

Отчет о прохождении внешнего курса

Основы информационной безопасности

**Выполнила: Пестова Ева
Константиновна**

Группа: НКАбд-03-23

Москва. Российский университет дружбы народов. 2025 год

Цель работы

Изучить основы кибербезопасности, с помощью курса на stepic и проверить свои знания с помощью контрольных вопросов.

Задание

- Пройти курс.
- Получить сертификат.
- Записать видео (с записью камерой лица) по прохождению контрольных мероприятий (тесты и задания) по каждому разделу + итоговая презентация по каждому этапу.
- Написать отчёт по прохождению контрольных мероприятий (тесты и задания) по каждому разделу.

Выполнение

2.1

Выберите один вариант из списка

☒ Отлично!

☐ UDP

☐ TCP

☒ HTTPS

☐ IP

Следующий шаг

Решить снова

Рисунок 2.1-1

Комментарий: Протокол HTTPS используется для безопасной передачи данных — в отличие от HTTP, он шифрует трафик.

На каком уровне работает протокол TCP?

Выберите один вариант из списка

✓ Правильно.

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

Следующий шаг

Решить снова

Рисунок 2.1-2

Комментарий: Протокол TCP работает на транспортном уровне, обеспечивая надёжную доставку данных.

Выберите все корректные адреса IPv4

Выберите все подходящие ответы из списка

✓ Хорошая работа.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [форуме решений](#), 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

Рисунок 2.1-3

Комментарий: Корректные IPv4-адреса должны быть в диапазоне от 0.0.0.0 до 255.255.255.255 без некорректных значений (например, 421 или 256).

DNS сервер

Выберите один вариант из списка

☒ Отлично!

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

Следующий шаг

Решить снова

Рисунок 2.1-4

Комментарий: DNS-сервер сопоставляет доменные имена с IP-адресами — именно это его основная функция.

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

✓ Отличное решение!

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

Следующий шаг

Решить снова

Рисунок 2.1-5

Комментарий: Правильная последовательность протоколов TCP/IP: прикладной → транспортный → сетевой → канальный.

Протокол http предполагает

Выберите один вариант из списка

✓ Абсолютно точно.

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

Следующий шаг

Решить снова

Рисунок 2.1-6

Комментарий: HTTP передаёт данные в открытом виде, без шифрования — это делает его небезопасным в публичных сетях.

Протокол https состоит из

Выберите один вариант из списка

✓ Отлично!

- ☐ 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

Рисунок 2.1-7

Комментарий: Протокол HTTPS состоит из двух фаз: рукопожатия и передачи данных — в первой фазе устанавливаются параметры безопасности.

Версия протокола TLS определяется

Выберите один вариант из списка

✓ Отличное решение!

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

Следующий шаг

Решить снова

Рисунок 2.1-8

Комментарий: Версия TLS определяется в процессе переговоров между клиентом и сервером — это двусторонний процесс.

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

☒ Правильно, молодец!

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

Следующий шаг

Решить снова

Рисунок 2.1-9

Комментарий: На этапе 'рукопожатия' TLS не происходит шифрования данных — только выбор параметров и аутентификация.

2.2

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

☒ Всё правильно.

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

Следующий шаг

Решить снова

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

Рисунок 2.2-1

Комментарий: Сессионные куки действительно хранятся в браузере только на время активного взаимодействия с сайтом — после закрытия вкладки или браузера они удаляются.

Куки генерируются

Выберите один вариант из списка

✓ Правильно.

☐ клиентом

☒ сервером

Следующий шаг

Решить снова

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

Рисунок 2.2-2

Комментарий: Куки создаются сервером, поскольку именно сервер управляет механизмом идентификации пользователя.

Куки не используются для

Выберите один вариант из списка

✓ Так точно!

☐ аутентификации пользователя

☐ персонализации веб-страниц

☐ отслеживания информации о пользователе

☐ сборе статистики посещаемости сайта

☒ улучшения надежности соединения

Следующий шаг

Решить снова

Рисунок 2.2-3

Комментарий: Куки не применяются для улучшения надёжности соединения — это задача других технологий, например, TCP и TLS.

Куки хранят:

Выберите все подходящие ответы из списка

☒ Всё получилось!

Вы решили сложную задачу, поздравляем! Вы можете помочь другим, отвечая на их вопросы, или сравнить своё решение с другими.

☒ идентификатор пользователя

☒ id сессии

☐ IP адрес

☐ пароль пользователя

Следующий шаг

Решить снова

Рисунок 2.2-4

Комментарий: Куки используются для хранения информации об идентификаторе пользователя и сессии — это необходимо для аутентификации и сохранения состояния входа.

2.3

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

Выберите один вариант из списка

☒ Так точно!

Верно решил 961 учащ
Из всех попыток 74% в

☐ Да
☒ Нет

Следующий шаг

Решить снова

Рисунок 2.3-1

Комментарий: Получателю не обязательно использовать браузер Tor — он получает пакеты через обычный браузер, если они были отправлены с маршрутизацией по Tor.

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

☒ Верно. Так держать!

☐ только с охранным узлом
☐ с охранным и промежуточным узлом
☒ с охранным, промежуточным и выходным узлом
☐ с промежуточным и выходным узлом

Следующий шаг

Решить снова

Рисунок 2.3-2

Комментарий: Общий секретный ключ генерируется отправителем для всех узлов маршрута (охранного, промежуточного и выходного), чтобы обеспечить шифрование на всём пути.

IP-адрес получателя известен

Выберите все подходящие ответы из списка

☒ Так точно!

Вы решили сложную задачу, поздравляем! Вы можете помочь другим, отвечая на их вопросы, или сравнить своё решение с другими на

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

Следующий шаг

Решить снова

Рисунок 2.3-3

Комментарий: IP-адрес получателя известен только отправителю и выходному узлу — остальные узлы не имеют этой информации, что обеспечивает анонимность.

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

☒ Абсолютно точно.

☐ 2

☒ 3

☐ 4

Следующий шаг

Решить снова

Рисунок 2.3-4

Комментарий: В луковой маршрутизации TOR используется 3 узла: охранный, промежуточный и выходной — они шифруют данные послойно, как "луковица".

2.4

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

☒ Здорово, всё верно.

☒ WPA2 Personal

☐ WPA2 Enterprise

Следующий шаг

Решить снова

Рисунок 2.4-1

Комментарий: В домашних сетях чаще всего используется метод аутентификации WPA2 Personal, поскольку он основан на общем пароле и не требует сложной инфраструктуры.

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

☒ Всё получилось!

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

Следующий шаг

Решить снова

Рисунок 2.4-2

Комментарий: После успешной аутентификации устройства, данные между хостом и роутером передаются в зашифрованном виде — это основа безопасности беспроводных сетей.

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

✓ Правильно.

- ☐ WPA
- ☒ WEP
- ☐ WPA2
- ☐ WPA3

Следующий шаг

Решить снова

Рисунок 2.4-3

Комментарий: WEP — устаревший и уязвимый стандарт безопасности Wi-Fi, давно признан небезопасным, его использование не рекомендуется.

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

✓ Отличное решение!

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

Следующий шаг

Решить снова

Рисунок 2.4-4

Комментарий: Протокол Wi-Fi работает на канальном уровне модели OSI, обеспечивая передачу кадров по беспроводному каналу.

Wi-Fi - это

Выберите один вариант из списка

☒ Верно. Так держать!

Be
Из

- ☐ 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

Рисунок 2.4-5

Комментарий: Wi-Fi — это технология беспроводной локальной сети (WLAN), работающая по стандарту IEEE 802.11.

3.1

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

✓ Хорошая работа.

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

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

Следующий шаг

Решить снова

Рисунок 3.1-1

Комментарий: BitLocker, Disk Utility и VeraCrypt — это программы для шифрования жёстких дисков. Wireshark не подходит, так как используется для анализа сетевого трафика.

Шифрование диска основано на

Выберите один вариант из списка

☒ Хорошая работа.

- ☐ хэшировании
- ☒ симметричном шифровании
- ☐ асимметричном шифровании

Следующий шаг

Решить снова

Рисунок 3.1-2

Комментарий: Шифрование диска обычно осуществляется с использованием симметричного шифрования — один ключ используется для шифрования и дешифрования данных.

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Правильно, молодец!

☒ Да

☐ Нет

Следующий шаг

Решить снова

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

Рисунок 3.1-3

Комментарий: Загрузочный сектор диска может быть зашифрован — это делает всю систему защищённой, начиная с момента запуска.

3.2

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

☒ Правильно, молодец!

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

Рисунок 3.2-1

Комментарий: Все перечисленные меры — уникальные и сложные пароли, смена паролей и капча — эффективно защищают от атак методом перебора.

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** учащихся
Из всех попыток **66%** верных

- ☐ Да
- ☒ Нет

Следующий шаг

Решить снова

Рисунок 3.2-2

Комментарий: Соль не улучшает стойкость паролей при атаке перебором, если злоумышленник уже получил доступ к серверу. Она помогает против атак по словарю и радужных таблиц.

Для чего применяется хэширование паролей?

Выберите один вариант из списка

☒ Абсолютно точно.

- ☐ 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

Рисунок 3.2-3

Комментарий: Хэширование паролей позволяет не хранить их в открытом виде — это критически важно для безопасности пользовательских данных.

Зачем нужна капча?

Выберите один вариант из списка

☒ Абсолютно точно.

Верно р
Из всех

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

Следующий шаг

Решить снова

Рисунок 3.2-4

Комментарий: Капча используется для защиты от автоматизированных атак, предотвращая массовый перебор паролей ботами.

Где безопасно хранить пароли?

Выберите один вариант из списка

☒ Так точно!

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

Следующий шаг

Решить снова

Рисунок 3.2-5

Комментарий: Пароли надёжнее всего хранить в специализированных менеджерах паролей, а не в заметках, файлах или на бумаге.

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

☒ Абсолютно точно.

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

Следующий шаг

Решить снова

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

Рисунок 3.2-6

Комментарий: Стойкий пароль — это сложная комбинация символов, цифр и знаков. Пример `UQr9@j4!S$$` отвечает требованиям безопасности.

3.3

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

☒ Всё правильно.

- ☒ Да
☐ Нет

Следующий шаг

Решить снова

Рисунок 3.3-1

Комментарий: Фишинговый e-mail вполне может прийти от знакомого адреса — злоумышленники могут подделывать адрес отправителя (спуфинг) или взломать почту реального человека.

Какие из следующих ссылок являются фишинговыми?

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](#).

- ☐ <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

Рисунок 3.3-2

Комментарий: Ссылки с поддоменами известных компаний на чужих доменах (например, `wix.ru`, `ucoz.ru`) являются фишинговыми — они маскируются под легитимные сервисы, но ведут на сторонние ресурсы.

3.4

Вирус-троян

Выберите один вариант из списка

☒ Верно. Так держать!

- ☐ обязательно шифрует данные и требует ключ дешифрования
- ☒ маскируется под легитимную программу
- ☐ работает исключительно под ОС Windows
- ☐ разработан греками

Следующий шаг

Решить снова

Рисунок 3.4-1

Комментарий: Троян — это тип вредоносного ПО, которое маскируется под легитимную программу, чтобы обманом заставить пользователя установить его на устройство.

Email Спуфинг -- это

Выберите один вариант из списка

☒ Прекрасный ответ.

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

Следующий шаг

Решить снова

Рисунок 3.4-2

Комментарий: Email спуфинг — это подмена адреса отправителя, при которой письмо выглядит как отправленное с доверенного источника. Этот метод используется в фишинговых атаках для повышения доверия к письму.

3.5

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

☒ Хорошая работа.

- ☒ 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

Рисунок 3.5-1

Комментарий: Суть сквозного шифрования (end-to-end encryption) заключается в том, что сообщение передаётся в зашифрованном виде через все промежуточные узлы, и только конечный получатель может его расшифровать.

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

☒ Здорово, всё верно.

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

Следующий шаг

Решить снова

Рисунок 3.5-2

Комментарий: В протоколе Signal ключ шифрования формируется при генерации первого сообщения отправителем. Это позволяет обеспечить защиту информации с самого начала общения.

4.1

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

✓ Хорошая работа.

- ☐ 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

Рисунок 4.1-1

Комментарий: Диффи-Хеллман используется для генерации общего секретного ключа между двумя сторонами по открытому каналу. Поэтому правильный ответ — *асимметричный примитив генерации общего секретного ключа*.

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Всё правильно.

- ☐ асимметричным примитивам
- ☒ симметричным примитивам

Следующий шаг

Решить снова

Рисунок 4.1-2

Комментарий: Код аутентификации сообщения (MAC) строится на основе симметричных криптографических примитивов, где используется общий секретный ключ.

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

✓ Всё получилось!

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

Рисунок 4.1-3

Комментарий: Алгоритмы RSA, ECDSA и ГОСТ Р 34.10-2012 являются стандартными схемами цифровой подписи. AES и SHA2 не относятся к цифровым подписям: AES — алгоритм шифрования, SHA2 — хеш-функция.

Криптографическая хэш-функция

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](#).

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

Следующий шаг

Решить снова

Рисунок 4.1-4

Комментарий: Хеш-функция должна быть стойкой к коллизиям, давать фиксированную длину хеша и эффективно вычисляться. Конфиденциальность данных — задача шифрования, а не хеширования.

В асимметричных криптографических примитивах

Выберите один вариант из списка

✓ Верно. Так держать!

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

Следующий шаг

Решить снова

Рисунок 4.1-5

Комментарий: В асимметричной криптографии каждая сторона имеет пару ключей (открытый и закрытый), что позволяет безопасно обмениваться информацией и проверять подписи.

4.2

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

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решил 971 уч
Из всех попыток 61%

- ☐ в любой организации, имеющей соответствующую лицензию ФСБ
- ☐ в минкомсвязи РФ
- ☒ в удостоверяющем (сертификационном) центре
- ☐ в любой организации по месту работы

Следующий шаг

Решить снова

Рисунок 4.2-1

Комментарий: Квалифицированный сертификат ключа проверки электронной подписи можно получить только в удостоверяющем центре, так как именно он аккредитован для выпуска таких сертификатов в соответствии с законодательством.

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

Выберите один вариант из списка

☒ Так точно!

☐ простая

☒ усиленная квалифицированная

☐ усиленная неквалифицированная

Следующий шаг

Решить снова

Верно
Из всех

Ваш ответ: **Правильно! 1 балл**

Рисунок 4.2-2

Комментарий: Для отправки отчётности в ФНС требуется усиленная квалифицированная электронная подпись, так как она имеет юридическую силу и соответствует требованиям к защите информации.

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

✓ Всё правильно.

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

Следующий шаг

Решить снова

Рисунок 4.2-3

Комментарий: Электронная подпись не обеспечивает конфиденциальность, она используется для аутентификации, целостности и невозможности отказа от авторства, но не шифрует передаваемые данные.

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

✓ Хорошая работа.

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

Следующий шаг

Решить снова

Рисунок 4.2-4

Комментарий: Для верификации электронной подписи необходимо использовать саму подпись, открытый ключ и сообщение — это позволяет проверить подлинность без знания закрытого ключа.

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Верно. Так держать!

- ☐ протоколам с симметричным ключом
- ☒ протоколам с публичным (или открытым) ключом

Следующий шаг

Решить снова

Рисунок 4.2-5

Комментарий: Протокол ЭЦП использует криптографию с открытым (публичным) ключом — именно эта модель обеспечивает проверку подписи без раскрытия закрытого ключа.

4.3

При онлайн платежах сегодня используется

Выберите один вариант из списка

✓ Здорово, всё верно.

- ☒ 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**

Рисунок 4.3-1

Комментарий: Сегодня при онлайн-платежах чаще всего используется многофакторная аутентификация перед банком-эмитентом — например, подтверждение через приложение или код из SMS, что позволяет надёжно идентифицировать пользователя.

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

☒ Всё правильно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся, 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

Рисунок 4.3-2

Комментарий: Многофакторная аутентификация — это сочетание разных факторов: знания (пароль), владения (смартфон с SMS), биометрии (отпечаток пальца). Поэтому комбинации пароля и кода, а также кода и отпечатка — корректные примеры.

Выберите из списка все платёжные системы.

Выберите все подходящие ответы из списка

✔ Отлично!

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

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

Рисунок 4.3-3

Комментарий: Платёжными системами являются именно сети и организации, обрабатывающие транзакции — например, MasterCard и МИР. Bitcoin — криптовалюта, а не платёжная система в традиционном смысле, POS-терминал и банкомат — устройства, а не системы.

4.4

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

✓ Хорошие новости, верно!

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

Следующий шаг

Решить снова

Рисунок 4.4-1

Комментарий: В блокчейне используются цифровые подписи, для которых участники хранят секретные ключи. Это необходимо для подтверждения подлинности транзакций и авторизации действий пользователя.

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 курсе, отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

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

Следующий шаг

Решить снова

Рисунок 4.4-2

Комментарий: Консенсус в блокчейн-системах обладает такими свойствами, как постоянство (данные не меняются), живучесть (система продолжает работу), открытость (участие доступно всем) и сам консенсус — достижение единства между узлами.

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

☒ Абсолютно точно.

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

Следующий шаг

Решить снова

Рисунок 4.4-3

Комментарий: Свойство криптографической хэш-функции, критически важное для доказательства работы (Proof of Work), — это сложность нахождения прообраза. Она обеспечивает необходимую вычислительную нагрузку для подтверждения блока.

Выводы

В результате прохождения курса я получила базовые и прикладные знания в области информационной безопасности. Разобралась в принципах работы электронной подписи, видах сертификатов и ключей, а также в способах защиты от основных угроз. Курс оказался полезным и дал понимание, как безопасно работать с электронными документами и защищать свои данные.

Список литературы

1. <https://stepik.org/course/111512>