Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістр

студента *Кравченка Богдана Сергійовича*

академічної групи *125м-22-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Виявлення DoS атак на основі гібридних нейронних мереж*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Романюк Н.М.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту *Кравченку Богдану Сергійовичу* **академічної групи** *125м-22-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Виявлення DoS атак на основі гібридних нейронних мереж***

затверджену наказом ректора НТУ «Дніпровська політехніка» від р. №

Розділ	Зміст	Термін виконання
Розділ 1	Провести аналіз загроз ІТС, розглянути атаки типу DoS і особливості їх реалізації, визначити інформативні параметри мережевого трафіку.	28.10.2023
Розділ 2	Визначити параметри трафіку, використовуючи які, можна ідентифікувати атаки типу DoS. У роботі синтезувати нейромережеві моделі, здатні на ідентифікацію атак типу DoS, а саме підтипів «back» та «neptune», проаналізувати адекватність синтезованих моделей.	16.11.2023
Розділ 3	В економічному розділі визначити витрати на впровадження результатів досліджень, а також розраховати характеристики підприємства, для якого використання результатів досліджень було б економічно доцільним.	08.12.2023

Завдання видано _____ Валерій КОРНІЄНКО
(підпис керівника) (ім'я, прізвище)

Дата видачі: 16.10.2023 р.

Дата подання до екзаменаційної комісії: 11.12.2023 р.

Прийнято до виконання _____ Богдан КРАВЧЕНКО
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 76 с., 16 рис., 3 табл., 4 додатка, 24 джерел.

Об'єкт дослідження: процес ідентифікації мережевих атак типу DoS (back, land, neptune, pod, smurf, teardrop).

Мета роботи: визначення можливості застосування нейромережевих моделей для ідентифікації мережевих атак типу DoS (back, land, neptune, pod, smurf, teardrop).

Методи дослідження: абстракція, дедукція, системний підхід, методи порівняння, кореляційний аналіз.

У спеціальній частині були розглянуті атаки типу DoS і особливості їх реалізації, визначені інформативні параметри мережевого трафіку, використовуючи які можна ідентифікувати ці атаки.

У роботі синтезовані нейромережеві моделі, здатні на ідентифікацію атак типу DoS, а саме підтипів «back» та «neptune», проаналізована адекватність синтезованих моделей.

В економічному розділі визначені витрати на впровадження результатів досліджень, а також розраховані характеристики підприємства, для якого використання результатів досліджень було б економічно доцільним.

Практичне значення роботи полягає у тому, що результати здійснених у роботі досліджень можуть бути використані у якості методологічної бази для розробки і впровадження ефективних нейромережевих засобів ідентифікації мережевих атак.

Новизна дослідження полягає у тому, що вперше визначено множину інформативних параметрів трафіку для нейромережевих моделей ідентифікації мережевих атак типів «back» та «neptune».

ІНФОРМАЦІЙНА БЕЗПКА, НЕЙРОННІ МЕРЕЖІ, НЕЙРОМЕРЕЖЕВІ МОДЕЛІ, ІДЕНТИФІКАЦІЯ КІБЕРАТАК, КІБЕРАТАКА, DoS.

ABSTRACT

Explanatory note: 76 p., 16 pic., 3 tabl., 4 app., 24 sources.

Object of study: the process of identifying network attacks such as DoS (back, land, neptune, pod, smurf, teardrop).

Purpose: to determine the possibility of using neural network models to identify network attacks such as DoS (back, land, neptune, pod, smurf, teardrop).

Research methods: abstraction, deduction, systematic approach, comparison methods, correlation analysis.

The special part of the paper discusses DoS attacks and features of their implementation, identifies informative parameters of network traffic that can be used to identify these attacks.

The paper synthesizes neural network models capable of identifying DoS attacks, namely the "back" and "neptune" subtypes and analyzes the adequacy of the synthesized models.

In the economic section, the costs of implementing the research results are determined, and the characteristics of the enterprise for which the use of the research results would be economically feasible are calculated.

The practical significance of the work is that the results of the research carried out in the thesis can be used as a methodological basis for the development and implementation of effective neural network-based means of identifying network attacks.

The novelty of the study is that for the first time a set of informative traffic parameters for neural network models for identifying network attacks of the "back" and "neptune" types was determined.

INFORMATION SECURITY, NEURONIC NETWORKS, NEURONIC NETWORK MODELS, IDENTIFICATION OF CYBER ATTACKS, CYBER ATTACKS, DoS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АНМ – асоціативних нейронних мереж;

АРТ – мережі адаптивної резонансної теорії;

БШП – багатошаровий персептрон;

ГОМ – глобальна обчислювальна мережа;

НМ – нейронна мережа;

НММ – нейромережева модель;

ПШН – прихований шар нейронів;

РБФ – нейронна мережа з радіальними базисними функціями;

СНМ – семантична нейронна мережа;

ТК – топографічна карта Кохонена;

DoS – Denial of Service, відмова в обслуговуванні;

IP – Internet Protocol;

TCP – Transmission Control Protocol, протокол керування передачею;

HTTP – Hyper Text Transfer Protocol, протокол передачі даних.

ЗМІСТ

с.

ВСТУП

Актуальність даного дослідження є вельми значущою в епоху, де інформаційні технології та програмне забезпечення є невід'ємною частиною повсякденного життя та діяльності людини. Неперервний розвиток цих технологій призводить до зростаючої інтеграції в різноманітні сфери, що підсилює важливість інформаційної безпеки.

В останні роки стало очевидно, що з кожним днем питання захисту інформаційних систем від мережевих атак стає все більш актуальним. Зростання популярності Інтернету супроводжується збільшенням кількості загроз для інформаційно-комунікаційних систем, які використовують Інтернет як канал передачі даних.

Значні економічні втрати, які можуть виникнути в результаті успішної реалізації мережевих атак, підкреслюють необхідність розвитку ефективних методів ідентифікації та запобігання таким атакам, як зовнішніх, так і внутрішніх.

Новітні дані від провідних організацій у сфері кібербезпеки, таких як ISACA та Symantec, свідчать про збільшення кількості та складності кібератак у порівнянні з попередніми роками. Це демонструє недостатню ефективність існуючих систем ідентифікації атак, які часто працюють на основі порівняння з вже відомими прикладами атак, та не здатні адекватно реагувати на нові, раніше невідомі види загроз.

У світлі цих викликів, вивчення і розробка нових, більш ефективних методів ідентифікації мережевих атак є вкрай важливими. Це становить основу для даного дослідження, яке має на меті внести вагомий вклад у покращення безпеки інформаційних систем.

Перспективним напрямком досліджень у цій області є використання штучних нейронних мереж для реалізації або доповнення існуючих систем ідентифікації мережевих атак, так як практична цінність існуючих рішень обмежена через велику кількість помилок, недостатню якість або довгий час

навчання, погана адаптація до багатьох особливостей функціонування різних інформаційних систем.

Мета роботи: визначення можливості застосування нейромережевих моделей для ідентифікації мережевих атак типу DoS (back, land, neptune, pod, smurf, teardrop).

Об'єкт дослідження – процес ідентифікації мережевих атак типу DoS (back, land, neptune, pod, smurf, teardrop).

Предмет дослідження – нейромережеві моделі процесу ідентифікації мережевих атак типу DoS (back, land, neptune, pod, smurf, teardrop).

Методи дослідження: абстракція, дедукція, системний підхід, методи порівняння, кореляційний аналіз.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Дослідження можливості використання методів теорії нейронних мереж для ідентифікації кібератак

У цьому розділі розглянуто існуючі типи нейронних мереж та проблеми, які можна вирішувати за допомогою їх застосування.

Під терміном «нейронна мережа» розуміють мережу елементів (штучних нейронів), пов'язаних між собою синаптичними зв'язками, [20] [21]. Основними конструктивними параметрами НМ є кількість вхідних, схованих і вихідних нейронів, структура зв’язків (топологія мережі), правила розповсюдження та комбінування сигналів, правила обчислення вихідного сигналу нейрона та правила навчання, що коректують зв'язки в мережі. Сукупність вказаних параметрів визначають (архітектуру НМ) вид НММ.

Окреслюючи сферу застосування НМ слід врахувати, що можливості мережі значною мірою залежать від виду НММ. Результати вказують на те, що розвиток сучасних НМ йде шляхом пристосування базових архітектур до вирішення практичних задач, [22]. При цьому ряд архітектур вже втратили свої передові позиції і використовуються тільки в якості допоміжних.

Нейронні мережі на базі багатошарового персептрону. БШП, представляє собою НМ з прямим розповсюдженням сигналу, яка складається із декількох послідовно з'єднаних між собою шарів штучних нейронів, [20] [22].

Навчання БШП виконується методом "з вчителем". При цьому вагові коефіцієнти змінюються так, щоб мінімізувати середньоквадратичний функціонал помилки НМ.

Кількість вхідних параметрів БШП має бути обмеженою. Вхідні параметри можуть бути як дискретні, так і неперервні. Вважається, що мінімальна кількість навчальних прикладів має бути в 10-20 разів більша від кількості вхідних параметрів. Максимальна кількість навчальних прикладів залежить від кількості схованих нейронів, [23].

До переваг БШП відносять можливість навчання на корельованих та зашумлених навчальних даних. Однак для якісного навчання необхідно пропорційно представити в навчальних даних всі аспекти піддослідного процесу. Процес навчання багато ітераційний та довготривалий. Особливістю навчання БШП є невелика кількість емпіричних параметрів величини яких можуть бути визначені в процесі адаптації НМ до поставленої задачі. Тому результати навчання на однакових прикладах практично незмінні.

Існує можливість донавчання БШП в процесі застосування, [23] [24], однак наведені підходи потребують доопрацювання.

Цим же пояснюється і необхідність вдосконалення методики автономного функціонування БШП. Результати навчання БШП інтерпретуються у вигляді ймовірності та піддаються вербалізації.

В теорії, [23] [24], - інтелектуальні можливості БШП, які оцінюються по критеріям якості навчання, екстраполяції навчальних результатів та обсягу пам'яті вважаються найвищими серед класичних НМ. Технічна реалізація БШП визначається достатньою швидкістю прийняття рішення, що пояснюється необхідністю проведення розрахунків, пов'язаних тільки з прямим проходженням сигналу. Традиційної сферою застосування БШП є системи розпізнавання образів.

Для моделювання часових рядів створено такі модифікації БШП, як мережі Елмена та Джордана, а для аналізу зображень – згорткові НМ. Основою архітектурною відмінністю НМ Джордана є наявність зворотних зв'язків, які використовуються для подачі на вхід мережі затриманий на один або декілька тактів вихідний сигнал. Мережа Елмана відрізняється від мережі Джордана тільки тим, що зворотні зв'язки йдуть не від вихідних, а від схованих нейронів. Вважається, [23] [24], що наявність зворотних зв'язків потенційно дозволяє ефективніше, по відношенню до БШП, врахувати передісторію піддослідних процесів та підвищити стійкість до часових спотворень. Однак використання зворотних зв'язків призводить до значного збільшення терміну навчання. Тому в класичному вигляді є сенс використовувати тільки відносно невеликі мережі

Елмена та Джордана. Зазначимо, що НМ Елмана знайшла застосування при розпізнавання фонем в процесі аналізу аудіо інформації та для класифікації відеоінформації.

Згорткові НМ являються модифікованим БШП, структура якого пристосована для розпізнавання двовимірних зображень з високим рівнем шуму. Їх основною сферою застосування є системи розпізнавання рукописного тексту. Крім того, відомі спроби використання в системах комп'ютерного зору та розпізнавання мови. В цих системах, по відношенню до БШП, згорткові НМ мають менші розміри та краще враховують топологію вхідних даних. Однак складний алгоритм навчання призводить до збільшення терміну навчання. В літературі не знайдено методики пристосування як згорткових НМ, так і мереж Єлмена та Джордана до автономного функціонування.

Мережа з радіальними базисними функціями. В найбільш простій формі РБФ складається із вхідного, схованого та вихідного нейронних шарів. Кожен з схованих нейронів призначений для зберігання окремого еталонного образу, який відповідає окремому класу. Після нелінійного перетворення сигнали від нейронів СШН потрапляють у вихідний шар нейронів, що мають лінійні функції активації. Вихід РБФ можливо трактувати як ймовірність віднесення невідомого образу до певного еталону. Процес навчання НМ багатоітераційний. Однак знайти теоретичний функціонал оптимальної кількості ітерацій не вдалось, хоча і вважається що їхня кількість менша ніж у БШП. Слід зазначити практичну незмінність результатів навчання на фіксованій навчальній вибірці. Методики вербалізації РБФ не знайдено. Вхідні параметри РБФ можуть бути як дискретні, так і неперервні. Максимальна кількість навчальних прикладів залежить від кількості схованих нейронів. Базуючись на аналізі структури РБФ можна зробити висновок про низьку якість навчання на корельованих та зашумлених даних. По відношенню до БШП, РБФ дозволяє моделювати довільну функцію за допомогою всього одного проміжного шару, що в деякій мірі спрощує архітектуру. Крім того, РБФ навчається на порядок швидше, а її програмна реалізація простіша.

Водночас мережа РБФ має і цілий ряд суттєвих недоліків. В першу чергу, це велика кількість емпіричних параметрів, що використовуються при визначенні вагових коефіцієнтів нейронів. Теоретичні методи не гарантують точного визначення оптимальної кількості схованих нейронів, яка є однією із найважливіших характеристик НМ. По цим причинам РБФ погано пристосована до автономного застосування. Ще одним важливим недоліком є погана екстраполяція результатів за межею області відомих даних. Тому в навчальній вибірці слід представити весь діапазон можливих вхідних даних та еталонних образів.

Наведені в, [20-24] , результати порівняння обчислювальних можливостей РБФ та БШП вказують на те, що для моделювання складних функцій мережа РБФ потребує більшого числа нейронів. Як наслідок, програмна реалізація РБФ буде проводити класифікацію довше та витрачати більше ресурсів, ніж БШП.

Традиційною сферою застосування РБФ є розпізнавання образів. Топографічна карта Кохонена. Структурно ТК складається із вхідного і вихідного (топографічного) нейронних шарів, [22]. Кількість нейронів вхідного шару дорівнює кількості компонент вхідних образів. Кожен вхідний нейрон пов'язаний з кожним топографічним нейроном, який відповідає певному класу образів. Обсяг навчальної вибірки, в якій можуть бути несистематичні помилки, повинен в 5-10 раз перевищувати кількість вхідних параметрів. Навчальні дані можуть мати як дискретний так і неперервний характер.

В процесі багатоітераційного навчання розраховуються вагові коефіцієнти топографічних нейронів та відбувається розподіл бібліотечних образів на класи (кластери), кількість яких визначається необхідною точністю розпізнавання. При цьому мережа організується так, що нейрони, які відповідають образам, розміщеним близько в просторі входів, розміщуються близько і на топографічній карті. Кількість навчальних ітерацій має бути як мінімум в 10 разів більша, ніж кількість навчальних прикладів. Після

закінчення навчання на вхід ТК можна подавати нові образи для розпізнавання. Крім того, ТК може використовуватись як детектор нових явищ.

Значним недоліком ТК є велика кількість емпіричних параметрів, від яких залежить якість навчання. Порівняння обчислювальних можливостей НМ типу ТК з БШП вказує на значно менший термін навчання, що разом з можливістю оперативної адаптації меж кластерів до зміни вхідної інформації зумовлює ефективність їх використання з метою розвідувального аналізу даних. Проте узагальнюючі можливості БШП, а також обсяг його пам'яті набагато вищі.

Традиційною сферою застосування ТК є візуалізація класифікованих даних в системах розпізнавання образів та аналізу текстової інформації. Відомі спроби застосування ТК в системах розпізнавання звукової інформації та для розв'язання оптимізаційних задач.

Базовим типом ймовірнісних НМ є PNN, в якій для віднесення невідомого образу x до k-го класу застосовується вираз

$$h_k c_k f_k(x) > h_i c_i f_i(x), \exists i \in \{N\} \qquad (1.1)$$

де {N} - множина всіх класів,

i - довільний клас,

hk (hi) - апріорна ймовірність класифікації образу як класу k (i),

ck (ci) - ціна помилки класифікації образу як класу k (i),

fk(x) і fi(x) - функції щільності ймовірності для класів k та i.

Оцінка функції fk(x) і fi(x) визначається на основі безітераційного запам'ятовування навчальних прикладів з застосуванням вагової функції Гауса. Тому процес навчання PNN відбувається швидко. Ще однією перевагою PNN є наявність тільки одного управляючого параметру (радіусу функції Гауса). Вхідні параметри можуть бути як дискретні, так і неперервні. Кількість навчальних прикладів дорівнює кількості схованих нейронів. Також до переваг PNN відноситься якісна класифікація на невеликій навчальній вибірці, низька

чутливість до помилок в навчальних даних, ймовірнісний зміст класифікації, простота реалізації, пристосованість до автономного функціонування.

Загальними недоліками PNN є якісна класифікація тільки в діапазоні навчальних даних, потенційно висока обчислювальна ресурсоємність. Традиційною PNN використовується для виділення найбільш інформативних параметрів

До класичних АНМ відносяться мережі Хопфілда, Хеммінга та Коско, [23] [24]. Їх основною перевагою відносно НМ з прямим розповсюдженням сигналу є динамічність та ітераційність обробки даних, що має позитивно впливати на обчислювальні можливості. Навчання АНМ відбувається шляхом безпосередньої обробки навчальних даних.

Однак обсяг пам'яті АНМ менший, в порівнянні з БШП. Так, в [12-20] наведено формулу для розрахунку максимального обсягу збережених образів в мережі Хопфілда при умові безпомилкового розпізнавання всього обсягу пам'яті:

$$p_{max} \leq (0{,}05 \times N) \tag{1.2}$$

де N - кількість нейронів в мережі.

Навчальні образи повинні бути слабо корельовані між собою. Інакше можливо виникнення перехресних асоціацій при їх пред'явленні на вході мережі. До особливостей мережі Хеммінга відносять можливість розпізнавання тільки бінарних образів, визначення тільки номеру еталону при класифікації та неможливість розпізнавання зашумлених сигналів. Мережу Коско вважають розвитком НМ Хопфілда, призначеним для вирішення задачі встановлення асоціації між вхідними та еталонними образами, [20]. Обсяг пам'яті таких НМ дещо вищий, але недостатня апробованість ускладнює їх використання в СЗІ. Традиційною сферою використання АНМ є вирішення задач класифікації зашумлених даних та виділення прототипів.

В [20] доведена доцільність обробки статистичних даних за допомогою асоціативних мереж перед їх використанням в БШП з метою зменшення кількість вхідних параметрів. Крім того, відомі спроби застосування АНМ для оптимального розподілу ресурсів та активної кластеризації.

До загальних недоліків АНМ відносять обмеженість пам'яті, квадратичну залежність кількості зв'язків від розмірності вхідного сигналу, непередбачуваність функціонування за рахунок помилкової і нестабільної класифікації та неможливість навчання на корельованих образах.

Основною особливістю мережі АРТ є можливість динамічного запам'ятовування нових образів без повного перенавчання та втрати інформації про образи, що вже були в ній збережені. Для цього в НМ використовується специфічний по відношенню до класичних НМ дворівневий алгоритм порівняння вхідного образу з вмістом пам'яті, [23] [24].

АРТ може використовуватись для розвідувального аналізу даних та здатна навчатись на корельованих навчальних прикладах, з фіксованою кількістю вхідних параметрів. Обсяг навчальної вибірки обмежується тільки обчислювальними можливостями програмно-апаратної реалізації. При цьому навчання мережі АРТ реалізується методом "без вчителя", а очікуваний вихід в навчальних прикладах не використовується. Для якісного навчання в навчальних прикладах слід відобразити всі аспекти піддослідного процесу. Екстраполяція результатів навчання за межі навчальної вибірки малодостовірна. Результат класифікації можливо представити у вигляді ймовірності. Аналіз літератури не виявив алгоритму вербалізації АРТ.

Різноманітні модифікації АРТ можуть працювати як з дискретним, так і з неперервними вхідними параметрами. Обсяг пам’яті АРТ по відношенню до БШП дещо менший. До позитивних рис АРТ відносять швидкий доступ до бібліотечних образів, стабільність і закінченість процесів навчання та розпізнавання, короткий термін навчання, зрозумілість функціонування та простоту програмної реалізації. Недоліками АРТ є неможливість довготривалої класифікації зашумлених образів, чутливість навчання до порядку пред'явлення

вхідних векторів та велика обчислювальна складність процесу класифікації, [22].

Традиційно АРТ використовуються для класифікації образів та розпізнавання зображень.

Семантична нейронна мережа є розвитком активних семантичних мереж та НМ Маккаллока-Піттса та може використовуватись на всіх етапах розбору тексту/ Особливістю СНМ є те, що проміжним нейронам призначається відповідність деяких елементів семантики предметної області або моделі тексту. Елемент може представляти окремий символ, сукупність деяких символів тексту або сукупність понять і відношень між поняттями, що можна абстрагувати як єдине ціле. В випадку наявності відповідного елементу в тексті нейрон приймає значення "істина", а в протилежному випадку - "не правда".

Зв'язки між нейронами представляють собою відношення між елементами семантики. Фактори впевненості представляються у вигляді градієнтних величин, що оброблюються і передаються нейронами. Зміст тексту, представлений станом СНМ, оброблюється як потік градієнтних даних, що передається між нейронами.

Навчальні дані СНМ повинні представляти базу даних та базу знань імітаційної моделі предметної області. При цьому кількість навчальних прикладів необмежена. Вони можуть бути частково зашумлені та корельовані. Для якісної класифікації в навчальних прикладах мають бути відображені більшість можливих варіантів тексту. Термін навчання досить короткий, а процес навчання та до навчання можна автоматизувати.

Крім задачі класифікації вхідної символьної послідовності, СНМ може вирішувати задачу формування коректних словозмін вказаної послідовності.

Проведений аналіз сучасних видів НММ дозволяє стверджувати, що з точки зору їх застосування характеристики задач можливо розділити на категорії, що відповідають: навчальним даним, обмеженням процесу навчання, обчислювальним потужностям, вихідній інформації, технічній реалізації, сфері застосування.

Деталізуємо вказані категорії.

1 Основними характеристики навчальних даних являються:

- кількість параметрів, що характеризують навчальний приклад.
- вид параметрів, дискретний (символьний) чи безперервний (числовий).
- кількість доступних навчальних прикладів. Наприклад, в задачах розпізнавання змісту тексту кількість навчальних прикладів можна вважати необмеженою. Для інших задач (розпізнавання мережевих кібератак) кількість навчальних прикладів може бути приблизно рівною кількості вхідних параметрів.
- наявність помилок (шуму) в навчальних прикладах.
- наявність кореляції навчальних прикладів.
- можливість попередньої обробки вхідних даних для та видалення шуму.
- можливість відображення в навчальній виборці всіх аспектів піддослідного процесу. Наприклад, чи можливо відобразити в навчальній виборці сигнатури всіх типів аномальної поведінки або сигнатури всіх вірусів.
- пропорційність навчальних прикладів, що відповідають різним аспектам піддослідного процесу.

2 Обмеження процесу навчання обумовлюються:

- максимальним терміном навчання.
- необхідністю представлення в навчальних даних очікуваного вихідного сигналу НМ.
- можливістю автоматизації процесу навчання.
- можливістю донавчання на експлуатації.
- вимогами до якості навчання, яке звичайно оцінюють по величині максимальної та середньої помилки розпізнавання навчальних та тестових даних.
- можливістю навчання НМ в лабораторних умовах.
- вимогою до незмінності вихідного сигналу мережі для різних прикладів з однаковими параметрами.

3 На практиці вимоги до обчислювальних потужностей визначаються максимальною кількістю прикладів (обсяг пам'яті), яку може запам'ятати НМ для досягнення необхідної точності розпізнавання. В свою чергу точність розпізнавання характеризується величинами максимальної та середньої помилки НМ на даних які можуть виходити за межі множини навчальної вибірки. Відповідно виникає задача екстраполяції результатів навчання НМ за межі навчальної вибірки прикладів.

4 Вимоги до вихідної інформації НМ вказують на те, в якому вигляді має бути представлена ця інформація. Наприклад, при розпізнавані вірусів може виникнути необхідність не тільки визначення ситуації типу “несправність в програмному забезпеченні”, але й розрахунку ймовірності цієї ситуації або графічного відображення таких ситуацій на площину, що дозволить провести остаточну класифікацію користувачеві. Ще однією вимогою може бути необхідність визначення вербальних залежностей між вхідною та вихідною інформацією.

5 Обмеження технічної реалізації НМ стосуються швидкості прийняття рішення, інтеграції в існуючі СЗІ, обсягу та складності програмної реалізації.

6 Сфера застосування визначає системи, в яких буде використовуватись НМ. На сьогодні достатньо дослідженим є використання НМ для розпізнавання образів, проведення оптимізації та аналізу тексту. Відзначимо, що системи розпізнавання образів принципово відрізняються від систем аналізу тексту тим, що в них кількість вихідних та кількість комбінацій вхідних параметрів принципово обмежена. В системах аналізу тексту ця кількість принципово необмежена. Крім того, сфера застосування визначається пристосованістю мережі до автономного функціонування. Для цього в архітектурі НМ повинно бути передбачено можливість повної автоматизації процесу донавчання на експлуатації.

1.2 Нейромережеві моделі та методи оцінювання параметрів безпеки інформаційних систем

У цьому підрозділі розглянуто сучасні нейромережеві моделі і методи, які застосовуються в СЗІ.

Методи простої та семантичної класифікації мережевих атак. Методи розроблено в межах нейромережевої технології виявлення мережевих комп'ютерних атак за допомогою програмного комплексу «Snort», описаної в роботі, [23]. Технологія передбачає застосування двох нейромережевих методів виявлення атак – простої класифікації (ПСК) та семантичної класифікації (ССК). В якості вхідних параметрів використовуються параметри мережевих пакетів транспортного рівня стеку протоколів TCP/IP. В методі ПСК використано БШП з 10 вхідними нейронами та 2 нейронами у вихідному шарі. Для оптимізації кількості схованих нейронів пропонується застосування конструктивних алгоритмів.

Наведено вираз для розрахунку корекції вагових коефіцієнтів нейронів вихідного шару:

$$\Delta w_{jk}(i) = -\eta\big(y_n(i) - f(x_i)\big)\varphi'\big(v_n(i)\big)y_n, \tag{1.4}$$

де η – коефіцієнт швидкості навчання,

n – номер нейрону у вихідному шарі,

i – номер навчальної ітерації,

v_n – інформаційне поле, отримане на вході функції активації,

y_n – вихідний сигнал n-го вихідного нейрону,

φ' – похідна функції активації,

$f(x_i)$ – бажаний відгук і-го нейрону.

Зазначимо відсутність детального опису процесу оптимізації структури БШП. В методі ССК пропонується використання топографічної ТК, вибір якої обґрунтовується її невисокою ресурсоємністю. В обох методах передбачено

обробку вхідних параметрів з метою зменшення кількості вхідних параметрів НМ.

Метод виділення мережевих атак із типового мережевого трафіку (ВМА), описаний в роботі [21-23]. Метод застосовується для розпізнавання мережевих атак. Запропоновано застосування БШП з 2 СШН. ВШ такого БШП складається із 9 нейронів, а ШВ – із 1 нейрону. Зазначено, що вибір БШП з такою структурою пояснюється вимогами гнучкості та функціональності. Тобто використано багатокритеріальну оптимізацію структури НМ. Вказано на попередню обробку статистики, що використовувалась для навчальної та тестової вибірки.

Спосіб виявлення DDoS-атак (СВДА), наведений в роботі [23]. Запропоновано використання нечітких НМ. Пропозиція ґрунтується на перспективності НМ такого типу. Акцент ставить на розпізнаванні DDoS-атаки типу SYN Flood. Для формалізації знань експертів про DDoS-атаки було створено 5 лінгвістичних змінних, кожна з яких характеризує одну з компонент вектора параметрів мережевого трафіку, що використовується для формування вхідних параметрів НМ. До вказаних лінгвістичних змінних відносяться: X1 – час отримання пакетів, X2 – процент пакетів з різних зовнішніх ip-адрес, X3 – процент пакетів з різних портів, X4 – процент пакетів з пошкодженими заголовками, S – степінь впевненості. Розроблено предикатні правила виду: Якщо X1 = «великий»-> Y-> «висока».

Запропоновано представити нечіткий класифікатор у вигляді НМ з прямим розповсюдженням сигналу, що навчається за допомогою модифікованого алгоритму зворотного розповсюдження помилки. Модифікація полягає у пристосуванні класичного алгоритму до нечітких нейронів «І» та «АБО». Таким чином, основною відмінністю СВДА є можливість застосування для навчання НМ експертних знань.

Метод використання нейронної мережі гібридної структури типу CounterPropagation (НМГС), описаний в роботах [21-23]. Метод призначено для виявлення мережевих атак на вебсервер. Особливістю мережі

CounterPropagation є комбінація ТК з БШП. Вхідними даними методу є параметри мережевого трафіку, що передається по протоколам IP, TCP, HTTP, HTTPS, CGI, SQLNet. В методі передбачена процедура попередньої обробки вхідних параметрів НМ за рахунок представлення їх у вигляді графічних образів (піфограм), котрі використовуються в когнітивній графіці. Метою попередньої обробки є мінімізація розмірності вхідних даних. Графічне представлення визначило необхідність застосування в методі шару Кохонена. Використання персептронного шару обґрунтоване з позицій обчислювальної ефективності. Таким чином, в методі передбачено багатокритеріальну оптимізацію виду та однокритеріальну оптимізацію параметрів НММ. Також в методі застосована процедура оптимізації параметрів навчання НМ, яка дозволяє до 10 разів зменшити величину помилки розпізнавання атак.

Адаптивна система виявлення атак (АСВА), описана в роботі,[21-23]. Система призначена для розпізнавання мережевих атак та базується на спільній роботі ТК і БШП, що виконують завдання кластеризації і класифікації даних. Виявлення атак, котре проводиться в декілька етапів, стало можливим завдяки тому, що в базу даних експертної системи вносилася інформація про зміни в поведінці конкретного об'єкта на протязі деякого відрізка часу. Доводиться, що оптимізація архітектури дозволить підвищити точність та оперативність розпізнавання. В якості вхідних даних використано параметри мережевого трафіку по протоколу TCP. Для обробки вхідних даних використано метод ковзаючого часового вікна. ТК використана для попередньої обробки даних, що поступають на вхід БШП з метою їх стиснення та підвищення інформативності. Наведено математичний вираз для розрахунку частоти визначення нейрону в позиції (i,j) в якості нейрону-переможця. Надалі ця частота використовується для визначення центрів та границь кластерів. Структура БШП оптимізована з точки зору відповідності обсягу контрольованих ресурсів.

Нейромережева технологія виявлення та класифікації мережевих атак (ВКМА), описана в роботі, [20-24]. В технології запропоновано використання тришарової НМ, що навчається методом зворотного поширення помилки. При

цьому для розпізнавання кожного виду мережевої атаки застосовується окрема НМ. Як вхідні параметри використовуються параметри мережевого трафіку по стеку протоколів TCP/IP. Для формування навчальної вибірки пропонується використати базу даних KDD. Наведено словесний опис та фрагменти програмного коду для підготовки вхідних даних із цієї бази даних до виду вхідних параметрів НМ. Однією із цілей підготовки є зменшення обсягу навчальної вибірки НМ. Описи підходів до оптимізації виду та параметрів НММ відсутні.

Метод розпізнавання аномалій мережевого трафіку (РАМТ), розроблений в роботі, [20-24]. Методом передбачене використання НМ типу БШП. В якості вхідних даних НМ використано параметри заголовків IP-дейтаграм. Вибір архітектури НМ базується на твердженні про високі апроксимаційні можливості БШП. БШП складається із трьох шарів нейронів. Кількість нейронів ВШ – 18, що дорівнює кількості параметрів заголовку IP-дейтаграми. Кількість нейронів у ШВ 2. Вихід нейрону №1 відповідає за наявність аномалії, а вихід нейрону №2 за безпечний стан мережевого трафіку. Наведені вирази для розрахунку кількості нейронів у СШН. Таким чином, методом передбачено оптимізацію параметрів архітектури НМ. Для спрощення створення репрезентативної вибірки розроблено метод уточнюючих сигнатур, суть якого полягає у введенні додаткових штучно створених сигнатур, що описують апріорно аномальний трафік. Таким чином, в методі в неявному вигляді можливо використати експертні дані про мережеві атаки.

Алгоритм перетворення параметрів трафіку (АППТ) описано в роботі, [20-24]. Алгоритм призначений для отримання із мережевого трафіку вхідних даних для нейромережевої системи виявлення мережевих атак. В якості вхідної інформації зазначеного алгоритму використовуються параметри TCP-сесії. Перетворення параметрів трафіку застосовується з метою зменшення кількості вхідних параметрів НМ і збільшення їх інформативності та реалізується за допомогою математичного апарату, що базується на методі головних компонент. В алгоритмі оптимізація виду та параметрів НММ не передбачена.

В результаті проведеного аналізу можливо зробити висновки про те, що важливим та актуальним напрямком підвищення ефективності систем розпізнавання кібератак на ресурси Інтернет-орієнтованих інформаційних систем є застосування нейромережевих моделей, методів та засобів оцінювання параметрів безпеки.

Не дивлячись на певні досягнення в цій області, ефективному застосуванню таких засобів оцінювання заважають ряд недоліків, для виправлення яких повинні бути проведені подальші дослідження.

Для досліджень по ідентифікації кібератак мною обрано метод використання нейронної мережі гібридної структури.

1.3 Висновки. Постановка завдання

Отже для визначення можливості застосування нейромережевих моделей для ідентифікації мережевих атак, на прикладі атак типу DoS (back, land, neptune, pod, smurf, teardrop), необхідно розв'язати такі основні задачі:

- визначити інформативні параметри мережевого трафіку з точки зору ідентифікації мережевих атак типу DoS (back, land, neptune, pod, smurf, teardrop);
- множину даних розподілити на три підмножини, зокрема: навчальну, тестову та контрольну вибірки;
- синтезувати гібридні моделі, які використовують нейронні мережі для ідентифікації мережевих атак типу DoS (back, land, neptune, pod, smurf, teardrop);
- проаналізувати адекватність синтезованих моделей.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Визначення інформативних параметрів мережевого трафіку, з точки зору ідентифікації мережевих атак типу DoS

У цьому підрозділі потрібно визначити інформативні параметри мережевого трафіку, з точки зору ідентифікації мережевих атак типу DoS. Для цього необхідно:

- визначити ключові особливості реалізації мережевих протоколів, через недоліки яких здійснюються мережеві атаки типу DoS;
- визначити ключові особливості мережевих сервісів, що використовують ці протоколи, на які направлені мережеві атаки типу DoS;
- відповідно до визначених особливостей мережевих протоколів та сервісів виділити вагомі параметри мережевого трафіку;
- виконати редукцію множини параметрів трафіку.

У якості вхідних даних для моделей буде використовуватись база KDD (набір даних - образів мережевих з'єднань, зареєстрованих через певні проміжки часу, для змагань «The Third International Knowledge Discovery and Data Mining Tools Competition»), так як в ній наведена множина даних мережевих з'єднань у різних станах функціонування, як при здійсненні атак, так і при їх відсутності.

Більшість непромислових мереж використовує стек протоколів TCP/IP. Його розроблено з ініціативи Міністерства оборони США, понад 20 років тому, як набір загальних протоколів для різнорідного мережевого середовища для зв'язку експериментальної мережі ARPAnet з іншими мережами.

У мережі ARPA зв'язок між двома комп'ютерами здійснювалася з використанням протоколу Internet Protocol (IP), який і донині є одним з основних у стеку TCP / IP і фігурує в назві стека. Значний внесок у розвиток стека, що отримав свою назву від популярних протоколів IP та TCP, внесли фахівці з університету Берклі, які реалізували протоколи стека у операційній системі UNIX. Через таку поширеність цього протоколу, з його застосуванням і

проводиться більшість кібератак, виходячи з цього для проведення досліджень у даній роботі обрано саме стек протоколів TCP/IP.

2.1.1 Структура стеку протоколів TCP / IP

Стек TCP/IP має чотирирівневу архітектуру, яка складається з таких рівнів, як прикладний, транспортний, міжмережевий та мережевий. Відносно до моделі OSI/ISO кожен рівень має один або декілька відповідних йому.

Таблиця 2.1 – Відповідність рівнів стеку TCP/IP до моделі OSI

прикладний	прикладний
представницький	
сеансовий	
транспортний	транспортний
мережевий	міжмережевий
канальний	фізичний
фізичний	

Самий нижній (рівень IV), фізичний рівень відповідає фізичному і канальному рівням моделі OSI. Цей рівень у протоколах TCP / IP не регламентується, але підтримує всі популярні стандарти фізичного і канального рівня: для локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet, 100VG-AnyLAN, для глобальних мереж - протоколи з'єднань "точка-точка" SLIP і PPP, протоколи територіальних мереж з комутацією пакетів X.25, frame relay. Розроблена також спеціальна специфікація, що визначає використання технології ATM як транспорт канального рівня. Зазвичай при появі нової технології локальних або глобальних мереж вона швидко включається в стек

TCP / IP за рахунок розробки відповідного RFC, що визначає метод інкапсуляції пакетів IP у її кадри.

Наступний рівень (рівень III) - це рівень міжмережевої взаємодії, що займається передачею пакетів з використанням різних транспортних технологій локальних мереж, територіальних мереж, ліній спеціального зв'язку і т. п. В якості основного протоколу мережевого рівня (у термінах моделі OSI) у стеку використовується протокол IP, що споконвічно проектувався як протокол передачі пакетів у складених мережах, що складаються з великої кількості локальних мереж, об'єднаних як локальними, так і глобальними зв'язками. Тому протокол IP добре працює в мережах зі складною топологією, раціонально використовуючи наявність у них підсистем і ощадливо витрачаючи пропускну здатність низькошвидкісних ліній зв'язку. Протокол IP є дейтаграмним протоколом, тобто він не гарантує доставку пакетів до вузла призначення, але намагається це зробити.

До рівня міжмережевої взаємодії відносяться і всі протоколи, пов'язані з складанням і модифікацією таблиць маршрутизації, такі як протоколи збору маршрутної інформації RIP (Routing Internet Protocol) і OSPF (Open Shortest Path First), а також протокол міжмережевих керуючих повідомлень ICMP (Internet Control Message Protocol). Останній протокол призначений для обміну інформацією про помилки між маршрутизаторами мережі і вузлом - джерелом пакета. За допомогою спеціальних пакетів ICMP повідомляється про неможливість доставки пакета, про перевищення часу життя або тривалості зборки пакета з фрагментів, про аномальні величини параметрів, про зміну маршруту пересилання і типу обслуговування, про стан системи і т.п.

Наступний рівень (рівень II) називається основним. На цьому рівні функціонують протокол керування передачею TCP (Transmission Control Protocol) і протокол дейтаграм користувача UDP (User Datagram Protocol). Протокол TCP забезпечує надійну передачу повідомлень між віддаленими прикладними процесами за рахунок утворення віртуальних з'єднань. Протокол UDP забезпечує передачу прикладних пакетів дейтаграмним способом, як і IP, і

виконує тільки функції сполучної ланки між мережним протоколом і численними прикладними процесами.

Верхній рівень (рівень I) називається прикладним. Прикладний рівень об'єднує всі служби, які надаються системою користувальницькими додатками. Прикладний рівень реалізується програмними системами, побудованими в архітектурі клієнт-сервер, що базуються на протоколах нижніх рівнів. Цей рівень постійно розширюється за рахунок приєднання до старих, мережевих служб типу Telnet, FTP, TFTP, DNS, SNMP порівняно нових служб таких як протокол передачі гіпертекстової інформації HTTP.

Отже кожен із цих рівнів несе на собі деяке навантаження за рішенням основного завдання - організації надійної й продуктивної роботи ГОМ (глобальних обчислювальних мереж), частини якої побудовані на основі різних мережевих технологій.

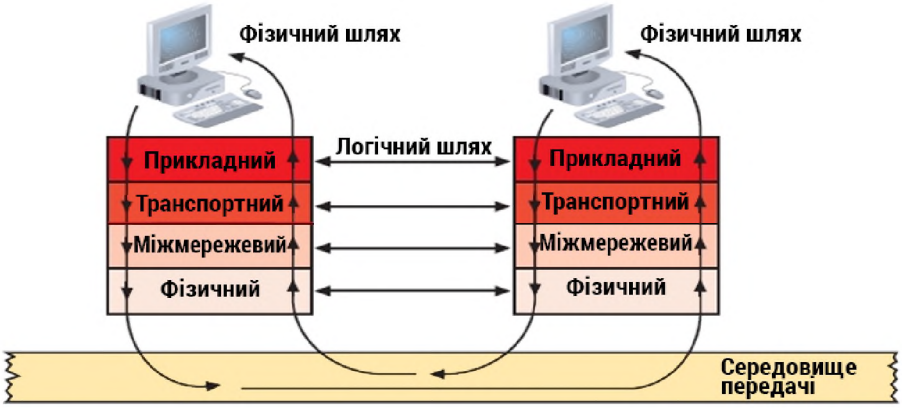


Рисунок 2.1 – Передача даних через структуру протоколу TCP/IP

Як і в моделі OSI, дані в більш верхніх рівнів інкапсулюються в блоки даних більше нижніх рівнів.

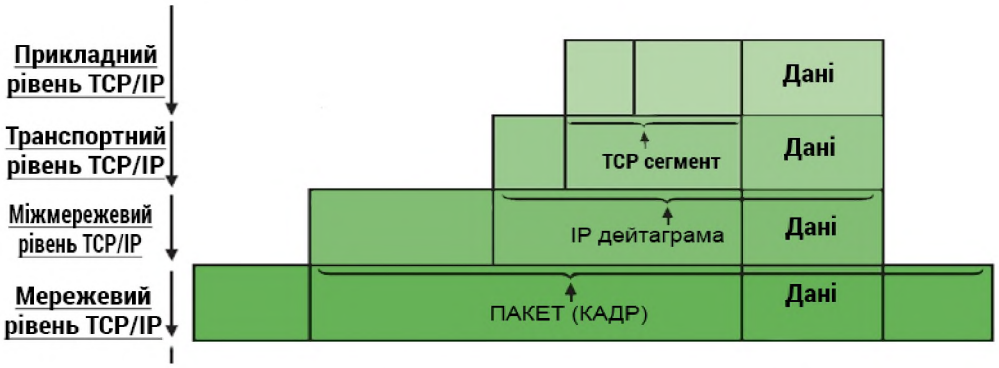


Рисунок 2.2 – Інкапсуляція у стеку TCP/IP

Ідеологічною відмінністю архітектури стека TCP/IP від багаторівневої організації інших є інтерпретація функцій нижнього рівня - рівня мережевих інтерфейсів. Протоколи цього рівня повинні забезпечувати інтеграцію в складену мережу інших мереж: мережа TCP/IP повинна мати засоби включення в себе будь-якої іншої мережі, яку б внутрішню технологію передачі даних ця мережа не використовувала. Як наслідок - цей рівень не можна визначити раз і назавжди. Для кожної технології, що включає в складену мережу підмережі, повинні бути розроблені власні інтерфейсові засоби. До таких інтерфейсових засобів належать протоколи інкапсуляції IP-пакетів рівня міжмережевої взаємодії в кадри локальних технологій.

Рівень мережевих інтерфейсів у протоколах TCP/IP не регламентується, але він підтримує всі популярні стандарти фізичного й канального рівнів: для локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, 100VG-AnyLAN, для глобальних мереж - протоколи з'єднань «точка-точка» SLIP і PPP, протоколи територіальних мереж з комутацією пакетів X.25, frame relay.

2.1.2 Особливості реалізації протоколу TCP/IP

Задачею протоколу, як випливає з його назви: «протокол керування передачею», є контроль надійної передачі даних між хостами, для забезпечення цього між хостами встановлюється логічне з'єднання, яке зветься TCP-сесією (рисунок 2.4). Протокол TCP працює у форматі архітектури клієнт-сервер. Хост який надсилає запит на отримання сервісу є клієнтом, той хто відповідає на запит зветься сервером. Хости зв'язуються один з одним по TCP-портам, на стороні клієнта це, як правило, динамічний порт, а на стороні сервера це загальновідомий або зареєстрований порт, номер якого відповідає протоколу прикладного рівня. Номери портів та значення інших параметрів заносяться до заголовка TCP-сегменту.

Під терміном сервер (server) прошу розуміти комп'ютер під управлінням операційної системи, який має доступ до IP-мережі та надає послуги одного чи

декількох сервісів прикладного рівня. В свою чергу на сервері-комп'ютері встановлені спеціальні сервер-програми, які забезпечують роботу протоколів прикладного рівня. Таким чином, якщо це веб-сервер, то на ньому мусить бути встановлена одна із таких програм, як наприклад: Apache HTTP Server. На практиці сервер-комп'ютер надає послуги відразу декількох сервісів, тобто на ньому може бути встановлено більше однієї сервер-програми, що забезпечують роботу декількох протоколів прикладного рівня. Наприклад сервер-комп'ютер може бути одночасно веб-сервером і FTP-сервером та забезпечувати роботу протоколів HTTP, HTTPS та FTP, а також забезпечувати функціонування пошти, PHP и MySQL.

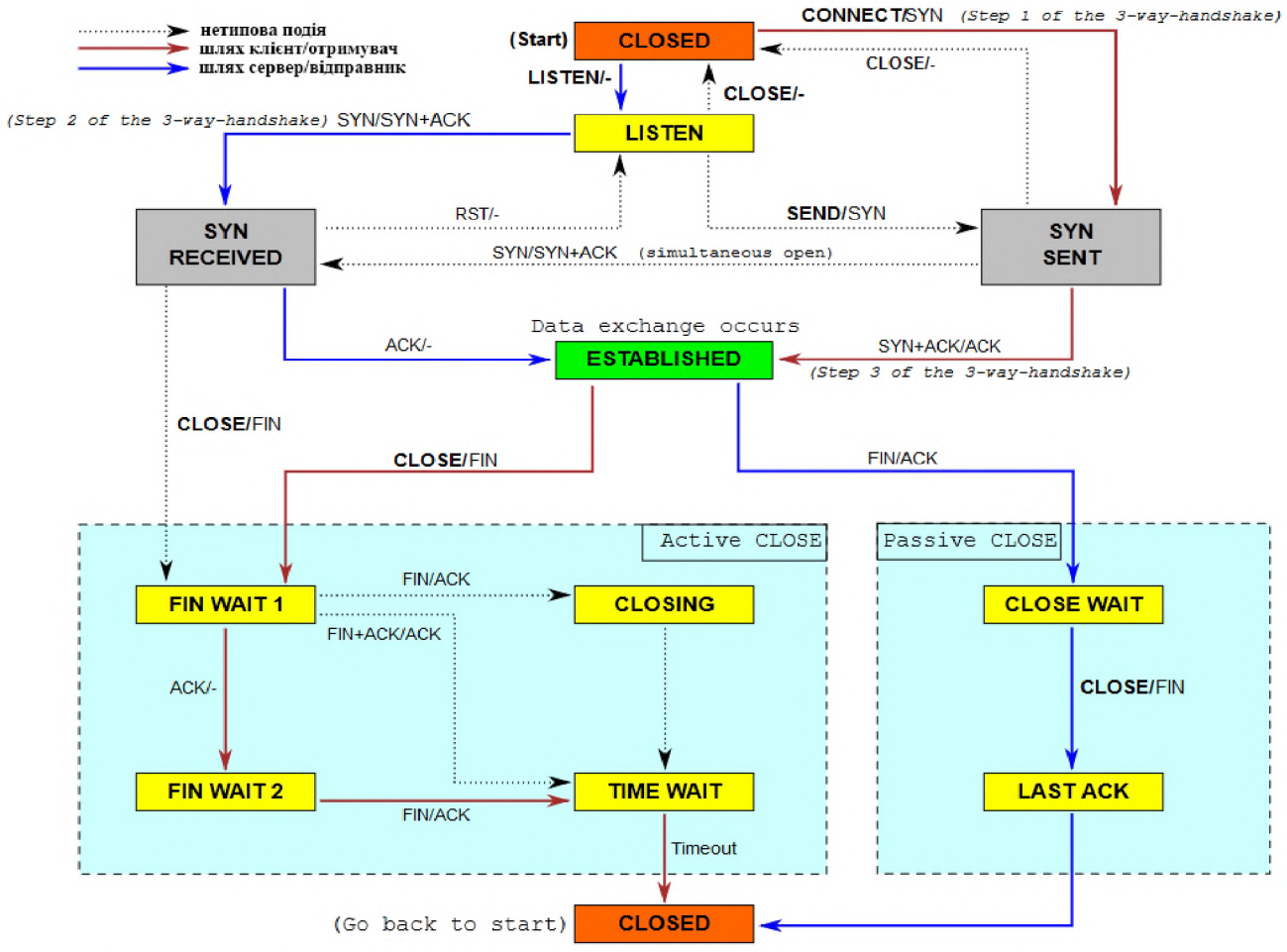


Рисунок 2.3 – Схема структури взаємодії між двома віддаленими вузлами за протоколом TCP

Важливо розуміти, що протягом TCP-сесії дані надсилаються в обох напрямках, як від сервера до клієнта так і від клієнта до сервера, тобто створюються два потоки даних. Причому не завжди більший потік даних прямує від сервера до клієнта.

Кожна окрема сесія роботи протоколу TCP може бути поділена на три фази:

1 Встановлення з'єднання;

2 Передача даних;

3 Закінчення з'єднання.

Необхідною умовою для встановлення TCP-сесії є відкритий доступ до програмного сокету процесу на сервері, що відповідає за роботу протоколу прикладного рівня, який на мові TCP зветься портом. За такої умови стан TCP-сесії на стороні сервера є LISTEN (слухати),[20-24]. Тобто сервер слухає, якийсь конкретний TCP-порт і очікує отримати запит від клієнта на надання послуг, що відповідають номеру цього порту. Початковий стан TCP-сесії на стороні клієнта є CLOSED.

Для встановлення з'єднання протокол TCP використовує триходове рукостискання (handshaking), назване так за кількістю повідомлень між хостами:

Клієнт формує TCP-заголовок: у поле порт джерела заносить свій номер TCP-порта, як правило динамічний, у поле порт призначення номер порту протоколу прикладного рівня, послуги якого хоче отримати, в поле номер послідовності сегменту довільне значення та встановлює та прапорець SYN. Сформований таким чином TCP-сегмент відправляється серверу. TCP-сесія на стороні клієнта переходить у стан SYN-SENT.

Сервер отримує TCP-сегмент від клієнта зі встановленим прапорцем SYN та у відповідь формує TCP-заголовок: у поле порт джерела заносить свій номер TCP-порта, у поле порт призначення номер порту клієнта. Додає до отриманого від клієнта номера послідовності сегменту 1 і поміщає отримане число до номеру підтвердження, вносить свій власний початковий номер послідовності

сегменту та відправляє сегмент до клієнта з прапорцями SYN та ACK. TCP-сесія на стороні сервера переходить у стан SYN-RECEIVED.

Після отримання TCP-сегмента зі встановленими прапорцями ACK та SYN клієнт переходить у стан ESTABLISHED та відповідає на запит сервера про синхронізацію шляхом додавання 1 до номера отриманої послідовності сегменту та поміщає це число до номера підтвердження. Далі клієнт надсилає таким чином сформований сегмент до сервера з прапорцем ACK

Після отримання сервером TCP-сегмента з прапорцем ACK стан TCP-сесії на його стороні стає також ESTABLISHED, разом з чим розпочинається передача даних.

Також на етапі встановлення з'єднання між хостами, як правило відбувається обмін опціями, тобто TCP-параметрами, які впливають на ефективність передачі даних.

Ініціатором закінчення з'єднання може бути, як клієнт так і сервер. Для закінчення TCP-сесії використовується так зване чотириходове рукостискання (four-way handshake).

Ініціатор розірвання з'єднання направляє своєму партнеру TCP-сегмент зі встановленим прапорцем FIN. TCP-сесія ініціатора переходить зі стану ESTABLISHED у стан FIN-WAIT-1.

Хост-отримувач приймає FIN від ініціатора та посилає у відповідь TCP-сегмент зі встановленим прапорцем ACK. TCP-сесія отримувача переходить зі стану ESTABLISHED у стан CLOSE-WAIT. З набуттям хостом цього стану TCP припиняє отримувати нові запити, на передачу даних, від відповідного протоколу верхнього рівня та встановлює таймер на завершення попередніх запитів. Ініціатор отримує ACK та переходить у стан FIN-WAIT-2.

Після закінчення оброблення всіх запитів протоколів верхнього рівня хост-отримувач переходить у стан LAST-ACK та відправляє ініціатору TCP-сегмент зі встановленим прапорцем FIN.

Ініціатора приймає FIN від отримувача та посилає у відповідь TCP-сегмент зі встановленим прапорцем ACK. Отримувач приймає ACK та переходить у стан CLOSED.

Ініціатор розірвання з'єднання чекає протягом подвійного часу від MSL (максимального життя сегмента, maximum segment lifetime), щоб переконатися, що посланий ACK був отриманий та також переходить у стан CLOSED.

Transmission Control Protocol, TCP (Протокол керування передачею) – протокол, призначений для управління передачею даних у комп'ютерних мережах, працює на транспортному рівні моделі OSI.

На відміну від іншого розповсюдженого протоколу транспортного рівня UDP, TCP забезпечує надійну доставку даних від хоста-відправника до хоста-отримувача, для цього встановлюється логічний зв'язок між хостами. Таким чином TCP належить до класу протоколів зі встановленим з'єднанням.

TCP отримує потоки даних від протоколів верхніх рівнів OSI-моделі, початковим джерелом яких є протоколи прикладного рівня, такі як HTTP, FTP та інші. Кожний протокол верхнього рівня має свій визначений TCP-порт.

TCP розбиває конкретний потік даних на порції, та додає до кожної з них заголовок з номером послідовності. Отримані таким чином порції даних традиційно називаються TCP-сегментами. Далі кожний сегмент інкапсулюється в IP-пакет і передається через IP-протокол до хоста-отримувача.

Після надходження IP-пакету до хоста-отримувача перевіряється коректність отриманих даних у TCP-сегменті, методом перерахування контрольної суми, та переконується, що попередні сегменти даних також були успішно отримані. Після чого хост-отримувач надсилає запит до хоста-відправника про нову, або повторну передачу порції даних, що одночасно є підтвердженням того, що всі сегменти з номерами послідовності, меншими ніж номер нового запиту, були успішно отримані.

У свою чергу TCP-сегменти деінкапсулюються з IP-пакетів, розміщуються в правильному порядку та з них вилучаються TCP-заголовки.

Отриманий таким чином потік даних передається до того протоколу верхнього рівня, з якого первісно надійшли дані на стороні хоста-відправника.

Блок даних (PDU, Protocol data unit) TCP називається сегментом (рисунок 2.3), хоча часто також використовують слово пакет, але таке вживання може вносити плутанину з IP-пакетом.

TCP-сегмент складається із TCP-заголовка і поля Дані (Data), яке називають сегментом даних або пейлодом (payload) або SDU (Service data unit).

Стандартний розмір TCP-заголовка – 20 байт, але з використанням опцій розмір може зростати до 60 байт. Як правило, опціями хости обмінюються на етапі встановлення з'єднання.

Октет		0								1								2								3							
	Біт	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Порт джерела (*Source port*)																Порт призначення (*Destination port*)															
4	32	Номер послідовності (*Sequence number*)																															
8	64	Номер підтвердження (*Acknowledgment number*)																															
12	96	Зміщення даних (*Data offset*)				Зарезервовано (*Reserved*) 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Розмір вікна (*Window Size*)														
16	128	Контрольна сума (*Checksum*)																Покажчик важливості (*Urgent pointer*)															
20 … 56	160 … 448	Опції (*Options*) *необов'язкове, розмір в залежності від значення поля «Зміщення даних»*																															
20+ …	160+ …	**Дані (*Data*)**																															

Рисунок 2.3 – Формат TCP сегменту

Розмір сегменту даних (поля даних) визначається опцією MSS (Максимальний розмір сегменту, Maximum segment size) на етапі встановлення з'єднання. Якщо обміну опціями не відбулося, то розмір сегменту даних встановлюється по-замовчуванню 536 байт. Розмір сегменту даних тісно пов'язаний з MTU (Максимальний блок передачі). Фактично MSS дорівнює MTU з відніманням розміру IP- і TCP-заголовків. Наприклад у сучасній мережі Ethernet MTU дорівнює 1500 байт; тоді оптимальний розмір MSS буде 1460 байтів (1500 мінус 20 байт заголовка IP і 20 байт заголовка TCP).

Поля заголовка:

1 Порт джерела -16 - 31 біти (Source port) - ідентифікує номер TCP-порту, з якого відправляється сегмент.

2 Порт призначення - 16 - 31 біти (Destination port) - ідентифікує номер TCP-порту, на який відправляється сегмент.

3 Номер послідовності – 32 - 63 біти (Sequence number) - число, що відображає номер першого байту в сегменті надісланих даних від хоста-відправника до хоста-отримувача. Це число є акумулювальним, тобто поточний номер послідовності є сумою номеру послідовності попереднього сегменту і кількості даних (в байтах) відправлених у ньому. Використовується для відстеження кількості та правильної послідовності отриманих сегментів даних.

4 Номер підтвердження - 64 - 95 біти (Acknowledgment number) фактично є запитом від хоста отримувача на надіслання нового сегменту даних починаючи зі вказаного номера. З іншого боку, коли хост відправник отримує це повідомлення, він переконується, що всі сегменти даних з номерами послідовності меншими за номер підтвердження були успішно прийняті отримувачем.

5 Зміщення даних - 96 - 99 біти (Data offset) - 4-бітний номер, який визначає розмір TCP-заголовка в 32-бітових словах. Мінімальний розмір становить 5 (0101) слів, а максимальний — 15 (1111), що є відповідно 20 і 60 байт. Фактично визначає розмір поля Опції (Options) від 0 до 40 байт.

6 Зарезервовано - 100 - 102 біти, зарезервовані для майбутнього використання і повинні містити нулі (000).

7 Прапорці (керуючі біти) - містить бітові прапорці. Прапорці вважаються встановленими, якщо їх бітове значення є 1.

- 103 NS — Одноразова сума (Nonce Sum), використовується з метою покращення роботи механізму явного повідомлення про перевантаження (Explicit Congestion Notification, ECN).

- 104 CWR — Вікно перевантаження зменшено (Congestion Window Reduced), прапорець встановлюється, щоб показати що TCP-сегмент був

отриманий зі встановленим полем ECE, іншими словами це є підтвердженням отримання сегменту даних з прапорцем ECE від хоста партнера.

- 105 ECE — ECN-Exo (ECN-Echo), поле показує, що відправник підтримує ECN.

- 106 URG — Важливість (Urgent), вказує, що TCP-сегмент містить важливі дані. Коли до хоста-отримувача надходить сегмент зі встановленим прапорцем URG, TCP відправляє важливі дані з цього сегменту, які знаходяться завдяки полю покажчик важливості до відповідного протоколу верхнього рівня минаючи чергу і без перевірки успішності надходження попередніх сегментів.

- 107 ACK — Підтвердження (Acknowledge) успішності отримання TCP-сегменту

- 108 PSH — Просування (Push), також як і прапорець URG, вказує, на пріоритетність TCP-сегменту. Хост-відрапнивник позачергово надсилає цей сегмент даних через IP-мережу. За аналогією з прапорцем URG, PSH інструктує хост-отримувач, що сегмент даних має бути негайно переданий до прикладного рівня (кінцевого споживача даних).

- 109 RST — Обривання (Reset) вказує, хосту-отримувачу негайно скинути з'єднання без подальшої взаємодії. Така ситуація наступає у разі, якщо сервер (хост-відправник) не надає послуги визначеного сервісу. Наприклад клієнт (хост-отримувач) запросив у веб-сервера послуги у форматі протоколу HTTPS (TCP-порт 443), але веб-сервер надає послуги лише у форматі HTTP (TCP-порт 80). Ця властивість TCP часто використовується хакерами для сканування портів мережі жертви.

- 110 SYN — Синхронізація (Synchronize) використовується для встановлення з'єднання між хостами при так званому триходовому рукостисканні (handshaking)

- 111 FIN — Фініш (Finish) вказує на завершення з'єднання.

8 Розмір вікна - 112—127 біти (Window Size) - визначає кількість байтів даних, які відправник може надіслати до того, як отримає підтвердження (запит на новий сегмент) від хоста-отримувача. Розмір вікна TCP вираховує на основі

пропускної здатності (bandwidth) лінії зв'язку між хостами (фактично це є пропускна здатність відрізка шляху з її найгіршим значенням) та загальній затримці (latency) (часу потрібному на доставку сегмента) на всьому шляху.

9 Контрольна сума – 128 - 143 біти (Checksum) - розраховується на основі усього TCP-сегменту включно із заголовком та важливих полів IP-пакету: IP-адрес хостів відправника та отримувача, номеру протоколу (TCP має номер 6) та загального розміру IP-пакету. Контрольна сума забезпечує можливість перевірки цілісності надісланих даних.

10 Покажчик важливості – 144-159 біти (Urgent pointer) - поле береться до уваги тільки в разі встановленого прапорця URG, та містить значення зміщення відносно номеру послідовності сегменту. Фактично це число вказує на позицію в TCP-сегменті де закінчуються важливі дані. Тобто важливі дані знаходяться зразу після TCP-заголовка і закінчуються перед місцем на яке вказує покажчик важливості.

11 Опції – 160-479 біти (Options) - необов'язкове поле, розмір якого визначається в залежності від значення поля зміщення даних та є кратним 8 (одному байту). Кожна опція в свою чергу складається з 3-х полів: Номер (kind) — 1 байт, Довжина (length, вказує на загальний розмір опції в байтах) — 1 байт, Дані (data) в залежності від поля довжина. Опції використовується для обміну додаткових параметрів між хостами з метою покращення функціонування протоколу TCP. Частіше за все це поле включає наступні опції:

- MSS (Максимальний розмір сегменту, Maximum segment size), RFC 793, номер — 2, довжина — 4. Опція максимальний розмір сегменту визначає максимальний розмір поля Дані в TCP-сегменті тобто кількість даних які можуть бути поміщені в один сегмент при їх передачі між хостами.
- Масштабування вікна (Window scale) - номер — 3, довжина — 3, слугує для збільшення значення TCP-вікна, максимальне значення цієї опції є 14. Новий розмір TCP-вікна вираховується по формулі: розмір вікна * 2n, де n є значення опції масштабування вікна. Стандартний максимальний розмір вікна відображається 16-ти бітовим числом, тобто може мати максимальне значення

— 65535 (64 Кб), використовуючи опцію масштабування вікна з максимально допустимим значенням 14, отримуємо 65535 * 214 = 65535 * 16384 = 1073725440 (1 Гб). Великі значення TCP-вікна використовуються коли на шляху пакетів із TCP-сегментами зустрічаються WAN-лінки зі значними пропускними здатностями (bandwidth) та великими затримками (latency).

- Вибіркові підтвердження (Selective Acknowledgments, SACK), RFC 2018, номер — 2, довжина — від 4 байт — верхня межа варіюється, як правило містить у собі два 2-х байтних поля даних. Мета її введення є покращення ефективності роботи TCP, як відомо TCP для передачі сегментів даних використовує протокол IP, який є протоколом без встановлення з'єднання, тобто доправлення пакетів з TCP-сегментами не є гарантованим, допускається, що частина IP-пакетів може бути втрачена. В свою чергу TCP забезпечує надійне доправляння даних, що базується на механізмі надсилання номерів підтвердження (acknowledgment number). Якщо якийсь сегмент від відправника до отримувача не надійшов у встановлений час то ініціюється повторна передача починаючи зі втраченого сегменту, навіть якщо TCP-сегменти з номерами послідовності більшими за номер втраченого сегменту були успішно отримані. Механізм вибіркового підтвердження дозволяє ретранслювати лише втрачені сегменти даних, чим суттєво покращує ефективність роботи TCP.

- Мітки часу (Timestamps), RFC 7323, номер — 8, довжина — 10, містить у собі два 4-х байтних поля Значення мітки часу (Timestamp Value) та Ехо-відповідь мітки часу (Timestamp Echo Reply). Як правило хости обмінюються значеннями міток часу на етапі встановлення з'єднання. За допомогою міток часу TCP визначає скільки потрібно часу на доправлення сегментів між хостами. На основі цих значень встановлюються TCP-таймери відповідальні на стороні хоста-відправника за повторну передачу даних, якщо підтвердження отримання не надійшло у встановлений час, а у разі використання опції вибіркового підтвердження хост-отримувач самостійно ініціює запит на повторну передачу конкретного сегменту даних.

Якщо деякий простір поля Опції лишається незаповненим то він заповнюється спеціальною опцією NOP (No-Operation, нічого не робити), RFC 793, номер – 1, довжина – відсутня.

2.1.3 Види DoS атак та особливості їх здійснення

Дослідження виявило, що найбільш повна класифікація атак представлена Національним інститутом стандартів і технології США, тому інформація з неї і використовується у роботі.

Згідно з нею, атака типу «Відмова в обслуговуванні» (DoS, Denial of Service) - це спроба уповільнити або вимкнути мережеві системи та служби жертви. Є два основних типи атак DOS: експлуатація вразливостей та flood-атаки, схематично класифікація наведена на рисунку 2.5.

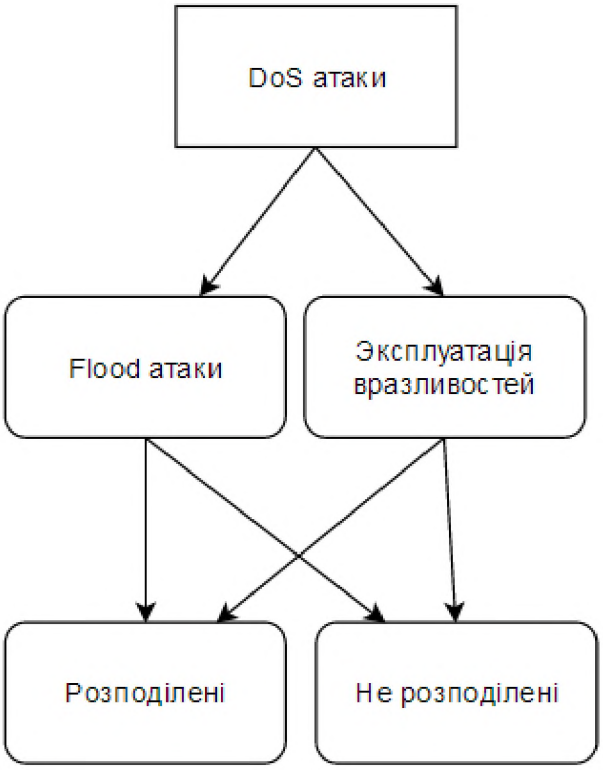


Рисунок 2.5 – Класифікація DoS атак

Атаки типу «експлуатація вразливостей» використовують вразливості в програмному забезпеченні цільової системи для того, щоб викликати збій обробки або привести до виснаження ресурсів системи. Прикладом такого збою

обробки є атака "ping смерті". Ця атака представляє з себе відправку несподівано великого ping-пакету деяким версіям операційної системи Windows - система не знала, що робити з цим нестандартним пакетом, і це приводило до збою (іноді навіть припинення роботи). Щодо виснаження ресурсів цілі порушника, ресурси включають в себе процесорний час, пам'ять, дисковий простір, простір в спеціальних буферах, та пропускну здатність мережі. У багатьох випадках, просто оновлення програмне забезпечення може уникнути таких DoS атак.

DOS-атаки типу flood полягають у тому, щоб просто відправляти більше інформації, ніж система-жертва може обробити. У тих випадках, коли порушник не може відправити системі досить інформації, щоб придушити ресурсний потенціал системи, порушник, тим не менш, може бути в змозі монополізувати підключення цілі до мережі, тим самим блокуючи використання ресурсу іншим. З такою атакою, не існує недоліків які можуть бути виправлений в системі. Хоча існує кілька загальних рішень, щоб зовсім зупинити flood атаки, є також низка технічних заходів, які можна вжити з метою пом'якшити атаку.

Термін "розподілена DOS" (DDOS) є підмножиною атак DOS. DDOS атаки просто використовують DOS-атаки, порушник використовує кілька комп'ютерів щоб розпочати атаку. Ці атакуючі комп'ютери централізовано контролюються комп'ютером порушник і, таким чином, діють як одна система. Зазвичай, поодинокий порушник не може «забити» головну мережу сайту електронної комерції, затоплюючи його мережевими пакетами з одного хоста. Проте, якщо порушник отримує контроль над 20,000 комп’ютерів і може запустити організовану атаку під його керівництвом, то він отримує засіб для успішних атак навіть на найшвидші системи, в результаті чого викликає їх зупинку або блокує їх для користувачів.

Однією з найпопулярніших DoS-атак є так-званий SYN-flood (також відома як Neptune), реалізація якої зводиться до простої відправки на відкритий порт сервера множини SYN-пакетів, що не приводять до встановлення

реального з'єднання по тим чи іншим причинам, що, в свою чергу, спричиняє за собою створення «напіввідкритих з'єднань», які переповнюють чергу підключень, змушуючи сервер відмовляти у обслуговуванні чергових клієнтів.

У контексті цієї атаки слід розглянути механізм встановлення TCP-з'єднання – триходове рукостискання. На рівні «клієнт-сервер» це виглядає так: клієнт відправляє серверу SYN-пакет, на який отримує відповідь SYN-ACK. Клієнт відправляє у якості відповіді ACK на SYN сервера і з'єднання переходить у стан встановленого.

Справа у тому, що TCP RFC зобов'язує сервер відповідати на кожен отримуваний SYN, що додатково б'є по ресурсам сервера та каналу передачі даних.

Заради підвищення ефективності SYN атаки, зловмисник може використовувати фіктивні IP-адреси в SYN-пактах. У цьому разі хост жертви не зможе швидко закінчити процес ініціалізації, так як початковий IP може бути недосяжен. Ця модифікація атаки називається SYN-спуфінгом.
Короткий список найбільш популярних TCP портів: (Secure Shell), 23 (Telnet), 53 (DNS) і 80 (HTTP/web). Також, фактично роутери всього Інтернету підтвердять TCP зв'язок на 179 порті.

Не менш поширеною є атака типу Smurf, з ефектом підсилення, який є результатом відправки прямих широкомовних запитів PING на системи, які забов'язані відправити відповідь. Запит направляють або на мережеву адресу (*.*.*.0 у стандартній мережі класу C), або на адресу широкомовної розсилки (*.*.*.255 у стандартній мережі класу C), однак у обох випадках прилад має виконати перетвореня з рівня IP до мережевого рівня, як цього потребує RFC 1812 "Requirements for IP Version 4 Routers" (Вимоги до маршрутизаторів протоколу IP версії 4).

Для реалізації атаки зловмисник відправляє пакет ICMP ECHO на адресу широкомовної розсилки підсилюваючої мережі. Адреса джерела цього пакету замінюється адресою жертви, щоб представити ситуацію так, ніби саме система жертви ініціювала запрос. Після цього відбувається наступне: так як пакет

ECHO відправлено на широкомовний адрес, всі системи підсилюючої мережі повертають жертві свої відповіді. Таким чином зловмисник, відправляючи лише один пакет у мережу з 100 систем, ініціює підсилення атаки у сто разів. Також актуальними є атаки типів back, PoD та Teardrop.

Атака типу Back здійснюється проти apache Web-сервера, який блокується великим потоком запитів, які містять велику кількість символів «/» в полі URL. Намагаючись обробити ці запити сервер перестає мати можливість обслуговувати інші запити.

При атаках Land, зловмисник посилає жертві пакет, що включає TCP SYN, де IP-адреса відправника та отримувача однакові. Такий пакет цілком блокує роботу системи жертви.

Під час пересилки до системи отримувача пакет може бути розділений на невеликі фрагменти. Атака TearDrop створює потік IP-фрагментів з надзвичайно великим значенням поля зсуву (offset). Отримувач, намагаючись відновити ці фальсифіковані фрагменти може блокуватися або навіть виконати операцію перезавантаження.

2.1.4 Визначення параметрів мережевого трафіка, доступних у базі KDD

У даній роботі в якості параметрів для аналізу будуть використовуватися параметри у базі KDD. База KDD була обрана через її зручність у використанні для вирішення задач даної роботи та відсутність можливості створити подібну базу власноруч.

База даних KDD містить близько 5 000 000 записів – образів мережевих з'єднань, зареєстрованих через певні проміжки часу. Кожна строка складається з 42 параметрів. У полях від 1 до 41 записані такі параметри мережевого з'єднання, у 42 полі записана інформація, що характеризує стан - відсутність атаки , або її тип (наприклад «Back»).

Необроблена база має приблизно такий вигляд:

	Имя	Тип	Ширина	Знаков ...	Метка	Значения	Пропущенн...	Ширина ...	Выравнивание	Мера	Роль
1	duration	Числовой	1	0		Нет	Нет	8	По право...	Шкалы	Входная
2	protocol_type	Текстовая	4	0		{icmp, icmp...	Нет	5	По левом...	Номинальная	Входная
3	service	Текстовая	10	0		{IRC, IRC}...	Нет	10	По левом...	Номинальная	Входная
4	flag	Текстовая	6	0		{OTH, OTH}...	Нет	7	По левом...	Номинальная	Входная
5	src_bytes	Числовой	3	0		Нет	Нет	8	По право...	Шкалы	Входная
6	dst_bytes	Числовой	5	0		Нет	Нет	8	По право...	Шкалы	Входная
7	land	Числовой	1	0		{0, connecti...	Нет	8	По право...	Номинальная	Входная
8	wrong_frag...	Числовой	1	0		Нет	Нет	8	По право...	Шкалы	Входная
9	urgent	Числовой	1	0		Нет	Нет	8	По право...	Шкалы	Входная
10	hot	Числовой	1	0		Нет	Нет	8	По право...	Шкалы	Входная
11	num_failed_...	Числовой	1	0		Нет	Нет	8	По право...	Шкалы	Входная
12	logged_in	Числовой	1	0		{0, not succ...	Нет	8	По право...	Номинальная	Входная
13	num_compr...	Числовой	1	0		Нет	Нет	8	По право...	Шкалы	Входная
14	root_shell	Числовой	1	0		{0, root shel...	Нет	8	По право...	Номинальная	Входная
15	su_attempted	Числовой	1	0		{0, "su root" ...	Нет	8	По право...	Номинальная	Входная
16	num_root	Числовой	1	0		Нет	Нет	8	По право...	Шкалы	Входная
17	num_file_cr...	Числовой	1	0		Нет	Нет	8	По право...	Шкалы	Входная
18	num_shells	Числовой	1	0		Нет	Нет	8	По право...	Шкалы	Входная
19	num_acces...	Числовой	1	0		Нет	Нет	8	По право...	Шкалы	Входная
20	num_outbou...	Числовой	1	0		Нет	Нет	8	По право...	Шкалы	Входная
21	is_hot_login	Числовой	1	0		{0, 1 if the l...	Нет	8	По право...	Номинальная	Входная
22	is_guest_login	Числовой	1	0		{0, the login...	Нет	8	По право...	Номинальная	Входная
23	count	Числовой	2	0		Нет	Нет	8	По право...	Шкалы	Входная
24	srv_count	Числовой	2	0		Нет	Нет	8	По право...	Шкалы	Входная

Рисунок 2.5 – Список всіх параметрів бази

Дані, у свою чергу, мають такий вигляд:

	durati on	protocol_ type	service	flag	src_b ytes	dst_byte s	land	wrong_ fragmen t	urg...	hot	num_fa iled_log ins	logged _in	num_c ompro mised	root_ shell	su_atte mpted	num_ro ot	num_file _creation s	num_s hells	num_ acces s_f...	num_ outbo un...	is_hot _login	is_gue st_logi n	count	srv_cou nt	serror_ ate	srv_serro r_rate	rerror_r ate	srv_rerro _rate
1	0	tcp	http	SF	181	5450	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	8	8	0%	0%	0%	0%
2	0	tcp	http	SF	239	486	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	8	8	0%	0%	0%	0%
3	0	tcp	http	SF	235	1337	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	8	8	0%	0%	0%	0%
4	0	tcp	http	SF	219	1337	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	6	6	0%	0%	0%	0%
5	0	tcp	http	SF	217	2032	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	6	6	0%	0%	0%	0%
6	0	tcp	http	SF	217	2032	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	6	6	0%	0%	0%	0%
7	0	tcp	http	SF	212	1940	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	2	0%	0%	0%	0%
8	0	tcp	http	SF	159	4087	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	5	5	0%	0%	0%	0%
9	0	tcp	http	SF	210	151	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	8	8	0%	0%	0%	0%
10	0	tcp	http	SF	212	786	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	8	8	0%	0%	0%	0%
11	0	tcp	http	SF	210	624	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	18	18	0%	0%	0%	0%
12	0	tcp	http	SF	177	1985	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0%	0%	0%	0%
13	0	tcp	http	SF	222	773	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	11	11	0%	0%	0%	0%
14	0	tcp	http	SF	256	1169	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	4	4	0%	0%	0%	0%
15	0	tcp	http	SF	241	259	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0%	0%	0%	0%
16	0	tcp	http	SF	260	1837	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	11	11	0%	0%	0%	0%
17	0	tcp	http	SF	241	261	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	2	2	0%	0%	0%	0%
18	0	tcp	http	SF	257	818	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	12	12	0%	0%	0%	0%
19	0	tcp	http	SF	233	255	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	2	8	0%	0%	0%	0%
20	0	tcp	http	SF	233	504	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	7	7	0%	0%	0%	0%
21	0	tcp	http	SF	256	1273	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	17	17	0%	0%	0%	0%

Рисунок 2.6 – Частина таблиці даних бази

Обрані для аналізу, серед доступних у базі KDD сервіси та види мережевих атак, прикладів реалізації яких достатньо для аналізу приведені у таблиці 2.1.

Таблиця 2.1 – Співвідношення мережевих сервісів та мережевих атак

	Типи атак	
Мережевий сервіс	Backscatter	SYN flood
HTTP	+	+

2.1.4.1 Визначення мережевого сервісу

Із бази KDD для аналізу у цій роботі були обрані розповсюджені мережеві сервіси (таблиця 2.1), на які у базі приведена достатня кількість записів атак та нормального стану.

HTTP (Hyper Text Transfer Protocol) - протокол передачі даних, що використовується в комп'ютерних мережах. Основним призначенням протоколу HTTP є передача об’єктів (веб-сторінок та будь-яких файлів).

HTTP - протокол прикладного рівня стеку TCP/IP, схожими на нього є FTP і SMTP. Обмін повідомленнями йде за звичайною схемою «запит-відповідь». Для ідентифікації ресурсів HTTP використовує глобальні URI. На відміну від багатьох інших протоколів, HTTP не зберігає свого стану. Це означає відсутність збереження проміжного стану між парами «запит-відповідь». Компоненти, що використовують HTTP, можуть самостійно здійснювати збереження інформації про стан, пов'язаний з останніми запитами та відповідями. Браузер, котрий посилає запити, може відстежувати затримки відповідей. Сервер може зберігати IP-адреси та заголовки запитів останніх клієнтів. Проте, згідно з протоколом, клієнт та сервер не мають бути обізнаними з попередніми запитами та відповідями, у протоколі не передбачена внутрішня підтримка стану й він не ставить таких вимог до клієнта та сервера.

HTTP встановлює окрему TCP-сесію на кожен запит; в більш пізніх версіях HTTP було дозволено робити кілька запитів в ході однієї TCP-сесії, але браузери зазвичай запитують тільки сторінку і включені в неї об'єкти, а потім відразу розривають TCP-сесію.

2.1.4.2 Визначення вагомих параметрів бази KDD

Поля у базі KDD умовно розділяються на категорії:

- базова інформація TCP з’єднань;
- інформація про з’єднання зі сторони домену.

Інформація про мережевий трафік у базі KDD розраховується з використанням часового вікна 2 секунди.

Серед усіх полів бази теоретично інформативними для виявлення атак є такі параметри із заголовків протоколів IP та TCP:

- service – сервіс призначення (http, FTP і тд);
- src_bytes – кількість байт із джерела до приймача;
- dst_bytes - кількість байт із приймача до джерела;
- flag – нормальний, або статус помилки з'єднання;
- count - кількість з'єднань до поточного хоста за останні 2 сек. Кількість з'єднань, що було встановлено хоста (ініціатором з'єднання являється віддалена сторона);
- srv_count - кількість з'єднань до поточної службі за останні 2 секунди. Скільки нових з'єднань встановилося на кожен конкретний порт протягом 2 останніх секунд;
- serror_rate - відсоток з'єднань з помилкою типу SYN для даного хоста джерела. Серед активних з'єднань число тих з'єднань, серед яких з'являлися спонтанні пакети з SYN - прапорами (тобто SYN -прапор з'являвся вже після встановлення з'єднання) для конкретного віддаленого хоста і потім підраховується їх відносна кількість;
- srv_serror_rate - відсоток з'єднань з помилкою типу SYN для даної служби. Те ж саме що serror_rate, але для порту;
- same_srv_rate - відсоток з'єднань до служби. Відносна кількість з'єднань до однієї служби (порту);
- diff_srv_rate - відсоток з'єднань до різних служб. Обчислюється як 1-same_srv_rate;
- srv_diff_host_rate - відсоток з'єднань до різних хостів. Обчислюється як 1-srv_same_host_rate;
- dst_host_count - кількість з'єднань до хоста;
- dst_host_srv_count - кількість з'єднань до служби;

- dst_host_same_srv_rate - відсоток з'єднань до даної службі (відсоток з'єднань до одного і того ж порту призначення одного й того ж хоста призначення;

- dst_host_diff_srv_rate - відсоток з'єднань до інших служб (відсоток різних служб на поточному хості)). Обчислюється як 1 - dst_host_same_srv_rate;

- dst_host_same_src_port_rate - відсоток з'єднань до даного хоста при поточному номеру порту джерела. Відносне число з'єднань від поточного віддаленого порту до мого хоста;

- dst_host_srv_diff_host_rate - відсоток з'єднань до служби різних хостів. Відсоток числа з'єднань на конкретному порту незалежно від ip-адреси віддаленої сторони;

- dst_host_serror_rate (S0 error) - відсоток з'єднань з помилкою типу SYN для даного хоста приймача;

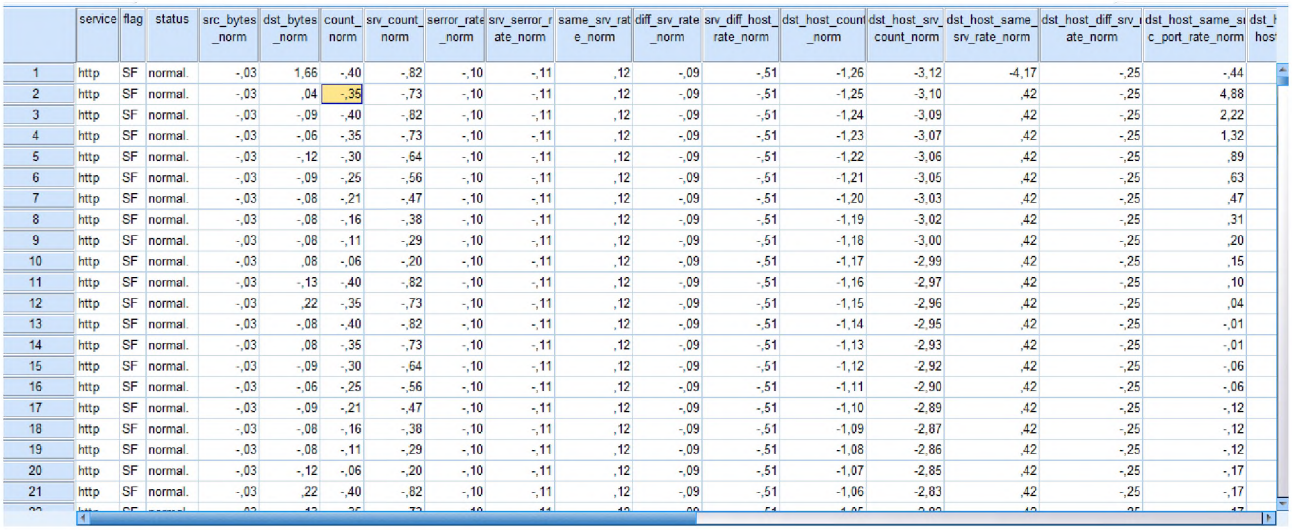
- dst_host_srv_ serror_rate (S0 error) - відсоток з'єднань з помилкою типу SYN для даної служби.

Данні, які не стосуються протоколу і видів атак обраних у таблиці 2.1 можна виділити, після чого параметри бази будуть мати наступний вигляд:

	Имя	Тип	Ширина	Знаков ...	Метка	Значения	Пропущенн...	Ширина ...	Выравнивание	Мера	Роль
1	service	Текстовая	8	0		Нет	Нет	9	По левом...	Номинальная	Нет
2	flag	Текстовая	4	0		Нет	Нет	7	По левом...	Номинальная	Нет
3	status	Текстовая	12	0		Нет	Нет	16	По левом...	Номинальная	Нет
4	src_bytes_n...	Числовой	8	2		Нет	Нет	16	По право...	Шкалы	Входная
5	dst_bytes_n...	Числовой	8	2		Нет	Нет	16	По право...	Шкалы	Входная
6	count_norm	Числовой	8	2		Нет	Нет	12	По право...	Шкалы	Входная
7	srv_count_n...	Числовой	8	2		Нет	Нет	16	По право...	Шкалы	Входная
8	serror_rate_...	Числовой	8	2		Нет	Нет	18	По право...	Шкалы	Входная
9	srv_serror_r...	Числовой	8	2		Нет	Нет	22	По право...	Шкалы	Входная
10	same_srv_r...	Числовой	8	2		Нет	Нет	20	По право...	Шкалы	Входная
11	diff_srv_rate...	Числовой	8	2		Нет	Нет	20	По право...	Шкалы	Входная
12	srv_diff_host...	Числовой	8	2		Нет	Нет	25	По право...	Шкалы	Входная
13	dst_host_co...	Числовой	8	2		Нет	Нет	21	По право...	Шкалы	Входная
14	dst_host_sr...	Числовой	8	2		Нет	Нет	25	По право...	Шкалы	Входная
15	dst_host_sa...	Числовой	8	2		Нет	Нет	29	По право...	Шкалы	Входная
16	dst_host_dif...	Числовой	8	2		Нет	Нет	29	По право...	Шкалы	Входная
17	dst_host_sa...	Числовой	8	2		Нет	Нет	34	По право...	Шкалы	Входная
18	dst_host_sr...	Числовой	8	2		Нет	Нет	34	По право...	Шкалы	Входная
19	dst_host_se...	Числовой	8	2		Нет	Нет	27	По право...	Шкалы	Входная
20	dst_host_sr...	Числовой	8	2		Нет	Нет	31	По право...	Шкалы	Входная
21	service_norm	Числовой	2	0		Нет	Нет	14	По право...	Номинальная	Входная
22	flag_norm	Числовой	2	0		Нет	Нет	11	По право...	Номинальная	Входная
23	status_norm	Числовой	2	0		Нет	Нет	13	По право...	Номинальная	Входная
24	status_num	Числовой	8	2		Нет	Нет	12	По право...	Номинальная	Входная

Рисунок 2.6 – Список всіх теоретично інформативних параметрів бази

А дані, в свою чергу, наступний:



	service	flag	status	src_bytes_norm	dst_bytes_norm	count_norm	srv_count_norm	serror_rate_norm	srv_serror_rate_norm	same_srv_rate_norm	diff_srv_rate_norm	srv_diff_host_rate_norm	dst_host_count_norm	dst_host_srv_count_norm	dst_host_same_srv_rate_norm	dst_host_diff_srv_rate_norm	dst_host_same_src_port_rate_norm	dst_h host
1	http	SF	normal.	-,03	1,66	-,40	-,82	-,10	-,11	,12	-,09	-,51	-1,26	-3,12	-4,17	-,25	-,44	
2	http	SF	normal.	-,03	,04	-,35	-,73	-,10	-,11	,12	-,09	-,51	-1,25	-3,10	,42	-,25	4,88	
3	http	SF	normal.	-,03	-,09	-,40	-,82	-,10	-,11	,12	-,09	-,51	-1,24	-3,09	,42	-,25	2,22	
4	http	SF	normal.	-,03	-,06	-,35	-,73	-,10	-,11	,12	-,09	-,51	-1,23	-3,07	,42	-,25	1,32	
5	http	SF	normal.	-,03	-,12	-,30	-,64	-,10	-,11	,12	-,09	-,51	-1,22	-3,06	,42	-,25	,89	
6	http	SF	normal.	-,03	-,09	-,25	-,56	-,10	-,11	,12	-,09	-,51	-1,21	-3,05	,42	-,25	,63	
7	http	SF	normal.	-,03	-,08	-,21	-,47	-,10	-,11	,12	-,09	-,51	-1,20	-3,03	,42	-,25	,47	
8	http	SF	normal.	-,03	-,08	-,16	-,38	-,10	-,11	,12	-,09	-,51	-1,19	-3,02	,42	-,25	,31	
9	http	SF	normal.	-,03	-,08	-,11	-,29	-,10	-,11	,12	-,09	-,51	-1,18	-3,00	,42	-,25	,20	
10	http	SF	normal.	-,03	,08	-,06	-,20	-,10	-,11	,12	-,09	-,51	-1,17	-2,99	,42	-,25	,15	
11	http	SF	normal.	-,03	-,13	-,40	-,82	-,10	-,11	,12	-,09	-,51	-1,16	-2,97	,42	-,25	,10	
12	http	SF	normal.	-,03	,22	-,35	-,73	-,10	-,11	,12	-,09	-,51	-1,15	-2,96	,42	-,25	,04	
13	http	SF	normal.	-,03	-,08	-,40	-,82	-,10	-,11	,12	-,09	-,51	-1,14	-2,95	,42	-,25	-,01	
14	http	SF	normal.	-,03	,08	-,35	-,73	-,10	-,11	,12	-,09	-,51	-1,13	-2,93	,42	-,25	-,01	
15	http	SF	normal.	-,03	-,09	-,30	-,64	-,10	-,11	,12	-,09	-,51	-1,12	-2,92	,42	-,25	-,06	
16	http	SF	normal.	-,03	-,06	-,25	-,56	-,10	-,11	,12	-,09	-,51	-1,11	-2,90	,42	-,25	-,06	
17	http	SF	normal.	-,03	-,09	-,21	-,47	-,10	-,11	,12	-,09	-,51	-1,10	-2,89	,42	-,25	-,12	
18	http	SF	normal.	-,03	-,08	-,16	-,38	-,10	-,11	,12	-,09	-,51	-1,09	-2,87	,42	-,25	-,12	
19	http	SF	normal.	-,03	-,08	-,11	-,29	-,10	-,11	,12	-,09	-,51	-1,08	-2,86	,42	-,25	-,12	
20	http	SF	normal.	-,03	-,12	-,06	-,20	-,10	-,11	,12	-,09	-,51	-1,07	-2,85	,42	-,25	-,17	
21	http	SF	normal.	-,03	,22	-,40	-,82	-,10	-,11	,12	-,09	-,51	-1,06	-2,83	,42	-,25	-,17	

Рисунок 2.7 – Дані бази по теоретично інформативним параметрам

Далі необхідно провести статистичний аналіз, та визначити найбільш інформативні з цих даних.

2.1.5 Статистичний аналіз інформативних параметрів мережевого трафіку бази KDD

Для проведення редукції множини інформативних параметрів доцільно провести статистичний аналіз, використовуючи методи, які дозволяють скоротити надлишковість та визначити ступінь інформативності параметрів. Вибір таких статистичних методів також є частиною задачі проведення редукції.

Для проведення аналізу даних бази KDD у даній роботі буде використана SPSS Statistics (Statistical Package for the Social Sciences) –програма для статистичної обробки даних.

2.1.5.1 Підготовка даних бази KDD для проведення статистичного аналізу

Дані база KDD преставляє у вигляді текстового файлу, в якому кожен рядок є одним спостереженням, зафіксованим через 2 секунді, після попереднього. Поля бази – параметри мережевого трафіку, розташовані у визначеному порядку з розділяючим знаком «,» (кома). Дані були імпортовані у

SPSS Statistics із врахуванням цих особливостей, поля названі відповідно до приведеної у базі інформації.

Беручи до уваги виділені у підрозділі (2.1.5.2) теоретично інформативні параметри, доцільно використовувати для аналізу тільки їх: із всіх параметрів у базі KDD сформована вибірка, що містить сервіси та атаки на них (таблиця 2.1), 23 обрані параметри та додатково останнє поле бази – стан (відсутність атаки, або її тип), назване у даній роботі «status».

Через те, що обрані параметри мають різні розмірності (наприклад відсоток з'єднань до конкретного сервісу та кількість з'єднань, бінарний стан «1» або «0»,), для проведення статистичного аналізу необхідно провести їх нормалізацію. Функціонал SPSS Statistics дозволяє нормалізувати дані швидко у автоматичному режимі. Це включає у себе покращення якості даних (заміна пропусків середніми значеннями, заміна викидів (результатів вимірювання, що виділяються із загальної вибірки) значеннями відсікання) та приведення до однієї розмірності перетворенням у z–значення. Після нормалізації на виході отримано всі параметрі в одній розмірності у числовому форматі.

2.1.5.2 Визначення методу статистичного аналізу даних

Для проведення статистичного аналізу даних обрано дискримінантний аналіз, який є розділом багатовимірного статистичного аналізу, який дозволяє вивчати відмінності між двома і більше групами об'єктів по декількох змінним одночасно.

Дискримінантний аналіз - це загальний термін, що стосується кількох тісно пов'язаних зі статистичними процедурами. Ці процедури можна розділити на методи інтерпретації міжгрупових відмінностей - дискримінації і методи класифікації спостережень за групами.

При інтерпретації метою є отримати відповіді на питання:

- чи можливо, використовуючи даний набір змінних, відрізнити одну групу від іншої;

- наскільки добре ці змінні допомагають провести дискримінацію і які з них найбільш інформативні.

Методи класифікації пов'язані з отриманням однієї або декількох функцій, що забезпечують можливість віднесення даного об'єкта до однієї з груп. Ці функції називаються класифікуючими і їх значення залежить від значень змінних таким чином, що з'являється можливість віднесення кожного з об'єктів до певної групи.

Завдання дискримінантного аналізу можна розділити на три типи. Завдання першого типу часто зустрічаються в медичній практиці. Припустимо, що ми маємо інформацію про деяке число індивідуумів, хвороба кожного з яких відноситься до одного з двох або більше діагнозів. На основі цієї інформації потрібно знайти функцію, що дозволяє поставити у відповідність новим індивідуумам характерні для них діагнози. Побудова такої функції і становить завдання дискримінації. Другий тип завдання відноситься до ситуації, коли ознаки приналежності об'єкта до тієї чи іншої групи втрачені, і їх потрібно відновити. Прикладом може служити визначення статі давно померлої людини по його останках, знайдених під час археологічних розкопок. Завдання третього типу пов'язані з передбаченням майбутніх подій на підставі наявних даних. Такі завдання виникають при прогнозі віддалених результатів лікування, наприклад, прогноз виживання оперованих хворих.

Основною метою дискримінації є знаходження такої лінійної комбінації даних (далі дискримінантні змінні), яка б оптимально розділила розглянуті групи.

Лінійна функція (2.1) називається канонічною дискримінантною функцією:

$$d_{km} = \beta_0 + \beta_1 x_{1km} + \cdots + \beta_p x_{pkm},\ m = 1, \dots, n,\ k = 1, \dots, g, \qquad (2.1)$$

де β_i – невідомі коефіцієнти;

d_{km} – значення дискримінантної функції для m-го об’єкту в групі k;

x_{ikm} – значення дискримінантної змінної X_i для m-го об’єкту в групі k.

Стосовно вибірки даних, що аналізуються у цій роботі, під об'єктом розуміється рядок бази KDD (одне спостереження), n – кількість спостережень, g – кількість груп. Для вирішення поставленої задачі визначена кількість груп – 2:

- нормальний стан обчислювальної системи;
- стан, коли на обчислювальну систему здійснюється мережева атака.

З геометричної точки зору дискримінантні функції визначають гіперповерхню у p-мірному просторі. Зокрема при $p = 2$ вона є прямою, а при $p = 3$ – поверхнею.

Коефіцієнти β_i першої канонічної дискримінантної функції обираються таким чином, щоб центроїди різних груп якомога більше відрізнялися один від одного. Коефіцієнти другої групи вибираються також, але при цьому накладається додаткова умова, щоб значення другої функції були некорельованими зі значеннями першої. Це правило єдине для коефіцієнтів всіх груп – коефіцієнти кожної функції не корельовані з коефіцієнтами інших функцій. Звідси випливає, що будь-яка канонічна дискримінантна функція має нульову внутрішньогрупову кореляцію з $d_1, \dots, d_{g-1}$. Якщо число груп дорівнює g, то число канонічних дискримінантних функцій буде $g - 1$.

Для вирішення задачі редукції простору інформативних параметрів був обраний саме дискримінантний аналіз тому, що у результаті його проведення представляє вагу кожного вхідного параметру (коефіцієнт лінійної комбінації всіх параметрів - дискримінантної функції). Через це результат цього виду аналізу легко інтерпретується. У SPSS Statistics реалізовано цей вид аналізу та його функціонал дозволяє вирішити задачу цієї роботи.

2.1.5.3 Проведення статистичного аналізу вибірки даних із бази KDD

Дискримінантний аналіз виконувався відносно вихідної числової змінної «target», що була визначена на основі змінної «status» як:

- «1» - якщо даний запис бази KDD здійснювався під час проведення мережевої атаки типу “Neptune”;

- «0» - якщо даний запис бази KDD здійснювався під час проведення мережевої атаки типу “Back”;
- «-1» - якщо даний запис бази KDD здійснювався під час нормального функціонування обчислювальної системи.

Ці три стани є трьома групами, у які буде відносити спостереження дискримінантні функції, побудовані в процесі аналізу.

У результаті виконання дискримінантного аналізу вибірки даних у SPSS був сформований звіт. Далі приведені важливі для вирішення задачі його показники.

Першим вагомим показником є канонічна кореляція - міра зв'язку між двома множинами змінних. Вона є кореляцією між множиною груп та множиною коефіцієнтів дискримінантної функції. Максимальна величина цього коефіцієнта дорівнює 1. Чим більша ця величина, тим краща розділова здатність дискримінантної функції. В результаті дискримінантного аналізу була отримана канонічна кореляція 0.82 - це означає, що відмінність між двома групами, відносно яких проводиться аналіз доволі велика і визначення належності спостереження до однієї із груп можливе.

Другим вагомим показником є лямбда Уілкса - відношення внутрішньогрупової суми квадратів до загальної суми квадратів. Даний коефіцієнт характеризує долю дисперсії оцінок дискримінантної функції, що не обумовлена відмінностями між групами, приймає значення 1 в разі, якщо середні значення для всіх груп виявляються рівними, і зменшується з ростом різниць середніх значень. Додатково визначається рівень значущості - характеристика ймовірності того, що відмінності між групами є випадковими. В результаті дискримінантного аналізу була отримана лямбда Уілкса 0.32 та рівень значущості 0 - це означає, що середні груп відрізняються доволі сильно та відмінності між групами не є випадковими.

Третім та четвертим вагомими показниками є матриця стандартизованих коефіцієнтів канонічної дискримінантної функції та матриця структурних

коефіцієнтів. Вони являються показниками ваги параметрів дискримінантного аналізу.

Структурні коефіцієнти визначаються коефіцієнтами взаємної кореляції між окремими змінними і дискримінантною функцією. Якщо щодо деякої змінної абсолютна величина коефіцієнта велика, то вся інформація про дискримінантну функцію укладена в цій змінній.

Структурні коефіцієнти по своїй інформативності дещо відрізняються від стандартизованих коефіцієнтів. Стандартизовані коефіцієнти показують внесок змінних в значення дискримінантної функції. Якщо дві змінні сильно корельовані, то їх стандартизовані коефіцієнти можуть бути менше в порівнянні з тими випадками, коли використовується тільки одна з цих змінних. Такий розподіл величини стандартизованого коефіцієнта пояснюється тим, що при їх обчисленні враховується вплив усіх змінних. Структурні ж коефіцієнти є парними кореляціями і на них не впливають взаємні залежності інших змінних.

У [20-24] рекомендується при проведенні дискримінантного аналізу для редукції простору параметрів відкидати найменш значущі параметри, покладаючись на стандартизовані коефіцієнти. У даній роботі редукція множини параметрів мережевого трафіку буде виконуватись на основі паралельного аналізу значень стандартизованих коефіцієнтів, структурних коефіцієнтів та парних кореляцій між параметрами що аналізуються.

Отримані стандартизовані та структурні коефіцієнти приведені у таблиці 2.2 (приведені абсолютні значення).

Таблиця 2.2 - Стандартизовані та структурні коефіцієнти дискримінантного аналізу

	Коефіцієнти стандартизованої канонічної дискримінантної функції		Матриця структури	
	Функція 1	Функція 2	Функція 1	Функція 2

src_bytes	1,076	0,272	0,901	0,112

Продовження таблиці 2.2

	Коефіцієнти стандартизованої канонічної дискримінантної функції		Матриця структури	
	Функція 1	Функція 2	Функція 1	Функція 2
dst_bytes	0,058	0,014	0,034	0,007
count	0,099	0,389	0,180	0,727
srv_count	0,001	0,140	0,087	0,356
serror_rate	0,406	0,275	0,086	0,349
srv_serror_rate	0,046	0,209	0,085	0,347
same_srv_rate	0,004	0,066	0,080	0,326
dst_host_same_srv_rate	0,264	1,029	0,041	0,156
dst_host_srv_serror_rate	0,467	0,675	0,032	0,118
flag_transformed	0,439	0,397	0,051	0,059

Як видно із таблиці 2.2 стандартизовані та структурні коефіцієнти у більшості випадків значно відрізняються між собою для кожного окремого параметру. Це свідчить про те, що деякі з цих у значній мірі корельовані один з одним. Діаграма по таблиці 2.2 приведена на рисунку 2.8.

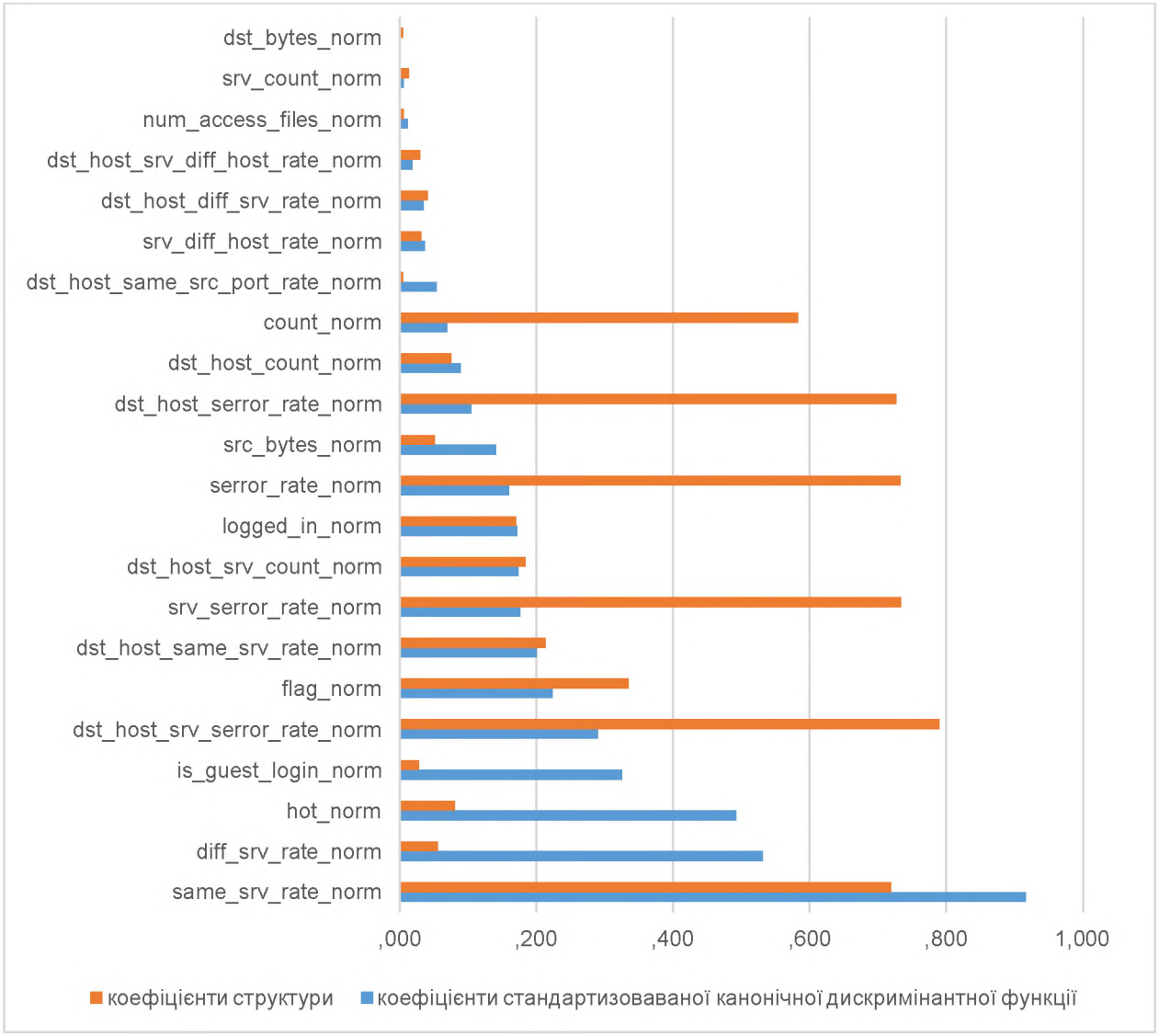


Рисунок 2.8 – Діаграма значень стандартизованих та структурних коефіцієнтів до редукції множини параметрів

На рисунку 2.8 показово відображені значення коефіцієнтів для кожного параметру мережевого трафіку. Найменш вагомі параметри видаляються.

Параметри, що залишилися аналізуються наступним чином:

- обчислюються парні кореляції;
- по значенням кореляцій визначаються найбільш корельовані параметри;
- із корельованих параметрів відкидаються ті, чиї коефіцієнти нижчі, зокрема структурні коефіцієнти.

У результаті усунення параметрів таким чином їх кількість була зменшена з 19 до 10. Для порівняння знову проводиться дискримінантний аналіз, тільки для параметрів що залишилися. Кінцева остаточна діаграма приведена на рисунку 2.9.

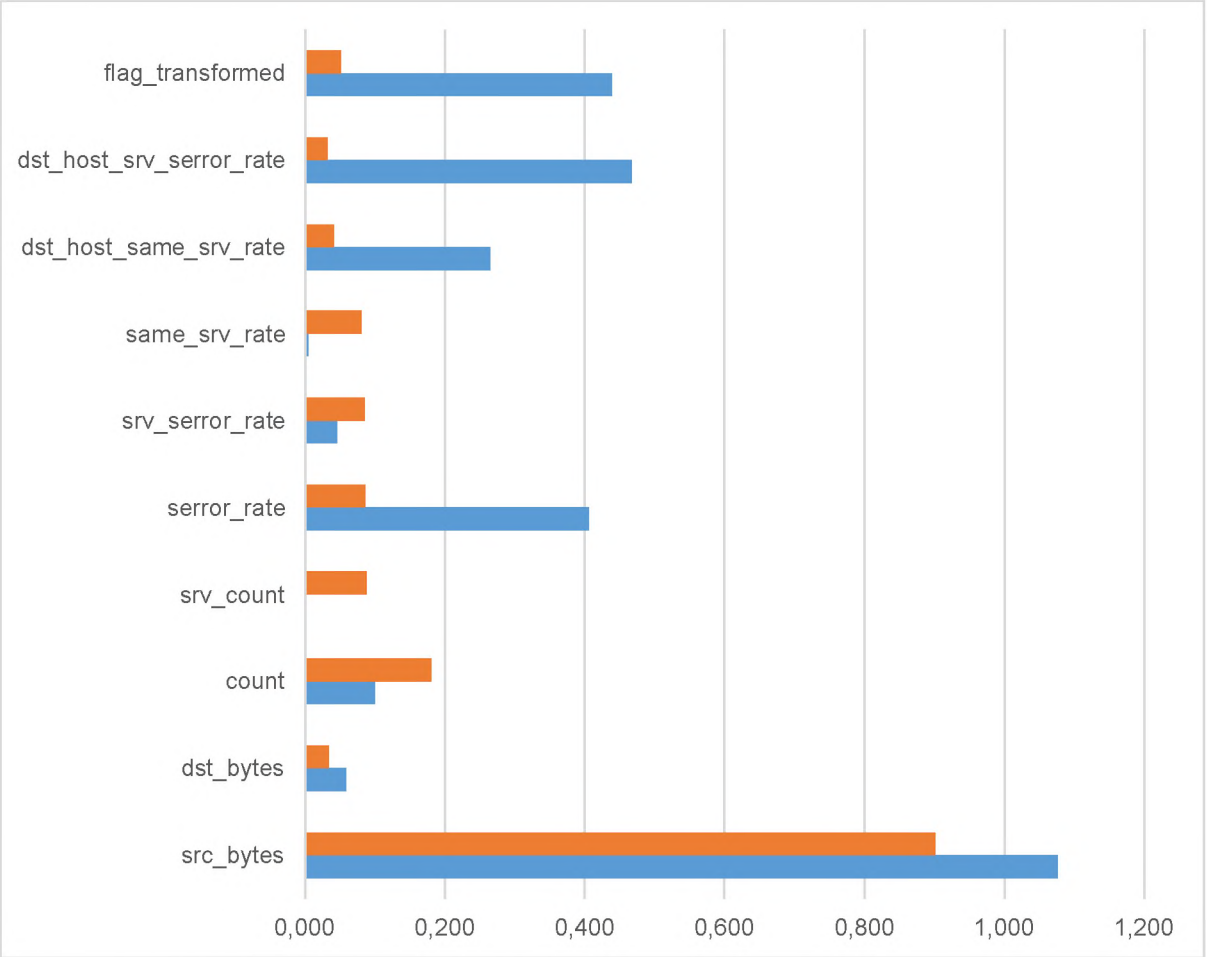


Рисунок 2.9 – Діаграма значень стандартизованих та структурних коефіцієнтів після редукції множини параметрів

Для оцінки результату редукції параметрів приведено рисунок 2.10.

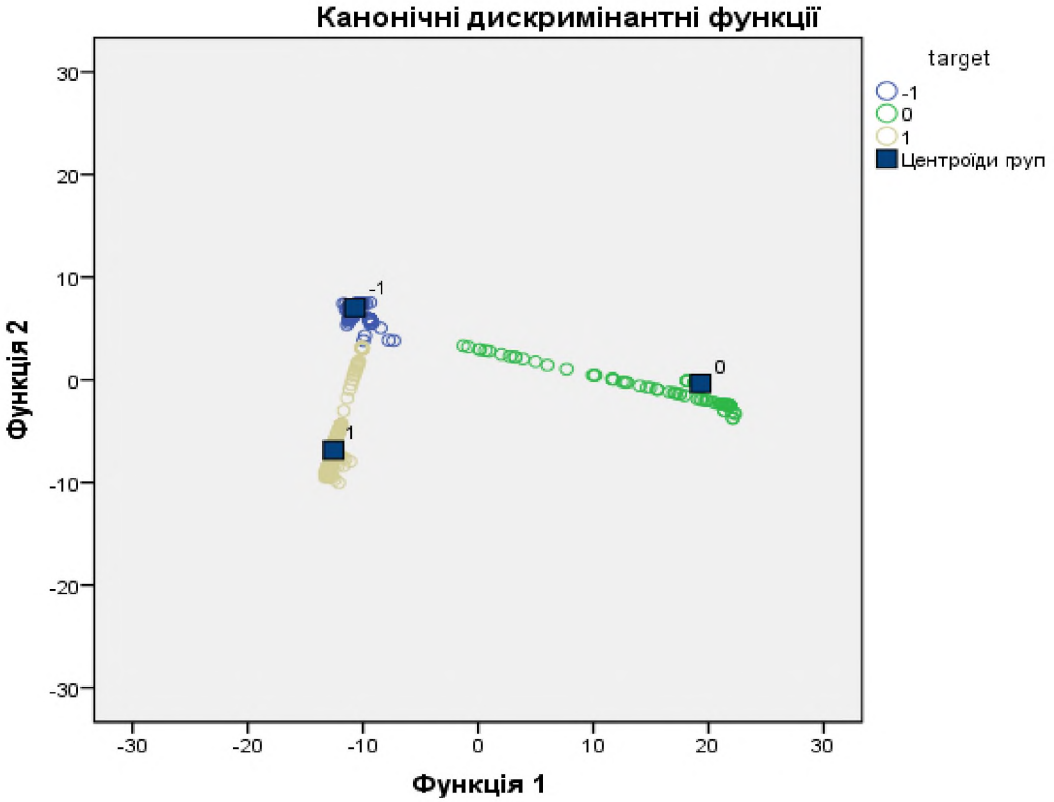


Рисунок 2.10 – Відображення класифікованих дискримінантними функціями даних

На рисунку можна спостерігати чітке розділення даних на три множини, що дає змогу стверджувати, що по ці дані можна класифікувати.

	Имя	Тип	Ширина	Знаков ...	Метка	Значения	Пропущенн...	Ширина ...
1	service	Текстовая	16	0		Нет	Нет	9
2	flag	Текстовая	7	0		Нет	Нет	7
3	flag_transformed	Числовой	1	0		Нет	Нет	18
4	src_bytes	Числовой	3	0		Нет	Нет	8
5	dst_bytes	Числовой	5	0		Нет	Нет	8
6	count	Числовой	2	0		Нет	Нет	8
7	srv_count	Числовой	2	0		Нет	Нет	8
8	serror_rate	Числовой	4	0		Нет	Нет	8
9	srv_serror_rate	Числовой	4	0		Нет	Нет	8
10	same_srv_rate	Числовой	4	0		Нет	Нет	8
11	dst_host_same_srv_rate	Числовой	4	0		Нет	Нет	8
12	dst_host_srv_serror_rate	Числовой	4	0		Нет	Нет	8
13	status	Текстовая	16	0		Нет	Нет	16
14	target	Числовой	8	2	target	Нет	Нет	10

Рисунок 2.11 – Кінцева вибірка вхідних параметрів для нейронної мережі, відокремлених з бази даних KDD

Отже, після виділення найбільш інформативних параметрів, з оброблюваної бази можна видалити всі інші та отримати базу, з якої можна зробити усі необхідні вибірки для навчання, перевірки і контролю нейронної мережі.

2.2 Синтез нейромережевих моделей для ідентифікації мережевих атак типу DoS (back та neptune)

У цьому підрозділі буде синтезовано НММ, здатну на ідентифікацію атак типу DoS (back та neptune). Для цього необхідно:

- визначити нейромережеву парадигму, яку буде використано для синтезу НММ;
- визначити оптимальні параметри НММ;
- сформувати вибірки даних – навчальну, тестову та контрольну, використовуючи першу провести навчання НМ, а потім проаналізувати адекватність синтезованої моделі.

2.2.1 Визначення парадигми для використання у нейромережевих моделях

Однією з основних проблем, які з’являються при вирішенні задач з використанням нейромережевого підходу, є вибір архітектури нейронної мережі.

Засновуючись на результаті проведеного аналізу літературних джерел та наукових праць для моделювання обрано парадигму мереж прямого розповсюдження сигналу, як найбільш частіше використовувану для вирішення подібних задач.

Парадигма НМ обрана для синтезу моделі – однонаправлена мережа прямого розповсюдження. Алгоритм навчання – зворотного розповсюдження.

У НМ синапси здійснюють зв'язок між нейронами і множать вхідний сигнал на число, що характеризує силу зв'язку – вагу синапсу. Суматор виконує додавання сигналів, що надходять по синаптичним зв'язкам від інших нейронів

і зовнішніх вхідних сигналів. Перетворювач реалізує функцію одного аргументу, виходу суматора, в деяку вихідну величину нейрона. Ця функція називається функцією активації нейрона. Нейрон в цілому реалізує скалярну функцію векторного аргументу.

Для НММ, що синтезується у даній роботі були обрані функції активації:

- сигмоїдна функція у вигляді гіперболічного тангенсу – для прихованих нейронів;
- лінійна функція – для вихідного нейрона.

У пакеті MATLAB сигмоїдна функція у вигляді гіперболічного тангенсу визначена як:

$$tansig(n) = \frac{2}{1 + \exp(-2n)} - 1$$

Лінійна функція активації визначена як:

$$purelin(n) = n$$

В якості навчальної функції зворотного поширення обраний метод метод Левенберга-Марквардта – метод нелінійної оптимізації, що використовує для пошуку мінімуму комбіновану стратегію – лінійну апроксимацію і градієнтний спуск. Перемикання з одного методу на інший відбувається в залежності від того, чи була успішною лінійна апроксимація; такий підхід називається моделлю довірчих областей. Алгоритм вдало поєднує в собі метод найшвидшого спуску (тобто мінімізації уздовж градієнта) і метод Ньютона (тобто використання квадратичної моделі для прискорення пошуку мінімуму функції). Від методу найшвидшого спуску алгоритм запозичив стабільність роботи, від методу Ньютона – прискорену збіжність в околицях мінімуму.

Ваги та зміщення підстроюються методом градієнтного спуску з іпульсом. Імпульс дозволяє мережі реагувати не тільки на локальний градієнт, а й на останні тенденції в поверхні помилок. Діючи як фільтр нижніх частот, імпульс дозволяє мережі ігнорувати невеликі особливості поверхні помилок. Без імпульсу мережа може застрягти в дрібному локальному мінімумі. З імпульсом мережа може ковзати через такий мінімум.

Імпульс може бути доданий до навчання зворотного поширення, роблячи зміни у вазі еквівалентними сумі частки останньої зміни ваги і нових змін, запропонованих правилом зворотного поширення. Величина ефекту, що остання зміна ваги спричинює мати опосередкований імпульсом постійного, МС, який може бути будь-яким числом від 0 до 1. Якщо константа імпульсу дорівнює 0, зміна ваги ґрунтується виключно на градієнті. Коли постійний імпульс дорівнює 1, то нова зміна ваги встановлюється рівною попередній зміні ваги, а градієнт просто ігнорується. Градієнт обчислюється шляхом підсумовування градієнтів, обчислених на кожному прикладі навчання, а також ваги і ухили оновлюються тільки після того, як були представлені всі навчальні приклади.

Якщо нова функція продуктивності на даній ітерації перевищує функцію продуктивності на попередній ітерації більш ніж на заздалегідь визначене співвідношення, то нові ваги і ухили відкидаються, а імпульсний коефіцієнт встановлюється рівним нулю.

Так як чітких рекомендацій по структурі нейронної мережі немає, її параметри обиралися експериментально. Кількість нейронів на вході и виходах відповідно дорівнюють кількості змінних у вхідних і вихідних вибірках. Експериментально визначено оптимальну структуру з трьома прихованими шарами нейронів, по 20, 10 і 5 нейронів відповідно.

2.2.2 Моделювання та перевірка адекватності

Для моделювання НМ у даній роботі використовується MATLAB – пакет прикладних програм для числового аналізу.

Процес навчання нейронної мережі полягає у налаштуванні її внутрішніх параметрів під конкретну задачу. Алгоритм роботи нейронної мережі є ітеративним, а його ітерації називають епохами або циклами.

Епоха – це одна ітерація процесу навчання, яка включає в себе надання усіх прикладів з навчальної вибірки і, можливо, перевірку якості навчання на контрольній множині.

Процес навчання здійснюється на навчальній вибірці, яка включає в себе вхідні значення та відповідні їм вихідні значення набору даних. У процесі навчання нейронна мережа знаходить деякі залежності вихідних значень від вхідних.

Для моделювання дані розділено на шість множин.

Дві множини – для навчання: навчальна та цільова. Ще дві на вхід мережі: тестова і контрольна. А також відповідні їм цільові множини для обчислення абсолютної помилки мережі.

У навчальних множинах близько 3 тисяч спостережень. Для навчальної множини сформована матриця 10 на 2867, у якій кожен стовпець представляє окреме спостереження. Щодо цільової множини для навчання, вона представляє собою вектор з 2867 значень, які можуть дорівнювати -1 (у нормальному стані мережі), 0 (при здійсненні атаки типу «back») та 1 (при здійсненні атаки типу «Neptune»).

Так само, за винятком кількості спостережень, влаштовано по дві множини, по 1500 спостережень для тесту та контролю роботи нейронної мережі.

Схожість трьох множин вхідних даних зображено на рисунку 2.12:

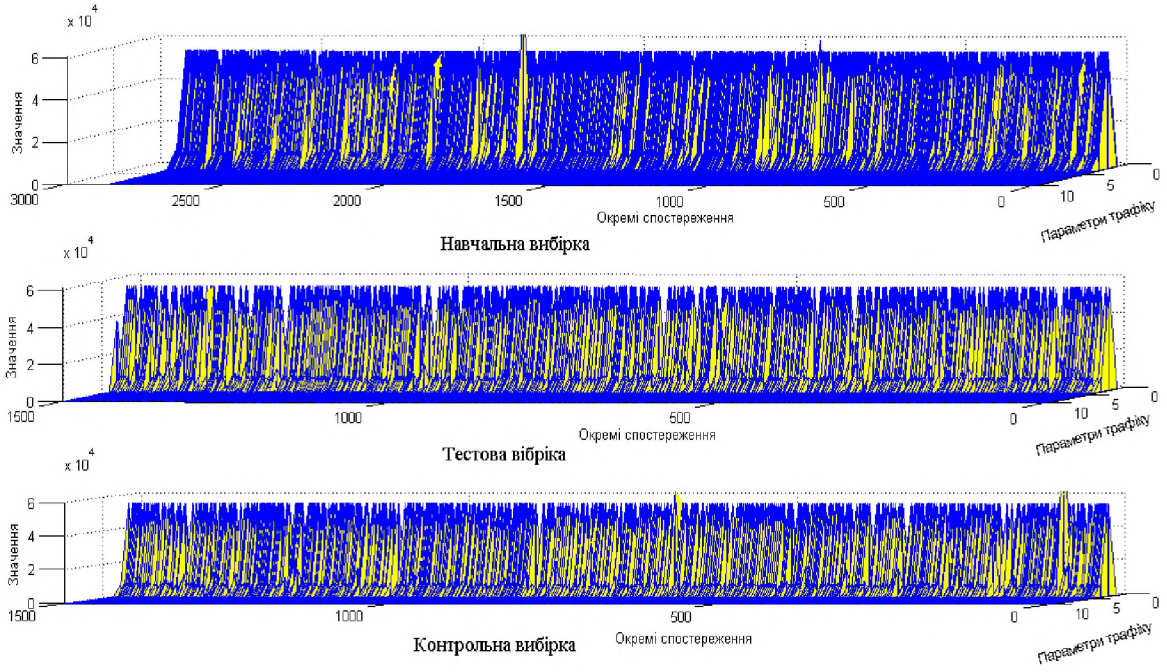


Рисунок 2.12 – Вибірки вхідних даних для нейронної мережі

Процес навчання зображено на рисунку 2.13.

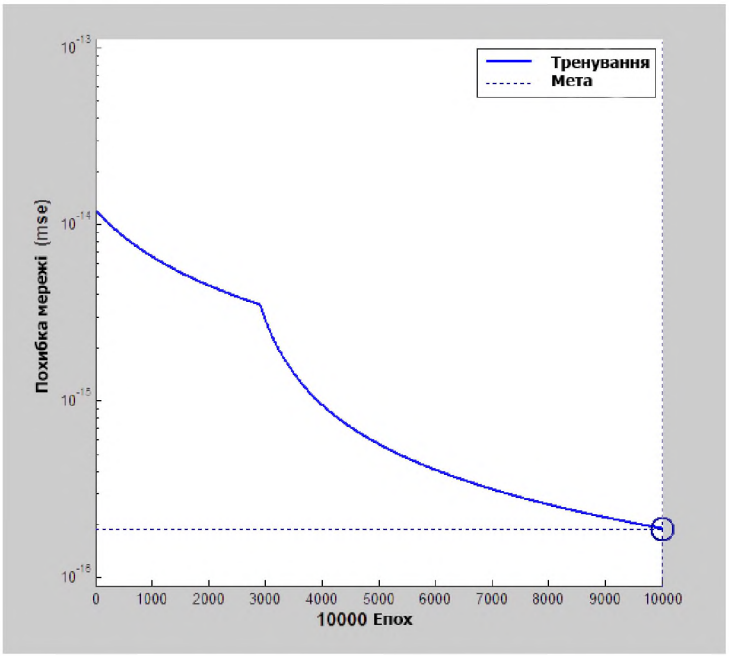
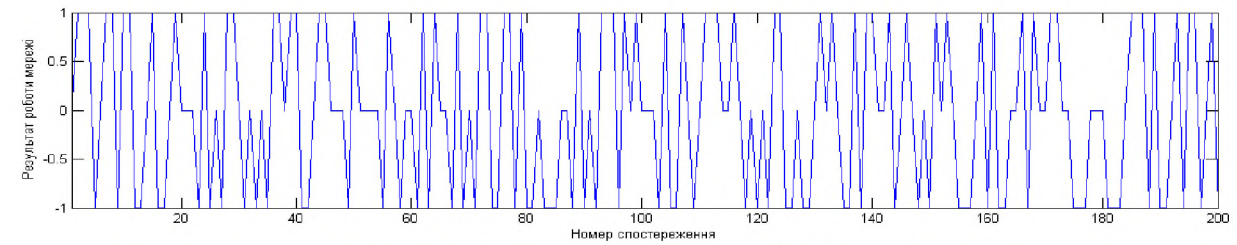


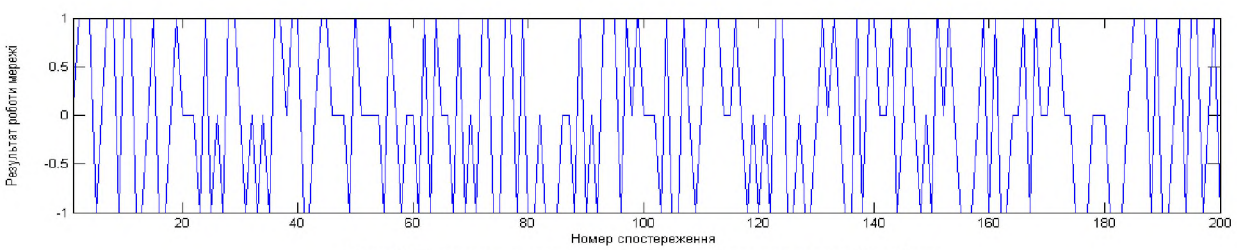
Рисунок 2.13 – Процес навчання нейронної мережі

Далі мережу було перевірено не тестовій і контрольних вибірках. Для перевірки симулювалася робота мережі з подачею на вхід тестової і контрольної вибірки. Результати роботи мережі можна візуально порівняти з еталонними даними. Оскільки порівняти два графіка по 1500 спостережень складно, на рисунках виведено частину по 200 перших результатів роботи мережі, відповідно для 200 перших спостережень.

Порівняння тестової вибірки з еталонними значеннями:



Перші 200 значень з вихідних даних нейромережі за тестовою вибіркою



Перші 200 значень з еталонних вихідних даних для тестової вибірки

Рисунок 2.14 – Порівняння результату роботи нейронної мережі на тестовій виборці з еталонними значеннями

Для контрольної вибірки вихідні дані, у порівнянні з еталонними виглядають так:

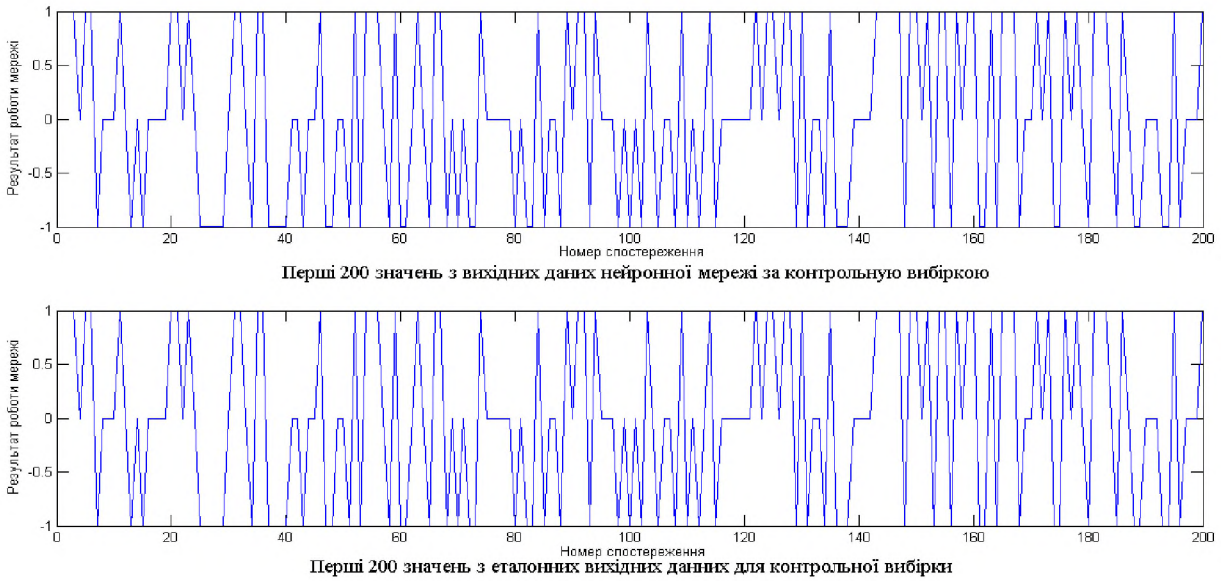


Рисунок 2.15 – Порівняння результату роботи нейронної мережі на контрольній виборці з еталонними значеннями

Після симуляцій для обох вибірок обчислювалася абсолютна похибка, як різниця цільових значень та виходу мережі, та відносна похибка, як абсолютна похибка, поділена на еталонні значення.

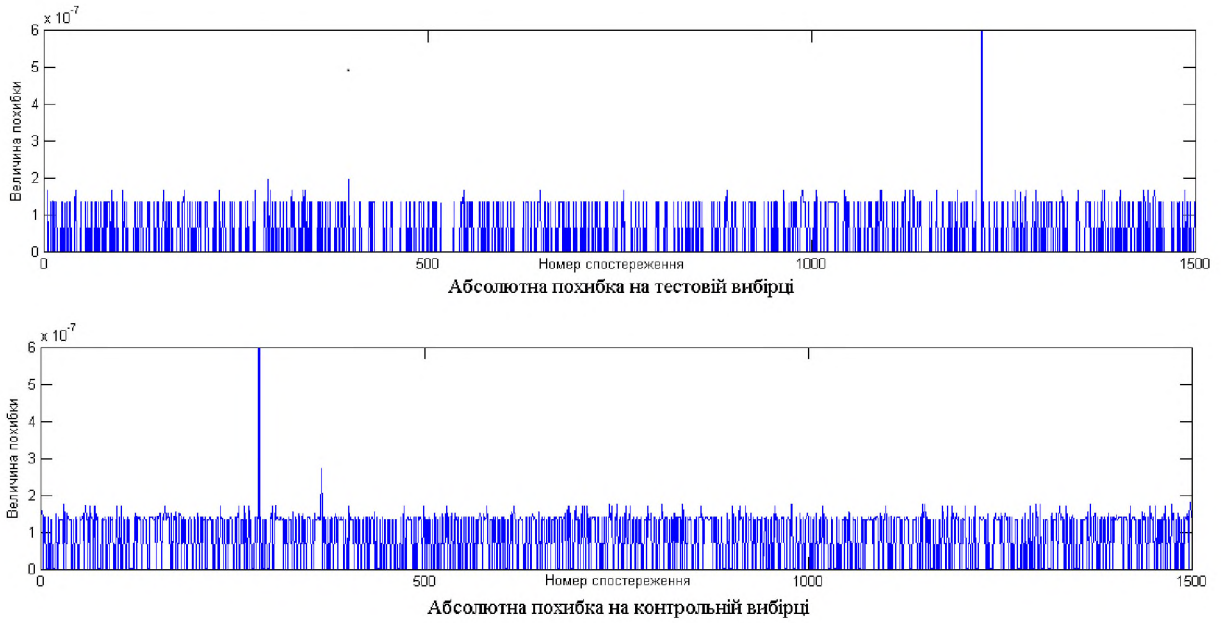


Рисунок 2.16 – Графіки абсолютної похибки для тестової і контрольної вибірок

Таблиця 2.3 – Значення відносної похибки для тестової і контрольної вибірок

Відносна помилка	для тестової вибірки	для контрольної вибірки
	0.000586%	0.00000739%

Через настільки низькі значення помилок при роботі такої архітектури можна зробити висновок, що її більш ніж достатньо, а необхідності в включенні іншої нейромережевої парадигми, для побудови гібридної моделі – немає.

2.3 Висновки до спеціальної частини

У спеціальній частині роботи, у ході аналізу, було визначено найбільш інформативні параметри, з точки зору ідентифікації даних мережевих атак типу DoS, а саме «back» та «neptune», визначено оптимальну структуру та синтезовано ефективні нейромережеві моделі ідентифікації мережевих атак.

Також перевірено їх адекватність на тестовій та контрольній вибірках даних.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Вступ

В економічній частині буде визначено витрати на дослідження можливості використання нейромережевих моделей для ідентифікації атак.

Вартість впровадження розроблених моделей розраховано за формулою 3.1.

$$C_{впр} = t_{впр} \cdot (C_{мч} + C_{зп}), грн, \quad (3.1)$$

де $t_{впр}$ – час досліджень;

$C_{мч}$ – вартість 1 години машинного часу, грн/год;

$C_{зп}$ – заробітна плата працівників, грн/год.

3.2 Капітальні витрати

3.2.1 Собівартість компонентів системи

У якості комп'ютера для досліджень використовувався персональний комп'ютер COBRA Advanced (A55.16.H1S4.36.16983). Його характеристик достатньо для виконання досліджень. Потужність комп'ютера дорівнює 0,6 кВт.

Щодо програмного забезпечення – вибір зроблений на користь пакету програмного забезпечення MatLab, що дозволяє моделювати нейронні мережі.

Інше обладнання було вибране серед того, що є доступним на ринку.

Вартість компонентів системи вказана у таблиці 3.1.

Таблиця 3.1 – Собівартість системи

№	Компонент	Ціна
Обладнання		
1	Монітор Dell S2722DC (210-BBRR)	12100 грн.

№	Компонент	Ціна
2	Персональний комп'ютер COBRA Advanced (A55.16.H1S4.36.16983)	29500 грн.
3	Маніпулятор миша Logitech G305 Wireless Black	2500 грн.
4	Клавіатура HP 450 Programmable Wireless Keyboard	1490 грн.
Ліцензійне ПЗ		
5	Програмне забезпечення MatLab	88830 грн.
	Усього	134420 грн.

Вартість обладнання становить 45590 грн.

Вартість ліцензійного ПЗ становить 88830 грн.

3.2.2 Розрахунок вартості 1 години машинного часу

Вартість 1 години машинного часу розраховується за формулою 3.2.

$$С_{мч} = P \cdot С_е + \frac{Ф_{перв} \cdot Н_а}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p}, \text{грн/год}, \quad (3.2)$$

де

Р – встановлена потужність сервера, кВт;

$С_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{перв}$ – первісна вартість обладнання на початок року, грн.;

$Н_а$ – річна норма амортизації на обладнання, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня Fр - 2080 год).

Тариф на електроенергію для населення, яке розраховується з енергопостачальною організацією за загальним розрахункових засобів обліку та

об'єднане шляхом створення юридичної особи, житлово-експлуатаційним організаціям, крім гуртожитків, становить 2,64 грн (за 1 кВт·год, з ПДВ).

Річну норму амортизації буде визначено за формулою 3.3

$$\text{Н} = \frac{1}{T} \cdot 100\%, \%, \tag{3.3}$$

де Т – період використання компонента.

Планується використовувати обладнання протягом 3 років. А програмне забезпечення - протягом 5 років.

Річна норма амортизації на обладнання – 33%.

Річна норма амортизації на ліцензійне ПЗ – 20%.

Отже, можна порахувати вартість 1 години машинного часу за формулою 3.4:

$$\text{С}_{\text{мч}} = 0{,}6 \cdot 2{,}64 + \frac{45590 \cdot 0{,}33}{2090} + \frac{88830 \cdot 0{,}2}{2090} = 17{,}36 \text{ грн/год} \tag{3.4}$$

3.2.3 Заробітна плата працівників

Для розрахунку буде прийматися до уваги лише мінімальна заробітна плата, яка становить 6700 грн, а з урахуванням податків (22%) - 1474 грн.

Враховуючи 40 годинний робочий тиждень, заробітна плата за годину буде складати 47,16 грн/год.

3.2.4 Розрахунок вартості впровадження результатів досліджень

Відповідно до формули 3.1, вартість впровадження результатів дослідження буде складати:

$$\text{С}_{\text{впр}} = 320 \cdot (17{,}36 + 47{,}16) = 20646{,}40 \text{ грн.} \tag{3.5}$$

3.3 Витрати на обслуговування

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е \text{ , грн,} \quad (3.6)$$

де

Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин

$$С_{ел} = 0,6 * 2,64 * 2080 = 3294,72$$

Річна сума амортизації обладнання та ПЗ визначається за формулою:

$$С_а = Ф_{перв} \cdot Н_а + К_{лпз} \cdot Н_{апз} \text{ , грн/год,} \quad (3.7)$$

де:

$Ф_{перв}$– первісна вартість обладнання на початок року, грн.;

$Н_а$ – річна норма амортизації на обладнання, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.

$$С_а = 45590 * 0,33 + 88830 * 0,2 = 32810,70 \text{ грн.}$$

Поточні витрати на обслуговування розраховуються за формулою (3.8).

$$С = С_{ел} + С_а \quad (3.8)$$

$$С = 3294,72 + 32810,70 = 36105,42 \text{ грн.}$$

3.4 Розрахунок NPV інвестиційного проєкту

NPV – це скорочення за першими літерами фрази «Net Present Value» і розшифровується це як чиста приведена (до сьогоднішнього дня) вартість.

$$NPV = \sum \frac{B_n}{(1+r)^T} - K \geq 0 \quad (3.9)$$

де

r – ціна капіталу, що дорівнює ставці НБУ 16% на 01.11.2023 р.,

Т – строк дії проєкту = 2 роки,

К – капітальні інвестиції = 134420 грн.,

B_n – грошовий потік, що складається з різниці між чистим прибутком після оподаткування та поточними витратами на обслуговування проекту.

$$B_n = П - С \geq {К}/{\sum \frac{1}{(1+r)^T}} \quad (3.10)$$

$$П = {134420}/{\sum \frac{1}{(1+0,18)^2}} + 36105,42$$

$$\geq {134420}/{(1,16^{-1} + 1,16^{-2})} + 36105,42$$

$$\geq {134420}/{(0,86 + 0,74)} + 19006,3 \geq {134420}/{1,6} + 36105,42$$

$$\geq 120117,92$$

$$П \geq 120117,92 \text{ грн.}$$

3.5 Висновки до розділу

В економічній частині роботи було визначено витрати на дослідження можливості використання нейромережевих моделей ідентифікації атак.

Впровадження синтезованої моделі є доцільним для підприємств з чистим річним прибутком після оподаткування $П \geq 120117{,}92$ грн.

Вартість обладнання становить 45590 грн. Вартість ліцензійного ПЗ становить 88830 грн. Поточні витрати на обслуговування системи на рік 36105,42 грн.

ВИСНОВКИ

У роботі було успішно вирішено важливе наукове завдання ідентифікації мережевих атак за допомогою нейромережевих моделей. Проведено глибокий аналіз видів мережевих атак, зокрема типів «Back» та «Neptune», та визначено ключові параметри трафіку для їх ідентифікації.

Розроблені нейромережеві моделі демонструють високу точність у виявленні мережевих атак, що було підтверджено за допомогою тестування на контрольних даних.

Результати дослідження вказують на значний потенціал нейромережевих моделей для подальшого вивчення та розширення їх застосування для ідентифікації ширшого спектра мережевих атак.

В економічній частині роботи визначено витрати на впровадження цих результатів та оцінено економічну доцільність їх використання для певних типів підприємств.

ПЕРЕЛІК ПОСИЛАНЬ

1. ISACA. State of Cybersecurity: Implications for 2015 // http://www.isaca.org/. 2015. URL: http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

2. МИКОЛАЙОВИЧ М.В. МЕТОД ПОБУДОВИ КЛАСИФІКАТОРА КІБЕРАТАК НА ДЕРЖАВНІ ІНФОРМАЦІЙНІ РЕСУРСИ Київ. 2015.

3. Symantec. INTERNET SECURITY THREAT REPORT 2015. URL: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

4. S. H. Cyberterrorism: history of current trends and countermeasures. Privacy notice. Vol. 9. No. 2. pp. 118 -129. 2013.

6. Лист № 67 від 14.04.2015 р. Президентові України URL: http://www.inau.org.ua/52.3150.1.0.1.0.phtml

7. Концепція інформаційної безпеки Укріїни URL: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf

8. Офіц. вісник України. Про рішення Ради національної безпеки і оборони України, Київ, 2010.

9. Петрович Ш.В. Поняття та сутність кібернетичної атаки // УДК 343.9:345.42. 2011.

10. Бусел г.р.В.Т. Великий тлумачний словник сучасної української мови. Ірпінь: ВТФ “Перун”, 2009. Р. 1736 с.

11. О. К.О. Актуальні проблеми управління інформаційною безпекою // In: Кіберпростір як нова арена воєнних дій. Наук.-вид. відділ НА СБ України, 2011.

12. України Н.і.т.с.д.п.П. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю URL: http://www.niss.gov.ua/articles/454/

13. И. Д. Медведовский П.В.С.В.В.П. Медведовский И. Д. Атака через INTERNET URL: http://citforum.univ.kiev.ua/internet/attack/c11.shtml

14. А. І.О. Захист інформаційно-телекомунікаційної сфери від стороннього кібернетичного впливу – одна з найважливіших проблем сучасності, 2011.

15. В М.С. До проблеми формування понятійно-термінологічного апарату кібербезпеки , 2011.

16. ISO/IEC 27000, Система менеджмента информационной безопасности. Общий обзор и терминология.

17. ISO/IEC 27001, Система менеджмента информационной безопасности. Требования.

18. ISO/IEC 27033-1 Методы и средства обеспечения безопасности. Безопасность сетей. Обзор и концепции.

19. Додонов А.Г. Л.Д.В. Живучесть информационных систем. 256 pp. Киев: Наук. думка, 2011.

20. Руденко О.Г. Б.Є.В. Штучні нейронні мережі. Навч. посіб. Харків: ТОВ "Компанія СМІТ", 404 с., 2006.

21. Chen Y. N.A..S.P..B.T. Multiple sequence alignment and artificial neuralnetworks for malicious software detection // Natural Computation P. 261 – 265.. 2012.

22. Du Toit T. K.H. Filtering spam e-mail with Generalized AdditiveNeural Networks // Information Security for South Africa., 2012. pp. 1-8.

23. Skaruz J. S.F. Recurrent neural networks towards detection of SQL attacks // Parallel and Distributed Processing Symposium., 2007.

24. KDD Cup Data [Электронный ресурс] // UCI Knowledge Discovery in Databases Archive: [сайт]. URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	15	
6	А4	2 Розділ	39	
7	А4	3 Розділ	6	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК
на кваліфікаційну роботу магістра на тему:
Виявлення DoS атак на основі гібридних нейронних мереж
студента групи 125м-22-1
Кравченка Богдана Сергійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 76 сторінках та містить 16 рисунків, 3 таблиць, 24 джерел та 4 додатка.

Об'єкт дослідження: процес ідентифікації мережевих атак типу DoS (back, land, neptune, pod, smurf, teardrop).

Мета роботи: визначення можливості застосування нейромережевих моделей для ідентифікації мережевих атак типу DoS (back, land, neptune, pod, smurf, teardrop).

Методи дослідження: абстракція, дедукція, системний підхід, методи порівняння, кореляційний аналіз.

У спеціальній частині були розглянуті атаки типу DoS і особливості їх реалізації, визначені інформативні параметри мережевого трафіку, використовуючи які можна ідентифікувати ці атаки.

У роботі синтезовані нейромережеві моделі, здатні на ідентифікацію атак типу DoS, а саме підтипів «back» та «neptune», проаналізована адекватність синтезованих моделей.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник