Система виявлення атак в комп'ютерних мережах на основі методів машинного навчання

Підготувала студентка 4 курсу КІ
Якушина Анастасія Олексіївна
Керівник: к.ф.-м.н., доц. Шпінарева І.М.

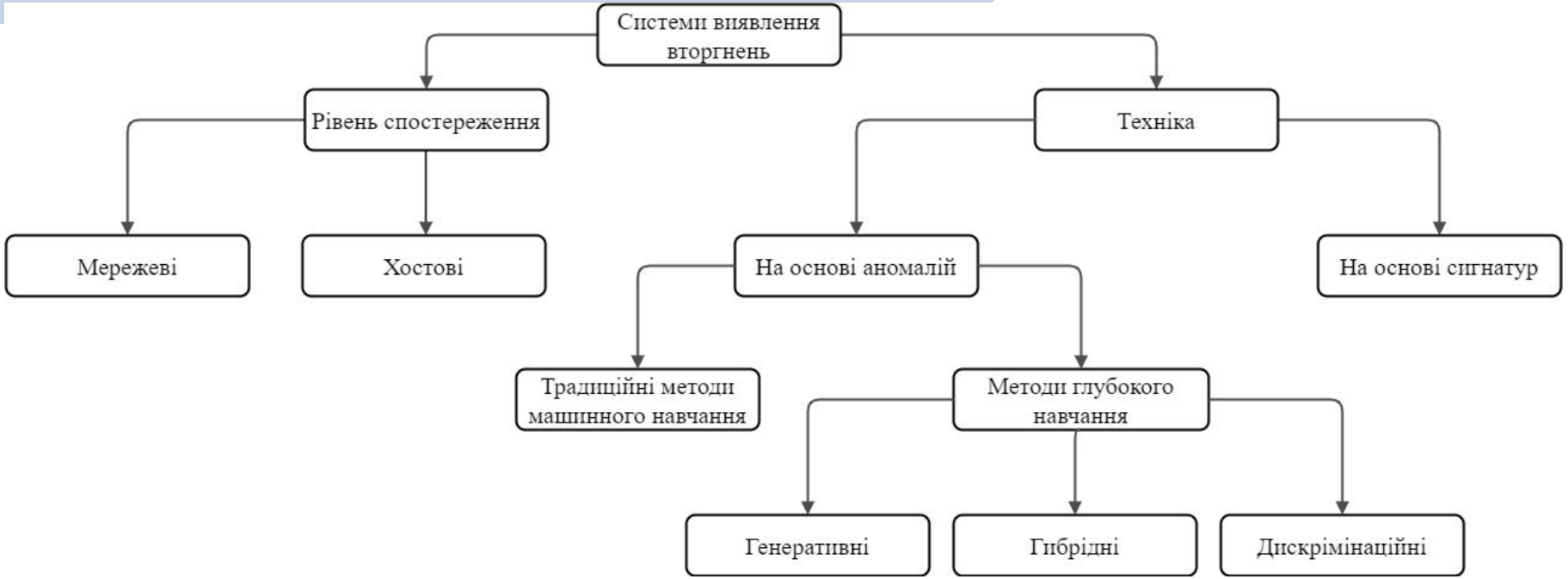
Мета роботи

створення системи виявлення атак (IDS) в комп’ютерних мережах з використанням методів машинного навчання

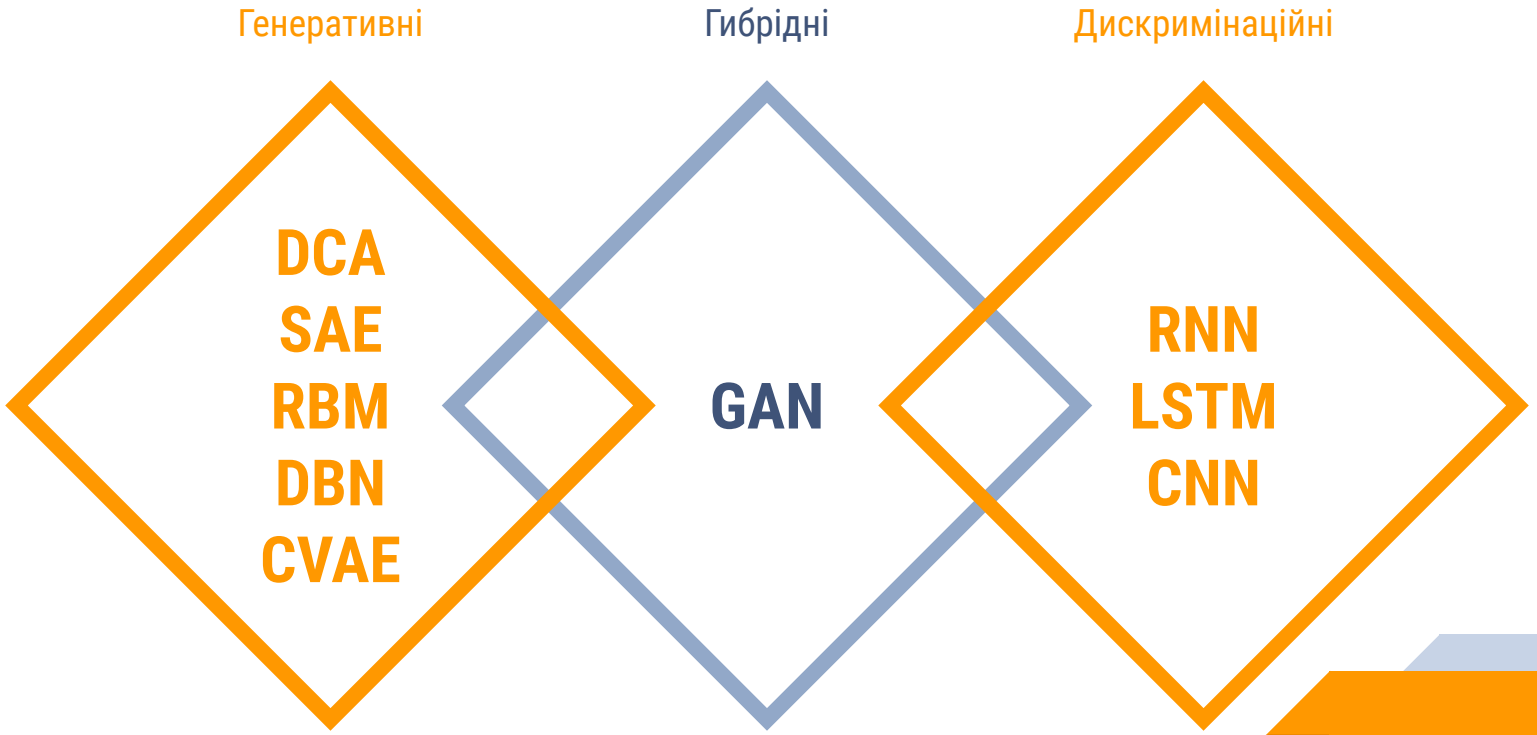
Задачі, які необхідно вирішити

- дослідження методів виявлення атак і їх характеристики;
- формування вимог до створюваного системи;
- вибір архітектури, технологій і засобів реалізації системи;
- реалізація алгоритму виявлення атак;
- реалізація системи виявлення атак;
- тестування обраного алгоритму на тестовій виборці;
- тестування системи в режимі реального часу.

Класифікація IDS та методів машинного навчання для виявлення вторгнень



Приклади методів глибокого навчання, що використовуються в сфері виявлення аномалій



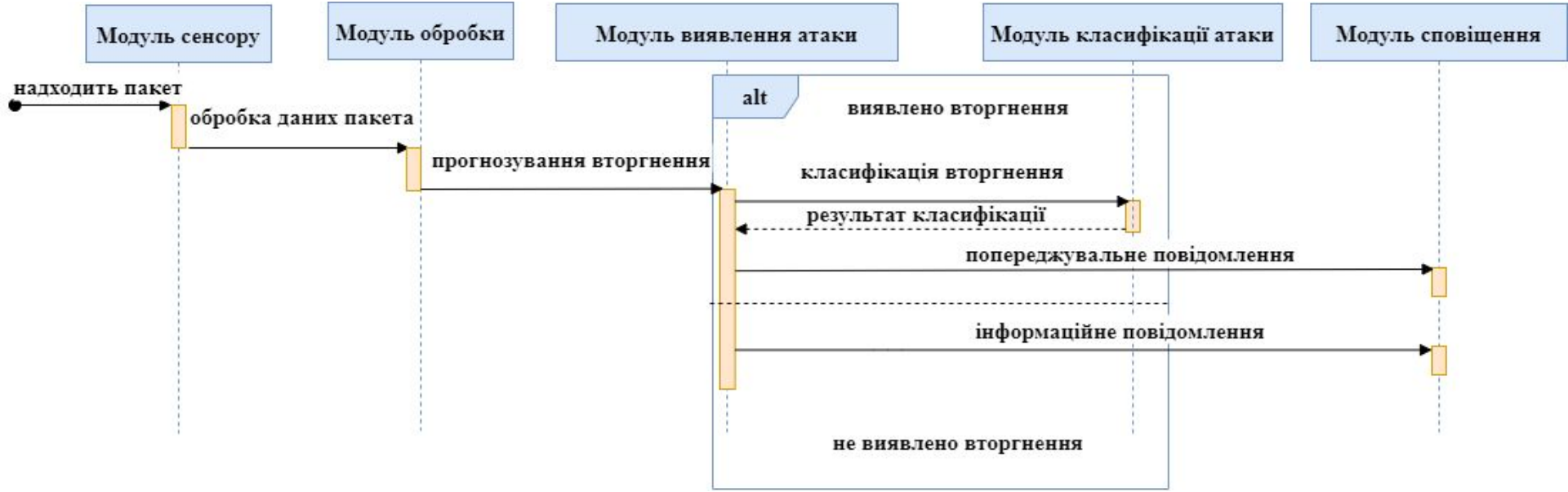
ПОРІВНЯННЯ ІСНУЮЧИХ IDS

	Методи виявлення			Рівень спостереження	
	Сигнатурний	Статистичний	Машинне навчання	Системний	Мережевий
Snort	✓	✓	✗	✗	✓
Suricata	✓	✗	✗	✗	✓
Bro	✓	✓	✗	✗	✓
OSSEC	✓	✗	✗	✓	✗

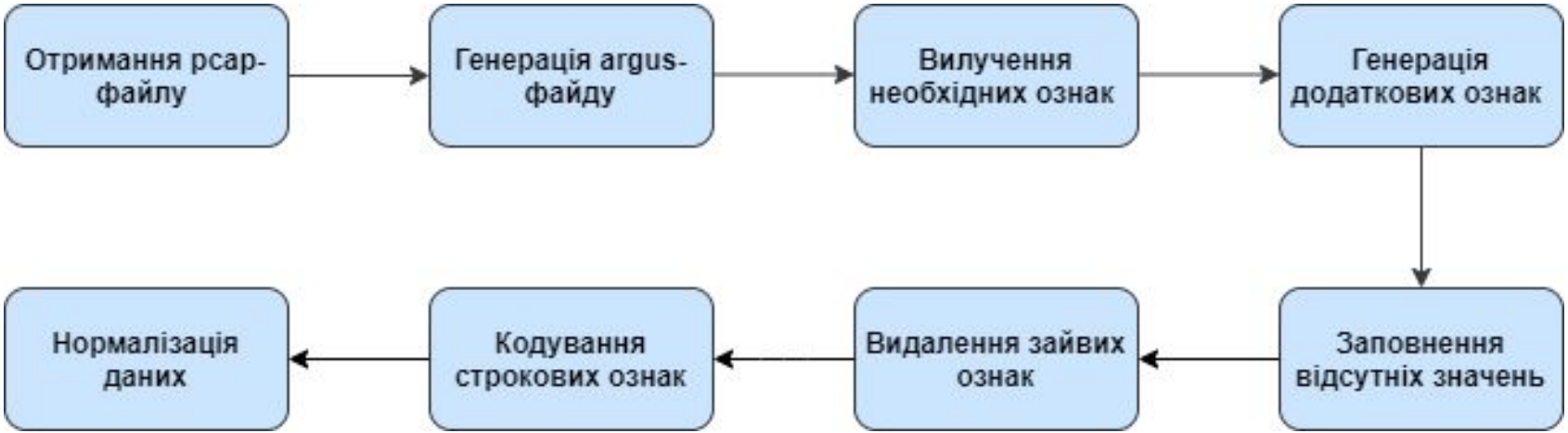
Вимоги до системи IDS

- система повинна виявляти атаки в режимі реального часу;
- виявляти погрозу застосовуючи методи аномалій;
- мати низьку ймовірність помилково-позитивних та помилково-негативних результатів;
- вміти виявляти нові різновидності атак;
- відображати результати аналізу мережевого трафіку.

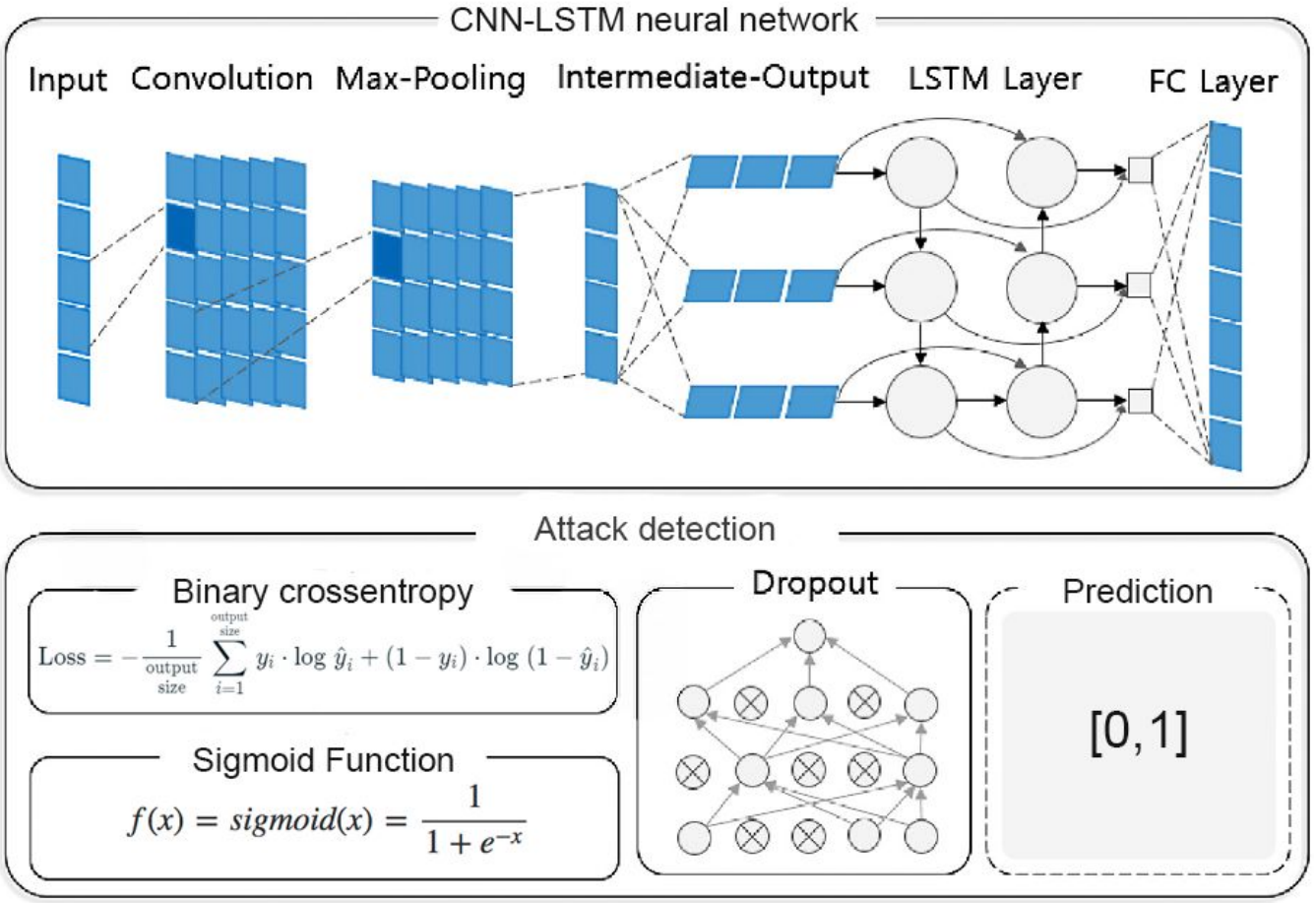
ДІАГРАМА ПОСЛІДОВНОСТІ СИСТЕМИ

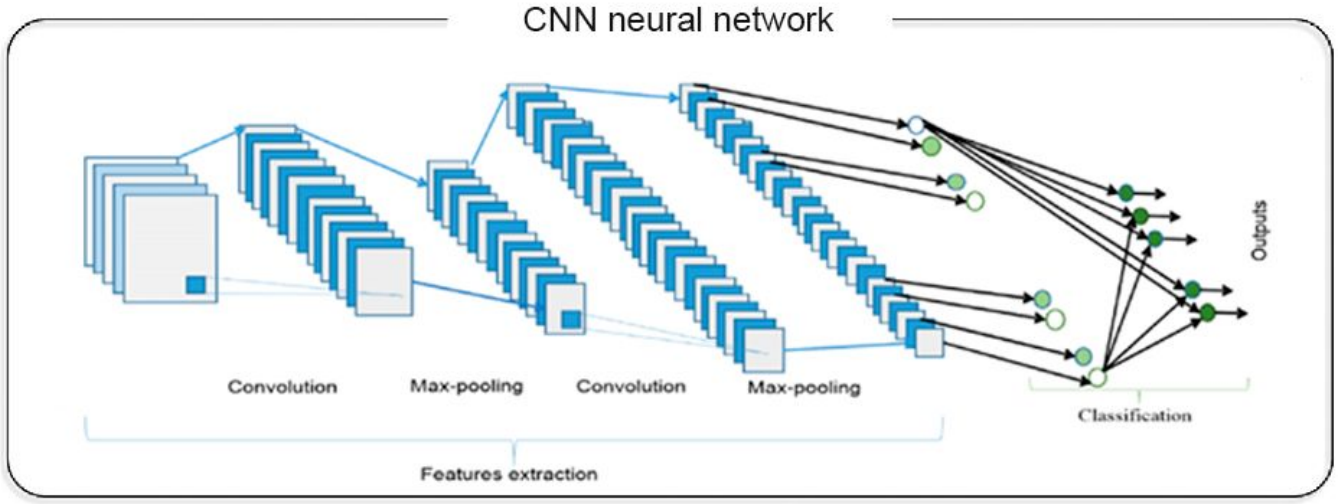


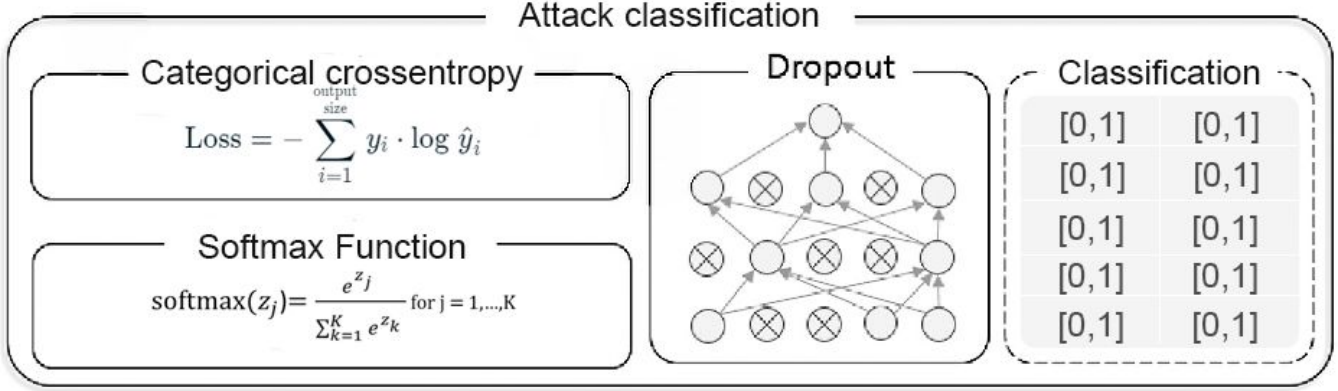
МОДУЛЬ ОБРОБКИ



- В результаті всіх перетворень на виході отримуємо вектор, що містить 176 атрибутів


CNN-LSTM neural network
Input
Convolution
Max-Pooling
Intermediate-Output
LSTM Layer
FC Layer
Attack detection
Binary crossentropy
$\text{Loss} = -\frac{1}{\text{output size}} \sum_{i=1}^{\text{output size}} y_i \cdot \log \hat{y}_i + (1 - y_i) \cdot \log (1 - \hat{y}_i)$
Sigmoid Function
$f(x) = sigmoid(x) = \frac{1}{1 + e^{-x}}$
Dropout
Prediction
[0,1]





Типи атак:

Fuzzers,
Analysis,
Backdoor,
DoS,
Exploits,
Generic,
Reconnaissance,
Shellcode,
Worm.

UNSW-NB15

2 540 044 записів

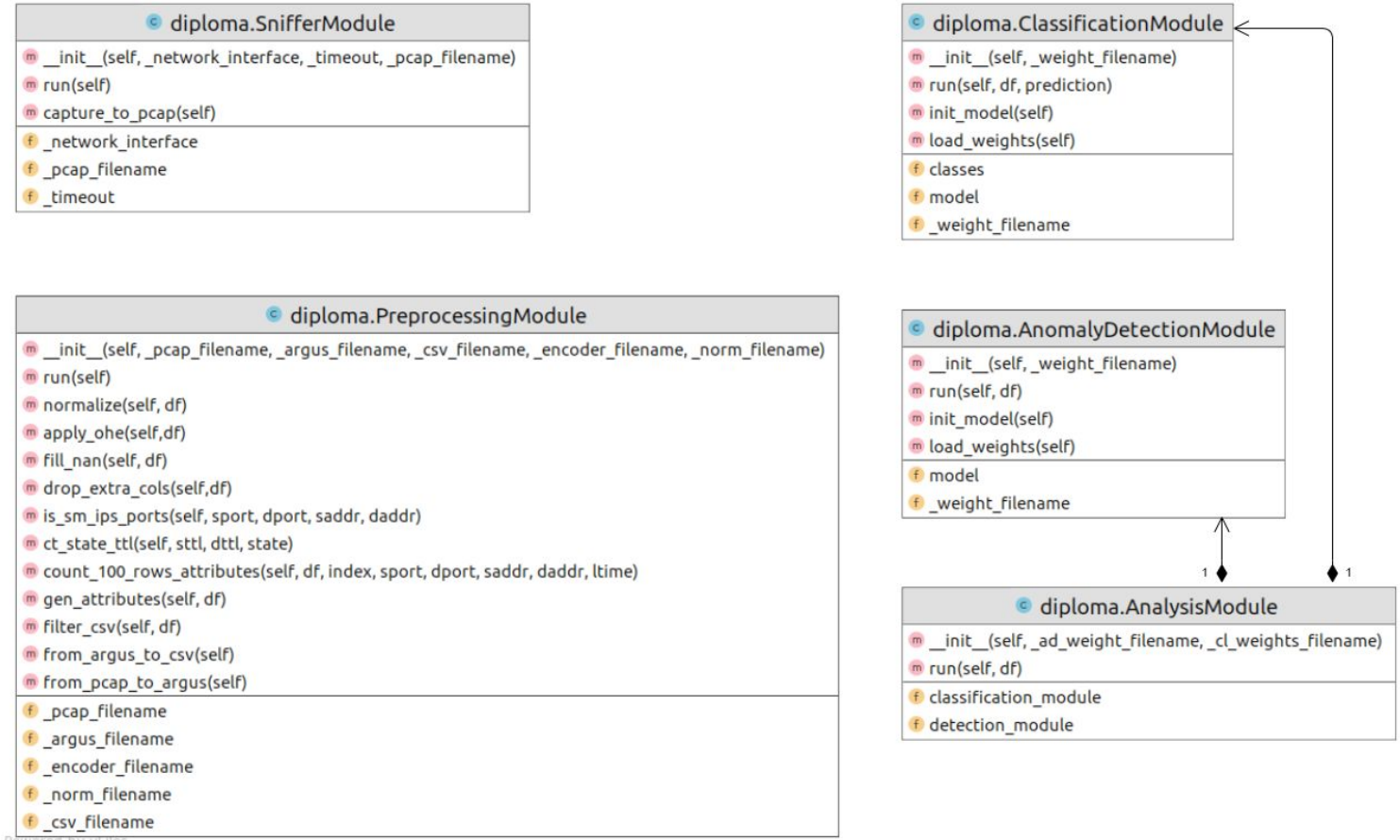
No.	Назва	Тип	Опис
1	srcip	nominal	IP-адрес відправника
2	sport	integer	Номер порту відправника
3	dstip	nominal	IP-адрес одержувача
4	dsport	integer	Номер порту одержувача
5	proto	nominal	Протокол транзакції
6	state	nominal	Вказує на стан і залежний від нього протокол
...	...		
48	attack_cat	nominal	Назва категорії атаки. У цьому наборі даних дев'ять категорій атак: Fuzzers, Analysis, Backdoors, DoS Exploits, Generic, Reconnaissance, Shellcode и Worms
49	Label	binary	0 для нормальних записів і 1 для атак

The UNSW-NB15 Dataset: https://researchdata.edu.au/unsw-nb15-dataset/1425943

ЗАСОБИ РЕАЛІЗАЦІЇ

Для розробки системи виявлення атак використані наступні інструменти:

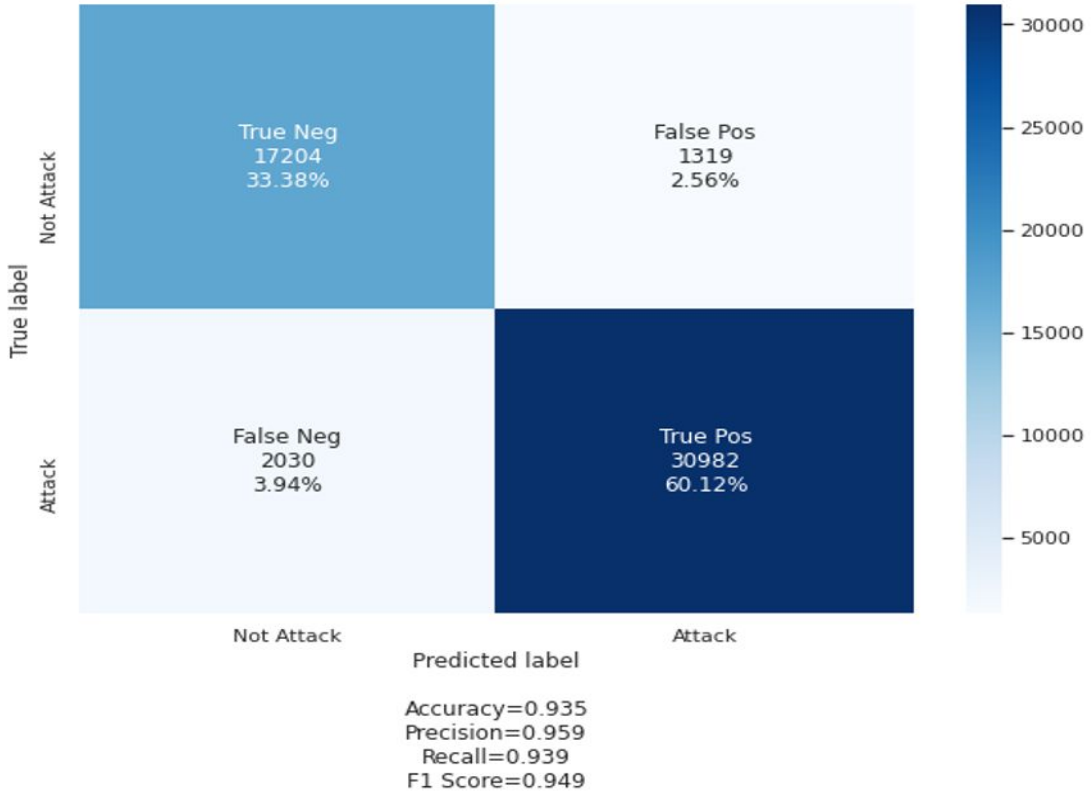
- сніфер - Tshark ;
- язик программування - Python;
- у модулі обробки даних використана:
  - утиліта - Argus,
  - бібліотеки: Numpy, Pandas, Scikit-learn;
- бібліотека для побудови НМ - Keras.



Діаграма класів

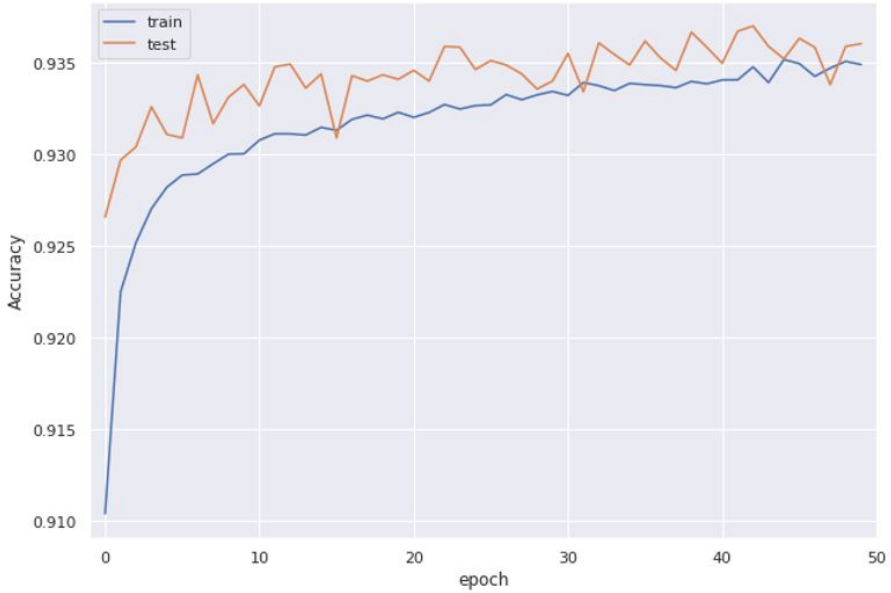
Оцінка ефективності нейронних мереж

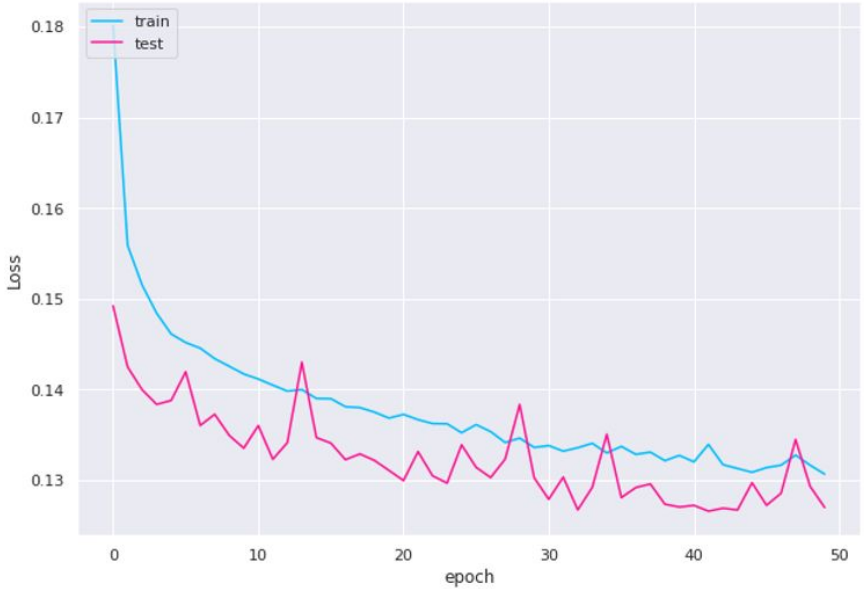
Матриця неточностей - це таблиця, яка дозволяє візуалізувати ефективність алгоритму класифікації шляхом порівняння прогнозованого значення цільової змінної з її фактичним значенням.



		Фактичні	
		Негативні	Позитивні
Предска-зані	Негативні	TN	FP
	Позитивні	FN	TP

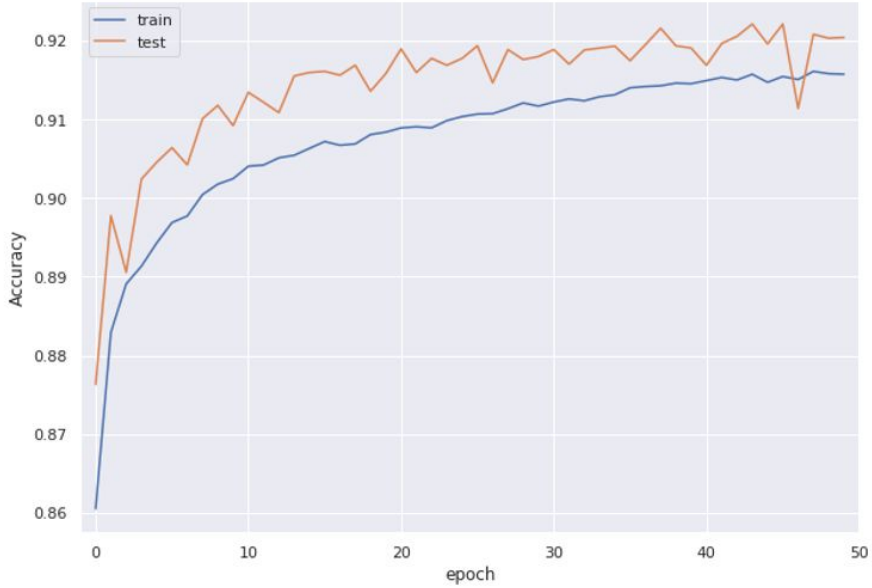
Значення показників точності та функції втрат під час тренування нейронної мережі модуля виявлення атаки

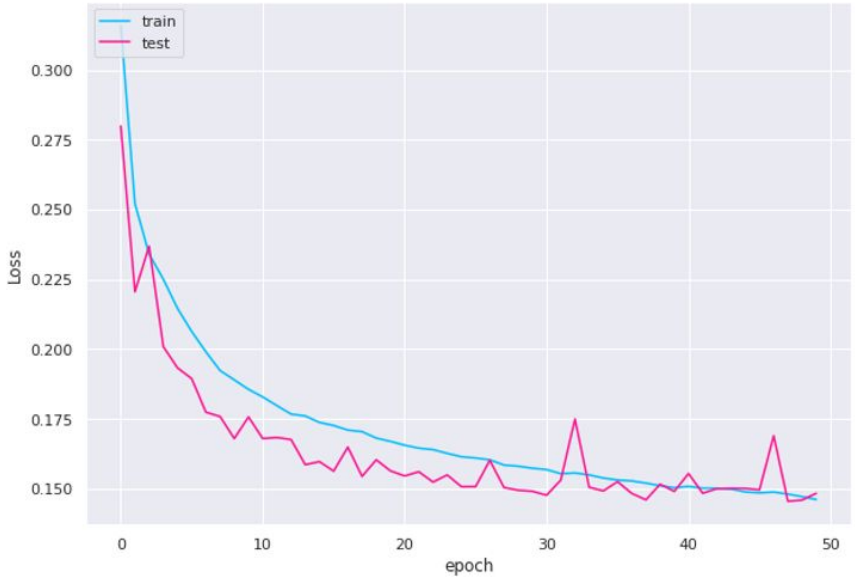




$$Accuracy = (TN + TP)/(TP + FP + TN + FN)$$

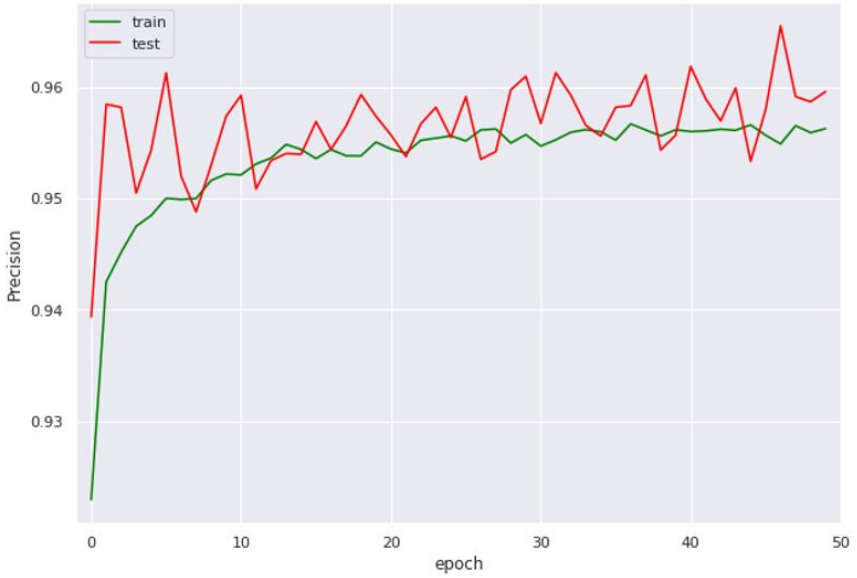
Значення показників точності та функції втрат під час тренування нейронної мережі модуля класифікації атаки

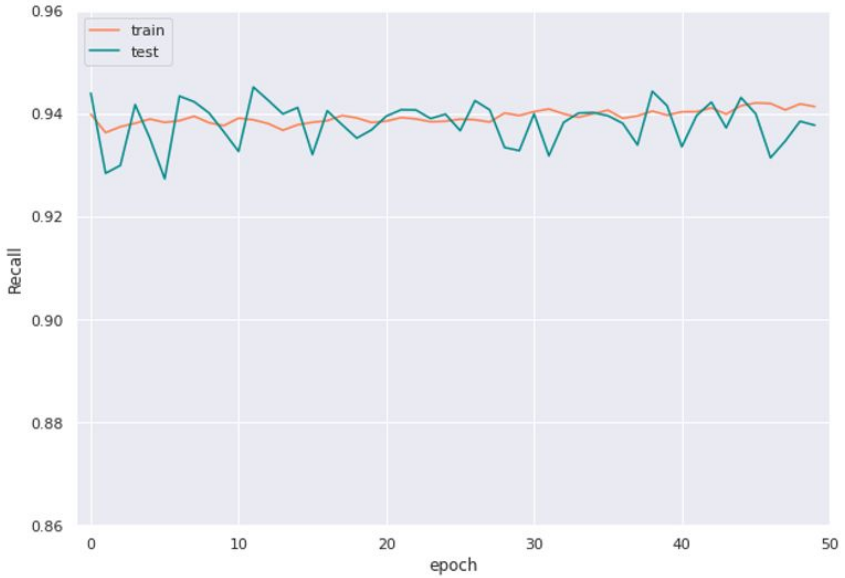




$$Accuracy = (TN + TP)/(TP + FP + TN + FN)$$

Значення показників Precision та Recall під час тренування нейронної мережі модуля виявлення атаки

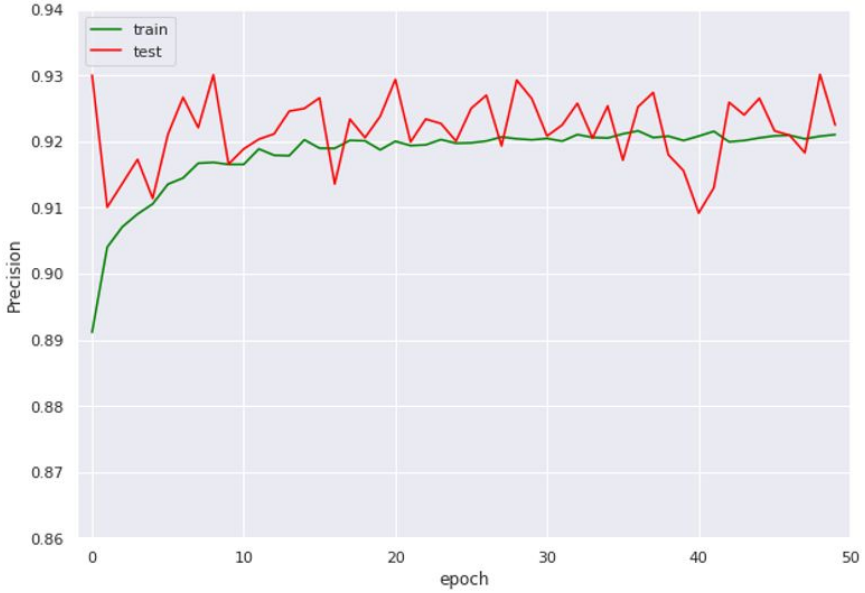


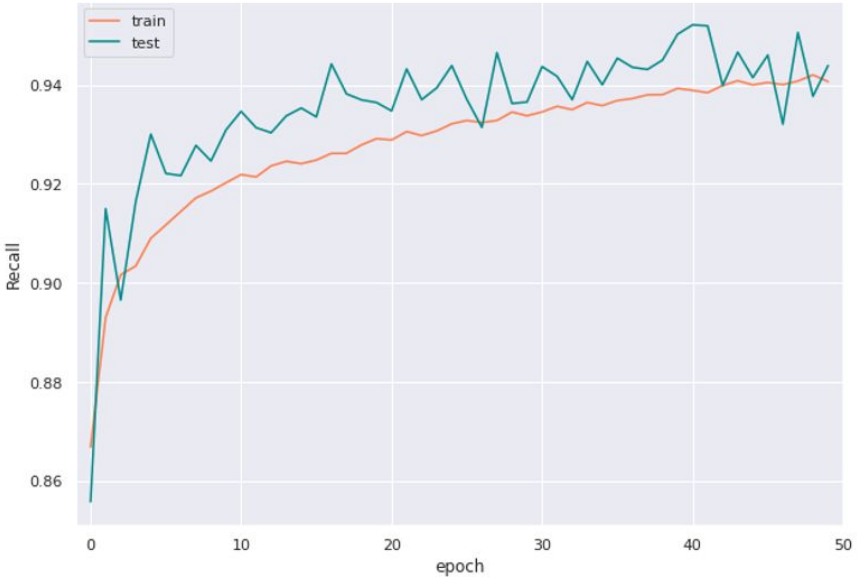


$$Precision = TP / (TP + FP)$$

$$Recall = TP / (TP + FN)$$

Значення показників Precision та Recall під час тренування нейронної мережі модуля класифікації атаки

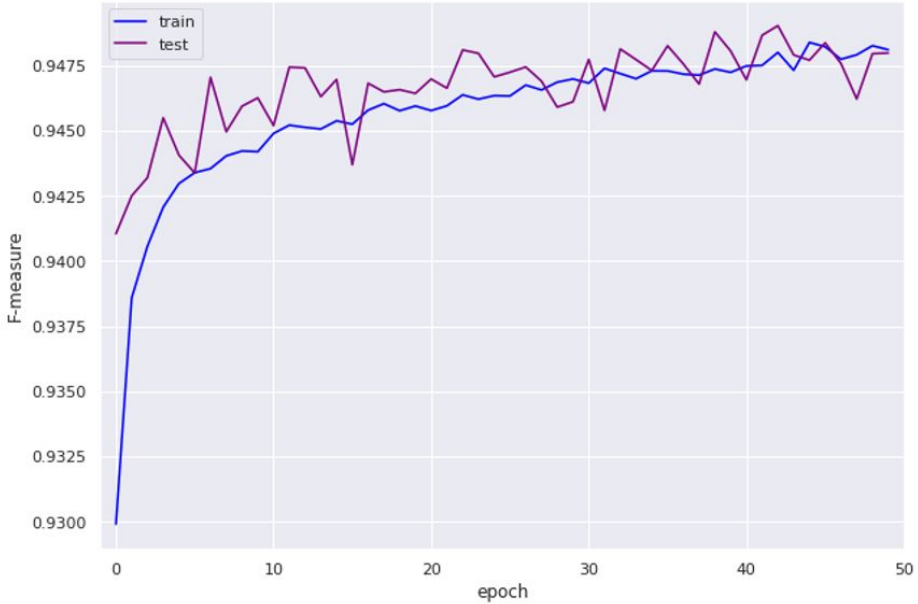




$$Precision = TP / (TP + FP)$$

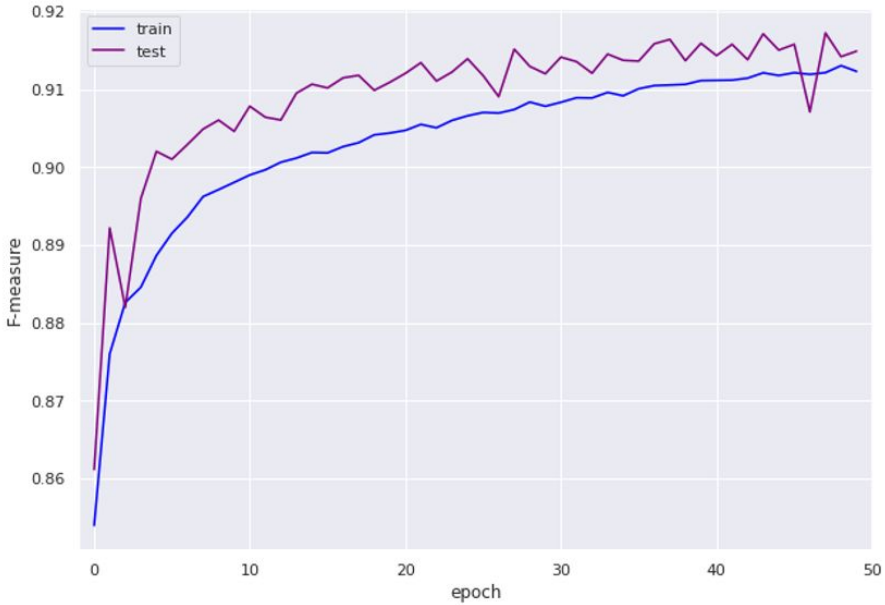
$$Recall = TP / (TP + FN)$$

Значення критерія F-міри під час тренування нейронної мережі модуля виявлення атаки



$$F - \text{міра} = 2 * (Precision * Recall) / (Precision + Recall)$$

Значення критерія F-міри під час тренування нейронної мережі модуля класифікації атаки



$$F - \text{міра} = 2 * (Precision * Recall) / (Precision + Recall)$$

```
------------------------------------------------------------------

listening on wlp3s0

------------------------------------------------------------------

01. Attack probability - 0.00000000
02. Attack probability - 4.82815218
03. Attack probability - 0.00000001
04. Attack probability - 0.00001626
05. Attack probability - 0.00000001
06. Attack probability - 98.65733337
    Attack type - Analysis with probability 0.00000000
    Attack type - Backdoor with probability 0.00000000
    Attack type - DoS with probability 0.00000000
    Attack type - Exploits with probability 0.00000000
    Attack type - Fuzzers with probability 0.00000000
    Attack type - Generic with probability 0.00000000
    Attack type - Not Attack with probability 100.00000000
    Attack type - Reconnaissance with probability 0.00000000
    Attack type - Shellcode with probability 0.00000000
    Attack type - Worms with probability 0.00000000
07. Attack probability - 0.00003558
08. Attack probability - 0.00000000
09. Attack probability - 99.39744568
    Attack type - Analysis with probability 0.00000000
    Attack type - Backdoor with probability 0.00000000
    Attack type - DoS with probability 0.00000000
    Attack type - Exploits with probability 0.00000000
    Attack type - Fuzzers with probability 0.00000000
    Attack type - Generic with probability 0.00000000
    Attack type - Not Attack with probability 100.00000000
    Attack type - Reconnaissance with probability 0.00000000
    Attack type - Shellcode with probability 0.00000000
    Attack type - Worms with probability 0.00000000
10. Attack probability - 0.00066655
11. Attack probability - 0.00000006
12. Attack probability - 0.00001213
13. Attack probability - 0.00052934
14. Attack probability - 0.00150545
```

```
06. Attack probability - 98.65733337
    Attack type - Analysis with probability 0.00000000
    Attack type - Backdoor with probability 0.00000000
    Attack type - DoS with probability 0.00000000
    Attack type - Exploits with probability 0.00000000
    Attack type - Fuzzers with probability 0.00000000
    Attack type - Generic with probability 0.00000000
    Attack type - Not Attack with probability 100.00000000
    Attack type - Reconnaissance with probability 0.00000000
    Attack type - Shellcode with probability 0.00000000
    Attack type - Worms with probability 0.00000000
```

Приклад результата роботи системи в режимі реального часу

```
01. Attack probability - 89.31539917
    Attack type - Analysis with probability 5.79201207
    Attack type - Backdoor with probability 1.26974592
    Attack type - DoS with probability 29.25128043
    Attack type - Exploits with probability 50.46548843
    Attack type - Fuzzers with probability 0.15782494
    Attack type - Generic with probability 0.68402784
    Attack type - Not Attack with probability 11.95866764
    Attack type - Reconnaissance with probability 0.41954229
    Attack type - Shellcode with probability 0.00000047
    Attack type - Worms with probability 0.00141398
02. Attack probability - 99.96312714
    Attack type - Analysis with probability 0.00023755
    Attack type - Backdoor with probability 0.00000336
    Attack type - DoS with probability 3.29988822
    Attack type - Exploits with probability 95.87666392
    Attack type - Fuzzers with probability 0.00763754
    Attack type - Generic with probability 0.74357353
    Attack type - Not Attack with probability 0.06114644
    Attack type - Reconnaissance with probability 0.00980773
    Attack type - Shellcode with probability 0.00000000
    Attack type - Worms with probability 0.00103563
03. Attack probability - 99.89464569
    Attack type - Analysis with probability 0.00059518
    Attack type - Backdoor with probability 0.00117074
    Attack type - DoS with probability 7.48423412
    Attack type - Exploits with probability 91.69430137
    Attack type - Fuzzers with probability 0.00846050
    Attack type - Generic with probability 0.68858368
    Attack type - Not Attack with probability 0.08806737
    Attack type - Reconnaissance with probability 0.03303131
    Attack type - Shellcode with probability 0.00041399
    Attack type - Worms with probability 0.00113760
```

```
Attack type - Exploits with probability 50.46548843
```

```
02. Attack probability - 99.96312714
    Attack type - Analysis with probability 0.00023755
    Attack type - Backdoor with probability 0.00000336
    Attack type - DoS with probability 3.29988822
    Attack type - Exploits with probability 95.87666392
    Attack type - Fuzzers with probability 0.00763754
    Attack type - Generic with probability 0.74357353
    Attack type - Not Attack with probability 0.06114644
    Attack type - Reconnaissance with probability 0.00980773
    Attack type - Shellcode with probability 0.00000000
    Attack type - Worms with probability 0.00103563
```

```
Attack type - Exploits with probability 91.69430137
```

Результат тестування системи на пакетах, які належать до атак, взяті з тестової вибірки

Висновки

- проведено аналіз існуючих методів виявлення атак та систем IDS;
- спроектована і реалізована система виявлення атак, яка складається з модуля сенсору, модуля обробки даних, модуля аналізу та модуля сповіщення;
- реалізований алгоритм виявлення аномальної поведінкі мережі на основі каскаду нейронних мереж: перша мережа перевіряє наявність атаки, а друга мережа класифікує атаку у разі її наявності ;
- для навчання нейронних мереж використовувався набір UNSW-NB15;
- Система протестована у режимі реального часу при моделюванні атаки TCP SYN Flood.

Всього було відправлено 15000 пакетів, з яких система розпізнала 14,182 як DoS атаку, що складає 94,54% точності.

ПУБЛІКАЦІЇ

Якушина А.О., Шпінарева І.М. Виявлення аномалій в мережевому трафіку з використанням методів глубокого навчання / Інформатика, інформаційні системи та технології: тези доповідей шістнадцятої всеукраїнської конференції студентів і молодих науковців. Одеса, 23 квітня 2021 р. – Одеса, 2021. – с. 172-174

ДЯКУЮ ЗА УВАГУ!

Email: anastasiia.yakushyna@gmail.com