Засоби для моніторингу безпеки комп’ютерних систем на основі нейронних мереж

ВИКОНАВ: ГЛАГОЛЄВ ОЛЕКСІЙ, КА-45, ІПСА

НАУК.КЕРІВНИК:ПРОФЕСОР, Д.Т.Н.,
МУХІН ВАДИМ ЄВГЕНОВИЧ

Актуальність роботи:

- З появою поняття «кібер-злочинності», виникла потреба захисту комп'ютерних систем.
- Виявлення підозрілої активності в системі дає можливість захистити її та протидіяти зловмиснику.
- Нейронна мережа може ефективно опрацьовувати статистичні дані, а також навчитись виявляти аномалії.

Існуючі програмні продукти та їх недоліки

- Zabbix – програма, що здійснює моніторинг пристроїв і їх компонентів в КС
- Nagios – здійснює моніторинг компонентів КС, запис лог-файлів
- Cacti – має зрозумілий та простий інтерфейс, висока швидкість роботи

Постановка задачі:

- Визначити дані про стан комп’ютерної системи (вектор стану), які буде враховувати програмний засіб при перевірці системи
- Обрати нейронну мережу, та навчити її за допомогою вибірки обраних даних для моніторингу, оптимізувати її роботу
- Розробити програмний продукт, який буде дозволить користувачу працювати з навченою нейронною мережею для виявлення потенційних небезпек на основі вхідних даних з векторами стану системи

Мета дослідження:

РОЗРОБКА ЗАСОБУ ДЛЯ МОНІТОРИНГУ БЕЗПЕКИ КОМП’ЮТЕРНИХ СИСТЕМ. ВИБІР ТА НАЛАШТУВАННЯ НЕЙРОННОЇ МЕРЕЖІ, ЗА ДОПОМОГОЮ ЯКОЇ БУДУТЬ ПРИЙМАТИСЬ РІШЕННЯ

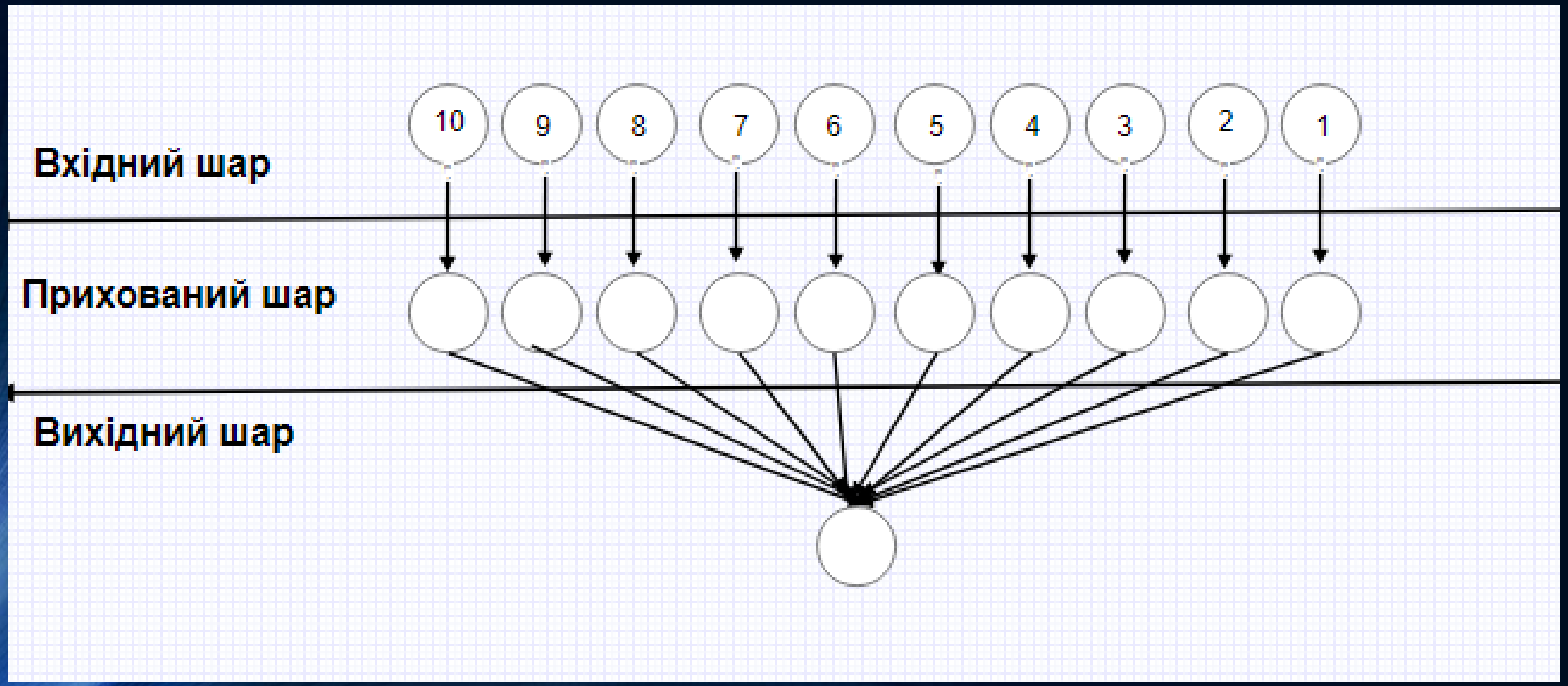
Об’єкт дослідження:

МЕТОДИ ВИЯВЛЕННЯ НЕБЕЗПЕКИ В КОМП’ЮТЕРНІЙ МЕРЕЖІ

Предмет дослідження:

ЗАСТОСУВАННЯ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ МОНІТОРИНГУ БЕЗПЕКИ КОМП’ЮТЕРНОЇ СИСТЕМИ

Архітектура нейронної мережі:



Вибір елементів для моніторингу

Вектор стану КС – це вектор, кожна координата якого є показником стану визначеного компонента КС, чи виконанням дії в КС:

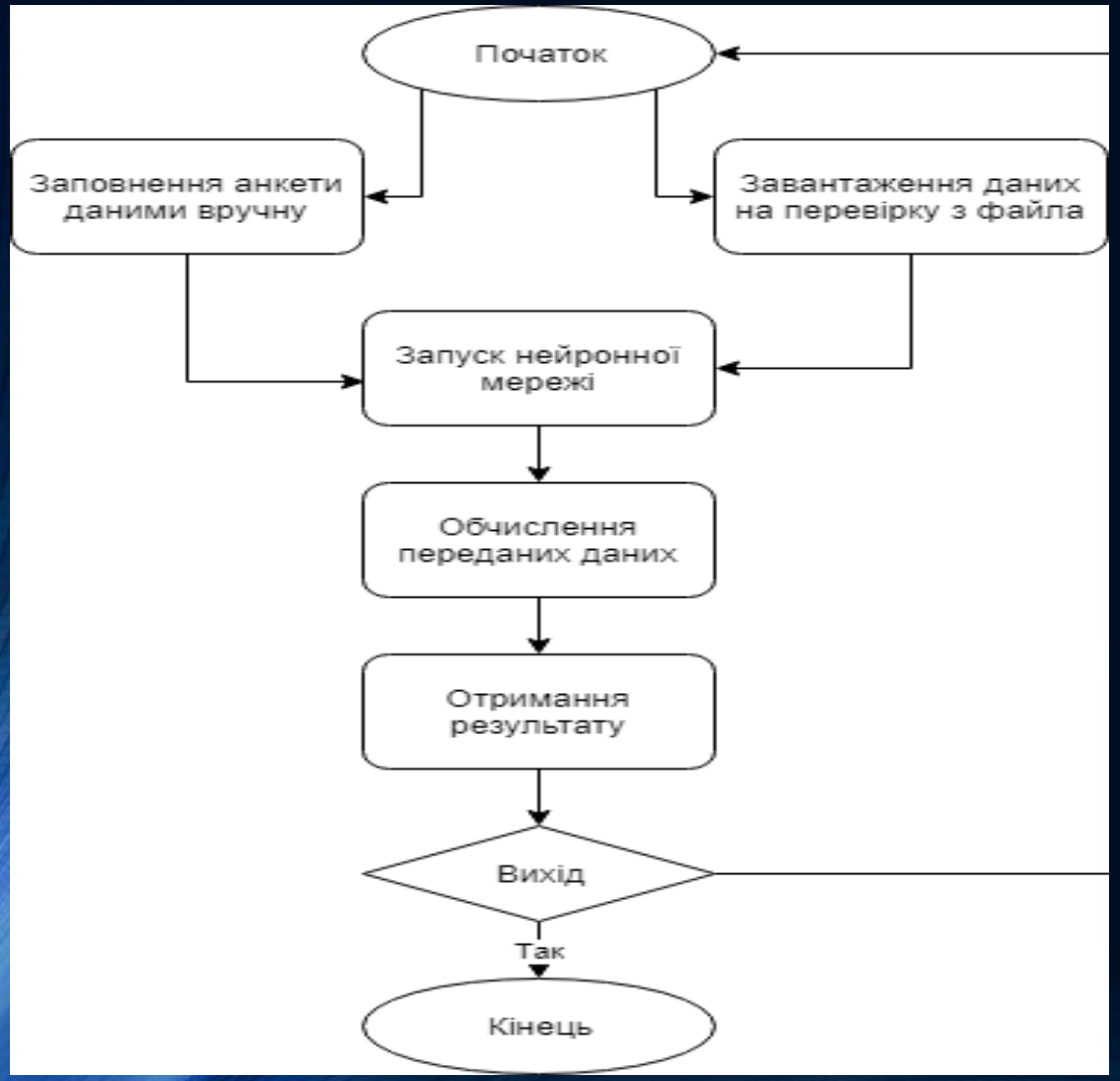
- Навантаження ЦП
- Навантаження на інтернет-мережу
- Навантаження на ОП
- Кількість вільної пам’яті ЖД
- Наявність незареєстрованих пристроїв
- Перевірка авторизації
- Кількість спроб введення пароля
- Кількість запущених програм
- Кількість дій на хвилину
- Виконання незареєстрованих програм

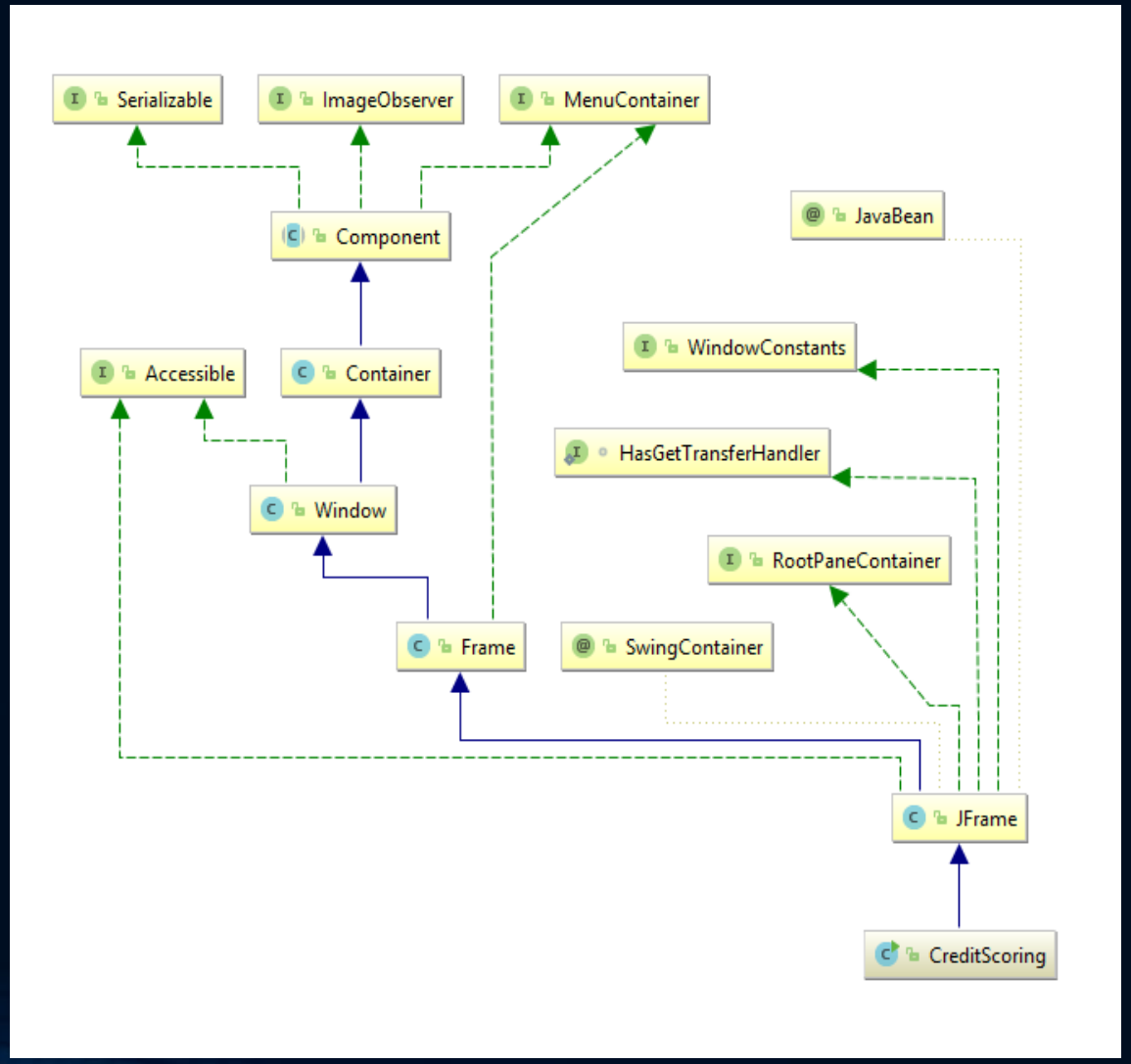
Алгоритм створення

Поєднання в ПЗ переваг існуючих програмних продуктів дозволяє створити універсальний та ефективний засіб для моніторингу безпеки.

Заміна експертної системи нейронною мережею, що навчена знаходити потенційну небезпеку на основі даних про стан системи та дій користувача

Архітектура програмного засобу





Критерії порівняння результатів

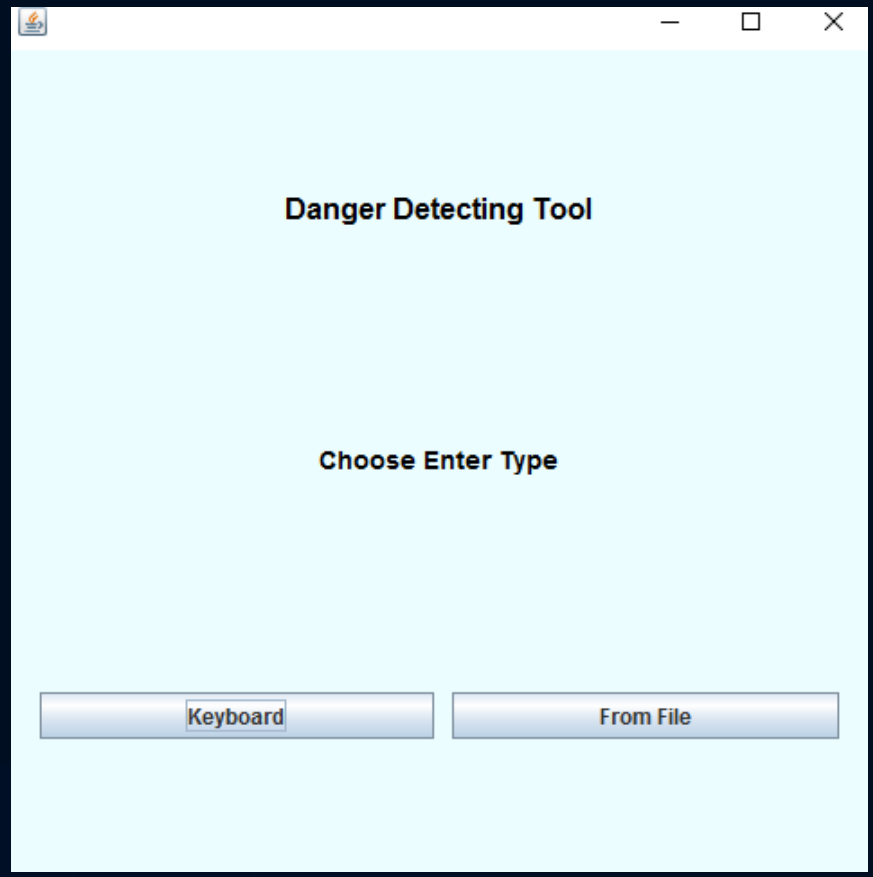
Основні критерії:

- Кількість правильних відповідей
- Швидкодія

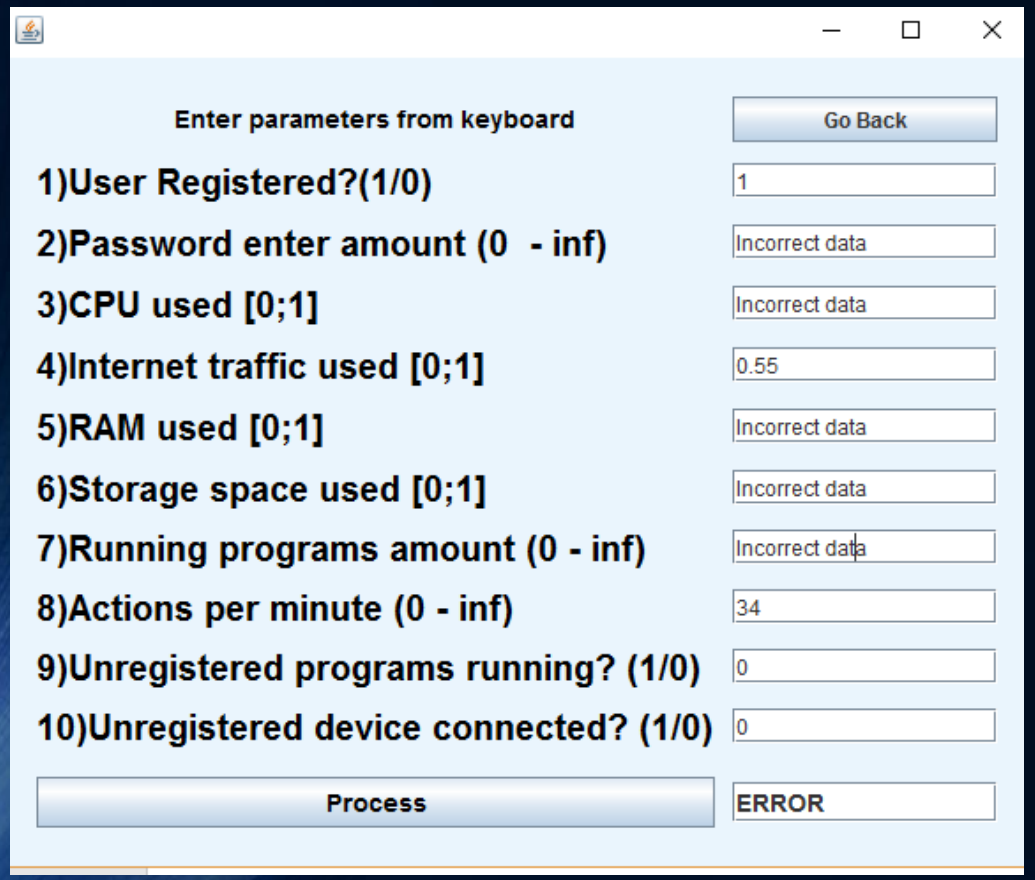
Інтерфейс програмного продукту

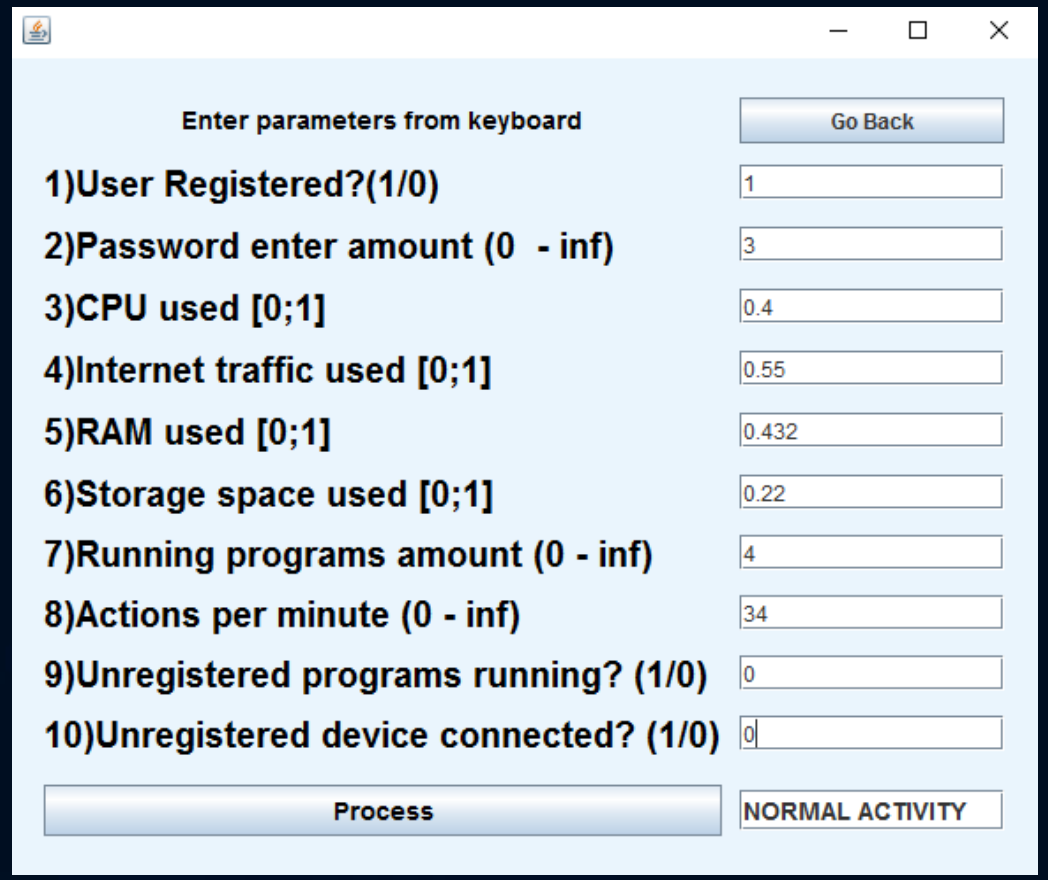
Дані оброблюються двома способами:

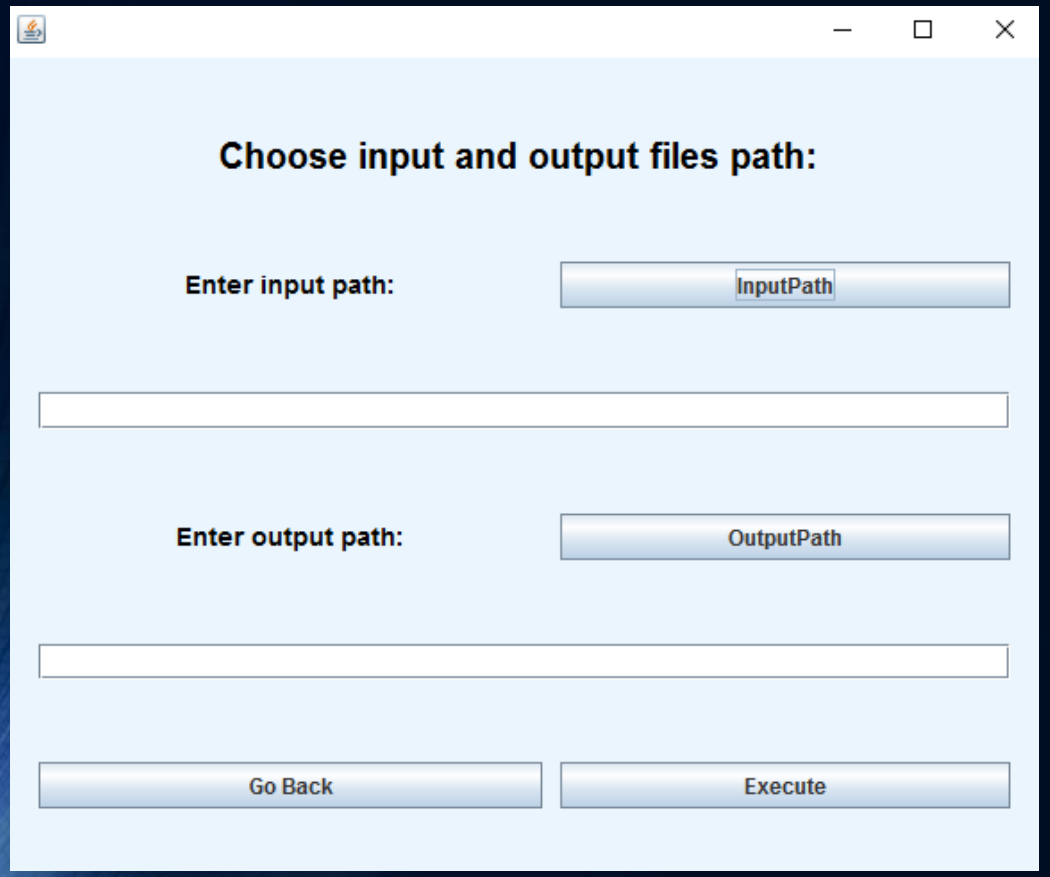
- Введення вектору стану системи користувачем з клавіатури, та виведення результату на екран
- Читання множини векторів стану з файлу, та запис результатів в файл

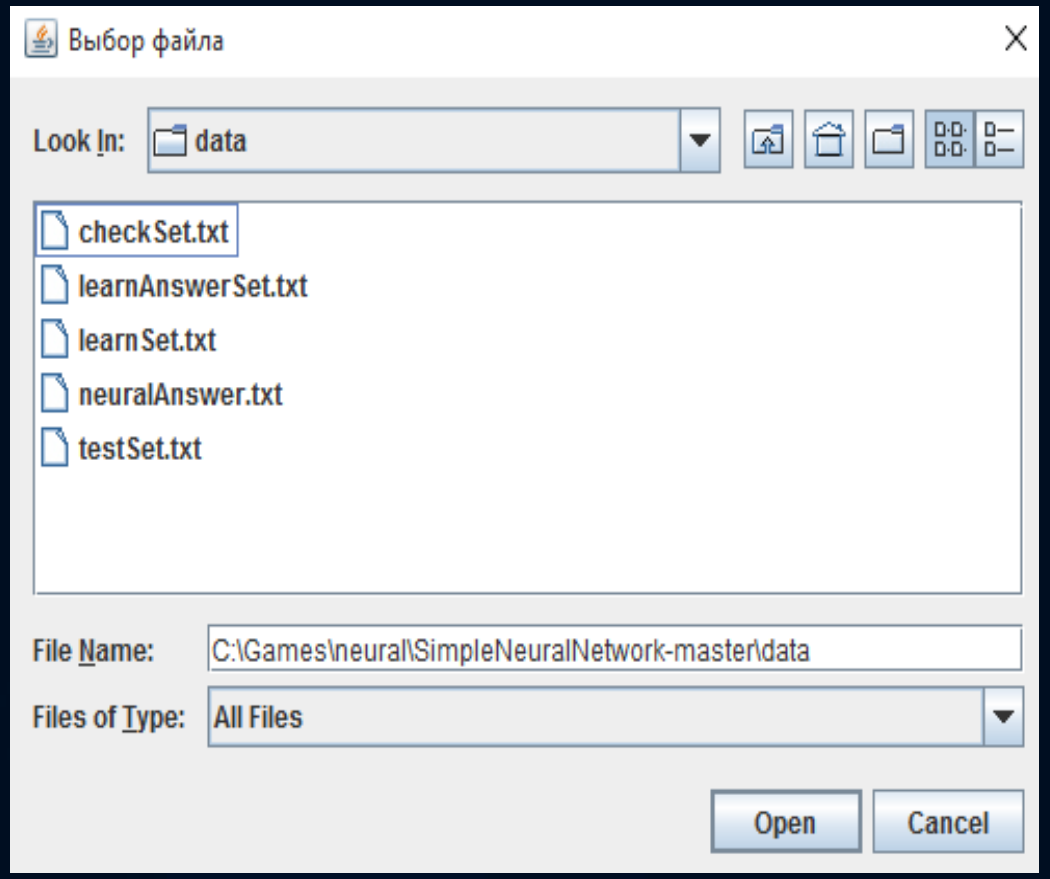


Результати роботи програми:






Choose input and output files path:
Enter input path:
InputPath
Enter output path:
OutputPath
Go Back
Execute


Выбор файла
Look In:
data
checkSet.txt
learnAnswerSet.txt
learnSet.txt
neuralAnswer.txt
testSet.txt
File Name:
C:\Games\neural\SimpleNeuralNetwork-master\data
Files of Type:
All Files
Open
Cancel

Висновки:

- Підключено та навчено нейронну мережу, яка на основі даних про стан системи та дій користувача в ній дозволяє виявити небезпеку
- Розроблено програмний продукт на основі цієї нейронної мережі, який розпізнає аномалії в роботі системи, та попереджає про потенційну загрозу

Шляхи подальшого розвитку:

- Покращення роботи нейронної мережі, збільшення кількості критеріїв на основі яких ця мережа приймає рішення
- Оптимізація роботи програми, пошук більш дієвих методів виявлення небажаної активності
- Розробка можливості для нейронної мережі не лише розпізнавати та попереджати про загрозу, а й визначення способу протидії цій загрозі

Дякую за увагу!