

Прохождения внешнего курса на тему Основы кибербезопасности. Часть 1

Основы информационной безопасности

Просина Ксения Максимовна

Содержание

1	1 0 курсе	5
2	2 Безопасность в сети	6
2.1	2.1 Как работает интернет: базовые сетевые протоколы	6
2.2	2.2 Персонализация сети.....	13
2.3	2.3 Браузер TOR. Анонимизация.....	17
2.4	2.4 Беспроводные сети WiFi.....	19

Список иллюстраций

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

Список таблиц

1 1 0 курсе

В этом разделе описана общая информация о курсе, определены цели и дальнейшие планы по курсу. Также даны ссылки на литературу и полезные ссылки.

2 2 Безопасность в сети

2.1 2.1 Как работает интернет: базовые сетевые протоколы

Вопрос/Ответ 1 (рис. 2.1)

Выберите один вариант из списка

☒ Всё правильно.

Верно решили **895** учащихся
Из всех попыток **58%** верных

☐ UDP
☐ TCP
☒ HTTPS
☐ IP

Следующий шаг Решить снова

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

👍 107 👎 14 Шаг 7 Следующий шаг >

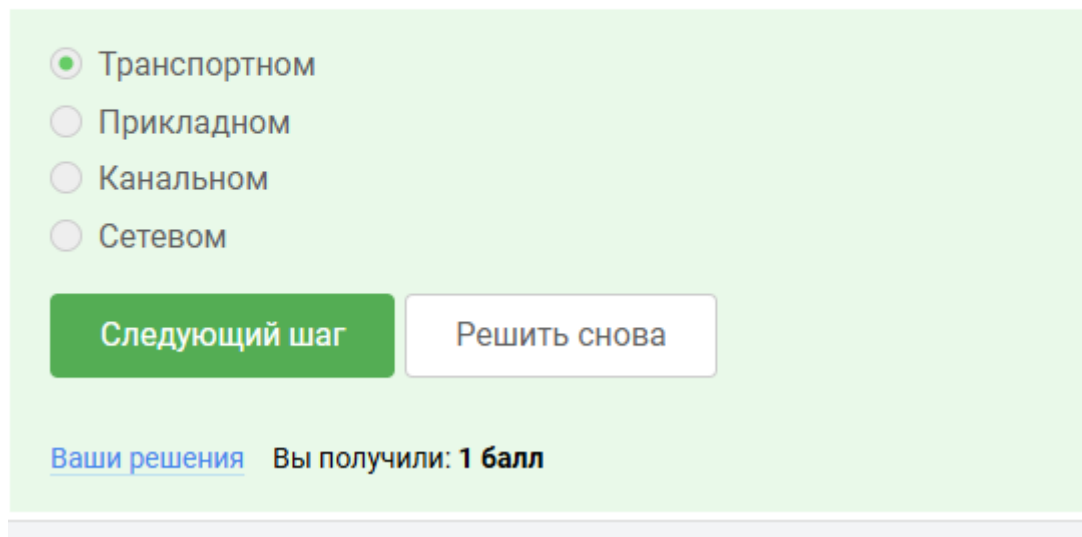
Рис. 2.1: Вопрос/Ответ 1

Пояснение ответа: HTTPS (Hypertext Transfer Protocol Secure) — это расширение протокола HTTP, которое обеспечивает безопасную передачу данных через шифрование с помощью SSL/TLS. Он использует TCP для гарантированной доставки данных, что делает его идеальным выбором для приложений, требующих как надежности, так и защиты информации, например, для онлайн-банкинга и интернет-магазинов.

Вопрос/Ответ 2 (рис. 2.2)

Выберите один вариант из списка

✓ Здорово, всё верно.



The screenshot shows a quiz interface with a light green background. At the top, there is a heading "Выберите один вариант из списка". Below it, a green checkmark icon is followed by the text "Здорово, всё верно.". In the center, there is a list of four radio button options: "Транспортном", "Прикладном", "Канальном", and "Сетевом". The "Транспортном" option is selected. Below the list are two buttons: a green "Следующий шаг" button and a white "Решить снова" button. At the bottom left, there is a link "Ваши решения" and a score display "Вы получили: 1 балл".

☒ Транспортном
☐ Прикладном
☐ Канальном
☐ Сетевом

Следующий шаг Решить снова

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

Рис. 2.2: Вопрос/Ответ 2

Пояснение ответа: Протокол TCP (Transmission Control Protocol) работает на транспортном уровне модели OSI (Open Systems Interconnection). Этот уровень отвечает за надежную передачу данных между узлами сети, обеспечивая такие функции, как управление потоком, контроль ошибок и установление соединений.

Вопрос/Ответ 3 (рис. 2.3)

Выберите все корректные адреса IPv4

Выберите все подходящие ответы из списка

✓ Верно. Так держать!

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

Следующий шаг

Решить снова

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

Рис. 2.3: Вопрос/Ответ 3

Пояснение ответа: 421.0.15.19 — некорректный, поскольку 421 превышает 255, 43.12.256.7 — некорректный, поскольку 256 превышает 255.

Вопрос/Ответ 4 (рис. 2.4)

DNS сервер

Выберите один вариант из списка

☒ Хорошая работа.

- ☒ 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**

Рис. 2.4: Вопрос/Ответ 4

Пояснение ответа: Основная задача DNS сервера это сопоставить название, то есть доменное имя, с корректным ip адресом, с тем, где лежит этот сервер, этот сайт.

Вопрос/Ответ 5 (рис. 2.5)

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

✓ Верно.

- ☐ 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/Ответ 5

Пояснение ответа: Модель TCP/IP состоит из четырех уровней: - Прикладной

- Транспортный
- Сетевой
- Канальный

Вопрос/Ответ 6 (рис. 2.6)

Протокол http предполагает

Выберите один вариант из списка

✓ Так точно!

- ☐ 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

Рис. 2.6: Вопрос/Ответ 6

Пояснение ответа: Протокол прикладного уровня http в отличие от https передает данные между клиентом и сервером в открытом виде.

Вопрос/Ответ 7 (рис. 2.7)

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

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.7: Вопрос/Ответ 7

Пояснение ответа: Протокол https состоит из двух фаз:

- Рукопожатие(идентификация между сервером и клиентом)

- Передача данных

Вопрос/Ответ 8 (рис. 2.8)

Версия протокола TLS определяется

Выберите один вариант из списка

☒ Верно. Так держать!

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

Следующий шаг

Решить снова

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

Рис. 2.8: Вопрос/Ответ 8

Пояснение ответа: В ходе TLS-рукопожатия клиент и сервер совместно выполняют следующие действия:

- Указывают какую версию TLS они будут использовать
- Какие наборы шрифтов они будут использовать
- Аутентификация идентичности сервера с помощью открытого ключа сервера и цифровой подписи центра сертификации ssl
- Генерация сеансовых ключей для использования симметричного шифрования после завершения рукопожатия.

Вопрос/Ответ 9 (рис. 2.9)

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

✓ Отлично!

- ☐ 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**

Рис. 2.9: Вопрос/Ответ 9

Пояснение ответа: Рукопожатие - идентификация между сервером и клиентом, оно не подразумевает шифрование данных.

2.2 2.2 Персонализация сети

Вопрос/Ответ 1 (рис. 2.10)

Куки хранят:

Выберите все подходящие ответы из списка

✓ Всё правильно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в их вопросы, или сравнить своё решение с другими на [форуме решений](#).

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

Следующий шаг

Решить снова

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

Рис. 2.10: Вопрос/Ответ 1

Пояснение ответа: Куки хранят:

- id пользователя
- id сессии
- тип браузера, время запросов
- некоторые действия пользователя

Вопрос/Ответ 2 (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**

Рис. 2.11: Вопрос/Ответ 2

Пояснение ответа: Куки - данные, передаваемые от сервера к клиенту для его идентификации. Куки позволяют:

- Сохранять сессионную информацию
- Персонализировать страницы

Вопрос/Ответ 3 (рис. 2.12)

Куки генерируются

Выберите один вариант из списка

☒ Верно. Так держать!

☒ сервером
☐ клиентом

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

[Следующий шаг](#) [Решить снова](#)

Рис. 2.12: Вопрос/Ответ 3

Пояснение ответа: Куки генерируется сервером, и запрашивает разрешение на использование клиентом.

Вопрос/Ответ 4 (рис. 2.13)

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

☒ Здорово, всё верно.

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

[Ваши решения](#) Вы получили: ...

[Следующий шаг](#) [Решить снова](#)

Рис. 2.13: Вопрос/Ответ 4

Пояснение ответа: Сессионные куки хранятся в браузере на время пользование веб сайтом.

2.3 2.3 Браузер TOR. Анонимизация

Вопрос/Ответ 1 (рис. 2.14)

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

☒ Так точно!

☐ 2

☒ 3

☐ 4

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.14: Вопрос/Ответ 1

Пояснение ответа: В луковой сети TOR три промежуточных узла:

- Охранный узел
- Промежуточный узел
- Выходной узел

Вопрос/Ответ 2 (рис. 2.15)

IP-адрес получателя известен

Выберите все подходящие ответы из списка

✓ Отличное решение!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [ком](#) 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/Ответ 2

Пояснение ответа: IP адрес отправителя известен только отправителю и выходному узлу, в охранном и промежуточном узле он зашифрован.

Вопрос/Ответ 3 (рис. 2.16)

Куки генерируются

Выберите один вариант из списка

✓ Верно. Так держать!

- ☒ сервером
- ☐ клиентом

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.16: Вопрос/Ответ 3

Пояснение ответа: Отправитель генерирует общий секретный ключ со всеми узлами(охранным, промежуточным, выходным), они одеты друг на друга как оболочка у лука.

Вопрос/Ответ 4 (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

✓ Так точно!

Верно решил 961 учащийся
Из всех попыток 74% верных

☒ Нет
☐ Да

Следующий шаг Решить снова

Рис. 2.17: Вопрос/Ответ 4

Пояснение ответа: Получателю не обязательно использовать браузер TOR для успешного получения пакетов.

2.4 2.4 Беспроводные сети WiFi

Вопрос/Ответ 1 (рис. 2.18)

Wi-Fi - это

Выберите один вариант из списка

✓ Правильно, молодец!

☐ 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

Рис. 2.18: Вопрос/Ответ 1

Пояснение ответа: WiFi - технология беспроводной локальной сети, работающей в соответствии со стандартами IEEE 802.11.

Вопрос/Ответ 2 (рис. 2.19)

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

✓ Правильно.

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

Следующий шаг

Решить снова

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

Рис. 2.19: Вопрос/Ответ 2

Пояснение ответа: Протокол WiFi работает на самом низком уровне, канальном уровне.

Вопрос/Ответ 3 (рис. 2.20)

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

✓ Правильно, молодец!

- ☐ WPA
- ☒ WEP
- ☐ WPA2
- ☐ WPA3

Следующий шаг

Решить снова

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

Рис. 2.20: Вопрос/Ответ 3

Пояснение ответа: Самым ранним и на сегодняшний день небезопасный метод шифрования данных WiFi называется WEP. Он устарел и уже категорически не рекомендуется к использованию, потому что использовал малую длину ключа, 40 бит.

Вопрос/Ответ 4 (рис. 2.21)

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

☒ Отлично!

☐ передаются в открытом виде после аутентификации устройств

☒ передаются в зашифрованном виде после аутентификации устройств

☐ передаются в зашифрованном виде

☐ передаются в открытом виде

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.21: Вопрос/Ответ 4

Пояснение ответа: Данные между хостом сети и роутером передаются в зашифрованном виде после аутентификации устройств.

Вопрос/Ответ 5 (рис. 2.22)

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

✓ Прекрасный ответ.

- ☒ WPA2 Personal
- ☐ WPA2 Enterprise

Следующий шаг

Решить снова

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

Рис. 2.22: Вопрос/Ответ 5

Пояснение ответа: Для домашней сети для аутентификации обычно используется метод WPA2 Personal, который использует пароль для аутентификации, в то время как WPA2 Enterprise использует базу данных с пользователями, которые могут подключиться к WiFi.