

# **Отчет по третьему этапу внешнего курса**

**Дисциплина: основы информационной безопасности**

Казазаев Даниил Михайлович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Этап первый</b>	<b>5</b>
<b>3</b>	<b>Выполнение первого этапа внешнего курса.</b>	<b>6</b>
3.1	Введеине в криптографиюВведеине в криптографию . . . . .	6
<b>4</b>	<b>Цифровая подпись</b>	<b>11</b>
<b>5</b>	<b>Электронные платежи</b>	<b>15</b>
<b>6</b>	<b>Блокчейн</b>	<b>19</b>
<b>7</b>	<b>Вывод</b>	<b>22</b>

## Список иллюстраций

3.1	Первый вопрос . . . . .	6
3.2	Второй вопрос . . . . .	7
3.3	Третий вопрос . . . . .	8
3.4	Четвертый вопрос . . . . .	9
3.5	Пятый вопрос . . . . .	10
4.1	Первый вопрос . . . . .	11
4.2	Второй вопрос . . . . .	12
4.3	Третий вопрос . . . . .	13
4.4	Четвертый вопрос . . . . .	14
4.5	Пятый вопрос . . . . .	14
5.1	Первый вопрос . . . . .	16
5.2	Второй вопрос . . . . .	17
5.3	Третий вопрос . . . . .	18
6.1	Первый вопрос . . . . .	19
6.2	Второй вопрос . . . . .	20
6.3	Третий вопрос . . . . .	21

# 1 Цель работы

Внешний кур состоит из трех этапов.

## 2 Этап первый

Первый этап курса состоит из 4 частей:

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

## 3 Выполнение первого этапа внешнего курса.

### 3.1 Введение в криптографию

В асимметричных криптографических примитивах обе стороны имеют пару ключей. (рис. 3.1)

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. 3.1: Первый вопрос

Хеш-функция стойкая к коллизиям, дает определенное кол-во бит вне зависимости от объема входных данных и эффективно вычисляется. (рис. 3.2)

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 захешированных данных
- ☒ эффективно вычисляется

Следующий шаг

Решить снова

Рис. 3.2: Второй вопрос

RSA, ECDSA и ГОСТ стандарт(кузнечик) - алгоритмы цифровой подписи. (рис. 3.3)

К алгоритмам цифровой подписи относятся

**Выберите все подходящие ответы из списка**

☒ Так точно!

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

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

Следующий шаг

Решить снова

Рис. 3.3: Третий вопрос

Код аутентификации сообщения относится к симметричным примитивам. (рис. 3.4)



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**

Рис. 3.4: Четвертый вопрос

Обмен ключами Диффи-Хэллмана - асимметрический примитив генерации общего секретного ключа. (рис. 3.5)

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

Верно решили  
Из всех попыт

✓ Всё правильно.

- ☐ 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**

Рис. 3.5: Пятый вопрос

## 4 Цифровая подпись

Протоколы цифровой подписи с публичным ключом.(рис. 4.1)

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. 4.1: Первый вопрос

Алгоритм верификации требует на вход: подпись, открытый ключ, сообщение.(рис. 4.2)

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

Верно решили **962** ученика  
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. 4.2: Второй вопрос

Электронная подпись не обеспечивает конфиденциальность.(рис. 4.3)

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**

Рис. 4.3: Третий вопрос

Для отправки налоговой отчетности необходим сертификат с усиленной квалификацией.(рис. 4.4)

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

Выберите один вариант из списка

Верно решили **975** у

Из всех попыток **68**

✓ Отлично!

- ☐ усиленная неквалифицированная
- ☒ усиленная квалифицированная
- ☐ простая

Следующий шаг

Решить снова

Рис. 4.4: Четвертый вопрос

Квалифицированный сертификат можно получить в удостоверяющем центре.(рис. 4.5)

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

Выберите один вариант из списка

Верно решил **971** участи

Из всех попыток **61%** ве

✓ 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. 4.5: Пятый вопрос

## **5 Электронные платежи**

МИР, MasterCard - платежные системы. (рис. 5.1)

Выберите из списка все платежные системы.

**Выберите все подходящие ответы из списка**

☒ Всё правильно.

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

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

Следующий шаг

Решить снова

Рис. 5.1: Первый вопрос

Отмеченные варианты ответов являются примером многофакторной аутентификации. (рис. 5.2)



Примером многофакторной аутентификации является

**Выберите все подходящие ответы из списка**

Верно

Из списка



Верно. Так держать!

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

- ☐ 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

Рис. 5.2: Второй вопрос

Сегодня при онлайн платежах используется многофакторная аутентификация покупателя перед банком-эмитентом. (рис. 5.3)

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. 5.3: Третий вопрос

## 6 Блокчейн

В доказательстве работы криптографической хэш-функции используется сложность нахождения прообраза. (рис. 6.1)

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 решено  
Из всех попыток

Рис. 6.1: Первый вопрос

Все ответы являются верными для консенсуса некоторых блокчейн систем. (рис. 6.2)

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

Верно решил **951** учащихся  
Из всех попыток **48%** верно

☒ Хорошие новости, верно!

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

Следующий шаг

Решить снова

Рис. 6.2: Второй вопрос

Участники криптографического примитива хранят при себе только цифровую подпись. (рис. 6.3)

Консенсус в некоторых системах блокчейн обладает свойствами

**Выберите все подходящие ответы из списка**

Верно решено.  
Из всех предложенных вариантов вы выбрали все подходящие.

✓ Прекрасный ответ.

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

- ☒ живучесть
- ☒ открытость
- ☒ консенсус
- ☒ постоянства

Следующий шаг

Решить снова

Рис. 6.3: Третий вопрос

## **7 Вывод**

Выполнен третий этап внешнего курса