

Отчёт по Внешнему Курсу - Этап 3

Основы информационной безопасности

Чистов Д. М.

17 мая 2025

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

Цель работы

Пройти внешний курс - Этап 3

Выполнение лабораторной работы

В лекционных материалах было сказано, что в протоколы прикладного уровня включён HTTPS

Выберите один вариант из списка

✓ Правильно, молодец!

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

☐ 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. 1: Задание 001

3/21

Выполнение лабораторной работы

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

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

☒ Здорово, всё верно.

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](#).

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 2: Задание 002

Всё подходит, но очевидно, что хэш-функция не обеспечивает конфиденциальность

К алгоритмам цифровой подписи относятся

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](#).

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

[Ваше решение](#) Вы получили: **1 балл**

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

[Следующий шаг](#) [Решить снова](#)

Рис. 3: Задание 003

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

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. 4: Задание 004

Т.к. обе стороны по сути проверяются по одному ключу, следовательно это симметричная криптография

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

☒ Всё получилось!

☐ 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**

Верно решили **948** учащихся
Из всех попыток **47%** верных

Рис. 5: Задание 005

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

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Отлично!

☐ протоколам с симметричным ключом

☒ протоколам с публичным (или открытым) ключом

[Следующий шаг](#) [Решить снова](#)

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

Верно решили **956** учащихся
Из всех попыток **71%** верных

Рис. 6: Задание 006

Т.к. для подписей используется асимметричная криптография, следовательно это публичный протокол

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Так точно!

☐ подпись, открытый ключ, сообщение
☐ подпись, секретный ключ, сообщение
☐ подпись, открытый ключ
☐ подпись, секретный ключ

[Следующий шаг](#) [Решить снова](#)

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

Верно решили **962** учащихся
Из всех попыток **46%** верных

Рис. 7: Задание 007

Открытый ключ используется для расшифровки подписи, подпись это зашифрованный хэш, ну и сам хэш

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. 8: Задание 008

Конфиденциальность не обеспечивается, т.к. сообщение не шифруется

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

Выберите один вариант из списка

☒ Верно. Так держать!

☐ усиленная неквалифицированная

☐ простая

☐ усиленная квалифицированная

[Ваше решение](#) Вы получили: **1 балл**

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

Следующий шаг Решить снова

Рис. 9: Задание 009

Она создаётся с использованием сертифицированных средств криптозащиты, а также имеет юридическую силу, что важно при работе с государством

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

Выберите один вариант из списка

☒ Правильно, молодец!

Верно решил **971** учащихся
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. 10: Задание 010

Выполнение лабораторной работы

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

Выберите из списка все платёжные системы.

Выберите все подходящие ответы из списка

☒ Верно.

Верно решили **900** учащихся
Из всех попыток **24%** 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](#).

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 11: Задание 011

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

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](#).

☐ комбинация проверки пароля + Капча
☒ комбинация проверка пароля + код в sms сообщении
☒ комбинация код в sms сообщении + отпечаток пальца
☐ комбинация PIN код + пароль

[Ваше решение](#) Вы получили: **1 балл**

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

[Следующий шаг](#) [Решить снова](#)

Рис. 12: Задание 012

Выполнение лабораторной работы

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)

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. 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)

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. 14: Задание 014

Выполнение лабораторной работы

При нахождении потребуется очень много вычислений, переборов - оттого и сложность, однако проверка результата будет быстрой

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. 15: Задание 015

Подходят все варианты

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. 16: Задание 016

Курс успешно пройден

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

Вы прошли больше 80% курса

Секретные ключи какого крипто...

Выберите один вариант ответа

☒ Абсолютно точно.

☐ обмен ключами

☐ шифрование

☒ цифровая подпись


☐ хэш-функция

Следующий шаг

Ваше решение: Вы получили: 1 балл




36 3 Шаг 6

Следующий шаг >



Поздравляем!
Вы завершили курс «Основы кибербезопасности».

Вы набрали **53 балла из 53**, изучив 100% материалов курса.
Сертификат в нём не выдаётся, но вы можете поделиться своим результатом в соцсетях.

☆ Оставить отзыв

Найти новый курс

Выводы

Этап 3 пройден успешно на максимальный балл.

Список литературы

Курс “Основы Кибербезопасности” на платформе Stepik