

Отчет по этапу выполнения внешнего курса

Безопасность в сети

Татьяна Александровна Буллер

Содержание

1	Цель работы	5
2	Выполнение контрольных заданий	6
2.1	Как работает Интернет	6
2.2	Персонализация сети	12
2.3	Браузер TOP. Анонимизация	16
2.4	Беспроводные сети Wi-Fi	19
3	Выводы	23

Список таблиц

Список иллюстраций

2.1 Задание 1	6
2.2 Задание 2	7
2.3 Задание 3	8
2.4 Задание 4	9
2.5 Задание 5	9
2.6 Задание 6	10
2.7 Задание 7	10
2.8 Задание 8	11
2.9 Задание 9	11
2.10 Задание 10	12
2.11 Задание 11	13
2.12 Задание 12	14
2.13 Задание 13	15
2.14 Задание 14	16
2.15 Задание 15	17
2.16 Задание 16	18
2.17 Задание 17	18
2.18 Задание 18	19
2.19 Задание 19	20
2.20 Задание 20	21
2.21 Задание 21	21
2.22 Задание 22	22

1 Цель работы

Получение и закрепление на практике знаний об основных механизмах работы сети Интернет и их слабых местах.

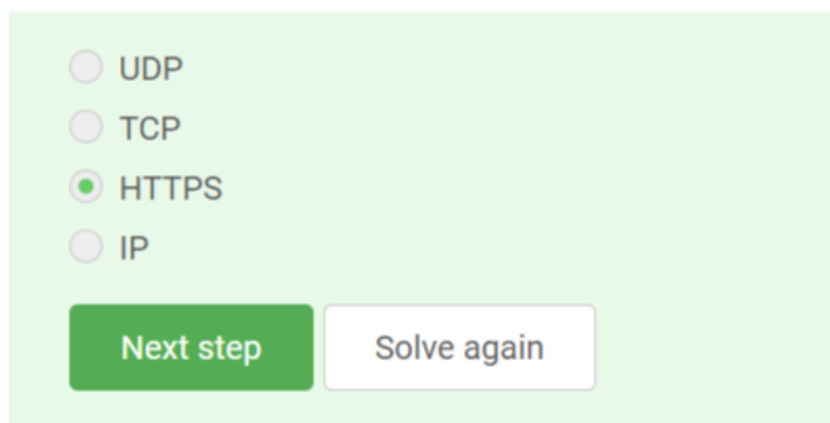
2 Выполнение контрольных заданий

2.1 Как работает Интернет

Выберите протокол прикладного уровня

Select one option from the list

✓ Totally right.



The screenshot shows a quiz interface with a light green background. At the top, there is a text prompt in Russian: "Выберите протокол прикладного уровня". Below it, an English instruction says "Select one option from the list". A green checkmark icon is followed by the text "Totally right.". Below this, there is a list of four protocols: UDP, TCP, HTTPS, and IP. Each protocol is preceded by a radio button. The radio button for HTTPS is filled with green, indicating it is the selected correct answer. At the bottom of the list, there are two buttons: a green "Next step" button and a white "Solve again" button with a grey border.

- ☐ UDP
- ☐ TCP
- ☒ HTTPS
- ☐ IP


Next step Solve again

Рис. 2.1: Задание 1

Протоколы TCP и UDP - протоколы транспортного уровня, IP - протокол сетевого уровня. Прикладным из перечисленных является только HTTPS. Это же рассуждение дает ответ на следующий вопрос.

На каком уровне работает протокол TCP?

Select one option from the list

 Fabulous answer.

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

Next step

Solve again

Рис. 2.2: Задание 2

Выберите все корректные адреса IPv4

Select all correct options from the list

✓ Right.

You've solved a complex problem, congratulations! Now you can ask more questions, or compare your solution with others on [solution](#)

- ☐ 421.0.15.19
- ☐ 43.12.256.7
- ☒ 90.11.90.22
- ☒ 25.198.0.15

Next step

Solve again

Рис. 2.3: Задание 3

Первый из адресов начинается с 421, второй содержит 256. Ни то, ни другое не может являться корректным адресом IPv4, так как исловный максимальный адрес, который можно получить в этом стандарте - 255.255.255.255

DNS сервер

Select one option from the list

✓ Well done!

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

Next step

Solve again

Рис. 2.4: Задание 4

DNS (Domain Name Server) сопоставляет адрес сайта с его доменным именем и обеспечивает “навигацию” в Интернете. Он не сегментирует данные, не выбирает маршруты для пакетов и не занимается адресацией.

Выберите корректную последовательность протоколов в модели TCP/IP

Select one option from the list

✓ Good news for you, correct!

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

Next step

Solve again

Рис. 2.5: Задание 5

Прикладной уровень должен быть “верхним”, канальный - нижним, таким образом, корректна только последняя цепочка.

Протокол http предполагает

Select one option from the list

✓ Fabulous answer.

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

Next step

Solve again

Рис. 2.6: Задание 6

HTTP не предполагает шифрования данных, поэтому считается небезопасным и устаревшим. Шифрует данные между клиентом и сервером HTTPS.

Протокол https состоит из

Select one option from the list

✓ Absolutely right.

- ☐ 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

Next step

Solve again

Рис. 2.7: Задание 7

HTTPS состоит из двух фаз: рукопожатия между клиентом и сервером, в результате которого устанавливаются “условия” общения, и обмена зашифрованными данными. Отсюда очевидно, что подходит только ответ 2.

Версия протокола TLS определяется

Select one option from the list

✓ You are right, well done!

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

Next step

Solve again

Рис. 2.8: Задание 8

Версия протокола TLS определяется совместно сервером и клиентом. ни одна из сторон не может “диктовать” свои условия другой.

В фазе “рукопожатия” протокола TLS не предусмотрено

Select one option from the list

✓ Good job.

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

Next step

Solve again

Рис. 2.9: Задание 9

В фазе рукопожатия не предусмотрено именно шифрования данных, так как

оно выполняется после установки условий обмена данными в отдельной фазе.

2.2 Персонализация сети

Куки хранят:

Select all correct options from the list

✓ Totally right.

You've solved a complex problem, congratulations! Now you can help other questions, or compare your solution with others on [solution forum](#).

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

Next step

Solve again

Рис. 2.10: Задание 10

По-хорошему куки не должны хранить конфиденциальную информацию, такую как пароль или адрес пользователя. поэтому подходят только два последних ответа: идентификатор пользователя и сессии.

Куки не используются для

Select one option from the list

✓ Right.

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

Next step

Solve again

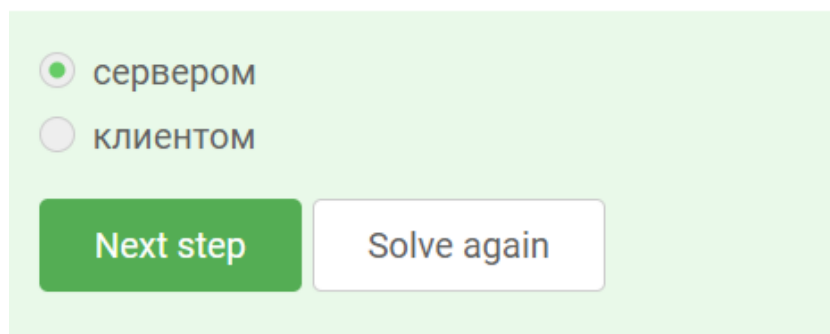
Рис. 2.11: Задание 11

Куки хранят информацию, но не используются для обеспечения надежности соединения самого по себе. Хотя хранение информации на стороне клиента может в общем и целом снижать загруженность сервера.

Куки генерируются

Select one option from the list

✓ Right.



The screenshot shows a quiz interface with a light green background. At the top, there is a green circle with a white checkmark followed by the text "Right.". Below this, there are two radio button options: "сервером" (selected) and "клиентом". At the bottom, there are two buttons: "Next step" (green) and "Solve again" (white with a green border).

Рис. 2.12: Задание 12

Куки присваиваются (генерируются) пользователю сервером и хранятся на стороне клиента.

Сессионные куки хранятся в браузере?

Select one option from the list

✓ Absolutely right.

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

Next step

Solve again

Рис. 2.13: Задание 13

Сессионные куки отвечают за хранение данных, связанных с конкретной сессией (моментом посещения и использования) сайта. Они хранятся в браузере только во время использования сайта (жизни сессии).

2.3 Браузер TOR. Анонимизация

Сколько промежуточных узлов в луковой сети TOR?

Select one option from the list

✓ You're right!

☐ 2

☒ 3

☐ 4

Next step

Solve again

Рис. 2.14: Задание 14

В сети TOR минимум три промежуточных узла: охранный, промежуточный и выходной.

IP-адрес получателя известен

Select all correct options from the list

✓ Good job.

You've solved a complex problem, congratulations! Now you can help others by answering questions, or compare your solution with others on [solution forum](#).

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

Next step

Solve again

Рис. 2.15: Задание 15

Адрес получателя известен отправителю (он выбирает, кому направить сообщение) и выходному узлу (он передает сообщение, полученное от предыдущих узлов цепи, непосредственно получателю).

Отправитель генерирует общий секретный ключ

Select one option from the list

✓ Correct.

☐ только с охранным узлом

☐ с охранным и промежуточным узлом

☒ с охранным, промежуточным и выходным узлом

☐ с промежуточным и выходным узлом

Next step Solve again

Рис. 2.16: Задание 16

Общий секретный ключ отправитель генерирует с каждым из узлов цепи для сохранения целостности передачи.

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

Select one option from the list

✓ You're right!

Correct answer from 961 learners
Total 74% of tries are correct

☐ Да

☒ Нет

Next step Solve again

Рис. 2.17: Задание 17

Получатель не должен использовать браузер, основанный на луковой маршрутизации, так как доставка сообщения не зависит от него.

2.4 Беспроводные сети Wi-Fi

Wi-Fi - это

Select one option from the list

✓ Fabulous answer.

Com
Tot

- ☐ 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

Next step Solve again

Рис. 2.18: Задание 18

Wi-Fi - технология беспроводной сети; работает не только со смартфонами или компьютерами и описана в стандарте 802.11

На каком уровне работает протокол WiFi?

Select one option from the list

✓ Fabulous answer.

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

Next step

Solve again

Рис. 2.19: Задание 19

Wi-Fi - канал передачи данных, и работает, соответственно, на канальном уровне. На сетевом работает IP, на прикладном - HTTP/HTTPS, на транспортном - TCP/UDP.

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Select one option from the list

✓ Correct.

☐ WPA

☒ WEP

☐ WPA2

☐ WPA3

Next step

Solve again

Рис. 2.20: Задание 20

Наименее безопасен из перечисленных WEP, так как длина ключа в этом протоколе не могла превышать 40 бит.

Данные между хостом сети (компьютером или смартфоном) и роутером

Select one option from the list

✓ Yes!

☐ передаются в открытом виде

☒ передаются в зашифрованном виде после аутентификации устройств

☐ передаются в открытом виде после аутентификации устройств

☐ передаются в зашифрованном виде

Next step

Solve again

Рис. 2.21: Задание 21

Данные между хостом и роутером передаются только после аутентификации устройства в сети в зашифрованном виде, поэтому все ответы, кроме 2, неверны.

Для домашней сети для аутентификации обычно используется метод

Select one option from the list

✓ Yes!

☒ WPA2 Personal

☐ WPA2 Enterprise

Next step

Solve again

Рис. 2.22: Задание 22

Энтерпрайс - решение для бизнеса. Для организации домашних сетей оно не используется.

3 Выводы

Получены и закреплены на практике знания об основных механизмах работы сети Интернет и их слабых местах.