

## **Внешний курс. Этап 3: Введение в Linux**

Скворцова Анастасия Дмитриевна

## Содержание

1	Цель работы .....	2
2	Выполнение блока 3: Криптография на практике .....	4
2.1	Введение в криптографию.....	4
2.2	Цифровая подпись .....	6
2.3	Электронные платежи.....	8
2.4	Блокчейн .....	9
3	Выводы.....	11

## **1      Цель работы**

Пройти третий блок курса “ Введение в Linux ”

## 2 Выполнение блока 3: Криптография на практике

### 2.1 Введение в криптографию

Для ответа на вопрос используется определение асимметричного шифрования с двумя ключами (рис. 1).

4.1 Введение в криптографию 7 из 7 шагов пройдено 5 из 5 баллов получено

В асимметричных криптографических примитивах

Выберите один вариант из списка

✓ Так точно!

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
- ☐ обе стороны имеют общий секретный ключ
- ☐ одна сторона публикует свой секретный ключ, другая – держит его в секрете

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 1: Вопрос 4.1.1

Отмечены основные условия для криптографической хэш-функции (рис. 2).

4.1 Введение в криптографию 7 из 7 шагов пройдено 5 из 5 баллов получено

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

✓ Все получилось!

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.

- ☒ даёт на выходе фиксированное число бит независимо от объёма входных данных
- ☐ обеспечивает конфиденциальность зашифрованных данных
- ☒ эффективно вычисляется
- ☒ стойкая к коллизиям

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2: Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. 3).

4.1 Введение в криптографию 7 из 7 шагов пройдено 5 из 5 баллов получено

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

✓ Отличное решение!

Верно решили 816 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 из 1

Рис. 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. 4)

4.1 Введение в криптографию 7 из 7 шагов пройдено 5 из 5 баллов получено

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 930 учащихся  
Из всех попыток 69% верных

☐ асимметричным примитивам

☒ симметричным примитивам

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 4: Вопрос 4.1.4

Определение обмена ключами Диффи-Хэллмана. (рис. 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

✓ Хорошая работа.

Верно решили 923 учащихся  
Из всех попыток 46% 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 из 1

Рис. 5: Вопрос 4.1.5

## 2.2 Цифровая подпись

По определению цифровой подписи протокол ЭЦП относится к протоколам с публичным ключом (рис. 6).

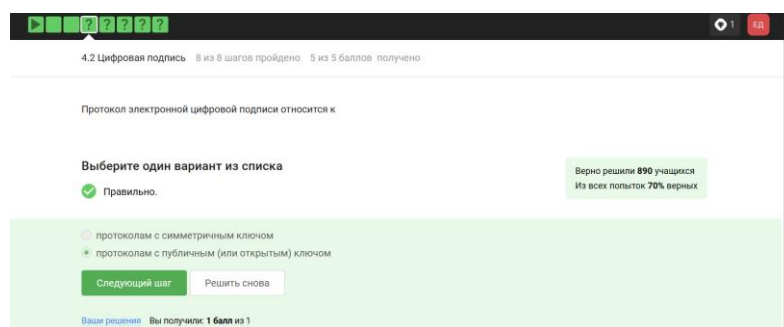


Рис. 6: Вопрос 4.2.1

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. 7).

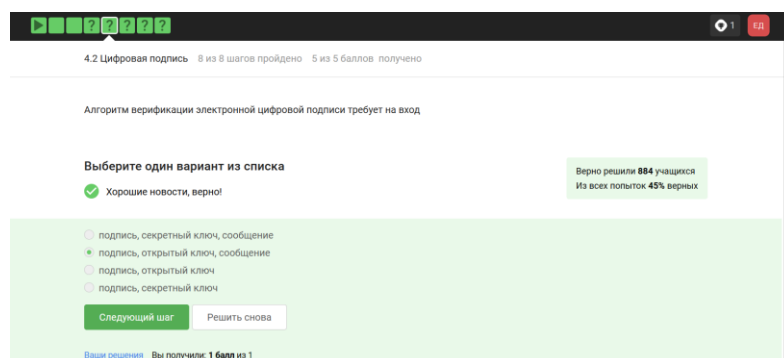


Рис. 7: Вопрос 4.2.2

Электронная подпись обеспечивает все указанное, кроме конфиденциальности (рис. 8).

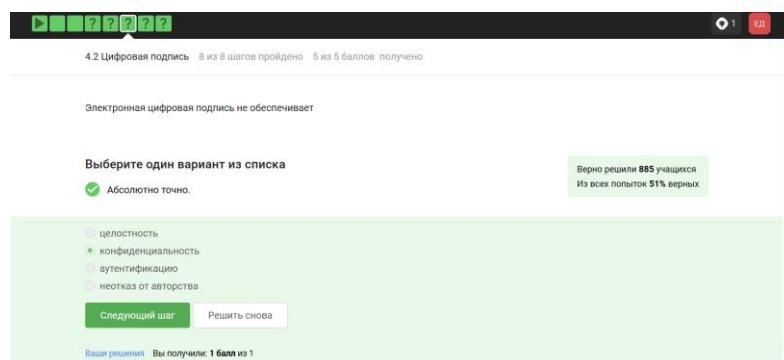


Рис. 8: Вопрос 4.2.3

Для отправки налоговой отчетности в ФНС используется усиленная квалифицированная электронная подпись (рис. 9).

4.2 Цифровая подпись 8 из 8 шагов пройдено 5 из 5 баллов получено

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

Выберите один вариант из списка

Отлично!

Верно решили 885 учащихся  
Из всех попыток 67% верных

- ☒ усиленная квалифицированная
- ☐ усиленная неквалифицированная
- ☐ простая

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 9: Вопрос 4.2.4

Верный ответ указан на изображении (рис. 10).

4.2 Цифровая подпись 8 из 8 шагов пройдено 5 из 5 баллов получено

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

Выберите один вариант из списка

Отлично!

Верно решили 883 учащихся  
Из всех попыток 60% 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 из 1

Рис. 10: Вопрос 4.2.5

## 2.3 Электронные платежи

Известные платежные системы - Visa, MasterCard, МИР (рис. 11).

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

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

✓ Здорово, всё верно.

Верно решили 814 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.

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 11: Вопрос 4.3.1

Верный ответ на изображении (рис. 12).

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

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✓ Отлично!

Верно решили 800 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.

- ☐ комбинация проверки пароля + Калча
- ☒ 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. 12: Вопрос 4.3.2

При онлайн платежах используется многофакторная аутентификация (рис. 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

✓ Так точно!

Верно решили 859 учащихся  
Из всех попыток 59% верных

- \* 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. 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. 14).

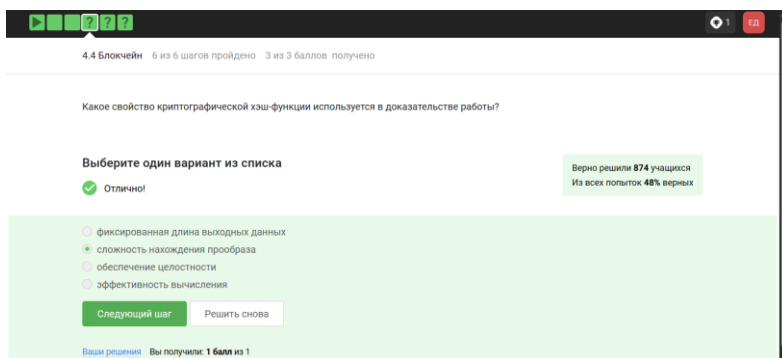


Рис. 14: Вопрос 4.4.1

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. 15).

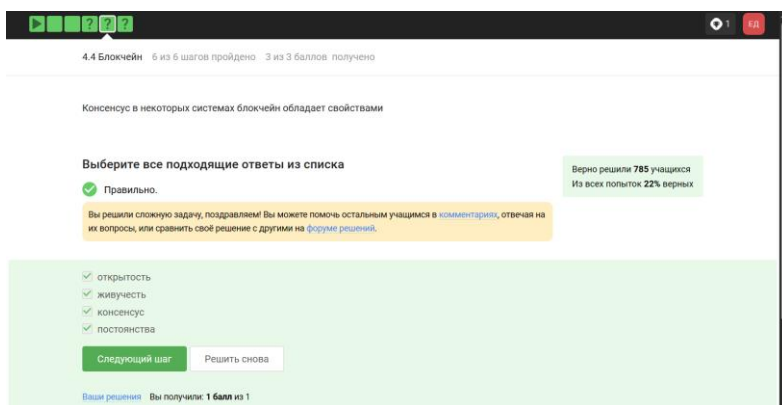


Рис. 15: Вопрос 4.4.2

Ответ - цифровая подпись (рис. 16).

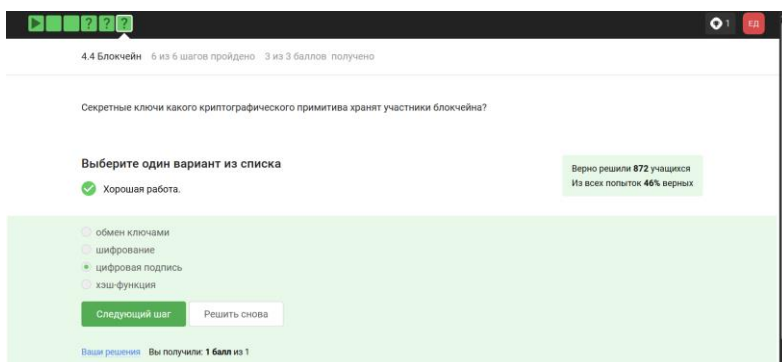


Рис. 16: Вопрос 4.4.3

### **3      Выводы**

Я прошла третий блок