Внешний курс раздел 1

Безопасность в сети

Александр Андреевич Шуплецов

Содержание

# 1 Цель работы

Изучить основы безопасности в сети.

# 2 Выполнение работы

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

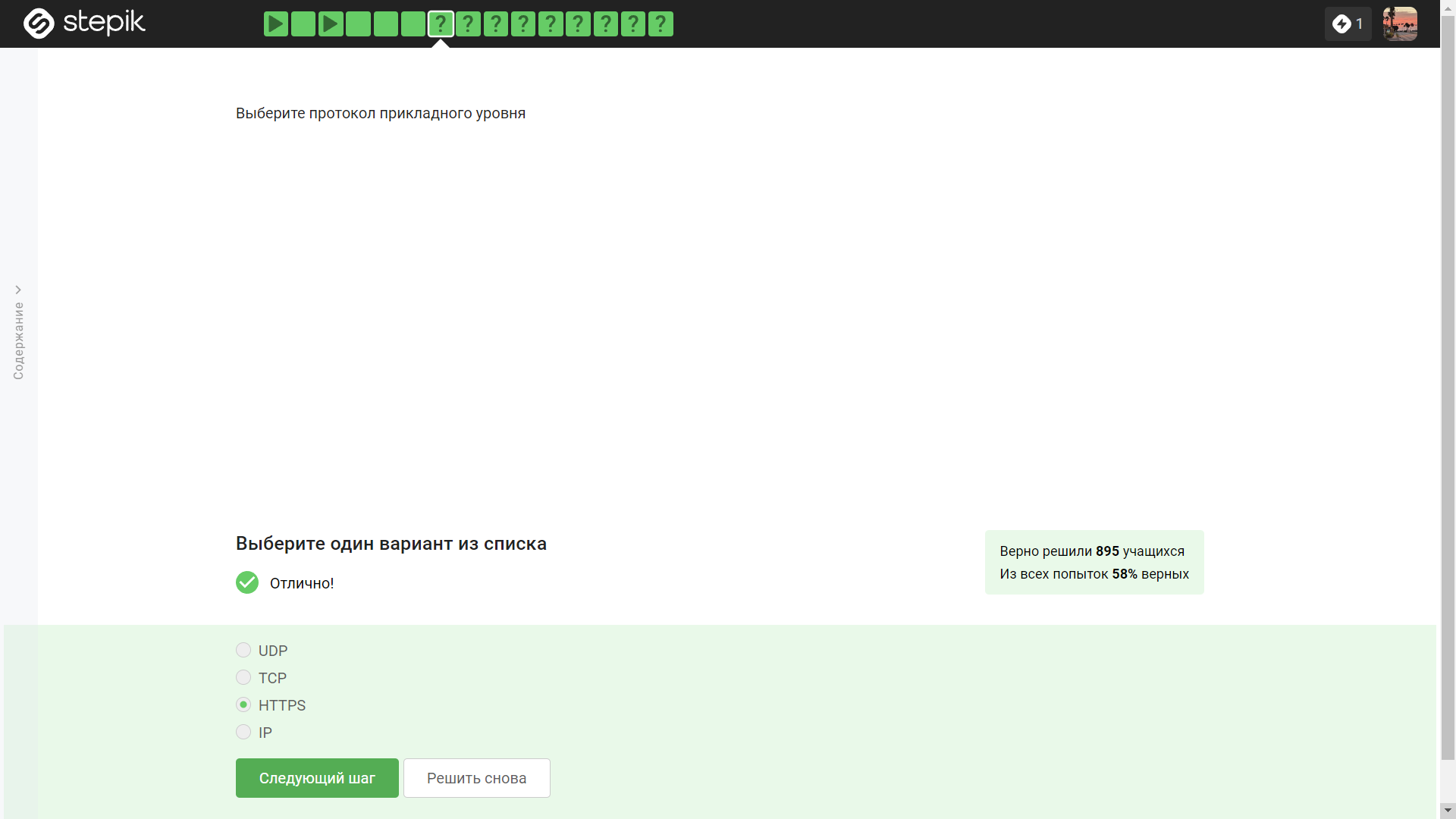


Figure 1: первое задание

1. Протокол TCP работает на транспортном уровне.

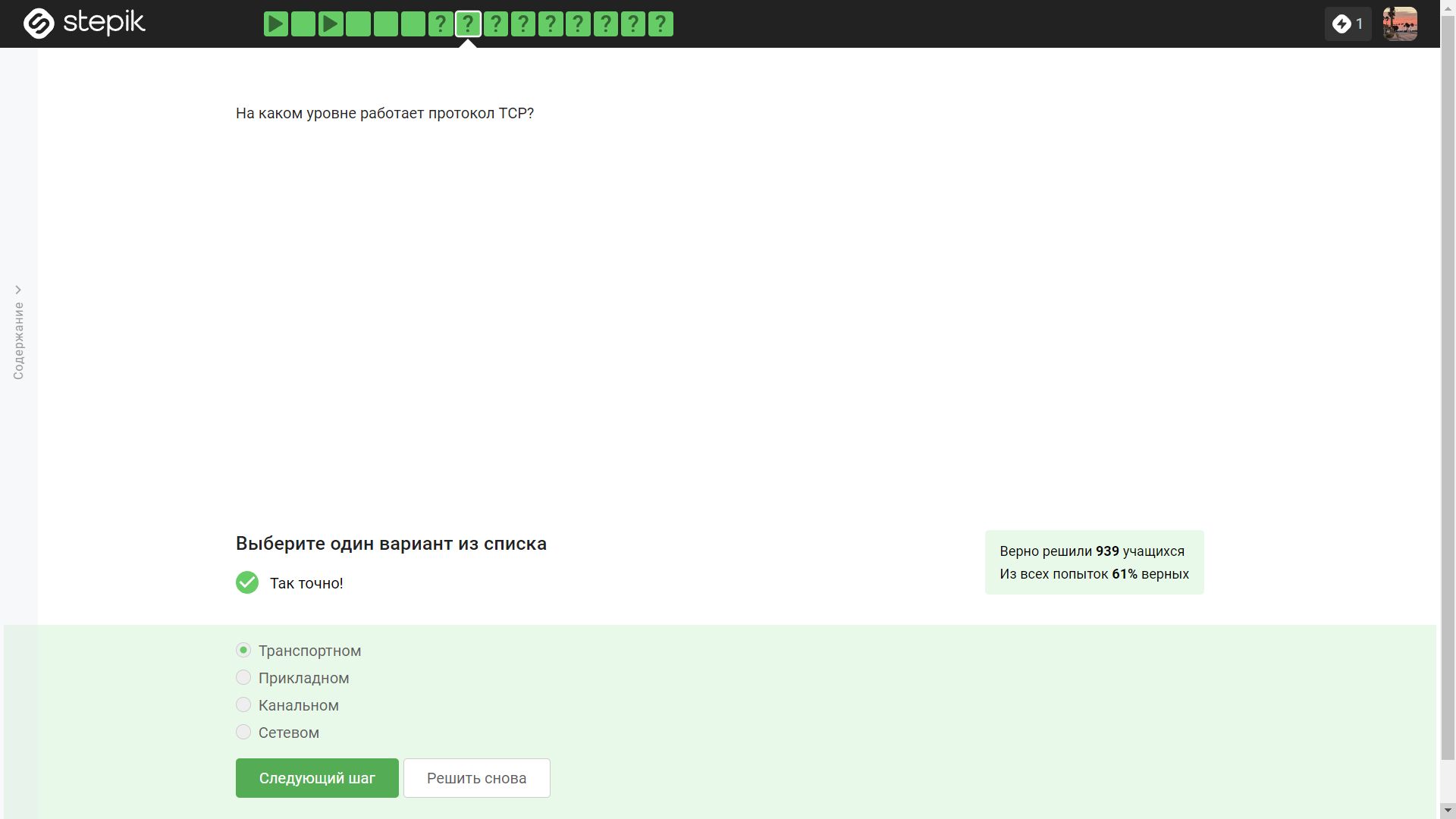


Figure 2: второе задание

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

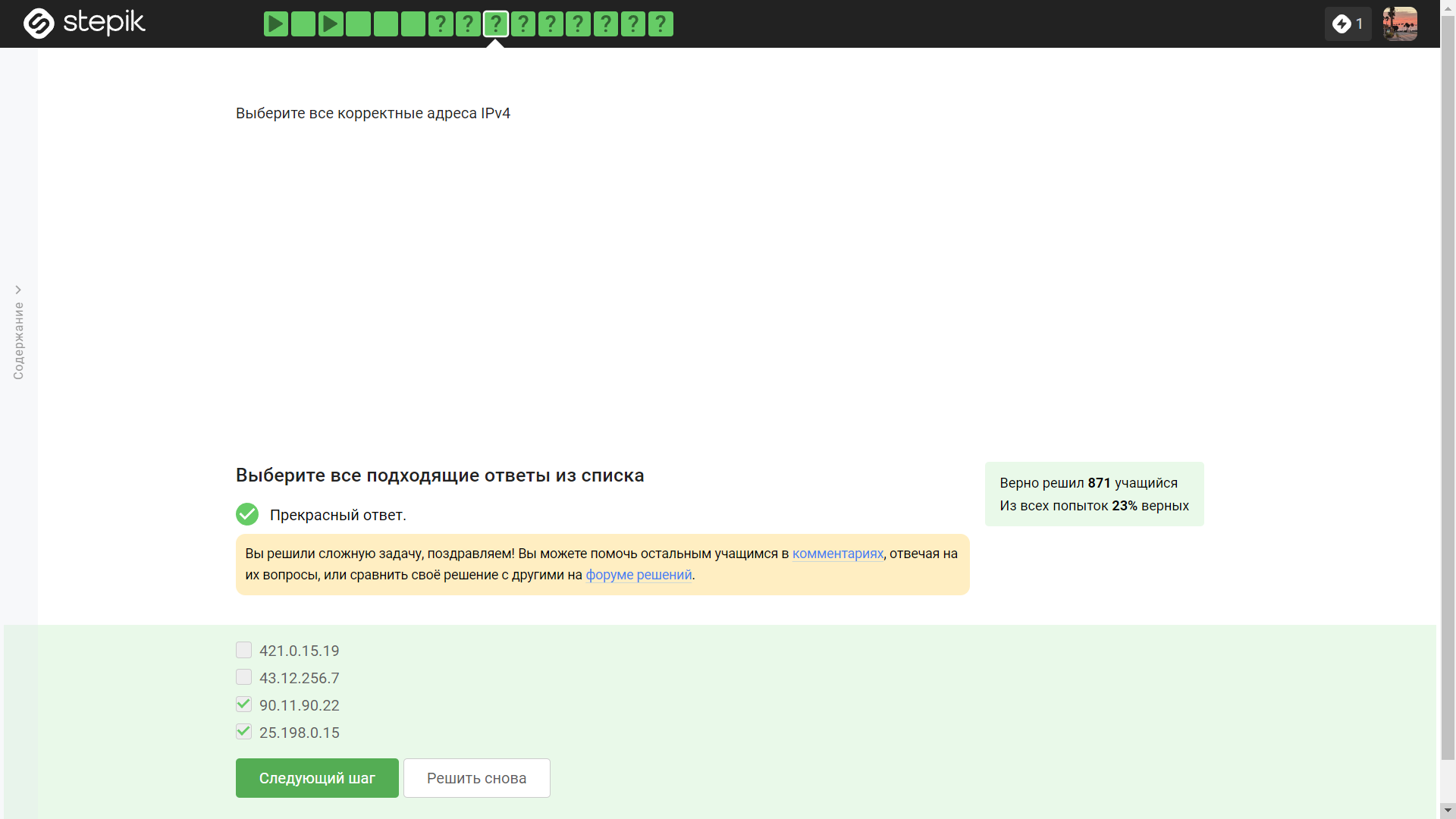


Figure 3: третье задание

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

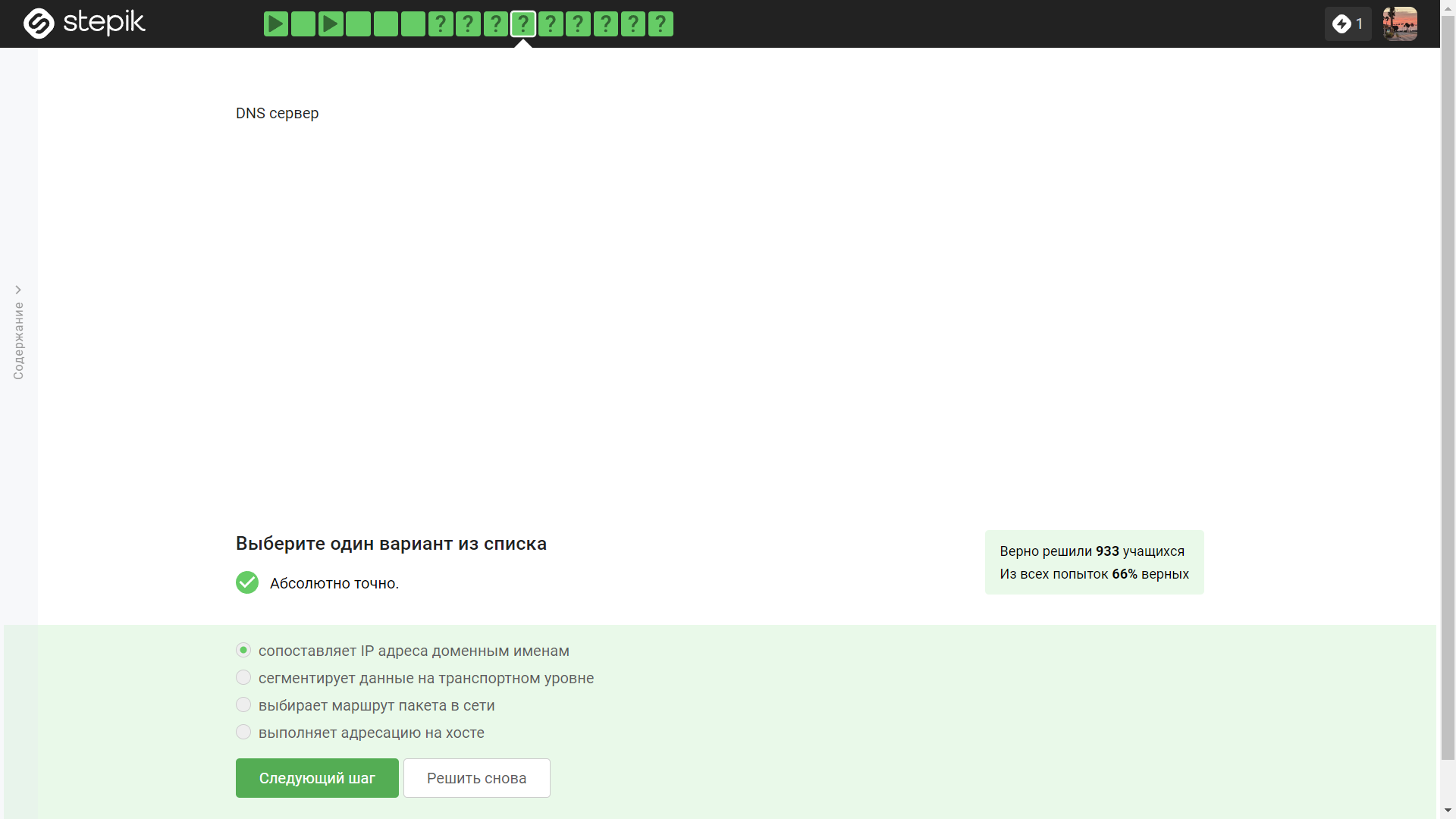


Figure 4: четвертое задание

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

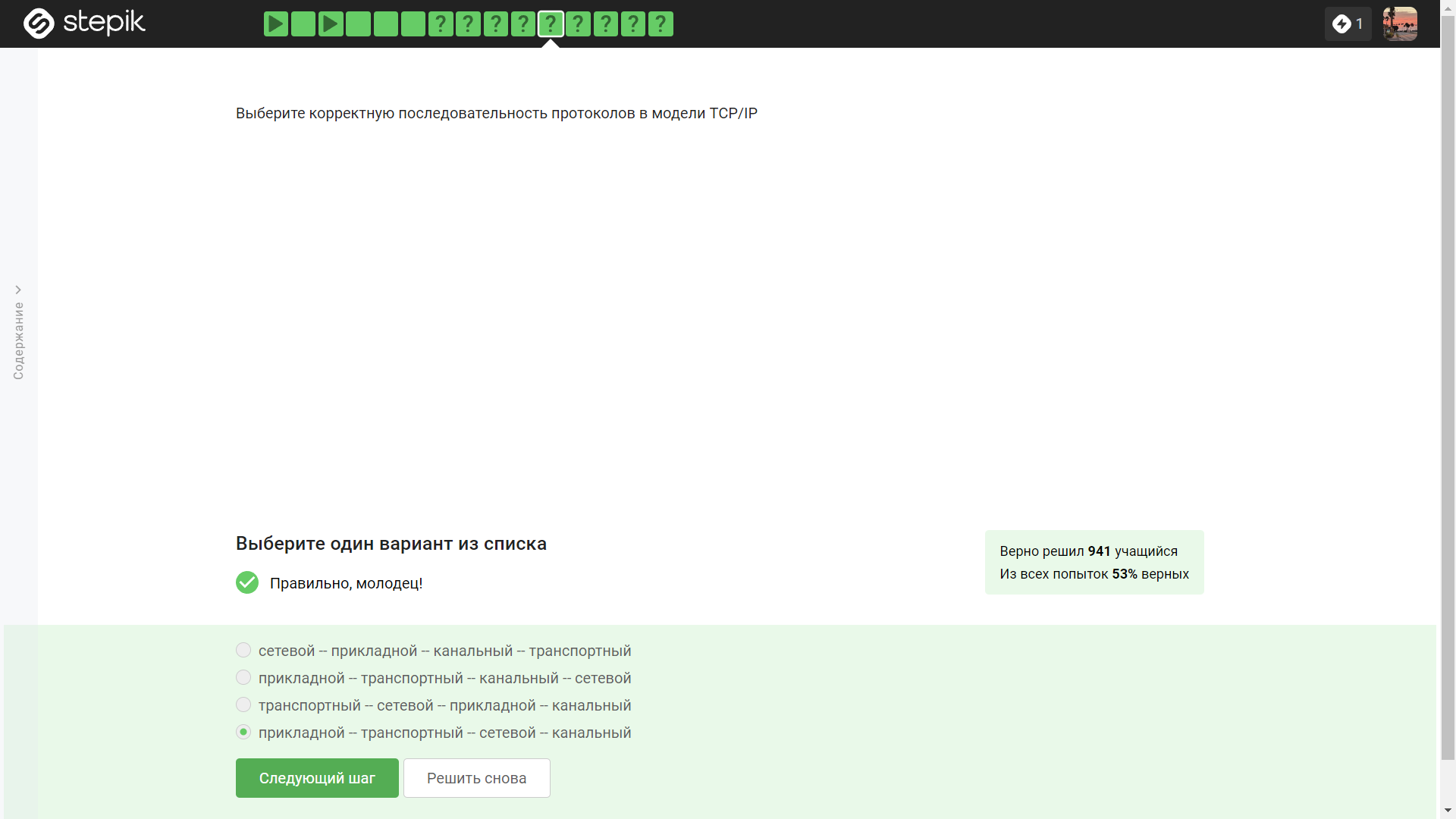


Figure 5: пятое задание

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

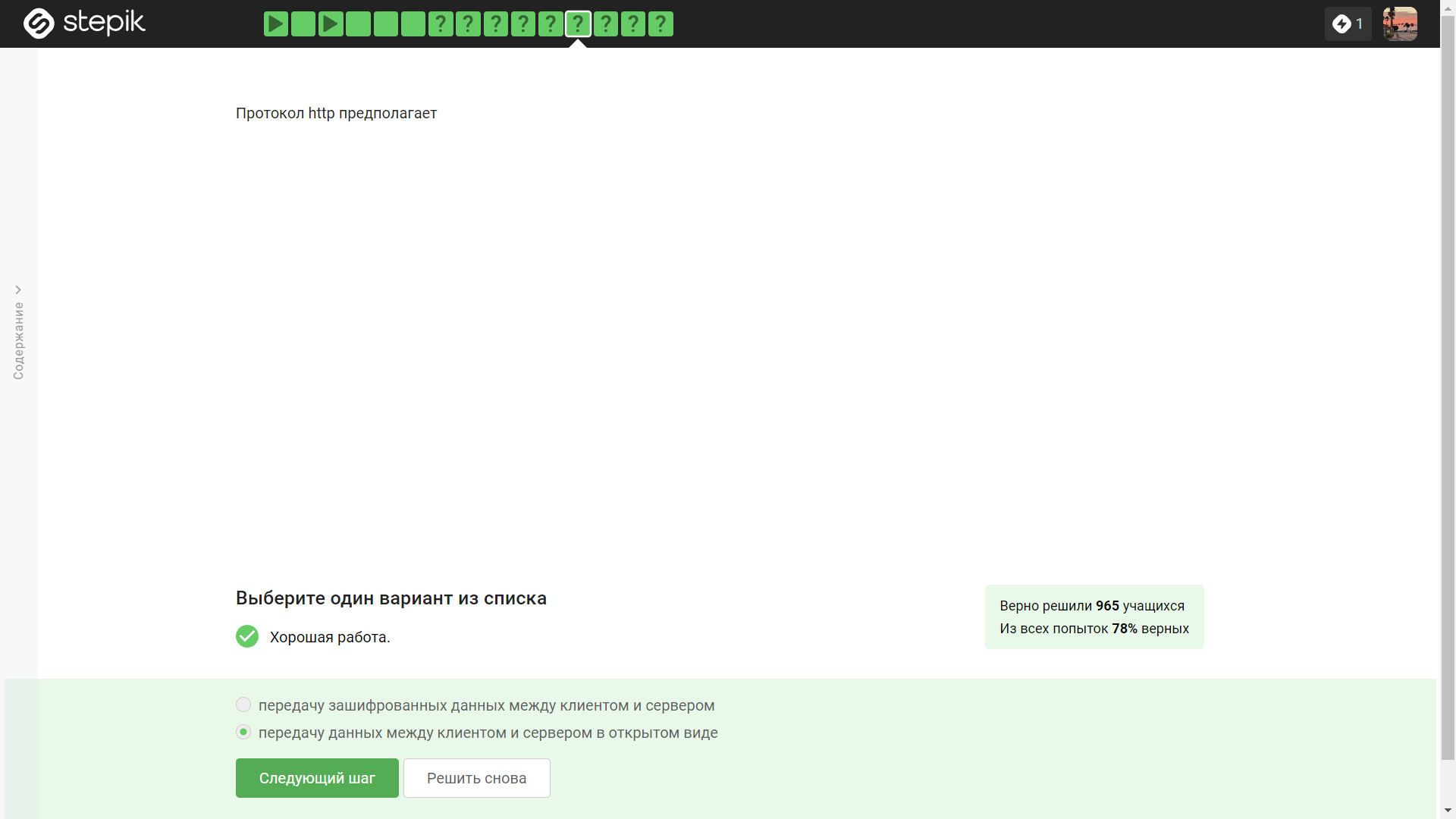


Figure 6: шестое задание

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

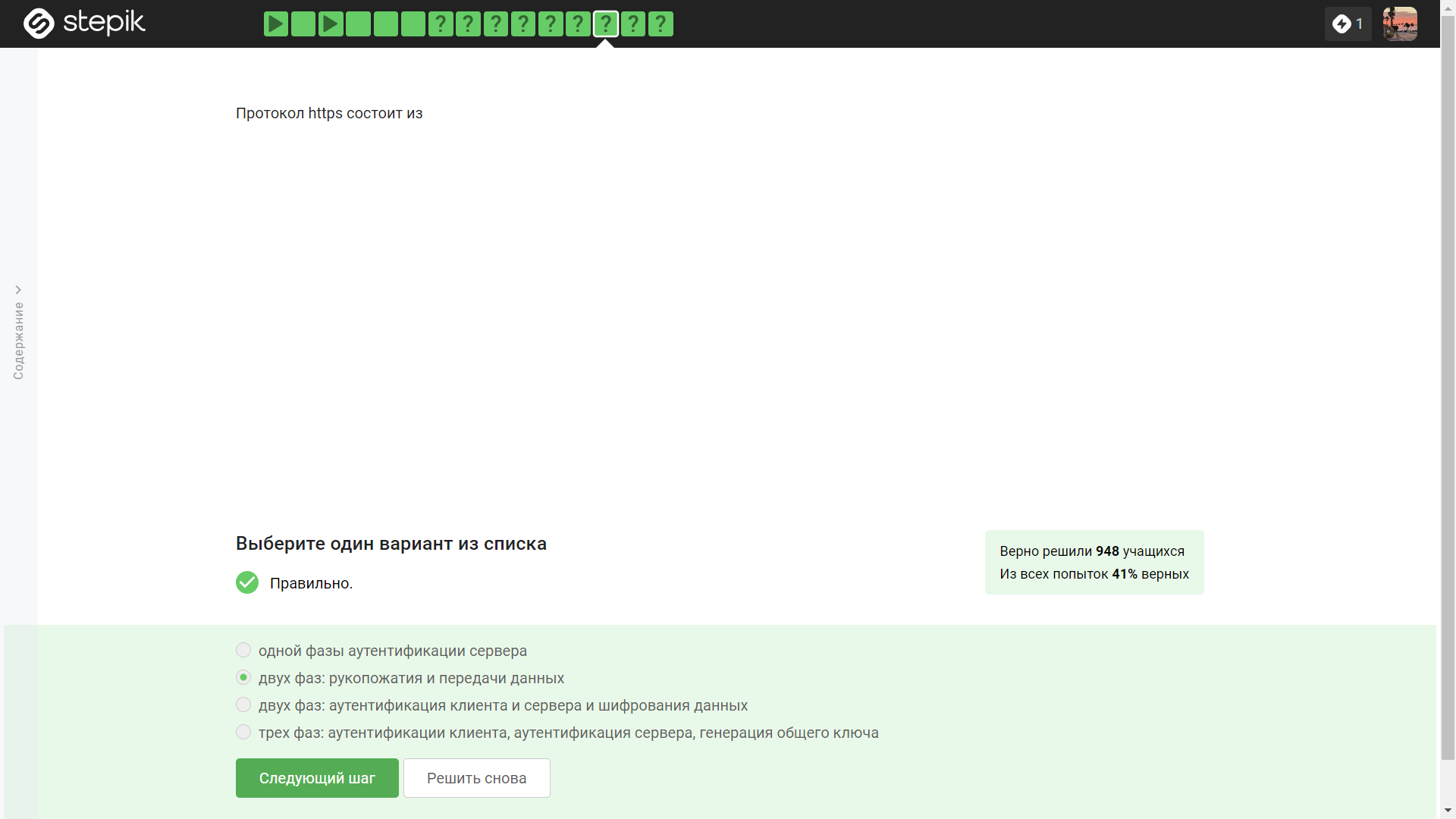


Figure 7: седьмое задание

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

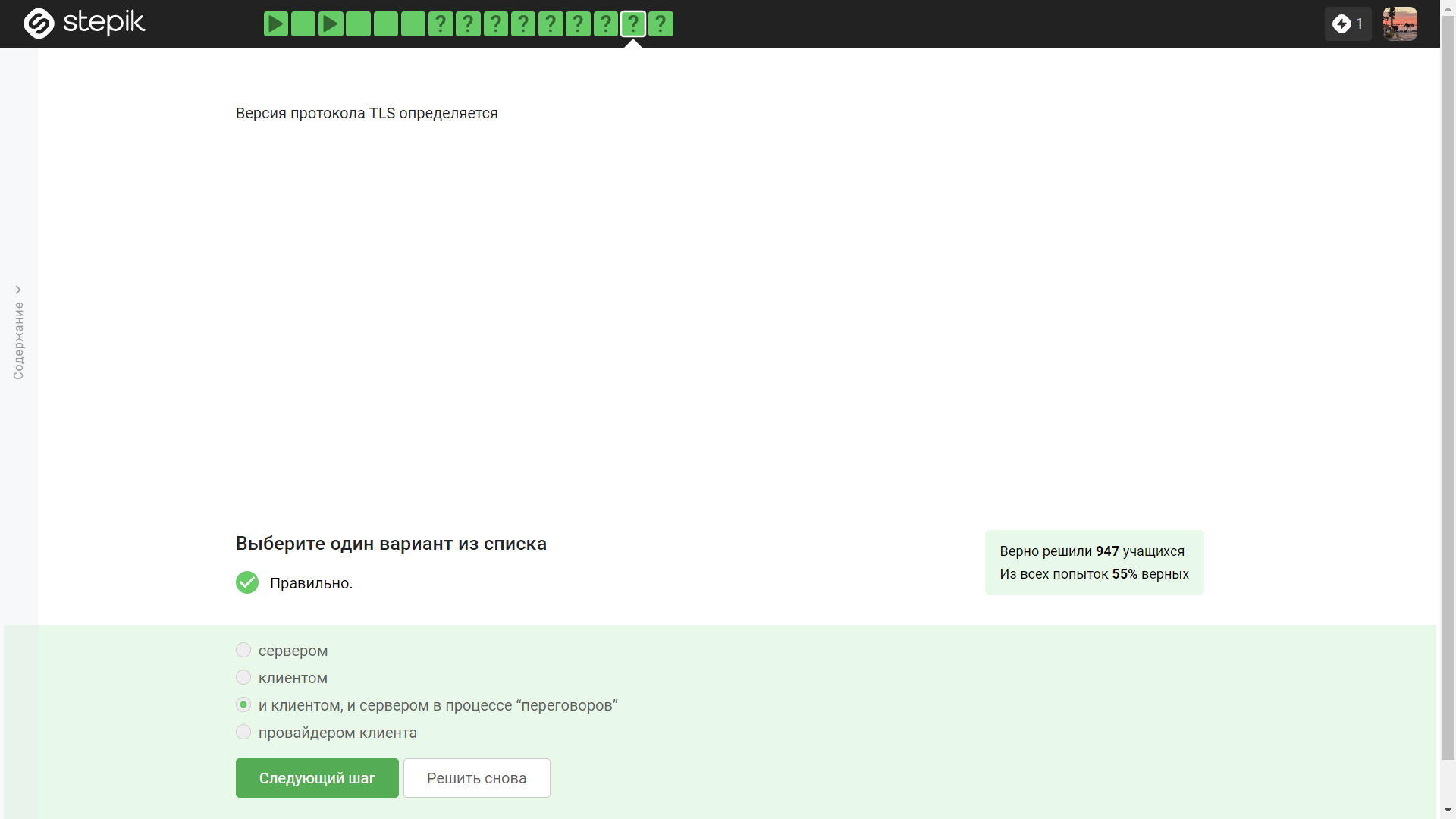


Figure 8: восьмое задание

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

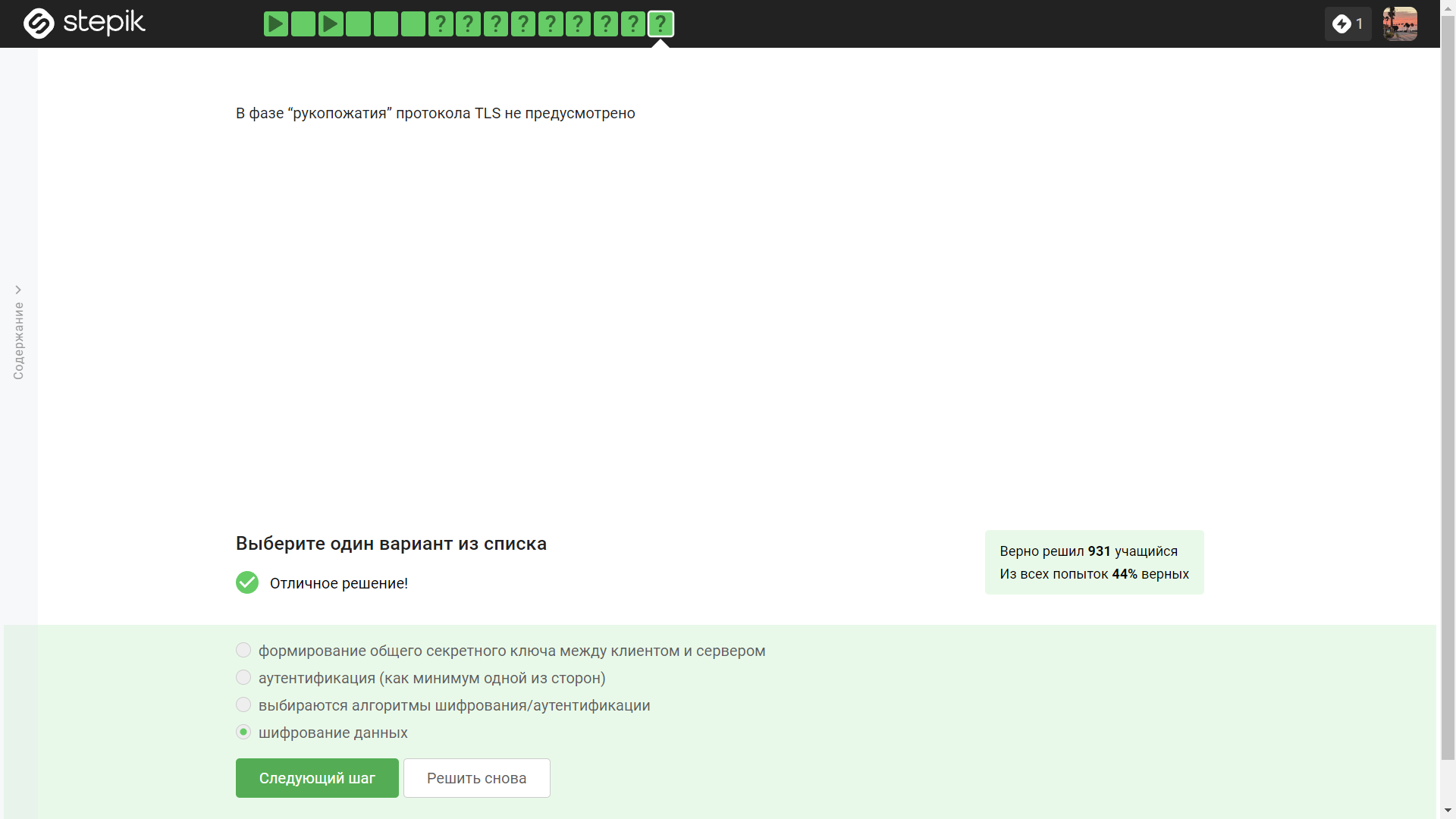


Figure 9: девятое задание

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

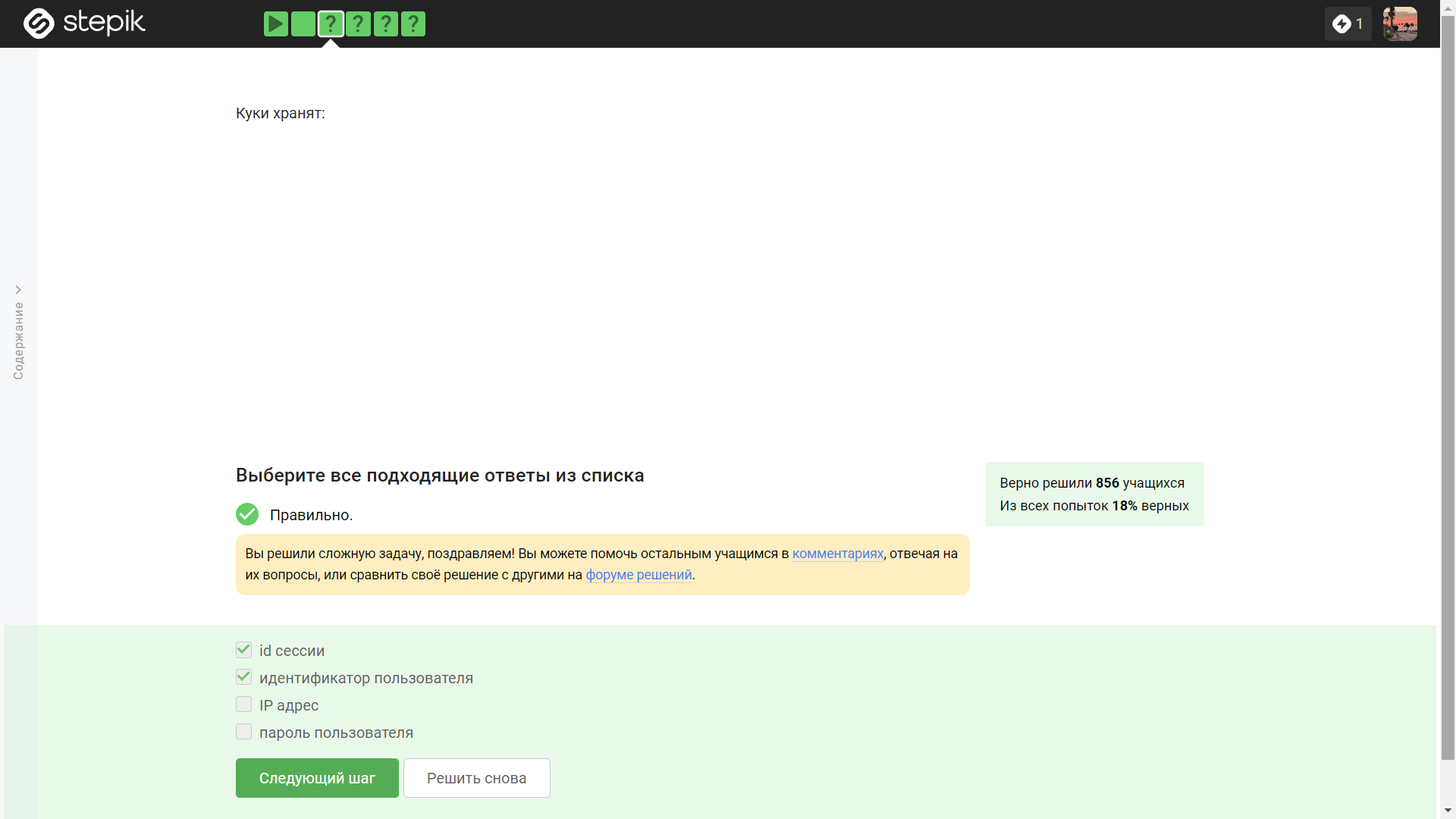


Figure 10: десятое задание

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

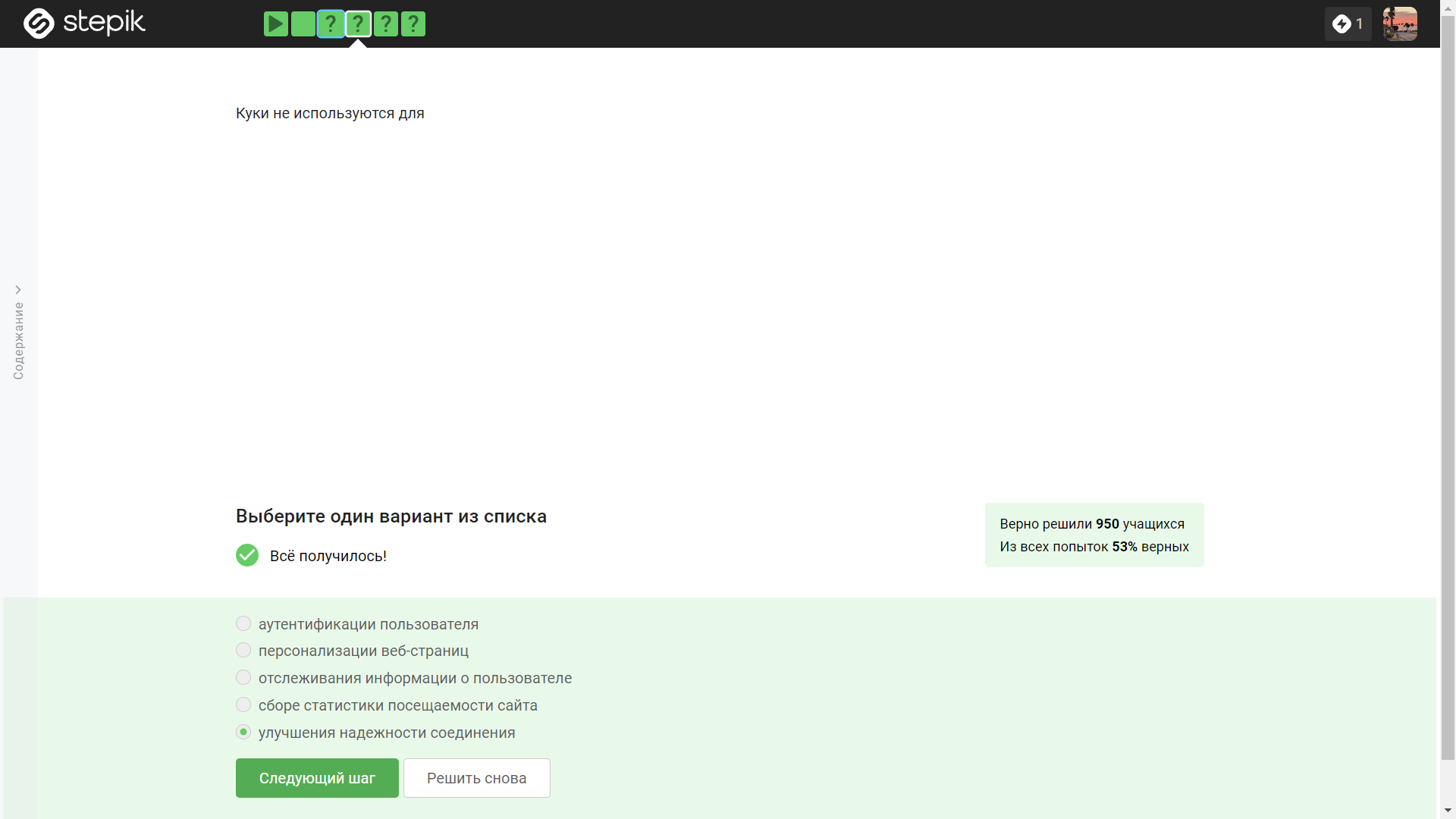


Figure 11: одиннадцатое задание

1. Куки генерируются сервером для клиента.

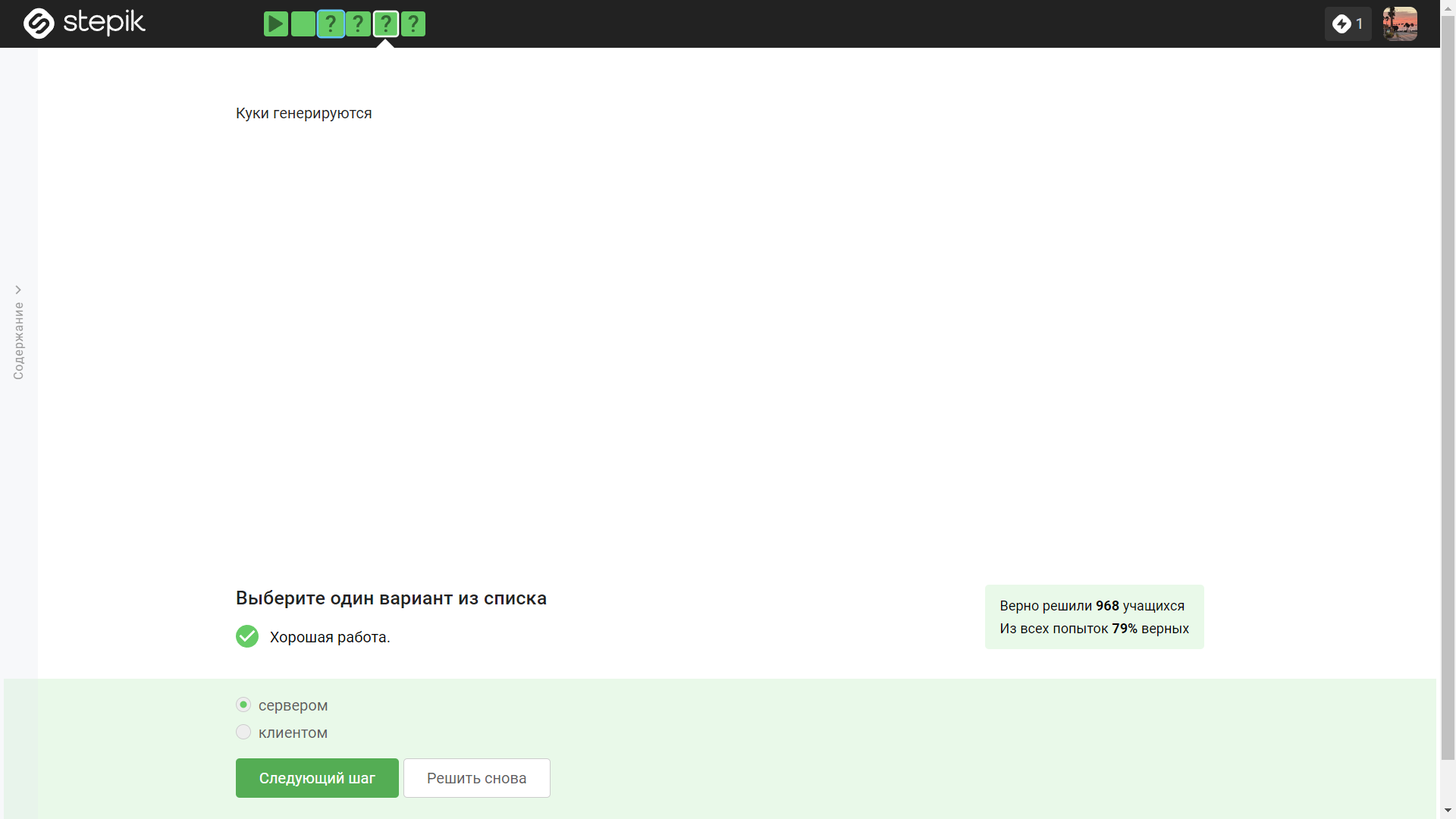


Figure 12: двенадцатое задание

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

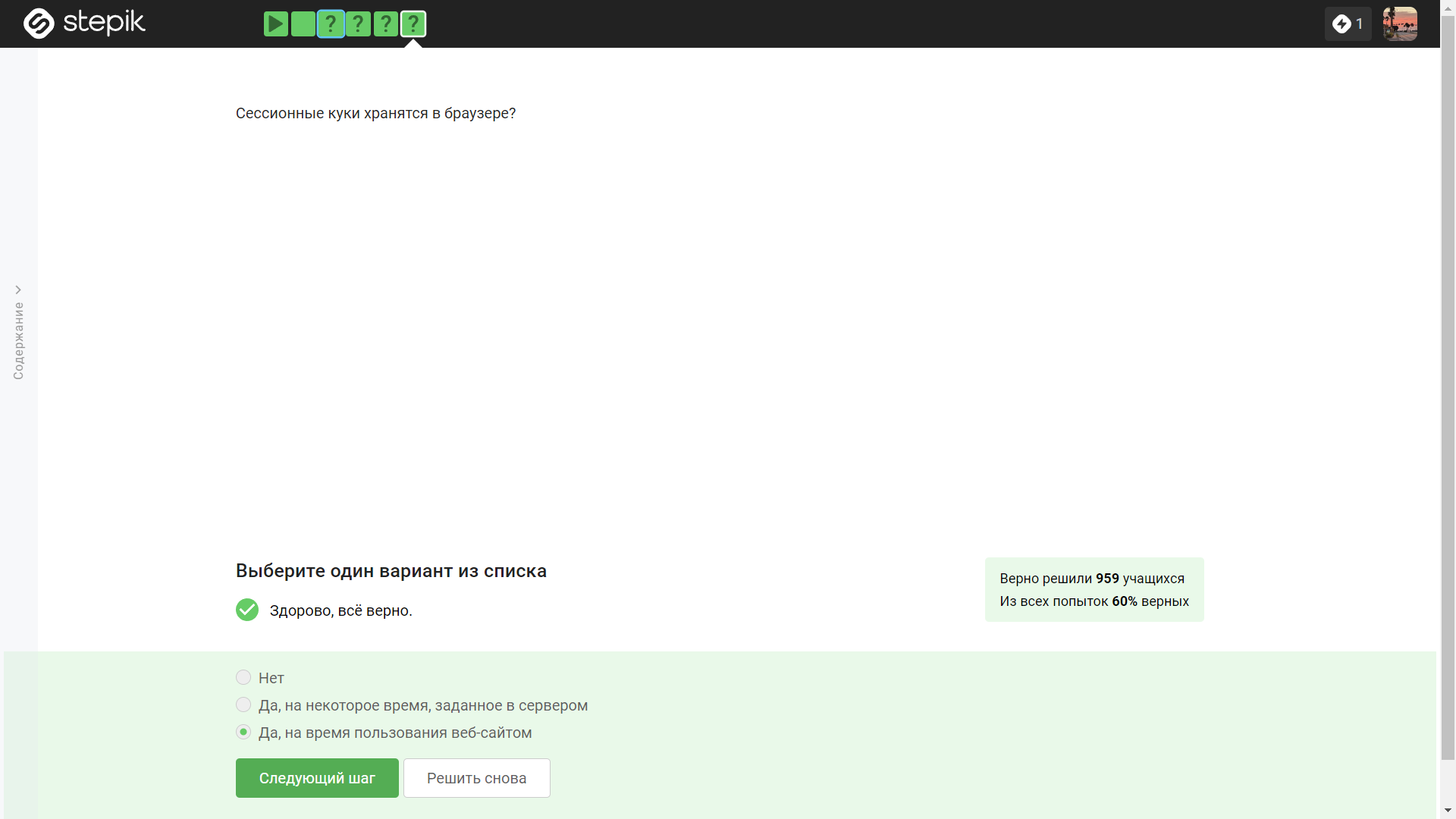


Figure 13: тринадцатое задание

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

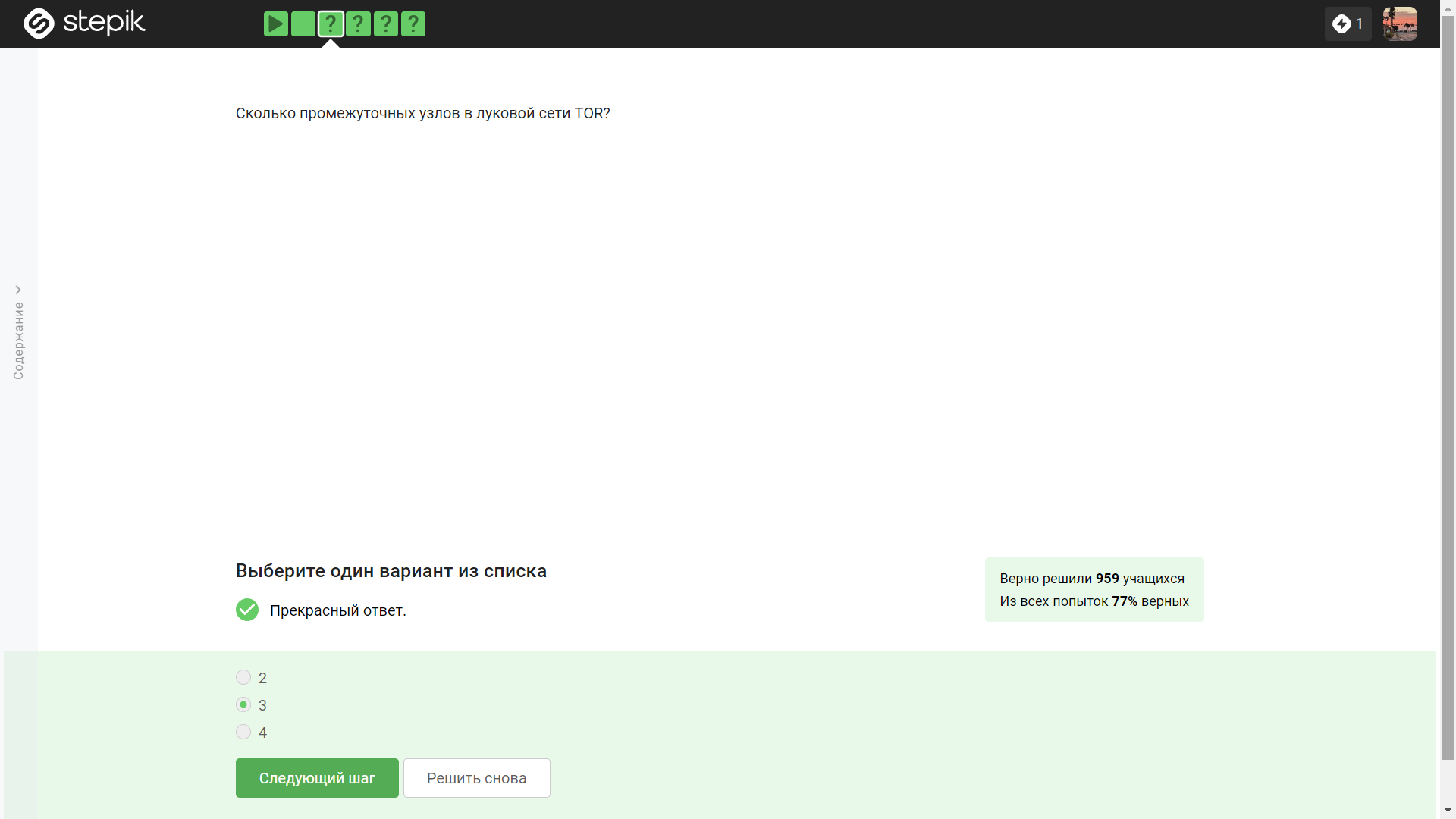


Figure 14: четырнадцатое задание

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

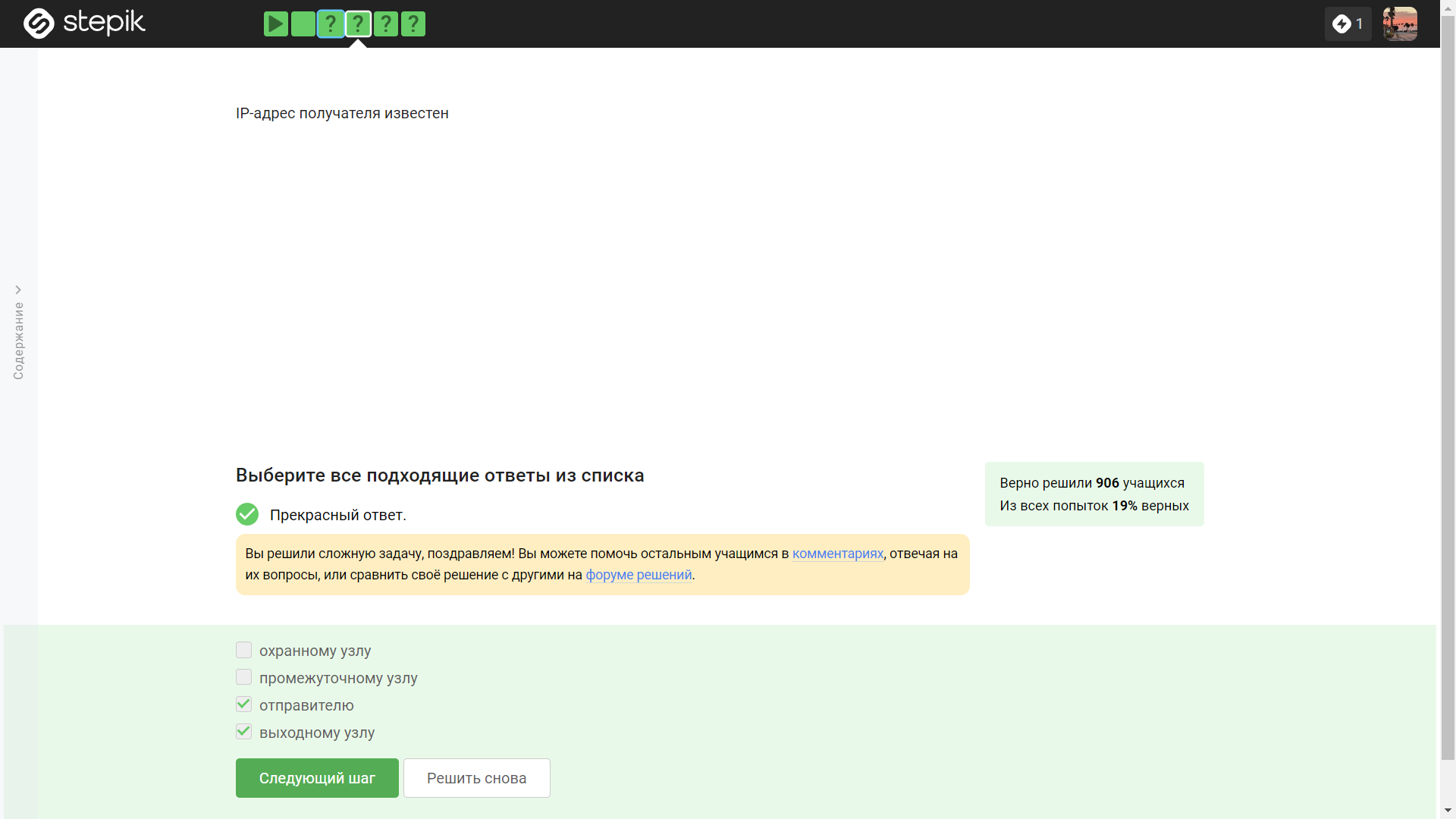


Figure 15: пятнадцатое задание

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

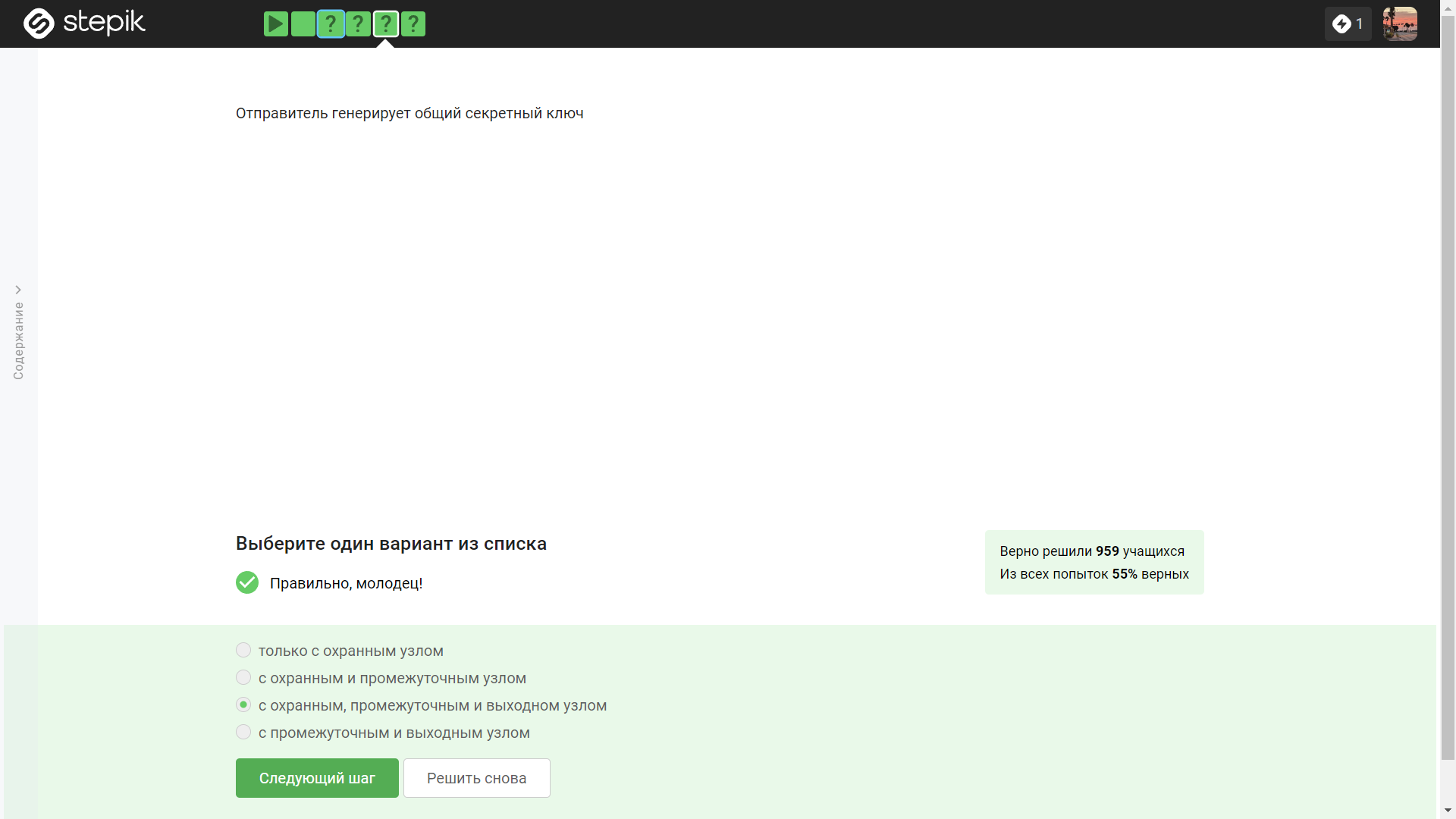


Figure 16: шестнадцатое задание

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

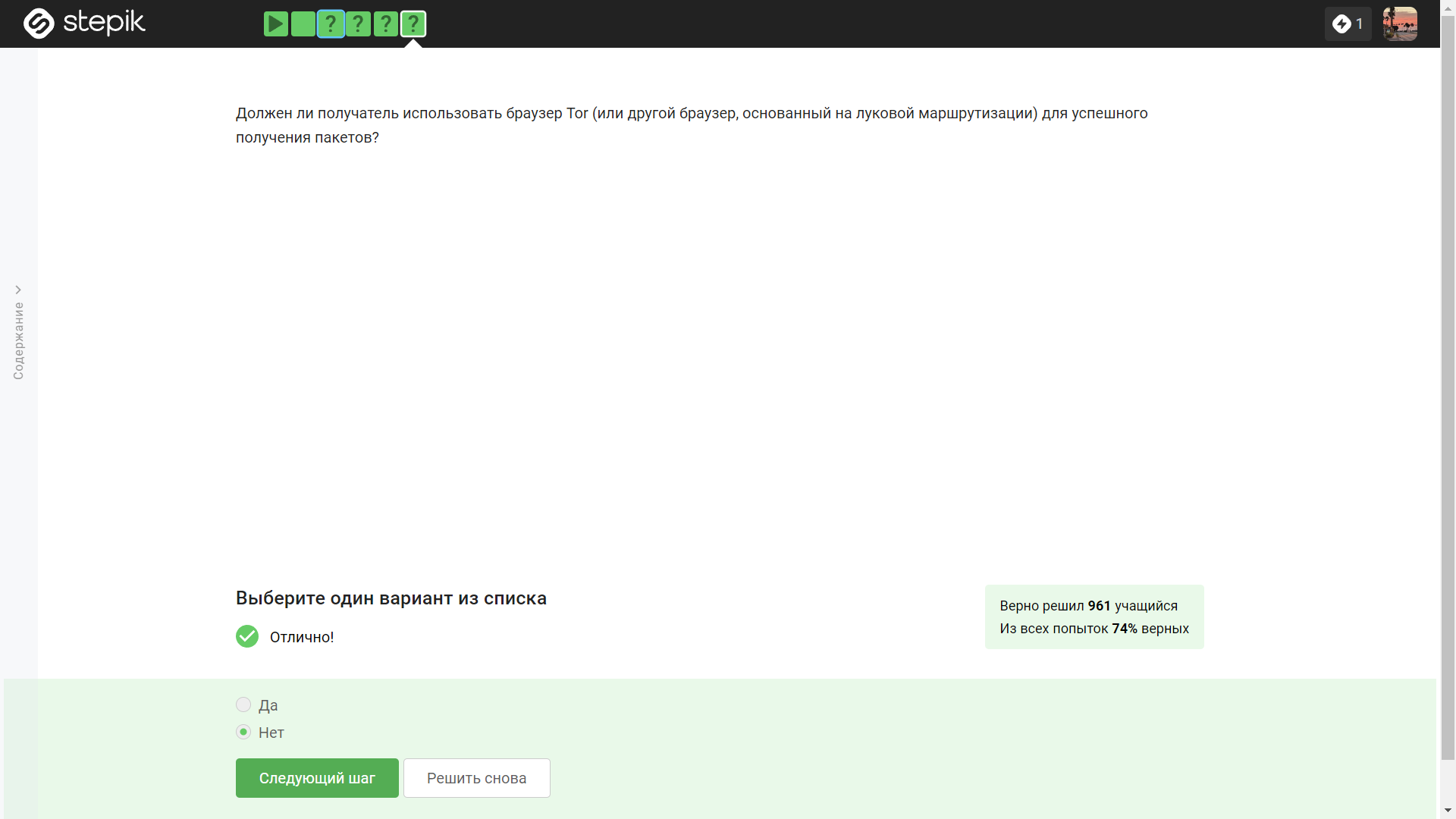


Figure 17: семнадцатое задание

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

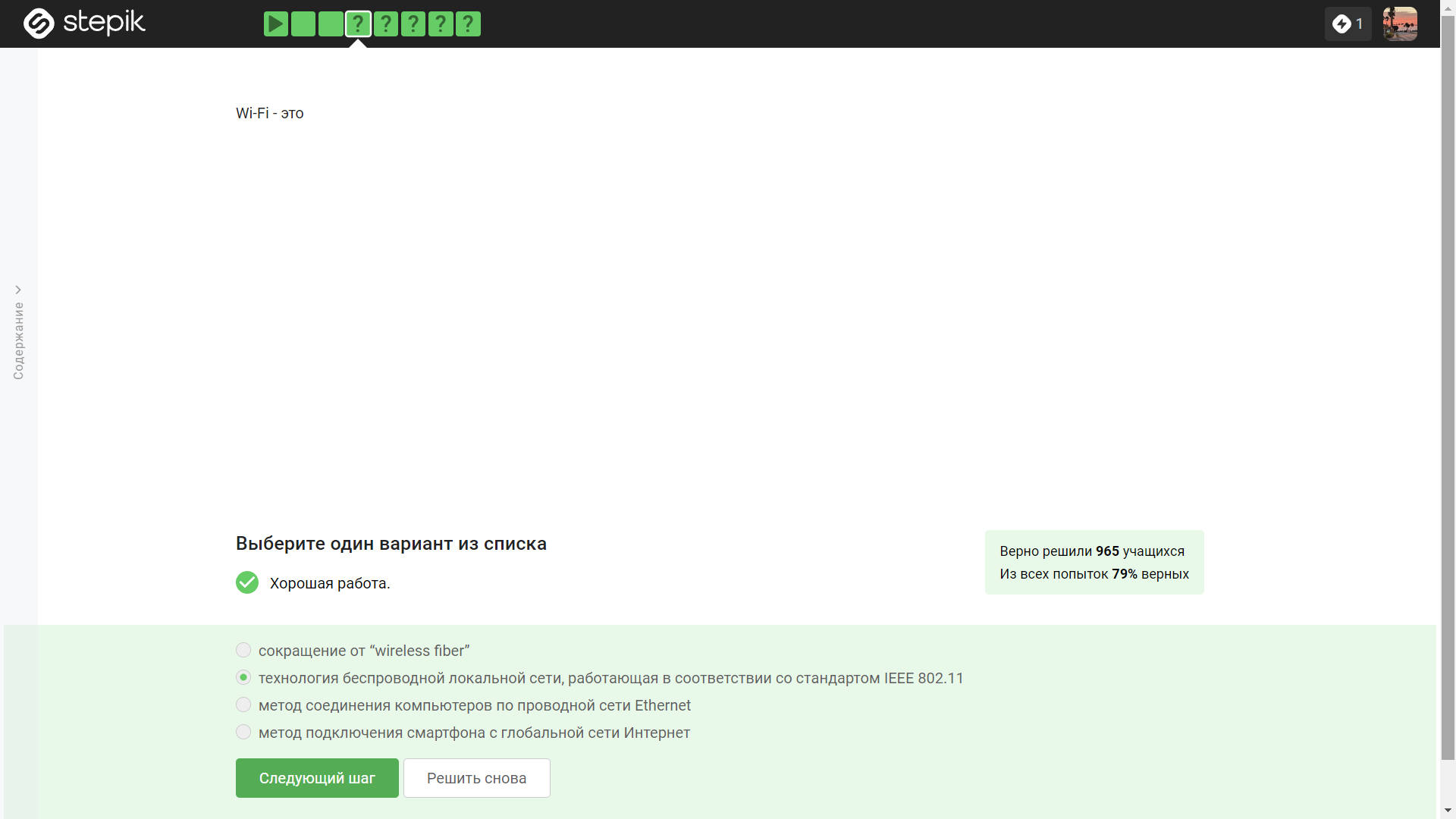


Figure 18: восемнадцатое задание

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

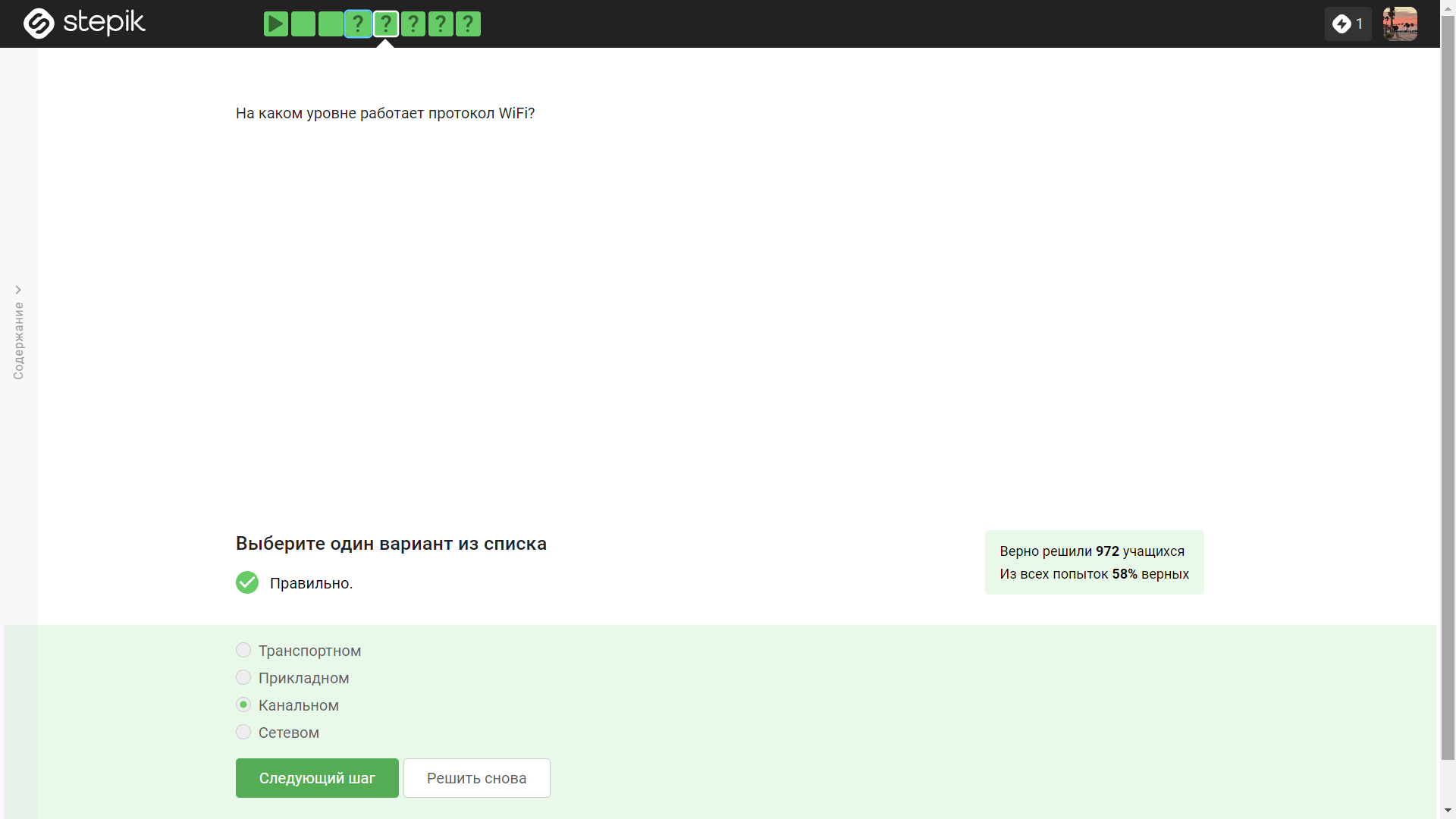


Figure 19: девятнадцатое задание

1. 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.

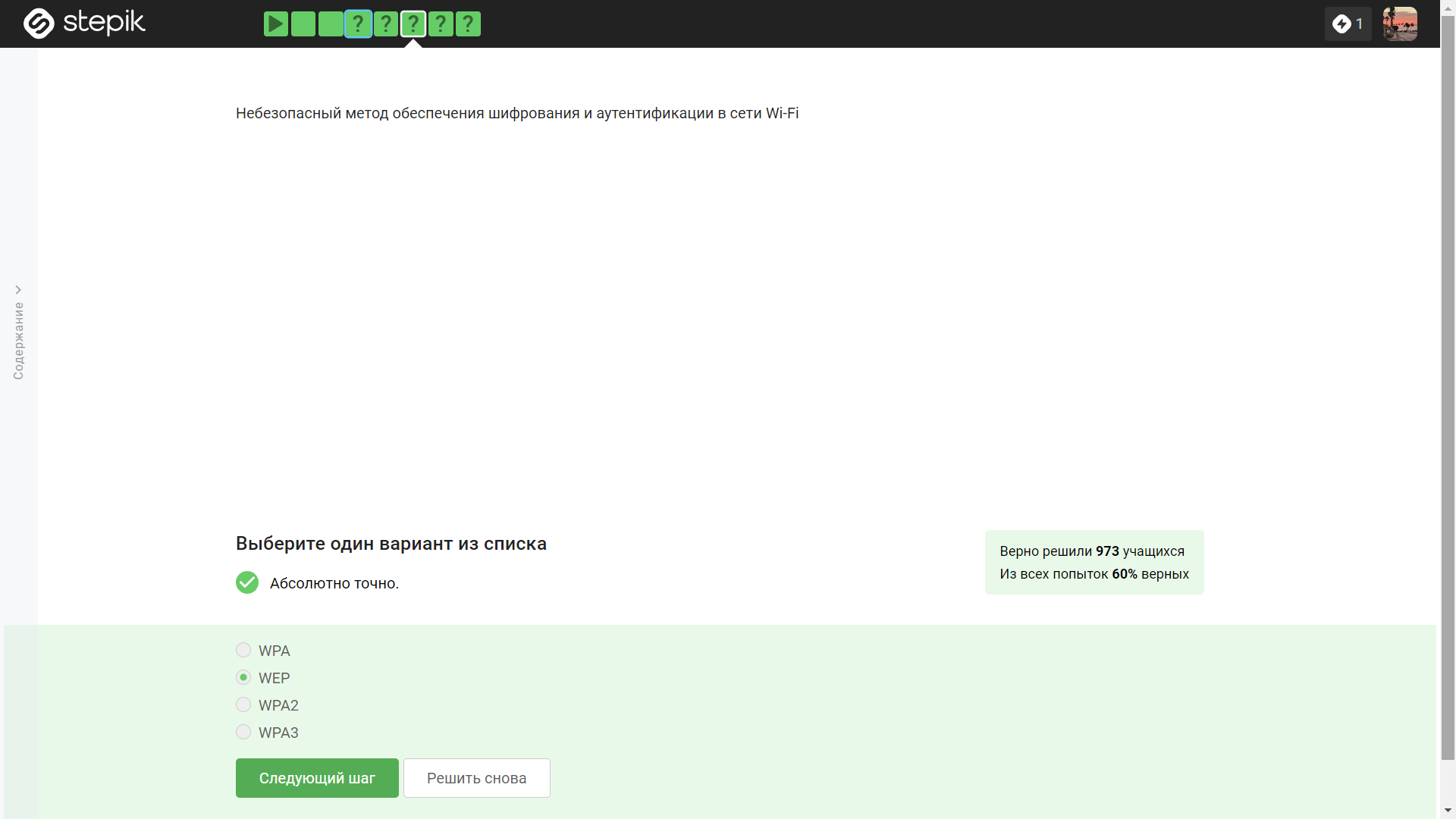


Figure 20: двадцатое задание

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

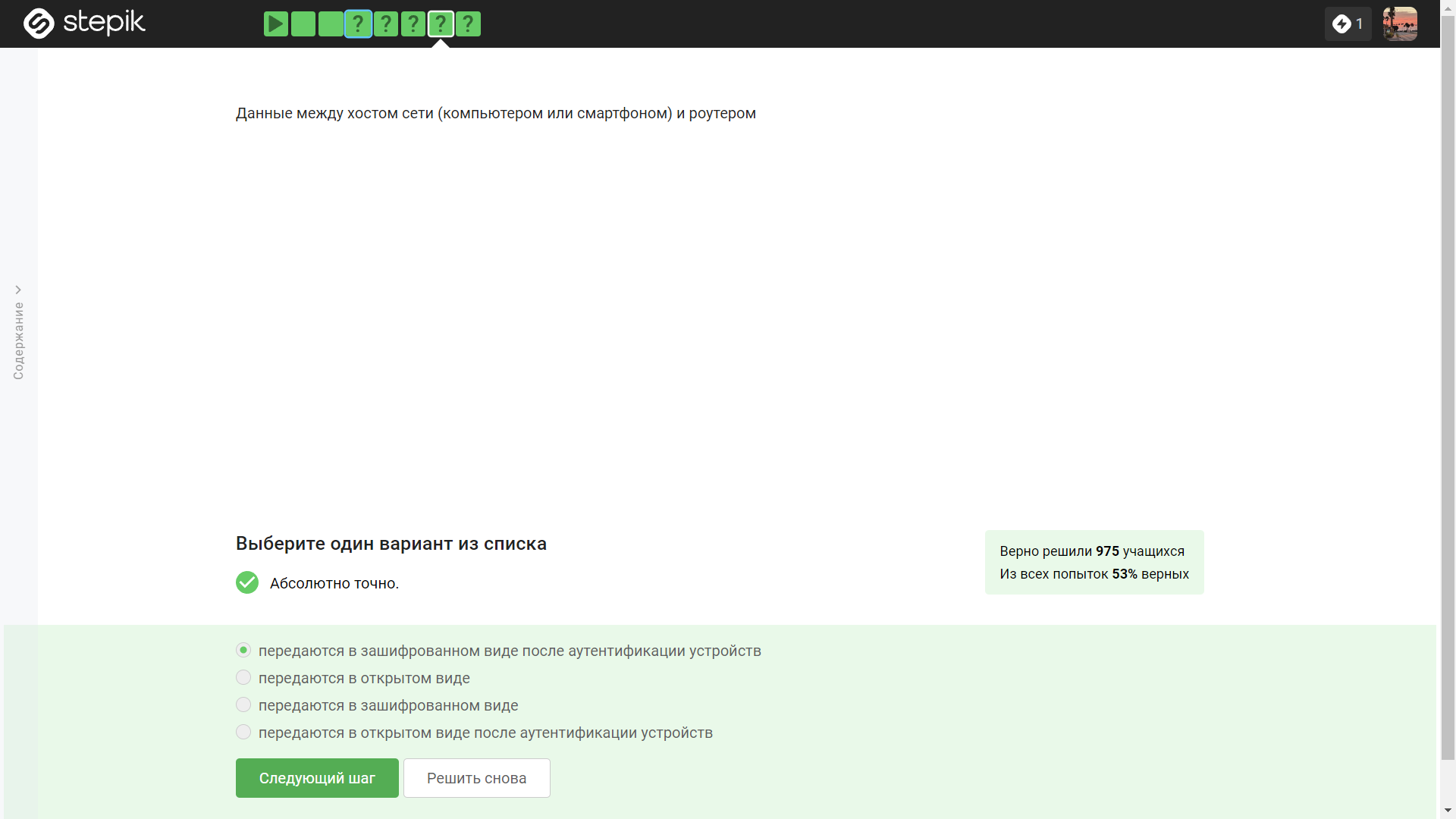


Figure 21: двадцать первое задание

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

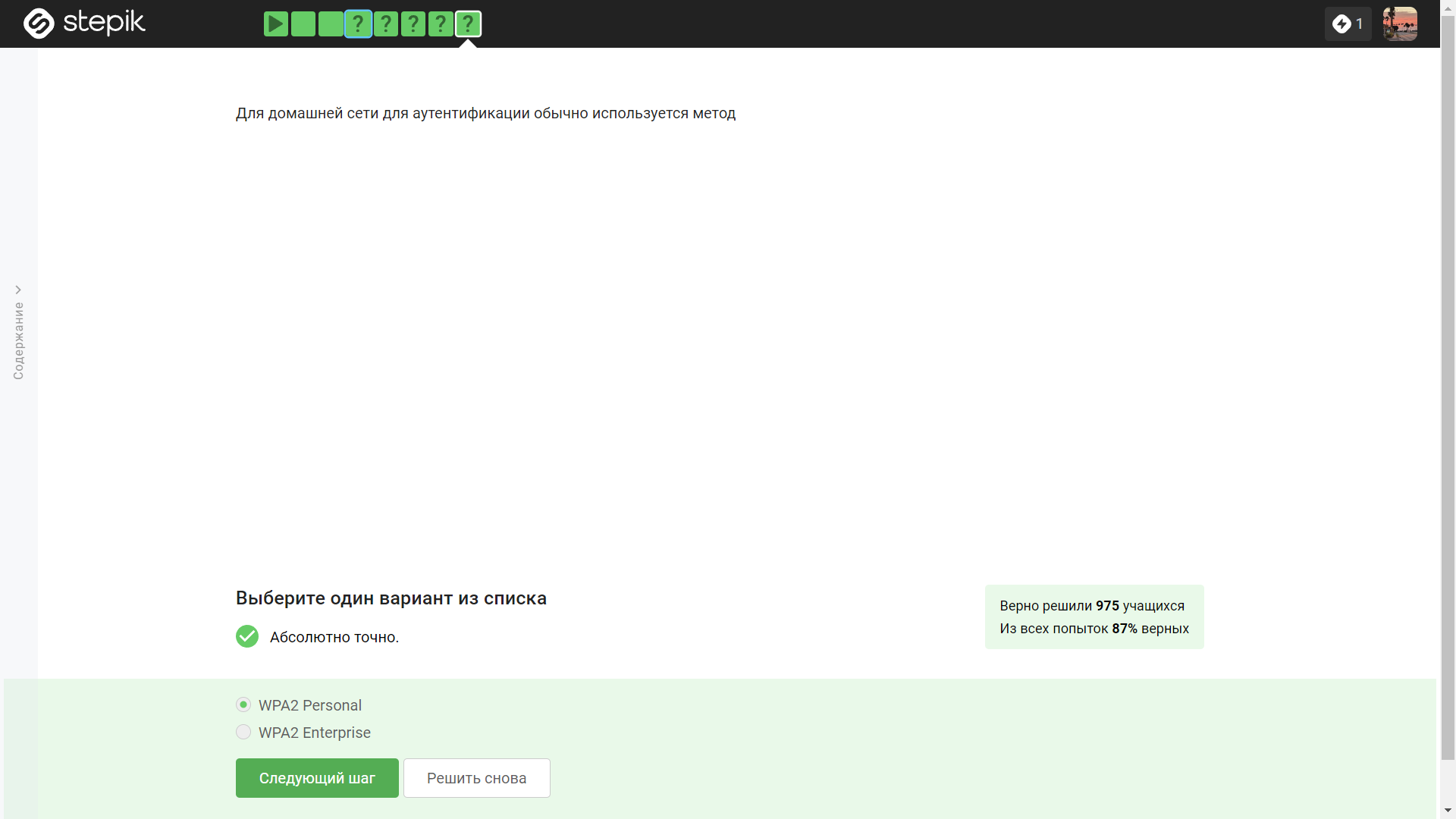


Figure 22: двадцать второе задание

# 3 Выводы

Я изучил основы безопасности в сети.

# 4 Список литературы

Конспекты к лекциям курса “Основы кибербезопасности”.