Основы кибербезопасности

Этап 3

Ведьмина Александра Сергеевна

Содержание

# 1 Цель работы

Выполнить задания третьей части курса по кибербезопасности.

# 2 Выполнение лабораторной работы

Два ключа - исходя из определения ассимитричного шифрования.

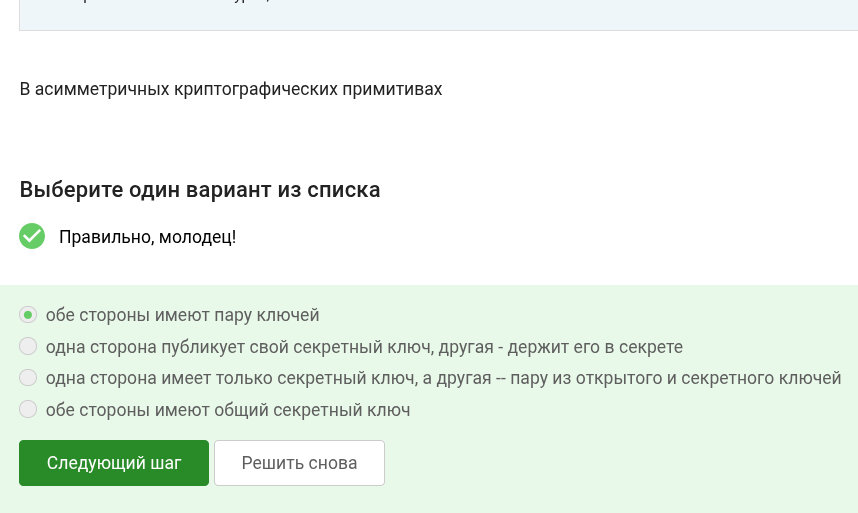


Рис. 1: Задание 1

По свойствам хэш-функции.

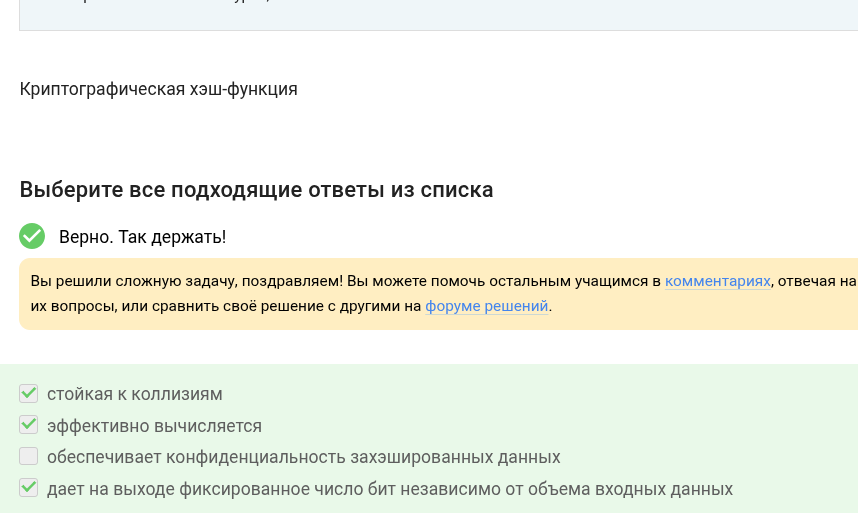


Рис. 2: Задание 2

Алгоритмы:

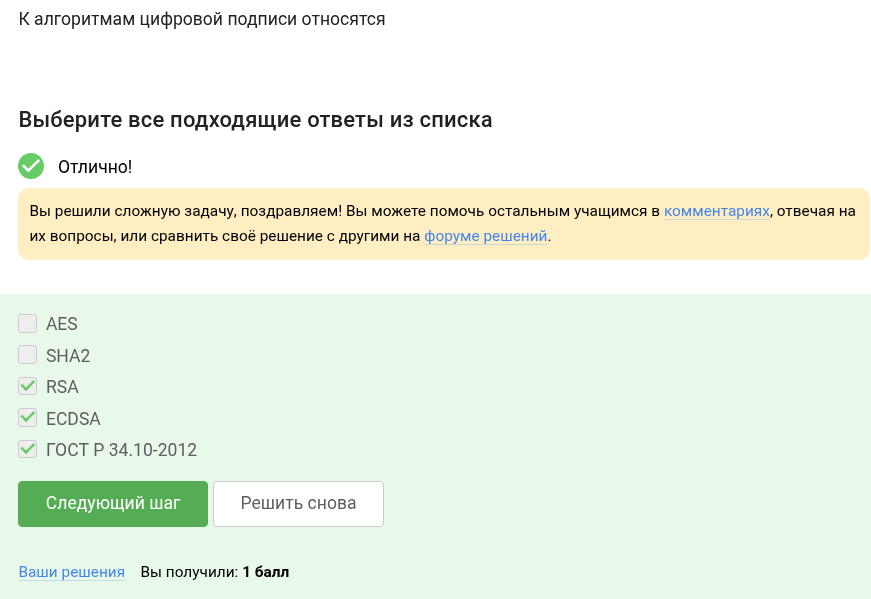


Рис. 3: Задание 3

Так как для шифровки и дешифровки используется один и тот же ключ.

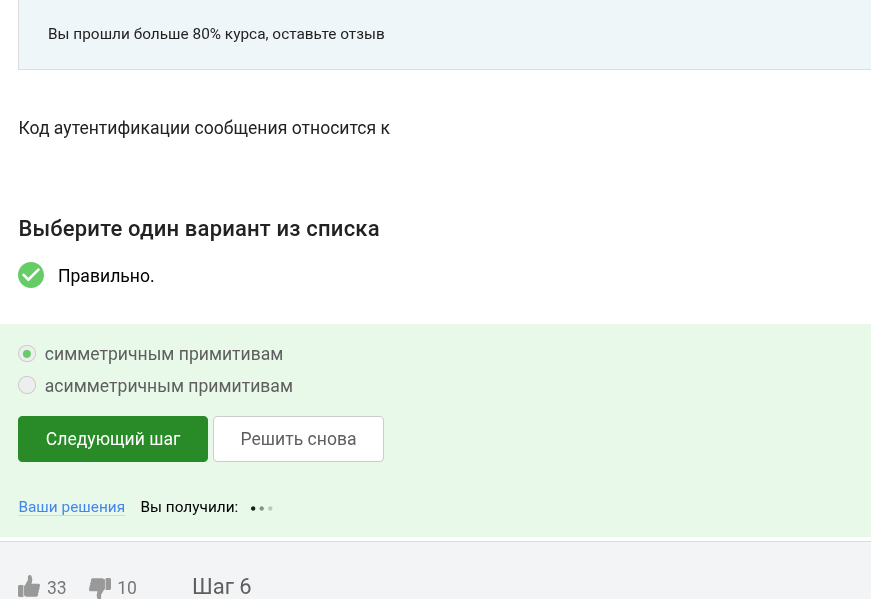


Рис. 4: Задание 4

По определению этого алгоритма.

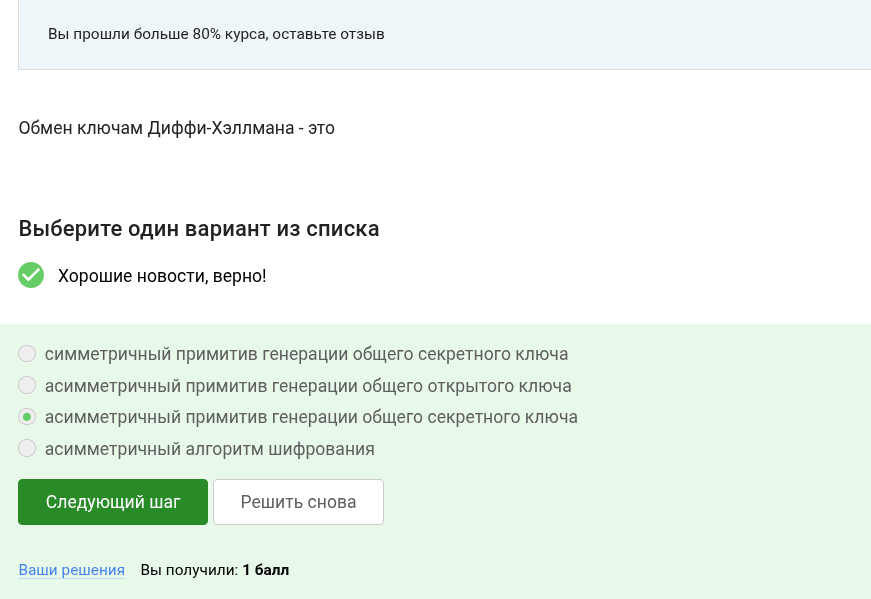


Рис. 5: Задание 5

Потому что используется ассиметричное шифрование.

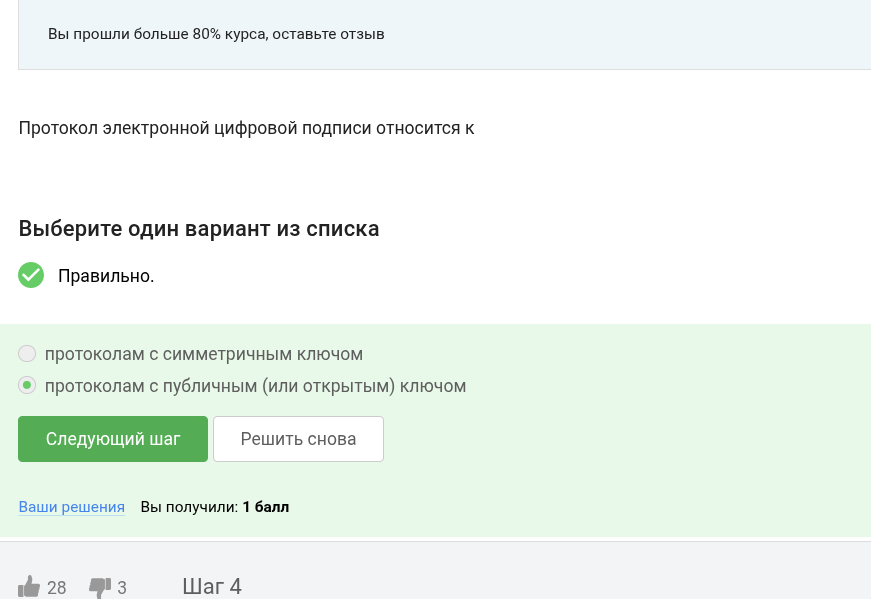


Рис. 6: Задание 6

Подписанное сообщение проверяется открытым ключом.

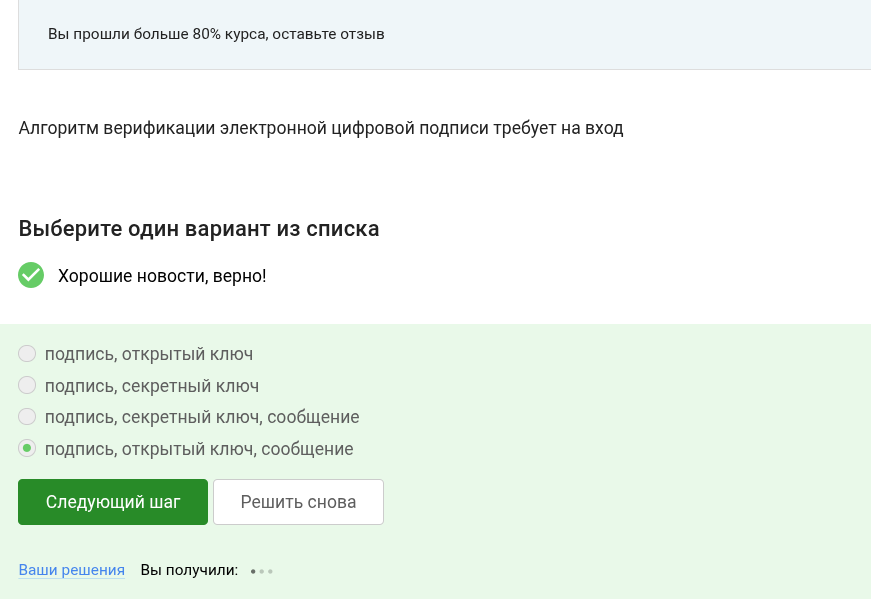


Рис. 7: Задание 7

Она наоборот гарантирует, что можно определить, кто подписал.

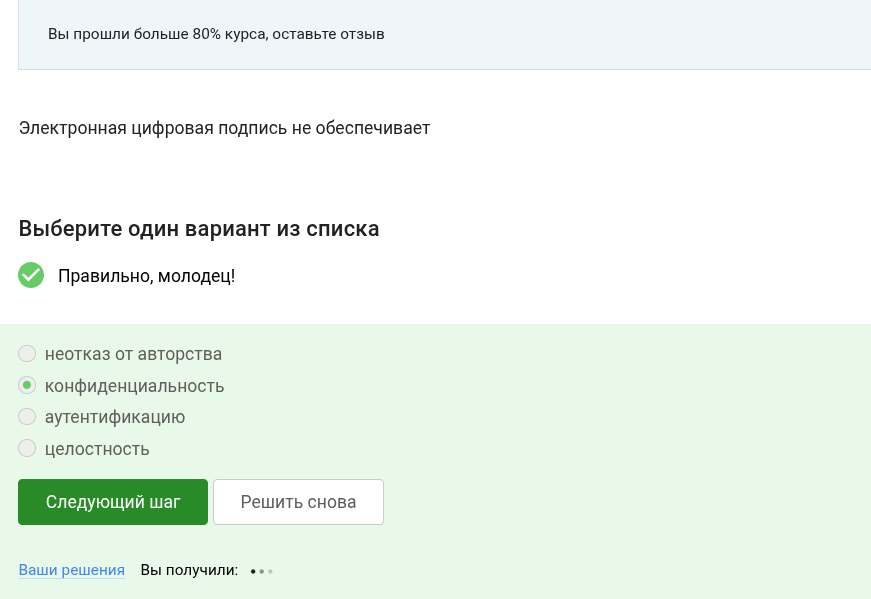


Рис. 8: Задание 8

Так как в налоговую нужны юридически значимые документы.

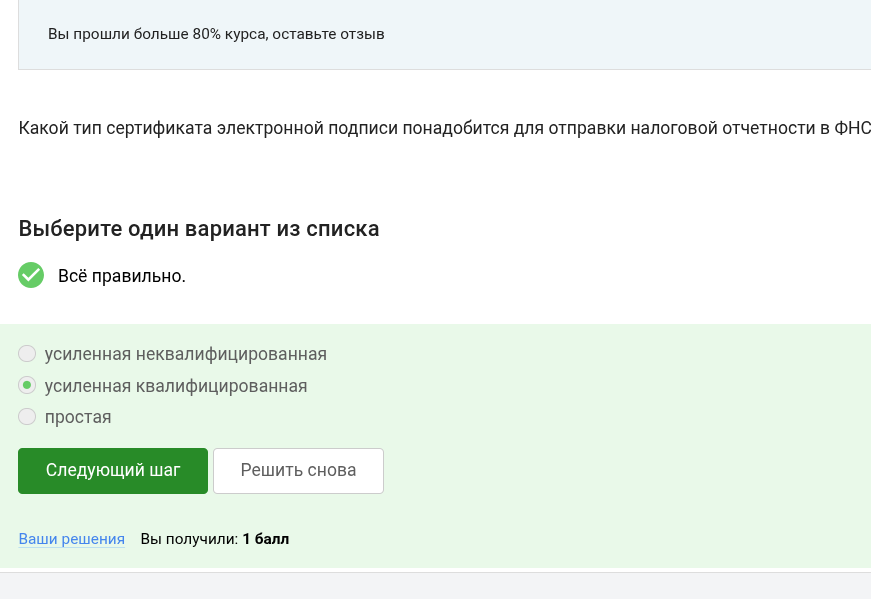


Рис. 9: Задание 9

В сертифицированном центре.

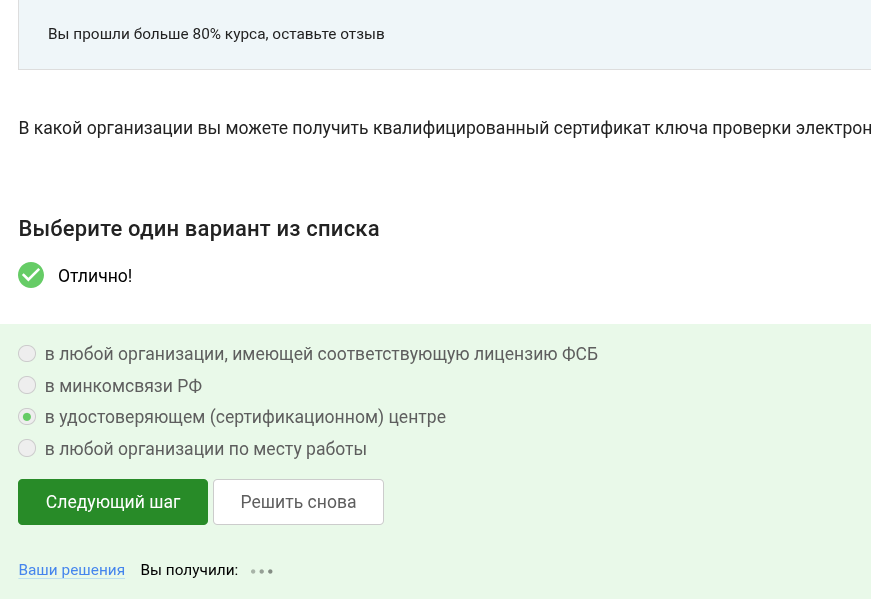


Рис. 10: Задание 10

МИР и Mastercard всем известны.

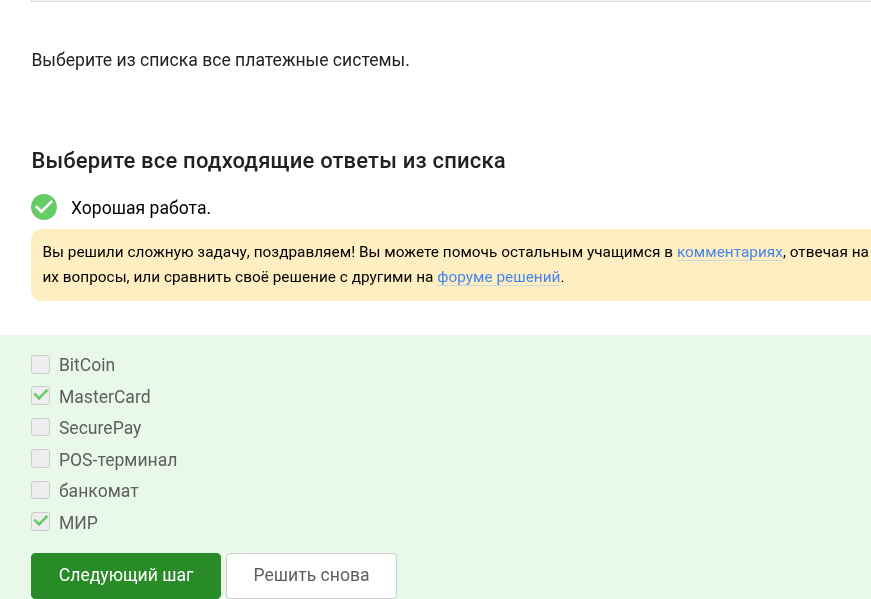


Рис. 11: Задание 11

Отметила верные методы.

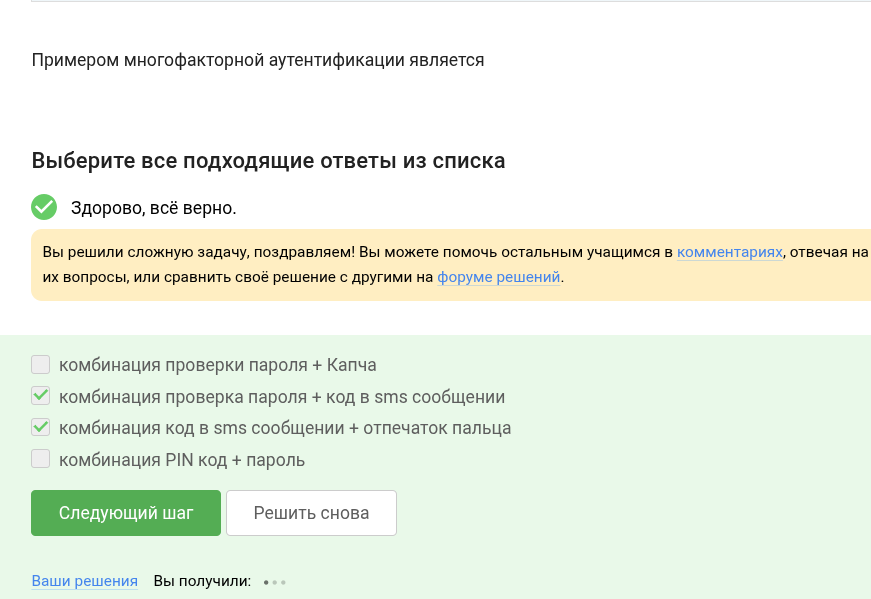


Рис. 12: Задание 12

Используется многофакторная аутентификация.

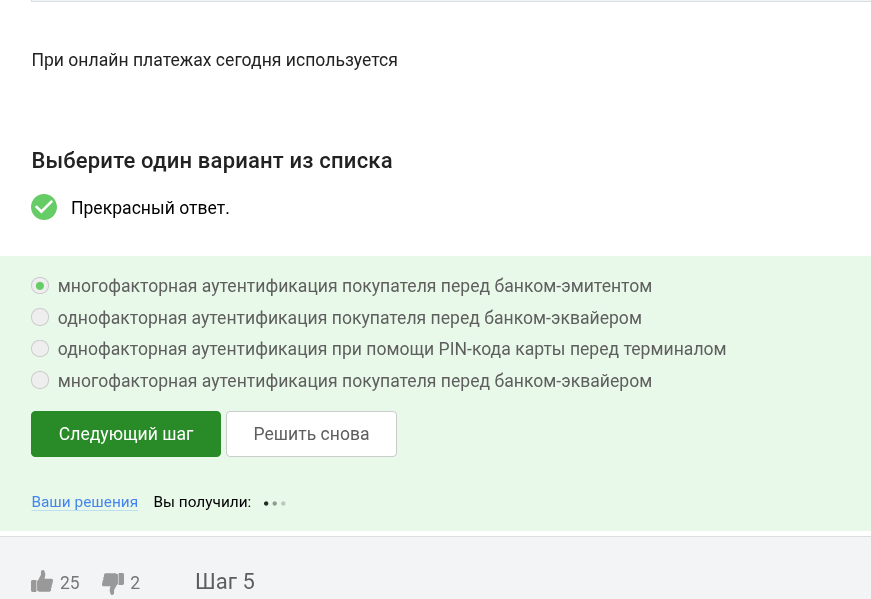


Рис. 13: Задание 13

Прообраз действительно сложно найти, поэтому она надёжна.

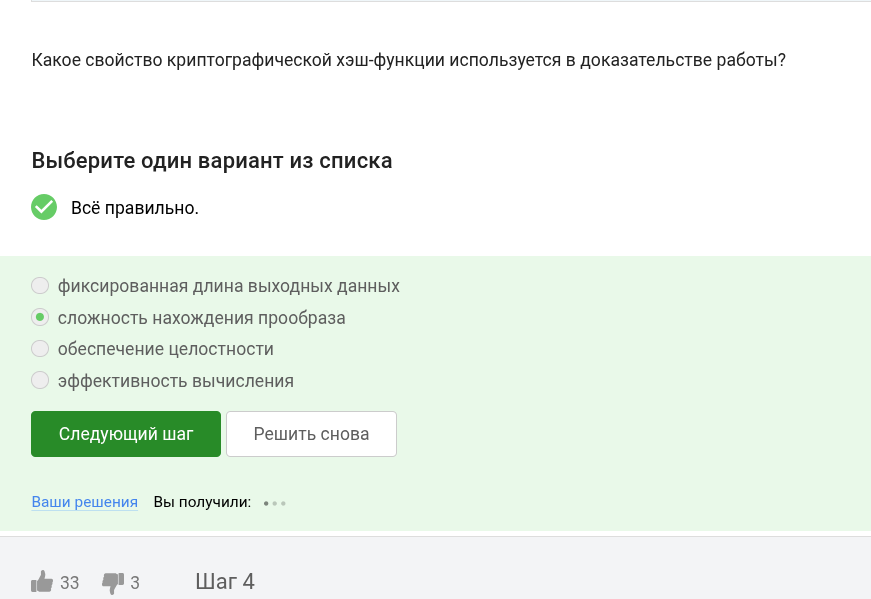


Рис. 14: Задание 14

По свойствам консенсуса.

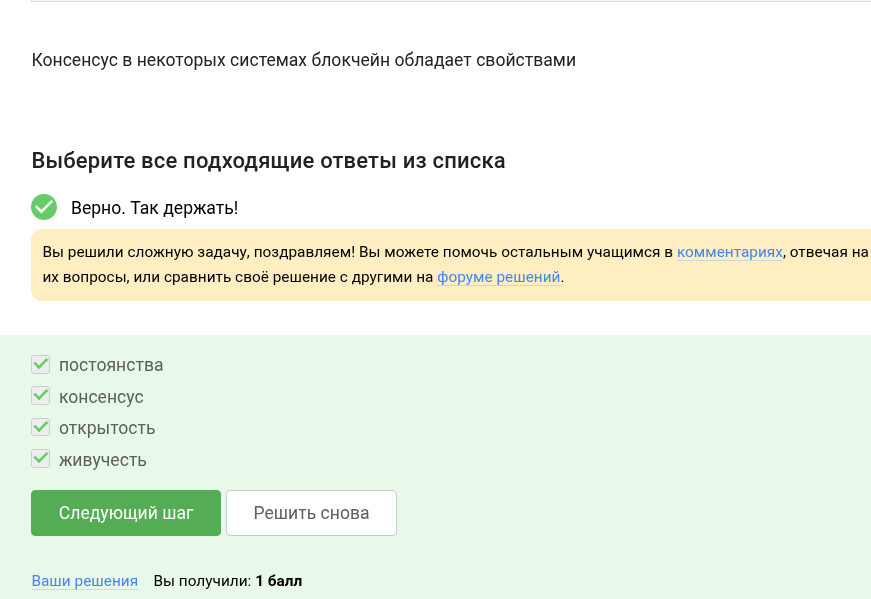


Рис. 15: Задание 15

Они хранят цифровые подписи.

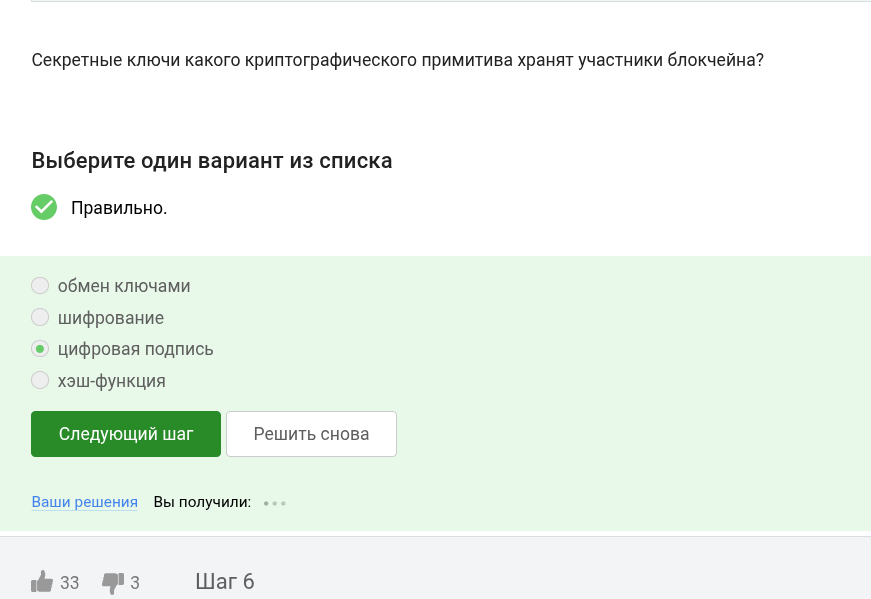


Рис. 16: Задание 16

Ура, я завершила курс!

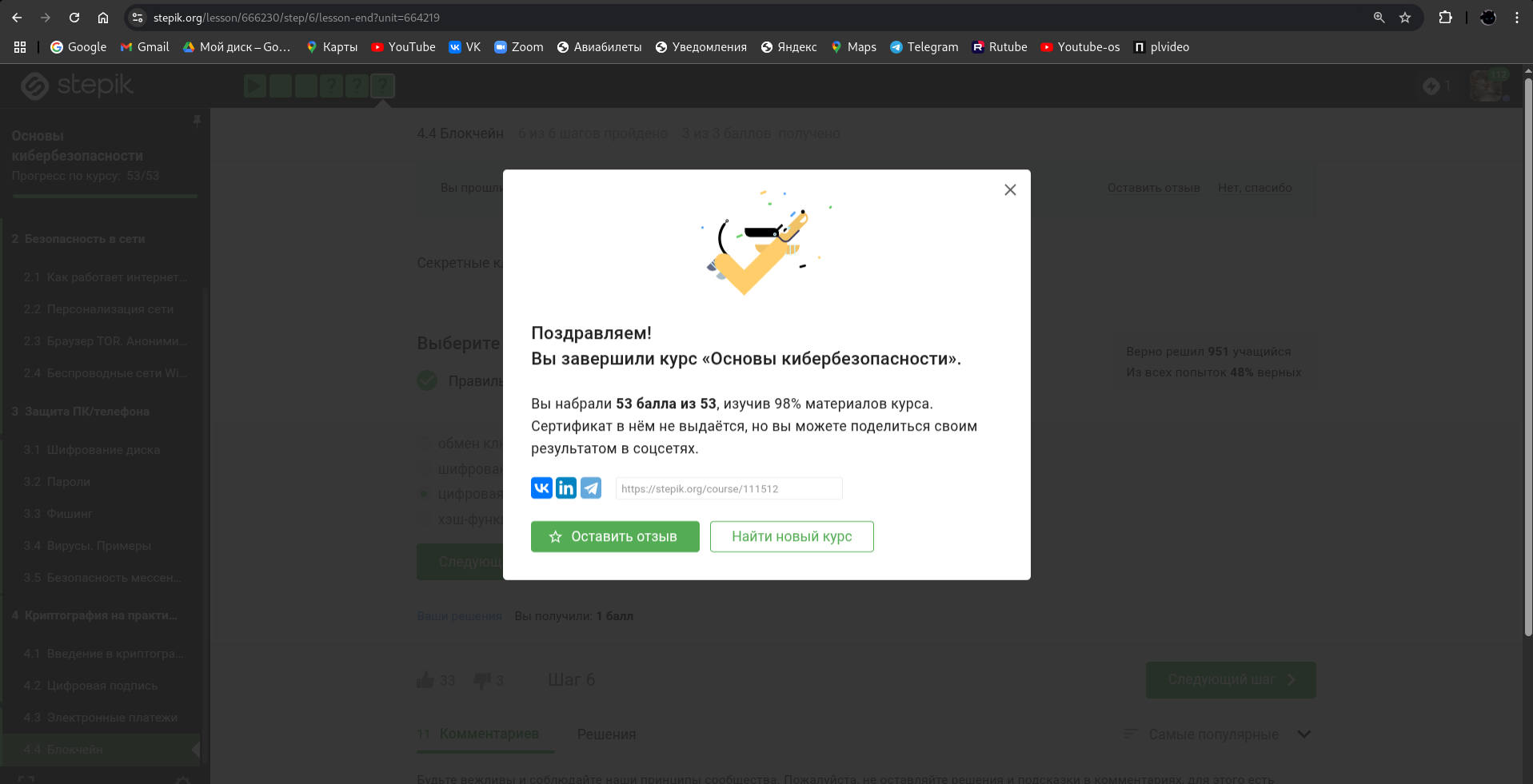


Рис. 17: Задание 17

# 3 Выводы

Все задания третьей части выполнены. Курс завершён.