

Министерство науки и высшего образования Российской Федерации  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ  
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»  
ФАКУЛЬТЕТ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

## **Управление мобильными устройствами**

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2

«Обработка и тарификация трафика NetFlow», вариант № 10

Выполнил Студент,  
группы N3352 – Кузнецов Богдан Викторович

Проверил:  
Федоров И. Р.

Санкт-Петербург, 2020

## Цель работы:

изучение технологии работы протокола NetFlow, а также разработка и реализация программного модуля обработки трафика NetFlow v5 и тарификации абонента.

## Обработка исходных данных.

В работе используется язык программирования Python v3.7.6. с такими библиотеками как: pandas, numpy, matplotlib.pyplot, math.

Для перевода дампа NetFlow в формат .csv была задействована консольная команда, указанная ниже.

```
root@LAPTOP-BIJEL6VR:/home# nfdump -r nfcapd.202002251200 -o "fmt:%td, %sa, %da, %byt" | sed "s/ //g" | head -n -4 > data_.csv
```

Далее следует вид, к которому был приведен дамп.

Datefirstseen	Duration	SrcIPAddr	DstIPAddr	Bytes
2020-02-25	11:21:06	190,533.000	192.168.250.3	23.226.231.226,572
2020-02-25	11:28:30	860,90.270	192.168.250.50	40.114.211.99,2241
2020-02-25	11:29:30	210,31.580	192.168.250.3	23.226.231.226,308
2020-02-25	11:30:01	860,0.000	192.168.250.62	192.168.250.1,152
2020-02-25	11:30:01	860,0.000	192.168.250.1	192.168.250.62,152
2020-02-25	11:30:02	530,0.000	192.168.250.50	192.168.250.1,132
2020-02-25	11:30:02	540,0.000	192.168.250.1	192.168.250.50,450
2020-02-25	11:30:02	540,0.000	192.168.250.50	173.194.73.95,5023
2020-02-25	11:30:02	550,0.000	173.194.73.95	217.15.20.194,6248
2020-02-25	11:30:02	700,0.000	192.168.250.50	192.168.250.1,126
2020-02-25	11:30:02	700,0.000	192.168.250.50	192.168.250.1,112
2020-02-25	11:30:02	700,0.000	192.168.250.1	192.168.250.50,616
2020-02-25	11:30:02	700,0.000	192.168.250.1	192.168.250.50,502
2020-02-25	11:30:02	710,0.000	192.168.250.50	108.177.14.94,4313
2020-02-25	11:30:02	730,0.000	108.177.14.94	217.15.20.194,4185

Для реализации таких задач, как тарификация абонента и построение графика зависимости объема трафика от времени были созданы 2 файла: main.py и graph2.py соответственно.

## Файл main.py

```
#Протарифицировать абонента с IP-адресом 192.0.73.2
#с коэффициентом k: 0,5руб/Мб первые 200Мб, далее 1руб/Мб
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import math
```

```

ip = '192.0.73.2'
k = 0.5

#nfdump -r nfcapd.202002251200 -o \"fmt:%td %sa %da %byt\" > data.csv
def bill(Q):
    X = (Q - 200) + 200 * k
    return X

df = pd.read_csv('data_t.csv', skiprows = 1, header = None)
df.columns = ['ts', 'dur', 'srcIP', 'dstIP', 'bytes']

#in_trf = (df[df.dstIP == ip].bytes.sum())
#in_trf = int(in_trf) / 2 ** 20

in_trf = (df[df.dstIP == ip].bytes.values.astype(int))
in_trf = np.sum(in_trf)
in_trf = in_trf / 2 ** 10

out_trf = (df[df.srcIP == ip].bytes.values.astype(int))
out_trf = np.sum(out_trf)
out_trf = out_trf / 2 ** 10

trf = out_trf + in_trf

connection_calc_src = df[df.srcIP == ip].bytes.count()
connection_calc_dst = df[df.dstIP == ip].bytes.count()
connection_calc = connection_calc_src + connection_calc_dst

print(f'Количество соединений с {ip} = {connection_calc}. В том числе
{connection_calc_dst} входящих и {connection_calc_src} исходящих')
print(f'Счет составил {bill(trf):.2f} руб. за {trf:.2f} КБ')

```

## Файл graph2.py

```

import pandas as pd
import matplotlib.pyplot as plt

df = pd.read_csv('data_t.csv', skiprows = 1, header = None)
df.columns = ['ts', 'dur', 'srcIP', 'dstIP', 'bytes']

df.bytes = df.bytes.apply(lambda row: int(row) if 'M' not in row else
(int(float(row[:-1])*10**6)))

ts = df.ts.apply(lambda row: row[:15])

df.ts = pd.to_datetime(ts, format='%Y-%m-%dH:%M')

df.plot(x='ts', y='bytes')
plt.title('График зависимости объема трафика от времени')
plt.ylabel('Количество байт')
plt.xlabel('Время')
plt.show()

```

## Вывод программ:

main.py

```
Количество соединений с 192.0.73.2 = 32. В том числе 16 входящих и 16 исходящих  
Счет составил 80.39 руб. за 180.39 КБ
```

graph2.py



## Выводы:

В данной Лабораторной работе были изучены технологии работы протокола NetFlow, а также разработан и реализован программный модуль обработки трафика NetFlow v5 и тарификации абонента с указанным IP-адресом.