Министерство НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Национальный исследовательский университет ИТМО

**факультет безопасности информационных технологий**

**Управление мобильными устройствами**

Лабораторная работа №2

«Обработка и тарификация трафика NetFlow»

Вариант№15

Работу выполнил:

Студент группы №3352   
Невесенко В. Н. \_\_\_\_\_\_\_\_\_

Работу 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.

**Описание выбранных средств реализации и обоснования выбора:**

Разработанный мною программный модуль был реализован на языке Python с использованием библиотеки обработки и анализа данных Pandas. Выбор данного языка программирования обусловлен крайне низким порогом вхождения, очень широким функционалом ввиду его «популярности» и очень динамично развивающегося сообщества, которое разрабатывает множество библиотек и модулей, а также издает множество обучающих материалов для повышения уровня владения данным языком программирования.

Библиотека Pandas выбрана, прежде всего, из-за внушительного функционала, связанного с обработкой данных. Данная библиотека позволяет оптимизировать код ввиду своих возможностей, позволяя реализовать одни и те же функции вводом значительно меньшего количества команд. Также данная библиотека позволяет добиваться высокой производительности от программы ввиду особенностей своего написания.

Также для построения и удобной реализации графиков мною были выбраны пакеты из библиотеки matplotlib – pyplot и dates. Первый нужен для непосредственно построения графика зависимости, а второй нужен для удобства отображения дат.

Для удобной обработки дампа NetFlow мною был выбран пакет numpy, для реализации перевода «сырого» дампа в файл .csv (для удобства его дальнейшей обработки), мною была задействована функция os, благодаря которой я смог реализовать выполнение терминальной команды *nfdump -r nfcapd.202002251200 -o \"fmt:%ts,%sa,%da,%ibyt,%obyt\" | sed \"s/ //g\" | ghead -n -4 > data.csv*

**Исходный код:**

Для оптимизации и разделения функций, были созданы три отдельных программных модуля - obrab.py, tarif.py, graphs.py. Как можно догадаться из названия, первый отвечает за обработку дампа Netflow, а также в нем реализованы функции, необходимые для дальнейшей работы, tarif.py необходим для произведения вычислений по тарификации, а последний же файл выводит график зависимости объема трафика от времени. Листинг всех программных модулей представлен ниже:

Файл obrab.py

Изображение выглядит как снимок экрана

Автоматически созданное описание

Файл tarif.py

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

Файл graphs.py

Изображение выглядит как снимок экрана, рисунок

Автоматически созданное описание

**Вывод программы:**

Так как объем трафика был маленький, то тарификация шла по коэффициенту 1,5 рубля за КИЛОБАЙТ. Вывод подсчета тарификации приведен ниже.

Изображение выглядит как текст, черный, белый

Автоматически созданное описание

Вывод зависимости представлен ниже:

Изображение выглядит как текст, карта

Автоматически созданное описание

Исходя из полученных данных можно проследить наиболее и наименее активное время течения трафика, следовательно, можно сделать вывод, что данный график является достаточно информативным

**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.