

## Этап 3

### Внешний проект

---

Улитина М.М.

17 мая 2025

Российский университет дружбы народов, Москва, Россия

## Информация

---

::::::::: {.columns align=center} :: {.column width="70%"}

- Улитина Мария Максимовна
- студентка

Выполнение второго этапа  
внешнего курса

---

В асимметричных криптографических примитивах

Выберите один вариант из списка



Отлично!

- ☒ 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

## Криптографическая хэш-функция

Выберите все подходящие ответы из списка



Хорошая работа.

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



обеспечивает конфиденциальность зашифрованных данных



эффективно вычисляется



дает на выходе фиксированное число бит независимо от объема входных данных

Следующий шаг

Решить снова

К алгоритмам цифровой подписи относятся

**Выберите все подходящие ответы из списка**



Правильно, молодец!

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

Код аутентификации сообщения относится к

**Выберите один вариант из списка**



Всё правильно.



асимметричным примитивам



симметричным примитивам

Следующий шаг

Решить снова



Обмен ключам Диффи-Хэллмана - это

**Выберите один вариант из списка**

☒ Верно.

- ☐ 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

Протокол электронной цифровой подписи относится к

**Выберите один вариант из списка**



Хорошая работа.



протоколам с симметричным ключом



протоколам с публичным (или открытым) ключом

Следующий шаг

Решить снова

Алгоритм верификации электронной цифровой подписи требует на вход

**Выберите один вариант из списка**



Абсолютно точно.

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

Следующий шаг

Решить снова

Электронная цифровая подпись не обеспечивает

**Выберите один вариант из списка**



Хорошая работа.


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

Следующий шаг

Решить снова

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

Выберите один вариант из списка

 Отлично!

- ☒ усиленная квалифицированная
- ☐ простая
- ☐ усиленная неквалифицированная

Следующий шаг

Решить снова

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

Верн  
Из в

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

Выберите один вариант из списка

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

☒ Верно. Так держать!

- ☐ 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**

Рис. 10: организация

Выберите из списка все платежные системы.

**Выберите все подходящие ответы из списка**



Всё правильно.

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

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

Следующий шаг

Решить снова

Примером многофакторной аутентификации является

**Выберите все подходящие ответы из списка**



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](#).

- ☐ 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 сегодня используется

**Выберите один вариант из списка**



Всё получилось!

- ☒ 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

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

Консенсус в некоторых системах блокчейн обладает свойствами

**Выберите все подходящие ответы из списка**



Верно.

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](#).



консенсус



постоянства



живучесть



открытость

Следующий шаг

Решить снова

Выполнен третий этап.