

# Внешний курс. Блок 3: Криптография на практике

Основы информационной безопасности

---

Петрова А.А.

16 мая 2025

Российский университет дружбы народов, Москва, Россия

# Информация

---

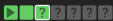
- Петрова Алевтина Александровна
- НКАбд-04-23
- Российский университет дружбы народов

Пройти третий блок курса “Основы кибербезопасности”

Выполнение контрольных заданий третьего блока внешнего курса “Основы Кибербезопасности”

## Вопрос 4.1.1

Для ответа на вопрос используется определение асимметричного шифрования с двумя ключами



В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Хорошая работа.

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

☐ обе стороны имеют общий секретный ключ

☒ обе стороны имеют пару ключей

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

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

Верно решил  
Из всех попы

## Вопрос 4.1.2

### Отмечены алгоритмы цифровой подписи



4.1 Введение в криптографию 4 из 7 шагов пройдено 2 из 5 баллов получено

Криптографическая хэш-функция

Выберите все подходящие ответы из списка



Здорово, всё верно.

Верно р

Из всех

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](#).

- ☒ дает на выходе фиксированное число бит независимо от объема входных данных
- ☐ обеспечивает конфиденциальность захешированных данных
- ☒ эффективно вычисляется
- ☒ стойкая к коллизиям

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

## Вопрос 4.1.3

### Отмечены алгоритмы цифровой подписи

1

4.1 Введение в криптографию 5 из 7 шагов пройдено 3 из 5 баллов получено

К алгоритмам цифровой подписи относятся

**Выберите все подходящие ответы из списка**

✓

Всё получилось!

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](#).

Верно решили **834** учащихся  
Из всех попыток **19%** верных

☐ AES

☐ SHA2

☒ RSA

☒ ECDSA

☒ ГОСТ Р 34.10-2012

Следующий шаг

Решить снова

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



## Вопрос 4.1.4

В информационной безопасности аутентификация сообщения или аутентификация источника данных-это свойство, которое гарантирует, что сообщение не было изменено во время передачи (целостность данных) и что принимающая сторона может проверить источник сообщения



4.1 Введение в криптографию 6 из 7 шагов пройдено 4 из 5 баллов получено

Код аутентификации сообщения относится к

Выберите один вариант из списка

☒ Абсолютно точно.

Верно реч  
Из всех пс

☐ симметричным примитивам

☐ асимметричным примитивам

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

# Вопрос 4.1.5

## Определение обмена ключами Диффи-Хэллмана.

???

4.1 Введение в криптографию 7 из 7 шагов пройдено 5 из 5 баллов получено

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

✓

Все правильно.

Верно решили **948** учащихся  
Из всех попыток **47%** верных

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

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

## Вопрос 4.2.1

По определению цифровой подписи протокол ЭЦП относится к протоколам с публичным ключом

?

?

?

?

?

4.2 Цифровая подпись 4 из 8 шагов пройдено 1 из 5 баллов получен

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв

Протокол электронной цифровой подписи относится к

**Выберите один вариант из списка**

☒ Верно.

Верно решил  
Из всех попь

☐ протоколам с симметричным ключом

☒ протоколам с публичным (или открытым) ключом

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: ...

## Вопрос 4.2.2

Алгоритм верификации электронной подписи состоит в следующем. На первом этапе получатель сообщения строит собственный вариант хэш-функции подписанного документа. На втором этапе происходит расшифровка хэш-функции, содержащейся в сообщении с помощью открытого ключа отправителя. На третьем этапе производится сравнение двух хэш-функций. Их совпадение гарантирует одновременно подлинность содержимого документа и его авторства



4.2 Цифровая подпись 5 из 8 шагов пройдено 2 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Всё получилось!

Верно реш  
Из всех poi

- ☒ подпись, открытый ключ, сообщение
- ☐ подпись, секретный ключ
- ☐ подпись, секретный ключ, сообщение

## Вопрос 4.2.3

Электронная подпись обеспечивает все указанное, кроме конфиденциальности

2

4.2 Цифровая подпись 6 из 8 шагов пройдено 3 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв Нет, спасибо

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

☒ Абсолютно точно.

Верно решили 968 учащихся  
Из всех попыток 53% верных

☐ аутентификацию

☐ неотказ от авторства

☒ конфиденциальность

☐ целостность

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

## Вопрос 4.2.4

Для отправки налоговой отчетности в ФНС используется усиленная квалифицированная электронная подпись

4.2 Цифровая подпись 7 из 8 шагов пройдено 4 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

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

Выберите один вариант из списка

☒ Хорошая работа.

☐ усиленная неквалифицированная

☒ усиленная квалифицированная

☐ простая

Следующий шаг

Решить снова

# Вопрос 4.2.5

## Верный ответ указан на изображении

4.2 Цифровая подпись 8 из 8 шагов пройдено 5 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

[Оставить отзыв](#) [Нет, спасибо](#)

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

**Выберите один вариант из списка**

☒ Здорово, всё верно.

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

☐ в любой организации, имеющей соответствующую лицензию ФСБ

☐ в минкомсвязи РФ

☒ в удостоверяющем (сертификационном) центре

☐ в любой организации по месту работы

Следующий шаг

Решить снова

Ваши решения Вы получили: **1 балл**

## Вопрос 4.3.1

### Известные платежные системы - Visa, MasterCard, МИР

4.3 Электронные платежи 3 из 5 шагов пройдено 1 из 3 баллов получен

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв

Выберите из списка все платежные системы.

**Выберите все подходящие ответы из списка**

✓

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](#).

☐ BitCoin

☒ MasterCard

☐ SecurePay

☐ POS-терминал

☐ банкомат

☒ МИР



## Вопрос 4.3.2

### Верный ответ на изображении



4.3 Электронные платежи 4 из 5 шагов пройдено 2 из 3 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

[Оставить отзыв](#)

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

☒ Хорошие новости, верно!

Верно решил

Из всех попыток

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](#).

- ☐ 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

## Вопрос 4.3.3

### При онлайн платежах используется многофакторная аутентификация

4.3 Электронные платежи 5 из 5 шагов пройдено 3 из 3 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв Нет, спасибо

При онлайн платежах сегодня используется

Выберите один вариант из списка

Верно. Так держать!

Верно решили 957 учащихся  
Из всех попыток 59% верных

☒ 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

Ваши решения Вы получили: 1 балл

## Вопрос 4.4.1

Proof-of-Work, или PoW, (доказательство выполнения работы) — это алгоритм достижения консенсуса в блокчейне; он используется для подтверждения транзакций и создания новых блоков. С помощью PoW майнеры конкурируют друг с другом за завершение транзакций в сети и за вознаграждение.

Пользователи сети отправляют друг другу цифровые токены, после чего все транзакции собираются в блоки и записываются в распределенный реестр, то есть в блокчейн.



4.4 Блокчейн 4 из 6 шагов пройдено 1 из 3 баллов получен

Вы прошли больше 80% курса, оставьте отзыв [Оставить отзыв](#)

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

☒ Отлично!

Верно решили  
Из всех попыт

## Вопрос 4.4.2

Консенсус блокчейна — это процедура, в ходе которой участники сети достигают согласия о текущем состоянии данных в сети. Благодаря этому алгоритмы консенсуса устанавливают надежность и доверие к самой сети.

4.4 Блокчейн 5 из 6 шагов пройдено 2 из 3 баллов получено

Вы прошли больше 80% курса, оставьте отзыв [Оставить отзыв](#)

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 учащимся в [комментариях](#), отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

☒ живучесть

☒ консенсус

☒ постоянства

## Вопрос 4.4.3

### Ответ - цифровая подпись



4.4 Блокчейн 6 из 6 шагов пройдено 3 из 3 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

[Ост](#)

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Всё получилось!

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

Следующий шаг

Решить снова

## Третий блок пройден успешно



Поздравляем!

Вы завершили курс «Основы кибербезопасности».

Вы набрали **53 балла из 53**, изучив 100% материалов курса.  
Сертификат в нём не выдаётся, но вы можете поделиться своим результатом в соцсетях.



<https://stepik.org/course/111512>

☆ Оставить отзыв

Найти новый курс