ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «**Методика побудови системи захисту від DDOS атак**»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Георгій ЯЦКОВСЬКИЙ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти гр. ТСДМ-63
Георгій ЯЦКОВСЬКИЙ
Ім'я, ПРІЗВИЩЕ

Керівник: Михайло МАЛЮЖЕНКО
к.т.н., доцент *Ім'я, ПРІЗВИЩЕ*

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ- 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Телекомунікацій

Кафедра ___Телекомунікаційних систем та мереж_____
Ступінь вищої освіти __магістр_____
Спеціальність ___172 Електронні комунікації та радіотехніка _____
Освітньо-професійна програма _____Телекомунікаційні системи та мережі_____

ЗАТВЕРДЖУЮ
Завідувач кафедрою ТСМ
_____ Віктор ЗАЇКА
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Яцковському Георгію Сергійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Методикапобудови системи захисту від DDOS атак
керівник кваліфікаційної роботи Михайло МАЛЮЖЕНКО, КТН, доцент
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « ___ » _____ 2025 р. № ___.

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.

3. Вихідні дані до кваліфікаційної роботи:
   1. Види DDoS атак
   2. Засоби виявлення DDoS атак
   3. Розробка методики захисту від DDOS атак

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
   1. Види DDoS атак
   2. Засоби виявлення DDoS атак
   3. Розробка методики захисту від DDOS атак

5. Перелік ілюстративного матеріалу: презентація (на слайдах)

6. Дата видачі завдання «___» _____ 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури	10.10.2025	Викон.
2	Види DDOS атак	20.10.2025	Викон.
3	Засоби виявлення DDOS атак	15.11.2025	Викон.
4	Розробка методики захисту від DDOS атак	30.11.2025	Викон.
5	Висновки, вступ, реферат	15.12.2025	Викон.
6	Розробка презентації	20.12.2025	Викон.

Здобувач вищої освіти _____ Георгій ЯЦКОВСЬКИЙ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Михайло МАЛЮЖЕНКО
(підпис) *(Ім'я ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій
ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Яцковський Г.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «Методика побудови системи захисту від DDOS атак».

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника магістерської роботи

Здобувач Яцковський Георгій Сергійович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до наукової роботи.
Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Яцковського Георгія Сергійовича на оцінку «добре» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи _____ Михайло МАЛЮЖЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 2025 року

Висновок кафедри про бакалаврську роботу

Кваліфікаційна робота розглянута. Здобувач Яцковський Г.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувача вищої освіти Яцковського Георгія Сергійовича
(прізвище, ім'я, по батькові)
на тему « Методика побудови системи захисту від DDOS атак»

Актуальність. Тема роботи є актуальною, оскільки з розвитком телекомунікаційних мереж та зростанням обсягу переданих даних зростає й кількість DDoS-атак. Ці атаки становлять значну загрозу для безперебійної роботи критичних інформаційних систем, порушуючи доступність послуг та викликаючи серйозні фінансові й репутаційні збитки для організацій.

Позитивні сторони. Робота детально розглядає сучасні методи виявлення та запобігання DDoS-атакам, включаючи мережеві, прикладні підходи та профілактичні заходи, що забезпечує її комплексність.

1. Робота містить практичні рекомендації щодо побудови систем захисту в реальних телекомунікаційних мережах.
2. Виконано порівняльний аналіз методів захисту з акцентом на їх ефективність, що підвищує цінність дослідження для практичного застосування.

Недоліки. 1. У роботі недостатньо розглянуто вплив комбінованих атак на різні рівні телекомунікаційних мереж.
2.Практична частина потребує більш детального аналізу впровадження методів у реальних мережах із різною архітектурою.

Відзначені зауваження не впливають на загальну позитивну оцінку бакалаврської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "добре", а здобувач Яцковський Георгій Сергійович заслуговує присвоєння кваліфікації магістр з електронних комунікацій та радіотехніки.*

Рецензент
науковий ступінь, вчене звання _____ (підпис) _____ *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: ___ стор., ___ рис., ___ табл., ___ джерел.

Об'єкт дослідження – Інформаційні системи та мережі зв'язку.

Предмет дослідження – Методи та засоби захисту від DDOS атак у межах інформаційних систем та мереж зв'язку.

Мета роботи – розробка ефективної методики захисту від атак типу DDOS у межах інформаційних систем та мереж зв'язку. Робота спрямована на створення комплексного підходу, який забезпечить високий рівень захисту інформаційних ресурсів від масштабних та розмаїтих DDOS атак.

В дипломній роботі показана розробка методики захисту від атак типу DDOS у контексті інформаційних систем та мереж зв'язку. Робота включає в себе аналіз сучасних підходів до вирішення проблеми, систематизацію термінології та визначення основних характеристик DDOS атак. Детальний розгляд типів атак, аналіз ризиків та уразливостей, розробка методів виявлення та ефективних заходів захисту входять до складу обґрунтованої методики, яку доповнюють розрахунки та експерименти для підтвердження її ефективності. Робота завершується висновками та вказівками на перспективи подальших досліджень у цій важливій галузі кібербезпеки.

КЛЮЧОВІ СЛОВА:

DDOS ATTACKS, TELECOMMUNICATION NETWORKS, CYBER SECURITY, DDOS PROTECTION

ABSTRACT

The text part of the master's thesis: ___ pages, ___ figures, ___ tables, ___ sources.

The purpose of the work is to study the principles of building IP telephony networks based on MGCP protocols.

The object of research is IP-Telephony networks.

The subject of the study is the construction of an IP telephony network based on the MGCP protocol.

The analysis of the capabilities of IP telephony networks based on the MGCP protocol showed:

The principles of building IP telephony networks make it possible to significantly reduce the bandwidth for the transmission of voice, video and data in the mode of multimedia messages and, thanks to this, to significantly reduce the cost of services provided to subscribers. The N.323 family of protocols provides the ability to transmit voice messages, video and data over IP telephony networks and is well integrated with the capabilities of TMZK. The MGCP protocol is more promising for building IP telephony networks because it is built on the decomposition of transport gateways, which allows to reduce the time of transmission of signaling messages.

KEY WORDS:

CHANNEL SWITCHING, PACKET SWITCHING, TCP/IP PROTOCOL STACK, IP TELEPHONY, MGCP PROTOCOL, OPPORTUNITIES FOR USING IP TELEPHONY NETWORKS.

ЗМІСТ

ВСТУП..... 9
1 ТЕОРЕТИЧНІ ОСНОВИ DDOS АТАК **Помилка! Закладку не визначено.**1
1.1 Основні принципи DDOS атак.... **Помилка! Закладку не визначено.**1
1.2 Аналіз масштабу атак та їх вплив на ресурси.. **Помилка! Закладку не визначено.**5
2 ЗАСОБИ ВИЯВЛЕННЯ DDOS АТАК... **Помилка! Закладку не визначено.**
2.1 Використання сенсорів та аналіз трафіку..... **Помилка! Закладку не визначено.**8
2.2 Методи аналізу трафіку для розпізнавання DDoS атак: ..... **Помилка! Закладку не визначено.**
2.3 Використання інтелектуальних алгоритмів в системах виявлення DDoS атак:..... 22
3 РОЗРОБКА ЗАХИСТУ ВІД DDOS АТАК З ВИКОРИСТАННЯМ ОБЛАКОВИХ ТЕХНОЛОГІЙ ..... **Помилка! Закладку не визначено.**4
3.1 Захист на рівні хмари: ..... **Помилка! Закладку не визначено.**
3.2 Технічні відомості, як захиститись від DDOS атак **Помилка! Закладку не визначено.**8
4 РОЗРОБКА ЗАХИСТУ ВІД DDOS АТАК 33
4.1 Розрахунок характеристик хмарного хостингу, для запобіганню DDOS атакам 33
4.2 Ввідні дані для розрахунку ..... **Помилка! Закладку не визначено.**9
4.3 Розрахунок потрібних характеристик..... 36
4.4 Висновки після розрахунків..... **Помилка! Закладку не визначено.**8
ВИСНОВКИ……...44
ПЕРЕЛІК ПОСИЛАНЬ……46
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ.....48

ВСТУП

В епоху, коли інформаційні технології проникають у всі аспекти сучасного суспільства, мережа Інтернет стає необхідною складовою нашого повсякденного життя. Зростання користувацької бази та перехід послуг у цифровий простір породжують високий попит на постійний та надійний доступ до мережі для максимізації доходу. Однак з розповсюдженням цифрових технологій збільшується й загроза Distributed Denial of Service (DDOS) атак.

DDOS атаки представляють собою спроби перекриття роботи веб-ресурсів чи комп'ютерних систем, переповнюючи їх запитаннями та знижуючи їх доступність. З використанням ботнетів, атакуючі можуть здійснювати атаки із розподіленого навантаження, ускладнюючи виявлення та протидію. Типи DDOS атак різноманітні, а їх масштаб та координація роблять їх особливо складними для виявлення та протистояння.

З урахуванням зростаючого ризику DDOS атак важливо розвивати ефективні методики захисту. У світі стрімкого технологічного розвитку, де важливу роль грають хмарні сервіси та пристрої Інтернету речей, кібербезпека стає ключовою проблемою. DDOS атаки впливають на найважливіші аспекти інтернет-екосистеми, а їх масштаб та організованість визначають необхідність постійного удосконалення захисних стратегій.

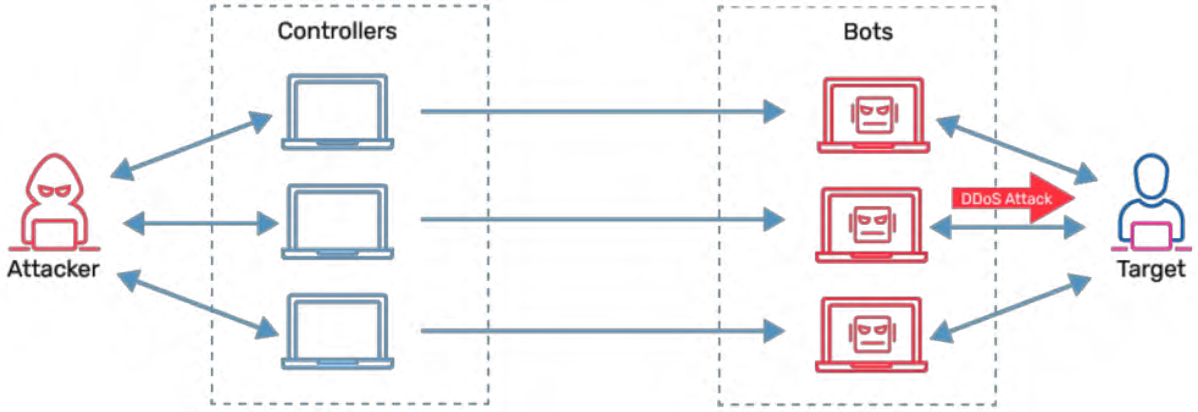


Рис.1.1 Схема DDOS атаки

Захист мереж стає надзвичайно важливим завданням, оскільки DDOS атаки можуть призвести до великої втрати продуктивності. Недоступність важливих мережевих ресурсів або сервісів може призвести до серйозних втрат для підприємств та організацій. Крім того, великі обсяги надмірного трафіку в мережі можуть спричинити перевантаження та втрату ефективності роботи мережевої інфраструктури.

Таким чином, в реалізації захисту від DDOS атак важливо не лише зменшувати поверхню атак, ефективно аналізувати трафік та вдосконалювати методи виявлення та протидії, але й забезпечувати стійкість мереж та мінімізувати вплив атак на їх продуктивність. Розробка та впровадження комплексних заходів захисту є важливою передумовою для надійності та безпеки інформаційних ресурсів.

Захист мереж від DDOS атак постійно стикається з викликами, оскільки атаки стають все більш винахідливими та складними. Розробники заходів безпеки повинні постійно адаптуватися до нових видів атак, вивчаючи їхні особливості та модифікуючи захисні стратегії. Важливо розвивати інтелектуальні системи аналізу трафіку, щоб ефективно розпізнавати та блокувати атаки з мінімальним впливом на легітимний трафік.

Сучасні підходи до захисту включають у себе використання штучного інтелекту та машинного навчання для передбачення та виявлення аномального трафіку. Такі системи можуть вчитися на основі історичних даних та реагувати на нові атаки в режимі реального часу. Застосування технологій блокчейн також виводить захист на новий рівень, дозволяючи створити розподілену систему моніторингу та фільтрації трафіку.

Захист мереж від DDOS атак вимагає співпраці та обміну досвідом серед Інтернет-провайдерів, підприємств та фахівців з кібербезпеки. Створення спільнот та платформ для обміну інформацією про нові види атак та

ефективні методи їхнього протидії може сприяти створенню більш безпечного інтернет-простору. Ініціативи по створенню таких спільнот та форумів для обговорення найновіших тенденцій у сфері кібербезпеки мають стратегічне значення для успішної боротьби із зростаючими загрозами DDOS атак в сучасному світі.

1. ТЕОРЕТИЧНІ АСПЕКТИ DDOS АТАК

1.1 Основні принципи DDOS атак

DDoS атаки є серйозною загрозою для сучасних інформаційних систем. Їхні принципи включають використання зомбі-комп'ютерів, ампліфікацію трафіку та синхронізовані атаки. Ці напади призводять до великих наслідків, таких як перевантаження серверів, великі витрати пропускної здатності та навіть відмова в обслуговуванні. У розділі також розглядається HTTP/HTTPS та DNS атаки, їхні методи розпізнавання та наслідки для потенційних жертв.

Нижче наведені основі принципи DDOS атак

1. **Зомбі-комп'ютери:** Атакуючі використовують мережу комп'ютерів, зазомбованих шкідливим програмним забезпеченням, щоб скоординовано взяти участь у DDOS атаках.

   Наслідки:

   - Перевантаження ресурсів цільового сервера.
   - Великі витрати пропускної здатності мережі.

2. **Ампліфікація трафіку:** Зловмисники використовують послуги, які надають ампліфікацію, збільшуючи обсяг трафіку для нападу.

   Наслідки:

   - Значний обсяг трафіку, який може призвести до відмови в обслуговуванні (DoS).
   - Великі навантаження на цільові сервери та мережеві засоби.

3. **Синхронізовані атаки:** Атаки, які виконуються одночасно з різних джерел для ускладнення виявлення та уникнення захисту.

   Наслідки:

   - Підвищений ризик успіху атаки.

- Утруднена можливість виявлення та блокування атак.

4. **HTTP/HTTPS атаки:** Використовуються для перевантаження веб-серверів за допомогою великої кількості запитів.

   Наслідки:

   - Зниження доступності веб-сервісів для законних користувачів.
   - Великі обсяги надмірного HTTP трафіку.

5. **DNS атаки:** Напади на сервери доменних імен з метою перевантаження та призводження до відмови в обслуговуванні.

   Наслідки:

   - Втрата доступності веб-сайтів та інших ресурсів, пов'язаних із DNS.
   - Можливість перехоплення DNS-запитів.

Таблиця 1.1

Типи і характеристики DDoS атак

Тип атаки	**Характеристики**
ICMP Flood	Використовує протокол ICMP для надсилання великої кількості пакетів на жертву, що призводить до перевантаження мережі.
UDP Flood	Використовує протокол UDP для надсилання великої кількості UDP-пакетів на жертву, що завантажує мережу.
SYN/ACK Flood	Атака на сервери, які використовують TCP, надсилаючи багато невірних TCP-запитів, що забирає ресурси сервера.
HTTP Flood	Використовується для атаки на веб-сервери, надсилаючи велику кількість HTTP-запитів, що завантажує сервер.
DNS Amplification	Зловмисники використовують DNS-сервери для відправки великої кількості запитів з

	підмінениими IP-адресами, щоб підсилити атаку.
Slowloris	Атака, в якій зловмисники встановлюють багато недоліких з'єднань з сервером і підтримують їх відкритими, споживаючи ресурси.
NTP Amplification	Використовує сервери точного часу для відправки великої кількості запитів з підмінениими IP-адресами, щоб підсилити атаку.
Smurf Attack	Використовує IP-адресу жертви для надсилання ICMP-пакетів до мережі, що відповідає на них, перевантажуючи мережу.
DNS Flood	Атака на DNS-сервер, надсилаючи велику кількість запитів на вимін IP-адреси для доменних імен.
Volumetric Attack	Атака, яка переповнює мережу великою кількістю трафіку, заважаючи легітимному трафіку проходити.
Application Layer	Використовує вразливості на рівні додатків для атаки, наприклад, SQL-ін'єкції або переповнення буфера.
Reflection Attack	Використовує ампліфікацію, наприклад, використовуючи відкриті DNS-сервери або NTP-

Продовження Талиці 1.1

	сервери, щоб збільшити потужність атаки.
Spoofed Attack	Зловмисники приховують свою ідентифікацію або IP-адресу, ускладнюючи виявлення та блокування атаки.

Нижче наведені основні види DDOS атак

1. **Атаки на рівні застосунків:** Ці атаки спрямовані на вразливості конкретних застосунків та можуть викликати:
    - **Затримки в відповіді сервера:** Захоплені ресурси сервера призводять до зниження швидкості відповіді на легітимні запити.
    - **Відмова в обслуговуванні веб-сайтів та сервісів:** Перевантаження веб-серверів може призвести до повної недоступності для користувачів.
2. **Атаки на рівні мережі:** Ці атаки націлені на протоколи мережі та можуть викликати:
    - **Відмова в обслуговуванні на рівні мережевих з'єднань:** Напади на інфраструктуру можуть перекрити доступ до мережевих ресурсів.
    - **Перевантаження комутаторів та маршрутизаторів:** Збільшення навантаження на мережеві пристрої може спричинити їх перевантаження та неправильне функціонування.
3. **Ампліфікаційні атаки:** Ці атаки можуть викликати великі обсяги трафіку та призвести до:
    - **Збільшення витрат пропускної здатності мережі:** Великі обсяги відповідей, що відправляються жертві, можуть виснажити пропускну здатність мережі.

- **Відмова в обслуговуванні при перевищенні пропускної здатності:** Мережева інфраструктура неспроможна обробити великі обсяги трафіку, що може призвести до недоступності ресурсів.

Ці конкретні наслідки демонструють складність та важливість розуміння різних видів DDoS атак для ефективної розробки та впровадження стратегій захисту.

1.2 Аналіз масштабу атак та їх вплив на ресурси

Аналіз масштабу атак включає в себе моніторинг величини трафіку, який надходить на сервери, та визначення тимчасових збоїв у роботі. Для виявлення атак служби безпеки використовують різноманітні інструменти, такі як системи виявлення вторгнень (IDS) та системи виявлення аномалій в мережі (NIDS).

1. **Обсяг трафіку:**
   - Визначення та класифікація обсягу трафіку, що випереджається DDoS атаками.
   - Аналіз обсягу трафіку у вигляді байтів або пакетів для визначення рівня потужності атаки.
2. **Продуктивність ресурсів:**
   - Вивчення впливу атак на роботу серверів, комутаторів та маршрутизаторів.
   - Аналіз швидкодії та реакції ресурсів на велику кількість запитів або пакетів.
3. **Динаміка атак:**

- Аналіз змін в обсязі трафіку та реакції ресурсів протягом тривалості атаки.
- Визначення пікових навантажень та періодів, коли атаки менш активні.

4. **Використання ампліфікації:**
   - Дослідження атак, що використовують ампліфікацію для створення великих обсягів трафіку.
   - Аналіз впливу ампліфікаційних атак на пропускну здатність та ефективність захисту.

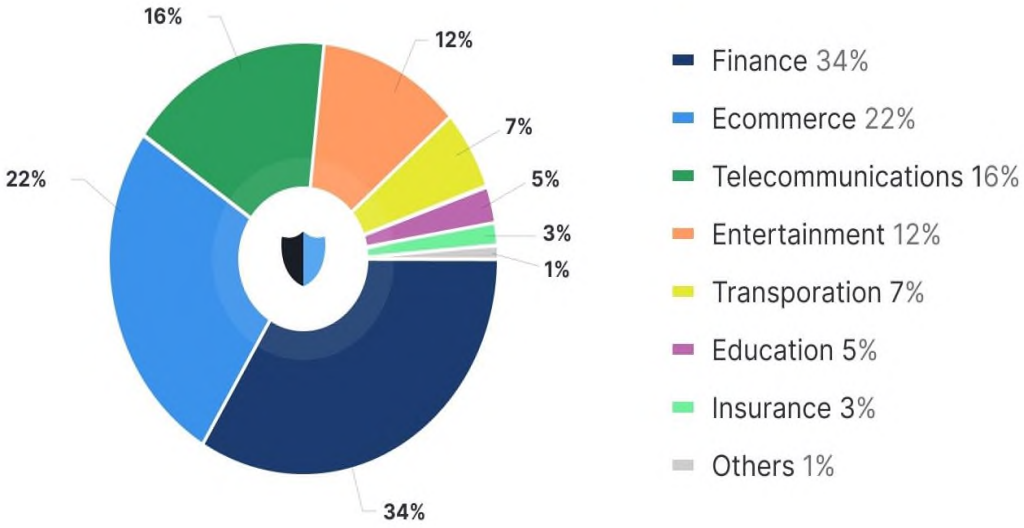


Рис. 1.2 Розподіл DDOS атак по нішам за перший квартал 2023 року

Потужність DDoS атак: DDoS (розподілене блокування послуг) атаки становлять серйозну загрозу для онлайн-ресурсів, і їх потужність може значно варіюватися. Потужність визначається кількістю запитів, які одночасно направляються до цільового сервера. Це може бути велика кількість запитів, яка перевищує ресурси сервера, призводячи до його відмови обслуговування. Атаки можуть бути великомасштабними, займаючи гігабітні або терабітні пропускні здатності, або ж невеликими, здійснюваними з використанням рядових пристроїв.

Вивчення патернів розподілу атак

Атаки можуть мати різні патерни розподілу, що означає різноманітні методи атакуючих для приховування своєї діяльності. Наприклад, атакуючі можуть варіювати частоту та обсяги атак, використовувати різні IP-адреси для зміни свого місця походження, чи модифікувати види трафіку для ухилення від виявлення. Вивчення цих патернів дозволяє розробникам засобів захисту створювати більш ефективні стратегії виявлення та протидії атакам.

1. **Географічний розподіл**
    - Аналіз місця походження трафіку атак з точки зору географічного розподілу;
    - Вивчення регіонів, що є основними джерелами DDoS атак.
2. **Види трафіку**
    - Класифікація різних типів трафіку, які використовуються в атаках (наприклад, HTTP, UDP);
    - Аналіз патернів розподілу ампліфікаційного трафіку та його особливостей.
3. **Синхронізація атак**
    - Вивчення атак, які виконуються синхронізовано з різних джерел;
    - Аналіз часових інтервалів та координації атак для виявлення спроб обхідної такти.

2 ЗАСОБИ ВИЯВЛЕННЯ DDOS АТАК

2.1 Використання сенсорів та аналіз трафіку

Системи виявлення DDoS атак використовують ряд технологій, серед яких основоположними є сенсори та аналіз трафіку. Ці інструменти дозволяють здійснювати ретельний моніторинг мережі та реагувати на зміни в режимі трафіку, що є критичним для виявлення та мінімізації впливу DDoS атак.

Системи виявлення аномалій:

В основі систем виявлення аномалій лежить аналіз трафіку з метою виявлення незвичайних або несподіваних патернів поведінки. Алгоритми цих систем враховують різноманітні параметри, такі як обсяг пакетів, швидкість передачі даних, типи запитів та відповідей, та інші характеристики мережевого трафіку.

Під час роботи системи виявлення аномалій використовують порігові значення, щоб визначити, коли певний показник перевищує нормативний рівень. Наприклад, зростання кількості запитів на один ресурс або підвищення швидкості трафіку може бути індикатором DDoS атаки. Аналізуючи ці аномалії, системи виявлення спроможні вчасно розпізнати потенційну загрозу та ініціювати відповідні захисні заходи.

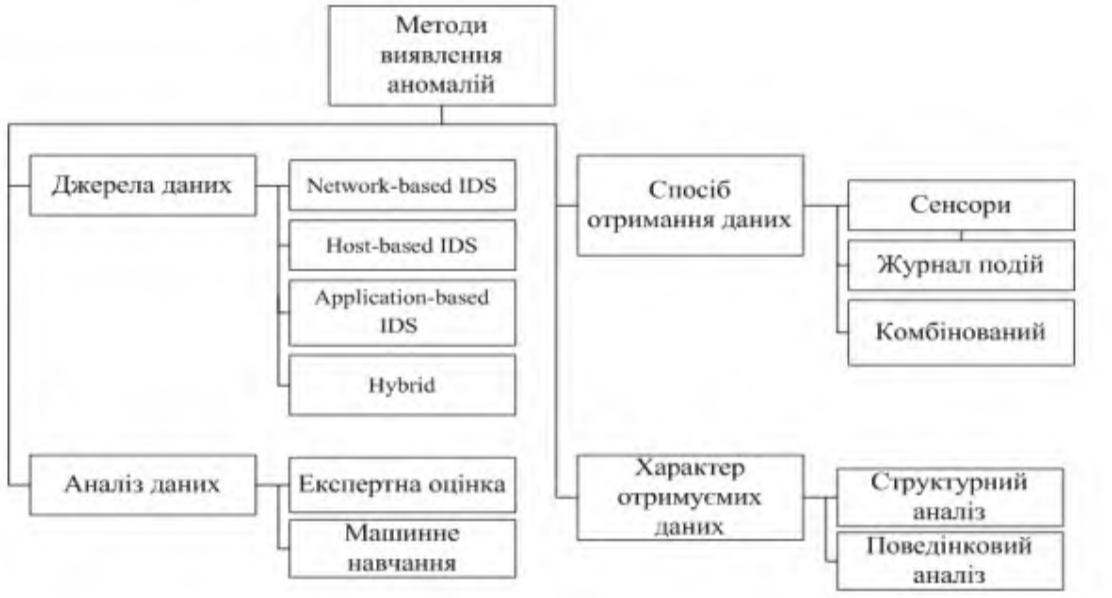


Рис.2.1 Схема роботи системи виявлення аномалій

Рис.2.1 надає візуальне подання схеми роботи системи виявлення аномалій. Зображено основні етапи процесу виявлення аномалій, включаючи моніторинг та аналіз трафіку, визначення аномалій та запуск захисних заходів.

Цей блок виокремлює ключові аспекти використання сенсорів та аналізу трафіку в системах виявлення DDoS атак, детально розглядаючи процес виявлення аномалій та методи аналізу трафіку для ефективного розпізнавання потенційних загроз.

Аналіз та класифікація аномалій у трафіку:

Системи виявлення аномалій базуються на аналізі широкого спектру параметрів мережевого трафіку для визначення відхилень від звичайних моделей. Вони ретельно аналізують пакети, що проходять через мережу, та звертають увагу на різноманітні характеристики, такі як час відповіді, обсяг передачі даних, типи запитів, та інші параметри.

Наприклад, система може виявити аномалію великої кількості запитів на один ресурс, яка може бути характерною для атак DDoS. Аналіз типів

запитів, які надходять, може розкрити використання певних атакуючих сценаріїв. Комбінування цих параметрів дозволяє системі розпізнавати навіть витончені форми атак та інші неправильності.

Використання порігових значень та статистичних методів:

Для ефективного виявлення аномалій системи використовують порігові значення та статистичні методи для ідентифікації несподіваних відхилень у трафіку. Порігові значення визначають граничні показники, які вказують на ненормативний обсяг певного параметра, такого як кількість запитів за певний час чи швидкість передачі даних.

Статистичні методи включають в себе аналіз розподілу параметрів та визначення середніх значень. Вони дозволяють системі автоматично визначати нормативні діапазони для різних характеристик трафіку та ідентифікувати аномалії, що виходять за межі цих норм.

Наприклад, якщо середня кількість запитів від користувача зазвичай не перевищує 100 запитів за хвилину, система може визначити велику кількість запитів як аномалію, що вказує на можливу DDoS атаку.

Цей підхід дозволяє системам виявлення аномалій забезпечувати широкий охоплення різноманітних загроз та надійно виявляти відхилення у поведінці мережі, що робить їх ефективними інструментами для забезпечення безпеки в умовах постійно зростаючих загроз кібербезпеки.

2.2 Методи аналізу трафіку для розпізнавання DDOS атак:

В контексті захисту від DDOS атак, розробка ефективних методів аналізу трафіку є важливим етапом для виявлення та відсіювання шкідливих атакуючих дій.

Вивчення характерних особливостей трафіку DDoS атак:

Аналізуючи характерні особливості трафіку, що характеризують DDOS атаки, системи безпеки можуть виділити та ідентифікувати певні патерни, що

вказують на незвичайну або зловмисну діяльність. Наприклад, збільшення обсягу запитів на конкретний ресурс, різке підвищення частоти запитів, або зміна типів запитів можуть бути характеристиками DDOS атак.

Також важливо дослідити властивості трафіку, такі як джерела запитів, їх географічне походження та розподіл часу. Аналізуючи ці параметри, система може виявити ненормативні зміни в патернах та акцентувати увагу на областях, які вимагають додаткового моніторингу.

Використання сигнатур та евристичних методів:

Використання сигнатур - це один із методів, що базується на визначенні унікальних підписів атак, що дозволяють розпізнавати конкретні шаблони атакуючих дій. Система порівнює актуальний трафік із заздалегідь визначеними сигнатурами DDOS атак, та виявляє відмінності.

Евристичні методи використовуються для виявлення нових атак, які можуть відрізнятися від відомих сигнатур. Аналізуючи структуру трафіку та специфічні особливості, евристичні алгоритми можуть виявити аномалії, що не входять в визначені сигнатури, і вживати відповідні заходи для їх придушення.

Розробка ефективних алгоритмів для реагування та відсіювання трафіку:

Однак аналіз трафіку – це лише перший крок. Системи також потребують ефективних алгоритмів для реагування на виявлені аномалії та відсіювання легітимного трафіку від атак. Це може включати в себе використання фільтрації на рівні мережевих елементів, розподілене зберігання та обробка запитів або навіть редиректори трафіку для розгортання альтернативних ресурсів.

Такий комплексний підхід забезпечує системі виявлення DDOS атак високий рівень ефективності та надійності, дозволяючи оперативно реагувати на різноманітні загрози та забезпечуючи безпеку мережевого середовища.

2.3 Використання інтелектуальних алгоритмів в системах виявлення DDOS атак:

Використання інтелектуальних алгоритмів, зокрема машинного навчання, є ключовим елементом в сучасних системах виявлення DDOS атак. Розглянемо детально основні аспекти цього підходу, включаючи різні методи машинного навчання та аналіз поведінки користувачів та систем.

Машинне навчання та інші методи для покращення виявлення:

Машинне навчання (ML) стає важливим інструментом для виявлення DDOS атак, пропонуючи широкий спектр методів для аналізу трафіку та розпізнавання аномалій.

- **Огляд різних методів машинного навчання:**
    - *Навчання з учителем:* Використання моделей, які навчаються на основі позначених даних, де алгоритм вивчає відповіді на конкретні DDoS атаки та нормальний трафік.
    - *Навчання без учителя:* Методи, що використовують алгоритми кластеризації та визначення аномалій для виявлення ненормативних зразків у трафіку.

- **Використання глибокого навчання та нейронних мереж:**
    - Глибоке навчання та нейронні мережі використовуються для розпізнавання складних аномалій, зокрема тих, які можуть бути важко виявити за допомогою традиційних методів. Вони можуть ефективно аналізувати великі обсяги даних та виявляти субтільні патерни.

Аналіз поведінки користувачів та систем:

Інтелектуальні алгоритми застосовуються для ретельного аналізу звичайного поведінки користувачів та інфраструктури, щоб виявити ненормативні аномалії.

- **Використання інтелектуальних алгоритмів для аналізу поведінки:**
  - За допомогою інтелектуальних алгоритмів можна визначати звичайні патерни та норми використання системи, включаючи частоту запитів, розподіл діапазонів IP-адрес, та інші характеристики.

- **Розробка моделей для виявлення невластивих аномалій:**

  - Розробка моделей, які вивчають та визначають нормальну поведінку, дозволяє автоматично виявляти невластиві аномалії. Ці моделі можуть враховувати динамічні зміни в середовищі та адаптуватися до нових видів атак.

У контексті виявлення DDOS атак, використання інтелектуальних алгоритмів представляє інноваційний підхід, що вдосконалює здатність систем розпізнавання атак. Машинне навчання, зокрема, надає гнучкість та точність виявлення, сприяючи ефективному аналізу та класифікації трафіку. Разом із застосуванням глибокого навчання та аналізу поведінки користувачів, ці інтелектуальні методи розширюють спектр захисту та забезпечують реакцію на змінні та вибагливі сценарії атак. Такий поєднаний підхід інтегрує передові технології для ефективної оборони від різноманітних DDoS загроз, забезпечуючи стійку та прогресивну кібербезпеку.

3 РОЗРОБКА ЗАХИСТУ ВІД DDOS АТАК З ВИКОРИСТАННЯМ ОБЛАКОВИХ ТЕХНОЛОГІЙ

3.1 Захист на рівні хмари:

Захист на рівні хмари визначається своєю здатністю працювати на великій території та забезпечувати централізовану, але еластичну оборону. Сучасні хмарові рішення використовують низку технік та стратегій для забезпечення повноцінного захисту від DDOS атак.

- **Проксі-сервіси та фільтрація трафіку:**
    - Хмарні платформи можуть використовувати проксі-сервіси для фільтрації трафіку, що надходить до користувача. Це дозволяє відсіювати шкідливий трафік ще на рівні хмари, перед тим як він досягне локальної інфраструктури.
- **Розподілені системи захисту:**
    - Застосування розподілених систем захисту в хмарових оточеннях дозволяє ефективно обробляти великі об'єми трафіку. Це здійснюється через використання глобальних мереж фільтрації, які можуть визначати та блокувати DDOS атаки на рівні глобальних вузлів.

Сучасні облачні технології для мінімізації впливу DDoS атак:

Облачні технології не лише забезпечують захист на рівні хмари, але й впроваджують низку передових методів для мінімізації впливу DDOS атак на інфраструктуру.

- **Запобігання атакам ампліфікації:**

    - Хмарні постачальники використовують алгоритми та механізми, щоб запобігти атакам ампліфікації, які можуть призводити до значного збільшення трафіку. Для цього застосовують фільтрацію пакетів та обмеження ресурсів, які можуть бути використані для підсилення атакуючими.
- **Автоматизована реакція на інциденти:**

    - За допомогою інтелектуальних систем виявлення та реагування, хмарні області можуть автоматично визначати DDOS атаки та надавати миттєву відповідь. Автоматизована реакція зменшує час реакції на інцидент та підвищує ефективність захисту.

- **Захист від різноманітних видів атак:**

    - Інтеграція різноманітних методів захисту від DDOS, включаючи DNS фільтрацію, SSL захист, та маршрутизацію трафіку, дозволяє забезпечити повноцінний захист від різних типів атак, таких як аплікаційні атаки та SYN/ACK-флуди.

Таблиця 3.1

Порівняння облачних рішень для захисту від DDOS

Особливості	**Amazon Web**	**Cloudflare**	**Akamai**	**Microsoft Azure**

	Services (AWS Shield)			**(Azure DDoS Protection)**
Типи DDoS-атак, що підтримуються	UDP і TCP флуди, HTTP флуди, ICMP флуди та інші	Всі типи DDoS-атак, включаючи веб-сервери та сетеві атаки	UDP і TCP флуди, SSL/TLS атаки, ICMP флуди та інші	UDP і TCP флуди, SYN/ACK атаки, ICMP флуди та інші
Мережевий пропускний потік	Від 40 Гбіт/с до сотень Гбіт/с	Від 100 Гбіт/с до Терабіт/с	Від 10 Гбіт/с до сотень Гбіт/с	Від 1 Гбіт/с до Терабіт/с
Глобальна мережева покриття	Так	Так	Так	Так
Аналітика трафіку	Так	Так	Так	Так
Можливість налаштування правил	Так	Так	Так	Так

Продовження Таблиці 3.1

Захист від заздалегідь відомих загроз	Так	Так	Так	Так

Технічна підтримка	24/7 служба підтримки	24/7 служба підтримки	24/7 служба підтримки	24/7 служба підтримки
Додаткові можливості	Інтеграція з AWS WAF, AWS Firewall Manager та іншими AWS-сервісами	Інтеграція з іншими Cloudflare-сервісами, включаючи CDN	Інтеграція з іншими Akamai-сервісами, CDN	Інтеграція з Azure Firewall, Azure Application Gateway та іншими Azure-сервісами

Таблиця 3.1 представляє об'єктивне порівняння різних облачних рішень для захисту від DDOS атак. Враховуючи параметри, які охоплюють ефективність, гнучкість, та цінову доступність, організації можуть зробити інформовані рішення щодо вибору найбільш відповідного захисту для своїх потреб.

- **Моніторинг та звітність:**

    - Хмарні рішення забезпечують регулярний моніторинг трафіку та надають деталізовані звіти про інциденти. Це допомагає адміністраторам збирати дані для подальшого аналізу та вдосконалення стратегій захисту.

- **Резервне копіювання та відновлення:**

    - Використання облакових технологій також дозволяє організаціям впроваджувати ефективні стратегії резервного копіювання та

відновлення, забезпечуючи можливість швидкого відновлення інфраструктури після DDOS атаки.

Загальною метою використання облакових технологій для захисту від DDoS атак є створення комплексних та стійких механізмів, які забезпечують безпеку інфраструктури та дозволяють бізнес-процесам функціонувати без перебоїв під час атак.

3.2 Технічні відомості, як захиститись від DDOS атак

Захист від DDOS атак вимагає комплексного підходу, включаючи як заходи на рівні мережі, так і на рівні застосунків. Нижче подано деякі технічні заходи, які можна вжити для захисту від DDOS атак:

1. **Firewalls та Фільтри:**

    - Використовуйте мережеві фільтри та файрволи для блокування трафіку від відомих атакуючих IP-адрес та застосовуваних підозрілих пакетів.
    - Налаштуйте фільтрацію на рівні мережевих пристроїв для реагування на різні типи DDoS атак, такі як SYN/ACK, UDP, або ICMP атаки.
    - *Мінуси:* Можливість легкої обхідної тактики для атакуючих, таких як використання змінених IP-адрес або розподілення атаки з великої кількості ботів.

2. **Rate Limiting:**

- Встановіть обмеження на кількість запитів чи пакетів, які може обробити сервер за певний час.
- Використовуйте інтелектуальні алгоритми для визначення аномального трафіку та обмеження його швидкості.
- *Мінуси:* Може призводити до втрати легітімного трафіку, якщо обмеження встановлено занадто низьким, що може вплинути на доступність та якість обслуговування.
-

3. **Intrusion Prevention Systems (IPS):**

- Використовуйте системи запобігання вторгнення для виявлення та блокування вразливостей та атак на рівні мережі та застосунків.

  Мінуси: Вимагає постійного оновлення для виявлення нових типів атак. Може виникнути проблема ложних позитивів, коли легітімний трафік помилково визначається як атака.

4. **Трафік Scrubbing Services:**
   - Перенаправляйте весь вхідний трафік через спеціалізовані служби заборони, які виявляють та фільтрують атаки перед тим, як вони досягнуть вашого сервера.

     Мінуси: Вартість таких послуг може бути високою, особливо для великих обсягів трафіку. Затримка у фільтрації трафіку може виникнути при великих атаках.

5. **Content Delivery Network (CDN):**

- Використовуйте CDN для розподілу трафіку між географічно розташованими серверами, що дозволяє вам локалізувати та відсіювати DDOS трафік на віддалених вузлах мережі.

Мінуси: Може призвести до збільшення затримок у відповіді сервера для деяких користувачів, зокрема тих, які знаходяться далеко від вузла CDN.

6. **Облікові записи і Контентів:**

- Використовуйте захищені облікові записи та застосовуйте криптографічні методи для захисту важливих даних.
- Кешуйте статичний контент, щоб зменшити навантаження на сервер та вартість атаки.

  Мінуси: Припинення атак на рівні облікових записів може вимагати додаткових процедур аутентифікації, що може ускладнити життя для користувачів.

7. **Anycast DNS:**

- Використовуйте Anycast DNS для розподілу трафіку між різними серверами, щоб забезпечити високу доступність та запобігти перевантаженню окремих серверів.

  Мінуси: Можливість атаки на DNS-сервери, якщо їхній розташування відоме, а також проблеми з локалізацією деяких користувачів через маршрутизацію трафіку.

8. **Моніторинг та Логування:**

- Реалізуйте системи моніторингу та логування для виявлення аномалій у трафіку та вчасного реагування на потенційні DDOS атаки.
- Аналізуйте логи для визначення характеристик атак і підготовки до майбутніх заходів захисту.

Мінуси: Великий обсяг логів може вимагати значних ресурсів для обробки і аналізу. Логи можуть бути піддавані атакам або фальсифікації.

9. **Апаратні Рішення:**

- Розгляньте використання спеціалізованих апаратних засобів для мітігації DDoS атак, таких як load balancers і апаратне обладнання для обробки трафіку.
  Мінуси: Вартість апаратного обладнання може бути високою, і не всі організації можуть собі це дозволити.

10. **Обмін інформацією:**

- Співпрацюйте з іншими організаціями і службами безпеки для обміну інформацією про нові атаки та вразливості.
  Мінуси: Недостатня взаємодія або недостатність широкомасштабних платформ для обміну інформацією можуть обмежити ефективність цього методу.

В цьому блоці обговорювалися технічні методи захисту від DDOS атак. Зокрема, висвітлені принципи використання мережевих фільтрів, систем інтрузії, обмеження швидкості, трафік-скрабінг сервісів, Content Delivery Network (CDN), а також апаратних рішень для мітігації атак. Кожен метод має свої переваги та недоліки. Наприклад, хоча використання CDN може зменшити навантаження на сервери, це може призвести до збільшення затримок для деяких користувачів. Підсумково, ефективний захист від DDOS вимагає комплексного підходу, включаючи використання різноманітних заходів, моніторинг та постійне оновлення стратегій відповіді на нові види атак.

Основні вимоги до систем захисту:

Захисні механізми повинні працювати в реальному часі, забезпечуючи миттєве виявлення шкідливого трафіку із мінімальними затримками. Фільтрація має виконуватися без помилкових спрацьовувань, щоб зберегти якість обслуговування для легітимних користувачів. Крім того, система повинна бути відмовостійкою та легко інтегруватися з існуючими мережевими інфраструктурами.

4 РОЗРОБКА ЗАХИСТУ ВІД DDOS АТАК

4.1 Розрахунок характеристик хмарного хостингу, для запобіганню DDOS атакам

Використання хмарних технологій стає важливим компонентом стратегії кібербезпеки для організацій у забезпеченні стійкості своєї інфраструктури перед DDoS атаками. Основна перевага полягає в гнучкості та ефективності захисту, які надає хмара.

- **Еластичність та масштабованість:** Хмарні платформи дозволяють організаціям ефективно масштабувати свої ресурси в залежності від навантаження. Це забезпечує еластичність у використанні ресурсів та масштабованість для пристосування до збільшених обсягів трафіку під час DDOS атак.
- **Глобальні системи розподіленого захисту:** Хмарні платформи можуть впроваджувати глобальні системи розподіленого захисту, які працюють на рівні вузлів в різних географічних регіонах. Це дозволяє ефективно виявляти та фільтрувати DDOS трафік ще до того, як він досягне локальних серверів або мережі.
- **Проксі-сервіси та фільтрація трафіку:** Хмарні постачальники можуть використовувати проксі-сервіси для фільтрації трафіку та видалення потенційно шкідливих запитів. Це дозволяє здійснювати захист ще на рівні хмари та мінімізувати навантаження на локальні сервери.
- **Автоматизовані системи моніторингу та реагування:** Використання хмарних технологій дозволяє імплементувати автоматизовані системи моніторингу та реагування. Інтелектуальні алгоритми можуть виявляти аномальний трафік та сприймати ефективні заходи щодо його блокування чи маршрутизації.

Захист на рівні хмари:

Захист на рівні хмари є ключовим аспектом сучасних стратегій кібербезпеки, оскільки DDoS атаки набувають складніших та високотехнологічних форм. Сучасні хмарні технології впроваджують різноманітні заходи для мінімізації впливу цих атак та забезпечення безперебійності служб.

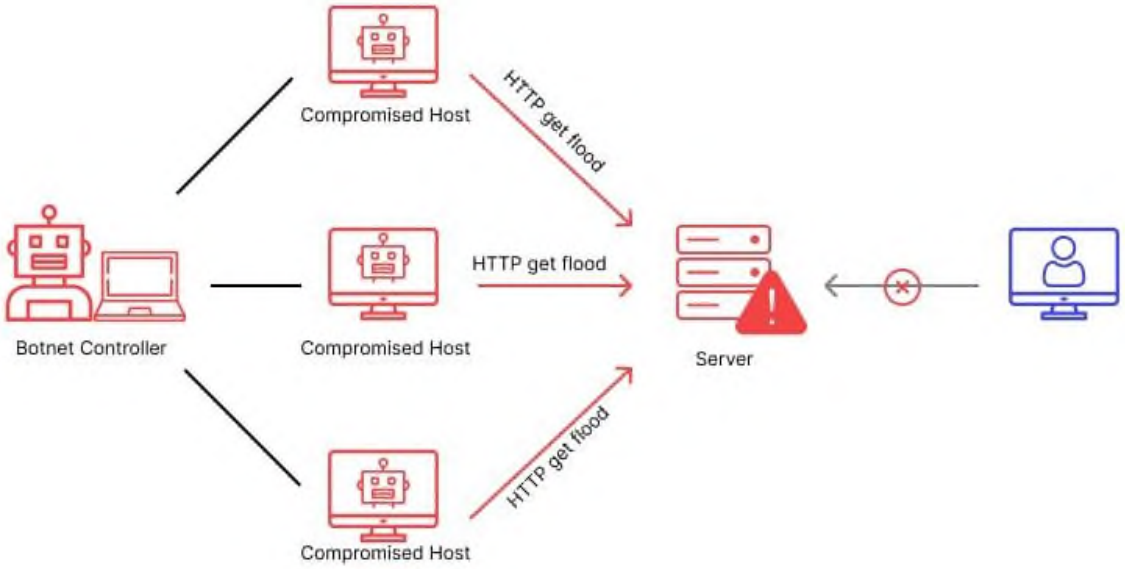
- **Запобігання атакам ампліфікації:** Однією з основних функцій хмарних технологій є запобігання атакам ампліфікації. Вони використовують фільтрацію пакетів та обмеження ресурсів, що можуть бути використані для підсилення атакуючими, зменшуючи ризик великих обсягів трафіку.
- **Системи виявлення та блокування:** Хмарні технології можуть впроваджувати системи виявлення та блокування DDOS атак. Ці системи базуються на аналізі трафіку, використанні сигнатур та розпізнаванні невластивого поведінки для швидкого виявлення та відсіювання атак.
- **Гнучкість та адаптабельність:** Однією з переваг захисту на рівні хмари є його гнучкість. Хмарні рішення можуть адаптуватися до змінюючихся обставин, вносити корективи в стратегії захисту та ефективно пристосовуватися до нових видів атак.
- **Моніторинг та аналітика:** Хмарні технології дозволяють проводити детальний моніторинг та аналіз атак. Це надає можливість вчасно реагувати на нові загрози, а також аналізувати здійснені атаки для вдосконалення стратегій захисту.

Використання хмарних технологій та захист на рівні хмари стає невід'ємною частиною сучасних інфраструктур для ефективного протистояння розмаїттю DDOS атак.

4.2 Вхідні дані для розрахунку

На сайт відбувається DDOS атака:

Вид атаки: **HTTP Flood;**



HTTP Flood (або атака на рівні застосунків HTTP) - це вид атаки на веб-сервер, при якій зловмисник відправляє велику кількість HTTP-запитів на цільовий сервер з метою перевантаження його ресурсів та призведення до відмови в обслуговуванні (атака DDOS - атака).

Основна ідея HTTP Flood полягає в створенні великого обсягу трафіку, перевантажуючи сервер запитами на рівні HTTP. Атакуючий може використовувати різні методи для досягнення цієї мети, наприклад, створювати багато хибних запитів, звертатися до великої кількості різних URL або використовувати компрометовані ботмережі для масштабування атаки.

Мета HTTP Flood - перевантажити сервер так, щоб він не міг ефективно обробляти легітимний трафік, що може призвести до того, що сайт або веб-застосунок стають недоступними для звичайних користувачів.

Для захисту від HTTP Flood можуть використовуватися різні техніки, такі як використання CDN (Content Delivery Network), WAF (Web Application Firewall), фільтрація трафіку на рівні мережі, а також використання спеціалізованих програмних і апаратних засобів для виявлення та запобігання DDOS-атак.

Наслідки атаки HTTP Flood можуть включати в себе недоступність веб-сайту або веб-додатка для користувачів, втрату репутації, фінансові збитки та інші проблеми, пов'язані з перервами у роботі відвідувачів.

Середній обсяг атаки складає: 5 Гбіт/с;

Тривалість атаки: 1 година.

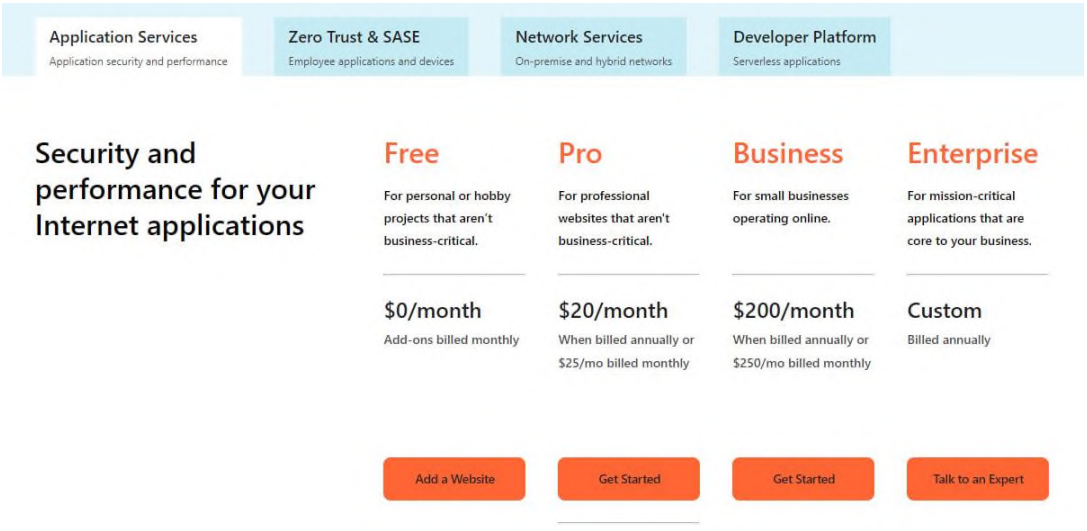
4.3 Розрахунок потрібних характеристик

Для витримання атаки HTTP Flood обсягом 5 Гбіт/с на протязі години, сервер повинен мати достатньо ресурсів, щоб обробляти і відповідати на велику кількість HTTP-запитів. Нижче розглянуті різні аспекти, які варто враховувати:

1. **Пропускна здатність мережі:**
    - **Вимога:** Пропускна здатність сервера повинна бути великою, щоб забезпечити пересилання та обробку 5 Гбіт/с трафіку.
    - **Розрахунок:** 5 Гбіт/с = 5000 Мбіт/с
    - Таким чином, розрахунок буде:
    - 5000 Мбіт/с * (1 КБ/8 біт) = 625 МБ/с
    - **Висновок:** Сервер повинен мати пропускну здатність мережі близько 625 МБ/с. Рекомендовано 10Гбіт/с
2. **Процесор та пам'ять:**
    - **Вимога:** Сервер повинен бути оснащений швидкодійним процесором та достатньою обсягом оперативної пам'яті для обробки великої кількості HTTP-запитів.

- **Вибір:** Процесор Intel Xeon або AMD EPYC, 16 ядер і більше, 32 ГБ RAM.
- **Висновок:** Використання високопродуктивного процесора та достатньої ОЗП є критичним для швидкодії сервера під час атаки.

3. **Система зберігання даних (диск):**
   - **Вимога:** Швидкодія диска важлива для швидкого читання та запису даних, що може зменшити вплив атаки на ввод/вивід.
   - **Вибір:** 500 ГБ SSD
   - **Висновок:** Рекомендується використовувати SSD для забезпечення високої швидкодії.
4. **Захист від DDoS:**
   - **Вимога:** Механізми захисту від DDOS, такі як мережеві фільтри та розподілення трафіку, є критичними для запобігання перевантаженню сервера.
   - **Вибір:** Хмарний Сервіс Cloudflare



   - **Висновок:** Важливо мати надійні засоби захисту від DDOS, можливо, навіть співпрацювати зі спеціалізованими службами безпеки.
5. **Масштабованість:**

- **Вимога:** Система повинна бути горизонтально масштабованою, щоб легко додавати додаткові ресурси для реагування на збільшення навантаження.
- **Висновок:** Забезпечення масштабованості є ключовим аспектом для витримання атак із збільшеним обсягом трафіку.

Загальний висновок: Для успішного витримання атаки HTTP Flood обсягом 5 Гбіт/с протягом години, сервер повинен бути добре обладнаним мережево, має мати швидкодійні компоненти (процесор, пам'ять, диск) та ефективні заходи захисту від DDOS.

4.4 Висновки після розрахунків

Таблиця. 4.1

Рекомендовані характеристики

Вимога	Пояснення
Пропускна здатність мережі	Мінімум 5 Гбіт/с пропускної здатності. Вибір 10 Гбіт/с мережевої карти забезпечить швидке реагування на атаки.
Процесор (CPU) та Оперативна пам'ять (RAM)	Многоядерний процесор (Intel Xeon або AMD EPYC) та мінімум 16 ГБ RAM для ефективного управління ресурсами.
Системний диск (SSD)	Використання SSD обсягом 500 ГБ для швидкодійного доступу до даних, особливо під час атак та зберігання даних.
Захист від DDoS	Співпраця з провайдером з ефективним захистом та адаптацією до нових методів DDoS-атак.
Масштабованість	Можливість горизонтального масштабування

	через хмарну інфраструктуру або кластер серверів.
Система кешування	Використання систем кешування (наприклад, Varnish або Redis) для оптимізації та зменшення навантаження.

Розглянемо детально кожну вимогу та вибір для створення оптимального хостингу для витримання атаки "HTTP Flood".

1. **Пропускна здатність мережі:**
    - **Вимога:** Мінімум 5 Гбіт/с пропускної здатності.
    - **Пояснення:** Вибір пропускної здатності пов'язаний із здатністю сервера обробляти велику кількість запитів і передавати великий обсяг даних в мережі під час атаки. Вибір 10 Гбіт/с мережевої карти дозволяє мати запас пропускної здатності для забезпечення швидкого реагування на атаки.
2. **Процесор (CPU) та Оперативна пам'ять (RAM):**
    - **Вимога:** Швидкодійний многоядерний процесор та мінімум 16 ГБ RAM.
    - **Пояснення:** Процесор та RAM важливі для швидкодії обробки запитів і управління великою кількістю одночасних з'єднань. Вибір процесора Intel Xeon або AMD EPYC забезпечить високу продуктивність, а 16 ГБ RAM - достатньою кількістю пам'яті для ефективного управління ресурсами.
3. **Системний диск (SSD):**
    - **Вимога:** SSD для швидкодійного читання/запису даних.
    - **Пояснення:** Використання SSD є ключовим для швидкого доступу до даних, особливо під час атаки, коли ресурси значно збільшуються. Вибір SSD обсягом 500 ГБ дозволяє забезпечити достатньої місця для системи та зберігання даних.

4. **Захист від DDOS:**
    - **Вимога:** Ефективний захист від DDOS-атак.
    - **Пояснення:** Співпраця з хостинг-провайдером, який надає передові рішення для фільтрації та реагування на DDOS, є критично важливою. Рекомендується обирати провайдера з високим рівнем захисту та можливістю адаптації до нових методів атак.
5. **Масштабованість:**
    - **Вимога:** Можливість горизонтального масштабування для розширення ресурсів у випадку збільшення навантаження.
    - **Пояснення:** Масштабованість важлива для того, щоб можна було легко додавати ресурси та розподіляти навантаження. Використання хмарної інфраструктури або кластера серверів дозволяє гнучко адаптуватися до змін в обсязі роботи.
6. **Система кешування:**
    - **Вимога:** Використання систем кешування для оптимізації та зменшення навантаження на сервер.
    - **Пояснення:** Системи кешування, такі як Varnish або Redis, допомагають зменшити навантаження на сервер, забезпечуючи швидкий доступ до попередньо збережених даних, особливо в умовах атаки, коли швидкодія - ключовий фактор.

Ці рекомендації надають фундамент для створення оптимального хостингу для витримання атаки "HTTP Flood". Однак реальні потреби можуть бути уточнені в залежності від специфіки вашого веб-сайту та інших обставин.

DDOS-атаки є серйозним викликом для безпеки мереж та вимагають постійного вдосконалення захисту. Одним із типів таких атак є атака на рівень захисту служби, при якій зловмисники переповнюють систему

запитами, щоб вона більше не могла відповідати на легітимні запити користувачів.

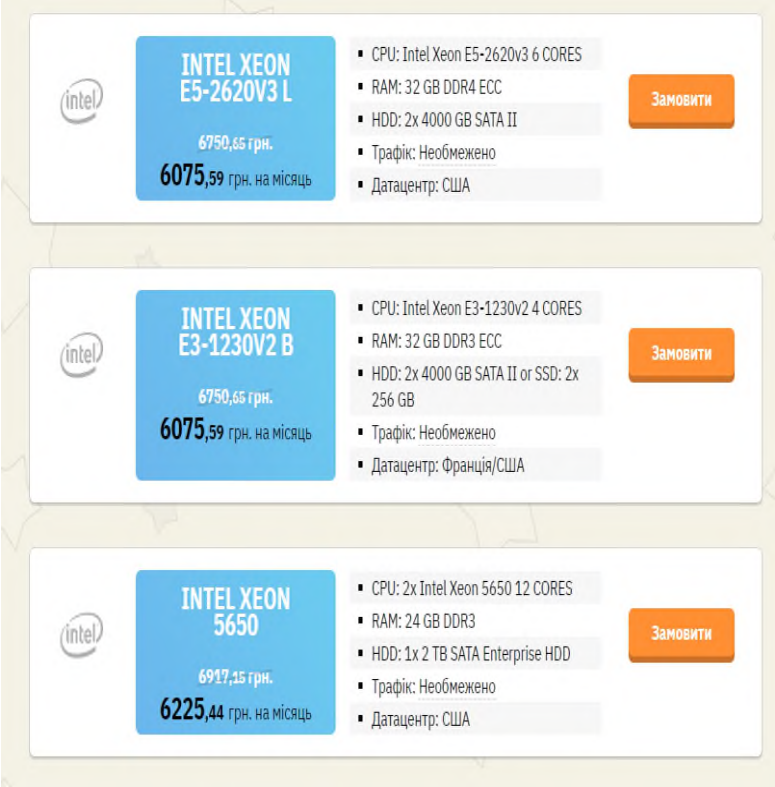
Різні рівні та типи DDOS-атак вимагають вивчення та аналізу, щоб розробляти ефективні методи протидії. Підвищення масштабів атаки, зокрема на великі бізнеси, ставить під загрозу функціонування та репутацію компаній. У таких випадках використання відокремлених серверів може стати ключовим заходом безпеки.

Одним з прикладів провідних українських хостингів, який спеціалізується на забезпеченні високого рівня безпеки, є HostiQ. Цей хостинг визначається надійністю і ефективністю своїх послуг. Зокрема, вони пропонують віртуальні приватні сервери (VPS), які можуть допомогти у вирішенні проблем DDOS-атак через ізоляцію ресурсів та забезпечення надійності мережі.

Щоб вдосконалити захист від DDOS-атак, компанії також використовують механізми виявлення та відповіді на інциденти, а також регулярно оновлюють програмне забезпечення та мережеве обладнання. Це дозволяє підтримувати високий рівень безпеки в умовах неперервно зростаючої загрози DDOS-атак.

Таблиця 4.2

Актуальні пропозиції HostiQ для великих проектів



У додаток до внутрішніх заходів безпеки та використання відокремлених серверів, компанії також можуть розглядати зовнішні сервіси для ефективного захисту від DDOS-атак. Один з таких сервісів - Cloudflare, пропонує різні пакети, призначені для захисту веб-сайтів від різних загроз, зокрема DDoS-атак.

Cloudflare відомий своєю глобальною мережею CDN, що дозволяє оптимізувати швидкість завантаження сторінок та зменшити ризик виникнення перевантажень на сервері під час DDOS-атак. Вони пропонують різні пакети для користувачів, які варіюються від базового рівня захисту до розширених функцій для корпоративних клієнтів.

Один із популярних пакетів - Cloudflare Business - включає захист від DDOS-атак та Web Application Firewall (WAF). Цей пакет призначений для

підприємств, які шукають комплексний захист та оптимізацію продуктивності.

Cloudflare Enterprise надає ще більше розширених функцій захисту та WAF, а також більше можливостей управління та налаштувань. Цей пакет може бути вибраний корпоративними клієнтами, які потребують високого рівня безпеки та індивідуалізованого підходу.

Крім того, Cloudflare Magic Transit - це спеціалізований пакет для захисту від DDOS для всієї мережі компанії. Цей варіант може бути важливим для організацій з великим обсягом трафіку, які шукають високоефективний та комплексний захист.

Важливо враховувати специфіку веб-сайту, обсяг трафіку та бюджетні обмеження при виборі пакету. Рекомендацією є звернутися до представників Cloudflare або скористатися їхнім калькулятором цін для отримання більш детальної інформації та консультацій, так як вони підбирають потрібні характеристики за запитом користувача.

ВИСНОВКИ

У сучасному цифровому світі, де зростаючий обсяг та складність кіберзагроз та DDOS атак стають великим викликом для бізнесу та організацій, ефективний захист інфраструктури стає пріоритетом. Цей дипломний проект розглядав різноманітні аспекти та методики розробки захисту від DDOS атак як на локальних серверах, так і на хмарних платформах.

Використання хмарних технологій для захисту від DDOS атак виявляється ключовим аспектом сучасних стратегій кібербезпеки. Велика еластичність та гнучкість цих хмарних рішень дозволяють організаціям ефективно масштабувати ресурси, глобально розподіляти захист, та мінімізувати вплив DDOS атак на локальні сервери. Проксі-сервіси та системи фільтрації трафіку, вбудовані в хмарні платформи, надають можливість реагувати на атаки на рівні хмари, зменшуючи навантаження на локальні сервери та забезпечуючи безперебійність обслуговування клієнтів.

У контексті локальних серверів важливим аспектом є вивчення різних типів DDOS атак та їх наслідків. Атаки на рівні застосунків можуть призвести до затримок у відповіді сервера та відмови в обслуговуванні веб-сайтів. Атаки на рівні мережі можуть спричинити відмову в обслуговуванні на рівні мережевих з'єднань та перевантаження комутаторів та маршрутизаторів. Ампліфікаційні атаки можуть викликати збільшення витрат пропускної здатності мережі та відмову в обслуговуванні при перевищенні мережевої пропускної здатності.

Методи виявлення DDOS атак, такі як використання сенсорів та аналіз трафіку, системи виявлення аномалій та інтелектуальні алгоритми, грають критичну роль у вчасному розпізнаванні та мінімізації впливу атак. Важливою є також аналіз та класифікація наслідків DDOS атак, що дозволяє розуміти шкоду, яку вони можуть завдати інфраструктурі та бізнес-процесам.

Розглянуті методи захисту від DDOS атак на локальних серверах та хмарних платформах включають в себе використання хмарних технологій, систем розподіленого захисту, та проксі-сервісів. Сучасні хмарні технології дозволяють мінімізувати вплив DDOS атак шляхом запобігання атакам ампліфікації, застосування систем виявлення та блокування, та гнучкою адаптацією до нових викликів кібербезпеки.

З проведених розрахунків випливає, що характеристики обраного серверу та хмарних сервісів відповідають потребам організації у високоефективному та надійному захисті від DDOS атак. Враховуючи всі аспекти, обговорені у цьому дипломному проекті, можна стверджувати, що поєднання локальних серверів із застосуванням хмарних технологій для захисту від DDOS атак формує потужний та комплексний механізм, здатний забезпечити надійний захист інфраструктури в умовах непередбачуваних кіберзагроз.

У цілому, даний дипломний проект спрямований на висвітлення актуальних проблем та сучасних стратегій захисту від DDOS атак. Впровадження розроблених методик та рекомендацій може значно поліпшити стійкість та безпеку інфраструктури, зменшуючи вплив DDOS атак на нормальну роботу бізнес-процесів.

ПЕРЕЛІК ПОСИЛАНЬ

1. "DDoS, Machine Learning, Measures". // "Understanding Denial-of-Service Attacks". / , 2016. – (Taylor & Francis Group). – (ISBN:13: 978-1-4987-2965-9). – С. 12–34.

2. The Crossfire Attack. // IEEE Symposium on Security and Privacy. – 2013. – С. 127– 142.

3. The Coremelt Attack [Електронний ресурс] – Режим доступу до ресурсу: https://netsec.ethz.ch/publications/papers/studer_esorics09.pdf.

4. D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events. // Journal of Network and Computer Applications. – 2018. – С. 49–63.

5. UPnP Design by Example, 2003. – (Intel Press). – (ISBN 0-9717861-1-9).

6. Internet Printing Protocol/1.0: Encoding and Transport [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc2565.

7. Security Flaws in Universal Plug and Play. // Rapid7. – 2013. – С. 10–11.

8. How DHCP Works [Електронний ресурс] // Oracle Corporation. – 2010. – Режим доступу до ресурсу: https://docs.oracle.com/cd/E19455-01/806-0916/6ja8539a4/index.html.

9. New DDoS Attack Method Demands a Fresh Approach to Amplification Assault Mitigation [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.imperva.com/blog/new-ddos-attack-method-demands-a-fresh-approachto-amplification-assault-mitigation/.

10. SSDP reflection DDoS attacks [Електронний ресурс] // Akamai. – 2014. – Режим доступу до ресурсу: https://www.akamai.com/fr/fr/multimedia/documents/state-ofthe-internet/ssdp-reflection-ddos-attacks-threat-advisory.pdf.

11. Threat Report DDoS. // NexusGuard. – 2018. – №3. – С. 7–8.

12. What is a DNS amplification attack [Електронний ресурс] – Режим доступу до ресурсу: https://www.imperva.com/learn/application-security/dns-amplification/. 61

13. Famous DDoS Attacks | The Largest DDoS Attacks Of All Time [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

Магістерська кваліфікаційна робота
на тему:

«Методика побудови системи захисту від DDOS атак»

Виконав: студент групи ТСДМ-63 Яцковський Г.С.
Керівник: доцент Малюженко М.В.

Київ-2025

Мета і завдання: розробка ефективної методики захисту від атак типу DDOS у межах інформаційних систем та мереж зв'язку. Робота спрямована на створення комплексного підходу, який забезпечить високий рівень захисту інформаційних ресурсів від масштабних та розмаїтих DDoS атак.

Об’єкт дослідження: Інформаційні системи та мережі зв'язку

Актуальність: Актуальність теми захисту від DDoS атак в сучасному цифровому середовищі визначається швидким розвитком технологій та збільшенням кількості онлайн-сервісів. Захист від DDoS стає важливим завданням, оскільки відсутність ефективного захисту може призвести до серйозних фінансових втрат, втрати репутації та перерв у обслуговуванні клієнтів.

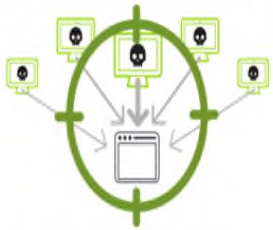
Актуальність теми, та визначення DDoS атак

В епоху, коли інформаційні технології проникають у всі аспекти сучасного суспільства, мережа Інтернет стає необхідною складовою нашого повсякденного життя. Зростання користувацької бази та перехід послуг у цифровий простір породжують високий попит на постійний та надійний доступ до мережі для максимізації доходу. Однак з розповсюдженням цифрових технологій збільшується й загроза Distributed Denial of Service (DDOS) атак.

DDOS атаки представляють собою спроби перекриття роботи веб-ресурсів чи комп'ютерних систем, переповнюючи їх запитаннями та знижуючи їх доступність. З використанням ботнетів, атакуючі можуть здійснювати атаки із розподіленого навантаження, ускладнюючи виявлення та протидію. Типи DDOS атак різноманітні, а їх масштаб та координація роблять їх особливо складними для виявлення та протистояння.







З урахуванням зростаючого ризику DDOS атак важливо розвивати ефективні методики захисту. У світі стрімкого технологічного розвитку, де важливу роль грають хмарні сервіси та пристрої Інтернету речей, кібербезпека стає ключовою проблемою. DDOS атаки впливають на найважливіші аспекти інтернет-екосистеми, а їх масштаб та організованість визначають необхідність постійного удосконалення захисних стратегій.

Захист мереж від DDOS атак постійно стикається з викликами, оскільки атаки стають все більш винахідливими та складними. Розробники заходів безпеки повинні постійно адаптуватися до нових видів атак, вивчаючи їхні особливості та модифікуючи захисні стратегії. Важливо розвивати інтелектуальні системи аналізу трафіку, щоб ефективно розпізнавати та блокувати атаки з мінімальним впливом на легітимний трафік.





Сучасні підходи до захисту включають у себе використання штучного інтелекту та машинного навчання для передбачення та виявлення аномального трафіку. Такі системи можуть вчитися на основі історичних даних та реагувати на нові атаки в режимі реального часу. Застосування технологій блокчейн також виводить захист на новий рівень, дозволяючи створити розподілену систему моніторингу та фільтрації трафіку.

Основні принципи DDoS атак

Зомбі-комп'ютери: Атакуючі використовують мережу комп'ютерів, зазомбованих шкідливим програмним забезпеченням, щоб скоординовано взяти участь у DDoS атаках.

Наслідки:

- Перевантаження ресурсів цільового сервера.
- Великі витрати пропускної здатності мережі.

Ампліфікація трафіку: Зловмисники використовують послуги, які надають ампліфікацію, збільшуючи обсяг трафіку для нападу.

Наслідки:

- Значний обсяг трафіку, який може призвести до відмови в обслуговуванні (DoS).
- Великі навантаження на цільові сервери та мережеві засоби



Синхронізовані атаки: Атаки, які виконуються одночасно з різних джерел для ускладнення виявлення та уникнення захисту.

Наслідки:

- Підвищений ризик успіху атаки.
- Утруднена можливість виявлення та блокування атак.

HTTP/HTTPS атаки: Використовуються для перевантаження веб-серверів за допомогою великої кількості запитів.

Наслідки:

- Зниження доступності веб-сервісів для законних користувачів.
- Великі обсяги надмірного HTTP трафіку.

DNS атаки: Напади на сервери доменних імен з метою перевантаження та призводження до відмови в обслуговуванні.

Наслідки:

- Втрата доступності веб-сайтів та інших ресурсів, пов'язаних із DNS.
- Можливість перехоплення DNS-запитів.

Типи і характеристики DDoS атак

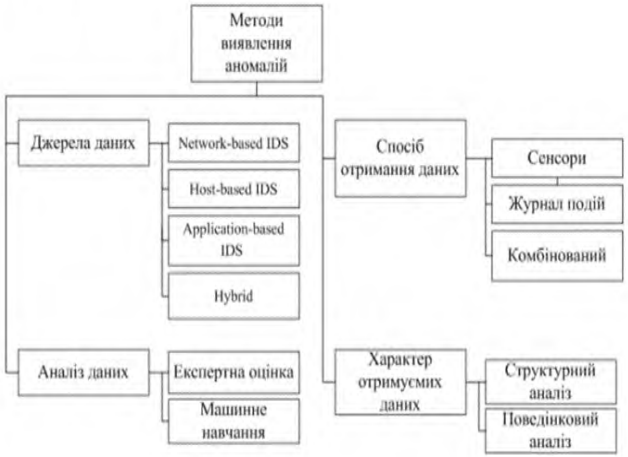
Тип атаки	Характеристики
ICMP Flood	Використовує протокол ICMP для надсилання великої кількості пакетів на жертву, що призводить до перевантаження мережі.
UDP Flood	Використовує протокол UDP для надсилання великої кількості UDP-пакетів на жертву, що завантажує мережу.
SYN/ACK Flood	Атака на сервери, які використовують TCP, надсилаючи багато невірних TCP-запитів, що забирає ресурси сервера.
HTTP Flood	Використовується для атаки на веб-сервери, надсилаючи велику кількість HTTP-запитів, що завантажує сервер.
DNS Amplification	Зловмисники використовують DNS-сервери для відправки великої кількості запитів з підміненими IP-адресами, щоб підсилити атаку.
Slowloris	Атака, в якій зловмисники встановлюють багато недоліких з'єднань з сервером і підтримують їх відкритими, споживаючи ресурси.
NTP Amplification	Використовує сервери точного часу для відправки великої кількості запитів з підміненими IP-адресами, щоб підсилити атаку.
Smurf Attack	Використовує IP-адресу жертви для надсилання ICMP-пакетів до мережі, що відповідає на них, перевантажуючи мережу.
DNS Flood	Атака на DNS-сервер, надсилаючи велику кількість запитів на вимін IP-адреси для доменних імен.
Volumetric Attack	Атака, яка переповнює мережу великою кількістю трафіку, заважаючи легітимному трафіку проходити.
Application Layer	Використовує вразливості на рівні додатків для атаки, наприклад, SQL-ін'єкції або переповнення буфера.
Reflection Attack	Використовує ампліфікацію, наприклад, використовуючи відкриті DNS-сервери або NTP-сервери, щоб збільшити потужність атаки.
Spoofed Attack	Зловмисники приховують свою ідентифікацію або IP-адресу, ускладнюючи виявлення та блокування атаки.

Засоби виявлення DDoS атак

- **Системи виявлення аномалій:**

- В основі систем виявлення аномалій лежить аналіз трафіку з метою виявлення незвичайних або несподіваних патернів поведінки. Алгоритми цих систем враховують різноманітні параметри, такі як обсяг пакетів, швидкість передачі даних, типи запитів та відповідей, та інші характеристики мережевого трафіку.

- Під час роботи системи виявлення аномалій використовують порогові значення, щоб визначити, коли певний показник перевищує нормативний рівень. Наприклад, зростання кількості запитів на один ресурс або підвищення швидкості трафіку може бути індикатором DDoS атаки. Аналізуючи ці аномалії, системи виявлення спроможні вчасно розпізнати потенційну загрозу та ініціювати відповідні захисні заходи.



- **Аналіз та класифікація аномалій у трафіку:** Системи виявлення аномалій базуються на аналізі широкого спектру параметрів мережевого трафіку для визначення відхилень від звичайних моделей. Вони ретельно аналізують пакети, що проходять через мережу, та звертають увагу на різноманітні характеристики, такі як час відповіді, обсяг передачі даних, типи запитів, та інші параметри. Наприклад, система може виявити аномалію великої кількості запитів на один ресурс, яка може бути характерною для атак DDoS. Аналіз типів запитів, які надходять, може розкрити використання певних атакуючих сценаріїв. Комбінування цих параметрів дозволяє системі розпізнавати навіть витончені форми атак та інші неправильності.

- **Вивчення характерних особливостей трафіку DDoS атак:** Аналізуючи характерні особливості трафіку, що характеризують DDoS атаки, системи безпеки можуть виділити та ідентифікувати певні патерни, що вказують на незвичайну або зловмисну діяльність. Наприклад, збільшення обсягу запитів на конкретний ресурс, різке підвищення частоти запитів, або зміна типів запитів можуть бути характеристиками DDoS атак.

- **Розробка ефективних алгоритмів для реагування та відсіювання трафіку:** Однак аналіз трафіку – це лише перший крок. Системи також потребують ефективних алгоритмів для реагування на виявлені аномалії та відсіювання легітимного трафіку від атак. Це може включати в себе використання фільтрації на рівні мережевих елементів, розподілене зберігання та обробка запитів або навіть редиректори трафіку для розгортання альтернативних ресурсів.Такий комплексний підхід забезпечує системі виявлення DDoS атак високий рівень ефективності та надійності, дозволяючи оперативно реагувати на різноманітні загрози та забезпечуючи безпеку мережевого середовища.



Розробка захисту від DDoS атак з використанням облакових технологій

Захист на рівні хмари визначається своєю здатністю працювати на великій території та забезпечувати централізовану, але еластичну оборону. Сучасні хмарові рішення використовують низку технік та стратегій для забезпечення повноцінного захисту від DDoS атак.

- **Проксі-сервіси та фільтрація трафіку:** Хмарні платформи можуть використовувати проксі-сервіси для фільтрації трафіку, що надходить до користувача. Це дозволяє відсіювати шкідливий трафік ще на рівні хмари, перед тим як він досягне локальної інфраструктури.

- **Розподілені системи захисту:** Застосування розподілених систем захисту в хмарових оточеннях дозволяє ефективно обробляти великі об'єми трафіку. Це здійснюється через використання глобальних мереж фільтрації, які можуть визначати та блокувати DDoS атаки на рівні глобальних вузлів.

Також Облачні технології не лише забезпечують захист на рівні хмари, але й мінімізують вплив DDoS атак на інфраструктуру, наприклад:

- **Автоматизована реакція на інциденти:** За допомогою інтелектуальних систем виявлення та реагування, хмарні області можуть автоматично визначати DDoS атаки та надавати миттєву відповідь. Автоматизована реакція зменшує час реакції на інцидент та підвищує ефективність захисту.

Порівняння облачних рішень для захисту від DDoS

Особливості	Amazon Web Services (AWS Shield)	Cloudflare	Akamai	Microsoft Azure (Azure DDoS Protection)
Типи DDoS-атак, що підтримуються	UDP і TCP флуди, HTTP флуди, ICMP флуди та інші	Всі типи DDoS-атак, включаючи веб-сервери та сетеві атаки	UDP і TCP флуди, SSL/TLS атаки, ICMP флуди та інші	UDP і TCP флуди, SYN/ACK атаки, ICMP флуди та інші
Мережевий пропускний потік	Від 40 Гбіт/с до сотень Гбіт/с	Від 100 Гбіт/с до Терабіт/с	Від 10 Гбіт/с до сотень Гбіт/с	Від 1 Гбіт/с до Терабіт/с
Глобальна мережева покриття	Так	Так	Так	Так
Аналітика трафіку	Так	Так	Так	Так
Можливість налаштування правил	Так	Так	Так	Так
Захист від заздалегідь відомих загроз	Так	Так	Так	Так
Технічна підтримка	24/7 служба підтримки	24/7 служба підтримки	24/7 служба підтримки	24/7 служба підтримки
Додаткові можливості	Інтеграція з AWS WAF, AWS Firewall Manager та іншими AWS-сервісами	Інтеграція з іншими Cloudflare сервісами, включаючи CDN	Інтеграція з іншими Akamai сервісами, CDN	Інтеграція з Azure Firewall, Azure Application Gateway таіншими Azure-сервісами

Таблиця представляє об'єктивне порівняння різних облачних рішень для захисту від DDoS атак. Враховуючи параметри, які охоплюють ефективність, гнучкість, та цінову доступність, організації можуть зробити інформовані рішення щодо вибору найбільш відповідного захисту для своїх потреб.

Технічні відомості, як захиститись від DDOS атак

Захист від DDoS атак вимагає комплексного підходу, включаючи як заходи на рівні мережі, так і на рівні застосунків. Нижче подано деякі технічні заходи, які можна вжити для захисту від DDoS атак:

Firewalls та Фільтри:

- Використовуйте мережеві фільтри та файрволи для блокування трафіку від відомих атакуючих IP-адрес та застосовуваних підозрілих пакетів.
- *Мінуси:* Можливість легкої обхідної тактики для атакуючих, таких як використання змінених IP-адрес або розподілення атаки з великої кількості ботів.

Rate Limiting:

- Встановіть обмеження на кількість запитів чи пакетів, які може обробити сервер за певний час.
- *Мінуси:* Може призводити до втрати легітімного трафіку, якщо обмеження встановлено занадто низьким, що може вплинути на доступність та якість обслуговування.

Intrusion Prevention Systems (IPS):

- Використовуйте системи запобігання вторгнення для виявлення та блокування вразливостей та атак на рівні мережі та застосунків.

  Мінуси: Вимагає постійного оновлення для виявлення нових типів атак. Може виникнути проблема ложних позитивів, коли легітімний трафік помилково визначається як атака.

Трафік Scrubbing Services:

- Перенаправляйте весь вхідний трафік через спеціалізовані служби заборони, які виявляють та фільтрують атаки перед тим, як вони досягнуть вашого сервера.

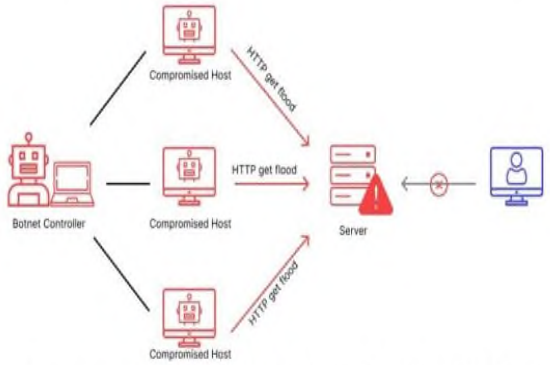
  Мінуси: Вартість таких послуг може бути високою, особливо для великих обсягів трафіку. Затримка у фільтрації трафіку може виникнути при великих атаках.

Розробка захисту від DDoS атак

Нижче буде розглянуто приклад DDoS атаки "HTTP Flood" (або атака на рівні застосунків HTTP) - це вид атаки на веб-сервер, при якій зловмисник відправляє велику кількість HTTP-запитів на цільовий сервер з метою перевантаження його ресурсів та призведення до відмови в обслуговуванні (атака DDoS - атака).

Основна ідея HTTP Flood полягає в створенні великого обсягу трафіку, перевантажуючи сервер запитами на рівні HTTP. Атакуючий може використовувати різні методи для досягнення цієї мети, наприклад, створювати багато хибних запитів, звертатися до великої кількості різних URL або використовувати компрометовані ботмережі для масштабування атаки.

Мета HTTP Flood - перевантажити сервер так, щоб він не міг ефективно обробляти легітимний трафік, що може призвести до того, що сайт або веб-застосунок стають недоступними для звичайних користувачів.Для захисту від HTTP Flood можуть використовуватися різні техніки, такі як використання **CDN (Content Delivery Network) - географічно розподілена мережева інфраструктура, що дозволяє оптимізувати доправлення та розповсюдження контенту кінцевим користувачам в мережі Інтернет, WAF (Web Application Firewall) - сукупність моніторів та фільтрів, призначених для виявлення та блокування мережевих атак на веб-додаток**, фільтрація трафіку на рівні мережі, а також використання спеціалізованих програмних і апаратних засобів для виявлення та запобігання DDoS-атак.

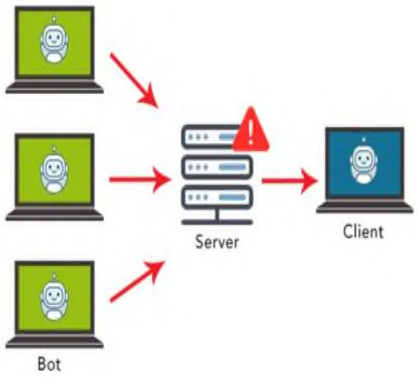


Наслідки атаки HTTP Flood можуть включати в себе недоступність веб-сайту або веб-додатка для користувачів, втрату репутації, фінансові збитки та інші проблеми, пов'язані з перервами у роботі відвідувачів.

Рогляд атаки HTTP Flood і розрахунок потрібних характеристик

Для витримання атаки HTTP Flood обсягом 5 Гбіт/с на протязі години, сервер повинен мати достатньо ресурсів, щоб обробляти і відповідати на велику кількість HTTP-запитів. Нижче розглянуті різні аспекти, які варто враховувати:

- Середній обсяг атаки складає: 5 Гбіт/с;
- Тривалість атаки: 1 година.



1. Пропускна здатність мережі:

- **Вимога:** Пропускна здатність сервера повинна бути великою, щоб забезпечити пересилання та обробку 5 Гбіт/с трафіку.
- **Розрахунок:** 5 Гбіт/с = 5000 Мбіт/с
- Таким чином, розрахунок буде:
- 5000 Мбіт/с * (1 КБ/8 біт) = 625 МБ/с
- **Висновок:** Сервер повинен мати пропускну здатність мережі близько 625 МБ/с. Рекомендовано 10Гбіт/с

2. Процесор та пам'ять:

- **Вимога:** Сервер повинен бути оснащений швидкодійним процесором та достатньою обсягом оперативної пам'яті для обробки великої кількості HTTP-запитів.
- **Вибір:** Процесор Intel Xeon або AMD EPYC, 16 ядер і більше, 32 ГБ RAM.
- **Висновок:** Використання високопродуктивного процесора та достатньої ОЗП є критичним для швидкодії сервера під час атаки.

- **Масштабованість:**
  - **Вимога:** Система повинна бути горизонтально масштабованою, щоб легко додавати додаткові ресурси для реагування на збільшення навантаження.
  - **Висновок:** Забезпечення масштабованості є ключовим аспектом для витримання атак із збільшеним обсягом трафіку.
- Загальний висновок: Для успішного витримання атаки HTTP Flood обсягом 5 Гбіт/с протягом години, сервер повинен бути добре обладнаним мережево, має мати швидкодійні компоненти (процесор, пам'ять, диск) та ефективні заходи захисту від DDoS.

Вимога	Пояснення
Пропускна здатність мережі	Мінімум 5 Гбіт/с пропускної здатності. Вибір 10 Гбіт/с мережевої карти забезпечить швидке реагування на атаки.
Процесор (CPU) та Оперативна пам'ять (RAM)	Многоядерний процесор (Intel Xeon або AMD EPYC) та мінімум 16 ГБ RAM для ефективного управління ресурсами.
Системний диск (SSD)	Використання SSD обсягом 500 ГБ для швидкодійного доступу до даних, особливо під час атак та зберігання даних.
Захист від DDoS	Співпраця з провайдером з ефективним захистом та адаптацією до нових методів DDoSатак.
Масштабованість	Можливість горизонтального масштабування через хмарну інфраструктуру або кластер серверів.
Система кешування	Використання систем кешування (наприклад, Varnish або Redis) для оптимізації та зменшення навантаження.

Висновок

У сучасному цифровому світі, де зростаючий обсяг та складність кіберзагроз та DDoS атак стають великим викликом для бізнесу та організацій, ефективний захист інфраструктури стає пріоритетом. Цей дипломний проект розглядав різноманітні аспекти та методики розробки захисту від DDoS атак як на локальних серверах, так і на хмарних платформах.

Використання хмарних технологій для захисту від DDoS атак виявляється ключовим аспектом сучасних стратегій кібербезпеки. Велика еластичність та гнучкість цих хмарних рішень дозволяють організаціям ефективно масштабувати ресурси, глобально розподіляти захист, та мінімізувати вплив DDoS атак на локальні сервери. Проксі-сервіси та системи фільтрації трафіку, вбудовані в хмарні платформи, надають можливість реагувати на атаки на рівні хмари, зменшуючи навантаження на локальні сервери та забезпечуючи безперебійність обслуговування клієнтів.







З проведених розрахунків випливає, що характеристики обраного серверу та хмарних сервісів відповідають потребам організації у високоефективному та надійному захисті від DDoS атак. Враховуючи всі аспекти, обговорені у цьому дипломному проекті, можна стверджувати, що поєднання локальних серверів із застосуванням хмарних технологій для захисту від DDoS атак формує потужний та комплексний механізм, здатний забезпечити надійний захист інфраструктури в умовах непередбачуваних кіберзагроз.

У цілому, даний дипломний проект спрямований на висвітлення актуальних проблем та сучасних стратегій захисту від DDoS атак. Впровадження розроблених методик та рекомендацій може значно поліпшити стійкість та безпеку інфраструктури, зменшуючи вплив DDoS атак на нормальну роботу бізнес-процесів.