

Курс по основам кибербезопасности

Этап 1

Ведьмина Александра Сергеевна

Российский университет дружбы народов, Москва, Россия

Информация

- Ведьмина Александра Сергеевна
- студентка
- Российский университет дружбы народов
- 1132236003@rudn.ru
- <https://asvedjmina.github.io/ru/>



Цель работы

Выполнить задания первой части курса по кибербезопасности.

Выполнение лабораторной работы

UPD, TCP, IP - протоколы других уровней.

Выберите протокол прикладного уровня

Выберите один вариант из списка



Хорошая работа.

- ☐ UDP
- ☐ TCP
- ☒ HTTPS
- ☐ IP

Следующий шаг

Решить снова

TCP вне всяких сомнений transmission - транспортный уровень.

На каком уровне работает протокол TCP?

Выберите один вариант из списка



Верно. Так держать!

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

Следующий шаг

Решить снова

В ip число между точками не больше 255.

Выберите все корректные адреса IPv4

Выберите все подходящие ответы из списка



Здорово, всё верно.

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](#).

☐ 421.0.15.19

☐ 43.12.256.7

☒ 90.11.90.22

☒ 25.198.0.15

DNS сервер преобразует имена в адреса.

DNS сервер

Выберите один вариант из списка



Абсолютно точно.

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

Следующий шаг

Решить снова

Протоколы действительно распределены по уровням, идущим в таком порядке.

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка



Правильно.

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

Следующий шаг

Решить снова

В http данные в открытом виде, в https - в закрытом.

Протокол http предполагает

Выберите один вариант из списка



Здорово, всё верно.

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

Следующий шаг

Решить снова

HTTPS включает две фазы - рукопожатие и передачу данных.

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

Это согласовывается клиентом и сервером.

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

Шифрования данных нет в рукопожатии.

В фазе “рукопожатия” протокола TLS не предусмотрено

Выберите один вариант из списка



Так точно!

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

Следующий шаг

Решить снова

Куки используются для персонализации контента, им не нужны пароли и ip.

Куки хранят:

Выберите все подходящие ответы из списка



Правильно, молодец!

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](#).

- ☐ пароль пользователя
- ☐ IP адрес
- ☒ id сессии
- ☒ идентификатор пользователя

Как отмечено ранее, у куки другие цели.

Куки не используются для

Выберите один вариант из списка



Всё получилось!

- ☐ аутентификации пользователя
- ☐ персонализации веб-страниц
- ☐ отслеживания информации о пользователе
- ☐ сборе статистики посещаемости сайта
- ☒ улучшения надежности соединения

Следующий шаг

Решить снова

Сервер создает куки.

Куки генерируются

Выберите один вариант из списка

☒ Хорошие новости, верно!

☒ сервером

☐ клиентом

Следующий шаг

Решить снова

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

Сессионные куки очищаются после завершения сессии.

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

☒ Отличное решение!

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

Следующий шаг

Решить снова

Всего три узла - входной, промежуточный, выходной.

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

☒ Отлично!

☐ 2

☒ 3

☐ 4

Следующий шаг

Решить снова

IP скрыт от охранного и промежуточного узла.

IP-адрес получателя известен

Выберите все подходящие ответы из списка



Прекрасный ответ.

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](#).

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

Общий ключ создается со всеми узлами.

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

☒ Хорошие новости, верно!

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

Следующий шаг

Решить снова

Это необязательно.

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

Выберите один вариант из списка

☒ Правильно.

☐ Да

☒ Нет

Следующий шаг

Решить снова

По определению:

Wi-Fi - это

Выберите один вариант из списка



Так точно!

- ☐ 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

Канальный, обеспечивает доступ в сеть.

На каком уровне работает протокол WiFi?

Выберите один вариант из списка



Правильно, молодец!

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

Следующий шаг

Решить снова

Устаревший протокол, легко взломать.

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка



Всё получилось!

- ☐ WPA
- ☒ WEP
- ☐ WPA2
- ☐ WPA3

Следующий шаг

Решить снова

Сначала аутентифицируют, потом передают данные.

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка



Здорово, всё верно.

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

Следующий шаг

Решить снова

Из названия понятно, что personal для личного пользования.

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка



Отличное решение!



WPA2 Personal



WPA2 Enterprise

Следующий шаг

Решить снова

[Ваши решения](#)

Вы получили: **1 балл**

Выводы

Все задания выполнены.