

Отчет по части “Безопасность в сети” курса “Основы кибербезопасности”

Стариков Данила Андреевич

Содержание

| | |
|--|-----------|
| Цель работы | 3 |
| 1 Первый модуль. Безопасность в сети. | 4 |
| 1.1 Как работает интернет: базовые сетевые протоколы | 4 |
| 1.2 Персонализация сети | 11 |
| 1.3 Браузер TOR. Анонимизация | 14 |
| 1.4 Беспроводные сети Wi-Fi. | 18 |
| 2 Второй модуль. Защита ПК/Телефона. | 22 |
| 2.1 Шифрование диска | 22 |
| 2.2 Пароли | 24 |
| 2.3 Фишинг | 28 |
| 2.4 Вирусы. Примеры | 30 |
| 2.5 Безопасность мессенджеров | 32 |
| 3 Третий модуль. Криптография на практике. | 34 |
| 3.1 Введение в криптографию | 34 |
| 3.2 Цифровая подпись | 37 |
| 3.3 Электронные платежи | 41 |
| 3.4 Блокчейн | 44 |
| 4 Выводы | 46 |

Цель работы

Цель курса:

- Понять, как происходит передача данных через Интернет, какие уязвимости могут возникнуть
- Разобраться, почему необходимо составлять сложные пароли
- Научиться различать шифрование и цифровую подпись
- Изучать работу электронных платежей

1 Первый модуль. Безопасность в сети.

1.1 Как работает интернет: базовые сетевые протоколы

- Вопрос 1. Выберите протокол прикладного уровня (рис. 1.1):

Ответ: *HTTPS*.

Выберите протокол прикладного уровня

Выберите один вариант из списка

☒ Абсолютно точно.

☐ UDP

☐ TCP

☒ HTTPS

☐ IP

Следующий шаг

Решить снова

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

Рис. 1.1: Скриншот выполнения задания

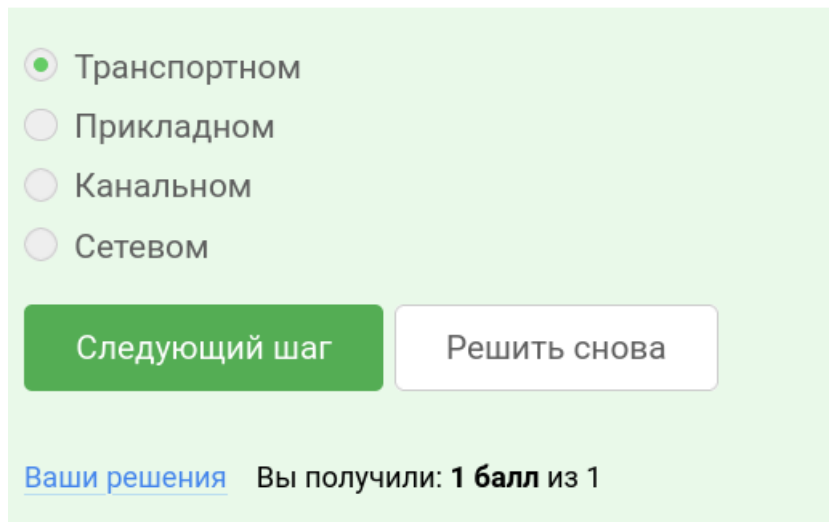
- Вопрос 2. На каком уровне работает протокол TCP? (рис. 1.2)

Ответ: *Транспортном*.

На каком уровне работает протокол TCP?

Выберите один вариант из списка

☒ Всё правильно.



The screenshot shows a quiz interface with a light green background. At the top, there is a list of radio button options: 'Транспортном' (selected), 'Прикладном', 'Канальном', and 'Сетевом'. Below the options are two buttons: a green 'Следующий шаг' button and a white 'Решить снова' button. At the bottom, there is a link 'Ваши решения' and a score display 'Вы получили: 1 балл из 1'.

Рис. 1.2: Скриншот выполнения задания

- Вопрос 3. Выберите все корректные адреса IPv4. (рис. 1.3)

Ответ: *90.11.90.22 и 25.198.0.15.*

Выберите все корректные адреса IPv4

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](#).

☐ 421.0.15.19

☐ 43.12.256.7

☒ 90.11.90.22

☒ 25.198.0.15

Следующий шаг

Решить снова

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

Рис. 1.3: Скриншот выполнения задания

- Вопрос 4. DNS сервер (рис. 1.4)

Ответ: сопоставляет IP адреса доменным именам.

DNS сервер

Выберите один вариант из списка

☒ Всё правильно.

- ☒ сопоставляет IP адреса доменным именам
- ☐ сегментирует данные на транспортном уровне
- ☐ выбирает маршрут пакета в сети
- ☐ выполняет адресацию на хосте

Следующий шаг

Решить снова

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

Рис. 1.4: Скриншот выполнения задания

- Вопрос 5. Выберите корректную последовательность протоколов в модели TCP/IP (рис. 1.5)

Ответ: *прикладной – транспортный – сетевой – канальный.*

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

☒ Здорово, всё верно.

- ☐ сетевой -- прикладной -- канальный -- транспортный
- ☐ прикладной -- транспортный -- канальный -- сетевой
- ☐ транспортный -- сетевой -- прикладной -- канальный
- ☒ прикладной -- транспортный -- сетевой -- канальный

Следующий шаг

Решить снова

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

Рис. 1.5: Скриншот выполнения задания

- Вопрос 6. Протокол http предполагает (рис. 1.6)

Ответ: *передачу данных между клиентом и сервером в открытом виде.*

Протокол http предполагает

Выберите один вариант из списка

☒ Верно.

- ☐ передачу зашифрованных данных между клиентом и сервером
- ☒ передачу данных между клиентом и сервером в открытом виде

Следующий шаг

Решить снова

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

Рис. 1.6: Скриншот выполнения задания

- Вопрос 7. Протокол https состоит из (рис. 1.7)

Ответ: *двух фаз: рукопожатия и передачи данных.*

Протокол https состоит из

Выберите один вариант из списка

☒ Хорошая работа.

- ☐ одной фазы аутентификации сервера
- ☒ двух фаз: рукопожатия и передачи данных
- ☐ двух фаз: аутентификация клиента и сервера и шифрования данных
- ☐ трех фаз: аутентификации клиента, аутентификация сервера, генерация общего ключа

Следующий шаг

Решить снова

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


Рис. 1.7: Скриншот выполнения задания

- Вопрос 8. Версия протокола TLS определяется (рис. 1.8)

Ответ: *и клиентом, и сервером в процессе “переговоров”.*

Версия протокола TLS определяется

Выберите один вариант из списка

 Правильно.

- ☐ сервером
- ☐ клиентом
- ☒ и клиентом, и сервером в процессе “переговоров”
- ☐ провайдером клиента

Следующий шаг

Решить снова

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

Рис. 1.8: Скриншот выполнения задания

- Вопрос 9. В фазе “рукопожатия” протокола TLS не предусмотрено (рис. 1.9)

Ответ: *шифрование данных.*

В фазе “рукопожатия” протокола TLS не предусмотрено

Выберите один вариант из списка

✓ Отлично!

☐ формирование общего секретного ключа между клиентом и сервером

☐ аутентификация (как минимум одной из сторон)

☐ выбираются алгоритмы шифрования/аутентификации

☒ шифрование данных

Следующий шаг Решить снова

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

Рис. 1.9: Скриншот выполнения задания

1.2 Персонализация сети

- Вопрос 1. Куки хранят: (рис. 1.10)

Ответ: *идентификатор пользователя и id сессии*

Куки хранят:

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](#).

☒ идентификатор пользователя

☐ IP адрес

☐ пароль пользователя

☒ id сессии

Следующий шаг Решить снова

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

Рис. 1.10: Скриншот выполнения задания

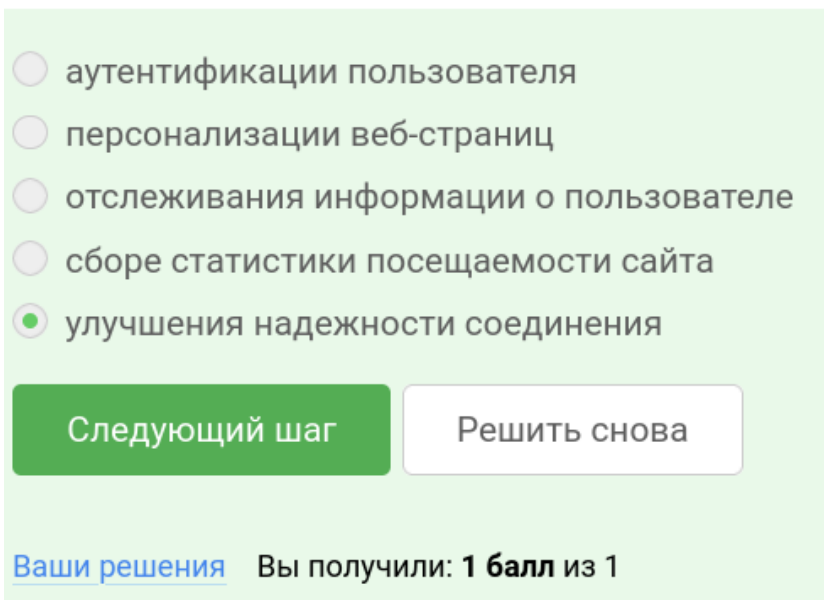
- Вопрос 2. Куки не используются для (рис. 1.11)

Ответ: *улучшения надежности соединения*

Куки не используются для

Выберите один вариант из списка

☒ Всё правильно.



☐ аутентификации пользователя

☐ персонализации веб-страниц

☐ отслеживания информации о пользователе

☐ сборе статистики посещаемости сайта

☒ улучшения надежности соединения

[Следующий шаг](#) [Решить снова](#)

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

Рис. 1.11: Скриншот выполнения задания

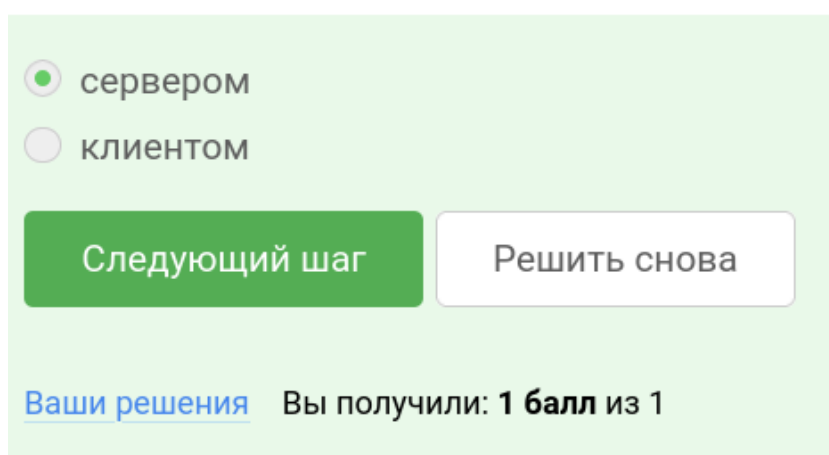
- Вопрос 3. Куки генерируются (рис. 1.12)

Ответ: *сервером*

Куки генерируются

Выберите один вариант из списка

 **Правильно, молодец!**



☒ сервером

☐ клиентом

Следующий шаг **Решить снова**

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

Рис. 1.12: Скриншот выполнения задания

- Вопрос 4. Сессионные куки хранятся в браузере? (рис. 1.13)

Ответ: *Да, на время пользования веб-сайтом*

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

☒ Верно. Так держать!

- ☒ Да, на время пользования веб-сайтом
- ☐ Да, на некоторое время, заданное в сервером
- ☐ Нет

Следующий шаг

Решить снова

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

Рис. 1.13: Скриншот выполнения задания

1.3 Браузер TOR. Анонимизация

- Вопрос 1. Сколько промежуточных узлов в луковой сети TOR? (рис. 1.14)

Ответ: 3

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка



Здорово, всё верно.

☐ 2

☒ 3

☐ 4

Следующий шаг

Решить снова

[Ваши решения](#)

Вы получили: **1 балл** из 1

Рис. 1.14: Скриншот выполнения задания

- Вопрос 2. IP-адрес получателя известен (рис. 1.15)

Ответ: *отправителю и выходному узлу*

IP-адрес получателя известен

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](#).

- ☐ охранному узлу
- ☐ промежуточному узлу
- ☒ отправителю
- ☒ выходному узлу

Следующий шаг

Решить снова

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

Рис. 1.15: Скриншот выполнения задания

- Вопрос 3. Отправитель генерирует общий секретный ключ (рис. 1.16)

Ответ: с охранным, промежуточным и выходном узлом

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

✓ Верно. Так держать!

☐ только с охранном узлом

☐ с охранном и промежуточным узлом

☒ с охранном, промежуточным и выходным узлом

☐ с промежуточным и выходным узлом

[Следующий шаг](#) [Решить снова](#)

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

Рис. 1.16: Скриншот выполнения задания

- Вопрос 4. Должен ли получатель использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов? (рис. 1.17)

Ответ: *Нет*

Должен ли получатель использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов?

Выберите один вариант из списка

✓ Так точно!

[Следующий шаг](#) [Решить снова](#)

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

Верно решил **961** учащихся
Из всех попыток **74%** верно

Рис. 1.17: Скриншот выполнения задания

1.4 Беспроводные сети Wi-Fi.

- Вопрос 1. Wi-Fi - это (рис. 1.18)

Ответ: *технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11*

Wi-Fi - это

Выберите один вариант из списка

✓ Прекрасный ответ.

- ☐ сокращение от "wireless fiber"
- ☒ технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11
- ☐ метод соединения компьютеров по проводной сети Ethernet
- ☐ метод подключения смартфона с глобальной сети Интернет

Следующий шаг

Решить снова

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

Рис. 1.18: Скриншот выполнения задания

- Вопрос 2. На каком уровне работает протокол WiFi? (рис. 1.19)

Ответ: *Канальном*

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

☒ Правильно.

- ☐ Транспортном
- ☐ Прикладном
- ☒ Канальном
- ☐ Сетевом

Следующий шаг

Решить снова

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

Рис. 1.19: Скриншот выполнения задания

- Вопрос 3. Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi (рис. 1.20)

Ответ: *WEP*

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

☒ Так точно!

- ☐ WPA
- ☒ WEP
- ☐ WPA2
- ☐ WPA3

Следующий шаг

Решить снова

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

Рис. 1.20: Скриншот выполнения задания

- Вопрос 4. Данные между хостом сети (компьютером или смартфоном) и роутером (рис. 1.21)

Ответ: *передаются в зашифрованном виде после аутентификации устройств*

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

☒ Отличное решение!

- ☐ передаются в открытом виде
- ☒ передаются в зашифрованном виде после аутентификации устройств
- ☐ передаются в открытом виде после аутентификации устройств
- ☐ передаются в зашифрованном виде

Следующий шаг

Решить снова

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

Рис. 1.21: Скриншот выполнения задания

- Вопрос 5. Для домашней сети для аутентификации обычно используется метод (рис. 1.22)

Ответ: *WPA2 Personal*

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

☒ Правильно, молодец!

- ☒ WPA2 Personal
☐ WPA2 Enterprise

Следующий шаг

Решить снова

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

Рис. 1.22: Скриншот выполнения задания

2 Второй модуль. Защита ПК/Телефона.

2.1 Шифрование диска

- Вопрос 1. Можно ли зашифровать загрузочный сектор диска (рис. 2.1)

Ответ: *Да*.

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Всё получилось!

☐ Да

☐ Нет

Следующий шаг

Решить снова

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

Рис. 2.1: Скриншот выполнения задания

- Вопрос 2. Шифрование диска основано на (рис. 2.2)

Ответ: *симметричном шифровании.*

Шифрование диска основано на

Выберите один вариант из списка

☒ Здорово, всё верно.

☐ хэшировании

☒ симметричном шифровании

☐ асимметричном шифровании

Следующий шаг

Решить снова

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

Рис. 2.2: Скриншот выполнения задания

- Вопрос 3. С помощью каких программ можно зашифровать жесткий диск?
(рис. 2.3)

Ответ: *BitLocker и VeraCrypt.*

С помощью каких программ можно зашифровать жесткий диск?

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](#).

- ☒ BitLocker
- ☐ Disk Utility
- ☒ VeraCrypt
- ☐ Wireshark

Следующий шаг

Решить снова

Рис. 2.3: Скриншот выполнения задания

2.2 Пароли

- Вопрос 1. Какие пароли можно отнести с стойким? (рис. 2.4)

Ответ: *UQr9@j4!S\$.*

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

✓ Всё получилось!

- ☐ qwerty12345
- ☐ ILOVECATS
- ☒ UQr9@j4!S\$
- ☐ IDONTLOVECATS

Следующий шаг

Решить снова

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

Рис. 2.4: Скриншот выполнения задания

- Вопрос 2. Где безопасно хранить пароли? (рис. 2.5)

Ответ: *В менеджерах паролей.*

Где безопасно хранить пароли?

Выберите один вариант из списка

☒ Верно.

☒ В менеджерах паролей
☐ В заметках на рабочем столе
☐ В заметках в телефоне
☐ На стикере, приклеенном к монитору
☐ В кошельке

Следующий шаг Решить снова

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

Рис. 2.5: Скриншот выполнения задания

- Вопрос 3. Зачем нужна капча? (рис. 2.6)

Ответ: *Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа.*

Зачем нужна капча?

Выберите один вариант из списка

Вер
Из

✓ Всё правильно.

- ☐ Для безопасного хранения паролей на сервере
- ☐ Для защиты кук пользователя
- ☐ Она заменяет пароли
- ☒ Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа

Следующий шаг

Решить снова

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

Рис. 2.6: Скриншот выполнения задания

- Вопрос 4. Для чего применяется хэширование паролей? (рис. 2.7)

Ответ: *Для того, чтобы не хранить пароли на сервере в открытом виде..*

Для чего применяется хэширование паролей?

Выберите один вариант из списка

✓ Всё правильно.

- ☐ Для того, чтобы пароль не передавался в открытом виде.
- ☐ Для того, чтобы ускорить процесс авторизации
- ☒ Для того, чтобы не хранить пароли на сервере в открытом виде.
- ☐ Для удобства разработчиков

Следующий шаг

Решить снова

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

Рис. 2.7: Скриншот выполнения задания

- Вопрос 5. Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу? (рис. 2.8)

Ответ: *Нет.*

Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу?

Выберите один вариант из списка

☒ Абсолютно точно.

Верно решили 967 уч
Из всех попыток 66%

☐ Да
☒ Нет

Следующий шаг Решить снова

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

Рис. 2.8: Скриншот выполнения задания

- Вопрос 6. Какие меры защищают от утечек данных атакой перебором? (рис. 2.9)

Ответ: *разные пароли на всех сайтах, периодическая смена паролей, сложные(=длинные) пароли, капча.*

Какие меры защищают от утечек данных атакой перебором?

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](#).

☒ разные пароли на всех сайтах
☒ периодическая смена паролей
☒ сложные(=длинные) пароли
☒ капча

Следующий шаг Решить снова

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

Рис. 2.9: Скриншот выполнения задания

2.3 Фишинг

- Вопрос 1. Какие из следующих ссылок являются фишинговыми? (рис. 2.10)

Ответ: *<https://online.sberbank.wix.ru/CSAFront/index.do> (вход в Сбербанк.Онлайн) и https://passport.yandex.ucoz.ru/auth?origin=home_desktop_ru (вход в аккаунт Яндекс).*

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

✓ Всё правильно.

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](#).

- ☐ <https://accounts.google.com.br/signin/v2/identifier?hl=ru> (страница входа в аккаунт Google)
- ✓ <https://online.sberbank.wix.ru/CSAFront/index.do> (вход в Сбербанк.Онлайн)
- ☐ https://e.mail.ru/login?lang=ru_RU (вход в аккаунт Mail.Ru)
- ✓ https://passport.yandex.ucoz.ru/auth?origin=home_desktop_ru (вход в аккаунт Яндекс)

[Следующий шаг](#) [Решить снова](#)

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

Рис. 2.10: Скриншот выполнения задания

- Вопрос 2. Может ли фишинговый имейл прийти от знакомого адреса? (рис. 2.11)

Ответ: *Да.*

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

☒ Так точно!

The screenshot shows a quiz interface with a light green background. At the top, the question is 'Может ли фишинговый имейл прийти от знакомого адреса?'. Below it, the instruction 'Выберите один вариант из списка' is displayed. A green checkmark icon is next to the selected answer 'Так точно!'. Below this, there are two radio button options: 'Да' (selected) and 'Нет'. At the bottom of the green area, there are two buttons: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). Below the green area, the text 'Ваши решения' (Your solutions) is followed by 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 2.11: Скриншот выполнения задания


2.4 Вирусы. Примеры

- Вопрос 1. Email Спуфинг – это (рис. 2.12)

Ответ: *подмена адреса отправителя в имейлах.*

Email Спуфинг – это

Выберите один вариант из списка

 Отлично!

- ☐ метод предотвращения фишинга
- ☒ подмена адреса отправителя в имейлах
- ☐ протокол для отправки имейлов
- ☐ атака перебором паролей

Следующий шаг

Решить снова

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

Рис. 2.12: Скриншот выполнения задания

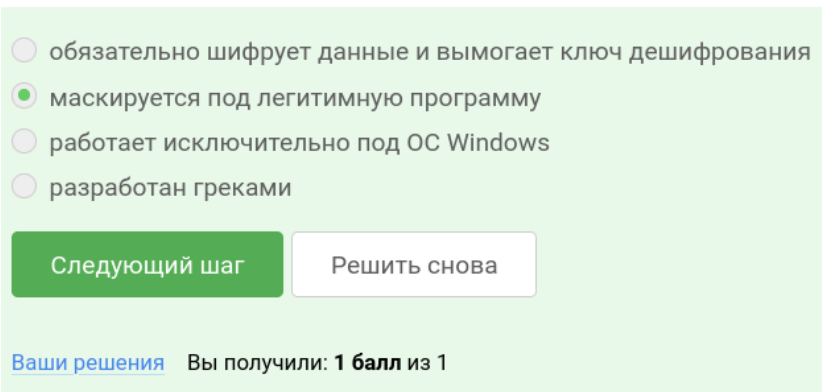
- Вопрос 2. Вирус-троян (рис. 2.13)

Ответ: *маскируется под легитимную программу.*

Вирус-троян

Выберите один вариант из списка

✓ Прекрасный ответ.



The screenshot shows a quiz interface with a light green background. At the top, the question "Вирус-троян" is displayed. Below it, the instruction "Выберите один вариант из списка" is shown. A green checkmark icon is followed by the text "Прекрасный ответ." Below this, there is a list of four radio button options: "обязательно шифрует данные и требует ключ дешифрования", "маскируется под легитимную программу", "работает исключительно под ОС Windows", and "разработан греками". The second option is selected. At the bottom of the list, there are two buttons: "Следующий шаг" (Next step) and "Решить снова" (Solve again). Below the buttons, the text "Ваши решения" (Your solutions) is followed by "Вы получили: 1 балл из 1" (You received: 1 point out of 1).

☐ обязательно шифрует данные и требует ключ дешифрования

☒ маскируется под легитимную программу

☐ работает исключительно под ОС Windows

☐ разработан греками

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.13: Скриншот выполнения задания

2.5 Безопасность мессенджеров

- Вопрос 1. На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal? (рис. 2.14)

Ответ: *при генерации первого сообщения стороной-отправителем.*

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

✓ Абсолютно точно.

- ☒ при генерации первого сообщения стороной-отправителем
- ☐ при установке приложения
- ☐ при каждом новом сообщении от стороны-отправителя
- ☐ при получении сообщения

Следующий шаг

Решить снова

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

Рис. 2.14: Скриншот выполнения задания

- Вопрос 2. Суть сквозного шифрования состоит в том, что (рис. 2.15)

Ответ: *сообщения передаются по узлам связи (серверам) в зашифрованном виде.*

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

✓ Всё правильно.

- ☒ сообщения передаются по узлам связи (серверам) в зашифрованном виде
- ☐ сервер получает сообщения в открытом виде для передачи нужному получателю
- ☐ сервер перешифровывает сообщения в процессе передачи
- ☐ сообщения передаются от отправителя к получателю без участия сервера

Следующий шаг

Решить снова

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

Рис. 2.15: Скриншот выполнения задания

3 Третий модуль. Криптография на практике.

3.1 Введение в криптографию

- Вопрос 1. В асимметричных криптографических примитивах (рис. 3.1):

Ответ: *обе стороны имеют пару ключей.*

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Так точно!

☐ одна сторона публикует свой секретный ключ, другая - держит его в секрете

☐ обе стороны имеют общий секретный ключ

☒ обе стороны имеют пару ключей

☐ одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Верно
Из всего

Рис. 3.1: Скриншот выполнения задания

- Вопрос 2. Криптографическая хэш-функция (рис. 3.2):

Ответ: *эффективно вычисляется, дает на выходе фиксированное число бит независимо от объема входных данных, стойкая к коллизиям.*

Выберите все подходящие ответы из списка

✓ Правильно, молодец!

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](#).

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

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

Рис. 3.2: Скриншот выполнения задания

- Вопрос 3. К алгоритмам цифровой подписи относятся (рис. 3.3):

Ответ: *RSA, ECDSA, ГОСТ Р 34.10-2012* .

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 из 1

Рис. 3.3: Скриншот выполнения задания

- Вопрос 4. Код аутентификации сообщения относится к (рис. 3.4):

Ответ: *симметричным примитивам.*

Код аутентификации сообщения относится к

Выберите один вариант из списка



Так точно!

☐ асимметричным примитивам

☒ симметричным примитивам

[Следующий шаг](#) [Решить снова](#)

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

Рис. 3.4: Скриншот выполнения задания

- Вопрос 5. Обмен ключам Диффи-Хэллмана - это (рис. 3.5):

Ответ: *асимметричный примитив генерации общего секретного ключа.*

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** из 1

Рис. 3.5: Скриншот выполнения задания

3.2 Цифровая подпись

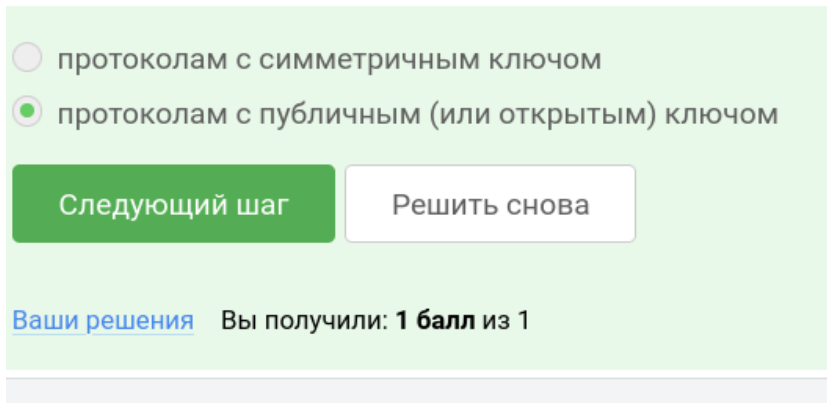
- Вопрос 1. Протокол электронной цифровой подписи относится к (рис. 3.6):

Ответ: *протоколам с публичным (или открытым) ключом.*

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Всё правильно.



The screenshot shows a quiz interface with a light green background. At the top, there is a green circle with a white checkmark and the text "Всё правильно." Below this, there are two radio button options: "протоколам с симметричным ключом" (unselected) and "протоколам с публичным (или открытым) ключом" (selected). Below the options are two buttons: a green button labeled "Следующий шаг" and a white button with a green border labeled "Решить снова". At the bottom, there is a link "Ваши решения" and the text "Вы получили: 1 балл из 1".

Рис. 3.6: Скриншот выполнения задания

- Вопрос 2. Алгоритм верификации электронной цифровой подписи требует на вход (рис. 3.7):

Ответ: *подпись, открытый ключ, сообщение.*

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Правильно, молодец!

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

Следующий шаг

Решить снова

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

Рис. 3.7: Скриншот выполнения задания

- Вопрос 3. Электронная цифровая подпись не обеспечивает (рис. 3.8):

Ответ: *конфиденциальность*.

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

☒ Отличное решение!

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

Следующий шаг

Решить снова

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

Рис. 3.8: Скриншот выполнения задания

- Вопрос 4. Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС? (рис. 3.9):

Ответ: *усиленная квалифицированная.*

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

Выберите один вариант из списка

☒ Абсолютно точно.

Верно реш
Из всех по

- ☐ простая
☐ усиленная неквалифицированная
☒ усиленная квалифицированная

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 3.9: Скриншот выполнения задания

- Вопрос 5. В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи? (рис. 3.10):

Ответ: *в удостоверяющем (сертификационном) центре.*

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

Выберите один вариант из списка

☒ Хорошая работа.

Верно решили 907 учас
Из всех попыток 60% вер

- ☐ 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 из 1

Рис. 3.10: Скриншот выполнения задания

3.3 Электронные платежи

- Вопрос 1. Выберите из списка все платежные системы. (рис. 3.11):

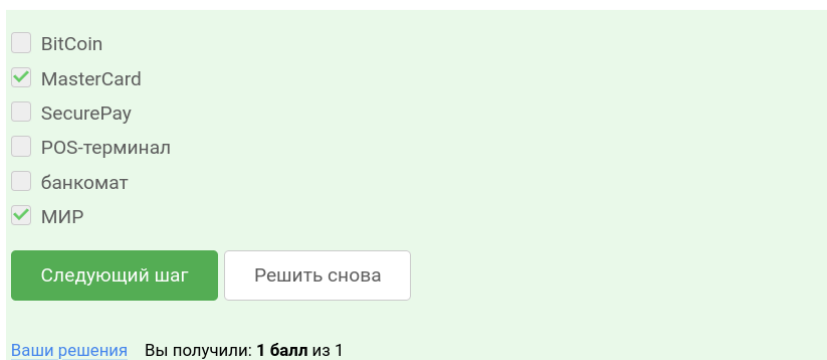
Ответ: *MasterCard, МИР.*

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

Ваши решения Вы получили: 1 балл из 1

Рис. 3.11: Скриншот выполнения задания

- Вопрос 2. Примером многофакторной аутентификации является (рис. 3.12):

Ответ: комбинация проверка пароля + код в sms сообщении, комбинация код в sms сообщении + отпечаток пальца .

Примером многофакторной аутентификации является

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](#).

☐ 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** из 1

Рис. 3.12: Скриншот выполнения задания

- Вопрос 3. При онлайн платежах сегодня используется (рис. 3.13):

Ответ: *многофакторная аутентификация покупателя перед банком-эмитентом.*

При онлайн платежах сегодня используется

Выберите один вариант из списка

✔ Так точно!

☒ 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** из 1

Рис. 3.13: Скриншот выполнения задания

3.4 Блокчейн

- Вопрос 1. Какое свойство криптографической хэш-функции используется в доказательстве работы? (рис. 3.14):

Ответ: *сложность нахождения прообраза.*

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 из 1

Рис. 3.14: Скриншот выполнения задания

- Вопрос 2. Консенсус в некоторых системах блокчейн обладает свойствами (рис. 3.15):

Ответ: *постоянства, консенсус, живучесть, открытость.*

Консенсус в некоторых системах блокчейн обладает свойствами

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](#).

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

Следующий шаг

Решить снова

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

Рис. 3.15: Скриншот выполнения задания

- Вопрос 3. Секретные ключи какого криптографического примитива хранят участники блокчейна? (рис. 3.16):

Ответ: *цифровая подпись*.

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

✔ Верно. Так держать!

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

Следующий шаг

Решить снова

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

Рис. 3.16: Скриншот выполнения задания

4 Выводы

В рамках прохождения курса разобрались в схеме передачи данных через Интернет, их шифровании. Получили практические советы по выбору более качественного пароля. Научились отличать шифрование от цифровой подписи, поняли, как работают системы электронных платежей.