UOT 004.056

***İmamverdiyev Y.N.*[1]*, Nəbiyev B.R.*[2]**
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]yadigar@lan.ab.az, [2]babek@iit.ab.az

İNFORMASİYA TƏHLÜKƏSİZLİYİNİN MONİTORİNQİ SİSTEMLƏRİ ÜÇÜN KÜTLƏVİ XİDMƏT MODELLƏRİ

İnformasiya təhlükəsizliyinin idarə edilməsi sistemlərində informasiya təhlükəsizliyi hadisələrinin emalı proseslərinin modelləşdirilməsi üçün kütləvi xidmət modeli təklif edilir. İnformasiya təhlükəsizliyi hadisələrinin emalı prosesi qarışıq prioritetli xidmət qaydası ilə işləyən M/G/1 modeli ilə təsvir edilir və üç prioritet sinfi – mütləq, nisbi və prioritetsiz xidmət rejimləri üçün orta gözləmə müddətlərinin analitik ifadələri verilir. Alınmış ehtimal xarakteristikaları əsasında informasiya təhlükəsizliyi hadisələrinin emalı üzrə fəaliyyətin effektivliyini qiymətləndirmək üçün cərimə funksiyaları daxil edilməklə model də təklif edilir.

Açar sözlər: *informasiya təhlükəsizliyi, informasiya təhlükəsizliyi hadisələri, şəbəkə trafiki, monitorinq, kütləvi xidmət nəzəriyyəsi, prioritetli emal.*

Giriş

Qloballaşan dünyada informasiya texnologiyaları sürətlə inkşaf etdikcə, yeni şəbəkə avadanlıqları və trafikdə axan kontent növləri çoxaldıqca, korporativ şəbəkənin (KŞ) idarə edilməsi prosesi həm çətin, həm də maliyyə cəhətdən bahalı prosesə çevrilir. Bunun səbəblərini monitorinq mexanizmləri və nəzarətə ehtiyac duyan obyeklərin çoxalması ilə monitorinq prosesinin külli miqdarda hesablama gücü tələb etməsilə izah etmək olar və bu da KŞ-nın iş prosesinə xələl gətirir. KŞ-da monitorinqin əsas məqsədi şəbəkənin fəaliyyətinin faziləsizliyinin, korporativ informasiyanın tamlığının və konfidensiallığının təmin edilməsidir. Bunun üçün ümumiləşdirilmiş formada trafikin axınına nəzarət edərək, insidentlərin aşkarlanması prosesi aparılır. Bu prosesin idarə olunması və ayrılmış büdcə daxilində görülərək maksimal dərəcədə təhlüksizliyin təmin olunması üçün informasiya təhlükəsizliyi xidməti (İTX) işinin effektivliyinin artırılması nəzərdə tutulur.

İnformasiya təhlükəsizliyinin monitorinqi KŞ-da informasiya təhlükəsizliyinin vəziyyəti barədə real zaman rejimində həqiqi məlumat əldə edilməsinə, vəziyyətin qiymətləndirilməsinə, aşkarlanan kiberhücumların və digər insidentlərin minimal xərclərlə və qisa müddətə aradan qaldırılmasına xidmət edir. Bu baxımdan monitorinq informasiya təhlükəsizliyinin təmin edilməsində aparıcı rol oynayır və İTX-nin bu istiqamətdə işinin effektiv təşkil edilməsi olduqca aktualdır.

Analiz göstərir ki, İTX-nin qarşısına çıxan əsas məsələ informasiya təhlükəsizliyi hadisələrinin sayının sürətlə artması və xidmətin sərəncamında olan insan və texniki resursların məhdud olmasıdır. Məhdud resursların meydana çıxan müxtəlif növ informasiya təhlükəsizliyi hadisələrinin emalı üçün effektiv paylanması və idarə olunması məsələsi qarşıda duran aktual problemlərdəndir. Bunları nəzərə alaraq, bu işdə İTX-nin iş parametrlərinin optimal seçilməsi məqsədilə kütləvi xidmət modelləri qurulur. Modellərdə fərz olunur ki, sistemin girişinə sensorlardan (IDS, şəbəkə ekranı, loq-fayl analizatorları, istifadəçi məlumatları və s.) informasiya təhlükəsizliyi hadisələrinin təsadüfi axını daxil olur. Hadisələrin emal müddəti təsadüfi kəmiyyətdir.

Kütləvi xidmət modelləri ehtimal nəzəriyyəsinin müxəlif praktiki məsələlərin həllində geniş tətbiq edilən sahələrindən biridir və elmi ədəbiyyatda bir çox analitik və imitasiya modelləri təklif edilmişdir [1]. Kütləvi xidmət nəzəriyyəsi telekommunikasiya sistemlərində geniş istifadə edilir və İnternetin elmi-metodoloji əsaslarının işlənməsində də xüsusi rol oynamışdır [2].

Əlaqədar tədqiqatlar

Ümumiyyətlə, kütləvi xidmət nəzəriyyəsi (KXN) nəinki informasiya texnologiyaları sahəsində, həmçinin xidmət göstərilən və növbə ardıcıllığı olan hər bir sahədə istifadə oluna bilər. Buna görə də, KXN-ın əsasında istifadə olunan tətqiqatlar müxtəlif eksperimentlərdən keçib və onlar haqqında geniş məlumat əldə etmək imkanı yaradır. Konkret olaraq informasiya texnologiyaları sahəsində KXN-dən istifadə edərək, QoS göstəricilərinin optimallaşdırılmasında [3], şəbəkənin idarə olunmasında, DDoS hücumların tədqiqində və qarşısının alınmasında [4], şəbəkə trafikinin proqnozlaşdırılmasında [5] və s. müraciət olunur.

[5]-də KXN-ın əsasında şəbəkə trafikinin monitorinqinin qiymətləndirilməsi göstərilmişdir. Korporativ mühitdə şəbəkə təhlükəsizliyinin monitorinqi şəbəkədə baş verən hadisələrin effektivliyinin və təhlükəsizliyinin qiymətləndirilməsi üçün zəruridir. Bundan savayı, şəbəkə trafikinin idarə olunması, proqnozlaşdırılması və keyfiyyəti müzakirə olunur. Şəbəkə trafikinin iş proesesinə nəzarət və yüklənmənin balanslaşdırılması üçün Little qanunundan istifadə olunur. Belə ki, intellektual proqnozlaşdırma prosesinin əsasında şəbəkə trafikinin vəziyyəti haqqında daha dolğun məlumat almaq mümkündür.

Şəbəkə trafikinin idarə olunması üçün idarəetmə nəzəriyyəsinin alətlərindən istifadə oluna bilər. Buna misal IP protokolun əlavə yüklənməsinə nəzarət prosesinin idarə olunmasıdır. [6]-da növbələrin aktiv idarə edilməsi texnologiyası və TCP protokolunda trafikin monitorinqi üçün zaman gecikmələrinin xətti müşahidəçisi işlənmişdir. Daha dəqiq desək, şəbəkə topologiyasının dar boğazları və marşrutlayıcılardan keçən uzunömürlü TCP-qoşulmaların tədqiqinə yönəlib. Marşrutlayıcıda yerləşdirilmiş mexanizm, TCP axının qiymətləndirilməsi əsasında şəbəkənin idarə olunması və anomaliyaların növünun müəyyən olunmasına şərait yaradır.

Kütləvi xidmət sistemi (KXS) əsasında şəbəkə trafikinin monitorinqinin baza modelinin yaradılması [7]-də öyrədilmişdir. Burada (M/M/1):((C+1)/FCFS) və (M/M/2): ((C+1)/FCFS) modelləri əsasında şəbəkə trafikinin yüklənmələrini proqnoz etmək mümkündür. Bu modellərə əsaslanaraq, şəbəkə trafikinin proqnozlaşdırılmasını və tıxacların stabil formulunu əldə edə bilərik.

Monitorinq məlumatlarının ötürülməsi prosesinin baza modelinə kütləvi xidmət modeli kimi baxılması [8]-də qeyd olunmuşdur. Bu yanaşma şəbəkə strukturunda OSI modelinin 1–5-ci səviyyələrində aparılan monitorinq prosesi əsasında sadə növbəyə əsaslanır. M/M/1 kütləvi xidmət modelini realizasiya etməklə, şəbəkə trafikinin proqnozlaşdırma yolları və sabit yüklənmə dərəcəsi düsturu verilmişdir.

Şəbəkəyə xaricdən gələn təhdidlərin idarə olunması üçün KŞ-larda şəbəkə ekranlarından istifadə edilir. Bu şəbəkə ekranları gələn trafikə uyğun olaraq onu yoxlayır və müəyyən təhdidlərin qarşısını ala bilir. Məlum olduğu kimi, DDoS hücumların qarşısını almaq üçün xüsusi qabaqlayıcı tədbirlər görülməsə, bu, sistemlərdə və xidmətlərdə əlyetənliyin pozulmasına gətirib çıxara bilər. [9]-da Markov zənciri əsasında analitik kütləvi xidmət modeli tətbiq olunur. Bu modelin əsasında şəbəkə ekranının normal və DDoS hücumuna məruz qalması zamanı məhsuldarlığı analiz olunur. Eksperimentlərin nəticəsi olaraq, əsas funksiyalar üçün düsturlar və məhsuldarlıq göstəriciləri alınmışdır.

Monitorinq vaxtının minimallaşdırılmasına imkan verən və verilmiş şəbəkə resursları çərçivəsində KŞ qovşaqlarının onlayn monitorinqinin optimallaşdırılması üçün müxtəlif kütləvi xidmət metodları təklif olunmuşdur. [10]-da bu məqsədə çatmaq üçün pollinq sisteminin modelindən istifadə edilməsi təklif edilir və onun optimallaşdırılması nəticəsində monitorinq vaxtının minimallaşdırılmasına nail olmağın mümkün olduğu sübut olunur.

İnformasiya təhlükəsizliyi hadisələrinin emalı üçün M/G/1 modeli

İTX-nin əsas xüsusiyyətlərindən biri odur ki, informasiya təhlükəsizliyi hadisələri (KXN terminləri ilə sifarişlər) müxtəlif sensorlardan (IDS, şəbəkələrarası ekranlar, informasiya təhlükəsizliyi vasitələri, tətbiqi proqramlar və istifadəçilər) real vaxt rejimində daxil olur və hər bir hadisə xidmətdən imtina edilmədən emal olunaraq reaksiya verilir. Bu proses ərzində heç bir

müraciətə baxılmasına vaxt məhdudiyyəti qoyulmur. Amma iş fəaliyyətinin effektiv idarə olunması üçün cərimə funksiyaları nəzərdə tutula bilər.

İTX-ya daxil olan hər bir informasiya təhlükəsizliyi hadisəsinə müəyyən kriteriyalar əsasında müsbət tam ədədlər şəklində prioritetlər verilir: 1, 2, 3,... . Nömrə artırdıqca, prioritet azalır, yəni 1 – ən yüksək prioriteti bildirir. Məsələn, insidentlərin idarə edilməsi üzrə ITIL yanaşmasında [11] prioritet 1–5 şkalasında olmaqla, insidentin təcilliyi (nə dərəcədə tez aradan qaldırılması) və insidentin təsirinin səviyyəsi əsasında müəyyən edilir. İnformasiya təhlükəsizliyi hadisələrinin prioritetlərinin müəyyən edilməsi üçün iyerarxik meyarlar sistemi və müvafiq qiymətləndirmə metodu [11]-də təklif edilir.

İTX hadisələrin emalını prioritetlərə əsasən təşkil edir. Kritik hadisələrlə mütləq prioritetli sifarişlər kimi davranırlar, yəni belə hadisə daxil olduqda, aşağı prioritetli hadisələrin emalı dayandırılır və xidmət heyəti mütləq prioritetli hadisəyə yönləndirilir. Fərz olunur ki, orta prioritetli hadisələr nisbi prioritetli sifarişlər kimi emal olunur, yəni xidmət prosesində nisbi prioritetli hadisə daxil olursa, onda cari hadisənin emalı dayandırılmır, daxil olan hadisə növbəyə qoyulur. Növbədən xidmət üçün seçim edildikdə, daha yüksək prioritetli hadisə seçilir.

Aşağı prioritetli hadisələr isə prioritetsiz rejimdə emal olunur. Prioritetsiz rejimdə xidmət zamanı sifarişlər növbəsiz xidmət imtiyazına malik deyil və növbədən *FIFD* (*First In - First Out), LIFO (Last In – First Out),* yaxud *RAND* (*Random* – təsadüfi) rejimdə xidmət üçün seçilirlər. Bu prioritetsiz xidmət qaydasının hər üçündə orta gözləmə müddətinin dispersiyası minimal olur.

Bu işdə İTX-nin iş prosesinin idarə olunması üçün KXN *M/G/1* modelinin tətbiq edilməsi təklif olunur. [12]-də qeyd olunduğu kimi, bu növ modellər daha çox verilənlərin emalı prosesində istifadə olunur.

Tutaq ki, KXS intensivlikləri $\lambda_i, i=\overline{1,M}$ olan sifarişlərin sadə axını daxil olur. KXS-da bir xidmət kanalının olması fərz olunur (bir *CERT*-komandası fəaliyyət göstərir). Bu axınlar toplama intensivliyi $\Lambda=\sum_{i=1}^{M}\lambda_i$ olan Puasson axını əmələ gətirir. Xidmət müddətinin paylanmasının ümumi paylanma olması fərz olunur. *i*-ci axın sifarişlərinin xidmət müddətinin riyazi gözləməsi b_i və başlanğıc 2-ci tərtib momenti $b_i^{(2)}$ ilə işarə olunur. KXS-nın *i*-ci növ sifarişlərlə yaranan yüklənməsi $\rho_i=\lambda_i b_i$ kimi ifadə olunur.

Hadisələrin emal qaydası olaraq, qarışıq prioritetli xidmət qaydası seçilib. Ümumi halda, qarışıq prioritetli xidmət qaydası olan KXS-na baxılır: prioritetləri $\overline{1,M_1}$ aralığında olan hadisələrə mütləq prioritetlər, prioritetləri $\overline{M_1+1,M_2+M_2}$ aralığında olan M_2 sayda sifarişə nisbi prioritetlər verilir, qalan M_3 sayda sifariş isə prioritetsiz rejimdə emal edilir.

Beləliklə, 3 prioritet sinfi olan sifarişlərə baxılır. Birinci sinfin sifarişləri ikinci və üçüncü sinfin sifarişlərinə nəzərən mütləq prioritetə, ikinci sinif isə üçüncü sinfə nəzərən nisbi prioritetə malikdir.

Müxtəlif prioritet siniflərindən olan sifarişlərin (informasiya təhlükəsizliyi hadisələrinin) KXS-da orta gözləmə müddətlərini tapaq:

Mütləq prioritetli hadisələr üçün gözləmə müddəti digər hadisələrin xidmət xarakteristikalarından asılı deyil. Bu hadisələr üçün orta gözləmə müddəti $w_k^{AP}, k=\overline{1,M_1}$ aşağıdakı düsturla hesablana bilər [1]:

$$w_k^{AP}=\frac{R_{k-1}b_k}{1-R_{k-1}}+\frac{\sum_{i=1}^{k}\lambda_i b_i^{(2)}}{2(1-R_k)(1-R_{k-1})},$$

burada $R_j=\sum_{i=1}^{j}\rho_j$ – ilk *j* prioritetli (yəni, yüksək prioritetli) hadisələr axınından yaranan toplam yükləmədir.

Birinci toplanan daha yüksək prioritetli hadisələrə görə xidmətin dayanması nəticəsində

növbədə sərf olunan müddəti göstərir.

Qeyd edək ki, k= 1 olduqda, $w_1^{AP} = \dfrac{\lambda_1 b_1^2}{2(1-\rho_1)}$ alınır.

Nisbi prioritetli hadisələr üçün orta gözləmə müddəti w_k^{RP} aşağıdakı düsturla müəyyən edilə bilər [2]:

$$w_k^{RP} = \frac{R_{M_1} b_k}{1-R_{M_1}} + \frac{\sum_{i=1}^{M} \lambda_i b^{(2)}}{2(1-R_{k-1})(1-R_k)}$$

burada $k = \overline{M_1+1, M_1+M_2}$, $R_j = \sum_{i=1}^{j} \rho_j$.

Prioritet verilməyən hadisələr üçün orta gözləmə müddəti w_k^{WP} oxşar qaydada müəyyən edilir [13]:

$$w_k^{WP} = \frac{R_{M_1} b_k}{1-R_{M_1}} + \frac{\sum_{i=1}^{M} \lambda_i b_i^{(2)}}{2(1-R_{M_1+M_2})(1-R)}, \quad k = \overline{M_1+M_2+1, M},$$

burada $R = \sum_{i=1}^{M} \rho_j$ toplam axının yaratdığı yükləmədir.

Hadisələrin emalı üzrə fəaliyyətin effektivliyinin qiymətləndirilməsi modeli

İTX-nin fəaliyyətinin effektivliyini qiymətləndirmək üçün də təklif edilmiş kütləvi xidmət modelindən istifadə etmək olar.

İTX-nin real zaman rejimində işləməsi arzuolunandır (ideal haldır), yəni hadisələrin daxilolma sürəti ilə ayaqlaşa bilməlidir. Praktikada bu o deməkdir ki, informasiya təhlükəsizliyi hadisələri müəyyən məhdud müddətdə emal olunmalıdırlar: $T_{p_i} < u_i^*$, burada T_{p_i} sistemin i-ci növ hadisəyə reaksiya müddəti, u_i^* − i-ci növ hadisənin sistemdə olmasının yolverilən maksimum müddətidir.

Zaman xarakeristiklarının tələblərdən asılı olaraq 3 halına baxmaq olar:

1) xidmət müddətinə məhdudiyyət qoyulmur;
2) sistemdə olma müddətinə və gözləmə müddətinə nisbi məhdudiyyət qoyulur (yəni, tələblər ortalama yerinə yetirilir);
3) sistemdə olma müddətinə və gözləmə müddətinə mütləq məhdudiyyət qoyulur (yəni, tələblər hər bir sifariş üçün yerinə yetirilir).

Birinci halda informasiya təhlükəsizliyi hadisələrinin emalı üzrə fəaliyyətin effektivliyinin qiymətləndirilməsi məsələsinin həllinə qısa nəzər salaq. Qiymətləndirmə üçün iki parametrdən istifadə edilir:

- λ_i − hadisələrin daxil olma intensivliyi, $i = \overline{1, M}$;
- θ_i və $\theta_i^{(2)}$ − uyğun olaraq, i-ci növ hadisənin emalının əmək tutumunun riyazi gözləməsi və ikinci başlanğıc anıdır, ixtiyari paylanma funksiyası ilə xarakterizə olunur.

Hadisələrə reaksiya müddətinə məhdudiyyət qoyulmamasına baxmayaraq, hesab olunur ki, hadisə sistemdə nə qədər uzun müddətə qalırsa, sistemin fəaliyyətinin keyfiyyəti bir o qədər aşağı olur. Belə sistemin effektivlik kriteriyası aşağıdakı cərimə funkisyası ilə xarakterizə oluna bilər:

$$F = \sum_{i=1}^{M} \alpha_i \lambda_i w_i,$$

burada α_i − cərimə əmsalıdır, i-ci növ hadisənin emalının gecikməsinin vahid zamanda dəyərini

müəyyən edir. Gecikmələr, yəni w_i zamanları iki faktordan: xidmət cihazının emal sürətindən və xidmət qaydasından asılıdır. Müvafiq olaraq, sistemin optimallaşdırılması üçün F-in minimallaşdırılması zəruridir.

Reaksiya müddətinə məhdudiyyət qoyulmayan sistemdə verilmiş hadisələr axınına imtinasız xidmət göstərilməsi üçün sürətin yetərli olması zəruridir. Aydındır ki, bu halda sistem stasionar rejimdə R<1 işləməlidir, yəni emal sürəti daxilolma sürətindən yüksək olmalıdır.

Qeyri-bircins hadisələr halında ümumi yüklənmə

$$R = \sum_{i=1}^{M} \rho_i = \sum_{i=1}^{M} \lambda_i b_i$$

olur. Lakin b_i hadisənin emalının əmək tutumu və xidmət cihazının sürəti ilə müəyyən edilir: $b_i = \frac{\theta_i}{B}$, burada B − xidmət cihazının emal sürətidir. Buradan emal sürətinin sərhəd qiyməti üçün

$$B > \sum_{i=1}^{M} \theta_i$$

alırıq. Yəni, baxılan halda sistemə qoyulan məhdudiyyətlər λ və θ parametrləri ilə müəyyən edilir. Hadisələr vacibliyinə görə ranqlaşdırıla bilər, yəni müvafiq α_i əmsallarına malik ola bilərlər. Əgər bütün informasiya təhlükəsizliyi hadisələri eyni ranqlıdırsa, onda uyğun α_i əmsalları $\alpha_i = \alpha = const$ olur və cərimə funksiyası sadələşir:

$$F = \sum_{i=1}^{M} \lambda_i w_i = L,$$

burada L − sistemdə növbənin toplam uzunluğudur və sistemin fəaliyyət keyfiyyətinin artırılması üçün onun minimallaşdırılmasına cəhd etmək lazımdır.

Nəticə

Bu məqalədə kütləvi xidmət nəzəriyyəsi əsasında informasiya təhlükəsizliyi hadisələrinin emal prosesinin modelləşdirilməsi üçün M/G/1 modeli təklif olunmuşdur. İnformasiya təhlükəsizliyi hadisələri müxtəlif sensorlardan real vaxt rejimində daxil olur və İTX-ya daxil olan hər bir informasiya təhlükəsizliyi hadisəsinə müəyyən kriteriyalar əsasında prioritetlər verilir və bu prioritetlərə uyğun olaraq emal olunur. Təklif olunmuş modeldə informasiya təhlükəsizliyi hadisələrinin üç prioritet sinfində – mütləq, nisbi və prioritetsiz xidmət rejimlərində emalı üçün orta gözləmə müddətlərinin analitik ifadələri verilir. Bu proses ərzində heç bir müraciətə baxılmasına vaxt məhdudiyyəti qoyulmur. Amma iş fəaliyyətinin effektiv idarə olunması üçün alınmış ehtimal xarakteristikalarından istifadə etməklə cərimə funksiyaları daxil edilməklə model də təklif edilmişdir.

Ədəbiyyat

1. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания, М.: Изд-во ЛКИ, 2007, 400 с.
2. Клейнрок Л. Вычислительные системы с очередями: пер. с англ. М.: Мир, 1979, 600 с.
3. Шыхалиев Р.Г. О методах мониторинга и управления QoS компьютерных сетей // İnformasiya texnologiyaları problemləri, 2013, № 1, s.15–23.
4. İnformasiya texnologiyaları problemləri, 2013, № 1, s.15–23.
5. Kumar S., Bhandari A., Sangal A. L. Comparison of Queuing Algorithms against DDoS Attack // International Journal of Computer Science and Information Technologies, 2011, vol.2, pp.1574–1580.
6. Hedayati M., Kamali S.H., Izadi A.S. Notice of retraction the monitoring of the network traffic based on queuing theory and simulation In heterogeneous network environment / International Conference on Information and Multimedia Technology, 2009, pp.396–402.
7. Ariba Y., Gouaisbaut F., Rahme S., Labit Y. Traffic monitoring in transmission control

protocol/active queue management networks through a time-delay observer // Control Theory & Applications, 2012, vol.6, no.2, pp.506–517.
8. Saha Ray S., Sahoo P. Monitoring of network traffic based on queuing theory / National technology institute of Rourkela, 2011, pp.30.
9. Kammas P., Komninos T., Stamatiou Y.C. Queuing theory based models for studying intrusion evolution and elimination in computer networks/ Fourth International Conference on Information Assurance and Security, 2008, pp.167–171.
10. Yang W., Chuang L., Quan-Lin L., Yuguang F. A queueing analysis for the denial of service (DoS) attacks in computer networks // IEEE Transactions on Network and Service Management, 2011, vol.9, no.1, pp.12–21.
11. Шыхалиев Р.Г. Повышение эффективности мониторинга компьютерных сетей на основе оптимизации поллинг системы // Информационные технологии, 2015, №8, с. 576–584.
12. Jan van Bon (ed.). Foundations of ITIL V3. 1st edition. Van Haren Publishing, 2007, 350 p.
13. Хрусталев Ю.П. Моделирование систем массового обслуживания. Иркутский национальный исследовательский технический университет, 2007, 116 с.
14. Imamverdiyev Y.N. An information security incident prioritization method / 7th Int-l Conf. on Application of Information and Communication Technologies (AICT'2013), 09-11 Oct. 2013, Baku, pp.183–187.

УДК 004.056

Имамвердиев Ядигар Н.[1], Набиев Бабек Р.[2]
Институт Информационных Технологий НАНА, Баку, Азербайджан
[1]yadigar@lan.ab.az, [2]babek@iit.ab.az

Модели массового обслуживания для систем мониторинга информационной безопасности

Для моделирования процесса обработки инцидентов в системах управления информационной безопасности была предложена модель массового обслуживания. Процесс обработки инцидентов осуществляется в смешанно-приоритетном порядке обслуживания, описываемом моделью M/G/1, и имеет три класса приоритетов – абсолютные, относительные и бесприоритетные, и для этих режимов обслуживания дано аналитическое выражение для среднего времени ожидания. На основе полученных характеристик вероятности для оценки эффективной деятельности по обработке инцидентов информационной безопасности в модель были включены функции штрафов.

Ключевые слова: *информационная безопасность, инциденты информационной безопасности, мониторинг сетевого трафика, теория массового обслуживания, приоритетная обработка*.

Yadigar N. Imamverdiyev[1], Babek R. Nabiyev[2]
Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]*yadigar@lan.ab.az*,[2]*babek@iit.ab.az*

Queuing model for information security monitoring systems

A model of queuing is proposed for the modeling of incidents handling process in the information security management system. Incident handling process is described by the model of M/G/1, which is carried out as mixed-priority services, and analytic expressions of the average waiting time are given for three priority classes, which are the absolute, relative and without priority modes of service. The model is proposed for the evaluation of the efficiency of the performance of the processing of information security incidents by including the penalty functions basing on the characteristics of the probabilities.

Keywords: *information security, information security incidents, network traffic, monitoring, queuing theory, priority handling.*