

Отчёт по Внешнему Курсу - Этап 3

Основы информационной безопасности

Чистов Даниил Максимович

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Выводы	13
4	Список литературы	14

Список иллюстраций

2.1	Задание 001	5
2.2	Задание 002	5
2.3	Задание 003	6
2.4	Задание 004	6
2.5	Задание 005	7
2.6	Задание 006	7
2.7	Задание 007	7
2.8	Задание 008	8
2.9	Задание 009	8
2.10	Задание 010	8
2.11	Задание 011	9
2.12	Задание 012	9
2.13	Задание 013	10
2.14	Задание 014	10
2.15	Задание 015	11
2.16	Задание 016	11
2.17	Курс успешно пройден	12

1 Цель работы

Пройти внешний курс - Этап 3

2 Выполнение лабораторной работы

В лекционных материалах было сказано, что в протоколы прикладного уровня включён HTTPS (рис. 2.1).

Выберите один вариант из списка

Верно решили 940 учащихся
Из всех попыток 42% верных

✓ Правильно, молодец!

- ☐ обе стороны имеют общий секретный ключ
- ☐ 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 пару ключей

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

👍 34 🗳️ 10 Шаг 3 Следующий шаг >

Комментарии Решения

Рис. 2.1: Задание 001

Обе стороны имеют публичный ключ и секретный ключ, одна сторона открывает публичный ключ, а другая использует его для шифрования, но только владелец секретного ключа его расшифровывает (рис. 2.2).

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

Верно решили 798 учащихся
Из всех попыток 11% верных

✓ 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](#).

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.2: Задание 002

Всё подходит, но очевидно, что хэш-функция не обеспечивает конфиденциальность (рис. 2.3).

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

✓ Здорово, всё верно.

Верно решили 834 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

Рис. 2.3: Задание 003

Первые два ответа - никак не относятся к цифровой подписи, это алгоритм симметричного шифрования (AES) и хэш-функция (рис. 2.4).

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Отлично!

Верно решили 955 учащихся
Из всех попыток 69% верных

☐ асимметричным примитивам
☒ симметричным примитивам

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.4: Задание 004

Т.к. обе стороны по сути проверяются по одному ключу, следовательно это симметричная криптография (рис. 2.5).

Обмен ключам Диффи-Хеллмана - это

Выберите один вариант из списка

✓ Всё получилось!

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: 1 балл

Рис. 2.5: Задание 005

Асимметричный, т.к. у каждой стороны и свой секретная и открытая часть, и он устанавливает ключ, но не шифрует (рис. 2.6).

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

✓ Отлично!

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

Рис. 2.6: Задание 006

Т.к. для подписей используется асимметричная криптография, следовательно это публичный протокол (рис. 2.7).

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

✓ Так точно!

Верно решили 962 учащихся
Из всех попыток 46% верных

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.7: Задание 007

Открытый ключ используется для расшифровки подписи, подпись это зашифрованный хэш, ну и сам хэш (рис. 2.8).

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

✓ Правильно.

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

Рис. 2.8: Задание 008

Конфиденциальность не обеспечивается, т.к. сообщение не шифруется (рис. 2.9).

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

Выберите один вариант из списка

✓ Верно. Так держаты!

Верно решили 975 учащихся
Из всех попыток 68% верных

- ☐ усиленная неквалифицированная
- ☐ простая
- ☒ усиленная квалифицированная

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.9: Задание 009

Она создаётся с использование сертифицированных средств криптозащиты, а также имеет юридическую силу, что важно при работе с государством (рис. 2.10).

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

Выберите один вариант из списка

✓ Правильно, молодец!

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

Рис. 2.10: Задание 010

Такие центры именно для этого и созданы, когда речь идёт о безопасности - это наилучший вариант, чем позволять выдавать сертификаты каждой желающей организации (рис. 2.11).

Выберите из списка все платёжные системы.

Выберите все подходящие ответы из списка

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 900 учащихся
Из всех попыток 24% верных

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.11: Задание 011

SecurePay не считается, т.к. это электронная платёжная система, по сути и Bitcoin по этому не считается (рис. 2.12).

Примером многофакторной аутентификации является

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](#).

Верно решили 896 учащихся
Из всех попыток 24% верных

- ☐ комбинация проверки пароля + Капча
- ☒ комбинация проверки 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. 2.12: Задание 012

Капча лишь может предотвратить (и то не всегда) автоматизированную атаку, а PIN-код + пароль тоже можно подобрать и не нужно иметь доступ к чему-нибудь стороннему (например, телефону) (рис. 2.13).

При онлайн платежах сегодня используется

Выберите один вариант из списка

✓ Здорово, всё верно.

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

Рис. 2.13: Задание 013

Банк-эмитент - тот, кто выпустил карту, следовательно он несёт ответственность за аутентификацию пользователя, также используется многофакторная аутентификация - что-то, что знает пользователь + что-то, что этот пользователь имеет (телефон) (рис. 2.14).

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили 932 учащихся
Из всех попыток 49% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.14: Задание 014

При нахождении потребуется очень много вычислений, переборов - оттого и сложность, однако проверка результата будет быстрой (рис. 2.15).

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

Отлично!

Верно решили 864 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](#).

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.15: Задание 015

Подходят все варианты (рис. 2.16).

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

Абсолютно точно.

Верно решил 951 учащийся
Из всех попыток 48% верных

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.16: Задание 016

Курс успешно пройден (рис. 2.17).

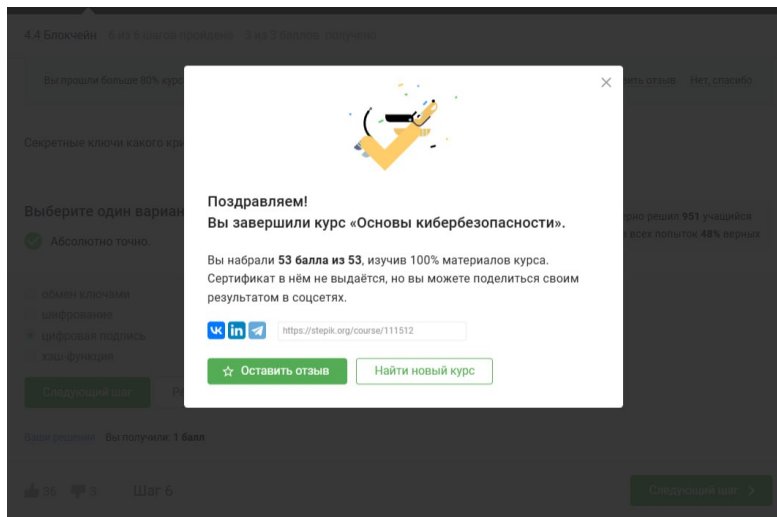


Рис. 2.17: Курс успешно пройден

3 Выводы

Этап 3 пройден успешно на максимальный балл.

4 Список литературы

Курс “Основы Кибербезопасности” на платформе Stepik