МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К КУРСОВОЙ РАБОТЕ

по дисциплине «Безопасность операционных систем»

для направления (специальности) 10.05.03 информационная безопасность автоматизированных систем

на тему

Вывод всех сокетов определенного процесса

Факультет «Информатики и вычислительной техники»

Кафедра «Информационная безопасность»

Руководитель,

Ст. преподаватель кафедры ИБ\_\_\_\_\_\_\_\_\_\_А.А. Кречетов

Исполнитель,

студент группы БИс-41 \_\_\_\_\_\_\_\_\_\_\_\_ С.Б. Константинов

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2017

Год

Содержание

[1.1. Постановка задачи 3](#_Toc500805049)

[1.2. Описание алгоритма программы 3](#_Toc500805050)

[1.3. Описание интерфейса программы 4](#_Toc500805051)

[1.4. Описание структуры программы 7](#_Toc500805052)

[1.4.1. Описание структуры программы для Windows 7](#_Toc500805053)

[1.4.2. Описание структуры программы для Linux 8](#_Toc500805054)

## Постановка задачи

* Задача - вывести информацию о сокетах определенного процесса.
* Операционная система - Windows и Linux.
* Язык реализации - С\С++.
* Входные данные - имя процесса.
* Выходные данные для программы на операционной системе семейства Windows - состояние сокета, локальный адрес и порт, удаленный адрес и порт, ID процесса, состояние.
* Выходные данные для программы на операционной системе семейства Linux – ID процесса, локальный адрес.
* Программа должна содержать информацию об авторе.

Исходный код программы должен находиться в папке bin.

Необходимо предоставить файл readme. В нем необходимо написать справочный материал к программе и информацию об авторе.

## Описание алгоритма программы

Программа получает имя процесса, находит его PID и по нему

выводит информацию о всех открытых сокетах этого процесса.

В информацию о сокетах входит:

* PID- ID процесса
* Локальный адрес
* Локальный порт
* Удаленный адрес
* Удаленный порт
* Тип протокола
* Состояние сокета

## Описание интерфейса программы

Программы представлены в консольном виде.

В версии под под Linux в качестве первого параметра принимается имя процесса или команда "/?".

* "/?" - выводит имя автора программы и назначение программы
* “ProcessName” – выводит информацию о процессе.

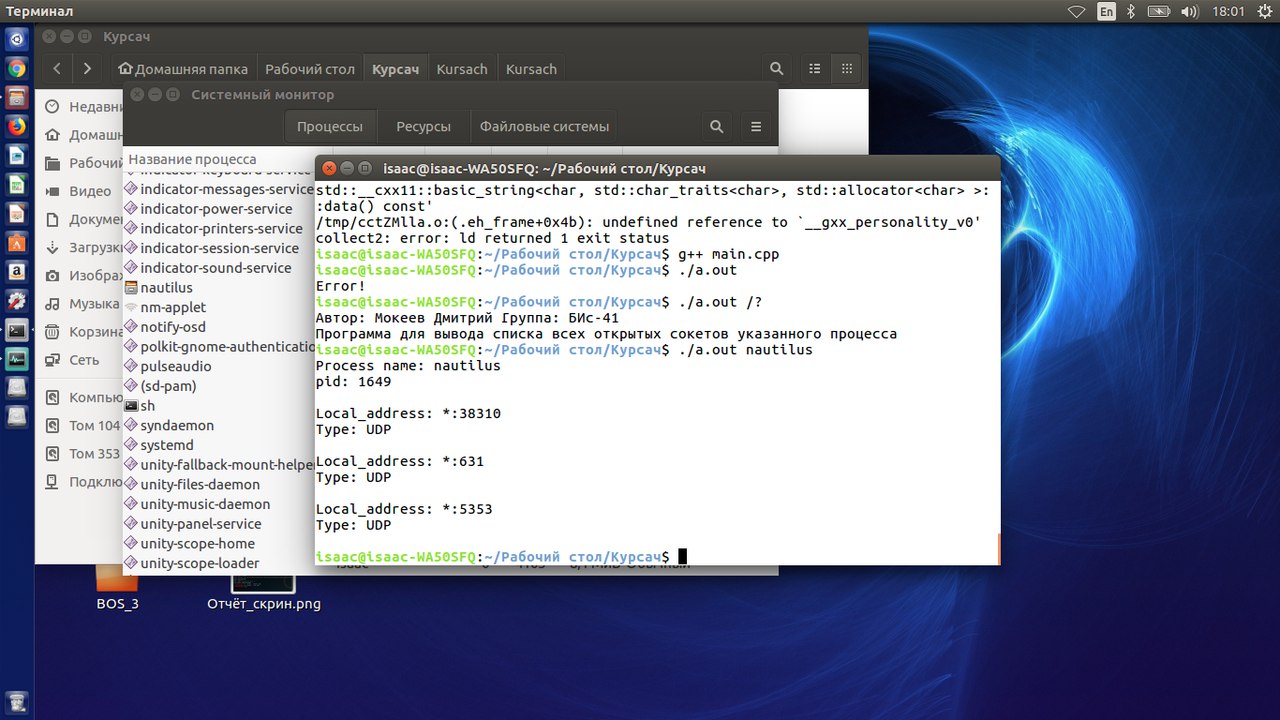
[](https://vk.com/photo208723149_456239506)

Рисунок 1 Демонстрация работы программы под Linux

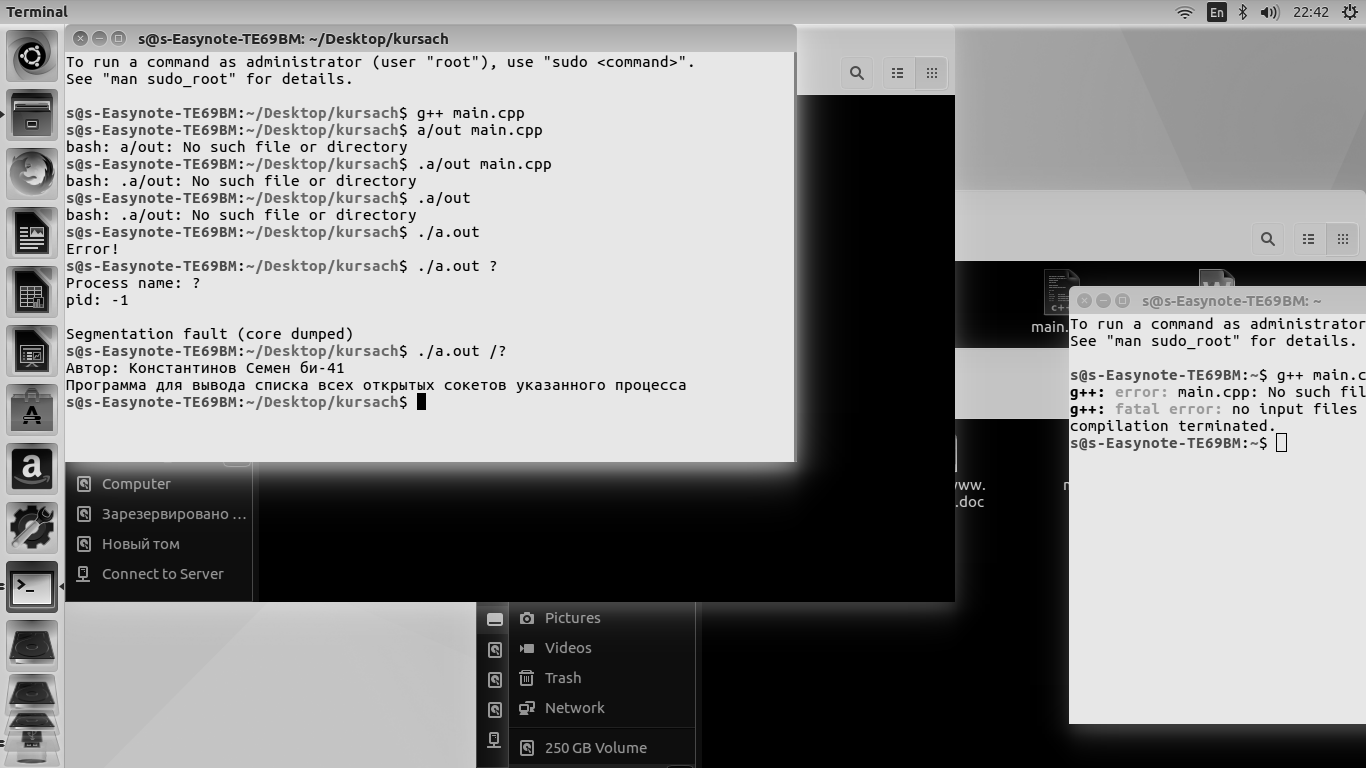


Рисунок 2 Интерфейс работы программы под Linux

Программа ищет информацию в файлах UDP и TCP по пути /proc/PID/net/udp или /proc/PID/net/tcp, где PID- ID процесса. ID процесса получаем при помощи функции int getProcIdByName(string procName)

Используется библиотека dirent.h для обеспечения совместимости с Unix-системами.

В версии под под Windows не принимается входных параметров. Все команды задаются внутри программы.

1 – команда вывода всех открытых сокетов указанного процесса.

2 – справка (Назначение программы и имя автора).

Esc – выход из программы.

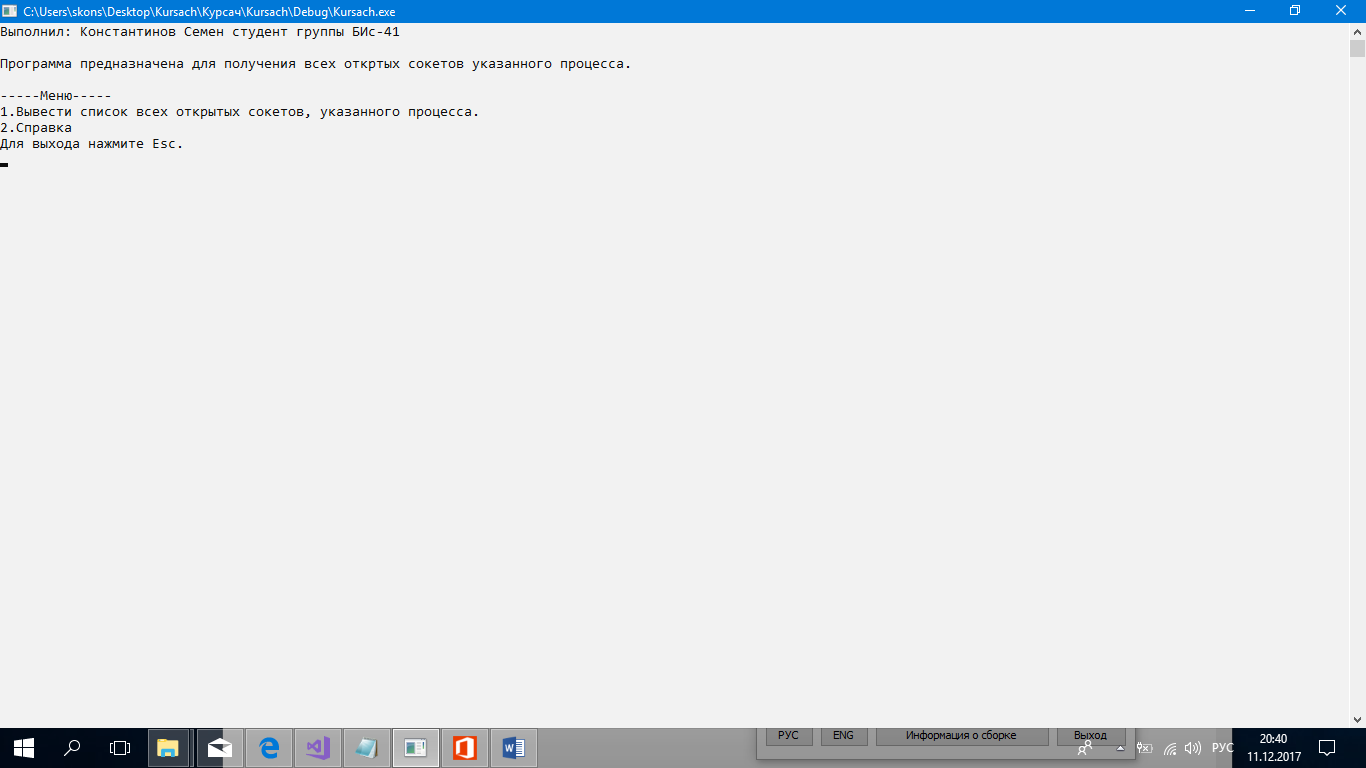


Рисунок 3 Интерфейс программы

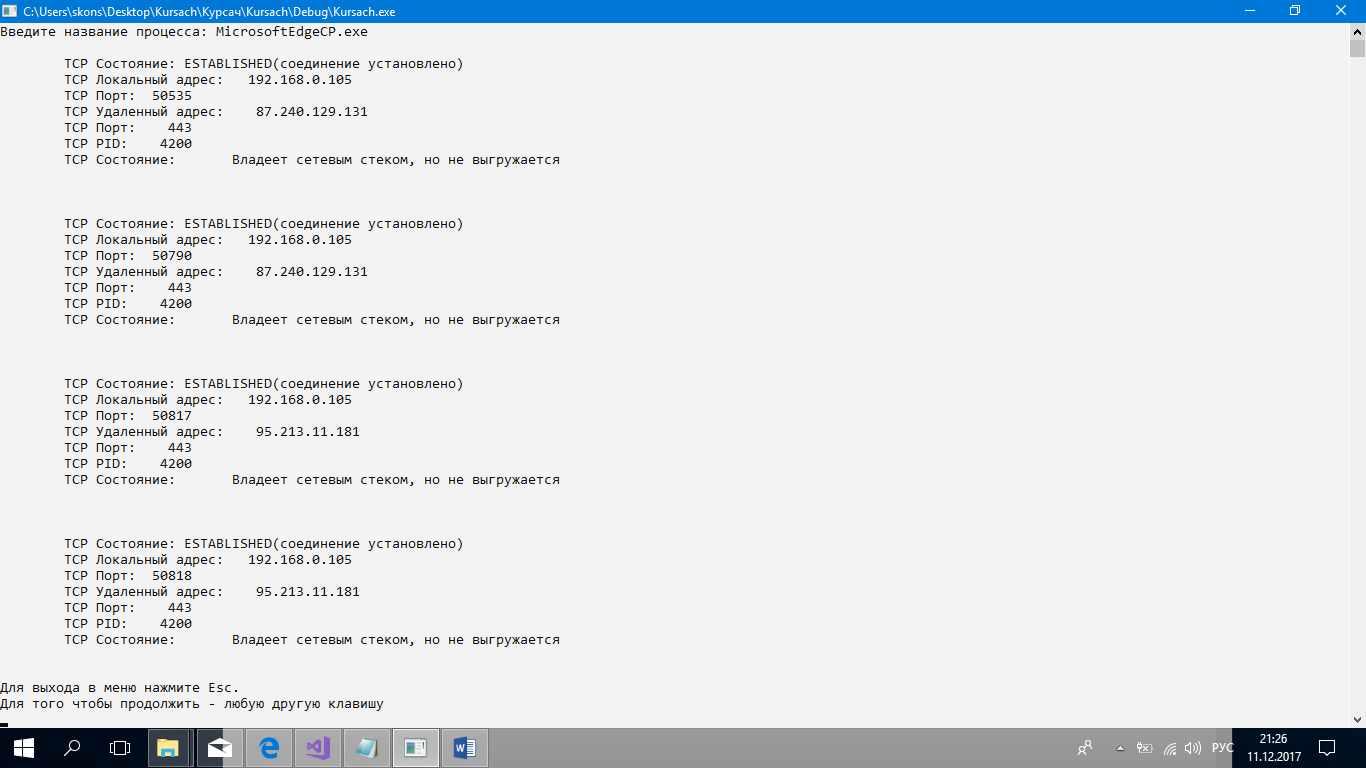


Рисунок 4 Описание интерфейса. Вывод сокетов процесса MicrosoftEdgeCP.exe

Используется библиотеки WinAPI, iphlpapi.lib, ws2\_32.lib; и заголовочные файлы tlhelp32.h, iphlpapi.h.

Программа получает имя процесса, находит его PID и при помощи функций библиотек TlHelp32.h и iphlpapi.h выводит информацию о сокетах указанного процесса.

## Описание структуры программы

## Описание структуры программы для Windows

HANDLE snapshot =CreateToolhelp32Snapshot (TH32CS\_SNAPPROCESS, 0)-cоздает снапшот запущенных процессов, модулей, нитей итд.

Process32First (snapshot, &process) - [Process32First](http://msdn.microsoft.com/en-us/library/windows/desktop/ms684834(v=vs.85).aspx) принимает хэндл, полученный от CreateToolhelp32Snapshot, вызванной с dwFlags = TH32CS\_SNAPPROCESS, а также указатель на структуру [PROCESSENTRY32](http://msdn.microsoft.com/en-us/library/windows/desktop/ms684839(v=vs.85).aspx).

Sockets(process.th32ProcessID)- принимает PID процесса.

GetTcpTable2(pTcpTable, &ulSize, TRUE))- получает ipv4 протоколы таблицы соединений.

switch (pTcpTable->table[i].dwState)- поиск состояния соеденения

Возможные состояния соедения

MIB\_TCP\_STATE\_CLOSED:

MIB\_TCP\_STATE\_LISTEN:

MIB\_TCP\_STATE\_SYN\_SENT:

MIB\_TCP\_STATE\_SYN\_RCVD:

MIB\_TCP\_STATE\_ESTAB:

MIB\_TCP\_STATE\_FIN\_WAIT1:

MIB\_TCP\_STATE\_FIN\_WAIT2:

MIB\_TCP\_STATE\_CLOSE\_WAIT:

MIB\_TCP\_STATE\_CLOSING:

MIB\_TCP\_STATE\_LAST\_ACK:

MIB\_TCP\_STATE\_TIME\_WAIT:

MIB\_TCP\_STATE\_DELETE\_TCB

## Описание структуры программы для Linux

Strcpy- при помощи этой функции выстраивается путь в /proc/PID/net/udp и /proc/PID/net/tcp в файловой системе Linux.

int HEX\_TO\_DEC(char st[10]) - переводит информации из 16-ричной системы счисления в 10-ричную

int getProcIdByName(string procName)-возвращает PID процесса, dirent используется для работы в Unix системах