ДОДАТОК А

СЛАЙДИ ПРЕЗЕНТАЦІЇ

Тема:
Дослідження методів побудови нейронних мереж для захисту від DDoS-атак

Виконав:
ст. групи ІПЗм-18-1
Зельонкін Д.О.

Керівник:
д.т.н., проф. Четвериков Г.Г.

АКТУАЛЬНІСТЬ ТЕМИ ДОСЛІДЖЕННЯ

- З розвитком мережевих технологій розвиваються і мережеві загрози. Останнім часом все більшої актуальності набувають DDoS-атаки. Робота присвячена виявленню DDoS-атак за допомогою нейронних мереж.
- Застосування штучних нейронних мереж дозволить створити ефективну адаптивну систему виявлення мережевих вторгнень і підвищити рівень захисту комп'ютерних систем від зовнішніх атак.

DDoS-атака

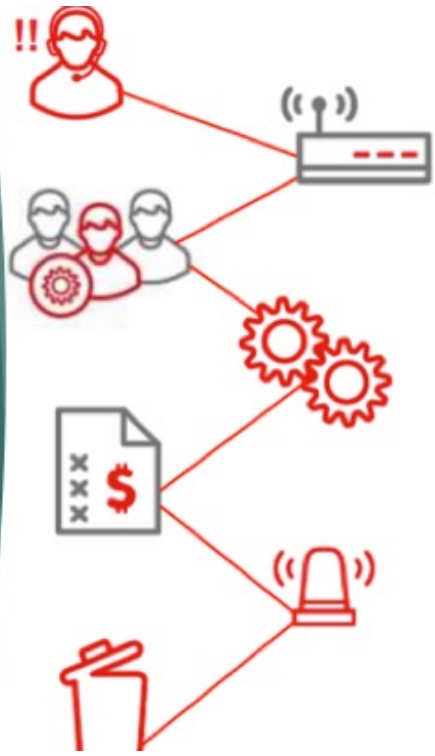
Атака типу «відмова в обслуговуванні» (DDoS) - це спроба завдати шкоди, зробивши недоступною цільову систему, наприклад веб-сайт або додаток, для звичайних кінцевих користувачів.

Мета дослідження

- Метою дослідження є аналіз та вдосконалення механізму захисту протидії на основі нейромережевого підходу задля підвищення точності виявлення DDoS-атак.

Вплив на діяльність організації

- Навантаження на helpdesk
- Непрацююча інфраструктура
- Навантаження на IT-департамент
- Втрата працездатності
- Репутаційний збиток
- Втрата клієнтів/можливостей



Класифікація атак

- За характером впливу
- За метою впливу
- За наявності зворотного зв'язку з атакується об'єктом
- За рівнем моделі OSI, на якому здійснюється вплив

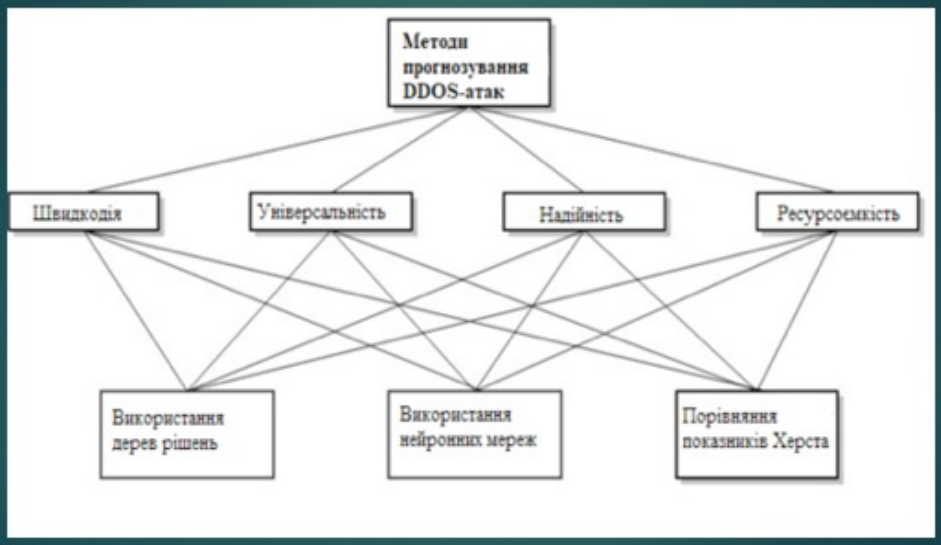
Типи DDoS трафіка

- HTTP-запити
- SYN-флуд
- ICMP-флуд

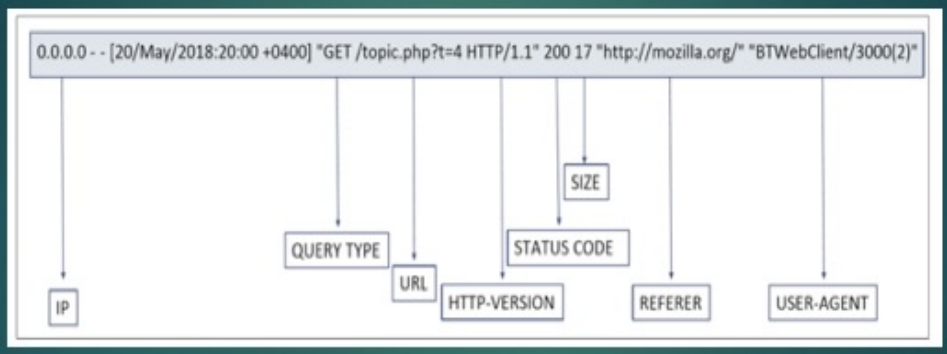
Методи виявлення мережевих атак

- Статистичний аналіз
- Експертні системи
- Нейронні мережі

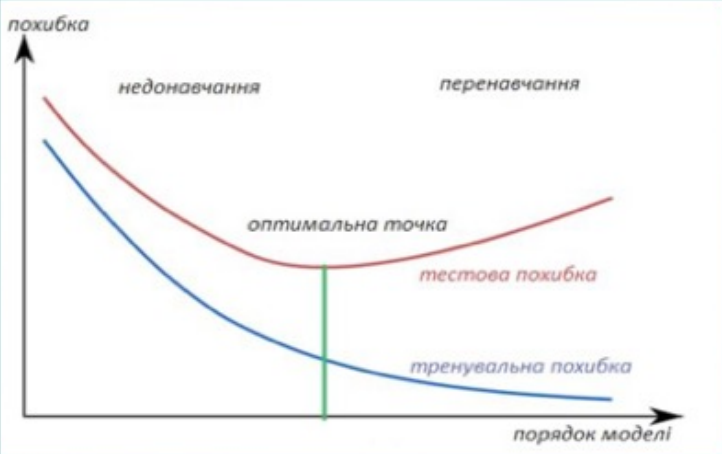
Аналізу методів прогнозування DDoS-атак



Аналіз HTTP запиту



Проблема перенавчання



Залежність похибки та часу роботи від кількості спроб

К-сть спроб (шт.)	5	10	25	50
Тестова похибка (%)	17,21	10,64	9,12	7,73
Час роботи алгоритму (с)	1,72	2,52	7,83	13,02

Залежність похибки та часу роботи від кількості процесів

К-сть процесів (шт.)	1	2	3	5
Тестова похибка (%)	1,98	3,12	4,86	6,01
Час роботи алгоритму (с)	59,96	38,45	23,30	15,97

Дослідження результатів

Довжина вибірки	Помилка першого роду (%)	Помилка другого роду (%)	Час відпрацювання алгоритму (с)
10	10,89	11,47	1,32
25	10,02	10,42	2,68
50	9,65	10,12	4,96
100	8,11	9,25	8,78
200	6,34	8,81	17,01
500	4,77	5,33	33,43
1000	2,76	2, 98	59,96

ВИСНОВКИ

- Розроблено механізм, що дозволяє класифікувати дані сервера з метою виявлення наявності DDoS-атаки. Проведено експерименти для підбору оптимальних параметрів нейронної мережі.

- Отримане програмне забезпечення можна інтегрувати у будь-яку систему, пов'язану з Інтернетом, для виконання фільтрації запитів. Даючи досить точні результати за короткий проміжок часу система придатна для використання як автономна модель класифікації даних, так і у більш складних системах, в якості їх компонента.