Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Відельського Ярослава Володимировича

на здобуття ступеня вищої освіти Бакалавра

Система виявлення DDoS-атаки

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.2101017.20.01.03 ПЗ

Виконав студент 4 курсу група КБ-20-1 Ярослав ВІДЕЛЬСЬКИЙ
Керівник канд. техн. наук, доцент Вікторія ОРЛЕНКО
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

12 06 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Відельському Ярославу Володимировичу

1 Тема роботи Система виявлення DDoS-атак

Керівник роботи к.т.н. доцент Вікторія ОРЛЕНКО

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру 12.06.2024

3 Вихідні дані до роботи Проаналізувати особливості реалізації DDoS-атак, зокрема типи протоколів, вміст пакетів даних, засоби та механізми реалізації атак. Порівняти існуючі методи їх виявлення, проаналізувати переваги та недоліки. Розробити алгоритм роботи системи виявлення атаки у мережі та змоделювати систему. Обґрунтувати обрані засоби моделювання Розробити систему виявлення DDoS-атак. Довести ефективність розробленої системи за допомогою тестових наборів даних.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Аналіз DDoS-атак та методів їх виявлення. Постановка задачі. Проектування системи виявлення DDoS-атаки. Вибір засобів для моделювання і реалізації системи виявлення. Алгоритм реалізації системи виявлення DDoS-атаки. Прототип системи виявлення DDoS-атаки. Програмна реалізація. Експериментальне дослідження роботоздатності. Доведення ефективності.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Моделювання системи нечіткого логічного висновку засобами Matlab. Схеми реалізації системи виявлення DDoS-атаки. Оцінка достовірності системи виявлення DDoS-атаки.

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., старший викладач кафедри кібербезпеки		

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Червень	
Захист КР	Червень	

Студент _____ Ярослав ВІДЕЛЬСЬКИЙ

Керівник кваліфікаційної роботи _____ Вікторія ОРЛЕНКО

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система виявлення DDoS-атаки»

Автор роботи: студент групи КБ–20–1 Відельський Я.В.

Керівник роботи: к.т.н. доц. Орленко В.С.

Пояснювальна записка: 60 с., 22 рисунки, 8 таблиць, 40 джерел, 3 креслення.

ПЕРЕЛІК КЛЮЧОВИХ СЛІВ: DDOS-АТАКА, СИГНАТУРА, НЕЧІТКИЙ ЛОГІЧНИЙ ВИСНОВОК, CIC-DDOS2019, МЕРЕЖЕВИЙ ТРАФІК.

Метою кваліфікаційної роботи є виявлення DDoS-атак, які реалізуються в середині локальної мережі на інших локальних користувачів або на сторонні ресурси. Тому робота спрямована на розробку системи виявлення DDoS-атак у мережі шляхом застосування нечіткої логіки для прийняття рішення. Основними завданнями, які було виконано є розробка алгоритму реалізації системи, підготовка набору даних, формування нечітких правил, розробка системи виявлення, опис технічних вимог задля забезпечення роботоздатності системи, тестування та доведення ефективності розробленої системи.

В роботі значну увагу приділено вибору засобу для моделювання системи виявлення DDoS-атаки. Також представлено набір даних CICDDoS 2019, що використовується для оцінки ефективності виявлення DDoS-атак.

Робота містить опис схеми комп'ютерної мережі, модель системи та алгоритм роботи системи з деталізацією всіх етапів прийняття рішення. Також описано ізольовану локальну мережу для дослідження та тестування роботи системи при реальних умовах.

10.06.2024

ABSTRACT

Topic of the qualification work: "DDoS attack detection system"

Author: student of group KB-20-1, Videlskyi Ya. V.

Supervisor: Ph.D., Associate Professor Orlenko V. S.

Explanatory note: 60 pages, 22 figures, 8 tables, 40 sources, 3 diagrams.

LIST OF KEYWORDS: DDoS ATTACK, SIGNATURE, FUZZY LOGIC INFERENCE, CIC-DDoS2019, NETWORK TRAFFIC.

The goal of the qualification work is to detect DDoS attacks occurring within a local network targeting other local users or external resources. The work is therefore focused on developing a DDoS attack detection system within a network using fuzzy logic for decision-making. The main tasks accomplished include the development of the system implementation algorithm, preparation of the dataset, formulation of fuzzy rules, development of the detection system, description of technical requirements to ensure system operability, testing, and proving the effectiveness of the developed system.

Significant attention is given to the selection of tools for modeling the DDoS attack detection system. The work also presents the CICDDoS 2019 dataset used to evaluate the effectiveness of DDoS attack detection.

The work contains a description of the computer network scheme, system model, and algorithm of the system's operation with detailed stages of decision-making. An isolated local network for research and testing the system under real conditions is also described.

10.06.2024

ЗМІСТ

ВСТУП

Розвиток мережевих технологій призводить до появи нових видів атак на комп'ютерні мережі. Із зростанням обсягу мережевого трафіку збільшується і кількість користувачів та переданої інформації. Це може викликати зниження якості мережевих послуг, що підкреслює потребу у вдосконаленні засобів для моніторингу та аналізу мережевого трафіку. Проблема аналізу трафіку вивчається протягом тривалого часу, існують багато досліджень, які ставлять за мету знаходження ефективних рішень в різних умовах і обмеженнях. Останнім часом зростає швидкість змін у мережевому ландшафті, що вимагає постійного оновлення методів і алгоритмів для аналізу трафіку. Таким чином, проблеми з аналізом трафіку та виявленням вторгнень в комп'ютерні мережі вимагають додаткових досліджень.

Дана кваліфікаційна робота спрямована на розробку системи виявлення DDoS-атак у мережі шляхом застосування нечіткої логіки для прийняття рішення. Проведення експериментів та оцінки ефективності здійснюється із використанням набору даних CIC-DDoS2019.

Метою роботи є виявлення DDoS-атак, які реалізуються в середині локальної мережі на інших локальних користувачів або на сторонні ресурси.

До завдань, які потрібно виконати в рамках роботи, варто віднести:

- підготовка набору даних;
- формування нечітких правил;
- розробка системи виявлення;
- тестування та доведення ефективності розробленої системи.

АНАЛІЗ DDOS-АТАК ТА МЕТОДІВ ЇХ ВИЯВЛЕННЯ

1.1 Типи DDoS-атак

DDoS атака (розподілена відмова в обслуговуванні, англ. Distributed Denial of Service) - це тип кібератаки, при якій зловмисники намагаються максимально завантажити або призупинити роботу цільового ресурсу, такого як веб-сайт чи мережа, шляхом одночасного відправлення великої кількості запитів чи трафіку.

Розподілена відмова в обслуговуванні виникає, коли сервер отримує настільки багато запитів, що він не здатний їх ефективно обробити. Причиною може бути нестача оперативної пам'яті або потужності процесора сервера, але результат залишається незмінним – веб-сторінки не відкриваються, і на екрані з'являються відповідні коди помилок (таблиця 1.1) [1].

Таблиця 1.1 – Можливі коди помилок при відмові в обслуговуванні сервером

Код помилки	Опис помилки
1	2
500	код стану HTTP, який означає, що сервер не зміг виконати запит через непередбачену помилку
502	недійсна відповідь від сервера
503	сервер тимчасово недоступний для обробки запиту
504	перевищено час відповіді сервера
509	хост отримує більше трафіку, ніж може впоратися
520	сервер повертає невідому помилку
521	оригінальний сервер веб-сайту недоступний для проміжного сервера (зазвичай Cloudflare)
522	час очікування з’єднання закінчився

Кінець таблиці 1.1

1	2
523	проміжний сервер не може підключитися до хост-сервера
524	Час очікування підключення через сервер Cloudflare минув

UDP-флуд - це форма атаки на відмову в обслуговуванні, при якій значна кількість пакетів протоколу дейтаграм користувача (UDP) надсилається на цільовий сервер з метою перевищення його здатності обробляти та відповідати. Для запуску атаки UDP flood, зловмисники надсилають великі обсяги UDP-трафіку з підробленими IP-адресами на випадкові порти цільової системи. При цьому система повинна перевіряти порт в кожному вхідному пакеті, визначений для програми, яка його очікує, та видавати відповідь. Це може швидко вичерпати ресурси цільового сервера, роблячи його недоступним для звичайного трафіку та легітимних користувачів. Підключення до Інтернету може стати перевантаженим і насиченим.

На відміну від TCP, UDP є протоколом без з'єднання, що означає, що з'єднання між клієнтом і сервером не встановлюється до передачі пакетів. Крім того, UDP не виявляє втрати пакетів і не надсилає повідомлень про втрату пакетів під час комунікації клієнт-сервер. Таким чином, UDP відрізняється низьким споживанням ресурсів і високою швидкістю обробки. Ці переваги роблять UDP популярним, але також надають зловмисникам можливість ініціювати атаки UDP flood [2].

Операційні системи можуть намагатися обмежити швидкість відповіді пакетів ICMP, що є частиною відповідей UDP, але цей підхід для протидії атакам є невибірковим і може також блокувати легітимний трафік. Зменшення впливу будь-якого типу DDoS слід проводити подалі від центру обробки даних або джерела, де ці інструменти атак менш ефективні.

Слід зазначити, що атаки UDP flood можуть бути викликані ботнетами, але зловмисники також використовують відкриті протоколи UDP, які легко атакують такі сервіси, як веб, DNS, SSH, SCP, SSL, TLS та інші.

У останні роки збільшилася популярність атак з підсиленням відображення UDP. Такі атаки мають дві основні характеристики: вони базуються на протоколі UDP і використовують фіксований номер порту цільової атаки. Принципи, що лежать в основі різних типів атак з підсиленням відображення UDP, подібні. Розповсюдженим видом є атака з підсиленням відображення протоколу мережевого часу (NTP), яка має дві основні особливості: відображення та підсилення. Під час UDP-зв'язку клієнт надсилає серверу пакет запиту, а сервер повертає клієнту відповідний пакет. Протягом усього спілкування перевірка не потрібна. Протокол UDP не передбачає встановлення з'єднання та не має механізму автентифікації джерела. Ці властивості використовуються зловмисниками для вчинення атак з підсиленням відображення. Під час таких атак IP-адреса джерела пакета запиту від клієнта змінюються на IP-адресу цільового об'єкта атаки, а пакет відповіді, відправлений сервером, надсилається до цілі атаки.

Об'ємну мережеву атаку можна визначити за раптовим стрибком обсягу вхідного мережевого трафіку.

Нижче наведено кілька заходів, які можна вжити для ефективного захисту від атаки UDP-флуду:

– обмеження швидкості відповідей ICMP, яке, зазвичай, реалізується на рівні операційної системи;

– фільтрація на рівні брандмауера на сервері, проте брандмауер також може стати уразливим під впливом UDP-атаки;

– фільтрація UDP-пакетів, крім DNS, на мережевому рівні [3].

Атака ICMP Flood, яка відноситься до типу атак на відмову в обслуговуванні, є однією із проблем у сфері кібербезпеки. Це може викликати невдоволення користувачів через недоступність послуг, суттєві втрати доходів і загальні незручності як на особистому, так і на корпоративному рівні.

Протокол ICMP представляє собою важливий протокол у наборі Інтернет-протоколів, використовуваний мережевими пристроями, такими як маршрутизатори. Він використовується для генерації повідомлень про помилки,

що вказують на недоступність служби або недоступність конкретного хоста чи маршрутизатора. Цей протокол забезпечує зворотний зв'язок стосовно проблем з підключенням до мережі, що вирішально важливо для роботи IP-мережі.

ICMP flood представляє собою атаку, під час якої зловмисник намагається переповнити доступну пропускну здатність цільової системи, використовуючи ехо-запити ICMP, відомі як пінги. Наслідком перевантаження мережі є неможливість легітимних мережевих запитів досягти сервера, що спричиняє відмову в обслуговуванні реальних користувачів. Згодом сервер або мережа змушені висилати кілька ехо-відповідей у формі "пінгу смерті", що, в кінцевому підсумку, призводить до перевантаження сервера [4].

Головна мета атаки ICMP Flood, яку ініціює зловмисник, полягає не в проникненні всередину системи для викрадення даних, а в перевантаженні мережевих ресурсів з метою встановлення контролю над системними збоями. Стратегія досить проста: затоплювати цільовий сервер настільки великою кількістю пакетів ICMP, не очікуючи відповідей. Це спричиняє сильне перевантаження мережі, що внаслідок цього призводить до втрати законного трафіку і, фактично, до відмови в обслуговуванні.

Атака ICMP flood створює загрозу для кібербезпеки різними способами. Внаслідок запобіжного або обмеженого доступу до мережевої послуги компанії можуть зазнати значних фінансових втрат, а також великих часових затримок. Окрім матеріальних втрат, це також призводить до підриву довіри до здатності компанії захищати свої системи, що може призвести до серйозних втрат репутації.

Атаки ICMP flood можуть бути помилково сприйняті як мережеві аномалії, що призводить до того, що IT-фахівці витрачають свої ресурси на відстеження помилково визначених системних проблем, замість того щоб фокусуватися на справжніх проблемах.

Для захисту від атаки ICMP flood компанії повинні вкладати значні ресурси в превентивні заходи з кібербезпеки. Ефективним заходом є обмеження швидкості трафіку ICMP, що зменшує ризик потенційної шкоди, завданої від атаки ICMP. Використання інтелектуальних систем моніторингу для виявлення нерегулярних

стрибків трафіку та аномальної активності системи є ще однією важливою стратегією. Застосування правил брандмауера для обмеження трафіку ICMP від надійних джерел або повне вимкнення такого трафіку може ефективно захистити систему.

Сервіси захисту від DDoS створюють суттєвий бар'єр проти атак ICMP flood. Ці служби розподіляють мережевий трафік рівномірно, запобігаючи затопленню цілей раптовими сплесками запитів. Також важливо враховувати антивірусні рішення, які, хоч і не можуть запобігти безпосередньо атакам ICMP flood, але можуть ідентифікувати явні моделі вторгнень, запобігаючи використанню зловмисником ботнету і, таким чином, зменшуючи ефективність атаки ICMP flood на початковому етапі.

Важливо усвідомити, що навіть такий стандартний протокол, як ICMP, може стати зброєю в руках зловмисників. Засвоєння знань про ці загрози підвищує рівень обізнаності щодо підтримки надійних підходів до кібербезпеки та етичного використання Інтернету. Це наголошує на важливості вживання ефективних заходів та включення елементів антивірусного програмного забезпечення для захисту від потенційних уразливостей, пов'язаних із атаками ICMP.

Суть атаки SYN flood полягає в тому, що клієнт неперервно надсилає пакети SYN (синхронізації) на кожен порт сервера, використовуючи підроблені IP-адреси. Під час атаки цільовий сервер спостерігає еквівалент декількох спроб встановити зв'язок. Він відправляє пакети SYN-ACK (підтвердження синхронізації) з усіх відкритих портів у відповідь на кожну спробу з'єднання, а також пакети RST (пакет скидання) з усіх закритих портів [5].

Процес тристороннього рукостискання складається з трьох етапів:

– клієнт ініціює з'єднання, відправляючи SYN-пакет на сервер;

– сервер відповідає, висилаючи SYN-ACK пакет;

– клієнт підтверджує отримання, відправляючи останній ACK-пакет.

Після виконання цих етапів розпочинається спілкування між клієнтом і сервером. У випадку SYN-флуду, ворожий клієнт не повертає ACK-пакет. Замість цього, він надсилає повторні SYN-запити на всі порти сервера. Зловмисники

використовують фальшиві IP-адреси, що ускладнює закриття з’єднання сервером за допомогою RST-пакетів.

У результаті залишається відкритий зв’язок, і нові SYN-пакети надходять до того, як стає можливим тайм-аут, утворюючи напіввідкрите з’єднання. Це переповнення запитами зловмисників робить важким або навіть неможливим з’єднання з легітимним трафіком [6].

Атака SYN flood може бути виконана різними способами, такими як підроблена, пряма або розподілена атака DDoS за допомогою ботнету. Існують також різні методи для пом’якшення цих атак, такі як обмеження швидкості, використання систем виявлення вторгнень, файли cookie SYN, збільшення черги відставання та переробка найстаріших напіврозкритих з'єднань. Важливо підібрати оптимальний метод в залежності від політики безпеки та конкретної інфраструктури мережі.

Надсилання значної кількості пакетів RTP протягом короткого періоду може викликати умови атаки на обслуговування. Ця стратегія особливо ефективна під час нападів на системи запису розмов, які використовують потоки RTP в якості вхідних даних. Інструмент за замовчуванням ініціює виклик за допомогою протоколу SIP, але може також приймати виклики або пропускати ініціалізацію сеансу, спровокуючи атаку RTP flood. Головною метою атаки є обробка RTP, тому інструмент встановлює лише один сеанс одночасно, але може генерувати кілька потоків RTP під час цього сеансу [7].

Потік RTP, який використовується під час атаки, складається з реальних пакетів RTP з правильними порядковими номерами та коректними даними. Це використовує той факт, що деякі системи запису можуть припускати, що швидкість пакетів для кожного окремого потоку RTP не є надто великою. Якщо це припущення порушується, то деякі системи можуть намагатися обробляти вхідні RTP-пакети. Це може вести до переповнення дискового простору та різкого зростання використання ЦП, що може призвести до відмови в обслуговуванні. За замовчуванням інструмент встановлює виклик через протокол SIP і направляє атаку на адресу RTP, яка вказана в тілі SDP [8].

HTTP або HTTPS-флуд – це форма розподіленої атаки типу "відмова в обслуговуванні", яка призводить до збою або уповільнення роботи сервера, веб-сайту або веб-програми, переповнюючи їх великою кількістю HTTP-запитів GET або POST. Ці запити виснажують обчислювальні ресурси та пропускну здатність сервера, призводячи до сповільнення або навіть відмови у обслуговуванні, що впливає на легітимних користувачів та трафік [10].

Зловмисник ініціює атаку, відправляючи надмірну кількість HTTP-запитів на цільовий хост. Це може бути досягнуто за допомогою сценарію або ботнетів. Крім того, ці запити можуть використовувати різні методи HTTP, такі як GET і POST. Як результат, цільовий веб-сайт переповнюється великою кількістю запитів, що спричиняє його сповільнення або відмову в обслуговуванні. В кінцевому підсумку законні користувачі не можуть отримати доступ до сервера, що призводить до втрати доступності служби [11].

Атака Slowloris тримає відкритими HTTP-з’єднання якнайдовше, використовуючи мінімальну пропускну здатність. В результаті зловмисник утримує веб-сервер в стані зайнятості, що призводить до перевантаження.

Трафік, який генерується зловмисником, часто може виглядати як легітимний, ускладнюючи виявлення атаки HTTP flood. Не залежно від типу, атаки HTTP flood важко виявити через великий обсяг генерованого трафіку. Тому важливо, щоб веб-сервери використовували ефективні засоби захисту для протидії таким атакам.

Для зменшення впливу атаки HTTP-flood організації можуть використовувати комбінацію оптимальних практик та кібербезпеки, включаючи:

– групи безпеки можуть слідкувати за трафіком і порівнювати IP-адреси з переліком IP у базі даних, щоб виявляти та блокувати аномальну активність, що може бути частиною HTTP-атаки;

– використання обчислювальних викликів JavaScript може перевірити, чи генерується трафік ботом;

– брандмауер веб-додатків використовує різні методи, такі як CAPTCHA та криптографічні виклики, для виявлення атак HTTP- flood;

– балансувальники навантаження можуть забезпечувати буферизацію та керування з’єднаннями, щоб запобігти впливу запитів HTTP GET і POST на ресурси веб-сервера;

– розгортання хмарної служби захисту від DDoS дозволяє виявляти підозрілу активність та швидко реагувати;

– обмеження кількості вхідних запитів з певної IP-адреси може запобігти DDoS-атакам.

Атака HTTP-flood може мати серйозний вплив, зокрема може викликати простої та збої в роботі, призводячи до фінансових втрат та шкоди репутації. Організації повинні вживати заходів для захисту від таких атак та забезпечення стійкості своїх веб-серверів.

Атака "Ping of Death" (PoD) представляє собою розповсюджений тип атаки на обслуговування, де зловмисник має за мету порушити або повністю вивести з ладу пристрій, сервер або сервіс жертви. Це досягається шляхом відправлення некоректних або завеликих пакетів за допомогою команди Ping. У випадку атаки, коли система жертви обробляє ці пакети, виникає помилка, яка може призвести до збою системи [12].

Порівнюючи концепцію атаки "Ping of Death" (PoD) з поштовою бомбою, можна сказати, що відкриваючи пакунок, одержувач активує механізм, що призводить до атаки або повного виснаження системи [13].

Назва атаки походить від команди Ping, яка є популярним інструментом для перевірки доступності мережі. Ця команда використовує протокол ICMP, щоб надавати інформацію про стан мережі.

Для виконання атаки "Ping of Death" зловмисники створюють пакет ICMP, розмір якого перевищує допустимий. Цей пакет розділяється на менші частини, і коли приймач їх збирає, максимально допустимий розмір перевищується. Це веде до переповнення буфера пам'яті та, в результаті, до збою системи.

Щоб узагальнити, максимальний розмір пакета для IPv4 становить 65 535 байт, включаючи загальне корисне навантаження у 84 байти. Таким чином, для запуску атаки "Ping of Death", кіберзлочинці надсилають понад 110 тисяч пакетів

ping на пристрій жертви. Також важливо відзначити, що зловмисники можуть використовувати цю DoS-атаку через інші протоколи, такі як протокол UDP, обмін пакетами в Інтернеті (IPX) і протокол TCP.

Хоча атака "Ping of Death" може здатися простою та обмеженою за масштабом, не слід недооцінювати її потенційну небезпеку. Якщо група пристроїв об'єднається, існує велика ймовірність того, що вони можуть вивести з ладу веб-сайт, який не обладнаний відповідною інфраструктурою для протистояння цій загрозі. Ці приклади з минулого служать свідченням того, що атака "Ping of Death" все ще може становити загрозу. Тому важливо, щоб організації приймали необхідні заходи для свого захисту.

Щодо профілактичних заходів проти атаки "Ping of Death", існує кілька шляхів для запобігання, зупинення та захисту від цієї атаки, більшість з яких є легко реалізованими:

– налаштування брандмауера для блокування повідомлень ICMP Ping, хоча це може також призвести до блокування легітимних пінг-програм;

– моніторинг за допомогою ICMP Ping для виявлення проблем з мережею;

– впровадження захисту від DDoS для загальної безпеки мережі;

– регулярне оновлення програмного забезпечення для усунення виявлених недоліків;

– використання буфера переповнення для покращення здатності приймати великі пакети;

– фільтрація трафіку для заборони фрагментованим запитам ping досягати пристроїв в мережі;

– включення перевірки в процесі складання для зупинки ненормальних пакетів та запобігання збою.

1.2 Ознаки DDoS-атаки

Вчасне виявлення DDoS -атаки є головним параметром для мінімізації її впливу. Ознаки, які можуть вказувати на потенційну DDoS-атаку наступні:

– різке та суттєве збільшення мережевого трафіку, особливо якщо воно перевищує пропускну здатність мережі;

– раптове погіршення продуктивності, таке як повільний час відповіді або збільшення затримок, адже атака може виснажувати ресурси системи та впливати на її здатність обробляти легітимні запити;

– повна або періодична недоступність серверів чи служб може свідчити про перевантаження ресурсів, що призводить до збоїв у роботі;

– нетипові IP-адреси, які надсилають запит чи отримують відповідь у залежності від особливостей роботи інформаційної системи;

– нетипові протоколи чи типи трафіку, які спрямовані на мережу чи служби;

– збільшення кількості невдалих спроб автентифікації;

– нетипова поведінка пристроїв Інтернету речей, якщо вони підключені до мережі.

Важливо зауважити, що одна або кілька з цих ознак не обов'язково свідчать про DDoS-атаку.

Аналіз DDoS-атак вказує на те, що переважно при атаках використовуються протоколи TCP, UDP, ICMP та HTTP. Протокол UDP використовується при атаках типу UDP flood, атаках транспортного рівня, UDP SYN, UDP dump. TCP протоколи часто задіяні при TCP requests, TCP SYN, атаках транспортного рівня, TCP fragment, established, random flag floods, RST packet floods, PUSH, TCP dump. Задіюються протоколи ICMP для атак транспортного рівня, ICMP flood, smurf, ICMP dump. HTTP протоколи задіяні при атаках HTTP flood [14-15].

1.3 Підходи до виявлення DDoS-атак

Методи виявлення DDoS-атак можна розділити на три основні категорії: виявлення на основі сигнатур; виявлення аномалій; гібридне виявлення [16-17].

Кожна із вказаних категорій має свої переваги та недоліки, що описано нижче у підпунктах 1.3.1-1.3.3. Поділ існуючих методів виявлення атаки до тієї чи

іншої категорії показано на рисунку 1.1.

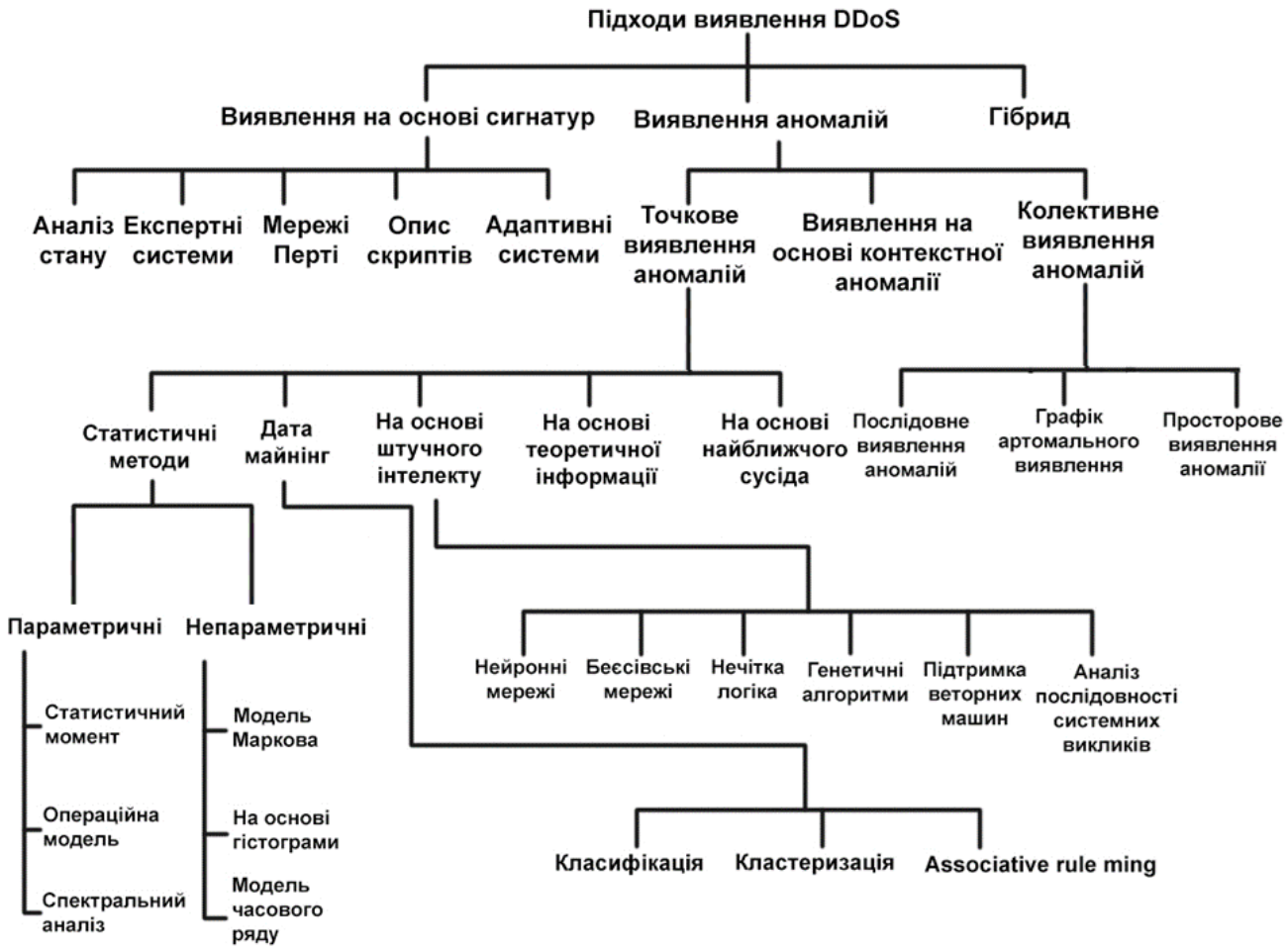


Рисунок 1.1 – Розподіл методів виявлення DDoS-атаки на категорії

Виявлення на основі сигнатур також відоме як виявлення зловживань, виявлення шаблонів, виявлення на основі знань або виявлення на основі правил. Цей підхід фіксує необхідну поведінку з наявного набору даних (наприклад, умови протоколу, генерація мережевого трафіку тощо) і збирає дані про різні атаки та вразливості системи. Отриманий досвід використовується для виявлення аномальних подій і генерації сповіщень у разі виявлення атаки. Цей підхід ефективний лише у випадку відомих атак; нові атаки та старі відомі атаки з незначними модифікаціями не виявляються, оскільки в базі даних немає сигнатур. Сигнатури або шаблони різних атак складаються з декількох полів в IP-пакеті (IP-адреси джерела і цілі, порти і ключові слова в корисному навантаженні пакета). Такі системи працюють занадто повільно і залежать від умов несправності (або

поведінки) системи-жертви; такі методи, як SNORT, BRO і IDES, засновані на підходах виявлення на основі сигнатур. В даний час цей підхід використовується лише мережевими адміністраторами. Дерева класифікації відокремлюють DDoS-трафік від звичайного трафіку, аналізуючи швидкість вхідних і вихідних пакетів, швидкість передачі і швидкість прапорців TCP, SYN і ACK. Алгоритми зіставлення шаблонів використовуються для виявлення потоків трафіку, ідентичних потокам атак, і для визначення місця розташування джерела атаки. Алгоритми аналізують TCP/IP-пакети відповідно до чітко визначених правилі умов, щоб відрізнити атаку від нормального трафіку [18]. Автори використовують швидкість передачі даних для розпізнавання атакуючого трафіку. Дослідження показує, що швидкість передачі атакуючого трафіку є вищою, ніж фактичний мережевий трафік. Це пов'язано з тим, що підлеглий агент, який отримує команди ведучого, генерує атакуючий трафік за дуже короткий час, тоді як звичайний трафік займає більше часу, оскільки він чекає на відповідь сервера. Такі методи не можливо ефективно виявити, оскільки зловмисники можуть легко використовувати флеш-події для надсилання жертві імітованого атакуючого трафіку. Для створення сигнатур атак використовуються різні методи, включаючи аналіз переходів стану, експертні системи, мережі Петрі, описові мови та адаптивні системи.

Підхід до виявлення аномалій, відомий також як виявлення новизни, виявлення викидів, схема на основі поведінки або однокласова схема навчання, є ефективним засобом виявлення невідомих та нових атак. Цей метод відображає стандартну поведінку мережі та порівнює її з екземплярами вхідних даних. Коли розбіжність між спостережуваною та очікуваною поведінкою перевищує попередньо визначений поріг, то система виявлення генерує сповіщення про аномалію, роблячи припущення щодо можливої атаки.

Схеми на основі аномалій, хоча і ефективні у виявленні нових загроз, проте можуть викликати багато помилкових спрацювань через різноманітність поведінки системи чи мережі та невизначеність в отриманих даних. Вхідні дані для цього підходу можуть бути подані у формі окремих екземплярів даних або у

вигляді набору екземплярів даних. Кожен вхідний екземпляр має свій набір атрибутів, які можуть бути дискретними, категоріальними або неперервними за своєю природою [19].

Багато схем виявлення аномалій спрямовані на обробку окремих екземплярів вхідних даних, де взаємозв'язку між ними може не бути. Залежно від природи аномалій, підходи до виявлення можуть бути класифіковані як точкова аномалія, контекстна аномалія та виявлення на основі колективної аномалії [20].

Особливу увагу слід приділяти виявленню колективних аномалій, яке вважається найскладнішим, оскільки воно вимагає аналізу взаємодії між різними елементами системи чи мережі. Такий підхід може значно підвищити ефективність виявлення, але в той же час викликати виклики у взаємодії різних методів та обробці великої кількості даних.

Гібридний підхід для виявлення DDoS-атак об'єднує різні стратегії виявлення, спрямовані на поліпшення можливостей моніторингу системи. Використання гібридної моделі передбачає аналіз як звичайної поведінки користувачів у системі, так і аномальної поведінки зловмисників. Цей підхід охоплює як відомі, так і раніше невідомі атаки, використовуючи як методи виявлення аномалій, так і ті, що базуються на сигнатурах.

Важливою особливістю гібридної моделі є поєднання переваг обох методів є виявлення аномалій і сигнатур, що призводить до високого рівня виявлення та низького рівня помилкових сигналів. В такому випадку система може виявити зловмисників, які намагаються змінити шаблони атак, що зберігаються в базі даних сигнатур [21].

Прикладом гібридного підходу є поєднання SNORT на основі сигнатур з методами на основі аномалій для розробки ефективної гібридної моделі виявлення в реальному часі. Іноді вихідні дані різних класифікаторів, таких як байєсовські мережі, нейронні мережі та дерева рішень, об'єднуються за допомогою різних методів для поліпшення результатів [22].

Хоча комбінація різних підходів робить систему виявлення ефективнішою, розробка гібридних систем може бути складною задачею через потребу в

правильній взаємодії різних методів. Незважаючи на те, що гібридні системи можуть значно підвищити ефективність виявлення, проте це не гарантує повне виявлення усіх загроз.

1.4 Постановка задачі

Сигнатурні методи виявляють атаку при наявності сигнатури цієї атаки у базі, але не виявляють атаки нульового дня. Методи виявлення аномалій базуються на типовій поведінці у мережі і все, що не є типовим, буде вважатися аномальним. Саме тому в мережах із низькою часткою самоподібного трафіку буде високий відсоток хибних спрацювань. Гібридні системи об’єднують попередні методи, проте їх розгортання потребує додаткових фінансових та часових затрат. Існуючі системи розраховані на корпоративні сегменти мережі та захищають мережу від зовнішнього впливу. Саме тому доцільно розробити систему, яка зможе виявляти не тільки атаку на мережу, а атаку із мережі.

Завданням даної роботи є розробка системи виявлення DDoS-атак, які запущені із мережі на сторонні ресурси, та в межах завдання потрібно: обрати оптимальний набір даних для тестування системи; розробити алгоритм реалізації системи; розробити схему включення в мережу; описати мінімальні технічні характеристики обладнання задля забезпечення роботоздатності системи; змоделювати тестове середовище та довести ефективність розробленої системи.

2.1 Вибір засобів для моделювання і реалізації системи виявлення

Нечітка логіка, також відома як нечітка теорія, представляє собою галузь математики, що розширює традиційну логіку та теорію множин. Запропонована вперше Лотфі Заде в 1965 році, вона вивчає об'єкти, які визначаються функцією належності до множини і приймають значення у діапазоні [0, 1], а не обмежені лише 0 або 1. Цей концепт використовується для введення логічних операцій для роботи з нечіткими множинами, а також висуває ідею лінгвістичної змінної, яка репрезентована нечіткими множинами [23-25]. Нечітка логіка призначена для наближення процесу прийняття рішень до того, як це робить людина. Системи, засновані на нечіткій логіці, виявили значний потенціал у вирішенні завдань, де інформація є розмитою та неточною. Застосовуються вони в різних програмах, починаючи від розпізнавання голосу і закінчуючи системами управління [26].

Теорія нечітких множин розширює класичну теорію множин. Вона відмовляється від строгого принципу дихотомії та дозволяє приналежність до множини розглядати як питання ступеня. Ця теорія стала популярною через свою кращу відповідність фізичному світу, де більшість знань є нечіткими та розмитими. Наприклад, поняття "хороший", "поганий", "високий" і "молодий" є нечіткими, тобто вони не мають чіткого визначення або меж. Візуальне відображення ще одного прикладу продемонстровано на рисунку 2.1 [27].

Основний об'єкт вивчення нечіткої логіки - це судження в умовах нечіткості, які подібні до тих, що використовуються в звичайних ситуаціях. Ця галузь також застосовується в обчислювальних системах для вирішення завдань, пов'язаних з нечіткістю та невизначеністю.

Застосовуючи нечітку логіку, можна створювати моделі систем підтримки прийняття рішень, які відображають основні вхідні дані, виходи та взаємозв'язки між ними.

Рисунок 2.1– Порівняння логічного та нечіткого рішень

Система нечіткого логічного висновку спрямована на надання підтримки у процесі прийняття рішень в конкретній сфері, де визначена основна логіка не є конкретною. У таких системах вхідні та вихідні параметри моделюються як нечіткі змінні, при цьому значення кожної з цих змінних виражається як нечітка функція належності. Правила для предметної області ідентифікуються та формалізуються, при цьому в кожному нечіткому правилі використовуються відповідні нечіткі змінні та їхні значення, що відображають основні принципи предметної області [28-29].

Зазначено, що нечітка змінна ідентична нечіткому числу, але з додаванням імені, що формалізує концепцію, описану цим числом. З людської точки зору, більш зручно виражати значення змінної словами, а не числами. Щодня ми приймаємо рішення, використовуючи лінгвістичну інформацію, таку як "дуже висока температура", "швидка відповідь", "красивий букет" і таке інше. Вивчено, що в людському мозку практично вся числова інформація перекодується вербально і зберігається у вигляді слів.

Ключовим концептом у нечіткій логіці є лінгвістичні змінні, які дозволяють машинам розуміти людську мову та робити висновки на основі нечітких та неточних висловлень.

Лінгвістична змінна представляє собою множину нечітких змінних та використовується для надання словесного опису деякому нечіткому числу, яке отримане в результаті виконання певних операцій [30-31].

Визначення лінгвістичної змінної включає параметри <x, L, U, G, M>, де x – назва змінної, L – множина її значень (базова терм-множина), що складається з

назв нечітких змінних, область визначення кожної з яких є множина U; G – синтаксична процедура (граматика), яка дозволяє операції з елементами терм-множини L, зокрема генерувати нові осмислені терми; L'=LÈG(L) визначає розширену терм-множину (È – об'єднання); M – семантична процедура, що дозволяє призначати кожному новому значенню лінгвістичної змінної нечітку семантику шляхом формування нової нечіткої множини.

Терм-множина є множиною всіх можливих значень лінгвістичної змінної, а терм - будь-яким елементом терм-множини. У теорії нечітких множин терм формалізується через нечітку множину за допомогою функції приналежності [32-34].

Використання нечітких множин та лінгвістичних змінних дозволяє краще моделювати людські знання. Таким чином працюють системи нечіткого висновку. Враховуючи вхідні та вихідні дані, система нечіткого логічного висновку формулює відображення, використовуючи набір нечітких правил (де нечіткі правила мають вигляд: "Якщо A, то B", де A і B - нечіткі множини).

Це відображення дозволяє системі приймати майбутні рішення та прозоро визначати закономірності.

Процес моделювання таких систем включає такі етапи (рисунок 2.2):

– фазифікація вхідних даних;
– використання нечітких операторів для антецедентів нечітких правил;
– здійснення імплікації від антецедентів до наслідків нечітких правил;
– агрегація наслідків нечітких правил;
– дефазифікація для визначення кінцевого результату.

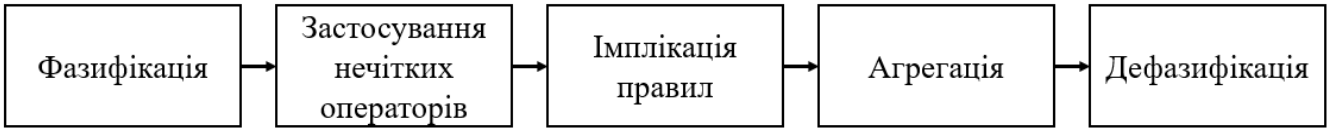


Рисунок 2.2– Етапи побудови нечіткого висновку

Існують, в основному, дві групи систем нечіткого висновку: Mamdani та

Sugeno. Вони відрізняються основним чином у структурі своїх нечітких правил. У системи нечіткого висновку Mamdani, послідовною частиною є нечітка множина. Навпаки, для системи нечіткого висновку Sugeno, наслідком є математична функція. Це призводить до того, що Sugeno може мати більшу прогностичну силу, тоді як Mamdani має більше можливостей для інтерпретації результатів. Такий підхід визначається відмінною природою їхніх відповідних вихідних параметрів: нечіткою множиною в разі Mamdani та математичною функцією в разі Sugeno.

Переваги системи нечіткої логіки:

– система може ефективно обробляти різноманітні типи вхідних даних, включаючи неточну або спотворену інформацію;

– побудова систем нечіткої логіки є простою і зрозумілою, що полегшує їхню реалізацію;

– нечітка логіка базується на математичних концепціях теорії множин, а її аргументація є достатньо простою;

– надає ефективні рішення для складних завдань у різних сферах життя, оскільки відображає людське мислення та процеси прийняття рішень;

– алгоритми можуть бути описані з використанням обмеженої кількості даних, що вимагає мало пам'яті.

Для оцінки ефективності архітектури виявлення атак DDoS рекомендується використовувати точний набір даних, який адекватно відображає подібні атаки. У цьому контексті важливо використовувати загальнодоступний набір даних CICDDoS 2019, створений Канадським інститутом кібербезпеки (CIC) при Університеті Нью-Брансвіка (UNB). Зазначений набір даних містить мітки, що робить його ідеальним джерелом інформації для виявлення атак DDoS. Набір даних CICDDoS2019 містить 50063112 записів, у тому числі 56863 рядки для безпечного трафіку та 50006249 для DDoS-атак [35]. Також важливо відзначити, що цей набір даних демонструє значну схожість із реальними атаками, що підсилює його значущість. Таксономія атак у цьому наборі даних визначається з точки зору експлуатації та атак на основі відображення. Збір даних відбувався протягом двох окремих днів для тренування та тестування. Тренувальний набір,

зібраний 12 січня 2019 року, містить 12 різних типів DDoS-атак, кожен представлений окремим файлом PCAP. Атаки на навчальний день включають UDP, SNMP, NetBIOS, LDAP, TFTP, NTP, SYN, DDoS-атаку на основі WebDDoS, MSSQL, UDP-Lag, DNS і SSDP. Дані для тестування були зібрані 11 березня 2019 року і включають 7 DDoS-атак: SYN, MSSQL, UDP-Lag, LDAP, UDP, PortScan і NetBIOS. Детальну класифікацію атак у наборі даних відображено у таблиці 2.1. Зокрема, він включає 80 атрибутів пакетів мережевого трафіку.

Таблиця 2.1 - Класифікація атак у наборі даних CICDDoS2019

Клас	Кількість потоків
DDoS_NetBIOS	4 093 279
DDoS_SNMP	5 159 870
DDoS_NTP	1 202 642
DDoS_TFTP	20 082 580
DDoS_SSDP	2 610 611
DDoS_SYN	1 582 289
DDoS_UDP-Lag	366 461
DDoS_DNS	5 071 011
DDoS_MSSQL	4 522 492
DDoS_LDAP	2 179 930
DDoS_UDP	3 134 645
DDoS_WebDDoS	439

DDoS-атаки використовують вірусні сервери, такі як DNS, LDAP, NETBIOS і SNMP, які забезпечують різноманітні мережеві сервіси. Такі атаки, як WebDDoS, SYN-флуд, UDP-флуд і UDPLag, спираються на вразливості протоколів TCP і UDP. Набір даних CICDoS2019 виявився корисним для навчання моделі, піддаючи йому попередню обробку, включаючи вилучення сторонніх атрибутів.

Перелік функцій набору даних CIC-DDOS2019 висвітлено у таблиці 2.2.

Таблиця 2.2 - Перелік функцій набору даних CIC-DDOS2019

Назви наборів функцій	Список функцій
Надіслані пакети Зворотні пакети На основі часу На основі потоку На основі заголовка пакета На основі корисного навантаження пакетів	Protocol,Flow Duration,Total Fwd Packets,Total Backward Packets,Fwd Packets Length Total,Bwd Packets Length Total,Fwd Packet Length Max,Fwd Packet Length Min,Fwd Packet Length Mean,Fwd Packet Length Std,Bwd Packet Length Max,Bwd Packet Length Min,Bwd Packet Length Mean,Bwd Packet Length Std,Flow Bytes/s,Flow Packets/s,Flow IAT Mean,Flow IAT Std,Flow IAT Max,Flow IAT Min,Fwd IAT Total,Fwd IAT Mean,Fwd IAT Std,Fwd IAT Max,Fwd IAT Min,Bwd IAT Total,Bwd IAT Mean,Bwd IAT Std,Bwd IAT Max,Bwd IAT Min,Fwd PSH Flags,Bwd PSH Flags,Fwd URG Flags,Bwd URG Flags,Fwd Header Length,Bwd Header Length,Fwd Packets/s,Bwd Packets/s,Packet Length Min,Packet Length Max,Packet Length Mean,Packet Length Std,Packet Length Variance,FIN Flag Count,SYN Flag Count,RST Flag Count,PSH Flag Count,ACK Flag Count,URG Flag Count,CWE Flag Count,ECE Flag Count,Down/Up Ratio,Avg Packet Size,Avg Fwd Segment Size,Avg Bwd Segment Size,Fwd Avg Bytes/Bulk,Fwd Avg Packets/Bulk,Fwd Avg Bulk Rate,Bwd Avg Bytes/Bulk,Bwd Avg Packets/Bulk,Bwd Avg Bulk Rate,Subflow Fwd Packets,Subflow Fwd Bytes,Subflow Bwd Packets,Subflow Bwd Bytes,Init Fwd Win Bytes,Init Bwd Win Bytes,Fwd Act Data Packets,Fwd Seg Size Min,Active Mean,Active Std,Active Max,Active Min,Idle Mean,Idle Std,Idle Max,Idle Min,Label,Class

Опис кожної із перелічених функцій знаходиться в таблиці 2.3.

Таблиця 2.3 - Функції CICDDoS2019

Назва функції	Опис
1	2
Flow Duration	Тривалість потоку
Total Fwd Packet	Загальна кількість пакетів у прямому напрямку
Total Bwd packets	Загальна кількість пакетів у зворотному напрямку
Total Length of Fwd Packet	Загальний розмір пакетів у прямому напрямку
Fwd Packet Length Max	Максимальний розмір пакетів у прямому напрямку
Fwd Packet Length Min	Мінімальний розмір пакетів у прямому напрямку
Fwd Packet Length Mean	Середній розмір пакетів у прямому напрямку
Fwd Packet Length Std	Розмір стандартного відхилення пакетів у прямому напрямку
Bwd Packet Length Max	Максимальний розмір пакетів у зворотному напрямку
Bwd Packet Length Min	Мінімальний розмір пакетів у зворотному напрямку
Bwd Packet Length Mean	Середній розмір пакетів у зворотному напрямку
Bwd Packet Length Std	Стандартне відхилення розміру пакетів у зворотному напрямку
Flow Bytes/s	Швидкість потоку в байтах, тобто кількість пакетів, що передаються за секунду
Flow Packets/s	Швидкість потоку пакетів, тобто кількість пакетів, переданих за секунду
Flow IAT Mean	Середній час між двома потоками
Flow IAT Std	Стандартне відхилення часу двох потоків
Flow IAT Max	Максимальний час між двома потоками
Flow IAT Min	Мінімальний час між двома потоками
Fwd IAT Total	Загальний час між двома пакетами, надісланими в прямому напрямку

Продовження таблиці 2.3

1	2
Fwd IAT Mean	Середній час між двома пакетами, надісланими в прямому напрямку
Fwd IAT Std	Час стандартного відхилення між двома пакетами, надісланими в прямому напрямку
Fwd IAT Max	Максимальний час між двома пакетами, надісланими в прямому напрямку
Fwd IAT Min	Мінімальний час між двома пакетами, надісланими в прямому напрямку
Bwd IAT Total	Загальний час між двома пакетами, надісланими у зворотному напрямку
Bwd IAT Mean	Середній час між двома пакетами, надісланими у зворотному напрямку
Bwd IAT Std	Час стандартного відхилення між двома пакетами, надісланими у зворотному напрямку
Bwd IAT Max	Максимальний час між двома пакетами, надісланими у зворотному напрямку
Bwd IAT Min	Мінімальний час між двома пакетами, надісланими у зворотному напрямку
Fwd PSH Flags	Кількість разів, коли PSH прапор було встановлено в пакетах, що рухаються в прямому напрямку (0 для UDP)
Bwd PSH Flags	Кількість разів, коли PSH прапор було встановлено в пакетах, що рухаються у зворотному напрямку (0 для UDP)
Fwd URG Flags	Кількість разів, коли URG прапор було встановлено в пакетах, що рухаються в прямому напрямку (0 для UDP)

Продовження таблиці 2.3

1	2
Bwd URG Flags	Кількість разів, коли URG прапор було встановлено в пакетах, що рухаються у зворотному напрямку (0 для UDP)
Fwd Header Length	Загальна кількість байтів, використаних для заголовків у прямому напрямку
Bwd Header Length	Загальна кількість байтів, використаних для заголовків у прямому напрямку
Fwd Packets/s	Кількість пакетів, що пересилаються за секунду
Bwd Packets/s	Кількість зворотних пакетів за секунду
Packet Length Min	Мінімальна довжина потоку
Packet Length Max	Максимальна довжина потоку
Packet Length Mean	Середня довжина потоку
Packet Length Std	Стандартне відхилення довжини потоку
Packet Length Variance	Мінімальний час між надходженнями пакета
FIN Flag Count	Кількість пакетів з FIN
SYN Flag Count	Кількість пакетів із SYN
RST Flag Count	Кількість пакетів з RST
PSH Flag Count	Кількість пакетів з PUSH
ACK Flag Count	Кількість пакетів з ACK
URG Flag Count	Кількість пакетів з URG
CWE Flag Count	Кількість пакетів з CWE
ECE Flag Count	Кількість пакетів з ECE
Down/Up Ratio	Співвідношення завантаження та відвантаження
Average Packet Size	Середній розмір пакетів
Fwd Segment Size Avg	Середній розмір спостерігається в напрямку вперед
Bwd Segment Size Avg	Середній розмір спостерігається в зворотному напрямку

Продовження таблиці 2.3

1	2
Fwd Bytes/Bulk Avg	Середня кількість байтів масової швидкості в прямому напрямку
Fwd Packet/Bulk Avg	Середня кількість пакетів масової швидкості в прямому напрямку
Fwd Bulk Rate Avg	Середня кількість об'ємної швидкості в прямому напрямку
Bwd Bytes/Bulk Avg	Середня кількість байтів у зворотному напрямку
Bwd Packet/Bulk Avg	Середня кількість пакетів у зворотному напрямку
Bwd Bulk Rate Avg	Середнє число об'ємної швидкості в зворотному напрямку
Subow Fwd Packets	Середня кількість пакетів у підрядці в прямому напрямку
Subow Fwd Bytes	Середня кількість байтів у підрядці в прямому напрямку
Subow Bwd Packets	Середня кількість пакетів у підрядці у зворотному напрямку
Subow Bwd Bytes	Середня кількість байтів у підрядці у зворотному напрямку
FWD Init Win Bytes	Кількість байтів, надісланих у початковому вікні в прямому напрямку
Bwd Init Win Bytes	Кількість байтів, надісланих у початковому вікні у зворотному напрямку
Fwd Act Data Pkts	Кількість пакетів із принаймні 1 байтом корисних даних TCP у прямому напрямку
Fwd Seg Size Min	Мінімальний розмір сегмента в прямому напрямку
Active Mean	Середній час, коли потік був активним, перш ніж стати неактивним

Кінець таблиці 2.3

1	2
Active Std	Час стандартного відхилення, протягом якого потік був активним, перш ніж стати неактивним
Active Max	Максимальний час, протягом якого потік був активним, перш ніж перейти в режим простою
Active Min	Мінімальний час, протягом якого потік був активним, перш ніж стати неактивним
Idle Mean	Середній час потік був неактивним, перш ніж стати активним
Idle Std	Час стандартного відхилення, коли потік був неактивний, перш ніж стати активним
Idle Max	Максимальний час, коли потік був неактивний, перш ніж стати активним
Idle Min	Мінімальний час, коли потік був неактивний, перш ніж стати активним

Фрагмент набору даних CIC-DDOS2019 у форматі csv показано на рисунку 2.3.

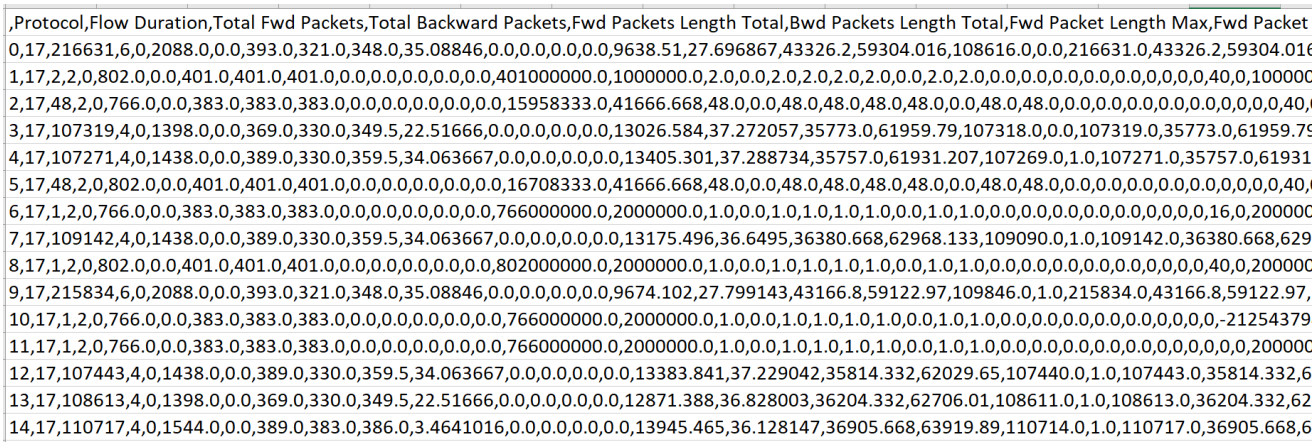


Рисунок 2.3 - Фрагмент набору даних CIC-DDOS2019

На етапі попередньої обробки даних виконуються різні операції, такі як

кодування ознак, виявлення викидів, усунення дублікатів, балансування даних та нормалізація. Важливо розділити набір даних на навчальний та тестовий набори у відповідності до співвідношення 70% і 30% для ефективного навчання та прогнозування моделі.

2.2 Алгоритм реалізації системи виявлення DDoS-атаки

На рисунку 2.4 зображено комп'ютерну мережу, де кінцевими пристроями можуть виступати смартфони, ноутбуки, IoT-пристрої, SMART-TV, персональні комп'ютери, сервери та інші пристрої. У якості комутуючих пристроїв можуть бути Wi-Fi точки доступу, роутери, комутатори та маршрутизатори. Задля безпеки сервери знаходяться у демілітаризованій зоні, а на вході мережі функціонує фаєрвол чи може бути розгорнуто систему виявлення вторгнень.

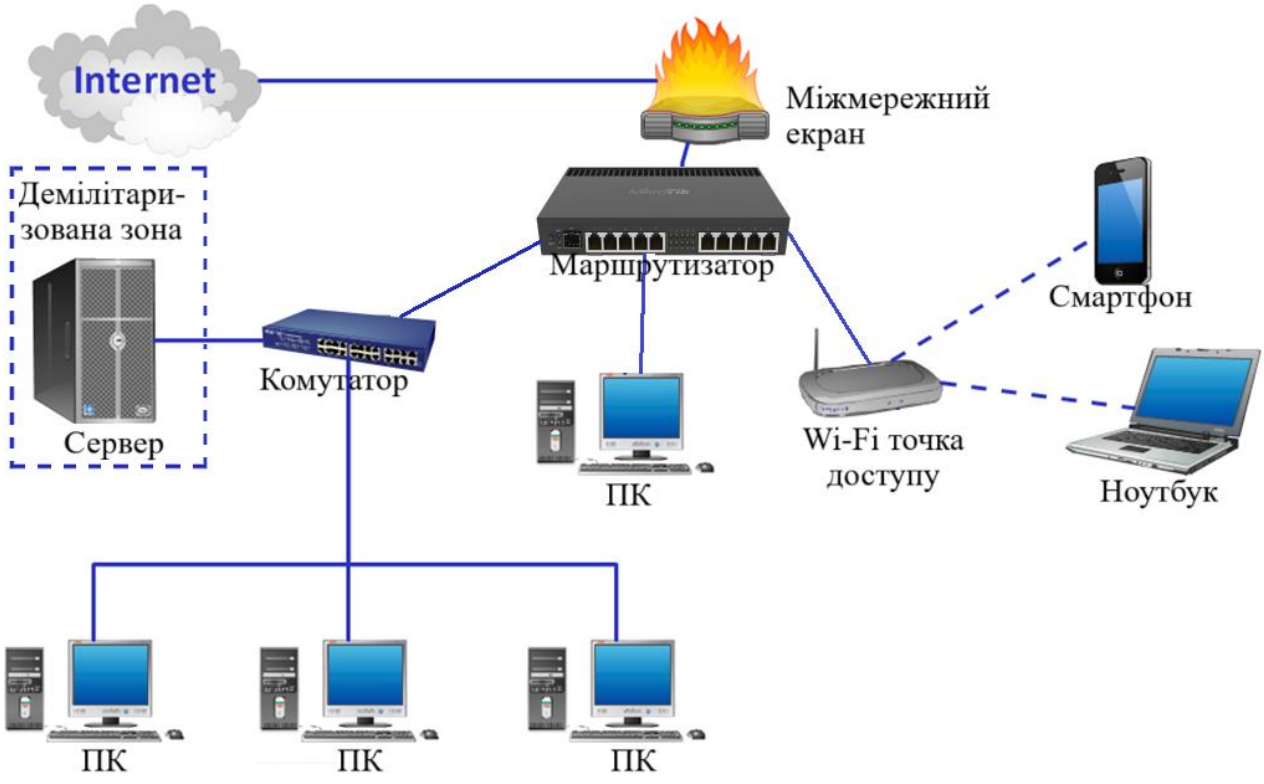


Рисунок 2.4 – Типова схема комп'ютерної мережі

Слід зазначити, що існуючі засоби захисту лише можуть виконувати функції

захисту мережі від сторонніх зловмисних дій. Якщо ж зловмисні дії ідуть в середині мережі з одних пристроїв на інші або виходять із мережі, то такі дії можуть лише фіксуватися як і нормальний мережевий трафік. Саме тому доцільно на центральному комутуючому пристрої реалізувати систему виявлення зловмисних дій, які надходять від кінцевих користувачів. У даній роботі буде реалізовано систему виявлення DDoS-атак, які запущені із мережі на сторонні ресурси.

Оскільки функцій у наборі даних досить велика кількість, то аналіз трафіку за всім набором спричинить пікове навантаження в роботі мережевого обладнання. Саме тому за допомогою методу експертних оцінок було обрано 9 найоптимальніших параметри (таблиця 2.4): Flow Duration, Fwd Packet Length Mean, Fwd Packet Length Std, Bwd Packet Length Mean, Bwd Packet Length Std, Flow IAT Mean, Flow IAT Std, Fwd Packets/s, Bwd Packets/s.

Flow Duration може приймати одне із п’яти значень: L – низьке; BA – нижче середнього; A – середнє; AA – вище середнього; H – високе.

Fwd Packet Length Mean: L – низьке; BA – нижче середнього; A – середнє; AA – вище середнього; H – високе.

Fwd Packet Length Std: L – низьке; BA – нижче середнього; A – середнє; AA – вище середнього; H – високе.

Bwd Packet Length Mean може приймати одне із п’яти значень: L – низьке; BA – нижче середнього; A – середнє; AA – вище середнього; H – високе.

Bwd Packet Length Std може приймати одне із п’яти значень: L – низьке; BA – нижче середнього; A – середнє; AA – вище середнього; H – високе.

Flow IAT Mean може приймати одне із п’яти значень: L – низьке; BA – нижче середнього; A – середнє; AA – вище середнього; H – високе.

Flow IAT Std може приймати одне із п’яти значень: L – низьке; BA – нижче середнього; A – середнє; AA – вище середнього; H – високе.

Fwd Packets/s може приймати одне із п’яти значень: L – низьке; BA – нижче середнього; A – середнє; AA – вище середнього; H – високе.

Bwd Packets/s може приймати одне із п’яти значень:

L – низьке;

ВА – нижче середнього;

А – середнє;

АА – вище середнього;

Н – високе.

Таблиця 2.4 – Параметри набору даних, які буде застосовано

Назва параметру	Скорочення
Flow Duration	FD
Fwd Packet Length Mean	FPLM
Fwd Packet Length Std	FPLS
Bwd Packet Length Mean	BPLM
Bwd Packet Length Std	BPLS
Flow IAT Mean	FIM
Flow IAT Std	FIS
Fwd Packets/s	FP
Bwd Packets/s	BP

На основі цих даних буде формуватися кортеж даних про потік:

<FD, FPLM, FPLS, BPLM, BPLS, FIM, FIS, FP, BP> (2.1)

Мережевий трафік можна розділити на три типи: G – нормальний трафік, M – зловмисний трафік.

Наступним кроком слід сформувати набір правил для моделювання у Matlab, які будуть при аналізі трафіку визначати DDoS-атаку.

Для критерію наведено графік, що відображає область визначення лінгвістичних означень (рисунок 2.5):

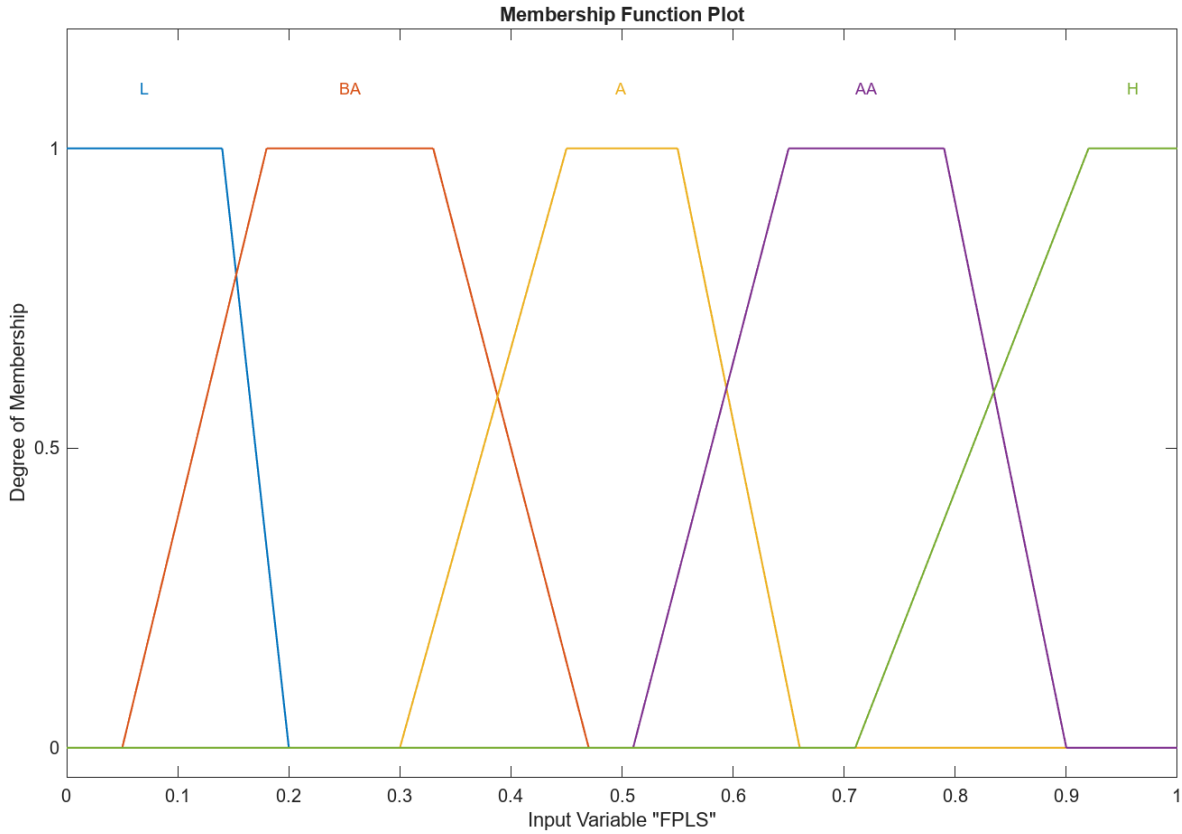


Рисунок 2.5 – Області належності змінної FPLS

Налаштування лінгвістичних означень для критерію FPLS показано на рисунку 2.6.

PROPERTY EDITOR: INPUT

Name: FPLS

Range: [0 1]

Number of MFs: 5

Evenly Distribute MFs

Name	Type	Parameters
L	Trapezoidal	[0 0 0.14 0.2]
BA	Trapezoidal	[0.05 0.18 0.33 0.47]
A	Trapezoidal	[0.3 0.45 0.55 0.66]
AA	Trapezoidal	[0.51 0.65 0.79 0.9]
H	Trapezoidal	[0.71 0.92 1 1]

Рисунок 2.6 - Налаштування лінгвістичних означень для критерію FPLS

Тоді множину лінгвістичних означень можна сформувати та подати як у таблиці 2.5.

Таблиця 2.5 – Сформовані лінгвістичні означення

Критерій	Множина можливих оцінок	Фазифікована медіанна оцінка
1	2	3
FD	FD = {L = низька тривалість потоку, BA = тривалість потоку нижча середнього, A = середня тривалість потоку, AA = тривалість потоку вища середнього, H = висока тривалість потоку}	FD = {L=0.1, BA=0.245, A=0.495, AA=0.745, H=0,885}
FPLM	FPLM = {L = низьке значення середнього розміру пакетів у прямому напрямку, BA = значення нижче середнього розміру пакетів у прямому напрямку, A = середнє значення середнього розміру пакетів у прямому напрямку, AA = вище середнього значення середнього розміру пакетів у прямому напрямку, H = високе значення середнього розміру пакетів у прямому напрямку }	FPLM = {L=0.21, BA= 0.22, A=0.49, AA=0.74 , H=0.9}
FPLS	FPLS = {L = низьке значення стандартного відхилення пакетів у прямому напрямку, BA = значення стандартного відхилення пакетів у прямому напрямку нижче середнього, A = значення стандартного відхилення пакетів у прямому напрямку середнє, AA = значення стандартного відхилення пакетів у прямому напрямку вище середнього, H = значення стандартного відхилення пакетів у прямому напрямку високе}	FPLS = {L=0.17, BA=0.25 , A=0.49, AA=0.71 , H=0.9}

Продовження таблиці 2.5

1	2	3
BPLM	BPLM = {L = низьке значення середнього розміру пакетів у зворотному напрямку, BA = значення середнього розміру пакетів у зворотному напрямку нижче середнього, A = середнє значення середнього розміру пакетів у зворотному напрямку, AA = значення середнього розміру пакетів у зворотному напрямку вище середнього, H = значення середнього розміру пакетів у зворотному напрямку високе}	BPLM = {L=0.135, BA=0.23, A=0.5, AA=0.72, H=0.91}
BPLS	BPLS = {L = низьке значення стандартного відхилення пакетів у зворотному напрямку, BA = значення стандартного відхилення пакетів у зворотному напрямку нижче середнього, A = середнє значення стандартного відхилення пакетів у зворотному напрямку, AA = значення стандартного відхилення пакетів у зворотному напрямку вище середнього, H = високе значення стандартного відхилення пакетів у зворотному напрямку }	BPLS = {L=0.07, BA=0.26, A=0.48, AA=0.75, H=0.92}
FIM	FIM = {L = низький середній час між двома потоками, BA = середній час між двома потоками нижче середнього, A = середній час між двома потоками середній, AA = середній час між двома потоками вище середнього, H = середній час між двома потоками високий}	FIM = {L=0.2, BA=0.31, A=0.56, AA= 0.79, H=0.94}

Продовження таблиці 2.5

1	2	3
FIS	FIS = {L = низьке значення стандартного відхилення часу двох потоків, BA = значення стандартного відхилення часу двох потоків нижче середнього, A = середнє значення стандартного відхилення часу двох потоків, AA = значення стандартного відхилення часу двох потоків вище середнього, H = значення стандартного відхилення часу двох потоків високе}	FIS = {L=0.13, BA=0.24, A=0.48, AA=0,74, H=0.93}
FP	FP = {L = низька кількість пакетів що пересилаються за секунду, BA = кількість пакетів що пересилаються за секунду нижча середньої, A = середня кількість пакетів що пересилаються за секунду, AA = кількість пакетів що пересилаються за секунду вища середнього, H = кількість пакетів, що пересилаються за секунду висока}	FP = {L=0.19, BA=0.3, A=0.54, AA=0.78, H=0.94}
BP	BP = {L = низька кількість зворотних пакетів за секунду, BA = кількість зворотних пакетів за секунду нижча середньої, A = середня кількість зворотних пакетів за секунду, AA = кількість зворотних пакетів за секунду вища середньої, H = висока кількість зворотних пакетів за секунду}	BP = {L=0.1, BA=0.18, A=0.43, AA=0.71, H=0.92}

Структуру системи нечіткого логічного висновку для класифікації ознак засобами Matlab відображено на рисунку 2.7.

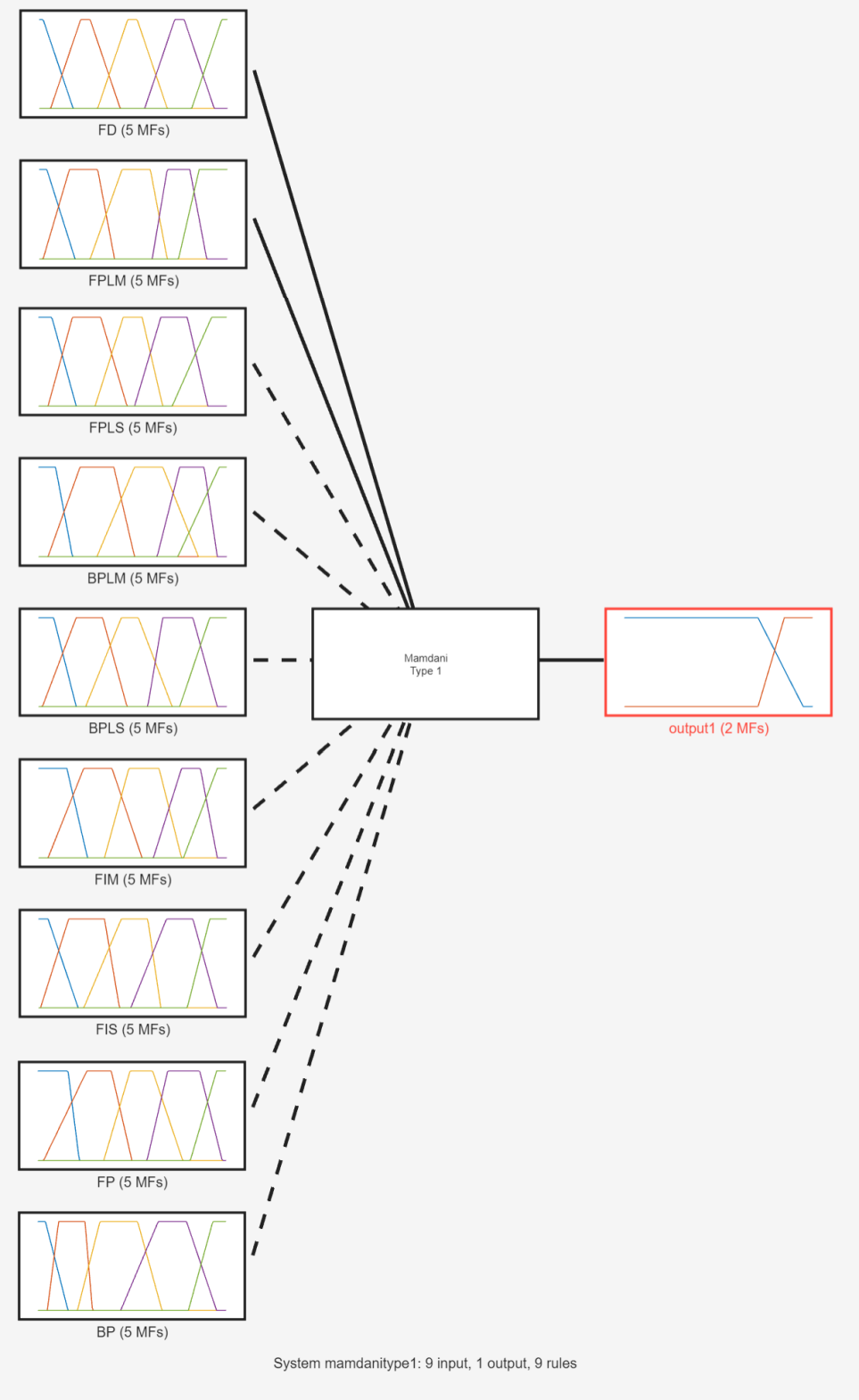


Рисунок 2.7 – Структура системи нечіткого логічного висновку

Добавлення та налаштування правил у середовищі моделювання Matlab показано на рисунку 2.8. Переглянути результат можна за допомогою візуалізації, як показано на рисунку 2.9.

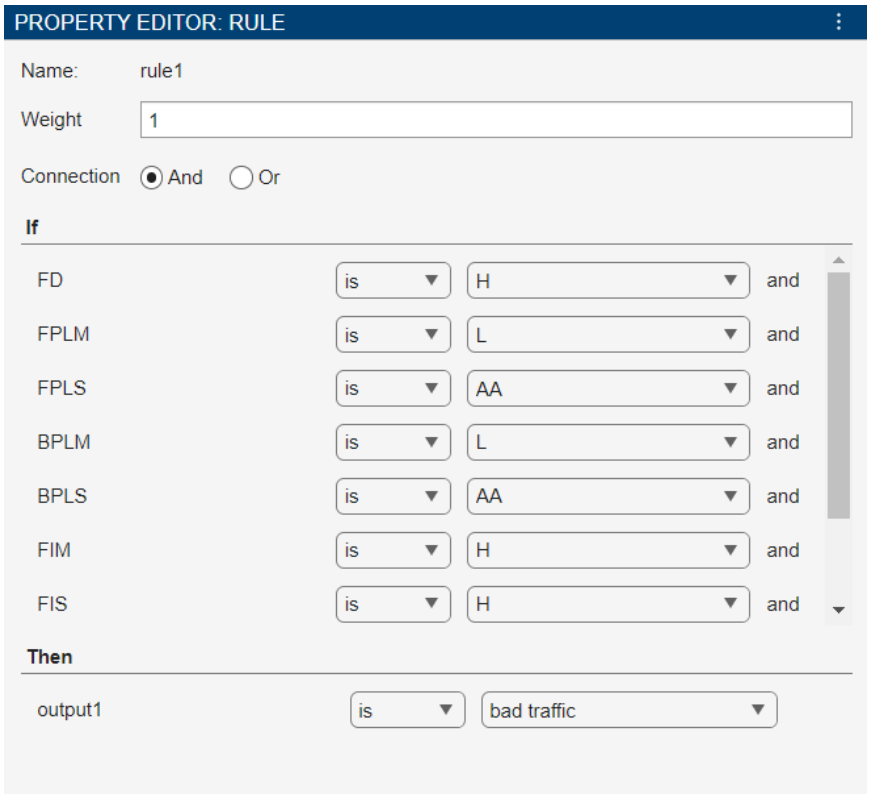


Рисунок 2.8 – База знань

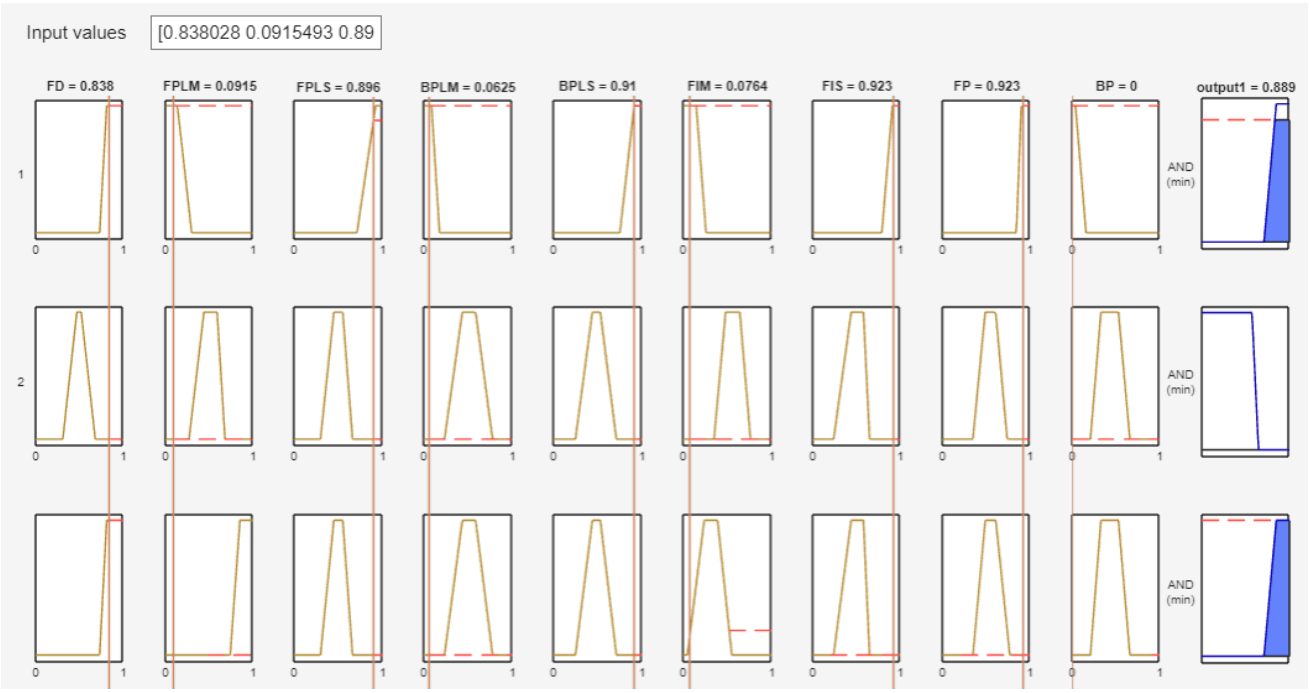


Рисунок 2.9 - . Візуалізація нечіткого висновку

Для того, щоб користувачі не відчували часових затримок і мережеве обладнання не працювало у пікових режимах, слід вихідний трафік дублювати на систему виявлення (для аналізу) та на зовні у Інтернет (безпосередньо для роботи).

Саме тому алгоритм роботи системи виявлення DDoS-атак (рис.2.10) буде розглядатися окремо від роботи усієї комп'ютерної мережі.

Послідовність перевірки потоку буде наступною.

Етап 1. Перевірка потоку даних на самоподібність.

Етап 2. Якщо потік самоподібний, то користувача можна вважати нормальним та дозволяти з'єднання. Якщо потік не самоподібний, то перехід до етапу 3.

Етап 3. Надходження потоку даних із мережі до системи виявлення DDoS-атак.

Етап 4. Формування кортежу потрібних даних із потоку.

Етап 5. Перевірка кортежу із набором заборонених правил.

Етап 6. Якщо сформований кортеж відповідає забороненим правилам, то користувача потрібно заблокувати.

Етап 7. Якщо сформований кортеж не відповідає забороненим правилам, то користувача можна вважати нормальним.

Рисунок 2.10 - Алгоритм роботи системи виявлення DDoS-атак

Розглянемо більш детально п’ятий етап (рисунок 2.11).

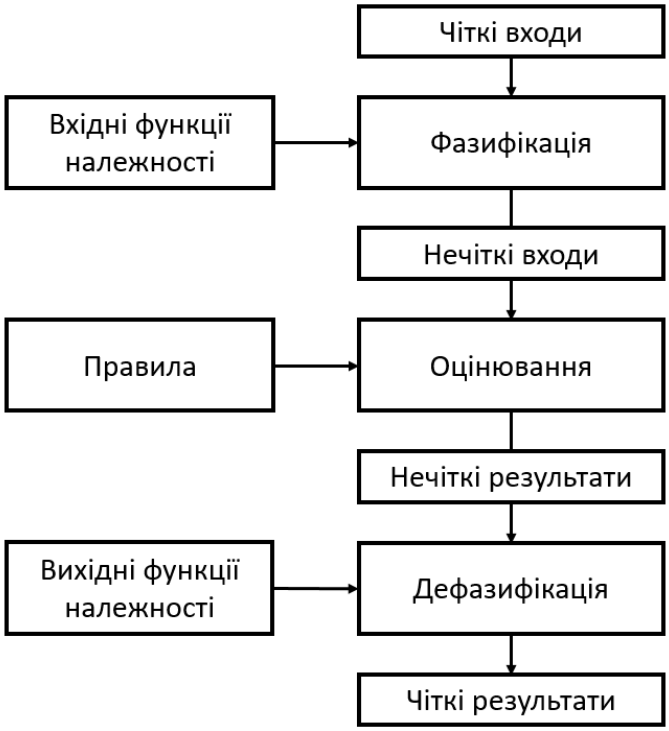


Рисунок 2.11 - Перевірка кортежу із набором заборонених правил

Спочатку у якості чітких входів подається сформований кортеж, який не відповідає вимогам самоподібності.

На етапі фазифікації проводиться перетворення вхідних чітких значень в нечіткі множини. Цей процес полягає в тому, що вхідні значення, які можуть бути конкретними або чіткими, перетворюються в нечіткі множини з числовими значеннями належності, що є одним і головних етапів у застосуванні нечіткої логіки для моделювання реальних систем і прийняття рішень. До прикладу, у даній роботі значенню кількості зворотних пакетів за секунду (BP) визначається приналежність до однієї із наявних множин: «низька» (L), «нижче середнього» (BA), «середня» (A), «вища середнього» (AA), «висока» (H). В параграфі 2.2.2 описано всі параметри та їх множини.

На етапі застосування нечітких операторів використовуються різні логічні операції для обробки нечітких значень і правил. Основні нечіткі оператори включають в себе операції кон'юнкції (AND), диз'юнкції (OR) та виключення

(NOT), які використовуються для обробки нечітких умовних правил. До прикладу, якщо тривалість потоку (FD) має належність 0,9 до множини «висока» (H) і середній розмір пакетів у прямому напрямку (FPLM) має належність 0,2 до множини «низьке» (L), то буде застосовано AND.

Оцінювання використовується для визначення ступеня належності вихідного значення на основі ступеня належності вхідних значень і правил. Основна операція імплікації визначає ступінь відповідності правила, якщо виконується певна умова. Перед застосуванням методу імплікації необхідно приділити увагу визначенню ваги правила. Кожне правило може мати свою вагу, що визначається числом від 0 до 1 та враховується при обчисленні відповідності правила. Будемо вважати, що вага кожного правила дорівнює 1 і, таким чином, не впливатиме на процес імплікації. У якості методу імплікації виберемо prod, яка масштабуватиме вихідний нечіткий набір.

Нечіткі результати буде отримано в результаті агрегації. Цей процес відбувається один раз для кожної вихідної змінної перед останнім кроком дефазифікації. У вхідних даних процесу агрегації є список відсічених вихідних функцій, які повертає процес імплікації для кожного правила. Результатом процесу агрегації є єдиний нечіткий набір для кожної вихідної змінної.

Дефазифікація - це процес перетворення нечіткого висновку, отриманого після агрегації, в чітке число, що відповідає конкретному рішенню. Цей процес важливий для того, щоб мати чітке числове значення, яке можна використовувати для подальшого керування або прийняття рішень. Саме тут рішення про нормальний чи заборонений трафік буде приймати числове значення з подальшим використанням для блокування користувача чи надання йому дозволу на подальше з’єднання.

2.3 Розробка схеми мережі

Для того, щоб була змога відслідковувати вихідний трафік всіх користувачів мережі, який виходить на зовні із мережі, найдоцільніше розташувати систему

виявлення DDoS-атак у вихідній точці всього трафіку із мережі. Такою точкою є центральний комутуючий вузол. Ним може бути маршрутизатор чи керований комутатор якщо мова йде про мережу середнього чи великого розміру. Якщо ж розглядати домашню мережу, то центральним вузлом може бути, до прикладу, роутер. На рисунку 2.12 показано оптимальне розміщення системи виявлення DDoS-атак.

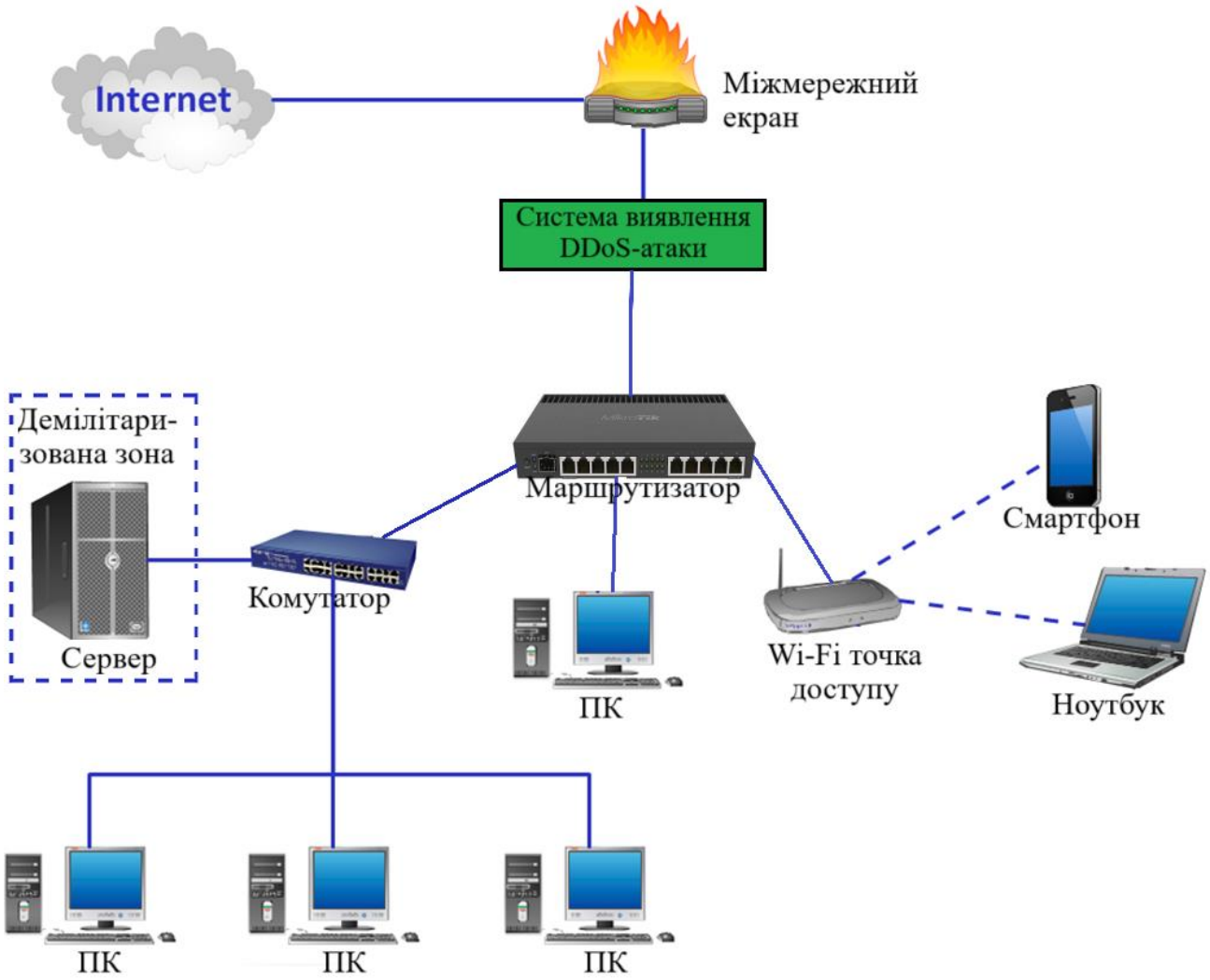


Рисунок 2.12 - Розміщення системи виявлення DDoS-атак

2.4 Висновки до розділу

У даному розділі значну увагу приділено вибору засобу для моделювання системи виявлення DDoS-атаки. Зокрема описано приклади та особливості

застосування нечіткої логіки для прийняття рішення. Оскільки основним об’єктом дослідження нечіткої логіки є це формулювання висновків у умовах нечіткості, що схожі на ті, які використовуються в звичайних ситуаціях та досить часто використовується в комп'ютерних системах для вирішення завдань, пов'язаних з нечіткістю та невизначеністю.

Також описано набір даних CICDDoS 2019, що буде використано для оцінки ефективності виявлення DDoS-атак: класифікація атак, перелік функцій набору даних та їх опис.

У параграфі 2.2.1 описано типову схему комп’ютерної мережі із її візуальною демонстрацією.

В параграфі 2.2.2 здійснюється моделювання системи, а саме виконано наступне:

- проведено оптимізацію параметрів із набору даних;
- описано всі параметри та налаштовано лінгвістичні означення відповідно до заданих множин;
- добавлено та налаштовано правила у середовищі моделювання.

В параграфі 2.2.3 описано алгоритм роботи системи із деталізацією всіх етапів прийняття рішення.

Параграф 2.3 демонструє оптимальний варіант розташування системи виявлення DDoS-атак у комп’ютерній мережі.

ПРОТОТИП СИСТЕМИ ВИЯВЛЕННЯ DDOS-АТАКИ

3.1 Програмна реалізація

MikroTik - це компанія, яка спеціалізується на створенні та виробництві мережевого обладнання, такого як маршрутизатори, комутатори, точки доступу, а також програмне забезпечення для управління мережею [36]. Однак, MikroTik часто відомий своєю лінією маршрутизаторів, які використовуються в багатьох типах мереж, включаючи офісні, домашні та провайдерські мережі. Продукція MikroTik відома своєю гнучкістю, ефективністю та широким функціоналом, що робить її популярним вибором для різноманітних завдань в області мережевого зв'язку. Маршрутизатори Маршрутизатори MikroTik працюють під управлінням високофункціональної операційної системи RouterOS, що забезпечує розширені можливості для налаштування та ефективного керування мережею.

RouterOS Scripting - це мова програмування, яка використовується для автоматизації різноманітних завдань на пристроях MikroTik, що працюють на операційній системі RouterOS. Ця мова надає можливості для створення скриптів, які дозволяють контролювати та автоматизувати різні аспекти роботи маршрутизатора MikroTik [37].

Для розробки системи було обрано мову RouterOS Scripting. Оскільки:

– дозволяє зчитувати та змінювати конфігурацію пристрою MikroTik, можна створювати та налаштовувати інтерфейси, маршрути, правила брандмауера, черги та багато іншого, використовуючи скрипти;

– підтримує механізм подій, що дозволяє виконувати скрипти автоматично при виникненні певних подій або за розкладом, що дозволяє реагувати на різні події в мережі та автоматизувати виконання певних дій;

– може взаємодіяти з API MikroTik, що дозволяє автоматизувати взаємодію з пристроями MikroTik через мережу.

Для того, щоб здійснювати перевірку трафіку слід спочатку отримати потік за допомогою скрипта як показано на рисунку 3.1

```
:local srcAddress [/ip firewall connection
                   get [find dst-port=80] src-address];
:local dstAddress [/ip firewall connection
                   get [find dst-port=80] dst-address];
:local dstPort [/ip firewall connection
                  get [find dst-port=80] dst-port];
```

Рисунок 3.1 – Отримання потоку даних

У цьому фрагменті потік трафіку отримується із 80 порту. У залежності від адміністративних налаштувань мережі можна змінити перелік портів із яких потрібно брати трафік. Далі відбуватиметься перевірка трафіку на самоподібність. Після цього, у разі необхідності додаткової перевірки, потрібно завантажити базу правил за допомогою скрипта як показано на рисунку 3.2.

```
:local ruleCount [/ip firewall filter count];
```

Рисунок 3.2 – Завантаження бази правил

Далі відбуватиметься перевірка на відповідність правилам із бази (рисунок 3.3).

```
:foreach i in=[/ip firewall filter find] do={
:local ruleSrcAddress [/ip firewall filter get $i src-address];
:local ruleDstAddress [/ip firewall filter get $i dst-address];
:local ruleDstPort [/ip firewall filter get $i dst-port];
:if (($srcAddress = $ruleSrcAddress) &&
 ($dstAddress = $ruleDstAddress) && ($dstPort = $ruleDstPort))
do={
:log info "Потік трафіку відповідає правилу $i";
}
}
```

Рисунок 3.3 – Перевірка на відповідність

Скрипт для потоку трафіку з метою блокування користувача за його IP-адресою, якщо правило забороняє з'єднання, показано на рисунку 3.4.

```
:if ($blockConnection != "") do={
:log info "Блокуємо IP: $srcAddress";
/ip firewall address-list add address=$srcAddress
    list=blocked_connections comment=
        "Заблокований IP через правило заборони з'єднання";
}
```

Рисунок 3.4 – Блокування користувача

Скрипт для потоку трафіку з метою дозволу з’єднання користувачеві за його IP-адресою, якщо правило дозволяє з'єднання, показано на рисунку 3.5.

```
:if ($allowConnection != "") do={
:log info "Дозволяємо IP: $srcAddress";
/ip firewall address-list add address=$srcAddress
    list=allowed_connections comment=
        "Дозволений IP через правило, що дозволяє з'єднання";
}
```

Рисунок 3.5 – Дозвіл з’єднання

3.2 Експериментальне дослідження

Ізольоване локальне середовище для дослідження DDoS-атак буде складається з маршрутизатора MikroTik і десять персональних комп'ютерів, двох комутаторів D-link, трьох серверів: DNS, Microsoft SQL, LDAP. Маршрутизатор MikroTik виступає центральним елементом комп’ютерної мережі. Він виконує роль маршрутизації, забезпечуючи передачу даних між ПК та серверами в мережі. Персональні комп'ютери будуть підключені до мережі через маршрутизатор

MikroTik.

На один персональний комп'ютер з ОС Windows 10 буде встановлено Wireshark, що здатний аналізувати дані, що пересилаються через різні мережеві протоколи, такі як Ethernet, Wi-Fi, TCP, UDP, IP і багато інших. Він може відображати інформацію про кожен пакет даних, включаючи джерело та призначення, тип протоколу, розмір пакету, час передачі тощо. Крім того, Wireshark може фільтрувати трафік за різними критеріями, щоб зосередитися на конкретних пакетах або виділити аномальність в мережі [38]. На цей ПК буде здійснюватися атака. Wireshark також забезпечує можливість глибокого аналізу мережевих взаємодій та дозволяє виявляти шкідливий код або зловмисні дії в мережі. Це робить його незамінним інструментом для аналізу безпеки, аудиту та виявлення збоїв в роботі мережевої інфраструктури. Завдяки графічному інтерфейсу та можливостям налаштування, Wireshark є зручним у використанні для професіоналів і аматорів у сфері мережевої безпеки.

На сервери DNS, Microsoft SQL та LDAP будуть здійснюватися атаки.

На дев’яти ПК буде інстальовано ОС Kali Linux, яка має в собі різноманітні інструменти для тестування на проникнення та аналізу безпеки мережі. Для моніторингу та аналізу мережевого трафіку під час проведення DDoS атаки будуть використовуватися програми такі як Wireshark або Tcpdump. На цих комп'ютерах буде запущено інструмент hping3 для здійснення DDoS атак для моделювання атак та вивчення їх впливу на мережеву інфраструктуру.

hping3 - це утиліта для мережевого тестування та аналізу мережевого трафіку, яка працює на рівні TCP/IP. Вона надає широкий спектр можливостей для тестування мережевих пристроїв, включаючи відправку і прийом пакетів з різними типами, портами та прапорами TCP, а також аналіз реакції мережевих пристроїв на ці пакети. hping3 може бути використано для проведення різноманітних тестів, таких як сканування портів, виявлення мережевих пристроїв, відслідковування шляху маршрутизації, випробування забезпечення мережевої безпеки та багато іншого [39]. Зловмисник використовує техніку TCP SYN flooding за допомогою підроблених IP-адрес для здійснення DoS-атаки.

Використовуючи hping3, можна моделювати атаки, такі як TCP SYN flooding, щоб оцінити стійкість мережі до такого типу атак. Ця можливість робить hping3 важливим інструментом у наборі інструментів адміністратора мережі та фахівця з кібербезпеки для випробування та покращення обороноздатності мережевої інфраструктури.

Також встановлено програму для здійснення атак High Orbit Ion Cannon. High Orbit Ion Cannon (HOIC) - це інструмент для атак на мережеві ресурси, який використовується в розподіленому режимі (DDoS). HOIC розроблений для накладання великого обсягу трафіку на цільовий сервер або мережевий ресурс з метою перевантаження його пропускної здатності і зниження доступності для законних користувачів. Цей інструмент дозволяє користувачам об'єднуватися в мережу ботів (botnet) і спрямовувати спільні атаки на цільові ресурси. HOIC може бути налаштований для генерації різних видів трафіку, включаючи HTTP-запити, UDP-пакети, ICMP-повідомлення та інше. HOIC реалізує DDoS-атаку на прикладному рівні, заповнюючи сервер жертви HTTP- запитами «GET» і «POST» з метою перевантаження потужності обробки запитів сервера. Для складних атак можна використовувати користувацькі сценарії для одночасного націлювання на кілька субдоменів сайту жертви.

Для тестування розроблених правил було створено систему нечіткого логічного висновку засобами Matlab. Всього було проаналізовано 50063112 записів із набору даних CICDDoS2019.

З них:

- 40756 записів було визначено як безпечних із 56863 записів безпечних всього;
- 16107 безпечних записів визначено як небезпечних;
- 46009408 записів визначено як небезпечних із 50006249 записів небезпечних всього;
- 3996841 записів небезпечних визначено як безпечних.

Після корегування розроблених правил наступний етап тестування показав такі результати:

- 56741 записів було визначено як безпечних із 56863 записів безпечних всього;

- 122 безпечних записів визначено як небезпечних;

- 50004984 записів визначено як небезпечних із 50006249 записів небезпечних всього;

- 14135 записів небезпечних визначено як безпечних.

Поділ виявлених зловмисних потоків відповідно до типів атак представлено на рисунку 3.6.

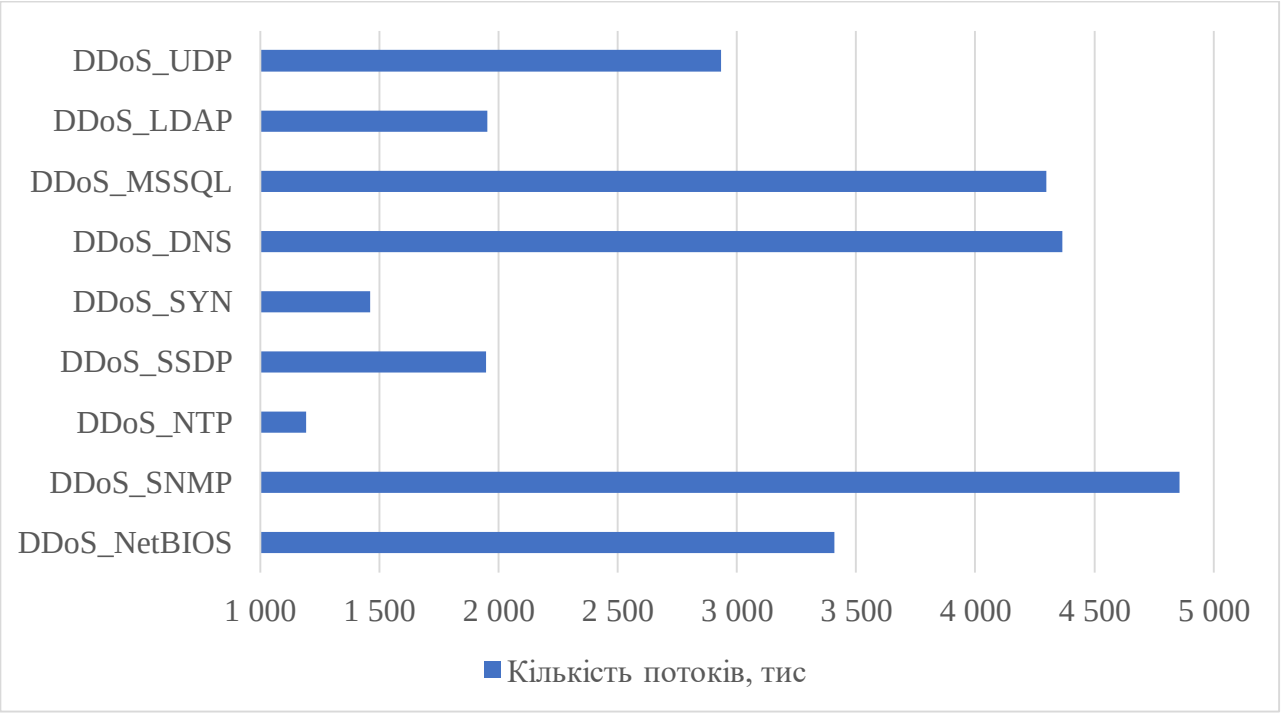


Рисунок 3.6 - Виявлених зловмисних потоків відповідно до типів атак при тестуванні системи за допомогою засобів Matlab

Наступним етапом буде тестування всієї системи у фізичному ізольованому середовищі, яке описано в параграфі 3.2.1. Тривалість роботи системи складала 24год – 3 дні по 8 год. Із восьми ПК (де інстальовано ОС Kali Linux) запускалися атаки різних типів (почергово) з використанням різних програмних застосунків. Один ПК не здійснював зловмисних дій та не підлягав атакам для наявності нормального трафіку в мережі. Всього було проаналізовано 31456 потоків. Метрика якості наступна:

- 2685 потоків було визначено як безпечних із 2733 безпечних потоків всього;

- 48 безпечних потоків визначено як небезпечних;

- 28194 потоків визначено як небезпечних із 28723 небезпечних потоків всього;

- 529 потоків небезпечних визначено як безпечних.

Поділ виявлених зловмисних потоків відповідно до типів атак представлено на рисунку 3.7.

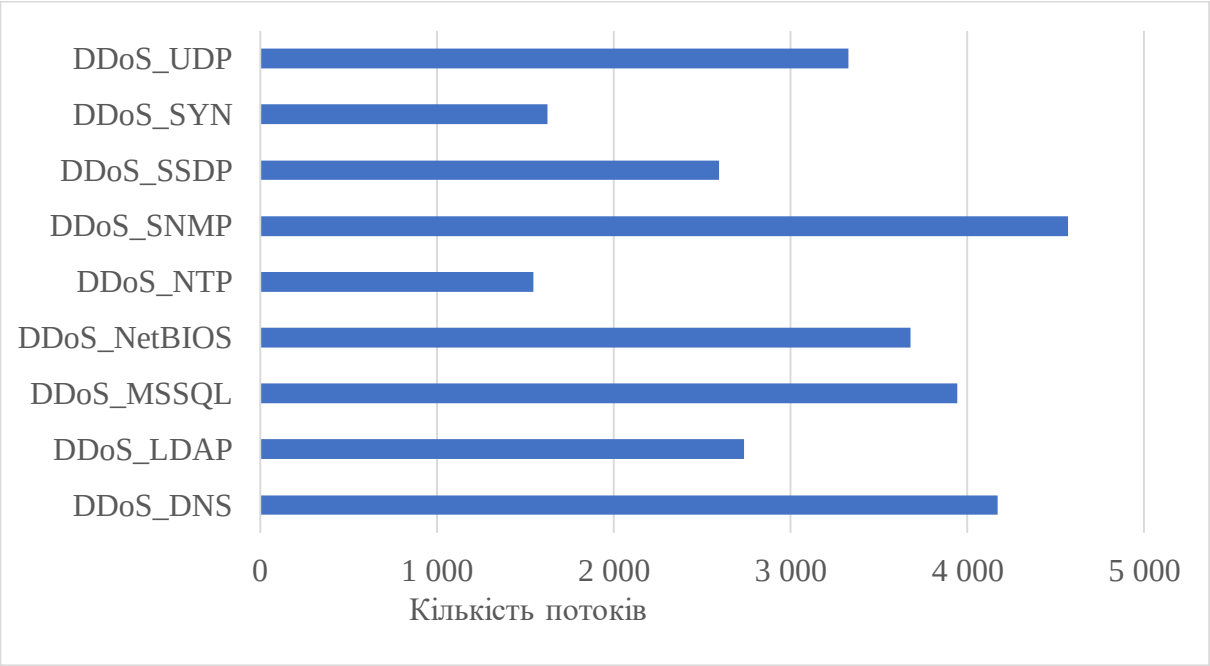


Рисунок 3.7 - Виявлених зловмисних потоків відповідно до типів атак при тестуванні системи у фізичному середовищі

3.3 Доведення ефективності

Оцінка ефективності включає наступні метрики [40]:

– TP (True Positive) – правильна класифікація позитивних проб як позитивних;

– FP (False Positive) – частка негативних зразків, помилково ідентифікованих як позитивні;

– TN (True Negative) – правильна класифікація негативних зразків як негативних;

– FN (False Positive) – неправильна класифікація позитивних зразків як негативних.

Результати метрик якості після тестування за допомогою Matlab та у фізичному тестовому середовищі відображено у таблиці 3.1.

Таблиця 3.1 – Результати метрик якості після тестування

Метрика / Середовище	TP	TN	FP	FN
Matlab із набором даних CICDDoS2019 (№1)	46009408	40756	16107	3996841
Matlab із набором даних CICDDoS2019 (№2)	50004984	56741	122	14135
Тестове середовище із реальними атаками	28194	2685	48	529

На основі отриманих даних можна розрахувати наступні показники продуктивності:

- повнота (recall) – співвідношення правильно класифікованих позитивних зразків до загальної кількості позитивних зразків:

$$Recall = \frac{TP}{TP + FN} \tag{3.1}$$

- точність (precision) – частка правильно визначених зловмисних подій серед усіх подій, які система визначила як зловмисні:

$$Precision = \frac{TP}{TP + FP} \tag{3.2}$$

- акуратність (accuracy) – частка правильно виявлених та правильно не виявлених подій серед усіх подій:

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \quad (3.3)$$

- помилка (specificity) – вимірює здатність системи виявлення зловмисників правильно ідентифікувати незловмисні об'єкти або події як незловмисні:

$$Specificity = \frac{FP + FN}{TP + FP + TN + FN} \quad (3.4)$$

- F-міра (F-score) –

$$F\ score = \frac{Recall + Precision}{2} \quad (3.5)$$

Повнота під час першого тестування:

$$Recall = \frac{46009408}{46009408 + 3996841} * 100\% = 92\% \quad (3.6)$$

Точність під час першого тестування:

$$Precision = \frac{46009408}{46009408 + 16107} * 100\% = 99\% \quad (3.7)$$

Акуратність під час першого тестування:

$$Accuracy = \frac{46009408 + 40756}{46009408 + 40756 + 16107 + 3996841} * 100\% = 91{,}9\% \quad (3.8)$$

Помилка під час першого тестування:

$$Specificity = \frac{16107 + 3996841}{46009408 + 40756 + 16107 + 3996841} * 100\% = 8{,}02\% \quad (3.9)$$

F-міра під час першого тестування:

$$F1\ score = \frac{92\% + 99\%}{2} = 95{,}5\% \quad (3.10)$$

Повнота під час другого тестування:

$$Recall = \frac{50004984}{50004984 + 14135} * 100\% = 99{,}97\% \quad (3.11)$$

Точність під час другого тестування:

$$Precision = \frac{50004984}{50004984 + 122} * 100\% = 99{,}9\% \quad (3.12)$$

Акуратність під час другого тестування:

$$Accuracy = \frac{50004984 + 56741}{50004984 + 56741 + 122 + 14135} * 100\% = 99{,}97\% \quad (3.13)$$

Помилка під час другого тестування:

$$Specificity = \frac{122 + 14135}{50004984 + 56741 + 122 + 14135} * 100\% = 0{,}03\% \quad (3.14)$$

F-міра під час другого тестування:

$$F1\ score = \frac{99{,}97\% + 99{,}9\%}{2} = 99{,}94\% \quad (3.15)$$

Повнота під час тестування у фізичному середовищі із запуском реальних атак:

$$Recall = \frac{28194}{28194 + 529} * 100\% = 98{,}16\% \quad (3.16)$$

Точність під час тестування у фізичному середовищі із запуском реальних атак:

$$Precision = \frac{28194}{28194 + 48} * 100\% = 99{,}8\% \quad (3.17)$$

Акуратність під час тестування у фізичному середовищі із запуском реальних атак:

$$Accuracy = \frac{28194 + 2685}{28194 + 2685 + 48 + 529} * 100\% = 98{,}17\% \quad (3.18)$$

Помилка під час тестування у фізичному середовищі із запуском реальних атак:

$$Specificity = \frac{48 + 529}{28194 + 2685 + 48 + 529} * 100\% = 1{,}83\% \quad (3.19)$$

F-міра під час тестування у фізичному середовищі із запуском реальних атак:

$$F1\ score = \frac{98{,}17\% + 99{,}8\%}{2} = 98{,}99\% \quad (3.20)$$

Порівнюючи результати тестування (табл.3.2), слід відмітити, що друга тестова вибірка у середовищі моделювання дала показник помилки 0,03%, а повнота становить 99,97%. Після таких результатів у фізичному середовищі

відсоток помилок становив 1,83%, а повнота 98,16%. Це означає, що при реальних атаках відсоток помилок більший, зокрема це пов'язано із реалізацією атак, які розтягнуто у часі.

Таблиця 3.2 – Порівняння результатів навчання та тестування

Метрика / Середовище	Повнота, %	Точність, %	Акуратність, %	Помилка, %	F-міра, %
Matlab із набором даних CICDDoS2019 (№1)	92	99	91,9	8,02	95,5
Matlab із набором даних CICDDoS2019 (№2)	99,97	99,9	99,97	0,03	99,94
Тестове середовище із реальними атаками	98,16	99,8	98,17	1,83	98,99

На рисунках 3.8-3.9 відображено графічне порівняння якості виявлення зловмисного трафіку під час всіх етапів тестування.

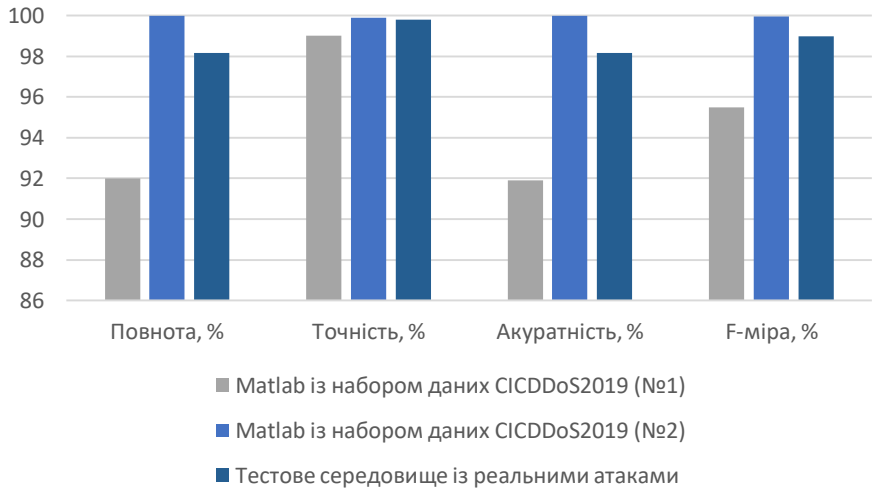


Рисунок 3.8 – Порівняння повноти, точності, акуратності та F-міри при виявленні DDoS-атак

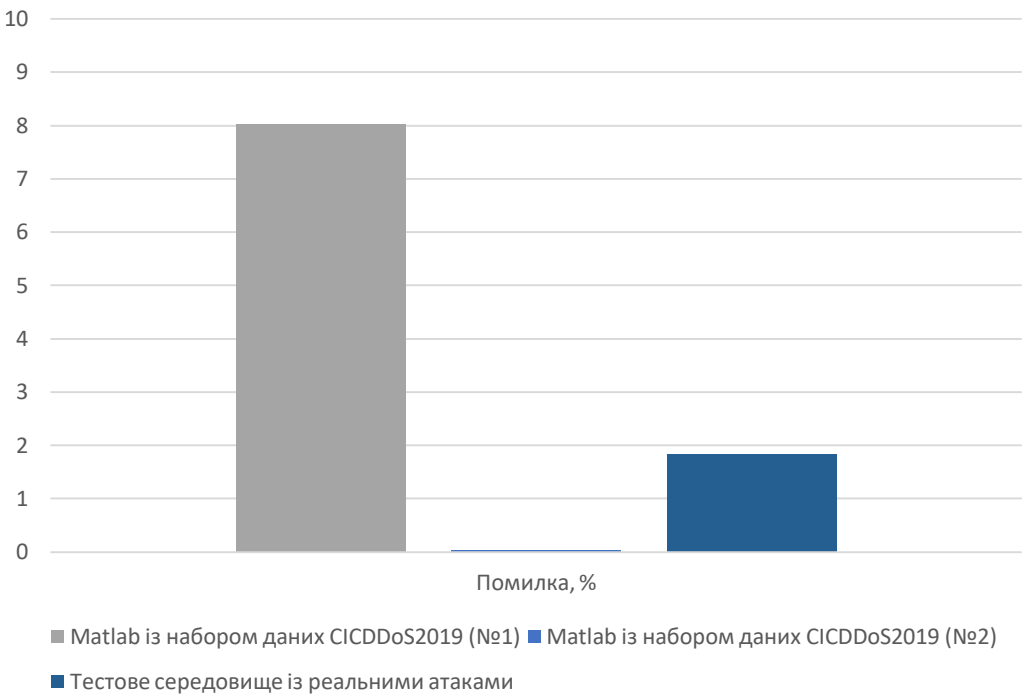


Рисунок 3.9 – Порівняння помилки при виявленні DDoS-атак

3.4 Висновки до розділу

У першому параграфі даного розділу було описано мову програмування RouterOS Scripting з обґрунтуванням вибору та наведено ключові фрагменти скриптів для виконання поставленого завдання, зокрема скрипти для формування потоків та ініціація порівнянь із розробленою базою правил, блокування користувача чи дозвіл на з'єднання.

В другому параграфі описано фізичне ізольоване середовище, де буде проходити дослідження роботи та ефективності розробленої системи при реальних атаках. Проведено тестування системи за допомогою Matlab задля її налаштування максимально близько до максимального показника виявлення атак. Також проведено дослідження роботи системи в умовах, що максимально наближені до реальних.

На основі отриманих результатів у третьому параграфі проведено розрахунок та доведення ефективності системи. Метрика повноти складає 98,16%, а відсоток помилок 1,83%.

ВИСНОВКИ

У даній роботі було вирішено завдання розробки системи виявлення DDoS-атак, які запущені із мережі на сторонні ресурси чи в межах мережі.

Значну увагу приділено вибору засобу для моделювання системи виявлення DDoS-атаки, зокрема описано приклади та особливості застосування нечіткої логіки для прийняття рішення. Крім того, було представлено набір даних CICDDoS 2019, що використовується для оцінки ефективності виявлення DDoS-атак: класифікація атак, перелік функцій набору даних та їх опис.

У другому розділі робота містить опис схеми комп'ютерної мережі, модель системи та алгоритм роботи системи з деталізацією всіх етапів прийняття рішення. Також описано ізольовану локальну мережу для дослідження та тестування роботи системи при реальних умовах.

Мова програмування RouterOS Scripting була розглянута з точки зору її придатності для виконання завдань у рамках проекту. Аналіз включав демонстрацію основних скриптів, зокрема, скрипти для створення потоків, порівняння з базою правил, блокування або дозволу доступу користувачам. Також було розкрито, як відбуватиметься дослідження в ізольованому фізичному середовищі, щоб оцінити роботу та ефективність системи під час реальних атак. Для досягнення оптимальної точності системи використовувався Matlab, що дозволило максимально наблизити систему до виявлення атак у відповідності з заданими метриками. Робота системи також була перевірена в умовах, що максимально наближені до реальних. На основі отриманих результатів було проведено розрахунок та доведення ефективності системи, яка показала високий рівень повноти (98.16%) та низький відсоток помилок (1.83%). Це свідчить про успішність розробленої системи виявлення DDoS-атак.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Коди стану HTTP. URL: https://hostiq.ua/wiki/ukr/http-status-codes/ (дата звернення 13.02.2024)

2. Protect your environment from UDP Flood Attacks. URL: https://www.radware.com/blog/ddos-protection/2023/10/protect-your-environment-from-udp-flood-attacks/ (дата звернення 13.02.2024)

3. UDP Flood Attack. URL: https://www.wallarm.com/what/udp-flood-attack (дата звернення 14.02.2024)

4. CAPEC-487: ICMP Flood. URL: https://capec.mitre.org/data/definitions/487.html (дата звернення 15.02.2024)

5. What Are SYN Flood DDoS Attacks? URL: https://www.akamai.com/glossary/what-are-syn-flood-ddos-attacks (дата звернення 16.02.2024)

6. Security Glossary: DDoS. What Are SYN Flood DDoS Attacks? URL: https://www.cdnetworks.com/glossary/syn-flood-ddos-attacks/ (дата звернення 17.02.2024)

7. IM Tas, S Baktir. A Novel Approach for Efficient Mitigation against the SIP-Based DRDoS Attack. *Applied Sciences*. 2023. Vol 13(3). DOI: 10.3390/app13031864

8. H. ASHRAF, A. ULLAH, S. TAHIRA, N. Jhanjhi. Intrusion Detection and Prevention System for Secure Multimedia sharing in Future Internet. *Preprints*. 2024. DOI: 10.20944/preprints202401.1313.v1

9. P. Shorubiga, R. Shyam. CNN-Based Model for the HTTP Flood Attack Detection. *2023 International Conference for Advancement in Technology (ICONAT), Goa*. 2023. PP. 1-6. DOI: 10.1109/ICONAT57137.2023.10080698

10. What Is an HTTP Flood DDoS Attack? URL: https://www.akamai.com/glossary/what-is-an-http-flood-ddos-attack (дата звернення 20.02.2024)

11. S. Black, Y. Kim. An Overview on Detection and Prevention of Application Layer DDoS Attacks. *2022 IEEE 12th Annual Computing and Communication*

Workshop and Conference (CCWC). 2022. PP. 0791-0800. DOI: 10.1109/CCWC54503.2022.9720741.

12. DoS Threat: Understanding the Risks and Protecting Your Systems. URL: https://hackyourmom.com/en/servisy/%E2%84%967-ethical-hacking-labs-dos-ataky/ (дата звернення 2.03.2024)

13. Ping of Death. URL: https://sourcedaddy.com/networking/ping-of-death.html (дата звернення 8.03.2024)

14. G. Sujatha, Y. Kanchhal, G. George. An Advanced Approach for Detection of Distributed Denial of Service (DDoS) Attacks Using Machine Learning Techniques. *2022 3rd International Conference on Smart Electronics and Communication (ICOSEC)*. 2022. PP. 821-827. DOI: 10.1109/ICOSEC54921.2022.9951944.

15. E. Navruzov, A. Kabulov. Detection and analysis types of DDoS attack. *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*. 2022. PP. 1-7. DOI: 10.1109/IEMTRONICS55184.2022.9795729.

16. M. Mittal, K. Kumar, S. Behal. Deep learning approaches for detecting DDoS attacks: a systematic review. *Soft Comput*. 2023. Vol. 27, PP. 13039–13075. DOI: 10.1007/s00500-021-06608-1

17. Danial Javaheri, Saeid Gorgin, Jeong-A Lee, Mohammad Masdari. Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives. *Information Sciences*. 2023. Vol. 626, PP. 315-338. DOI: 10.1016/j.ins.2023.01.067.

18. H.-Y. Kwon, T. Kim, M.-K. Lee. Advanced Intrusion Detection Combining Signature-Based and Behavior-Based Detection Methods. *Electronics*. 2022. Vol. 11, P. 867. DOI: 10.3390/electronics11060867

19. M. Gniewkowski, H. Maciejewski, T. Surmacz. Anomaly Detection Techniques for Different DDoS Attack Types. *Lecture Notes in Networks and Systems. Springer*. 2022. Vol. 484. DOI:10.1007/978-3-031-06746-4_7

20. Mahmood A. Al-Shareeda, Selvakumar Manickam, Murtaja Ali. DDoS Attacks Detection Using Machine Learning and Deep Learning Techniques: Analysis

and Comparison. *Bulletin of Electrical Engineering and Informatics*. 2023. Vol. 12, No. 2, PP. 930-939.

21. M.M. Saeed. A real-time adaptive network intrusion detection for streaming data: a hybrid approach. *Neural Comput & Applic*. 2022. Vol. 34, PP. 6227–6240. DOI: 10.1007/s00521-021-06786-x

22. S. Muthukumar, A.K. Ashfauk Ahamed. A Novel Framework of DDoS Attack Detection in Network Using Hybrid Heuristic Deep Learning Approaches with Attention Mechanism. *IOS Press*. 2024. Vol. 30, No. 2, PP. 251–277.

23. Michael Voskoglou. Fuzzy Sets, Fuzzy Logic and Their Applications. *Mathematics*. 2020. P. 366. DOI: 10.3390/books978-3-03928-521-1

24. Jenny Carter, Francisco Chiclana, Arjab Singh Khuman, Tianhua Chen Fuzzy Logic: Recent Applications and Developments. 2021. 385 p.

25. Guanrong Chen, Trung Tat Pham. Introduction to Fuzzy Sets, Fuzzy Logic, and Fuzzy Control Systems. 2019. 328 p

26. Субач І.Ю. Здоренко Ю.М. Фесьоха В.В. Методика виявлення кібератак типу js(html)/scrinject на основі застосування математичного апарату теорії нечітких множин. *Збірник наукових праць ВІТІ*. 2018. Випуск 4, ст. 125-131.

27. Кондратенко Ю. П. Нечіткі множини та нечітка логіка : метод. рек. та вказівки для виконання лабораторних робіт студентами спец. 122 «Комп'ютерні науки» / Ю. П. Кондратенко, Г. В. Кондратенко, Є. В. Сіденко ; під ред. Ю. П. Кондратенка. – Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2019. – 36 с. – (Методична серія ; вип. 267).

28. O. Castillo, P. Melin. Conclusions of Type-3 Fuzzy Logic in Prediction. In: Type-3 Fuzzy Logic in Time Series Prediction. *SpringerBriefs in Applied Sciences and Technology. Springer*. 2024. DOI: 10.1007/978-3-031-59714-5_8

29. Fuzzy Logic System. URL: https://www.educba.com/fuzzy-logic-system/ (дата звернення 24.04.2024)

30. Pham Hai, Long Cu, Khanh Phan, Ha Quoc. A Fuzzy Knowledge Graph PairsBased Application for Classification in Decision Making: Case Study of Preeclampsia Signs. *Information*. 2023. Vol. 14, P.104. DOI: 10.3390/info14020104

31. I. Lekshmi, M. Regees. Review on fuzzy multi-criteria decision-making methods in medical diagnosis. *International journal of health sciences*. 2022. PP. 2546-2554. DOI: 10.53730/ijhs.v6nS5.9198.

32. L.A. Zadeh. Fuzzy Logic. *Springer*. 2023. DOI: 10.1007/978-1-0716-2628-3_234

33. Shu Gong, Gang Hua, Wei Gao. Connectivity Analysis of Bipolar Fuzzy Networks. *Mathematical Problems in Engineering*. 2022. Vol. 1. DOI: 10.1155/2022/6398599.

34. N. Jan, J. Gwak, J. Pei, R. Maqsood, A. Nasir. Analysis of Networks and Digital Systems by Using the Novel Technique Based on Complex Fuzzy Soft Information. *IEEE Transactions on Consumer Electronics*. 2023. Vol. 69, No. 2, PP. 183-193. DOI: 10.1109/TCE.2022.3226819.

35. DDoS evaluation dataset (CIC-DDoS2019). URL: https://www.unb.ca/cic/datasets/ddos-2019.html (дата звернення 26.04.2024)

36. MikroTik Routers and Wireless. URL: https://mikrotik.com/ (дата звернення 27.04.2024)

37. Scripting - RouterOS - MikroTik Documentation - Support. URL: https://help.mikrotik.com/docs/display/ROS/Scripting (дата звернення 28.04.2024)

38. Wireshark User's Guide. URL: https://www.wireshark.org/docs/wsug_html_chunked/ (дата звернення 29.04.2024)

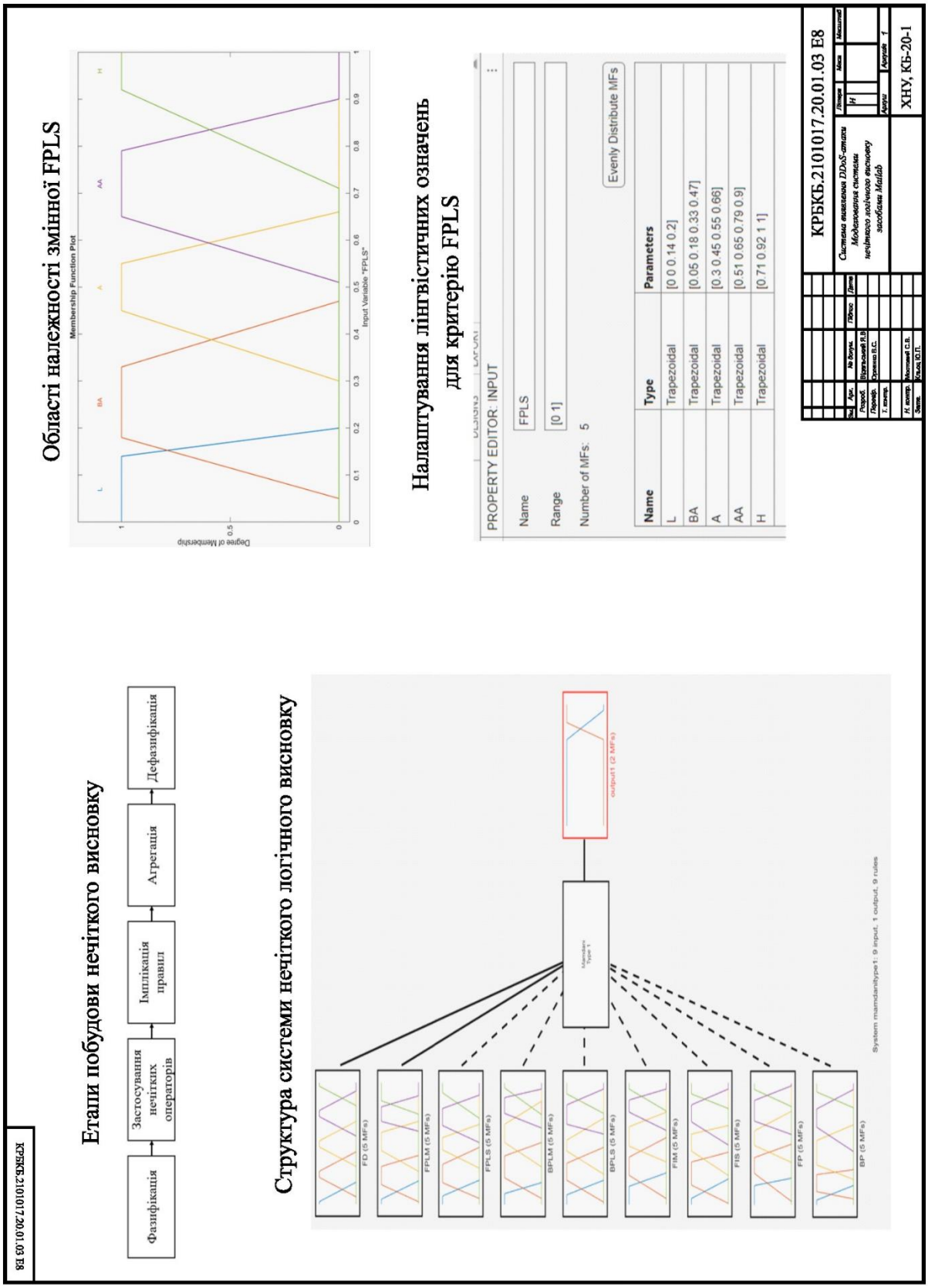
39. hping3 | Kali Linux Tools. URL: https://www.kali.org/tools/hping3/ (дата звернення 29.04.2024)

40. Wahyudi Setiawan, Fitri Damayanti. Layers Modification of Convolutional Neural Network for Pneumonia Detection. *Journal of Physics: Conference Series*. 2020. Vol. 1477. DOI: 10.1088/1742-6596/1477/5/052055.

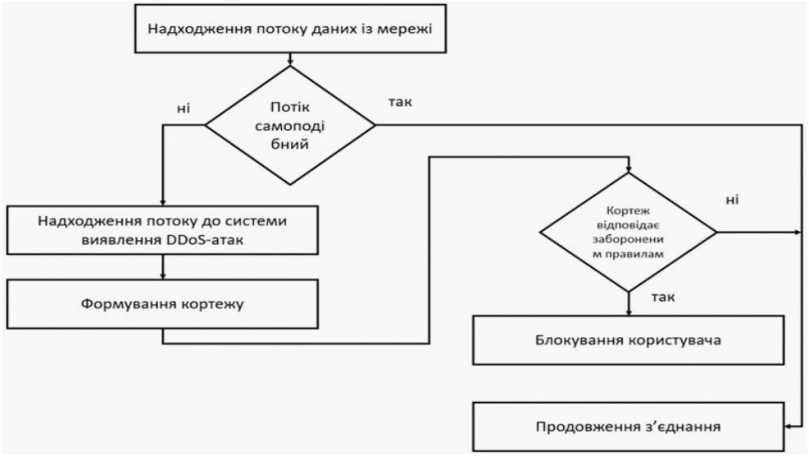
ДОДАТОК А

(обов'язковий)

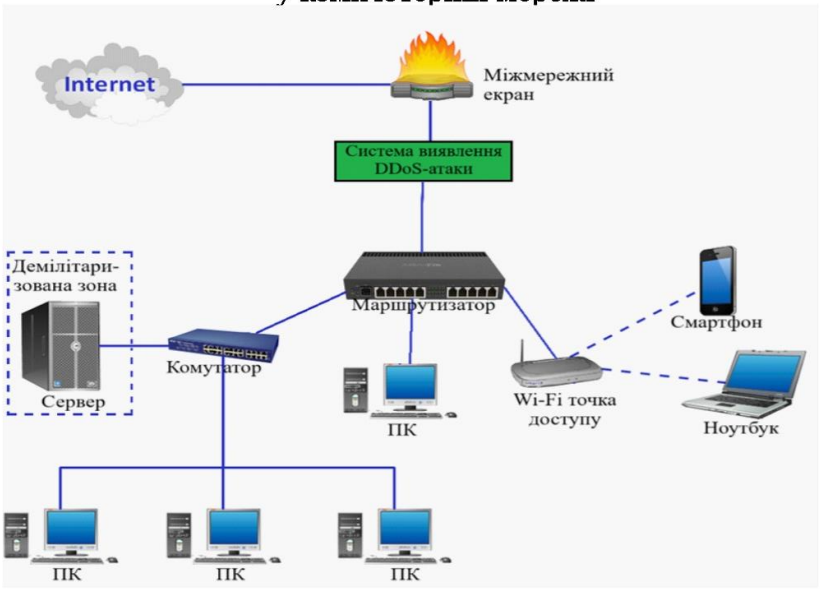
Копія графічної частини



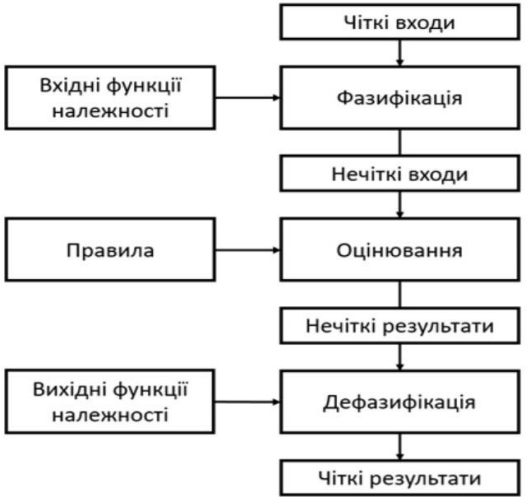
Алгоритм роботи системи виявлення DDoS-атак



Розміщення системи виявлення DDoS-атак у комп'ютерній мережі

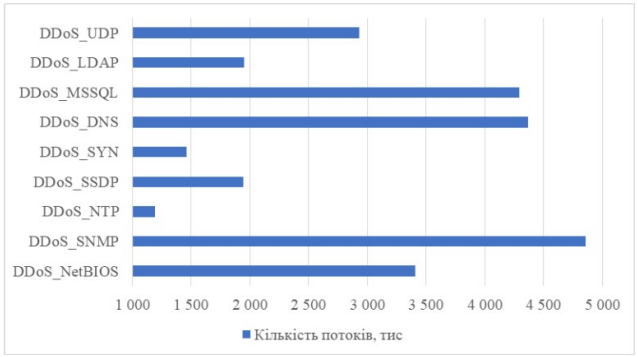


Перевірка кортежу із набором заборонених правил

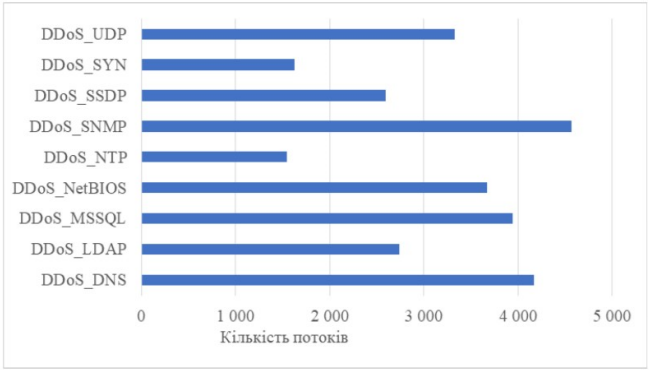


						КРБКБ.2101017.20.01.03 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата			Літера / Маса / Масштаб
Розроб.		Відзвський Я.В.			Система виявлення DDoS-атаки. Схеми реалізації системи виявлення DDoS-атаки		Н
Перевір.		Орленко В.С.					Аркуш / Аркушів 1
Т. контр.							
Н. контр.		Мостовий С.В.				ХНУ, КБ-20-1	
Затв.		Кільоц Ю.П.					

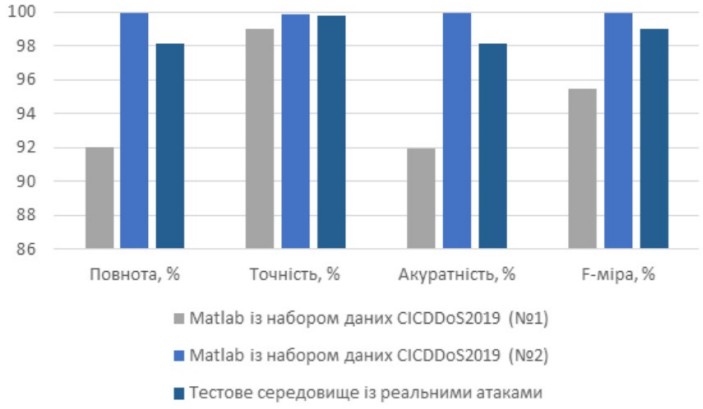
Виявлених зловмисних потоків відповідно до типів атак при тестуванні системи за допомогою засобів Matlab



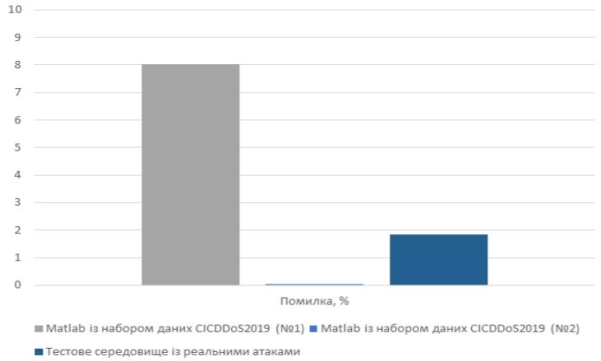
Виявлених зловмисних потоків відповідно до типів атак при тестуванні системи у фізичному середовищі



Порівняння повноти, точності, акуратності та F-міри при виявленні DDoS-атак



Порівняння відсотка помилки при виявленні DDoS-атак



					КРБКБ.2101017.20.01.03 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Система виявлення DDoS-атаки. Оцінка достовірності системи виявлення DDoS-атаки	Літера	Маса	Масштаб
Розроб.		Відзяський Я.В.				Н		
Перевір.		Орлянко В.С.				Аркуш	Аркушів 1	
Т. контр.								
Н. контр.		Мостовий С.В.				ХНУ, КБ-20-1		
Затв.		Кільоц Ю.П.						

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Відельського Ярослава Володимировича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-20-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

10.06.2024
дата


підпис

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 9%**

	Документ		Сумарний збіг по Базі Даних	
ID: 129624 Назва: Система виявлення DDoS-атаки Додано в БД: 2024-06-11 Автора: Відельський Я.В. Керівники: Орленко В.С. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	66141	573	268 (0%)	3 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1016346946

Дата перевірки:
11.06.2024 20:02:44 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
11.06.2024 22:34:12 EEST

ID користувача:
100008300

Назва документа: **Відельський_Записка на плагіат**

Кількість сторінок: **56** Кількість слів: **10068** Кількість символів: **75808** Розмір файлу: **1.32 MB** ID файлу: **1016148836**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

5.93%
Схожість

Найбільша схожість: **2.29%** з Інтернет-джерелом (https://ela.kpi.ua/bitstream/123456789/53380/1/Diakovskyi_bakalavr.p.

4.22% Джерела з Інтернету	190	Сторінка 58
2.21% Джерела з Бібліотеки	94	Сторінка 59

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	1
Підозріле форматування	14 сторінок

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система виявлення DDoS-атаки

Автор: Відельський Ярослав Володимирович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Орленко Вікторія Сергіївна, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 94,07%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 100%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за , освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи _____ Вікторія ОРЛЕНКО

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Відельський Ярослав Володимирович

Тема Система виявлення DDoS-атаки

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3; кількість сторінок записки 60.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі була розроблена система виявлення DDoS-атаки, яка надходить з мережі. Проаналізовано різні типи DDoS-атак, їх механізми та методи реалізації. Проведено порівняння існуючих методів виявлення атак, визначено їхні переваги та недоліки. Розроблено алгоритм роботи системи виявлення атак у мережі та змодельовано систему за допомогою обраних засобів моделювання. Робота також включає експериментальну перевірку ефективності запропонованої системи з використанням тестових наборів даних.

2. Висновок про відповідність кваліфікаційної роботи завданню У кваліфікаційній роботі було виконано поставлене завдання як у теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі роботи наведено загальну характеристику задачі, визначено об'єкт, предмет та методи дослідження, а також сформульовано мету. Зазначено задачі, що потрібно виконати для досягнення поставленої мети. Проведено аналіз досліджуваної проблеми та обґрунтовано підхід до її вирішення. У першому розділі розглядаються основні види DDoS-атак, їх класифікація та особливості, підходи до виявлення. Другий розділ присвячений розробці алгоритму для системи виявлення, вибору засобів для моделювання. Третій розділ описує програмну реалізацію та тестування.

4. Позитивні сторони роботи Кваліфікаційна робота має практичну цінність. Вона полягає у розробці системи виявлення DDoS-атак, яка реалізовується із комп'ютерної мережі щодо сторонніх ресурсів. А виявлення таких атак може запобігти компрометації мережі та зменшити пікове навантаження на мережеве обладнання.

5. Негативні сторони роботи Несвоєчасність внесення нових правил у систему виявлення DDoS-атак для ідентифікації атак може призвести до нижчого відсотка виявлених атак.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень для досягнення мети.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Мартинюк Валерій Володимирович, завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, доктор технічних наук, професор

« 12 » червня 2024. (підпис)