Отчет по этапу выполнения внешнего курса

Безопасность в сети

Татьяна Александровна Буллер

Содержание

# 1 Цель работы

Получение и закрепление на практике знаний об основных механизмах работы сети Интернет и их слабых местах.

# 2 Выполнение контрольных заданий

## 2.1 Как работает Интернет

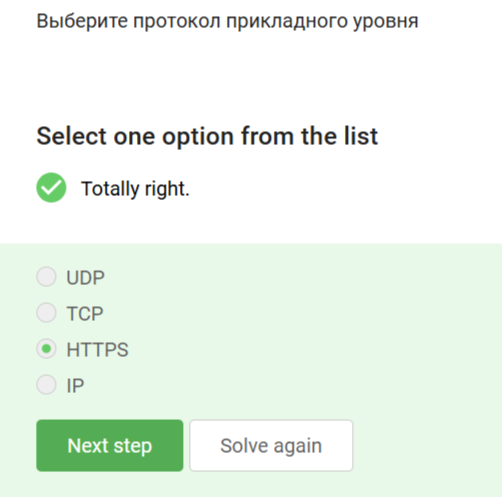


Рис. 1: Задание 1

Протоколы TCP и UDP - протоколы транспортного уровня, IP - протокол сетевого уровня. Прикладным из перечисленных является только HTTPS. Это же рассуждение дает ответ на следующий вопрос.

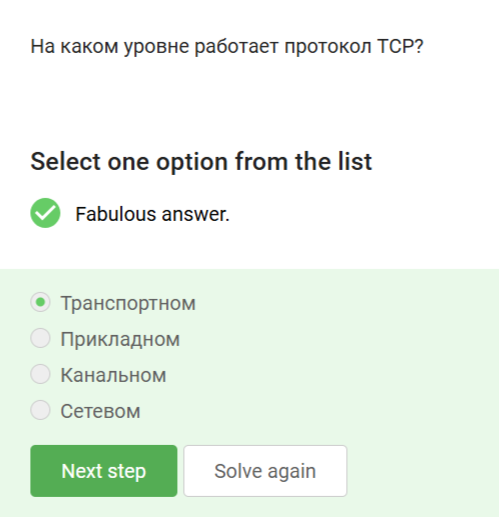


Рис. 2: Задание 2

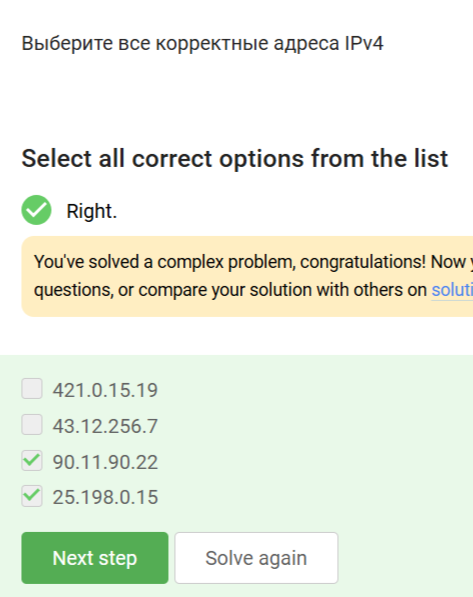


Рис. 3: Задание 3

Первый из адресов начинается с 421, второй содержит 256. Ни то, ни другое не может являться корректным адресом IPv4, так как исловный максимальный адрес, который можно получить в этом стандарте - 255.255.255.255

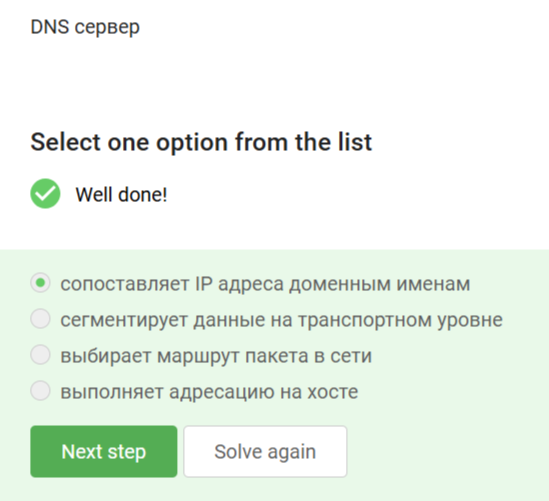


Рис. 4: Задание 4

DNS (Domain Name Server) сопоставляет адрес сайта с его доменным именем и обеспечивает “навигацию” в Интернете. Он не сегментирует данные, не выбирает маршруты для пакетов и не занимается адресацией.

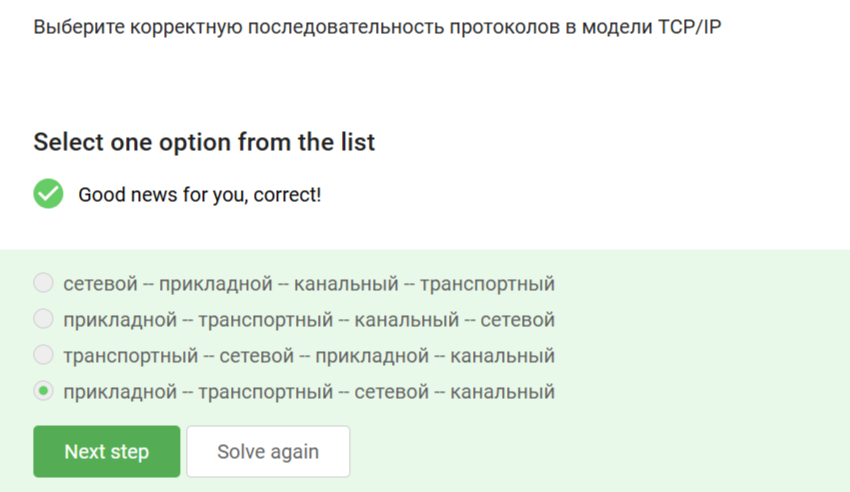


Рис. 5: Задание 5

Прикладной уровень должен быть “верхним”, канальный - нижним, таким образом, корректна только последняя цепочка.

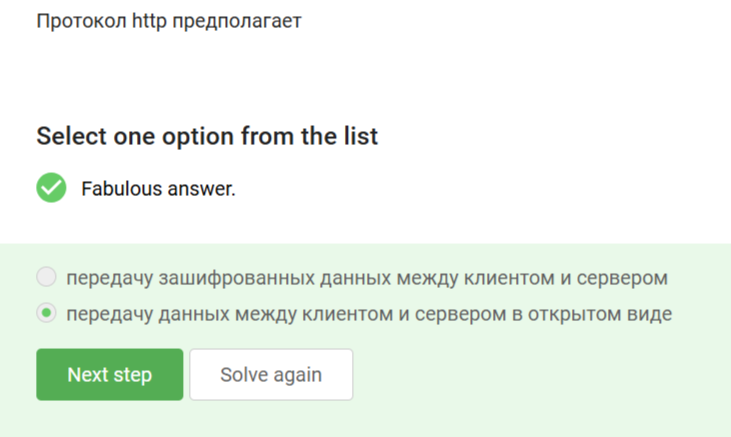


Рис. 6: Задание 6

HTTP не предполагает шифрования данных, поэтому считается небезопасным и устаревшим. Шифрует данные между клиентом и сервером HTTPS.

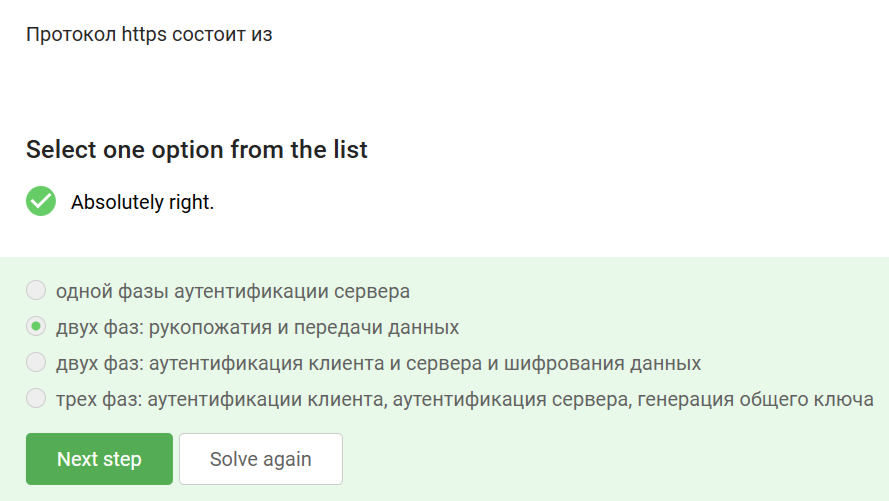


Рис. 7: Задание 7

HTTPS состоит из двух фаз: рукопожатия между клиентом и сервером, в результате которого устанавливаются “условия” общения, и обмена зашифрованными данными. Отсюда очевидно, что подходит только ответ 2.

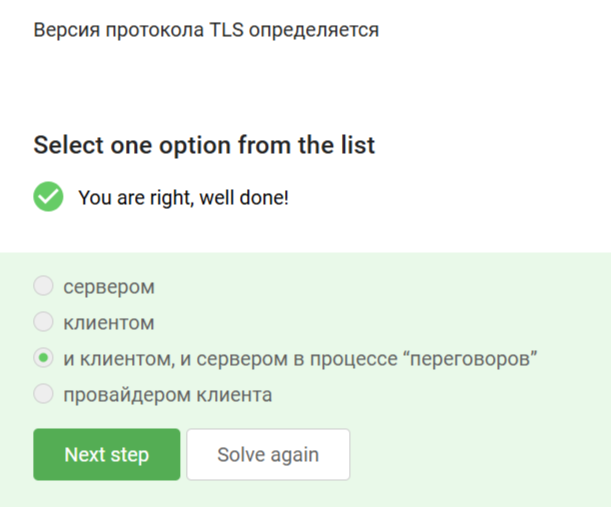


Рис. 8: Задание 8

Версия протокола TLS определяется совместно сервером и клиентом. ни одна из сторон не может “диктовать” свои условия другой.

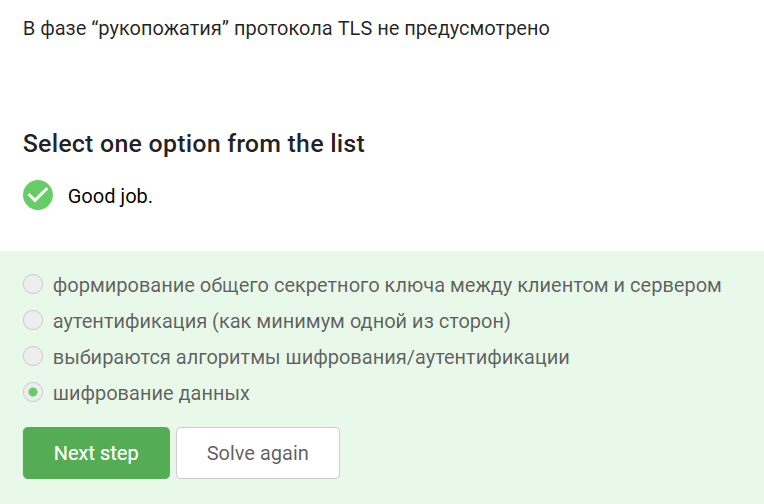


Рис. 9: Задание 9

В фазе рукопожатия не предусмотрено именно шифрования данных, так как оно выполняется после установки условий обмена данными в отдельной фазе.

## 2.2 Персонализация сети

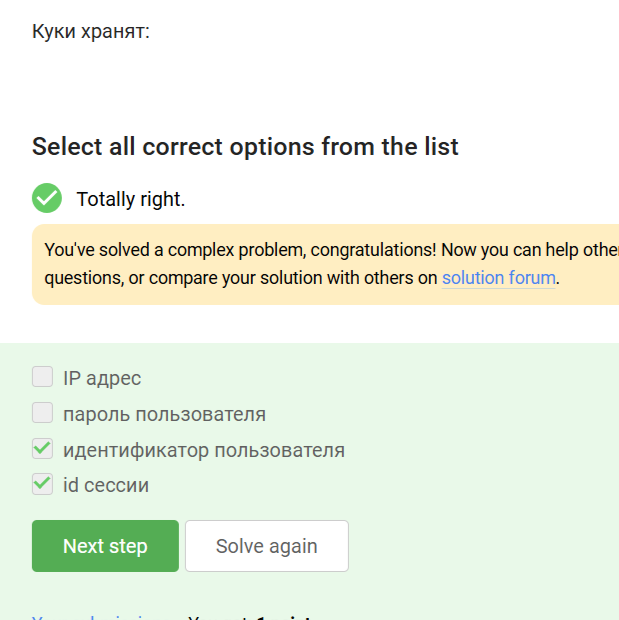


Рис. 10: Задание 10

По-хорошему куки не должны хранить конфиденциальную информацию, такую как пароль или адрес пользователя. поэтому подходят только два последних ответа: идентификатор пользователя и сессии.

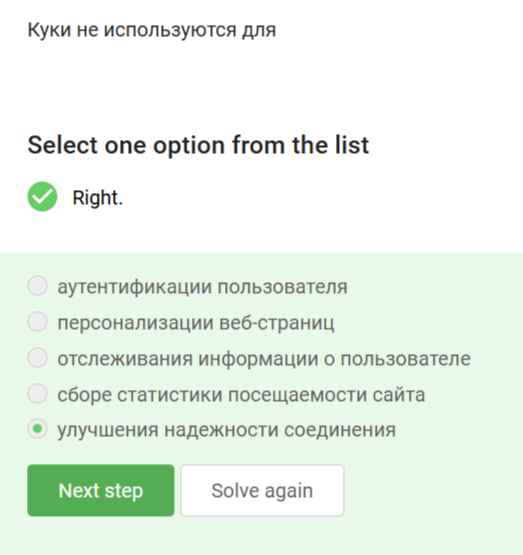


Рис. 11: Задание 11

Куки хранят информацию, но не используются для обеспечения надежности соединения самого по себе. Хотя хранение информации на стороне клиента может в общем и целом снижать загруженность сервера.

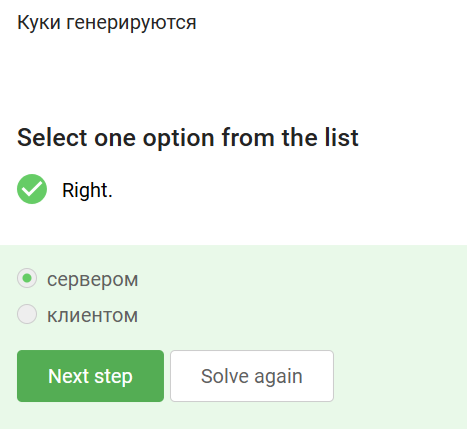


Рис. 12: Задание 12

Куки присваиваются (генерируются) пользователю сервером и хранятся на стороне клиента.

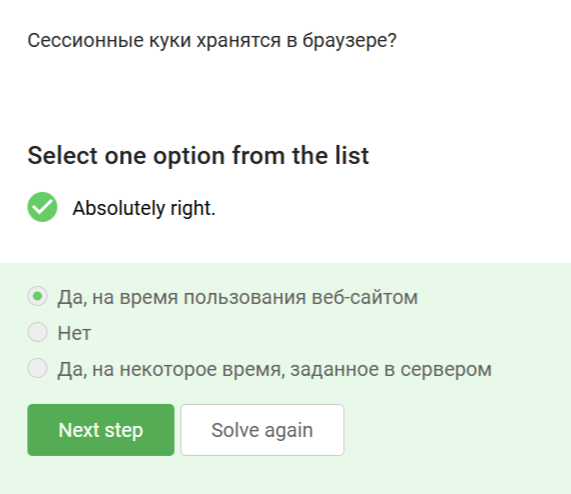


Рис. 13: Задание 13

Сессионные куки отвечают за хранение данных, связанных с конкретной сессией (моментом посещения и использования) сайта. Они храняется в браузере только во время использования сайта (жизни сессии).

## 2.3 Браузер ТОР. Анонимизация

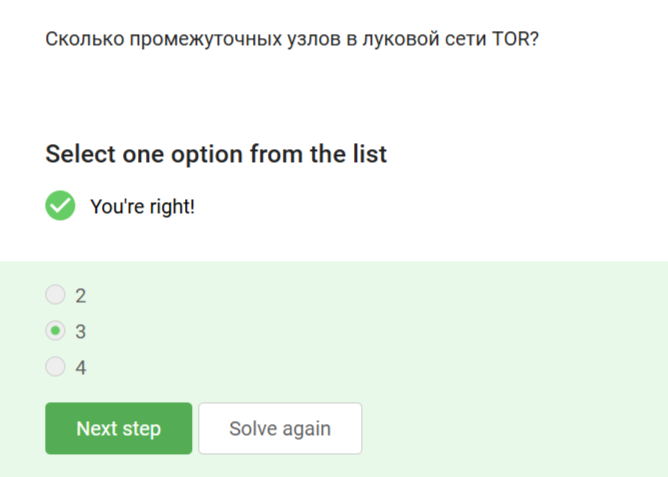


Рис. 14: Задание 14

В сети ТОР минимум три промежуточных узла: охранный, промежуточный и выходной.

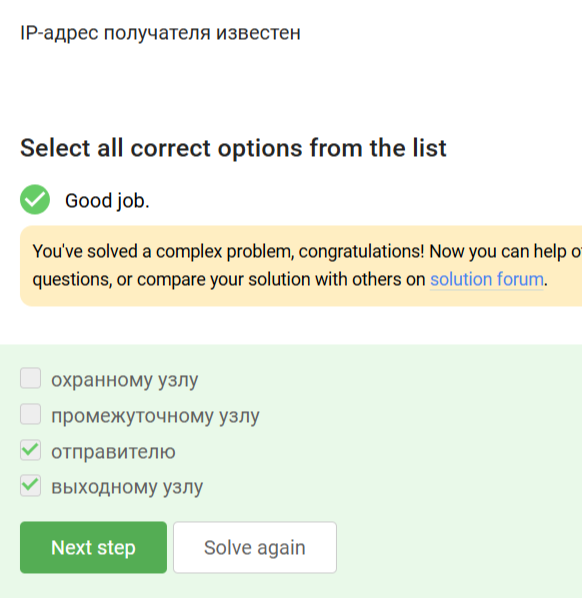


Рис. 15: Задание 15

Адрес получателя известен отправителю (он выбирает, кому направить сообщение) и выходному узлу (он передает сообщение, полученное от предыдущих узлов цепи, непосредственно получателю).

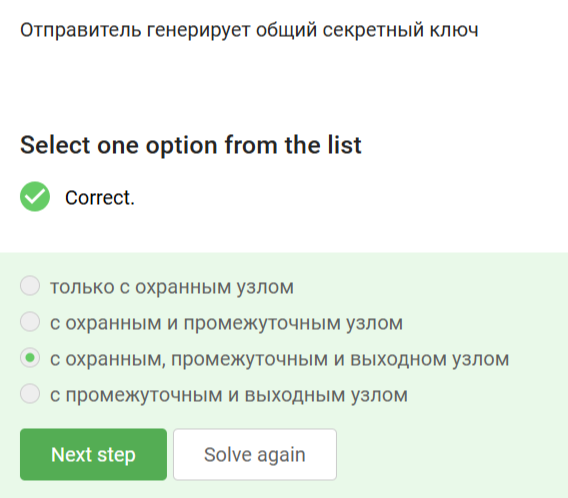


Рис. 16: Задание 16

Общий секретный ключ отправитель генерирует с каждым из узлов цепи для сохранения целостности передачи.

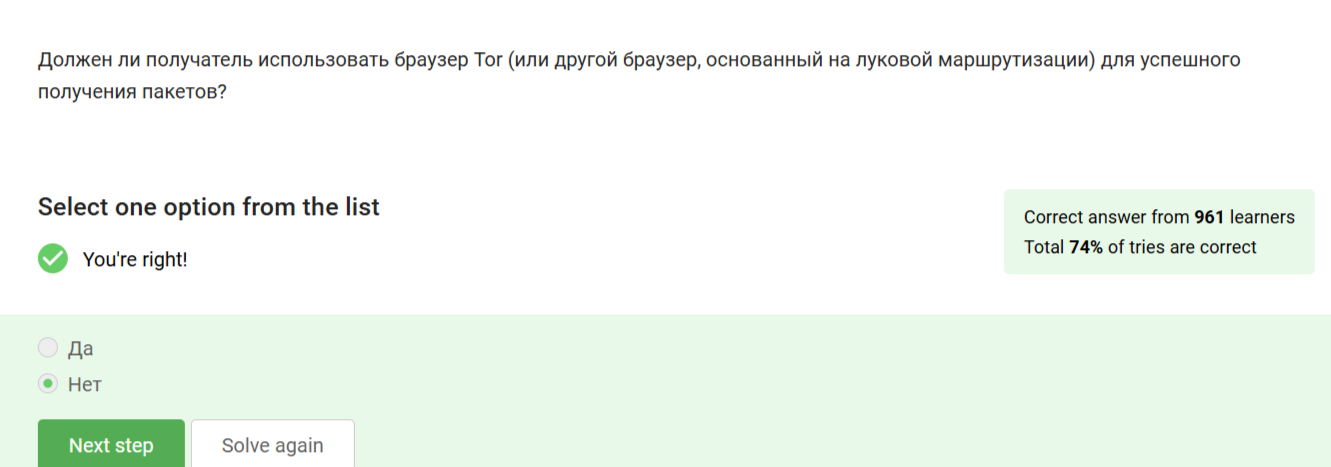


Рис. 17: Задание 17

Получатель не должен использовать браузер, основанный на луковой маршрутизации, так как доставка сообщения не зависит от него.

## 2.4 Беспроводные сети Wi-Fi

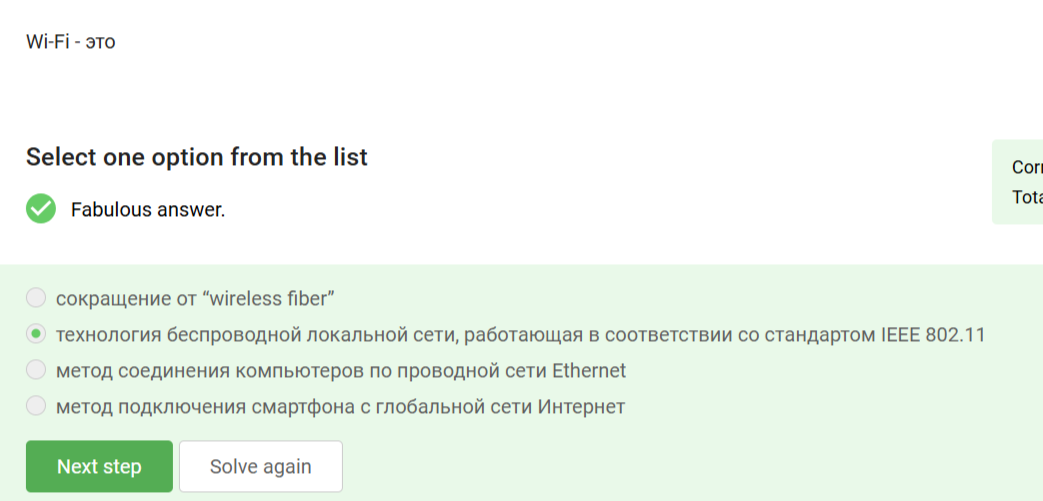


Рис. 18: Задание 18

Wi-Fi - технология беспроводной сети; работает не только со смартфонами или компьютерами и описана в стандартве 802.11

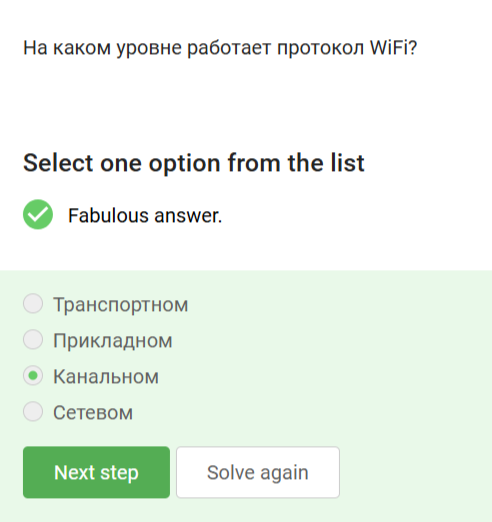


Рис. 19: Задание 19

Wi-Fi - канал передачи данных, и работает, соответственно, на канальном уровне. На сетевом работает IP, на прикладном - HTTP/HTTPS, на транспортном - TCP/UDP.

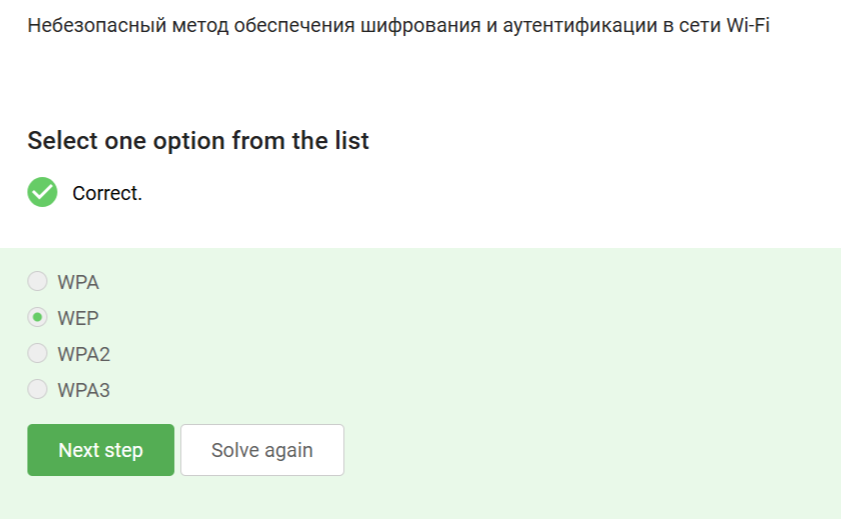


Рис. 20: Задание 20

Наименее безопасен из перечисленных WEP, так как длина ключа в этом протоколе не могла превышать 40 бит.

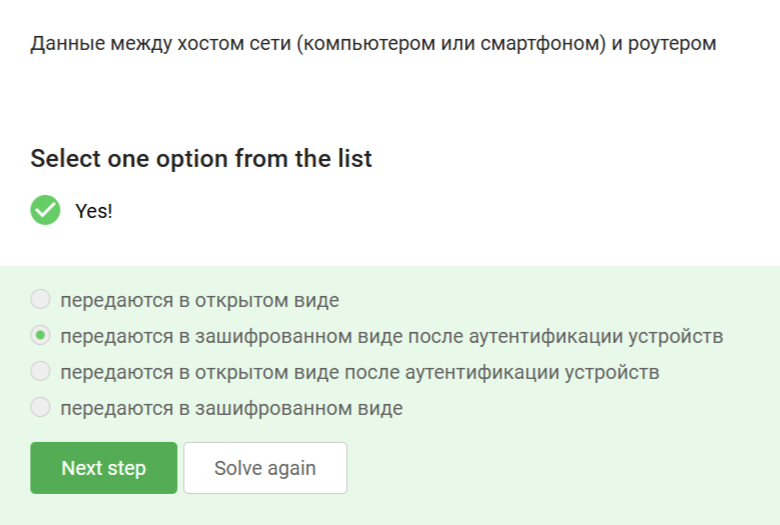


Рис. 21: Задание 21

Данные между хостом и роутером передаются только после аутентификации устройства в сети в зашифрованном виде, поэтому все ответы, кроме 2, неверны.

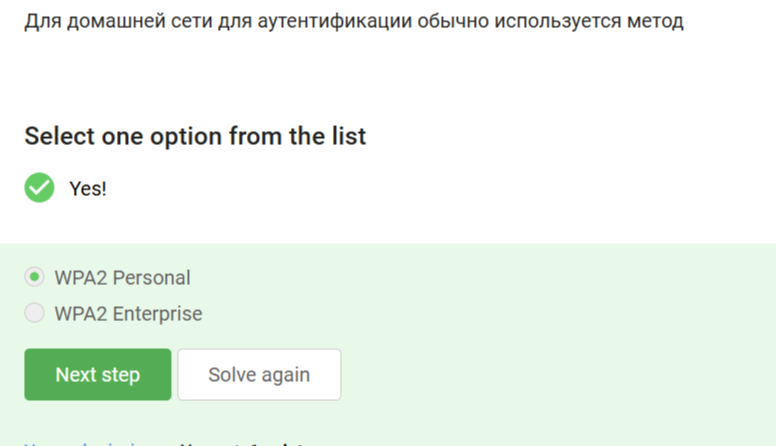


Рис. 22: Задание 22

Энтерпрайс - решение для бизнеса. Для организации домашних сетей оно не используется.

# 3 Выводы

Получены и закреплены на практике знания об основных механизмах работы сети Интернет и их слабых местах.