# Третий этап внешнего курса

Основы информационной безопасности

Казазаев Д. М.

Российский университет дружбы народов, Москва, Россия



#### Докладчик

- Казазаев Даниил Михайлович
- Студент бакалавриата
- Российский университет дружбы народов
- · [1132231427@rudn.ru]
- https://github.com/KazazaevDaniil/study\_2024-2025\_infosecintro

# Вводная часть

## Материалы и методы

Внешний кур состоит из трех этапов.

## Этап второй

# Первый этап курса состоит из 4 частей:

- 1. Введине в криптографию
- 2. Цифровая подпись
- 3. Электронные платежи
- 4. Блокчейн

внешнего курса.

Выполнение третьего этапа

В ассиметричных криптографических примитивах обестороны имеют пару ключей. (рис. 1)

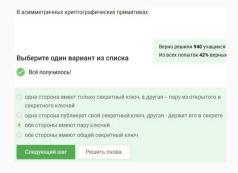


Рис. 1: Первый вопрос

Хещ-функция стойкая к колизиям, дает определенное кол-во бит вне зависимости от объема входных данных и эффективно вычисляется. (рис. 2)

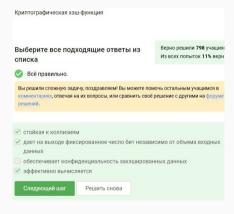
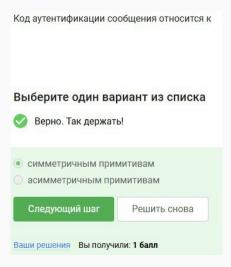


Рис. 2: Второй вопрос

RSA, ECDSA и ГОСТ стандарт(кузнечик) - алгоритмы цифровой подписи. (рис. 3)

К алгоритмам цифровой подписи относятся Выберите все подходящие ответы из списка Так точно! Вы решили сложную задачу, поздравляем! Вы можете комментариях, отвечая на их вопросы, или сравнить ( решений. AES SHA2 ✓ RSA ✓ ECDSA ▼ FOCT P 34.10-2012

Код аунтификации сообщения отеосится к симмитричным примитивам. (рис. 4)



Обмен ключами Диффи-Хэллмана - ассиметрический примитив генерации обзего секретного ключа. (рис. 5)

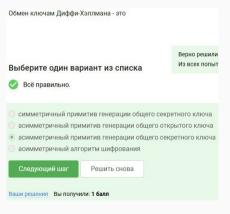


Рис. 5: Пятый вопрос

Протоколы цифровой подписи с публичным ключом.(рис. 6)

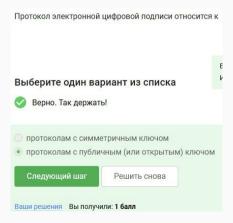


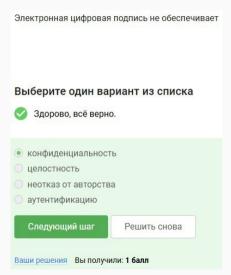
Рис. 6: Первый вопрос

Алгоритм верификации требует на вход: подпись, открытый ключ, сообщение.(рис. 7)

Алгоритм верификации электронной цифровой под	цписи требует на вход
Выберите один вариант из списка	Верно решили <b>962</b> у Из всех попыток <b>46</b>
Здорово, всё верно.	
подпись, открытый ключ, сообщение     подпись, секретный ключ     подпись, открытый ключ     подпись, секретный ключ, сообщение	
Следующий шаг	
Ваши решения Вы получили: 1 балл	

Рис. 7: Второй вопрос

Электронная подпись не обеспечивает конфиденциальность. (рис. 8)



Для отправки налоговой отчетности необходим сертификат с усилненной квалификацией.(рис. 9)

Какой тип сертификата электронной под налоговой отчетности в ФНС?	писи понадобится для отправки
Выберите один вариант из спист	Верно решили <b>975</b> у Из всех попыток <b>68</b>
усиленная неквалифицированная усиленная квалифицированная простая	
Следующий шаг	

Рис. 9: Четвертый вопрос

Квалифицированный сертификат можно получить в удостоверяющем центре.(рис. 10)

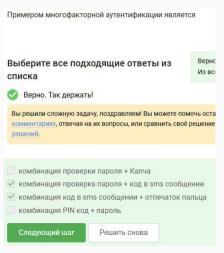
В какой организации вы можете получить квалифиц ключа проверки электронной подписи?	ированный сертификат
Выберите один вариант из списка	Верно решил <b>971</b> учащи Из всех попыток <b>61</b> % ве
<ul> <li>Хорошие новости, верно!</li> <li>Задание было изменено авторами. Баллы за прошлы</li> </ul>	е решения сохранены.
в любой организации, имеющей соответствующу     в минкомсвязи РФ     в удостоверяющем (сертификационном) центре     в любой организации по месту работы	ю лицензию ФСБ
Следующий шаг	

Рис. 10: Пятый вопрос

#### МИР, MasterCard - платежные системы. (рис. 11)

Выберите из списка все платежные системы. Выберите все подходящие ответы и списка Всё правильно. Вы решили сложную задачу, поздравляем! Вы мож комментариях, отвечая на их вопросы, или сравнит решений. BitCoin MasterCard SecurePay POS-терминал банкомат

Отмеченные варианты ответов являются примером многофакторной аутентификации. (рис. 12)



Сегодня при онлайн платежах используется многофакторная аутентификация покупателя перед банком-эмитентом. (рис. 13)

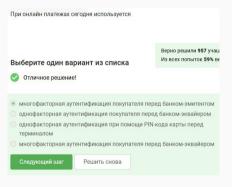


Рис. 13: Третий вопрос

В доказательстве работы криптографической хеш-функции используется сложность нахождения прообраза. (рис. 14)

Какое свойство криптографической хэш-фун доказательстве работы?	кции используется в
Выберите один вариант из списка	Верно реши Из всех поп
<b>В</b> ерно.	
фиксированная длина выходных данных • сложность нахождения прообраза обеспечение целостности эффективность вычисления	
Следующий шаг Решить снова	

Рис. 14: Первый вопрос

Все ответы являются верными для консенсуса некоторых блокчейн систем. (рис. 15)

Секретные ключи какого криптографического при блокчейна?	имитива хранят участники
Выберите один вариант из списка	Верно решил <b>951</b> учащи Из всех попыток <b>48</b> % ве
Хорошие новости, верно!	
<ul><li>Обмен ключами</li><li>шифрование</li><li>цифровая подпись</li><li>хэш-функция</li></ul>	
Следующий шаг	

Рис. 15: Второй вопрос

Участники криптографического примитива хранят при себе только цифровую подпись. (рис. 16)

Консенсус в некоторых	системах блокчейн облад	цает свойствами
Выберите все поду списка	одящие ответы из	Верно реші Из всех пог
	ичу, поздравляем! Вы можете а их вопросы, или сравнить с	
<ul><li>✓ живучесть</li><li>✓ открытость</li><li>✓ консенсус</li><li>✓ постоянства</li></ul>		
Следующий шаг	Решить снова	

Вывод

## Вывод

Выполнен третий этап внешнего курса