# Прохождения внешнего курса на тему Основы кибербезопасности.

Часть 3

Основы информационной безопасности

Просина К. М.

17 май 2025

Российский университет дружбы народов, Москва, Россия

Информация

#### Докладчик

- Просина Ксения Максимовна
- студент 2 курса
- факультет физико-математических и естественных наук
- Российский университет дружбы народов
- 1132231938@rudn.ru

# 4 Криптография на практике

#### Вопрос/Ответ 1

В асимметричных криптографических примитивах

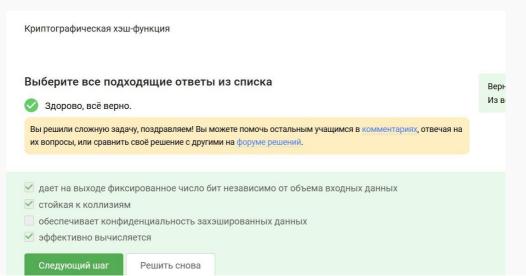
### Выберите один вариант из списка

- Абсолютно точно.
- 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

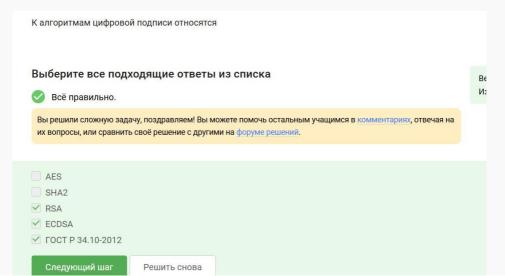
Решить снова

Пояснение ответа: В асимметричных криптографических примитивах обе стороны имеют пару ключей, у каждого из сторон есть пара ключей: открытый ключ и секретный ключ. Открытый ключ публикуется в открытом доступе, а закрытый или секретный сторона хранит у себя.



Пояснение ответа: Криптографическая хэш-функция:

- Дает на выходк фиксированное число бит независимо от объема входных данных
- Стойкая к коллизиям
- Эффективно вычисляется

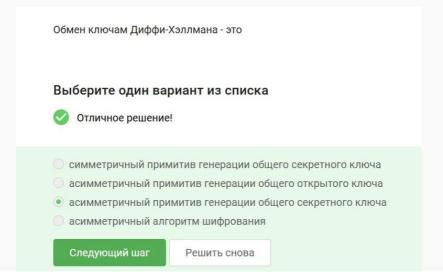




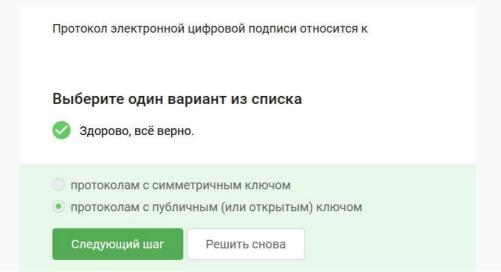
Пояснение ответа: К алгоритмам цифровой подписи относятся: RSA, ECDSA, ГОСТ 34.10-2012



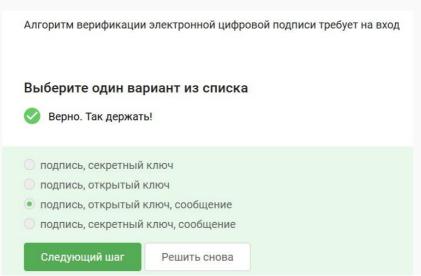
Пояснение ответа: Код аутентификации сообщения относится к симметричным примитивам, так как имеется общий ключ.



Пояснение ответа: Обмен ключами Диффи-Хэллмана-это асимметричный примитив генерации общего секретного ключа.

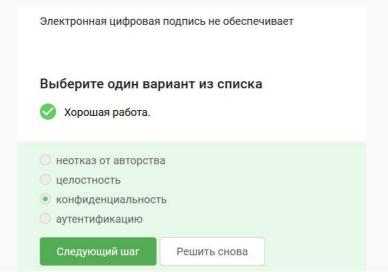


Пояснение ответа: Протокол электронной цифровой подписи относится протоколам с публичным (или открытым) ключом.



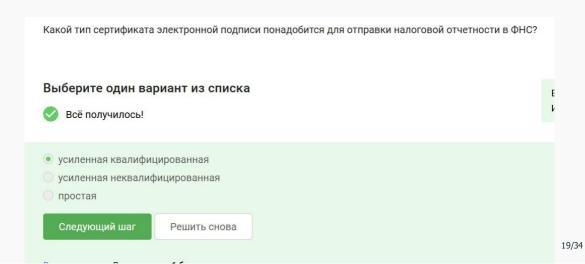
Пояснение ответа: Алгоритм верификации электронной цифровой подписи требует на вход:

- подпись
- открытый ключ
- сообщение



Пояснение ответа: Цифровая подпись предназначена для:

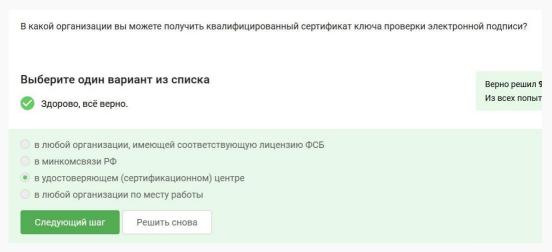
- Обеспечение целостности сообщения (любое изменение сообщения будет обнаружено)
- Аутентификации сообщения(устанавливается принадлежность подписи владельцу)
- Неотказ от авторства (невозможно отказаться от факта подписи в будущем)



Пояснение ответа: Усиленной квалификацированной:

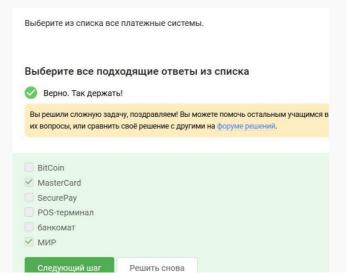
- равнозначно рукописей
- подтверждается сертификатом, выпущенным организацией, аккредитованной минкомсвязи РФ
- госуслуги, государственный документооборот

#### Вопрос/Ответ 5

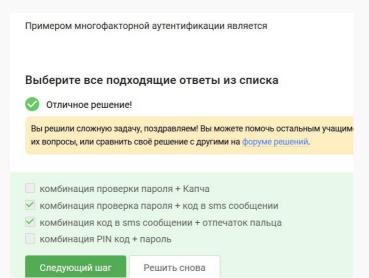


21/34

Пояснение ответа: В удостоверяющем(сертифиционном) центре можно получить квалифицированный сертификат ключа проверки электронной записи.

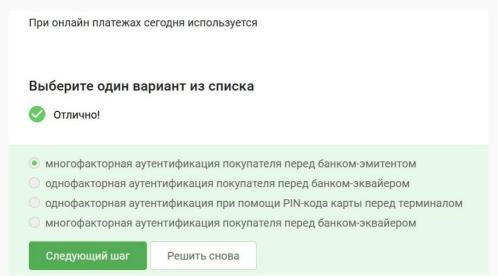


Пояснение ответа: MИР и MasterCard являются платежными системами.



Пояснение ответа: Многократная аутентификация заключается в том, что мы доказываем в ходе этого протокола несколько вещей есть. Основные категории вещей, которые мы можем доказать:

- 1. то, что я знаю-это либо пароль, либо пин код, либо в случае онлайн платежей это секретный код
- 2. конкретно в онлайн платежах мы используем второй фактор-это то, чем я владею, который вы должны подтвердить или вбить в ваш браузер
- 3. другой фактор аутентификации-это свойства например биометрия, отпечаток пальца
- 4. четвертый фактор аутентификации -локация.



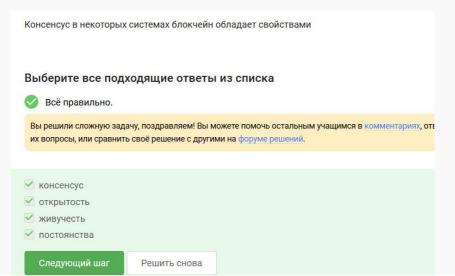
Пояснение ответа: При онлайн платежах сегодня используется многофакторная аутентификация покупателя перед банком-эмитентом

#### Вопрос/Ответ 1

Какое свойство криптографической хэш-функции используется в доказательстве работы? Выберите один вариант из списка Здорово, всё верно. фиксированная длина выходных данных сложность нахождения прообраза обеспечение целостности эффективность вычисления Следующий шаг Решить снова

29/34

Пояснение ответа: Сложность нахождения прообраза криптографической хэш функции используется в доказательстве работы.



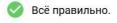
Пояснение ответа: В основе блокчейна лежит консенсус- публичная структура данных или леджер(бухгалтерская книга), которая обеспечивает:

- постоянство(добавленные когда-либо данные не могут быть удалены)
- консенсус(все участники видят одни и те же данные за исключением пары блоков)
- живучесть(участники могут добавлять новые транзакции)
- открытость(любой может стать участником блокчейна)

#### Вопрос/Ответ 3

Секретные ключи какого криптографического примитива хранят участники блокчейна?

# Выберите один вариант из списка



- обмен ключами
- шифрование
- цифровая подпись
- 🔾 хэш-функция

Следующий шаг

Решить снова

Пояснение ответа: Участники блокчейна хранят секретные ключи цифровой подписи каждой транзакции, эта подпись доказывает, что транзакция создана владельцем средств. Только владелец приватного ключа может распорядиться средствами, хранящимися на связанном адресе.