**Министерство науки и высшего образования Российской Федерации**

**ФГАОУ ВО «Севастопольский государственный университет»**

**Институт информационных технологий и управления в технических процессах**

**Отчёт**

ПО ЛАБОРАТОРНОЙ РАБОТЕ №7

«ВЫЯВЛЕНИЕ ПРИСУТСТВИЯ НА КОМЬЮТЕРЕ ВРЕДОНОСНЫХ ПРОГРАММ»

по дисциплине «Операционные системы»

Выполнил:

студент группы ПИ/б-18-1-о

Николенко Виктория

Проверил:

ст.пр. Шалимова Е.М.

Севастополь

2020

**7.1 Цель работы:** получить практические навыки по выявлению вредоносных программ на локальном компьютере под управлением ОС Windows .

**7.2 Порядок выполнения**

7.2.1 Отслеживание подозрительных процессов

7.2.2 Элементы автозапуска

7.2.3 Сетевая активность

**7.3 Ход работы**

7.3.1 Отслеживание подозрительных процессов

Перейдём к Диспетчеру задач Windows, нажав одновременно клавиши Ctrl, Shift и Esc. Отсортируем все процессы по использованию ресурсов процессора. Нажав на заголовок поля ЦП .В диспечере задач мы можем проследить различные процессы и при необходимости снять задачи.

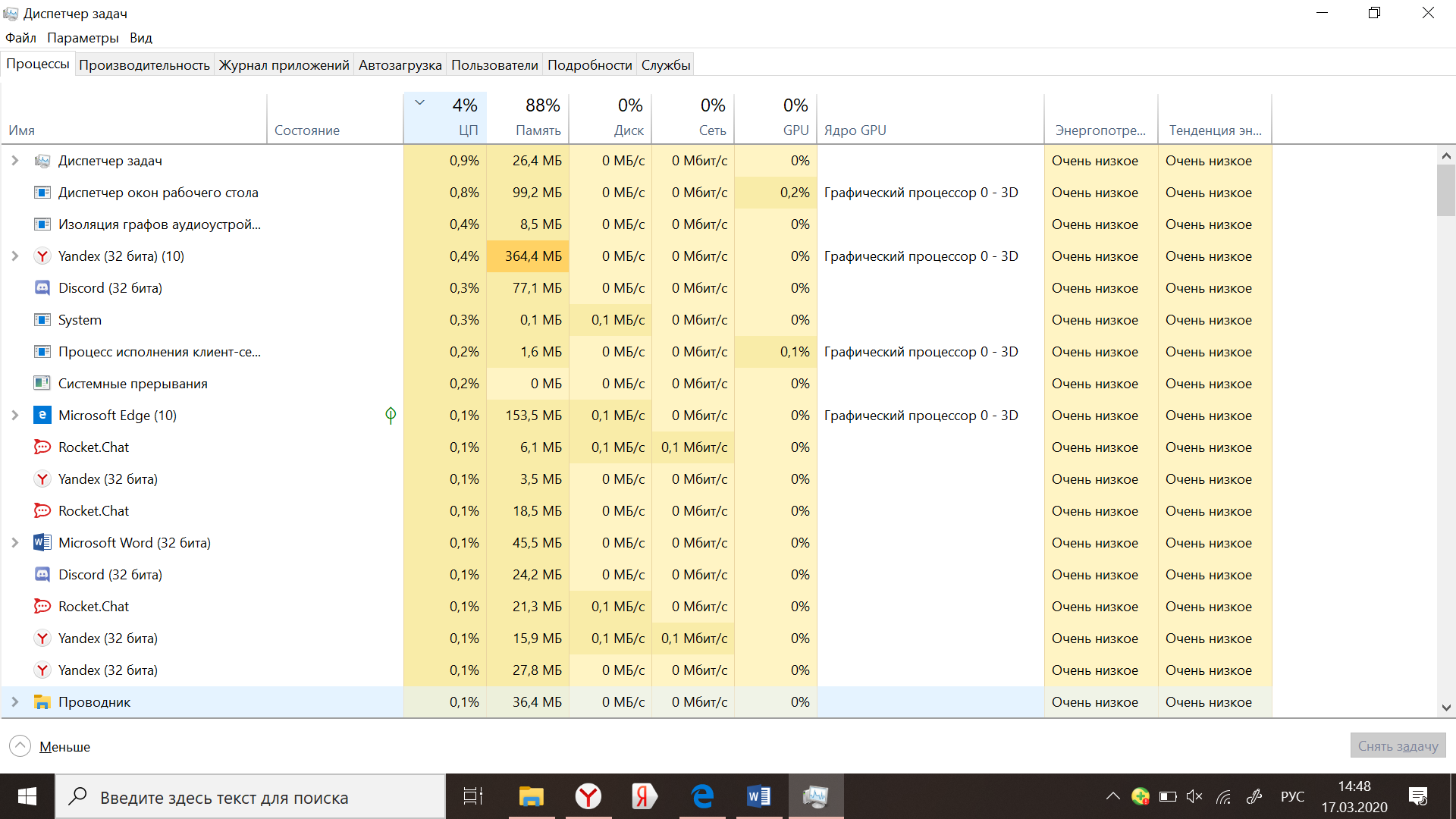


Рисунок 7.1 – Окно Диспетчера задач

7.3.2 Элементы автозапуска

Чтобы зайти а автозапуск нужно нажать : Пуск – Параметры – Приложения –Автозапуск

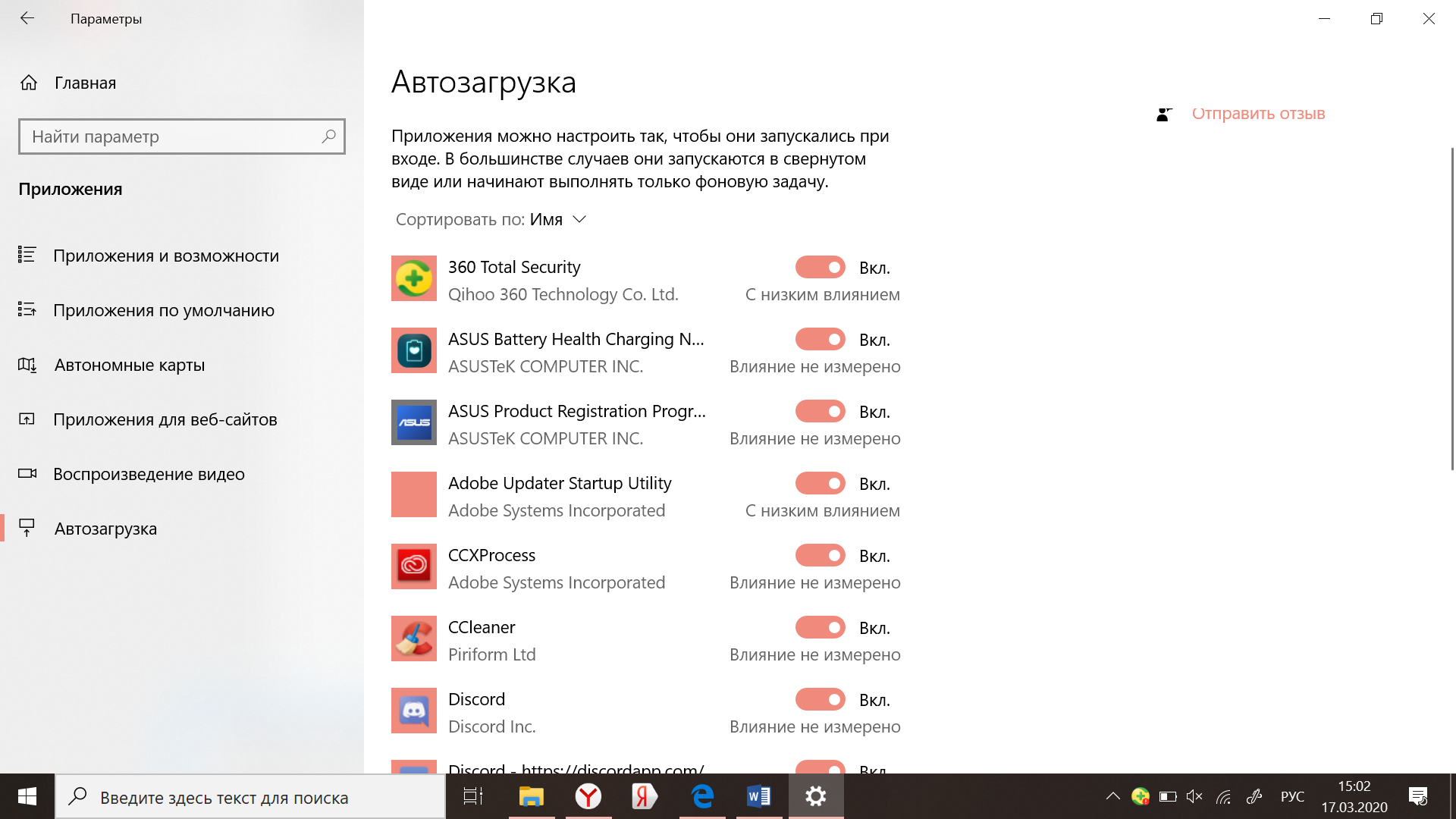


Рисунок 7.2 – Окно Автозапуска

Другой способ зайти в автозапуск это через системную утилиту Настройка системы. В окне Поиск набрать msconfig, в окне Программы выполнить двойной щелчок по имени утилиты. Откроется окно (рис.7.2). На первой закладке, Общие, можно выбрать вариант запуска операционной системы.

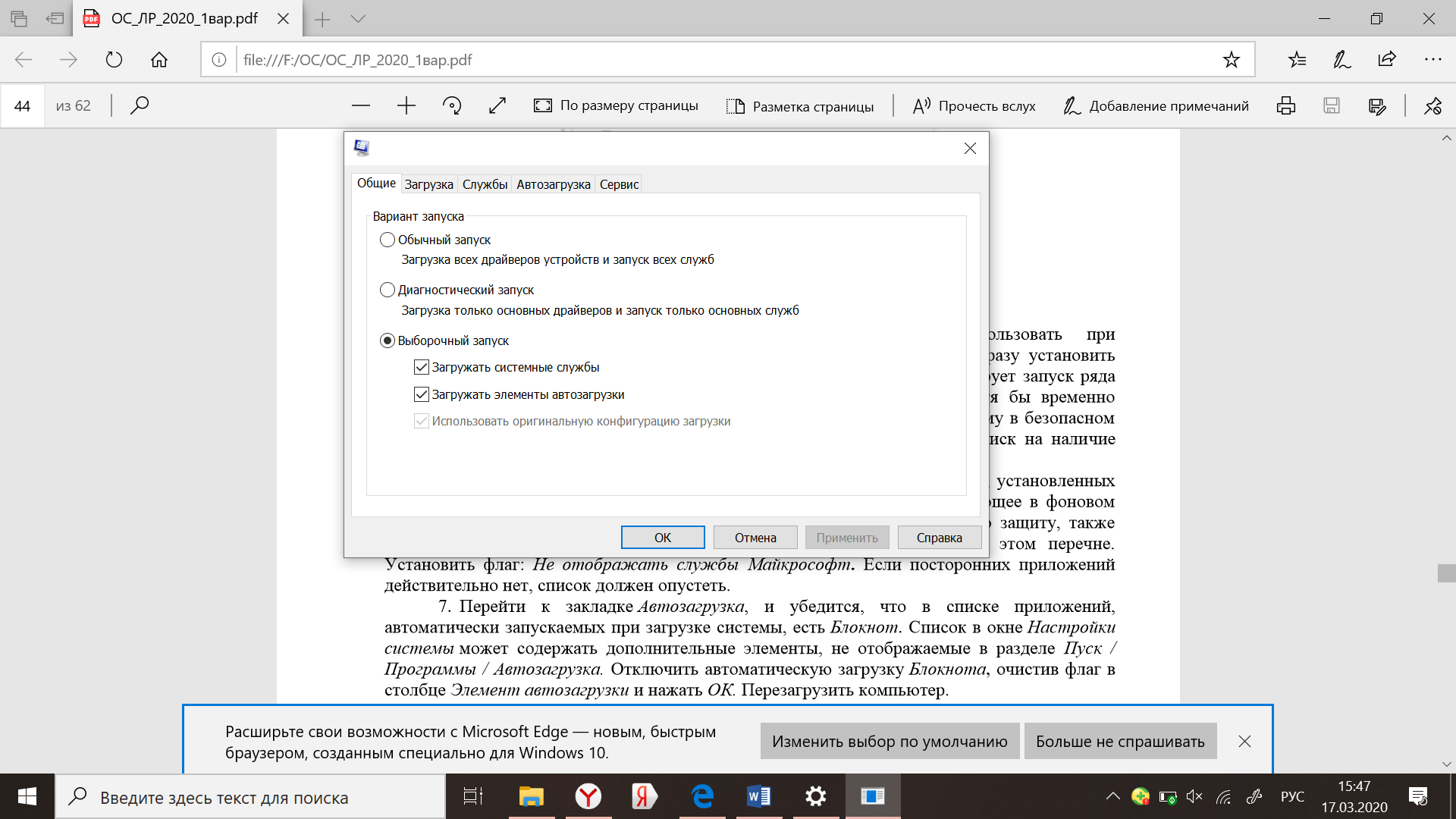


Рисунок 7.3 – Окно «Настройка системы»

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

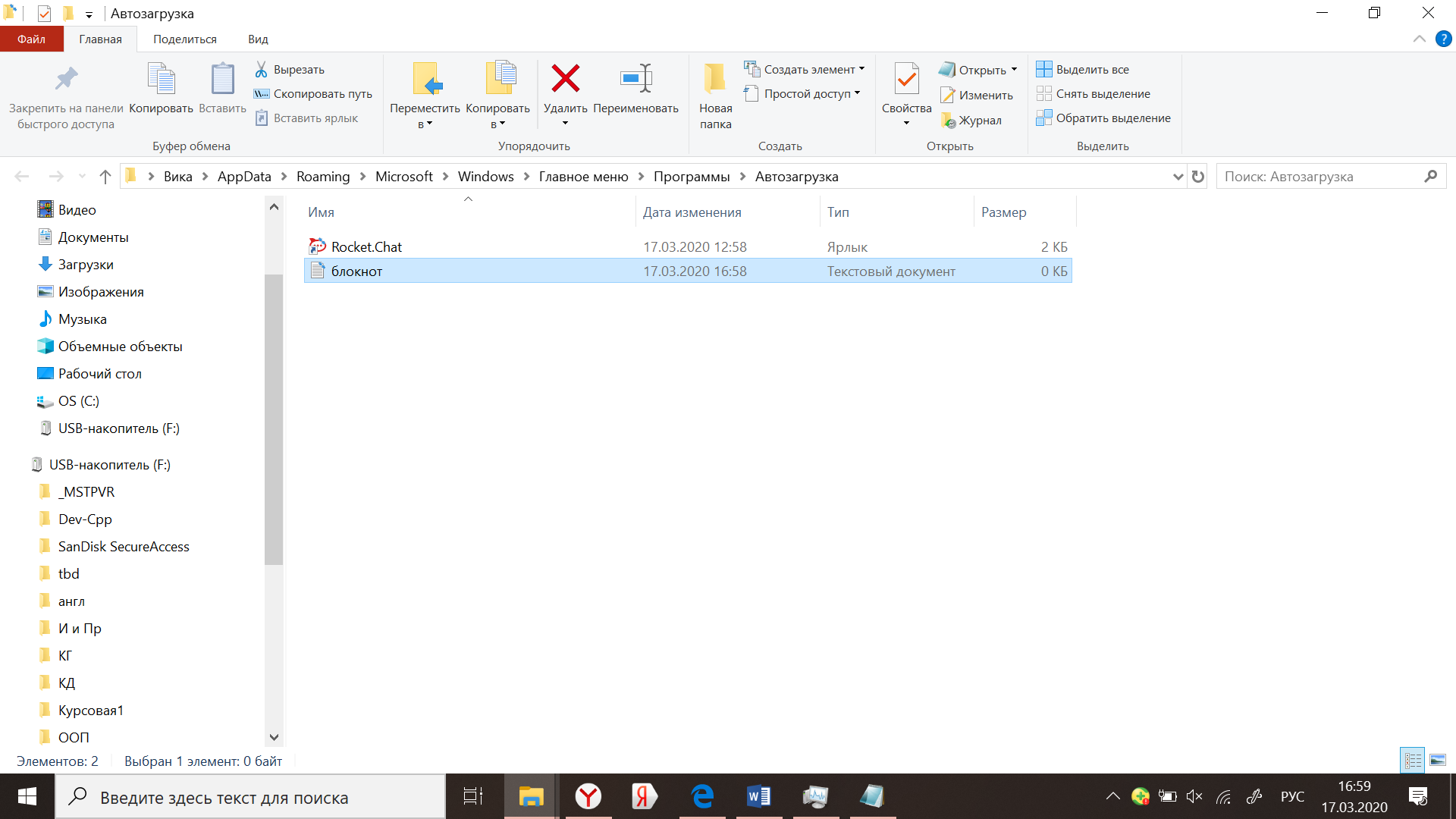


Рисунок 7.4 – Окно папки «Автозапуск»

7.3.3 Сетевая активность

Чтобы посмотреть сетевую активность необходимо зайти в Диспечер задач.Перейти во вкладку Производительность и выбрать Сеть.

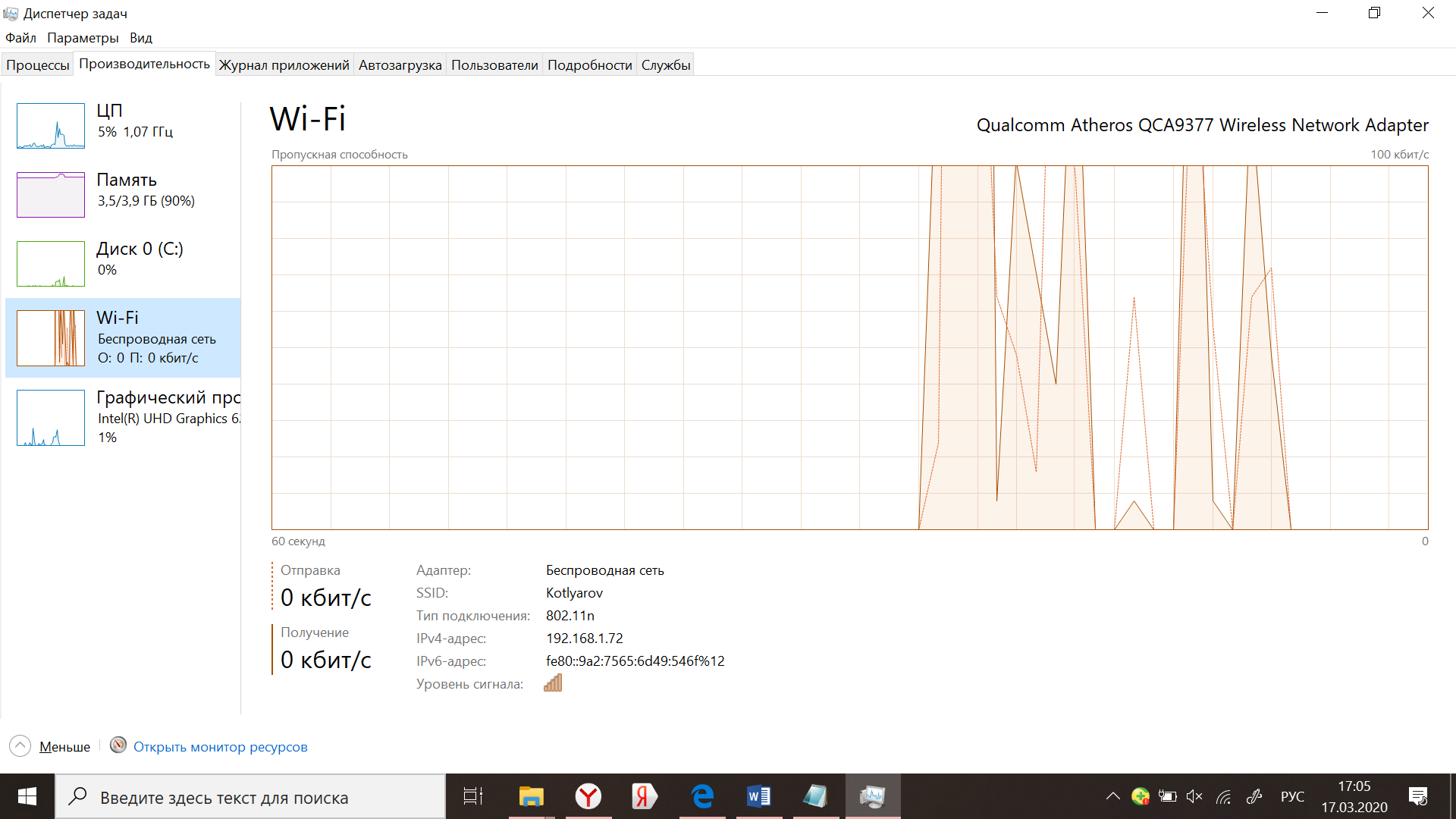


Рисунок 7.5 – Закладка «Сеть» диспетчера задач

Для получения более подробных данных можно воспользоваться утилитой netstat. Перейдём к системному меню Пуск / Программы / Стандартные / Командная строка. Наберём netstat /? и нажмём Enter.

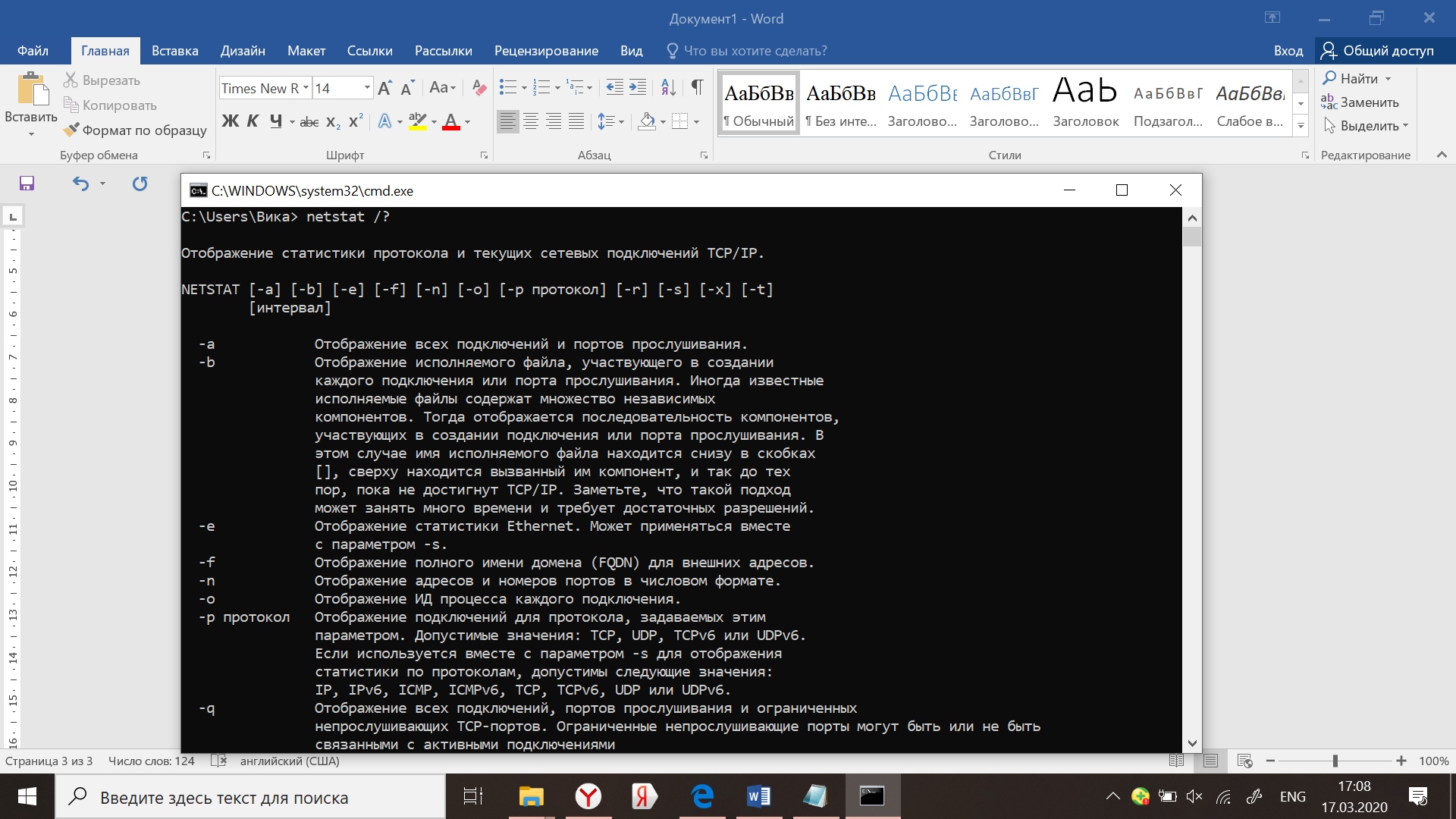


Рисунок 7.6 – Эмулятор MS DOS

**Вывод**

В ходе лабораторной работы были получены практические навыки по выявлению вредоносных программ на локальном компьютере под управлением ОС Windows . Более поробно исследована работа с Диспечером задач Windows.