

Основы кибербезопасности

Этап 3

Ведьмина Александра Сергеевна

Содержание

1	Цель работы	1
2	Выполнение лабораторной работы	1
3	Выводы.....	16

1 Цель работы

Выполнить задания третьей части курса по кибербезопасности.

2 Выполнение лабораторной работы

Два ключа - исходя из определения ассимитричного шифрования.

В ассиметричных криптографических примитивах

Выберите один вариант из списка

✓ Правильно, молодец!

- ☒ 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

Рис. 1: Задание 1

По свойствам хэш-функции.

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

☒ Верно. Так держать!

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
- ☐ обеспечивает конфиденциальность зашифрованных данных
- ☒ дает на выходе фиксированное число бит независимо от объема входных данных

Рис. 2: Задание 2

Алгоритмы:

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

☒ Отлично!

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. 3: Задание 3

Так как для шифровки и дешифровки используется один и тот же ключ.

Вы прошли больше 80% курса, оставьте отзыв

Код аутентификации сообщения относится к

Выберите один вариант из списка

 Правильно.

- ☒ симметричным примитивам
- ☐ асимметричным примитивам

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: ...



33



10

Шаг 6

Рис. 4: Задание 4

По определению этого алгоритма.

Вы прошли больше 80% курса, оставьте отзыв

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

✓ Хорошие новости, верно!

- ☐ 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. 5: Задание 5

Потому что используется ассиметричное шифрование.

Вы прошли больше 80% курса, оставьте отзыв

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Правильно.

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

Следующий шаг

Решить снова

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



28



3

Шаг 4

Рис. 6: Задание 6

Подписанное сообщение проверяется открытым ключом.

Вы прошли больше 80% курса, оставьте отзыв

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Хорошие новости, верно!

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: ...

Рис. 7: Задание 7

Она наоборот гарантирует, что можно определить, кто подписал.

Вы прошли больше 80% курса, оставьте отзыв

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

 **Правильно, молодец!**

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: ...

Рис. 8: Задание 8

Так как в налоговую нужны юридически значимые документы.

Вы прошли больше 80% курса, оставьте отзыв

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

Выберите один вариант из списка

☒ Всё правильно.

☐ усиленная неквалифицированная

☒ усиленная квалифицированная

☐ простая

Следующий шаг

Решить снова

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


Рис. 9: Задание 9

В сертифицированном центре.

Вы прошли больше 80% курса, оставьте отзыв

В какой организации вы можете получить квалифицированный сертификат ключа проверки электрон

Выберите один вариант из списка

 Отлично!

- ☐ 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: ...

Рис. 10: Задание 10

МИР и Mastercard всем известны.

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

☒ Хорошая работа.

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. 11: Задание 11

Отметила верные методы.

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

☒ Здорово, всё 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](#).

- ☐ 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: ...

Рис. 12: Задание 12

Используется многофакторная аутентификация.

При онлайн платежах сегодня используется

Выберите один вариант из списка

☒ Прекрасный ответ.

- ☒ 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: ...



25



2

Шаг 5

Рис. 13: Задание 13

Прообраз действительно сложно найти, поэтому она надёжна.

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

☒ Всё правильно.

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: ...



33



3

Шаг 4

Рис. 14: Задание 14

По свойствам консенсуса.

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

☒ Верно. Так держать!

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](#).

☒ постоянства

☒ консенсус

☒ открытость

☒ живучесть

Следующий шаг

Решить снова

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

Рис. 15: Задание 15

Они хранят цифровые подписи.

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Правильно.

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

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: ...



33



3

Шаг 6

Рис. 16: Задание 16

Ура, я завершила курс!

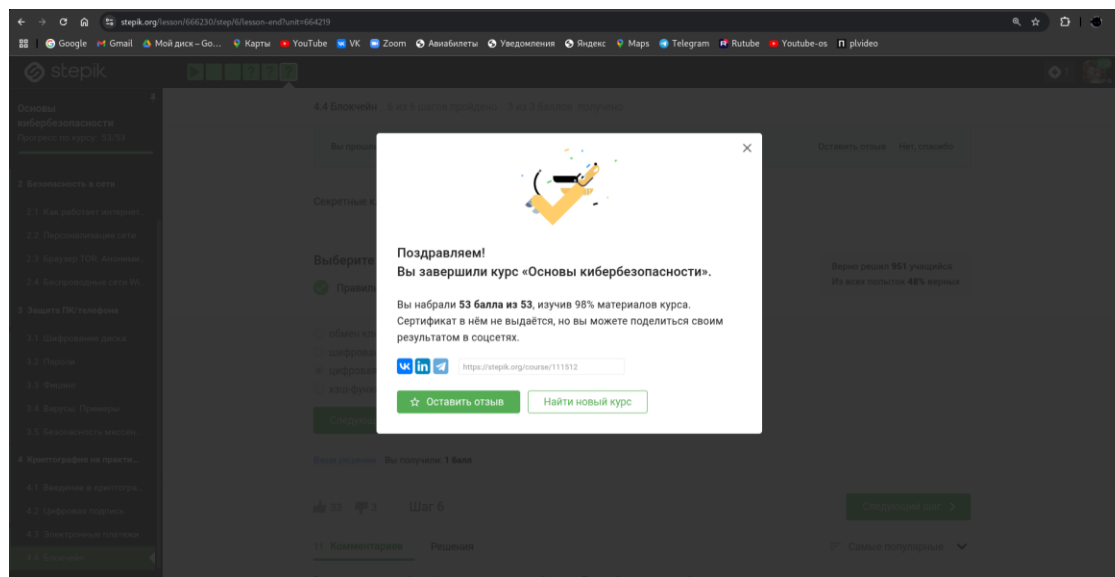


Рис. 17: Задание 17

3 Выводы

Все задания третьей части выполнены. Курс завершён.