# Прохождение внешнего курса 1 часть

**Безопасность в сети**

Кроитору Екатерина НБИ-бд-03-22

# Содержание

**1 Цель работы** **5**

**2 Задание** **6**

**3 Теоретическое введение** **7**

**4 Выполнение лабораторной работы** **10**

**5 Выводы** **25**

# Список иллюстраций


4.1 Тест 1 . . . . . 10
4.2 Тест 2 . . . . . 11
4.3 Тест 3 . . . . . 11
4.4 Тест 4 . . . . . 12
4.5 Пояснение ответа . . . . . 12
4.6 Тест 5 . . . . . 13
4.7 Тест 6 . . . . . 13
4.8 Тест 7 . . . . . 14
4.9 Тест 8 . . . . . 14
4.10 Тест 9 . . . . . 15
4.11 Тест 10 . . . . . 15
4.12 Тест 11 . . . . . 16
4.13 Тест 12 . . . . . 16
4.14 Тест 13 . . . . . 17
4.15 Тест 14 . . . . . 17
4.16 Тест 15 . . . . . 19
4.17 Тест 16 . . . . . 19
4.18 Тест 17 . . . . . 20
4.19 Тест 18 . . . . . 20
4.20 Пояснение ответа . . . . . 21
4.21 Тест 19 . . . . . 21
4.22 Пояснение ответа . . . . . 22
4.23 Тест 20 . . . . . 22
4.24 Тест 21 . . . . . 23
4.25 Тест 22 . . . . . 24

# Список таблиц

# 1 Цель работы

Понять, что происходит при открытии ссылки в браузере, как работает персонализация сети, Браузер TOR, анонимизация и беспроводные сети Wi-fi.

# 2 Задание

Выполнить тестовую часть курса

# 3 Теоретическое введение

Сетевой протокол - это некая последовательность правил, по которым, во-первых, устанавливается соединение между устройствами сети, то есть между вашим роутером, который, скорее всего, стоит у вас дома, и другими устройствами сети. И во-вторых, когда соединение установлено, начинается обмен данных, то есть с вашей стороны идет запрос в Сеть на открытие страницы поисковика, а к вам из Сети приходит страница этого поисковика.

Современные сетевые протоколы удобно описывать в виде модели протоколов, и современный Интернет работает в так называемой модели TCP/IP. Название TCP/IP состоит из двух самых популярных сетевых протоколов: это протокол TCP и протокол IP. Мы более подробно изучим эти протоколы далее в этой лекции. Сейчас важно понимать следующее: протокол TCP, если переводить его с английского, означает протокол управления передачей, и этот протокол отвечает за формирование пакетов данных. Все данные, которые передаются по сети, сформированы в некие пакеты, то есть в кусочки данных, в сегменты. И все данные, которые мы отправляем или получаем, мы получаем сегментировано по пакетам. Второй протокол - протокол IP, ответственный за передачу этих пакетов от одной машины к другой машине. Иными словами, он ответственен за корректную адресацию пакетов в Сети.

В модели TCP/IP существует несколько уровней, а именно 4. И сейчас мы рассмотрим последовательно все четыре уровня модели TCP/IP. На самом верхнем уровне, прикладном работают пользовательские программы, и задача прикладного уровня - обеспечить доступ для этих пользовательских программ к услугам

Интернет. Мы с вами пользуемся достаточно большим спектром программ в интернете, и каждая программа использует свой протокол. Например, браузеры и веб-страницы используют протокол HTTP или его современную версию HTTPS. Ни для кого не секрет, что URL странички начинается с HTTP или HTTPS. S означает, что мы общаемся с веб-страницей по зашифрованному каналу. И более подробно мы рассмотрим протокол HTTPS в следующей лекции. Вообще, протокол HTTP(S) является примером протокола прикладного уровня, по которому передаются веб-страницы. Кроме того, мы с вами можем скачивать или загружать какие-то файлы: для этого часто используется протокол FTP. Кроме того, мы с вами пользуемся почтой, и для доставки и отправки имейлов существуют другие протоколы - протокол SMTP или протокол POP3. И в зависимости от того, что мы делаем интернете, работает тот или иной протокол прикладного уровня. Вообще, cookies переводится с английского как печенье, хотя в терминологии веб-браузинга cookie никак не переводится, термин так и остаётся куки или cookie(s). Так вот, куки - это данные, которые передаются от сервера клиенту для его идентификации. Мы далее с вами разберём, что мы понимаем под идентификацией. Вообще, cookie есть полезные, они позволяют нам комфортно проводить некоторые вещи в сети. Так, например, они сохраняют сессионную информацию. Примером является тот факт, что, когда вы, например, заходите на какой-то интернет-магазин, наполняете корзину каким-то покупками, но не завершайте покупку, а закрываете эту страницу, а потом открываете её когда-нибудь снова, часто получается так, что содержимое корзины запоминается. Интернет-магазин запомнил те товары, которые вы выбрали в прошлый раз, и не удалил их. Сохранил и запомнил он эту информацию как раз с помощью этих куки, которые позволили ему идентифицировать вас (ваш браузер) как человека, который хотел купить какие-то конкретные вещи. Кроме этого, куки позволяют персонализировать страницы: например, смена языка страницы, или когда браузер спрашивает, нужно ли перевести эту страницу на русский язык. А если вы попадаете на страницу с финским языком, и вы не часто или почти никогда

не смотрите страницы на финском языке, то вас спрашивают, стоит изменить язык на какой-то другой. В этой лекции мы с вами посмотрим, как работает браузер Tor и какие механизмы существуют для анонимизации пользователя в сети. Что такое Tor? Tor - это аббревиатура от the onion router или луковая маршрутизация. То есть Tor - это сеть, которая использует так называемую луковую маршрутизацию. Вообще, Tor - это еще название проекта, который предоставляет бесплатный браузер, работающий как раз вот по этой модели луковой маршрутизации. Основные задачи, которые преследуют разработчики этого браузера – это, во-первых, анонимность пользователя, и во-вторых, конфиденциальность информации, которая передается по сети с помощью браузера Tor. Вообще, WiFi - это технология беспроводной локальной сети, она основана на стандарте IEEE 802.11. IEEE – это организация, которая описывает вообще любые стандарты того, как работает интернет. В частности, она описывает, как должен работать беспроводной интернет, и номер этого стандарта 802.11, и все последующие модификации (этот стандарт модифицируется с течением времени) носят название 802.11 и далее какие-то буквы.

# 4 Выполнение лабораторной работы

Прикладной уровень • доступ для пользовательских программ к службам Интрнета Примеры: HTTP(S), FTP, SSH (рис. 4.1).

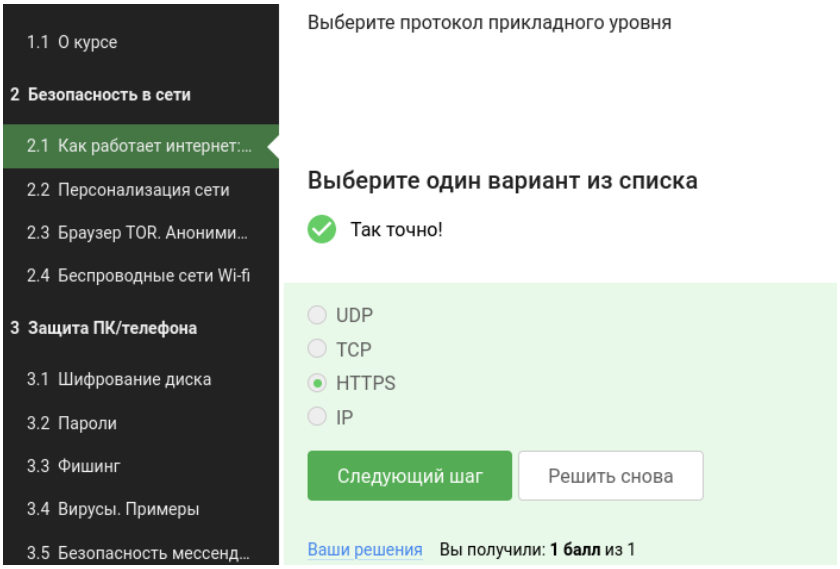


Рис. 4.1: Тест 1

Транспортный уровень • надежная передча данных между процессами в машине (хосте) • адрессация (для какого процесса пришел пакет) Примеры: TCP, UDP (рис. 4.2).

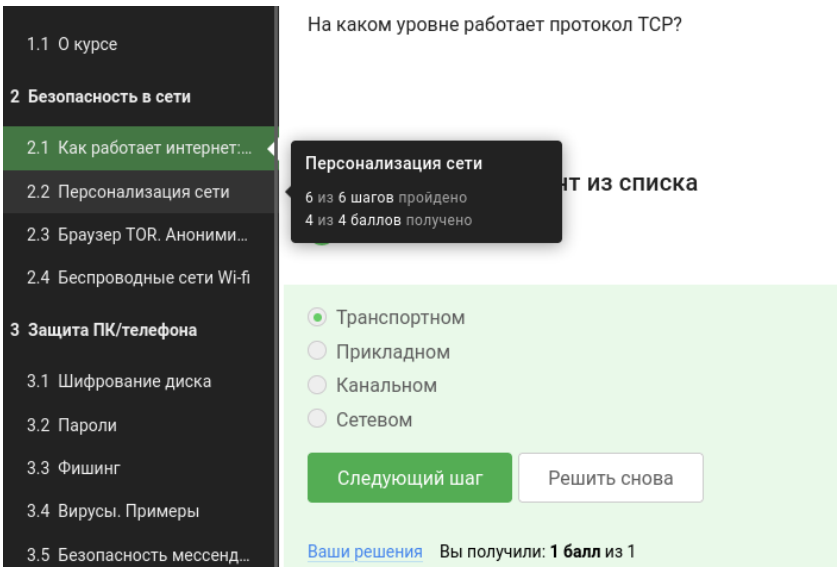


Рис. 4.2: Тест 2

Адрес IPv4 — набор из 4х чисел от 0 до 255, разделенные точкой (рис. 4.3).

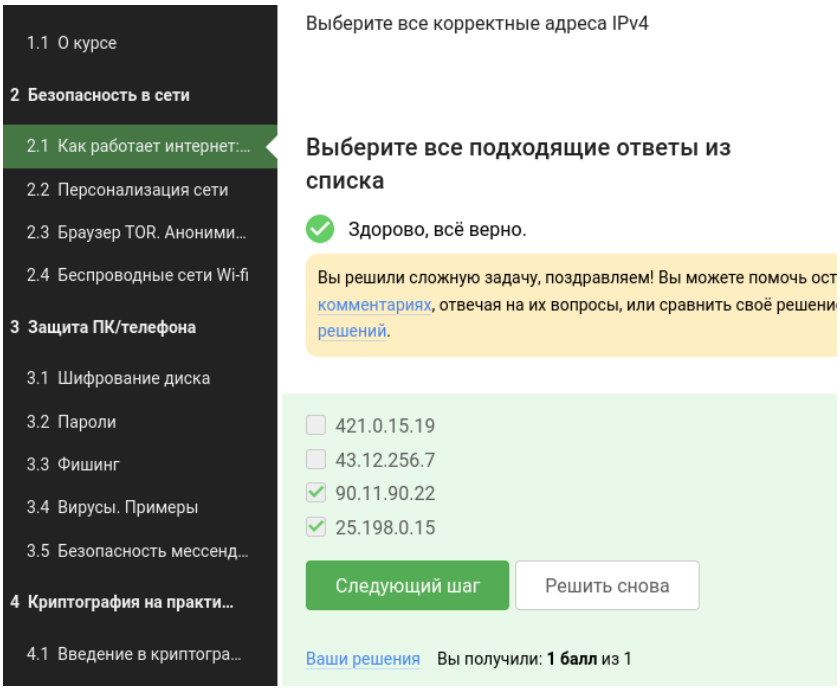


Рис. 4.3: Тест 3

DNS (Domain Name Server) — сервер доменных имён (рис. 4.4).

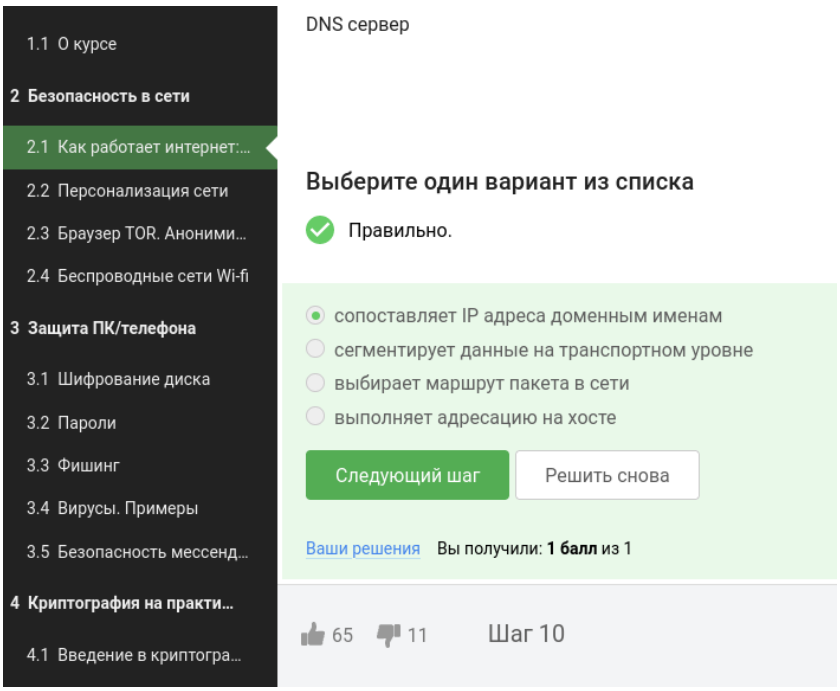


Рис. 4.4: Тест 4

(рис. 4.5).

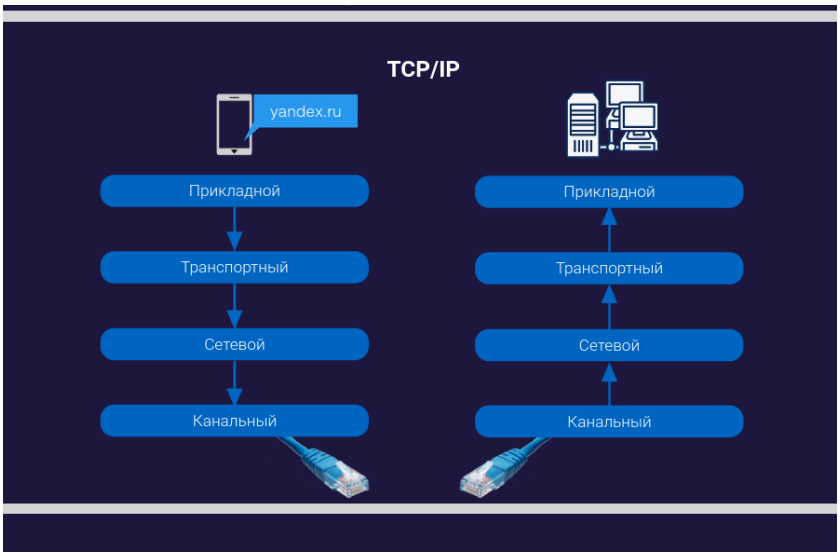


Рис. 4.5: Пояснение ответа

(рис. 4.6).

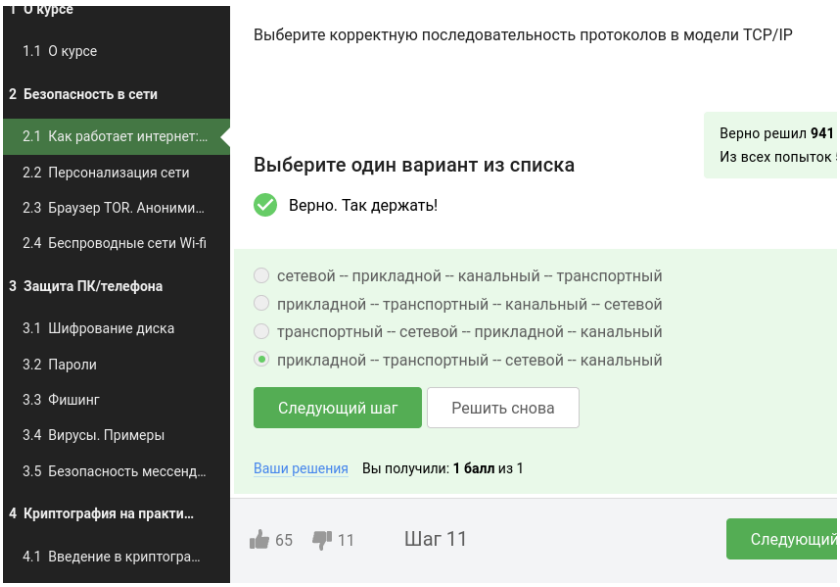


Рис. 4.6: Тест 5

Протокол http считается не надежным (рис. 4.7).

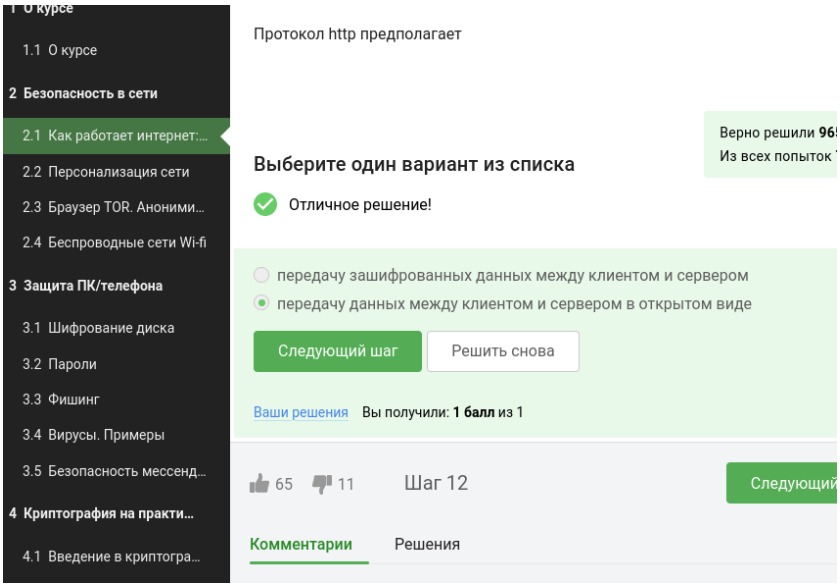


Рис. 4.7: Тест 6

Протокол https считается надежным, потому что данные шифруются (рис. 4.8).

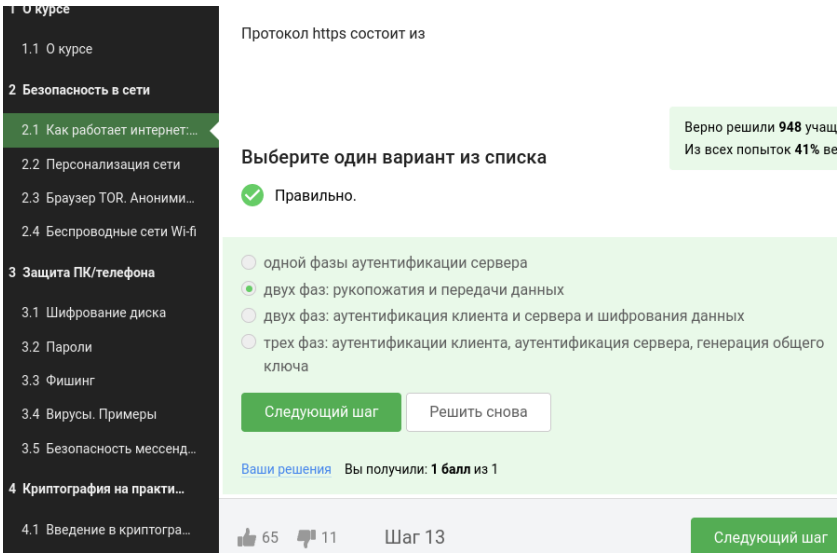


Рис. 4.8: Тест 7

TCP = Transmission Control Protocol (протокол управления передачей), он управляет передачей и зависит и от сервера и от клиента (рис. 4.9).

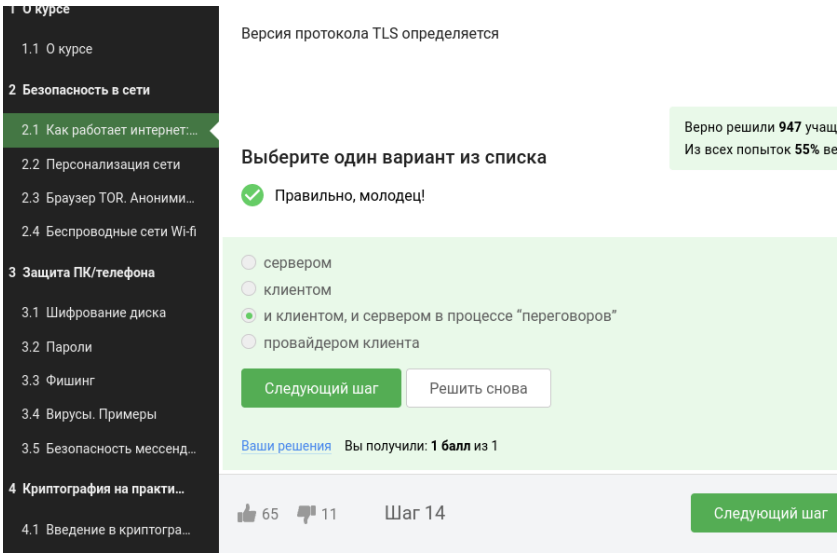


Рис. 4.9: Тест 8

TLS-рукопожатие — это процесс, который запускает сеанс связи, использующий TLS (рис. 4.10).

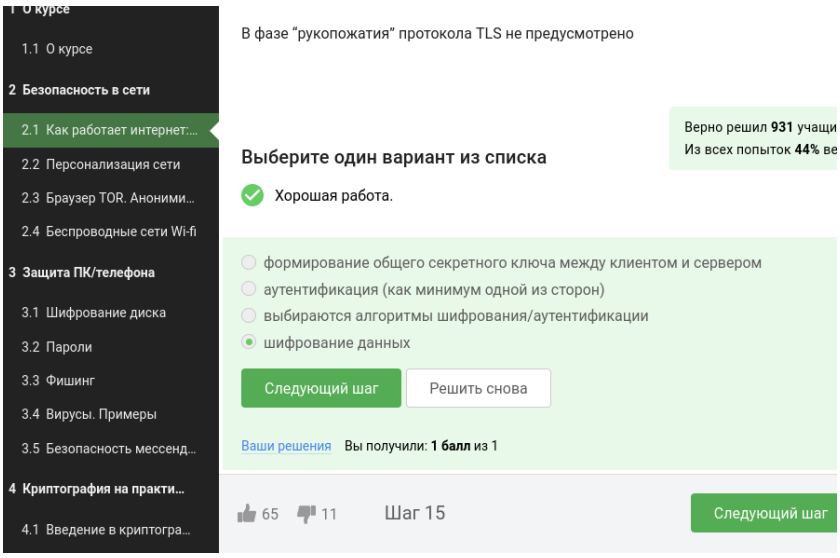


Рис. 4.10: Тест 9

Куки, как правило, хранят в себе список параметров и их значений. Этими параметрами могут быть id пользователя, id сессии, иногда описан тип браузера и время запросов и некоторые действия пользователей. Опять же, если это интернет-магазин, то в куки может храниться то, что мы просматривали, какие страницы мы посещали (рис. 4.11).

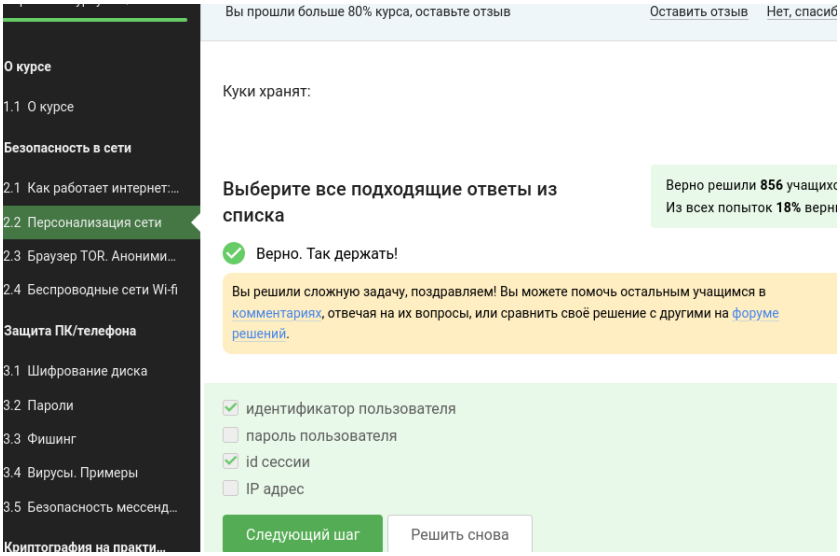


Рис. 4.11: Тест 10

(рис. 4.12).

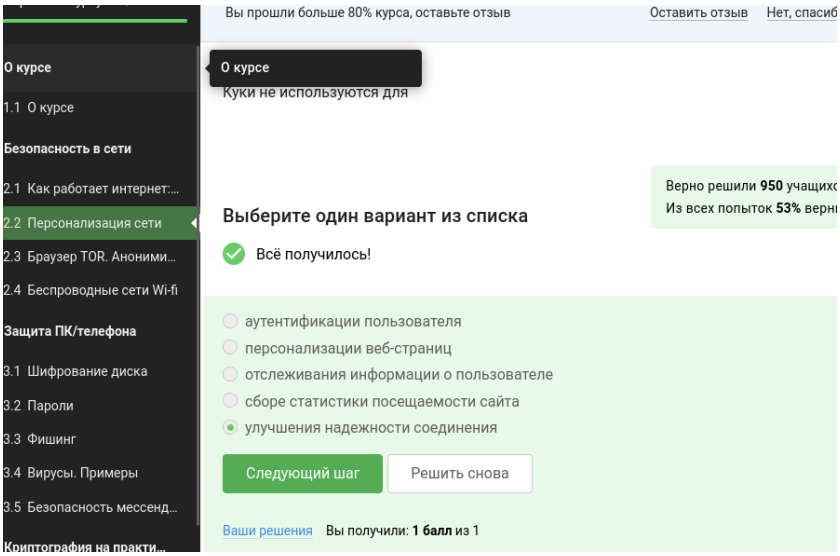


Рис. 4.12: Тест 11

куки - это данные, которые передаются от сервера клиенту для его идентификации (рис. 4.13).

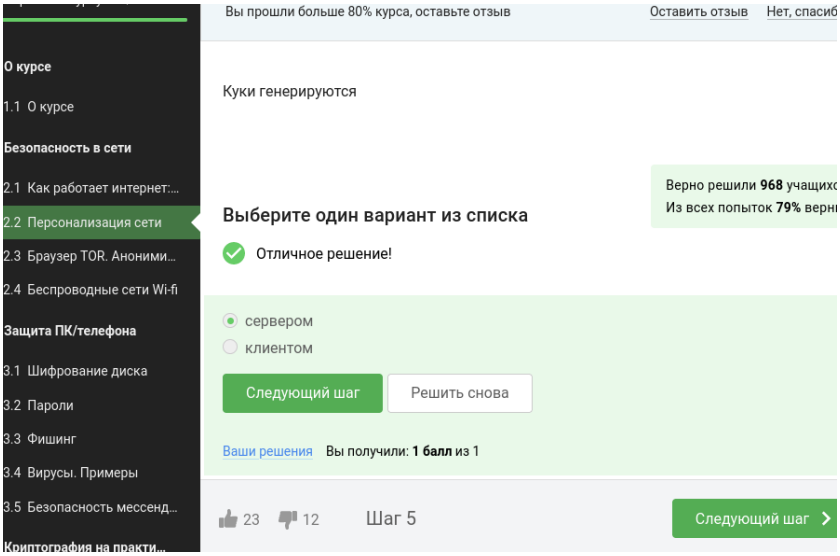


Рис. 4.13: Тест 12

Откуда, например, известно, сколько раз вы посетили какой-то сайт - это записывается в куках. Хотя они и называются постоянными, как правило, у всех кук

есть срок жизни, и он также записан в ещё одном значении в куках.

Мы как пользователи не управляем, какой тип куки используется на конкретном сайте, этим занимается разработчик (рис. 4.14).

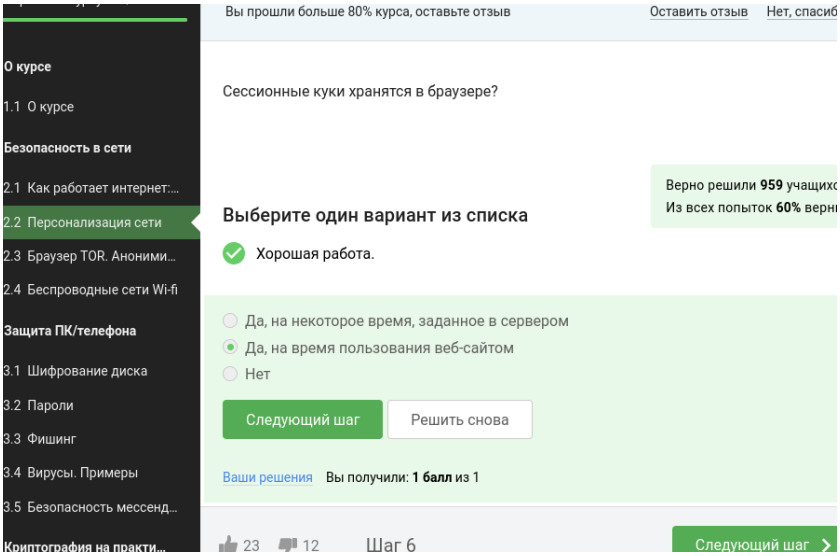


Рис. 4.14: Тест 13

В браузере Tor всегда есть три роутера, их не больше и не меньше (рис. 4.15).

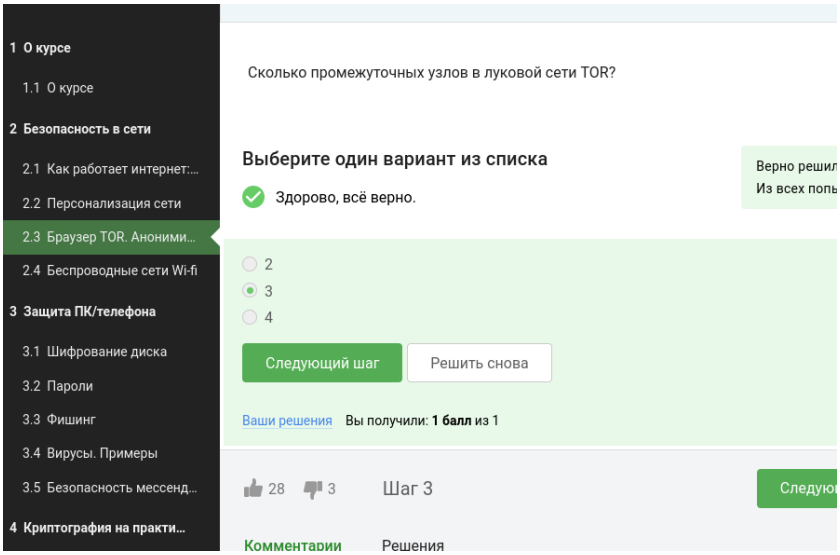


Рис. 4.15: Тест 14

Посмотрим теперь, за счет чего достигается конфиденциальность. Допустим, у

нас с вами есть отправитель, мы обозначим его буквой S, и три узла: охранный A, промежуточный B и выходной C. Первым делом алгоритм выбирает выходной узел C, затем два других узла. Это выбирает встроенный алгоритм в вашем браузере, который знает, кому в итоге пакет должен прийти и какие узлы могут доставить ваш пакет тому, куда он должен прийти. Далее отправитель генерирует общие ключи с помощью определенного криптографического алгоритма, того же самого, который используется в TLS-протоколе. Он генерирует общие ключи последовательно с охранным узлом A, далее с промежуточным узлом B, а потом и с выходным узлом C. Вначале он непосредственно генерирует общий ключ KSA, то есть между отправителем S и охранным узлом A, потом охранный узел помогает сгенерировать общий ключ между S и между B, промежуточным узлом. Он перенаправляет данные, которые идут от отправителя к промежуточному узлу. Таким образом, охранный узел не знает, какой ключ между ними сгенерировался, то есть он не знает KSB. Однако он помогает при передаче публичной информации, с помощью которой два узла могут сгенерировать общий ключ. И то же самое с последним выходным узлом, тут уже и A, и B помогают перенаправлять данные в процессе генерации этого ключа.

В общем, в итоге отправитель сгенерировал общие ключи с тремя промежуточным узлами. Далее он шифрует свои данные под каждым из этих ключей. В начале он шифрует данные для выходного узла, сверху он шифрует зашифрованные уже данные с помощью ключа промежуточного узла, и наконец он шифрует данные с помощью ключа с охранным узлом и отправляет это тройное шифрование в сеть.

Первым этот шифр-текст получает охранный узел, и он его дешифрует под своим ключом, поскольку он может его корректно дешифровать. При дешифровке он понимает, что следующий в сети должен быть узел B, и он отправляет дешифрованные под своим ключом данные в узел B. Узел B видит, что ему пришли какие-то данные, у него есть свой ключ для того, чтобы дешифровать эти данные. Он дешифрует их и видит, что этот пакет должен идти в узел C, и направляет этот

пакет зашифрованный уже только под одним ключом C соответственно в узел C (рис. 4.16).

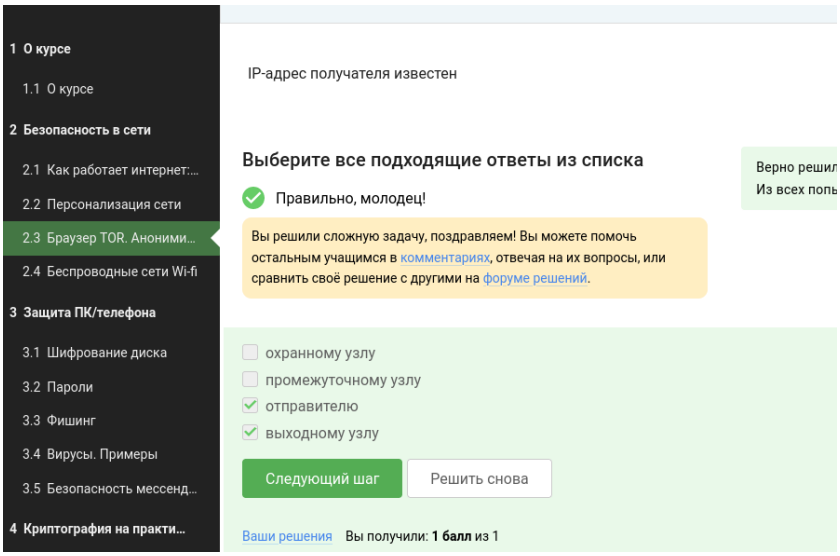


Рис. 4.16: Тест 15

(рис. 4.17).

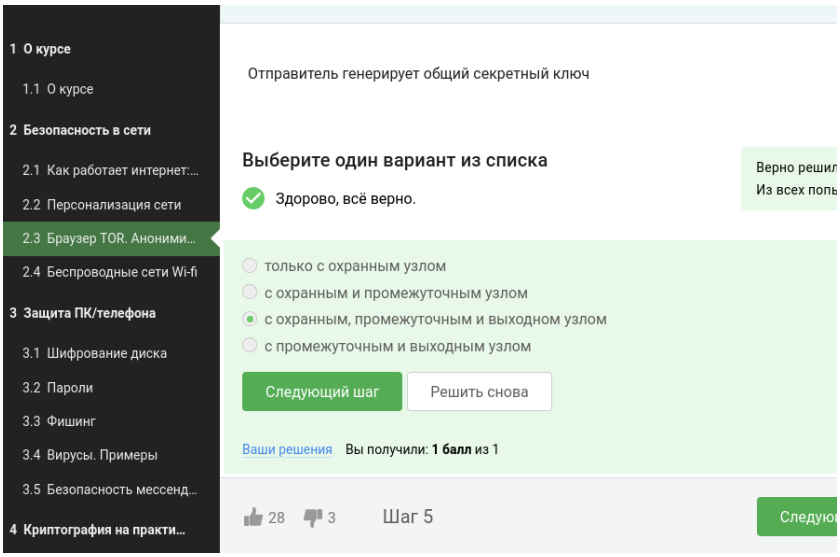


Рис. 4.17: Тест 16

(рис. 4.18).

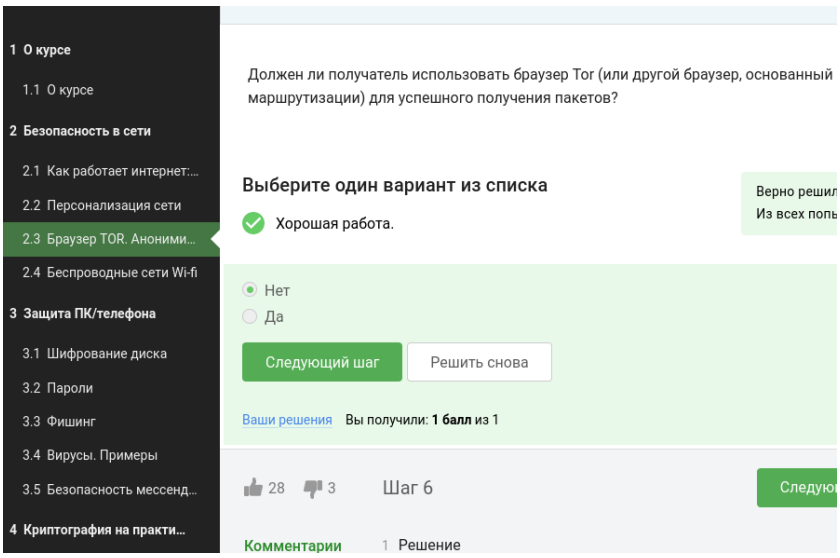


Рис. 4.18: Тест 17

WiFi – это технология беспроводной локальной сети на основе стандартов IEEE 802.11 (рис. 4.19).

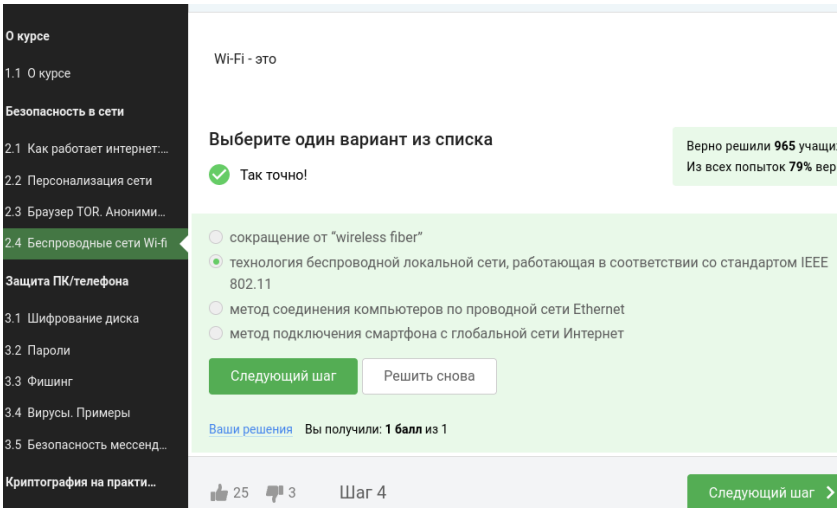


Рис. 4.19: Тест 18

(рис. 4.20).


Рис. 4.20: Пояснение ответа

(рис. 4.21).

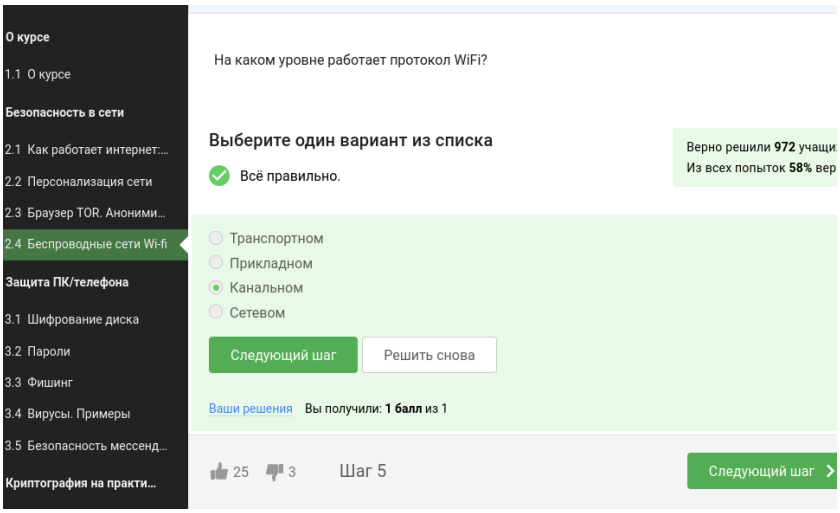


Рис. 4.21: Тест 19

(рис. 4.22).

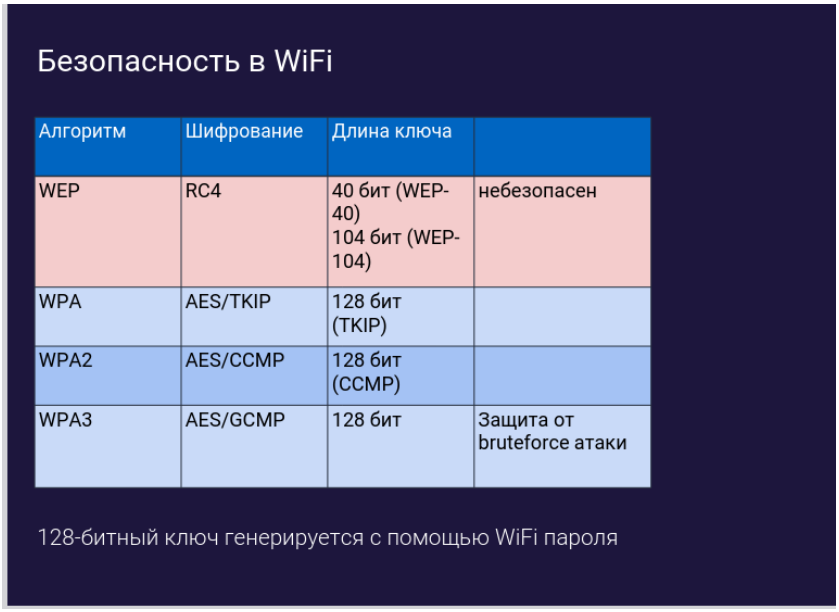


Рис. 4.22: Пояснение ответа

(рис. 4.23).

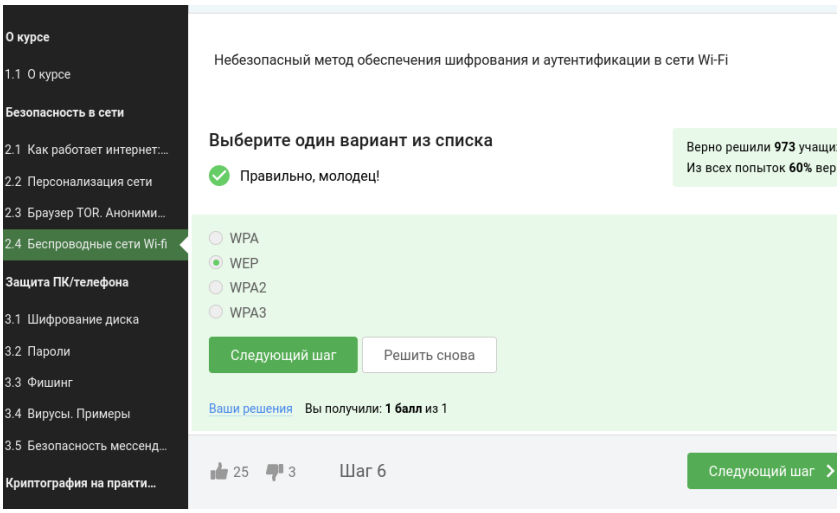


Рис. 4.23: Тест 20

В WPA алгоритмах используется шифрование AES. Это симметричное шифрование. Это означает, что на моем смартфоне или на моем компьютере, а также на роутере есть какой-то общий секретный ключ длиннее 128 бит. Общий сек-

ретный ключ мы генерируем, когда мы подключаемся к WiFi сети с помощью пароля. Так, мы задаем какой-то пароль у себя, дальше происходит генерация общего ключа, с помощью которого на моей стороне (на смартфоне) происходит шифрование данных, а на роутере происходит дешифрование этих же самых данных с помощью того же общего ключа. Кроме того, что мы шифрует данные, мы также хотим, чтобы они были аутентифицированы, то есть чтобы не было возможности у стороннего человека подключиться к нашей сети WiFi (рис. 4.24).

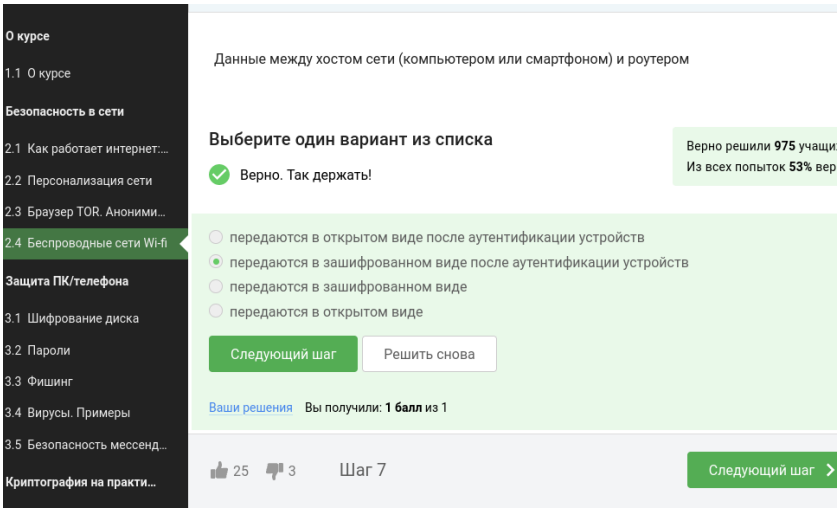


Рис. 4.24: Тест 21

WPA2 Personal: аутентификация по паролю (используется в домашних сетях) (рис. 4.25).

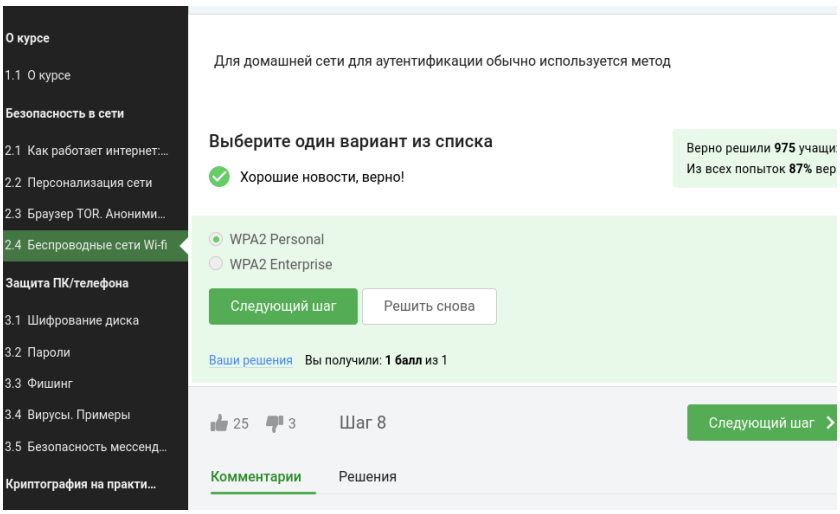


Рис. 4.25: Тест 22

# 5 Выводы

Мы поняли, что происходит при открытии ссылки в браузере, как работает персонализация сети, Браузер TOR, анонимизация и беспроводные сети Wi-fi.