

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

**Основы информационной безопасности**

**БАХИ СИДИ АЛИ ТЕМАССИНИ**

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение блока 3: Криптография на практике</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	. . . . .	14
2.16	Вопрос 4.4.3	. . . . .	14

## Список таблиц

# **1 Цель работы**

Пройти третий блок курса “Основы кибербезопасности”

## 2 Выполнение блока 3: Криптография на практике

### 2.1 Введение в криптографию

Для ответа на вопрос используется определение асимметричного шифрования с двумя ключами (рис. 2.1).

The screenshot shows a quiz interface for the topic '4.1 Введение в криптографию'. At the top, a progress bar indicates '7 из 7 шагов пройдено' and '5 из 5 баллов получено'. Below this, a light blue banner contains the text 'Вы прошли больше 80% курса, оставьте отзыв' with buttons 'Оставить отзыв' and 'Нет, спасибо'. The main question area is titled 'В асимметричных криптографических примитивах' and asks to 'Выберите один вариант из списка'. A green checkmark indicates the correct answer is 'Верно'. To the right, a green box shows statistics: 'Верно решили 940 учащихся' and 'Из всех попыток 42% верных'. The list of options includes: 'обе стороны имеют пару ключей' (selected), 'одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей', 'обе стороны имеют общий секретный ключ', and 'одна сторона публикует свой секретный ключ, другая - держит его в секрете'. At the bottom are buttons 'Следующий шаг' and 'Решить снова'.

Рис. 2.1: Вопрос 4.1.1

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

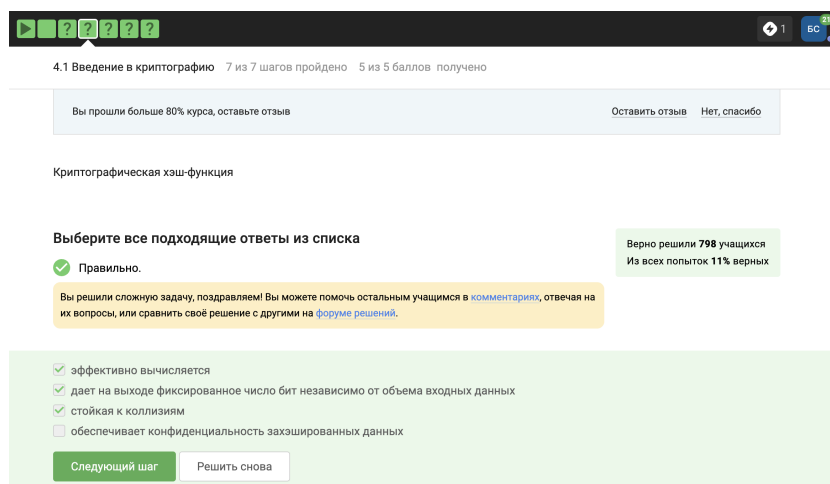


Рис. 2.2: Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. 2.3).

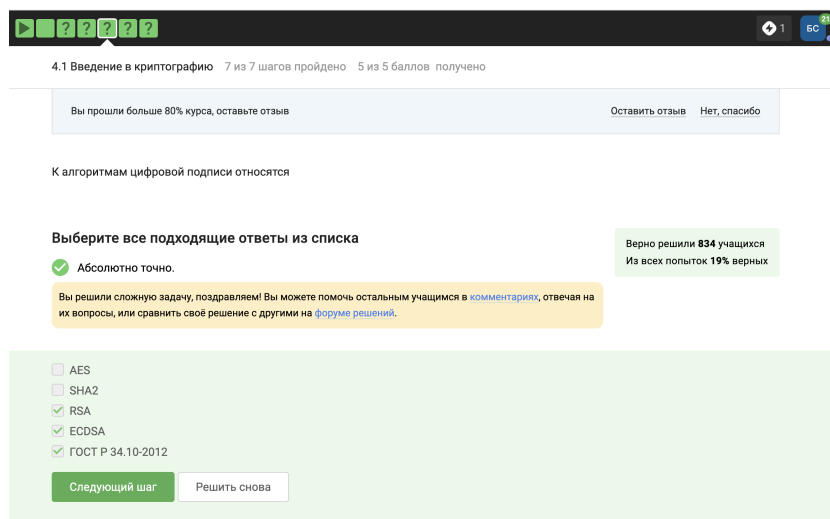


Рис. 2.3: Вопрос 4.1.3

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 7 из 7 шагов пройдено 5 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв [Оставить отзыв](#) [Нет, спасибо](#)

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Всё правильно.

Верно решили 955 учащихся  
Из всех попыток 69% верных

☒ симметричным примитивам  
☐ асимметричным 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

Вы прошли больше 80% курса, оставьте отзыв [Оставить отзыв](#) [Нет, спасибо](#)

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

✓ Всё правильно.

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 8 из 8 шагов пройдено 5 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв [Оставить отзыв](#) [Нет, спасибо](#)

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Прекрасный ответ.

Верно решили 956 учащихся  
Из всех попыток 71% верных

☐ протоколам с симметричным ключом

☒ протоколам с публичным (или открытым) ключом

[Следующий шаг](#) [Решить снова](#)

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 8 из 8 шагов пройдено 5 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

☒ Хорошие новости, верно!

Верно решили 962 учащихся  
Из всех попыток 46% верных

☐ подпись, секретный ключ, сообщение

☒ подпись, открытый ключ, сообщение

☐ подпись, открытый ключ

☐ подпись, секретный ключ

[Следующий шаг](#) [Решить снова](#)

Рис. 2.7: Вопрос 4.2.2

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

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](#)

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

✓ Правильно.

Верно решили 968 учащихся  
Из всех попыток 53% верных

☒ конфиденциальность  
☐ неотказ от авторства  
☐ целостность  
☐ аутентификацию

[Следующий шаг](#) [Решить снова](#)

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 8 из 8 шагов пройдено 5 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

✓ Правильно, молодец!

Верно решили 975 учащихся  
Из всех попыток 68% верных

☐ простая  
☐ усиленная неквалифицированная  
☒ усиленная квалифицированная

[Следующий шаг](#) [Решить снова](#)

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

Отлично!

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](#)

Рис. 2.10: Вопрос 4.2.5

## 2.3 Электронные платежи

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

4.3 Электронные платежи 8 из 8 шагов пройдено 5 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв [Оставить отзыв](#) [Нет, спасибо](#)

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

Здорово, всё верно.

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](#)

Рис. 2.11: Вопрос 4.3.1

Верный ответ на изображении (рис. 2.12).

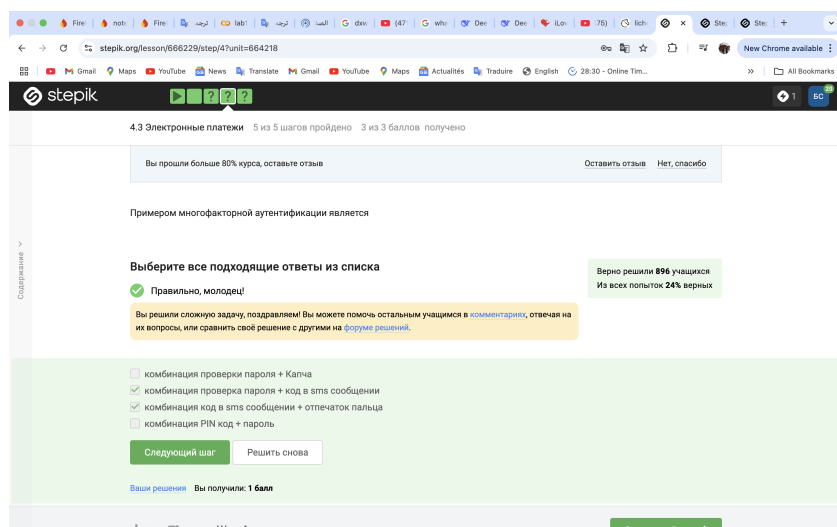


Рис. 2.12: Вопрос 4.3.2

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

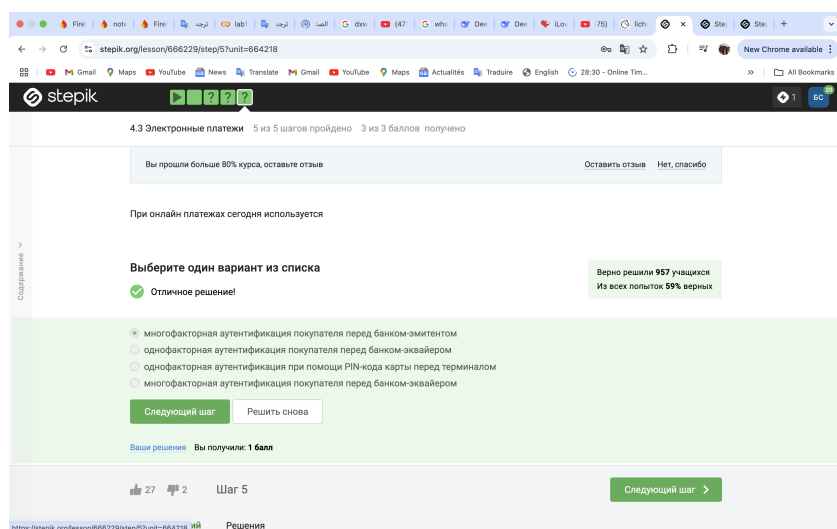


Рис. 2.13: Вопрос 4.3.3

## 2.4 Блокчейн

Proof-of-Work, или PoW, (доказательство выполнения работы) — это алгоритм достижения консенсуса в блокчейне; он используется для подтверждения тран-

закций 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).

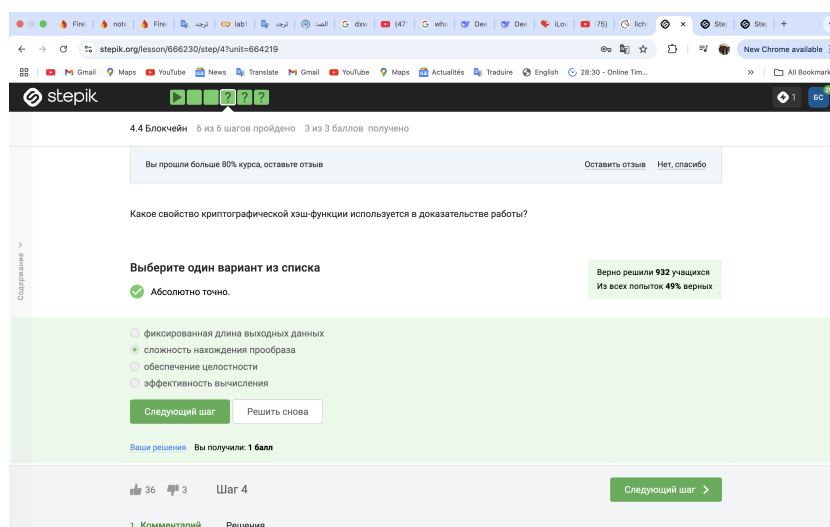


Рис. 2.14: Вопрос 4.4.1

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 самой сети. (рис. 2.15).

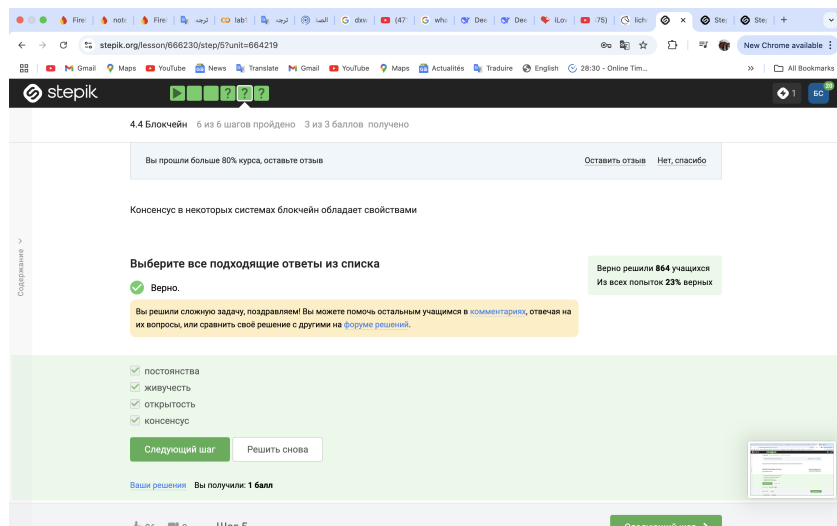


Рис. 2.15: Вопрос 4.4.2

Ответ - цифровая подпись (рис. 2.16).

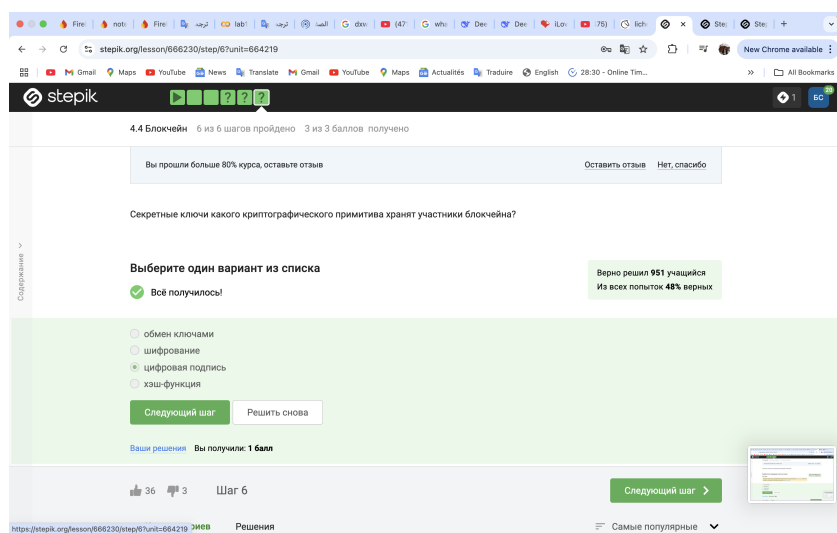


Рис. 2.16: Вопрос 4.4.3

## 3 Выводы

Я прошла третий блок