

# **Внешний курс. Блок 3. Криптография на практике**

**Основы информационной безопасности**

Мурашов Иван Вячеславович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение заданий</b>	<b>6</b>
2.1	Введение в криптографию . . . . .	6
2.2	Цифровая подпись . . . . .	8
2.3	Электронные платежи . . . . .	11
2.4	Блокчейн . . . . .	12
<b>3</b>	<b>Выводы</b>	<b>15</b>

# Список иллюстраций

2.1	Вопрос 4.1.1	. . . . .	6
2.2	Вопрос 4.1.2	. . . . .	7
2.3	Вопрос 4.1.3	. . . . .	7
2.4	Вопрос 4.1.4	. . . . .	8
2.5	Вопрос 4.1.5	. . . . .	8
2.6	Вопрос 4.2.1	. . . . .	9
2.7	Вопрос 4.2.2	. . . . .	9
2.8	Вопрос 4.2.3	. . . . .	10
2.9	Вопрос 4.2.4	. . . . .	10
2.10	Вопрос 4.2.5	. . . . .	11
2.11	Вопрос 4.3.1	. . . . .	11
2.12	Вопрос 4.3.2	. . . . .	12
2.13	Вопрос 4.3.3	. . . . .	12
2.14	Вопрос 4.4.1	. . . . .	13
2.15	Вопрос 4.4.2	. . . . .	13
2.16	Вопрос 4.4.3	. . . . .	14

## **Список таблиц**

# **1 Цель работы**

Выполнение контрольных заданий 3го блока внешнего курса “Основы Кибер-безопасности”.

## 2 Выполнение заданий

### 2.1 Введение в криптографию

Асимметричные криптографические системы подразумевают под собой то, что пара ключей есть у обеих сторон (рис. 2.1).

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

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.1: Вопрос 4.1.1

Отмечены основные условия для криптографической хэш-функции (рис. 2.2).

#### 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 зашифрованных данных

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.2: Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. 2.3).

#### 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

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.3: Вопрос 4.1.3

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 (рис. 2.4)

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.

Верно решили 955 учащихся  
Из всех попыток 69% верных

☐ асимметричным примитивам  
☒ симметричным примитивам

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.4: Вопрос 4.1.4

## Определение обмена ключами Диффи-Хэллмана. (рис. 2.5).

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!

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

Рис. 2.5: Вопрос 4.1.5

## 2.2 Цифровая подпись

По определению цифровой подписи протокол ЭЦП относится к протоколам с публичным ключом (рис. 2.6).



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**

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

☐ протоколам с симметричным ключом

☒ протоколам с публичным (или открытым) ключом

[Следующий шаг](#) [Решить снова](#)

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

Рис. 2.6: Вопрос 4.2.1

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 (рис. 2.7).

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  
Из всех попыток **46%** верных

☒ Хорошая работа.

☐ подпись, секретный ключ, сообщение

☐ подпись, открытый ключ

☒ подпись, открытый ключ, сообщение

☐ подпись, секретный ключ

[Следующий шаг](#) [Решить снова](#)

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

Рис. 2.7: Вопрос 4.2.2

Электронная подпись обеспечивает все указанное, кроме конфиденциальности (рис. 2.8).

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

[Следующий шаг](#)
[Решить снова](#)

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

Рис. 2.8: Вопрос 4.2.3

Для отправки налоговой отчетности в ФНС используется усиленная квалифицированная электронная подпись (рис. 2.9).

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](#)

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

Рис. 2.9: Вопрос 4.2.4

Верный ответ указан на изображении (рис. 2.10).

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 учащийся  
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

Рис. 2.10: Вопрос 4.2.5

## 2.3 Электронные платежи

Известные платежные системы - Visa, MasterCard, МИР (рис. 2.11).

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

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.11: Вопрос 4.3.1

Верный ответ на изображении (рис. 2.12).

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 решили 896 учащихся  
Из всех попыток 24% верных

✓ Верно. Так держать!

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

Рис. 2.12: Вопрос 4.3.2

При онлайн платежах используется многофакторная аутентификация (рис. 2.13).

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

При онлайн платежах сегодня используется

Выберите один вариант из списка

Верно решили 957 учащихся  
Из всех попыток 59% верных

✓ Всё правильно.

☒ 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

Рис. 2.13: Вопрос 4.3.3

## 2.4 Блокчейн

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 (рис. 2.14).

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

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.14: Вопрос 4.4.1

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 самоу сети. (рис. 2.15).

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
- ☒ консенсус

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.15: Вопрос 4.4.2

Ответ - цифровая подпись (рис. 2.16).

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

Ваши решения Вы получили: 1 балл

Рис. 2.16: Вопрос 4.4.3

## 3 Выводы

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