

Прохождения внешнего курса на тему Основы кибербезопасности. Часть 3

Основы информационной безопасности

Тойчубекова Асель Нурлановна

Содержание

1	4 Криптография на практике	5
1.1	4.1 Введение в криптографию	5
1.2	4.2 Цифровая подпись	8
1.3	4.3 Электронные платежи	12
1.4	4.4 Блокчейн	14

Список иллюстраций

1.1	Вопрос/Ответ 1	5
1.2	Вопрос/Ответ 2	6
1.3	Вопрос/Ответ 3	6
1.4	Вопрос/Ответ 4	7
1.5	Вопрос/Ответ 5	8
1.6	Вопрос/Ответ 1	9
1.7	Вопрос/Ответ 2	9
1.8	Вопрос/Ответ 3	10
1.9	Вопрос/Ответ 4	11
1.10	Вопрос/Ответ 5	11
1.11	Вопрос/Ответ 1	12
1.12	Вопрос/Ответ 2	13
1.13	Вопрос/Ответ 3	14
1.14	Вопрос/Ответ 1	14
1.15	Вопрос/Ответ 2	15
1.16	Вопрос/Ответ 3	16

Список таблиц

1 4 Криптография на практике

1.1 4.1 Введение в криптографию

Вопрос/Ответ 1 (рис. 1.1)

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Абсолютно точно.

- ☒ обе стороны имеют пару ключей
- ☐ 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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 1.1: Вопрос/Ответ 1

Пояснение ответа: В асимметричных криптографических примитивах обе стороны имеют пару ключей, у каждого из сторон есть пара ключей: открытый ключ и секретный ключ. Открытый ключ публикуется в открытом доступе, а закрытый или секретный сторона хранит у себя.

Вопрос/Ответ 2 (рис. 1.2)

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

☒ Здорово, всё верно.

Верн
Из в

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
- ☒ стойкая к коллизиям
- ☐ обеспечивает конфиденциальность зашифрованных данных
- ☒ эффективно вычисляется

Следующий шаг

Решить снова

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

Рис. 1.2: Вопрос/Ответ 2

Пояснение ответа: Криптографическая хэш-функция:

- Дает на выход фиксированное число бит независимо от объема входных данных
- Стойкая к коллизиям
- Эффективно вычисляется

Вопрос/Ответ 3 (рис. 1.3)

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

☒ Всё правильно.

Всё
Из

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. 1.3: Вопрос/Ответ 3

Пояснение ответа: К алгоритмам цифровой подписи относятся: RSA, ECDSA, ГОСТ 34.10-2012

Вопрос/Ответ 4 (рис. 1.4)

Код аутентификации сообщения относится к

Выберите один вариант из списка

☒ Хорошая работа.

- ☒ симметричным примитивам
- ☐ асимметричным примитивам

Следующий шаг

Решить снова

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

Рис. 1.4: Вопрос/Ответ 4

Пояснение ответа: Код аутентификации сообщения относится к симметричным примитивам, так как имеется общий ключ.

Вопрос/Ответ 5 (рис. 1.5)

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

✓ Отличное решение!

- ☐ 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. 1.5: Вопрос/Ответ 5

Пояснение ответа: Обмен ключами Диффи-Хэллмана-это асимметричный примитив генерации общего секретного ключа.

1.2 4.2 Цифровая подпись

Вопрос/Ответ 1 (рис. 1.6)

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Здорово, всё верно.

- ☐ протоколам с симметричным ключом
- ☒ протоколам с публичным (или открытым) ключом

Следующий шаг

Решить снова

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

Рис. 1.6: Вопрос/Ответ 1

Пояснение ответа: Протокол электронной цифровой подписи относится протоколам с публичным (или открытым) ключом.

Вопрос/Ответ 2 (рис. 1.7)

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Верно. Так держать!

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

Следующий шаг

Решить снова

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

Рис. 1.7: Вопрос/Ответ 2

Пояснение ответа: Алгоритм верификации электронной цифровой подписи требует на вход:

- подпись
- открытый ключ
- сообщение

Вопрос/Ответ 3 (рис. 1.8)

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

☒ Хорошая работа.

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

Следующий шаг

Решить снова

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

Рис. 1.8: Вопрос/Ответ 3

Пояснение ответа: Цифровая подпись предназначена для:

- Обеспечение целостности сообщения(любое изменение сообщения будет обнаружено)
- Аутентификации сообщения(устанавливается принадлежность подписи владельцу)
- Неотказ от авторства(невозможно отказаться от факта подписи в будущем)

Вопрос/Ответ 4 (рис. 1.9)

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

Выберите один вариант из списка

✓ Всё получилось!

☒ усиленная квалифицированная
☐ усиленная неквалифицированная
☐ простая

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 1.9: Вопрос/Ответ 4

Пояснение ответа: Усиленной квалифицированной:

- равнозначно рукописей
- подтверждается сертификатом, выпущенным организацией, аккредитованной минкомсвязи РФ
- госуслуги, государственный документооборот

Вопрос/Ответ 5 (рис. 1.10)

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

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решил 9
Из всех попыт

☐ 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. 1.10: Вопрос/Ответ 5

Пояснение ответа: В удостоверяющем(сертификационном) центре можно получить квалифицированный сертификат ключа проверки электронной записи.

1.3 4.3 Электронные платежи

Вопрос/Ответ 1 (рис. 1.11)

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

☒ Верно. Так держать!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в 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. 1.11: Вопрос/Ответ 1

Пояснение ответа: МИР и MasterCard являются платежными системами.

Вопрос/Ответ 2 (рис. 1.12)

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✓ Отличное решение!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащим 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. 1.12: Вопрос/Ответ 2

Пояснение ответа: Многократная аутентификация заключается в том, что мы доказываем в ходе этого протокола несколько вещей есть. Основные категории вещей, которые мы можем доказать:

1. то, что я знаю-это либо пароль,либо пин код, либо в случае онлайн платежей это секретный код
2. конкретно в онлайн платежах мы используем второй фактор-это то, чем я владею, который вы должны подтвердить или вбить в ваш браузер
3. другой фактор аутентификации-это свойства например биометрия,отпечаток пальца
4. четвертый фактор аутентификации -локация.

Вопрос/Ответ 3 (рис. 1.13)

При онлайн платежах сегодня используется

Выберите один вариант из списка

✓ Отлично!

- ☒ 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. 1.13: Вопрос/Ответ 3

Пояснение ответа: При онлайн платежах сегодня используется многофакторная аутентификация покупателя перед банком-эмитентом

1.4 4.4 Блокчейн

Вопрос/Ответ 1 (рис. 1.14)

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

✓ Здорово, всё верно.

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

Следующий шаг

Решить снова

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

Рис. 1.14: Вопрос/Ответ 1

Пояснение ответа: Сложность нахождения прообраза криптографической хэш

функции используется в доказательстве работы.

Вопрос/Ответ 2 (рис. 1.15)

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

✓ Всё правильно.

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

- ✓ консенсус
- ✓ открытость
- ✓ живучесть
- ✓ постоянства

[Следующий шаг](#) [Решить снова](#)

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

Рис. 1.15: Вопрос/Ответ 2

Пояснение ответа: В основе блокчейна лежит консенсус- публичная структура данных или леджер(бухгалтерская книга), которая обеспечивает:

- постоянство(добавленные когда-либо данные не могут быть удалены)
- консенсус(все участники видят одни и те же данные за исключением пары блоков)
- живучесть(участники могут добавлять новые транзакции)
- открытость(любой может стать участником блокчейна)

Вопрос/Ответ 3 (рис. 1.16)

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

✓ Всё правильно.

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

Следующий шаг

Решить снова

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

Рис. 1.16: Вопрос/Ответ 3

Пояснение ответа: Участники блокчейна хранят секретные ключи цифровой подписи каждой транзакции, эта подпись доказывает, что транзакция создана владельцем средств. Только владелец приватного ключа может распорядиться средствами, хранящимися на связанном адресе.