УДК 004

**В. В. Скомаровський**
**І. О. Бондаренко**

# ТИПИ DDoS-АТАК НА ІНТЕРНЕТ-РЕСУРСИ

Вінницький національний технічний університет

***Анотація***

*Розподілені атаки на відмову в обслуговуванні (DDoS) — це тип кібератаки, який передбачає заповнення цільового веб-сайту або мережі трафіком із кількох джерел, щоб перевантажити ціль і запобігти доступу законних користувачів до сайту. DDoS-атаки можуть мати серйозні наслідки для організацій і окремих осіб, оскільки вони можуть порушити роботу критично важливих служб і спричинити фінансові збитки. У цій статті ми обговоримо різні типи DDoS-атак та їх характеристики, відмінності між DDoS-атаками та вимогами до послуг, юридичні аспекти DDoS-атак, а також можливості відстеження та запобігання цим атакам.*

**Ключові слова:** DDoS-атака, кібератаки, інтернет-ресурси, трафік, порушення, запобігання.

***Abstract***

*Distributed denial of service (DDoS) attacks are a type of cyber-attack that involves inundating a targeted website or network with traffic from multiple sources in order to overwhelm the target and prevent legitimate users from accessing the site. DDoS attacks can have serious consequences for organizations and individuals, as they can disrupt critical services and cause financial losses. In this article, we will discuss the different types of DDoS attacks and their characteristics, the differences between DDoS attacks and service requirements, the legal aspects of DDoS attacks, and the possibilities of tracking and preventing these attacks.*

**Keywords:** DDoS-attacks, cyber-attacks, internet resources, traffic, disruption, prevention.

## Вступ

Інтернет став невід'ємною частиною сучасного суспільства, і окремі особи та організації покладаються на нього для широкого кола видів діяльності, таких як спілкування, торгівля та доступ до інформації. Проте все більша залежність від Інтернету також зробила його мішенню для кібератак, однією з найпоширеніших з яких є розподілена відмова в обслуговуванні (DDoS).

DDoS-атака – це тип кібератаки, під час якої цільовий веб-сайт або мережа переповнюється трафіком із кількох джерел, щоб перевантажити ціль і запобігти доступу законних користувачів до сайту. DDoS-атаки можуть мати серйозні наслідки, оскільки вони можуть порушити роботу критично важливих служб і спричинити фінансові збитки для організацій і окремих осіб. [1].

## Результати дослідження

Однією з ключових відмінностей між DDoS-атаками та звичайними вимогами до обслуговування є обсяг трафіку. Звичайні вимоги до обслуговування передбачають передбачуваний і керований рівень трафіку, тоді як DDoS-атаки передбачають набагато вищий рівень трафіку, який призначений для перевантаження цілі [2].

Існує кілька різних типів DDoS-атак, кожна з яких має свої особливості. Деякі з найпоширеніших типів DDoS-атак включають:

– Об'ємні атаки: ці атаки передбачають переповнення цілі великим обсягом трафіку з метою використання пропускної здатності та виснаження ресурсів цілі. Приклади об'ємних атак включають UDP-флуди та ICMP-флуди.

– Атаки по протоколам: ці атаки спрямовані на певні рівні стеку мережевих протоколів, щоб порушити зв'язок цільової мережі. Приклади атак на протокол включають SYN-флуд і атаки на виснаження з'єднання TCP.

– Атаки на прикладному рівні: ці атаки спрямовані на прикладний рівень стека мережевих протоколів і спрямовані на споживання ресурсів і порушення роботи цільових служб. Приклади атак прикладного рівня включають HTTP-флуди та атаки Slowloris [3-4].

DDoS-атаки можуть мати серйозні наслідки для організацій і окремих осіб. Вони можуть порушити роботу критично важливих послуг і спричинити фінансові збитки, а також завдати шкоди репутації організації. DDoS-атаки також можна використовувати як димову завісу для інших кібератак, таких як витік даних або зараження шкідливим програмним забезпеченням. DDoS-атаки є незаконними в багатьох країнах і можуть призвести до кримінальної відповідальності для винних.

Відстеження DDoS-атаки може бути складним, оскільки трафік, залучений до атаки, часто походить із кількох джерел, і його важко відрізнити від законного трафіку. Однак існує ряд інструментів і методів, які можна використовувати для виявлення та відстеження DDoS-атак, включаючи засоби моніторингу мережі, системи виявлення вторгнень і брандмауери веб-додатків [5].

Запобігання DDoS-атакам є складним завданням, оскільки існує багато різних типів атак, а методи, які використовують зловмисники, постійно вдосконалюються. Проте існує ряд кроків, які організації та окремі особи можуть зробити, щоб захиститися від атак DDoS, зокрема:

– Впровадження заходів безпеки мережі: це може включати такі заходи, як брандмауери, системи виявлення вторгнень і балансувальники навантаження, які можуть допомогти відфільтрувати зловмисний трафік і захистити від атак DDoS.

– Використання мереж доставки контенту (CDN): CDN можуть допомогти розподілити трафік через мережу серверів, що може ускладнити атаку зловмисників на одну ціль.

– Впровадження обмеження швидкості: обмеження швидкості – це техніка, яка передбачає обмеження кількості запитів, які сервер оброблятиме з одного джерела протягом певного періоду часу. Це може допомогти запобігти DDoS-атакам, обмежуючи обсяг трафіку, який може генерувати одне джерело.

– Відстеження незвичайних моделей трафіку: регулярний моніторинг моделей трафіку може допомогти організаціям виявити потенційні атаки DDoS і вжити відповідних заходів.

– Реалізація планів на випадок надзвичайних ситуацій. Наявність плану боротьби з DDoS-атаками може допомогти організаціям мінімізувати вплив атаки та якнайшвидше відновити критично важливі служби [5].

## Висновки

Отже, DDoS-атаки є однією з найпоширеніших загроз для інтернет-ресурсів, оскільки вони можуть порушити роботу критично важливих сервісів і завдати фінансових збитків. Розуміння різних типів DDoS-атак і методів, що використовуються для їх запобігання, є важливим для будь-якої організацій і окремих осіб, які покладаються на Інтернет.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Distributed Denial of Service (DDoS) Attacks [Електронний ресурс] – Режим доступу: https://www.imperva.com/learn/ddos/denial-of-service/ (дата звернення 27.02.2023).

2. What is a DDoS attack?" (n.d.). [Електронний ресурс] – Режим доступу: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (дата звернення 28.02.2023).

3. DDoS attack meaning [Електронний ресурс] – Режим доступу: https://www.akamai.com/our-thinking/ddos (дата звернення 03.03.2023).

4. 12 Common Types of DDoS Attacks Explained [Електронний ресурс] – Режим доступу: https://easydmarc.com/blog/12-common-types-of-ddos-attacks-explained/ (дата звернення 04.03.2023).

5. Joseph Steinberg. Cybersecurity for Dummies , John Wiley & Sons, Inc., 2019. – 368 с.

***Скомаровський Владислав Володимирович*** – студент групи 2КІТС-22м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: vladyslav.skomarovskyy@gmail.com

***Бондаренко Ірина Олексіївна –*** асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

***Skomarovskyy Vladyslav V.*** – student of 2CSITS-22m group, Department of Management and Information Security, Vinnytsa National Technical University, Vinnytsia**,** e-mail: vladyslav.skomarovskyy@gmail.com

***Bondarenko Iryna O. –*** assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua