

Результат выполнения внешнего курса на Степике

Внешний курс

Лазарев Даниил Михайлович

Содержание

1 Цель работы	6
2 Выполнение заданий блока “Основы Кибербезопасности”	7
2.1 Как работает интернет: базовые сетевые протоколы	7
2.2 Персонализация сети	11
2.3 Браузер TOR. Анонимизация	13
2.4 Беспроводные сети Wi-fi	14
3 Выполнение заданий блока “Основы Кибербезопасности”	17
3.1 Шифрование диска	17
3.2 Пароли	18
3.3 Фишинг	21
3.4 Вирусы.	22
3.5 Безопасность мессенджеров	23
4 Выполнение заданий блока “Основы Кибербезопасности”	25
4.1 Введение в криптографию	25
4.2 Цифровая подпись	27
4.3 Электронные платежи	30
4.4 Блокчейн	32
5 Общий результат	34

Список иллюстраций

2.1	Вопрос 2.1	7
2.2	Вопрос 2.1	8
2.3	Вопрос 2.1	8
2.4	Вопрос 2.1	9
2.5	Вопрос 2.1	9
2.6	Вопрос 2.1	10
2.7	Вопрос 2.1	10
2.8	Вопрос 2.1	10
2.9	Вопрос 2.1	11
2.10	Вопрос 2.2	11
2.11	Вопрос 2.2	12
2.12	Вопрос 2.2	12
2.13	Вопрос 2.2	12
2.14	Вопрос 2.3	13
2.15	Вопрос 2.3	13
2.16	Вопрос 2.3	14
2.17	Вопрос 2.3	14
2.18	Вопрос 2.4	15
2.19	Вопрос 2.4	15
2.20	Вопрос 2.4	15
2.21	Вопрос 2.4	16
2.22	Вопрос 2.4	16
3.1	Вопрос 3.1.	17
3.2	Вопрос 3.1	18
3.3	Вопрос 3.1	18
3.4	Вопрос 3.2	19
3.5	Вопрос 3.2	19
3.6	Вопрос 3.2	19
3.7	Вопрос 3.2	20
3.8	Вопрос 3.2	20
3.9	Вопрос 3.2	21
3.10	Вопрос 3.3	21
3.11	Вопрос 3.3	22
3.12	Вопрос 3.4	22
3.13	Вопрос 3.4	23
3.14	Вопрос 3.5	23

3.15 Вопрос 3.5	24
4.1 Вопрос 4.1	25
4.2 Вопрос 4.1	26
4.3 Вопрос 4.1	26
4.4 Вопрос 4.1	27
4.5 Вопрос 4.1	27
4.6 Вопрос 4.2	28
4.7 Вопрос 4.2	28
4.8 Вопрос 4.2	29
4.9 Вопрос 4.2	29
4.10 Вопрос 4.2	30
4.11 Вопрос 4.3	30
4.12 Вопрос 4.3	31
4.13 Вопрос 4.3	31
4.14 Вопрос 4.4	32
4.15 Вопрос 4.4	33
4.16 Вопрос 4.4	33
5.1 Финал	34

Список таблиц

1 Цель работы

Выполнить контрольные задания первого блока “Безопасность в сети” внешнего курса “Основы кибербезопасности”.

2 Выполнение заданий блока “Основы Кибербезопасности”

2.1 Как работает интернет: базовые сетевые протоколы

Протокол HTTP(S) протокол прикладного уровня, ответ на вопрос 1 - HTTPS (рис. 2.1).

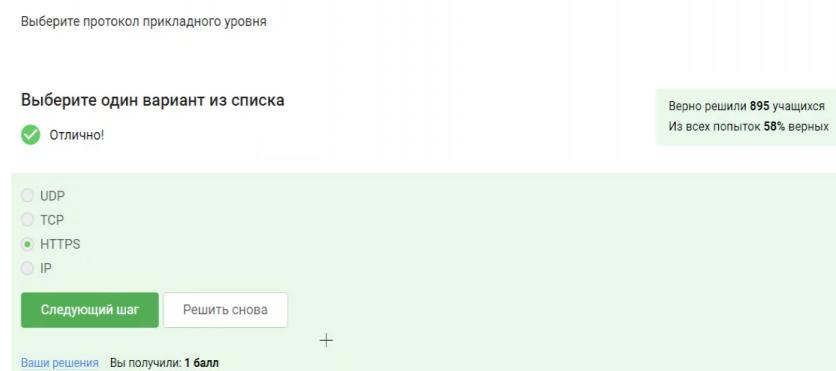


Рис. 2.1: Вопрос 2.1

На транспортном уровне существует два примера протокола: первый - это TCP, в честь которого названа модель. (рис. 2.2).

На каком уровне работает протокол TCP?

Выберите один вариант из списка

Всё правильно.

- Транспортном
- Прикладном
- Канальном
- Сетевом

Следующий шаг

Решить снова

Верно решили **939** учащихся
Из всех попыток **61%** верных

Ваши решения Вы получили: **1 балл**

Рис. 2.2: Вопрос 2.1

Т.к адрес состоит из большего набора чисел, а именно это 4 или 6 цифр от 0 до 255. В двух вариантах встречаются цифры больше 255, что неверно(рис. 2.3).

Выберите все корректные адреса IPv4

Выберите все подходящие ответы из списка

Так точно!

Верно решил **871** учащийся
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](#).

- 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**

Рис. 2.3: Вопрос 2.1

Основная задача DNC это сопоставлять название (доменное имя, с коректным IP-адресом) с тем, где лежит этот сервер, этот сайт. (рис. 2.4).

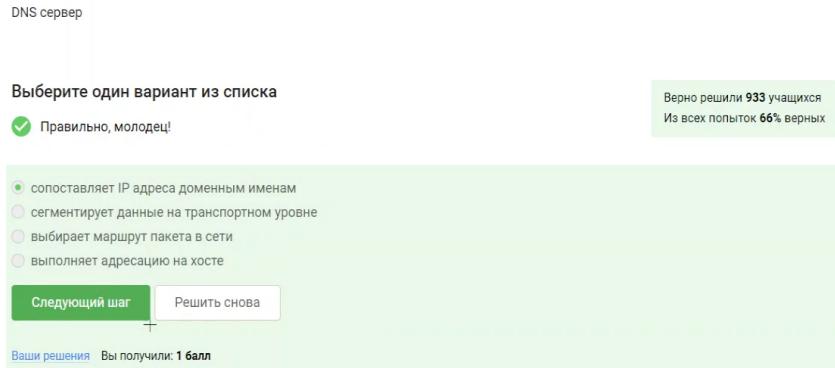


Рис. 2.4: Вопрос 2.1

Классификация протоколов в модели TCP/IP:

- Прикладной уровень: HTTP, RTSP, FTP, DNS.
- Транспортный уровень: TCP, UDP, SCTP, DCCP.
- Сетевой уровень: IP.
- Уровень сетевого доступа (Канальный) (Link Layer): Ethernet, IEEE 802.11, WLAN, SLIP, Token Ring, ATM и MPLS(рис. 2.5).

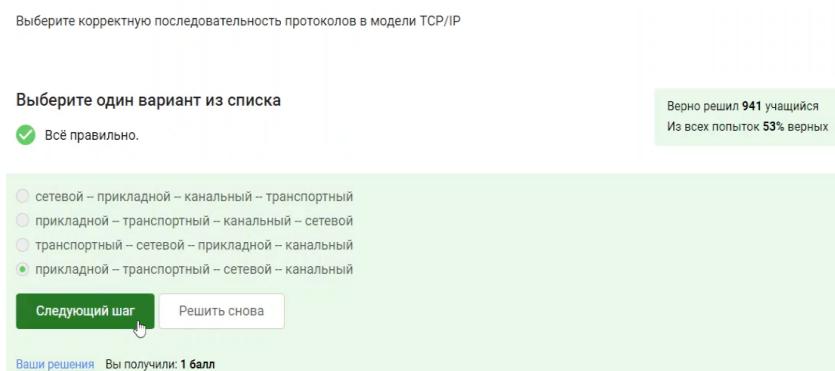


Рис. 2.5: Вопрос 2.1

Протокол http передает не зашифрованные данные, а протокол https уже будет передавать зашифрованные данные (рис. 2.6).

https передает зашифрованные данные, поэтому одна из фаз это передача данных, другая должна быть рукопожатием

Протокол http предполагает

Выберите один вариант из списка

Абсолютно точно.

Верно решили 965 учащихся
Из всех попыток 78% верных

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

Рис. 2.6: Вопрос 2.1

TLS определяется и клиентом, и сервером, чтобы было возможно подключиться (рис. 2.7).

Протокол https состоит из

Выберите один вариант из списка

Прекрасный ответ.

Верно решили 948 учащихся
Из всех попыток 41% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: ***



Рис. 2.7: Вопрос 2.1

TLS определяется клиентом и сервером, чтобы возможно было подключиться (рис. 2.8).

Версия протокола TLS определяется

Выберите один вариант из списка

Абсолютно точно.

Верно решили 947 учащихся
Из всех попыток 55% верных

сервером
 клиентом
 и клиентом, и сервером в процессе "переговоров"
 провайдером клиента

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

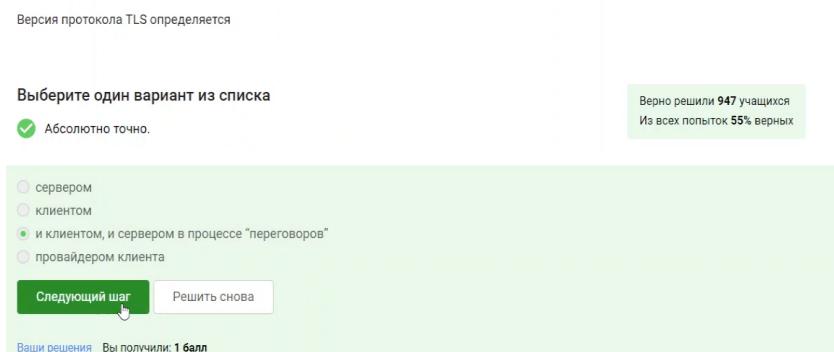


Рис. 2.8: Вопрос 2.1

Фаза рукопожатия включает в себя:

- выбор параметров, протоколов
- аутентификация (как минимум, сервера)
- формируется общий секретный ключ K

Следовательно вариант с шифрованием лишний (рис. 2.9).

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

Хорошие новости, верно!

формирование общего секретного ключа между клиентом и сервером
 аутентификация (как минимум одной из сторон)
 выбираются алгоритмы шифрования/аутентификации
 шифрование данных

Следующий шаг **Решить снова**

Ваше решение: Вы получили: * * *

Верно решил 931 учащийся
Из всех попыток 44% верных

Рис. 2.9: Вопрос 2.1

2.2 Персонализация сети

Куки хранят в себе список параметров и их значений. Этими параметрами могут быть id пользователя, id сессии, тип браузера и некоторые действия пользователей(рис. 2.10).

Куки хранят:

Выберите все подходящие ответы из списка

Так точно!

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

IP адрес
 идентификатор пользователя
 id сессии
 пароль пользователя

Следующий шаг **Решить снова**

Ваше решение: Вы получили: 1 балл

Верно решили 856 учащихся
Из всех попыток 18% верных

Рис. 2.10: Вопрос 2.2

Куки не делают соединение надежным (рис. 2.11).

Куки не используются для

Выберите один вариант из списка

Верно.

Верно решили **950** учащихся
Из всех попыток **53%** верных

- 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**

Рис. 2.11: Вопрос 2.2

Куки генерируются сервером(рис. 2.12).

Куки генерируются

Выберите один вариант из списка

Так точно!

Верно решили **968** учащихся
Из всех попыток **79%** верных

- сервером
- клиентом

Следующий шаг

Решить снова

Ваши решения Вы получили: ***

Рис. 2.12: Вопрос 2.2.

Куки бывают сессионные, удаляются при закрытии окна браузера (рис. 2.13).

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

Правильно.

Верно решили **959** учащихся
Из всех попыток **60%** верных

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

Следующий шаг

Решить снова

+
Ваши решения Вы получили: **1 балл**

Рис. 2.13: Вопрос 2.2

2.3 Браузер TOR. Анонимизация

В луковой модели маршрутизации у нас тоже есть узлы. Они разделяются на охранный узел, промежуточный и выходной. В браузере Tor всегда есть три роутера, их не больше и не меньше (рис. 2.14).

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

Так точно!

2
 3
 4

Следующий шаг **Решить снова**

Верно решили 959 учащихся
Из всех попыток 77% верных

Ваши решения Вы получили: 1 балл

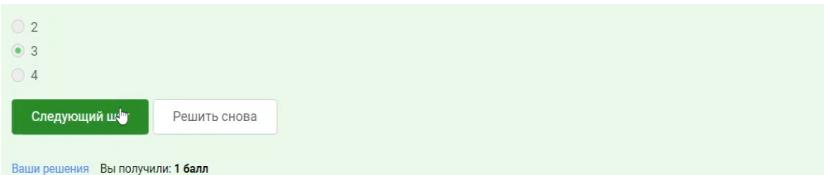


Рис. 2.14: Вопрос 2.3

IP-адрес не должен быть известен охранному и промежуточному узлам (рис. 2.15).

IP-адрес получателя известен

Выберите все подходящие ответы из списка

Так точно!

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**

Верно решили 906 учащихся
Из всех попыток 19% верных

Ваши решения Вы получили: 1 балл

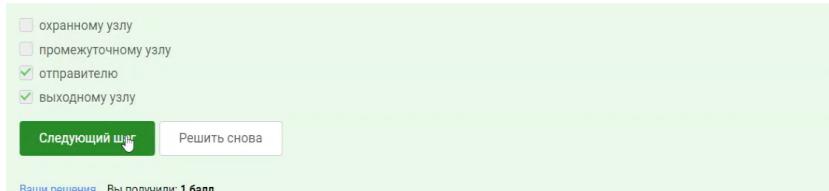


Рис. 2.15: Вопрос 2.3.

В анонимных сетях, таких как Тор, общий секретный ключ для сквозного шифрования требует участия всех трех типов узлов: охранного, промежуточного и выходного. Охранный узел сам по себе не обеспечивает генерацию ключа. Каждый узел вносит свой вклад в криптографический протокол (например, Diffie-Hellman), обеспечивая анонимность и защиту от перехвата. (рис. 2.16).

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

Правильно, молодец!

Верно решили 959 учащихся
Из всех попыток 55% верных

- только с охранным узлом
- с охранным и промежуточным узлом
- с охранным, промежуточным и выходным узлом
- с промежуточным и выходным узлом

[Следующий шаг](#)

[Решить снова](#)

Ваши решения Вы получили: 1 балл

Рис. 2.16: Вопрос 2.3

Для получения пакетов не нужно использовать TOR. TOR — это технология, которая позволяет с некоторым успехом скрыть личность человека в интернете.(рис. 2.17).

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

Выберите один вариант из списка

Отлично!

Верно решил 961 учащийся
Из всех попыток 74% верных

- Да
- Нет

+

[Следующий шаг](#)

[Решить снова](#)

Ваши решения Вы получили: 1 балл

Рис. 2.17: Вопрос 2.3

2.4 Беспроводные сети Wi-fi

WiFi - это технология беспроводной локальной сети, она основана на стандарте IEEE 802.11 (рис. 2.18).

Wi-Fi - это

Выберите один вариант из списка

Хорошая работа.

Верно решили 965 учащихся

Из всех попыток 79% верных

- 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

Рис. 2.18: Вопрос 2.4

WiFi работает на самом нижнем канальном уровне (рис. 2.19).

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

Здорово, всё верно.

Верно решили 972 учащихся

Из всех попыток 58% верных

- Транспортном
- Прикладном
- Канальном
- Сетевом

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.19: Вопрос 2.4

WEP - устаревший и небезопасный метод шифрования WiFi из-за короткой длины ключа (40 бит), что делает его легко взламываемым. Использовать WEP категорически не рекомендуется.(рис. 2.20).

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

Верно. Так держать!

Верно решили 973 учащихся

Из всех попыток 60% верных

- WPA
- WEP
- WPA2
- WPA3

Следующий шаг

Решить снова

Ваши решения Вы получили: ***

Рис. 2.20: Вопрос 2.4

Безопасность WiFi подразумевает защиту передачи данных между устройством (телефон, компьютер) и роутером (подключенным к интернету), осуществляющую с помощью шифрования и аутентификации.(рис. 2.21).

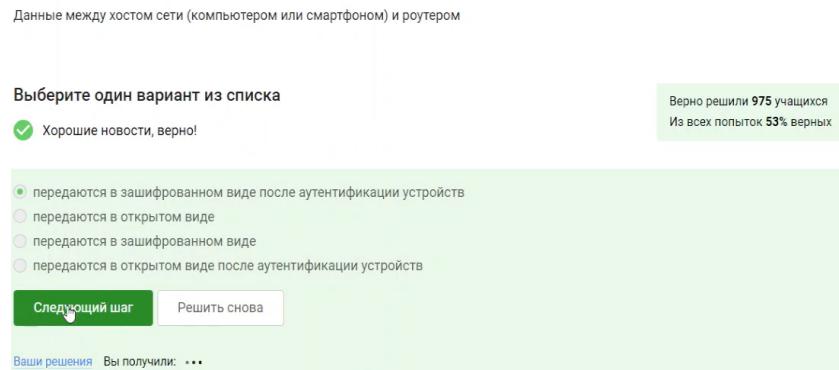


Рис. 2.21: Вопрос 2.4

WPA2 Personal предназначен для домашнего использования, а WPA2 Enterprise - для коммерческих организаций. (рис. 2.22).

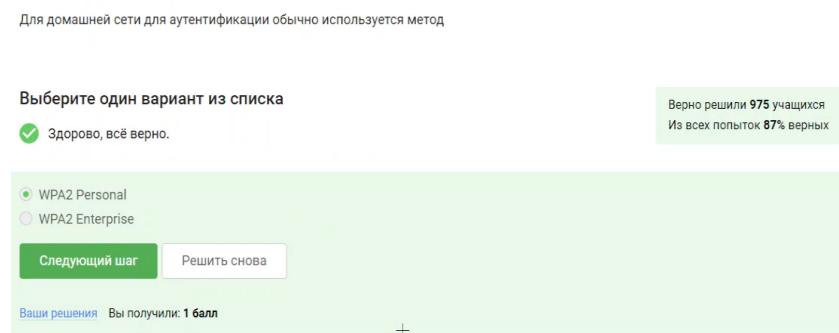


Рис. 2.22: Вопрос 2.4

3 Выполнение заданий блока “Основы Кибербезопасности”

3.1 Шифрование диска

Шифровать нужно не только жесткий диск, но и загрузочный сектор диска.
Ответ-можно (рис. 3.1).

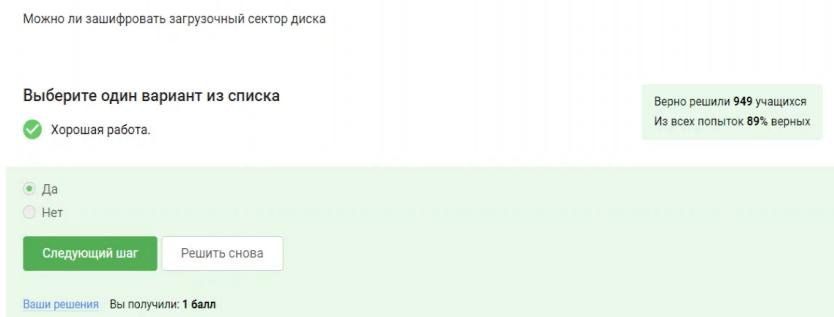


Рис. 3.1: Вопрос 3.1.

Шифрование диска основано на симметричном шифровании (рис. 3.2).

Шифрование диска основано на

Выберите один вариант из списка

Так точно!

Верно решили 972 учащихся
Из всех попыток 66% верных

- хэшировании
- симметричном шифровании
- асимметричном шифровании

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

Рис. 3.2: Вопрос 3.1

Популярные ОС имеют встроенные инструменты для шифрования дисков: Windows (Bitlocker), Linux (LUKS), MacOS (FileVault). Также доступны бесплатные опенсорсные альтернативы, такие как VeraCrypt и PGPDisk. (рис. 3.3).

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

Верно.

Верно решили 906 учащихся
Из всех попыток 28% 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](#).

- Disk Utility
- Wireshark
- VeraCrypt
- BitLocker

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

Рис. 3.3: Вопрос 3.1

3.2 Пароли

Стойкий пароль содержит цифры строчные и заглавные буквы и специальные символы. Это усложняет перебор пароля (рис. 3.4).

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

qwerty12345
 ILOVECATS
 UQr9@j4SS
 IDONTLOVECATS

Следующий шаг **Решить снова**

Верно решили 969 учащихся
Из всех попыток 85% верных

Ваши решения Вы получили: 1 балл

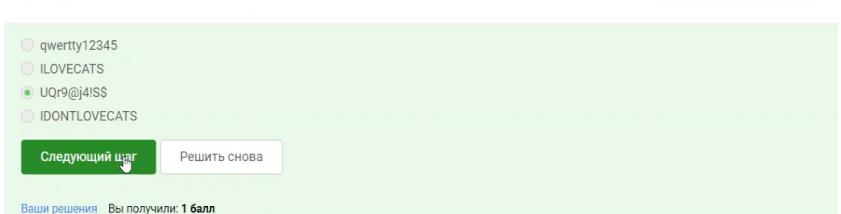


Рис. 3.4: Вопрос 3.2

Безопасно хранить пароли нужно только в месенджерах (рис. 3.5).

Где безопасно хранить пароли?

Выберите один вариант из списка

Всё правильно.

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

Следующий шаг **Решить снова**

Верно решил 971 учащийся
Из всех попыток 74% верных

Ваши решения Вы получили: 1 балл



Рис. 3.5: Вопрос 3.2

Капча - тест для определения, кто общается с веб-сервисом, человек или бот(рис. 3.6).

Зачем нужна капча?

Выберите один вариант из списка

Верно.

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

Следующий шаг **Решить снова**

Верно решили 974 учащихся
Из всех попыток 77% верных

Ваши решения Вы получили: 1 балл

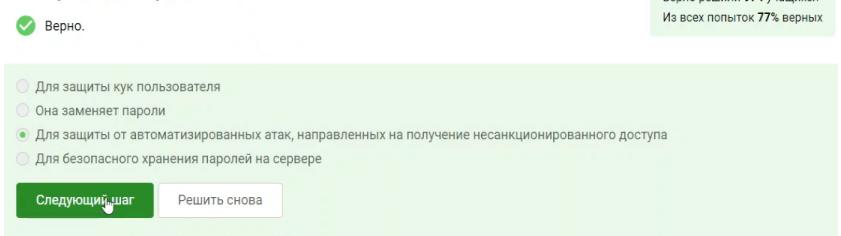


Рис. 3.6: Вопрос 3.2

В целях безопасности пароли хранят не в открытом виде, а в виде хешей (рис. 3.7).

Для чего применяется хэширование паролей?

Выберите один вариант из списка

Хорошие новости, верно!

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

Верно решили 973 учащихся
Из всех попыток 61% верных

Ваши решения Вы получили: + + +

Рис. 3.7: Вопрос 3.2

Соль - это метод защиты слабых паролей. Сервер добавляет соль к паролю пользователя. Это делает взлом слабых паролей сложнее (рис. 3.8).

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

Выберите один вариант из списка

Хорошая работа.

Да
 Нет

Следующий шаг

Верно решили 967 учащихся
Из всех попыток 66% верных

Ваши решения Вы получили: 1 балл

Рис. 3.8: Вопрос 3.2

Для безопасности нужно использовать длинные, сложные пароли, регулярно обновлять и хранить пароли в мессенджерах паролей. (рис. 3.9).

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

Всё получилось!

Верно решили **895** учащихся
Из всех попыток **16%** 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](#).

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

[Следующий шаг](#)

[Решить снова](#)

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

Рис. 3.9: Вопрос 3.2

3.3 Фишинг

Пример фишинга - эта маскировка под известные веб-сайты только с другим доменным именем (рис. 3.10).

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

Так точно!

Верно решил **861** учащийся
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](#).

- <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**

Рис. 3.10: Вопрос 3.3

Может фишинговое письмо прийти и от знакомого(рис. 3.11).

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

Абсолютно точно.

Да
 Нет

Следующий шаг **Решить снова**

Верно решили 966 учащихся
Из всех попыток 90% верных

Ваши решения Вы получили: 1 балл

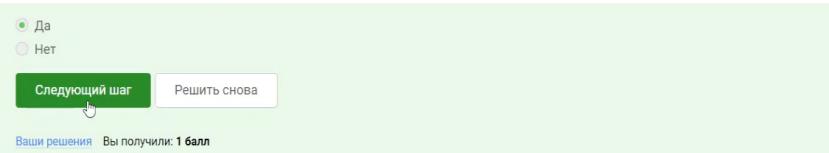


Рис. 3.11: Вопрос 3.3

3.4 Вирусы.

Спупинг - это подмена адреса отправителя в имейлах (рис. 3.12).

Email Спупинг -- это

Выберите один вариант из списка

Верно.

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

Следующий шаг **Решить снова**

Верно решили 960 учащихся
Из всех попыток 65% верных

Ваши решения Вы получили: ...

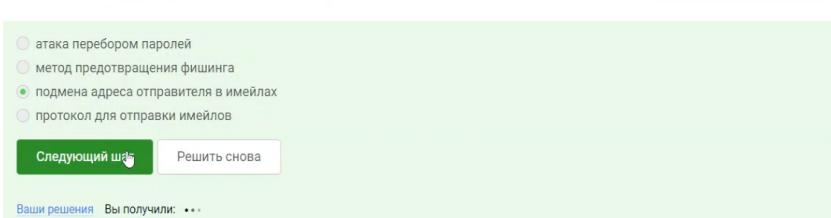


Рис. 3.12: Вопрос 3.4

Троян маскируется под обычновенную безобидную программу, при запуске которой вирус легко проникает в ваш компьютер и поражает его(рис. 3.13).

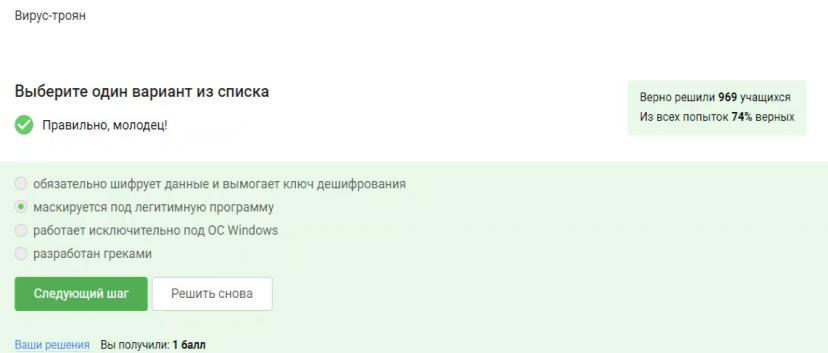


Рис. 3.13: Вопрос 3.4

3.5 Безопасность мессенджеров

При генерации первого сообщения отправителем формируется ключ шифрования (рис. 3.14).

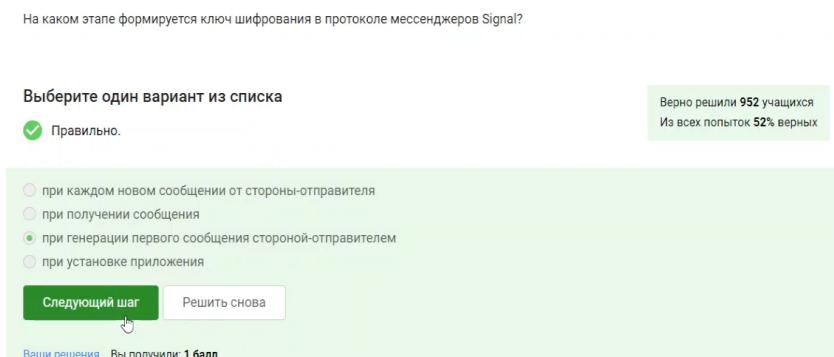


Рис. 3.14: Вопрос 3.5

Сквозное шифрование позволяет передавать сообщения между пользователями (Алиса и Боб) так, что сервер знает только адресата, но не может прочитать содержимое. Алиса шифрует сообщение, сервер передает шифрованный текст Бобу, а Боб его расшифровывает. Сервер не имеет доступа к ключам или открытому тексту сообщения. (рис. 3.15).

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

 Отличное решение!

Верно решили **964** учащихся
Из всех попыток **60%** верных

- 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**

Рис. 3.15: Вопрос 3.5

4 Выполнение заданий блока “Основы Кибербезопасности”

4.1 Введение в криптографию

В асимметричной криптографии у каждой из сторон есть пара ключей: открытый и секретный ключ (рис. 4.1).

В асимметричных криптографических примитивах

Выберите один вариант из списка

Хорошие новости, верно!

Верно решили 940 учащихся
Из всех попыток 42% верных

обе стороны имеют общий секретный ключ
 одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей
 обе стороны имеют пару ключей
 одна сторона публикует свой секретный ключ, другая – держит его в секрете

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

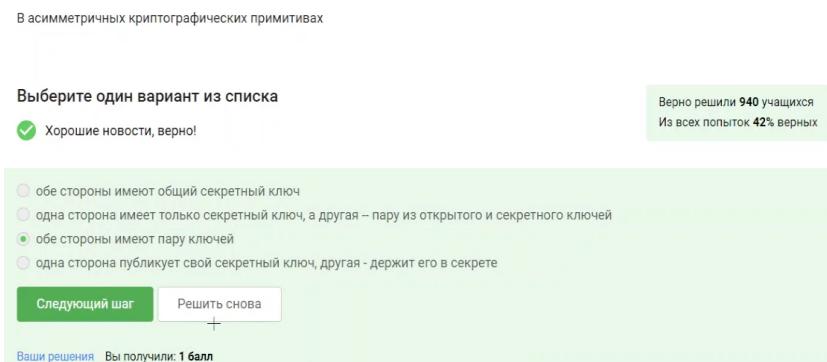


Рис. 4.1: Вопрос 4.1

Криптографическая хэш-функция обладает важным свойством стойкости к коллизиям, что означает, что крайне сложно найти два разных входа, которые дают одинаковый хэш. Она принимает произвольный объем данных и выдает фиксированную строку заданной длины (например, n). Обычно функция сжимает данные, преобразуя большой набор информации в небольшое значение. (рис. 4.2).

Выберите все подходящие ответы из списка

Правильно, молодец!

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](#).

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

[Следующий шаг](#)

[Решить снова](#)

Ваши решения Вы получили: 1 балл

Рис. 4.2: Вопрос 4.1

Отмечены алгоритмы цифровой подписи (рис. 4.3).

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

Всё правильно.

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 свое 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. 4.3: Вопрос 4.1

Код аутентификации сообщения (MAC) относится к симметричным примитивам, поскольку для его генерации и проверки используется общий секретный ключ, известный только отправителю и получателю, что обеспечивает целостность и аутентичность данных.(рис. 4.4).

Код аутентификации сообщения относится к

Выберите один вариант из списка

Отличное решение!

асимметричным примитивам
 симметричным примитивам

Следующий шаг **Решить снова**

Ваши решения Вы получили: 1 балл

Верно решили 955 учащихся
Из всех попыток 69% верных

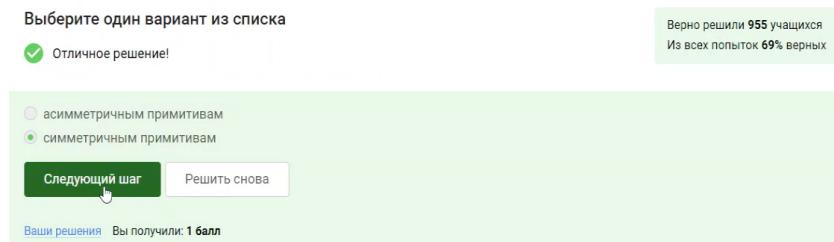


Рис. 4.4: Вопрос 4.1

Чтобы ответить на данный вопрос использую определение Диффи-Хэллмана (рис. 4.5).

Обмен ключом Диффи-Хэллмана - это

Выберите один вариант из списка

Верно. Так держать!

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

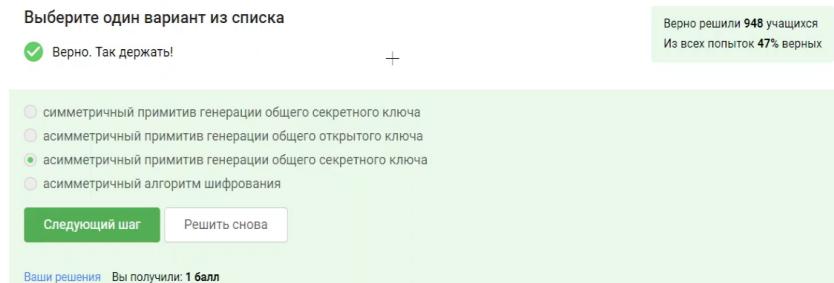


Рис. 4.5: Вопрос 4.1

4.2 Цифровая подпись

По определению цифровой подписи протокол ЭЦП относиться к протоколам с публичным ключом (рис. 4.6).

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

Верно. Так держать!

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. 4.6: Вопрос 4.2

Каждая машина процедуру верификации, которая берет на вход само обновление, подпись и открытый ключ разработчика (рис. 4.7).

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

Отлично!

Верно решили 962 учащихся

Из всех попыток 46% верных

- подпись, секретный ключ, сообщение
 подпись, открытый ключ
 подпись, открытый ключ, сообщение
 подпись, секретный ключ

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

Рис. 4.7: Вопрос 4.2

Цифровая подпись обеспечивает три ключевых функции:

1. Целостность сообщения — изменения в сообщении приводят к некорректной проверке подписи.
2. Аутентификация — позволяет установить, что подпись принадлежит конкретному владельцу.
3. Неотказ от авторства — подписавший не может отказаться от своей подписи.

Однако, если секретный ключ украден, безопасность подписи подрывается, и она не обеспечивает конфиденциальности.(рис. 4.8).

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

Всё правильно.

целостность
 аутентификацию
 конфиденциальность
 неотказ от авторства

Следующий шаг **Решить снова**

Верно решили 968 учащихся
Из всех попыток 53% верных

Ваши решения Вы получили: 1 балл

Рис. 4.8: Вопрос 4.2

Усиленная квалифицированная подпись (УКЭП) имеет юридическую силу и равнозначна рукописной подписи. Для её получения необходимо обратиться в аккредитованный сертификационный центр с паспортом и другими данными. (рис. 4.9).

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

Выберите один вариант из списка

Так точно!

усиленная квалифицированная
 простая
 усиленная неквалифицированная

Следующий шаг **Решить снова**

Верно решили 975 учащихся
Из всех попыток 68% верных

Ваши решения Вы получили: 1 балл

Рис. 4.9: Вопрос 4.2

Сертификат подписывается с помощью электронной подписи уже доверенной стороной, удостоверяющим центром. (рис. 4.10).

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

Выберите один вариант из списка

Хорошая работа.

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. 4.10: Вопрос 4.2

4.3 Электронные платежи

На данный момент существуют такие платежные системы, как: Visa, MasterCard, МИР (рис. 4.11).

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

Правильно.

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. 4.11: Вопрос 4.3

Основные категории вещей, которые мы можем использовать для доказательства своей идентичности:

1. Знание: Это что-то, что я знаю, например, пароль, PIN-код или секретный код для онлайн-платежей.

2. Владение: В онлайн-платежах используется второй фактор — это то, чем я владею, например, телефон, на который приходит код для подтверждения.
3. Свойства: Биометрические данные, такие как отпечаток пальца или сетчатка глаза, служат третьим фактором аутентификации.
4. Локация: Четвертый фактор аутентификации — это место, откуда осуществляется доступ, что также может быть учтено при проверке идентичности. (рис. 4.12).

Примером многофакторной аутентификации является

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](#).

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**

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

Рис. 4.12: Вопрос 4.3

При онлайн платежах используется многофакторная аутентификация банком-эмитентом (выпустившим карту), чтобы удостовериться, что транзакцию совершают именно владелец карты или счета, а не злоумышленник(рис. 4.13).

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**

Верно решили **957** учащихся
Из всех попыток **59%** верных

Рис. 4.13: Вопрос 4.3

4.4 Блокчейн

Proof-of-Work (PoW) — это способ, который используется в блокчейне для подтверждения транзакций и создания новых блоков. В этом процессе майнеры (люди, которые занимаются добычей криптовалюты) соревнуются друг с другом за завершение транзакций в сети и за вознаграждение.

Когда люди отправляют друг другу цифровые деньги, эти транзакции собираются в блоки и добавляются в общую базу данных, называемую блокчейном. Чтобы сделать сеть безопасной и защитить её от мошенничества, PoW требует много вычислительных ресурсов. Это значит, что для успешного участия в процессе нужно много мощных компьютеров.(рис. 4.14).

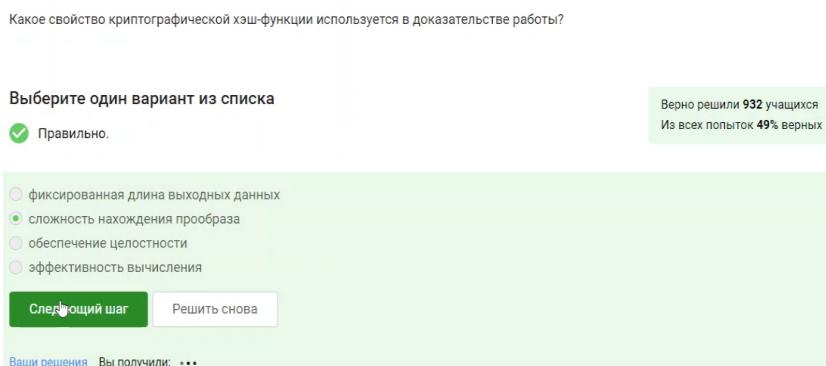


Рис. 4.14: Вопрос 4.4

В основе любого блокчейна, включая биткоин, лежит консенсус — публичная структура данных (ledger), содержащая историю всех транзакций. Консенсус обеспечивает четыре ключевых свойства:

1. Постоянство: Добавленные данные не могут быть удалены.
2. Согласованность: Все участники видят и согласны с одними и теми же данными, за исключением последних изменений.
3. Живучесть: Возможность добавления новых транзакций в любое время.
4. Открытость: Любой желающий может стать участником блокчейна.

Эти свойства обеспечивают надежность и безопасность системы. (рис. 4.15).

Консенсус в некоторых системах блокчейн обладает свойствами

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](#).

постоянства
 живучесть
 открытость
 консенсус

[Следующий шаг](#) [Решить снова](#)

Верно решили 864 учащихся
Из всех попыток 23% верных

Ваши решения Вы получили: 1 балл

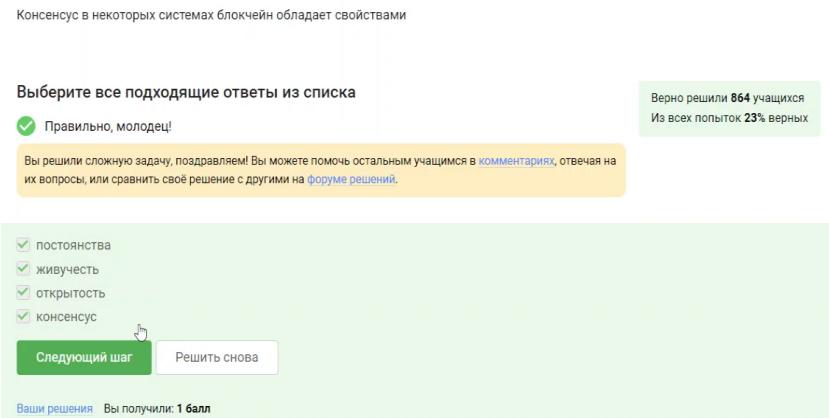


Рис. 4.15: Вопрос 4.4

В блокчейне у каждого из трех участников есть секретный ключ, который они используют для подтверждения транзакций. Этот секретный ключ позволяет создавать цифровую подпись, которая служит доказательством того, что транзакция была инициирована конкретным участником. Цифровая подпись основана на паре ключей — секретном и открытом. Секретный ключ используется для подписания транзакции, а открытый ключ позволяет другим участникам проверить подлинность этой подписи. Таким образом, цифровая подпись обеспечивает безопасность и аутентичность транзакций в блокчейне. (рис. 4.16).

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

Отличное решение!

обмен ключами
 шифрование
 цифровая подпись
 хэш-функция

[Следующий шаг](#) [Решить снова](#)

Верно решил 951 учащийся
Из всех попыток 48% верных

Ваши решения Вы получили: 1 балл

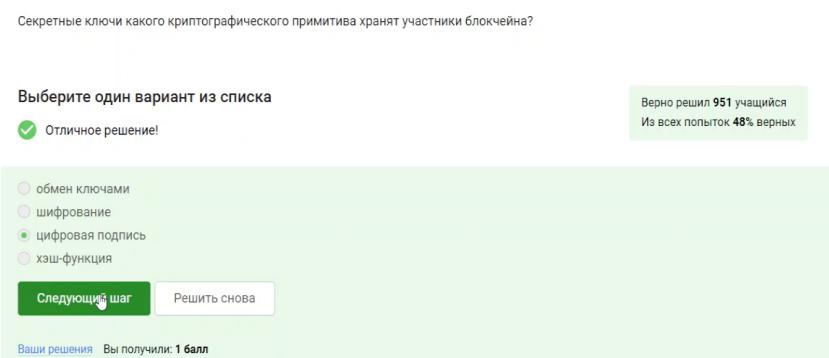


Рис. 4.16: Вопрос 4.4

5 Общий результат

Финальный результат (рис. 5.1).

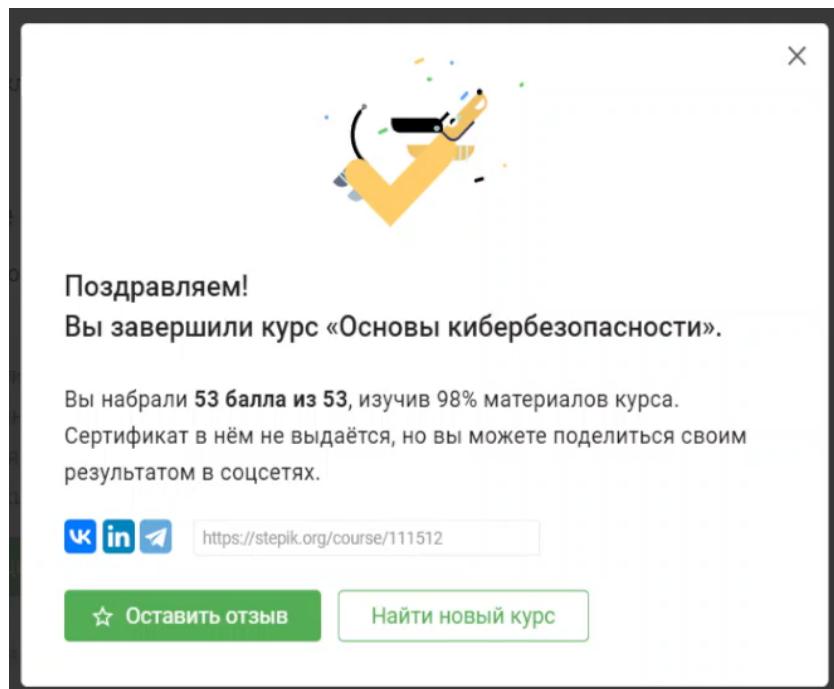


Рис. 5.1: Финал