AZƏRBAYCAN MİLLİ ELMLƏR AKADEMİYASI
İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU

Əlyazması hüququnda

BABƏK RASİM OĞLU NƏBİYEV

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNİN İNTELLEKTUAL MONİTORİNQİ SİSTEMİNİN SİNTEZİ ÜÇÜN METOD VƏ ALQORİTMLƏRİN İŞLƏNİLMƏSİ

3338.01 – Sistemli analiz, idarəetmə və informasiyanın işlənməsi

Texnika üzrə fəlsəfə doktoru elmi dərəcəsi almaq üçün
təqdim edilmiş dissertasiyanın

A V T O R E F E R A T I

BAKI – 2018

Dissertasiya işi Azərbaycan Milli Elmlər Akademiyası İnformasiya Texnologiyaları İnstitutunda yerinə yetirilmişdir.

Elmi rəhbər:
AMEA-nın həqiqi üzvü,
texnika elmləri doktoru, professor **R.M. ƏLİQULİYEV**

Rəsmi opponentlər:

AMEA-nın müxbir üzvü,
texnika elmləri doktoru **R.M. ALIQULİYEV**

texnika üzrə fəlsəfə doktoru, dosent **Z.Ə. CƏFƏROV**

Aparıcı təşkilat:
Milli Aviasiya Akademiyasının "İnformasiya Texnologiyaları" kafedrası

Müdafiə **25 may 2018-ci il tarixində saat 16^{00}**-da AMEA İnformasiya Texnologiyaları İnstitutunun nəzdindəki FD.01.231 dissertasiya şurasının iclasında keçiriləcəkdir.

Ünvan: AZ 1141, Bakı şəhəri, B. Vahabzadə küç., 9A.

Dissertasiya işi ilə Azərbaycan Milli Elmlər Akademiyası İnformasiya Texnologiyaları İnstitutunun kitabxanasında tanış olmaq olar.

Avtoreferat "24" aprel 2018-ci tarixində paylanmışdır.

FD.01.231 Dissertasiya şurasının elmi katibi,
texnika üzrə fəlsəfə doktoru, dosent **R.H. ŞIXƏLİYEV**

İŞİN ÜMUMİ XARAKTERİSTİKASI

İşin aktuallığı. Kompüter şəbəkələri müasir cəmiyyətin informasiya infrastrukturunda kritik vacib sistemyaradıcı elementlərdən birinə çevrilmişdir. Bu şəbəkələrin miqyasının böyüməsi, şəbəkədə emal olunan informasiyanın həcminin artması, şəbəkə xidmətlərinin spektrinin genişlənməsi informasiya təhlükəsizliyi boşluqlarının artmasına səbəb olur.

İnformasiya təhlükəsizliyinin monitorinqi kompüter şəbəkələrində təhlükəsizliyin vəziyyəti barədə real zaman rejimində həqiqi məlumat əldə edilməsinə, vəziyyətin qiymətləndirilməsinə, aşkarlanan kiberhücumların və digər insidentlərin aradan qaldırılmasına xidmət edir. Bu baxımdan monitorinq informasiya təhlükəsizliyinin təmin edilməsində aparıcı rol oynayır. Ona görədə informasiya təhlükəsizliyi xidmətinin (İTX) işinin effektiv təşkil edilməsi olduqca aktualdır və bu istiqamətdə bir çox elmi-praktiki işlər mövcuddur. Bu işlərə təhdidlərin aşkarlanması və aradan qaldırılması kimi yanaşmaları misal göstərmək olar: təhlükəsizlik əməliyyatları mərkəzləri (ing. security operation center, SOC), informasiya təhlükəsizliyi və hadisələrinin idarə olunması (ing. security information and event management, SIEM) və kompüter təhlükəsizliyi insidentlərinə cavabvermə komandaları (ing. Computer Security Incident Response Team, CSIRT). Analiz göstərir ki, məlum İTX-lərın qarşısına çıxan əsas məsələ informasiya təhlükəsizliyi hadisələrinin sürətlə artması və xidmətin sərəncamında olan insan və texniki resursların məhdud olmasıdır. Meydana çıxan müxtəlif növ informasiya təhlükəsizliyi hadisələrinin emalı üçün məhdud resursların effektiv paylanması və idarə olunması məsələsi qarşıda duran aktual problemlərdəndir. Buna görə də, kompüter şəbəkələrinin fəaliyyəti və təhlükəsizliyi haqqında lazımi verilənlərin toplanması, analiz edilməsi və şəbəkə təhlükəsizliyinin təmin edilməsi məqsədilə əsaslandırılmış qərarların qəbul edilməsi üçün verilənlərin intellektual analizi texnologiyalarından istifadə edilməsi aktuallıq kəsb edir.

İşin məqsədi. Şəbəkə təhlükəsizliyinin real vəziyyətinin operativ qiymətləndirilməsi, təhlükəsizlik siyasətinin pozulması hallarının erkən aşkarlanması və hadisələrə çevik reaksiya qərarları qəbul etməyə imkan verən intellektual monitorinq sisteminin sintezi üçün metod və alqoritmlərin işlənməsidir.

Dissertasiya işində qarşıya qoyulmuş məqsədə çatmaq üçün aşağıdakı məsələlər araşdırılmışdır:

- şəbəkə təhlükəsizliyinin intellektual monitorinqi sistemlərinin müasir vəziyyəti analiz edilmiş, mövcud elmi-nəzəri problemlər və onların həlli yolları müəyyənləşdirilmişdir;
- şəbəkə təhlükəsizliyinin intellektual monitorinqi üçün konseptual modelin işlənməsi;
- klasterizasiya əsasında veb trafikdən istifadə və davranış profilinin qurulması metodunun işlənməsi;
- şəbəkə trafikinin siniflərə ayrılması üçün ikimərhələli klassifikator modelinin işlənməsi;
- DDoS hücumların aşkarlanması üçün şəbəkə trafikinin klasterizasiyası metodunun işlənməsi;
- şəbəkə təhlükəsizliyinin monitorinqi üzrə qərarların qəbulu metodunun işlənməsi;
- informasiya təhlükəsizliyinin monitorinqi sistemi üçün hadisələrin emalı modelinin işlənməsi;
- şəbəkə təhlükəsizliyinin intellektual monitorinqi mərkəzinin arxitekturunun sintezi;
- əldə olunan nəticələrin yoxlanılması məqsədi ilə eksperimentlərin aparılması.

Tədqiqat metodları. Dissertasiya işində qarşıya qoyulmuş məsələlərin həlli üçün klasterizasiya, klassifikasiya, presedentlər və kütləvi xidmət nəzəriyyələrinin metodlarından istifadə olunmuşdur.

Müdafiəyə çıxarılan əsas müddəalar:

- şəbəkə təhlükəsizliyinin intellektual monitorinqi sisteminin konseptual modeli;
- veb trafikdən istifadə və davranış profilinin qurulması üçün klasterizasiya metodu;
- şəbəkə trafikinin siniflərə ayrılması üçün ikimərhələli klassifikator modeli;
- DDoS hücumların aşkarlanması üçün şəbəkə trafikinin klasterizasiyası metodu;
- presedentlər nəzəriyyəsi əsasında şəbəkə təhlükəsizliyinin monitorinqi üzrə qərarların qəbulu metodu;
- informasiya təhlükəsizliyinin monitorinqi sistemi üçün hadisələrin emalı modeli;
- şəbəkə təhlükəsizliyinin intellektual monitorinqi mərkəzinin arxitekturu.

Elmi yeniliklər. Dissertasiya işində alınmış əsas elmi yeniliklər aşağıdakılardır:

- şəbəkə təhlükəsizliyinin intellektual monitorinqi sistemi üçün konseptual modeli işlənmişdir;
- veb trafikdən istifadə və davranış profilinin qurulması üçün klasterizasiya metodu işlənmişdir;
- şəbəkə trafikinin siniflərə ayrılması üçün ikimərhələli klassifikator modeli işlənmişdir;
- DDoS hücumların aşkarlanması üçün şəbəkə trafikinin klasterizasiyası metodu işlənmişdir;
- presedentlər nəzəriyyəsi əsasında şəbəkə təhlükəsizliyinin monitorinqi üzrə qərarların qəbulu metodu işlənmişdir;
- informasiya təhlükəsizliyinin monitorinqi sistemi üçün hadisələrin emalı modelinin işlənməsi.

İşin praktiki əhəmiyyəti. Dissertasiya işində təklif olunan metod və alqoritmlər kompüter şəbəkələrində böyük informasiya axınının təhlükəsizlik monitorinqinin intellektual idarə olunması, bütün müraciətlərin vaxtında cavablandırılması, şəbəkə trafikinin düzgün təsnifatlandırılması, təhdidlərin qarşısının alınması və dəyə biləcək zərərin minimallaşdırılması, trafikin vəziyyəti haqqında lazımi instansiyalara dolğun məlumatın verilməsi üçün istifadə oluna bilər.

Dissertasiya işində təklif olunmuş yanaşmalar AzScinceNet elm kompüter şəbəkəsində sınaqdan keçirilmiş və müvafiq akt alınmışdır. Alınmış nəticələrə əsaslanaraq, sistemin genişləndirilməsi və inkişafı üçün qeyd olunan şəbəkənin təhlükəsizlik xidməti yaradılmışdır. Yaradılmış xidmət həmçinin AzScienceCERT adı altında Trusted Introducer beynəlxalq təşkilatında akreditasiyadan keşmişdir.

İşin aprobasiyası. Dissertasiya işinin əsas elmi-nəzəri və praktiki nəticələri: "Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları" 2-ci respublika Elmi Konfransında (27-28 noyabr 2012, Sumqayıt ş.), "Elektron elm problemləri" üzrə 1-ci respublika konfransında (15-16 noyabr 2012, Bakı ş.), "Beynəlxalq İnformasiya Təhlükəsizliyi Gününə həsr olunmuş elmi-praktiki seminarda (30 noyabr 2012, Bakı ş.), Azərbaycan xalqının Ümummilli lideri Heydər Əliyevin 90 illik yubileyinə həsr olunmuş "İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransında" (17-18 may 2013, Bakı ş.), Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş "İnformasiya təhlükəsizliyinin multidissiplinar problemləri" üzrə II respublika elmi-praktiki konfransında (14 may

2015, Bakı ş.), "Big data: imkanları, multidissiplinar problemləri və perspektivləri" I respublika elmi-praktiki konfransında (26 fevral 2016, Bakı ş.) və "İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarında (8 dekabr 2017, Bakı ş.) məruzə və müzakirə edilmişdir.

Elmi nəşrlər. Dissertasiya mövzusu üzrə 15 elmi iş çap olunmuşdur. Onlardan 7 məqalə resenziya olunan beynəlxalq və respublika səviyyəli elmi jurnallarda və 8 məruzə isə nüfuzlu konfransların materiallarında nəşr olunmuşdur.

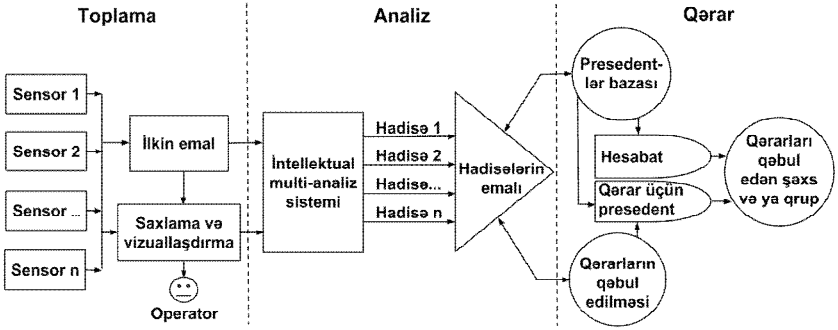
Dissertasiya işinin strukturu və həcmi. Dissertasiya işi giriş, dörd fəsil, nəticə və 146 adda ədəbiyyat siyahısından ibarətdir. İşin əsas məzmunu 126 səhifədən, 31 şəkil və 13 cədvəldən ibarətdir.

İŞİN MƏZMUNU

Girişdə dissertasiya işinin aktuallığı əsaslandırılmış, tədqiqatın məqsədi və həll olunacaq məsələlər müəyyən edilmişdir. Əldə edilmiş nəticələrin elmi yeniliyi və praktiki əhəmiyyəti göstərilmişdir.

Birinci fəsildə şəbəkə təhlükəsizliyinin monitorinqi texnologiyalarının müasir vəziyyəti - əsas anlayışları, funksiyaları, idarəetmədə əhəmiyyəti, inkişaf mərhələləri və perspektivləri, dünya təcrübəsi araşdırılmış və problemlər müəyyənləşdirilmişdir.

İkinci fəsildə şəbəkə təhlükəsizliyinin intellektual monitorinqinin konseptual modeli təklif edilmiş, veb trafikdən istifadə və davranış



Şəkil 1. Şəbəkə təhlükəsizliyinin intellektual monitorinqi sisteminin konseptual modeli.

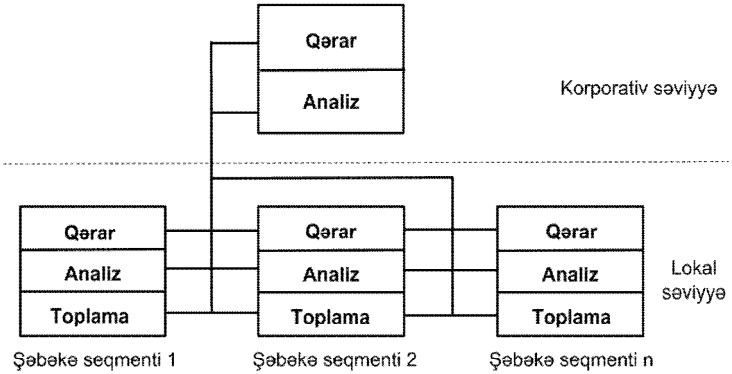
profilinin qurulması üçün klasterizasiya metodu işlənmiş, şəbəkə trafikində real vaxt rejimində anomal aktivliyin mənsubiyyətinin ilkin

mərhələdə aşkarlanması üçün ikimərhələli klassifikator modeli təklif edilmişdir.

Şəkil 1-dən göründüyü kimi, koseptual model ümumi olaraq toplama, analiz və qərar bloklarından ibarətdir. Hər bir blok isə müəyyən
funksiyaları yerinə yetirən alt bloklardan ibarətdir.

Korporativ şəbəkələrin müxtəlif lokal şəbəkələrdən təşkil olunduğunu nəzərə alsaq, baş vermiş insident və ya ümumiyyətlə vəziyyət haqqında şəbəkələrarası monitorinq verilənlərinin mübadiləsinin, informasiya təhlükəsizliyi nöqteyi nəzərindən nədərəcədə vacib olduğunu qiymətləndirə bilərik.

Buna görə də, şəbəkə təhlükəsizliyinin intellektual monitorinqinin ierarxik struktura malik olan konseptual modelinin makro arxitekturunun (şək. 2) formalaşması vacibdir.



Şəkil 2. Şəbəkə təhlükəsizliyinin intellektual monitorinqi sisteminin iyerarxik arxitekturu

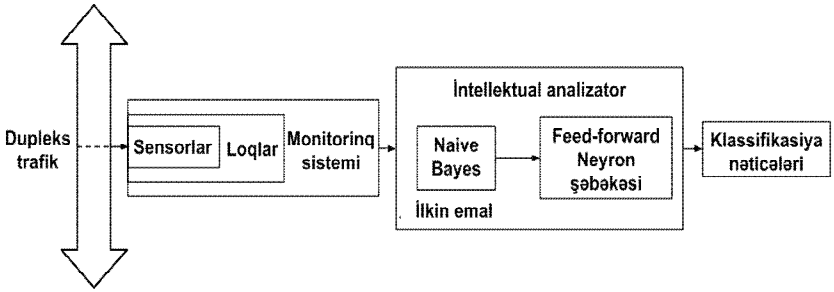
Şəkil 2-dən göründüyü kimi korporativ səviyyədə yerləşən blokun toplama funksiyası yoxdur. Bu blokun əsas vəzifəsi aşağı səviyyəli blokların fəaliyyətinə nəzarət, xüsusi hallarda lokal səviyyədə yerləşən blokların emal edə bilmədiyi hadisələrə reaksiya vermək və həllər generasiya etməkdir.

Əsas məsələlərdən biri də şəbəkə trafikinin real vaxt rejimində klassifikasiyası prosesini aparmaqla anomal aktivliyin mənşəyini ilkin mərhələdə aşkarlamaqdır.

Kompüter şəbəkələrində trafik axınının operativ klassifikasiyasının təmin olunması üçün ikimərhələli klassifikator yanaşması tətbiq edilmişdir (şək. 3). Burada monitorinq sistemi vasitəsilə, dupleks

trafikdə göndərilən və qəbul olunana şəbəkə trafikini sensorlar vasitəsi ilə toplayaraq loqlaqlaşdırır. Daha sonra informasiya intellektual analizatora ötürülür.

Birinci mərhələdə Naive Bayes klassifikatoru ilə axına uyğun olaraq ən yaxın iki sinif seçilir. Bu daha tez cavab almaq üçün əlverişlidir. İkinci mərhələdə isə neyron şəbəkə vaxitəsilə bu iki siniflərdən daha uyğununu seçib dolğun nəticə əldə edilir.



Şəkil 3. İkimərhələli klassifikator

Üçüncü fəsildə DDoS hücumların aşkarlanması üçün şəbəkə trafikinin klasterizasiyası metodu işlənmiş, kompüter şəbəkəsi qovşaqlarının onlayn monitorinqinin optimallaşdırılması üçün kütləvi xidmət nəzəriyyəsi əsasında metod və keyfiyyətə nəzarət üçün cərimə funksiyası təklif olunmuş, presedentlər nəzəriyyəsi əsasında qərarların qəbul edilməsi metodu işlənmişdir.

DDoS hücumların aşkarlanması üçün ilkin olaraq k -means klasterizasiya alqoritmi tətbiq olunur. Tutaq ki, $X = [x_1, \dots, x_n]$ verilənlər toplusu n trafik sessiyalarından ibarətdir. Hər bir trafik-sessiyası x_i Evklid fəzasında m -ölçülü nöqtə kimi təsvir edilmişdir: $x_i - (x_{i1}, \dots, x_{im})$, burada x_{ij} i -ci trafik sessiyanın j -ci atributudur, ($i = 1, \dots, n$; $j = 1, \dots, m$). Məqsəd trafik-sessiyaları, başqa sözlə $X = [x_1, \dots, x_n]$ verilənlər toplusunu K sayda klasterlərə bölməkdir: $C = (C_1, \dots, C_K)$. Burada fərz edirik ki, aşağıdakı şərtlər ödənilir:

1) İxtiyari p $C_p \neq \emptyset$, başqa sözlə hər bir klasterdə heç olmazsa bir nöqtə olmalıdır, $p - 1,2, \dots, K$.

2) İxtiyari $p1 \neq p2$ üçün $C_{p1} \cap C_{p2} = \emptyset$, yəni iki müxtəlif klasterin ortaq elementləri olmamalıdır, $p1, p2 = 1, \dots, K$;

$\bigcup_{p=1}^{K} C_p = X$

3) , yəni hər bir nöqtə hər hansı bir klasterə mütləq aid edilməlidir;

4) Klasterlər üzərinə əvvəlcədən heç bir şərt qoyulmur.

k -means alqoritm aşağıdakı mərhələlərdən ibarətdir:

1. İlk olaraq $X = \{x_1, \dots, x_n\}$ nöqtələr toplusundan K sayda nöqtə klasterlərin mərkəzi kimi seçilir. Bu mərkəzləri $O = \{o_1, \dots, o_K\}$ ilə işarə edək və $s = 0$ qəbul edək (s iterasiyaların sayını göstərir).

2. Hər bir verilən $x_i = (x_{i1}, \dots, x_{im})$ ilə p -ci klasterin mərkəzi, $o_p = (o_{p1}, \dots, o_{pm})$, arasındakı məsafə hesablanır. Bu məsafəni hesablamaq üçün Evklid metrikasından istifadə olunur:

$$d(x_i, o_p) = \left(\sum_{j=1}^{m} (x_{ij} - o_{pj})^2 \right)^{\frac{1}{2}}, \quad i = 1, \dots, n \; ; \; p = 1, \dots, K \;, \qquad (1)$$

burada o_{pj} – p -ci klasterin mərkəzinin j -cu koordinatıdır.

3. x_i nöqtəsi o klasterə aid edilir ki, $d(x_i, o_p)$-nin qiyməti minimum olsun, yəni $x_i \in C_p$, əgər $d(x_i, o_p) = \min_q d(x_i, o_q)$.

4. Bütün nöqtələr klasterlərə aid edildikdən sonra, aşağıdakı məqsəd finksiyasının qiyməti hesablanır:

$$f^{\uparrow}((s)\,)\,(x) = \sum\nolimits_{\downarrow}(p = 1)^{\uparrow}K \sum\nolimits_{\downarrow}(x \in C_{\downarrow}p) \llbracket ||x - o_{\downarrow}p \llbracket ||\rrbracket \uparrow 2 \rrbracket \qquad (2)$$

bu funksiyanın qiyməti nə qədər kiçik olarsa, klasterləşmə o qədər yaxşı hesab olunur.

5. Sonra hər bir klasterin mərkəzi aşağıdakı düsturun köməyilə yenidən hesablanır:

$$o_{pj} = \frac{1}{|C_p|} \sum_{x_i \in C_p}' x_{ij} \;, \quad p = 1, \dots, K \;, \; j = 1, \dots, m \qquad (3)$$

burada $|C_p|$ – p -ci klasterdəki nöqtələrin sayı, o_{pj} - p-ci klasterin mərkəzinin j-cu kordinatıdır.

6. $s = s + 1$

7. 3-5 addımları o vaxta qədər təkrarlanır ki, aşağıdakı yığılma şərti ödənilisin:

$$\left| \frac{f^{(s+1)}(x) - f^{(s)}(x)}{f^{(s)}(x)} \right| \leq \varepsilon \;, \qquad (4)$$

burada ε əvvəlcədən verilmiş parametrdir.

Klasterləşmənin keyfiyyətini qiymətləndirmək üçün aşağıdakı indeksdən istifadə olunur:

$$Validity = \frac{\sum_{p=1}^{K}\left\{\frac{1}{|C_p|}\max_{x_i \in C_p} d(x_i, o_p)\right\}}{\sum_{p-1}^{K}\left\{\min_{\substack{q=1,\dots,K \\ q \neq p}} d(o_p, o_q)\right\}} \quad (5)$$

Bu indeksin qiyməti nə qədər kiçik olarsa, klasterləşmənin keyfiyyəti o qədər yüksək hesab olunur.

DDoS hücumların aşkarlanması üçün tətbiq olunacaq ikinci metod isə EM (ing. Expectation Maximization) alqoritmidir. Çünki, EM alqoritmi müşahidə edilən məlumatların ehtimalını maksimum dərəcədə artırmaq üçün parametrləri qiymətləndirir. Bu məqsədlə, aşağıda iki addım arasında təkrarlanan loqarifmik ehtimal $L_c(\Psi)$ haqqında məlumat veriləcək.

EM alqoritminin E addımı aşağıdakı hesablamadan ibarətdir:

$$Q(\Psi, \Psi^{(q)}) = E_{\Psi(q)}[log\, L_c(\Psi)|y, z]; \quad (6)$$

burada $\Psi^{(q)}$ Ψ-nin q iterasiyasına uyğunluğudur. $E_{\Psi(q)}$ isə $\Psi_{(q)}$ parametrlərindən istifadə etməyə hesablanmış riyazi gözləməni təmsil edir. Yəni,

$$t_{ik} = E_{\Psi(q)}[Z_{ik}|x_i, \Psi_k] = P_{\Psi(q)}[Z_{ik} = 1|x_i] = \frac{\pi_k g_k(x_i; \Psi_k)}{\sum_{k=1}^{g} \pi_k g_k(x_i; \Psi_k)}$$

(7)

sonra,

$$Q(\Psi, \Psi^{(q)}) = \sum_{k=1}^{g} log\pi_k \sum_{i=1}^{n} t_{ik} - \frac{np}{2}\log(2\pi) - \sum_{k=1}^{g}\sum_{i=1}^{n} t_{ik} \sum_{j=1}^{p} \log(\sigma_{jk}) - \frac{1}{2}\sum$$

(8)

EM alqoritminin M addımı $Q(\Psi, \Psi^{(q)})$ ilə əlaqədar $\Psi^{(q)}$ gözləmənin maksimallaşdırılmasını nəzərdə tutur; yəni Ψ_{q+1} hesablanması zamanı $Q(\Psi_{q+1}, \Psi^{(q)}) \geq Q(\Psi, \Psi^{(q)})$ belə müəyyən olunur və hamısı üçün $\Psi \in \Omega$ qəbul edilir. Praktikada yeniləmə tənlikləri $Q(\Psi, \Psi^{(q)})$ törəmələrinin hər bir komponentinə

görə Ψ sıfra bərabər olur. Kovarians matrisin dioqanal qəbul etsək, onda

$$\pi_k^{(q+1)} = \frac{1}{n}\sum_{i=1}^{n} t_{ik}; \tag{9}$$

$$m_{jk}^{(q+1)} = \frac{\sum_{i=1}^{n} t_{ik} x_{ij}}{\sum_{i=1}^{n} t_{ik}} \tag{10}$$

$$\sigma_{jk}^{(q+1)} = \sqrt{\sum_{i=1}^{n} \frac{t_{ik}\left(x_{ij} - m_{jk}^{(q+1)}\right)^2}{\sum_{i=1}^{n} t_{ik}}} \tag{11}$$

Burada təklif olunan metodun yoxlanılması üçün DARPA tərəfindən hazırlanmış KDD CUP 99 verilənlər toplusundan istifadə olunur.

İlkin mərhələdə 6 adda DoS hücum və normal trafik iki sinifə ayrılmış və EM alqoritmi tətbiq olunmuşdur. Amma alınan nəticələr məqsədə uyğun olmamışdır..

Analiz üçün istifadə olunan WEKA aləti İntel Xeon x5670 2 nüvəli 2.93Ghz prosessor və 12Gb əməli yaddaşa sahib olan VMware virtual serverlərinin bazasında quraşdırılmışdır. Təhlil zamanı 10 pilləli kross yoxlama intervalı seçilmişdir.

İki klaster üzrə *k-means* metodunun nəticələrinin xəta faizi 22.8381%-dir. Göründüyü kimi, bu nəticə məqsədə uyğun deyil və reallığı əks etdirmir. Daha sonra eyni verilənlər və eyni şərtlər daxilində EM alqoritmi tətbiq edildi. Bu halda isə klasterizasiyanın nəticələri xəta faizi 41.7308%-dir.

Göründüyü kimi bu nəticələr məqsədə uyğun deyil və reallığı əks etdirmir. Tətqiqat nəticəsində müəyyən olunmuşdur ki, "smurf" DoS hücum trafikinin xüsusiyyətləri normal trafikin xüsusiyyətlərinə yaxındır. Buna görə də klasterizasiyanın nəticələrinin daha dəqiq və dolğun olması üçün, DoS sinfi 2 yerə bölünür. DoS1 (back, teardrop, neptune, land, pod,), DoS2 (smurf). Belə olduğu halda, artıq 3 sinif olur. Bunlar DoS1, DoS2 və NORMAL siniflərdir. Buna uyğun olaraq, 1-ci eksperimentdə göstərilən parametrlər yenidən 3 sinif üçün tətbiq olundu. *k-means* metodu üçün alınan nəticənin xəta faizi 0.843%-dir. Daha sonra

eyni verilənlər və eyni şərtlər əsasında EM alqoritmi tətbiq edildi.və nəticənin xəta faizi 0.8162%-dir.

Klasterizasiya nəticələrinin keyfiyyətinin qiymətləndirilməsi üçün ilkin metrikalar TP, TN, FP, FN istifadə olunur və onların əasasında Rand index, Precision, Recall, F1 metrikalarında hesablanır. Nəticələr aşağıdakı cədvəldə göstərilir:

Beləliklə, təhlükə identifikasiya olunduqdan və onun mənbəyi aşkarlandıqdan sonra təhlükənin nə dərəcədə risqli olması qiymətləndirilir. Təhlükə qiymətləndirildikdən sonra qərarlara dəstək sistemi vasitəsi ilə təhlükə və presedentlər bazası arasında əks-əlaqə yaradılır. Qərarlara dəstək sistemi isə Presedentlər nəzəriyyəsinin metodlarına əsaslanır.

Cədvəl

Klasterizasiyanın keyfiyyət göstəriciləri

Keyfiyyət metrikaları	Klasterizasiya metodları	
	k-means	EM alqoritmi
Rand index ((TP + TN) / (TP + FP + FN + TN))	0.991646	0.992488
Precision (TP / (TP + FP))	0.988831	0.992228
Recall (TP / (TP + FN))	0.991352	0.989909
F1 (((2 * Precision * Recall) / (Precision + Recall)))	0.990090	0.991067

İnformasiya təhlükəsizliyi hadisələrinin təsviri üçün bir sıra yanaşmalar təklif edilib. Qeyd edək ki, konkret hadisənin təsviri tətbiq sahəsi ilə müəyyən edilir və bura tətbiq sahəsi üçün maraqlı olan bütün informasiya daxil edilə bilər. Bu işdə *e* informasiya təhlükəsizliyi hadisəsi formal olaraq aşağıdakı kimi təsvir edilir:

$$e = (Etype, DT, ID, rb, sev, v_1, ..., v_n), \quad (12)$$

burada *Etype* – hadisənin tipini təsvir edir, *DT* – hadisənin başvermə vaxtını bildirir, *ID* – hadisənin aşkarlandığı mənbənin identifikatorlarıdır, *rb* – mənbənin etibarlılıq dərəcəsidir, *sev* – hadisənin risk dərəcəsidir, v_1, ..., v_n – hadisəni təsvir etmək üçün tətbiq sahəsindən asılı olaraq tələb edilən digər atributlardır (məsələn, IP ünvan, protokol, port nömrəsi və s.). v_i atributları tək qiymətlər və ya

elementlər toplusu kimi qiymətlər ala bilər. Eyni tipli hadisələr eyni atributlar çoxluğuna malik olur.

Bütün parametrlər üzrə presendentə yaxınlıq dərəcəsini hesablamaq üçün aşağıdakı düsturdan istifadə etmək olar:

$$sim(i,k) = \frac{\sum_{j=1}^{n} w_j \cdot sim(e_{ij}, e_{kj})}{\sum_{j=1}^{n} w_j}, \qquad (13)$$

w_j – j əlamətinin çəkisi; sim – oxşarlıq metrikası; e_{ij} və e_{kj} – uyğun olaraq cari i hadisəsi və k presedenti üçün e_j əlamətinin qiymətləridir.

Oxşarlıq metrikasının seçilməsi olduqca vacib məsələdir, çünki oxşar presedentlərin axtarışı bu seçimdən çox asılıdır. Adətən, presedentlərin yaxınlıq və ya oxşarlıq metrikası kimi Evklid məsafəsi, Hemminq məsafəsi, Manhetten məsafəsi və s. İstifadə edilir. Hər bir konkret halda metrikanın seçilməsi istifadə edilən informasiyanın fiziki və ya statistik təbiəti də nəzərə alınmaqla aparılır.

İnformasiya təhlükəsizlik xidmətininin əsas xüsusiyyətlərindən biri odur ki, informasiya təhlükəsizliyi hadisələri (kütləvi xidmət nəzəriyyəsi terminləri ilə sifarişlər) müxtəlif sensorlardan (IDS, tətbiqi proqramlar və s.) real vaxt rejimində daxil olur və hər bir hadisə xidmətdən imtina edilmədən emal olunaraq reaksiya verilir.

İnformasiya təhlükəsizliyi xidmətinin iş prosesinin idarə olunması üçün kütləvi xidmət nəzəriyyəsinin M/G/1 modelinin tətbiq edilməsi təklif olunur. Bu növ modellər daha çox verilənlərin emalı prosesində istifadə olunur.

Tutaq ki, kütləvi xidmət sisteminə intensivlikləri $\lambda_i, i = \overline{1, M}$ olan sifarişlərin sadə axını daxil olur. Kütləvi xidmət sistemində (KXS) bir xidmət kanalının olması fərz olunur (informasiya təhlükəsizliyi xidmətinin bir komandası fəaliyyət göstərir). Bu axınlar toplam 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. Kütləvi xidmət sisteminin 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-nə

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-də 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:

$$, \qquad (14)$$

burada $R_j = \sum_{i=1}^{j} P_j$ − 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 $W_1^{AP} = \frac{\lambda_1 b_1^2}{1(1-p_1)}$ alınır.

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

$$w_k^{RP} = \frac{R_{M_1} b_k}{1 - R_{M_1}} + \frac{\sum_{i=1}^{M} \lambda_i b^{(2)}}{2(1 - R_{k-1})(1 - R_k)}, \qquad (15)$$

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:

$$w_k^{WP} = \frac{R_{M_1} b_k}{1 - R_{M_1}} + \frac{\sum_{i=1}^{M} \lambda_i b_i^{(2)}}{2(1 - R_{M_1+M_2})(1 - R)}, \quad k = \overline{M_1 + M_2 + 1, M}, \qquad (16)$$

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

İnformasiya təhlükəsizliyi xidmətinin fəaliyyətinin effektivliyini qiymətləndirmək üçün də təklif edilmiş kütləvi xidmət modelindən istifadə etmək olar.

İnformasiya təhlükəsizlyi xidmətinin real zaman rejimində işləməsi arzuolunandır (ideal haldır), yəni hadisələrin emal sürəti onların daxilolma sürətindən yüksək olmalıdır. Praktikada bu o deməkdir ki, informasiya təhlükəsizliyi hadisələri müəyyən məhdud müddətdə emal olunmalıdır: $T_{p_i} < u_i^*$, burada T_{p_i} sistemin *i*-ci növ hadisəyə reaksiya müddəti, u_i^* – *i*-ci növ hadisənin sistemdə olmasının yolverilən maksimum müddətidir.

Zaman xarakeristiklarına tələblərdən asılı olaraq 3 hala 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 emala tələb edilən vaxt tutumunun riyazi gözləməsi və ikinci başlanğıc momentidir.

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 funksiyası ilə xarakterizə oluna bilər:

$$F = \sum_{i=1}^{M} \alpha_i \lambda_i w_i, \qquad (17)$$

burada α_i – cərimə əmsalıdır, *i*-ci növ hadisənin emalının gecikməsinin vahid zamanda dəyərini müəyyən edir. Gecikmələr, yəni w_i zamanları iki faktordan: cavablandırma qrupunun 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

$$R = \sum_{i=1}^{M} \rho_i = \sum_{i=1}^{M} \lambda_i b_i \tag{18}$$

olur. Lakin b_i hadisənin emalına tələb edilən vaxt ilə cavablandırma qrupunun sürəti ilə müəyyən edilir: $b_i = \dfrac{\theta_i}{B}$, burada B – cavablandırma qrupunun emal sürətidir. Buradan emal sürətinin sərhəd qiyməti üçün

$$B > \sum_{i=1}^{M} \theta_i \tag{19}$$

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.

$$F = \sum_{i=1}^{M} \lambda_i w_i = L, \tag{20}$$

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

Dördüncü fəsildə Şəbəkənin daha səmərəli və təhlükəsiz idarə edilməsini təmin etmək üçün müəyyən qərarların qəbul edilməsinə dəstək verə bilən yeni arxitektur işlənmişdir (şək. 4). Bundan başqa şəbəkə təhlükəsizliyinin intellektual monitorinqi sistemi vaxsitəsilə AzSciencenet şəbəkəsinin və istifadəçilərin profilləri qurulmuşdur.

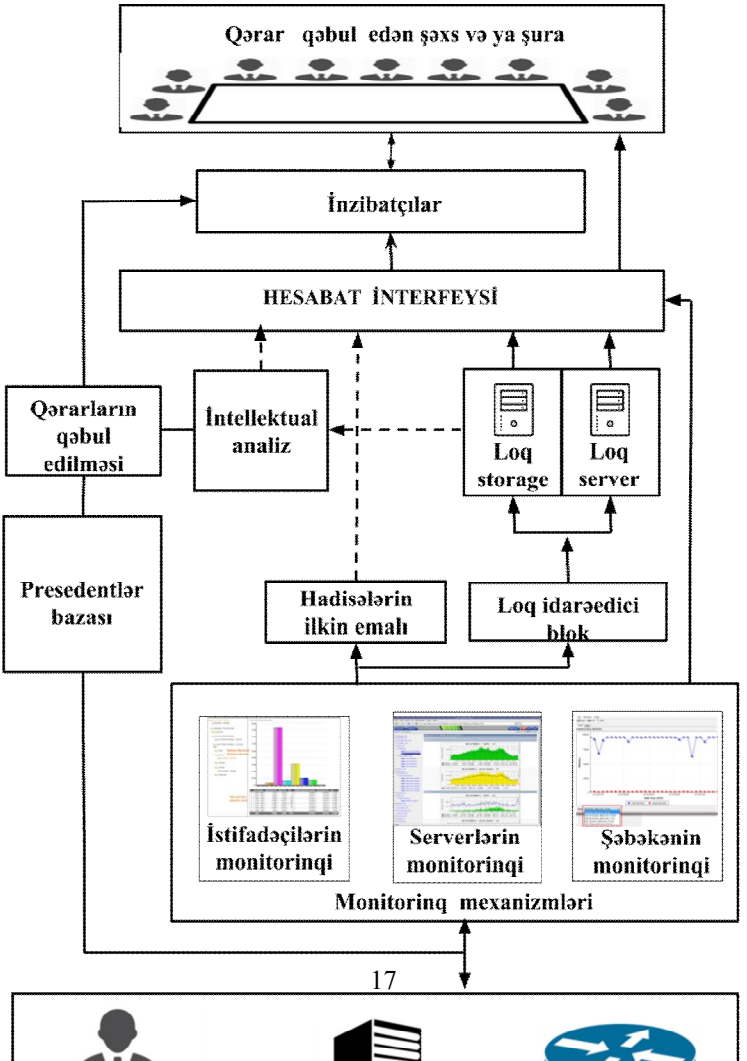
Bu arxitekturda hadisələrin aşkarlanması, təsnifatı və qərarvermə prosesi intellektual analiz metodları vasitəsilə həyata keçirilir. İntellektual analiz metodları şəbəkələrarası ekranlarda realizasiya olunmuşdur və bu baş verə biləcək hadisələrə operativ və birbaşa müdaxilə etmək üçün əlverişlidir.

Şəbəkə Təhlükəsizliyi Əməliyyat Mərkəzi hal-hazırda AzScienceNet şəbəkəsində eksperimental formada fəaliyyət göstərməkdədir. AzScienceNet şəbəkəsində 40 institut və təşkilatlar

üzrə, ümumilikdə 6000-dən çox istifadəçiyə 20-yə yaxın xidmət göstərir. Bunlara misal olaraq, AzCloud xidməti, hostinq xidməti, eduroam xidməti, elektron poçt xidməti, OwnCloud, distant təhsil xidməti, IP telefoniya xidməti, onlayn TV yayımı xidməti, operativ məlumatlandırma sistemi və s. xidmətləri göstərmək olar.

Bu mərkəzin istifadəçi monitorinqi sistemi AMEA rəhbərliyinin qərarı ilə təsdiq olunmuş "İstifadəçi siyasəti" əsasında fəaliyyət göstərir.

Belə mərkəzlərin fəaliyyəti və baş mərkəz altında koordinasiyası gələcəkdə baş verə biləcək hadisələrin qarşısının əvvəlcədən alınmasına kömək edə biləcək.



Şəkil 4. Şəbəkə təhlükəsizliyinin intellektual monitorinqi mərkəzinin arxitekturu.

DİSSERTASİYA İŞİNİN ƏSAS NƏTİCƏLƏRİ

Dissertasiya işi üzrə qoyulmuş məsələlər həll olunmuş və aşağıdakı əsas elmi nəticələr əldə olunmuşdur:

- Şəbəkə təhlükəsizliyinin intellektual monitorinqi sistemlərinin müasir vəziyyəti analiz edilmiş, mövcud elmi-nəzəri problemlər və onların həlli yolları müəyyənləşdirilmişdir;
- Şəbəkə təhlükəsizliyinin intellektual monitorinqi üçün konseptual model işlənmişdir;
- Klasterizasiya əsasında veb trafikdən istifadə və davranış profilinin qurulması metodu işlənmişdir;
- Şəbəkə trafikinin siniflərə ayrılması üçün ikimərhələli klassifikator modeli işlənmişdir;
- DDoS hücumlarının aşkarlanması üçün şəbəkə trafikinin klasterizasiyası metodu təklif edilmişdir;
- Şəbəkə təhlükəsizliyinin monitorinqi üçün qərarların qəbulu metodu işlənmişdir;
- İnformasiya təhlükəsizliyinin monitorinqi sistemi üçün hadisələrin emalı modeli işlənmişdir;
- Şəbəkə təhlükəsizliyinin intellektual monitorinqi mərkəzinin arxitekturu işlənmişdir;
- Təklif olunmuş konseptual model və metodlar əsasında şəbəkənin təhlükəsizliyinin intellektual monitorinqi mərkəzinin arxitekturu işlənmişdir;
- Alınmış elmi-nəzəri və praktiki nəticələr Azərbaycan Milli Elmlər Akademiyasının AzScienceNet şəbəkəsində informasiya təhlükəsizliyi və monitorinq sistemində tətbiq olunmuşdur.

Dissertasiyanın əsas müddəaları aşağıdakı elmi işlərdə dərc edilmişdir:

1. İmamverdiyev Y.N., Nəbiyev B.R. Presedentlər nəzəriyyəsi əsasında şəbəkə təhlükəsizliyinin monitorinqi üzrə qərarların qəbulu metodu // **İnformasiya texnologiyaları problemləri**, 2012, №2, s. 53-58.
2. Nəbiyev B.R. Şəbəkə təhlükəsizliyinin monitorinqi sistemlərinin və vasitələrinin analizi / **Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları 2-ci respublika elmi konfransı,** 27-28 noyabr 2012, Sumqayıt, s.188-189.
3. Nəbiyev B.R. AzScienceNet şəbəkəsinin informasiya təhlükəsizliyi siyasəti haqqında / **Elektron elm problemləri üzrə 1-ci respublika konfransı,** 15-16 noyabr 2012, Bakı, s.57-58.
4. Nəbiyev B.R. Şəbəkə təhlükəsizliyinin monitorinqi üzrə aktual elmi-praktiki problemlərin analizi / **Beynəlxalq İnformasiya Təhlükəsizliyi Gününə həsr olunmuş elmi-praktiki seminar,** 30 noyabr 2012, Bakı, s. 43-48.
5. Nəbiyev B.R. İnformasiya təhlükəsizliyi baxımından kritik vəzifələr üçün tələblər sisteminin formalaşdırılması / **Azərbaycan xalqının ümummilli lideri Heydər Əliyevin 90 illik yubileyinə həsr olunmuş "İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfrans",** 17-18 may 2013, Bakı, s. 128-132.
6. Nəbiyev B.R. AzScienceNet şəbəkəsində informasiya təhlükəsizliyinin monitorinqi sistemi haqqında / **Azərbaycan xalqının ümummilli lideri Heydər Əliyevin 90 illik yubileyinə həsr olunmuş "İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı"**, 17-18 may 2013, Bakı, s. 165-170.
7. Əliquliyev R.M., İmamverdiyev Y.N., Nəbiyev B.R. Şəbəkə təhlükəsizliyinin monitorinqi metodlarinin analizi // **İnformasiya texnologiyaları problemləri**, 2014, №1, s. 60-68.
8. İmamverdiyev Y.N., Nəbiyev B.R. Şəbəkə trafiki üçün multi-klassifikator modeli // **İnformasiya texnologiyaları problemləri**, 2014, №2, s. 68-74.
9. Nəbiyev B.R. Şəbəkə trafikinin klasterizasiya metodu haqqında / **Beynəlxalq telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş "İnformasiya təhlükəsizliyinin multididdiplinar problemləri üzrə II respublika elmi-praktiki konfransı",** 14 2015 may, Bakı, s. 213-215.

10. İmamverdiyev Y.N., Nəbiyev B.R. İnformasiya təhlükəsizliyinin monitorinqi sistemləri üçün kütləvi xidmət modelləri // **İnformasiya texnologiyaları problemləri**, 2016, №1, s. 33-38.
11. Nəbiyev B.R. Veb istifadəçilərin profilinin qurulması metodu / **"Big data:imkanları, multidissiplinar problemləri və perspektivləri I respublika elmi-praktiki konfransı"**, 25 fevral, 2016, Bakı, s. 70-73.
12. Nəbiyev B.R. Şəbəkə təhlükəsizliyinin intellektual monitorinqi üçün konseptual model // **İnformasiya Cəmiyyəti Problemləri**, 2017, №1, s. 81–89.
13. Алгулиев Р.М., Имамвердиев Я.Н., Набиев Б.Р. О методе создания профиля для веб-пользователей // **Известия ЮФУ. Технические науки**, 2017, №7, с. 219-227.
14. İmamverdiyev Y.N., Nəbiyev B.R. Şəbəkə təhlükəsizliyi əməliyyat mərkəzinin arxitektur modeli / **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarı**, 8 dekabr, 2017, Bakı, s. 100-103.
15. Nəbiyev B.R. DDoS hücumların aşkarlanması üçün şəbəkə trafikinin klasterizasiyası metodunun tətbiqi // **İnformasiya Texnologiyaları Problemləri**, 2018, №1, s. 110-120.

Həmmüəlliflərlə dərc olunmuş işlərdə iddiaçının şəxsi rolu:

[1] - presedentlər nəzəriyyəsinin kompüter şəbəkələrinin informasiya təhlükəsizliyinin monitorinqi sistemlərində qərarların qəbulu üçün tətbiqi təklif edilmişdir.
[7] - şəbəkə təhlükəsizliyinin monitorinqi texnologiyalarının müasir vəziyyəti, inkişaf perspektivləri, dünya təcrübəsi araşdırılmış, mövcud problemlər müəyyənləşdirilmişdir.
[8] - kompüter şəbəkələrində trafik axının operativ klassifikasiyası üçün ikimərhələli klassifikator tətbiq edilmişdir.
[10] - informasiya təhülükəsizliyi hadisələrinin emalı proseslərinin modelləşdirilməsi üçün M/G/1 kütləvi xidmət modeli işlənmişdur.
[13] korporativ istifadəçilərin şəbəkə və veb profillərinin müəyyən olunması metodu işlənmişdir.
[14] – intellektual şəbəkə təhlükəsizliyi əməliyyat mərkəzinin arxitektur modeli işlənmişdir.

БАБЕК РАСИМ ОГЛУ НАБИЕВ

РАЗРАБОТКА МЕТОДОВ И АЛГОРИТМОВ ДЛЯ СИНТЕЗА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ МОНИТОРИНГА СЕТЕВОЙ БЕЗОПАСНОСТИ

АННОТАЦИЯ

Целью диссертационной работы является разработка методов и алгоритмов для синтеза интеллектуальной системы мониторинга сетевой безопасности. Разработанная интеллектуальная система мониторинга сетевой безопасности позволяет быстро оценивать сетевую безопасность в режиме реального времени и предоставляет возможность для раннего обнаружения нарушений политики безопасности и быстрой реакции на события.

В рамках диссертационной работы получены следующие основные результаты, обладающие научной новизной:

− разработана концептуальная модель интеллектуальной системы мониторинга сетевой безопасности;

− предложен метод кластеризации для создания поведенческого и пользовательского профиля веб-пользователей;

− предложена двухступенчатая модель последовательного классификатора для классификации сетевого трафика;

− предложен метод рассуждения на основе прецедентов для принятия решений о событиях, выявленных с помощью системы интеллектуального мониторинга;

− разработана модель обработки событий для системы мониторинга информационной безопасности;

− предложена архитектура центра интеллектуального мониторинга сетевой безопасности.

BABAK RASIM OGLU NABIYEV

DEVELOPMENT OF METHODS AND ALGORITHMS FOR SYNTHESIS OF INTELLIGENT NETWORK SECURITY MONITORING SYSTEM

SUMMARY

The main goal of the dissertation is to develop methods and algorithms for the synthesis of an intelligent network security monitoring system. The developed intelligent network security monitoring system allows to assess network security in real time and provides an opportunity for early detection of security policy violations and quick response to events.

In dissertation following new results are obtained:

- a conceptual model of an intelligent system for monitoring network security is developed;
- a clustering method for creating a behavioral and user profile of web users is proposed;
- a two-stage model for the classification of network traffic is proposed;
- case-based reasoning method is used to make decisions about events identified through the intelligent monitoring system;
- a event processing method for the information security monitoring system is developed;
- the architecture of the intelligent network security monitoring center is proposed.

Çapa imzalanıb: 20.04.2018. Tirajı 100 nüsxə.
AMEA İnformasiya Texnologiyaları İnstitutunun
"İnformasiya Texnologiyaları" nəşriyyatı

НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АЗЕРБАЙДЖАНА
ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

На правах рукописи

БАБЕК РАСИМ ОГЛУ НАБИЕВ

РАЗРАБОТКА МЕТОДОВ И АЛГОРИТМОВ ДЛЯ СИНТЕЗА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ МОНИТОРИНГА СЕТЕВОЙ БЕЗОПАСНОСТИ

3338.01 - Системный анализ, управление и обработка информации

А В Т О Р Е Ф Е Р А Т

Диссертации на соискание ученой степени
доктора философии по технике

БАКУ - 2018