Внешний курс раздел 3

Криптография на практике

Александр Андреевич Шуплецов

Содержание

# 1 Цель работы

Изучить основы криптографии.

# 2 Выполнение работы

1. В асимметричных криптографических примитивах обе стороны имеют пару ключей - публичный и секретный.

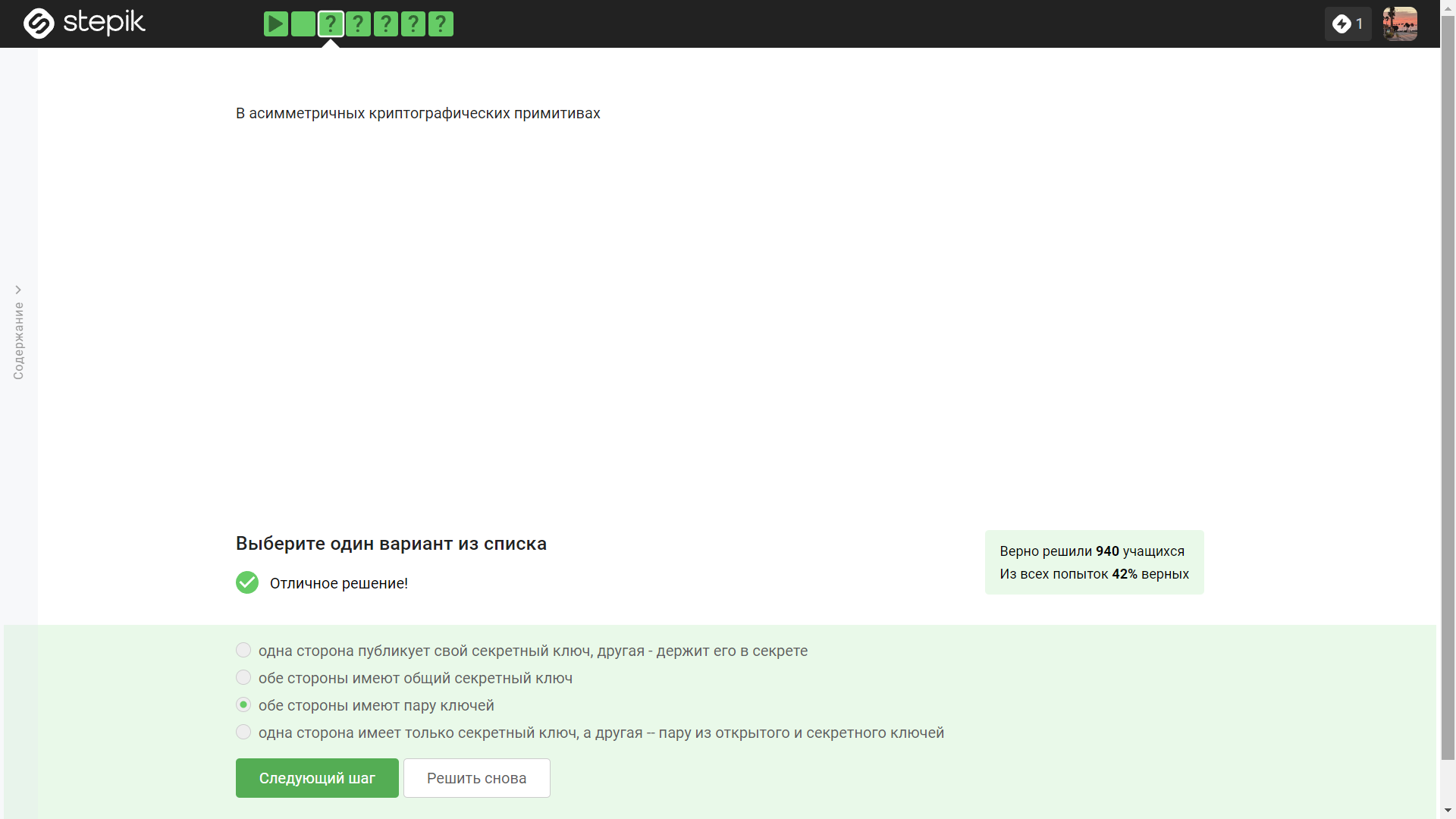


Figure 1: первое задание

1. Криптографическая хэш-функция, в отличие от обычной хэш-функции, не обеспечивает конфиденциальность захэшированных данных, но она стойкая к коллизиям, эффективно вычисляется, дает на выходе фиксированное число бит независимо от объема входных данных.

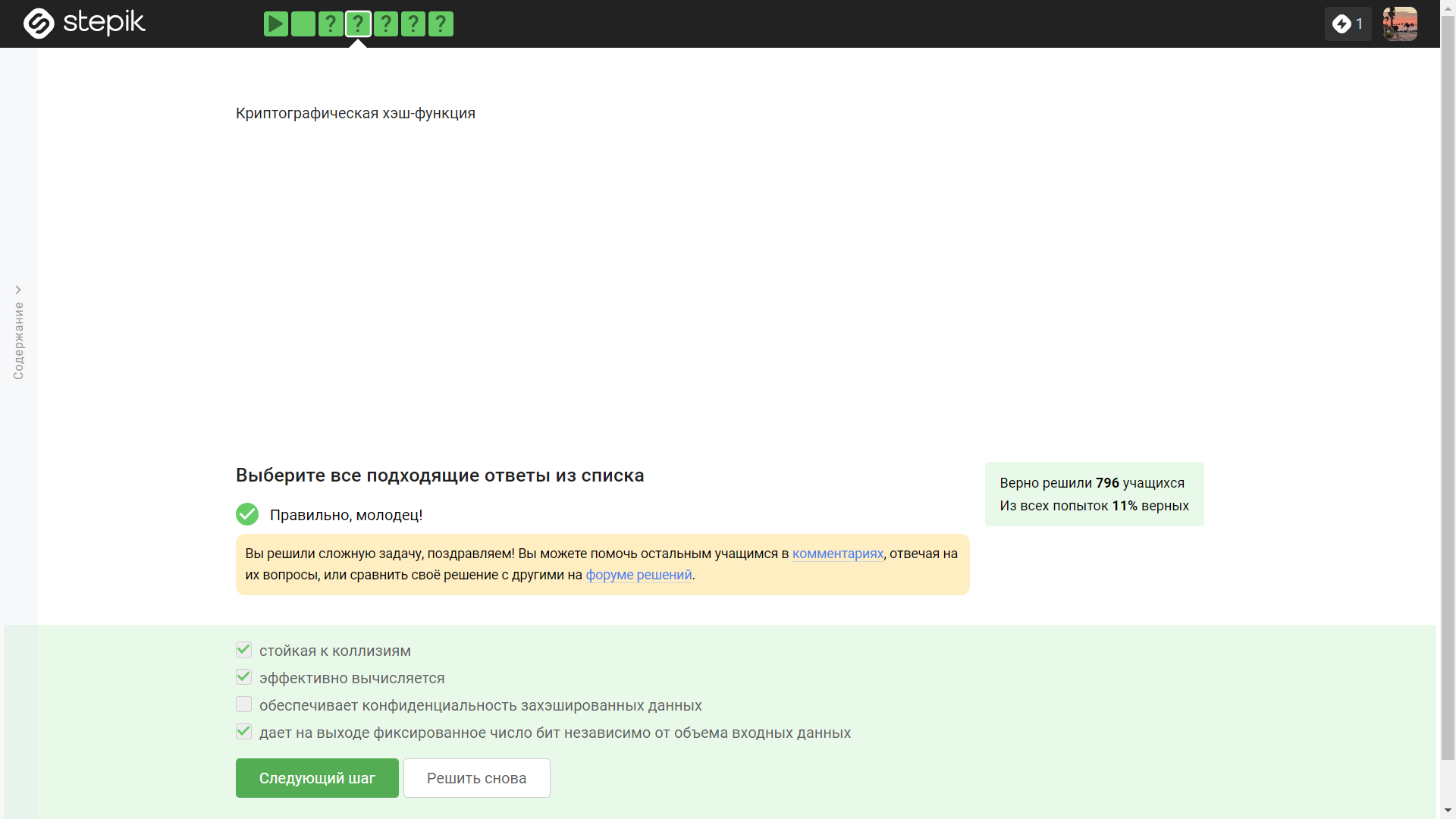


Figure 2: второе задание

1. К алгоритмам цифровой подписи относятся зарубежные RSA и ECDSA, российский ГОСТ Р 34.10-2012.

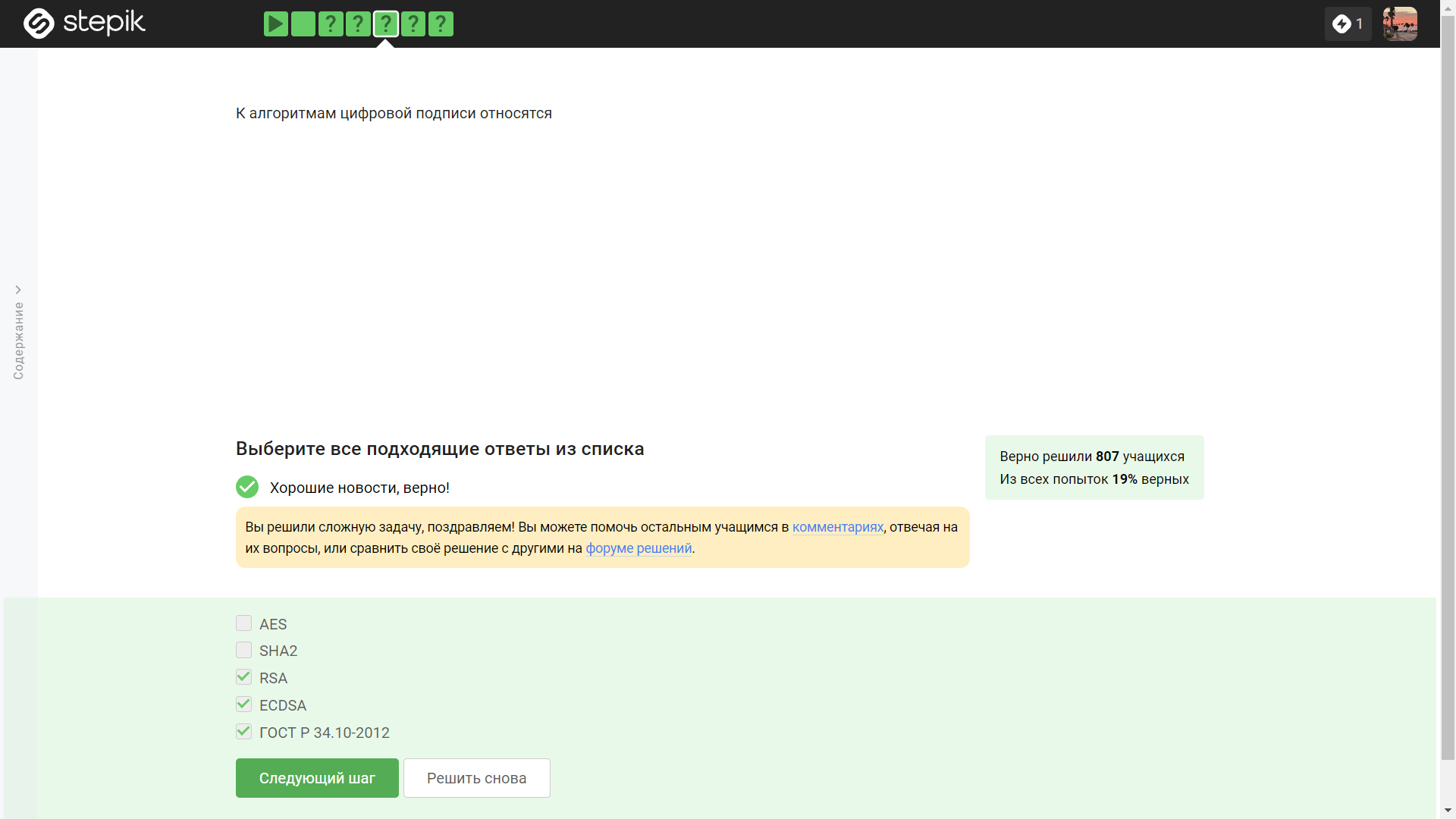


Figure 3: третье задание

1. Код аутентификации сообщения относится к симметричным примитивам.

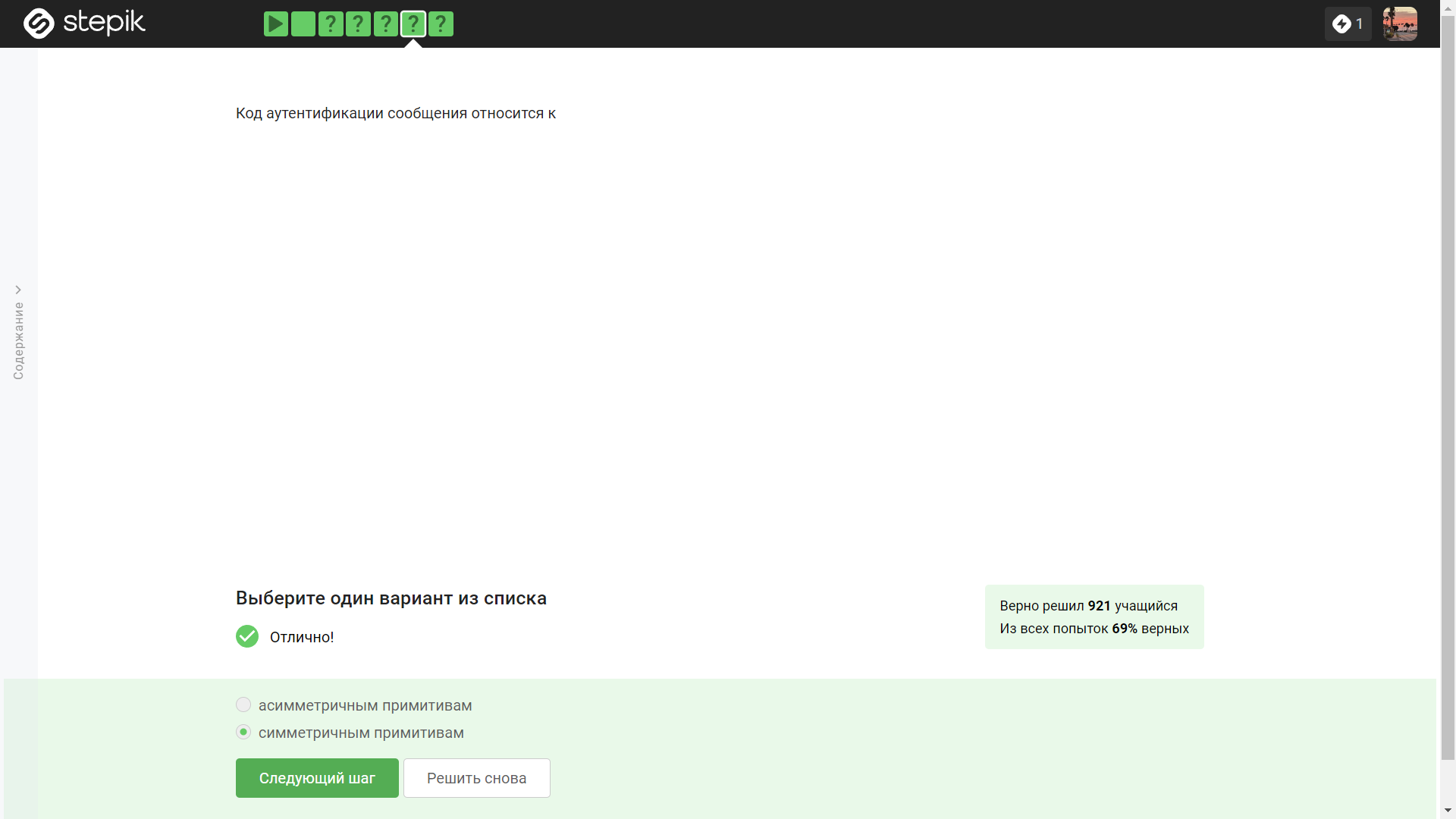


Figure 4: четвертое задание

1. Обмен ключами Диффи-Хэллмана - это асимметричный примитив генерации общего секретного ключа.

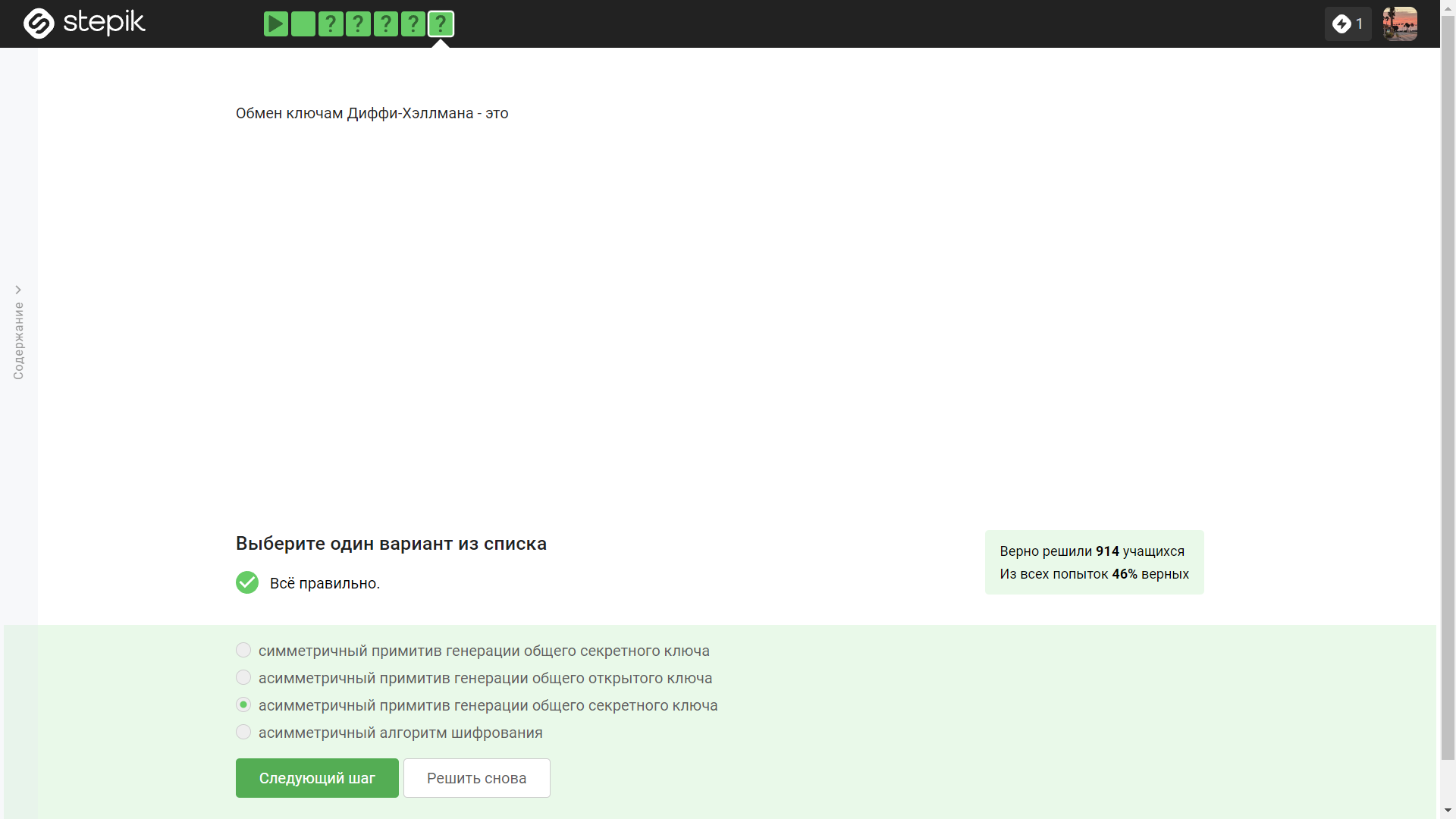


Figure 5: пятое задание

1. Протокол электронной цифровой подписи относится к протоколам с публичным ключом.

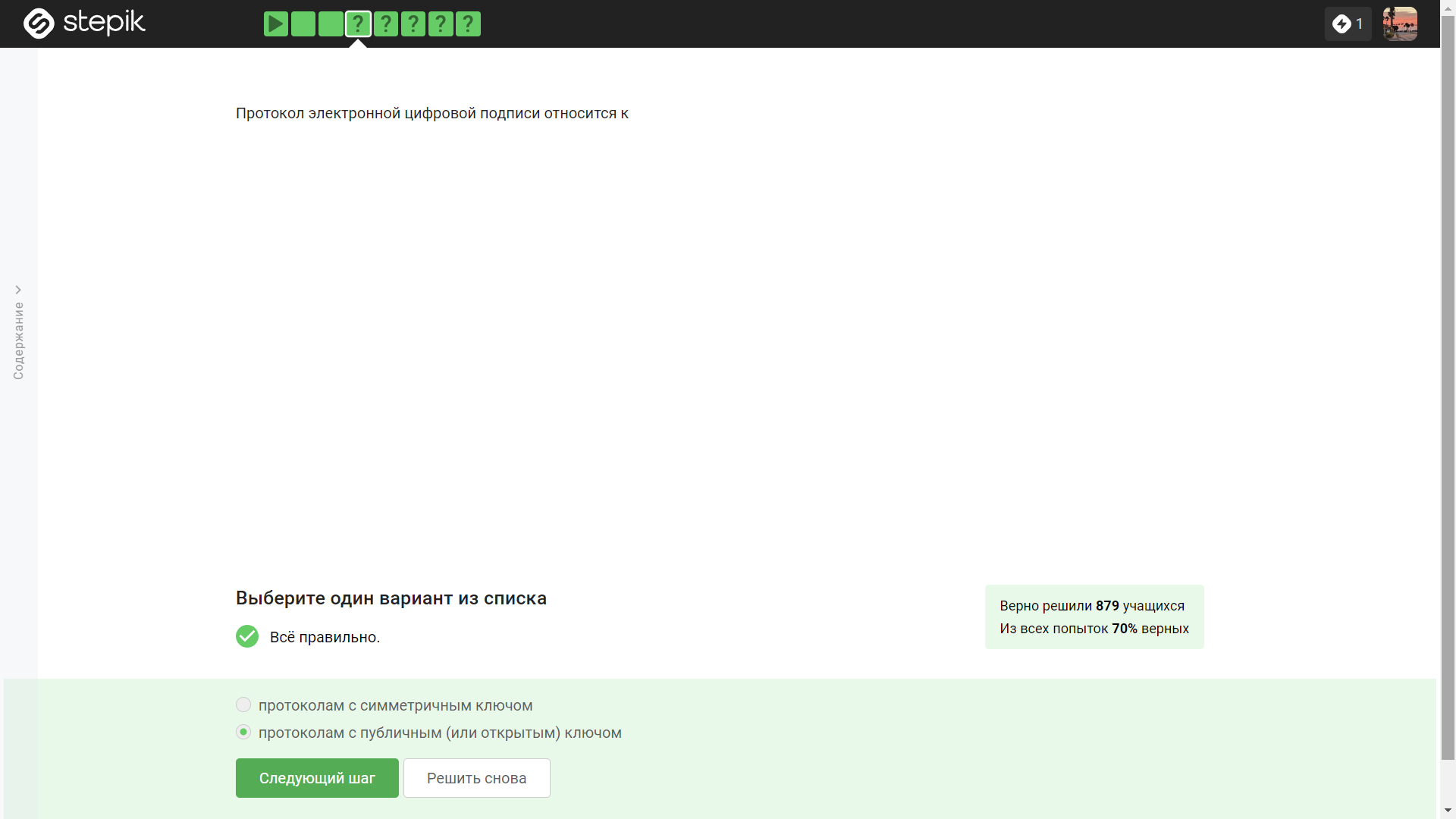


Figure 6: шестое задание

1. Алгоритм верификации электронной цифровой подписи требует на вход подпись, открытый ключ, сообщение.

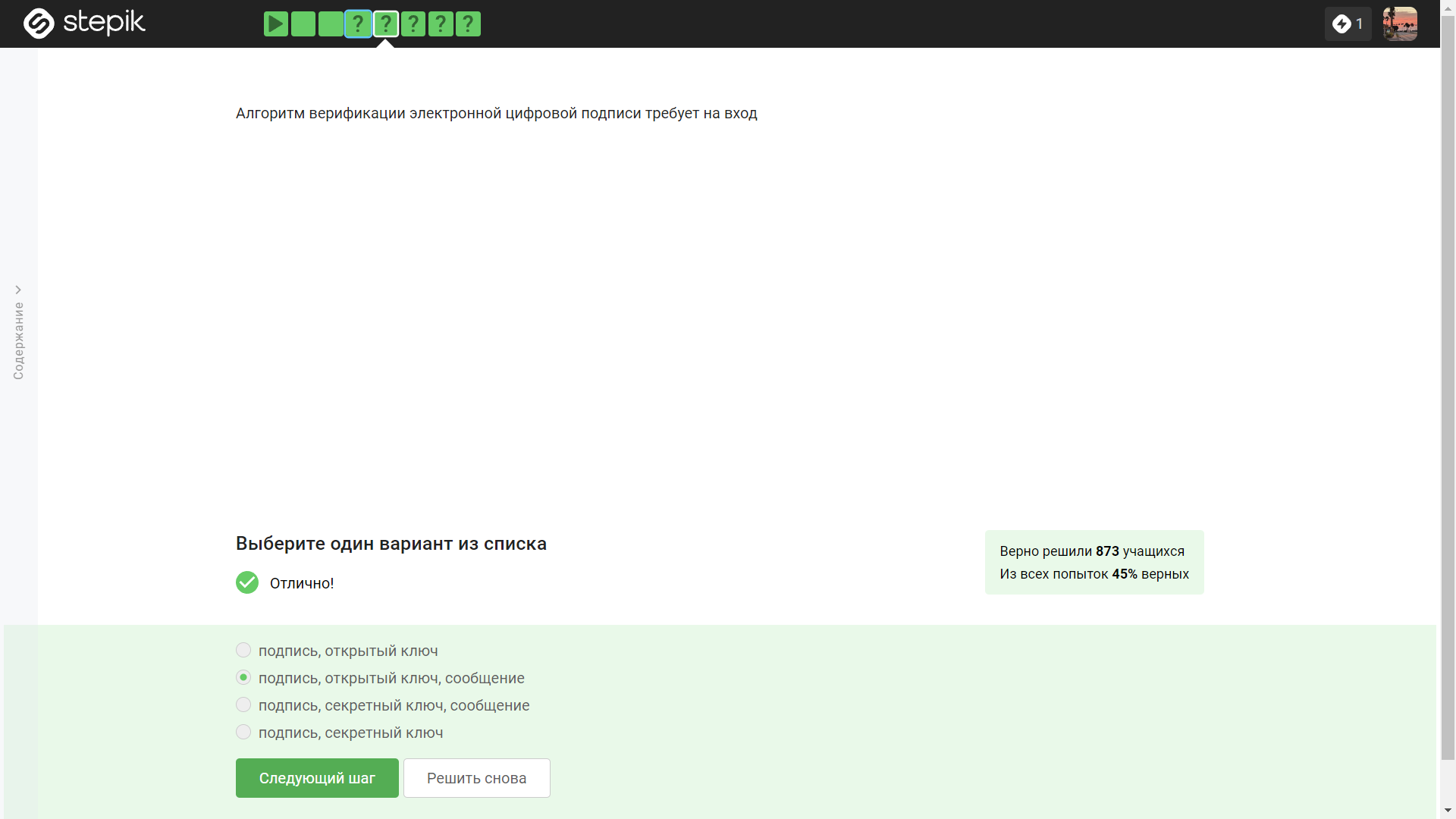


Figure 7: седьмое задание

1. Электронная цифровая подпись не обеспечивает конфиденциальность.

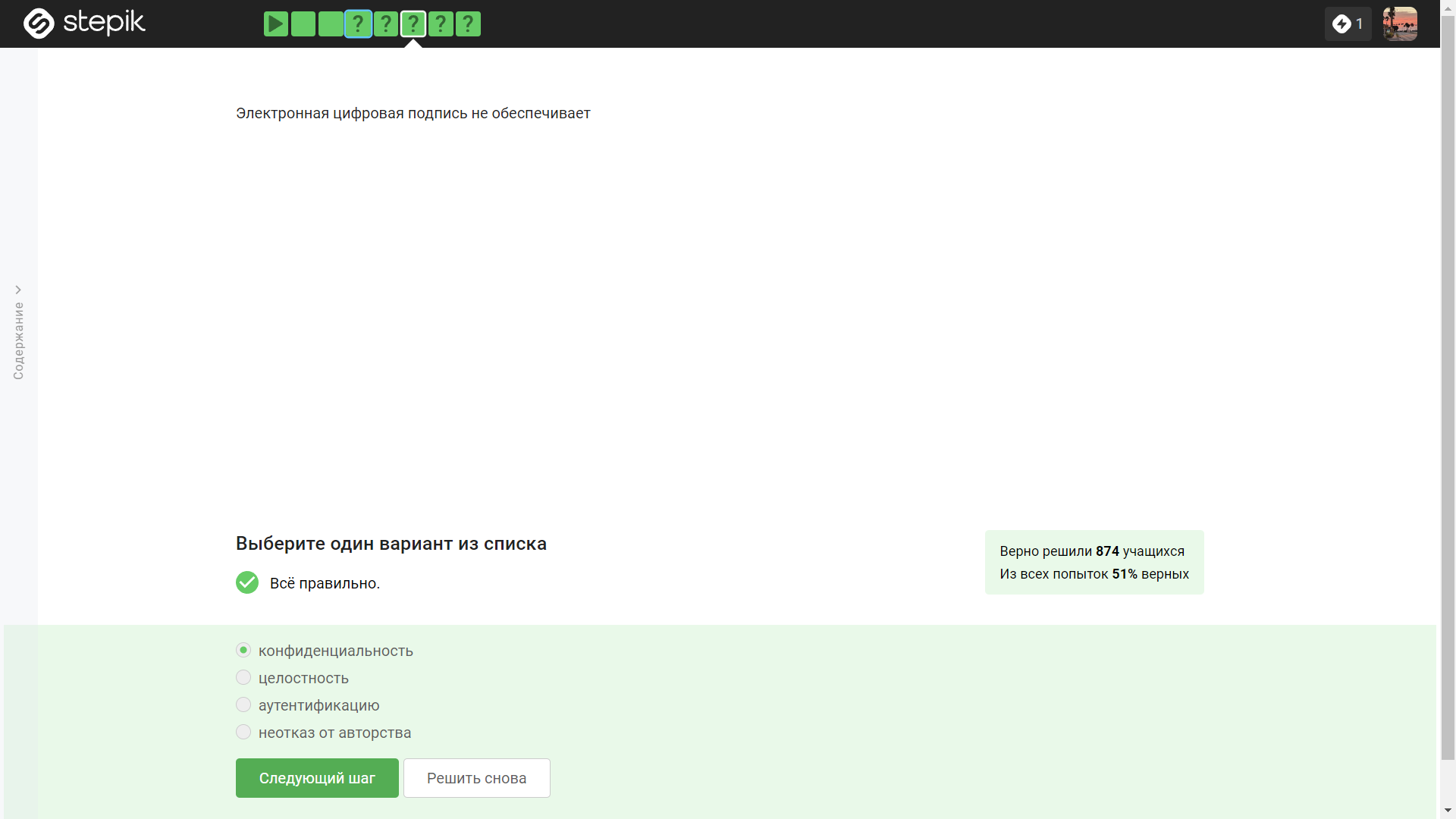


Figure 8: восьмое задание

1. Для отправки налоговой отчетности в ФНС понадобится самый сильный тип сертификата электронной подписи - усиленная квалификационная.

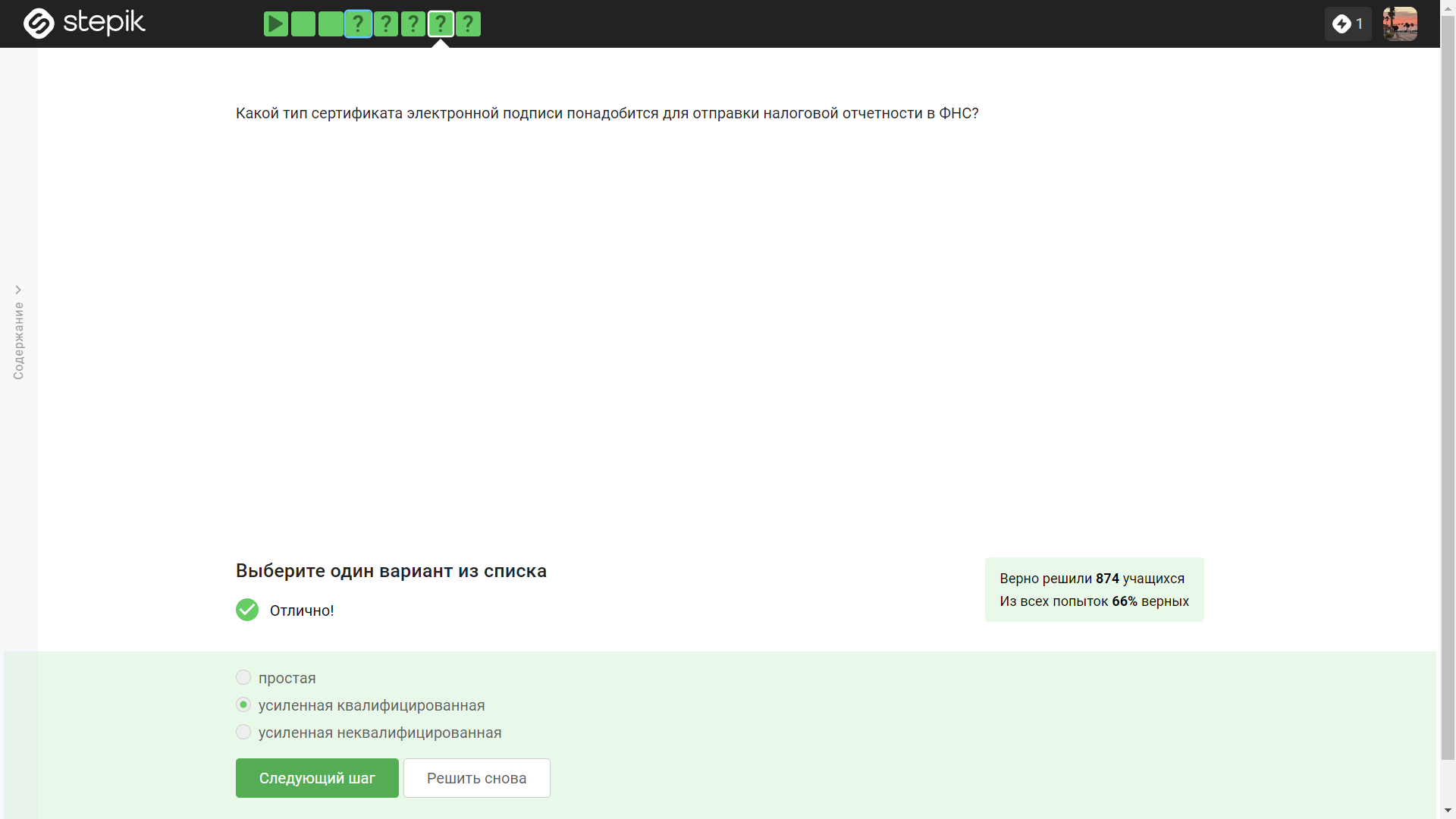


Figure 9: девятое задание

1. Квалифицированный сертификат ключа проверки электронной подписи можно получить в удостоверяющем (сертификационном) центре.

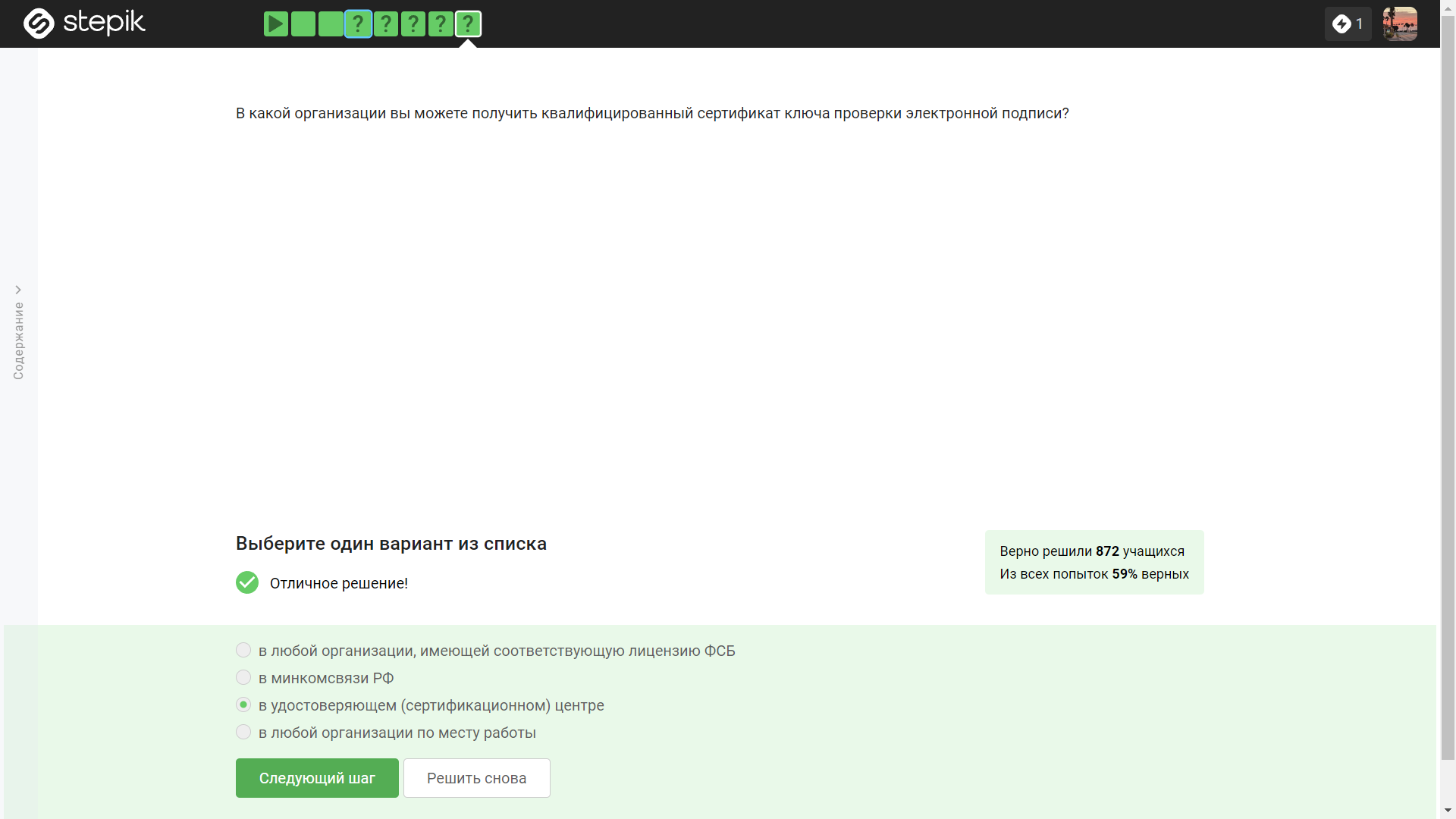


Figure 10: десятое задание

1. MasterCard и МИР являются платежными системами в предоставленном в задании списке.

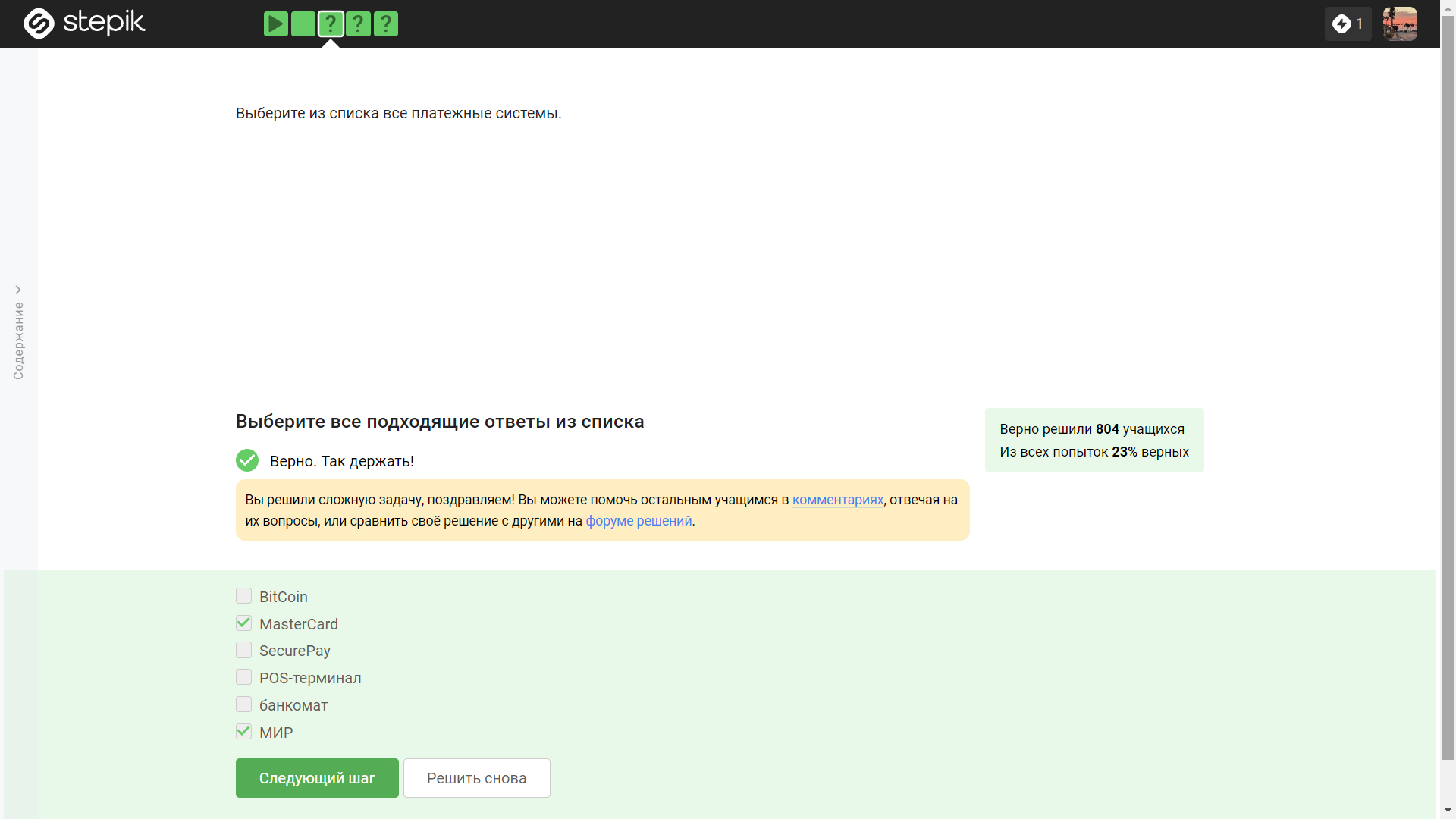


Figure 11: одиннадцатое задание

1. Примерами многофакторной аутентификации являются комбинация проверка пароля + код в sms сообщении, комбинация код в sms сообщении + отпечаток пальца, капча с паролем и пароль с пин кодом не являются примерами многофакторной аутентификации.

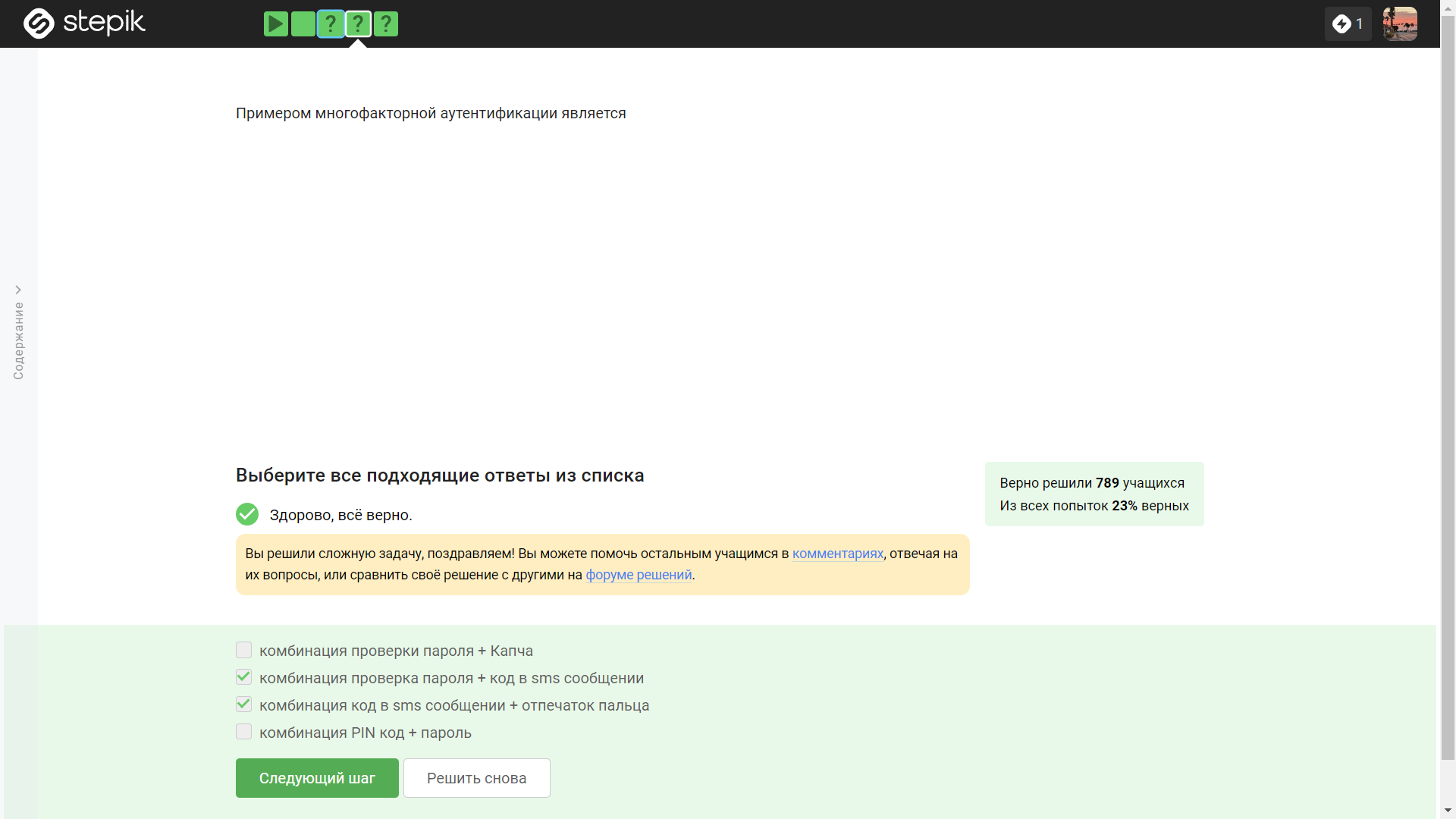


Figure 12: двенадцатое задание

1. При онлайн платежах сегодня используется многофакторная аутентификация покупателя перед банком-эмитентом - банком, на счете которого покупатель хранит денежные средства.

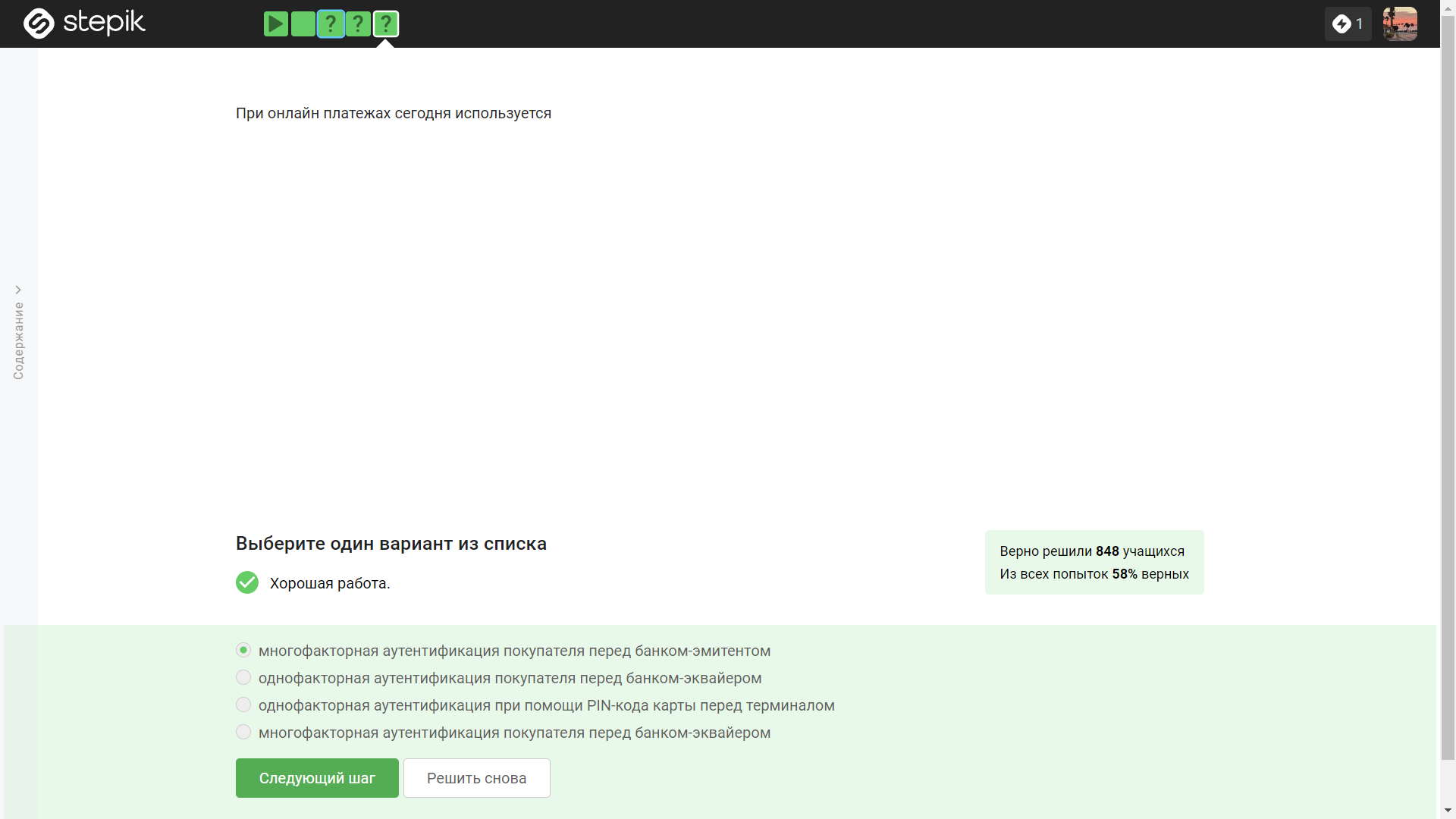


Figure 13: тринадцатое задание

1. Сложность нахождения прообраза как свойство криптографической хэш-функции используется в доказательстве работы майнера.

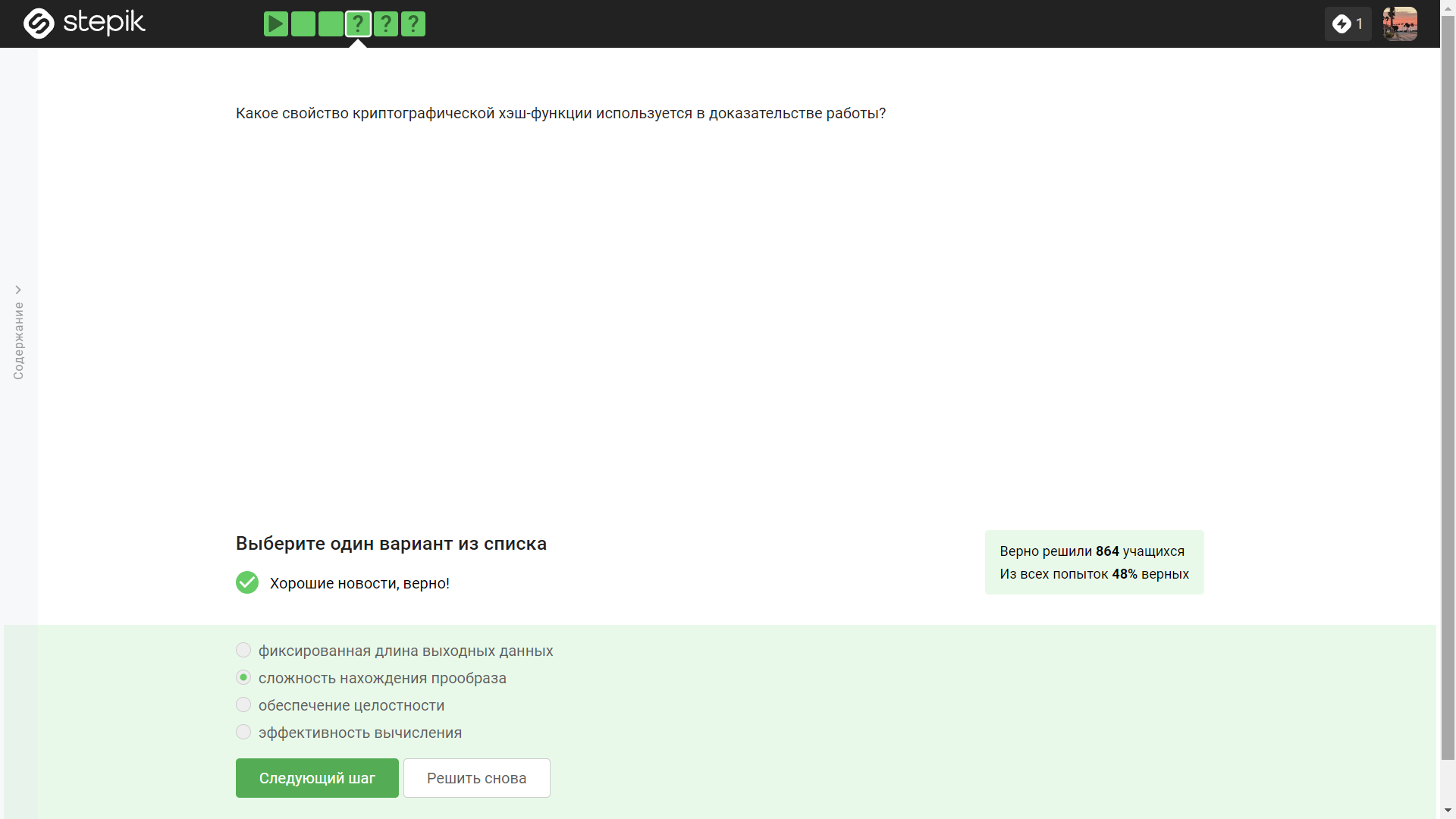


Figure 14: четырнадцатое задание

1. Консенсус в некоторых системах блокчейн обладает свойствами: открытость, живучесть, постоянство.

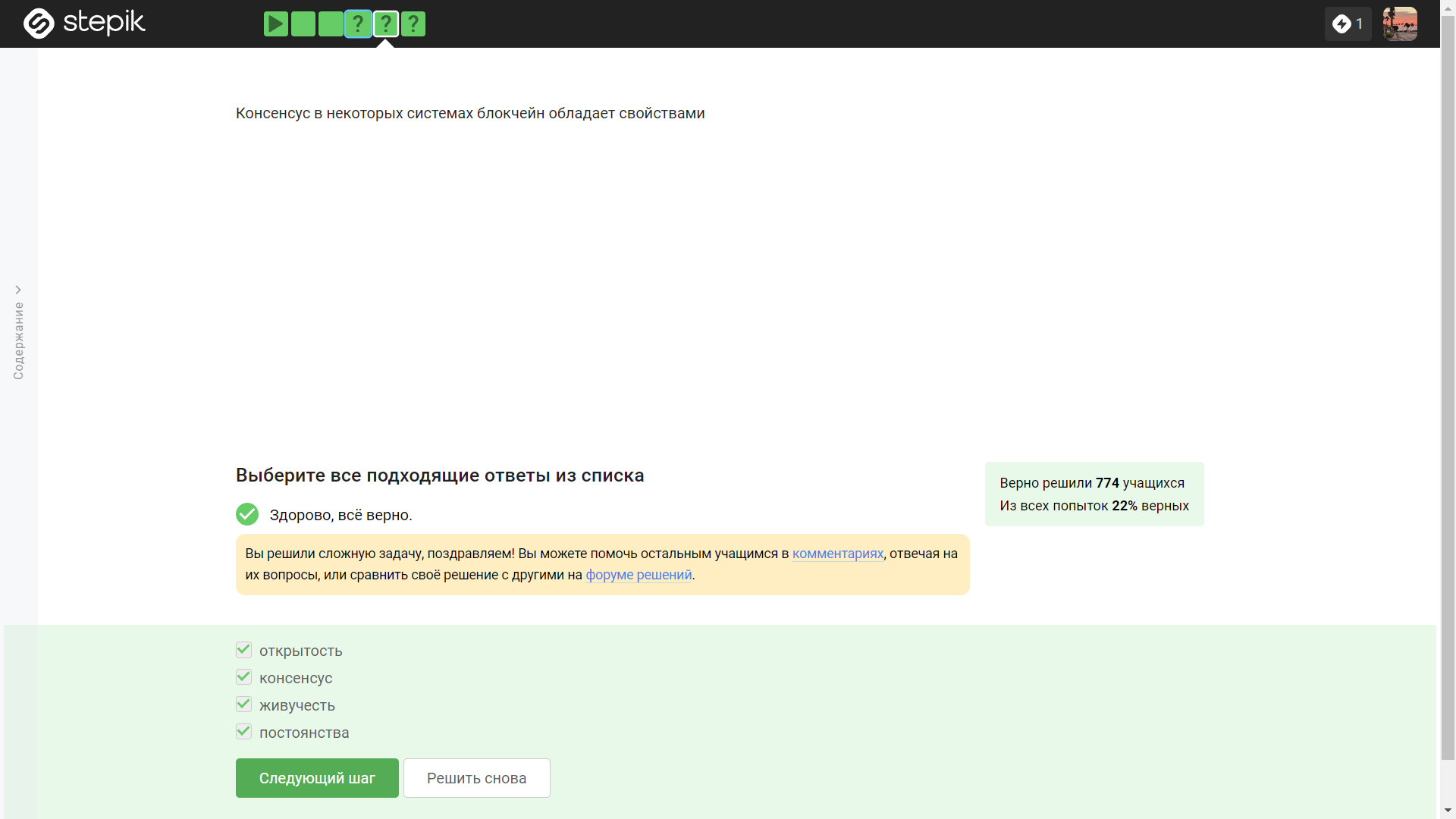


Figure 15: пятнадцатое задание

1. Цифровая подпись используется в качестве криптографического примитива в блокчейне.

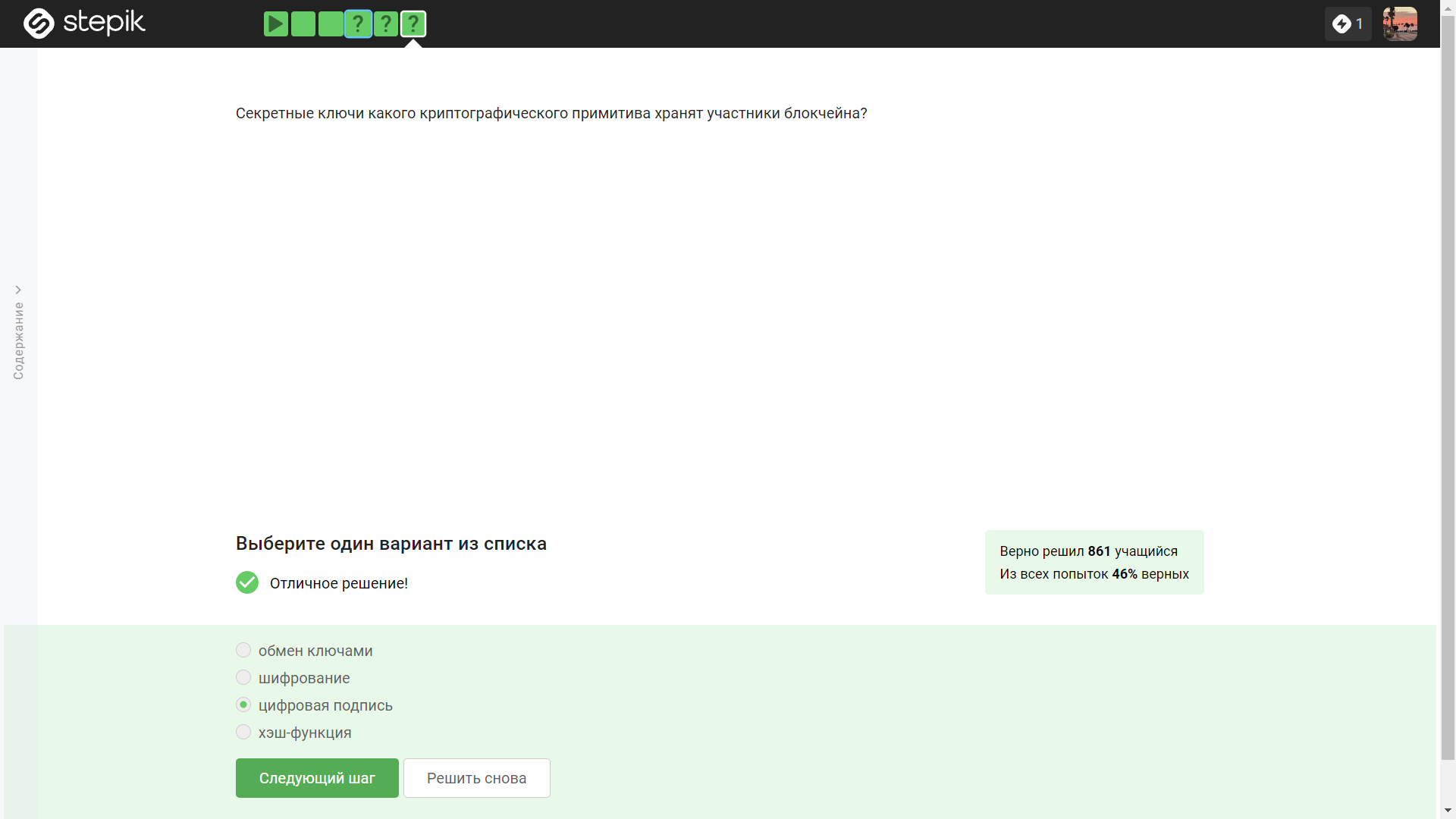


Figure 16: шестнадцатое задание

# 3 Выводы

Я изучил основы криптографии.

# 4 Список литературы

Конспекты к лекциям курса “Основы кибербезопасности”.