Інтелектуальна система класифікації мережевих атак у системах захисту, що базується на генетичному алгоритмі

Виконав: студент групи 1КН-14 зн
Вовк С.
Керівник: к.т.н., доцент каф. КН
Суприган О. І.

- **Мета роботи** - підвищення точності визначення класу мережевої атаки у системах захисту за рахунок використання генетичного алгоритму.
- **Об’єктом роботи** є процес визначення класу мережевої атаки.
- **Предметом розробки** є програмне забезпечення для класифікації мережевих атак у системах захисту.
- Для досягнення поставленої мети слід вирішити такі **задачі**:

- провести аналіз предметної області та класифікувати мережеві атаки у системах захисту;
- виконати аналіз систем-аналогів для класифікації мережевих атак у системах захисту;
- розробити структурну модель інтелектуальної системи класифікації мережевих атак;
- розробити математичну модель та алгоритм;
- розробити модель стану та поведінки об’єктів системи;
- створити код інтелектуальної системи для класифікації мережевих атак у системах захисту.

Класифікація мережевих атак

Основні підходи при виявленні та класифікації мережевих атак

- - статистичний аналіз;
- - експертні системи;
- - нейронні мережі.

Моделі виявлення і запобігання мережевих атак

Моделі виявлення

- Хостова (*host-based)*
- Мережева (*network-based*)

Методи запобігання

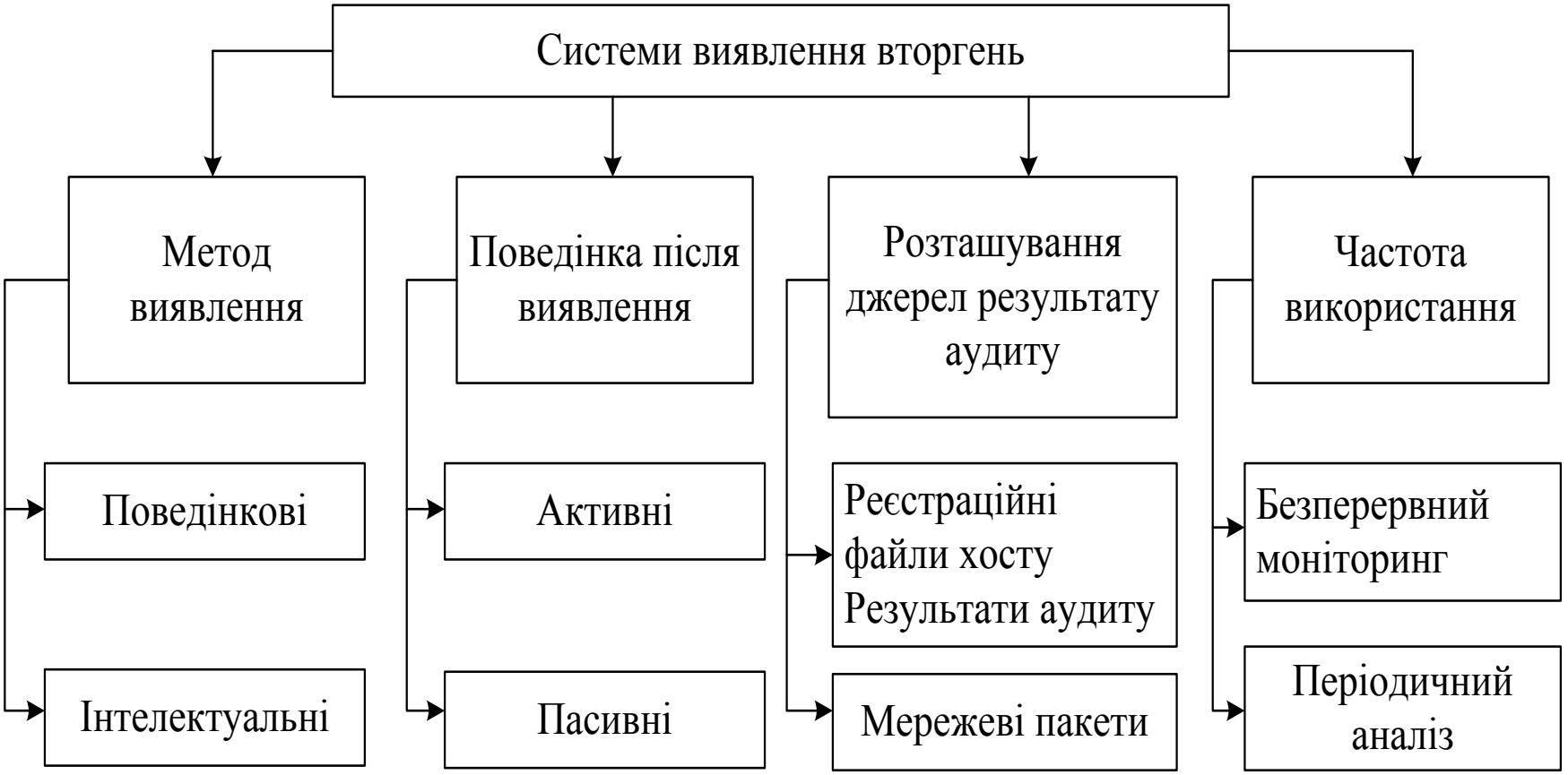
- Статистичний метод.
- Приховані марківські моделі.
- Нечітка логіка.
- Експертні системи.
- Використання прогнозованих шаблонів.
- Генетичні алгоритми.
- Штучні нейронні мережі.
- Аналіз переходів зі стану в стан.
- *Data mining*-методи.

Недоліки таких моделей:

•для моделей, які використовують статистичні методики – велика кількість помилкових тривог і помилок другого роду,

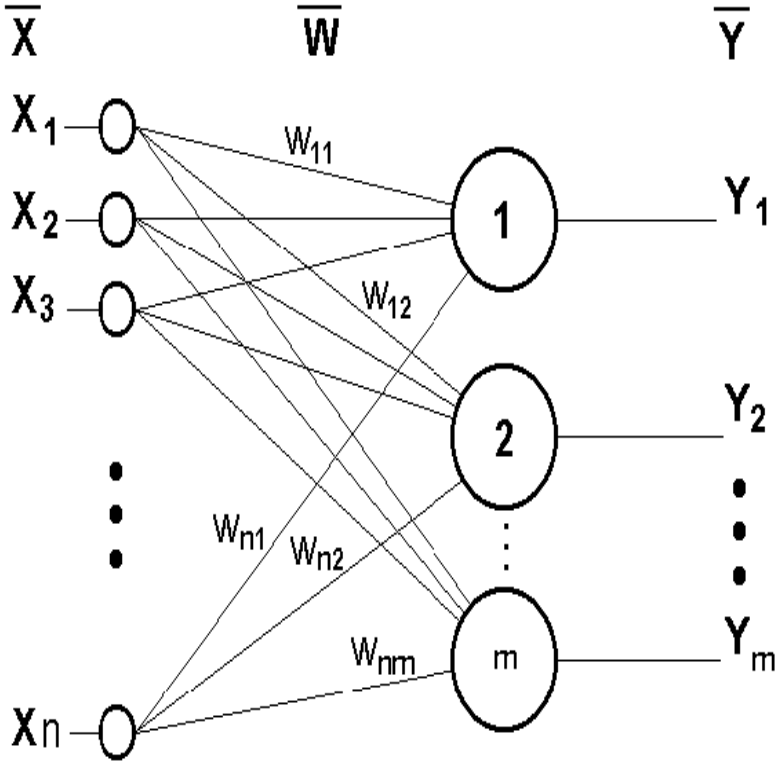
•для моделей, що використовують сигнатурні методики – неможливість самостійного виявлення нових атак і постійна необхідність оновлення бази сигнатур.

Засоби захисту від мережевих атак

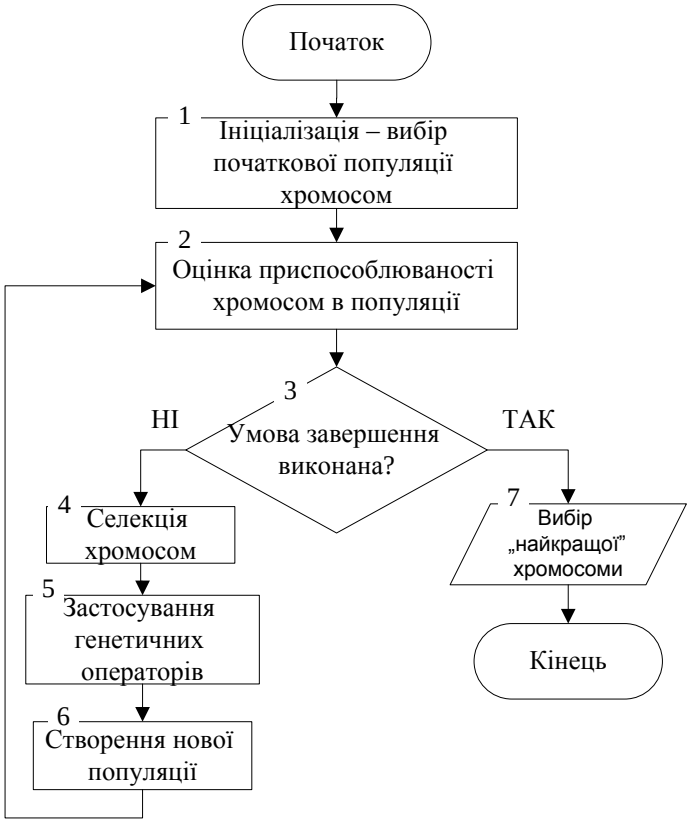


Системи-аналогі для класифікації мережевих атак у системах захисту

Нейронні мережі



Генетичні алгоритми



МАТЕМАТИЧНА РЕАЛІЗАЦІЯ КЛАСИФІКАЦІЇ МЕРЕЖЕВИХ АТАК

Структурна модель представлення системи інформаційної безпеки

Математична модель методу класифікації мережевих атак

. $v_{ij}(0)=1;W_{ij}(0)=1/(1+N)$

де $w_{ij}(t)$ - синаптична вага зв'язку від першого прошарку до другого прошарку в момент часу t,
$v_{ij}(t)$ - синаптична вага зв'язку від другого прошарку до першого прошарку в момент часу t,
b - значення порога.

f * = max {F (i) | I I 0}, k: = 0.

Обчислення значень відповідності:

$$y_i = \sum_{i=1}^{N} w_{ij}(t)x_i$$

Вибір зразка з найбільшою відповідністю: $y_j=\max(y_j)$

$$\|X\| = \sum_{j=1}^{N} x_j \qquad \|V \cdot X\| = \sum_{j=1}^{N} v_{ij} \times x_i$$

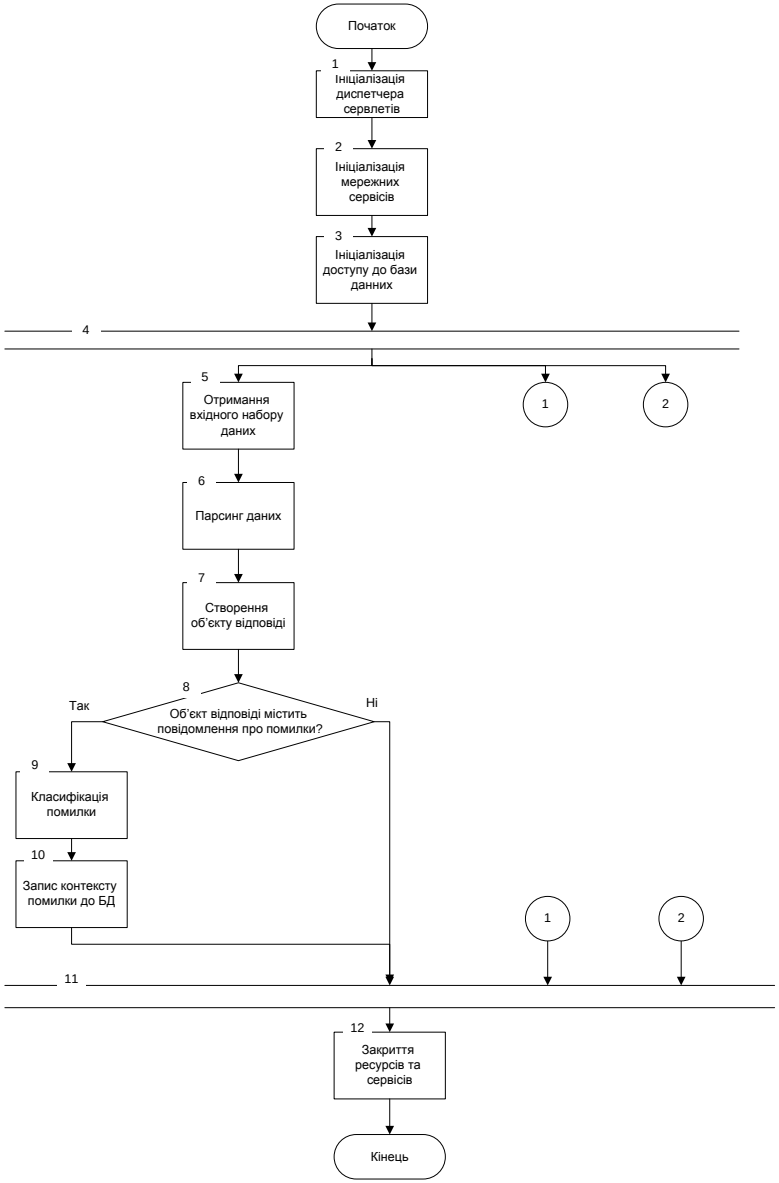
f * <f (I'), то f *: = f (I').

Адаптація приклада з найбільшим значенням відповідності:

$v_{ij}(t+1)=v_{ij}(t)x_j$

$$w_{ij}(t+1) = \frac{v_{ij}(t)x_j}{0{,}5 + \sum_{j=1}^{N} v_{ij}(t)x_j}$$

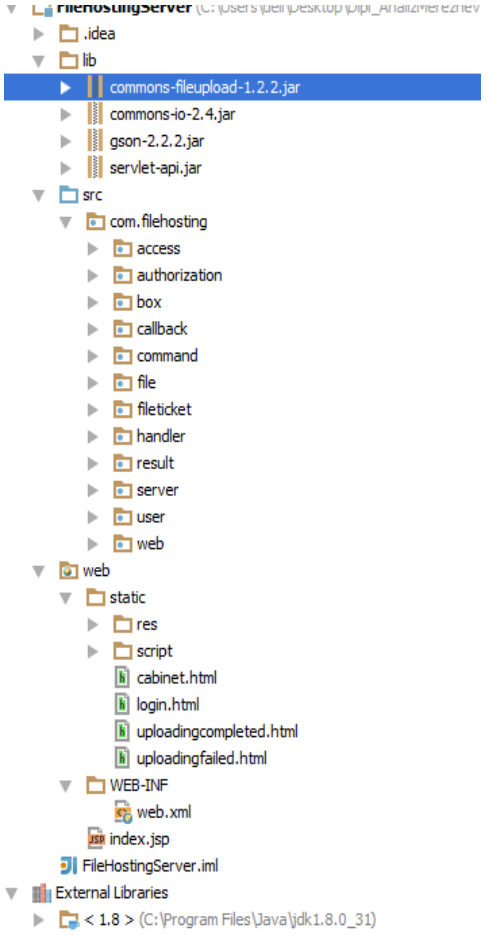
Алгоритм класифікації мережевих атак



Структурна реалізація програми

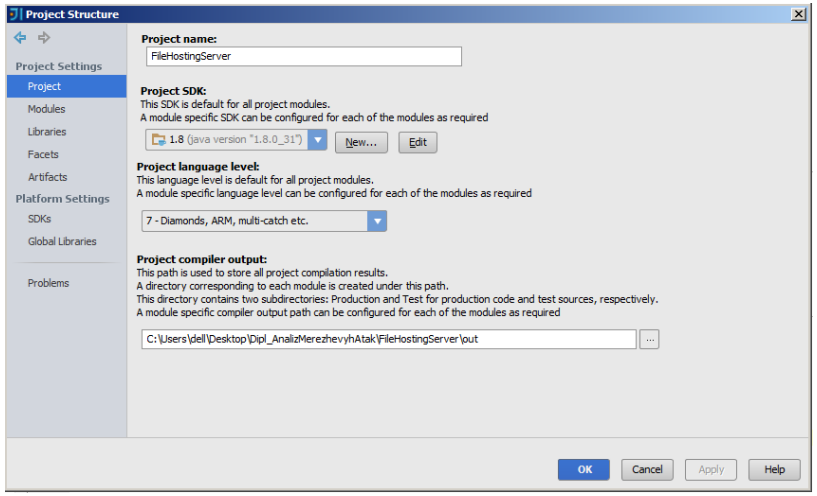
Основні частини проекту :

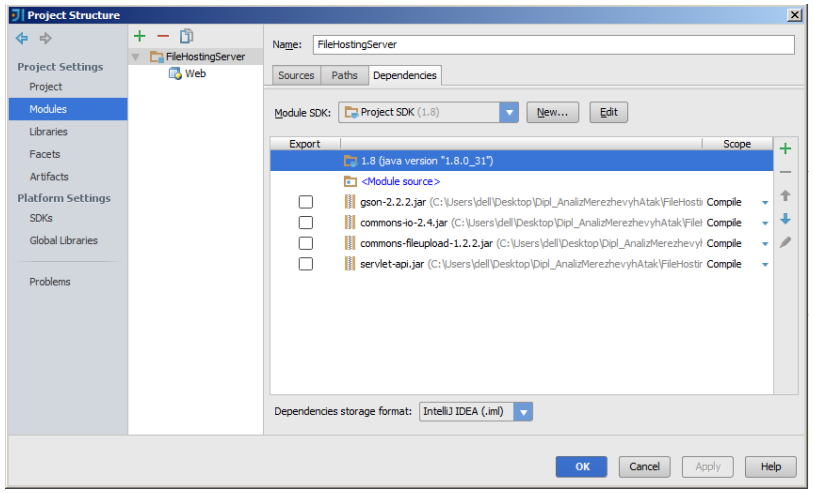
- 1. Бібліотеки, які підключені до проекту «вручну».
- 2. Код програми, який розділений по різних пакетах за функціональною ознакою.
- 3. Веб-частина, у якій зосереджено код для взаємодії із користувачем.
- 4. Зовнішні бібліотеки, які підключені через classpath.

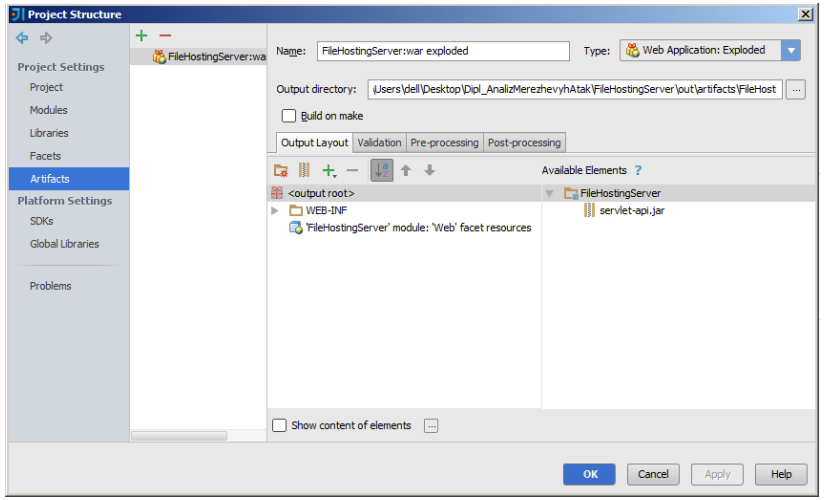


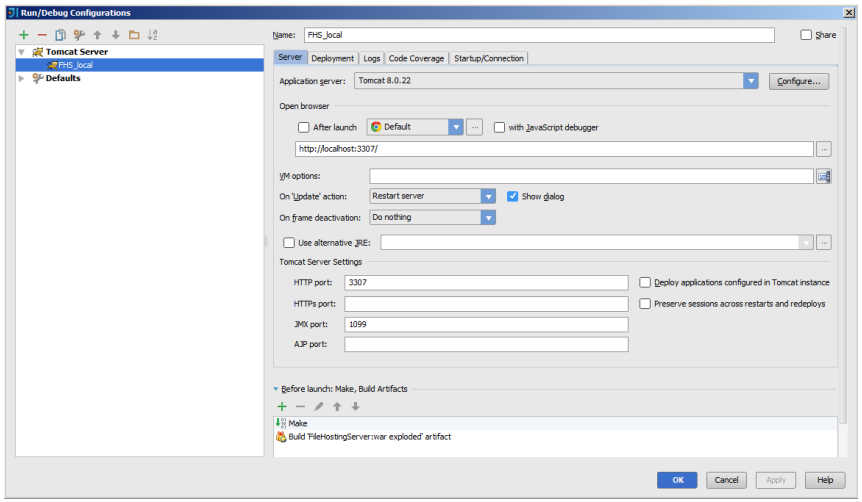
Тестування програми

Налаштування структури проекту

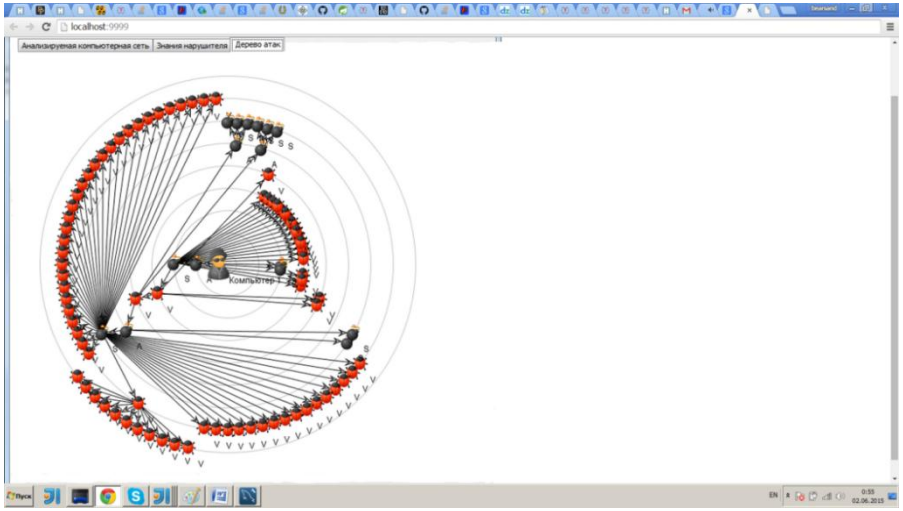




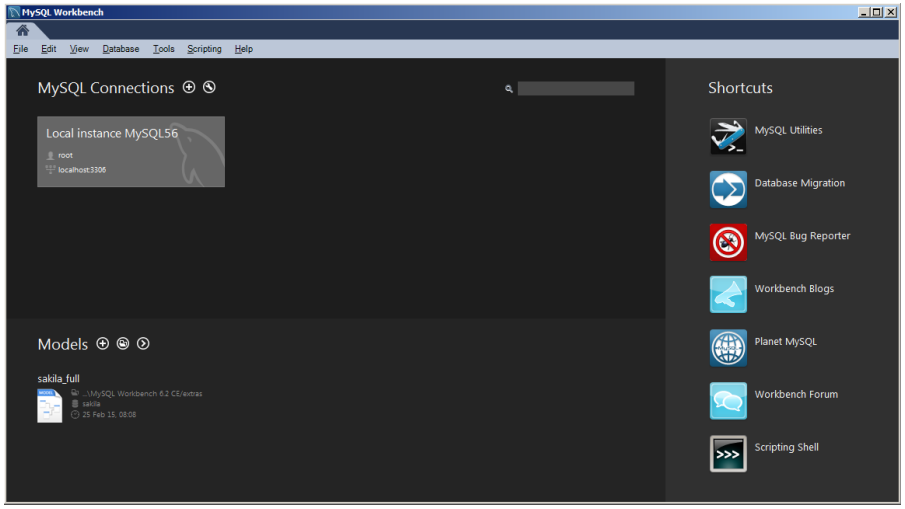




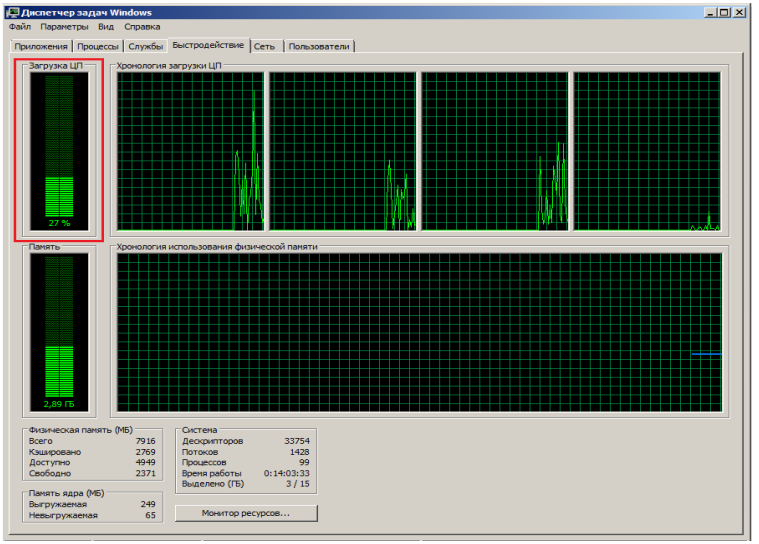
Візуалізація пошуку та класифікації мережевих атак



Сервер бази даних



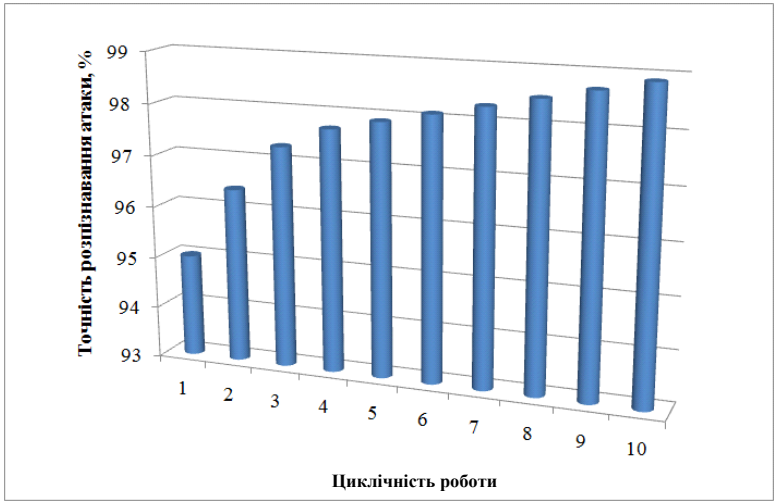
Діагностика стану завантаження процесору



Результат роботи програми

Залежність достовірності від завантаження процесору

Залежність точності від циклів генетичного алгоритму



Парам.	веб-інтерфейс	Методи сканування	платформи ОС
Прототип	Присутній	TCP	Windows
Nmap	Відсутній	UDP, TCP, TCP SYN , FTP proxy, Reverse-ident, ICMP, FIN, ACK, Xmas tree, SYN	Linux/BSD/Solaris Windows Mac OS X

Дякую за увагу!