**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Національний університет кораблебудування імені адмірала Макарова**

Навчально-науковий інститут автоматики і електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
_____ С.М. Нужний
«28» 12 2024 р.

Кваліфікаційна робота
на правах рукопису

# КВАЛІФІКАЦІЙНА РОБОТА

## Розробка системи підтримки прийняття рішень щодо вибору засобів захисту від DDoS-атак

Ступінь вищої освіти: магістр
Галузь знань: 14 Електрична інженерія
Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»
Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

Виконала: студентка 6 курсу групи 6366м
Садалюк Єлизавета Олександрівна _____

Кваліфікаційна робота містить результати самостійного виконання навчального завдання. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Є.О. Садалюк

Керівник:
к.т.н., доцент, доцент кафедри комп'ютерних технологій та інформаційної безпеки

Турти Марина Валентинівна _____

Миколаїв – 2024

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Національний університет кораблебудування імені адмірала Макарова**

Навчально-науковий інститут автоматики і електротехніки

ЗАТВЕРДЖУЮ
Гарант освітньої програми, к.т.н.,
доцент, доцент кафедри КТІБ
_____ Турти М.В.
«_4_» _11_____ 2024 р.

ЗАВДАННЯ

на кваліфікаційну роботу

Студентка: Садалюк Єлизавета Олександрівна

Курс:6

Група: 6366м

Ступінь вищої освіти: магістр

Галузь знань: 14 Електрична інженерія

Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»

Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

1. Тема роботи: Розробка системи підтримки прийняття рішень щодо вибору засобів захисту від DDoS-атак
затверджена наказом НУК від «_14__» жовтня 2024 р. № 1075 - уч

2. Вихідні дані до роботи: нормативно-правова база і теоретичні основи побудови захищених комп'ютерних систем і систем підтримки прийняття рішень

3. Перелік питань, які необхідно розробити: провести аналіз відкритих літературних джерел і визначити критерії класифікації DDoS-атак, параметри наявних на ринку засобів захисту від DDoS-атак і критерії прийняття рішень щодо їх вибору; розробити основні алгоритми, створити структуру системи прийняття рішень щодо вибору засобів захисту від DDoS-атак як складової комплексу засобів захисту

4. Терміни виконання завдання:
термін видачі завдання: « 04 » вересня 2024 р.
термін подання роботи: «19»грудня 2024 р.

## 6. План-графік виконання кваліфікаційної роботи

| № п/п | Заходи | Дата | | Готовність | Відмітка про виконання |
|---|---|---|---|---|---|
| | | Навч. тиждень | Контрольна дата | | |
| 1. | Наукове стажування | 1 - 8 | 25.10.2024 | Звіт з наукового стажування | Виконано |
| 2. | Організаційні збори | 9 | 31.10.2024 | Попередній варіант змісту КР | Виконано |
| 3. | Рубіжний контроль | 10 | 05.11.2024 | Попередній варіант оглядових розділів | Виконано |
| 4. | Рубіжний контроль | 13 | 28-29.11.2024 | 1. Попередній варіант повної КР.<br>2. Попередній варіант презентації. | Виконано |
| 5. | Рубіжний контроль | 15 | 12.12.2024 | Доповідь на 12-ій Всеукраїнській науково-технічній конференції з міжнародною участю «СПІБТ–2024» | Виконано |
| 6. | Перевірка на плагіат | 15 | 12-13.12.2024 | Електронний варіант кваліфікаційної роботи | Виконано |
| 7. | КЕ на рівень « магістра» | 16 | 17-18.12.2024 | Здавання державного екзамену зі спеціальності на ступінь бакалавра | Виконано |
| 8. | Кафедральний захист | 16 | 19.12.2024 | 1. Оформлена КР (в форматі pdf) (передається студентом на кафедрі для внутрішньої рецензії). У разі отримання позитивної внутрішньої рецензії, КР подається на зовнішню рецензію.<br>2. Оформлена презентація (в форматі pdf). | Виконано |
| 9. | Подання документів на захист | 16 | 20.12.2024 | 1. Подання щодо захисту КР: тема, успішність, висновок керівника та висновок кафедри про КР.<br>2. Зовнішня рецензія (окремо від КР). Резюме на КР.<br>3. Електронний варіант та роздрукована презентація в кількості 5 примірників.<br>4. Електронний варіант КР на диску | Виконано |
| 10. | Захист ДР | 17 | 24,26,27, 28.12.2024 | 1. Приєднання студента до засідання кваліфікаційної комісії (конференції) у встановлений час для проведення процедури дистанційного захисту<br>2. Процедура захисту КР. | Виконано |

*ПРИМІТКА: Завдання додається до виконаної роботи та подається до атестаційної комісії.*

Керівник
доцент кафедри комп'ютерних технологій
та інформаційної безпеки, к.т.н., доцент _____ М.В. Турти
Студентка _____ Є.О. Садалюк

# АННОТАЦІЯ

*Садалюк Є.О.* системи підтримки прийняття рішень щодо вибору засобів захисту від *DDoS*-атак.

Кваліфікаційна робота на здобуття ступеня вищої освіти «магістр» за спеціальністю 141 «Електроенергетика, електротехніка та електромеханіка» галузі знань: 14 «Електрична інженерія» і освітньо-професійною програмою «Системи технічного захисту інформації, автоматизація її обробки». – Національний університет кораблебудування імені адмірала Макарова, Миколаїв, 2024.

Пояснювальна записка: 120 с., 10 рис., 43 посилання.

Кваліфікаційна робота присвячена актуальній темі – розробці ефективних систем захисту комп'ютерних мереж.

Об'єктом дослідження в даній роботі є системи технічного захисту комп'ютерних мереж. Предметом дослідження є засоби захисту від *DDoS*-атак. Методами дослідження є теоретичні основи побудови захищених мереж і систем підтримки прийняття рішень, метод аналізу ієрархій. Метою роботи є розробка системи прийняття рішень щодо вибору засобів захисту від *DDoS*атак як складової комплексу засобів захисту комп'ютерних мереж.

У роботі здійснено аналіз відкритих літературних джерел, визначено критерії класифікації *DDoS*-атак, параметри доступних на ринку засобів захисту від цих атак, а також критерії для прийняття рішень щодо вибору відповідних засобів; розроблено основні алгоритми, структуру системи прийняття рішень для вибору засобів захисту від *DDoS*-атак як частини загальної системи захисту комп'ютерних мереж.

Робота має практичну значимість, її результати можуть бути використані при проектуванні захищених локальних мереж та в навчальному процесі за освітньою програмою «Системи технічного захисту інформації, автоматизація її обробки» зі спеціальностей 125 «Кібербезпека» та 141 «Електроенергетика, електротехніка та електромеханіка».

**Ключові слова**: кібербезпека, *DDoS*-атака, прийняття рішень, система прийняття рішень, критерії вибору.

# ANNOTATION

*Sadaliuk Y.O.* Development of an information model for decision-making regarding the choice of means of protection against DDoS-attacks.

Qualifying work on receiving degree of "Master" in the specialty 141 "Electrical energetics, Electrical Engineering and Electromechanics" in the field of knowledge 14 "Electrical Engineering" and educational and professional program "Systems of technical protection of information, automation of its processing." - Admiral Makarov National University of Shipbuilding, Mykolaiv, 2024.

Explanatory note: 120 pp., 10 figs., 43 references.

Qualification work is devoted to a topical issue - the development of effective means of protecting computer networks.

The object of research in this work is systems of technical protection of computer networks. The subject of research is means of protection against *DDoS*-attacks. The research methods are the theoretical foundations of building secure networks and decision support systems, the method of analyzing hierarchies. The purpose of the work is to deveop an of a decision-making system regarding the selection of means of protection against *DDoS* attacks as a component of the complex of computer network protection means.

In thesis open literary sources have been analized and the classification criteria for the classification of *DDoS*-attacks, the parameters of the means of protection against *DDoS* attacks available on the market and the decision-making criteria for the selection of these means have been determined; the main algorithms and structure of the decision-making system regarding the selection of means of protection against *DDoS*-attacks as a component of the complex of means for protection of computer networks have been developed.

The results of the work can be used in the design of protected local networks and in the educational process under the educational program "Systems of the information technical protection, automation of its processing" in specialties 125 "Cybersecurity" and 141 "Electric power engineering, electrical engineering and electromechanics".

**Keywords:** cyber security, *DDoS* attack, decision-making, decision-making system, selection criteria.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ……..……..8
ВСТУП……11
1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ВИБОРУ ТА ОЦІНКИ ЕФЕКТИВНОСТІ ЗАСОБІВ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ ВІД *DDoS*-АТАК……13
1.2 Статистичний аналіз сучасних *DDoS*-атак та їх вплив на комп'ютерні мережі ..... 17
1.3 Огляд законодавчих та нормативних актів, пов'язаних із захистом комп'ютерних мереж від DDoS-атак ..... 201
2 ДОСЛІДЖЕННЯ МЕТОДІВ І ЗАСОБІВ ПРОВЕДЕННЯ *DDoS*-АТАК..... 36
2.1 Інструменти для здійснення *DDoS*-атак ..... 36
2.2 Класифікація *DDoS*-атак ..... 45
2.3 *Slowloris* і *NXDOMAIN* атаки ..... 55
2.4 Спам-атаки на мобільні телефони ..... 58
2.5 Вразливі точки сенсорних підмереж в архітектурі *IoT* до *DDoS*-атак ..... 60
2.6 Ознаки *DDoS*-атак ..... 66
3 ДОСЛІДЖЕННЯ МЕТОДІВ І ЗАСОБІВ ПРОТИДІЇ *DDOS*-АТАКАМ ..... 69
3.1 Стратегії захисту від *DDoS*-атак ..... 69
3.2 Протидія ботнетам як джерелу *DDoS*-атак ..... 71
3.3 Протидія *flood*-атакам ..... 72
3.4 Захист від атак *Slowloris та NXDOMAIN* ..... 77
3.5 Захист *IoT*-пристроїв від *DDoS*-атак ..... 78
3.6 Захист серверу від *DDoS*-атак ..... 80
3.7 Захист *DNS*-серверів від *DDoS*-атак..... 82
3.8 Захист мережі від *DDoS*-атак ..... 84
3.9 Сучасні професійні засоби захисту від *DDoS*-атак ..... 88
4 РОЗРОБКА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ……..95

4.1 Системи підтримки прийняття рішень ..... 95
4.2 Методи прийняття рішень ..... 97
4.3 Визначення критеріїв захисту від *DDoS*-атак..... 101
4.4 Створення алгоритмів для вибору засобів захисту від *DDoS*-атак ..... 107
4.5 Розробка структури системи прийняття рішень щодо вибору засобів захисту від *DDoS*-атак ..... 110
ВИСНОВКИ……..... 115
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..... 116

# ПЕРЕЛІК СКОРОЧЕНЬ

*ACK – Acknowledgment;*

*APDoS – Application Layer Denial of Service;*

*API – Application Programming Interface;*

*APS – Advanced Port Scanner;*

*ASCII – American Standard Code for Information Interchange;*

*BGP – Border Gateway Protocol;*

*CDN – Content Delivery Network;*

*CLI – Command Line Interface;*

*DDoS – distributed denial-of-service attack;*

*DHCP – Dynamic Host Configuration Protocol;*

*DNS - Domain Name System;*

*DPI – Deep Packet Inspection;*

*DSS – Decision Support System;*

*ESP – Protocol Encapsulating Security Payload;*

*FIN – Finish;*

*FUSN – Flying Ubiquitous Sensor Network;*

*FTP – File Transfer Protocol;*

*GUI – graphical user interface;*

*GAS – generalized audit software;*

*GRE – Generic Routing Encapsulation;*

*HULK – HTTP Unbearable Load King;*

*HTML – HyperText Markup Language;*

*HTTP – HyperText Transfer Protocol;*

*ICMP – Internet Control Message Protocol;*

*IMAP – Internet Message Access Protocol;*

*IDS – Intrusion Detection System;*

*IoE – Internet of Everything;*

*IP − Internet Protocol;*

*IPS – Intrusion Prevention System;*

*IoT – Internet of Things;*

*LOIC – Low Orbit Ion Cannon;*

*MEMS – Micro-Electro-Mechanical Systems;*

*NTP – Network Time Protocol;*

*NGN – Next Generation Network;*

*OS – operating system;*

*OSI− Open Systems Interconnection Basic Reference Mode;*

*OSPF – Open Shortest Path First;*

*PHP – Personal Home Page;*

*QoS – Quality of Service;*

*RST – Reset;*

*SEO – Search Engine Optimization;*

*SCTP – Stream Control Transmission Protocol;*

*SMTP – Simple Mail Transfer Protocol;*

*SQL – Structured Query Language;*

*SSDP – Simple Service Discovery Protocol;*

*SSL – Secure Sockets Layer;*

*SYN – Synchronize;*

*UDP – User Datagram Protocol;*

*TCP – Transmission Control Protocol;*

*TLS – Transport Layer Security;*

*TLSP – Transport Layer Service Protocol;*

*TOS – Type of Service;*

*UDP – User Datagram Protocol;*

*URL – Uniform Resource Locator;*

*VoIP – Voice over Internet Protocol;*

*XML – Extensible Markup Language;*

АС− автоматизована система;

БСМ – безпровідна сенсорна мережа;

ДССЗЗІ – Державна служба спеціального зв’язку та захисту інформації;

ЗСВ – збірні сенсорні вузли;

ІБ – інформаційна безпека;

ІзОД − інформація з обмеженим доступом;

ІКС − інформаційно-комунікаційна система;

ІТ – інформаційні технології;

КЗЗ – комплекс засобів захисту;

КС – комп’ютерна система;

КСЗІ – комплексна система захисту інформації;

НД – нормативні документи;

ОПР – особа, що приймає рішення;

ПЗ – програмне забезпечення;

СЗІ – система захисту інформації;

СППР– система підтримки прийняття рішень;

ТЗІ − технічний захист інформації;

ЦП – центральний процесор;

ШІ – штучний інтелект.

# ВСТУП

Сучасний етап розвитку інформаційно-комунікаційних технологій характеризується стрімким збільшенням обсягів даних, які створюються, обробляються та зберігаються у комп'ютерних системах. Універсальність використання інформаційних технологій у різних сферах діяльності зумовлює підвищену залежність суспільства, бізнесу та держави від стабільності та надійності функціонування інформаційних мереж. Однак, зростання масштабів і складності цих систем супроводжується появою нових кіберзагроз, які ставлять під загрозу конфіденційність, цілісність та доступність інформації.

Швидкий розвиток апаратно-програмних технологій стимулює появу нових кіберзагроз, а також удосконалює методи атак і захисту від них. Попри це, *DoS*- і *DDoS*-атаки продовжують залишатися значним джерелом кіберризиків. Численні дослідження українських [15, 28, 41-43] і зарубіжних вчених [1, 4, 5, 8, 9] спрямовані на створення ефективних способів виявлення, запобігання і протидії таким атакам.

Ринок пропонує широкий спектр засобів для захисту від *DoS*- і *DDoS*-атак, які відрізняються принципами функціонування, технічними можливостями та умовами експлуатації [7, 11, 14, 16, 29, 37, 38, 40]. Проте відсутність чіткої методики для їх раціонального вибору значно ускладнює ефективне управління ризиками, що створює серйозні виклики для користувачів і адміністраторів мереж.

Метою даної роботи є розробка системи підтримки прийняття рішень для ефективного та оптимального вибору засобів захисту від *DDoS*-атак, що забезпечує підвищення рівня безпеки комп'ютерних мереж шляхом автоматизації процесу аналізу характеристик загроз, вибору відповідних засобів протидії та обґрунтування рішень на основі заданих критеріїв.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

− провести аналіз відкритих літературних джерел для визначення ознак і класифікацій *DDoS*-атак і характеристик існуючих на ринку засобів захисту.

− визначити критерії прийняття рішень щодо вибору оптимальних засобів захисту від *DDoS*-атак;

− розробити алгоритми і структуру системи, яка забезпечить підтримку прийняття рішень при виборі засобів захисту від *DDoS*-атак, як частини комплексного захисту комп'ютерних мереж.

Об'єктом дослідження в даній роботі є системи технічного захисту комп'ютерних мереж.

Предметом дослідження в даній роботі є засоби захисту від *DDoS*-атак.

Методами дослідження є теоретичний аналіз основ побудови захищених мереж, методологія створення систем підтримки прийняття рішень, застосування методу аналізу ієрархій для визначення оптимальних рішень.

# 1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ВИБОРУ ТА ОЦІНКИ ЕФЕКТИВНОСТІ ЗАСОБІВ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ ВІД *DDoS*-АТАК

## 1.1 Принцип дії *Dos* і *DDoS*-атак

*DoS*-атака (англ. *denial-of-service attack, DoS attack*) – це вид кібернападів, який має на меті порушити нормальну роботу комп'ютерної системи (КС) шляхом перевантаження її ресурсів або зупинки її функціонування. Основною метою таких атак є створення умов, за яких легітимні користувачі не можуть отримати доступ до ресурсів системи або ці ресурси стають недоступними через перевантаження.

Доступність ресурсів КС для легітимних користувачів може бути порушена через дії зловмисника, що спричиняють:

– примусове припинення функціонування конкретного програмного забезпечення;

– перенаправлення всіх доступних системних ресурсів на виконання задач, заданих зловмисником;

– спрямування всіх ресурсів КС на виконання заданих зловмисником задач;

– витрачання ресурсів системи на виконання нецільових операцій;

– порушення роботи комунікаційних каналів, наприклад, каналів зв'язку між легітимними користувачами та атакованою системою, коли зловмисник генерує настільки великий обсяг даних для передачі через ці канали, що їх пропускна здатність вичерпується.

Найбільш розповсюдженою технікою *DoS*-атак є надсилання величезної кількості запитів до цілі, що призводить до виснаження ресурсів системи. Це викликає її перевантаження, що унеможливлює обробку запитів від легітимних

користувачів або сповільнює її роботу до такого рівня, що система фактично стає недоступною.

*DDoS*-атака – розподілена атака на відмову в обслуговуванні (англ. *distributed denial-of-service attack, DDoS attack*), яка полягає в одночасному нападі на КС з великої кількості *IP*-адрес з метою порушення доступності ресурсів КС для легітимних користувачів.

*DDoS*-атаки здійснюються за допомогою кількох десятків або навіть тисяч заражених пристроїв, які одночасно починають атакувати цільову систему. Вони набагато складніші за звичайні *DoS*-атаки через свою розподілену природу. Відмова в доступі до ресурсів або обслуговуванні може статися через різні фактори, які впливають на систему або сервіс. Серед таких факторів виділяються:

– слешдот-ефект (англ. *slashdot effect*) – потужний сплеск відвідуваності *web*-сайту, що призводить до перевищення допустимого навантаження на сервер, внаслідок чого частина користувачів отримує відмову в обслуговуванні. Причиною такої ненавмисної *DDoS*-атаки може бути розташування на популярному інтернет-ресурсі посилання на інший сайт, який міститься на не дуже продуктивному сервері. Назва ефекту походить від назви популярного блогу *Slashdot*, на якому вперше було зареєстровано таку відмову в обслуговуванні.

– використання групою зловмисників флешмобу (англ. *flash mob* - «блискавична юрба») – групи користувачів можуть домовлятися про одночасне направлення запитів до сервера або сайту, що призводить до перевантаження його ресурсів. Такі атаки можуть бути сплановані за допомогою відкритих каналів або соціальних мереж, де кілька осіб узгоджують час для спільного нападу на об'єкт;

– використання ботнетів для масових атак – ботнети є однією з найбільш ефективних і небезпечних форм атак. Це мережа комп'ютерів, які були заражені шкідливим програмним забезпеченням і контролюються зловмисником без відома власників, кожен з яких у певний момент починає надсилати запити до об’єкта атаки;

Ботнет (англ. *botnet*, від *robot* і *network*) – це мережі з інфікованих комп'ютерів, які, на яких запущені боти – програмне забезпечення (ПЗ), без відома їхніх власників, виконують накази зловмисників. Кожен комп'ютер у ботнеті працює як "зомбі", надсилаючи запити до цільової системи. Ботнети можуть бути створені через вірусні програми, які заражають комп'ютери, перетворюючи їх на частину великої атаки. Зловмисник може керувати всіма зараженими комп'ютерами через командний сервер і направляти їх для виконання атак.

Реалізація *DDoS*-атаки за допомогою ботнету, відомої також як «армія зомбі», є однією з найефективніших методів для перевантаження системи або мережі, що забезпечує зловмисникові великий контроль над атакою. Нижче наведено основний алгоритм здійснення такої атаки (рис. 1.1).

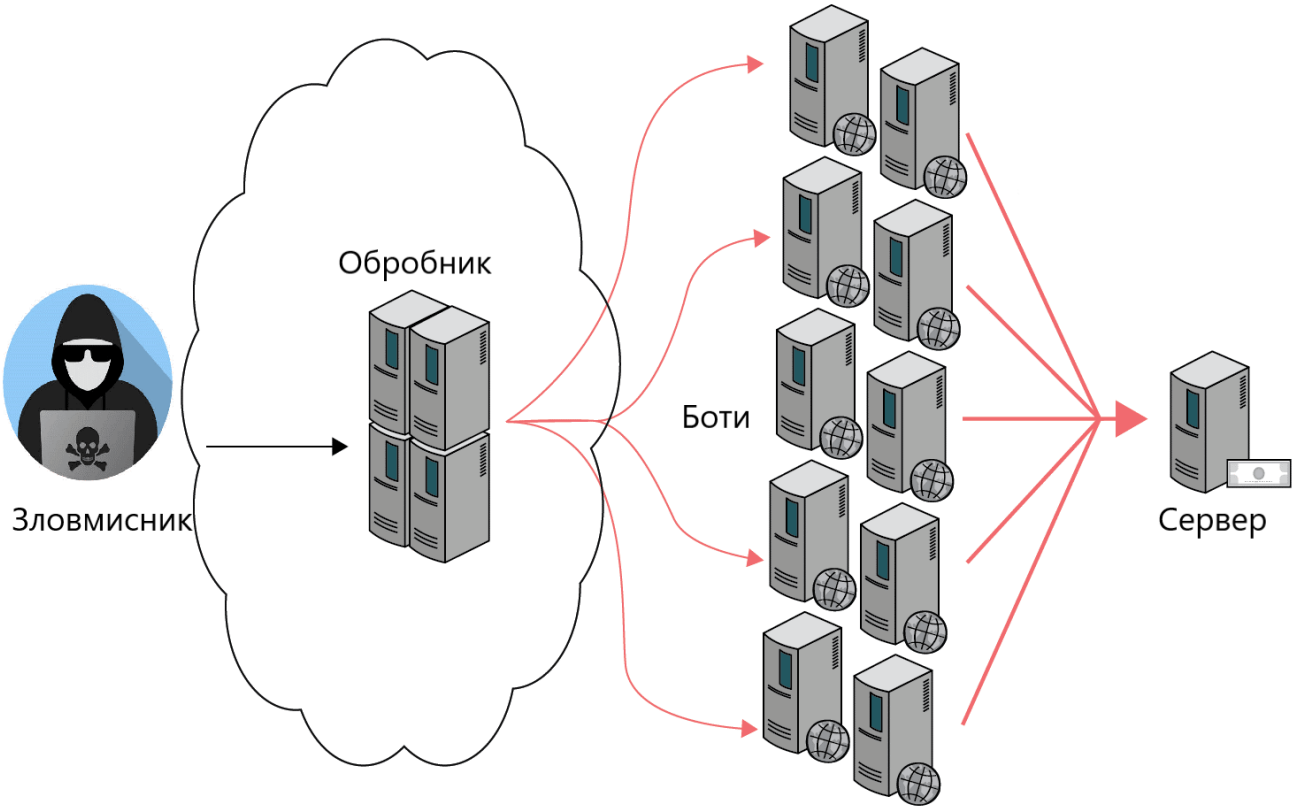



Рисунок 1.1 – Схема реалізації *DDoS*-атаки з використанням ботнет

По-перше, зловмисник використовує різноманітні методи, щоб заразити велику кількість комп'ютерів або інших пристроїв шкідливим програмним забезпеченням (наприклад, вірусами, троянами або експлойтами). Це може відбуватися через завантаження шкідливих файлів, відкриття заражених електронних листів або відвідування компрометованих веб-сайтів.

По-друге, після зараження, пристрої (комп'ютери, маршрутизатори, смартфони) автоматично підключаються до централізованої керуючої системи або командного серверу, який управляє ботнетом. Ці пристрої стають частиною «армії зомбі» і готові до виконання наказів зловмисника.

По-третє, зловмисник передає команду всім інфікованим пристроям у ботнеті, інструктуючи їх надіслати запити до обраної цілі одночасно. Це може бути запит на відкриття веб-сторінки, надсилання великих обсягів даних або інші дії, які завантажують сервер.

По-четверте, усі заражені пристрої починають одночасно надсилати запити або дані до цілі (сайту, серверу або мережі), що призводить до різкого збільшення трафіку на сервері та перевантаження його ресурсів.

По-пяте, внаслідок великої кількості запитів сервер або мережа не може обробити їх належним чином, що призводить до відмови в обслуговуванні для легітимних користувачів. Всі системні ресурси вичерпуються, і сервер стає недоступним.

Атака може тривати від кількох хвилин до кількох годин, в залежності від масштабів ботнету і наданої зловмисником інфраструктури для підтримки атаки. Після того, як атака досягає своїх цілей (порушення доступу до сервера або мережі), зловмисник може припинити команду або змінити стратегію атаки, змушуючи ботнети виконувати інші завдання.

Цей алгоритм часто використовуються для атак на великі організації, що можуть включати фінансові установи, державні установи або популярні веб-ресурси, у результаті чого можуть виникнути значні збитки, втрати довіри та репутації.

Популярність *DoS* і *DDoS*-атак в сучасному кіберпросторі зумовлена тим, що вони дозволяють довести до відмови практично будь-яку систему, не залишаючи при цьому юридично значущих доказів.

## 1.2 Статистичний аналіз сучасних *DDoS*-атак та їх вплив на комп'ютерні мережі

Провідні компанії в галузі інформаційної безпеки (ІБ) збирають статистику щодо атак різного типу у кіберпросторах окремих країн і світу та періодично оприлюднюють результати її аналізу.

У 2024 році *DDoS*-атаки (розподілені атаки на відмову в обслуговуванні) продовжують еволюціонувати, з'являються нові тенденції та патерни.

Згідно з останніми статистичними даними щодо *DDoS*-атак, американська компанія *Cloudflare*, що спеціалізується на захисті від атак, опублікувала дані за третій квартал 2024 року, атаки *DDoS* показали значне збільшення як за частотою, так і за масштабами. *Cloudflare* повідомила про запобігання понад 6 мільйонам атак *DDoS* лише в третьому кварталі, що на 49% більше порівняно з попереднім кварталом та на 55% більше порівняно з аналогічним періодом минулого року (рис. 1.2). Серед цих атак було понад 200 гіперволюметричних атак, що перевищували 3 терабіти на секунду (*Tbps*), при цьому найбільша атака досягала піку в 4,2 *Tbps* протягом хвилини.

За даними поданими таких компаній, як *Cloudflare*, *Cisco* та інших, які фіксують рекордні рівні інтенсивності атак, можна визначити наступні тенденції *DDoS*-атак за 2024 рік:

– зростання частоти *DDoS*-атак в більшості галузей;
– зростання потужності атак;
– зростання обсягу атак;

– спрямованість атак на критично важливу інфраструктуру;

– впровадження штучного інтелекту;

– атаки через *IPv*6;

– активне використання пристроїв Інтернету речей (*IoT*), що дозволяє створювати потужніші ботнети;

– застосування *DDoS*-атак як інструменту конкурентної боротьби;

– зростання кількості політично мотивованих атак.

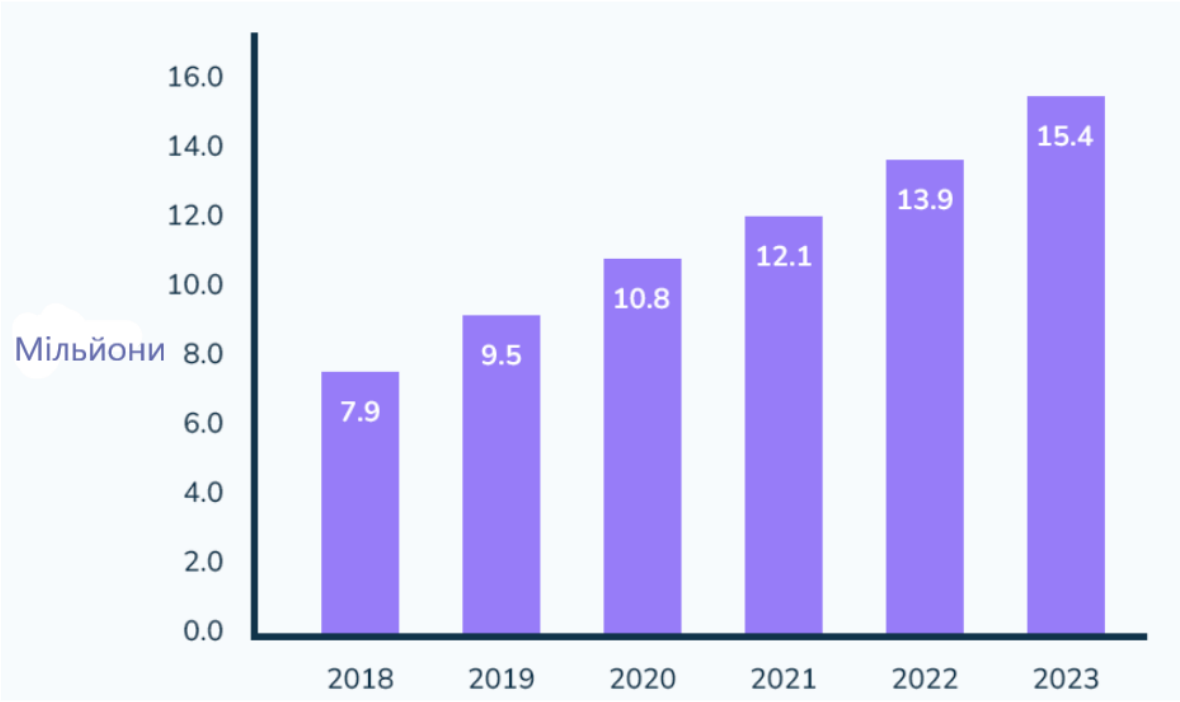



Рисунок 1.2– Динаміка кількості *DDoS*-атак за останні п’ять років

За даними журналу *Security Today*, що висвітлює новини та тенденції в галузі безпеки, у 2023 році було зафіксовано приблизно 15,4 мільйонів атак *DDoS*. У першій половині 2024 року здійснено близько 7,9 мільйона атак, що на 31% більше, ніж за аналогічний період 2022 року. У 2023 році було зафіксовано майже вдвічі більше атак ніж у 2018 році. Спостерігається також тенденція до зростання пікової потужності і глобального обсягу *DDoS*-атак . Пікова потужність *DDoS*-

атак у першому півріччі 2024 року доссягла 1,7 Тбит/с. При цьому більшість атак є короткотривалими – до 20 хвилин, однак спостерігалися й атаки, що діяли протягом десятків годин. Так у 2023 році атака на аеропорти тривала майже три дні, а під час атаки на «Кихвстар» 12 грудня 2023 року хакер вивели з ладу головний пункт управління мережею «Київстар» і «знесди» конфігурацію на транзитних базових станціях, і відновлення тривало до 21 грудня. У серпні 2024 року сталася потужна атака на *Monobank,* яка проводилася повторюваними хвилями і тривала три дні.

За даними компанії *Cisco* тенденція до зростання кількості *DDoS*-атак, яка спостерігається протягом останніх років (рис. 1.2), зберігатиметься і у 2025 році може досягти 20 млн.

Найбільш атакованими галузями за результатами аналізу тенденцій *DDoS*-атак є фінансовий сектор, оскільки зловмисники часто намагаються перервати роботу банківських і фінансових систем. Часто атакуються IT та технологічні компанії, напади можуть спричинити значні збитки через втрачену продуктивність або порушення послуг. Телекомунікації — це ще одна галузь, що страждає від таких атак, оскільки зловмисники можуть спричинити збій у передачі даних або вивести з ладу важливі канали зв'язку. Урядові організації також часто є цільовими об'єктами атак, зокрема для досягнення політичних цілей або для завдання економічної шкоди.

*Cloudflare* зазначила, у третьому кварталі 2024 року Китай зайняв перше місце серед найбільш атакованих країн у світі. Цей рейтинг враховує *HTTP DDoS*-атаки, атаки на рівні мережі, загальний обсяг трафіку та відсоток трафіку *DDoS*-атак від загального трафіку. Після Китаю на другому місці опинилися Об'єднані Арабські Емірати, Гонконг – третє, за ними йдуть Сінгапур, Німеччина та Бразилія. Канада зайняла сьоме місце, за нею йдуть Південна Корея, США та Тайвань, які посіли десяте місце (рис. 1.3).


Рисунок 1.3 – Найбільш атаковані країни у третьому кварталі 2024 року

В Україні моніторингом кіберподій, розробкою і оприлюдненням найкращих методів протидії, а в окремих випадках і реалізацією цих методів, займається *CERT-UA* - урядова команда реагування на комп'ютерні надзвичайні події, яка діє при Державній службі спеціального зв'язку та захисту інформації (ДССЗЗІ). *CERT-UA* щоденно опрацьовує 200-300 кіберінцидентів та кібератак. За даними *CERT-UA* в Україні спостерігається значне зростання кількості *DDoS*-атак в умовах війни. У 2023 та на початку 2024 року ці атаки стали одним з основних кіберзагроз, з якими стикаються українські організації. Відзначається, що значна частина атак походить з Росії, а ці атаки мають на меті знищення або сповільнення критичної інфраструктури, а також ведення інформаційної війни. У листопаді-грудні 2024 року *CERT-UA* виявила серію нових *DDoS*-атак на державні установи хакерського угруповання *UAC*-0099.

## 1.3 Огляд законодавчих та нормативних актів, пов’язаних із захистом комп’ютерних мереж від *DDoS*-атак

### 1.3.1 Нормативні вимоги до забезпечення доступності інформації

Кібербезпека є складовою національної безпеки України згідно Закону України “Про національну безпеку України” [20] і Стратегії кібербезпеки України [41]. Однією з основних загроз інформаційній безпеці є порушення доступності даних, зокрема через *DDoS*-атаки. Україна активно накопичує досвід і вдосконалює свою нормативно-правову базу для захисту IT-інфраструктури від кіберзагроз у різних секторах економіки, зокрема особливу увагу приділяючи захисту критичної інформаційної інфраструктури.

Забезпечення безпеки інформації в таких сферах, як транспорт (морський, річковий, залізничний, авіаційний, автотранспорт), є важливою складовою підтримки стабільної роботи цих галузей. Наприклад, у судноплавстві *DDoS*-атаки на інформаційно-керуючі системи судна можуть спричинити аварії, викликані збоєм обладнання чи неправильними режимами роботи, що може призвести до попадання судна в небезпечні зони з рифами або мілинами. Атаки на інформаційно-керуючі системи аеропортів, залізниць або метрополітену можуть спричинити серйозні наслідки, такі як зіткнення транспортних засобів.

Управління транспортними галузями здійснюється органами, підпорядкованими Міністерству інфраструктури України. Одним з ключових завдань морської політики України є забезпечення безпеки судноплавства у внутрішніх водах та територіальному морі відповідно до міжнародного морського права та стандартів безпеки, як це визначено в «Морській доктрині України до 2035 року» [30]. Важливим аспектом є захист від *DDoS*-атак згідно з вимогами міжнародних та національних нормативно-правових актів.

У банківській сфері, відповідно до статті 67 Закону України «Про платіжні послуги» (прийнятий 4 квітня 2022 року) [23], система захисту інформації

повинна забезпечувати доступність даних, що обробляються, зберігаються або передаються під час виконання платіжних операцій. У разі порушення термінів виконання операцій через *DDoS*-атаки на платіжні системи, закон вимагає надання компенсації у вигляді пені. Для забезпечення стабільної роботи платіжних систем використовуються резервні сервери, криптографічні засоби та автоматизовані робочі місця.

Банківські автоматизовані системи зазвичай є розподіленими, тобто згідно НД ТЗІ 2.5-005-99 відносяться до третього класу. Для банківських систем повинні використовуватися комплекси засобів захисту (КЗЗ), які гарантують конфіденційність, цілісність і доступність даних. Ці вимоги віддзеркалюються у функціональних профілях захищеності формату 3. КЦД.х., рекомендованих НД ТЗІ 2.5-005-99 [32] для КС, що входять до складу автоматизованих систем, призначених для автоматизації банківської діяльності. Найбільш міцний захист забезпечується при реалізації п’ятої версії профілю: КЦД.5 = {КД-4, КА-4, КО1, КК-2, КВ-4, ЦД-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-5, НИ-2, НК2, НО-3, НЦ-3, НТ-2, НА-1, НП-1, НВ-2, НА-1, НП-1}.

В загальному випадку доступність гарантується при реалізації стандартних функціональних профілів захищеності наступних форматів: х.Д.х, х.КД.х, х.ЦД.х, х.КЦД.х. Наприклад:

1.Д.1 = { ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 };

2.КД.1 = { КД-2, КА-2, КО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2 }

В НД ТЗІ 2.5-004-99 [31] системи захисту інформації розглядаються як набори засобів, що реалізують певні набори функціональних послуг у відповідності до певного функціонального профілю захищеності (НД ТЗІ 2.5-00599). Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Згідно НД ТЗІ 2.5-005-99 [32] КС відповідає критеріям доступності, якщо її КЗЗ надає послуги щодо забезпечення на певному проміжку

часу можливості використання окремих функцій КС, оброблюваної в КС інформації і КС в цілому, а також щодо гарантування здатності КС функціонувати у випадку відмови її компонентів. Критеріями доступності оцінюваної КС є реалізація КЗЗ послуг, наведених в табл.1.2

Критерії [31] є методологічною базою для визначення вимог з захисту інформації при проектуванні та модернізації КС і оцінювання захищеності інформації в КС.

Порядок оцінки КС на предмет відповідності НД ТЗІ 2.5-004-99 і НД ТЗІ 2.5005-99, методики оцінювання функціональних послуг безпеки і реалізованих рівнів гарантій, методики порівняння оцінок захищеності КС, розроблених за вітчизняними і міжнородними нормативними вимогами, визначаються іншими нормативними документами:

–НД ТЗІ 2.7-009-09 «Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу»;

–НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу»;

–Положення про державну експертизу в сфері технічного захисту інформації;

–НД ТЗІ 2.7-013-2016 «Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам *ISO*/*IEC* 15408 з вимогами НД ТЗІ 2.5-004-99»;

–НД ТЗІ 2.6-002-2015 «Порядок зіставлення функціональних компонентів безпеки, визначених *ISO*/*IEC* 15408, з вимогами НД ТЗІ 2.5-004-99»;

– НД ТЗІ 2.6-003-2015 «Порядок зіставлення компонентів довіри до безпеки, визначених*ISO*/*IEC* 15408, з вимогами НД ТЗІ 2.5-004-99»;

Окремими НД ТЗІ визначаються особливості захисту інформації АС 2-го класу (НД ТЗІ 2.5-008-02) і *web*-сторінок (НД ТЗІ 2.5-010-03).

Таблиця 1.2 – Критерії доступності [31]

| Послуга | Позначення | Призначення | Принципи ранжування рівнів послуги | **Рівні** | | | Необхідні умови |
|---|---|---|---|---|---|---|---|
| **Використання ресурсів** | ДР | Дозволяє користувачам керувати використанням послуг і ресурсів | За повнотою захисту і вибірковістю керування доступністю послуг КС | **ДР-1. Квоти** | **ДР-2. Недопущення захоплення ресурсів** | **ДР-3. Пріоритетність використання ресурсів** | Реалізація послуги розподілу обов'язків рівня НО-1 «Виділення адміністратора» Реалізація послуги ідентифікації і автентифікації рівня НИ-1 «Зовнішня ідентифікація і автентифікація» |
| | | | | Найслабша форма контролю за використанням ресурсів. Всі захищені об'єкти КС (дисковий простір, час використання центрального процесора, тривалість сеансу тощо) повинні ідентифікуватись і контролюватись диспетчером доступу шляхом накладення обмежень на максимальний обсяг даного ресурсу, що може бути виділений користувачу. На даному рівні послуги немає гарантій, що користувач не зможе повністю захопити решту певного ресурсу, обмежуючи тим самим доступ до нього інших користувачів. | Реалізація більш досконалої форми квот. Квоти використовуються таким чином, щоб гарантувати, що жоден користувач не зможе захопити решту певного ресурсу, дозволяючи виділяти менші обсяги ресурсів, ніж максимальна квота користувача, гарантуючи таким чином іншому користувачеві доступ до розділюваного ресурсу. | Дозволяє управляти пріоритетністю використання ресурсів. Користувачі групуються адміністратором у групи за їх пріоритетами. У разі високого завантаження КС користувачі, що мають високий приорітет, отримують доступ до ресурсів КС за рахунок інших користувачів. | |
| **Стійкість до відмов** | ДС | Гарантує можливість використання інформації, окремих функцій або КС в цілому після відмови компонента КС. | За спроможністю КЗЗ забезпечити можливість функціонування КС в залежності від кількості відмов і послуг, доступних після відмови. | **ДС-1. Стійкість при обмежених відмовах** | **ДС-2. Стійкість з погіршенням характеристик обслуговування** | **ДС-3. Стійкість без погіршення характеристик обслуговування** | Реалізація послуги розподілу обов'язків рівня НО-1 «Виділення адміністратора» Реалізація послуги |
| | | | | Повинна бути визначена множина компонентів КС, до яких відноситься політика стійкості до відмов, і типи відмов | Політика стійкості до відмов, що реалізується КЗЗ, повинна відноситися до всіх компонентів КС | | |

Продовження таблиці 1.2

| Послуга | Позначення | Призначення | Принципи ранжування рівнів послуги | **Рівні** | | | Необхідні умови |
|---|---|---|---|---|---|---|---|
| | | КЗЗ має повідомляти адміністратора про відмову будь-якого захищеного компонента | Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниженняхарактеристик обслуговування або недоступності послуги | компонентів КС, після яких вона в змозі продовжувати функціонування. | | | ідентифікації і автентифікації рівня НИ-1 «Зовнішня ідентифікація і автентифікація» |
| | | | | Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг, а має в гіршому випадку проявлятися в зниженні характеристик обслуговування | Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг або до зниження характеристик обслуговування | | |
| **Гаряча заміна** | ДЗ | Гарантує доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Встановлення нової версії системи, відмова або заміна захищеного компонента не повинні призводити до того, що система потрапить до стану, коли політика безпеки, що реалізується нею, буде скомпрометована | За повнотою реалізації захисту | **ДЗ-1. Модернізація** | **ДЗ-2. Обмежена гаряча заміна** | **ДЗ-3. Гаряча заміна будь-якого компонента** | Реалізація послуги розподілу обов'язків рівня НО-1 «Виділення адміністратора» Реалізація послуги ідентифікації і автентифікації рівня НИ-1 «Зовнішня ідентифікація і автентифікація» Додатково для рівнів ДЗ-2 і ДЗ-3 - реалізація послуги стійкість до відмов рівня ДС-1 «Стійкість при обмежених відмовах», оскільки для того, |
| | | | | Політика гарячої заміни, повинна визначати політику проведення модернізації КС | Політика гарячої заміни повинна визначати множину компонентів КС, які можуть бути замінені без переривання обслуговування | Політика гарячої заміни повинна забезпечувати можливість заміни будь-якого компонента без переривання обслуговування | |
| | | | | Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію (*upgrade*) КС. Модернізація КС не повинна призводити до необхідності проводити реінсталяції КС або до переривання виконання КЗЗ функцій захисту | Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість замінити будь-який захищений компонент | | |

Продовження таблиці 1.2

<table>
<tr><th>Послуга</th><th>Позначення</th><th>Призначення</th><th>Принципи ранжування рівнів послуги</th><th colspan="3">Рівні</th><th>Необхідні умови</th></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="3"></td><td>гарячої заміни компонента, система повинна забезпечувати свою працездат-ність у разі відмови даного компонента.</td></tr>
<tr><td rowspan="3">Відновлення після збоїв</td><td rowspan="3">ДВ</td><td rowspan="3">Забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування Відновлення може вимагати втручання оператора, а для її більш високих рівнів реалізації КЗЗ може продукувати відновлення працездатності автоматично. Якщо відновлення неможливе, то КЗЗ повинен переводити систему до</td><td rowspan="3">За ступенем автоматизації процесу відновлення</td><td>ДВ-1. Ручне відновлення</td><td>ДВ-2. Автоматизоване відновлення</td><td>ДВ-3. Вибіркове відновлення</td><td rowspan="3">Реалізація послуги розподілу обов'язків рівня НО-1 «Виділення адміністратора» Реалізація послуги ідентифікації і автентифікації рівня НИ-1 «Зовнішня ідентифікація і автентифікація»</td></tr>
<tr><td colspan="3">Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС</td></tr>
<tr><td>Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження</td><td>Після відмови КС або переривання обслуго-вування КЗЗ має бути здатним визначити, чи можуть бути використані автоматизовані процедури для повернення КС до нормального функціонування безпечним чином. Якщо такі процедури можуть</td><td>Після будь-якої відмови КС або переривання обслуговування, що не призводить до необхідності реінсталювати КС, КЗЗ повинен бути здатним виконати необхідні процедури і безпечним чином повернути КС до нормального функціонування.</td></tr>
</table>

Продовження таблиці 1.2

| Послуга | Позначення | Призначення | Принципи ранжування рівнів послуги | **Рівні** | | | Необхідні умови |
|---|---|---|---|---|---|---|---|
| | | стану, з якого її може повернути до нормального функціонування тільки адміністратор | | | бути використані, то КЗЗ має бути здатним виконати їх і повернути КС до нормального функціонування | режимі з погіршеними характеристиками обслуговування | |
| | | | | | Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження | | |
| | | | | Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування | | Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС з погіршеними характеристиками обслуговування в режим нормального функціонування | |

1.3.2 Особливості гарантування доступності інформації в автоматизованих системах другого класу

До другого класу автоматизованих систем (АС) згідно [32] відносяться локалізовані багатомашинні багатокористувачеві комплекси, що обробляють інформацію різних категорій конфіденційності, тобто в таких КС наявні користувачі з різними повноваженнями по доступу і/або технічні засоби, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності, але відсутній вихід в глобальну мережу (відсутня зміна політики безпеки). Прикладом АС класу 2 є локальна обчислювальна мережа організації.

Для АС класу 2 в НД ТЗІ 2.5-008-02 [33] визначаються такі стандартні функціональні профілі захищеності оброблюваної інформації, що забезпечують доступність інформації:

– при наявності підвищених вимог до забезпечення конфіденційності та доступності оброблюваної інформації: 2.КД.1а = {КД-2, КА-2, КО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2};

– при наявності підвищених вимог до забезпечення конфіденційності, цілісності та доступності оброблюваної інформації: 2.КЦД.2а = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2}.

В НД ТЗІ 2.5-008-02 [33] введено ряд визначень, що використовуються в цьому нормативному документі для формулювання вимог до КЗЗ:

«Сильнозв’язані об’єкти - сукупність наборів даних, що характеризується наявністю мінімальної надлишковості і допускають їх оптимальне використання одним чи декількома процесами як одночасно, так і в різні проміжки часу і вимагають безумовного забезпечення цілісності цих наборів даних як сукупності.» «Фактично сильнозв’язаними об’єктами можуть бути бази даних, що підтримуються стандартними для галузі системами управління, сукупності наборів даних, які генеруються й модифікуються будь-якими функціональними

або системними процесами і кожний з наборів даних, які складають цю множину, не може самостійно оброблятися, зберігатися і передаватися.»

«Слабозв'язані об'єкти – відносно незалежні набори даних, що генеруються, модифікуються, зберігаються й обробляються в АС.»

«Фактично слабозв'язані об'єкти - це інформаційні структури, представлені у вигляді окремих файлів, що підтримуються штатними операційними системами робочих станцій та серверів, і кожний з них може оброблятися, зберігатися й передаватися як самостійний об'єкт.»

Вимоги, сформульовані в [33] до забезпечення КЗЗ доступності оброблюваної інформації, зведені в табл.1.3.

### 1.3.3 Особливості забезпечення доступності інформації на *web*-сторінках

В НД ТЗІ 2.5-0010-03 [34] розглядаються дві технології, які різняться за вимогами до КЗЗ:

– технологія Т1: *web*-сервер і робочі станції розташовуються на території установи-власника *web*-сторінки або на території оператора;

– технологія Т2: *web*-сервер розташовується у оператора, а робочі станції – на території власника *web*–сторінки. Взаємодія робочх станцій з *web*-сервером здійснюється з використанням мереж передачі даних.

Відмінність технологій Т1 і Т2 полягає у способі передачі інформації від робочої станції до *web*-сервера: при застосуванні технології Т2 передача інформації здійснюється крізь незахищене і неконтрольоване середовище висуваються додаткові вимоги щодо ідентифікації та автентифікації між КЗЗ робочої станції й КЗЗ *web*-сервера під час спроби розпочати обмін інформацією та забезпечення цілісності інформації при обміні.

Політика безпеки інформації в АС поширюється на об'єкти КС, які мають безпосередній чи опосередкований вплив на безпеку інформації. До таких об'єктів належать:

Таблиця 1.3 – Вимоги до КЗЗ АС класу 2 щодо забезпечення доступності інформації

| Послуга | Рівень послуги | Політика, що реалізується КЗЗ | |
|---|---|---|---|
| | | Область застосування | Зміст |
| Використання ресурсів КЗЗ | ДР-1 | – сильно- та слабозв'язані об'єкти, що містять інформацію будь-яких категорій;<br>– файлова система (логічні диски, каталоги, підкаталоги тощо);<br>– системне та функціональне програмне забезпечення;<br>– технологічна інформація щодо управління АС;<br>– окремі периферійні пристрої (принтери, накопичувачі інформації, змінні носії інформації і т.п.);<br>─обчислювальні ресурси АС | Забезпечує взаємодію об’єктів області застосування, передбачаючи можливість встановлення обмежень на їх використання користувачами всіх категорій.<br>Обмеження щодо використання окремим користувачем та/або процесом обсягів обчислювальних ресурсів АС або кількості об’єктів встановлюються адміністратором безпеки або користувачами, яким надано повноваження інших адміністраторів.<br>Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів.<br>Спроби користувачів перевищити встановлені обмеження на використання ресурсів повинні реєструватися в системному журналі. |
| Стійкість до відмов КЗЗ | ДС-1 | – сильно- та слабозв'язані об'єкти, що містять конфіденційну інформацію;<br>– файлова система (логічні диски, каталоги, підкаталоги тощо);<br>– системне та функціональне ПЗ;<br>– технологічна інформація КСЗІ;<br>– технологічна інформація щодо управління АС;<br>─окремі периферійні пристрої (принтери, накопичувачі інформації, змінні носії інформації і т.ін.) | Забезпечує взаємодію об’єктів області застосування.<br>Послуга гарантує доступність АС в цілому або окремих її об'єктів і процесів після відмови якогось компонента АС.<br>Розробниками АС повинен бути виконаний аналіз можливих відмов компонентів АС.<br>Адміністратор безпеки (служба захисту інформації) спільно з користувачами, яким надано повноваження інших адміністраторів, повинен проаналізувати стійкість окремих компонентів АС до відмов та визначити:<br>- множину компонентів АС, що є критичними стосовно забезпечення стійкого функціонування, та типи відмов цих компонентів, після яких АС здатна продовжувати функціонування;<br>- рівні відмов, у разі перевищення яких відмови призводять до погіршення характеристик обслуговування або недоступності послуг.<br>Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг і, в гіршому випадку, має виявлятися в погіршенні характеристик обслуговування користувачів.<br>КЗЗ повинен мати можливість реєстрації факту відмови будь-якого захищеного компонента АС та повідомлення щодо цієї події адміністратора безпеки та/або іншого адміністратора. |
| Гаряча заміна | ДЗ-1 | – системне та функціональне ПЗ;<br>– засоби захисту інформації та засоби управління КСЗІ;<br>─засоби адміністрування та управління обчислювальною системою АС; | Забезпечує взаємодію об’єктів області застосування.<br>Послуга гарантує, що модернізація АС (встановлення нової версії програмного або апаратного забезпечення, заміна захищеного компонента та ін.) не призведе до компрометації політики безпеки інформації в АС. |

Продовження таблиці 1.3

| Послуга | Рівень послуги | Політика, що реалізується КЗЗ | |
|---|---|---|---|
| | | Область застосування | Зміст |
| | | – окремі периферійні пристрої (принтери, накопичувачі та змінні носії інформації і т.ін.), які задіяні для обробки службової інформації | Політика проведення модернізації АС повинна надавати можливість провести модернізацію АС адміністратору безпеки, уповноваженим співробітникам СЗІ, іншим адміністраторам (адмністратору операційної системи, адміністратору баз даних, адміністраторам сервісів та ін.), а також визначати для кожного з них повноваження та множину виконуваних ними допустимих операцій з метою модернізації АС.<br>Модернізація окремих компонентів АС не повинна призводити до необхідності проведення повторної інсталяції програмного забезпечення цих компонентів або до переривання виконання КЗЗ функцій захисту. |
| Відновлення після збоїв | ДВ-1 | ─системне та функціональне ПЗ;<br>─засоби захисту інформації та засоби управління КСЗІ;<br>─засоби адміністрування та управління обчислювальною системою АС;<br>─окремі периферійні пристрої (принтери, накопичувачі інформації, змінні носії інформації і т.і.), які задіяні для обробки службової інформації | Забезпечує взаємодію об'єктів області застосування.<br>Послуга гарантує повернення АС у відомий захищений стан після відмов або переривання обслуговування, спричинених помилковими діями користувачів, неврахованою функціональною недостатністю програмного та апаратного забезпечення (наприклад, можливою наявністю не виявлених під час проектування незадекларованих функцій), іншими непередбачуваними ситуаціями.<br>Політикою відновлення після збоїв повинна бути визначена й задокументована множина типів відмов і переривань обслуговування АС або окремих її компонентів, після яких можливе повернення у відомий захищений стан без порушення політики безпеки.<br>Для кожної з відмов повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція АС.<br>Після відмови АС або окремих її компонентів, або переривання обслуговування КЗЗ повинен перевести АС або окремі її компоненти до стану, із якого повернути до нормального функціонування може тільки адміністратор безпеки, інші адміністратори або співробітники СЗІ.<br>Повинні бути визначені повноваження адміністратора безпеки, уповноважених співробітників СЗІ, інших адміністраторів (адміністратора операційної системи, адміністратора баз даних, адміністраторів сервісів та ін.) та множина виконуваних ними допустимих операцій з метою повернення АС у відомий захищений стан.<br>Повернення АС (окремих компонентів) із режиму, що визначається погіршеними характеристиками обслуговування, в режим нормального функціонування повинно здійснюватися за допомогою ручних (не автоматизованих) процедур |

Відмінність технологій Т1 і Т2 полягає у способі передачі інформації від робочої станції до *web*-сервера: при застосуванні технології Т2 передача інформації здійснюється крізь незахищене і неконтрольоване середовище висуваються додаткові вимоги щодо ідентифікації та автентифікації між КЗЗ робочої станції й КЗЗ *web*-сервера під час спроби розпочати обмін інформацією та забезпечення цілісності інформації при обміні.

Політика безпеки інформації в АС поширюється на об’єкти КС, які мають безпосередній чи опосередкований вплив на безпеку інформації. До таких об’єктів належать:

– адміністратор безпеки та співробітники служби захисту інформації;

– користувачі, яким здійснюють управління АС, і яким надані відповідні повноваження;

– користувачі, що мають права доступу тільки до загальнодоступної інформації;

– інформаційні об’єкти, що містять загальнодоступну інформацію;

– системне та функціональне ПЗ, яке використовується в АС для обробки інформації або для забезпечення функцій КЗЗ;

– технологічна інформація КСЗІ (дані про мережеві адреси, імена, персональні ідентифікатори та паролі користувачів, їхні повноваження та права доступу до об’єктів, встановлені робочі параметри окремих механізмів або засобів захисту, інша інформація баз даних захисту, інформація журналів реєстрації дій користувачів тощо);

– засоби адміністрування і управління обчислювальною системою АС та технологічна інформація, яка при цьому використовується;

– обчислювальні ресурси АС, захоплення яких окремим користувачем або безконтрольне використання може призвести до блокування роботи АС в цілому або компонентів АС, блокування роботи інших користувачів. Прикладами таких

обчислювальних ресурсів є дисковий простір, час використання центрального процесора, тривалість сеансу роботи користувача із засобами АС тощо.

Для *web*-сторінок в НД ТЗІ 2.5-0010-03 [34] визначаються два мінімально необхідні функціональні профіля захищеності, що відповідають різним технологіям і враховують особливості надання доступу до інформації *web*-сторінки, типові характеристики середовищ функціонування АС та особливості технологічних процесів обробки інформації:

– технологія Т1: { КА-2, ЦА-1, ЦО-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1};

– технологія Т2: 2.КЦД.2а = { КА-2, КВ-1, ЦА-1, ЦО-1, ЦВ-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1,НЦ-1, НТ-1, НВ-1}.

В обох цих профілях доступність інформації забезпечується за рахунок послуг використання ресурсів рівня ДР-1 та відновлення після збоїв рівня ДВ-1. Вимоги, сформульовані в [34] до забезпечення КЗЗ доступності оброблюваної інформації, зведені в табл.1.4, в якій для кожного рівня послуг вказано область застосування і зміст послуги.

Власник *web*-сторінки має право, у разі необхідності, реалізувати окремі послуги безпеки інформації профілів, визначених НД ТЗІ 2.5-0010-03 [34], з більш високим рівнем чи доповнити ці профілі іншими послугами. Власник *web*-сторінки також має право реалізувати послуги безпеки з більш високим рівнем гарантій, наприклад, не ДВ-1 «Ручне відновлення», а ДВ-2 «Автоматизоване відновлення».

«У тих випадках, коли в АС вимоги до політики реалізації якоїсь з послуг безпеки забезпечуються організаційними або іншими заходами захисту, які в повному обсязі відповідають встановленим НД ТЗІ 2.5-004 специфікаціям для певного рівня послуги безпеки, то рівень такої послуги, що входить до визначених профілів захищеності, може бути знижений на відповідну величину» [34].

Таблиця 1.4 – Вимоги до КЗЗ *web*-сторінок щодо забезпечення доступності інформації

| Послуга | Рівень послуги | Політика, що реалізується КЗЗ | |
|---|---|---|---|
| | | Область застосування | Зміст |
| Використання ресурсів КЗЗ | ДР-1 | – користувачі загальнодоступної інформації;<br>– адміністратор безпеки та користувачі, яким надано повноваження щодо управління АС;<br>– файлова система;<br>– системне та функціональне ПЗ;<br>– технологічна інформація щодо управління АС;<br>– окремих периферійні пристрої (принтери, накопичувачі інформації тощо.);<br>–обчислювальних ресурсів АС | Передбачає можливість встановлення обмежень на використання об'єктів області застосування.<br>Обмеження щодо використання окремим користувачем та/або процесом обсягів обчислювальних ресурсів АС або кількості об'єктів встановлюються адміністратором безпеки або користувачами, яким надано повноваження щодо управління АС.<br>Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від зазначених користувачів.<br>Спроби користувачів перевищити встановлені обмеження на використання ресурсів повинні реєструватися в системному журналі. |
| Відновлення після збоїв | ДВ-1 | –системне та функціональне ПЗ;<br>–засоби захисту інформації та засоби управління КСЗІ;<br>–засоби адміністрування та управління обчислювальною системою АС | Гарантує повернення АС у відомий захищений стан після відмов або переривання обслуговування, спричинених помилковими діями користувачів, неврахованою функціональною недостатністю програмного та апаратного забезпечення (наприклад, можливою наявністю не виявлених під час проектування незадекларованих функцій), іншими непередбачуваними ситуаціями.<br>Політика відновлення, яка реалізується КЗЗ, повинна визначати множину типів відмов *web*-сторінки і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки.<br>Для кожної з відмов повинні бути чітко визначені і задокументовані рівні відмов, у разі перевищення яких необхідна повторна інсталяція *web*-сторінки.<br>Після відмови *web*-сторінки або переривання обслуговування, КЗЗ повинен перевести *web*-сторінку до стану, з якого повернути її в режим нормального функціонування може тільки адміністратор безпеки і користувачі, які мають повноваження щодо управління АС. Для кожного з них повинна бути визначена множина допустимих виконуваних ними операцій з метою повернення АС у відомий захищений стан.<br>Повернення АС з режиму, що визначається погіршеними характеристиками обслуговування, в режим нормального функціонування повинно здійснюватися за допомогою ручних (не автоматизованих) процедур. |

### 1.3.4 Індикатори кіберзагроз

Індикатори кіберзагроз (англ. *Indicator of Compromise, або IoC*) - це ознаки або артефакти, які вказують на можливу компрометацію системи або мережі. Вони можуть бути використані для виявлення, аналізу та запобігання кіберзагрозам.

Існують різні типи індикаторів, серед яких можна виділити *IP*-адреси, домени, *URL*-адреси, хеші файлів, порти та протоколи, електронні листи, шляхи файлів, ключі реєстру (для *Windows*), невідомі процеси та підвищений рівень активності, а також аномальні мережеві запити.

Сумнівні або відомі зловмисні *IP*-адреси, з яких здійснюється доступ або атаки на систему, можуть бути індикаторами кіберзагроз, подібно до зловмисних доменів, які використовуються для фішингу, передачі шкідливого ПЗ або командного управління.

Шкідливі *URL*-адреси, що ведуть до фішингових сайтів чи сайтів для розповсюдження шкідливого ПЗ, також є важливими індикаторами.

Хеші файлів, зокрема *MD5, SHA-1, SHA-256*, використовуються для ідентифікації шкідливих програм або документів, що дозволяє швидко визначити, чи є файли на комп'ютері чи сервері шкідливими.

Використання специфічних портів або протоколів для несанкціонованого доступу може також бути ознакою кіберзагрози, так само як і підозрілі електронні листи, зокрема підроблені адреси відправників або шкідливі вкладення. Зміни в шляху файлів, які зазвичай не використовуються в нормальній роботі, але з’являються під час атак, можуть свідчити про інфікування системи.

Ключі реєстру *Windows*, що змінюються, можуть бути ще одним індикатором наявності шкідливого ПЗ. Аномальна активність на системі, така як підвищене використання ресурсів без очевидної причини, а також створення нових процесів, також можуть свідчити про кіберзагрозу.

Неавторизовані або аномальні мережеві запити, які вказують на спроби шкідливого ПЗ підключитися до віддаленого сервера, є важливими індикаторами. Індикатори кіберзагроз використовуються для розслідування інцидентів безпеки та для автоматизованого виявлення і реагування на загрози.

# 2 ДОСЛІДЖЕННЯ МЕТОДІВ І ЗАСОБІВ ПРОВЕДЕННЯ *DDoS*-АТАК

## 2.1 Інструменти для здійснення *DDoS*-атак

### 2.1.1 Експлойти

*DoS*-атаки поділяються на локальні та віддалені. Для локальної *DoS*-атаки зловмиснику необхідно отримати права доступу до об'єкта атаки на рівні, достатньому для захоплення ресурсів.

Інструментами локальних атак є різні експлойти, які ініціюють процеси, що вичерпують ресурси процесора і пам'яті, наприклад, форк-бомби; програми, що відкривають дуже багато файлів чи якийсь циклічний алгоритм тощо.

Експлойт (англ. *exploit* – експлуатувати) – це ПЗ або послідовність команд, які призначені для проведення атаки на КС шляхом експлуатації (використання) вразливостей в ПЗ жертви. Метою застосування експлойта може бути захоплення контролю над атакованою КС (несанкціоноване підвищення привілеїв) або порушення її функціонування, прикладом якого є *DoS*-атака.

Експлойти можуть бути класифіковані за наступними ознаками.

За методом отримання доступу до уразливого ПЗ розрізняють:

– віддалені (англ. *remote*) експлойти, які отримують доступ до вразливості через мережу;

– локальні (англ. *local*) експлойти, які вимагають наперед отриманого доступу до КС-жертви і запускаються безпосередньо у вразливій системі.

За цільовими компонентами обчислювальної системи виділяють експлойти, які спрямовані на:

– клієнтські програми. Експлуатація вразливості клієнта здійснюється за більш складним алгоритмом, оскільки необхідно змусити жертву підключитися до підробленого сервера, наприклад, якщо потенційна жертва (уразливий клієнт) є

браузером, то слід умовити жертву (часто з використанням методів соціальної інженерії) перейти за певним посиланням;

– серверні програми. При наявності серверної уразливості експлойту для реалізації певних етапів атаки достатньо сформувати та надіслати на сервер запит із зловмисним кодом;

– модулі операційної системи.

За типом використовуваної вразливості розрізняють експлойти на основі:

– переповнення буфера,

– *SQL* ін'єкції,

– міжсайтовий скриптинг,

– підробку міжсайтових запитів тощо

За метою втручання в роботу системи розмежування прав:

– отримання прав суперкористувача (адміністратора, *root*);

– отримання низькорівневих прав доступу;

– несанкціоноване підвищення рівня прав доступу.

За типом мови програмування, на якій створено експлойт:

– експлойти, створені на компільованій мові програмування;

– експлойти, створені на скриптовій мові програмування.

За мовою програмування, на якій створено експлойт: найчастіше використовуються *C/C++*, *Perl*, *PHP*, *HTML+JavaScript*.

За способом представлення експлойтів в процесі поширення розрізняють експлойти у вигляді:

– словесного опису способу використання вразливості;

– виконуваних модулів;

– «сирцевих» кодів – фрагментів коду, які для виконання мають бути перетворені у машинний код за допомогою компілятора для певної комп'ютерної архітектури або можуть виконуватися безпосередньо за текстом в разі використання інтерпретатора;

### 2.1.2 *Fork*-бомби

В *Unix* і *UNIX*-подібних операційних системах *fork* - це системний виклик, який реалізований зазвичай на рівні ядра операційної системи і створює новий процес. В таких операційних системах це основний метод створення процесу.

*Fork*-бомба – це цілеспрямовано написана або помилково створена програма, яка системним викликом *fork*() створює свої копії, які, в свою чергу також створюють свої копії і так далі до нескінченності. В результаті рекурсивного лавиноподібного породження процесів навантаження на обчислювальну систему зростає, і нестача таких системних ресурсів як дескриптори процесів, пам'яті, процесорного часу може призвести до відмови в обслуговуванні.

При спрацьовуванні *fork*-бомба:

– намагається заповнити власними копіями вільне місце у списку активних процесів операційної системи;

– унеможливлює старт корисних програм внаслідок відсутності вільного місця у списку активних процесів операційної системи;

– робить малоймовірним успішний старт корисної програми навіть у випадку, якщо якійсь активний процес припинить роботу і звільнить місце в списку процесів, оскільки на цей момент є величезна кількість копій *fork*-бомби, що готові запустити свою чергову копію;

– може заповнювати не тільки список процесів, а й віртуальну пам'ять, процесорний час, сокети та інші системні ресурси.

Результатом вичерпання системних ресурсів стає поступове уповільнення роботи комп'ютера аж до зависання - практичної зупинки операційної системи і/або корисних програм.

До наслідків, подібних до ефекту дії *fork*-бомби, може привести й проста помилка програмування. Наприклад, у нескінченний цикл створення власних копій для обробки пакета або з'єднання може потрапити програма, яка слухає мережевий порт, при отриманні мережевого пакету або при встановленні з'єднання.

2.1.3 Інтернет-ресурси організації *DDoS*-атак

Для організації *DDoS*-атак за даними компанії *TechUkraine.net* найкращими безкоштовними інструментами *DDoS*-атак в Інтернеті є засоби, наведені в табл.2.1. Більшість перелічених у табл.2.1 інструментів призначені для *DDoS*-атаки у *Windows*, але деякі доступні й в інших операційних системах (*Linux, macOS*).

Існують програми, які призначені для *GAS* (англ. *generalized audit software* - аудиторське ПЗ загального призначення) на основі *LOIC*. Форк *LOIC*, що активно розробляється і містить код біля 10 різних версій атак. Має консольну версію, що дозволяє атакувати з сервера. Працює ефективніше за оригінальну версію:

– *IRC-LOIC*, забезпечує анонімність в *Operation Payback*. Вимагає *Windows* та *.NET* не нижче версії 3.5. Від звичайного *LOIC* відрізняється наявністю «режиму хайвмайнда»: можливістю синхронізації через *IRC* або *Twitter* для одночасної атаки на один сайт-жертву десятків тисяч комп'ютерів. Тобто утворюється добровільний ботнет. Однак, *IRC*-канал та *Twitter* є доступними будь-кому, що дозволяє агентам *ZOG* легко припиняти атаку при виявленні джерела загрози;

– *LOIC Hive Mind*,що може отримувати завдання на атаку автоматично через *IRC, RSS* або *Twitter*;

– *HOIC*, описаний в табл.2.1.

Існують унікальні засоби *DDoS*, часто створені для атак певної групи атакуючих, і універсальні засоби.

Прикладами універсальних «іонних гармат» є:

– *JavaLOIC* - клон *LOIC*, написаний на *Java*. Працює так само як *LOIC*, *.NET* не вимагає. Хайвмайнд має тільки через *Twitter*. У цілому не дуже корисний;

– *LOIQ* - повноцінна альтернатива *LOIC* на *C++/Qt*4. Має синхронізацю через *IRC* та локалізацію (різні мови інтерфейсу);

– *JS-LOIC* - *LOIC* для мобільного телефону. Не вимагає ніяких завантажень та інсталяції, працює з будь-якої операційної системи, де є браузер. Однак, ефективність *JS-LOIC* нижча за *LOIC* навіть у першій версії.

Таблиця 2.1 – Безкоштовні засоби організації *DDoS*-атак

| № | Назва | Принципи дії | Особливості |
|---|---|---|---|
| 1 | *HULK* (*HTTP Unbearable Load King* - Король непосильного навантаження) | Надсилає унікальний і незрозумілий і трафік на *web*-сервер.<br>*HULK* стверджує, що ПЗ створене лише для дослідницьких цілей | На цільовий *web*-сервер генерується великий обсяг унікального трафіку.<br>Вражає безпосередньо пул ресурсів серверів, минаючи систему кешу.<br>Важко, але можливо виявити<br>Трафік може бути заблокованй<br>Зловмисник не може бути повністю анонімним |
| 2 | *Tor's Hammer* (Молот Тора) | Створений для тестування, може бути використаний для повільної пост-атаки. Цільові сервери - *IIS* і *Apache* | Працює на рівні 7 моделі *OSI*<br>Спеціалізується на анонімних атаках.<br>Вкористовується для проведення демонстраційних атак на структури безпеки при пен-тестуванні. |
| 3 | THC-SSL-DOS (*The Hacker's Choice SSL Denial of Service* Атака відмови в обслуговуванні *SSL* від *The Hacker's Choice*) | Генерує велику кількість запитів на встановлення *SSL/TLS* з'єднання<br>Технічно атака здійснюється через неповне завершення процесу *handshake* (обміну ключами та аутентифікації) *SSL/TLS*. | Користувачі можуть перевірити ефективність *SSL*.<br>Також використовує функцію безпечного повторного узгодження *SSL*.<br>Підтримує *Linux, Windows* і *macOS*. |
| 4 | *LOIC* ( *Low Orbit Ion Cannon* Низькоорбітальна іонна гармата) | Засіб стресового тестування.<br>Надсилає на сервери *HTTP*, *UDP* і *TCP* запити.<br>Цільовий *web*-сайт припиняє роботу протягом кількох секунд після початку атаки | В основному використовується для атак на невеликі сервери.<br>Написана на C#.<br>Доступно для *Linux, Windows* і *Android*.<br>Для роботи під *Windows* потрібно мати *.NET* версії не нижче 2.0. Для роботи під *Linux – Mono*.<br>Простий у використанні інтерфейс.<br>Не приховує *IP*-адресу атакуючого навіть після використання проксі-сервера.<br>Існують різні редакції програми з різними функціональними можливостями і для різних галузей застосування |

Продовження таблиці 2.1

| № | Назва | Принципи дії | Особливості |
|---|---|---|---|
| 5 | *RU-Dead-Yet* (РУДІ, *RU* ще мертвий) | Автоматично переглядає цільовий сайт *DDoS*, знаходить вбудовані *web*-форми і надсилає поля довгої форми, що знижує швидкість трафіку | Працює повільно, виконує короткі повільні атаки.<br>Виконує лише один тип атаки на рівні 7 *OSI*.<br>Важко виявляється.<br>Має інтерактивне меню консолі. |
| 6 | *PyLoris* | Засіб перевірки вразливості сервера до одночасної підтримки сукупності багатьох з'єднань *TCP*, на які є обмеження. Така вразливість найчастіше присутня у службах, які витрачають на з'єднання багато пам'яті або здійснюють обробку з'єднання в незалежних потоках | Цілями атаки можуть бути *SMTP, HTTP, FTP, Telnet* і *IMAP*.<br>Має простий у використанні інтерактивний інтерфейс.<br>Використовує *SOCK*-проксі та *SSL*-з'єднання. |
| 7 | *DDOSIM* (*DDoS Simulater* - Симулятор розподіленої відмови в обслуговуванні) | Імітує *DDoS*-атаки на мережі та *web* –сайти.<br>Імітує зомбі-хости з різними *IP*-адресами. Копіює різні хости-зомбі, після чого хости-зомбі встановлюють з об'єктом атаки повне *TCP*-з'єднання. Після завершення з'єднання *DDOSIM* починає діалог із прослуховуючим додатком (наприклад, *HTTP*-сервером) | *HTTP DDoS*-атаки можуть здійснюватися за допомогою дійсних запитів.<br>*DDoS*-атаки можуть здійснюватися за допомогою хибних запитів.<br>Працює на *Linux* і *Windows*.<br>Працє на рівні 7 моделі *OSI*.<br>Атаки на основі *TCP*<br>Моделювання декількох зомбі.<br>Використовує випадкові вихідні *IP*-адреси. |
| 8 | *DAVOSET* | Здійснює атаки на *web*-сайти шляхом отримання доступу через інші сайти. Широко використовується хакерами | Забезпечує підтримку файлів *cookie*.<br>Безкоштовне програмне забезпечення, яке надає інтерфейс командного рядка для здійснення атаки.<br>Проводить атаку з використанням зовнішніх об'єктів *XML*. |
| 9 | *GoldenEye* (Золоте око) | Здійснює атаки на сервери шляхом надсиання жертві *HTTP*-запиту і використання всіх сокетів *HTTP/S*, | Утворює змішаний трафік на основі рандомізації *GET*, *POST*.<br>Написаний на *Python*.<br>Простий у використанні. |

Продовження таблиці 2.1

| № | Назва | Принципи дії | Особливості |
|---|---|---|---|
| | | наявних на сервері-жертві для *DDoS*-атаки | результат, інструменту не потрібно використовувати багато трафіку Створює повне *TCP*-з'єднання, а потім вимагає лише кілька сотень запитів через тривалі та регулярні проміжки часу. Як, щоб вичерпати доступні з'єднання на сервері-жертві. |
| 10 | *OWASP HTTP POST* | Дозволяє перевірити стійкість *web* – програм до атак *HTTP GET* і *HTTP POST* (перевірити мережеву продуктивність). *HTTP*-запит *POST* включає тіло повідомлення на додаток до *URL*-адреси, яка використовується для вказівки інформації про дію, що виконується. Частина *HTTP*-заголовка є повною та повністю надсилається на *web*-сервер, отже обходячи внутрішній захист *IIS*. | Був створений, щоб подолати недоліки інших інструментів HTTP-атаки, таких як *Slowloris* і *PyLoris*.<br>Ввикористовує запити *HTTP POST* замість запитів *HTTP GET* для атаки на ціль, оскільки:<br>–системи захисту від *DDoS* можуть використовувати відкладене зв'язування або з'єднання *TCP* для захисту від атак *HTTP GET*;<br>–*HTTP GET DDoS*-атаки не працюють на *web*-серверах *IIS* або *web*-серверах з обмеженнями часу очікування для заголовків *http*;<br>–від *HTTP GET DDoS*-атаки легко захистити за допомогою популярних балансувальників навантаження, таких як *F5* і *Cisco*, зворотних проксі та певних модулів *Apache*, таких як *mod_antiloris*.<br>Користувачі можуть обрати потужність сервера.<br>Безкоштовне використання навіть у комерційних цілях.<br>Дозволяє користувачу протестувати стійкість до атак прикладного рівня. |
| 11 | *XOIC (High Orbit Ion Cannon* Високоорбітальна іонна гармата) | Здійснює атаки на невеликі *web* - сайти шляхом надсилання жертві повідомлень *ICMP, UDP, HTTP* або *TCP*. Виконує *DoS* -атаку на будь-який сервер із *IP*-адресою, вибраним користувачем портом і вибраним користувачем протоколом. | Здійснює *DoS*-атаки за допомогою повідомлень *ICMP, UDP, HTTP* або *TCP*.<br>Має три вбудовані режими атаки:<br>–режим тестування;<br>–звичайний режим атаки *DoS*;<br>–*DoS*-атака з повідомленнями *TCP, HTTP, UDP* або *ICMP*.<br>Атаки, які здійснює *Xoic*, можна легко виявити та заблокувати.<br>Дуже простий у використанні. |

Продовження таблиці 2.1

| № | Назва | Принципи дії | Особливості |
|---|---|---|---|
| 12 | *HOIC (High Orbit Ion Cannon* Високоорбітальна іонна гармата) | Заміна *LOIC*. Заповнює цільову систему небажаними запитами, щоб не можна було обробити корисний запит. Використовує *HTTP* флуд (в тому числі *POST/GET* запити), змушуючи сервер-жертву генерувати у відповідь трафік, що за об'ємом набагато перевищує отриманий.<br>Може одночасно виконувати 256 сеансів атаки.<br>змушуючи сервер-жертву генерувати у відповідь трафік, що за об'ємом набагато перевищує отриманий.<br>Може одночасно виконувати 256 сеансів атаки. | Абсолютно безкоштовний у використанні.<br>Доступний для *Windows, Mac* і *Linux*.<br>Вимагає *Windows*, але не вимагає *.NET*, завдяки чому працює під *Wine*.<br>Дозволяє користувачам контролювати атаки з низькими,<br>Вимагає *Windows*, але не вимагає *.NET*, завдяки чому працює під *Wine*.<br>Дозволяє користувачам контролювати атаки з низькимисередніми та високими налаштуваннями.<br>Хайвмайнда не має.<br>Має серйозний витік пам'яті при атаці у порівнянні з *LOIC*.<br>Внаслідок чого може використовуватися доти, поки файл підкачки не досягне максимального розміру, тобто недовго |
| 13 | *Hyenae* (Гієни) | Гнучкий, платформенно-незалежний генератор мережевих пакетів. Дозволяє створювати кілька сценаріїв *MITM, DoS* і *DDoS*-атак. Постачається з кластеризованим віддаленим демоном і інтерактивним помічником для атак | Демон для налаштування мереж віддаленої атаки<br>Інтелектуальне виявлення адреси та адресного протоколу<br>Конфігурація адреси пакета на основі шаблону<br>Інтелектуальна рандомізація на основі шаблонів підстановки певних підстановочних знаків<br>Злам активного маршрутизатора *Cisco HSRP*<br>Підтримка *HyenaeFE QT-Frontend*<br>Дуже багато функцій:<br>– *ARP*-запит флуд;<br>– отруєння *ARP*-кешу;<br>– лавинне розсилання ініціювання сеансу *PPPoE*.<br>– сліпе завершення сеансу *PPPoE*;<br>– *ICMP*-луна-флуд; скидання з'єднання *TCP* на основі *ICMP*; |

Продовження таблиці 2.1

| № | Назва | Принципи дії | Особливості |
|---|---|---|---|
| 14 | *THC-SSL-DOS* | Перевіряє продуктивність *SSL*. Здійснює атаку на цільовий *web*-сайт, вичерпує всі *SSL*-з'єднання та | Підтримує *Linux, Windows* і *MacOS*. Користувачі можуть перевірити ефективність *SSL*. Використовує властивість асиметричності навантаження на |
| | | відключає сервер жертви за рахунок того, що встановлення захищеного з'єднання *SSL* вимагає в 15 разів більшої обчислювальної потужності на сервері, ніж на клієнті. Додатково використовує функцію безпечного повторного узгодження SSL, щоб ініціювати тисячі повторних узгоджень через одне з'єднання TCP. | сервер і клієнта при встановленні , захищеного з'єднання *SSL*. Використовує функцію безпечного повторного узгодження *SSL*. Форк *thc-ssl-dos* підтримує всі реалізації *SSL/TLS, UDP* (з використанням *DTLS*), проксі-сервер *SOCKS*5, а також атаки перегляду та повторного з'єднання. Він також містить лабораторію докерів для тестування експлойту. |
| 15 | *Apache Benchmark Tool* | Інструмент порівняльного аналізу, який вимірює продуктивність *web*-сервера, заповнюючи його *HTTP*-запитами та записуючи показники затримки та успіху. Дозволяє визначити обсяг трафіку, який може підтримувати *HTTP*-сервер до того, як продуктивність знизиться, і встановити базові показники для типового часу відповіді. | Підтримує Windows і MacOS. Незважаючи на те, що *ApacheBench* було розроблено для порівняльного тестування *web* -сервера *Apache*, це повноцінний *HTTP*-клієнт, який перевіряє фактичні з'єднання, і він може використовуватися для тестування продуктивності будь-якої серверної частини, яка обробляє *HTTP*-запити, тобто може тестувати будь-який *HTTP*-сервер і використовуватися для *DDoS*-атаки. Показує результат в кінці. Показники *ApacheBench* можуть допомогти налаштувати *web*-сервери та оптимізувати програми, зокрема: – показники для затримки запиту, які варіюються від процентильних розподілів усіх запитів до тривалості певних фаз у *TCP*-з'єднаннях; – показники статусу запиту та підключення, включаючи коди статусу *HTTP* та помилки запитів. Найкращий інструмент *DDoS*-атаки для *Windows* |

За організацію *DDoS*-атак у більшості країн світу передбачена кримінальна відповідальність (наприклад, у США винна особа може бути ув’язнена на термін до 10 років), але часто *DDoS*-атаки проводяться в рамках пентестингу. *DDoS*-атаки є незаконними, але деякі інструменти, які зараз використовуються для їх здійснення, розроблялися із законною метою – для проведення тестування. З іншого боку, існують способи використання інструментів розроблених спеціально для *DDoS*-атак, для абсолютно законних речей, наприклад для блокування власного власного сервера або служби, якщо власник хоче тимчасово відокремити їх від Інтернет.

Для того, щоб успішно протидіяти кіберзагрозам, необхідно добре знати свого «супротивника». Тому при організації кіберзахисту необхідно враховувати особливості кожного типу атак; особливості інструментів, які може застосувати зловмисник для проведення атаки; вразливості ресурсів конкретної КС, ознаки атак і способи їх ідентифікації; функціональні, вартісні і надійнісні показники методів і засобів захисту.

## 2.2 Класифікація *DDoS*-атак

### 2.2.1 Принципи класифікації *DDoS*-атак

*DDoS*- атаки можуть бути різних типів, але всі вони мають спільну мету – перевантажити сервер і призвести до відмови в обслуговуванні. Деякі з найпоширеніших видів *DDoS*- атак включають [11]:

– атаки на рівні мережі (наприклад, атаки на протоколи *ICMP, UDP*, *TCP*), які спрямовані на зупинку сервера шляхом перевантаження мережевих з'єднань;

– атаки на рівні програми (наприклад, атаки на *HTTP, HTTPS, DNS*), які спрямовані на виснаження ресурсів сервера, пов'язаних з обробкою запитів клієнта;

– атаки на рівні інфраструктури (наприклад, атаки на *DNS*-серверии або маршрутизатори), які спрямовані на перевантаження сервера *DNS*, шляхом надсилання великої кількості хибних запитів на *DNS*-сервер з метою змусити його витрачати ресурси на формування відповідей;

– змішані атаки, що поєднують кілька видів *DDoS*-атак, спрямованих на різні рівні сервера з метою посилення ефекту. Більшість *DDoS*-атак є змішаними.

Критеріями класифікації *DDoS*-атак можуть бути:

– рівень моделі *OSI*, на якому здійснюється атака;

– тип протоколу;

– механізм впливу;

– кількість нападників на одну жертву (на даний час схема «один нападник — одна жертва» не застосовується, оскільки ширина каналу сучасних серверів, їх потужність і активне використання різних засобів і прийомів протидії *DDoS*атакам, наприклад, створення затримки у випадку багаторазового виконання однакових дій одним клієнтом, роблять її неефективною з точки зору зловмисників, які зараз використовують хости-зомбі) .

### 2.2.2 Класифікація *DDoS*-атак за рівнями моделі *OSI*

Модель стеку мережевих протоколів *OSI*, яка описує роботу Інтернету, складається з 7 рівнів, кожному з яких відповідають протоколи, що визначають формати даних і процедури їх приймання-передавання на певному рівні. Особливості протоколів кожного рівня зумовлюють доступність для зловмисника способів організації *DDoS*-атак (табл.2.2.).

Таблиця 2.2 - *DDoS*-атаки на рівнях моделі *OSI*

| Рівні | | | *DDoS*-атаки | |
|---|---|---|---|---|
| № | Назва | Процеси і протоколи | Група | Тип атаки |
| 1 | Фізичний | Робота з сигналами і бітами, передавання необроблених | | *DoS* або *DDoS*-атака неможлива. Загрозу |

Продовження таблиці 2.2

| Рівні | | | *DDoS*-атаки | |
|---|---|---|---|---|
| № | Назва | Процеси і протоколи | Група | Тип атаки |
| | | двійкових даних між машинами. Використовуються протоколи *Bluetooth*, *USB*, інфрачервоних портів, а також концентратори, розетки та патч-панелі | **Низькорівневі атаки** | можуть становити фізичні руйнування або будь-які інші перешкоди в роботі мережі. Штучно створені збої можуть привести до повної непридатності обладнання |
| 2 | Канальний | Створення з'єднання і фізична адресація. Обмін даними між вузлами в локальній мережі. Дані формуються в спеціальні блоки (кадри) і передаються на фізичний рівень. Присвоєння унікальних ідентифікаторів мережевим адаптерм (*MAC*- адрес) | | Найбільш поширена *DDoS*-атака - *MAC*-флуд. Мережеві комутатори навантажуються пакетами даних так, щоб вивести з ладу всі порти з'єднання |
| 3 | Мережний | Початок взаємодії комутаторів і маршрутизаторів, розташо-ваних в різних мережах. Головна задача - побудувати оптимальний шлях для передавання даних між пристроями. Маршрутизація, що побудована на перетворенні *MAC*-адрес в мережеві адреси. | | *ICMP*-флуд з метою перевантаження цільового набору *ICMP*-повідомленнями. Врезультаті знижується пропускна здатність та обмежується кількість запитів, що може бути опрацьована за *ICMP*-протоколом. |
| 4 | Транспортний | Обробка і транспортування паке-тів даних між вузлами зв'язку. Контроль потоку інформації та виявлення помилок. Повторне відправлення даних в разі наявності помилок. Використовуються протоколи *UDP* і *TCP* | | Зловмисники створюють умови, при яких перевищуються порогові значення за шириною каналу та кількістю доступних підключень. Найбільш поширені типи *DDoS*-атак - *Smurf* і *SYN* - флуд. |
| 5 | Сеансовий | Управління взаємодією між додатками, а також управління з'єднаннями (встановлення і завершення), синхронізація завдань операційної системи. | **Високорівневі атаки** | Зловмисники використовують слабкі місця ПЗ через протокол *Telnet*, що може призвести до втрати адміністратором доступу до сервера |

Продовження таблиці 2.2

| Рівні | | | *DDoS*-атаки | |
|---|---|---|---|---|
| № | Назва | Процеси і протоколи | Група | Тип атаки |
| 6 | Представлення | Кодування і декодування даних, їх адаптація для людини або машини, у зрозумілому для них вигляді. Сюда входять відеодані, аудіодані, зображення та текст. Між 6 і 7 рівнями моделей *OSI* знаходиться *SSL* –протокол, який забезпечує клієнту безпечне з'єднання з сервером і надає можливість взаємної перевірки довжини | **Високорівневі атаки** | *SSL*-флуд зі зміненими пакетами - зловмисники генерують пошукові *SSL*-запити для атаки на сервер-жертву. Процеси в системі-жертві гальмуються, бо перевірка зашифрованих *SSL*-пакетів займає багато часу. |
| 7 | Прикладний (рівень додатків) | Доступ до мережевих ресурсів. Надання користувачу даних у зрозумілому для нього вигляді. | | *HTTP*-флуд: на підключення, на вхід логінів, на замовлення товару, завантаження відео тощо. Легітимні користувачі не можуть потрапити на сайт, бо він перевантажений сміттєвими запитами |

2.2.3 Класифікація *DDoS*-атак за протоколами

Класифікація DDoS-атак за протоколами включає різні типи атак, кожна з яких використовує специфічні протоколи для досягнення своєї мети. Найпоширеніші типи включають:

– *ICMP Flood* – використовується протокол ICMP для відправлення великої кількості пакетів *Echo Request* (*ping*). Сервер перевантажується спробами відповісти.

– *Ping of Death* (пінг смерті) – зловмисник постійно генерує неправильно сформовані або занадто великі пакети за допомогою команди *ping*. Якщо системажертва працює на базі протоколу *IPv*4, то суммарний об’єм отриманого пакета не може перевищувати 65 535 байт. Коли приходить більший за обсягом

пакет, то виникає переповнення пам'яті. Якщо система-жертва працює на базі *IPv*6, то зловмисники відправляють фрагменти пакетів, при збірці яких системою-жертвою отримується занадто великий пакет, що призводить до переповнення пам'яті та збоїв у роботі;

– *SYN*-флуд – зловмисники з великою швидкістю відправляють запити на з'єднання з сервером із підробленою хибною *IP*-адресою джерела. Більшість операційних систем декілька разів намагаються відіслати у відповідь на недоступну адресу *ACK*-пакет, а потім ставлять невстановлене з'єднання в чергу і продовжують спроби надіслати відповідь. З'єднання закривається лише після того, як певна *n*-на спроба відправити відповідь виявляється невдалою. В процесі триетапного алгоритму рукостискання великий потік *ACK*-пакетів заповнює чергу, і ядро не дає дозволу на відкриття нових з'єднань. Окремі боти аналізують систему перед початком атаки і потім надсилають запити тільки на відкриті і життєво важливі порти, що збільшує ефективність атаки;

– *UDP-флуд* – зловмисники відправляють на сервер-жертву велику кількість *UDP*-пакетів на випадкові порти від імені різних *IP*-адрес, в результаті чого вичерпується смуга пропускання, перевантажується мережеве обладнання;

– *HTTP Flood* – використовує легітимні *HTTP*-запити для перевантаження веб-серверів або веб-додатків. Атака спрямована на виснаження ресурсів цільового сервера, таких як процесорний час, пам'ять або пропускна здатність, роблячи його недоступним для звичайних користувачів;

– *SSDP Amplification* – використовує протокол *Simple Service Discovery Protocol (SSDP),* компонент *Universal Plug and Play (UPnP),* для посилення обсягу трафіку, спрямованого на жертву. Зловмисники надсилають запити на уразливі *SSDP*-пристрої, підроблюючи *IP*-адресу жертви. У відповідь ці пристрої генерують великий обсяг даних, що перевантажує мережу цілі. Основна особливість цієї атаки — високий коефіцієнт посилення: відповідь від серверів може перевищувати початковий запит у 30-100 разів. Часто для атак

використовуються пристрої Інтернету речей *(IoT),* такі як камери, маршрутизатори та медіа-сервери, які не мають належного захисту.

### 2.2.4 Класифікація *DDoS*-атак за механізмом дії

У сучасному світі *DDoS*-атаки розділяють на три основні групи за механізмом їх дії:

– атаки на основі флуду;

– атаки на основі протоколів;

– атаки на рівень додатків;

Флуд передбачає створення великої кількості неправильно сформованих або беззмістовних повідомлень з метою перевантаження пропускної здатності каналу зв’язку жертви.Групу атак на основі флуду складають:

– *DNS*-флуд. На *DNS* -сервер направляється маса *DNS* -запитів з широкого діапазону *IP*-адрес. Сервер-жертва не може визначити, який із пакетів прийшов від легітимного користувача, а який - ні, і вимушений відповісти на всі запити;

– *DNS* –ампліфікація. Публічному *DNS* –серверу надсилають запит щодо даних про домен і направляють його відповідь на атакований сервер. Запит формується таким чином, щоб у відповідь повернулося як мога більше даних;

– фрагментований *UDP*-флуд. Зловмисник використовує пакети максимально допустимого розміру, щоб заповнити канал мінімальною кількістю пакетів. Фрагменти пакетів є фальсифікованими, а сервер-жертва використовує всі ресурси для того, щоб відновити неіснуючі пакети з фальшивих фрагментів;

– *ICMP*-флуд. На сервер-жертву зловмисником розсилається велика кількість підробних *ICMP*-пакетів із широким діапазоном *IP*-адрес з метою заповнення каналу сервера-жертви потоком підробних запитів;

– *Ping*-флуд. Це різновид *ICMP*-флуду, призначена для виведення з ладу сервера за допомогою утиліти *ping*;

– фрагментований *ICMP*-флуд. На сервер-жертву направляється потік фрагментованих *ICMP*-пакетів максимального розміру. Смуга пропускання забивається сміттєвим трафіком, виникає небезпека вичерпування обмежених ресурсів;

– *NTP*-флуд. Зловмисник генерує велику кількість підробних *NTP*-запитів з широким діапазоном *IP*-адрес. *NTP*- сервер намагається опрацювати всі запити, витрачаючи системні та мережеві ресурси;

– *NTP*-підсилювач. Зловмисник багатократно відправляє запит *monlist* на *NTP*-сервер, одночасно змінюючи свою *IP*-адресу на адресу сервера-жертви. Відповідь *monlist* може містити список до 600 останніх клієнтів. Мета атаки - відправлення великого потоку *UDP*-трафіку на сервер-жертву у відповідь на невеликий запит;

– фрагментований *ACK*-флуд. Використовуються пакети максимально допустимого розміру для заповнення смуги пропускання каналу, при невеликій кількості пакетів, що передаються;

– *UDP*-флуд з ботнетом. Алгоритм атаки, схожий зі звичайним *UDP*–флудом (див.п.2.2.3), але пакети генеруються ботами. Системні ресурси заповнюють нецільовим трафіком і вичерпуються;

– атака широкосповіщувальними *UDP*-пакетами. Кібератака будується на виправленні *UDP*-пакетів з підміненою *IP*-адресою, в розрахунку на те, що кожен із цих пакетів буде відправлений кожному клієнту цієї мережі.

– *VoIP*-флуд. На сервер-жертву відправляють велику кількість підроблених *VoIP*-пакетів з широким діапазоном *IP*-адрес. Сервер витрачає ресурси, щоб опрацювати як підробні, так і легітимні запити;

– флуд медіа-даними. Зловмисник відправляє велику кількість окремих пакетів у вигляді відео- або аудіо-даних на сервер-жертву. Файли з медіа-даними характеризуються великим обсягом, і обчислювальні ресурси мережевого обладнання вичерпуються на їх обробку.

До групи атак на основі протоколу входять:

– атаки з модифікаціями поля *TOS* (англ. *Type of Service*). Зловмисник,використовуючи поля *TOS* і *ECN* (англ. *Explicit Congestion Notification*) в *IP*-пакетах, щоб створити ілюзію перевантаженості мережі. Це змушує сервер самостійно обмежувати пропускну здатність для підключення, що призводить до втрати продуктивності і збоїв у роботі сервісів;

– *ACK* – флуд. Зловмисники надсилають підроблені *ACK*-пакети на сервер-жертву. Ці пакети не мають відношення до жодної сесії в базі даних з'єднань сервера, що ускладнює його здатність ідентифікувати правильні з'єднання. Це може привести до збоїв у роботі сервера через надлишкові і непотрібні спроби підключення;

– *RST*, *FIN*–флуд. Сервер-жертва отримує окремі *RST*- або *FIN*-пакети, які не мають стосунку до жодної із сесій в базі даних сервера; Це викликає помилки в управлінні з'єднаннями і може призвести до падіння продуктивності або повної недоступності сервера;

– атака за допомогою створення підроблених *TCP*-сесій з кількома *SYN-ACK*. Зловмисник генерує підробні сесії кількома *SYN*- і *ACK*-пакетами, що дозволяє йому визначити механізми захисту та створити трафік, схожий на легітимний;

– атака за допомогою перенаправлення трафіку високонавантажених сервісів. Зловмисник перенаправляє трафік високонавантажених додатків легітимних користувачів на сервер-жертву. Це призводить до збоїв внаслідок встановлення великої кількості з'єднань, які вимагають обробки;

До третьої групи атак відносять атаки на рівень додатків (рівень 7 моделі *OSI*, див. табл.2.2):

– *HTTP*-флуд. Зловмисник генерує велику кількість запитів, спрямованих на сервер-жертву, щоб зменшити долю ресурсів, що припадає на обробку корисного трафіку. Для цього зловмисник неперервно надсилає *http*-повідомлення *GET* на 80-ий порт. Метою *HTTP*-флуду може бути не тільки корінь *web*-сервера, а й

певний скрипт, що працює з базою даних чи виконує інші ресурсоємні завдання. *HTTP*-флуд на сьогоднішній день є одним з найпоширеніших способів флуду;

– *XML-RPC*-флуд. Атака через інтерфейс віддалених процедур XML-RPC, який використовується в багатьох вебсервісах, наприклад, WordPress. Вона спрямована на виснаження ресурсів сервера, використовуючи масовий виклик функцій;

– *APIs Abuse* (Зловживання *API*). Атака через інтерфейси API, що надсилає численні запити для виконання ресурсозатратних операцій, таких як отримання даних, виконання пошуку або обробка транзакцій.

– *HTTP*-флуд одиничними запитами. На відміну від звичайного флуду, коли зловмисник атакує сервер-жертву потоком окремих запитів, цей тип атаки передбачає відправлення одного великого пакета, всередині якого одночасно передається 500-600 запитів;

– атака фрагментованими *HTTP*-пакетами. Зловмисник виправляє на адресу жертви невеликі фрагменти даних, які неможливо зібрати в єдиний об'єкт. При цьому спочатку встановлюється правильне *HTTP*-з'єднання з *web*-сервером. Далі легітимні *HTTP*-пакети розділяються на маленькі фрагменти, які передаються настільки повільно, наскільки це дозволяє тайм-аут сервера. Таким чином зловмисник уникає спрацьовування механізмів захисту і непомітно призводить ть *web* -сервер до відмови за допомогою шкідливих ботів;

– *HTTP*-флуд одиничними сесіями. Зловмисник атакує сесію з вищим лімітом на боці жертви, щоб безперервно в рамках кожної *HTTP*-сесії надсилати безліч запитів, вичерпуючи наявні ресурси для обслуговування атак.

– *Application Login Attacks.* Спроби виконати багаторазові логіни в додаток, використовуючи запити на сторінку входу, щоб перевантажити сервер аутентифікації.

– *DNS Query*-флуд. Генерується великий обсяг запитів до серверів DNS на розв'язання імен доменів, що спрямоване на перевантаження серверів.

– *APT*-атака. Метою зловмисника є пошук на пристрої-жертві цінної інформації, яку він може використати. Першою задачею зловмисника є непомітне проникнення в КС. Щоб отримати несанкціонований доступ до потрібної КС, зловмисники використовують соціальну інженерію, експлуатують уразливості системи захисту тощо. Після проникнення зловмисник вивчає КС тривалий час, відстежує дії користувачів, аналізує трафік в КС, і виявляє таким чином інформаційні ресурси, що можуть становити інтерс для нього. Наступним кроком зловмисника є отримання доступу потрібного рівня до цих ресурсів і виконання з ними необхідних дій – копіювання, модифікація, розповсюдження тощо;

– *WordPress XML-RPC Flood.* Атака через функцію *XML-RPC* у *WordPress*, яка дозволяє виконувати багаторазові запити, наприклад, масові пінгбеки, що створюють значне навантаження на сервер.

Нові атаки на основі флуду, особливо *DDoS*-атаки, еволюціонують у 2024 році, стаючи складнішими та багатовекторними. Розглянемо основні тенденції.

*HTTP*-флуд та *DNS*-флуд тепер комбінуються з більш складними векторами атаки, які важче виявити. Наприклад, використовуються складні пакети даних, які перевантажують сервери та обходять базові системи захисту (*IPS/IDS*) через їхню повільну обробку.

Атаки з використанням ботнетів та *IoT* збільшують використання заражених *IoT*-пристроїв для масштабних атак, оскільки ці пристрої часто мають слабкі системи захисту. Ботнети стають інструментом для комбінованих *DDoS*-атак, спрямованих на критичну інфраструктуру.

Штучний інтелект кіберзлочинці активно застосовують для оптимізації атак.

Наприклад, генеративні моделі ШІ допомагають створювати зловмисний код та автоматизувати атаки. Це робить можливим створення більш реалістичних фішингових повідомлень і навіть нових типів флуду, які обходять традиційні засоби захисту.

Мультивекторні атаки. Нові методи включають поєднання різних видів атак, таких як *DDoS* і проникнення у внутрішню мережу. Наприклад, флуд може використовуватися для перевантаження мережі й паралельного запуску більш небезпечних векторів атак, як-от впровадження шкідливого програмного забезпечення.

У цьому розділі кваліфікаційної роботи розглянуто лише деякі з типів *DDoS*-атак, оскільки з часом вони стають дедалі частішими, більш складними, потужними та ефективними.

## 2.3 *Slowloris* і *NXDOMAIN* атаки

Атака *Slowloris* — це *DDoS*-атака на рівні додатків, яка функціонує шляхом використання неповних *HTTP*-запитів. Атака полягає у відкритті підключень до цільового веб-сервера, а потім утриманні їх якомога довше.

*Slowloris* використовує мінімальний обсяг трафіку, при цьому намагаючись використати ресурси сервера з запитами, що ніби-то повільніші, ніж зазвичай, але імітують регулярний трафік. Атака відноситься до категорії "повільних атак" через те, що сервери мають обмежену кількість потоків для обробки одночасних з’єднань. Кожен серверний потік намагається залишитися активним, чекаючи на завершення повільного запиту, який ніколи не відбувається. Коли сервер досягає свого максимального числа можливих підключень, будь-яке нове підключення не буде оброблено, що призведе до відмови у доступі.

Атака *Slowloris* відбувається у 4 кроки:

1. Атака починається з відкриття кількох з'єднань до цільового сервера шляхом надсилання кількох неповних *HTTP*-запитів.

2. Цільовий сервер відкриває поток для кожного надісланого запиту, з наміром закрити його після завершення з'єднання. Для ефективності, якщо

з'єднання триває занадто довго, сервер призупинить надзвичайно довге з'єднання, звільняючи потік для наступного запиту.

3. Щоб запобігти часу виконання з'єднань цільового сервера, нападник періодично надсилає неповні заголовки запитів цільовому серверу, щоб зберегти з'єднання активним.

4. Цільовий сервер не може звільнити жодне з відкритих неповних з'єднань, поки чекає завершення запиту. Як тільки всі доступні потоки використовуються, сервер не зможе відповідати на додаткові запити, які надходять з регулярного трафіку, що призведе до відмови в обслуговуванні.

Slowloris має здатність завдавати значної шкоди з дуже низьким споживанням пропускної здатності, що робить його ефективним інструментом для *DDoS*-атак.

Ця атака вважається розподіленною відмовою в обслуговуванні, і вона може залишатися непомітною традиційними системами виявлення вторжень. Slowloris працює, надсилаючи справжні *HTTP*-запити з низькою частотою запитів в секунду, а не великими обсягами або високою частотою *HTTP*-запитів в секунду. Крім того, оскільки журнал файлів не може бути записаний до завершення запиту, атака Slowloris може надовго вивести з ладу сервер без єдиної запису в журналі, яка б викликала тривогу у спостерігачів

Атака *NXDOMAIN* — це *DDoS*-атаки, яка використовує запити *DNS* для порушення роботи мережі. зловмисники заповнюють *DNS*-сервер великим обсягом запитів на неіснуючі або недійсні записи. У результаті цільовий проксі-сервер *DNS* використовує свої ресурси для запитів до авторитетного сервера, що призводить до уповільнення роботи обох *DNS*-серверів і зрештою перестає відповідати.

Атака працює за таким принципом:

1. Створення запитів до неіснуючих доменів. Зловмисник генерує тисячі або мільйони *DNS*-запитів до доменів, яких не існує.

2. Навмисне виснаження ресурсів. *DNS*-сервер намагається знайти ці домени у своїх кешованих даних або передає запит на інші *DNS*-сервери. Оскільки домени не існують, сервер витрачає час і обчислювальні ресурси, формуючи відповідь типу *NXDOMAIN*.

3. Перевантаження мережі. Обсяг запитів може бути настільки великим, що DNS-сервер перестає справлятися з роботою, зупиняється або стає недоступним для легітимних користувачів.

Атаки *NXDOMAIN* можуть мати серйозні наслідки для *DNS*-інфраструктури та сервісів, які вона обслуговує. Ось основні наслідки, які виникають внаслідок таких атак:

– виснаження ресурсів *DNS*-сервера. Атака створює велике навантаження на сервери *DNS*, що призводить до перевищення їх пропускної здатності, а також перевантаження процесора й оперативної пам’яті. Це може спричинити збої або значне зниження продуктивності роботи сервера;

– недоступність сервісів. У випадку, коли *DNS*-сервер виходить з ладу через надмірне навантаження, користувачі втрачають можливість отримати доступ до веб-сайтів, додатків та інших інтернет-ресурсів, які залежать від роботи цього сервера;

– ланцюгова реакція. *DNS*-запити, які не можуть бути оброблені основним сервером, перенаправляються до інших серверів. Це може спричинити аналогічні проблеми у всій мережі *DNS*, що створює масштабні збої в роботі інфраструктури;

– використання у складних атаках. *NXDOMAIN*-атаки часто комбінуються з іншими типами *DDoS*-атак для збільшення загального навантаження та складності атаки. Такі комбіновані атаки можуть мати руйнівні наслідки, особливо якщо вони націлені на критично важливі ресурси.

Атаки *NXDOMAIN* можуть завдати шкоди різним групам організацій та користувачів, які залежать від стабільної роботи *DNS*-серверів. Основними потенційними жертвами таких атак є:

1. Постачальники мережевих послуг. Організації, які керують *DNS*-серверами несуть основний удар від атак. Вони ризикують втратити стабільність сервісів, які обслуговують багатьох клієнтів. Це може призвести до масових перебоїв у доступі до веб-сайтів і онлайн-послуг.

2. Власники веб-сайтів. Атаки *NXDOMAIN* можуть зробити сайти недоступними для законних користувачів. Це негативно впливає на їхню здатність продавати продукти або надавати послуги, що призводить до фінансових втрат і шкоди репутації.

3. Кінцеві користувачі: Люди, які користуються постраждалими веб-сайтами та сервісами, втрачають доступ до продуктів чи послуг, на які вони підписані. Це створює значні незручності та знижує довіру до постачальника послуг.

У 2024 році ці атаки стали більш витонченими завдяки використанню автоматизованих ботнетів і штучного інтелекту для створення і виконання великомасштабних атак.

Атаки *NXDOMAIN* мають широкий спектр негативного впливу, тому всі учасники мережевої інфраструктури повинні впроваджувати заходи для запобігання таким атакам.

## 2.4 Спам-атаки на мобільні телефони

Мобільні телефони часто використовують різноманітні додатки для виконання різних функцій — від ігор до фінансових операцій. На жаль, деякі мобільні додатки можуть бути скомпрометовані або включати в себе шкідливий код, який активується після встановлення. Такі додатки можуть не лише відслідковувати активність користувача, а й виконувати шкідливі операції, наприклад, запускати *DDoS*-атаки. Ці додатки зазвичай працюють у фоновому режимі, і користувач може навіть не підозрювати, що його телефон використовується для атак.

Мобільні пристрої можуть стати частиною ботнета через шкідливі додатки або віруси. Після зараження мобільний телефон перетворюється на «бот», який автоматично виконує команди атакуючих. Це може включати направлення величезної кількості запитів на сервери, що призводить до їх перевантаження. Оскільки мобільні телефони мають обмежену потужність, таке використання їх для атаки може призвести до швидкого розряджання акумулятора та сильного перевантаження системи.

*DDoS*-атаки можуть бути спрямовані не тільки на окремі мобільні пристрої, а й на інфраструктуру мобільних мереж. Це означає, що атакуючі можуть спричиняти перевантаження мобільних мереж, що призводить до зниження якості зв'язку або повної відсутності доступу до інтернет-ресурсів для користувачів мережі. Мобільні оператори можуть стати ціллю для атак, оскільки їхні інфраструктури містять велику кількість сервісів, до яких звертаються мобільні телефони.

Сучасні технології дозволяють організовувати DDoS-атаки, використовуючи мобільні мережі, за допомогою спам-дзвінків або спам-повідомлень. Це може призвести до того, що користувачі телефонів будуть отримувати величезну кількість несанкціонованих повідомлень або дзвінків, що може перевантажити систему, в результаті чого користувачі не зможуть здійснювати важливі дзвінки або отримувати потрібні повідомлення.

*DDoS*-атаки на мобільні телефони є серйозною загрозою для сучасних користувачів, які активно використовують мобільні пристрої для доступу до Інтернету та різноманітних сервісів. Враховуючи обмежені ресурси мобільних телефонів та можливість їх зараження шкідливими програмами, захист від таких атак є необхідністю. Важливо постійно оновлювати програмне забезпечення, використовувати антивірусні рішення та застосовувати фільтрацію трафіку на рівні мобільних мереж для забезпечення безпеки мобільних пристроїв і запобігання великим збиткам від таких атак.

## 2.5 Вразливі точки сенсорних підмереж в архітектурі *IoT* до *DDoS*-атак

Концепція Інтернету речей (англ. *Internet of Things, IoT*) охоплює мережу взаємопов’язаних фізичних пристроїв, які мають датчики та виконавчі блоки, а також можливість взаємодії через дротові або бездротові мережі. Програмне забезпечення дозволяє дистанційне керування цими пристроями в автоматичному або автоматизованому режимі на основі обміну даними між фізичними пристроями та комп’ютерними системами за стандартними протоколами зв’язку. Використання інтелектуальних інтерфейсів виключає людину з процесів ідентифікації пристроїв, зчитування даних датчиків, активації виконавчих блоків тощо, що призвело до появи нових термінів, таких як Інтернет всього (*IoE*) і безпека Інтернету речей.

У рамках *IoT* "речами" можуть бути будь-які пристрої, яким можна присвоїти IP-адресу і які здатні приймати і передавати дані через мережу за стандартними протоколами. Сучасний ринок пропонує не лише "розумні" пристрої, які підключаються до *IoT*, а й відповідні послуги провайдерів мережевого зв’язку.

Зростання кількості підключених пристроїв *IoT* зумовлює зростання ризиків ІБ. В роботі [15] визначені наступні проблеми і уразливості *IoT*:

– атаки *DoS* на *IoT*. Стали серйозною проблемою через зростання кількості та різноманітності підключених до мережі пристроїв, які часто мають обмежені ресурси пам'яті та обчислювальної потужності. Це ускладнює застосування складних засобів захисту, роблячи багато таких пристроїв вразливими до захоплення ботнетами. Під час проведення розподілених атак зловмисники можуть використати ці пристрої для організації *DDoS*-атак. Мета таких атак — фізичне пошкодження підключених до мережі пристроїв або компрометація додатків, які використовуються на цих пристроях. Відстеження джерела таких атак є складним і тривалим процесом, що зменшує ризик викриття для зловмисників. Це робить боротьбу з такими загрозами особливо складною, оскільки низька обчислювальна потужність IoT пристроїв дозволяє використовувати їх для масштабних та потужних атак;

– прослуховування в *IoT*. Пасивні атаки можуть бути використані зловмисниками для перехоплення даних з інформаційних потоків, що дозволяє їм отримати доступ до певної інфраструктури або відновити інформацію, яка передається через неї. Це може загрожувати безпеці систем, що використовують ці пристрої;

– захоплення вузлів в *IoT*. Зловмисники можуть знешкодити або викрасти інформацію з *IoT*-пристроїв, що містить дані щодо інфраструктури, яка використовується для зберігання або обробки даних. Це може призвести до великих проблем, якщо ці пристрої критичні для функціонування системи;

– фізична безпека датчиків в *IoT*. Датчики в *IoT* можуть бути виявлені та зламані зловмисником через аналіз різних сигналів, таких як радіо-, теплові, магнітні, візуальні тощо. Це робить їх вразливими до фізичного втручання або викрадення даних.

В статті [16] забезпечення безпеки сенсорної мережі має враховувати захист комунікацій, управління пристроями, а також розробку нових моделей довіри. Сенсорна мережа складається з пристроїв, які збирають та транслюють параметри середовища, що дозволяє проводити моніторинг і аудит контрольованих середовищ, таких як відеоспостереження чи моніторинг мікроклімату.

Сенсорна мережа складається з пристроїв, які реєструють та передають різні параметри середовища до інших пристроїв, дозволяючи здійснювати моніторинг і аудит контрольованих середовищ. Це може включати спостереження за відео, контроль мікроклімату в приміщенні та інші вимірювання, що допомагають підтримувати безпеку та ефективність роботи системи.

Сенсорні мережі можуть бути безпровідними і використовувати різні стандарти для комунікації та взаємодії між пристроями. Ось основні з них:

– *IEEE* 802.15.4. Це стандарт, який забезпечує низьку потужність і низьку швидкість передачі даних, використовується для персональних мереж (*PANs*). Він

працює на частотах 2.4 *GHz*, 915 *MHz* та 868 *MHz* і підходить для пристроїв з обмеженим терміном служби батареї;

– *ZigBee*. Створений на базі *IEEE* 802.15.4, *ZigBee* є протокольним стеком, який забезпечує стандарт для низької потужності та низької швидкості передачі даних, зокрема для «розумного дому», автоматизації будинків та індустріальних систем контролю. *ZigBee* використовує мережевий підхід до побудови мережі, що забезпечує надійність і масштабованість;

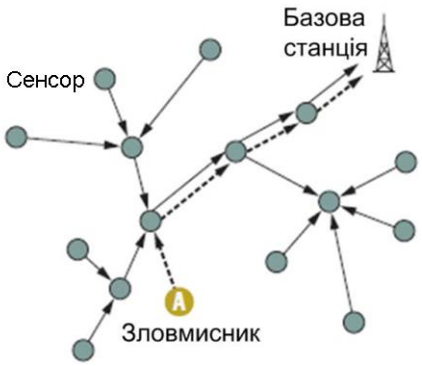
– *LoRaWAN* (англ. *Long Range Wide Area Network*). Використовується для широкосмугових низькопотужних мереж (*LPWAN*). Забезпечує довгий радіус дії для батарейних пристроїв у віддалених локаціях. Використовує піддіапазони *ISM* та підтримує низькі швидкості передачі даних, що робить його підходящим для застосувань у смарт-містах, сільському господарстві та промисловій автоматизації;

– *NB-IoT* (англ. *Narrowband Internet of Things*). Частина сімейства *3GPP*, *NB-IoT* надає вузькосмугову комунікацію через стільникові мережі. Підтримує довгий радіус дії та глибоке проникнення в приміщення, підходить для пристроїв *IoT*, які мають відправляти невеликі об’єми даних на великі відстані;

Безпровідні сенсорні мережі (БСМ), в яких передача сигналів сенсорів здійснюється по безпровідному, наприклад, радіоканалу, мають характерні вразливості і можуть потерпати від різних типів кібератак. На рис.2.1, а наведено схему ймовірної DoS-атаки у сенсорній мережі.

Для сенсорних мереж важливим є забезпечення безпечного обміну даними між різними типами таких мереж, зокрема, забезпечення захисту від *DoS*-атак у збірних сенсорних вузлах (ЗСВ), реалізація яких може привести до втрати або несанкціонованої модифікації інформації від сенсорів і відповідних збитків. Задача визначення найбільш ефективної схеми взаємодії мереж в [С8] розвязується як задача мінімізації ризиків безпеки сенсорних вузлів в умовах обмежень вартості, технічних можливостей тощо.

а) схема *DoS*-атаки




б) спрощена структура БСМ

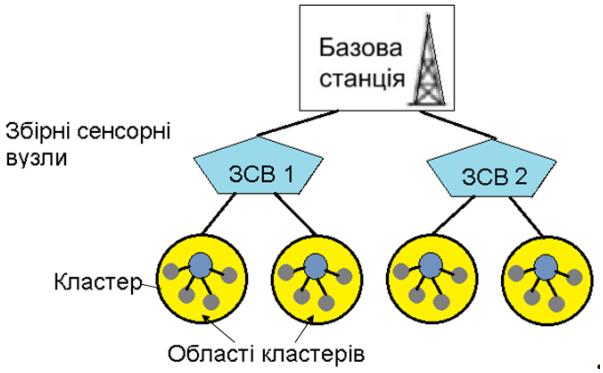



Рисунок 2.1 – Сенсорні мережі

Спрощена БСМ (рис.2.1, б) складається кластерів, інформація з яких збирається двома ЗСВ за схемою «один ЗСВ - два кластера», і однієї базової станції, що збирає інформацію із ЗСВ 1 та ЗСВ 2. При *DoS*-атаці на сенсорну мережу збитки внаслідок її реалізації можуть бути зумовлені порушенням ІБ базової станції та ЗСВ 1 і ЗСВ 2. Відповідно можна визначити і проаналізувати ризики для базової станції, всіх транзитних ЗСВ і мережі в цілому. Ці ризики залежать від сенсорних датчиків і додатків, які використовуються на них.

БСМ у 2024 році продовжують активно розвиватися завдяки новітнім технологіям та тенденціям. Деякі з основних напрямків розвитку БСМ:

– машинне навчання та штучний інтелект (*AI*). Використання *AI* для обробки даних, отриманих через біосенсори, дозволяє отримувати більш точні та персоналізовані результати в різних галузях, таких як охорона здоров'я та безпека. Завдяки *AI*, біосенсори можуть самостійно визначати патерни в даних, виявляти аномалії та реагувати на події без участі людини;

– розвиток біосенсорних технологій у хмарних рішеннях. З появою нових хмарних платформ, біосенсори можуть бути інтегровані для моніторингу і зберігання великих обсягів даних у реальному часі;

– моніторинг інфраструктури та даних. Важливим напрямком є використання БСМ для моніторингу стану серверних та мережевих пристроїв. Такі сенсори здатні виявляти перегрів, перевантаження, збій системи;

– забезпечення ефективності мережевих комунікацій. Використання БСМ у мережах для контролю та оптимізації передачі даних. Мережі, підтримувані біосенсорами, можуть автоматично налаштовувати параметри передачі даних;

*DoS*-атаки на сенсорні вузли та базову станцію можуть мати різну природу (рис.2.2) і проводитися на різних рівнях моделі *OSI* (табл.2.3).


Рисунок 2.2 – Властивості *DoS*-атак на сенсорні вузли та базову станцію

Таблиця 2.3 - *DoS*-атаки на сенсорні вузли та базову станцію

| Рівень | Тип атаки | Заходи протидії |
|---|---|---|
| Фізичний | *JAMMING* (глушіння) | Розширення спектру, пріоритетні повідомлення, картування областей |
| | *TAMPERING* (підробка) | Випробувальні пакети проти підробки, використання нечутливих до відмов протоколів |
| Канальний | Колізії | Корегувальне кодування |
| | Виснаження | Обмеження швидкості передавання даних |
| | Збирання інформації | Захист проти повторних відправлень, сильна автентифікація на канальному рівні |

Продовження таблиці 2.3

| Рівень | Тип атаки | Заходи протидії |
|---|---|---|
| Мережевий | Фальсифікація маршрутної інформації | Автентифікація, використання захисту проти повторних відправлень |
| | Селективне просування | Використання різних маршрутів, підтвердження доставки |
| | *Sinkhole*-атака | Перевірка надмірності |
| | Атака *Sybil* | Автентифікація, надмірність, моніторинг |
| Транспортний | Флуд-атаки | Клієнтські пазли |
| | Порушення синхронізації | Автентифікація |
| Прикладний | *DoS*-атака на базі маршруту | Автентифікація, використання захисту проти повторних відправлень |

В результаті аналізу, проведеного в статті [10], було виявлено, що:

– невірно налаштовані служби, такі як *NTP*, *DNS* і *SSDP*, часто використовуються зловмисниками для підміни вихідних *IP*-адрес і відправлення величезної кількості запитів на сервери-жертви;

– більшість *DDoS*-атак на даний час здійснюються за протоколом *IPv*4;

– поширюються *DDoS*-атаки за протоколом *IPv*6;

– провайдери і адміністратори на даний час в разі застосування протоколу *IPv*6 не контролюють трафік належним чином і не здійснюють ефективну фільтрацію шкідливих пакетів внаслідок відносної новизни цього протоколу;

– зловмисники здатні відносно легко зламати шлюзові пристрої, які зв'язують *IPv*4- і *IPv*6-мережі, оскільки ці пристрої «змушені зберігати інформацію про весь трафік мережі, що через них передається»;

– більшість пристроїв *IoT* мають серйозні уразливості;

– встановлені за замовчуванням налаштування систем безпеки не забезпечують потрібний рівень захищеності;

– «використовуючи відсутність повноцінних засобів моніторингу *IPv*6-трафіку, слабкий рівень захисту *IPv*4/*IPv*6-шлюзів і величезну кількість незахищених пристроїв Інтернету речей, зловмисники зможуть створювати *DDoS*-ботнети величезних масштабів».

## 2.6 Ознаки *DDoS*-атак

Ознаки *DDoS*-атак можуть варіюватися в залежності від типу атаки та її масштабу, але є кілька загальних характеристик, які дозволяють виявити атаку на ранніх етапах.

1. Різке збільшення трафіку. Атки *DDoS* зазвичай супроводжуються різким збільшенням обсягу трафіку до мережі або серверів. Це може бути як підвищена кількість запитів на певні веб-ресурси, так і збільшений трафік до конкретних портів.

2. Втрата пакетів або проблеми з підключенням.

3. Нестабільність ресурсів ЦП, памяті. Системи можуть почати демонструвати високий рівень використання центрального процесора або пам'яті через велику кількість запитів від зловмисників.

4. Незвичайні шаблони запитів. Однотипні запити або велике. числом схожих запитів з різних джерел.

5. Повторювані спроби аутентифікації або входу. Зловмисники можуть спробувати зламати систему за допомогою багатьох однотипних запитів, що може призвести до перевантаження серверів.

6. Множинні з’єднання від одних і тих же *IP*-адрес.

Виявлення *DDoS*-атак може здійснюватися за різними ознаками, які залежать від технологій проведення атаки.

Атаки *HTTP*-флуд часто спричиняють спроби доступу до неіснуючих або маловідомих ресурсів на веб-серверах.

При атаці *DNS*-флуд спостерігається великий потік *DNS*-запитів.

Для ідентифікації атаки *UDP*-флуду, слід звертати увагу на незвичайні патерни трафіку, такі як велика кількість *UDP*-пакетів з випадковими джерельними адресами та надмірне використання ЦП і пам'яті. Можна також помітити збільшення запитів *DNS* без законних відповідей.

Атака *ICMP*-флуду може бути ідентифікована за значним збільшенням *ICMP* пакетів з боку однієї джерела до атакованого сервісу. Це проявляється у вигляді великої кількості *ICMP Echo Request* (*ping*) пакетів, що надходять одночасно, що перевантажує мережу та знижує продуктивність сервісу. Також може спостерігатися високе використання пропускної здатності та зростання навантаження на сервер, що вказує на наявність атаки.

Під час атаки *SYN*-флуду можна спостерігати такі ознаки: труднощі при підключенні до атакованого сервісу, або довге очікування для встановлення з'єднання. Крім того, можна побачити збільшення кількості неповних запитів на підключення (*SYN* сесій).

Атаки *VoIP*-флуду можна ідентифікувати за збільшеною кількістю втрат викликів, незвичайними патернами спроб встановлення викликів та ознаками перевантаження мережевого інтерфейсу, такими як високе використання ЦП або надмірне споживання пропускної здатності.

При спуфінг-атаці в мережевому трафіку виникає аномально велика кількість пакетів з однаковою адресою відправника і отримувача і наявні провали у трафіку, що відображений графічно.

При пошуку ознак спуфінгу кількість пакетів в одиницю часу у реальному трафіку, що мають однакові адреси і порти (*SRC* і *DST*) відправника і отримувача у поточний момент часу, порівнюється з кількістю таких пакетів, що властива нормальному режиму роботи і визначається експериментально. Суттєві відмінності між цими кількісними показниками свідчать про наявність спуфінгу.

На рис.2.3 представлено графік зміни кількості таких пакетів в експерименті, результати якого наводяться в [28]. Згідно рис.2.3 кількість пакетів з однаковими адресами відправника і отримувача в нормальному режимі роботи не перевищує 10, тобто кількість пакетів більша за 10 свідчать про наявність спуфінгу

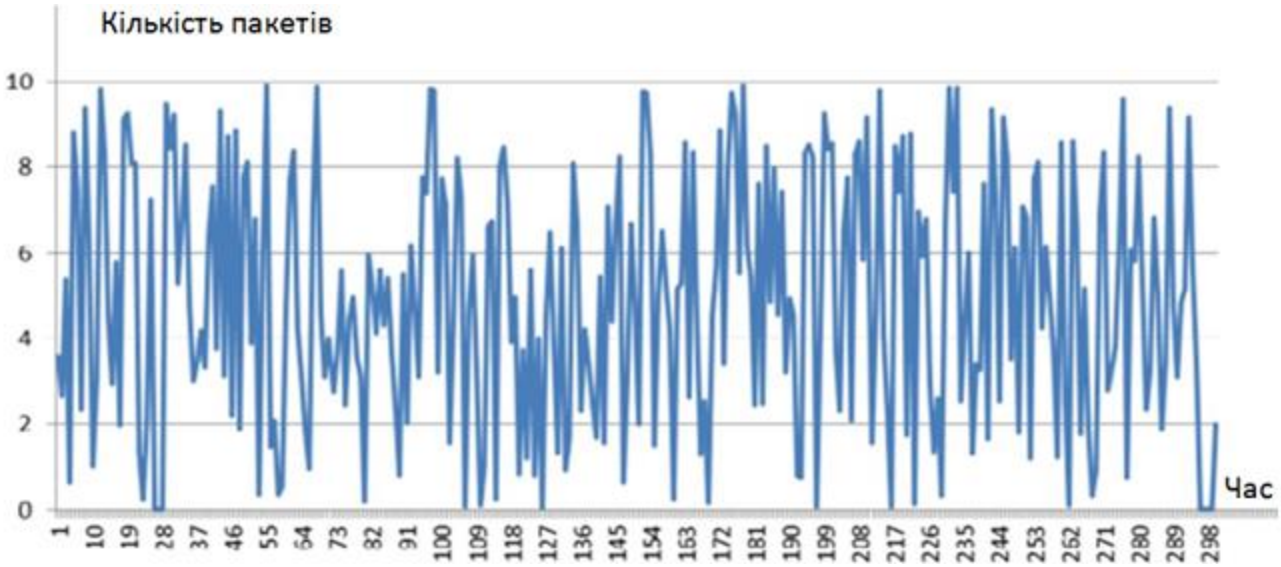



Рисунок 2.3 – Кількість специфічних пакетів при відсутності атаки [20]

# 3 ДОСЛІДЖЕННЯ МЕТОДІВ І ЗАСОБІВ ПРОТИДІЇ *DDOS*-АТАКАМ

## 3.1 Стратегії захисту від *DDoS*-атак

*DDoS*- атаки є серйозною загрозою, що в останні роки, як випливає з п.1.2 даної кваліфікаційної роботи, має тенденцію до зростання практично у всіх країнах і галузях. Для безпечної роботи в Інтернеті компанії повинні на основі розуміння природи, технологій та наслідків *DDoS*-атак впроваджувати:

– ефективні засоби захисту від *DDoS*- атак (засоби виявлення *DDoS*-атак, засоби реагування на *DDoS*-атаки і засоби запобігання *DDoS*- атакам);

– ефективні стратегії пом'якшення наслідків *DDoS*–атак для компанії;

– ефективні засоби і стратегії забезпечення захищеності спільного кіберпростору від *DDoS*-атак, що включають унеможливлення використання ресурсів компанії як зомбі;

Складність боротьби з DDoS-атаками зумовлена тим, що повна витрата ресурсів стає майже буденним явищем, яке може виникати з різних причин, таких як нестача ресурсів сервера, недостатня пропускна здатність або вразливість до слешдот-ефекту. Щоб протидіяти цим загрозам, важливо:

– фільтрувати шкідливий трафік і підтримувати доступність послуг через маршрутизатори і брандмауери;

– постійно моніторити трафік, виявляти аномалії та аналізувати їх;

– досліджувати властивості ІКС, виявляти і нейтралізувати вразливості;

– контролювати продуктивність ІКС в реальному часі;

– формувати у співробітників здатність протидіяти *DDoS*-атакам;

– інформувати працівників про ознаки актуальних *DDoS*-атак і ефективні методи протидії їм;

Для фільтрування шкідливого трафіку та підтримки доступності використовуються брандмауери, балансувальники навантажень, хмарні сервіси, фільтрувальні мережі. Фільтрувальна мережа приймає на себе трафік, фільтрує його і надсилає на цільовий сервер ту частину вхідного трафіку, що відповідає налаштуванням фільтрів, тобто є якісною і надійшла від реальних користувачів. При цьому дуже важливим є правильне налаштування застосованих апаратних і програмних засобів.

Для ефективного контролю мережевого трафіку і продуктивності ІКС, виявлення потенційних вразливостей і джерел атак, вибору впроваджуваних в організації методів і засобів захисту від них необхідною є співпраця з постачальниками інтернет-послуг, розробниками апаратного і програмного забезпечення, а також обмін інформацією та досвідом на рівні організації, галузі, держави і на міжнародному рівні.

Фахівцями [11] рекомендують впроваджувати наступні практики:

1. Вивчення і моніторинг рівня вразливості своєї мережі. Регулярне тестування на вразливості дозволяє виявляти слабкі місця захисту і зміцнювати захист компанії.

2. Використання багаторівневого захисту, комбінуючи різні технології: хмарні рішення, спеціалізоване апаратне і програмне забезпечення, щоб забезпечити надійніший захист від *DDoS*-атак.

3. Регулярне оновлення ліцензійного ПЗ. Оновлення патчів допомагає нейтралізувати вразливості, підвищуючи міцність захисту від DDoS-атак.

4. Планування аудиту кібербезпеки і бізнес-процесів у разі кібератак, включаючи *DDoS*-атаки. Наявність чітких планів дій дозволяє мінімізувати збитки для бізнесу.

5. Навчання співробітників, особливо тих, що працюють з веб-сайтами та онлайн-сервісами. Періодичне підвищення кваліфікації та тренінги дозволяють підтримувати високий рівень обізнаності співробітників щодо ознак кібератак і ефективних методів протидії.

## 3.2 Протидія ботнетам як джерелу *DDoS*-атак

Ботнети є одним із найпоширеніших інструментів для здійснення DDoS-атак. Вони складаються з великої кількості заражених пристроїв, які контролюються зловмисниками для генерації шкідливого трафіку. Ефективна протидія ботнетам включає широкий спектр заходів, спрямованих на виявлення, ізоляцію та знищення бот-мереж, а також на запобігання їх створенню.

Основними методами протидіїї ботнетам є:

1. Виявлення ботнетів:

– використання систем моніторингу для аналізу аномалій у мережевому трафіку, таких як раптове зростання обсягу запитів, нерівномірність географічного походження трафіку або специфічні шаблони запитів;

– отримання інформації про ботнети через співпрацю з організаціями з кібербезпеки або відкритими базами даних, такими як *AbuseIPDB* чи *VirusTotal;*

– виявлення серверів, які керують ботнетом, через аналіз *DNS*-запитів, *IP*-адрес і протоколів;

2. Запобігання зараженню пристроїв:

– навчання користувачів виявляти фішингові листи, шкідливі вебсайти та підозрілі програми, які можуть заразити їхні пристрої;

– забезпечення оновлення прошивки, встановлення складних паролів і використання сегментованих мереж для *IoT*-пристроїв, щоб уникнути їх перетворення на ботів;

– регулярне оновлення програмного забезпечення для виявлення шкідливого коду, який може використовуватися для ботнетів;

3. Ізоляція ботнетів:

– використання списків блокування для обмеження доступу пристроїв, підозрюваних у зараженні ботнетами;

– заборона підключення до відомих командних серверів через фільтрацію DNS на рівні провайдера або корпоративної мережі;

4. Знищення ботнетів:

– співпраця з правоохоронними органами, провайдерами та реєстраторами доменів для закриття командних серверів;

– створення "білих ботнетів", які проникають у шкідливі мережі для їх аналізу та руйнування;

– запуск захисного програмного забезпечення, наприклад, *Botnet Tracker* може автоматично ізолювати заражені пристрої і виявляти їх взаємодію з командними серверами.

Ці методи можуть значно зменшити ризик створення і впливу ботнетів, знижуючи загрозу *DDoS*-атак для мереж та окремих пристроїв.

## 3.3 Протидія *flood*-атакам

Найпоширеніші *DoS*/*DDoS*-атаки базуються на застосуванні флуду, який може бути представлений пакетами різного типу (див. п.2.2.4 даної кваліфікаційної роботи) і реалізовуватися на різних рівнях моделі *OSI* (див. табл.2.2, табл.2.3).

Захист від *flood*-атак (від «затоплення») слід будувати з врахуванням того, що сучасні *DoS*-боти і ботнети можуть використовувати окремі або всі види *flood*-атак одночасно.

Способи боротьби із флудом, що є ефективними для різних типів флуду наведені в табл.3.1. Вони можуть включати в себе налаштування брандмауерів і серверів, впровадження технічних рішень і організаційних заходів тощо.

Таблиця 3.1 – Способи подолання *flood*-атак

| Тип | Характеристика | Способи подолання | |
|---|---|---|---|
| | | Спосіб | Команда |
| *ICMP*-флуд | Забивається смуга пропускання і створюються навантаження на мережевий стек шляхом простого монотонного надсилання запитів *ICMP ECHO* (пінг).<br>Атака легко ідентифікується за допомогою аналізу потоків трафіку в обидві боки: під час атаки типу *ICMP*-флуд обидва трафіки практично ідентичні. | Відключенні відповідей на запити *ICMP ECHO* | # sysctl net.ipv4.icmp_echo_ignore_all=1 |
| | | За допомогою брандмауера | # iptables -A INPUT -p icmp -j DROP --icmp-type 8 |
| *SYN*-флуд | Спосіб забити канал зв'язку і унеможливити приймання мережевим стеком нових запитів на підключення шляхом ініціалізації багатьох одночасних *TCP*-з'єднань за допомогою *SYN*-пакетів з неіснуючою зворотною адресою.<br>Атака ідентифікується шляхом спроби підключитися до одного із сервісів. | Збільшення черги «напіввідкритих» *TCP*-з'єднань | # sysctl -w net.ipv4.tcp_max_syn_backlog=1024 |
| | | Зменшення часу утримання «напіввідкритих» з'єднань | # sysctl -w net.ipv4.tcp_synack_retries=1 |
| | | Включення механізму *TCP syncookies* | # sysctl -w net.ipv4.tcp_syncookies=1 |
| | | Обмеження максимальної кількості «напіввідкритих» з'єднань з одного *IP* до конкретного порту | # iptables -i INPUT -p tcp --syn --dport 80 -m iplimit --iplimit-above 10 -j DROP |
| *UDP*-флуд | Забивається смуга пропускання з використанням нескінченного надсидання *UDP*-пакетів на порти різних *UDP*-сервісів. | Обмеження кількість з'єднань в одиницю часу із *DNS*-сервером на боці шлюзу | # iptables -i INPUT -p udp --dport 53 -j DROP -m iplimit --iplimit-above 1 |
| | | Заборона зовнішніх доступів, фактична ізоляція *UDP* сервісів від зовнішнього світу і | |
| *HTTP*-флуд | *Web*-сервер перевантажується *http*-повідомленнями *GET* на 80-й порт і втрачає здатність обробляти решту запитів, або перевантажується один ресурсоємний скрипт. Найчастіше | Конфігурування *web*-сервера і бази даних з метою зниження негативного ефекту від атаки | |
| | | Протидія *DoS*-ботам шляхом: | Приклад: |

Продовження таблиці 3.1

| Тип | Характеристика | Способи подолання | |
|---|---|---|---|
| | | Спосіб | Команда |
| | проводиться ботнетом<br>Атака ідентифікується за аномально швидким зростанням логів *web*-сервера. | Збільшення максимально припустимої кількості одночасних з'єднань до бази даних | # vi /etc/nginx/nginx.conf<br># Збільшує максимальну кількість використовуваних файлів<br>worker_rlimit_nofile 80000;<br>events {<br># Збільшує максимальну кількість з'єднань<br>worker_connections 65536;<br># Використовувати ефективний метод метод epoll для обробки з'єднань<br>use epoll;}<br>http {<br>gzip off;<br># Відключаємо таймаут на закриття keep-alive з'єднань<br>keepalive_timeout 0;<br># Не віддавати версію nginx в заголовку відповіді<br># Скидати з'єднання після таймауту<br>reset_timedout_connection on;<br>}<br>server_tokens off;<br># Стандартні налаштування для роботи як проксі<br>server {<br>listen 111.111.111.111 default deferred;<br>server_name host.com www.host.com;<br>log_format IP $remote_addr;<br>location / {<br>proxy_pass http://127.0.0.1/;}<br>location ~*<br>\.(jpeg\|jpg\|gif\|png\|css\|js\|pdf\|txt\|tar)$ {<br>root /home/www/host.com/httpdocs;}} |
| | | Встановлення перед *web*-сервером *Apache* легкого і продуктивного *nginx*, який буде кешувати запити і видавати статику | |
| | | Для захисту від атаки з використанням фреймів або посилань: знайти *URL* ресурсу, з якого перейшов за посиланням користувач, у заголовку *referer HTTP* запиту, що встановлюється браузером користувача. Сформувати на основі статистики за кількістю переходів перелік дозволених сайтів, з якого виключи сайти, на яких офіційно розміщені рекламні або інші посилання на ресурс (каталоги, прайс агрегатори). Застосувати цей перелік для фільтрування зв'язків. | |
| | | Для захисту від атак із застосуванням ботнет: у відповідь на запит користувача, який невідомий *web*-серверу, надсилати скрипт на мові *Javascript* і надавати доступ до запрошених | |

Продовження таблиці 3.1

| Тип | Характеристика | Способи подолання | |
|---|---|---|---|
| | | Спосіб | Команда |
| | | користувачем даних тільки після правильного виконання коду скрипту. Метод базується на тому, що боти найчастіше не здатні інтерпретувати скрипт на *Javascript*. Проблемою при використанні даного способу захисту є необхідність забезпечення безперешкодного доступу до даних *web*-сервера пошукових ботів. | |
| | | Для захисту від атак, що організовані групою зловмисників необхідно застосовувати засоби їх виокремлення із маси звичайних користувачів. З цією метою збирається і аналізується статистика доступу користувачів до ресурсу. Якщо частота відвідувань з одної IP адреси перевищує заданий поріг, то користувачу може бути запропоновано ввести перевірочні символи і подальший зв'язок з ним визначається результатами перевірки.<br>Кількість одночасних підключень з однієї адреси може бути обмежена *nginx*-модулем *ngx_http_limit_req_module.* | |

Проти усіх видів флуду рекомендується впроваджувати наступні заходи, які є універсальними:

– усі сервери з прямим доступом до зовнішньої мережі мають можливість швидко перемикатися на інший мережевий інтерфейс або відокремлений режим у разі, якщо основний канал зайнятий. Це забезпечує доступ до сервера навіть при атаці;

– використання актуального програмного забезпечення на серверах є критично важливим. Регулярне застосування оновлень і патчів захищає від вразливостей і недоліків, які можуть бути використані під час *DoS* і *DDoS* атак;

– адміністративні служби, такі як для прослуховування, мають бути приховані брандмауером. Це запобігає використанню їх зловмисниками длядля *DoS* чи *DDoS* атаки (за виключенням випадку вдалого підвищення ним власних прав до рівня адміністратора, що є складною задачею і трапляється не часто);

– установлення системи аналізу трафіку на найближчому до сервера маршрутизаторі дозволяє виявити ознаки початку атаки і вчасно застосувати захисні заходи;

– передбачити у конфігураційному файлі фільтрацію від спуфінгу, часті перевірки *TCP*-з’єднання (легальні машини швидко відповідатимуть), проведення декількох перевірок перед закриттям з’єднання. Наприклад, в */etc/sysctl.conf* можна додати:

–

```
# vi /etc/sysctl.conf
# Захист від спуфінгу
net.ipv4.conf.default.rp_filter = 1
# Перевіряти TCP-з'єднання кожну хвилину. Якщо на іншій
стороні – легальна машина, вона зразу відповість.
# Значення за замовчуванням – 2 години.
net.ipv4.tcp_keepalive_time = 60
<# Повторити спробу через десять секунд
net.ipv4.tcp_keepalive_intvl = 10
# Кількість повірок перед закриттям з'єднання
net.ipv4.tcp_keepalive_probes = 5
```

Для ефективного захисту від *DDoS*-атак також важливо мати широкий канал пропускної здатності, здатний поглинати невеликий трафік ботнетів, оскільки більшість ботнетів є відносно невеликими. Вкрай важливим є також використання розподіленої обчислювальної мережі з дублюючими серверами, підключеними до різних магістральних каналів. Це забезпечує високу стійкість до атак, особливо у разі вичерпання ресурсів однієї лінії або сервера.

Ці заходи знижують витрати ресурсів системи, відповідно знижуючи ефективність *DDoS*-атак. Зокрема, це включає налаштування параметрів або структури самої системи, що дозволяє протистояти флуд-атак без істотного впливу на клієнтів або репутацію компанії.

## 3.4 Захист від атак *Slowloris* та *NXDOMAIN*

Протидія атакам *Slowloris* включає наступні підходи:

1. Здійснення моніторингу *HTTP*-запитів на сервері з метою виявлення аномальних патернів, таких як велика кількість відкритих, але не завершених з’єднань. Це дозволяє вчасно виявити атаки і заблокувати зловмисний трафік.

2. Веб-сервери можуть бути налаштовані для обмеження кількості одночасних запитів від одного користувача або *IP*-адреси. Це допомагає знизити ризик атак *Slowloris*, оскільки зловмисник не зможе утримувати відкриті з’єднання без блокування нових.

3. Використання мережевих фаєрволів, які можуть виявляти та блокувати запити, які залишають з’єднання відкритими надто довго. Системи виявлення вторгнень або системи запобігання вторгненням можуть також бути налаштовані для ідентифікації та реагування на атаки *Slowloris*.

4. Використання *CAPTCHA*, обмежень швидкості запитів або обмежень на *IP*-адреси під час великих обсягів трафіку допомагає відсіяти автоматизовані атаки *Slowloris.*

5. Регулярне оновлення веб-сервера та компонентів, пов’язаних з обробкою запитів, допомагає усунути вразливості, які можуть бути використані для проведення *Slowloris* атак.

Протидія атакам *NXDOMAIN* включає наступні підходи:

1. Використання спеціалізованих систем для моніторингу та аналізу *DNS*-запитів на аномалії. Це дозволяє виявити ненормальні патерни, такі як запити з великим обсягом неправильної інформації або запити, що надходять з нестандартних джерел, і заблокувати їх.

2. Встановлення обмежень на кількість одночасних запитів з одного *IP*-адреси. Це допомагає запобігти спам атак *NXDOMAIN*, коли зловмисники генерують величезну кількість запитів з однієї *IP*-адреси.

3. Використання *DNS* секретів або криптографічних підписів для верифікації *DNS*-запитів. Це дозволяє уникнути відповідей з неправильними або несправжніми запитами, оскільки серверам важко підробити справжні відповіді без ключа.

4. Розглянути використання спеціалізованих протоколів, таких як *DNSSEC* (*DNS Security Extensions*), які додають додатковий рівень захисту шляхом підписування відповідей *DNS* і перевірки їх достовірності.

5. Розробка політики *DNS* для обробки запитів з певними характеристиками, що можуть бути аномальними або небезпечними, і встановлення відповідних обмежень або фільтраційних правил.

## 3.5 Захист *IoT*-пристроїв від *DDoS*-атак

*IoT*-пристрої стають одними з найуразливіших цілей для *DDoS*-атак через обмежені ресурси, низький рівень безпеки та відсутність належного оновлення програмного забезпечення. Щоб запобігти використанню *IoT*-пристроїв як інструментів для атак чи забезпечити їх стійкість до атак, необхідно застосовувати низку заходів.

Першим і одним із найважливіших методів захисту є регулярне оновлення програмного забезпечення та прошивки. Це дозволяє усувати відомі вразливості, якими можуть скористатися зловмисники.

Рекомендується використовувати автоматичні механізми оновлення, щоб гарантувати своєчасне застосування патчів безпеки.

Надійні паролі та автентифікація є наступним важливим кроком. Для кожного пристрою потрібно встановлювати унікальні й складні паролі. Використання простих або однакових паролів на кількох пристроях значно підвищує ризик компрометації. Додатково рекомендується впроваджувати двофакторну автентифікацію, яка додає ще один рівень захисту.

Щоб запобігти несанкціонованому доступу до *IoT*-пристроїв, необхідно налаштовувати міжмережевий екран (фаєрвол), який фільтрує вхідний і вихідний трафік, обмежуючи доступ лише для довірених *IP*-адрес. Варто також сегментувати мережі, відокремлюючи *IoT*-пристрої в окремі підмережі. Це допоможе мінімізувати ризики поширення загрози на інші пристрої при атаці.

Шифрування даних також відіграє важливу роль у захисті *IoT*-пристроїв. Використання протоколів *SSL/TLS* для передачі даних між пристроями забезпечує конфіденційність і запобігає перехопленню важливої інформації.

Моніторинг активності *IoT*-пристроїв дозволяє виявляти аномалії в їхній поведінці, що може свідчити про спроби атак. Постійний аналіз мережевого трафіку за допомогою систем виявлення вторгнень є ефективним способом раннього виявлення загроз.

Не менш важливою є деактивація невикористовуваних функцій пристроїв. Багато *IoT*-пристроїв мають відкриті порти або активовані сервіси, які фактично не використовуються. Відключення таких функцій зменшує вектор атак і підвищує загальну безпеку системи.

Захист від ботнетів включає інтеграцію антивірусного програмного забезпечення та використання спеціалізованих хмарних платформ для *IoT*-безпеки. Ці заходи допомагають виявляти та ізолювати шкідливі програми, які можуть бути використані для залучення пристроїв до бот-мереж.

Застосування всіх цих заходів у комплексі дозволяє значно знизити ризик використання *IoT*-пристроїв для здійснення *DDoS*-атак, підвищити їх стійкість до зовнішніх загроз. Постійне оновлення безпекових рішень і моніторинг стану пристроїв є обов'язковими складовими ефективної стратегії захисту.

## 3.6 Захист серверу від *DDoS*-атак

Для організації захисту важливо вивчити типи атак, їх ознаки (індикатори) та можливі вектори атак.

На сервері можливі *DDoS*-атаки, спрямовані на служби додатків, протоколів, сервісів:

– атаки на транспортному і мережному рівні моделі *OSI*. Такі атаки мають на меті заповнення черги на підключення чи заповнення смуги пропускання і можуть реалізовуватися за різними технологіями, наприклад, *SYN flood* чи *UDP*-спуфінг;

– атаки на протоколи, які спрямовані на сервери, що використовують конкретний протокол (наприклад, *HTTP*, *FTP*, *SMTP*) для ускладнення або повного блокування доступу до сервера. Наприклад, при атаці на *DNS* зловмисник відправляє фальсифіковані запити до відкритого *DNS*-сервера з хибною *IP*-адресою;

– атаки на вразливі місця інфраструктури, наприклад, сервіси автентифікації, фаєрволи, сервери Reverse проксі, DNS, VPN тощо.

Рекомендовані заходи і засоби захисту сервера від *DDoS*-атак визначаються типами атак, актуальних для конкретної ІКС. В загальному випадку рекомендується:

– організувати фільтрацію трафіку за допомогою встановлення на маршрутизаторі спеціального ПЗ-фільтр, яке буде аналізувати вхідні пакети, визначати їх відповідність настроюванням фільтра і видаляти хибні або навіть просто підозрілі пакети. Нелігітимний трафік до серверу, який захищається,

буде мінімальним, якщо фільтр встановлюється щонайближче до точки входу трафіку в інфраструктуру, тобто на найближчому до сервера маршрутизаторі;

– застосувати фаєрвол і налаштувати його так, щоб відкритими були тільки ті порти і сервіси на них, які потрібні для виконання функцій ІКС, що захищається, тобто за принципом «заборонено все, що не дозволено;

– визначити і впровадити доцільні обмеження на кількість запитів з однієї *IP*–адреси та на кількість запитів від одного користувача

– використовувати послуги *CDN*. *CDN* є географічно розподіленою мережею серверів доставки контенту, яка зберігає копії необхідного користувачам контенту. Користувачі в *CDN* отримують контент з фізично найближчих до них вузлів мережі, а не з центрального сервера, завдяки чому навантаження на центральний сервер знижується, і він стає стійкішим до *DDoS*-атак, особливо до атак невеликими ботами. *CDN* дозволяє пом'якшити наслідки *DDoS*-атак, але не дозволяє зупинити чи запобігти саму атаку;

– використовувати послуги провайдерів для захисту сервера. Провайдер зазвичай здатен забезпечити професійний захист, оскільки має фінансову змогу і технічні засоби для застосування широкого спектру технологій, якісної фільтрації трафіку, контролю та захисту системи на мережевих рівнях 3-7;

– орендувати захищений виділений сервер, що забезпечує міцний захист від *DDoS*-атак на на мережевих рівнях 3-7 і, в разі потреби, надає ресурси для масштабування проекту. Це одне з кращих рішень для високонавантажених проектів;

– регулярно оновлювати ПЗ (як операційну систему, так і додатки на сервері);

– регулярно аналізувати систему, застосовуючи сканери вразливостей (наприклад, *OpenVas, Nikto, Nessus, XSSer* тощо) і інструменти пентестингу;

– щорічно проводити стрес-тестування для визначення стійкості системи до *DDoS*-атак і поточних параметрів системи, які необхідні для налагодження засобів захисту, зокрема для обмеження кількості запитів з однієї адреси і від одного користувача;

– періодично проводити комплексну перевірку стійкості проекту до кіберзагроз, в ідеалі – із залученням фірм що спеціалізуються в галузі ІБ. Наприклад, глибока діагностична інфраструктура *DDoS-Guard* виявляє шкідливе ПЗ, *IP* -адреси та відкриті порти, які становлять загрозу для безпеки, і надає клієнтам повний звіт щодо виявлених уразливих елементів і помилок та рекомендації щодо їх усунення;

– регулярно проводити резервне копіювання системи для забезпечення її швидкого відновлення у випадку *DDoS*-атак;

– враховувати, що міцний захист від *DDoS*-атак самостійно забезпечити може лише організація, яка займається ІБ, має відповідні кадри і кошти. Для всіх інших організацій найліпшим рішенням щодо захисту сервера є підключення професійного захисту або оренда серверу у надійного провайдера, який має захист від *DDoS*- атак усіх типів.

Інструментами захисту сервера від *DDoS*-атак можуть бути (див.п.3.9 даної кваліфікаційної роботи):

– засоби, які пропонують хостингові компанії;

– спеціалізовані сервіси: *IPTables* (фільтрація трафіку), *Fail2ban* (надбудова до фаєрволу);

– програмні фільтри, що використовують *JavaScript*.

Захист сервера від *DDoS*-атак здійснюється за принципами, наведеними в п.3.1 даної кваліфікаційної роботи.

## 3.7 Захист *DNS*-серверів від *DDoS*-атак

*DNS*-сервери є критично важливими для функціонування Інтернету, оскільки вони забезпечують перетворення доменних імен у *IP*-адреси. Через це вони часто стають цілями для *DDoS*-атак, які можуть призвести до недоступності веб-сайтів та онлайн-сервісів. Для захисту *DNS*-серверів

використовуються різні методи та технології, спрямовані на зниження ризиків і забезпечення безперервної роботи.

1. Розподіл серверів та резервування.

Рекомендується розташовувати *DNS*-сервери в різних географічних точках. Це дозволяє рівномірно розподілити навантаження, а в разі виходу одного сервера з ладу інші можуть взяти на себе його роботу.

2. Обмеження швидкості запитів.

Необхідно встановити обмеження на кількість запитів від одного користувача. Це допомагає уникнути перевантаження через занадто велику кількість запитів, що характерно для флуд-атак.

3. Фільтрація трафіку.

Використання фаєрволів і систем для виявлення вторгнень дозволяє блокувати підозрілий трафік. Також можна налаштувати блокування запитів із небезпечних *IP*-адрес чи підозрілих країн.

4. *Anycast*-мережі.

*Anycast* – це технологія, яка перенаправляє запити до найближчого DNS-сервера. Завдяки цьому атака на один сервер не виведе з ладу всю систему, адже запити автоматично перенаправляться на інші сервери.

5. *DNSSEC* – захист від підробки.

*DNSSEC* додає до *DNS*-записів цифрові підписи. Це не зупиняє *DDoS*-атаки, але гарантує, що користувач отримає справжню відповідь, а не підроблену.

6. Захист кешу.

Щоб уникнути атак на кеш *DNS*-сервера, варто регулярно його очищати і використовувати додаткові механізми автентифікації.

7. Хмарні сервіси для захисту *DNS*.

Спеціалізовані сервіси, такі як *Cloudflare* чи *Akamai*, забезпечують фільтрацію трафіку, захист від атак і автоматичний перерозподіл навантаження. Це значно підвищує стабільність і безпеку серверів.

8. Моніторинг і виявлення аномалій.

Постійний моніторинг трафіку допомагає вчасно виявити підозрілі дії. Якщо спостерігається різке збільшення запитів, це може свідчити про атаку.

9. Відмовостійкість серверів.

Слід використовувати технології, які дозволяють серверу працювати навіть при дуже великому навантаженні. Це включає резервування потужностей і оптимізацію роботи обладнання.

Комплексний підхід до захисту *DNS*-серверів включає в себе всі вищезазначені заходи. Це забезпечує стійкість до різних типів атак і допомагає підтримувати стабільну роботу сервісів навіть у найскладніших умовах.

## 3.8 Захист мережі від *DDoS*-атак

*DDoS* -атаки є однми з найбільш поширених і небезпечних загроз, а мережева інфраструктура є важливою складовою бізнесу, що забезпечує співробітникам постійний доступ до інформаційних ресурсів, необхідних в процесі роботи, і можливість обмінюватися інформацією. *DDoS* -атаки можуть призвести до серйозних наслідків для бізнесу, тому для захисту мереж застосовуються спеціальні засоби захисту, які дозволяють:

– запобігти порушенням бізнес-процесів, які призводять до фінансових витрат, до втрати клієнтів, до порушення взаємодії з партнерами;

– забезпечити відповідність законодавчо встановленим для галузі застосування ІКС вимогам щодо захисту інформації;

– запобігти порушенням не тільки доступності, а й цілісності і конфіденційності інформації, що можуть статися у випадку вторгнення зловмисника в мережу при реалізації ним складних атак, однією із складових котрих є *DDoS* –атака.

До заходів захисту мереж від *DDoS*-атак відносяться:

– проведення аналізу інфраструктури і мережевих ресурсів з метою визначення ознак «нормальної» поведінки вхідного трафіку і сервісів. Ці

ознаки мають бути визначені для різних періодів роботи ІКС, які різняться обсягом і параметрами трафіку, наприклад, для різних періодів доби, пори року тощо. Наявність шаблону «нормальної поведінки» дозволить визначати аномалії, що можуть бути ознаками атак. Аномалії трафіку можуть проявляти як перевищення максимальних параметрів для нормального режиму у характерний період часу. В якості таких параметрів можуть виступати:

а) *BPS* - кількість біт в секунду;

б) *PPS* - кількість пакетів у секунду;

в) *RPS* - кількість запитів у секунду.

– вибір способу захисту мережі відповідно до актуальних для даної ІКС потужностей атак:

а) для боротьби з потужними *DDoS*-атаками - автоматичний захист, наприклад, блекхол (англ. *Remotely - Triggered Black Hole, RTBH*), який дозволяє блокувати небажаний трафік на боці провайдера, тобто до того як він потрапить в атаковану систему;

б) для боротьби з *DDoS*-атаками середньої і малої потужності – гранулярний захист, при якому трафік повністю не блокується: спочатку трафік за допомогою програми-аналізатора аналізується на рівні хмарного провайдера захисту або всередині периметра мережі, і тільки потім, якщо виявлена небезпека, починається фільтрація шкідливого трафіку;

– використання професійного захисту від *DDoS*-атак. Рішення, які пропонують спеціалізовані провайдери можуть забезпечити цілодобовий аналіз трафіку, оперативне реагування на атаки і високий рівень відмовостійкості мережі за рахунок високовартісних засобів і технологій. При підключенні захисту клієнту необхідно враховувати:

а) спосіб підключення до мережі провайдера. Наприклад, підключення до мережі провайдера може бути виконано фізичним способом через інфраструктуру клієнта з кількома вузлами, на яких встановлена система захисту (наприклад, *DDoS-Guard*), або, якщо обладнання клієнта знаходиться

далеко від точки фізичного з'єднання, - через загальнодоступну мережу за допомогою *GRE* - і *IPIP* -тунелювання;

б) схему фільтрації трафіку. Симетрична схема фільтрації (рис.3.2). застосовується, якщо необхідно здійснювати маршрутизацію як вхідного, так і вихідного трафіку через установку провайдера захисту. Аналіз вихідного трафіку надає системі фільтрації додаткові дані. Відповідно, рішення, прийняте на основі більшої кількості даних є більш точним. Асиметрична схема фільтрації (рис.3.3) передбачає, що провайдер не бачить трафік клієнта, а клієнт має високу кваліфікацію і добре розуміється на принципах і процесах маршрутизації та принципах функціонування мережевого обладнання. В окремих випадках, внаслідок недостатньої інформації про вихідний трафік, відбиття *DDoS*-атаки за цією схемою займатиме більше часу. Асиметрична схема фільтрації трафіку може бути застосована тільки при наявності у клієнта штату досвідчених мережевих інженерів, а в іншому випадку слід обирати симетричну схему;

в) тип маршрутизації: за допомогою *IP*-адрес, коли діапазон адрес клієнта делегується провайдеру; за допомогою динамічної маршрутизації (*Border Gateway Protocol, BGP*), за допомогою статичної маршрутизації.

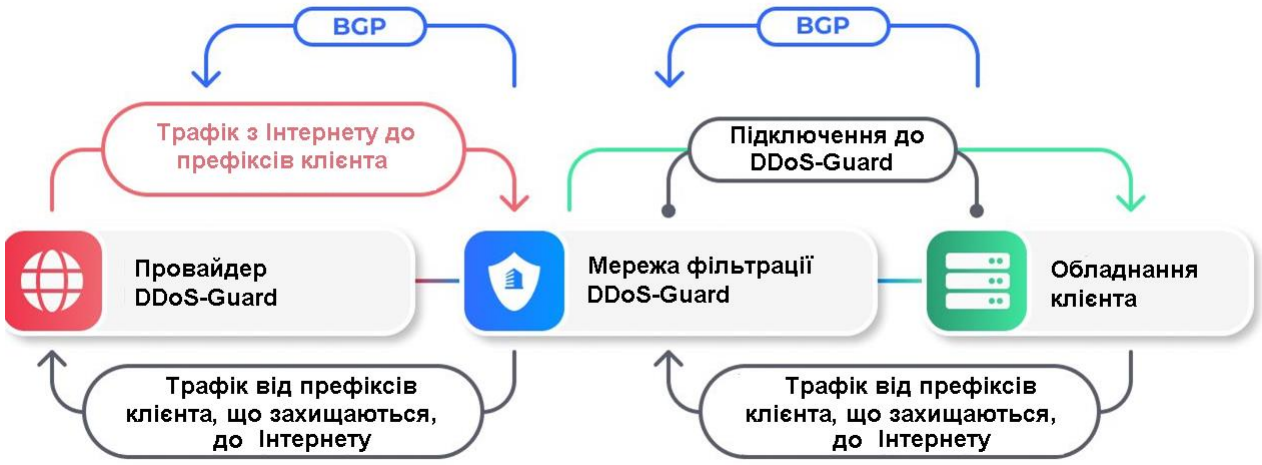



Рисунок 3.2 – Симетрична схема підключення захисту

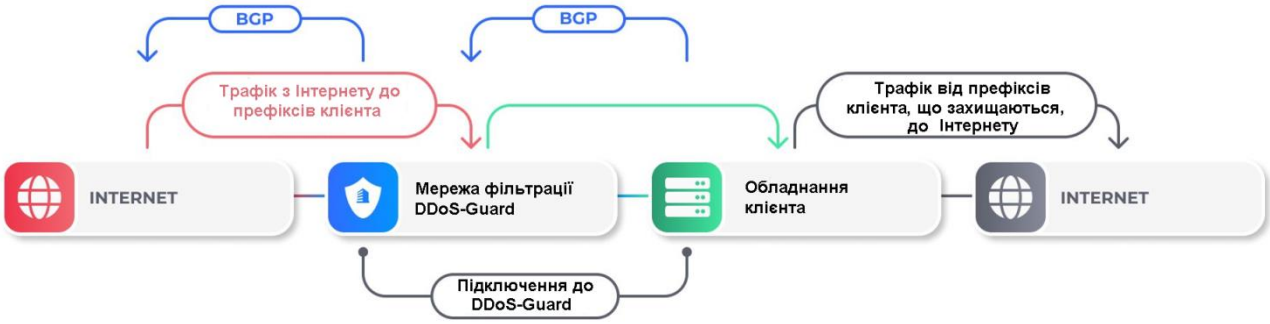



Рисунок 3.3 – Асиметрична схема підключення захисту

– регулярне оновлення ПЗ, особливо на серверах, оскільки багато *DDoS*-атак використовують наявні в ПЗ вразливості;

– проведення аналізу метаданих поточного трафіку: за заголовками та тілами пакетів визначати відправників і адресатів, типи пакетів, кількість пакетів з однієї адреси і на кожний порт тощо. За допомогою комплексної програми аналізу потоку можна виявити *DDoS*-атаку і її тип, а також дослідити профіль використання каналів і в подальшому оптимізувати мережу;

– створення команди із забезпечення кібербезпеки з чітко визначеними функціями її членів, яка при реальній атаці буде реалізовувати заходи протидії, усувати наслідки атаки, збирати та аналізувати дані щодо атак і складати відповідні звіти, вести архіви атак;

– розробка плану реагування на загрози і підготовка команди до його реалізації. План реагування має містити усі *DDoS*- атаки, які можуть бути спрямовані на ІКС, алгоритми оперативних дій для кожного випадку атаки, алгоритми мінімізації критичності наслідків атак, алгоритми врахування набутого досвіду для запобігання успіху атаки в майбутньому і прийняття рішення щодо проведення додаткового аудиту і модернізації системи захисту. План реагування може бути орієнтований на реалізацію спеціалізованою командою або, в разі відсутності можливості її створення, не реалізацію штатними співробітниками. Для того, щоб у випадку атаки дії членів спеціалізованої команди або співробітників були швидкими і ефективними, необхідно періодично проводити навчання у формі тест-драйву.

Таким чином, захист мережі від *DDoS*-атак є багаторівневим динамічним процесом, вимагає моніторингу трафіку, його постійного аналізу та оновлення заходів і засобів захисту, високої кваліфікації виконавців і фінансових витрат на новітні засоби і технології захисту.

## 3.9 Сучасні професійні засоби захисту від *DDoS*-атак

### 3.9.1 Аналізатори трафіку

Аналізатори трафіку (англ. *Traffic Analyzers*) або сніфери (від англ. *sniff* - нюхати) є програмними або апаратно-програмними засобами виявлення та аналізу різних параметрів мережевого трафіку. В плані захисту від *DDoS*-атак вони використовуються для ідентифікації різноманітних аномалій поведінки за наявними образами (шаблонами) нормальної поведінки.

Основними функціями аналізаторів трафіку, які використовуються для захисту від *DDoS* є:

– виявлення аномалій: аналізатори трафіку перехоплюють і аналізують трафік, шукаючи відповідність аномальним шаблонам трафіку, які можуть вказувати на *DDoS* атаку. Наприклад, велика кількість запитів з однієї *IP*-адреси або неочікувані зміни у розподілі трафіку можуть бути ознаками атаки;

– фільтрація трафіку: аналізатори трафіку здатні відфільтровувати шкідливий трафік, що може бути пов'язаний з *DDoS*-атакою, наприклад, шляхом блокування *IP*-адрес, з яких надходять шкідливі запити, або шляхом відтинання трафіку, який відповідає аномалії за певними критеріями;

– візуалізація та аналіз: аналізатори трафіку мають вбудовані інструменти візуалізації та аналізу трафіку, що допомагають адміністраторам швидше виявляти *DDoS* атаки, зокрема, шляхом виявлення аномалій при візуальному аналізу графіків (рис.2.3-2.5), та розробляти ефективні стратегії протидії;

– розподілені системи захисту (англ. *Distributed Defense Systems*): деякі аналізатори трафіку можуть бути інтегровані з розподіленими системами

захисту, які використовують розподілені сервери для фільтрації трафіку перед тим, як він досягне основного сервера. Це дозволяє розподілити навантаження та ефективно фільтрувати шкідливий трафік, що допомагає запобігти перенавантаженню мережі під час *DDoS* атак;

– машинне навчання та аналітика: деякі сучасні аналізатори трафіку використовують методи машинного навчання та аналітику для виявлення та прогнозування *DDoS* атак. Вони навчаються до початку роботи розпізнавати відомі атаки, а потім в процесі роботи вдосконалюють свої знання та розпізнають образи нових, навіть раніше невідомих атак.

У 2024 році на ринку представлені кілька популярних і високоефективних інструментів для аналізу трафіку, які використовуються для виявлення мережевих атак, зокрема *DDoS*, а також для моніторингу та оптимізації мережевих ресурсів, наприклад: *Wireshark, Netscout, Snort* тощо. Розглянемо деякі з них детальніше.

*Wireshark* - це безкоштовний та відкритий аналізатор мережевого трафіку. Він надає можливість захоплювати, відображати та аналізувати пакети даних, що передаються через мережу. *Wireshark* підтримує багато протоколів, включаючи *Ethernet, Wi-Fi, TCP/IP, HTTP, DNS, SSL, SSH* та багато інших. Він може використовуватися для моніторингу мережевої активності, відлагодження проблем з мережею, аналізу безпеки та виявлення аномалій. *Wireshark* надає потужний графічний інтерфейс, який дозволяє переглядати, фільтрувати та аналізувати пакети з детальною інформацією про протоколи, адреси, порти, дані пакетів та інші параметри. *Wireshark* є ПЗ, що поширюється під ліцензією *GNU GPL*, використовує кросплатформову бібліотеку *GTK+* для створення графічного інтерфейсу. Вона має версії для різних типів *UNIX*-подібних операційних систем, включаючи *GNU/Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X*, а також для *Microsoft Windows*. З 2013 року розробники *Wireshark* перейшли на використання бібліотеки *Qt* замість *GTK+*. Причиною такого переходу були проблеми з ефективною підтримкою *GTK+* на всіх платформах, для яких була випущена *Wireshark* і

бажання розробників підготувати версії *Wireshark* для платформ *Apple iOS* і *Android*, підтримка яких доступна в *Qt*.

*Netscout* є однією з провідних платформ для глибокого аналізу мережевого трафіку, яка активно використовується для виявлення аномалій і *DDoS*-атак. Netscout використовує технологію *DPI* для розгляду та аналізу кожного пакету даних, що проходить через мережу. Це дозволяє детально вивчати протоколи, розпізнавати аномальні або шкідливі пакети та виявляти аномалії. Завдяки використанню машинного навчання, *Netscout* автоматично виявляє відхилення у мережевому трафіку, такі як різке збільшення обсягу даних або незвична поведінка пристроїв у мережі. Це дозволяє системі швидко адаптуватися до змін і вживати необхідних заходів без затримок. Наприклад, якщо система виявляє підозріле зростання трафіку, вона може автоматично збільшити пропускну здатність серверів або вжити інших заходів для запобігання збоїв у мережі. Однією з ключових переваг *Netscout* є її здатність до автоматичного масштабування ресурсів у відповідь на високі навантаження. Це означає, що система може оперативно збільшити серверні потужності та інші мережеві ресурси під час *DDoS*-атаки, що допомагає зберегти продуктивність і доступність мережі.

*Snort* – це популярний інструмент з відкритим вихідним кодом, який використовують для виявлення мережевих атак і вторгнень. Він забезпечує детальний аналіз трафіку, аналізуючи кожен пакет даних, що проходить через мережу. Snort використовує сигнатури для виявлення шкідливих активностей, таких як сканування, експлуатація уразливостей, *DDoS*-атаки та інші види шкідливої активності. Інструмент дозволяє гнучке налаштування, що дозволяє користувачам створювати власні правила для ідентифікації специфічних загроз. *Snort* інтегрується з іншими системами безпеки, такими як брандмауери та системи виявлення і запобігання вторгненням, для забезпечення комплексного захисту мережі. Завдяки реалістичному моніторингу трафіку в реальному часі, може своєчасно попереджати адміністраторів про підозрілі дії, що допомагає швидко реагувати на загрози.

*Flowmon* – це інструмент для аналізу мережевого трафіку, який використовує технологію *NetFlow* для збору та обробки даних з метою виявлення аномалій, загроз і забезпечення оптимальної продуктивності мережі. Він здатний в реальному часі аналізувати мережевий трафік і надавати глибокий огляд стану мережі. Аналізує пакети даних на рівні протоколу, що дозволяє виявляти аномалії, такі як шкідливий трафік, незвичайне збільшення обсягу даних або підозріла поведінка користувачів. Інструмент забезпечує реалістичний моніторинг мережевої продуктивності, що дозволяє виявляти вузькі місця, затримки і проблеми з пропускною здатністю. *Flowmon* створює детальні звіти про використання ресурсів, активність трафіку та інші метрики. Може автоматично виявляти і блокувати шкідливий трафік на основі своїх аналізів, зменшуючи ризики проникнення зловмисників у мережу.

Наведені програмні засоби є лише частиною засобів, що пропонуються на ринку для аналізу трафіку. При цьому вони можуть бути спеціалізованими (виконувати тільки аналіз трафіку) і багатофункціональними.

### 3.9.2 Засоби аналізу мережевого трафіку на *Linux*

*IPTraf-ng* — це консольна програма моніторингу статистики мережі Linux. Він надає зручний графічний інтерфейс, що дозволяє користувачам переглядати детальну інформацію про поточний трафік, з’єднання, використання ресурсів і статистику пакетів. Дозволяє користувачам переглядати поточний трафік у реальному часі, включаючи статистику за протоколами (*TCP, UDP, ICMP* тощо).

Інтерфейс користувача *IPTraf-ng* дозволяє налаштовувати фільтри за *IP*-адресами або портами, щоб зосередитися на конкретних з’єднаннях або типах трафіку. Наприклад, можна відстежувати трафік тільки з певних джерел або на певні порти, що допомагає краще контролювати мережу. Підтримує моніторинг кількох мережевих інтерфейсів одночасно, що корисно, якщо є сервер з різними підключеннями. Це дозволяє одночасно бачити всі активні

з’єднання і потік даних, що проходить через різні інтерфейси, що робить його універсальним рішенням для детального контролю трафіку.

*MTR* (англ. *My Traceroute*) – це інструмент для моніторингу мережі, який об’єднує функціонал традиційного трейсрута (*traceroute*) та пінга. Це робить його дуже корисним для аналізу мережевих шляхів і виявлення проблем з підключенням. *MTR* поєднує функціональність трейсрута і ping в одному інтерфейсі. Це означає, що він не лише відстежує, через які маршрутизатори проходить ваш трафік, але й постійно перевіряє час відгуку між кожним маршрутизатором та відслідковує втрати пакетів. Постійно відправляє пакети запитів на зазначену адресу, наприклад, сервер або іншу мережеву точку, і отримує відповіді. Кожен пакет повертається назад з інформацією про час відгуку (латентність) і статус (втрата пакетів). Це дозволяє користувачам бачити, як швидко йде інформація через різні маршрути і чи є втрати на шляху.

*Fail2ban* є програмним забезпеченням, яке додає інтелектуальні функції безпеки, спрямовані на захист від атаки грубою силою, до фаєрволу в операційній системі сервера. Це розширення адаптується до зовнішніх впливів на систему і використовується для реагування на спроби несанкціонованого доступу до сервера з некоректними логінами та паролями. *Fail2ban* аналізує лог-файли системи і, базуючись на цих даних, блокує осіб або *IP*-адреси, що порушують доступність сервера в мережі. Це дозволяє захистити сервер від таких атак як перебір паролів або масові запити до ресурсів, а також від *DDoS*-атак на прикладному рівні. Для ефективного захисту сервера від несанкціонованого доступу та атак на безпеку за допомогою *Fail2ban* необхідно:

– завантажити останню версію *Fail2ban*, яка підходить до встановленої операційної системи;

– створити фільтр для пошуку *IP*-адреси або інших ознак порушення безпеки;

– налаштувати правила блокування, які визначають дії, що будуть вживатися при виявленні випадків порушення безпеки;

– перезавантажити *Fail2ban*, щоб застосувати нові налаштування.

### 3.9.3 Файрволи з функцією захисту від *DDoS*

Файрволи з функцією захисту від *DDoS* – це спеціалізовані системи або пристрої, які допомагають захищати комп'ютерні мережі від масованих атак *DDoS*. Виконують наступні функції:

– постійно моніторять мережевий трафік і використовують алгоритми для виявлення аномалій, які можуть вказувати на *DDoS*-атаку (наприклад, значне збільшення обсягу трафіку за короткий час);

– блокують або обмежують певні типи трафіку, який визначається як потенційно шкідливий (наприклад, трафік з великої кількості *IP*-адрес або з певними шаблонами трафіку);

– можуть автоматично застосовувати обмеження або інші заходи для захисту мережі у разі виявлення *DDoS*-атаки, зменшуючи її вплив на сервіс;

– налаштовуються для специфічних потреб організації, дозволяючи настроювати рівні захисту в залежності від інтенсивності атак, типу трафіку тощо;

Багато сучасних систем використовують штучний інтелект і машинне навчання для виявлення аномалій. Вони можуть використовувати алгоритми для навчання на нормальному трафіку і порівнювати його з поточним, щоб виявити відхилення. Деякі файрволи можуть автоматично ініціювати більш потужні механізми захисту, такі як використання проксі-серверів, розподілених мереж доставки контенту або віртуальних приватних мереж, для фільтрації трафіку і зменшення навантаження. Розглянемо популярні файрволи, які мають функцію захисту від *DDoS*.

*Cloudflare* використовує інтелектуальні алгоритми для розпізнавання і блокування шкідливого трафіку до того, як він досягне кінцевого сервера. Це включає в себе розпізнавання аномальних моделей трафіку і фільтрацію трафіку, що може спричинити перевантаження системи. Автоматично знижує або блокує підозрілий трафік, забезпечуючи швидке реагування на атаки, що дозволяє скоротити час простою і мінімізувати вплив на ресурси сервера. Завдяки наявності серверів у різних частинах світу, *Cloudflare* може швидко реагувати на атаки та забезпечити стабільність під час пікових навантажень.

*Akamai* використовує алгоритми машинного навчання та реальний час аналіз трафіку, щоб виявити аномалії, які можуть свідчити про *DDoS*-атаку. Якщо файрвол виявляє підозрілу активність, він автоматично змінює правила фільтрації та блокування, щоб обмежити вплив трафіку, який може бути частиною *DDoS*-атаки. Це дозволяє зменшити навантаження на сервери та зупинити шкідливий трафік на рівні мережі. Використовує глибинний аналіз трафіку для відокремлення нормального користувацького трафіку від шкідливого. Цей аналіз включає перевірку на зміну моделей трафіку, аномальних запитів і спроб спаму або обману. *Akamai* має можливість автоматично масштабувати свої ресурси для обробки великих сплесків трафіку. Це дозволяє зберігати стабільність сервісів навіть під час пікових навантажень, таких як *DDoS*-атаки. Окрім захисту файрволу, *Akamai* пропонує автоматичне масштабування ресурсів для підвищення пропускної здатності серверів під час пікових навантажень. Це дозволяє оперативно збільшити кількість серверів для обробки трафіку, забезпечуючи захист від *DDoS*-атак. Якщо обсяг трафіку стає критичним, *Akamai* може автоматично розподіляти трафік між різними частинами мережі, мінімізуючи ризик зниження продуктивності і доступності.

*Imperva* – файрвол використовує детектування на основі аналізу поведінки, що дозволяє виявляти аномалії в трафіку ще до того, як вони можуть завдати шкоди серверу. Завдяки автоматичному масштабуванню може миттєво збільшити пропускну здатність і обчислювальні потужності для обробки великого об’єму легітимного трафіку під час пікових атак, що дозволяє підтримувати стабільність і доступність сервісів. Підтримує широкий спектр протоколів, включаючи *HTTP, HTTPS, DNS, FTP, SMTP, POP3*, що дозволяє захищати різні види мережевих додатків і сервісів, незалежно від їх специфіки.

Файрволи з функцією захисту від *DDoS* є важливими інструментами для забезпечення безпеки інтернет-ресурсів та сервісів від атак, що намагаються перевантажити сервер або мережу надмірним трафіком. Такі файрволи можуть забезпечити швидке виявлення та захист від *DDoS*-атак, зменшуючи вплив на доступність систем та покращуючи загальну стабільність роботи.

# 4 РОЗРОБКА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

## 4.1 Системи підтримки прийняття рішень

Система підтримки прийняття рішень (СППР, англ. *Decision Support System, DSS*) – це автоматизована система, яка:

– містить великий обсяг структурованої інформації з певної предметної галузі;

– здатна проводити аналіз інформації користувача, зіставляючи її з інформацією у вбудованій базі даних чи знань;

– здатна виробляти рекомендації щодо проектних і управлінських рішень у при вирішенні певних неструктурованих і слабко структурованих задачах, здійснювати вибір оптимального рішення за багатьма критеріями оцінювання тощо.

Остаточне рішення обирається з множини рекомендованих СППР рішень людиною – особою, що приймає рішення (ОПР).

СППР призначені для розв'язання слабоструктурованих задач, які включають як кількісні, так і якісні дані, часто з невизначеними або суб'єктивними характеристиками. Такі задачі завжди супроводжуються певним ризиком вибору неправильного або неоптимального рішення. Іноді рішення можуть бути отримані у вигляді формального розв'язку з використанням теорії нечітких множин.

СППР можуть бути класифіковані за кількома критеріями:

1. За принципом визначення рішень:

− пасивні СППР, які визначають можливі рішення в межах заданих обмежень без оцінки їх оптимальності;

− активні СППР, які надають оцінки можливих рішень за оптимальністю;

− кооперативні СППР, які реалізують ітераційний процес вибору оптимального рішення шляхом коригування пропонованих рішень;

2. За концепцією управління процесом прийняття рішень:

− СППР, що керуються повідомленнями (групове рішення);

− СППР, що керуються даними (обробка даних);

− СППР, що керуються документами (пошук і обробка неструктурованої інформації);

− СППР, що керуються знаннями (розв’язання задач за допомогою евристик);

− СППР, що керуються моделями (визначення рішень на основі математичних моделей);

3. За кількістю користувачів і масштабом задач:

− СППР для кількох ОПР, що використовують великі сховища інформації;

− настільні СППР для одного ОПР, що вирішують вузькоспеціалізовані завдання;

4. За метою отримання рішення:

− оперативні СППР для негайного реагування на зміни.

− стратегічні СППР для довгострокового аналізу та визначення трендів.

Архітектура СППР включає різні блоки, такі як база даних, система управління даними і знаннями, інтерфейси користувачів та інші системи, які допомагають у прийнятті рішень;

Рішення приймаються на основі двох типів моделей пошуку:

− нормативні моделі, що використовують методи математики, логіки та статистики.

− дескриптивні (описові) моделі, які описують спостережувані процеси або шукають шлях до бажаного стану об’єкта керування.

СППР для слабко структурованих задач призначені для індивідуального використання і підтримуються адміністратором, який може модифікувати базові набори даних і правила. Вони дозволяють вибирати альтернативні варіанти на основі сукупності критеріїв з різними ваговими коефіцієнтами.

## 4.2 Методи прийняття рішень

Прийняття управлінських рішень може здійснюватися в різних умовах:

- в умовах недостатньої інформації;
- в умовах умовно достатньої інформації;
- в умовах достатньої інформації.

Для кожного з цих варіантів умов прийняття рішення можуть використовуватися різні методи (рис.4.1). При цьому процесс прийняття рішення щодо практичної задачі може мати ієрархічну ітераційну структуру, що відображається деревом рішень, і може використовувати різні методи у вузлах ієрархії чи на ієрархічних рівнях. При застосуванні будь-якого методу використовують апріорні і апостеріорні оцінки якості рішень.

В якості методу прийняття рішень в СППР вибору засобів захисту від *DDoS*-атак пропонується застосовувати метод аналізу ієрархій [19], що дозволяє обрати варіант рішення за складною системою критеріїв, кожен з яких має власну вагу для прийняття рішення, і базується на побудові та аналізі матриці попарних порівнянь критеріїв вибору та матриць попарних порівнянь альтернативних рішень між собою за кожним критерієм. Рішення вважається оптимальним, якщо його розрахований глобальний пріоритет є найбільшим.

СППР може видавати ОПР повну множину впорядкованих за глобальними пріоритетами альтернативних рішень, або певну уільність рішень з найвищими пріоритетами.

Процес визначення оптимального за сукупністю критеріїв рішення, які різняться за значимістю для прийняття рішення в конкретних умовах і згруповані за типом оцінюваних узагальнених параметрів, складається з трьох етапів.

На першому етапі методом попарних порівнянь послідовно оцінюються узагальнені критерії на кожному рівні ієрархії критеріїв, починаючи з першого рівня. Групи критеріїв, що знаходяться на одному рівні ієрархії критеріїв, порівнюютьс за важливістю. Для цього користувач заповнює квадратну матрицю попарних порівнянь $A = \{a_{ij}\}$ за множиною правил (4.1).


Рисунок 4.1 – Класифікація методів прийняття управлінських рішень

$$a_{ij} = \begin{cases} 1 \quad при \quad i = j; \\ \dfrac{1}{a_{ji}} \quad при \quad i \neq j \quad та \quad i > j; \\ \dfrac{a_{1j}}{a_{1i}} \quad при \quad i \neq j \quad та \quad i < j. \end{cases} \tag{4.1}$$

де $a_{ij}$ – порівняльні оцінки важливості критеріїв, які відповідають рядку матриці $i$ і стовпцю матриці $j$. Значення $a_{ij}$ визначаються за шкалою Саатті: $a_{ij} \in \left\{\frac{1}{k}, \frac{1}{k-1}, \ldots, \frac{1}{3}, \frac{1}{2}, 1, 2, ,3, \ldots, k\right\}$.

За матрицями попарних порівнянь критеріїв, груп критеріїв та альтернатив обчислюються їх вектори пріоритетів за формулою

$$x_i = \frac{\sqrt[q]{\prod_{j=1}^{q} a_{ij}}}{\sum_{i=1}^{q} \sqrt[q]{\prod_{j=1}^{q} a_{ij}}}. \tag{4.2}$$

де $q$ – кількість критеріїв (груп критеріїв, альтернативних рішень), що порівнюються між собою (матриця $A$ має розмірність $q \times q$, яка залежть від складу групи порівнюваних об’єктів).

При обчисленні пріоритетів критеріїв вибору альтернативних рішень ті критерії, що мають найменші пріоритети можуть бути вилучені з подальшого аналізу. Тоді пріоритети критеріїв і груп критеріїв мають бути перераховані, оскільки розмірність матриці попарних порівнянь зменшується, і самі матриця перевизначається. Процедуру повторюють доти, поки структура ієрархії критеріїв не буде остаточно визначена. Тоді на останньому кроці першого етапу обчислюють глобальні пріоритети елементарних критеріїв як добуток пріоритету критерію в групі і пріоритетів всіх предків групи по ланцюгу в

ієрархії критеріїв до кореневого вузла. В результаті багатошарова ієрархія зводиться до тришарової, в якій листям є альтернативи рішень, другий рівень є рівнем елементарних критеріїв, а третій рівень містить кореневий вузол - мету вибору, тобто оптимальне за сукупністю критеріїїв рішення.

На другому етапі методу аналізу ієрархій проводяться порівняння порівняння альтернатив за кожним критерієм – будуються *m* матриць попарних порівнянь розмірності *n*×*n* (*n* – кількість альтернатив) альтернатив за кожним *r*-им елементарним критерієм $\left(r = \overline{1, m}\right)$ за правилами (4.1), Для кожної матриці обчислюється вектор пріоритетів альтернатив за відповідним *r*-им елементарним критерієм за формулою (4.2).

На третьому етапі методу аналізу ієрархій з *m* векторів пріоритетів альтернатив за елементарними критеріями формується матриця пріоритетів альтернатив $P = \left\lfloor p_t^r \right\rfloor$, де $t = \overline{1, n}$, яка множиться на вектор пріоритетів елементарних критеріїв $\left[pk_t\right]$:

$$PG = \begin{bmatrix} p_1^1 & p_1^2 & \cdots & p_1^r & \cdots & p_1^m \\ p_2^1 & p_2^2 & \cdots & p_2^r & \cdots & p_2^m \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p_t^1 & p_t^2 & \cdots & p_t^r & \cdots & p_t^m \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p_n^1 & p_n^2 & \cdots & p_n^r & \cdots & p_n^m \end{bmatrix} \times \begin{bmatrix} pk_1 \\ pk_2 \\ \cdots \\ pk_r \\ \cdots \\ pk_m \end{bmatrix} = \begin{bmatrix} pg_1 \\ pg_2 \\ \cdots \\ pg_t \\ \cdots \\ pg_n \end{bmatrix}. \qquad (4.3)$$

В результаті отримується вектор глобальних пріоритетів альтернатив $PG = \left[pg_t\right]$ за сукупністю всіх *m* критеріїв з врахуванням важливості критеріїв

Оптимальним є рішення з найбільшим глобальним пріоритетом $pg_{opt} = \max\limits_{t=\overline{1, n}}\left(pg_t\right)$. СППР може видавати ОПР:

– впорядковану за пріоритетами всю множину альтернатив, які розглядалися;

– одне рекомендоване рішення з $pg_t = pg_{opt}$;

– задану кількість рішень з найвищими пріоритетами;

– множину рішень, пріоритети яких відрізняються від $pg_{opt}$ на величину не більшу за задану. Ця величина може бути виражена в абсолютних одиницях або у відсотках від $pg_{opt}$.

## 4.3 Визначення критеріїв захисту від *DDoS*-атак

Як показав проведений в розділах 2 і 3 даної кваліфікаційної роботи аналіз особливостей *DDoS*-атак і наявних на ринку засобів протидії, визначення найбільш доцільного засобу захисту можна здійснити за множиною критеріїв, яка може бути умовно поділена на чотири підмножини:

– критерії придатності;

– ресурсні критерії;

– функціональні критерії;

– якісні критерії;

Критерії придатності визначають можливість застосування певного засобу захисту в конкретних умовах, наприклад, у відповідності до певної операційної системи, сумісності з певними протоколами, чи необхідності інтеграції з іншими ІКС.

До критеріїв придатності належать:

1. Область захисту: сайт, сервер, мережа, мобільний пристрій, Інтернет речей, летючі мережі.

2. Підтримка наявною операційною системою: *Unix, Linux, Windows, Mac, Android.*

3. Підтримувані протоколи: *TCP/IP*, *UDP*, *HTTP*, *HTTPS*, *DNS* і інші.

4. Кількість підтримуваних протоколів: Чим більше протоколів підтримує засіб захисту, тим краще він підготовлений до різних видів атак.

5. Спосіб підключення до мережі провайдера: Інтерфейси підключення (*Ethernet, Fiber, Wireless*).

6. Спосіб маршрутизації: *IP*-адреси, динамічна маршрутизація, статична маршрутизація.

7. Місце розташування відносно мережевого екрану: до мережевого екрану, після мережевого екрану.

8. Схема підключення: асиметрична схема, симетрична схема.

9. Пропускна здатність.

10. Можливість додавання сигнатур інших розробників.

11. Можливість додавання сигнатур користувача.

12. Рівнь виявлення атак: засоби захисту від *DDoS*-атак на рівні мережі, на рівні хосту, на рівні додатків.

Пропускна здатність визначає чи буде засіб захисту уповільнювати роботу ІКС. З цієї точки зору перевагу мають системи захисту, що використовують багатоядерні відеокарти та процесори.

Засоби захисту мережевого рівня досліджують вхідний (іноді - і вихідний) трафік у всій системі на всіх пристроях методом сигнатур або аномалій. Зазвичай такі засоби розташовуються у підмережі біля мережевого екрану задля контролю брандмауеру, не впливають на продуктивність мережі, керуються централізовано і не мають негативного впливу на топологію мережі. Однак такі системи не розпізнають зашифровану інформацію, є високонавантаженими, тобто вимагають додаткових налаштувань і функціональності мережевих пристроїв, найчастіше є пасивними і контролюють тільки внутрішню структуру.

Засоби захисту рівня хосту встановлюються на хості і з нього виявляють атаки або спроби реалізації атаки. Сенсори таких засобів контролюють цілісність файлів, час внесення змін у файли (в тому числу у файли реєстрації, файли системи контролю доступу, файли операційної системи тощо), стан

оперативної памяті і системні логи; аналізують журнали, системні виклики і поведінку програм; збирають відомості про контрольовані параметри трафіку, що є ознаками атак і/або параметрами, врахованими в шаблоні нормального стану системи. Хостові системи захисту є високоточними і продуктивними, однак вони також не мають централізованого управління, є пасивними і працюють лише на одній машині, через яку має проходити весь трафік.

Ресурсні критерії визначають відповідність засобу захисту наявним фінансовим, часовим, людським та апаратним ресурсам.

До ресурсних критеріїв належать:

1. Наявність документації.

2. Наявність персоналу з достатнім рівнем кваліфікації.

3. Умови розпосвюдження: вільне, тріал-версія, платне.

4. Вартість.

5. Вартість навчання персоналу.

6. Вирати часу на встановлення і налаштування засобу та підготовку персоналу.

7. Вартість підтримки розробника при налаштуванні та експлуатації засобу.

8. Необхідний обсяг пам’яті.

9. Можливість співпрацювати із виробниками і розповсюджувачами.

Функціональні критерії характеризують здатність засобу захисту виконувати певні функції, такі як виявлення різних типів DDoS-атак та ефективна реакція на них.

Функціональні критерії включають:

1. Типи *DDoS*-атак, які можуть бути виявлені засобом захисту (сигнатури, аномалії, гібридний аналіз).

2. Кількість типів *DDoS*-атак, які можуть бути виявлені засобом захисту.

3. Рівні моделі *OSI,* , на яких може аналізувати трафік.

4. Метод аналізу трафіку: метод сигнатур, метод аномалій, гібридний аналіз.

5. Кількість рівнів моделі *OSI*: здатність проводити аналіз пакетів на декількох рівнях *OSI* дозволяє засобу захисту виявити більше атак, однак такі системи вимагають більше ресурсів оперативної пам’яті і процесора.

6. Орієнтований обсяг оброблюваної інформації: малий, середній і великий бізнес.

7. Можливість роботи у багатопоточному режимі, що підвищує швидкість, ефективність і допомагає розділяти навантаження.

8. Характер реакції в разі виявлення атаки: пасивні засоби, активні засоби.

9. Спектр дій (можуть комбінуватися) в разі виявлення атаки: розривання з’єднання; відключення системи; блокування зловмисного трафіку; блокування *IP*-адреси; відновлення лог файлів у разі їх втрати; блокування потенційно небезпечних акаунтів; реєстрація в журналі; надсилання повідомлення користувачу; надсилання повідомлення адміністратору.

10. Відкритість коду.

11. *Libpcap* основа.

12. Визначення прихованих даних.

13. Відображення в додатку шару протоколу.

14. Декодування протоколу.

15. Відновлення *TCP* потоку (в т. ч. обмежене – тільки форматоване).

16. Виявлення аномальних даних (в тому числі обмежене, наприклад, просто видача попереджень).

17. Сповіщення знаходження.

18. Відновлення *HTTP web*- сторінки.

19. Мережева комунікаційна матрична мапа.

20. Оцінка критичності трафіку для бізнесу.

21. Здатність обмінюватися даними з іншими ІКС і додатками.

22. *UDP* трафік.

Засіб захисту, що використовує метод аналізу сигнатур розшукує у трафіку блоки, що відповідають образам відомих *DDoS*-атак, що знаходяться в базі даних, і не може виявляти новітні атаки. Образи атак визначають середовище, умови, зв'язки між подіями і параметри трафіку. Відповідність образу атаки може бути повною або частковою. Частковий збіг сигнатур відповідає спробі вторгнення. Сигнатури потрібно постійно оновлювати;

Засоби, що використовують метод виявлення аномалій, можуть виявляти наявність чи підготовку відомої або невідомої атаки за аномаліями параметрів чи подій трафіку.

Пасивні засоби в разі виявлення *DDoS*–атаки тільки надсилають повідомлення користувачу або адміністратору і реєструють атаку в журналі, а активні засоби дозволяють не тільки виявляти загрозу, а й відразу реагувати на поточну (системи виявлення вторгнень) чи потенційно можливу (системи запобігання вторгненням) атаку.

Якісні критерії оцінюють зручність використання засобу захисту та його ефективність

До якісних критеріїв належать:

1. Кількість використовуваних сигнатур.

2. Кількість шаблонів нормального стану.

3. Ефективність виявлення атак: відносна кількість невиявлених атак; відносна кількість хибних спрацьовувань.

4. Ефективність протидії *DDoS*-атакам певного типу: ймовірність виявлення, час придушення, граничні значення стійкості системи.

5. Зручність використання.

6. Зручність оновлення сигнатур.

7. Зручність оновлення шаблонів нормального стану.

8. Наявність підтримки розробника при налаштуванні та експлуатації.

9. Інтерфейс користувача.

10. Наявність декількох інтерфейсів.

11. Адаптовність налаштувань під вимоги користувача.

Визначені вище критерії можуть використовуватися як для вибору засобу захисту методом аналізу ієрархій (MAI) з врахуванням важливості кожного критерію, так і для простого порівняння засобів захисту за бажаними рівнозначними властивостями за вибірковими критеріями (табл.4.1).

Таблиця 4.1 - Порівняльний аналіз сніферів за вибіркою критеріїв

| Критерій | *TCPdump* | *Wireshark* | *Colasoft Packet Sniffing Tools* | *Microsoft Message Analyzer* | *Packet Capture (PCAP)* |
|---|---|---|---|---|---|
| Відкритий код | + | + | - | - | Так |
| Операційні системи | *Linux, macOS* | *Linux, Windows, macOS* | *Windows* | *Windows* | *Linux, Windows, macOS* |
| Кількість підтримуваних протоколів | 200+ | 1200+ | 300+ | 200+ | 200+ |
| Вартість | Безкоштовно | Безкоштовно | Від 999 $ | Безкоштовно | Безкоштовно |
| Використання місця на диску | 10 МБ | 449 МБ для Unix<br>100 МБ для Windows | 320 МБ | 150МБ | 20МБ |
| *Libpcap* основа | + | + | - | - | + |
| Визначення прихованих даних | - | + | + | + | - |
| Відображення в додатку шару протоколу | - | + | + | + | - |
| Декодування протоколу | *Hex, ASCII* | *Hex, ASCI* | *EBDIC, Hex, ASCII* | *Hex, ASCII* | *Hex, ASCII* |
| Відновлення *TCP* потоку | - | Обмежене (тільки форматоване) | + | + | _ |

Продовження таблиці 4.1

| Критерій | *TCPdump* | *Wireshark* | *Colasoft Packet Sniffing Tools* | *Microsoft Message Analyzer* | *Packet Capture (PCAP)* |
|---|---|---|---|---|---|
| Виявлення аномальних даних | - | Дуже обмежене (тільки видача сповіщень) | + | + | _ |
| Сповіщення знаходження | - | + | + | + | _ |
| Відновлення *HTTP web*-сторінки | - | Обмежено (показує актуальний контент трафіку індивідуально) | Обмежено (показує лінки контенту трафіка індивідуально) | + | _ |
| Мережева комунікаційна матрична мапа | - | - | + | + | _ |
| Оцінка критичності трафіку для бізнесу | - | Обмежено (за допомогою створення нових фільтрів та пошуку) | + | + | _ |
| *UDP* трафік | + | + | + | + | + |
| Інтерфейс користувача | *CLI* | *CLI, GUI* | *GUI* | *GUI* | *CLI* |
| Наявність декількох інтерфейсів | - | + | + | + | _ |
| Адаптовність налаштувань під вимоги користувача | + | + | Обмежено (лише розробником на замовлення) | + | _ |

## 4.4 Створення алгоритмів для вибору засобів захисту від *DDoS*-атак

Розробка алгоритмів вибору засобів захисту від *DDoS*-атак є важливою складовою забезпечення безпеки ІКС та мережевої інфраструктури. Він має бути здатним здійснювати класифікацію атак, оцінювати їхній рівень загрози та обирати найбільш ефективні заходи для мінімізації впливу атак.

Узагальнений алгоритм вибору засобів захисту від *DDoS*-атак, який використовується в розроблюваній СППР наведено на рис.4.2. цей алгоритм складається з восьми етапів, на яких виконуються типові процедури.

Етап 1. Формування первинного переліку критеріїв. На цьому етапі формуються критерії, за якими буде здійснюватися вибір оптимального засобу захисту. В СППР є вбудований список стандартних критеріїв (визначених у пункті 4.3 цієї роботи), а також інструменти для додавання власних критеріїв користувачем. Первинний перелік формується шляхом вибору критеріїв з вбудованого списку та, за потреби, доповнення їх новими критеріїми, визначеними користувачем, залежно від специфіки задачі та вимог.

Етап 2. Побудова матриці попарних порівнянь критеріїв. На основі сформованого переліку критеріїв створюється матриця попарних порівнянь, що визначає відносну важливість кожного критерію.

Етап 3. Аналіз вектору глобальних пріоритетів критеріїв. Після побудови матриці попарних порівнянь отримується вектор глобальних пріоритетів критеріїв. Здійснюється аналіз для виявлення критеріїв з низьким рівнем важливості. Ці критерії можуть бути видалені з подальшого розгляду. Якщо всі критерії мають значущий вплив на вибір, то список критеріїв вважається остаточним, і переходимо до наступного етапу.

Етап 4. Видалення критеріїв малої значимості та повторна оцінка. Якщо на етапі аналізу виявлені критерії, що мають низький вплив на загальний вибір, вони видаляються з переліку. Після цього створюється нова матриця попарних порівнянь для меншої кількості критеріїв. Перераховуються їх пріоритети, і результат використовується для подальшої оцінки варіантів засобів захисту. Цей цикл повторюється, поки всі критерії не будуть значущими.

Етап 5. Отримання векторів пріоритетів для альтернативних варіантів засобів захисту. Для кожного варіанту засобу захисту обчислюються вектори пріоритетів за кожним з визначених критеріїв. Це дозволяє порівняти різні засоби захисту на основі їхніх характеристик і здатності задовольнити вимоги користувача.

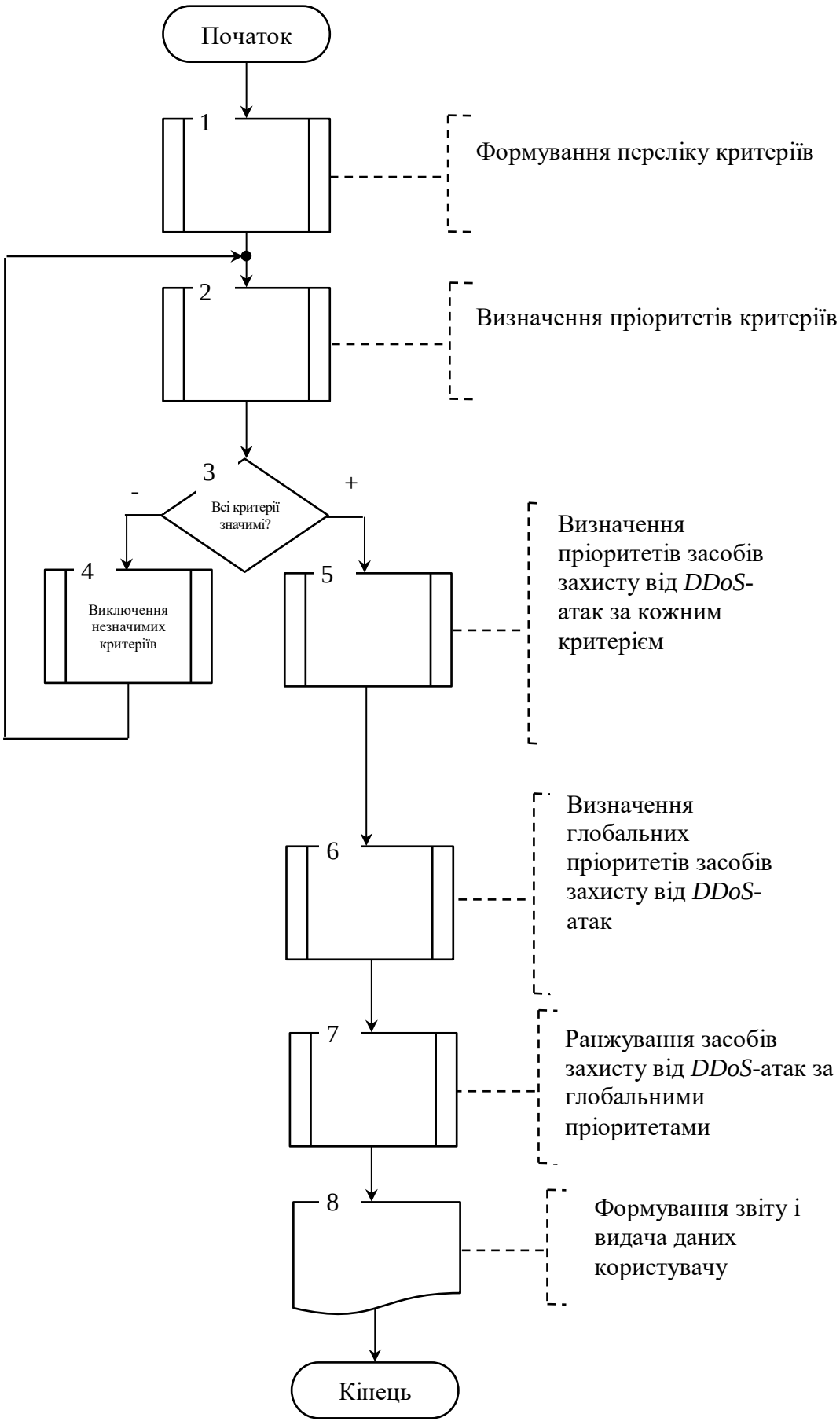



Рисунок 4.2 – Узагальнений алгоритм вибору засобів захисту від *DDoS*-атак

Етап 6. Обчислення вектору глобальних пріоритетів засобів захисту. Обчислюється вектор глобальних пріоритетів для кожного варіанту засобу захисту з урахуванням важливості кожного критерію. Важливість критеріїв може змінюватися в залежності від конкретних умов атаки (наприклад, величина трафіку або тип атаки). Дозволяє визначити загальну оцінку кожного засобу захисту і оцінити його ефективність в конкретних умовах.

Етап 7. Ранжування засобів захисту та вибір оптимального варіанту. Здійснюється ранжування альтернативних варіантів засобів захисту від *DDoS*-атак на основі їх глобальних пріоритетів. Це дає можливість виявити оптимальний засіб або кілька засобів з однаковими максимальними пріоритетами, які є рівнозначними для конкретної ситуації. Під час цього етапу також можна врахувати додаткові фактори, такі як вартість, швидкість реагування або адаптивність засобів.

Етап 8. Формування звіту та видача результатів користувачу. Після того як оптимальні варіанти засобів захисту визначені, формується звіт, який містить докладний аналіз вибору. Звіт включає в себе порівняння всіх розглянутих варіантів, їхні переваги та недоліки, а також рекомендації для користувача. Користувач отримує результат у вигляді звіту, який можна використовувати для прийняття остаточного рішення щодо вибору засобу захисту від *DDoS*-атак.

## 4.5 Розробка структури системи прийняття рішень щодо вибору засобів захисту від *DDoS*-атак

Розробка структури системи прийняття рішень (СППР) для вибору засобів захисту від *DDoS*-атак передбачає інтеграцію різних типів даних і методів їх обробки для забезпечення ефективного та обґрунтованого вибору засобів захисту в конкретних умовах. Така система має враховувати

різноманітні фактори, що впливають на вибір, дозволяти користувачу адаптувати рішення відповідно до специфіки його мережі та вимог безпеки.

Система прийняття рішень створюється для підтримки вибору оптимальних засобів захисту від *DDoS*-атак шляхом аналізу критеріїв (див. п.4.3), що визначають ефективність, вартість та адаптивність кожного засобу.

Основні компоненти СППР (рис.4.3):

– інтерфейс користувача;

– база знань, що містить стандартні критерії оцінки, можливі альтернативи засобів захисту, а також їх характеристики;

– модуль аналізу даних, що обчислює пріоритети критеріїв і альтернатив, виконує порівняння варіантів та визначає оптимальні засоби захисту;

– модуль генерації звітів, що автоматично формує звіт із детальним описом обраного рішення, включаючи порівняльний аналіз та рекомендації;

Користувач через інтерфейс обирає критерії з вбудованого списку або додає нові залежно від специфіки задачі. Для цього створюється форма, яка дозволяє вибрати необхідні критерії або ввести індивідуальні, такі як: тип атаки, обсяг трафіку тощо. Ці дані передаються в базу знань та модуль аналізу даних для подальшої обробки.

База знань містить, наприклад, такі критерії оцінки:

– швидкість обробки атакуючого трафіку;

– одноразові витрати чи вартість підписки;

– зручність впровадження в існуючу інфраструктуру;

– здатність ефективно працювати з ростом трафіку;

– ефективність протидії новим типам атак;

– наявність технічної підтримки;

– сумісність із обладнанням або ПЗ;

Також в базі наявні хмарні рішення, такі як *Cloudflare, Microsoft Azure DDoS Protection*, забезпечують безпеку через централізовані сервіси.

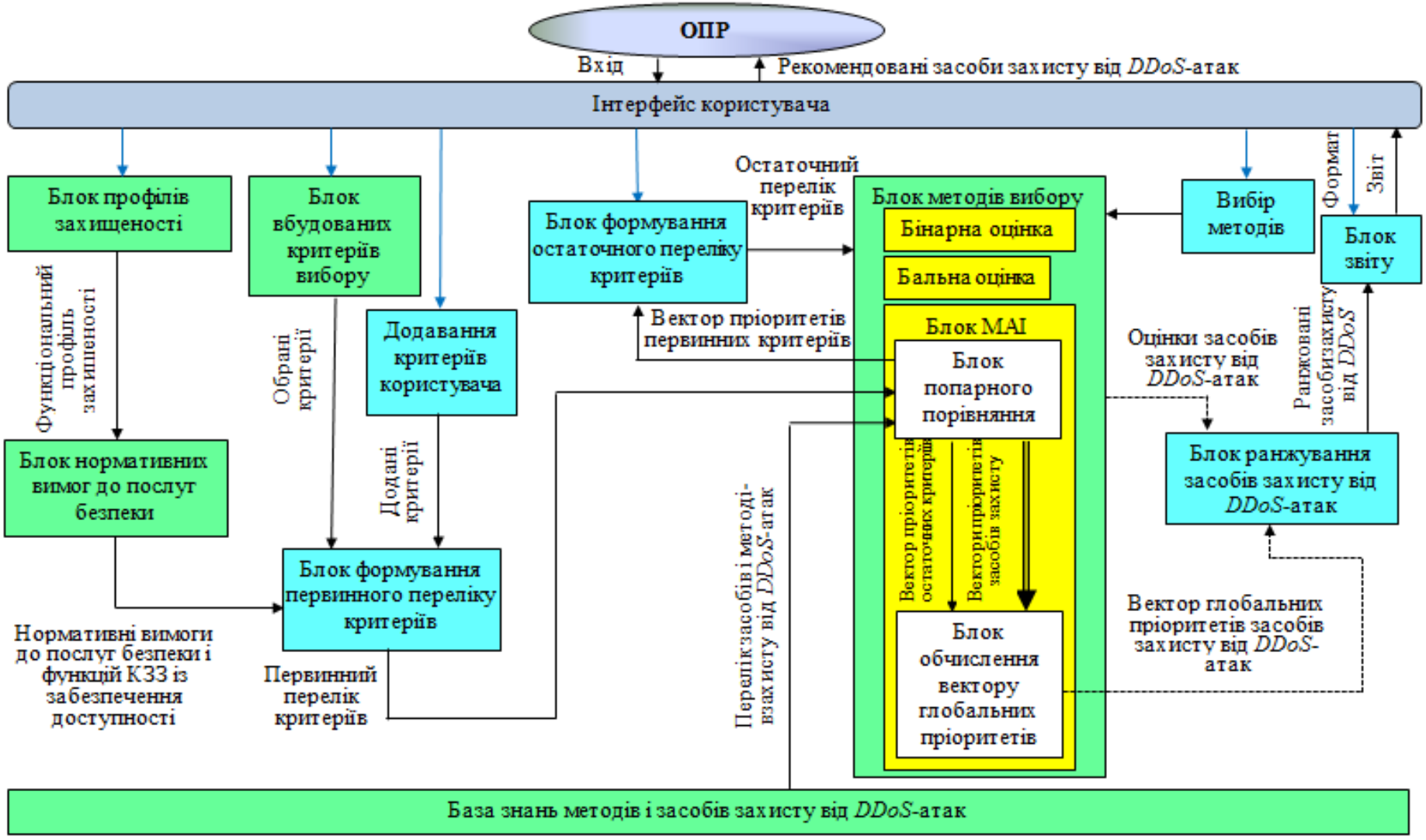



Рисунок 4.3 – Структура СППР

Апаратні засоби, такі як *Cisco* та *Arbor Networks*, включають фізичні пристрої для мережевого захисту, зокрема міжмережеві екрани та системи виявлення вторгнень. Та гібридні рішення, що поєднують переваги хмарних та апаратних засобів, дозволяючи організаціям використовувати як масштабовані хмарні сервіси для початкового захисту, так і апаратні засоби для детального контролю та додаткового рівня безпеки на периметрі мережі.

Модуль аналізу даних здійснює побудову матриці попарних порівнянь, де кожен критерій оцінюється за важливістю (наприклад, за допомогою експертних оцінок або стандартних шаблонів). Це дозволяє розрахувати локальні та глобальні пріоритети для кожного критерію та альтернативи. Далі здійснюється оцінка кожної альтернативи за кожним із критеріїв за шкалою (наприклад, від 1 до 10), що дозволяє отримати інтегральний показник ефективності кожного засобу захисту.

Алгоритм роботи:

1. Користувач вводить критерії та визначає їх ваги (наприклад, важливість продуктивності, вартості, адаптивності тощо).

2. База знань надає дані про доступні засоби захисту, які відповідають вибраним критеріям.

3. Модуль аналізу проводить багатокритеріальний аналіз, застосовуючи методи, такі як метод аналізу ієрархій (*AHP*), для оцінки альтернатив.

4. Модуль обчислює глобальні пріоритети для кожної альтернативи, враховуючи важливість критеріїв та їх оцінки.

5. Формуються ранжування альтернатив, що дозволяє користувачеві зрозуміти, який засіб захисту найбільш ефективний в умовах заданих критеріїв.

Модуль генерації звітів формує звіти, що містять результати багатокритеріального аналізу, порівняння альтернатив та їх характеристик. Звіти можуть бути представлені в різних форматах, включаючи текстові та графічні елементи. У звіті порівнюються характеристики всіх доступних варіантів захисту за обраними критеріями, що дає змогу користувачеві швидко

порівняти ефективність різних засобів захисту за такими параметрами, як продуктивність, вартість, адаптивність та інші. Модуль надає графіки, діаграми та таблиці для зручного сприйняття результатів аналізу.

Зміст звіту включає:

– резюме вибору оптимального засобу захисту;

– таблиця з ранжуванням критеріїв та альтернатив;

– візуалізація результатів;

– рекомендації для впровадження обраного засобу захисту;

Модуль генерації звітів забезпечує користувача усією необхідною інформацією для прийняття обґрунтованого рішення.

СППР має пройти перевірку її правильності та ефективності у виборі засобів захисту від *DDoS*-атак. Це здійснюється через тестові сценарії, такі як вибір засобу захисту за одним або кількома критеріями (наприклад, продуктивність, вартість, масштабованість), перевірку обробки некоректних даних та оцінку додаткових критеріїв (наприклад, технічна підтримка). Оцінка точності результатів проводиться шляхом порівняння рекомендацій СППР з експертними оцінками, використання реальних даних про *DDoS*-атаки, збору зворотного зв'язку від користувачів та аналізу чутливості до змін параметрів. Ці методи дозволяють підтвердити правильність роботи системи та її здатність надавати точні рекомендації для захисту від *DDoS*-атак.

# ВИСНОВКИ

В даній кваліфікаційній роботі проведено аналіз наявних літературних джерел, визначено критерії класифікації *DDoS*-атак та параметри існуючих засобів захисту від них, а також критерії класифікації систем виявлення вторгнень, які є доцільними для застосування в рамках цієї роботи.

Були визначені критерії для прийняття рішень при виборі засобів захисту від *DDoS*-атак, розроблені основні алгоритми та створена структура системи прийняття рішень, що забезпечують вибір засобів захисту від *DDoS*-атак як частину комплексу захисту комп'ютерних мереж за множиною критеріїв, набір і важливість яких для вирішуваної прикладної задачі визначається ОПР.

Робота має наукову новизну і практичну значимість. Наукова новизна роботи полягає у визначенні множини критеріїв, за якими можуть бути оцінені засоби захисту від *DDoS*-атак. Практичну значимість мають розроблені алгоритми і структура СППР, що створюють основу для розробки повнофункціональної СППР. Результати роботи можуть бути застосовані при проектуванні захищених локальних мереж та в освітньому процесі за освітньою програмою «Системи технічного захисту інформації, автоматизація її обробки» зі спеціальностей 125 «Кібербезпека» та 141 «Електроенергетика, електротехніка та електромеханіка».

Дана робота була апробована на XI (2023 р.) і XII (2024 р.) Всеукраїнських науково-технічних конференціях з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Anthony D. Wood and John A. Stankovic A Taxonomy for Denial-ofServi ce Attacks in Wireless Sensor Networks. URL: https://www.cs.virginia.edu/ ~stankovic/psfi les/computer02-dos.pdf*

2. *Blackert W.J., Gregg D.M., Castner A.K., Kyle E.M., Hom R.L., Jokerst R.M. Analyzing interaction between distributed denial of service attacks and mitigation technologies // Proc. DARPA Information Survivability Conference and Exposition. - Vol.1. -- 24 April, - 2003. - P. 26-36. URL: https://ieeexplore.ieee. org/abstract/document/1194870/authors#authors*

3. Cyber Threat Trends in 2024. *URL:* https://www.msspalert.com/native/ cyber-threat-trends-in-2024-the-landscape-according-to-top-industry-reports

4. *Chris Karlof C., Wagner D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, AdHoc Networks (elsevier). – 2003. – P.299302. URL: http://www.chriskarlof.com/papers/senroute-adnj.pdf*

5. *Jenniefer A., Raybin J. Techniques for Identifying Denial of Service Attack in Wireless Sensor Network // Survey International Journal of Advanced Research in Computer and Communication Engineering. - Vol. 3. - Issue 6. -2014.*

6. *URL: https: //arxiv.org/ftp/arxiv/papers/1011/1011.1529.pdf*

7. *NXDOMAIN Attack. URL:* https://threat.media/definition/what-is-an nxdomain-attack/

8. *Perrig A., Stankovic J., Wagner D. Security in Wireless Sensor Networks Communications of the ACM. – 2004. – P.53-57. URL: https://arxiv .org/ftp/arxiv /paper s/1301/1301.5065.pdf*

9. *Raymond D. R., Midkiff S. F. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. - IEEE Pervasive Computing. - January-March 2008. - P. 74-81. URL: http://irep.iium.edu.my/576/1/Pathan-P.pdf*

10. *Slowloris. URL:* https://www.netscout.com/what-is-ddos/slowloris

11. *DDoS*-атаки . *URL: https:// ictn e ws./28/03/2023/ddos/*

12. *DDoS*-атаки . *URL:* https://www.netscout.com/ddos-attack

13. *DDoS Attack Classification. URL:* https://ddos-guard.net/blog/classification-of-ddos-attacks

14. 15 найкращих безкоштовних інструментів *DDoS*-атаки в Інтернеті. *URL: https://techukraine.net/15-%D0%BD%D0%B0%D0%B9%D0%BA%D1*

15. Александер М., Корченко О., Карпінський М., Одарченко Р. Дослідження вразливостей сенсорних підмереж архітектури інтернету речей до різних типів атак // Безпека інформації. - 2016. – Том 22. №1. - С.12-19. *URL: https://dspace.nau. edu.ua/bitstream/NAU/36403/1/10448-26997-1-SM.pdf*

16. Дайджест событий в мире кибербезопасности за первый квартал 2024 года. *URL: https://ddos-guard.net/ru/blog/daidzhest-kiberbezopasnosti-2024*

17. ДБН В.2.5-28-2018. Природне та штучне освітлення. *URL: http: //online.budstandart.com/ua/catalog/doc-page.html?id_doc=79885*

18. ДСанПіН 3.3.2-007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. *URL: https://zakon.rada.gov.ua/rada/show/v0007282-98#Text*

19. ДСН 3.3.6.042.Санітарні норми мікроклімату виробничих приміщень. *URL: https:// zakon.rada.gov.ua/rada/show/va042282-99#Text*

20. Закон України «Про національну безпеку України». *URL*: *https ://zakon. rada.gov.ua/laws/show/2469-19.*

21. Закон України «Про основні засади забезпечення кібербезпеки України». *URL: https://zakon.rada.gov.ua/laws/show/2163-19*

22. Закон України «Про охорону праці». *URL*: *https://www.Google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjpsM3s0vDYAhWD6CwKHfPJChMQFggnMAA&url=http%3A%2F%2Fzakon.rada.gov.ua%2Fgo%2F269412&usg=AOvVaw0KZHyXdio5nFLTg5IjnVgA*

23. Закон України «Про платіжні послуги». *URL*: *https://zakon.rada. gov.ua/l aws/show/1591-20#Text* Звіт про загрози DDoS 2024 року. *URL*: https://blog.cloudflare.com/d dos-threat-report-for-2024-q1/

24. Катренко А.В. Системний аналіз об"єктів та процесів комп’ютеризації: Навчальний посібник. - Львів : Новий Світ-2000", 2003. - 424

с. Конституція України. *URL*: https://zakon.rada.gov.ua/laws/show/25 4%D0 %BA/96-%D0%B2%D1%80#Text

25. Левіна-Костюк М.О., Мельничук О.І. Методи прийняття управлінських рішень в умовах недостатньої інформації //Економіка та суспільство. – 2022. – Вип.43. *URL: https://economyandsociety.in.ua/index.php /journal/artic le/download/172 6/1663*

26. Луцкий М.Г., Гавриленко А.В., Корченко А.А., Охрименко А.А. Модели эталонов лингвистических переменных для систем выявления атак //Захист інформації. – 2012. - №12. – С.5-12. *URL*: *https://jrnl.nau.edu.ua/ index.php /ZI/article/view/2188/13231*

27. Матвеев В.А., Бельфер Р.А., Глинская Е.В. Угрозы и методы защиты в сборных сенсорных узлах летающих сенсорных сетей // Вопросы кибербезопасности. - 2015. - №5 (13). Морська доктрина України на період до 2035 року, затверджена постановою Кабінету Міністрів України від 7 жовтня 2009 р. №1307. *URL*: *https://zakon.rada.gov.ua/laws/show/1307-2009-%D0%BF#Text*

28. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. *URL: http://www.dssz zi.gov.ua/dsszzi/doccatalog/document?id=106342*

29. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – *URL: http://dstszi.kmu.gov.ua/dstszi/control/uk/ publish/ article; jsessionid=afd6198c23cb1f96abafd7189bbdce03?showhidden=1& art_id=101870&cat_id=89734&ctime=1344501089407*

30. НД ТЗІ 2.5-008-02. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу *URL: http://info-stand.com/nb-ukraine/by-type/nd-tzi/22-ndtzi25-008-02.html*

31. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації *WEB*-сторінки від несанкціонованого доступу. *URL: http://www.dsszzi.gov.ua%2fdstszi%2fdoc catalo*

*g%2fdocument%3fid%3d41647&ei=guz5uk3xg8z3sga4r4cwcq&usg=afqjcnfye5 \kjfd qsympy-ekqedagtercmw&cad=rja*

32. План реалізації Стратегії кібербезпеки України. *URL*: *https://zak on.rada.gov.ua/laws/show/n0087525-21#Text*

33. Про затвердження переліку професійних захворювань. Постанова Кабінету Міністрів України від 08.11.2000 №1662 *URL: https://zakon.rada.gov. ua /laws/sho w/1662-2000-%D0%BF#Text*

34. Про затвердження Переліку установ і закладів, що мають право встановлювати остаточний діагноз хронічних професійних захворювань. Постанова Кабінету Міністрів України від 09.04.2022 № 603. *URL: https://zakon .rada .gov.ua/laws/sho w/z0428-22#Text*

35. Про затвердження Примірної інструкції з охорони праці під час експлуатації електронно-обчислювальних машин. Постанова Кабінету Міністрів України від 05.09.2013 № 443. *URL: https://ips.ligazakon.net/document/MDS00228*

36. СН 2152-80. Санітарно-гігієнічні норми допустимих рівнів іонізації повітря виробничих і громадських приміщень. *URL*: *https://dnaop.co m/html /2296/doc-ГН_2152-80*

37. Спам-атака на телефон. *URL*: *https://promov.one/spam-ataka-natele fon/*

38. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука безпечного розвитку країни. *URL*: *https://zakon.rada.gov.ua/la ws/show/ 447/20 21#n7*

39. «Україна є другою країною у світі за кількістю кібератак на неї». Заступник голови Держспецзв'язку Віктор Жора — про сучасних хакерів, єдиний роумінг і кіберпростір НАТО. *URL*: *https://dou.ua/lenta/interviews/derzhsp etszvia zku/*

40. Україна щодоби відбиває до 40 потужних кібератак – Держспецзв'язку. *URL*: *https://4www.ukrinform.ua/rubric-technology/3654348uk raina-so do bi-vidbivae-do-40-potuznih-kiberatak-derzspeczvazku.html*

41. Управління ключами в інформаційній системі. *URL*: *http://pidruchniki.com/13410927/informatika/upravlinnya_klyuchami_informatsiyniy_siste mi.*

42. Хакери здійснили потужну атаку на державні ресурси України. *URL:https://zmina.info/news/hakery-zdijsnyly-potuzhnu-ataku-na-derzhavniresurs yukrayiny/*

43. Юрченко Ю.Ю., Куцолабський В.П. Сенсорні мережі загального використання *URL*: *https://ir.lib.vntu.edu.ua/bitstream/hand le/123456789/2918 3/8940. pdf?sequence=3&isAllowed=y*