Отчёт по выполнению внешних курсов

Основы кибербезопасности

Боровиков Даниил Александрович НПИбд-01-22

Содержание

# 1 Цель работы

Пройти спец. курс “Основы кибербезопасности” и получить сертификат.

# 2 Выполнение лабораторной работы

## 2.1 Раздел 2: “Безопасность в сети”

### 2.1.1 (2.1) “Как работает интернет: базовые сетевые протоколы”

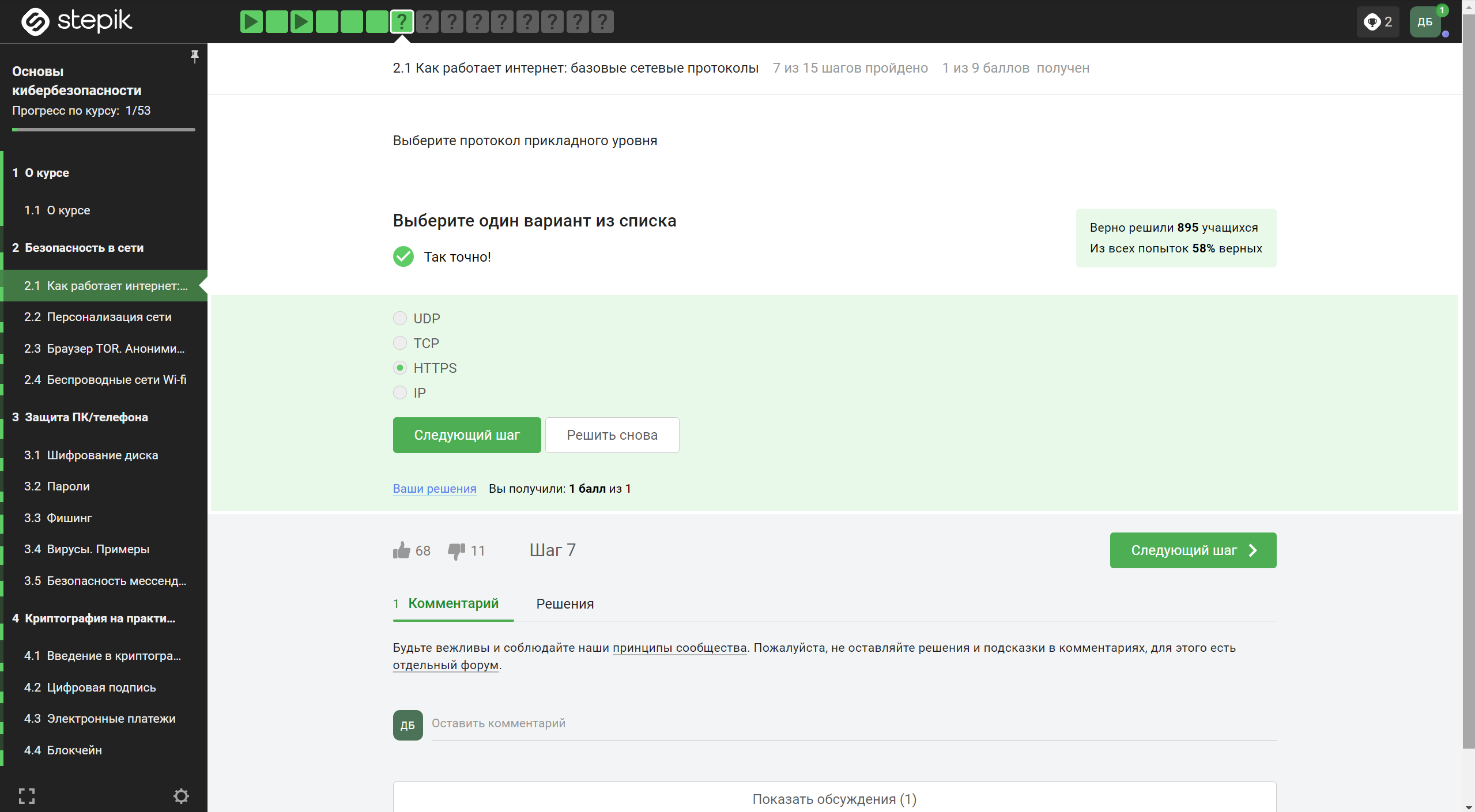


Figure 1: Рис. 1. Раздел (2.1) – Вопрос 1

**Вопрос:** Выберите протокол прикладного уровня  
**Ответ:**  
- HTTPS  
- UPD – транспортного уровня  
- TCP – транспортного уровня  
- HTTPS – прикладного уровня  
- IP – сетевого уровня

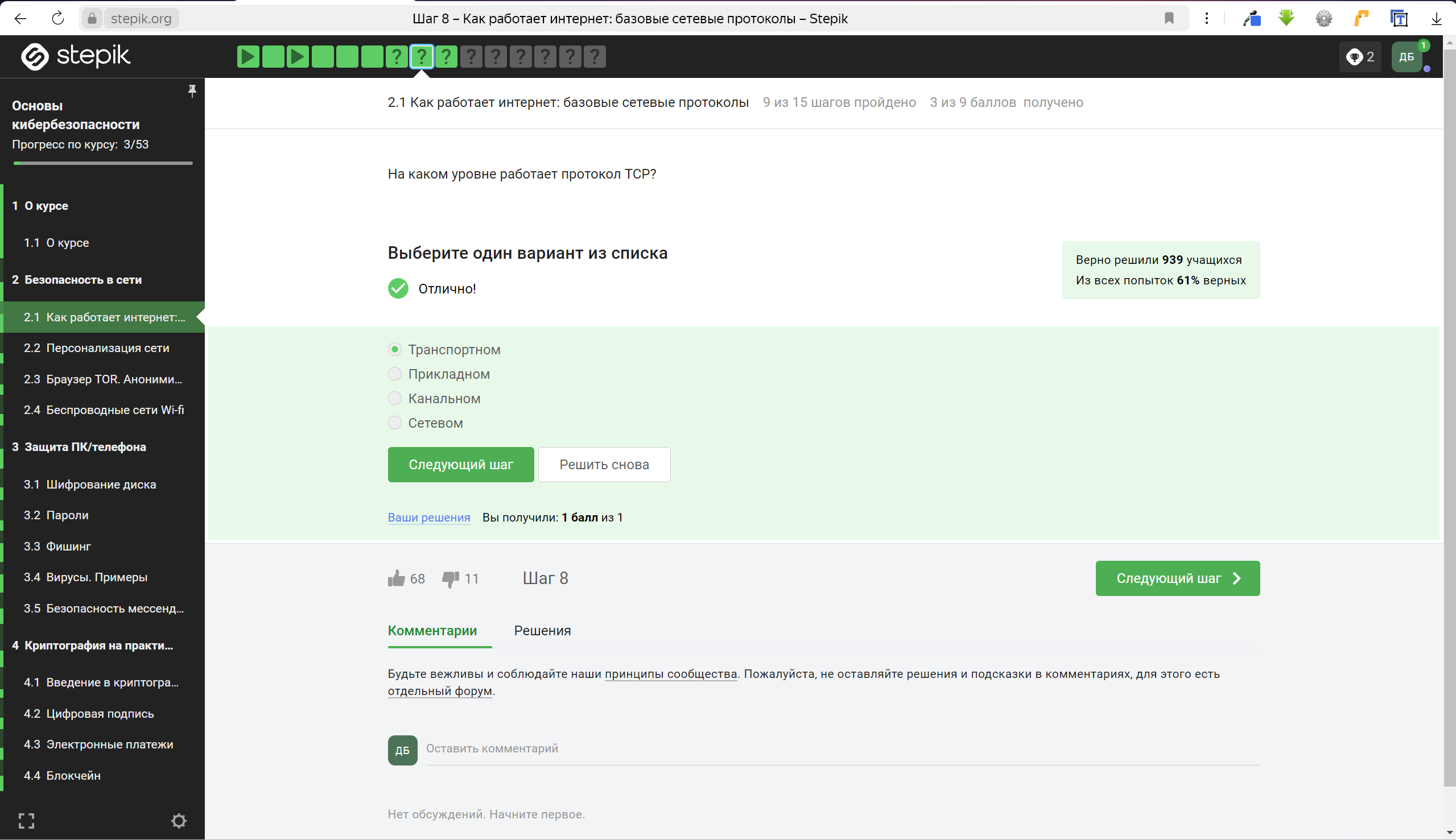
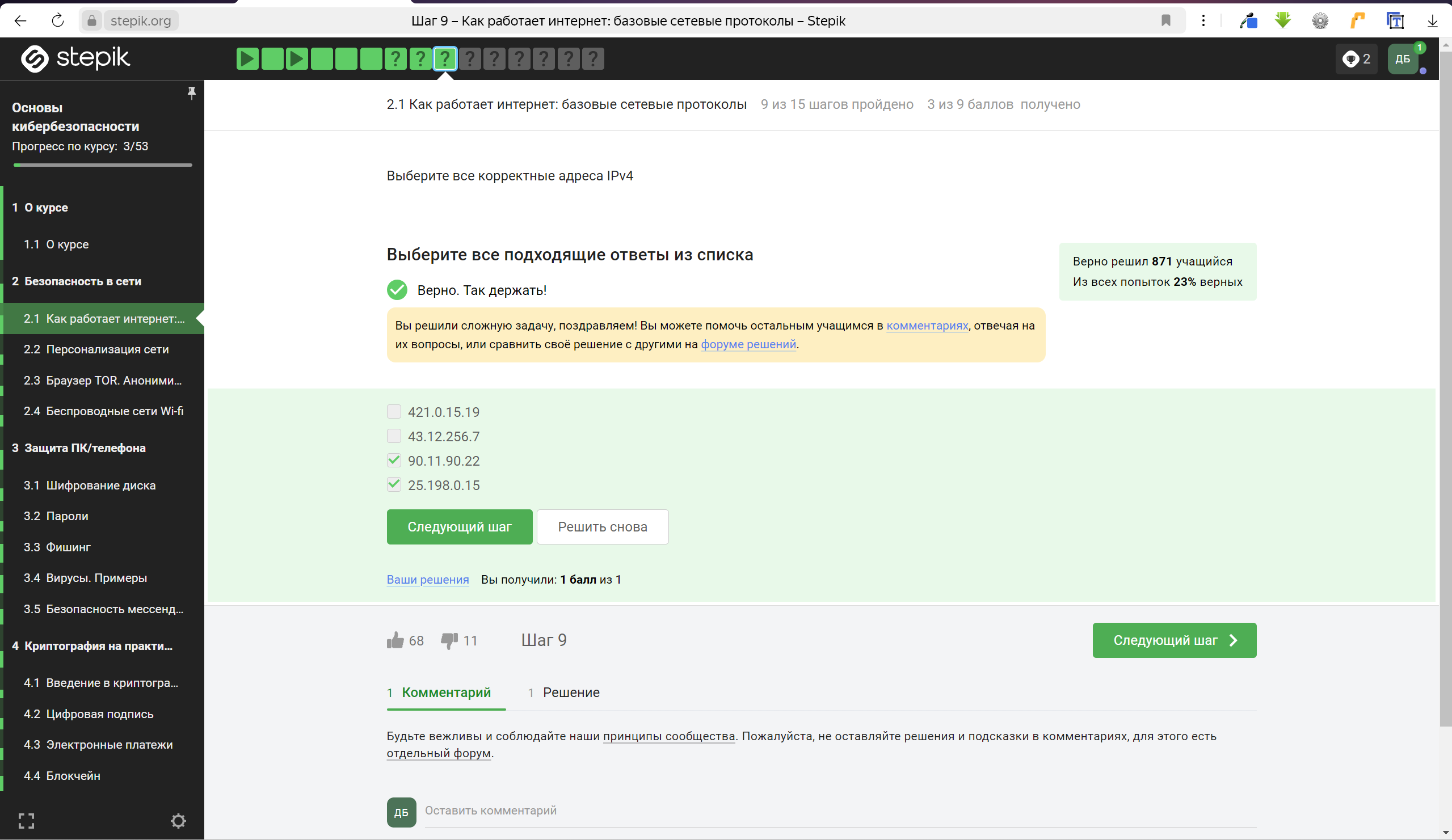


Figure 2: Рис. 2. Раздел (2.1) – Вопрос 2

**Вопрос:** На каком уровне работает протокол TCP?  
**Ответ:** TCP работает на транспортном уровне, который является 4-м уровнем в модели OSI

 **Вопрос:** Выберите все корректные адреса IPv4  
**Ответ:** Корректные адреса IPv4 состоят из чисел от 0 до 255

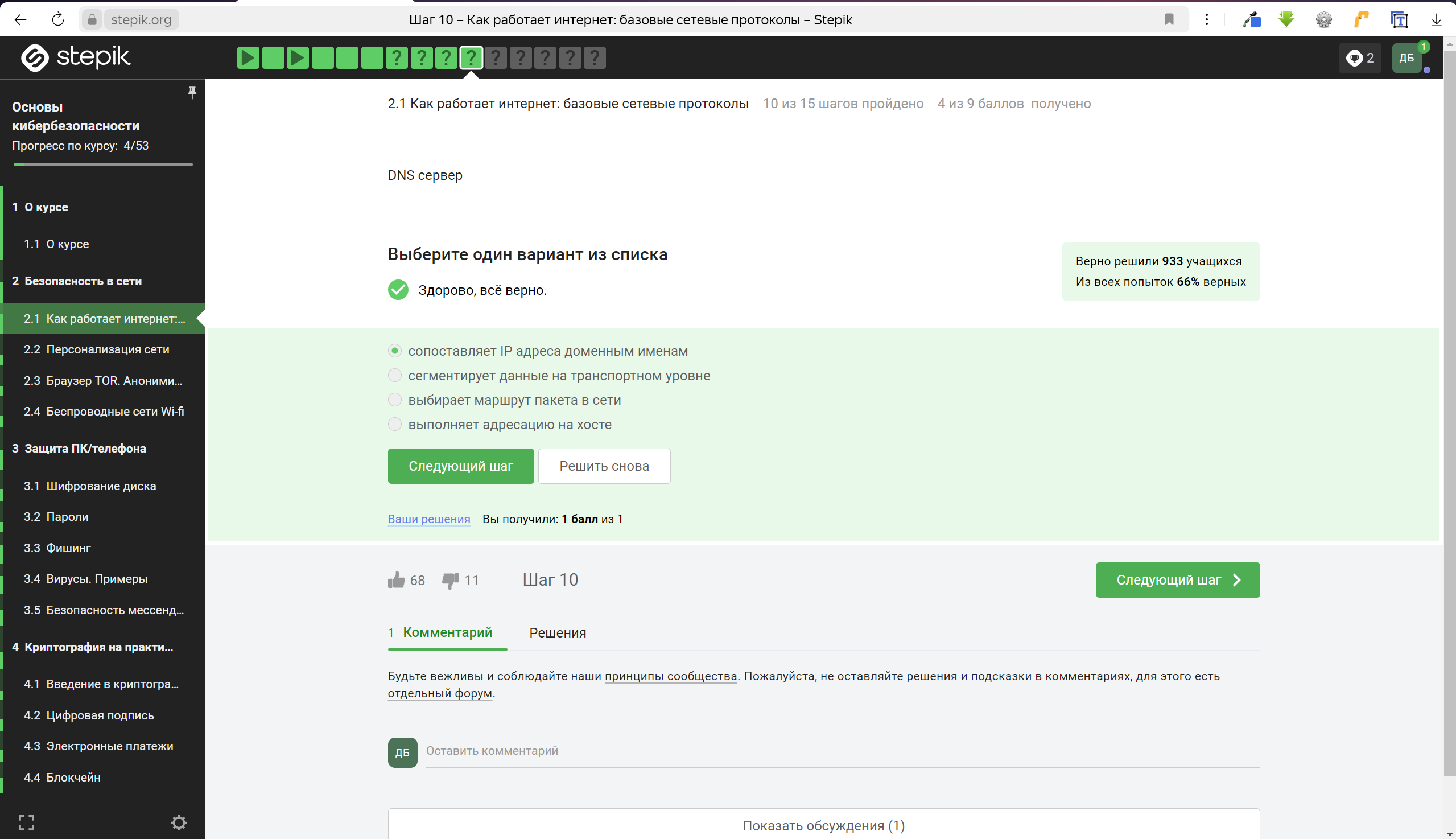


Figure 3: Рис. 4. Раздел (2.1) – Вопрос 4

**Вопрос:** DNS сервер это  
**Ответ:** DNS сервер - система, переводящая доменные имена в IP-адреса, позволяя пользователям легко находить веб-сайты в интернете.

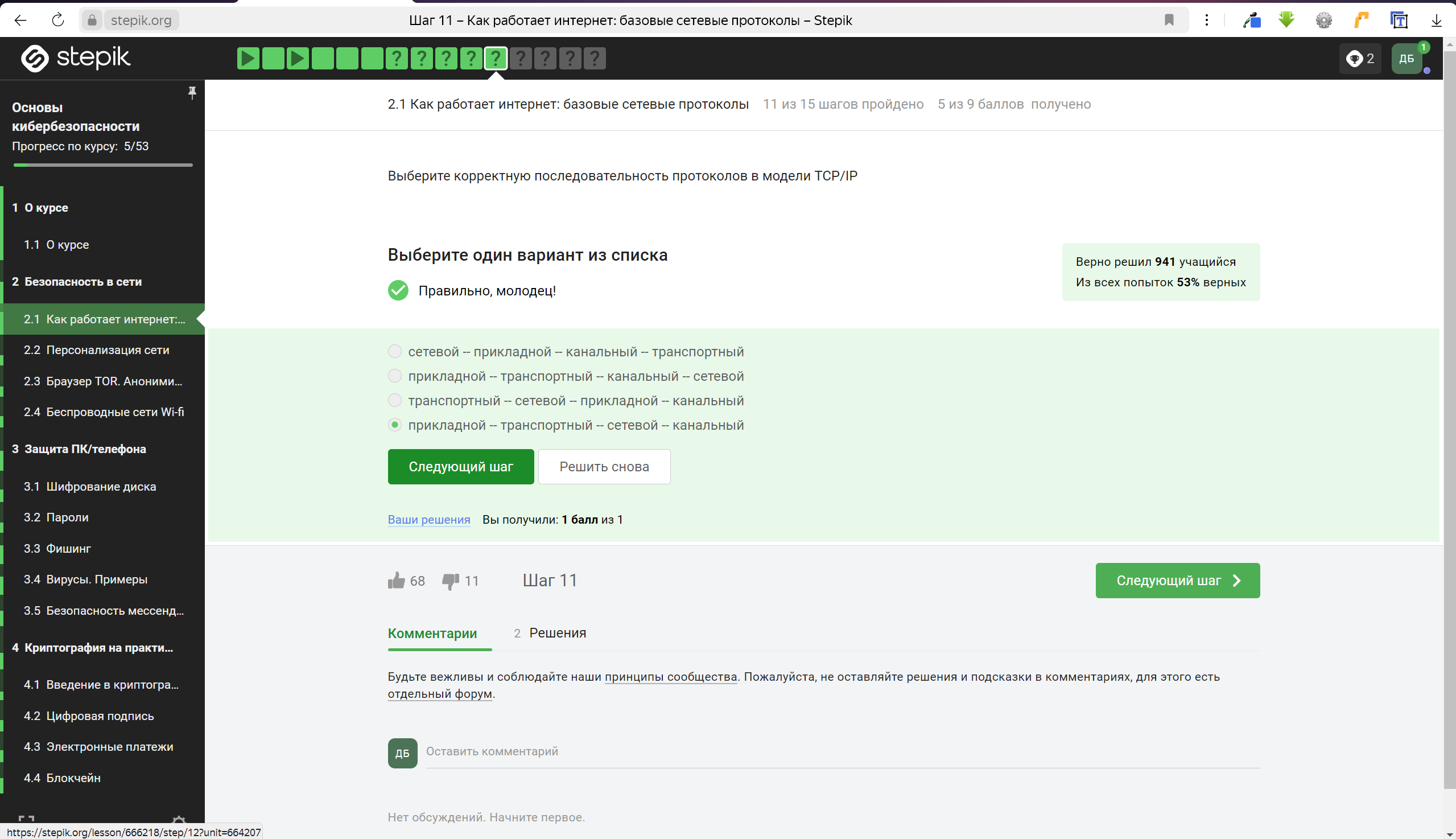


Figure 4: Рис. 5. Раздел (2.1) – Вопрос 5

**Вопрос:** Выберите корректную последовательность протоколов в модели TCP/IP  
**Ответ:** В модели TCP/IP, которая является набором сетевых протоколов, используемых для передачи данных в интернете, протоколы организованы в четыре уровня: прикладной - транспортный - сетевой - канальный

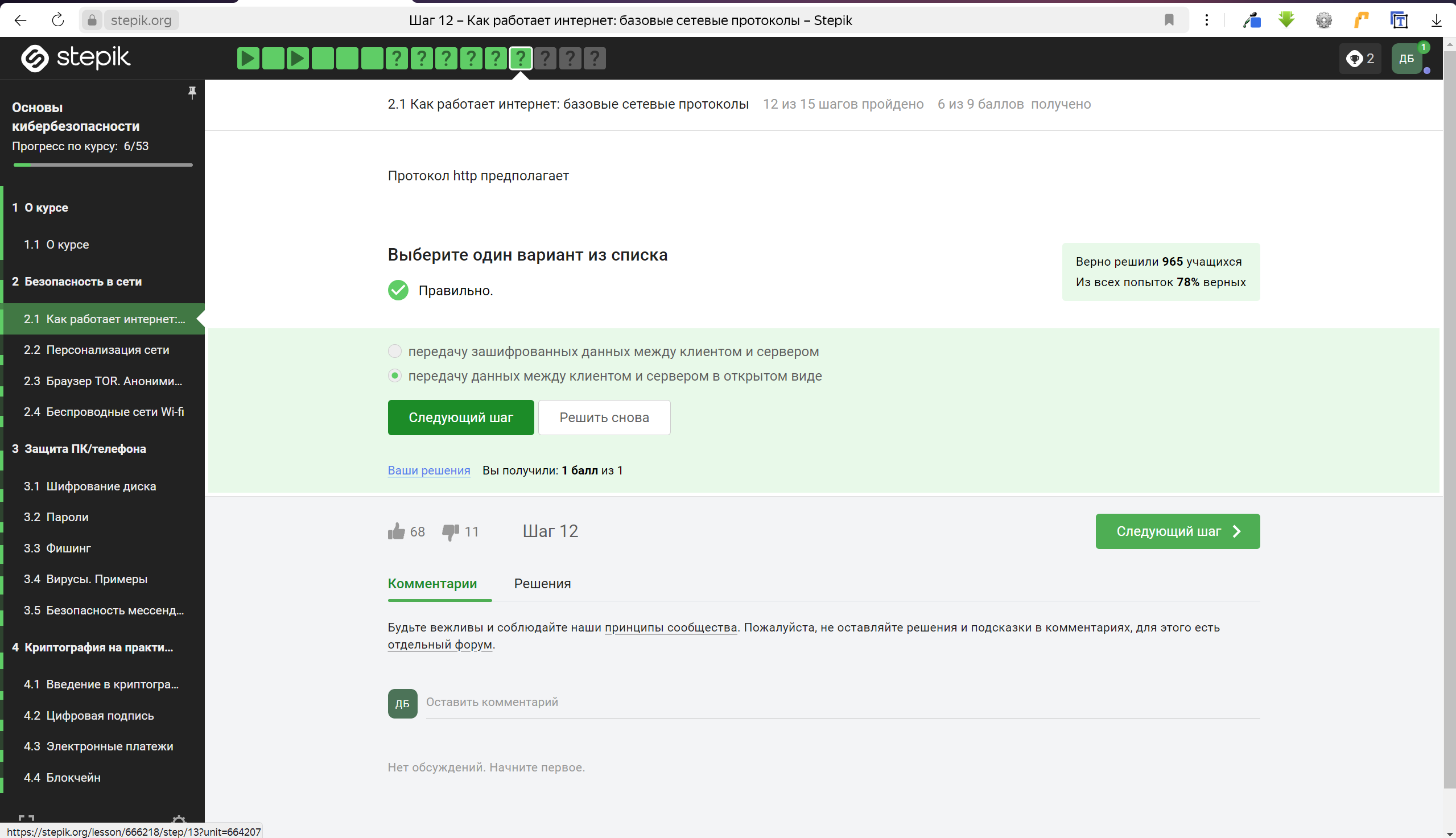


Figure 5: Рис. 6. Раздел (2.1) – Вопрос 6

**Вопрос:** Протокол http предполагает  
**Ответ:** Протокол HTTP предполагает стандартный способ передачи веб-страниц от сервера к клиенту

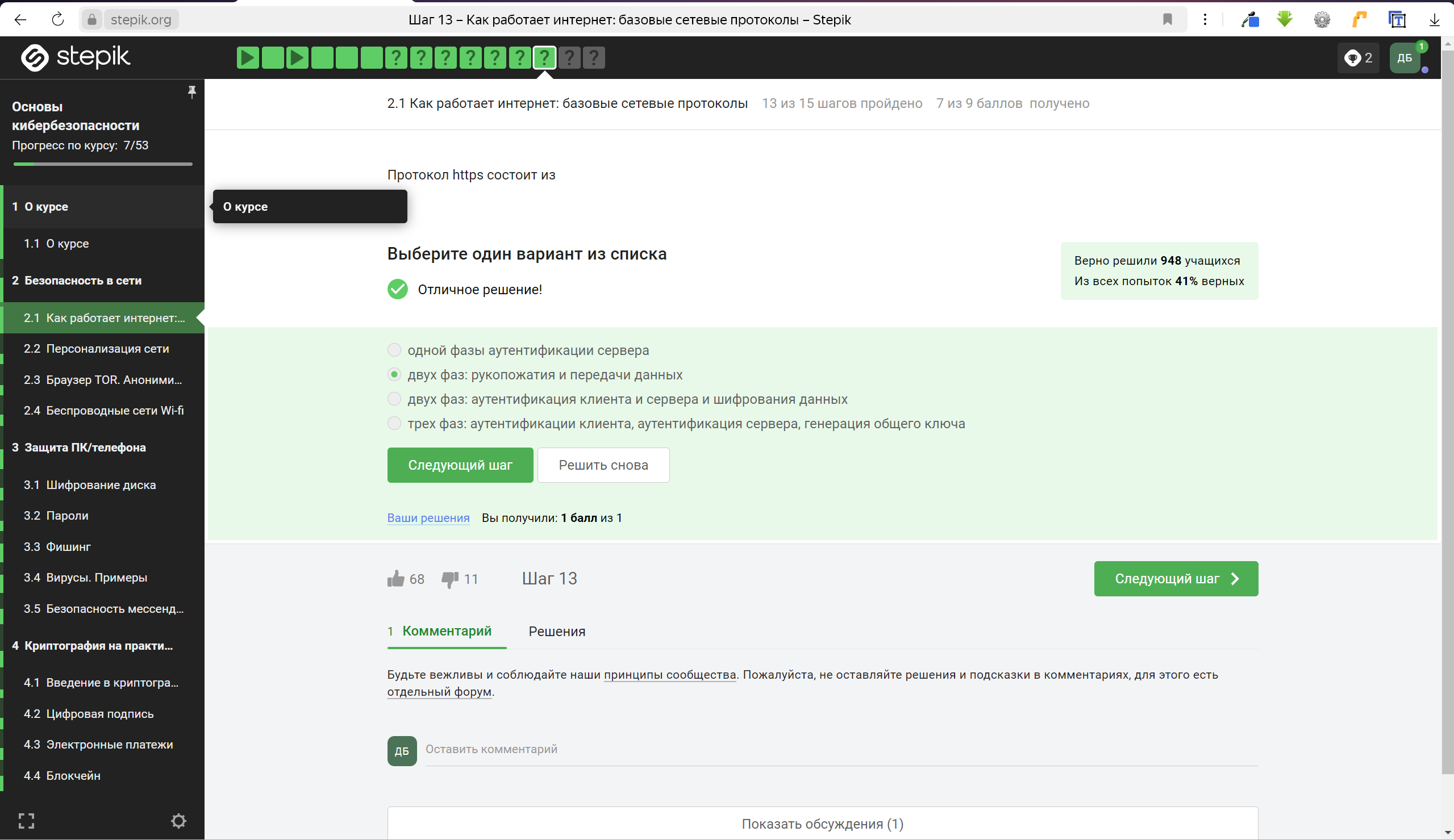


Figure 6: Рис. 7. Раздел (2.1) – Вопрос 7

**Вопрос:** Протокол https состоит из  
**Ответ:** Протокол HTTPS включает в себя две основные фазы в процессе установления защищенного соединения между клиентом и сервером:  
1. **Фаза рукопожатия:** В этой фазе клиент и сервер обмениваются информацией, необходимой для установления безопасного соединения.  
2. **Фаза передачи данных:** После успешного рукопожатия и установления защищенного канала связи начинается передача зашифрованных данных.

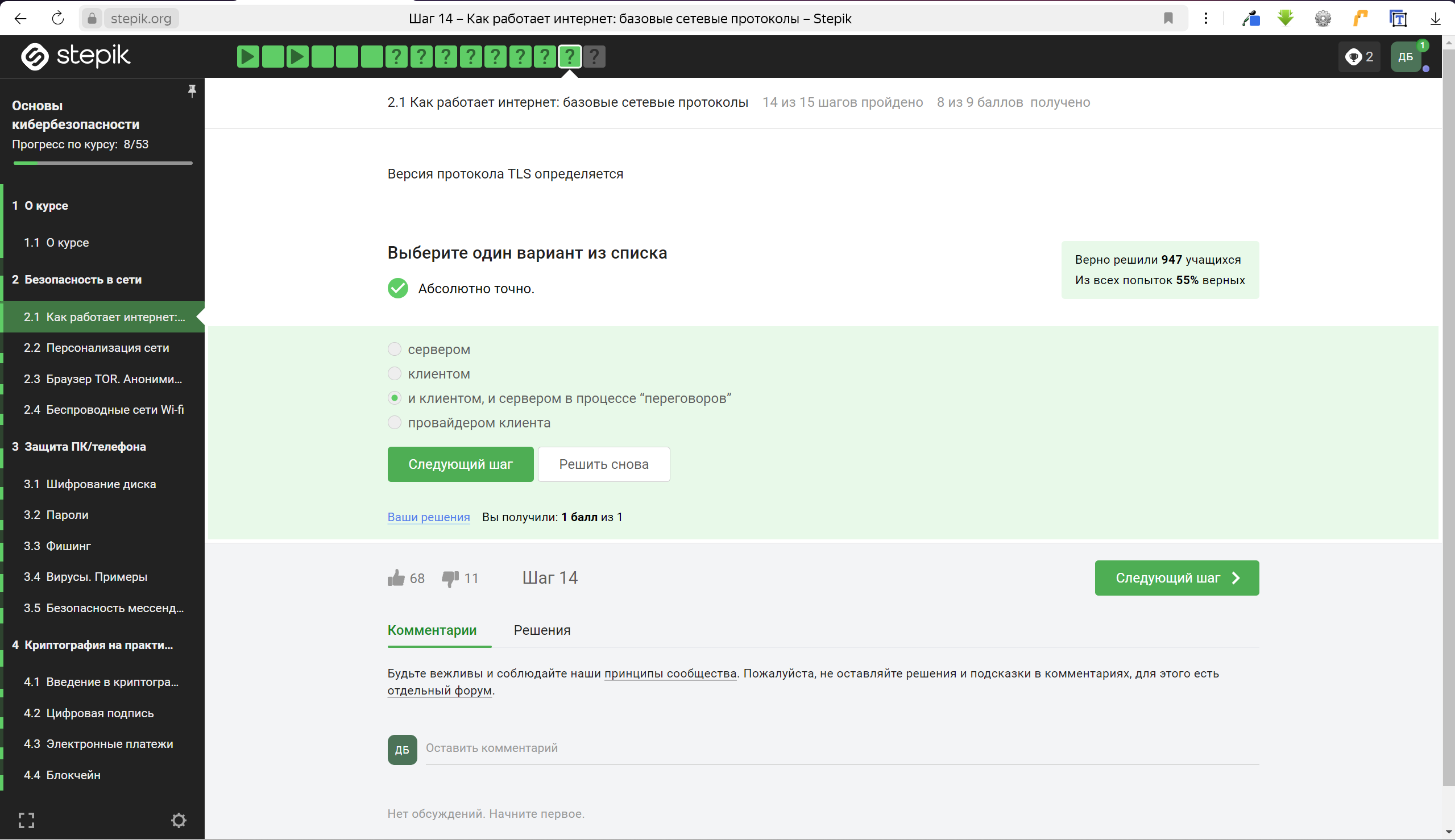


Figure 7: Рис. 8. Раздел (2.1) – Вопрос 8

**Вопрос:** Версия протокола TLS определяется  
**Ответ:** Версия протокола TLS определяется и клиентом, и сервером в процессе “переговоров”. Процесс переговоров - согласование обоих сторон на общие параметры безопасности, для обеспечения надежного и защищенного соединения.

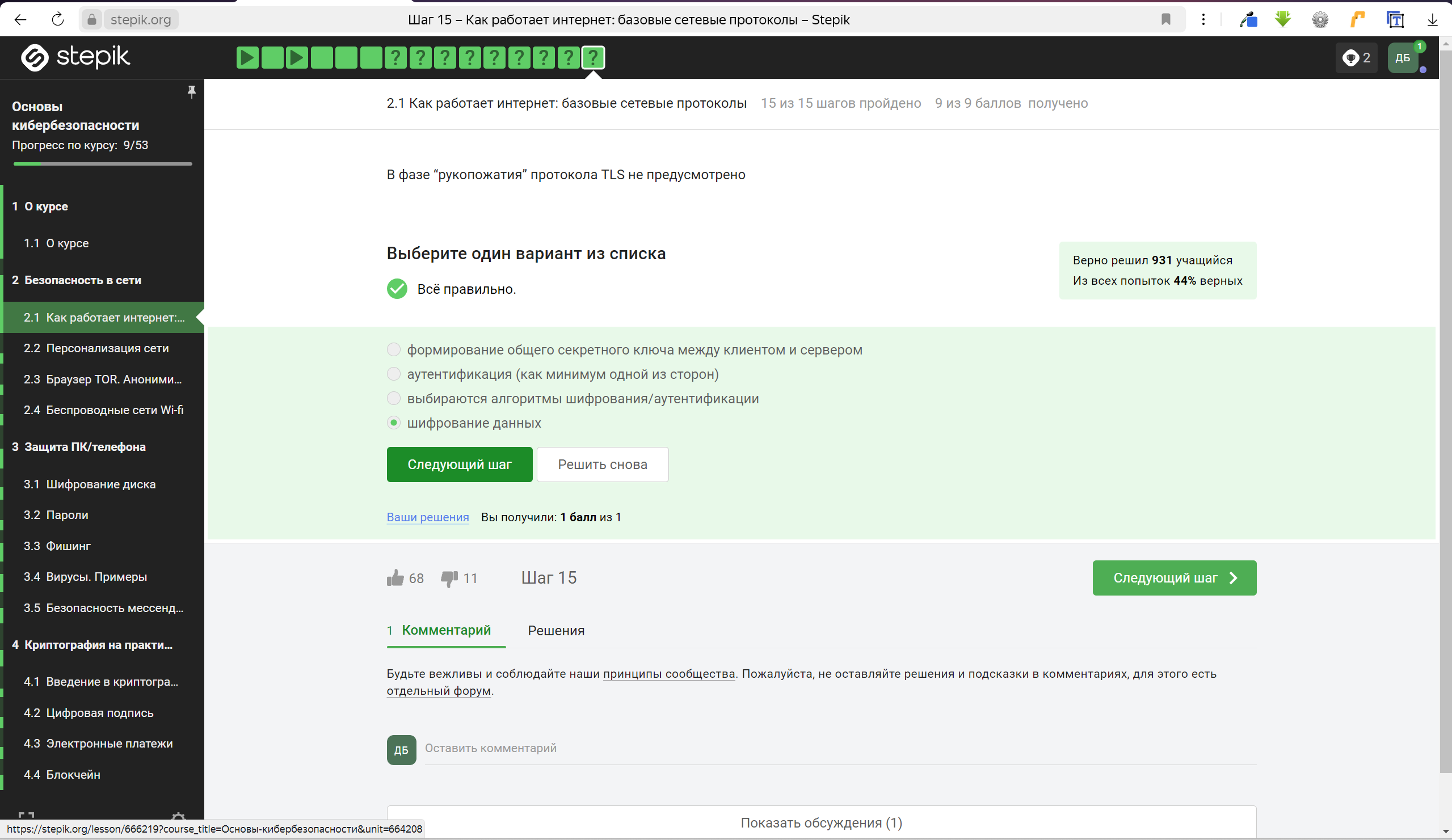


Figure 8: Рис. 9. Раздел (2.1) – Вопрос 9

**Вопрос:** В фазе “рукопожатия” протокола TLS не предусмотрено  
**Ответ:** В фазе “рукопожатия” протокола TLS не предусмотрено шифрование

### 2.1.2 (2.2) “Персонализация сети”

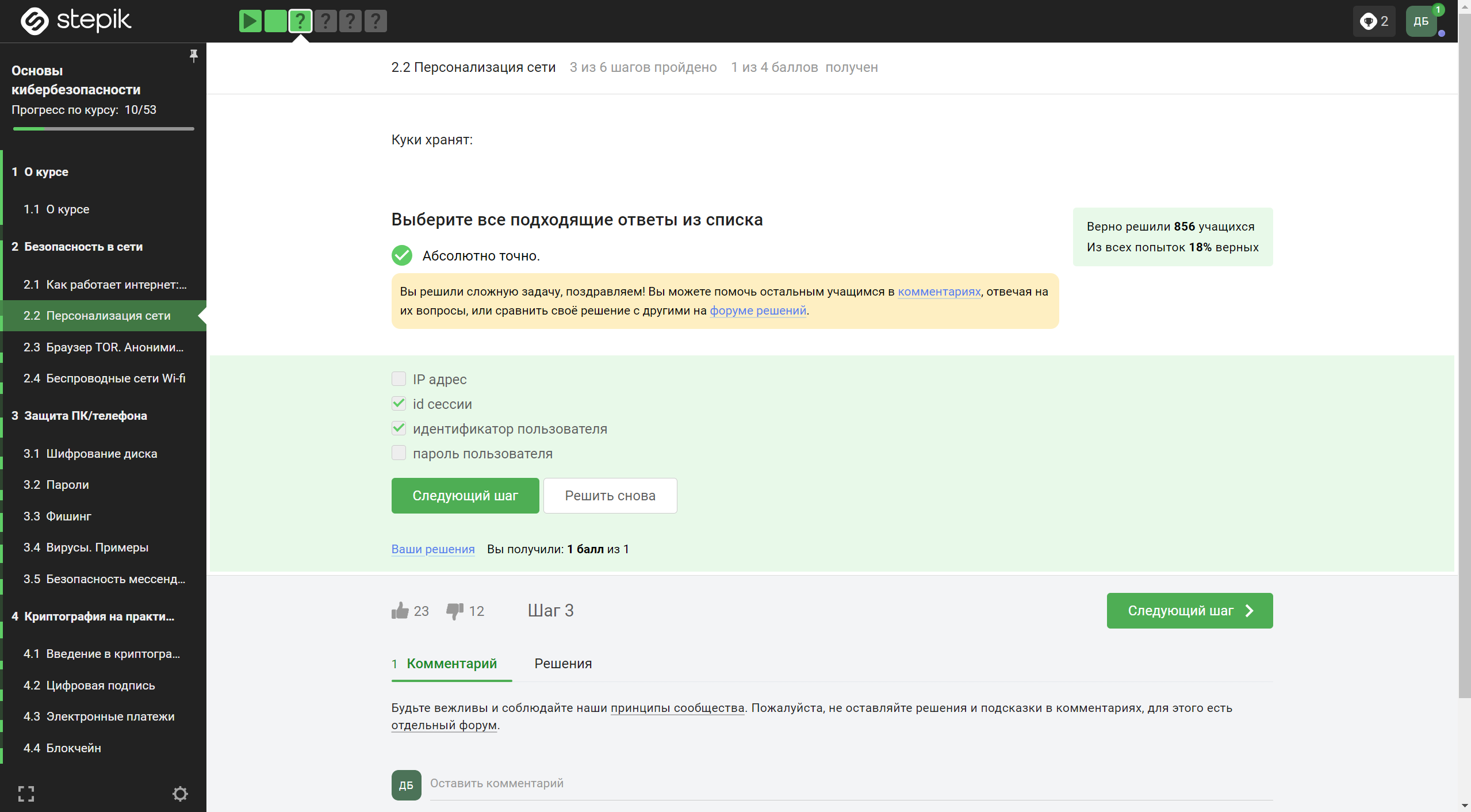


Figure 9: Рис. 10. Раздел (2.2) – Вопрос 1

**Вопрос:** Куки хранят:  
**Ответ:** Куки - это небольшие текстовые файлы, которые веб-сайты могут использовать для хранения информации на компьютере пользователя. IP хранится в базе данных провайдеров интернет-услуг. А пароли пользователей обычно хранятся в базах данных на серверах приложений или веб-сайтов.

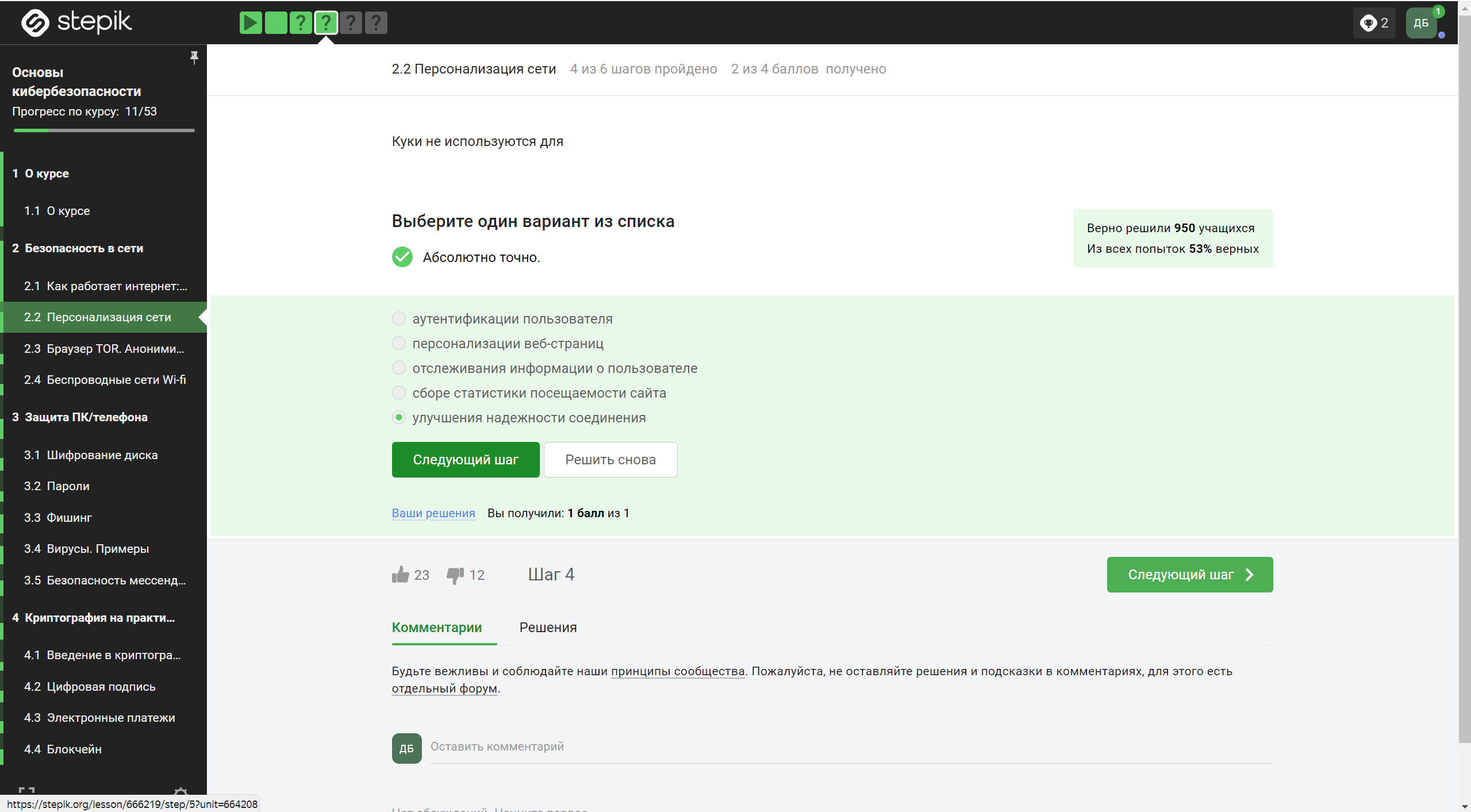


Figure 10: Рис. 11. Раздел (2.2) – Вопрос 2

**Вопрос:** Куки не используются для  
**Ответ:** Для улучшения надежности сетевого соединения используются различные технологии и протоколы (TCP, HTTPS)

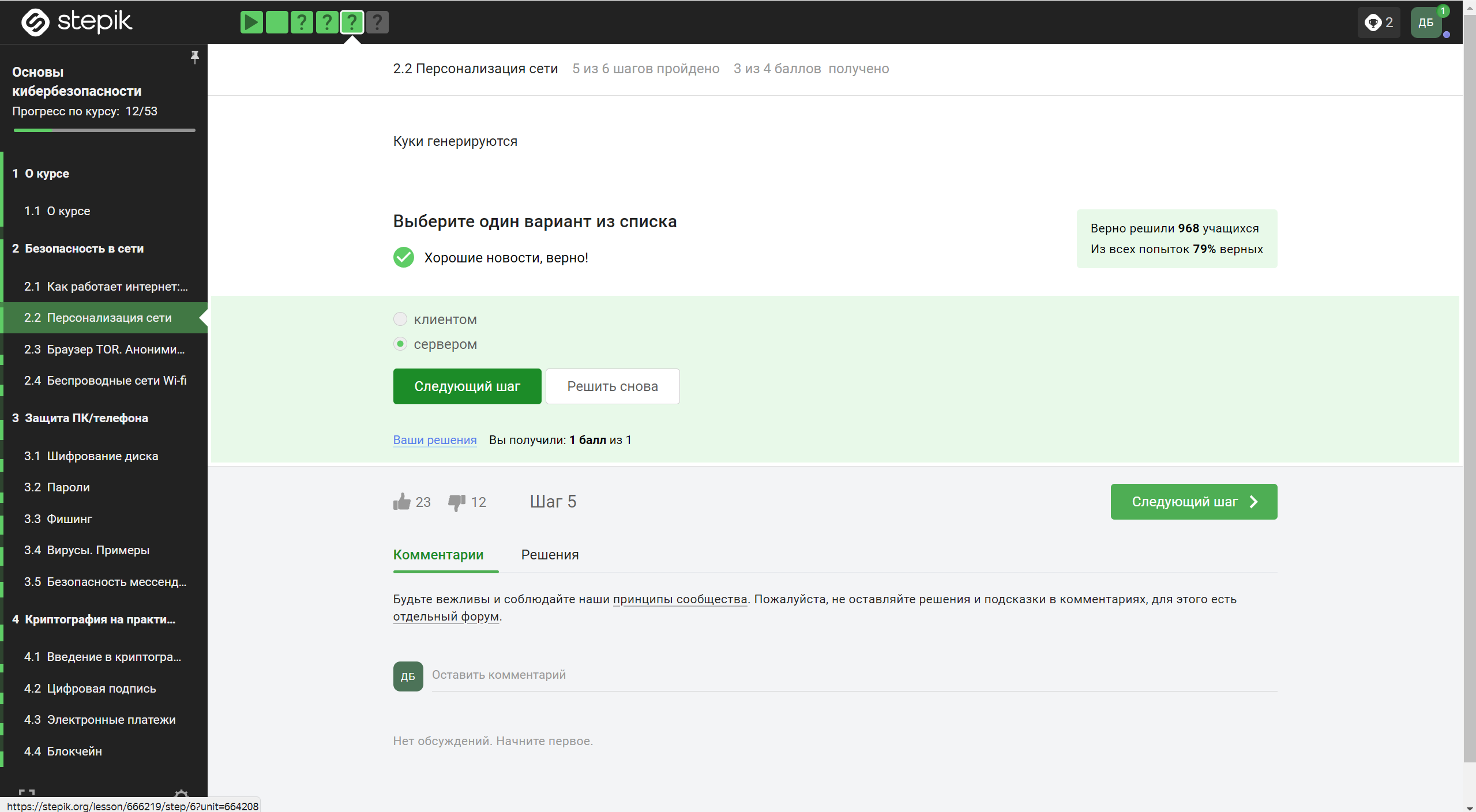


Figure 11: Рис. 12. Раздел (2.2) – Вопрос 3

**Вопрос:** Куки генерируются  
**Ответ:** Когда пользователь посещает веб-сайт, сервер может отправить куки в браузер пользователя для сохранения определённой информации.

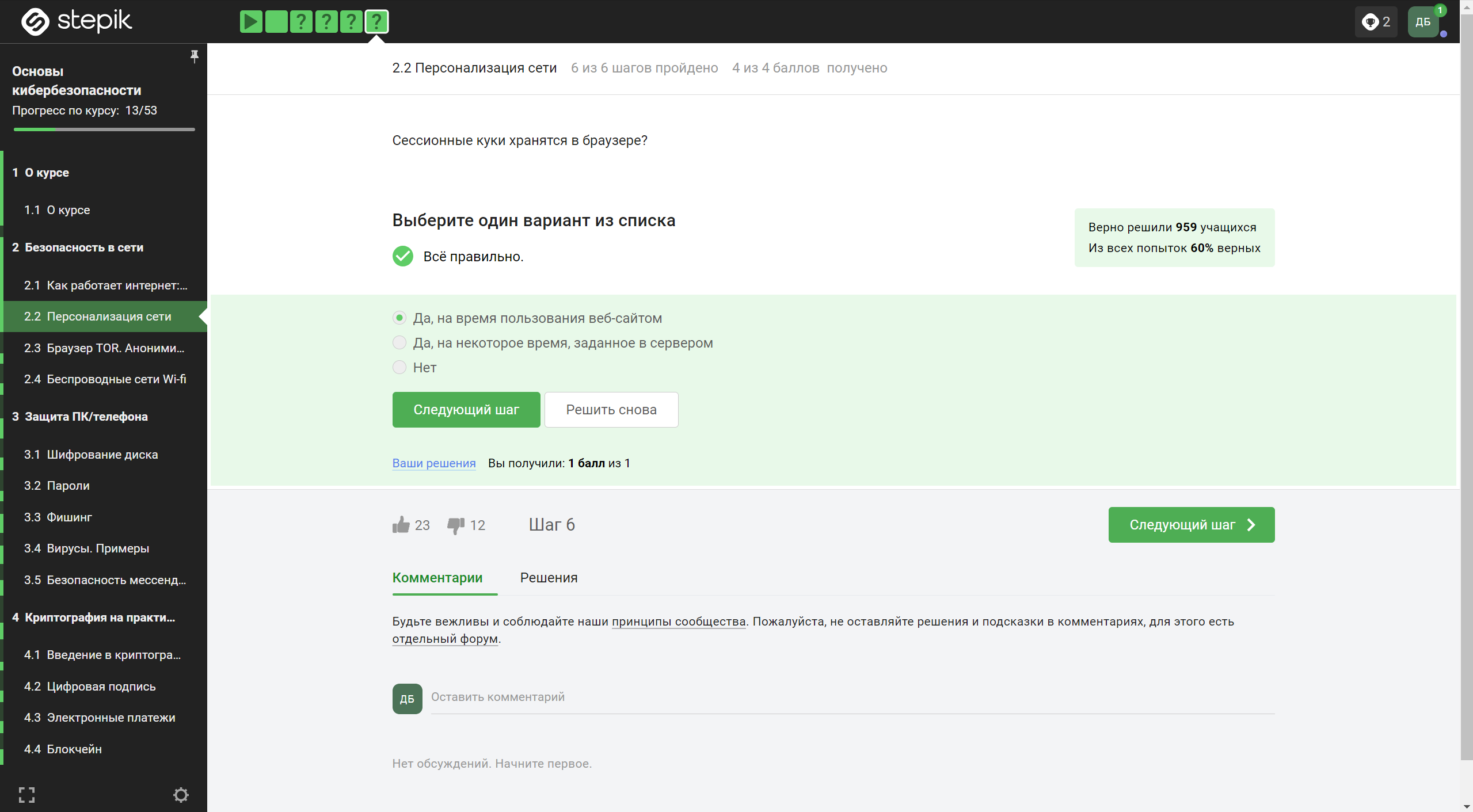


Figure 12: Рис. 13. Раздел (2.2) – Вопрос 4

**Вопрос:** Сессионные куки хранятся в браузере?  
**Ответ:** Сессионные куки хранятся в браузере на время пользования веб-сайтом

### 2.1.3 (2.3) “Браузер TOR. Анонимизация”

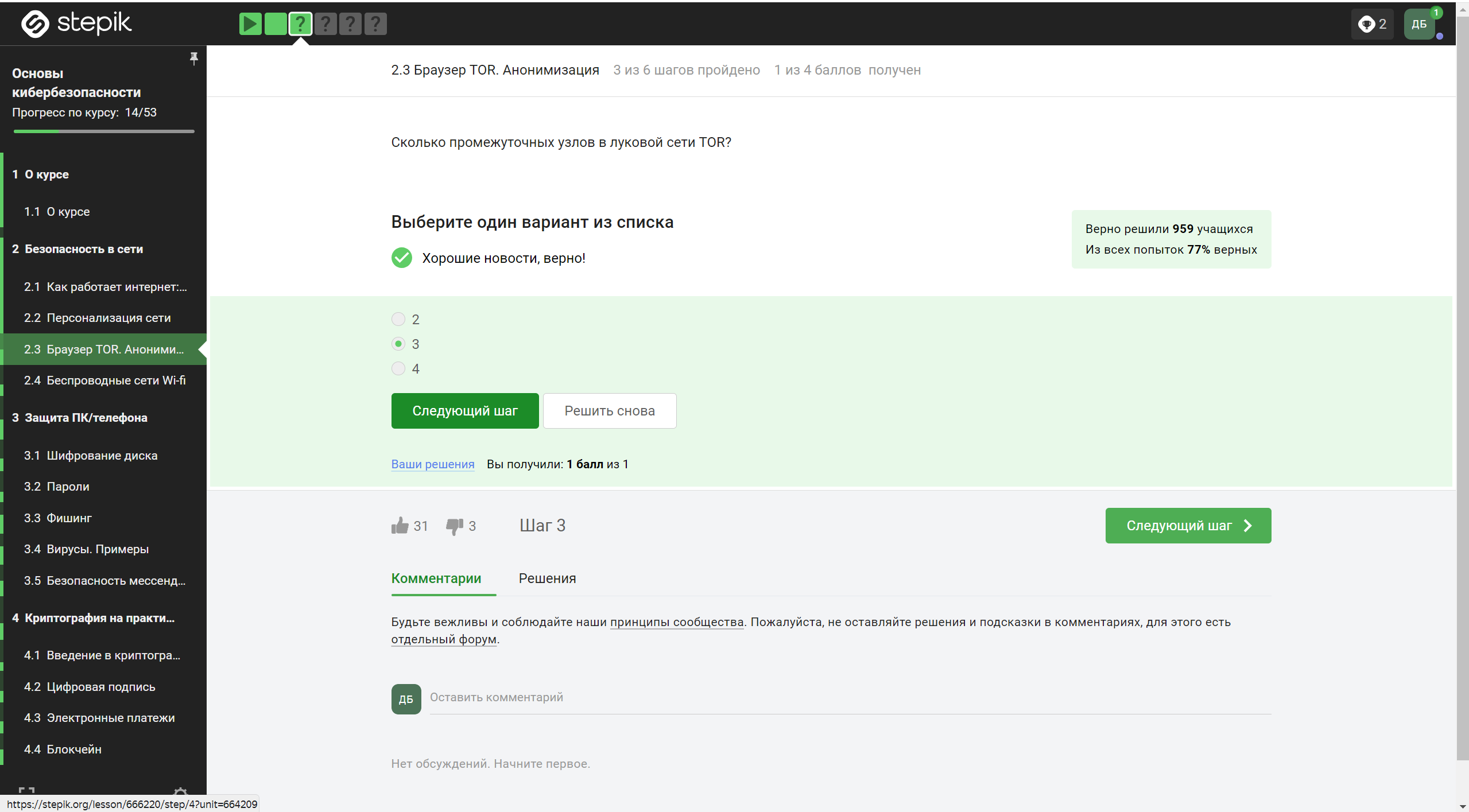


Figure 13: Рис. 14. Раздел (2.3) – Вопрос 1

**Вопрос:** Сколько промежуточных узлов в луковой сети TOR?  
**Ответ:** В сети TOR всего 3 промежуточных узла

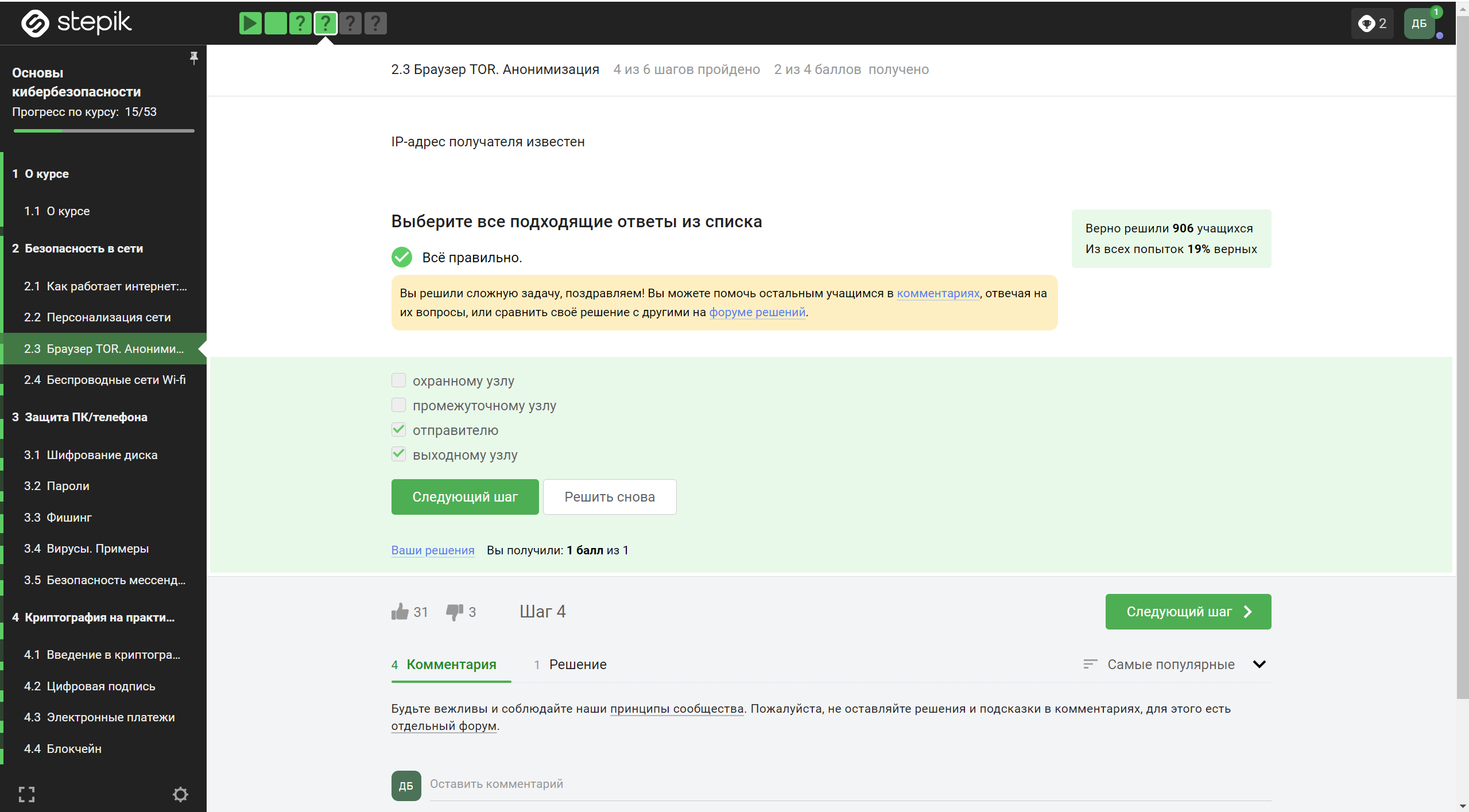


Figure 14: Рис. 15. Раздел (2.3) – Вопрос 2

**Вопрос:** IP-адрес получателя известен  
**Ответ:** IP-адрес получателя известен только отправителю и выходному узлу

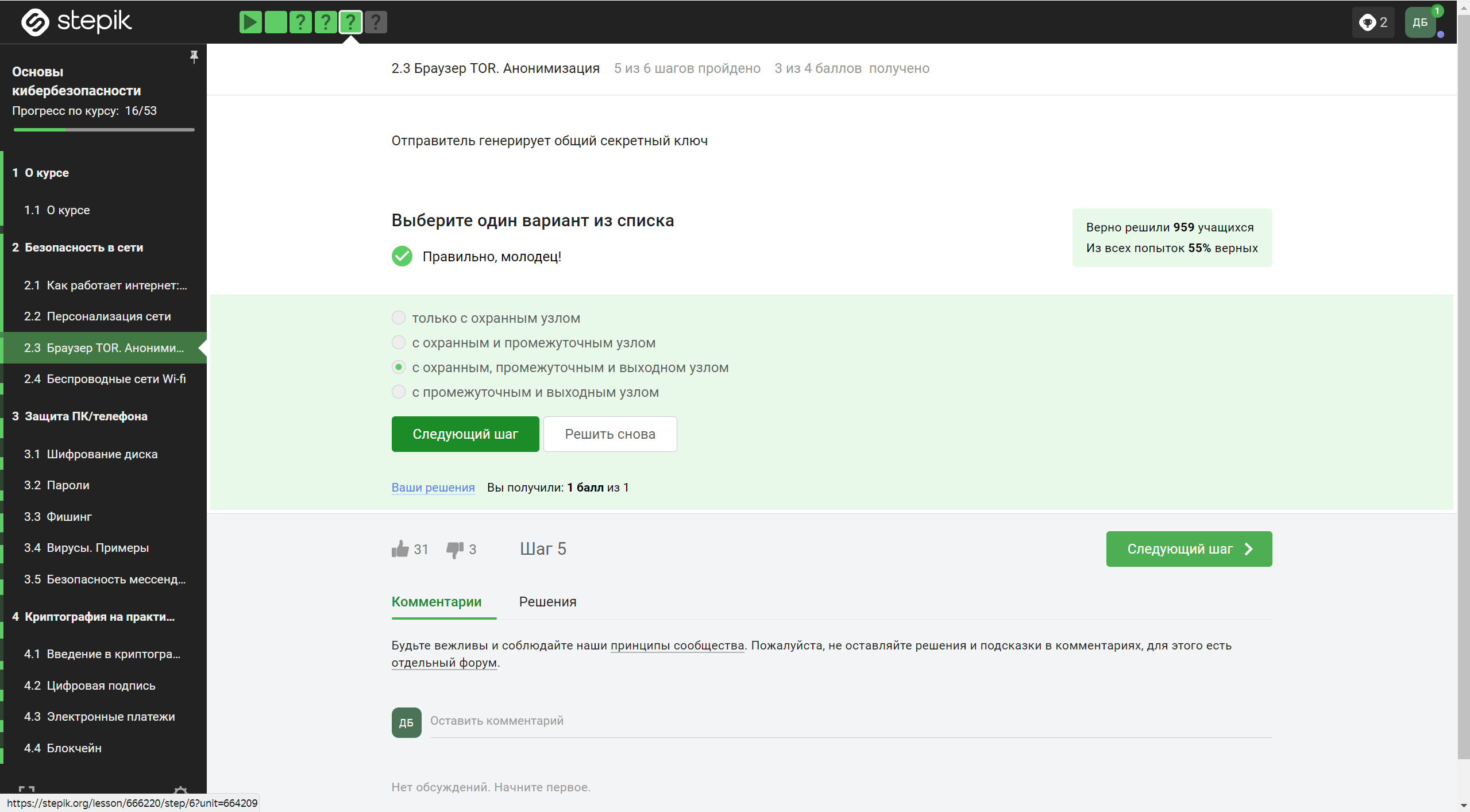


Figure 15: Рис. 16. Раздел (2.3) – Вопрос 3

**Вопрос:** Отправитель генерирует общий секретный ключ  
**Ответ:** Отправитель генерирует общий секретный ключ с охранным, промежуточным и выходным ключом.

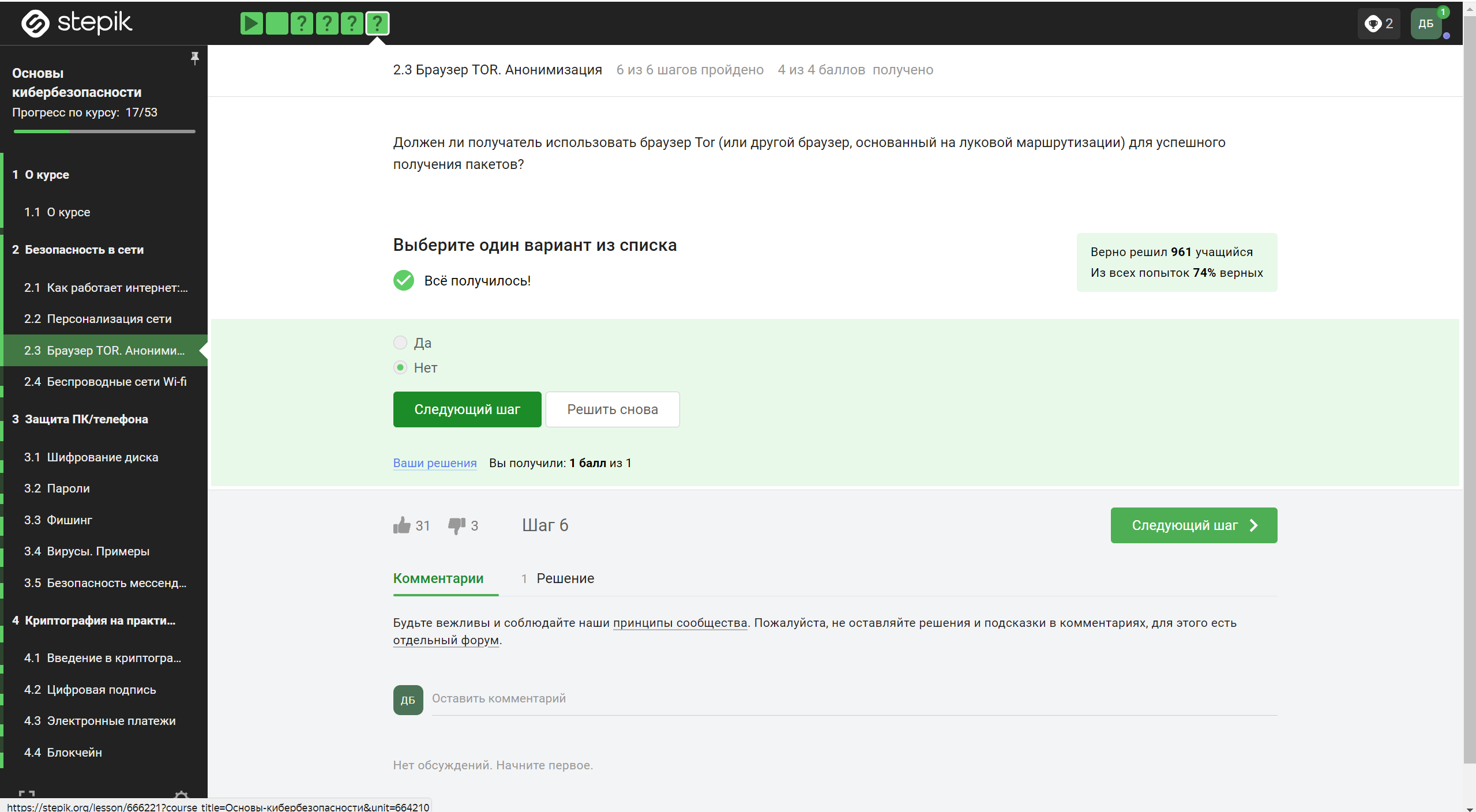


Figure 16: Рис. 17. Раздел (2.3) – Вопрос 4

**Вопрос:** Должен ли получатель использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов?  
**Ответ:** Эти браузеры полезны для обеспечения анонимности в Интернете, а не для успешного получения пакетов.

### 2.1.4 (2.4) “Беспроводные сети Wi-fi”

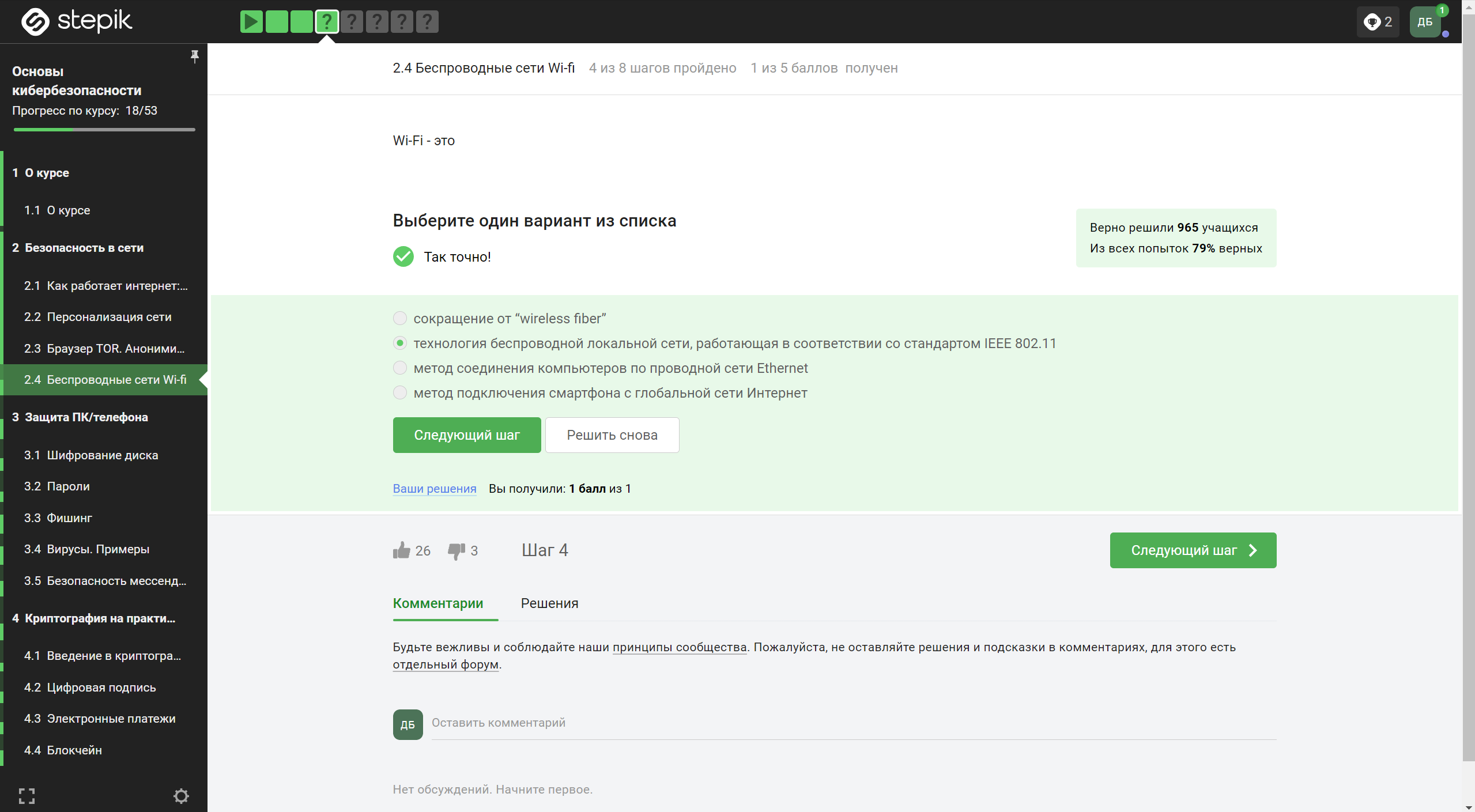


Figure 17: Рис. 18. Раздел (2.4) – Вопрос 1

**Вопрос:** Wi-Fi это  
**Ответ:** Wi-Fi - это беспроводная технология, которая позволяет электронным устройствам подключаться к интернету или обмениваться данными через радиоволны без физического подключения к проводной сети.

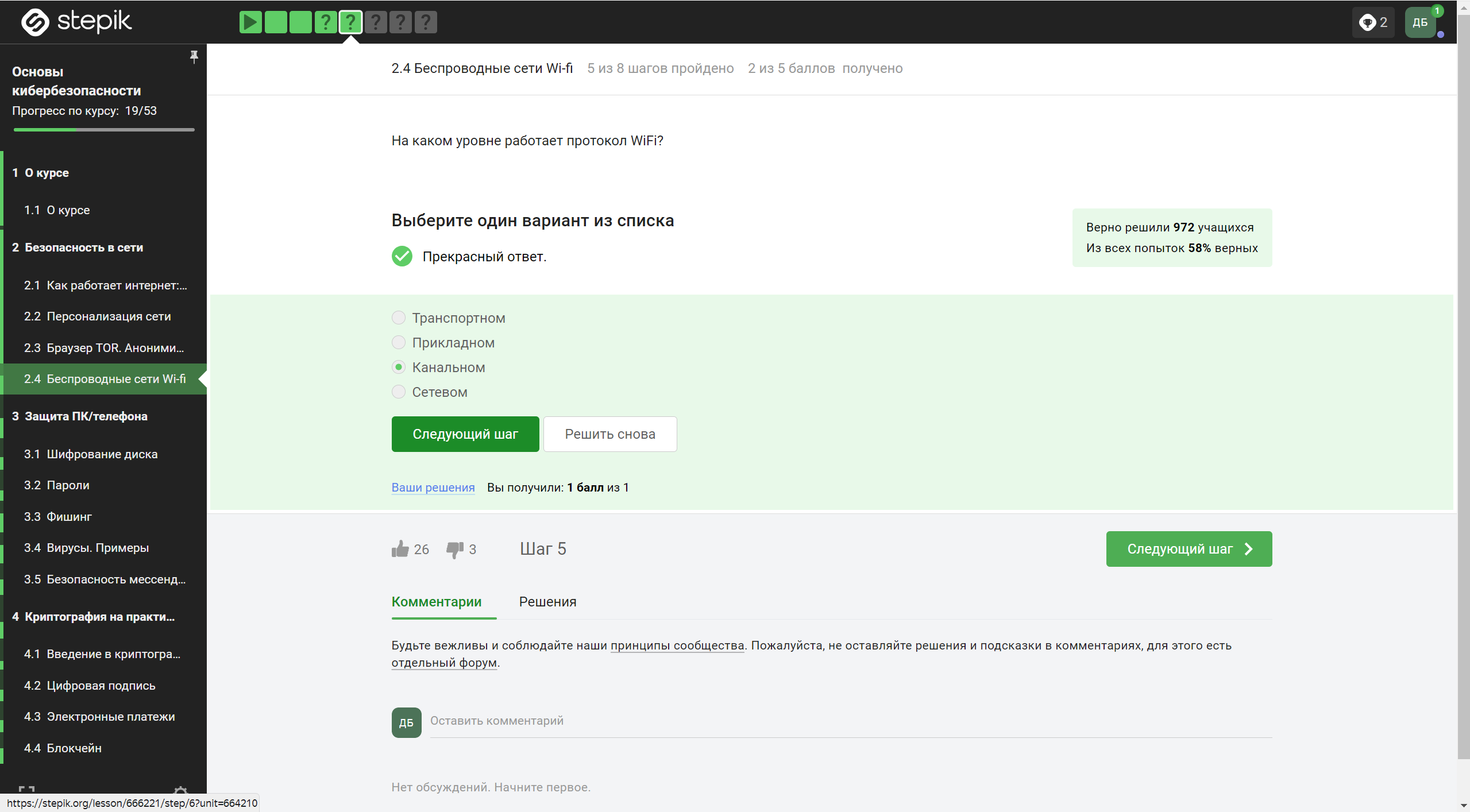


Figure 18: Рис. 19. Раздел (2.4) – Вопрос 2

**Вопрос:** На каком уровне работает протокол WiFi?  
**Ответ:** WiFi протокол работает на канальном уровне

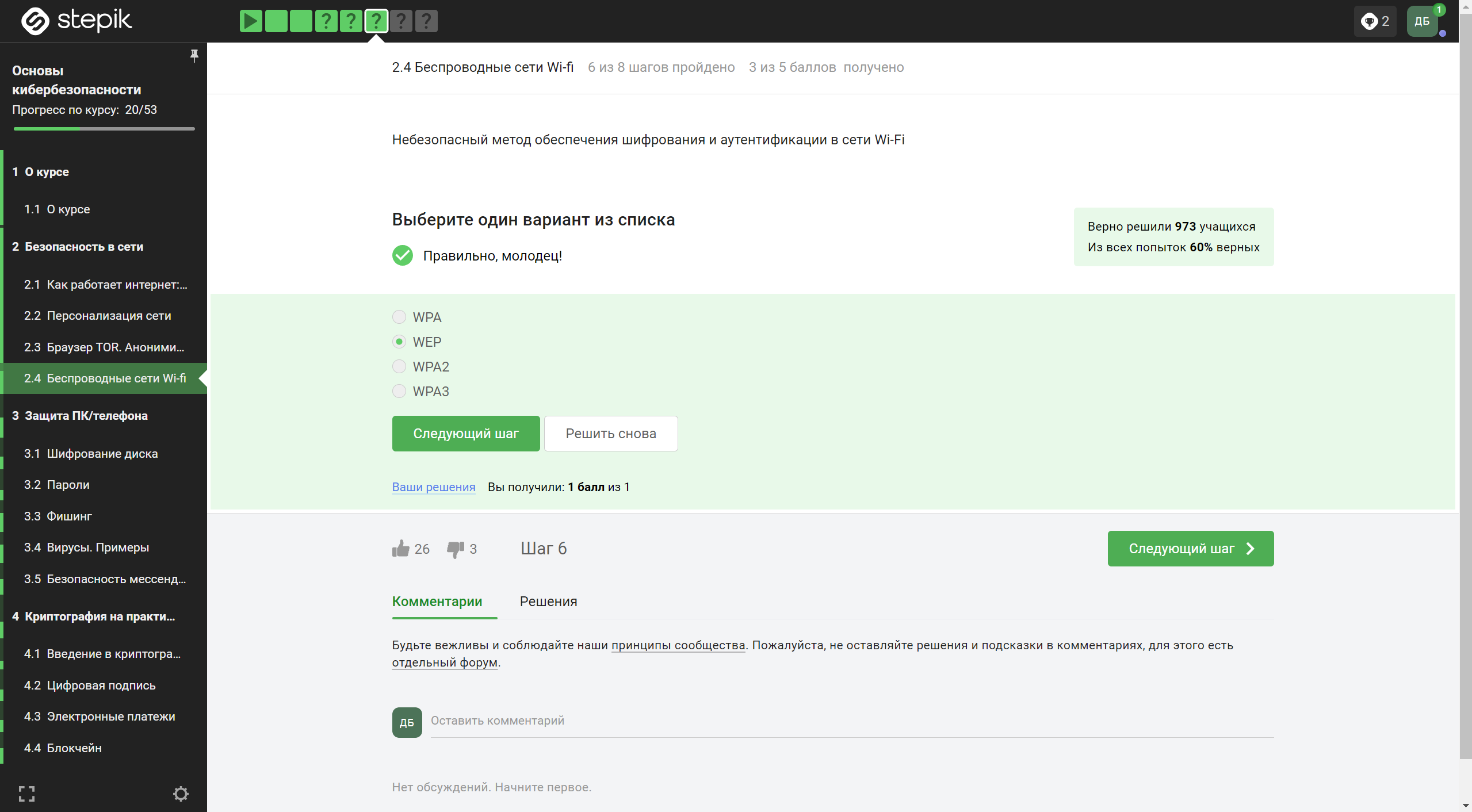


Figure 19: Рис. 20. Раздел (2.4) – Вопрос 3

**Вопрос:** Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi  
**Ответ:** WEP считается небезопасным для шифрования и аутентификации в Wi-Fi

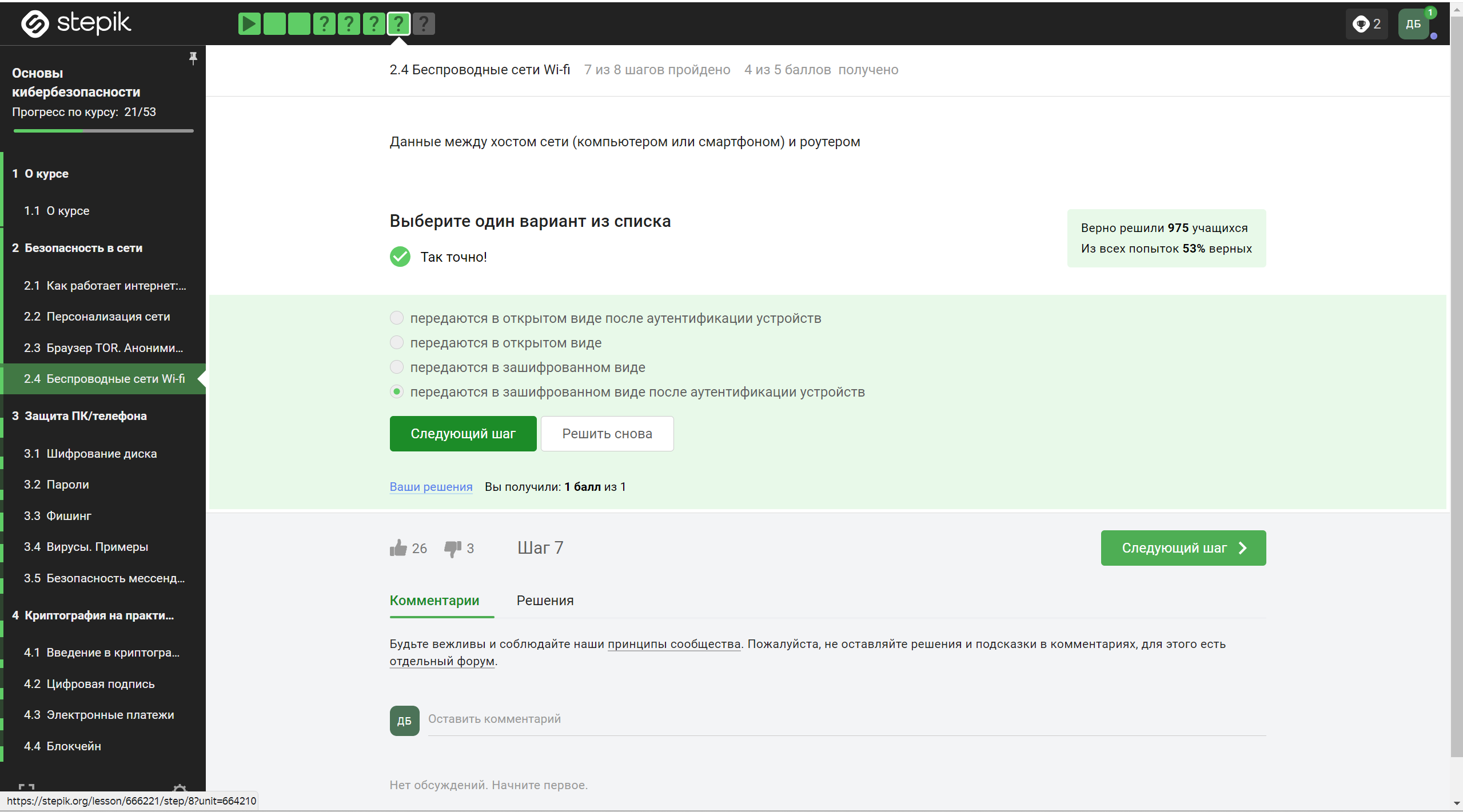


Figure 20: Рис. 21. Раздел (2.4) – Вопрос 4

**Вопрос:** Данные между хостом сети (компьютером или смартфоном) и роутером  
**Ответ:** Данные между хостом сети (компьютером или смартфоном) и роутером передаются в зашифрованном виде после аутентификации устройств

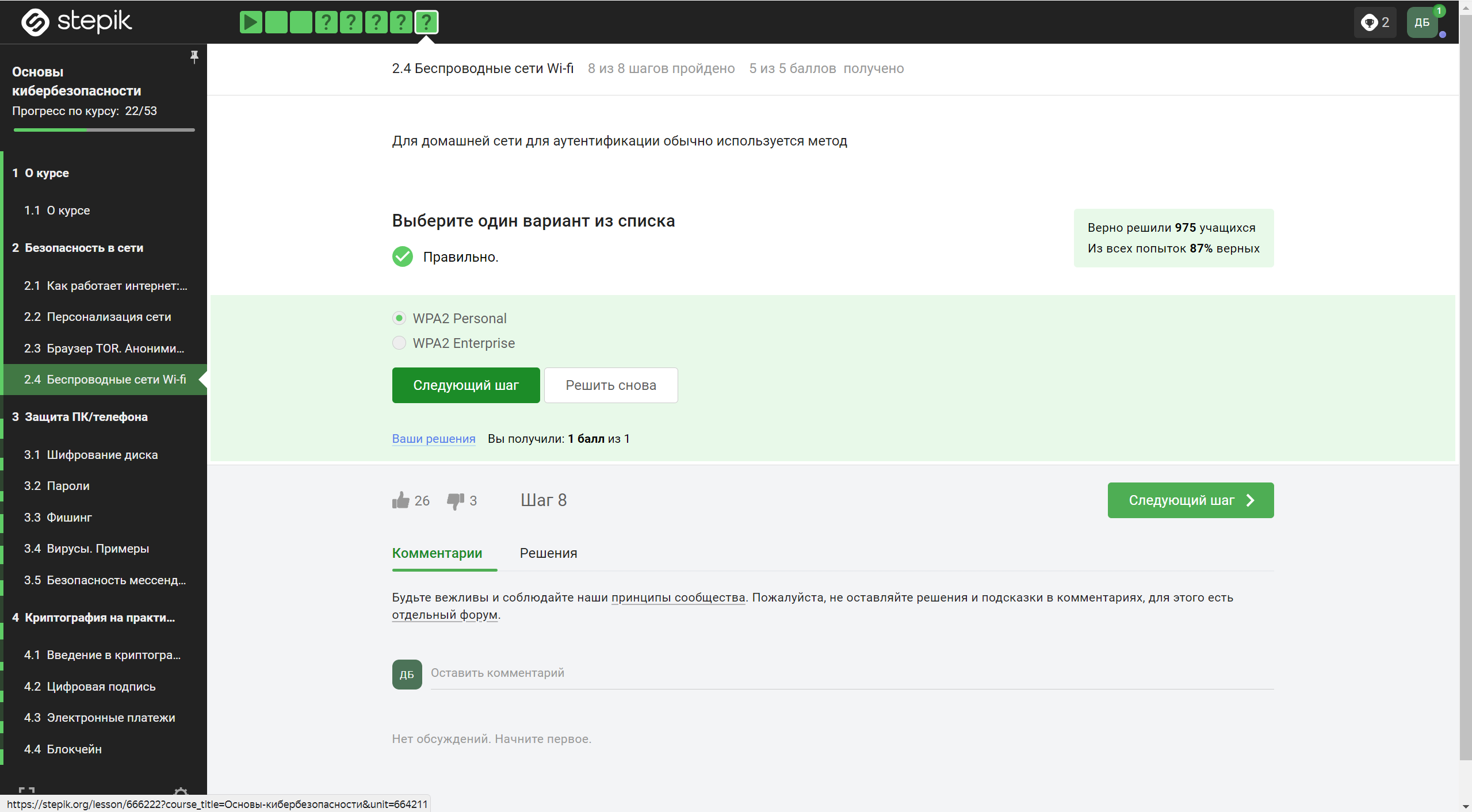


Figure 21: Рис. 22. Раздел (2.4) – Вопрос 5

**Вопрос:** Для домашней сети для аутентификации обычно используется метод  
**Ответ:** Для домашней сети для аутентификации обычно используется метод WPA2 Personal

# 3 Вывод

В ходе прохождения внешних курсов были получены навыки о “Безопасности в сети”, “Защите ПК/телефона” и “Криптографии”.