Отчёт прохождения внешнего курса

Безопасность в сети

Тарутина Кристина

Содержание

# 1 Цель работы

Провести контроль усвоения теоритического материала раздела “Безопасность в сети”

# 2 Выполнение контрольных заданий

Протокол HTTP(S) является примером протокола прикладного уровня, по которому передаются веб-страницы. Об этом как раз говорилось в лекции. (рис. 1).

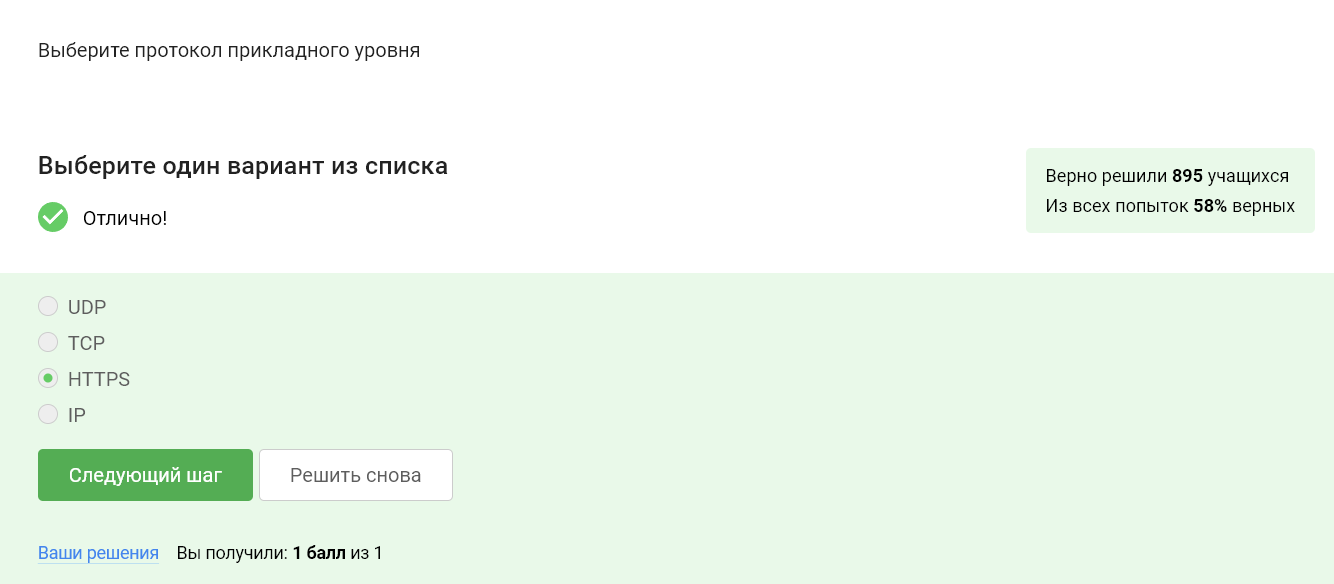


Рис. 1: Задание 1

На транспортном уровне существуют два основных протокола: TCP и UDP. TCP, в честь которого названа модель, обеспечивает надежную передачу пакетов данных. В отличие от него, UDP не гарантирует надежную доставку. Протокол TCP используется для передачи таких данных, как электронная почта или веб-страницы, где важна целостность информации.(рис. 2).

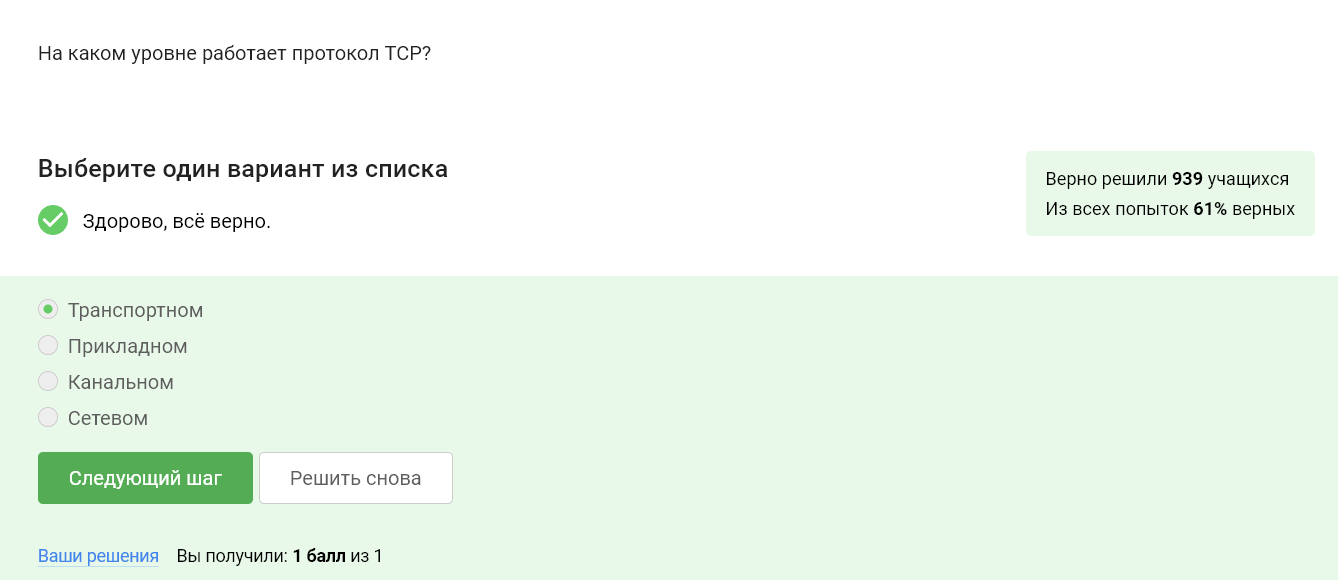


Рис. 2: Задание 2

IP-адреса представляют из себя числа от 0 до 255, разделённый точкой, так что выбираете те варианты, где числа находятся в данном диапазоне(рис. 3).

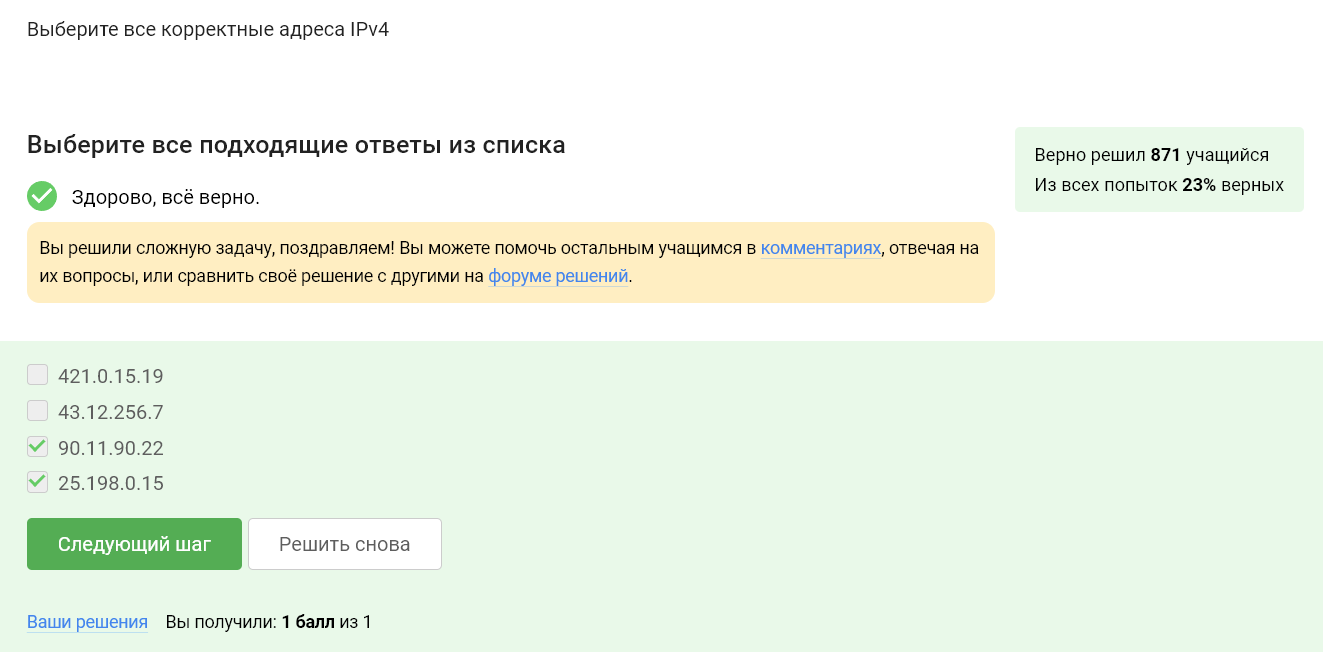


Рис. 3: Задание 3

В лекции говорилось, что: “основная задача этого DNS-сервера - это сопоставить название, то есть доменное имя, с корректным IP-адресом, с тем, где лежит этот сервер, этот сайт” (рис. 4).

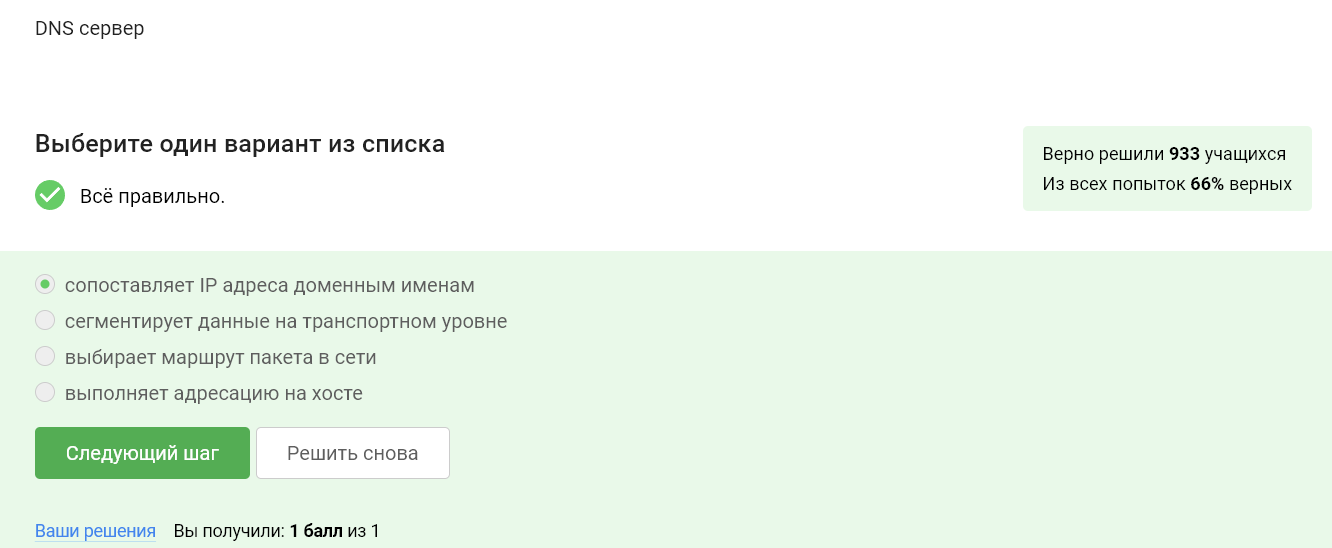


Рис. 4: Задание 4

Всё начинается с прикладного уровня, предоставляющего доступ для пользовательских программ к службам интернета, после чего переходит на транспортный. Там происходит адресация и передача данных. Потом мы переходим на сетевой уровень, где вычисляем возможность доставки данных и они передаются между физичскими сетями. И уже потом идёт канальный уровень(рис. 5).

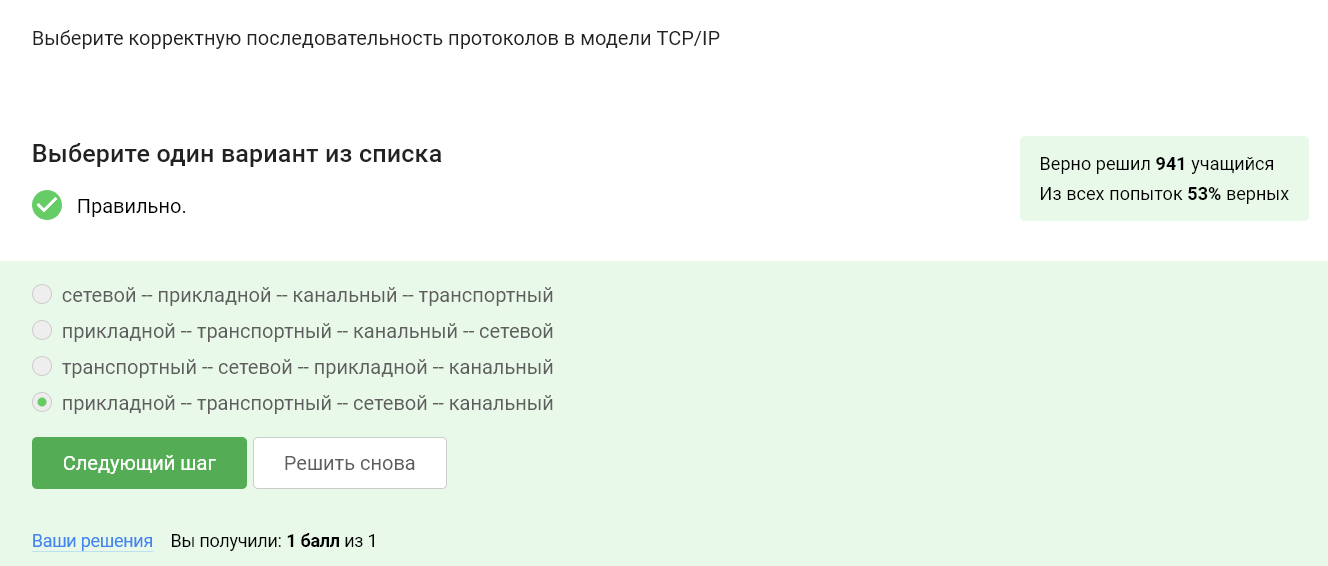


Рис. 5: Задание 5

Он предполагает передачу данных между клиентом и сервером в открытом виде, а вот HTTPS в зашифрованном. ДОполнительная буква s как бы даже намекает нам на это(рис. 6).

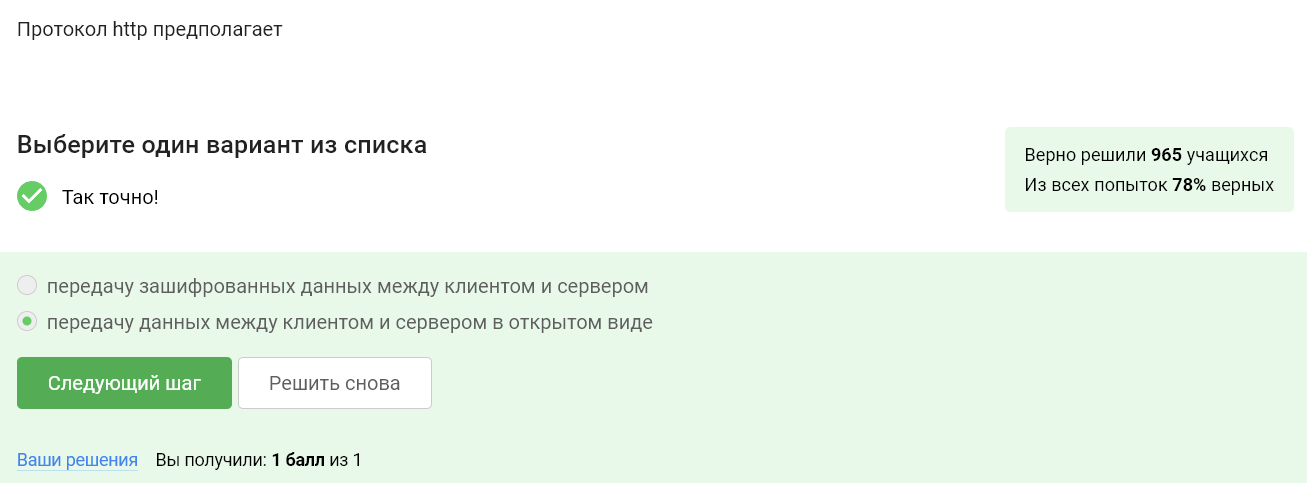


Рис. 6: Задание 6

Из двух фактов. СНачала происходит процесс “рукопожатия”, а уже потом пердачи данных.(рис. 7).

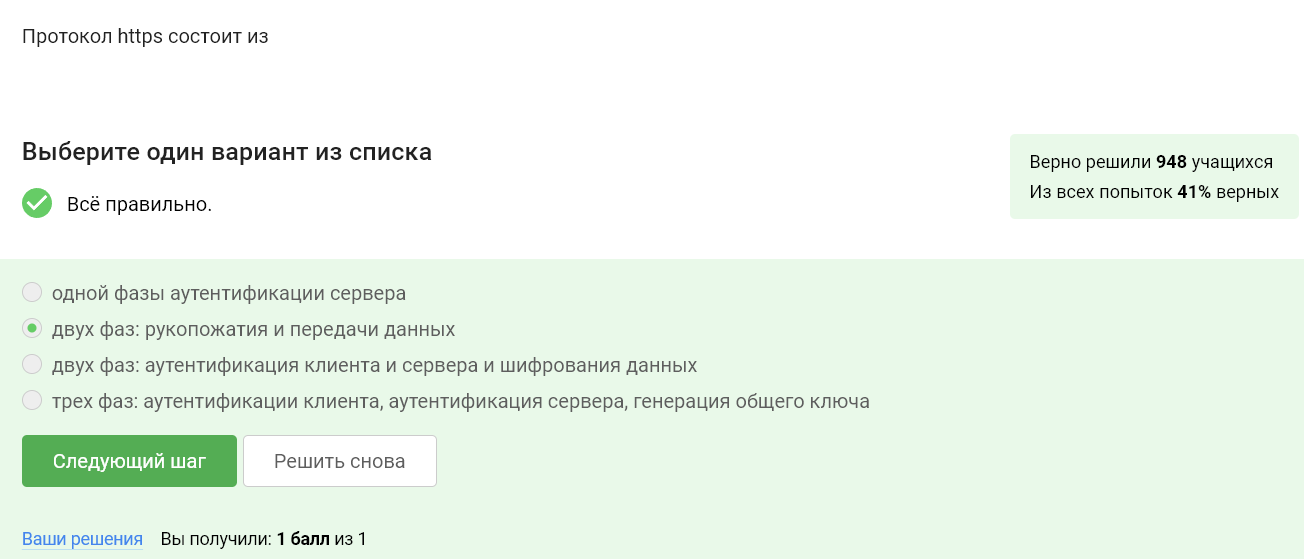


Рис. 7: Задание 7

ВЕрсия протокола определяется не только клиентом, она также определяется сервером, как бы с двух сторон одновременно(рис. 8).

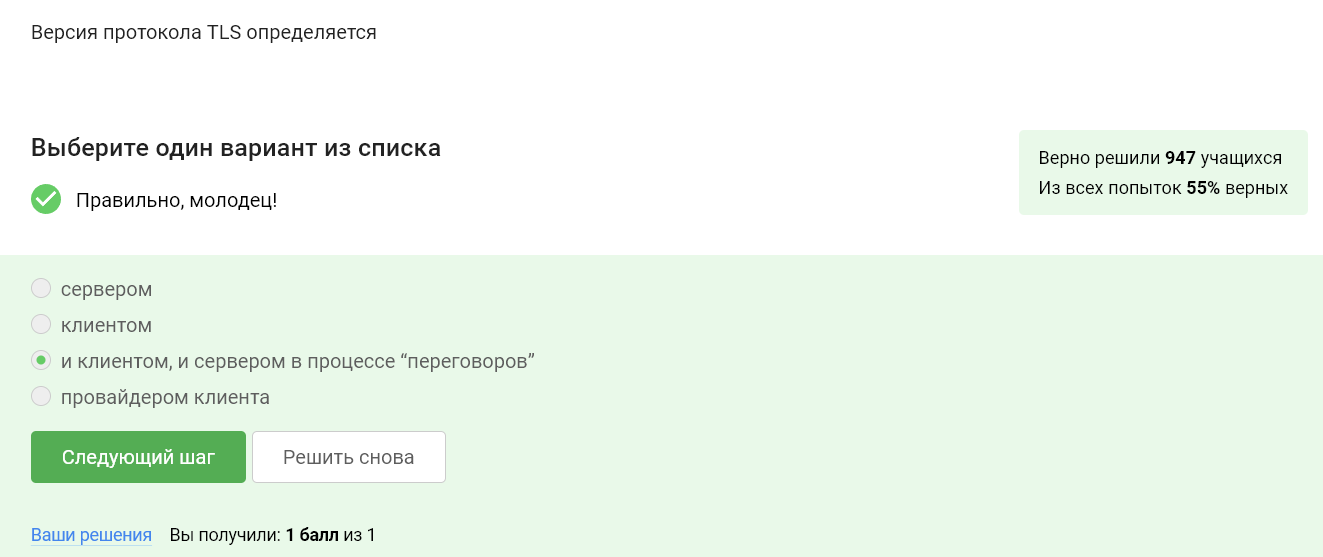


Рис. 8: Задание 8

Шифрования данных. Оно происходит позже, а вот все подготовительные этапы, выбор алгоритмов, формирование секретного ключа как раз происходят в фазе рукопожатия(рис. 9).

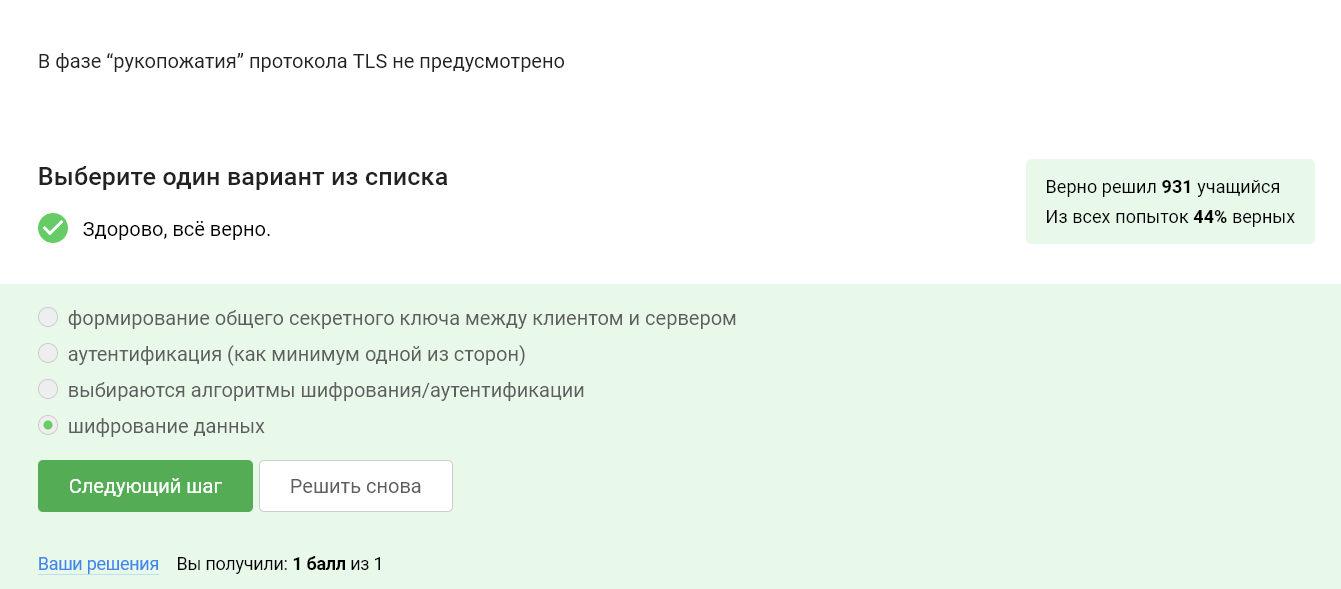


Рис. 9: Задание 9

Куки хранят индентификатор пользователя и id сессии, но они никога, ни в коем случае не будут хранить пароля пользователя. Это не только нецелесообразно, но и попросту опасно(рис. 10).

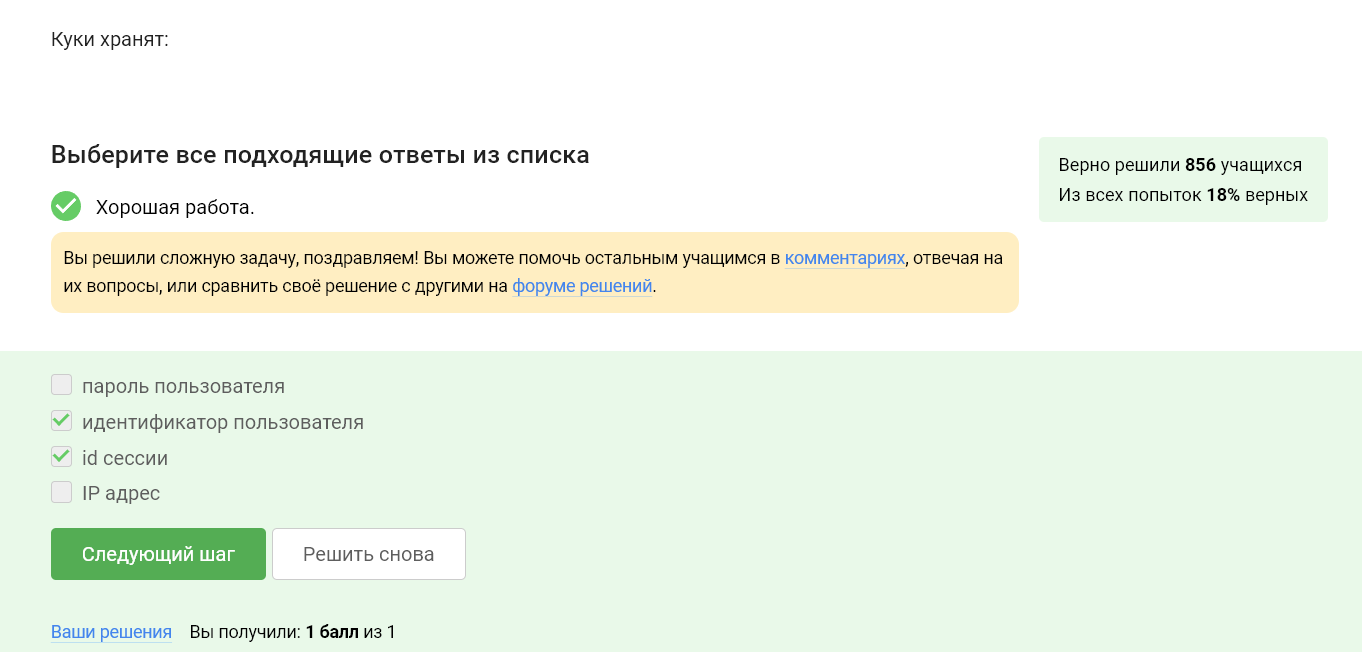


Рис. 10: Задание 10

Для улучшения надежности соединения, для всего остального они используются. ДАже наша персонализирующая реклама, удивляющая многих не сведущих в этой теме пользователей, существует благодаря куки(рис. 11).

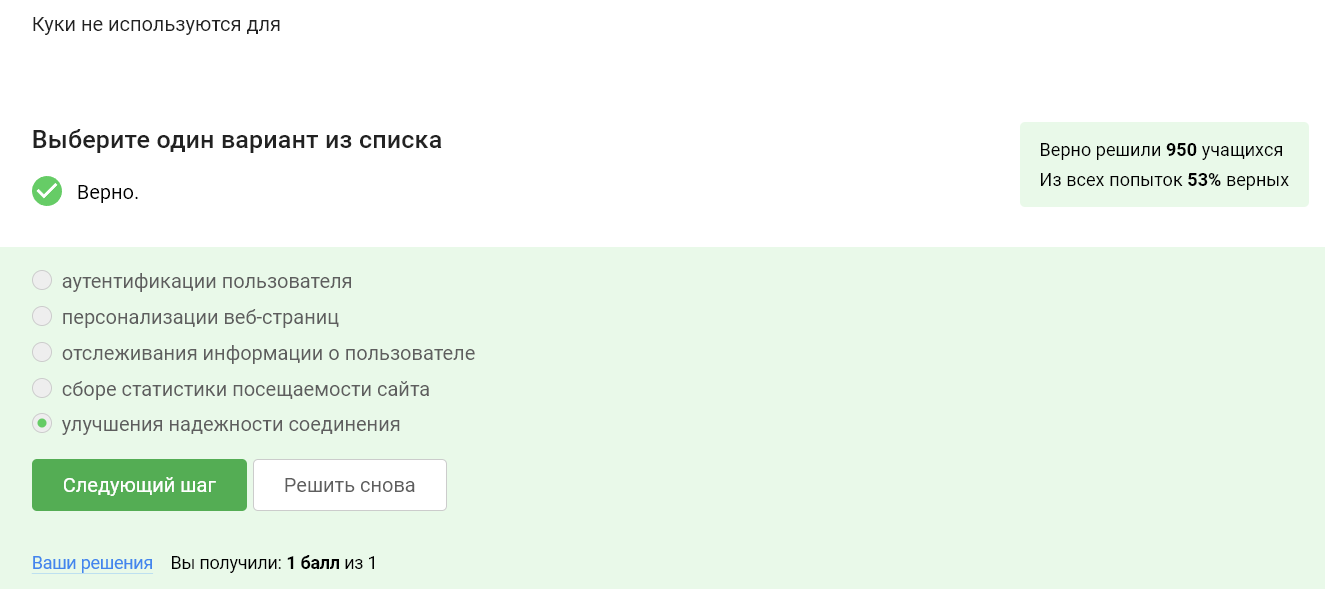


Рис. 11: Задание 11

Куки генерируются сервером, они не могут быть созданы клиентом(рис. 12).

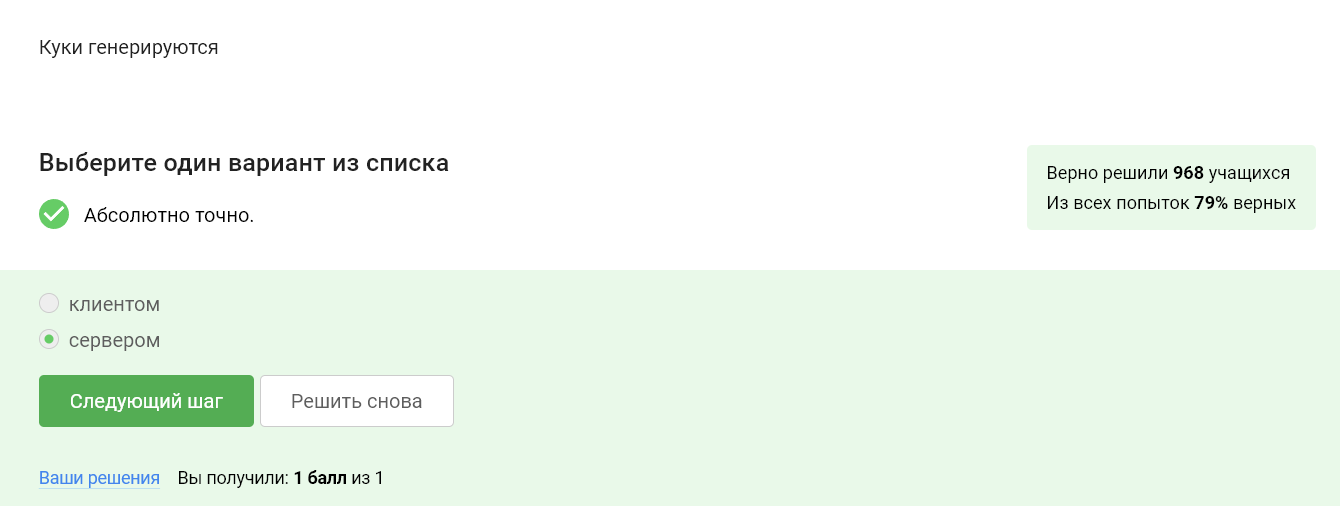


Рис. 12: Задание 12

Да, на время пользования веб-сайтом. Если, допустим, закрыть вкладку, то содержимое корзины в каком-нибудь онлайн магазине, использующим сессионные куки, пропадёт(рис. 13).

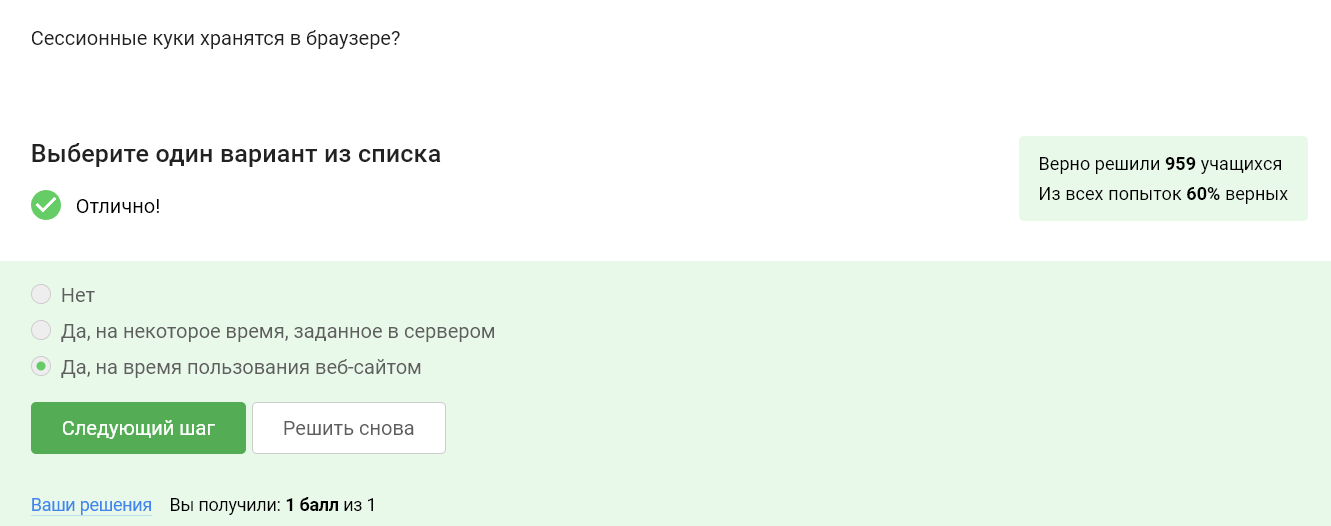


Рис. 13: Задание 13

Промежуточных узлов три. Два узла не гарантируют анонимизации, а 4 уже избыточно и не добавляет никакой эффективности(рис. 14).

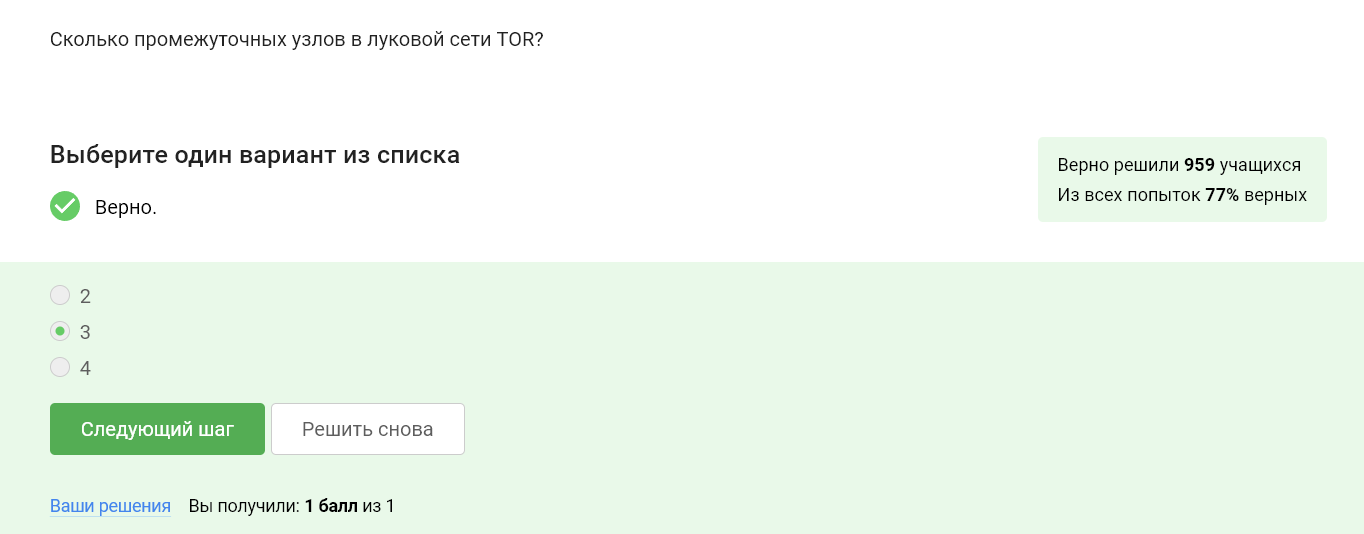


Рис. 14: Задание 14

Известен отправителю и выходному узлу. Ни охранный, ни промежуточный его не знают.(рис. 15).

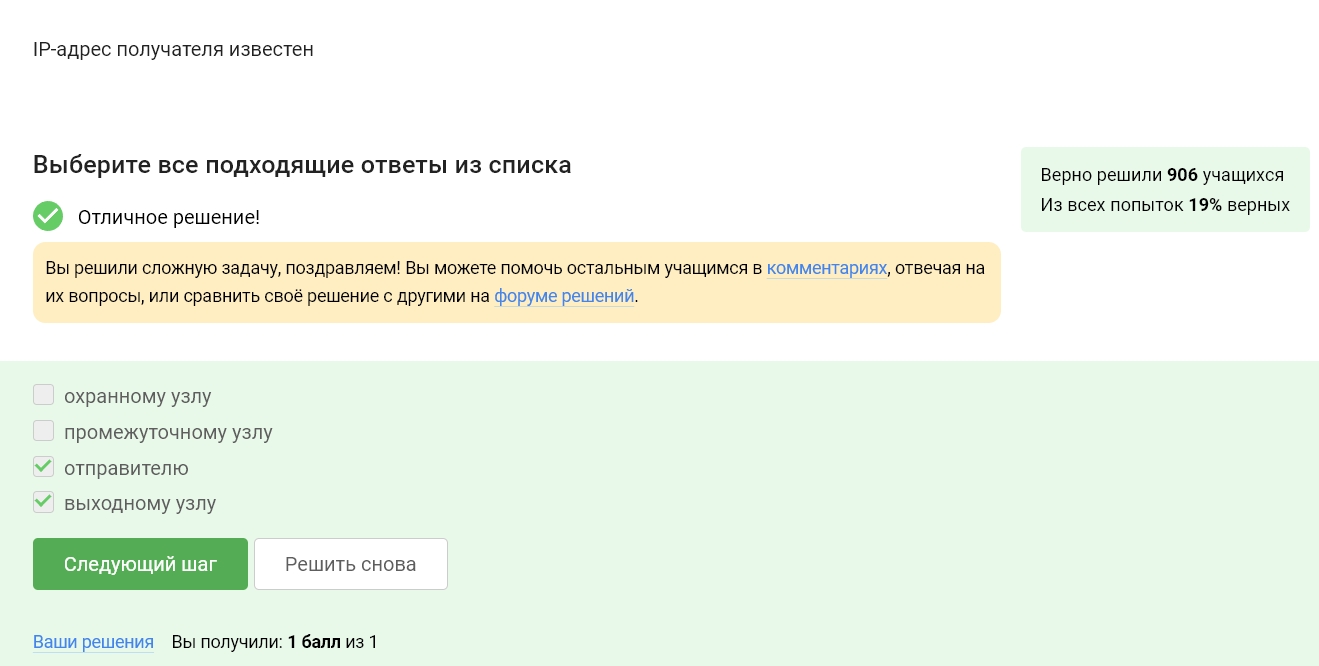


Рис. 15: Задание 15

С охранным, выходным и промежуточным узлом. Причём с промежуточным и выходным узлом он генерирует ключ с помощью охранного узла(рис. 16).

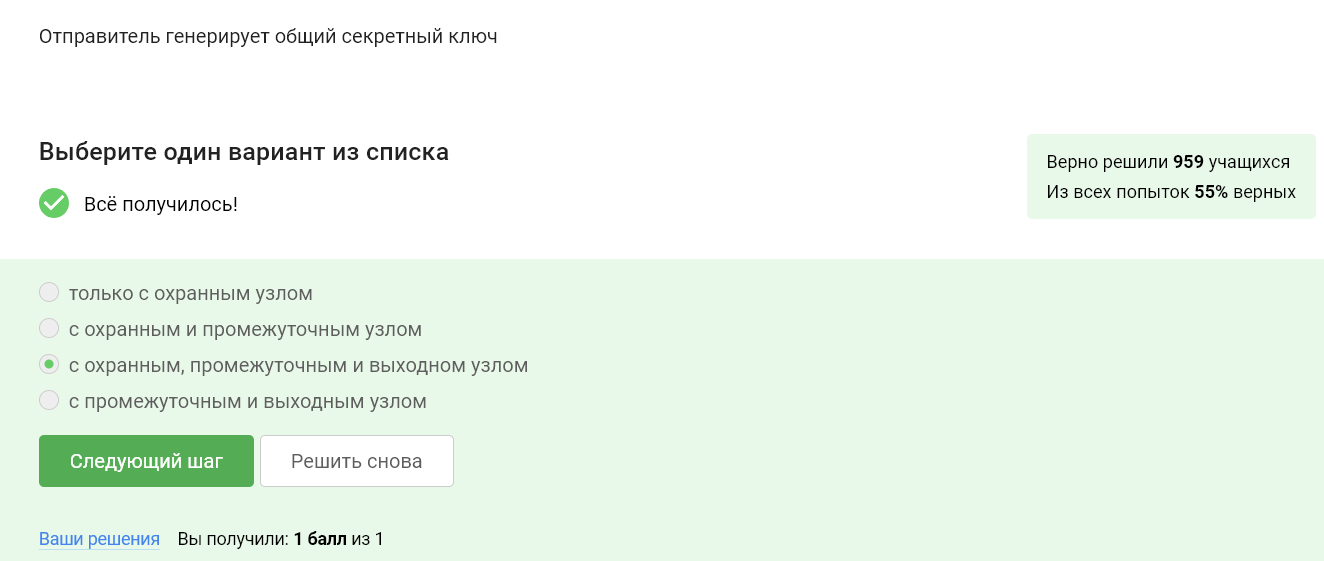


Рис. 16: Задание 16

Конечно нет. С этим могут справиться и другие браузеры.(рис. 17).

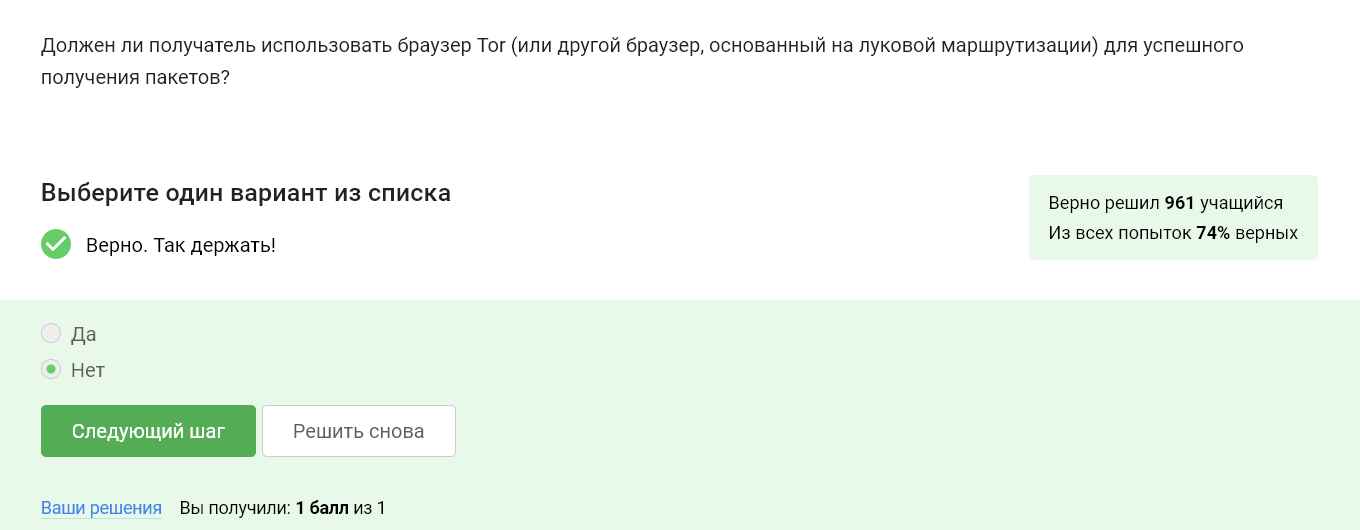


Рис. 17: Задание 17

В общем, WiFi – это технология беспроводной локальной сети, которая базируется на стандарте IEEE 802.11. IEEE представляет собой организацию, которая устанавливает стандарты для работы сети Интернет. Она определяет принципы функционирования беспроводного интернета, начиная с номера стандарта 802.11, и все последующие модификации этого стандарта носят аналогичное обозначение, за которым следуют дополнительные буквы.(рис. 18).

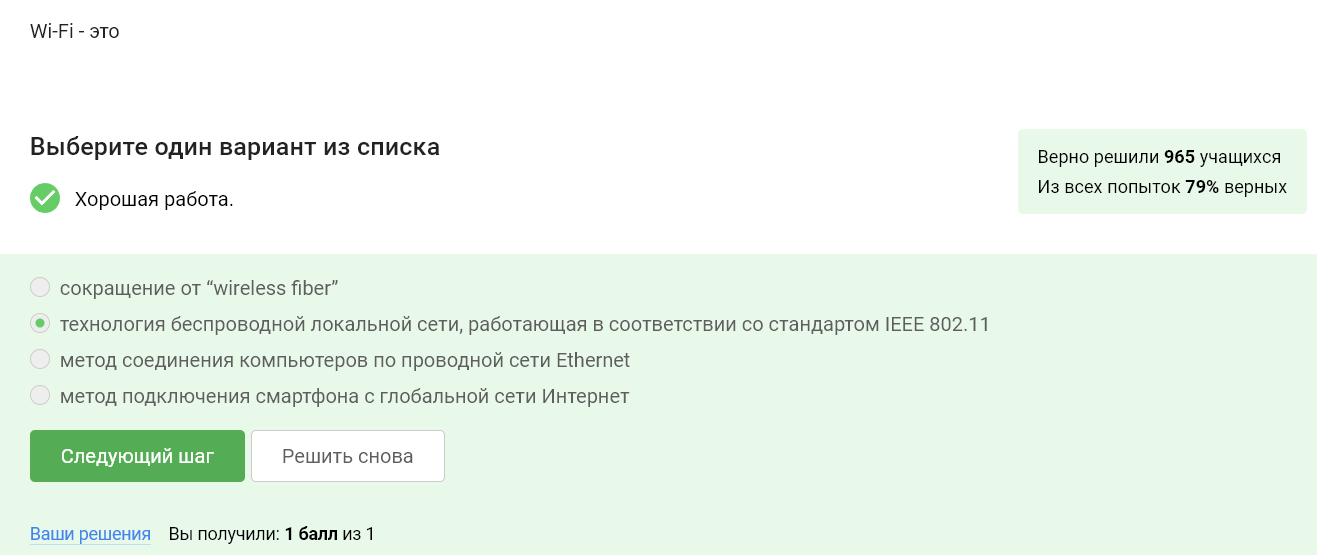


Рис. 18: Задание 18

На канальном уровне. В том числе канальный уровень обеспечивает помехоустойчивость(рис. 19).

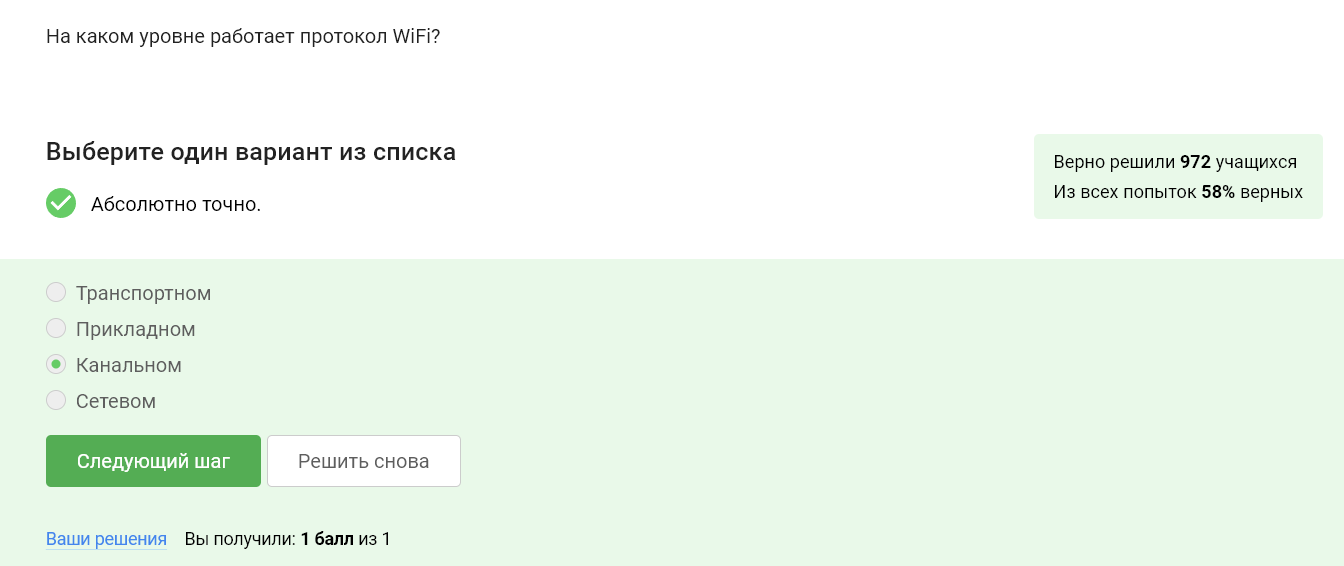


Рис. 19: Задание 19

Это WEP. А вот остальные методы вполне безопасны(рис. 20).

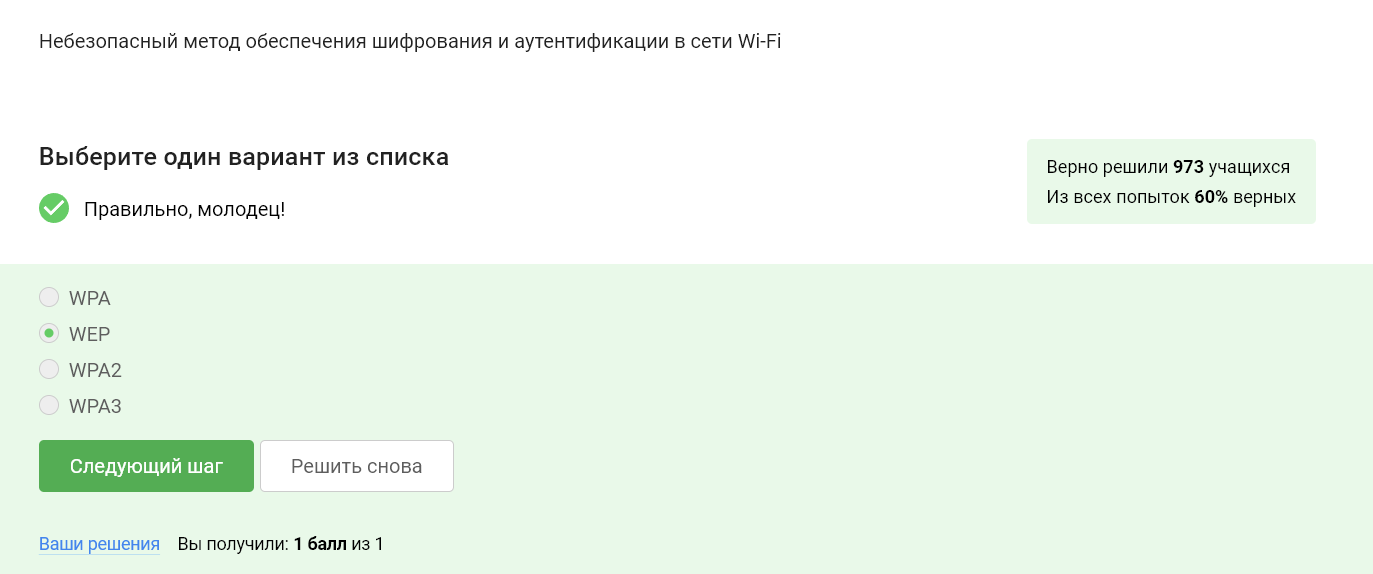


Рис. 20: Задание 20

Передаются в зашифрованном виде только после аутентификации устройств. Это обеспечивает защиту данных, иначе бы их могли украсть(рис. 21).

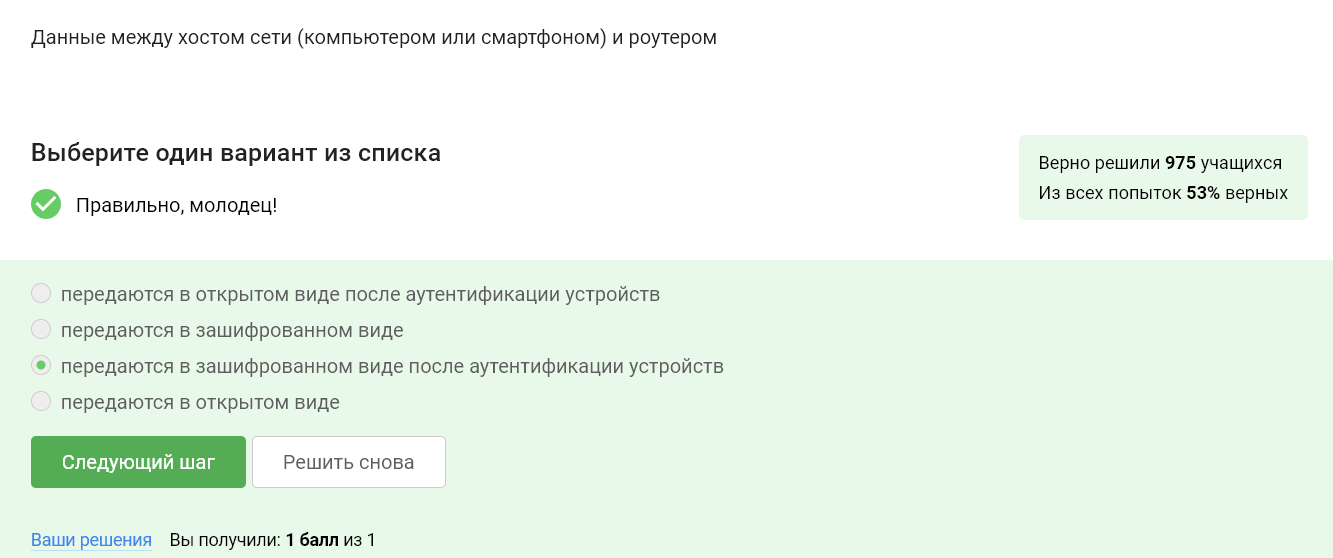


Рис. 21: Задание 21

НУ здесь можно догадаться даже не изучая курс, только по самим названиям. Хотя конечно об этом говорилось и в лекции.(рис. 22).

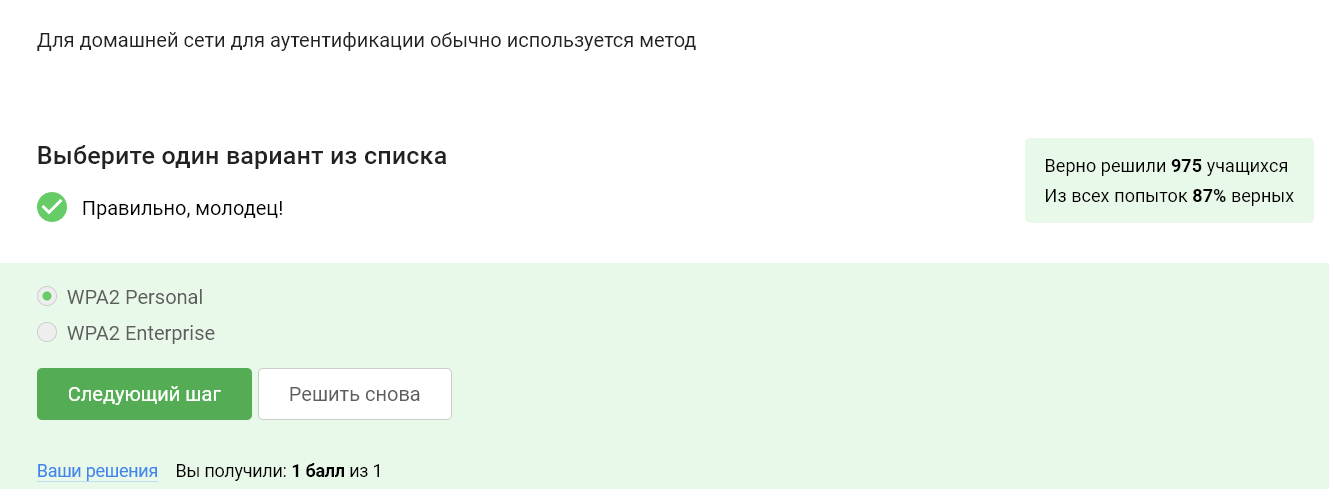


Рис. 22: Задание 22

# 3 Выводы

Мы успешно прошли контроль усвоения теоритического материала раздела “Безопасность в сети”

# Список литературы