# МЕТОДИ ТА ЗАСОБИ МОНИТОРІНГУ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ НА ОСНОВІ АДАПТИВНОГО ПІДХОДУ

Виконав: Абібулаєв Євген

Ка-45 ІПСА

Науковий керівник:

д.т.н., професор Мухін Вадим Євгенович

- Мета роботи

Створення системи моніторингу безпеки мережі з адаптацією, її реалізація та дослідження.

- Об’єкт дослідження

Моделі, що застосовуються у системах моніторингу безпеки мереж, їх види та модифікації

- Метод дослідження

Розгляд та аналіз методів моніторингу безпеки та різного роду класифікаторів для цього

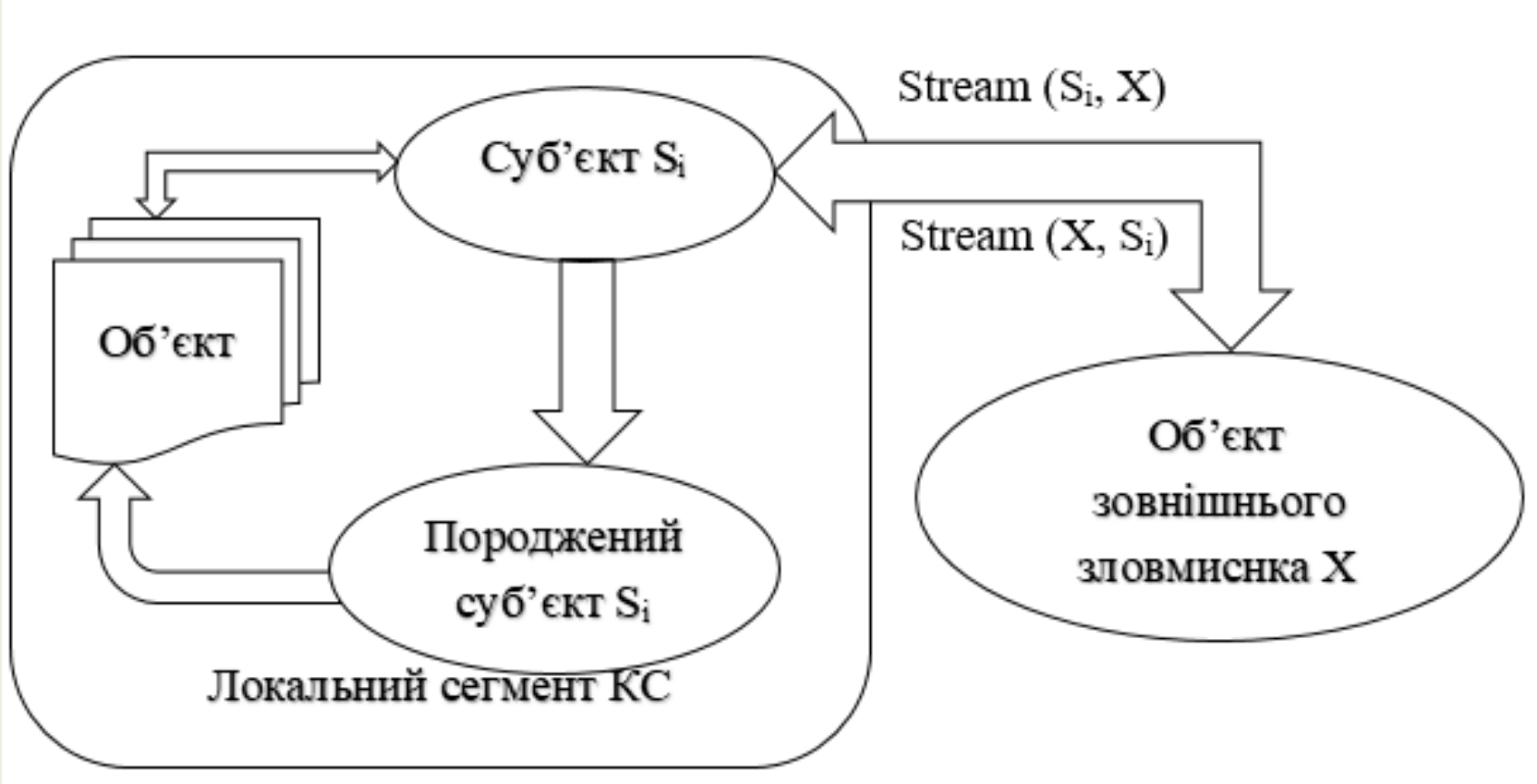
- Актуальність

Забезпечення захисту мережі при мінімально необхідному використанню ресурсів.

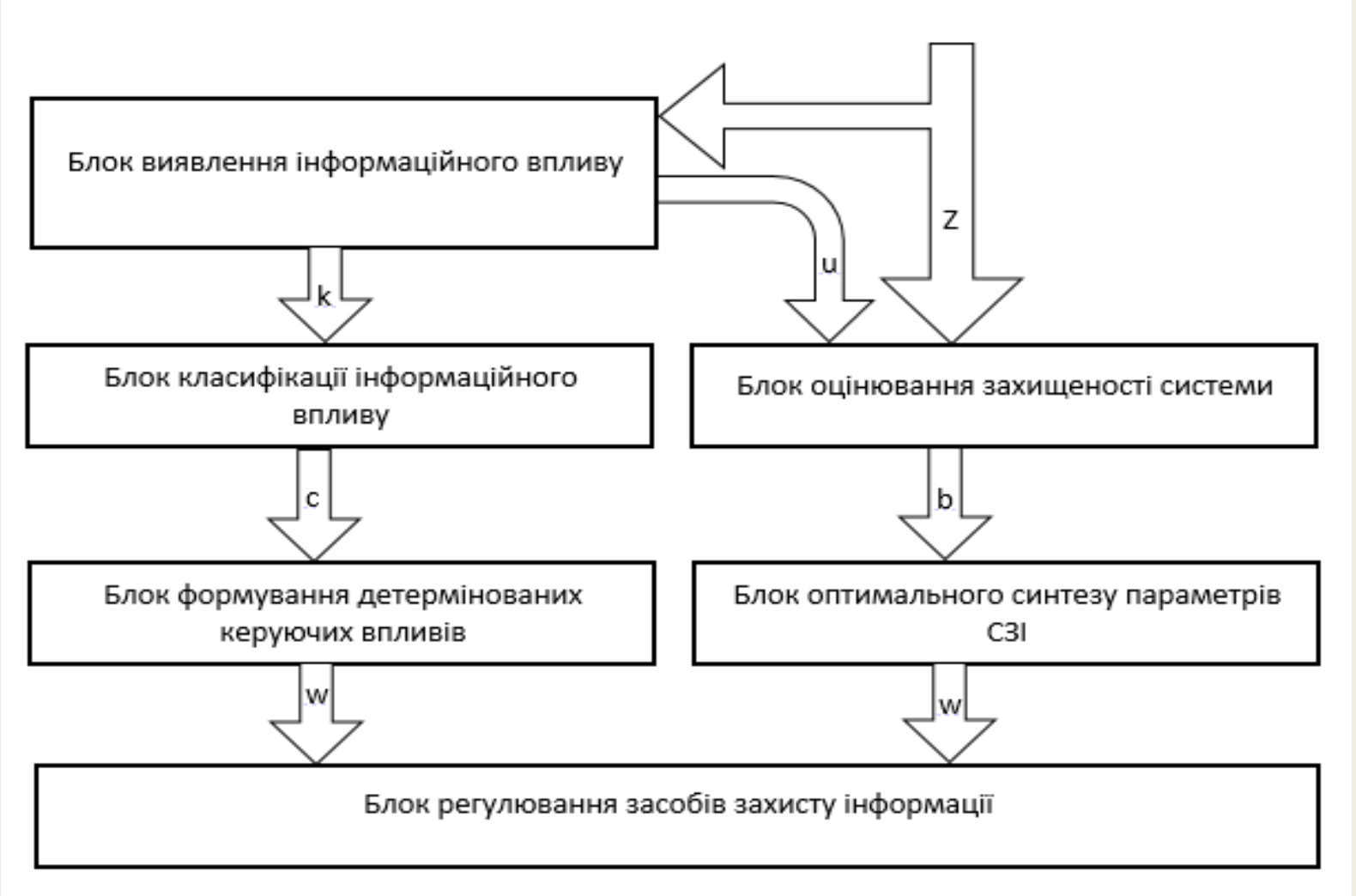
# ПОСТАНОВКА ЗАДАЧІ

- Проаналізувати існуючі методи та підходи методів моніторингу комп’ютерних мереж
- Реалізувати програмний продукт на основі проаналізованих методів
- Зробити експериментальне дослідження розробленої системи
- Сформулювати висновки щодо роботи алгоритму

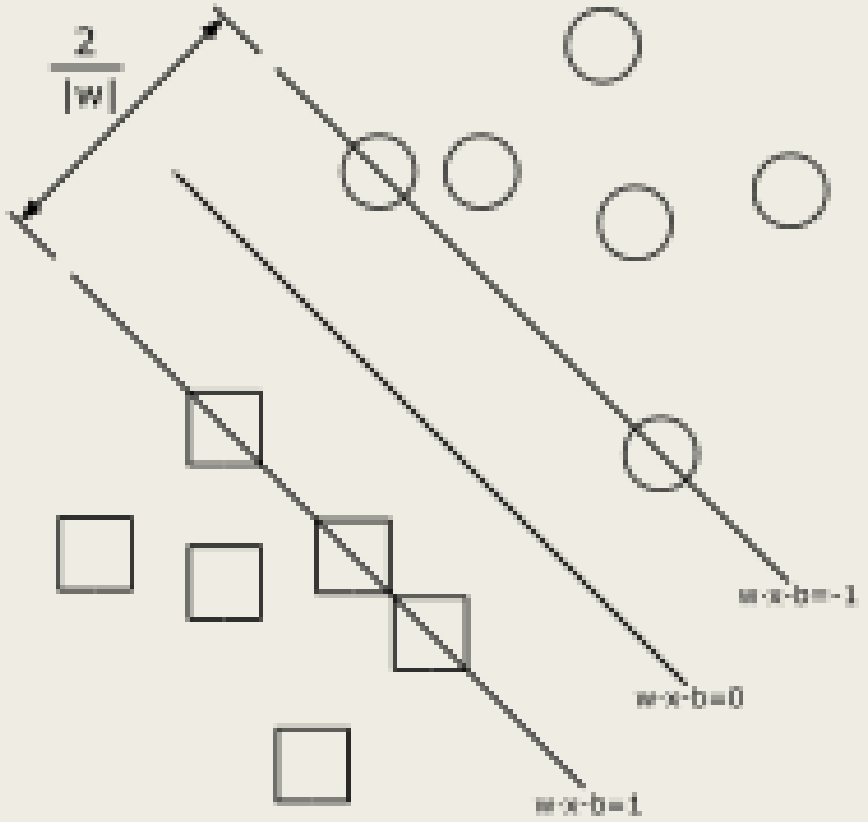
# Модель учасників комп’ютерної мережі



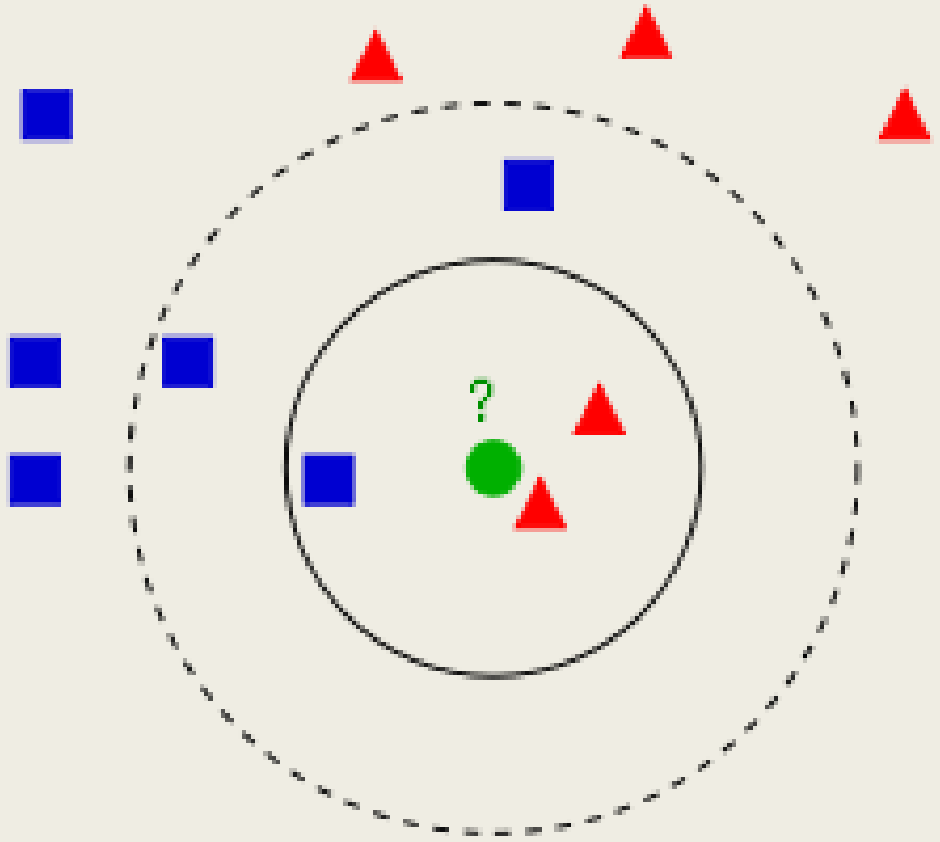
# Структура блоку адаптації з диференційованої реакцією на інформаційні впливи



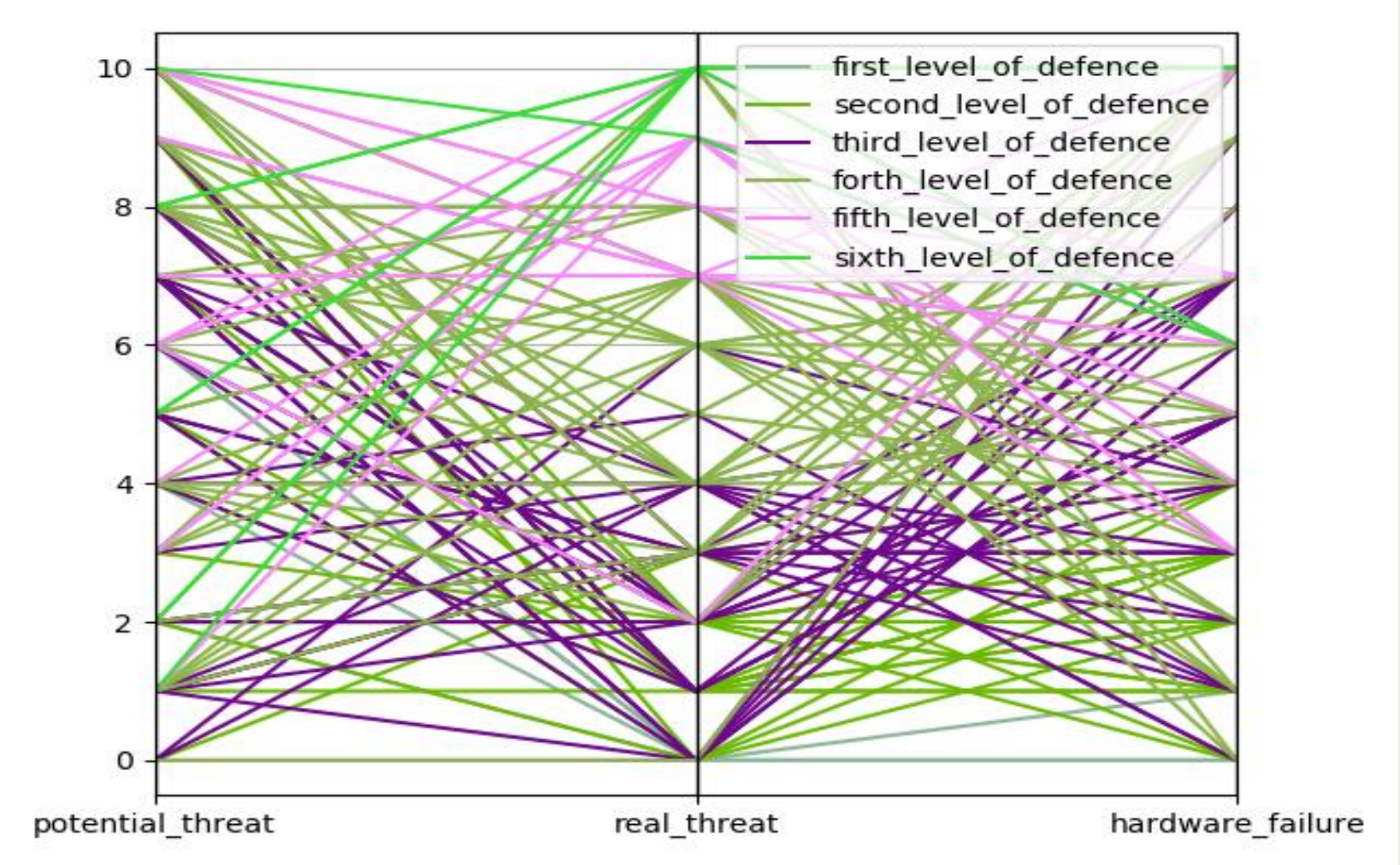
# Метод опорних векторів



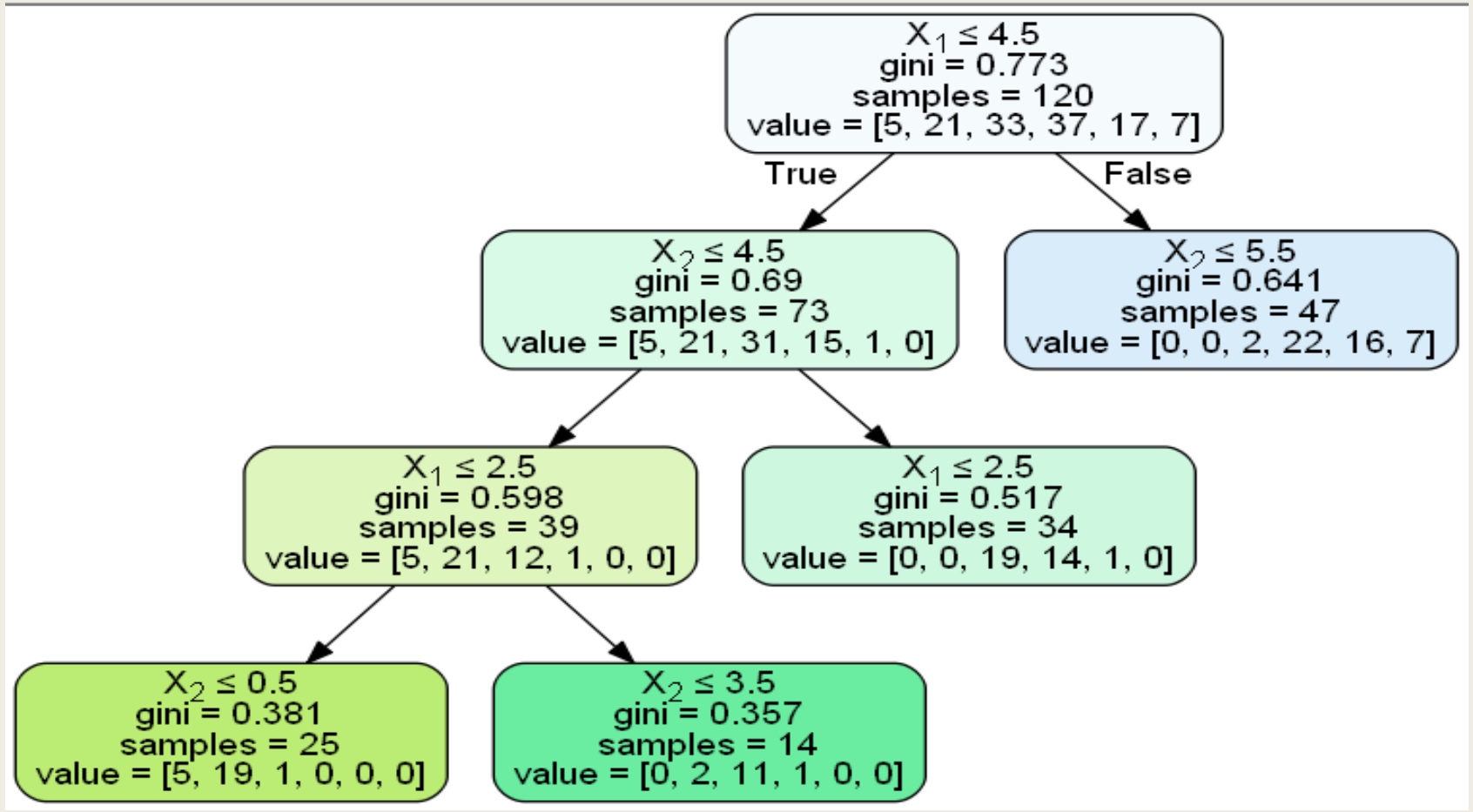
# Метод найближчього сусіда



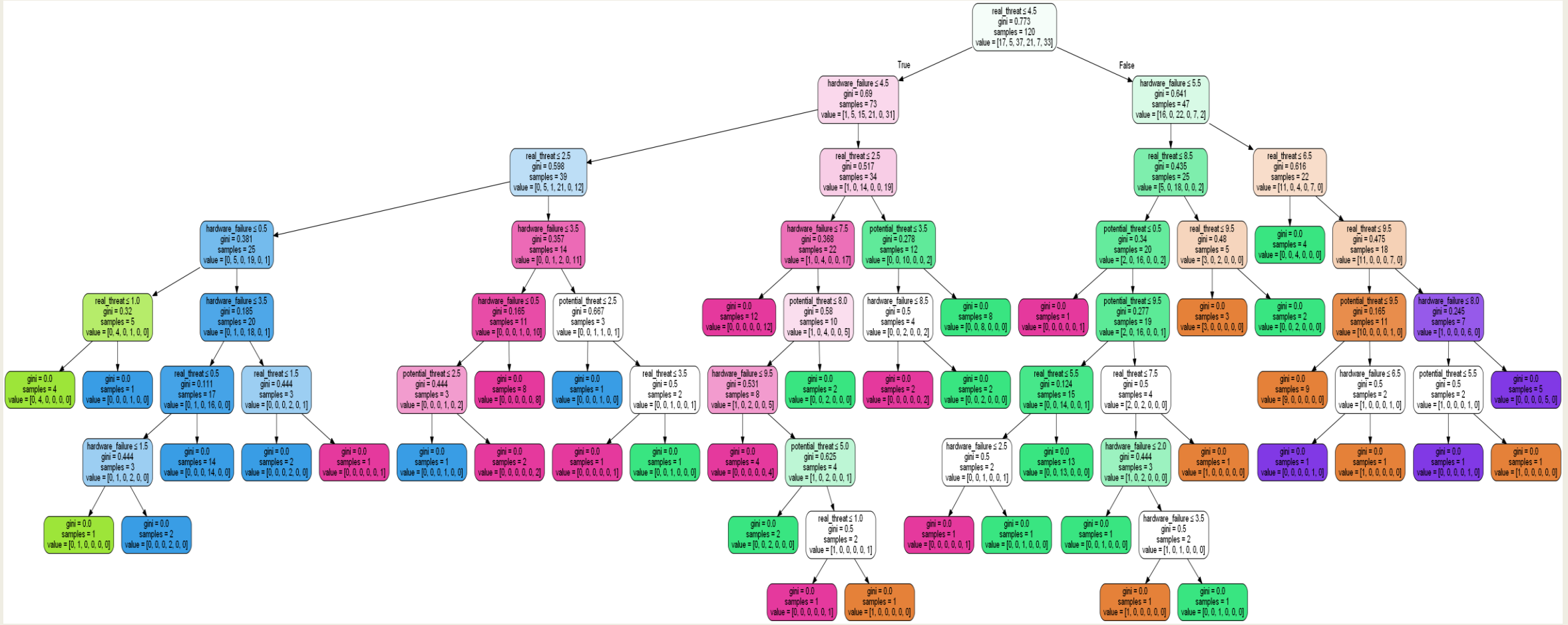
# Графічне зображення навчальної вибірки



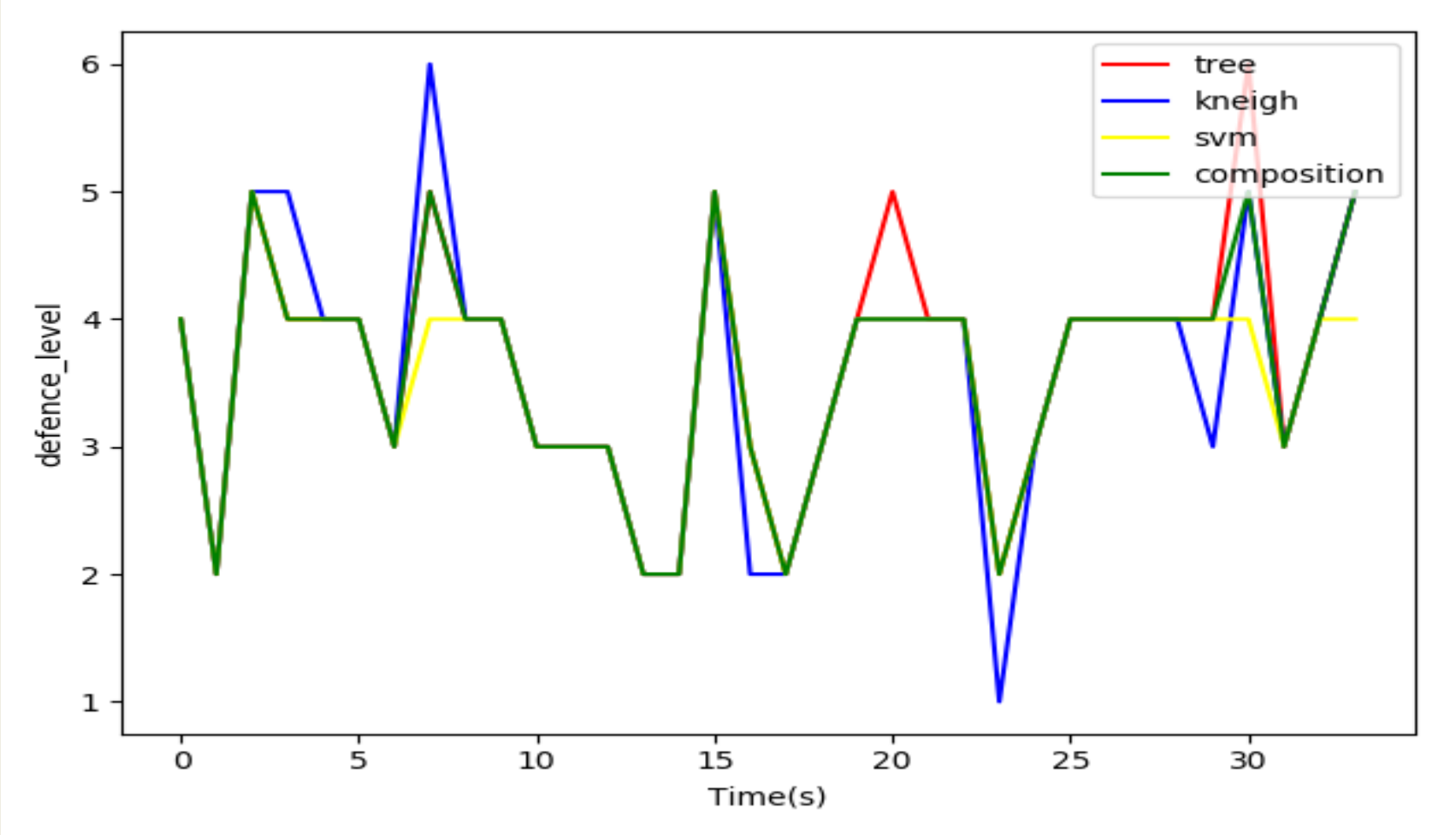
# Результати роботи програмного продукту



# Результати роботи програмного продукту



# Результати роботи програмного продукту



# Висновки

- Розглянуто існуючі системи моніторингу безпеки. Проаналізовано принципи їхнього функціонування. В результаті було виявлено, що нині є дуже важливою проблема, що розглядається в роботі.
- Розглянуто основні підходи до побудови алгоритмів моніторингу безпеки, наведено найпопулярніші та найпоширеніші алгоритми, проаналізовано їхні переваги та недоліки.
- Проаналізовано основні методи класифікації, що характеризують ситуацію в мережі на данний час, та описано їх математичні основи.
- Запропоновано композицію декількох класифікаторів, як методу класифікації, що дає більш точний результат.
- Розроблено програмний продукт, що дає змогу моніторити мережу в режимі реального часу, та змінювати її рівень захисту в залежності від поточного рівня загрози.

Дякую за увагу