НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
Факультет прикладної математики
Кафедра прикладної математики

Звіт
із лабораторної роботи №3
з дисципліни «Системи нейронних мереж»
на тему
«Нейромережеве розпізнавання кібератак»

Виконав:
студент групи КМ-02
Пилипченко Б. О.

Керівник:
Терейковський І. А.

Київ—2023

Мета роботи:

Розробка програмного забезпечення для реалізації нейронної мережі PNN, призначеної для розпізнавання кібератак, сигнатури яких представлені у базах даних KDD-99.

Теоретичні відомості:

Роберт Каллан Основні концепції нейронних мереж ст. 152—164

Архітектура мережі

PNN мережа складається з трьох шарів:

1. Вхідний шар:

   Вхідний шар розподіляє характеристики вхідного зразка на шар зразків. Кожен нейрон вхідного шару пов'язаний із кожним нейроном шару зв'язків.

2. Шар зразків:

   Шар зразків має по одному нейрону для кожного зразка. Вагові коефіцієнти вхідних сигналів нейрону дорівнюють значенням характеристик відповідного зразка.

   Функція активації нейрону шару зразків:

$$O_j = \exp\left(\frac{-\sum(w_{ij} - x_i)^2}{\sigma^2}\right)$$

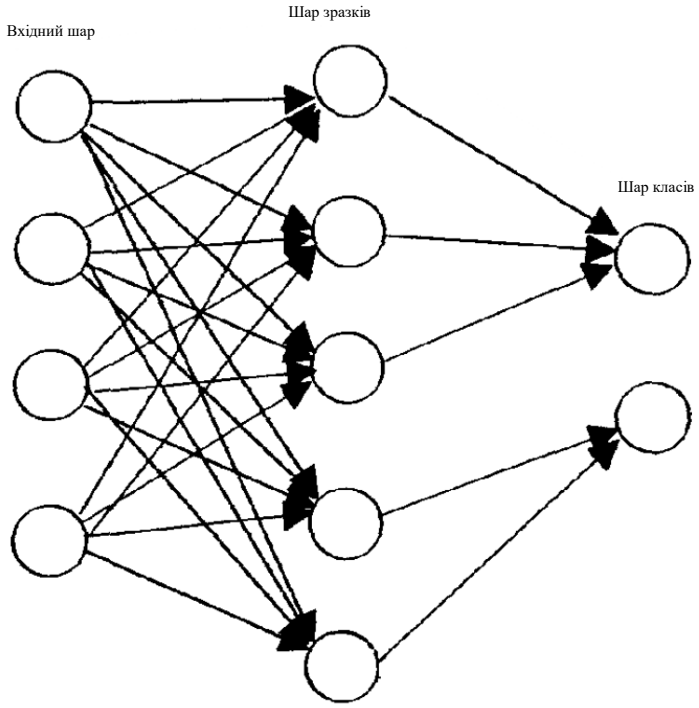
Oj—характеристика близькості вхідного зразка до j-того зразка класу;
xi—i-та характеристика вхідного зразка;
wij—i-та характеристика j– того зразка класу;
σ—параметр мережі.

3. Шар класів:

   Шар класів має по одному нейрону для кожного класу. Кожен нейрон шару класів має зв'язки лише з нейронами зв'язків, які належать до класу. Всі вагові коефіцієнти між шаром зразків та шаром класів рівні 1.

   Функція активації нейрону шару класів є сумою вхідних сигналів нейрону.

PNN мережа не потребує навчання, подібного до навчання мереж із оберненим поширенням сигналу. Всі параметри мережі PNN, крім значення сігми, визначаються безпосередньо навчальними даними:
Кількість нейронів вхідного шару = кількість характеристик зразків
Кількість нейронів шару зразків = кількість зразків
Кількість нейронів шару класів = кількість класів
Навчання мережі полягає у підборі оптимального значення сігми.
В роботі сігма підбиралась експериментально.



Огляд даних

В якості датасету було обрано KDD99. Остаточне тестування мереж здійснювалось на всьому датасеті (490020 зразків).

Початковий датасет містить 42 колонки (41 ознака + label):

```
>>> Column types >>>
 duration                int64
protocol_type           object
service                 object
flag                    object
src_bytes               int64
dst_bytes               int64
land                    int64
wrong_fragment          int64
urgent                  int64
hot                     int64
num_failed_logins       int64
logged_in               int64
lnum_compromised        int64
lroot_shell             int64
lsu_attempted           int64
lnum_root               int64
lnum_file_creations     int64
lnum_shells             int64
lnum_access_files       int64
lnum_outbound_cmds      int64
is_host_login           int64
is_guest_login          int64
count                   int64
srv_count               int64
serror_rate             float64
srv_serror_rate         float64
rerror_rate             float64
srv_rerror_rate         float64
same_srv_rate           float64
diff_srv_rate           float64
srv_diff_host_rate      float64
dst_host_count          int64
dst_host_srv_count      int64
dst_host_same_srv_rate  float64
dst_host_diff_srv_rate  float64
dst_host_same_src_port_rate  float64
dst_host_srv_diff_host_rate  float64
dst_host_serror_rate    float64
dst_host_srv_serror_rate  float64
dst_host_rerror_rate    float64
dst_host_srv_rerror_rate  float64
label                   object
```

Колонки lnum_outbound_cmds, is_host_login дорівнюють нулю для всіх зразків у датасеті:

```
Column: lnum_outbound_cmds
Unique Values Count: 1
Unique Values: [0]

Column: is_host_login
Unique Values Count: 1
Unique Values: [0]
```

тому було вирішено видалити ці колонки для всіх зразків. Остаточний датасет має 39 ознак.

В датасеті наявні ознаки, значеннями яких є рядкові літерали. Для таких ознак було застосовано LabelEncoder із бібліотеки sklearn. Таким чином нечислові ознаки було перетворено на числові, значення яких змінюється від 0 до n-1, де n—кількість унікальних значень ознаки.

Останнім кроком перед розбиттям даних на тренувальну та тестувальну вибірки є нормалізація значень ознак.

Розбиття даних

Параметри розбиття:

PNN_REFERENCE_COUNT_BY_CLASS	Набір пар «назва класу» - кількість прикладів класу pnn мережі відносно тренувальної вибірки
TEST_SIZE	Розмір тестової вибірки відносно вхідного (обробленого) датасету
REAL_DATA_COUNT_PER_CLASS	Максимальна кількість зразків класу в pnn мережі. Якщо кількість зразків класу перевищує параметр, то із всіх зразків класу обирається RE-AL_DATA_COUNT_PER_CLASS зразків випадковим чином.
RANDOM_STATE	Єдине значення random_state для всіх функцій, що потребують встановлення зерна.

Приклад набору параметрів:

```
PNN_REFERENCE_COUNT_BY_CLASS = {
   "smurf":          0.6,
   "neptune":        0.6,
   "normal":         0.6,
   "back":           1.0,
   "satan":          1.0,
   "ipsweep":        1.0,
   "portsweep":      1.0,
   "warezclient":    1.0,
   "teardrop":       1.0,
   "pod":            1.0,
   "nmap":           1.0,
   "guess_passwd":   1.0,
   "buffer_overflow": 1.0,
   "land":           1.0,
   "warezmaster":    1.0,
   "imap":           1.0,
   "rootkit":        1.0,
   "loadmodule":     1.0,
   "ftp_write":      1.0,
   "multihop":       1.0,
   "phf":            1.0,
   "perl":           1.0,
   "spy":            1.0
}
TEST_SIZE = 0.25
REAL_DATA_COUNT_PER_CLASS = 150
RANDOM_STATE = 1450
```

Розбиття обробленого датасету на тренувальну та навчальну вибірки виконується наступним чином:

1. Оброблений датасет розбивається на «елементарні» датасети—кожен елементарний датасет містить всі зразки одного класу, лише зразки одного класу.
2. Для кожного елементарного датасету: кроки 3 або 4
3. Якщо кількість записів у елементарному датасеті менша за REAL_DATA_COUNT_PER_CLASS—всі записи елементарного датасету заносяться у pnn мережу, навчальну вибірку, тестову вибірку.
4. Якщо кількість записів у елементарному датасеті більша за REAL_DATA_COUNT_PER_CLASS, тоді береться випадкова вибірка з елементарного датасету розміром REAL_DATA_COUNT_PER_CLASS. Отримана вибірка розбивається на тренувальну та тестову вибірки у співвідношенні TEST_SIZE. Далі із тренувальної вибірки обираються приклади, що будуть занесені у власне pnn мережу у співвідношенні, заданому PNN_REFERENCE_COUNT_BY_CLASS.
5. Внаслідок кроків 3, 4 отримуємо 3 набори даних для кожного класу: pnn набір, тренувальний набір, тестовий набір. Виконується об’єднання відповідних наборів у кінцеві pnn дані, тренувальні дані, тестові дані.

Навчання мережі

Тренувальні, тестові вибірки, текстові представлення pnn мереж: MLDL-lab3
Код скрипта-генератора даних, реалізації PNN: https://github.com/Bohdan628318ylypchenko/MLDL-Lab3.git

Параметри генерації PNN, тестової вибірки, валідаційної вибірки:

```
PNN_REFERENCE_COUNT_BY_CLASS = {
    "smurf":           0.6,
    "neptune":         0.6,
    "normal":          0.6,
    "back":           1.0,
    "satan":          1.0,
    "ipsweep":         1.0,
    "portsweep":       1.0,
    "warezclient":     1.0,
    "teardrop":        1.0,
    "pod":            1.0,
    "nmap":           1.0,
    "guess_passwd":    1.0,
    "buffer_overflow": 1.0,
    "land":           1.0,
    "warezmaster":     1.0,
    "imap":           1.0,
    "rootkit":         1.0,
    "loadmodule":      1.0,
    "ftp_write":       1.0,
    "multihop":        1.0,
    "phf":            1.0,
    "perl":           1.0,
    "spy":            1.0
}
TEST_SIZE = 0.25
REAL_DATA_COUNT_PER_CLASS = 2000
RANDOM_STATE_1 = 1450
RANDOM_STATE_2 = 860
```

Остаточні дані можна переглянути в репозиторії (файли pnn-2000.txt, train-2000.txt, test-2000.txt

Початкове значення s = 0.01

Запуск мережі на тренувальній вибірці:

```
t
Class: back-1600; eval: 1.0000000000000000000
Class: buffer_overflow-30; eval: 0.90000000000000002220
Class: ftp_write-8; eval: 1.0000000000000000000
Class: guess_passwd-53; eval: 1.0000000000000000000
Class: imap-12; eval: 1.0000000000000000000
Class: ipsweep-1247; eval: 1.0000000000000000000
Class: land-21; eval: 1.0000000000000000000
Class: loadmodule-9; eval: 1.0000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-960; eval: 0.99937500000000001332
Class: nmap-231; eval: 0.98701298701298700866
Class: normal-960; eval: 0.95750000000000001776
Class: perl-3; eval: 1.0000000000000000000
Class: phf-4; eval: 1.0000000000000000000
Class: pod-264; eval: 1.0000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 1.0000000000000000000
Class: satan-1589; eval: 1.0000000000000000000
Class: smurf-960; eval: 1.0000000000000000000
Class: spy-2; eval: 1.0000000000000000000
Class: teardrop-979; eval: 1.0000000000000000000
Class: warezclient-1020; eval: 1.0000000000000000000
Class: warezmaster-20; eval: 1.0000000000000000000
zero count: 0
time: 3.097883
```

Запуск мережі на тестовій вибірці:

```
v
Class: back-1600; eval: 1.0000000000000000000
Class: buffer_overflow-30; eval: 0.90000000000000002220
Class: ftp_write-8; eval: 1.0000000000000000000
Class: guess_passwd-53; eval: 1.0000000000000000000
Class: imap-12; eval: 1.0000000000000000000
Class: ipsweep-1247; eval: 1.0000000000000000000
Class: land-21; eval: 1.0000000000000000000
Class: loadmodule-9; eval: 1.0000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-960; eval: 0.99750000000000005329
Class: nmap-231; eval: 0.98701298701298700866
Class: normal-960; eval: 0.89500000000000001776
Class: perl-3; eval: 1.0000000000000000000
Class: phf-4; eval: 1.0000000000000000000
Class: pod-264; eval: 1.0000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 1.0000000000000000000
Class: satan-1589; eval: 1.0000000000000000000
Class: smurf-960; eval: 0.99750000000000005329
Class: spy-2; eval: 1.0000000000000000000
Class: teardrop-979; eval: 1.0000000000000000000
Class: warezclient-1020; eval: 1.0000000000000000000
Class: warezmaster-20; eval: 1.0000000000000000000
```

Загалом результати позитивні: для більшості класів мережа вірно класифікує усі приклади класу, наявні у вибірці. Найгірші показники мають класи normal (0.95 | 0.89) та multihop (0.85 | 0.85).
Особливо цікавим є клас multihop, оскільки, не зважаючи на те, що ВСІ приклади з початкового датасету наявні в мережі, мережа не дає правильної відповіді на деякі з прикладів цього класу.

Спробуємо запустити мережу на кожному прикладі класу multihop окремо:

```
Enter command:
r 0.00,0.50,0.28,0.90,0.00,0.00,0.00,0.00,0.00,0.07,0.00,1.00,0.00,0.00,0.00,0.00,0.04,0.00,0.00,1.00,0.00,0.00,0.00,0.00,0.00,0.00,1.00,0.00,0.00,1.00,0.00,0.00,0.01,0.00,0.00,0.00,0.00,0.04,0.00
back-1600 : 0.000000000000000000
buffer_overflow-30 : 0.000000000000000000
ftp_write-8 : 0.000000000000000000
guess_passwd-53 : 0.000000000000000000
imap-12 : 0.000000000000000000
ipsweep-1247 : 0.000000000000000000
land-21 : 0.000000000000000000
loadmodule-9 : 0.000000000000000000
multihop-7 : 0.482749206693218857
neptune-960 : 0.000000000000000000
nmap-231 : 0.000000000000000000
normal-960 : 0.000000000000000000
perl-3 : 0.000000000000000000
phf-4 : 0.000000000000000000
pod-264 : 0.000000000000000000
portsweep-1040 : 0.000000000000000000
rootkit-10 : 0.000000000000000000
satan-1589 : 0.000000000000000000
smurf-960 : 0.000000000000000000
spy-2 : 0.000000000000000000
teardrop-979 : 0.000000000000000000
warezclient-1020 : 0.000000000000000000
warezmaster-20 : 0.000000000000000000
```

```
Enter command:
r
0.00,0.50,0.28,0.90,0.00,0.00,0.00,0.00,0.00,0.03,0.00,1.00,0.00,0.00,0.00,0.00,0.04,0.00,0.00,1.00,0.00,0.00,0.00,0.00,0.00,0.00,1.00,0.00,0.00,1.00,0.01,0.01,0.01,0.00,0.00,0.00,0.00
,0.04,0.00
back-1600 : 0.000000000000000000
buffer_overflow-30 : 0.000000000000000000
ftp_write-8 : 0.000000000000000000
guess_passwd-53 : 0.000000000000000000
imap-12 : 0.000000000000000000
ipsweep-1247 : 0.000000000000000000
land-21 : 0.000000000000000000
loadmodule-9 : 0.000000000000000000
multihop-7 : 0.545100167113102940
neptune-960 : 0.000000000000000000
nmap-231 : 0.000000000000000000
normal-960 : 0.000000000000000000
perl-3 : 0.000000000000000000
phf-4 : 0.000000000000000000
pod-264 : 0.000000000000000000
portsweep-1040 : 0.000000000000000000
rootkit-10 : 0.000000000000000000
satan-1589 : 0.000000000000000000
smurf-960 : 0.000000000000000000
spy-2 : 0.000000000000000000
teardrop-979 : 0.000000000000000000
warezclient-1020 : 0.000000000000000000
warezmaster-20 : 0.000000000000000000
```

```
Enter command:
r
0.00,0.50,0.29,0.90,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,
1.00,0.00,0.00,0.00,0.00,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.00
back-1600 : 0.000000000000000000
buffer_overflow-30 : 0.000000000000000000
ftp_write-8 : 0.000000000000000000
guess_passwd-53 : 0.000000000000000000
imap-12 : 0.000000000000000000
ipsweep-1247 : 0.000000000000000000
land-21 : 0.000000000000000000
loadmodule-9 : 0.000000000000000000
multihop-7 : 0.645699336191089213
neptune-960 : 0.000000000000000000
nmap-231 : 0.000000000000000000
normal-960 : 0.000000000000000000
perl-3 : 0.000000000000000000
phf-4 : 0.000000000000000000
pod-264 : 0.000000000000000000
portsweep-1040 : 0.000000000000000000
rootkit-10 : 0.000000000000000000
satan-1589 : 0.000000000000000000
smurf-960 : 0.000000000000000000
spy-2 : 0.000000000000000000
teardrop-979 : 0.000000000000000000
warezclient-1020 : 0.000000000000000000
warezmaster-20 : 0.837178979793791633
```

```
r 0.00,0.50,0.29,0.90,0.00,0.09,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,1.00,0.00,0.00,0.01,0.01,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.00
back-1600 : 0.000000000000000000
buffer_overflow-30 : 0.000000000000000000
ftp_write-8 : 0.000000000000000000
guess_passwd-53 : 0.000000000000000000
imap-12 : 0.000000000000000000
ipsweep-1247 : 0.000000000000000000
land-21 : 0.000000000000000000
loadmodule-9 : 0.000000000000000000
multihop-7 : 0.795459086582364638
neptune-960 : 0.000000000000000000
nmap-231 : 0.000000000000000000
normal-960 : 0.000000000000000000
perl-3 : 0.000000000000000000
phf-4 : 0.000000000000000000
pod-264 : 0.000000000000000000
portsweep-1040 : 0.000000000000000000
rootkit-10 : 0.000000000000000000
satan-1589 : 0.000000000000000000
smurf-960 : 0.000000000000000000
spy-2 : 0.000000000000000000
teardrop-979 : 0.000000000000000000
warezclient-1020 : 0.000000000000000000
warezmaster-20 : 0.000000000000000000
```

```
r
0.00,0.50,0.29,0.90,0.00,0.19,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,1.00,0.00,1.00,0.01,0.01,1.00,0.00,1.00,0.00,0
.00,0.00,0.00,0.00
back-1600 : 0.000000000000000000
buffer_overflow-30 : 0.000000000000000000
ftp_write-8 : 0.000000000000000000
guess_passwd-53 : 0.000000000000000000
imap-12 : 0.000000000000000000
ipsweep-1247 : 0.000000000000000000
land-21 : 0.000000000000000000
loadmodule-9 : 0.000000000000000000
multihop-7 : 0.716074647101321404
neptune-960 : 0.000000000000000000
nmap-231 : 0.000000000000000000
normal-960 : 0.000000000000000000
perl-3 : 0.000000000000000000
phf-4 : 0.000000000000000000
pod-264 : 0.000000000000000000
portsweep-1040 : 0.000000000000000000
rootkit-10 : 0.000000000000000000
satan-1589 : 0.000000000000000000
smurf-960 : 0.000000000000000000
spy-2 : 0.000000000000000000
teardrop-979 : 0.000000000000000000
warezclient-1020 : 0.000000000000000000
warezmaster-20 : 0.000000000000000000
```

```
r
0.00,0.50,0.86,0.90,0.00,0.00,0.00,0.00,0.00,0.10,0.00,1.00,0.02,1.00,0.00,0.04,0.14,1.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,1.
00,0.00,0.00,0.00,0.00,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.00
back-1600 : 0.000000000000000000
buffer_overflow-30 : 0.000000000000000000
ftp_write-8 : 0.000000000000000000
guess_passwd-53 : 0.000000000000000000
imap-12 : 0.000000000000000000
ipsweep-1247 : 0.000000000000000000
land-21 : 0.000000000000000000
loadmodule-9 : 0.000000000000000000
multihop-7 : 0.414702410466252780
neptune-960 : 0.000000000000000000
nmap-231 : 0.000000000000000000
normal-960 : 0.000000000000000000
perl-3 : 0.000000000000000000
phf-4 : 0.000000000000000000
pod-264 : 0.000000000000000000
portsweep-1040 : 0.000000000000000000
rootkit-10 : 0.000000000000000000
satan-1589 : 0.000000000000000000
smurf-960 : 0.000000000000000000
spy-2 : 0.000000000000000000
teardrop-979 : 0.000000000000000000
warezclient-1020 : 0.000000000000000000
warezmaster-20 : 0.000000000000000000
```

```
r
0.01,0.50,0.86,0.90,0.00,0.00,0.00,0.00,0.00,0.50,0.00,1.00,0.04,1.00,0.00,0.05,0.14,0.50,0.25,0.00,0.00,0.00,0.00,0.00,0.00,0.00,1.00,0.00,0.00,0.00,0.00,1.00,0.00,1.00,0.00,0.00,0.00,0.00,0.00
back-1600 : 0.000000000000000000
buffer_overflow-30 : 0.000000000000000000
ftp_write-8 : 0.000000000000000000
guess_passwd-53 : 0.000000000000000000
imap-12 : 0.000000000000000000
ipsweep-1247 : 0.000000000000000000
land-21 : 0.000000000000000000
loadmodule-9 : 0.000000000000000000
multihop-7 : 0.345086233247635987
neptune-960 : 0.000000000000000000
nmap-231 : 0.000000000000000000
normal-960 : 0.000000000000000000
perl-3 : 0.000000000000000000
phf-4 : 0.000000000000000000
pod-264 : 0.000000000000000000
portsweep-1040 : 0.000000000000000000
rootkit-10 : 0.000000000000000000
satan-1589 : 0.000000000000000000
smurf-960 : 0.000000000000000000
spy-2 : 0.000000000000000000
teardrop-979 : 0.000000000000000000
warezclient-1020 : 0.000000000000000000
warezmaster-20 : 0.000000000000000000
```

Дійсно, мережа класифікує приклад з id = 53129 як warezmaster, не multihop.
Спробуємо «перенавчити» мережу, встановивши сігму рівній 0.001.

Результат роботи мережі, s = 0.001

Тренувальна вибірка:

t
Class: back-1600; eval: 1.0000000000000000000
Class: buffer_overflow-30; eval: 0.93333333333333334814
Class: ftp_write-8; eval: 1.0000000000000000000
Class: guess_passwd-53; eval: 1.0000000000000000000
Class: imap-12; eval: 1.0000000000000000000
Class: ipsweep-1247; eval: 1.0000000000000000000
Class: land-21; eval: 1.0000000000000000000
Class: loadmodule-9; eval: 1.0000000000000000000
Class: multihop-7; eval: 1.0000000000000000000
Class: neptune-960; eval: 0.95437499999999997335
Class: nmap-231; eval: 1.0000000000000000000
Class: normal-960; eval: 0.78812499999999996447
Class: perl-3; eval: 1.0000000000000000000
Class: phf-4; eval: 1.0000000000000000000
Class: pod-264; eval: 1.0000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 1.0000000000000000000
Class: satan-1589; eval: 1.0000000000000000000
Class: smurf-960; eval: 1.0000000000000000000
Class: spy-2; eval: 1.0000000000000000000
Class: teardrop-979; eval: 1.0000000000000000000
Class: warezclient-1020; eval: 1.0000000000000000000
Class: warezmaster-20; eval: 1.0000000000000000000
zero count: 0
time: 4.042179

Тестова вибірка:

v
Class: back-1600; eval: 1.0000000000000000000
Class: buffer_overflow-30; eval: 0.93333333333333334814
Class: ftp_write-8; eval: 1.0000000000000000000
Class: guess_passwd-53; eval: 1.0000000000000000000
Class: imap-12; eval: 1.0000000000000000000
Class: ipsweep-1247; eval: 1.0000000000000000000
Class: land-21; eval: 1.0000000000000000000
Class: loadmodule-9; eval: 1.0000000000000000000
Class: multihop-7; eval: 1.0000000000000000000
Class: neptune-960; eval: 0.87500000000000000000
Class: nmap-231; eval: 1.0000000000000000000
Class: normal-960; eval: 0.48249999999999998446
Class: perl-3; eval: 1.0000000000000000000
Class: phf-4; eval: 1.0000000000000000000
Class: pod-264; eval: 1.0000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 1.0000000000000000000
Class: satan-1589; eval: 1.0000000000000000000
Class: smurf-960; eval: 0.99750000000000005329
Class: spy-2; eval: 1.0000000000000000000
Class: teardrop-979; eval: 1.0000000000000000000
Class: warezclient-1020; eval: 1.0000000000000000000
Class: warezmaster-20; eval: 1.0000000000000000000
zero count: 0
time: 2.273892

Мережа змогла перенавчитись, для обох вибірок правильно класифікує всі приклади multihop. При цьому результати розпізнавання інших класів очікувано погіршились (клас normal (s = 0.01) t: 0.9575; v: 0.895 проти (s = 0.001) t: 0.7881; v: 0.4824 | клас neptune (s = 0.01) t: 0.9993; v: 0.9975 проти (s = 0.001) t: 0.9543; v: 0.8750).
Враховуючи кількість зразків класу normal (97277 у початковому датасеті), не має сенсу розпізнавати всі приклади multihop за рахунок 0.4824 правильних відповідей для класу normal.

Оберемо сігму рівній 0.1

Результат роботи мережі, s = 0.1

Тренувальна вибірка:

t
Class: back-1600; eval: 0.99875000000000002665
Class: buffer_overflow-30; eval: 0.76666666666666671848
Class: ftp_write-8; eval: 0.87500000000000000000
Class: guess_passwd-53; eval: 1.0000000000000000000
Class: imap-12; eval: 1.0000000000000000000
Class: ipsweep-1247; eval: 0.99438652766639934466
Class: land-21; eval: 1.0000000000000000000
Class: loadmodule-9; eval: 1.0000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-960; eval: 1.0000000000000000000
Class: nmap-231; eval: 0.98701298701298700866
Class: normal-960; eval: 0.80500000000000004885
Class: perl-3; eval: 1.0000000000000000000
Class: phf-4; eval: 1.0000000000000000000
Class: pod-264; eval: 1.0000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 0.80000000000000004441
Class: satan-1589; eval: 1.0000000000000000000
Class: smurf-960; eval: 1.0000000000000000000
Class: spy-2; eval: 1.0000000000000000000
Class: teardrop-979; eval: 1.0000000000000000000
Class: warezclient-1020; eval: 1.0000000000000000000
Class: warezmaster-20; eval: 1.0000000000000000000
zero count: 0
time: 2.449062

Тестова вибірка:

v
Class: back-1600; eval: 1.0000000000000000000
Class: buffer_overflow-30; eval: 0.76666666666666671848
Class: ftp_write-8; eval: 0.87500000000000000000
Class: guess_passwd-53; eval: 1.0000000000000000000
Class: imap-12; eval: 1.0000000000000000000
Class: ipsweep-1247; eval: 0.99438652766639934466
Class: land-21; eval: 1.0000000000000000000
Class: loadmodule-9; eval: 1.0000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-960; eval: 1.0000000000000000000
Class: nmap-231; eval: 0.98701298701298700866
Class: normal-960; eval: 0.76249999999999995559
Class: perl-3; eval: 1.0000000000000000000
Class: phf-4; eval: 1.0000000000000000000
Class: pod-264; eval: 1.0000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 0.80000000000000004441
Class: satan-1589; eval: 1.0000000000000000000
Class: smurf-960; eval: 1.0000000000000000000
Class: spy-2; eval: 1.0000000000000000000
Class: teardrop-979; eval: 1.0000000000000000000
Class: warezclient-1020; eval: 1.0000000000000000000
Class: warezmaster-20; eval: 1.0000000000000000000
zero count: 0
time: 1.756200

Мережа є більш точною при s = 0.1 аніж при s = 0.001. При цьому результати для s = 0.1 гірші за результати для s = 0.01 (наприклад клас buffer_overflow (s = 0.1) t: 0.7666; v: 0.7666 проти (s = 0.01) t: 0.9000; v: 0.9000).
Отже оптимальна сігма знаходиться в межах (0.01; 0.1).

Протестуємо мережу для значень сігми (0.015, 0.025, 0.035, 0.045):

s = 0.015

t
Class: back-1600; eval: 1.0000000000000000000
Class: buffer_overflow-30; eval: 0.90000000000000002220
Class: ftp_write-8; eval: 0.87500000000000000000
Class: guess_passwd-53; eval: 1.00000000000000000000
Class: imap-12; eval: 1.00000000000000000000
Class: ipsweep-1247; eval: 1.00000000000000000000
Class: land-21; eval: 1.00000000000000000000
Class: loadmodule-9; eval: 1.00000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-960; eval: 0.99937500000000001332
Class: nmap-231; eval: 0.98701298701298700866
Class: normal-960; eval: 0.96937499999999998668
Class: perl-3; eval: 1.00000000000000000000
Class: phf-4; eval: 1.00000000000000000000
Class: pod-264; eval: 1.00000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 0.90000000000000002220
Class: satan-1589; eval: 1.00000000000000000000
Class: smurf-960; eval: 1.00000000000000000000
Class: spy-2; eval: 1.00000000000000000000
Class: teardrop-979; eval: 1.00000000000000000000
Class: warezclient-1020; eval: 1.00000000000000000000
Class: warezmaster-20; eval: 1.00000000000000000000
zero count: 0
time: 3.141179

v
Class: back-1600; eval: 1.00000000000000000000
Class: buffer_overflow-30; eval: 0.90000000000000002220
Class: ftp_write-8; eval: 0.87500000000000000000
Class: guess_passwd-53; eval: 1.00000000000000000000
Class: imap-12; eval: 1.00000000000000000000
Class: ipsweep-1247; eval: 1.00000000000000000000
Class: land-21; eval: 1.00000000000000000000
Class: loadmodule-9; eval: 1.00000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-960; eval: 1.00000000000000000000
Class: nmap-231; eval: 0.98701298701298700866
Class: normal-960; eval: 0.92500000000000004441
Class: perl-3; eval: 1.00000000000000000000
Class: phf-4; eval: 1.00000000000000000000
Class: pod-264; eval: 1.00000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 0.90000000000000002220
Class: satan-1589; eval: 1.00000000000000000000
Class: smurf-960; eval: 1.00000000000000000000
Class: spy-2; eval: 1.00000000000000000000
Class: teardrop-979; eval: 1.00000000000000000000
Class: warezclient-1020; eval: 1.00000000000000000000
Class: warezmaster-20; eval: 1.00000000000000000000
zero count: 0
time: 2.272826

s = 0.025

t
Class: back-1600; eval: 0.99937500000000001332
Class: buffer_overflow-30; eval: 0.90000000000000002220
Class: ftp_write-8; eval: 0.87500000000000000000
Class: guess_passwd-53; eval: 1.00000000000000000000
Class: imap-12; eval: 1.00000000000000000000
Class: ipsweep-1247; eval: 0.99919807538091420795
Class: land-21; eval: 1.00000000000000000000
Class: loadmodule-9; eval: 1.00000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-960; eval: 1.00000000000000000000
Class: nmap-231; eval: 0.97835497835497831076
Class: normal-960; eval: 0.97624999999999995115
Class: perl-3; eval: 1.00000000000000000000
Class: phf-4; eval: 1.00000000000000000000
Class: pod-264; eval: 1.00000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 0.90000000000000002220
Class: satan-1589; eval: 1.00000000000000000000
Class: smurf-960; eval: 1.00000000000000000000
Class: spy-2; eval: 1.00000000000000000000
Class: teardrop-979; eval: 1.00000000000000000000
Class: warezclient-1020; eval: 1.00000000000000000000
Class: warezmaster-20; eval: 1.00000000000000000000
zero count: 0
time: 3.096189

v
Class: back-1600; eval: 1.00000000000000000000
Class: buffer_overflow-30; eval: 0.90000000000000002220
Class: ftp_write-8; eval: 0.87500000000000000000
Class: guess_passwd-53; eval: 1.00000000000000000000
Class: imap-12; eval: 1.00000000000000000000
Class: ipsweep-1247; eval: 0.99919807538091420795
Class: land-21; eval: 1.00000000000000000000
Class: loadmodule-9; eval: 1.00000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-960; eval: 1.00000000000000000000
Class: nmap-231; eval: 0.97835497835497831076
Class: normal-960; eval: 0.93500000000000005329
Class: perl-3; eval: 1.00000000000000000000
Class: phf-4; eval: 1.00000000000000000000
Class: pod-264; eval: 1.00000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 0.90000000000000002220
Class: satan-1589; eval: 1.00000000000000000000
Class: smurf-960; eval: 1.00000000000000000000
Class: spy-2; eval: 1.00000000000000000000
Class: teardrop-979; eval: 1.00000000000000000000
Class: warezclient-1020; eval: 1.00000000000000000000
Class: warezmaster-20; eval: 1.00000000000000000000
zero count: 0
time: 2.230893

s = 0.035

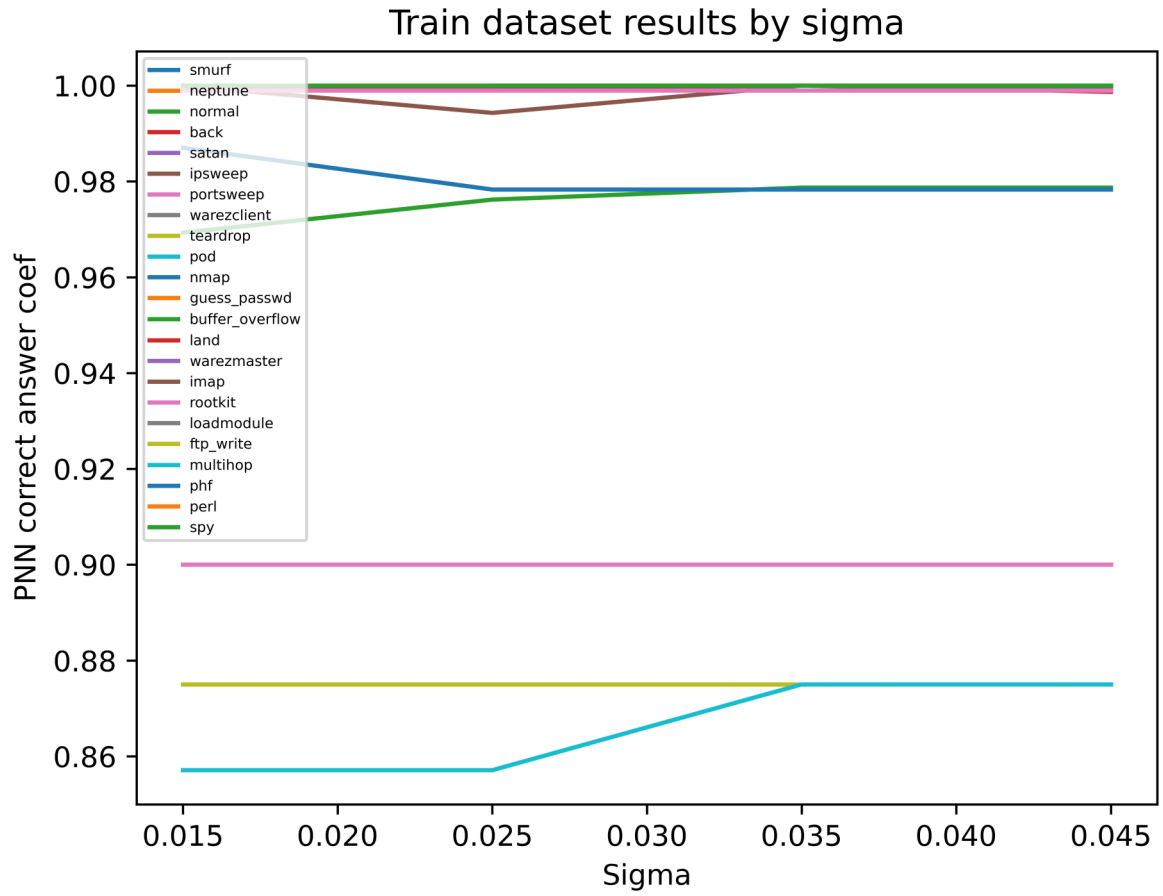
t
Class: back-1600; eval: 1.0000000000000000000
Class: buffer_overflow-30; eval: 0.90000000000000002220
Class: ftp_write-8; eval: 0.87500000000000000000
Class: guess_passwd-53; eval: 1.00000000000000000000
Class: imap-12; eval: 1.00000000000000000000
Class: ipsweep-1247; eval: 0.99759422614274262386
Class: land-21; eval: 1.00000000000000000000
Class: loadmodule-9; eval: 1.00000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-960; eval: 1.00000000000000000000
Class: nmap-231; eval: 0.97835497835497831076
Class: normal-960; eval: 0.97875000000000000888
Class: perl-3; eval: 1.00000000000000000000
Class: phf-4; eval: 1.00000000000000000000
Class: pod-264; eval: 1.00000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 0.90000000000000002220
Class: satan-1589; eval: 1.00000000000000000000
Class: smurf-960; eval: 1.00000000000000000000
Class: spy-2; eval: 1.00000000000000000000
Class: teardrop-979; eval: 1.00000000000000000000
Class: warezclient-1020; eval: 1.00000000000000000000
Class: warezmaster-20; eval: 1.00000000000000000000
zero count: 0
time: 3.171035

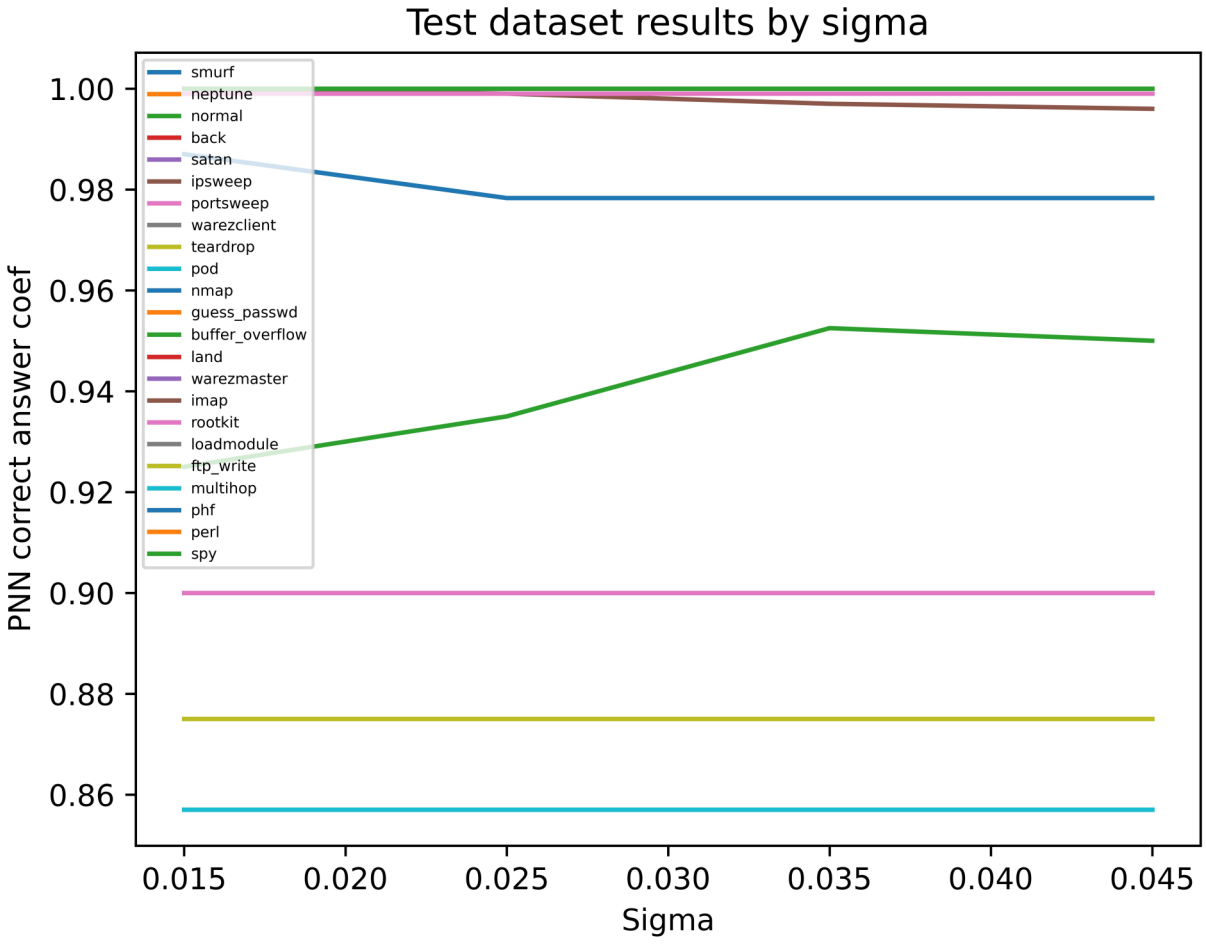
v
Class: back-1600; eval: 1.0000000000000000000
Class: buffer_overflow-30; eval: 0.90000000000000002220
Class: ftp_write-8; eval: 0.87500000000000000000
Class: guess_passwd-53; eval: 1.00000000000000000000
Class: imap-12; eval: 1.00000000000000000000
Class: ipsweep-1247; eval: 0.99759422614274262386
Class: land-21; eval: 1.00000000000000000000
Class: loadmodule-9; eval: 1.00000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-960; eval: 1.00000000000000000000
Class: nmap-231; eval: 0.97835497835497831076
Class: normal-960; eval: 0.95250000000000001332
Class: perl-3; eval: 1.00000000000000000000
Class: phf-4; eval: 1.00000000000000000000
Class: pod-264; eval: 1.00000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 0.90000000000000002220
Class: satan-1589; eval: 1.00000000000000000000
Class: smurf-960; eval: 1.00000000000000000000
Class: spy-2; eval: 1.00000000000000000000
Class: teardrop-979; eval: 1.00000000000000000000
Class: warezclient-1020; eval: 1.00000000000000000000
Class: warezmaster-20; eval: 1.00000000000000000000
zero count: 0
time: 2.225466

s = 0.045

t
Class: back-1600; eval: 0.99875000000000002665
Class: buffer_overflow-30; eval: 0.90000000000000002220
Class: ftp_write-8; eval: 0.87500000000000000000
Class: guess_passwd-53; eval: 1.00000000000000000000
Class: imap-12; eval: 1.00000000000000000000
Class: ipsweep-1247; eval: 0.99679230152365672080
Class: land-21; eval: 1.00000000000000000000
Class: loadmodule-9; eval: 1.00000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-960; eval: 1.00000000000000000000
Class: nmap-231; eval: 0.97835497835497831076
Class: normal-960; eval: 0.97812500000000002220
Class: perl-3; eval: 1.00000000000000000000
Class: phf-4; eval: 1.00000000000000000000
Class: pod-264; eval: 1.00000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 0.90000000000000002220
Class: satan-1589; eval: 1.00000000000000000000
Class: smurf-960; eval: 1.00000000000000000000
Class: spy-2; eval: 1.00000000000000000000
Class: teardrop-979; eval: 1.00000000000000000000
Class: warezclient-1020; eval: 1.00000000000000000000
Class: warezmaster-20; eval: 1.00000000000000000000
zero count: 0
time: 3.217059

v
Class: back-1600; eval: 1.0000000000000000000
Class: buffer_overflow-30; eval: 0.90000000000000002220
Class: ftp_write-8; eval: 0.87500000000000000000
Class: guess_passwd-53; eval: 1.00000000000000000000
Class: imap-12; eval: 1.00000000000000000000
Class: ipsweep-1247; eval: 0.99679230152365672080
Class: land-21; eval: 1.00000000000000000000
Class: loadmodule-9; eval: 1.00000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-960; eval: 1.00000000000000000000
Class: nmap-231; eval: 0.97835497835497831076
Class: normal-960; eval: 0.94999999999999995559
Class: perl-3; eval: 1.00000000000000000000
Class: phf-4; eval: 1.00000000000000000000
Class: pod-264; eval: 1.00000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 0.90000000000000002220
Class: satan-1589; eval: 1.00000000000000000000
Class: smurf-960; eval: 1.00000000000000000000
Class: spy-2; eval: 1.00000000000000000000
Class: teardrop-979; eval: 1.00000000000000000000
Class: warezclient-1020; eval: 1.00000000000000000000
Class: warezmaster-20; eval: 1.00000000000000000000
zero count: 0
time: 2.195528


Train dataset results by sigma
smurf
neptune
normal
back
satan
ipsweep
portsweep
warezclient
teardrop
pod
nmap
guess_passwd
buffer_overflow
land
warezmaster
imap
rootkit
loadmodule
ftp_write
multihop
phf
perl
spy
PNN correct answer coef
1.00
0.98
0.96
0.94
0.92
0.90
0.88
0.86
0.015
0.020
0.025
0.030
0.035
0.040
0.045
Sigma


Test dataset results by sigma
smurf
neptune
normal
back
satan
ipsweep
portsweep
warezclient
teardrop
pod
nmap
guess_passwd
buffer_overflow
land
warezmaster
imap
rootkit
loadmodule
ftp_write
multihop
phf
perl
spy
PNN correct answer coef
1.00
0.98
0.96
0.94
0.92
0.90
0.88
0.86
0.015
0.020
0.025
0.030
0.035
0.040
0.045
Sigma

Виходячи з наведених графіків, в якості оптимального значення сігми було обрано 0.035.
Протестуємо мережу на всьому датасеті:

v
Class: back-1600; eval: 1.0000000000000000000
Class: buffer_overflow-30; eval: 0.90000000000000002220
Class: ftp_write-8; eval: 0.87500000000000000000
Class: guess_passwd-53; eval: 1.00000000000000000000
Class: imap-12; eval: 1.00000000000000000000
Class: ipsweep-1247; eval: 0.99759422614274262386
Class: land-21; eval: 1.00000000000000000000
Class: loadmodule-9; eval: 1.00000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-960; eval: 0.99978544976259553501
Class: nmap-231; eval: 0.97835497835497831076
Class: normal-960; eval: 0.95845883405121456988
Class: perl-3; eval: 1.00000000000000000000
Class: phf-4; eval: 1.00000000000000000000
Class: pod-264; eval: 1.00000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 0.90000000000000002220
Class: satan-1589; eval: 1.00000000000000000000
Class: smurf-960; eval: 0.99919868941201606116
Class: spy-2; eval: 1.00000000000000000000
Class: teardrop-979; eval: 1.00000000000000000000
Class: warezclient-1020; eval: 1.00000000000000000000
Class: warezmaster-20; eval: 1.00000000000000000000
zero count: 0
time: 143.127316

На всіх класах, крім ftp_write, multihop, buffer_overflow, rootkit маємо точність, більшу за 95%. На інших класах точність є не меншою за 85%.
Окремо варто виділити той факт, що тестування мережі, загальна кількість зразків в якій дорівнює 11029, на датасеті розміром 494020 зразків, зайняло всього лиш ~143 секунди.

В оригінальному датасеті клас normal містить 97277 зразків. Клас normal відповідає нормальному трафіку. В наведеній нейронній мережі наявно лише 960 зразків класу normal. Значення характеристик зразків, що належать класу normal, можуть сильно варіюватись, оскільки характер «нормального» трафіку визначається лише діями користувачів. Збільшимо кількість зразків класу normal до 3600 (за рахунок зміни значення REAL_DATA_COUNT_PER_CLASS, зміна цього параметра також впливає на кількість прикладів у pnn для інших класів).

Параметри генерації даних:
```
PNN_REFERENCE_COUNT_BY_CLASS = {
    "smurf":          0.6,
    "neptune":        0.6,
    "normal":         0.6,
    "back":           1.0,
    "satan":          1.0,
    "ipsweep":        1.0,
    "portsweep":      1.0,
    "warezclient":    1.0,
    "teardrop":       1.0,
    "pod":            1.0,
    "nmap":           1.0,
    "guess_passwd":   1.0,
    "buffer_overflow": 1.0,
    "land":           1.0,
    "warezmaster":    1.0,
    "imap":           1.0,
    "rootkit":        1.0,
    "loadmodule":     1.0,
    "ftp_write":      1.0,
    "multihop":       1.0,
    "phf":            1.0,
    "perl":           1.0,
    "spy":            1.0
}
TEST_SIZE = 0.25
REAL_DATA_COUNT_PER_CLASS = 8000
RANDOM_STATE_1 = 1450
```

v
Class: back-2203; eval: 0.99954607353608715403
Class: buffer_overflow-30; eval: 0.90000000000000002220
Class: ftp_write-8; eval: 0.87500000000000000000
Class: guess_passwd-53; eval: 1.00000000000000000000
Class: imap-12; eval: 1.00000000000000000000
Class: ipsweep-1247; eval: 0.99759422614274262386
Class: land-21; eval: 1.00000000000000000000
Class: loadmodule-9; eval: 1.00000000000000000000
Class: multihop-7; eval: 0.85714285714285709528
Class: neptune-3600; eval: 0.99977612149140404618
Class: nmap-231; eval: 0.97835497835497831076
Class: normal-3600; eval: 0.98229797382731787181
Class: perl-3; eval: 1.00000000000000000000
Class: phf-4; eval: 1.00000000000000000000
Class: pod-264; eval: 1.00000000000000000000
Class: portsweep-1040; eval: 0.99903846153846154188
Class: rootkit-10; eval: 0.90000000000000002220
Class: satan-1589; eval: 0.99937067337948393142
Class: smurf-3600; eval: 0.99949784536486341313
Class: spy-2; eval: 1.00000000000000000000
Class: teardrop-979; eval: 1.00000000000000000000
Class: warezclient-1020; eval: 1.00000000000000000000
Class: warezmaster-20; eval: 1.00000000000000000000
zero count: 0
time: 240.441858

Спостерігаємо очікуване покращення результату для класу normal:
0.98229797382731787181 (3600 зразків normal) проти 0.95845883405121456988 (960 зразків normal).

Текстове представлення остаточної мережі—файл pnn-8000.txt у репозиторії.

Варто зауважити, що мережа помилково розпізнає деякі приклади класів малої розмірності (buffer_overflow, ftp_write, multihop, rootkit). В роботі було показано що показники розпізнавання таких класів можна покращити, значно зменшивши сігму. Але в такому випадку значно погіршуються показники «основних» класів.

Лог процесу навчання—файл report-session.txt у репозиторії.

Окремо хотілось виділити швидкодію мережі:
Розпізнавання 494020 зразків мережею, що містить 11029 зразків, займає 143 секунди. Розпізнавання одного зразка— ~1.5 мілісекунд.
Розпізнавання 494020 зразків мережею, що містить 19552 зразків, займає 240 секунди. Розпізнавання одного зразка— ~2.8 мілісекунд.

Тестування здійснювалось на процесорі Intel Core I5-8250U (1.6GHz—3.4GHz, 4 cores / 8 threads).

Таким чином використання мови C та технології OpenMP для реалізації мережі є виправданим.

p.s.

Як виявилось, за посиланням Kddcup99 - Dataset - DataHub - Frictionless Data—лише вибірка розміром 10% із оригінального датасету KDD99. Оригінальний датасет Kdd99 можна знайти за посиланням: KDD Cup 1999 Data (uci.edu). Цей датасет містить 4898431 зразків.
Кількість зразків кожного класу в датасеті:

```
>>> Class | Count >>>
label
smurf              2807886
neptune            1072017
normal              972781
satan                15892
ipsweep              12481
portsweep            10413
nmap                  2316
back                  2203
warezclient           1020
teardrop               979
pod                    264
guess_passwd            53
buffer_overflow         30
land                    21
warezmaster             20
imap                    12
rootkit                 10
loadmodule               9
ftp_write                8
multihop                 7
phf                      4
perl                     3
spy                      2
Name: count, dtype: int64
```

Протестуємо остаточну мережу (представлення—файл pnn-8000.txt у репозиторії) на всіх ~4.8M прикладів. Результат:

```
v
Class: back-2203; eval: 0.99773036768043577016
Class: buffer_overflow-30; eval: 0.86666666666666669627
Class: ftp_write-8; eval: 0.87500000000000000000
Class: guess_passwd-53; eval: 1.00000000000000000000
Class: imap-12; eval: 1.00000000000000000000
Class: ipsweep-1247; eval: 0.99679512859546515191
Class: land-21; eval: 1.00000000000000000000
Class: loadmodule-9; eval: 1.00000000000000000000
Class: multihop-7; eval: 0.71428571428571430157
Class: neptune-3600; eval: 0.99978171987944219889
Class: nmap-231; eval: 0.96243523316062173922
Class: normal-3600; eval: 0.98279880055223123314
Class: perl-3; eval: 1.00000000000000000000
Class: phf-4; eval: 1.00000000000000000000
Class: pod-264; eval: 1.00000000000000000000
Class: portsweep-1040; eval: 0.99654278305963694962
Class: rootkit-10; eval: 0.90000000000000002220
Class: satan-1589; eval: 0.99496602063931538495
Class: smurf-3600; eval: 0.99951743055095543244
Class: spy-2; eval: 1.00000000000000000000
Class: teardrop-979; eval: 1.00000000000000000000
Class: warezclient-1020; eval: 0.85882352941176465233
Class: warezmaster-20; eval: 1.00000000000000000000
zero count: 0
time: 2349.750440
```

Точність розпізнавання прикладів мережею є задовільна: для більшості класів точність є більшою за 95%. Винятком є класи ftp_write, multihop, warezclient.
В якості подальших покращень можна запропонувати незначно збільшити кількість зразків класу warezclient в мережі. Враховуючи, що всі приклади класів ftp_write та multihop наявні в мережі (7 та 8 прикладів відповідно), покращити результати розпізнавання цих класів можна лише зменшивши сігму—але тоді значно погіршаться показники інших класів.

Окремо варто відмітити, що мережа розміром 19552 зразків розпізнала ~4.8M прикладів за 2349.750440 / 60 = ~39.16 хвилин.