|  |
| --- |
| **МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ** |
| **ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ** |
| **УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ** |
| **«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»** |
|  |
| Институт информационных технологий и управления в технических системах |
| (полное название института) |
|  |
| кафедра «Информационные системы» |
| (полное название кафедры) |

**ОТЧЁТ**

по лабораторной работе №7

на тему«выявление присутствия на компьютере вредоносных программ»

по дисциплине **«**Операционные системы»

Выполнил

студент ИИТУТС

группы ИС/б-18-2-о

Радыгина Екатерина

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | | | | | | | |
|  | (должность, учёная степень преподавателя) | | | | | | | | |
|  |  | | | | | | | | |
|  | (ФИО преподавателя) | | | | | | | | |
|  | « |  | » |  |  |  | 20 | 20 | г. |
|  |  | | | | | | | | |
|  | (оценка) | | | | | | | | |
|  |  | | | | | | | | |
|  |  | | | | | | | | |

Севастополь 2020

**7.1 Цель работы**

Получить практические навыки по выявлению вредоносных программ на локальном компьютере под управлением ОС Windows.

**7.2 Ход работы**

7.2.1. Отслеживание подозрительных процессов. Откроем Диспетчер задач и отсортируем процессы по использованию ресурсов процессора (рисунок 7.1).

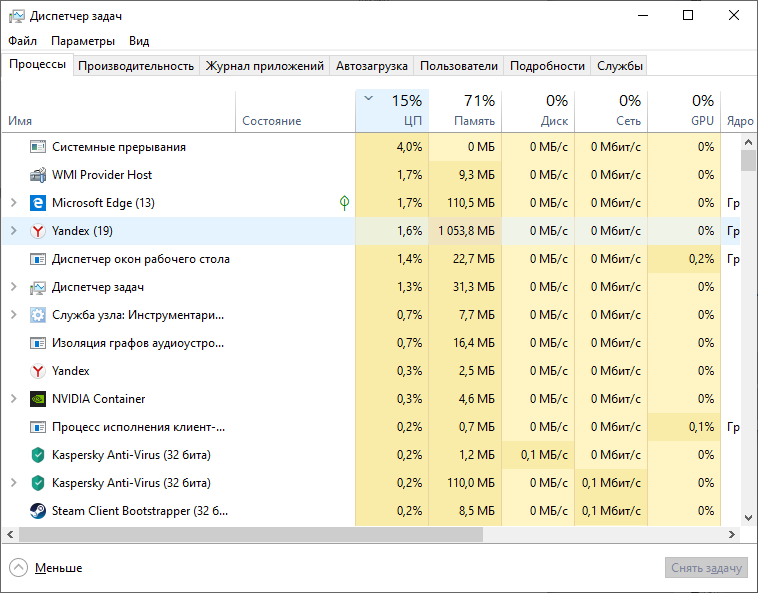


Рисунок 7.1 – Окно Диспетчера задач

Откроем программу Paint и проследим за изменениями на закладке Приложения (рисунок 7.2).

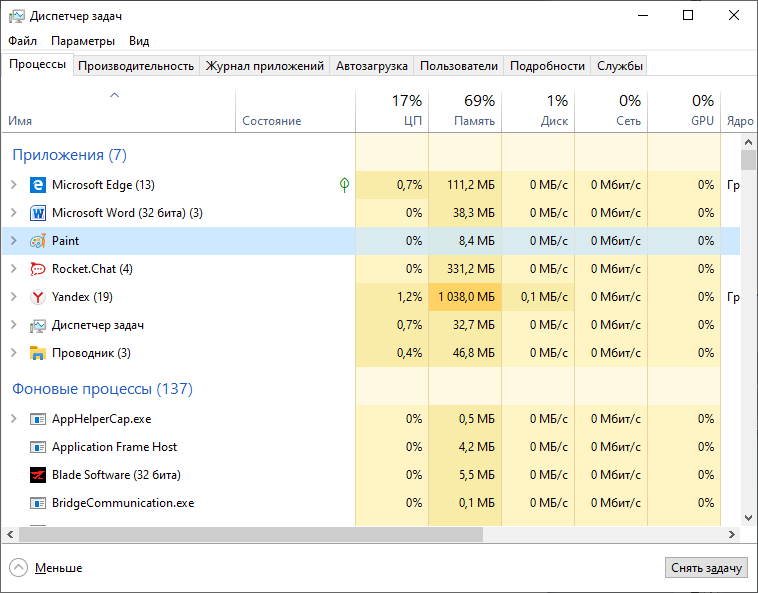


Рисунок 7.2 – Закладка Приложение

7.2.2 Элементы автозапуска. Откроем Автозагрузку (рисунок 7.3).

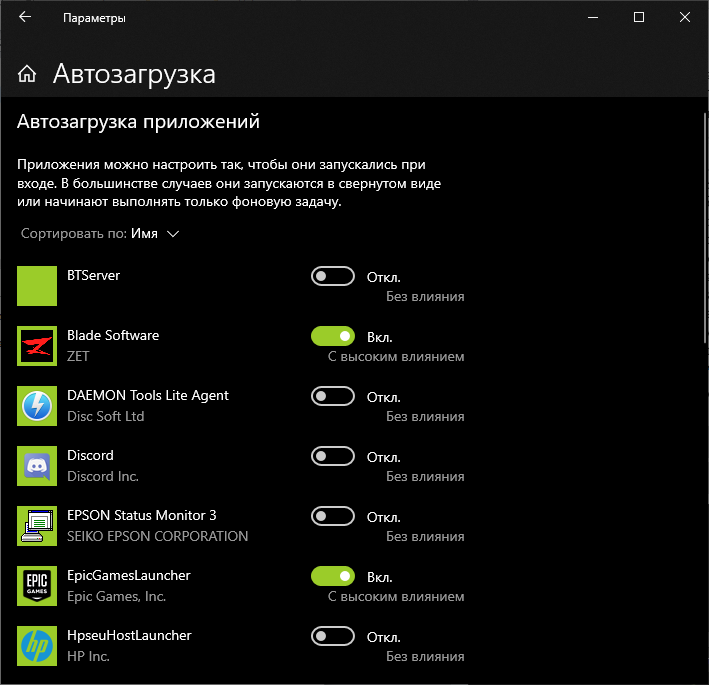


Рисунок 7.3 – Автозагрузка

Для большинства ситуаций, связанных с автозапуском, достаточно использовать системную утилиту Настройка системы. В окне Поиск набрем msconfig, в окне Программы выполним двойной щелчок по имени утилиты. Откроется окно (рис.7.4). На первой закладке, Общие, можно выбрать вариант запуска операционной системы.

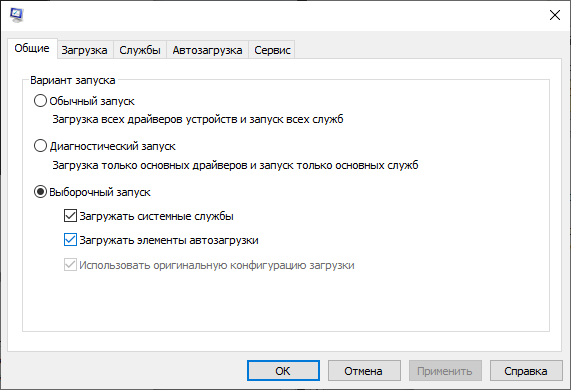


Рисунок 7.4 – Окно Настройка системы

Для открытия папки автозапуска нажимаем клавиши Win+R и вводим в окно «Выполнить» следующее: *shell:startup* после чего нажмем Ок, сразу откроется папка с ярлыками программ для автозапуска. Добавляем туда необходимые программы (рисунок 7.5).

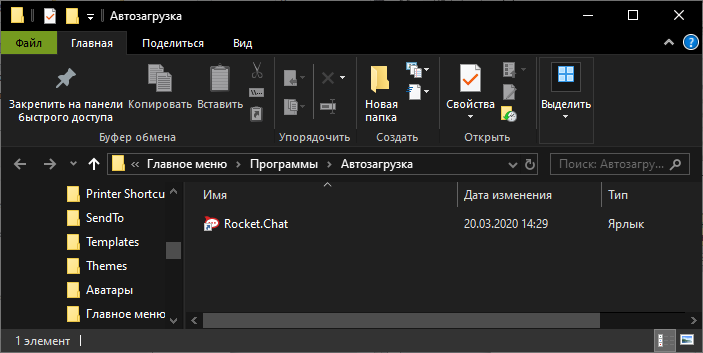


Рисунок 7.5 – Папка автозагрузки

7.2.3 Сетевая активность. Откроем окно Диспетчера задач Windows, нажав одновременно клавиши Ctrl, Shift и Esc, и перейдем к закладке Сеть (рисунок 7.6).

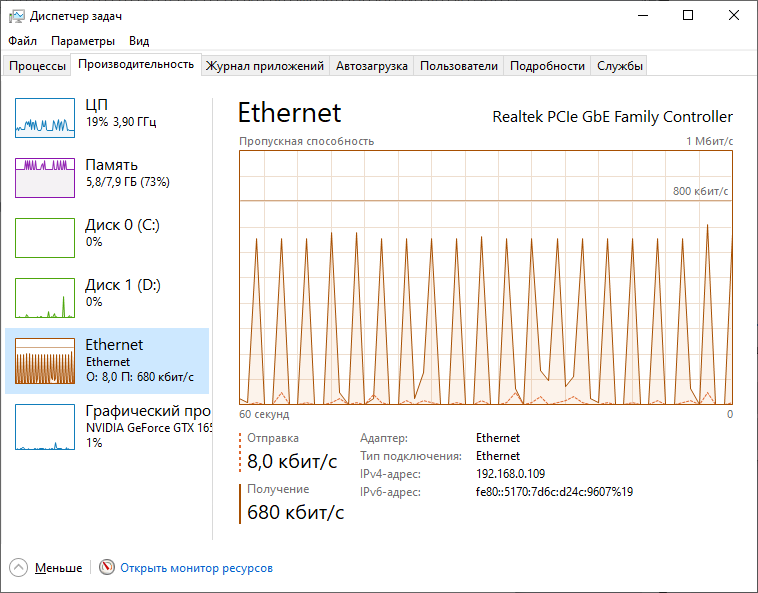


Рисунок 7.6 – Закладка Сеть

Для получения более подробных данных можно воспользоваться утилитой netstat. Закрыть окно Диспетчера задач Windows и перейти к системному меню Пуск/Программы/Стандартные/Командная строка. Набрать netstat /? и нажать Enter (рисунок 7.7).

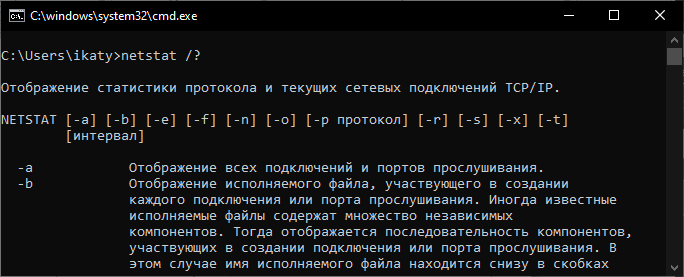


Рисунок 7.7 – Использование netstat

Введем netstat –a и нажмем Enter. Результатом выполнения команды является список активных подключений, в который входят установленные соединения и открытые порты (рисунок 7.8).

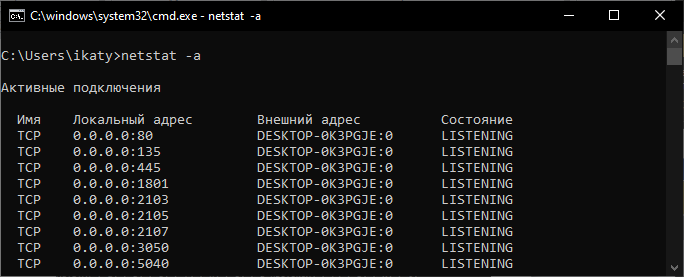


Рисунок 7.8 – Использование netstat –a

**Вывод**

В ходе лабораторной работы были получены практические навыки по выявлению вредоносных программ на локальном компьютере под управлением ОС Windows.