Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

В.о. зав. кафедрою КІСМіТ
Марина ЄСІНА
"Допущено до захисту"

« »_____2025р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Аналіз методів та технологій захисту від DDos атак»

оцінка « _____ »

Голова ЕК
Мичуда Л.З.

Керівник: к.т.н. Шеханін К. Ю.

Рецензент: к. т. н. Лещинин Ю. З.

Виконавець: студент групи КБ-41
Бибко Д. В.

Харків 2025

РЕФЕРАТ

Пояснювальна записка до бакалаврської дипломної роботи містить 44 сторінок, 13 рисунків, 4 таблиці, 23 джерела посилань.

Метою роботи є дослідження актуальних методів і технологій захисту від DDoS-атак, зосереджуючись на аналізі їхньої ефективності та застосовності в умовах сучасних інформаційно-комунікаційних систем. Об’єктом дослідження виступають розподілені атаки на відмову в обслуговуванні (DDoS).

Предметом дослідження є способи виявлення, протидії та мінімізації наслідків DDoS-атак.

У роботі розглянуто теоретичні аспекти DDoS-атак, їх класифікацію, принципи реалізації та поширені вектори впливу. Особливу увагу приділено аналізу сучасних технологій захисту, включаючи методи фільтрації, маршрутизації, виявлення аномалій та побудови стійких архітектур безпеки. Робота також містить етап моделювання одного з типів атак із використанням симуляційного середовища, що дозволяє наочно оцінити результативність деяких підходів до захисту.

Отримані результати доповнюють теоретичні положення аналізом практичних сценаріїв, що може бути корисним при формуванні рекомендацій щодо захисту критичної інфраструктури від DDoS-атак.

Ключові слова: DDoS-АТАКА, REFLECTION ATTACK, КІБЕРБЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ, ФІЛЬТРАЦІЯ, МАРШРУТИЗАЦІЯ, BLACK HOLE, SFQ, АНАЛІЗ ВРАЗЛИВОСТЕЙ, МЕРЕЖЕВА БЕЗПЕКА.

ABSTRACT

The explanatory note to the master`s project contains 44 pages, 13 images, 4 charts and 23 references to sources.

The aim of this thesis is to explore current methods and technologies for protecting against DDoS attacks, focusing on the analysis of their effectiveness and applicability in modern information and communication systems.
The object of the study is distributed denial-of-service (DDoS) attacks.
The subject of the study is the methods of detection, mitigation, and response to DDoS attacks, particularly those utilizing reflection-based mechanisms.

The work examines the theoretical aspects of DDoS attacks, including their classification, implementation principles, and common attack vectors. Particular attention is given to analyzing modern protection technologies such as filtering, routing, anomaly detection, and the design of resilient security architectures. The thesis also includes a simulation stage for one type of attack using a modeling environment, providing a visual assessment of the effectiveness of selected defense strategies.

The obtained results complement the theoretical framework with practical insights, which can be useful in developing recommendations for protecting critical infrastructure against DDoS threats.

Keywords: DDoS ATTACK, REFLECTION ATTACK, CYBERSECURITY, INFORMATION PROTECTION, FILTERING, ROUTING, BLACK HOLE, SFQ, VULNERABILITY ANALYSIS, NETWORK SECURITY.

ЗМІСТ

ПЕРЕЛІК ПОЗНАЧЕНЬ І СКОРОЧЕНЬ 5

ВСТУП 6

1 АНАЛІЗ ПРИРОДИ ТА КЛАСИФІКАЦІЇ DDoS-АТАК 8

1.1 Основні поняття та класифікація DDoS-атак 8

1.2 Історія розвитку та тенденції DDoS-атак 10

1.3 Основні методи реалізації атак 11

1.4 Типові наслідки для інфраструктури 14

1.5 Сучасні приклади DDoS-атак 15

1.6 Чому DDoS-атаки залишаються привабливими для зловмисників 18

2 МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ ВІД DDos-АТАК 20

2.1 Принципи побудови систем захисту 20

2.2 Методи виявлення атак 22

2.3 Технології захисту 23

2.4 Хмарні сервіси та інфраструктурні рішення 26

3 АНАЛІЗ ЕФЕКТИВНОСТІ МЕТОДІВ ЗАХИСТУ ВІД DDos-АТАК 30

3.1 Опис параметрів та сценаріїв симуляції 30

3.2 Аналіз симуляції DDoS Reflection Attack 32

3.3 Аналіз симуляції методики запобігання DDoS-атаці за допомогою «Чорної діри» 37

3.4 Порівняння методів чергування Drop Tail і SFQ як засобу захисту від DDoS-атак 40

ВИСНОВКИ 44

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 46

ПЕРЕЛІК ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

DDoS	— Distributed Denial of Service
DoS	— Denial of Service
UDP	— User Datagram Protocol
TCP	— Transmission Control Protocol
IP	— Internet Protocol
DNS	— Domain Name System
ICMP	— Internet Control Message Protocol
SFQ	— Stochastic Fair Queuing
NS-2	— Network Simulator 2
X-Graph	— Графічний інструмент для візуалізації результатів
ARP	— Address Resolution Protocol
DHCP	— Dynamic Host Configuration Protocol
IDS	— Intrusion Detection System
IPS	— Intrusion Prevention System
PN	— Virtual Private Network
CDN	— Content Delivery Network
WAF	— Web Application Firewall
IoT	— Internet of Things

ВСТУП

Сучасне суспільство переживає стрімкий розвиток цифрових технологій, що охоплює всі сфери життєдіяльності — від бізнесу до державного управління та побуту. У таких умовах інформаційно-комунікаційні системи стали критично важливими елементами інфраструктури, від надійності та безперервності функціонування яких залежить стабільність роботи цілих організацій і галузей. Однією з головних загроз для цих систем залишаються розподілені атаки на відмову в обслуговуванні, відомі як DDoS-атаки. Метою DDoS-атак є виведення з ладу інформаційного ресурсу або сервісу шляхом перевантаження його запитами з багатьох джерел. Внаслідок цього сервер або мережа перестає відповідати на легітимні запити користувачів, що може призвести до фінансових збитків, порушення репутації, втрати даних чи зупинки критичних процесів. Враховуючи постійне вдосконалення методів атак і доступність інструментів для їх здійснення навіть для малокваліфікованих зловмисників, проблема захисту від DDoS залишається надзвичайно актуальною.

DDoS-атаки еволюціонували від простих пакетних атак до складних багаторівневих сценаріїв, що маскуються під легітимний трафік і важко виявляються традиційними засобами захисту. Водночас ринок пропонує різноманітні методи протидії таким загрозам — від локальних рішень на рівні маршрутизаторів до потужних хмарних сервісів, що забезпечують інтелектуальне фільтрування трафіку та автоматичне масштабування захисту. Ефективна реалізація DDoS-захисту вимагає глибокого розуміння як принципів функціонування самих атак, так і механізмів їх виявлення, блокування та пом’якшення наслідків.

Метою дипломної роботи є аналіз методів і технологій захисту від DDoS-атак. Для досягнення цієї мети поставлено такі завдання: узагальнити класифікацію та основні характеристики DDoS-атак; дослідити тенденції розвитку атак та інструментів для їх реалізації; проаналізувати існуючі методи та технології захисту; порівняти ефективність різних підходів; розробити та протестувати прототип системи захисту.

Об’єктом дослідження є процеси забезпечення безпеки інформаційних ресурсів у мережевих середовищах. Предметом дослідження є методи виявлення та запобігання DDoS-атакам з використанням програмних та апаратно-програмних рішень. У роботі застосовано аналітичні, порівняльні та експериментальні методи дослідження. Використано аналіз наукових публікацій, нормативних документів та технічної документації, а також методи моделювання мережевого трафіку для практичної частини.

Дипломна робота складається з трьох розділів. У першому розділі розглянуто теоретичні аспекти DDoS-атак, їх класифікацію, історію та типові приклади. У другому — проаналізовано сучасні методи та технології захисту від атак. У третьому розділі проведено практичне дослідження ефективності різних методів захисту від DDoS-атак на основі моделювання атаки типу Reflection attack у середовищі NS-2. Представлено параметри симуляції, описано обрані сценарії та проаналізовано результати застосування методик запобігання, таких як механізм «чорної діри» (Black hole) та алгоритм стохастичного справедливого планування черг (SFQ). Результати експериментів дозволили оцінити вплив обраних підходів на характеристики мережевого трафіку та ефективність протидії розподіленим атакам на відмову в обслуговуванні.

1 АНАЛІЗ ПРИРОДИ ТА КЛАСИФІКАЦІЇ DDoS-АТАК

1.1 Основні поняття та класифікація DDoS-атак

DDoS-атаки (Distributed Denial of Service) є одним із найнебезпечніших видів кіберзагроз, спрямованих на порушення доступності інформаційних ресурсів. Суть таких атак полягає в створенні надмірного навантаження на цільовий сервер, мережу або сервіс шляхом одночасної генерації великої кількості запитів з різних джерел. Унаслідок цього легітимні користувачі втрачають можливість отримати доступ до ресурсу, що негативно впливає як на роботу окремих систем, так і на бізнес-процеси організацій загалом. На відміну від звичайної DoS-атаки, яка здійснюється з одного джерела, DDoS-атака базується на використанні великої кількості скоординованих пристроїв, часто об’єднаних у ботнет — мережу заражених шкідливим програмним забезпеченням комп’ютерів або IoT-пристроїв, керованих зловмисником (див. рис. 1.1).

Класифікація DDoS-атак здійснюється за кількома критеріями, зокрема за рівнем моделі OSI, на який спрямована атака, за використовуваними протоколами, за способом впливу на систему та за рівнем складності. Залежно від рівня OSI-моделі розрізняють атаки мережевого рівня (L3), транспортного (L4) та прикладного рівня (L7). Атаки мережевого рівня, такі як ICMP Flood або IP Fragmentation Attack, спрямовані на перевантаження пропускної здатності мережі. Транспортний рівень включає атаки типу TCP SYN Flood, UDP Flood, які порушують нормальне встановлення з'єднання. Атаки прикладного рівня, такі як HTTP Flood або Slowloris, імітують легітимну взаємодію з вебсервісом, ускладнюючи їх виявлення традиційними методами.

Окремим видом є атаки, що використовують техніку підсилення (amplification). Такі атаки базуються на використанні відкритих серверів, які відповідають на малі запити великою кількістю даних, наприклад, DNS Amplification або NTP Amplification. Зловмисник підмінює IP-адресу жертви у запиті, внаслідок чого відповідь надходить не йому, а цільовій системі, створюючи великий обсяг небажаного трафіку.

Залежно від рівня складності та координації DDoS-атаки поділяють на низькорівневі (low and slow атаки, які працюють повільно, але стабільно виводять систему з ладу) та високоінтенсивні (які створюють миттєвий та потужний пік навантаження). Також розрізняють одновекторні атаки, що використовують один тип трафіку або один протокол, та багатовекторні, які поєднують декілька способів впливу одночасно для ускладнення захисту.

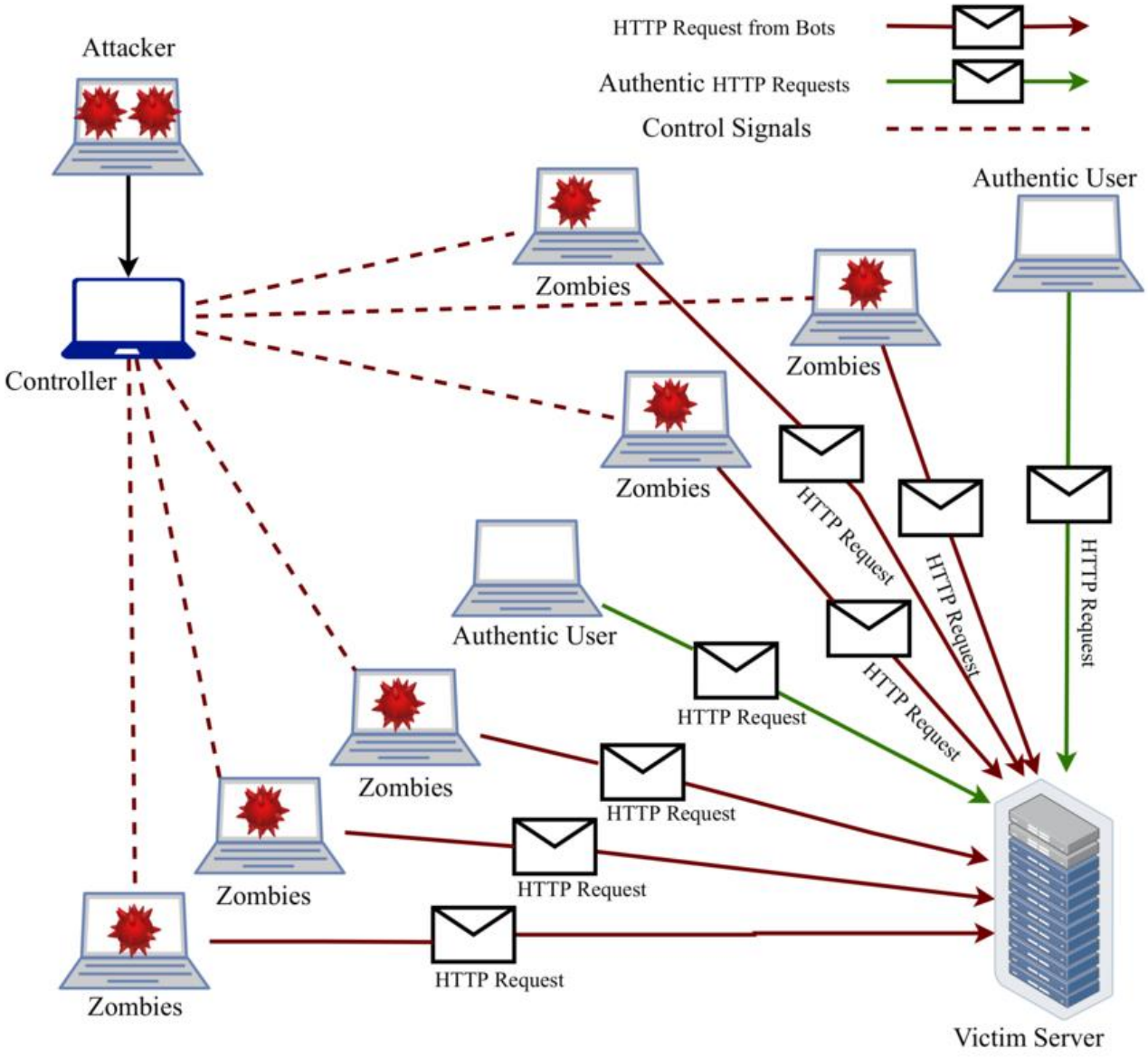

Рисунок 1.1 – Схема роботи DDoS-атаки

У сучасних умовах DDoS-атаки можуть мати різні цілі: від демонстрації протесту або політичного тиску до шантажу, конкурентної боротьби чи дестабілізації критичної інфраструктури. З огляду на постійне зростання масштабів та складності DDoS-загроз, розуміння їх сутності, різновидів і механізмів є необхідною передумовою для розробки ефективних систем захисту.

1.2 Історія розвитку та тенденції DDoS-атак

Перші відомі випадки атак на відмову в обслуговуванні з'явилися ще в 1990-х роках, коли інтернет лише починав набирати обертів. Однією з перших зафіксованих DoS-атак вважається інцидент 1996 року, коли панк-хакер Джо Ірасіа (Jester) атакував сервери Лос-Анджелеської газети. Проте справжній резонанс викликали події лютого 2000 року, коли низка великих інтернет-компаній, зокрема Yahoo!, Amazon, CNN та eBay, зазнали масштабних DDoS-атак. Тоді атаки були здійснені з використанням заздалегідь заражених комп'ютерів, що стало початком епохи розповсюдження ботнетів.

У подальші роки DDoS-атаки набували дедалі більшого масштабу та складності. У 2007 році світ побачив перші приклади кібервійн, коли Естонія зазнала масованих DDoS-атак, що паралізували роботу банків, державних установ та ЗМІ. Це стало поворотним моментом у розумінні того, що подібні атаки можуть використовуватися як інструмент політичного чи військового впливу. У 2010-х роках активізувалися численні хактивістські угруповання, такі як Anonymous чи Lizard Squad, які неодноразово вдавалися до DDoS-атак у відповідь на політичні події чи рішення корпорацій.

З 2016 року спостерігається новий етап еволюції загрози — використання Інтернету речей (IoT) для створення надпотужних ботнетів. Прикладом цього є ботнет Mirai, який інфікував тисячі слабо захищених IoT-пристроїв і використав їх для атаки на DNS-провайдера Dyn, що спричинило перебої в роботі таких сервісів, як Twitter, Netflix, Spotify та GitHub. Особливість Mirai полягала в автоматизованому пошуку вразливих пристроїв і простоті експлуатації, що зробило цей підхід популярним серед зловмисників.

У подальші роки масштаби атак продовжували зростати. Зафіксовано випадки, коли інтенсивність DDoS-атак перевищувала 2,5 Тбіт/с. Паралельно удосконалювалися методи обходу класичних захисних механізмів, зокрема застосовувалися багатовекторні атаки, комбінації з іншими типами атак, а також техніки шифрування трафіку для ускладнення виявлення.

Сучасні тенденції свідчать про зростання автоматизації атак, використання штучного інтелекту для адаптації сценаріїв атаки в реальному часі, а також

активізацію діяльності кіберзлочинних сервісів на умовах DDoS-as-a-Service. Такі сервіси пропонують можливість запуску атак за оплату, без необхідності мати технічні навички, що значно розширює коло потенційних зловмисників.

Очевидно, що DDoS-атаки перетворилися з технічного експерименту окремих хакерів на інструмент організованої злочинності, економічного шантажу та кіберзбройного тиску. Це вимагає постійного оновлення знань, розвитку нових технологій захисту та глобального співробітництва між державами, бізнесом і фахівцями з кібербезпеки.

1.3 Основні методи реалізації атак

Методи реалізації DDoS-атак надзвичайно різноманітні. Вони можуть відрізнятися за рівнем мережевої моделі (OSI), на якому здійснюється атака, типом протоколів, що використовуються, складністю реалізації, а також рівнем замаскованості. Основна мета — зробити інтернет-сервіс, вебсайт або сервер недоступним для легітимних користувачів шляхом вичерпання обчислювальних ресурсів, пропускної здатності каналів або логіки обробки запитів. Існують такі найбільш поширені типи методів реалізації DDoS-атак:

1) Атаки на мережевому рівні (L3–L4)

Ці атаки спрямовані на перевантаження інфраструктурних ресурсів, таких як маршрутизатори, фаєрволи або канали зв’язку. Вони, як правило, генерують великий обсяг однотипного трафіку.

– TCP SYN Flood – полягає у надсиланні великої кількості TCP SYN-пакетів до цільового сервера без завершення тристороннього «рукостискання». Це призводить до накопичення напіввідкритих з’єднань і вичерпання пулу доступних ресурсів.

– UDP Flood – реалізується шляхом масової відправки UDP-пакетів на випадкові порти. Оскільки UDP є безз’єднувальним протоколом, сервер відповідає ICMP-повідомленнями про недоступність, що призводить до перевантаження.

– ICMP Flood (Ping Flood) – використовує потоки ICMP Echo-запитів, які заповнюють смугу пропускання або ресурси системи. Якщо система не має належного фільтрування, вона може швидко вийти з ладу.

– Ping of Death – атака, що базується на надсиланні фрагментованих ICMP-пакетів з неправильною довжиною. При їх обробці можуть виникати збої у функціонуванні операційної системи.

2) Атаки з підсиленням (amplification attacks)

Ці атаки використовують уразливі або відкриті сервери для генерації надмірного трафіку на адресу жертви.

– DNS Amplification – атакуючий надсилає невеликий DNS-запит до відкритого DNS-сервера, підставляючи IP-адресу жертви. Відповідь у десятки разів більша за розміром, що дозволяє значно підсилити атаку.

– NTP Amplification – аналогічна логіка використовується із сервером Network Time Protocol. Команди типу “monlist” можуть створювати великі обсяги вихідного трафіку.

– Memcached Amplification – одна з найнебезпечніших форм атак з коефіцієнтом підсилення понад 50000. Вразливі Memcached-сервери відповідають великими об’ємами даних на підставний запит.

3) Атаки на прикладному рівні (L7).

Ці атаки імітують реальні дії користувачів, роблячи їх надзвичайно складними для виявлення та блокування.

– HTTP Flood – багаторазове надсилання запитів GET або POST на вебсервер, що призводить до перевантаження вебдодатку або бази даних. Часто використовуються автоматизовані скрипти або ботнети.

– Slowloris – повільно відкриває численні HTTP-з’єднання та надсилає заголовки надзвичайно повільно, утримуючи ці з’єднання відкритими якнайдовше. Це блокує доступ для нових легітимних користувачів.

– Low and slow – загальна назва для атак, які характеризуються повільним і тривалим трафіком. Їх мета — залишатися непомітними для традиційних засобів виявлення, не створюючи різкого піку навантаження.

4) Багатовекторні атаки

Сучасні DDoS-атаки все частіше реалізуються як комбінація декількох методів одночасно. Наприклад, може бути поєднано:

• UDP Flood для перевантаження мережевих каналів

• DNS Amplification для підсилення обсягів трафіку

• HTTP Flood для навантаження вебдодатку

Такі атаки ускладнюють виявлення, оскільки створюють навантаження на різних рівнях — від транспортного до прикладного.

5) Використання ботнетів і IoT.

Для реалізації більшості DDoS-атак сьогодні використовуються ботнети — великі мережі інфікованих пристроїв, які керуються централізовано або через P2P-механізми. Особливо активно використовуються пристрої Інтернету речей (IoT), які часто мають слабкий захист і погано налаштовану безпеку.

– Ботнети, такі як Mirai, показали вражаючу ефективність, залучаючи тисячі або навіть мільйони пристроїв для одночасної атаки.

– Інфікування зазвичай здійснюється через стандартні логіни/паролі або відомі вразливості у ПЗ, після чого пристрій стає «солдатом» у мережі ботнету.

6) Сучасні техніки обходу захисту.

Зловмисники дедалі частіше використовують технології обходу захисту:

– IP spoofing – підміна IP-адрес для ускладнення фільтрації трафіку.

– Encrypted attacks (TLS flood) – атаки, які використовують зашифрований трафік для обхід традиційних фільтрів. Розшифрування такого трафіку потребує додаткових ресурсів.

– Geo-distributed traffic – трафік генерується з різних географічних регіонів, щоб знизити ефективність гео-фільтрації.

– Attack randomization – варіація вмісту запитів для уникнення виявлення за сигнатурами.

Таким чином, методи реалізації DDoS-атак охоплюють повний спектр технік — від простих перевантажень на мережевому рівні до складних, маскованих атак на прикладному рівні. Розуміння цих технік є критично важливим для ефективного виявлення, профілактики та реагування на інциденти, пов’язані з DDoS. У сучасному цифровому середовищі жодна організація не може вважати себе повністю захищеною без постійного аналізу нових векторів атак та оновлення захисних систем.

1.4 Типові наслідки для інфраструктури

DDoS-атаки становлять одну з найнебезпечніших кіберзагроз для сучасних інформаційних систем. Їхній головний цільовий ефект — виведення з ладу онлайн-сервісів, що критично важливо як для бізнесу, так і для державних установ. Проте наслідки таких атак не обмежуються лише тимчасовою втратою доступу до сайту. У сучасних умовах комплексного розвитку цифрових сервісів DDoS-атаки можуть мати довгостроковий і багатогранний вплив на всю IT-інфраструктуру організації.

Щоб наочно продемонструвати типи можливих наслідків DDoS-атак та їх прояви, нижче наведено узагальнену таблицю 1.1:

Таблиця 1.1 - Наслідки для інфраструктури від DDoS-атак

Тип наслідку	Прояв атаки	Конкретні приклади	Можливі наслідки
Технічні	Перевантаження мережі, збої сервісів	Відмова серверів, timeout при завантаженні сайтів, збільшення часу відповіді	Втрата доступності сервісів, вихід з ладу маршрутизаторів або балансувальників
Фінансові	Зупинка онлайн-продажів або транзакцій	Неможливість обробки покупок в інтернет-магазині або банківських операцій	Прямі фінансові втрати, штрафи за невиконання SLA, додаткові витрати на відновлення

Подовження таблиці 1.1

Репутаційні	Невдоволення клієнтів, негатив у ЗМІ або соцмережах	Хештеги про збій у Twitter, скарги у Google Play/App Store	Втрата довіри, зменшення клієнтської бази, перехід користувачів до конкурентів
Організаційні	Перевантаження команд підтримки та безпеки	Позапланові нічні чергування, авральна робота персоналу	Виснаження працівників, зниження ефективності, зростання кількості помилок
Інфраструктурні	Необхідність оновлення систем, переходу на нові рішення	Закупівля потужнішого обладнання, підключення до CDN, впровадження хмарних WAF	Значні капітальні витрати, зміна архітектури, перехід на дорогі рішення
Юридичні та регуляторні	Порушення норм законодавства або вимог з кібербезпеки	Зрив вимог GDPR, NIS2 або українських норм у сфері захисту критичної інфраструктури	Штрафи, перевірки, призупинка діяльності, втрата ліцензій

1.5 Сучасні приклади DDoS-атак

Сучасний ландшафт DDoS-атак постійно змінюється, відзначаючись зростанням масштабу, складності та різноманітності застосованих технік. Кіберзлочинці дедалі частіше поєднують різні вектори атак, використовують автоматизовані інструменти, ботнети на базі IoT-пристроїв і навіть хмарну

інфраструктуру для збільшення ефективності своїх дій. Нижче наведено кілька найбільш резонансних прикладів останніх років, що ілюструють сучасні тенденції у цій сфері.

Одним із найбільш відомих інцидентів стала атака на інфраструктуру компанії Dyn у жовтні 2016 року. Ця атака була реалізована за допомогою ботнету Mirai, який складався з великої кількості заражених пристроїв Інтернету речей (IoT), таких як веб-камери, маршрутизатори та цифрові відеореєстратори. Загальний обсяг трафіку перевищував 1 Тбіт/с, що призвело до значних перебоїв у роботі популярних інтернет-сервісів, таких як Twitter, Netflix, Reddit та інших. Цей випадок наочно продемонстрував вразливість poorly-secured IoT-пристроїв і необхідність їхнього захисту на рівні прошивок та налаштувань за замовчуванням.

Ще одним значущим прикладом стала атака на Amazon Web Services (AWS) у лютому 2020 року. Потужність атаки досягла рекордного показника у понад 2,3 Тбіт/с, що зробило її на той момент найбільшою DDoS-атакою в історії. Напад тривав близько трьох днів і був реалізований із використанням reflection-атаки через протокол CLDAP (Connectionless Lightweight Directory Access Protocol), що дозволяє значно збільшити обсяг трафіку за рахунок мультиплікації запитів. Попри успішне відбиття атаки з боку AWS, цей інцидент привернув увагу до ризиків навіть для гіпермасштабних провайдерів хмарних сервісів.

У 2020 році під багатовекторну DDoS-атаку потрапила також криптовалютна біржа Coinbase. Атака комбінувала UDP Flood, TCP SYN Flood, HTTP Flood і навіть короткі хвилі TLS-атаки, спрямовані на виснаження ресурсів TLS-обробки. Завдяки добре налаштованим захисним механізмам та оперативним діям команди безпеки вдалося уникнути критичних збоїв у роботі біржі. Проте інцидент ще раз засвідчив, що навіть компанії з високим рівнем захисту залишаються потенційними мішенями.

Особливу увагу привертають DDoS-атаки з політичним підтекстом. Яскравим прикладом стала серія атак на урядові сайти Естонії у 2019 році, яка стала продовженням кібератак ще з 2007 року. Напади мали на меті тимчасове виведення з ладу онлайн-сервісів уряду, банківських структур, засобів масової

інформації та комунікаційних платформ. Було використано як класичні методи об’ємного перевантаження каналів, так і цільові атаки на конкретні вебсервіси з метою порушення їхньої функціональності.

У 2022 році стало відомо про DDoS-атаки, організовані хактивістськими угрупованнями, на інфраструктуру кількох західноєвропейських аеропортів. У цьому випадку атаки мали на меті не знищення або крадіжку даних, а виключно порушення доступності онлайн-сервісів бронювання, розкладів рейсів та інформаційних порталів. Такі дії свідчать про розширення переліку цілей кібератак на критичну інфраструктуру, особливо у контексті зростаючих геополітичних напружень.

У 2023 році відбулося кілька скоординованих атак на фінансові установи у країнах Східної Європи. Під удар потрапили онлайн-банкінг, мобільні додатки та сайти банків. Частина атак супроводжувалася вимогами викупу, що класифікує їх як DDoS-for-ransom (RDoS). Подібні інциденти створюють серйозні ризики для стабільної роботи банківського сектору, а також викликають недовіру користувачів до цифрових сервісів.

Ще одним показовим випадком стала атака на популярну ігрову платформу Blizzard у 2023 році, яка викликала тимчасову недоступність серверів і унеможливила вхід до ігор для мільйонів користувачів по всьому світу. Атака була реалізована через ботнет, який використовував проксі-з'єднання для приховування джерел трафіку, ускладнюючи фільтрацію.

Таким чином, сучасні приклади DDoS-атак демонструють зростання їхньої потужності, високий рівень координації, а також використання новітніх технічних прийомів. Атаки можуть бути спрямовані як на державні, так і на приватні структури, мати економічне, політичне або хактивістське підґрунтя. Це вимагає від організацій постійного вдосконалення засобів виявлення, нейтралізації та протидії таким загрозам. Ефективна боротьба з DDoS-атаками можлива лише за умов поєднання сучасних технологій захисту, глобальної кооперації фахівців з кібербезпеки та обізнаності користувачів щодо основ кібергігієни.

1.6 Чому DDoS-атаки залишаються привабливими для зловмисників

DDoS-атаки продовжують залишатися одним із найпоширеніших інструментів кіберзлочинців попри розвиток сучасних систем захисту. Їхня популярність зумовлена низкою об’єктивних причин, які охоплюють технічні, економічні, організаційні та психологічні аспекти.

Перш за все, привабливість DDoS-атак полягає у відносній технічній простоті їх реалізації. Зловмисникам не обов’язково володіти глибокими технічними знаннями чи мати доступ до спеціалізованого програмного забезпечення. У відкритому доступі або на чорному ринку існує значна кількість готових інструментів та сервісів, що дозволяють запускати атаки навіть користувачам без відповідної підготовки. Зокрема, так звані сервіси DDoS-as-a-Service пропонують оренду потужностей ботнетів за доступними цінами, що фактично робить атаку товаром, який можна замовити онлайн.

Ще одним важливим фактором є широке поширення вразливих пристроїв, особливо в сегменті Інтернету речей (IoT). Багато таких пристроїв мають слабкий рівень безпеки: типові паролі, відсутність оновлень прошивки або взагалі мінімальний захист. Це дає змогу легко долучити їх до ботнетів, які згодом використовуються для DDoS-атак.

DDoS також приваблює через високу анонімність виконавців. Зловмисники часто використовують проксі-сервери, VPN, Tor або ботнети, що ускладнює ідентифікацію справжніх організаторів. Це мінімізує юридичні ризики для нападників і робить такі атаки ще безпечнішими для них.

Крім технічної доступності, атаки мають і психологічну складову. Вони нерідко застосовуються для шантажу, протесту чи залякування. Наприклад, деякі хактивісти атакують урядові або корпоративні ресурси як форму політичного висловлення. Інші надсилають жертвам попередження про можливу атаку з вимогою сплатити «викуп». Навіть якщо атака не досягає мети, сам факт загрози викликає стрес і невизначеність.

З економічної точки зору, DDoS-атаки вигідні:

- зловмисники можуть досягати значного ефекту за мінімальних витрат,

- організаціям, навпаки, необхідно інвестувати значні кошти в інфраструктуру, фахівців, захисні технології, резервні канали та відновлення.

Таке співвідношення витрат і результату робить DDoS-атаки привабливими з позиції економічної ефективності.

Нарешті, не варто недооцінювати соціальний аспект. Для деяких осіб, особливо в онлайн-спільнотах, успішна атака є способом самоствердження. У мережі неодноразово фіксувалися випадки, коли зловмисники публічно хизувалися скриншотами недоступних сайтів або залишали повідомлення на форумах у стилі «трофеїв».

Таким чином, DDoS-атаки залишаються популярними через поєднання таких факторів: простота реалізації, можливість використання вразливих пристроїв, складність ідентифікації виконавця, психологічний вплив, економічна вигода та соціальний резонанс. Це створює постійну загрозу для інформаційних систем різного рівня й вимагає впровадження комплексних підходів до запобігання, виявлення та протидії таким атакам.

2 МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ ВІД DDos-АТАК

2.1 Принципи побудови систем захисту

Побудова ефективних систем захисту від DDoS-атак базується на низці ключових принципів, що дозволяють забезпечити не лише надійність, але й масштабованість, адаптивність та оперативність захисних заходів. Ці принципи визначають загальну архітектуру, логіку роботи та інструментарій системи, що дає змогу ефективно протидіяти постійно ускладненим та різноманітним атакам.

Перш за все, системи захисту мають бути здатними до швидкого і достовірного виявлення аномальної активності у мережевому трафіку. Це означає, що вони повинні використовувати комплексний моніторинг у реальному часі, який включає збір та аналіз статистичних даних про потоки трафіку, пакети, типи запитів та їхню поведінку. Важливим є також застосування методів аналізу поведінкових патернів, які допомагають відокремити легітимний трафік від трафіку, що генерується в ході атаки. Такий підхід дозволяє знизити кількість хибних спрацьовувань та уникнути зайвого блокування користувачів.

Другий важливий принцип полягає в багатоетапності та багаторівневості захисту. Ефективна система захисту повинна включати кілька рівнів фільтрації і контролю трафіку. На мережевому рівні відбувається первинне відсіювання зайвого або підозрілого трафіку, наприклад, шляхом блокування IP-адрес, які виявилися джерелом атаки, або відсіювання пакетів з підозрілими параметрами. Наступний рівень – транспортний, де аналізуються особливості сесійного трафіку, а також застосовуються методи фільтрації за протоколами. На прикладному рівні здійснюється глибокий аналіз конкретних запитів, що надходять до серверів, що дозволяє відфільтрувати атаки на веб-додатки, наприклад HTTP-флуд або SYN-флуд. Такий багаторівневий підхід значно підвищує стійкість системи, дозволяє враховувати різні типи атак і оперативно адаптувати заходи реагування.

Третій принцип — масштабованість системи захисту. У разі DDoS-атаки обсяг трафіку, що генерується зловмисниками, може досягати сотень гігабітів або навіть терабітів на секунду, що значно перевищує нормальні навантаження.

Тому захисна система повинна мати можливість динамічно масштабувати свої обчислювальні ресурси та пропускну здатність. Це досягається за допомогою розподілених архітектур, хмарних технологій та кластеризації. Масштабованість дозволяє не лише витримувати атаки великої інтенсивності, а й ефективно розподіляти навантаження між різними центрами обробки даних.

Четвертий принцип — автоматизація процесів реагування. У реальних умовах кіберзагроз швидкість реагування є критичною, оскільки атака може призвести до відмови сервісів вже за кілька хвилин. Ручне втручання у більшості випадків є надто повільним і неефективним. Тому сучасні системи захисту використовують автоматизовані механізми, які можуть виявляти аномалії, приймати рішення про блокування або обмеження трафіку без участі людини. Водночас такі системи мають підтримувати баланс між безпекою і доступністю послуг, щоб не допустити помилкового блокування легітимних користувачів.

П’ятий принцип — гнучкість та адаптивність. Загрози у кіберпросторі постійно еволюціонують, з’являються нові види атак і методи обходу захисту. Тому системи повинні мати змогу оперативно оновлювати свої правила та алгоритми на основі аналізу нових загроз. Важливим напрямом у цьому є інтеграція сучасних технологій штучного інтелекту, машинного навчання та поведінкового аналізу. Ці технології дозволяють не лише автоматично виявляти раніше невідомі атаки, але й прогнозувати потенційні ризики, що підвищує загальну ефективність захисту.

Нарешті, системи захисту мають інтегруватися з іншими компонентами безпеки та мережевою інфраструктурою організації. Це забезпечує комплексний підхід до кіберзахисту і дозволяє координувати роботу між фаєрволами, системами виявлення вторгнень, антивірусним програмним забезпеченням, проксі-серверами та хмарними платформами. Така взаємодія підвищує рівень безпеки, дозволяючи швидше виявляти інциденти і мінімізувати їхні наслідки.

Таким чином, принципи побудови систем захисту від DDoS-атак базуються на поєднанні швидкого виявлення загроз, багаторівневої фільтрації, масштабованості, автоматизації, гнучкості та інтеграції з іншими захисними засобами. Виконання цих принципів є ключовим фактором для забезпечення

стійкості та безперервності функціонування інформаційної інфраструктури в умовах постійно зростаючих кіберзагроз.

2.2 Методи виявлення атак

Методи виявлення DDoS-атак є одним із фундаментальних елементів сучасних систем захисту, оскільки своєчасне та точне розпізнавання аномалій у мережевому трафіку є ключовим для запобігання масштабним збоям у роботі сервісів. Ці методи базуються на ретельному аналізі різноманітних параметрів трафіку, а також поведінки користувачів і мережевих пристроїв, що дозволяє виявляти ознаки атаки на ранніх етапах.

Сучасні підходи до виявлення DDoS-атак поєднують класичні технології з новітніми методами штучного інтелекту, що значно підвищує їхню ефективність. Одним із найпоширеніших традиційних засобів є системи виявлення вторгнень (IDS), які здійснюють моніторинг мережевого трафіку або логів систем для виявлення характерних ознак атак. IDS бувають:

- Сигнатурні — використовують шаблони (сигнатури) відомих атак. Ефективні проти вже вивчених загроз, але не здатні виявляти нові або модифіковані варіанти.
- Аномалійні — орієнтуються на виявлення відхилень від «нормальної» поведінки мережі. Перевагою є здатність виявляти нові атаки, але вони потребують точного налаштування, інакше можуть генерувати хибні спрацювання.

Поведінковий аналіз — ще один важливий підхід, який ґрунтується на вивченні типової активності користувачів, пристроїв і сервісів. Наприклад, відстежуються:

- інтенсивність запитів,
- тривалість сесій,
- розподіл IP-адрес,
- частота певних операцій.

Значні відхилення від цих норм можуть свідчити про потенційну DDoS-атаку, особливо якщо йдеться про багатовекторні атаки (SYN-флуд, HTTP-флуд тощо), які маскуються під легітимну активність.

Із розвитком машинного навчання (ML) можливості виявлення атак значно розширилися. Використання ML дає змогу автоматично будувати моделі звичайної поведінки та виявляти аномалії в режимі реального часу. Застосовуються такі підходи:

1) Кластеризація — для групування трафіку та виявлення «випадань» з кластерів.
2) Методи опорних векторів (SVM) — добре працюють для розділення «нормального» і «аномального» трафіку.
3) Нейронні мережі — здатні ловити складні залежності у даних, що корисно при виявленні складних атак.
4) Ансамблеві методи — поєднують декілька моделей для підвищення точності.

Комбінований підхід, що поєднує IDS, поведінковий аналіз і ML, дозволяє підвищити точність і адаптивність системи виявлення. Сучасні рішення також часто використовують багаторівневий аналіз:

- мережевий рівень (пакети, порти, протоколи),
- прикладний рівень (HTTP, DNS тощо).

Це допомагає зменшити кількість хибних спрацювань і підвищити ефективність реагування.

Крім того, важливу роль відіграють механізми колективного аналізу загроз, коли дані про аномалії централізовано збираються, обробляються й використовуються для оновлення систем захисту у масштабах організації чи навіть глобально (наприклад, через хмарні платформи).

Отже, ефективне виявлення DDoS-атак базується на синергії класичних підходів, поведінкового аналізу та інтелектуальних алгоритмів, що забезпечує високу швидкість, точність і гнучкість захисних систем у сучасному мережевому середовищі.

2.3 Технології захисту

Сучасні технології захисту від DDoS-атак передбачають застосування комплексних механізмів фільтрації, контролю трафіку та обмеження доступу, які дозволяють не лише зменшити навантаження на мережеву інфраструктуру, але й

зберегти безперервність та стабільність роботи критично важливих сервісів і додатків. Успішний захист базується на багаторівневому підході, який поєднує різні методи і технології, що доповнюють одна одну.

Однією з базових і найпоширеніших технологій є фільтрація пакетів, яка реалізується на рівні мережевих пристроїв — маршрутизаторів, фаєрволів, проксі-серверів та спеціалізованих систем захисту. Принцип її роботи полягає в ідентифікації та блокуванні шкідливих пакетів, які відповідають певним правилам. Ці правила можуть базуватися на різних критеріях: IP-адреси джерела чи призначення, порти, мережеві протоколи (TCP, UDP, ICMP), а також специфічні сигнатури трафіку, характерні для різних типів DDoS-атак. Наприклад, при атаках SYN flood можна налаштувати фільтри, які обмежують кількість незавершених TCP-з'єднань від одного IP-адреса, що дозволяє запобігти вичерпанню ресурсів сервера.

Ще одним важливим інструментом є механізм rate limiting (обмеження швидкості), який контролює кількість запитів або пакетів, що надходять від одного джерела за певний проміжок часу. Цей метод дозволяє розподіляти навантаження рівномірно, не даючи зловмисникам перевантажувати сервер або мережеве обладнання. Rate limiting особливо ефективний проти атак типу HTTP flood, SYN flood, UDP flood та інших, де відбувається масове надсилання запитів з метою виснажити ресурси. Сучасні системи забезпечують гнучке налаштування порогів для різних типів трафіку або окремих сервісів, що дозволяє адаптувати захист під конкретні умови та мінімізувати вплив на легітимних користувачів.

Blackholing (або «чорна діра») — це радикальний, але часто необхідний метод захисту, який полягає у перенаправленні підозрілого або надмірного трафіку на невідповідний IP-адрес, де він ігнорується і не досягає цільового сервера. Такий підхід дозволяє оперативно розвантажити мережу під час масштабних DDoS-атак, що загрожують повним відмовленням у обслуговуванні. Однак цей метод має суттєвий недолік — можливе блокування частини легітимного трафіку, що може негативно вплинути на користувацький досвід та

бізнес-процеси. Тому blackholing зазвичай застосовується як крайній захід, коли інші методи не дають достатнього результату.

Крім зазначених, широко застосовуються технології stateful inspection — аналіз стану мережевих сесій, який дає змогу більш точно відрізняти легітимний трафік від шкідливого. На відміну від простих пакетних фільтрів, stateful inspection відслідковує повний контекст мережевої сесії (стан TCP-з'єднання, послідовність пакетів тощо), що допомагає уникнути помилкових блокувань і підвищує ефективність виявлення атак.

Важливе значення мають також методи фільтрації, засновані на поведінкових ознаках. Вони базуються на аналізі нетипових моделей трафіку, частоти та послідовності запитів, що дозволяє виявляти складні багатовекторні атаки, які часто не піддаються традиційній фільтрації. Інтеграція цих методів із системами виявлення атак (IDS/IPS) створює більш адаптивний та інтелектуальний захист, здатний своєчасно реагувати на нові загрози.

Крім технічних методів, у сучасних системах захисту застосовуються також хмарні сервіси DDoS-міттінгу (scrubbing), які перенаправляють трафік через глобальну мережу дата-центрів для очищення від шкідливих потоків. Ці сервіси здійснюють глибокий аналіз трафіку на основі поведінкових моделей і машинного навчання, що забезпечує масштабований і ефективний захист навіть від дуже потужних атак.

Загалом, комбінування технологій фільтрації пакетів, rate limiting, blackholing, stateful inspection, поведінкового аналізу та інтеграції з IDS створює багаторівневі системи захисту. Вони здатні ефективно протистояти широкому спектру DDoS-атак, забезпечуючи баланс між надійністю блокування шкідливого трафіку і мінімальним впливом на роботу легітимних користувачів і бізнес-процесів. Такий підхід дозволяє організаціям підтримувати стабільність роботи своїх мереж і сервісів навіть у складних умовах кібератак (див. рис. 2.1).

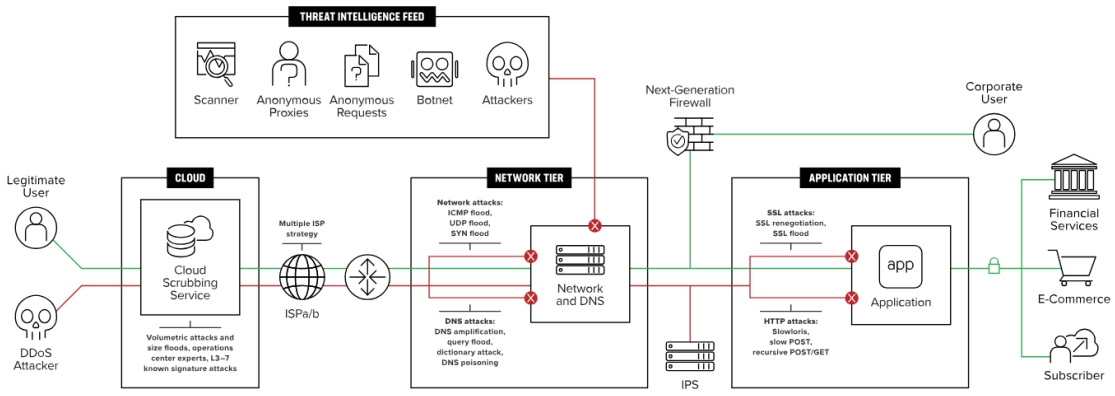

Рисунок 2.1 – Приклад схеми захисту від DDos-атак

2.4 Хмарні сервіси та інфраструктурні рішення

У сучасних умовах стрімкого зростання кіберзагроз та масштабних DDoS-атак, хмарні сервіси та інфраструктурні рішення стали одними з найефективніших і найпоширеніших засобів захисту мережевих ресурсів та інформаційних систем. Використання хмарних платформ дає змогу динамічно масштабувати захисні механізми у режимі реального часу, адаптуючись до поточної інтенсивності атак, а також розподіляти трафік і навантаження між великою кількістю дата-центрів по всьому світу. Такий підхід забезпечує не лише високий рівень захисту, а й покращує продуктивність та доступність сервісів для кінцевих користувачів.

Одним із ключових компонентів сучасних інфраструктурних рішень є мережі доставки контенту (Content Delivery Network, CDN). CDN забезпечують кешування статичного та динамічного контенту на численних серверних вузлах, розташованих ближче до користувачів. Це дозволяє значно знизити навантаження на основні сервери, розподіляючи вхідні запити по глобальній мережі. Крім того, CDN активно пом’якшують вплив DDoS-атак, оскільки атаки розпорошуються по численних точках присутності мережі, що ускладнює зловмисникам сконцентрувати потік шкідливих запитів на одному вузлі. За допомогою CDN можна швидко адаптуватися до змін у схемах атаки та забезпечувати стабільність роботи навіть у разі потужних DDoS-флудів.

Важливою складовою багаторівневої системи захисту є веб-аплікаційні фаєрволи (Web Application Firewall, WAF). WAF аналізують HTTP/HTTPS

трафік, виявляючи та блокуючи різноманітні шкідливі запити, такі як SQL-ін’єкції, крос-сайтові скриптові атаки (XSS), атаки на сесійну безпеку, а також численні варіанти DDoS-атак на прикладному рівні. WAF може бути розгорнутий як на стороні самого сервера, так і в хмарі, що дозволяє гнучко інтегрувати його в існуючу IT-інфраструктуру. Хмарні WAF-сервіси, зокрема, мають перевагу швидкого оновлення сигнатур, масштабованості та можливості працювати як розподілений фільтр, що забезпечує додатковий рівень безпеки.

Технологія Anycast — це ще один потужний інструмент у арсеналі хмарних сервісів захисту. Вона базується на принципі, коли один і той самий IP-адрес присвоюється кільком географічно розташованим серверам або дата-центрам. Запити користувачів автоматично маршрутизуються до найближчого або найменш навантаженого сервера. Це дозволяє не лише підвищити швидкість доставки контенту та доступність сервісів, але й ефективно розподіляти навантаження під час DDoS-атак. За допомогою Anycast трафік зловмисників розсіюється по різних вузлах, що суттєво знижує ефективність атак і допомагає уникнути «завантаження» окремих точок.

Не менш важливу роль у захисті відіграють проксі-сервери, які працюють як проміжні ланки між клієнтами та основними серверами. Вони здатні фільтрувати трафік, кешувати запити та відповіді, що значно розвантажує внутрішні ресурси. Крім того, проксі-сервери приховують реальні IP-адреси серверів, що робить неможливим пряме цілеспрямоване сканування чи атаки на внутрішню інфраструктуру. Поєднання проксі із CDN, Anycast та WAF формує багаторівневу систему захисту, яка підвищує загальну стійкість та забезпечує надійне відбиття атак різної інтенсивності.

Окремо варто відзначити, що сучасні хмарні сервіси захисту часто інтегрують автоматизовані системи моніторингу та аналізу трафіку з елементами штучного інтелекту і машинного навчання. Вони здатні виявляти аномалії в мережевому трафіку, прогнозувати потенційні загрози і оперативно застосовувати заходи захисту. Це дозволяє не лише реагувати на атаки у реальному часі, але й підвищувати ефективність системи захисту в

довгостроковій перспективі. Узагальнену інформацію про хмарні технології для захисту від DDoS-атак наведено в таблиці 2.1:

Таблиця 2.1 - Порівняння хмарних технологій для захисту від DDoS-атак

Технологія / Сервіс	Основна функція	Переваги	Обмеження / Особливості
CDN	Розподіл контенту, кешування запитів	Зменшення навантаження, георозподілення, пом'якшення DDoS	Не блокує атаки напряму, а лише знижує їх ефект
WAF	Аналіз HTTP/HTTPS трафіку, фільтрація шкідливих запитів	Захист на прикладному рівні, гнучка конфігурація, швидке оновлення правил	Потребує налаштування, можливі хибні спрацювання
Anycast	Розподіл трафіку до найближчих серверів	Підвищення доступності, балансування навантаження	Потребує глобальної інфраструктури
Проксі-сервери	Посередник між клієнтом і сервером, приховування IP	Фільтрація, кешування, захист бекенду	Не захищає повністю без інтеграції з іншими засобами
ML/AI-аналітика	Виявлення аномалій у трафіку, прогнозування атак	Адаптивність, робота в реальному часі	Потребує якісних даних, складність налаштування

Таким чином, хмарні сервіси та інфраструктурні рішення — такі як CDN, WAF, Anycast, проксі-сервери, а також сучасні аналітичні платформи — є невід’ємною частиною сучасних стратегій захисту від DDoS-атак. Вони забезпечують необхідну масштабованість, гнучкість та високу ефективність навіть в умовах постійно зростаючих загроз, допомагаючи організаціям підтримувати стабільність і безперервність своїх онлайн-сервісів.

3 АНАЛІЗ ЕФЕКТИВНОСТІ МЕТОДІВ ЗАХИСТУ ВІД DDos-АТАК

3.1 Опис параметрів та сценаріїв симуляції

У цьому підрозділі представлено опис параметрів та сценаріїв симуляції, що були використані для моделювання DDoS-атаки типу Reflection attack. Варто зазначити, що наведені результати і параметри симуляції взяті із раніше підготовлених науково-технічних матеріалів та адаптовані для проведення аналізу ефективності застосування методів захисту від розподілених атак на відмову в обслуговуванні. Дослідження проводилося із застосуванням платформи ns-2, графічного інструменту X-graph, а також операційної системи Ubuntu 14.04 LTS.

У контексті цієї роботи під атакою типу Reflection attack мається на увазі різновид DDoS-атаки, в якому зловмисник використовує проміжні вузли — так звані "відбивачі" — для генерації великого обсягу трафіку на адресу жертви. Особливістю такої атаки є те, що сам атакувальник не звертається безпосередньо до цільової системи. Натомість він надсилає підроблені запити до скомпрометованих або відкритих UDP-серверів, вказуючи у заголовках IP-адресу жертви як адресу відправника. У результаті відповідь на запит автоматично пересилається до жертви, створюючи ефект "відбиття".

У змодельованому сценарії роль таких "відбивачів" відіграють зомбі-машини, які інтенсивно генерують UDP-трафік до сервера, з імітацією підробки джерела трафіку. Завдяки простоті UDP-протоколу, який не вимагає встановлення з'єднання або перевірки автентичності, подібні атаки легко реалізовуються та важко фільтруються без втрат легітимного трафіку. Саме цей принцип було використано для побудови симуляційної моделі, яка дозволяє дослідити вплив таких атак на пропускну здатність мережі та ефективність різних чергувальних алгоритмів (наприклад, Drop Tail і Stochastic Fair Queuing) у точках маршрутизації.

Для моделювання були обрані два основні сценарії. Перший сценарій включає одного атакувальника, три «зомбі» (компрометовані машини) і шість клієнтів, які генерують звичайний трафік (див. рис. 3.1).

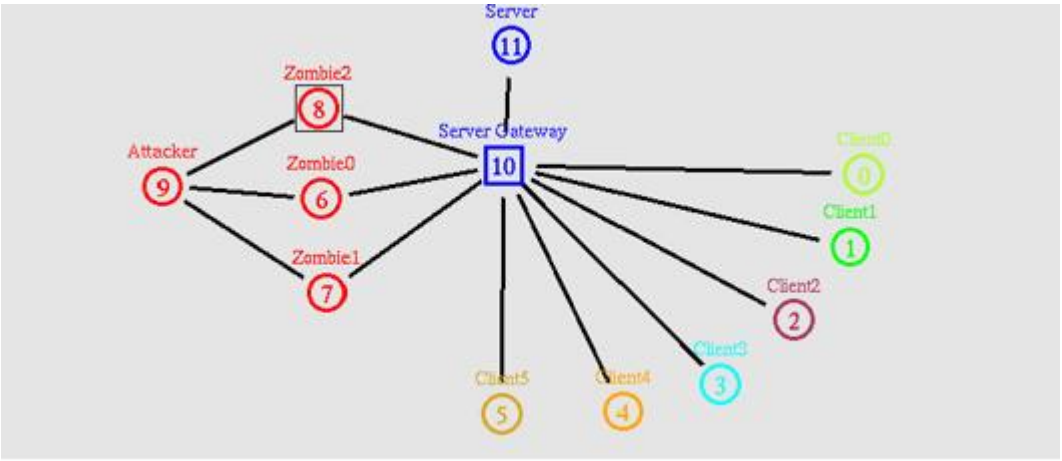

Рисунок 3.1 – Топологія 1: один атакуючий, три «зомбі», шість клієнтів

Другий сценарій відрізняється наявністю додаткового елементу — «Чорної діри» (Black hole), що слугує для фільтрації шкідливого трафіку та захисту серверної системи від атаки (див. рис. 3.2).

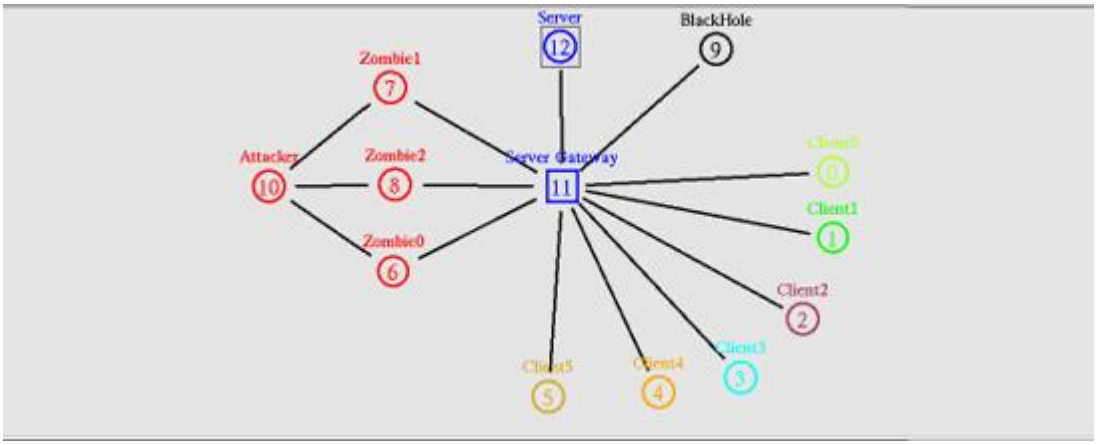

Рисунок 3.2 – Топологія 2: один атакуючий, три «зомбі», шість клієнтів, 1 «чорна діра»

Обрана техніка запобігання DDoS-атаці включає використання DNSBL (DNS Blacklist) і маршрутування трафіку до null route.

Параметри симуляції задавалися з урахуванням реалістичних характеристик мережі та трафіку. Клієнти передавали дані розміром 50 байт зі швидкістю 0.5 Мбіт/с, «зомбі» — 50 байт при 5.0 Мбіт/с, а атакуючий вузол посилав сигнали по 50 байт зі швидкістю 0.01 Мбіт/с. Протокол передачі даних — UDP з фіксованою швидкістю потоку (CBR), черга обробки пакетів — Drop tail, а затримка в мережі складала 10 мс. Пропускна здатність каналів між клієнтом і шлюзом, а також між «зомбі» і шлюзом, встановлена на рівні 45 Мбіт/с (ТЗ-з’єднання), тоді як між шлюзом і сервером пропускна здатність обмежена

12.5 Мбіт/с, що створювало умови для моделювання обмежень каналу і можливих наслідків атак.

У процесі моделювання було також враховано часові параметри, що дозволили відслідкувати динаміку розвитку DDoS-атаки та ефективність захисних заходів. Симуляція тривала загалом 50 секунд і включала кілька ключових часових інтервалів. На початковому етапі (від 0 до 10 секунд) трафік не передавався, що слугувало базовою лінією для порівняння. В період з 10 до 19.9 секунди клієнти безперервно надсилали дані серверу, які успішно до нього доходили, демонструючи нормальний режим роботи системи.

На позначці 19.9 секунди атакуючий вузол ініціював передачу команд «зомбі» для початку DDoS-атаки. У часовому проміжку від 20 до 40 секунд відбулося активне протистояння: масована атака призвела до значного зниження пропускної здатності для звичайних клієнтів, що відобразилось у зниженні їхнього трафіку до сервера. Близько 39.9 секунди атакуючий вузол надіслав сигнал «зомбі» припинити атаку, а з 40 секунди трафік клієнтів відновився і знову надходив на сервер без перешкод.

Заключним етапом симуляції стала зупинка всього трафіку на 50 секунді, що означало завершення тестового періоду. Така послідовність подій надала можливість оцінити не лише характер впливу атаки на мережу, але й продемонструвати дієвість «Чорної діри» як методу нейтралізації шкідливого трафіку.

У ході дослідження було змодельовано дві топології мережі для оцінки впливу DDoS-атаки на систему клієнт-сервер. Перша топологія складалася з одного атакуючого вузла, трьох «зомбі» і шести клієнтів, у той час як друга топологія додатково включала «Чорну діру» для блокування небажаного трафіку. Результати симуляції дозволили наочно продемонструвати, як застосування механізму «Чорної діри» може запобігти перевантаженню серверної системи та зберегти працездатність мережі.

3.2 Аналіз симуляції DDoS Reflection Attack

В інтервалі часу від 0 до 9.9 секунд відсутній потік даних між клієнтами та сервером. Починаючи з 10 секунди і до 50 секунди спостерігається активний

обмін даними: клієнти надсилають серверу пакети об’ємом 50 байт зі швидкістю 0.5 Мбіт/с. До початку атаки (перед 20 секундою) передача даних проходить безперешкодно, що підтверджується мережею в ns-2, на якій відображено топологію системи у проміжку часу з 10 до 20 секунд (див. рис. 3.3).

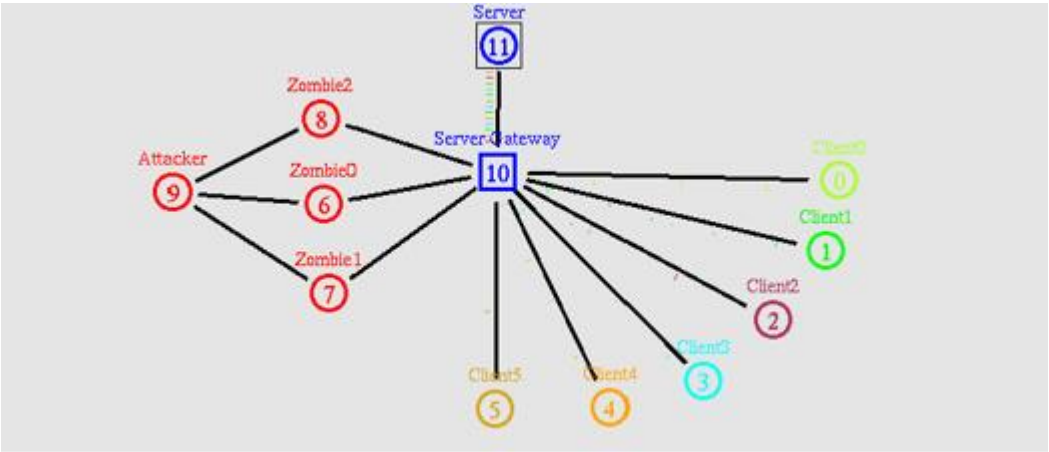

Рисунок 3.3 – Топологія мережі між 10 та 20 секундами

Атака DDoS розпочинається на 20 секунді і триває до 40 секунди. За 0.1 секунди до початку атаки (19.9 с) атакуючий вузол надсилає команду трьом «зомбі» для ініціації атаки. «Зомбі» починають масовано надсилати пакети розміром 50 байт із швидкістю 5 Мбіт/с, що спричиняє перевантаження пропускної здатності сервера, яка складає 12.5 Мбіт/с. Як наслідок, потік даних від клієнтів істотно обмежується, і відбувається втрата пакетів. Атака припиняється після сигналу від атакуючого вузла на 39.9 секунді, «зомбі» припиняють надсилати дані о 40 секунді, після чого нормальний потік клієнтських даних відновлюється.

Варто відзначити, що хоча швидкість передачі запитів від атакуючого вузла становить лише 0.01 Мбіт/с, використання «зомбі» дозволяє перевантажити серверну пропускну здатність, яка дорівнює 12.5 Мбіт/с. Це свідчить про те, що атакуючий може здійснити масштабну DDoS-атаку у мережах, навіть маючи обмежене інтернет-з’єднання. Розмах атаки безпосередньо залежить від кількості задіяних «зомбі» та їх швидкості передачі даних. На рисунку нижче наведено топологію мережі у ns-2 для проміжку часу від 20 до 40 секунд, де видно випадки втрати даних (див. рис. 3.4).

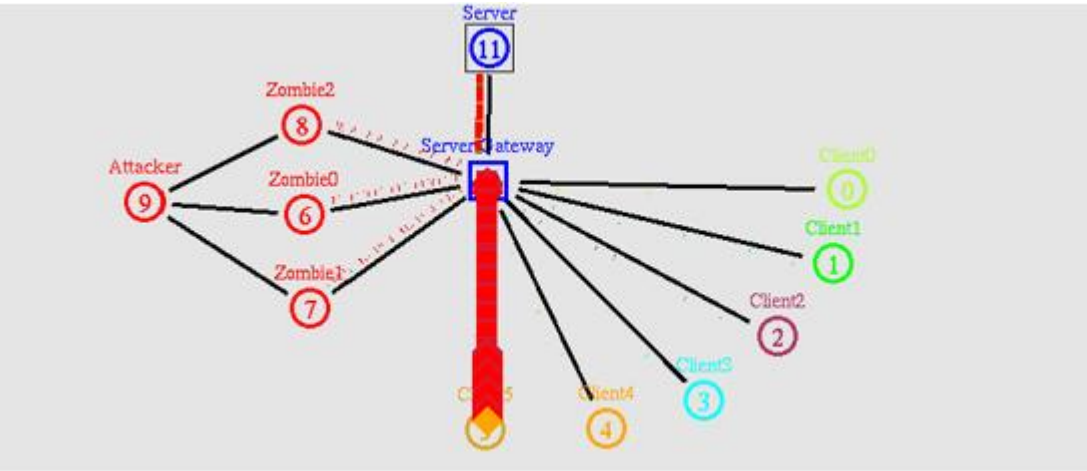

Рисунок 3.4 – Топологія мережі між 20 та 40 секундами

Результати проведеної симуляції були нанесені на графік залежності пропускної здатності від часу (bandwidth vs. time) за допомогою програми X-Graph для інтервалу 0с < t < 60с (див. рис. 3.5).

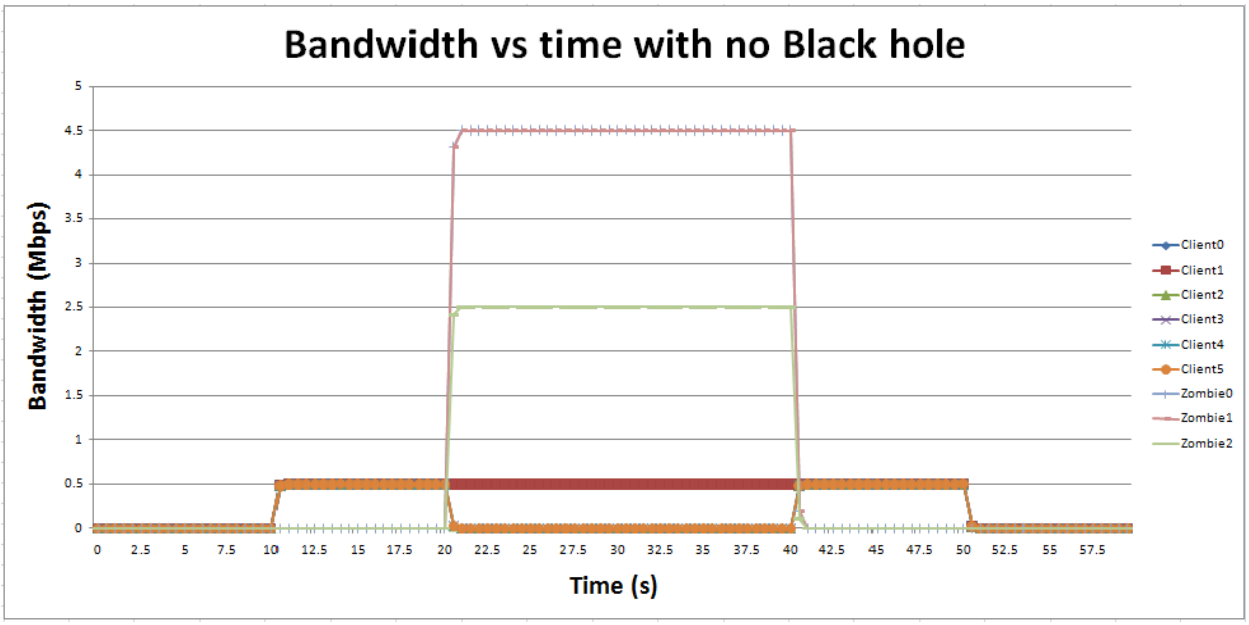

Рисунок 3.5 – Графік пропускної здатності до часу під час тесту для Топології 1

Основні спостереження за цим графіком такі:

- У проміжках часу 0с < t < 10с та 50с < t < 60с трафік на сервер відсутній, що підтверджує початкові умови симуляції. Загальна використана пропускна здатність у ці моменти дорівнює нулю.
- Потік даних від клієнтів розпочинається о 10-й секунді і завершується о 50-й секунді. Всі шість клієнтів надсилають однакові за розміром дані зі швидкістю 0.5 Мбіт/с. Відповідно, пропускна здатність сервера у цей

період дорівнює 3 Мбіт/с (6 клієнтів × 0.5 Мбіт/с). Це справедливо як до, так і після DDoS-атаки, тобто в проміжках 10с < t < 20с та 40с < t < 50с.

- Три «зомбі» здійснюють потік даних зі швидкістю 5 Мбіт/с кожен у проміжку 20с < t < 40с. Однак сервер не здатен обробити всі запити в повному обсязі: він приймає 4.5 Мбіт/с від zombie 0 та zombie 1 і лише 2.5 Мбіт/с від zombie 2. Загальна пропускна здатність сервера досягає максимального значення 12.5 Мбіт/с, і сервер перестає обслуговувати додаткові запити.
- Клієнти 2, 3, 4 та 5 повністю втрачають можливість передачі даних, їх швидкість падає до 0 Мбіт/с, тобто їм відмовлено в обслуговуванні. Водночас клієнти 0 та 1 продовжують передачу даних зі швидкістю 0.5 Мбіт/с. Використання алгоритму Drop Tail, який є пасивним механізмом керування чергою, що встановлює максимальну довжину черги на маршрутизаторі, може пояснювати цей факт: пакети передаються за принципом FIFO (перший прийшов — перший пішов).

Нижче наведено таблицю (див. таблицю 3.1), що демонструє швидкості передачі даних клієнтів і «зомбі» у проміжку часу від t=20.5с до t=25с. Клієнти 0 та 1 продовжують передавати дані зі швидкістю 0.5 Мбіт/с, ця тенденція зберігається до завершення DDoS-атаки (t=40с).

Таблиця 3.1 - Передача інформації під час тесту для Топології 1 в проміжку 20-25 секунд

Time (s)	**Client 0 (Mbps)**	**Client 1 (Mbps)**	**Client 2 (Mbps)**	**Client 3 (Mbps)**	**Client 4 (Mbps)**	**Client 5 (Mbps)**	**Zombie 0 (Mbps)**	**Zombie 1 (Mbps)**	**Zombie 2 (Mbps)**	**Total (Mbps)**
20.5	0.498432	0.498432	0.023808	0.023808	0.02304	0.02304	4.310016	4.310016	2.408448	12.11904
21	0.499968	0.499968	0	0	0	0	4.50048	4.499712	2.49984	12.49997
21.5	0.499968	0.499968	0	0	0	0	4.499712	4.50048	2.49984	12.49997
22	0.499968	0.499968	0	0	0	0	4.499712	4.499712	2.500608	12.49997
22.5	0.500736	0.499968	0	0	0	0	4.499712	4.499712	2.49984	12.49997
23	0.499968	0.500736	0	0	0	0	4.499712	4.499712	2.49984	12.49997
23.5	0.499968	0.499968	0	0	0	0	4.50048	4.499712	2.49984	12.49997
24	0.499968	0.499968	0	0	0	0	4.499712	4.50048	2.500608	12.50074
24.5	0.499968	0.499968	0	0	0	0	4.50048	4.499712	2.49984	12.49997

Подовження таблиці 3.1

25	0.499968	0.499968	0	0	0	0	4.499712	4.50048	2.49984	12.49997

Далі проаналізовано першу похідну від кривої «пропускна здатність — час». Перша похідна функції вимірює чутливість залежної змінної (швидкості передачі даних клієнтів та загальної пропускної здатності) до змін незалежної змінної (швидкості передачі даних «зомбі»). Графік першої похідної підтверджує кореляцію між високими швидкостями передачі даних «зомбі» та зниженням швидкостей передачі клієнтів і загальної пропускної здатності сервера (див рис. 3.6).

Дві невеликі пікові зміни у t=10с та t=50с відображають початок та завершення передачі даних клієнтами на сервер. Особливу увагу привертають великі піки у t=20с та t=40с, які свідчать про:

- Різку зміну пропускної здатності сервера через атаку «зомбі».
- Неможливість досягнення «зомбі» повної заявленої швидкості 5 Мбіт/с кожним через обмеження серверних ресурсів. Система не може одночасно обробити три запити по 5 Мбіт/с, що вказує на нелінійну залежність між DDoS-атакою та її впливом на сервер.
- Обернену пропорційність швидкості передачі даних клієнтів щодо цих змін: при збільшенні швидкості «зомбі» до 5 Мбіт/с о 20-й секунді швидкість клієнтів різко падає, а при припиненні атаки о 40-й секунді відбувається відновлення швидкостей.

Рисунок 3.6 – Графік похідної

3.3 Аналіз симуляції методики запобігання DDoS-атаці за допомогою «Чорної діри»

У цій симуляції передбачається наявність механізму «Чорної діри» ('Black hole') у системі, і повторно моделюється сценарій з попереднього розділу. Час проведення симуляції залишається незмінним: 0с < t < 50с. Потік даних починається о 10-й секунді і триває до 50-ї секунди. DDoS-атака відбувається у проміжку 20с < t < 40с.

У контексті захисту від DDoS-атак, термін *«Чорна діра»* (Black hole) означає спеціально налаштований маршрут або вузол у мережі, через який зловмисний трафік перенаправляється та відкидається без обробки. Іншими словами, весь підозрілий або явно шкідливий трафік спрямовується у «порожнечу», звідки він вже не повертається і не досягає цільової системи. Цей підхід дозволяє мінімізувати навантаження на сервер або маршрутизатор, який інакше був би перевантажений під час атаки.

У межах даної симуляції механізм «Чорної діри» реалізується як фільтр, який активується у момент виявлення аномального трафіку від зомбі-машин. Після ідентифікації шкідливих джерел, їхній трафік перенаправляється на інтерфейс, що не обробляє пакети далі — таким чином, атака не досягає сервера, і легітимні клієнти можуть продовжувати нормальну роботу. Це дозволяє

ефективно дослідити вплив подібного захисного підходу в умовах моделювання DDoS-атаки типу Reflection.

Нижче наведена топологія(див. рис. 3.7) мережі у ns-2 для проміжку часу 10c < t < 20c, що повністю відповідає топології попередньої симуляції:

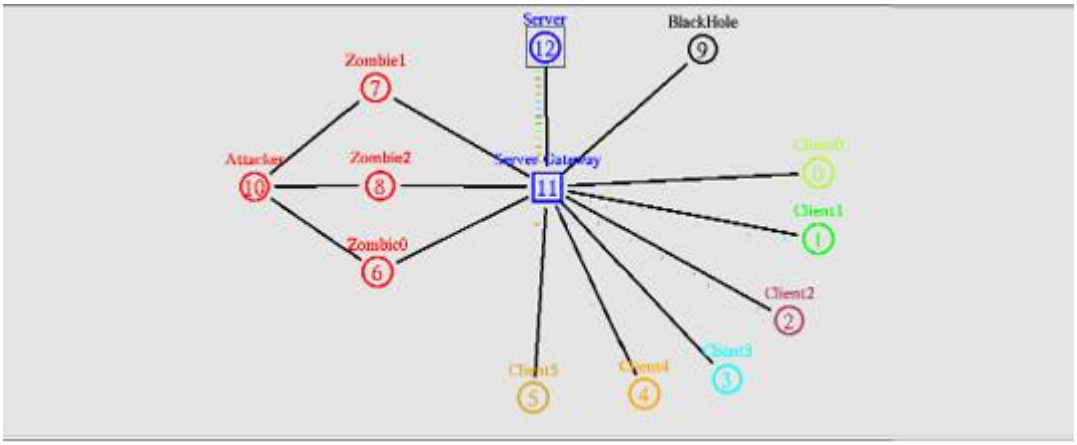

Рисунок 3.7 - Топологія мережі між 10 та 20 секундами

На 20-й секунді ініціюється DDoS-атака. Важливо відзначити, що за наявності механізму «Чорної діри» трафік «зомбі» не досягає сервера. Шкідливі запити перенаправляються у «Чорну діру» і блокуються там протягом усього часу атаки — до 40-ї секунди.

Швидкість передачі даних від клієнтів залишається стабільною та незмінною протягом всієї симуляції. Клієнти не зазнають відмови в обслуговуванні.

Нижче наведена топологія мережі у ns-2 для проміжку 20c < t < 40c із увімкненим механізмом «Чорної діри»:

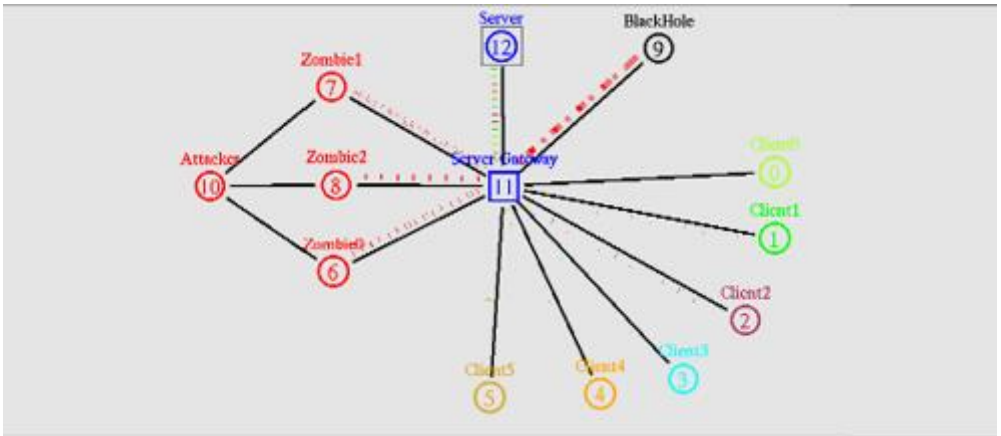

Рисунок 3.8 - Топологія мережі між 20 та 40 секундами

На основі повних результатів симуляції за проміжок часу 0s < t < 60s побудовано графік «пропускна здатність vs. час» (див. рис. 3.9):

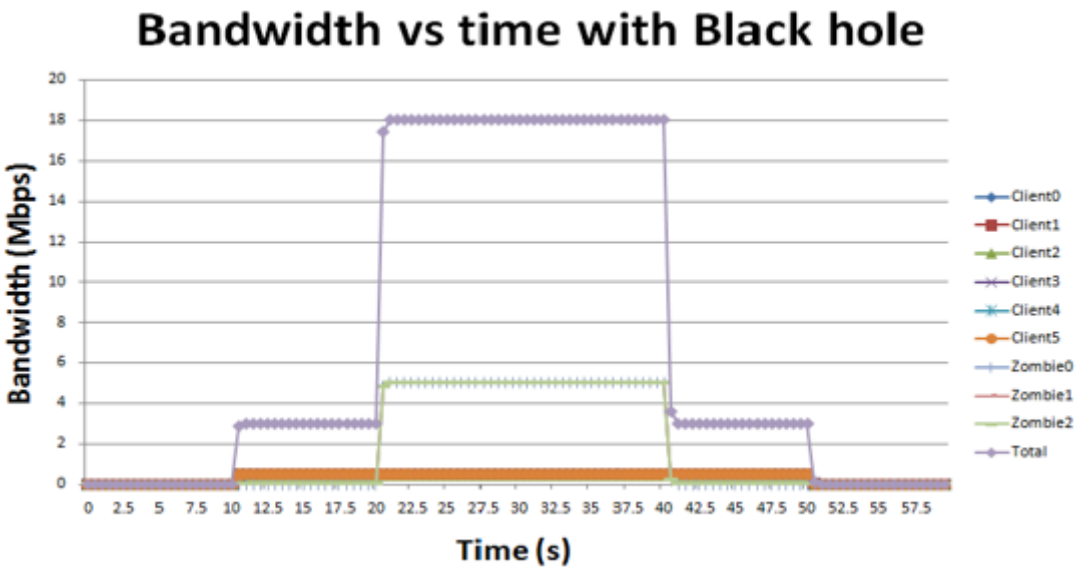

Рисунок 3.9 – Графік пропускної здатності до часу під час тесту для Топології 1

Основні спостереження, що випливають із графіка:

- Аналогічно першому сценарію, трафік на сервер відсутній у періоди 0s < t < 10s та 50s < t < 60s. Передача даних від клієнтів стабільно підтримується на рівні 0.5 Мбіт/с у проміжках 10s < t < 20s та 40s < t < 50s.
- Три зомбі посилають дані зі швидкістю 5 Мбіт/с у проміжку 20s < t < 40s. Графік X Graph підтверджує, що ці дані надходять із заданою швидкістю. Проте тепер ця передача не впливає на загальне обмеження пропускної здатності сервера у 12.5 Мбіт/с, оскільки трафік перенаправляється до «Чорної діри».
- Додатковим підтвердженням ефективності методу «Чорної діри» є спостереження за сумарною пропускною здатністю системи в період 20s < t < 40s — вона становить 18 Мбіт/с, що є сумою трьох потоків по 5 Мбіт/с від зомбі та шести потоків по 0.5 Мбіт/с від клієнтів. Зазначена величина 18 Мбіт/с не відповідає пропускній здатності лінка між шлюзом і сервером, а є загальною пропускною здатністю системи за цей період.
- Дані від шести клієнтів залишаються стабільними на рівні 0.5 Мбіт/с протягом 10s < t < 50s і не зазнають впливу DDoS-атаки.

Порівняння першої похідної графіка «пропускна здатність vs. час» з аналогічним графіком з попереднього сценарію показує, що малі сплески у точках t=10s та t=50s відповідають початку та завершенню передачі даних відповідно. Водночас великі сплески у точках t=20s та t=40s змінили свій характер:

- Відсутня нелінійна залежність між швидкістю передачі даних зомбі та загальною пропускною здатністю системи — замість цього спостерігається лінійна залежність, що підтверджується різницею у величинах сплесків.
- Зникла обернена залежність між швидкістю передачі даних клієнтів і DDoS-атакою.

Рисунок 3.10 – Графік похідної

3.4 Порівняння методів чергування Drop Tail і SFQ як засобу захисту від DDoS-атак

Для подальшого аналізу ефективності захисту від DDoS-атак було змодельовано мережеву інфраструктуру з використанням іншого методу чергування — Stochastic Fair Queuing (SFQ). При цьому топологія залишалася незмінною: один атакувальний вузол, три зомбі-хости та шість клієнтів.

Для моделювання та аналізу було використано метод чергування Stochastic Fair Queuing (SFQ), який забезпечує більш справедливий розподіл мережевих ресурсів між різними потоками даних. SFQ — це алгоритм управління чергами, що розподіляє трафік по декількох окремих FIFO-чергах на основі хешування пакетів, що дозволяє уникнути блокування одного потоку за рахунок інших. Такий підхід дає змогу гарантувати мінімальний рівень пропускної здатності для кожного потоку та захищає мережу від домінування шкідливих джерел.

У контексті захисту від DDoS-атак застосування SFQ допомагає обмежити надмірний трафік з боку атакувальних вузлів (зокрема зомбі-хостів), при цьому не обмежуючи легітимний трафік клієнтів. Це особливо важливо для сценаріїв, де необхідно підтримувати нормальне функціонування мережі під час атаки, розподіляючи ресурси більш справедливо між користувачами.

В рамках цієї роботи SFQ використовується для оцінки ефективності запобігання DDoS-атакам шляхом порівняння пропускної здатності клієнтів і атакуючих хостів, що дозволяє зробити висновки щодо переваг цієї методики в порівнянні з традиційним методом чергування Drop Tail.

Тривалість симуляції була ідентичною попереднім дослідженням.

У моделюванні були використані такі параметри:

- Обсяг переданих даних для всіх вузлів: 50 байтів
- Швидкість передачі даних:
    1. Клієнт 0: 0.1 Мбіт/с
    2. Клієнт 1: 0.2 Мбіт/с
    3. Клієнт 2: 0.3 Мбіт/с
    4. Клієнт 3: 0.4 Мбіт/с
    5. Клієнт 4: 0.5 Мбіт/с
    6. Клієнт 5: 0.6 Мбіт/с
    7. Зомбі 0: 4.0 Мбіт/с
    8. Зомбі 1: 5.0 Мбіт/с
    9. Зомбі 2: 6.0 Мбіт/с
    10. Атакувальний вузол: 0.01 Мбіт/с
- Транспортний протокол: UDP

- Тип застосування: CBR (постійна бітова швидкість)
- Метод чергування: SFQ
- Затримка: 10 мс
- Пропускна здатність:
    - Від клієнта до шлюзу: 45 Мбіт/с
    - Від зомбі до шлюзу: 45 Мбіт/с
    - Від шлюзу до сервера: 12.5 Мбіт/с

У часовому проміжку між 20.5 с і 25 с було зафіксовано швидкості передачі даних клієнтами та зомбі-хостами. Ці значення залишалися стабільними протягом усього часу атаки (з 20 с до 40 с).

Таблиця 3.2 - Передача інформації під час тесту

Time (s)	Client 0 (Mbps)	Client 1 (Mbps)	Client 2 (Mbps)	Client 3 (Mbps)	Client 4 (Mbps)	Client 5 (Mbps)	Zombie 0 (Mbps)	Zombie 1 (Mbps)	Zombie 2 (Mbps)	Total (Mbps)
20.5	0.100608	0.200448	0.300288	0.400128	0.499968	0.599808	3.327744	3.327744	3.327744	12.08448
21	0.09984	0.19968	0.300288	0.400128	0.499968	0.599808	3.466752	3.466752	3.466752	12.499968
21.5	0.09984	0.200448	0.29952	0.400128	0.499968	0.600576	3.465984	3.466752	3.466752	12.499968
22	0.09984	0.19968	0.300288	0.400128	0.499968	0.599808	3.466752	3.466752	3.466752	12.499968
22.5	0.09984	0.19968	0.29952	0.39936	0.499968	0.599808	3.46752	3.466752	3.46752	12.499968
23	0.100608	0.200448	0.300288	0.400128	0.499968	0.600576	3.465984	3.465984	3.465984	12.499968
23.5	0.09984	0.19968	0.300288	0.400128	0.499968	0.599808	3.466752	3.466752	3.466752	12.499968
24	0.09984	0.200448	0.29952	0.400128	0.499968	0.599808	3.466752	3.46752	3.466752	12.500736
24.5	0.09984	0.19968	0.300288	0.400128	0.499968	0.599808	3.466752	3.466752	3.466752	12.499968
25	0.09984	0.19968	0.29952	0.400128	0.499968	0.599808	3.46752	3.466752	3.466752	12.499968

Цікаво, що при використанні методу SFQ швидкості клієнтів залишились незмінними, на відміну від зомбі-хостів. Їхній трафік був значно обмежений — кожен зомбі міг передавати дані лише на рівні приблизно 3.466 Мбіт/с, що не призвело до виникнення атаки типу DDoS.

Це цілком відповідає принципам роботи SFQ, що базується на справедливому розподілі черг. Метод використовує алгоритм хешування, який рівномірно розподіляє трафік між кількома FIFO-чергами, надаючи кожному потоку рівний доступ до ресурсу. Оскільки клієнти почали передавати дані ще з 10-ї секунди, а зомбі лише з 20-ї, трафік клієнтів отримав пріоритет і був

оброблений першим. Потоки від зомбі були розділені між трьома чергами, що знизило навантаження на сервер і унеможливило виникнення перевантаження.

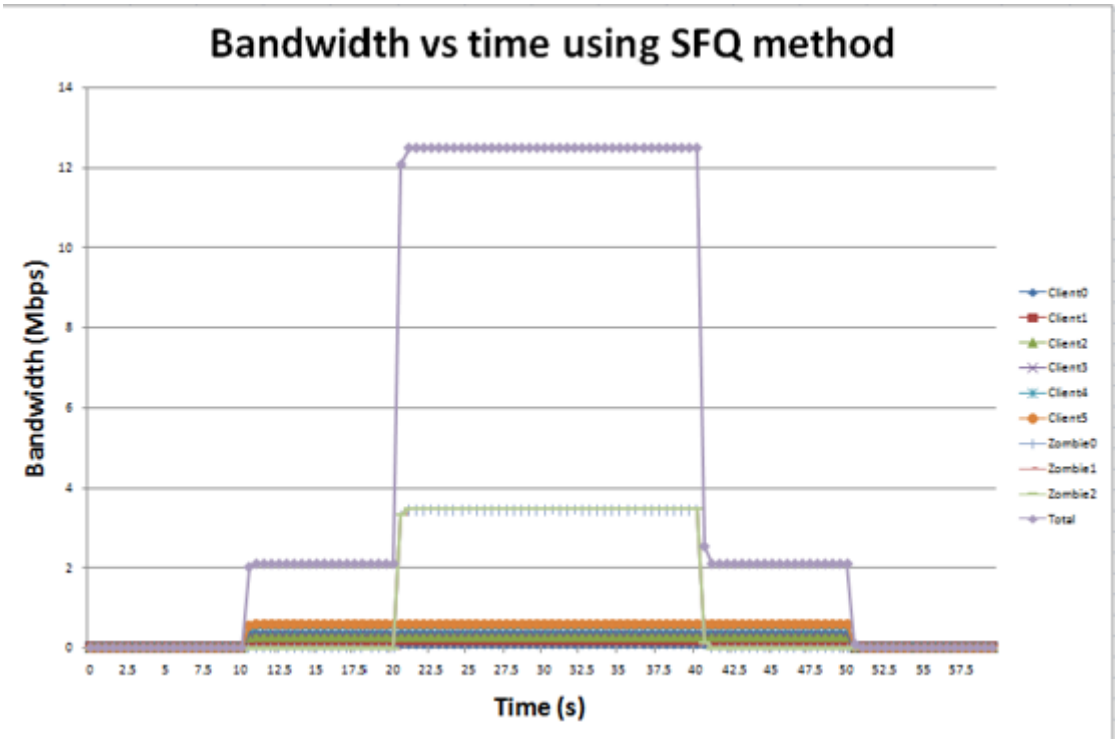

Рисунок 3.11 – Графік пропускної здатності до часу під час тесту

Таким чином, результати симуляції показують ефективність SFQ як методу протидії DDoS-атакам завдяки його здатності забезпечувати справедливий розподіл пропускної здатності навіть за наявності великої кількості ворожих потоків.

ВИСНОВКИ

У межах дипломної роботи було виконано комплексне дослідження методів і технологій захисту від розподілених атак типу відмови в обслуговуванні (DDoS), з особливим акцентом на аналіз їх впливу на функціонування та ефективність застосування різних механізмів запобігання. Робота складалася з трьох основних розділів, кожен з яких був присвячений певному аспекту проблематики.

У першому розділі було проведено теоретичний аналіз природи та класифікації DDoS-атак. Розглянуто основні типи атак, такі як атаки на пропускну здатність, атаки на рівень протоколів, а також атаки на рівень додатків. Окремо були охарактеризовані найпоширеніші протоколи, які використовуються в рефлективних атаках: DNS, NTP, SSDP тощо. Крім того, у розділі було охарактеризовано базові засоби захисту від DDoS-атак, включаючи фільтрацію трафіку, обмеження швидкості, використання CDN та розподілених проксі.

У другому розділі було зосереджено увагу на вразливостях локальних комп’ютерних мереж, які можуть бути використані для здійснення або ескалації DDoS-атак. Було проаналізовано типові вразливості мережевих протоколів, таких як ARP, DHCP, ICMP, а також загрози, пов’язані з погано сконфігурованими сервісами. Далі розглянуто найбільш поширені типи атак, зокрема ARP-spoofing, DHCP-spoofing, MITM, DoS/DDoS, sniffer-атаки, MAC-флудинг тощо. У підсумку було обґрунтовано необхідність застосування активних методів запобігання, таких як контроль маршрутизації, мережеві екрани, а також інтеграція із системами виявлення вторгнень (IDS).

У третьому розділі було здійснено практичне моделювання сценаріїв DDoS-атак з використанням платформи ns-2. Основна увага була приділена атаці типу Reflection. Було змодельовано топологію з одним атакувальним вузлом, трьома зомбі-хостами та шістьма легітимними клієнтами. На базовому рівні симуляції, без будь-яких механізмів захисту, спостерігалося перевантаження каналу зв’язку між шлюзом і сервером у період атаки (20–40с).

Для протидії атаці були протестовані два методи:

1) «Чорна діра» (Black hole) — метод, при якому шкідливий трафік перенаправляється або знищується ще на рівні шлюзу. У симуляції використання чорної діри дозволило відсікати пакети, що надходили від зомбі-хостів, завдяки чому пропускна здатність з боку клієнтів залишалася стабільною і DDoS не виникав. Це підтверджує ефективність цього підходу як простого й оперативного рішення.
2) Алгоритм стохастичного справедливого чергування (SFQ) — більш гнучкий механізм, який розподіляє трафік по чергах за допомогою хеш-функцій, надаючи рівні шанси кожному потоку. У дослідженні SFQ показав, що навіть при збереженні всього трафіку (включно з трафіком атакувальників), зомбі не змогли повністю витіснити легітимних користувачів із каналу. Кожен потік (зомбі й клієнти) отримував справедливу долю пропускної здатності, в результаті чого атака не досягла своєї мети.

Порівняння результатів показало, що обидва методи є ефективними, проте мають свої переваги та обмеження. Метод «чорної діри» дозволяє радикально усунути джерело атаки, але потребує точного виявлення шкідливих вузлів. SFQ, у свою чергу, більш підходить для умов, де неможливо або недоцільно блокувати весь трафік, та забезпечує більш контрольований і рівномірний розподіл ресурсів між усіма користувачами.

У підсумку, на основі проведених теоретичних і практичних досліджень, можна зробити висновок, що сучасні мережеві інфраструктури потребують гнучкого підходу до забезпечення стійкості проти DDoS-атак. Комбінація методів виявлення, аналізу трафіку та динамічного управління чергами є найбільш перспективним напрямком розвитку засобів захисту. Результати симуляцій демонструють можливість практичного застосування даних підходів для захисту як локальних, так і глобальних мережевих систем.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is a distributed denial-of-service (DDoS) attack? [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

2. DDoS Attack Types & Mitigation Methods. [Електронний ресурс]. – Режим доступу: https://www.imperva.com/learn/ddos/ddos-attacks/

3. DDoS Attack Classification: A Complete Guide. [Електронний ресурс]. – Режим доступу: https://ddos-guard.net/blog/classification-of-ddos-attacks

4. Different Types of DDoS Attacks Explained. [Електронний ресурс]. – Режим доступу: https://www.connectwise.com/blog/cybersecurity/types-of-ddos-attacks

5. History of Distributed Denial of Service Attacks. [Електронний ресурс]. – Режим доступу: https://stormwall.network/resources/blog/ddos-history

6. The history of DDoS and DoS. [Електронний ресурс]. – Режим доступу: https://www.senki.org/ddos-attack-preparation-workbook/history-of-denial-of-services-dos-attacks/

7. Five Most Famous DDoS Attacks. [Електронний ресурс]. – Режим доступу: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

8. Famous DDoS attacks. [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

9. Reasons for DDoS – Why Do Hackers Attack? [Електронний ресурс]. – Режим доступу: https://stormwall.network/resources/blog/why-do-ddos-attacks-happen

10. Why is DDoS Still So Effective After 20 Years? [Електронний ресурс]. – Режим доступу: https://innovatecybersecurity.com/news/why-is-ddos-still-so-effective-after-20-years/

11. Impact of DDoS Attacks on Business. [Електронний ресурс]. – Режим доступу: https://stormwall.network/resources/blog/impact-of-ddos-attacks-on-businesses

12. The Damaging Impacts of DDoS Attacks. [Електронний ресурс]. – Режим доступу: https://www.corero.com/the-damaging-impacts-of-ddos-attacks/

13. Ghazali K.. Flooding distributed denial of service attacks — A review., / Ghazali K., Hassan R.// - 2011. – 1218-1223.

14. Mirkovic J.. A taxonomy of DDoS attack and DDoS defense mechanisms.,/ Mirkovic J., Reiher P.// 2004 – 39-53.

15. Types of Network Protocols and Their Uses. [Електронний ресурс]. – Режим доступу: https://www.geeksforgeeks.org/types-of-network-protocols-and-their-uses/

16. 15 Common Network Protocols and Their Functions. [Електронний ресурс]. – Режим доступу: https://www.techtarget.com/searchnetworking/feature/12-common-network-protocols-and-their-functions-explained

17. Zargar S.. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks.,/ Zargar S., Joshi J., Tipper D.// - 2013. Режим доступу: https://ieeexplore.ieee.org/document/6547839

18. Understanding Cloud-based DDoS Protection. [Електронний ресурс]. – Режим доступу: https://www.indusface.com/blog/understanding-cloud-ddos-attacks-and-cloud-based-ddos-protection/

19. Defense of DDoS attack for cloud computing. [Електронний ресурс]. – Режим доступу: https://ieeexplore.ieee.org/document/6272848

20. ns-2 Documentation. [Електронний ресурс]. – Режим доступу: https://www.isi.edu/websites/nsnam/ns/ns-documentation.html

21. What is Blackholing | Mitigating DDoS Attacks. [Електронний ресурс]. – Режим доступу: https://www.imperva.com/learn/ddos/blackholing/

22. What is DDoS blackhole routing. [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/learning/ddos/glossary/ddos-blackhole-routing/

23. Modern DDoS Attack. [Електронний ресурс]. – Режим доступу: https://nsfocusglobal.com/modern-ddos-attacks-and-the-rise-of-ddos-coalitions/