УДК 004.732.056

С.Ю. Гавриленко, С.А. Володін

*Національний технічний університет «Харківський політехнічний інститут», Харків*

# АНАЛІЗ АНОМАЛІЙ ТРАФІКУ КОМП'ЮТЕРНОЇ СИСТЕМИ НА ОСНОВІ КОНТРОЛЬНИХ КАРТ

*В роботі досліджено можливість використання контрольних карт EMWA та КУСУМ для аналізу аномалій трафіку комп'ютерної системи. Розроблені адаптивні шаблони фіксації аномальної поведінки комп'ютерної системи. Проведені дослідження показали працездатність системи в умовах як короткострокової так і довгострокової DOS-атаки.*

***Ключові слова**: контрольні карти EMWA, контрольні карти КУСУМ, комп'ютерні системи, аномалії трафіку.*

## Вступ

**Постановка проблеми і аналіз літератури.** Мережеві технології стали невід'ємною частиною життєдіяльності сучасного суспільства. Одною з причин, які впливають на ефективність роботи обчислювальної мережі є аномалії трафіку. Аномалії трафіку можуть бути викликані несправністю мережевого обладнання, випадковими чи навмисними діями зі сторони користувачів, невірною роботою програм, діями зловмисників та ін [1].

Одним із найпоширеніших методів нападу на комп'ютерну систему є DoS-атака – напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам.

Найпоширенішим методом нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (DDoS атакою [2]. Таким чином атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним [3]. Особливістю даного виду комп'ютерного злочину є те, що зловмисники не ставлять метою незаконне проникнення до захищеної комп'ютерної системи з ціллю крадіжки чи знищення інформації. Вони блокують роботу серверу, а вже потім виставляють свої вимоги до власників. DDos-атаки є одним із видів віртуального тероризму [4]. Аналіз літератури показав [1-6], що на даний момент існує безліч як апаратно-програмних засобів захисту, так і організаційних методів протистояння, але повністю захиститися від DDoS-атак на сьогоднішній день неможливо [3].

Відомо, що для виявлення аномалій в управлінні виробництвом, бізнес-процесами широко використовують статистичний контроль на основі контрольних карт [7-11]. Причина проста – це відносно доступний спосіб збору та аналізу даних в реальному часі, який, крім того, ще й дає можливість приймати, на основі отриманих результатів, негайні коригуючі і / або превентивні заходи. Контрольні карти мають ряд переваг. Зокрема, вони дають можливість візуально визначити момент зміни процесу, створюють основу для поліпшення процесу, виявляють відмінності між випадковими і системними порушеннями в процесі, знижують втрати за рахунок запобігання появи дефектів.

**Метою статті** є дослідження аномалій трафіку комп'ютерної системи за допомогою контрольних карт на прикладі DDoS-атак.

## Основна частина

Для проведення аналізу трафіку комп'ютерної системи на наявність помилок та аномалій було обрано карти EMWA (контрольна карта експоненціально-зваженого ковзного середнього) та КУСУМ-карти (контрольна карта накопичених сум).

КУСУМ-карти є одним з поширених статистичних методів виявлення зміни показника процесу та встановлення причин цієї зміни [8].

Значення кумулятивних сум $C_i$ відкладають на осі де наступне спостереження призводить до різниці значення спостережуваної змінної і опорного значення. Значення різниць підсумовують, утворюючи кумулятивні суми $C_i$ за формулою:

$$C_i = \sum_{i=1}^{n} (X_i - T), \qquad (1)$$

де $X_i$ – значення спостережуваної змінної; T – опорне (або цільове) значення; n – кількість спостережень; i – номер вибірки.

Опорне значення T встановлюють залежно від конкретної ситуації і від типу даних, з якими необхідно працювати. Найчастіше за T приймають цільовий рівень спостережуваної змінної (еталонне значення), або середній рівень показника змінної, розрахований по попередній серії даних, отриманій при роботі стабільного процесу.

EWMA (Exponentially Weighted Moving Averages) карта є графічним зображенням експонентіального зваженого ковзного середнього значення. Центральна лінія EWMA-карти розраховується як середнє арифметичне спостережуваної змінної (2):

$$\mu = \sum_{i=1}^{n} X_i \Big/ n, \qquad (2)$$

де μ – значення центральної лінії, $X_i$ – значення спостережуваної змінної, n – кількість спостережень.

Класичний розрахунок середньої лінії бере до уваги всі спостереження. Однак, в деяких випадках, для обчислення центральної лінії і лімітів, приймають тільки певну кількість останніх (або попередніх) результатів. Розрахункове значення карти обчислюють таким чином:

$$Z_i = \lambda X_i + (1 - \lambda) \cdot Z_{i-1}, \qquad (3)$$

де $Z_i$ – розрахункове значення, λ – фактор згладжування, $X_i$ – спостережуване значення або середнє арифметичне групи спостережуваних значень (вибірки), а $Z_{i-1}$ – попереднє розрахункове значення.

Наявність розрахункового значення передбачає відміну величин, що відкладаються на карті, від результатів спостережень. Проте, це значення тісно пов'язане зі спостереженням, а його відміну покликане згладити природну варіацію процесу. Розрахунок контрольних меж карти виконуються таким чином:

$$CL = \mu \pm \frac{s}{\sqrt{n}} \sqrt{\frac{\lambda}{2-\lambda} \cdot \left[1 - (1-\lambda)^{2i}\right]}, \qquad (4)$$

Однією з відмінних рис EWMA карт є їх гнучкість, що дає можливість використовувати їх для контролю різних процесів, аналізувати дані в випадках не рівних вибірок і т.д. Це вимагає від дослідника певних навичок і додаткових знань в області статистики [11]. При моніторингу та управлінні процесом карти КУСУМ та EWMA допомагають вирішувати два завдання [8]: виявлення значимих зрушень (змін) процесу за рахунок виходу за контрольні межі карти ; - визначення точок їх виникнення.

Для проведення експерименту з урахуванням можливостей мови програмування C# була розроблена програмна модель проведення DoS-атаки. Для проведення аналізу було використано віртуальну машину за допомогою програми VirtualBox від компанії Oracle. В якості вхідних даних використовувалась загрузка мережевої карти (кількість запитів за секунду). Результати нормальної роботи системи наведені на рис. 1, 2. Як видно із рисунків значення загрузки мережевої карти комп'ютерної системи знаходиться в межах контрольних ліній. На рис. 3, 4 наведені результати короткострокової атаки. Атака тривала усього 2 секунди і розпочалася на 16 секунді. Контрольні карти це зафіксували: на 16-й секунді показник стрімко злетів вгору. Пік атаки зафіксовано на 17-й секунді. Після припинення DOS-атаки значення карти КУСУМ залишалося за межами контрольної лінії. Значення карти EWMA через деякий час повернулося в межі контрольних ліній.

Довгострокова атака, тривалістю 15 сек, розпочалася на 16 секунді. До початку атаки система функціонувала у штатному режимі (близько 500-700 запитів за секунду), після початку атаки кількість

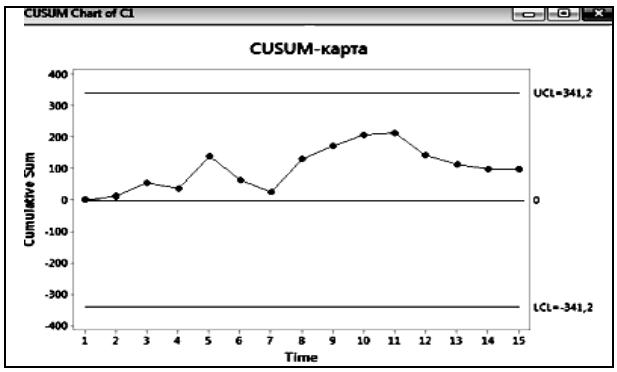


Рис. 1. КУСУМ карта
для нормальної роботи системи

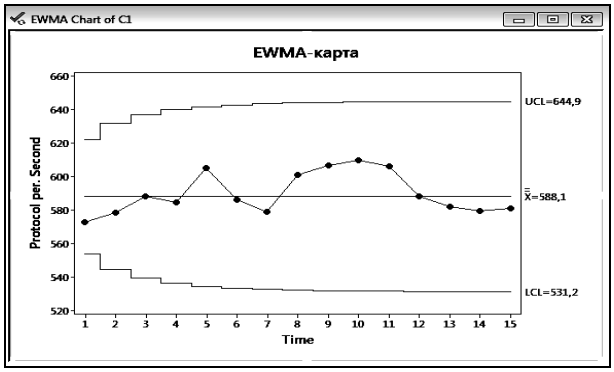


Рис. 2. EWMA карта
для нормальної роботи системи

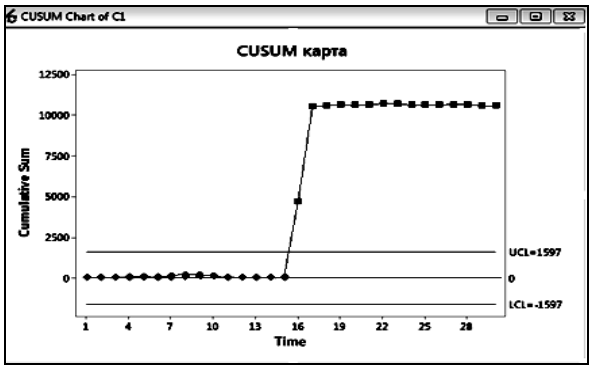


Рис. 3. КУСУМ карта
при короткостроковій за часом атаці

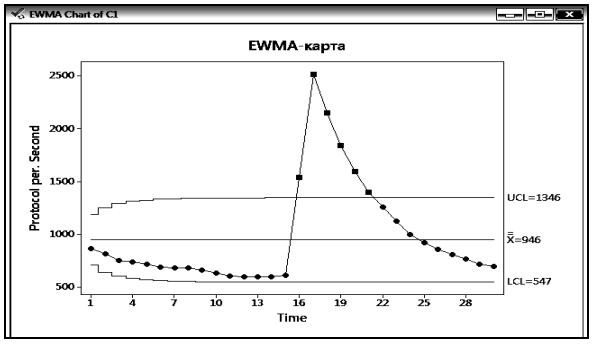


Рис. 4. EWMA-карта
при короткостроковій за часом атаці

запитів зросла до 6500. Контрольні карти зафіксували вихід системи за контрольні межі. Результати атаки наведені на рис. 5, 6.

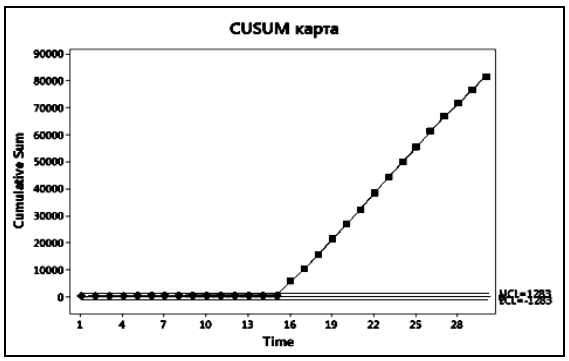


Рис. 5. КУСУМ карта
при довгостроковій за часом атаці

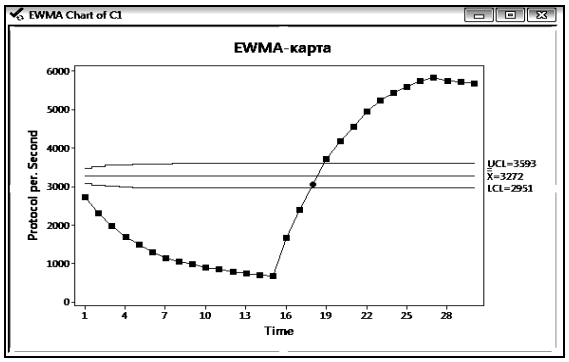


Рис. 6. Карта EWMA
при довгостроковій за часом атаці

## Висновки

В роботі досліджено можливість використання контрольних карт EMWA та КУСУМ для аналізу аномалій трафіку комп'ютерної системи. Для ідентифікації стану комп'ютерної системи в умовах DOS-атаки була розроблена імітаційна модель.

Експериментальні дослідження показали:

– короткострокова за часом DoS-атака на комп'ютерну систему призводить до виходу графіка за контрольні межі для карт КУСУМ та EMWA. Після закінчення короткострокової вірусної атаки графік повертається в межі для карти EMWA;

– довгострокова за часом DoS-атака на комп'ютерну систему призводить до виходу графіка за контрольні межі карт КУСУМ та EMWA та до зміни кута нахилу графіка так званих «локальних середніх», що визначається за послідовним точкам для карт КУСУМ.

Отримані результати досліджень дозволяють зробити висновок про можливість використання розроблених шаблонів фіксації аномальної поведінки комп'ютерних систем на основі контрольних карт EMWA та КУСУМ в евристичних аналізаторах систем виявлення вторгнень в комп'ютерні системи.

## Список літератури

*1. Статистика глобальної мережевої активності [Електронний ресурс]. – Режим доступу: http://atlas.arbor.net/summary/attacks.*

*2. Лукацкий А.В. Обнаружение атак / А.В. Лукацкий. – Спб: BXB-Петербург, 2001. – 624 с.*

*3. Семенов. С.Г. Защита данных в компьютеризированных управляющих системах (монография) / С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко.– «LAP LAMBERT ACADEMIC PUBLISHING» Германия, 2014.– 236 с.*

*4. DDoS and Security Reports:The Arbor Networks Security Blog. [Електронний ресурс]. –Режим доступу: http://www.arbornetworks.com/.*

*5. Сайт Лабораторії Касперського [Електр. ресурс]. – Режим доступу: http://www.securelist.com/ru/analysis.*

*6. Касперский К. Записки исследователя компьютерных вирусов. / К. Касперский. – СПб.: Питер, 2006. – 316 с.*

*7. Шелухин О.И. Обнаружение вторжений в компьютерные сети / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. – М.: Гарячая линия-Телеком, 2013. – 220 с*

*8. Общие сведения о картах кумулятивных сумм. [Электронный ресурс]. – Режим доступу: http://www.uran.donetsk.ua/~masters/2011/fimm/merkulov/ library/translate.htm./*

*9. Карты контроля качества. [Електронний ресурс]. – Режим доступу: http://www.statsoft.ru/home/textbook/modules/stquacon.html.*

*10. Контрольные карты [Электронной ресурс]. – Режим доступу: http://standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1…*

*11. Контрольные карты экспоненциально взвешенного скользящего среднего. [Електронний ресурс]. – Режим доступу: http://sixsigmaonline.ru/load/22-1-0-236*

*.Надійшла до редколегії 26.02.2016*

**Рецензент***:* д-р техн. наук, с.н.с. С.Г. Семенов Національний технічний університет «ХПІ», Харків.

### АНАЛИЗ АНОМАЛИЙ ТРАФИКА КОМПЬЮТЕРНОЙ СИСТЕМЫ НА ОСНОВЕ КОНТРОЛЬНЫХ КАРТ

С.Ю. Гавриленко, С.А. Володин

*В работе исследована возможность использования контрольных карт EMWA и КУСУМ для анализа аномалий трафика компьютерной системы. Разработаны адаптивные шаблоны фиксации аномального поведения компьютерной системы. Проведенные исследования показали работоспособность системы в условиях как краткосрочной так и долгосрочной DOS-атаки.*

***Ключевые слова:*** *контрольные карты EMWA, контрольные карты КУСУМ, компьютерные системы, аномалии трафика.*

### AN ANALYSIS OF THE COMPUTER SYSTEM TRAFFIC ANOMALIES BASED ON CONTROL CARDS

S.Yu. Gavrilenko, S.A. Volodin

*In this work are represented the possibility of using control card EMWA and CUSUM for analyzing traffic anomalies of computer system . The adaptive templates for the anomalous behavior of the computer system were developed. Studies have shown the system performance under both short-term and long-DOS-attack.,*

***Keywords:*** *control card EMWA, control cards CUSUM, computer systems, traffic anomalies.*