УДК 004.056

ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЯ DDOS-АТАК.

Фесенко А.І.
Науковий керівник – к.т.н., доц.. Войтович О.П.

Останнім часом спостерігається тенденція до підвищення кількості та потужності атак на інфраструктури обчислювальних мереж. Потужність розподілених атак на відмову в обслуговуванні зросла до рівня понад 100 Гбіт за секунду. Незважаючи на численні дослідження та існуючі підходи до попередження та відбивання атак на відмову в обслуговуванні, питання досліджень в даному напрямку, залишається актуальним.

З ціллю мінімізації наслідків від атак на відмову в обслуговуванні надзвичайно важливими є задачі їх виявлення та ідентифікації. Дана проблема широко розглядалась в різних наукових та практичних роботах. Зокрема, зроблено акцент на малій ефективності сучасних методів виявлення та захисту від низькоактивних розподілених атак на відмову в обслуговуванні. Вказаний клас атак виник відносно недавно і сьогодні становить основну загрозу доступності інформації в розподілених комп'ютерних системах та мережах.

Своєчасне виявлення проведення DDoS-атаки на ресурс є передумовою успішного захисту від неї. Для цього необхідними є актуальність переліку можливих типів атак та глибоке розуміння використовуваних алгоритмів та методів реалізації. Відповідно, на стороні об'єкта захисту повинен бути налаштований моніторинг усіх об'єктів, що потенційно можуть бути атаковані.

Атаки можуть бути виявлені на кількох рівнях: рівні трафіку, рівні операційної системи та на рівні конкретного додатку чи сервісу. Класифікація атак передбачає об'єднання різних типів у групу за певним ключовим критерієм. Наприклад: суб'єкт атаки, вразливість об'єкта, тип атаки, одиниці виміру потужності, мета тощо.

Задачею ідентифікації є аналіз ситуації, що склалась у результаті проведення DDoS-атаки (пост-ідентифікація) або ще під час її проведення (ідентифікація у реальному часі). Варто зазначити, можливість online-ідентифікації можлива лише після збору необхідної статистичної інформації.

Комплексний підхід до захисту має містити такі основні складові як: виявлення факту атаки; класифікація; автоматизація в прийнятті рішень щодо захисту; побудова чи адаптація системи захисту від атаки; попередження та вдосконалення системи захисту на основі попереднього досвіду.