Прохождение внешнего курса 1 часть

Безопасность в сети

Павлов Арсений НБИбд-03-22

Содержание

Список иллюстраций

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).

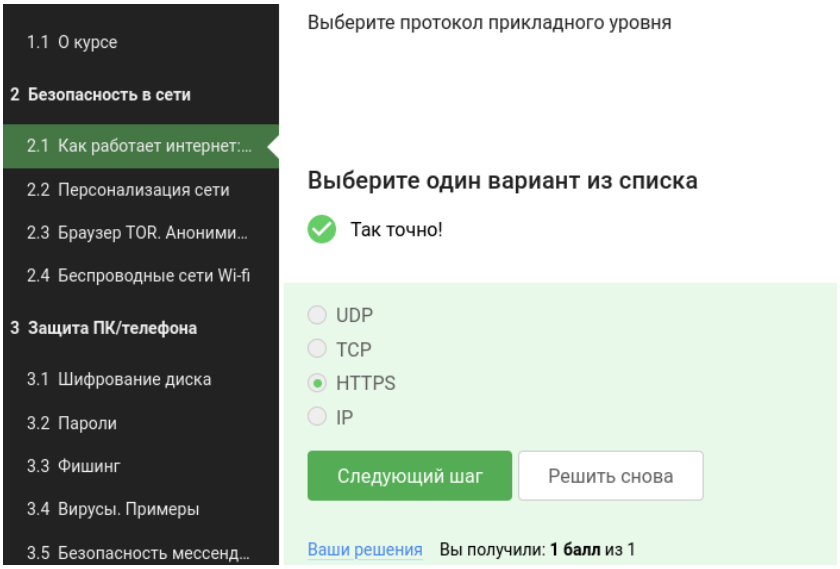


Рис. 4.1: Тест 1

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

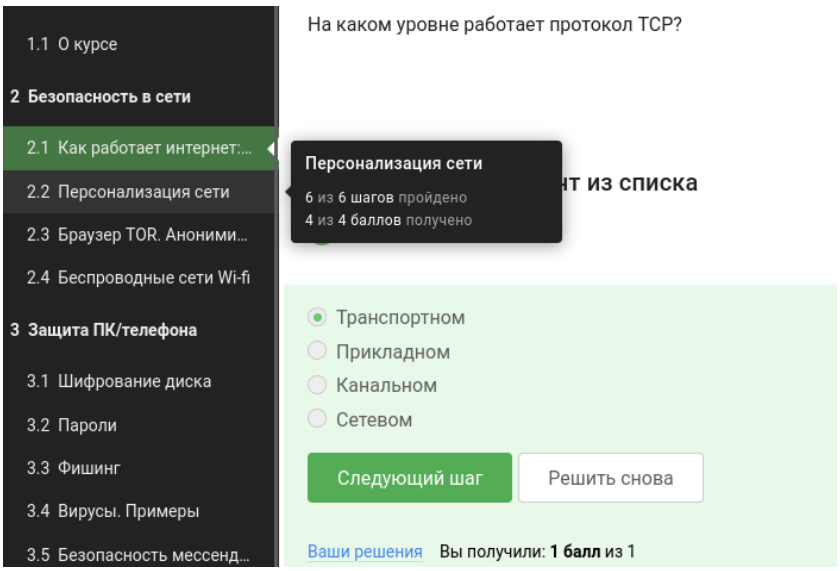


Рис. 4.2: Тест 2

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

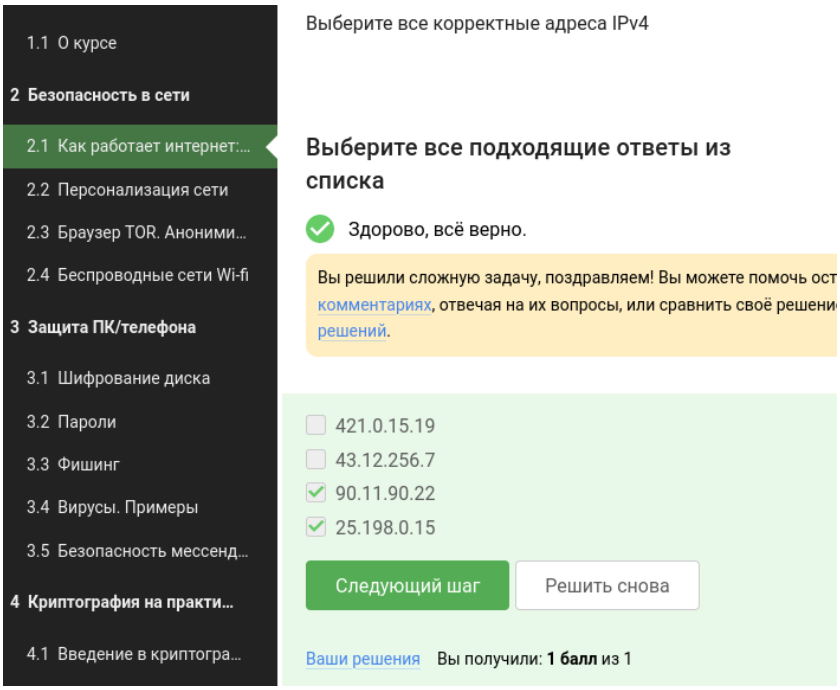


Рис. 4.3: Тест 3

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

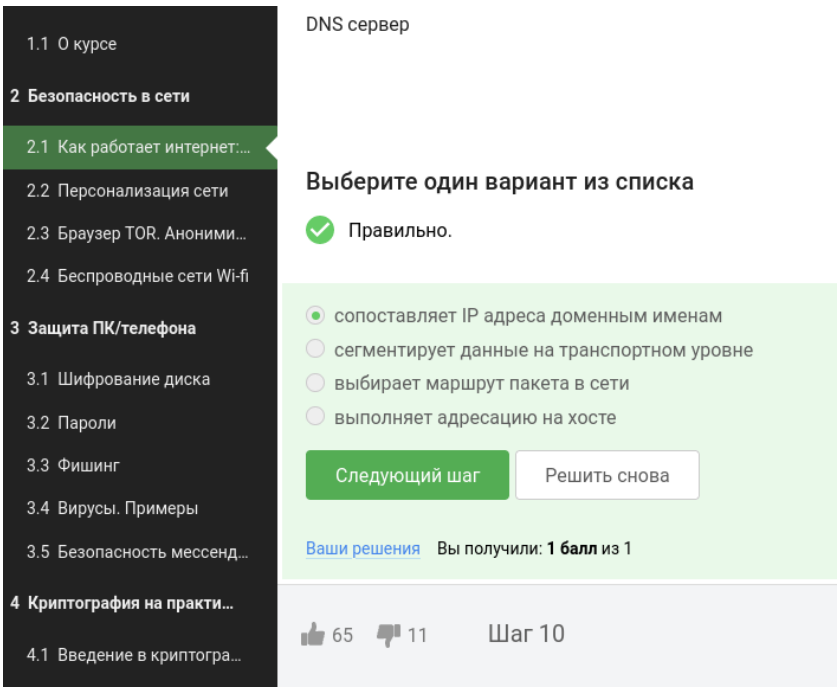


Рис. 4.4: Тест 4

(рис. 4.5).

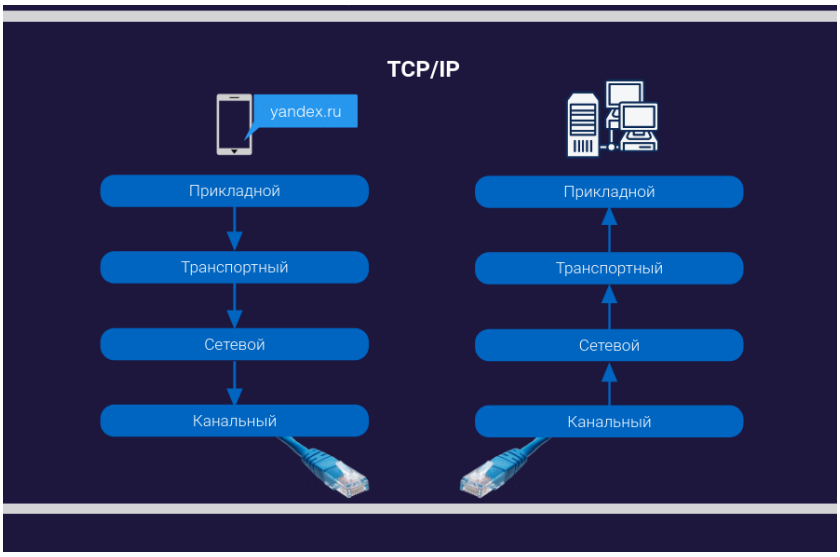


Рис. 4.5: Пояснение ответа

(рис. 4.6).

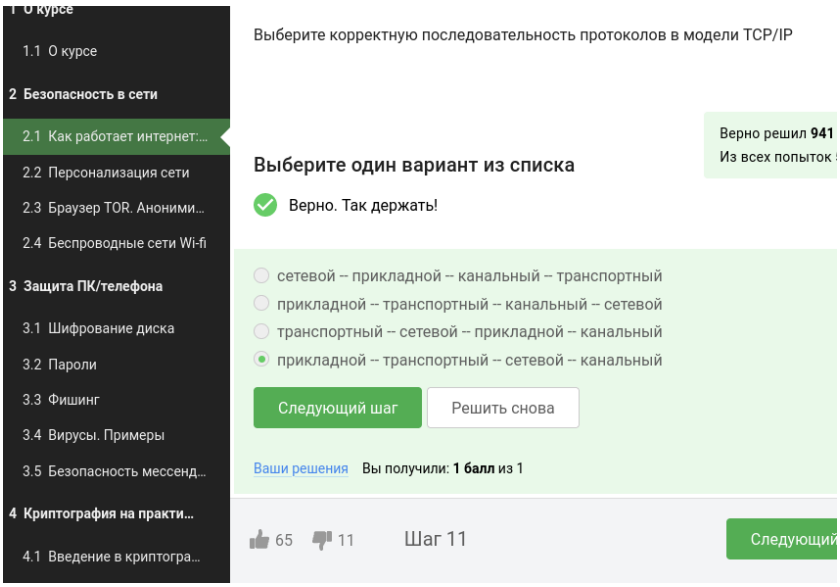


Рис. 4.6: Тест 5

Протокол http считается не надежным (рис. 4.7).

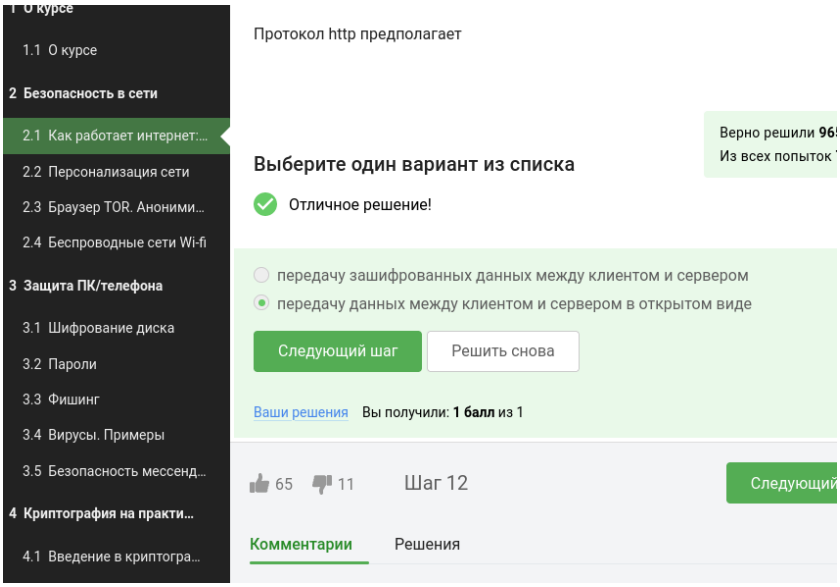


Рис. 4.7: Тест 6

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

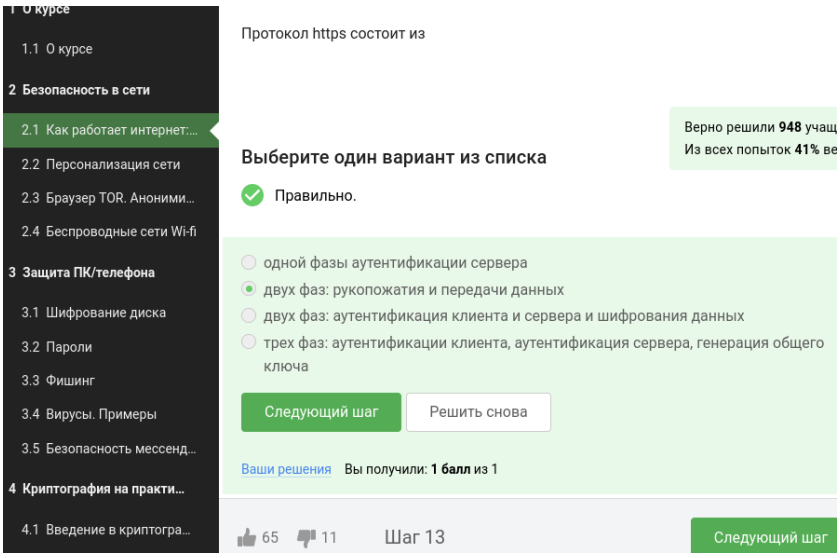


Рис. 4.8: Тест 7

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

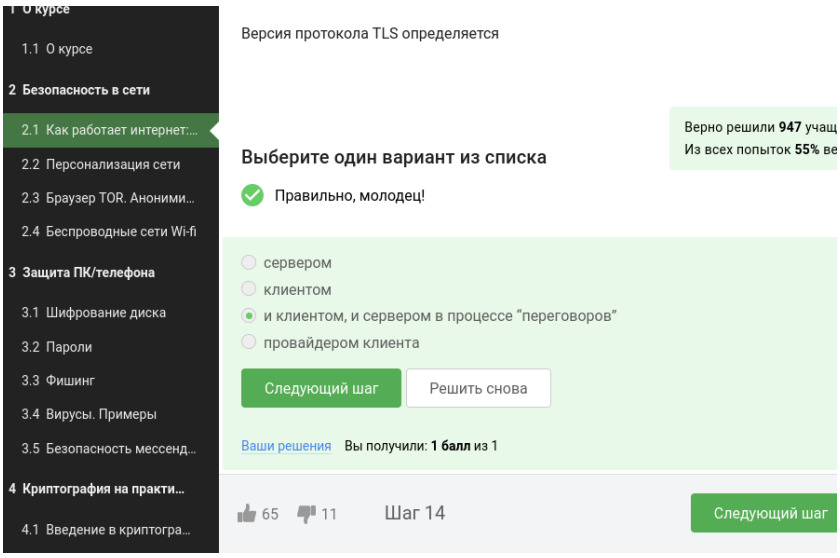


Рис. 4.9: Тест 8

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

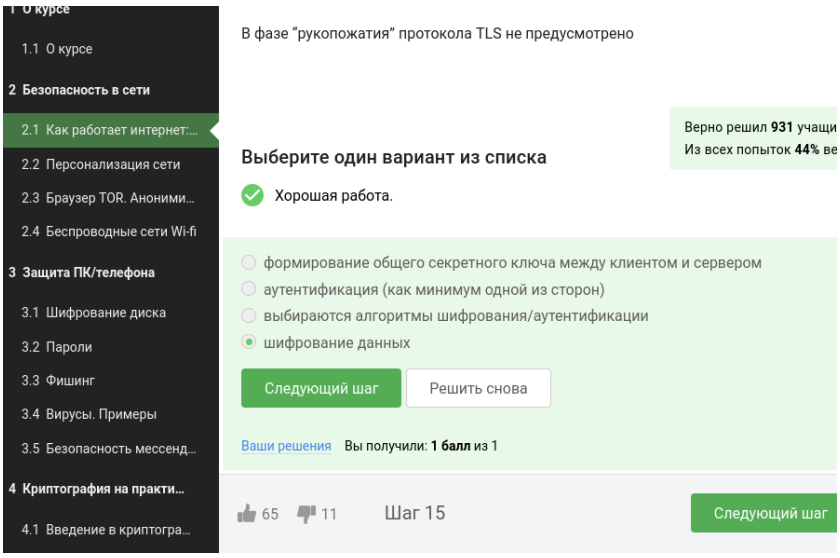


Рис. 4.10: Тест 9

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).

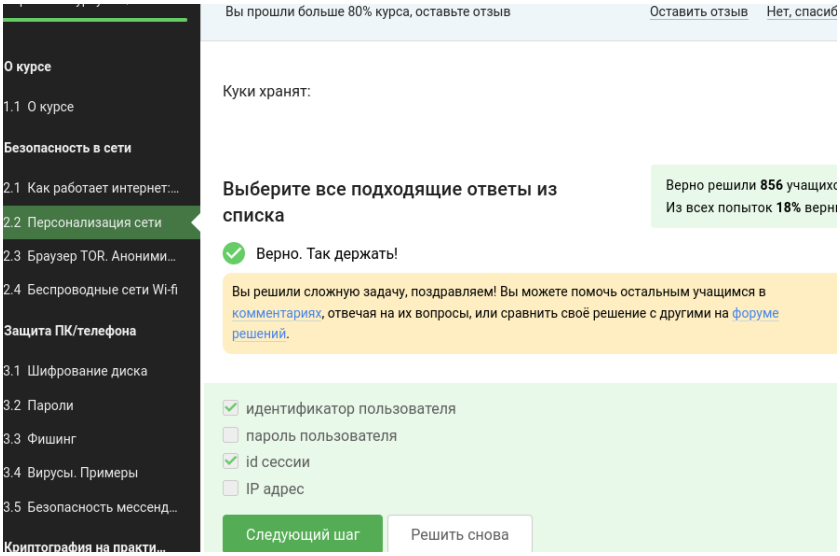


Рис. 4.11: Тест 10

(рис. 4.12).

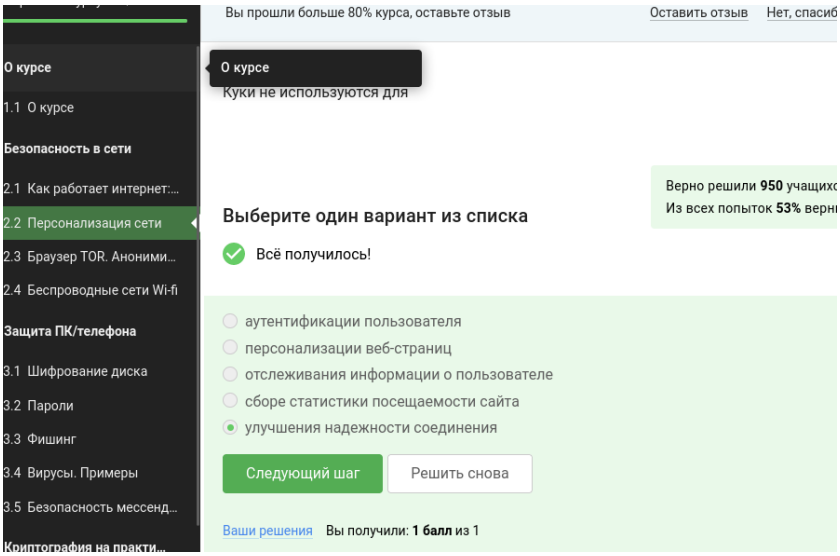


Рис. 4.12: Тест 11

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

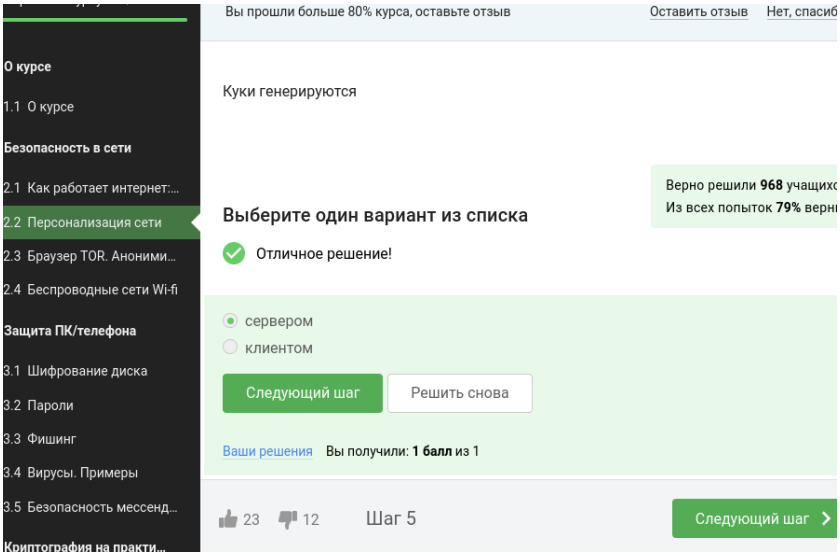


Рис. 4.13: Тест 12

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).

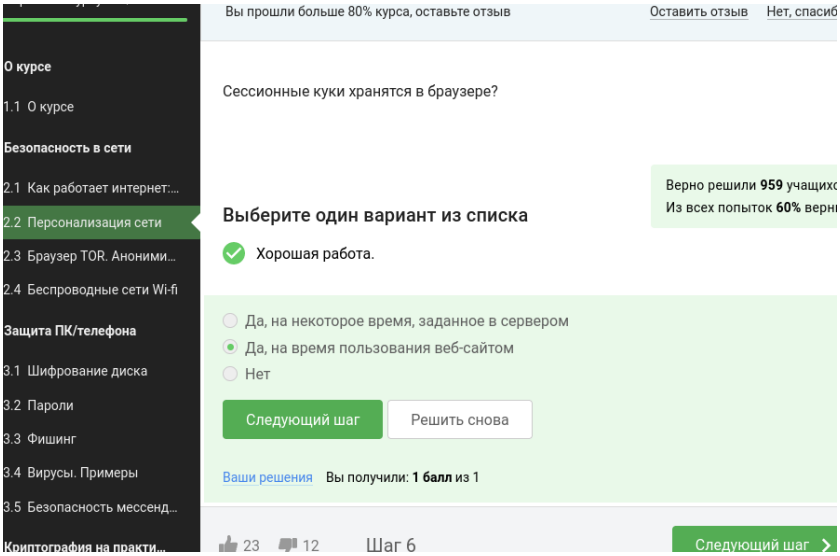


Рис. 4.14: Тест 13

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

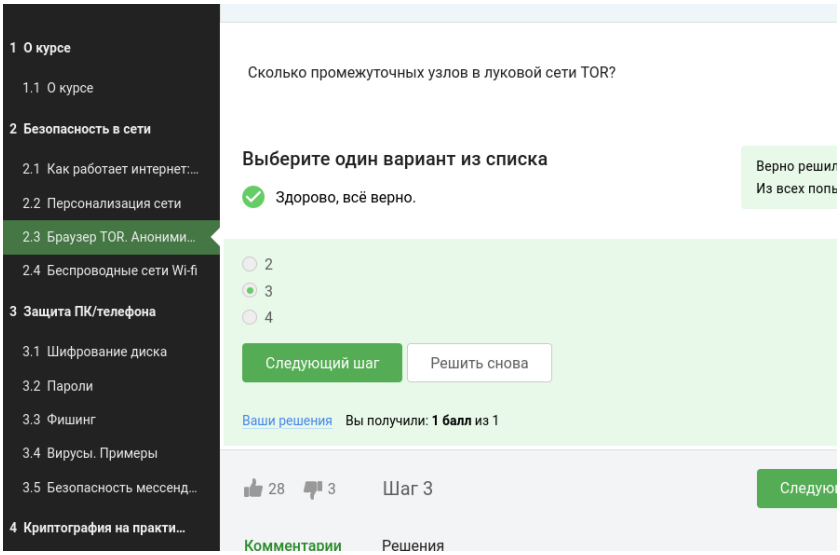


Рис. 4.15: Тест 14

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).

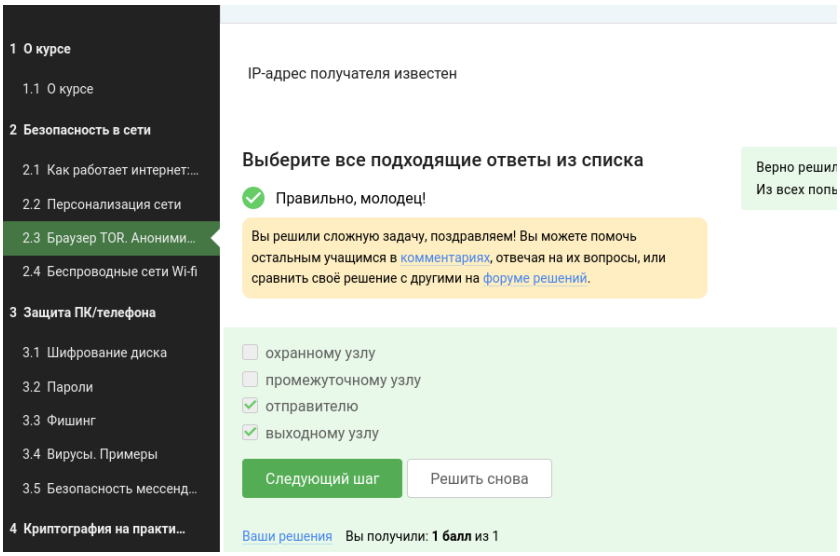


Рис. 4.16: Тест 15

(рис. 4.17).

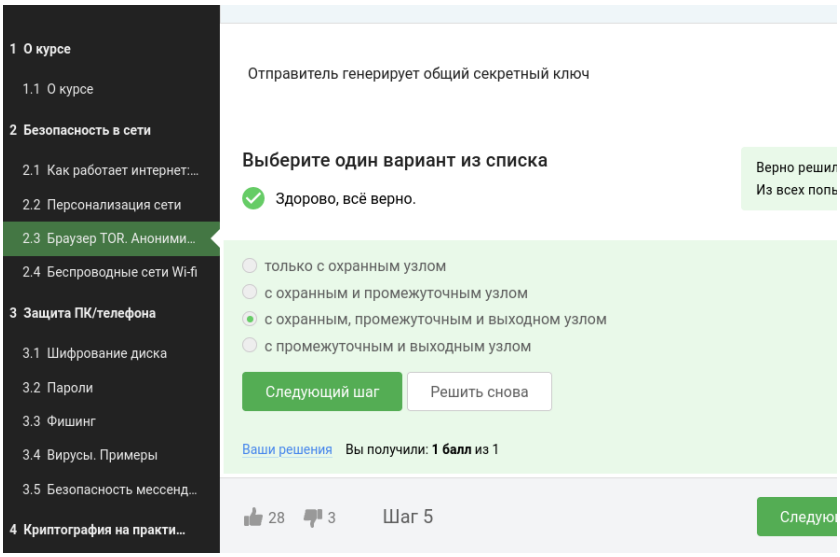


Рис. 4.17: Тест 16

(рис. 4.18).

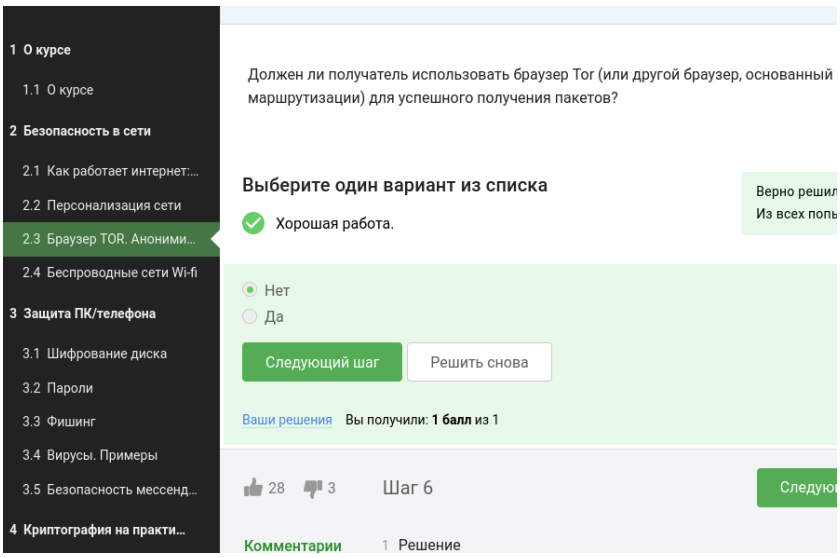


Рис. 4.18: Тест 17

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

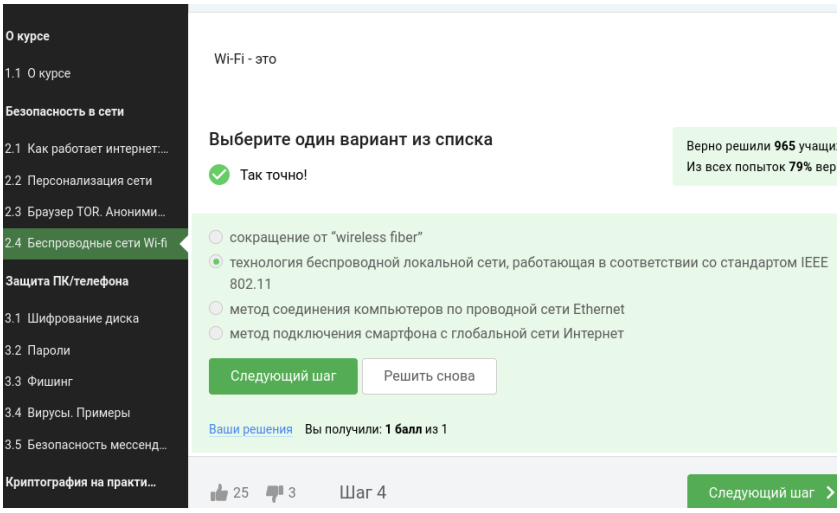


Рис. 4.19: Тест 18

(рис. 4.20).

Рис. 4.20: Пояснение ответа

(рис. 4.21).

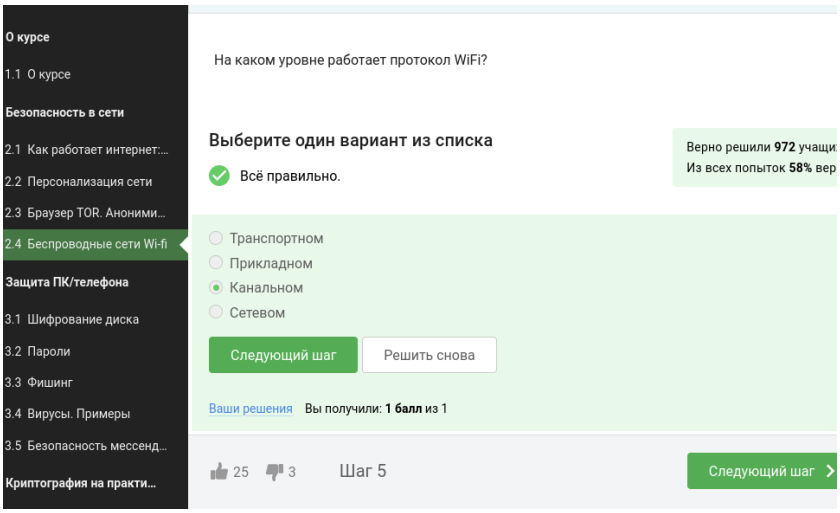


Рис. 4.21: Тест 19

(рис. 4.22).

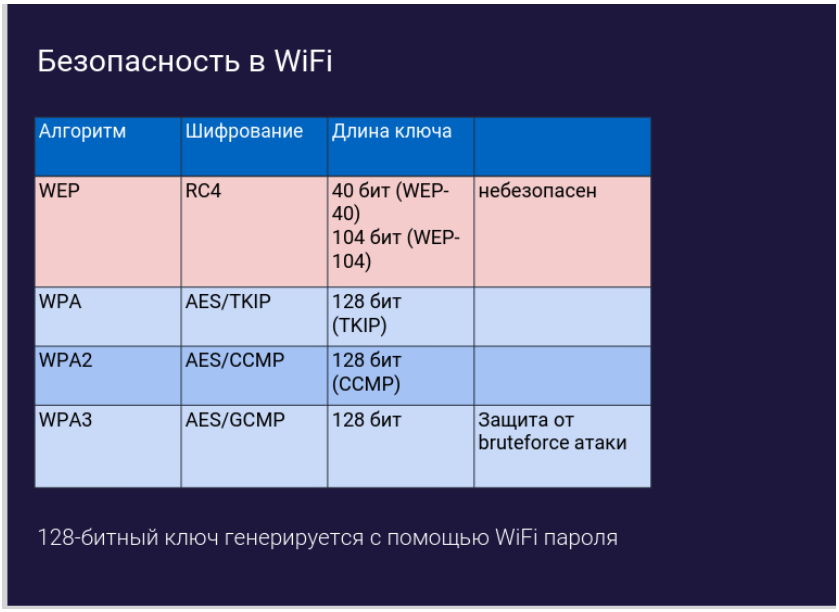


Рис. 4.22: Пояснение ответа

(рис. 4.23).

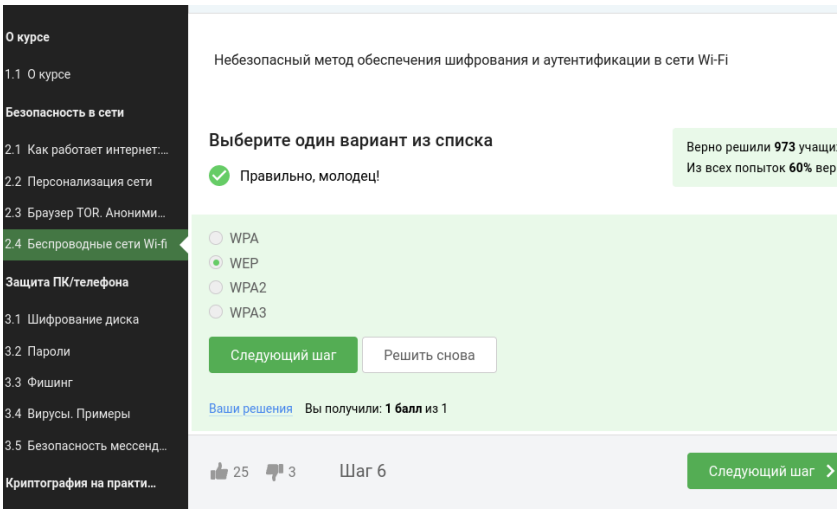


Рис. 4.23: Тест 20

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).

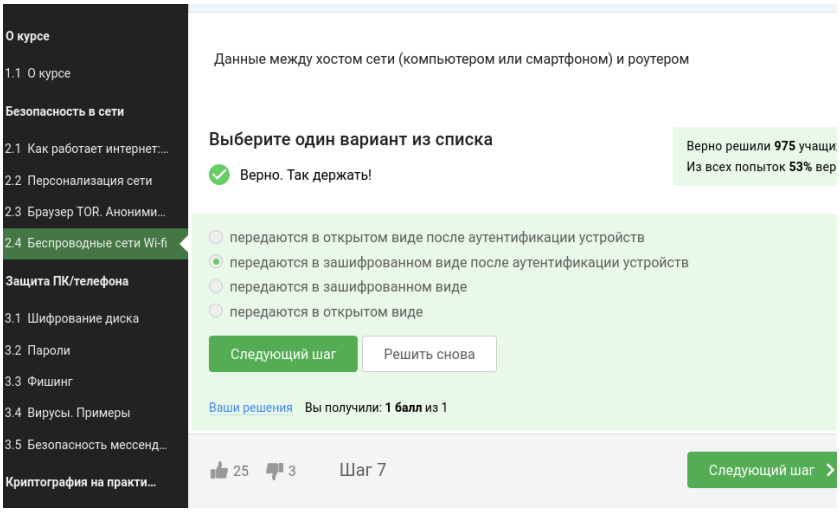


Рис. 4.24: Тест 21

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

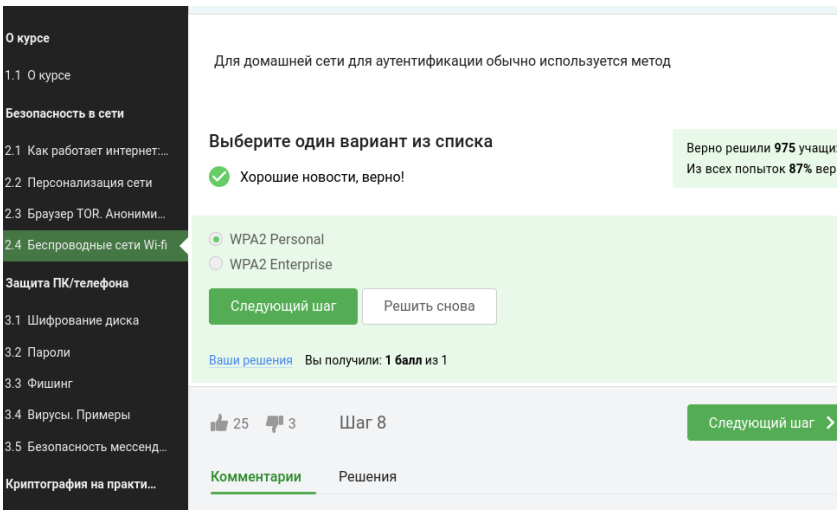


Рис. 4.25: Тест 22

5 Выводы

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

Прохождение внешнего курса 2 часть

Защита ПК/телефона

Павлов Арсений НБИбд-03-22

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Научиться Шифровать диск. Выбрать правильный пароль. Понять, что такое фишинг и вирусы и как обезопасить свои менеджеры.

2 Задание

Выполнить тестовую часть курса

3 Теоретическое введение

Поговорим немного о деталях, о том, как происходит шифрование. Шифрование больших объемов данных, например, жесткого диска или сегмента жесткого диска или какой-то большой флешки, осуществляется с помощью симметричного шифрования, как правило, алгоритма AES. Это американский стандарт симметричного шифрования, он также используется для конфиденциальной передачи данных по сети. Это эффективный алгоритм, который реализован в процессорах быстро, то есть на аппаратном уровне. Благодаря тому, что это хороший алгоритм, пользователь практически не наблюдает задержек в работе, то есть данные шифруются-дешифруются быстро. Как правило, это происходит на заднем фоне, мы можем при этом работать на компьютере, будут происходить какие-то параллельные операции на шифрование и дешифрование. Мы используем пароли для • аутентификации в сети (логинимся в соц. сети, почту, Skype) • получения доступа к банковским картам (PIN код) • разблокировки телефона • доступа к компьютеру • физического доступа в здания (биометрические пароли) • доступа к электронному кошельку (парольные фразы в bitcoin) Фишинг — заполучение информации у пользователя, маскируясь под реальный сервис/продукт • поддельные интернет- страницы • телефонные звонки (от якобы банков) Mydoom почтовый червь для Microsoft Windows и Windows NT, 2004 год Червь — вредоносное ПО, распространяющееся по сети Инетнет Распространялся по почте как письмо с пометкой “Mail Delivery System” Письмо содержало вложение, открытие которого запускало червя. Червь выискивал имейл адреса во всех локальных файлах и отправлял им письмо Ущерб оценивается в $38 биллионов

Sobig почтовый червь и троян под Microsoft Windows 2003 год Троян — вирус, проникающий в систему под видом легитимного ПО Распространялся по почте как письмо с темой “Re: Details” (или подобными) Само письмо содержало текст “See the attached file for details” Вложение устанавливало утилиту WinGate proxy server для рассылки зараженных имейлов Ущерб оценивается в $30 биллионов WannaCry червь и программа-вымогатель денежных средств под Windows 2017 год Программа-вымогатель (ransomware) — вредоносное ПО, блокирующее доступ к данным (часто с помощью шифрования), и вымогающее деньги в обмен на ключ дешифрвания Эксплуатирует уязвимость реализации протокола SMB в Windows (сетевой протокол для удаленного доступа к файлам, принтерам) Ущерб оценивается в $4 биллиона Вирус самостоятельно устанавливается, генерирует ключи шифрования и шифрует некоторые файлы системы Flashback троян под MacOS 2011 год Фейковый установщик Adobe Flash Player Загружался через поддельный веб-сайт Pegasus шпионское ПО под iOS и Android 2021 год Вирус-шпион (spyware) — ПО, нацеленное на сбор приватной информации Разработка израильской компании NSO Group Вирус-троян заражет устройства через заражает через SMS, WhatsApp, iMessage Умеет читать SMS, имейлы, контакты прослушивать звонки, делать скриншоты, записывать нажатия клавиш Для начала давайте обсудим, какие требования мы выдвигаем к безопасности мессенджеров. Во-первых, мы хотим, чтобы наши сообщения доходили корректно, то есть, если мы написали «Я буду через пять минут», мы хотим, чтобы отправитель получил именно это сообщение «Я буду через пять минут», а не «через 15, 20» или «Я не буду через 5 минут». Конечно же, мы хотим, чтобы сообщения были конфиденциальны, то есть само сообщение знал только отправитель и получатель. В идеале мы хотим аутентификацию, то есть, если нам пришло сообщение от какого-то человека, мы знаем, что оно пришло от него, если мы посылаем какому-то человеку сообщение, мы знаем, что оно придет конкретно к нему, и ни к кому другу. Поскольку мы говорим с вами о сообщениях, коммуникация должна быть стойка к потере сообщений. Мы все знаем, что иногда человек бывает не в сети, иногда бывают

проблемы со связью, однако, когда человек заходит в сеть, то все сообщения, которые он не получил за это время, ему должны прийти. И два последних довольно специфичных требования к безопасности, которые мы на сегодня выдвигаем не только к мессенджерам, но и вообще к любой конфиденциальной коммуникации. Первое - это прямая секретность; прямая секретность (от английского forward secrecy) гарантирует безопасность сообщений в прошлом: имеется в виду до компрометации ключа.

4 Выполнение лабораторной работы

. Шифрование больших объемов данных, например, жесткого диска или сегмента жесткого диска или какой-то большой флешки, осуществляется с помощью симметричного шифрования, как правило, алгоритма AES (рис. 4.1).

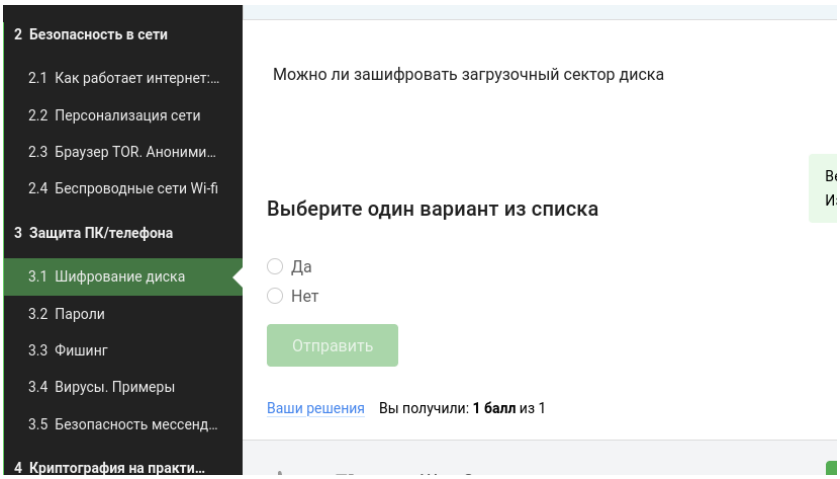


Рис. 4.1: Тест 1

Алгоритм AES это американский стандарт симметричного шифрования, он также используется для конфиденциальной передачи данных по сети. (рис. 4.2).

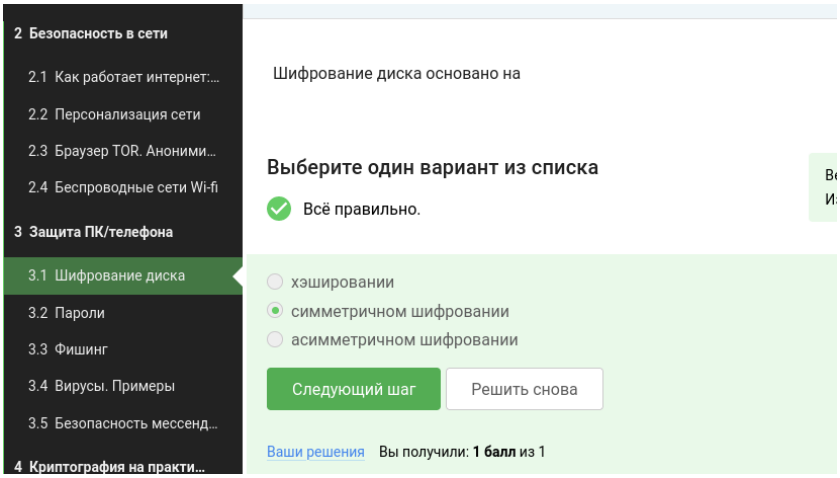


Рис. 4.2: Тест 2

Во всех популярных операционных системах есть встроенные утилиты, которые позволяют шифровать жесткий диск: для Windows это Bitlocker, в Linux – LUKS, в MacOS – это FileVault. Кроме того, есть и сторонние опенсорсные (open source) программы, то есть бесплатные: это Veracrypt, PGPDisk (рис. 4.3).

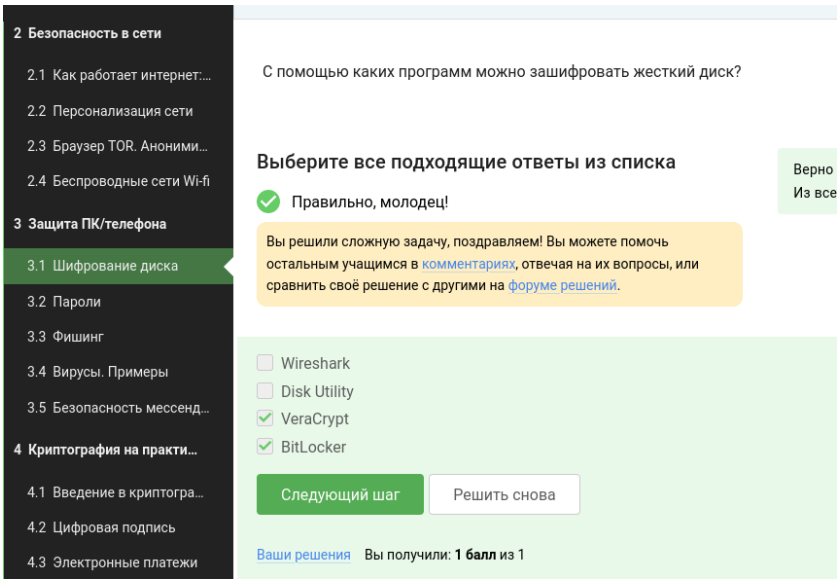


Рис. 4.3: Тест 3

Основной критерий стойкости пароля — это сложность его перебора Пример паролей длины 8, состоящих из цифр, алфавита и спец. символов ![_?]$&+*()

(26+10+13)8 =33 232 930 569 601 перебор практически невыполним (рис. 4.4).

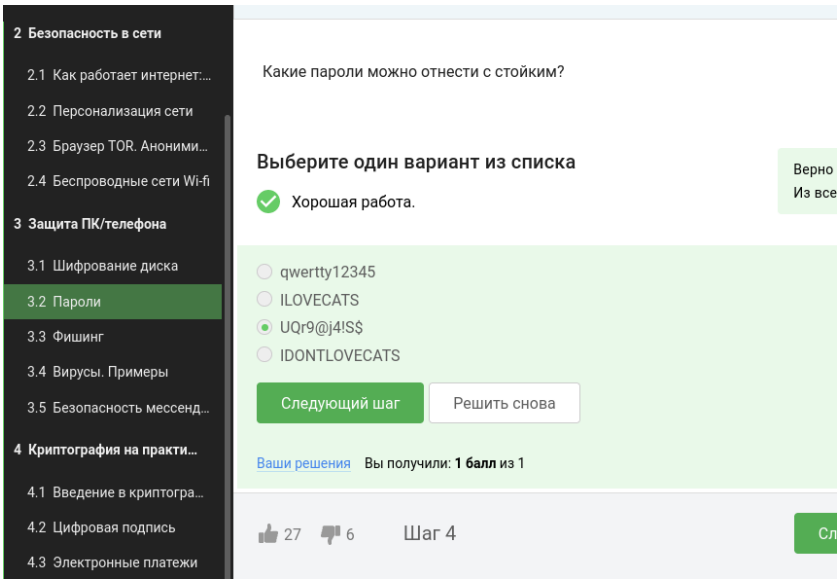


Рис. 4.4: Тест 4

Рекомендации • используйте длинные пароли с символами алфавита разного регистра, цифрами, спец. символами • используйте менеджеры паролей для хранения • регулярно меняйте пароли к критическим сервисам (почте) • используйте разные пароли для разных сайтов, программ (рис. 4.5).

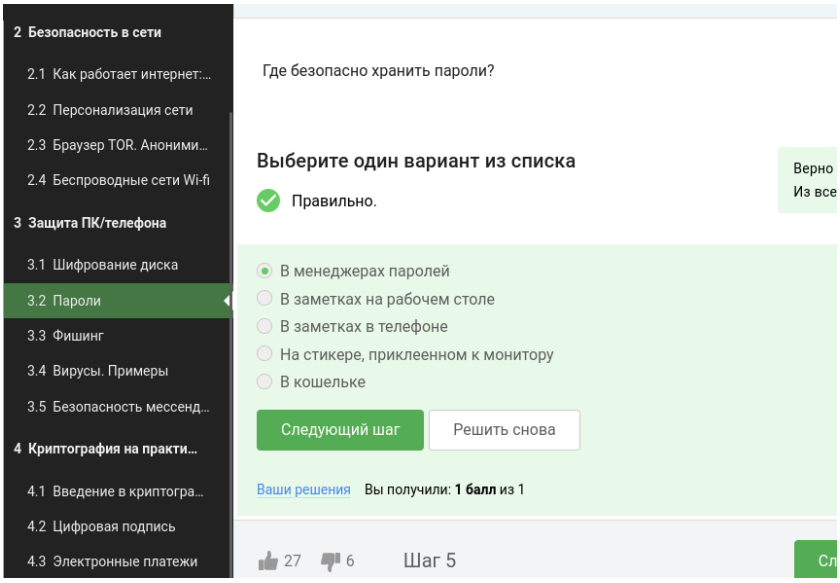


Рис. 4.5: Тест 5

Капча — тест для определения, является ли пользователь человеком или компьютером Цель — противостоять автоматизированному перебору / доступу к ресурсу (рис. 4.6).

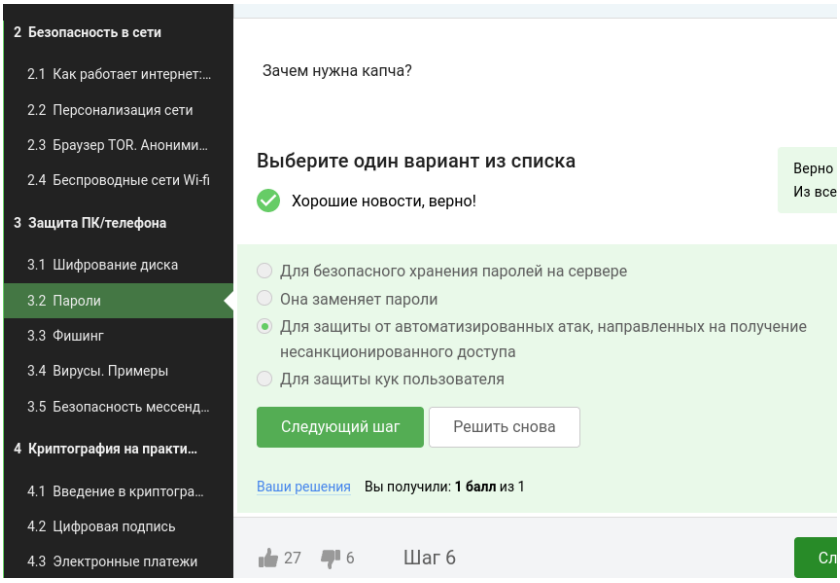


Рис. 4.6: Тест 6

Криптографическая хэш-функция получает на вход произвольные данные и

выдает фиксированное число бит Идея: имея выход хэш-функции (образ) сложно найти вход (прообраз) Примеры: SHA2, SHA3, ГОСТ 34.11-2018 (рис. 4.7).

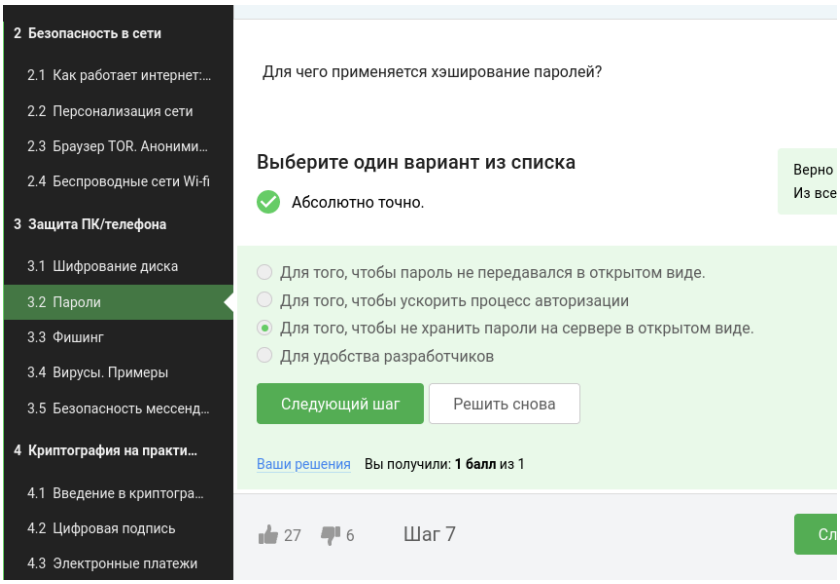


Рис. 4.7: Тест 7

Если злоумышленник получил доступ к серверу соль не поможет (рис. 4.8).

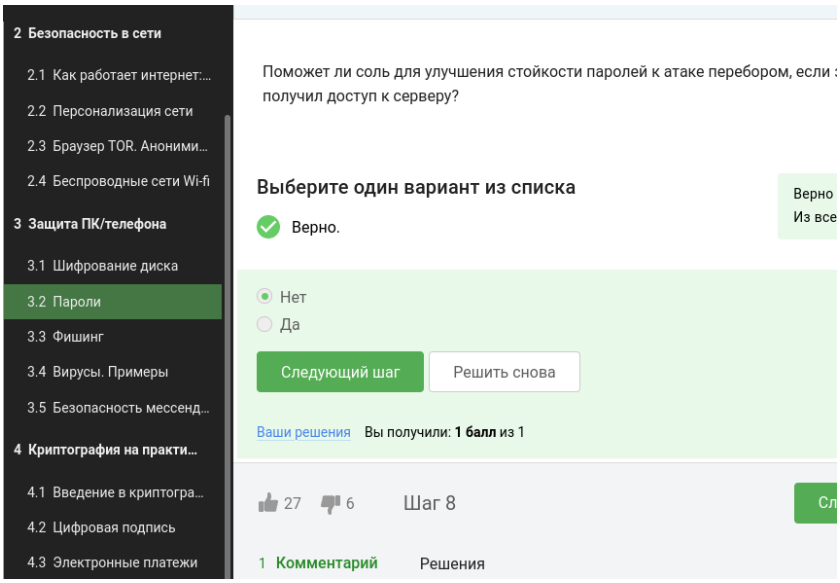


Рис. 4.8: Тест 8

Рекомендации • используйте длинные пароли с символами алфавита разного

регистра, цифрами, спец. символами • используйте менеджеры паролей для хранения • регулярно меняйте пароли к критическим сервисам (почте) • используйте разные пароли для разных сайтов, программ (рис. 4.9).

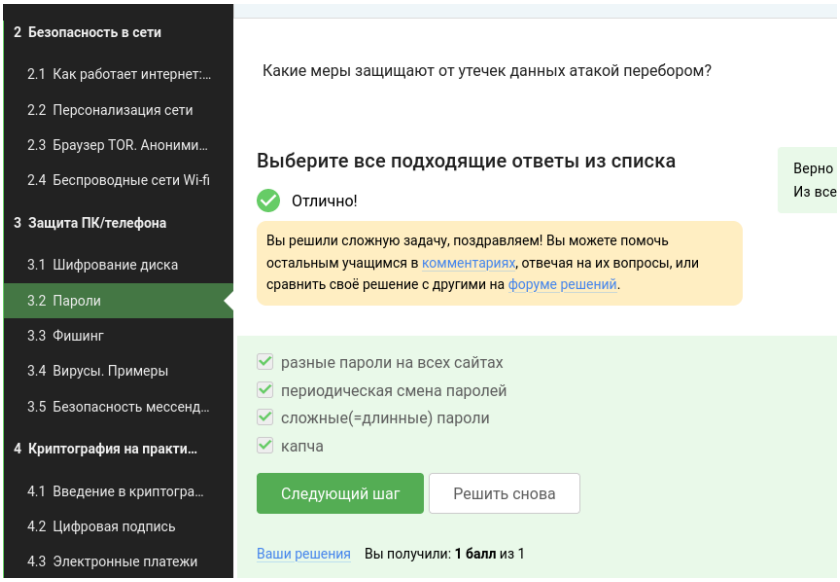
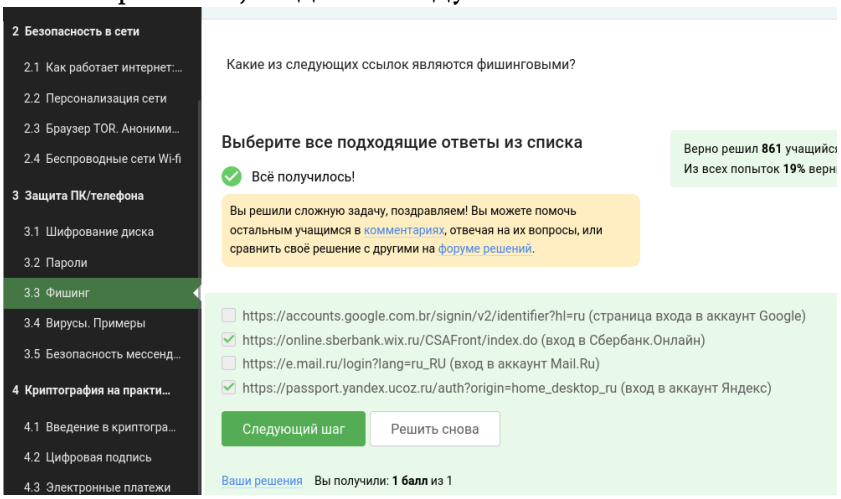


Рис. 4.9: Тест 9

(рис. **??**).

Название может и быть похожа на оригинал, но дальше идут не понятные сим-



волы, которых не должно быть

Чаще всего этим методом и пользуются мошенники (рис. 4.10).

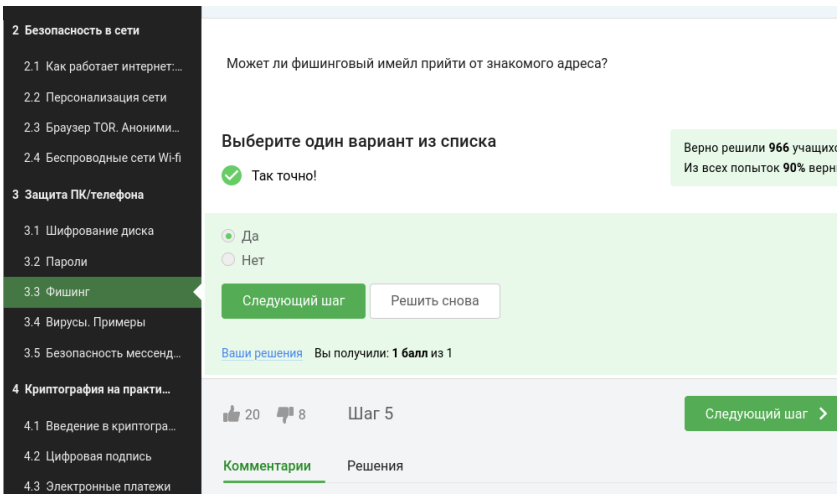


Рис. 4.10: Тест 11

Email спуфинг от англ. spoofing — подмена Суть: отправка писем с поддельным адресом отправителя. Почему работает: протокол для отправки писем SMTP не включает проверку адреса (рис. 4.11).

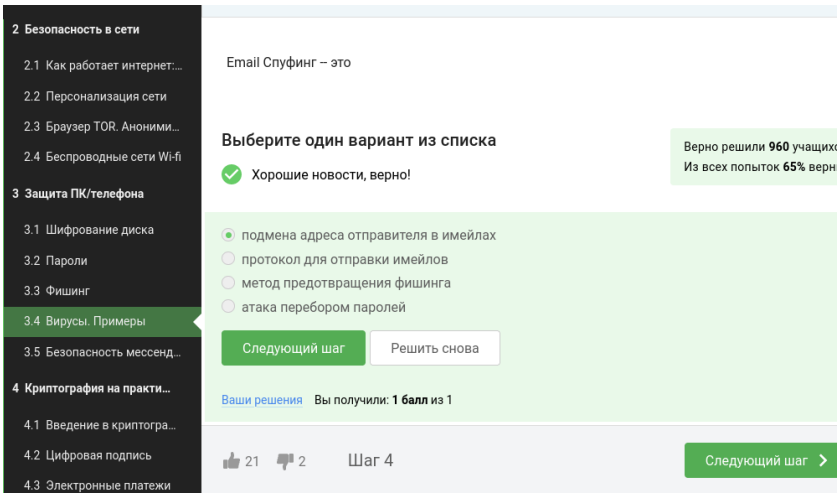


Рис. 4.11: Тест 12

Троян - это вирус, который проникает в систему под видом какого-то легитимного программного обеспечения, это аллюзия к троянскому коню. Этот вирус также распространялся по почте с вполне себе невинным письмом. Само вложение

устанавливало вполне себе легитимную утилиту от Windows, которая называлась WinGate proxy. (рис. 4.12).

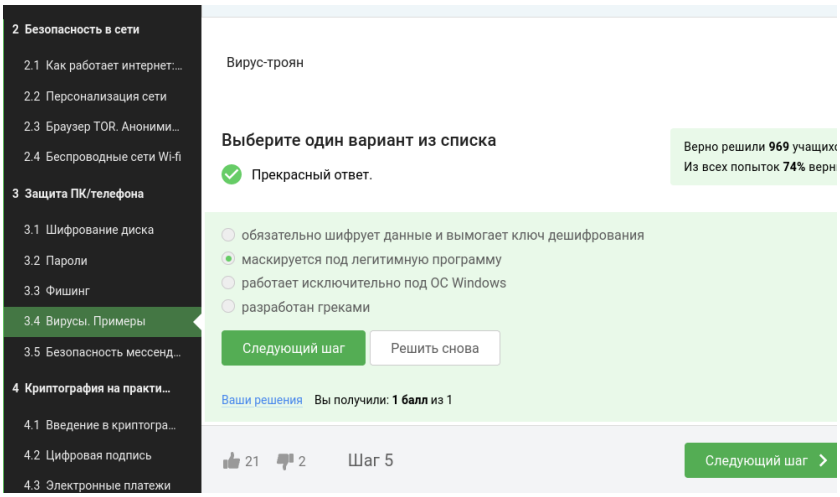


Рис. 4.12: Тест 13

сквозное шифрование - по-английски E2E или End-to-End encryption. Суть довольно простая: у нас есть два участника - Алиса и Боб, A и B, и сквозное шифрование заключается в том, что сервер, который передает сообщение, который направляет сообщение от Алисы к Бобу или от Бобу к Алисе, знает только то, куда эти сообщения должны быть направлены, но сообщения он передает в зашифрованном виде, то есть он как бы работает маршрутизатором сообщений, не зная о том, что он передает. Что происходит, если мы хотим отправить сообщение от Алисы к Бобу? Алиса шифрует свои данные, кладет на сервере шифр-текст с пометкой, что этот шифр-текст предназначен для Боба. Когда Боб заходит в сеть, сервер видит: «Ага, Боб зашел в сеть, надо обновить его сообщение», и отправляет шифр-текст от Алисы. Боб получает этот шифр-текст, дешифрует его, получает сообщение в открытом виде. При этом сервер не знает ни ключ, с помощью которого Алиса шифровала, ни тем более сообщение в открытом виде. (рис. 4.13).

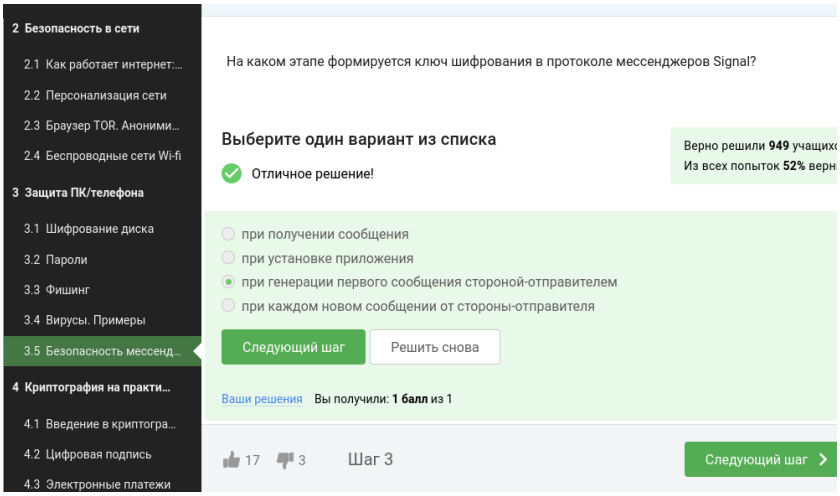


Рис. 4.13: Тест 14

(рис. 4.14).

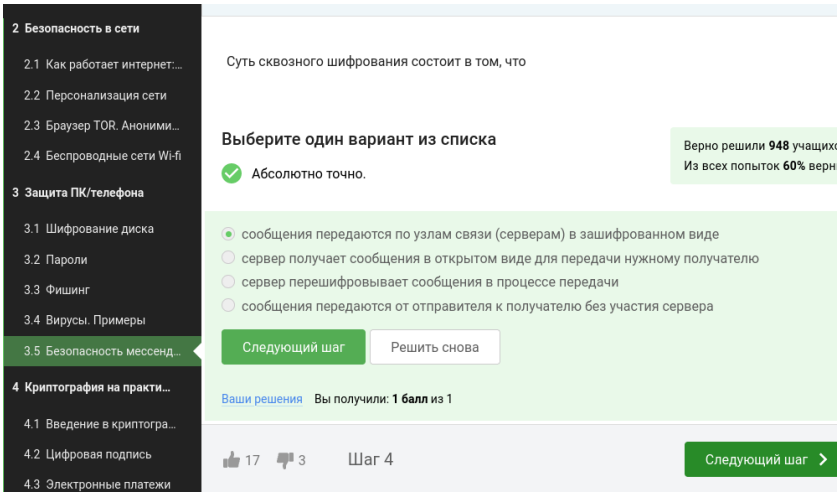


Рис. 4.14: Тест 15

5 Выводы

Мы научились Шифровать диск. Выбирать правильный пароль. Поняли, что такое фишинг и вирусы и как обезопасить свои менеджеры.

Прохождение внешнего курса 3 часть

Криптография на практике

Павлов Арсений НБИбд-03-22

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Рассмотрим что такое криптография на практике. Узнаем для чего нужна цифровая подпись. Как работают электронный платежи и разберем откуда появился блокчейн и как он работает. # Задание

Выполнить тестовую часть курса

2 Теоретическое введение

В асимметричной криптографии (её еще называют криптографией с открытым ключом) у каждой из сторон есть пара ключей: открытый ключ и секретный ключ. Открытый ключ публикуется в открытом доступе, а закрытый или секретный ключ сторона хранит у себя. К протоколам асимметричной криптографии относят электронно-цифровую подпись и протокол генерации общего ключа – это этот протокол, который позволяет нам не общаться физически друг с другом, а установить и вычислить общий секретный ключ.

Как правило, в современных протоколах, в современных конфиденциальных коммуникациях используются вместе симметричная криптография и асимметричная криптография. Это сделано, в частности, для того, чтобы сделать конфиденциальную коммуникацию эффективной, так как симметричные примитивы обычно являются более эффективными по времени, чем асимметричные примитивы. Во-вторых, цифровая подпись обеспечивает аутентификацию сообщения, то есть мы можем установить принадлежность подписи владельцу, иными словами, никто другой не смог бы поставить такую подпись под этим сообщением. Ну и последнее, третье – это неотказ от авторства, то есть как только подпись подписана, подписавший её человек не может отказаться от того факта, что он ее подписал. Конечно, в случае кражи секретного ключа, с помощью которого подписывается сообщение, формируется подпись, о корректной безопасности цифровой подписи никакой речи быть не может, поскольку секретный ключ украден. Вообще, этап авторизации покупки зависит от того, какой у нас платеж. Платежи делятся на две категории: первая – это card present или CP, это означает,

что у нас есть физический доступ к нашей карточке, например, когда мы делаем покупки в супермаркете и, оплачивая, мы прикладываем нашу карту к терминалу, либо считываем. Что при этом происходит? При этом терминал, как правило, запрашивает у вас PIN-код. Вы вводите PIN-код, после этого формируется подпись, то есть с помощью вашего PIN-кода на ваш чек, на вашу покупку ставится ваша подпись. У вас как бы есть свой секретный ключ, вшитый в вашу карточку, который генерирует подпись. Эта подпись отправляется банку-эмитенту, он проверяет с помощью вашего публичного ключа, который лежит у банка, эту подпись. Если подпись верна, банк подтверждает транзакцию, вы себя аутентифицировали как владельца этой карты. Для начала разберемся с двумя важными понятиями. Первое: между понятиями крипто (Crypto) и криптовалюта (Cryptocurrency) не стоит знак равенства. Под крипто мы понимаем криптографию как науку, и вы уже знаете довольно много примитивов и терминов из этой области. А вот криптовалюта - это разновидность цифровых денег, которые построены на основе технологии блокчейн. Почему она называется криптовалютой? Потому что для ее корректной работы используются криптографические примитивы. Что я понимаю под корректной работой? Мы все знаем, что деньги должно быть сложно скопировать, и для того, чтобы криптографическую валюту было сложно подделать или скопировать, используются криптографические примитивы. Вторая цель - это обеспечение того, чтобы в криптовалюте одни и те же деньги нельзя было потратить дважды. То есть, когда монеты уже были потрачены или заплачены мной кому-то еще, я не могу эти же самые деньги потратить второй раз. Это свойство также достигается за счет криптографических примитивов. Второе, что нужно понимать - это то, что между биткоином и блокчейном не стоит знак равенства. Несмотря то, что биткоин - это самая популярная криптовалюта на сегодняшний день и первая из криптовалют, это всего лишь одна из возможных криптовалют. Кроме того, это ещё и платежная система, которая использует одноименную валюту. Но у нас есть и другие, не менее интересные криптовалюты, такие как Эфир, Monero, Tether, Zcash, их довольно много на сегодняшний день,

и все они популярны настолько, насколько популярен Биткоин. Однако у них есть свои преимущества относительно Биткоина. Мы не будем в этой лекции углубляться в каждую из них, мы рассмотрим, как работает технология блокчейн.

Зачем вообще она нужна? Основная причина создания криптовалют - это желание работать с децентрализованной платежной системой. Децентрализованная означает, что в этой системе нет какого-то банка как центральной единицы, а значит и нет государственного контроля над средствами. Кому и когда эта идея пришла в голову? Академическая статья о Биткоине вышла 12 января 2009 года и была подписана именем Сатоши Накамото. На самом деле, мы до сих пор не знаем, кто такой Сатоши Накамото, существует ли этот человек на самом деле, это несколько человек или эта компания, но это не важно; важно то, что эта статья положила начало криптографической валюте. В аннотации статьи написано, что она предлагает версию электронных денег. На самом деле электронные деньги как примитив существовали задолго до 2009 года, но важно то, что в этой статье предлагается механизм построения электронных денег, который бы позволил осуществлять онлайн платежи от одного человека к другому без какого-либо финансового института и без какой-либо третьей доверенной стороны, и это положило начало тому, что мы сегодня называем криптографическая валюта. В первой статье была предложена версия криптографической валюты Bitcoin.

3 Выполнение лабораторной работы

В асимметричной криптографии (её еще называют криптографией с открытым ключом) у каждой из сторон есть пара ключей: открытый ключ и секретный ключ. (рис. 3.1).

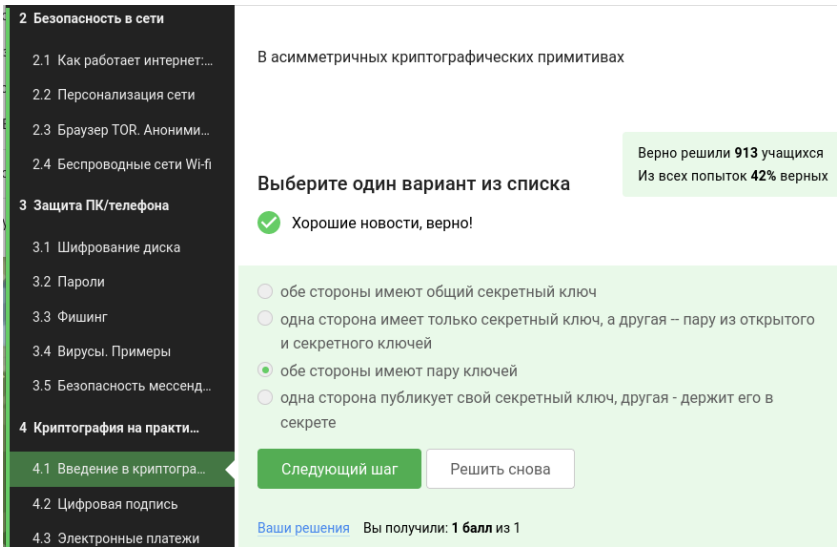


Рис. 3.1: Тест 1

Важное свойство криптографической хэш-функций, то, что делает её криптографической – это стойкость к коллизиям. Что такое коллизия? Коллизия – это два разных входа в хэш-функцию, которые дают одинаковый выход. То есть это две разные строки например x и x’, где $x \neq x'$, такие, что значения хэш-функции на них совпадают, то есть $h(x) = h(x')$. Это важное свойство отличает криптографическую функцию от некриптографической. Можно доказать (мы этого делать с вами не будем), что из этого свойства коллизии следует другое важное свойство,

а именно то, что криптографическую хэш-функцию сложно обратить. То есть, если я вам даю какое-то значение этой функции в точке h(x) и спрашиваю вас, как найти x, то есть вход в эту функцию, для современных криптографических хэш-функций это сделать сложно.

Благодаря этим свойствам, криптографические функции широко применяются в коммуникациях, мы с вами в одной из лекций говорили о том, как криптографическую хэш-функцию можно использовать для хранения паролей. Она также используются для протоколов, подтверждающих целостность данных, ну и современное довольно популярное применение хэш-функции – это доказательство работы. По-другому это называется протоколом proof of work, который используется, например, в таком блокчейне, как биткойн. (рис. 3.2).

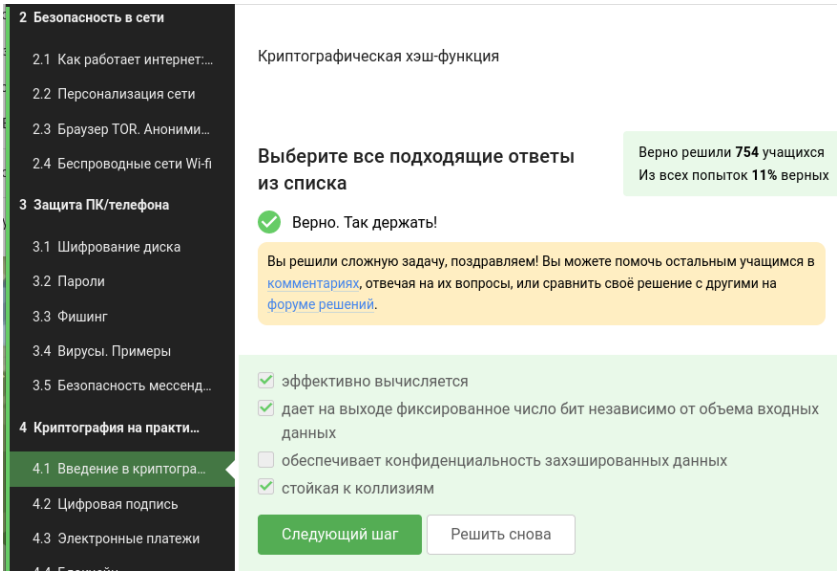


Рис. 3.2: Тест 2

К примерам цифровой подписи относятся интернет-сертификаты, подпись RSA, американский стандарт ECDSA и отечественный стандарт ГОСТ стандарт Р 34.10.2012. (рис. 3.3).

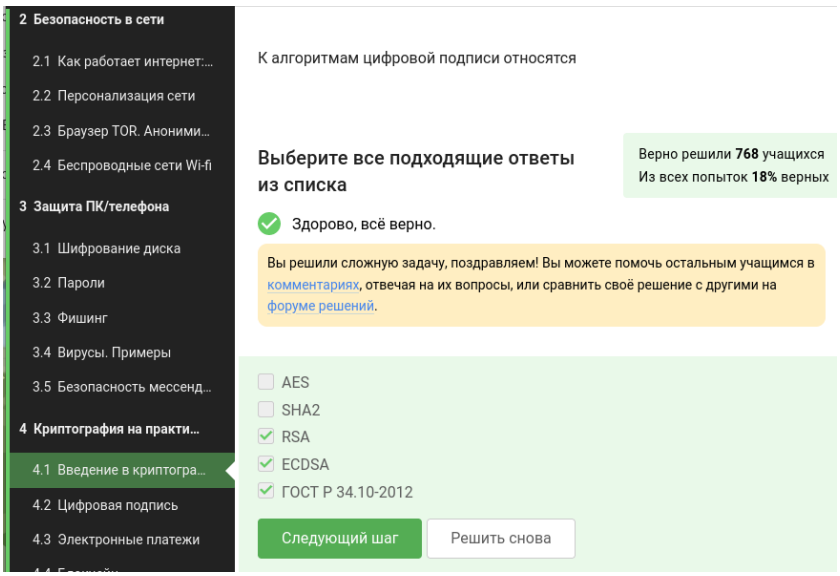


Рис. 3.3: Тест 3

Определяющее свойство симметричной криптографии состоит в том, что она включает себя протоколы, где две или более стороны имеют общие секретные ключи, поэтому она и называется симметричной. К таким протоколам относят симметричное шифрование и некоторые протоколы аутентификации. (рис. 3.4).

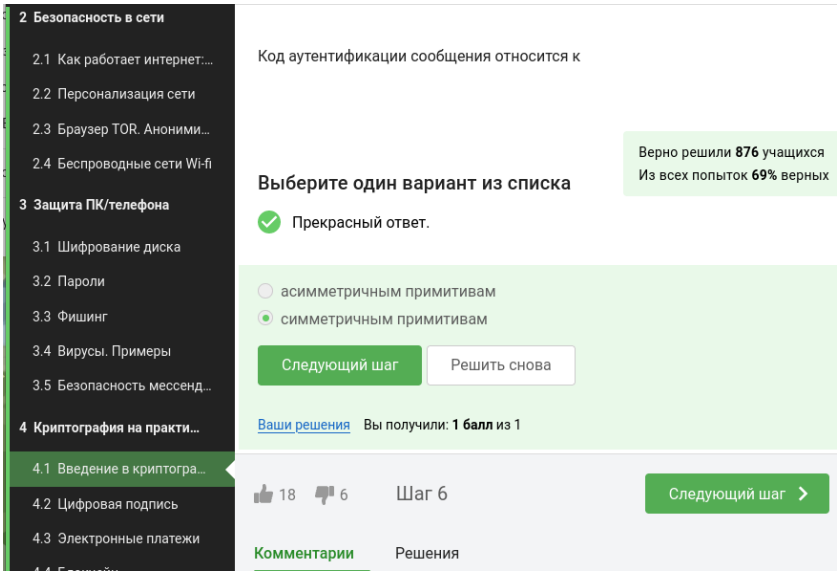


Рис. 3.4: Тест 4

Самым популярным примером протокола обмена ключами является протокол Диффи-Хэллмана, как раз он, либо его модификации используются в современных мессенджерах и в протоколе TLS для того, чтобы мы смогли сгенерировать общий секретный ключ и дальше шифровать наши данные с помощью симметричного алгоритма, то есть с помощью ключа skAB. Если реализовать генерацию общего ключа так, как она описана у Диффи-Хэллмана, мы получим довольно слабый протокол, нестойкий к активным злоумышленникам. (рис. 3.5).

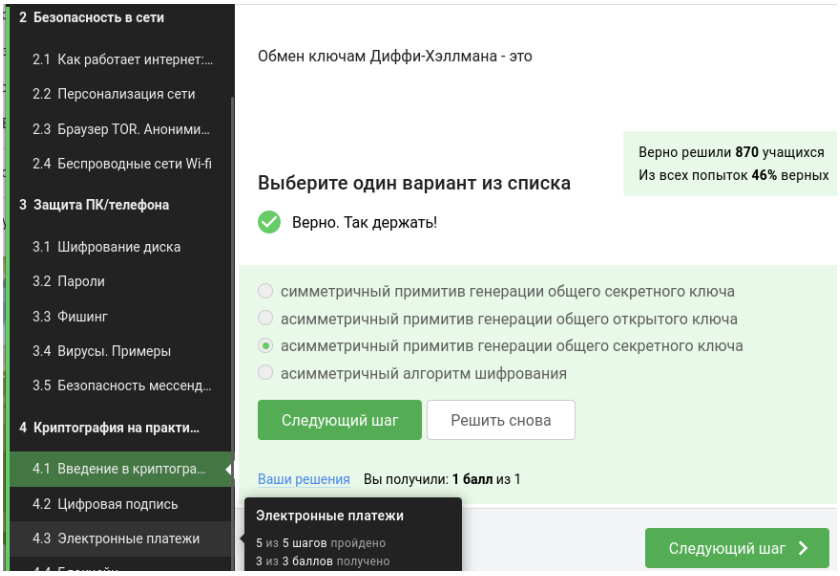


Рис. 3.5: Тест 5

Цифровая подпись имеет прямую связь с асимметричной криптографии (её еще называют криптографией с открытым ключом) у каждой из сторон есть пара ключей: открытый ключ и секретный ключ. Открытый ключ публикуется в открытом доступе, а закрытый или секретный ключ сторона хранит у себя. (рис. 3.6).

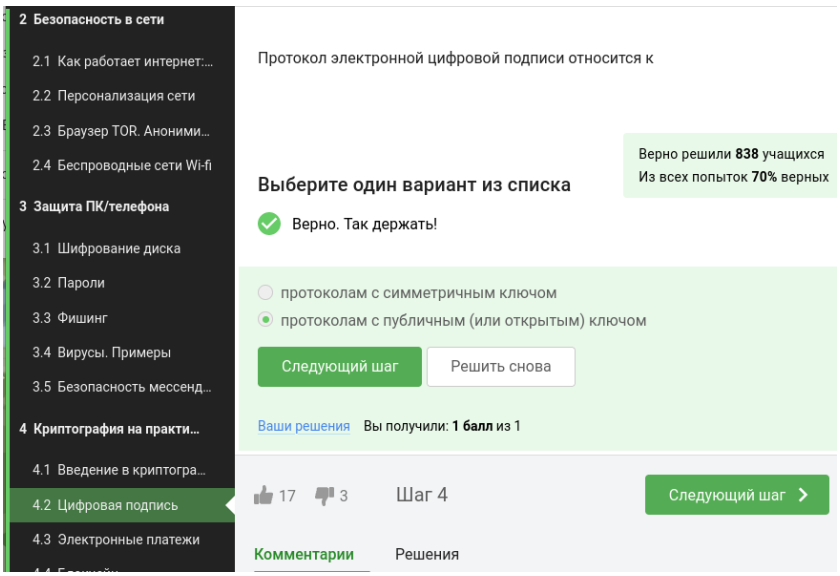


Рис. 3.6: Тест 6

Первый алгоритм занимается генерацией ключей, он генерирует публичный ключ и секретный ключ. Публичный ключ мы держим в открытом доступе, секретный ключ – у себя, никому не показываем. Секретный ключ еще называется подписывающим ключом, а открытый – проверяющим или ключом верификации. Второй алгоритм – это генерация подписи, которая берет на вход сообщение и секретный ключ и выдает нам подпись. И третий – это верификация подписи, которая берёт на вход подпись, сообщение и открытый ключ и выдает нам либо тот факт, что подпись верна, либо тот факт, что подпись неверна. (рис. 3.7).

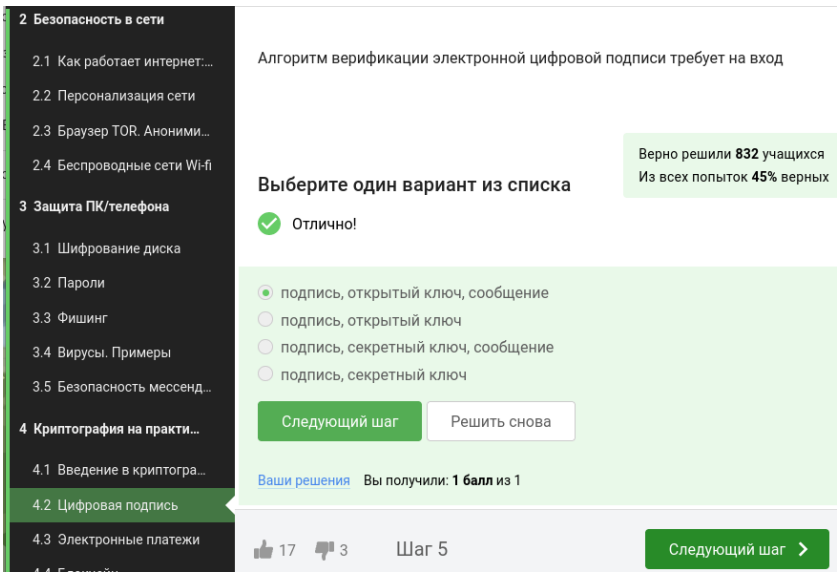


Рис. 3.7: Тест 7

Цифровая подпись предназначена, во-первых, для обеспечения целостности сообщения, иными словами, если сообщение в процессе передачи было изменено, то подпись этого измененного сообщения будет проверена некорректно, то есть при проверке корректности подписи мы узнаем о том, что сообщение было изменено. Во-вторых, цифровая подпись обеспечивает аутентификацию сообщения, то есть мы можем установить принадлежность подписи владельцу, иными словами, никто другой не смог бы поставить такую подпись под этим сообщением. Ну и последнее, третье – это неотказ от авторства, то есть как только подпись подписана, подписавший её человек не может отказаться от того факта, что он ее подписал. (рис. 3.8).

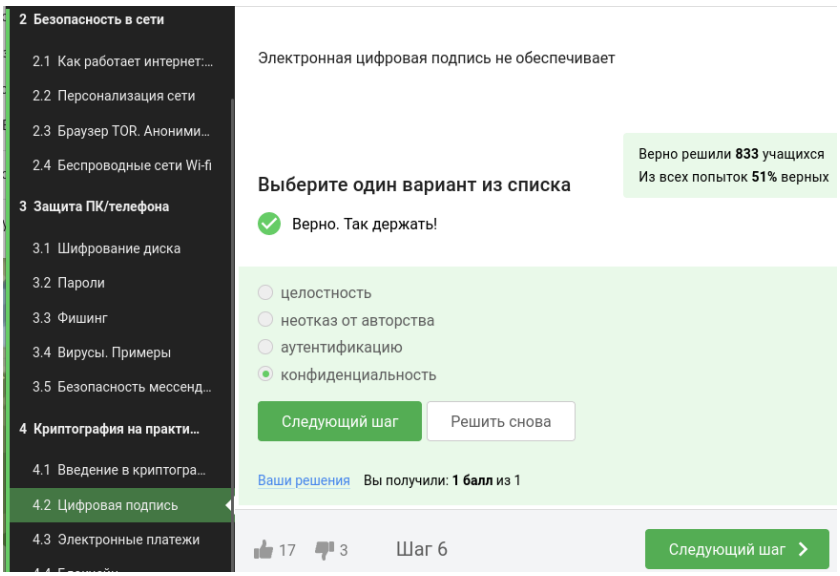


Рис. 3.8: Тест 8

Существует три различных точки зрения на подписи: простая, усиленная неквалифицированая и усиленная квалифицированная. Первые два типа не имеет юридической силы или она довольно ограничена (рис. 3.9).

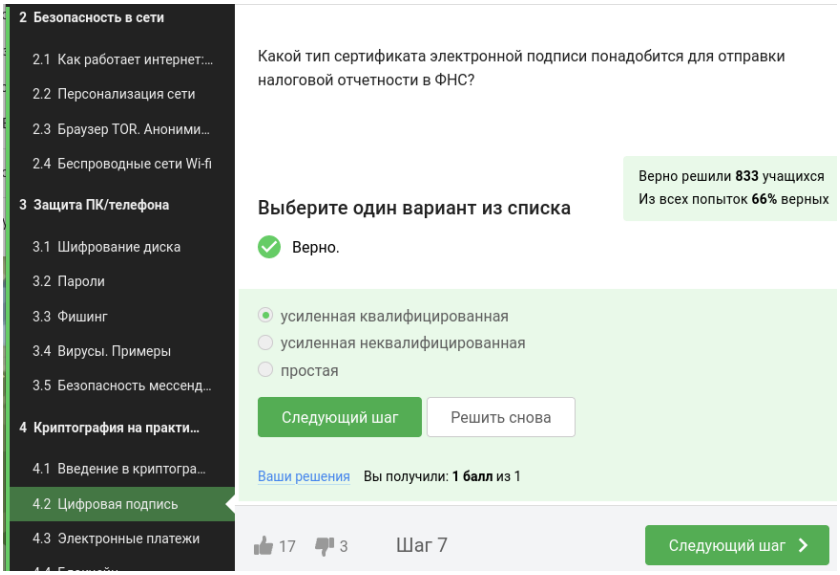


Рис. 3.9: Тест 9

А вот что касается усиленной квалифицированной подписи, эта подпись уже

имеет юридическую силу, она, как правило, равнозначна рукописной. Для того, чтобы получить такую подпись, вам нужно пойти со своим паспортом и с другими данными в сертификационный центр, который должен быть аккредитован конкретным министерством. Такие подписи используются на Госуслугах, в государственном документообороте. (рис. 3.10).

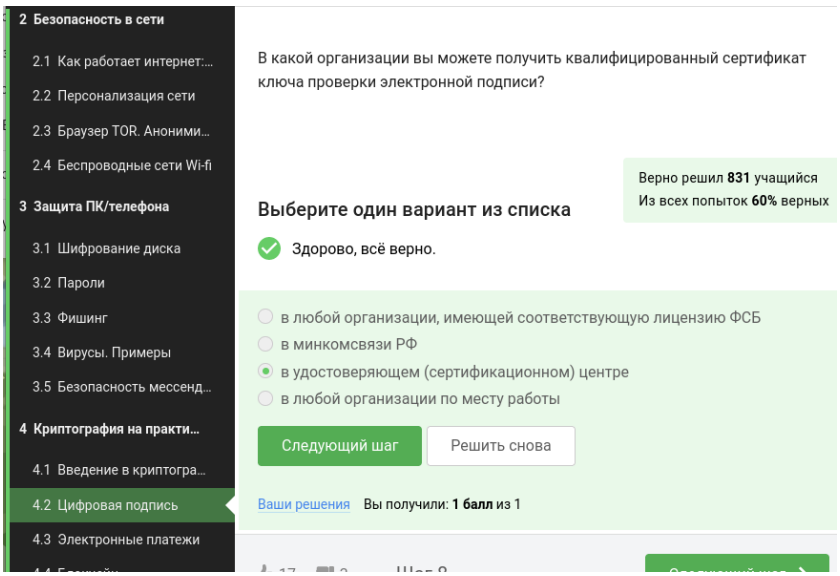


Рис. 3.10: Тест 10

Данные платежные системы самые популярные (рис. 3.11).

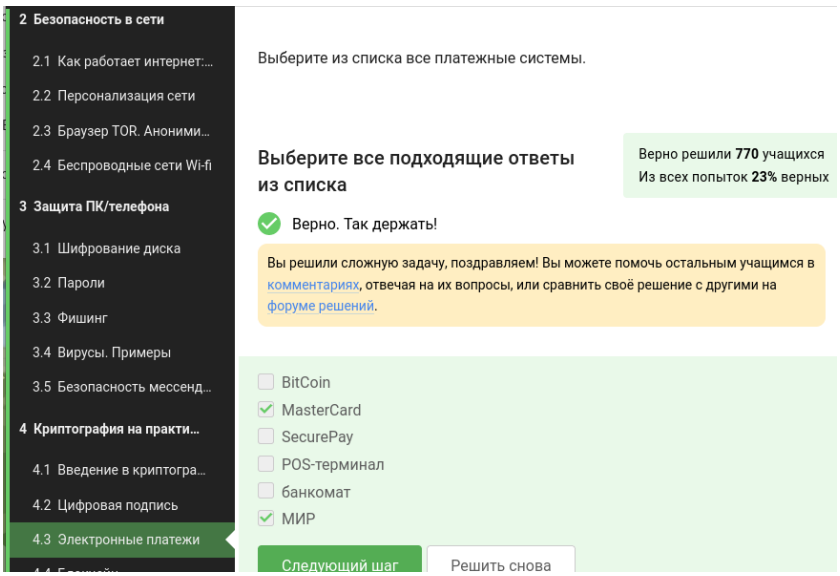


Рис. 3.11: Тест 11

Многофакторная аутентификация заключается в том, что мы доказываем в ходе этого протокола несколько вещей есть. Основные категории вещей, которые мы можем доказать: 1) то, что я знаю – это либо пароль, либо PIN-код, либо в случае онлайн-платежей это секретный код, 2) конкретно в онлайн-платежах мы еще используем второй фактор – это то, чем я владею, например, телефон, именно поэтому нам часто приходит код, который вы должны подтвердить или вбить в ваш браузер, 3) другой фактор аутентификации – это свойства, например, биометрия, опечаток пальца, сетчатки глаза, 4) четвертый фактор аутентификации – локация. Способ аутентификации, как правило, выбирается банком. (рис. 3.12).

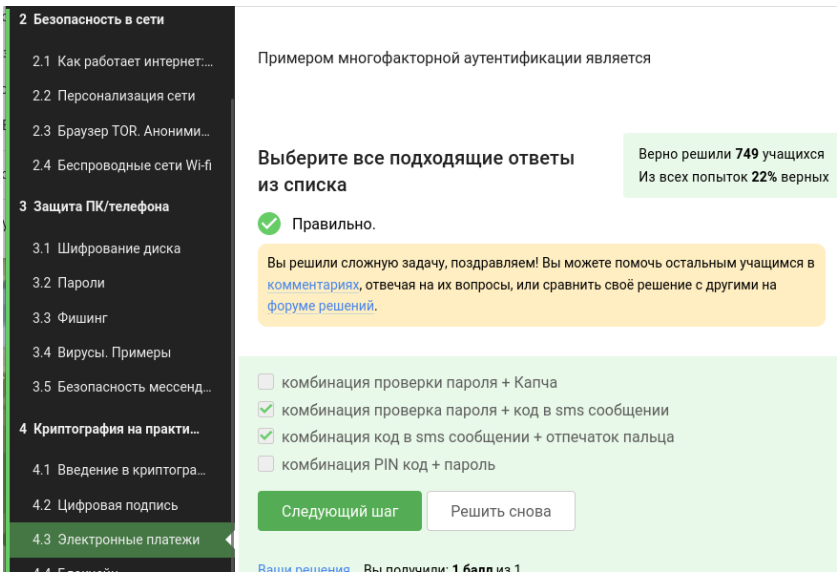


Рис. 3.12: Тест 12

Происходит многофакторная аутентификация. Аутентификация вообще – это криптографический протокол, в котором есть две стороны: первая – это доказующая (в этом случае покупатель) и проверяющая (в этом случае это банк), которые доказывают, что некое утверждение верно. В аутентификации при покупке утверждение, которое я как покупатель хочу доказать, это то, что это моя карта и она мне принадлежит. Вообще, аутентификация может осуществляться не только при покупке, онлайн-платежах, она может осуществляется, когда мы открываем свою машину бесконтактным ключом, мы тоже пытаемся себя аутентифицировать. (рис. 3.13).

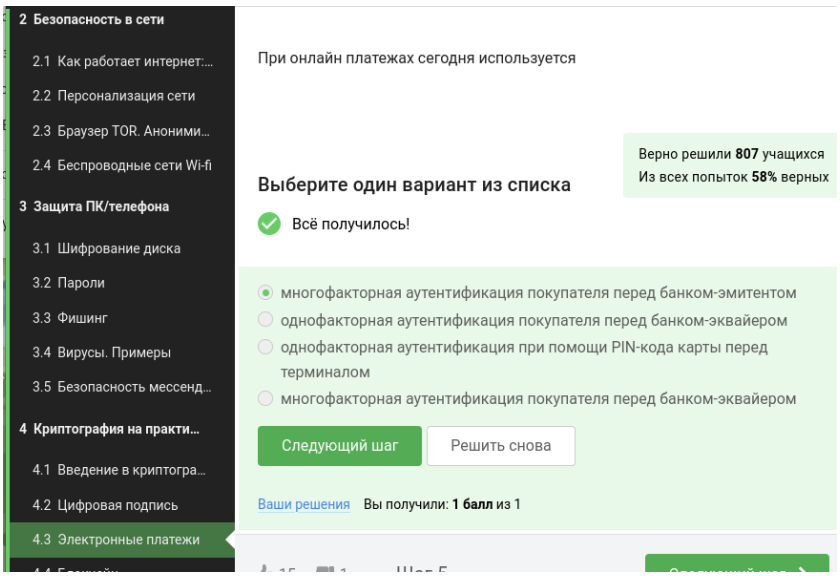


Рис. 3.13: Тест 13

Рассмотрим, наконец, одно из этих доказательств, например, доказательство работы, потому что оно сегодня самое популярное, поскольку оно используется в биткоине, самой распространённой криптовалюте. Как работает доказательство работы? Тут мы с вами вспоминаем старую добрую криптографическую хэш-функцию, это функция, которая берет на вход любые данные и выдает за какое-то быстрое время фиксированное число бит. И задача майнера в доказательстве работы - это отыскать такой вход в хэш-функцию, что ее значение имеет определенный паттерн, иными словами, отыскать такой x, что h(x) имеет, например, 17 первых нулей или 17 первых единиц, это неважно. В биткоине используют 18 или 19 первых нулей. Это число на самом деле может быть модифицировано относительно производительности сети в тот или иной момент времени. (рис. 3.14).

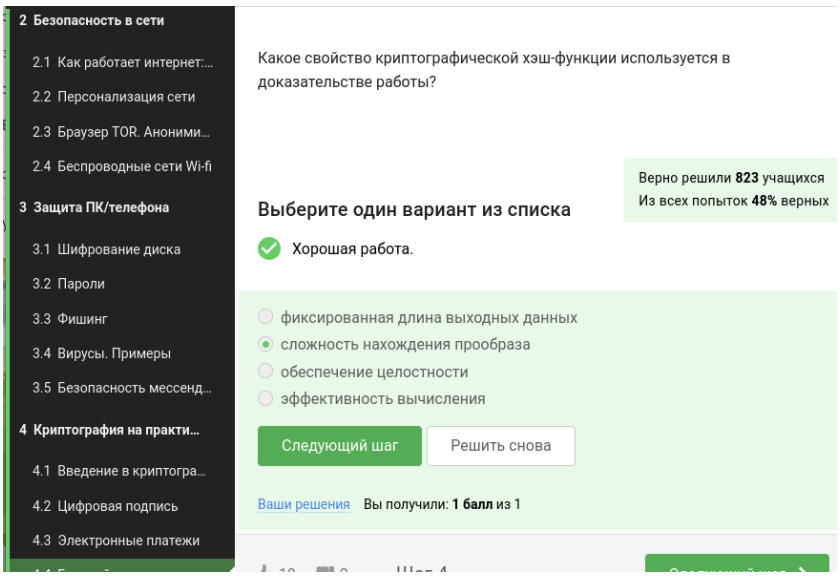


Рис. 3.14: Тест 14

В основе блокчейна лежит консенсус — — публичная структура данных или леджер (бухгалтерская книга), которая обеспечивает • постоянство добавленные когда-либо данные не могут быть удалены • консенсус все участники видят одни и те же данные (за исключением последних пары блоков) • живучесть участники могут добавлять новые транзакции • открытость (не для всех блокчейнов) любой может стать участником блокчейна (рис. 3.15).

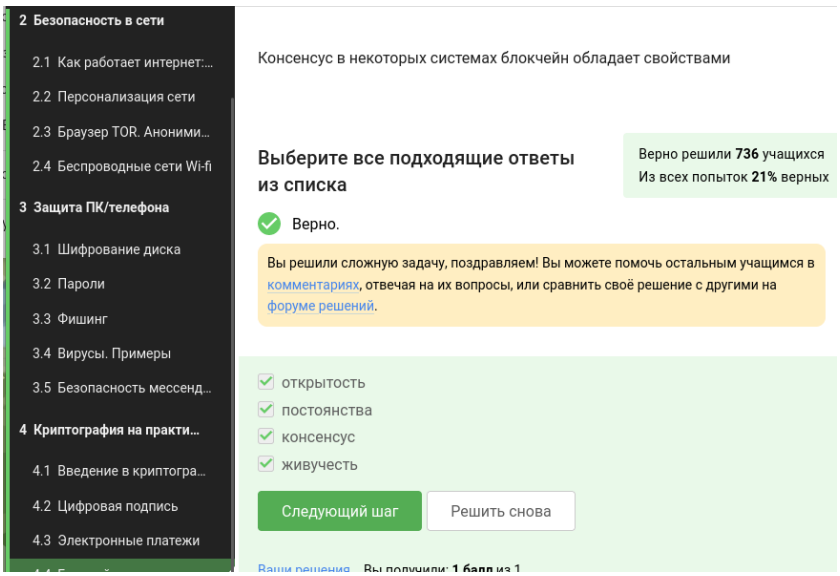


Рис. 3.15: Тест 15

Важно то, что у каждого участника есть свой секретный ключ, и своим секретным ключом мы всегда будем подтверждать какую-то транзакцию. Важно то, что этот ключ у нас секретный, мы его используем для подписи. Подпись – это и есть подтверждение моей транзакции. Мы с вами разбирали в одной из лекций, как работает электронная цифровая подпись, у этого примитива есть секретный и открытый ключи, и наш секретный ключ - это то, что позволяет нам совершать транзакции от нашего лица. (рис. 3.16).

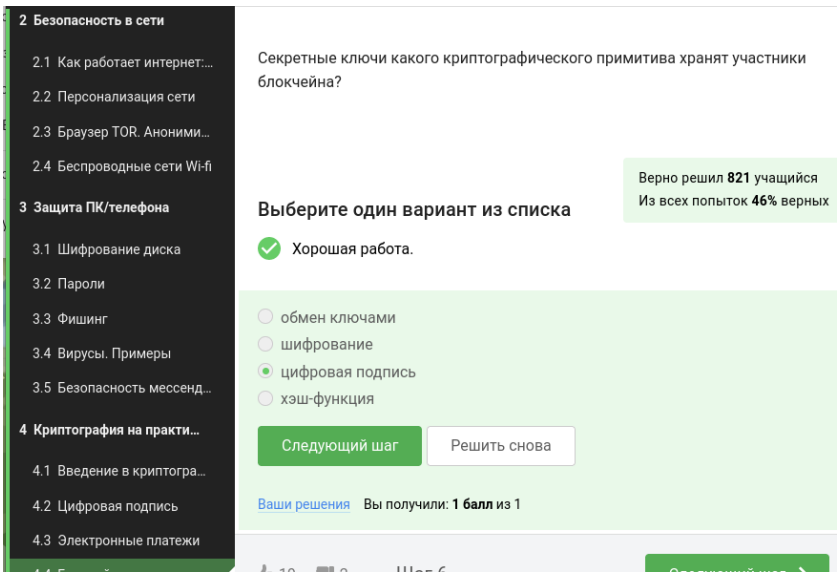


Рис. 3.16: Тест 16

4 Выводы

Мы рассмотрели что такое криптография на практике. Узнали для чего нужна цифровая подпись и как работают электронный платежи. Разобрались откуда появился блокчейн и как он работает.