

ВИЯВЛЕННЯ ВІДХИЛЕНЬ В РОБОТІ КОМП'ЮТЕРА

KEYLOGGER



MONITORING SOFTWARE

Харченко Євгеній Андрійович

АКТУАЛЬНІСТЬ: існують віруси, які не можна визначити антивірусами бо вони використовують обхідні шляхи для роботи з інформацією, тому потрібні нові методи виявлення активності вірусів.

МЕТА ДОСЛІДЖЕННЯ: створити програмне забезпечення, яке виявляло би за поведінкою системи ознаки роботи шкідливих програмних утиліт.

ОБ'ЄКТ: методи компрометації вірусів.

ПРЕДМЕТ ДОСЛІДЖЕННЯ: робота шкідливих програмних забезпечень та їх детекція

Наукові методи використані в дослідженні

- Аналіз принципу роботи шкідливих програмних забезпечень;
- Порівняння принципів роботи різних комп'ютерних вірусів;
- Узагальнення роботи вірусів;

ЗАВДАННЯ ДОСЛІДЖЕННЯ:

- 1) Розглянути загальні відомості про параметри комп'ютера за якими можна стежити .
- 2) Визначити метод, за яким можна відрізнити нормальний від нормального режиму роботи.
- 3) Реалізувати збір статистики режиму роботи.
- 4) Дослідити та реалізувати засобами машинного навчання детектор відхилення від норм.

ВИМІРЮВАННЯ ЗАВАНТАЖЕНОСТІ МЕРЕЖІ ТА ДИСКУ

- private static PerformanceCounter diskPerformance;
- public static void CreatePerformanceDiskCounter(){
- diskPerformance = new PerformanceCounter("Network",
- "% Disk Time", "_Total");
- }
- public static void Main(string[] args)
- {
- CreatePerformanceDiskCounter();
- for(int i=0; i<100; i++){
- Thread.Sleep(1000);
- Console.WriteLine("Disk usage: {0}",
- diskPerformance.NextValue());
- }
- }

ВИМІРЮВАННЯ ЗАВАНТАЖЕНОСТІ РАМ ТА CPU

Process p = get the desired process here;

```
PerformanceCounter ramCounter = new  
PerformanceCounter("Process", "Working Set",  
p.ProcessName);
```

```
PerformanceCounter cpuCounter = new  
PerformanceCounter("Process", "% Processor  
Time", p.ProcessName);
```

```
double ram = ramCounter.NextValue();
```

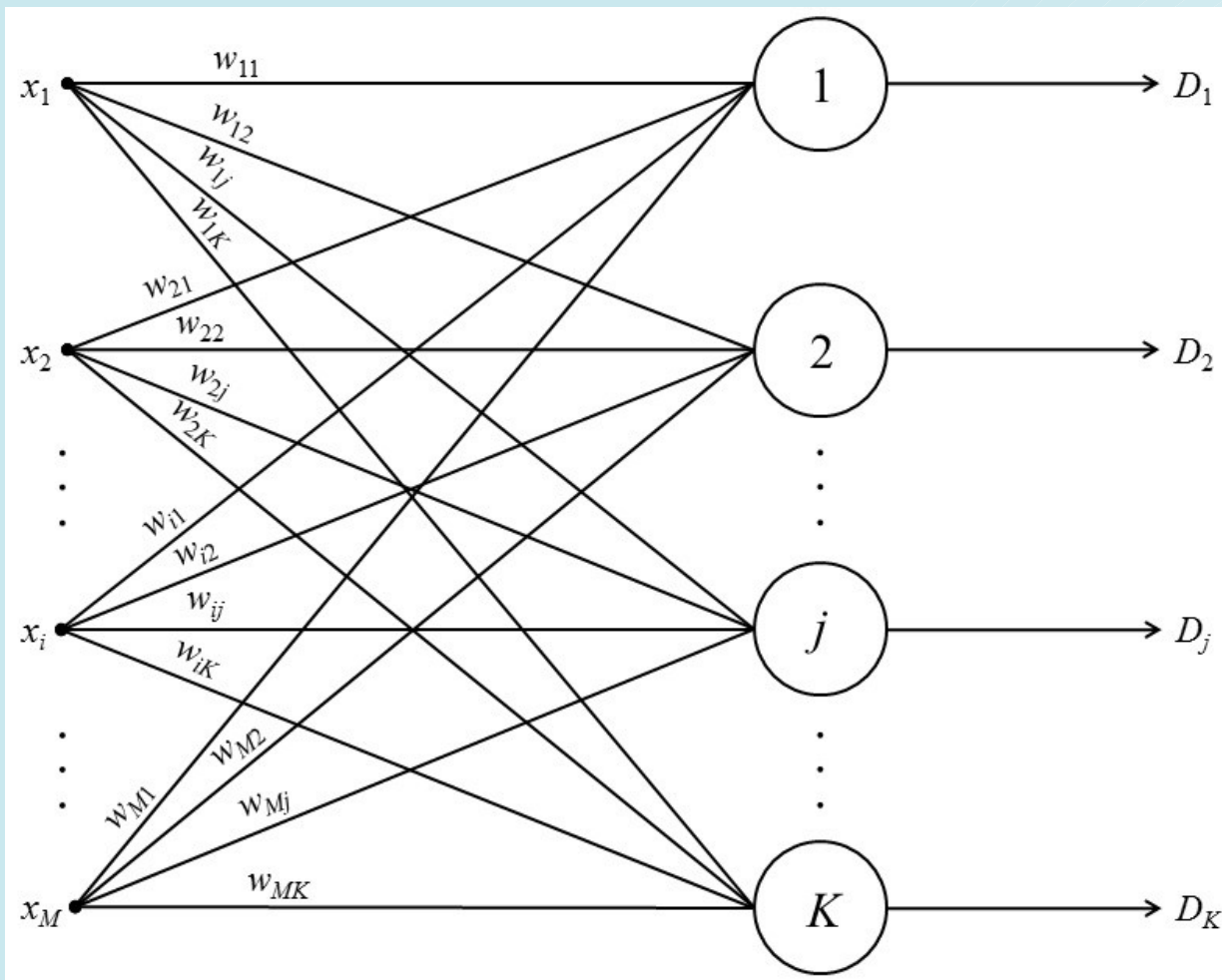
```
double cpu = cpuCounter.NextValue();
```

ВИМІРЮВАННЯ ТЕМПЕРАТУРИ ПРОЦЕСОРА

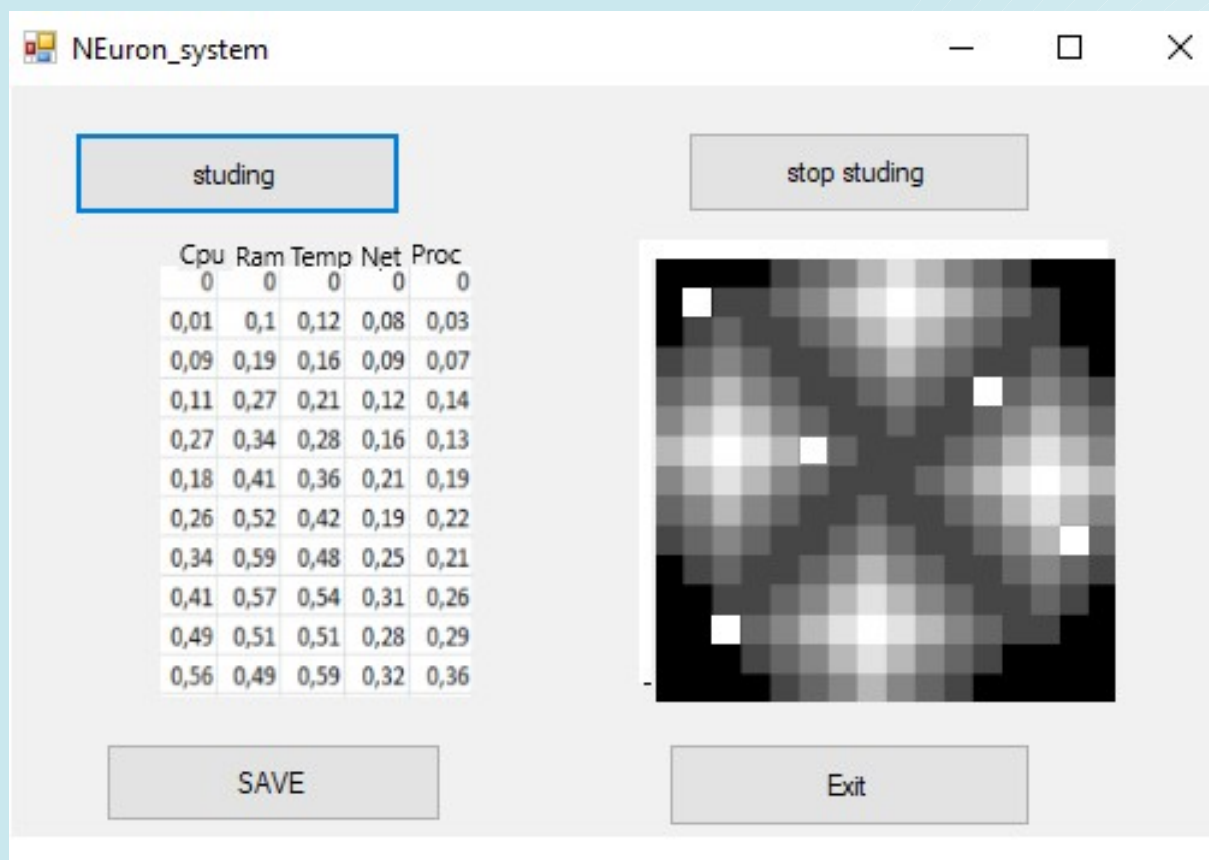
```
ManagementObjectSearcher searcher = new
ManagementObjectSearcher(@"root\WMI", "SELECT * FROM
MSAcpi_ThermalZoneTemperature");
foreach (ManagementObject obj in searcher.Get()) {
    double t, kelvin, celsius, farenheight;
    double.TryParse(obj["CurrentTemperature"].ToString(), out t);

    kelvin = t / 10;
        celsius = (t / 10) - 273.15;
        farenheight = ((t / 10) - 273.15) ;/ }
```

НЕЙРОННА МЕРЕЖА КОХОХЕНА



ІЛЮСТРАЦІЯ РОБОТИ ПРОГРАМИ



ВИСНОВКИ:

- 1) Розглянуто загальні відомості про параметри комп'ютера за якими можна стежити . В результаті, віділено параметри: завантаженність процесору, диску мережі, температура процесора і реалізовано збір цих параметрів один раз за сек на мові с#.
- 2) Для виявлення аномалій даних було обрано мережу Кохонена.
- 3) Розроблено алгоритми застосування мережі Кохонена для даних, які характеризують роботу компютера
- 4) Розроблений зовнішній вигляд та порядок роботи програми детектору відхилення від норм

ВИЯВЛЕННЯ ВІДХИЛЕНЬ В РОБОТІ КОМП'ЮТЕРА

KEYLOGGER



MONITORING SOFTWARE

Харченко Євгеній Андрійович