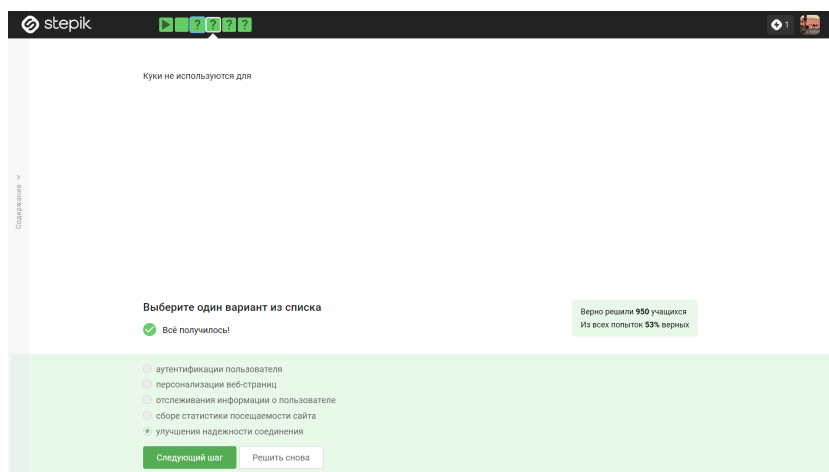


Рис. 2.11: одиннадцатое задание

12. Куки генерируются сервером для клиента.

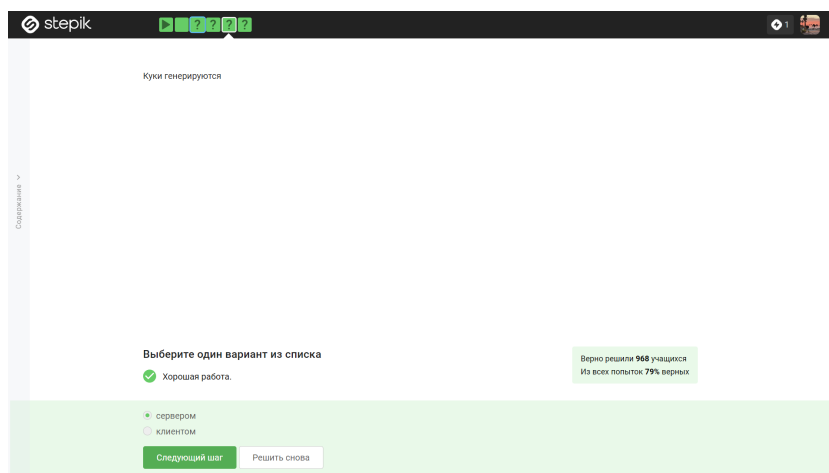


Рис. 2.12: двенадцатое задание

13. Сессионные куки хранятся в браузере до конца сессии, то есть на время пользования веб-сайтом.

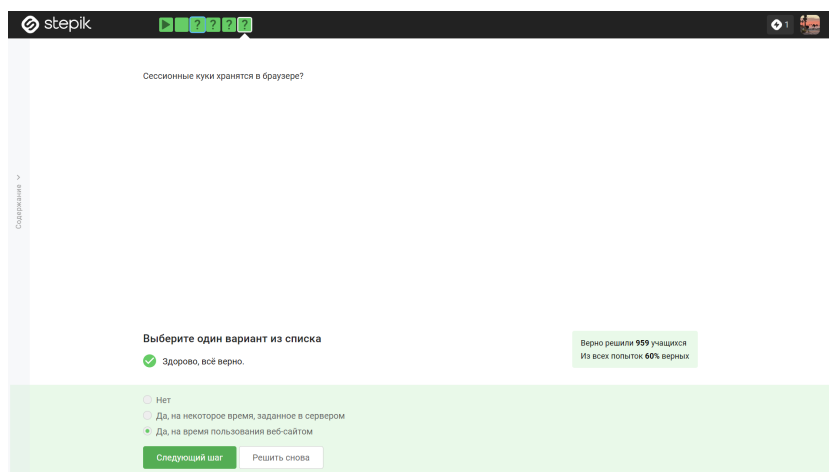


Рис. 2.13: тринадцатое задание

14. В луковой сети TOR 3 промежуточных узла: охранный, промежуточный и выходной.

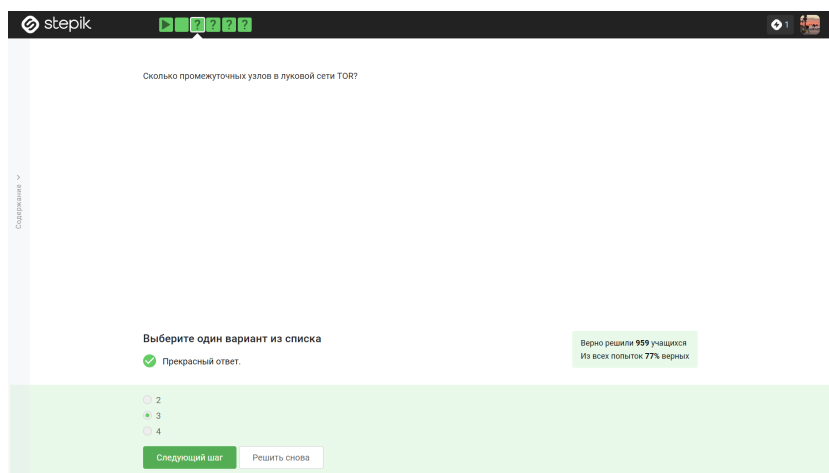


Рис. 2.14: четырнадцатое задание

15. В TOR IP-адрес получателя известен лишь отправителю и выходному узлу, это одна из причин почему TOR считается конфиденциальной сетью.

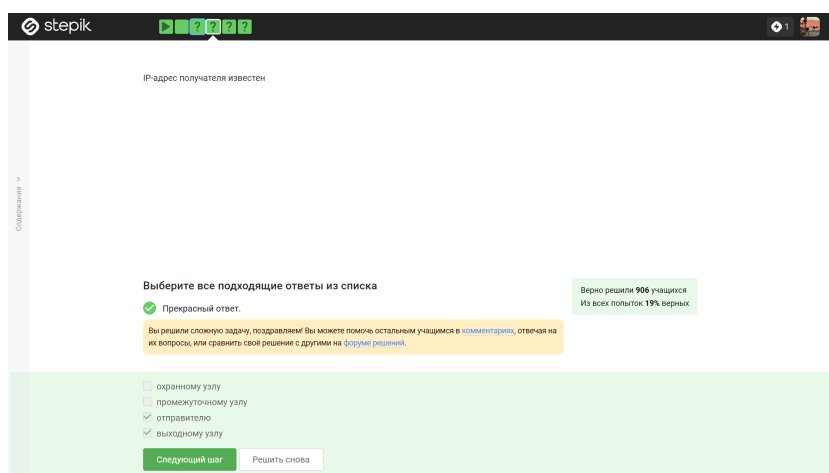


Рис. 2.15: пятнадцатое задание

16. Отправитель генерирует общий секретный ключ со всеми тремя узлами: с охранным, с промежуточным, с выходным. Этот процесс делает передачу данных крайне защищенной.

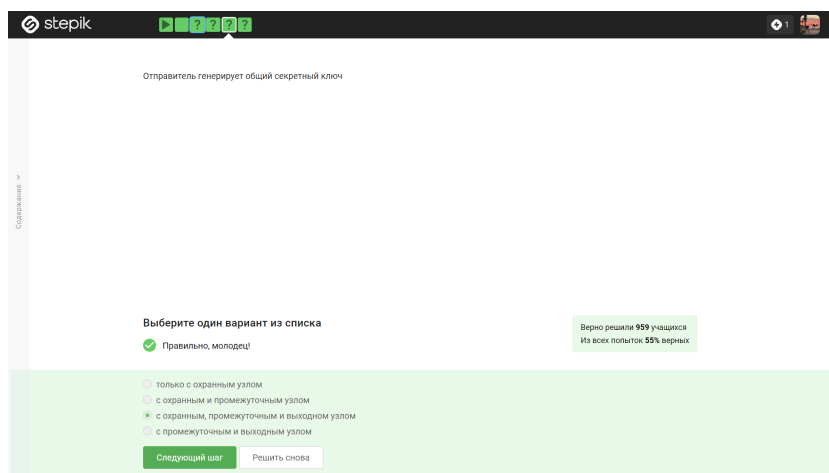


Рис. 2.16: шестнадцатое задание

- Для получения пакетов через луковую маршрутизацию необязательно использовать браузер, основанный на луковой маршрутизации, это обязательно для отправителя пакетов.

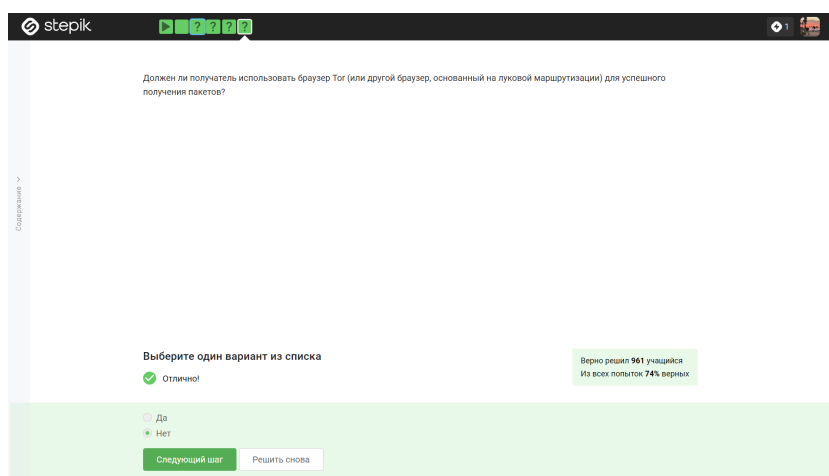


Рис. 2.17: семнадцатое задание

- Согласно определению, Wi-Fi - это технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11.

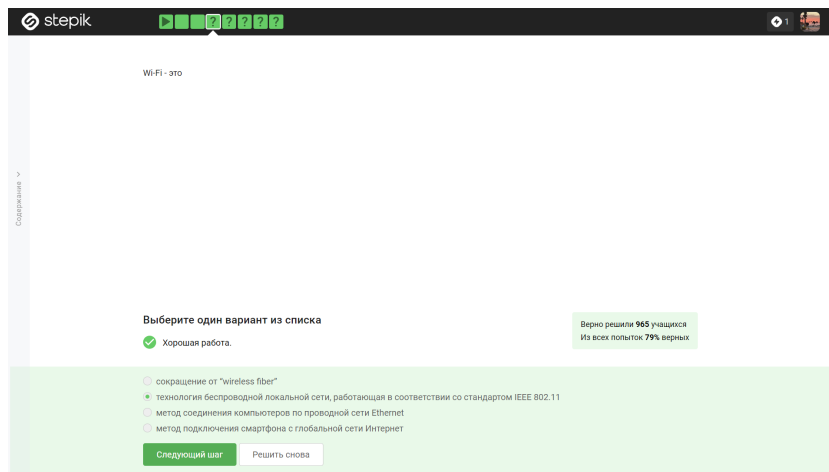


Рис. 2.18: восемнадцатое задание

19. Протокол Wifi работает на самом нижнем, канальном уровне.

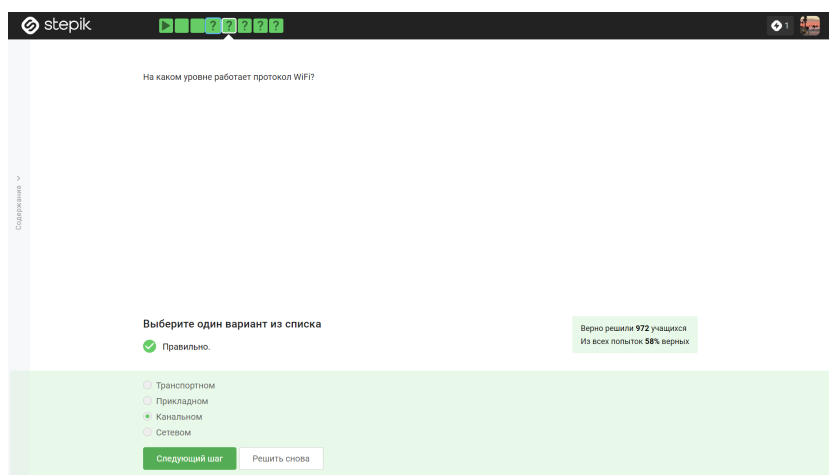


Рис. 2.19: девятнадцатое задание

20. Небезопасным методом обеспечения шифрования и аутентификации в сети Wifi является WEP, так как 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.

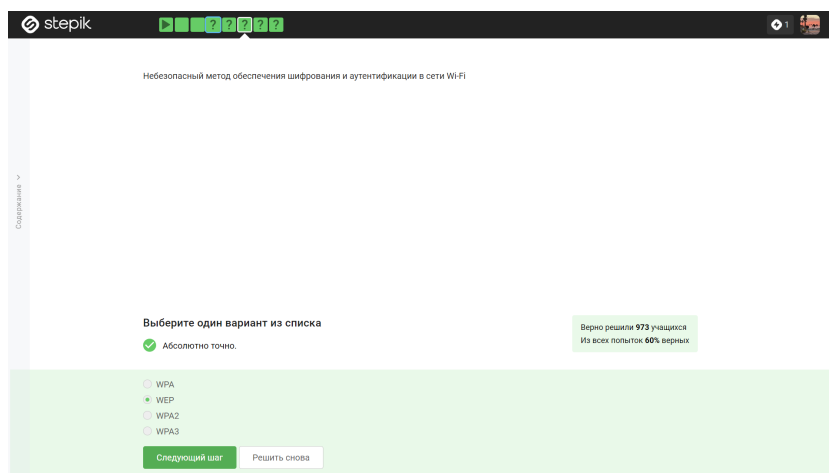


Рис. 2.20: двадцатое задание

21. Данные между хостом сети (компьютером или смартфоном) и роутером передаются в зашифрованном виде после аутентификации устройств.

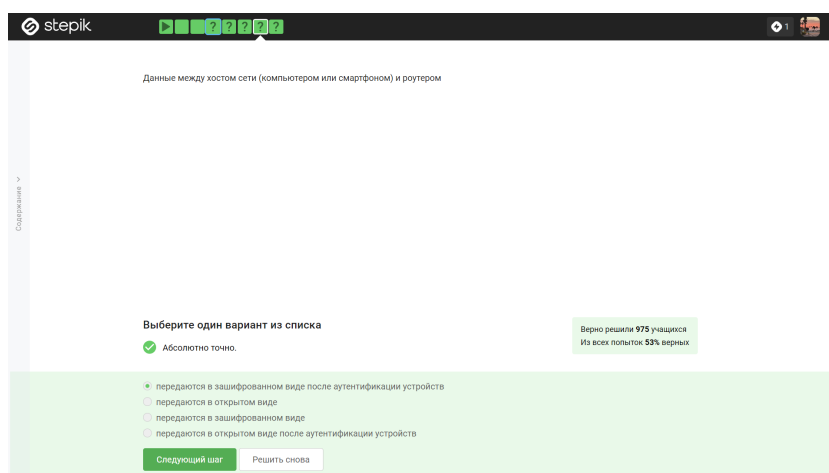


Рис. 2.21: двадцать первое задание

22. Для домашней сети для аутентификации обычно используется метод WPA2 Personal, WPA2 Enterprise используется для корпоративных сетей.



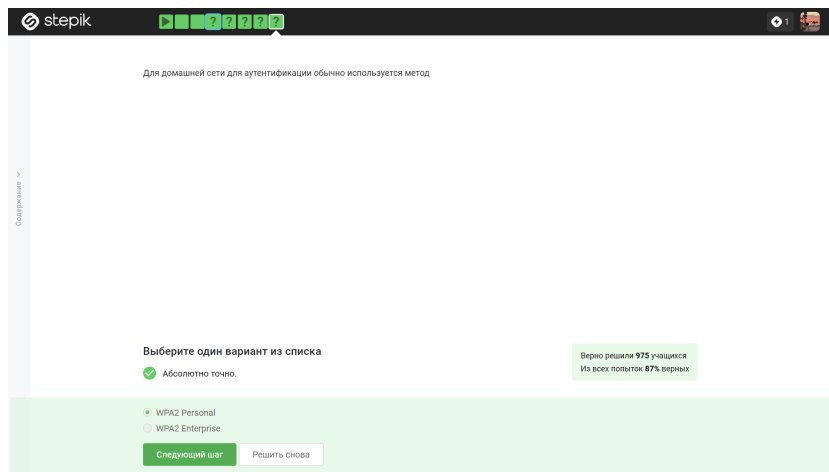


Рис. 2.22: двадцать второе задание

## **3 Выводы**

Я изучил основы безопасности в сети.

## **4 Список литературы**

Конспекты к лекциям курса “Основы кибербезопасности”.