Основы кибербезопастности

Прохождение курса

Астраханцева А. А.

Содержание

# 1 Цель работы

Прохождение курса “Основы кибербезопастности” и получение сертификата.

# 2 Выполнение

## 2.1 Безопасность в сети

### 2.1.1 Как работает интернет: базовые сетевые протоколы

Протокол прикладного уровня в данном списке — это HTTPS.

UDP, TCP и IP являются протоколами более низких уровней. UDP и TCP относятся к транспортному уровню, а IP — к сетевому уровню (рис. 1).

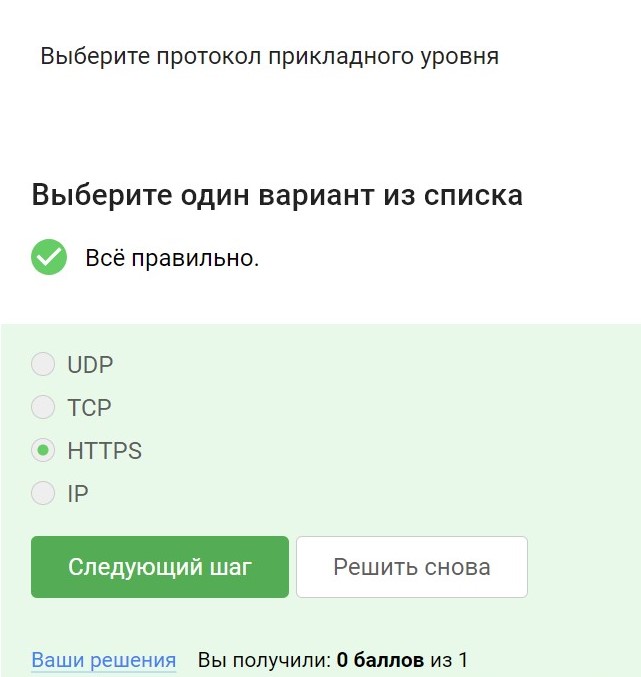


Рис. 1: Как работает интернет. Вопрос №1

Протокол TCP работает на транспортном уровне (рис. 2).

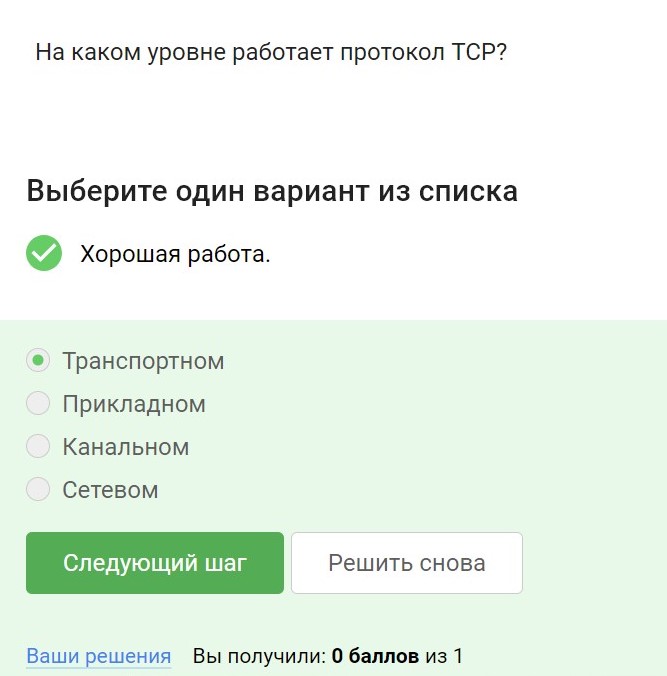


Рис. 2: Как работает интернет. Вопрос №2

Корректные адреса IPv4 в данном списке: 90.11.90.22 и 25.198.0.15. Варианты 421.0.15.19 и 43.12.256.7 - некорректные, так как значения в каждом октете могут быть от 0 до 255 (рис. 3).

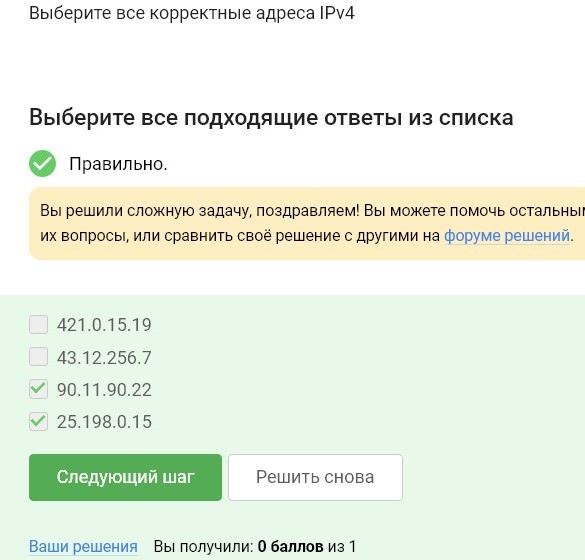


Рис. 3: Как работает интернет. Вопрос №3

DNS (Domain Name System) сервер переводит понятные для человека доменные имена (например, www.example.com) в IP адреса, которые используются устройствами для взаимодействия в сети. Это позволяет пользователям легко запоминать и вводить веб-адреса, вместо использования числовых IP адресов (рис. 4).

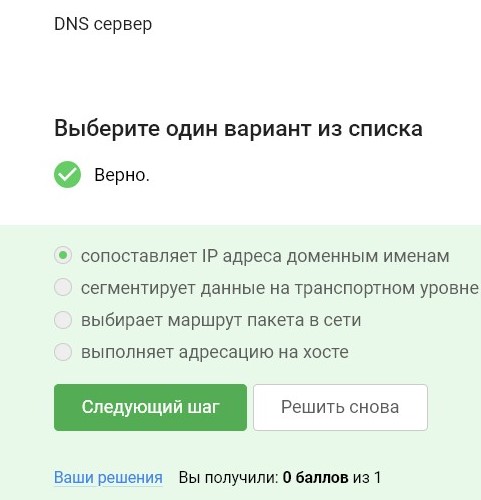


Рис. 4: Как работает интернет. Вопрос №4

Модель TCP/IP состоит из четырех уровней. На верхнем уровне находится прикладной уровень, который взаимодействует с пользовательскими приложениями. Ниже него идет транспортный уровень, обеспечивающий передачу данных между хостами. Следующим идет сетевой уровень, отвечающий за маршрутизацию пакетов. На нижнем уровне находится канальный уровень, который управляет физической передачей данных через сеть. (рис. 5).

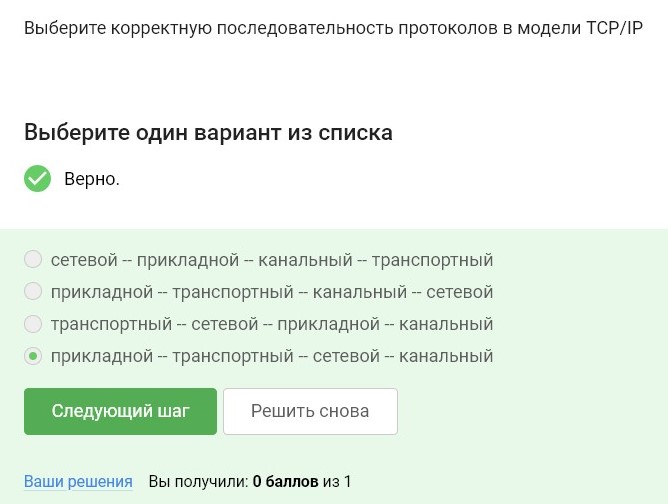


Рис. 5: Как работает интернет. Вопрос №5

Протокол HTTP (HyperText Transfer Protocol) передает данные в незашифрованном виде. Это означает, что данные, передаваемые между клиентом и сервером, могут быть перехвачены и прочитаны третьими сторонами. Для безопасной передачи данных используется протокол HTTPS, который шифрует данные с помощью SSL/TLS (рис. 6).

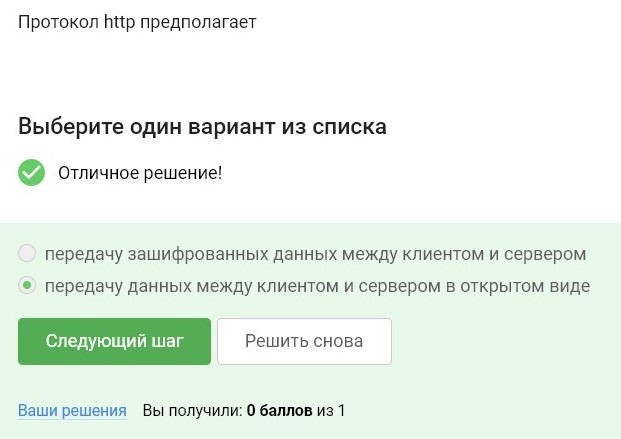


Рис. 6: Как работает интернет. Вопрос №6

Протокол HTTPS (HyperText Transfer Protocol Secure) включает в себя две основные фазы. Первая фаза — это “рукопожатие” (handshake), в ходе которой клиент и сервер устанавливают защищенное соединение, согласовывают параметры шифрования и аутентифицируют сервер (и, возможно, клиента). Вторая фаза — это передача данных, во время которой данные передаются в зашифрованном виде, обеспечивая их конфиденциальность и целостность (рис. 7).

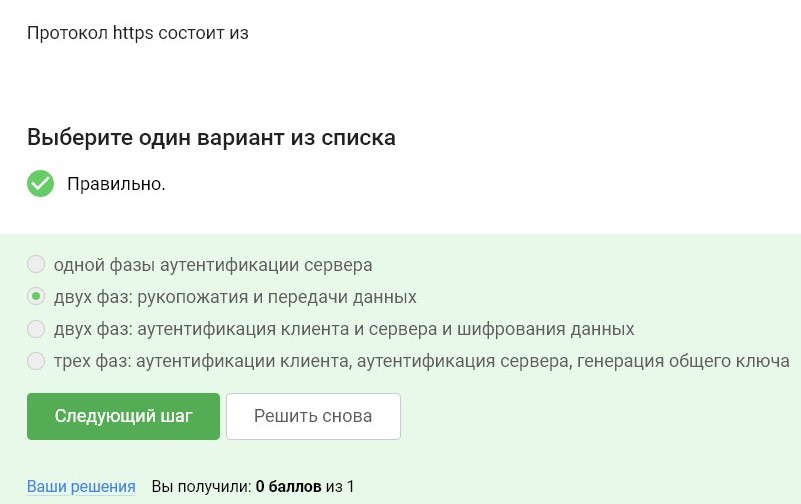


Рис. 7: Как работает интернет. Вопрос №7

Во время установления защищенного соединения по протоколу TLS, клиент и сервер договариваются о версии протокола, которую они будут использовать. Этот процесс происходит в ходе “рукопожатия” (TLS handshake), где обе стороны сообщают свои поддерживаемые версии и выбирают наивысшую общую версию, чтобы обеспечить совместимость и безопасность соединения (рис. 8).

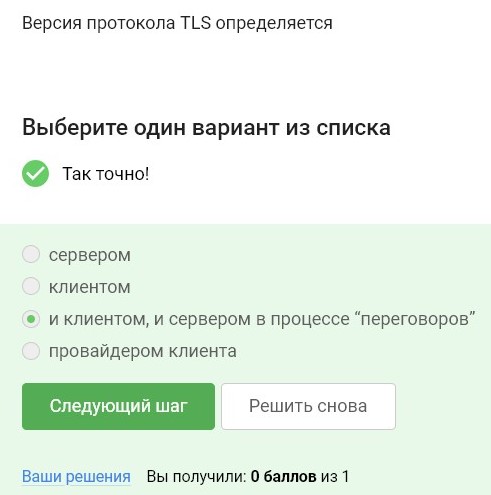


Рис. 8: Как работает интернет. Вопрос №8

Во время “рукопожатия” (TLS handshake), клиент и сервер согласовывают параметры для установки безопасного соединения, такие как выбор версии протокола, выбор алгоритмов шифрования и аутентификации, а также происходит аутентификация (как минимум одной из сторон) и формирование общего секретного ключа. Однако фаза “рукопожатия” не включает в себя шифрование данных, так как шифрование начинается только после успешного завершения этой фазы и установления защищенного соединения (рис. 9).

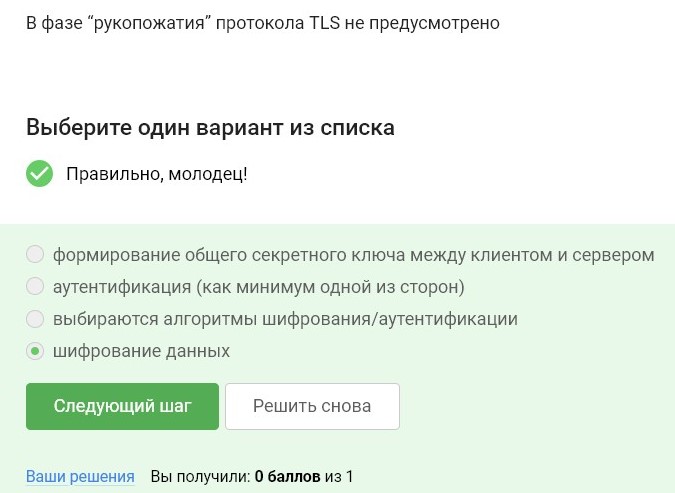


Рис. 9: Как работает интернет. Вопрос №9

### 2.1.2 Персонализация сети

Куки могут хранить идентификатор пользователя, что позволяет веб-сайтам отслеживать пользователя и его предпочтения, и идентификатор сеанса, который помогает серверу отслеживать состояние сеанса для конкретного пользователя.

Пароль пользователя и IP-адрес обычно не хранятся в куки из соображений безопасности. Вместо этого пароль обычно хранится в зашифрованной форме на сервере, а IP-адрес может использоваться для идентификации пользователя, но не хранится непосредственно в куках (рис. 10).

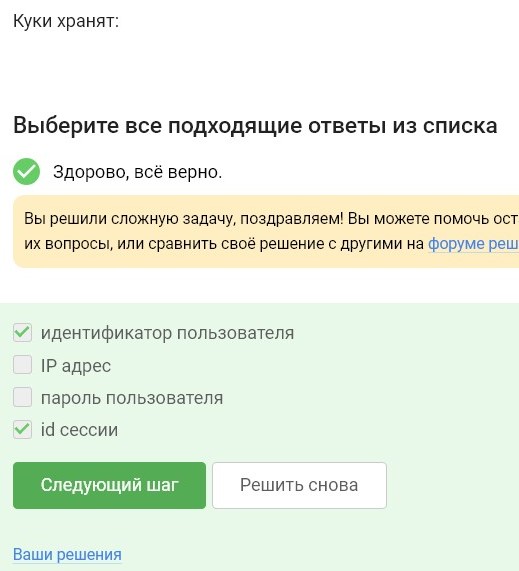


Рис. 10: Персонализация сети. Вопрос №1

Куки применяются для различных целей, включая аутентификацию пользователя, персонализацию веб-страниц, отслеживание информации о пользователе и сбор статистики посещаемости сайта. Однако они не прямо связаны с улучшением надежности соединения. Улучшение надежности соединения может быть достигнуто за счет других мер безопасности, таких как использование протоколов шифрования (например, HTTPS) (рис. 11).

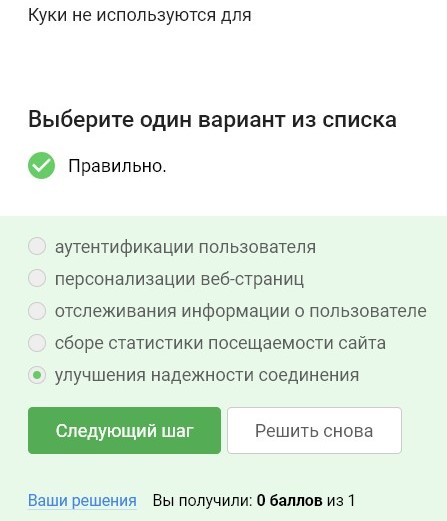


Рис. 11: Персонализация сети. Вопрос №2

Куки генерируются и отправляются сервером в ответ на запрос от клиента. Когда клиент отправляет запрос на сервер, сервер может включить в ответ заголовок Set-Cookie, чтобы установить куки на стороне клиента (рис. 12).

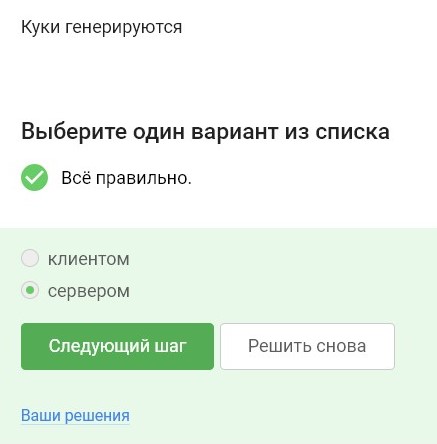


Рис. 12: Персонализация сети. Вопрос №3

Сессионные куки хранятся в браузере только на время активной сессии пользователя на веб-сайте. Как только пользователь закрывает окно браузера или завершает сеанс, сессионные куки обычно удаляются. (рис. 13).

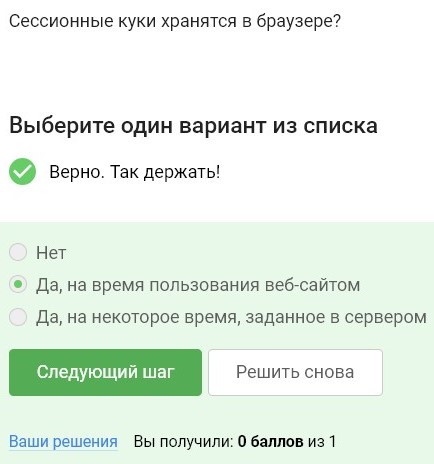


Рис. 13: Персонализация сети. Вопрос №4

### 2.1.3 Браузер TOR. Анонимизация

Луковая сеть TOR использует три промежуточных узла для обеспечения анонимности пользователей. Когда пользователь отправляет запрос на веб-сайт через TOR, его запрос проходит через три промежуточных узла, прежде чем достигнет конечного назначения (рис. 14).

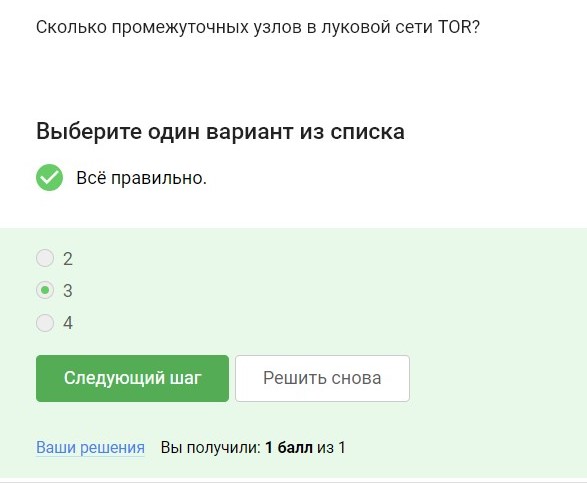


Рис. 14: Браузер TOR. Анонимизация. Вопрос №1

В луковой сети TOR IP-адрес получателя известен отправителю, так как он должен знать, куда отправлять данные. Также IP-адрес получателя известен выходному узлу, так как это последний узел в цепочке, который фактически отправляет запрос на сервер получателя (рис. 15).

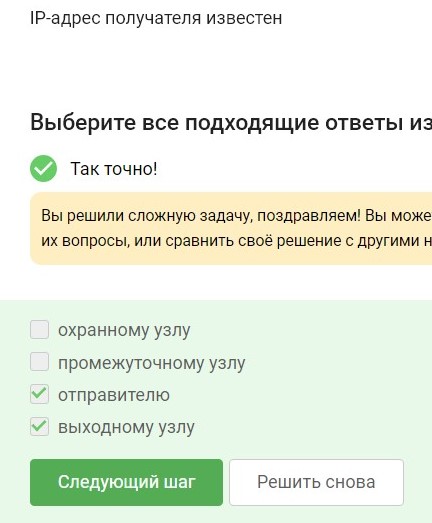


Рис. 15: Браузер TOR. Анонимизация. Вопрос №2

В луковой сети TOR общий секретный ключ генерируется между отправителем и каждым узлом в цепочке (охранным, промежуточным и выходным), так как каждый из узлов “снимает” один из слоев шифра (расшифровывает) (рис. 16).

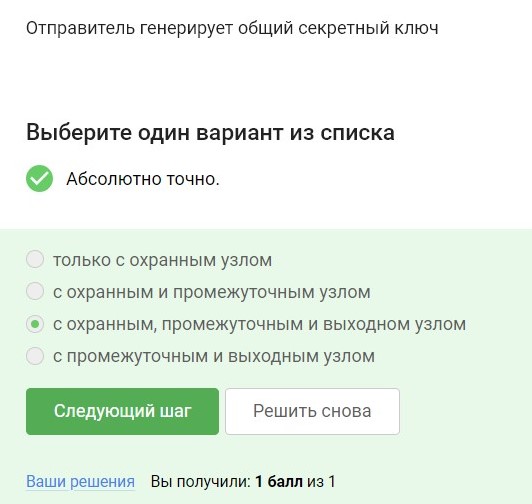


Рис. 16: Браузер TOR. Анонимизация. Вопрос №3

Нет, пользователь не обязан использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов. TOR используется для анонимного и безопасного доступа к ресурсам в сети (рис. 17).

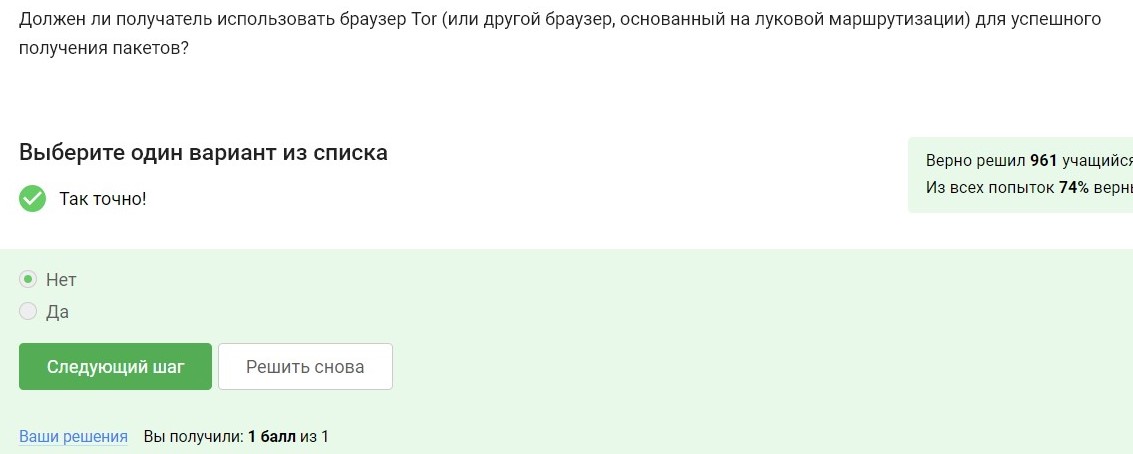


Рис. 17: Браузер TOR. Анонимизация. Вопрос №4

### 2.1.4 Беспроводные сети Wi-fi

Wi-Fi является стандартом беспроводной связи, который позволяет устройствам подключаться к сети и обмениваться данными через радиоволновой сигнал. Этот стандарт определяется в IEEE 802.11 и используется для создания беспроводных локальных сетей (WLAN) (рис. 18).

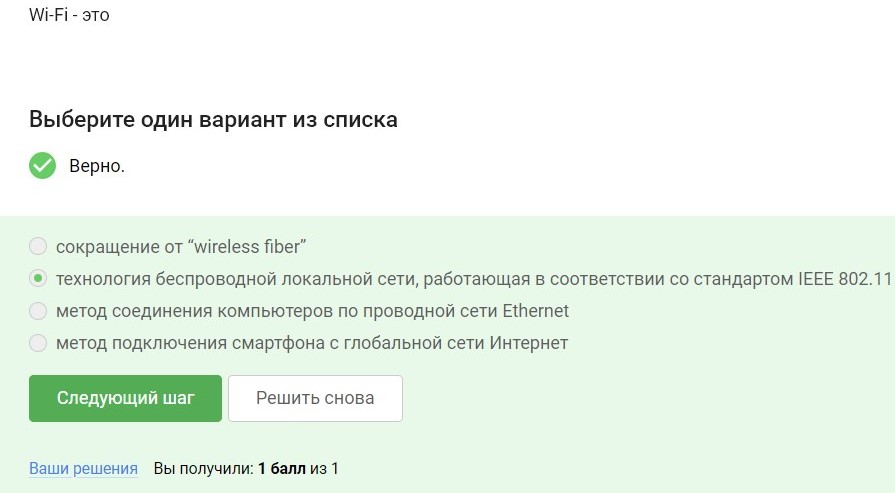


Рис. 18: Беспроводные сети Wi-fi. Вопрос №1

Протокол WiFi определяет способы доступа к беспроводной среде и форматирование данных для передачи через радиоканал. Это происходит на канальном уровне модели OSI, который отвечает за передачу данных по физической среде. (рис. 19).

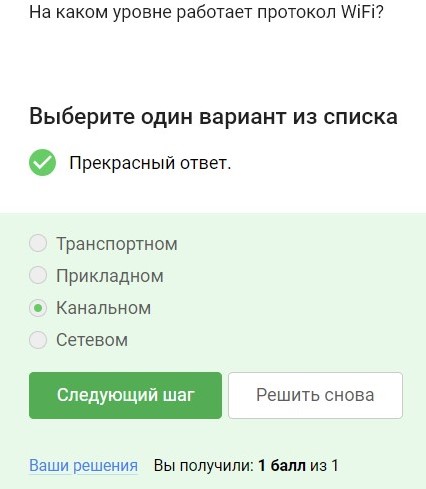


Рис. 19: Беспроводные сети Wi-fi. Вопрос №2

WEP (Wired Equivalent Privacy) был одним из первых методов шифрования, использованных в беспроводных сетях Wi-Fi. Он устарел, в частности, потому, что использовал малую длину ключа: так, например, он использовал длину ключа в 40 бит, это довольно мало на сегодняшний день, он может быть легко взломан (рис. 20).

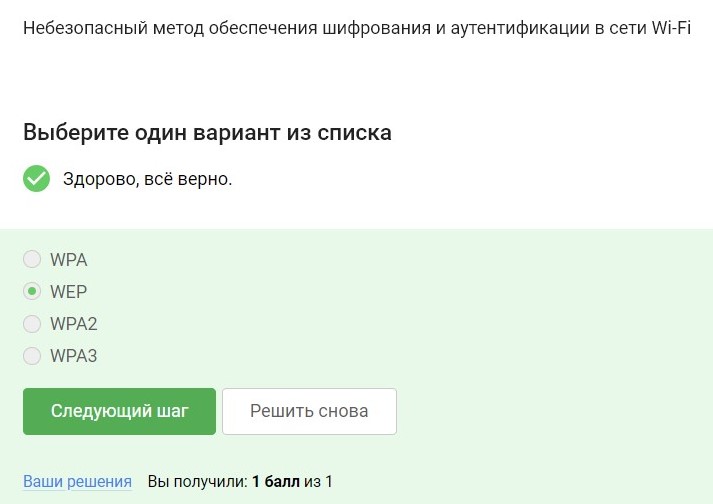


Рис. 20: Беспроводные сети Wi-fi. Вопрос №3

После успешной аутентификации устройств в сети Wi-Fi, данные, передаваемые между этими устройствами и роутером, могут передаваться в открытом виде. Тем не менее, если используется шифрование (например, WPA2 или WPA3), то данные передаются в зашифрованном виде после успешной аутентификации. (рис. 21).

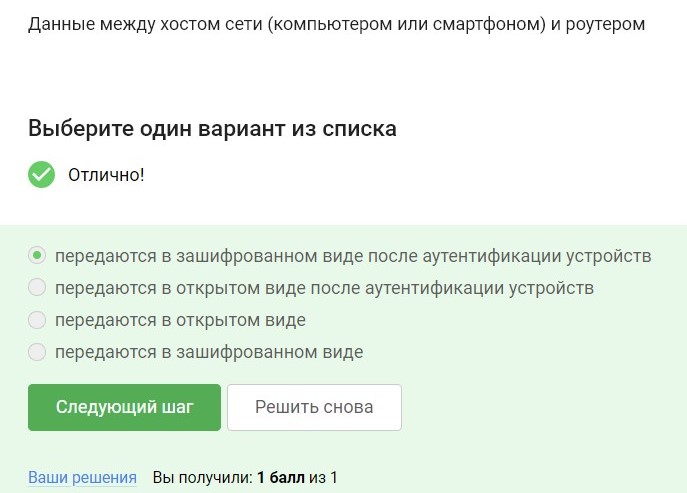


Рис. 21: Беспроводные сети Wi-fi. Вопрос №4

WPA Personal — это тип аутентификации по паролю, который часто применяется в домашних сетях или небольших корпоративных сетях. В случае использования этого метода, каждый пользователь подключается к сети, используя общий предварительно установленный пароль. В отличие от этого, WPA Enterprise — это более сложный метод аутентификации, при котором существует централизованная база данных всех пользователей. При подключении к сети WiFi, пользователь проверяется в этой базе данных, что обычно хранится на специальных серверах. Этот метод обеспечивает более высокий уровень безопасности, но, как правило, он не требуется для небольших домашних сетей (рис. 22).

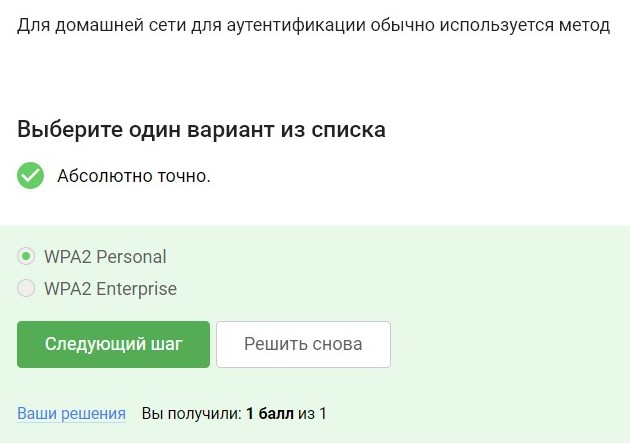


Рис. 22: Беспроводные сети Wi-fi. Вопрос №5

## 2.2 Защита ПК/телефона

### 2.2.1 Шифрование диска

Загрузочный сектор диска содержит информацию, необходимую для загрузки операционной системы при запуске компьютера. Этот сектор также может быть зашифрован, чтобы обеспечить дополнительный уровень безопасности и защиты данных на диске от несанкционированного доступа. (рис. 23).

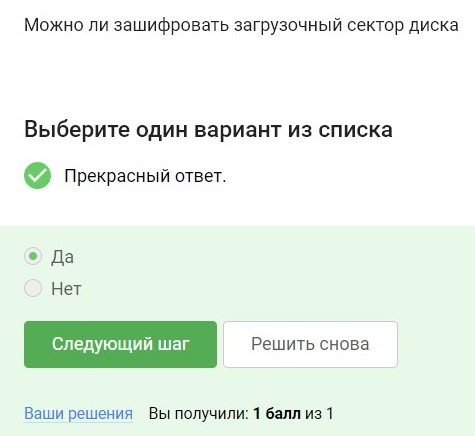


Рис. 23: Шифрование диска. Вопрос №1

В симметричном шифровании используется один и тот же ключ для шифрования и дешифрования данных. При шифровании диска такой ключ используется для зашифрования данных, а затем для их дешифрования при необходимости доступа к данным на диске (рис. 24).

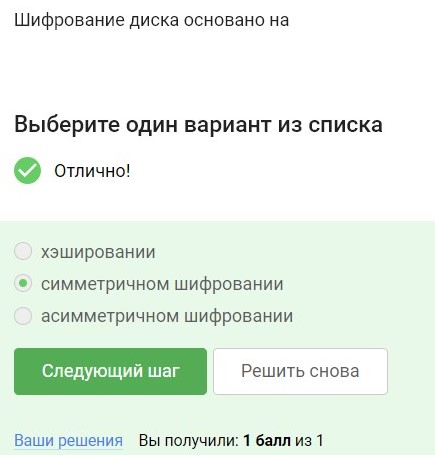


Рис. 24: Шифрование диска. Вопрос №2

Зашифровать жесткий диск с помощью следующих программ: BitLocker и VeraCrypt. Обе эти программы предоставляют возможность шифрования данных на жестком диске для обеспечения их безопасности и защиты от несанкционированного доступа.

Wireshark используется для анализа сетевого трафика, а Disk Utility (или Дисковая утилита) преимущественно для работы с дисками на операционных системах Mac OS (рис. 25).

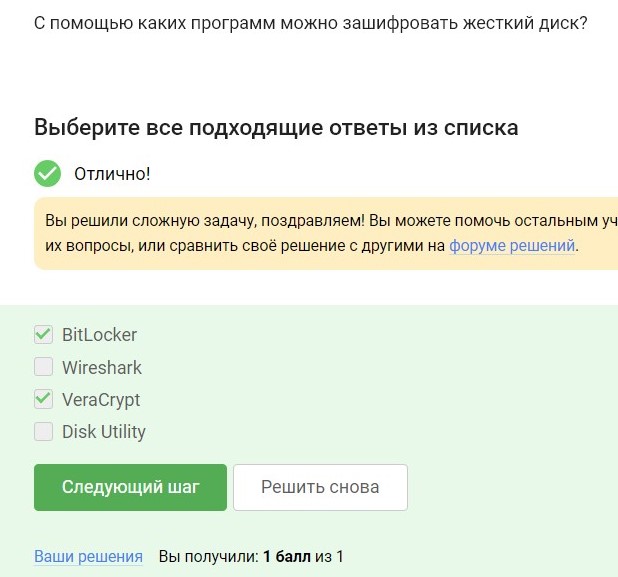


Рис. 25: Шифрование диска. Вопрос №3

### 2.2.2 Пароли

Стойкими можно считать пароли, которые включают в себя сложную комбинацию символов, такие как буквы в верхнем и нижнем регистрах, цифры и специальные символы, и имеют достаточную длину для предотвращения атак методом перебора (рис. 26).

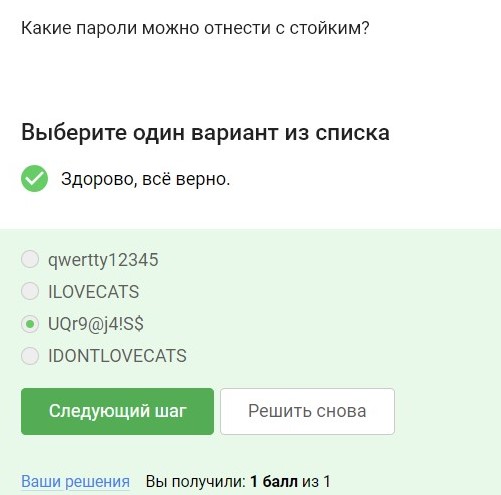


Рис. 26: Пароли. Вопрос №1

Менеджеры паролей представляют собой защищенное приложение, которое помогает хранить и организовывать пароли, обеспечивая их безопасность с помощью мощного шифрования и других мер безопасности. При использовании менеджера паролей пользователю необходимо помнить только один основной пароль для доступа к приложению, а все остальные пароли хранятся в безопасном хранилище (рис. 27).

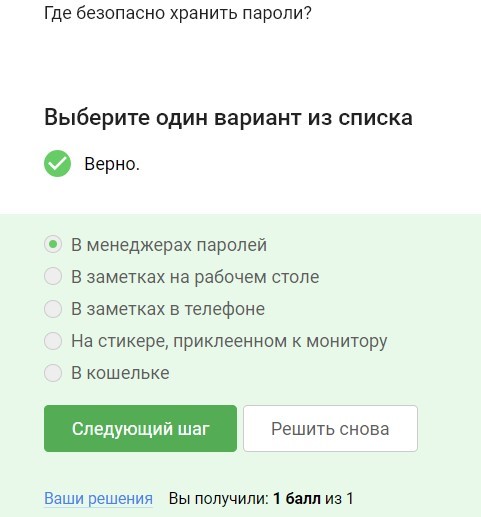


Рис. 27: Пароли. Вопрос №2

Капча представляет собой тест, который обычно решают люди легко, но который сложно или невозможно выполнить для компьютерных программ или роботов. Она используется для различия между человеком и автоматизированными программами (ботами), что помогает защитить веб-ресурсы от спама, несанкционированного доступа и других видов вредоносной деятельности (рис. 28).

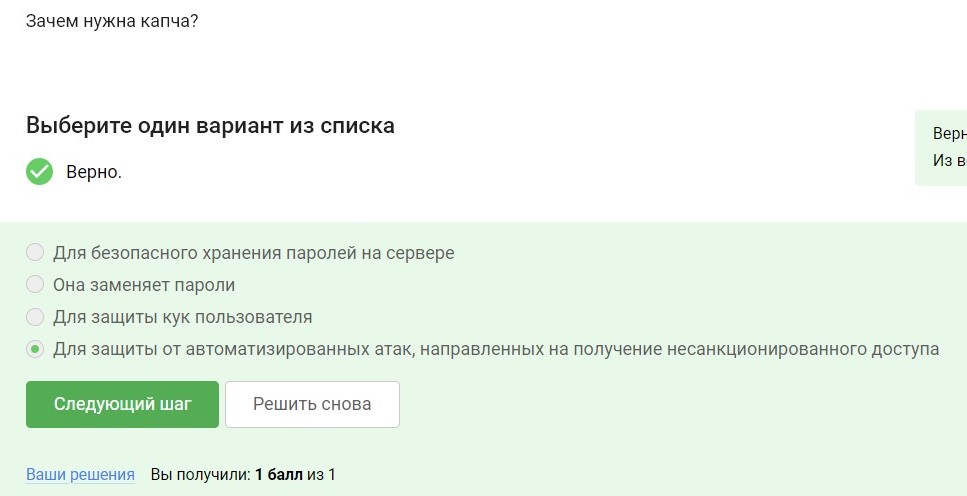


Рис. 28: Пароли. Вопрос №3

Хэширование паролей преобразует пароль в непонятную для человека строку (хэш), которая не может быть преобразована обратно в исходный пароль. Это обеспечивает безопасное хранение паролей на сервере, так как даже если злоумышленник получит доступ к базе данных хэшей паролей, ему будет крайне сложно или невозможно восстановить исходные пароли (рис. 29).

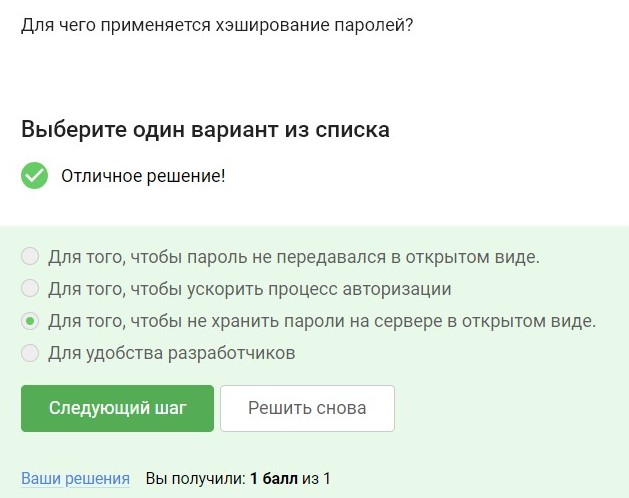


Рис. 29: Пароли. Вопрос №4

Использование соли (случайной дополнительной строки, добавляемой к паролю перед хэшированием) не поможет улучшить стойкость паролей к атаке перебором, если злоумышленник получил доступ к серверу.

Соль предназначена для усложнения процесса подбора паролей. Однако, если злоумышленник получил доступ к серверу и базе данных паролей, то соль также будет доступна ему, что делает ее бесполезной для защиты паролей в этом случае. (рис. 30).

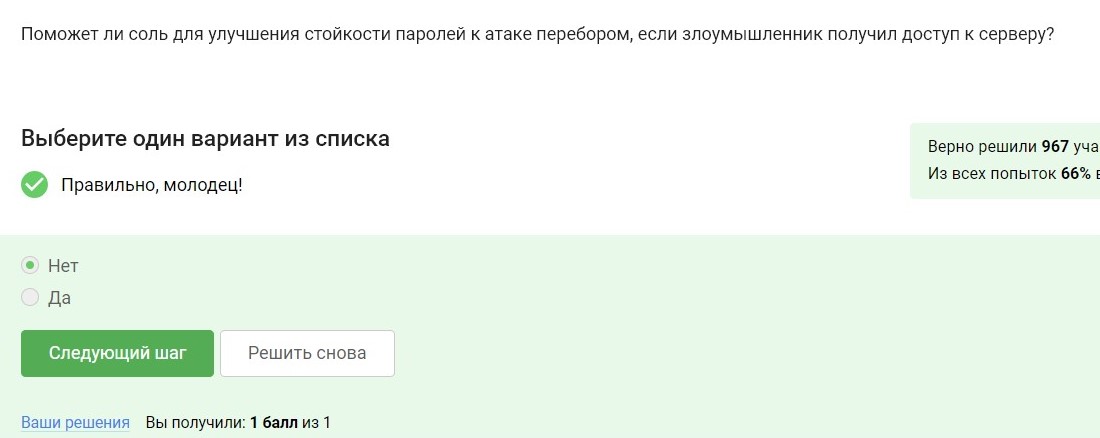


Рис. 30: Пароли. Вопрос №5

Все приведенные методы защищают от утечек данных атакой перебором (рис. 31).

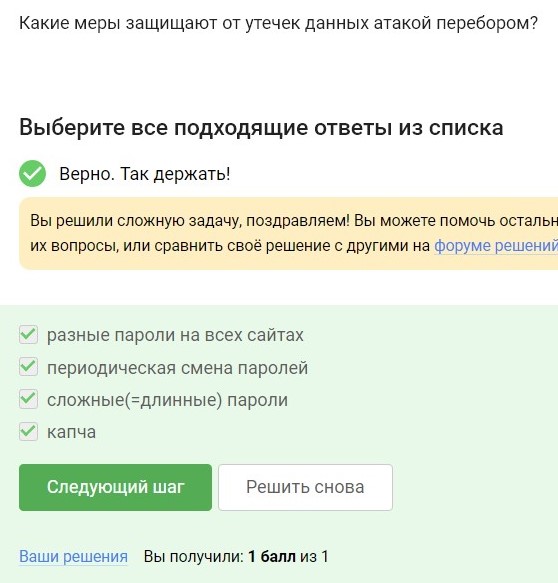


Рис. 31: Пароли. Вопрос №6

### 2.2.3 Фишинг

Выбранные ссылки могут пытаться подделать легитимные веб-сайты банков и интернет-провайдеров, чтобы получить доступ к учетным данным пользователей. Необходимо обратить внимание, что настоящие страницы входа в банковские или почтовые аккаунты обычно имеют домены, которые принадлежат этим организациям, а не сторонним сервисам, как в приведенных примерах. (рис. 32).

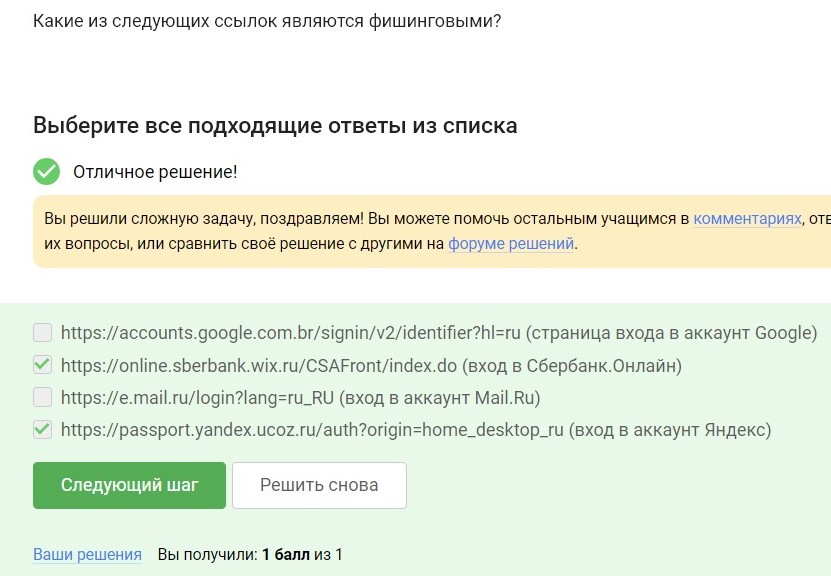


Рис. 32: Фишинг. Вопрос №1

Фишинговое письмо может прийти от знакомого адреса. Злоумышленники могут подделывать адрес отправителя, делая его похожим на адрес знакомого или даже настоящего контакта, чтобы убедить получателя открыть вредоносный вложение или перейти по ссылке на поддельный веб-сайт (рис. 33).

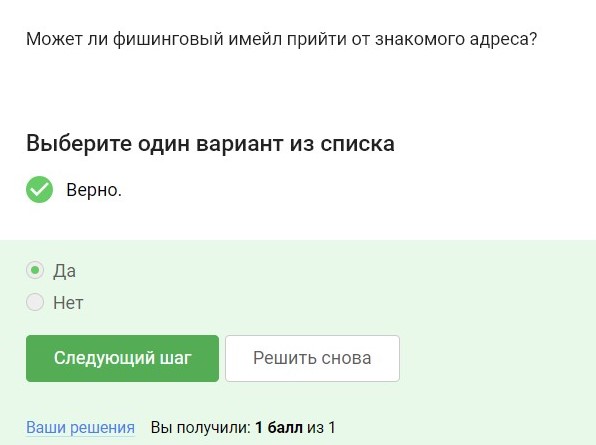


Рис. 33: Фишинг. Вопрос №2

### 2.2.4 Вирусы. Примеры

Спуфинг - это метод, который используется для изменения адреса отправителя электронной почты, делая его похожим на адрес, с которого обычно приходят легитимные сообщения. Это может использоваться злоумышленниками для фишинговых атак или распространения вредоносных программ (рис. 34).

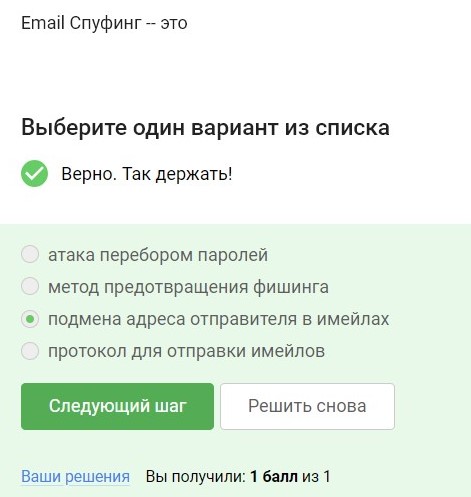


Рис. 34: Вирусы. Примеры. Вопрос №1

Вирус-троян получил свое название от легенды о древнегреческом троянском коне, который скрывал в себе вооруженных воинов. Такой вирус маскируется под полезное или легитимное программное обеспечение, чтобы обмануть пользователя и получить доступ к системе или данных (рис. 35).

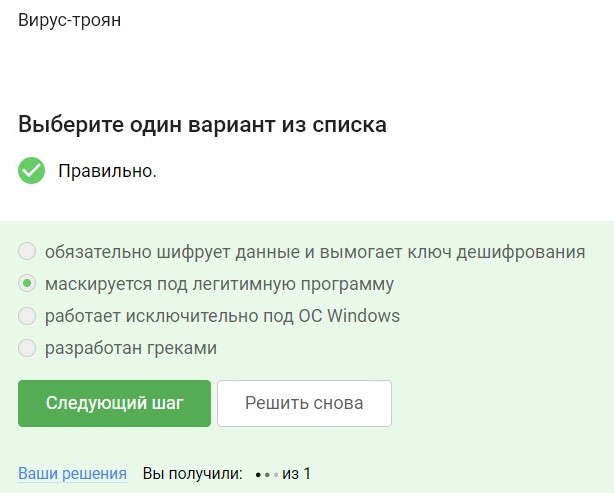


Рис. 35: Вирусы. Примеры. Вопрос №2

### 2.2.5 Безопасность мессенджеров

Ключ шифрования в протоколе мессенджеров Signal формируется при генерации первого сообщения стороной-отправителем. Это обеспечивает конфиденциальность и безопасность обмена сообщениями с момента начала общения между отправителем и получателем (рис. 36).

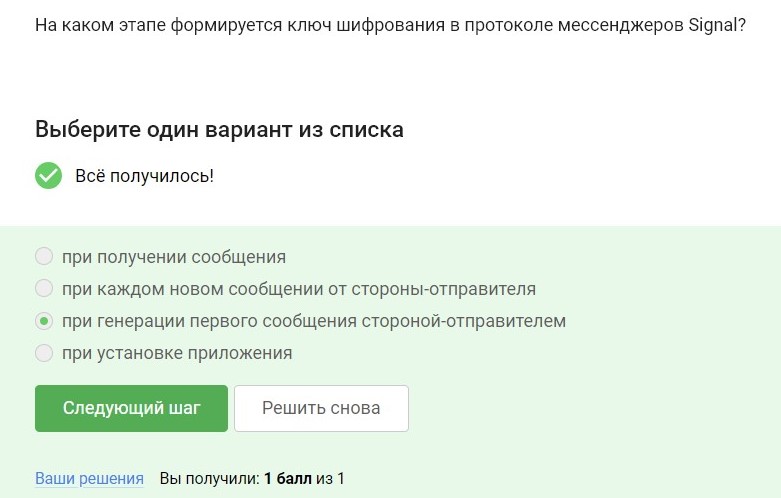


Рис. 36: Безопасность мессенджеров. Вопрос №1

Суть сквозного шифрования заключается в том, что сообщения передаются по узлам связи (серверам) в зашифрованном виде. Это означает, что данные шифруются на устройстве отправителя и дешифруются только на устройстве получателя, при этом промежуточные серверы (узлы связи) не имеют доступа к содержанию сообщений (рис. 37).

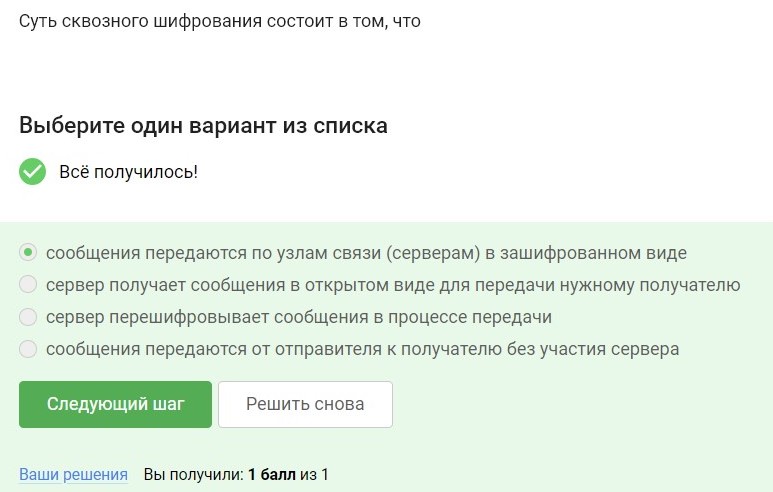


Рис. 37: Безопасность мессенджеров. Вопрос №2

## 2.3 Криптография на практике

### 2.3.1 Введение в криптографию

В асимметричных криптографических примитивах обе стороны имеют пару ключей. Это пара ключей состоит из открытого и секретного ключей. Открытый ключ публикуется в открытом доступе, а закрытый или секретный ключ сторона хранит у себя (рис. 38).

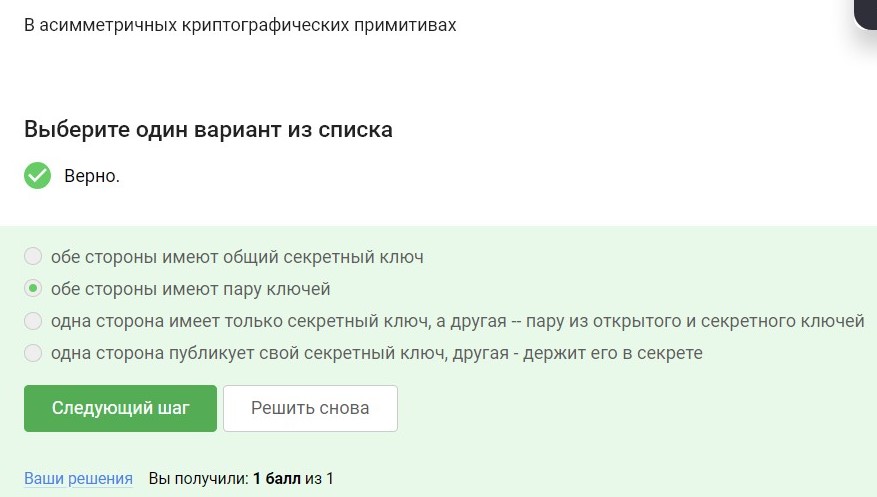


Рис. 38: Введение в криптографию. Вопрос №1

Криптографическая хэш-функция является стойкой к коллизиям, эффективно вычисляется и дает на выходе фиксированное число бит независимо от объема входных данных.Криптографическая хэш-функция не обеспечивает конфиденциальность данных, она используется для генерации хэш-кодов (рис. 39).

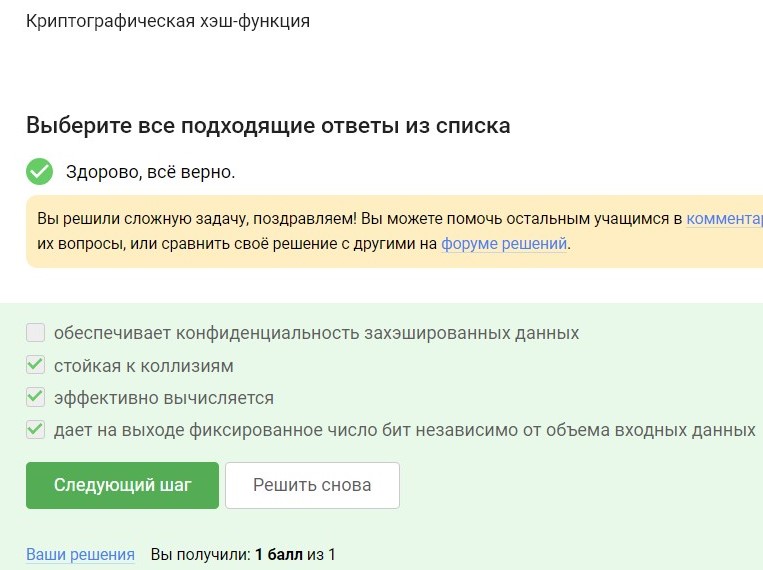


Рис. 39: Введение в криптографию. Вопрос №2

К алгоритмам цифровой подписи относятся RSA, ECDSA и ГОСТ Р 34.10-2012. AES и SHA2 относятся к алгоритмам шифрования, но не к алгоритмам цифровой подписи (рис. 40).

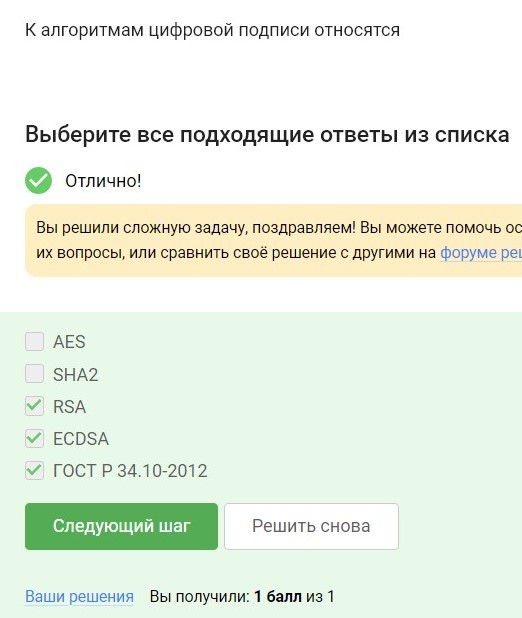


Рис. 40: Введение в криптографию. Вопрос №3

Код аутентификации - это симметричный примитив, который берет на вход какой-то ключ (это должен быть другой ключ, не тот, с которого мы шифровали) и сообщение и выдает код аутентификации сообщения. Корректно об этом примитиве думать, как о симметричной версии подписи. Как правило, код аутентификации сообщения строится с помощью хэш-функции или симметричного шифрования. Код аутентификации обеспечивает целостность данных (рис. 41).

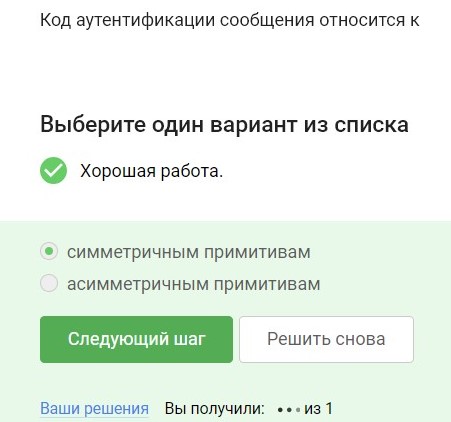


Рис. 41: Введение в криптографию. Вопрос №4

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. Сделать этот протокол стойким к активным злоумышленникам помогает цифровая подпись (рис. 42).

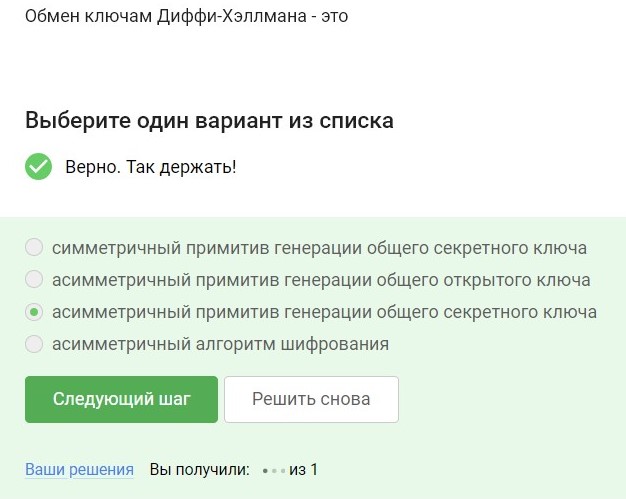


Рис. 42: Введение в криптографию. Вопрос №5

### 2.3.2 Цифровая подпись

Протокол электронной цифровой подписи относится к протоколам с публичным (или открытым) ключом. Эти протоколы используют пару ключей - публичный (или открытый) и приватный (секретный) - для создания и проверки цифровых подписей (рис. 43).

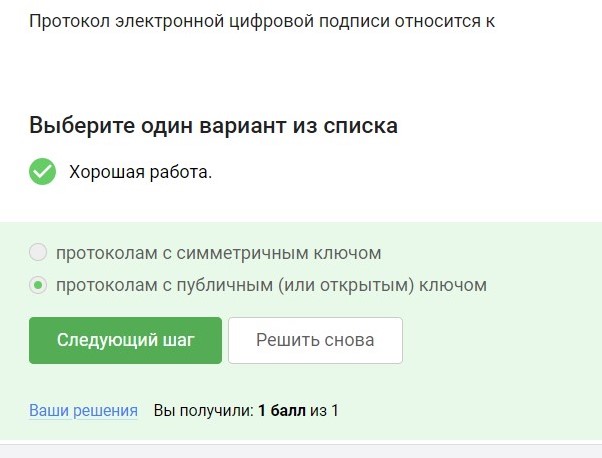


Рис. 43: Цифровая подпись. Вопрос №1

Алгоритм верификации электронной цифровой подписи требует на вход подпись, открытый ключ, сообщение. Это позволяет алгоритму проверить подлинность сообщения с использованием открытого ключа, соответствующего закрытому ключу, с помощью которого была создана цифровая подпись (рис. 44).

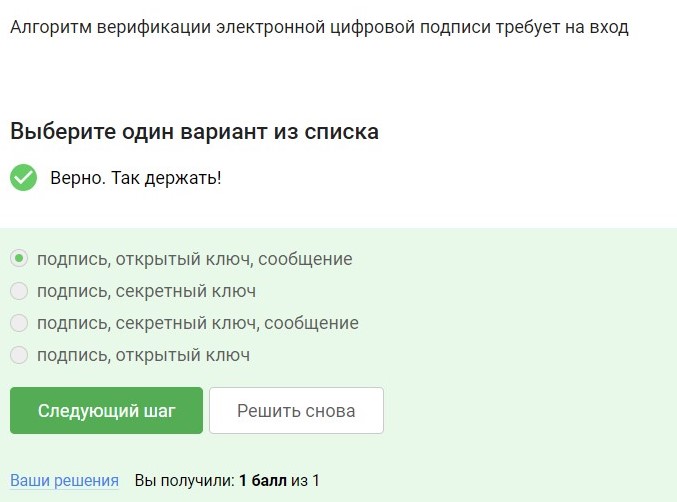


Рис. 44: Цифровая подпись. Вопрос №2

Электронная цифровая подпись не обеспечивает конфиденциальность. Электронная цифровая подпись обеспечивает аутентификацию, целостность и неотказ от авторства, но не скрывает содержимое сообщения от посторонних лиц (рис. 45).

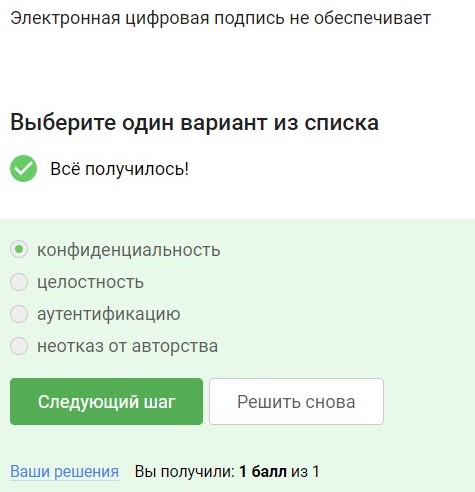


Рис. 45: Цифровая подпись. Вопрос №3

Усиленная неквалифицированная подпись может быть подтверждена сертификатом, который может быть выпущен самостоятелно, то есть кроме того, что пользователь выпускает свою пару секретных ключей, он еще и может сам их сертифицировать. Такая подпись может быть использована в коммерческом документообороте в небольших негосударственных структурах. А вот что касается усиленной квалифицированной подписи, эта подпись уже имеет юридическую силу, она, как правило, равнозначна рукописной (рис. 46).

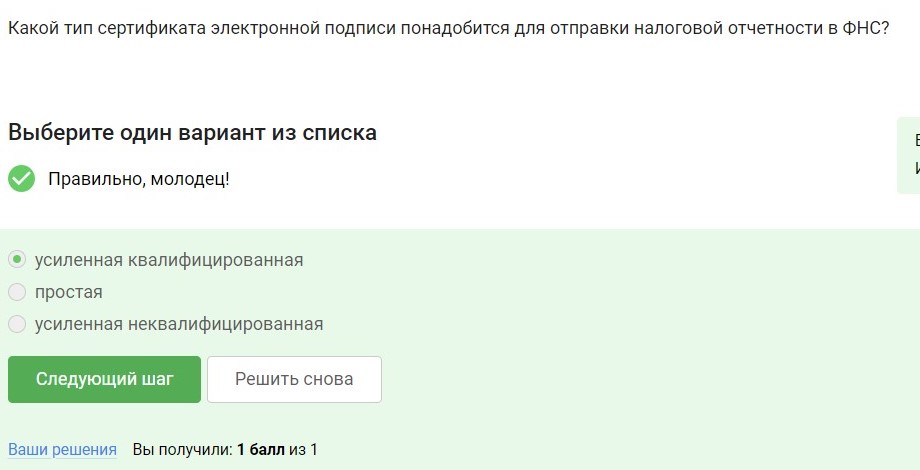


Рис. 46: Цифровая подпись. Вопрос №4

Получиь квалифицированный сертификат ключа проверки электронной подписи можно в удостоверяющем (сертификационном) центре. Эти центры имеют соответствующие полномочия и аккредитации для выдачи квалифицированных сертификатов, которые имеют юридическую силу (рис. 47).

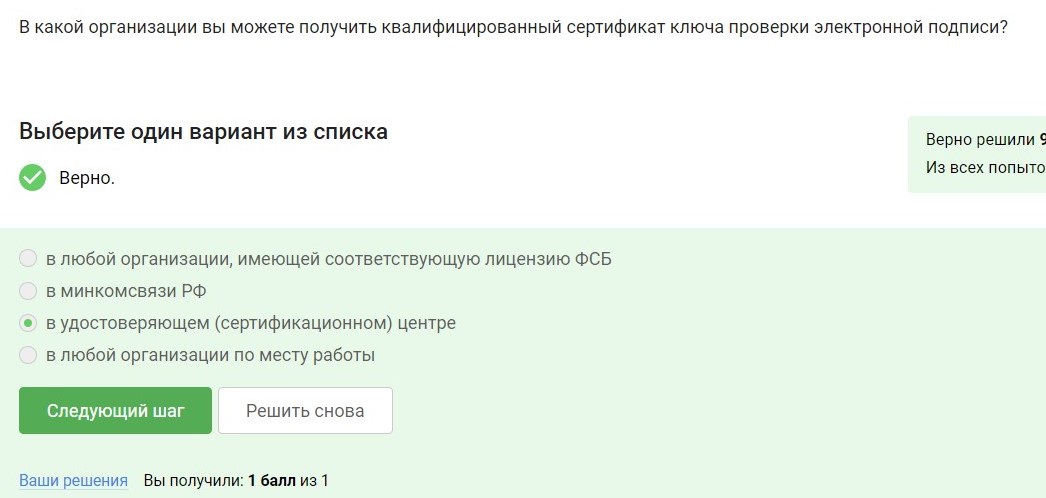


Рис. 47: Цифровая подпись. Вопрос №5

### 2.3.3 Электронные платежи

Платежные системы: MasterCard - одна из крупнейших мировых платежных систем. МИР - российская национальная платежная система. Платежные системы обычно обеспечивают возможность осуществления электронных и физических транзакций между покупателем и продавцом, включая торговлю онлайн, в магазинах и через банкоматы (рис. 48).

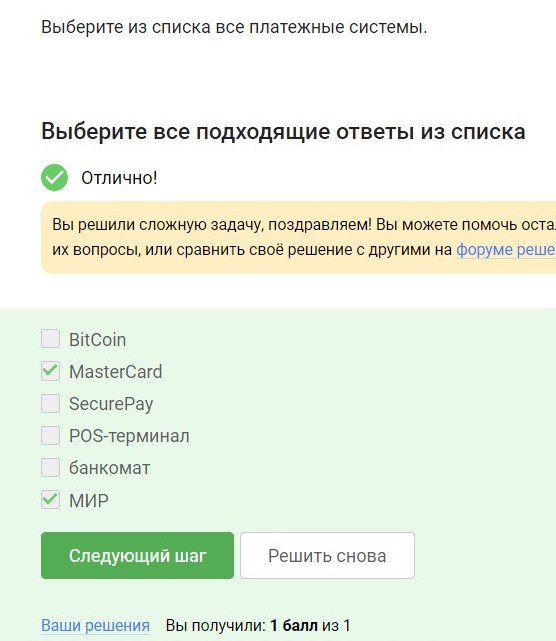


Рис. 48: Электронные платежи. Вопрос №1

Данные примеры демонстрируют использование нескольких факторов (что-то, что пользователь знает и что-то, что пользователь имеет или может получить) для повышения безопасности процесса аутентификации (рис. 49).

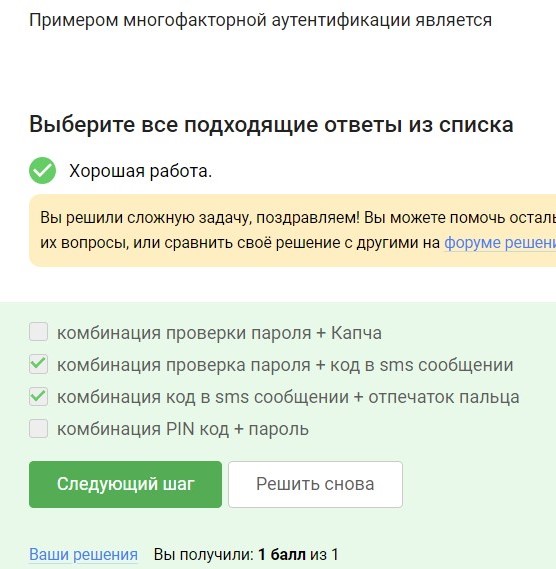


Рис. 49: Электронные платежи. Вопрос №2

При онлайн платежах сегодня используется многофакторная аутентификация покупателя перед банком-эмитентом. Это означает, что для подтверждения платежа требуется предоставление нескольких видов аутентификационных данных или факторов безопасности, таких как пароль, одноразовый код, отпечаток пальца или другие подтверждения, чтобы обеспечить дополнительный уровень безопасности и защиты от мошенничества (рис. 50).

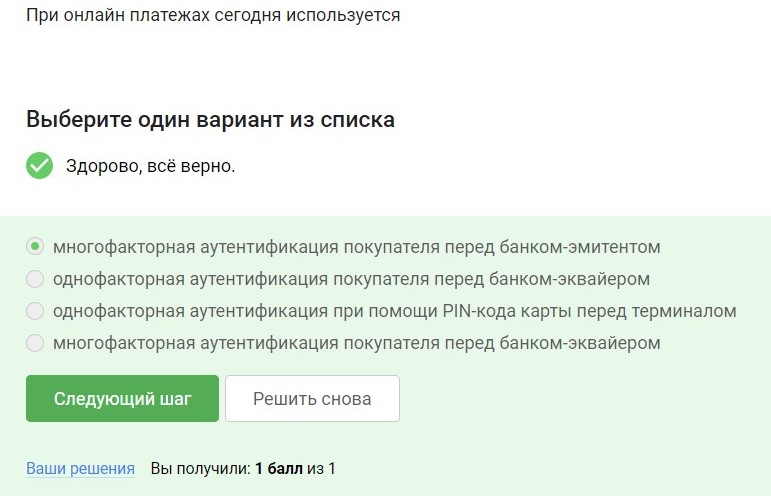


Рис. 50: Электронные платежи. Вопрос №3

### 2.3.4 Блокчейн

Свойство криптографической хэш-функции, которое используется в доказательстве работы, это сложность нахождения прообраза. Доказательство работы включает в себя выполнение некоторой вычислительной работы, результат которой должен удовлетворять определенным критериям, например, начинать с определенного количества нулей в хэш-значении. Это требование обеспечивает, что выполнение работы требует значительных вычислительных ресурсов (рис. 51).

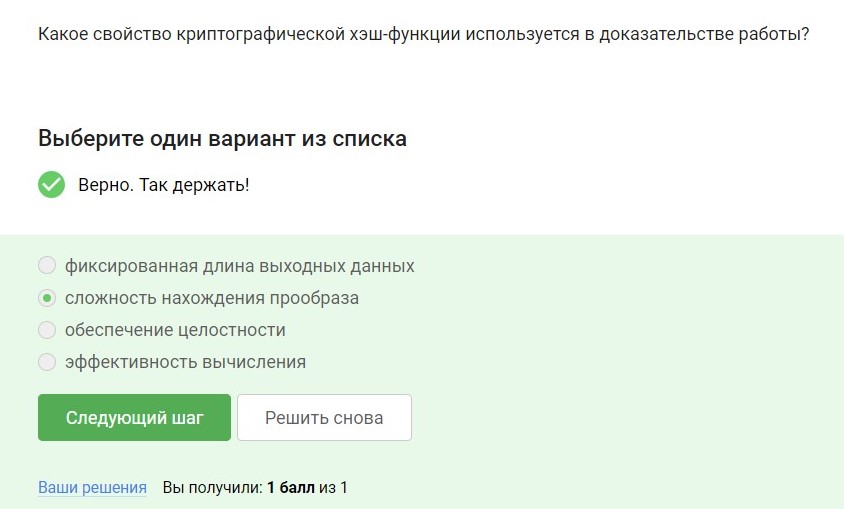


Рис. 51: Блокчейн. Вопрос №1

Консенсус в терминах криптовалют представляет собой общепризнанное соглашение, закодированное в общедоступной структуре данных, известной как “бухгалтерская книга”. Этот “ledger” хранит историю всех транзакций, учитывая, кто передал какие средства кому и когда. Эта структура данных должна соответствовать четырем основным принципам. Во-первых, это постоянство, что означает, что добавленные данные не должны быть удалены. Во-вторых, это единое мнение, или сам конченсу, когда все участники видят и соглашаются с одинаковыми данными, за исключением недавних изменений. В-третьих, это живучесть, что позволяет добавлять новые транзакции по мере необходимости. И, наконец, открытость, так как любой может стать участником этой структуры данных блокчейна, по крайней мере, в случае с Bitcoin (рис. 52).

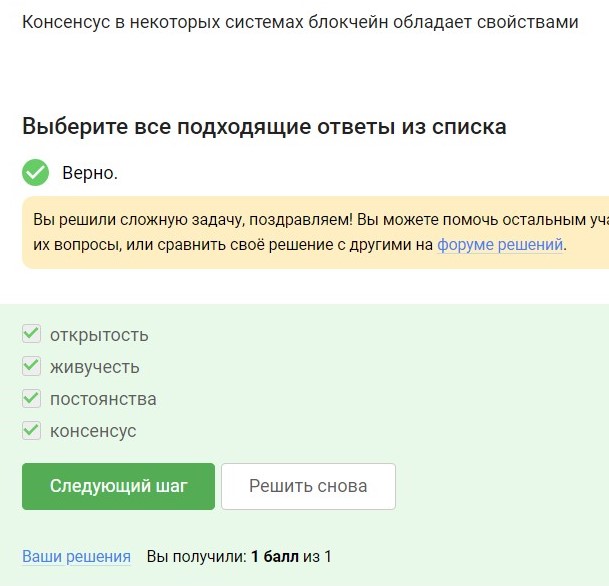


Рис. 52: Блокчейн. Вопрос №2

Секретные ключи, которые хранят участники блокчейна, относятся к криптографическому примитиву “цифровая подпись”. Эти ключи используются для создания и верификации цифровых подписей, которые подтверждают подлинность и авторство транзакций в блокчейне (рис. 53).

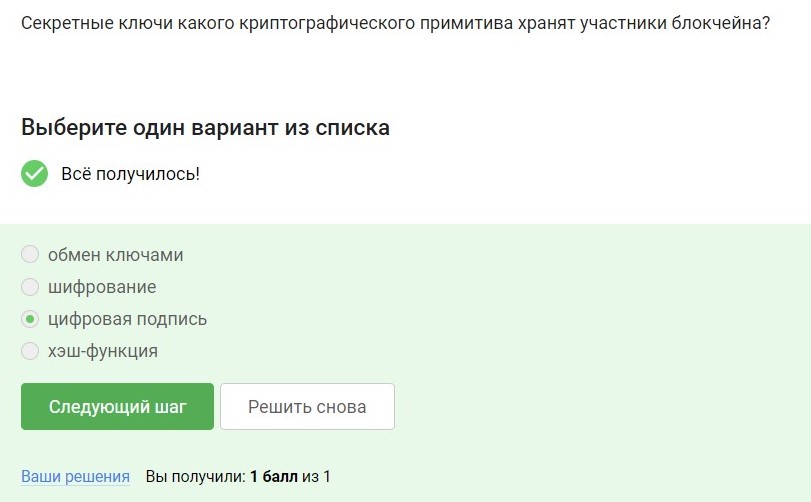


Рис. 53: Блокчейн. Вопрос №3

На этом курс заканчивается. После прохождения сертификат не выдается, а лишь появляется уведомление об успешном пролхождении (рис. 54).

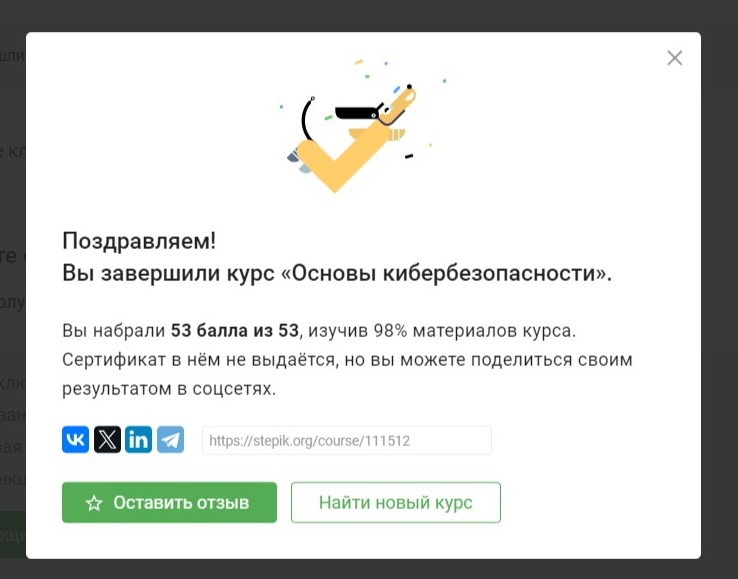


Рис. 54: Окончание курса

# 3 Выводы

В ходе прохождения курса “Основы кибербезопастности” я узнала новую полезную информацию о бнзопасности в сети и криптографии.