UDC 004.732.056 DOI: 10.30748/soi.2019.157.15

S. Gavrilenko

National Technical University "Kharkiv Polytechnic Institute", Kharkiv

DEVELOPMENT OF IDENTIFICATION TEMPLATES OF ANOMAL COMPUTER SYSTEMS STATUS BASED ON CONTROL CHARTS

The purpose of the article is to propose a method for identifying the state of the computer system based on EWMA control charts and CUSUM charts. The software for construction of templates for fixing abnormal state of a computer system on the basis of traffic analysis was developed. The testing was conducted in the conditions of long-term and short-term DOS-attack, which showed the system efficiency. It was found that the system's operation returns to the limit of both maps in the conditions of a short-term attack. The analysis of the obtained results showed that developed express methods based on control charts increased the reliability of making decision on the state of computer system to 10%.

***Keywords**: computer systems of critical use, state identification, EWMA and CUSUM control charts, traffic anomalies.*

Introduction

Formulation of the problem. One of the key roles of the safe life of modern society is computer systems critical use, as a component of the most important areas of the state.

During the experiments, we showed that there is no general approach to solving the problem of detecting abnormal situations in the process of operation of such systems. However, in the context of the rapid development of information technology and as a consequence of the continuous upgrading of software and hardware of computer systems critical use, solving private problems detection of anomalies cannot provide system security.

A more universal and, at the same time, scientifically grounded approach to the identification of the states of the computer system is needed.

One of the reasons that affect the efficiency of a computer network is traffic anomaly. Traffic anomalies can be caused by malfunction of network equipment, accidental or intentional actions of users, improper work of programs, actions of intruders, etc. [1].

One of the most common methods of attacking a computer system (CS) is a DoS attack. The DoS attack is the attack on a computer system with the intent of making computer resources inaccessible to users for whom a computer system has been designated. The most common method of attack is the saturation of the attacked computer or network equipment with a large number of external queries. As a result, the attacked equipment cannot respond to users or it responds so slowly that it becomes inaccessible [2].

If an attack occurs simultaneously with a large number of IP addresses, it is called distributed (Distributed Denial-of-Service – DDoS) [3].

The peculiarity of this type of computer crime is that the intruders do not attempt to illegally penetrate into a secure computer system for the purpose of theft or destruction of information. They block the work of the server, and then post their claims to the owners. DDos-attacks are one of the types of virtual terrorism [4].

The analysis of literature has shown [5] that there are many hardware and software protection tools now, as well as organizational methods of confrontation, but it is impossible to completely defend against DDoS attacks [6].

It is known that for the detection of anomalies in production management and business processes, statistical control based on control charts are widely used [7]. The reason is simple - it is an accessible way of collecting and analyzing data in real time, which, in addition, also allows them to take immediate corrective and/or preventive measures based on the obtained results. Control charts have a number of benefits. In particular, they provide an opportunity to visually identify the moment of change in the process, create the basis for improving the process, identify the differences between random and systemic offences in the process, and reduce losses through the prevention of defects.

The disadvantages of control charts include higher requirements for staff training and the need for work in real time.

The purpose of this article is to study the anomalies of computer system traffic based on control charts on the example of DDoS attacks.

Principles of control charts functioning

To analyze the traffic of the computer system for errors and anomalies, the EMWA (control chart of the exponentially-weighted moving average) and CUSUM-charts (the control chart of accumulated amounts) were selected.

CUSUM-charts are one of the most common statistical methods for detecting changes in the quality indicator and identifying the causes of this change [8–12].

The values of accumulated sums C_i are deposited on the axis where the next observation leads to a difference in the value of the observed variable and the supporting value. The values of the differences are summed up, forming the cumulative sums of C_i and by the formula:

$$C_i = \sum_{r=1}^{i} (y_r - T), \quad (1)$$

where y_r – a value of the observed variable; T – reference (or target) value; i – the sample number.

The reference value T is set depending on the particular situation and the type of data that you must work with.

More often, the target level of the quality indicator (reference value) or the average level of quality, calculated on the previous series of data obtained during the stable process, is adopted as T [13–14].

While monitoring and process control, CUSUM helps to solve two problems [15–17]:

– identification of significant changes (changes) of the process from the target level;

– determining the points of their occurrence.

EWMA (Exponentially Weighted Moving Averages) chart is a graphic representation of an exponential weighted moving average.

The middle line of the EWMA chart is calculated as the arithmetic average of observations:

$$\mu = \frac{\sum_{i=1}^{n} x_i}{n}, \quad (2)$$

where μ – the middle line value; x_i – is the observable value, n – the number of observations

The classical calculation of the middle line takes into account all observations. However, in some cases, for the calculation of the middle line and the limits, a certain number of recent (or previous) results are only accepted.

The estimated value (the value deposited on the chart) is calculated as follows:

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

where Z_i – estimated value, λ – smoothing factor, X_i – observed value or average arithmetic group of observed values (sampling); Z_{i-1} – previous estimated value.

The presence of the estimated value involves the abolition of the values deposited on the chart, from the results of observations.

However, this value is closely related to observation, and its elimination is intended to smooth the natural variation of the process.

Calculation of chart limits:

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

One of the great features of EWMA charts is their flexibility, which makes it possible to use them to control various processes, analyze data in cases of non-even samples, etc. The researcher is required to have certain skills and additional knowledge in the field of statistics [18].

Experiment results

To conduct an experiment based on the capabilities of the C# programming language, a software model for DDOS attack was developed. For analysis, a virtual machine was created using Oracle's VirtualBox program.

Experiment results for normal system work are given on fig. 1–2.

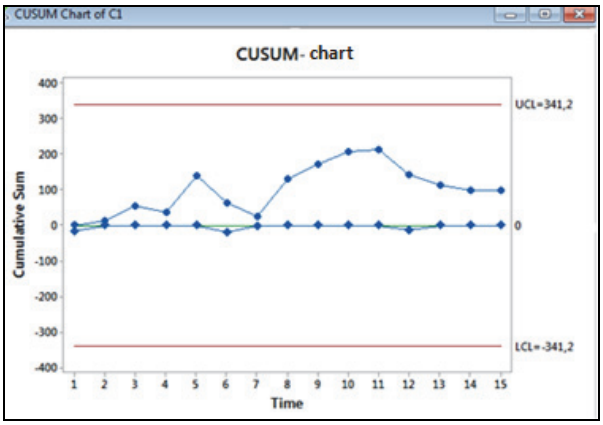

Fig. 1. CUSUM chart for normal system work

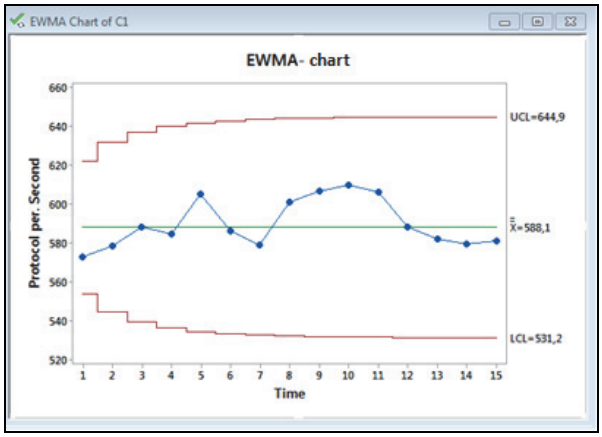

Fig. 2. EWMA chart for normal system work

The attack lasted only 2 seconds, but the control chart fixed it: at the 16th second the indicator shoot up. The peak of the attack was fixed at 17th second. After termination of a DOS attack, the system returned to equilibrium after some time. The results of the attack are shown in fig. 3–4 (long-term attack, lasting 15 seconds, began at 16 seconds).

Before the attack, the system functioned in normal mode (about 500–700 requests per second), after the attack began, the number of requests increased to 6500. The results of the attack are shown in fig. 5–6.

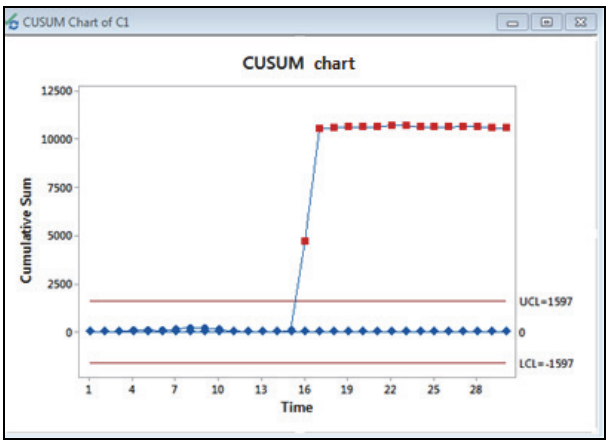

Fig. 3. CUSUM chart with short-term attack

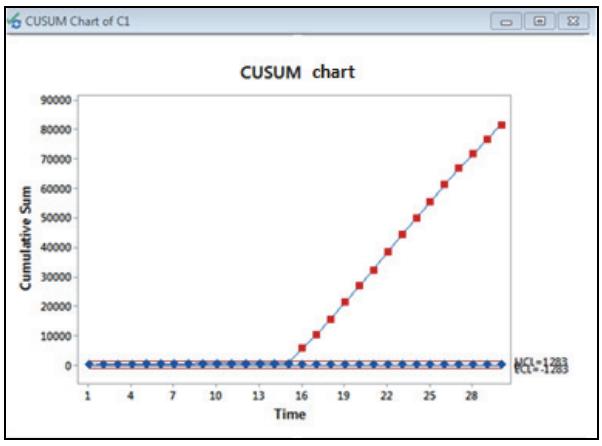

Fig. 5. CUSUM chart with long-term attack

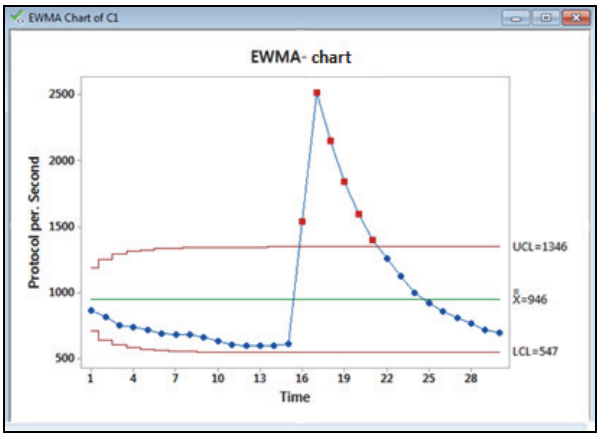

Fig. 4. EWMA chart with short-term attack

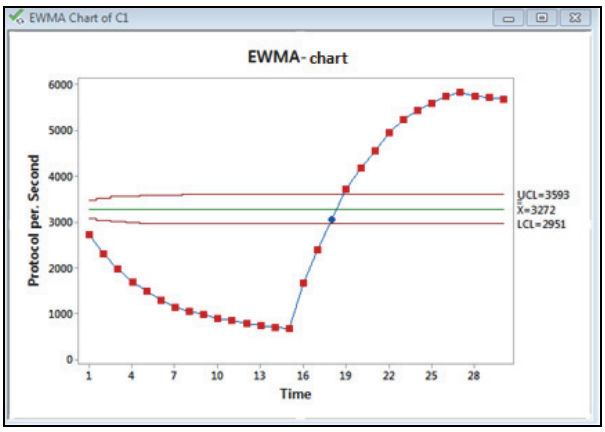

Fig. 6. EWMA chart with long-term attack

Conclusions

The analysis of anomalies of traffic of a computer system based on control charts was investigated.

To identify the state of the computer system in a Denial-of-Service DoS attack, an imitation model was developed, with its input data being the number of requests per second.

Experimental studies have shown:

– the short-term impact of viruses on the computer system leads to the outrun of the diagram at the control limits for CUSUM and EMWA; after the short-term viral attack, the diagram returns to the limit for both charts;

– the long-term effects of viruses on a computer system leads to a change in the angle of inclination of the so-called “local mean” diagram, which is determined by successive points for the CUSUM and EMWA charts or the outrun of the diagram at the control limits of the CUSUM and EMWA charts.

The developed templates allowed to increase the accuracy of the identification of the state of the computer system by 10% and can be used as express methods of assessment of the state.

Список літератури

1. Kuchuk G.A. An Approach To Development Of Complex Metric For Multiservice Network Security Assessment / G.A. Kuchuk, A.A. Kovalenko, A.A. Mozhaev // Statistical Methods Of Signal and Data Processing (SMSDP – 2010): Proc. Int. Conf., October 13-14, 2010. – Kiev: NAU, RED, IEEE Ukraine section joint SP, 2010. – P. 158-160.

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

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

4. Ruban I. Redistribution of base stations load in mobile communication networks / I. Ruban, H. Kuchuk, A. Kovalenko // Innovative technologies and scientific solutions for industries. – 2017. – No. 1 (1). – P. 75-81. https://doi.org/10.30837/2522-9818.2017.1.075.

5. Kuchuk G. Two-stage optimization of resource allocation for hybrid cloud data store / G. Kuchuk, S. Nechausov, V. Kharchenko // International Conference on Information and Digital Technologies. – Zilina, 2015. – P. 266-271. http://dx.doi.org/10.1109/DT.2015.7222982.

6. Семенов С.Г. Защита данных в компьютеризированных управляющих системах: монография / С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко. – Германия : LAP LAMBERT ACADEMIC PUBLISHING, 2014. – 236 с.

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

8. ГОСТ Р ИСО 7870-3-2013. Контрольные карты [Електронний ресурс]. – Режим доступу: http://standartgost.ru/g/%D0%93% D0%9E%D0%A1%D0%A2_%D0%A0_%D0%98%D0%A1%D0%9E_7870-2-2013.

9. Detection And Removal Of Black Hole Attack In Mobile Ad Hoc Networks Using Grp Protocol / M. Amin Salih, D. Yuvaraj, M. Sivaram, V. Porkodi // International Journal of Advanced Research in Computer Science. – 2018. – Vol. 9, No 6. – P. 1-6. http://dx.doi.org/10.26483/ijarcs.v9i6.6335.

10. Amin Salih M. A Method for Compensation of TCP Throughput Degrading During Movement Of Mobile Node / M. Amin Salih, M.Y. Potrus // ZANCO Journal of Pure and Applied Sciences. – 2015. – Vol. 27, No 6. – P. 59-68.

11. Gomathi B. Epsilon-Fuzzy Dominance Sort Based Composite Discrete Artificial Bee Colony optimization for Multi-Objective Cloud Task Scheduling Problem / B. Gomathi, N.K. Karthikeyan, B. Saravana Balaji // International Journal of Business Intelligence and Data Mining. – 2018. – Vol. 13, Issue 1–3. – P. 247-266. https://doi.org/10.1504/IJBIDM.2018.088435.

12. Optimized Secure Scan Flip Flop to Thwart Side Channel Attack in Crypto-Chip / S. Saravanan, M. Hailu, G.M. Gouse, M. Lavanya, R. Vijaysai // International Conference on Advances of Science and Technology, ICAST 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. – Vol 274. – Springer, Cham. https://doi.org/10.1007/978-3-030-15357-1_34.

13. Statistical Score Calculation of Information Retrieval Systems using Data Fusion Technique / B. Dhivakar, S.V. Saravanan, M. Sivaram, R.A. Krishnan // Computer Science and Engineering. – 2012. – Vol. 2, Issue 5. – P. 43-45. https://doi.org/10.5923/j.computer.20120205.01.

14. Коваленко А.А. Методи синтезу інформаційної та технічної структур системи управління об'єктом критичного застосування / А.А. Коваленко, Г.А. Кучук // Сучасні інформаційні системи. – 2018. – Т. 2, № 1. – С. 22-27.

15. Кучук Г.А. Метод оценки характеристик АТМ-трафика / Г.А. Кучук // Інформаційно-керуючі системи на залізничному транспорті.– 2003. – № 6. – С. 44-48.

16. Свиридов А.С. Метод перерозподілу пропускної здатності критичної ділянки мережі на основі удосконалення ON/OFF-моделі трафіку / А.С. Свиридов, А.А. Коваленко, Г.А. Кучук // Сучасні інформаційні системи. – 2018. – Т. 2, № 2. – С. 139-144.

17. Privacy Preserving Data Mining Using Threshold Based Fuzzy cmeans Clustering / V. Manikandan, V. Porkodi, A.S. Mohammed, M. Sivaram // ICTACT Journal on Soft Computing. – 2018. – Vol. 9, Is. 1. – P. 1813-1816. https://doi.org/10.21917/ijsc.2018.0252.

18. Survey on White-Box Attacks and Solutions / V. Porkodi, M. Sivaram, A.S. Mohammed, V. Manikandan // Asian Journal of Computer Science and Technology. 2018. – Vol. 7, Is. 3. – P. 28-32.

References

1. Kuchuk, G.A., Kovalenko, A.A. and Mozhaev, A.A. (2010), An Approach To Development Of Complex Metric For Multiservice Network Security Assessment, *Statistical Methods Of Signal and Data Processing (SMSDP – 2010)*, Proc. Int. Conf., October 13-14, 2010, NAU, RED, IEEE Ukraine section joint SP, Kyiv, pp. 158-160.

2. Shelukhin, O.I., Sakalema, D.J. and Filinova, A.S. (2013), "*Obnaruzhenye vtorzhenyj v kompjjuternye sety*" [*Intrusion Detection in Computer Networks*], Hotline Telecom, Moscow, 220 p.

3. Lukatskii, A.V. (2001), "*Obnaruzhenye atak*" [*Intrusion Detection*], HCS-Petersburg, St. Petersburg, 624 p.

4. Ruban, I., Kuchuk, H. and Kovalenko, A. (2017), Redistribution of base stations load in mobile communication networks, *Innovative technologies and scientific solutions for industries*, No. 1(1), pp. 75-81: https://doi.org/10.30837/2522-9818.2017.1.075.

5. Kuchuk, G., Nechausov, S. and Kharchenko, V. (2015), Two-stage optimization of resource allocation for hybrid cloud data store, *International Conference on Information and Digital Technologies*, Zilina, pp. 266-271. http://dx.doi.org/10.1109/DT.2015.7222982.

6. Semenov, S.G., Davydov, V.V. and Gavrilenko, S.Y. (2014), "*Zashhyta dannykh v kompjjuteryzyrovannykh upravljajushhykh systemakh*" [*Data protection in computerized control systems*], LAP LAMBERT ACADEMIC PUBLISHING, Germany, 236 p.

7. Oleshko, V. (2013), "*Kontroljnye karty eksponencyaljno vzveshennogho skoljzjashhegho srednegho*" [*Control Charts of exponentially weighted moving average*], available at: www.sixsigmaonline.ru/load/22-1-0-236.

8. GOST R ISO 7870-3-201 (2013), "*Kontroljnye karty*" [*Control Charts*], available at: www.standartgost.ru/g/%D0%93%D0%9E%D0%A1%D0%A2 %D0%A0 %D0%98%D0%A1%D0%9E 7870-2-2013.

9. Amin Salih, M., Yuvaraj, D., Sivaram, M. and Porkodi, V. (2018), Detection And Removal Of Black Hole Attack In Mobile Ad Hoc Networks Using Grp Protocol, *International Journal of Advanced Research in Computer Science*, Vol. 9, No. 6, pp. 1-6. http://dx.doi.org/10.26483/ijarcs.v9i6.6335.

10. Amin Salih, M. and Potrus, M.Y. (2015), A Method for Compensation of Tcp Throughput Degrading During Movement Of Mobile Node, *ZANCO Journal of Pure and Applied Sciences*, Vol. 27, No. 6, pp. 59-68.

11. Gomathi, B., Karthikeyan, N.K. and Saravana, Balaji B. (2018), Epsilon-Fuzzy Dominance Sort Based Composite Discrete Artificial Bee Colony optimization for Multi-Objective Cloud Task Scheduling Problem, *International Journal of Business Intelligence and Data Mining*, Vol. 13, Issue 1-3, pp. 247-266. https://doi.org/10.1504/IJBIDM.2018.088435.

12. Saravanan, S., Hailu, M., Gouse, G.M., Lavanya, M. and Vijaysai, R. (2019), Optimized Secure Scan Flip Flop to Thwart Side Channel Attack in Crypto-Chip, *International Conference on Advances of Science and Technology*, ICAST 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 274, Springer, Cham. https://doi.org/10.1007/978-3-030-15357-1_34.

13. Dhivakar, B., Saravanan, S.V., Sivaram, M. and Krishnan, R.A. (2012), Statistical Score Calculation of Information Retrieval Systems using Data Fusion Technique, *Computer Science and Engineering*, Vol. 2, Issue 5, pp 43-45. https://doi.org/10.5923/j.computer.20120205.01.

14. Kovalenko, A. and Kuchuk, H. (2018), “Metody syntezu informacijnoji ta tekhnichnoji struktur systemy upravlinnja ob'jektom krytychnogho zastosuvannja” [Methods for synthesis of informational and technical structures of critical application object’s control system], *Advanced Information Systems*, Vol. 2, No. 1, pp. 22-27.

15. Kuchuk, G.A. (2003), “Metod ocenky kharakterystyk ATM-trafyka” [Method of estimation of characteristics of ATM traffic], *Information and control systems in the railway transport*, No. 6, pp. 44-48.

16. Sviridov, A., Kovalenko, A. and Kuchuk, H. (2018), “Metod pererozpodilu propusknoji zdatnosti krytychnoji diljanky merezhi na osnovi udoskonalennja ON/OFF-modeli trafiku” [The pass-through capacity redevelopment method of net critical section based on improvement ON/OFF models of traffic], *Advanced Information Systems*, Vol. 2, No. 2, pp. 139-144.

17. Manikandan, V., Porkodi, V., Mohammed, A.S. and Sivaram, M. (2018), Privacy Preserving Data Mining Using Threshold Based Fuzzy cmeans Clustering, *ICTACT Journal on Soft Computing*, Vol. 9, Issue 1, pp.1813-1816. https://doi.org/10.21917/ijsc.2018.0252.

18. Porkodi, V., Sivaram, M., Mohammed, A.S. and Manikandan, V. (2018), Survey on White-Box Attacks and Solutions, *Asian Journal of Computer Science and Technology*, Vol. 7, Issue 3, pp. 28-32.

Received by Editorial Board 21.03.2019
Signed for Printing 23.04.2019

Відомості про автора:

Гавриленко Світлана Юріївна
кандидат технічних наук доцент доцент кафедри
Національного технічного університету
“Харківський політехнічний інститут”,
Харків, Україна
https://orcid.org/0000-0002-6919-0055

Information about the author:

Svitlana Gavrylenko
Candidate of Technical Sciences Associate Professor
Senior Lecturer of National Technical University
“Kharkiv Polytechnic Institute”,
Kharkiv, Ukraine
https://orcid.org/0000-0002-6919-0055

РОЗРОБКА ШАБЛОНІВ ІДЕНТИФІКАЦІЇ АНОМАЛЬНОГО СТАНУ КОМП’ЮТЕРНОЇ СИСТЕМИ НА ОСНОВІ КОНТРОЛЬНИХ КАРТ

С.Ю. Гавриленко

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. Відомо, що для виявлення аномалій в управлінні виробництвом, бізнес-процесами широко використовують статистичний контроль на основі контрольних карт. 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. До недоліків контрольних карт можна віднести більш високі вимоги до підготовки персоналу та необхідність роботи в реальному часі. Метою статті є дослідження аномалій трафіка комп'ютерної системи на основі контрольних карт на прикладі DDoS-атак. В роботі запропоновано метод ідентифікації стану комп’ютерної системи на основі контрольних карт EWMA та КУСУМ карт. Розроблено програмне забезпечення для побудови шаблонів фіксації аномальної стану комп’ютерної системи на основі аналізу трафіка. Проведено тестування в умовах довгострокової та короткострокової атаки DOS-атаки, яке показало працездатність системи. Отримано, що в умовах короткострокової атаки, функціонування системи повертається в межі обох карт.

Експериментальні дослідження показали: короткостроковий вплив вірусів 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 обох карт; довгостроковий вплив вірусів на комп'ютерну систему призводить до зміни кута нахилу графіка так званих “локальних середніх”, що визначається за послідовним точкам для карт КУСУМ та EMWA або вихід графіка за контрольні межі карт КУСУМ та EMWA. Аналіз отриманих результатів показав, що розроблені експрес методи на основі контрольних карт підвищили достовірність прийняття рішень про стан КС до 10%.

Ключові слова: *комп’ютерні системи критичного застосування, ідентифікація стану, контрольні карти EWMA та КУСУМ, аномалії трафіка.*

РАЗРАБОТКА ШАБЛОНОВ ИДЕНТИФИКАЦИИ АНОМАЛЬНОГО СОСТОЯНИЯ КОМПЬЮТЕРНОЙ СИСТЕМЫ НА ОСНОВЕ КОНТРОЛЬНЫХ КАРТ

С.Ю. Гавриленко

В работе предложен метод идентификации состояния компьютерной системы на основе контрольных карт EWMA и КУСУМ карт. Разработано программное обеспечение для построения шаблонов фиксации аномального состояния компьютерной системы на основе анализа трафика. Проведено тестирование в условиях долгосрочной и краткосрочной атаки DOS-атаки, которое показали работоспособность системы. Получено, что в условиях краткосрочной атаки, функционирования системы возвращается в пределы обеих карт. Анализ полученных результатов показал, что разработанные экспресс-методы на основе контрольных карт повысили достоверность принятия решений о состоянии КС до 10%.

Ключевые слова: *компьютерные системы критического применения, идентификация состояния, контрольные карты EWMA и КУСУМ, аномалии трафика.*