Этап3

НКАбд-01-23

Улитина Мария Максимовна

Содержание

# 1 Выполнение второго этапа внешнего курса

Имеют пару ключей (рис. 1).

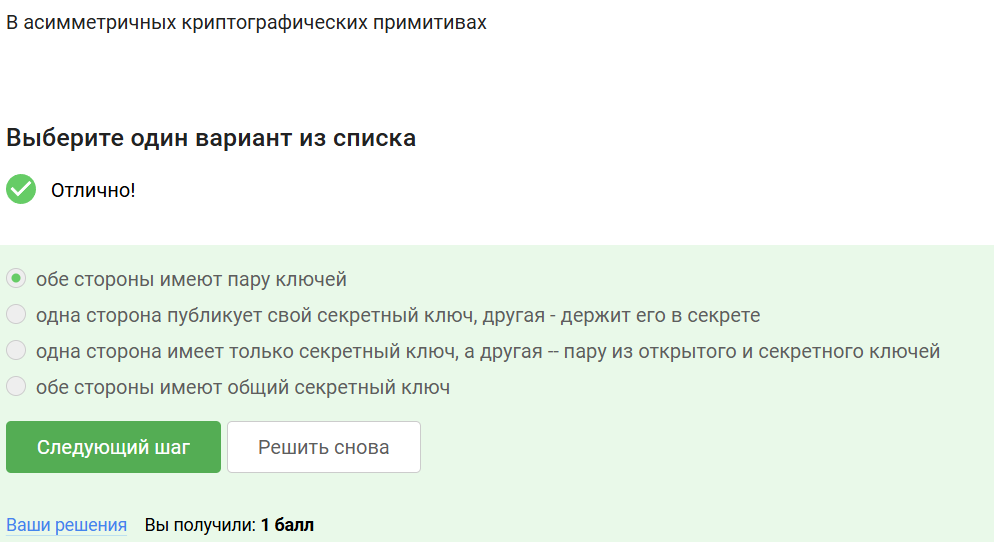


Рис. 1: ключи

Свойсва хэш-функции(рис. 2).

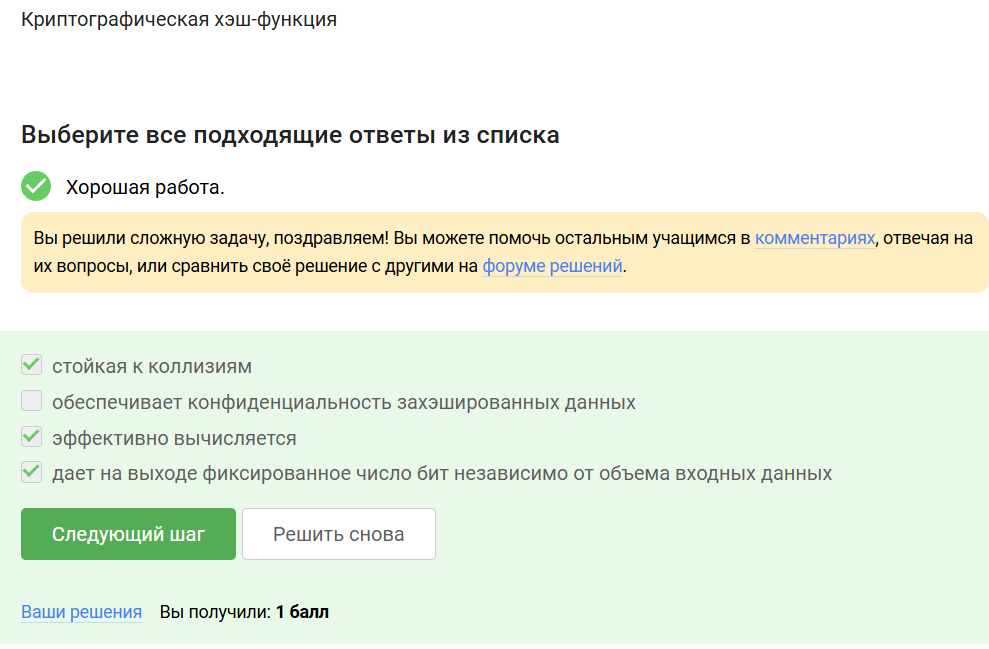


Рис. 2: хэш-функция

Алгоритмы цифровой функции (рис. 3).

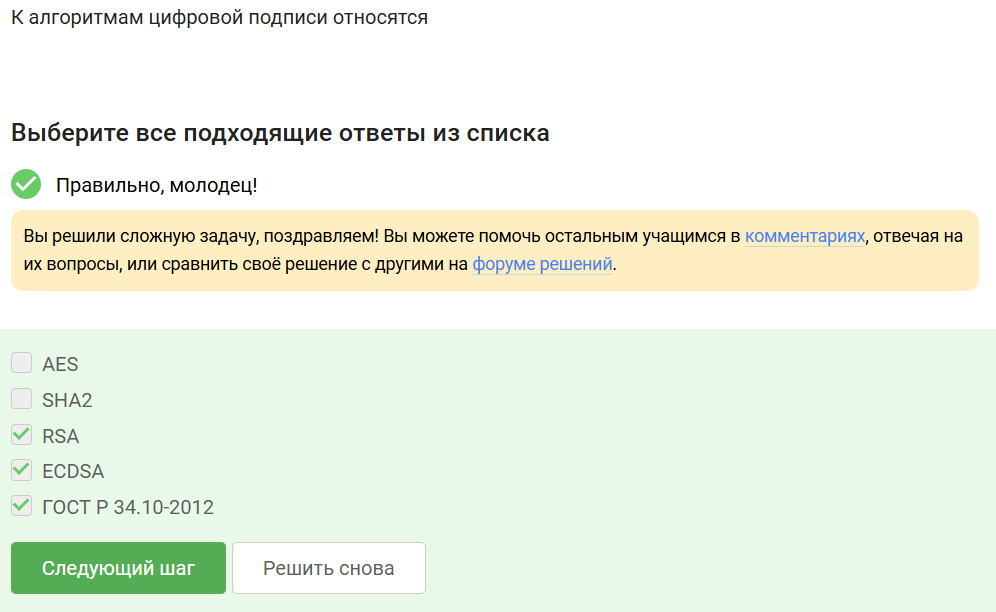


Рис. 3: функция

Код аутентификации (рис. 4).

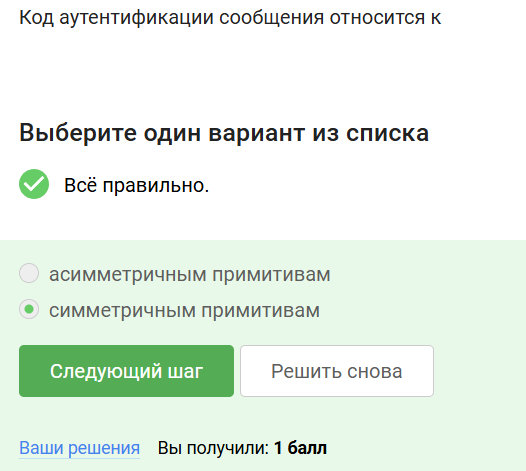


Рис. 4: код

Ключи Диффи-хеллмэна(рис. 5).

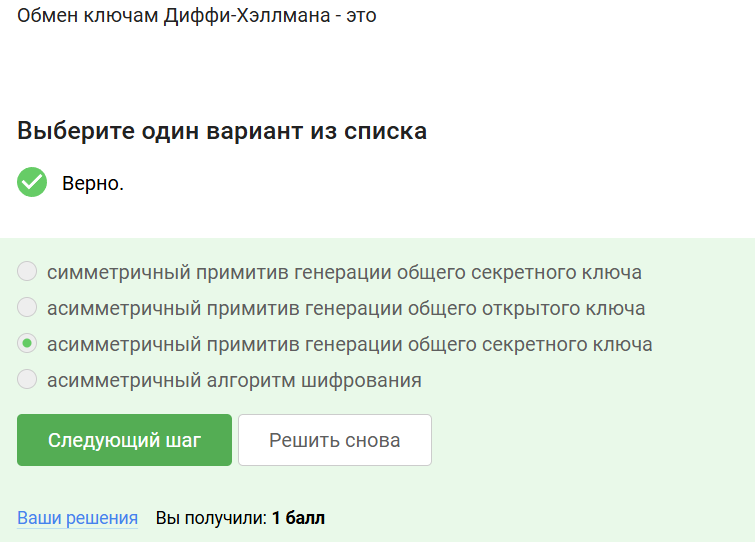


Рис. 5: ключи

Электронная цифровая подпись(рис. 6).

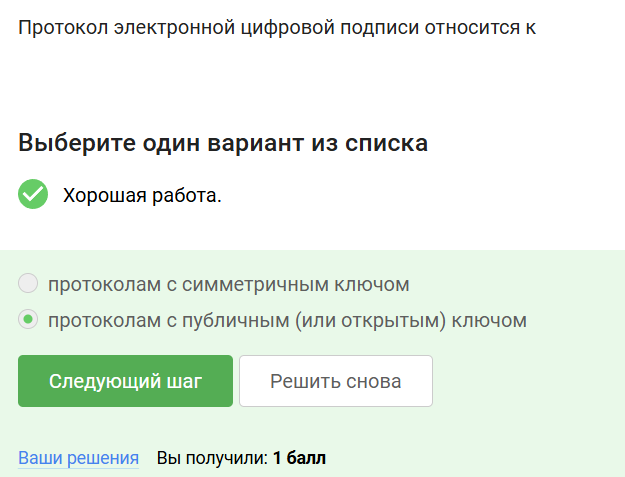


Рис. 6: подпись

Алгоритм верификации (рис. 7).

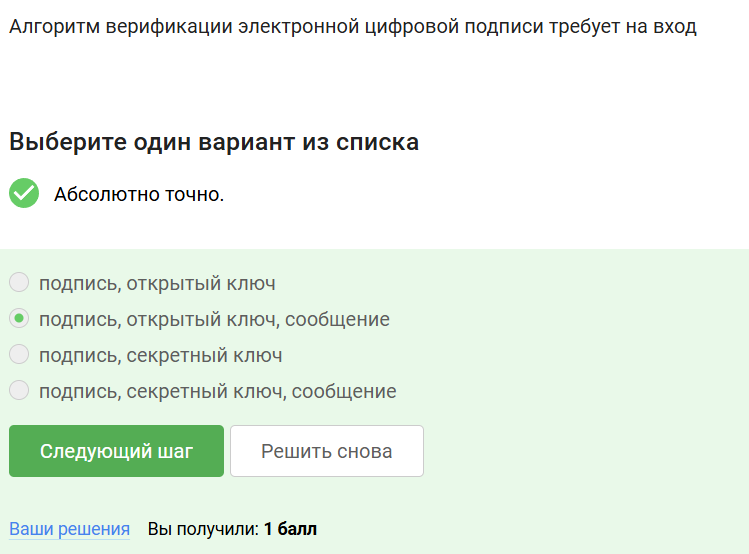


Рис. 7: алгоритм

Не обеспечивает конфиденциальность(рис. 8).

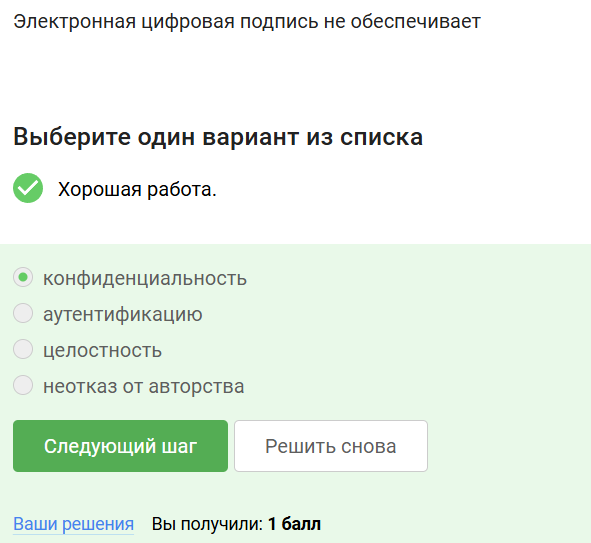


Рис. 8: подпись

Усиленная квалифицированная(рис. 9).

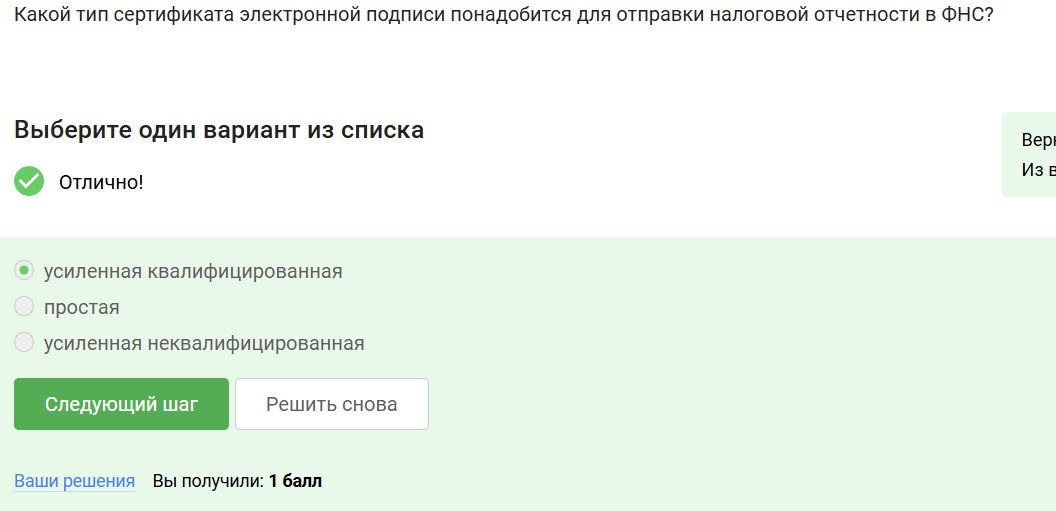


Рис. 9: подпись

Организация(рис. 10).

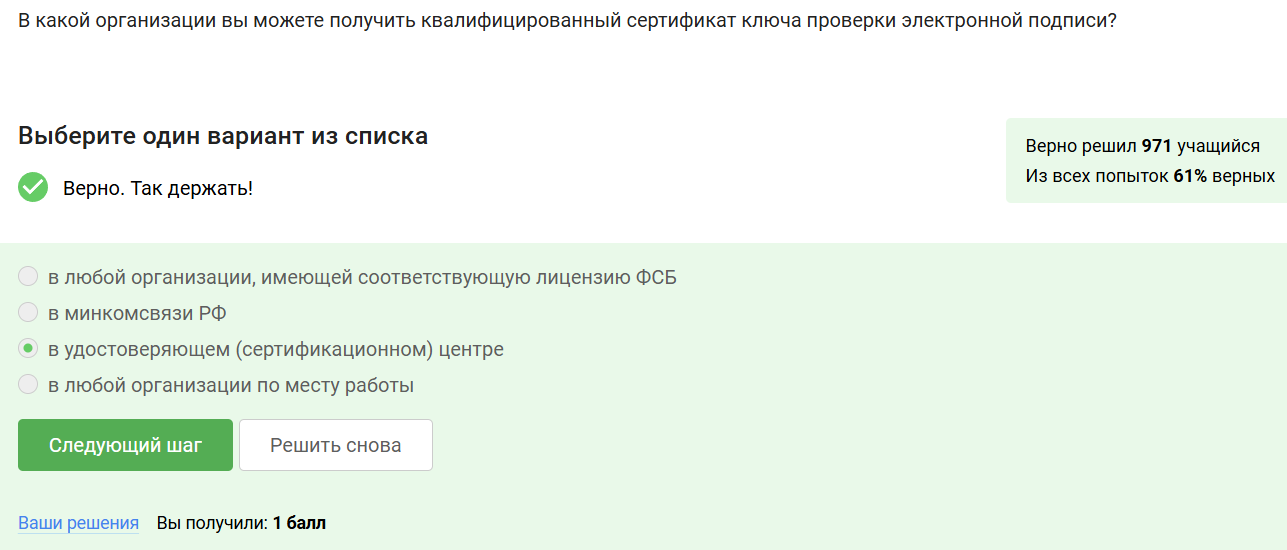


Рис. 10: организация

Платежные системы МИР и Мастер Кард(рис. 11).

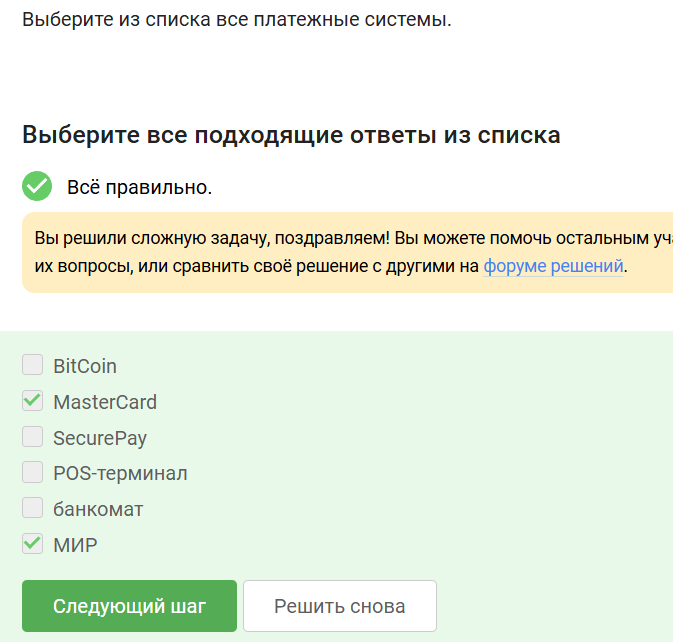


Рис. 11: платежные системы

МФ аутентификация(рис. 12).

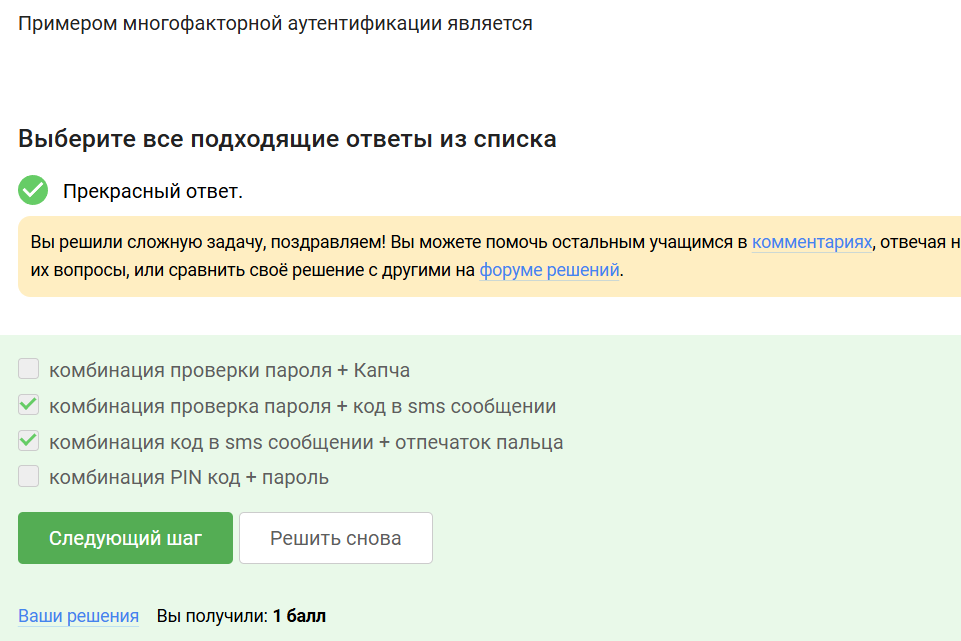


Рис. 12: примеры

Гдеиспользуется мфа(рис. 13).

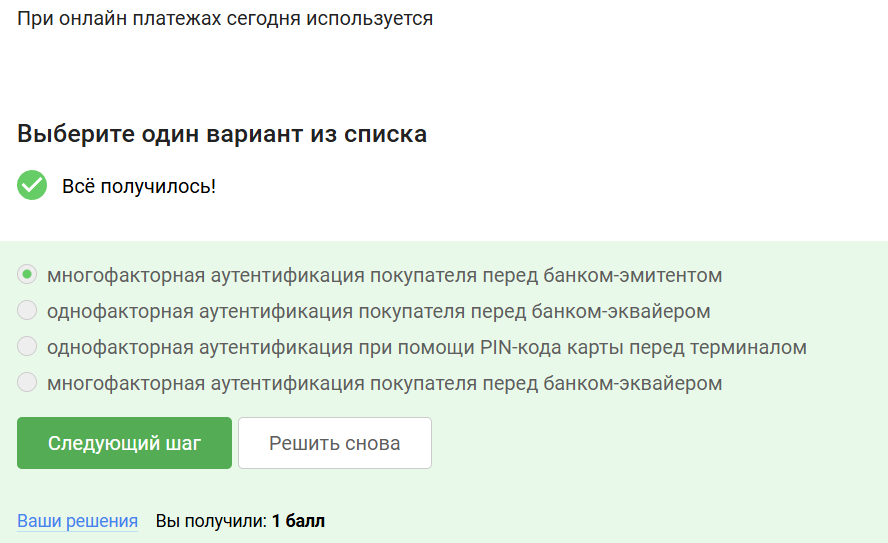


Рис. 13: мфа

Сложность нахождения прообраза (рис. 14).

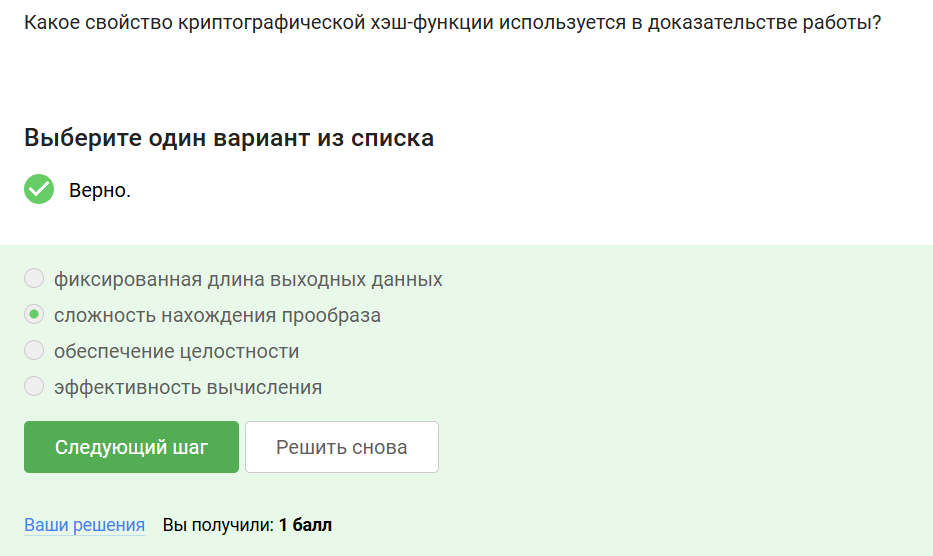


Рис. 14: хэш-функция

консенсус(рис. 15).

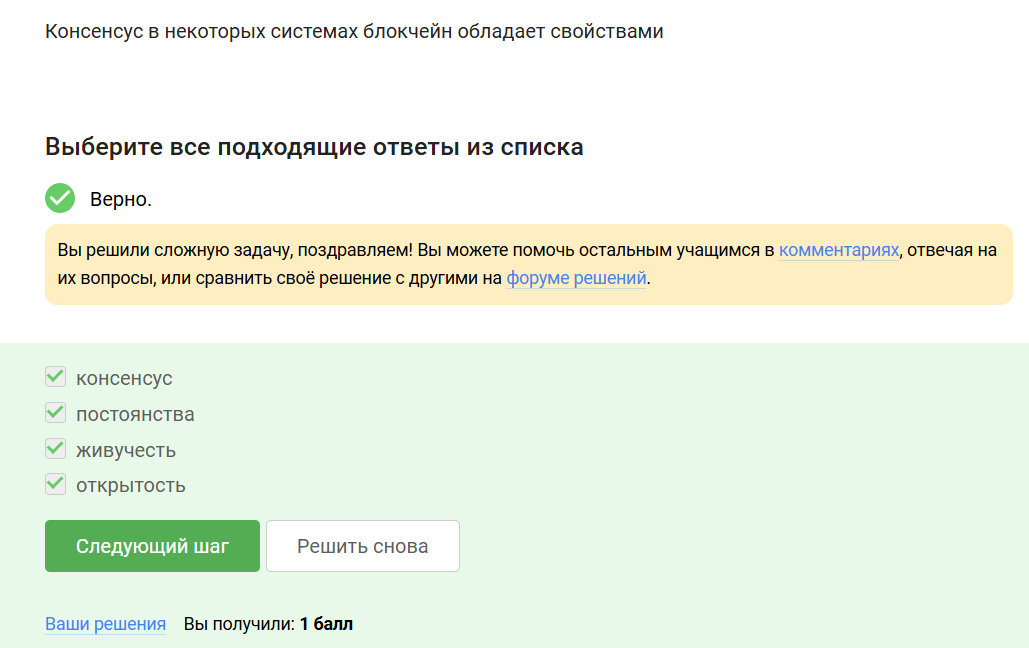


Рис. 15: консенсус

# 2 Выводы

Выволнен третий этап.