Дисципліна «Методи глибинного навчання»

Лабораторна робота №3

Тема: Нейромережеве розпізнавання кібератак
Мета: Розробка програмного забезпечення для реалізації нейронних мереж типу PNN та ДШП, призначених для розпізнавання кібератак, сигнатури яких представлені в базах даних KDD-99 або NLS KDD.
Теоретичні відомості: лекції №1-7.
Література:
1. Руденко О.Г. Штучні нейронні мережі. Навч. посіб. / О. Г. Руденко, Є. В. Бодянський.
2. Корченко О. Методологія розроблення нейромережевих засобів інформаційної безпеки Інтернет-орієнтованих інформаційних систем / О. Корченко, І. Терейковський, А. Білощицький. – К.: ТОВ «Наш Формат». 2017. – 249 с..

Зміст звіту:
- характеристика вибірки, що використовується для навчання та тестування НМ (опис джерела даних, які вибірка включає приклади, в якому вигляді вони описані, вхідні, вихідні параметри, процедура нормалізації вхідних параметрів);
- опис реалізації розробленого модуля (алгоритм, скриншот інтерфейсу програми);
- опис та результати експериментальних досліджень (як проводили навчання, на якому комп'ютері, термін навчання, результати розпізнавання);
- висновки.

Варіанти:

1. Розпізнавання мережевої кібератаки типу neptune за допомогою ДШП.
2. Розпізнавання мережевої кібератаки типу smurf за допомогою ДШП.
3. Розпізнавання мережевої кібератаки типу Pod за допомогою ДШП.
4. Розпізнавання мережевої кібератаки типу teardrop за допомогою ДШП.
5. Розпізнавання мережевої кібератаки типу land за допомогою ДШП.
6. Розпізнавання мережевої кібератаки типу back за допомогою ДШП.
7. Розпізнавання мережевої кібератаки типу guess_passwd за допомогою ДШП.
8. Розпізнавання мережевої кібератаки типу ftp_write за допомогою ДШП.
9. Розпізнавання мережевої кібератаки типу imap за допомогою ДШП.
10. Розпізнавання мережевої кібератаки типу phf за допомогою ДШП.
11. Розпізнавання мережевої кібератаки типу multihop за допомогою ДШП.
12. Розпізнавання мережевої кібератаки типу warezmaster за допомогою ДШП.
13. Розпізнавання мережевої кібератаки типу buffer_overflow за допомогою ДШП.
14. Розпізнавання мережевої кібератаки типу loadmodule за допомогою ДШП.
15. Розпізнавання мережевої кібератаки типу perl за допомогою ДШП.
16. Розпізнавання мережевої кібератаки типу rootkit за допомогою ДШП.
17. Розпізнавання мережевої кібератаки типу portsweep за допомогою ДШП.

18. Розпізнавання мережевої кібератаки типу neptune та smurf за допомогою PNN.
19. Розпізнавання мережевої кібератаки типу smurf та Pod за допомогою PNN.
20. Розпізнавання мережевої кібератаки типу Pod та teardrop за допомогою PNN.
21. Розпізнавання мережевої кібератаки типу teardrop та land за допомогою PNN.
22. Розпізнавання мережевої кібератаки типу land та back за допомогою PNN.
23. Розпізнавання мережевої кібератаки типу back та guess_passwd за допомогою PNN.
24. Розпізнавання мережевої кібератаки типу guess_passwd та ftp_write за допомогою PNN.
25. Розпізнавання мережевої кібератаки типу ftp_write та imap за допомогою PNN.
26. Розпізнавання мережевої кібератаки типу imap та phf за допомогою PNN.
27. Розпізнавання мережевої кібератаки типу phf та multihop за допомогою PNN.
28. Розпізнавання мережевої кібератаки типу multihop та warezmaster за допомогою PNN.
29. Розпізнавання мережевої кібератаки типу warezmaster та buffer_overflow за допомогою PNN.
30. Розпізнавання мережевої кібератаки типу buffer_overflow та loadmodule за допомогою PNN.
31. Розпізнавання мережевої кібератаки типу loadmodule та perl за допомогою PNN.
32. Розпізнавання мережевої кібератаки типу perl та rootkit за допомогою PNN.
33. Розпізнавання мережевої кібератаки типу rootkit та portsweep за допомогою PNN.
34. Розпізнавання мережевої кібератаки типу portsweep та neptune за допомогою PNN.