МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Український державний університет
науки і технологій**

Кафедра «Електронні обчислювальні машини»

В авторській редакції

ЛОКАЛЬНІ МЕРЕЖІ

Навчально-методичні рекомендації щодо виконання групового завдання
за результатами самостійної роботи

ДНІПРО
2024

УДК 004.732(076.5)
Л 73

Упорядник:
В. М. Пахомова

Електронний аналог
друкованого видання

Схвалено Групою забезпечення якості освітніх програм
123 «Комп'ютерна інженерія»; 125 «Кібербезпека та безпека інформації»
Протокол №7 від 16.02.2024

Л 73 Локальні мережі : навчально-методичні рекомендації щодо виконання групового завдання за результатами самостійної роботи / упоряд. В. М. Пахомова ; Укр. держ. ун-т науки і технологій. Дніпро : УДУНТ, 2024. – 20 с.

Навчально-методичні рекомендації призначені для використання студентами безвідривної форми навчання спеціальностей 123 «Комп'ютерна інженерія» та 125 «Кібербезпека та безпека інформації» під час виконання групового завдання за результатами самостійної роботи з дисципліни «Локальні мережі».

Іл. 11. Табл. 5. Бібліогр. назв. 7.

ЗМІСТ

ВСТУП

Методичні рекомендації щодо виконання групового завдання за результатами самостійної роботи на тему: «Визначення мережевих атак засобами нейронної мережі (НМ)» з дисципліни «Локальні мережі» [1], що призначені здобувачам ступеня «бакалавр».

Виконання самостійної роботи здобувачами спеціальності «Кібербезпека та безпека інформації» сприяють досягненню наступних результатів навчання: здатність до пошуку, оброблення та аналізу інформації; здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

Виконання самостійної роботи здобувачами спеціальності «Комп'ютерна інженерія» сприяють досягненню результатів навчання: здатність вчитися і оволодівати сучасними знаннями; здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

Крім того, при виконанні групового завдання за результатами самостійної роботи у здобувачів спеціальностей «Комп'ютерна інженерія» і «Кібербезпека та безпека інформації» формуються наступні «Soft skills»: розвиток уміння керувати власним часом; здатність працювати в команді; розвиток членів команди, коли результат групи визначається як сумарний і враховує досягнення кожного студента групи.

У методичних рекомендаціях сформульована постановка групового завдання, виконання якого складається із двох частин: теоретичної та практичної, наведені параметри мережевого трафіку на основі бази даних NSL-KDD [5], а також приклад виконання завдання [4]. Теоретична частина передбачає: складання конфігурації НМ з описом нейронів першого та результуючого шарів, а також розрахунок кількості прихованих нейронів; підготовка вибірки з вказівкою кількості прикладів на кожний мережевий клас. Практична частина передбачає: створення НМ відповідно до складеної конфігурації НМ за допомогою обраного нейропакету; навчання та тестування НМ; дослідження на створеній НМ (результати у табличному та графічному вигляді).

На при кінці навчально-методичного видання представлені контрольні запитання щодо захисту отриманих результатів самостійної роботи, а також поданий перелік рекомендованих джерел [1-7].

1. ЗМІСТ ЗАВДАННЯ

DoS – мережеві атаки, спрямовані на виникнення ситуації, коли на атакованій системі відбувається відмова в обслуговуванні.

Probe полягає в скануванні мережних портів з метою отримання конфіденційної інформації.

U2R передбачає отримання зареєстрованим користувачем привілегій локального суперкористувача.

R2L характеризується отриманням доступу незареєстрованого користувача до комп'ютера з віддаленого комп'ютера та відповідні типи атак.

Відповідність мережевих класів атак до їх категорій показана в табл. 1.1.

Таблиця 1.1 – Мережеві класи атак на основі бази даних NSL-KDD

DoS	**Probe**	**U2R**	**R2L**
Apache2	Ipsweep	Buffer_overflow	Ftp_write
Back	Mscan	Loadmodule	Guess_passwd
Land	Nmap	Perl	Httptunnel
Neptune	Portsweep	Ps	Imap
Mailbomb	Saint	Rootkit	Multihop
Pod	Satan	Sqlattack	Named
Processtable		Xterm	Phf
Smurf			Sendmail
Teardrop			Snmpgetattack
Udpstorm			Spy
Worm			Snmpguess
			Warezclient
			Warezmaster
			Xlock
			Xsnoop

У базі NSL-KDD збережені параметри мережевого трафіку (табл. 1.2).

Таблиця 1.2 – Параметри мережевого трафіку на основі бази даних NSL-KDD

№№	**Параметр**	**Опис**
1	**2**	**3**
1	Duration	Час з'єднання
2	Protocol Type	Тип протоколу
3	Service	Мережева служба
4	Flag	Статус з'єднання (нормальний / з помилкою)

Продовження таблиці 1.2

1	2	3
5	Src Bytes	Кількість біт переданих даних від джерела на вузол призначення
6	Dst Bytes	Кількість біт даних, що приймаються від вузла призначення
7	Land	1 – якщо ip (або порти) джерела і приймача рівні, 0 – інакше
8	Wrong Fragment	Кількість невірних фрагментів за сеанс
9	Urgent	1 – якщо успішний вхід в систему; 0 – якщо неуспішний
10	Hot	Кількість «гарячих» індикаторів
11	Num Failed Logins	Кількість невдалих спроб входу
12	Logged In	Статус входження: 1 – успішний, 0 – неуспішний
13	Num Compromised	Кількість скомпрометованих станів
14	Root Shell	1 – якщо root-права отримані успішно, 0 – інакше
15	Su Attempted	1 – якщо su root-права отримані успішно, 0 – інакше
16	Num Root	Кількість root-доступів
17	Num File Creations	Кількість операцій по створенню файлів під час з’єднання
18	Num Shells	Кількість викликів shell-оболонки
19	Num Access Files	Кількість операцій по отриманню доступу до файлів
20	Is Hot Logins	1 – якщо логін належить hot-листу (тобто якщо є root або адміністратором), 0 – інакше
21	Is Guest Login	1 – якщо отримано, що не пройшли ідентифікацію, 0 – інакше
22	Count	Кількість підключень до цільового хосту за останні 2 секунди
23	Srv Count	Кількість з’єднань зі службою за останні 2 секунди
24	Serror Rate	Відсоток з’єднань з хостом з count із SYN-помилками
25	Srv Serror Rate	Відсоток з’єднань з SYN-помилками при з’єднанні за

		службою з sry_count

Продовження таблиці 1.2

1	2	3
26	Rerror Rate	Відсоток з'єднань з хостом з count із REJ-помилками
27	Srv Rerror Rate	Відсоток з'єднань з REJ-помилками при з'єднанні за службою з sry_count
28	Same Srv Rate	Відсоток з'єднань з хостом з count, що використовують одні і ті ж служби
29	Diff Srv Rate	Відсоток підключень до різних сервісів
30	Srv Diff Host Rate	Відсоток підключень до різних хостів
31	Dst Host Count	Кількість з'єднань до локального хосту, встановлених віддаленою стороною
32	Dst Host Srv Count	Кількість з'єднань з тим же самим номером порту
33	Dst Host Diff Srv Rate	Відсоткова кількість з'єднань до локального хосту, встановлених віддаленою стороною і використовують одну і ту ж службу
34	Dst Host Diff Srv Rate	Відсоток з'єднань за різними службами під час з'єднання з ip з dst_host_count
35	Dst Host Same Src Port Rate	Відсоток з'єднань до того ж самому хосту приймача під час зв'язку через порт з dst_host_srv_count
36	Dst Host Srv Diff Host Rate	Відсоток з'єднань з різними хостами приймачами під час зв'язку через порт з dst_host_srv_count
37	Dst Host Serror Rate	Відсоток з'єднань з хостом з dst_host_count із SYN-помилками
38	Dst Host Srv Serror Rate	Відсоток з'єднань з SYN-помилками при з'єднанні за службою з dst_host_srv_count
39	Dst Host Rerror Rate	Відсоток з'єднань з SYN-помилками при з'єднанні за службою з dst_host_srv_count
40	Dst Host Srv Rerror Rate	Відсоток з'єднань з REJ-помилками при з'єднанні за службою з dst_host srv_count
41	Sroce	Складність рівня

Необхідно визначити мережеві атаки на локальну мережу засобами багатошарової нейронної мережі на основі відкритої бази даних NSL-KDD (за виданим варіантом, табл. 1.3).

Таблиця 1.3 – Варіанти щодо виконання курсового завдання

№вар.	Категорія	Мережеві класи	Параметри трафіку
1	**2**	**3**	**4**
1	DoS	Apache2; Back; Land	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
2	Probe	Ipsweep; Mscan; Nmap	11, 12, 13, 14, 15, 16, 17, 18,19, 20
3	U2R	Buffer_overflow; Loadmodule; Perl	20, 21, 22, 23, 24, 25, 26, 27, 28, 29
4	R2L	Ftp_write; Httptunnel	30, 31, 32, 33, 34, 35, 36, 37, 38, 39
5	DoS	Neptune; Mailbomb; Processtable	15, 16, 17, 18, 19, 20, 21, 22, 23, 24
6	Probe	Portsweep; Saint; Satan	25, 26, 27, 28, 29, 30, 31, 32, 33, 34
7	U2R	Ps; Rootkit; Sqlattack; Xterm	1, 2, 3, 35, 36, 37, 38, 39, 40, 41
8	R2L	Imap; Multihop; Named	2, 4, 6, 8, 10, 12, 14, 16, 18, 20
9	DoS	Smurf; Teardrop; Udpstorm; Worm	1, 3, 5, 7, 9, 11, 13, 15, 17, 19
10	R2L	Phf; Sendmail; Snmpgetattack	22, 24, 26, 28, 30, 32, 34, 36, 38, 40
11	R2L	Spy; Snmpguess; Warezclient	21, 23, 25, 27, 29, 31, 33, 35, 37, 39
12	R2L	Warezmaster; Xlock; Xsnoop	1, 2, 5, 10, 15, 20, 25, 30, 35, 40
13	DoS	Apache2; Land; Mailbomb; Pod	3, 6, 9, 12, 15, 18, 21, 24, 27, 30
14	Probe	Ipsweep; Nmap; Saint	11, 12, 13, 17, 18,19, 23, 24, 25, 35
15	U2R	Buffer_overflow; Perl; Rootkit	9, 10, 19, 20, 29, 30, 39, 40
16	R2L	Ftp_write; Httptunnel; Multihop; Phf	9, 19, 29, 30, 31, 32, 33, 39, 40, 41
17	DoS	Back; Neptune; Processtable	15, 16, 17, 18, 19, 20, 21, 22, 23, 24
18	Probe	Mscan; Portsweep; Satan	25, 26, 27, 28, 29, 30, 31, 32, 33, 34
19	U2R	Loadmodule; Ps; Sqlattack	4, 5, 6, 25, 26, 27, 28, 29, 30, 31
20	R2L	Snmpgetattack; Snmpguess; Xlock	2, 4, 6, 8, 10, 12, 14, 16, 18, 20
21	DoS	Smurf; Teardrop; Pod	1, 3, 5, 7, 9, 11, 13, 15, 17, 19
22	U2R	Rootkit; Xterm	22, 24, 26, 28, 30, 32, 34, 36, 38, 40
23	R2L	Guess_passwd; Imap;	21, 23, 25, 27, 29, 31, 33, 35, 37, 39

		Named; Phf	Продовження таблиці 1.3
1	**2**	**3**	**4**
24	R2L	Sendmail; Spy; Warezclient; Xsnoop	1, 2, 5, 10, 15, 20, 25, 30, 35, 40, 41
25	DoS	Udpstorm; Worm	5, 6, 7, 8, 9, 10, 30, 33, 39, 41
26	DoS	Apache2; Mailbomb; Udpstorm	4, 8, 12, 16, 20, 24, 28, 32,36, 40
27	Probe	Ipsweep; Satan	3, 5, 8, 10, 18, 20, 28, 30, 38, 40, 41
28	R2L	Named; Spy; Xsnoop	15, 16, 17, 18, 19, 30, 31, 32, 33, 34
29	R2L	Imap; Multihop; Spy	15, 16, 17, 18, 19, 20, 21, 22, 23, 24
30	DoS	Land; Pod; Teardrop	25, 26, 27, 28, 29, 30, 31, 32, 33, 34
31	Probe	Mscan; Saint	7, 8, 9, 15, 16, 17, 18, 19, 20, 21
32	U2R	Multihop; Snmpgetattack	2, 4, 6, 8, 10, 12, 14, 16, 18, 20
33	R2L	Warezclient; Warezmaster; Phf	1, 3, 5, 7, 9, 11, 13, 15, 17, 19
34	DoS	Back; Processtable; Smurf	22, 24, 26, 28, 30, 32, 34, 36, 38, 40
35	Probe	Nmap; Portsweep; Satan	21, 23, 25, 27, 29, 31, 33, 35, 37, 39
36	U2R	Imap; Phf; Spy; Xlock	1, 2, 5, 10, 15, 20, 25, 30, 35, 40, 41
37	R2L	Httptunnel; Snmpgetattack	1, 5, 6, 7, 8, 9, 10, 11, 21, 31, 41
38	DoS	Pod; Smurf; Udpstorm; Worm	6, 12, 18, 24, 30, 36, 37, 38, 39, 40
39	U2R	Httptunnel; Sendmail; Spy	7, 10, 17, 20, 23, 25, 27, 30, 37, 40
40	R2L	Guess_passwd; Snmpguess	30, 31, 32, 33, 34, 35, 36, 37, 38, 40

2. ПРИКЛАД ВИКОНАННЯ ЗАВДАННЯ

2.1. Формулювання постановки задачі

Категорія PROBE представляє одну з чотирьох категорій атак на мережі, які спрямовані на сканування портів з метою отримання конфіденційної інформації та виявлення вразливостей в мережах з метою здійснення подальших атак. PROBE включає в себе різноманітні класи атак:

Ipsweep – ця атака полягає у скануванні мережевого простору з метою виявлення активних хостів.

Nmap – ця атака використовується для сканування портів хостів з метою виявлення відкритих портів та отримання інформації про сервіси, які запущені на цих портах.

Portsweep – ця атака полягає у скануванні портів на окремому хості з метою виявлення відкритих портів та отримання інформації про сервіси, які запущені на цих портах.

Satan – ця атака включає в себе комбінацію Ipsweep, Nmap та Portsweep атак з метою збору детальної інформації про систему та виявлення вразливостей, які можна використати для злому.

Ці класи атак використовуються з метою виявлення потенційних слабких місць у системі та підготовки до можливих подальших вторгнень. Однак, їх також можна використовувати для моніторингу мережі та виявлення потенційних загроз безпеці.

Створити нейронну мережу (НМ) для виявлення наступних атак: Ipsweep; Nmap; Portsweep; Satan з використанням відкритої бази даних NSL-KDD.

2.2. Складання конфігурації нейронної мережі

На основі постановки задачі визначається кількість нейронів першого шару (X1, X2, …, X41), що відповідають параметрам мережевого трафіку (їх 41), а також кількість результуючих нейронів: Y1 – normal (немає атаки); Y2 – атака Nmap; Y3 – атака Satan; Y4 – атака Ipsweep; Y5 – атака Portsweep).

Для визначення кількості прихованих нейронів є кілька емпіричних правил і рекомендацій, які можна використовувати для оцінки, наприклад:

1. Емпіричне «правило пальця» свідчить, що кількість прихованих нейронів може бути приблизно вдвічі більшою, ніж кількість нейронів першого шару: 2*41 = 82.

2. Формула розрахунку на основі загальної кількості нейронів свідчить, що кількість прихованих нейронів може дорівнювати приблизно половині суми кількості нейронів першого та результуючого шарів: (41 + 5)/2 = 23.

Ці формули є емпіричними та надають лише грубу оцінку. Найкращим підходом є проведення додаткового дослідження з метою визначення оптимального значення кількості прихованих нейронів.

Таким чином, можна взяти НМ конфігурації 41-X-20-5, де 41 – кількість нейронів першого шару (параметри мережевого трафіку); X – кількість прихованих шарів; 20 – кількість прихованих нейронів (приблизне значення, яке повинно додатково досліджуватися); 5 – кількість результуючих нейронів (ознаки наявності мережевих класів атак категорії PROBE та їх відсутності), що представлена на рис. 2.1.

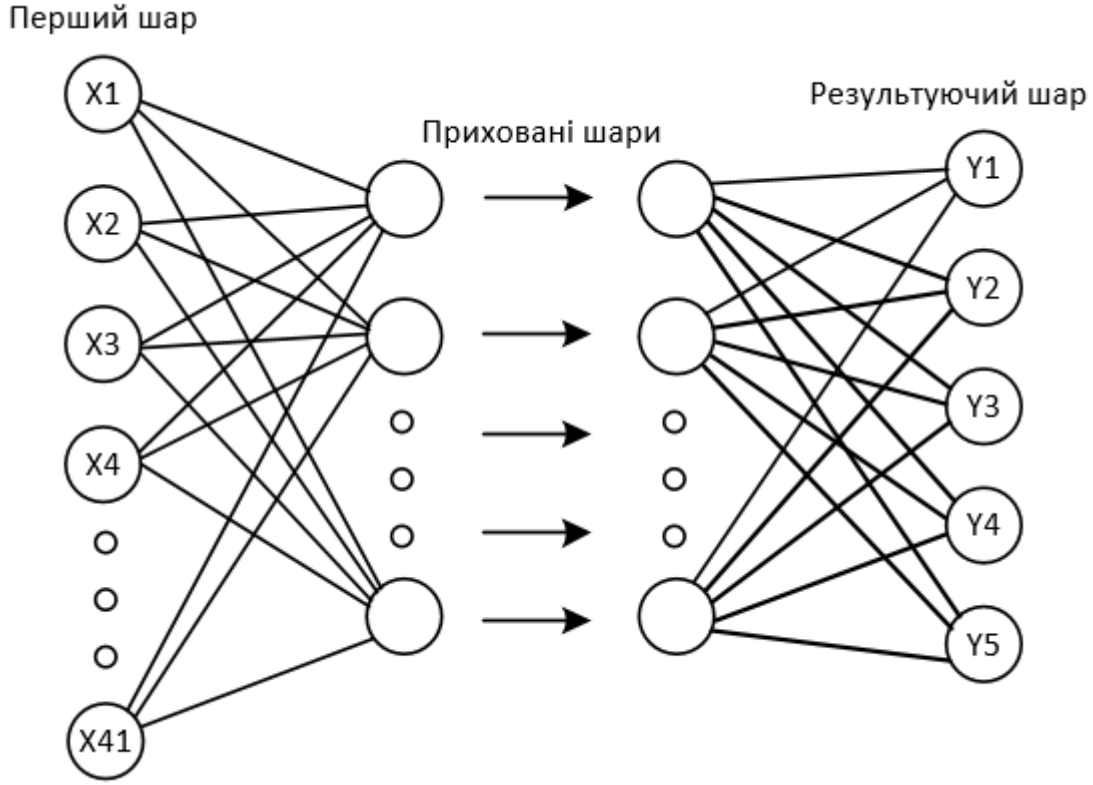

Рис. 2.1. НМ конфігурації 41-X-20-5

2.3. Підготовка вибірки

Вибірка складається на основі відкритої бази даних NSL-KDD. До вибірки додається однакова кількість прикладів на кожний мережевий клас, а також на випадок відсутності атаки, наприклад, 5*5 = 25 прикладів. Фрагменти вибірки (із 10 прикладів) для нейронів першого та результуючого шарів зведені відповідно до таблиць 2.1-2.2.

Таблиця 2.1 – Фрагмент вибірки для нейронів першого шару

X1	X2	X3	X4	X5	X6	X7	X8	X9	X10	X11	X12	X13	X14	X15
0	2	1	1	8	0	0	1	0	0	0	0	0	0	0
0	1	2	2	0	0	0	2	0	0	0	0	0	0	0
0	2	1	1	8	0	0	1	0	0	0	0	0	0	0
0	3	3	1	207	0	0	3	0	0	0	0	0	0	0
0	2	1	1	8	0	0	1	0	0	0	0	0	0	0
10	1	3	3	0	0	0	3	0	0	0	0	0	0	0
0	2	1	1	8	0	0	1	0	0	0	0	0	0	0
0	1	4	4	0	0	0	4	0	0	0	0	0	0	0
0	1	3	2	0	0	0	3	0	0	0	0	0	0	0
0	2	1	1	8	0	0	1	0	0	0	0	0	0	0

Продовження таблиці 2.1

X16	X17	X18	X19	X20	X21	X22	X23	X24	X25	X26	X27	X28
0	0	0	0	0	0	0	0	1	26	0	0	0
0	0	0	0	0	0	0	0	365	1	0,1	0	0,9
0	0	0	0	0	0	0	0	1	41	0	0	0
0	0	0	0	0	0	0	0	2	2	0	0	0
0	0	0	0	0	0	0	0	1	44	0	0	0
0	0	0	0	0	0	0	0	1	1	0	0	1
0	0	0	0	0	0	0	0	1	36	0	0	0
0	0	0	0	0	0	0	0	1	1	1	1	0
0	0	0	0	0	0	0	0	230	1	0,06	0	0,89
0	0	0	0	0	0	0	0	1	2	0	0	0

Продовження таблиці 2.1

X29	X30	X31	X32	X33	X34	X35	X36	X37	X38	X39	X40	X41
0	1	0	1	3	115	1	0	1	0,25	0	0	0
1	0	1	0	255	1	0	1	0	0	0,11	0	0,89
0	1	0	1	2	106	1	0	1	0,5	0	0	0
0	1	0	0	52	44	0,85	0,04	0,85	0	0	0	0
0	1	0	1	1	111	1	0	1	0,51	0	0	0
1	1	0	0	255	1	0	0,48	0,47	0	0	0	0,47
0	1	0	1	1	73	1	0	1	0,51	0	0	0
0	1	0	0	73	1	0,01	0,86	0,89	0	0,89	1	0
1	0	1	0	255	1	0	0,91	0	0	0,05	0	0,8
0	1	0	1	1	17	1	0	1	0,53	0	0	0

Таблиця 2.2 – Фрагмент вибірки результуючих нейронів

Y1	Y2	Y3	Y4	Y5
0	1	0	0	0
0	0	1	0	0
0	0	0	1	0
0	1	0	0	0
0	0	0	1	0
0	0	0	0	1
0	0	0	1	0
0	1	0	0	0
0	0	1	0	0
0	1	0	0	0

2.4. Створення нейронної мережі

За допомогою додатку Toolbox системи MatLAB створено НМ конфігурації 41-1-20-5 (див. рис. 2.1), структуру якої показано на рис. 2.2.

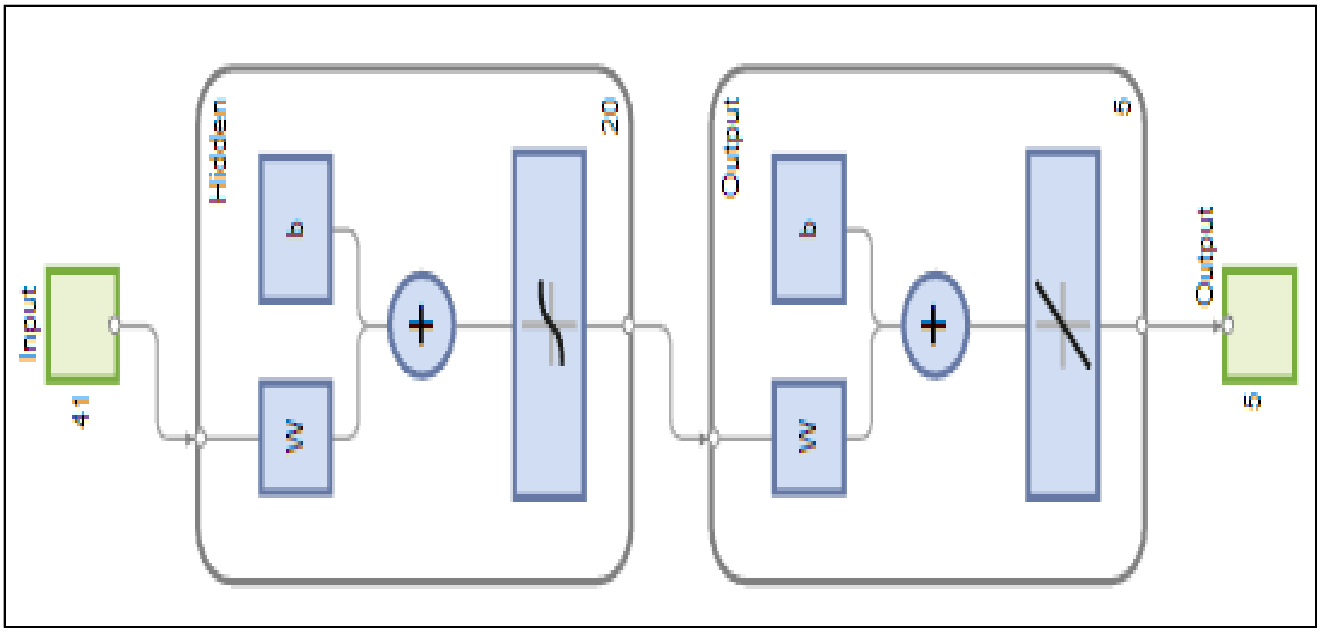

Рис. 2.2. Структура створеної НМ в MatLAB

Встановимо необхідний відсоток загальної вибірки для навчання, тестування та валідації НМ (рис. 2.3).

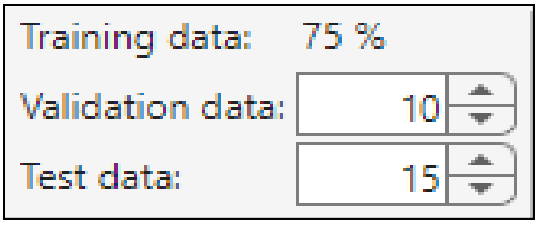

Рис. 2.3. Розбиття загальної вибірки на відсоткові складові

Оберемо необхідний розмір прихованого шару, як це показано на рис. 2.4.

Рис. 2.4. Розмір прихованого шару

2.5. Навчання та тестування створеної нейронної мережі

Для навчання НМ оберемо алгоритм Левенберга-Марквардта із можливих, що показані на рис. 2.5.

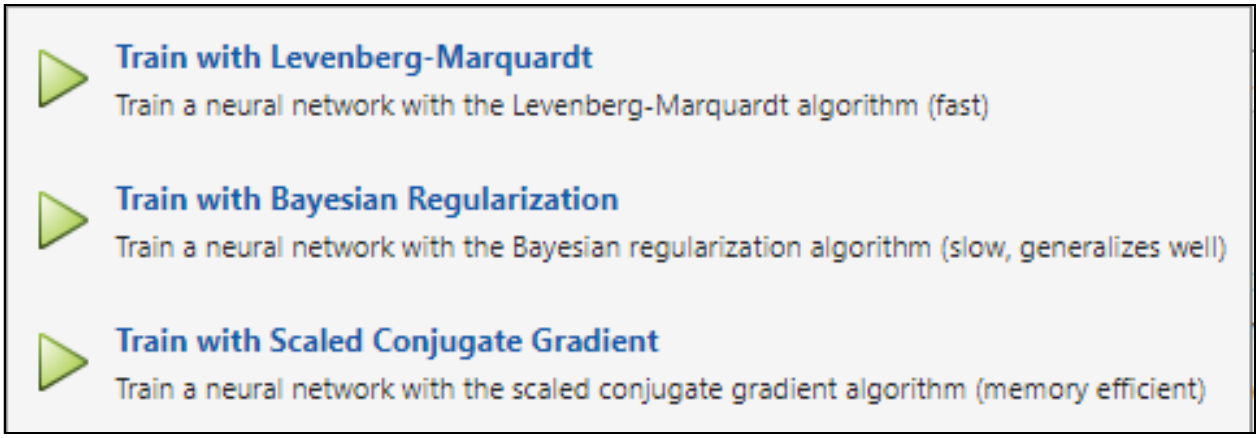

Рис. 2.5. Алгоритми навчання нейромережі

Після навчання створенної НМ можна подивитися відповідну статистику (рис. 2.6).

Unit	Initial Value	Stopped Value	Target Value
Epoch	0	26	1000
Elapsed Time	-	00:00:01	-
Performance	2.03	4.24e-05	0
Gradient	3.34	0.000763	1e-07
Mu	0.001	1e-06	1e+10
Validation Checks	0	6	6

Рис. 2.6. Статистика

Так, наприклад, графік «Gradient» показує зміну значень градієнта ваги нейронної мережі в процесі навчання, графік «Mu» відображає зміну значення коефіцієнта моменту протягом процесу навчання, графік «Validation Checks» відображає кількість проведених перевірок на валідаційному наборі даних у процесі навчання (рис. 2.7).

Графік «Performance» дозволяє оцінити, як продуктивність нейронної моделі змінюється під час навчання та допомагає приймати рішення щодо необхідності внесення змін до процесу навчання (рис. 2.8).

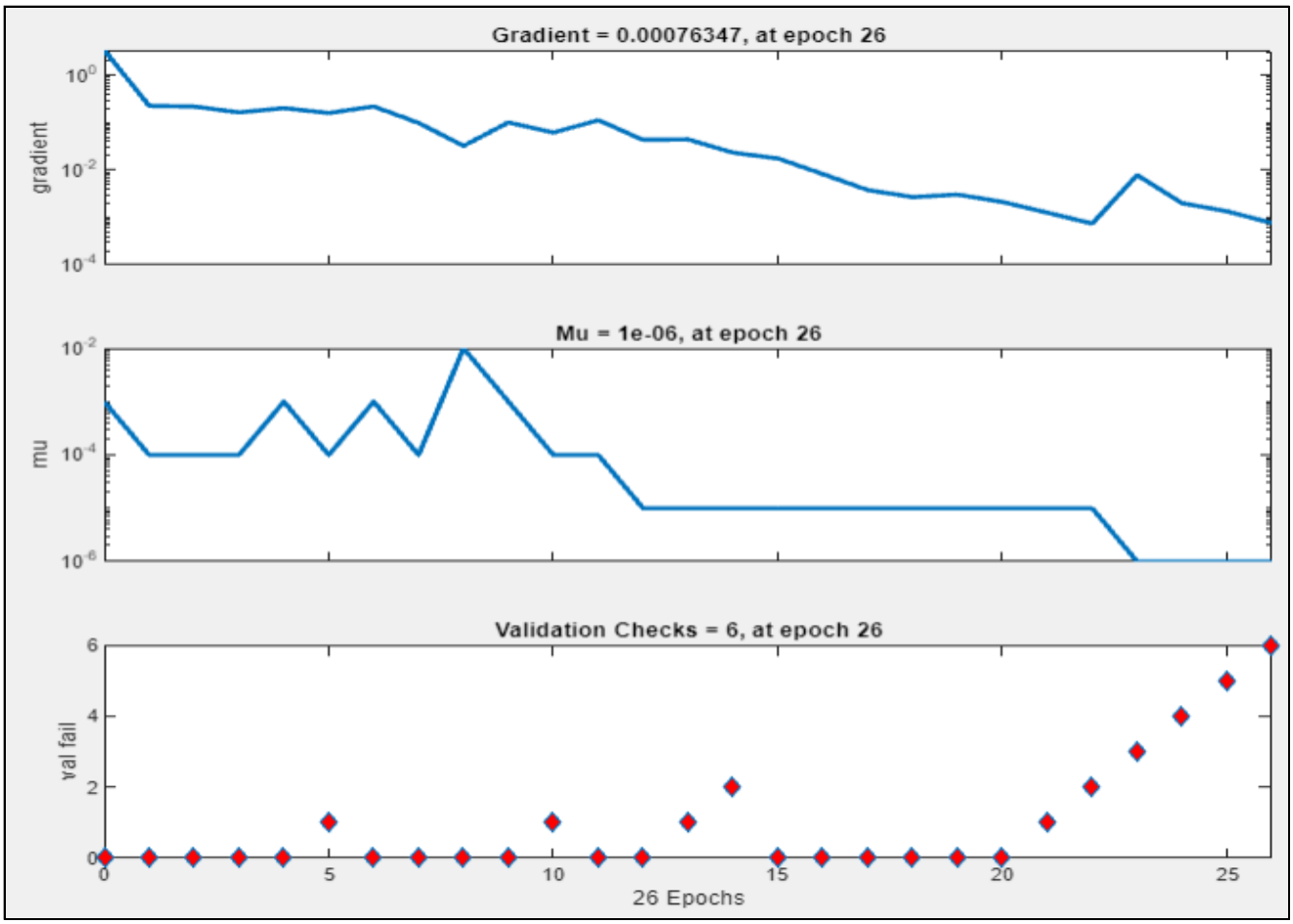

Рис. 2.7. Графік стану навчання НМ

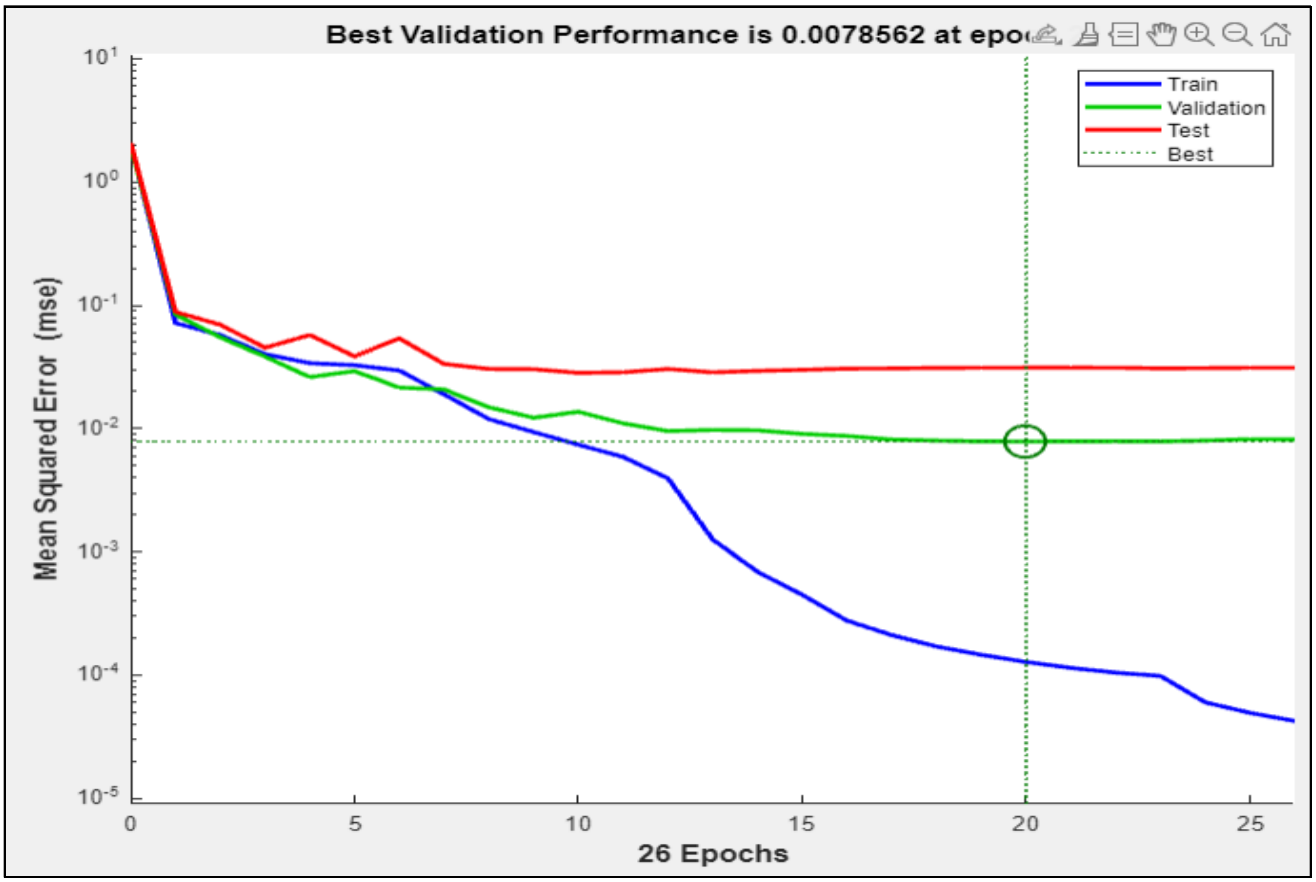

Рис. 2.8. Графік продуктивності НМ

Гістограма помилок показує, як часто різні помилки зустрічаються під час навчання чи тестування НМ, а також може допомогти оцінити, як НМ справляється з різними видами помилок і дозволяє ідентифікувати області, де НМ виявляє найкращу чи найгіршу продуктивність (рис. 2.9).

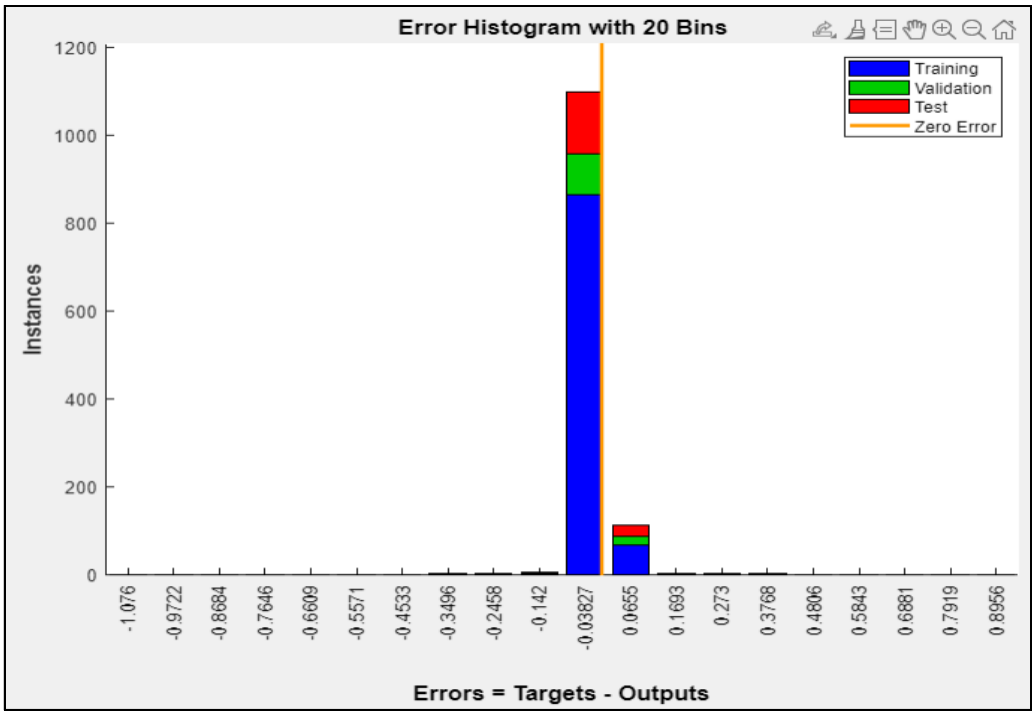

Рис. 2.9. Гістограма помилок НМ

Графік регресії допомагає оцінити якість передбачення НМ та визначити, наскільки добре вона відповідає реальним даним (рис. 2.10).

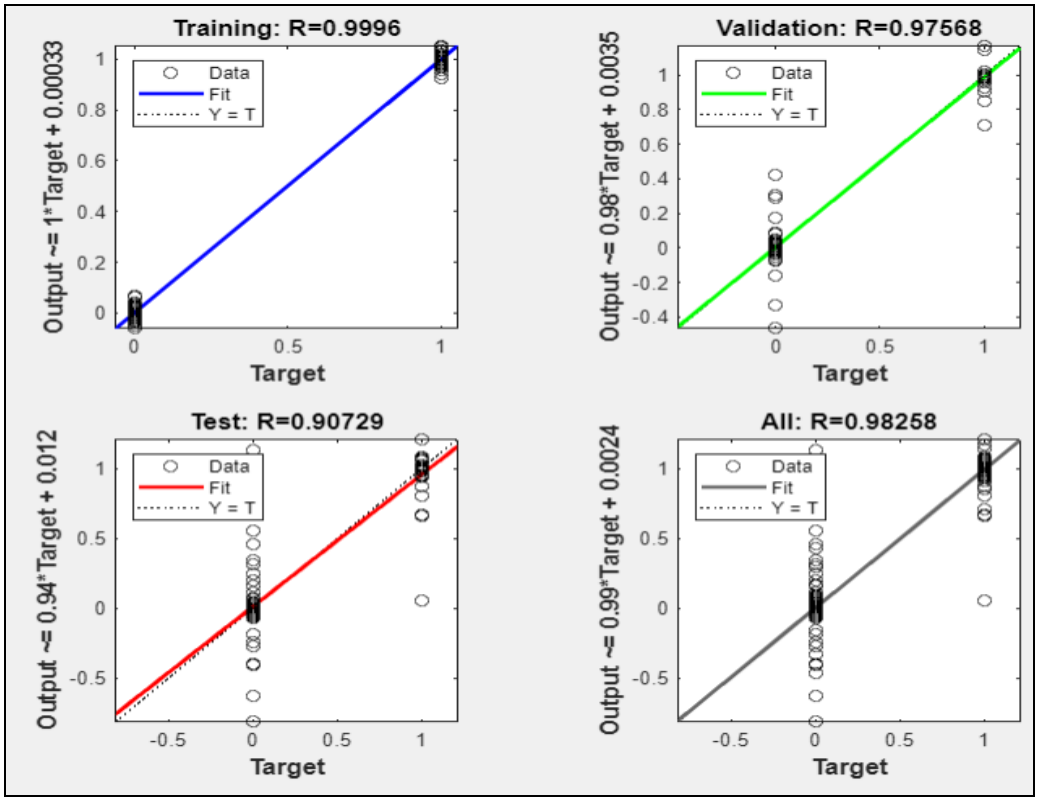

Рис. 2.10. Графік регресії

Кількість спостережень (Observations) вказує на кількість доступних даних, використаних для навчання або тестування НМ; рис. 2.11.

Середньоквадратична помилка (MSE) є метрикою, яка використовується для вимірювання відхилення між реальними значеннями та передбаченими значеннями НМ. Коефіцієнт кореляції оцінює прогнозну здатність НМ.

	Observations	MSE	R
Training	187	0.0001	0.9996
Validation	25	0.0079	0.9757
Test	38	0.0312	0.9073

Рис. 2.11. Підсумкова таблиця

2.6. Основні висновки

1. НМ конфігурації 41-1-20-5, де 41 – кількість нейронів першого шару (параметри мережевого трафіку); 1 – кількість прихованих шарів; 20 – кількість прихованих нейронів; 5 – кількість результуючих нейронів для виявлення наступних мережевих атак: Ipsweep; Nmap; Portsweep; Satan.

2. Сформульована вибірка (75 % для навчання, 15 % для тестування; 10 % для валідації) нейронів першого та результуючого шарів на основі відкритої бази даних NSL-KDD. Для кожного мережевого класу, а також для випадку відсутності атаки наведено однакову кількість навчальних прикладів.

3. Створена за допомогою додатку Toolbox системи MatLAB НМ конфігурації 41-1-20-5 з використанням гіперболічного тангенсу на прихованому шарі та лінійної функції активації на результуючому шарі, що навчалася за алгоритмом Левенберга-Марквардта протягом 26 епох. Визначені оптимальні параметри НМ (*їх назвати*), при яких отримано наступне значення MSE (*навести числове значення*).

4. (*Аналіз отриманих результатів досліджень на створеній НМ*).

3. КОНТРОЛЬНІ ЗАПИТАННЯ ТА ЗАВДАННЯ

1. Загальна характеристика категорій мережевих атак.
2. Класифікація мережевих атак відповідно до їх категорій.
3. Стисла характеристика бази даних NSL-KDD.
4. Мережевий трафік та його параметри.
5. Конфігурація багатошарової нейронної мережі.
6. Визначення кількості прихованих нейронів НМ.
7. Функції активації нейронів.
8. Алгоритми навчання НМ.
9. Основні вимоги до формування вибірки.
10. Навчання та тестування НМ. Значення MSE та R.

БІБЛІОГРАФІЧНИЙ СПИСОК

1. Дистанційний курс з навчальної дисципліни «Локальні мережі» для студентів III-го курсу спеціальностей «Комп'ютерна інженерія» та «Кібербезпека» / уклад.: В. М Пахомова. Сертифікат ДК0287 від 20.07.2018. URL: https://lider.diit.edu.ua/course/view.php?id=344. (дата звернення: 09.02.2024).

2. Пахомова В. М., Коннов М. С. Дослідження двох підходів до виявлення мережних атак із використанням нейромережної технології. *Наука та прогрес транспорту*. 2020. № 3(87). С. 81-93. DOI: 10.15802/stp2020/208233 (дата звернення: 07.02.2024).

3. Пахомова В. М., Видиш А. Д. Дослідження комбінованого варіанту визначення атак з використанням нейромережних технологій. *Системні технології. Регіональний міжвузівський збірник наукових праць*. 2022. № 3(140). С. 79-86. DOI:10.34185/1562-9945-3-140-2022-08 (дата звернення: 07.02.2024).

4. Пахомова В. М., Квочка М. Ю. Визначення мережевих атак категорії Probe засобами багатошарової нейронної мережі. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки*. 2023. Том 34(73), № 4, С. 93-98.

5. NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB. *University of New Brunswick | UNB*. URL: https://www.unb.ca/cic/datasets/nsl.html (date of access: 06.02.2024).

6. Pakhomova V., Bikovska D. Investigation of multilayer neural network parameters for determination of R2L category network attacks. *Modern engineering and innovative technologies*. 2021. № 18-02. P. 39–43. DOI: 10.30890/2567-5273.2021-18-02-059 (date of access: 09.02.2024).

7. Pakhomova V., Mihelbei Y. Detection of attacks of the U2R category by means of the SOM on database NSL-KDD. *Системні технології*. 2022. № 5(142). С. 18–27. DOI 10.34185/1562-9945-5-142-2022-03 (date of access: 06.02.2024).

ДОДАТОК

Український державний університет науки і технологій

Кафедра ЕОМ

Укладач завдання:
доц. Пахомова В.М

ЗАВДАННЯ ЗА РЕЗУЛЬТАТАМИ САМОСТІЙНОЇ РОБОТИ

з дисципліни “ *Локальні мережі* “

здобувача _____ групи _____ за варіантом _____

Тема завдання *(видається викладачем)**:*** **“***Визначення мережевих атак засобами нейронної мережі при наступних параметрах: _____*”

Мета завдання: *ознайомитися з можливостями нейронної мережі (НМ) щодо виявлення мережевих атак*

Зміст завдання:

Теоретична частина: постановка задачі (відповідно до виданого варіанту); складання конфігурації НМ (рисунок) з описом нейронів першого та результуючого шарів, а також розрахунок кількості прихованих нейронів; підготовка вибірки (таблиці) з вказівкою кількості прикладів на кожний мережевий клас.

Практична частина: створення НМ відповідно до складеної конфігурації НМ за допомогою обраного нейропакету (скриншот); навчання та тестування НМ (скриншоти з похибками); дослідження (одне на вибір) на створеній НМ (результати у табличному та графічному вигляді).

Звіт завдання: титульний аркуш; бланк завдання; виконання частини 1; виконання частини 2; висновки; перелік використаних джерел (за вимогами ДСТУ8302:2015); дата і підпис здобувача.

Рекомендовані джерела:

1. NSL-KDD dataset. URL: https://www.unb.ca/cic/datasets/nsl.html
2. Дистанційний курс з навчальної дисципліни «Локальні мережі» для студентів ІІІ-го курсу спеціальностей «Комп’ютерна інженерія» та «Кібербезпека»; укладач: доц. Пахомова В.М. Сертифікат ДК0287 від 20.07.2018. URL: https://lider.diit.edu.ua/course/view.php?id=344.
3. Пахомова В.М. Навчально-методичні рекомендації щодо виконання групового завдання за результатами самостійної роботи з дисципліни «Локальні мережі» для здобувачів спеціальностей «Кібербезпека та безпека інформації» та «Комп’ютерна інженерія». Дніпро : УДУНТ. 2024. 20 с.

Навчально-методичне видання

Пахомова Вікторія Миколаївна

ЛОКАЛЬНІ МЕРЕЖІ

Навчально-методичні рекомендації щодо виконання групового завдання
за результатами самостійної роботи

В авторській редакції
Комп’ютерна верстка В. М. Пахомова

Експертний висновок склали: проф. Жуковицький І. В., доц. Єгоров О. Й.

Зареєстровано НМВ УДУНТ (№704 від 01.03.2024)

Формат 60х84 1/16. Ум. друк. арк. 1,74. Обл.-вид. арк. 0,57.

Зам. № 30

Видавець: Український державний університет науки і технологій
вул. Лазаряна, 2, ауд. 2216, м. Дніпро, 49010.
Свідоцтво суб’єкта видавничої справи ДК № 7709 від 14.12.2022

Адреса видавця та дільниці оперативної поліграфії:
вул. Лазаряна, 2, Дніпро, 49010