

# Внешний курс. Блок 3. Криптография на практике

## Основы информационной безопасности

---

Мурашов И. В., НКАбд-03-23

17 мая 2025

Российский университет дружбы народов, Москва, Россия

- Мурашов Иван Вячеславович
- Студент, 2 курс, группа НКАбд-03-23
- Российский университет дружбы народов
- 1132236018@rudn.ru
- <https://neve7mind.github.io>

Выполнение контрольных заданий 3го блока внешнего курса “Основы Кибербезопасности”.

Асимметричные криптографические системы подразумевают под собой то, что пара ключей есть у обеих сторон.

4.1 Введение в криптографию 3 из 7 шагов пройдено 1 из 5 баллов получен

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Прекрасный ответ.

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

- ☒ обе стороны имеют пару ключей
- ☐ 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 общий секретный ключ

Следующий шаг

Решить снова

## Отмечены основные условия для криптографической хэш-функции.

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

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

☒ Хорошая работа.

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

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
- ☒ эффективно вычисляется
- ☒ стойкая к коллизиям
- ☐ обеспечивает конфиденциальность захэшированных данных

Следующий шаг

Решить снова

## Отмечены алгоритмы цифровой подписи.

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

☒ Хорошие новости, верно!

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

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

Решить снова

# Введение в криптографию

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

☒ Всё правильно.

☐ асимметричным примитивам

☒ симметричным примитивам

Верно решили **955** учащихся  
Из всех попыток **69%** верных

## 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

☒ Верно. Так держать!

- ☐ 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

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



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](#) [Нет, спасибо](#)

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Всё правильно.

Верно решили **956** учащихся  
Из всех попыток **71%** верных

- ☐ протоколам с симметричным ключом
- ☒ протоколам с публичным (или открытым) ключом

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](#)

[Нет, спасибо](#)

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

Верно решили 962 учащихся

Электронная подпись обеспечивает все указанное, кроме конфиденциальности.

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

☒ Верно. Так держать!

Верно решили **968** учащихся  
Из всех попыток **53%** верных

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

# Цифровая подпись

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

[Оставить отзыв](#) [Нет, спасибо](#)

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

Выберите один вариант из списка

☒ Отлично!

Верно решили **975** учащихся  
Из всех попыток **68%** верных

- ☐ усиленная неквалифицированная
- ☒ усиленная квалифицированная
- ☐ простая

[Следующий шаг](#)

[Решить снова](#)

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

☒ 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

## 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](#) [Нет, спасибо](#)

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

☒ Прекрасный ответ.

Верно решили **900** учащихся  
Из всех попыток **24%** верных

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

## Верный ответ на изображении.

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

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка



Верно. Так держать!

Верно решили **896** учащихся  
Из всех попыток **24%** верных

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

При онлайн платежах используется многофакторная аутентификация.

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

При онлайн платежах сегодня используется

Выберите один вариант из списка

☒ Всё правильно.

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




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

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

 Прекрасный ответ

Верно решили **932** учащихся  
Из всех попыток **49%** верных

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

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

☒ Абсолютно точно.

Верно решили **864** учащихся  
Из всех попыток **23%** верных

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](#).

☒ постоянства

☒ живучесть

☒ открытость

Ответ - цифровая подпись.

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

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка



Отличное решение!

Верно решил **951** учащийся

Из всех попыток **48%** верных

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

Следующий шаг

Решить снова

Был пройден третий блок курса “Основы кибербезопасности”, мной были изучены такие понятия как цифровая подпись, электронные платежи и блокчейн.