

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій  
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки  
(повне найменування кафедри)

## Пояснювальна записка

до дипломного проєкту (роботи)

магістр

(ступінь вищої освіти)

на тему Дослідження ефективності захисту від DDoS-атак у розподілених

мережах

(назва теми)

Виконав(ла): студент(ка) IIм курсу,  
групи БКЗ-813м

Спеціальності 125 Кібербезпека та  
захист інформації

(код і найменування спеціальності)

Освітня програма (спеціалізація)

Безпека інформаційних і комунікаційних  
систем

ВСЬЧЕВА О.В.

(ПРИЗВИЩЕ та ініціали)

Керівник КОРОЛЬКОВ Р.Ю.

(ПРИЗВИЩЕ та ініціали)

Рецензент ЛИТВИЦЬКИЙ О.П.

(ПРИЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій

Кафедра інформаційної безпеки та наноелектроніки

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека та захист інформації

(код і найменування)

Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних систем

(назва освітньої програми (спеціалізації))

**ЗАТВЕРДЖУЮ**

Завідувач кафедри ІБтаН

Андрій КОРОТУН

«\_\_\_» \_\_\_\_\_ 2024 року

**З А В Д А Н Н Я**  
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

**ВСЬЧЕВОЇ Ольги Валентинівни**

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Дослідження ефективності захисту від DDoS-атак у розподілених мережах

Research on the effectiveness of protection against DDoS attacks in distributed networks

керівник проєкту (роботи) к.т.н., КОРОЛЬКОВ Роман Юрійович,

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від «05» грудня 2024 року №507

2. Строк подання студентом проєкту (роботи) 10.12.2024

3. Вихідні дані до проєкту (роботи) види розподілених атак із відмовою в обслуговуванні

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

Захист від розподілених атак із відмовою в обслуговуванні

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Презентація доповіді (в MS PowerPoint), 12 слайдів.

6. Консультанти розділів проєкту (роботи)

| Розділ        | ПРИЗВИЩЕ, ініціали та посада консультанта | Підпис, дата   |                           |
|---------------|-------------------------------------------|----------------|---------------------------|
|               |                                           | завдання видав | прийняв виконане завдання |
| 1 – 3         | КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН     | 02.09.2024     | 05.12.2024                |
| Нормоконтроль | КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН     |                | 09.12.2024                |
|               |                                           |                |                           |
|               |                                           |                |                           |
|               |                                           |                |                           |
|               |                                           |                |                           |
|               |                                           |                |                           |

7. Дата видачі завдання «02» вересня 2024року.

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів дипломного проєкту (роботи)                                   | Строк виконання етапів проєкту (роботи) | Примітка |
|-------|----------------------------------------------------------------------------|-----------------------------------------|----------|
| 1.    | Збір та аналіз інформації про класифікацію DDoS-атак                       | 02.09.24 – 16.09.24                     | виконано |
| 2.    | Систематизація літературних даних                                          | 17.09.24 – 23.09.24                     | виконано |
| 3.    | Складання і затвердження наукового завдання                                | 24.09.24 – 29.09.24                     | виконано |
| 4.    | Формування та уточнення наукового завдання                                 | 30.09.24 – 05.10.24                     | виконано |
| 5.    | Аналіз методів захисту від DDoS-атак                                       | 06.10.24 – 15.10.24                     | виконано |
| 6.    | Аналіз методів захисту хмарних сервісів, IoT та SMART-систем від DDoS-атак | 16.10.24 – 13.11.24                     | виконано |
| 7.    | Оформлення графічної частини                                               | 14.11.24 – 19.11.24                     | виконано |
| 8.    | Оформлення ПЗ                                                              | 20.11.24 – 30.11.24                     | виконано |
|       |                                                                            |                                         |          |
|       |                                                                            |                                         |          |
|       |                                                                            |                                         |          |
|       |                                                                            |                                         |          |
|       |                                                                            |                                         |          |
|       |                                                                            |                                         |          |

Студент(ка)

Ольга ВСЬЛЬЧЕВА

(підпис) (Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

Роман КОРОЛЬКОВ

(підпис) (Ім'я ПРИЗВИЩЕ)

## АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 79 с., 11 рис., 141 джерело.

DDOS-АТАКА, БОТ, ЗЛОВМИСНИК, ЗАХИСТ ВІД DDOS-АТАК, ЗАПОБІГАННЯ DDOS-АТАКАМ, ФІЛЬТРИ

Мета роботи: дослідження методів захисту від DDoS-атак та підходів до запобігання цим атакам.

Об'єкт та предмет дослідження: об'єктом дослідження є розподілені атаки на відмову в обслуговуванні (DDoS); предметом дослідження є методи захисту від DDoS-атак.

Методи дослідження: описово-аналітичний.

Результати: результатом дослідження є виявлення сильних та слабких сторін різних методів захисту від DDoS-атак.

Рекомендації щодо впровадження: робота носить прикладний характер, а її результати можуть бути використані для розробки методів захисту від DDoS-атак нових типів.

Практична цінність: досліджено та класифіковано різні методи захисту від DDoS-атак.

## **ABSTRACT**

Explanatory note to the master's thesis: 79 p., 11 figure, 141 sources.

**DDOS ATTACK, BOT, ANNULER, DDOS ATTACK PROTECTION,  
DDOS ATTACK PREVENTION, FILTERS**

The purpose of the work: study of methods of protection against DDoS attacks and approaches to preventing these attacks.

Object and subject of research: the object of the research is distributed denial of service attacks (DDoS); the subject of the research is methods of protection against DDoS attacks.

Research methods: descriptive-analytical.

Results: the result of the research is the identification of the strengths and weaknesses of various methods of protection against DDoS attacks.

Recommendations for implementation: the work is of an applied nature, and its results can be used to develop methods of protection against new types of DDoS attacks.

Practical value: various methods of protection against DDoS attacks have been studied and classified.

## ЗМІСТ

|                                                           |    |
|-----------------------------------------------------------|----|
|                                                           | C. |
| Вступ. ....                                               | 8  |
| 1 Атаки у розподілених мережах. ....                      | 11 |
| 1.1 Класифікація DDoS-атак. ....                          | 11 |
| 1.2 Стратегії атак. ....                                  | 12 |
| 1.2.1 Синопис атаки на основі ступеня автоматизації. .... | 14 |
| 1.2.2 Фази атаки ....                                     | 15 |
| 1.3 Механізми атак. ....                                  | 20 |
| 1.3.1 Атаки з виснаженням ресурсів. ....                  | 22 |
| 1.3.2 Атака на виснаження пропускної здатності ....       | 28 |
| 1.3.3 Атака на інфраструктуру ....                        | 33 |
| 1.3.4 Атака нульового дня ....                            | 35 |
| 2 Протидія DDoS-атакам. ....                              | 36 |
| 2.1 Запобігання DDoS-атакам. ....                         | 36 |
| 2.1.1 Профілактика за допомогою фільтрів. ....            | 37 |
| 2.1.2 Створення накладної мережі ....                     | 42 |
| 2.1.3 Імітування законної мережі ....                     | 42 |
| 2.1.4 Балансування навантаження. ....                     | 43 |
| 2.1.5 Профілактика, заснована на обізнаності. ....        | 43 |
| 2.2 Захист від DDoS-атак ....                             | 44 |
| 2.2.1 Виявлення. ....                                     | 45 |
| 2.2.2 Механізм реагування. ....                           | 53 |
| 2.2.3 Мінімізація впливу атак. ....                       | 54 |
| 3 DDoS-атаки на інші системи. ....                        | 55 |
| 3.1 DDoS-атаки на хмари. ....                             | 55 |
| 3.2 DDoS-атаки на розумні мережі. ....                    | 57 |
| 3.3 DDoS-атаки на розумні будинки. ....                   | 58 |
| 3.4 DDoS-атаки на системи IoT. ....                       | 59 |

|                                      |    |
|--------------------------------------|----|
| 3.5 DDoS-атаки на CPS . . . . .      | 60 |
| 3.6 Обговорення результатів. . . . . | 61 |
| Висновки. . . . .                    | 63 |
| Перелік джерел посилення. . . . .    | 64 |

## ВСТУП

21 жовтня 2016 року був відмічений потік розподілених атак на відмову в обслуговуванні (DDoS), в якому було задіяно десятки мільйонів адрес Інтернет-протоколів (IP), що атакували систему доменних імен `dyn` (DNS) [1]. Стверджується, що швидкість атаки становила 1,2 Тбіт/с, і вона задіяла пристрої Інтернету речей (IoT). Цей значний випадок довів величезну небезпеку, притаманну DDoS-атакам, і зайняла увагу сучасного кіберсвіту. Ця атака відкрила важливу дискусію про кібербезпеку та її непередбачуваність. Відповідно до дванадцятого річного звіту мережі Arbor, розмір і зростання DDoS-атак були найбільшими в останні роки, і їх частота також зросла за останні кілька років.

Дизайн Інтернету забезпечує найкращі зусилля стосовно послуг з комутацією пакетів для користувачів [2,3]. Результатом є спільне використання ресурсів різними користувачами. Як наслідок, поведінка одного користувача може створювати перешкоди для послуг інших користувачів. Одна з цілей DDoS-атаки це внести порушення цільовим користувачам, відомим як «жертви». Загалом, DDoS-атака спрямована на перешкоджання доступу законних користувачів до цільової системи або послуг шляхом переважної передачі ресурсів [4]. Наприклад, мережі жертв або потужності обробки споживаються величезним потоком пакетів зломисників, що використовують Інтернет-додатки або служби та протоколи мережевого рівня. Отже, мережі жертв або можливості обробки можуть не обслуговувати у нормальний спосіб і відмовляють у наданні послуг жертвам. Крім того, жертва DDoS-атаки може постраждати внаслідок повної або часткової втрати своїх служб і файлів, якщо не застосувати ретельний метод пом'якшення [5]. Поки що основна загроза цієї атаки походить від її розподіленої природи. У 1999 році консультативна функція комп'ютерних інцидентів (CIAC) [6] повідомила про першу DDoS-атаку.

Загалом пакети DDoS-атаки не показують жодних очевидні характеристики, які можуть відокремити зловмисний потік від законного. Крім того, інструменти, які використовують ці атаки легко доступні зловмисникам і це збільшує частоту та загрозу атак. Таким чином, якщо напад розпочато; його складність і вплив стають пропорційно високими. Все, що користується перевагами менш безпечної архітектури Інтернету з моменту його створення має просту архітектуру, яка зменшує складність базових мереж. Таким чином, основні маршрутизатори мають деякі обмеження, які допомагають DDoS-атакам. Основні маршрутизатори не можуть надавати послуги автентифікації доставленим IP-пакетам. Це обмеження є глибокою проблемою, відома як підробка IP-адреси, яка є однією з ключові можливості DDoS-атак. Під час IP-спуфінгу зловмисники надають неправдиву інформацію, наприклад підроблене джерело IP-адреси в IP-пакетах. Крім того, маршрутизатори також не можуть забезпечити механізми відстеження пакетів через величезний трафік, який вони обробляють. Ці обмеження надають зловмисникам можливість залишатися прихованими під час виконання DDoS-атак. Дизайн Інтернету також забезпечує високу пропускну здатність трафіку підтримки обробки базових мереж і підтримки обробки трафіку низької потужності для крайових мереж. Така конструкція забезпечує максимальне використання посилань з мінімальними витратами. Однак це також представляє можливість перевантажити периферійну мережу, якщо декілька джерела спілкуються з одним пунктом призначення. Це те, що відбувається під час DDoS-атаки. У децентралізованому характер управління Інтернетом, усіма мережами керують локально, а не за допомогою центрального органу управління або ієрархії. Ця децентралізована структура допомогла зростанню Інтернету. Однак цей механізм також допомагає зловмисникам і реалізація надійного механізму захисту стає надзвичайно складною для децентралізованої структури. Без централізованого контролю неможливо розгорнути розподілене рішення для вирішення проблеми DDoS-атак, тому що вони є

повністю розподіленими атаками, а поодинокі точкові рішення не покращують захист від цих атак. Таким чином, цілком очевидно, що навіть високозахищена система не забезпечує захисту від DDoS-атак. Крім того, ресурс жертви завжди обмежений у порівнянні з ресурсом зловмисників, оскільки вони можуть використовувати сценарій розподіленої атаки. Усе це збільшує складність виявлення, запобігання та пом'якшення DDoS-атаки.

# 1 АТАКИ У РОЗПОДІЛЕНИХ МЕРЕЖАХ

## 1.1 Класифікація DDoS-атак

За даними мережі Arbor, кожен день вони відстежують понад 1000 значних різних DDoS-атак по всьому світу [7]. Цілі цих DDoS-атак варіюються від власного домашнього користувача до уряду. У деяких атаках жертвою може бути сайт електронної комерції, банк, комерційна організація або навіть постачальник послуг Інтернету (ISP). Однією з головних причин нападу на цих користувачів є певна фінансова вигода. Однак привабливою мішенню для DDoS-атаки може бути порнографія або азартні онлайн-сайти. Крім того, політичні організації та уряди також є основними цілями DDoS-атак. Ігрові сайти або фондові біржі також можуть бути цілями DDoS-атак.

Таким чином, причини або мотиви DDoS-атак можуть відрізнятися. Однак можна виділити п'ять різних категорій, щоб охарактеризувати мотивацію DDoS-атак [8]:

1. Фінансова чи економічна вигода. Атаки, які підпадають під цю мотивацію, вважаються найнебезпечнішими атаками, оскільки вони намагаються отримати певну фінансову вигоду від атак. Зловмисниками в такому випадку є досвідчені технічні спеціалісти. Таким чином, цей тип атак важко зупинити в нинішньому сценарії.

2. Помста. Це ще одна мотивація для DDoS-атак, коли деякі розчаровані (можливо, технічно менш кваліфіковані) особи здійснюють атаки як відплату за деякі уявні утиски.

3. Ідейні переконання. Деякі зловмисники мотивуються атакувати ціль через свої ідеологічні переконання. Це стало вагомою причиною DDoS-атак. Хоча вони не такі великі за частотою порівняно з іншими мотивами, їхні впливи та розміри такі ж значні, як це спостерігалось в останні роки. Атака на Естонію у 2007 році, атака на Китай і CNN у 2008 році [9], атака на Іран у 2009 році [10], та WikiLeaks у 2010 році [11] є одними з найбільш

висвітлюваних DDoS-атак за останні 10 років, де мотивація атак є або ідеологічною, або політичною.

4. Інтелектуальний виклик. Зловмисники цієї групи в основному мотивовані проводити DDoS-атаки, щоб продемонструвати свої можливості та силу. Наявність простих у використанні інструментів атак і ботнетів мотивує цих зловмисників проводити експерименти з DDoS-атаками.

5. Кібер-тероризм. Це ще одна важлива атака мотивація, яка створює небезпеку та значний економічний вплив на її цілі. Як правило, кілька добре навчених людей військової або терористичної організації здійснюють атаку такого типу. Тут зловмисники належать до одних країн і здійснюють свої атаки на організації інших країн. Для здійснення таких атак використовується значна кількість ресурсів і часу, і це може паралізувати кіберсвіт країни та критичну інфраструктуру через збої в роботі послуг.

## 1.2 Стратегії атак

Базову структуру DDoS-атаки наведено на рис. 1.1 [12]. Вона складається з трьох різних фаз і чотирьох різних компонентів [13]. Компоненти відомі як зловмисник (нападник), кілька обробників, зомбі, а також жертва або цільова машина.

На першому етапі зловмисник витрачає багато свого часу на створення значної кількості скомпрометованих машин, які називаються майстрами або обробниками, оскільки вони призначають і контролюють інші машини нападників. Створення групи обробників зазвичай є автоматизованим процесом, де відбувається безперервне сканування виконане для пошуку машин із лазівками в системі безпеки. Шкідливі коди, встановлені зловмисником у цих обробників, працюють далі, додаючи більше заражених

машин до групи нападників. Підлеглі машини безпосередньо контролюються ботами і опосередковано контролюються зловмисником через цих ботів.

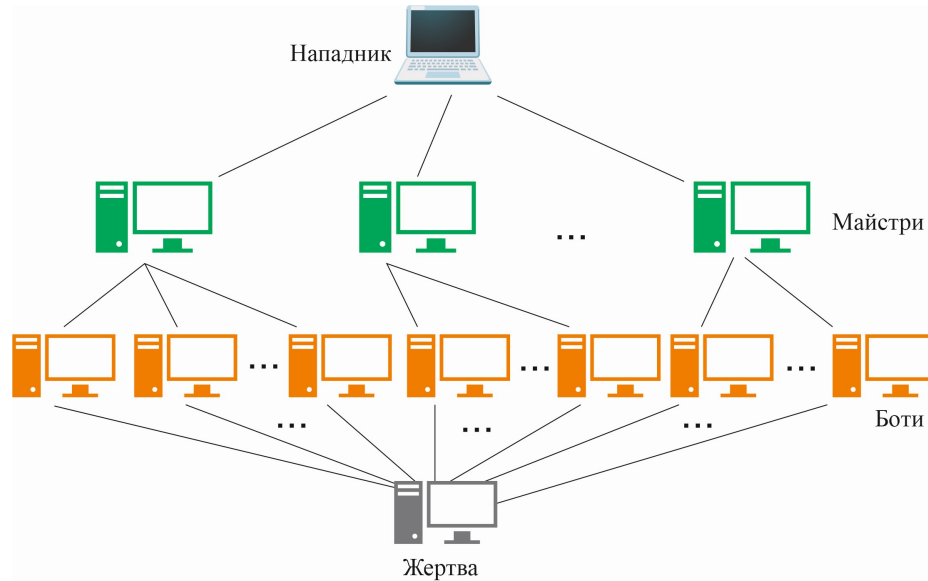


Рисунок 1.1 – Структура DDoS-атаки

Друга фаза починається, якщо достатня кількість пристроїв об'єдналася в ботнет [12]. На другому етапі зловмисник передає всю необхідну інформацію, таку як коди та команди, нападникам, які, у свою чергу, надсилають їх усім зомбі, щоб підготуватися до атаки.

На заключній фазі зловмисник командує своїй армії ботів ініціювати та виконувати атаки. Таким чином, він атакує жертву розподіленим способом і надсилає великий потік пакетів, які, у свою чергу, переповнюють систему або основні ресурси жертви. У цих атаках зловмисник зазвичай використовує підроблені IP-адреси, що допомагає йому приховати ідентифікаційні дані скомпрометованих пристроїв. У більшості випадків таке використання підроблених IP-адрес також перешкоджає жертвам фільтрувати шкідливий трафік, щоб знайти зловмисника.

Тепер детально проілюструємо стратегії атак, які допоможуть досягти кращого розуміння сценаріїв DDoS-атак. Зробимо короткий опис атаки на основі ступеня автоматизації. Також перерахуємо та проаналізуємо методи, задіяні на різних етапах DDoS-атак.

### 1.2.1 Синопис атаки на основі ступеня автоматизації

Різні фази та характеристики DDoS-атак можна встановлювати вручну, контролювати зловмисником або автоматизувати. Тому існує три різні типи сценаріїв атак: ручний, напівавтоматичний і автоматичний, які представлені нижче.

У сценарії атаки вручну зловмисник виконує всю роботу атаки вручну. Сканування машин для пошуку лазівок у безпеці та контроль зламаних машин виконується вручну. Це сценарій, який спостерігався в перші дні DDoS. Сьогодні всі дії стали автоматизованими, що зробило DDoS-атаки більш простими та частими.

Напівавтомат. Механізм атаки агент-обробник за своєю природою є напівавтоматичним. Тут комунікація між обробником і агентами частково ручна, оскільки вони спілкуються, щоб знати один одного. На основі інструкцій, отриманих від зловмисника, ці повідомлення також встановлюють тип, тривалість і жертву атаки. Однак у цьому сценарії атаки сканування, вербування та компрометація машин обробником відбуваються автоматично. Знову ж таки, виходячи з типу зв'язку між обробником і агентами, напівавтоматичні атаки класифікуються на два типи:

Пряме спілкування. У механізмі прямого спілкування обробник і агент знають один одного для подальшого спілкування. Таким чином, IP-адреса обробника жорстко закодована в код атаки. Агент отримує цю IP-адресу, коли код атаки встановлено на скомпрометованій машині агента. Мотивація такого спілкування полягає в тому, щоб повідомити обробників про готовність агентів. Однак цей тип зв'язку можна розпізнати, а також можна виявити DDoS-атаку за допомогою зворотного відстеження.

Непряме спілкування. У цьому сценарії атаки виключено пряме спілкування між обробниками та агентами. Навпаки, для регулювання роботи агентів використовуються деякі Інтернет-комунікаційні служби, такі як

програма Інтернет-чату, канал Інтернет-релейного чату (IRC). Це усуває недолік прямого зв'язку, оскільки легітимна служба IRC ускладнює виявлення шкідливих повідомлень. Крім того, розподілений характер IRC перешкоджає виявленню та дослідженню зв'язку, а також виявленню кореня атаки.

Автоматичний. У цьому сценарії атаки всі етапи та вимоги до здійснення атаки автоматизовані. Тут зломисник атакує жертву без жодного спілкування з обробниками чи агентами. Усі вимоги армії ботів кодуються в коді атаки, який встановлюється на зламаних машинах і пізніше виконується для здійснення атаки. Однак бекдори, створені під час механізму розповсюдження, залишаються відкритими, та їх можна використовувати надалі для зміни існуючих кодів.

### 1.2.2 Фази атаки

Проаналізуємо різні механізми, задіяні в різних фазах атаки. Існує три різні фази DDoS-атак, які можна назвати фаза I – вербування армії ботів, фаза II – розповсюдження та фаза III – атака. Подробиці цих етапів наведено нижче.

Фаза I: вербування армії ботів. Перший етап DDoS-атак полягає у створенні армії атаки або ботнету, як згадувалося раніше. З цією метою зломисник використовує черв'яків (програми, що саморозповсюджуються) [14], які заражають пристрої користувачів, користуючись перевагами їхніх недоліків безпеки [15]. Багато різних методів використовуються для створення цієї армії, як згадується в різних роботах [15-19]. Основна тема полягає в скануванні мереж, щоб знайти машини з недоліками. Ці основні методи зараження машини є такими:

– Випадкове сканування. У стратегії випадкового сканування вже заражені машини перевіряють випадкові IP-адреси з простору IP-адрес для зараження нових машин. Наприклад, для виконання цього сканування можна використовувати добре відомого хробака Code-Red (CRv2) [20]. Це сканування створює величезний трафік, оскільки дуже ймовірно, що машини знаходяться в різних мережах. Крім того, відсутність синхронізації між різними скомпрометованими машинами створює велику кількість повторюваних зондів із заражених машин. Зі збільшенням кількості заражених машин збільшується ймовірність зараження більшої кількості машин. Однак екстремальний трафік, створений ними, також створює можливість виявити атаку.

– Сканування хітів. Сканування списку влучень намагається скоротити час початкового зараження для зараження значної кількості машин. У цій техніці зловмисник створює початковий список машин, які вважаються потенційно вразливими. Коли хробак вивільняється, він переглядає список і, заражаючи машину, передає половину списку на заражену машину. Таким чином, лише за кілька секунд активний хробак може заразити всі ризиковані машини у своєму списку. Наприклад, флеш-хробак може заразити всі машини лише за десятки секунд. Основними витратами цього методу є створення необхідного "списку звернень", але існує багато різних способів його створення. Наприклад, приховане сканування (де зловмисник застосовує сканування портів протягом тривалого періоду часу) і розподілене сканування (де для створення списку використовуються вже скомпрометовані машини) є добре відомими стратегіями сканування для створення списку влучень. Для створення списку зловмисники також можуть використовувати методи веб-сканування або публічні опитування, такі як Netcraft Survey [21]. Також є випадки, коли хробаки транслюють список своїх заражених машин для майбутніх атак. Усе це можна застосувати для створення ефективного списку влучень заздалегідь. Однак під час сканування

списку влучень передача надзвичайно великого списку, а також дубльовані передачі можуть спричинити виявлення атаки.

– Скандування з перестановкою. Скандування з перестановкою — це інтелектуальна техніка скандування, у якій запроваджується самокоординація, щоб зупинити численні перевірки однієї IP-адреси. Крім того, він може визначити, коли будь-яке подальше скандування дасть обмежену користь. Він також може вирішити, коли зупинити процес, вивчаючи розвиток нової інфекції. У цій техніці використовується спільний список псевдовипадкових перестановок простору IP-адрес. Тут для відображення IP-адрес використовується індекс перестановки. Під час скандування перестановок, для вже інфікованого пристрою через скандування списку влучень, нове зараження починається з наступної точки в списку перестановок. Однак, якщо пристрій інфіковано в результаті скандування перестановок, він починає заражати нові пристрої з випадкової точки в списку. Таким чином, якщо під час процесу скандування буде знайдено вже заражену машину, вона не буде заражена знову, а буде обрана новою випадковою початковою точкою для подальших заражень. Крім того, якщо черв'як виявляє, що подальше скандування більше не приносить користі, він може припинити скандування та змінити ключ перестановки, щоб створити новий список перестановок. Це збільшує швидкість зараження та зменшує будь-які повторні зараження.

– Топологічне скандування. Топологічне скандування розглядається як альтернатива скандуванню списку влучень. У цьому процесі скандування, коли пристрій заражається, хробак вибирає свою нову ціль з інформації, що міститься на скомпрометованій машині. У одноранговій програмі, якщо хробак може заразити програму, він може мати список однорангових пристроїв, які є дуже привабливими цілями для наступного зараження. Таким чином, топологічне скандування не потребує попередньо створеного списку пристроїв і може створити власний список, що робить це скандування привабливим для початкового поширення хробака. Крім того, під час інфікування на веб-сервері хробак може поширюватися й інфікувати різних

клієнтів і сервери подібно до поширення інфекційної хвороби. У цьому випадку хробаки у вразливому веб-браузері поширюються, якщо клієнти відвідують сервер, а також клацають певний вміст. Клієнти переносять хробака на інші сервери, які вони відвідують, і посилюють зараження через його розповсюдження [22]. Цей тип розповсюдження не створює інтенсивного трафіку, оскільки виявити такий механізм атаки нелегко. Однак, загалом, топологічне сканування залежить від дій скомпрометованої машини, а не від дій зловмисника. Таким чином, можна отримати повільніший і неповний набір порівняно з іншими типами сканування [23].

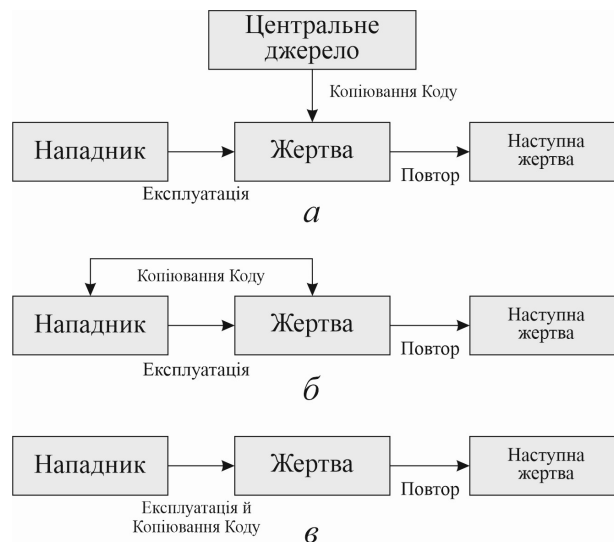
- Сканування локальної підмережі. Під час сканування локальної підмережі вже скомпрометований хост шукає нові цілі у власній локальній підмережі та намагається зламати ці машини. Щоб збільшити кількість скомпрометованих машин, він може спільно використовувати інші вже згадані методи. Основною метою цього методу сканування є зараження якомога більшої кількості локальних машин у підмережі, які зазвичай захищені брандмауером.

Фаза II: розмноження. Наступним етапом після створення армії атаки є поширення коду атаки на скомпрометовані пристрої. Цей код атаки містить інформацію про жертву, час і тривалість атаки тощо:

- Центральне джерело поширення. У механізмі розповсюдження центрального джерела код атаки поширюється від центрального сервера до скомпрометованої машини, як показано на рис.1.2, *а*. Прикладом цього є хробак *l0p*, який розмножується таким чином [24]. Оскільки кожен скомпрометований пристрій спілкується та завантажує копію атаки коду з деяких центральних точок, це вводить величезний обсяг трафіку в мережу, що може зрештою призвести до виявлення атаки. Крім того, ця техніка має потенціал до односторонньої відмови. Таким чином, у разі виявлення атаки видалення центральної точки може зупинити подальше зараження та включення армії атаки.

– Зворотне розповсюдження. У зворотному ланцюжку розповсюдження скомпрометована машина завантажує код атаки із зараженої машини. Цей сценарій показано на рис. 1.2, б. По суті, під час фази зараження зловмисник керує методом, який встановлює зв'язок між зловмисником і скомпрометованою машиною. У цьому механізмі можна використовувати тривіальний протокол передачі файлів (TFTP). Дуже відомий хробак Ramen worm використовує цю техніку розповсюдження в процесі створення армії атаки.

– Автономне розповсюдження. Під час автономного розповсюдження, як випливає з назви, усі коди атаки автоматично передаються від зловмисника до зараженої системи під час експлуатації, як показано на рис 1.2, в. Для передачі кодів атаки не потрібне подальше спілкування з іншими системами. Code-Red є прикладом хробака, який використовує цей механізм розповсюдження. При автономному розповсюдженні трафік, необхідний для розповсюдження коду, суттєво обмежений порівняно з двома іншими методами, і, таким чином, шанс виявити атаку є обмеженим.



*а* – метод розповсюдження з центрального джерела,

*б* – метод розповсюдження зворотного зв'язку,

*в* – метод автономного розповсюдження

Рисунок 1.2 – Розповсюдження коду атаки

Третя фаза DDoS-атак полягає в спробі атаки. Існує багато методів ініціалізації та виконання DDoS-атак, які поділяються на різні категорії. Оскільки аналіз має на меті зрозуміти механізми атаки детально, розглянемо третю фазу DDoS-атак в наступному розділі.

### 1.3 Механізми атак

Щоб зрозуміти дослідження DDoS-атак, важливо розуміти механізми класифікації DDoS-атак. В останні десятиліття в літературі зустрічаються різні класифікації DDoS-атак [3,8,13,16,25,26]. Проаналізуємо всі класифікації атак і представимо простий для розуміння механізм класифікації. На рис. 1.3 представлено механізм класифікації, який охоплює всі аспекти DDoS-атак. [16] Ця класифікація базується на наслідках атак у мережах або ресурсах жертв. Загалом, веб-сервер або проксі-сервер є основною жертвою DDoS-атаки та керує обмеженими ресурсами для надання своїх послуг. Таким чином, загальний сценарій керування надлишковим мережевим трафіком полягає у відкиданні пакетів, які перевищують певні порогові обмеження. Відкидання пакетів також передає повідомлення відправникам пакетів, щоб зменшити швидкість їх надсилання. Законний відправник відповідає на це повідомлення, обмежуючи швидкість надсилання. Однак зловмисник сприймає це як успішне виконання початкової атаки та збільшує її швидкість у відповідь на скидання пакета. Як наслідок, ресурси, призначені системам жертв, такі як пам'ять і ЦП, перевантажуються і не можуть продовжувати свою нормальну роботу. Тому жертва зрештою відхиляє запити від справжніх користувачів. Крім того, ще одним і більш вразливим впливом атаки є виснаження пропускну здатності мережі. У цьому випадку надмірна кількість шкідливих потоків переповнює пропускну здатність мережі, і це впливає не лише на жертву, але й на інші

системи, які залежать від цього шляху атаки. Таким чином, це робить величезний вплив на мережу та системи, підключені до цієї мережі. Тому наша класифікація DDoS-атак враховує ці два впливи та класифікує DDoS-атаки на дві широкі групи: атаки із зменшенням пропускної здатності та атаки із виснаженням ресурсів. Однак насправді атака може мати обидва наслідки та завдати максимально можливих наслідків для всього Інтернету. Цей тип атаки називається інфраструктурною. Також представимо інший тип атак, відомий як атака нульового дня, де наслідки атаки невідомі.

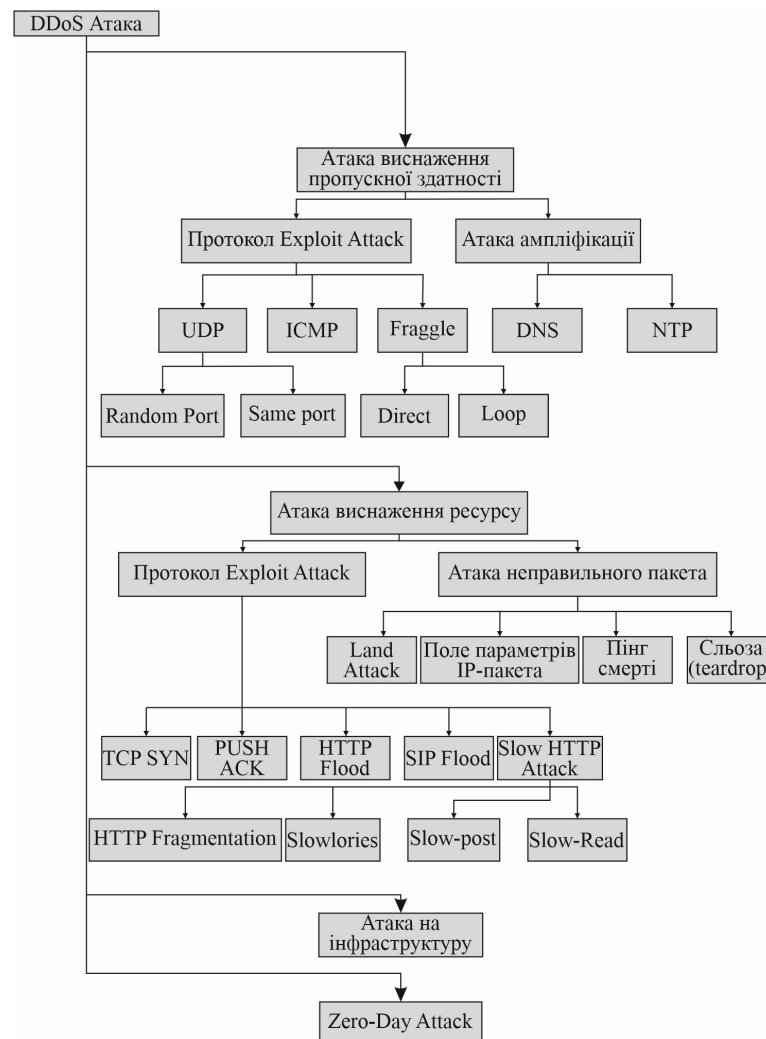


Рисунок 1.3 – Різні типи DDoS-атак

### 1.3.1 Атаки з виснаженням ресурсів

Метою атак із виснаженням ресурсів є переповнення або збій усіх основних ресурсів системи, таких як пам'ять, сокети та процесор. Існує два різних способи реалізації цього типу атак. У першому випадку зломисник використовує деякі мережі, протоколи транспортного та прикладного рівня для досягнення своїх цілей. У другому способі для здійснення атак використовуються неправильно сформовані пакети.

Атаки використання протоколу. Існують деякі основні атаки на основі протоколів, які використовують слабкі місця протоколів різних мережевих рівнів. Це змушує жертву використовувати весь свій процесор і пам'ять для виконання деяких операцій, які потребують великої кількості пам'яті. Наприклад, атаки цієї групи під час виконання атак використовують протоколи транспортного рівня, такі як Transmission Control Protocol (TCP) [27], і деякі протоколи прикладного рівня, такі як Hypertext Transfer Protocol (HTTP) і Session Initiation Protocol (SIP).

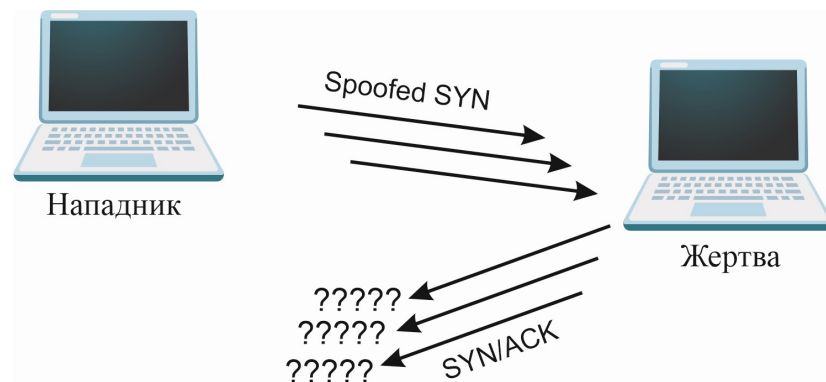


Рисунок 1.4 – Атака TCP SYN[28]

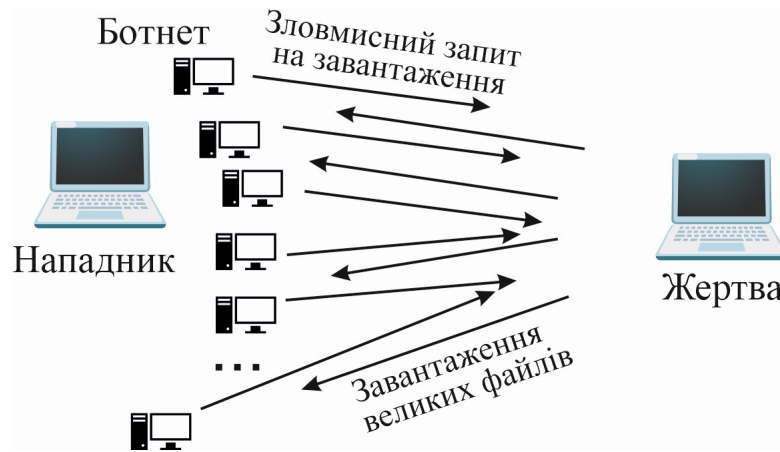


Рисунок 1.5 – Атака HTTP flood (використовує запит HTTP GET) [29]

Атака TCP SYN. Під час атаки TCP SYN зловмисник використовує механізм тристороннього встановлення з'єднання TCP. Для встановлення з'єднання TCP вимагає послідовних підтвердження між двома сторонами, які хочуть створити з'єднання TCP. Це досягається за допомогою тристороннього рукостискання. Під час тристороннього встановлення зв'язку спочатку пакет SYN надсилається від клієнта до сервера, щоб розпочати встановлення зв'язку. Отримавши цей пакет SYN, сервер підтверджує клієнта, надсилаючи пакет SYN + ACK. Нарешті, у відповідь на цей пакет клієнт надсилає останній пакет ACK, який завершує квиткування та встановлює з'єднання TCP. Під час цього процесу сервер зберігає всі проміжні стани в стеках пам'яті, доки не буде встановлено з'єднання або не настане час очікування через пошук і підтвердження ідентичності клієнта. Зловмисник використовує цю функцію та переповнює пам'ять сервера, який зрештою відхиляє запити на з'єднання від дійсних і законних користувачів. Щоб затопити пам'ять жертви, зловмисник не завершує процес рукостискання і таким чином створює величезну кількість неповних з'єднань. Щоб встановити це неповне з'єднання, зловмисник підмінює джерело за допомогою неіснуючих IP-адрес і надсилає SYN-пакети з цими підробленими IP-адресами. Отримавши пакети, сервер відповідає пакетами SYN + ACK, але оскільки IP-адреси джерела не існують, він ніколи не отримує пакети ACK від джерел, як показано на рис. 1.4. Однак, оскільки сервер очікує на пакети

ACK, зрештою всі його таблиці підключень стають заповненими. Таким чином, зловмисник заливає пам'ять жертви та успішно позбавляє законних користувачів. Цю атаку також можна здійснити, використовуючи справжні IP-адреси скомпрометованих машин. У цьому випадку скомпрометовані вихідні машини ігнорують повідомлення SYN + ACK, отримані від жертви, і таким чином можуть здійснити успішну SYN-атаку.

Атака TCP PUSH + ACK. Метою атак цього типу є вичерпання пам'яті та обчислювальної потужності ЦП, щоб перешкодити законним користувачам користуватися їхніми звичайними послугами. Під час цієї атаки скомпрометовані агенти ботнету надсилають велику кількість TCP-пакетів і встановлюють «1» для бітів PUSH і ACK заголовка. Це змушує цільову жертву очистити свій стек пам'яті та надіслати клієнту підтвердження. Оскільки зловмисник наповнює жертву такими повідомленнями, зрештою обчислювальна потужність і пам'ять жертви перевантажуються та вичерпуються. Як наслідок, він не може обробляти запити від законних клієнтів і, таким чином, не в змозі встановити з ними зв'язок.

HTTP flood атака. Атака HTTP flood є ще одним прикладом атак із виснаженням ресурсів, коли протокол прикладного рівня HTTP використовується для атаки на жертву. Зокрема, у цьому типі атак зловмисник маніпулює запитами HTTP GET і HTTP POST під час спілкування з сервером або певною програмою. Тут концепція така ж, як і раніше, тобто перевищення ресурсів для того, щоб веб-сервер відмовив законним користувачам. Для проведення цієї атаки необхідно налаштувати TCP-з'єднання з дійсною IP-адресою. Зловмисник використовує IP-адреси своїх ботнетів для встановлення з'єднань. На рис. 1.5 показано приклад атаки HTTP flood, яка використовує запит HTTP GET. Тут зловмисник виконує HTTP-запит GET для завантаження дуже великого файлу. Він надсилає кілька запитів зі своїх ботнетів. У відповідь на цей запит жертва виконує ряд дій. У відповідь потрібно прочитати файл із внутрішнього сховища, зберегти

його в робочій пам'яті, а також розрізати на кілька пакетів для відправки в ботнети. Таким чином, реакція передбачає використання пам'яті та обчислювальної потужності жертви. Таким чином, велика кількість запитів цього типу заповнює цілі ресурси жертви та робить її нездатною відповідати дійсним користувачам. Щоб ускладнити або навіть унеможливити виявлення такого типу атак, зломисник може також розкрити посилання, додані до відповіді, і перейти за цими посиланнями. Це робить трафік, створений зломисником, схожим на звичайний трафік.

SIP flood атака. Це ще один приклад, у якому використовується інший протокол прикладного рівня під назвою SIP, який використовується для налаштування виклику голосового зв'язку через IP (VOIP). Атаку можна здійснити за допомогою різних типів повідомлень із запитами SIP (таких як SIP REQUEST, SIP INVITE) або повідомлень керування викликами SIP (SIP INFO, SIP NOTIFY) [30]. Метою цієї атаки є затоплення проксі-сервера або сервера реєстрації SIP (SIP REGISTRAR) і використання всіх його ресурсів (ЦП, пам'яті та пропускної здатності мережі) за допомогою армії ботів, як показано на рис. 1.6. Тут будь-яка армія з ботнету надсилає тисячі повідомлень на сервер реєстратора SIP, який відповідає за прийом запитів REGISTRAR, а також за збереження адрес і параметрів агентів користувача, якщо він не отримує повідомлення про помилку сервера. В результаті сервер перевантажується; законні користувачі відчують збій служби та не можуть підключитися до сервера.

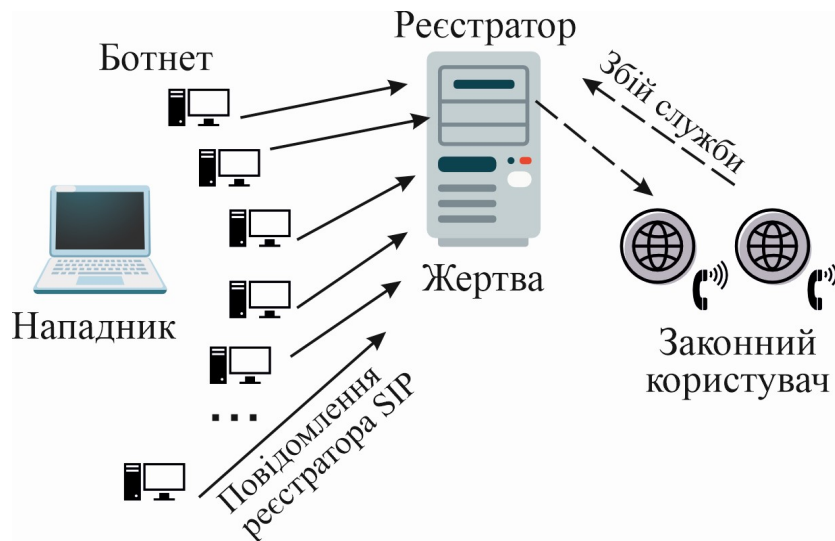


Рисунок 1.6 – SIP flood атака [30]

Повільна атака на запит/відповідь. У цьому типі атак він повільно споживає всі ресурси жертви. Slowlories, атака фрагментації HTTP, атака Slowpost або RUDY (RU Dead Yet), атака повільного читання є деякими прикладами цього типу атак [31-34]. У Slowlories ідея полягає в тому, щоб вимкнути систему жертви за допомогою лише однієї машини. Він починає атаку з часткового HTTP-запиту. Потім він регулярно надсилає іншу інформацію заголовка, щоб сокети залишалися відкритими. Таким чином він споживає всі сокети, і в результаті веб-сервер відхиляє своїх законних клієнтів. Поки що цей тип атак неможливо запобігти, але їх можна пом'якшити, встановивши обмеження на кількість підключень або мінімальну швидкість передачі даних клієнта. Атака фрагментації HTTP розбиває пакет HTTP на дрібні можливі фрагменти та надсилає їх через дійсне з'єднання HTTP з мінімальною можливою швидкістю. Таким чином, він утримує з'єднання якомога довше і робить веб-сайт несправним через кілька з'єднань із ботнету. Slowpost або RUDY або атака на повільний запит також є атакою на прикладному рівні, яка використовує поле подання форми на веб-сайтах. Під час цієї атаки зловмисник відкриває кілька паралельних з'єднань HTTP POST. Зловмисник надсилає інформацію у формі, поданій у

пакеті дуже малого розміру (1 байт) з дуже повільною швидкістю. Таким чином, з'єднання залишаються відкритими протягом дуже тривалого часу і використовують усі з'єднання в таблиці з'єднань сервера. В результаті сервер дає збій і атака стає успішною. Розробником атаки Slow Read DDoS є Shekhan [35], який розробив цю атаку, щоб побачити реакцію HTTP-сервера у разі повільної відповіді. Основна ідея цієї атаки полягає у встановленні з'єднання за допомогою дійсного запиту HTTP. Але зловмисник читає відповідь дуже повільно, щоб зробити з'єднання відкритим якомога довше. Таким чином, кілька таких запитів забирають усі з'єднання та роблять сервер недоступним для законних клієнтів. Загалом від цих повільних HTTP-атак можна захиститися, якщо до потоку застосувати набір спостережень і обмеження швидкості. Наприклад, відхилення непідтримуваних HTTP-з'єднань або застосування обмежень на швидкість вхідних даних або обмеження довжини заголовка чи тіла повідомлення тощо може бути хорошим заходом захисту від повільних HTTP-атак [36].

Атака неправильного пакета. Основна ідея атаки зі спотвореним пакетом полягає в тому, щоб атакувати жертву за допомогою деформованого пакета, який може заплутати жертву і, як наслідок, спричинити збій системи. Нижче наведено деякі з цих атак:

1. Сухопутна атака. У цьому типі атак він встановлює IP-адресу жертви на IP-адреси джерела та призначення пакету. Щоразу, коли система отримує цей тип пакету, вона відповідає сама собі, що, у свою чергу, створює нескінченний цикл. В результаті цього в кінцевому підсумку система виходить з ладу.

2. IP packet option field атака. Ця атака націлена на необов'язкові поля IP-пакету та рандомізує його значення. Наприклад, якщо в IP-пакеті всі біти якості обслуговування встановлені на 1, це змушує жертву застосувати додатковий час для аналізу пакета. Таким чином, це може затопити здатність жертви обробляти, якщо потік пакетів надходить із такою деформацією.

3. Пінг смертельної атаки. У ping of death attack, an зловмисник навмисно створює пакет даних, який перевищує максимальний розмір пакета, що призводить до зависання або збою жертви [26, 37]. Ця атака може бути ініційована лише зловмисником без необхідності використання ботнету. На щастя, поточні хост-системи захищені від таких атак.

4. Краплеподібний напад. Ця атака передбачає маніпуляції зі значенням зміщення, що, у свою чергу, створює помилки під час фрагментації та повторного збирання пакетів. В основному зловмисник надсилає фрагментовані пакети з числами зміщення, що перекриваються. Таким чином, під час повторного збирання пакетів створюються недійсні пакети, які призводять до збою або перезавантаження цільової машини.

### 1.3.2 Атака на зменшення пропускної здатності

Атака із зменшенням пропускної здатності є ще одним важливим типом атак у світі DDoS. Мета зловмисника – використати всю пропускну здатність мережі системи жертви за допомогою армії атаки. Як наслідок, жертва відмовляє в обслуговуванні законним користувачам протягом невеликого чи великого періоду часу, доки атака не буде пом'якшена. Атаку з виснаженням пропускної здатності також можна використати за допомогою протоколу [38], і це можна зробити шляхом посилення, де задіяний рефлектор або підсилювач для збільшення щільності атаки, а також пошкодження мережі [39]. Далі представимо цей механізм атаки на відповідних прикладах.

Атака з використанням протоколу. Атаки з використанням протоколу можуть використовувати протокол транспортного рівня, наприклад протокол дейтаграм користувача (UDP), або протокол мережевого рівня, наприклад протокол керуючих повідомлень Інтернету (ICMP). Основні типи таких атак:

UDP flood атака. Атака UDP flood є дуже поширеною DDoS-атакою, коли зловмисник надсилає великий потік UDP-пакетів зі своєї армії ботів. Тут зловмисник може націлитися на певний або випадковий порт жертви, щоб затопити його. Зазвичай, коли система отримує пакет UDP, вона намагається визначити тип програми, яка очікує на порту призначення. Коли стає впевненим, що жодна програма не очікує, вона відповідає пакетом ICMP, як показано на рис. 1.7. Зловмисник використовує підроблені IP-адреси та продовжує надсилати пакети, доки не буде використано всю смугу пропускання, а жертва не вийде з нормальної роботи.

ICMP flood атака. Атака ICMP flood, також відома як атака ping flood, використовує пакети ICMP\_ECHO\_REQUEST протоколу IP-рівня ICMP. Цей пакет (ping) використовується для перевірки, чи живий віддалений хост чи ні. У DDoS-атаках зловмисник надсилає цей пакет, використовуючи широкомовну IP-адресу. Таким чином, він доставляється на всі машини в мережі жертви. Комп'ютери відповідатимуть на підроблену адресу джерела, націлену на жертву, пакетом ICMP\_ECHO\_REPLY. Крім того, зловмисник може використовувати посередницьку мережу, щоб затопити жертву. У результаті пропускна здатність мережі жертви стає насиченою, і, як наслідок, вона відхиляє запити від законних користувачів. Прикладом цього типу є атака «Smurf», яка використовує деякі мережі-посередники, також відомі як рефлектори, для посилення атаки. Цей сценарій показано на рис. 1.8.

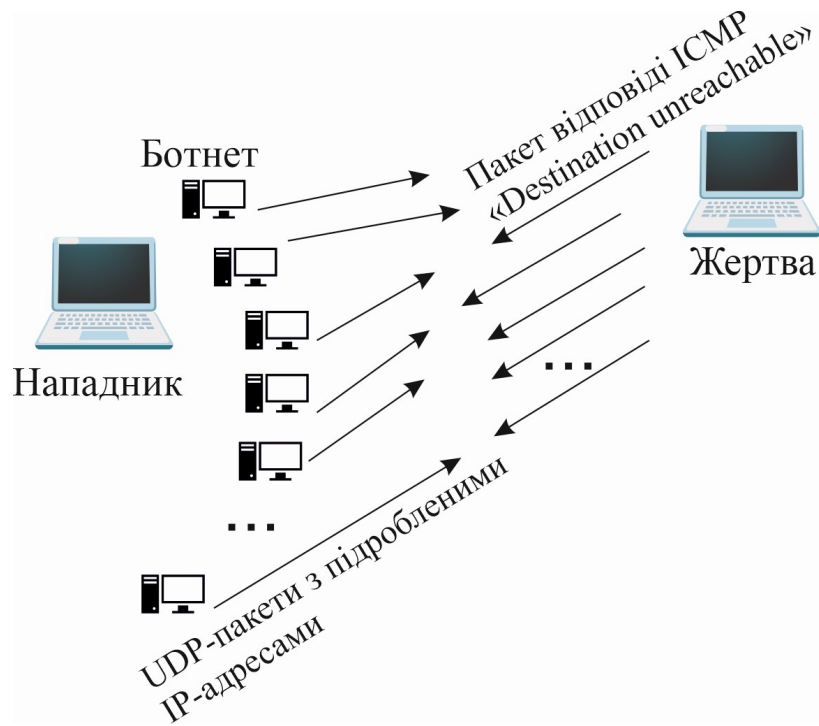


Рисунок 1.7 – Атака затоплення UDP

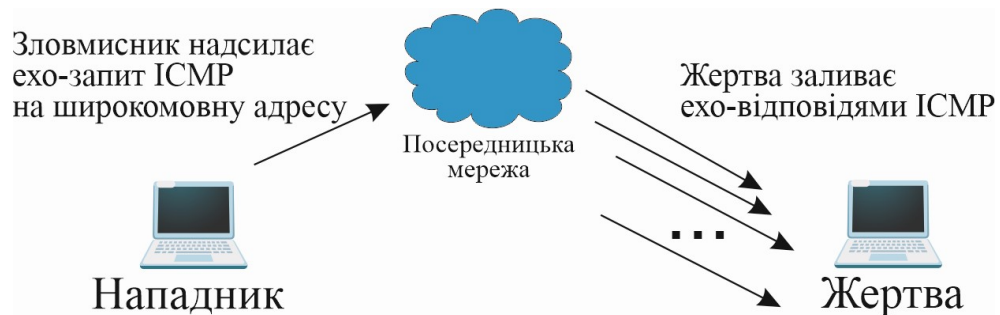


Рисунок 1.8 – Атака ICMP flood

Fraggle атака. Атака Fraggle схожа на атаку Smurf і на сьогодні також застаріла [40]. Він надсилає пакети UDP\_ECHO мережевим підсилювачам для флуду пропускної здатності жертв або може надіслати його до певного порту для створення нескінченного циклу. Атаки Smurf і Fraggle також відомі як атаки посилення, які використовують рефлектор(и) як засоби запуску атак. Будь-який IP-хост, який повертає пакет у відповідь на отриманий пакет, відомий як рефлектор. Таким чином, маршрутизатори, DNS-сервери або веб-сервери є прикладами рефлекторів. Ці рефлектори запускають атаку,

надсилаючи відповіді жертві як відповідь на отримані пакети, які містять підроблену IP-адресу джерела як IP-адресу жертви. Рефлектори використовують власні законні IP-адреси, тому їх можна виявити. Однак зловмисник, який залучає рефлектори до атаки, залишається прихованим, оскільки він підмінив свою вихідну IP-адресу на IP-адресу жертви.

Атаки посилення. У цьому розділі ми збираємося окреслити дві дуже схожі та поширені атаки посилення: атаку посилення DNS і атаку посилення протоколу мережевого часу (NTP). Основна ідея цих типів атак полягає в тому, щоб створити велику відповідь на дуже маленький запит і спрямувати ці відповіді жертві, яка в кінцевому підсумку споживає всю пропускну здатність мережі жертви.

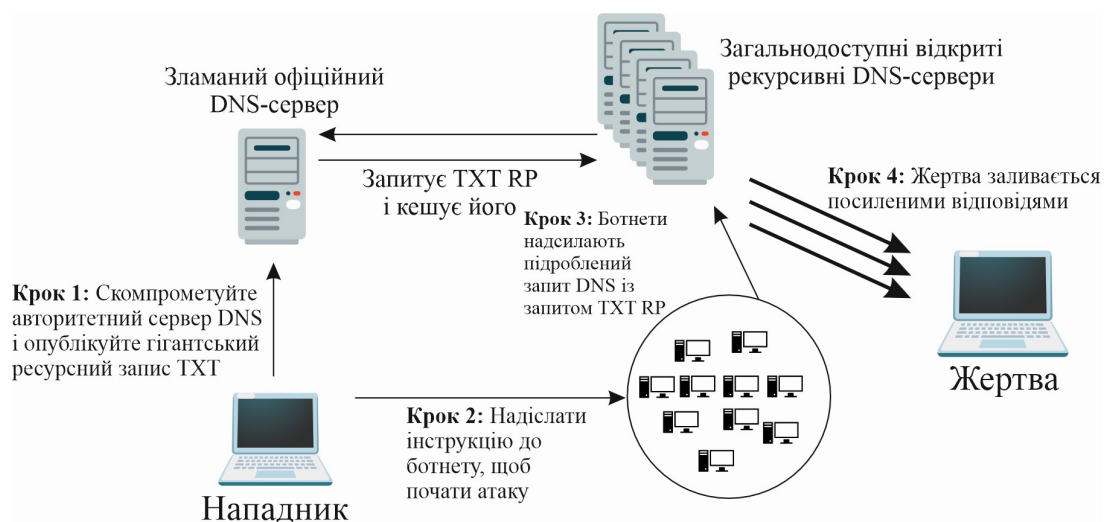


Рисунок 1.9 – Атака посилення DNS

Атака посилення DNS. Це одна з найпоширеніших атак сучасного світу, спрямована на пропускну здатність мережі жертви. Зловмисник використовує вразливі функції DNS для посилення атаки в набагато більшому масштабі [41, 42]. Ця атака також є прикладом атаки відображення, яка використовує кілька відкритих рекурсивних DNS-серверів для надсилення величезної кількості UDP-пакетів для лавинної передачі жертві. Використовуючи різні типи методів посилення, зловмисник може збільшити обсяг трафіку атаки, що може призвести до катастрофічного впливу на

найбільш безпечну систему жертви. Загальний сценарій процесу атаки такий самий, як і для всіх інших DDoS-атак: надсилання відображених відповідей на підроблену IP-адресу джерела (IP-адресу жертви) для використання пропускної здатності мережі. Загалом відповідь DNS є великою порівняно з запитом, надісланим до нього. Отже, збільшення розміру цього повідомлення відповіді споживає більше пропускної здатності, ніж у звичайній ситуації. Для цього зловмисник може скомпрометувати авторитетний сервер DNS. Рис. 1.9 ілюструє цей сценарій. Тут спочатку зловмисник використовує авторитетний DNS-сервер і, використовуючи цей сервер, розкриває значний ресурсний запис (RR) типу TXT. Цей тип TXT RR використовується в DNS, щоб зробити можливим зберігання інформації, яка раніше не була класифікована [43]. Це може включати ім'я хоста, ім'я сервера або деяку інформацію про сервер або центр обробки даних. Зловмисник маніпулює цим записом, щоб збільшити розмір повідомлення. Потім зловмисник запускає атаку через ботнет і дає йому вказівку надсилати запити до відкритих рекурсивних серверів DNS і запитувати великі повідомлення. Після обробки запитів відкриті DNS-сервери надсилають розширені відповіді на підроблену адресу джерела, яка насправді є адресою жертви. Теоретично, щоб генерувати 10 Гбіт/с флуд для жертви, лише 140 Мбіт/с початкового трафіку надсилається з ботнету. Крім того, щоб посилити атаку, зловмисник може надіслати запит DNS за допомогою розширеного протоколу DNS (EDNSO). Це розширення підтримує великі DNS-повідомлення. Щоб збільшити розмір повідомлення, зловмисник також може використовувати розширення безпеки системи доменних імен (DNSSEC). Тут вони можуть застосувати деякі криптографічні функції, що збільшує розмір повідомлення. Однак, за даними US-CERT [42], більшість спостережених ними атак використовують DNS-запит «БУДЬ-ЯКИЙ». В одному запиті він повертає всю можливу відому інформацію про зону DNS. Таким чином, відповідь стає більшою, що збільшує трафік до жертви.

Атака посилення NTP. Це дуже схоже на атаку посилення DNS і використовує NTP [44]. NTP використовується для синхронізації годинників машин, підключених до Інтернету [45]. Під час DDoS-атаки зломисник надсилає команду MON\_GETLIST серверу NTP, який відповідає останніми 600 запитами, які були зроблені серверу. Таким чином, повідомлення-відповідь величезне (приблизно в 19 разів більше) порівняно з повідомленням-запитом. Зломисник підробляє IP-адресу джерела та направляє всі відповіді на комп'ютер жертви. Таким чином, ці посилені відповіді перевантажують пропускну здатність мережі жертви та перешкоджають законним користувачам потрапити на сервер.

### 1.3.3 Атака на інфраструктуру

Найбільш небезпечним типом DDoS-атак є атака на інфраструктуру. Метою цієї атаки є пошкодження важливих ключових елементів Інтернету. Таким чином, він націлений не лише на пропуску здатність мережі, але й на ресурси (пам'ять, ЦП) цільової системи. Наприклад, атака на інфраструктуру спрямована на DNS, особливо на кореневу DNS, оскільки вони є найвищими ієрархічними точками обслуговування та надають послуги всім користувачам Інтернету в усьому світі. Оскільки DNS підтримує ієрархічну структуру, атака такого типу, спрямована лише на кореневі сервери імен, не може завдати дуже серйозного впливу на Інтернет-сервіс у всьому світі. Зазвичай зломисники використовують методи DNS-затоки для запуску атаки. Під час атаки DNS-затоки ботнет надсилає звичайні UDP-запити на сервер DNS. Однак кількість таких запитів настільки величезна, що вона переповнює систему і врешті-решт витрачає всі ресурси. Таким чином, система відхиляє всі законні запити протягом значного часу. 21 жовтня 2002 року було розпочато атаку на інфраструктуру, спрямовану на всі 13 корневих серверів

імен [46]. Ця атака не виявилася дуже успішною, але запровадила атаки такого типу. Рівно через 14 років, 21 жовтня 2016 року, найбільша DDoS-атака була спрямована на велику інфраструктуру, відому як Dyn DNS. Ця система надає послугу визначення адреси DNS більш ніж 3500 підприємствам, серед яких також деякі відомі організації, такі як Netflix, Twitter, LinkedIn тощо [47]. Він надає високопродуктивні послуги з керованою інфраструктурою DNS, яка включає численні центри обробки даних, розташовані на багатьох континентах та має здатність аналізувати 3 мільярди точок даних на день. Згідно з джерелом Dyn, щомісяця 50 значних DDoS-атак виявляють і пом'якшують досвідчені експерти DNS Dyn. Однак іронія полягає в тому, що під час жовтневої DDoS-атаки ця високопродуктивна система вийшла з ладу на значний проміжок часу. Зловмисники залучили до цієї атаки мільйони погано захищених пристроїв IoT, які не є потужними комп'ютерами, а деякими інтелектуальними пристроями, такими як розумний холодильник, веб-камери та цифрові відеореєстратори (DVR) [48]. Таким чином, це створює значну загрозу в сучасному світі кібербезпеки. Це пов'язано з тим, що на даний момент кількість пристроїв IoT становить 28,4 мільярда, і це число надзвичайно швидко зростає [49]. Повідомлялося, що для зараження цієї величезної кількості пристроїв використовується зловмисне програмне забезпечення ботнету з відкритим кодом Mirai. Це зловмисне програмне забезпечення призначене для зараження пристроїв IoT і запуску DDoS-атак на основі вказівок зловмисника [50]. Нарешті, ця атака знову підкреслила необхідність глобального спільного вирішення загроз сучасного світу.

### 1.3.4 Атака нульового дня

Атака нульового дня відбувається в день 0 з використанням невідомих лазівок або вразливостей безпеки. Його називають нульовим днем, оскільки вразливі місця системи відомі на перший день після атаки. Різні організації безпеки або приватні фірми, що займаються програмним забезпеченням, пропонують стимули та винагороди за повідомлення про вразливості нульового дня [51]. Вплив і ознаки цього типу атак також невідомі, доки атака не буде розпочата.

## 2 ПРОТИДІЯ DDOS-АТАКАМ

### 2.1 Запобігання DDoS-атакам

Запобігання DDoS-атакам є найбільш бажаною технікою захисту для боротьби з ними. В основному, як згадувалося в попередньому розділі, DDoS-атаки становлять величезну загрозу для ресурсів жертви (ЦП, пам'ять), а також для пропускної здатності мережі та інфраструктури. Таким чином, якщо атака вже була запущена і стала успішною, вона може завдати значної шкоди системі жертви. Таким чином, захист від DDoS-атак більш ефективний проти DDoS-атак, оскільки він забезпечує запобігання трафіку DDoS-атаки, а також керує великим навантаженням атаки, перш ніж це може призвести до успішної атаки. Це забезпечує нормальну роботу жертви.

DDoS-атаки стали дуже поширеними в сучасному кіберсвіті. У підсумковому звіті Akamai за четвертий квартал повідомляється, що в середньому ціль може зазнати 30 DDoS-атак на квартал, а також від трьох до п'яти атак на день [52]. Звіт про дослідження опублікований у 2012 році дослідником безпеки та захисту даних Ponemon Institute [53] показує, що середня вартість 1 хвилини простою в результаті DDoS-атак становила приблизно 22 000 доларів США, та може коливатися від 1 до 100 000 доларів США. Ці статистичні дані показують величезну потребу методів захисту від DdoS-атак. Надамо вичерпний підсумок усіх важливих методів профілактики, щоб побачити їх ефективність і засоби виправлення. В аналізі будемо дотримуватися класифікації, показаної на рис. 2.1.

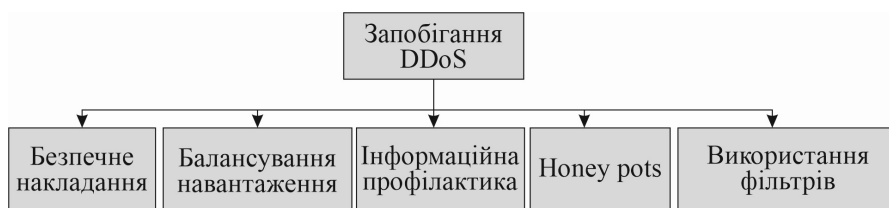


Рисунок 2.1 – Запобігання DdoS-атакам

### 2.1.1 Профілактика за допомогою фільтрів

Щоб запобігти трафіку атак, дуже важливо відфільтрувати їх. Методи фільтрації головним чином допомагають жертві запобігти від такої, а також від того, щоб вона стала несвідомим зловмисником. По суті, до маршрутизаторів застосовуються всі методи фільтрації, які гарантують, що лише законний трафік може отримати доступ до системи. Розглянемо різні методи фільтрації, а також їхні успіхи та невдачі в запобіганні DDoS-атакам.

Фільтр входу/виходу. Дуже поширеною і добре відомою технікою фільтрації є фільтрація входу/виходу. Ці методи запобігають потраплянню трафіку з підробленими IP-адресами в захищену мережу. По суті, вхідна фільтрація фільтрує зловмисний трафік, спрямований до локальної мережі, а вихідна фільтрація відкидає шкідливий трафік, що виходить із локальної мережі. Вхідна фільтрація, визначена в RFC 2267 [54], дозволяє входити в мережу трафіку, який відповідає попередньо визначеному діапазону доменних префіксів мережі. Таким чином, якщо зловмисник використовує підроблену IP-адресу, яка не збігається з префіксом, вона скидається в маршрутизаторах. Таким чином, ці методи фільтрації забезпечують запобігання значній кількості DDoS-атак, у яких використовується підроблена IP-адреса. Однак це не є корисним механізмом у випадках, коли дійсні IP-адреси ботнетів використовуються як вихідні IP під час атаки. Крім того, успіх цієї фільтрації залежить від знання діапазону очікуваних IP для порту, що не завжди досяжно для складних топологій, що використовуються в різних мережах. Крім того, якщо зловмисник використовує деякі підроблені IP-адреси, які потрапляють у дійсний діапазон адрес, фільтри в маршрутизаторах не можуть виявити зловмисний трафік у таких випадках. Знову ж таки, для цих фільтрів tunneling потрібне для мобільних IP-користувачів, щоб маршрутизатори не фільтрували їх за допомогою фільтрації входу/виходу. Нарешті, оскільки він не забезпечує стимулів для провайдерів, він частково розгортається в мережах. Іншими словами, багато провайдерів не застосовують цей підхід.

Марсіанська фільтрація адрес і перевірка вихідних адрес. Фільтрування марсіанських адрес визначено в RFC 1812 і працює для фільтрації підроблених IP-адрес, які генеруються з обмеженого набору адрес [55]. Ця фільтрація гарантує, що маршрутизатор не повинен пересилати будь-які пакети, які мають недійсну IP-адресу джерела або призначення. Ці недійсні IP-адреси варіюються від зарезервованих або спеціальних IP-адрес, а також нерозподіленого діапазону IP-адрес. Це також гарантує, що будь-який пакет із IP-адресою призначення 255.255.255.255/32 має бути відкинутий на маршрутизаторі.

Перевірка адреси джерела також вказана в RFC 1812, який також реалізовано в маршрутизаторах. У цій фільтрації маршрутизатор порівнює адресу джерела пакета з логічним інтерфейсом пакета, де він отриманий. Якщо цей інтерфейс не збігається з інтерфейсом, через який пакет повинен досягти вказаної адреси джерела, маршрутизатор відкидає пакет. Таким чином, він може фільтрувати пакети з підробленими вихідними IP-адресами. Однак рівень помилкових спрацьовувань може стати високим для асиметричних маршрутів Інтернету. Ця асиметрична природа не гарантує збіг інтерфейсів після отримання або повернення пакета з певної адреси джерела. Таким чином, це фільтрування може відхилити велику кількість законного трафіку. Крім того, істотна проблема полягає і в тому, що не всі маршрутизатори в Інтернеті реалізують ці підходи.

Фільтрація пакетів на основі маршруту. Фільтрація пакетів на основі маршруту (RPF) фільтрує пакети з підробленими вихідними IP-адресами. Ця техніка фільтрації збільшує сферу вхідної фільтрації, надаючи послуги основним маршрутизаторам [56]. Він забезпечує фільтрацію на основі інформації про маршрут пакета в кожному каналі основного маршрутизатора. Це залежить від принципу, згідно з яким кожна ланка основного маршрутизатора приймає трафік лише з обмеженої кількості вихідних адрес. Таким чином, IP-пакет, який має адреси джерела, відмінні від цього набору адрес, відхиляється основними маршрутизаторами, оскільки він виглядає підробленим для маршрутизатора. Щоб реалізувати цю техніку, потрібна інформація про топологію маршрутизації Border Gateway Protocol (BGP). Згідно з моделюванням в роботі [56] значний успіх такої

техніки буде досягнутий, якщо 18% автономної системи (AS) реалізує саме цю техніку фільтрації. Однак цей підхід вважається непрактичним у поточному Інтернет-сценарії. Крім того, щоб включити адреси джерела в повідомлення BGP, потрібно змінити схему, яка використовується в обміні повідомленнями BGP. Це збільшує розмір повідомлення, а також час обробки повідомлень BGP. Крім того, якщо маршрутизатори не зберігають оновлену інформацію, ця техніка може відкидати легітимні пакети через небажані кореневі зміни (через збій зв'язку, зміну політики тощо). Крім того, оскільки RPF фільтрує пакети на основі інформації про обмін повідомленнями BGP, зломисник може ошукати кореневу інформацію, а також правила фільтрації, викравши сеанси BGP. Нарешті, зломисник може ретельно вибрати IP-адреси, які не схожі на підроблені IP-адреси. Це може зробити метод неефективним для захисту від DDoS-атак від підроблених IP-адрес. В [57] розширюють ідею роботи [56] шляхом розробки механізму фільтрації пакетів, який розглядає повідомлення про оновлення локальних BGP для фільтрації підроблених IP-адрес. Цей метод легко розгорнути на поточній архітектурі, яка базується на протоколі маршрутизації BGP. Це також зменшує рівень помилкових спрацьовувань і спрощує процес відстеження IP-адреси.

*Протокол перевірки дійсності адреси джерела.* Протокол Source Address Validity Enforcement (SAVE) є вдосконаленням раніше згаданого RPF [58]. Він змушує маршрутизатори надсилати повідомлення, що містять оновлену інформацію про джерело, кожному маршрутизатору призначення, підключеному до джерела. Потім кожен маршрутизатор оновлює свою таблицю пересилання поточною інформацією та використовує її для фільтрації пакетів на основі методів RPF. Таким чином, він долає проблему асиметричного та динамічного характеру Інтернету, яка виникає в RPF. Однак реалізація такого протоколу вимагає зміни в існуючому протоколі маршрутизації, що є трудомістким процесом. Крім того, часткове розгортання протоколу не гарантує повного успіху у фільтрації підроблених IP-адрес.

Фільтрування кількості стрибків. Фільтрація кількості переходів також фільтрує пакети з підробленими IP-адресами [59]. У цьому методі автори

використали концепцію про те, що неможливо змінити кількість переходів IP-пакету, коли він переміщається від джерела до пункту призначення. Тому автори використовували цей підрахунок для визначення дійсності пакета. У цьому методі значення часу життя (TTL) використовується для підрахунку кількості переходів. Ця кількість переходів зберігається в таблиці відображення для кожної адреси джерела. Після отримання пакета кількість переходів, необхідних для цього пакету, обчислюється та порівнюється з таблицею відображення. Пакет визначається як підроблений, якщо під час цього порівняння виявлено невідповідність. Якщо потік пакетів визначається як потік підроблених пакетів, фільтр відкидає ці пакети для запобігання атаці. Розгортання такої техніки простіше, оскільки вона вимагає впровадження в систему жертви. Однак він має серйозні обмеження в процесі підрахунку стрибків. Оскільки цей метод підраховує кількість переходів на основі TTL, у цьому методі кількість хибних спрацьовувань більша. Це має місце тому, що початкове значення TTL зазвичай різне для різних операційних систем. Крім того, зломисник може підробити дійсну кількість переходів у своїх пакетах, що дозволить пакетам пройти фільтр. Нарешті, для потоку зломисних пакетів система не може виконати обчислення та порівняння, тому стає жертвою атаки.

Фільтрування на основі історії. Це ще один механізм фільтрації на основі маркування пакетів, у якому історія звичайного трафіку використовується для фільтрації зломисного трафіку [60]. У цьому методі адресат атаки підтримує базу даних IP-адрес. Ця база даних містить IP-адреси, які зазвичай зустрічаються в пунктах призначення. Таким чином, коли атака на пропускну здатність спрямована на цю систему, система дозволяє лише ті IP-адреси, які з'являються в їхній базі даних, і відкидає всі інші IP-пакети. Однак, якщо зломисник може імітувати свій трафік атаки як звичайний трафік, ця техніка фільтрації не зможе успішно виявити та відхилити шкідливий потік.

Ідентифікатор шляху. Метод ідентифікатора шляху (Pi) відфільтровує пакети на основі ідентифікатора шляху, який визначає шлях зломисника [61]. Це детермінований підхід, коли кожен пакет маркується ідентифікатором на основі шляху, який він пройшов. Пакети, які проходять по одному шляху, містять

однаковий ідентифікатор. Таким чином, якщо жертва може ідентифікувати пакет, що йде від зловмисника, вона може відфільтрувати всі наступні пакети, надіслані зловмисником. Однак цей механізм добре працює, коли половина маршрутизаторів задіяна для позначення пакетів. Крім того, оскільки він працює з невеликим полем ідентифікації, залишається ймовірність того, що різні шляхи відображатимуть однакову інформацію про шлях. Таким чином, це збільшує ймовірність хибнопозитивних і хибнонегативних результатів.

Пізніше в роботі [62] було запропоновано покращену версію методу *Pi* під назвою *StackPi*, яка покращує продуктивність *Pi* з точки зору поступового розгортання. Крім того, покращений механізм фільтрації здатний виявляти шкідливі потоки лише на основі одного пакета. На думку авторів, цей метод може забезпечити розумну кількість DDoS-захисту тільки в тому випадку, якщо 20% роутерів реалізують таку схему маркування. Однак цей метод не розглядає виявлення підроблених IP-пакетів, а позначає та фільтрує шкідливий пакет на основі детермінованого механізму маркування пакетів. Крім того, хосту або маршрутизатору, який шукає інформацію про шлях за допомогою цього методу, може знадобитися певне допоміжне програмне забезпечення, а також витрати на обробку, які є перешкодами для розгортання цього методу [63].

*PacketScore*. Це метод проактивної фільтрації, який використовує теорему Байєса для обчислення умовної легітимної ймовірності (CLP) [64]. Цей CLP використовується для визначення ймовірності законного пакета на основі значення базового профілю та значення атрибута пакета. Фільтрування пакетів працює на основі цього значення CLP і динамічного порогу. Оскільки фільтрація враховує статистичний аналіз, цей метод добре працює для нових сигнатур атак, а також для непідробленого трафіку атак. Однак цей метод потребує великого обсягу пам'яті для боротьби зі зростаючою кількістю атрибутів атак. Пізніше в роботі [65] було запропоновано метод під назвою *ScoreForCore*, який працює на основі механізму *PacketScore*, але вводить ефективну властивість для вибору відповідних атрибутів поточних атак. Однак цей метод вимагає співпраці для збору інформації про мережу.

### 2.1.2 Створення накладної мережі

Це ще один запобіжний механізм проти DDoS, який захищає підмножину мереж [66, 67]. Ідея цього методу полягає в тому, щоб створити накладену мережу поверх мережі IP. Ця накладена мережа є точкою входу для зовнішньої мережі для встановлення зв'язку із захищеною мережею. Передбачається, що ізоляція може бути досягнута, якщо захищена мережа приховує свої IP-адреси або використовує розподілений брандмауер. Цей брандмауер гарантує, що лише довірений трафік із вузлів накладеної мережі може отримати доступ до захищеної мережі. Хоча цей механізм забезпечує запобігання DDoS-атакам, він застосовний до приватної мережі та не підходить для публічного сервера.

### 2.1.3 Імітування законної мережі

Honeypots. Honeypot/honeynet — цікавий механізм запобігання DdoS [68, 69]. Тут honeypots/honeynets — це деякі менш безпечні системи, які приваблюють зловмисників атакувати їх. Honeynet імітує законну мережу, щоб обдурити зловмисника, щоб зловмисник подумав, що він атакував справжню систему. Таким чином, фактична система залишається захищеною. Використовуючи honeypot, можна не тільки отримати важливу інформацію (записи про дії атаки, інструменти та програмне забезпечення, що використовується для атаки) про зловмисника. Ця інформація далі використовується для виявлення та запобігання DDoS-атаки та її зловмисника. Однак ця техніка також має деякі недоліки. Наприклад, статична та пасивна природа honeypots/honeynets не забезпечує повного маскуванню від зловмисника. Крім того, якщо honeypot/honeynet не може виявити атаку за допомогою своїх інструментів виявлення на основі сигнатур, пакети атаки пересилаються фактичному адресату.

#### 2.1.4 Балансування навантаження

Це підхід, який намагається збалансувати навантаження різних систем, щоб жодна система не була перевантажена [70]. Результат балансування навантаження допомагає отримати оптимальну продуктивність, а також максимальний час безвідмовної роботи. У випадках, коли сервер стикається з DDoS-атакою, балансувальник навантаження забезпечує стійкість, оскільки він перенаправляє трафік на інші активні та неатаковані сервери. Щоб забезпечити максимальне балансування навантаження, потрібне збільшення пропускну здатності для всіх критичних з'єднань. Також потрібна значна кількість реплікованих серверів і центрів обробки даних, щоб забезпечити усунення збоїв в одній точці. Це також допомагає зменшити поверхню атаки та створює труднощі з вичерпанням наявних ресурсів і насиченням зв'язку.

#### 2.1.5 Профілактика, заснована на обізнаності

Останні DDoS-атаки, переважно DDoS-атаки на основі бот-мережі IoT, вимагають обізнаності користувачів IoT. Це тому, що пристрої IoT дуже ненадійні з точки зору безпеки. Крім того, деяким DDoS-атаки можна запобігти, якщо звичайний користувач вживе профілактичних заходів у власній системі. Це не тільки гарантує їх безпеку від нападу, але й від того, щоб стати ботом. Нижче наведено деякі ініціативи з боку користувачів, які можуть допомогти запобігти DDoS-атаці.

Зміна IP-адресу. У цій техніці комп'ютерна система змінює свою IP-адресу, щоб зробити стару адресу недійсною, яка може бути потенційною метою DDoS-атак [71]. Цей процес успішний, якщо атака здійснюється на основі IP-адреси. Однак це також спричиняє багато накладних витрат, наприклад оновлення іншої інформації

про введення. Цей метод працює успішно, доки зломисник не отримує інформацію про нову IP-адресу.

Відключення незвичних служб. Це підхід для запобігання DDoS-атакам. Деякі служби, такі як UDP echo, служби генератора символів, можуть викликати загрози DDoS-атак. Таким чином, відключення таких служб може захистити систему від деяких типів DDoS-атак. Крім того, щоб запобігти створенню ботнетів IoT, рекомендується вимкнути опції віддаленого доступу (Telnet і SSH) до систем IoT [50].

Застосування патчів безпеки. Також необхідно регулярно оновлювати всі патчі безпеки, щоб переконатися, що система не заражена помилками або хробаками. Крім того, щоб запобігти створенню ботнету IoT, обов'язково потрібно змінити стандартні або загальні паролі пристроїв IoT [72]. Це важливе усвідомлення користувачів, які можуть боротися з масовими DDoS-атаками на основі Інтернету речей. Однак іронія полягає в тому, що більшість користувачів пристроїв IoT не знають про загрози або навіть не знають назви DDoS-атак. Коли зломисник компрометує пристрій для армії ботів, користувач пристроїв не помічає жодних змін у їх продуктивності чи поведінці. Таким чином, непомітно вони допомагають в атаці, навіть не знаючи назви атаки, в якій беруть участь.

## 2.2 Захист від DDoS-атак

Запобігання DDoS-атакам є частиною захисту від них. Цей підхід є дуже важливим для захисту від значної кількості DDoS-атак. Проте, все ще залишаються загрози DDoS-атак з новою сигнатурою атаки та виправленнями. Таким чином, наступний етап захисту, який є засобом пом'якшення DDoS, описаний у великій кількості статей. Пом'якшення DDoS-атак складається з трьох різних механізмів: механізмів виявлення, механізмів реагування та механізмів терпимості, як показано на рис. 2.2.

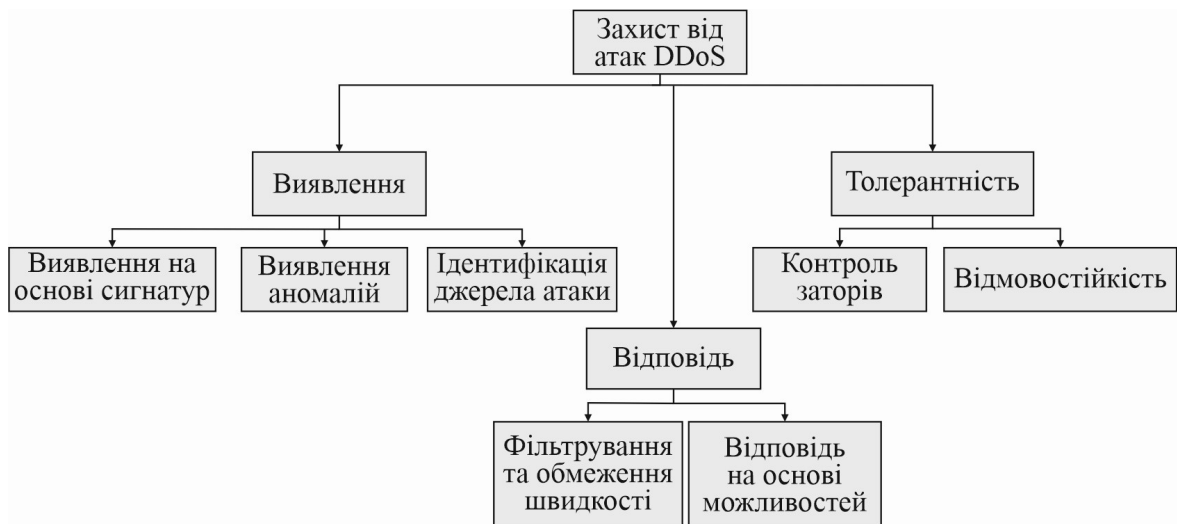


Рисунок 2.2 – Захист від атак DDoS

### 2.2.1 Виявлення

Виявлення атаки є важливим кроком до пом'якшення DDoS. Виявлення дуже просте, оскільки продуктивність служби або системи різко погіршується під час атаки. Однак завжди складно відрізнити зловмисні потоки від легальних. Іноді відповідь вимагає виявлення зловмисних подій, тоді як інша вимагає ідентифікації джерела атаки. У літературі зустрічаються дві різні методики виявлення шкідливих потоків: виявлення на основі сигнатур і виявлення на основі аномалій. З іншого боку, методи ідентифікації джерела атаки також важливі для визначення джерела атаки.

Виявлення на основі сигнатур. Механізми виявлення на основі сигнатур покладаються на відомі атаки DDoS для визначення сигнатур атак, які відрізняють звичайний трафік від зловмисного [73]. Таким чином, вони успішно виявляють відомі DDoS-атаки. Однак будь-які варіації вже існуючих атак залишаються непоміченими цими механізмами виявлення. Крім того, оскільки методи не знають про нові сигнатури, вони не працюють для будь-яких нових типів атак, які не були

помічені раніше. Обговоримо деякі добре відомі механізми виявлення на основі сигнатур.

Механізми виявлення на основі сигнатур Bro (Zeek). Це система виявлення вторгнень у мережу в реальному часі, яка працює, відстежуючи мережевий трафік зловмисника [74]. Він містить багато потужних функцій, таких як мова підписів на основі регулярних виразів, надійний підхід до виявлення атак, можливості розширення для нових подій. Однак він може постраждати від атак DoS, які використовують складні алгоритми. Крім того, йому потрібно створити свій підпис атаки, а також сценарії для обробки його події вручну. Тому в таких випадках важливо залучати досвідченого адміністратора.

Кореляція змінних трафіку інформаційної бази управління. Цей метод аналізує змінну трафіку інформаційної бази керування (MIB), щоб знайти сигнатури атаки[75]. На основі триетапного методу вилучення сигнатур витягується набір сигнатур атаки. Виходячи з цього, відстежуваний трафік визначається як атакуючий трафік або законний трафік. Ця техніка може виявити статистичні порушення, характерні для пакетів TCP, UDP і ICMP, які беруть участь у DDoS-атаках. Однак точність виявлення методу вважається мінімальною, якщо цей метод оцінюється в середовищі з контрольованим трафіком. Крім того, цей метод не застосовний до всього Інтернету.

SNORT. SNORT є дуже популярним інструментом виявлення мережевих вторгнень [76]. Це легкий інструмент на основі правил для виявлення широкого спектру атак і зондів. Щоб збільшити діапазон виявлення атак, він поєднав виявлення на основі сигнатур і захист на основі аномалій. Однак, оскільки SNORT залежить від точної відповідності шаблону, це може стати вузьким місцем у продуктивності системи за великого трафіку, а також швидкості Інтернету.

Спектральний аналіз. Наведені тут методи виконують спектральний аналіз, щоб відрізнити трафік атаки від звичайного трафіку. Наприклад, у роботі [77], спектральна щільність потужності пакетів використовується для виявлення потоку атаки. Крім того, інший підхід зустрічається в роботах [78, 79], де виконується спектральний аналіз для класифікації характеристик трафіку атаки.

Виявлення аномалій. Механізм виявлення аномалій може обробляти атаки з новими сигнатурами, а також нові атаки [80]. Однак вибір порогового значення для розрізнення трафіку атаки від звичайного трафіку є відкритою проблемою для цих методів [81]. Проаналізуємо деякі популярні методи виявлення аномалій.

MULTOPS. Багаторівневе дерево для онлайн-статистики пакетів (MULTOPS) — це метод виявлення атак на основі дерева, спеціально розроблений для виявлення атак переповнення пропускної здатності [82]. Цей метод виявляє трафік атаки на основі непропорційності швидкості пакетів. Кожного разу, коли швидкість передачі пакетів у підмережі досягає свого порогового значення, MULTOPS створює новий підвузол. Це забезпечує стабільну швидкість відстеження пакетів. Однак передбачається, що швидкість вхідного та вихідного трафіку пропорційна, що не є практичним припущенням для сучасних потоків мультимедійних повідомлень. Таким чином, ця методика може мати високий рівень хибнопозитивних результатів. Крім того, зломисник може націлитися на MULTOPS за допомогою атаки на виснаження пам'яті. Нарешті, в [83] запропоновано вдосконалений метод порівняно з MULTOPS. У цьому методі використовується структура даних, яка називається табличною онлайн-статистикою пакетів (TOPS), яка є більш ефективною, ніж MULTOPS.

DWARD. DWARD — це метод виявлення DDoS-атак і обмеження швидкості, який працює поблизу джерела атаки [84]. Він також виявляє аномалії на основі статистики трафіку, отриманої від вихідних периферійних маршрутизаторів під час фази моніторингу, і специфікації мережевого трафіку в додатку та транспортному протоколі. На основі цієї інформації він застосовує динамічне обмеження швидкості до трьох різних категорій трафіку: законного, підозрілого та атакуючого трафіку. Однак цей метод також може помилково класифікувати законний трафік як підозрілий або атакуючий. Крім того, оскільки цей метод працює поблизу джерела атаки, необхідно широко розгорнути метод. Однак це розгортання не забезпечує жодних стимулів для операторів мережі.

Інші методи. Крім того, у літературі можна знайти багато інших методів [85, 86], які намагаються відрізнити трафік атаки від легального трафіку на основі

аналізу та виявлення аномалій у потоках трафіку. В [87] запропоновано метод виявлення аномалій у поведінці користувачів у веб-переглядачі на основі прихованої напівмарковської моделі. Цей метод працює для виявлення DDoS-атак прикладного рівня на основі поведінки користувачів у веб-переглядачі. Однак цей метод не може впоратися з атаками, які здійснюються динамічною веб-сторінкою, або він не може належним чином виявити атаку, якщо атака слідує за поведінкою проксі-серверів. У роботі [88] представлено метод виявлення атак з низькою швидкістю на основі інформаційних показників. Це також метод виявлення DdoS- атак на основі аномалій, який працює краще, ніж метрика Шеннона або методи розбіжності Кульбака-Лейблера. Крім того, документ містить механізм відстеження IP-адреси, який здатний виявляти атаку та злоумисників, а також може фільтрувати трафік атак. Однак для цих методів важко працювати з мережевим характером атаки. Пізніше в [89] було реалізовано метод виявлення відхилень у загальномеревому трафіку за допомогою аналізу домену трансформації. По суті, вони виявили аномалію на основі аналізу топологічної інформації мережі, а також трафіку всієї мережі. Крім того, вони застосували аналіз часових вікон, який зменшує витрати на обчислення та підвищує ефективність виявлення. Крім того, у роботі [90] запропоновано метод виявлення аномалії на основі ентропії, який використовує варіацію показника Ляпунова. У цьому методі автори розглянули наслідки IP-адрес джерела та призначення в трафіку атаки. В [91] запропоновано метод, заснований на метриці розширеної ентропії, який перевершує попередній метод з точки зору точності виявлення. Цей метод працює з меншою кількістю функцій IP-трафіку та використовує меншу кількість переходів для відстеження до локальної мережі армій ботів. Крім того, в [92] запропоновано метод, який може адаптувати порогове значення, щоб збільшити складність для злоумисника, який хоче налаштувати трафік на основі порогового значення. Для цього він відстежує поведінку хоста або систем обслуговування. Вони також врахували значення апаратного лічильника продуктивності (НРС) і статистику кореляції трафіку мережі та підходів машинного навчання. Усі вони використовуються для виявлення DDoS-атак, які досягають 99,8% точності виявлення.

Ідентифікація джерела атаки. Методи виявлення працюють для виявлення шкідливого трафіку мережевого потоку. Тому ці методи в основному працюють поблизу цілі атаки. Таким чином, якщо на стороні жертви застосовуються механізми фільтрації або реагування, це не може забезпечити мінімальний рівень хибнопозитивних результатів. Тобто існує можливість відхилити легітимний трафік для методів, які намагаються застосувати фільтрацію в мережі жертви. Таким чином, ефективніше, якщо можна визначити джерело атаки та застосувати фільтрацію або обмеження швидкості. Це забезпечить прийняття більш законного трафіку в системі. Ідентифікація джерела атаки, а також мережевого шляху трафіку атаки відома як відстеження IP.

*Імовірнісне маркування пакетів.* Ця техніка ймовірнісним чином кодує інформацію в заголовок пакета для одержувача, який використовує цю інформацію для реконструкції шляху проходження пакета. Таким чином, без будь-якого додаткового трафіку для відстеження або будь-якого зовнішнього зв'язку та підтримки, цей механізм може ідентифікувати джерело атаки за допомогою реконструкції шляху атаки. Перший метод відстеження IP, заснований на імовірнісному маркуванні пакетів, був знайдений у роботі [93]. У цьому методі маршрутизатор позначає пакет деякою частковою інформацією про шлях, який пройшов пакет. Тут ідентифікаційне поле використовується для зберігання позначки. Цей метод також можна використовувати для проведення посмертного дослідження нападу. Однак обчислювальна складність реконструкції шляху для кількох зломисників занадто велика ( $O(n^8)$  для  $n$  зломисників) для цього методу [94]. Крім того, він дає велику кількість хибнопозитивних результатів для кількох зломисників. Інший метод, подібний до попереднього, реалізовано в роботі [95]. Цей метод використовує алгебраїчні методи, щоб зробити його надійним. Таким чином, ця техніка забезпечує більшу гнучкість дизайну. Також можна відфільтрувати шум, створюваний зломисником, а також визначити та відокремити більше одного шляху атаки. Однак цей метод є менш ефективним, якщо до атак залучено багато зломисників, оскільки кількість пакетів, необхідних для реконструкції шляху атаки, збільшується квадратично зі збільшенням кількості

зловмисників. Крім того, оскільки цей метод не використовує таблицю відстаней, зловмисник може підробити маркувальну інформацію, що зрештою спричинить неправильний шлях атаки. Пізніше в роботі [96] було запропоновано дві схеми. Одна – розширена, а інша – автентифікована схема маркування. Автори врахували мінімальні накладні витрати на маршрутизацію та мережу. Метод має мінімальну обчислювальну складність і більш високу точність для масштабної DDoS-атаки в порівнянні з раніше згаданою. Також схема автентифікації забезпечує захист від підробки (з використанням скомпрометованого маршрутизатора) зловмисника. Методи працюють залежно від карти вищестоящих маршрутизаторів. Незважаючи на те, що створення або збір цієї карти є доцільним і практичним, для отримання карти потрібна певна робота в режимі офлайн або в спокійний час. В [97] запропоновано розширений метод на основі ймовірнісного маркування пакетів (PPM), який може визначити швидкість трафіку. Таким чином, на основі цієї швидкості трафіку метод може ідентифікувати вузол зловмисника, який генерує максимальний трафік. Для того, щоб покращити масштабованість механізму PPM в [98] запропоновано метод, який використовує шпур великої контрольної суми. Автори зазначили деякі переваги використання цього шпура контрольної суми. Наприклад, використання такої контрольної суми підвищує ефективність алгоритму реконструкції. Крім того, він служить асоціативною адресою та перевіркою цілісності. Це також допомагає зменшити підробку, яку може зробити зловмисник, вставляючи підроблені повідомлення, які викликають зіткнення з легітимними повідомленнями. Для того, щоб зменшити кількість пакетів для реконструкції шляху атаки, адаптивна ймовірнісна схема маркування запропонована в роботі [99]. Тут значення TTL використовується для обчислення відстані, яку подолав пакет, а також використовує цю відстань для визначення ймовірності позначення. Цей метод скорочує час реконструкції на 20% порівняно з попередніми методами. Він також захищає маркування підроблених пакетів. В [100] запроваджено схему PPM із регульованою ймовірністю, а не фіксованою на основі позицій маршрутизаторів на шляху атаки. Інша схема PPM, заснована на динамічній ймовірності та коді перетворення Лубі (LT-код) [101], також пропонується в статті для зменшення

кількості пакетів для виявлення джерела, а також колізій пакетів. В [102] пропонується метод, за допомогою якого маршрутизатори можуть адаптувати ймовірність маркування своїх пакетів. Це робиться на основі швидкості перезапису маркування пакета. Це збільшує ймовірність надходження пакетів від далеких маршрутизаторів. Таким чином, маркувальна інформація від віддалених роутерів доходить до жертви з підвищеною ймовірністю. У результаті це зменшує кількість пакетів для реконструкції зворотного шляху.

Детермінована маркування пакетів. Детермінована маркування пакетів (DPM) використовує деякі детерміновані методи для позначення пакетів маршрутизаторів, які знаходяться ближче до джерела атаки. Порівняно з методами RPM, які можуть ідентифікувати джерело атаки в основному для атак flooding (що включає величезну кількість пакетів), метод DPM може працювати для атак, що включають невелику кількість пакетів [103]. Ця схема також зменшує витрати на зберігання та обчислення, пов'язані зі схемами RPM на сайті жертв. Першу схему DPM запропоновано в [104]. Основна ідея полягає в тому, щоб вставити IP-адресу початкового маршрутизатора в пакет. У своєму методі автори розглядають інтерфейси як їхні атомні одиниці трасування. Таким чином, він може розділяти вхідні та вихідні пакети і таким чином може по-різному обробляти пакети для різних напрямків. Це також покращує випадки підробки позначок, забезпечуючи маркування всіх пакетів, що проходять через мережу. Таким чином, піддроблена позначка буде перезаписана правильною позначкою. Цей початковий метод не може ідентифікувати кількох зломисників. Щоб вирішити цю проблему, пізніше автори запропонували метод відстеження кількох зломисників [105]. Тут вони представили хеш-функцію, яка створює хеш-значення для вхідних адрес. Це хеш-значення використовується жертвою для визначення правильної інформації про позначку. У роботі [106] запропоновано метод покращення продуктивності методу DPM. Тут поле розмітки розділено на дві частини: інформаційну та індексну. Інформаційний розділ містить фрагмент адреси або значення кореляційної функції. Автори запровадили ефективні методи зберігання даних в інформаційному розділі. В [107] запропоновано гнучку схему DPM. Підхід «гнучкої довжини позначки» зробив його

придатним для різних мережевих середовищ. Він також містить схему запобігання перевантаженню для відстеження IP-адрес. Встановлено, що продуктивність методу краща, ніж інші методи DPM. В [108,109] запропоновано схему маркування на вимогу (MOD) на основі DPM, яка покращує масштабованість існуючих методів DPM. Цей метод динамічно позначає кодування трасування та може виявляти всі джерела атак. Однак сервер MOD, який вони використовували у своєму методі, може стати ціллю DDoS-атаки. Крім того, оскільки база даних MOD містить великий набір інформації про атаку, ефективність отримання інформації з цієї бази даних стає проблемою для користувачів.

Повідомлення відстеження ICMP. У цьому методі повідомлення ICMP (iTrace Packet) генерується в кожному маршрутизаторі та надсилається одержувачу, що допомагає відстежити джерело атаки [110]. Щоб зменшити навантаження на одержувача, йому надсилається регульоване повідомлення зворотного зв'язку з низькою ймовірністю (не більше 1/1000). Таким чином, цей простий і легкий метод може допомогти одержувачу відстежити джерело атаки. Однак цей метод створює додатковий трафік і потребує цифрового підпису для забезпечення цілісності повідомлення відстеження. В [111] запропонували вдосконалення iTrace під назвою (iTrace -CP), яке передає інформацію про весь шлях у своєму повідомленні ICMP. Таким чином, якщо жертва може ідентифікувати пакет атаки, вона може побудувати весь шлях/граф атаки. Однак цей метод вимагає деяких змін у маршрутизаторі для обробки, а також вимагає додаткового розгляду місця для зберігання в пакеті. Щоб підвищити точність виявлення джерела атаки, коли законний користувач також використовує той самий шлях, який використав зловмисник, у роботі [112] модифікували керовану наміром модель iTrace. В [113] запропонували розширену версію методів відстеження. Цей метод в основному працює для атаки рефлектора та здатний безпосередньо ідентифікувати крайовий маршрутизатор, який дозволяє передавати пакети атаки. У цьому методі також використовуються потужні фільтри Блума, щоб зменшити кількість згенерованих повідомлень зворотного відстеження. Цей високомасштабований метод також може виявити атаку на ранній стадії. У роботі [114] запропоновано метод, названий пасивним відстеженням IP (PIT). Цей

метод аналізує повідомлення про помилки ICMP, які фактично створені зловмисним трафіком (підроблений трафік), а також використовує загальнодоступну інформацію, наприклад топологічну інформацію, щоб відстежити спуфер. Хоча цей метод не працює для всіх типів атак або спуферів, він може усунути вимогу розгортання для визначення місцезнаходження деяких із них.

### 2.2.2 Механізм реагування

Після виявлення трафіку або джерела атаки важливо швидко відреагувати, щоб пом'якшити атаку. Надійний механізм реагування може зменшити або усунути наслідки DDoS-атаки. Визначимо деякі дослідницькі дії щодо двох різних добре відомих механізмів реагування: фільтрації або обмеження швидкості та можливості.

Фільтрування або обмеження швидкості. Фільтрування або обмеження швидкості є одним із найбільш застосовних способів реагування на DDoS-атаки. Система застосовує ці методи на основі результатів механізмів виявлення. Загалом, якщо результати механізму виявлення виявляються частково успішними, тобто якщо він дає великі помилкові негативи або не може визначити точну межу між законним і зловмисним трафіком, доцільно застосувати обмеження швидкості, а не фільтрацію. З іншого боку, якщо механізм виявлення може успішно розрізнити потік атаки, доцільніше фільтрувати цей шкідливий трафік. Деякі загальні методи фільтрації та обмеження швидкості наведено в [115,116].

Реакція на основі можливостей. Основна техніка DDoS, яка заповнює жертву небажаним трафіком, полягає в тому, що будь-який відправник може надіслати одержувачу скільки завгодно трафіку. Одержувач не може контролювати, скільки трафіку він отримає. Існують механізми керування потоком і перевантаженістю, але відправника, це не хвилює. Таким чином, методи, задіяні у відповіді DDoS на основі можливостей, працюють, щоб знайти рішення для контролю такого неналежного поведіння відправника.

Міжпоточковий фільтр без збереження стану (SIFF) [117] і архітектура перевірки трафіку (TVA) [118] є двома прикладами методів цього типу.

### 2.2.3 Мінімізація впливу атак

Толерантність. Коли результати алгоритму виявлення виявляються невдалими або коли стає важко застосувати процес виявлення, важливо знайти альтернативи. Альтернативою цьому є механізм толерантності [119]. Техніки механізму толерантності працюють з дуже невеликим знанням або навіть без знання про результат виявлення. Таким чином, це завершальний етап захисту, коли інші етапи (запобігання та виявлення) зазнають невдачі. Таким чином, метою цього механізму є забезпечення максимально можливої якості обслуговування шляхом мінімізації впливу атаки. Дослідження, проведені в цій галузі, можна класифікувати як контроль перевантаження та відмовостійкість.

Контроль перевантаження. Основна мета атаки із затопленням пропускної здатності – перевантажити ресурс. Вплив цього типу атак можна зменшити або усунути шляхом застосування механізму контролю перевантаження. Повторний зворотній зв'язок [120] і NetFence [121] є двома прикладами механізмів, у яких для захисту DDoS-атак застосовується контроль перевантаження.

Відмовостійкість. Відмовостійкість забезпечує високу доступність системи. У відмовостійкій системі основна ідея полягає в повторенні або примноженні ресурсів системи, таких як програмне забезпечення, апаратне забезпечення. У цій галузі було знайдено кілька досліджень, які спрямовані на визначення застосовності системи відмовостійкості та її впливу на DDoS-атаки [122].

## 3 DDOS-АТАКИ НА ІНШІ СИСТЕМИ

### 3.1 DDoS-атаки на хмари

Вище були розглянуті DDoS-атаки на традиційні системи. Тепер обговоримо DDoS-атаки на нетрадиційні системи, такі як хмари, розумні мережі, розумні будинки, CPS і системи IoT.

DDoS-атаки на хмари. Хмари або хмарні обчислення — це онлайн-платформа, яка надає доступ за принципом «оплата за використання» або доступ на основі підписки до різних послуг, таких як зберігання, розробка програмного забезпечення, потокове аудіо/відео, аналіз даних, обмін файлами [123,124]. Це розподілена інфраструктура з високим ступенем масштабування, яка полегшує отримання найкращих хмарних послуг з будь-якої точки світу. Це також усуває витрати на налаштування і обслуговування інфраструктури та забезпечує автоматичне масштабування (зменшення або розширення ресурсів за вимогою), що забезпечує високу швидкість і продуктивність. Однак ця платформа також може бути мішенню для всіх типів атак, включаючи порушення даних, порушення обчислень, атаки затоплення, атаки DoS/DDoS, атаки на цілісність хмари, атаки між віртуальними машинами (VM), атаки на синхронізацію, атаки спільного проживання VM, і т. і. [125]. Наприклад, труднощі боротьби з атаками на цілісність хмари включають ненадійні хмарні сервери та обчислювальну складність деяких підходів. Нижче наведено деякі останні методи протидії атакам на цілісність хмари. У роботі [126] пропонується метод пошуку подібності для зашифрованих документів на основі simhash для пошуку схожих зашифрованих документів, що зберігаються в хмарах. У роботі [127] щоб запобігти напівчесним хмарним серверам, вміст зображення шифрується за допомогою потокового шифру для додавання водяного знака та індексується за допомогою хешу, чутливого до місцевості. У [128] запропоновано схему нечіткого ранжованого пошуку з кількома ключовими словами для пошуку на основі ключових слів над зашифрованими зовнішніми даними з перетворенням ключового слова та вагою ключового слова. У

роботі [129] шифрування з можливістю пошуку базується на схемі пошуку з урахуванням вмісту з використанням концептуальних графів із числовими векторами лінійних форм і ранжувального пошуку за кількома ключовими словами в зашифрованих хмарних даних. У [130] шифрування з можливістю пошуку базується на концептуальних графіках над зашифрованими зовнішніми даними з оцінкою речень у підсумку тексту та Tregex для вилучення тематичних речень із документів для перетворення на концептуальні графіки. У роботі [131] для протидії напівдовіреному через хмарного провайдера як третьої сторони, запропоновано структуру для обміну міськими даними шляхом використання криптографії на основі атрибутів для підтримки динамічних операцій.

Хмари також можуть бути ціллю DDoS-атак. Info Security повідомила, що в першому кварталі 2015 року одна третина послуг пом'якшення DDoS була застосована до секторів IT-сервісів/хмари/SaaS. Хмарні обчислення забезпечують автоматичне масштабування, оплату за використання, багатокористувацький обліковий сервіс, що робить його привабливим вибором для людей у всьому світі. Але в той же час ці функції також дуже корисні для успішної DDoS-атаки. У хмарній інфраструктурі хмарні сервери запускають багато віртуальних машин, щоб забезпечити обслуговування користувачів. Коли зловмисник атакує сервер, сервер може сприйняти цю ситуацію як сценарій високого використання ресурсів. Потім функція автоматичного масштабування застосовує розподіл ресурсів, міграцію або процес розміщення, щоб вирішити цю перевантажену ситуацію. Якщо цей процес продовжується, нарешті, DDoS-атака стає успішною, і ця атака накладає певний прямий і непрямий вплив на послуги та доходи. IP-спуфінг, SYN-флуд, переповнення буфера, пінг смерті та наземна атака – це деякі приклади DDoS-атак на хмарних платформах. Захист від DDoS-атак на хмари також можна організувати трьома різними способами: запобігання атак, виявлення атак і пом'якшення атак. Методи запобігання атакам включають автентифікацію у відповідь на виклик, приховані сервери або порти, методи обмеження ресурсів, коли методи виявлення атак використовують виявлення аномалій, методи виявлення BotCloud для запобігання та виявлення DDoS-атак. Крім того, також знайдено деякі методи

пом'якшення, включаючи масштабування ресурсів програмно-визначених мереж (SDN) для пом'якшення DDoS-атак на хмари.

### 3.2 DDoS-атаки на розумні мережі

Smart Grid — це еволюція традиційної електромережі до розумної інфраструктури, яка включає інформаційно-комунікаційні технології (ІКТ) у традиційні системи електропостачання [132]. Це розподілене джерело живлення з автоматизованими можливостями обслуговування та експлуатації, які покращують надійність і якість електроенергії, а також підвищують потужність і ефективність традиційних систем живлення. Для надійного доступу, обробки та доставки інформації потрібна надійна комунікаційна мережа. Ця доставка пошкоджується або переривається, коли DDoS -атака досягає успіху в інтелектуальній мережі, і, як зазначено в роботі [133] існує значна кількість атак у розумних мережах. Крім того, в інтелектуальній мережі дуже важливо забезпечити часові обмеження переданих повідомлень, оскільки це часові обмеження є еталоном для надійного моніторингу та керування системами. Це обмеження також створює загрозу для інтелектуальної мережі, оскільки основний вплив DDoS -атаки полягає в тому, щоб зробити систему недоступною для доступу, що вносить затримку в передачу повідомлень. У Smart Grid атаки DDoS можуть бути спрямовані на різні рівні зв'язку: мережевий, транспортний, контроль доступу до середовища (MAC) і фізичні рівні через затоплення або перешкоди на підстанціях. Крім того, об'єктом DDoS -атак можуть бути інтелектуальні електронні пристрої (IED) або центри диспетчерського контролю та збору даних. Таким чином, успішна атака DDoS може призвести до серйозного погіршення якості обслуговування, оскільки операції контролю та моніторингу залежать від своєчасної передачі повідомлень. Механізми виявлення та пом'якшення атак є двома основними методологіями захисту від DDoS -атак у розумній мережі. Існує багато різних методів виявлення атак, які працюють для

виявлення атак DDoS у розумній мережі. Методи виявлення на основі сигналу і виявлення на основі пакетів працюють для виявлення атак з перешкодами в мережах. Ці схеми виявлення також застосовні для пасивного виявлення DDoS -атак у бездротових додатках інтелектуальної мережі, а також для загального виявлення DDoS -атак. Крім того, методи обмеження швидкості або фільтрації на мережевому рівні працюють для пом'якшення впливу DDoS -атак у розумній мережі. Крім того, стійкі до перешкод схеми, які використовувалися в бездротовій мережі, також можна використовувати для пом'якшення атак DDoS у залежній від бездротового зв'язку інтелектуальній мережі.

### 3.3 DDoS-атаки на розумні будинки

Завдяки швидкому зростанню Інтернету та технологій наше життя з кожним днем стає розумнішим. Як наслідок, сучасний будинок вважається розумним будинком, якщо він підключений до мережі зв'язку. Використовуючи це з'єднання, мешканець будинку може контролювати та програмувати всю розумну побутову техніку (розумний холодильник, смарт-телевізор, охоронну сигналізацію тощо) з віддаленого місця. Ці розумні домашні пристрої полегшують життя та підвищують безпеку власника будинку. Але в той же час ці пристрої можуть становити величезну загрозу, якщо на них буде здійснена будь-яка кібератака. Згідно з роботою [134] безпека розумного дому залежить від шести основних властивостей: конфіденційності, цілісності, автентифікації, авторизації, невідмовності та доступності. Атака DoS/DDoS спрямована на доступність інтелектуальних пристроїв шляхом часткового або повного переривання системи зв'язку. В роботах [135,136] повідомлялося, що DDoS -атаки на смарт-телевізори призводять до зависання нормального обслуговування та роботи пристроїв. Щоб захистити розумний пристрій від DDoS -атаки, важливо забезпечити аутентифікацію системи. Таким чином можна буде блокувати неавторизовані пристрої та сервіси.

Крім того, більш загрозливим сценарієм є використання інтелектуальних пристроїв для створення ботнетів для DDoS-атак. Розумні пристрої дуже вразливі до ботів, оскільки вони є менш безпечними пристроями. Більшість пристроїв мають заводські паролі. Тому зловмисникам дуже легко взяти під контроль такі пристрої та зробити з них ботнет. Як зазначено раніше, атаку 21 жовтня 2016 року в основному здійснили деякі «розумні пристрої», зокрема камери відеоспостереження. Ця атака стосується десятків мільйонів IP-адрес, більшість із яких походять від цих інтелектуальних пристроїв. Ця атака є найбільшою (за масштабами) в історії. Оскільки ці загрози не дуже старі, на сьогоднішній день єдиний спосіб запобігти тому, щоб інтелектуальні пристрої були частиною ботнету, — це підвищити безпеку самих пристроїв, і це може бути забезпечено виробниками або кінцевими користувачами.

### 3.4 DDoS-атаки на системи IoT

IoT з'єднує мережеві об'єкти різних типів, починаючи від тостера вдома і закінчуючи пристроєм для моніторингу серця, імплантованим у тіло людини, підключеним автомобілем, інфраструктурою розумної мережі або веб-камерою комп'ютера. Таким чином, об'єкти IoT називаються «дуже неоднорідними» мережевими об'єктами. У роботі [137] Міжнародний союз електрозв'язку (ITU) згадав про своє бачення світу IoT як «технології, яка забезпечує підключення будь-чого». Автори [138] зазначили, що в 2015 році кількість підключених пристроїв стало 10-20 мільярдів, тоді як у 2003 році було лише 500 мільйонів підключених пристроїв, а через 5 років кількість підключених пристроїв зросте до 40-50 мільярдів. Цей сценарій демонструє надзвичайне зростання світу IoT, що добре і погано водночас. Це пояснюється тим, що, за даними Trend Micro, Inc. занадто багато з цих пристроїв IoT взагалі не захищені, оскільки постачальники або виробники цих пристроїв не стурбовані проблемами безпеки цих пристроїв. Крім

того, деякі виробники жорстко закодували менш безпечні облікові дані пристроїв IoT, які неможливо змінити, але їх дуже легко вгадати. У результаті за останні кілька місяців 2016 року кіберсвіт зіткнувся з одними з найбільших (за розміром) DDoS-атак у своїй історії. Усі ці атаки стосуються мільйонів IP-адрес з усіх цих інтелектуальних пристроїв. Як вже раніше зазначено, дуже важливо забезпечити безпеку пристрою за допомогою дій виробників пристрою та кінцевих користувачів. З іншого боку, оскільки пристрої IoT працюють у різних складних сферах, таких як охорона здоров'я, рятувальні служби, підключені транспортні засоби, якщо ці пристрої стикаються з DoS-атакою, може статися катастрофічна подія, якщо пристрої відмовляться спілкуватися та надавати послуги в критичних ситуаціях. Наразі аутентифікація є рішенням DoS-атак у таких пристроях. Таким чином, дуже важливо приділяти більше уваги цій галузі Інтернету, що швидко розвивається.

### 3.5 DDoS-атаки на CPS

Відповідно до роботи [139] CPS відноситься до нового покоління систем з інтегрованими обчислювальними та фізичними можливостями. Таким чином, це система майбутнього, яка працюватиме як міст між кібернетичним і фізичним світами обчислень. Основна ідея полягає в тому, щоб запровадити посилений контроль, моніторинг і координацію в різних критично важливих системах, таких як аерокосмічна, охорона здоров'я, міський автомобіль. Оскільки ця система також залежить від довіреного зв'язку, атака DDoS може створити значні загрози для доступності та обслуговування системи. Це питання постійного дослідження, яке необхідно розглянути для надійної CPS загалом.

### 3.6 Обговорення результатів

Існує багато досліджень, присвячених боротьбі з DDoS-атаками. Проте впровадження чи розробка ефективних методів і механізмів цих досліджень не може протистояти DDoS-атакам у наш час. Швидше, його частота та розмір зростають. Таким чином, також важливо визначити, чому ці дослідження захисту DDoS-атак не стають успішними в запобіганні цим загрозам.

Як відповідь на це питання можна зробити ряд тверджень. Найважливішим з них є відсутність розподіленої взаємодії між багатьма точками в мережі. Це через розподілене адміністрування Інтернету, яке не може забезпечити глобальну співпрацю. Також задіяні деякі соціально-економічні фактори, які ускладнюють впровадження методів у всьому світі. Оскільки DDoS-атаки є розподіленими атаками, розгортання в одній точці не може забезпечити найкращий захист від атак.

Окреслимо деякі інші проблеми, які потребують подальших досліджень у майбутньому. По-перше, зростання Інтернету та доступність незахищених пристроїв IoT є дуже великою загрозою для сучасного кіберсвіту. Усі останні великі атаки DDoS базуються на ботнетах IoT. Користувачі цих величезних систем не знають про безпеку своїх пристроїв. Однак головною профілактикою створення цього величезного ботнету є забезпечення безпеки пристрою з боку користувача. Забезпечення захисту від DDoS-атак на основі IoT є надзвичайно важливою галуззю досліджень, де існує багато різних невирішених проблем, які потребують особливої уваги. Запобігання створенню бот-мереж IoT, виявлення та відхилення потоків від нескладних пристроїв IoT (таких як камери безпеки, інтелектуальний холодильник, домашні маршрутизатори) є прикладами проблем, які потребують додаткових досліджень.

По-друге, також складно підтримувати компроміс між ефективністю методів захисту онлайн (у реальному часі) та споживанням ресурсів жертви. Оскільки DDoS-атаки вже створюють величезний тиск на ресурси (обчислювальну потужність, пам'ять, пропускну здатність) системи жертви, дуже важливо

забезпечити найкращу ефективність методів захисту від DDoS. Тобто, важливо забезпечити мінімальне споживання ресурсів жертви механізмами захисту під час боротьби з DDoS. Це надзвичайно важливий напрямок досліджень, оскільки найкраще ефективні механізми захисту забезпечують мінімальний час простою, а також мінімальні втрати прибутку з боку жертви.

По-третє, масштабованість — ще одна проблема, виявлена в дослідженнях DDoS-атак. Вони включають різні сценарії та сигнатури атак. Тому дослідники намагаються забезпечити найкращий можливий захист, враховуючи різні аспекти атак. Дуже важливо перевірити ефективність цих досліджень у реальному житті. Крім того, важливо перевірити продуктивність у реальному часі, коли різні методи співпрацюють один з одним, оскільки різні методи працюють над вирішенням проблеми з різних сторін. Сценарій атаки в реальному житті дуже відрізняється від середовища тестування, яке працює на основі певного фіксованого набору даних і фіксованих сигнатур атаки. Тому важливо забезпечити масштабованість механізмів захисту в сценаріях атак у реальному часі.

По-четверте, забезпечення захисту від атаки нульового дня завжди є відкритою дослідницькою проблемою. DDoS-зловмисники постійно працюють над впровадженням нових типів атак з підвищеною потужністю та складністю. Тому дослідження захисту від атак нульового дня є найскладнішим. Крім усіх основних технічних навичок, це дослідження також вимагає розуміння психології зловмисників і навичок, які виявляють нові типи DDoS-атак.

Іншим аспектом покращення виявлення атак DDoS є включення в Інтернеті додаткових функцій підзвітності та функцій аудиту. В [140] був представлений підзвітний метод журналювання, який називається flow-net, для кращого журналювання для комп'ютерних і мережевих систем. Однак цей підхід вимагає від усіх маршрутизаторів реалізації методу потокової мережі, і це навряд чи буде досягнуто в реальності. В [141] був запропонований протокол публічного аудиту з використанням подвійно пов'язаної інформаційної таблиці та масиву розташування з глобальною перевіркою для проведення як одиночного, так і групового аудиту. Однак, якщо застосувати цей підхід до Інтернету, дуже важкі криптографічні функції призведуть до сповільнення системи.

## ВИСНОВКИ

Представлено комплексний і систематичний аналіз DDoS-атак, а також поточний стан проблеми. Наведено інформацію про різні типи атак, які існують на даний момент. Обговорено DDoS-атаки на нетрадиційні системи, такі як хмари, розумні електромережі, розумні будинки, CPS і системи IoT.

Проаналізовано методи запобігання DDoS-атакам та пом'якшення наслідків на основі їх успіху та невдач.

Визначено ключові особливості атак, а також переваги та недоліки різних механізмів захисту.

Виділено проблеми, пов'язані з дослідженням DDoS-атак.

Відзначено деякі майбутні напрямки досліджень, які заслуговують на увагу.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. York K. Dyn statement on 10/21/2016 ddos attack. *cyber-peace.org - trust building in cyberspace*. URL: [https://cyber-peace.org/wp-content/uploads/2016/10/Dyn-Statement-on-10\\_21\\_2016-DDoS-Attack.pdf](https://cyber-peace.org/wp-content/uploads/2016/10/Dyn-Statement-on-10_21_2016-DDoS-Attack.pdf).
2. Liu B. High performance simulation technology in the Internet of Things. *International journal of sensor networks*. 2015. T. 17, № 3. C. 195. URL: <https://doi.org/10.1504/ijsn.2015.068184>.
3. Peng T., Leckie C., Ramamohanarao K. Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM computing surveys*. 2007. T. 39, № 1. C. 3. URL: <https://doi.org/10.1145/1216370.1216373>.
4. Guo Y., Perreau S. Detect DDoS flooding attacks in mobile ad hoc networks. *International journal of security and networks*. 2010. T. 5, № 4. C. 259. URL: <https://doi.org/10.1504/ijsn.2010.037666>.
5. Deng J., Han R., Mishra S. Limiting DoS attacks during multihop data delivery in wireless sensor networks. *International journal of security and networks*. 2006. T. 1, № 3/4. C. 167. URL: <https://doi.org/10.1504/ijsn.2006.011776>.
6. Criscuolo P. J. Distributed denial of service tools, trin00, tribe flood network, tribe flood network 2000 and stacheldraht. Office of Scientific and Technical Information (OSTI), 2000. URL: <https://doi.org/10.2172/792253>.
7. Nazario J. DDoS attack evolution. *Network security*. 2008. T. 2008, № 7. C. 7–10. URL: [https://doi.org/10.1016/s1353-4858\(08\)70086-2](https://doi.org/10.1016/s1353-4858(08)70086-2).
8. Zargar S. T., Joshi J., Tipper D. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. *IEEE communications surveys & tutorials*. 2013. T. 15, № 4. C. 2046–2069. URL: <https://doi.org/10.1109/surv.2013.031413.00127>.
9. Nazario J. Politically motivated denial of service attacks. *ResearchGate*. URL:

[https://www.researchgate.net/publication/237393633\\_POLITICALLY\\_MOTIVATED\\_DENIAL\\_OF\\_SERVICE\\_ATTACKS](https://www.researchgate.net/publication/237393633_POLITICALLY_MOTIVATED_DENIAL_OF_SERVICE_ATTACKS).

10. Contributors to Wikimedia projects. Internet activism during the 2009 Iranian election protests - Wikipedia. *Wikipedia, the free encyclopedia*. URL: [https://en.wikipedia.org/w/index.php?title=Internet\\_activism\\_during\\_the\\_2009\\_Iranian\\_election\\_protests&oldid=769078109](https://en.wikipedia.org/w/index.php?title=Internet_activism_during_the_2009_Iranian_election_protests&oldid=769078109).

11. E S. WikiLeaks reports it is under A denial of service attack | techcrunch. *TechCrunch*. URL: <https://techcrunch.com/2010/11/28/wikileaks-ddos-attack/>.

12. Botnet: classification, attacks, detection, tracing, and preventive measures / J. Liu та ін. *EURASIP journal on wireless communications and networking*. 2009. Т. 2009, № 1. URL: <https://doi.org/10.1155/2009/692654>.

13. Douligieris C., Mitrokotsa A. DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer networks*. 2004. Т. 44, № 5. С. 643–666. URL: <https://doi.org/10.1016/j.comnet.2003.10.003>.

14. Self-propagating mal-packets in wireless sensor networks: dynamics and defense implications / B. Sun та ін. *Ad hoc networks*. 2009. Т. 7, № 8. С. 1489–1500. URL: <https://doi.org/10.1016/j.adhoc.2009.04.003>.

15. Staniford S., Paxson V., Weaver N. How to own the internet in your spare time. *ResearchGate*. URL: [https://www.researchgate.net/publication/221260442\\_How\\_to\\_Own\\_the\\_Internet\\_in\\_Your\\_Spare\\_Time](https://www.researchgate.net/publication/221260442_How_to_Own_the_Internet_in_Your_Spare_Time).

16. Mirkovic J., Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM computer communication review*. 2004. Т. 34, № 2. С. 39–53. URL: <https://doi.org/10.1145/997150.997156>.

17. Patrikakis C. Z., Masikos M., Zouraraki O. Distributed denial of service attacks. *ResearchGate*. URL: [https://www.researchgate.net/publication/256567797\\_Distributed\\_Denial\\_of\\_Service\\_Attacks](https://www.researchgate.net/publication/256567797_Distributed_Denial_of_Service_Attacks).

18. Weaver N. Potential strategies for high speed active worms: a worst case analysis. *Maui Gateway*. URL: <http://www.surfer.mauigateway.com/library/worms.pdf>.
19. Weaver N. Warhol worms: the potential for very fast internet plagues. *ResearchGate*. URL: [https://www.researchgate.net/publication/228705611\\_Warhol\\_worms\\_The\\_potential\\_for\\_very\\_fast\\_internet\\_plagues](https://www.researchgate.net/publication/228705611_Warhol_worms_The_potential_for_very_fast_internet_plagues).
20. Moore D., Shannon C., Claffy K. Code-Red. *The second ACM SIGCOMM Workshop*, м. Marseille, France, 6–8 листоп. 2002 р. New York, New York, USA, 2002. URL: <https://doi.org/10.1145/637201.637244>.
21. Blog, case studies and resources | Netcraft. *Blog, case studies and resources | Netcraft*. URL: <https://news.netcraft.com/archives/category/web-server-survey/>.
22. Chen Z., Ji C. Optimal worm-scanning method using vulnerable-host distributions. *International journal of security and networks*. 2007. Т. 2, № 1/2. С. 71. URL: <https://doi.org/10.1504/ijsn.2007.012826>.
23. Chen Z., Chen C. Characterising heterogeneity in vulnerable hosts on worm propagation. *International journal of security and networks*. 2016. Т. 11, № 4. С. 224. URL: <https://doi.org/10.1504/ijsn.2016.079276>.
24. Long N., Thomas R. Trends in denial of service attack technology. *Software Engineering Institute*. URL: [https://resources.sei.cmu.edu/asset\\_files/WhitePaper/2001\\_019\\_001\\_52491.pdf](https://resources.sei.cmu.edu/asset_files/WhitePaper/2001_019_001_52491.pdf).
25. Mansfield-Devine S. DDoS: threats and mitigation. *Network security*. 2011. Т. 2011, № 12. С. 5–12. URL: [https://doi.org/10.1016/s1353-4858\(11\)70128-3](https://doi.org/10.1016/s1353-4858(11)70128-3).
26. A recent survey on ddos attacks and defense mechanisms / A. Srivastava та ін. *Advances in parallel distributed computing*. Berlin, Heidelberg, 2011. С. 570–580. URL: [https://doi.org/10.1007/978-3-642-24037-9\\_57](https://doi.org/10.1007/978-3-642-24037-9_57).
27. Specht S. M., Lee R. B. Distributed denial of service: taxonomies of attacks, tools, and countermeasures. *ResearchGate*. URL:

[https://www.researchgate.net/publication/220922510\\_Distributed\\_Denial\\_of\\_Service\\_Taxonomies\\_of\\_Attacks\\_Tools\\_and\\_Countermeasures](https://www.researchgate.net/publication/220922510_Distributed_Denial_of_Service_Taxonomies_of_Attacks_Tools_and_Countermeasures).

28. Cybersecurity training & certifications | infosec. *Cybersecurity Training & Certifications* | Infosec. URL: <https://www.infosecinstitute.com/>.

29. Verisign is a global provider of domain name registry services and internet infrastructure - Verisign. *Verisign is a global provider of domain name registry services and internet infrastructure - Verisign*. URL: <https://www.verisign.com/>.

30. Park P. Call flooding attack. *Network World*. URL: <https://www.networkworld.com/article/762121/call-flooding-attack.html>.

31. RSnake J., Lee R. Slowloris HTTP DoS. *GitHub*. URL: <https://gist.github.com/steakknife/1865841>.

32. Taxonomy of DDoS Attacks. *RioRey*. URL: [https://static1.squarespace.com/static/5548bab5e4b08ecb6652391c/t/554923d6e4b03d6d83ac7c5e/1430856662717/RioRey\\_Taxonomy\\_DDoS\\_Attacks\\_2.6\\_2015-1.pdf](https://static1.squarespace.com/static/5548bab5e4b08ecb6652391c/t/554923d6e4b03d6d83ac7c5e/1430856662717/RioRey_Taxonomy_DDoS_Attacks_2.6_2015-1.pdf).

33. R.U.D.Y. (R-U-Dead-Yet?). *Imperva*. URL: <https://www.imperva.com/learn/ddos/rudy-r-u-dead-yet/?redirect=Incapsula>.

34. Analysis of slow read dos attack / J. Park та ін. *2014 international symposium on information theory and its applications* : Symposium, м. Victoria, BC. URL: <https://ieeexplore.ieee.org/document/6979803>.

35. Are you ready for slow reading?. *Notes On Security*. URL: <https://blog.shekyan.com/2012/01/are-you-ready-for-slow-reading.html>.

36. How to protect against slow HTTP attacks | qualys security blog. *Qualys Security Blog*. URL: <https://blog.qualys.com/vulnerabilities-threat-research/2011/11/02/how-to-protect-against-slow-http-attacks>.

37. DoS ddos attacks and countermeasures. *You Deserve a Better Experience*. URL: <https://www.linearstack.com/blog/dos-ddos-attacks-and-countermeasures>.

38. Implementation of DoS attack and mitigation strategies in IEEE 802.11b/g WLAN / J. Deng та ін. *SPIE defense, security, and sensing*, м. Orlando, Florida / ред. E. M. Carapezza. 2010. URL: <https://doi.org/10.1117/12.851259>.

39. Defending dos attacks on broadcast authentication in wireless sensor networks / X. Du та ін. *2008 IEEE international conference on communications*, м. Beijing, China, 19–23 трав. 2008 р. 2008. URL: <https://doi.org/10.1109/icc.2008.319>.

40. What is a ddos attack? How it works, trends, types & mitigation. *Radware*. URL: <https://www.radware.com/cyberpedia/ddospedia/ddos-meaning-what-is-ddos-attack/>.

41. What is DNS amplification attack? | knowledge base ddos-guard. *DDoS-GUARD*. URL: <https://ddos-guard.net/terms/ddos-attack-types/dns-amplification>.

42. DNS amplification attacks. *CISA*. URL: <https://www.cisa.gov/news-events/alerts/2013/03/29/dns-amplification-attacks>.

43. Rosenbaum R. Using the domain name system to store arbitrary string attributes. RFC Editor, 1993. URL: <https://doi.org/10.17487/rfc1464>.

44. Graham-Cumming J. Understanding and mitigating NTP-based DDoS attacks. *cloudflare*. URL: <https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks>.

45. Network time protocol - wikipedia. *Wikipedia, the free encyclopedia*. URL: [https://en.wikipedia.org/wiki/Network\\_Time\\_Protocol](https://en.wikipedia.org/wiki/Network_Time_Protocol).

46. Distributed denial-of-service attacks on root nameservers - Wikipedia. *Wikipedia, the free encyclopedia*. URL: [https://en.wikipedia.org/wiki/Distributed\\_denial-of-service\\_attacks\\_on\\_root\\_nameservers](https://en.wikipedia.org/wiki/Distributed_denial-of-service_attacks_on_root_nameservers).

47. My dyn account. *Domain Name System (DNS) | Oracle*. URL: <http://dyn.com/dns/>.

48. Limer E. How hackers wrecked the internet using dvrs and webcams. *Popular Mechanics*. URL:

<https://www.popularmechanics.com/technology/infrastructure/a23504/mirai-botnet-internet-of-things-ddos-attack/>.

49. IoT devices installed base worldwide 2015-2025 | Statista. *Statista*. URL: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>.

50. Herzberg B., Bekerman D., Zeifman I. Breaking down mirai: an iot ddos botnet analysis. *Incapsula*. URL: <http://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html>.

51. What is a Zero-Day Attack?. *Radware*. URL: <https://www.radware.com/blog/security/what-is-a-zero-day-attack/>.

52. Akamai releases fourth quarter 2016 state of the internet / security report. *Akamai*. URL: <https://www.akamai.com/newsroom/press-release/akamai-releases-fourth-quarter-2016-state-of-the-internet-security-report>.

53. Security studies | ponemon institute. *Ponemon Institute*. URL: <https://www.ponemon.org/research/ponemon-library/security/security.html>.

54. Ferguson P., Senie D. Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing. RFC Editor, 1998. URL: <https://doi.org/10.17487/rfc2267>.

55. Requirements for IP version 4 routers / ред. F. Baker. RFC Editor, 1995. URL: <https://doi.org/10.17487/rfc1812>.

56. Park K., Lee H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. *ACM SIGCOMM computer communication review*. 2001. T. 31, № 4. C. 15–26. URL: <https://doi.org/10.1145/964723.383061>.

57. Zhenhai Duan, Xin Yuan, Chandrashekar J. Controlling IP spoofing through interdomain packet filters. *IEEE transactions on dependable and secure computing*. 2008. T. 5, № 1. C. 22–36. URL: <https://doi.org/10.1109/tdsc.2007.70224>.

58. SAVE: source address validity enforcement protocol / Jun Li та ін. *IEEE information communications conference (INFOCOM 2002)*, м. New York, NY, USA. URL: <https://doi.org/10.1109/infcom.2002.1019407>.
59. Wang H., Jin C., Shin K. G. Defense against spoofed IP traffic using hop-count filtering. *IEEE/ACM transactions on networking*. 2007. Т. 15, № 1. С. 40–53. URL: <https://doi.org/10.1109/tnet.2006.890133>.
60. Tao Peng, Leckie C., Ramamohanarao K. Protection from distributed denial of service attacks using history-based IP filtering. *IEEE international conference on communications*, м. Anchorage, AK, USA. URL: <https://doi.org/10.1109/icc.2003.1204223>.
61. Yaar A., Perrig A., Song D. Pi: a path identification mechanism to defend against DDoS attacks. *2003 symposium on security and privacy*, м. Berkeley, CA, USA. URL: <https://doi.org/10.1109/secpri.2003.1199330>.
62. Yaar A., Perrig A., Song D. StackPi: new packet marking and filtering mechanisms for ddos and IP spoofing defense. *IEEE journal on selected areas in communications*. 2006. Т. 24, № 10. С. 1853–1863. URL: <https://doi.org/10.1109/jsac.2006.877138>.
63. Understanding the efficacy of deployed internet source address validation filtering / R. Beverly та ін. *The 9th ACM SIGCOMM conference*, м. Chicago, Illinois, USA, 4–6 листоп. 2009 р. New York, New York, USA, 2009. URL: <https://doi.org/10.1145/1644893.1644936>.
64. PacketScore: a statistics-based packet filtering scheme against distributed denial-of-service attacks / Yoohwan Kim та ін. *IEEE transactions on dependable and secure computing*. 2006. Т. 3, № 2. С. 141–155. URL: <https://doi.org/10.1109/tdsc.2006.25>.
65. Kalkan K., Alagöz F. A distributed filtering mechanism against DDoS attacks: ScoreForCore. *Computer networks*. 2016. Т. 108. С. 199–209. URL: <https://doi.org/10.1016/j.comnet.2016.08.023>.

66. Towards a more functional and secure network infrastructure | EECS at UC Berkeley. *Home | EECS at UC Berkeley*. URL: <https://www2.eecs.berkeley.edu/Pubs/TechRpts/2003/6241.html>.

67. Keromytis A. D., Misra V., Rubenstein D. Secure overlay services (SOS). Fort Belvoir, VA : Defense Technical Information Center, 2004. URL: <https://doi.org/10.21236/ada426757>.

68. AmpPot: monitoring and defending against amplification ddos attacks / L. Krämer та ін. *Research in attacks, intrusions, and defenses*. Cham, 2015. C. 615–636. URL: [https://doi.org/10.1007/978-3-319-26362-5\\_28](https://doi.org/10.1007/978-3-319-26362-5_28).

69. Weiler N. Honeypots for distributed denial-of-service attacks. *Eleventh IEEE international workshops on enabling technologies: infrastructure for collaborative enterprises. WET ICE 2002*, м. Pittsburgh, PA, USA. URL: <https://doi.org/10.1109/enabl.2002.1029997>.

70. McMullin M. DNS, load balancing and DDOS attacks - load balancers. *Load Balancer For Always-On Application Experience - Kemp*. URL: <https://kemptechnologies.com/blog/load-balancing-and-ddos-attacks/>.

71. Xianjun Geng, Whinston A. B. Defeating distributed denial of service attacks. *IT professional*. 2000. Т. 2, № 4. С. 36–42. URL: <https://doi.org/10.1109/6294.869381>.

72. Liu J., Xiao Y., Chen C. L. P. Internet of things' authentication and access control. *International journal of security and networks*. 2012. Т. 7, № 4. С. 228. URL: <https://doi.org/10.1504/ijasn.2012.053461>.

73. Intrusion detection techniques in mobile ad hoc and wireless sensor networks / B. Sun та ін. *IEEE wireless communications*. 2007. Т. 14, № 5. С. 56–63. URL: <https://doi.org/10.1109/mwc.2007.4396943>.

74. Paxson V. Bro: a system for detecting network intruders in real-time. *Computer networks*. 1999. Т. 31, № 23-24. С. 2435–2463. URL: [https://doi.org/10.1016/s1389-1286\(99\)00112-7](https://doi.org/10.1016/s1389-1286(99)00112-7).

75. Proactive detection of distributed denial of service attacks using MIB traffic variables-a feasibility study / J. B. D. Cabrera та ін. *2001 international*

*symposium on integrated network management*, м. Seattle, WA, USA. URL: <https://doi.org/10.1109/inm.2001.918069>.

76. Roesch M. Snort – lightweight intrusion detection for networks. *USENIX*. URL: [https://www.usenix.org/event/lisa99/full\\_papers/roesch/roesch.pdf](https://www.usenix.org/event/lisa99/full_papers/roesch/roesch.pdf).

77. Chen-Mou Cheng, Kung H. T., Koan-Sin Tan. Use of spectral analysis in defense against DoS attacks. *GLOBECOM 2002 - IEEE global communications conference*, м. Taipei, Taiwan. URL: <https://doi.org/10.1109/glocom.2002.1189011>.

78. Hussain A., Heidemann J., Papadopoulos C. A framework for classifying denial of service attacks. *The 2003 conference*, м. Karlsruhe, Germany, 25–29 септ. 2003 p. New York, New York, USA, 2003. URL: <https://doi.org/10.1145/863955.863968>.

79. Hussain A., Heidemann J., Papadopoulos C. Identification of repeated denial of service attacks. *Proceedings IEEE INFOCOM 2006. 25TH IEEE international conference on computer communications*, м. Barcelona, Spain, 23–29 квіт. 2006 p. 2006. URL: <https://doi.org/10.1109/infocom.2006.126>.

80. Jow J., Xiao Y., Han W. A survey of intrusion detection systems in smart grid. *International journal of sensor networks*. 2017. Т. 23, № 3. С. 170. URL: <https://doi.org/10.1504/ijsn.2017.083410>.

81. Bo Sun, Yang Xiao, Ruhai Wang. Detection of fraudulent usage in wireless networks. *IEEE transactions on vehicular technology*. 2007. Т. 56, № 6. С. 3912–3923. URL: <https://doi.org/10.1109/tvt.2007.901875>.

82. Gil T. M., Poletto M. MULTOPS: a data-structure for bandwidth attack detection. Fort Belvoir, VA : Defense Technical Information Center, 2001. URL: <https://doi.org/10.21236/ada401819>.

83. An efficient filter for denial-of-service bandwidth attacks / S. Abdelsayed та ін. *GLOBECOM '03. IEEE global telecommunications conference*, м. San Francisco, CA, USA. URL: <https://doi.org/10.1109/glocom.2003.1258459>.

84. Mirkovic J., Prier G., Reiher P. Attacking DDoS at the source. *10th IEEE international conference on network protocols*, м. Paris, France. URL: <https://doi.org/10.1109/icnp.2002.1181418>.

85. A signal analysis of network traffic anomalies / P. Barford та ін. *The second ACM SIGCOMM Workshop*, м. Marseille, France, 6–8 листоп. 2002 р. New York, New York, USA, 2002. URL: <https://doi.org/10.1145/637201.637210>.

86. Talpade R., Kim G., Khurana S. NOMAD: traffic-based network monitoring framework for anomaly detection. *IEEE international symposium on computers and communications*, м. Red Sea, Egypt. URL: <https://doi.org/10.1109/iscc.1999.780942>.

87. Yi Xie, Shun-Zheng Yu. A large-scale hidden semi-markov model for anomaly detection on user browsing behaviors. *IEEE/ACM transactions on networking*. 2009. Т. 17, № 1. С. 54–65. URL: <https://doi.org/10.1109/tnet.2008.923716>.

88. Xiang Y., Li K., Zhou W. Low-Rate ddos attacks detection and traceback by using new information metrics. *IEEE transactions on information forensics and security*. 2011. Т. 6, № 2. С. 426–437. URL: <https://doi.org/10.1109/tifs.2011.2107320>.

89. A transform domain-based anomaly detection approach to network-wide traffic / D. Jiang та ін. *Journal of network and computer applications*. 2014. Т. 40. С. 292–306. URL: <https://doi.org/10.1016/j.jnca.2013.09.014>.

90. Ma X., Chen Y. DDoS detection method based on chaos analysis of network traffic entropy. *IEEE communications letters*. 2014. Т. 18, № 1. С. 114–117. URL: <https://doi.org/10.1109/lcomm.2013.112613.132275>.

91. Bhuyan M. H., Bhattacharyya D. K., Kalita J. K. E-LDAT: a lightweight system for DDoS flooding attack detection and IP traceback using extended entropy metric. *Security and communication networks*. 2016. Т. 9, № 16. С. 3251–3270. URL: <https://doi.org/10.1002/sec.1530>.

92. BRAIN: behavior based adaptive intrusion detection in networks: using hardware performance counters to detect ddos attacks / V. Jyothi та ін. *2016 29th*

*international conference on VLSI design and 2016 15th international conference on embedded systems (VLSID)*, м. Kolkata, India, 4–8 січ. 2016 р. 2016. URL: <https://doi.org/10.1109/vlsid.2016.115>.

93. Practical network support for IP traceback / S. Savage та ін. *ACM SIGCOMM computer communication review*. 2000. Т. 30, № 4. С. 295–306. URL: <https://doi.org/10.1145/347057.347560>.

94. Chen R., Park J., Marchany R. TRACK: a novel approach for defending against distributed denial-of-service attacks. *CiteSeerX*. URL: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=63770920aa42eedc2ae23e5e728ba61610332959>.

95. Dean D., Franklin M., Stubblefield A. An algebraic approach to IP traceback. *ACM transactions on information and system security*. 2002. Т. 5, № 2. С. 119–137. URL: <https://doi.org/10.1145/505586.505588>.

96. Dawn Xiaodong Song, Perrig A. Advanced and authenticated marking schemes for IP traceback. *IEEE INFOCOM 2001. conference on computer communications. twentieth annual joint conference of the IEEE computer and communications society*, м. Anchorage, AK, USA. URL: <https://doi.org/10.1109/infcom.2001.916279>.

97. Law T. K. T., Lui J. C. S., Yau D. K. Y. You can run, but you can't hide: an effective statistical methodology to trace back DDoS attackers. *IEEE transactions on parallel and distributed systems*. 2005. Т. 16, № 9. С. 799–813. URL: <https://doi.org/10.1109/tpds.2005.114>.

98. Goodrich M. T. Probabilistic packet marking for large-scale IP traceback. *IEEE/ACM transactions on networking*. 2008. Т. 16, № 1. С. 15–24. URL: <https://doi.org/10.1109/tnet.2007.910594>.

99. Tian H., Bi J., Jiang X. An adaptive probabilistic marking scheme for fast and secure traceback. *Networking science*. 2012. Т. 2, № 1-2. С. 42–51. URL: <https://doi.org/10.1007/s13119-012-0007-x>.

100. Peng T., Leckie C., Ramamohanarao K. Adjusted probabilistic packet marking for IP traceback. *NETWORKING 2002: networking technologies*,

*services, and protocols; performance of computer and communication networks; mobile and wireless communications*. Berlin, Heidelberg, 2002. C. 697–708. URL: [https://doi.org/10.1007/3-540-47906-6\\_56](https://doi.org/10.1007/3-540-47906-6_56).

101. Luby transform code - Wikipedia. *Wikipedia, the free encyclopedia*. URL: [https://en.wikipedia.org/wiki/Luby\\_transform\\_code](https://en.wikipedia.org/wiki/Luby_transform_code).

102. Fadlallah A. Adaptive probabilistic packet marking scheme for IP traceback. *2014 world congress on computer applications and information systems (WCCAIS)*, м. Hammamet, Tunisia, 17–19 січ. 2014 р. 2014. URL: <https://doi.org/10.1109/wccais.2014.6916548>.

103. Yu S. Distributed denial of service attack and defense. New York, NY : Springer New York, 2014. URL: <https://doi.org/10.1007/978-1-4614-9491-1>.

104. Belenky A., Ansari N. IP traceback with deterministic packet marking. *IEEE communications letters*. 2003. T. 7, № 4. C. 162–164. URL: <https://doi.org/10.1109/lcomm.2003.811200>.

105. Belenky A., Ansari N. Tracing multiple attackers with deterministic packet marking (DPM). *2003 IEEE pacific rim conference on communications computers and signal processing (PACRIM 2003)*, м. Victoria, BC, Canada. URL: <https://doi.org/10.1109/pacrim.2003.1235716>.

106. Guang Jin, Jiangang Yang. Deterministic packet marking based on redundant decomposition for IP traceback. *IEEE communications letters*. 2006. T. 10, № 3. C. 204–206. URL: <https://doi.org/10.1109/lcomm.2006.1603385>.

107. Yang Xiang, Wanlei Zhou, Minyi Guo. Flexible deterministic packet marking: an IP traceback system to find the real source of attacks. *IEEE transactions on parallel and distributed systems*. 2009. T. 20, № 4. C. 567–580. URL: <https://doi.org/10.1109/tpds.2008.132>.

108. A dynamical Deterministic Packet Marking scheme for DDoS traceback / Shui Yu та ін. *2013 IEEE global communications conference (GLOBECOM 2013)*, м. Atlanta, GA, 9–13 груд. 2013 р. 2013. URL: <https://doi.org/10.1109/glocom.2013.6831159>.

109. A feasible IP traceback framework through dynamic deterministic packet marking / S. Yu та ін. *IEEE transactions on computers*. 2016. T. 65, № 5. C. 1418–1427. URL: <https://doi.org/10.1109/tc.2015.2439287>.

110. Bellovin S. M., Leech M., Taylor T. ICMP traceback messages. Internet Engineering Task Force, 2010. 13 с. URL: <https://doi.org/10.7916/D8FF406R>.

111. ICMP traceback with cumulative path, an efficient solution for IP traceback / H. C. J. Lee та ін. *Information and communications security*. Berlin, Heidelberg, 2003. C. 124–135. URL: [https://doi.org/10.1007/978-3-540-39927-8\\_12](https://doi.org/10.1007/978-3-540-39927-8_12).

112. Izaddoost A., Othman M., Rasid M. F. A. Accurate ICMP TraceBack Model under DoS/DDoS Attack. *15th international conference on advanced computing and communications (ADCOM 2007)*, м. Guwahati, Assam, India, 18–21 груд. 2007 р. 2007. URL: <https://doi.org/10.1109/adcom.2007.103>.

113. Saurabh S., Sairam A. S. ICMP based IP traceback with negligible overhead for highly distributed reflector attack using bloom filters. *Computer communications*. 2014. T. 42. C. 60–69. URL: <https://doi.org/10.1016/j.comcom.2014.01.003>.

114. Yao G., Bi J., Vasilakos A. V. Passive IP traceback: disclosing the locations of IP spoofers from path backscatter. *IEEE transactions on information forensics and security*. 2015. T. 10, № 3. C. 471–484. URL: <https://doi.org/10.1109/tifs.2014.2381873>.

115. Liu X., Yang X., Lu Y. To filter or to authorize. *The ACM SIGCOMM 2008 conference*, м. Seattle, WA, USA, 17–22 серп. 2008 р. New York, New York, USA, 2008. URL: <https://doi.org/10.1145/1402958.1402981>.

116. Controlling high bandwidth aggregates in the network / R. Mahajan та ін. *ACM SIGCOMM computer communication review*. 2002. T. 32, № 3. C. 62–73. URL: <https://doi.org/10.1145/571697.571724>.

117. Yaar A., Perrig A., Song D. SIFF: a stateless internet flow filter to mitigate DDoS flooding attacks. *IEEE symposium on security and privacy, 2004. 2004*, м. Berkeley, CA, USA. URL: <https://doi.org/10.1109/secpri.2004.1301320>.
118. Yang X., Wetherall D., Anderson T. A DoS-limiting network architecture. *ACM SIGCOMM computer communication review*. 2005. Т. 35, № 4. С. 241–252. URL: <https://doi.org/10.1145/1090191.1080120>.
119. Fault-tolerant topology evolution and analysis of sensing systems in IoT based on complex networks / S. Xiong та ін. *International journal of sensor networks*. 2015. Т. 18, № 1/2. С. 22. URL: <https://doi.org/10.1504/ijsnnet.2015.069873>.
120. Policing congestion response in an internetwork using re-feedback / B. Briscoe та ін. *ACM SIGCOMM computer communication review*. 2005. Т. 35, № 4. С. 277–288. URL: <https://doi.org/10.1145/1090191.1080124>.
121. Liu X., Yang X., Xia Y. NetFence. *ACM SIGCOMM computer communication review*. 2010. Т. 40, № 4. С. 255–266. URL: <https://doi.org/10.1145/1851275.1851214>.
122. Menth M., Martin R., Charzinski J. Capacity overprovisioning for networks with resilience requirements. *ACM SIGCOMM computer communication review*. 2006. Т. 36, № 4. С. 87–98. URL: <https://doi.org/10.1145/1151659.1159925>.
123. What is cloud computing? A beginner's guide. *microsoft*. URL: <https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/>.
124. DDoS attacks in cloud computing: issues, taxonomy, and future directions / G. Somani та ін. *Computer communications*. 2017. Т. 107. С. 30–48. URL: <https://doi.org/10.1016/j.comcom.2017.03.010>.
125. Xiao Z., Xiao Y. Security and privacy in cloud computing. *IEEE communications surveys & tutorials*. 2013. Т. 15, № 2. С. 843–859. URL: <https://doi.org/10.1109/surv.2012.060912.00182>.
126. Privacy-Preserving smart similarity search based on simhash over encrypted data in cloud computing / Z. Fu та ін. *Journal of internet technology*.

2015. T. 16, № 3. C. 453–460. URL: <https://doi.org/10.6138/JIT.2015.16.3.20140918>.

127. A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing / Z. Xia та ін. *IEEE transactions on information forensics and security*. 2016. T. 11, № 11. C. 2594–2608. URL: <https://doi.org/10.1109/tifs.2016.2590944>.

128. Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement / Z. Fu та ін. *IEEE transactions on information forensics and security*. 2016. T. 11, № 12. C. 2706–2716. URL: <https://doi.org/10.1109/tifs.2016.2596138>.

129. Privacy-Preserving smart semantic search based on conceptual graphs over encrypted outsourced data / Z. Fu та ін. *IEEE transactions on information forensics and security*. 2017. T. 12, № 8. C. 1874–1884. URL: <https://doi.org/10.1109/tifs.2017.2692728>.

130. Enabling semantic search based on conceptual graphs over encrypted outsourced data / Z. Fu та ін. *IEEE transactions on services computing*. 2019. T. 12, № 5. C. 813–823. URL: <https://doi.org/10.1109/tsc.2016.2622697>.

131. A secure cloud-assisted urban data sharing framework for ubiquitous-cities / J. Shen та ін. *Pervasive and mobile computing*. 2017. T. 41. C. 219–230. URL: <https://doi.org/10.1016/j.pmcj.2017.03.013>.

132. Wang W., Lu Z. Cyber security in the smart grid: survey and challenges. *Computer networks*. 2013. T. 57, № 5. C. 1344–1371. URL: <https://doi.org/10.1016/j.comnet.2012.12.017>.

133. Cyber security and privacy issues in smart grids / J. Liu та ін. *IEEE communications surveys & tutorials*. 2012. T. 14, № 4. C. 981–997. URL: <https://doi.org/10.1109/surv.2011.1221111.00145>.

134. Mantas G., Lymberopoulos D., Komninos N. Security in smart home environment. *Wireless technologies for ambient assisted living and healthcare*. C. 170–191. URL: <https://doi.org/10.4018/978-1-61520-805-0.ch010>.

135. Auriemma L. Samsung devices with support for remote controllers. *altervista*. URL: [https://alugi.altervista.org/adv/samsux\\_1-adv.txt](https://alugi.altervista.org/adv/samsux_1-adv.txt).
136. Nunes G. M. Sony bravia - remote denial of service. *Exploit Database*. URL: <https://www.exploit-db.com/exploits/18705>.
137. Strategy I., Unit P. ITU internet report 2005 : the internet of things / ITU. 7-ме вид. Geneva : International Telecommunication Union, 2005. 186 с. URL: <https://itu.tind.io/record/6354>.
138. DuBravac S., Ratti C. The internet of things: evolution or revolution?. *The Digital Insurer*. URL: <https://www.the-digital-insurer.com/wp-content/uploads/2015/07/549-AIG-White-Paper-IoT.pdf>.
139. Baheti R., Gill H. Part 3: cross-cutting research directions, cyber-physical systems. *The impact of control technology* / ред.: Т. Samad, A. Annaswamy. 2011. С. 161–166. URL: <https://ieeecss.org/sites/ieeecss/files/2019-07/IoCT-Part3-02CyberphysicalSystems.pdf>.
140. Xiao Y. Flow-net methodology for accountability in wireless networks. *IEEE network*. 2009. Т. 23, № 5. С. 30–37. URL: <https://doi.org/10.1109/mnet.2009.5274919>.
141. An efficient public auditing protocol with novel dynamic structure for cloud data / J. Shen та ін. *IEEE transactions on information forensics and security*. 2017. Т. 12, № 10. С. 2402–2415. URL: <https://doi.org/10.1109/tifs.2017.2705620>.