Прохождение внешних курсов

Дисциплина: Основы информационной безопасности

Дудырев Глеб Андреевич НПИбд-01-22

Содержание

# 1 Цель работы

Познакомиться с основами кибербезопасности

# 2 Безопасность в сети

## 2.1 Как работает интернет базовые сетевые протоколы

1. Протоколом прикладного уровня является протокол HTTPS, он отвечает за работу с приложениями. (рис. 1)

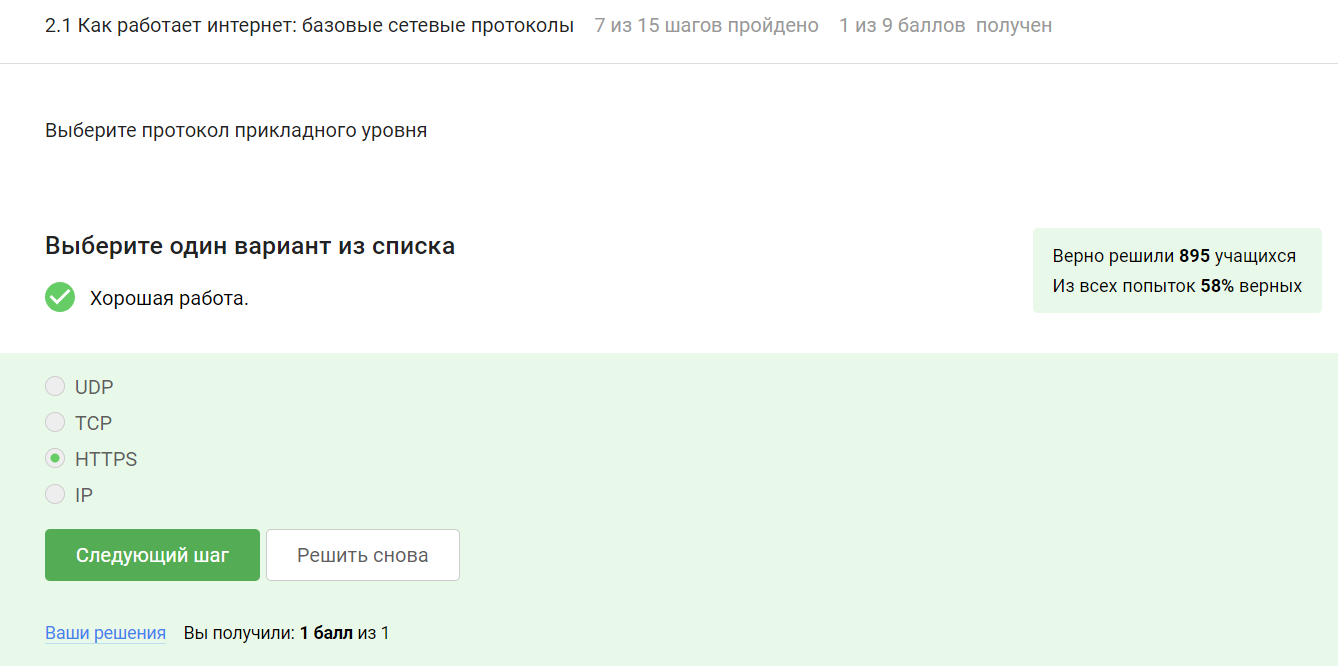


Рис. 1: Задание 1.1.1

1. Протокол TCP отвечает за передачу данных внутри одной машины, следовательно, он работает на транспортном уровне. (рис. 2)

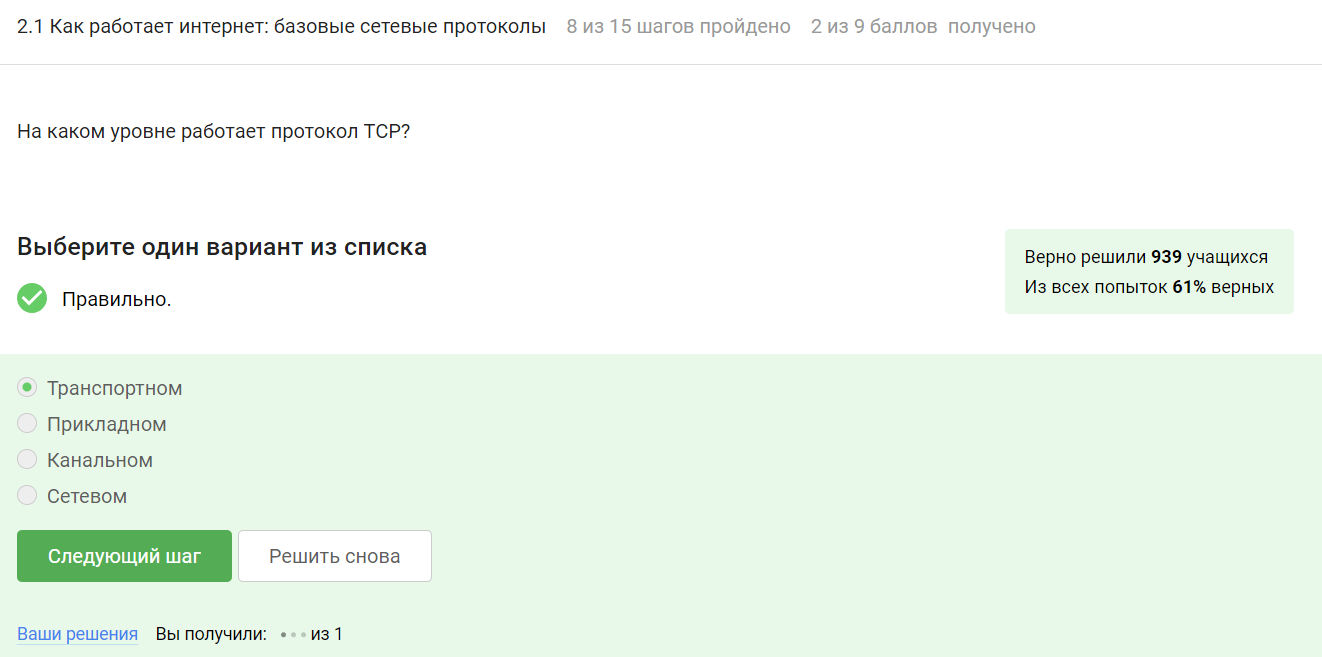


Рис. 2: Задание 1.1.2

1. Адреса IPv4 состает из 4 чисел от 0 до 255. (рис. 3)

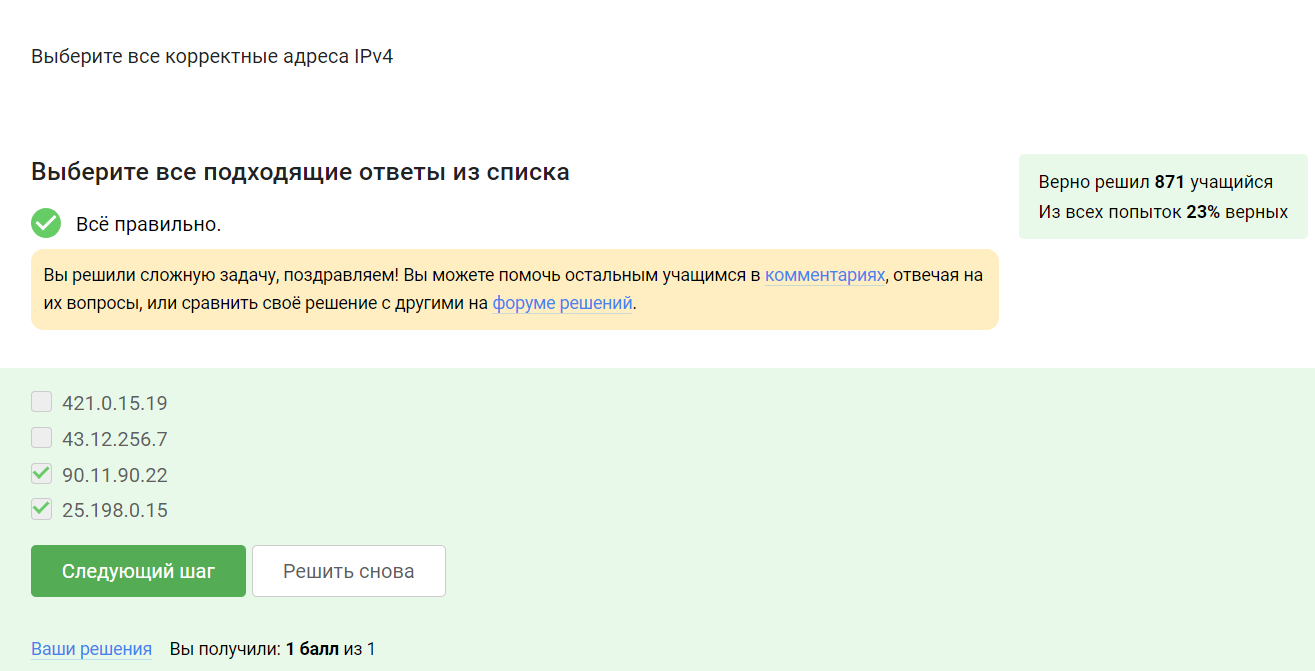


Рис. 3: Задание 1.1.3

1. Функцие DNS сервера является: соспоставить доменный и IP адреса. (рис. 4)

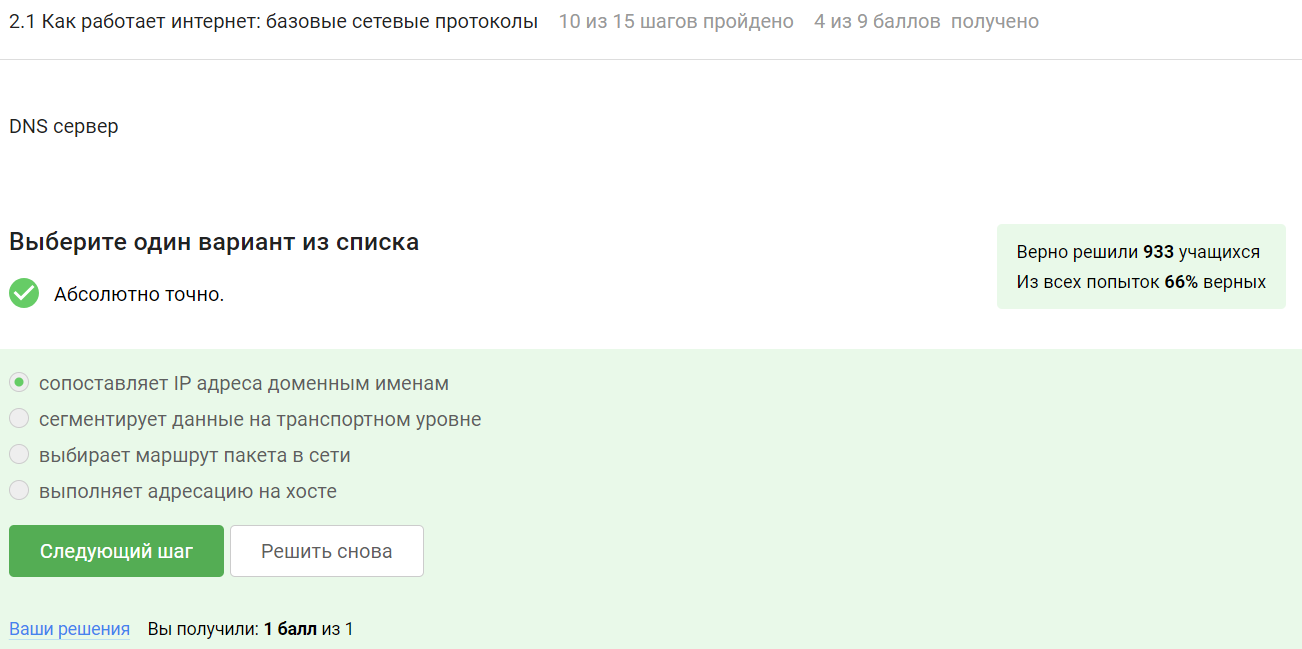


Рис. 4: Задание 1.1.4

1. Модель TCP/IP состоит из следующих уровней: прикладной(работа с приложением) - траспортный(передача информации внутри машины) - сетевой(передача информации по сети) - канальный(работа с информацией на физическом уровне). (рис. 5)

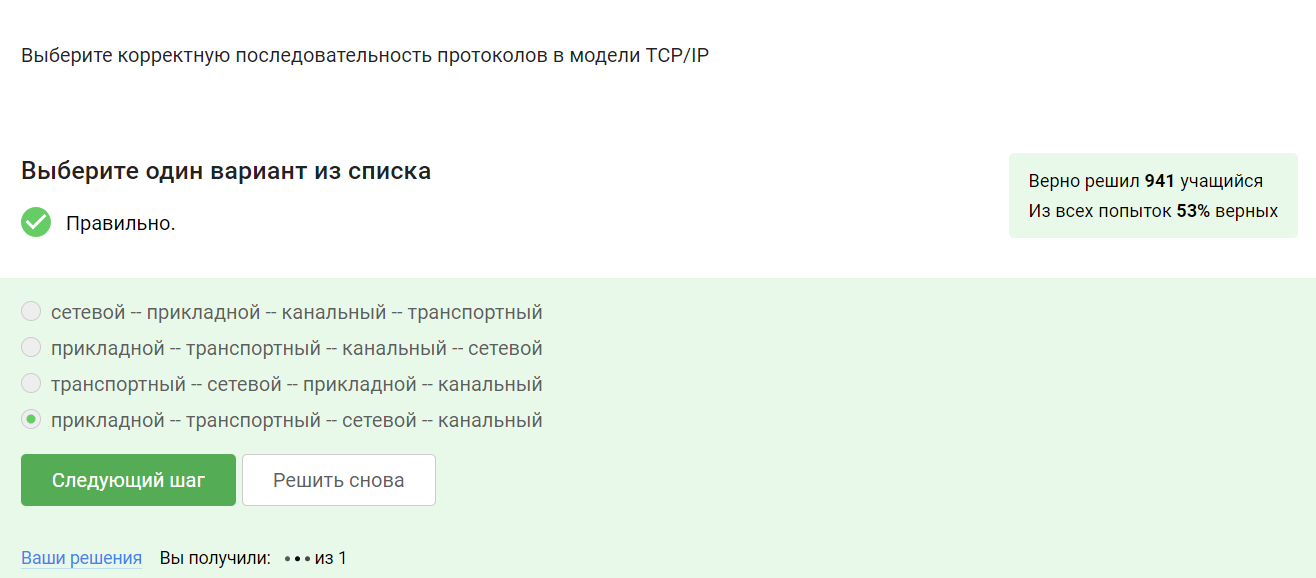


Рис. 5: Задание 1.1.5

1. Протокол HTTP предполагает передачу данных в открытом виде, а протокол HTTPS, который использует TLS, передает зашифрованные даннные. (рис. 6)

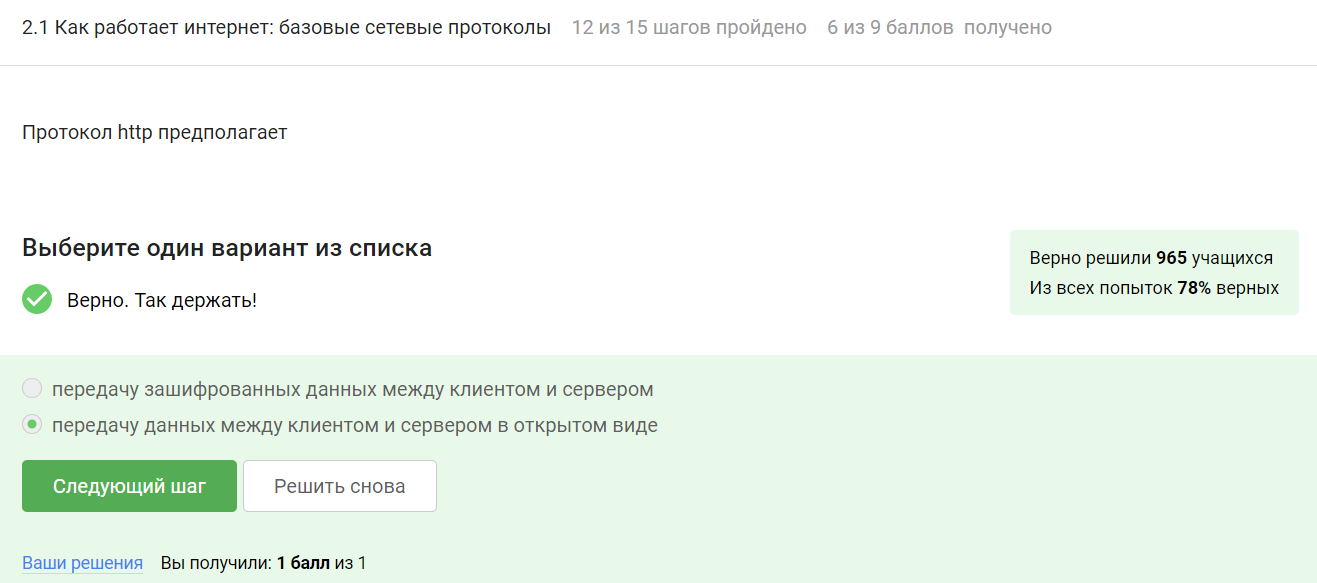


Рис. 6: Задание 1.1.6

1. Так как http не использует TLS при передаче данных, то этот протокол состоит из двух фаз: рукопожатие и передача данных. (рис. 7)

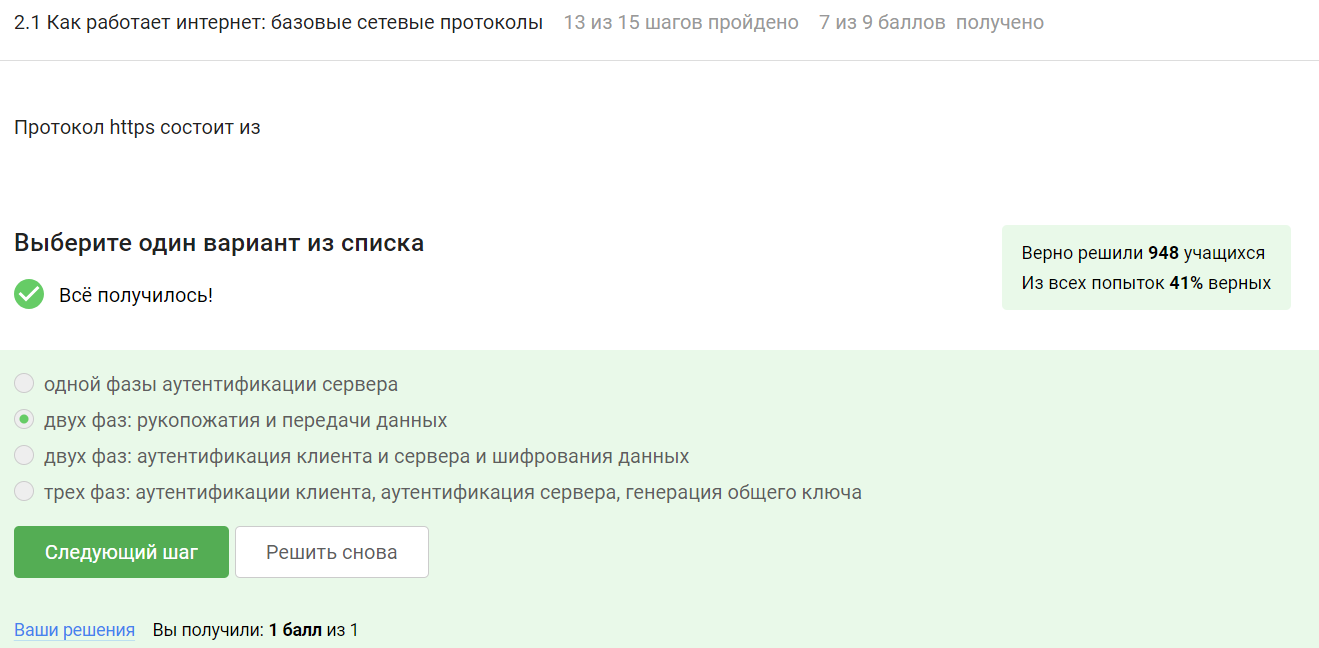


Рис. 7: Задание 1.1.7

1. Версию TLS клиент и сервер определяют во время ‘переговоров’. (рис. 8)

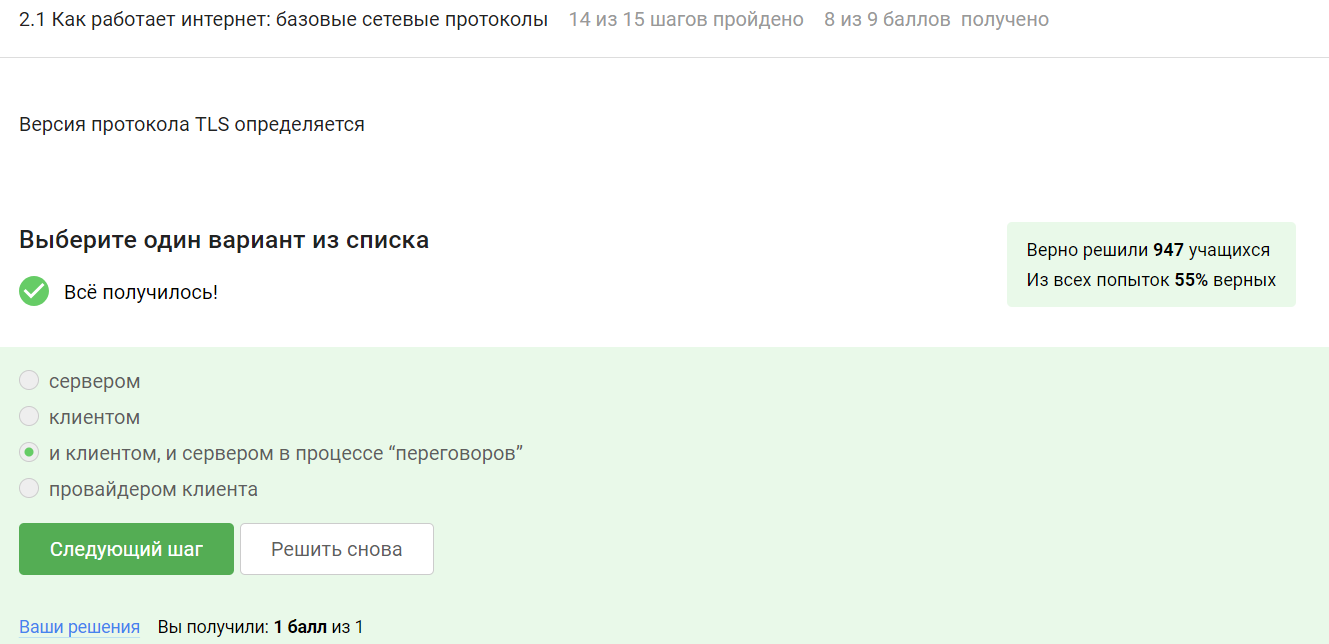


Рис. 8: Задание 1.1.8

1. В протоколе TLS шифрование данных предусмотрено в фазе: “Данных” (рис. 9)

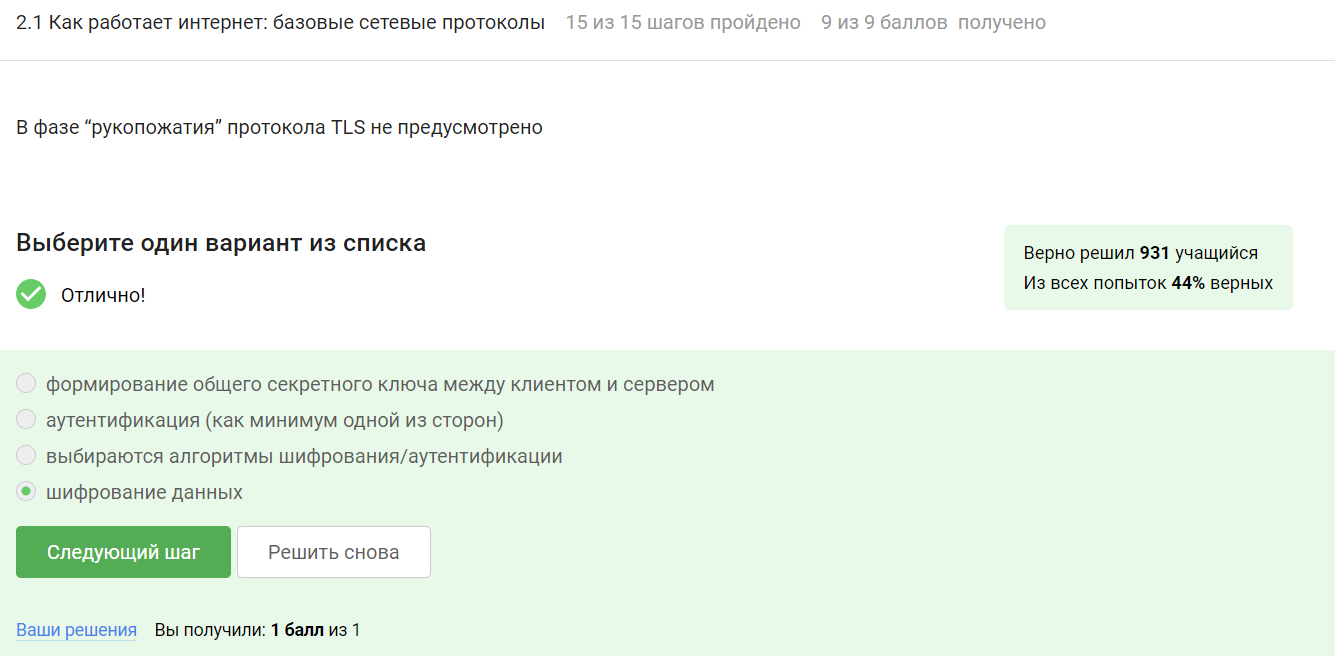


Рис. 9: Задание 1.1.9

## 2.2 Персонализация сети

1. Куки хранят id пользователя и id сессии, а также информацию о действиях пользователя на сайте. (рис. **¿fig:010?**)

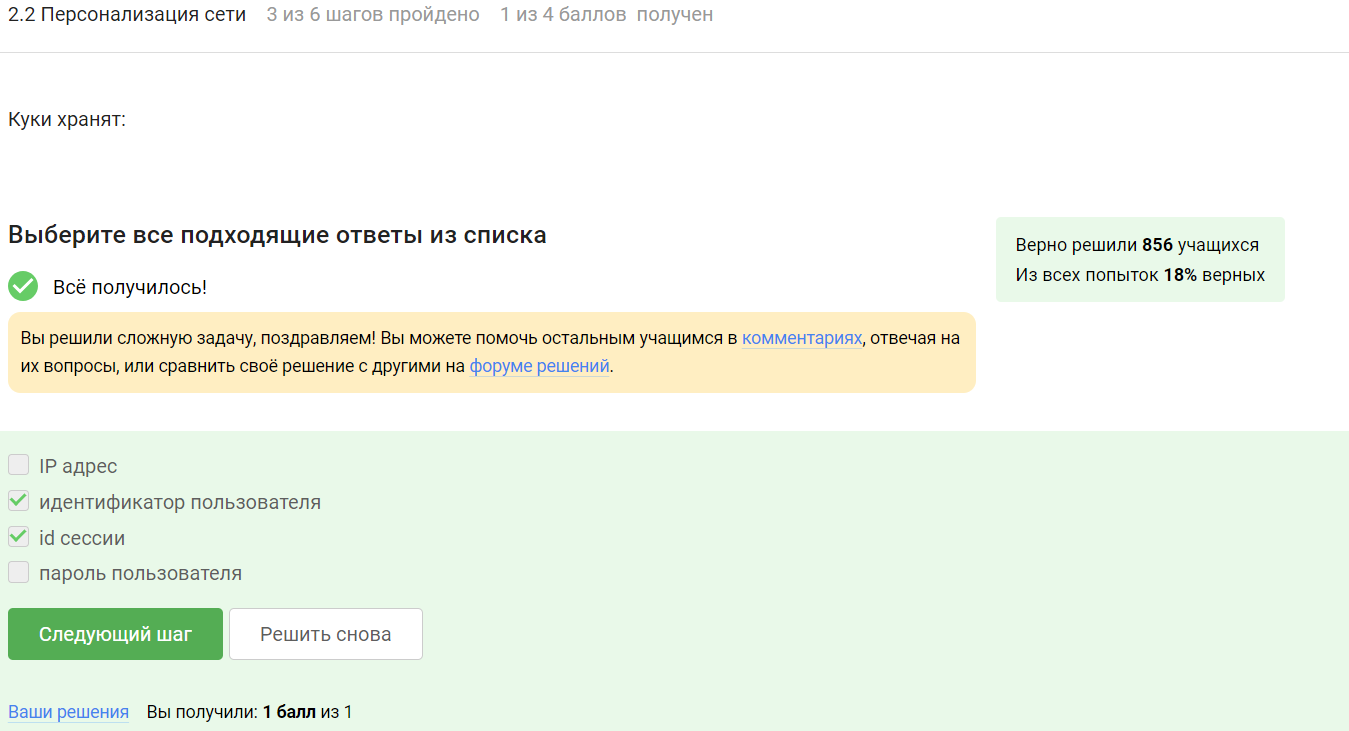


Рис. 10: Задание 1.2.1

1. Куки не используются для улучшения надежности соединения, они служат для того, чтобы сохранять информацию о сессии на сервере. (рис. **¿fig:011?**)

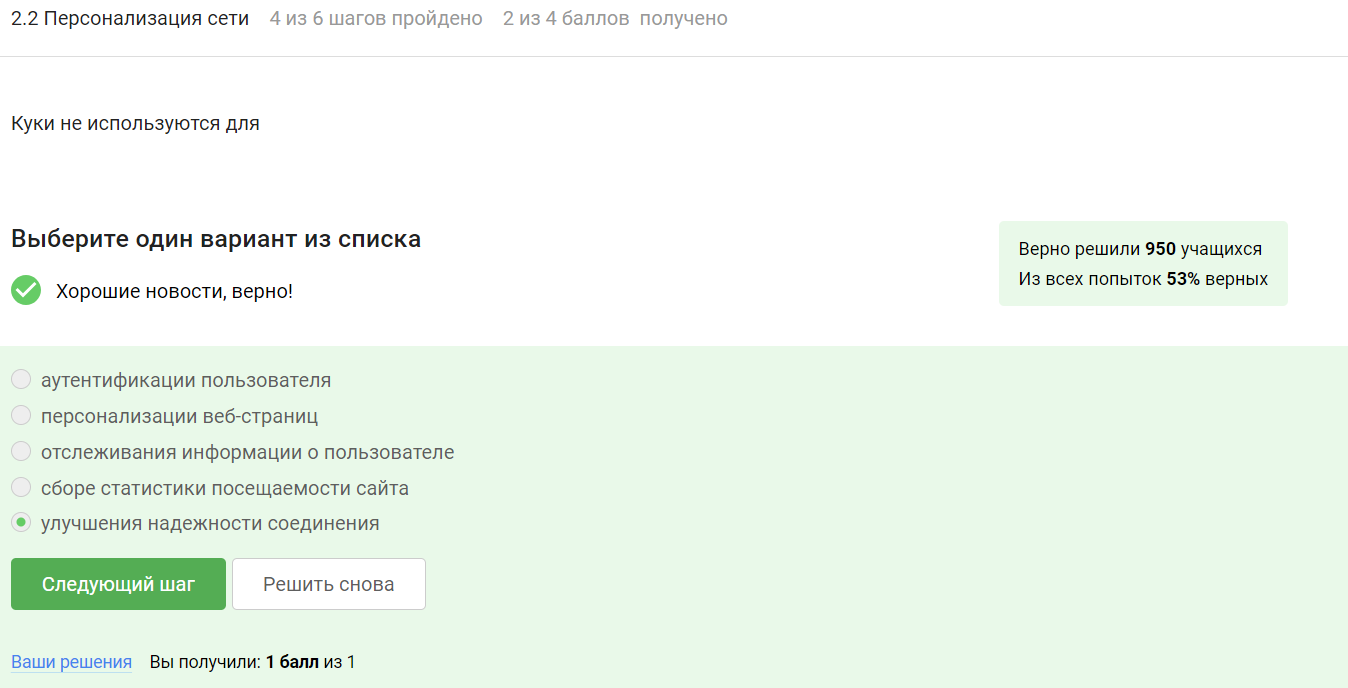


Рис. 11: Задание 1.2.2

1. Сервер генерирует куки и возвращает их вместе с ответом на запрос. (рис. **¿fig:012?**)

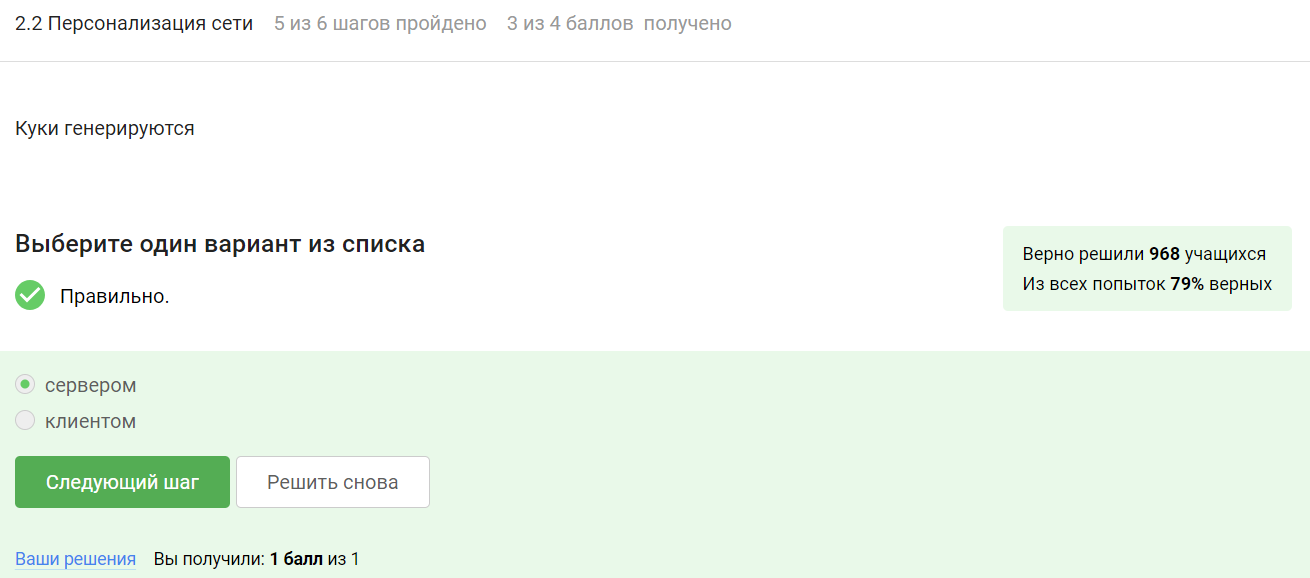


Рис. 12: Задание 1.2.3

1. Куки бывают сессионные и постоянные, первые хранятся на сервере и удаляются после закрытия сайта. (рис. 13)

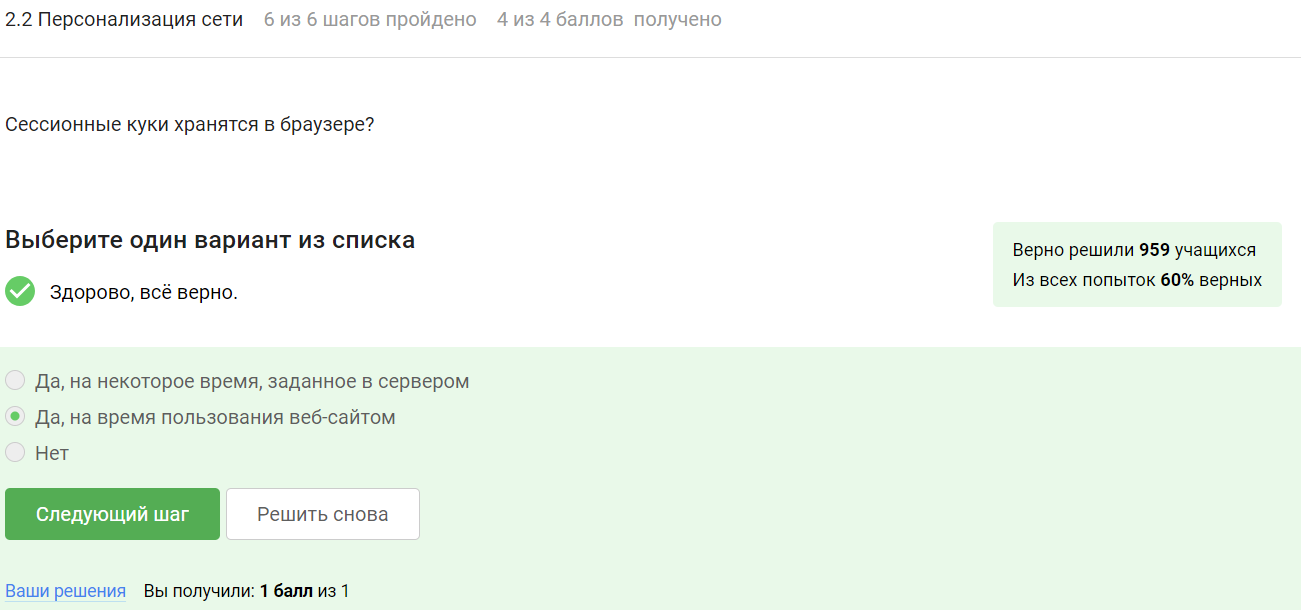


Рис. 13: Задание 1.2.4

## 2.3 Браузер TOR. Анонимизация

1. В луковой маршрутизации существует три узла: охранный, промежуточный и выходной. (рис. 14)

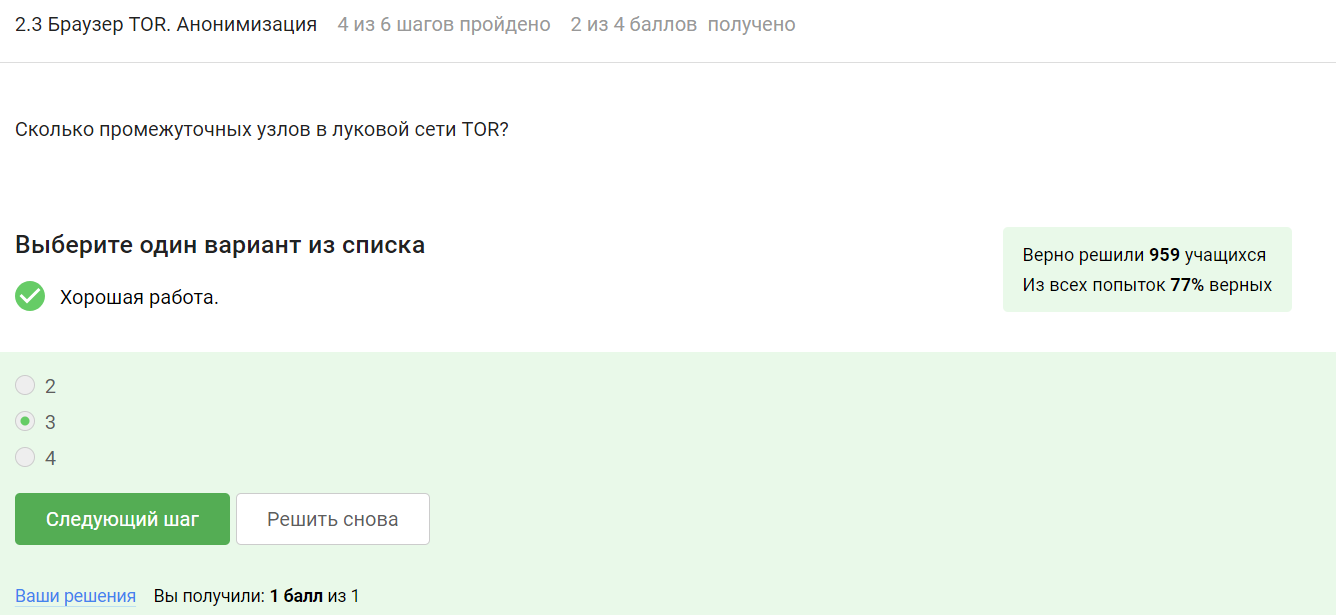


Рис. 14: Задание 1.3.1

1. В луковой маршрутизации IP адрес получателя известен: отправителю и выходному узлу. (рис. 15)

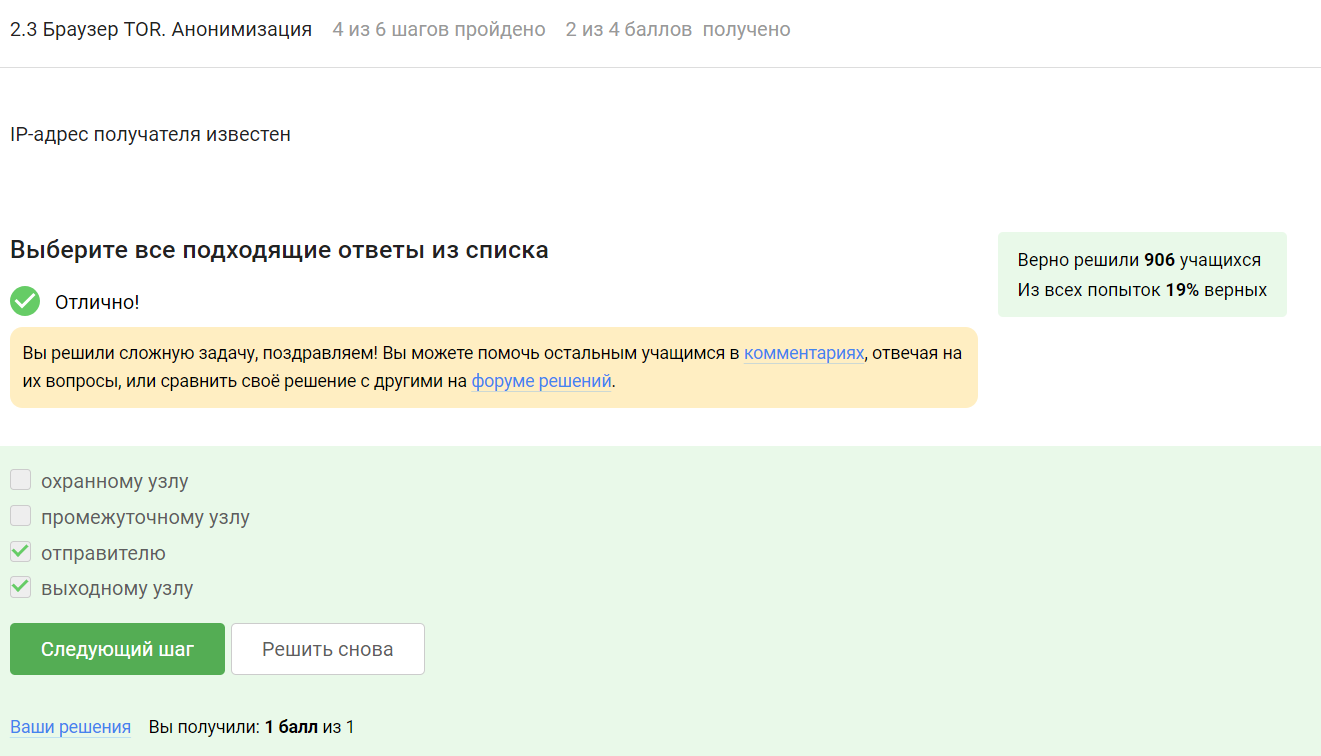


Рис. 15: Задание 1.3.2

1. Отправитель генерирует три общих секретных ключа: для охранного узла, для промежуточного и для выходного. (рис. 16)

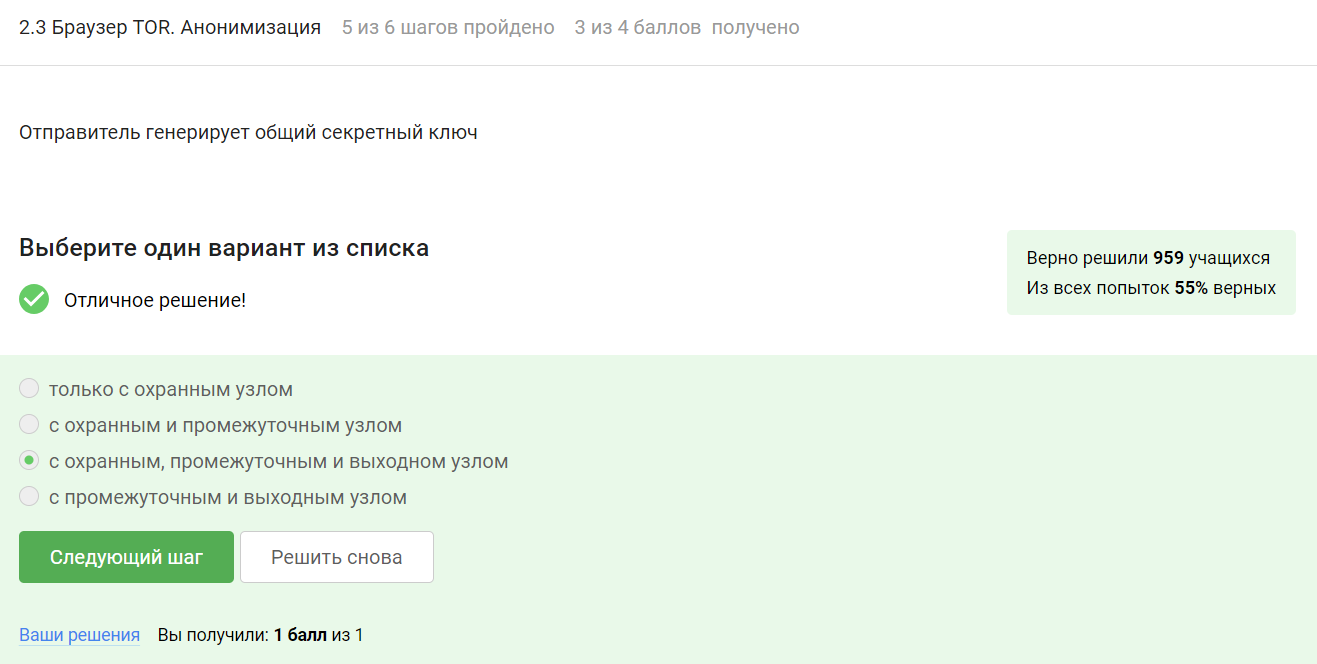


Рис. 16: Задание 1.3.3

1. Браузер Tor используется для анонимизации, а не для гарантии успешного получения пакетов. (рис. 17)

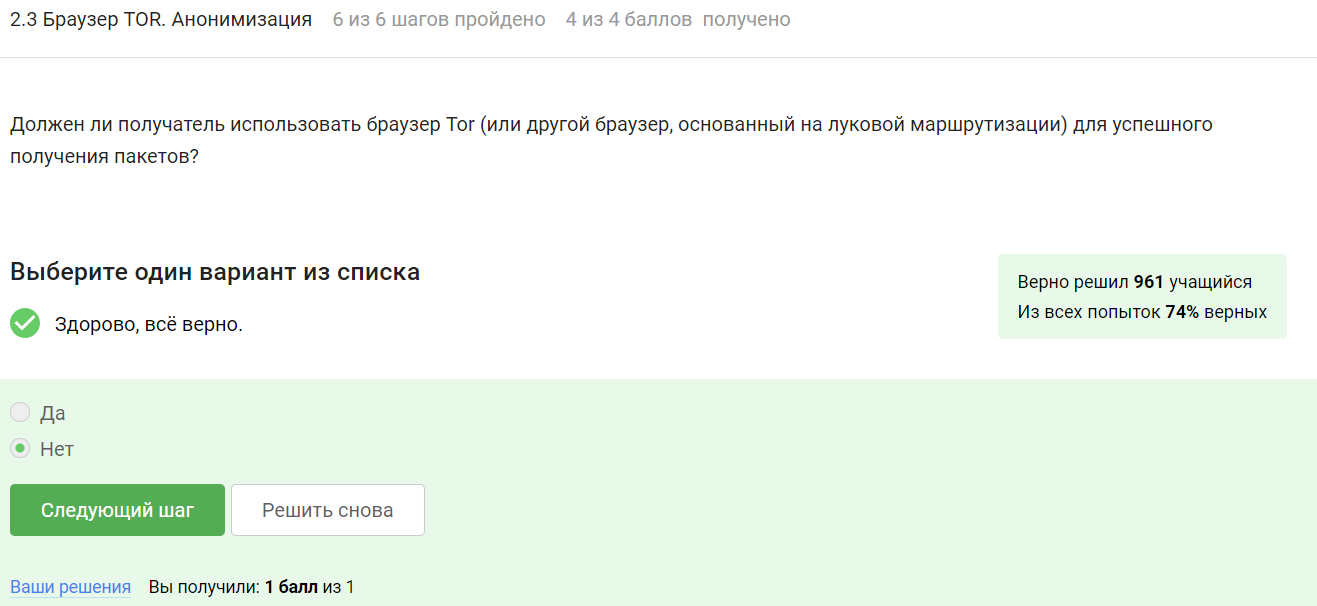


Рис. 17: Задание 1.3.4

## 2.4 Беспроводные сети Wi-fi

1. Wi-fi - это технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11. (рис. 18)

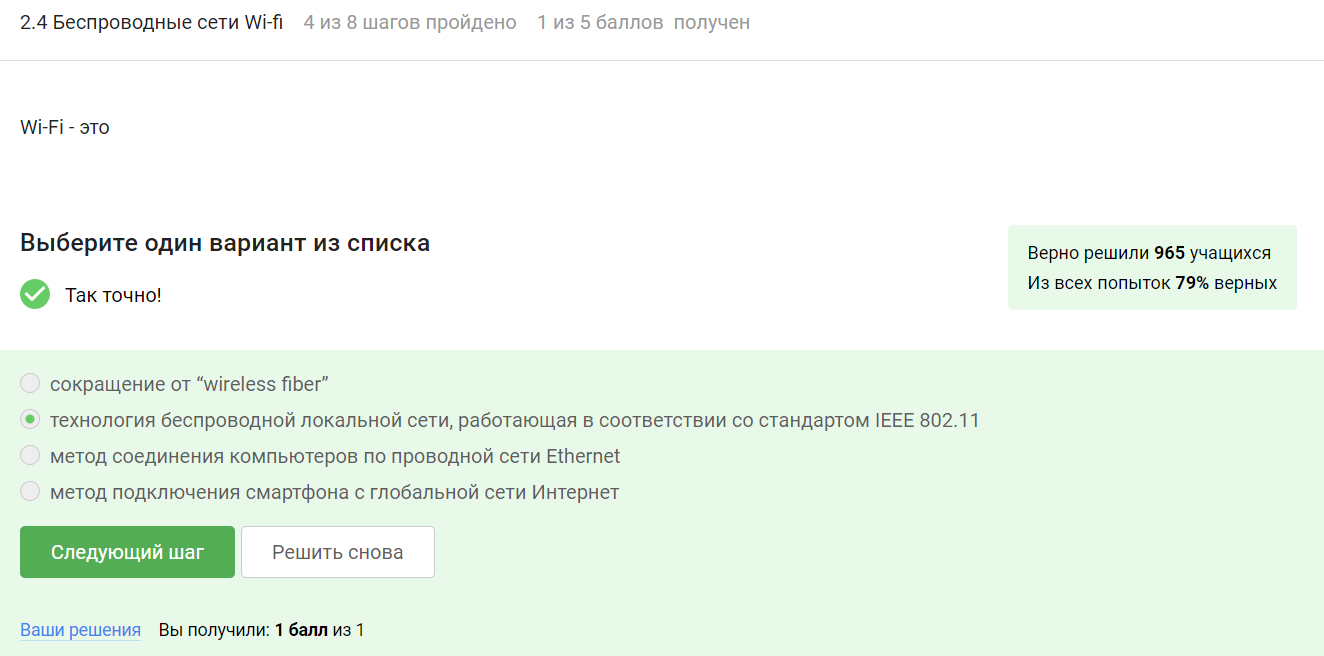


Рис. 18: Задание 1.4.1

1. Протокол Wi-fi работает на самом низком канальном уровне, как Ethernet. (рис. 19)

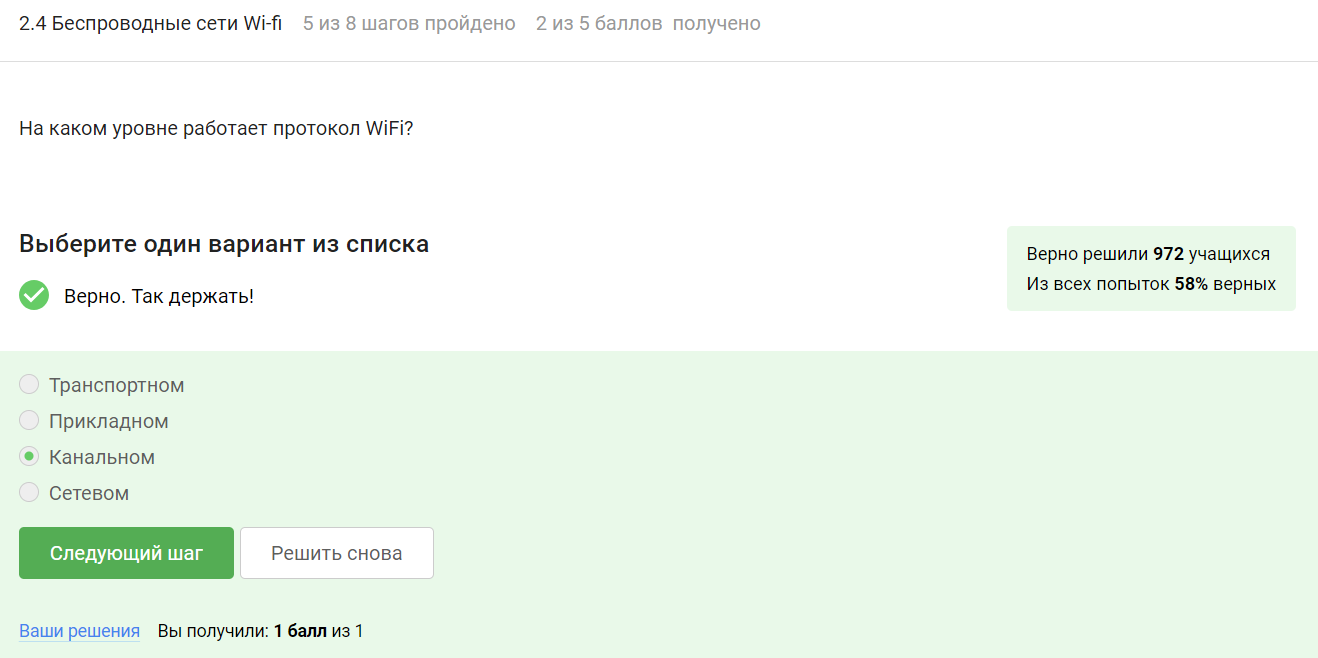


Рис. 19: Задание 1.4.2

1. WEP является небезопасным методом шифрования, так как имеет очень короткую длину ключа. (рис. 20)

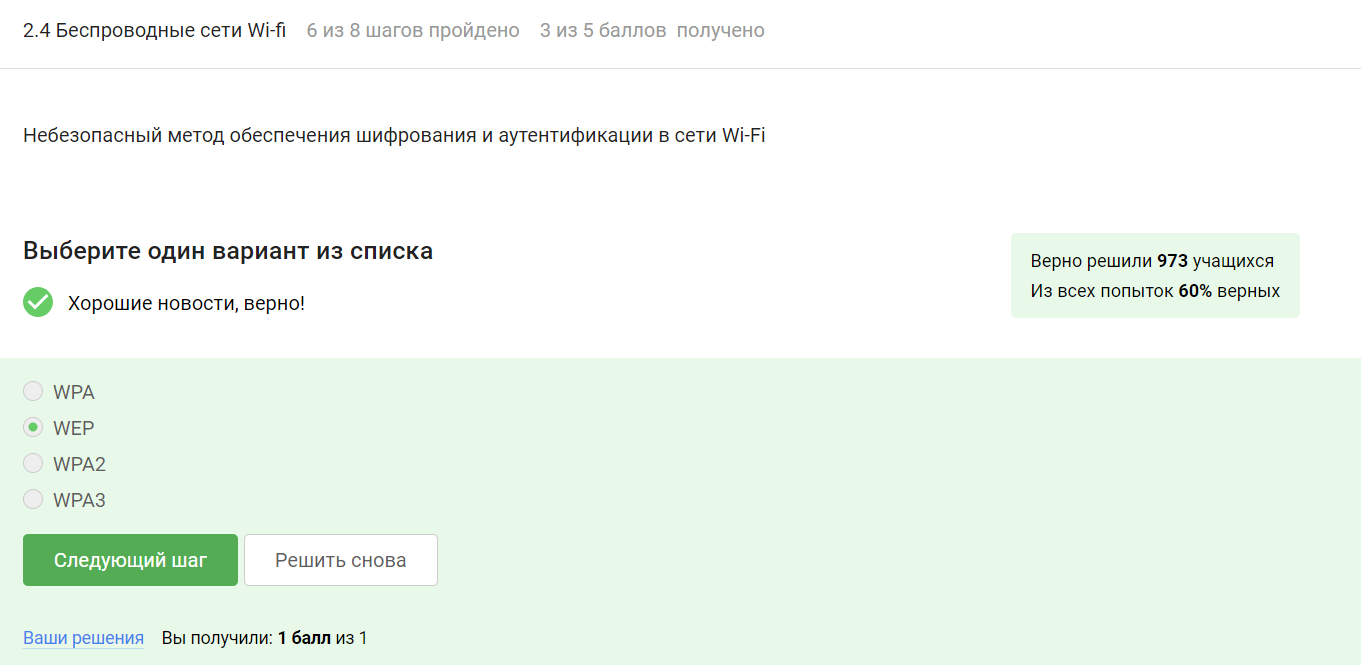


Рис. 20: Задание 1.4.3

1. Данные между хостом сети и роутером передаются в зашифрованном виде, после аутентификации, чтобы их нельзя было перехватить. (рис. 21)

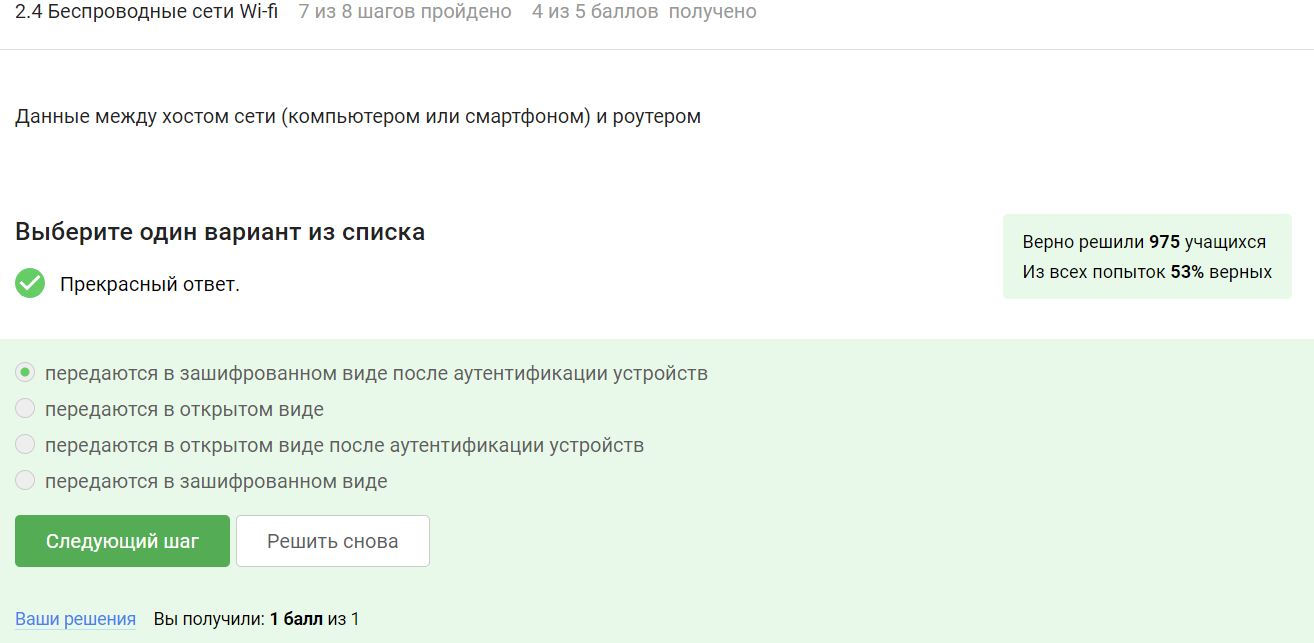


Рис. 21: Задание 1.4.4

1. Для домашней сети для аутентификации обычно используется метод Personal(подключение по поролю), второй метод используется для больших корпоративных сетей, он проверяет есть ли пользователь в базе данных. (рис. 22)

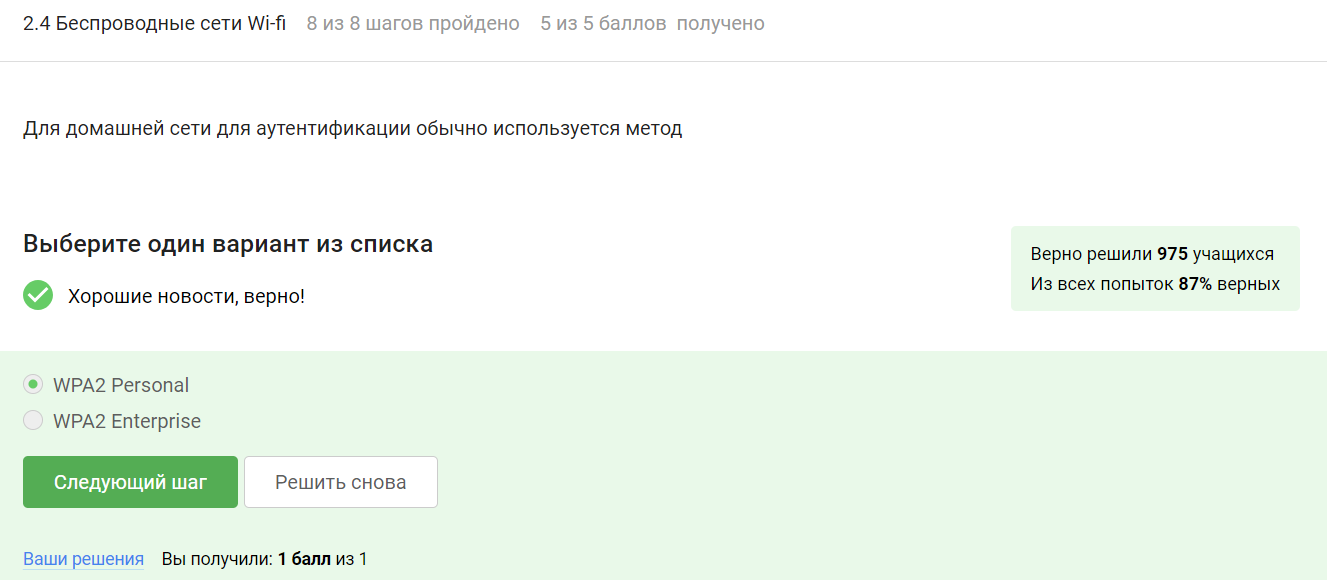


Рис. 22: Задание 1.4.5

# 3 Защита ПК/телефона

## 3.1 Шифрование диска

1. Можно зашифровать любой сектор диска. (рис. 23)

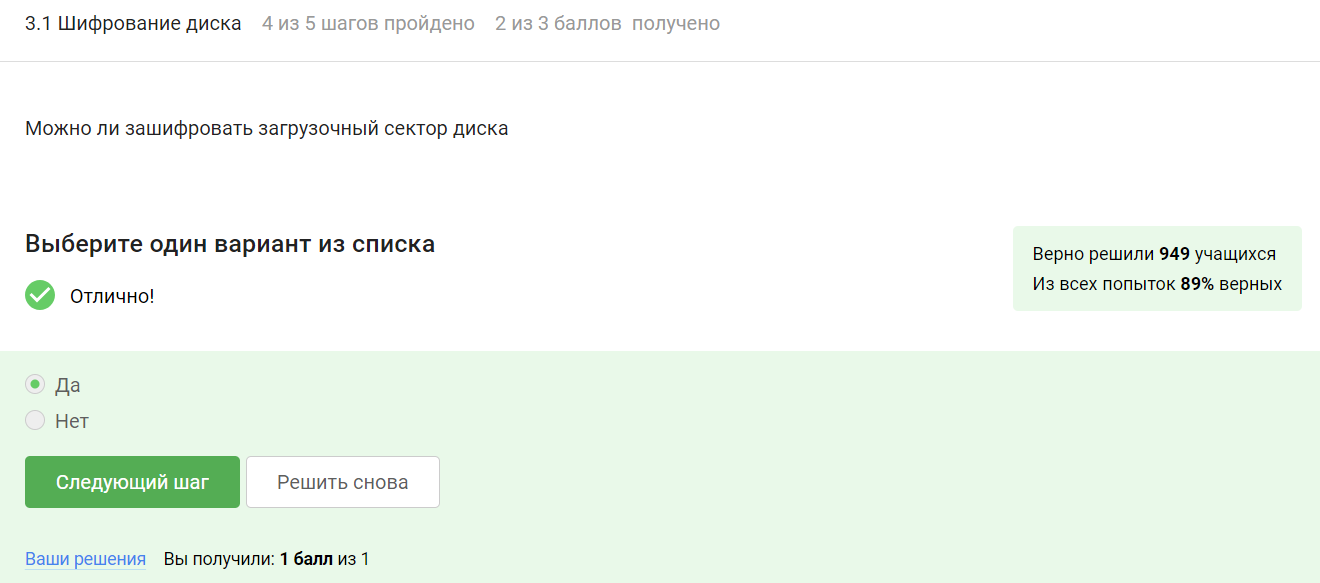


Рис. 23: Задание 2.1.1

1. Для шифрования диска используется симметричное шифрование, то есть один секретный ключ для шифрования и дешифрования данных. (рис. 24)

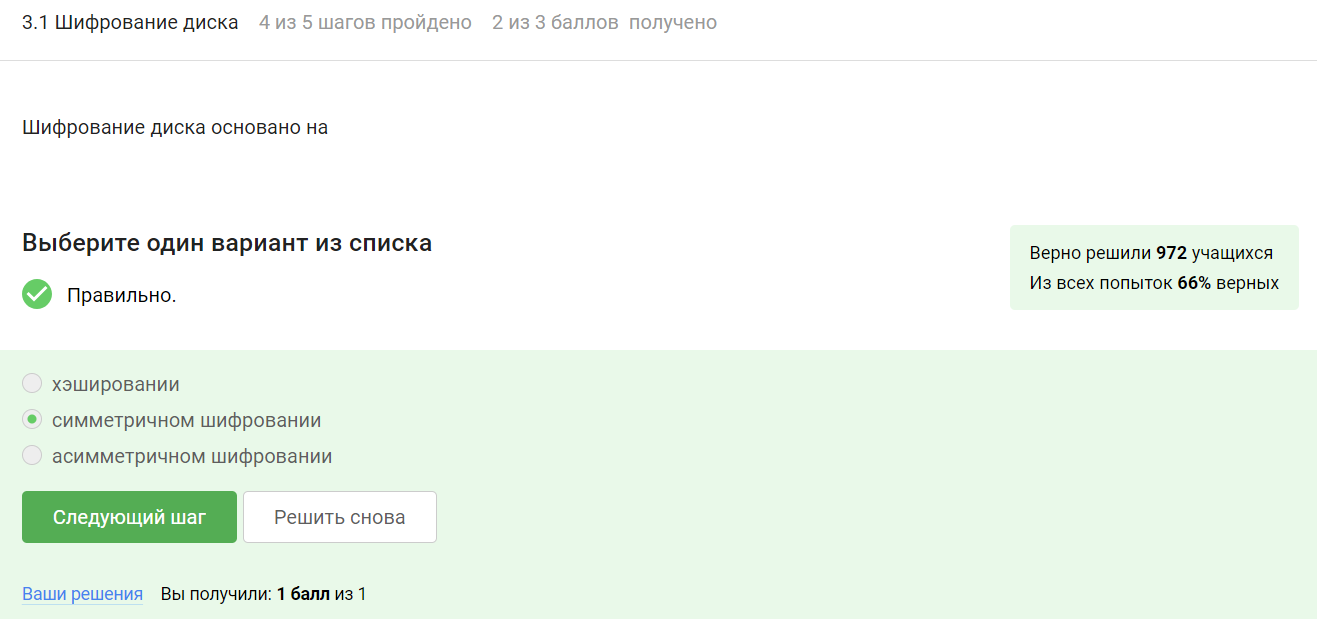


Рис. 24: Задание 2.1.2

1. BitLocker - для Windows, в Linux – LUKS, в MacOS – это FileVault. (рис. 25)

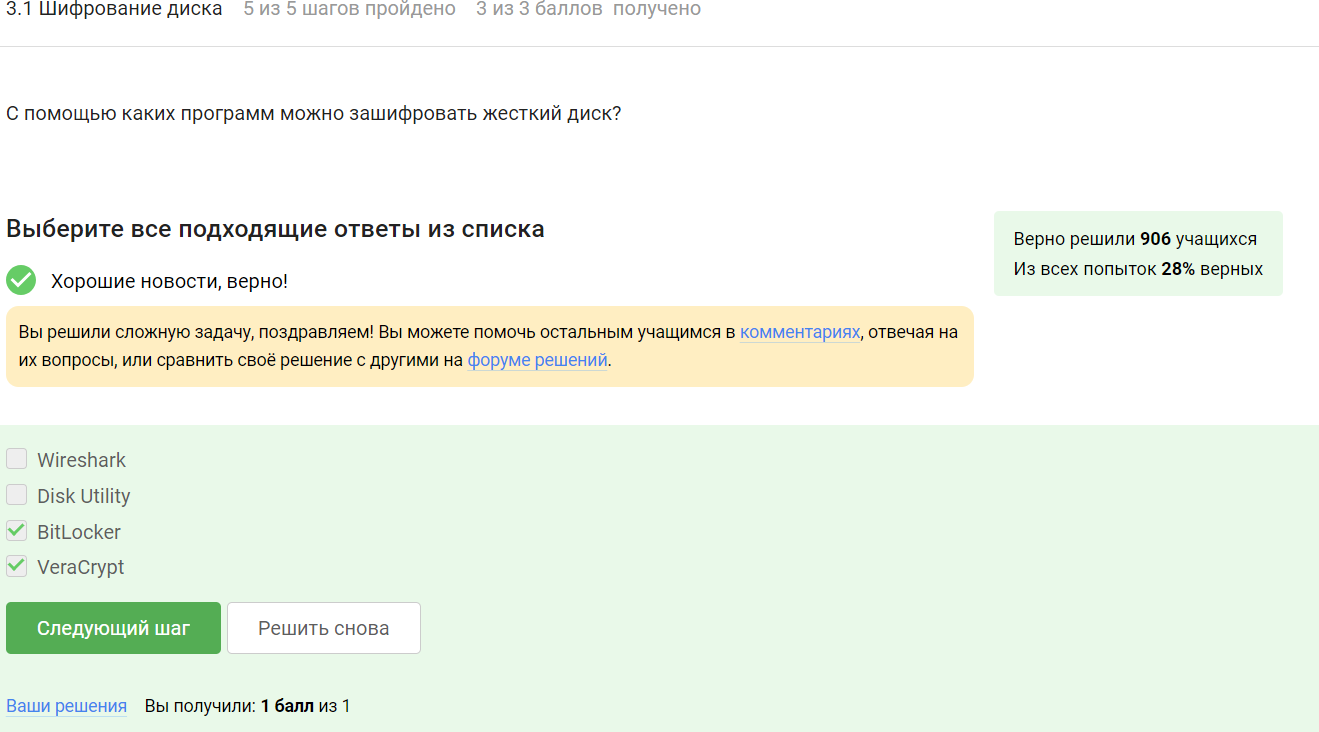


Рис. 25: Задание 2.1.3

## 3.2 Пароли

1. Стойкий пароль не должен быть коротким и должен состоять из различных символов, букв разного регистра и цифр. (рис. 26)

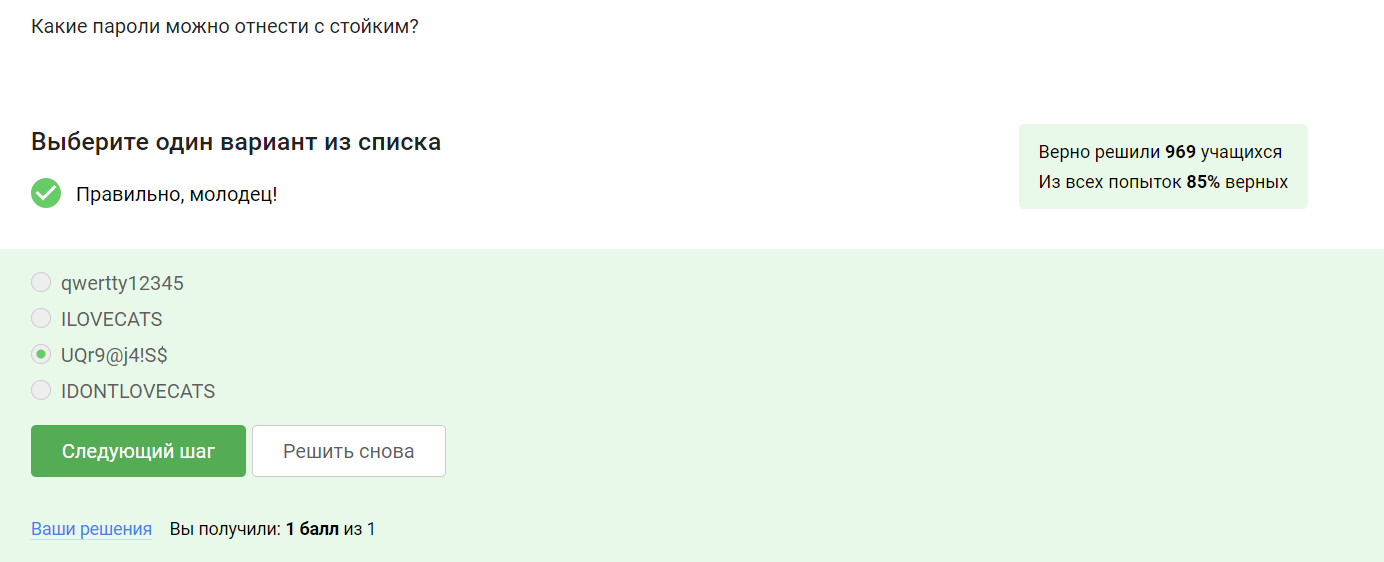


Рис. 26: Задание 2.2.1

1. Пароли необзодимо хранить в безопасном месте, чтобы их не смогли обнаружить случайно, например, в менеджерах для паролей. (рис. 27)

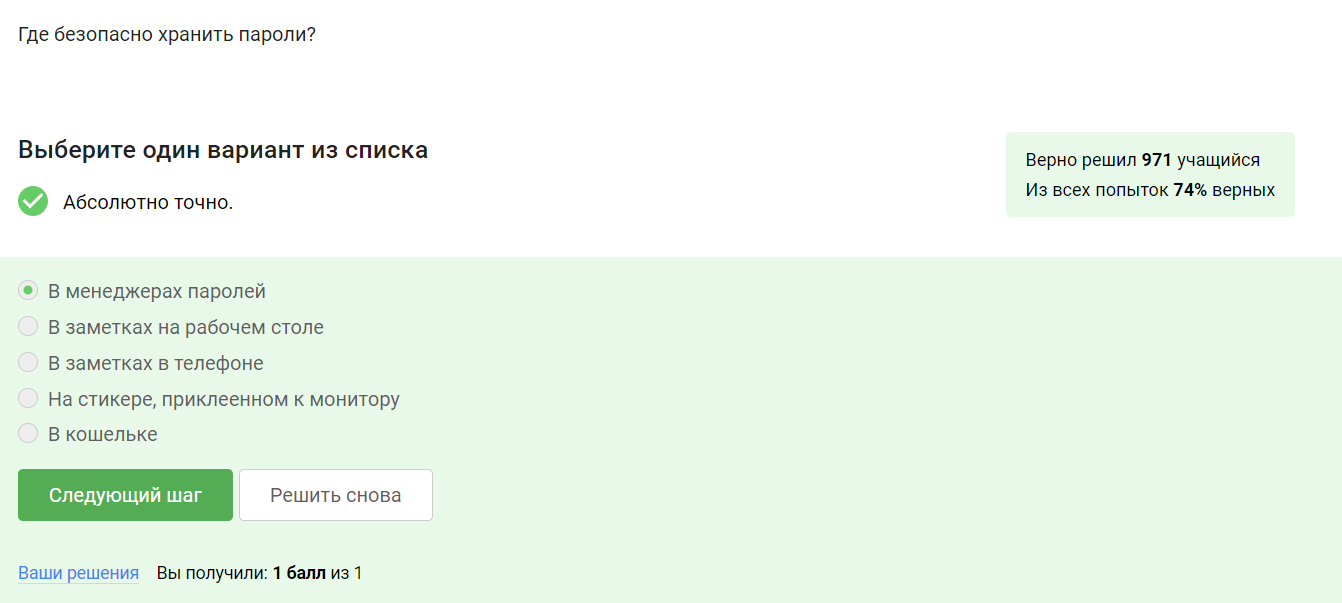


Рис. 27: Задание 2.2.2

1. Капча используется для предотвращения запросов к серверу со стороны ботов, что затрудняет автоматизированный перебор паролей. (рис. 28)

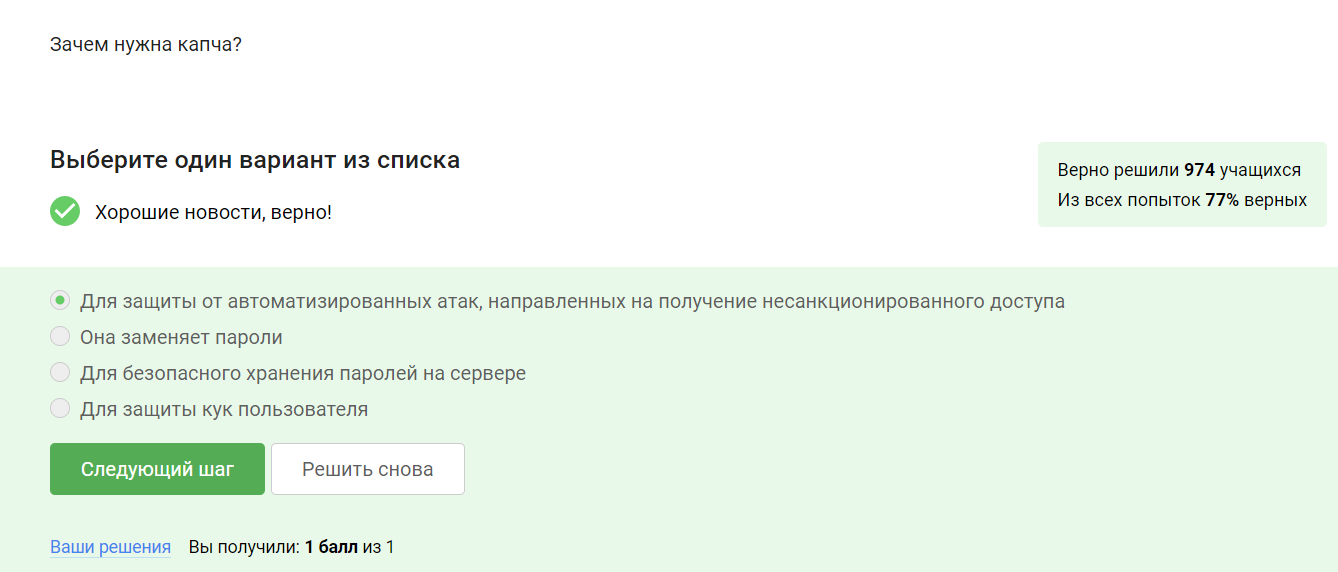


Рис. 28: Задание 2.2.3

1. Хэширование паролей используется серверами, чтобы не хранить пароль в открытом виде, а вместо него хранить результат применения хэш-функции к паролю. (рис. 29)

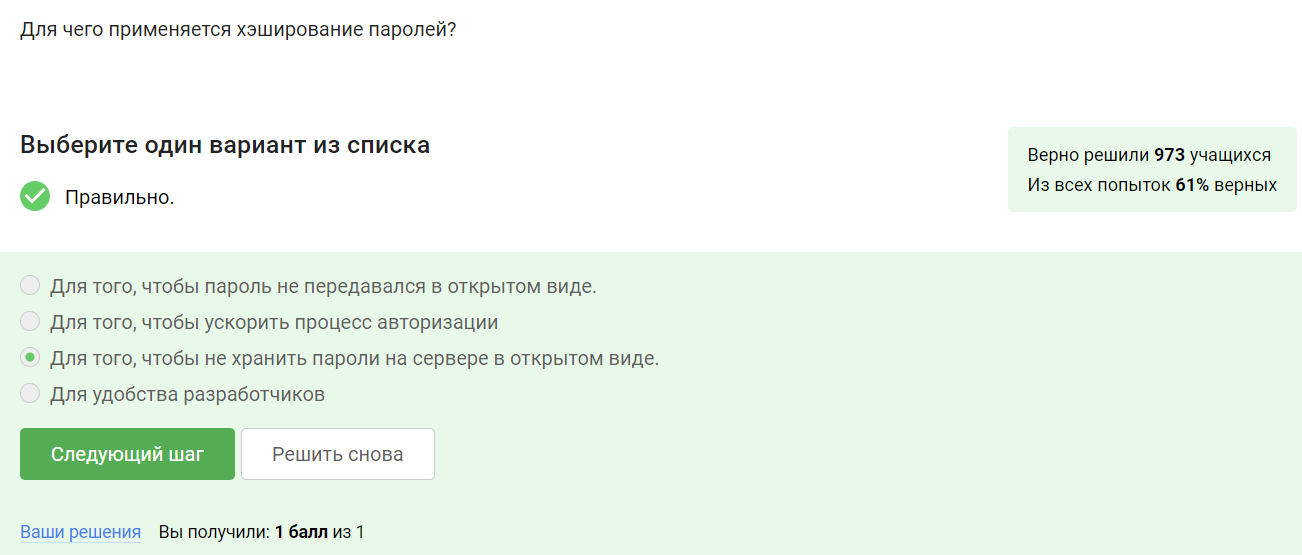


Рис. 29: Задание 2.2.4

1. Ответ нет, так как соль используется для того, чтобы не хранить результат хэширования часто используемого пароля, так как если злоумышленник получит доступ к серверу, где хранятся хэш-пароли, он сразу поймет прообраз хэширования. (рис. 30)

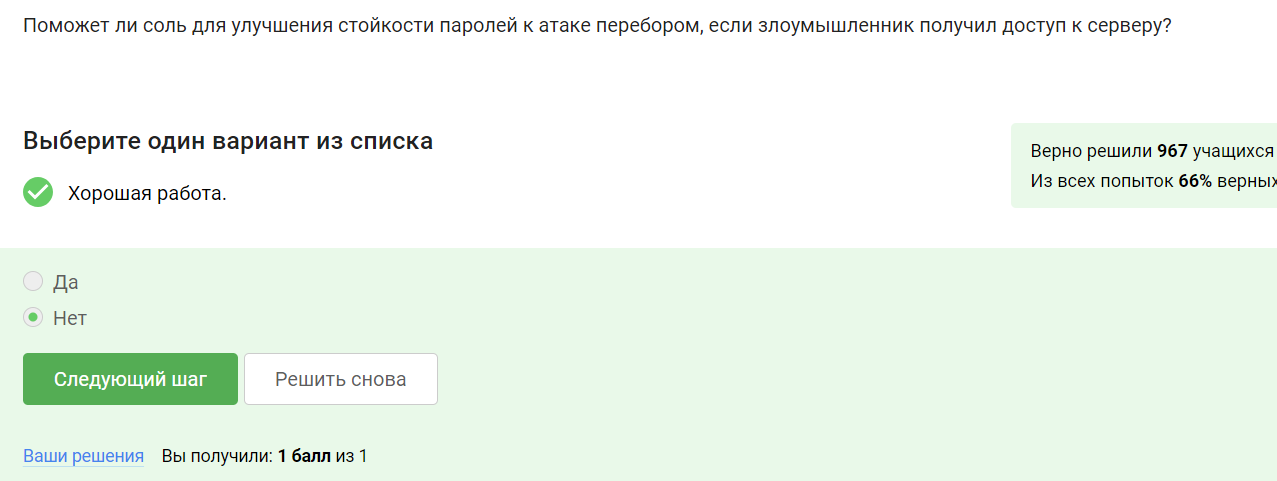


Рис. 30: Задание 2.2.5

1. От атак перебором помогают следующие действия: капча, длинные и сложные пароли, различные пароли, переодическая смена паролей. (рис. 31)

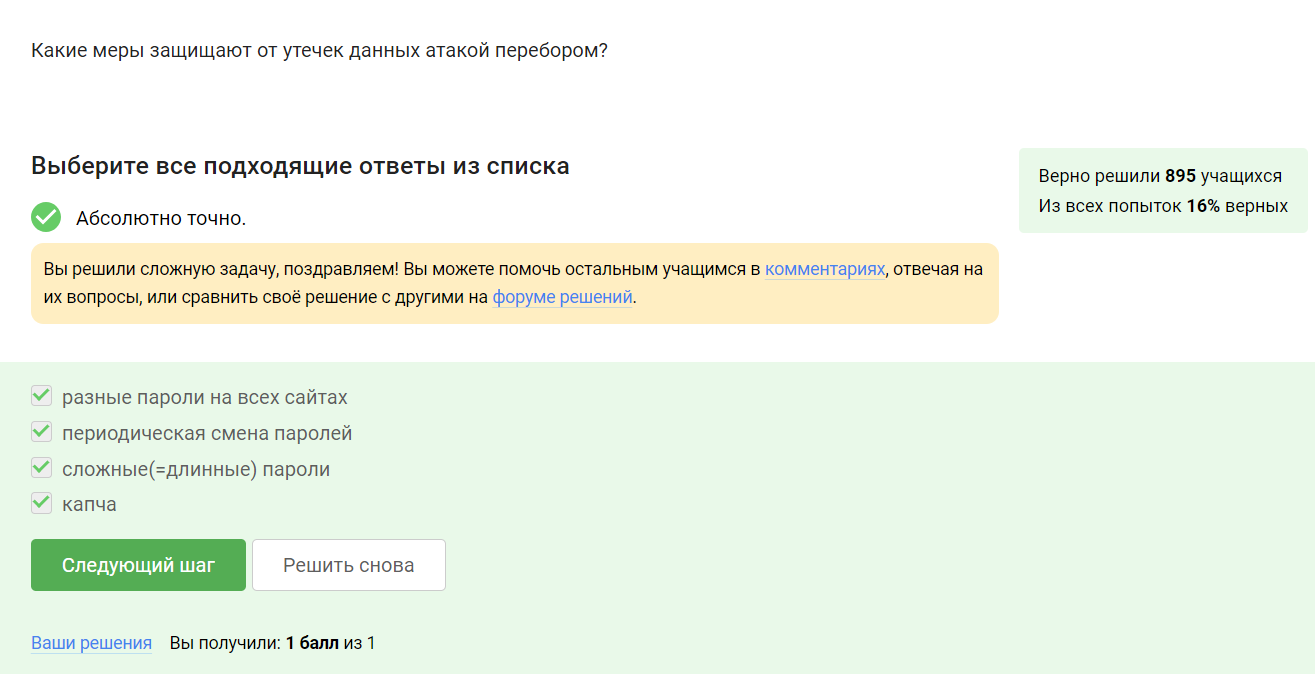


Рис. 31: Задание 2.2.6

## 3.3 Фишинг

1. В данном задании рассматривается такой тип фишинговых атак, как адресный фишинг, когда мы вроде бы переходим на известную нам страницу, но она является поддельной. (рис. 32)

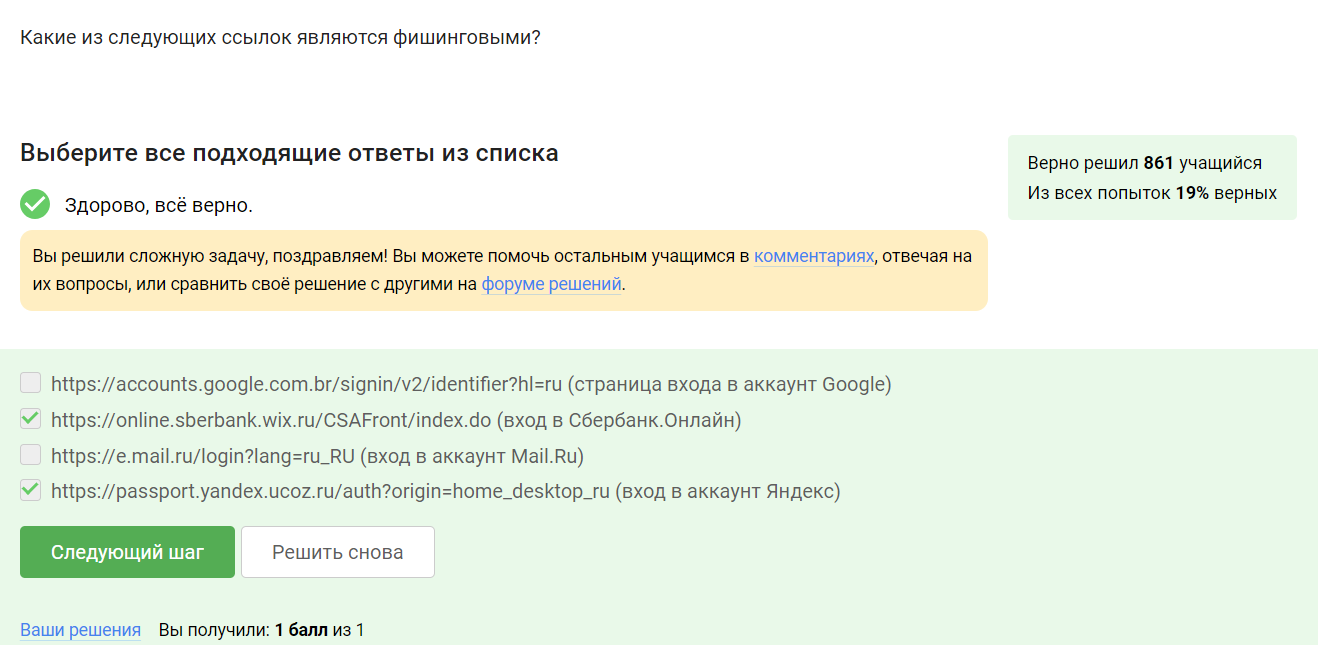


Рис. 32: Задание 2.3.1

1. Да такое возможно, это называет спуфинг, это происходит, потому что SMTP не включает в себя проверку адреса отправителя. (рис. 33)

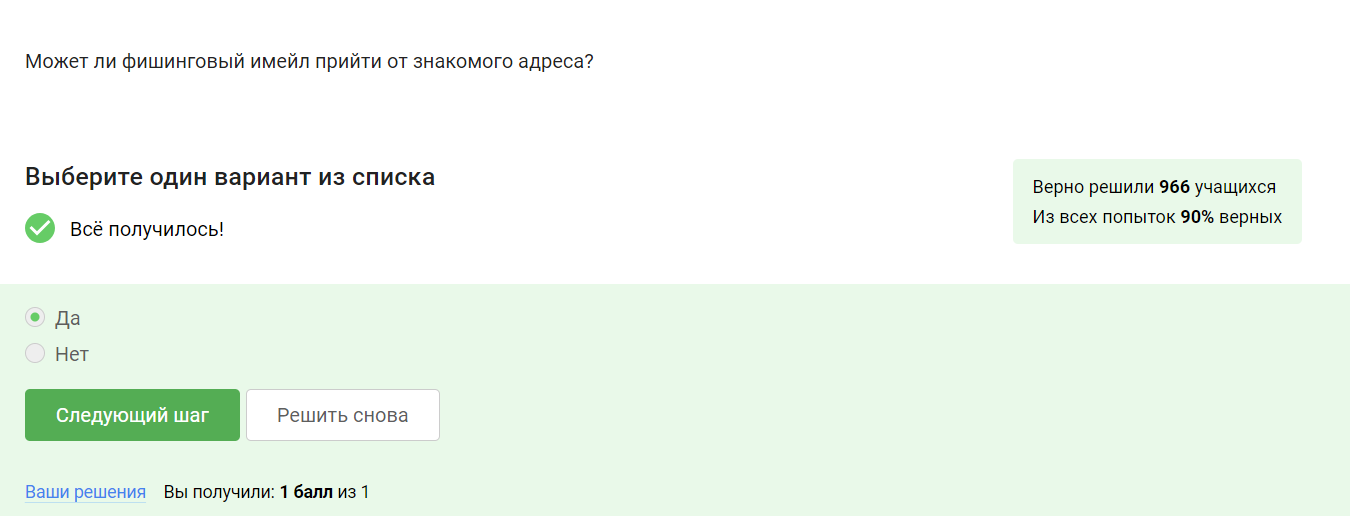


Рис. 33: Задание 2.3.2

## 3.4 Вирусы. Примеры

1. Email спуфинг - это подмена адреса отправителя в емайлах. (рис. 34)

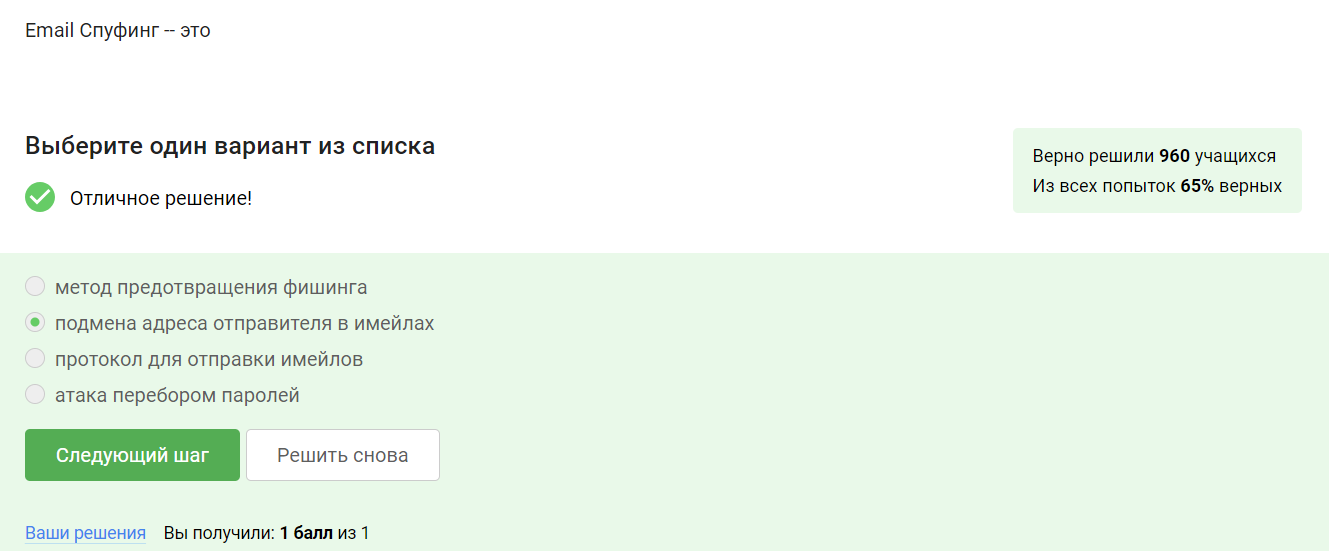


Рис. 34: Задание 2.4.1

1. Троян - это вирус, который маскируется под легитимное ПО. (рис. 35)

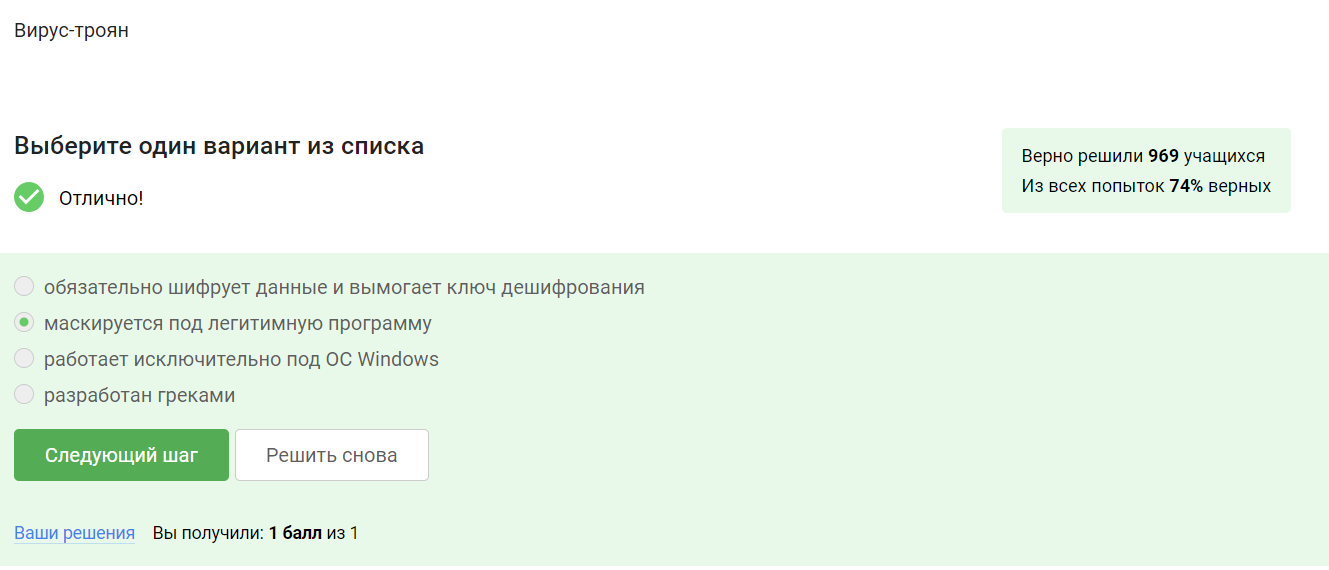


Рис. 35: Задание 2.4.2

## 3.5 Безопасность мессенджеров

1. В протоколе мессенджеров Signal ключ формируется при генерации первого сообщения строной-отправителем. (рис. 36)

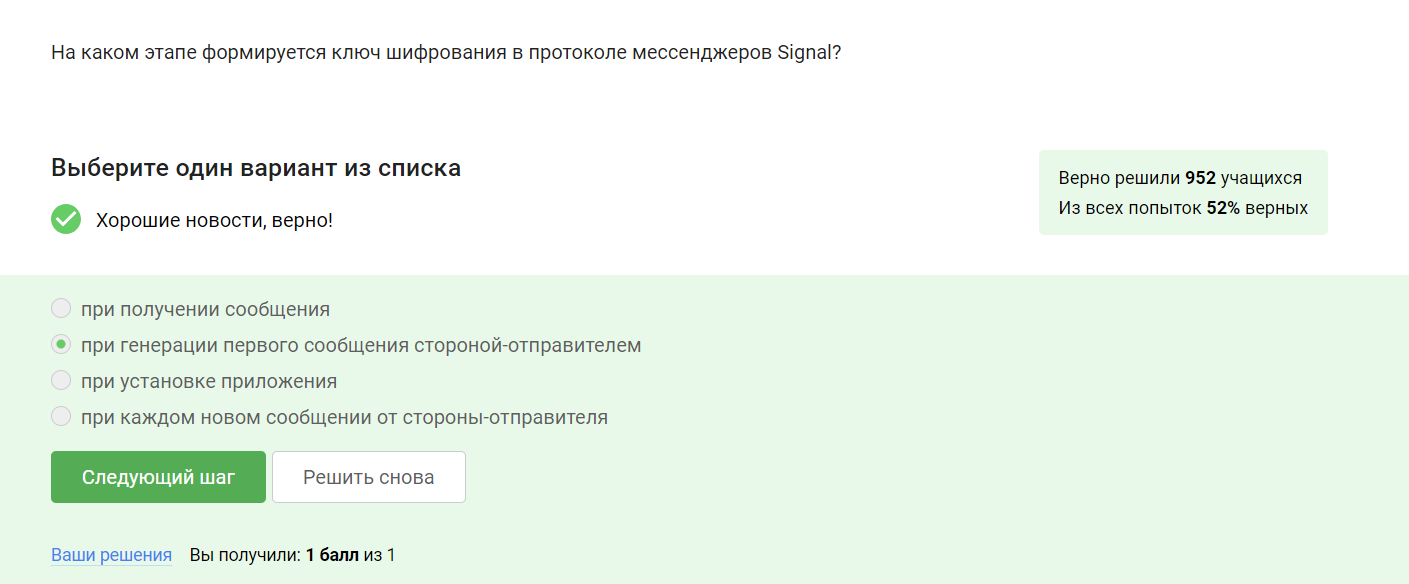


Рис. 36: Задание 2.5.1

1. Суть сквозного шифрования состоит в том, что отправитель передает на сервер уже зашифрованное сообщение, сервер отправляет шифрованные данные получателю, а тот их дешифрует, таким образом сервер значет только куда надо передать сообщение. (рис. 37)

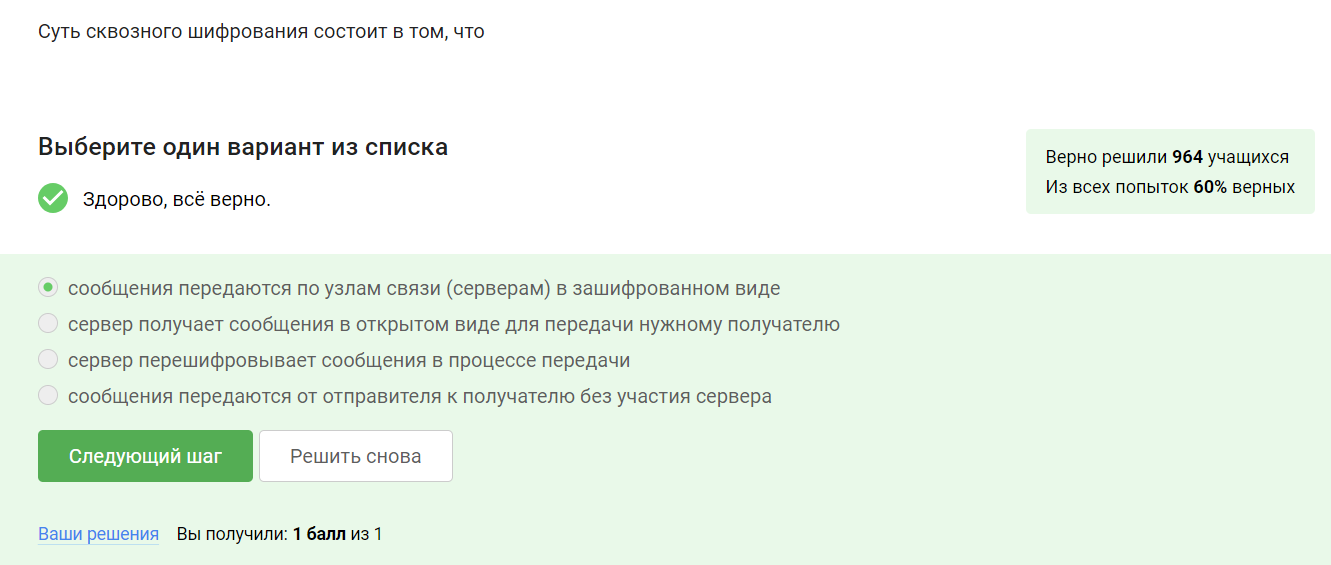


Рис. 37: Задание 2.5.2

# 4 Криптография на практике

## 4.1 Введение в криптографию

1. В асимметричных криптографических примитивах обе стороны имеют пару ключей - публичный и секретный. (рис. 38)

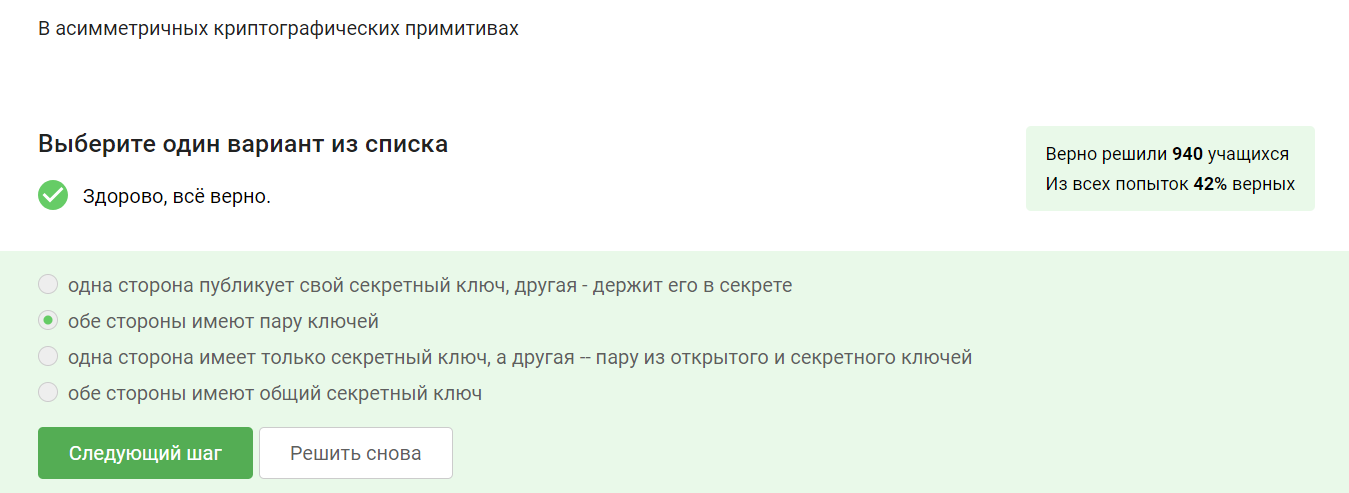


Рис. 38: Задание 3.1.1

1. Криптографическая хэш-функция обладает следующими свойствами: возвращает последовательность бит фиксированной длинны, устойчива к коллизиям и эффективно вычисляется. (рис. 39)

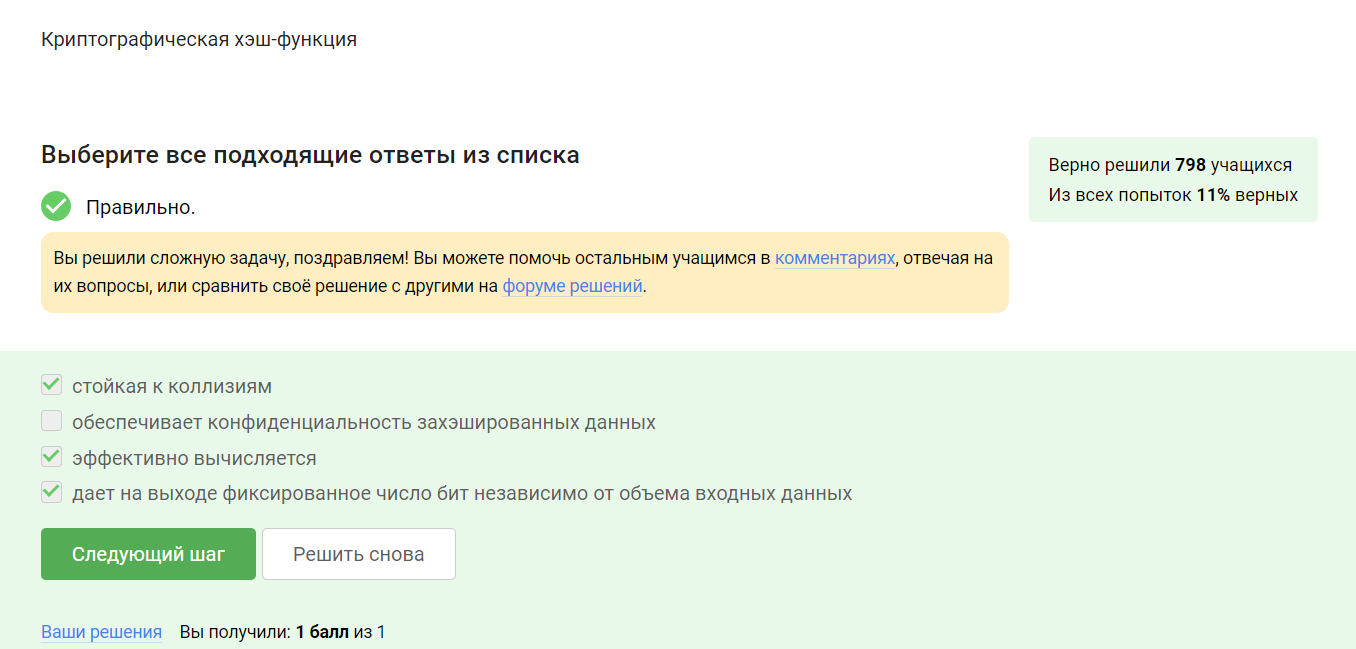


Рис. 39: Задание 3.1.2

1. К алгоритмам цифровой подписи относятся: RSA, американский стандарт ECDSA, российский стандарт ГОСТ Р 34.10-2012. (рис. 40)

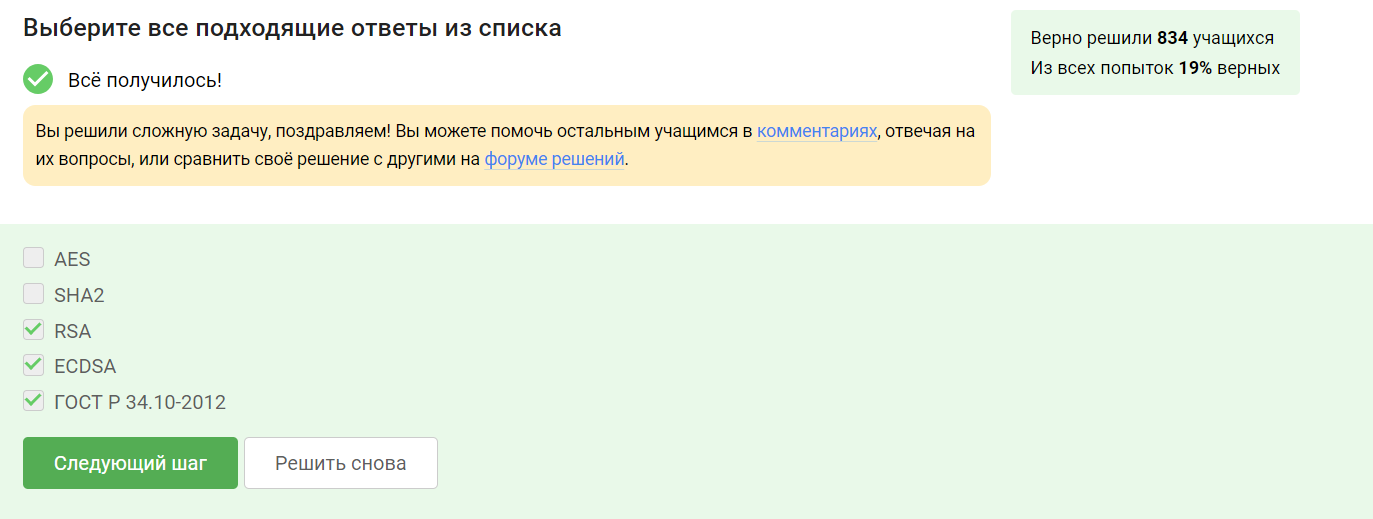


Рис. 40: Задание 3.1.3

1. Код аутентификации сообщения относится к симметричным примитивам. (рис. 41)

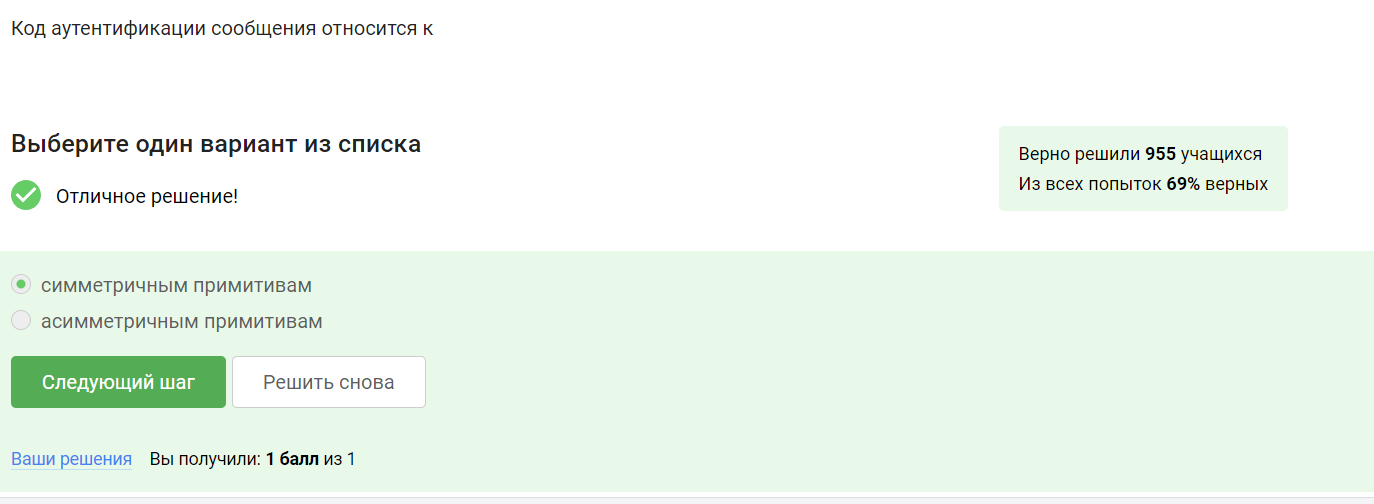


Рис. 41: Задание 3.1.4

1. Обмен ключам Диффи-Хэллмана - это ассиметричный примитив, который используется для генерации общего секретного ключа. (рис. 42)

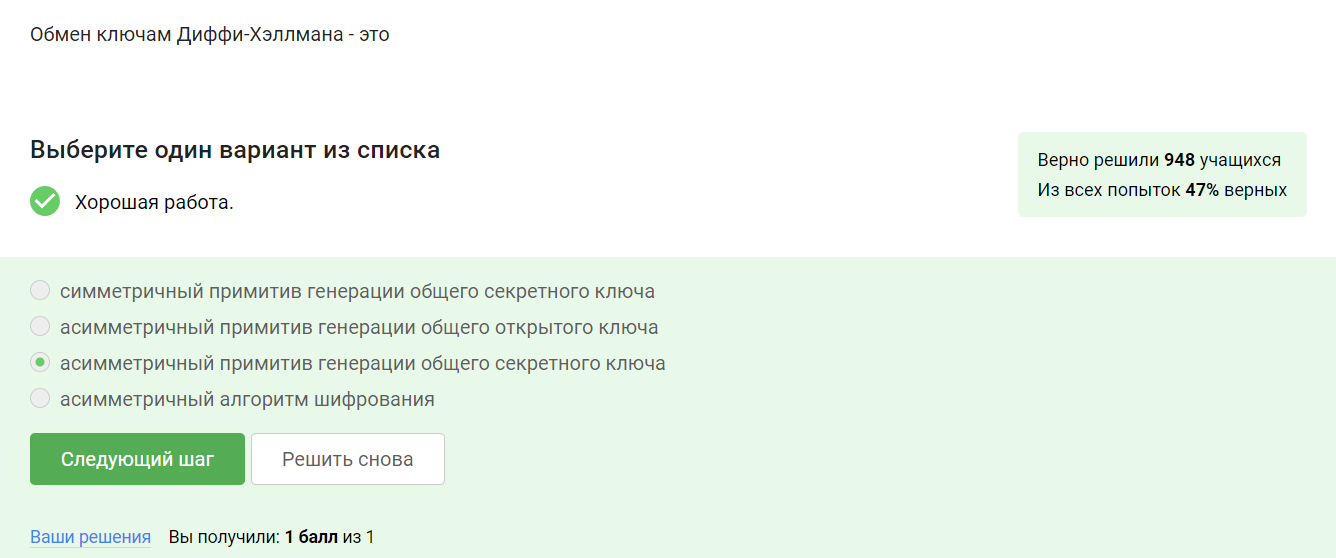


Рис. 42: Задание 3.1.5

## 4.2 Цифровая подпись

1. Протокол электронной цифровой подписи относится к ассиметричным протоколам, то есть с публичным и секретным ключами. (рис. 43)

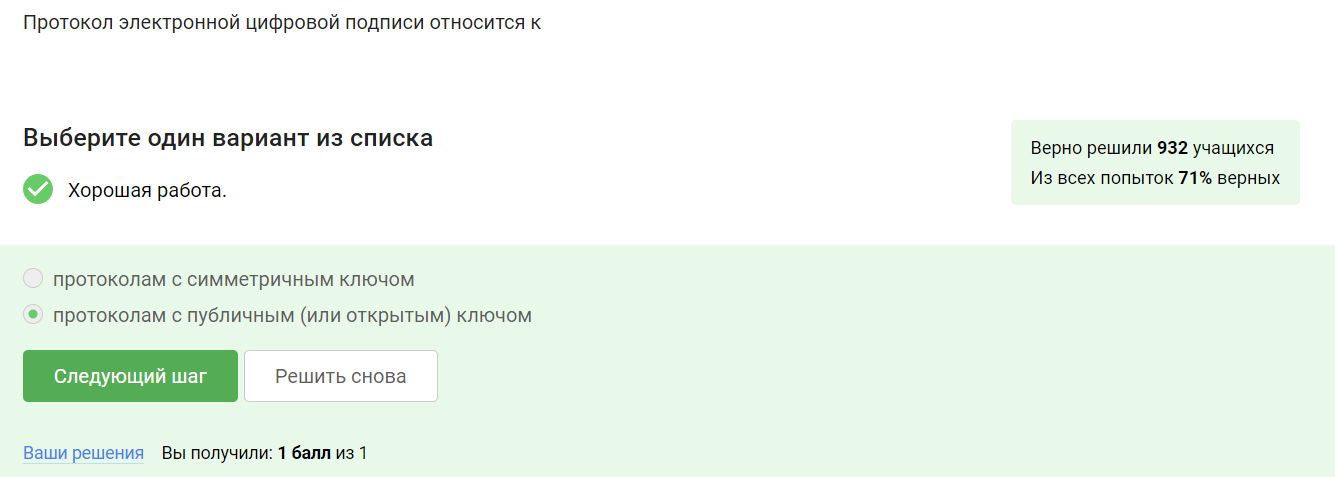


Рис. 43: Задание 3.2.1

1. Алгоритм верификации электронной цифровой подписи требует на вход три вещи - это подпись, сообщение и открытый ключ. (рис. 44)

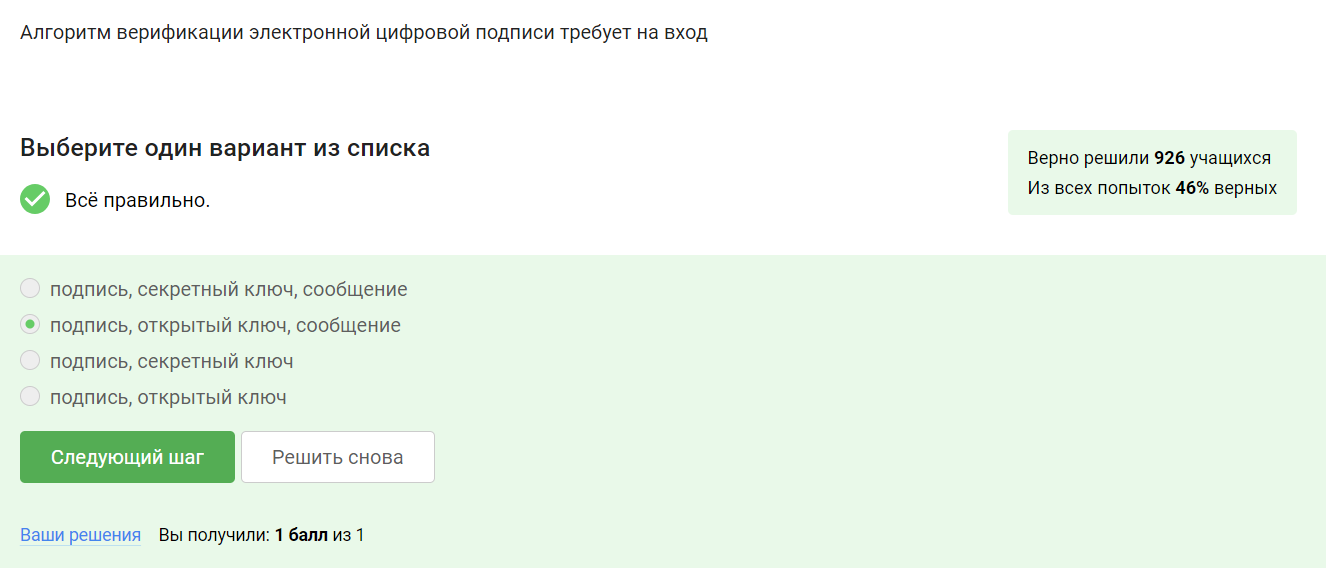


Рис. 44: Задание 3.2.2

1. Электронная цифровая подпись не обеспечивает конфиденциальности - она используется для аутентификации, проверки на целостность и неотказ от авторства. (рис. 45)

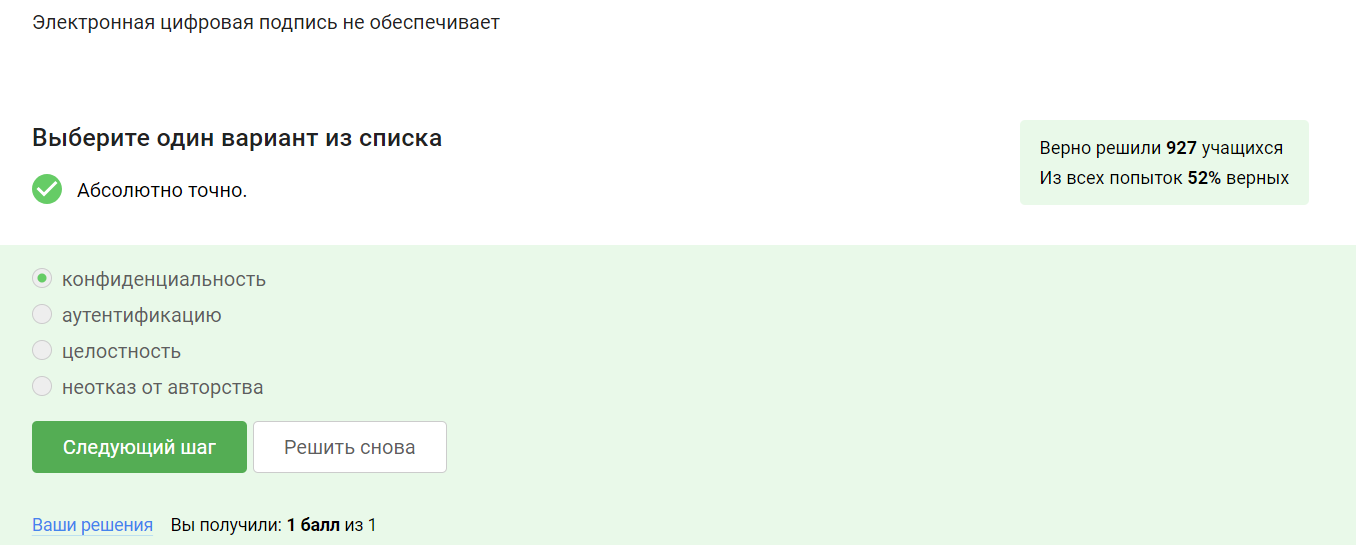


Рис. 45: Задание 3.2.3

1. Для отправки налоговой отчетности в ФНС необходимо использовать усиленную квалифицированную подпись. (рис. 46)

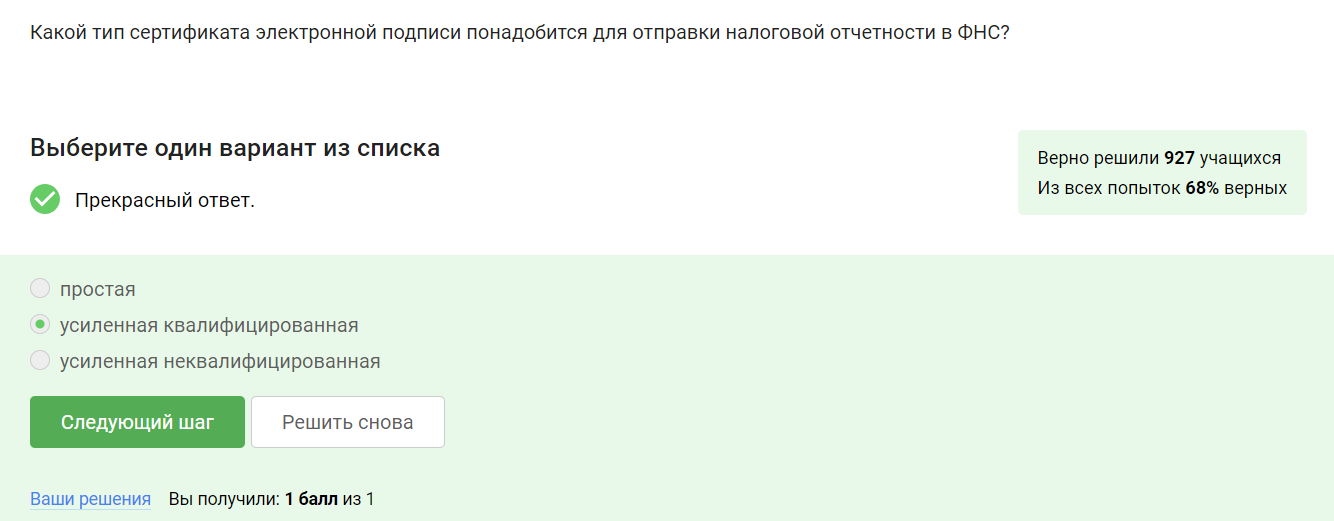


Рис. 46: Задание 3.2.4

1. Квалифицированный сертификат можно получить в сертификационном центре. (рис. 47)

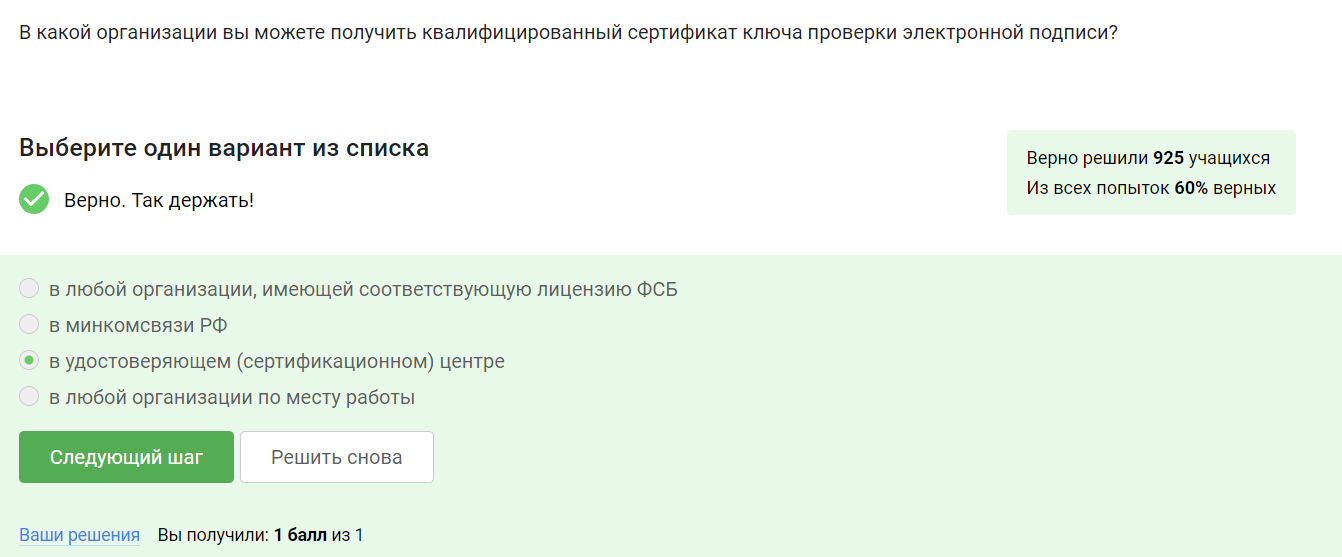


Рис. 47: Задание 3.2.5

## 4.3 Электронные платежи

1. Выбираем платежные системы MasterCard и МИР. (рис. 48)

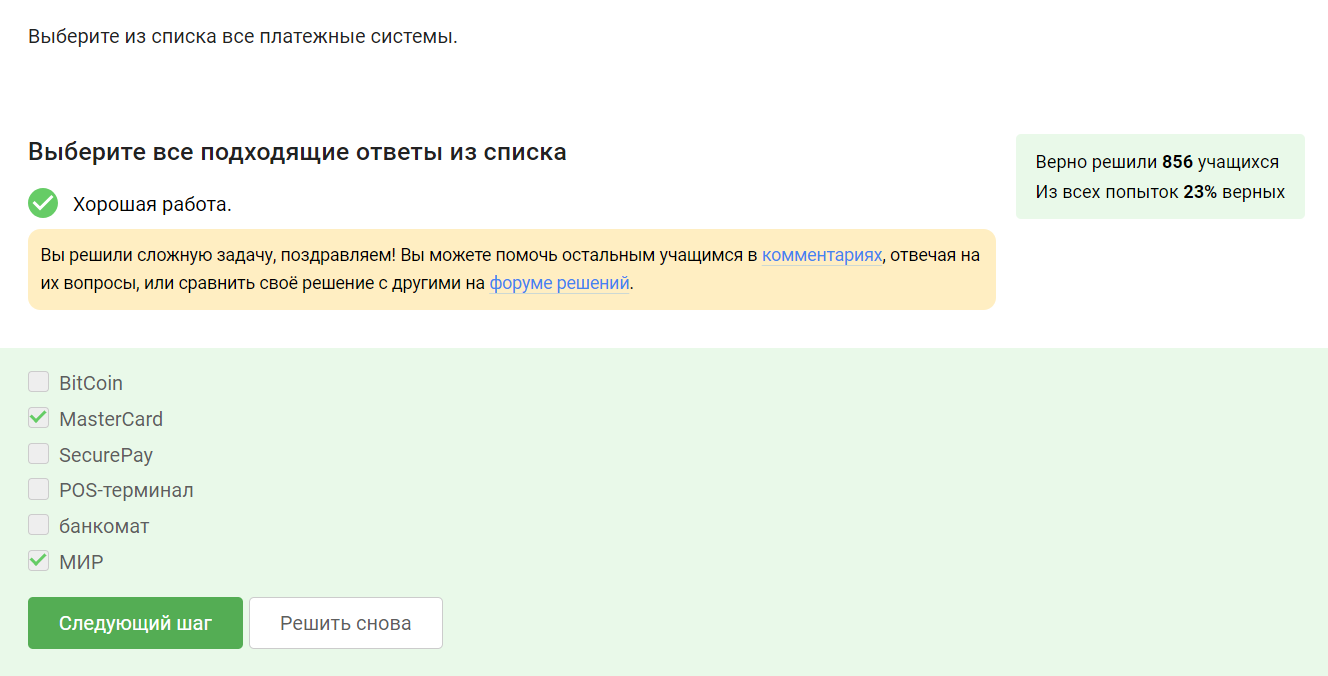


Рис. 48: Задание 3.3.1

1. Примером многофакторной аутентификации является те, что я выбрал. (рис. 49)

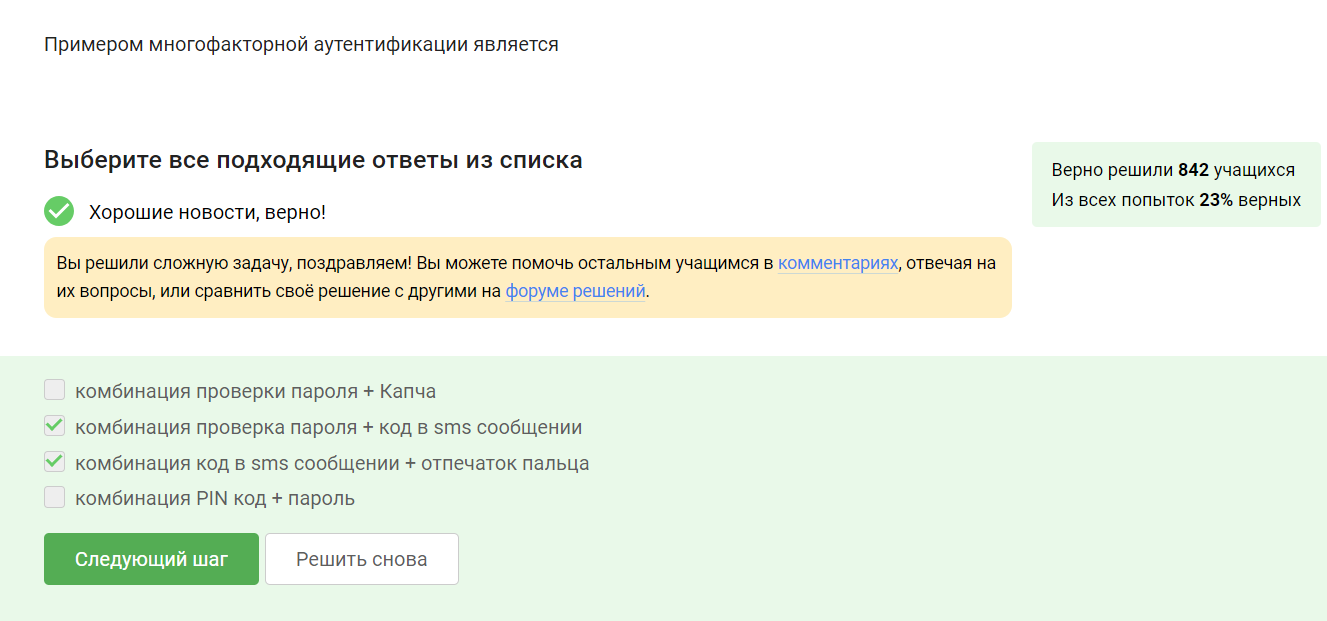


Рис. 49: Задание 3.3.2

1. При онлайн платежах сегодня используется многофакторная аутентификация покупателя перед банком-эмитентом. (рис. 50)

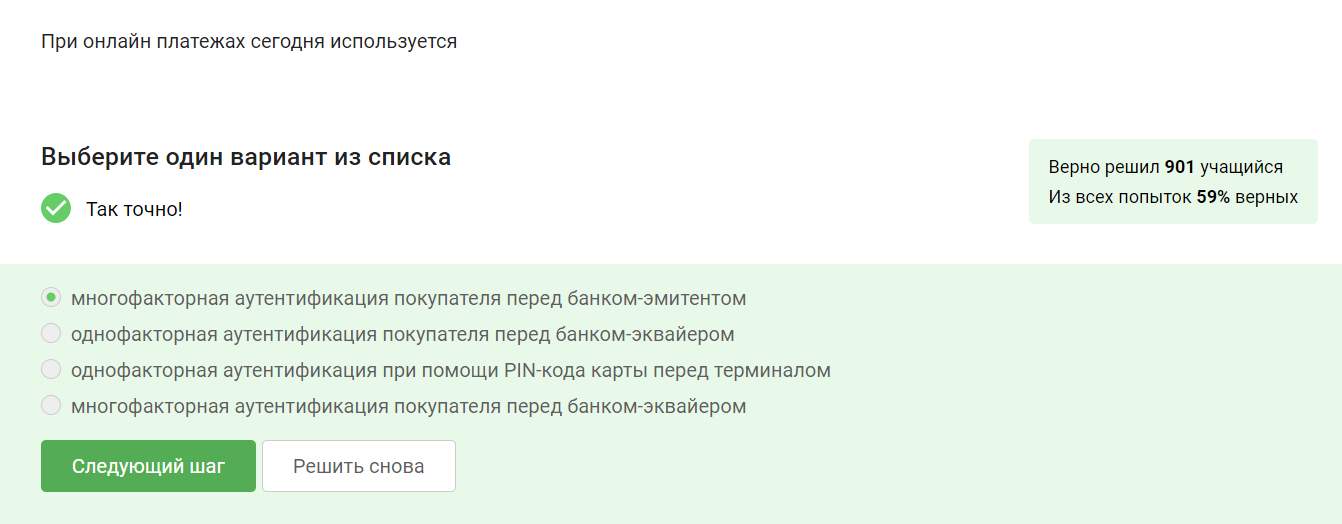


Рис. 50: Задание 3.3.3

## 4.4 Блокчейн

1. В доказательстве работы используется сложность вычисления прообраза хэш-функции, так как единственным эффективным способом атаки на хэш-функцию является перебор. (рис. 51)

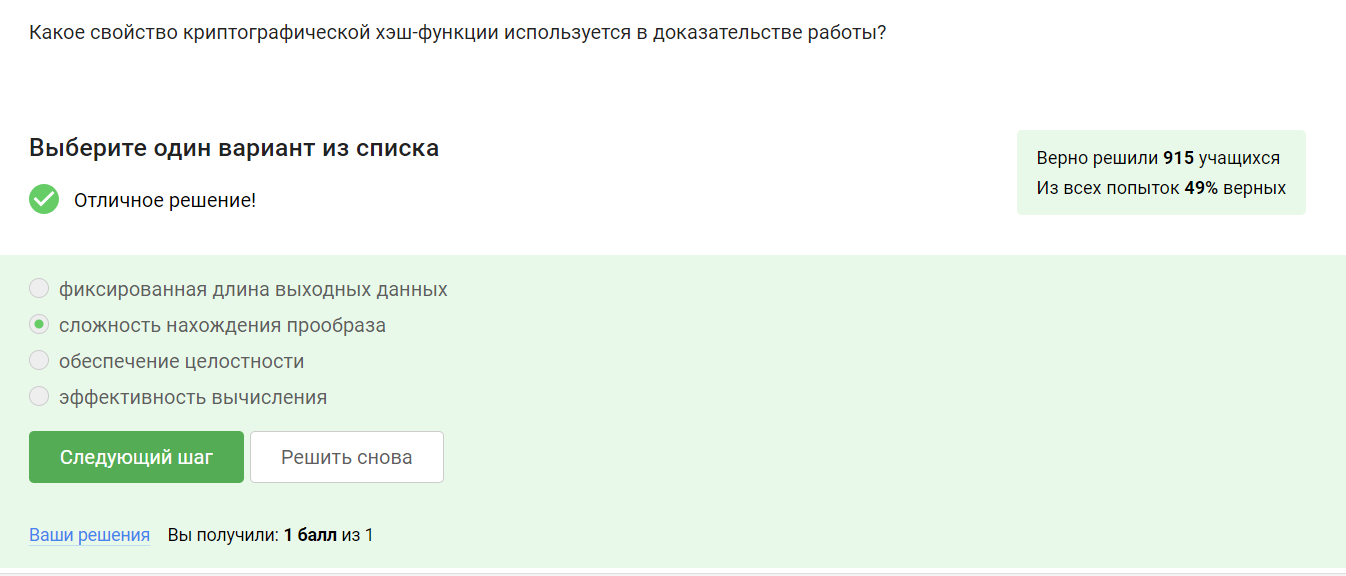


Рис. 51: Задание 3.4.1

1. Консенсус в некоторых системах блокчейн обладает свойствами - живучесть, консенсус, постоянства, открытость. (рис. 52)

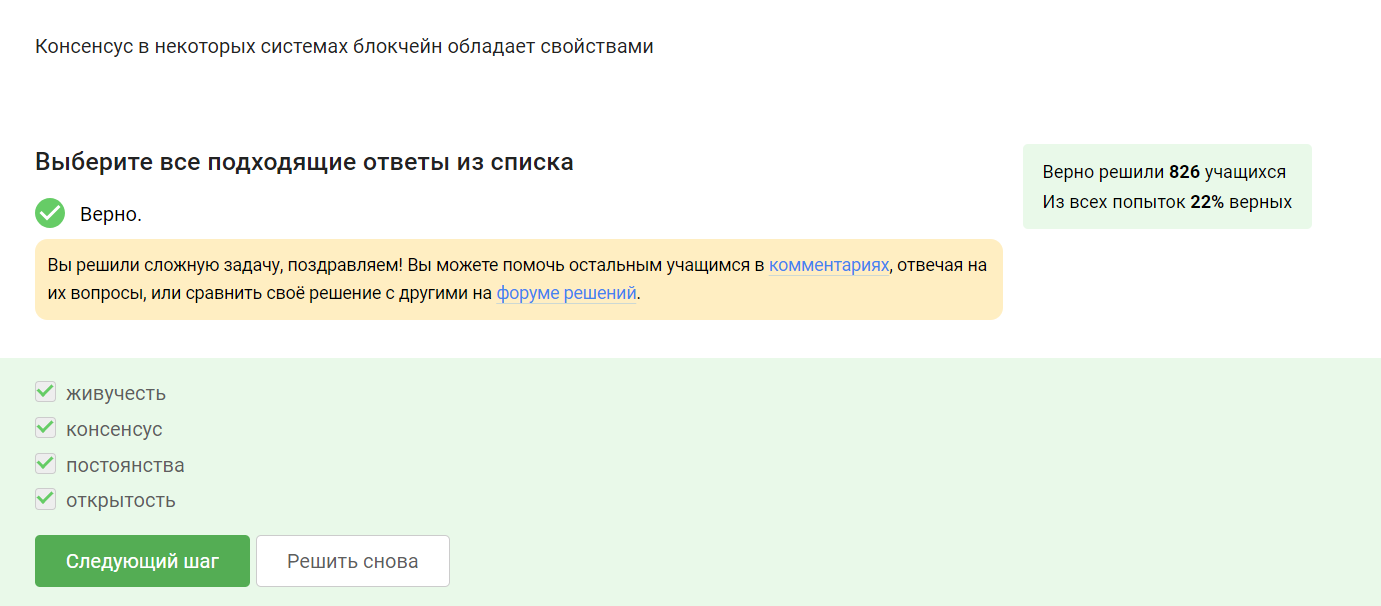


Рис. 52: Задание 3.4.2

1. Участники блокчейна хранят секретные ключи электронной подписи, которые используют для подписи транзакций. (рис. 53)

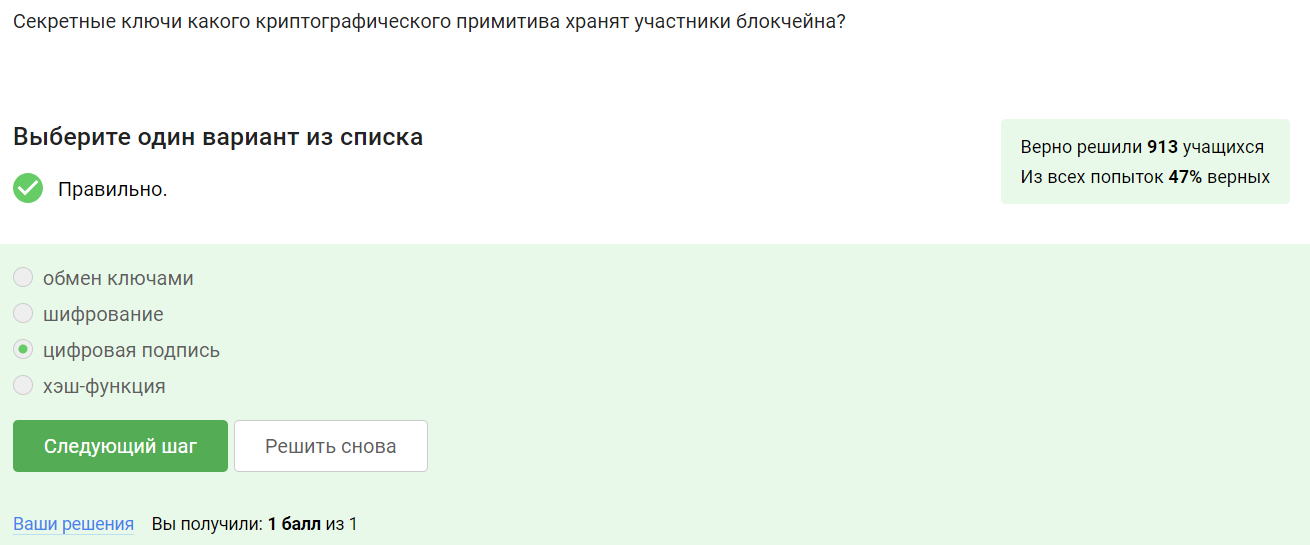


Рис. 53: Задание 3.4.3

# 5 Выводы

Были изучены основы кибербезопасности.