Отчет по третьему этапу внешнего курса

Дисциплина: основы информационнной безопасности

Казазаев Даниил Михайлович

Содержание

Список иллюстраций

1 Цель работы

Внешний кур состоит из трех этапов.

2 Этап первый

Первый этап курса состоит из 4 частей:

1. Введине в криптографию
2. Цифровая подпись
3. Электронные платежи
4. Блокчейн

3 Выполнение первого этапа внешнего курса.

3.1 Введине в криптографиюВведине в криптографию

В ассиметричных криптографических примитивах обестороны имеют пару ключей. (рис. 3.1)

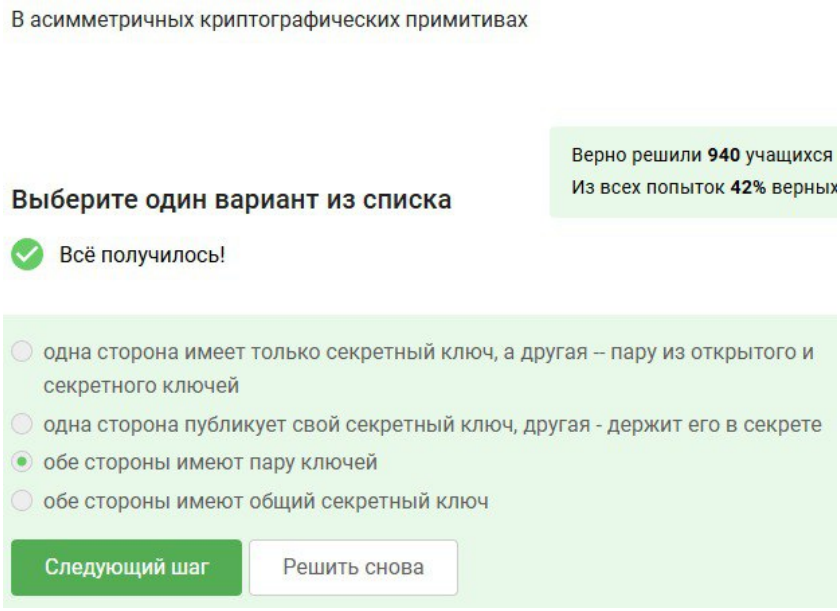

Рис. 3.1: Первый вопрос

Хещ-функция стойкая к колизиям, дает определенное кол-во бит вне зависимости от объема входных данных и эффективно вычисляется. (рис. 3.2)

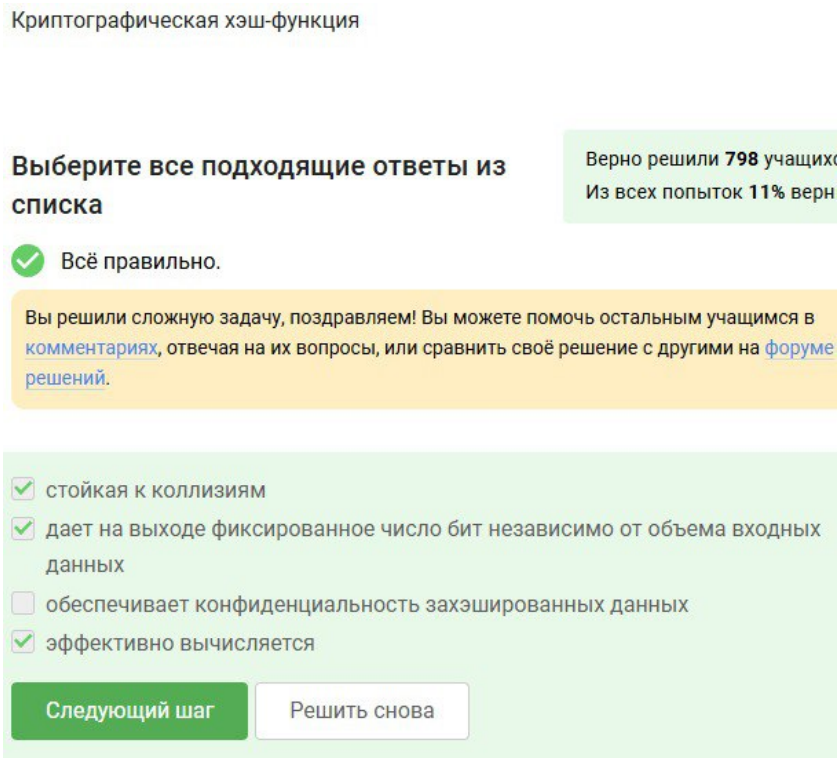

Рис. 3.2: Второй вопрос

RSA, ECDSA и ГОСТ стандарт(кузнечик) - алгоритмы цифровой подписи. (рис. 3.3)

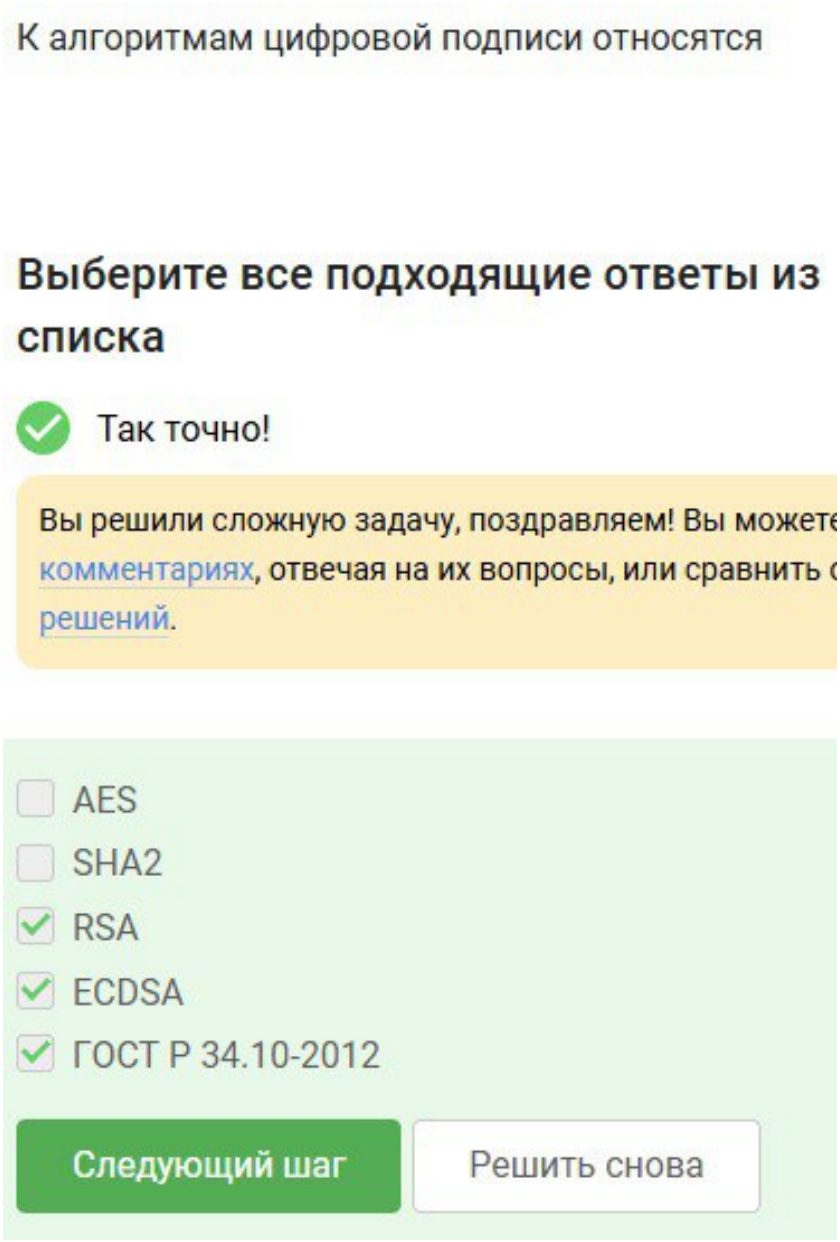

Рис. 3.3: Третий вопрос

Код аунтификации сообщения отеосится к симмитричным примитивам. (рис. 3.4)

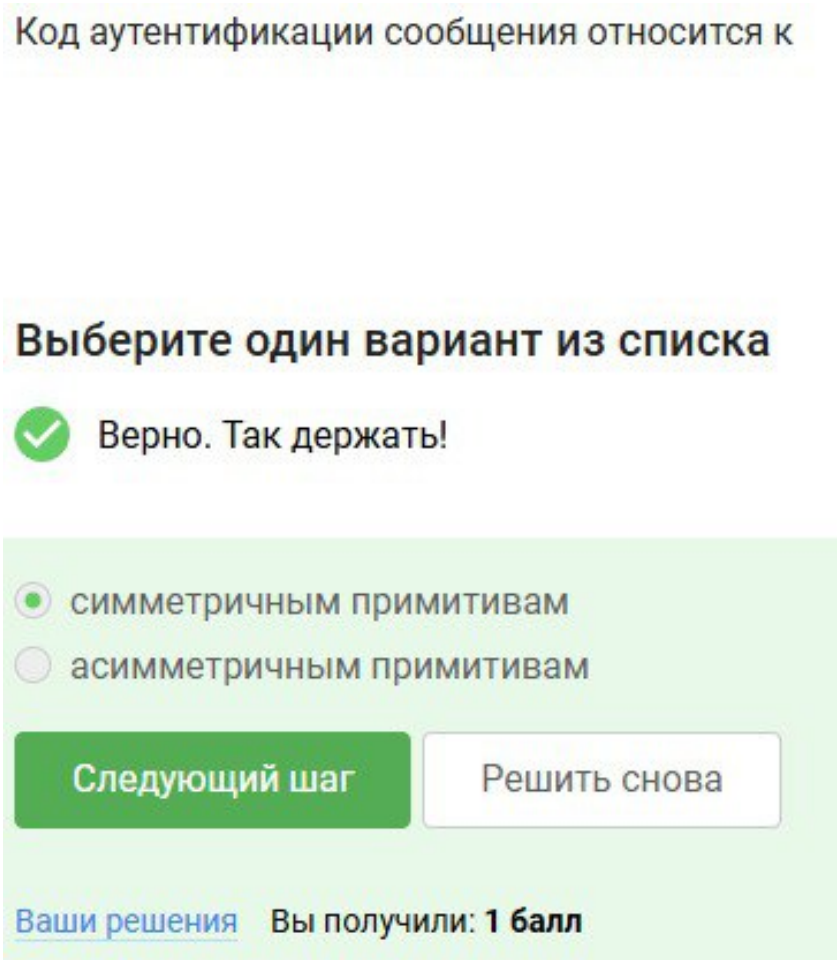

Рис. 3.4: Четвертый вопрос

Обмен ключами Диффи-Хэллмана - ассиметрический примитив генерации обзего секретного ключа. (рис. 3.5)

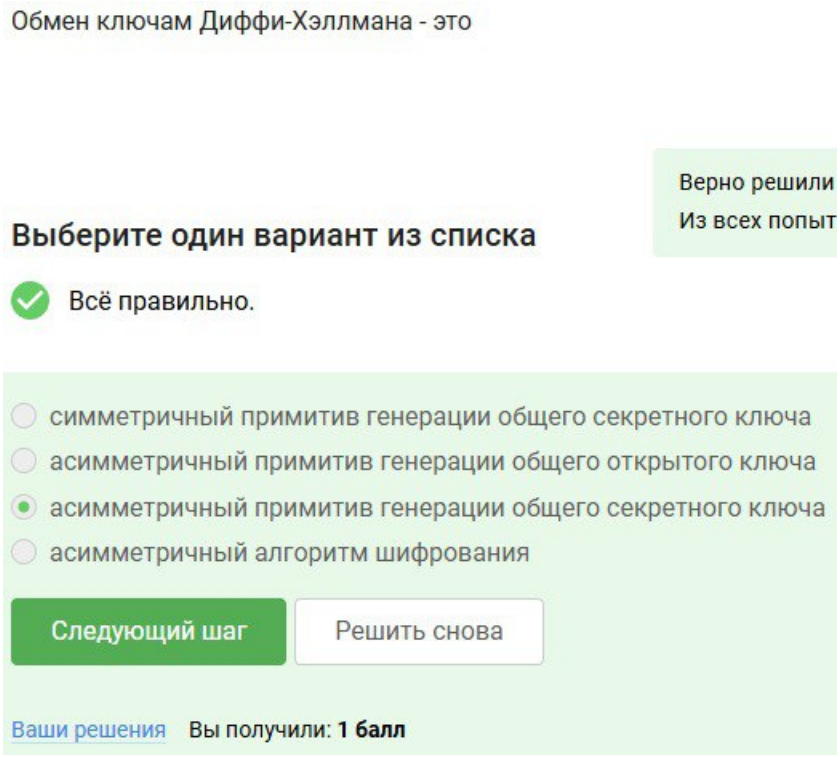

Рис. 3.5: Пятый вопрос

4 Цифровая подпись

Протоколы цифровой подписи с публичным ключом.(рис. 4.1)

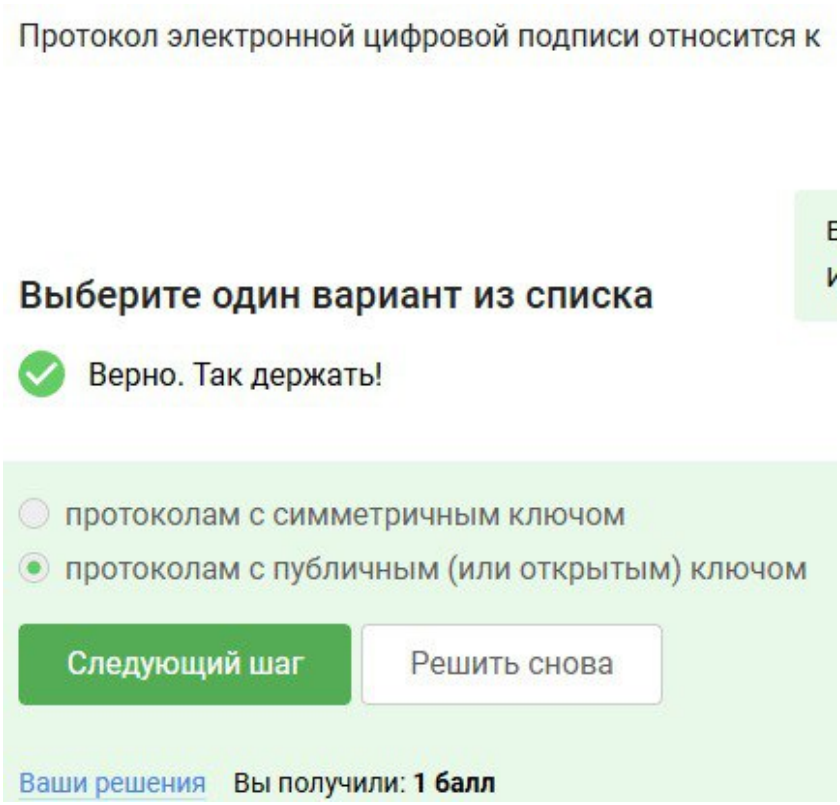

Рис. 4.1: Первый вопрос

Алгоритм верификации требует на вход: подпись, открытый ключ, сообщение.(рис. 4.2)

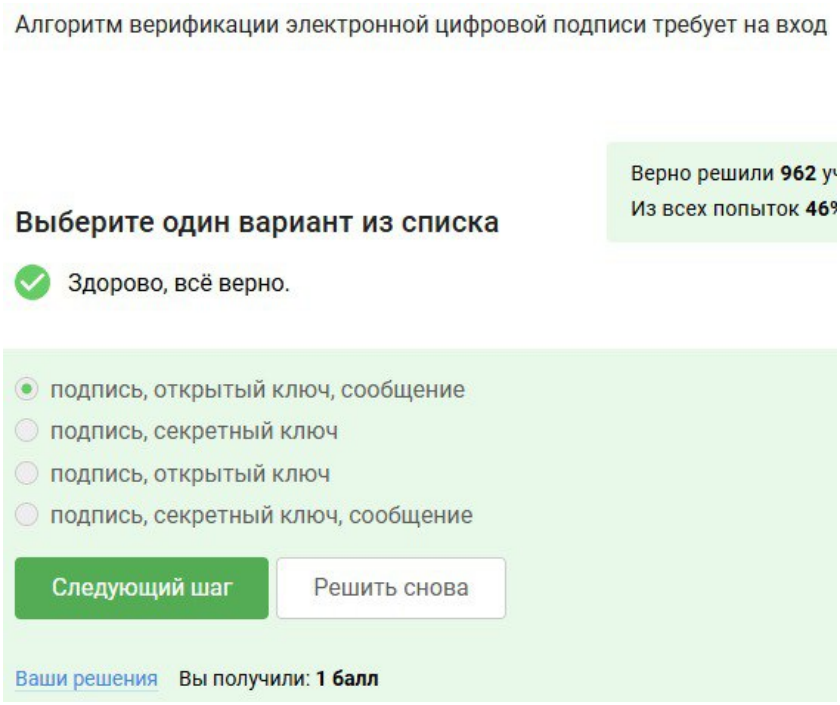

Рис. 4.2: Второй вопрос

Электронная подпись не обеспечивает конфиденциальность.(рис. 4.3)

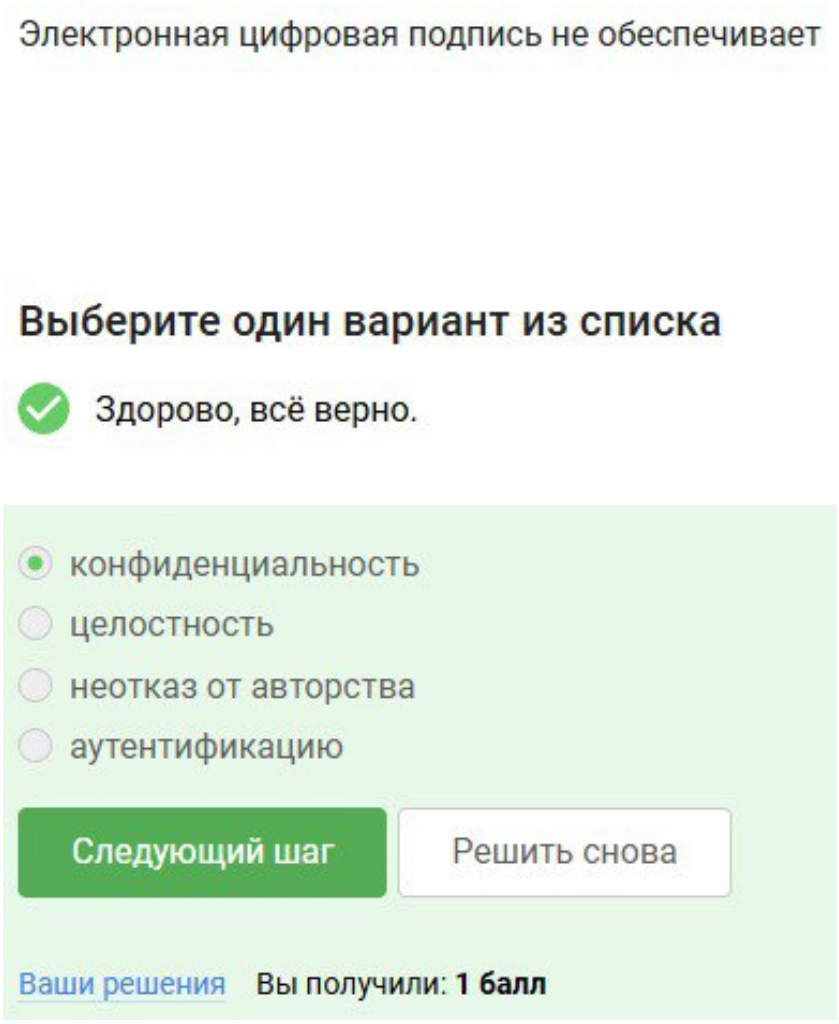

Рис. 4.3: Третий вопрос

Для отправки налоговой отчетности необходим сертификат с усиленной квалификацией.(рис. 4.4)

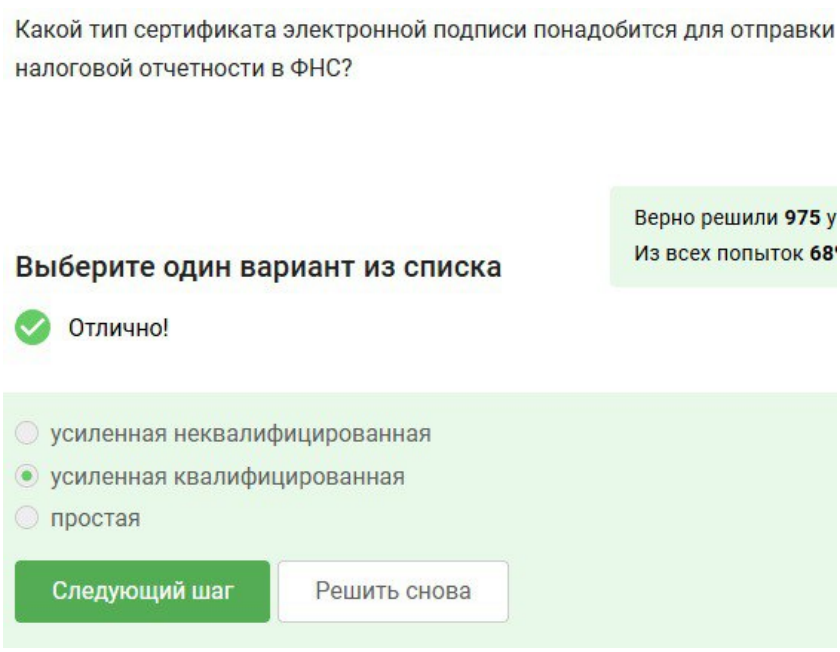

Рис. 4.4: Четвертый вопрос

Квалифицированный сертификат можно получить в удостоверяющем центре.(рис. 4.5)

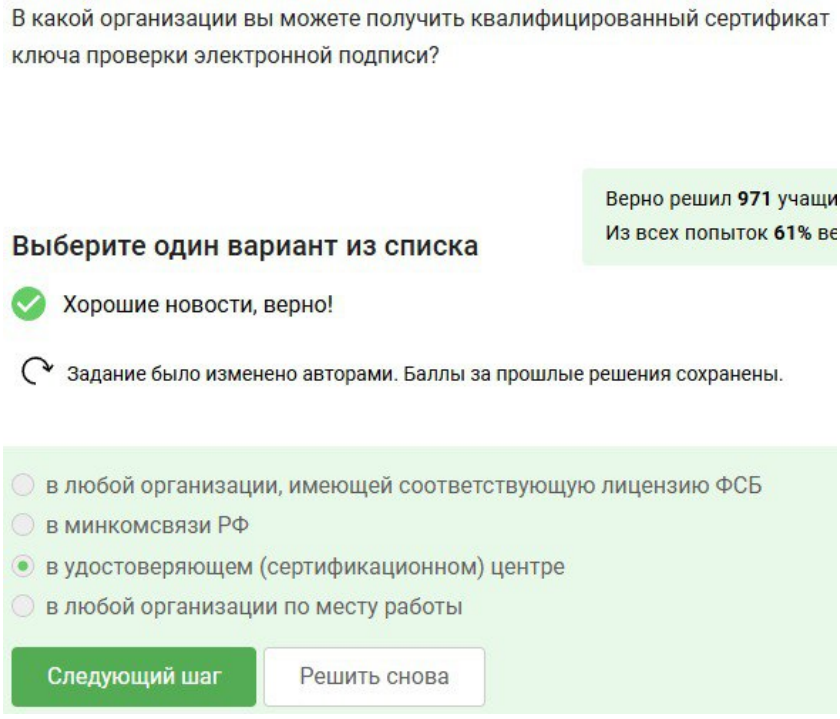

Рис. 4.5: Пятый вопрос

5 Электронные платежи

МИР, MasterCard - платежные системы. (рис. 5.1)

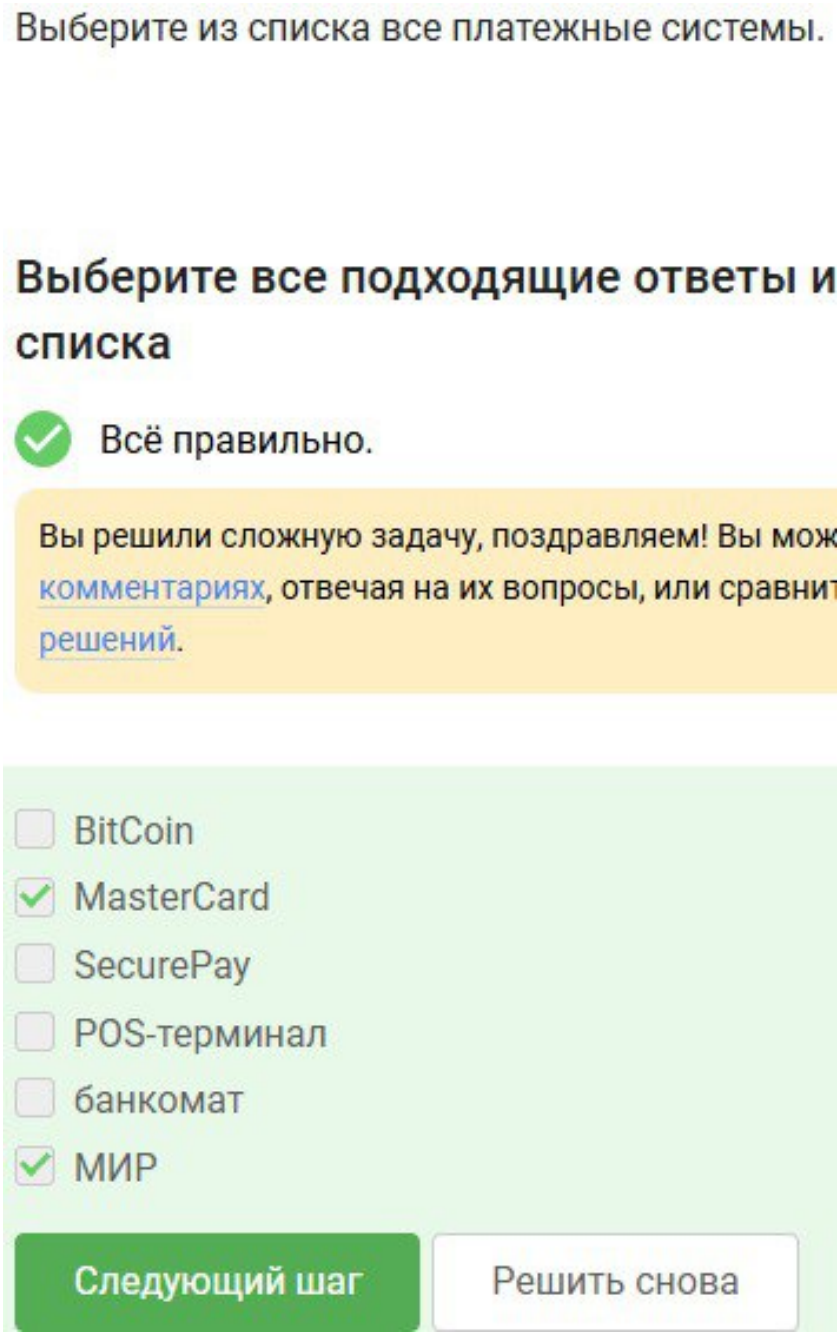

Рис. 5.1: Первый вопрос

Отмеченные варианты ответов являются примером многофакторной аутентификации. (рис. 5.2)

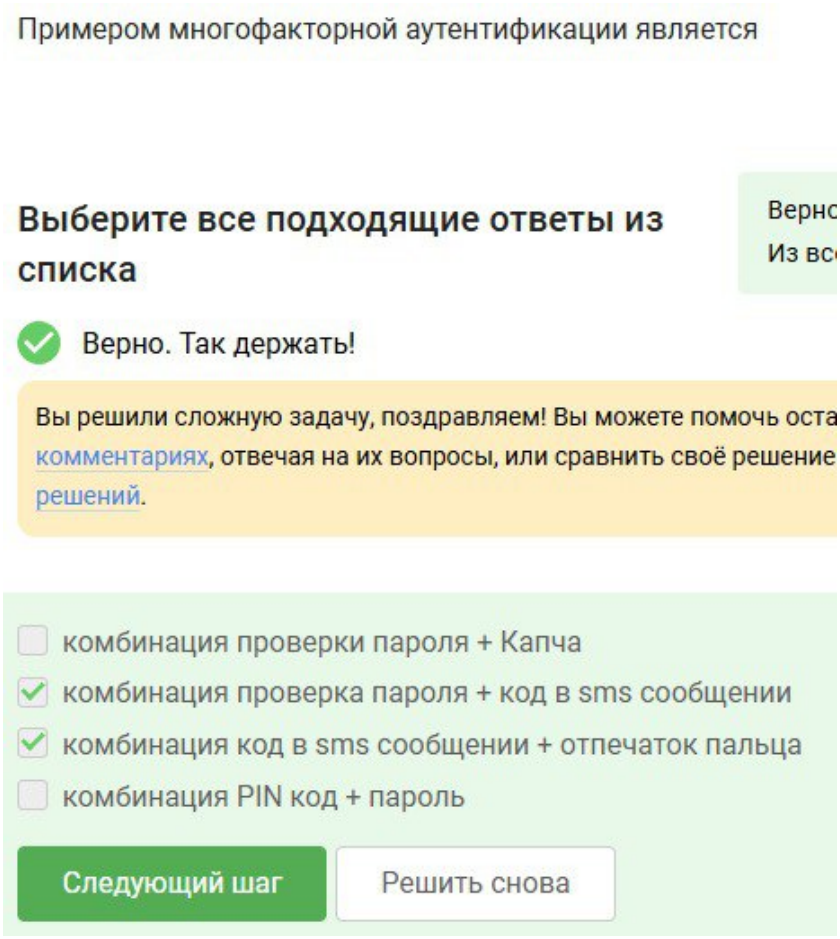

Рис. 5.2: Второй вопрос

Сегодня при онлайн платежах используется многофакторная аутентификация покупателя перед банком-эмитентом. (рис. 5.3)

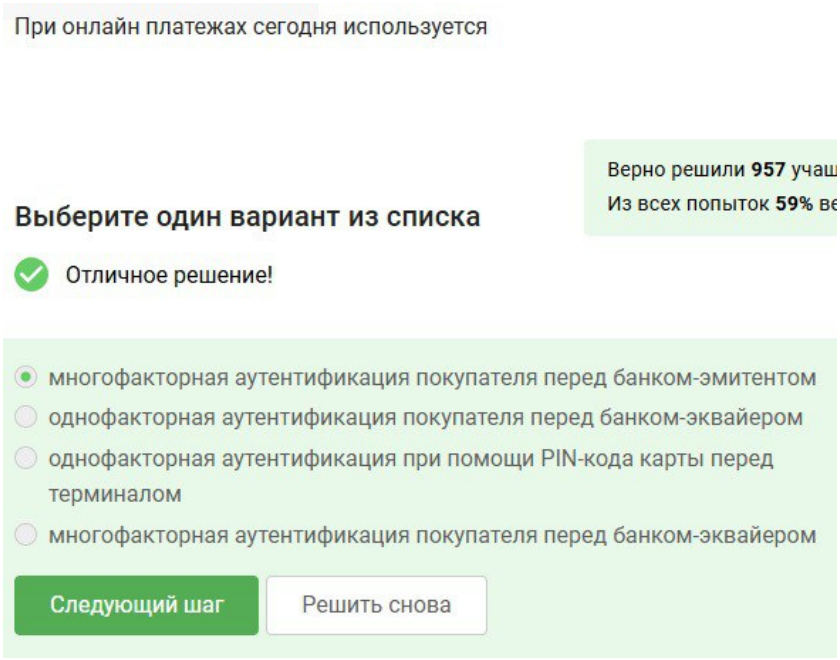

Рис. 5.3: Третий вопрос

6 Блокчейн

В доказательстве работы криптографической хеш-функции используется сложность нахождения прообраза. (рис. 6.1)

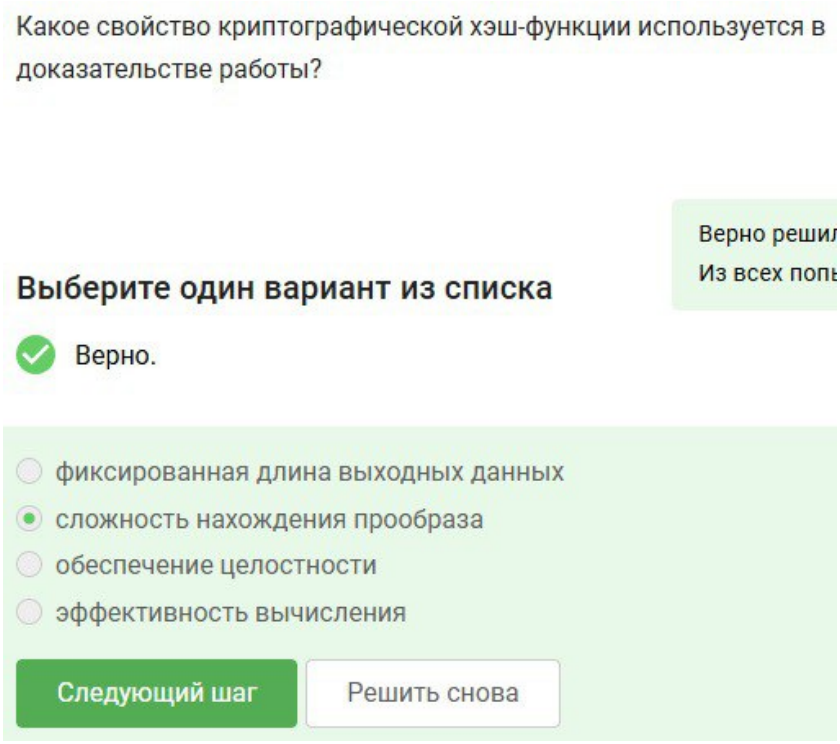

Рис. 6.1: Первый вопрос

Все ответы являются верными для консенсуса некоторых блокчейн систем. (рис. 6.2)

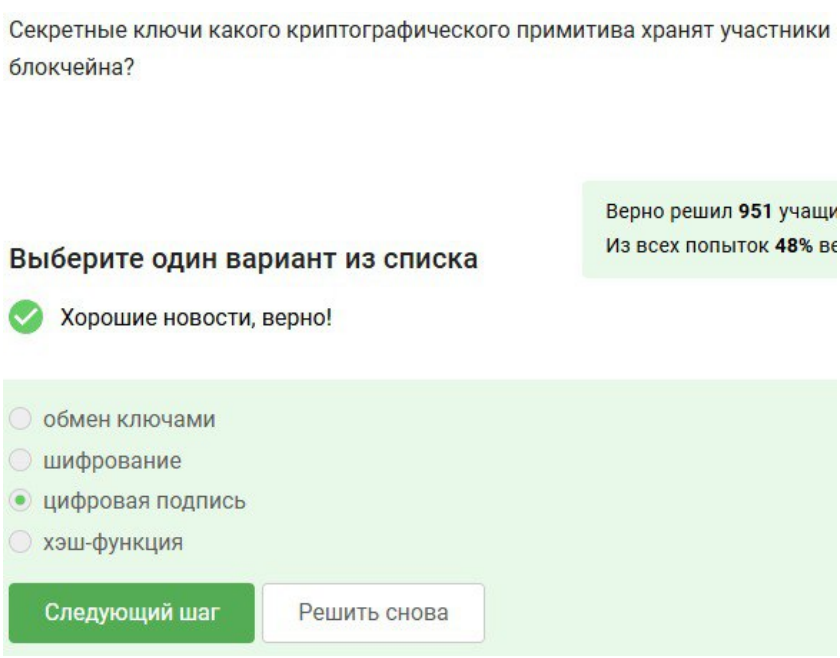

Рис. 6.2: Второй вопрос

Участники криптографического примитива хранят при себе только цифровую подпись. (рис. 6.3)

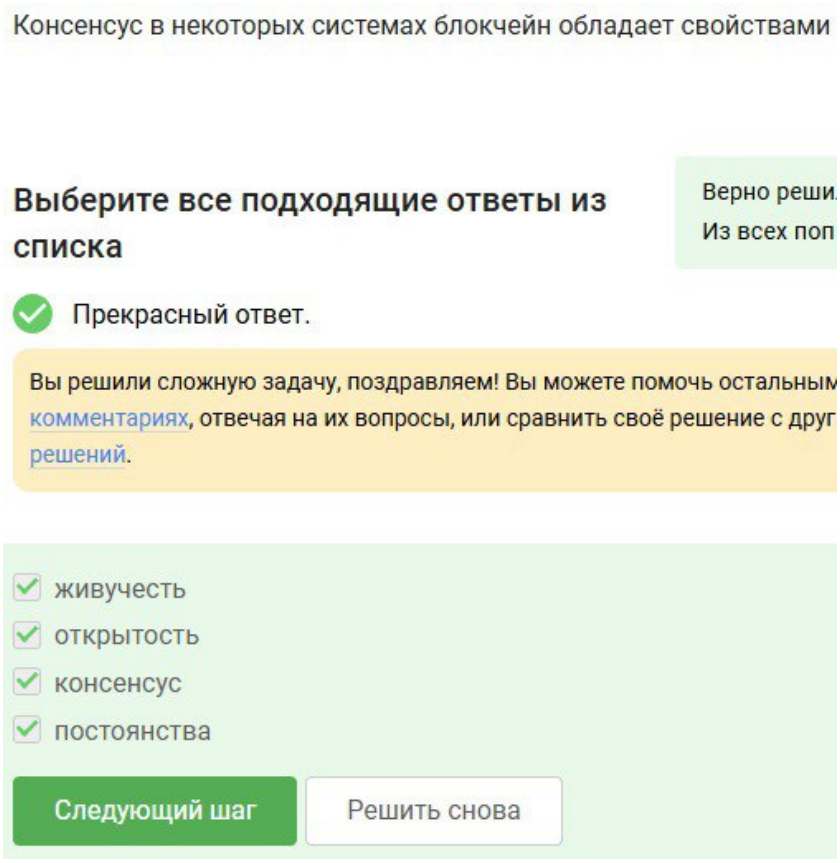

Рис. 6.3: Третий вопрос

7 Вывод

Выполнен третий этап внешнего курса