

Внешний курс. Блок 1: Безопасность в сети

Основы информационной безопасности

Петрова Алевтина Александровна

Содержание

1 Цель работы

Выполнение контрольных заданий первого блока внешнего курса “Основы Кибербезопасности”

2 Выполнение заданий блока “Основы Кибербезопасности”

2.1 Как работает интернет: базовые сетевые протоколы

UDP - протокол сетевого уровня TCP - протокол транспортного уровня HTTPS - протокол прикладного уровня IP - протокол сетевого уровня, поэтому ответ HTTPS (рис. 1).

Выберите протокол прикладного уровня

Верно решили 939 учащихся
Из всех попыток 61% верных

Выберите один вариант из списка

☐ UDP
☐ TCP
☒ HTTPS
☐ IP

1 балл за решение.

Отправить

Вопрос 2.1.1

Ранее было упомянуто, что протокол TCP - transmission control protocol - работает на транспортном уровне (рис. 2).

На каком уровне работает протокол TCP?

Верно решили 939 учащихся
Из всех попыток 61% верных

Выберите один вариант из списка

☒ Транспортном
☐ Прикладном
☐ Канальном
☐ Сетевом

1 балл за решение.

Отправить

Вопрос 2.1.2

В адресе типа IPv4 не может быть чисел больше 255, поэтому первые два варианта не подходят (рис.3).

Выберите все подходящие ответы из списка

Верно решил 871 учащийся
Из всех попыток 23% верных

✓ Все получилось!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментарии](#), 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

Следующий шаг Решить снова

Вопрос 2.1.3

DNS-сервер, Domain name server — приложение, предназначенное для ответов на DNS-запросы по соответствующему протоколу Обязательное условие – Сопоставление сервером доменных имен доменного имени с IP-адресом называется разрешением имени и адреса (рис.4]).

DNS сервер

Верно решили 933 учащихся
Из всех попыток 66% верных

Выберите один вариант из списка

✓ Отличное решение!

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: < >

Вопрос 2.1.4

Распределение протоколов в модели TCP/IP:

- Прикладной уровень (Application Layer): HTTP, RTSP, FTP, DNS.
- Транспортный уровень (Transport Layer): TCP, UDP, SCTP, DCCP.
- Сетевой (Межсетевой) уровень (Network Layer): IP.
- Уровень сетевого доступа (Канальный) (Link Layer): Ethernet, IEEE 802.11, WLAN, SLIP, Token Ring, ATM и MPLS. (рис.5).

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

☐ сетевой – прикладной – канальный – транспортный

☐ прикладной – транспортный – канальный – сетевой

☐ транспортный – сетевой – прикладной – канальный

☒ прикладной – транспортный – сетевой – канальный

1 балл за решение

Отправить

Верно решил
Из всех попыток

Вопрос 2.1.5

Протокол http передает не зашифрованные данные, а протокол https уже будет передавать зашифрованные данные (рис.6).

Протокол http предполагает

Выберите один вариант из списка

✓ Всё правильно.

Верно решили 965 учащихся
Из всех попыток 78% верных

☐ передачу зашифрованных данных между клиентом и сервером

☒ передачу данных между клиентом и сервером в открытом виде

Следующий шаг

Решить снова

Вопрос 2.1.6

https передает зашифрованные данные, одна из фаз - передача данных, другая должна быть рукопожатием (рис.7).

Протокол https состоит из

Выберите один вариант из списка

✓ Отличное решение!

Верно решили 948 учащихся
Из всех попыток 41% верных

☐ одной фазы аутентификации сервера

☒ двух фаз: рукопожатия и передачи данных

☐ двух фаз: аутентификация клиента и сервера и шифрования данных

☐ трех фаз: аутентификация клиента, аутентификация сервера, генерация общего ключа

Следующий шаг

Решить снова

Вопрос 2.1.7

TLS определяется и клиентом, и сервером, чтобы было возможно подключиться (рис.8).

Версия протокола TLS определяется

Выберите один вариант из списка

✓ Всё правильно.

Верно решено
Из всех попыток

- ☐ сервером
- ☐ клиентом
- ☒ и клиентом, и сервером в процессе "переговоров"
- ☐ провайдером клиента

Следующий шаг Решить снова

Вопрос 2.1.8

Ответ на изображении, остальные варианты в протоколе предусмотрены (рис.9).

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

✓ Верно. Так держат!

Верно решено
Из всех попыток

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

Следующий шаг Решить снова

Вопрос 2.1.9

2.2 Персонализация сети

Куки точно не хранят пароли и IP-адреса, а id сессии и идентификатор хранят (рис.10).

2.2 Персонализация сети 3 из 6 шагов пройдено 1 из 4 баллов получен

Куки хранят:

Выберите все подходящие ответы из списка

✓ Хорошая работа.

Верно решено
Из всех попыток

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

Следующий шаг Решить снова

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

Вопрос 2.2.1

Конечно же, куки не делают соединение более надежным (рис.11).

2.2 Персонализация сети 4 из 6 шагов пройдено 2 из 4 баллов получено

Куки не используются для

Выберите один вариант из списка

☒ Правильно, молодец!

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Вопрос 2.2.2

Ответ на изображении (рис.12).

2.2 Персонализация сети 5 из 6 шагов пройдено 3 из 4 баллов получено

Куки генерируются

Выберите один вариант из списка

☒ Абсолютно точно.

Верно решили 94 Из всех попыток

- ☐ клиентом
- ☒ сервером

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: ...

Вопрос 2.2.3

Сессионные куки хранятся в течение сессии, то есть пока используется веб-сайт (рис.13).

2.2 Персонализация сети 6 из 6 шагов пройдено 4 из 4 баллов получено

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

☒ Здорово, всё верно.

Верно решили 94 Из всех попыток

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

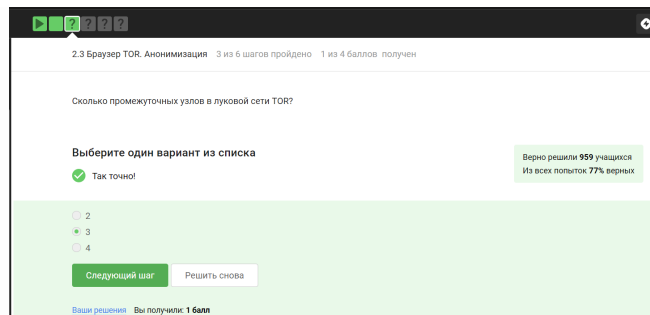
Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Вопрос 2.2.4

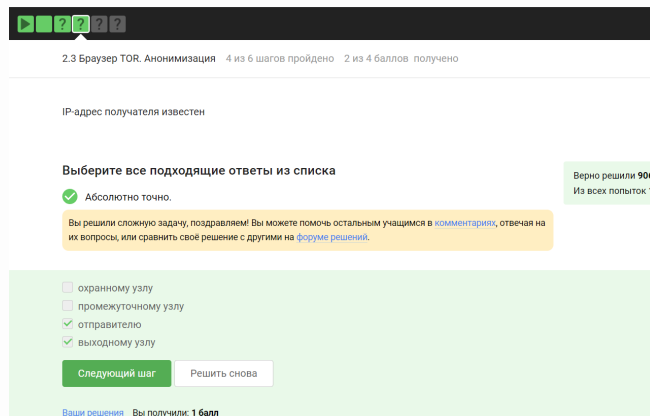
2.3 Браузер TOR. Анонимизация

Необходимо три узла - входной, промежуточный и выходной (рис.14).



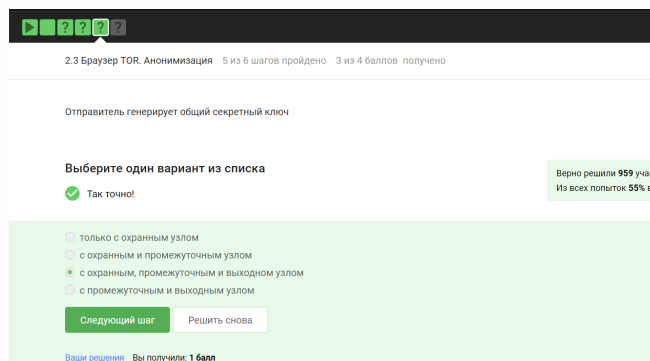
Вопрос 2.3.1

IP-адрес не должен быть известен охранному и промежуточному узлам (рис.15).



Вопрос 2.3.2

Отправитель генерирует общий секретный ключ со узлами, через которые идет передача, то есть со всеми (рис.16).



Вопрос 2.3.3

Для получения пакетов не нужно использовать TOR. TOR — это технология, которая позволяет с некоторым успехом скрыть личность человека в интернете (рис. 17).

2.3 Браузер TOR. Анонимизация 6 из 6 шагов пройдено 4 из 4 баллов получено

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

Выберите один вариант из списка

☒ Всё правильно.

Верно решил 961 участник
Из всех попыток 74% верны

☐ Нет

☐ Да

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Вопрос 2.3.4

2.4 Беспроводные сети Wi-fi

Действительно, это определение Wi-Fi (рис.18).

2.4 Беспроводные сети Wi-Fi 4 из 8 шагов пройдено 1 из 5 баллов получен

Wi-Fi - это

Выберите один вариант из списка

☒ Хорошие новости, верно!

Верно решили 965 учащихся
Из всех попыток 79% верны

☐ 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

Ваши решения Вы получили: 1 балл

Вопрос 2.4.1

Для целей работы в Интернете Wi-Fi обычно располагается как канальный уровень (эквивалентный физическому и канальному уровням модели OSI) ниже интернет-уровня интернет-протокола. Это означает, что узлы имеют связанный интернет-адрес, и при подходящем подключении это обеспечивает полный доступ в Интернет. (рис.19).

2.4 Беспроводные сети Wi-Fi 5 из 8 шагов пройдено 2 из 5 баллов получено

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

☒ Верно.

Верно решили 972 учащихся
Из всех попыток 58% верных

☐ Транспортном

☐ Прикладном

☒ Канальном

☐ Сетевом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Вопрос 2.4.2

WEP (Wired Equivalent Privacy) – устаревший и небезопасный метод проверки подлинности. Это первый и не очень удачный метод защиты. Злоумышленники без проблем получают доступ к беспроводным сетям, которые защищены с помощью WEP, был заменен остальными представленными (рис. 20).

2.4 Беспроводные сети Wi-Fi 6 из 8 шагов пройдено 3 из 5 баллов получено

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 973 учащихся
Из всех попыток 60% верных

☐ WPA
☒ WEP
☐ WPA2
☐ WPA3

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Вопрос 2.4.3

Нужно аутентифицировать устройства и позже передаются зашифрованные данные (рис. 21).

2.4 Беспроводные сети Wi-Fi 7 из 8 шагов пройдено 4 из 5 баллов получено

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

✓ Отлично!

Верно решили 975 учащихся
Из всех попыток 53% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Вопрос 2.4.4

В целом, понятно по названию, что WPA2 Personal для личного использования, то есть для домашней сети, enterprise - для предприятий (рис.22).

2.4 Беспроводные сети Wi-Fi 8 из 8 шагов пройдено 5 из 5 баллов получено

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

✓ Всё правильно.

Верно решили 975 учащихся
Из всех попыток 53% верных

☒ WPA2 Personal
☐ WPA2 Enterprise

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Вопрос 2.4.5

3 Выводы

В ходе выполнения блока “Безопасность в сети” узнала о работе базовых сетевых протоколов, куки сетей Wi-Fi и браузера TOR.