УДК 004.7

О.В. Коваленко[1]
Кіровоградський національний технічний університет

Дослідження методів захисту телекомунікаційних мереж від розподілених DDoS атак

На сьогоднішній день DDoS-атаки є найнебезпечнішою кібернетичною зброєю. Цілі таких атак зводяться до підриву нормального функціонування мережі за рахунок обробки пакетів або витрат системних ресурсів. Виникає гостра проблема в пошуку методів захисту від DDoS атак в телекомунікаційних мережах. Проведені дослідження виявили наступні найпоширеніші варіанти DDoS атак:

– HTTP GET - скоординована відправка на Web сервер великої кількості запитів;

– DNS flood - відправка аномально великого числа DNS запитів;

– UDP flood - відправка на адресу системи, що атакується, безлічі пакетів UDP великого розміру;

– TCP SYN flood - відправка великої кількості запитів на ініціалізацію TCP з'єднань з вузлом мережі, якому в результаті доводиться витрачати всі свої ресурси на обробку цих частково відкритих з'єднань.

Крім того, проведені дослідження показали, що традиційні технічні рішення для забезпечення захисту телекомунікаційних мереж такі, як міжмережні екрани та системи виявлення вторгнень (IDS), самі по собі не забезпечують захисту від DDoS атак. Єдиним ефективним методом виявлення DDoS-атаки залишається аналіз аномалій в мережному трафіку.

Також найбільш поширеним і ефективним можна назвати метод захисту від DDoS атак на основі технології Cisco Clean Pipes. Технологія передбачає використання модулів Cisco Anomaly Detector і Cisco Guard, а також різних систем статистичного аналізу мережевого трафіку, заснованих на даних, одержуваних з маршрутизаторів по протоколу Cisco Netflow.

Anomaly Detector і системи статистичного аналізу трафіку призначені для виявлення DDoS атак, а Cisco Guard виступає вже як засіб протидії виявленій атаці. Cisco Guard аналізує трафік з виявленими аномаліями і створює безперервно змінюваний набір фільтрів з перенаправленням на модуль аутентифікації.

Таким чином можливо зробити наступні висновки. До загальних рекомендацій щодо зниження небезпеки і зменшення збитку від атак можливо віднести маскування ip-адреси і конфігурацію функцій антіспуфінга на маршрутизаторах і міжмережних екранах. Ці функції обмежують число напіввідкритих каналів, не дозволяючи перевантажувати систему.

---

[1] кандидат технічних наук, доцент кафедри програмного забезпечення