Внешний курс

Основы кибербезопасности

Галиева Аделина Руслановна

Содержание

# 1 Цель работы

Изучить основы кибербезопасности.

# 2 Прохождение курса

1. Введение в курс

# 3 Безопасность в сети

* 1. Как работает интернет: базовые сетевые протоколы.

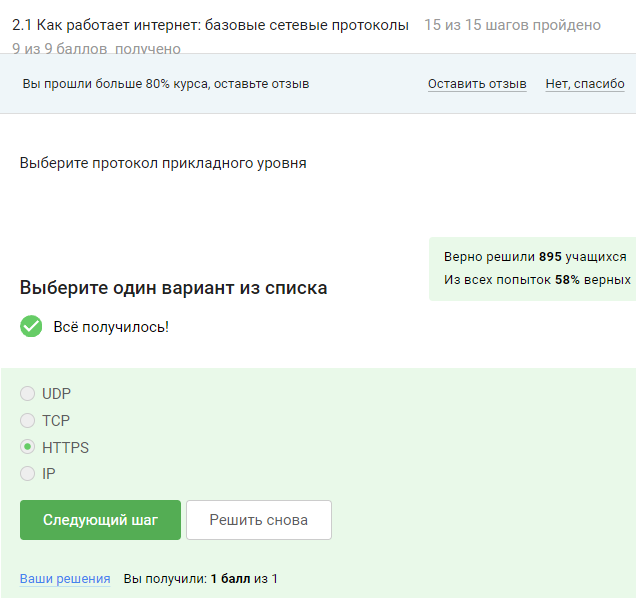


Figure 1: Протокол прикладного уровня

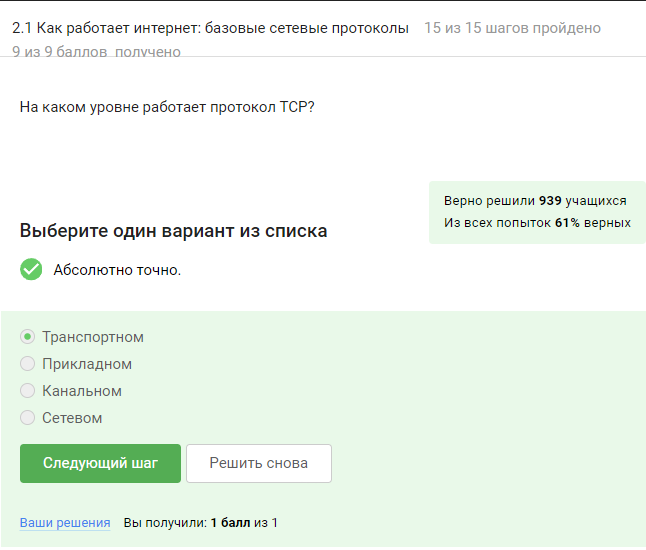


Figure 2: Протокол ТСР

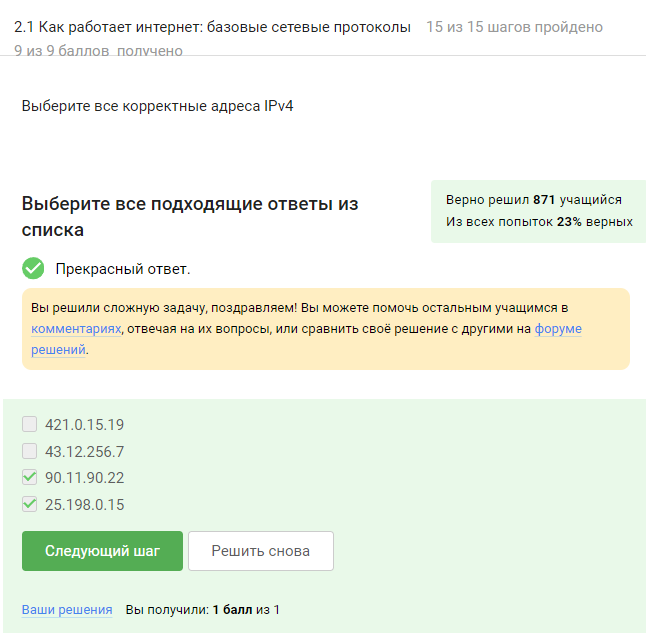


Figure 3: Адреса IPv-4

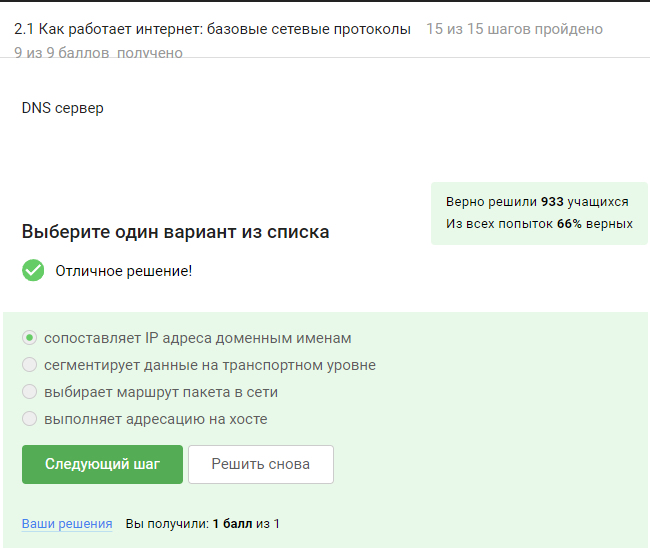


Figure 4: DNS сервер

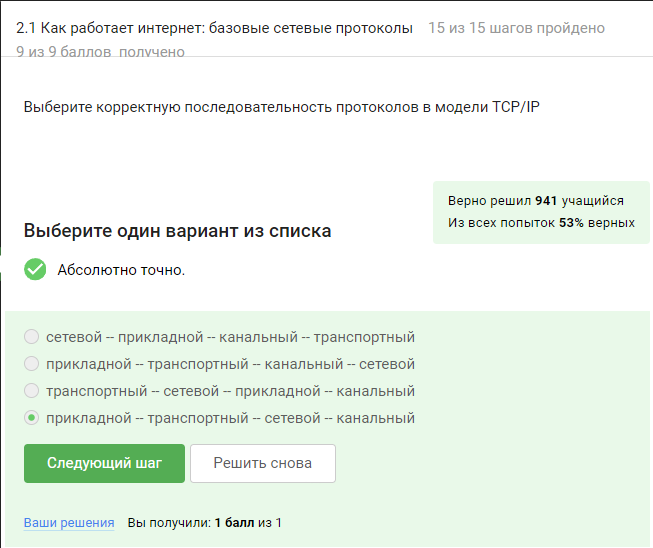


Figure 5: Протокол в модели ТСР/IP

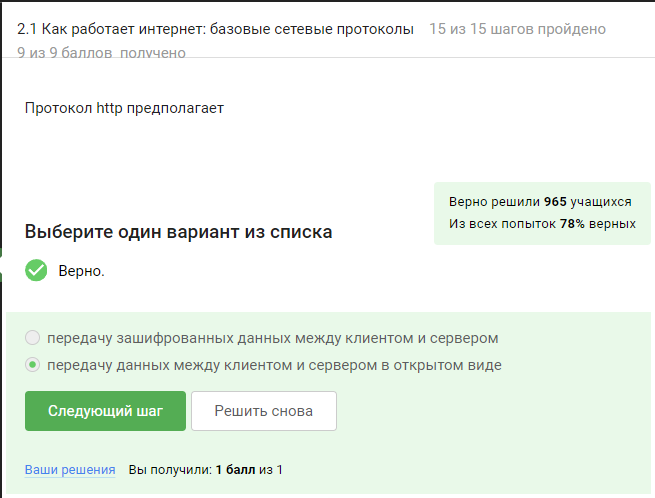


Figure 6: Протокол htpp

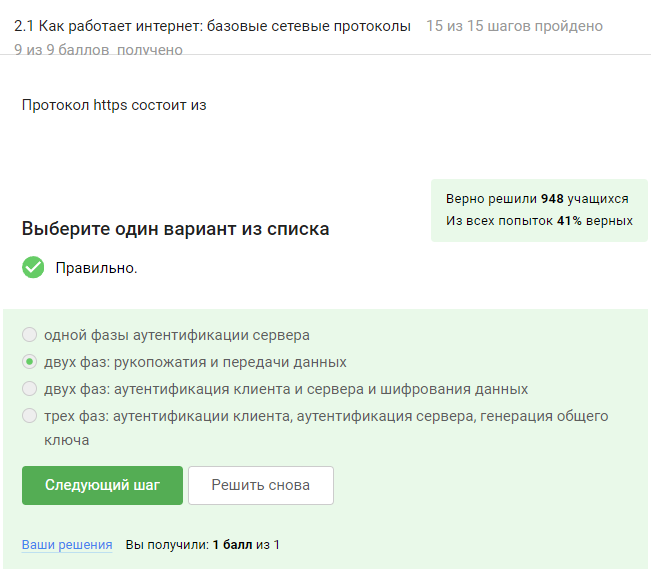


Figure 7: Протокол https

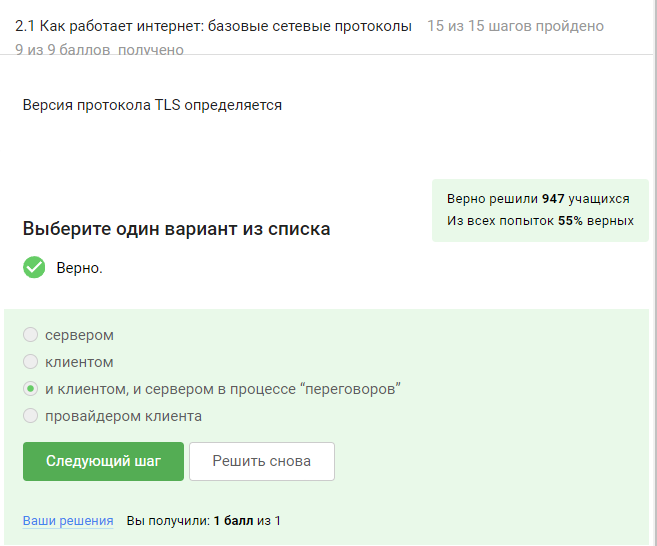


Figure 8: Протокол TLS

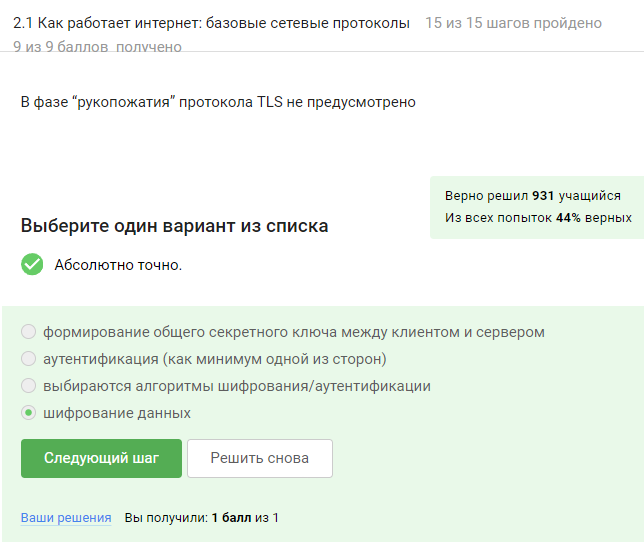


Figure 9: Протокол TLS

* 1. Персонализация сети.

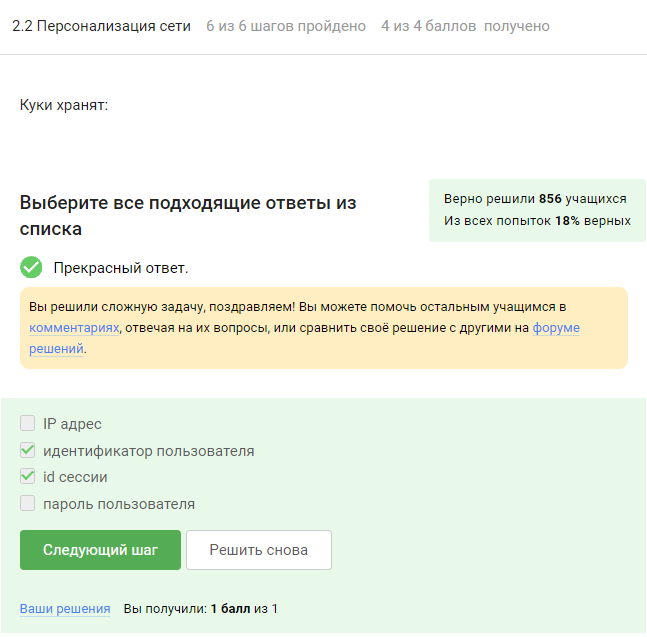


Figure 10: Куки хранят

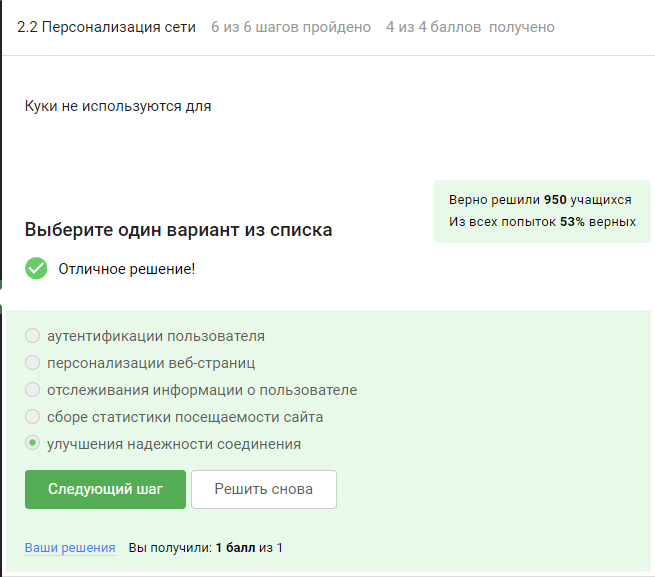


Figure 11: Куки не используются

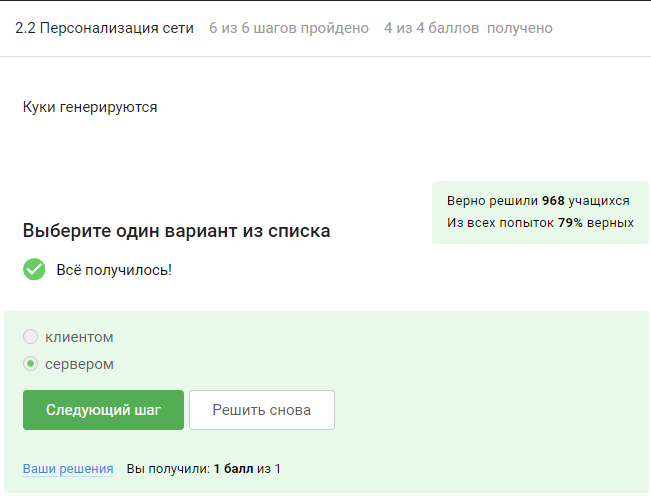


Figure 12: Куки генерируются

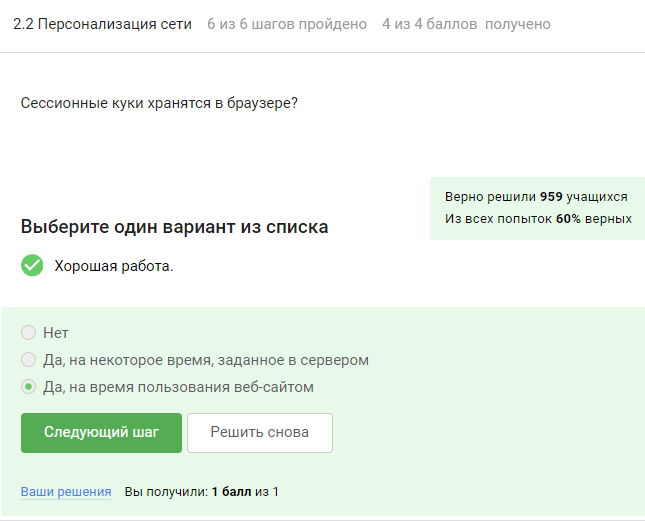


Figure 13: Сессионные куки

* 1. Браузер TOR. Анимация.

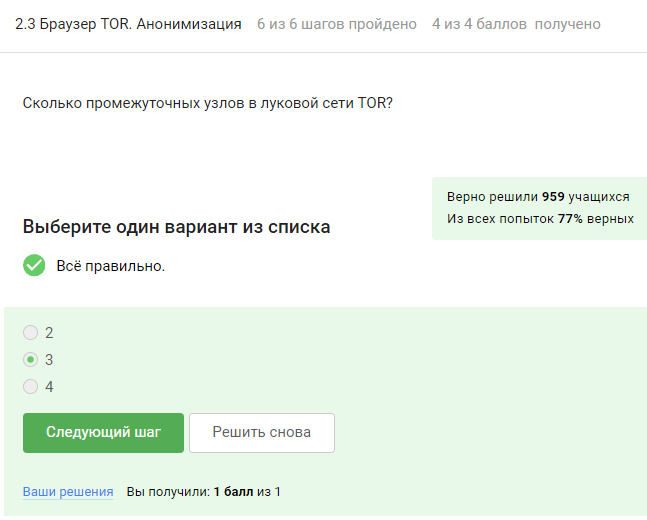


Figure 14: Промежуточные узлы TOR

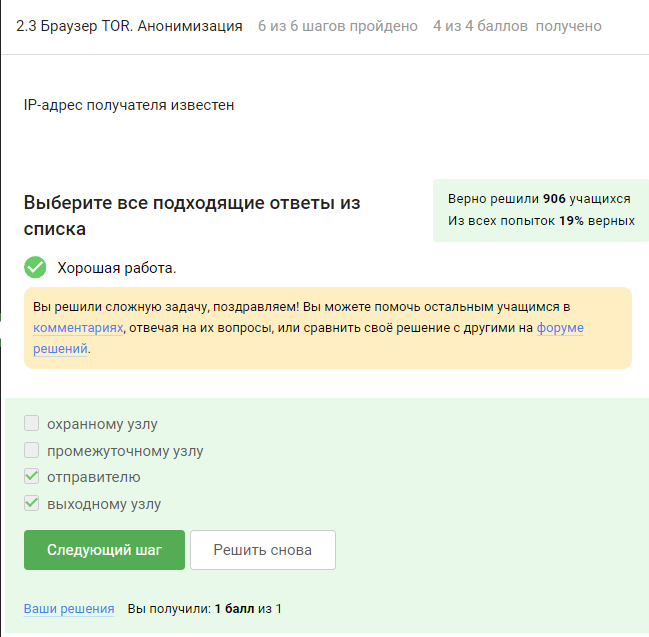


Figure 15: Браузер TOR

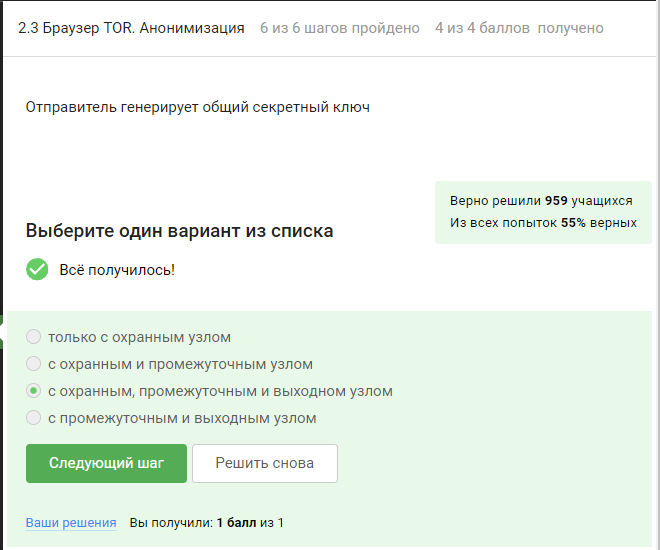


Figure 16: Секретный ключ

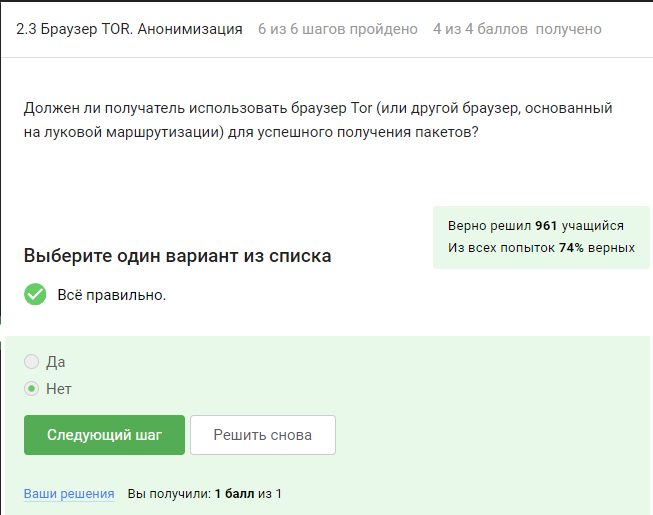


Figure 17: Браузер TOR

* 1. Беспроводные сети Wi-Fi.

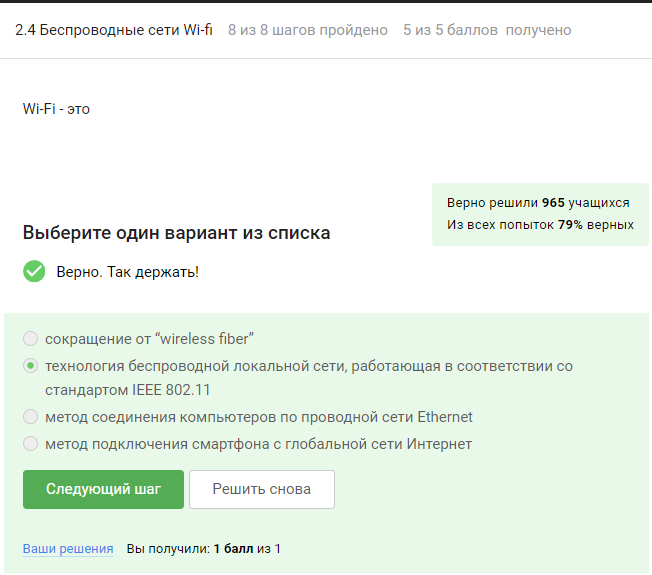


Figure 18: Wi-Fi

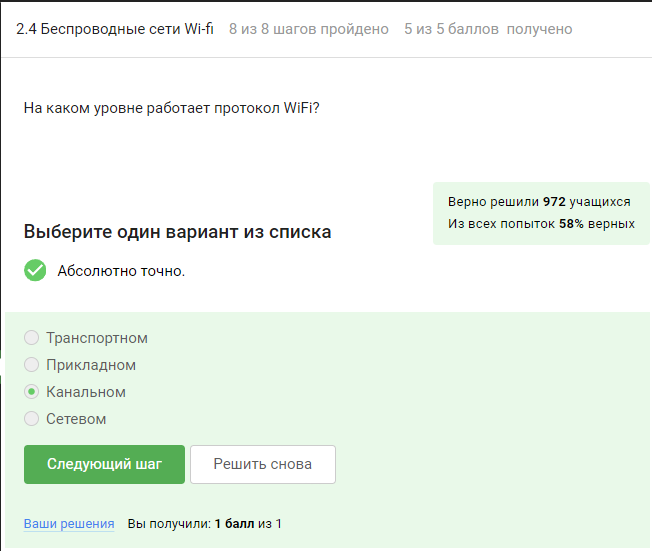


Figure 19: Протокол Wi-Fi

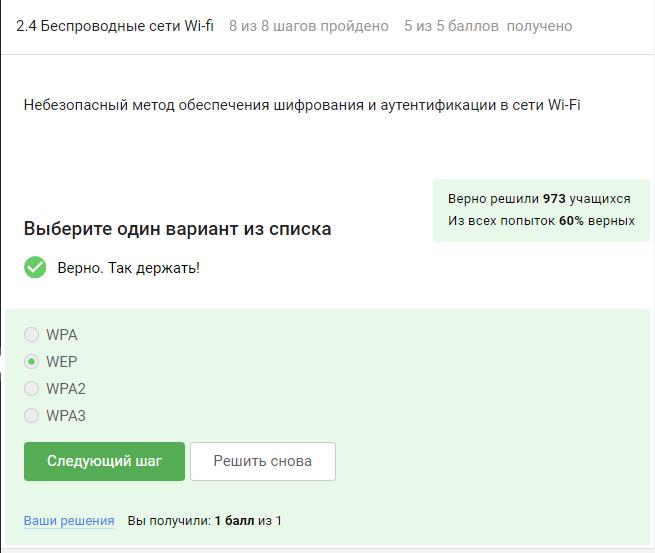


Figure 20: Шифрование Wi-Fi

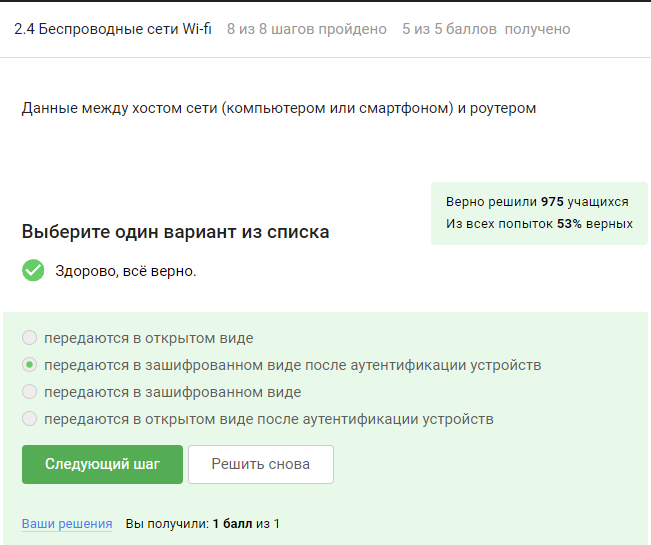


Figure 21: Данные между хостом и роутером

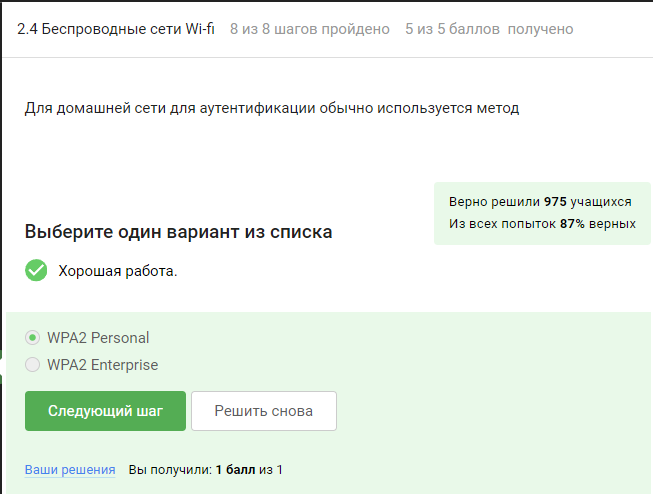


Figure 22: Метод

# 4 Защита ПК/телефона

* 1. Шифрование диска.

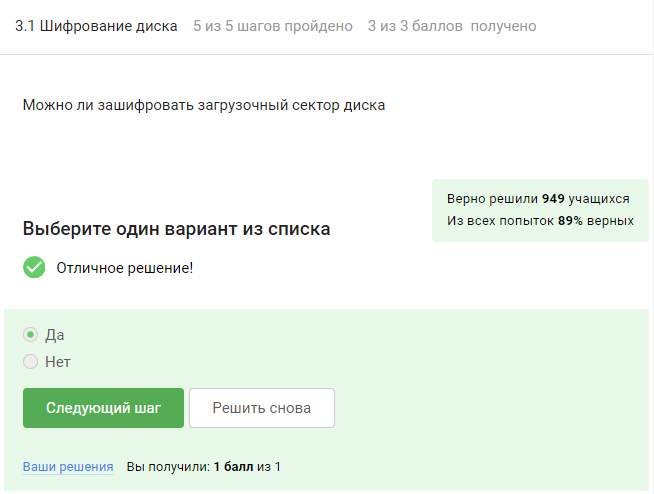


Figure 23: Загрузочный сектор диска

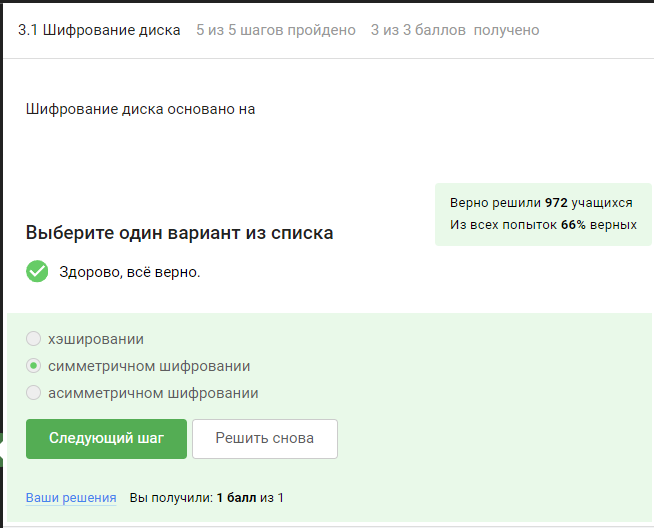


Figure 24: Шифрование диска

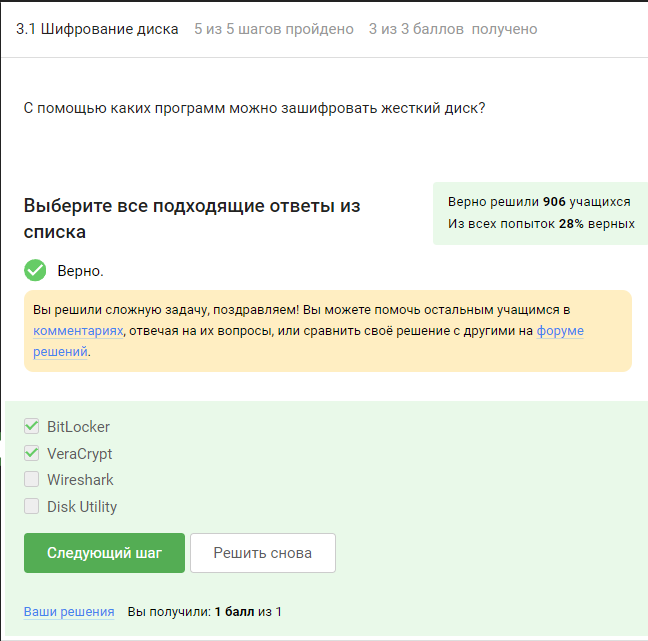


Figure 25: Жесткий диск

* 1. Пароли.

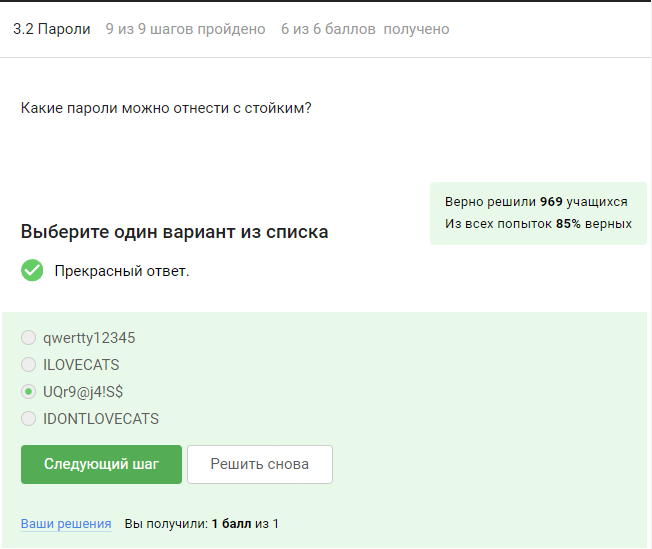


Figure 26: Пароли

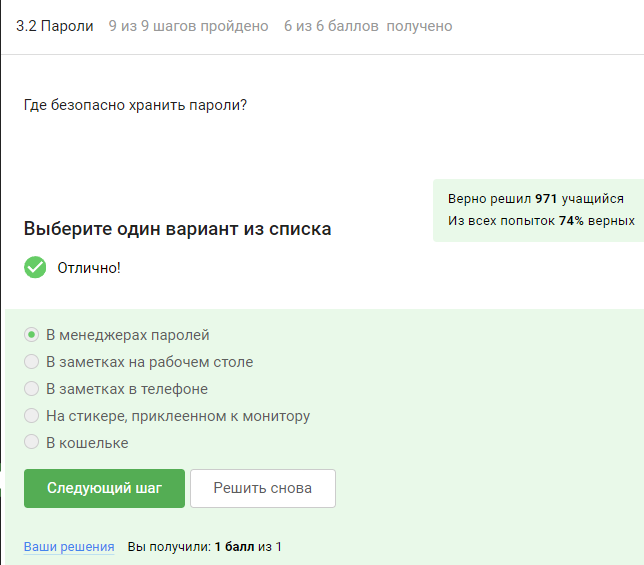


Figure 27: Хранение паролей

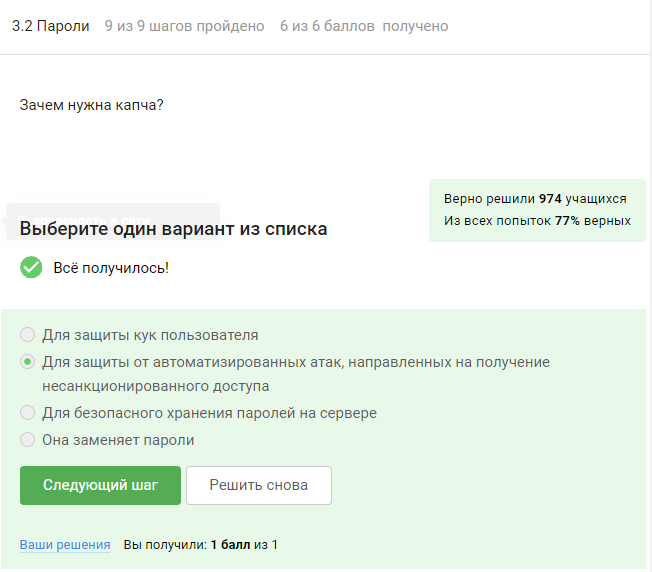


Figure 28: Капча

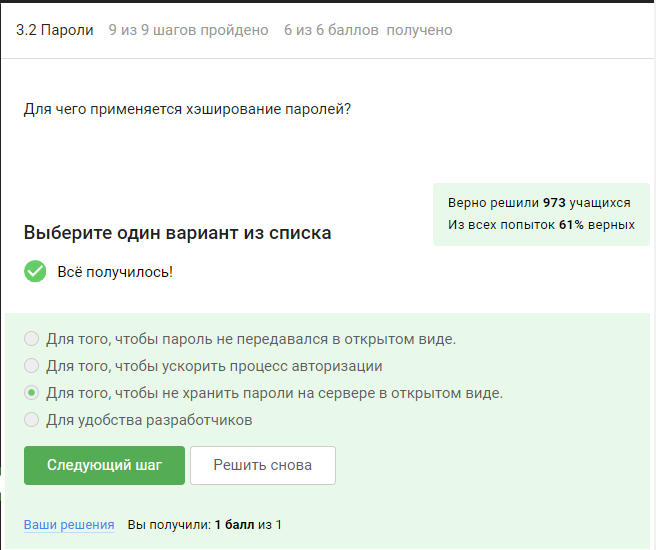


Figure 29: Хэширование паролей

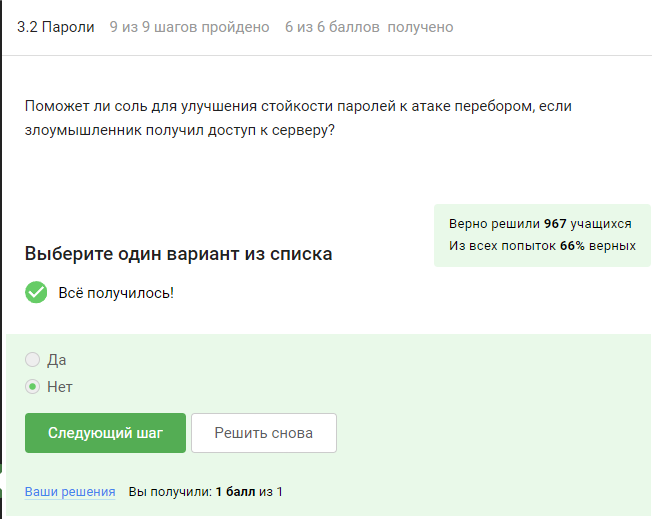


Figure 30: Стойкость паролей

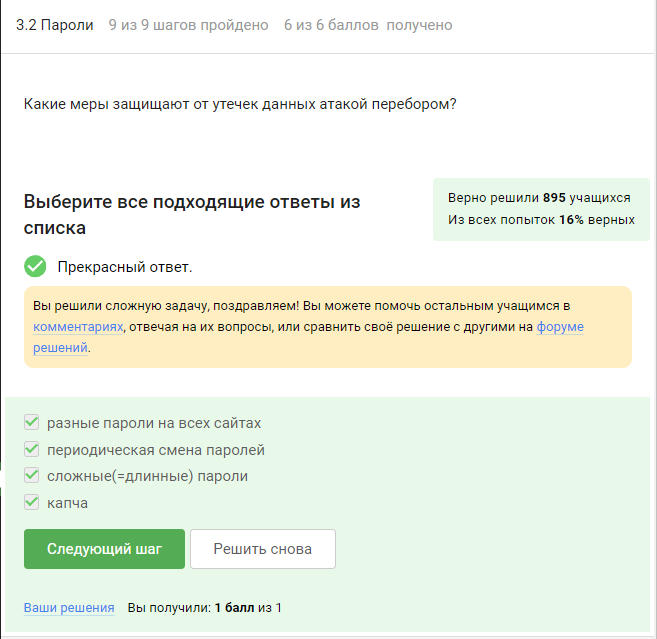


Figure 31: Меры защиты паролей

* 1. Фишинг.

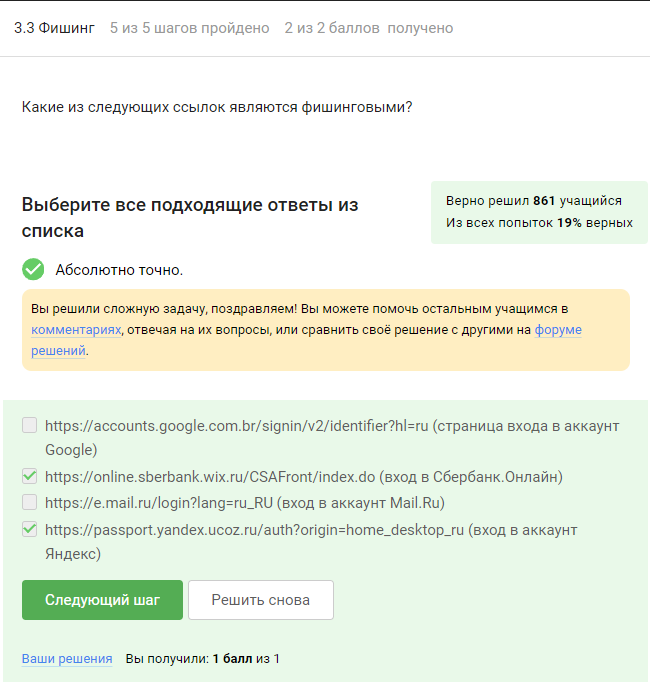


Figure 32: Фишинговые ссылки

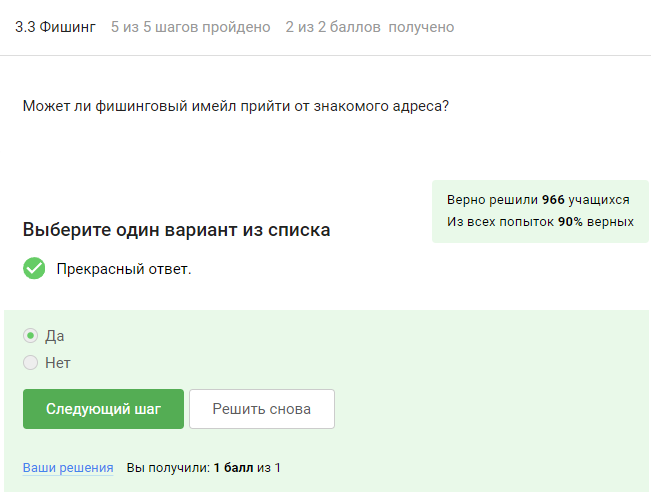


Figure 33: Фишинговый имейл

* 1. Вирусы. Примеры.

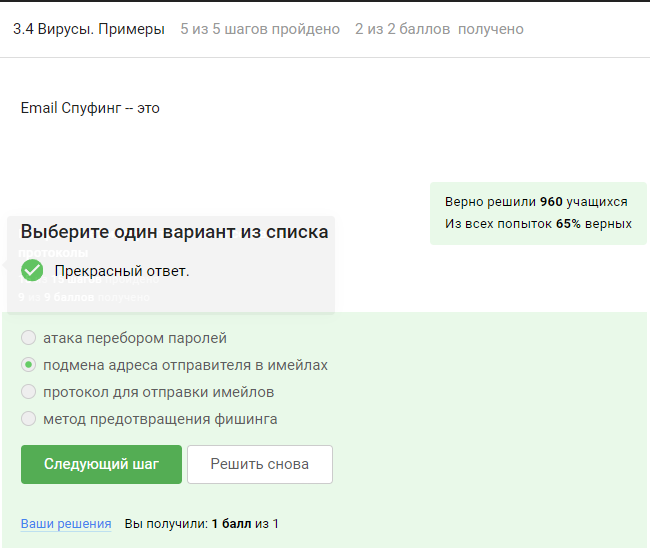


Figure 34: Спуфинг

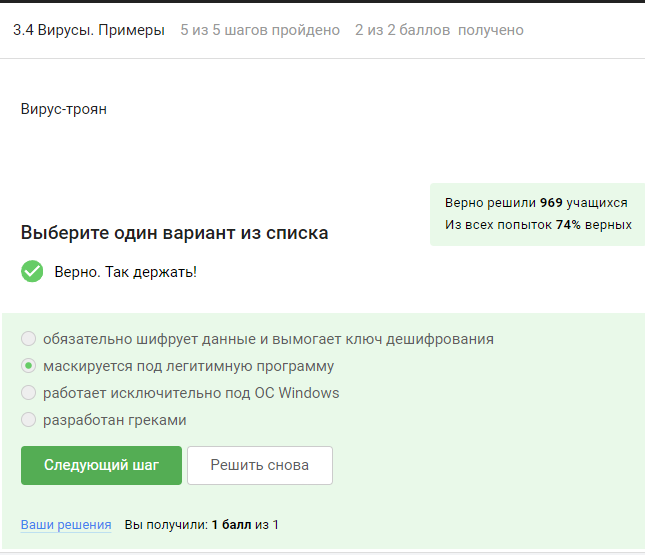


Figure 35: Вирус-троян

* 1. Безопасность мессенджеров.

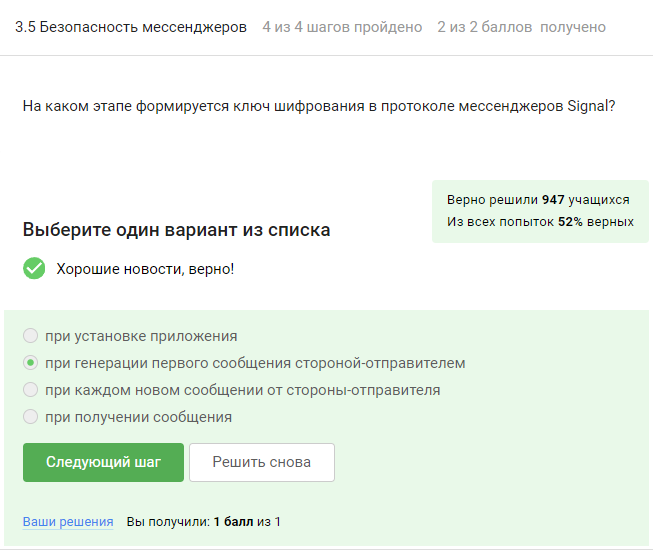


Figure 36: Мессенджер Signal

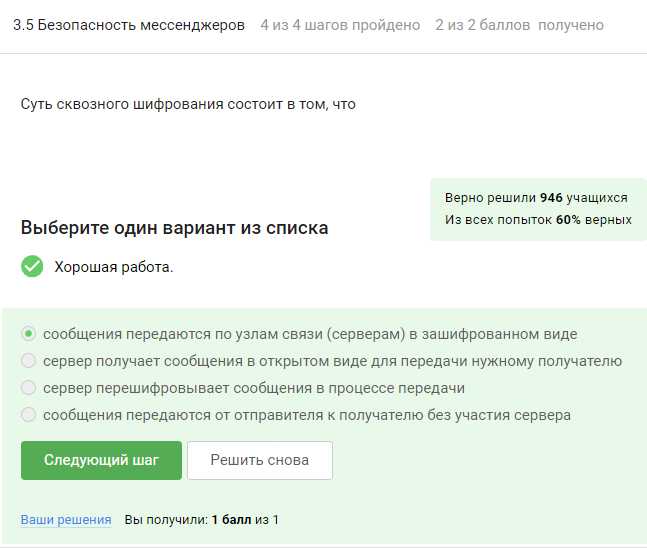


Figure 37: Сквозное шифрование

# 5 Криптография на практике

* 1. Введение в криптографию.

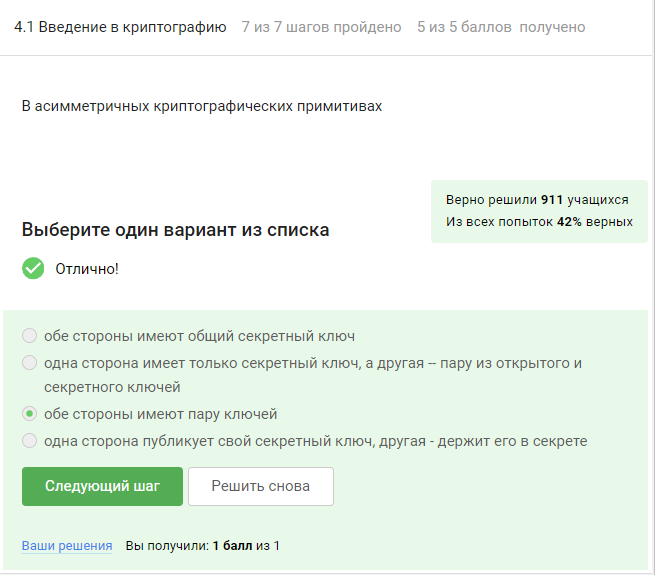


Figure 38: Криптографические примитивы

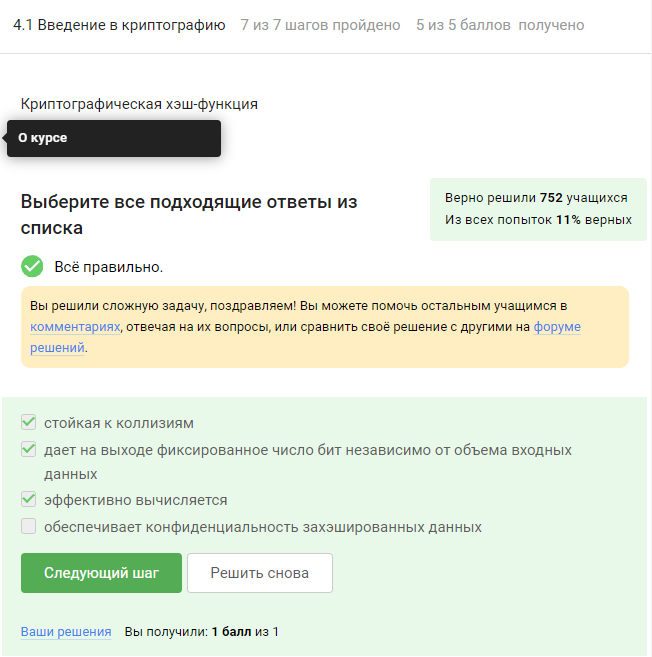


Figure 39: Криптографическая хэш-функция

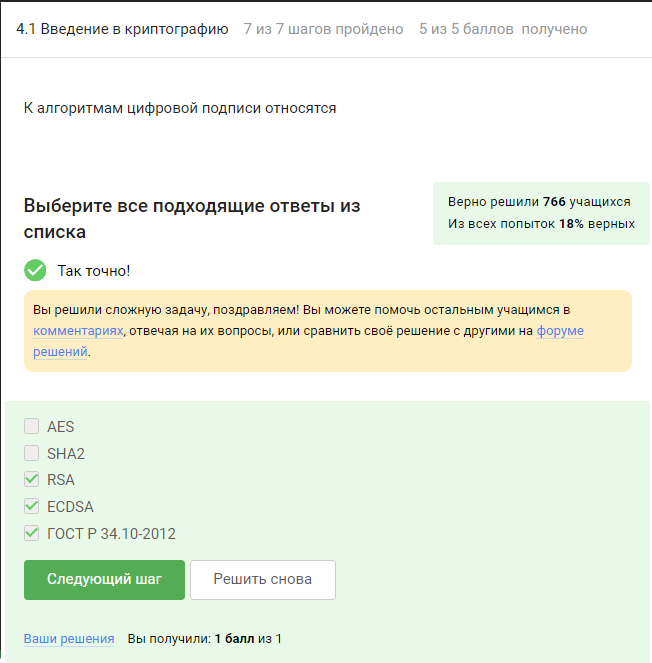


Figure 40: Цифровые подписи

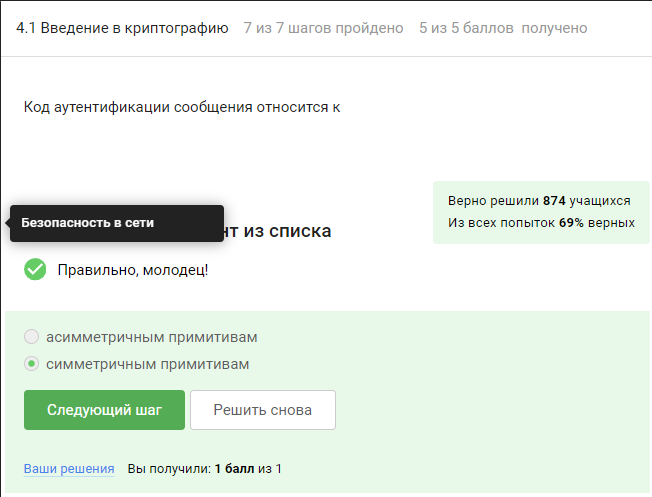


Figure 41: Аутентификация сообщения

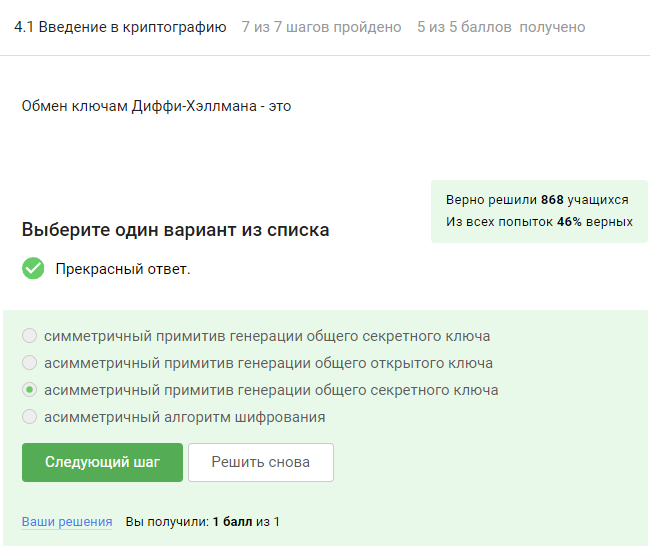


Figure 42: Обмен ключам

* 1. Цифровая подпись.

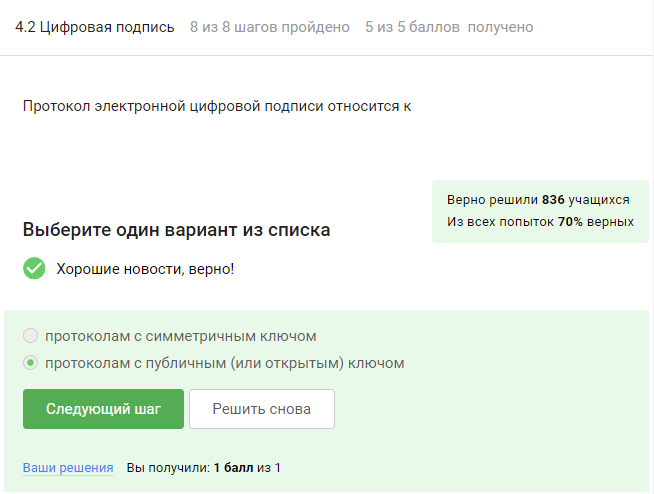


Figure 43: Протокол электронной подписи

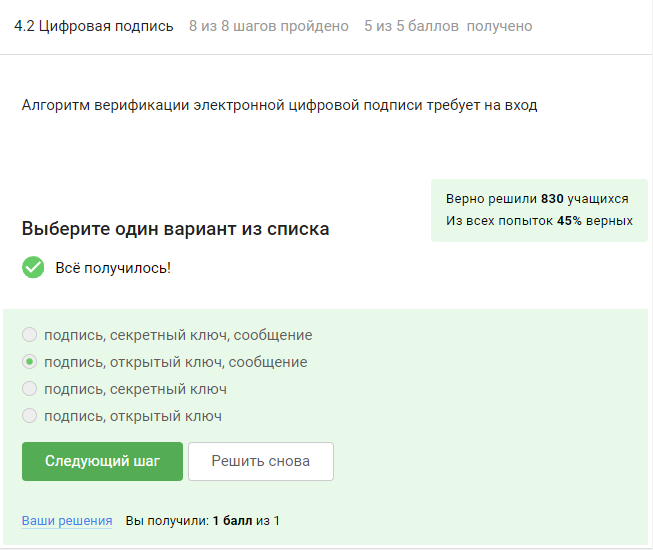


Figure 44: Алгоритм верификации

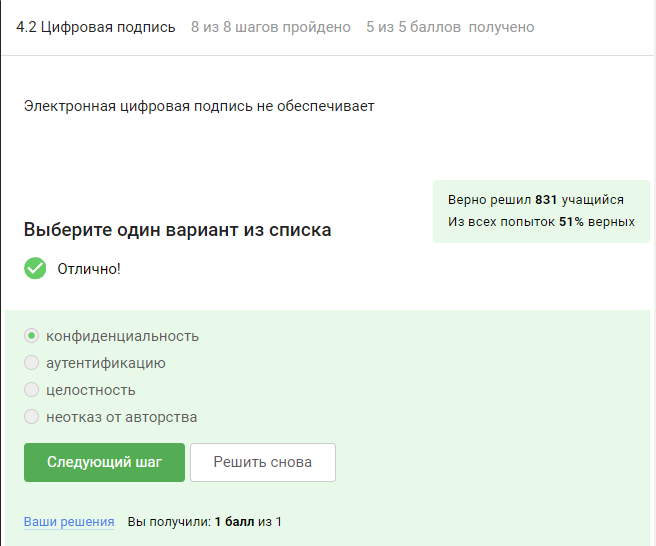


Figure 45: Электронная подпись

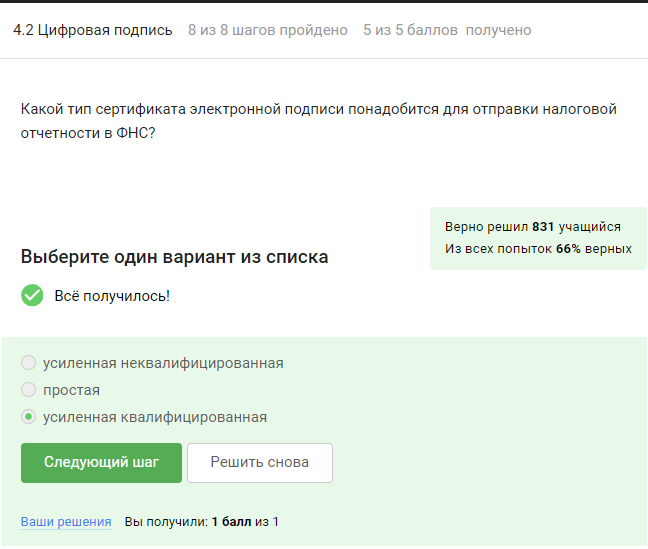


Figure 46: ФНС

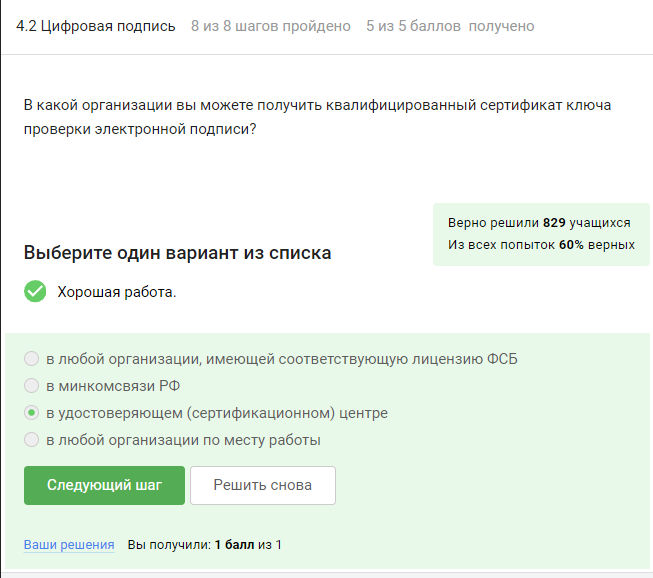


Figure 47: Сертификат ключа

* 1. Электронные платежи.

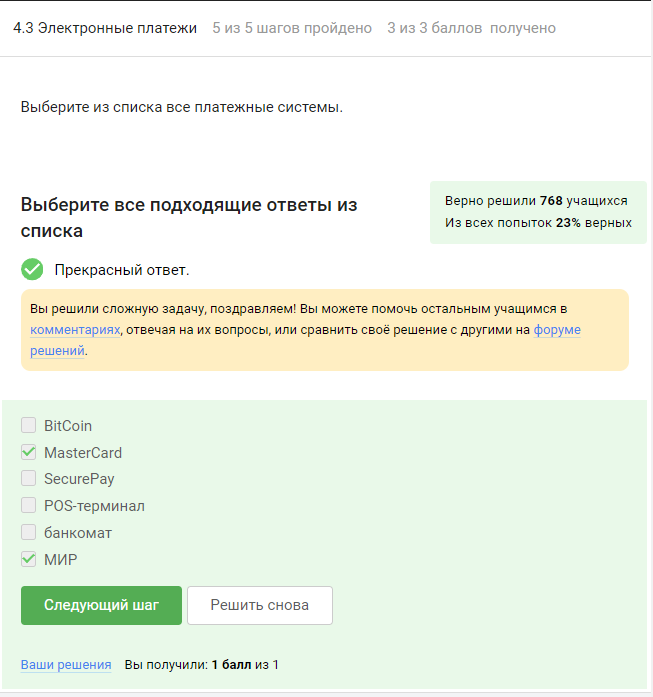


Figure 48: Платежные системы

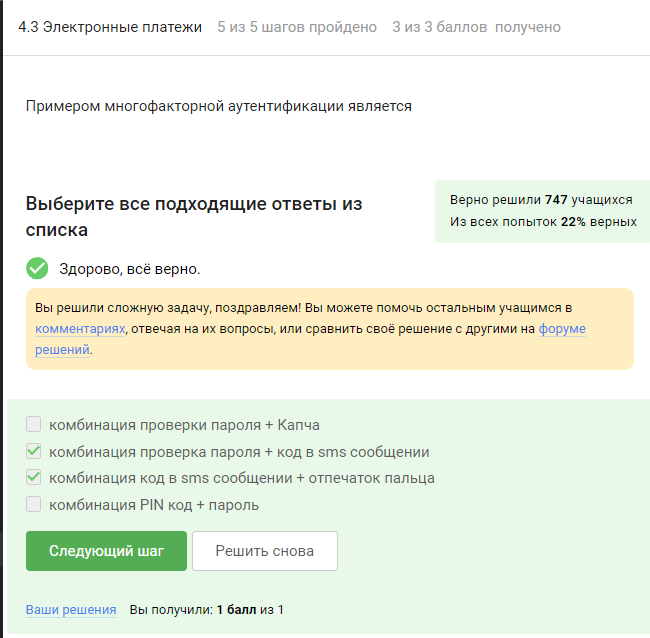


Figure 49: Многофакторная аутентификация

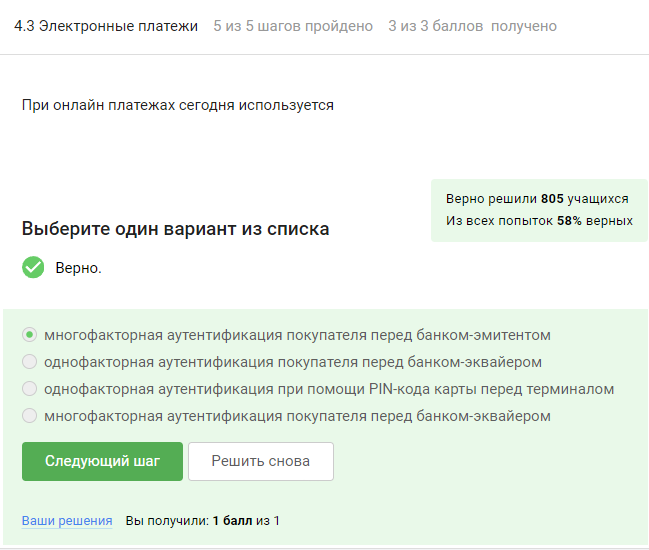


Figure 50: Онлайн платежи

* 1. Блокчейн.

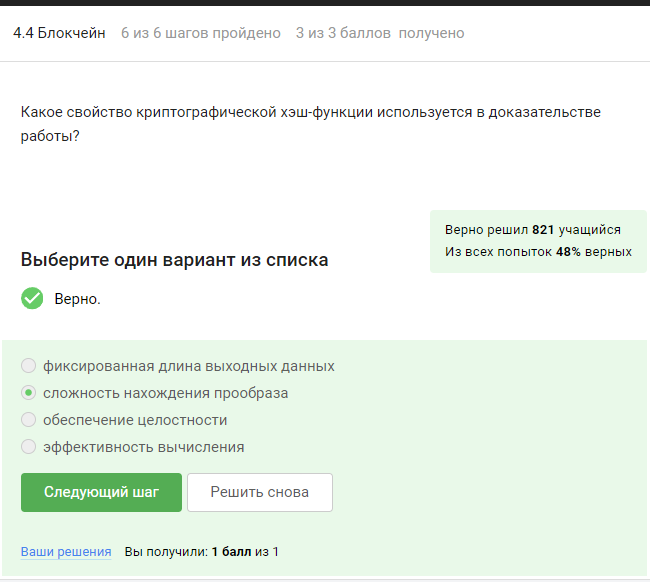


Figure 51: Криптографическая хэш-функция

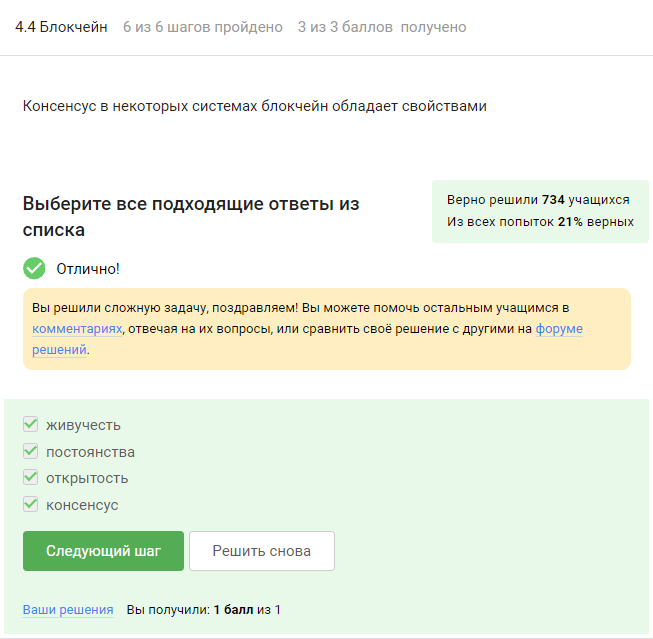


Figure 52: Консенсус в некоторых системах

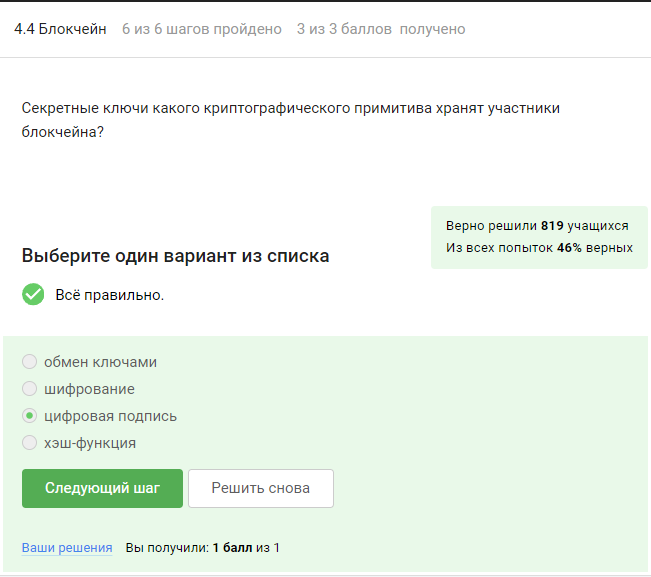


Figure 53: Секретные ключи

# 6 Выводы

Сертификат не выдается.

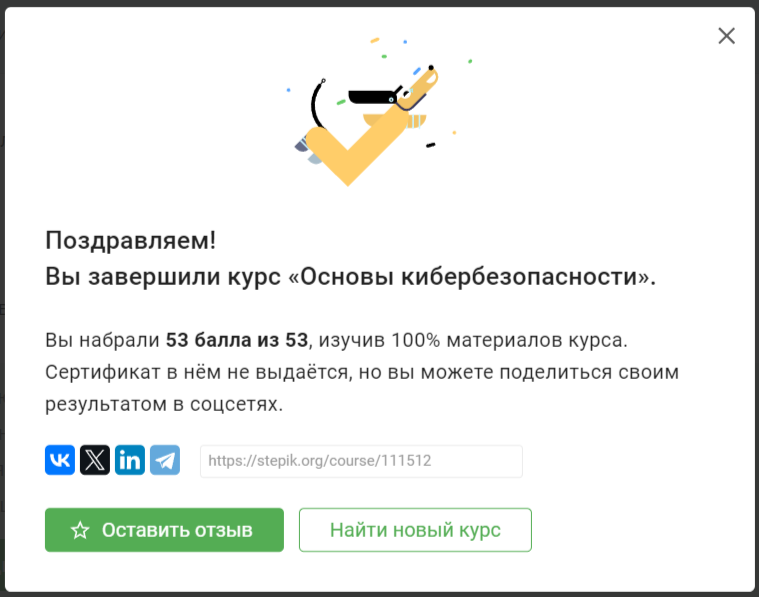


Figure 54: Окончание курса