УДК 004.056.53

І.В. Леонтьєв
І.О. Дьогтєва

ВАРІАНТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ УСУНЕННЯ DDOS-АТАК НА ВЕБ-РЕСУРС НА ОСНОВІ ТИМЧАСОВОГО БЛОКУВАННЯ IP-АДРЕС З ПІДВИЩЕНОЮ АКТИВНІСТЮ

Вінницький національний технічний університет

Анотація
Описано варіант розробки програмного забезпечення для усунення DDoS-атак на веб-ресурс, яка враховує сезонні відхилення в навантаженні, що дає можливість виявляти точку початку атаки на ранніх стадіях.
Ключові слова: DDoS-атака, запит, трафік, кластер.

Abstract
Describes a variant of software development to eliminate DDoS-attacks on the web resource, which takes into account seasonal deviations in the load, which makes it possible to identify the starting point of the attack in the early stages.
Keywords: DDoS-attack, query, traffic, cluster.

Вступ

Щорічно різні компанії, що надають послуги в галузі забезпечення інформаційної безпеки і протидії кібератакам, фіксують збільшення кількості DDoS-атаки, їх потужності. Періодичні повідомлення в засобах масової інформації про недоступність тих чи інших ресурсів в результаті розподілених атак, спрямованих на відмову в обслуговуванні, свідчать про неефективність засобів протидії щодо подібних атак. Варто також зазначити, що окрім атак на ресурси провідних IT-корпорацій також збільшується кількість атак на невеликі, «середні» сайти, які до недавнього часу не становили інтересу для зловмисників [1].

Результати дослідження

В рамках запропонованого підходу виявлення DDoS-атак і шкідливого трафіку розроблений алгоритм виявлення на ранніх стадіях точки початку розподіленої атаки, спрямованої на відмову в обслуговуванні. Алгоритм враховує сезонні відхилення в навантаженні, що дає можливість виявляти точку початку атаки з більшою точністю.

Додатково проведено дослідження, яке спрямоване на підтвердження існування сезонності і виявлення типових сезонних періодів. В результаті виявлені тижнева, добова і невизначена сезонність та досліджено причини її виникнення.

Для поділу змішаного трафіку використовується алгоритм кластеризації kmeans. Обгрунтовано вибір даного алгоритму, підтверджено його ефективність. [1]

Для алгоритму підібрані оптимальні характеристики і розмірність даних, вироблені критерії успішності.

Розроблені алгоритми складають основу узагальненого методу виявлення DDoS-атак і шкідливого трафіку, який може бути представлений таким чином: визначаємо існуючі сезонні періоди за допомогою статистичних даних; для кожного сезонного періоду визначаємо допустиму верхню межу кількості запитів; в разі порушення границі, фіксуємо точку початку атаки; відносимо трафік, що передує початку атаки, до кластеру, відповідному легітивному трафіку; за допомогою алгоритму класифікуємо змішаний трафік на легітивний і шкідливий; порівнюємо трафік, що передує початку атаки, з кластером, легітивного трафіку, виділеного зі змішаного трафіку; на підставі результатів, отриманих на попередньому кроці, і з урахуванням вироблених критеріїв успішності, коригуємо

кластери; трафік, що надходить, аналізуємо з урахуванням отриманих в попередньому пункті результатів [2].

На рис. 1 продемонстровані схеми алгоритмів визначення початку атаки та виділення шкідливого трафіку, зокрема, перша схема (рис. 1, а) описує алгоритм виділення шкідливого трафіку, друга (рис. 1, б) і третя (рис. 1, в) — алгоритми визначення початку атаки.

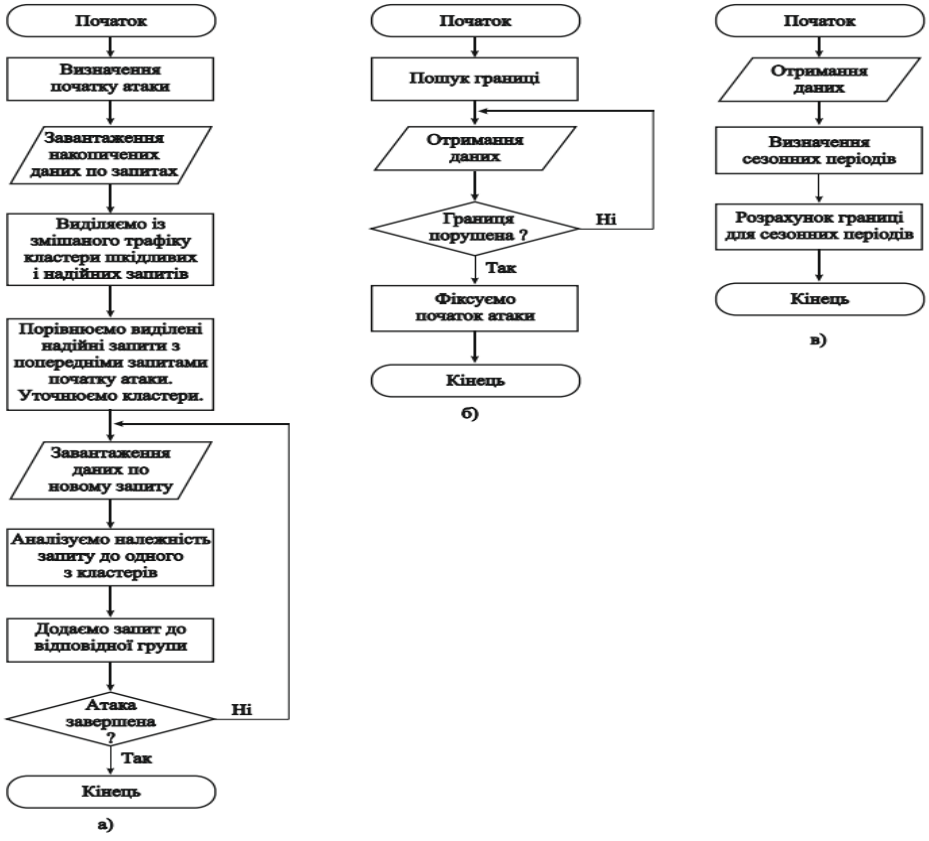

Рисунок 1 - Алгоритм визначення початку атаки та виділення шкідливого трафіку [2]

В алгоритмах на першому кроці відбувається виклик підпрограм виявлення сезонних періодів, розрахнку для них допустимої межі кількості запитів, визначення початку атаки. У разі початку атаки, алгоритм повинен розподілити змішаний трафік на два кластери, один містить шкідливі запити, інший відповідно надійні запити. Далі уточнюються дані кластерів. Потім нові запити аналізуються на належність певному кластеру і за результатами перевірки додаються до нього.

Висновки

У роботі запропонований опис розробки щодо виявлення початку DDoS-атаки і подальшого визначення шкідливих запитів. В основі розробленого методу лежать методи теорії ймовірностей, кластерного і статистичного аналізу, принципи машинного навчання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум : учеб. пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - 2-е изд., стер. - М. : КНОРУС, 2016. - 132 с.

2. Бабаш, А.В. Криптографические методы защиты информации : учебник для студ. вузов / А. В. Бабаш, Е. К. Баранова. - М. : КНОРУС, 2016. - 190 с.

Леонтьєв Ігор Віталійович *— студент факультету менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: leontiev3igor@gmail.com.*

Дьогтєва Ірина Оксентіївна — *асистент кафедри менеджменту та безпеки інформаційних систем, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця.*

Leontiev Igor — *student of the Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: leontiev3igor@gmail.com.*

Dyogteva Iryna - Assistant of the Department of Management and Security of Information Systems, Faculty of

Management and Information Security, Vinnytsia National Technical University, Vinnytsia.

Dohtieva Iryna *— Assistant of the Department of Management and Security of Information Systems, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia.*