

# **Отчет по первому этапу внешнего курса**

**Дисциплина: основы информационной безопасности**

Казазаев Даниил Михайлович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Этап первый</b>	<b>5</b>
<b>3</b>	<b>Выполнение первого этапа внешнего курса.</b>	<b>6</b>
3.1	Базовые сетевые протоколы . . . . .	6
3.2	Персонализация сети . . . . .	12
<b>4</b>	<b>Браузер TOR</b>	<b>17</b>
<b>5</b>	<b>Беспроводные сети Wi-fi</b>	<b>21</b>
<b>6</b>	<b>Вывод</b>	<b>24</b>

## Список иллюстраций

3.1	Первый вопрос . . . . .	6
3.2	Второй вопрос . . . . .	7
3.3	Третий вопрос . . . . .	8
3.4	Четвертый вопрос . . . . .	9
3.5	Пятый вопрос . . . . .	10
3.6	Шестой вопрос . . . . .	10
3.7	Седьмой вопрос . . . . .	11
3.8	Восьмой вопрос . . . . .	11
3.9	Девятый вопрос . . . . .	12
3.10	Первый вопрос . . . . .	13
3.11	Второй вопрос . . . . .	14
3.12	Третий вопрос . . . . .	15
3.13	Четвертый вопрос . . . . .	16
4.1	Первый вопрос . . . . .	17
4.2	Второй вопрос . . . . .	18
4.3	Третий вопрос . . . . .	19
4.4	Четвертый вопрос . . . . .	20
5.1	Первый вопрос . . . . .	21
5.2	Второй вопрос . . . . .	22
5.3	Третий вопрос . . . . .	22
5.4	Четвертый вопрос . . . . .	23
5.5	Пятый вопрос . . . . .	23

# 1 Цель работы

Внешний кур состоит из трех этапов.

## 2 Этап первый

Первый этап курса состоит из 4 частей:

1. Базовые сетевые протоколы
2. Персонализация сети
3. Браузер TOR
4. Беспроводные сети Wi-fi

## 3 Выполнение первого этапа внешнего курса.

### 3.1 Базовые сетевые протоколы

HTTPS является протоколом прикладного уровня. (рис. 3.1)

Выберите протокол прикладного уровня

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решили 895 учащихся  
Из всех попыток 58% верных

☐ UDP  
☐ TCP  
☒ HTTPS  
☐ IP

Следующий шаг    Решить снова

Ваши решения    Вы получили: 1 балл

👍 105    🗳️ 14    Шаг 7    Следующий шаг >

Рис. 3.1: Первый вопрос

Протокол TCP работает на транспортном уровне. (рис. 3.2)

На каком уровне работает протокол TCP?

Выберите один вариант из списка

☒ Так точно!

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

Следующий шаг

Решить снова

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

Рис. 3.2: Второй вопрос

Адреса формата IPv4 состоят из 4-х значений от 0 до 255. (рис. 3.3)

Выберите все корректные адреса IPv4

**Выберите все подходящие ответы из списка**

✓ Правильно, молодец!

Вы решили сложную задачу, поздравляем! Вы можете по [комментариях](#), отвечая на их вопросы, или сравнить свои [решений](#).

☐ 421.0.15.19

☐ 43.12.256.7

☒ 90.11.90.22

☒ 25.198.0.15

Следующий шаг

Решить снова

Рис. 3.3: Третий вопрос

DNS сервера необходимы для сопоставления IP адреса с доменным именем при маршрутизации запроса. (рис. 3.4)



DNS сервер

**Выберите один вариант из списка**

☒ Верно. Так держать!

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

Следующий шаг

Решить снова

Рис. 3.4: Четвертый вопрос

Корректная последовательность протоколов в модели TCP/IP. (рис. 3.5)

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

Верно решил **941** учащ  
Из всех попыток **53%** е

✓ Правильно.

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

Следующий шаг

Решить снова

Рис. 3.5: Пятый вопрос

Так как http это незащищенный протокол, он предполагает передачу данных в открытом виде.(рис. 3.6)

Протокол http предполагает

Выберите один вариант из списка

Верно решили **965** ,  
Из всех попыток **78**

✓ Отлично!

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

Следующий шаг

Решить снова

Рис. 3.6: Шестой вопрос

HTTPS протокол состоит из двух фаз: рукопожатия и передачи данных.(рис. 3.7)

Протокол https состоит из

Выберите один вариант из списка

Верно решили **948** учащихся  
Из всех попыток **41%** верно

✓ Правильно.

- ☐ 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

Рис. 3.7: Седьмой вопрос

Версия протокола TLS определяется как клиентом, так и сервером на стадии “переговоров”.(рис. 3.8)

Версия протокола TLS определяется

Выберите один вариант из списка

Верно решили  
Из всех попыток

✓ Правильно, молодец!

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

Следующий шаг

Решить снова

Рис. 3.8: Восьмой вопрос

На фазе рукопожатия протокола TLS не предусмотрено шифрование данных.(рис. 3.9)

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

Верно решил **931** учащихся  
Из всех попыток **44%** верно

☒ Всё правильно.

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

[Следующий шаг](#) [Решить снова](#)

Рис. 3.9: Девятый вопрос

## 3.2 Персонализация сети

Куки-файлы хранят в себе информацию о идентификаторе пользователя и id сессии.(рис. 3.10)

Куки хранят:

**Выберите все подходящие ответы из списка**

☒ Хорошие новости, верно!

Вы решили сложную задачу, поздравляем! Вы можете почитать [комментариях](#), отвечая на их вопросы, или сравнить свои [решений](#).

☒ идентификатор пользователя

☐ IP адрес

☒ id сессии

☐ пароль пользователя

Следующий шаг

Решить снова

Рис. 3.10: Первый вопрос

Куки-файлы не используются для улучшения надежности соединения. (рис. 3.11)

Куки не используются для

**Выберите один вариант из списка**

☒ Верно. Так держать!

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

Следующий шаг

Решить снова

Рис. 3.11: Второй вопрос

Куки-файлы генерируются сервером. (рис. 3.12)

Куки генерируются

**Выберите один вариант из списка**

☒ Всё получилось!

☒ сервером

☐ клиентом

**Следующий шаг**

Решить снова

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

Рис. 3.12: Третий вопрос

Сессионные куки хранятся в браузере на время пользования им. (рис. 3.13)

Сессионные куки хранятся в браузере?

**Выберите один вариант из списка**

☒ Хорошие новости, верно!

☐ Да, на время пользования веб-сайтом

☐ Нет

☐ Да, на некоторое время, заданное в сервером

Следующий шаг

Решить снова

Рис. 3.13: Четвертый вопрос



## 4 Браузер TOR

В браузере на основе TOR три промежуточных узла: охранный, промежуточный, выходной. (рис. 4.1)

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

☒ Так точно!

☐ 2

☒ 3

☐ 4

Следующий шаг

Решить снова

Рис. 4.1: Первый вопрос

IP-адрес получателя в системе TOR измещен только отправителю и выходному узлу. (рис. 4.2)

IP-адрес получателя известен

**Выберите все подходящие ответы из списка**

☒ Отличное решение!

Вы решили сложную задачу, поздравляем! Вы можете почитать [комментариях](#), отвечая на их вопросы, или сравнить свои [решений](#).

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

Следующий шаг

Решить снова

Рис. 4.2: Второй вопрос

При запросе через TOR отправитель генерирует общий секретный ключ со всеми узлами. (рис. 4.3)

Отправитель генерирует общий секретный ключ

**Выберите один вариант из списка**

☒ Верно.

- ☐ только с охранным узлом
- ☐ с охранным и промежуточным узлом
- ☒ с охранным, промежуточным и выходным узлом
- ☐ с промежуточным и выходным узлом

Следующий шаг

Решить снова

Рис. 4.3: Третий вопрос

Получатель может использовать любой браузер для принятия запроса из TOR.  
(рис. 4.4)

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

Выберите один вариант из списка

☒ Хорошая работа.

☐ Нет

☐ Да

Следующий шаг

Решить снова

Верно решил **961** учащийся  
Из всех попыток **74%** верно

Рис. 4.4: Четвертый вопрос

## 5 Беспроводные сети Wi-fi

Wf-fi - это ... (рис. 5.1)

Wi-Fi - это

Выберите один вариант из списка

Верно решили **965** учащихся  
Из всех попыток **79%** верно

☒ Здорово, всё верно.

☐ 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

Рис. 5.1: Первый вопрос

Протоколы Wf-fi работают на канальном уровне. (рис. 5.2)

На каком уровне работает протокол WiFi?

Верно решено  
Из всех попыток 100% верно

Выберите один вариант из списка

✓ Отличное решение!

☐ Транспортном  
☐ Прикладном  
☒ Канальном  
☐ Сетевом

Следующий шаг    Решить снова

Рис. 5.2: Второй вопрос

Самой небезопасный метод шифрования и аутентификации Wf-fi это WEP, так как он старый и в нем используется малое количество бит для шифрования. (рис. 5.3)

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Верно решили 973 учащихся  
Из всех попыток 60% верно

Выберите один вариант из списка

✓ Всё получилось!

☐ WPA  
☒ WEP  
☐ WPA2  
☐ WPA3

Следующий шаг    Решить снова

Рис. 5.3: Третий вопрос

Данные шифруются после аутентификации пользователя. (рис. 5.4)

Данные между хостом сети (компьютером или смартфоном) и роутером

Верно решили **975** учас  
Из всех попыток **53%** в

**Выберите один вариант из списка**

☒ Так точно!

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

**Следующий шаг** Решить снова

Рис. 5.4: Четвертый вопрос

Для домашних сетей используется аутентификатор Wi-fi Personal. (рис. 5.5)

Для домашней сети для аутентификации обычно используется метод

Верно решили **975** у  
Из всех попыток **87%**

**Выберите один вариант из списка**

☒ Отличное решение!

- ☒ WPA2 Personal
- ☐ WPA2 Enterprise

**Следующий шаг** Решить снова

Рис. 5.5: Пятый вопрос

## **6 Вывод**

Выполнен первый этап внешнего курса