

Внешний курс. Основы Кибербезопасности

Воробьев Д.П.

Российский университет дружбы народов, Москва, Россия

Информация

- Воробьев Данил Павлович
- Студент группы НБИ 02-23
- Российский университет дружбы народов

- Кулябов Дмитрий Сергеевич
- д.ф.-м.н., профессор
- профессор кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов

Блок 1

Вводная часть

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

Интернет-ресурсы

Основная часть

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

Выберите один вариант из списка



Всё получилось!

Верно решили **895** учащихся

Из всех попыток **58%** верных

☐ UDP

☐ TCP

☒ HTTPS

☐ IP

Следующий шаг

Решить снова

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

Вопрос 2.1.2

На транспортном уровне существует два примера протокола: первый - это ТСР, в честь которого названа модель.

Выберите один вариант из списка



Верно. Так держать!

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

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

Следующий шаг

Решить снова

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

Вопрос 2.1.3

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

Выберите все подходящие ответы из списка

☒ Отлично!

Верно решил **871** 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](#).

☐ 421.0.15.19

☐ 43.12.256.7

☒ 90.11.90.22

☒ 25.198.0.15

Следующий шаг

Решить снова

Вопрос 2.1.4

Основная задача DNS это сопоставлять название (доменное имя, с корректным IP-адресом) с тем, где лежит этот сервер, этот сайт

Выберите один вариант из списка



Абсолютно точно.

Верно решили **933** учащихся
Из всех попыток **66%** верных

- ☒ 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**

[Вопрос 2.1.5

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

Выберите один вариант из списка

☒ Так точно!

Верно решил **941** учащихся
Из всех попыток **53%** верных

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

Вопрос 2.1.6

Протокол http передает не зашифрованные данные, а протокол https уже будет передавать зашифрованные данные

Выберите один вариант из списка

☒ Здорово, всё 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**

Верно решили **965** учащихся
Из всех попыток **78%** верных

Вопрос 2.1.7

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

Выберите один вариант из списка



Хорошая работа.

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, аутентификация сервера, генерация общего ключа

Следующий шаг

Решить снова

Вопрос 2.1.8

TLS определяется клиентом и сервером, чтобы возможно было подключиться

Выберите один вариант из списка



Правильно, молодец!

Верно решили **947** учащихся
Из всех попыток **55%** верных

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

Следующий шаг

Решить снова

Вопрос 2.1.9

Фаза рукопожатия включает в себя:

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

Следовательно вариант с шифрованием лишний

Выберите один вариант из списка

☒ Хорошая работа.

Верно решил **931** учащихся
Из всех попыток **44%** верных

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

Следующий шаг

Решить снова

Персонализация сети Вопрос 2.2.1

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

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 **856** учащихся
Из всех попыток **18%** верных

- ☐ пароль пользователя
- ☒ идентификатор пользователя
- ☒ id сессии
- ☐ IP адрес

Следующий шаг

Решить снова

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

Вопрос 2.2.2

Куки не делают соединение надежным

Выберите один вариант из списка



Так точно!

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**

Куки генерируются сервером

Выберите один вариант из списка

☒ Хорошая работа.

☒ сервером

☐ клиентом

Следующий шаг

Решить снова

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

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

Вопрос 2.2.4

Куки бывают сессионные, удаляются при закрытии окна браузера

Выберите один вариант из списка



Хорошие новости, верно!

Верно решили **959** учащихся

Из всех попыток **60%** верных



Нет



Да, на некоторое время, заданное в сервером



Да, на время пользования веб-сайтом

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: • • •

Браузер TOR. Анонимизация Вопрос 2.3.1

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

Выберите один вариант из списка

☒ Так точно!

Верно решили **959** учащихся
Из всех попыток **77%** верных

☐ 2

☒ 3

☐ 4

Следующий шаг

Решить снова

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

Вопрос 2.3.2

IP-адрес не должен быть известен охранному и промежуточному узлам

Выберите все подходящие ответы из списка



Хорошая работа.

Верно решили **906** 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](#).

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

Следующий шаг

Решить снова

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

Вопрос 2.3.3

В анонимных сетях, таких как Tor, 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.

Выберите один вариант из списка

☒ Отличное решение!

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

Вопрос 2.3.4

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

Выберите один вариант из списка

☒ Так точно!

☐ Да

☒ Нет

Следующий шаг

Решить снова

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

Верно решил **961** учащийся
Из всех попыток **74%** верных

Беспроводные сети Wi-fi Вопрос 2.4.1

WiFi - это технология беспроводной локальной сети, она основана на стандарте IEEE 802.11

Выберите один вариант из списка



Правильно, молодец!

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**

Вопрос 2.4.1

WiFi работает на самом нижнем канальном уровне

Выберите один вариант из списка



Прекрасный ответ.

Верно решили **972** учащихся
Из всех попыток **58%** верных

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

Следующий шаг

Решить снова

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

Вопрос 2.4.1

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

Выберите один вариант из списка



Отлично!

Верно решили **973** учащихся

Из всех попыток **60%** верных

☐ WPA

☒ WEP

☐ WPA2

☐ WPA3

Следующий шаг


Решить снова

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

Вопрос 2.4.1

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

Выберите один вариант из списка

 Правильно, молодец!

Верно решили **975** учащихся
Из всех попыток **53%** верных

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

Следующий шаг

Решить снова

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

Вопрос 2.4.1

WPA2 Personal предназначен для домашнего использования, а WPA2 Enterprise - для коммерческих организаций.

Выберите один вариант из списка

☒ Всё правильно.

Верно решили **975** учащихся
Из всех попыток **87%** верных

☐ WPA2 Personal

☐ WPA2 Enterprise

Следующий шаг

Решить снова

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

Вывод

При выполнении блока “Безопасность в сети” выяснено, как работают сетевые протоколы, куки-файлы, сети вайфай и для чего нужен браузер Tor.

Блок 2

Вводная часть

Выполнить контрольные задания второго блока “Защита ПК/телефона” внешнего курса “Основы кибербезопасности”.

Интернет-ресурсы

Основная часть

Шифрование диска Вопрос 3.1.1

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

Выберите один вариант из списка

☒ Правильно, молодец!

Верно решили **949** учащихся
Из всех попыток **89%** верных

☐ Да

☐ Нет

Следующий шаг

Решить снова

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

Вопрос 3.1.2

Шифрование диска основано на симметричном шифровании

Выберите один вариант из списка

☒ Прекрасный ответ.

Верно решили **972** учащихся
Из всех попыток **66%** верных

- ☐ хэшировании
- ☒ симметричном шифровании
- ☐ асимметричном шифровании

Следующий шаг

Решить снова

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

Вопрос 3.1.3

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



Всё получилось!

Верно решили 28% участников
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
- ☒ VeraCrypt
- ☒ BitLocker
- ☐ Wireshark

Следующий шаг

Решить снова

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

Вопрос 3.2.1 Пароли

Стойкий пароль содержит цифры строчные и заглавные буквы и специальные символы. Это усложняет перебор пароля

Выберите один вариант из списка



Так точно!

Верно решили **969** учащихся
Из всех попыток **85%** верных

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

Следующий шаг

Решить снова

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

Безопасно хранить пароли нужно только в месенджерах

Выберите один вариант из списка



Хорошие новости, верно!

Верно решил **971** учащийся
Из всех попыток **74%** верных

- ☒ 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**

Вопрос 3.2.3

Капча - тест для определения, кто общается с веб-сервисом, человек или бот

Выберите один вариант из списка



Правильно.

Верно решили **974** учащихся

Из всех попыток **77%** верных

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

Следующий шаг

Решить снова

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

Вопрос 3.2.4

В целях безопасности пароли хранят не в открытом виде, а в виде хешей

Выберите один вариант из списка



Верно. Так держать!

Верно решили **973** учащихся

Из всех попыток **61%** верных

- ☐ 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**

Вопрос 3.2.5

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

Выберите один вариант из списка

☒ Хорошие новости, верно!

☐ Да

☒ Нет

Следующий шаг

Решить снова

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

Верно решили **967** учащихся
Из всех попыток **66%** верных

Вопрос 3.2.6

Для безопасности нужно использовать длинные, сложные пароли, регулярно обновлять и хранить пароли в месенджерах паролей.

Выберите все подходящие ответы из списка



Прекрасный ответ.

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**

Фишинг Вопрос 3.3.1

Пример фишинга - эта маскировка под известные веб-сайты только с другим доменным именем

Выберите все подходящие ответы из списка



Прекрасный ответ.

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: ...

Вопрос 3.3.2

Может фишинговое письмо прийти и от знакомого

Выберите один вариант из списка

☒ Прекрасный ответ.

Верно решили **966** учащихся
Из всех попыток **90%** верных

☐ Да

☐ Нет

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: •••

Спуфинг - это подмена адреса отправителя в имейлах

Выберите один вариант из списка



Так точно!

Верно решили **960** учащихся

Из всех попыток **65%** верных

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

Следующий шаг

Решить снова

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

Вопрос 3.4.2

Троян маскируется под обыкновенную безобидную программу, при запуске которой вирус легко проникает в ваш компьютер и поражает его

Выберите один вариант из списка



Правильно.

Верно решили **969** учащихся

Из всех попыток **74%** верных

- ☐ 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**

Безопасность мессенджеров Вопрос 3.5.1

При генерации первого сообщения отправителем формируется ключ шифрования

Выберите один вариант из списка



Правильно.

Верно решили **952** учащихся
Из всех попыток **52%** верных

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

Следующий шаг

Решить снова

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

Вопрос 3.5.2

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 зашифрованный текст Бобу, а Боб его расшифровывает. Сервер не имеет доступа к ключам или открытому тексту сообщения.

Выберите один вариант из списка

☒ Абсолютно точно.

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**

Второй блок курса “Основы кибербезопасности” дал понять правила составления и хранения паролей, понял много нового о вирусах и мерах безопасности против них.

Блок 3

Вводная часть

Выполнить контрольные задания третьего блока “Криптография на практике” внешнего курса “Основы кибербезопасности”.

Интернет-ресурсы, Информация с лекций курса.

Основная часть

Выполнение заданий блока “Основы Кибербезопасности”

В асимметричной криптографии у каждой из сторон есть пара ключей: открытый и секретный ключ

Выберите один вариант из списка

☒ Отлично!

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

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

Следующий шаг

Решить снова

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

Выполнение заданий блока “Основы Кибербезопасности”

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

Выберите все подходящие ответы из списка



Всё правильно.

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
- ☐ обеспечивает конфиденциальность захешированных данных
- ☒ эффективно вычисляется

Следующий шаг

Решить снова

Выполнение заданий блока “Основы Кибербезопасности”

Отмечены алгоритмы цифровой подписи

Выберите все подходящие ответы из списка



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 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**

Выполнение заданий блока “Основы Кибербезопасности”

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

Выберите один вариант из списка



Здорово, всё верно.

Верно решили **955** учащихся
Из всех попыток **69%** верных



асимметричным примитивам



симметричным примитивам

Следующий шаг

Решить снова

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

Выполнение заданий блока “Основы Кибербезопасности”

Чтобы ответить на данный вопрос использую определение Диффи-Хэллмана

Выберите один вариант из списка

✓ Отлично!

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**

Выполнение заданий блока Цифровая подпись

По определению цифровой подписи протокол ЭЦП относится к протоколам с публичным ключом

протокол электронной цифровой подписи относится к

Выберите один вариант из списка



Хорошие новости, верно!

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**

Выполнение заданий блока Цифровая подпись

Каждая машина процедуру верификации, которая берет на вход само обновление, подпись и открытый ключ разработчика

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Верно.

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

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

Следующий шаг

Решить снова

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

Выполнение заданий блока Цифровая подпись

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

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

Верно решили 968 учащихся

Выполнение заданий блока Цифровая подпись

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.

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

Выберите один вариант из списка

☒ Верно. Так держать!

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

- ☐ простая
- ☐ усиленная неквалифицированная
- ☒ усиленная квалифицированная

Следующий шаг

Решить снова

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

Выполнение заданий блока Цифровая подпись

Сертификат подписывается с помощью электронной подписи уже доверенной стороной, удостоверяющим центром.

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

Выберите один вариант из списка

☒ Отлично!

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**

Выполнение заданий блока Электронные платежи

На данный момент существуют такие платежные системы, как: Visa, MasterCard, МИР

Выберите из списка все платежные 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

Выполнение заданий блока Электронные платежи

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.

Выполнение заданий блока 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

При онлайн платежах сегодня используется

Выберите один вариант из списка

☒ Так точно!

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

Выполнение заданий блока Блокчейн

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.

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выполнение заданий блока Блокчейн

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.

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка



Хорошие новости, верно!

Верно решили **864** учащихся
Из всех попыток **23%** верных

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на

В результате 3 этапа я узнал много нового о криптографии, цифровых подписях и технологиях блокчейна. Выяснил как обеспечивается безопасность транзакций.

Общий вывод

В результате выполнения внешнего курса я узнал как работают сетевые пратаколы, куки-файлы, сети вайфай и для чего нужен браузер Tor. :::