Этап1

НКАбд-01-23

Улитина Мария Максимовна

Содержание

# 1 Выполнение первого этапа внешнего курса

HTTPS - протокол прикладного уровня (рис. 1).

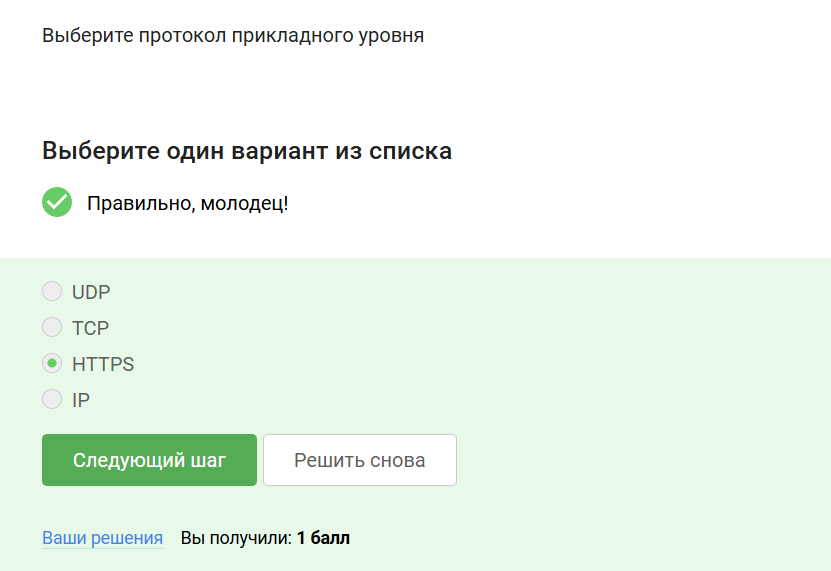


Рис. 1: HTTPS

TCP - протокол транспортного уровня (рис. 2).

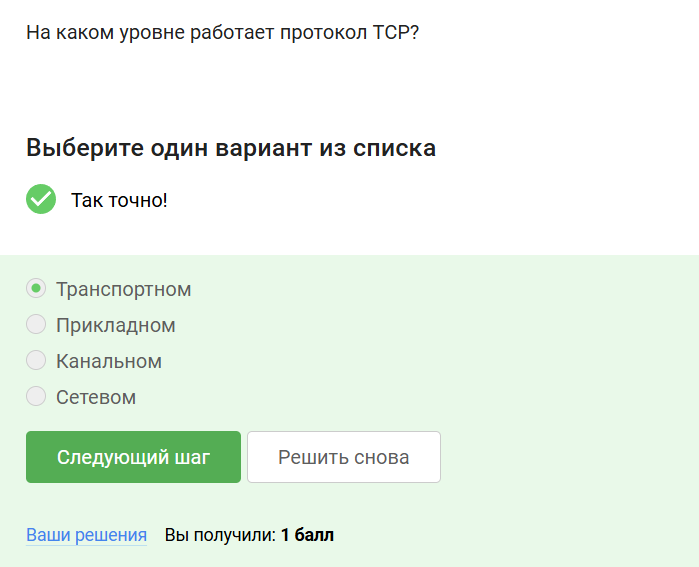


Рис. 2: TCP

225 и меньше (рис. 3).

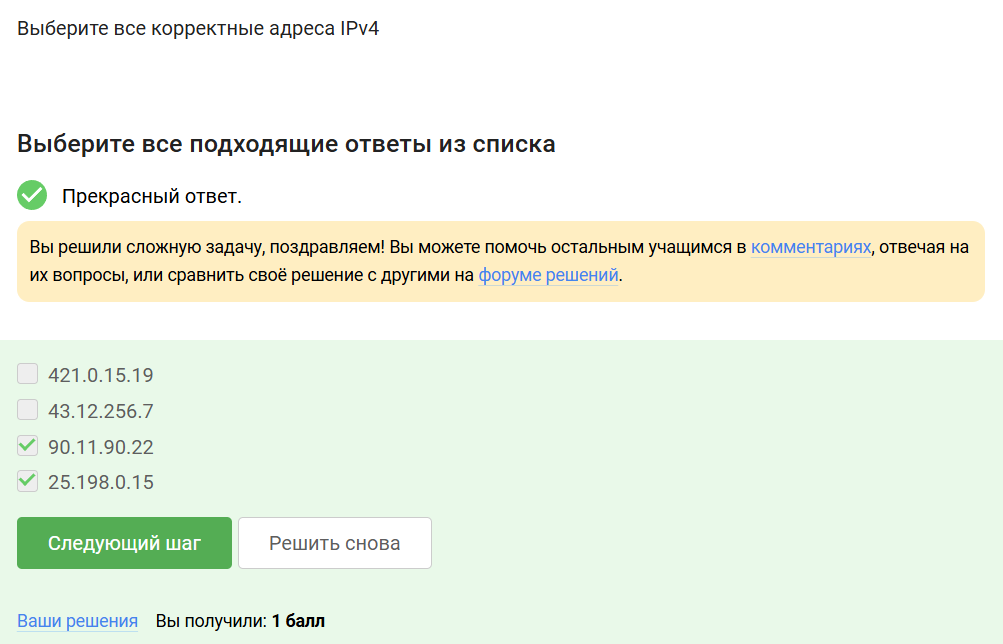


Рис. 3: IP

DNS сервер сопоставляет IP адреса доменным именам (рис. 4).

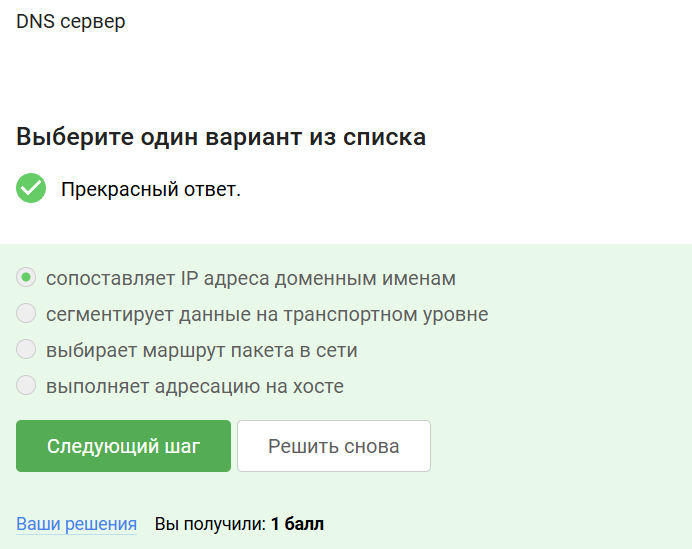


Рис. 4: DNS

Последовательность протоколов (рис. 5).

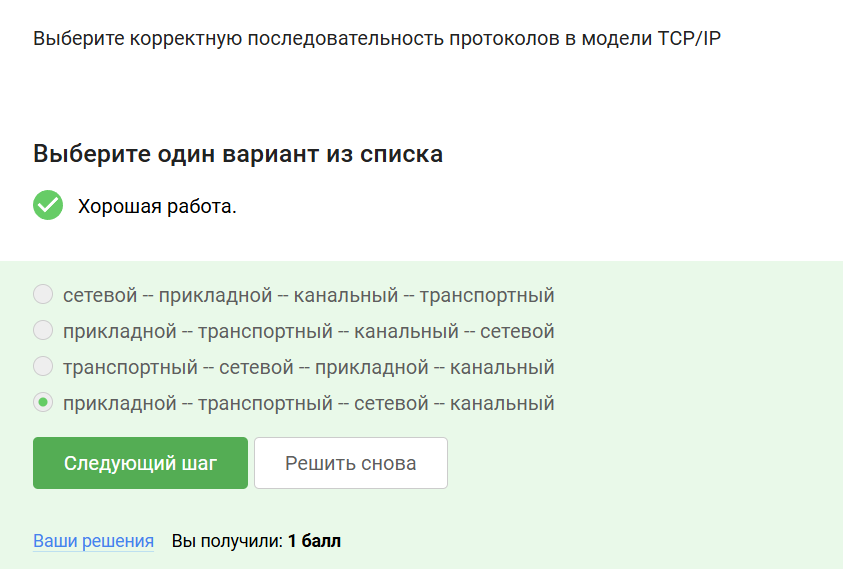


Рис. 5: TCP/IP

http передает в открытом виде (рис. 6).

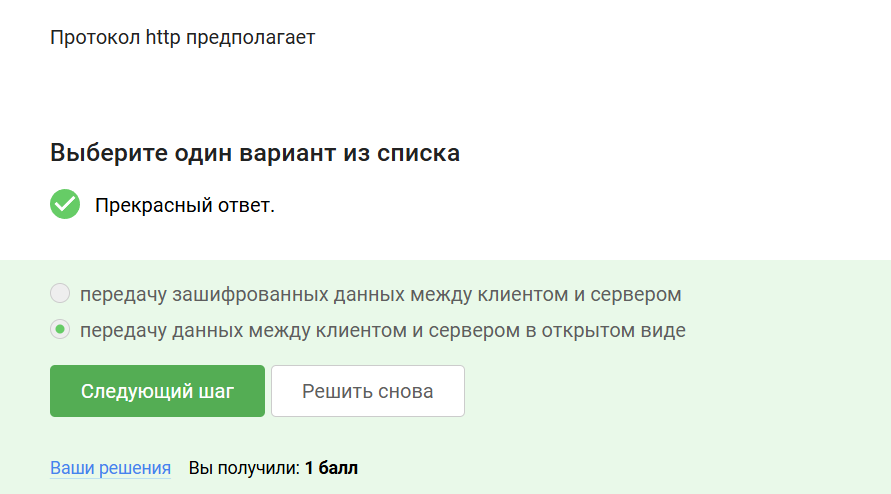


Рис. 6: HTTP

HTTPS состоит из двух фаз (рис. 7).

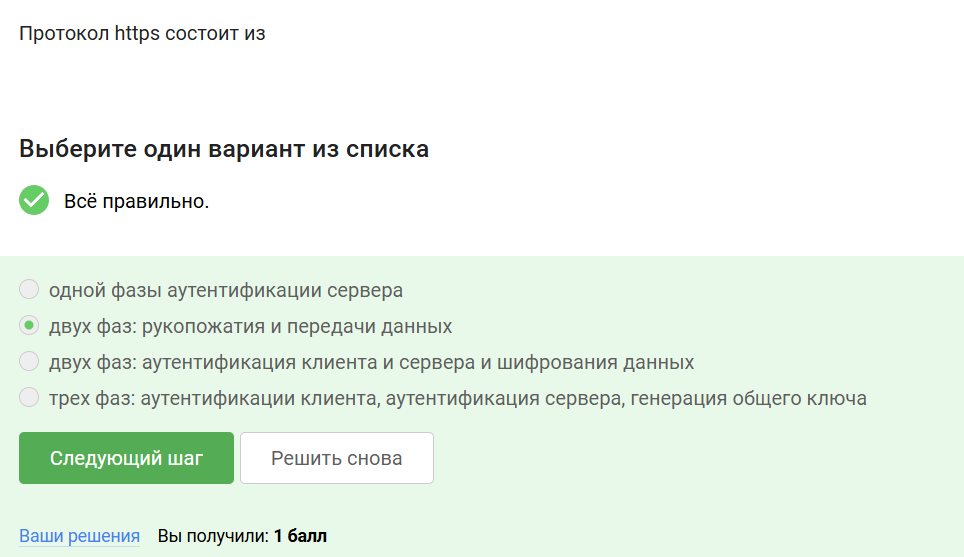


Рис. 7: HTTPS

Версия TLS определяется и клиентом, и сервером (рис. 8).

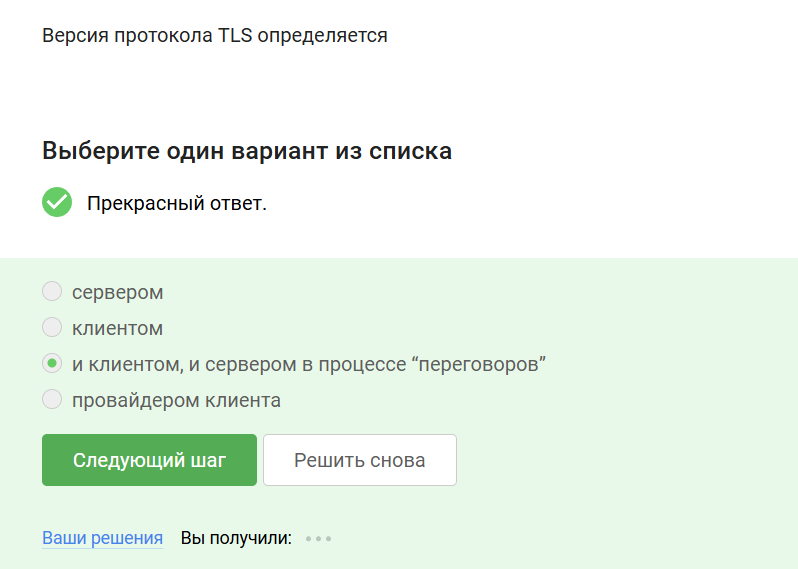


Рис. 8: TLS

Шифрование данных не предусмотрено (рис. 9).

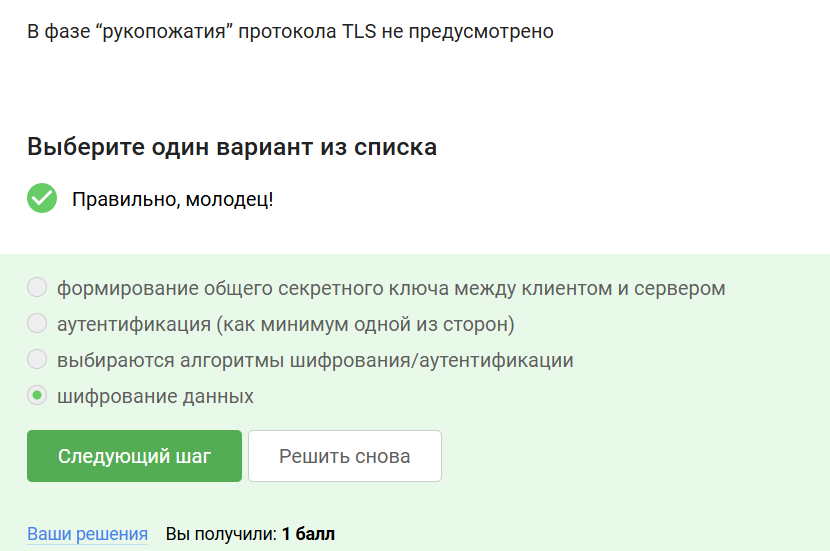


Рис. 9: TLS

Куки хранит id сессии и идентификатор пользователя (рис. 10).

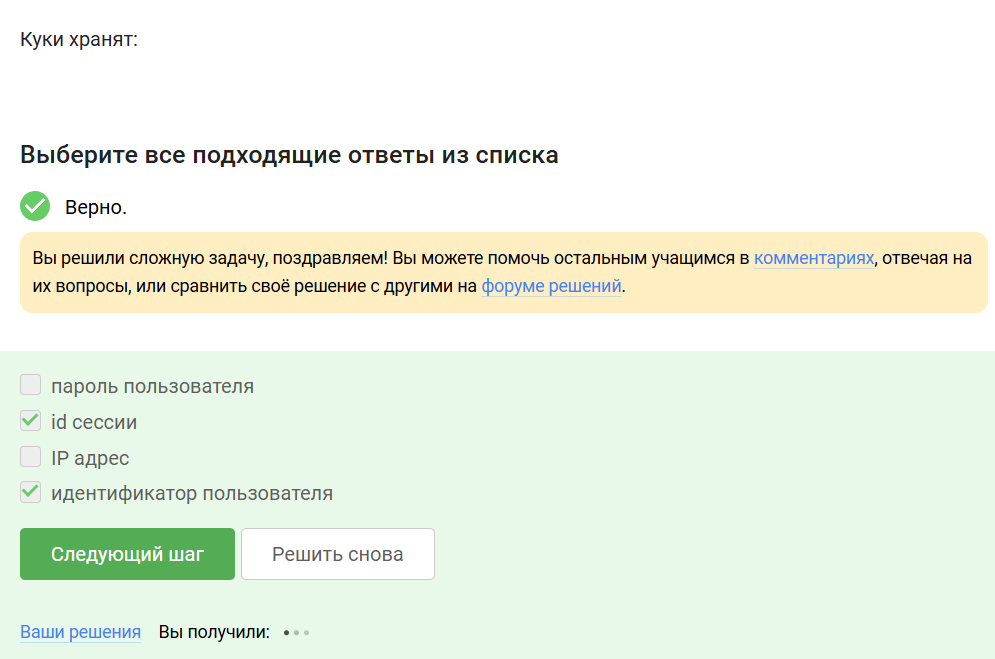


Рис. 10: cookie

Куки НЕ используется для улучшени надежности соединения (рис. 11).

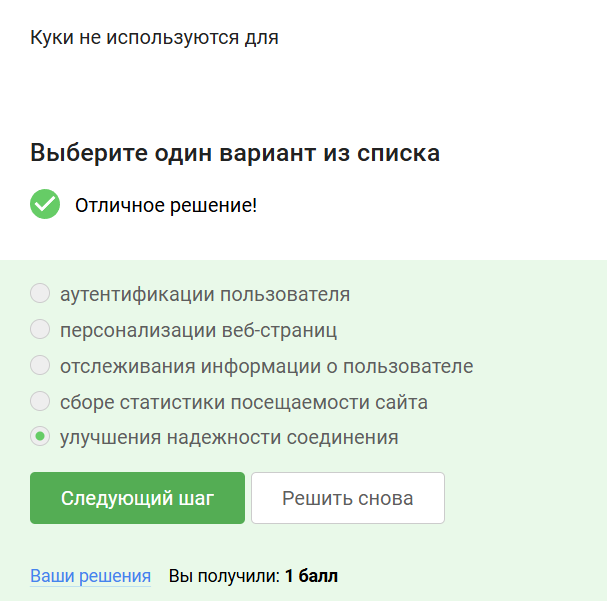


Рис. 11: куки

Куки генерируются сервером (рис. 12).

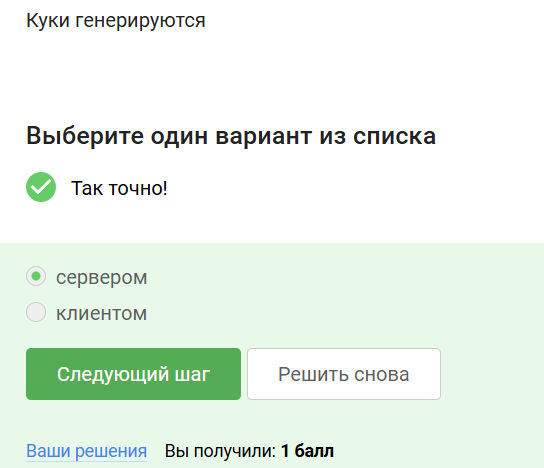


Рис. 12: куки

Сессионные куки хранятся в браузере на время пользования веб сайтом (рис. 13).

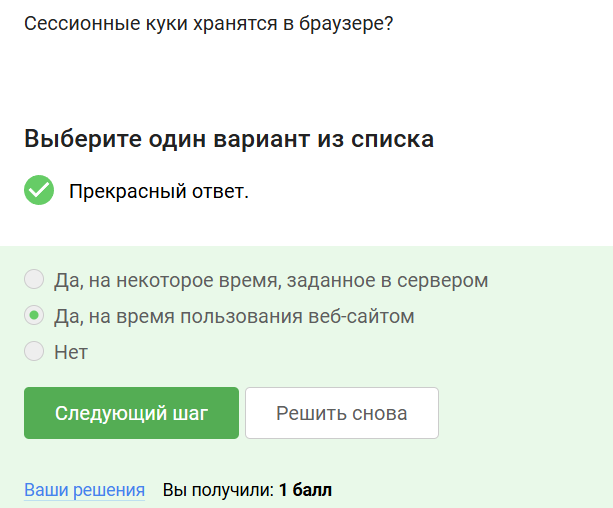


Рис. 13: куки

ТОР имеет 3 промежуточных узла (рис. 14).

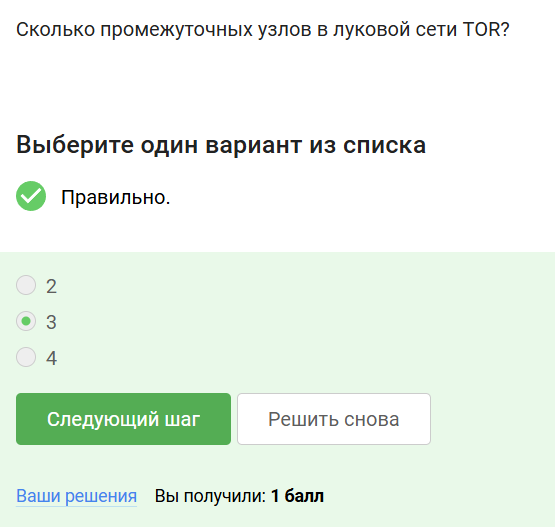


Рис. 14: тор

IP адрес получателя известен отправителю и выходному узлу (рис. 15).

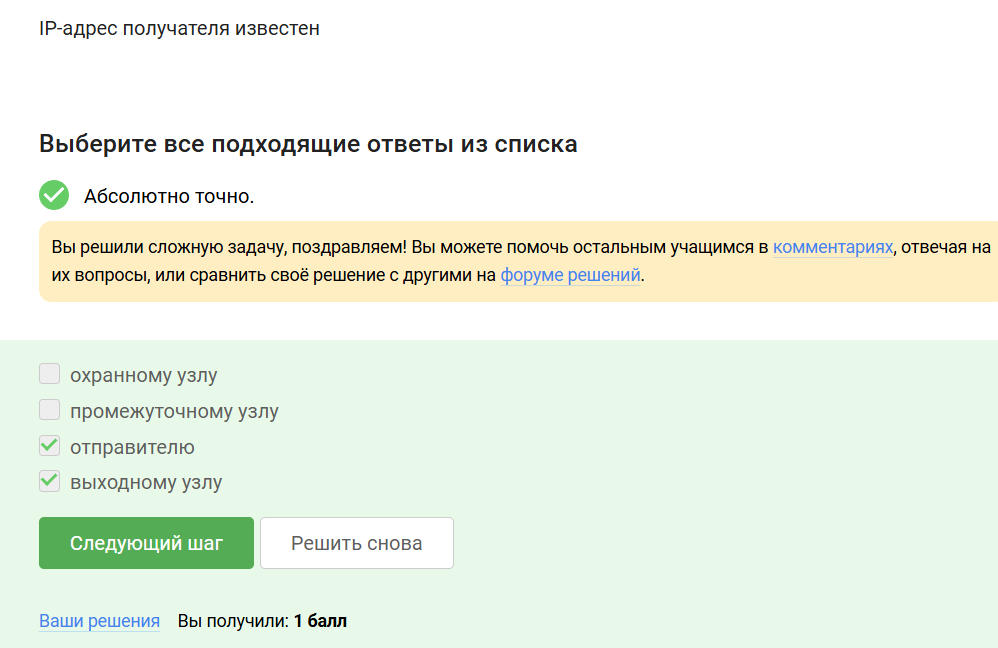


Рис. 15: тор

Отправитель генерирует общий секретный ключ с охранным, промежуточным и выходным узлом (рис. 16).

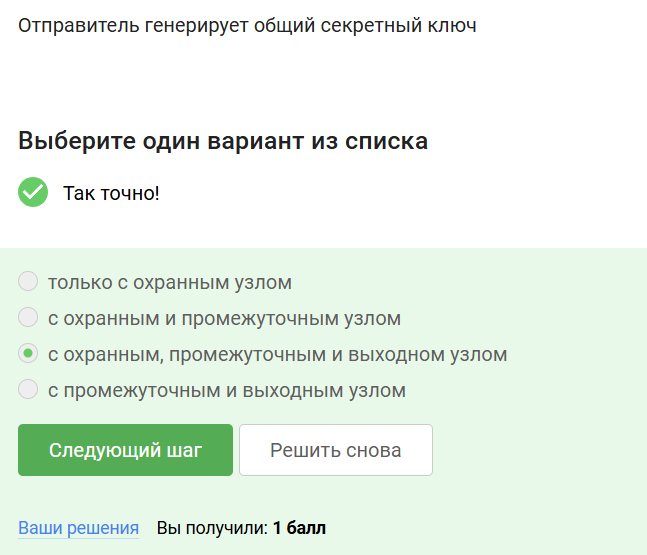


Рис. 16: секретный ключ

Нет, не должен (рис. 17).

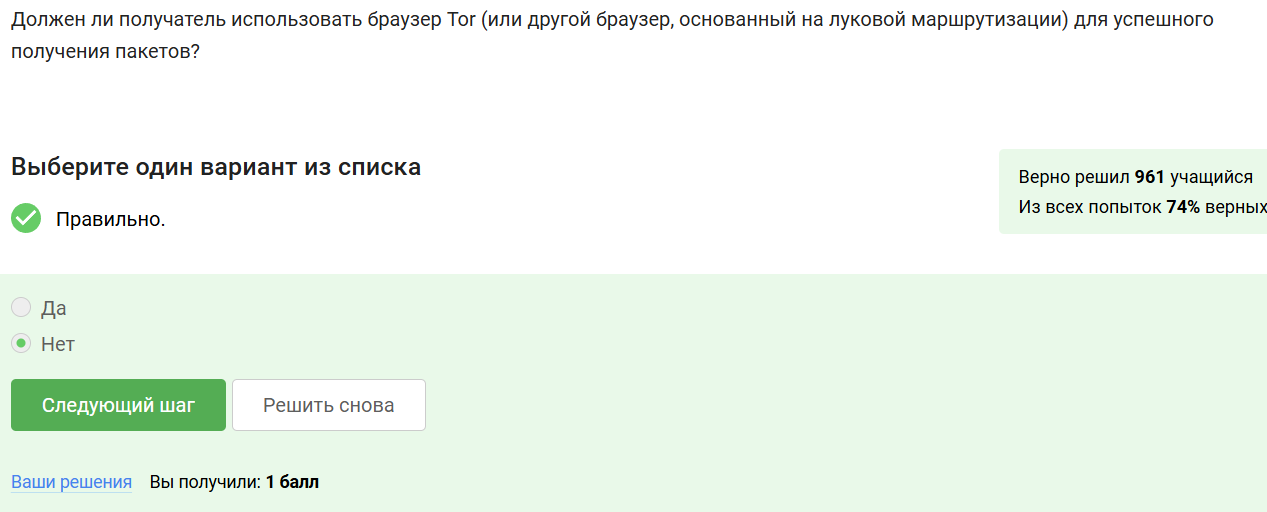


Рис. 17: секретный ключ

Wi-Fi технология (рис. 18).

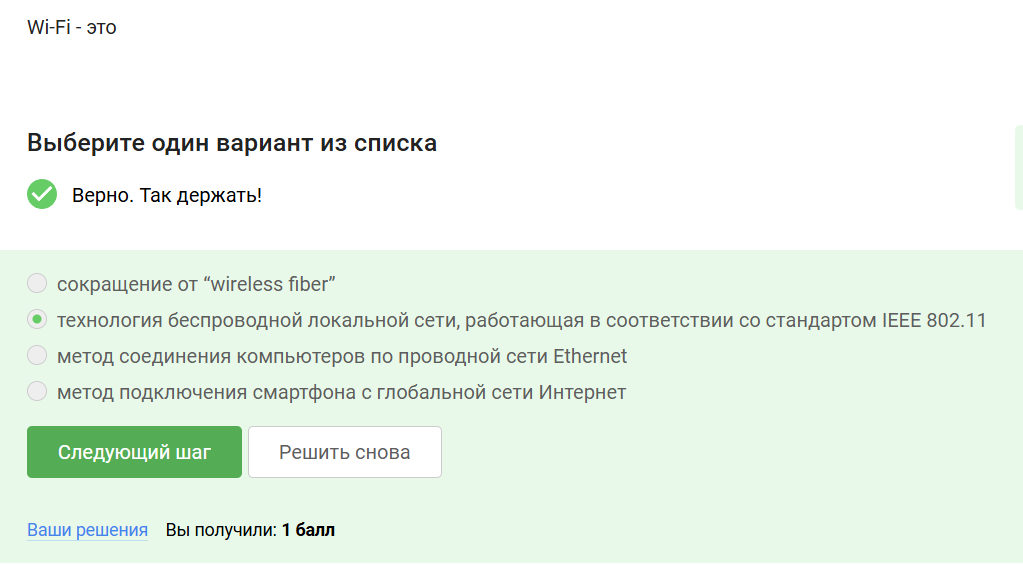


Рис. 18: WiFi

Работает на канальном уровне (рис. 19).

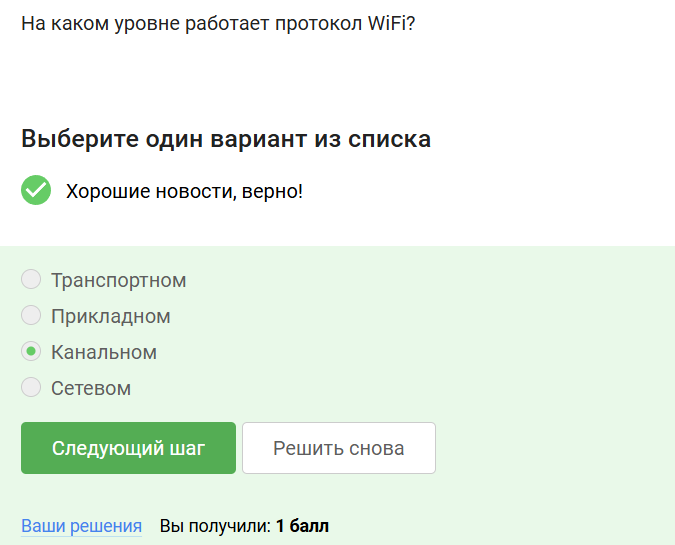


Рис. 19: вайфай

WEP - небезопасный метод (рис. 20).

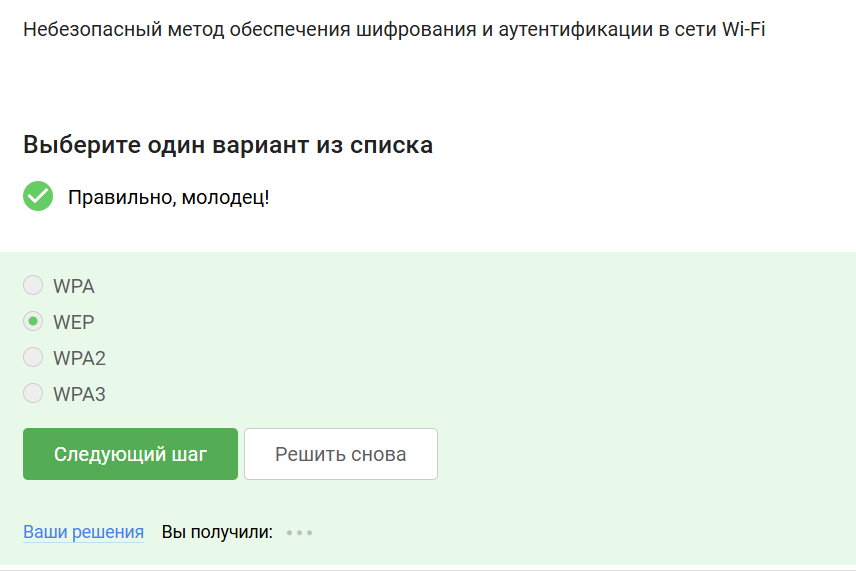


Рис. 20: вайфай

Данные передаются в зашифрованном виде (рис. 21).

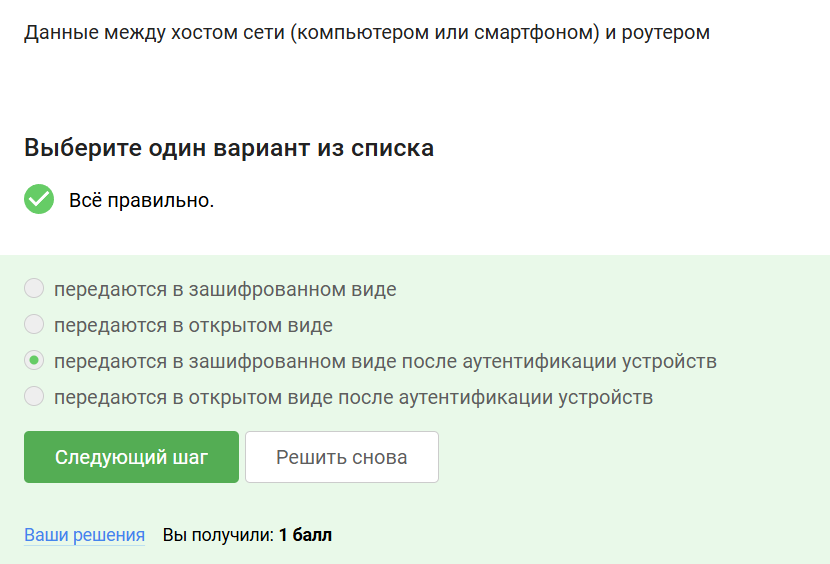


Рис. 21: вайфай

Для домашней сети (рис. 22).

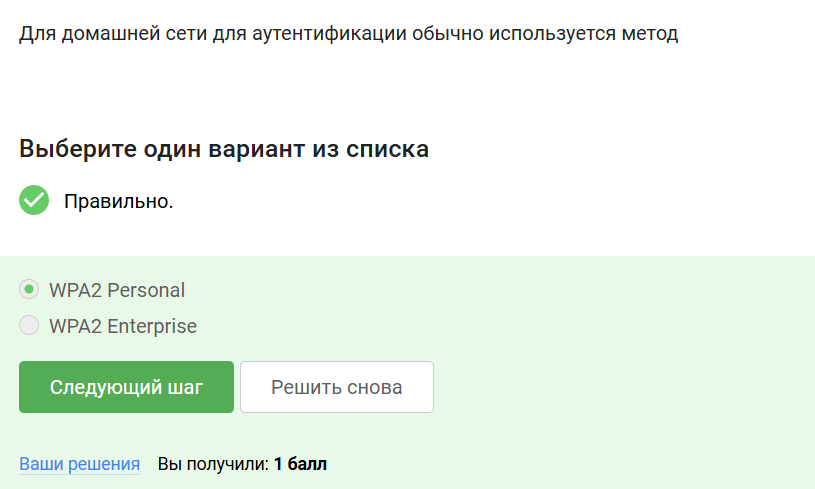


Рис. 22: вайфай

# 2 Выводы

Выволнен первый этап.