Внешний курс

Степик по основам безопасности

Воробьев Данил Павлович

Содержание

# 1 Блок 1

# 2 Цель работы

Выполнить контрольные задания первого блока “Безопасность в сети” внешнего курса “Основы кибербезопасности”.

# 3 Выполнение заданий блока “Основы Кибербезопасности”

## 3.1 Как работает интернет: базовые сетевые протоколы

Протокол HTTP(S) протокол прикладного уровня, ответ на вопрос 1 - HTTPS (рис. 1).

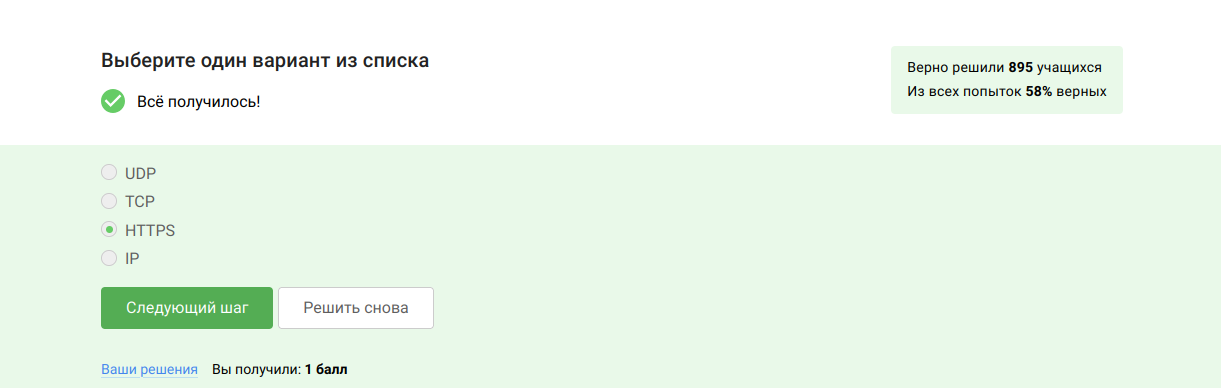


Рис. 1: Вопрос 2.1.1

На транспортном уровне существует два примера протокола: первый - это TCP, в честь которого названа модель. (рис. 2).

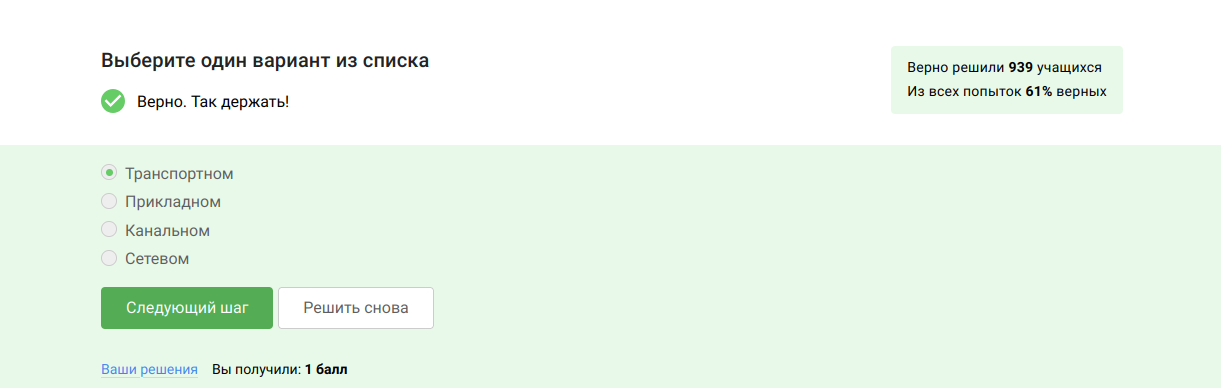


Рис. 2: Вопрос 2.1.2

Т.к адрес состоит из большего набора чисел, а именно это 4 или 6 цифер от 0 до 255. В двух вариантах встречаются цифры больше 255, что неверно(рис. 3).

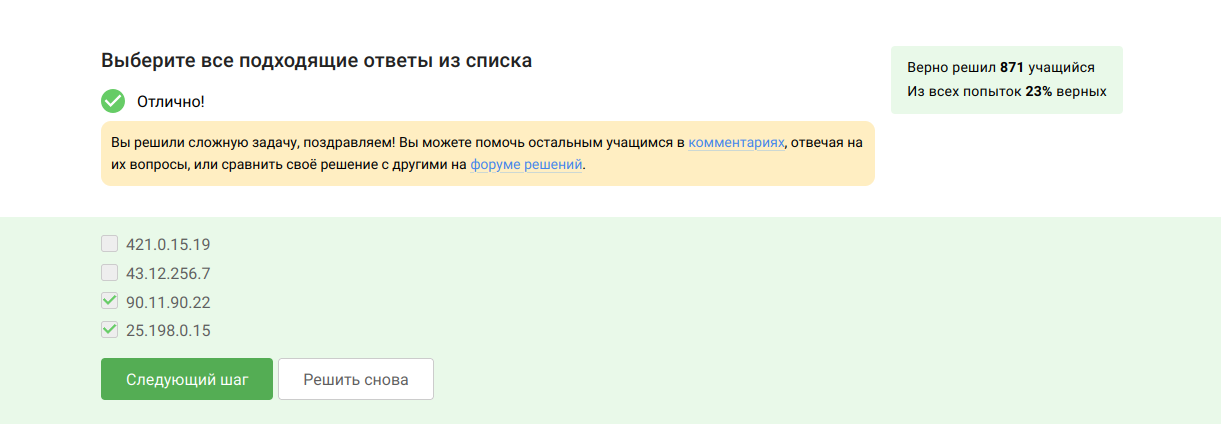


Рис. 3: Вопрос 2.1.3

Основная задача DNC это сопоставлять название ( доменное имя, с корекстым IP-адресом) с тем, где лежит этот сервер, этот сайт. (рис. 4).

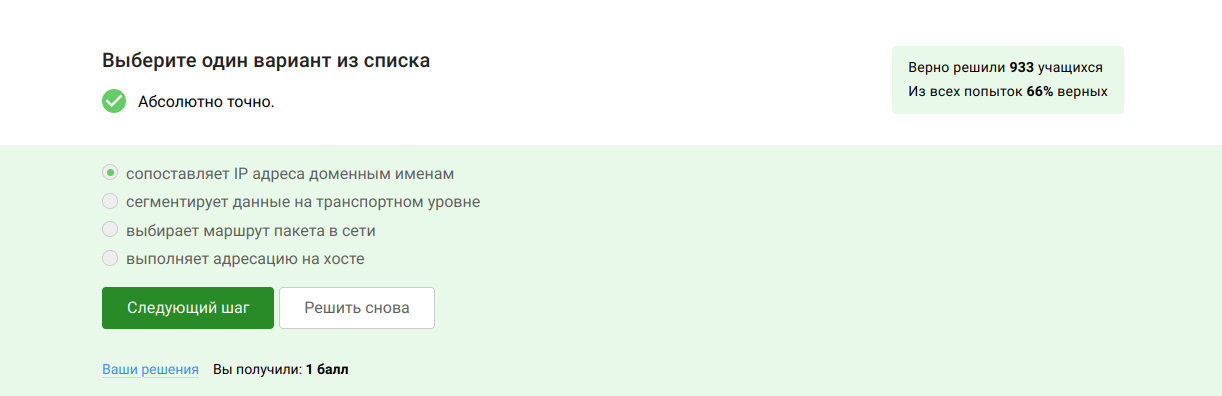


Рис. 4: Вопрос 2.1.4

Классификация протоколов в модели TCP/IP:

* Прикладной уровень: HTTP, RTSP, FTP, DNS.
* Транспортный уровень: TCP, UDP, SCTP, DCCP.
* Сетевой уровень: IP.
* Уровень сетевого доступа (Канальный) (Link Layer): Ethernet, IEEE 802.11, WLAN, SLIP, Token Ring, ATM и MPLS(рис. 5).

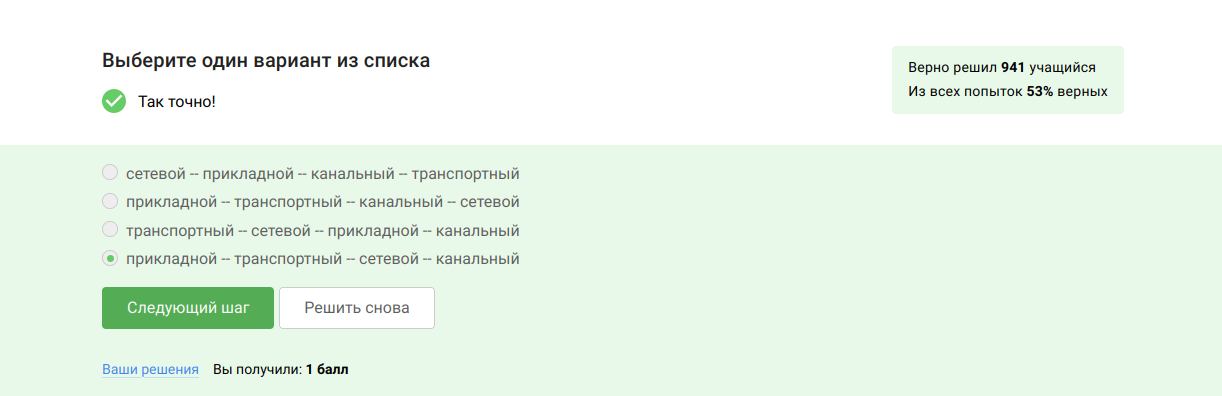


Рис. 5: Вопрос 2.1.5

Протокол http передает не зашифрованные данные, а протокол https уже будет передавать зашифрованные данные (рис. 6).

https передает зашифрованные данные, поэтому одна из фаз это передача данных, другая должна быть рукопожатием

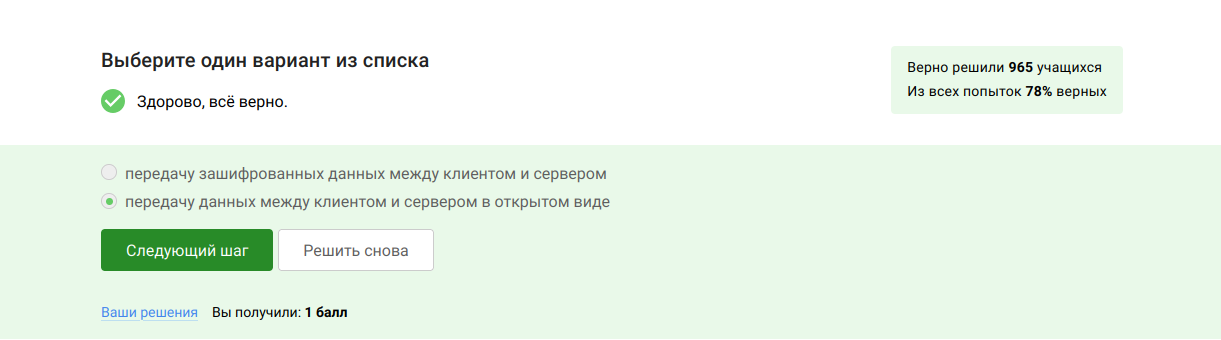


Рис. 6: Вопрос 2.1.6

TLS определяется и клиентом, и сервером, чтобы было возможно подключиться (рис. 7).

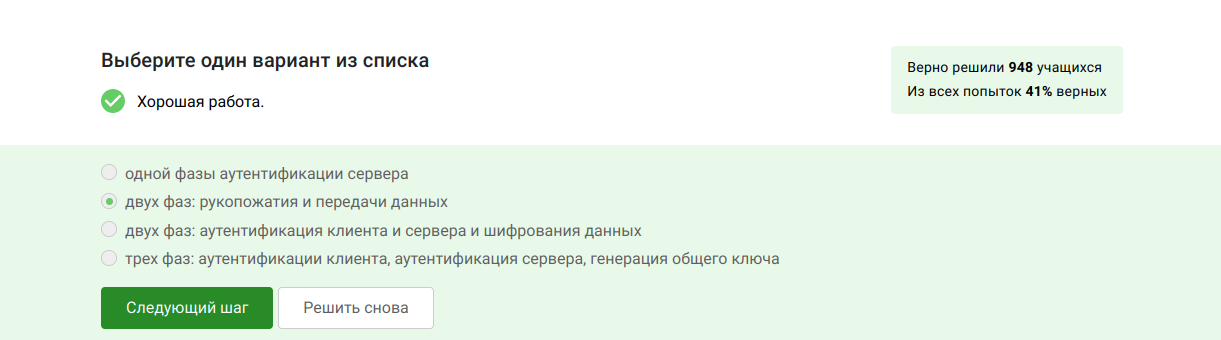


Рис. 7: Вопрос 2.1.7

TLS определяется клиентом и сервером, чтобы возможно было подключиться (рис. 8).

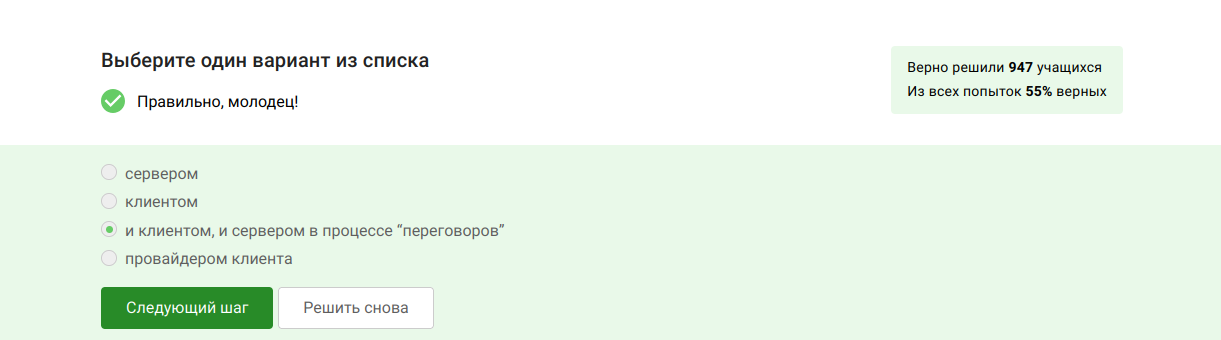


Рис. 8: Вопрос 2.1.8

Фаза рукопожатия вкючает в себя:

* выбор параметров, протоколов
* аутентификация (как минимум, сервера)
* формируется общий секретный ключ K

Следовательно вариант с шифрованием лишний (рис. 9).

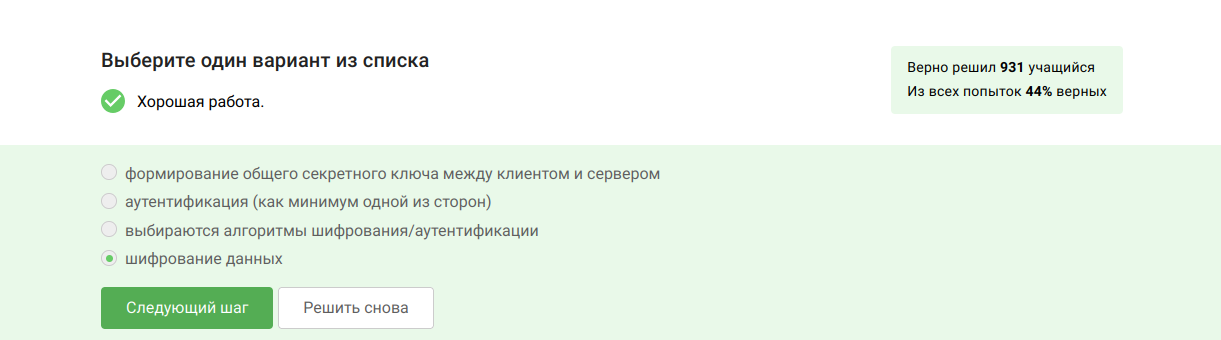


Рис. 9: Вопрос 2.1.9

## 3.2 Персонализация сети

Куки хранят в себе список параметров и их значений. Этими параметрами могут быть id пользователя, id сессии, тип браузера и некоторые действия пользователей(рис. 10).

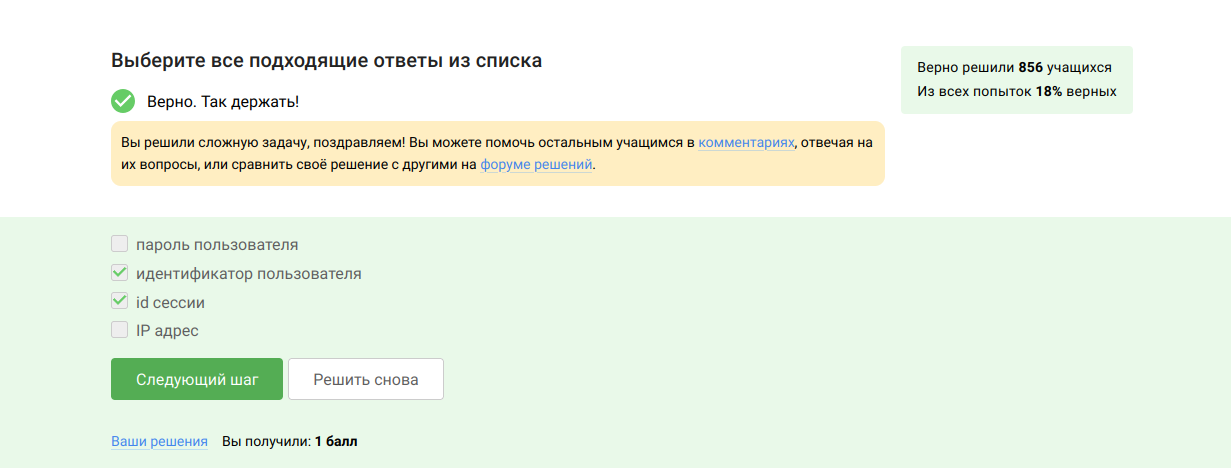


Рис. 10: Вопрос 2.2.1

Куки не делают соединение надежным (рис. 11).

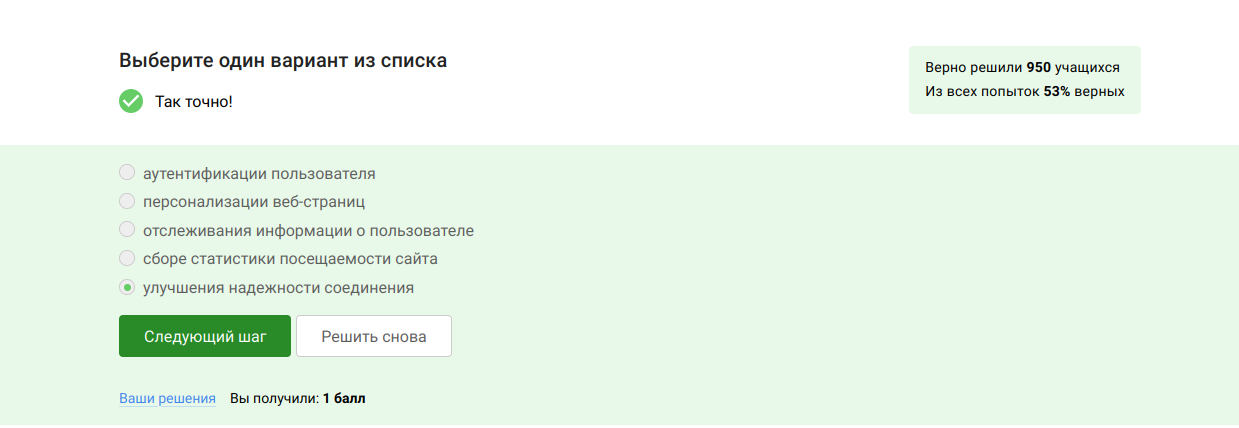


Рис. 11: Вопрос 2.2.2

Куки генерируются сервером(рис. 12).

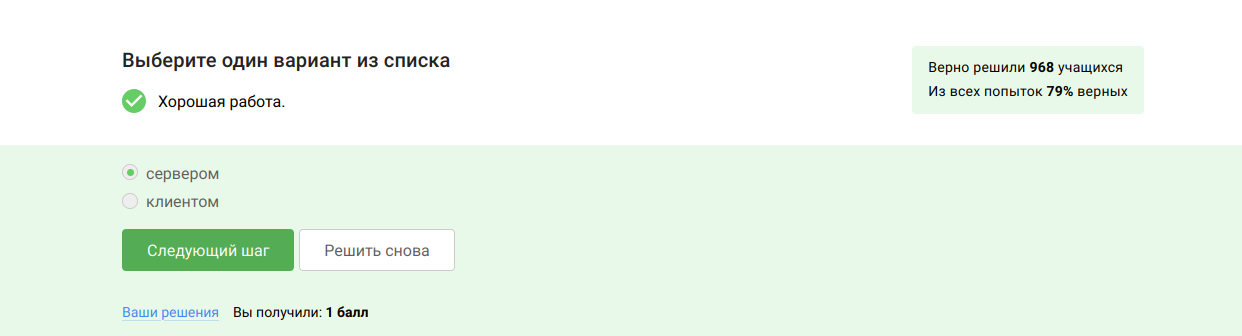


Рис. 12: Вопрос 2.2.3

Куки бывают сессионные, удаляются при закрытии окна браузера (рис. 13).

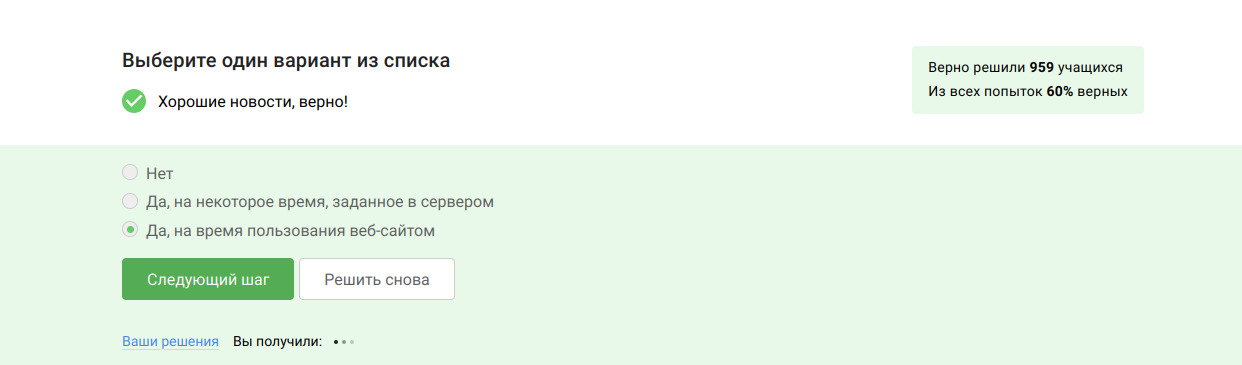


Рис. 13: Вопрос 2.2.4

## 3.3 Браузер TOR. Анонимизация

В луковой модели маршрутизации у нас тоже есть узлы. Они разделяются на охранный узел, промежуточный и выходной. В браузере Tor всегда есть три роутера, их не больше и не меньше (рис. 14).

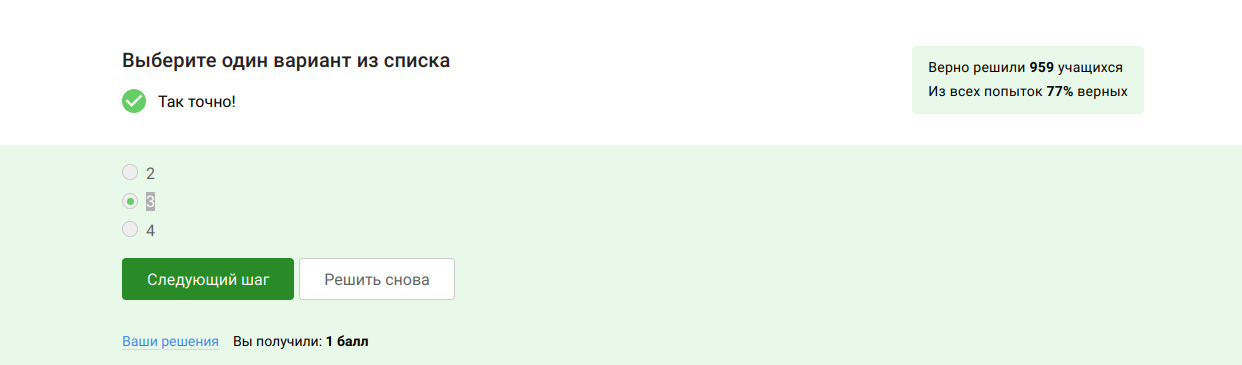


Рис. 14: Вопрос 2.3.1

IP-адрес не должен быть известен охранному и промежуточному узлам (рис. 15).

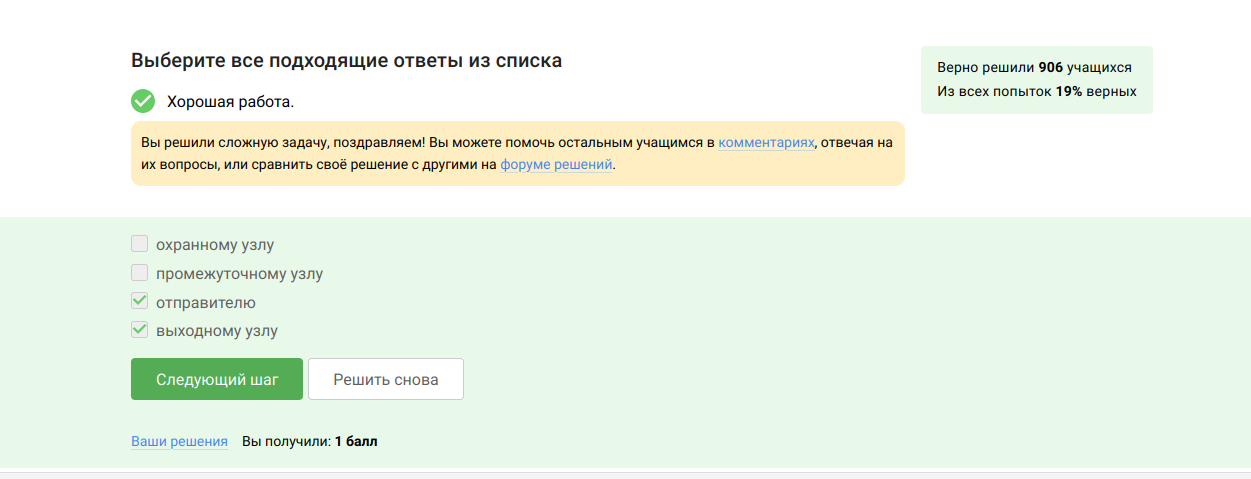


Рис. 15: Вопрос 2.3.2

В анонимных сетях, таких как Tor, общий секретный ключ для сквозного шифрования требует участия всех трех типов узлов: охранного, промежуточного и выходного. Охранный узел сам по себе не обеспечивает генерацию ключа. Каждый узел вносит свой вклад в криптографический протокол (например, Diffie-Hellman), обеспечивая анонимность и защиту от перехвата. (рис. 16).

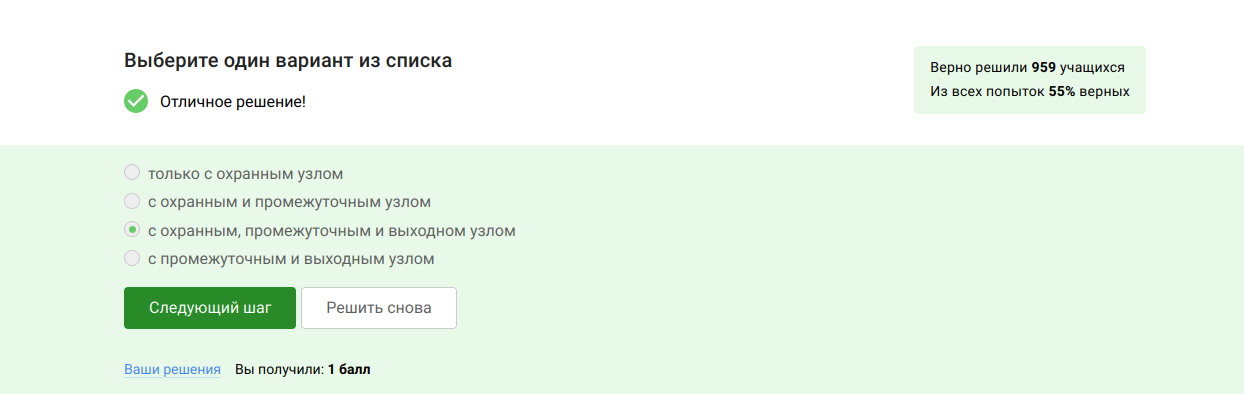


Рис. 16: Вопрос 2.3.3

Для получения пакетов не нужно использовать TOR. TOR — это технология, которая позволяет с некоторым успехом скрыть личность человека в интернете.(рис. 17).

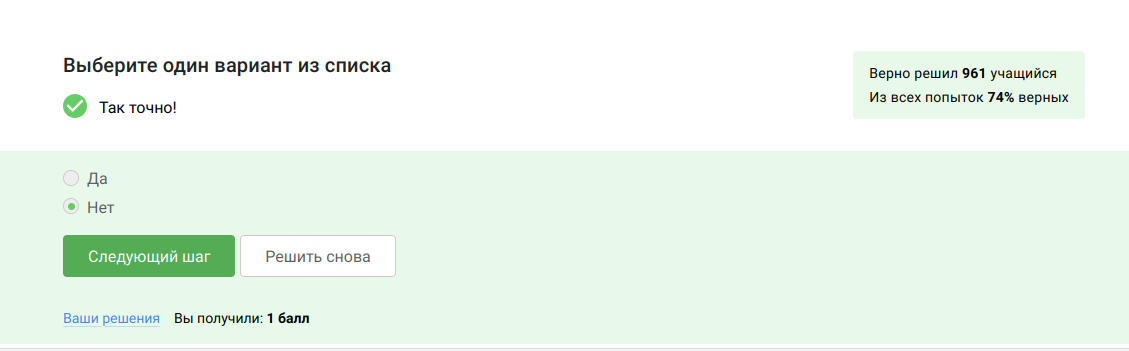


Рис. 17: Вопрос 2.3.4

## 3.4 Беспроводные сети Wi-fi

WiFi - это технология беспроводной локальной сети, она основана на стандарте IEEE 802.11 (рис. 18).

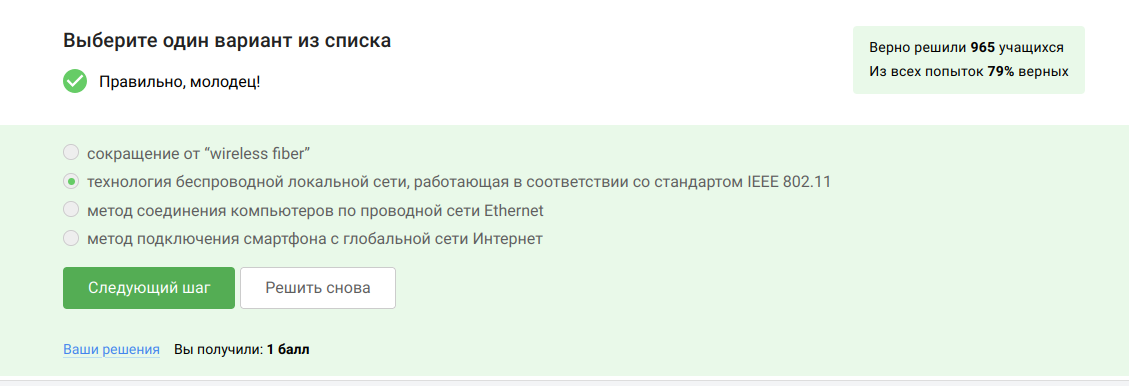


Рис. 18: Вопрос 2.4.1

WiFi работает на самом нижнем канальном уровне (рис. 19).

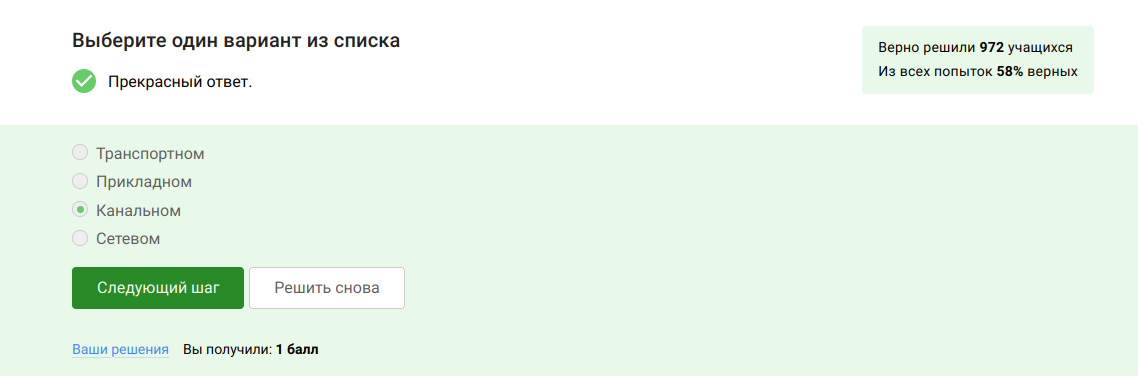


Рис. 19: Вопрос 2.4.2

WEP - устаревший и небезопасный метод шифрования WiFi из-за короткой длины ключа (40 бит), что делает его легко взламываемым. Использовать WEP категорически не рекомендуется.(рис. 20).

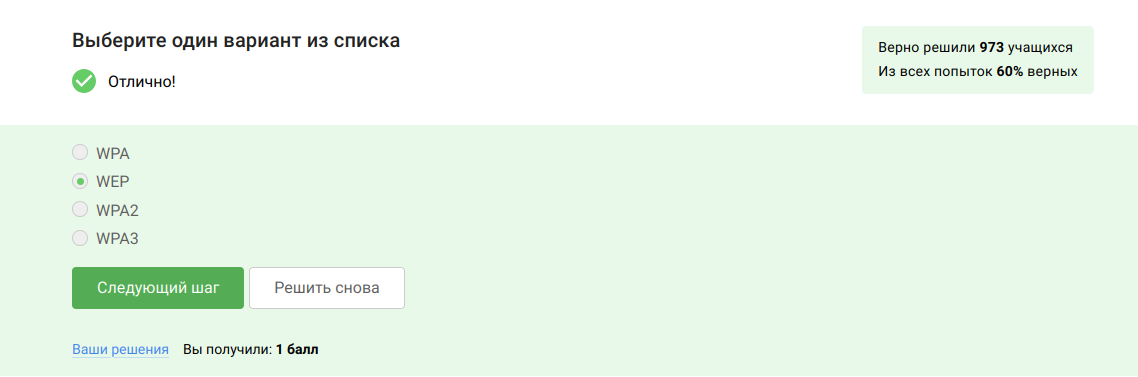


Рис. 20: Вопрос 2.4.3

Безопасность WiFi подразумевает защиту передачи данных между устройством (телефон, компьютер) и роутером (подключенным к интернету), осуществляемую с помощью шифрования и аутентификации.(рис. 21).

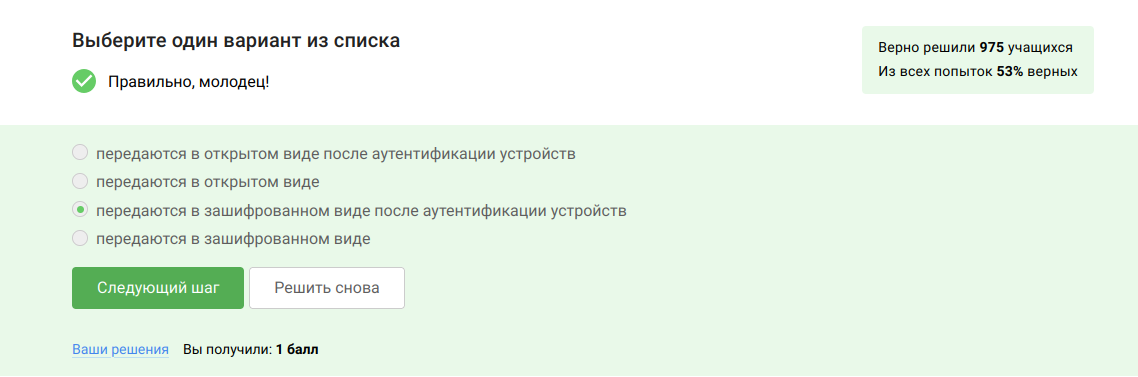


Рис. 21: Вопрос 2.4.4

WPA2 Personal предназначен для домашнего использования, а WPA2 Enterprise - для коммерческих организаций. (рис. 22).

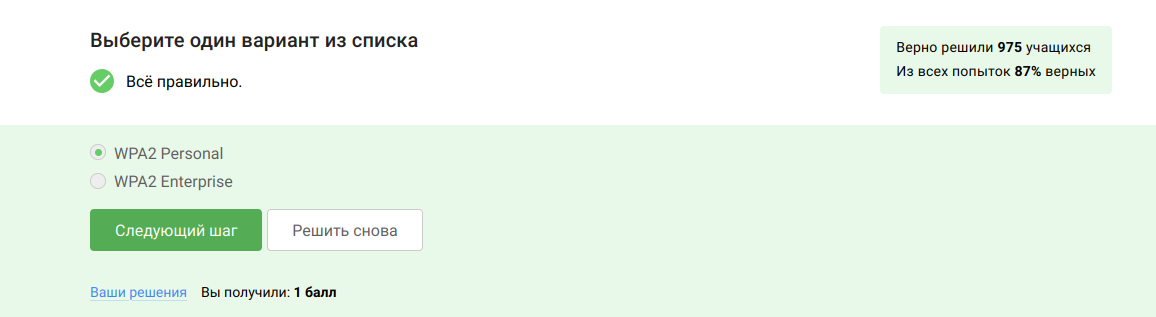


Рис. 22: Вопрос 2.4.5

# 4 Блок 2

# 5 Цель работы

Выполнить контрольные задания второго блока “Защита ПК/телефона” внешнего курса “Основы кибербезопасности”.

# 6 Выполнение заданий блока “Основы Кибербезопасности”

## 6.1 Шифрование диска

Шифровать нужно не только жесткий диск, но и загрузочный сектор диска. Ответ-можно (рис. 23).

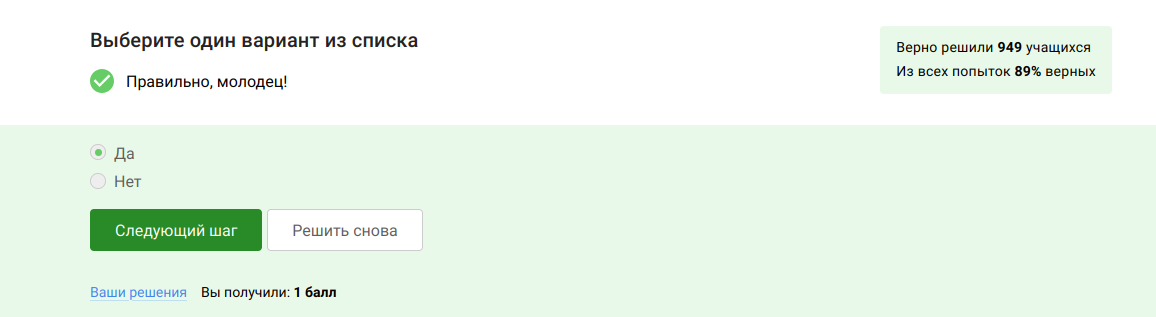


Рис. 23: Вопрос 3.1.1

Шифрование диска основано на симметричном шифровании (рис. 24).

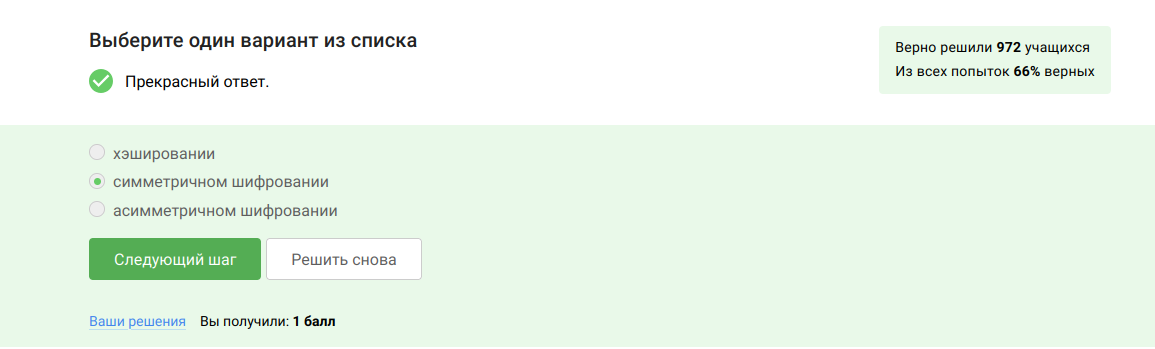


Рис. 24: Вопрос 3.1.2

Популярные ОС имеют встроенные инструменты для шифрования дисков: Windows (Bitlocker), Linux (LUKS), MacOS (FileVault). Также доступны бесплатные опенсорсные альтернативы, такие как Veracrypt и PGPDisk. (рис. 25).

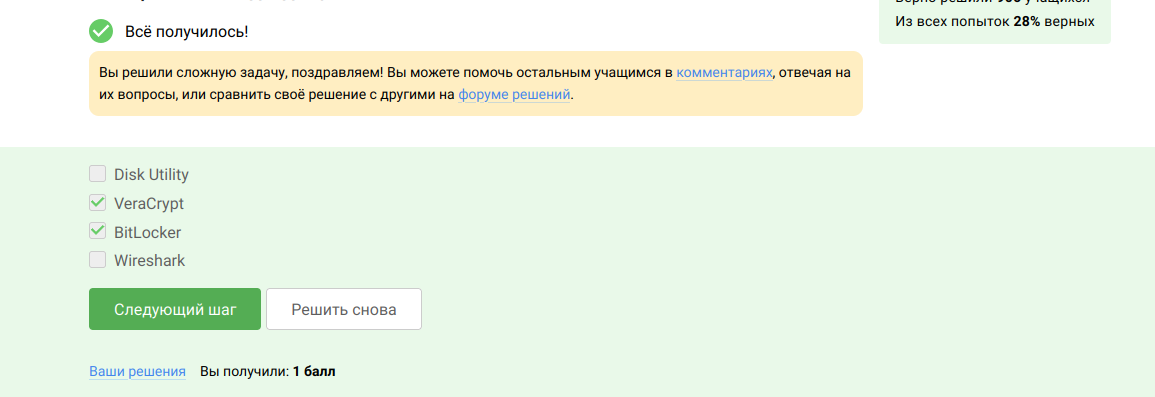


Рис. 25: Вопрос 3.1.3

## 6.2 Пароли

Стойкий пароль содержит цифры стройчные и заглавные буквы и специальные символы. Это усложняет перебор пароля (рис. 26).

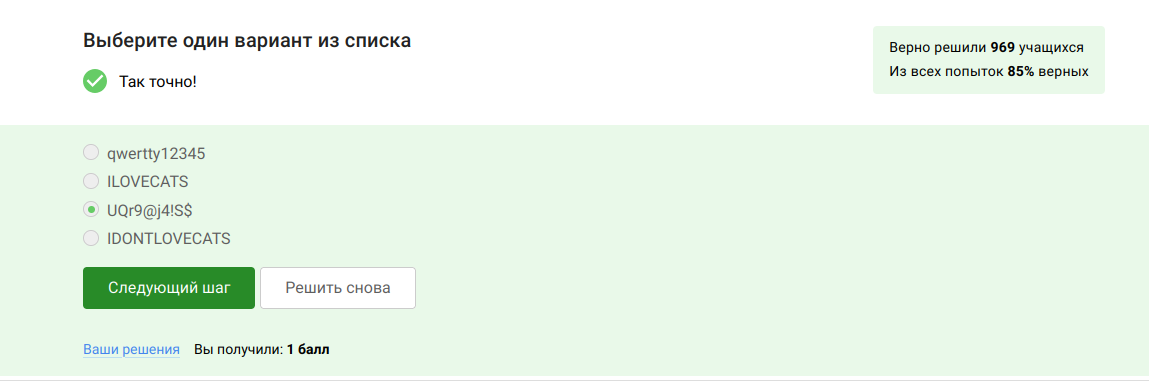


Рис. 26: Вопрос 3.2.1

Безопасно хранить пароли нужно только в месенджерах (рис. 27).

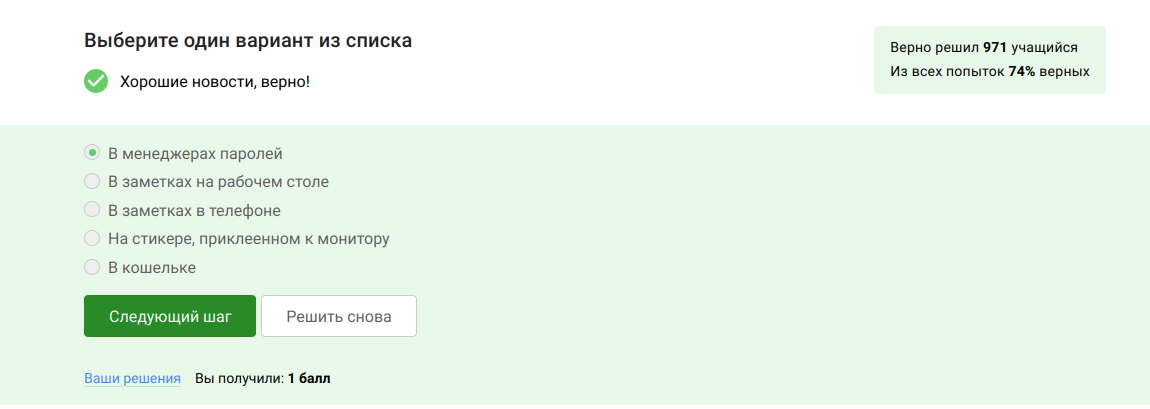


Рис. 27: Вопрос 3.2.2

Капча - тест для определения, кто общается с веб-сервисом, человек или бот(рис. 28).

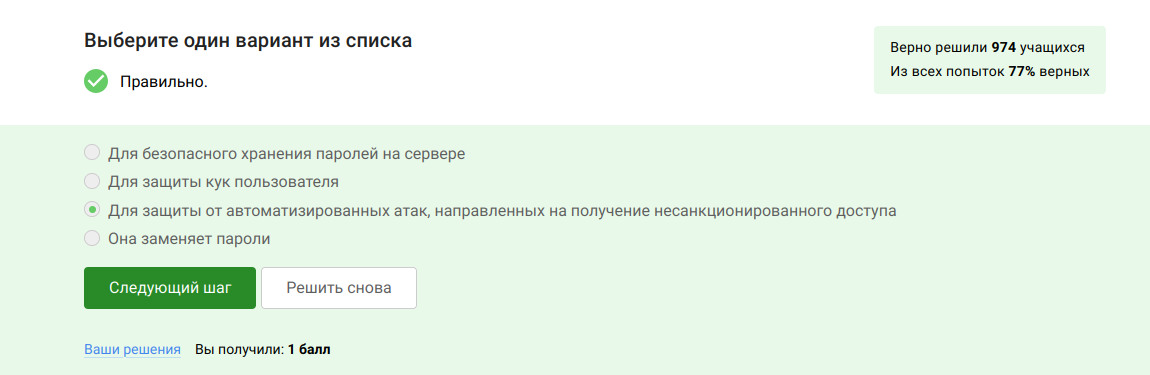


Рис. 28: Вопрос 3.2.3

В целях безопасности пароли хранят не в открвтом виде, а в виде хешей (рис. 29).

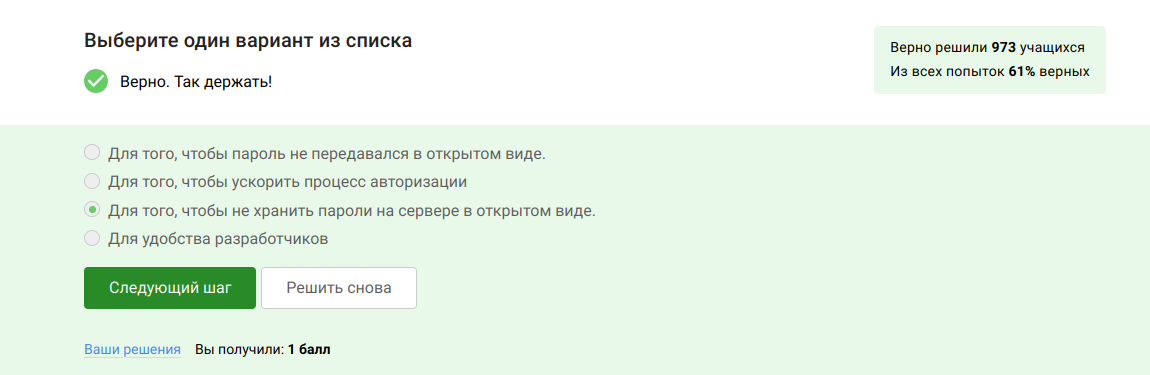


Рис. 29: Вопрос 3.2.4

Соль - это метод защиты слабых паролей. Сервер добавляет соль к паролю пользователя. Это делает взлом слабых паролей сложнее (рис. 30).

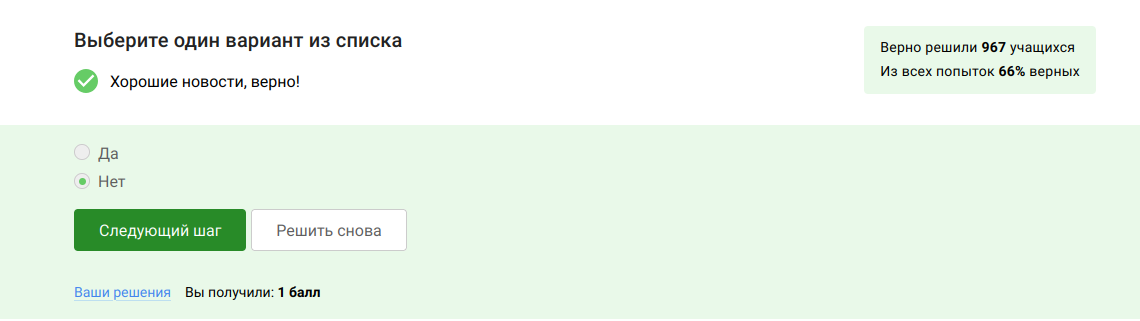


Рис. 30: Вопрос 3.2.5

Для безопасности нужно использовать длинные, сложные пароли, регулярно обновлять и хранить пароли в месенджерах паролей. (рис. 31).

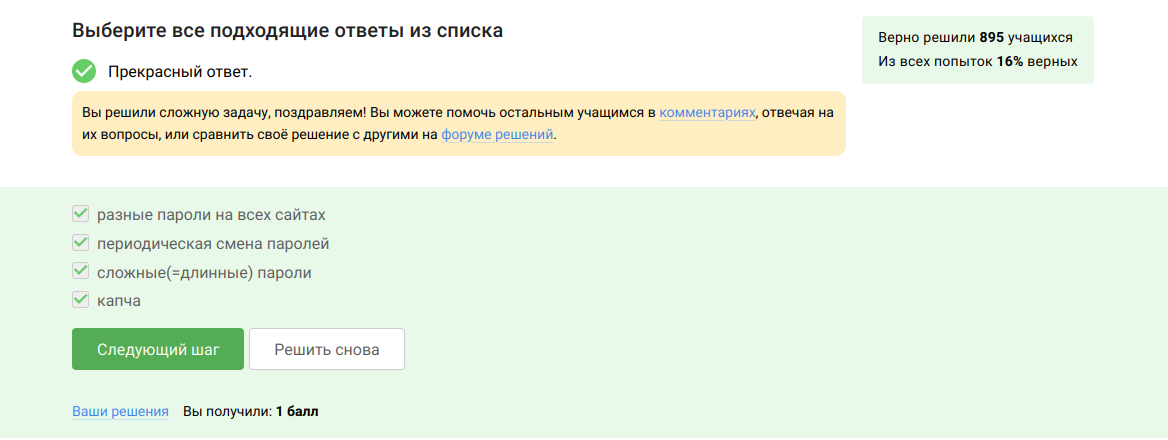


Рис. 31: Вопрос 3.2.6

## 6.3 Фишинг

Пример фишинга - эта маскировка под известные веб-сайты только с другим доменным именем (рис. 32).

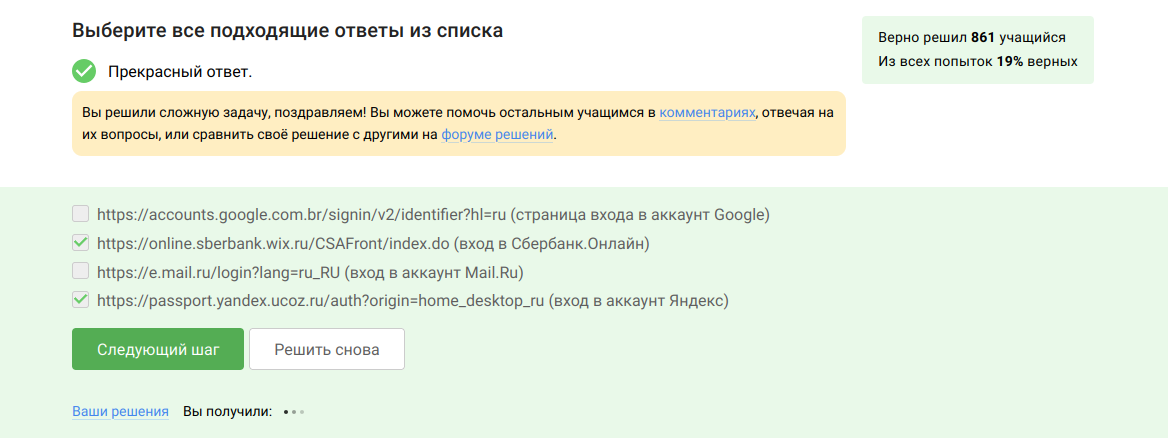


Рис. 32: Вопрос 3.3.1

Может фишинговое письмо прийти и от знакомого(рис. 33).

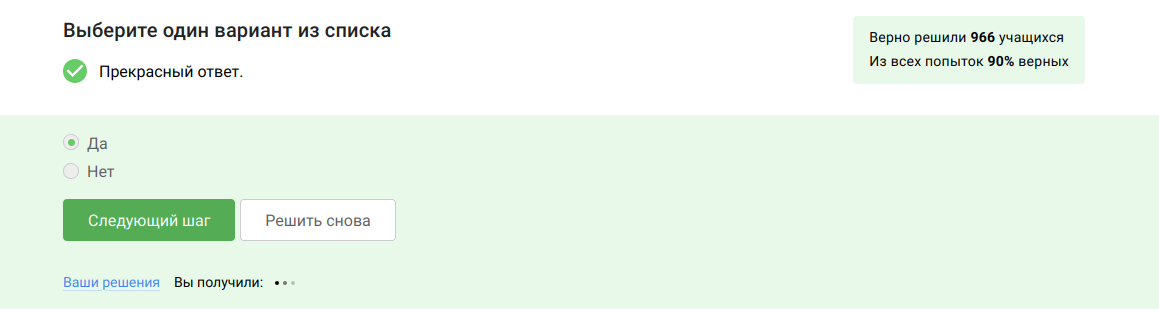


Рис. 33: Вопрос 3.3.2

## 6.4 Вирусы.

Спуфинг - это подмена адреса отправителя в имейлах (рис. 34).

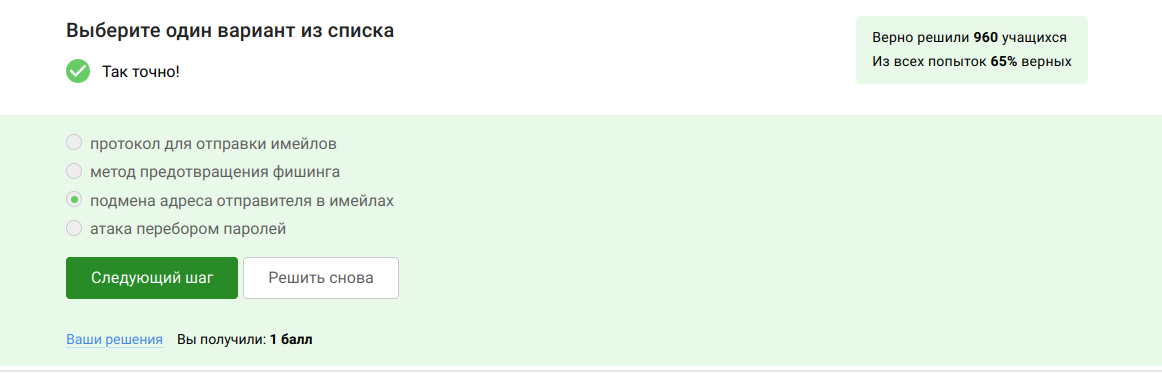


Рис. 34: Вопрос 3.4.1

Троян маскируется под обыкновенную безобидную программу, при запуске которой вирус легко проникает в ваш компьютер и поражает его(рис. 35).

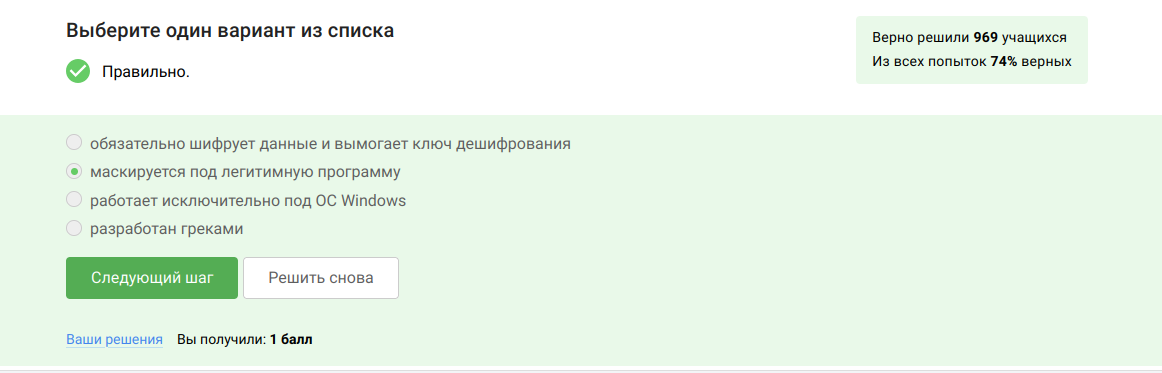


Рис. 35: Вопрос 3.4.2

## 6.5 Безопасность мессенджеров

При генерации первого сообщения отправителем формируется ключ шифрования (рис. 36).

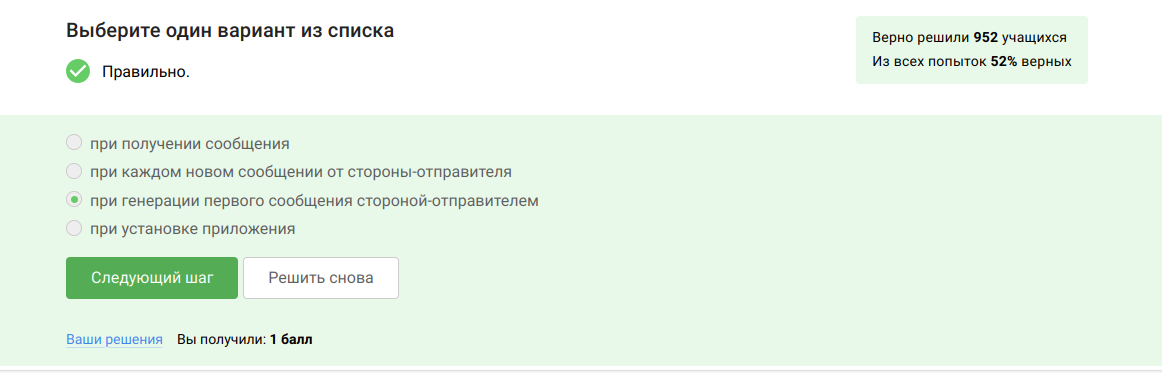


Рис. 36: Вопрос 3.5.1

Сквозное шифрование позволяет передавать сообщения между пользователями (Алиса и Боб) так, что сервер знает только адресата, но не может прочитать содержимое. Алиса шифрует сообщение, сервер передает шифрованный текст Бобу, а Боб его расшифровывает. Сервер не имеет доступа к ключам или открытому тексту сообщения. (рис. 37).

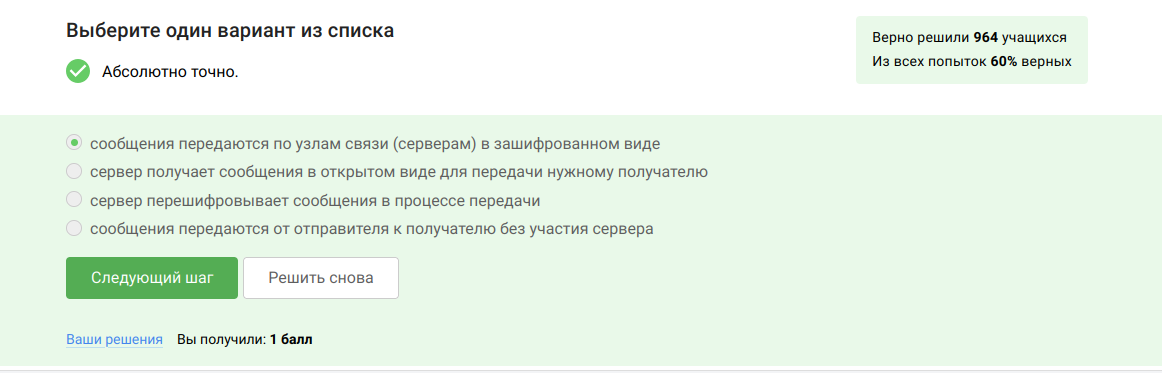


Рис. 37: Вопрос 3.5.1

# 7 Выводы

В результате я сделал второй блок курса “Основы кибербезопасности”. Узнал правила составления и хранения паролей, понял много нового о вирусах и мерах безопасности против них.

# 8 Блок 3

# 9 Цель работы

Выполнить контрольные задания третьего блока “Криптография на практи” внешнего курса “Основы кибербезопасности”.

# 10 Выполнение заданий блока “Основы Кибербезопасности”

## 10.1 Введение в криптографию

В асимметричной криптографии у каждой из старон есть пара ключей: открытый и секретный ключ (рис. 38).

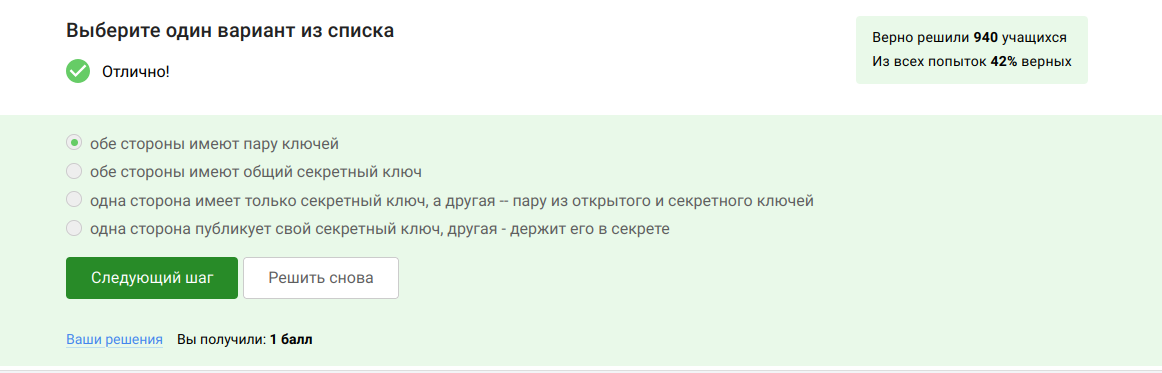


Рис. 38: Вопрос 4.1.1

Криптографическая хэш-функция обладает важным свойством стойкости к коллизиям, что означает, что крайне сложно найти два разных входа, которые дают одинаковый хэш. Она принимает произвольный объем данных и выдает фиксированную строку заданной длины (например, n). Обычно функция сжимает данные, преобразуя большой набор информации в небольшое значение. (рис. 39).

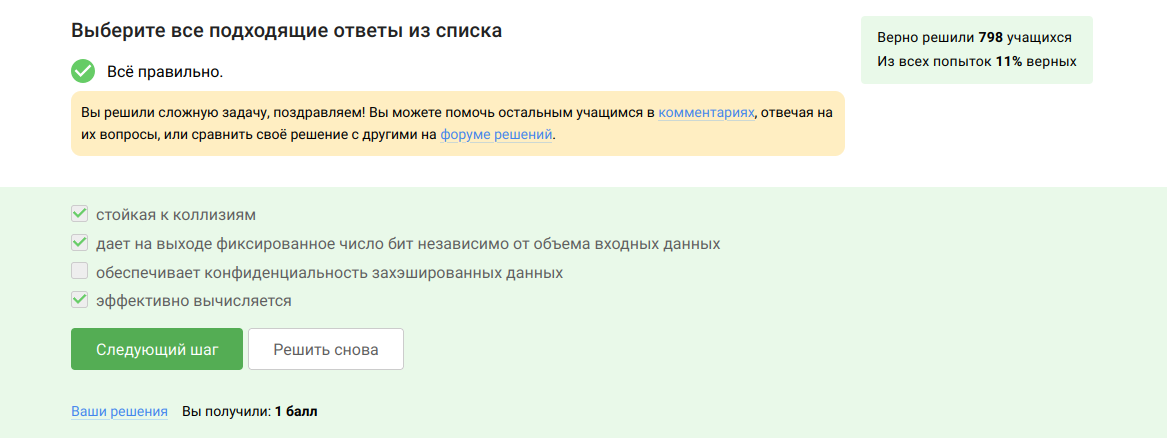


Рис. 39: Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. 40).

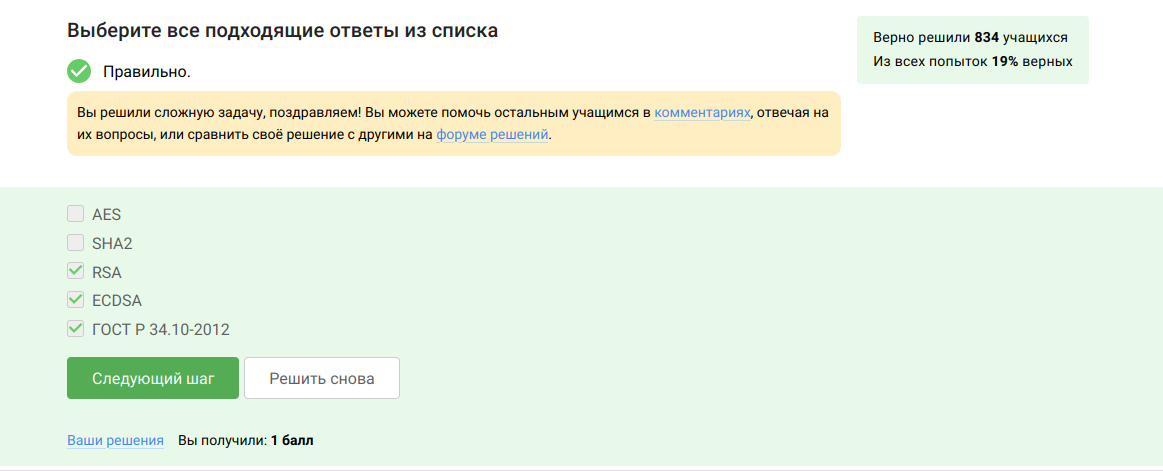


Рис. 40: Вопрос 4.1.3

Код аутентификации сообщения (MAC) относится к симметричным примитивам, поскольку для его генерации и проверки используется общий секретный ключ, известный только отправителю и получателю, что обеспечивает целостность и аутентичность данных.(рис. 41).

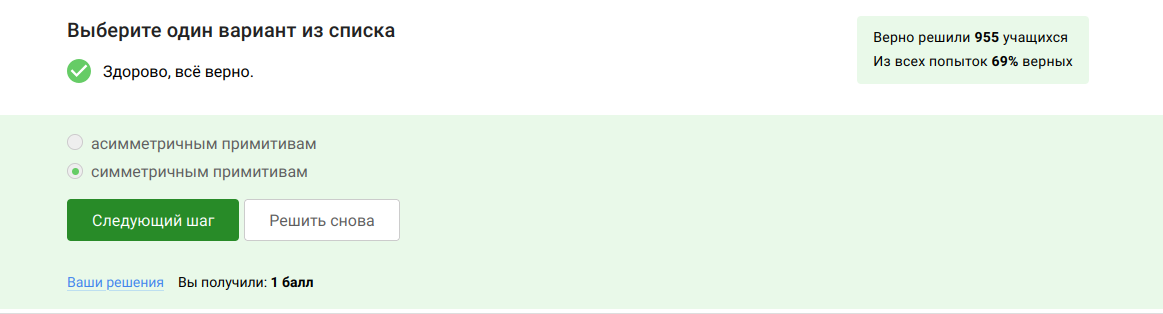


Рис. 41: Вопрос 4.1.4

Чтобы ответить на данный вопрос использую определение Диффи-Хэллмана (рис. 42).

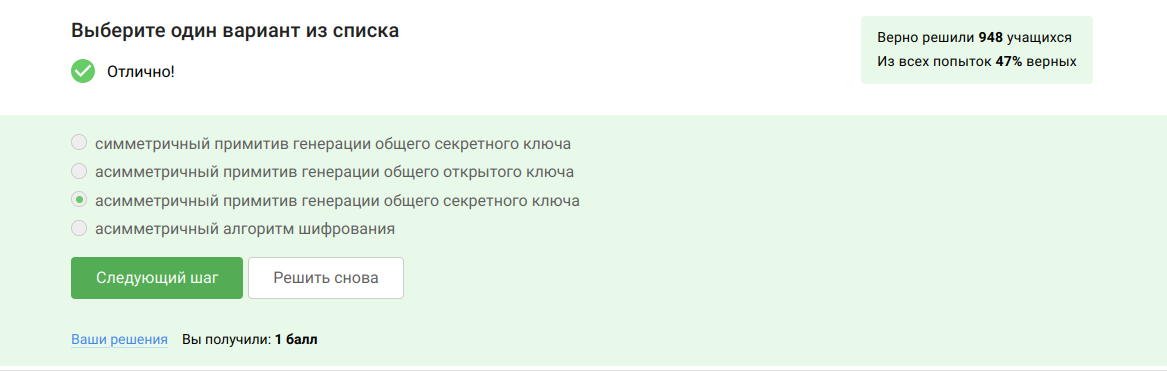


Рис. 42: Вопрос 4.1.5

## 10.2 Цифровая подпись

По определению цифровой подписи протокол ЭЦП относиться к протоколам с публичным ключом (рис. 43).

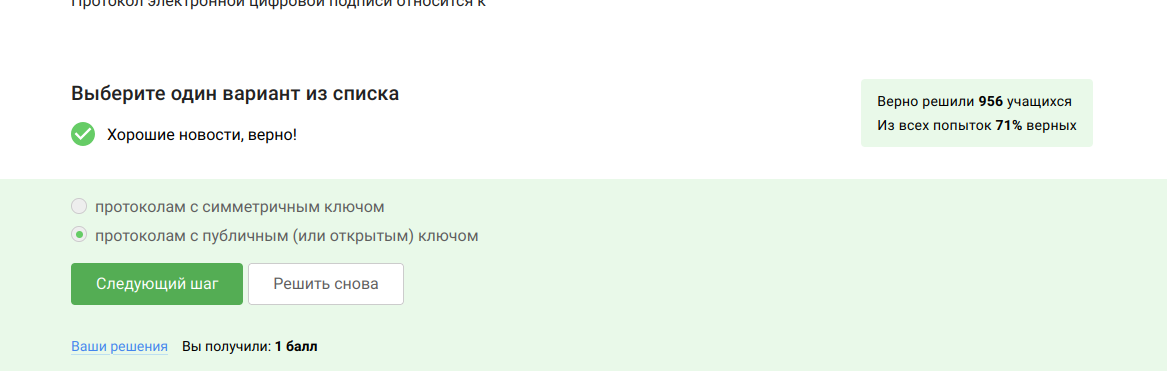


Рис. 43: Вопрос 4.2.1

Каждая машина процедуру верификации, которая берет на вход само обновление, подпись и открытый ключ разработчика (рис. 44).

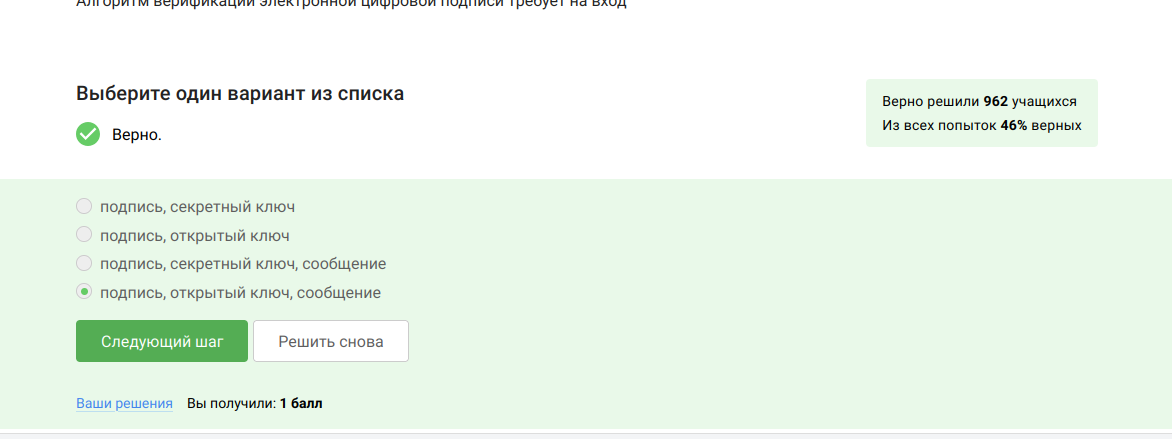


Рис. 44: Вопрос 4.2.2

Цифровая подпись обеспечивает три ключевых функции:

1. Целостность сообщения — изменения в сообщении приводят к некорректной проверке подписи.
2. Аутентификация — позволяет установить, что подпись принадлежит конкретному владельцу.
3. Неотказ от авторства — подписавший не может отказаться от своей подписи.

Однако, если секретный ключ украден, безопасность подписи подрывается, и она не обеспечивает конфиденциальности.(рис. 45).

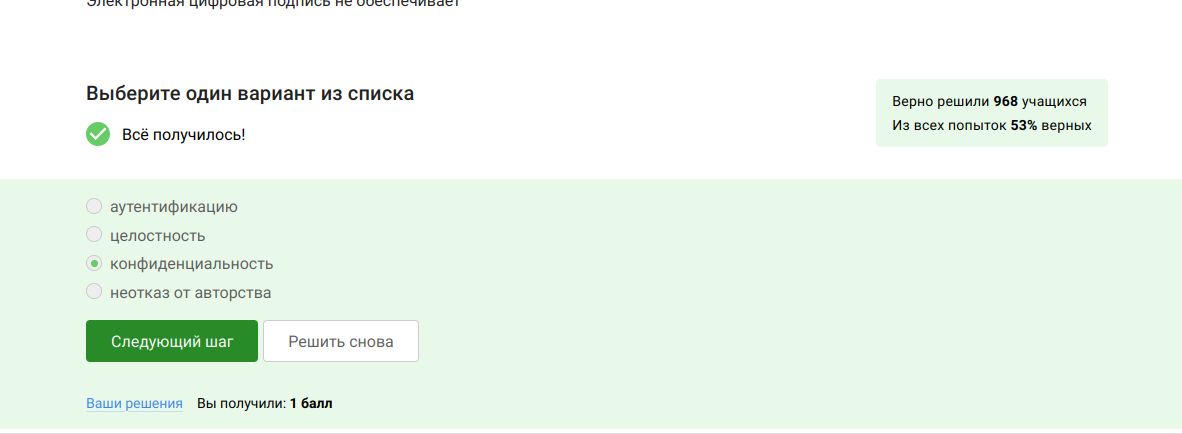


Рис. 45: Вопрос 4.2.3

Усиленная квалифицированная подпись (УКЭП) имеет юридическую силу и равнозначна рукописной подписи. Для её получения необходимо обратиться в аккредитованный сертификационный центр с паспортом и другими данными. (рис. 46).

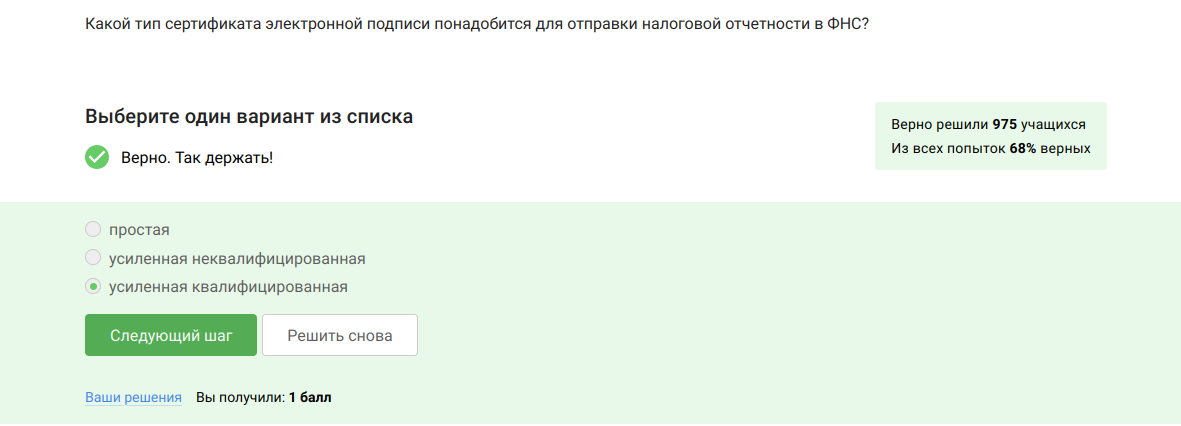


Рис. 46: Вопрос 4.2.4

Сертификат подписывается с помощью электронной подписи уже доверенной стороной, удостоверяющим центром. (рис. 47).

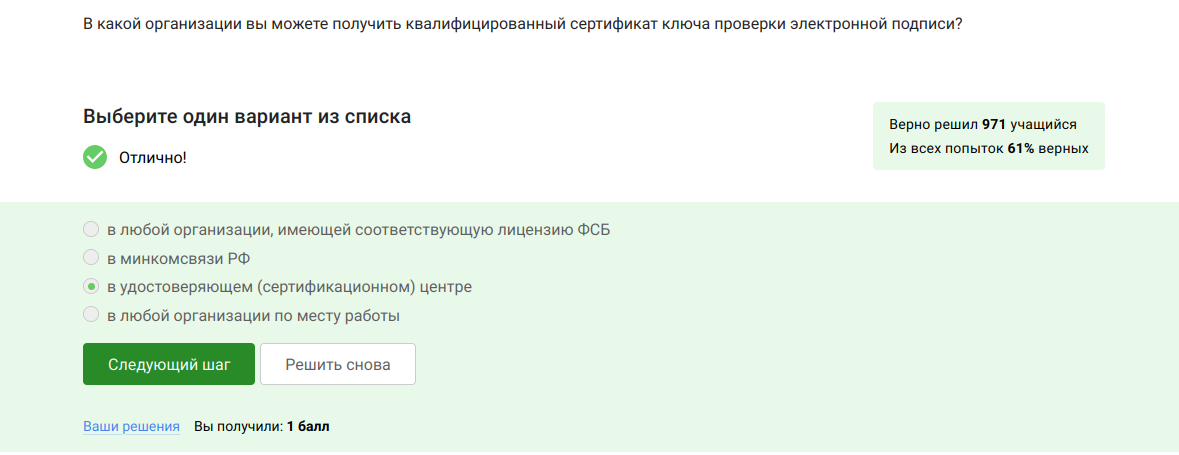


Рис. 47: Вопрос 4.2.5

## 10.3 Электронные платежи

На данный момент существуют такие платежные системы, как: Visa, MasterCard, МИР (рис. 48).

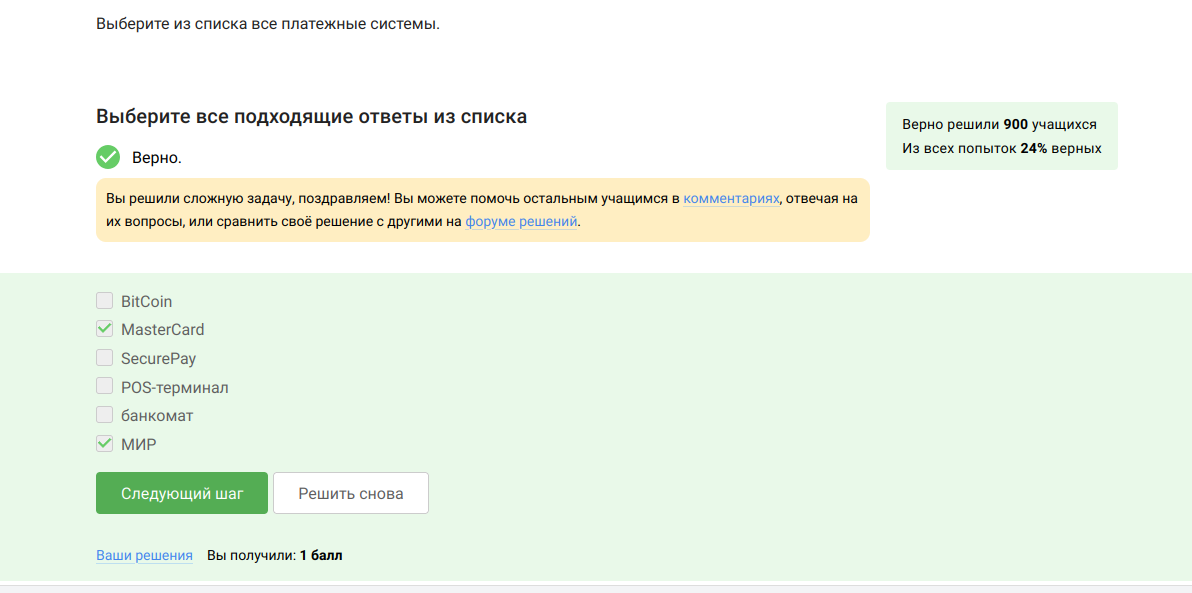


Рис. 48: Вопрос 4.3.1

Основные категории вещей, которые мы можем использовать для доказательства своей идентичности:

1. Знание: Это что-то, что я знаю, например, пароль, PIN-код или секретный код для онлайн-платежей.
2. Владение: В онлайн-платежах используется второй фактор — это то, чем я владею, например, телефон, на который приходит код для подтверждения.
3. Свойства: Биометрические данные, такие как отпечаток пальца или сетчатка глаза, служат третьим фактором аутентификации.
4. Локация: Четвертый фактор аутентификации — это место, откуда осуществляется доступ, что также может быть учтено при проверке идентичности. (рис. 49).

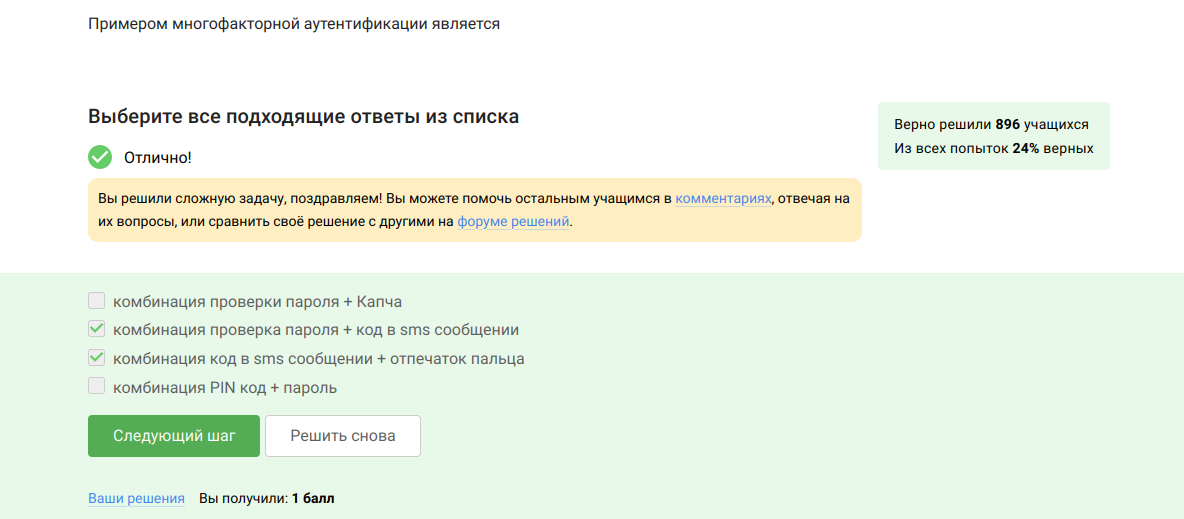


Рис. 49: Вопрос 4.3.2

При онлайн платежах используется многофакторная аутентификация банком-эмитентом (выпустившим карту), чтобы удостовериться, что транзакцию совершает именно владелец карты или счета, а не злоумышленник(рис. 50).

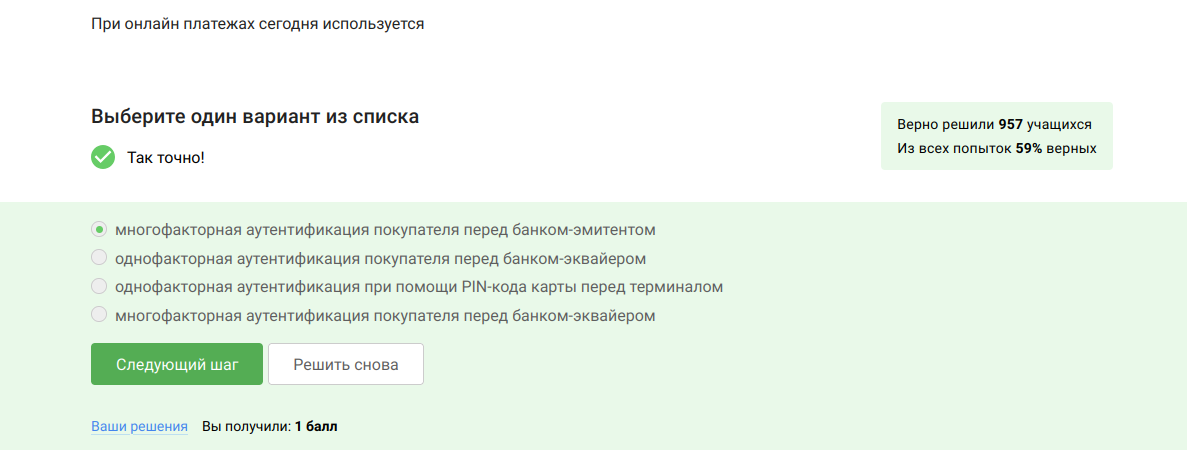


Рис. 50: Вопрос 4.3.3

## 10.4 Блокчейн

Proof-of-Work (PoW) — это способ, который используется в блокчейне для подтверждения транзакций и создания новых блоков. В этом процессе майнеры (люди, которые занимаются добычей криптовалюты) соревнуются друг с другом за завершение транзакций в сети и за вознаграждение

Когда люди отправляют друг другу цифровые деньги, эти транзакции собираются в блоки и добавляются в общую базу данных, называемую блокчейном. Чтобы сделать сеть безопасной и защитить её от мошенничества, PoW требует много вычислительных ресурсов. Это значит, что для успешного участия в процессе нужно много мощных компьютеров.(рис. 51).

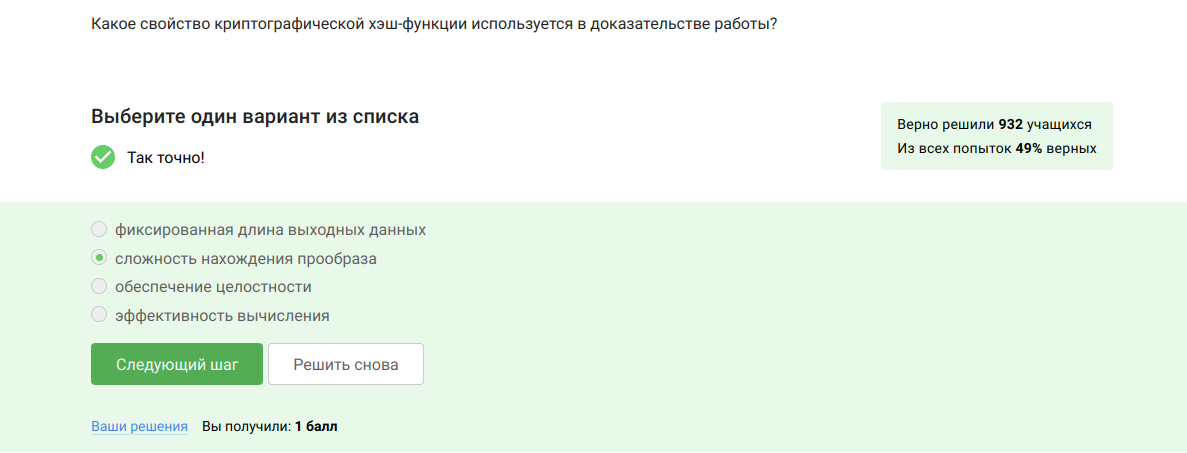


Рис. 51: Вопрос 4.4.1

В основе любого блокчейна, включая биткоин, лежит консенсус — публичная структура данных (ledger), содержащая историю всех транзакций. Консенсус обеспечивает четыре ключевых свойства:

1. Постоянство: Добавленные данные не могут быть удалены.
2. Согласованность: Все участники видят и согласны с одними и теми же данными, за исключением последних изменений.
3. Живучесть: Возможность добавления новых транзакций в любое время.
4. Открытость: Любой желающий может стать участником блокчейна.

Эти свойства обеспечивают надежность и безопасность системы. (рис. 52).

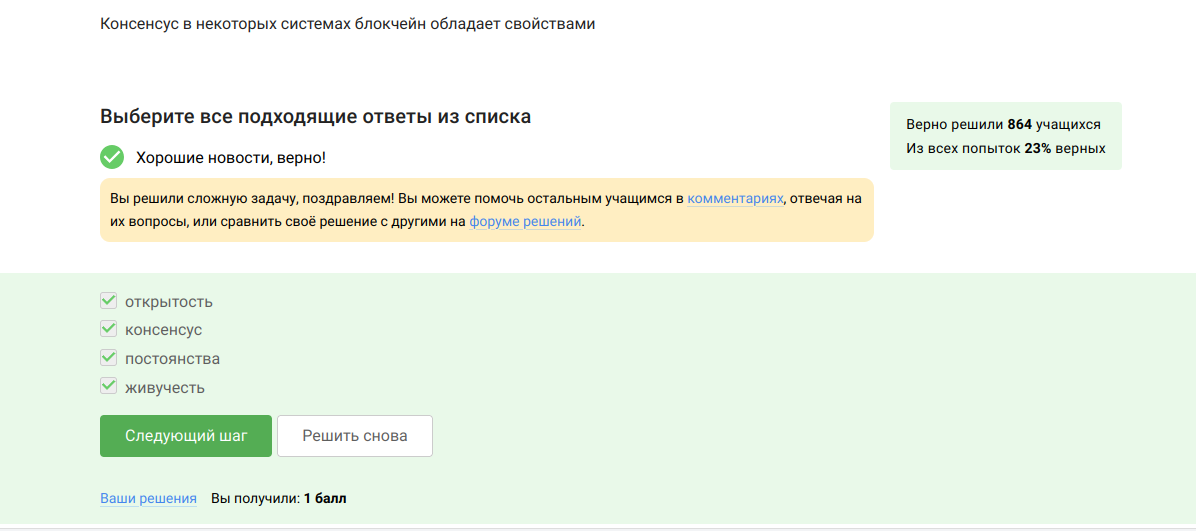


Рис. 52: Вопрос 4.4.2

В блокчейне у каждого из трех участников есть секретный ключ, который они используют для подтверждения транзакций. Этот секретный ключ позволяет создавать цифровую подпись, которая служит доказательством того, что транзакция была инициирована конкретным участником. Цифровая подпись основана на паре ключей — секретном и открытом. Секретный ключ используется для подписания транзакции, а открытый ключ позволяет другим участникам проверить подлинность этой подписи. Таким образом, цифровая подпись обеспечивает безопасность и аутентичность транзакций в блокчейне. (рис. 53).

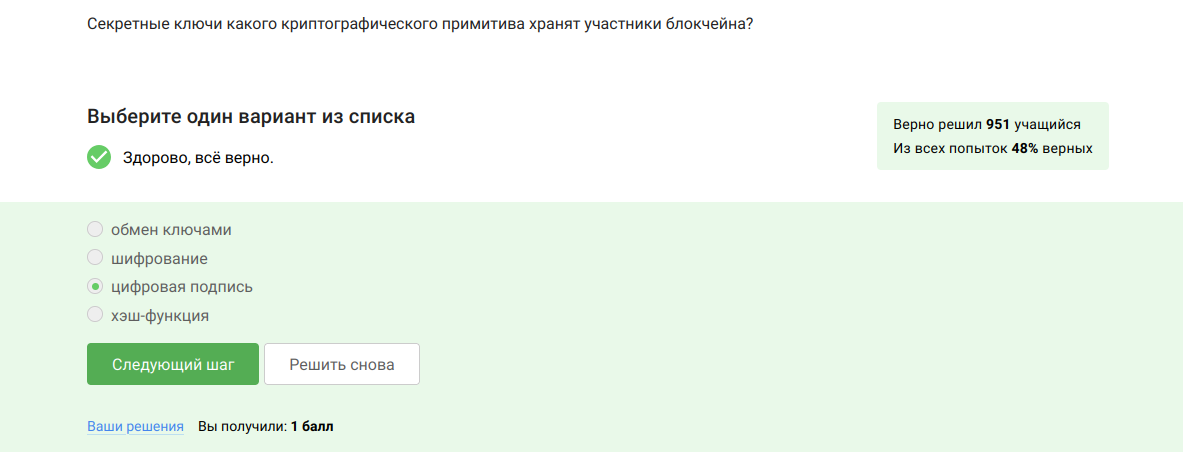


Рис. 53: Вопрос 4.4.3

# 11 Выводы

В результате 3 этапа я узнал много нового о криптографии, цифровых подписях и технологиях блокчейна. Выяснил как обеспечивается безопасность транзакций.

# 12 Выводы

В результате выполнения блока “Безопасность в сети” я узнал как работают сетевые протоколы, куки-файлы, сети вайфай и для чего нужен браузер Tor.