#### Этап 3

## Внешний проект

Улитина М.М.

17 мая 2025

Российский университет дружбы народов, Москва, Россия



#### Докладчик

```
::::::::::: {.columns align=center} ::: {.column width="70%"}
```

- Улитина Мария Максимовна
- студентка

Выполнение второго этапа

внешнего курса

#### Имеют пару ключей

В асимметричных криптографических примитивах

#### Выберите один вариант из списка

- Отлично!
- обе стороны имеют пару ключей
- одна сторона публикует свой секретный ключ, другая держит его в секрете
- 🔘 одна сторона имеет только секретный ключ, а другая пару из открытого и секретного ключей
- 🔾 обе стороны имеют общий секретный ключ

Следующий шаг

#### Свойсва хэш-функции

Криптографическая хэш-функция Выберите все подходящие ответы из списка Хорошая работа. Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить своё решение с другими на форуме решений. стойкая к коллизиям обеспечивает конфиденциальность захэшированных данных эффективно вычисляется Дает на выходе фиксированное число бит независимо от объема входных данных Следующий шаг Решить снова Ваши решения Вы получили: 1 балл

## Алгоритмы цифровой функции

К алгоритмам цифровой подписи относятся

#### Выберите все подходящие ответы из списка



Правильно, молодец!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить своё решение с другими на форуме решений.

- AES
- SHA2
- ✓ RSA
- ECDSA
- ✓ ГОСТ Р 34.10-2012

Следующий шаг

#### Код аутентификации

Код аутентификации сообщения относится к

# Выберите один вариант из списка

Всё правильно.

асимметричным примитивам

• симметричным примитивам

Следующий шаг

Решить снова

## Ключи Диффи-хеллмэна

Обмен ключам Диффи-Хэллмана - это

## Выберите один вариант из списка



- 🔘 симметричный примитив генерации общего секретного ключа
- 🔾 асимметричный примитив генерации общего открытого ключа
- асимметричный примитив генерации общего секретного ключа
- асимметричный алгоритм шифрования

Следующий шаг

Решить снова

#### Электронная цифровая подпись

Протокол электронной цифровой подписи относится к

# Выберите один вариант из списка

🗸 Хорошая работа.

протоколам с симметричным ключом

• протоколам с публичным (или открытым) ключом

Следующий шаг

Решить снова

#### Алгоритм верификации

Алгоритм верификации электронной цифровой подписи требует на вход

#### Выберите один вариант из списка



- подпись, открытый ключ
- подпись, открытый ключ, сообщение
- подпись, секретный ключ
- 🔵 подпись, секретный ключ, сообщение

Следующий шаг

Решить снова

#### Не обеспечивает конфиденциальность

Электронная цифровая подпись не обеспечивает

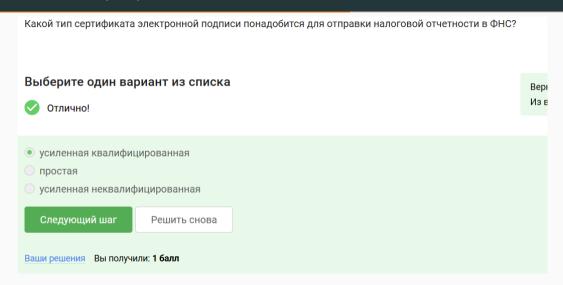
#### Выберите один вариант из списка



- конфиденциальность
- аутентификацию
- целостность
- неотказ от авторства

Следующий шаг

#### Усиленная квалифицированная



#### Организация

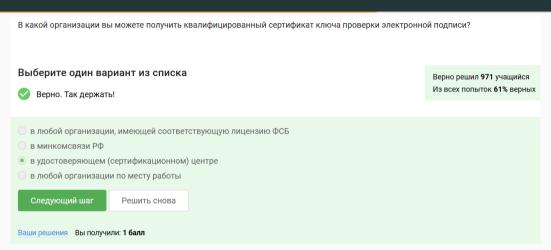
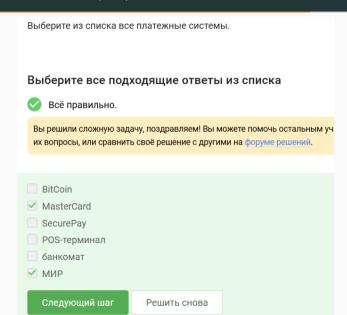


Рис. 10: организация

#### Платежные системы МИР и Мастер Кард



#### МФ аутентификация

Примером многофакторной аутентификации является Выберите все подходящие ответы из списка Прекрасный ответ. Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая н их вопросы, или сравнить своё решение с другими на форуме решений. комбинация проверки пароля + Капча ✓ комбинация проверка пароля + код в sms сообщении ✓ комбинация код в sms сообщении + отпечаток пальца комбинация PIN код + пароль Следующий шаг Решить снова

#### Где используется мфа

При онлайн платежах сегодня используется

## Выберите один вариант из списка

- Всё получилось!
- многофакторная аутентификация покупателя перед банком-эмитентом
- однофакторная аутентификация покупателя перед банком-эквайером
- O однофакторная аутентификация при помощи PIN-кода карты перед терминалом
- 🔘 многофакторная аутентификация покупателя перед банком-эквайером

Следующий шаг

#### Сложность нахождения прообраза

Какое свойство криптографической хэш-функции используется в доказательстве работы?

#### Выберите один вариант из списка



- фиксированная длина выходных данных
- сложность нахождения прообраза
- обеспечение целостности
- эффективность вычисления

Следующий шаг Решить снова

#### консенсус

Консенсус в некоторых системах блокчейн обладает свойствами

#### Выберите все подходящие ответы из списка



Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить своё решение с другими на форуме решений.

- ✓ консенсус
- постоянства
- ✓ живучесть
- открытость

Следующий шаг

## Выводы

Выволнен третий этап.