# Отчёт по Внешнему Курсу - Этап 1

Основы информационной безопасности

Чистов Д. М.

17 мая 2025

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

Цель работы

# Цель работы

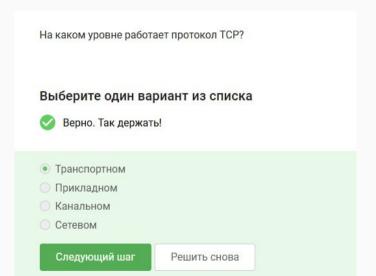
Пройти внешний курс - Этап 1

В лекционных материалах было сказано, что в протоколы прикладного уровня включён HTTPS.

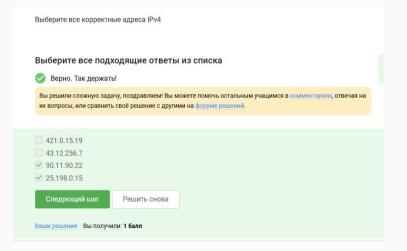
	710	всех попыток 58% верных

**Рис. 1:** Задание 1

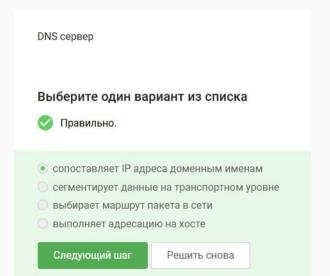
TCP работает на транспортном уровне, IP - на сетевом.



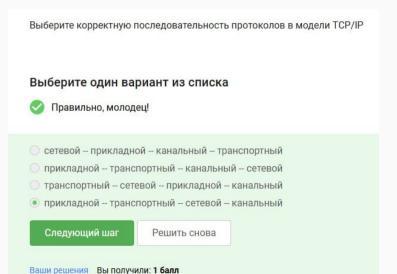
Т.к. IPv4 - набор цифр от 0 до 255, следовательно исключаем варианты, которые содержат числа больше/меньше этого набора.



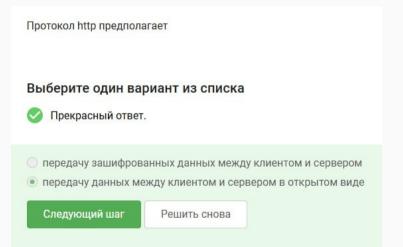
DNS сопоставляет доменное имя соответствующий ему IP.



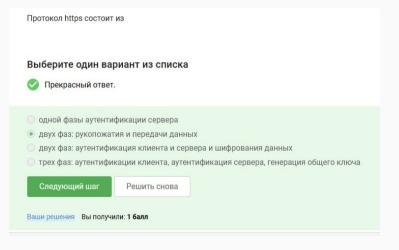
Порядок такой.



http - предоставляет в открытом виде, именно эту проблему решает https, он работает также, только в этот раз данные шифруются.

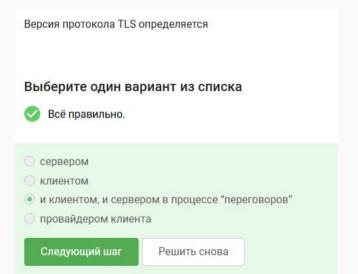


Рукопожатие и передача данных, аутентификации не входит.

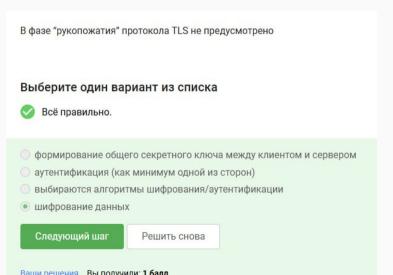


9/26

Обязательно версия протокола определяется обоими.



Шифрование данных не происходит в фазе рукопожатия, только после неё.



Куки не хранят пароль пользователя или его ІР адрес.

Куки хранят:	
Выберите все подходящие ответы из списка	Верно решили <b>856</b> учащихся Из всех попыток <b>18%</b> верных
Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить свое решение с другими на форуме решений.	
□ IP адрес  ✓ идентификатор пользователя □ пароль пользователя ✓ Id сессии  Следующий шаг Решить снова	
Ваши решения Выполучин: 1 баля	

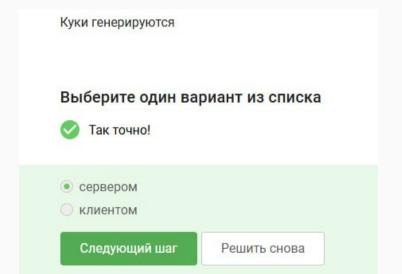
Рис. 10: Задание 010

Куки не сильно влияют на безопасность, скорее упрощают работу пользователям.

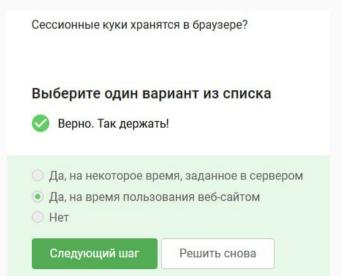
Куки не используются для	
Выберите один вариант из списка  Правильно.	Верно решили <b>950</b> учащихся Из всех попыток <b>53%</b> верных
аутентификации пользователя персонализации веб-страниц отслеживания информации о пользователе сборе статистики посещаемости сайта улучшения надежности соединения Спедующий шаг Решить снова Ваши решения Вы получили: 1 балл	

Рис. 11: Задание 011

Куки генерируются сервером и отправляются клиенту, а не наоборот.



Сессионные куки исчезнут, как только мы закроем окно с веб-сайтом.



3, т.к. больше узлов анонимности не прибавляют, а при меньших узлах теряется смысл всего алгоритма маршрутизации TOR.



Рис. 14: Задание 014

При шифровании так получается, что охранный узел и промежуточный узел не знают по итогу IP адрес получателя данных.

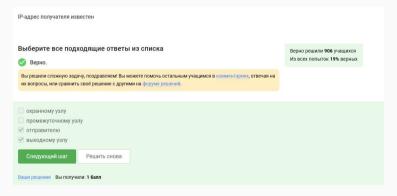


Рис. 15: Задание 015

Отправитель генерирует общий секретный ключ со всеми тремя узлами.

Отправитель генерирует общий секретный ключ	
Выберите один вариант из списка Всё получилосы!	Верно решили <b>959</b> учащихся Из всех попыток <b>55</b> % верных
только с охранным узлом     с охранным и промежуточным узлом     с охранным, промежуточным и выходном узлом     с промежуточным и выходным узлом     Спедующий шаг     Решить снова  Ввши решения Вы получили: 1 балл	

Рис. 16: Задание 016

Нет, не должен, далее возвращение данных происходит как обычно.

Должен ли получатель использовать браузер Тог (или другой браузер, основанный на луковой маршрути получения пакетов?	зации) для успешного
Выберите один вариант из списка  У хорошая работа.	Верно решил <b>961</b> учащийся Из всех попыток <b>74%</b> верных
○ Да • Нет	
Следующий шаг	
Ваши решения Вы получили: 1 балл	

Рис. 17: Задание 017

У Wi-fi нет расшифроки, вообще это была такая пометка от компании, которая проверяла поддерживает ли устройство беспроводную сеть, а так это технология беспроводной сети.



Рис. 18: Задание 018

На канальном уровне, т.к. речь всё-таки идёт о физическом излучении и приёме сигнала.

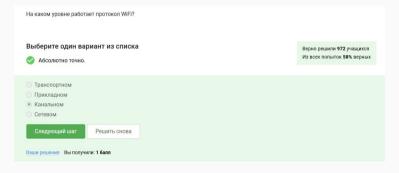


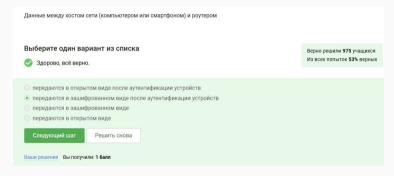
Рис. 19: Задание 019

WEP самый первый, но и к сожалению, небезопасный, на данный момент самый безопасный - WPA3.

Небезопасный метод обеспечения шифрования и аутентификации в сети WI-Fi	
Выберите один вариант из списка  Так точно!	Верно решили <b>973</b> учащихся Из всех попыток <b>60%</b> верных
● WPA ● WEP ● WPA2 ● WPA3	
Спедующий шаг Решить снова  Ваши решения Вы получили: 1 балл	

Рис. 20: Задание 020

На новых версиях беспроводных сетей происходит шифрование, но перед этим обязательно аутентификация.



**Рис. 21:** Задание 021

Для домашней сети - personal, для Корпоративных сетей используют Enterprise, т.к. есть база данных её пользователей. Это усиливает безопасность корпорации..

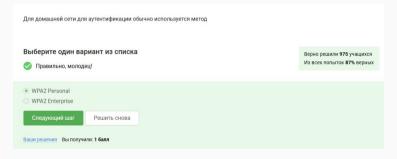


Рис. 22: Задание 022

Выводы



Этап 1 пройден успешно на максимальный балл.

Список литературы

#### Список литературы

Курс "Основы Кибербезопасности" на платформе Stepik