МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія (кафедра) комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

БЕЗПЕКА В КОМП`ЮТЕРНИХ МЕРЕЖАХ ВІД DDoS АТАК

Виконав: студент групи 1К-21
Спеціальності 123 Комп’ютерна інженерія
Олег САМОЙЛОВ
Керівник:
Павло РАТАЙЧУК

Черкаси 2025

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

Кафедра комп'ютерної інженерії та інформаційних технологій

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувач кафедри КІ та ІТ

_____ Владислав ХОТУНОВ
(підпис)
«_____»_____2024 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Самойлову Олегу Олеговичу

1. Тема кваліфікаційної роботи «Безпека в комп'ютерних мережах від DDoS атак»
Керівник роботи Ратайчук Павло Єгорович, викладач методист

затверджені наказом закладу вищої освіти від «07» жовтня 2024 року № 68у.
2. Строк подання студентом кваліфікаційної роботи 02.06.2025
3. Вихідні дані до кваліфікаційної роботи Аналіз методів виявлення та захисту від DDoS-атак, а також оцінка ефективності різних стратегій безпеки в комп'ютерних мережах, методи атаки, виявлення та захисту від DDoS у сучасних мережах.
4. Зміст кваліфікаційної роботи (перелік питань, які потрібно розробити) Визначити основні види DDoS-атак та їх вплив на мережеві інфраструктури, проаналізувати сучасні методи виявлення та класифікації DDoS-атак, дослідити засоби захисту та стратегії мінімізації ризиків: мережеві засоби захисту (брандмауери, IDS/IPS), використання CDN, Load Balancing, Rate Limiting, методи виявлення атак на основі штучного інтелекту (AI) та аналізу поведінки, виконати експериментальне дослідження в середовищі GNS3, Kali Linux або Cloudflare, оцінити ефективність різних засобів захисту та розробити рекомендації.
5. Дата видачі завдання 16.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання з підписами керівника і студента
1	Вступ	14.10.2024	
2	Розділ 1 (АНАЛІЗ DDOS-АТАК ЯК ЗАГРОЗИ БЕЗПЕЦІ КОМП'ЮТЕРНИХ МЕРЕЖ)	9.12.2024	
3	Розділ 2 (МЕТОДИ ВИЯВЛЕННЯ, ЗАХИСТУ ТА АНАЛІЗУ DDOS-АТАК)	10.03.2025	
4	Розділ 3 (ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ТА ОЦІНКА ЗАХИСТУ)	28.04.2025	
5	Висновки	12.05.2025	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2025	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	02.06.2025	
8	Подання кваліфікаційної роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	10.06.2025	

Студент _____ Олег САМОЙЛОВ
(підпис)

Керівник роботи _____ Павло РАТАЙЧУК
(підпис)

АНОТАЦІЯ

У сучасному цифровому середовищі проблема забезпечення безпеки комп’ютерних мереж від DDoS-атак (Distributed Denial of Service) є надзвичайно актуальною. Цей тип атаки спрямований на виведення з ладу інформаційних систем шляхом перевантаження їх численними запитами з великої кількості джерел, що унеможливлює нормальне функціонування веб-ресурсів, серверів або корпоративної інфраструктури. У межах дослідження розглядаються класифікація DDoS-атак, їх механізми реалізації, основні вектори впливу на мережеві сервіси, а також сучасні методи виявлення та захисту, включаючи фільтрацію трафіку, використання систем виявлення вторгнень (IDS), хмарні рішення та алгоритми машинного навчання. Аналізуються практичні підходи до побудови стійкої до DDoS-атак архітектури мережі та рекомендації щодо мінімізації ризиків. Особлива увага приділяється актуальним загрозам та динаміці розвитку атак у контексті зростання кількості IoT-пристроїв і складності ботнетів. Результати дослідження спрямовані на підвищення ефективності захисту критично важливих інформаційних систем та формування комплексного підходу до кібербезпеки в організаціях.

ABSTRACT

In today's digital landscape, ensuring the security of computer networks against Distributed Denial of Service (DDoS) attacks is a critical and urgent challenge. DDoS attacks aim to disrupt the availability of online services and network infrastructure by overwhelming them with massive volumes of traffic from multiple sources, rendering them inaccessible to legitimate users. This study explores the classification of DDoS attacks, their operating mechanisms, main vectors of impact on network services, and contemporary defense techniques. Among these are traffic filtering, intrusion detection systems (IDS), cloud-based mitigation solutions, and machine learning-based detection algorithms. The research also focuses on practical strategies for building DDoS-resilient network architectures and provides recommendations for reducing security risks. Special attention is given to emerging threats linked to the growing number of IoT devices and the increasing complexity of botnets. The findings aim to enhance the effectiveness of protecting critical information infrastructure and promote a comprehensive cybersecurity approach within modern organizations.

ЗМІСТ

ВСТУП

Актуальність обраної теми. У сучасному світі комп'ютерні мережі є основою інформаційної інфраструктури, що забезпечує функціонування критичних систем, таких як фінансові платформи, державні сервіси, хмарні обчислення та Інтернет речей (IoT). Зі зростанням кількості підключених пристроїв (понад 15 мільярдів IoT-пристроїв у 2024 році) і цифровізацією суспільства мережі стають дедалі вразливішими до кіберзагроз. Розподілені атаки типу «відмова в обслуговуванні» (DDoS) вирізняються своєю здатністю швидко виводити з ладу мережеві ресурси, спричиняючи значні економічні, репутаційні та безпекові втрати. За даними Cloudflare, у 2024 році кількість DDoS-атак зросла на 20% порівняно з 2023 роком, а піковий обсяг трафіку досяг 2 Тбіт/с. Доступність інструментів для здійснення атак (оренда ботнету від $10 за годину) і їхня складність, зокрема через використання штучного інтелекту, підкреслюють необхідність розробки ефективних методів виявлення, захисту та протидії. Таким чином, дослідження DDoS-атак і способів їх нейтралізації є актуальним для забезпечення кібербезпеки сучасних інформаційних систем.

Об’єкт дослідження. Комп'ютерні мережі та їхня безпека в контексті кіберзагроз.

Предмет дослідження. Методи та інструменти виявлення, захисту й аналізу DDoS-атак у комп'ютерних мережах.

Мета дослідження. Всебічний аналіз DDoS-атак як загрози безпеці комп'ютерних мереж, розробка та оцінка ефективності методів їх виявлення, захисту й протидії з метою підвищення стійкості інформаційних систем.

Завдання дослідження: Провести аналіз DDoS-атак, їхньої природи, класифікації, методів здійснення та впливу на комп'ютерні мережі. Дослідити сучасні методи виявлення DDoS-атак, включаючи системи IDS/IPS, поведінковий аналіз, штучний інтелект і машинне навчання. Оцінити захисні механізми, такі як фільтрація трафіку, використання CDN, проксі-серверів, Rate

Limiting, Load Balancing і Anycast. Виконати експериментальне моделювання DDoS-атак у тестовому середовищі для оцінки їхнього впливу та ефективності захисних рішень. Провести порівняльний аналіз різних методів захисту та розробити рекомендації для підвищення безпеки комп'ютерних мереж.

РОЗДІЛ 1

АНАЛІЗ DDoS-АТАК ЯК ЗАГРОЗИ БЕЗПЕЦІ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Загальна характеристика кіберзагроз у комп’ютерних мережах

Кіберзагрози в комп’ютерних мережах становлять одну з ключових проблем сучасної інформаційної безпеки, зумовлюючи значні ризики для конфіденційності, цілісності та доступності даних і систем. Зі зростанням цифровізації суспільства та інтеграції інформаційних технологій у критичну інфраструктуру, кіберзагрози набувають дедалі більшої складності, масштабності та впливу. Цей аналіз має на меті висвітлити природу кіберзагроз, їх основні типи, механізми реалізації, наслідки та сучасні тенденції розвитку в науковому контексті з опорою на авторитетні джерела.

Визначення та природа кіберзагроз. Кіберзагроза – це потенційна або фактична дія, спрямована на використання вразливостей інформаційних систем з метою порушення їх функціонування, викрадення даних або завдання іншої шкоди. Згідно з NIST SP 800-30, кіберзагрози характеризуються як події, що можуть спричинити негативний вплив на активи організації через експлуатацію вразливостей (NIST, 2012). Вони загрожують трьом основним аспектам інформаційної безпеки:

- Конфіденційність: захист даних від несанкціонованого доступу.
- Цілісність: забезпечення незмінності та достовірності інформації.
- Доступність: гарантія безперебійного доступу до систем і даних.

Кіберзагрози можуть походити від різних суб’єктів: кіберзлочинців, хактивістів, державних акторів або внутрішніх порушників, що ускладнює їх прогнозування та нейтралізацію.

Типологія кіберзагроз. Кіберзагрози класифікуються за методами реалізації та цілями. Основні категорії включають:

Шкідливе програмне забезпечення (Malware): Включає віруси, черв'яки, трояни, програми-вимагачі (ransomware) та шпигунське ПЗ. Наприклад, атака WannaCry у 2017 році використала вразливість EternalBlue для шифрування даних на тисячах пристроїв (FireEye, 2017).

Фішинг та соціальна інженерія: Маніпулятивні методи для отримання конфіденційних даних, такі як підроблені електронні листи чи вебсайти. Spear-phishing є прикладом цільових атак на високопоставлених осіб.

Атаки відмови в обслуговуванні (DDoS): Перевантаження мережевих ресурсів для порушення їх доступності, як у випадку атаки на Dyn у 2016 році через ботнет Mirai (Kaspersky Lab, 2016).

Експлуатація вразливостей: Використання недоліків у програмному забезпеченні, наприклад, вразливість Log4j у 2021 році (CISA, 2021).

Цільові атаки (APT): Довготривалі, складні атаки, часто спонсоровані державами, як Stuxnet, спрямований на іранську ядерну програму (Symantec, 2010).

Механізми реалізації кіберзагроз:

Кіберзагрози реалізуються через експлуатацію технічних, людських і організаційних вразливостей. Основні механізми включають:

- Технічні вразливості: Використання незакритих недоліків у програмному чи апаратному забезпеченні, таких як застарілі версії ПЗ.
- Соціальна інженерія: Маніпуляція довірою користувачів для отримання доступу до систем.
- Мережеві атаки: Перехоплення даних (Man-in-the-Middle), підміна DNS або атаки на протоколи.
- Автоматизація та штучний інтелект: Використання AI для створення адаптивних атак, наприклад, deepfake у фішингових кампаніях (ENISA, 2023).

Кіберзагрози у комп'ютерних мережах є складним і динамічним викликом, що вимагає постійного вдосконалення методів захисту. Їх еволюція, підкріплена технологічними інноваціями, такими як AI та IoT, посилює

необхідність інтеграції технічних, організаційних і міжнародних заходів для забезпечення кібербезпеки. Подальші дослідження мають зосередитися на прогнозуванні нових векторів атак та розробці адаптивних стратегій захисту.

1.2 Визначення та класифікація DDoS-атак

DDoS-атака – це скоординована спроба перевантажити ресурси цільової системи, мережі або сервера шляхом надсилання великої кількості запитів із множини джерел, що унеможливлює нормальне функціонування системи. Згідно з NIST SP 800-61, DDoS-атаки мають на меті порушення доступності інформаційних ресурсів, що є одним із трьох ключових аспектів інформаційної безпеки (конфіденційність, цілісність, доступність) (NIST, 2012). На відміну від DoS-атак (Denial of Service), які зазвичай походять із одного джерела, DDoS-атаки використовують розподілену мережу пристроїв, часто об’єднаних у ботнети, що значно ускладнює їх виявлення та нейтралізацію.

Основними цілями DDoS-атак є:

- Порушення роботи вебсайтів, серверів або мережевої інфраструктури.
- Завдання економічних збитків через припинення бізнес-процесів.
- Відволікання уваги для здійснення інших кібератак (наприклад, крадіжки даних).

Класифікація DDoS-атак. DDoS-атаки класифікуються за кількома критеріями: рівнем мережевої моделі OSI, на який спрямована атака, типом використовуваних ресурсів, складністю та мотивацією. Нижче наведено детальну класифікацію.

1. За рівнем моделі OSI

DDoS-атаки поділяються залежно від рівня мережевої моделі OSI, на якому вони здійснюються (Bhadauria & Sanyal, 2012):

Атаки на мережевий/транспортний рівень (рівні 3–4)**:**

Об’ємні атаки (Volumetric Attacks)**:** Генерують величезний обсяг трафіку, щоб перевантажити пропускну здатність мережі.

Наприклад: UDP Flood**:** Надсилання великої кількості UDP-пакетів на випадкові порти цільового сервера. ICMP Flood (Ping Flood)**:** Використання запитів ICMP для перевантаження сервера.

Приклад**:** Атака на Dyn у 2016 році, яка використовувала ботнет Mirai для генерації трафіку через IoT-пристрої, порушила роботу таких сервісів, як Twitter і Netflix (Kaspersky Lab, 2016).

Атаки на прикладний рівень (рівень 7)**:**

Спрямовані на вичерпання ресурсів сервера шляхом імітації легітимних запитів користувачів.

Наприклад: HTTP Flood**:** Надсилання великої кількості HTTP-запитів (GET або POST) до вебсайту. Slowloris**:** Утримання відкритих з’єднань із сервером шляхом повільного надсилання HTTP-запитів.

Особливість: Ці атаки складніше виявити, оскільки вони імітують поведінку реальних користувачів.

Протокольні атаки (рівні 3–4)**:**

Використовують вразливості мережевих протоколів для вичерпання ресурсів.

Наприклад: SYN Flood**:** Надсилання численних SYN-запитів для переповнення таблиці з’єднань сервера. Smurf Attack**:** Використання підроблених ICMP-запитів для перенаправлення відповідей на цільовий сервер.

2. За типом використовуваних ресурсів

Ботнет-атаки**:** Використовують мережі заражених пристроїв (ботнети), таких як комп’ютери, IoT-пристрої чи сервери. Наприклад, ботнет Mirai заразив сотні тисяч IoT-пристроїв для здійснення масових атак (Antonakakis et al., 2017).

Атаки з підсиленням (Amplification Attacks)**:** Використовують сервери з відкритими протоколами (наприклад, DNS, NTP) для підсилення трафіку. Наприклад, DNS Amplification може збільшувати обсяг трафіку в десятки разів.

Прямі атаки**:** Здійснюються з використанням власних ресурсів зловмисника, але рідше через їхню високу вартість.

3. За складністю

Прості атаки**:** Використовують базові інструменти, доступні в темній мережі, такі як LOIC (Low Orbit Ion Cannon).

Складні атаки**:** Поєднують кілька векторів (наприклад, об'ємні та прикладні атаки) для максимального ефекту. Наприклад, атака на GitHub у 2018 році досягла піку в 1,35 Тбіт/с (Cloudflare, 2018).

4. За мотивацією

Фінансові**:** Вимагання викупу (наприклад, DDoS як частина шантажу).

Політичні/хактивізм: Вплив на урядові чи корпоративні ресурси (наприклад, дії Anonymous).

Конкурентні: Порушення роботи конкурентів.

Тестування вразливостей: Використання DDoS як відволікання для інших атак.

Механізми реалізації DDoS-атакою. DDoS-атаки реалізуються через скоординоване використання розподілених ресурсів, що включає:

- Формування ботнетів: Зловмисники заражають пристрої шкідливим ПЗ, створюючи мережі для координації атак.
- Експлуатація вразливостей: Використання відкритих протоколів (DNS, NTP) або слабких конфігурацій серверів.
- Автоматизація**:** Використання скриптів і платформ типу DDoS-as-a-Service, доступних у темній мережі.
- Підсилення трафіку**:** Використання серверів із високим коефіцієнтом підсилення для генерації масового трафіку.

Наслідки DDoS-атак. DDoS-атаки мають значний вплив на організації та суспільство:

- Економічні збитки**:** За даними Cybersecurity Ventures, середня вартість DDoS-атаки для бізнесу становить $2 млн (Cybersecurity Ventures, 2024).
- Репутаційні втрати: Порушення доступності сервісів призводить до втрати довіри клієнтів.
- Технічні наслідки**:** Вичерпання ресурсів серверів, мереж або хмарних сервісів.
- Національна безпека**:** Атаки на критичну інфраструктуру (енергетика, транспорт) можуть мати катастрофічні наслідки.

1.3 Основні методи здійснення DDoS-атак

Розподілені атаки типу «відмова в обслуговуванні» (DDoS, Distributed Denial of Service) є однією з найпоширеніших форм кіберзагроз, спрямованих на порушення доступності інформаційних систем. Вони характеризуються скоординованим перевантаженням цільових ресурсів (серверів, мереж, вебсайтів) через масові запити з множини джерел, що ускладнює їх виявлення та нейтралізацію. Цей аналіз розкриває основні методи здійснення DDoS-атак, їхні технічні особливості, механізми реалізації та сучасні тенденції, спираючись на наукові джерела. Для структуризації інформації додано порівняльну таблицю методів.

Методи DDoS-атак розрізняються за рівнем моделі OSI, на який вони спрямовані, типом використовуваних ресурсів і технікою реалізації. Нижче детально розглянуто основні методи, структуризовані за рівнями моделі OSI.

Об’ємні атаки (Volumetric Attacks). Ці атаки спрямовані на перевантаження пропускної здатності мережі шляхом генерації великого обсягу трафіку (рівні 3–4 моделі OSI). Основна мета – вичерпати мережеві ресурси, такі як пропускна здатність каналу зв’язку.

UDP Flood**:** Надсилання великої кількості UDP-пакетів на випадкові порти цільового сервера. Сервер змушений перевіряти кожен пакет, що

призводить до вичерпання ресурсів. Наприклад, атака може використовувати відправлення пакетів на порт 53 (DNS).

ICMP Flood (Ping Flood)**:** Використання запитів ICMP (наприклад, ping) для перевантаження сервера відповідями. Часто застосовується через простоту реалізації.

Приклад**:** Атака на Dyn у 2016 році, здійснена ботнетом Mirai, генерувала трафік до 1,2 Тбіт/с, використовуючи IoT-пристрої (Antonakakis et al., 2017).

Протокольні атаки. Ці атаки експлуатують вразливості мережевих протоколів (рівні 3–4), щоб вичерпати ресурси обробки сервера або мережевого обладнання.

SYN Flood**:** Зловмисник надсилає численні SYN-запити для ініціації TCP-з'єднань, не завершуючи їх. Це переповнює таблицю з'єднань сервера, що призводить до відмови в обслуговуванні легітимним користувачам.

Smurf Attack**:** Використання підроблених ICMP-запитів, спрямованих на широкомовні адреси, що викликає масові відповіді на цільовий сервер.

Приклад**:** Атаки типу SYN Flood часто використовуються через їхню ефективність у перевантаженні серверів із обмеженими обчислювальними ресурсами (Bhadauria & Sanyal, 2012).

Атаки на прикладний рівень. Ці атаки спрямовані на вичерпання ресурсів сервера через імітацію легітимних запитів на рівні 7 моделі OSI. Вони складніші для виявлення, оскільки виглядають як звичайна активність користувачів.

HTTP Flood**:** Надсилання численних HTTP-запитів (GET або POST) до вебсайту, що перевантажує вебсервер. Наприклад, атака може імітувати запити до сторінки авторизації.

Slowloris**:** Утримання відкритих HTTP-з'єднань шляхом повільного надсилання часткових запитів, що вичерпує пул з'єднань сервера.

Приклад**:** Атака на GitHub у 2018 році досягла піку в 1,35 Тбіт/с, використовуючи комбінацію HTTP Flood та інших методів (Cloudflare, 2018).

Атаки з підсиленням (Amplification Attacks). Ці атаки використовують сервери з відкритими протоколами (наприклад, DNS, NTP) для підсилення трафіку, спрямованого на ціль.

DNS Amplification**:** Надсилання запитів до відкритих DNS-серверів із підробленою IP-адресою жертви, що викликає масові відповіді. Коефіцієнт підсилення може досягати 50:1.

NTP Amplification: Використання серверів Network Time Protocol для генерації великих відповідей на малі запити.

Приклад**:** Атака на Spamhaus у 2013 році використовувала DNS Amplification, генеруючи до 300 Гбіт/с трафіку (Kaspersky Lab, 2013).

Гібридні атаки. Сучасні DDoS-атаки часто поєднують кілька методів для максимізації ефекту. Наприклад, одночасне використання об'ємних атак (UDP Flood) і атак на прикладний рівень (HTTP Flood) ускладнює захист, оскільки вимагає фільтрації на різних рівнях мережі.

Таблиця 1.1 - Порівняльна таблиця методів DDoS-атак

Метод	Рівень OSI	Тип атаки	Механізм	Приклад	Складність виявлення
UDP Flood	3–4	Об'ємна	Надсилання UDP-пакетів на випадкові порти	Атака на Dyn (2016)	Низька
ICMP Flood	3–4	Об'ємна	Генерація ICMP-запитів для перевантаження сервера	Атаки на ігрові сервери	Низька
SYN Flood	3–4	Протокольна	Переповнення таблиці TCP-з'єднань через незавершені SYN-запити	Атаки на фінансові установи	Середня
HTTP Flood	7	Прикладна	Надсилання легітимних HTTP-запитів для вичерпання ресурсів сервера	Атака на GitHub (2018)	Висока
Slowloris	7	Прикладна	Утримання відкритих HTTP-з'єднань через повільні запити	Атаки на вебсервери Apache	Висока
DNS Amplification	3–4	З підсиленням	Використання відкритих DNS-серверів для підсилення трафіку	Атака на Spamhaus (2013)	Середня

Механізми реалізації DDoS-атак

1. Формування ботнетів**:** Зловмисники заражають пристрої (ПК, IoT-пристрої, сервери) шкідливим ПЗ, створюючи мережі для координації атак. Наприклад, ботнет Mirai заразив сотні тисяч IoT-пристроїв (Antonakakis et al., 2017).

2. Експлуатація вразливостей**:** Використання відкритих протоколів (DNS, NTP) або слабких конфігурацій серверів.
3. Автоматизація**:** Використання інструментів типу DDoS-as-a-Service, доступних у темній мережі, що знижує бар'єри для зловмисників.
4. Підсилення трафіку**:** Використання серверів із високим коефіцієнтом підсилення для генерації масового трафіку.

1.4 Вплив DDoS-атак на комп'ютерні мережі та сервіси

Розподілені атаки типу «відмова в обслуговуванні» (DDoS, Distributed Denial of Service) становлять серйозну загрозу для комп'ютерних мереж і сервісів, порушуючи їхню доступність, що є ключовим аспектом інформаційної безпеки. Ці атаки, реалізовані через масові запити з розподілених джерел, таких як ботнети, мають багатогранний вплив, охоплюючи економічні, технічні, соціальні та безпекові наслідки. У цьому аналізі розглянуто вплив DDoS-атак на комп'ютерні мережі та сервіси, їхні механізми та наслідки, з опорою на наукові джерела.

DDoS-атаки чинять комплексний вплив на комп'ютерні мережі та сервіси, що проявляється в кількох вимірах.

Економічний вплив. DDoS-атаки спричиняють значні фінансові втрати. Прямі збитки виникають через зупинку бізнес-процесів, зокрема для компаній, що залежать від онлайн-сервісів, таких як електронна комерція чи хмарні платформи. За оцінками Cybersecurity Ventures, середня вартість однієї DDoS-атаки становить приблизно $2 млн, враховуючи втрати доходів і витрати на відновлення (Cybersecurity Ventures, 2024). Непрямі витрати включають інвестиції в захисні технології, такі як системи фільтрації трафіку чи CDN, а також залучення експертів із кібербезпеки. Наприклад, атака на Amazon Web Services у 2020 році спричинила перебої в роботі клієнтських сервісів, що призвело до значних збитків (Cloudflare, 2020).

Технічний вплив. DDoS-атаки створюють надмірне навантаження на технічну інфраструктуру. Об’ємні атаки, такі як UDP Flood або DNS Amplification, вичерпують пропускну здатність мережі, блокуючи легітимний трафік. Протокольні атаки, наприклад SYN Flood, перевантажують таблиці з’єднань серверів, а атаки на прикладний рівень, такі як HTTP Flood, імітують легітимні запити, ускладнюючи їх виявлення. Атака на Dyn у 2016 році, здійснена ботнетом Mirai, досягла обсягу трафіку 1,2 Тбіт/с, що призвело до відключення великих платформ, таких як Twitter і Netflix (Antonakakis et al., 2017). У рідкісних випадках надмірне навантаження може спричинити фізичне пошкодження обладнання.

Соціальний вплив. Перебої в роботі сервісів підривають довіру користувачів і завдають репутаційних збитків. Наприклад, атака на Sony PlayStation Network у 2011 році призвела до тривалого простою, що негативно вплинуло на лояльність клієнтів (Kaspersky Lab, 2011). У разі атак на сервіси критичних сфер, таких як охорона здоров’я, наслідки можуть стосуватися суспільного благополуччя. Наприклад, атака WannaCry у 2017 році частково порушила роботу NHS у Великобританії, обмеживши доступ до медичних послуг.

Безпековий вплив. DDoS-атаки загрожують національній безпеці, особливо коли спрямовані на критичну інфраструктуру. Атака на енергосистему України в 2015 році, що включала елементи DDoS, спричинила відключення електроенергії для тисяч споживачів (ENISA, 2016). У контексті кібервійн DDoS-атаки використовуються для дестабілізації державних інститутів, як це було під час атак на урядові сайти Естонії у 2007 році (Symantec, 2007).

Юридичний вплив. Порушення доступності сервісів може призвести до невідповідності регуляторним стандартам, таким як GDPR, що тягне за собою штрафи. Організації також можуть стикатися з юридичними позовами від клієнтів або партнерів через втрати, спричинені перебоями.

Сучасні тенденції. Сучасні DDoS-атаки стають дедалі складнішими через технологічний прогрес. Зростання кількості IoT-пристроїв (понад 75 млрд до 2025 року за даними Statista) сприяє формуванню потужних ботнетів (Statista, 2025). Штучний інтелект використовується для оптимізації атак, зокрема для адаптивного вибору векторів (ENISA, 2023). Модель DDoS-as-a-Service знижує бар'єри для зловмисників, роблячи атаки доступними навіть для некваліфікованих осіб. Гібридні атаки, що поєднують DDoS із іншими загрозами, такими як ransomware, підсилюють їхній вплив, як це було під час атаки на Colonial Pipeline у 2021 році (FireEye, 2021).

Заходи пом'якшення впливу. Протидія DDoS-атакам вимагає комплексного підходу. Технічні заходи включають використання CDN, систем виявлення вторгнень (IDS/IPS) і фільтрацію трафіку. Організаційні заходи передбачають розробку планів реагування на інциденти та навчання персоналу. Моніторинг за допомогою SIEM-систем забезпечує раннє виявлення аномалій. Міжнародна співпраця через організації, такі як ENISA, сприяє обміну інформацією про загрози.

Таблиця 1.2 - Порівняльна таблиця впливу DDoS-атак

Аспект впливу	**Опис**	**Приклад**	**Наслідки**
Економічний	Втрата доходів, витрати на відновлення	Amazon AWS (2020)	Збитки до $2 млн за атаку
Технічний	Перевантаження серверів і мереж	Dyn (2016)	Перебої в роботі платформ
Соціальний	Втрата довіри, репутаційні збитки	Sony PSN (2011)	Зменшення клієнтської бази
Безпековий	Порушення критичної інфраструктури	Україна (2015)	Загроза національній безпеці
Юридичний	Порушення стандартів, штрафи	Порушення GDPR	Штрафи, юридичні позови

1.5 Механізми ідентифікації атак у реальному часі

Розподілені атаки типу «відмова в обслуговуванні» (DDoS, Distributed Denial of Service) становлять значну загрозу для комп'ютерних мереж і сервісів, порушуючи їхню доступність через перевантаження ресурсів масовими запитами з розподілених джерел. Своєчасна ідентифікація таких атак у реальному часі є критично важливою для мінімізації їхнього впливу. Цей аналіз розглядає основні механізми виявлення DDoS-атак у реальному часі, їхні технічні принципи, переваги, обмеження та сучасні тенденції, спираючись на наукові джерела. Для структуризації інформації додано порівняльну таблицю.

Механізми ідентифікації DDoS-атак. Ідентифікація DDoS-атак у реальному часі базується на аналізі мережевого трафіку, поведінки системи та інтеграції інтелектуальних технологій. Нижче розглянуто основні підходи.

Аналіз мережевого трафіку. Цей підхід передбачає моніторинг мережевого трафіку для виявлення аномалій, таких як різке зростання обсягу запитів або незвичайні шаблони. Порогові методи порівнюють параметри трафіку (наприклад, кількість пакетів за секунду) із заданими межами, тоді як статистичні моделі аналізують відхилення від історичних даних. Наприклад, зростання UDP-пакетів може свідчити про атаку типу UDP Flood (Bhadauria & Sanyal, 2012). Цей метод ефективний для об'ємних атак, але схильний до хибнопозитивних спрацьовувань і менш ефективний для атак на прикладний рівень.

Системи виявлення та запобігання вторгненням (IDS/IPS). IDS/IPS аналізують трафік і поведінку системи для ідентифікації зловмисної активності. Сигнатурний аналіз порівнює трафік із базою відомих шаблонів атак, таких як SYN Flood, тоді як аномальний аналіз виявляє відхилення від нормальної поведінки. Системи, такі як Snort, використовують оновлювані бази сигнатур для швидкого реагування (Snort, 2023). Проте їхня ефективність знижується для нових або складних атак, таких як Slowloris.

Аналіз на основі машинного навчання. Машинне навчання (ML) і штучний інтелект (AI) застосовуються для виявлення складних шаблонів атак. Класифікаційні алгоритми, такі як Random Forest, або нейронні мережі навчаються на історичних даних для розрізнення легітимного та зловмисного трафіку. Наприклад, рекурентні нейронні мережі можуть ідентифікувати послідовності, характерні для атак на прикладний рівень (Somani et al., 2017). Цей підхід адаптивний до нових загроз, але потребує значних обчислювальних ресурсів і даних для навчання.

Системи управління інформацією та подіями безпеки (SIEM). SIEM-системи, такі як Splunk або IBM QRadar, інтегрують дані з різних джерел (журнали, метрики продуктивності) для кореляційного аналізу. Вони здатні виявляти гібридні атаки шляхом поєднання інформації про трафік і поведінку системи. Однак впровадження таких систем є дорогим і потребує кваліфікованого персоналу.

Хмарні технології. Хмарні рішення, такі як Cloudflare або Akamai, використовують розподілені мережі серверів для моніторингу та фільтрації трафіку. Технологія Anycast дозволяє аналізувати трафік на різних вузлах, виявляючи аномалії в реальному часі (Cloudflare, 2023). Цей підхід масштабований, але залежить від зовнішніх постачальників.

Таблиця 1.3 - Порівняльна таблиця механізмів ідентифікації DDoS-атак

Механізм	**Принцип роботи**	**Переваги**	**Обмеження**	**Приклад застосування**
Аналіз трафіку	Моніторинг обсягу та шаблонів	Простота, швидкість	Хибнопозитивні спрацьовування	NetFlow, Wireshark
IDS/IPS	Сигнатурний/аномальний аналіз	Точність для відомих атак	Низька ефективність для нових атак	Snort, Suricata
Машинне навчання	Класифікація, аналіз поведінки	Адаптивність, висока точність	Висока обчислювальна складність	Random Forest
SIEM	Кореляція даних із різних джерел	Комплексний аналіз	Висока вартість, складність	Splunk, QRadar
Хмарні технології	Розподілений моніторинг і фільтрація	Масштабованість, швидкість	Залежність від постачальника	Cloudflare, Akamai

Складність DDoS-атак зростає через технологічний прогрес. Збільшення кількості IoT-пристроїв (понад 75 млрд до 2025 року за даними Statista) сприяє створенню потужних ботнетів, що ускладнює їх виявлення (Statista, 2025). Штучний інтелект використовується як для атак (наприклад, адаптивні HTTP Flood), так і для захисту, підвищуючи точність ідентифікації (ENISA, 2023). Гібридні атаки, що поєднують кілька векторів, вимагають інтеграції різних методів аналізу. Автоматизація реагування, інтегрована з IDS/IPS або хмарними рішеннями, скорочує час реакції на атаки.

РОЗДІЛ 2

МЕТОДИ ВИЯВЛЕННЯ, ЗАХИСТУ ТА АНАЛІЗУ DDOS-АТАК

2.1 Використання систем IDS/IPS для виявлення аномалій: науковий аналіз

Системи виявлення вторгнень (Intrusion Detection Systems, IDS) та системи запобігання вторгненням (Intrusion Prevention Systems, IPS) є фундаментальними інструментами кібербезпеки, призначеними для захисту інформаційних систем шляхом моніторингу та реагування на аномальні активності, які можуть свідчити про кібератаки, несанкціонований доступ або порушення безпеки. IDS виконують пасивний аналіз мережевого трафіку, системних логів або поведінки користувачів, генеруючи попередження для адміністраторів, тоді як IPS додатково активно блокують виявлені загрози в реальному часі. Виявлення аномалій, як ключовий механізм цих систем, базується на ідентифікації відхилень від нормальної поведінки, що дозволяє виявляти як відомі, так і невідомі загрози, включаючи атаки типу "zero-day". У цьому аналізі розглядаються принципи функціонування IDS/IPS, методи виявлення аномалій, їх порівняльні характеристики, переваги, обмеження та практичне застосування в контексті забезпечення кібербезпеки.

Виявлення аномалій у IDS/IPS ґрунтується на створенні базового профілю нормальної поведінки системи чи мережі, який формується шляхом аналізу історичних даних. Поточна активність порівнюється з цим профілем для ідентифікації відхилень, що можуть вказувати на потенційні загрози. Процес охоплює збір даних (мережевий трафік, логи, поведінка користувачів), побудову моделі нормальної поведінки за допомогою статистичних методів або алгоритмів машинного навчання, аналіз відхилень і реагування шляхом генерації попереджень (IDS) або автоматичного блокування (IPS). Основними методами виявлення аномалій є статистичний аналіз, який використовує метрики, такі як обсяг трафіку чи частота подій, для виявлення відхилень, наприклад, різкого зростання трафіку, що може свідчити про DDoS-атаку;

методи машинного навчання, які застосовують алгоритми кластеризації (k-means), класифікації (SVM, Random Forest) або нейронні мережі (автоенкодери) для ідентифікації складних патернів; поведінковий аналіз, що фокусується на профілях поведінки користувачів чи пристроїв, наприклад, виявленні незвичайного часу входу чи доступу до ресурсів; а також гібридний підхід, який поєднує сигнатурний та аномальний методи для підвищення точності.

IDS та IPS мають спільну мету захисту інформаційних систем, але їх функціональні характеристики суттєво відрізняються. IDS працюють у пасивному режимі, аналізуючи дані поза основним потоком трафіку, що знижує ризик впливу на продуктивність мережі, але потребує ручного реагування на попередження. IPS, навпаки, функціонують у потоці трафіку, що дозволяє активно блокувати загрози, але може викликати затримки або помилкове блокування нормальної активності. Наприклад, такі системи, як Snort, Suricata чи Zeek, є типовими IDS, тоді як Cisco Secure IPS, FortiGate або Palo Alto Networks IPS забезпечують активний захист. Порівняльна характеристика цих систем показує, що IDS мають перевагу в низькому ризику помилкових блокувань, тоді як IPS вирізняються швидким реагуванням і можливістю запобігання атакам у реальному часі. Однак IPS можуть створювати затримки в мережі, а IDS потребують додаткових ресурсів для обробки попереджень.

Використання IDS/IPS для виявлення аномалій має низку переваг. По-перше, аномальний підхід дозволяє ідентифікувати невідомі загрози, для яких відсутні сигнатури, що є критично важливим у контексті "zero-day" атак. По-друге, системи є адаптивними, оскільки оновлення профілів або моделей машинного навчання дає змогу реагувати на нові типи загроз. Для IPS характерна автоматизація реагування, що зменшує час реагування та залежність від людського фактора. Проте ці системи мають обмеження. Хибнопозитивні спрацьовування виникають, коли нормальна, але рідкісна поведінка класифікується як аномалія, що може перевантажувати адміністраторів попередженнями. Аналіз великих обсягів даних у реальному часі, особливо при використанні машинного навчання, вимагає значних обчислювальних ресурсів.

Крім того, створення точного базового профілю нормальної поведінки є складним завданням, яке потребує ретельного аналізу та тривалого збору даних.

Практичне застосування IDS/IPS охоплює корпоративні мережі, хмарні середовища та критичні інфраструктури. Наприклад, Snort, відкрита IDS, підтримує аналіз аномалій через модулі для статистичної обробки, тоді як Suricata інтегрується з інструментами машинного навчання для підвищення ефективності. Комерційні рішення, такі як Palo Alto Networks IPS, використовують хмарні технології для аналізу та блокування загроз у реальному часі. Порівняння методів виявлення аномалій показує, що статистичний аналіз є простим, але схильним до хибнопозитивних спрацьовувань, машинне навчання забезпечує високу точність, але потребує значних ресурсів, поведінковий аналіз ефективний для внутрішніх загроз, а гібридний підхід пропонує комплексний захист, але є складним у реалізації.

У підсумку, системи IDS та IPS є невід’ємними компонентами кібербезпеки, забезпечуючи ефективне виявлення та нейтралізацію аномалій. IDS оптимальні для моніторингу та аналізу, тоді як IPS забезпечують активне реагування, що є критично важливим для швидкого запобігання загрозам. Ефективність цих систем залежить від якості базового профілю, точності налаштувань і здатності мінімізувати хибнопозитивні спрацьовування. Інтеграція статистичних методів, машинного навчання та поведінкового аналізу дозволяє адаптувати IDS/IPS до динамічних кіберзагроз, забезпечуючи комплексний захист інформаційних систем. Для уточнення деталей чи аналізу конкретних систем рекомендується надати додаткові вимоги.

Таблиця 2.1 - Порівняльна таблиці між IDS та IPS

Характеристика	IDS	IPS
Функціональність	Моніторинг мережевого трафіку та генерація попереджень про аномалії	Моніторинг і активне блокування аномального трафіку в реальному часі
Режим роботи	Пасивний (out-of-band), аналіз поза основним потоком трафіку	Активний (in-line), розташування в потоці трафіку
Методи виявлення аномалій	Статистичний аналіз, машинне навчання, поведінковий аналіз	Статистичний аналіз, машинне навчання, поведінковий аналіз
Переваги	- Низький ризик помилкового блокування - Не впливає на продуктивність мережі	- Швидке реагування на загрози - Запобігання атакам у реальному часі
Недоліки	- Не блокує загрози - Потребує ручного реагування адміністратора	- Можливі затримки мережі - Ризик помилкового блокування
Приклади систем	Snort, Suricata, Zeek (Bro)	Cisco Secure IPS, FortiGate, Palo Alto Networks IPS
Типові сценарії використання	Моніторинг корпоративних мереж, аналіз логів, виявлення внутрішніх загроз	Захист критичних інфраструктур, блокування DDoS-атак, хмарні середовища

2.2 Методи поведінкового аналізу для детектування атак

Методи поведінкового аналізу для детектування атак є важливою складовою сучасних систем кібербезпеки, оскільки вони дозволяють виявляти загрози на основі відхилень у поведінці користувачів, пристроїв або мережевих процесів, а не лише за сигнатурами відомих атак. Цей підхід ґрунтується на припущенні, що шкідлива активність, навіть якщо вона не відповідає відомим шаблонам, проявляється через аномалії в поведінкових патернах. Поведінковий аналіз використовує комбінацію статистичних, машинно-навчальних та евристичних методів для ідентифікації таких відхилень, що робить його ефективним інструментом для виявлення як відомих, так і нових, раніше не зафіксованих атак, включаючи атаки нульового дня.

Основна ідея поведінкового аналізу полягає у створенні базової моделі нормальної поведінки системи, користувача або мережі. Ця модель формується на основі історичних даних, які включають такі параметри, як частота запитів,

типи операцій, час активності, обсяг переданих даних, географічне розташування тощо. Наприклад, у корпоративних мережах нормальна поведінка користувача може включати регулярний доступ до певних серверів у робочий час, тоді як спроба завантаження великих обсягів даних у неробочий час або з незвичного місця може бути позначена як підозріла. Для створення таких моделей часто застосовуються методи машинного навчання, зокрема кластеризація, класифікація та аналіз часових рядів. Алгоритми, такі як k-середніх, ізоляційний ліс або рекурентні нейронні мережі, дозволяють ефективно обробляти великі обсяги даних і виявляти аномалії в реальному часі.

Одним із ключових напрямів поведінкового аналізу є аналіз поведінки користувачів і об’єктів (User and Entity Behavior Analytics, UEBA). UEBA фокусується на моніторингу дій користувачів і пристроїв у мережі, враховуючи їхні ролі, привілеї та контекст. Наприклад, система UEBA може виявити, що обліковий запис, який зазвичай використовується для адміністративних завдань, раптово виконує незвичні дії, такі як доступ до бази даних, до якої він раніше не звертався. Це може свідчити про компрометацію облікового запису або інсайдерську загрозу. Для підвищення точності UEBA часто інтегрується з системами SIEM (Security Information and Event Management), що дозволяє корелювати поведінкові дані з іншими подіями безпеки.

Інший важливий аспект поведінкового аналізу — це детектування аномалій у мережевому трафіку. Наприклад, різке зростання обсягу вихідного трафіку може вказувати на витік даних, а незвичайні патерни зв’язків між вузлами мережі можуть свідчити про активність ботнету. Для аналізу мережевого трафіку часто застосовуються методи глибокого навчання, такі як автокодери, які здатні виявляти приховані структури в даних і позначати відхилення. Крім того, аналіз поведінки програмного забезпечення, наприклад, відстеження системних викликів або використання ресурсів, дозволяє виявляти шкідливі програми, які змінюють нормальну поведінку додатків.

Перевагою методів поведінкового аналізу є їхня здатність адаптуватися до нових загроз без необхідності оновлення сигнатур. Однак ці методи мають і

певні обмеження. По-перше, створення точної моделі нормальної поведінки вимагає значної кількості даних і може бути ускладненим у динамічних середовищах, де поведінка користувачів або систем постійно змінюється. По-друге, високий рівень помилкових спрацьовувань може виникати через недостатню специфіку моделей або через природні зміни в поведінці, які не пов’язані з атаками. Для зменшення цих недоліків застосовуються гібридні підходи, що поєднують поведінковий аналіз із сигнатурними методами та контекстним аналізом.

У сучасних умовах, коли кібератаки стають дедалі складнішими та використовують техніки маскування, методи поведінкового аналізу набувають особливого значення. Вони дозволяють не лише реагувати на відомі загрози, але й прогнозувати потенційні атаки, аналізуючи відхилення в реальному часі. Подальший розвиток цих методів пов’язаний із удосконаленням алгоритмів штучного інтелекту, зокрема глибокого навчання, а також із інтеграцією з іншими технологіями кібербезпеки, такими як аналіз великих даних і автоматизоване реагування на інциденти. Таким чином, поведінковий аналіз залишається ключовим інструментом у забезпеченні проактивного захисту інформаційних систем.

2.3 Роль штучного інтелекту та машинного навчання у розпізнаванні атак

Штучний інтелект (ШІ) та машинне навчання (МН) відіграють ключову роль у сучасних системах кібербезпеки, забезпечуючи здатність виявляти складні, динамічні та раніше невідомі кібератаки в умовах зростання обсягу даних і ускладнення загроз. Традиційні методи захисту, такі як сигнатурний аналіз, стають менш ефективними через швидке зростання атак нульового дня, поліморфних шкідливих програм і технік маскування, які унеможливлюють своєчасне виявлення на основі заздалегідь визначених шаблонів. ШІ та МН пропонують проактивний підхід, який ґрунтується на аналізі великих обсягів

даних, виявленні аномалій і прогнозуванні потенційних загроз у реальному часі, що робить їх незамінними інструментами в боротьбі з кіберзагрозами.

Таблиця 2.2 – Методи розпізнавання атак

Метод ШІ/МН	**Опис**	**Приклади використання**	**Переваги**	**Обмеження**
Кластеризація	Використання алгоритмів (наприклад, k-середніх) для групування даних за схожими характеристиками та виявлення аномалій, які не відповідають кластерам нормальної поведінки.	Виявлення незвичайних дій користувачів у системах UEBA, наприклад, нетиповий доступ до ресурсів.	Не потребує попереднього маркування даних; ефективний для виявлення нових загроз.	Високий ризик помилкових спрацьовувань через природні відхилення; залежить від якості даних.
Класифікація	Застосування алгоритмів (наприклад, логістична регресія, підтримуючі векторні машини) для категоризації подій як нормальних або шкідливих на основі навчальних даних.	Класифікація мережевих пакетів як шкідливих у системах IDS (Intrusion Detection Systems).	Висока точність за наявності якісних навчальних даних; швидке прийняття рішень.	Потребує маркованих даних; менш ефективний проти атак нульового дня.
Глибоке навчання (автокодери)	Використання нейронних мереж для аналізу складних даних і виявлення прихованих аномалій у великих обсягах мережевого трафіку.	Виявлення DDoS-атак або витоку даних шляхом аналізу аномалій у трафіку.	Здатність обробляти великі обсяги даних; висока ефективність для складних атак.	Вимагає значних обчислювальних ресурсів; складність інтерпретації результатів.
Рекурентні нейронні мережі (RNN)	Аналіз часових рядів для виявлення послідовних аномалій у поведінці користувачів або систем.	Моніторинг послідовності системних викликів для виявлення шкідливих програм.	Ефективний для аналізу динамічних процесів; враховує часову залежність.	Висока складність навчання; чутливість до шуму в даних.

Продовження таблиці 2.2 - Методи розпізнавання атак

Метод ШІ/МН	Опис	Приклади використання	Переваги	Обмеження
Ізоляційні ліси	Алгоритм для швидкого виявлення аномалій шляхом ізоляції даних у бінарних деревах.	Виявлення шкідливих програм, які маскуються під легітимні процеси.	Швидке виконання; не залежить від розподілу даних.	Менш ефективний для складних багатовимірних даних; потребує налаштування параметрів.

Одним із основних застосувань ШІ та МН у розпізнаванні атак є аналіз поведінки користувачів і об’єктів (User and Entity Behavior Analytics, UEBA). Цей підхід передбачає створення моделей нормальної поведінки на основі історичних даних, таких як частота входів у систему, типи операцій, географічне розташування, час активності тощо. Алгоритми МН, зокрема класифікація (наприклад, логістична регресія, підтримуючі векторні машини) і кластеризація (наприклад, k-середніх), дозволяють виявляти відхилення від нормальної поведінки, які можуть свідчити про компрометацію облікового запису, інсайдерські загрози або інші аномалії. Наприклад, якщо користувач, який зазвичай працює з офісної мережі в робочий час, раптово здійснює доступ до критичних систем із незвичайної локації вночі, система UEBA, побудована на основі МН, може позначити таку активність як підозрілу. Інтеграція UEBA з системами управління інформацією та подіями безпеки (SIEM) підвищує точність виявлення завдяки кореляції поведінкових даних із контекстними подіями безпеки.

Ще одним важливим напрямом є аналіз мережевого трафіку для виявлення аномалій. Алгоритми глибокого навчання, такі як автокодери або рекурентні нейронні мережі, здатні аналізувати великі обсяги трафіку в реальному часі, виявляючи незвичайні патерни, які можуть вказувати на атаки, наприклад, розподілені атаки типу "відмова в обслуговуванні" (DDoS) або витік

даних. Наприклад, різке зростання вихідного трафіку може свідчити про ексфільтрацію даних, а незвичайні зв’язки між вузлами мережі можуть вказувати на активність ботнету. Такі методи є особливо ефективними для виявлення атак, які не мають чітких сигнатур, як-от цілеспрямовані атаки (Advanced Persistent Threats, APT).

ШІ та МН також застосовуються для аналізу поведінки програмного забезпечення. Наприклад, моніторинг системних викликів або використання ресурсів дозволяє виявляти шкідливі програми, які маскуються під легітимні процеси. Алгоритми МН, такі як ізоляційні ліси, ефективно ідентифікують аномалії в поведінці програм, що може свідчити про наявність шкідливого коду. Крім того, ШІ використовується для прогнозного аналізу, який дозволяє передбачати потенційні атаки на основі історичних даних і поточних тенденцій, що особливо важливо для захисту критичної інфраструктури.

Переваги ШІ та МН у розпізнаванні атак включають їхню здатність обробляти великі обсяги даних, адаптуватися до нових загроз і виявляти аномалії без необхідності оновлення сигнатур. Однак ці технології мають і обмеження. По-перше, створення точних моделей нормальної поведінки вимагає значної кількості даних і може бути ускладненим у динамічних середовищах. По-друге, високий рівень помилкових спрацьовувань може виникати через недостатню специфіку моделей або природні зміни в поведінці, не пов’язані з атаками. Для зменшення цих недоліків застосовуються гібридні підходи, що поєднують ШІ та МН із сигнатурними методами та контекстним аналізом.

Подальший розвиток ШІ та МН у кібербезпеці пов’язаний із удосконаленням алгоритмів глибокого навчання, зокрема нейронних мереж із трансформерною архітектурою, а також із інтеграцією з технологіями аналізу великих даних і автоматизованого реагування на інциденти. Ці технології дозволяють створювати більш точні та адаптивні системи захисту, здатні протистояти складним кібератакам у реальному часі. Таким чином, ШІ та МН є

основою для проактивного підходу до кібербезпеки, забезпечуючи захист від сучасних і майбутніх загроз.

2.4 Фільтрація трафіку на рівні мережі та застосування брандмауерів

Фільтрація трафіку на рівні мережі є ключовим елементом забезпечення кібербезпеки, спрямованим на контроль і захист інформаційних потоків у комп'ютерних мережах. Цей процес передбачає аналіз і регулювання мережевого трафіку на основі заздалегідь визначених правил, що дозволяє блокувати шкідливі дані, обмежувати несанкціонований доступ і забезпечувати безпечну взаємодію між мережевими вузлами. Брандмауери (firewalls) є основним інструментом для реалізації фільтрації трафіку, виконуючи функції бар'єру між довіреними та недовіряними сегментами мережі. Вони аналізують пакети даних, застосовуючи правила фільтрації, які базуються на таких параметрах, як IP-адреси, порти, протоколи, а також, у сучасних системах, на основі поведінкового аналізу та контексту.

Принципи фільтрації трафіку на рівні мережі

Фільтрація мережевого трафіку ґрунтується на обробці пакетів даних на різних рівнях моделі OSI, зокрема мережевому (Layer 3) і транспортному (Layer 4). Основна мета полягає в тому, щоб дозволити проходження легітимного трафіку, одночасно блокуючи потенційно шкідливі або несанкціоновані запити. Фільтрація може здійснюватися на основі статичних правил (наприклад, блокування певних IP-адрес) або динамічних підходів, що враховують контекст і поведінку мережі. Основні методи фільтрації включають:

- Фільтрація за статичними правилами**:** базується на аналізі заголовків пакетів (IP-адреси джерела та призначення, порти, протоколи). Наприклад, брандмауер може блокувати весь трафік із певної IP-адреси, якщо вона асоціюється з відомим джерелом атак.
- Станова фільтрація (stateful inspection)**:** відстежує стан мережевих з'єднань (наприклад, встановлені, закриті) і дозволяє пропускати пакети лише в

рамках активних сесій. Це дозволяє ефективніше блокувати атаки, такі як спуфінг.

- Фільтрація на основі вмісту**:** аналізує не лише заголовки, а й вміст пакетів (deep packet inspection, DPI), що дає змогу виявляти шкідливі дані, такі як сигнатури вірусів або специфічні патерни атак.
- Поведінковий аналіз**:** сучасні брандмауери використовують алгоритми машинного навчання для виявлення аномалій у трафіку, наприклад, незвичайного зростання обсягу даних, що може вказувати на DDoS-атаку або витік інформації.

Роль брандмауерів у фільтрації трафіку

Брандмауери є основним інструментом для реалізації фільтрації мережевого трафіку та захисту від кіберзагроз. Вони можуть бути апаратними, програмними або хмарними, залежно від архітектури мережі та вимог безпеки. За функціональними можливостями брандмауери поділяються на кілька типів:

- Пакетні фільтри**:** працюють на мережевому рівні, аналізуючи заголовки пакетів і застосовуючи правила на основі IP-адрес, портів і протоколів. Вони є швидкими, але обмеженими через відсутність аналізу стану з’єднань.
- Станові брандмауери**:** відстежують стан з’єднань, що дозволяє ефективніше блокувати несанкціонований доступ і атаки, які використовують уразливості протоколів.
- Брандмауери наступного покоління (Next-Generation Firewalls, NGFW)**:** поєднують традиційну фільтрацію з розширеними функціями, такими як глибока перевірка пакетів (DPI), інтеграція з системами виявлення вторгнень (IDS/IPS), аналіз поведінки та підтримка шифрованого трафіку (наприклад, TLS/SSL).
- Хмарні брандмауери**:** застосовуються в хмарних середовищах для захисту віртуалізованих мереж, забезпечуючи гнучкість і масштабованість.

Брандмауери відіграють критичну роль у захисті від різноманітних атак, включаючи DDoS, SQL-ін’єкції, міжсайтові сценарії (XSS), а також у

запобіганні несанкціонованому доступу до внутрішніх ресурсів. Вони також можуть обмежувати вихідний трафік для запобігання витоку даних, що особливо важливо для захисту конфіденційної інформації в організаціях.

Застосування брандмауерів у сучасних мережах

У сучасних мережах брандмауери застосовуються для захисту як локальних, так і хмарних інфраструктур. Наприклад, у корпоративних мережах брандмауери розгортаються на периметрі для захисту від зовнішніх загроз, а також у внутрішніх сегментах для ізоляції критичних систем. У хмарних середовищах, таких як AWS або Azure, хмарні брандмауери забезпечують захист віртуальних машин і контейнерів, адаптуючись до динамічних змін у конфігурації мережі. Крім того, брандмауери інтегруються з іншими системами безпеки, такими як SIEM і IDS/IPS, для створення комплексного підходу до моніторингу та реагування на загрози.

2.5 Технології розподілу навантаження (Load Balancing, Anycast)

Технології розподілу навантаження є критично важливими для забезпечення високої доступності, масштабованості та ефективності сучасних мережевих систем. Вони дозволяють оптимізувати використання ресурсів, зменшувати час відповіді та підвищувати стійкість до збоїв і атак. Два ключові підходи до розподілу навантаження — це **Load Balancing** (балансування навантаження) та **Anycast** — використовуються для управління трафіком у мережах, але мають різні принципи роботи, сфери застосування та технічні особливості. У цьому розділі розглядаються основи цих технологій, їхні реалізації, переваги, обмеження та роль у сучасних інформаційних системах.

Балансування навантаження (Load Balancing)

Балансування навантаження — це технологія, яка розподіляє вхідний мережевий трафік між кількома серверами або ресурсами для забезпечення

оптимального використання обчислювальних потужностей, зниження затримок і запобігання перевантаженню окремих вузлів. Балансувальники навантаження діють як посередники між клієнтами та серверами, направляючи запити на основі заздалегідь визначених алгоритмів. Балансування може застосовуватися на різних рівнях моделі OSI, зокрема на транспортному (Layer 4) і прикладному (Layer 7) рівнях.

Застосування

Балансування навантаження широко використовується в веб-додатках, базах даних, хмарних сервісах і центрах обробки даних. Наприклад, у веб-додатках балансувальники розподіляють запити до серверів, які обробляють статичний або динамічний контент, забезпечуючи швидкий час відповіді. У хмарних середовищах вони дозволяють масштабувати програми горизонтально, додаючи нові сервери за потреби.

Anycast

Anycast — це технологія маршрутизації, яка дозволяє направляти запити від клієнта до найближчого (з точки зору мережевої топології) або найменш завантаженого вузла з однаковою IP-адресою, що використовується кількома серверами в різних географічних розташуваннях. Anycast базується на протоколі BGP (Border Gateway Protocol) і використовується в основному для підвищення доступності та зниження затримок у глобальних мережах, таких як системи доставки контенту (CDN) і DNS.

Принцип роботи Anycast

У мережі Anycast одна IP-адреса призначається кільком вузлам, розташованим у різних точках. Протокол BGP визначає найкоротший шлях до одного з цих вузлів на основі метрик маршрутизації, таких як кількість стрибків (hops) або затримка. Наприклад, запит до DNS-сервера з IP-адресою Anycast буде направлено до найближчого доступного сервера, що значно знижує час відповіді.

Застосування

- Системи доставки контенту (CDN)**:** компанії, такі як Cloudflare або Akamai, використовують Anycast для направлення користувачів до найближчого дата-центру, що прискорює завантаження веб-сторінок.
- DNS-сервіси**:** Anycast застосовується в кореневих DNS-серверах (наприклад, Google Public DNS — 8.8.8.8), щоб забезпечити швидке та надійне розв’язання доменів.
- Захист від DDoS-атак**:** Anycast розподіляє трафік атаки між кількома вузлами, зменшуючи навантаження на окремі сервери.

Таблиця 2.3 – Порівняння Load Balancing та Anycast

Характеристика	Load Balancing	Anycast
Принцип роботи	Розподіляє вхідний трафік між кількома серверами за допомогою алгоритмів (Round Robin, Least Connections тощо) у межах одного дата-центру чи хмари.	Направляє запити до найближчого вузла з однаковою IP-адресою через BGP-маршрутизацію.
Рівень OSI	Транспортний (Layer 4) або прикладний (Layer 7).	Мережевий (Layer 3).
Сфера застосування	Веб-додатки, бази даних, хмарні сервіси, внутрішні інфраструктури.	CDN, DNS, глобальні сервіси, захист від DDoS.
Алгоритми / механізми	Round Robin, Least Connections, Weighted, IP Hash, Least Response Time.	BGP-маршрутизація, вибір найкоротшого маршруту.
Переваги	- Гнучкість налаштувань- Підтримка сталості сесій- Висока продуктивність у межах однієї інфраструктури- Масштабованість у хмарі	- Мінімальні затримки завдяки географічній близькості- Стійкість до збоїв- Легка масштабованість- Ідеально для глобальних сервісів
Обмеження	- Складність у масштабних конфігураціях- Потенційна точка відмови без резервування- Недостатній захист від DDoS без додаткових засобів	- Складне керування BGP- Проблеми з постійністю сесій- Не підходить для станозалежних додатків
Приклади реалізації	NGINX, HAProxy, AWS ELB, F5 BIG-IP	Cloudflare, Google Public DNS (8.8.8.8), Akamai
Захист від атак	Потребує зовнішніх рішень (IDS/IPS, WAF)	Вбудована стійкість до DDoS через розподіл трафіку
Масштаб	Локальний або в межах хмари	Глобальний, з географічно розподіленими вузлами

Порівняння Load Balancing і Anycast

Load Balancing і Anycast виконують схожі функції, але мають різні сфери застосування. Load Balancing працює на рівні одного дата-центру або хмарного середовища, розподіляючи трафік між серверами за допомогою спеціалізованих алгоритмів. Anycast, навпаки, діє на глобальному рівні, використовуючи мережеву маршрутизацію для направлення запитів до географічно розподілених вузлів. Наприклад, Load Balancing підходить для веб-додатків у межах однієї інфраструктури, тоді як Anycast ідеальний для глобальних сервісів, таких як CDN або DNS.

2.6 Використання CDN та проксі-серверів для мінімізації впливу атак

Мережі доставки контенту (CDN) та проксі-сервери є важливими інструментами сучасної кібербезпеки, спрямованими на захист веб-ресурсів від атак, зокрема розподілених атак типу "відмова в обслуговуванні" (DDoS), атак на прикладний рівень та інших загроз, таких як перехоплення даних чи експлуатація вразливостей. Ці технології забезпечують не лише підвищення продуктивності та доступності веб-додатків, але й ефективне пом’якшення впливу шкідливого трафіку шляхом розподілу навантаження, кешування контенту та фільтрації запитів. Їхня інтеграція дозволяє створювати комплексні системи захисту, які поєднують швидкість доставки даних із надійним захистом від кіберзагроз.

Мережі доставки контенту функціонують як географічно розподілена інфраструктура, що складається з крайових серверів, які кешують статичний контент (зображення, скрипти, відео) і доставляють його користувачам із найближчого розташування. Це знижує затримки та зменшує навантаження на вихідний сервер. У контексті безпеки CDN відіграють ключову роль у пом’якшенні DDoS-атак шляхом розподілу трафіку між численними вузлами, що ускладнює перевантаження цільового сервера. Використання технології Anycast дозволяє направляти запити до найближчого доступного вузла, що

підвищує стійкість до атак і знижує час відповіді. Багато сучасних CDN, таких як Cloudflare або Akamai, інтегрують веб-фільтри (WAF), які аналізують запити на прикладному рівні та блокують шкідливі дії, наприклад, SQL-ін’єкції чи міжсайтові сценарії (XSS). Крім того, CDN забезпечують шифрування трафіку через HTTPS і приховують IP-адресу вихідного сервера, ускладнюючи прямі атаки. Проте їхня ефективність обмежується залежністю від постачальника та недостатньою адаптивністю до складних цілеспрямованих атак, таких як APT.

Проксі-сервери, діючи як посередники між клієнтом і сервером, забезпечують додатковий рівень захисту шляхом фільтрації та обробки запитів. Зворотні проксі, розташовані перед вихідним сервером, виконують функції балансування навантаження, кешування та глибокої перевірки пакетів (DPI), що дозволяє виявляти й блокувати шкідливі запити. Вони ефективно захищають від атак на прикладний рівень, таких як XSS або CSRF, а також можуть обмежувати доступ на основі географії чи IP-адрес. Проксі-сервери здатні аналізувати шифрований трафік, якщо налаштоване дешифрування HTTPS, що підвищує їхню ефективність проти прихованих загроз. Однак проксі-сервери можуть створювати додаткові затримки через обробку запитів і потребують ретельного налаштування для уникнення помилкових блокувань.

Комбіноване використання CDN і проксі-серверів забезпечує синергетичний ефект. CDN поглинає масові атаки та прискорює доставку контенту, тоді як проксі-сервери забезпечують детальну фільтрацію та захист від складних атак. Наприклад, CDN може розподілити трафік DDoS-атаки між крайовими вузлами, а зворотний проксі, розташований між CDN і вихідним сервером, фільтруватиме залишки шкідливого трафіку, аналізуючи його вміст. Такі рішення, як AWS CloudFront із WAF або NGINX як зворотний проксі, демонструють ефективність цього підходу.

Незважаючи на численні переваги, ці технології мають обмеження. CDN залежать від інфраструктури постачальника, що може створювати ризики в разі компрометації. Проксі-сервери, своєю чергою, потребують значних обчислювальних ресурсів для аналізу шифрованого трафіку та можуть бути

вразливими до неправильної конфігурації. Подальший розвиток цих технологій пов’язаний із інтеграцією штучного інтелекту та машинного навчання для адаптивного виявлення аномалій, а також із впровадженням принципів нульової довіри (Zero Trust), які вимагають постійної верифікації всіх запитів. Такі підходи дозволяють створювати більш стійкі та ефективні системи захисту від сучасних кіберзагроз.

Табличка 2.4 - Плюси та мінуси технологій CDN та Проксі-сервери

Технологія	**Переваги**	**Недоліки**
CDN	- Географічно розподілена інфраструктура поглинає великі обсяги трафіку. - Захист від DDoS за рахунок Anycast-маршрутизації. - Вбудований WAF блокує SQL-ін’єкції, XSS тощо. - Підтримка HTTPS та шифрування. - Приховує IP основного сервера. - Кешування зменшує навантаження на бекенд.	- Залежність від провайдера (ризик при його компрометації). - Обмежена ефективність проти складних цільових атак (APT). - Платні розширені функції. - Менша гнучкість у порівнянні з проксі-серверами.
Проксі-сервери	- Глибока перевірка пакетів (DPI) для виявлення XSS, CSRF, SQL-ін’єкцій. - Приховування IP основного сервера. - Гнучке налаштування фільтрів та підтримка HTTPS-аналізу. - Можливість кешування динамічних запитів. - Балансування навантаження.	- Можливі затримки при обробці трафіку, особливо шифрованого. - Складна конфігурація у великих системах. - Ризик блокування легітимного трафіку при помилках у налаштуваннях. - Недостатній захист від масових DDoS без CDN.

	- Легка інтеграція з WAF, IDS/IPS.	

2.7 Rate Limiting та обмеження запитів як стратегія захисту

Rate Limiting (обмеження швидкості запитів) та обмеження запитів є важливими стратегіями кібербезпеки, спрямованими на захист веб-ресурсів від зловмисного використання, зокрема атак типу "відмова в обслуговуванні" (DDoS), брутфорс-атак, а також надмірного навантаження, спричиненого автоматизованими запитами (ботами). Ці методи дозволяють контролювати обсяг і частоту запитів до серверів, API чи веб-додатків, забезпечуючи їхню стабільність і доступність. У науковому контексті ці стратегії розглядаються як ключові елементи захисту прикладного рівня, що доповнюють традиційні мережеві механізми, такі як брандмауери чи системи виявлення вторгнень.

Принципи Rate Limiting та обмеження запитів

Rate Limiting передбачає встановлення максимальної кількості запитів, які може надіслати користувач, IP-адреса або інший ідентифікатор за певний проміжок часу (наприклад, секунду, хвилину чи годину). Обмеження запитів, як ширший термін, включає не лише обмеження за частотою, але й інші параметри, такі як розмір даних, тип запитів або кількість одночасних з’єднань. Ці методи базуються на аналізі трафіку та застосуванні правил, які можуть бути статичними (наприклад, фіксована кількість запитів) або адаптивними (залежно від поведінки користувача чи контексту).

Основна мета цих стратегій полягає в запобіганні перевантаженню серверів, захисті від зловмисного використання API та забезпеченні справедливого розподілу ресурсів між легітимними користувачами. Наприклад, обмеження кількості запитів до API автентифікації може запобігти брутфорс-атакам, коли зловмисник намагається підібрати пароль шляхом багаторазового введення комбінацій.

Механізми реалізації

Rate Limiting та обмеження запитів реалізуються на різних рівнях інфраструктури:

- На рівні сервера**:** Веб-сервери (наприклад, NGINX, Apache) або проксі-сервери (HAProxy) можуть налаштовуватися для обмеження запитів за IP-адресою, HTTP-заголовками чи іншими ідентифікаторами
- На рівні API: API-шлюзи (наприклад, AWS API Gateway, Kong) застосовують обмеження на основі токенів, ключів API або ідентифікаторів клієнтів, що дозволяє контролювати доступ до конкретних ендпоінтів.
- На рівні CDN**:** Мережі доставки контенту, такі як Cloudflare або Akamai, інтегрують Rate Limiting для фільтрації трафіку ще до того, як він досягне вихідного сервера, що особливо ефективно проти DDoS-атак.
- Адаптивне обмеження: Сучасні системи використовують алгоритми машинного навчання для динамічного налаштування лімітів на основі поведінки користувачів, що дозволяє відрізняти легітимний трафік від шкідливого.

Застосування в захисті від атак

Rate Limiting та обмеження запитів є ефективними проти широкого спектру загроз:

- DDoS-атаки**:** Обмеження швидкості запитів на рівні CDN або проксі-сервера дозволяє блокувати масові запити від ботнетів, зменшуючи навантаження на вихідний сервер.
- Брутфорс-атаки**:** Обмеження кількості спроб автентифікації за IP-адресою чи користувачем запобігає підбору паролів.
- Скрейпінг контенту**:** Обмеження запитів до API чи веб-сторінок унеможливлює автоматизоване збирання даних ботами.
- Зловживання API**:** Rate Limiting захищає API від надмірного використання, забезпечуючи справедливий доступ для всіх клієнтів.

Переваги та обмеження

Rate Limiting та обмеження запитів мають низку переваг, що роблять їх незамінними в системах кібербезпеки. По-перше, вони забезпечують захист від перевантаження серверів, дозволяючи підтримувати доступність навіть під час атак. По-друге, ці методи є відносно простими у реалізації та можуть бути інтегровані з іншими інструментами безпеки, такими як WAF чи системи виявлення аномалій. По-третє, адаптивні алгоритми дозволяють налаштовувати обмеження залежно від контексту, що підвищує гнучкість.

Однак ці стратегії мають і обмеження. Неправильне налаштування лімітів може призвести до блокування легітимного трафіку, особливо в системах із високою варіативністю запитів (наприклад, під час пікових навантажень). Крім того, зловмисники можуть використовувати розподілені джерела (ботнети), щоб обійти обмеження за IP-адресами, що вимагає комбінації з іншими методами захисту, такими як аналіз поведінки. Нарешті, обробка великої кількості запитів для динамічного Rate Limiting може створювати додаткове навантаження на інфраструктуру, особливо в розподілених системах.

РОЗДІЛ 3

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ТА ОЦІНКА ЗАХИСТУ

3.1 Хмарні сервіси та їх роль у протидії DdoS

Хмарні сервіси забезпечують захист від DDoS-атак шляхом динамічного масштабування ресурсів, що дозволяє поглинати значні обсяги трафіку. Наприклад, у 2023 році Cloudflare успішно нейтралізував атаку обсягом 3,8 Тбіт/с, спрямовану на фінансовий сектор, використовуючи свою глобальну мережу пропускною здатністю 192 Тбіт/с. Фільтрація трафіку реалізується через комбінацію методів, включаючи поведінковий аналіз для виявлення аномалій, сигнатурний аналіз для ідентифікації відомих шаблонів атак, гео-фільтрацію для блокування запитів із підозрілих регіонів і обмеження частоти запитів (rate limiting). Алгоритми машинного навчання, інтегровані в системи провайдерів, таких як AWS Shield, Microsoft Azure DDoS Protection чи Google Cloud Armor, дозволяють оперативно відокремлювати легітимний трафік від шкідливого. Глобальна мережа дата-центрів (Points of Presence, PoP) провайдерів забезпечує перенаправлення трафіку через найближчі вузли, що зменшує навантаження на цільові сервери та мінімізує затримки.

Переваги хмарних сервісів у протидії DDoS-атакам включають високу пропускну здатність, яка дозволяє обробляти навіть наймасштабніші атаки, автоматизацію реагування, що забезпечує швидке виявлення та нейтралізацію загроз, і економічну ефективність завдяки моделі оплати за використання (pay-as-you-go). Наприклад, базові плани, такі як AWS Shield Standard або Azure DDoS Protection Basic, надаються безкоштовно в рамках хмарних пакетів, що робить їх доступними для організацій різного масштабу. Крім того, хмарні сервіси демонструють адаптивність до нових векторів атак завдяки регулярним оновленням алгоритмів і сигнатур.

Проте хмарні сервіси мають обмеження. Залежність від провайдера може створювати ризики, пов’язані з безпекою даних або перебоями в роботі.

Безкоштовні плани часто не забезпечують захисту від складних атак, таких як атаки рівня 7, а перенаправлення трафіку через хмарну інфраструктуру може викликати незначну латентність, що критично для додатків із високими вимогами до швидкості, наприклад, потокового відео чи онлайн-ігор. Крім того, захист від масштабних атак може потребувати дорогих підписок, таких як AWS Shield Advanced або Cloudflare Enterprise, що може бути фінансово обтяжливим для малих організацій.

Перспективи розвитку хмарних сервісів у протидії DDoS-атакам пов’язані з інтеграцією штучного інтелекту для прогнозування та автоматичного налаштування захисту, впровадженням edge computing для обробки трафіку ближче до джерела запитів і застосуванням моделі "нульової довіри" (Zero Trust), яка передбачає перевірку всіх запитів незалежно від їхнього походження. Крос-провайдерська співпраця також може підвищити ефективність захисту шляхом об’єднання ресурсів кількох хмарних платформ для протидії глобальним атакам.

Хмарні сервіси залишаються критично важливим інструментом у забезпеченні кібербезпеки, пропонуючи ефективний і гнучкий захист від DDoS-атак. Однак їхнє застосування вимагає ретельного аналізу потреб організації, врахування потенційних ризиків і оцінки співвідношення витрат і ефективності.

3.2 Моделювання DDoS-атак у тестовому середовищі

Моделювання DDoS-атак у тестовому середовищі передбачає кілька ключових етапів: створення ізольованого середовища, вибір інструментів, розробку сценаріїв, виконання тестів і аналіз даних.

Тестове середовище має бути ізольованим від реальних систем, щоб уникнути ненавмисного впливу. Воно зазвичай включає віртуалізовані сервери (наприклад, на платформах VMware, VirtualBox або хмарних сервісах, таких як AWS, Azure чи Google Cloud), мережеві симулятори та системи моніторингу продуктивності. Для забезпечення реалістичності середовище конфігурується з

урахуванням параметрів цільової системи, таких як пропускна здатність мережі, обчислювальні ресурси та конфігурація програмного забезпечення.

Інструменти для моделювання DDoS-атак включають спеціалізоване програмне забезпечення, здатне генерувати контрольований трафік. Наприклад, інструменти типу LOIC (Low Orbit Ion Cannon), hping3, Slowloris або Apache JMeter дозволяють симулювати атаки різних типів, включаючи об’ємні (Volumetric), протокольні (Protocol) та атаки рівня прикладного рівня (Application Layer). Хмарні сервіси, такі як AWS Lambda або Azure Functions, можуть використовуватися для масштабування тестового трафіку, імітуючи розподілені джерела атак.

Сценарії атак розробляються з урахуванням типів DDoS-атак: об’ємні атаки (наприклад, UDP Flood, ICMP Flood), протокольні атаки (SYN Flood, Ping of Death) та атаки рівня 7 (HTTP Flood, Slowloris). Кожен сценарій включає параметри, такі як обсяг трафіку, частота запитів, тривалість атаки та географічна розподіленість джерел. Для оцінки захисту моделюються як прості, так і складні атаки, що комбінують різні вектори.

Виконання тестів передбачає запуск сценаріїв у контрольованому середовищі з одночасним моніторингом продуктивності системи. Використовуються метрики, такі як час відгуку сервера, пропускна здатність, рівень використання процесора та пам’яті, а також кількість оброблених легітимних запитів. Системи моніторингу, наприклад, Nagios, Zabbix або Prometheus, дозволяють у реальному часі відстежувати поведінку системи під навантаженням.

Моделювання DDoS-атак у тестовому середовищі дозволяє виявити слабкі місця системи до виникнення реальних загроз, оптимізувати захисні механізми та підготувати персонал до реагування. Хмарні сервіси, такі як AWS Shield або Cloudflare, можуть бути інтегровані в тестування для оцінки їхньої ефективності. Проте моделювання має обмеження: складність відтворення всіх аспектів реальних атак, зокрема їхньої непередбачуваності, а також витрати на

створення реалістичного тестового середовища. Крім того, некоректна конфігурація може призвести до помилкових результатів.

Подальший розвиток моделювання DDoS-атак пов’язаний із застосуванням штучного інтелекту для створення адаптивних сценаріїв, що імітують поведінку реальних атак, та інтеграцією технологій edge computing для підвищення реалістичності тестів. Використання хмарних платформ дозволяє масштабувати тестові середовища, забезпечуючи економічно ефективне моделювання.

3.3 Аналіз впливу атак на мережеві ресурси

DDoS-атаки класифікуються за рівнем моделі OSI, на який вони спрямовані: об’ємні (Volumetric), протокольні (Protocol) та атаки рівня прикладного рівня (Application Layer). Об’ємні атаки, такі як UDP Flood або ICMP Flood, вичерпують пропускну здатність мережі, генеруючи значні обсяги трафіку (наприклад, атака обсягом 3,8 Тбіт/с, зафіксована Cloudflare у 2023 році). Протокольні атаки, зокрема SYN Flood, перевантажують ресурси обробки серверів або мережевого обладнання. Атаки рівня 7, як HTTP Flood або Slowloris, спрямовані на вичерпання обчислювальних ресурсів шляхом надсилання легітимних на вигляд запитів, що ускладнює їх виявлення.

Механізми впливу DDoS-атак включають вичерпання пропускної здатності, що унеможливлює передачу легітимного трафіку, та перевантаження обчислювальних ресурсів, що знижує продуктивність серверів. Наприклад, атака Slowloris утримує відкриті HTTP-з’єднання, перешкоджаючи обробці нових запитів. Це призводить до порушення доступності сервісів, затримок у транзакціях і збоїв у критичних системах. Фінансові наслідки включають прямі витрати на відновлення та непрямі втрати через простої (згідно з IBM Security, 2023, середня вартість кібератаки становить 4,45 млн дол. США). Репутаційні втрати, особливо в секторах електронної комерції та фінансових послуг, знижують довіру клієнтів.

Аналіз впливу DDoS-атак передбачає моніторинг продуктивності за допомогою систем, таких як Prometheus або Zabbix, для вимірювання метрик (час відгуку, використання процесора, пропускна здатність). Аналіз логів серверів і мережевого обладнання дозволяє ідентифікувати джерела атак і вразливості. Моделювання атак у тестовому середовищі з використанням інструментів, таких як hping3 або Apache JMeter, допомагає оцінити стійкість системи. Економічний аналіз включає оцінку прямих і непрямих втрат, а також витрат на впровадження захисних заходів.

Для пом’якшення впливу застосовуються хмарні сервіси захисту (наприклад, AWS Shield, Cloudflare), які поглинають і фільтрують шкідливий трафік, використовуючи глобальну інфраструктуру. Фільтрація на основі поведінкового аналізу, гео-фільтрації та обмеження частоти запитів дозволяє відокремлювати легітимний трафік. Резервування ресурсів і плани реагування на інциденти забезпечують швидке відновлення. Перспективи розвитку включають інтеграцію штучного інтелекту для прогнозування атак, використання edge computing для зниження затримок і впровадження моделі "нульової довіри".

DDoS-атаки мають значний вплив на мережеві ресурси, спричиняючи технічні збої, операційні перерви, фінансові втрати та репутаційні ризики. Комплексний аналіз їхнього впливу з використанням моніторингу, моделювання та економічної оцінки дозволяє розробляти ефективні стратегії захисту. Хмарні технології та інноваційні підходи, такі як ШІ, відіграють ключову роль у підвищенні стійкості мережевих ресурсів до цих загроз.

3.4 Тестування ефективності захисних механізмів

Методологія тестування передбачає створення ізольованого середовища, яке виключає вплив на реальні системи. Таке середовище включає віртуалізовані сервери, створені за допомогою платформ VMware, VirtualBox або хмарних сервісів, таких як AWS, Microsoft Azure чи Google Cloud, а також

конфігурацію мережевої інфраструктури з маршрутизаторами, брандмауерами та системами моніторингу, такими як Prometheus або Zabbix, для відстеження продуктивності в реальному часі. Для моделювання атак використовуються спеціалізовані інструменти, зокрема hping3 для протокольних атак типу SYN Flood, Slowloris для атак рівня прикладного рівня, Apache JMeter для симуляції HTTP Flood, а також хмарні сервіси, такі як AWS Lambda, для створення розподіленого трафіку. Сценарії тестування відтворюють різні типи атак, включаючи об'ємні (UDP Flood), протокольні (Ping of Death) та атаки рівня 7 (HTTP Flood), із заданими параметрами, такими як обсяг трафіку, тривалість і географічна розподіленість джерел.

Виконання тестів передбачає запуск сценаріїв із активованими захисними механізмами, такими як хмарні сервіси Cloudflare або AWS Shield, які поглинають і фільтрують шкідливий трафік. Під час тестування відстежуються метрики продуктивності: час відгуку сервера, пропускна здатність, використання процесора та пам'яті, відсоток заблокованого шкідливого трафіку та час відновлення системи. Аналіз результатів оцінює ефективність виявлення атак, точність фільтрації, стійкість системи та економічну доцільність захисних рішень. Результати документуються у вигляді звітів із графіками продуктивності та рекомендаціями щодо вдосконалення.

Тестування дозволяє виявити вразливості до виникнення реальних атак і оптимізувати захист. Хмарні сервіси, наприклад, Cloudflare, продемонстрували здатність нейтралізувати атаку обсягом 3,8 Тбіт/с у 2023 році, що підкреслює їхню ефективність. Проте тестування має обмеження: складність відтворення непередбачуваних реальних атак, високі витрати на створення реалістичного середовища та ризик помилкових результатів через некоректну конфігурацію. Етичні аспекти вимагають проведення тестів лише за згодою власників систем і в ізольованому середовищі, щоб уникнути правових порушень.

Перспективи розвитку тестування пов'язані з інтеграцією штучного інтелекту для створення адаптивних сценаріїв, використанням edge computing для підвищення реалістичності та автоматизацією аналізу результатів. Хмарні

платформи забезпечують економічно ефективне масштабування тестових середовищ, сприяючи вдосконаленню захисних механізмів.

Тестування ефективності захисних механізмів проти DDoS-атак є важливим інструментом забезпечення кібербезпеки. Воно дозволяє оцінити стійкість систем, виявити слабкі місця та оптимізувати стратегії захисту. Незважаючи на обмеження, пов’язані з витратами та складністю моделювання, інноваційні технології, такі як ШІ та edge computing, підвищують точність і ефективність тестування, зміцнюючи захист від кіберзагроз.

3.5 Порівняльний аналіз різних методів захисту

Методи захисту від DDoS-атак можна класифікувати за їхньою архітектурою та принципами роботи. Локальні апаратні рішення, такі як спеціалізовані брандмауери та системи виявлення вторгнень (IDS/IPS), встановлюються безпосередньо в інфраструктурі організації. Вони аналізують вхідний трафік, блокуючи шкідливі запити на основі сигнатур або аномалій. Хмарні сервіси, такі як Cloudflare, AWS Shield і Microsoft Azure DDoS Protection, використовують глобальну розподілену інфраструктуру для поглинання та фільтрації трафіку. Програмні системи фільтрації, наприклад, ModSecurity або Suricata, інтегруються в серверне програмне забезпечення для аналізу запитів на рівні додатків. Гібридні підходи поєднують локальні та хмарні рішення, забезпечуючи комплексний захист.

Локальні апаратні рішення ефективні для захисту від атак середнього масштабу, оскільки дозволяють точно налаштувати фільтрацію відповідно до потреб організації. Вони забезпечують низьку латентність, оскільки обробка трафіку відбувається на локальному рівні, і не залежать від сторонніх провайдерів. Проте їхня ефективність обмежується пропускною здатністю обладнання, що робить їх вразливими до об’ємних атак, таких як UDP Flood обсягом 3,8 Тбіт/с, зафіксований у 2023 році. Крім того, такі рішення вимагають значних капітальних витрат на закупівлю, встановлення та

обслуговування, а також регулярного оновлення сигнатур для протидії новим загрозам.

Хмарні сервіси є найпоширенішим методом захисту завдяки їхній здатності масштабувати ресурси та поглинати великі обсяги трафіку. Наприклад, Cloudflare у 2023 році успішно нейтралізував атаку обсягом 3,8 Тбіт/с, використовуючи мережу пропускною здатністю 192 Тбіт/с. Ці сервіси застосовують поведінковий аналіз, гео-фільтрацію та алгоритми машинного навчання для відокремлення легітимного трафіку від шкідливого. Хмарні рішення економічно ефективні завдяки моделі оплати за використання, але можуть викликати незначну латентність через перенаправлення трафіку та створюють залежність від провайдера, що пов’язано з ризиками доступності або безпеки даних.

Програмні системи фільтрації підходять для захисту на рівні додатків, зокрема від атак типу HTTP Flood або Slowloris. Вони інтегруються в серверне програмне забезпечення, дозволяючи аналізувати запити в реальному часі. Такі системи є гнучкими та відносно недорогими, але їхня ефективність залежить від обчислювальних ресурсів сервера, що робить їх менш стійкими до об’ємних атак. Крім того, вони потребують регулярного оновлення правил фільтрації для протидії новим загрозам.

Гібридні підходи поєднують переваги локальних і хмарних рішень, забезпечуючи локальну фільтрацію для швидкого реагування та хмарне масштабування для поглинання великих обсягів трафіку. Наприклад, організація може використовувати локальний брандмауер для захисту від протокольних атак і хмарний сервіс, такий як AWS Shield, для нейтралізації об’ємних атак. Гібридні системи є ефективними для складних атак, але їх впровадження та підтримка є складними та витратними, що може бути недоцільним для малих організацій.

Порівняння методів за ключовими критеріями показує, що хмарні сервіси мають перевагу в масштабованості та економічній ефективності, тоді як локальні рішення вирізняються низькою латентністю та автономністю.

Програмні системи є оптимальними для захисту на рівні додатків, але менш ефективні проти об’ємних атак. Гібридні підходи забезпечують комплексний захист, але вимагають значних ресурсів. Вибір методу залежить від потреб організації, типу очікуваних атак і доступного бюджету.

Перспективи розвитку методів захисту включають інтеграцію штучного інтелекту для прогнозування атак, використання edge computing для обробки трафіку ближче до джерела та впровадження архітектури "нульової довіри" для перевірки всіх запитів. Крос-провайдерська співпраця може підвищити ефективність захисту від глобальних атак.

Порівняльний аналіз методів захисту від DDoS-атак демонструє, що кожен підхід має свої сильні та слабкі сторони. Хмарні сервіси є найбільш універсальними завдяки масштабованості та автоматизації, тоді як локальні та програмні рішення підходять для специфічних сценаріїв. Гібридні підходи забезпечують максимальну стійкість, але потребують ретельного планування. Вибір оптимального методу залежить від аналізу ризиків, інфраструктури та фінансових можливостей організації, а подальший розвиток технологій ШІ та edge computing сприятиме підвищенню ефективності захисту.

Таблиця 3.1 - Порівняння методів захисту від DDoS-атак

Критерій	**Локальні апаратні рішення**	**Хмарні сервіси**	**Програмні системи**	**Гібридні підходи**
Ефективність	Середня; слабкі проти об’ємних атак (>1 Тбіт/с)	Висока, включаючи об’ємні атаки (3,8 Тбіт/с, Cloudflare 2023)	Ефективні для атак рівня 7	Комплексний захист
Масштабованість	Обмежена апаратними ресурсами	Висока (глобальна інфраструктура)	Залежить від серверів	Висока
Вартість	Високі капітальні витрати	Економічна (pay-as-you-go)	Низька; потребує ресурсів	Висока
Сфера застосування	Малі організації	Універсальна	Веб-додатки	Критичні системи

ВИСНОВКИ

DDoS-атаки є однією з найсерйозніших кіберзагроз сучасності, що характеризуються високою доступністю для зловмисників (DDoS-as-a-Service від $10 за годину) та значним впливом на доступність мережевих ресурсів. Зростання кількості IoT-пристроїв (понад 15 млрд у 2024 році) і використання штучного інтелекту для створення адаптивних атак ускладнюють їх виявлення та нейтралізацію. Атаки класифікуються за рівнем моделі OSI (об'ємні, протокольні, прикладного рівня) та мають економічні (збитки до $2 млн за атаку), технічні, соціальні та безпекові наслідки, що підтверджується прикладами атак на Dyn (2016), GitHub (2018) та Amazon AWS (2020).

Методи виявлення DDoS-атак включають аналіз мережевого трафіку, використання систем IDS/IPS, поведінковий аналіз, машинне навчання та хмарні технології. IDS/IPS ефективні для відомих атак, але мають обмеження для нових загроз через залежність від сигнатур. Поведінковий аналіз і машинне навчання (алгоритми Random Forest, нейронні мережі) дозволяють виявляти аномалії в реальному часі, але потребують значних обчислювальних ресурсів і якісних даних для навчання. Хмарні рішення, такі як Cloudflare і AWS Shield, забезпечують швидке реагування завдяки глобальній інфраструктурі, але створюють залежність від провайдера.

Захисні механізми включають локальні апаратні рішення, хмарні сервіси, програмні системи фільтрації та гібридні підходи. Хмарні сервіси вирізняються високою масштабованістю, нейтралізуючи атаки обсягом до 3,8 Тбіт/с (Cloudflare, 2023), але можуть викликати латентність. Локальні рішення забезпечують автономність, але обмежені пропускною здатністю. Програмні системи ефективні для атак рівня 7, але вразливі до об'ємних атак. Гібридні підходи пропонують комплексний захист, але є складними та витратними.

Експериментальне дослідження показало, що моделювання атак у тестовому середовищі (з використанням hping3, Slowloris, JMeter) дозволяє оцінити стійкість систем і оптимізувати захист. Хмарні сервіси відіграють

ключову роль у поглинанні трафіку, тоді як аналіз впливу атак (за метриками продуктивності) допомагає виявити вразливості. Обмеженнями є складність відтворення реальних атак і витрати на тестування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. National Institute of Standards and Technology (NIST). (2012). SP 800-30: Guide for Conducting Risk Assessments.

2. FireEye. (2017). WannaCry Ransomware Campaign: Technical Analysis.

3. Kaspersky Lab. (2016). The Mirai Botnet: A Look into IoT-Based Attacks.

4. National Institute of Standards and Technology (NIST). (2012). SP 800-61: Computer Security Incident Handling Guide.

5. Cloudflare. (2018). The GitHub DDoS Attack: Technical Analysis.

6. Cybersecurity Ventures. (2024). Cybercrime Report 2024: Global Costs and Trends.

7. National Institute of Standards and Technology (NIST). (2012). SP 800-61: Computer Security Incident Handling Guide. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

8.ENISA. (2023). Threat Landscape 2023: Emerging Trends in Cybersecurity. Available: https://www.enisa.europa.eu

9.Statista. (2025). IoT Connected Devices Forecast. Available: https://www.statista.com

10. Antonakakis, M., et al. (2017). Understanding the Mirai Botnet. USENIX Security Symposium.

11. Symantec. (2007). Estonia Cyberattacks: Technical Report. https://www.symantec.com

12. Bhadauria, R., & Sanyal, S. (2012). Survey on DDoS Attacks and Defense Mechanisms. International Journal of Computer Applications, 45(7).

13. Somani, G., et al. (2017). DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions. Computer Communications.

14. Bhadauria, R., & Sanyal, S. (2012). Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. International Journal of Computer Applications, 47(18), 47-66.

15. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges. Computers & Security, 28(1-2), 18-28.

16. Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion Detection System: A Comprehensive Review. Journal of Network and Computer Applications, 36(1), 16-24.

17. Suricata Team. (2023). Suricata User Guide. Доступно за: https://suricata.io/documentation/.

18. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. National Institute of Standards and Technology.

19. Liu, Y., & Sun, Y. (2019). Anomaly detection in user behavior using machine learning techniques. Journal of Cybersecurity, 5(1), 45-60.

20. Miloslavskaya, N., & Tolstoy, A. (2018). Big data, fast data and data lake concepts for SIEM systems. Procedia Computer Science, 135, 14-23.

21. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

22. Zeadally, S., & Tsikerdekis, M. (2020). Securing Internet of Things (IoT) with machine learning. International Journal of Communication Systems.

23. Stallings, W. (2017). Network Security Essentials: Applications and Standards. Pearson.

24. Kurose, J. F., & Ross, K. W. (2016). Computer Networking: A Top-Down Approach. Pearson.

25. Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks. Prentice Hall.

26. AWS. (2023). AWS Shield Documentation. Retrieved from https://aws.amazon.com/shield.

27. Microsoft Azure. (2023). Azure DDoS Protection Documentation. Retrieved from https://azure.microsoft.com.

28. Bhadauria, R., & Sanyal, S. (2012). Survey on security issues in cloud computing and associated mitigation techniques. International Journal of Computer Applications, 47-66.

29. IBM Security. (2023). Cost of a Data Breach Report. Retrieved from https://www.ibm.com.

30. Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyuka, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 30-48.