

Внешний курс. Блок 3: Криптография на практике

Основы информационной безопасности

Петрова Алевтина Александровна

Содержание

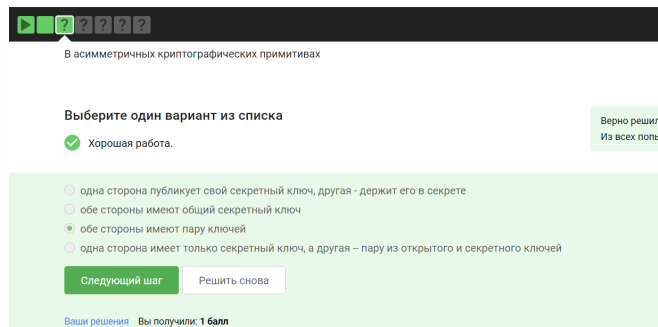
1 Цель работы

Пройти третий блок курса “Основы кибербезопасности”

2 Выполнение блока 3: Криптография на практике

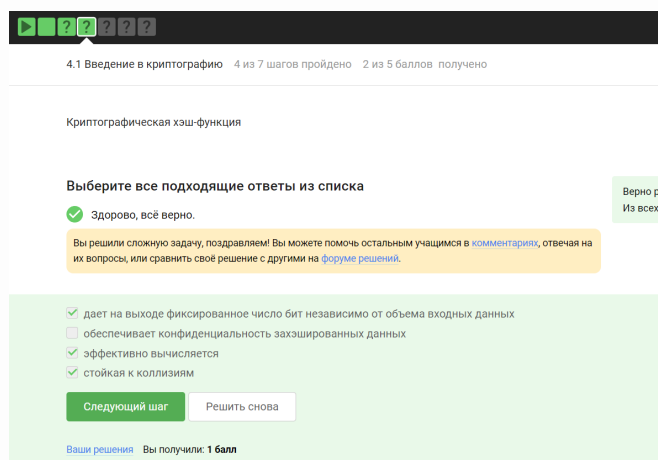
2.1 Введение в криптографию

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



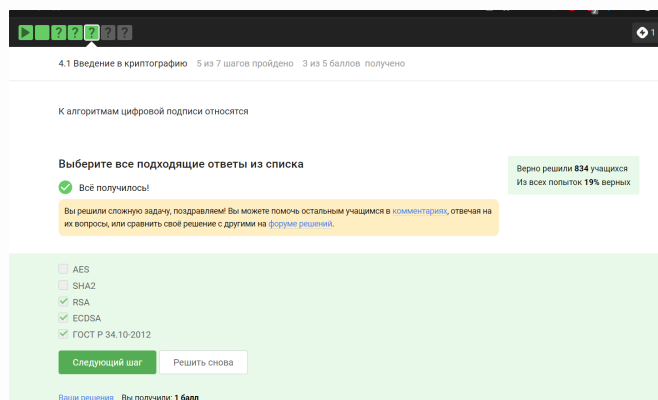
Вопрос 4.1.1

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



Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (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 6 из 7 шагов пройдено 4 из 5 баллов получено

Код аутентификации сообщения относится к

Выберите один вариант из списка

☒ Абсолютно точно.

☐ симметричным примитивам

☐ асимметричным примитивам

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

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

☒ 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

Вопрос 4.1.5

2.2 Цифровая подпись

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

4.2 Цифровая подпись 4 из 8 шагов пройдено 1 из 5 баллов получен

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Верно.

☐ протоколам с симметричным ключом

☐ протоколам с публичным (или открытым) ключом

Следующий шаг Решить снова

Ваши решения Вы получили: ...

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, содержа-

щейся 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).

4.2 Цифровая подпись 5 из 8 шагов пройдено 2 из 5 баллов получено

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

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Всё получилось!

[Верно решил](#)
Из всех по

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

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: ...

Вопрос 4.2.2

Электронная подпись обеспечивает все указанное, кроме конфиденциальности (рис. 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

☒ Абсолютно точно.

[Верно решили 968 учащихся](#)
Из всех попыток 53% верных

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

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: 1 балл

Вопрос 4.2.3

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

4.2 Цифровая подпись 7 из 8 шагов пройдено 4 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

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

Выберите один вариант из списка

☒ Хорошая работа.

☐ усиленная неквалифицированная

☒ усиленная квалифицированная

☐ простая

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

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

Вы прошли больше 80% курса, оставьте отзыв

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

Выберите один вариант из списка

☒ Здорово, всё верно.

☐ в любой организации, имеющей соответствующую лицензию ФСБ

☐ в минкомсвязи РФ

☒ в удостоверяющем (сертификационном) центре

☐ в любой организации по месту работы

Следующий шаг Решить снова

Верно решил 971 учащийся
Из всех попыток 61% верных

Ваши решения Вы получили: 1 балл

Вопрос 4.2.5

2.3 Электронные платежи

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

4.3 Электронные платежи 3 из 5 шагов пройдено 1 из 3 баллов получен

Вы прошли больше 80% курса, оставьте отзыв

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

☒ Всё правильно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на их вопросы, или сравнить свое решение с другими на [форуме решений](#).

☐ BitCoin

☒ MasterCard

☐ SecurePay

☐ POS-терминал

☐ банкомат

☒ МИР

Следующий шаг Решить снова

Верно решил 971 учащийся
Из всех попыток 61% верных

Вопрос 4.3.1

Верный ответ на изображении (рис. 12).

4.3 Электронные платежи 4 из 5 шагов пройдено 2 из 3 баллов получено

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

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✓ Хорошие новости, 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](#).

Верно решили Из всех попыток 59% верных

☐ 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

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

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

При онлайн платежах сегодня используется

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили 957 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

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).

4.4 Блокчейн 4 из 6 шагов пройдено 1 из 3 баллов получен

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

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

✓ Отлично!

Верно решили
Из всех попыток

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

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: 1 балл

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. 15).

4.4 Блокчейн 5 из 6 шагов пройдено 2 из 3 баллов получено

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

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

✓ Прекрасный ответ.

Верно решили
Из всех попыток

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на их вопросы, или сравнить свое решение с другими на [форуме решений](#).

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

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: 1 балл

Вопрос 4.4.2

Ответ - цифровая подпись (рис. 16).

4.4 Блокчейн 6 из 6 шагов пройдено 3 из 3 баллов получено

Вы прошли больше 80% курса, оставьте отзыв [Ост](#)

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

✓ Всё получилось!

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

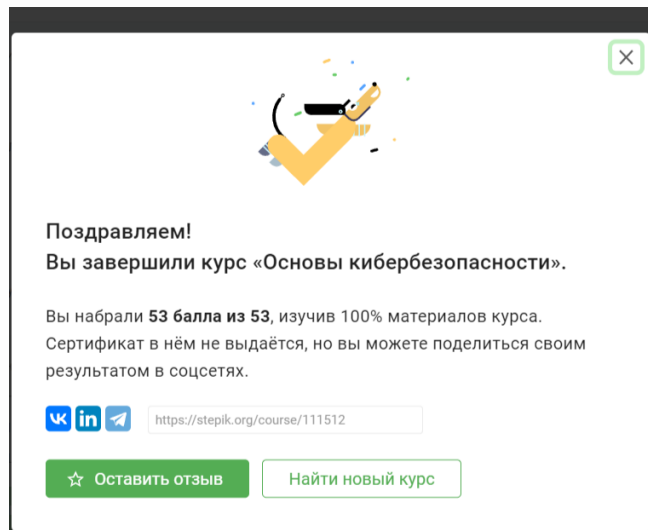
[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: 1 балл

Вопрос 4.4.3

3 Выводы

Третий блок пройден успешно



Итоги