# Отчёт по прохождению контрольных мероприятий дополнительного курса

**Основы информационной безопасноти Соловьев Богдан НКАбд-04-23**

1

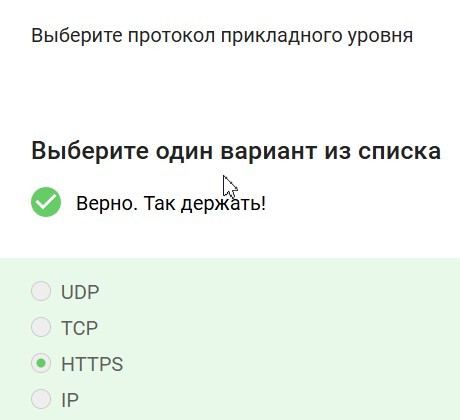
# Содержание

1. Вторая глава
2. Третья глава
3. Четвёртая глава

2

# Вторая глава: Безопасность в сети

3



UDP (User Datagram Protocol) — это один из основных протоколов для передачи данных в сети. Он не нуждается в установлении соединения перед передачей данных и не гарантирует их

доставку. 4

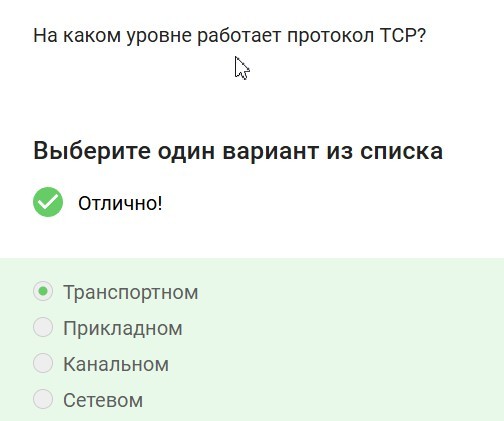
Проще говоря, UDP используется в случаях, когда важнее снизить задержки, чем обеспечить полную надёжность доставки.

TCP (Transmission Control Protocol) — протокол обмена сообщениями в сети Интернет. Он управляет отправкой данных и следит за тем, чтобы они дошли до получателя в целости.

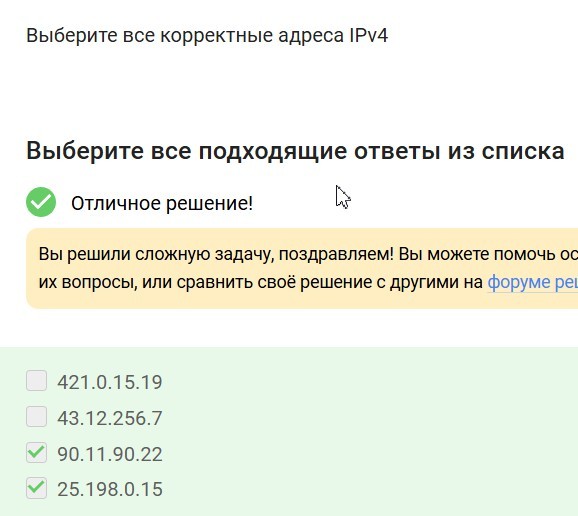
HTTP (HyperText Transfer Protocol) — это протокол для передачи информации в интернете. Он является основой для обмена информацией между веб-браузерами и серверами.

С помощью HTTP пользователи получают доступ к веб-страницам, загружают файлы и отправляют данные через интернет.

5

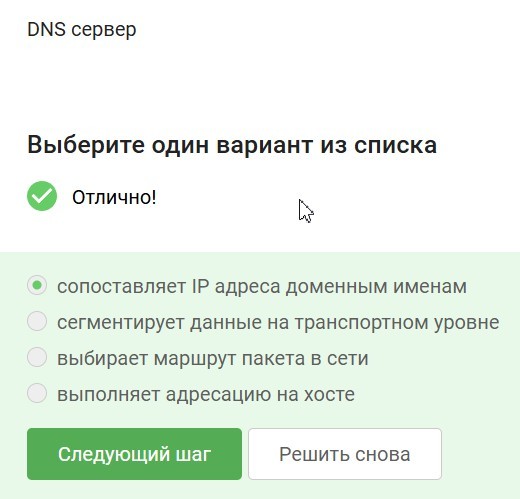


6

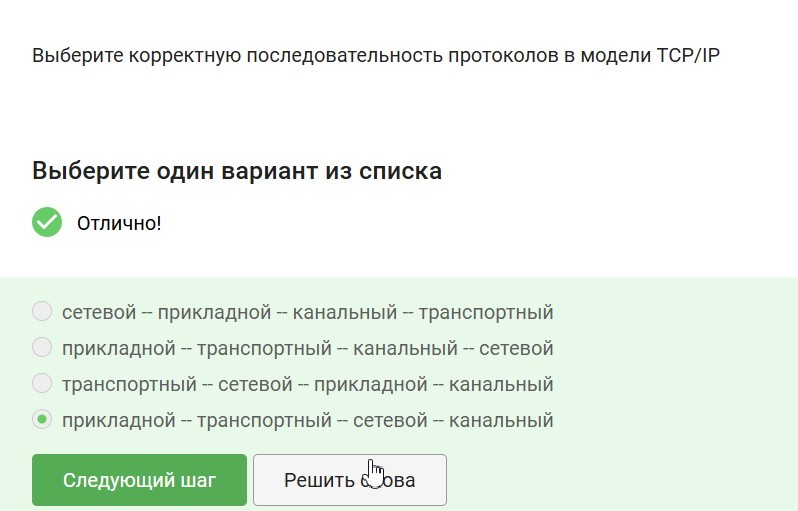


Значения не могут первышать 255 в десятичной системе

исчисления 7



8



Корректная последовательность уровней системы протоколов

TCP/IP выглядит следующим образом:

9

Канальный уровень. Отвечает за взаимодействие по сетевому оборудованию, например по Ethernet-кабелю или Wi-Fi. Примеры протоколов: Ethernet, Wi-Fi, Bluetooth.

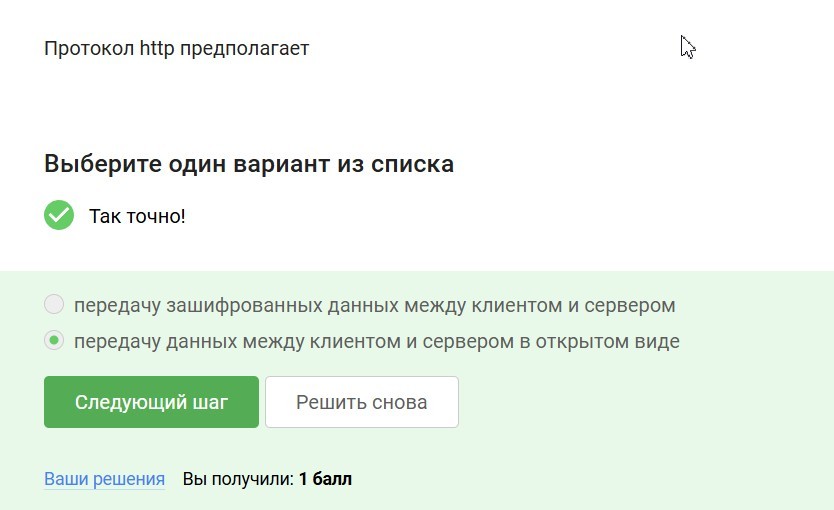
Межсетевой уровень. Помогает отдельным сетям общаться друг с другом. Основной протокол — IP (Internet Protocol). Здесь также работают такие дополнительные протоколы, как ICMP, ARRP и DHCP.

Транспортный уровень. Отвечает за передачу данных между устройствами, например, по протоколам TCP и UDP.

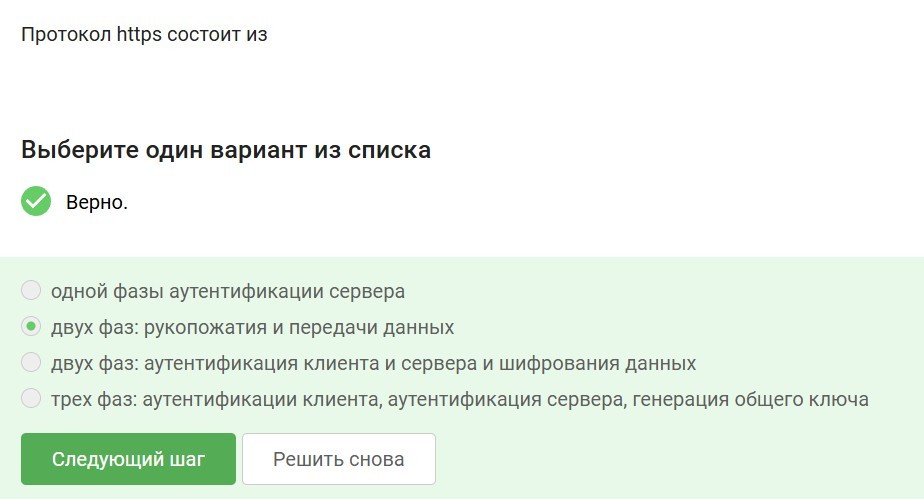
10

Прикладной уровень. Помогает приложениям общаться друг с другом с помощью интерфейсов или API. Содержит набор протоколов, которые отвечают за работу различных сервисов, таких как HTTP для веб-страниц, SMTP для электронной почты и FTP для передачи файлов.

11

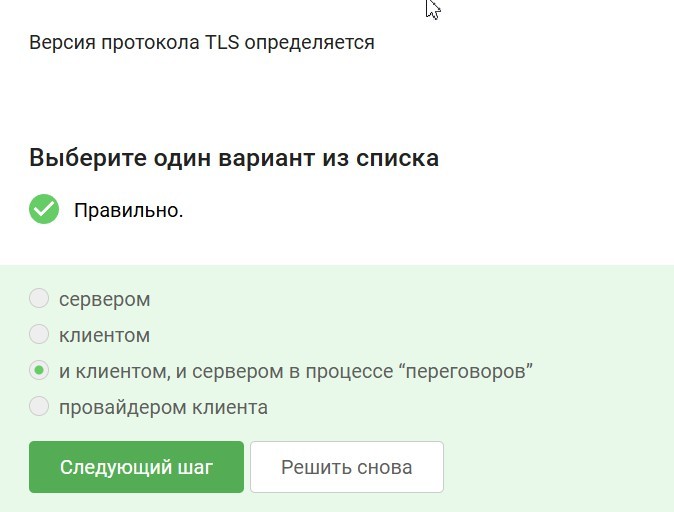


12

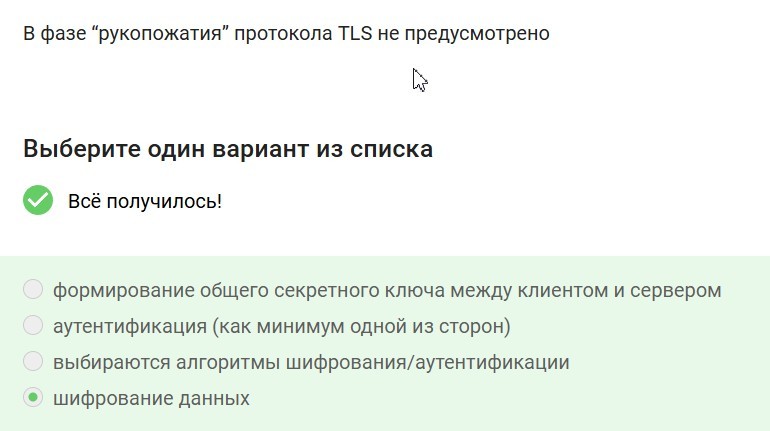


HTTP (HyperText Transfer Protocol) — это протокол прикладного уровня, который используется для передачи данных в сети Интернет. Он определяет правила и формат обмена данными между клиентом (например, веб-браузером) и сервером

13



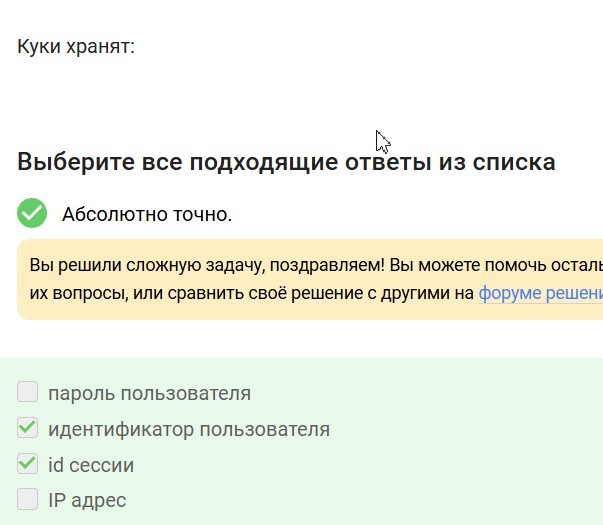
14



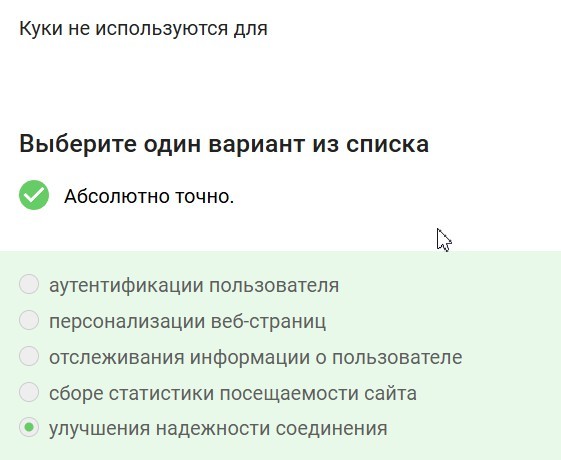
В фазе рукопотажия происходит:

1. выбор параметров, протоколов
2. аутентификация (как минимум, сервера)
3. формируется общий секретный ключ K

15



16



Сбор куки упрощает и делает комфортным взаимодействие с веб- ресурсом. Благодаря им не требуется заново заходить в свой аккаунт в соцсетях или собирать корзину в интернет-магазинах.

17

Какую информацию собирают куки-файлы:

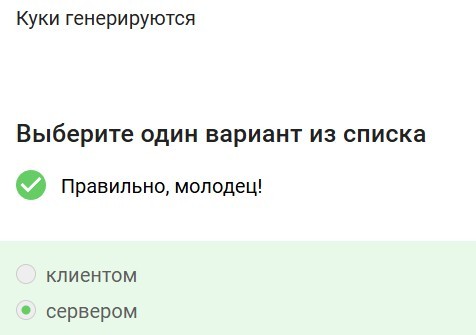
Учётные данные. Cookies помогают отмечать, что пользователь уже был авторизован ранее. Благодаря этому не нужно каждый раз заново входить в личный кабинет при открытии или обновлении страницы. Даже если у пользователя нет учётной записи, сайт может присвоить ему уникальный идентификатор, чтобы в следующий раз «узнать» посетителя.

Персональные настройки. Сайты запоминают выбранный город,

язык, товары в корзине, валюту и масштаб страницы. Эти данные собирают интернет-магазины. Они нужны, чтобы автоматически подставлять нужную валюту, город доставки и содержимое корзины с товарами. Благодаря этому пользователи могут в любой

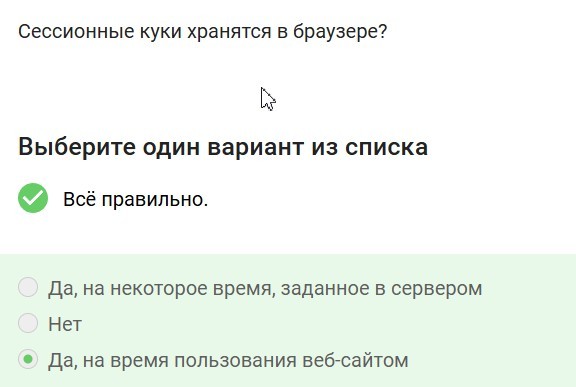
момент быстро продолжить покупки.

18

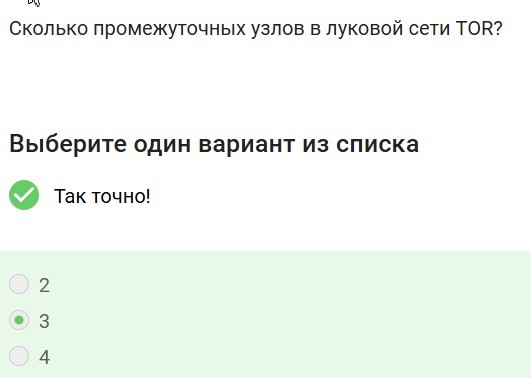


Куки генерируются сервером, чтобы запомнить пользователя и показать ему ответ в соответствии с его предпочтениями при повторном посещении веб-сайта

19

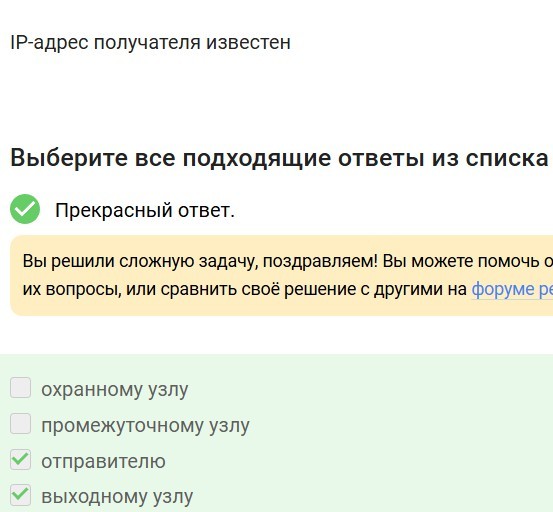


20



количество узлов задано жёстко в коде программы и не изменяется через конфигурационные файлы. Длина цепочки из трёх узлов оптимальна, так как наиболее опасными считаются атаки пересечения, которые эффективны при съёме трафика с начального узла (или перед ним) и с конечного узла (или после

него). 21



Узлы разделяются на охранный узел, промежуточный и выходной. Соответственно выходной узел, поскольку он является узлом перед получателем, знает, кому направлен пакет.

22

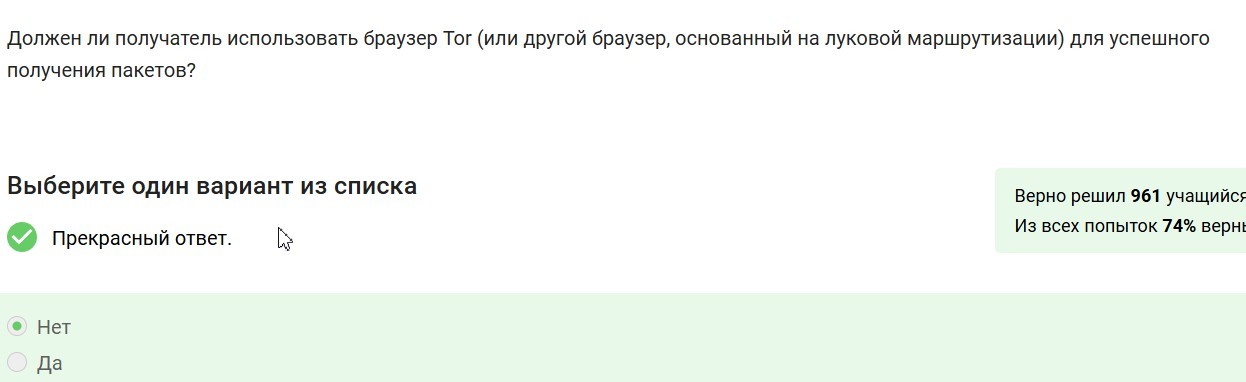
Охранный узел знает, от кого пришёл пакет, поскольку он непосредственно является следующим узлом после отправителя, в то время как промежуточный узел не знает ни от кого этот пакет, ни кому он предназначен. В браузере Tor всегда есть три роутера, их не больше и не меньше. Их не меньше потому, что меньшего числа узлов не хватает для анонимизации, а большее число узлов не дает большую анонимизацию, поэтому выбирается всегда 3 луковых роутера.

23



пояснение выше

24

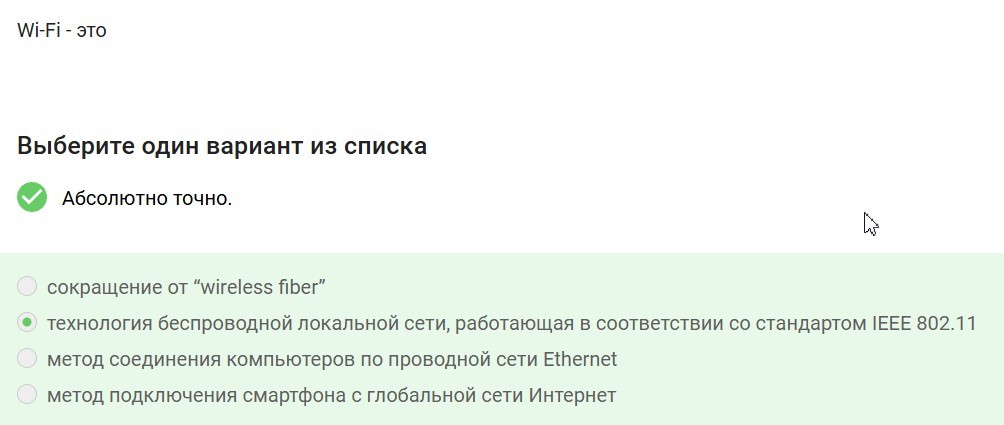


Получателю не обязательно использовать браузер Tor или другой луковый браузер для успешного получения пакетов.

25

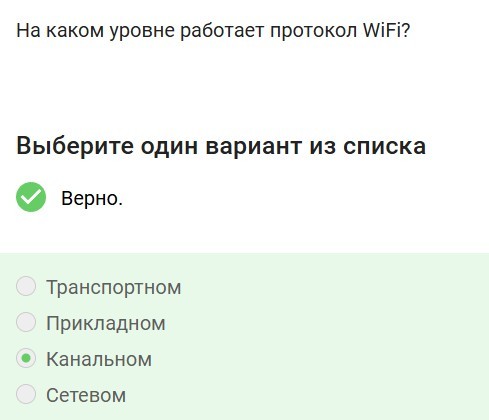
Tor скрывает маршрутизацию и обеспечивает анонимность, но сам протокол передачи данных (например, TCP/IP) работает независимо от того, использует ли получатель Tor. Главное — чтобы отправитель правильно указал адрес получателя, а сеть обеспечила доставку пакетов.

26



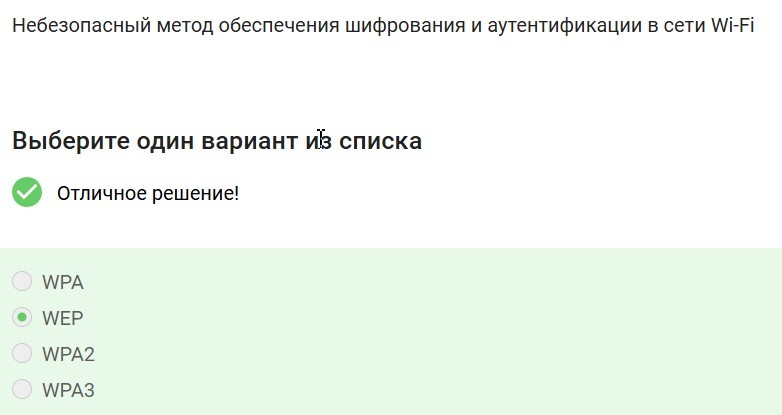
Можно догаться методом исключения

27



Канальный уровень — это второй уровень модели OSI, который объединяет устройства в одной локальной сети, например компьютеры, принтеры и коммутаторы. Его функция — правильно передать данные между этими узлами.

28



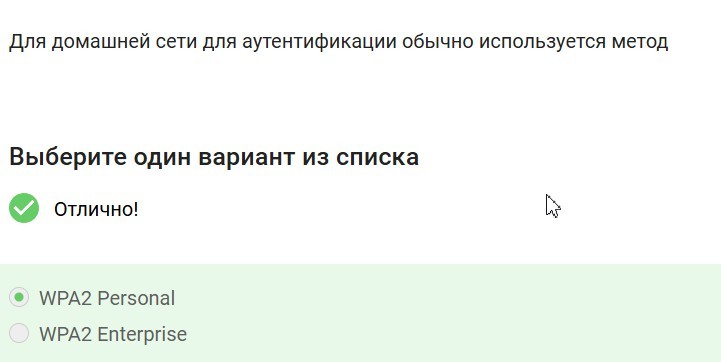
WEP (Wired Equivalent Privacy) — один из старейших протоколов безопасности беспроводных сетей. Он был разработан в конце 1990-х годов как способ защиты беспроводных сетей и призван обеспечить уровень безопасности, эквивалентный проводным сетям.

29



В большинстве домашних и офисных сетей данные между устройством (компьютером, смартфоном) и роутером передаются в открытом виде, если не используется дополнительное

шифрование 30

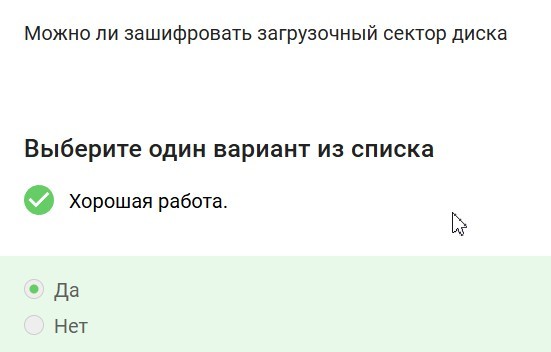


Enterprise используется когда есть база данных пользователей

31

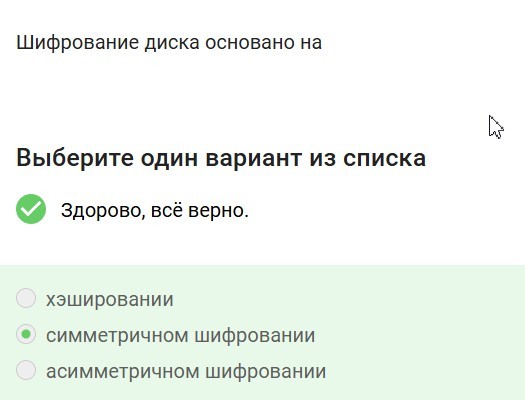
# Третья глава: Защита ПК/телефона

32



Можно

33

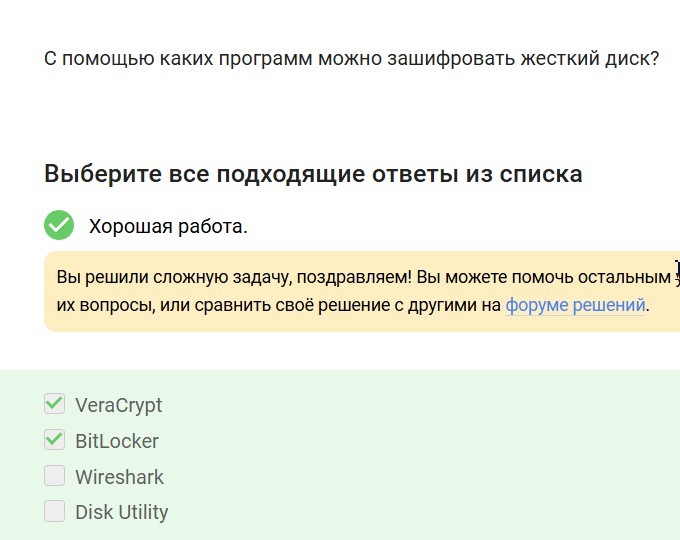


Симметричное шифрование — это метод, при котором для шифрования и дешифрования данных используется один и тот же ключ. То есть и отправитель, и получатель информации должны иметь одинаковый секретный ключ, чтобы зашифровать и расшифровать сообщения.

34

Асимметричное шифрование — это метод, в котором используются два ключа: открытый (публичный) и закрытый (приватный). 12 Открытый ключ используется для шифрования, а закрытый — для дешифрования. В отличие от симметричного метода, ключи не совпадают, что делает возможным обмен информацией без предварительного обмена секретами

35

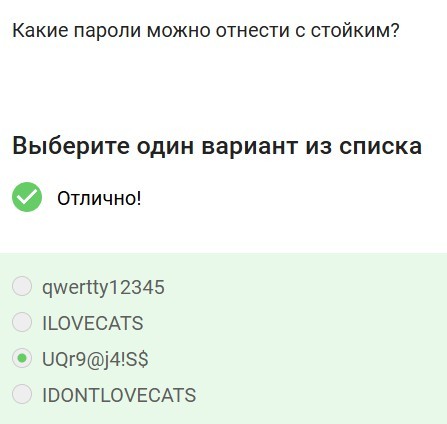


Wireshark — бесплатная профессиональная программа для анализа сетевой активности, изучения пакетов, просмотра сетевой статистики и составления отчётов.

36

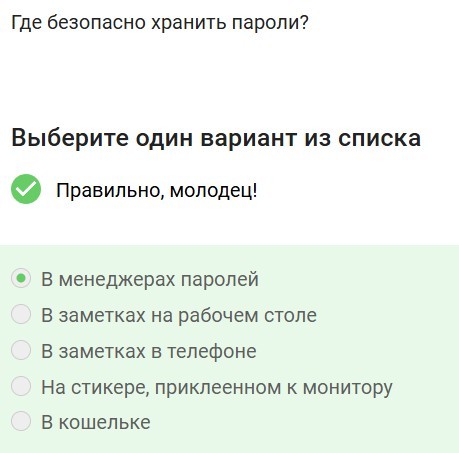
Disk Utility — утилита для работы с файловыми системами жёстких и оптических дисков в macOS. Но зашифровать не получится с её помощью

37



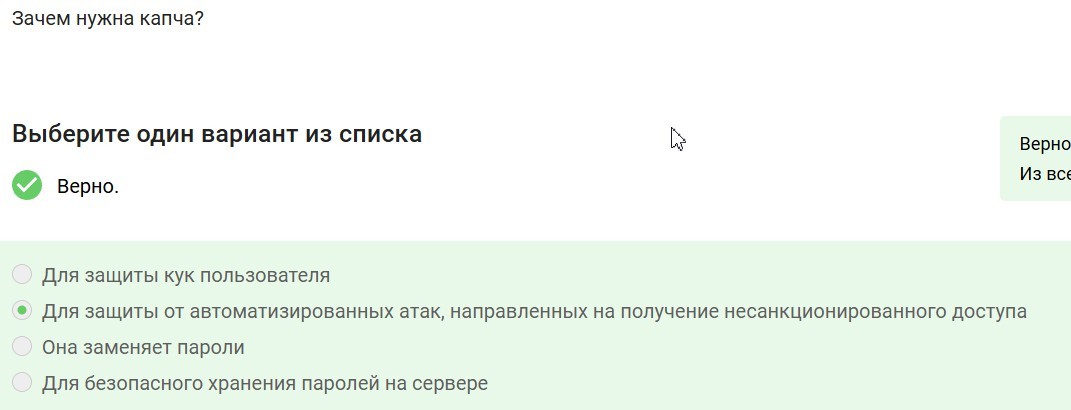
Хороший пароль должен содержать цифры, буквы в разных регистрах, специальные знаки и быть длинным

38



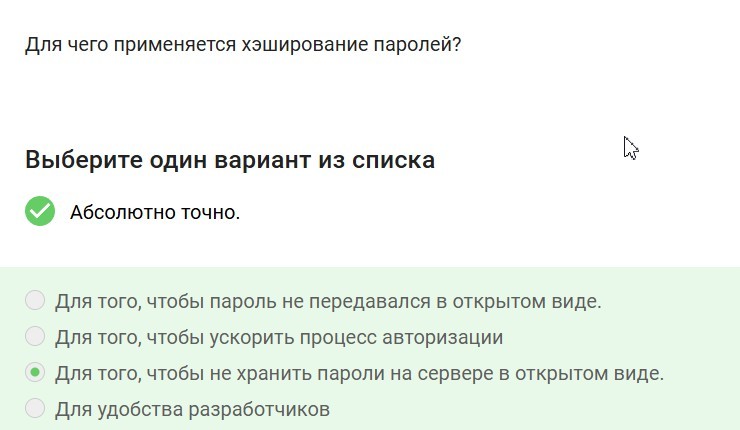
Пароли нельзя хранить в заметках, потому что эти программы никак дополнительно не защищены, в кошельке и на стикере не

стоит хранить, потому что, по личному опыту, легко потерять 39



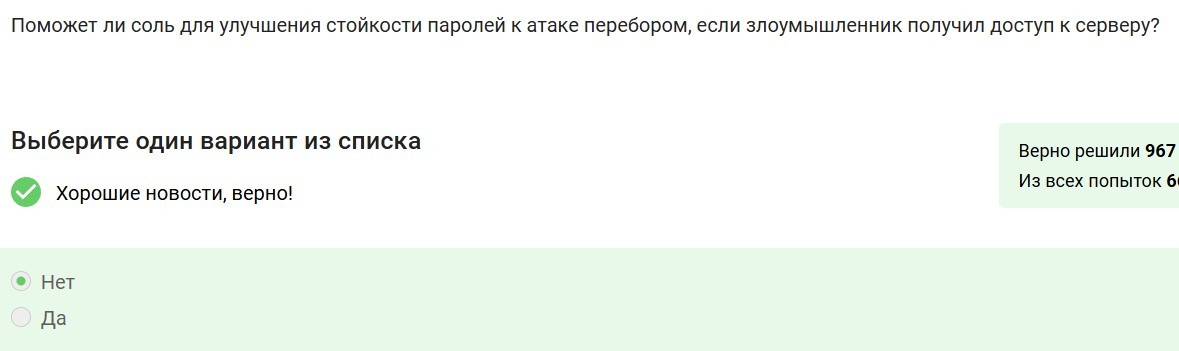
Капча не позволяет заходить на сайт автоматически (и обучает ИИ)

40



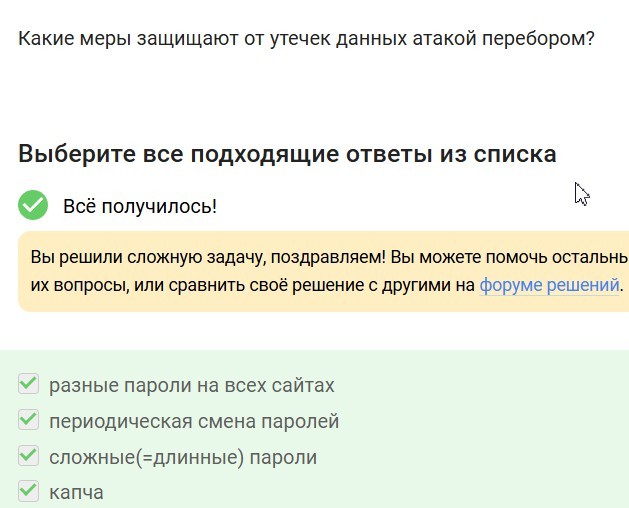
Если удастся взломать базу данных, то если пароль хэширован, им всё равно нельзя будет воспользоваться

41



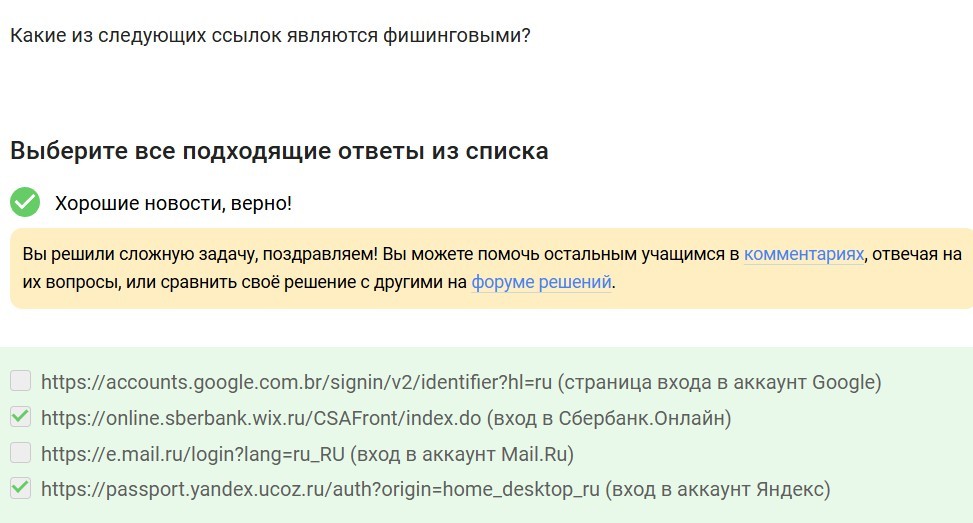
это шутка

42

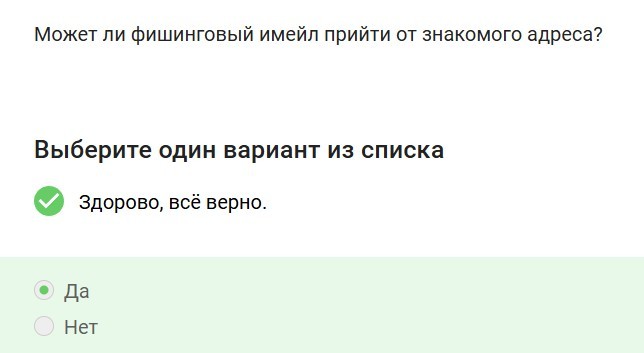


все вышеперечисленное помогает

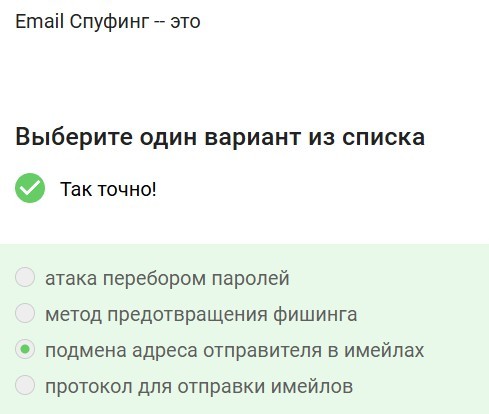
43



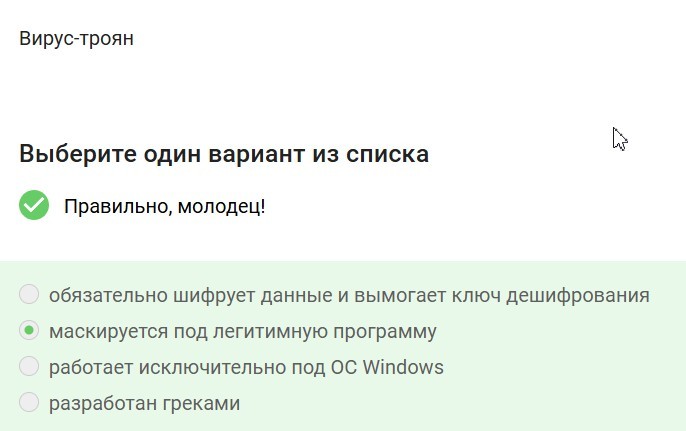
в ссылках присутствуют лишние элементы (wix и ucoz) 44



45



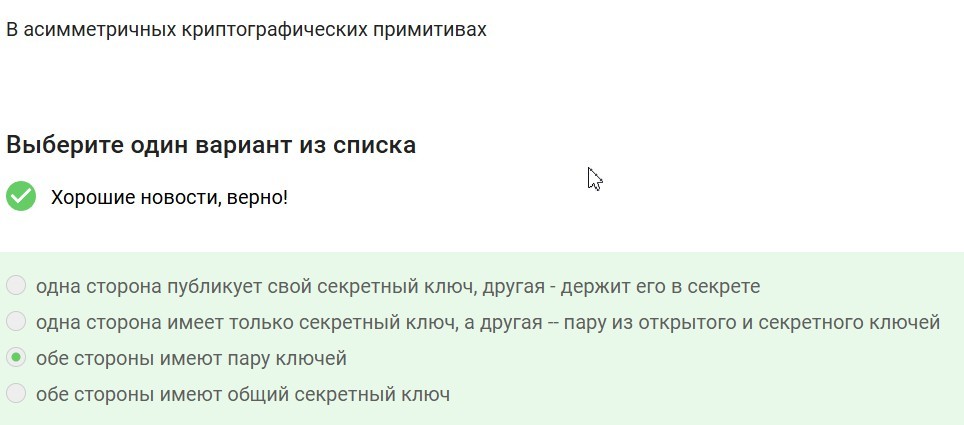
46



47

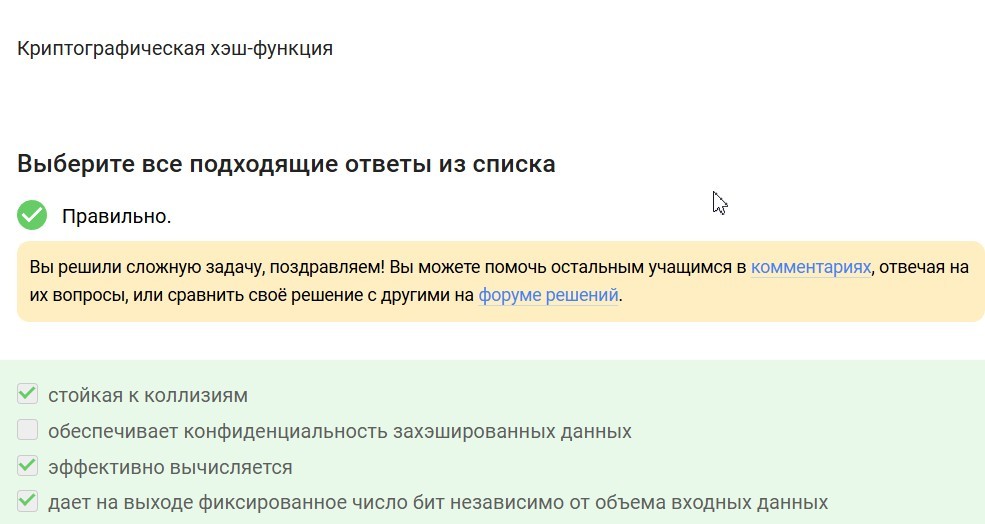
# Четвертая глава: Криптография на практике

48

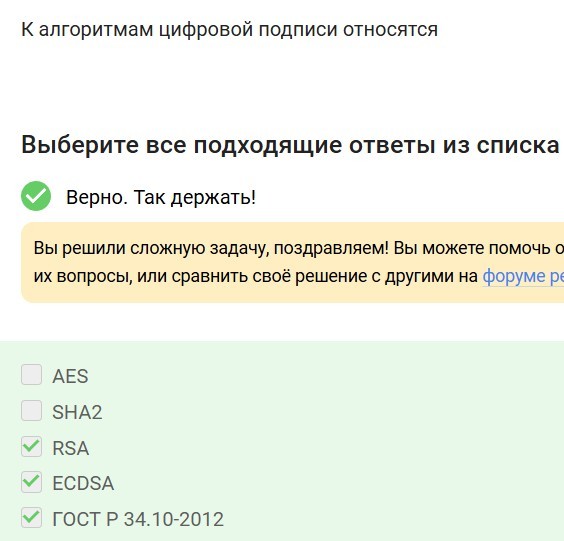


Асимметричное шифрование — это метод, в котором используются два ключа: открытый (публичный) и закрытый (приватный). 12 Открытый ключ используется для шифрования, а закрытый — для дешифрования. В отличие от симметричного метода, ключи не совпадают, что делает возможным обмен

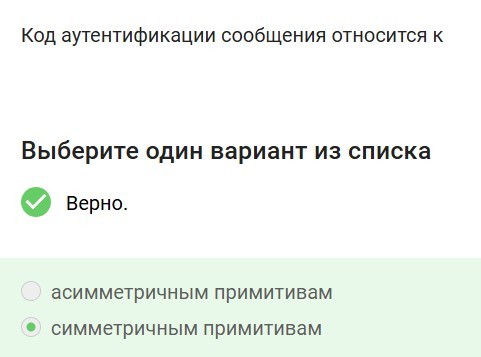
информацией без предварительного обмена секретами 49



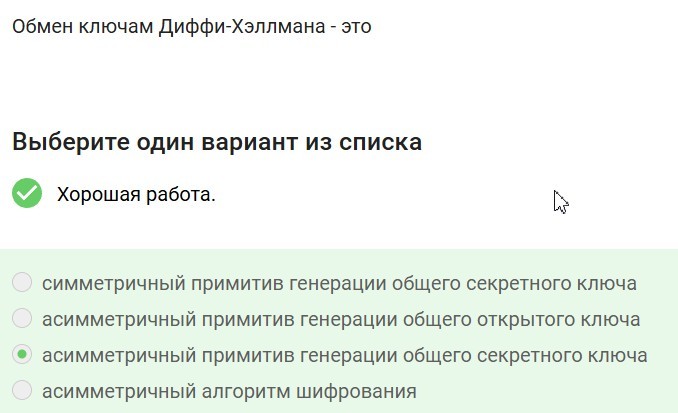
50



51



52

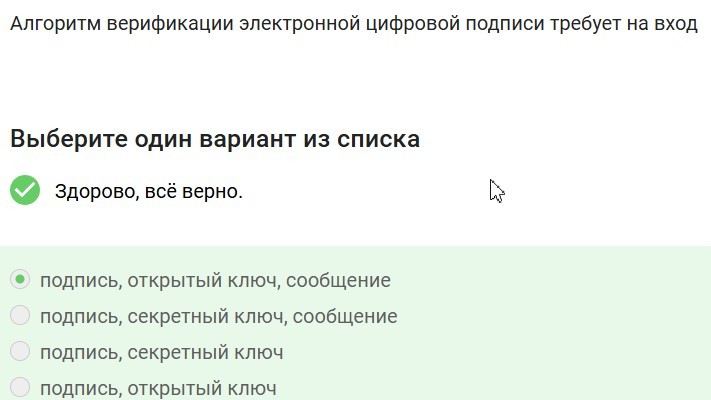


Протокол Ди́ффи — Хе́ллмана (англ. Diffie–Hellman key exchange protocol, DH) — криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью

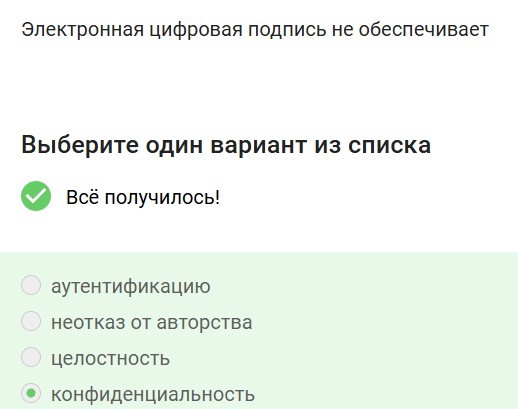
алгоритмов симметричного шифрования. 53



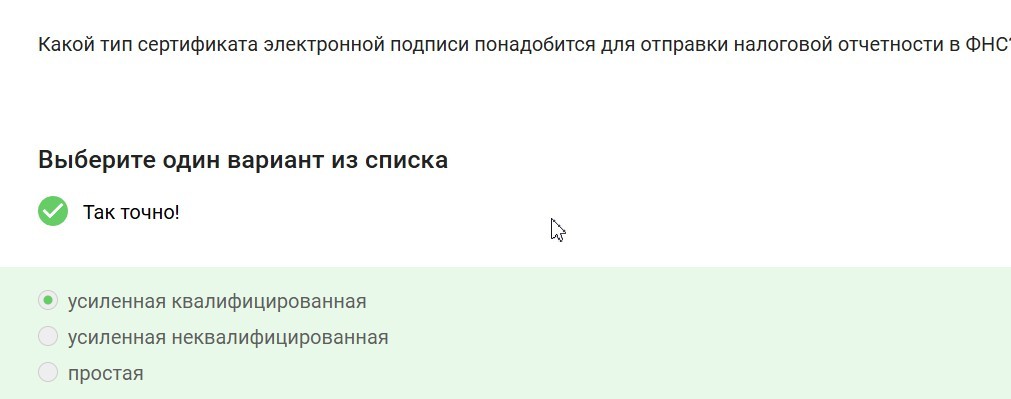
54



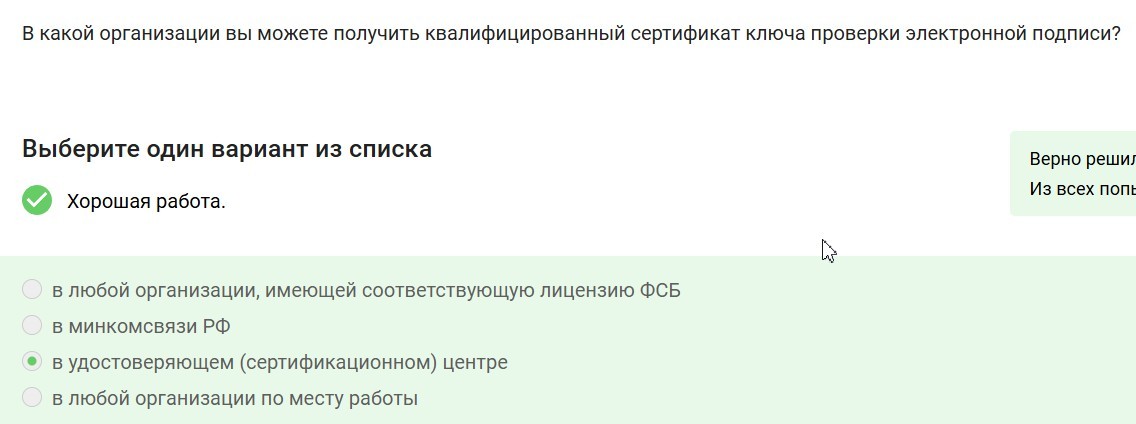
55



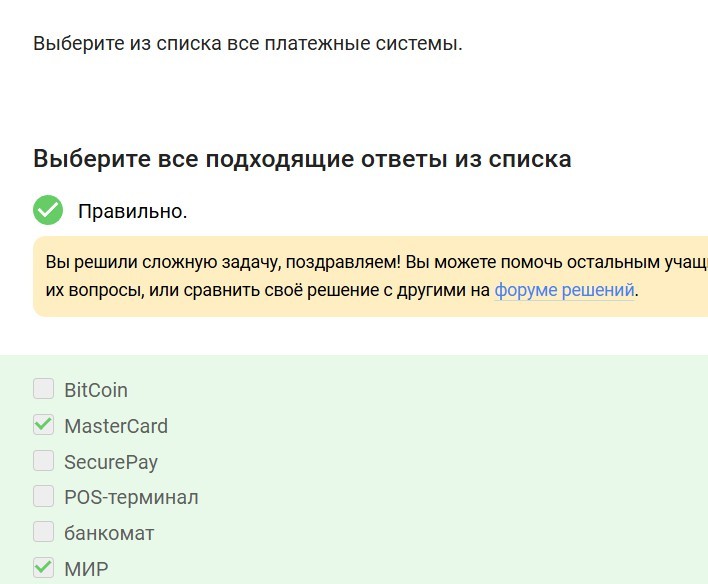
56



57



58

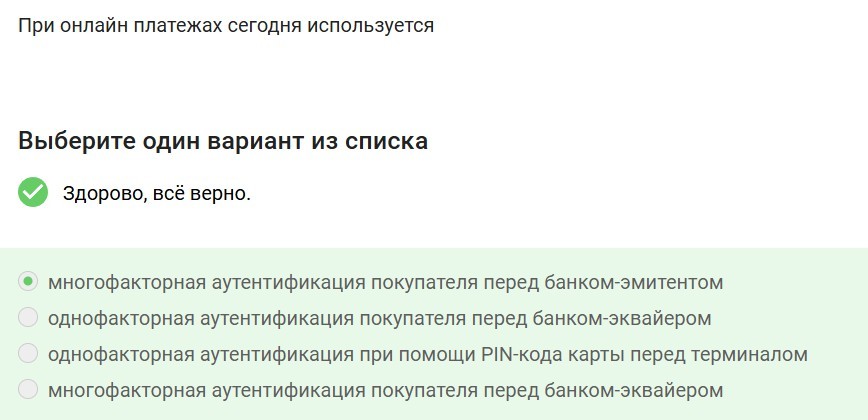


BitCoin - криптовалюта, SecurePay - ПО, POS терминал - это терминал, как и банкомат

59

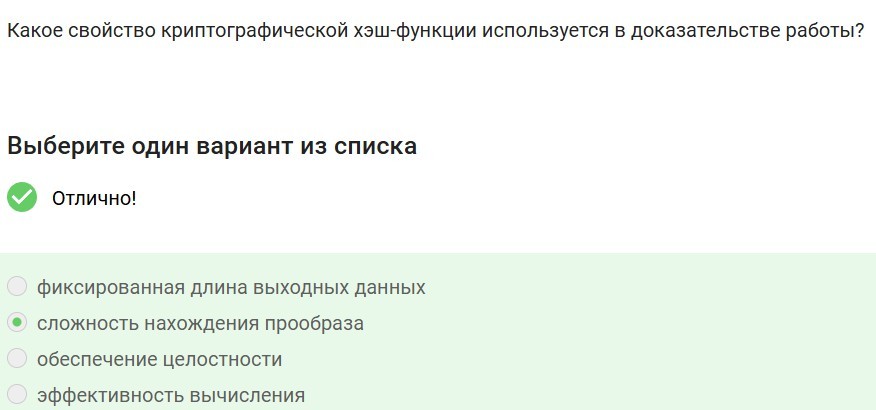


Капча не является частью аутентификации, пин-код и пароль - это просто пароль, то есть это один тип аутентификации 60



Потому что важнее защитить счёт человека от краж, а не от случайных зачислений

61

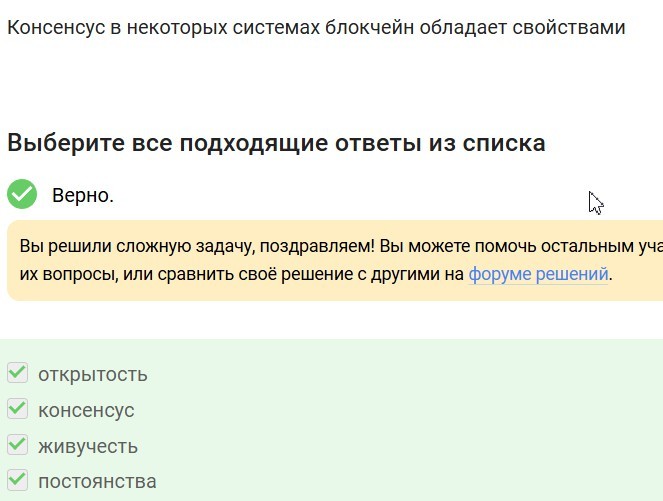


В доказательстве работы (Proof of Work, PoW), используемом в блокчейне (например, в Bitcoin), ключевое свойство хэш-функции

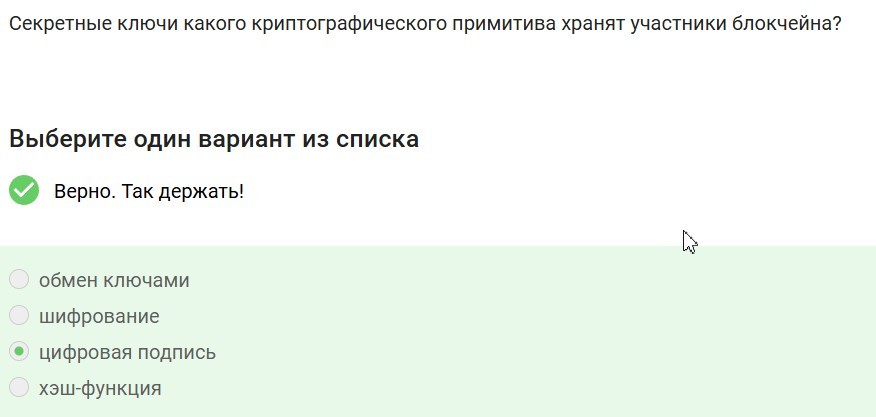
— это вычислительная сложность подбора входных данных для

получения хэша с заданными условиями (например, хэш с определённым количеством нулей в начале).

62



63



участники хранят адрес кошелька

64