Прохождения внешнего курса на тему Основы кибербезопасности. Часть 1

Основы информационной безопасности

Просина К. М.

17 май 2025

Российский университет дружбы народов, Москва, Россия



Докладчик

- Просина Ксения Максимовна
- студент 2 курса
- факультет физико-математических и естественных наук
- Российский университет дружбы народов
- 1132231938@rudn.ru

1 О курсе

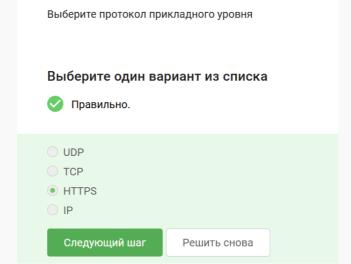
1 О курсе

В этом разделе описана общая информация о курсе, определены цели и дальнейшие планы по курсу. Также даны ссылки на литературу и полезные ссылки.

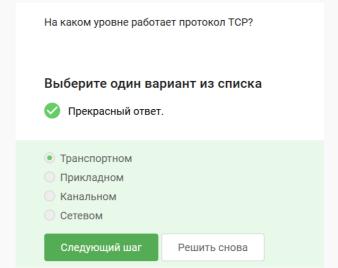
2 Безопасность в сети

21 Как работает интернет: базовые

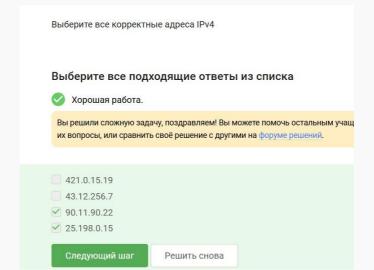
сетевые протоколы



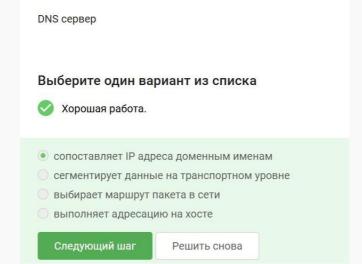
Пояснение ответа: Протоколы UDP, TCP относятся к транспортному уровню, HTTPS к прикладному, IP к сетевому уровню.



Пояснение ответа: Протокол ТСР работает на транспортном уровне и отвечает за надежную передачу данных.



Пояснение ответа: В 4 версии ір адрес представляет собой 32 битное число, записывается в виде четырех десятичных чисел значения от 0 до 255(8 битов). Из чего следует, что 421.0.15.19 и 43.12.256.7 не подходят.



Пояснение ответа: Основная задача DNS сервера это сопоставить название, то есть доменное имя, с корректным ір адресом, с тем, где лежит этот сервер, этот сайт.

Вопрос/Ответ 5

Выберите корректную последовательность протоколов в модели TCP/IP Выберите один вариант из списка Верно. сетевой – прикладной – канальный – транспортный прикладной -- транспортный -- канальный -- сетевой транспортный -- сетевой -- прикладной -- канальный прикладной -- транспортный -- сетевой -- канальный Следующий шаг Решить снова

Пояснение ответа: Модель TCP/IP состоит из четырех уровней: - Прикладной

- Транспортный
- Сетевой
- Канальный

Вопрос/Ответ 6

Протокол http предполагает Выберите один вариант из списка Так точно! передачу зашифрованных данных между клиентом и сервером 🍥 передачу данных между клиентом и сервером в открытом виде Следующий шаг Решить снова

Пояснение ответа: Протокол прикладного уровня http в отличие от https передает данные между клиентом и сервером в открытом виде.

Вопрос/Ответ 7

Протокол https состоит из

Выберите один вариант из списка

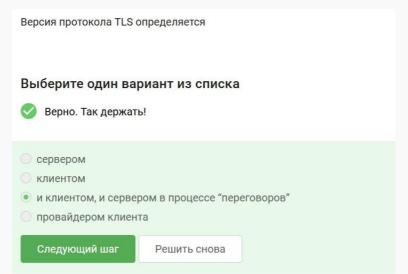
- Правильно, молодец!
- одной фазы аутентификации сервера
- двух фаз: рукопожатия и передачи данных
- 🔘 двух фаз: аутентификация клиента и сервера и шифрования данных
- 🔾 трех фаз: аутентификации клиента, аутентификация сервера, генерация общего ключа

Следующий шаг

Решить снова

Пояснение ответа: Протокол https состоит из двух фаз:

- Рукопожатие(идентификация между сервером и клиентом)
- Передача данных



Пояснение ответа: В ходе TLS-рукопожатия клиент и сервер совместно авполняют следующие действия:

- Указывают какую версию TLS они будут использовать
- Какие наборы шрифтов они будут использовать
- Аутентификация идентичности сервера с помощью открытого ключа сервера и цифровой подписи центра сертификации ssl
- Генерация сеансовых ключей для использования симметричного шифрования после завершения рукопожатия.

Вопрос/Ответ 9

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

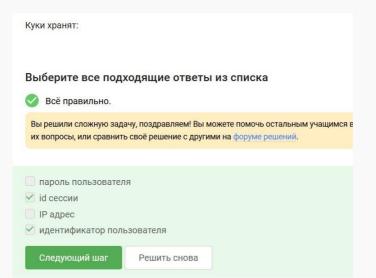


- 🔾 формирование общего секретного ключа между клиентом и сервером
- аутентификация (как минимум одной из сторон)
- 🔘 выбираются алгоритмы шифрования/аутентификации
- шифрование данных

Следующий шаг

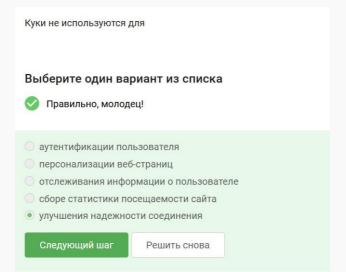
Решить снова

Пояснение ответа: Рукопожатие - идентификация между сервером и клиентом, оно не подразумевает шифрование данных.



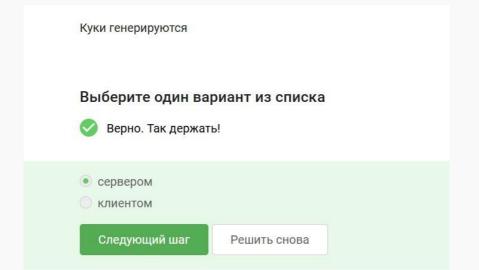
Пояснение ответа: Куки хранят:

- id пользователя
- id сессии
- тип браузера, время запросов
- некоторые действия пользователя

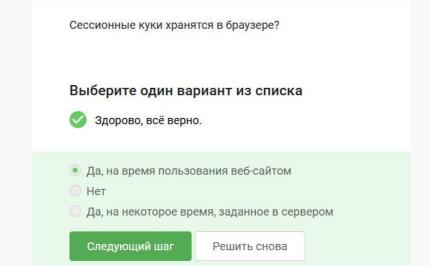


Пояснение ответа: Куки - данные, передаваемые от сервера к клиенту для его идентификации. Куки позволяют:

- Сохранять сессионную информацию
- Персонализировать страницы



Пояснение ответа: Куки генерируется сервером, и запрашивает разрешение на использование клиентом.





Пояснение ответа: Сессионные куки хранятся в браузере на время пользование веб сайтом.

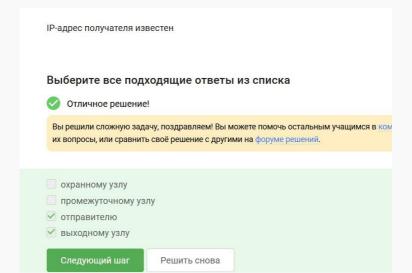
23 Браузер TOR. Анонимизация

2.3 Браузер TOR. Анонимизация

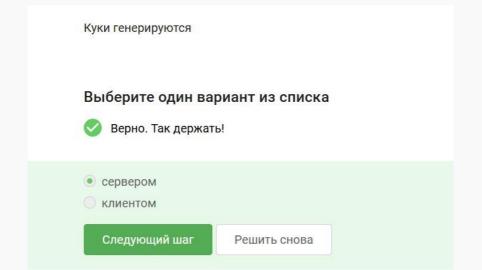


Пояснение ответа: В луковой сети TOR три промежуточных узла:

- Охранный узел
- Промежуточный узел
- Выходной узел



Пояснение ответа: IP адрес отправителя известен только отправителю и выходному узлу, в охранном и промежуточном узле он зашифрован.



Пояснение ответа: Отправитель генерирует общий секретный ключ со всеми узлами(охранным, промежуточным, выходным), они одеты друг на друга как оболочка у лука.

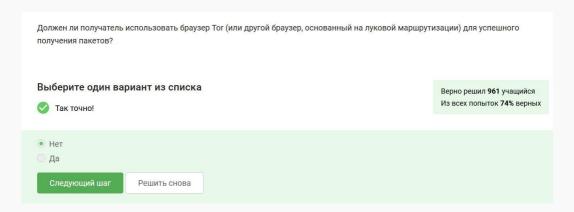


Рис. 17: Вопрос/Ответ 4

Пояснение ответа: Получателю не обязательно использовать браузер TOR для успешного получения пакетов.

Вопрос/Ответ 1

Wi-Fi - это

Выберите один вариант из списка

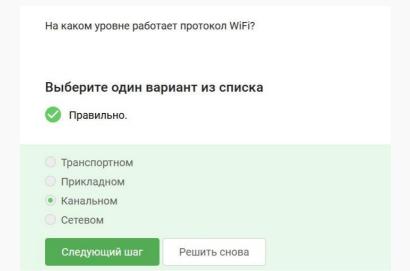


- окращение от "wireless fiber"
- 🌒 технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11
- метод соединения компьютеров по проводной сети Ethernet
- 🔘 метод подключения смартфона с глобальной сети Интернет

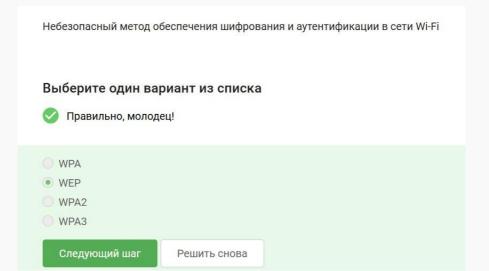
Следующий шаг

Решить снова

Пояснение ответа: WiFi - технология беспроводной локальной сети, работающей в соответствии со стандартами IEEE 802.11.



Пояснение ответа: Протокол WiFi работает на самом низком уровне, канальном уровне.



Пояснение ответа: Самым ранним и на сегодняшний день небезопасный метод шифрования данных WiFi называется WEP. Он устарел и уже категорически не рекомендуется к использованию, потому что использовал малую длину ключа, 40 бит.

Вопрос/Ответ 4

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка



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

Следующий шаг

Решить снова

Пояснение ответа: Данные между хостом сети и роутером передаются в зашифрованном виде после аутентификации устройств.

Вопрос/Ответ 5

Для домашней сети для аутентификации обычно используется метод Выберите один вариант из списка Прекрасный ответ. WPA2 Personal WPA2 Enterprise Следующий шаг Решить снова

Пояснение ответа: Для домашней сети для аутентификации обычно используется метод WPA2 Personal, который использует пароль для аутентификации, в то время как WPA2 Enterprise использует базу данных с пользователями, которые могут подключиться к WiFi.