## Первый этап внешнего курса

Основы информационной безопасности

Казазаев Д. М.

Российский университет дружбы народов, Москва, Россия

Информация

#### Докладчик

- Казазаев Даниил Михайлович
- Студент бакалавриата
- Российский университет дружбы народов
- · [1132231427@rudn.ru]
- https://github.com/KazazaevDaniil/study\_2024-2025\_infosecintro

## Вводная часть

#### Материалы и методы

Внешний кур состоит из трех этапов.

### Этап первый

### Первый этап курса состоит из 4 частей:

- 1. Базовые сетевые протоколы
- 2. Персонализация сети
- 3. Браузер TOR
- 4. Беспроводные сети Wi-fi

# Выполнение первого этапа

внешнего курса.

HTTPS является протоколом прикладного уровня. (рис. 1])



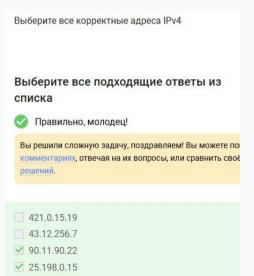
Рис. 1: Первый вопрос

#### Протокол ТСР работает на транспортном уровне. (рис. 2)

✓ Так то		риант из с	писка
<ul><li>Трацап</li></ul>			
Прикла Каналь Сетево	ном		
Следук	ощий шаг	Решить с	нова

Рис. 2: Второй вопрос

Адреса формата IPv4 состоят из 4-х значений от 0 до 255. (рис. 3)



DNS сервера необходимы для сопоставления IP адреса с доменным именем при маршрутизации запроса. (рис. 4)

## DNS cepsep Выберите один вариант из списка Верно. Так держать! сопоставляет IP адреса доменным именам сегментирует данные на транспортном уровне выбирает маршрут пакета в сети выполняет адресацию на хосте

Корректная последовательность протоколов в модели TCP/IP. (рис. 5)

Выберите корректную последовательность протокол	пов в модели ТСР/ІР
Выберите один вариант из списка	Верно решил <b>941</b> учаш Из всех попыток <b>53</b> % в
сетевой – прикладной – канальный – транспортні прикладной – транспортный – канальный – сетев	
<ul> <li>транспортный – сетевой – прикладной – канальні</li> <li>прикладной – транспортный – сетевой – канальні</li> <li>Следующий шаг</li> </ul> Решить снова	

Рис. 5: Пятый вопрос

Так как http это незащищенный протокол, он предполагает передачу данных в открытом виде.(рис. 6)

Протокол http предпола	пает	
Выберите один вар	риант из списка	Верно решили <b>965</b> у Из всех попыток <b>78</b>
	анных данных между клиен жду клиентом и сервером в Решить снова	

Рис. 6: Шестой вопрос

HTTPS протокол состоит из двух фаз: рукопожатия и передачи данных.(рис. 7)

Протокол https состоит из	
Выберите один вариант из списка	Верно решили <b>948</b> учащи Из всех попыток <b>41</b> % вер
Правильно.	
<ul> <li>одной фазы аутентификации сервера</li> <li>двух фаз: рукопожатия и передачи данных</li> <li>двух фаз: аутентификация клиента и сервера и ш</li> <li>трех фаз: аутентификации клиента, аутентификацобщего ключа</li> </ul>	
Следующий шаг	

Рис. 7: Седьмой вопрос

Версия протокола TLS определяется как клиентом, так и сервером на стадии "переговоров".(рис. 8)

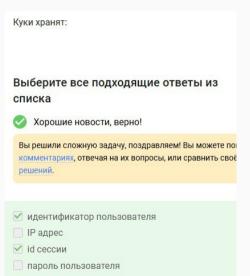
Версия протокола TLS (	определяется	
Выберите один ва	риант из списка	Верно решили Из всех попыт
Правильно, молод	ец!	
сервером клиентом и клиентом, и серве	ром в процессе "переговој та	ров"
Следующий шаг	Решить снова	

На фазе рукопожатия протокола TLS не предусмотрено шифрование данных.(рис. 9)

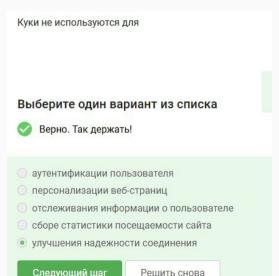
В фазе "рукопожатия" протокола TLS не предусмотре	но
Выберите один вариант из списка	Верно решил <b>931</b> учащи Из всех попыток <b>44</b> % вє
🐼 Всё правильно.	
формирование общего секретного ключа между к аутентификация (как минимум одной из сторон) выбираются алгоритмы шифрования/аутентифик в шифрование данных	
Следующий шаг	

Рис. 9: Девятый вопрос

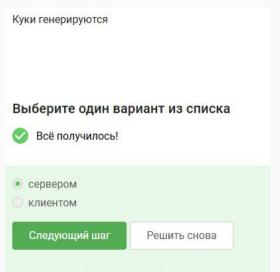
Куки-файлы хранят в себе информацию о идентификаторе пользователя и id сессии.(рис. 10)



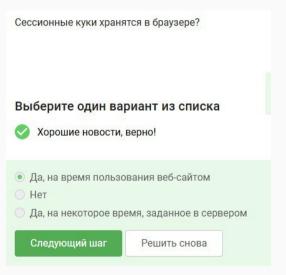
Куки-файлы не используются для улучшения надежности соединения. (рис. 11)



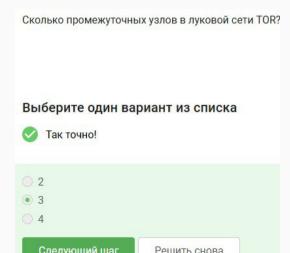
Куки-файлы генерируются сервером. (рис. 12)



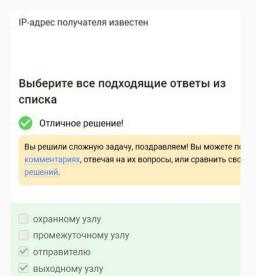
Сессионные куки хранятся в браузере на время пользования им. (рис. [13)



В браузере на основе TOR три промежуточных узла: охранный, промежуточный, выходной. (рис. 14)



IP-адрес получателя в системе TOR изместен только отправителю и выходному узлу. (рис. 15)



При запросе через TOR отправитель гененирует общий секрутный ключ со всеми узлами. (рис. 16)

Отправитель генерирует общий секретный ключ Выберите один вариант из списка Верно. отолько с охранным узлом с охранным и промежуточным узлом с охранным, промежуточным и выходном узлом с промежуточным и выходным узлом

Получатель может использовать любой браузер для принятия запроса из TOR. (рис. 17)

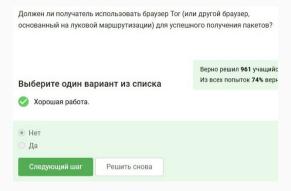


Рис. 17: Четвертый вопрос

Wf-fi - это ... (рис. 18)

WI-Fi - это	
Выберите один вариант из списка	Верно решили <b>965</b> учащихс Из всех попыток <b>79</b> % верны
Здорово, всё верно.	
<ul> <li>сокращение от "wireless fiber"</li> <li>технология беспроводной локальной сети, ра стандартом IEEE 802.11</li> <li>метод соединения компьютеров по проводно метод подключения смартфона с глобальной</li> </ul>	ой сети Ethernet
Следующий шаг	

Рис. 18: Первый вопрос

Протоколы Wf-fi работают на канальном уровне. (рис. 19)

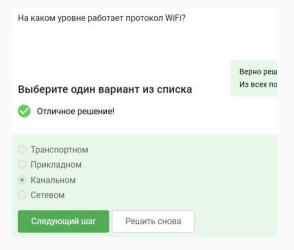


Рис. 19: Второй вопрос

Самой небезопасный метод шифрования и аунтификации Wf-fi это WEP, так как он старый и в нем используется малое кольчество бит для шифрования. (рис. 20)

Небезопасный метод обеспечения	шифрования и аутентификации в сети Wi-Fi
Выберите один вариант из	Верно решили <b>973</b> учащихс Из всех попыток <b>60%</b> вернь
WPA WEP WPA2 WPA3	
Следующий шаг Решить	снова

Рис. 20: Третий вопрос

Данные шифруются после аунтификации польователя. (рис. 21)

Данные между хостом	сети (компьютером или сма	артфоном) и роутером
Выберите один ва	риант из списка	Верно решили <b>975</b> учац Из всех попыток <b>53%</b> в
передаются в откры передаются в зашиф передаются в откры	том виде	
Следующий шаг	Решить снова	

Рис. 21: Четвертый вопрос

Для домашних сетей используется аунтификатор Wi-fi Personal. (рис. 22)

Для домашней сети для	я аутентификации обычно ис	пользуется метод
Выберите один вар		Верно решили <b>975</b> у Из всех попыток <b>87</b> °
WPA2 Personal     WPA2 Enterprise		
Следующий шаг	Решить снова	

Рис. 22: Пятый вопрос



#### Вывод

Выполнен первый этап внешнего курса