**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

# ПОЯСНЮВАЛЬНА ЗАПИСКА

## кваліфікаційної роботи магістра

**галузь знань** *12 Інформаційні технології*
(шифр і назва галузі знань)

**спеціальність** *125 Кібербезпека*
(код і назва спеціальності)

**освітній ступень** *магістр*

**освітньо-наукова програма** *Кібербезпека*
(назва освітньої програми)

**на тему:** «Методи захисту веб-ресурсів від DDoS-атак»

**Виконавець:** студент ІІ курсу, групи КБм-21

(підпис) **Віктор МИРУН** (Ім'я, ПРІЗВИЩЕ)

| | **Ім'я, ПРІЗВИЩЕ** | **Підпис** |
|---|---|---|
| **Науковий керівник** | Володимир НАКОНЕЧНИЙ | |
| **Нормоконтроль** | Олена БОГУСЛАВСЬКА | |

**Київ 2023**

**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО:**
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

# ЗАВДАННЯ
## на виконання кваліфікаційної роботи

**спеціальності** *125 Кібербезпека*
(код і назва спеціальності)

**освітній ступень** *магістр*

**Здобувача** КБм-21 (група) Мируна Віктора Олександровича (прізвище ім'я по-батькові)

**Тема кваліфікаційної роботи** Методи захисту веб-ресурсів від DDoS-атак

### 1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 3 від 20.10.2022

### 2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

| | |
|---|---|
| **Об'єкт досліджень** | Процес захисту веб-сайтів від DDoS-атак |
| **Предмет досліджень** | Методи захисту веб-сайтів від повільних та малопотужних DDoS-атак |
| **Мета** | Досягнення підвищення ефективності захисту веб-сайтів від повільних та малопотужних DDoS-атак шляхом удосконалення моделі виявлення та блокування таких атак |

## 3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

**Наукова новизна** удосконалення моделі виявлення та блокування повільних DDoS-атак на основі прогнозування користувача

**Практична цінність** Підвищення ефективності захисту веб-сайтів від повільних та малопотужних DDoS-атак

## 4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

## 5. ЕТАПИ ВИКОНАННЯ РОБОТИ

| Найменування етапів робіт | Строки виконання робіт (початок-кінець) |
|---|---|
| Розробка плану для досягнення мети роботи | 24.10.2022 – 23.01.2022 |
| Аналіз літературних джерел | 24.01.2022 – 14.02.2022 |
| Розробка рекомендацій для удосконалення моделі виявлення та блокування повільних DDoS-атак на основі прогнозування поведінки користувача | 15.02.2022 – 24.04.2022 |
| Оформлення і друк пояснювальної записки | 25.04.2022 – 19.05.2023 |

## 6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

**Економічний ефект** Зниження збитків через DDoS-атаки

**Соціальний ефект** Покращення технологій захисту веб-сайтів від DDoS-атак.

## 7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Володимир НАКОНЕЧНИЙ
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Віктор МИРУН
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 24.10.2022 р.
Термін подання кваліфікаційної роботи до ЕК 19.05.2023 р.

УДК. 004.432.16

# РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Методи захисту веб-ресурсів від DDoS-атак»: 78 сторінок, 19 рисунків та 1 таблицю і 34 літературних джерел.

Об’єкт дослідження – процес захисту процес захисту веб-сайтів від DDoS-атак.

Мета роботи – досягнення підвищення ефективності захисту веб-сайтів від повільних та малопотужних DDoS-атак шляхом удосконалення методу виявлення та блокування таких атак

Методи дослідження – спостереження, аналіз, індукція.

У роботі досліджено актуальні види DDoS-атак та методи захисту веб-сайтів від даних кібератак. Проведено аналіз ефективності методів захисту веб-сайтів від повільних та малопотужних DDoS-атак.

Наукова новизна: розроблено пропозиції для удосконалення методу виявлення та блокування повільних та малопотужних DDoS-атак на основі прогнозування поведінки користувача.

Актуальність теми: DDoS-атаки є серйозною загрозою для будь-яких веб-сайтів. З кожним роком їх кількість зростає. Особливо це актуально для України оскільки на початку повномасштабного вторгнення розпочалась гібридна війна, в тому числі і кібервійна. Злочинці зі сторони нападників вдаються до атак рівня L7 на якому здійснюються більш “інтелектуальні” атаки.

Типовими представниками таких атака є повільні та малопотужні DDoS-атаки. Вони набули більш інтелектуального характеру оскільки вони є більш складними за інші атаки та з ними досить важко боротися. Тому питання в ефективній протидії таким атакам стоїть дуже гостро.

Ключові слова: кібератака, веб-сайт, DDoS-атака, повільна та малопотужна DDoS-атака, модель виявлення та блокування повільних та малопотужних DDoS-атак, прогнозування поведінки користувача.

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

| | | |
|---|---|---|
| **ПЗ** | – | Програмне забезпечення |
| **ШПЗ** | – | Шкідливе програмне забезпечення |
| **(D)DoS** | – | (Distributed) Denial-of-Service |
| **TTL** | – | Time to live |
| **ICMP** | – | Internet Control Message Protocol |
| **UDP** | – | User Datagram Protocol |
| **HTTP(S)** | – | Hypertext Transfer Protocol (Secure) |
| **OSI** | – | Open Systems Interconnection |
| **TCP** | – | Transmission Control Protocol |
| **SSL** | – | Secure Sockets Layer |
| **DNS** | – | Domain Name System |
| **NTP** | – | Network Time Protocol |
| **VoIP** | – | Voice over IP |

# ЗМІСТ

# ВСТУП

На відміну від більш традиційних атак великих потужностей, низькі та повільні атаки вимагають значно менше пропускної здатності і їх важко подолати, оскільки вони створюють трафік, який важко відрізнити від звичайного трафіку. У той час як великомасштабні DDoS-атаки, швидше за все, можуть бути помічені швидко, низькі та повільні атаки практично залишаються непоміченими протягом тривалого періоду часу, сповільнюючи обслуговування реальних користувачів.

Повільні DDoS-атаки не викликають різке збільшення трафіку, яке приводить до миттєвої відмови в обслуговуванні. Таким чином визначити момент початку атаки практично неможливо. Відповідно, значно ускладнюється відокремлення шкідливого трафіку від нормального.

Основна проблема в виявленні повільних DDoS-атак – це нездатність запобігти їм, оскільки процес визначення базується на вивченні існуючого трафіку без можливості його прогнозування в залежності від активності користувачів. Без сумніву, прогнозована поведінка користувачів дасть змогу виявити аномальну поведінку і запобігати появі повільних DDoS-атак.

Актуальністю даної роботи є удосконалення моделі виявлення та блокування повільних DDoS-атак на основі прогнозування поведінки користувача. Удосконалена модель може використовуватися для виявлення та блокування сучасних видів повільних та малопотужних DDoS-атак.

Тому метою своєї роботи автор бачить розв’язання питання підвищення ефективності захисту веб-сайтів від повільних та малопотужних DDoS-атак.

Для досягнення зазначеної мети необхідне вирішення наступних задач:

1. Розглянути та проаналізувати основні існуючі методи захисту веб-сайтів від DDoS-атак.

2. Дати оцінку їх ефективності для захисту веб-сайтів від повільних та малопотужних DDoS-атак.

3. Розглянути та проаналізувати модель виявлення та блокування повільних та малопотужних DDoS-атак.

4. Розробити пропозиції для удосконалення даної моделі.

*Науковою новизною* цієї кваліфікаційної роботи є розробка власних пропозицій для удосконалення існуючої моделі виявлення та блокування повільних і малопотужних DDoS-атак.

*Об'єктом дослідження* є процес захисту веб-сайтів від DDoS-атак.

*Предметом дослідження* є методи захисту веб-сайтів від повільних та малопотужних DDoS-атак.

*Методами дослідження* є методи аналізу, спостереження та індуктивний метод.

*Сформовані в результаті, теоретичні та практичні рекомендації* можуть бути використані для покращення моделі виявлення та блокування повільних та малопотужних DDoS-атак за допомогою прогнозування поведінки користувача.

# РОЗДІЛ 1
# ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО ПОНЯТТЯ КІБЕРАТАКИ. ОГЛЯД DDOS-АТАК

## 1.1 Поняття та основні види кібератак

Кібератака — навмисні дії в кіберпросторі, що здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або декількох цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» [1].

Кібератака - це свідомий і небажаний акт, спрямований на нанесення шкоди, перешкоджанню доступу або зламу системи, комп'ютерної мережі, програмного забезпечення або електронних пристроїв, використовуючи технології, пов'язані з комп'ютерами та мережами. Кібератаки можуть бути виконані з різних мотивів, таких як фінансова вигода, політичні цілі, крадіжка інформації або завдання шкоди репутації.

Метою кібератак можуть бути порушення нормального функціонування системи, викрадення важливої інформації, вплив на інфраструктуру, спричинення збитків або завдання іншої шкоди.

Цілі кібератак є досить різноманітними і залежать від мотивів та інтересів зловмисників. До найпоширеніших цілей кібератак відносяться [2]:

1. Крадіжка інформації. Кіберзлочинці можуть використовувати атаки для незаконного доступу до конфіденційної інформації, такої як особисті дані, фінансові відомості, бізнес-секрети або інтелектуальна власність. Ці дані можуть продаватись на чорному ринку або використовуватись для шахрайства, шпигунства, шантажу або нанесення шкоди конкурентам.
2. Злам інфраструктури. Зловмисники можуть намагатись проникнути в комп'ютерні мережі, системи керування, телекомунікаційні системи, електроенергетичні мережі або інші критичні інфраструктурні об'єкти. Це може призвести до перерви у роботі, зупинки послуг, економічних втрат або навіть загрози громадській безпеці.
3. Витік інформації. Зловмисники можуть спробувати викрасти, розповсюдити або оприлюднити конфіденційну або небажану інформацію. Це може бути особиста інформація про користувачів, внутрішні документи компанії, державні секрети, незаконно здобута інформація або інша важлива інформація, що може завдати шкоди особам, організаціям або суспільству в цілому.
4. Вплив на репутацію. Кібератаки можуть бути спрямовані на нанесення шкоди репутації іміджу особи, компанії, бренду або організації.
5. Фінансове шахрайство. Кіберзлочинці можуть використовувати атаки з метою шахрайства, які спрямовані на отримання фінансової вигоди. Це може включати шахрайство з використанням кредитних карт, крадіжку банківських реквізитів, шахрайства зі страховками, розповсюдження фішингових сайтів або вимагання викупу в обмін на відновлення доступу до системи або даних.
6. Перешкоджання нормальному функціонуванню. Кібератаки можуть бути спрямовані на створення перешкод нормальному функціонуванню системи, мережі або послуг.
7. Шпигунство та розвідка. Деякі кібератаки можуть бути спрямовані на отримання інформації з метою шпигунства або розвідки. Це може включати злам електронної пошти, незаконний доступ до комп'ютерних

систем, перехоплення комунікацій або викрадення інформації з метою отримання важливих даних, документів, планів або військової розвідки.

Наведені цілі кібератак залежать від мотивації зловмисників, їх цілей та типу атаки, яку вони використовують.

Кібератаки можна класифікувати за різними ознаками, такими як спосіб виконання, ціль атаки, використовувані засоби та інше.

Умовно кібератаки можна поділити [3, 4]:

1. За типом атаки:

- Віруси та хробаки. Віруси та хробаки є двома типами шкідливих програм, які поширюються в комп’ютерних системах і можуть завдати шкоди або виконати небажані дії без дозволу користувача. Основна відмінність між вірусами та хробаками полягає в їхньому методі поширення. Віруси є шкідливими програмами, які вбудовуються в існуючі файли або програми. Вони поширюються шляхом розповсюдження інфікованих файлів між комп’ютерами. Коли інфікований файл виконується, вірус активується і може розповсюджуватися далі шляхом інфікування інших файлів. Віруси можуть виконувати різноманітні шкідливі дії, включаючи видалення, модифікацію або шифрування файлів, знищення даних, перешкоджання нормальному функціонуванню системи або навіть отримання конфіденційної інформації. Хробаки є автономними шкідливими програмами, які можуть самостійно розповсюджуватися через комп’ютерні мережі, використовуючи вразливості або слабкі місця в системах. Вони можуть розповсюджуватись шляхом відправки копій себе на інші комп’ютери через електронну пошту, обмін файлами, веб-сайти або інші канали комунікацій. Коли хробак вражає комп’ютер, він може виконувати дії, включаючи копіювання, видалення або модифікацію файлів, встановлення зловмисного програмного забезпечення, перевантаження системи або створення ботнету (мережі комп’ютерів, що керовані зловмисниками).

- Фішинг. Фішинг є одним з найбільш поширених методів атак на інтернет-користувачів і полягає у використанні підроблених веб-сайтів, електронних листів або інших комунікаційних засобів для шахрайського здобування конфіденційних даних, таких як паролі, кредитні картки, банківські реквізити, особисті ідентифікатори тощо. Це соціально-інженерна атака, в якій зловмисники підробляютть себе під довірче джерело, щоб надурити свою жертву. Основна мета фішингу – отримати конфіденційну інформацію, що може бути використана для крадіжки грошей, ідентичності, доступу до систем або здійснення інших злочинів. Для досягнення цієї мети зловмисники застосовують різні методи, наприклад:

  - Підроблені веб-сайти: Зловмисники створюють підроблені веб-сайти, які схожі на офіційні веб-сайти банків, онлайн-магазинів, платіжних систем тощо. Жертвам надсилаються спамові листи або повідомлення з посиланнями на ці підроблені сайти, змушуючи їх ввести свої конфіденційні дані.

  - Соціальні мережі: Зловмисники використовують соціальні мережі, такі як Facebook, Twitter, Linkedln, для встановлення контакту з потенційними жертвами. Вони можуть створювати фальшиві профілі, які імітують відомих осіб або організації, і намагатися отримати конфіденційну інформацію через особисті повідомлення або спілкування.

  - Електронна пошта: Фішингові повідомлення надсилаються на електронну пошту, в яких зловмисники підробляються під відомі компанії, банки, служби підтримки. У таких повідомленнях можуть міститися посилання на підроблені веб-сайти або вкладені файли, які при відкритті виконують шкідливі дії.

  - Телефонні дзвінки: Зловмисники можуть здійснювати телефонні дзвінки, в яких вони видають себе за представників банків, компаній або служб підтримки. Вони намагаються отримати конфіденційну інформацію від жертв, таку як паролі, підтвердження тощо.

- (D)DoS атаки. (D)DoS атаки (розподілена)(атака з відмовою в обслугованні) – це форма кібератаки, в якій зловмисники намагаються перевантажити цільовий ресурс (веб-сайт, сервер, мережу) шляхом надмірного навантаження його інфраструктури. Атакуючи організацію або систему з багатьох джерел, DDoS-атаки спрямовані на перекриття доступу для легітимних користувачів та завдають шкоди нормальному функціонуванню послуги.
- Соціальний інжиніринг. Соціальний інжиніринг є методом маніпулювання, в якому зловмисники використовують психологічні та маніпулятивні техніки для отримання конфіденційної інформації або навмисного впливу на людей з метою отримання несанкціонованого доступу до систем, викрадення ідентифікаційних даних, розповсюдження шкідливого програмного забезпечення або здійснення інших кримінальних дій. Основна ідея соціального інжинірингу полягає в тому, що зловмисник використовує вразливості людської психології, довіри та недосконалості систем, щоб змусити людей виконувати певні дії або розкривати конфіденційну інформацію. Основні методи соціального інжинірингу включають:

  - Фішинг: Це використання підроблених електронних листів, веб-сайтів або повідомлень, щоб надати вигляд легітимних джерел і заманити людей виконати певні дії, такі як надання паролів, ідентифікаційних даних або фінансових реквізитів.
  - Відволікання: Це створення штучних ситуацій або використання відволікаючих технік, щоб звернути увагу людини на певний аспект та викликати в неї потребу відкрити доступ до системи або розкрити інформацію.
  - Імперсонація: Це представлення себе як авторитетного або довіреного джерела, такого як робітник служби підтримки, представник компанії або колега, з метою отримання доступу до систем або інформації.

- Соціальна інформація: Це збір інформації про людей з відкритих джерел, таких як соціальні мережі, дописи на форумах або відкриті джерела, для використання цієї інформації для атаки. Зловмисники можуть використовувати отриману інформацію для переконання людини в своїй автентичності або створення персоналізованих атак.

- Інжиніринг довіри: Це створення довірливих взаємин з людьми, шляхом будь-яких доступних засобів, таких як побудова відносин, допомога в розв'язанні проблем або надання допомоги, метою отримання несанкціонованого доступу або інформації.

Ці методи соціального інжинірингу можуть використовуватись окремо або комбінуватись для досягнення бажаної мети зловмисника. Основна ідея полягає в тому, щоб обманом змусити людей здійснити дії, які створюють безпекові ризики або розкривають конфіденційну інформацію.

2. За метою атаки:

- Фінансове шахрайство. Фінансове шахрайство (англ. financial fraud) - це вид злочину, який включає обман і маніпулювання з метою незаконного отримання грошей або інших матеріальних цінностей. Це одна з найбільш поширених форм кіберзлочинності, яка завдає серйозних фінансових втрат і пошкоджень для фізичних осіб, бізнесів і організацій. Фінансове шахрайство може приймати різні форми та використовувати різні методики для досягнення своїх цілей. До найпоширеніших видів фінансового шахрайства можна віднести:

- Фішинг. Зловмисники використовують електронні повідомлення, веб-сторінки або телефонні дзвінки для вигадки відомих організацій або осіб і спонукання людей надати свої конфіденційні дані, такі як паролі, номери кредитних карток або банківські реквізити. Ці дані потім використовуються зловмисниками для злочинних цілей, таких як крадіжка грошей з банківського рахунку або ідентифікаційний злочин.

- Бізнес–шахрайство. Це шахрайство, спрямоване на підприємства і організації. Воно може включати в себе такі дії, як вигадування фіктивних компаній, підроблення фінансових звітів, використання внутрішньої інформації для отримання незаконних фінансових вигод або незаконних дій з акціями компанії.

- Кредитне шахрайство. Цей вид шахрайства включає крадіжку особистих фінансових даних, таких я номери кредитних карток, для отримання незаконного доступу до чужого кредитного рахунку або використання чужих фінансових ресурсів. Зловмисники можуть використовувати ці дані для здійснення покупок, відкриття фальшивих рахунків або отримання кредитів на ім’я потерпілого.

- Інвестиційне шахрайство. Це шахрайство, пов’язане з фінансовими інвестиціями. Зловмисники можуть пропонувати фальшиві інвестиційні можливості або маніпулювати ринком для отримання незаконних прибутків. Вони можуть обманювати людей, обіцяючи високі прибутки, але насправді вкладення коштів зникають або нічого не приносять.

Фінансове шахрайство може мати серйозні наслідки для жертв, включаючи фінансові втрати, крадіжку особистої ідентичності, пошкодження кредитного рейтингу та негативний вплив на їх фінансову стабільність та життя.

- Шпигунство та розвідка. Шпигунство та розвідка – це види діяльності, спрямовані на отримання конфіденційної інформації про індивідів, організації, уряди та інші суб’єкти з метою політичних, військових, економічних або комерційних переваг. Ці терміни часто використовуються в контексті державної безпеки і міжнародних відносин, але шпигунство і розвідка можуть бути проведені як державними службами, так і недержавними суб’єктами. Шпигунство – це процес отримання та збирання конфіденційної інформації шляхом нелегального проникнення в об’єкт, використання підроблених документів, встановлення слідкування, або залучення джерел-шпигунів.

Шпигунство може включати перехоплення комунікацій, підроблення документів, розміщення підслуховуючих пристроїв або використання технологій кібершпигунства для отримання секретної інформації. Розвідка - це законна діяльність, яка полягає в систематичному зборі інформації з відкритих джерел, розвідувальних джерел, аналізі даних та інших джерел для оцінки загроз і забезпечення безпеки держави або організації. Розвідка може включати збір відомостей про ворогів, потенційних конкурентів, наукові розробки, технології, військові плани, політичні зміни та іншу важливу інформацію. Шпигунство та розвідка мають велике значення для державної безпеки та геополітичних відносин. Держави здійснюють розвідувальні дії для отримання інформації про ворогів, оцінки військових загроз, політичного впливу та іншої конфіденційної інформації. Крім того, комерційні організації можуть займатися шпигунством, щоб отримати конкурентні переваги, викрасти комерційну інтелектуальну власність або виконати інші злочинні дії. Основними методами шпигунства та розвідки можуть бути агентурна діяльність, відстеження, перехоплення комунікацій, кібершпигунство, використання джерел внутрішньої інформації, хакерство та соціальний інжиніринг. Основною метою цих дій є отримання конфіденційної інформації, яка зможе бути використана для стратегічних, політичних або економічних цілей.

- Саботаж. Саботаж – це діяльність, спрямована на нанесення шкоди, заваду або перешкоду в роботі, функціонуванні або виконанні завдань організацій, систем або інфраструктури. Саботаж може бути фізичним, технічним або кібернетичним. Саботаж може бути фізичним, технічним або кібернетичним, і його метою може бути знищення ресурсів, руйнування операцій або пошкодження репутації. Основна мета саботажу – знизити ефективність, відключити чи зупинити роботу системи, організації або інфраструктури. Дії саботажу можуть включати фізичне пошкодження обладнання, злам комп’ютерних систем, недоступність

сервісів або розповсюдження неправдивої інформації. Крім того, саботаж може мати різноманітні мотиви, включаючи політичні, економічні, соціальні або особисті. Він може бути проведений як внутрішнім агентами організації, так і зовнішніми суб'єктами, такими як конкуренти, хакери або терористичні групи. Саботаж може мати серйозні наслідки для цілей, які підлягають саботажу, включаючи фінансові втрати, порушення безпеки, втрату довіри клієнтів або громадських організацій, а також загрозу життю та здоров'ю людей.

- Активізація ворожих дій. Активізація ворожих дій відбувається, коли ворожа сторона збільшує свою активність і зосереджується на нападі або агресивних діях проти цілей, які вона вважає своїми противниками. У кібернетичній сфері активізація ворожих дій може включати збільшення кількості кібератак, хакерських вторгнень, поширення шкідливих програм або крадіжку конфіденційної інформації. Ці атаки можуть бути спрямовані на державні системи, комерційні підприємства або приватних користувача з метою завдання шкоди, отримання конфіденційних даних або впливу на критичну інфраструктуру.

3. За об'єктом атаки:

- Мережеві атаки. Мережеві атаки – це зловживання та незаконне використання мережевих ресурсів з метою завдання шкоди, отримання несанкціонованого доступу або порушення нормального функціонування мережевих систем. Ці атаки можуть бути спрямовані на комп'ютерні мережі, сервери, роутери, файрволи або будь-які інші пристрої, які забезпечують зв'язок і обмін даними. Існує безліч видів мережевих атак, і кожен з них має свою специфіку. До найпоширеніших з них відносять:
  - (D)Dos-атаки.
  - Фішинг.
  - Шкідливі програми (Malware)
  - Сканування портів
  - Man-in-the-Middle (MITM) атаки.

- Системні атаки. Це атаки, що спрямовані на операційні системи та інші компоненти системи, що використовуються для управління та функціонування комп'ютерів і мереж. Ці атаки мають на меті незаконне отримання доступу, знищення доступу, знищення даних, зміну налаштувань системи або завдання іншої шкоди. Прикладами системних атаках можуть слугувати:

  - Атаки на вразливості безпеки ОС. Це атаки, що використовують вразливості в операційній системі, такі як слабкі паролі адміністратора, недостатнє оновлення системи або наявність вразливостей в програмному забезпеченні. Зловмисники можуть скористатися цими вразливостями для незаконного доступу до системи, виконання коду або запуску шкідливих програм.

  - Атаки на аунтефікацію. Це атаки, спрямовані на злам паролів або механізми аунтефікації користувачів. Це може включати перебір паролів, використання вразливостей автентифікаційних протоколів або соціальний інжиніринг для отримання доступу до системи.

  - Атака на вразливості програм. Зловмисники можуть використовувати вразливості в програмах, що встановлені на системі, для незаконного отримання доступу або виконання шкідливого коду. Це може бути вразливість у веб-браузері, електронний пошті або інших програмах, які використовуються на системі.

  - Rootkit атаки. Це набір програм, що приховують свою присутність на комп'ютері або маскують діяльність інших шкідливих програм. Зловмисники використовують rootkit для незаконного отримання доступу до системи, виконання шкідливого коду або зміни налаштувань системи (рис. 1.1).

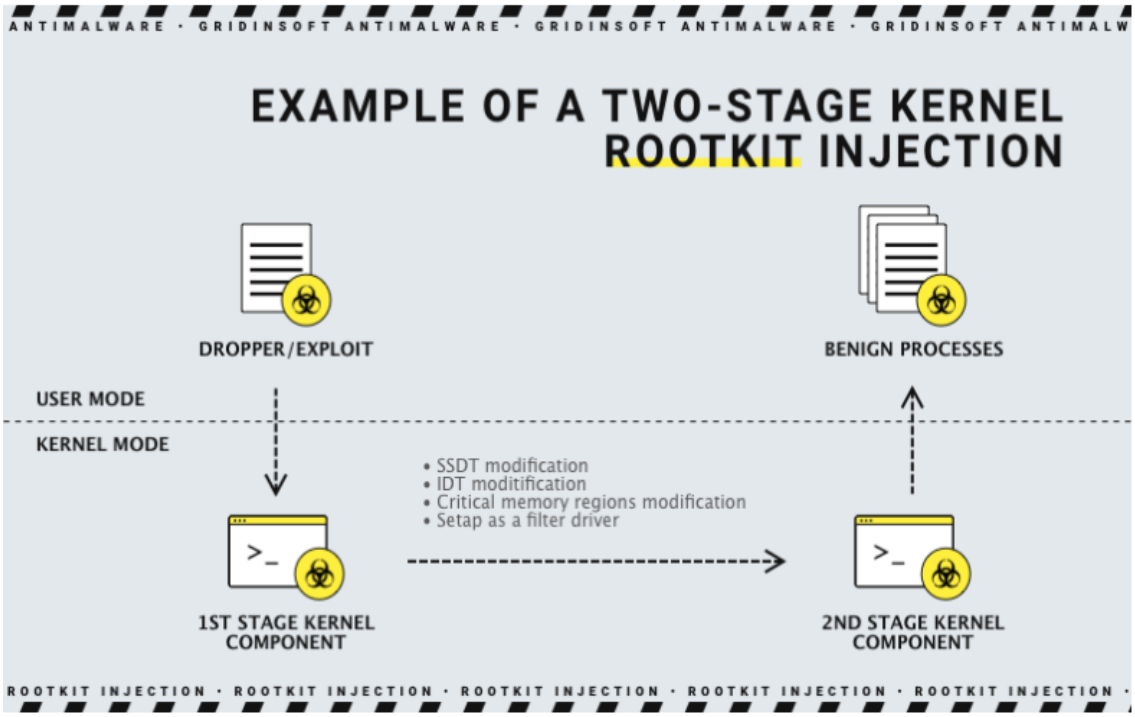



Рисунок 1.1 – Приклад роботи руткіт

- Ескейп-атаки. Даний вид атак спрямований на отримання доступу до підсистеми або режимів, до яких зловмиснику не повинно бути доступу. Наприклад, ескейп-атаки можуть дозволити зловмиснику отримати підвищені привілеї адміністратора або отримати доступ до ізольованих віртуальних середовищ.

Це лише кілька прикладів системних атак. Існує багато інших методів та вразливостей, які можуть бути використані зловмисниками для атак на системи.

- Прикладне програмне забезпечення. Кібератаки на прикладне програмне забезпечення (Application Layer Attacks) спрямовані на вразливості та слабкі місця в програмах, які використовуються для взаємодії з користувачами або надання послуг через мережу. Ці атаки часто мають на меті знищення функціональності програми, викрадення конфіденційної інформації, зміну налаштувань програми або незаконний доступ до системи. До основних кібератак на прикладне програмне забезпечення можна віднести:

- SQL Injection (SQL-ін’єкція). Ця атака використовується для отримання несанкціонованого доступу до бази даних, що використовується програмою. Зловмисники використовують вразливості в механізмах обробки SQL-запитів, вводячи шкідливий SQL-код у вхідні дані. Це може призвести до витоку важливої інформації, зміни або видалення даних в базі даних (рис 1.2).

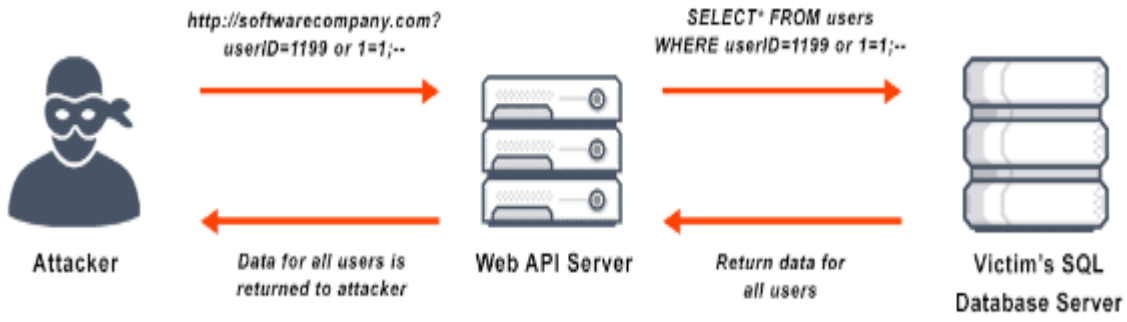



Рисунок 1.2 – SQL-ін’єкція

- Cross-Site Scripting (XSS, міжсайтовий скриптинг). Ця атака використовується для впровадження та виконання шкідливого скрипту на веб-сторінці, який відображається користувачам (рис.1.3). Зловмисники використовують вразливості веб-додатків, щоб впровадити шкідливий скрипт, який може перехоплювати дані, виконувати дії від імені користувача або перенаправляти на інші шкідливі сторінки.

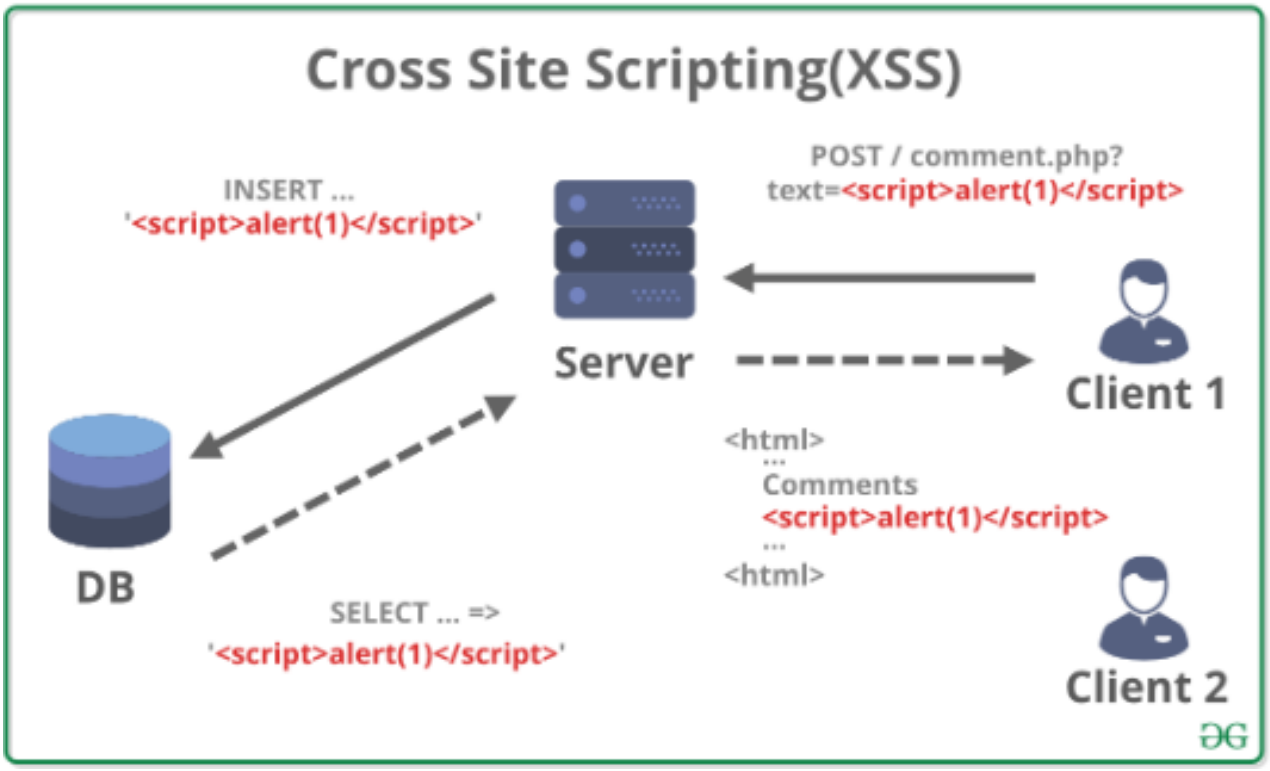



Рисунок 1.3 – Схема XSS

- Remote Code Execution (Віддалене виконання коду). Це атака, при якій зловмисники намагаються впровадити та виконати свій власний код на вразливій системі або програмі. Це може дозволити їм отримати повний контроль над системою, виконувати команди, отримувати конфіденційні дані або навіть поширювати іншу шкідливі програми.

- XML External Entity (XXE) атаки. Ці атаки використовуються для виклику небезпечних дій, використовуючи вразливості обробки зовнішніх сутностей XML. Зловмисники можуть зловживати можливістю завантаження віддалених файлів, виконання віддалених запитів або витоку конфіденційної інформації (рис.1.4).

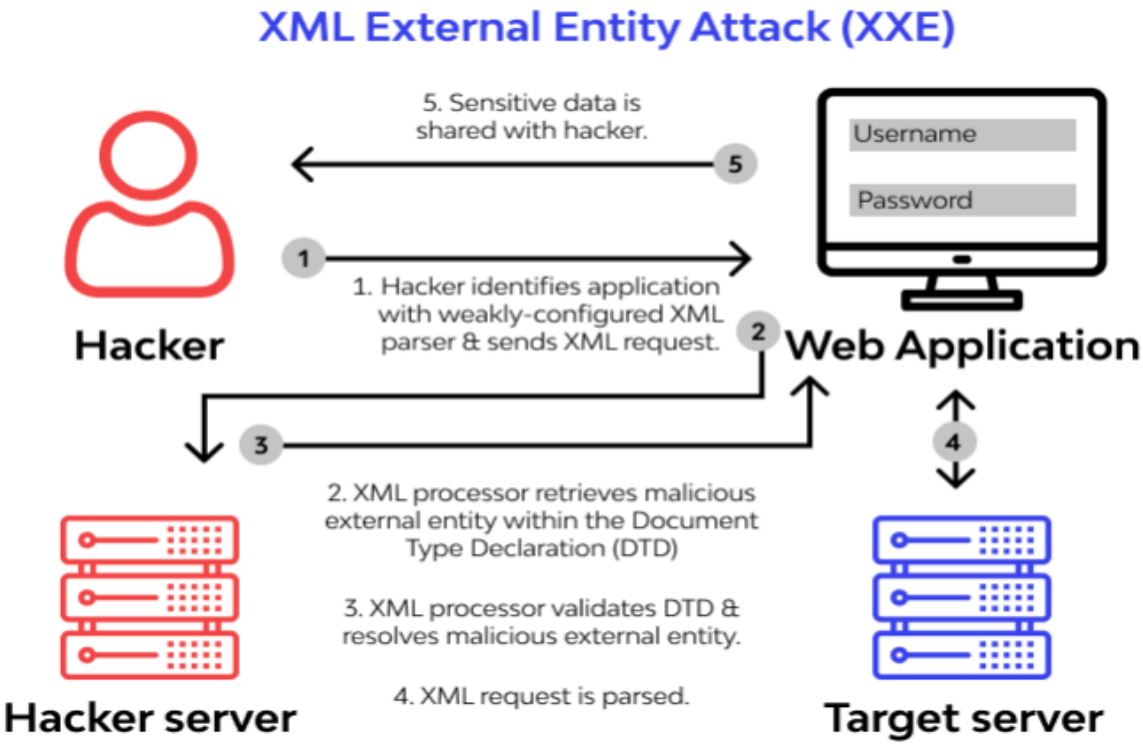



Рисунок 1.4 – XXE-атака

- Cross-Site Request Forgery (CSRF, міжсайтове підроблення запит). Ця атака залучає користувачів до виконання небажаних дій без їхньої належної авторизації. Зловмисники створюють спеціальні підроблені запити, які використовують довіреність аунтефікації користувача, шоб виконати небажані дії, такі як відправка фальшивих повідомлень або виконання несанкціонованих операцій на боці сервера.

- Remote File Inclusion (RFI) та Local File Inclusion (LFI). Ці атаки використовуються для включення та виконання віддалених або локальних файлів на цільовій системі. Зловмисники можуть скерувати програми на включення шкідливого коду або використовувати неправильне оброблення файлових шляхів для отримання доступу до конфіденційної інформації або виконання віддалених команд (рис. 1.5).

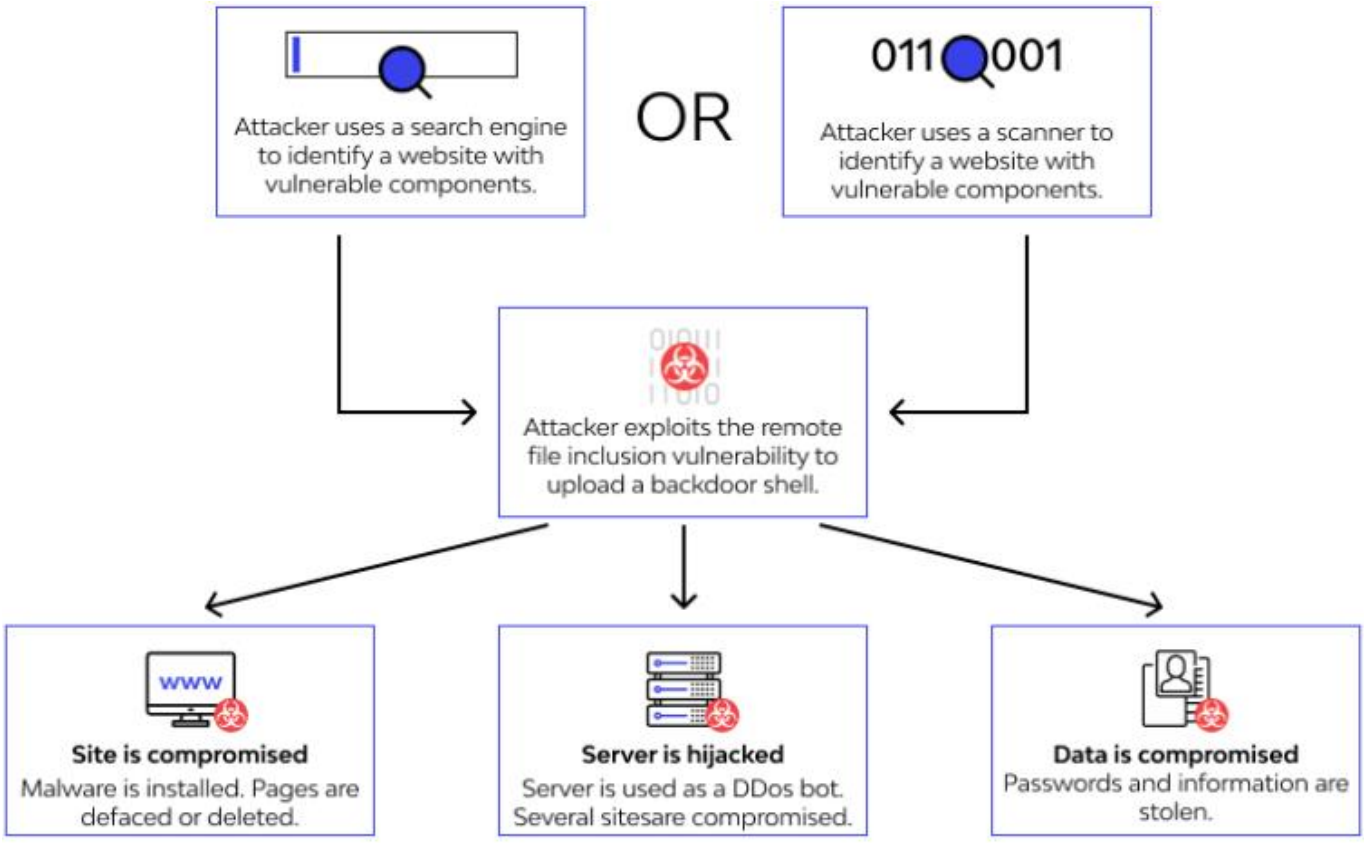



Рисунок 1.5 – Приклад RFI

Дана класифікація є загальною оскільки може існувати багато інших видів кібератак, які можуть бути специфічними для певних сценаріїв або використовувати нові методи та технології.

### 1.2 Наслідки кібератак

Кібератаки можуть мати серйозні наслідки, як для індивідуальних користувачів, так і для організацій та суспільства в цілому. До загальних наслідків кібератак можна віднести [5]:

- Втрата конфіденційності: Кібератаки можуть призводити до витоку конфіденційної інформації, такої як особисті дані користувачів, фінансові дані, комерційні та технічні відомості. Це може спричинити порушення приватності користувачів та втрату довіри.

- Пошкодження репутації: У разі успішної кібератаки організації можуть зазнати значних збитків у сфері репутації. Втрата довіри клієнтів і партнерів може призвести до втрати бізнесу та негативного впливу на фінансовий стан компанії.
- Втрата доступності: Деякі кібератаки спрямовані на перешкоджання нормальному функціонуванню систем або сервісів. Наприклад, DDoS-атаки можуть призвести до відмови в обслуговуванні, коли зловмисники намагаються перевантажити мережу або сервери шкідливим трафіком. Це може спричинити значні збитки в роботі бізнесу та втрату прибутків.
- Фінансові втрати: Кібератаки можуть призвести до прямих фінансових збитків, таких як втрата грошей з банківських рахунків, крадіжка ідентифікаційних даних для використання у шахрайських операціях або шахрайство з використанням кредитних карток. Крім того, організації можуть зазнати значних витрат на відновлення систем, виявлення і розслідування атаки, а також вдосконалення заходів безпеки для запобігання майбутнім інцидентам.
- Порушення безпеки користувачів: Кібератаки можуть використовуватись для отримання доступу до пристроїв користувачів, включаючи комп’ютери, смартфони, планшети та підключені пристрої Інтернету речей. Це може призвести до втрати особистої інформації, такої як паролі, фотографії, контакти, а також до зловживання цією інформацією зловмисниками.
- Порушення правової відповідальності: В разі виявлення кібератаки, зловмисників може очікувати правова відповідальність. Багато країн мають законодавство, що криміналізує кіберзлочини, і судові переслідування можуть мати серйозні наслідки для зловмисників.

Отже, кібератаки можуть нести серйозні наслідки як і для індивідуальних користувачів так і для організацій та суспільства в цілому.

### 1.3 Визначення та структура DDoS-атак

DDoS (Distributed Denial of Service) атака – це вид кібератаки, що полягає в нападі на інтернет-ресурси з наміром зробити їх недоступними користувачам [6].

Інтернет-ресурси є загальним терміном, який може включати в себе будь-який об’єкт, що може бути доступним через Інтернет, включаючи веб-сайти, онлайн-сервіси, ігрові сервери, банківські системи та інше. Саме ці об’єкти здебільшого є цілями нападу методом DDoS-атак. В контексті теми кваліфікаційної роботи буде розглянуто проблему і можливості щодо її мінімізації, яка пов’язана з DDoS-атаками на веб-сайти.

DDoS-атака на веб-сайти умовно складається з трьох основних етапів [7]:

1. Етап захоплення: Ініціатор DDoS-атаки застосовує спеціальний шкідливий код, що використовується для зараження комп'ютерів інших користувачів через Інтернет. Після зараження ці комп'ютери стають частинами ботнету - мережі комп'ютерів, що можуть бути використані для здійснення DDoS-атак. Бот-мережі створюють для зростання, автоматизації та прискорення здатності хакерів здійснювати масштабні атаки. Зловмисник керує групою захоплених пристроїв за допомогою дистанційних команд [7]. Після компіляції ботів злодій використовує командне програмування, щоб керувати своїми наступними діями. При цьому комп’ютерами-зомбі є кожен заражений зловмисним програмним забезпеченням (ПЗ) пристрій користувача, який є частиною ботнету. Ці пристрої підпорядковуються командам, розробленими ботом-пастухом. Умовно процес створення ботнету можна поділити на декілька кроків [8]:

- Підготовка та викриття – хакер використовує вразливість, щоб наражати користувачів на зловмисне програмне забезпечення.

- Інфікування – пристрої користувачів заражаються шкідливим програмним забезпеченням (ШПЗ), яке може отримати контроль над їх пристроєм.

- Активація – хакери мобілізують заражені пристрої для здійснення атак.

Першим кроком хакери знаходять вразливості веб-сайту, програми чи поведінки людини. Мета полягає в тому, щоб налаштувати користувача на несвідоме зараження шкідливим програмним забезпеченням. Зазвичай спостерігається, як хакери використовують проблеми безпеки програмного забезпечення чи веб-сайтів через електронні листи та інші онлайн-повідомлення.

На другому кроці пристрій жертви заражається шкідливим програмним забезпеченням ботнету після виконання дій, які компрометують його пристрій. Багато з цих методів передбачають переконання користувачів за допомогою методу соціальної інженерії завантажити спеціальний троянський вірус. Інші зловмисники можуть бути більш агресивними, використовуючи завантаження піратського ПЗ, як метод поширення вірусних файлів на зараженому веб-порталі. Незалежно від способу доставки, кіберзлочинці зрештою порушують безпеку комп'ютерів багатьох користувачів.

Останнім кроком створення ботнету є захоплення контролю над комп'ютером жертви. Зловмисник організовує всі заражені машини в мережу ботів, якими він може віддалено керувати.

Після зараження комп'ютер жертви надає доступ до операцій на рівні адміністратора, таких як [8]:

- Читання та запис системних даних.
- Збір персональних даних користувача.
- Відправка файлів та інших даних.
- Моніторинг дій користувача.
- Пошук вразливостей в інших пристроях.
- Встановлення та запуск будь-яких додатків.

2. Етап підготовки: Атакуючий підготовлює ботнет, наприклад, вибирає тип атаки, яку буде використовувати, та встановлює необхідні параметри. Цей етап може включати ідентифікацію цільового веб-сайту та його інфраструктури, визначення слабких місць та вибір найбільш ефективних методів атаки. Безперечно, в основі даного етапу лежить процес аналізу вразливостей об'єктів, що обираються, як цілі для DDoS-атак.

Аналіз вразливостей цілей для DDoS-атак – це процес визначення слабких місць у системі та пошук методів їх використання з метою завдання шкоди. Основними методами аналізу вразливостей цілей для DDoS-атак на веб-сайти є [9]:

a. Сканування портів: це процес перевірки доступності портів на сервері веб-сайту. Атакуючий може використовувати спеціальні програми для сканування портів з метою знаходження вразливостей та використання їх для запуску атаки.

b. Використання тестових векторів: це процес використання відомих вразливостей та побічних ефектів веб-додатків з метою виявлення слабких місць та вразливостей веб-сайту.

c. Аналіз логів: це процес аналізу записів в лог-файлах сервера веб-сайту, щоб знайти слабкі місця в захисті та можливість використання їх для запуску атаки.

d. Тестування на проникнення: це процес перевірки веб-сайту на наявність слабких місць в захисті шляхом спроб проникнення в систему на зміни її поведінки.

e. Моніторинг трафіку: це процес аналізу трафіку, який надходить на сервер веб-сайту з метою виявлення аномальних запитів та спроб атак.

f. Використання соціальної інженерії: це процес злочинної маніпуляції або переконання людей з метою отримання від них необхідної інформації.

Звичайно, аналіз вразливостей веб-сайту – це багатоаспектний процес, який може мати й інші методи чи підходи до процесу, але вищезгадані методи, на думку автора цієї роботи, є основними.

3. Етап атаки: Атакуючий запускає ботнет на цільовий веб-сайт з метою перевантаження сервера і зниження доступності веб-сайту для користувачів. Жертва атаки, тривалість атаки, а також особливості атаки, такі як тип, довжина TTL і номери портів можна регулювати. Зловмисники використовують доступну пропускну здатність, і кожен з них посилає велику кількість пакетів на цільовий хост або мережу, щоб негайно перенавантажити їх ресурси. Цей етап може включати такі типи атак, як наприклад SYN flood, ICMP flood, UDP flood, HTTP flood та інші.

Ця структура є загальною для більшості DDoS-атак на веб-сайти, але деталі можуть відрізнятися в залежності від типу атаки.

## 1.4 Класифікація DDoS-атак

Існує декілька основних класифікацій DDoS-атак [7]. Зокрема, вони поділяються на окремі види в залежності від:

- вибору атаки на основі рівнів моделі OSI;
- підходу, що використовується для запуску атак;
- обсягу створеного трафіку;
- динаміки рівня атаки.

### 1.4.1 Класифікація DDoS-атак за вибором атаки на основі моделі OSI

DDoS-атаки, що пов’язані з рівнями моделі OSI можна розділити на дві категорії: DDoS-атака прикладного рівня і атаки мережевого та транспортного рівнів [7].

При атаках прикладного рівня зловмисник використовує рівень 7, тобто протоколи, такі як HTTP і HTTPS, щоб передавати трафік жертві. Такий трафік зазвичай відправляє запити на сервер, що завантажує процесор та перешкоджає його нормальній роботі. Обсяг трафіку, необхідний для блокування сервера, є порівняно меншим, ніж в інших видах атак. Трафік в атаках прикладного рівня не відрізняється від легітимного, що ускладнює його виявлення.

Атаки на мережевому або транспортному рівнях зловмисник намагається вичерпати ресурси, такі як пропускна здатність або пам’ять пристроїв, таких як маршрутизатори, комутатори та брандмауери. Для досягнення цієї мети інфіковані машини передають жертві велику кількість трафіку в рівнях 3 і 4. Такі атаки зазвичай є об’ємними, від декількох сотень Мбіт/с до декількох сотень Гбіт/с, і використовують різні протоколи мережевого рівня, такі як протокол ICMP, протокол UDP та протокол керування передачею TCP. Найбільш часто використовувані DDoS-атаки мережевого рівня – це затоплення (перевантаження цільового сервера за допомогою великої кількості підроблених запитів) TCP/SYN, ICMP echo, UDP-flood, підсилення DNS та NTP.

### 1.4.2 Класифікація DDoS-атак за підходами для запуску атак

В DDoS-нападах не завжди скомпрометовані комп’ютери відправляють трафік жертві атаки. Сервери, які працюють на основі UDP-сервісів, часто використовуються кіберзлочинцями для проведення масштабних DDoS-атак. Такі сервери функціонують як рефлектори, якими користуються зловмисники. Залежно від способу використання комп’ютера для здійснення атаки, DDoS-атаки поділяються на дві категорії: прямі і рефлекторні [7].

У прямій атаці кіберзлочинець використовує скомпрометовані комп’ютери безпосередньо для запуску різних типів DDoS-атак (рис 1.6), тоді як у рефлекторній атаці часто використовуються багато невинних проміжних вузлів для посилення атаки.

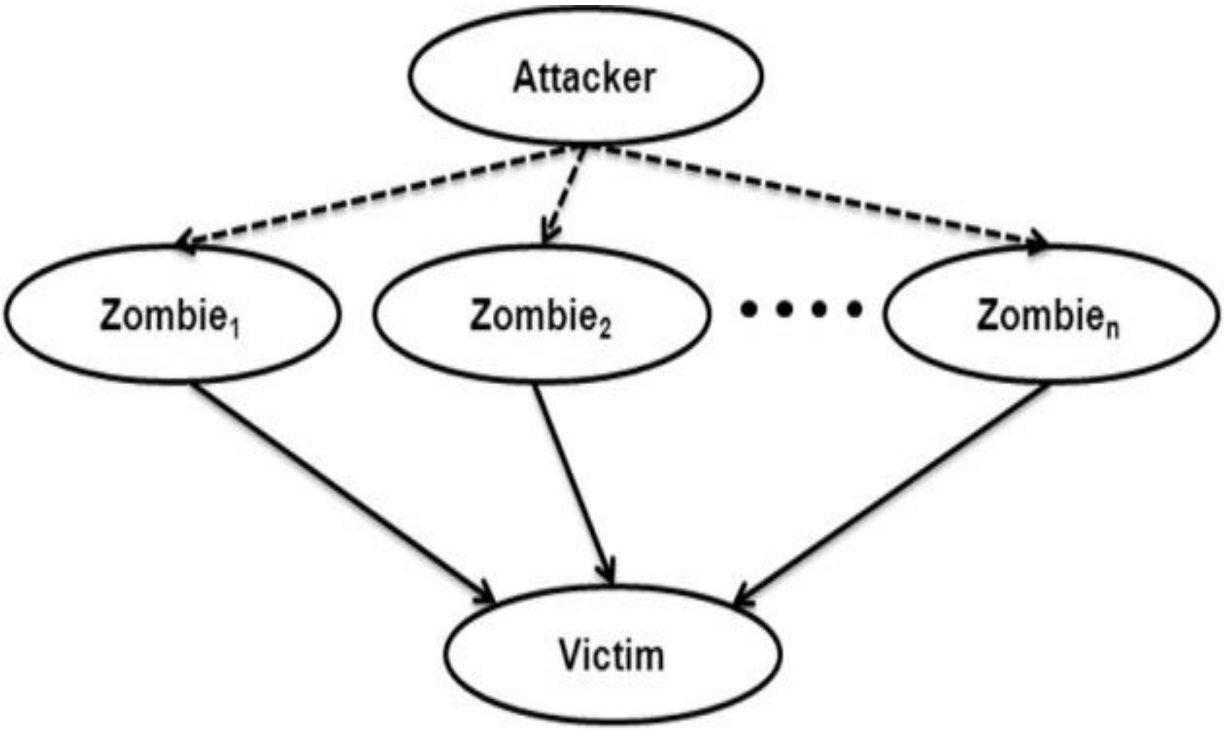



Рисунок 1.6 - Пряма DDoS-атака

Зловмисник посилає запити на рефлекторні сервери, замінюючи IP-адресу джерела, ніби вона була IP-адресою жертви (рис.1.7). В результаті ці сервери

відповідають жертві, надсилаючи повідомлення, обсяг яких зазвичай у багато разів перевищує початковий розмір повідомлення запиту. Тому цей тип DDoS-атаки також відомий як атака з підсиленням [7].

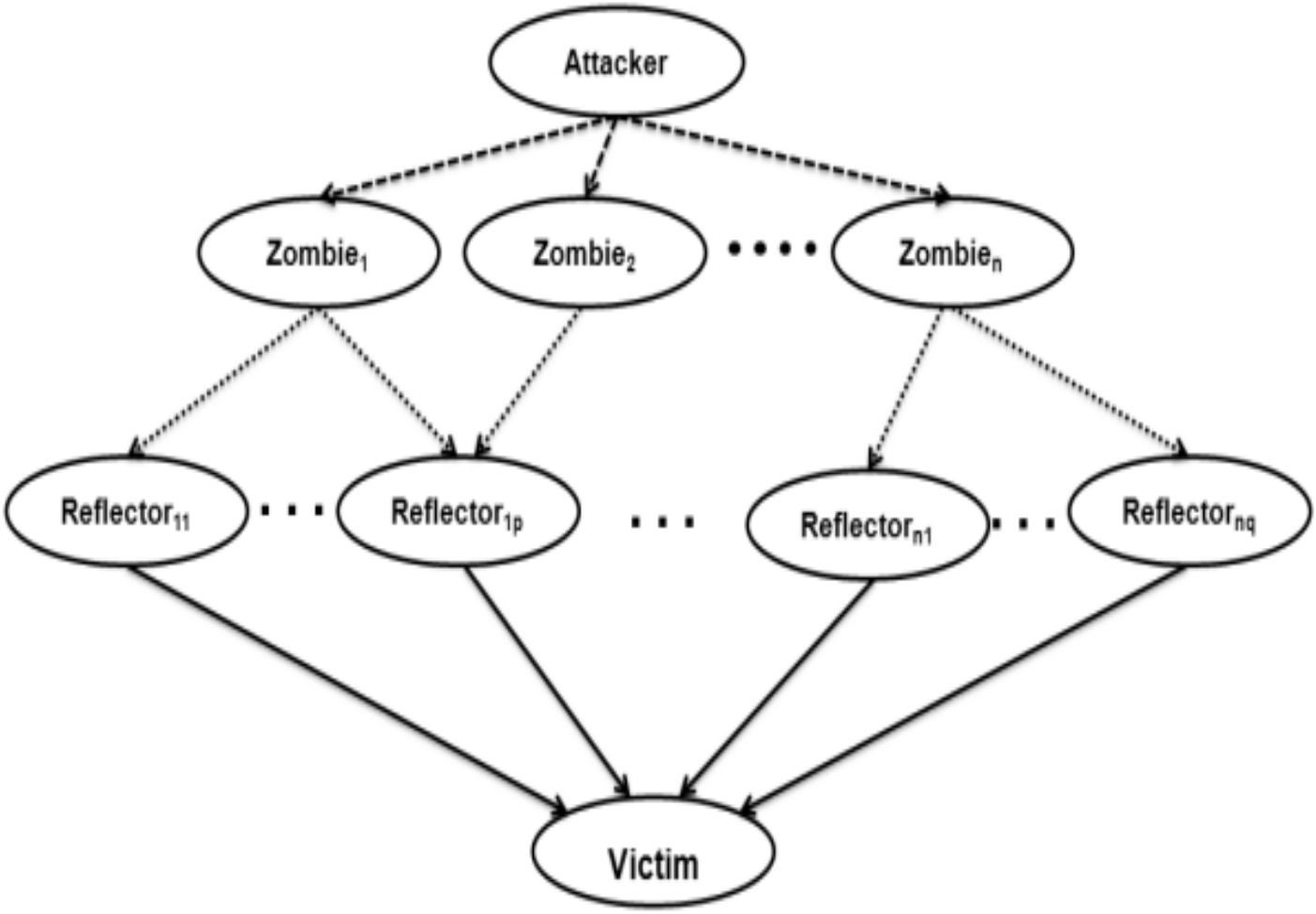



Рисунок 1.7 - Рефлекторна DDoS-атака

Зловмисник використовує цю техніку для посилення трафіку атаки до декількох сотень разів. Використання DNS і NTP для посилення атаки є прикладами DDoS-атак на основі відображення.

Також на основі підходу, що використовується в залежності від шляху передачі трафіку DDoS-атаки можна розділити на прямі й непрямі. У прямій атаці зловмисник відправляє трафік безпосередньо до жертви, користуючись багатьма скомпрометованими машинами.

При непрямій атаці злодій, замість безпосередньої атаки на жертву, атакує інші сервіси, котрі є важливими для того, щоб жертва залишалася функціональною. Атаки типу Link flooding, такі як crossfire і coremelt, є прикладами непрямих DDoS-атак.

### 1.4.3 Класифікація DDoS-атак за обсягом створеного трафіку

DDoS-напади також можуть бути розділені на основі обсягу трафіку, який може бути як малим, так і великим. У випадку DDoS-атаки з низькою швидкістю, зловмисник зазвичай намагається напасти, відправляючи трафік атаки повільно і з низькою швидкістю, що схоже на легітимний трафік.

Наприклад, у випадку атаки на рівні додатку, зловмисник намагається знищити ресурси процесора жертви, відправляючи запит, який вимагає великої кількості ресурсів процесора. Також існує shrew-напад, де обсяг трафіку порівняно невеликий [7].

У потужних DDoS-атаках зловмисник надсилає на жертву величезний обсяг трафіку, це найпоширеніший тип DDoS-атак. Іноді великий об’єм трафіку, відомий як “flash crowd”, помилково сприймають за DDoS-атаку, це може призвести до відмови в обслуговуванні законних запитів користувачів.

Однак “flash crowd” можна відрізнити від шкідливого трафіку, спостерігаючи за швидкістю введення нових адрес. У “flash crowd” раптово вводяться нові IP-адреси, що нагадує “flooding attack”, але швидкість введення нових IP-адрес зменшується через деякий час, хоча рівень запитів від нескомпрометованих користувачів може залишатися високим.

Класифікація DDoS-атак за обсягом створеного трафіку дозволяє розуміти різний рівень навантаження, який може бути згенерований нападниками. Враховуючи цей аспект, організації можуть приймати відповідні заходи захисту, щоб запобігти атакам або пом'якшити їх наслідки.

### 1.4.4 Класифікація DDoS-атак за динамікою рівня атаки

Крім згаданої вище категоризації, DDoS-атаки можуть бути розподілені за іншими ознаками трафіку, наприклад за динамікою швидкості атаки (рис. 1.8) DDoS-атаки за динамікою швидкості можна розподілити на чотири типи [7]:

i. Атака сталої швидкості: Швидкість атаки досягає максимального значення протягом дуже короткого періоду часу. Всі інфіковані машини, що отримали команду від зловмисника, починають відправляти трафік з постійною швидкістю. Цей вид атаки створює раптовий потік пакетів на стороні жертви.

ii. Атака зі збільшенням швидкості: Замість того, щоб атакувати жертву з повною силою миттєво, зловмисник поступово збільшує інтенсивність атаки. Зловмисник використовує збільшення інтенсивності атаки, щоб зрозуміти реакцію жертви на атаку та уникнути механізмів виявлення жертви.

iii. Пульсуюча атака: У цьому випадку атакуючий періодично активує групу ботів, щоб передати трафік жертві. Такий механізм використовується для того, щоб залишатися непоміченим від виявлення. Shrew 52 є прикладом пульсуючої DDoS-атаки, яка передає короткі синхронізовані пакети трафіку для зриву TCP-з'єднань на одній лінії, використовуючи слабкість механізму тайм-ауту повторної передачі TCP.

iv. Атака підгрупами: Як і у випадку пульсуючої атаки, тут атакуючий також посилає імпульси трафіку жертві. Однак інфіковані машини поділяються на групи і ці групи активуються і деактивуються в різних комбінаціях. Такий комбінований підхід атаки використовується зловмисником, щоб залишатися замаскованим і продовжувати атаку протягом більш тривалого часу.

Класифікація DDoS-атак за динамікою рівня атаки дозволяє розуміти різні підходи та стратегії, що використовуються нападниками для затримки або унеможливлення функціонування цільової системи. Розуміння цих типів атак допомагає в розробці ефективних заходів захисту та виявлення DDoS-атак.

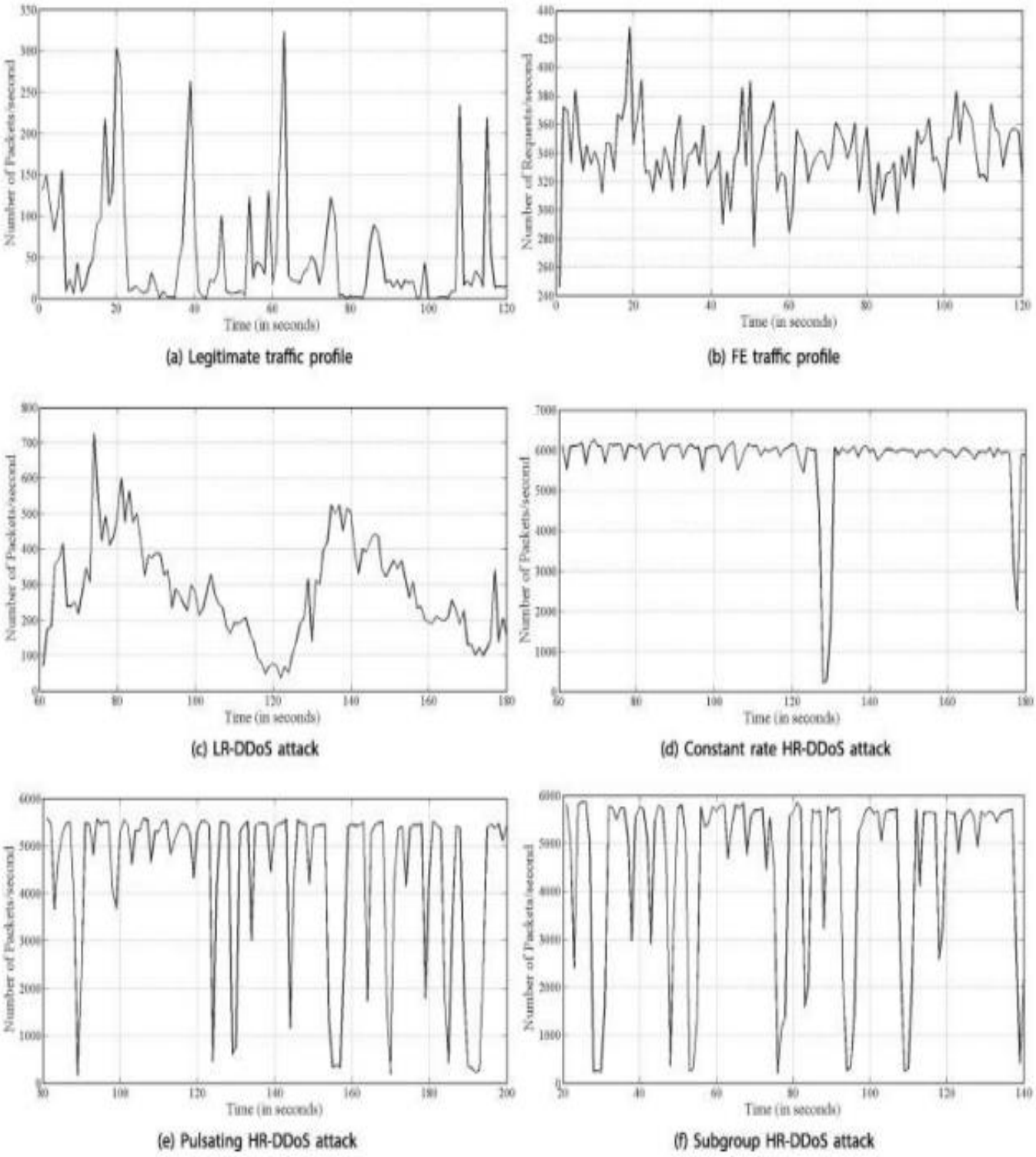



Рисунок 1.8 – Типи атак на основі динаміки

На рисунку 1.8 відображено графіки DDoS-атак на основі динаміки швидкості, а також їх порівняння з графіком легітимного трафіку.

## 1.5 Масштаби впливу DDoS-атак на веб-сайти

З кожним роком явище DDoS-атаки спостерігається дедалі частіше і немає жодних ознак уповільнення їх розповсюдження. Згідно з останніми дослідженнями, очікується, що кількість DDoS-атак у 2023 році зросте більш ніж на 300% [10]. Це викликає серйозне занепокоєння як для компаній, так і для окремих осіб, оскільки ці атаки можуть завдати серйозної шкоди як особистим, так і корпоративним веб-сайтам.

### 1.5.1 Статистика DDoS-атак за 2022-2023 роки

Ось деякі з найпопулярніших статистичних даних DDoS-атак за 2022-2023 роки [10]:

1. Відповідно до квартального звіту “Лабораторія Касперського” зареєструвала 57116 DDoS-атак.

2. “Cloudflare” стверджує, що у 2022 році кількість DDoS-атак з викупом зросла на 67%.

3. П’ятниця була найактивнішим днем атак з результатом 15,36% від загальної кількості атак, тоді як відсоток атак був найнижчим у четвер - маючи 12,99%.

4. У 2022 році компанії в США, Великобританії та Канаді постраждали від DDoS-атак на провайдерів VOIP.

У 2022 році було зафіксовано кілька надзвичайних DDoS-атак, особливо в третьому кварталі. Світ став свідком кількох рекордних атак. Ці атаки часто є політично вмотивованими і можуть здійснюватися з кількох географічних регіонів одночасно [10].

1 червня атака на клієнта Google Cloud Armor побила чимало рекордів.

Послідовність HTTPS DDoS-атак досягла рекордного піку – 46 мільйонів запитів на секунду [10].

Це найбільша DDoS-атака на рівні програми, про яку повідомлялося на сьогоднішній день, на 77% більше, ніж друга за величиною атака, коли-небудь зареєстрована.

Ця атака була здійснена з понад 5000 IP-адрес у 132 країнах.

30 відсотків трафіку, надісланого під час цієї атаки, було з чотирьох країн: Бразилії, Індії, Росії та Індонезії [10].

Рухи DDoS-атак були досить заплутаними протягом 2022 року

Оскільки DDoS виникає з різних соціально-політичних мотивів, глобальна політика та економіка часто сприяють моделям атак. Нижче наведено кілька цікавих фрагментів звіту Cloudflare про загрози DDoS.

DDoS-атака зі швидкістю 26 мільйонів запитів на секунду почалася з невеликого, але потужного ботнету з 5067 пристроїв. Щоб оцінити міцність цієї мережі, Cloudflare порівняв його іншим відомим компанії бонетом, який містить понад 730 000 пристроїв. Останній не зміг генерувати більше мільйона запитів в секунду.

Компанія Cloudflare, що допомагає підтримувати безпеку, конфіденційність та швидку роботу сервісів у інтернеті, автоматично виявила та пом’якшила найбільшу DDoS-атаку HTTPS за історію

Атака була спрямована на вебсайт неназваного клієнта за допомогою безкоштовного плану Cloudflare. Вона тривала менш ніж за 30 секунд. За цей час ботнет створив понад 212 мільйонів HTTPS-запитів із понад 1500 мереж у 121 країні. Більшість походила з Індонезії, США, Бразилії та Росії.

Попередній рекорд за кількістю запитів належав HTTPS DDoS-атаці, яку Cloudflare зафіксував у квітні. Під час неї відбувалось 15,3 мільйона запитів на секунду.

У 2022 році DDoS-атаки HTTP зросли на 111% порівняно з 2021 роком, а кількість атак програм-вимагачів зросла на 67% за той самий період [10].

Статистика QoQ дещо інша: 10% зниження в Q3 порівняно з Q2.

У певних географічних регіонах є деякі неймовірні відхилення від цієї моделі.

Між другим і третім кварталами 2022 року на Тайвані спостерігався тривожний сплеск HTTP DDoS-атак на 200% [10].

Атаки на Японію за той же період зросли на 105% [10].

Тенденції DDoS-атак за 1 квартал 2023 року від компанії Cloudflare [10]:

- Спостерігалось збільшення кількості гіпероб'ємних DDoS-атак, запущених іншими загрозливими суб'єктами, причому найбільша з них перевищила 71 мільйон запитів на секунду (rps), що перевищило попередній світовий рекорд Google у 46 мільйонів rps на 55%. Гіпероб'ємні атаки використовують нове покоління ботнетів, які складаються з віртуальних приватних серверів (VPS) замість пристроїв Інтернету речей (IoT). Історично склалося так, що великі бот-мережі покладалися на придатні для експлуатації пристрої IoT, такі як розумні камери безпеки, щоб оркеструвати свої атаки. Незважаючи на обмежену пропускну здатність кожного IoT-пристрою, разом — зазвичай нараховуючи сотні тисяч або мільйони — вони генерували достатньо трафіку, щоб порушити свої цілі. Нове покоління ботнетів використовує незначну кількість пристроїв, але кожен пристрій є значно потужнішим. Постачальники хмарних обчислень пропонують віртуальні приватні сервери, щоб дозволити стартапам і підприємствам створювати ефективні програми. Недоліком є те, що це також дозволяє зловмисникам створювати високопродуктивні ботнети, які можуть бути в 5000 разів сильнішими.

- Ще одна велика атака, яка спостерігалась в першому кварталі, — DDoS-атака зі швидкістю 1,3 Тбіт/с (терабіт на секунду), спрямована на південноамериканського телекомунікаційного постачальника (рис.1.12). Напад тривав лише хвилину. Це була багатовекторна атака із залученням трафіку атак DNS і UDP. Атака була частиною ширшої кампанії, яка включала численні атаки на Terbit, які походили з 20 000-ти сильних ботнетів типу Mirai. Більшість трафіку атак надходила зі США, Бразилії, Японії, Гонконгу та Індії. Системи Cloudflare автоматично виявили та пом'якшили його без будь-якого впливу на мережі клієнта.

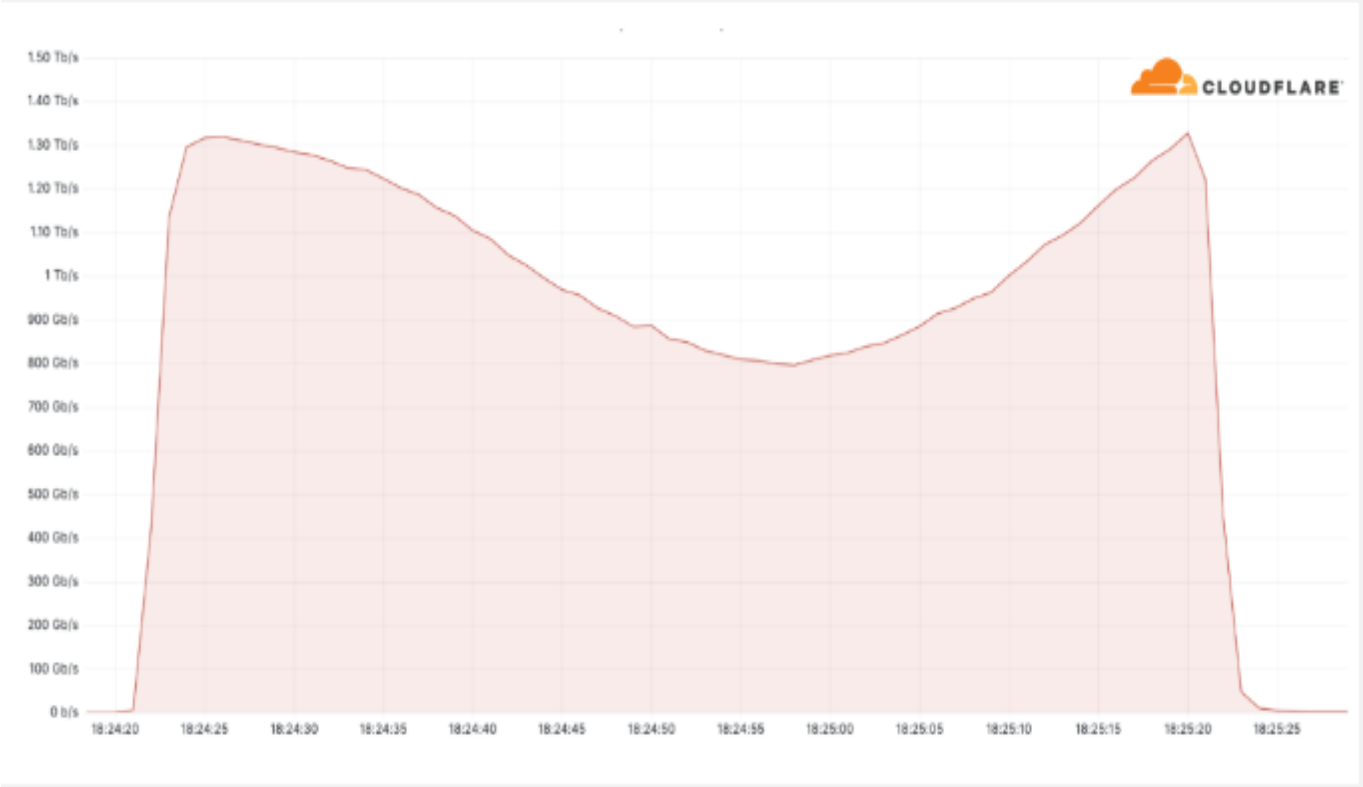



Рисунок 1.9 – 1,3 Тб/с DDoS-атака Mirai

Ключовими моментами цього кварталу стали [10]:

1. У першому кварталі 16% опитаних клієнтів повідомили про DDoS-атаку Ransom — цей показник залишається стабільним порівняно з попереднім кварталом, але на 60% більше порівняно з минулим роком.

2. Некомерційні організації та телерадіомовлення були двома галузями, які найбільше націлені. Фінляндія була найбільшим джерелом HTTP DDoS-атак з точки зору відсотка трафіку атак і основною метою DDoS-атак на мережевому рівні. Ізраїль був найбільш атакованою країною у світі за допомогою HTTP DDoS-атак.

3. Масштабні об’ємні DDoS-атаки — атаки понад 100 Гбіт/с — зросли на 6% порівняно з кварталом. Атаки на основі DNS стали найпопулярнішим вектором. Подібним чином спостерігались сплески в SPSS-bas під час DDoS-атаки ed, ампліфікації DNS і DDoS-атаки на основі GRE.

### 1.5.2 DDoS-атаки в рамках війни в Україні

Як аналізувалися статистичні дані про DDoS-атаки на веб-сайти в рамках повномасштабної війни, яка почалася в Україні в лютому 2022 року, важко сказати, оскільки немає офіційних даних про кількість інцидентів та їхню динаміку. Проте, відомо, що війна між Україною та росією стала причиною багатьох кібератак, включаючи DDoS-атаки, на веб-сайти українських урядових і недержавних організацій.

За даними деяких вітчизняних IT-експертів, в кінці лютого 2022 року було зафіксовано DDoS-атаку на сайт Міністерства внутрішніх справ України [11]. Також повідомляється про подібні атаки на сайти державних установ, таких як Державна фіскальна служба, а також на сайти видань та ЗМІ.

На жаль, точних даних про кількість інцидентів та їхню динаміку немає, оскільки багато з цих атак не були офіційно зафіксовані або не набули розголосу у відкритих джерелах. Зокрема, за словами голови Державної служби спеціального зв’язку та захисту інформації України бригадного генерала Юрія Щиголя: “СЗДІ, функціонування якої забезпечують фахівці Держспецзв’язку, – один із наших надійних щитів, що забезпечує кіберстійкість держави, припиняє і блокує спроби втручання, DDoS, зараження та розповсюдження ШПЗ тощо. Йдеться про тисячі таких кібератак щодня. Щодоби ми відбиваємо від 5 до 40 потужних DDoS-атак високого рівня. За грудень нами припинено та заблоковано 395 таких атак. Також лише за грудень системою зафіксовано та поінформовано споживачів про 170 тисяч лише спроб експлуатації вразливостей на державних інформаційних ресурсах, які ми захищаємо. Кіберзахист – це наша щоденна робота” [11].

Країна-агресор також отримала чимало збитків, що завдані анти-російськими хактивістами [12]:

- Банк «Відкриття» повідомив про проблеми з інтернет-банкінгом і мобільним додатком.

- Впали веб-сайти ФСБ, роскомнадзору, президента рф, уряду рф, держдуми, ради федерації та ще низка інших.

- Зламані сайти найбільших російських ЗМІ: ТАСС, “Комерсант” та “Фонтанка”.

- У перші два місяці третього кварталу 2022 року Сбербанк захистив себе від 450 розповсюджених атак типу «відмова в обслуговуванні». Це число дорівнює кількості DDoS-атак, з якими вони зіткнулися за останні п'ять років [12].

### 1.5.3 Вартість DDoS-атак

Відома наступна інформація, щодо вартості DDoS- атак [12]:

1. Дослідження Ponemon Institute показало, що під час DDoS-атаки кожна хвилина простою коштує 22 000 доларів.

2. Відновлення послуг і операцій після атаки може коштувати малому або середньому бізнесу 120 000 доларів.

3. DDoS-атаки на прикладному рівні завдали онлайн-індустрії більше шкоди, ніж будь-який інший тип атак, збільшившись на 131% порівняно з попереднім кварталом (і на 300% за рік).

## 1.6 Проблема реагування на повільні й малопотужні DDoS-атаки

Низька та повільна атака – це тип атаки, що покладається на невеликий потік дуже повільного трафіку, націленого на ресурси програми або сервера [13]. На відміну від більш традиційних атак великих потужностей, низькі та повільні атаки вимагають значно менше пропускної здатності і їх важко подолати, оскільки вони створюють трафік, який важко відрізнити від звичайного трафіку. У той час як великомасштабні DDoS-атаки, швидше за все, будуть помічені швидко, низькі та повільні атаки можуть залишатися непоміченими протягом тривалого періоду часу, при цьому відмовляючи або сповільнюючи обслуговування реальних користувачів.

**Означення проблеми.** Повільні DDoS-атаки не викликають різке збільшення трафіку, яке приводить до миттєвої відмови в обслуговуванні. Тобто визначити момент початку атаки майже неможливо. Відповідно, значно ускладнюється

відокремлення шкідливого трафіку від нормального. Основна проблема в виявленні повільних DDoS-атак – це нездатність запобігти їм, оскільки процес визначення базується на вивченні існуючого трафіку без можливості його прогнозування в залежності від активності користувачів. Без сумніву, прогнозована поведінка користувачів дасть змогу виявити аномальну поведінку і запобігати появі повільних DDoS-атак.

Виходячи з вищезазначеного за мету своєї роботи автор ставить розв'язання питання досягнення підвищення ефективності захисту веб-сайтів від повільних та малопотужних DDoS-атак.

Для досягнення поставленої в роботі мети необхідне вирішення наступних задач:

1. Розглянути та проаналізувати основні існуючі методи захисту веб-сайтів від DDoS-атак.

2. Дати оцінку їх ефективності для захисту веб-сайтів від повільних та малопотужних DDoS-атак.

3. Розглянути та проаналізувати модель виявлення та блокування повільних та малопотужних DDoS-атак.

4. Розробити пропозиції для удосконалення даної моделі.

### 1.7 Аналіз останніх досліджень і публікацій

Питанням виявлення розподілених атак типу «відмова в обслуговуванні» або DDoS присвячено значну кількість публікацій. Якщо зловмисник бажає паралізувати роботу програми, найлегший спосіб – передача надлишкового обсягу трафіку з метою відключення сервера програми. Однак сьогодні існує величезна кількість технологій, здатних виявляти та блокувати такі атаки на основі IP-адрес або сигнатур, управління квотами, а також за допомогою спеціалізованих рішень для запобігання DDoS-атакам. Існує величезна кількість публікацій, що досліджують способи виявлення DDoS-атак. Так у дослідженні [15] запропоновано новий метод виявлення повільних HTTP-атак у хмарі. Рішення дозволяє виявити атаки Slow HTTP Header (Slowloris), Slow HTTP

Body (RUDY) або Slow Read HTTP DDoS. Інша робота [16] пропонує нову модель класифікації атак, для пом’якшення впливу атак у хмарі. В той же час такі підходи не дають гарантію ефективного виявлення атак на ранніх стадіях їх розвитку. У роботі [17] запропоновано систему, яка має змогу виявити і пом’якшити атаки в межах мережевої інфраструктури. Аналіз продовжується роботою [18] у якій досліджено модель захисту бічного каналу. Головними ідентифікаційними параметрами в обох моделях є швидкість передачі пакету та рівномірна відстань між пакетами, що дозволяє передбачити дії зловмисників. Тому у роботі [19] розглядається вибірка для створення різних розподілів класів для протидії впливу незбалансованих повільних наборів даних HTTP DoS.

У роботах [20, 21] приводяться дослідження, які розвивають систему захисту основою якої є метрики для виявлення типових повільних атак, що можуть бути ефективними маючи обмежені ресурси на основі подібності дослідження та впровадження евклідової метрики. Цей підхід може бути ефективним лише в тому випадку, якщо в наявності є зразки великої кількості повільних атак, і ймовірніше такий підхід навряд чи буде ефективним.

У роботі [22] уточняється якість параметрів TCP-з’єднань, які є характерними для повільного HTTP нападу. Отримані формули дають оцінку імовірності та часу переходу веб-сервера в режим перевантаження. Незважаючи на детальне вивчення, таке виявлення атак базується на спостереженні статистики та не стосується прогнозування. У роботах [23, 24] запропоновано алгоритм виявлення повільних DDoS-атак на основі моделей трафіку залежно від стану завантаження сервера. Водночас процес пошуку рішення для запобігання не розглядаються. У роботі [25] розглянуто різні сценарії та запропоновано гібридні нейронні мережі для виявлення DDoS-атак, але метод і методика виявлення DDoS-атак низької інтенсивності не розглядається. У роботі [26] розглянуто інтервал прогнозу на основі імовірнісної нейронної мережі з динамічним оновленням параметра згладжування. Але проблема динаміки такої моделі залишається невирішеною. Робота [27] представляє новий метод для виявлення DDoS-атаки RUDY на основі самоподібності мережевого трафіку. Проте в роботі не враховано різноманітність навчальних зразків і процес

отримання навчальної множини для навчання. У роботі [28] представлена система для виявлення атак HTP DTP у хмарі на основі інформації індикатори ентропії та випадкові дерева. Такий підхід цілком ефективний, хоча він не вирішує питань прогнозування розвитотку нападу. Таким чином, більшість робіт, які присвячено протидії повільним DDoS-атаки не вирішують проблеми прогнозування поведінки користувача і тому є недостатньо ефективними для виявлення нападів на ранніх стадіях атак. Метою запропонованого рішення є формування системи виявлення повільних DDoS-атак на основі прогнозування поведінки користувачів в мережі. Для успішного вирішення існуючої проблеми, необхідно побудувати модель і розробити технологію прогнозування поведінки користувачів з урахуванням історії їх взаємодії з сервером, а також висунути пропозицію топології для розпізнавання повільних DDoS-атак.

**Висновок до розділу 1**

В першому розділі дипломної роботи розглянуто поняття кібератаки. Наведено умовну класифікацію актуальних видів атак і їх короткий опис. Описані можливі наслідки кібератак, які можуть завдати величезної шкоди як і підприємствам так і звичайним інтернет-користувачам.

Більш детально охарактеризовано поняття DDoS-атаки. Наведено класифікацію DDoS-атак з прикладами, а також представлено деякі статистичні дані по DDoS-атакам за останні роки.

Наведено короткий опис проблеми, що пов’язана зі складністю виявлення повільних та малопотужних DDoS-атак на веб-сайти.

Сформульовано мету роботи, яка полягає в підвищенні ефективності захисту веб-сайтів від повільних та малопотужних DDoS-атак.

Для досягнення сформованої мети роботи були поставлені наступні задачі, які потрібно вирішити:

1. Розглянути та проаналізувати основні існуючі методи захисту веб-сайтів від DDoS-атак.

2. Дати оцінку їх ефективності для захисту веб-сайтів від повільних та малопотужних DDoS-атак.

3. Розглянути та проаналізувати модель виявлення та блокування повільних та малопотужних DDoS-атак.

4. Розробити пропозиції для удосконалення даної моделі.

# РОЗДІЛ 2
# АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗАХИСТУ ВЕБ-САЙТІВ ВІД DDOS-АТАК

## 2.1 Огляд сучасних підходів до захисту веб-сайтів від DDoS-атак

До основних підходів захисту веб-сайтів від DDoS-атак відносяться [29, 30]:

1. Фільтрація трафіку.
2. Кешування контенту.
3. Розподілення DNS.
4. Використання CDN.
5. Використання WAF.

**Фільтрація трафіку**

Фільтрація трафіку – це метод, який полягає у відсіюванні трафіку, що надходить на сервери веб-сайту, із заборонених IP-адрес або протоколів (рис. 2.1). Цей метод використовується для зменшення навантаження на сервери, що дозволяє зберігати доступність веб-сайту. Фільтрація трафіку може бути реалізована на різних рівнях, від фільтрації IP-адрес і до аналізу вмісту запитів. Метод фільтрації трафіку є одним з ефективних підходів до захисту веб-сайтів від DDoS-атак. Основна ідея полягає в тому, щоб виділити нормальний трафік і блокувати шкідливий трафік, який спричиняє атаку.

Процес фільтрації трафіку складається з кількох етапів. На першому етапі встановлюється моніторинг трафіку. Для цього можуть використовуватися різні інструменти, такі як спеціалізовані програми або апаратне забезпечення, яке забезпечує моніторинг трафіку в реальному часі.

Після того, як моніторинг трафіку встановлено, наступний крок полягає в аналізі трафіку. Цей етап включає в себе аналіз заголовків трафіку та даних, які містяться в пакетах. За допомогою алгоритмів аналізу трафіку можна визначити, який трафік є нормальним, а який є шкідливим.

Далі використовується система правил, яка визначає, який трафік слід блокувати, а який можна пропустити. Ці правила можуть бути налаштовані вручну адміністратором, або вони можуть бути автоматично вивчені системою з використанням машинного навчання.

Після того, як система правил встановлена, система фільтрації трафіку перевіряє кожен пакет, який надходить на сервер. Якщо пакет відповідає правилам, то він пропускається, якщо ж пакет визнано шкідливим, то він блокується.

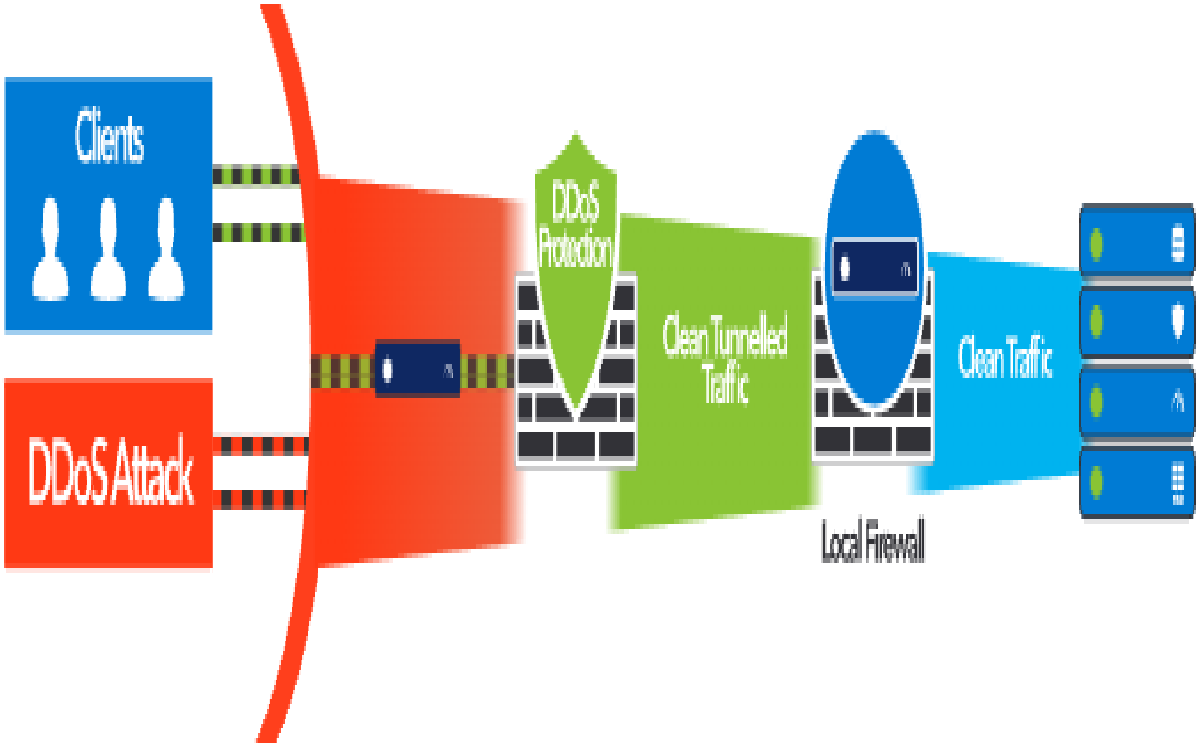



Рисунок 2.1 – Метод фільтрації трафіку

Метод фільтрації трафіку є ефективним і надійним підходом до захисту веб-сайтів від DDoS-атак

**Кешування контенту**

Метод кешування контенту є одним із методів захисту веб-сайту від DDoS-атак, який полягає в тому, щоб зберігати статичний контент в кеші (тимчасовому сховищі) на проміжному сервері (cache server) з метою зменшення навантаження на основний сервер, який обслуговує запити користувачів (рис. 2.2).

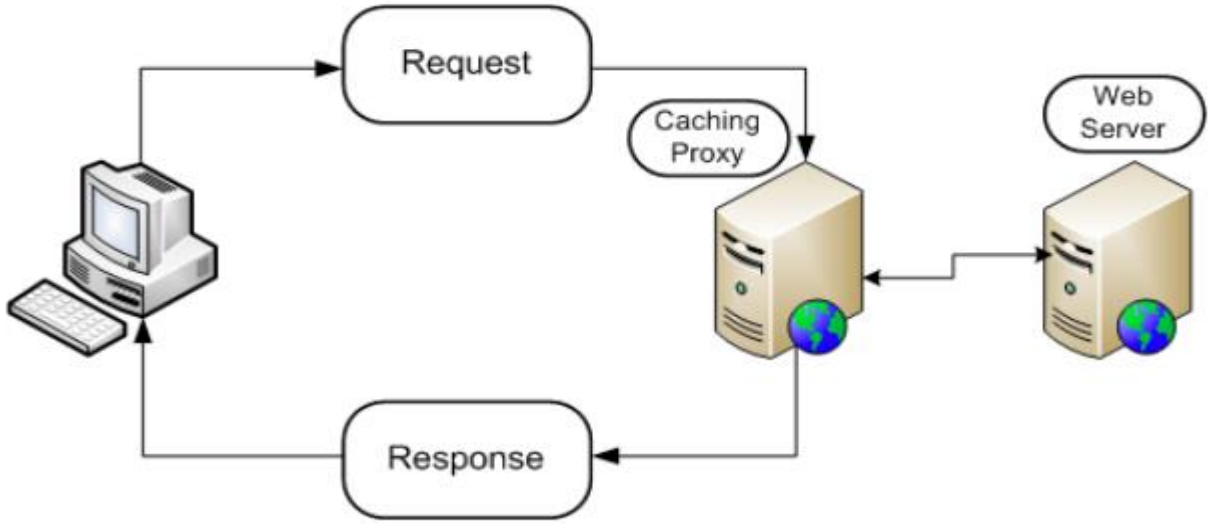



Рисунок 2.2 – Кешування контенту

Коли користувач робить запити, щоб отримати вміст веб-сайту, проміжний сервер спочатку перевіряє, чи міститься ця інформація в його кеші. Якщо вміст знаходиться в кеші, сервер може відправити його користувачеві без необхідності звертатися до основного сервера. Це зменшує кількість запитів до основного сервера та скорочує час відповіді на запити, що робить веб-сайт доступним для користувачів, навіть якщо основний сервер перебуває під атакою.

При кешуванні контенту важливо враховувати те, що статичний контент, який рідко змінюється, підходить для кешування, а вміст, що містить динамічний контент, наприклад, персоналізований вміст, не підходить для кешування, оскільки він змінюється від користувача до користувача. Також, при неправильному налаштуванні кешування може виникнути проблема синхронізації контенту між кеш-сервером та основним сервером.

**Розподілення DNS**

Метод розподілення DNS (Domain Name System) використовується для розподілу трафіку між кількома серверами, що мають одне і те ж доменне ім'я, з метою забезпечення балансу навантаження та підвищення доступності веб-сайту .

Концепція методу розподілення DNS базується на використанні DNS-серверів, які відповідають за перетворення доменних імен в IP-адреси. Зазвичай, коли користувач вводить URL веб-сайту у веб-браузері, DNS-сервер перетворює це доменне ім'я в IP-адресу сервера, де знаходиться веб-сайт. Однак, у методі розподілення DNS використовується додатковий рівень DNS-серверів, який дозволяє розподіляти трафік між кількома серверами.

Основними елементами методу розподілення DNS є [31]:

- DNS-сервери: Використовуються спеціальні DNS-сервери, які налаштовані для розподілення трафіку (рис. 2.3)

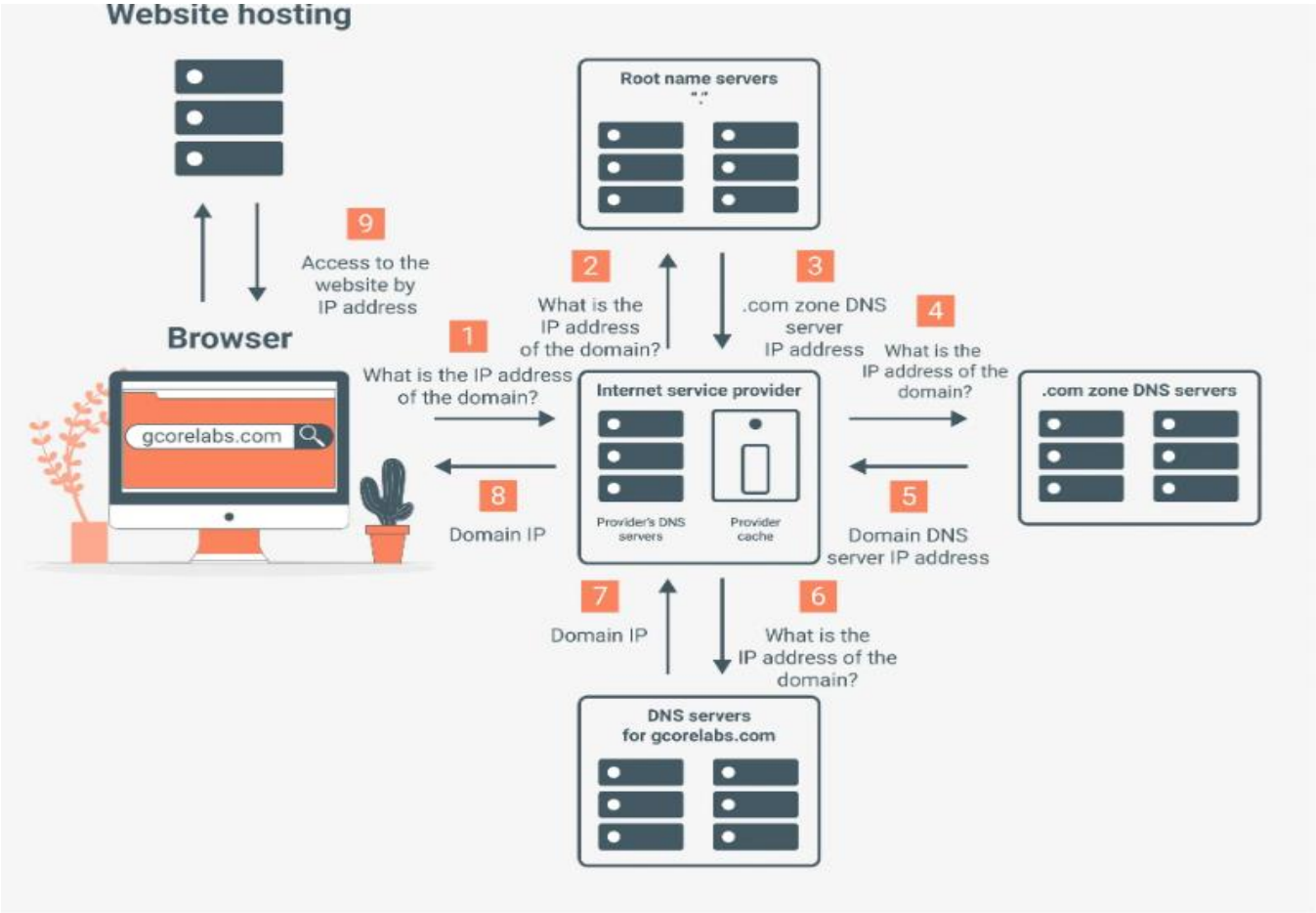



Рис. 2.3 – DNS-сервер

Існують 2 основні види DNS-серверів. Кешований (локальний) та авторитетний. Кешовані DNS-сервери, як правило, належать інтернет провайдерам і обробляють

клієнтські запити. Зазвичай вони містять доменні імена та IP-адреси, які найчастіше запитують найближчі клієнти. Кешування є основною функцією цих серверів. Вони отримують запити від користувачів і або надають інформацію з кешу, або запитують IP-адреси від авторитетних серверів DNS. Авторитетні – сервери, які фактично зберігають вихідну інформацію. Вони можуть відповідати за всю доменну зону, наприклад, .ua або .com, зберігаючи адреси DNS-серверів кожного домену в зоні. Одним із авторитетних типів серверів є кореневі сервери – вершина ієрархії, точка входу в простір інтернет-імен, до якого ми всі звикли.

Ці сервери містять записи DNS, які вказують на різні IP-адреси серверів, що мають одне і те ж доменне ім'я.

- Записи DNS: На DNS-серверах створюються записи DNS, які вказують на різні IP-адреси серверів. Ці записи бувають 8 типів (рис. 2.4):

DNS Activity | Threat Activity

| DATE & TIME | SOURCE IP | QUERY NAME | SITE |
|---|---|---|---|
| 01-03-2020 15:50:34 | 172.16.22.56 | data.cnn.com. | BlueCat BPC |
| 01-03-2020 15:50:34 | 172.16.22.56 | data.cnn.com. | BlueCat BPC |
| 01-03-2020 15:50:08 | 172.16.22.56 | scout.us1.salesloft.com. | BlueCat BPC |
| 01-03-2020 15:50:06 | 172.16.22.56 | edgeapi.slack.com. | BlueCat BPC |
| 01-03-2020 15:49:52 | 172.16.22.56 | amazon.com. | BlueCat BPC |
| 01-03-2020 15:49:50 | 172.16.22.56 | amazon.com. | BlueCat BPC |
| 01-03-2020 15:49:46 | 172.16.22.56 | amazon.com. | BlueCat BPC |
| 01-03-2020 15:49:44 | 172.16.22.56 | wpad.bluecatnetworks.corp. | BlueCat BPC |
| 01-03-2020 15:49:14 | 172.16.22.56 | cnn.com. | BlueCat BPC |
| 01-03-2020 15:49:12 | 172.16.22.56 | cnn.com. | BlueCat BPC |
| 01-03-2020 15:48:59 | 172.16.22.56 | gmail.com. | BlueCat BPC |
| 01-03-2020 15:48:53 | 172.16.22.56 | gmail.com. | BlueCat BPC |
| 01-03-2020 15:48:50 | 172.16.22.56 | gmail.com. | BlueCat BPC |
| 01-03-2020 15:48:48 | 172.16.22.56 | upload.fp.measure.office.com. | BlueCat BPC |
| 01-03-2020 15:48:48 | 172.16.22.56 | upload.fp.measure.office.com. | BlueCat BPC |
| 01-03-2020 15:48:47 | 172.16.22.56 | k-ring.msedge.net. | BlueCat BPC |
| 01-03-2020 15:48:47 | 172.16.22.56 | k-ring.msedge.net. | BlueCat BPC |
| 01-03-2020 15:48:46 | 172.16.22.56 | b-ring.msedge.net. | BlueCat BPC |
| 01-03-2020 15:48:46 | 172.16.22.56 | b-ring.msedge.net. | BlueCat BPC |
| 01-03-2020 15:48:45 | 172.16.22.56 | b74311977aee419ea658ef8a9c33562f.fp.measure.office.com. | BlueCat BPC |

Рисунок 2.4 - DNS-записи

1. A-записи. Ці записи зіставляють доменні імена на адреси типу IPv4.
2. AAAA-записи. Аналогічно, але для адрес типу IPv6.

3. CNAME-записи. Переспрямовують домен на інший домен.

4. PTR. Перетворюють адреси IPv4 або IPv6 в доменні імена.

5. NS. Надають списки авторитетних серверів імен, відповідальних за домен.

6. MX. Надають доменні імена поштових серверів, які отримують електронні листи від імені домену.

7. SOA. Надають важливі відомості про зону DNS; необхідні для кожної зони DNS.

8. TXT. Надають будь-який тип основної описової інформації в текстовому форматі.

- Алгоритми розподілення: При запиті DNS-сервер використовує алгоритм розподілення для вибору IP-адреси сервера, яку поверне користувачеві. Існує кілька алгоритмів розподілення DNS, які використовуються для визначення того, який сервер DNS буде відповідати на запити користувачів.

Деякі з найпоширеніших алгоритмів роздподілення DNS включають [31]:

- Round Robin (RR): Цей алгоритм використовується для розподілу навантаження між серверами DNS в рівномірний спосіб. Кожен запит обслуговується сервером в послідовному порядку, поки не буде досягнуто кінця списку серверів. Потім процес повторюється з початку.
- Least Connections: Цей алгоритм призначає запити користувачів серверу DNS з найменшою кількістю активних з’єднань. Він спрямовує трафік до сервера, який має найменшу відсоткову завантаженість, що дозволяє рівномірно розподілити навантаження між серверами.
- IP Hash: Цей алгоритм використовується для розподілу запитів на основі IP-адреси користувача. Хеш-функція застосовується до IP-адреси, і результат використовується для визначення сервера DNS, який буде обслуговувати запит.
- Weighted Round Robin: Цей алгоритм надає різну вагу (пріоритет) кожному серверу DNS в залежності від його потужності або ресурсів. Запити розподіляються між серверами згідно з їх пріоритетом. Сервери з

більшою перевагою отримують більше запитів, що дозволяє ефективніше використовувати ресурси мережі.

- Ці алгоритми роздподілення DNS можуть бути використані окремо або в комбінації [31].

Чудовим прикладом  реалізації методу розподілення DNS є технологія DNS Anycast. Вона використовується для надання одного IP-адресу для декількох серверів DNS, розташованих у різних географічних регіонах. Коли клієнт робить запит до відповідної IP-адреси, мережевий шлях автоматично обирає найближчий сервер DNS з використанням протоколу маршрутизації.

Мережевим шляхом є послідовність мережевих вузлів (роутерів або комутаторів) та зв'язків, які дозволяють передавати пакети даних від джерела до призначення в комп'ютерних мережах. Він визначає шлях, по якому будуть направлятися пакети даних, щоб доставити їх від одного вузла мережі до іншого.

**Використання CDN**

*CDN (Content Delivery Network)* - це мережа з серверів, які розташовані в різних точках світу, яка співпрацює з оригінальним веб-сервером для ефективної доставки контенту до кінцевих користувачів (рис.2.5).

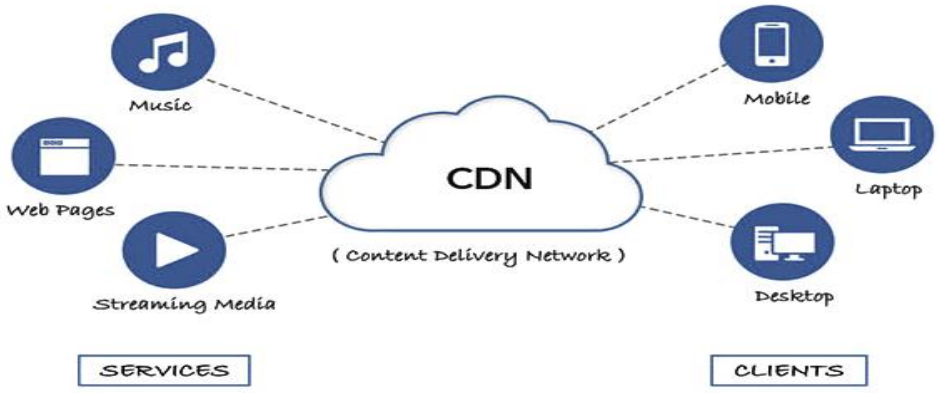



Рисунок 2.5 – Content Delivery Network

Принцип роботи CDN полягає в тому, що веб-сайт розподіляє свій контент на сервери CDN. Коли користувач робить запит до веб-серверу, мережа визначає його

місцезнаходження та направляє його до найближчого сервера CDN. Цей сервер містить кешовану копію контенту, що дозволяє швидко його доставити користувачеві. Якщо контент не знаходиться в кеші серверу, CDN запитує оригінальний сервер веб-сайту, отримує контент і кешує його на сервері для майбутнього використання [27].

**Використання WAF**

WAF – це програмне забезпечення, що використовується, як міжмережевий екран для веб-додатків (рис. 2.6).

Це інструмент для фільтрації трафіку, що працює на прикладному рівні та захищає веб-додатки методом аналізу трафіку http/https і семантики xml/soap. WAF може встановлюватися на фізичний або віртуальний сервер і виявляти найрізноманітніші види атак. Серед яких можуть бути:

- SQL-ін’єкції
- OSCI (впровадження команд операційної системи)
- RFI
- LFI
- XSS

Цей список не є вичерпним окрім цього даних інструмент може забезпечити симетричну фільтрацію шляхом очищення не лише вхідних запитів, але й вихідного трафіку. Зловмисний вихідний трафік може генеруватися, якщо в мережі є інфіковані комп’ютери. У цьому разі WAF здатний блокувати потенційно небезпечний трафік інфікованих комп’ютерів і забезпечити захист також і від (D)DoS-атак.

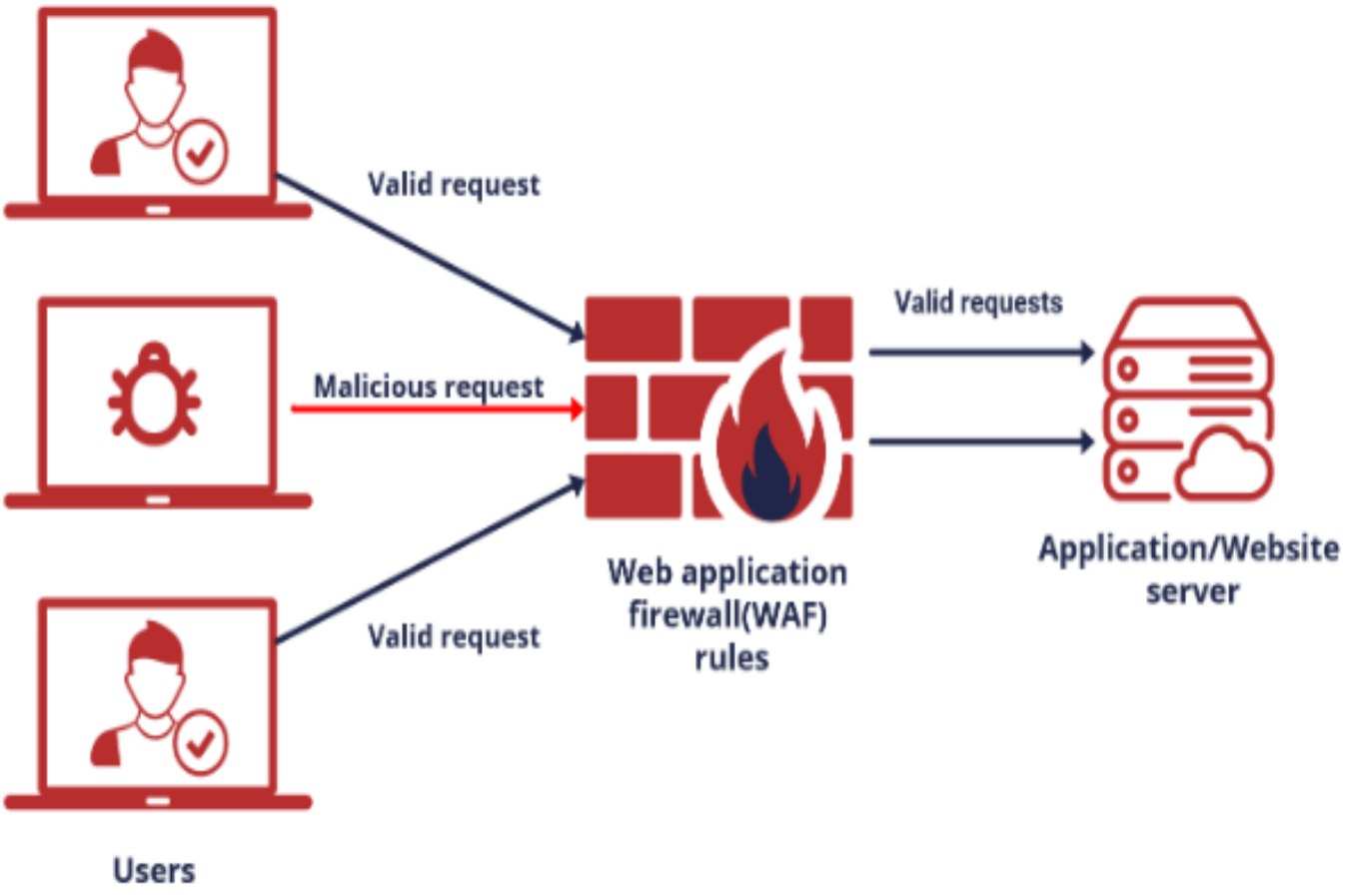



Рисунок 2.6 – Принцип роботи WAF

Діє міжмережевий екран як проксі-сервер, але маючи можливість видавати https-трафік методом перевірки сертифіката конкретного серверу, WAF також розрахований на виконання додаткових операцій: балансування навантаження на сервер, термінацію трафіку SSL і т.д.

WAF може вбудовуватися в мережу як [33]:

- Монітор. Для моніторингу мережі в режимі реального часу за допомогою порту SPAN.
- Мережевий шлюз з 3 режимами проксі: transparent, bridge та reverse.

Працює WAF за двома моделями безпеки [33]:

- Negative. «Чорний список», що забороняє прийом тієї інформації, що записана в налаштуваннях. Захищає веб-застосунки на прикладному рівні, але вміє оцінювати

потенційні загрози детальніше і частіше застосовується для забезпечення захисту від специфічних типів атак. Аналізує вразливість конкретних веб-застосунків.

- Positive. «Білий список», який дозволяє приймати інформацію, яка була заздалегідь вказана в налаштуваннях. Дозволяє отримати максимальний захист, оскільки застосовується як доповнення до моделей. Залучає правила, які визначають, що конкретно має бути дозволено [33].

### 2.1.1 Оцінка ефективності методів захисту веб-сайтів від повільних та малопотужних DDoS-атак

Ефективність наведених методів захисту буде залежати від багатьох факторів серед яких специфіка кожної атаки, конфігурація системи захисту, досвід нападників тощо. Наявність багатьох інструментів захисту і використання навіть всіх названих методів захисту проти DDoS-атак не є гарантією 100% успіху у відбитті всіх DDos-атак, особливо повільних та малопотужних, які складно виявити на початку. Зокрема кожен із методів може бути корисним, маючи свої переваги та недоліки. Нижче представлено короткий аналіз ефективності кожного з методів захисту веб-сайтів від повільних та малопотужних DDoS-атак:

1. Фільтрація трафіку.

Метод фільтрації трафіку може бути ефективним інструментом для захисту від повільних та малопотужних DDoS-атак, якщо він вчасно ідентифікує та блокує підозрілий трафік перед тим, як він досягне сервера. Основна мета фільтрації трафіку - забезпечити, що на сервер надходять запити від реальних користувачів, а не від шкідливих ботів.

Головними перевагами даного методу є [37]:

1) Можливість виявлення неправильних або неповних запитів: Фільтри трафіку можуть аналізувати вхідний трафік та виявляти шкідливі запити, які є характерними ознаками повільних та малопотужних атак типу slowloris, R.U.D.Y і т.п. Це дозволяє відокремити шкідливий трафік від легітимного та вжити відповідних заходів для блокування атакуючих ботів.

2) Обмеження кількості одночасних з'єднань: Фільтри трафіку можуть встановлювати обмеження на кількість одночасних з'єднань, що дозволяє відмовляти запити утримуючим з'єднання ботам. Slowloris атаки зазвичай спрямовані на затримку доступу для легітимних користувачів, використовуючи всі доступні з'єднання. В деяких випадках фільтри трафіку можуть розпізнавати цей шаблон і блокувати ботів, що спробують встановити надмірну кількість з'єднань.

3) Аналіз поведінки трафіку: Деякі фільтри трафіку використовують методи аналізу поведінки трафіку для виявлення slowloris атак. Вони можуть аналізувати шаблони вхідного трафіку і виявляти відмінності у поведінці запитів від звичайного руху. Slowloris атаки характеризуються тривалим затриманням або повільною передачею даних. Фільтри трафіку можуть виявити ці аномальні шаблони та автоматично блокувати атакуючий трафік.

Однак, попри вищезгадані переваги, використаний метод має і свої недоліки [33]:

- Обмеження можливості легітимних користувачів доступу до веб-сайту, якщо фільтри некоректно налаштовані.
- Нездатність ефективно захистити від розподілених DDoS-атак, де атаки здійснюються з великої кількості джерел.
- Вимагання постійного моніторингу та налаштування фільтрів для виявлення та блокування нових варіацій атак.

2. Кешування контенту.

Метод кешування контенту також може бути корисним при захисті веб-сайтів від повільних та малопотужних DDoS-атак. Однак корисність цього методу залежить від конкретних випадків та налаштувань. Наприклад, якщо веб-сайт має багато динамічного або персоналізованого контенту, кешування може бути менш ефективним, оскільки кожний запит спочатку вимагатиме перевірку на основному сервері, щоб забезпечити актуальну версію контенту.

Для веб-сайтів, що містять статичний контент даний метод буде працювати ефективніше оскільки він призведе до зменшення навантажень на основний сервер, а кешований зміст буде відправлятись з проміжного, тобто кеш-серверу. Таким чином

сервер веб-сайту буде швидше відповідати на запити, оскільки він просто повертає кешовану версію контенту.

Також слід враховувати, що кешування контенту може мати обмеження щодо доступної пам’яті на кеш-сервері. Якщо вміст сайту має великий обсяг контенту, це може призвести до обмеження кількості кешованого контенту і, відповідно, до меншої ефективності DDoS-атак.

3. Розподілення DNS.

Метод розподілення DNS може бути також ефективним інструментом для захисту веб-сайтів від повільних та малопотужних DDoS-атак. Він дозволяє розподілити трафік між кількома серверами, що зменшує навантаження на кожен окремий сервер і розподіляє ризик атаки.

Однією з основних переваг методу полягає в тому, що він розділяє запити від користувачів між декількома серверами, використовуючи розподілені DNS-сервери. При отриманні запиту від клієнта, DNS-сервер вибирає оптимальний сервер для обробки запиту на основі різних факторів, таких як місцезнаходження сервера, його навантаження та доступність. Це дозволяє забезпечити балансування навантаження між серверами, що дозволяє сайту витримувати більше запитів і забезпечувати стабільну доступність навіть під час DDoS-атаки. Коли один сервер перевантажений або стає недоступний, інші сервери можуть приймати запити та обслуговувати їх, що забезпечує неперервну роботу веб-сайту.

Варто зазначити, що даний метод не є універсальним рішенням для всіх видів DDoS-атак. Він є більш ефективним для повільних та малопотужних атак, які не здатні перевантажити мережеві ресурси. Також варто враховувати, що ефективність методу також сильно залежить від багатьох факторів ключовим з яких є конфігурація конкретної DNS-системи та особливість DDoS-атаки.

4. Використання CDN.

Метод використання CDN (Content Delivery Network) є ефективним інструментом для захисту веб-сайтів від повільних та малопотужних DDoS-атак. Він спрямований на забезпечення швидкої та надійної доставки контенту до користувачів, а також розподіл навантаження між різними серверами.

Однією з основних переваг CDN є розташування серверів в різних географічних областях, ближче до користувачів. Це дозволяє знизити затримку відповіді і покращити швидкість завантаження контенту. При DDoS-атаках, що характеризуються малою потужністю або повільними запитами, CDN може бути ефективним, оскільки він розподіляє трафік між різними серверами, розташованими у різних локаціях.

Крім того, CDN має вбудовані механізми кешування, які дозволяють зберігати копії статичного контенту на різних серверах. Це означає, що при отриманні запиту на контент, CDN може надати його безпосередньо з кешу, що зменшує навантаження на оригінальний сервер. Під час повільних та малопотужних атаках, CDN може продовжувати обслуговувати запити з кешу, забезпечуючи доступність контенту навіть під час атаки.

Однак, варто враховувати, що CDN може мати свої обмеження. Він ефективний лише для статичного або кешованого контенту, тоді як динамічний вимагає безпосереднього доступу до оригінального серверу.

5. Використання WAF.

Метод використання WAF (Web Application Firewall) для захисту веб-сайтів від повільних та малопотужних DDoS-атак може також бути ефективним для захисту від такого роду атак, але його ефективність також залежить від обставин його використання.

Основна перевага методу використання WAF полягає в його здатності виявляти та блокувати шкідливий http-трафік. WAF може встановлювати правила фільтрації, які аналізують http-запити і відповіді на предмет аномалій або відхилень від допустимих правил. В результаті, він може блокувати зловмисний трафік, включаючи запити, що спрямовані на вразливості, та запобігти їх впливу на роботу веб-сайтів.

Проте, варто враховувати, що WAF може бути менш ефективним проти повільних та малопотужних DDoS-атак. Це пов’язано з тим, що ці атаки характеризуються низьким обсягом трафіку або низькою швидкістю, що не завдає значної шкоди самому мережевому ресурсу, але може перевантажити рівень додатків.

WAF може мати лімітовану пропускну здатність або обробку запитів, тому його ефективність у розпізнаванні та блокуванні таких атак має свої обмеження.

**Висновок до розділу 2**

Отже, до основних актуальних методів захисту веб-сайтів від DDoS-атак належать:

- фільтрація трафіку;
- кешування контенту;
- розподілення DNS;
- використання CDN;
- метод використання WAF.

Наведені методи захисту мають свої переваги та недоліки, однак все ще не є достатньо ефективними проти боротьби із повільними та малопотужними DDoS-атаками.

В залежності від обставин їх використання дані методи можуть бути корисними при використанні в ролі інструментів захисту веб-сайтів від повільних та малопотужних DDoS-атак. Але, використання будь-яких з них, включаючи їх комбінування, не є гарантією 100% захисту від повільних та малопотужних DDoS-атак.

Логічним кроком для підняття ефективності захисту від повільних та малопотужних DDoS-атак будуть кроки у напрямках поліпшення виявлення та реагування на даний тип DDoS-атак.

# РОЗДІЛ 3
# ПРОПОЗИЦІЇ ЩОДО ПРАКТИЧНОЇ РЕАЛІЗАЦІЇ ШЛЯХІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ВЕБ-САЙТІВ ВІД ПОВІЛЬНИХ ТА МАЛОПОТУЖНИХ DDOS-АТАК

## 3.1 Аналіз методу виявлення та блокування повільних і малопотужних DDoS-атак за допомогою прогнозування поведінки користувача

Для ефективної протидії повільним та малопотужним DDoS-атакам необхідно відокремити і надати перевагу двом основним заходам, а саме [14]:

1) діагностувати атаку якомога раніше;

2) при цьому відокремити шкідливий трафік від легітимного.

Основною проблемою в виявленні повільних DDoS-атак є неспроможність запобігти їм, адже процес ідентифікації атаки базується на вивченні існуючого трафіку, не маючи можливості його прогнозування в залежності від активності користувачів.

Безсумнівно, прогнозовані дії користувачів зможуть допомогти виявити аномальну поведінку і уникати повільні DDoS-атаки.

### 3.1.1 Розрахунок параметрів трафіку для виявлення повільної DDoS-атаки

Основними компонентами у виявленні повільної DDoS-атаки системи були запропоновані в [15]. Структура такої системи містила 4 ключових модулі:

1) збір трафіку;

2) розрахунок параметрів руху;

3) розрахунок мережевої статистики;

4) класифікатор атак.

Робочий процес системи повинен будуватися на основі наступних кроків [16]:

1. Модуль збору трафіку за певний проміжок часу реєструє дані про рух, що є необхідними для подальшого здійснення обчислення:

- IP-адреси відправника та одержувача;

- TCP розмір вікна;

- час прибуття посилки.

2. Для кожної IP адреси у модулі розрахунку параметрів трафіку розраховуються характеристики трафіку, наприклад, середня затримка між надісланими пакетами (3.1).

$$T = \frac{\sum_{i=1}^{k}(t_{i+1} - t_i)}{k - 1}, \tag{3.1}$$

де: $t_i$ – час прибуття $i$-го пакету;

$t_{i+1}$ – час надходження $i$+1-го пакету;

$k$ – кількість пакетів, отриманих під час аналізу.

Вбудований таймер дає змогу записувати початок і кінець сесії, що дозволяє відстежувати тривалість відкритих з’єднань. Також й інші параметри можуть бути використані в залежності від налаштувань системи.

3. Після порівняння отриманих показників з пороговими значеннями у модулі класифікації атак можна зробити рішення про можливу наявність повільної HTTP-атаки. Користуючись цим підходом, рішення про наявність або відсутність повільної DDoS-атаки можливо прийняти лише після збору достатньої кількості статистичної інформації.

Також у такій ситуації адміністратори системи нерідко не мають часу для активних дій. Відповідно, рішення про наявність повільної DDoS-атаки, має базуватись за рахунок прогнозу поведінки користувача, яке можливо сформувати, вивчаючи статистику схожих дій інших користувачів.

### 3.1.2 Прогнозування поведінки користувача

Особистісну траєкторію зміни параметрів трафіку конкретного користувача формує його поведінка в мережі. Ці траєкторії є характерними як і для звичайного руху, так і для випадків при повільних DDoS-атаках.

Поведінка користувача в мережі створює особистісну траєкторію для зміни параметрів трафіку конкретного користувача. Дані траєкторії будуть характерні як для звичайного руху, так і у випадку повільної DDoS-атаки.

Для визначення відповідного часу для початку нейтралізації повільної DDoS-атаки, розроблено рішення задачі індивідуального передбачення. В [17] досліджено та продемонстровано прогнозування параметрів руху по індивідууму, де були показані параметри руху, що визначаються великими проміжками часу (тиждень, місяць). Частково цей підхід використовувався для захисту інформації в соціальних мережах [18] і для прогнозування в мультиагентному середовищі [19]. Однак, в той же час точність системи розпізнавання повільної DDoS-атаки мала бути значно вища і тому даному підходу необхідне вдосконалення.

Вхідні дані в цьому випадку використано в якості спостереження за рухом параметрів, наприклад, середнім інтервалом часу між відправленими пакетами, затримкою між пакетами в сеансі тощо, які утворюють вектор параметрів $X = (X_1, X_2, ..., X_H)$.

Виконання умови

$$X \in S_0,$$

де $S_0$ – область допуску вектора $X$.

Випадковий процес $X(t)$ формувався з часовими інтервалами між пакетами або затримками між ними у часі та описував еволюцію мережі параметрів у часі.

Припустивши також, що процес $X(t)$ статистично визначався при

$$t \geq t_1,$$

де $t_1$ – момент початку спостережень.

На рисунку 3.1 продемонстровано конкретні траєкторії контрольного моменту спостереження $t_k \geq t_1$ [15].

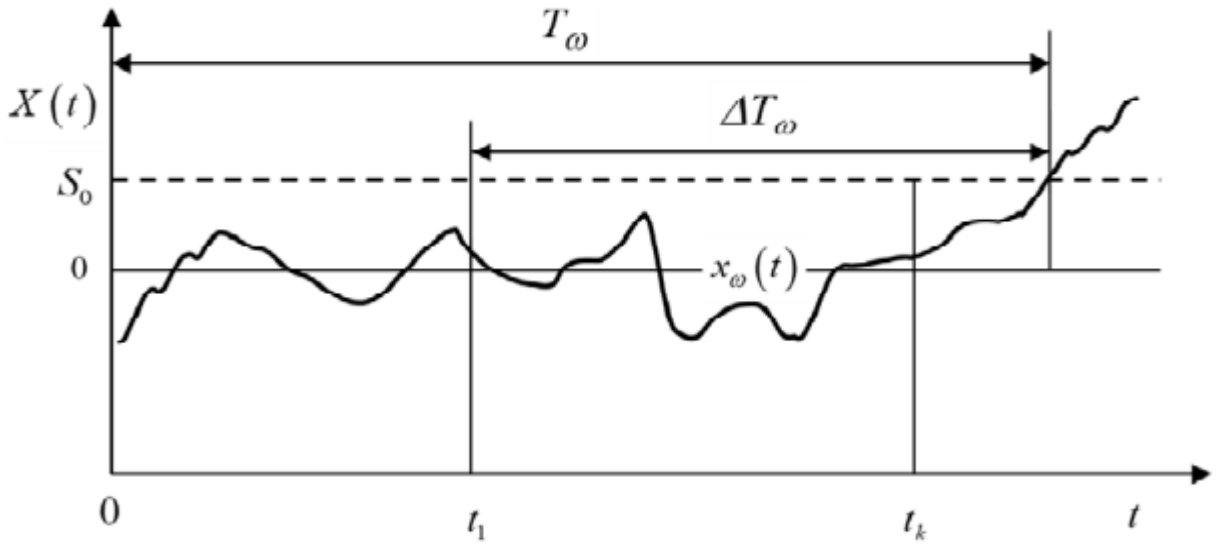



Рисунок 3.1 – Прогноз трафіку

Інформацію про початок траєкторії руху параметра ω позначено як $x_\omega\,(t) \in S_0$, $t_1 \leq t \leq t_k$ і отримано зі спостережень за параметром руху $X(t)$.

В даному випадку проблема індивідуального прогнозування трафіку, параметру поведінки сформульовано, як проблему визначення апостеріорного розподілу результату процесу часу $T_\omega\,(t)$.

*X(t)* поза зоною допуску $S_0$ відносно реалізації $x_\omega\,(t)$ представлено як задачу:

$$P^{ps}(s) = P\{X\,(s) \in S_0\, x_\omega\}, t_1 \leq t \leq t_k\,,\ s \geq t_k\,. \qquad (3.2)$$

За формулою (3.2) дано ймовірність того, що конкретна траєкторія, параметр ω гарантовано потрапляє в межі допустимого діапазону s > $t_k$, до моменту $t_k$ включно. При цьому умову описано як $x_\omega\,(t)$, $t_1 < t < t_k$. Тобто, проблему індивідуального прогнозування траєкторії мережевого трафіку вирішено.

Для вирішення задачі прогнозування, досліджуваний процес представлено формулою (3.3):

$$X(t) = m(t) + \sum_v V_v \cdot \varphi_v(t), \tag{3.3}$$

де *m(t)* – середня функція процесу;

$\varphi_v(t)$ – невипадкові (координатні) функції часу;

$V_v$ – випадкові, некорельовані коефіцієнти.

$$(M[V_v] = 0, M[V_v, V_\mu] = 0,\ v \neq \mu).$$

Це представлення, запропоноване в [30], давало змогу використати його для будь-якого параметра трафіку, який представлено як часовий ряд.

Процес X(t) записано у вигляді випадкової послідовності $X(t_i) = X(i), i = [1, i]$ у дискретній серії спостережень $t_i$:

$$\text{X(t)} = \text{m(t)} + \sum_{v=1}^{i} V_v \cdot \varphi_v(i), i \in [1, I], \tag{3.4}$$

де $V_v$ – випадковий коефіцієнт з параметрами;

$$M[V_v] = 0, M[V_v, V_\mu] = 0,\ v \neq \mu;\ [V_V^2] = D_V;$$

$\varphi_v(i)$ – невипадкова функція координат, $\varphi_v(t) = 1,\ \varphi_v(i) = 0$ тоді як $v > i$.

Формули для дисперсії та кореляційної функції мали наступний вигляд (3.5, 3.6):

$$D(i) = \sum_{v=1}^{inf(i,j)} D_v \cdot \varphi_v^2(i), i \in [1, I], \tag{3.5}$$

$$D(i, j) = \sum_{v=1}^{inf(i,j)} D_v \cdot \varphi_v(j),\ i, j \in [1, I], \tag{3.6}$$

Для представлення випадкових процесів руху параметрів (3.2) надано змогу виконати завдання виявлення повільної DDoS-атаки на основі прогнозування поведінки конкретного користувача.

Алгоритм виявлення повільної DDoS-атаки на основі прогнозування поведінки користувача.

Даний алгоритм складався з таких кроків [21]:

1. Визначення характеристик апріорного випадкового процесу *X(t)* за допомогою рівняння (3.4) на дискретний ряд точки $t_i$.

Для цього згенеровано результати контролю параметрів *x*(μ), у вигляді часового поясу, де розглядаються результати спостережень, які співвіднесені до моментів часу $t_\mu$, $\mu \in [1, k]$, $k < I$.

2. Встановлення значення процесу реалізації x(1), що отримувалися в результаті контролю, в момент часу μ=1, і представлені у вигляді:

$$\text{x}(1) = m(1) + \nu_1. \tag{3.7}$$

3. Конкретизація значення $\nu_1$ випадковго коефіцієнту $V_1$ за допомогою формули (3.7), що відповідало результатам першого спостереження. Уточнення значення $V_1$ призводило до зміни в щільності розподілу решти коефіцієнтів $V_i$. $i \in [2, I]$.

4. Визначення типу апостеріорного випадкового процесу, котрий в момент $i$ = 1 проходив через точку x(1) за допомогою підстановки значення $V_1$ з (3.7) у формулу (3.4):

$$X^1(i) = m(i) - (x(1) - m(1)) \cdot \varphi_1(i) + \sum_{\nu=1}^{i} V_\nu \cdot \varphi_\nu(i),\ i \in [1, I] \tag{3.8}$$

5. Визначення середнього значення для процесу (3.8), що знаходилось в моменті проходження $i$ = 1 через точку *x*(1):

$$m^1(i) = m(i) + (x(1) - m(1) \cdot \varphi_1(i),\ i \in [1, I]. \tag{3.9}$$

6. Встановлення загальної залежності для процесу, що проходив точку x(1):

$$X^1(i) = m^1(i) + \sum_{\nu=1}^{i} V_\nu \cdot \varphi_\nu(i), \in [1, I]. \quad (3.10)$$

7. При μ = k, здійснювався перехід до кроку 9; інакше – до наступного кроку.

8. Встановлення значення процесу реалізації x(2), відповіді отримані в результаті контролю в момент часу μ = 2, при врахуванні (3.10) представлялися у вигляді:

$$x(2) = m^2(2) + \upsilon_2. \quad (3.11)$$

Повернення до кроку 3 та повторення операції, як при випадку μ =1, давало результат:

$$m^2(i) = m^1(i) + (x(2) - m(2)) \cdot \varphi_2(i), \; i \in [1, I], \quad (3.12)$$

$$X^2(i) = m^2(i) + \sum_{\nu=1}^{i} V_\nu \cdot \varphi_\nu(i), i \in [1, I]. \quad (3.13)$$

9. Визначення оператору екстраполяції для функції середнього апостеріорного випадкового процесу та довільного числа $k < I$ в момент контролю $m^0(i) = m(i)$, $i \in [1, I]$:

$$m^k(i) = m^{k-1}(i) + (x(k) - m(k-1)) \cdot \varphi_k(i), i \in [1, I], \quad (3.14)$$

$$X^k(i) = m^k(i) + \sum_{\upsilon=k+1}^{i} V_\nu \cdot \varphi_\nu(i), \; i \in [1, I]. \quad (3.15)$$

Таким чином, формули (3.13)-(3.15) повністю описували процес, в якому вираз (3.14) є середньою функцією цього процесу для точки $t_i$.

10. Побудова прогнозу параметра трафіку та визначення моменту перевищення параметром критичного значення.

11. Класифікація трафіку як повільна DDoS-атака та запровадження заходів безпеки.

12. Кінець алгоритму.

Формула (3.14) надавала змогу оптимально виконати завдання екстраполяції процесу, а формула (3.15) – відтворити апостеріорний випадковий процес основою якого є моделювання.

Було задано лінійну аналітичну модель апостеріорного випадкового процесу на основі такого уявлення, що дозволяло вирішити проблеми прогнозування параметрів мережевого трафіку.

При таких обставинах рішення про повільну DDoS-атаку повинно прийнятись для кожної IP-адреси відправника на основі порівняння прогнозованих параметрів з критичними значеннями, щоб визначити час входження параметру в зону критичних значень. Даний підхід враховував статистку конкретної поведінки користувача, а також подібну поведінку інших користувачів у випадку повільної DDoS-атаки.

Моделювання алгоритму детектування повільної DDoS-атаки на основі прогнозування поведінки користувачів.

Симуляцією виявлення повільної DDoS-атаки на базі поведінки користувача було розроблено для атаки RUDY та спрогнозовано її поведінку. Для простоти, був розглянутий тільки один випадок нападу на фоні легітимного трафік (рис.3.2) [20].

Досліджуваний параметр розглядався як середня затримка між переданими пакетами.

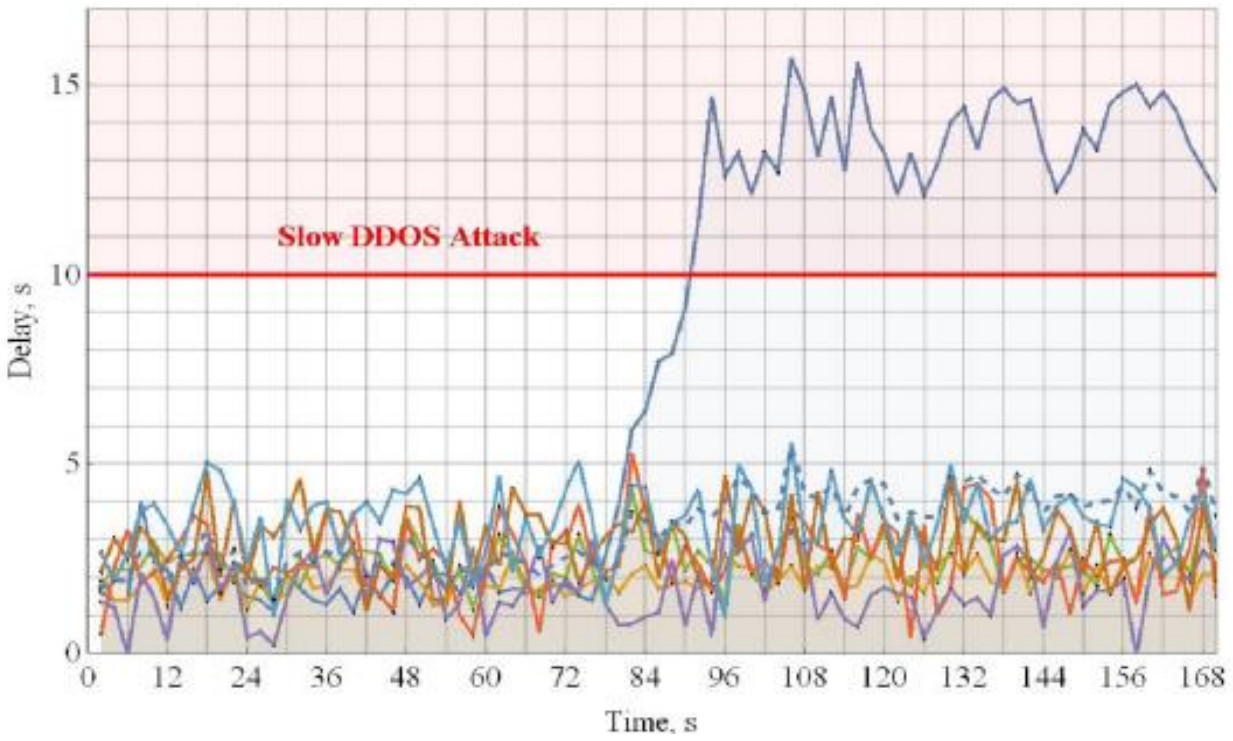



Рисунок 3.2 – Графік повільної DDoS-атаки

RUDY – це вид атаки на мережевий сервер, яка призначена для провокування збою веб-сервера. Причиною цього є надсилання довгих запитів. Атака виконується за допомогою інструмента, що сканує цільовий веб-сайт і помічає вбудовані веб-форми.

Після виявлення форм, атака надсилала легітимні HTTP POST-запити, які мають аномальну довжину полів заголовків content-length, після чого починається введення інформації, що має розмір одного байту на пакет. Описану атаку складно виявити через досить малі коливання вхідного трафіку.

Для процесу, що показаний на рис. 3.2, застосовувано вирази (3.14)-(3.15), беручи за вихідні значення спостережень окремі точки динамічного ряду, що відповідають частковій траєкторії №1 (рис. 3.2, темна крива).

Беручи дану криву в якості контрольної, за вихідні дані спостережень взято перші значення динамічного ряду, шо відповідають t = 1, 40, 90 секунд спостереження.

Беручи до уваги результати прогнозування при t = 1 с, зроблено висновок, що невелика кількість початкових контрольних даних дає змогу лиш відтворити процес в цілому (середня крива процесу), але конкретні значення в прогнозованому трафіку досить сильно будуть відрізнятися від реальних (траєкторія керування).

Тому, знаючи середні параметри в мережевому трафіку та точку входу в прогноз, не давало змоги точно передбачити поведінку системи в майбутньому.

Підсумовуючи, зроблено висновок, що даний метод “обирав” потрібну траєкторію в залежності від точки входу та середньої траєкторії.

Підвищення часу спостережень до t = 40, 90 с (рис. 3.3) збільшував достовірність прогнозування, тому при t = 90 с можна було говорити про достатньо точний прогноз.

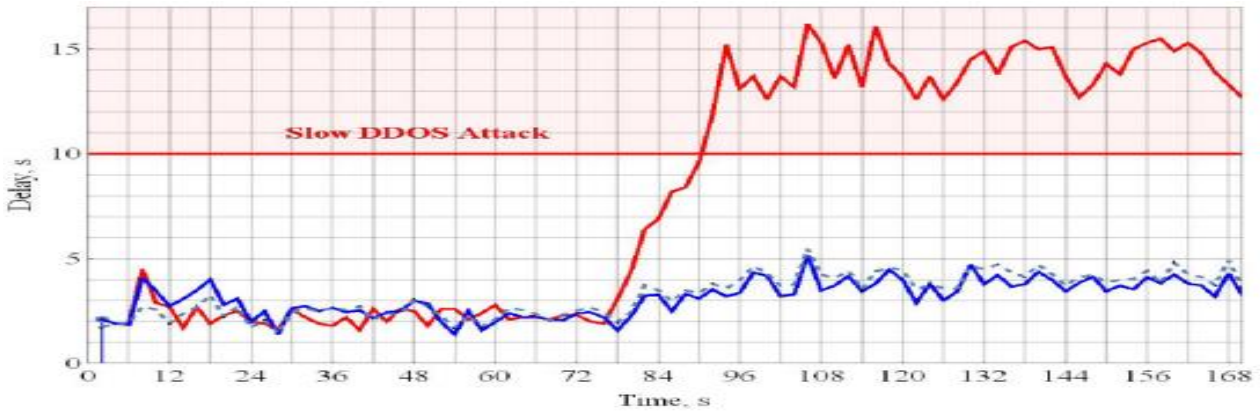
$$P^{ps} = P\{X(s) \in S_0 \ / \ x_\omega(t)\} \geq 0{,}99.$$

На малюнках 3.3 (б) і 3.3 (в) позначено криві інших кольорів, що демонстрували спосіб здійснення прогнозування при отриманні даних від інших контрольних точок $t_{\mu,}\mu = [1, k]$, $k < I$, що відбувається після моменту $t_{k,}$.

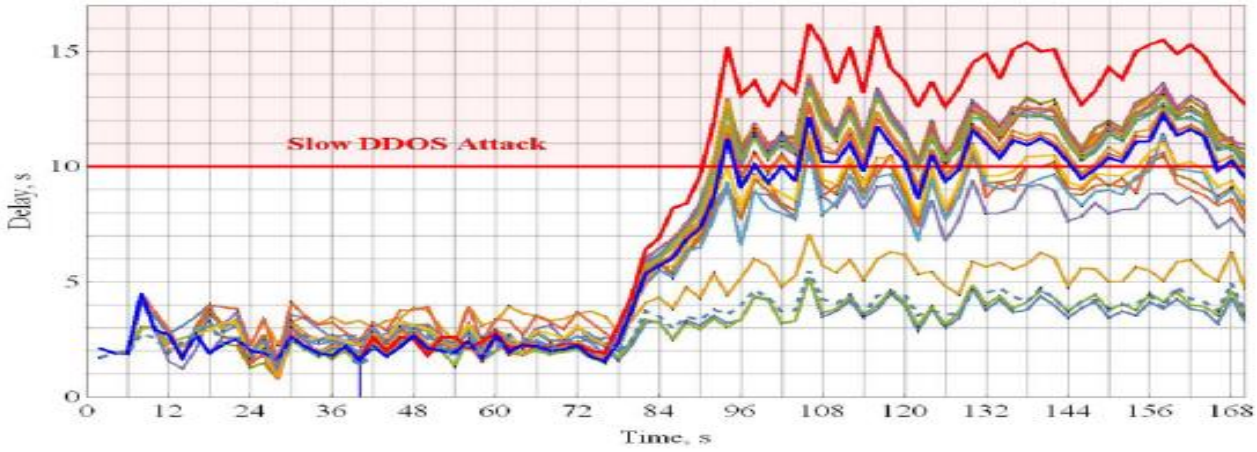
Ймовірність неправильного вибору траєкторії залежала від обсягу вихідних даних, які знаходились під спостереженням.

В даному випадку точність прогнозу залежала від особливостей поведінки траєкторії, що призводила до аномального трафіку.

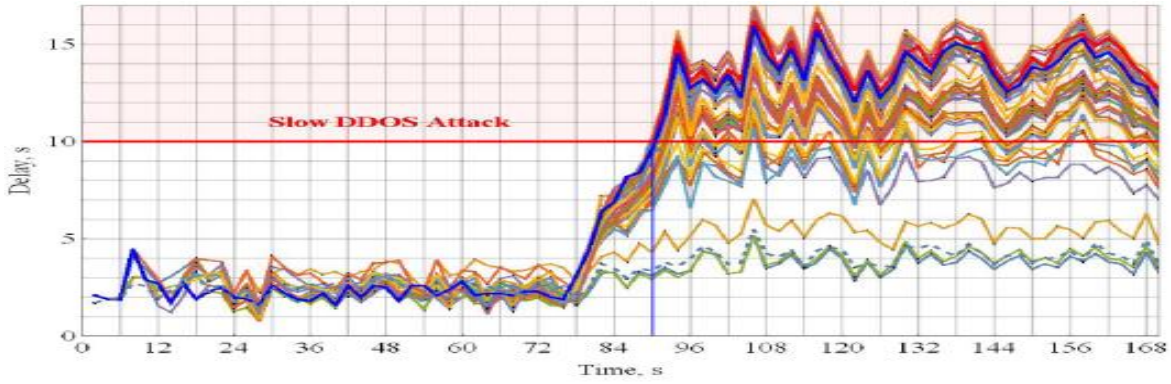
Для прикладу даної моделі поставало питання про потрібну кількість спостережень і точність прогнозування траєкторії руху атаки.




*а*) при t = 1 с




*б*) при t = 40 с




*в*) при t = 90 с

Рисунок 3.3 – Прогнозування поведінки користувача

На рисунках 3.3 (а, б) продемонстровані криві трафіку при часі спостереження довжиною в 1 та 40 секунд відповідно.

Недостатня кількість часу спостереження не дала очікуваного результату у виявленні аномального трафіку.

У таблиці 3.1 наведено результати розрахунків, які показали, що збільшення точності передбачення відбувається при більш тривалому спостереженні за поведінкою користувача і досягає < 1% при часі спостереження 90 секунд.

Таблиця 1

Середнє відхилення прогнозу від здійснення контролю поведінки користувача

| Час спостереження, с | 1 | 10 | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 |
|---|---|---|---|---|---|---|---|---|---|---|
| Відхилення, % | 86 | 64 | 44 | 28 | 19 | 12 | 6 | 3 | 2 | ≤1 |

Отже, результатами моделювання підтверджено адекватність моделі прогнозування для ідентифікації повільних DDoS-атак, що базується на індивідуальному передбаченні поведінки користувача.

Випадковий процес в цьому випадку визначався в контрольних точках та забезпечував мінімум середньої квадратичної помилки в інтервалах між цими точками.

### 3.2 Пропозиції щодо удосконалення методу

Можливим шляхом удосконалення роботи даного методу є оновлення модулей моделі виявлення та блокування повільних та малопотужних DDoS-атак. Після створення моделі модуль класифікатора атак міг коректно ідентифікувати лиш актуальні на той момент види повільних та малопотужних DDoS-атак. Таким чином , покращення моделі шляхом оновлення модулю класифікатора атак є досить логічним кроком.

Автором даної роботи запропоновано оновити модулі моделі шляхом синхронізації бази даних модулів збору трафіка та класифікаторів атак і з базами даних сучасних аналізаторів мережевого трафіку. Прикладами актуальних

аналізаторів мережевого трафіку є інструменти: SolarWinds, Paessler, Wireshark, NetFort LANGuardian, ManageEngine NetFlow Analyzer, Harioc, Ісинга, Громада спостережень, SolarWinds Network Traffic Monitor, ntopng і т.п [29]. Більш докладна інформація про 1 із прикладів сучасних аналізаторів трафіку наведена нижче:

Сучасним прикладом безкоштовного аналізатору трафіку є програма WireShark. Wireshark (раніше звався **Ethereal**) — програма для аналізу мережевих пакетів Ethernet і інших мереж (сніфер) з вільним вихідним кодом. Має графічний інтерфейс користувача.

Функціональність, яку надає Wireshark, дуже схожа з можливостями програми tcpdump, проте Wireshark має графічний інтерфейс користувача і значно більше можливостей із сортування і фільтрації інформації. Програма дозволяє користувачеві переглядати весь трафік, що проходить по мережі, в режимі реального часу (рис. 3.4).

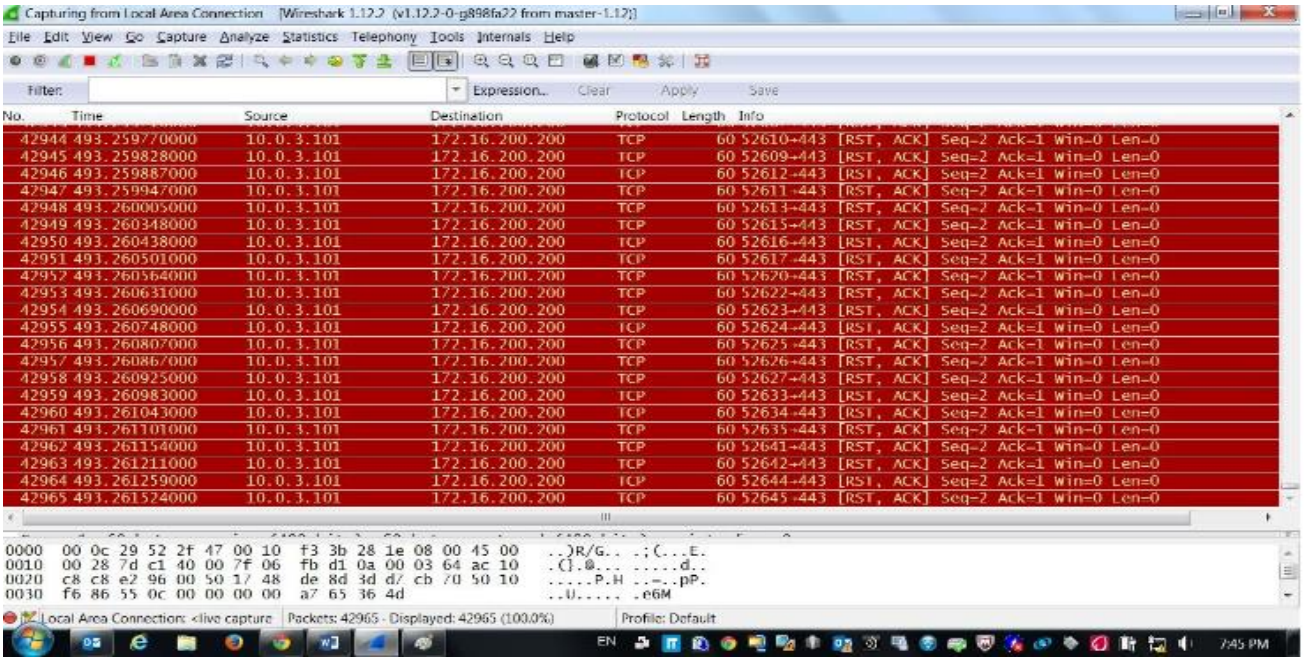



Рисунок 3.4 – Відображення DDoS-атаки у програмі WireShark

Отже, після успішного злиття з базами даних наведених аналізаторів трафіку, дана модель зможе коректно класифікувати більшість сучасних видів повільних та малопотужних DDoS-атак.

Таким чином, на основі методу і його удосконаленої моделі виявлення та блокування повільних та малопотужних DDoS-атак шляхом прогнозування поведінки користувача можуть створюватися сучасні інструменти для захисту веб-сайтів від повільних та малопотужних DDoS-атак. Також дана модель може використовуватись в якості допоміжного інструменту для вже існуючих консервативних методів захисту веб-сайтів від DDoS-атак серед яких є: WAF, NGFW та інше.

Удосконалення моделі подібним шляхом забезпечить її актуалізацію для використання в різних випадках, коли йде мова про захист веб-сайтів від повільних та малопотужних DDoS-атак.

**Висновок до розділу 3**

Повільні DDoS-атаки стають все поширенішими через їхню легкість виконання та складність виявлення. Традиційні методи виявлення атак виявляються неефективними через затримку в реагуванні на атаки та аналіз трафіку.

Ефективнішим підходом є прогнозування поведінки користувачів на основі статистики попередніх атак. Прогнозування індивідуальної поведінки користувача дозволяє виявляти повільні DDoS-атаки, використовуючи алгоритм пошуку невідомих майбутніх значень для параметрів руху.

Такий підхід дозволяє точно визначати випадкові процеси в контрольних точках і мінімізувати середньоквадратичну помилку апроксимації в інтервалах між ними.

Однак, даний метод потребує вдосконалення. Для покращення і актуалізації даного методу, автором роботи було запропоновано оновити модулі даної моделі шляхом синхронізації бази даних модулів відповідної моделі з базами даних сучасних мережевих аналізаторів трафіка. Запропоновані кроки дадуть змогу коректно класифікувати більшість сучасних повільних та малопотужних DDoS-атак у разі виявлення моделлю аномального трафіку.

На основі запропонованих пропозицій для удосконаленої методу шляхом оновлення моделі виявлення та блокування повільних та малопотужних DDoS-атак

за допомогою прогнозування поведінки користувача можуть створюватися сучасні інструменти для захисту веб-сайтів від DDoS-атак. Також даний метод може використовуватись в якості допоміжного інструменту для вже існуючих консервативних методів захисту веб-сайтів від DDoS-атак серед яких є: WAF, NGFW та інше. Це забезпечить підвищення ефективності захисту веб-сайтів від DDoS-атак за допомогою ефективного виявлення та блокування повільних та малопотужних DDoS-атак.

# ВИСНОВКИ

У кваліфікаційній роботі розв’язано актуальне наукове завдання щодо розробки пропозицій для удосконалення методу виявлення та блокування повільних та малопотужних DDoS-атак. В ході розв’язання поставлених задач були отримані наступні наукові та практичні результати:

1. Проведено огляд та аналіз сучасних методів захисту веб-сайтів від DDoS-атак.

2. Надано оцінку їх ефективності для захисту веб-сайтів від повільних та малопотужних DDoS-атак.

3. Проведено огляд та аналіз моделі виявлення та блокування повільних та малопотужних DDoS-атак.

4. Розроблено пропозиції для удосконалення даної моделі.

Результатом даної роботи є розроблені рекомендації для удосконалення моделі методу виявлення та блокування повільних та малопотужних DDoS-атак на основі прогнозування поведінки користувача, а також способи можливі способи використання удосконаленого методу.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. What is a cyber attack? [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.logpoint.com/en/blog/cyber-attack/.

3. What is a cyberattack? [Електронний ресурс] – Режим доступу до ресурсу: https://www.chathamhouse.org/2022/02/what-cyber-attack?gclid=CjwKCAjwgqejBhBAEiwAuWHioGOQ6uQ6898sqjIj7bENpqijfQQKu42cAVTjnPVjtM5X4_aoejaAhxoCXr0QAvD_BwE.

4. Baker K. 10 MOST COMMON TYPES OF CYBER ATTACKS [Електронний ресурс] / Kurt Baker // 2023 – Режим доступу до ресурсу: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/.

5. The Consequences of Cyber Attacks and Their Impact on Cybersecurity [Електронний ресурс] // CopyCEI. – 2023. – Режим доступу до ресурсу: https://www.copycei.com/the-consequences-of-cyber-attacks-and-their-impact-on-cybersecurity/.

6. DoS-атака [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B03.

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

8. Baivab Kumar Jena. What Is a Botnet, Its Architecture and How Does It Work? [Електронний ресурс] / Baivab Kumar Jena – Режим доступу до ресурсу: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-a-botnet.

9. What is a Content Delivery Network (CDN)? | How do CDNs work? [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudflare.com/learning/cdn/what-is-a-cdn/.

10. What is a Botnet? [Електронний ресурс] – Режим доступу до ресурсу: https://usa.kaspersky.com/resource-center/threats/botnet-attacks.

11. Nivedita J. 45 Global DDOS Attack Statistics 2023 [Електронний ресурс] / James Nivedita. – 2023. – Режим доступу до ресурсу: https://www.getastra.com/blog/security-audit/ddosattackstatistics/#:~:text=According%20to%20Kaspersky's%20quarterly%20report,lowest%20(12.99%25)%20on%20Thursday.

12. Готовність України до нових викликів. Кібербезпека і зв'язок [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://cip.gov.ua/ua/news/gotovnist-ukrayini-do-novikh-viklikiv-kiberbezpeka-i-zv-yazok

13. IT-армія блокує російські сайти за декілька хвилин — головні перемоги України на кіберфронті [Електронний ресурс] // Міністерство цифрової трансформації України. – 2022. – Режим доступу до ресурсу: https://www.kmu.gov.ua/news/mincifri-it-armiya-blokuye-rosijski-sajti-za-dekilka-hvilin-golovni-peremogi-ukrayini-na-kiberfronti.

14. What is a low and slow attack? [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudflare.com/learning/ddos/ddos-low-and-slow-attack/.

15. A. Dhanapal and P. Nithyanandam. The Slow HTTP DDOS Attacks: Detection, Mitigation and Prevention in the Cloud Environment. Scalable Computing: Practice and Experience. 2019. Volume 20, Number 4, pp. 669–685. https://doi.org/ 10.12694/ scpe.v20i4.1569

16. H. Abusaimeh, H. Atta, H. Shihadeh. Survey on Cache-Based Side-Channel Attacks in Cloud Computing. International Journal of Emerging Trends in Engineering Research. 2020. Volume 8, No. 4, p. 1019–1026.

17. Лаптев О. А., Собчук В. В., Саланди И. П., Сачук Ю. В. Математична модель структури інформаційної мережі на основі нестаціонарної ієрархічної та стаціонарної

гіпермережі. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. 2019. Вип. 64. С. 124–132.

18. C. L. Calvert, T. M. Khoshgoftaar Impact of class distribution on the detection of slow HTTP DoS attacks using Big Data. Journal of Big Data. 2019. Volume 6, No. 67 https://doi.org/10.1186/s40537- 019-0230-3.

19. Karaboga D. An idea based on honey bee swarm for numerical optimization Technical Report TR06, Erciyes University, Engineering Faculty, Computer Engineering Department, 2005.

20. Ya. V. Tarasov. Investigation of the application of neural networks for the detection of low-intensity DDoS-attacks of the application level. Cybersecurity. 2017. Issues №5(24). PP. 23–29. https://doi.org/ 10.21681/2311-3456-2017-5-23-29.

21. Kureichik V. V., Zaruba D. V., Zaporozhets D. Y. Algoritm parametricheskoy optimizatsii na osnove modeli povedeniya roya svetlyachkov. Parametric optimization algorithm based on the model of glowworm swarm behavior. Izvestiya SFedU. Engineering Sciences. 2015, no. 6 (167), pp. 6–15.

22. Лаптєв О. А., Собчук В. В., Савченко В. А. Метод підвищення завадостійкості системи виявлення, розпізнавання і локалізації цифрових сигналів в інформаційних системах. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. 2019. Вип. 66. С. 124–132.

23. M. Idhammad, K. Afdel, and M. Belouch. Detection System of HTTP DDoS Attacks in a Cloud Environment Based on Information Theoretic Entropy and Random Forest. Security and Communication Networks. 2018, Volume Article ID 1263123, 13 p. https://doi.org/10.1155/2018/1263123.

24. Лаптєв О. А. Експериментально-статистичний метод обчислення кореляційної взаємозалежності параметрів розпізнавання засобів негласного отримання інформації. Сучасний захист інформації. 2019. № 3(39). С. 23–29.

25. S. Lysenko, V. Tkachuk. Method and software for detecting r.u.d.y. attack based on the usage of the algorithm of determining traffic self-similarity. Herald of Khmelnytskyi national university. 2019. Issue 3, p. 273.

26. Sobchuk A. V., Sobchuk V. V., Barabash O. V., Lyashenko I. O. Functionally sustainable wireless sensor network technologies aspects analysis. Science and Education a New Dimension. Natural and Technical Sciences. 2019. VII (23), Issue 193, Budapest, Hungary, pp. 46–48. Наукоємні технології № 3(55), 2022 © Лаптєв О. А., Бучик С. С., Савченко В. А., Наконечний В. С., Михальчук І. І., Шестак Я. В., 2022 191

27. B. Cusack, and Z. Tian. Detecting and tracing slow attacks on mobile phone user service. In Valli, C. (Ed.). The Proceedings of 14th Australian Digital Forensics Conference, 5–6 December 2016, Edith Cowan University, Perth, Australia. pp. 4–10, 2016

28. V. Savchenko, O. Matsko, O. Vorobiov, Y. Kizyak, L. Kriuchkova, Y. Tikhonov, A. Kotenko Network traffic forecasting based on the canonical expansion of a random process. Eastern European Journal of Enterprise Technologies. 2018. VOL 3, NO 2 (93). p. 33–41

29. Gopalan V. Top 15 DDoS Protection Best Practices [Електронний ресурс] / Vivek Gopalan. – 2023. – Режим доступу до ресурсу: https://www.indusface.com/blog/best-practices-to-prevent-ddos-attacks/.

30. Stopping Infrastructure Attacks and Application Attacks with DDoS Tools and Threat Intelligence [Електронний ресурс] // A10 Staff. – 2022. – Режим доступу до ресурсу: https://www.a10networks.com/blog/ddos-attack-prevention-and-ddos-protection-best-practices/.

31. DNS Amplification [Електронний ресурс] – Режим доступу до ресурсу: https://www.imperva.com/learn/ddos/dns-amplification/.

32. ЩО ТАКЕ CDN? НАВІЩО ВІН ПОТРІБЕН? ЩО ДАЄ ЙОГО ВИКОРИСТАННЯ? [Електронний ресурс] – Режим доступу до ресурсу: https://zahid.host/uk/cdn/.

33. WAF [Електронний ресурс] – Режим доступу до ресурсу: https://itglobal.com/ru-ru/company/glossary/waf/.

34. Аналізатор мережевого трафіку [Електронний ресурс] – Режим доступу до ресурсу: https://uk.myservername.com/11-best-network-traffic-analyzers#1_SolarWinds_Network_Traffic_Analysis_Tool.