Прохождения внешнего курса на тему Основы кибербезопасности. Часть 3

Основы информационной безопасности

Просина Ксения Максимовна

Содержание

# 1 4 Криптография на практике

## 1.1 4.1 Введение в криптографию

Вопрос/Ответ 1 (рис. 1)

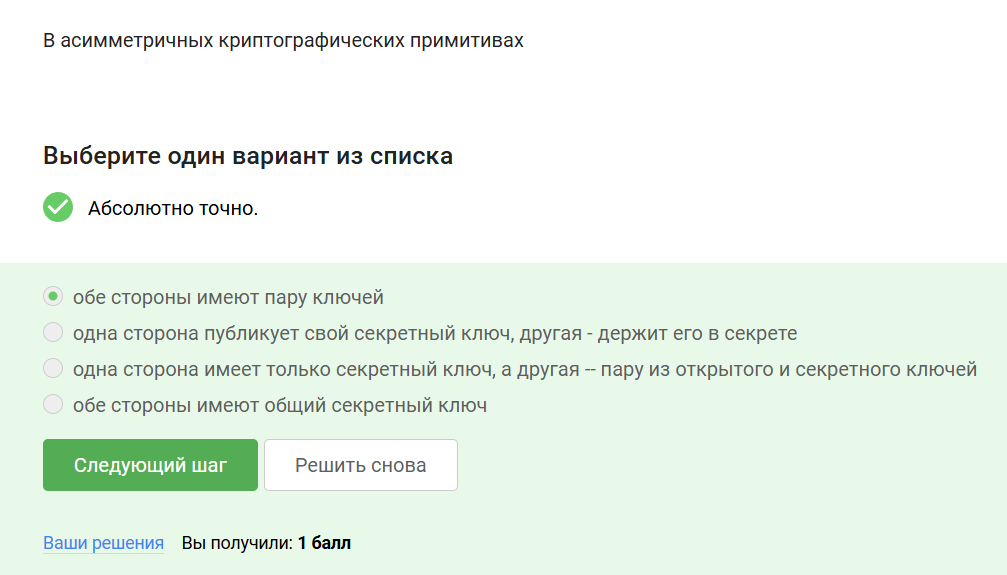


Рис. 1: Вопрос/Ответ 1

Пояснение ответа: В асимметричных криптографических примитивах обе стороны имеют пару ключей, у каждого из сторон есть пара ключей: открытый ключ и секретный ключ. Открытый ключ публикуется в открытом доступе, а закрытый или секретный сторона хранит у себя.

Вопрос/Ответ 2 (рис. 2)

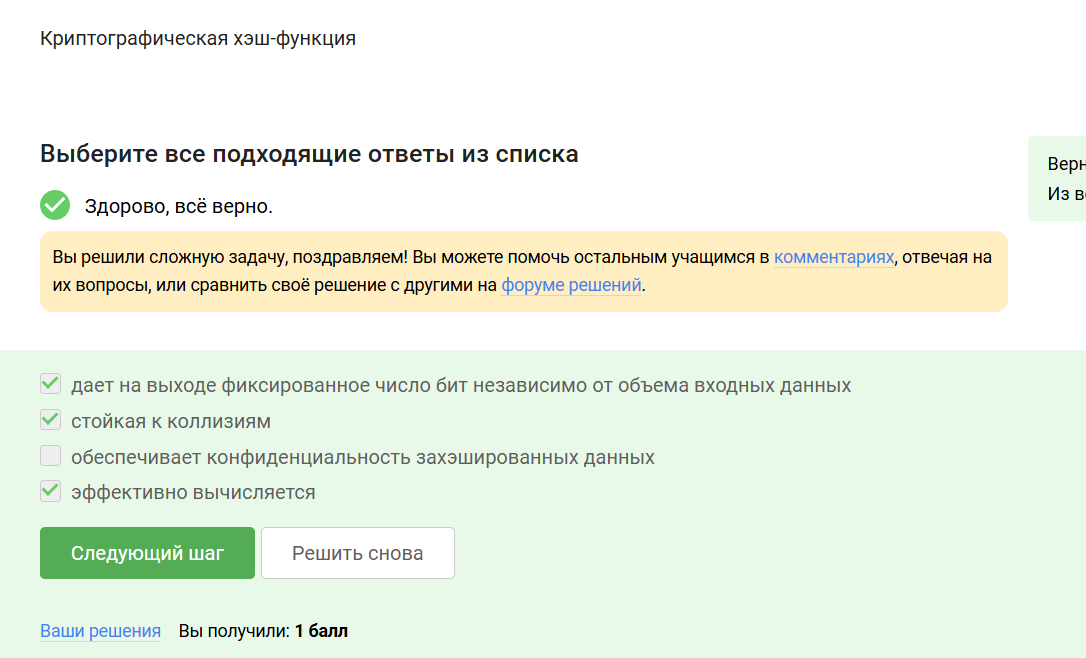


Рис. 2: Вопрос/Ответ 2

Пояснение ответа: Криптографическая хэш-функция:

* Дает на выходк фиксированное число бит независимо от объема входных данных
* Стойкая к коллизиям
* Эффективно вычисляется

Вопрос/Ответ 3 (рис. 3)

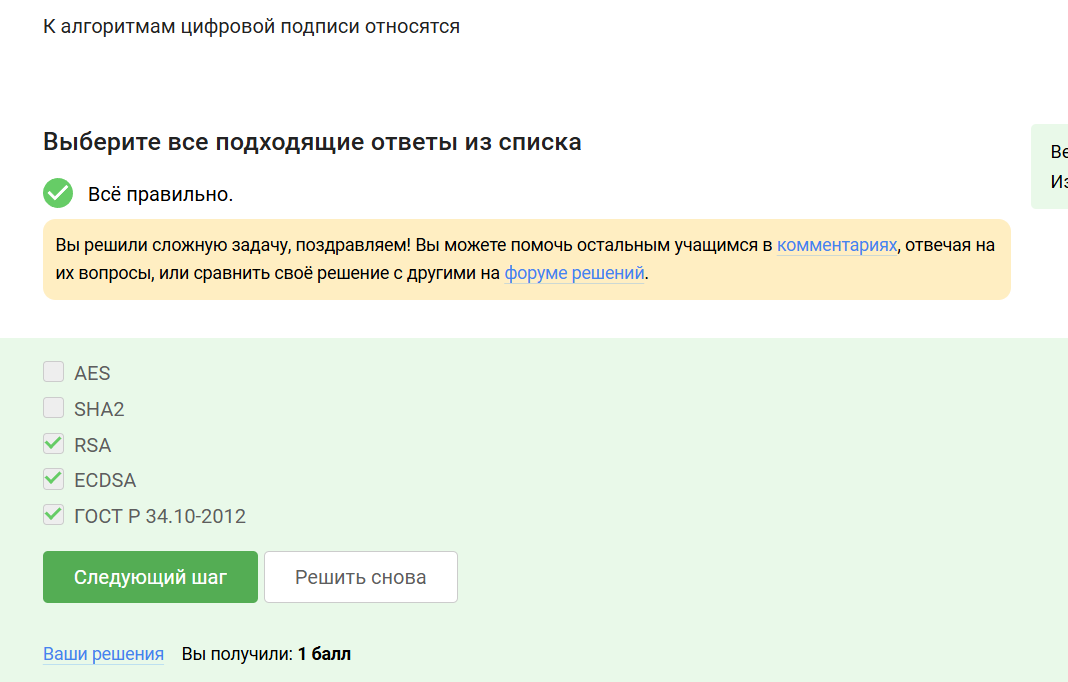


Рис. 3: Вопрос/Ответ 3

Пояснение ответа: К алгоритмам цифровой подписи относятся: RSA, ECDSA, ГОСТ 34.10-2012

Вопрос/Ответ 4 (рис. 4)

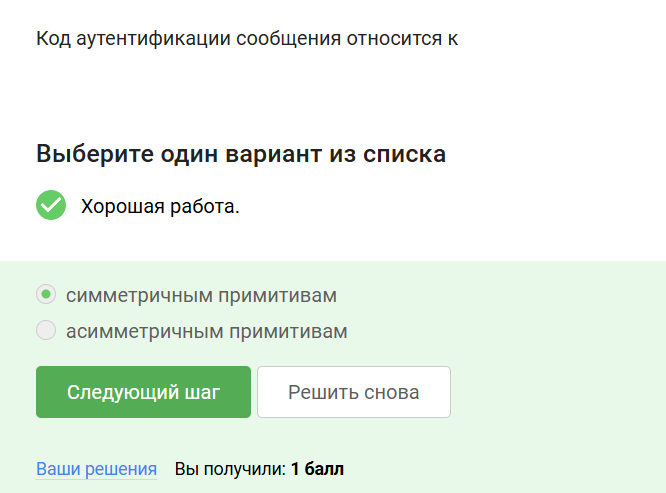


Рис. 4: Вопрос/Ответ 4

Пояснение ответа: Код аутентификации сообщения относится к симметричным примитивам, так как имеется общий ключ.

Вопрос/Ответ 5 (рис. 5)

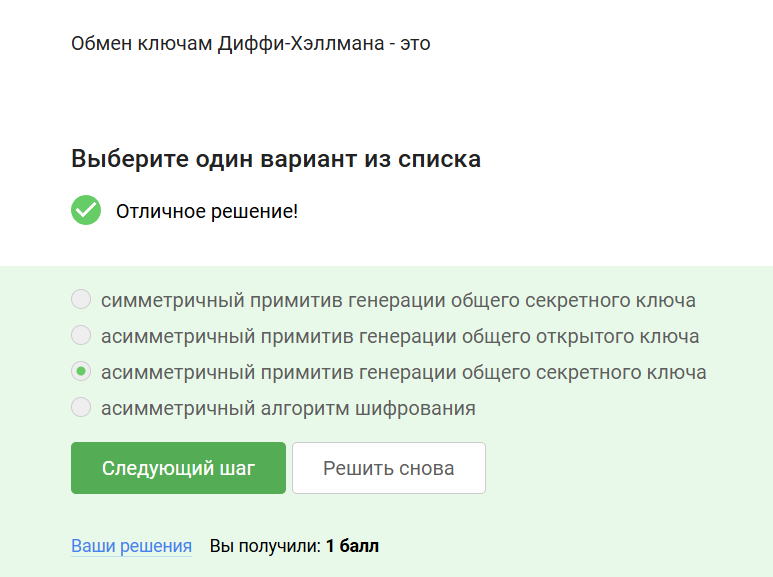


Рис. 5: Вопрос/Ответ 5

Пояснение ответа: Обмен ключами Диффи-Хэллмана-это асимметричный примитив генерации общего секретного ключа.

## 1.2 4.2 Цифровая подпись

Вопрос/Ответ 1 (рис. 6)

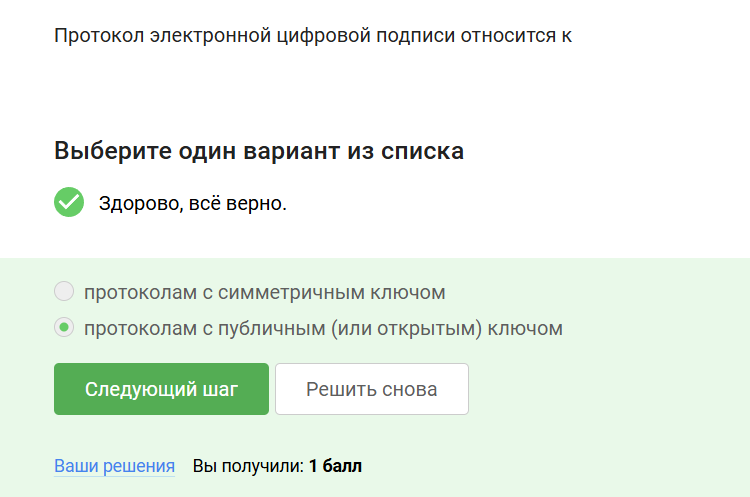


Рис. 6: Вопрос/Ответ 1

Пояснение ответа: Протокол электронной цифровой подписи относится протоколам с публичным (или открытым) ключом.

Вопрос/Ответ 2 (рис. 7)

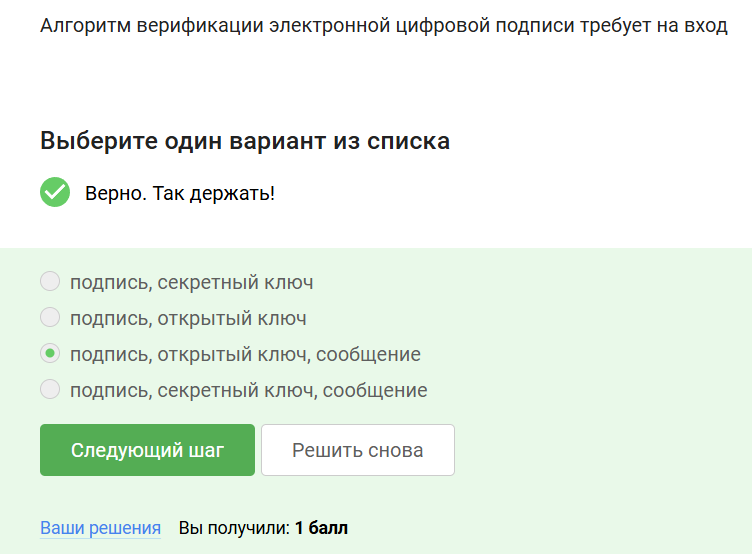


Рис. 7: Вопрос/Ответ 2

Пояснение ответа: Алгоритм верификации электронной цифровой подписи требует на вход:

* подпись
* открытый ключ
* сообщение

Вопрос/Ответ 3 (рис. 8)

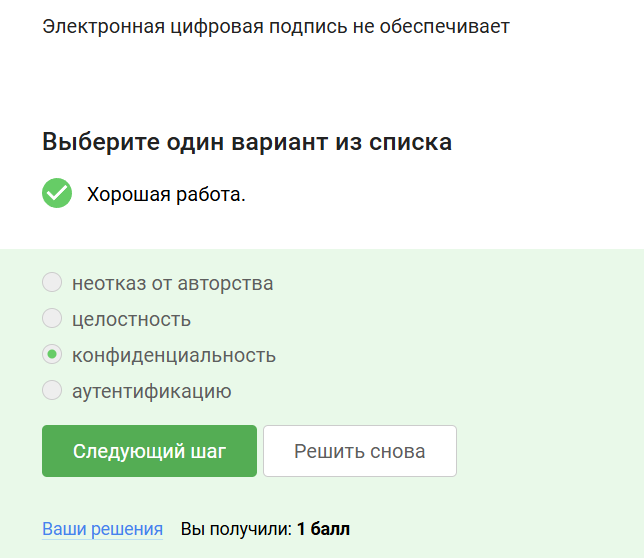


Рис. 8: Вопрос/Ответ 3

Пояснение ответа: Цифровая подпись предназначена для:

* Обеспечение целостности сообщения(любое изменение сообщения будет обнаружено)
* Аутентификации сообщения(устанавливается принадлежность подписи владельцу)
* Неотказ от авторства(невозможно отказаться от факта подписи в будущем)

Вопрос/Ответ 4 (рис. 9)

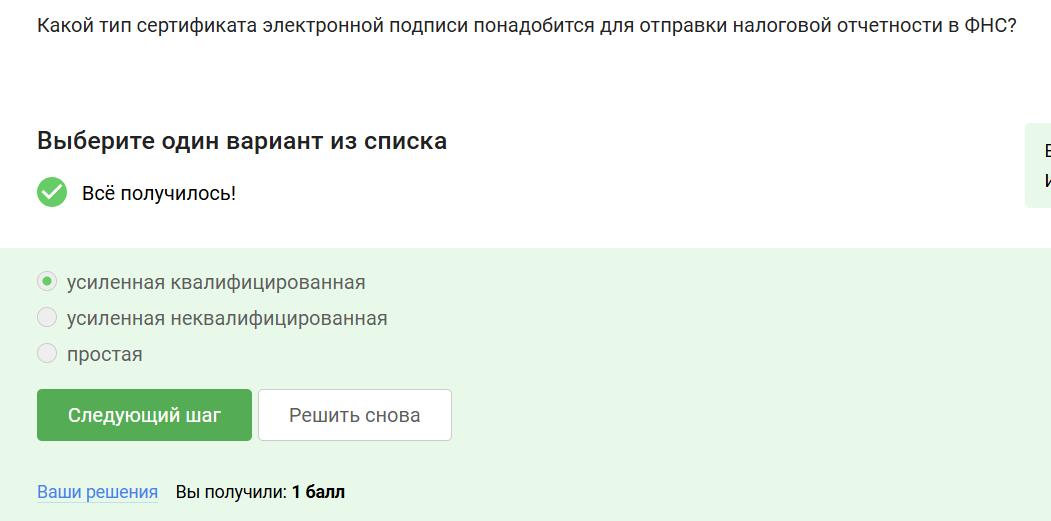


Рис. 9: Вопрос/Ответ 4

Пояснение ответа: Усиленной квалификацированной:

* равнозначно рукописей
* подтверждается сертификатом, выпущенным организацией, аккредитованной минкомсвязи РФ
* госуслуги, государственный документооборот

Вопрос/Ответ 5 (рис. 10)

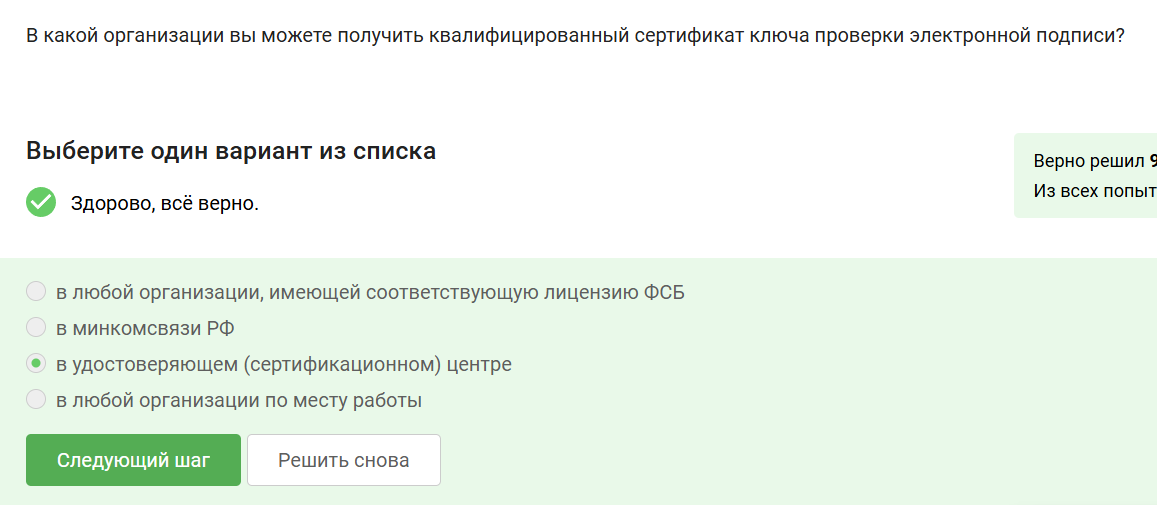


Рис. 10: Вопрос/Ответ 5

Пояснение ответа: В удостоверяющем(сертифиционном) центре можно получить квалифицированный сертификат ключа проверки электронной записи.

## 1.3 4.3 Электронные платежи

Вопрос/Ответ 1 (рис. 11)

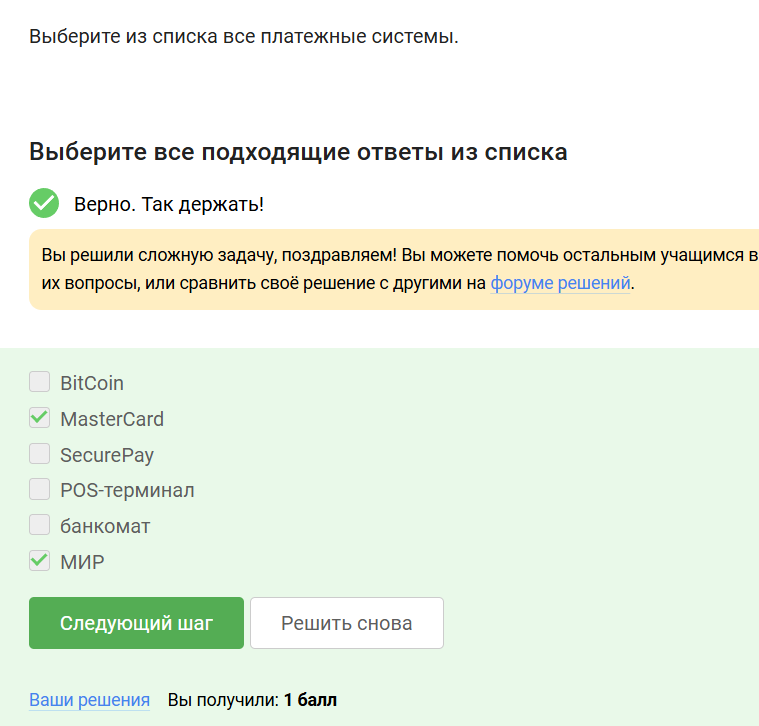


Рис. 11: Вопрос/Ответ 1

Пояснение ответа: МИР и MasterCard являются платежными системами.

Вопрос/Ответ 2 (рис. 12)

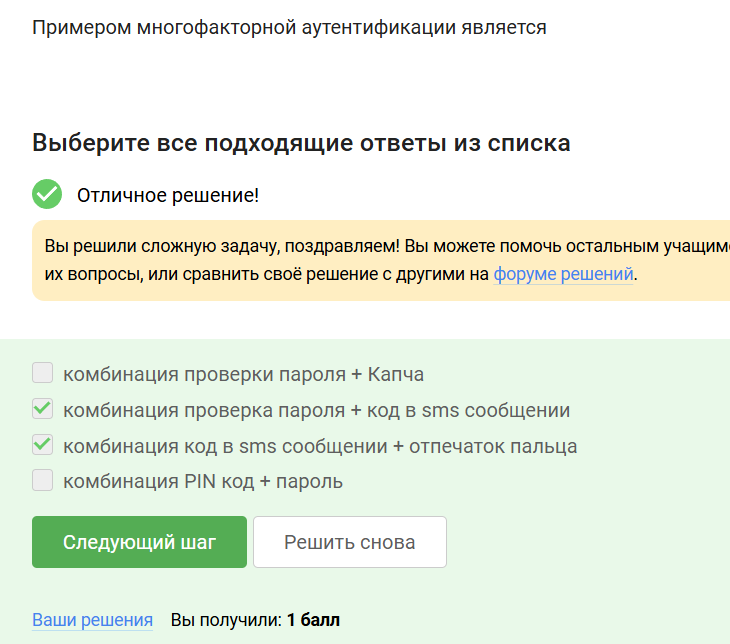


Рис. 12: Вопрос/Ответ 2

Пояснение ответа: Многократная аутентификация заключается в том, что мы доказываем в ходе этого протокола несколько вещей есть. Основные категории вещей, которые мы можем доказать:

1. то, что я знаю-это либо пароль,либо пин код, либо в случае онлайн платежей это секретный код
2. конкретно в онлайн платежах мы используем второй фактор-это то, чем я владею, который вы должны подтвердить или вбить в ваш браузер
3. другой фактор аутентификации-это свойства например биометрия,отпечаток пальца
4. четвертый фактор аутентификации -локация.

Вопрос/Ответ 3 (рис. 13)

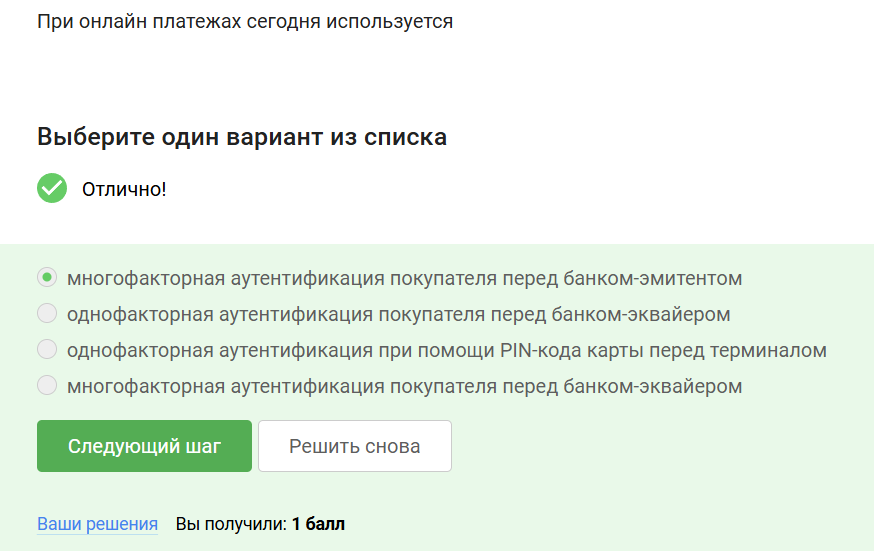


Рис. 13: Вопрос/Ответ 3

Пояснение ответа: При онлайн платежах сегодня используется многофакторная аутентификация покупателя перед банком-эмитентом

## 1.4 4.4 Блокчейн

Вопрос/Ответ 1 (рис. 14)

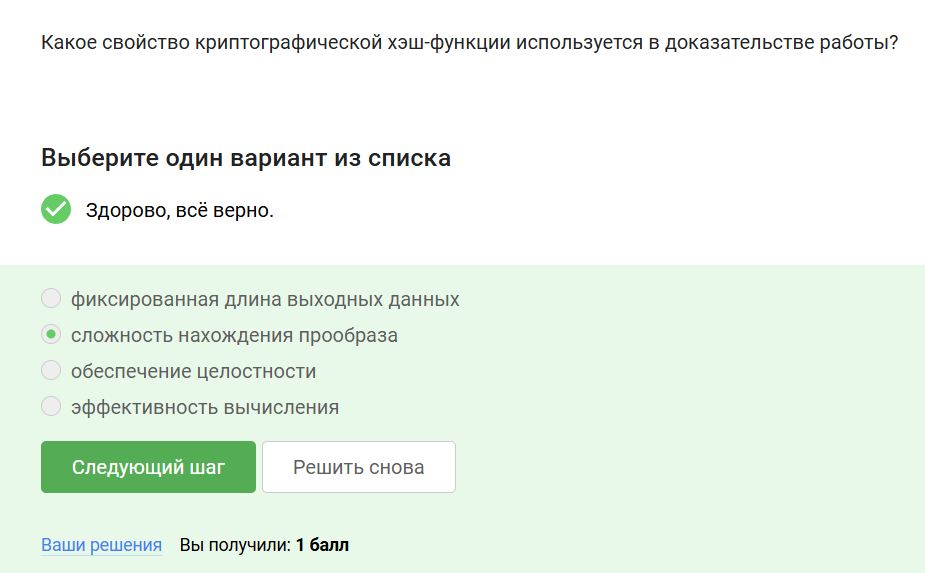


Рис. 14: Вопрос/Ответ 1

Пояснение ответа: Сложность нахождения прообраза криптографической хэш функции используется в доказательстве работы.

Вопрос/Ответ 2 (рис. 15)

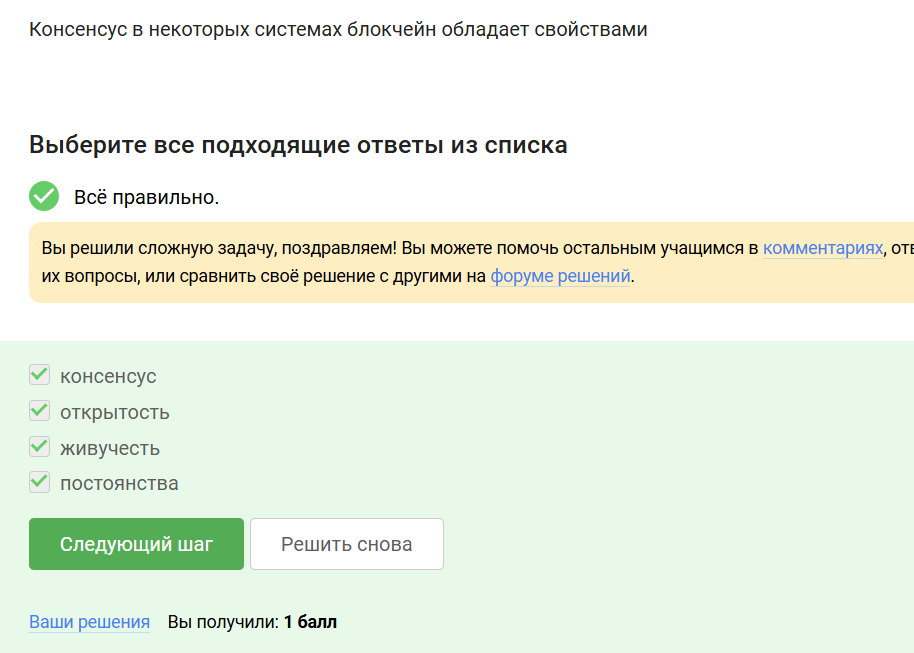


Рис. 15: Вопрос/Ответ 2

Пояснение ответа: В основе блокчейна лежит консенсус- публичная структура данных или леджер(бухгалтерская книга), которая обеспечивает:

* постоянство(добавленные когда-либо данные не могут быть удалены)
* консенсус(все участники видят одни и те же данные за исключением пары блоков)
* живучесть(участники могут добавлять новые транзакции)
* открытость(любой может стать участником блокчейна)

Вопрос/Ответ 3 (рис. 16)

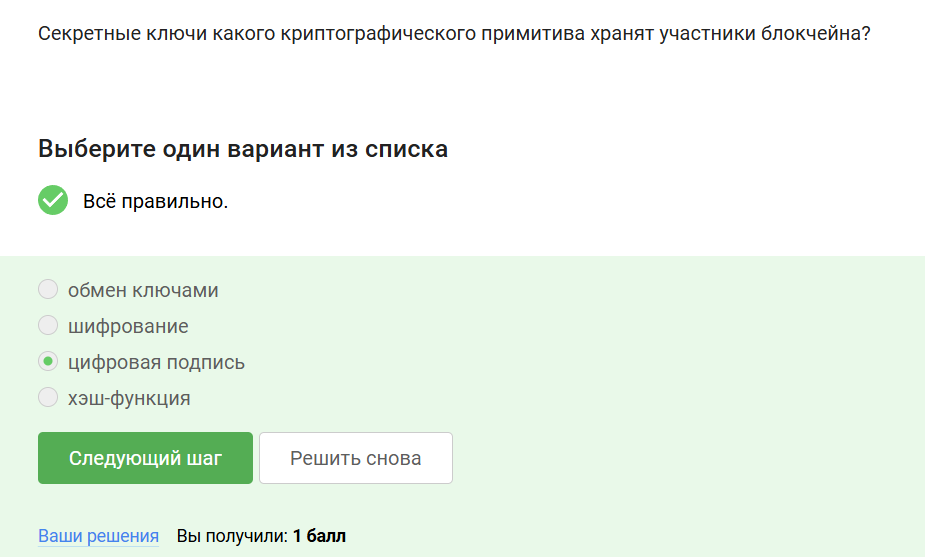


Рис. 16: Вопрос/Ответ 3

Пояснение ответа: Участники блокчейна хранят секретные ключи цифровой подписи каждой транзакции, эта подпись доказывает, что транзакция создана владельцем средств. Только владелец приватного ключа может распорядиться средствами, хранящимися на связанном адресе.