

# **Отчет по части “Криптография на практике” курса “Основы кибербезопасности”**

Стариков Данила Андреевич

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>3</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>4</b>
2.1	Введение в криптографию . . . . .	4
2.2	Цифровая подпись . . . . .	7
2.3	Электронные платежи . . . . .	11
2.4	Блокчейн . . . . .	14
<b>3</b>	<b>Выводы</b>	<b>16</b>

# 1 Цель работы

Познакомиться со следующими понятиями: - Электронная подпись -  
Электронные платежи - Блокчейн

## 2 Выполнение лабораторной работы

### 2.1 Введение в криптографию

- Вопрос 1. В асимметричных криптографических примитивах(рис. 2.1):

Ответ: *обе стороны имеют пару ключей.*

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Так точно!

[Вернуться к списку вопросов](#)

- ☐ 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** из 1

Рис. 2.1: Скриншот выполнения задания

- Вопрос 2. Криптографическая хэш-функция(рис. 2.2):

Ответ: *эффективно вычисляется, дает на выходе фиксированное число бит независимо от объема входных данных, стойкая к коллизиям.*

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](#).

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 2.2: Скриншот выполнения задания

- Вопрос 3. К алгоритмам цифровой подписи относятся(рис. 2.3):

Ответ: *RSA, ECDSA, ГОСТ Р 34.10-2012* .

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

✓ Здорово, всё 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](#).

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 2.3: Скриншот выполнения задания

- Вопрос 4. Код аутентификации сообщения относится к(рис. 2.4):

Ответ: *симметричным примитивам.*

Код аутентификации сообщения относится к

**Выберите один вариант из списка**



Так точно!



асимметричным примитивам



симметричным примитивам

Следующий шаг

Решить снова

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

Рис. 2.4: Скриншот выполнения задания

- Вопрос 5. Обмен ключам Диффи-Хэллмана - это(рис. 2.5):

Ответ: *асимметричный примитив генерации общего секретного ключа.*

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

✓ Всё получилось!

- ☐ 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** из 1

Рис. 2.5: Скриншот выполнения задания

## 2.2 Цифровая подпись

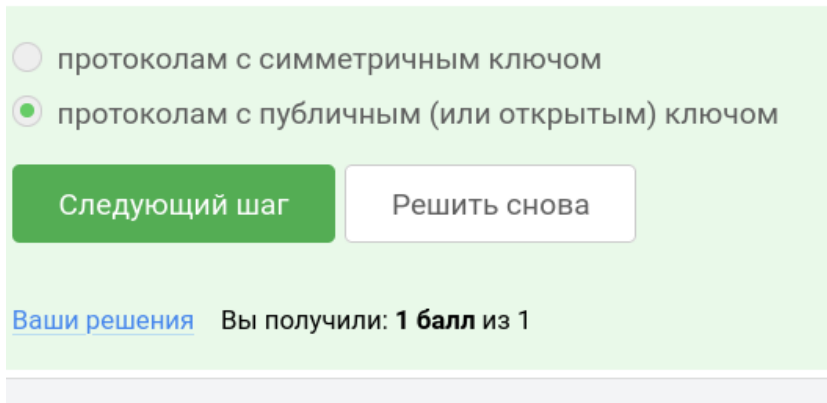
- Вопрос 1. Протокол электронной цифровой подписи относится к(рис. 2.6):

Ответ: *протоколам с публичным (или открытым) ключом.*

Протокол электронной цифровой подписи относится к

**Выберите один вариант из списка**

☒ Всё правильно.



☐ протоколам с симметричным ключом

☒ протоколам с публичным (или открытым) ключом

Следующий шаг

Решить снова

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

Рис. 2.6: Скриншот выполнения задания

- Вопрос 2. Алгоритм верификации электронной цифровой подписи требует на вход(рис. 2.7):

Ответ: *подпись, открытый ключ, сообщение.*



Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Правильно, молодец!

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

Следующий шаг

Решить снова

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

Рис. 2.7: Скриншот выполнения задания

- Вопрос 3. Электронная цифровая подпись не обеспечивает(рис. 2.8):

Ответ: *конфиденциальность.*

Электронная цифровая подпись не обеспечивает

### Выберите один вариант из списка

☒ Отличное решение!

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

Следующий шаг

Решить снова

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

Рис. 2.8: Скриншот выполнения задания

- Вопрос 4. Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?(рис. 2.9):

Ответ: *усиленная квалифицированная.*

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

Выберите один вариант из списка

☒ Абсолютно точно.

Верно реш  
Из всех по

- ☐ простая  
☐ усиленная неквалифицированная  
☒ усиленная квалифицированная

Следующий шаг

Решить снова

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

Рис. 2.9: Скриншот выполнения задания

- Вопрос 5. В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?(рис. 2.10):

Ответ: *в удостоверяющем (сертификационном) центре.*

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

Выберите один вариант из списка

☒ Хорошая работа.

Верно решили **907** учас  
Из всех попыток **60%** вер

- ☐ 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** из 1

Рис. 2.10: Скриншот выполнения задания

## 2.3 Электронные платежи

- Вопрос 1. Выберите из списка все платежные системы.(рис. 2.11):

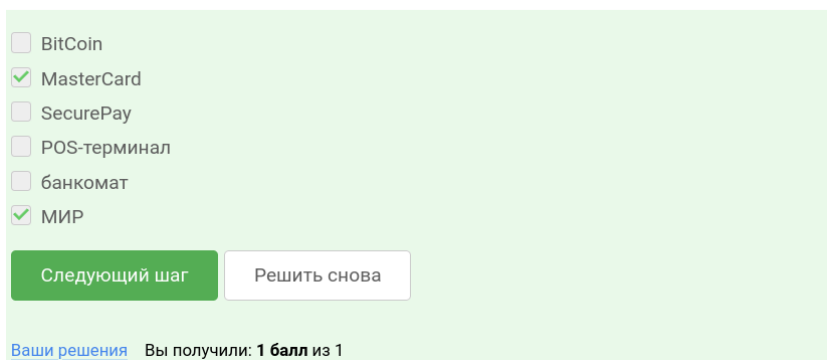
Ответ: *MasterCard, МИР.*

Выберите из списка все платежные системы.

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](#).



☐ BitCoin

☒ MasterCard

☐ SecurePay

☐ POS-терминал

☐ банкомат

☒ МИР

Следующий шаг

Решить снова

Ваши решения    Вы получили: 1 балл из 1

Рис. 2.11: Скриншот выполнения задания

- Вопрос 2. Примером многофакторной аутентификации является(рис. 2.12):

Ответ: комбинация проверка пароля + код в sms сообщении, комбинация код в sms сообщении + отпечаток пальца .

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✔ Отлично!

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](#)

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

Рис. 2.12: Скриншот выполнения задания

- Вопрос 3. При онлайн платежах сегодня используется(рис. 2.13):

Ответ: *многофакторная аутентификация покупателя перед банком-эмитентом.*

При онлайн платежах сегодня используется

Выберите один вариант из списка

✔ Так точно!

☒ 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** из 1

Рис. 2.13: Скриншот выполнения задания

## 2.4 Блокчейн

- Вопрос 1. Какое свойство криптографической хэш-функции используется в доказательстве работы?(рис. 2.14):

Ответ: *сложность нахождения прообраза.*

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

☒ Здорово, всё верно.

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

Следующий шаг

Решить снова

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

Рис. 2.14: Скриншот выполнения задания

- Вопрос 2. Консенсус в некоторых системах блокчейн обладает свойствами(рис. 2.15):

Ответ: *постоянства, консенсус, живучесть, открытость.*

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

✔ Отлично!

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
- ☒ консенсус
- ☒ живучесть
- ☒ открытость

Следующий шаг

Решить снова

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

Рис. 2.15: Скриншот выполнения задания

- Вопрос 3. Секретные ключи какого криптографического примитива хранят участники блокчейна?(рис. 2.16):

Ответ: *цифровая подпись*.

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

✔ Верно. Так держать!

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

Следующий шаг

Решить снова

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

Рис. 2.16: Скриншот выполнения задания

## 3 Выводы

В рамках третьего модуля познакомились с основами криптографии: электронной подписью, электронными платежами, блокчейном.