Отчет по части “Криптография на практике” курса “Основы кибербезопасности”

Стариков Данила Андреевич

Содержание

# 1 Цель работы

Познакомиться со следующими понятиями: - Электронная подпись - Электронные платежи - Блокчейн

# 2 Выполнение лабораторной работы

## 2.1 Введение в криптографию

* Вопрос 1. В асимметричных криптографических примитивах(рис. 1):

Ответ: *обе стороны имеют пару ключей*.

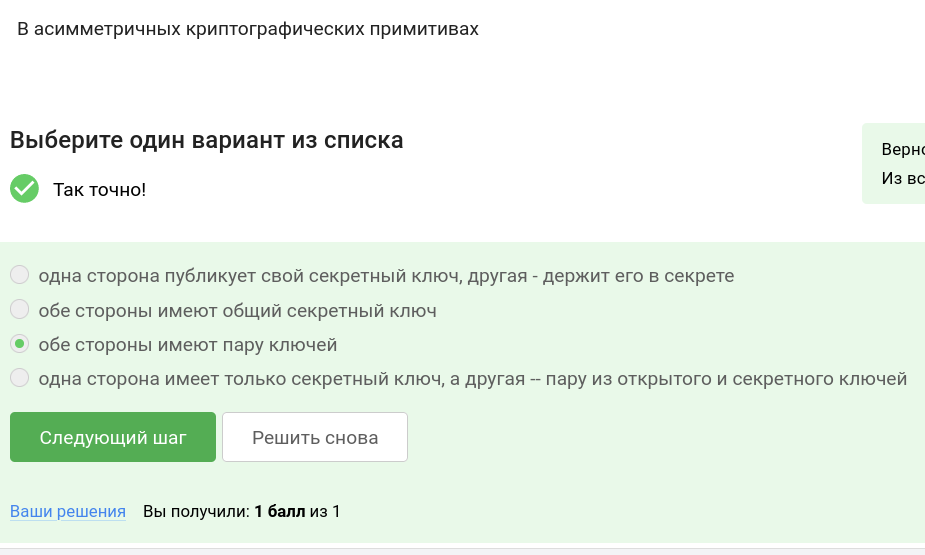


Рис. 1: Скриншот выполнения задания

* Вопрос 2. Криптографическая хэш-функция(рис. 2):

Ответ: *эффективно вычисляется, дает на выходе фиксированное число бит независимо от объема входных данных, стойкая к коллизиям*.

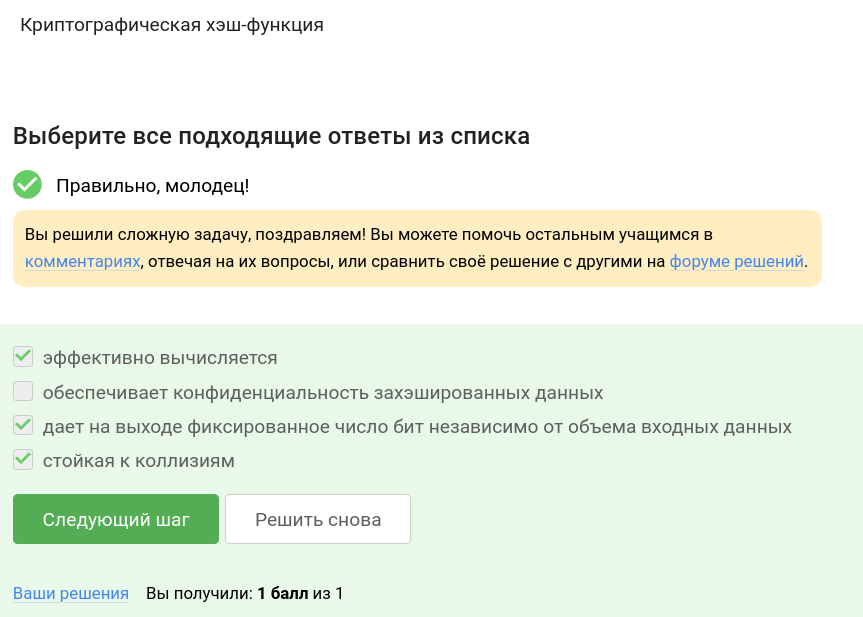


Рис. 2: Скриншот выполнения задания

* Вопрос 3. К алгоритмам цифровой подписи относятся(рис. 3):

Ответ: *RSA, ECDSA, ГОСТ Р 34.10-2012* .

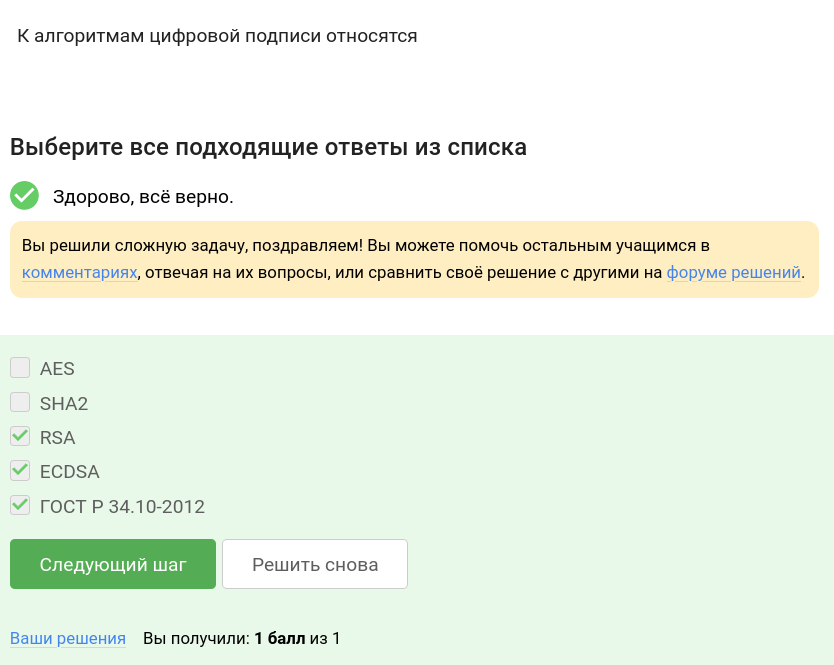


Рис. 3: Скриншот выполнения задания

* Вопрос 4. Код аутентификации сообщения относится к(рис. 4):

Ответ: *симметричным примитивам*.

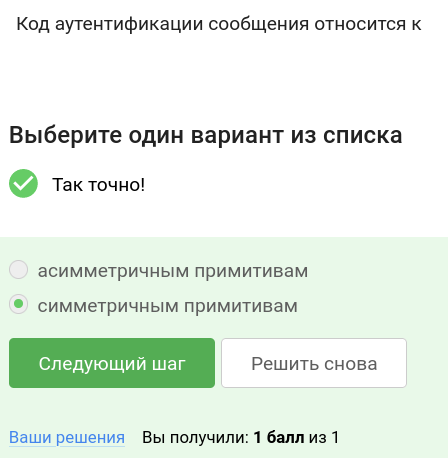


Рис. 4: Скриншот выполнения задания

* Вопрос 5. Обмен ключам Диффи-Хэллмана - это(рис. 5):

Ответ: *асимметричный примитив генерации общего секретного ключа*.

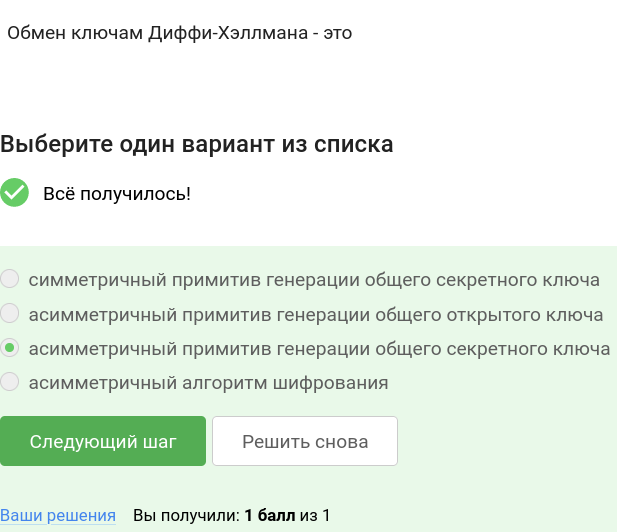


Рис. 5: Скриншот выполнения задания

## 2.2 Цифровая подпись

* Вопрос 1. Протокол электронной цифровой подписи относится к(рис. 6):

Ответ: *протоколам с публичным (или открытым) ключом*.

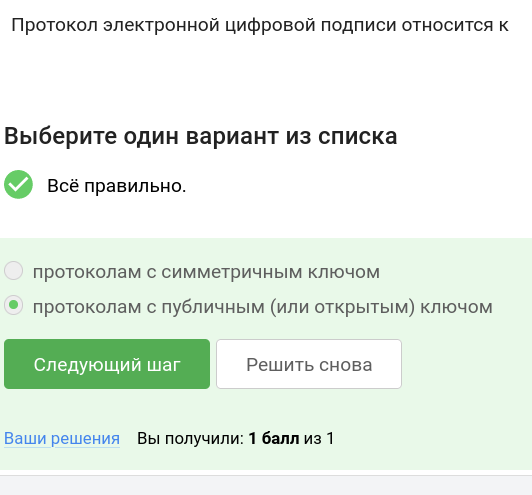


Рис. 6: Скриншот выполнения задания

* Вопрос 2. Алгоритм верификации электронной цифровой подписи требует на вход(рис. 7):

Ответ: *подпись, открытый ключ, сообщение*.

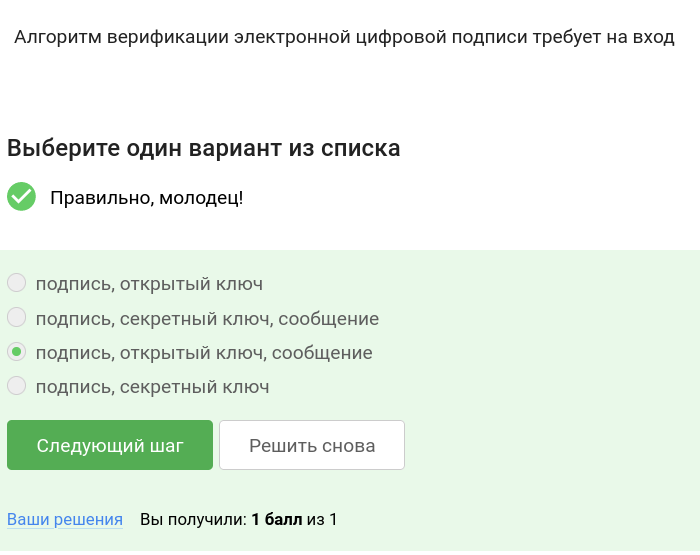


Рис. 7: Скриншот выполнения задания

* Вопрос 3. Электронная цифровая подпись не обеспечивает(рис. 8):

Ответ: *конфиденциальность*.

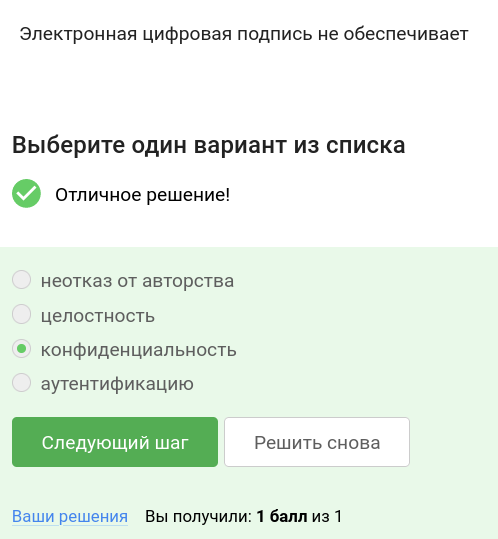


Рис. 8: Скриншот выполнения задания

* Вопрос 4. Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?(рис. 9):

Ответ: *усиленная квалифицированная*.

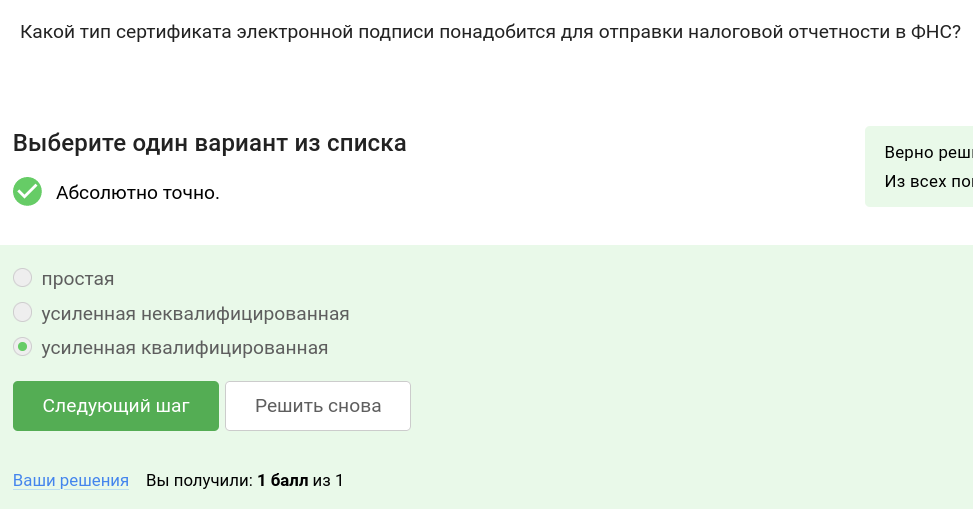


Рис. 9: Скриншот выполнения задания

* Вопрос 5. В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?(рис. 10):

Ответ: *в удостоверяющем (сертификационном) центре*.

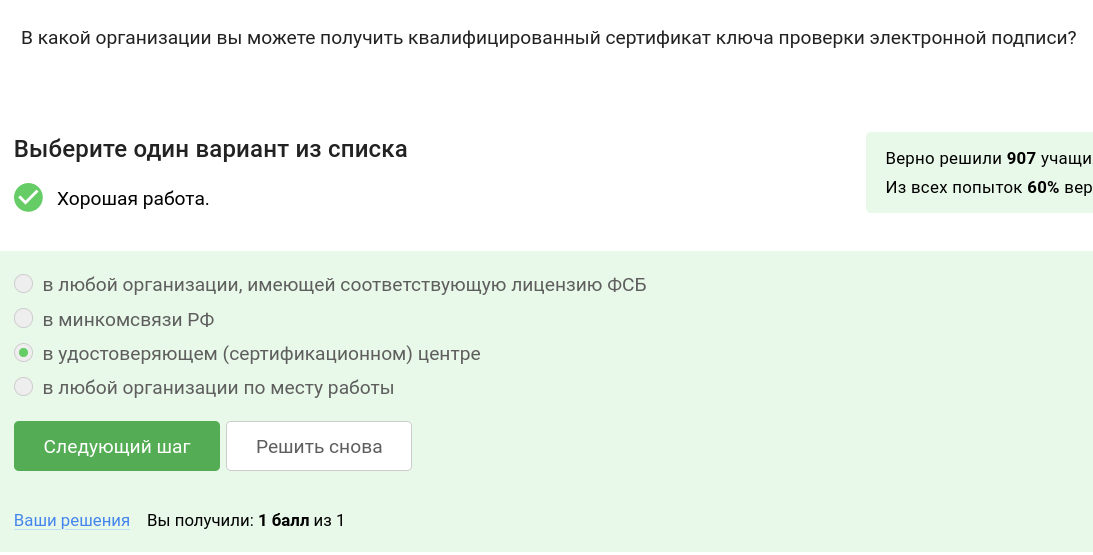


Рис. 10: Скриншот выполнения задания

## 2.3 Электронные платежи

* Вопрос 1. Выберите из списка все платежные системы.(рис. 11):

Ответ: *MasterCard, МИР*.

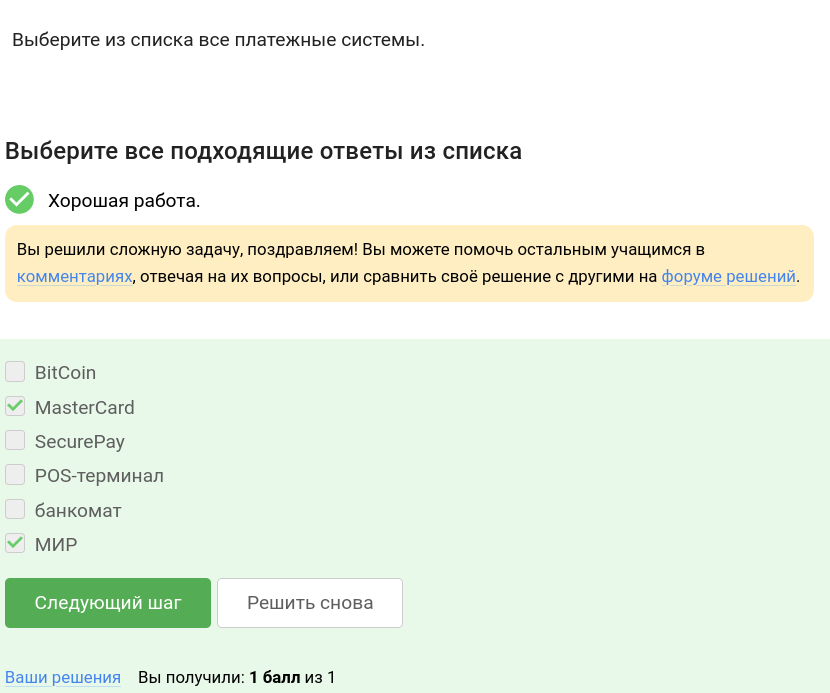


Рис. 11: Скриншот выполнения задания

* Вопрос 2. Примером многофакторной аутентификации является(рис. 12):

Ответ: *комбинация проверка пароля + код в sms сообщении, комбинация код в sms сообщении + отпечаток пальца* .

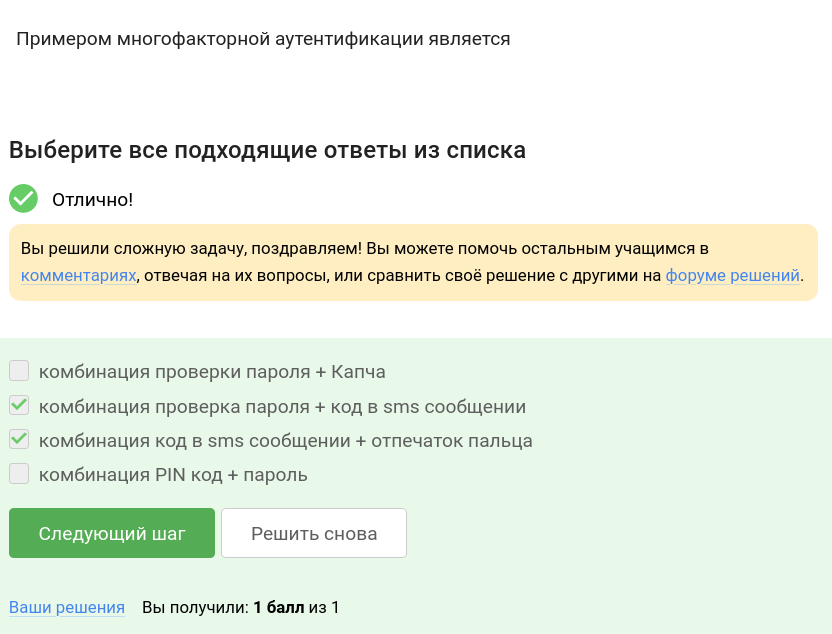


Рис. 12: Скриншот выполнения задания

* Вопрос 3. При онлайн платежах сегодня используется(рис. 13):

Ответ: *многофакторная аутентификация покупателя перед банком-эмитентом*.

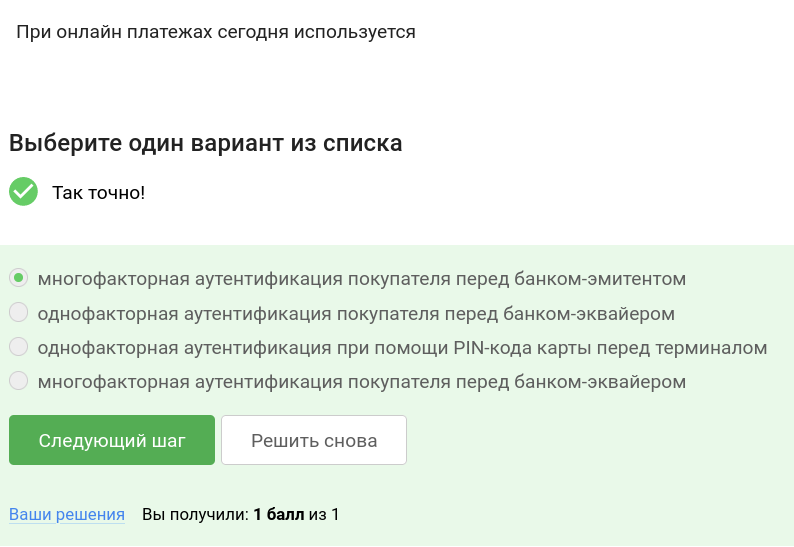


Рис. 13: Скриншот выполнения задания

## 2.4 Блокчейн

* Вопрос 1. Какое свойство криптографической хэш-функции используется в доказательстве работы?(рис. 14):

Ответ: *сложность нахождения прообраза*.

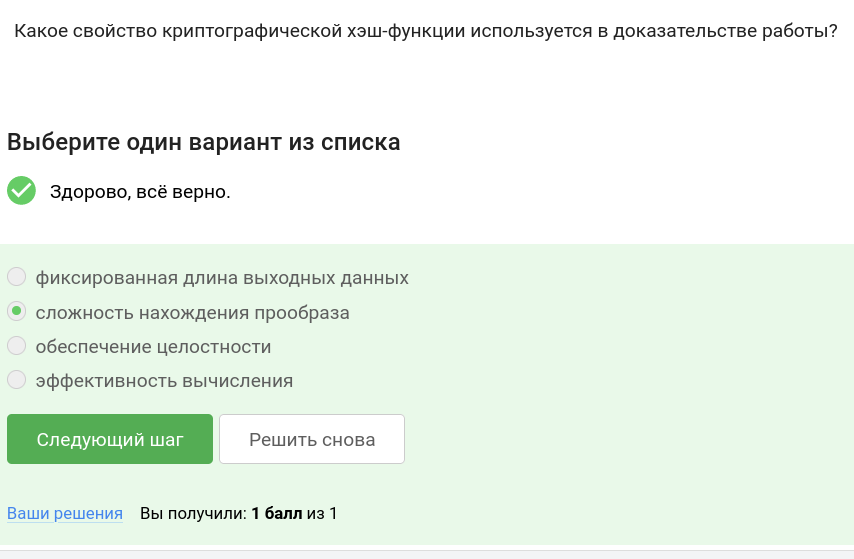


Рис. 14: Скриншот выполнения задания

* Вопрос 2. Консенсус в некоторых системах блокчейн обладает свойствами(рис. 15):

Ответ: *постоянства, консенсус, живучесть, открытость*.

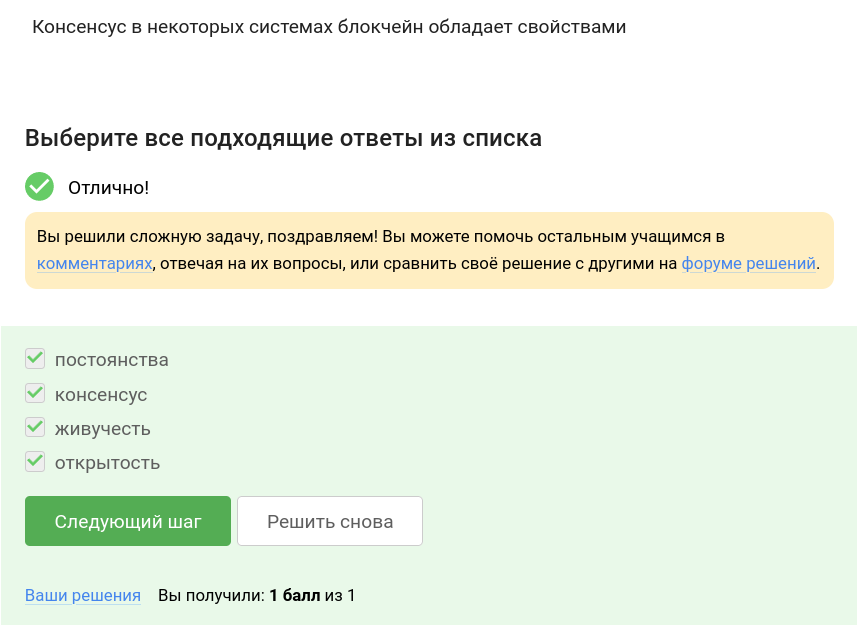


Рис. 15: Скриншот выполнения задания

* Вопрос 3. Секретные ключи какого криптографического примитива хранят участники блокчейна?(рис. 16):

Ответ: *цифровая подпись*.

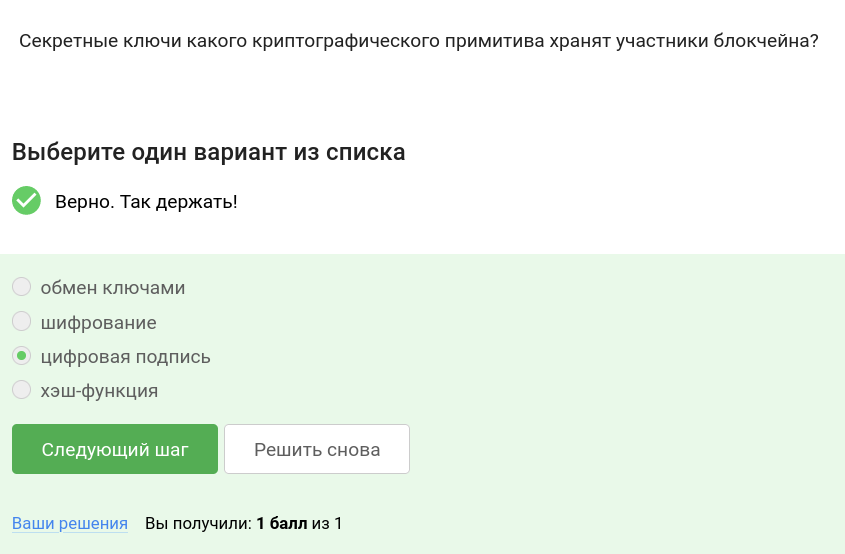


Рис. 16: Скриншот выполнения задания

# 3 Выводы

В рамках третьего модуля познакомились с основами криптографии: электронной подписью, электронными платежами, блокчейном.