Прохождения внешнего курса на тему Основы кибербезопасности. Часть 1

Основы информационной безопасности

Тойчубекова Асель Нурлановна

Содержание

# 1 1 О курсе

В этом разделе описана общая информация о курсе, определены цели и дальнейшие планы по курсу. Также даны ссылки на литературу и полезные ссылки.

# 2 2 Безопасность в сети

## 2.1 2.1 Как работает интернет: базовые сетевые протоколы

Вопрос/Ответ 1 (рис. 1)

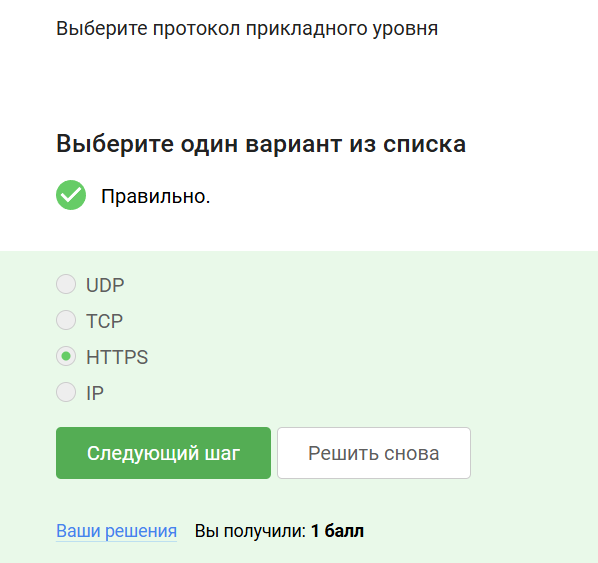


Рис. 1: Вопрос/Ответ 1

Пояснение ответа: Протоколы UDP, TCP относятся к транспортному уровню, HTTPS к прикладному, IP к сетевому уровню.

Вопрос/Ответ 2 (рис. 2)

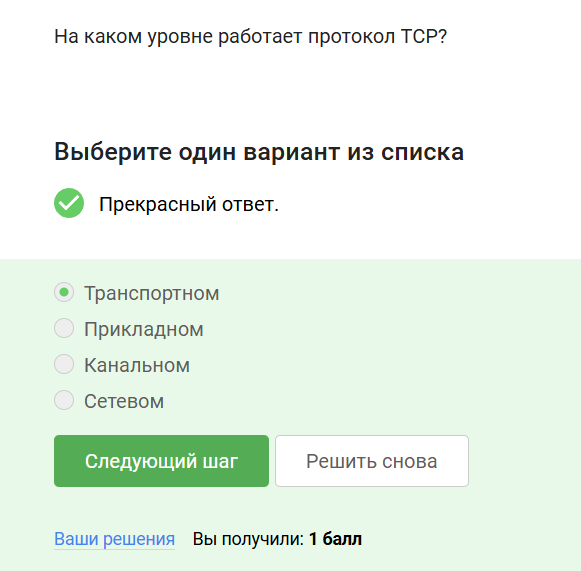


Рис. 2: Вопрос/Ответ 2

Пояснение ответа: Протокол TCP работает на транспортном уровне и отвечает за надежную передачу данных.

Вопрос/Ответ 3 (рис. 3)

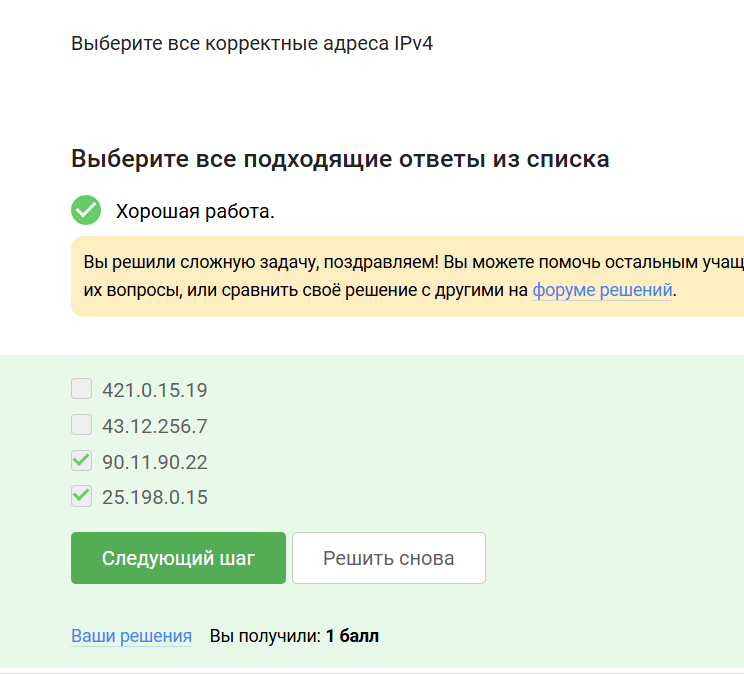


Рис. 3: Вопрос/Ответ 3

Пояснение ответа: В 4 версии ip адрес представляет собой 32 битное число, записывается в виде четырех десятичных чисел значения от 0 до 255(8 битов). Из чего следует, что 421.0.15.19 и 43.12.256.7 не подходят.

Вопрос/Ответ 4 (рис. 4)

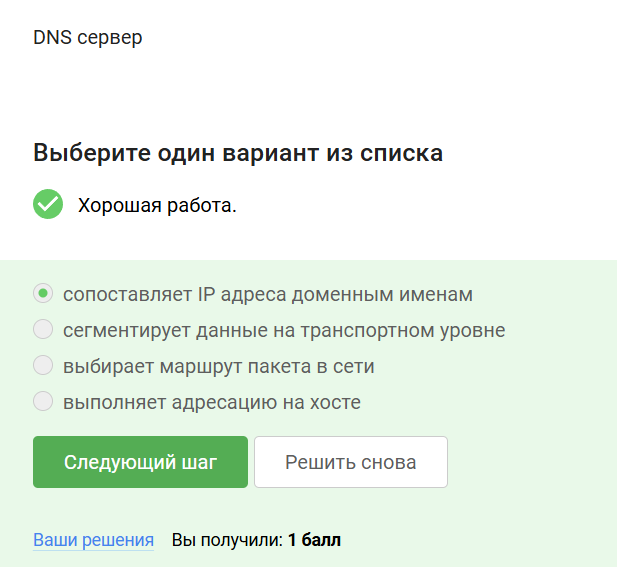


Рис. 4: Вопрос/Ответ 4

Пояснение ответа: Основная задача DNS сервера это сопоставить название, то есть доменное имя, с корректным ip адресом, с тем, где лежит этот сервер, этот сайт.

Вопрос/Ответ 5 (рис. 5)

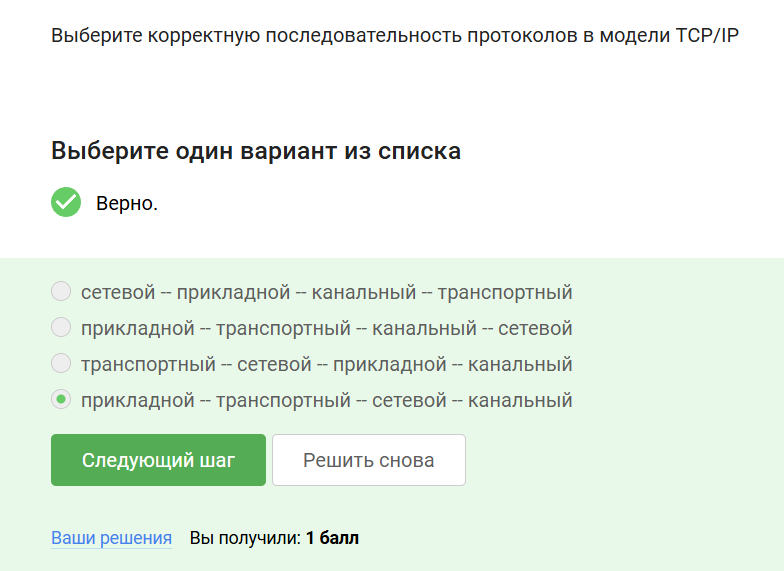


Рис. 5: Вопрос/Ответ 5

Пояснение ответа: Модель TCP/IP состоит из четырех уровней: - Прикладной

* Транспортный
* Сетевой
* Канальный

Вопрос/Ответ 6 (рис. 6)

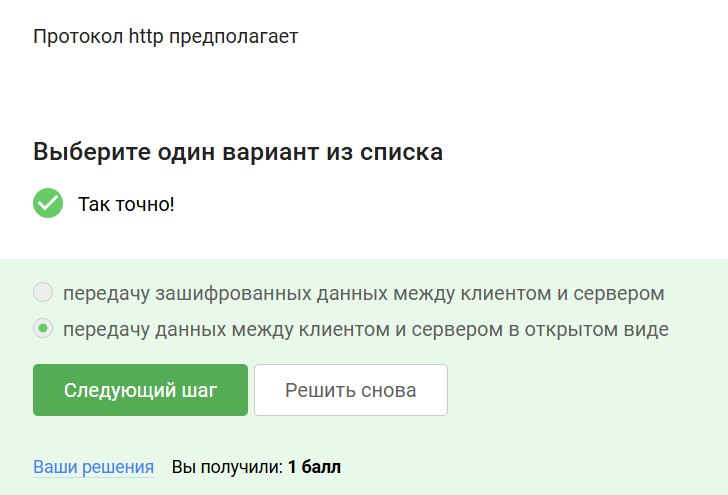


Рис. 6: Вопрос/Ответ 6

Пояснение ответа: Протокол прикладного уровня http в отличие от https передает данные между клиентом и сервером в открытом виде.

Вопрос/Ответ 7 (рис. 7)

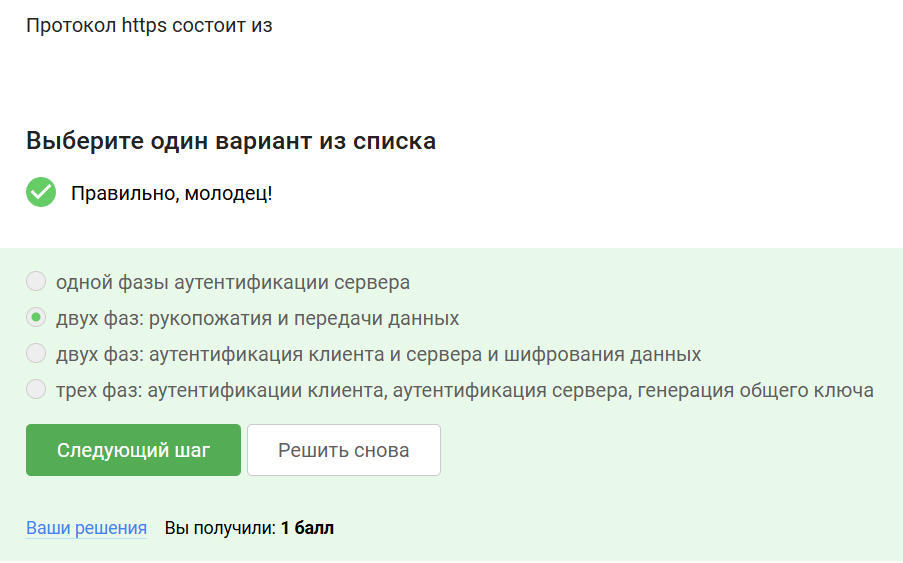


Рис. 7: Вопрос/Ответ 7

Пояснение ответа: Протокол https состоит из двух фаз:

* Рукопожатие(идентификация между сервером и клиентом)
* Передача данных

Вопрос/Ответ 8 (рис. 8)

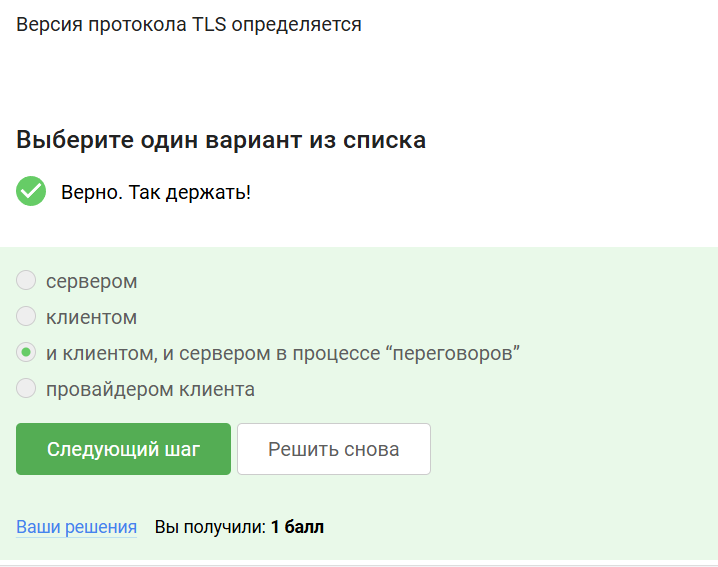


Рис. 8: Вопрос/Ответ 8

Пояснение ответа: В ходе TLS-рукопожатия клиент и сервер совместно авполняют следующие действия:

* Указывают какую версию TLS они будут использовать
* Какие наборы шрифтов они будут использовать
* Аутентификация идентичности сервера с помощью открытого ключа сервера и цифровой подписи центра сертификации ssl
* Генерация сеансовых ключей для использования симметричного шифрования после завершения рукопожатия.

Вопрос/Ответ 9 (рис. 9)

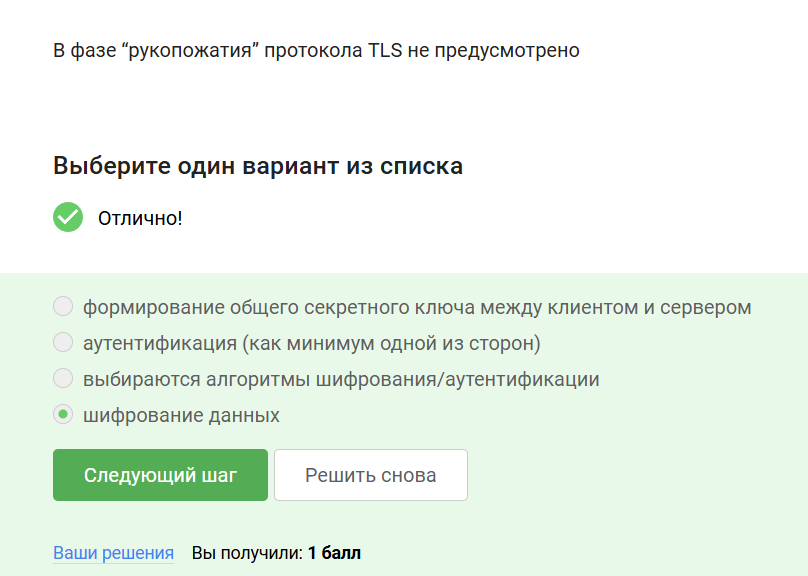


Рис. 9: Вопрос/Ответ 9

Пояснение ответа: Рукопожатие - идентификация между сервером и клиентом, оно не подразумевает шифрование данных.

## 2.2 2.2 Персонализация сети

Вопрос/Ответ 1 (рис. 10)

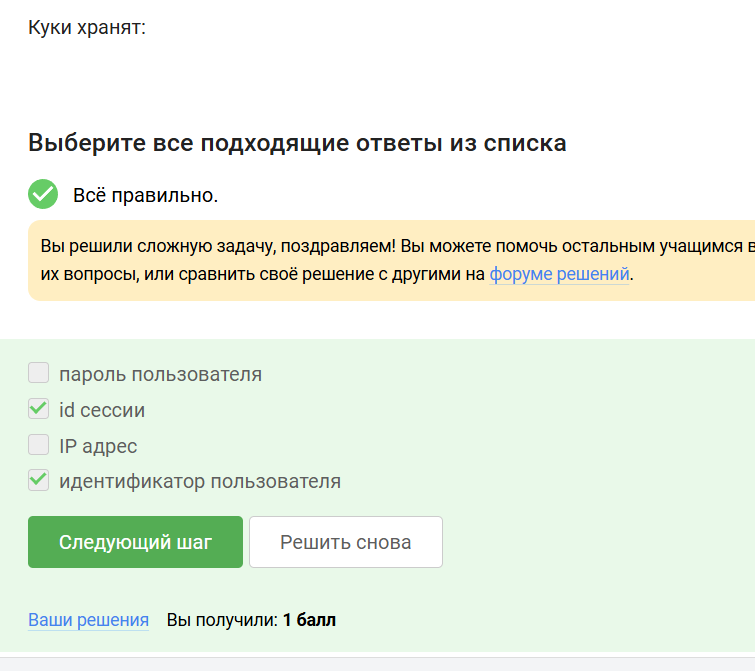


Рис. 10: Вопрос/Ответ 1

Пояснение ответа: Куки хранят:

* id пользователя
* id сессии
* тип браузера, время запросов
* некоторые действия пользователя

Вопрос/Ответ 2 (рис. 11)

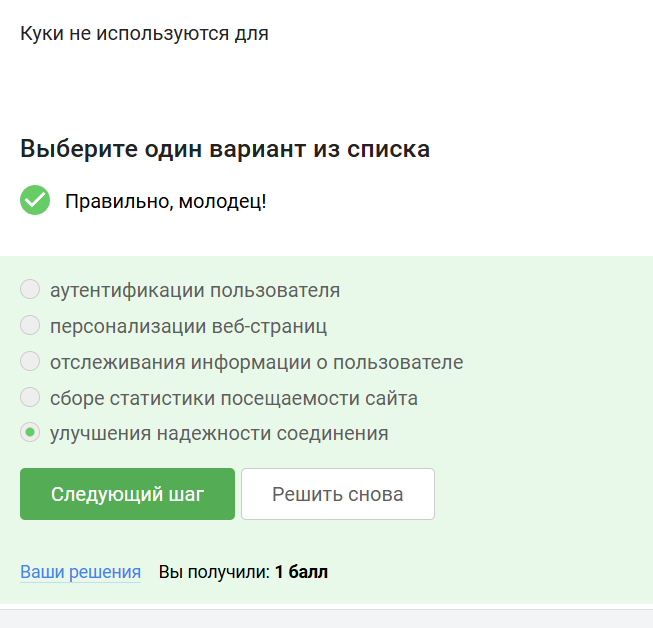


Рис. 11: Вопрос/Ответ 2

Пояснение ответа: Куки - данные, передаваемые от сервера к клиенту для его идентификации. Куки позволяют:

* Сохранять сессионную информацию
* Персонализировать страницы

Вопрос/Ответ 3 (рис. 12)

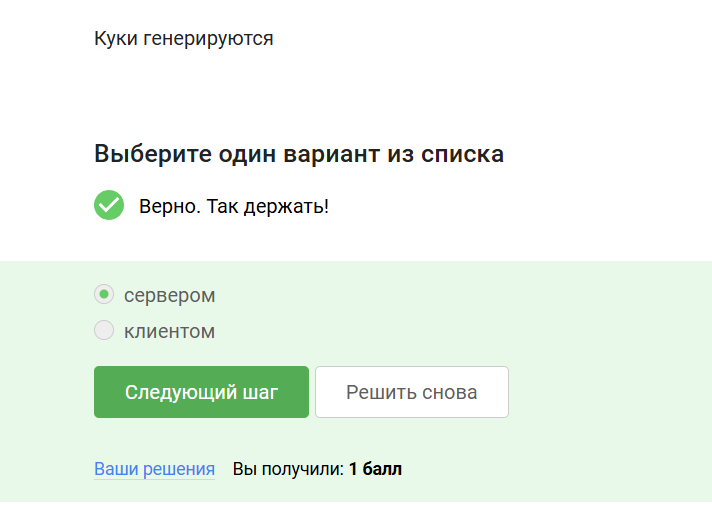


Рис. 12: Вопрос/Ответ 3

Пояснение ответа: Куки генерируется сервером, и запрашивает разрешение на использование клиентом.

Вопрос/Ответ 4 (рис. 13)

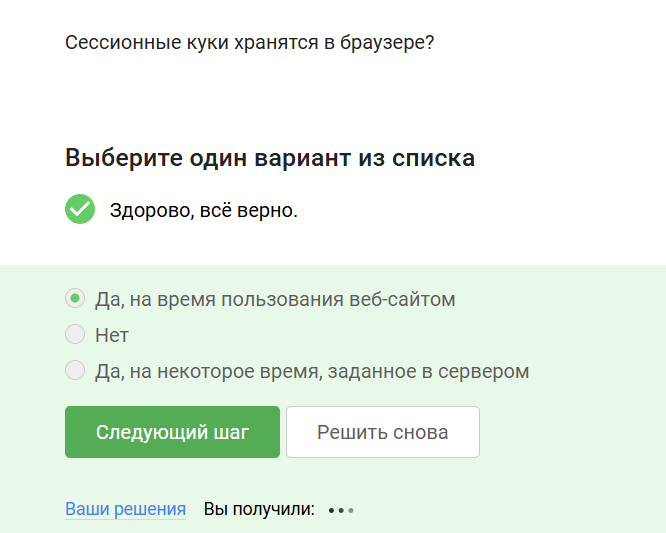


Рис. 13: Вопрос/Ответ 4

Пояснение ответа: Сессионные куки хранятся в браузере на время пользование веб сайтом.

## 2.3 2.3 Браузер TOR. Анонимизация

Вопрос/Ответ 1 (рис. 14)

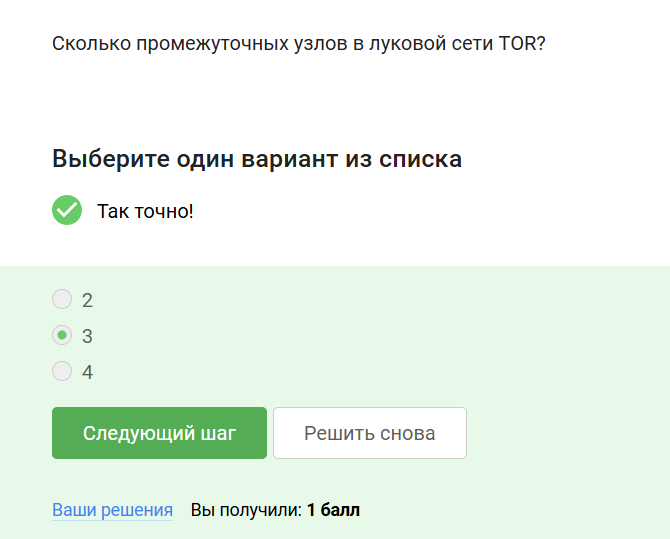


Рис. 14: Вопрос/Ответ 1

Пояснение ответа: В луковой сети TOR три промежуточных узла:

* Охранный узел
* Промежуточный узел
* Выходной узел

Вопрос/Ответ 2 (рис. 15)

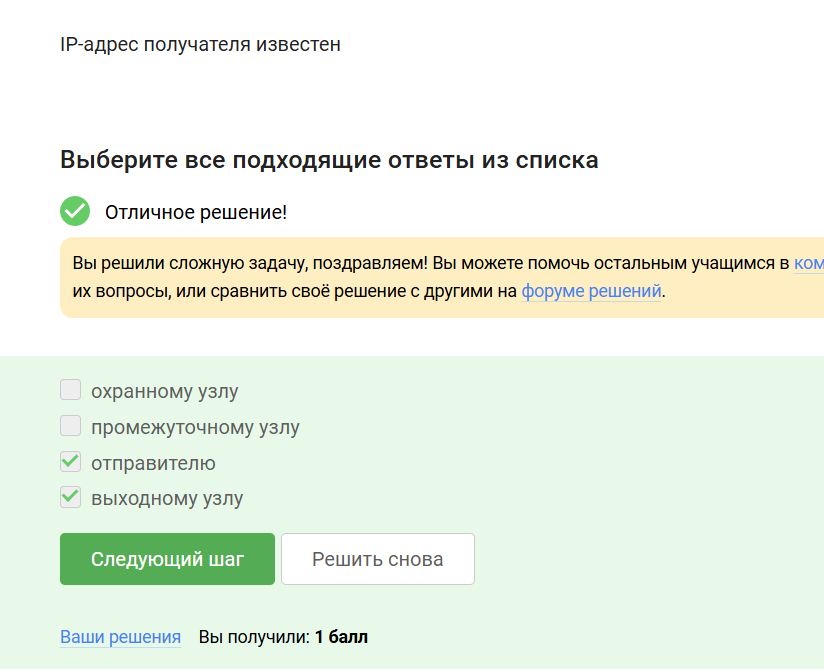


Рис. 15: Вопрос/Ответ 2

Пояснение ответа: IP адрес отправителя известен только отправителю и выходному узлу, в охранном и промежуточном узле он зашифрован.

Вопрос/Ответ 3 (рис. 16)

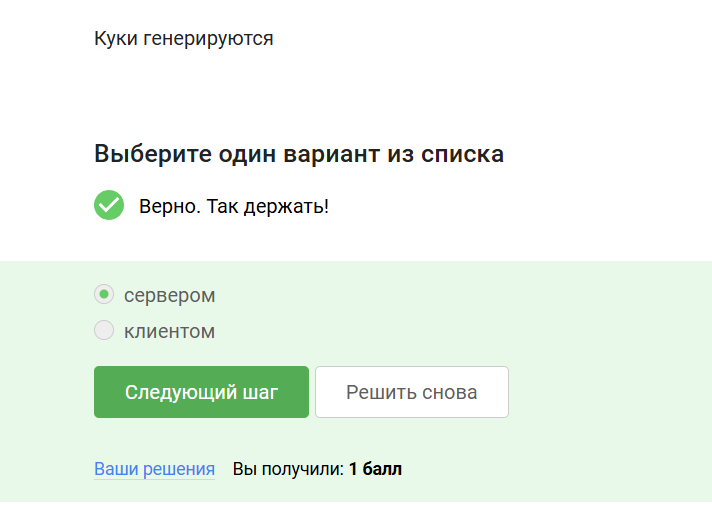


Рис. 16: Вопрос/Ответ 3

Пояснение ответа: Отправитель генерирует общий секретный ключ со всеми узлами(охранным, промежуточным, выходным), они одеты друг на друга как оболочка у лука.

Вопрос/Ответ 4 (рис. 17)

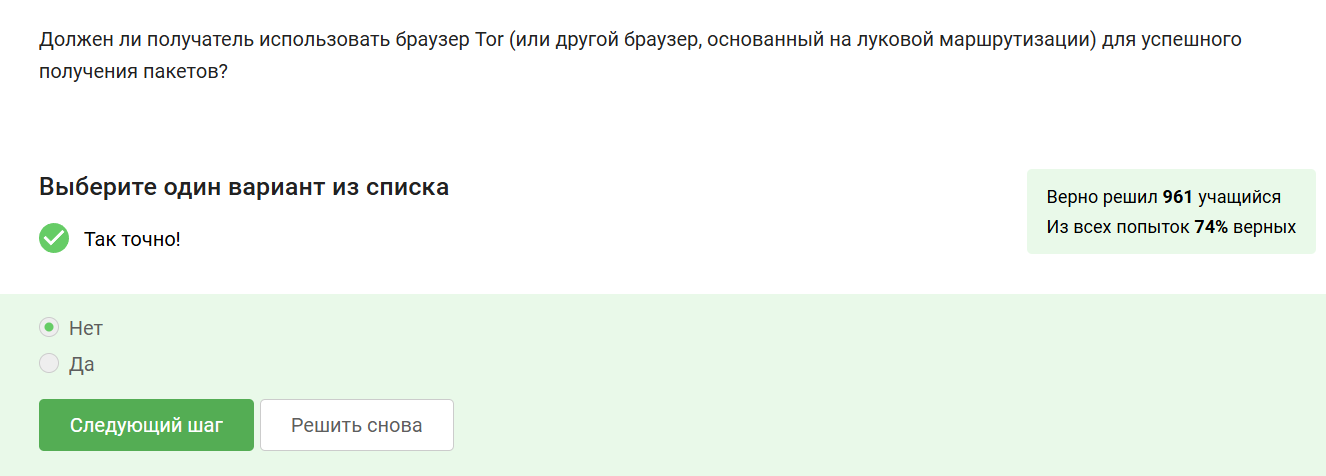


Рис. 17: Вопрос/Ответ 4

Пояснение ответа: Получателю не обязательно использовать браузер TOR для успешного получения пакетов.

## 2.4 2.4 Беспроводные сети WiFi

Вопрос/Ответ 1 (рис. 18)

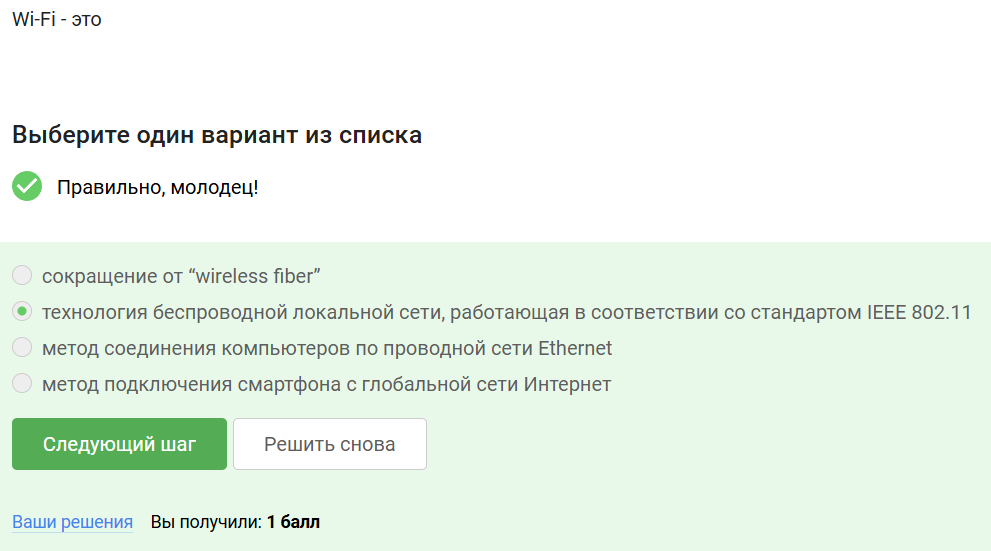


Рис. 18: Вопрос/Ответ 1

Пояснение ответа: WiFi - технология беспроводной локальной сети, работающей в соответствии со стандартами IEEE 802.11.

Вопрос/Ответ 2 (рис. 19)

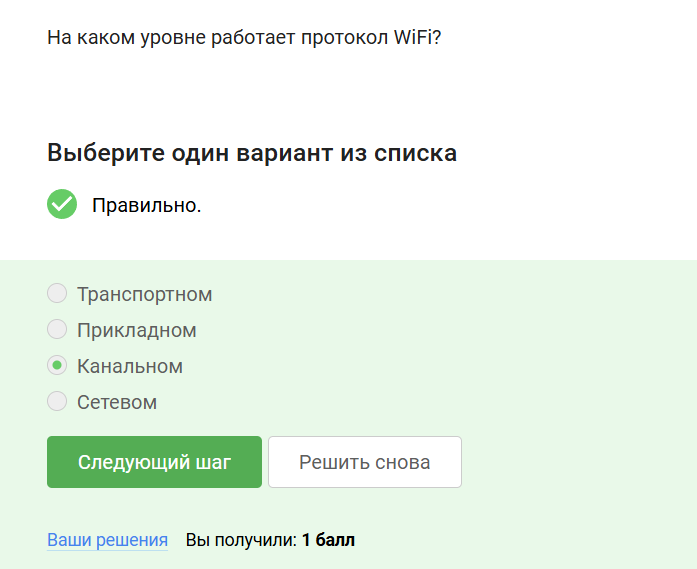


Рис. 19: Вопрос/Ответ 2

Пояснение ответа: Протокол WiFi работает на самом низком уровне, канальном уровне.

Вопрос/Ответ 3 (рис. 20)

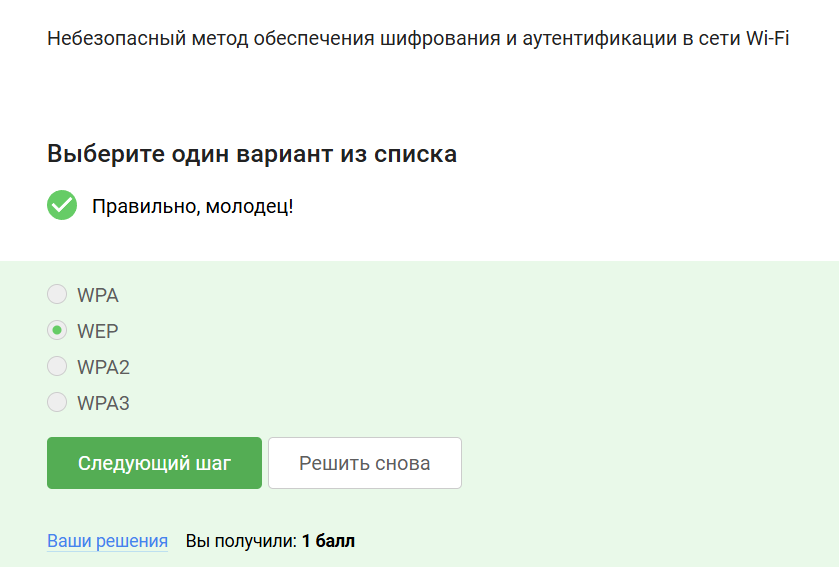


Рис. 20: Вопрос/Ответ 3

Пояснение ответа: Самым ранним и на сегодняшний день небезопасный метод шифрования данных WiFi называется WEP. Он устарел и уже категорически не рекомендуется к использованию, потому что использовал малую длину ключа, 40 бит.

Вопрос/Ответ 4 (рис. 21)

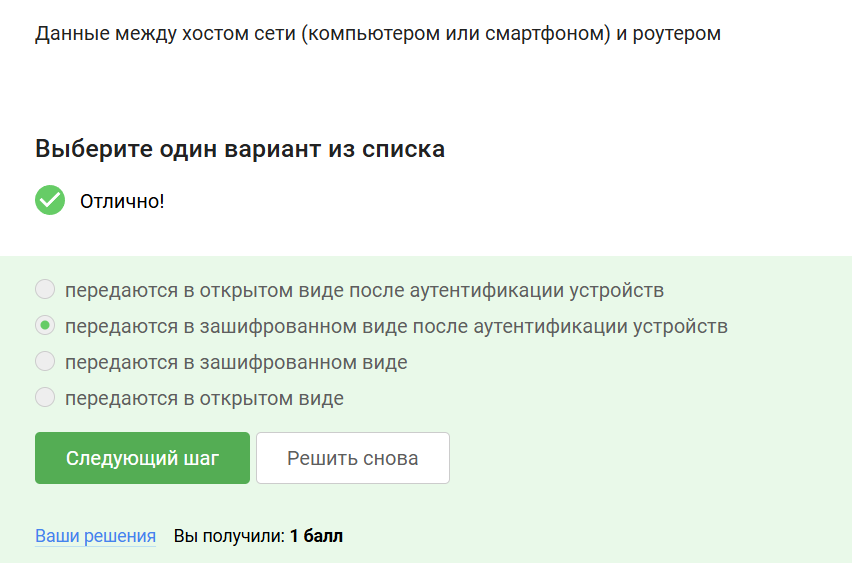


Рис. 21: Вопрос/Ответ 4

Пояснение ответа: Данные между хостом сети и роутером передаются в зашифрованном виде после аутентификации устройств.

Вопрос/Ответ 5 (рис. 22)

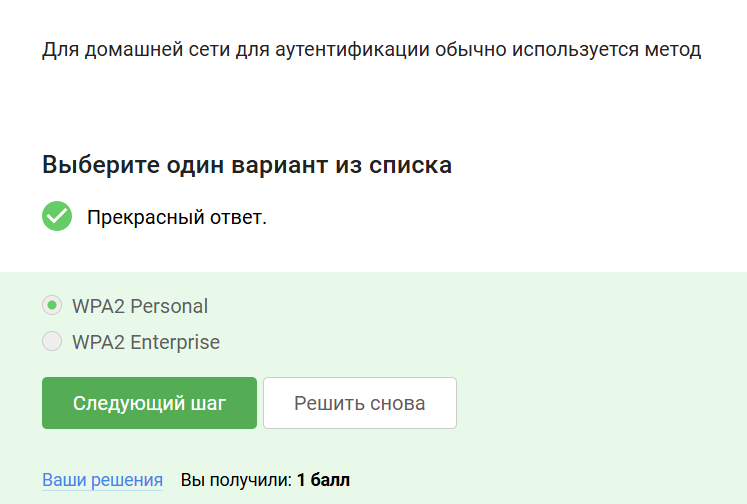


Рис. 22: Вопрос/Ответ 5

Пояснение ответа: Для домашней сети для аутентификации обычно используется метод WPA2 Personal, который использует пароль для аутентификации, в то время как WPA2 Enterprise использует базу данных с пользователями, которые могут подключиться к WiFi.