Внешний курс

Основы кибербезопасности

Бекназарова Виктория Тиграновна

Содержание

1	Цель работы	6
2	Прохождение курса	7
3	Цифровая подпись	47
4	Электронные платежи	52
5	Блокчейн	55
6	Выводы	58

Список иллюстраций

2.1	Протокол прикладного уровня	7
2.2	Протокол ТСР	8
2.3	Адреса IPv-4	9
2.4	DNS сервер	10
2.5	Протокол в модели TCP/IP	11
2.6	Протокол htpl	12
2.7	Протокол https	13
2.8	Протокол TLS	14
2.9	Протокол TLS	15
2.10	Куки хранят	16
	Куки не используются	17
	Куки генерируются	18
2.13	Сессионные куки	19
2.14	Промежуточные узлы TOR	20
2.15	Браузер TOR	21
2.16	Секретный ключ	22
2.17	Браузер TOR	23
2.18	Wi-Fi	24
2.19	Протокол Wi-Fi	25
2.20	Шифрование Wi-Fi	26
2.21	Загрузочный сектор диска	27
2.22	Шифрование диска	28
2.23	Жесткий диск	29
2.24	Пароли	30
	Хранение паролей	31
2.26	Капча	32
2.27	Хэширование паролей	33
2.28	Стойкость паролей	34
2.29	Меры защиты паролей	35
	Фишинговые ссылки	36
2.31	Фишинговый имейл	37
	Спуфинг	38
2.33	Вирус-троян	39
2.34	Mecceнджер Signal	40
2.35	Сквозное шифрование	41
	Криптографические примитивы	42
	Клиптографицеская уаш-функция	17

2.38	Цифровые подписи								•	44
2.39	Аутентификация сообщения									45
	Обмен ключам									46
3.1	Протокол электронной подписи									47
3.2	Алгоритм верификации									48
3.3	Электронная подпись									49
3.4	ФНС									50
3.5										51
4.1	Платежные системы							•		52
4.2	Многофакторная аутентификация .									53
4.3										54
5.1	Криптографическая хэш-функция .							•		55
5.2	Консенсус в некоторых системах									
5.3	Секретные ключи									

Список таблиц

1 Цель работы

Изучить основы кибербезопасности

2 Прохождение курса

- 1. Введение в курс #Безопасность в сети
- 2. 1.Как работает интернет:базовые сетевые протоколы.

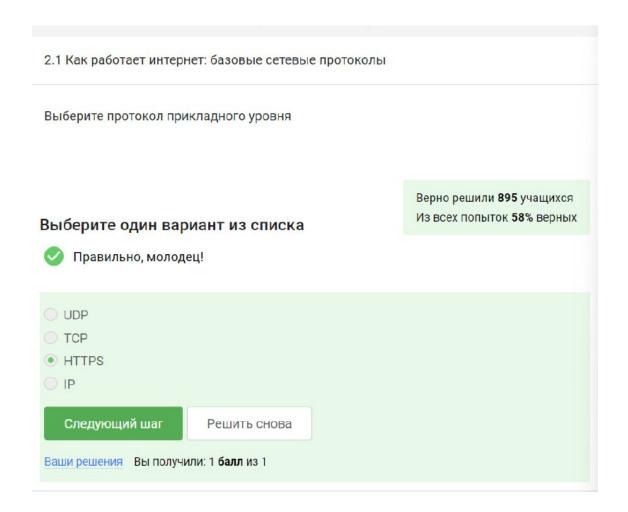


Рис. 2.1: Протокол прикладного уровня

Рис. 2.2: Протокол ТСР

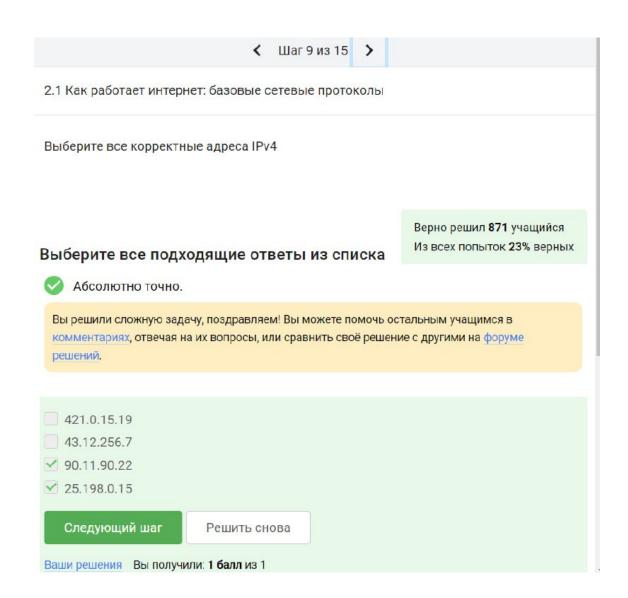


Рис. 2.3: Адреса IPv-4

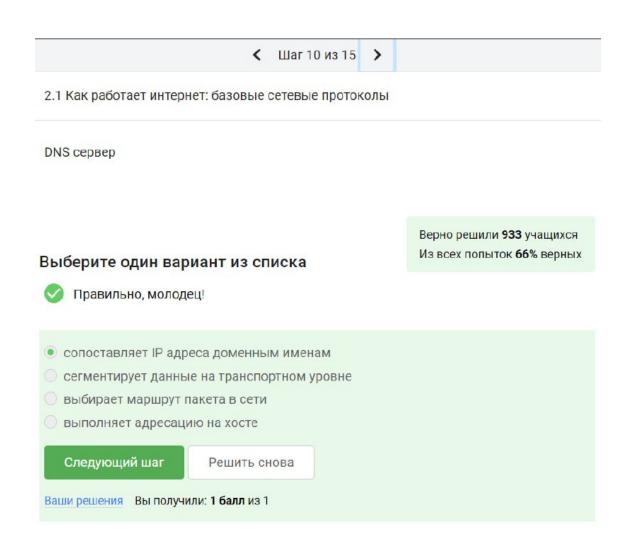


Рис. 2.4: DNS сервер

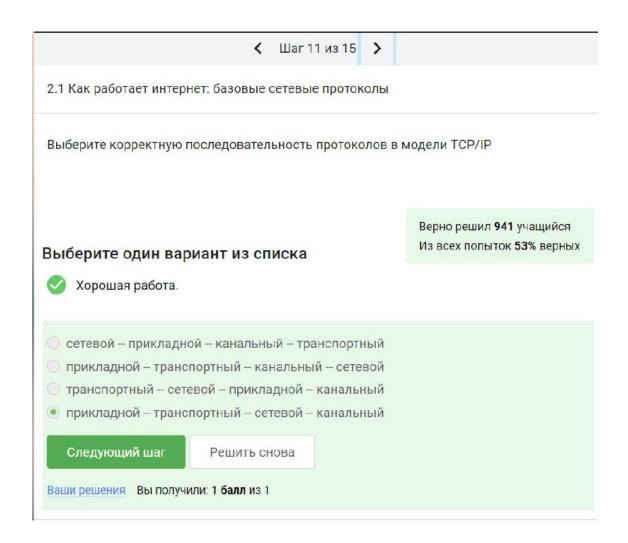


Рис. 2.5: Протокол в модели ТСР/ІР

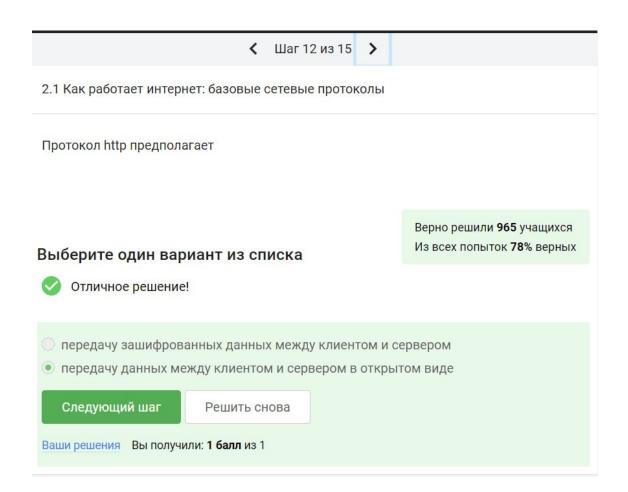


Рис. 2.6: Протокол htpl

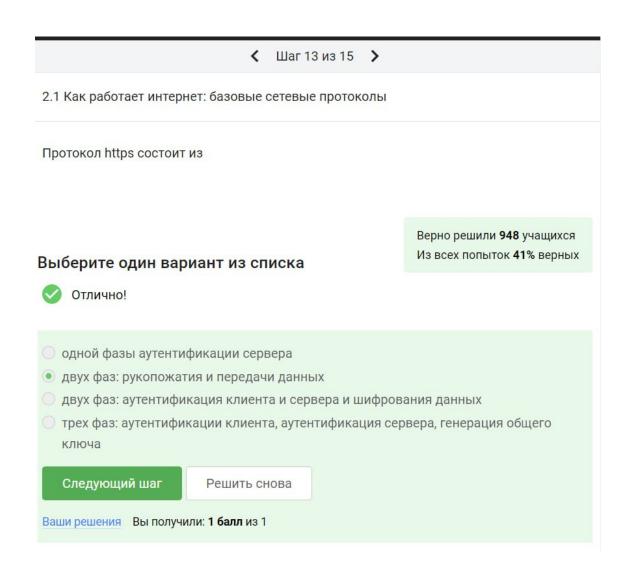


Рис. 2.7: Протокол https

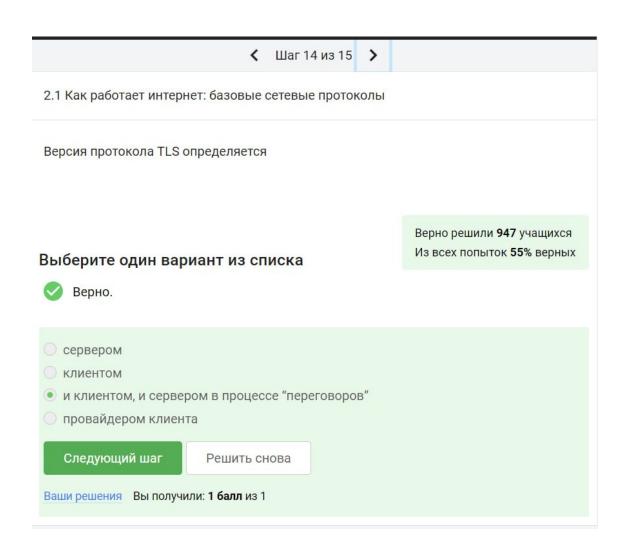


Рис. 2.8: Протокол TLS

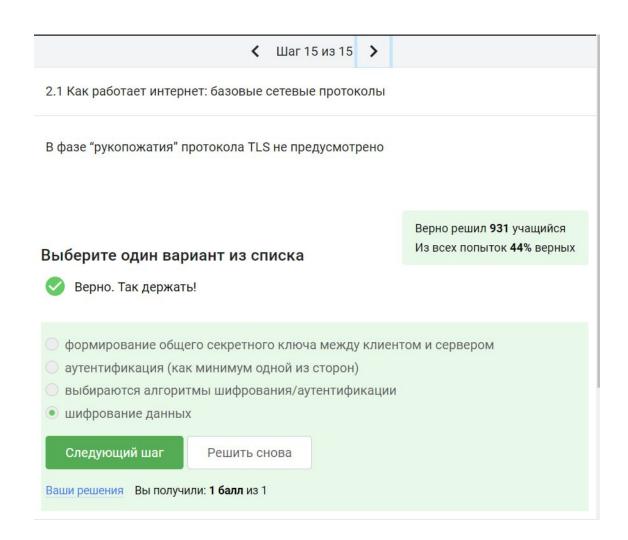


Рис. 2.9: Протокол TLS

#Персонализация сети.

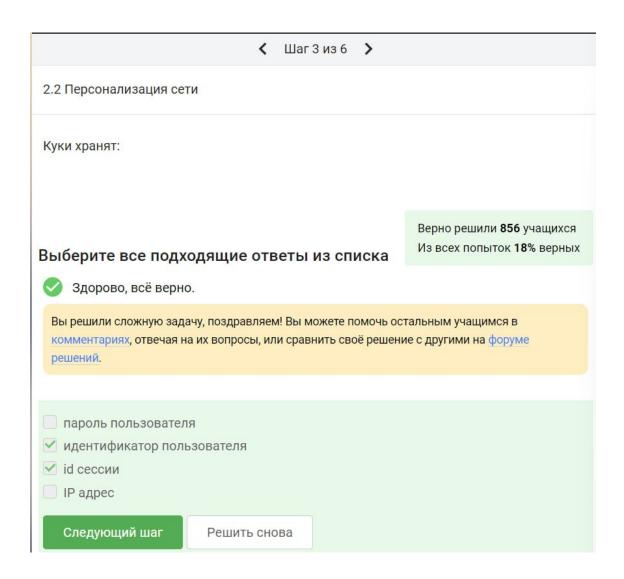


Рис. 2.10: Куки хранят

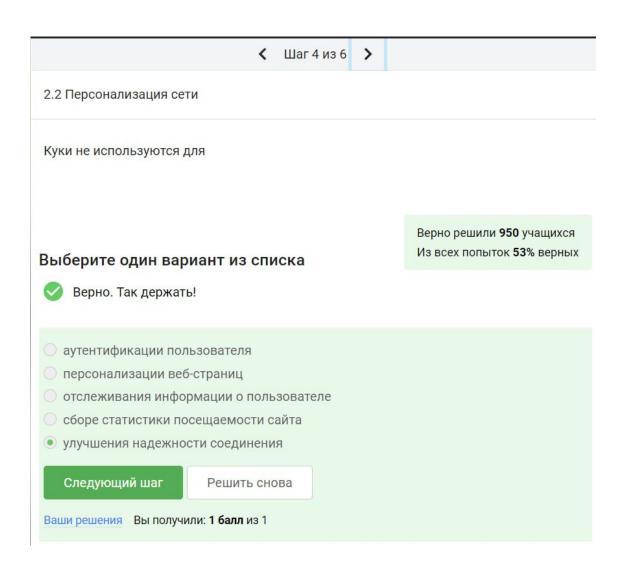


Рис. 2.11: Куки не используются

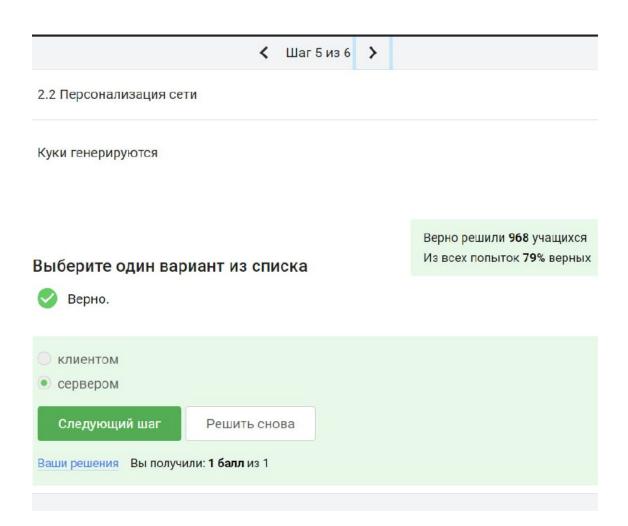


Рис. 2.12: Куки генерируются

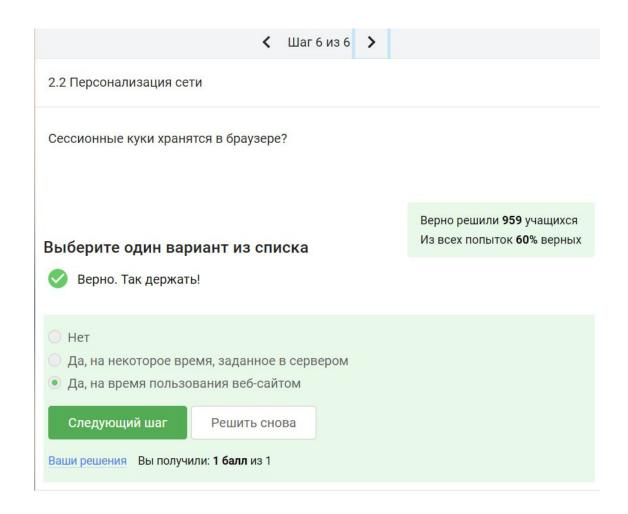


Рис. 2.13: Сессионные куки

#Браузер TOR. Анимация.

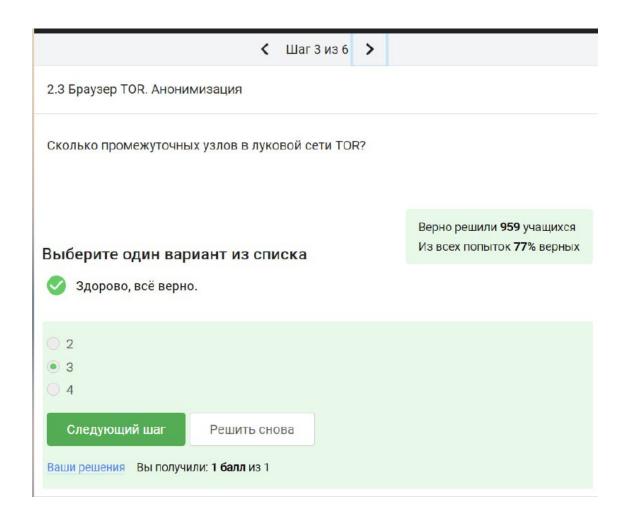


Рис. 2.14: Промежуточные узлы TOR

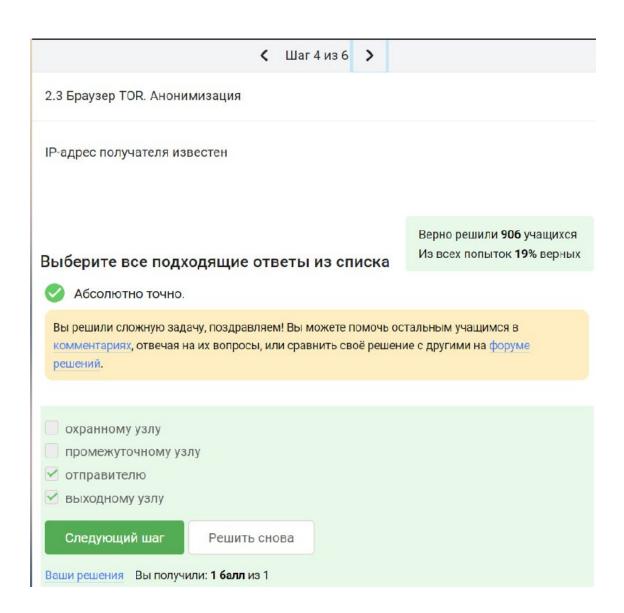


Рис. 2.15: Браузер TOR

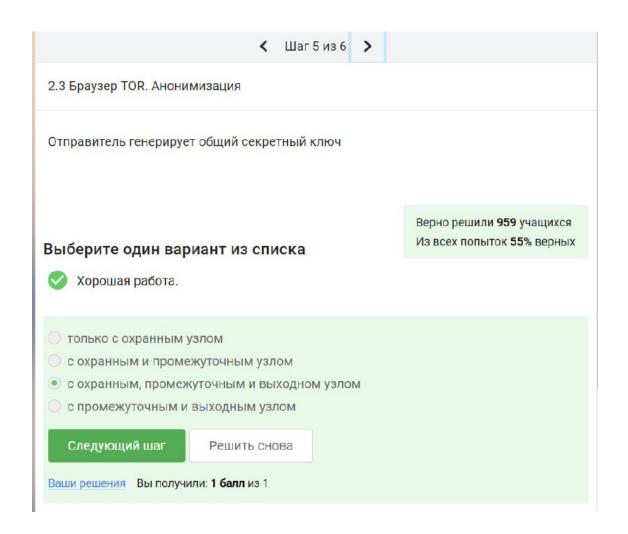


Рис. 2.16: Секретный ключ

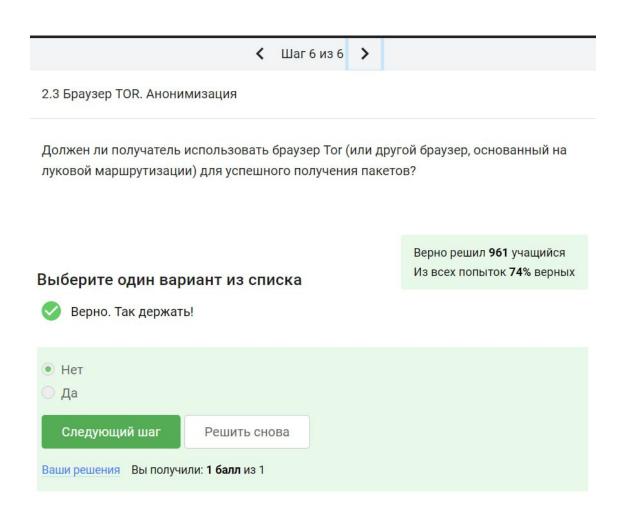


Рис. 2.17: Браузер TOR

#Беспроводные сети. Wi-Fi

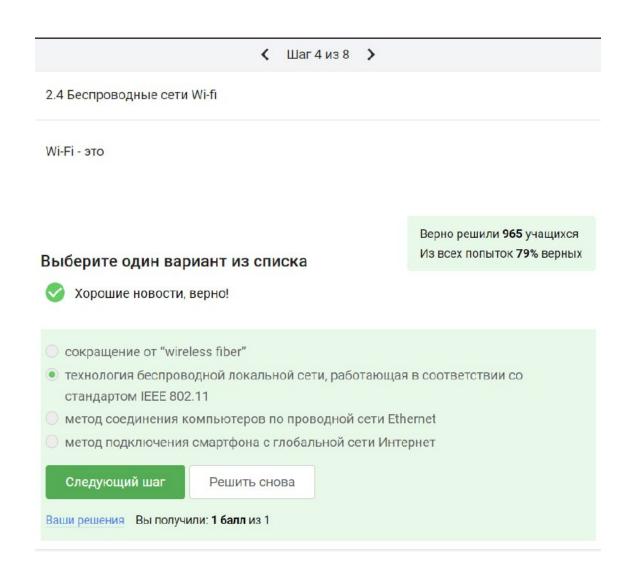


Рис. 2.18: Wi-Fi

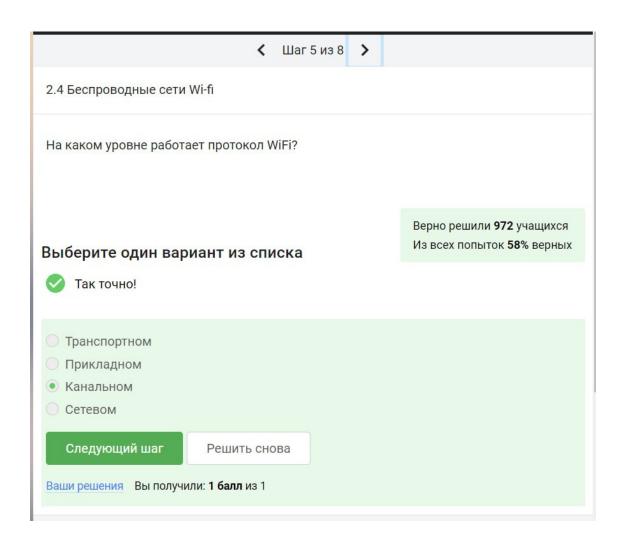


Рис. 2.19: Протокол Wi-Fi

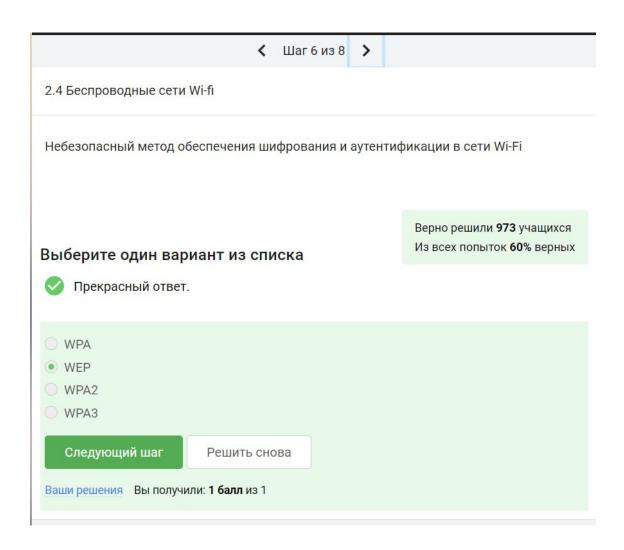


Рис. 2.20: Шифрование Wi-Fi

#3.Защита ПК/телефона #Шифрование диска

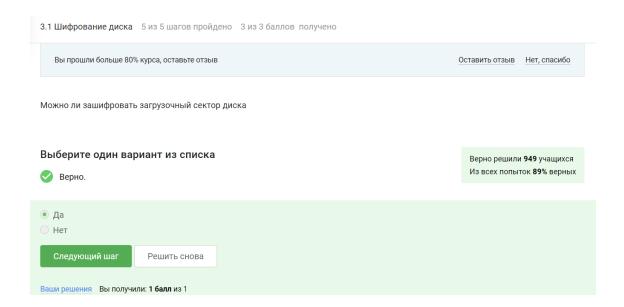


Рис. 2.21: Загрузочный сектор диска

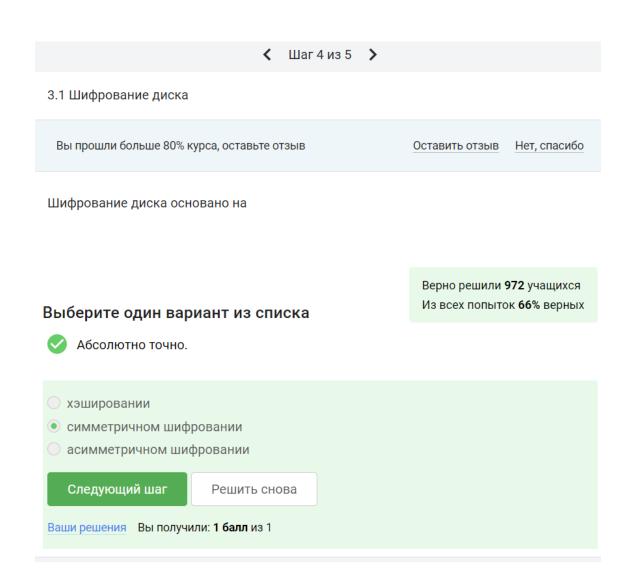


Рис. 2.22: Шифрование диска

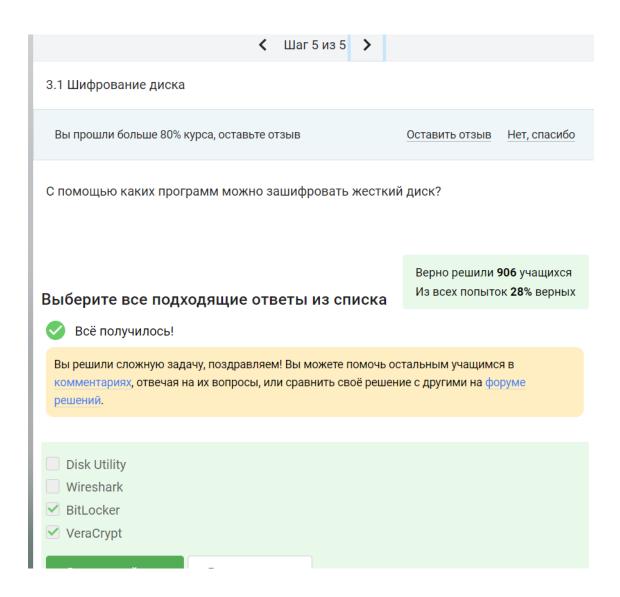


Рис. 2.23: Жесткий диск

#Пароли

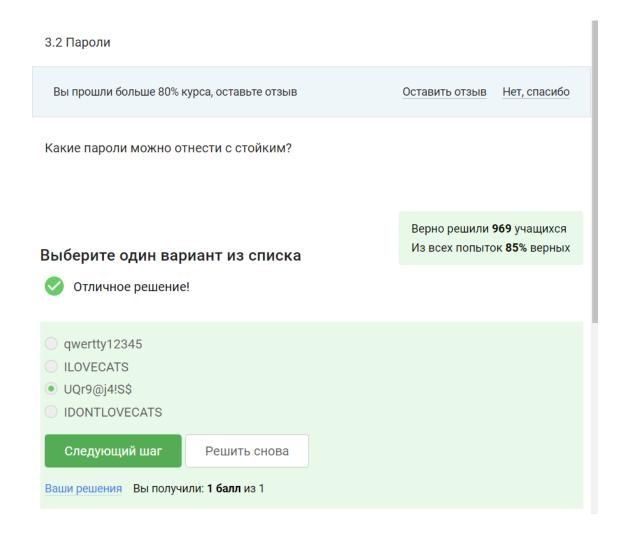


Рис. 2.24: Пароли

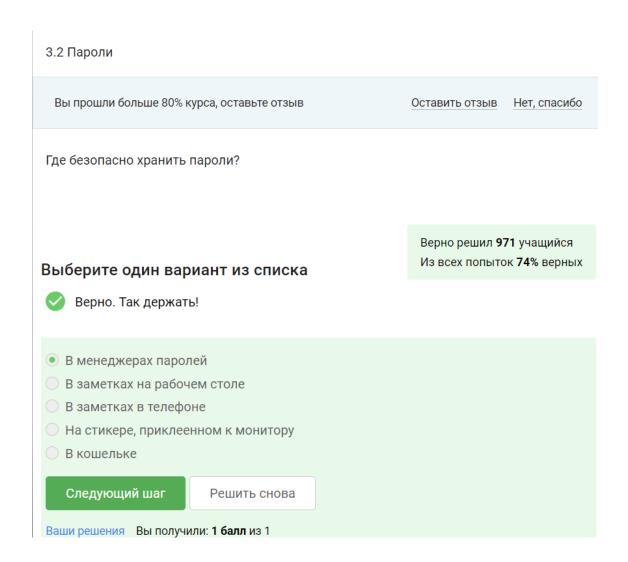


Рис. 2.25: Хранение паролей

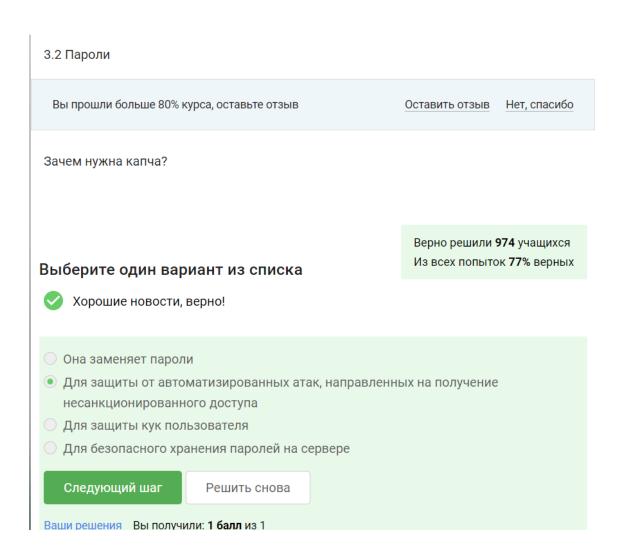


Рис. 2.26: Капча

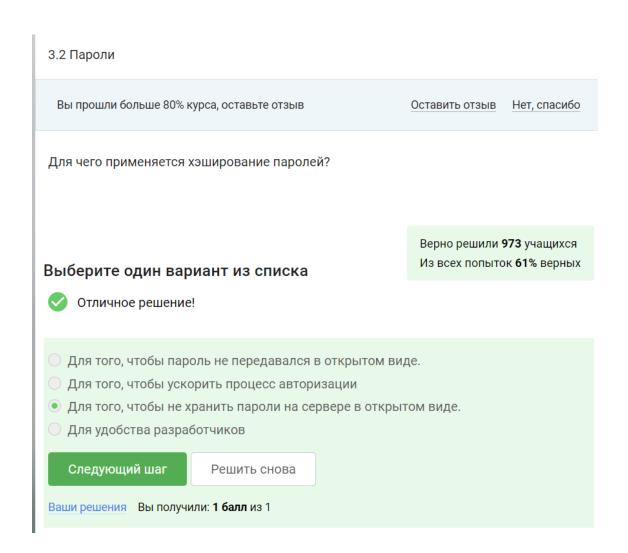


Рис. 2.27: Хэширование паролей



Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу?

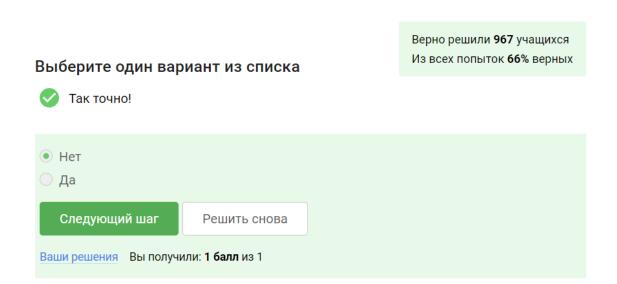


Рис. 2.28: Стойкость паролей

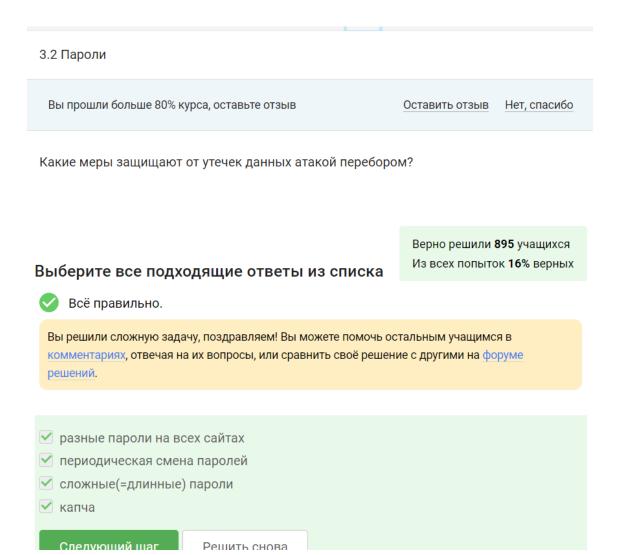


Рис. 2.29: Меры защиты паролей

#Фишинг

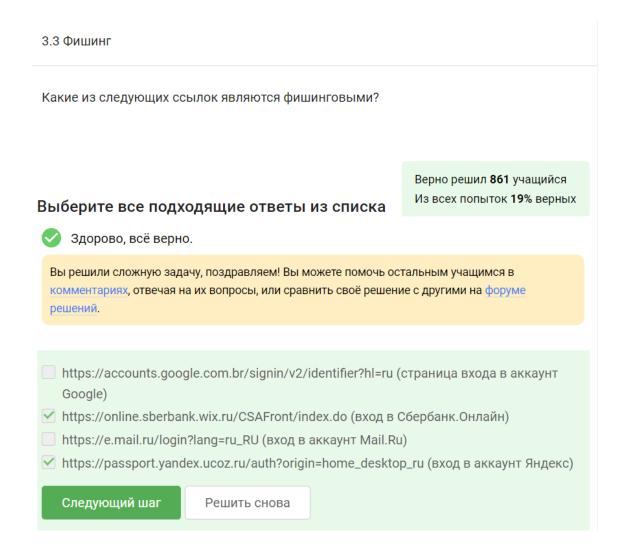


Рис. 2.30: Фишинговые ссылки

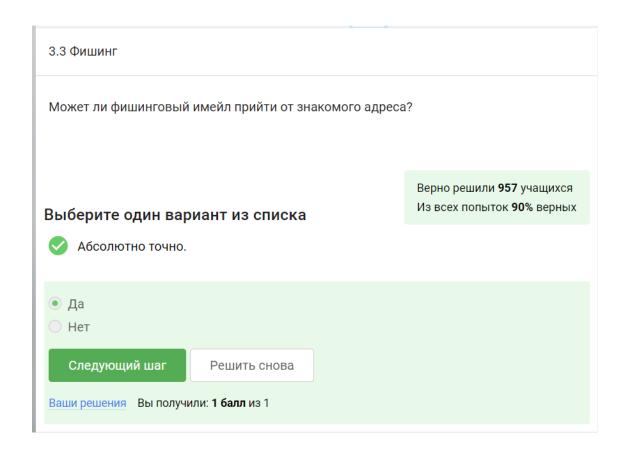


Рис. 2.31: Фишинговый имейл

#Вирусы.Примеры

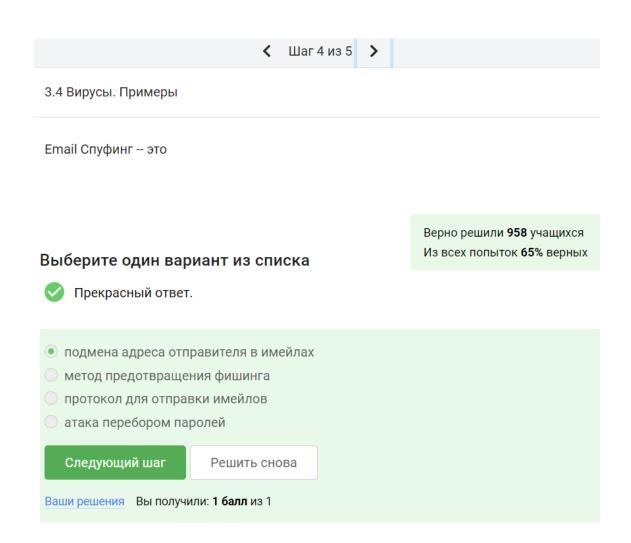


Рис. 2.32: Спуфинг

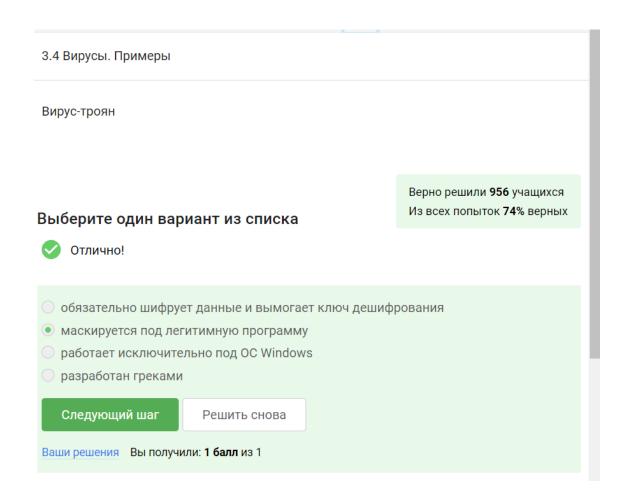


Рис. 2.33: Вирус-троян

#Безопасность мессенджеров

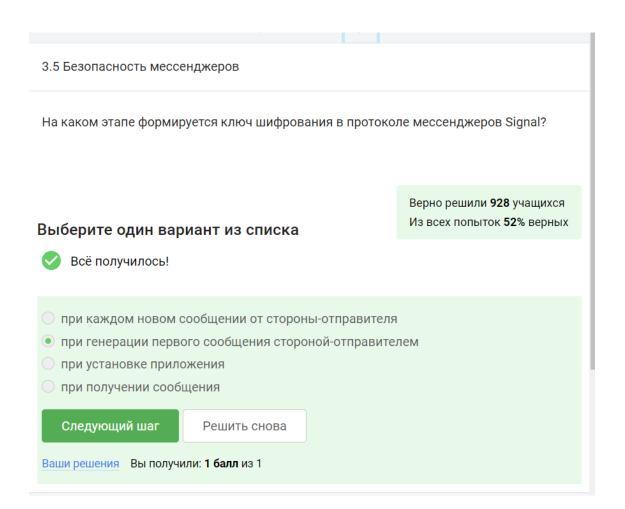


Рис. 2.34: Мессенджер Signal

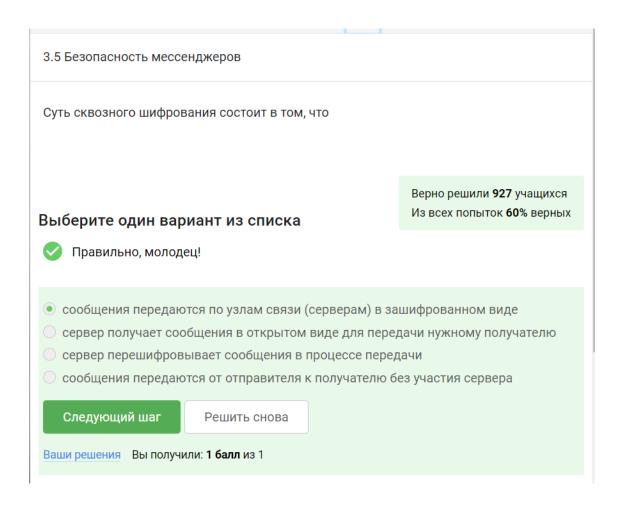


Рис. 2.35: Сквозное шифрование

#4.Криптография на практике # ВВедение в криптографию

В асимметричных криптографических примитивах

Верно решили **892** учащихся Из всех попыток **42**% верных

Выберите один вариант из списка



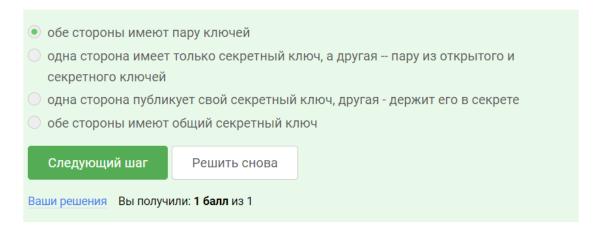


Рис. 2.36: Криптографические примитивы

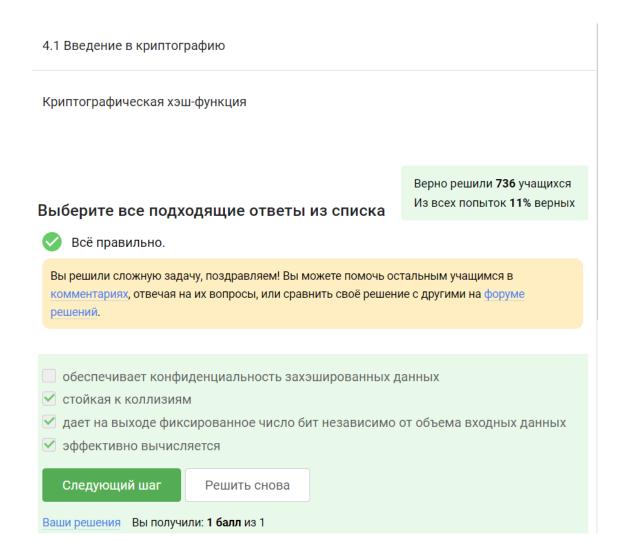


Рис. 2.37: Криптографическая хэш-функция

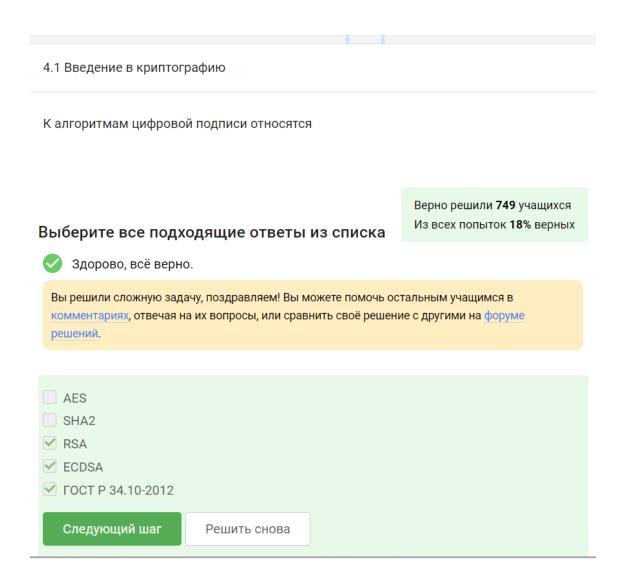


Рис. 2.38: Цифровые подписи

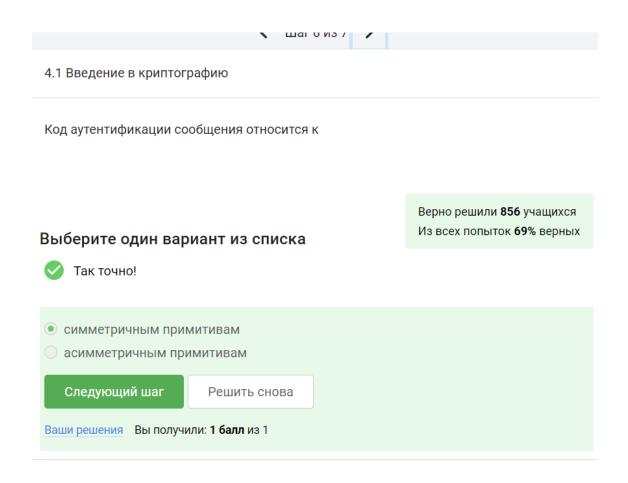


Рис. 2.39: Аутентификация сообщения

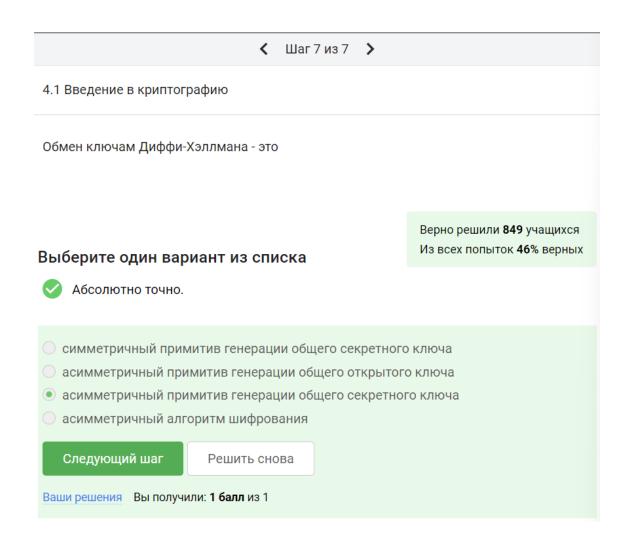


Рис. 2.40: Обмен ключам

3 Цифровая подпись

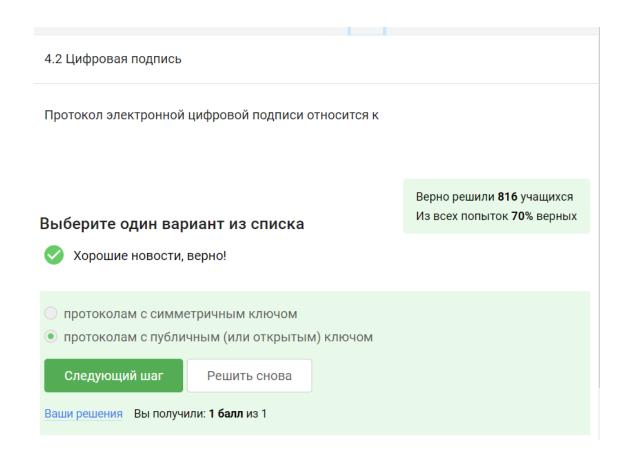


Рис. 3.1: Протокол электронной подписи

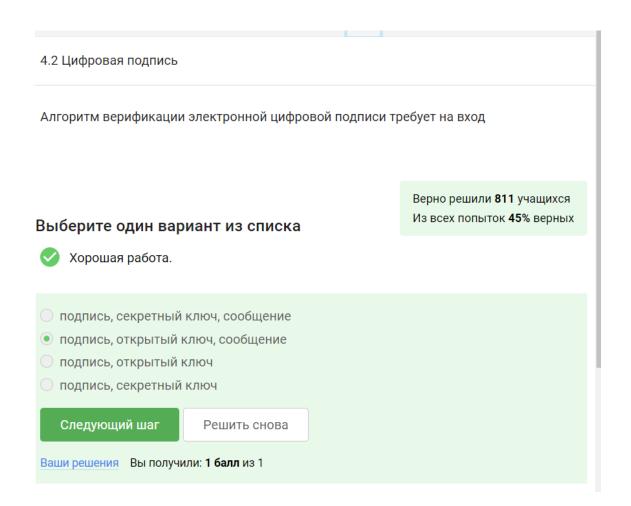


Рис. 3.2: Алгоритм верификации

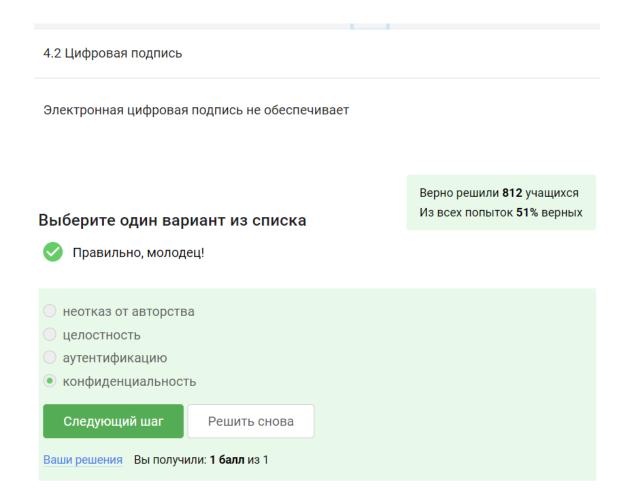


Рис. 3.3: Электронная подпись

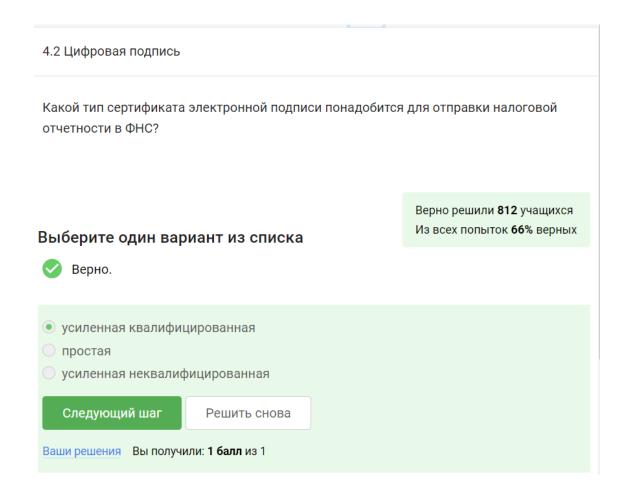


Рис. 3.4: ФНС

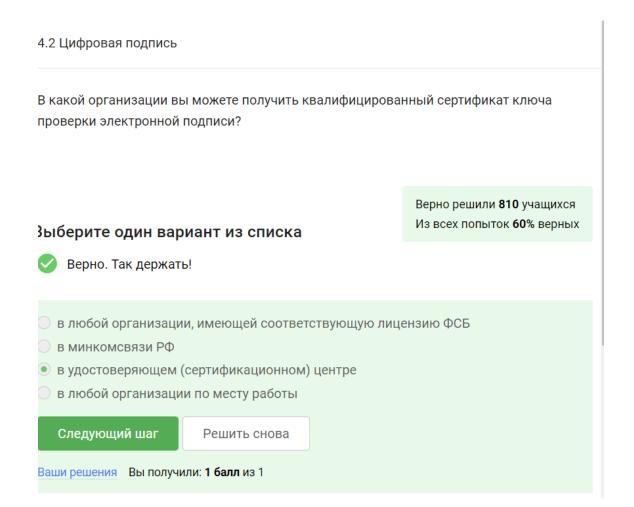


Рис. 3.5: Сертификат ключа

4 Электронные платежи

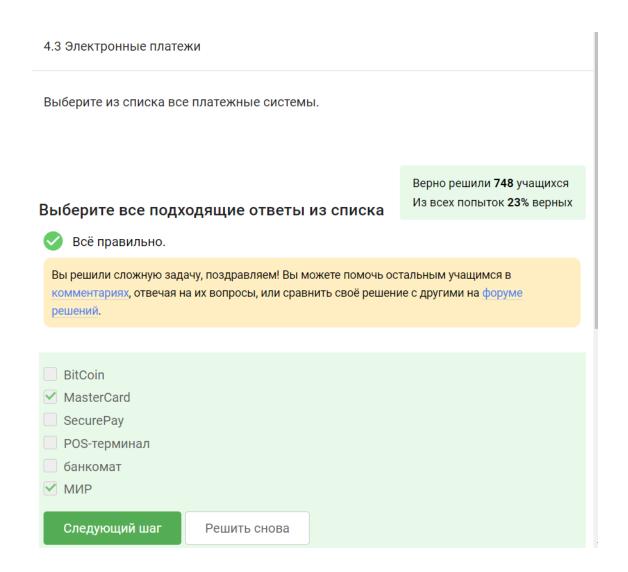


Рис. 4.1: Платежные системы

Примером многофакторной аутентификации является

Верно решили **728** учащихся Из всех попыток **22**% верных

Выберите все подходящие ответы из списка

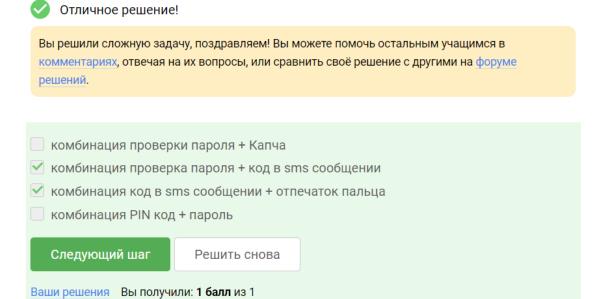


Рис. 4.2: Многофакторная аутентификация

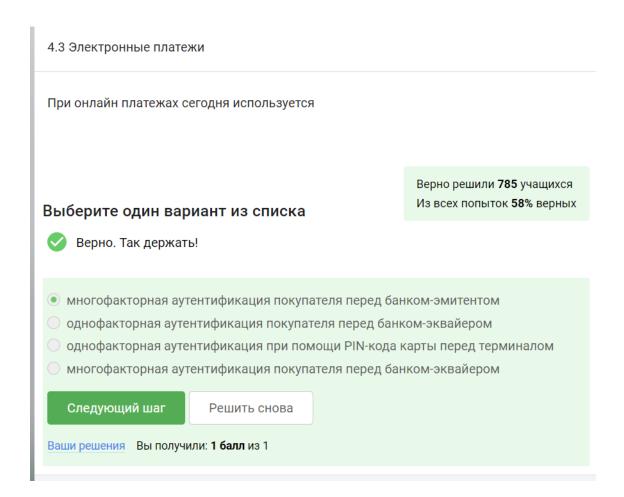


Рис. 4.3: Онлайн платежи

5 Блокчейн

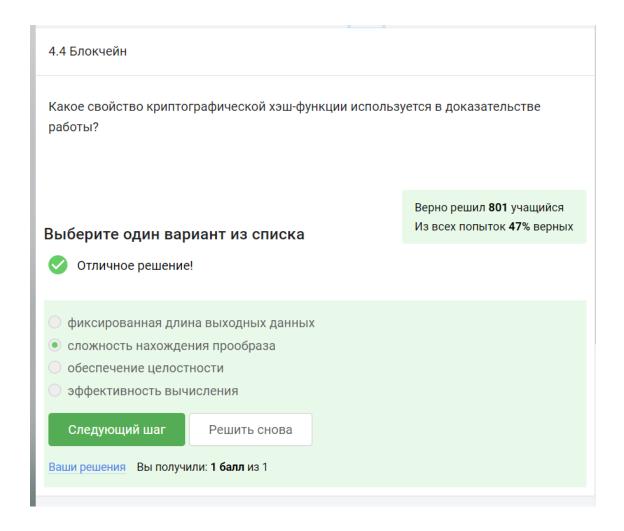


Рис. 5.1: Криптографическая хэш-функция

Консенсус в некоторых системах блокчейн обладает свойствами

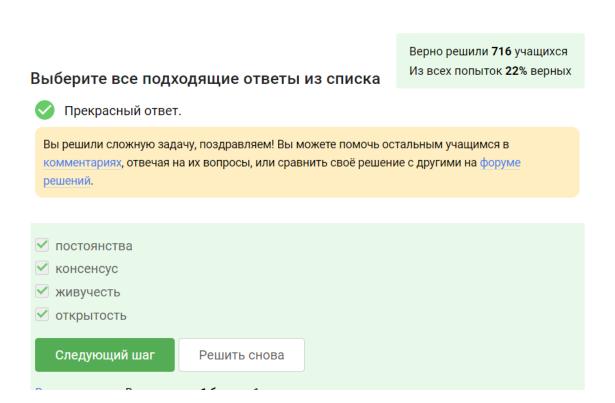


Рис. 5.2: Консенсус в некоторых системах

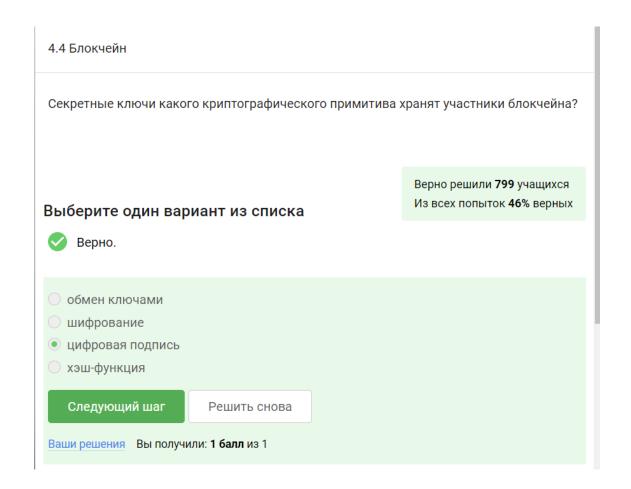
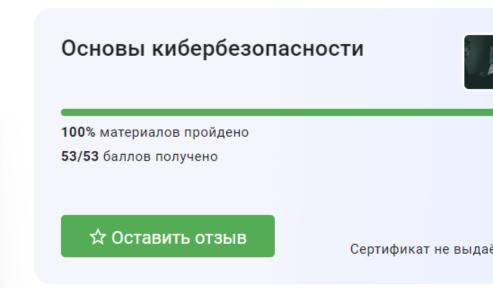


Рис. 5.3: Секретные ключи

6 Выводы

Моё обучение



Сертификат не выдается.