

Внешний курс. Блок 1: Безопасность в сети

Дисциплина: Основы информационной безопасности

Неустроева Ирина Николаевна

Содержание

1	Цель работы	5
2	Выполнение заданий блока “Основы Кибербезопасности”	6
2.1	Как работает интернет: базовые сетевые протоколы	6
2.2	Персонализация сети	10
2.3	Браузер TOR. Анонимизация	12
2.4	Беспроводные сети Wi-fi	14
3	Выводы	18

Список иллюстраций

2.1	Вопрос 2.1.1	6
2.2	Вопрос 2.1.2	7
2.3	Вопрос 2.1.3	7
2.4	Вопрос 2.1.4	8
2.5	Вопрос 2.1.5	8
2.6	Вопрос 2.1.6	9
2.7	Вопрос 2.1.7	9
2.8	Вопрос 2.1.8	10
2.9	Вопрос 2.1.9	10
2.10	Вопрос 2.2.1	11
2.11	Вопрос 2.2.2	11
2.12	Вопрос 2.2.3	12
2.13	Вопрос 2.2.4	12
2.14	Вопрос 2.3.1	13
2.15	Вопрос 2.3.2	13
2.16	Вопрос 2.3.3	14
2.17	Вопрос 2.3.4	14
2.18	Вопрос 2.4.1	15
2.19	Вопрос 2.4.2	15
2.20	Вопрос 2.4.3	16
2.21	Вопрос 2.4.4	16
2.22	Вопрос 2.4.5	17

Список таблиц

1 Цель работы

Выполнить контрольные задания первого блока “Безопасность в сети” внешнего курса “Основы кибербезопасности”.

2 Выполнение заданий блока “Основы Кибербезопасности”

2.1 Как работает интернет: базовые сетевые протоколы

Протокол HTTP(S) протокол прикладного уровня, ответ на вопрос 1 - HTTPS (рис. 2.1).

Выберите один вариант из списка

✓ Абсолютно точно.

Верно решили 895 учащихся
Из всех попыток 58% верных

☐ UDP
☐ TCP
☒ HTTPS
☐ IP

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

98 13 Шаг 7 Следующий шаг >

Рис. 2.1: Вопрос 2.1.1

На транспортном уровне существует два примера протокола: первый - это TCP, в честь которого названа модель. (рис. 2.2).

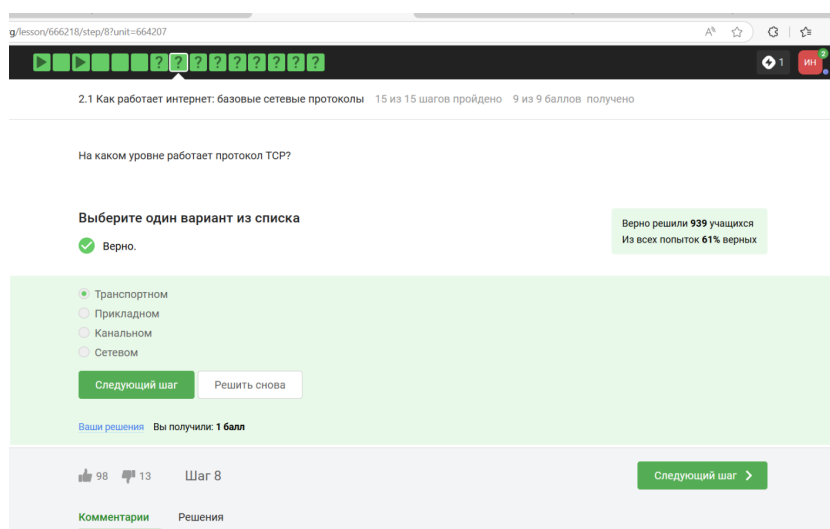


Рис. 2.2: Вопрос 2.1.2

Т.к адрес состоит из большого набора чисел, а именно это 4 или 6 цифр от 0 до 255. В двух вариантах встречаются цифры больше 255, что неверно(рис. 2.3).

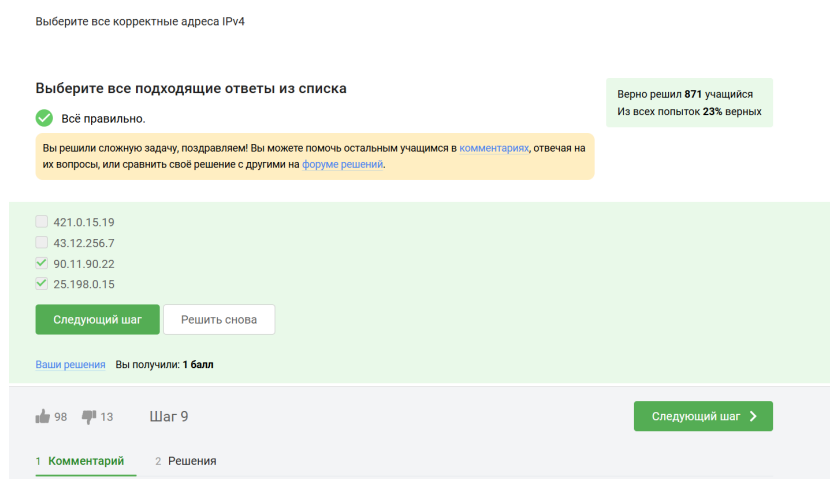


Рис. 2.3: Вопрос 2.1.3

Основная задача DNS это сопоставлять название (доменное имя, с корректным IP-адресом) с тем, где лежит этот сервер, этот сайт. (рис. 2.4).

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решили 933 учащихся
Из всех попыток 66% верных

☒ 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: 1 балл

👍 98 🗣️ 13 Шаг 10 Следующий шаг >

Рис. 2.4: Вопрос 2.1.4

Классификация протоколов в модели TCP/IP:

- Прикладной уровень: HTTP, RTSP, FTP, DNS.
- Транспортный уровень: TCP, UDP, SCTP, DCCP.
- Сетевой уровень: IP.
- Уровень сетевого доступа (Канальный) (Link Layer): Ethernet, IEEE 802.11, WLAN, SLIP, Token Ring, ATM и MPLS(рис. 2.5).

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решил 941 учащийся
Из всех попыток 53% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.5: Вопрос 2.1.5

Протокол http передает не зашифрованные данные, а протокол https уже будет передавать зашифрованные данные (рис. 2.6).

https передает зашифрованные данные, поэтому одна из фаз это передача данных, другая должна быть рукопожатием

Протокол http предполагает

Выберите один вариант из списка

✓ Так точно!

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

Ваши решения Вы получили: 1 балл

👍 98 🗳 13 Шаг 12 Следующий шаг >

Рис. 2.6: Вопрос 2.1.6

TLS определяется и клиентом, и сервером, чтобы было возможно подключиться (рис. 2.7).

Протокол https состоит из

Выберите один вариант из списка

✓ Хорошая работа.

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

Ваши решения Вы получили: 1 балл

👍 98 🗳 13 Шаг 13 Следующий шаг >

Рис. 2.7: Вопрос 2.1.7

TLS определяется клиентом и сервером, чтобы возможно было подключиться (рис. 2.8).

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

✓ Верно. Так держаты!

Верно решил 931 учащийся
Из всех попыток 44% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

👍 98 👎 13 Шаг 15 Следующий шаг >

Рис. 2.8: Вопрос 2.1.8

Фаза рукопожатия включает в себя:

- выбор параметров, протоколов
- аутентификация (как минимум, сервера)
- формируется общий секретный ключ K

Следовательно вариант с шифрованием лишний (рис. 2.9).

Куки хранят:

Выберите все подходящие ответы из списка

✓ Прекрасный ответ.

Верно решили 856 учащихся
Из всех попыток 16% верных

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](#).

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.9: Вопрос 2.1.9

2.2 Персонализация сети

Куки хранят в себе список параметров и их значений. Этими параметрами могут быть id пользователя, id сессии, тип браузера и некоторые действия поль-

зователей(рис. 2.10).

Куки хранят:

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](#).

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 2.10: Вопрос 2.2.1

Куки не делают соединение надежным (рис. 2.11).

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**

[Шаг 4](#) [Следующий шаг >](#)

Рис. 2.11: Вопрос 2.2.2

Куки генерируются сервером(рис. 2.12).

Куки генерируются

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 968 учащихся
Из всех попыток 79% верных

☐ клиентом
☒ сервером

Следующий шаг
 Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.12: Вопрос 2.2.3

Куки бывают сессионные, удаляются при закрытии окна браузера (рис. 2.13).

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

✓ Абсолютно точно.

Верно решили 959 учащихся
Из всех попыток 60% верных

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

Следующий шаг
 Решить снова

Ваши решения Вы получили: 1 балл

👍 40 👎 13 Шаг 6
 Следующий шаг >

Рис. 2.13: Вопрос 2.2.4

2.3 Браузер TOR. Анонимизация

В луковой модели маршрутизации у нас тоже есть узлы. Они разделяются на охранный узел, промежуточный и выходной. В браузере Tor всегда есть три роутера, их не больше и не меньше (рис. 2.14).

Выберите один вариант из списка

✓ Отличное решение!

Верно решили 959 учащихся
Из всех попыток 77% верных

☐ 2
☒ 3
☐ 4

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

👍 48 👎 4 Шаг 3 Следующий шаг >

Рис. 2.14: Вопрос 2.3.1

IP-адрес не должен быть известен охранному и промежуточному узлам (рис. 2.15).

IP-адрес получателя известен

Выберите все подходящие ответы из списка

✓ Правильно.

Верно решили 906 учащихся
Из всех попыток 19% верных

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

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.15: Вопрос 2.3.2

В анонимных сетях, таких как Tor, общий секретный ключ для сквозного шифрования требует участия всех трех типов узлов: охранного, промежуточного и выходного. Охранный узел сам по себе не обеспечивает генерацию ключа. Каждый узел вносит свой вклад в криптографический протокол (например, Diffie-Hellman), обеспечивая анонимность и защиту от перехвата. (рис. 2.16).

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

✓ Отлично!

Верно решили 959 учащихся
Из всех попыток 55% верных

☐ только с охраным узлом
☐ с охраным и промежуточным узлом
☒ с охраным, промежуточным и выходным узлом
☐ с промежуточным и выходным узлом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

👍 48 🗳️ 4 Шаг 5 Следующий шаг >

Рис. 2.16: 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. 2.17).

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

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решил 961 учащийся
Из всех попыток 74% верных

☒ Нет
☐ Да

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

👍 48 🗳️ 4 Шаг 6 Следующий шаг >

Рис. 2.17: Вопрос 2.3.4

2.4 Беспроводные сети Wi-fi

WiFi - это технология беспроводной локальной сети, она основана на стандарте IEEE 802.11 (рис. 2.18).

Wi-Fi - это

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 965 учащихся
Из всех попыток 79% верных

- ☐ 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

41 4 Шаг 4 Следующий шаг >

1 Комментарий Решения

Рис. 2.18: Вопрос 2.4.1

WiFi работает на самом нижнем канальном уровне (рис. 2.19).

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 972 учащихся
Из всех попыток 58% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

41 4 Шаг 5 Следующий шаг >

Рис. 2.19: Вопрос 2.4.2

WEP - устаревший и небезопасный метод шифрования WiFi из-за короткой длины ключа (40 бит), что делает его легко взламываемым. Использовать WEP категорически не рекомендуется.(рис. 2.20).

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

41 4 Шаг 6 Следующий шаг >

Рис. 2.20: Вопрос 2.4.3

Безопасность WiFi подразумевает защиту передачи данных между устройством (телефон, компьютер) и роутером (подключенным к интернету), осуществляемую с помощью шифрования и аутентификации.(рис. 2.21).

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

41 4 Шаг 7 Следующий шаг >

Комментарии Решения

Рис. 2.21: Вопрос 2.4.4

WPA2 Personal предназначен для домашнего использования, а WPA2 Enterprise - для коммерческих организаций. (рис. 2.22).

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

Верно.

Верно решили 975 учащихся
Из всех попыток 87% верных

☒ WPA2 Personal
☐ WPA2 Enterprise

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

41 4 Шаг 8

Следующий шаг >

Комментарии Решения

Рис. 2.22: Вопрос 2.4.5

3 Выводы

В результате выполнения блока “Безопасность в сети” я узнала, как работают сетевые пратаколы, куки-файлы, сети вайфай и для чего нужен браузер Tor.