***Защита информации от утечки по скрытым каналам.***

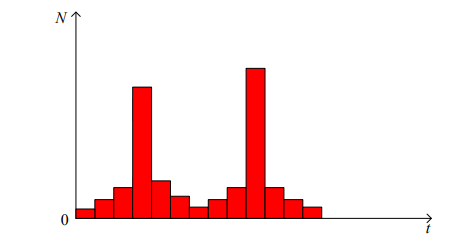
***Отчет по лабораторной работе №2.***

***Вариант дампа: 1.***

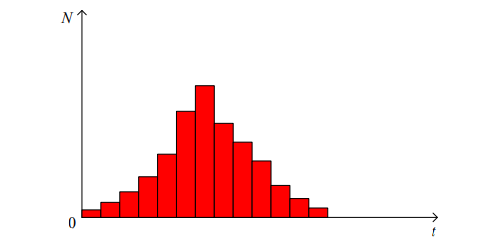
***Введение***

В рамках данной лабораторной работы изучался метод обнаружения бинарного сетевого скрытого канала в заранее подготовленном дампе трафика.

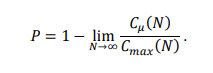
Пусть дан бинарный скрытый канал, основанный на изменении длин межпакетных интервалов. Будет выбрано два отрезка времени, один из которых будет кодироваться нулем, другой — единицей. Для передачи скрытой информации будут посылаться пакеты с задержкой, попадающей в один из двух данных интервалов. Таким образом, если построить гистограмму поведения трафика в сети для канала связи, в котором присутствует описанный скрытый канал, представленную на рисунке 1, где будет представлено распределение числа пакетов в зависимости от длин межпакетных интервалов, то на данной гистограмме будут видны два пика с максимальным числом переданных пакетов 𝐶𝑚𝑎𝑥, сосредоточенных возле выбранных на этапе кодирования временных интервалов. Среднее значение времени межпакетных интервалов µ, в свою очередь, будет находиться между двумя данными пиками. При этом количество пакетов 𝐶𝜇 в точке μ будет мало.



С другой стороны, если построить гистограмму, изображенную на рисунке 2, для канала связи без присутствия скрытого канала, то она будет заметно отличаться. Присутствует один пик, находящийся примерно по центру, в котором количество пакетов 𝐶𝜇 максимально по отношению к другим, то есть 𝐶𝜇 = 𝐶𝑚𝑎𝑥.



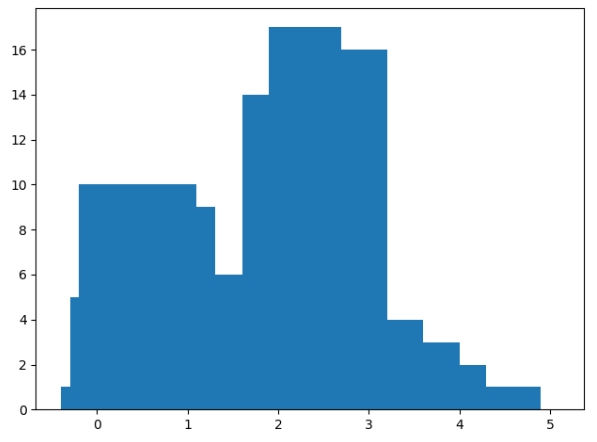
Тогда вероятность присутствия скрытого канала будет определяться по формуле



***Задание 1***

***Построение гистограммы длин межпакетных интервалов и определение вероятности присутствия в сети скрытого канала для всего дампа***

Для построения гистограммы исходный дамп был переведен в формат csv, распаршен с использованием модуля csv. За размер шага межпакетного интервала было взято значение в 0.1 секунду. После этого все пакеты были распределены по межпакетным интервалам и затем для каждого из межпакетных интервалов было посчитано количество пакетов. После этого на основе полученных данных была построена гистограмма:



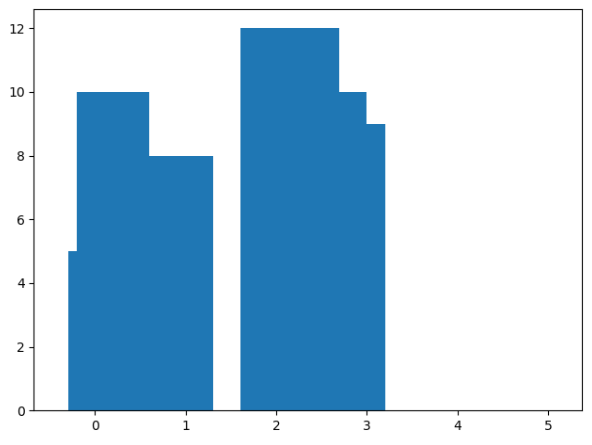
Исходя из данных, полученных на гистограмме была посчитана вероятность присутствия в сети бинарного скрытого канала, которая получилась равна:

(1 – 6 / 17) \* 100 = 64%

***Задание 2***

***Построение гистограммы длин межпакетных интервалов и определение вероятности присутствия в сети скрытого канала для последних 100 пакетов***

Программа реализующая это задание выполняет ровно то же самое, что и программа для первого задания, однако она работает только с последними 100 пакетами из дампа, так как по условию известно, что именно эти 100 пакетов используются для передачи сообщения по скрытому каналу. Результатом работы программы является гистограмма:



Исходя из данных, полученных на гистограмме была посчитана вероятность присутствия в сети бинарного скрытого канала, которая получилась равна:

(1 – 0 / 12) \* 100 = 100%

***Задание 3***

***Декодирование сообщения, переданного по скрытому каналу***

На основе данных, полученных в предыдущем шаге было сделано предположение о том, что все пакеты с межпакетным интервалом из левого пика кодируют ноль, а пакеты из правого пика – единицу. После этого предположения была получена бинарная строка, которая потом была переведена в текст. Полученное сообщение: **some\_cc\_ez\_2\_dtct.**

Код для всех трёх заданий доступен в GitHub репозитории: <https://github.com/BychkovGeorge/dumpScanner>

***Заключение***

В ходе выполнения данной работы были получены практические и теоретические навыки для обнаружения сетевых скрытых каналов. Были получены навыки для нахождения вероятности присутствия бинарного скрытого канала, основанного на изменении длин межпакетных интервалов в сети, а также навыки декодирования сообщений, передаваемых по таким скрытым каналам.