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

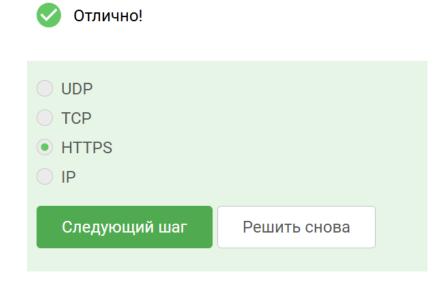


Рисунок 2.1-1

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

На каком уровне работает протокол ТСР?

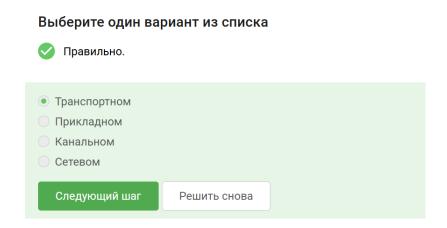


Рисунок 2.1-2

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

Выберите все корректные адреса IPv4



Рисунок 2.1-3

Комментарий: Корректные IPv4-адреса должны быть в диапазоне от 0.0.0.0 до 255.255.255 без некорректных значений (например, 421 или 256).

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.

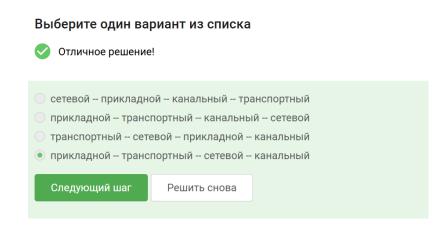


Рисунок 2.1-5

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

Протокол http предпол	агает	
Выберите один вар Абсолютно точно.	риант из списка	
 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.

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.

Сессионные куки хранятся в браузере?

Ваши решения Вы получили: 1 балл

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

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.

Выберите один вариант из списка Правильно.



Рисунок 2.2-2

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

Куки не используются для

Выберите один вариант из списка

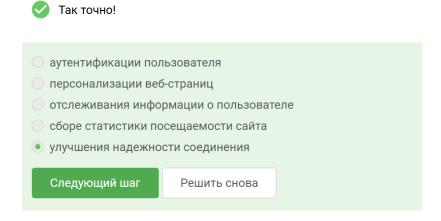


Рисунок 2.2-3

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

Куки хранят:

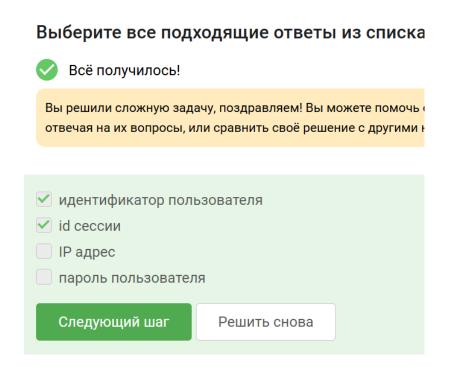


Рисунок 2.2-4

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

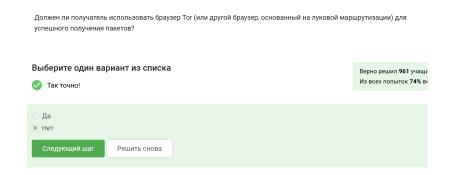


Рисунок 2.3-1

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!

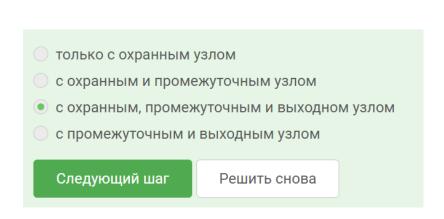


Рисунок 2.3-2

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

ІР-адрес получателя известен

выоерите все подх	одящие ответь	і из списка
🗸 Так точно!		
Вы решили сложную зада отвечая на их вопросы, ил		
охранному узлу		
промежуточному узл	іу	
✓ 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.

Выберите один вариант из списка ✓ Абсолютно точно. ✓ 2 ✓ 3 ✓ 4 Следующий шаг Решить снова

Рисунок 2.3-4

Комментарий: В луковой маршрутизации ТОR 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 ва	риант из списка	
Всё получилось!		
🔾 передаются в открь	том виде после ауте	нтификации устройств
🔾 передаются в зашис	ррованном виде	
🔾 передаются в открь	том 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.

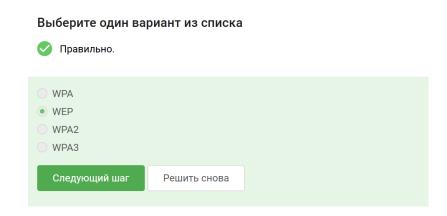


Рисунок 2.4-3

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

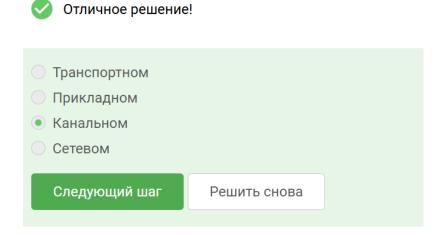


Рисунок 2.4-4

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

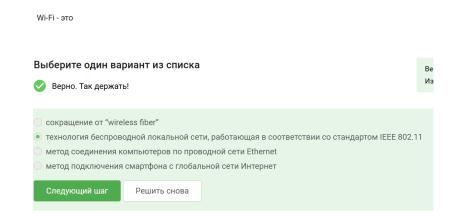


Рисунок 2.4-5

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

Выберите все подходящие ответы из списка

Хорошая работа.

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

Wireshark

BitLocker

Disk Utility

VeraCrypt

Следующий шаг

Решить снова

С помощью каких программ можно зашифровать жесткий диск?

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.

Выберите один вариант из списка

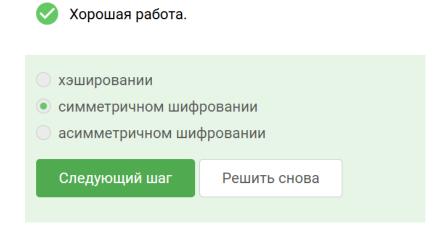


Рисунок 3.1-2

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

Выберите один вариант из списка ✓ Правильно, молодец! Ода 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.

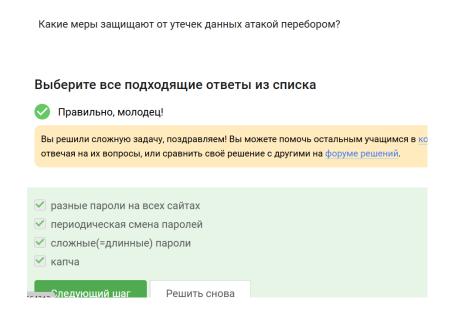


Рисунок 3.2-1

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

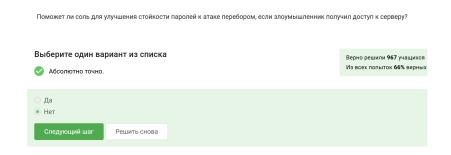


Рисунок 3.2-2

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.

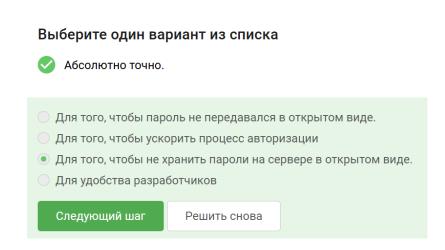


Рисунок 3.2-3

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

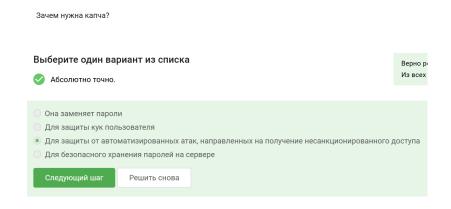


Рисунок 3.2-4

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

Выберите один вариант из списка

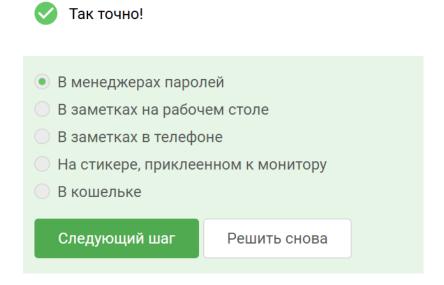


Рисунок 3.2-5

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.

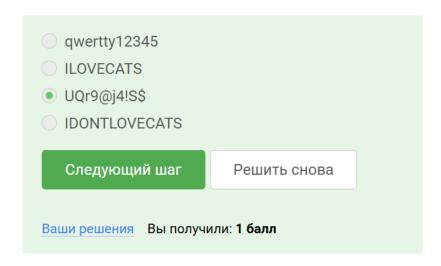


Рисунок 3.2-6

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

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.

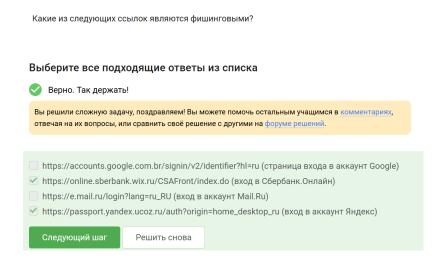


Рисунок 3.3-2

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 вар	риант из списка	
🛭 Верно. Так держаты	,!	
обязательно шифруемаскируется под легработает исключителразработан греками	итимную программ	
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.

Следующий шаг

Выберите один вариант из списка Прекрасный ответ. метод предотвращения фишинга протокол для отправки имейлов атака перебором паролей подмена адреса отправителя в имейлах

Рисунок 3.4-2

Решить снова

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.

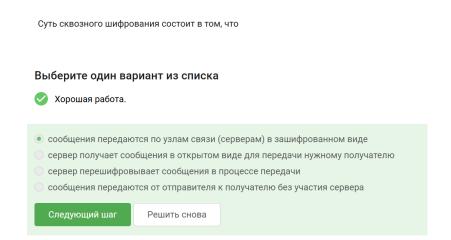


Рисунок 3.5-1

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.

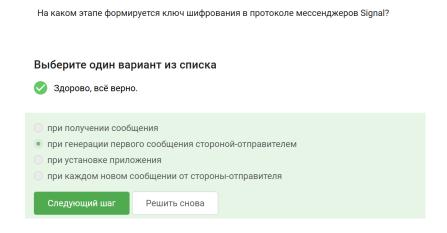


Рисунок 3.5-2

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	I-Хэллмана - это
Выберите один ва	риант из списка
🗸 Хорошая работа.	
асимметричный при	митив генерации общего секретного ключа имитив генерации общего открытого ключа имитив генерации общего секретного ключа
асимметричный алг	
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

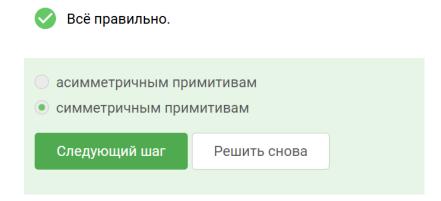
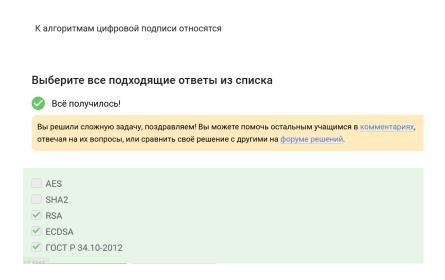


Рисунок 4.1-2

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



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.

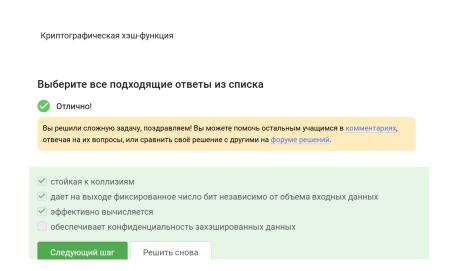


Рисунок 4.1-4

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

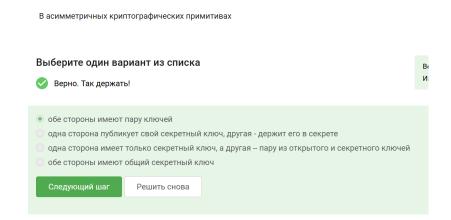


Рисунок 4.1-5

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

4.2

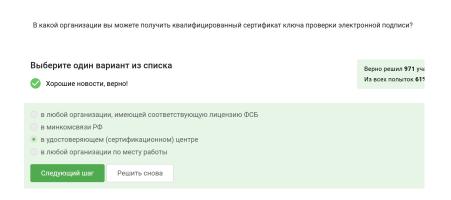


Рисунок 4.2-1

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.

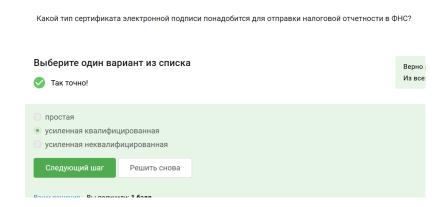


Рисунок 4.2-2

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

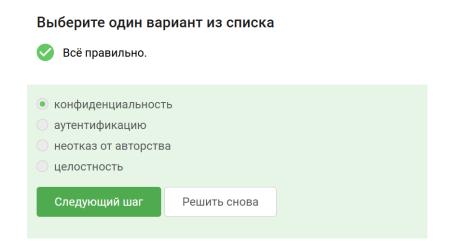


Рисунок 4.2-3

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

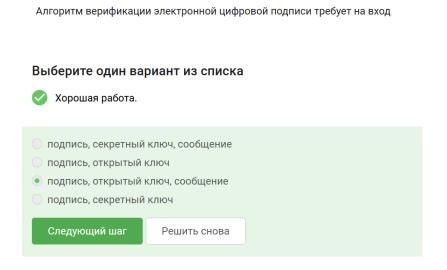


Рисунок 4.2-4

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.

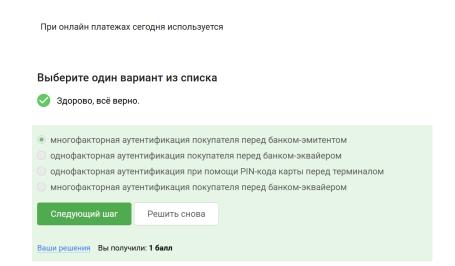


Рисунок 4.3-1

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.

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 платежные системы.

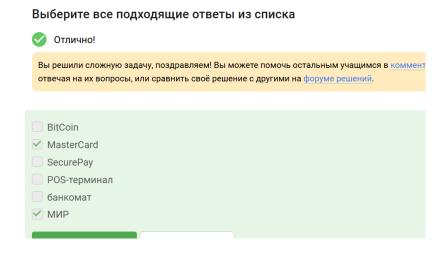


Рисунок 4.3-3

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.

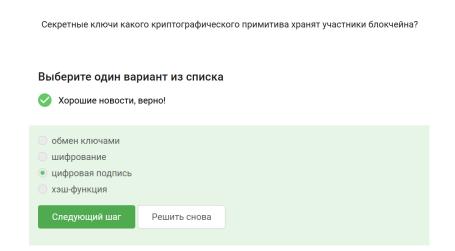


Рисунок 4.4-1

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

Выберите все подходящие ответы из списка

Консенсус в некоторых системах блокчейн обладает свойствами

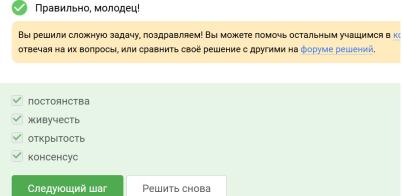


Рисунок 4.4-2

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 крипт	ографической хэш-функции используется в доказательстве работы?
Выберите один ва	риант из списка
Абсолютно точно.	
фиксированная дли	на выходных данных
• сложность нахожде	ния прообраза
обеспечение целост	ности
эффективность выч	исления
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