КІРОВОГРАДСЬКА
МАЛА АКАДЕМІЯ НАУК
УЧНІВСЬКОЇ МОЛОДІ

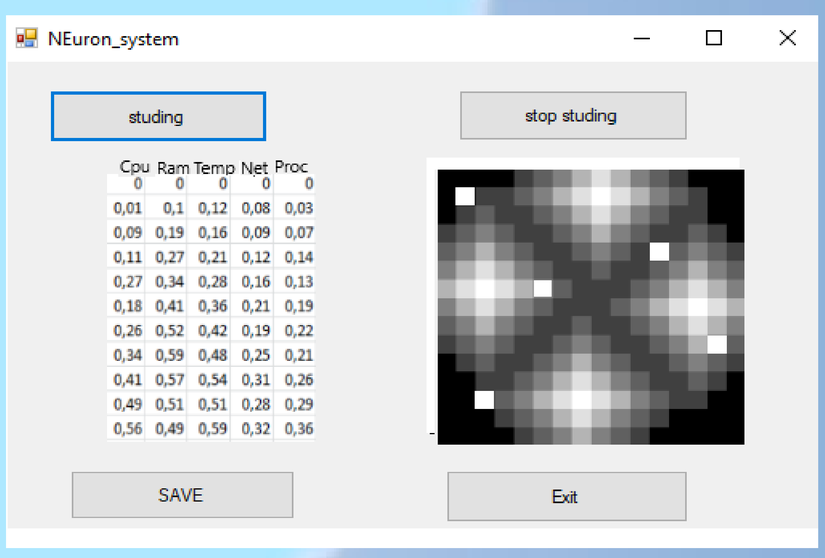
ВИЯВЛЕННЯ ВІДХИЛЕНЬ В РОБОТІ КОМП'ЮТЕРА

ХАРЧЕНКО ЄВГЕНІЙ АНДРІЙОВИЧ, 11 клас, комунальний заклад «Центральноукраїнський науковий ліцей-інтернат Кіровоградської обласної ради», місто Кропивницький.
Наукові керівники: ДРЄЄВ ОЛЕКСАНДР МИКОЛАЙОВИЧ, доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, кандидат технічних наук;
СВИРИДЕНКО ОЛЕНА ЛЕОНІДІВНА, вчитель математики комунального закладу «Центральноукраїнський науковий ліцей-інтернат Кіровоградської обласної ради», місто Кропивницький.

МЕТА: створити програмне забезпечення, яке виявляло би за поведінкою системи ознаки роботи шкідливих програм.
ОБ'ЄКТ: процеси в роботі комп'ютера.
ПРЕДМЕТ: алгоритми виділення нестандартних режимів роботи системи.
ЗАВДАННЯ: розглянути загальні відомості про параметри комп'ютера за якими можна стежити; визначити метод, за яким можна відрізнити аномальний від нормального режиму роботи; реалізувати збір статистики показників роботи; дослідити та реалізувати засобами машинного навчання детектор відхилення від норм.

ВИКОРИСТАНІ МЕТОДИ: аналіз принципу роботи шкідливих програмних забезпечень; порівняння принципів роботи різних комп'ютерних вірусів; узагальнення роботи вірусів; комп'ютерне навчання для запам'ятовування показників штатної роботи

ХІД РОБОТИ: мережа запам'ятовує нормальні режими роботи, які підсвічено на контрольному зображенні. Вихід за зону звичної роботи свідчить про короткочасні процеси або про наявність сторонніх чинників, яких раніше не було. На практиці легко визначалися сайти, які завантажували систему.



Зовнішній вигляд програмного забезпечення

ВИСНОВКИ: розглянуто загальні відомості про параметри комп'ютера за якими можна стежити. В результаті виділено параметри: завантаженість процесору, диску мережі, температура процесора і реалізовано збір цих параметрів один раз за сек на мові c#. Розроблено алгоритми застосування мережі Кохонена для даних, які характеризують роботу комп'ютера. Розроблена програма детектору відхилення від нормальних режимів роботи.