

Отчёт по Внешнему Курсу - Этап 1

Основы информационной безопасности

Чистов Даниил Максимович

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Выводы	16
4	Список литературы	17

Список иллюстраций

2.1	Задание 1	5
2.2	Задание 002	6
2.3	Задание 003	6
2.4	Задание 004	7
2.5	Задание 005	8
2.6	Задание 006	8
2.7	Задание 007	9
2.8	Задание 008	9
2.9	Задание 009	10
2.10	Задание 010	10
2.11	Задание 011	11
2.12	Задание 012	11
2.13	Задание 013	12
2.14	Задание 014	12
2.15	Задание 015	13
2.16	Задание 016	13
2.17	Задание 017	13
2.18	Задание 018	14
2.19	Задание 019	14
2.20	Задание 020	15
2.21	Задание 021	15
2.22	Задание 022	15

1 Цель работы

Пройти внешний курс - Этап 1

2 Выполнение лабораторной работы

В лекционных материалах было сказано, что в протоколы прикладного уровня включён HTTPS (рис. 2.1).

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

Рис. 2.1: Задание 1

TCP работает на транспортном уровне, IP - на сетевом (рис. 2.2).

На каком уровне работает протокол TCP?

Выберите один вариант из списка

☒ Верно. Так держать!

☐ Транспортном

☐ Прикладном

☐ Канальном

☐ Сетевом

Следующий шаг

Решить снова

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

Рис. 2.2: Задание 002

Т.к. IPv4 - набор цифр от 0 до 255, следовательно исключаем варианты, которые содержат числа больше/меньше этого набора (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: Задание 003

DNS сопоставляет доменное имя соответствующий ему IP (рис. 2.4).

DNS сервер

Выберите один вариант из списка

 **Правильно.**

- ☒ 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: Задание 004

Порядок такой (рис. 2.5).

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

✓ Правильно, молодец!

- ☐ 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: Задание 005

http - предоставляет в открытом виде, именно эту проблему решает https, он работает также, только в этот раз данные шифруются (рис. 2.6).

Протокол http предполагает

Выберите один вариант из списка

✓ Прекрасный ответ.

- ☐ 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: Задание 006

Рукопожатие и передача данных, аутентификации не входит (рис. 2.7).

Протокол https состоит из

Выберите один вариант из списка

✓ Прекрасный ответ.

- ☐ 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**

Рис. 2.7: Задание 007

Обязательно версия протокола определяется обоими (рис. 2.8).

Версия протокола TLS определяется

Выберите один вариант из списка

✓ Всё правильно.

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

Следующий шаг

Решить снова

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

Рис. 2.8: Задание 008

Шифрование данных не происходит в фазе рукопожатия, только после неё (рис. 2.9).

В фазе “рукопожатия” протокола TLS не предусмотрено

Выберите один вариант из списка

✓ 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

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

Рис. 2.9: Задание 009

Куки не хранят пароль пользователя или его IP адрес (рис. 2.10).

Куки хранят:

Выберите все подходящие ответы из списка

✓ Правильно.

Верно решили **856** учащихся
Из всех попыток **18%** 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](#).

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

Следующий шаг

Решить снова

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

Рис. 2.10: Задание 010

Куки не сильно влияют на безопасность, скорее упрощают работу пользователям (рис. 2.11).

Куки не используются для

Выберите один вариант из списка

✓ Правильно.

Верно решили 950 учащихся
Из всех попыток 53% верных

- ☐ 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: Задание 011

Куки генерируются сервером и отправляются клиенту, а не наоборот (рис. 2.12).

Куки генерируются

Выберите один вариант из списка

✓ Так точно!

- ☒ сервером
- ☐ клиентом

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.12: Задание 012

Сессионные куки исчезнут, как только мы закроем окно с веб-сайтом (рис. 2.13).

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

☒ Верно. Так держать!

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

Следующий шаг

Решить снова

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

Рис. 2.13: Задание 013

3, т.к. больше узлов анонимности не прибавляют, а при меньших узлах теряется смысл всего алгоритма маршрутизации TOR (рис. 2.14).

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

☒ Всё получилось!

Верно решили 959 учащихся
Из всех попыток 77% верных

- ☐ 2
- ☒ 3
- ☐ 4

Следующий шаг

Решить снова

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

Рис. 2.14: Задание 014

При шифровании так получается, что охранный узел и промежуточный узел не знают по итогу IP адрес получателя данных (рис. 2.15).

IP-адрес получателя известен

Выберите все подходящие ответы из списка

✓ 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 **906** учащихся
Из всех попыток **19%** верных

☐ охранному узлу
☐ промежуточному узлу
☒ отправителю
☒ выходному узлу

Следующий шаг Решить снова

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

Рис. 2.15: Задание 015

Отправитель генерирует общий секретный ключ со всеми тремя узлами (рис. 2.16).

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

✓ Всё получилось!

Верно решили **959** учащихся
Из всех попыток **55%** верных

☐ только с охранном 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**

Рис. 2.16: Задание 016

Нет, не должен, далее возвращение данных происходит как обычно (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

✓ Хорошая работа.

Верно решил **961** учащихся
Из всех попыток **74%** верных

☐ Да
☒ Нет

Следующий шаг Решить снова

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

Рис. 2.17: Задание 017

У Wi-fi нет расшифровки, вообще это была такая пометка от компании, которая

проверяла поддерживает ли устройство беспроводную сеть, а так это технология беспроводной сети (рис. 2.18).

Wi-Fi - это

Выберите один вариант из списка

✓ Всё правильно.

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

Рис. 2.18: Задание 018

На канальном уровне, т.к. речь всё-таки идёт о физическом излучении и приёме сигнала (рис. 2.19).

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

✓ Абсолютно точно.

Верно решили 972 учащихся
Из всех попыток 56% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.19: Задание 019

WEP самый первый, но и к сожалению, небезопасный, на данный момент самый безопасный - WPA3 (рис. 2.20).

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

✓ Так точно!

Верно решили 973 учащихся
Из всех попыток 60% верных

☐ WPA
☒ WEP
☐ WPA2
☐ WPA3

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.20: Задание 020

На новых версиях беспроводных сетей происходит шифрование, но перед этим обязательно аутентификация (рис. 2.21).

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решили 975 учащихся
Из всех попыток 53% верных

☐ 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: Задание 021

Для домашней сети - personal, для Корпоративных сетей используют Enterprise, т.к. есть база данных её пользователей. Это усиливает безопасность корпорации. (рис. 2.22).

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решили 975 учащихся
Из всех попыток 87% верных

☒ WPA2 Personal
☐ WPA2 Enterprise

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 2.22: Задание 022

3 Выводы

Этап 1 пройден успешно на максимальный балл.

4 Список литературы

Курс “Основы Кибербезопасности” на платформе Stepik