Отчет о выполнении внешнего курса:

Основы кибербезопасности

Ежова Алиса Михайловна

Содержание

Список иллюстраций

1 Цель работы

Освоить основные принципы и концепции кибербезопасности, овладеть ключевыми навыками для обеспечения защиты информации и данных, улучшить понимание угроз в сети интернет и способов их предотвращения, а также подготовиться к применению полученных знаний в реальных ситуациях для обеспечения безопасности в цифровом пространстве.

2 Задание

1. Пройти курс.
2. Выполнить все задания и тесты.
3. Получить сертификат.

3 Выполнение внешнего курса

4 Безопасность в сети

5 2.1) Как работает интернет: базовые сетевые протоколы

1. Выберите протокол прикладного уровня:

HTTPS является протоколом прикдладного уровня Протокол прикладного уровня сетевой протокол верхнего уровня (7-го в сетевой модели OSI и 4-го в стеке протоколов TCP/IP), обеспечивает взаимодействие сети и пользователя.

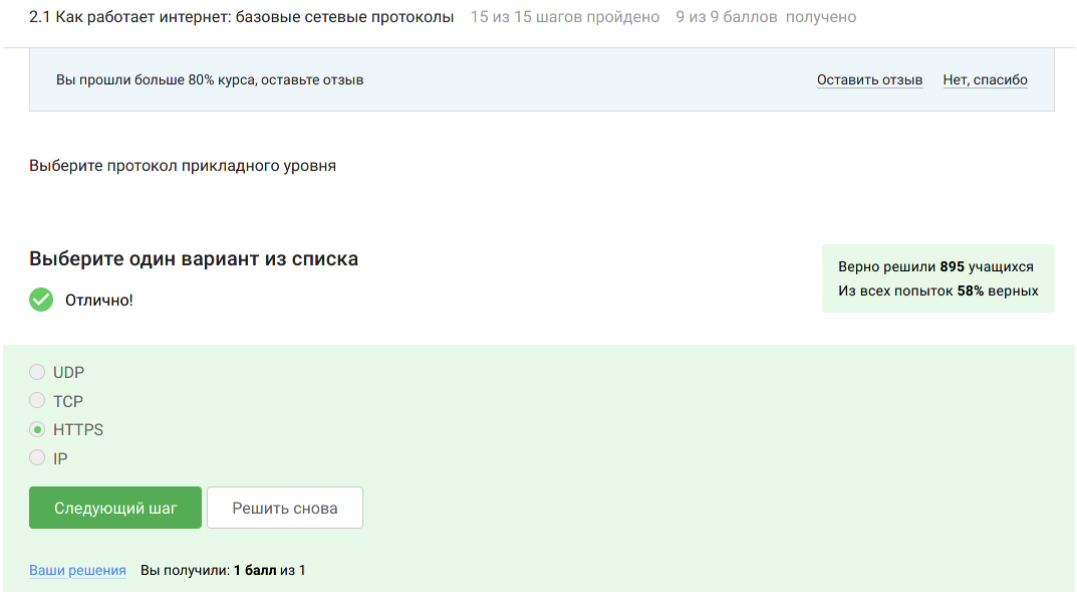

Рис. 5.1: Протокол прикладного уровня

2. На каком уровне работает протокол TCP?:

TCP — это протокол управления передачей (Transmission Control Protocol). Его задача — управлять отправкой данных и следить за тем, чтобы они были гаран-

тированно приняты получателем. Именно гарантия получения данных и сделала этот протокол таким востребованным

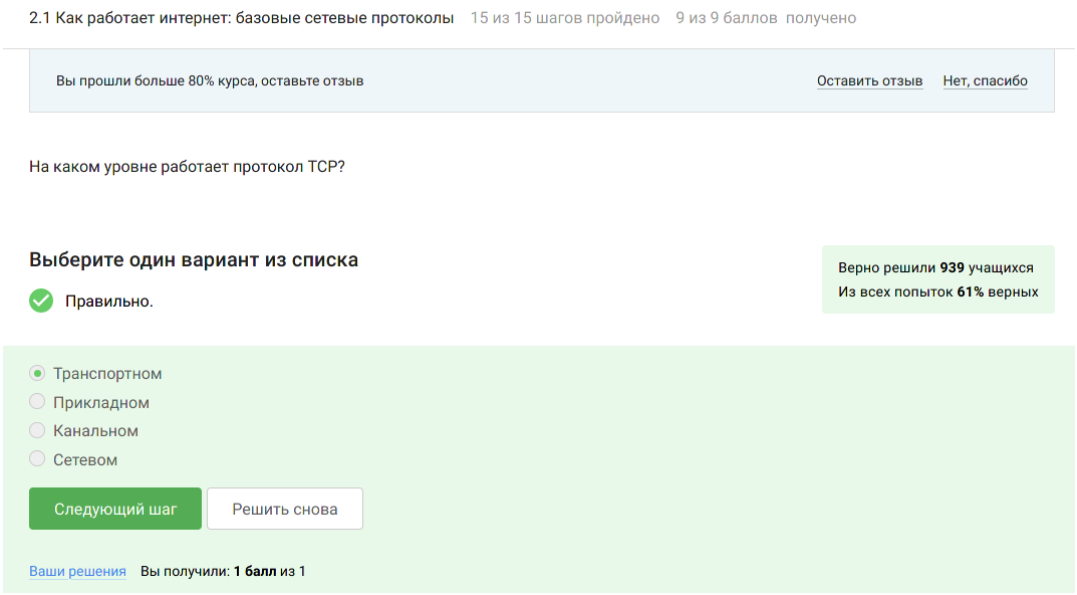

Рис. 5.2: Уровень протокола TCP

3. Выберите все корректные адреса IPv4:

Стандартный IP-адрес называется IPv4. Это четыре числа, разделенные между собой точкой, причем каждое число в двоичном формате состоит из 8 цифр. В переводе в десятичные числа это значит, что все они находятся в диапазоне от 0 до 255. Одна цифра — один бит, и выходит, что в каждом IP-адресе четыре восьмибитных числа.

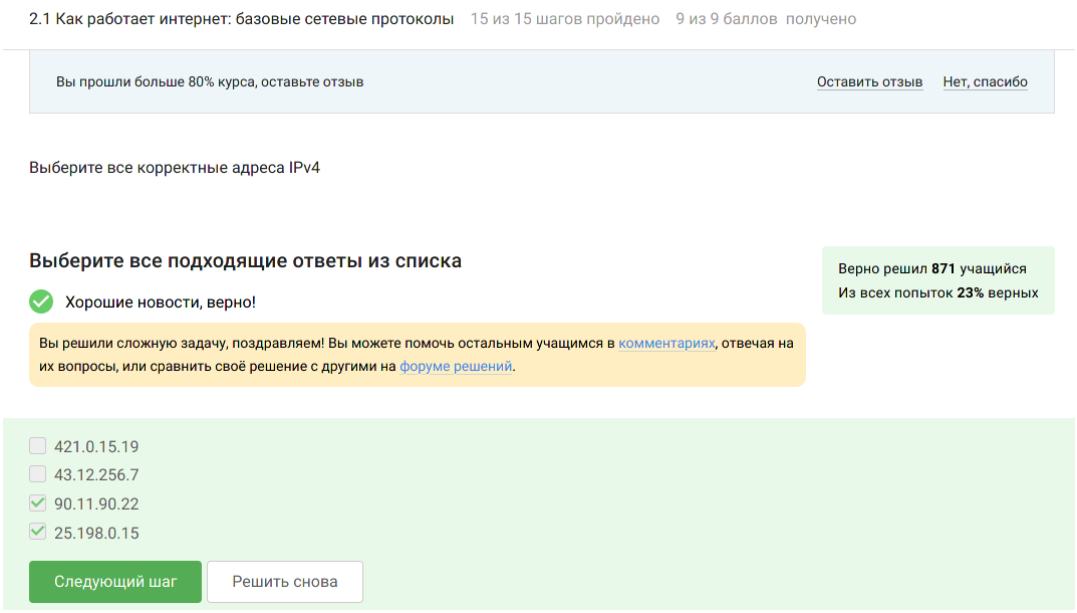

Рис. 5.3: Корректные адреса IPv4

4. DNS сервер:

DNS-сервер — это специализированный компьютер (или группа), который хранит IP-адреса сайтов. Последние, в свою очередь, привязаны к именам сайтов и обрабатывает запросы пользователя. В интернете много DNS-серверов, они есть у каждого провайдера и обслуживают их пользователей.

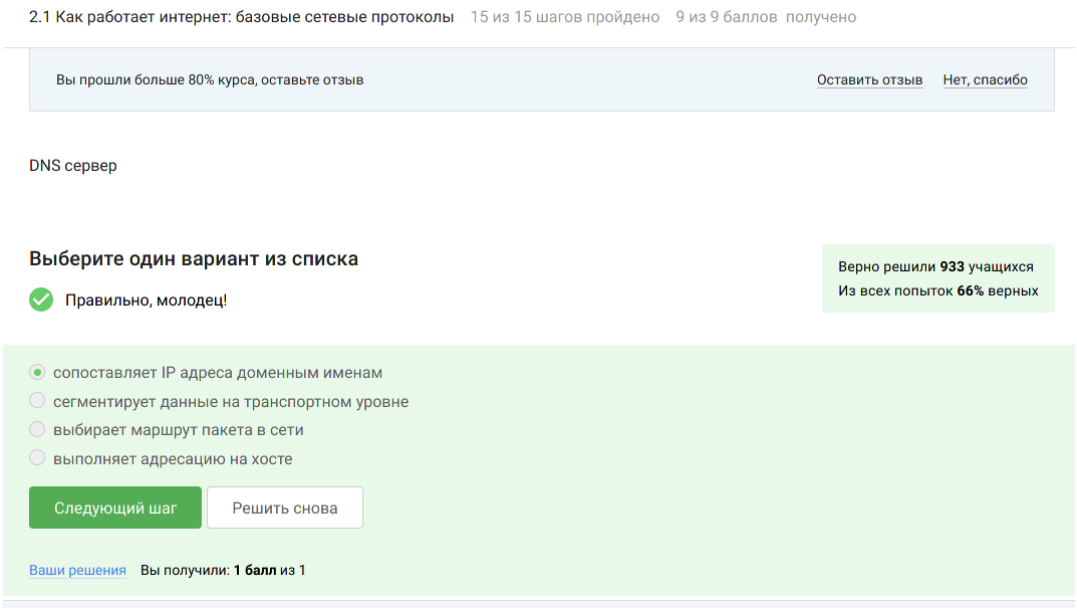

Рис. 5.4: DNS сервер

5. Выберите корректную последовательность протоколов в модели TCP/IP:

Прикладной – транспортный – сетевой – канальный Модель TCP/IP — это набор правил, по которым данные перемещаются по интернету. Главными здесь являются два протокола: TCP и IP. Они нужны, чтобы устанавливать надёжный канал связи между устройствами и передавать по нему данные. Кроме TCP и IP в модели есть и другие протоколы — например, HTTP, Ethernet, FTP и UDP.

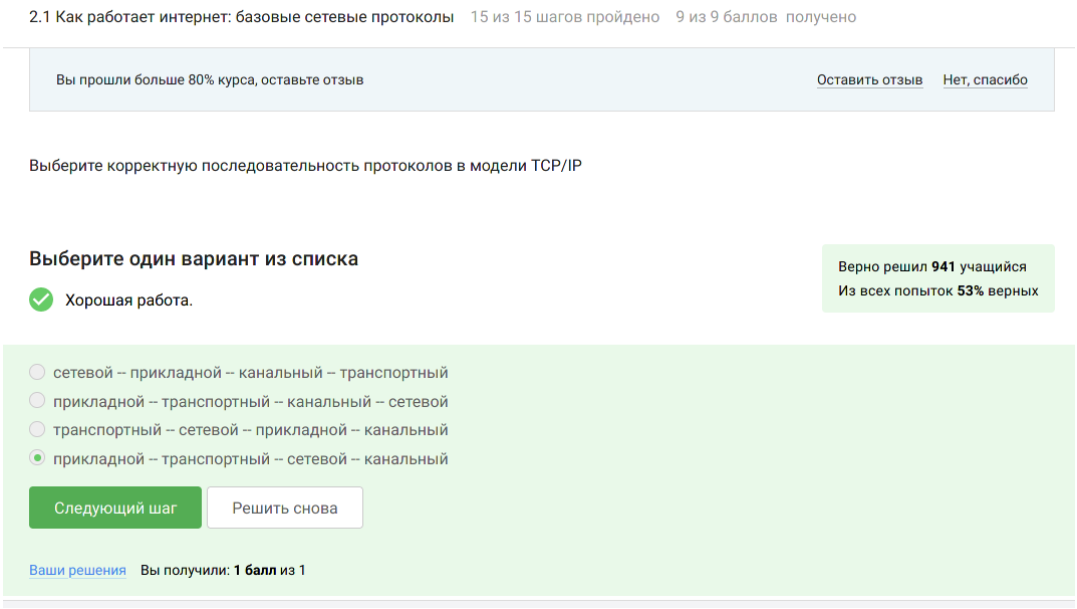

Рис. 5.5: Модель TCP/IP

6. Протокол http предполагает:

Передачу данных между клиентом и сервером в открытом виде. HTTP — это протокол, позволяющий получать различные ресурсы, например HTML-документы. Протокол HTTP лежит в основе обмена данными в Интернете. HTTP является протоколом клиент-серверного взаимодействия, что означает инициирование запросов к серверу самим получателем, обычно веб-браузером (web-browser).

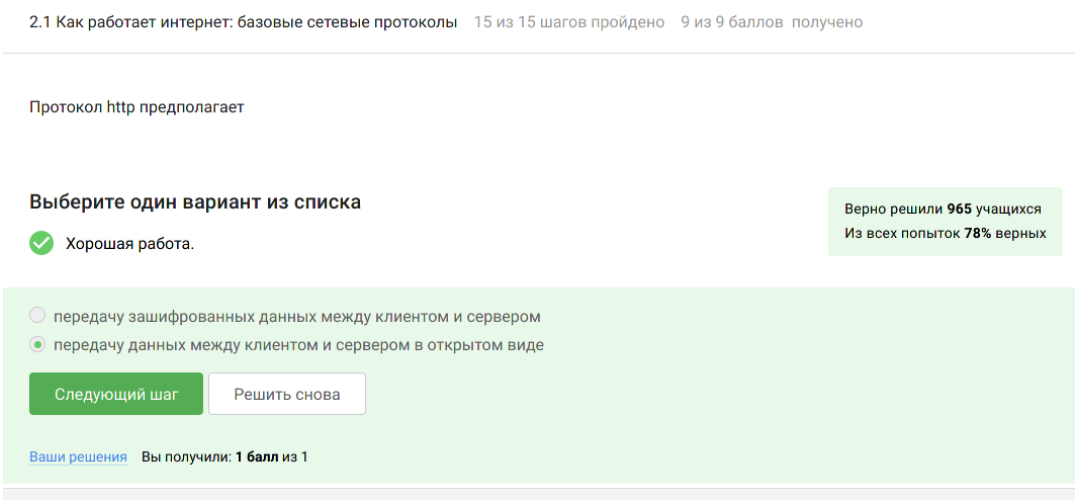

Рис. 5.6: Протокол http предполагает

7. Протокол https состоит из:

Двух фаз: рукопожатия и передачи данных. Система HTTPS похожа на провод, который состоит из двух слоёв: медная сердцевина и оболочка. Медная сердцевина ⊠ основная часть провода, по которой идёт ток. Оболочка защищает контакты от внешних воздействий. Так, медная сердцевина ⊠ это HTTP-протокол, а защитная оболочка ⊠ это SSL-сертификат.

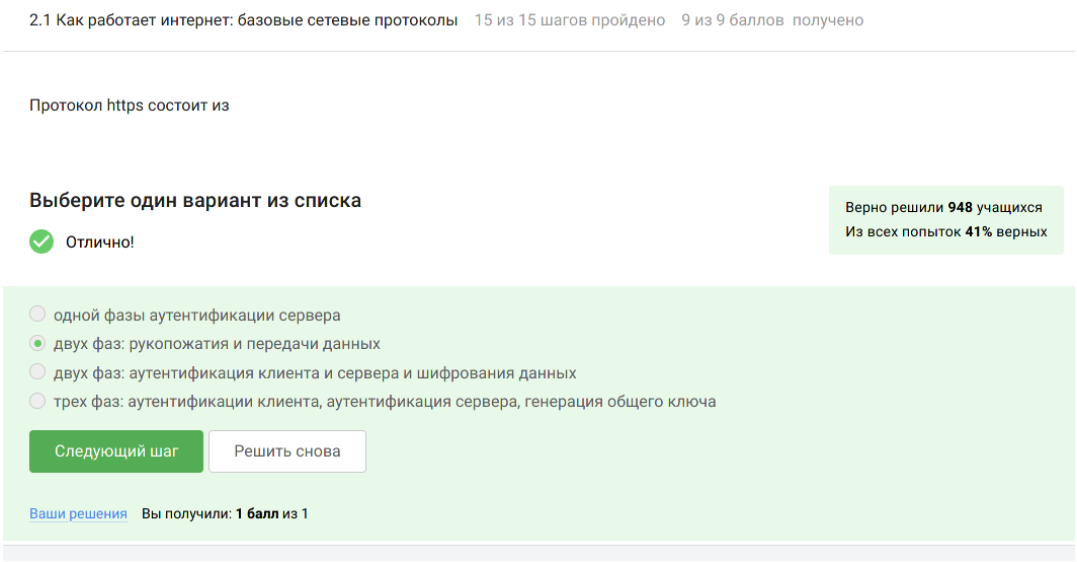

Рис. 5.7: Протокол http состоит из

8. Версия протокола TLS определяется:

И клиентом, и сервером в процессе “переговоров”. TLS — это протокол шифрования и аутентификации, разработанный для защиты интернет-коммуникаций.

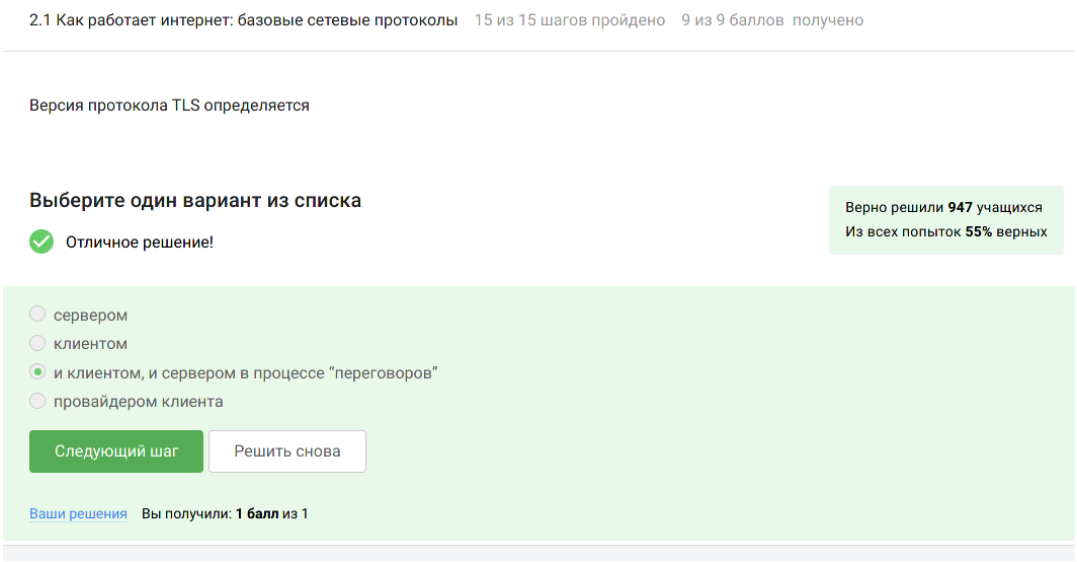

Рис. 5.8: Версия протокола TLS

9. В фазе “рукопожатия” протокола TLS не предусмотрено:

Шифрование данных. Если проверка TLS не работает, убедитесь, что на устройстве нет сертификатов, добавленных вручную. Они могут конфликтовать с сертификатами, развернутыми с помощью консоли администратора. Чтобы узнать об альтернативных способах настройки, обратитесь к поставщику веб-фильтра.

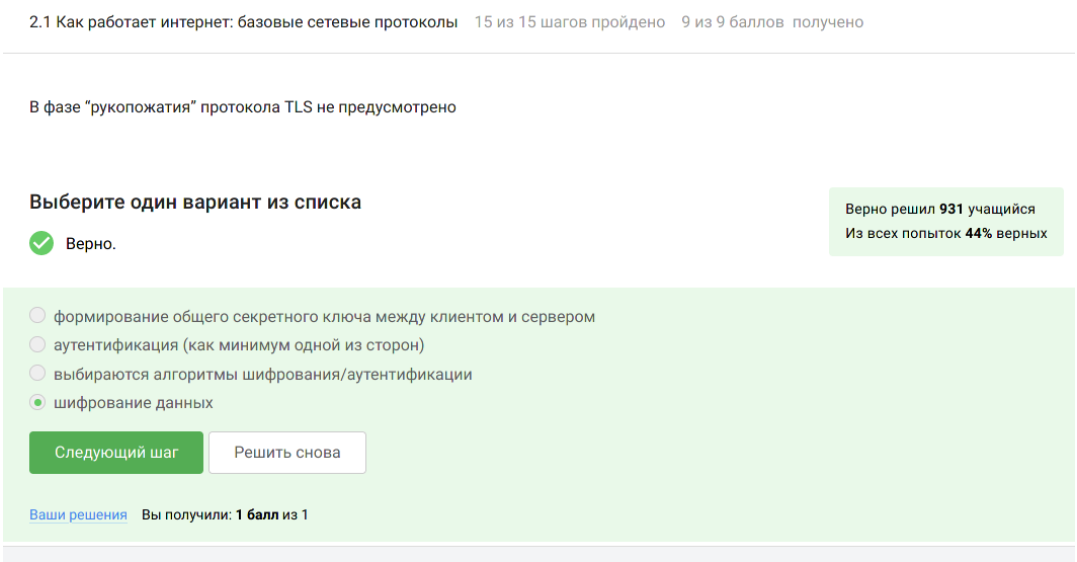

Рис. 5.9: Фаза “рукопожатия”

6 2.2) Персонализация сети:

1. Куки хранят:

Идентификатор пользователя и id сессии. Файлы cookie – это небольшие фрагменты текста, передаваемые в браузер с сайта, который вы открываете. С их помощью сайт запоминает информацию о ваших посещениях.

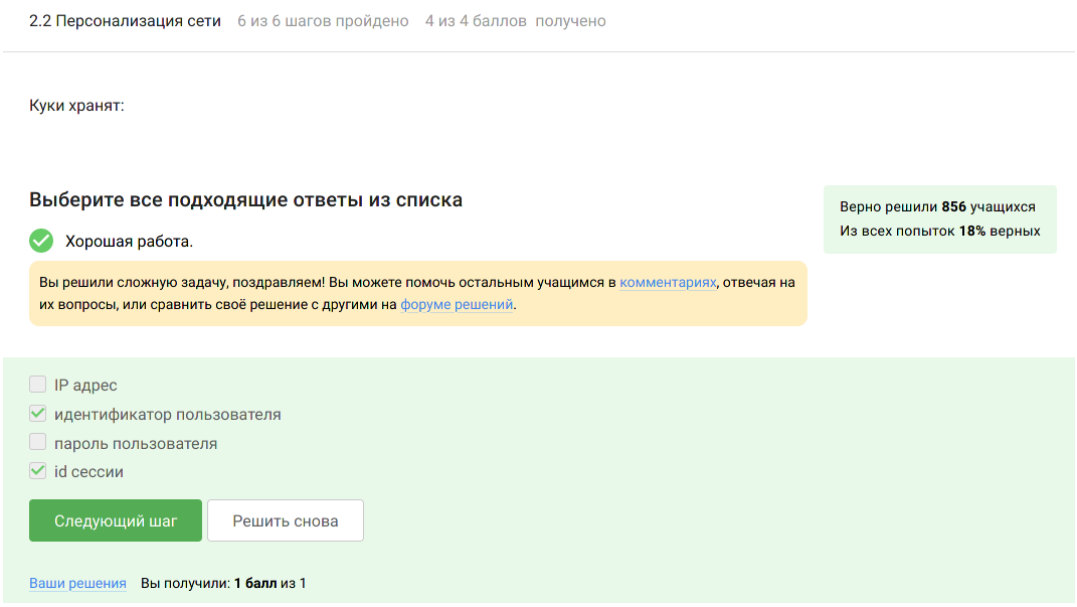

Рис. 6.1: Хранение куки-файлов

2. Куки не используются для:

Улучшения надежности соединения. Информация является анонимной и используется исключительно в статистических целях. Данные веб-аналитики и cookie-файлы невозможно использовать для того, чтобы установить Вашу лич-

ность, поскольку они никогда не содержат персональные данные, включая Ваши имя или адрес электронной почты.

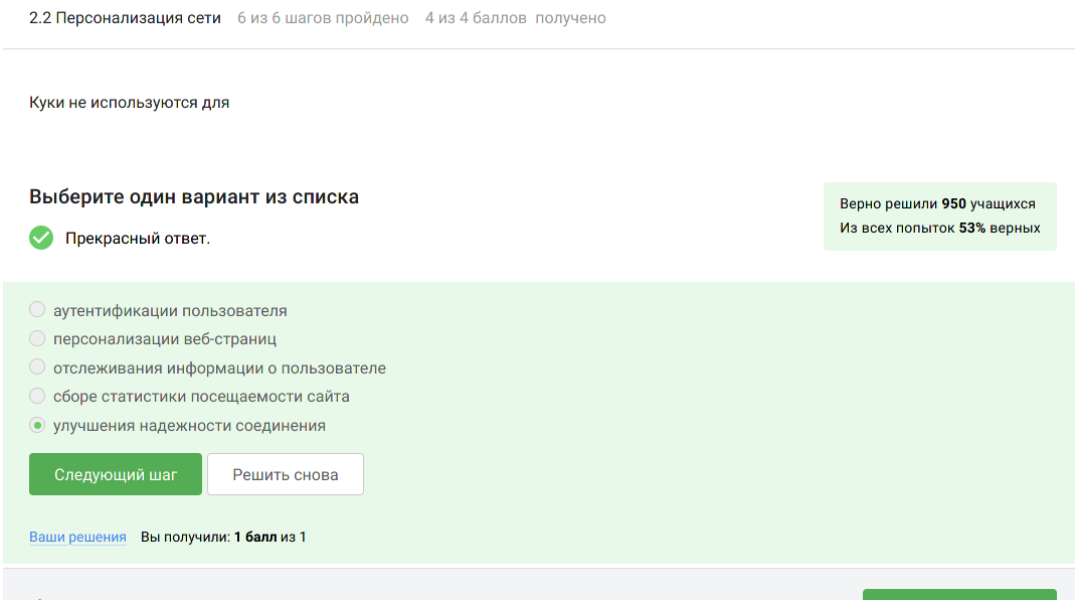

Рис. 6.2: Куки не используются для

3. Куки генерируются:

Сервером. Когда устройство подключается к серверу, он генерирует данные, которые записываются в файлы cookie. Эти данные содержат уникальный идентификатор пользователя и его устройства. Компьютер отправляет эти данные на сервер, который узнает вас по ID и предлагает информацию с учетом ваших предыдущих взаимодействий с сайтом.

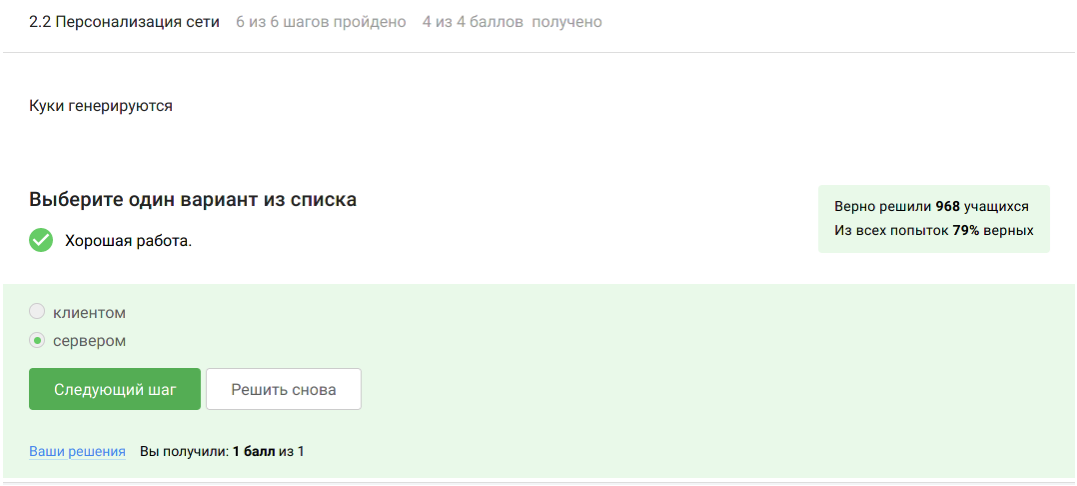

Рис. 6.3: Куки генерируются

4. Сессионные куки хранятся в браузере?:

Да, на время пользования веб-сайтом. Временные («сессионные») файлы cookie — эти файлы позволяют Администрации Сайта соединять действия пользователя во время сеанса браузера. Сеанс браузера начинается, когда пользователь открывает окно браузера, и завершается, когда пользователь закрывает его. Временные файлы cookie создаются на короткое время.

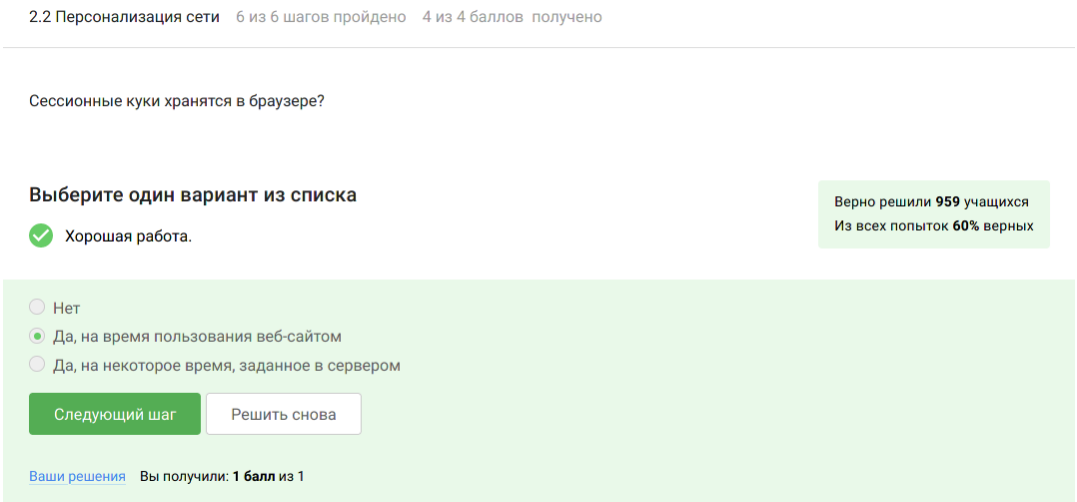

Рис. 6.4: Сессионное хранение куки-файлов

7 2.3) Браузер TOR. Анонимизация:

1. Сколько промежуточных узлов в луковой сети TOR?:

В луковой сети TOR 3 промежуточных узла. Зашифрованные данные передаются через несколько сетевых узлов, называемых «луковыми роутерами», каждый из которых открывает один слой шифрования, чтобы узнать следующую точку передачи данных.

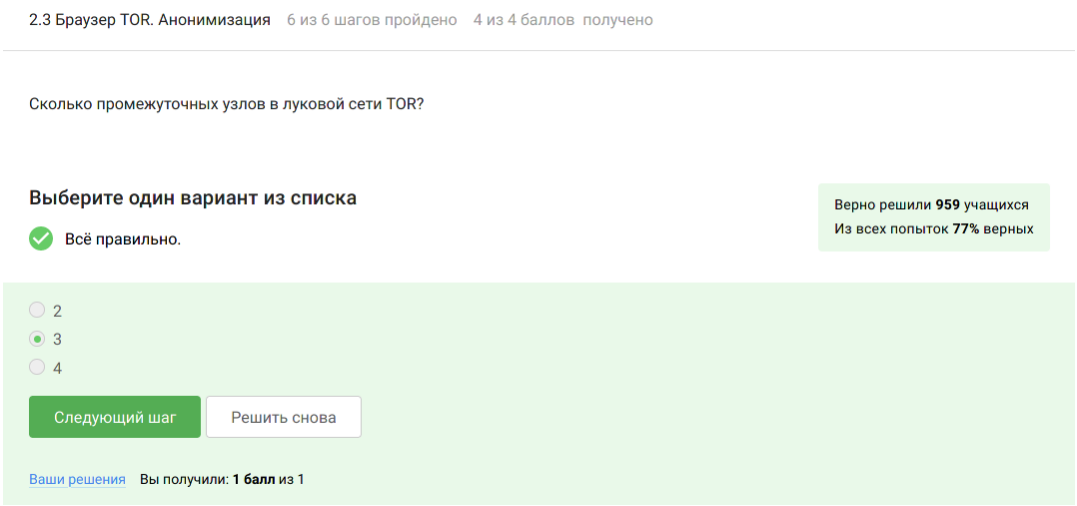

Рис. 7.1: Узлы в луковой сети TOR?

2. IP-адрес получателя известен:

Отправителю и выходному узлу. То есть каждый узел, принимая пакет отправителя, смотрит, может ли он доставить его конечному получателю. Если может, он его перенаправляет в соответствии со своей таблицей маршрутизации на следующий узел. Следующий узел видит, что он тоже может доставить пакет, ну и так далее, пока пакет не дойдёт до финального адреса.

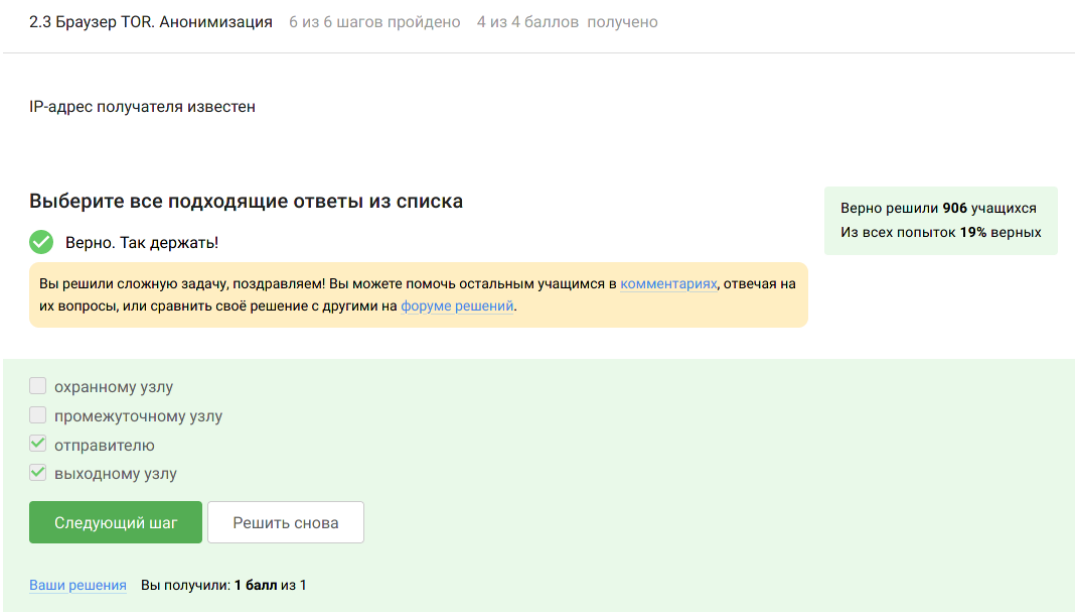

Рис. 7.2: IP-адрес получателя известен

3. Отправитель генерирует общий секретный ключ:

С охранным, промежуточным и выходном узлом. 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.

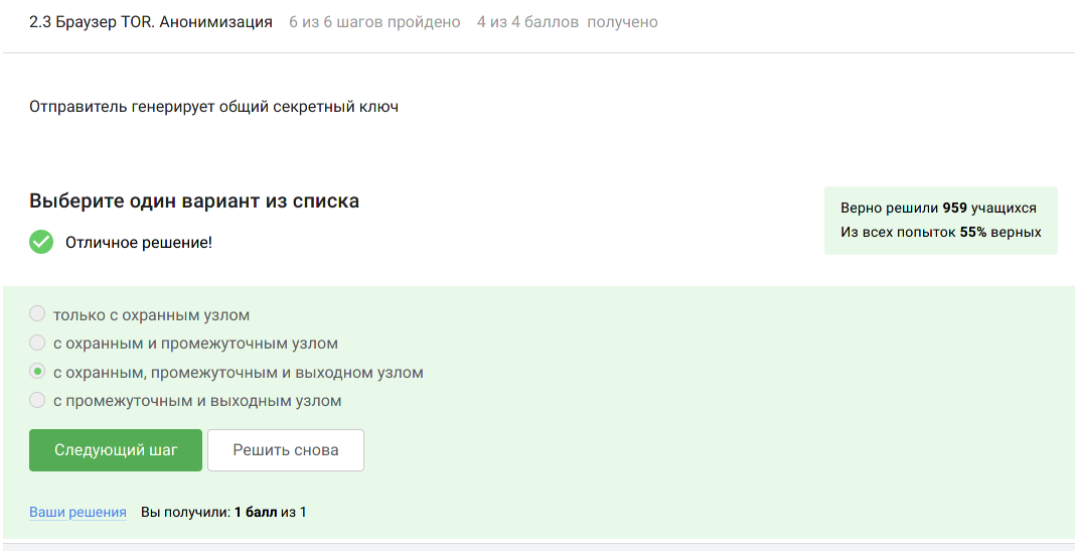

Рис. 7.3: Общий секретный ключ

4. Должен ли получатель использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов?:

Нет, браузер Tor использует сеть Tor для защиты конфиденциальности и анонимности. Использование сети Tor имеет две основных особенности: Ваш интернет-провайдер и все, кто способен наблюдать за вашими подключениями, не смогут отслеживать ваши действия в сети, включая названия и адреса посещаемых сайтов.

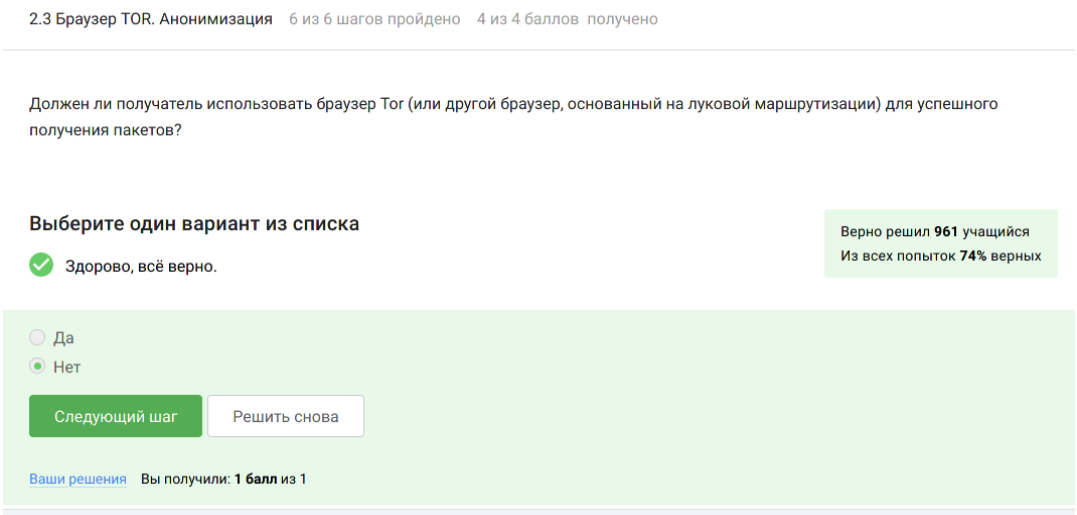

Рис. 7.4: Использование браузера Tor

8 2.4) Беспроводные сети Wi-fi:

1. Wi-Fi - это:

Технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11. EEE 802.11 - набор стандартов связи, для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 2,4; 3,6 и 5 ГГц. Пользователям более известен по названию Wi-Fi, фактически являющемуся брендом, предложенным и продвигаемым организацией Wi-Fi Alliance.

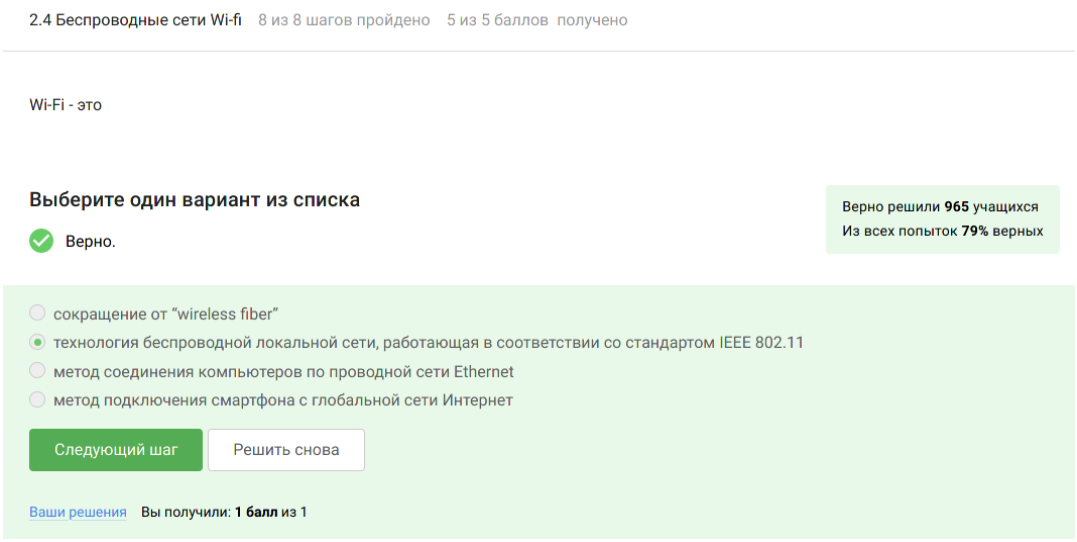

Рис. 8.1: Wi-Fi - это

2. На каком уровне работает протокол WiFi?:

Канальном. Как и все стандарты этого семейства, Fi-Wi 802.11 работает на нижних двух уровнях модели ISO/OSI, физическом и канальном.

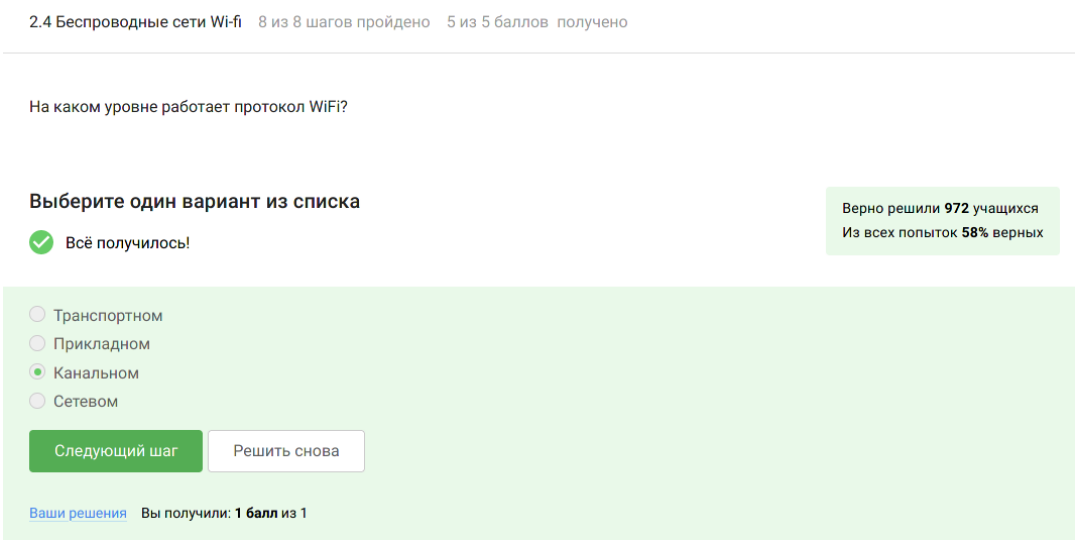

Рис. 8.2: Уроень протокола WiFi

3. Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi:

WEP, WEP был быстро признан небезопасным, и в 2003 году ему на смену пришел WPA (Wi-Fi Protected Access). WPA значительно превосходит WEP по уровню безопасности. В WPA используются более мощные алгоритмы шифрования, более надежный протокол аутентификации и более широкий набор функций безопасности.

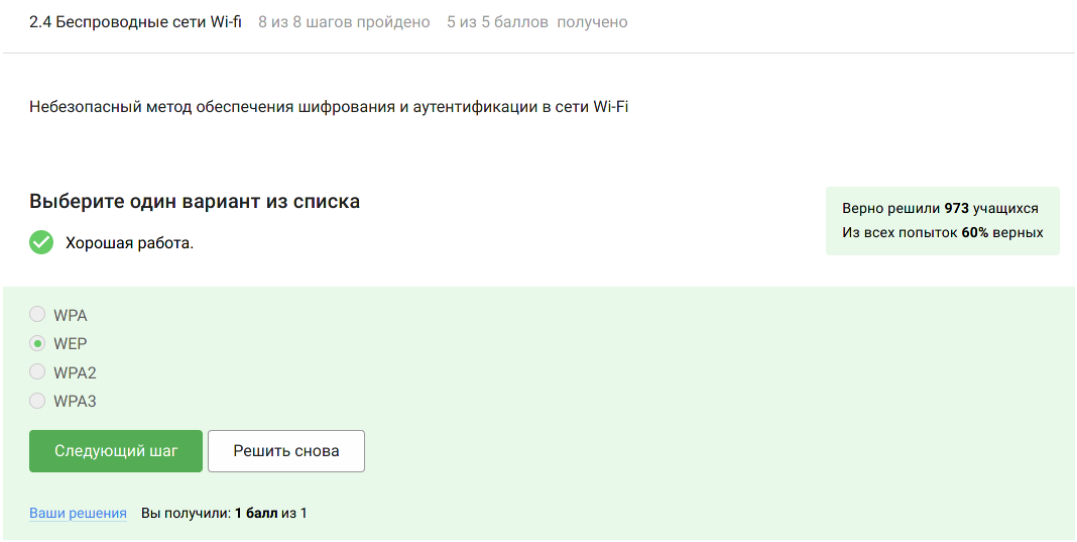

Рис. 8.3: Уроень протокола WiFi

4. Данные между хостом сети (компьютером или смартфоном) и роутером:

Передаются в зашифрованном виде после аутентификации устройств. Wi-Fi-роутер раздает сигнал в виде радиоволн другим устройствам. Излучения разлетаются во все стороны, проходят сквозь воздух и стены, чтобы долететь до ноутбука и смартфонов. Телефон, Smart TV и другие устройства подключаются к маршрутизатору, чтобы получить доступ к интернету.

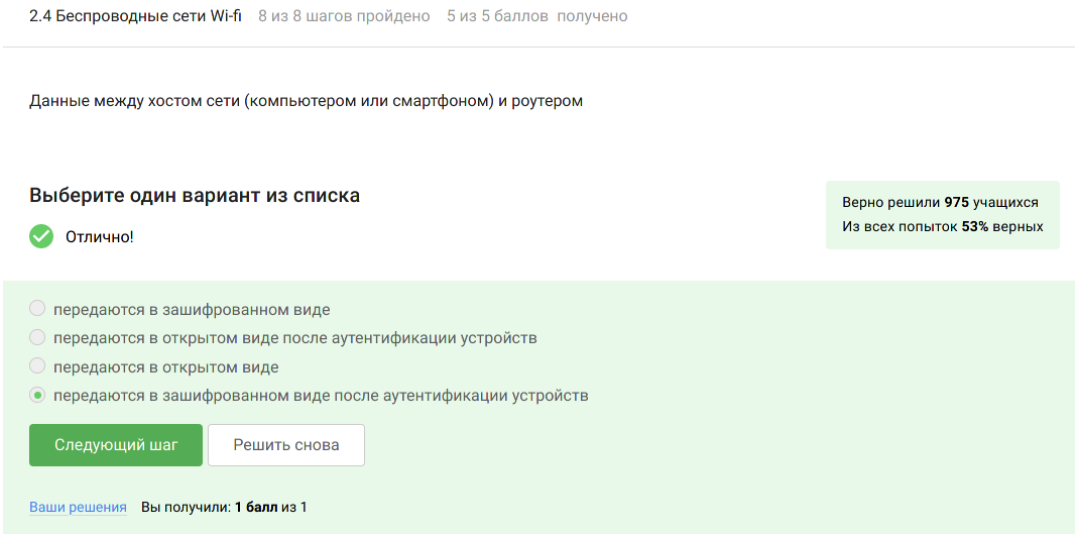

Рис. 8.4: Передача данных между хостом сети и роутером

5. Для домашней сети для аутентификации обычно используется метод:

WPA2 Personal, если вы подключаетесь к домашней сети и получаете сообщение о слабом шифровании, измените тип шифрования на более надежный. Распространенные типы шифрования беспроводных сетей: WEP, TKIP, WPA, WPA2 (AES/CCMP). Главное отличие между ними — уровень защиты.

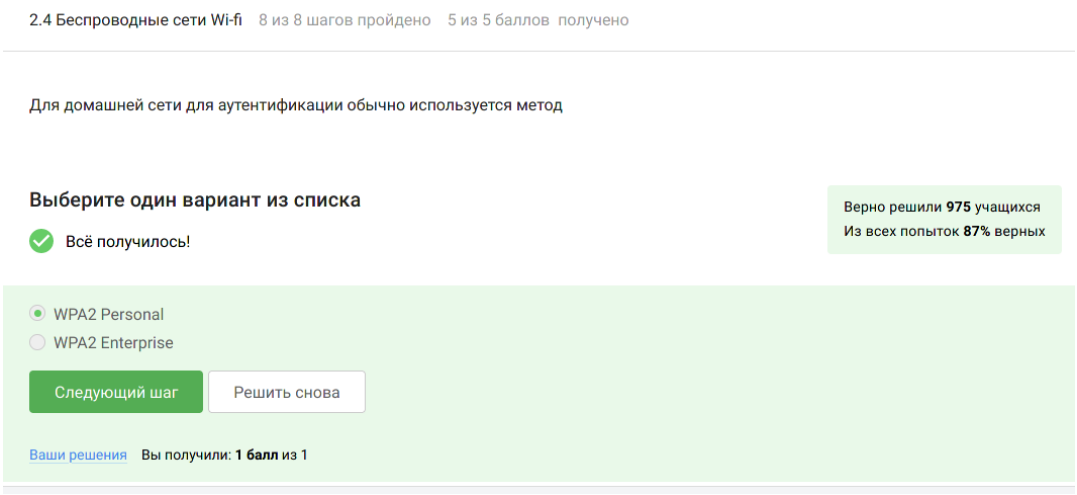

Рис. 8.5: Метод для домашней сети для аутентификации

9 Защита ПК/телефона

10 3.1) Шифрование диска:

1. Можно ли зашифровать загрузочный сектор диска?:

Да, можно зашифровать загрузочный сектор диска. Защита загрузочного сектора диска позволяет усилить безопасность системы, так как это первый сектор, который загружается при запуске компьютера.

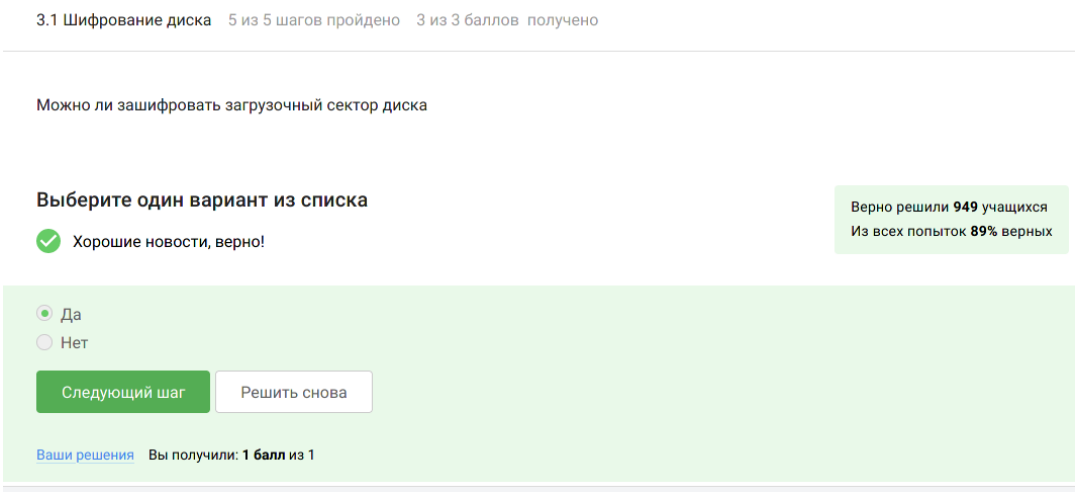

Рис. 10.1: Шифровка загрузочного сектора диска

2. Шифрование диска основано на:

Шифрование диска на основе использования ключей симметричного шифрования - это один из наиболее распространенных методов шифрования данных на диске. Симметричное шифрование использует один и тот же ключ как для шифрования, так и для расшифрования данных.

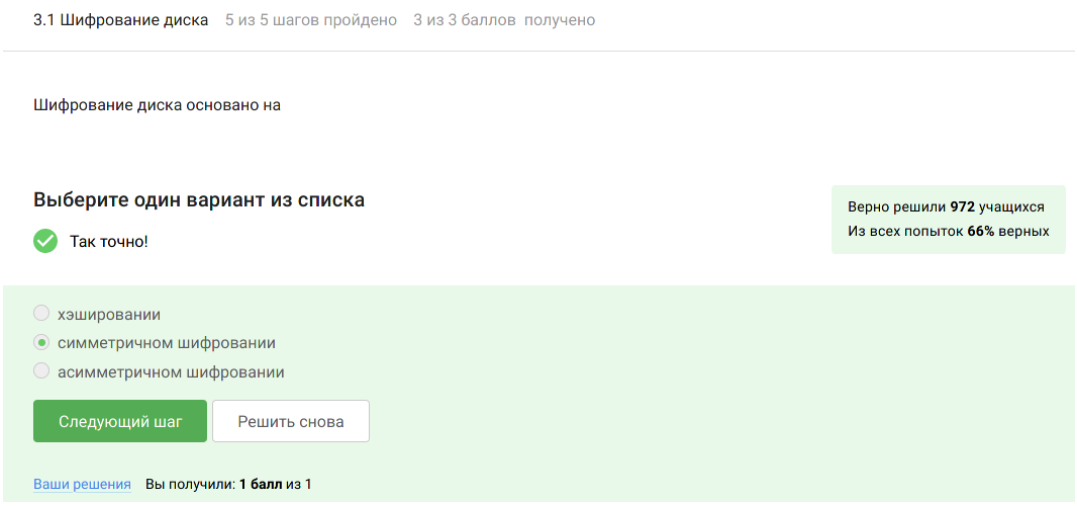

Рис. 10.2: На чем основано шифрование диска

3. С помощью каких программ можно зашифровать жесткий диск?: BitLocker и VeraCrypt

Да, с помощью программного обеспечения BitLocker и VeraCrypt можно зашифровать жесткий диск для обеспечения безопасности данных. Вот краткое объяснение обеих программ:

BitLocker - это интегрированное средство шифрования диска, предоставляемое компанией Microsoft для операционных систем Windows. VeraCrypt - это бесплатное программное обеспечение с открытым исходным кодом, которое предоставляет возможности шифрования дисков на различных операционных системах, включая Windows, macOS и Linux.

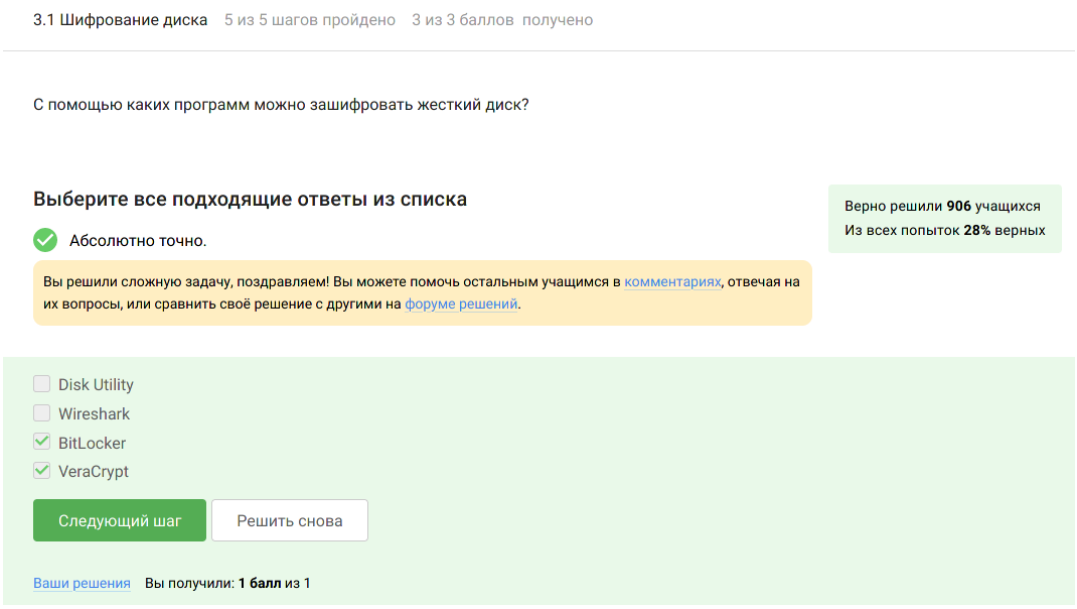

Рис. 10.3: С помощью каких программ можно зашифровать жесткий диск

11 3.2) Пароли:

1. Какие пароли можно отнести с стойким?:

Пароль - UQr9@j4!S$ можно отнести к стойким, так как содержит 10 разнообразных символов, наличие специальных символов и случайность.

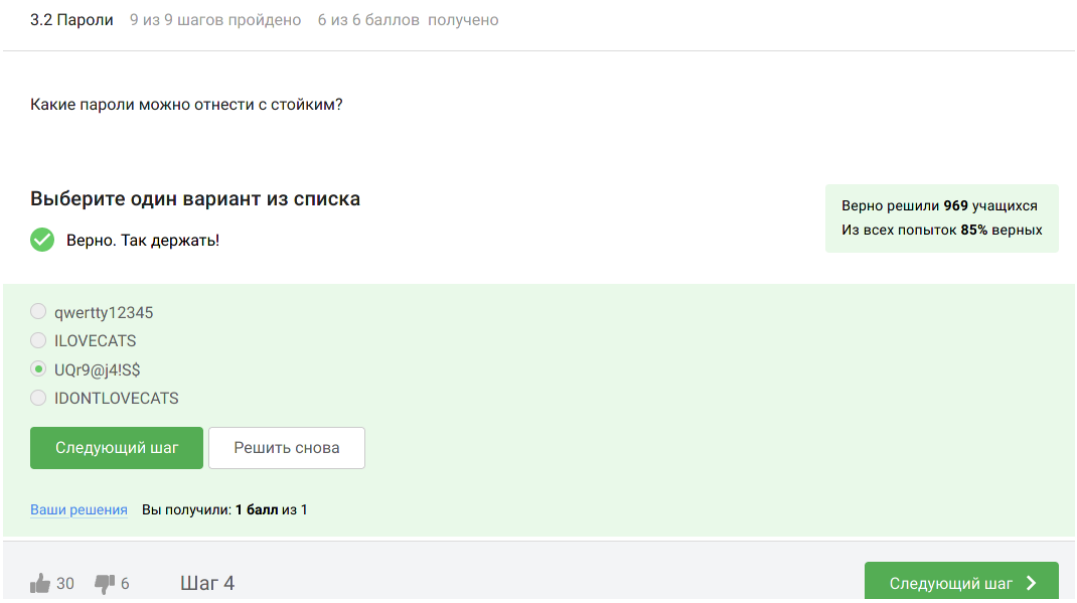

Рис. 11.1: Стойкий пароль

2. Где безопасно хранить пароли?:

В менеджерах паролей. Менеджеры паролей используют сильное шифрование для хранения паролей, что делает их практически непроницаемыми для злоумышленников.

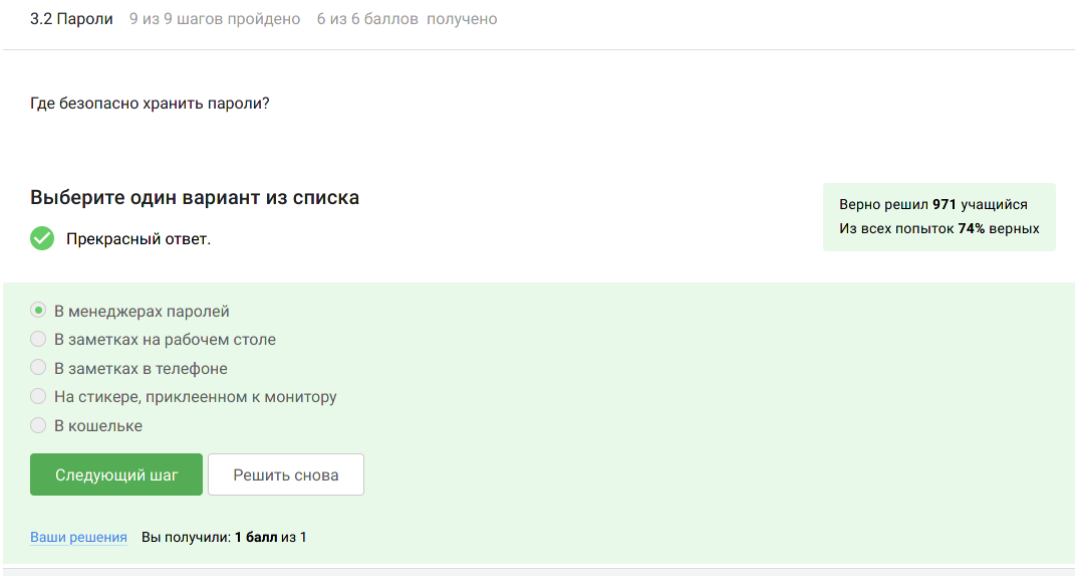

Рис. 11.2: Менеджер паролей

3. Зачем нужна капча?:

Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа. Капча необходима для защиты от различных видов автоматизированных атак, таких как спам-боты, бот-атаки на веб-ресурсы, попытки взлома аккаунтов и т.д. Поскольку автоматизированные программы часто не могут успешно пройти капчу, она помогает обеспечить защиту от несанкционированного доступа и злоупотреблений.

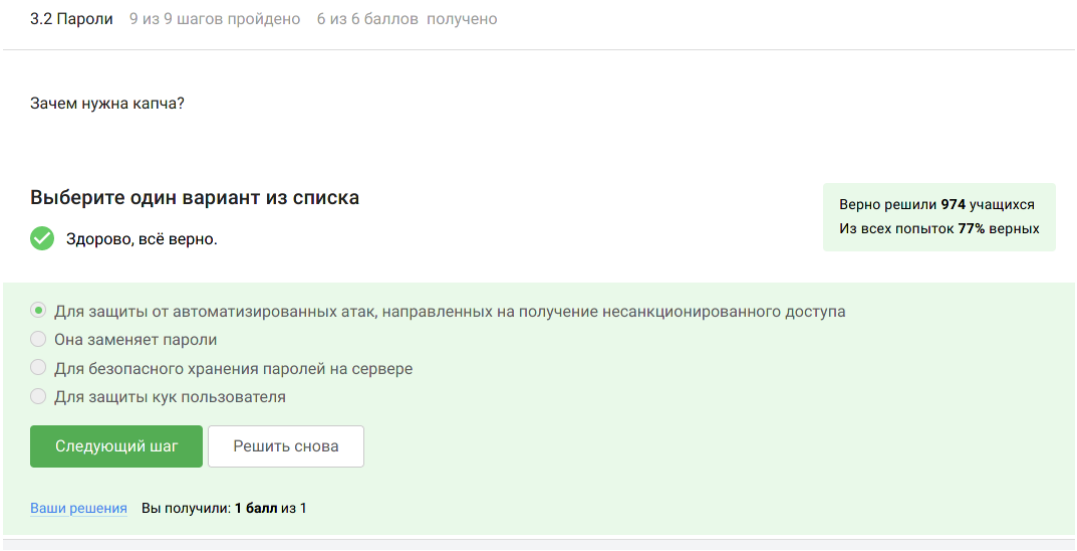

Рис. 11.3: Необходимость капчи

4. Для чего применяется хэширование паролей?:

Для того, чтобы не хранить пароли на сервере в открытом виде. Хэширование паролей применяется для обеспечения безопасности пользовательских данных. Когда пользователь создает учетную запись и устанавливает пароль, этот пароль хэшируется - таким образом, он преобразуется в набор символов, который нельзя прочитать обратно. Этот хэшированный пароль затем сохраняется на сервере. Когда пользователь входит в систему, введенный им пароль также хэшируется и сравнивается с хэшем, хранящимся на сервере.

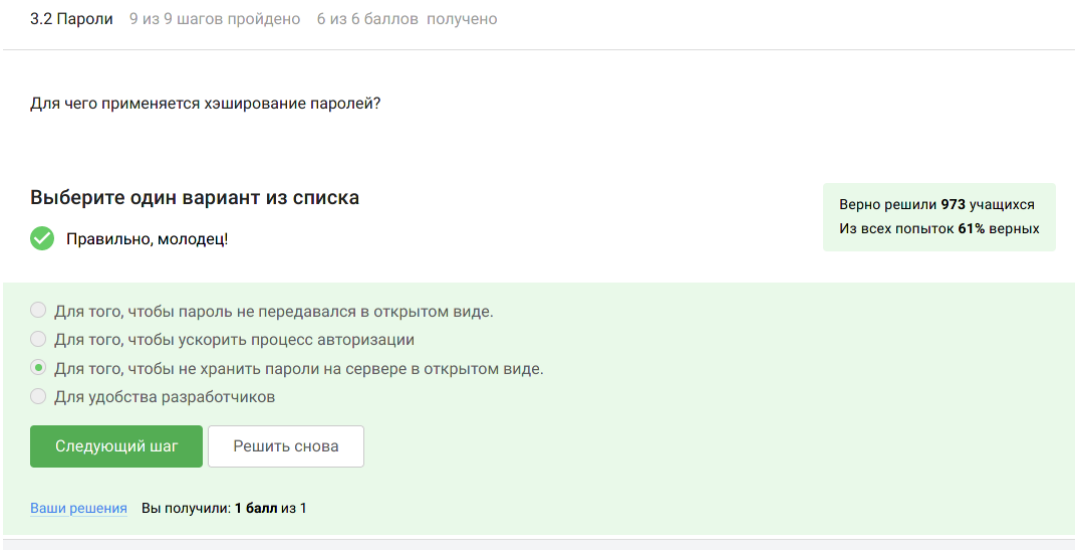

Рис. 11.4: Хэширование паролей

5. Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу?:

Нет, если злоумышленник уже получил доступ к серверу, соль не будет эффективной, потому что она хранится вместе с зашифрованными паролями на сервере. Поэтому, если злоумышленник имеет доступ к серверу, он сможет получить и соль, и зашифрованные пароли, и, возможно, восстановить исходные пароли с помощью атаки перебором.

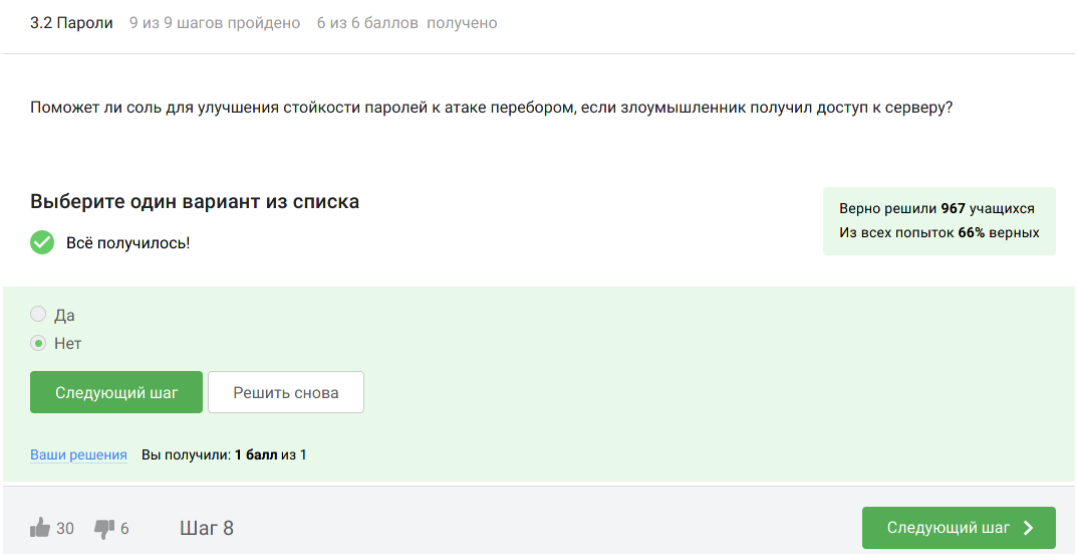

Рис. 11.5: Соль дял улучшения стойкости

6. Какие меры защищают от утечек данных атакой перебором?:

Разные пароли на всех сайтах, Периодическая смена паролей, Сложные(=длинные) пароли, капча. Все варианты верны, в ходе прохождения курса мы в этом убедились.

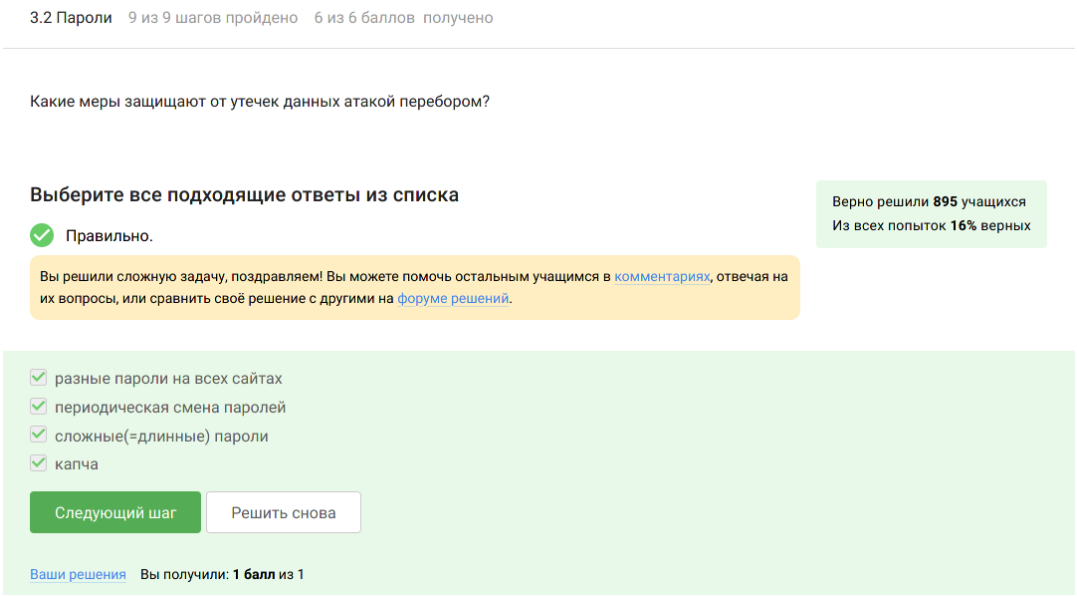

Рис. 11.6: Меры защищают от утечек данных

12 3.3) Фишинг:

1. Какие из следующих ссылок являются фишинговыми?:

https://online.sberbank.wix.ru/CSAFront/index.do (вход в Сбербанк.Онлайн) и https://passport.yandex.ucoz.ru/auth?origin=home_desktop_ru (вход в аккаунт Яндекс). Эти ссылки выглядят как фишинговые, потому что они содержат доменные имена, отличные от официальных доменов Сбербанка и Яндекса. Настоящие сайты Сбербанка и Яндекса имеют другие домены: sberbank.ru и yandex.ru соответственно.

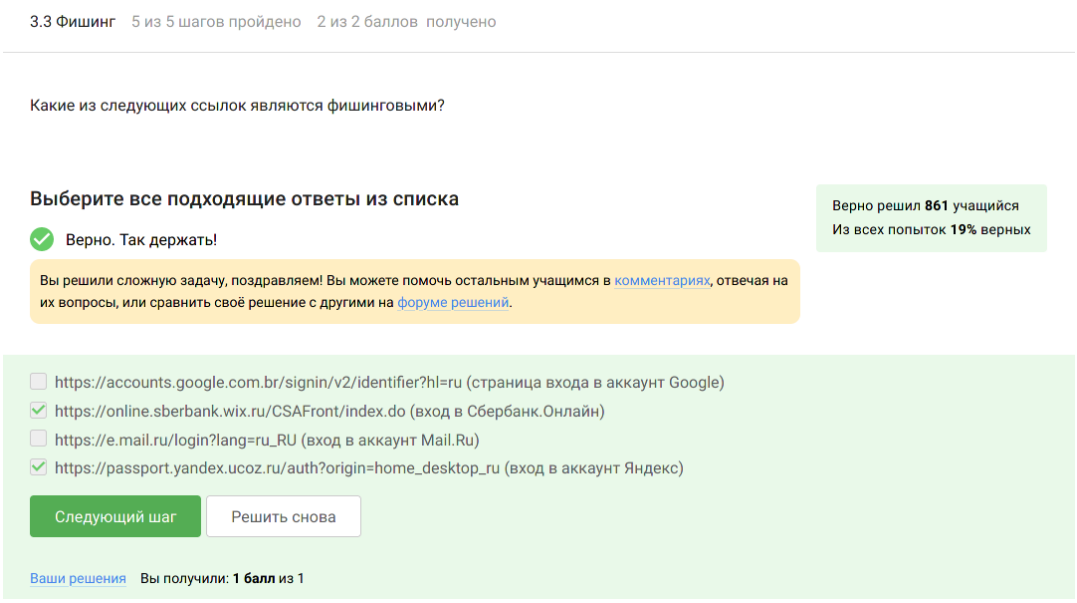

Рис. 12.1: Фишинговые ссылки

2. Может ли фишинговый имейл прийти от знакомого адреса?:

Да, фишинговый имейл может прийти от знакомого адреса. Киберпреступники могут подделывать адреса отправителей, чтобы создать впечатление, что имейлы приходят от знакомых или официальных организаций. Это может включать в себя подделку адресов электронной почты, чтобы выглядеть как отправитель известного человека или компании.

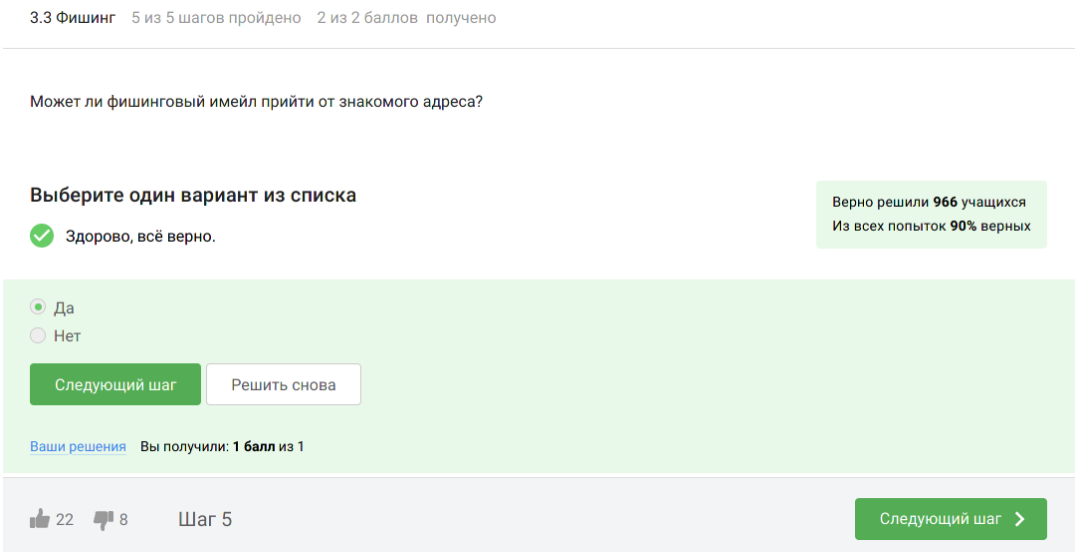

Рис. 12.2: Фишинговый имейл

13 3.4) Вирусы. Примеры:

1. Email Спуфинг – это:

Подмена адреса отправителя в имейлах.

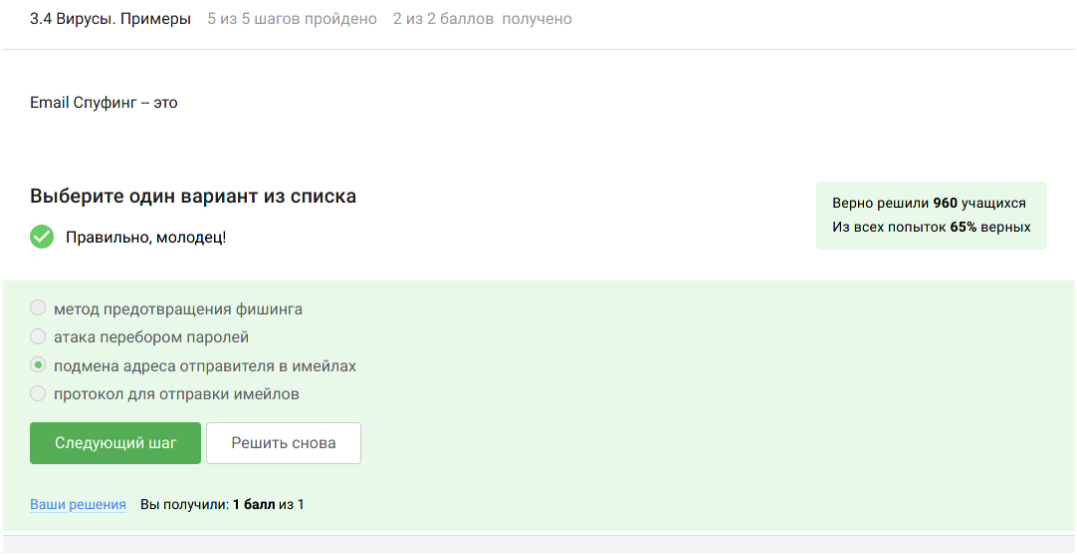

Рис. 13.1: Email Спуфинг

2. Вирус-троян:

Маскируется под легитимную программу. Когда вирус-троян маскируется под легитимную программу, он представляет себя как полезное или безопасное программное обеспечение, чтобы обмануть пользователей и получить доступ к их компьютерам или украсть их конфиденциальные данные.

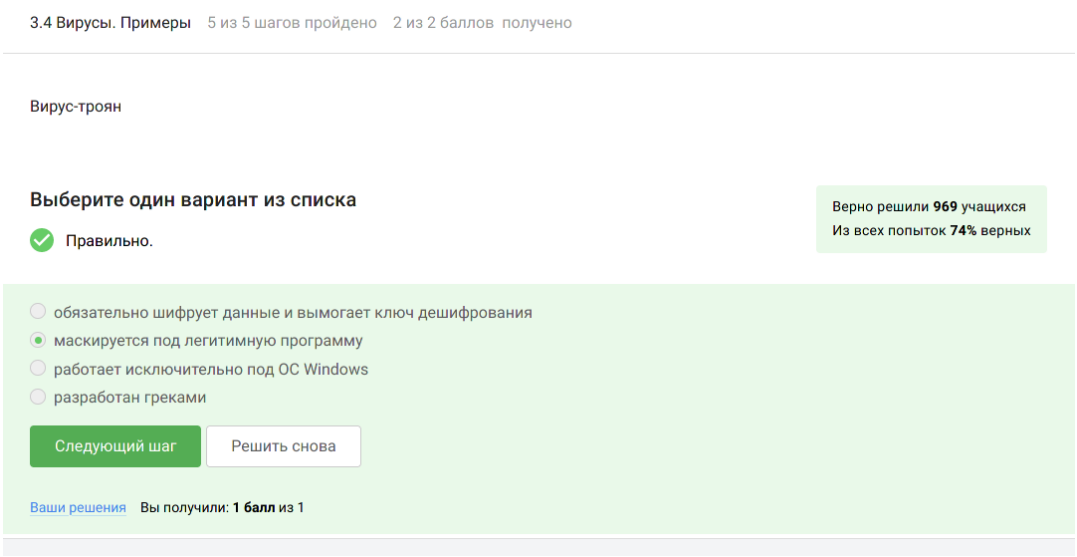

Рис. 13.2: Вирус-троян

14 3.5) Безопасность мессенджеров:

1. На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?:

При генерации первого сообщения стороной-отправителем. Signal использует протокол двухфакторной аутентификации для формирования ключа шифрования при генерации первого сообщения стороной-отправителем. Этот процесс включает в себя обмен ключами Diffie-Hellman, который позволяет сторонам обмениваться секретными ключами, не передавая их по открытым каналам связи. В итоге формируется общий секретный ключ, который используется для шифрования и расшифрования сообщений.

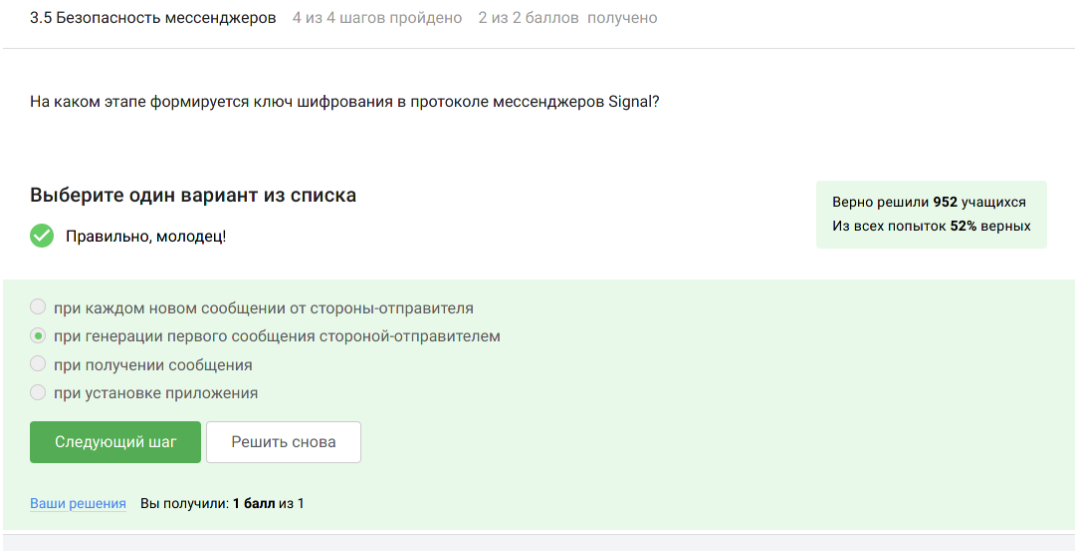

Рис. 14.1: Этап формирования ключа шифрования в протоколе мессенджеров Signal

2. Суть сквозного шифрования состоит в том, что:

Сообщения передаются по узлам связи (серверам) в зашифрованном виде. Сквозное шифрование используется для обеспечения конфиденциальности и безопасности передаваемых сообщений. Каждый узел расшифровывает сообщение только в том случае, если он является адресатом. Это обеспечивает защиту данных во время их передачи по сети.

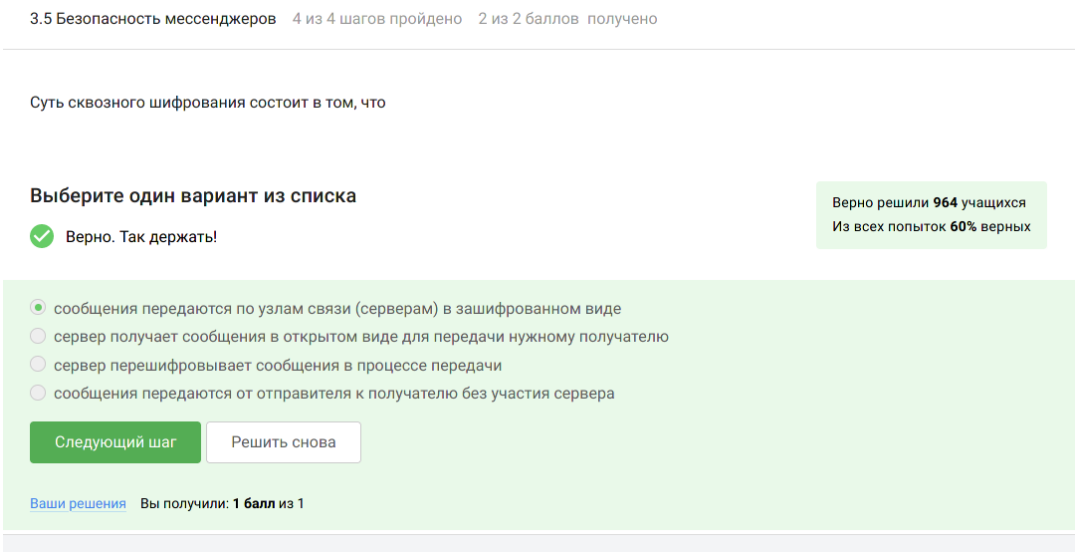

Рис. 14.2: Суть сквозного щифрования

15 Криптография на практике

16 4.1) Введение в криптографию

1. В асимметричных криптографических примитивах?

Обе стороны имеют пару ключей. В асимметричной криптографии каждая сторона имеет два ключа: открытый и закрытый. Открытый ключ используется для зашифрования данных, в то время как закрытый ключ используется для их расшифровки. Использование пары ключей позволяет обеспечить безопасную передачу информации, поскольку один из ключей может быть использован для шифрования сообщения, а другой - для его расшифровки. Этот подход позволяет уменьшить риски компрометации безопасности, поскольку открытый ключ может быть распространен свободно, в то время как закрытый ключ хранится в секрете.

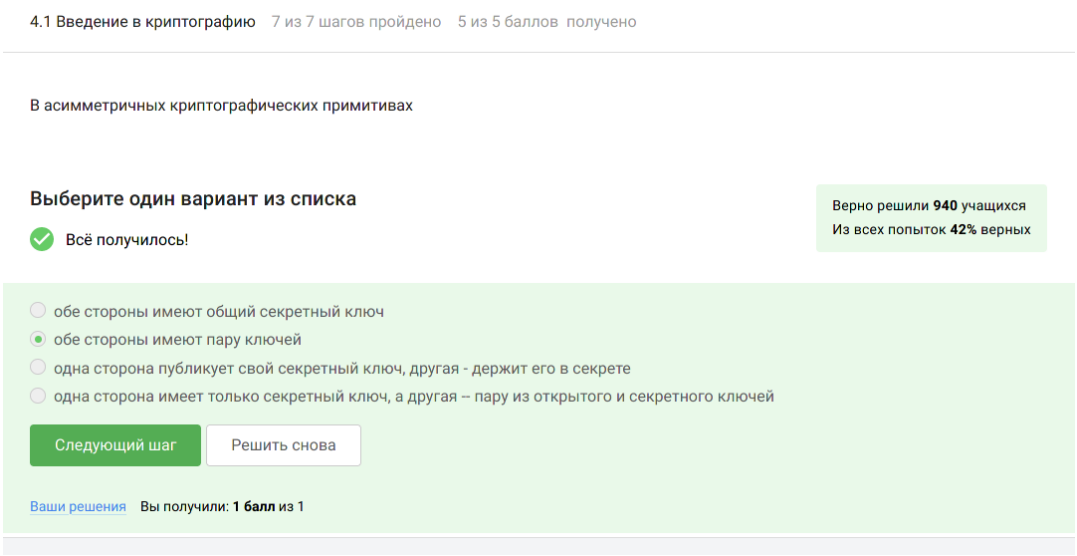

Рис. 16.1: Асимметричные криптографические примитивы

2. Криптографическая хэш-функция:

Стойкая к коллизиям, дает на выходе фиксированное число бит независимо от объема входных данных, эффективно вычисляется. Примитив, который выходит за рамки симметричной и асимметричной криптографии, поскольку он бесключевой. Примером такого криптографического примитива является криптографическая хэш-функция. В науке есть просто хэш-функция, а есть криптографическая хэш-функция. Криптографическая хэш-функция берет на вход произвольный объем данных, то есть какие-то биты и выдает на выходе фиксированную строку, например длины n.

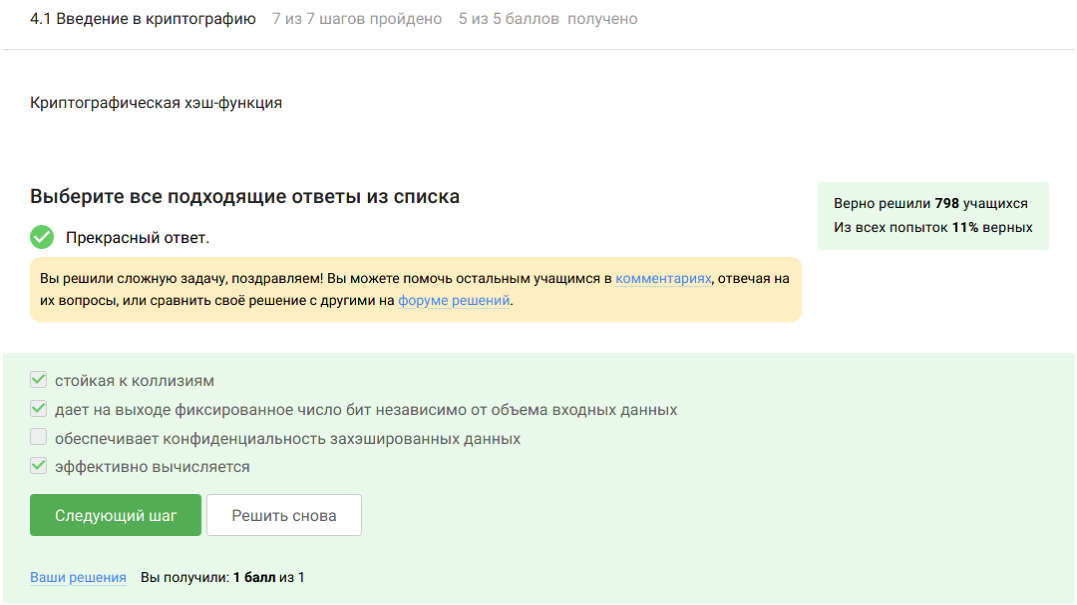

Рис. 16.2: Криптографическая хэш-функция

3. К алгоритмам цифровой подписи относятся:

RSA, ECDSA, ГОСТ Р 34.10-2012. Ежедневное применение цифровой подписи – это сертификаты. К примерам цифровой подписи относятся интернет-сертификаты, подпись RSA, американский стандарт ECDSA и отечественный стандарт ГОСТ стандарт Р 34.20.2012.

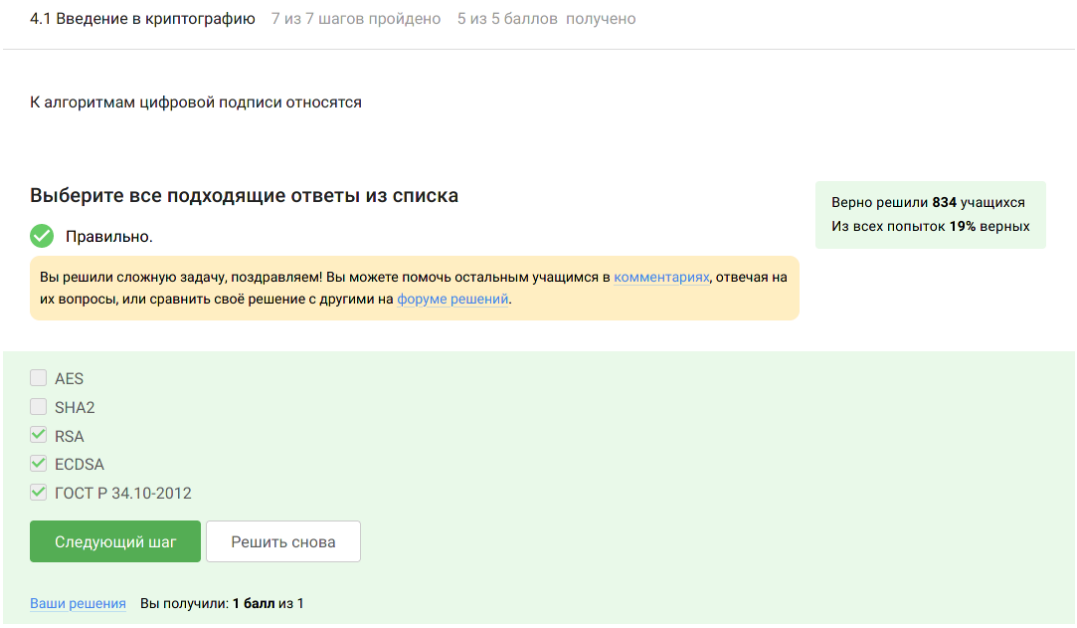

Рис. 16.3: Алгоритмы цифровой подписи

4. Код аутентификации сообщения относится к:

Симметричным примитивам. Как правило, код аутентификации сообщения относится к симметричным примитивам криптографии, поскольку он использует один и тот же секретный ключ для создания и проверки подписи сообщения. В отличие от асимметричной криптографии, где используются пары открытого и закрытого ключей, симметричная криптография применяет только один общий ключ.

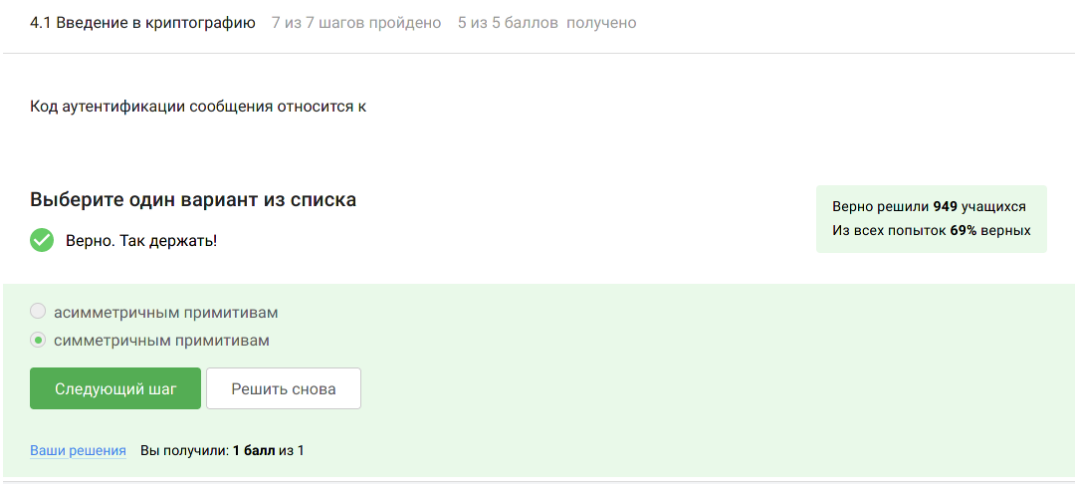

Рис. 16.4: Код аутентификации сообщения

5. Обмен ключам Диффи-Хэллмана - это:

Асимметричный примитив генерации общего секретного ключа. Этот метод использует асимметричное шифрование, где каждая сторона генерирует свой закрытый и открытый ключи. Стороны обмениваются открытыми ключами, после чего они могут вычислить общий секретный ключ, который будет использоваться для шифрования и дешифрования сообщений между ними.

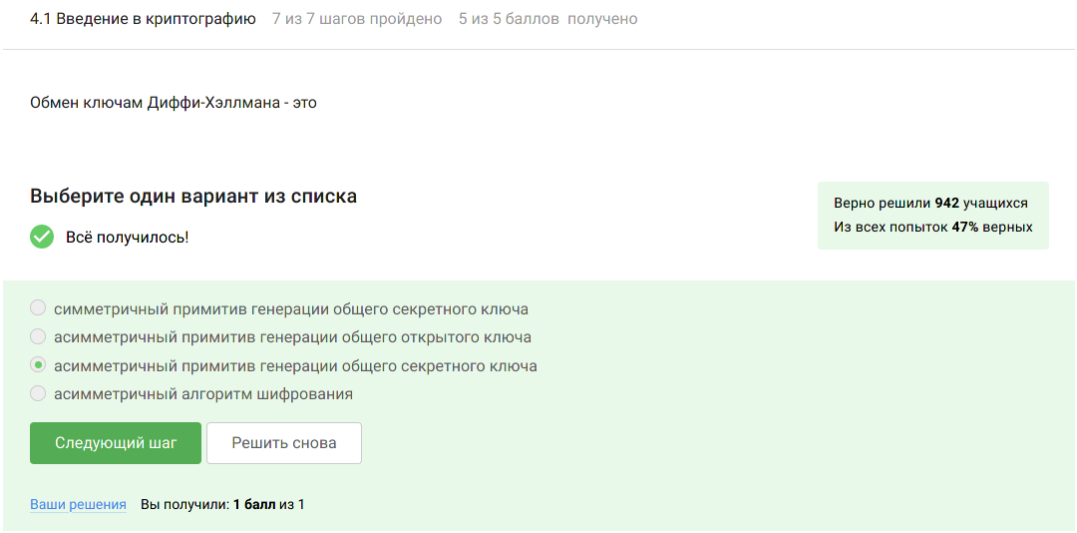

Рис. 16.5: Обмен ключам Диффи-Хэллмана

17 4.2) Цифровая подпись:

1. Протокол электронной цифровой подписи относится к:

Протоколам с публичным (или открытым) ключом. Протокол электронной цифровой подписи относится к протоколам с публичным (или открытым) ключом, так как он использует асимметричное шифрование. В этом случае у каждого участника есть пара ключей: закрытый и открытый. Закрытый ключ известен только владельцу, а открытый ключ может быть распространен публично. При создании электронной цифровой подписи сообщения подписывается закрытым ключом отправителя, а затем можно проверить подлинность подписи с помощью открытого ключа получателя.

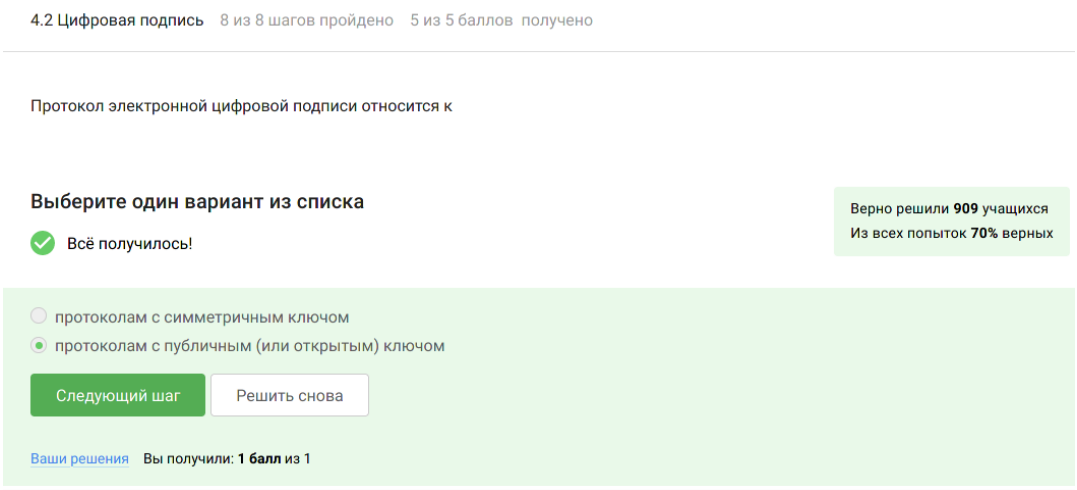

Рис. 17.1: Протокол электронной цифровой подписи относится к

2. Алгоритм верификации электронной цифровой подписи требует на вход:

Подпись, открытый ключ, сообщение. Алгоритм верификации электронной цифровой подписи использует подпись, открытый ключ и сообщение для проверки подлинности и целостности данных. Когда получатель получает подпись и сообщение, он использует открытый ключ отправителя для проверки подписи. Алгоритм проверяет, что подпись действительно была создана закрытым ключом отправителя и что данные не были изменены после создания подписи.

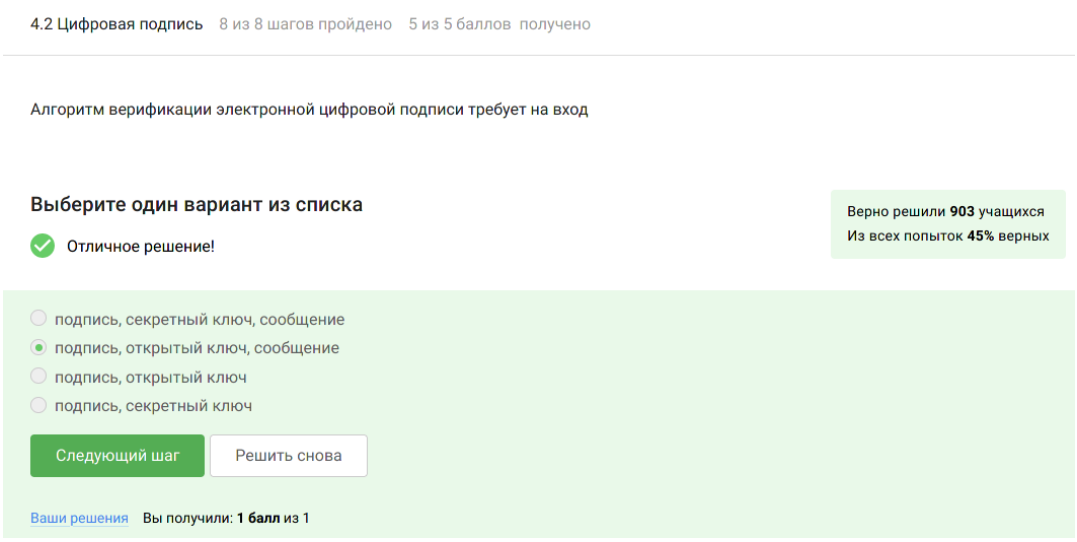

Рис. 17.2: Требования на вход

3. Электронная цифровая подпись не обеспечивает:

Конфиденциальность. Она предназначена для проверки подлинности и целостности данных, а не для их защиты от несанкционированного доступа. Для обеспечения конфиденциальности данных необходимо использовать другие методы, такие как шифрование. Шифрование позволяет скрыть содержимое сообщения от посторонних лиц, в то время как электронная цифровая подпись обеспечивает возможность проверки авторства и целостности данных.

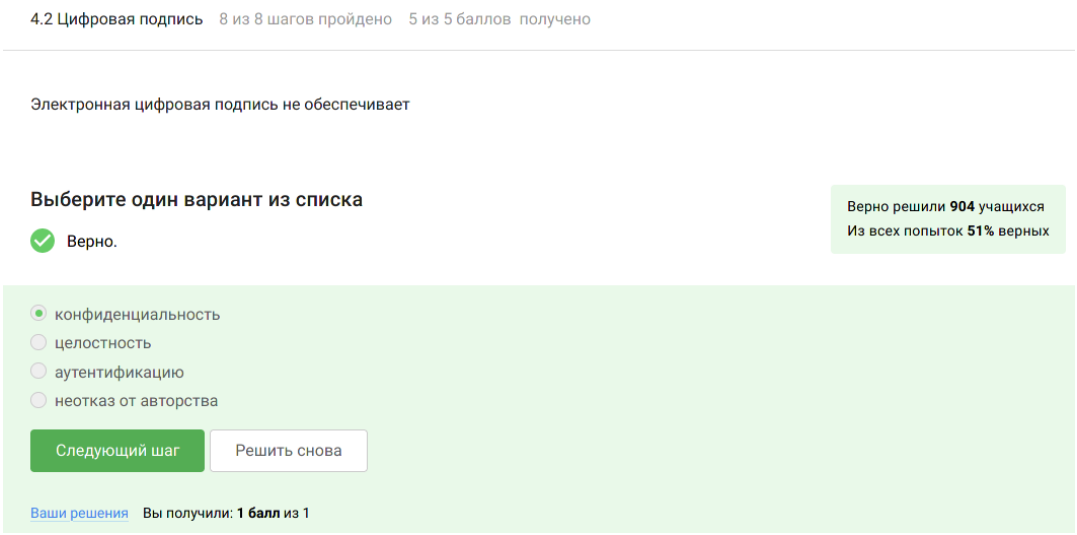

Рис. 17.3: Электронная цифровая подпись не обеспечивает

4. Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?:

Усиленная квалифицированная. Усиленная квалифицированная электронная подпись (ЭП) - это самый высокий уровень сертификата электронной подписи, который обеспечивает наивысший уровень безопасности и подлинности. Для отправки налоговой отчетности в Федеральную налоговую службу (ФНС) требуется использование усиленной квалифицированной ЭП. Такой сертификат подтверждает личность владельца ЭП и его право действовать от имени организации или индивидуального предпринимателя.

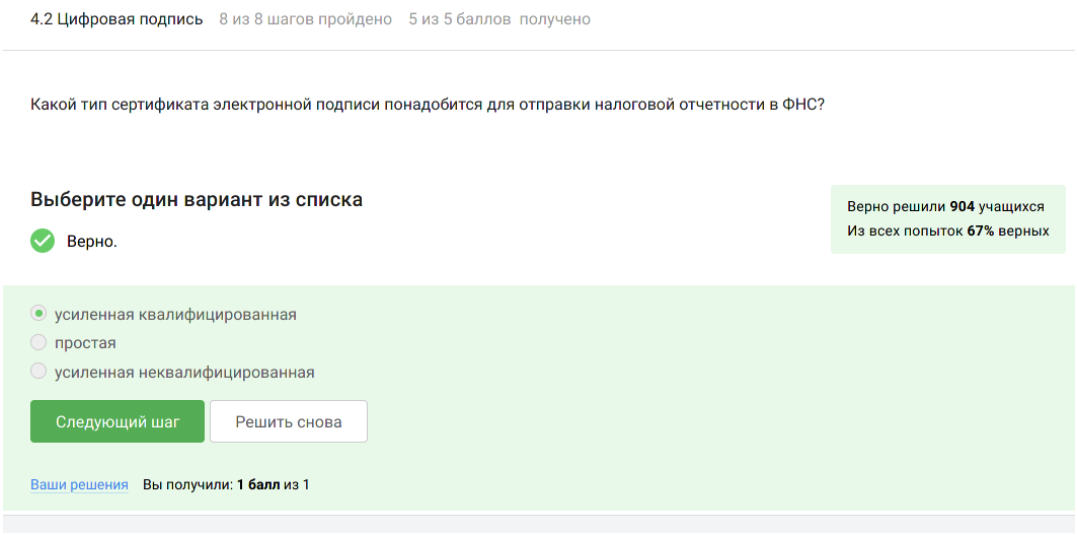

Рис. 17.4: Тип сертификата электронной подписи для налоговой отчетности ФНС

5. В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?:

В удостоверяющем (сертификационном) центре. Квалифицированный сертификат ключа проверки электронной подписи можно получить в удостоверяющем (сертификационном) центре. Удостоверяющие центры выпускают сертификаты, подтверждающие подлинность и квалификацию электронной подписи, что позволяет использовать ее для юридически значимых документов и процессов, включая отправку налоговой отчетности в налоговые органы.

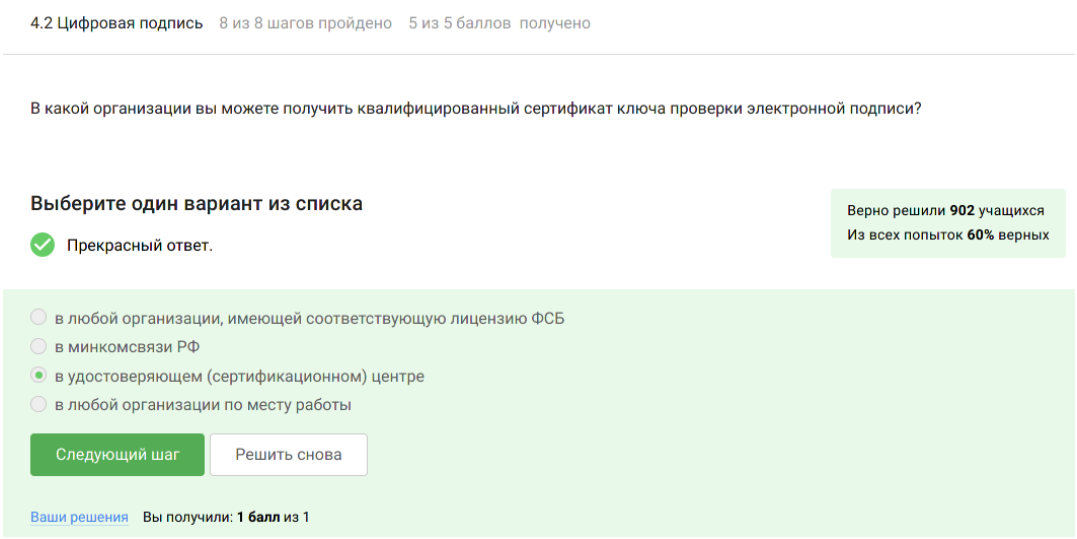

Рис. 17.5: Организация для выдачи сертификатов

18 4.3) Электронные платежи

1. Выберите из списка все платежные системы:

MasterCard и МИР, самые распространненые платежные системы.

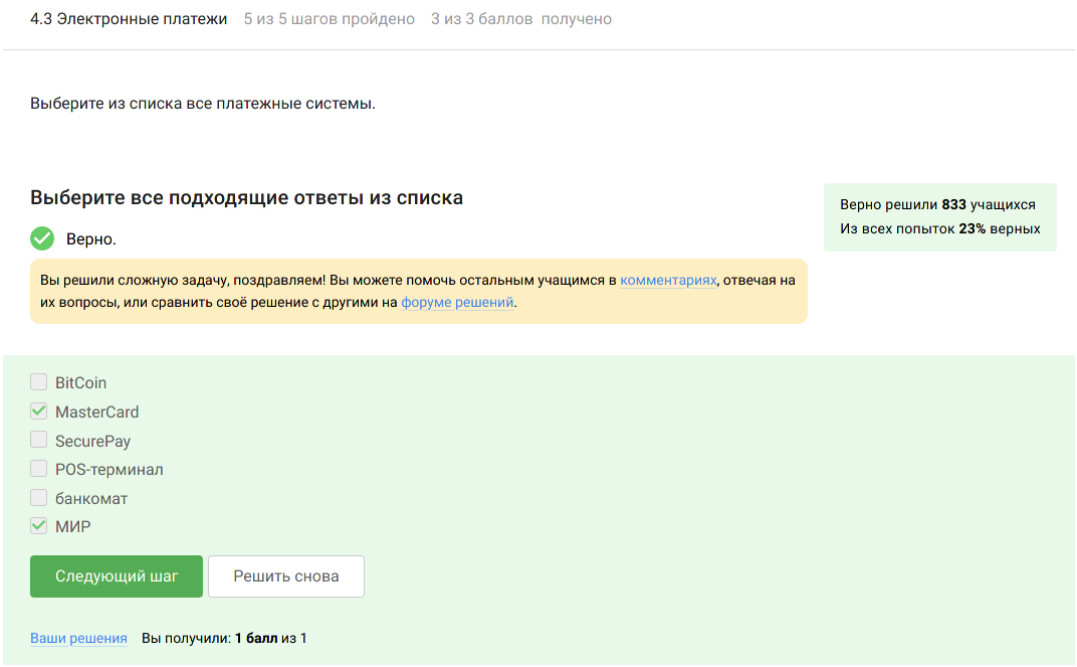

Рис. 18.1: Платежные системы

2. Примером многофакторной аутентификации является:

Комбинация проверка пароля + код в sms сообщении и комбинация код в sms сообщении + отпечаток пальца. Многофакторная аутентификация представляет собой процесс проверки личности пользователя с использованием нескольких различных методов подтверждения.

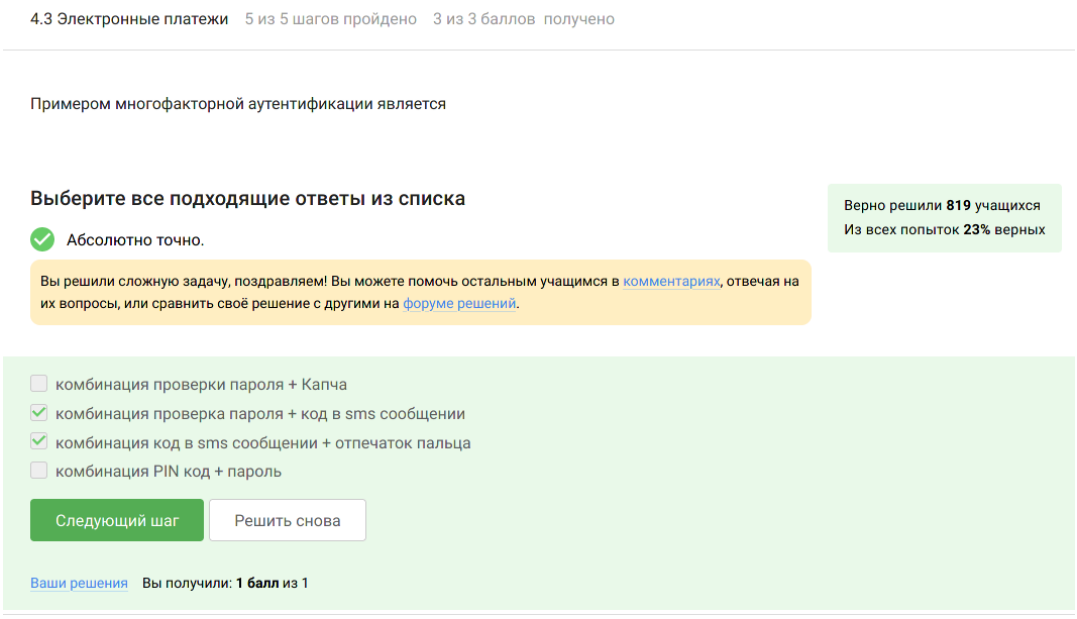

Рис. 18.2: Многофакторнуя аутентификация

3. При онлайн платежах сегодня используется:

Многофакторная аутентификация покупателя перед банком-эмитентом. Многофакторная аутентификация покупателя перед банком-эмитентом означает, что для завершения транзакции покупатель должен пройти процесс проверки личности с использованием нескольких различных методов подтверждения перед своим банком-эмитентом. Это делается для повышения безопасности онлайн платежей и защиты от мошенничества.

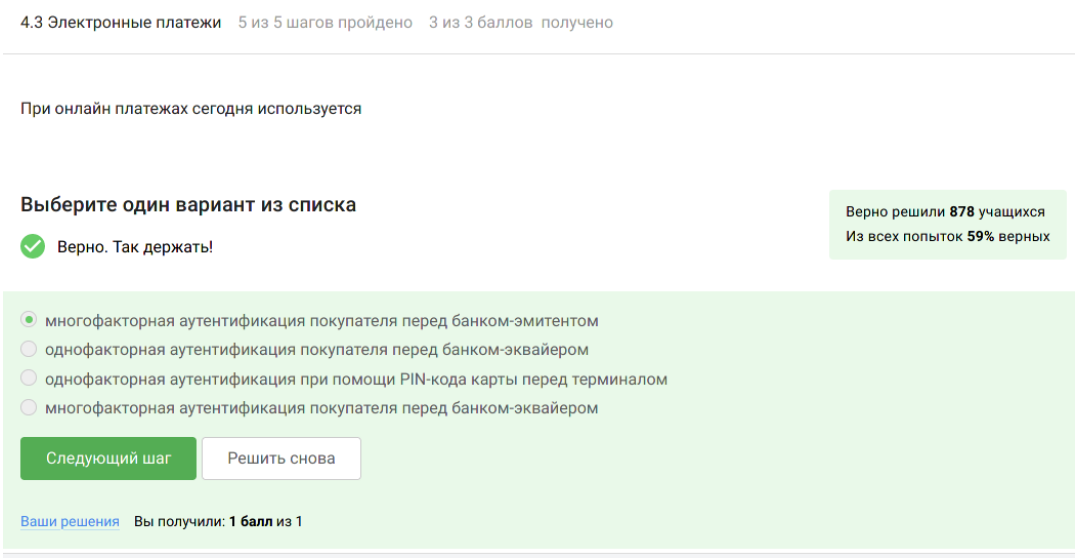

Рис. 18.3: Онлайн платежи

19 4.4) Блокчейн

1. Какое свойство криптографической хэш-функции используется в доказательстве работы?:

Сложность нахождения прообраза. Свойство криптографической хэш-функции, которое используется в доказательстве работы (Proof of Work), это сложность нахождения прообраза. Криптографическая хэш-функция преобразует входные данные произвольной длины в фиксированную строку определенной длины (хэш). Однако, важной характеристикой криптографической хэш-функции является то, что она должна быть устойчива к обратному поиску - то есть, при известном хэше сложно найти исходные данные (прообраз), которые привели к этому хэшу.

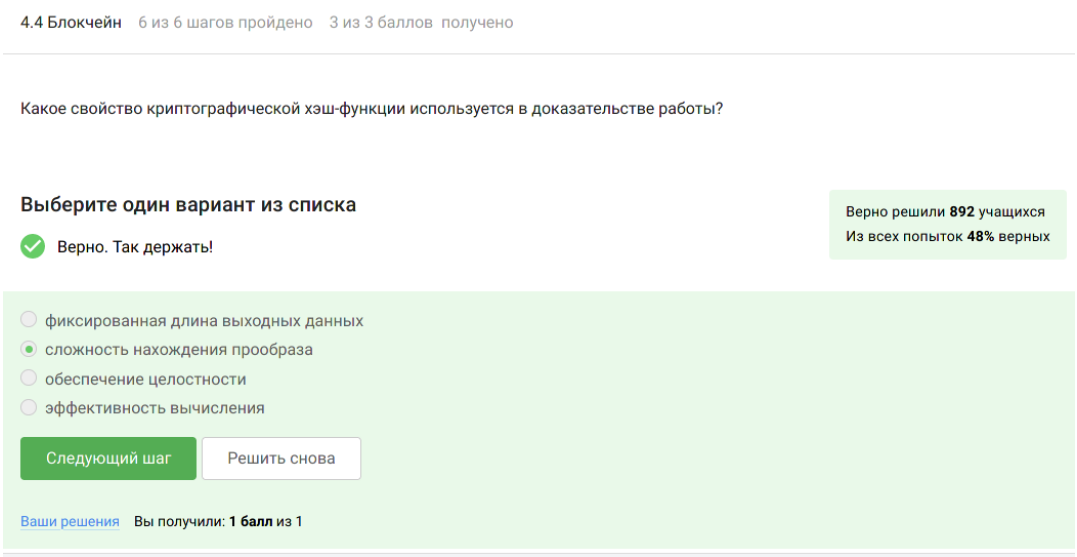

Рис. 19.1: Доказательство функции

2. Консенсус в некоторых системах блокчейн обладает свойствами:

Консенсус, живучесть, открытость, постоянства. Консенсус в системах блокчейн означает достижение единства и согласия между всеми участниками сети относительно правильности и последовательности транзакций. Это важное свойство обеспечивает работоспособность и надежность блокчейн-сети.

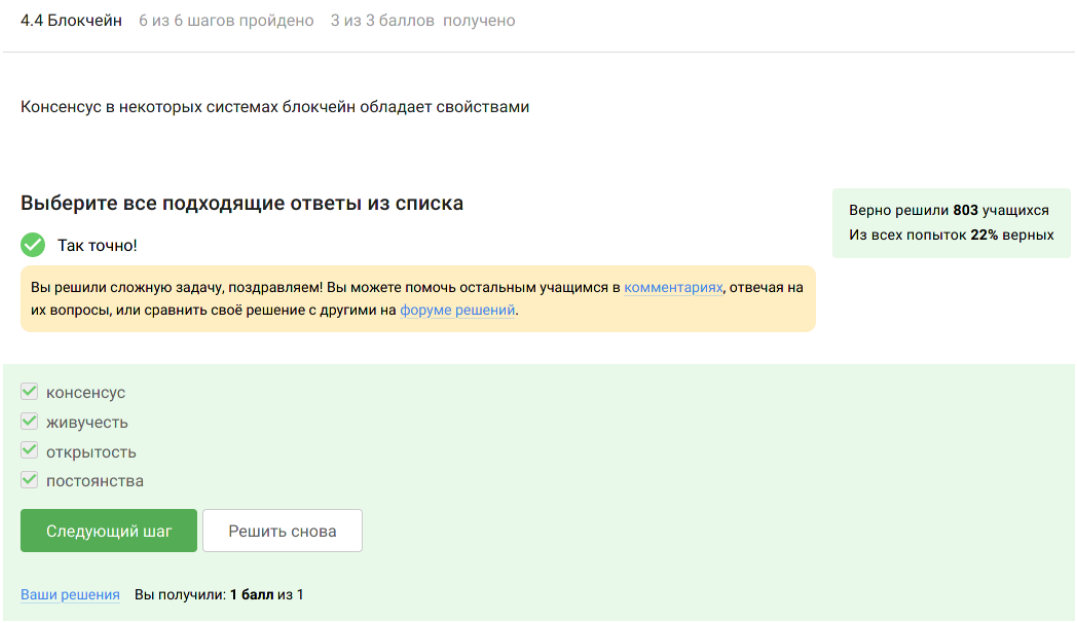

Рис. 19.2: Свойства консенсуса в системах блокчейна

3. Секретные ключи какого криптографического примитива хранят участники блокчейна?:

Цифровая подпись. Участники блокчейна хранят секретные ключи для использования в криптографической подписи. Цифровая подпись - это криптографический примитив, который используется для аутентификации и подтверждения подлинности цифровой информации. При проведении транзакций в блокчейне участники создают цифровую подпись, используя свой секретный ключ, чтобы подтвердить свое согласие на выполнение операции.

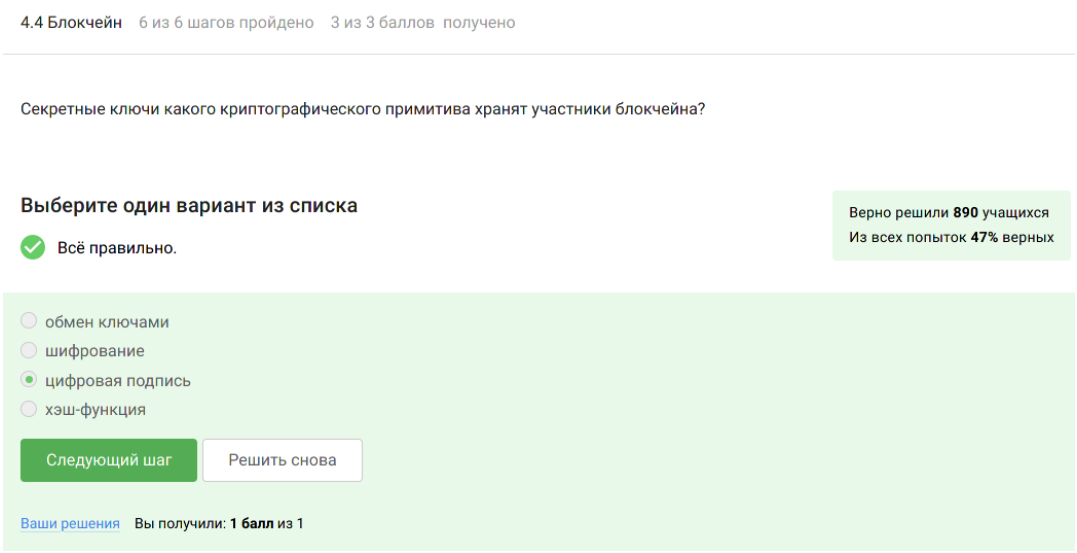

Рис. 19.3: Секретные ключи

20 Выводы

Кибербезопасность также стала важной темой для многих образовательных программ. Университеты и колледжи по всему миру активно включают курсы по кибербезопасности в свои программы, понимая актуальность и востребованность данной профессии в современном мире.

В целом, кибербезопасность является многогранной проблемой, требующей постоянного внимания, инноваций и адаптации к меняющемуся цифровому миру.

В заключение можно сказать, что вопросы кибербезопасности требуют комплексного подхода, включая технические, организационные и образовательные меры. Только совместные усилия могут обеспечить адекватный уровень защиты в условиях постоянно меняющегося цифрового ландшафта.

В этой работе я: - поняла, как работает Интернет, и какие у него “слабые” места

- уяснила, почему 1245YOURNAME – плохой пароль
- научилась отличать шифрование от электронной подписи
- узнать, как работают электронные платежи