

# Третий этап внешнего курса

## Основы информационной безопасности

---

Казазаев Д. М.

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Казазаев Даниил Михайлович
- Студент бакалавриата
- Российский университет дружбы народов
- [1132231427@rudn.ru]
- [https://github.com/KazazaevDaniil/study\\_2024-2025\\_infosec-intro](https://github.com/KazazaevDaniil/study_2024-2025_infosec-intro)

## Вводная часть

---

Внешний кур состоит из трех этапов.

Первый этап курса состоит из 4 частей:

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

Выполнение третьего этапа  
внешнего курса.

---

Введение в криптографиюВведение в  
криптографию

---



В асимметричных криптографических примитивах обе стороны имеют пару ключей. (рис. 1)

В асимметричных криптографических примитивах

Выберите один вариант из списка

Верно решили **940** учащихся  
Из всех попыток **42%** верных

☒ Всё получилось!

☐ одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей

☐ одна сторона публикует свой секретный ключ, другая - держит его в секрете

☒ обе стороны имеют пару ключей

☐ обе стороны имеют общий секретный ключ

Следующий шаг

Решить снова

Рис. 1: Первый вопрос

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

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

Верно решили **798** учащихся  
Из всех попыток **11%** верно

☒ Всё правильно.

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
- ☒ дает на выходе фиксированное число бит независимо от объема входных данных
- ☐ обеспечивает конфиденциальность зашифрованных данных
- ☒ эффективно вычисляется

Следующий шаг    Решить снова

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 с [решений](#).

- ☐ AES
- ☐ SHA2
- ☒ RSA
- ☒ ECDSA
- ☒ ГОСТ Р 34.10-2012

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

Код аутентификации сообщения относится к

**Выберите один вариант из списка**



Верно. Так держать!



симметричным примитивам



асимметричным примитивам

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл**

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

Обмен ключам Диффи-Хэллмана - это

Верно решили  
Из всех попыт

Выберите один вариант из списка

☒ Всё правильно.

☐ симметричный примитив генерации общего секретного ключа

☐ ассиметричный примитив генерации общего открытого ключа

☒ ассиметричный примитив генерации общего секретного ключа

☐ ассиметричный алгоритм шифрования

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл**

Рис. 5: Пятый вопрос

## Цифровая подпись

---

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

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка



Верно. Так держать!



протоколам с симметричным ключом



протоколам с публичным (или открытым) ключом

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл**

Рис. 6: Первый вопрос

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

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

Верно решили 962 уч.  
Из всех попыток 46%

☒ Здорово, всё верно.

☐ подпись, открытый ключ, сообщение

☐ подпись, секретный ключ

☐ подпись, открытый ключ

☐ подпись, секретный ключ, сообщение

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 7: Второй вопрос



Электронная подпись не обеспечивает конфиденциальность.(рис. 8)

Электронная цифровая подпись не обеспечивает

**Выберите один вариант из списка**



Здорово, всё верно.

- ☒ конфиденциальность
- ☐ целостность
- ☐ неотказ от авторства
- ☐ аутентификацию

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **1 балл**

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

Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?

Выберите один вариант из списка

☒ Отлично!

- ☐ усиленная неквалифицированная
- ☒ усиленная квалифицированная
- ☐ простая

Следующий шаг

Решить снова

Верно решили 975 у  
Из всех попыток 68

Рис. 9: Четвертый вопрос

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

В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?

Выберите один вариант из списка

Верно решил **971** учащихся  
Из всех попыток **61%** верно

✓ Хорошие новости, верно!

↻ Задание было изменено авторами. Баллы за прошлые решения сохранены.

- ☐ в любой организации, имеющей соответствующую лицензию ФСБ
- ☐ в минкомсвязи РФ
- ☒ в удостоверяющем (сертификационном) центре
- ☐ в любой организации по месту работы

Следующий шаг

Решить снова

Рис. 10: Пятый вопрос


## Электронные платежи

---

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

Выберите из списка все платежные системы.

**Выберите все подходящие ответы из списка**

 Всё правильно.

Вы решили сложную задачу, поздравляем! Вы можете оставить [комментариях](#), отвечая на их вопросы, или сравнить [решений](#).

- ☐ BitCoin
- ☒ MasterCard
- ☐ SecurePay
- ☐ POS-терминал
- ☐ банкомат
- ☒ МИР

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

Примером многофакторной аутентификации является

**Выберите все подходящие ответы из списка**

[Вернуться к списку](#)

☒ Верно. Так держать!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальных пользователей, оставив [комментариях](#), отвечая на их вопросы, или сравнить своё решение с решениями.

☐ 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](#)

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

При онлайн платежах сегодня используется

**Выберите один вариант из списка**

Верно решили **957** учас  
Из всех попыток **59%** ве

☒ Отличное решение!

- ☒ многофакторная аутентификация покупателя перед банком-эмитентом
- ☐ однофакторная аутентификация покупателя перед банком-эквайером
- ☐ однофакторная аутентификация при помощи PIN-кода карты перед терминалом
- ☐ многофакторная аутентификация покупателя перед банком-эквайером

**Следующий шаг** Решить снова

Рис. 13: Третий вопрос

# Блокчейн

---



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

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

☒ Верно.

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

Следующий шаг

Решить снова

Верно решил  
Из всех попыток

Рис. 14: Первый вопрос

# Блокчейн

---

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

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Хорошие новости, верно!

- ☐ обмен ключами
- ☐ шифрование
- ☒ цифровая подпись
- ☐ хэш-функция

Следующий шаг

Решить снова

Верно решил 951 учащихся  
Из всех попыток 48% верных

Рис. 15: Второй вопрос

## Блокчейн

---

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

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

Верно решено  
Из всех предложенных

✓ Прекрасный ответ.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным [комментариях](#), отвечая на их вопросы, или сравнить своё решение с другими [решений](#).

- ✓ живучесть
- ✓ открытость
- ✓ консенсус
- ✓ постоянства

Следующий шаг

Решить снова

## Вывод

---

Выполнен третий этап внешнего курса