

Внешний курс. Блок 1: Безопасность в сети

Воинов Кирилл Викторович

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	17

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	11
2.13	Вопрос 2.2.4	12
2.14	Вопрос 2.3.1	12
2.15	Вопрос 2.3.2	13
2.16	Вопрос 2.3.3	13
2.17	Вопрос 2.3.4	14
2.18	Вопрос 2.4.1	14
2.19	Вопрос 2.4.2	15
2.20	Вопрос 2.4.3	15
2.21	Вопрос 2.4.4	16
2.22	Вопрос 2.4.5	16

Список таблиц

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. 2.1).

2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено 9 из 9 баллов получено

Выберите протокол прикладного уровня

Выберите один вариант из списка

☒ Верно.

Верно решили 895 учащихся
Из всех попыток 58% верных

☐ UDP
☐ TCP
☒ HTTPS
☐ IP

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

103 13 Шаг 7 Следующий шаг >

Рис. 2.1: Вопрос 2.1.1

Ранее было упомянуто, что протокол TCP - transmission control protocol - работает на транспортном уровне (рис. 2.2).

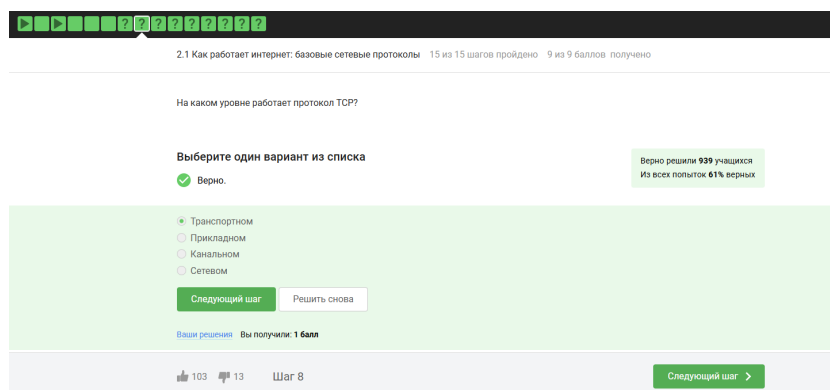


Рис. 2.2: Вопрос 2.1.2

В адресе типа IPv4 не может быть чисел больше 255, поэтому первые два варианта не подходят (рис. 2.3).

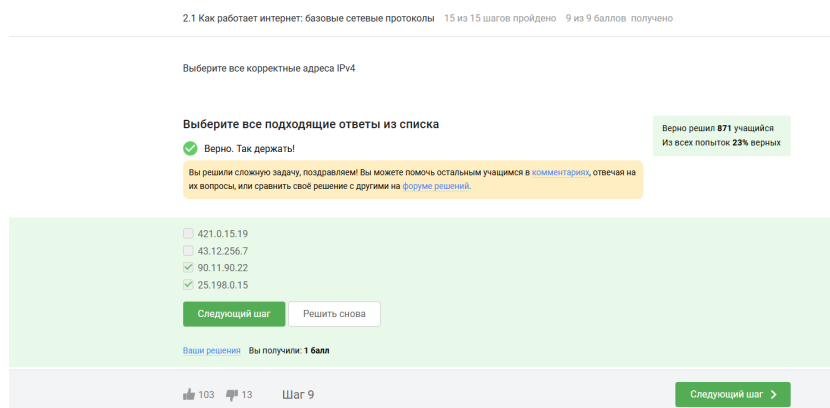


Рис. 2.3: Вопрос 2.1.3

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. 2.4).

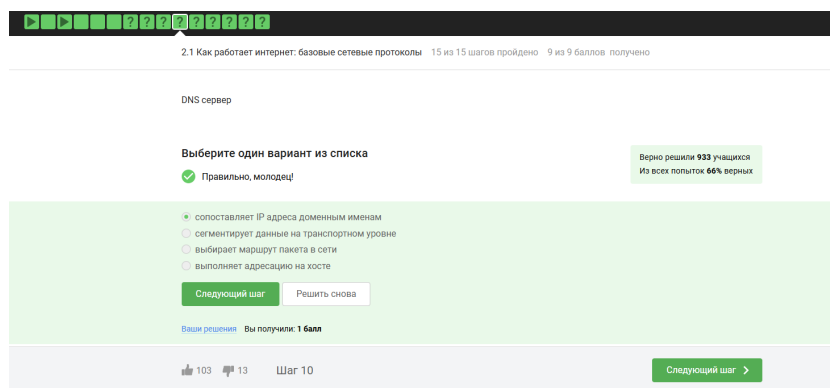


Рис. 2.4: Вопрос 2.1.4

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. 2.5).

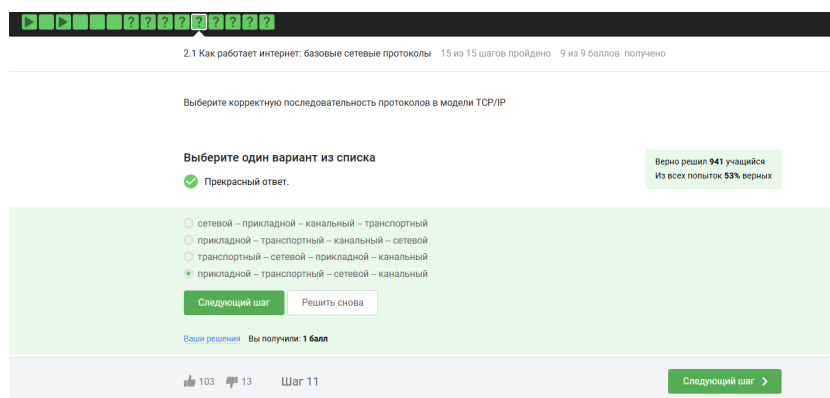


Рис. 2.5: Вопрос 2.1.5

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

2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено 9 из 9 баллов получено

Протокол http предполагает

Выберите один вариант из списка

✓ Прекрасный ответ.

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

103 13 Шаг 12 Следующий шаг >

Рис. 2.6: Вопрос 2.1.6

https передает зашифрованные данные, одна из фаз - передача данных, другая должна быть рукопожатием (рис. 2.7).

2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено 9 из 9 баллов получено

Протокол https состоит из

Выберите один вариант из списка

✓ Всё правильно.

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: аутентификации клиента, аутентификация сервера, генерация общего ключа

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

103 13 Шаг 13 Следующий шаг >

Рис. 2.7: Вопрос 2.1.7

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

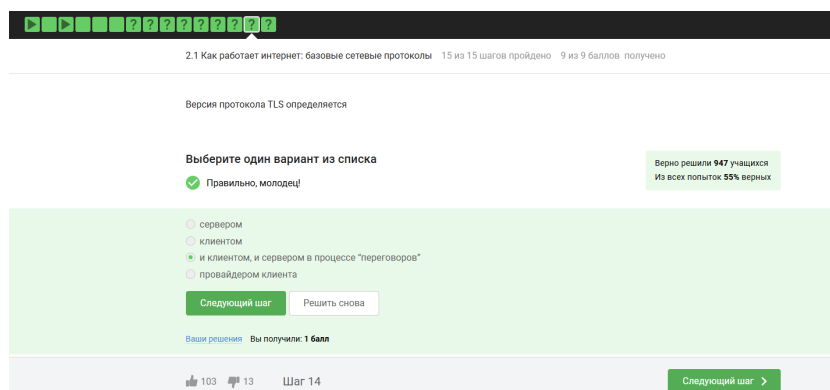


Рис. 2.8: Вопрос 2.1.8

Ответ на изображении, остальные варианты в протоколе предусмотрены (рис. 2.9).

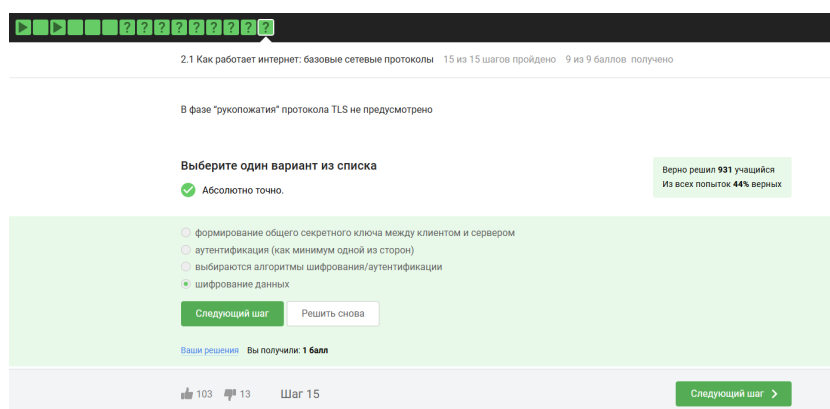


Рис. 2.9: Вопрос 2.1.9

2.2 Персонализация сети

Куки точно не хранят пароли и IP-адреса, а id сессии и идентификатор хранят (рис. 2.10).

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

Куки хранят:

Выберите все подходящие ответы из списка

✓ Хорошие новости, 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](#).

Верно решили 856 учащихся
Из всех попыток 18% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

40 13 Шаг 3 Следующий шаг >

Рис. 2.10: Вопрос 2.2.1

Конечно же, куки не делают соединение более надежным (рис. 2.11).

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

Куки не используются для

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 950 учащихся
Из всех попыток 53% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

40 13 Шаг 4 Следующий шаг >

Рис. 2.11: Вопрос 2.2.2

Ответ на изображении (рис. 2.12).

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

Куки генерируются

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили 968 учащихся
Из всех попыток 79% верных

☒ сервером
☐ клиентом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

40 13 Шаг 5 Следующий шаг >

Рис. 2.12: Вопрос 2.2.3

Сессионные куки хранятся в течение сессии, то есть пока используется веб-сайт (рис. 2.13).

The screenshot shows a quiz interface for '2.2 Персонализация сети'. The question is 'Сессионные куки хранятся в браузере?'. The correct answer is 'Да, на время пользования веб-сайтом'. The interface includes a progress bar at the top, a list of options with radio buttons, and buttons for 'Следующий шаг' and 'Решить снова'. A green box on the right indicates that 959 students answered correctly with a 60% success rate. The bottom of the screen shows a score of 40/13 and a 'Шаг 6' indicator.

Рис. 2.13: Вопрос 2.2.4

2.3 Браузер TOR. Анонимизация

Необходимо три узла - входной, промежуточный и выходной (рис. 2.14).

The screenshot shows a quiz interface for '2.3 Браузер TOR. Анонимизация'. The question is 'Сколько промежуточных узлов в луковой сети TOR?'. The correct answer is '3'. The interface includes a progress bar at the top, a list of options with radio buttons, and buttons for 'Следующий шаг' and 'Решить снова'. A green box on the right indicates that 959 students answered correctly with a 77% success rate. The bottom of the screen shows a score of 49/4 and a 'Шаг 3' indicator.

Рис. 2.14: Вопрос 2.3.1

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

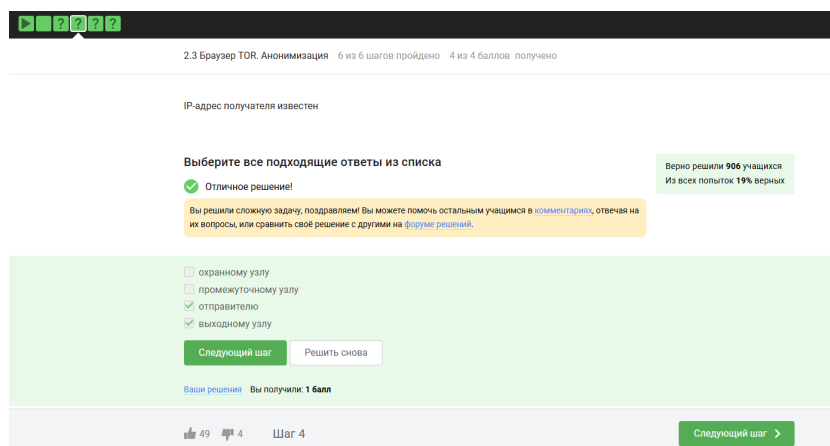


Рис. 2.15: Вопрос 2.3.2

Отправитель генерирует общий секретный ключ со узлами, через которые идет передача, то есть со всеми (рис. 2.16).

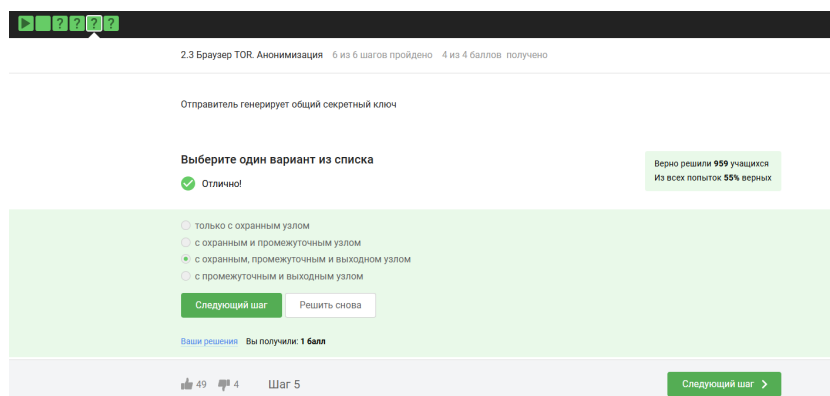


Рис. 2.16: Вопрос 2.3.3

Для получения пакетов не нужно использовать TOR. TOR — это технология, которая позволяет с некоторым успехом скрыть личность человека в интернете (рис. 2.17).

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

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

Выберите один вариант из списка

☒ Так точно!

Верно решили 961 учащихся
Из всех попыток 74% верных

☐ Да

☐ Нет

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

49 4 Шаг 6 Следующий шаг >

Рис. 2.17: Вопрос 2.3.4

2.4 Беспроводные сети Wi-Fi

Действительно, это определение Wi-Fi (рис. 2.18).

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

Wi-Fi - это

Выберите один вариант из списка

☒ Верно. Так держатся!

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

42 4 Шаг 4 Следующий шаг >

Рис. 2.18: 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. 2.19).

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

На каком уровне работает протокол WIFI?

Выберите один вариант из списка

✓ Хорошие новости, верно!

Верно решили 972 учащихся
Из всех попыток 58% верных

☐ Транспортном
☐ Прикладном
☒ Канальном
☐ Сетевом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

42 4 Шаг 5 Следующий шаг >

Рис. 2.19: 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. 2.20).

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

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

✓ Верно. Так держать!

Верно решили 973 учащихся
Из всех попыток 60% верных

☐ WPA
☒ WEP
☐ WPA2
☐ WPA3

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

42 4 Шаг 6 Следующий шаг >

Рис. 2.20: Вопрос 2.4.3

Нужно аутентифицировать устройства и позже передаются зашифрованные данные (рис. 2.21).

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

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

✓ Хорошая работа.

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

42 4 Шаг 7 Следующий шаг >

Рис. 2.21: Вопрос 2.4.4

В целом, понятно по названию, что WPA2 Personal для личного использования, то есть для домашней сети, enterprise - для предприятий (рис. 2.22).

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

✓ Прекрасный ответ.

Верно решили 975 учащихся
Из всех попыток 87% верных

- ☒ WPA2 Personal
- ☐ WPA2 Enterprise

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

42 4 Шаг 8 Следующий шаг >

Рис. 2.22: Вопрос 2.4.5

3 Выводы

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