**Аналіз самоподібного трафіку з метою захисту**

**корпоративних мереж від прихованих DdOS-атак.**

**Анотація**

У рамках цієї роботи розглядаються методи аналізу самоподібності трафіку з використанням математичних та статистичних інструментів, таких як фрактальний аналіз та методи дослідження кореляційної структури даних. Особлива увага приділяється застосуванню цих методів для захисту корпоративних мереж від прихованих DDoS-атак, які можуть маскуватися під легітимний трафік, що значно ускладнює їх виявлення традиційними методами.

**Вступ**

У сучасному цифровому світі корпоративні мережі відіграють важливу роль в економіці, бізнесі та технологіях. Проте вони постійно піддаються загрозам кібератак, серед яких особливе місце займають DDoS-атаки (розподілені атаки на відмову в обслуговуванні). Ці атаки спрямовані на перевантаження мережевих ресурсів, що призводить до їх відмови в наданні послуг. Однією з найбільш небезпечних форм цих атак є приховані DDoS-атаки, які можуть бути важко виявленими через схожість з нормальним трафіком. Тому захист корпоративних мереж від таких атак вимагає нових підходів, серед яких аналіз самоподібного трафіку є ефективним методом.

Мережевий трафік в реальних системах має властивість самоподібності, що означає схожість структури трафіку на різних часових масштабах. Самоподібність полягає в тому, що статистичні властивості трафіку, такі як частота передачі пакетів і розподіл затримок, можуть бути подібними незалежно від того, на якому часовому інтервалі вони розглядаються. Ця властивість дозволяє будувати моделі мережевого трафіку, що можуть допомогти у виявленні аномалій, таких як DDoS-атаки.Фрактальна природа трафіку робить його більш стійким до випадкових коливань і дозволяє виявляти відхилення, які можуть бути спричинені кібератаками. Відповідно, аналіз самоподібного трафіку стає ключовим інструментом для моніторингу корпоративних мереж з метою попередження та виявлення прихованих DDoS-атак.

Приховані DDoS-атаки відрізняються тим, що вони маскуються під легітимний трафік. Це робить їх особливо небезпечними для корпоративних мереж, оскільки традиційні системи захисту, які спираються на фіксовані шаблони або чітко виражені аномалії, можуть не виявити такі атаки. Зазвичай ці атаки використовують ботнети для генерування трафіку, що виглядає природно, проте їхня мета перевантажити ресурси мережі, що призводить до відмови в обслуговуванні.

Аналіз самоподібного трафіку ґрунтується на математичних і статистичних методах дослідження кореляційної структури трафіку. Одним із ключових інструментів є фрактальний аналіз, який дозволяє вимірювати самоподібність трафіку. Найчастіше використовують такі методи, як:

1. **Масштабно-інваріантні методи** – вони допомагають визначити самоподібність на різних часових масштабах. Для цього використовують параметр Херста, який показує ступінь довгострокової залежності у часовому ряду.
2. **Мультифрактальний аналіз** – досліджує різні фрактальні властивості мережевого трафіку і дозволяє виявляти складніші патерни аномалій.
3. **Кореляційний аналіз** – визначає зв’язок між різними часовими інтервалами трафіку, що дозволяє ідентифікувати приховані DDoS-атаки через зміну кореляційних властивостей.

Самоподібність забезпечує можливість відстежувати структуру трафіку на різних масштабах часу. Якщо в певний момент з'являються порушення в характері самоподібності, це може свідчити про приховані DDoS-атаки. Такі порушення важко помітити в короткострокових часових інтервалах, але їх можна зафіксувати при аналізі на довготривалій основі.

Аналіз самоподібного трафіку є потужним інструментом для захисту корпоративних мереж від прихованих DDoS-атак. Використання математичних і статистичних методів дозволяє виявляти відхилення в поведінці мережевого трафіку, які можуть бути наслідком кіберзагроз. Це забезпечує можливість своєчасного попередження про потенційні атаки та підвищує ефективність захисту корпоративної інфраструктури.

Однак слід зазначити, що використання цього підходу потребує глибокого розуміння мережевої архітектури та доступу до інструментів аналізу великих обсягів даних. Поєднання фрактального аналізу з іншими методами кіберзахисту створює потужну систему захисту від кібератак, яка може забезпечити надійність і безпеку корпоративних мереж.

Список використаних джерел

[1] S. Sengupta, A. Greenberg, P. Patel, R. Chaiken, The nature of data center traffic: Measurements & analysis

[2] A. Lara, A. Kolasani, B. Ramamurthy, Network innovation using openflow

[3] H. Lai, S. Cai, H. Huang, J. Xie, H. Li, A parallel intrusion detection system for high-speed networks