

Внешний курс. Блок 3: Криптография на практике

Воинов Кирилл



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

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Правильно, молодец!

Верно решили **940** учащихся
Из всех попыток **42%** верных

- ☐ одна сторона публикует свой секретный ключ, другая - держит его в секрете
- ☐ одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей
- ☐ обе стороны имеют общий секретный ключ
- ☒ обе стороны имеют пару ключей

Следующий шаг

Решить снова

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

33 10

Шаг 3

Следующий шаг >

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

✓ Правильно.

Верно решили **798** учащихся
Из всех попыток **11%** верных

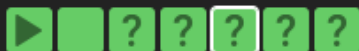
Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

- ☒ стойкая к коллизиям
- ☒ эффективно вычисляется
- ☒ дает на выходе фиксированное число бит независимо от объема входных данных
- ☐ обеспечивает конфиденциальность захешированных данных

Следующий шаг

Решить снова

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



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

☒ Так точно!

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 **834** учащихся
Из всех попыток **19%** верных

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

Следующий шаг

Решить снова

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

33 10

Шаг 5

Следующий шаг >



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

☒ Так точно!

☐ симметричным примитивам

☐ асимметричным примитивам

Следующий шаг

Решить снова

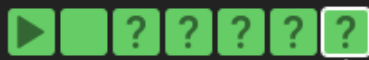
[Ваши решения](#) Вы получили: 1 балл

Верно решили **955** учащихся
Из всех попыток **69%** верных

33 10

Шаг 6

Следующий шаг >



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

☒ Абсолютно точно.

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

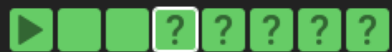
Решить снова

[Ваши решения](#) Вы получили: ...

33 10

Шаг 7

Следующий шаг >



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

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка



Правильно, молодец!

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**



29



3

Шаг 4

Следующий шаг >



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

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Правильно, молодец!

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

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

29 3

Шаг 5

Следующий шаг >



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

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка



Отлично!

Верно решили **968** учащихся
Из всех попыток **53%** верных

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

Следующий шаг

Решить снова

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

29 3

Шаг 6

Следующий шаг >



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

☒ Так точно!

- ☐ усиленная неквалифицированная
- ☒ усиленная квалифицированная
- ☐ простая

Следующий шаг

Решить снова

Верно решили **975** учащихся
Из всех попыток **68%** верных

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

29 3

Шаг 7

Следующий шаг >



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

☒ Абсолютно точно.

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**

29 3

Шаг 8

Следующий шаг >

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

✓ Прекрасный ответ.

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 **900** учащихся
Из всех попыток **24%** верных

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

Следующий шаг Решить снова

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



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

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

☒ Абсолютно точно.

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 **896** учащихся
Из всех попыток **24%** верных

- ☐ 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**

26 2

Шаг 4

Следующий шаг >



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

При онлайн платежах сегодня используется

Выберите один вариант из списка

☒ Отличное решение!

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**

26 2

Шаг 5

Следующий шаг >



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

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

☒ Так точно!

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

Следующий шаг

Решить снова

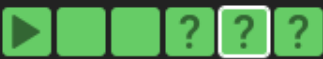
Верно решили **932** учащихся
Из всех попыток **49%** верных

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

35 3

Шаг 4

Следующий шаг >



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

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

☒ Всё получилось!

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 **864** учащихся
Из всех попыток **23%** верных

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

Следующий шаг

Решить снова

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

35 3

Шаг 5

Следующий шаг >



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

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Абсолютно точно.

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

Следующий шаг

Решить снова

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

Верно решил **951** учащийся
Из всех попыток **48%** верных

36 3

Шаг 6

Следующий шаг >