UOT 004.09

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

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNİN İNTELLEKTUAL MONİTORİNQİ ÜÇÜN KONSEPTUAL MODEL

Məqalədə şəbəkə təhlükəsizliyinin prinsipial baxımdan yeni və daha effektli olan intellektual monitorinqinin konseptual modeli təklif olunur. Modeldə monitorinq prosesinin ümumi intellektual arxitekturuna, funksional bloklarına, emal proseslərinə və tətbiq istiqamətlərinə baxılır. Bundan başqa, monitorinq sisteminin boşluqları və zəif nöqtələri araşdırılır. Göstərilən problemlərin aradan qaldırılması üçün təklif olunan model problemyönümlü informasiya monitorinqi, toplanan verilənlərin ilkin emalı, verilənlərin indeksləşdirilməsi və strukturlaşdırılması, toplanan informasiyanın saxlanılması və idarə olunması, qərar qəbul edən şəxslərin tələblərinə uyğun informasiyanın seçilməsi və oxunaqlı, analiz edilə bilən hesabatların generasiyası kimi funksional imkanları özündə birləşdirir.

Açar sözlər: *şəbəkə təhlükəsizliyi, monitorinq, süni intellekt, şəbəkə trafiki, konseptual model.*

Giriş

Şəbəkə təhlükəsizliyinin intellektual monitorinqi kompüter şəbəkəsinin təhlükəsizliyini təhdid edən müxtəlif müdaxilələri aşkarlamaq və cavab tədbirləri görmək üçün əlamətlərin və xəbərdarlıqların analizidir. Bu sistemin əsas üstünlüklərindən biri, adından göründüyü kimi, intellektual olmasıdır. İntellektual dedikdə, süni intellekt metodlarının istifadəsi nəzərdə tutulur. Şəbəkə təhlükəsizliyinin monitorinqi süni intellekt metodları tətbiq olunmadan da həyata keçirilə bilər, amma bunun üçün çoxlu maddi vəsait və insan resursları tələb olunur. Süni intellekt metodlarının tətbiqi ilə bu prosesi məqsədəuyğun olaraq qismən və ya tamamilə avtomatlaşdıraraq maddi vəsaitlərə və insan əməyinə qənaət etmək olar. Xüsusi olaraq, şəbəkə təhlükəsizliyinin intellektual monitorinqi sistemində sensorlardan başlayaraq, qərarların qəbul edilməsinə qədər bütün prosesləri süni intellekt metodlarına əsaslanan aparat və proqram təminatlarının tətbiqi ilə reallaşdırmaq məqsədəuyğundur.

Kompüter şəbəkələrinin fəaliyyəti və təhlükəsizliyi haqqında lazımi verilənlərin toplanması, dəqiq analiz edilməsi və şəbəkə təhlükəsizliyinin təmin edilməsi haqqında əsaslandırılmış qərarların qəbul edilməsi üçün şəbəkə təhlükəsizliyinin monitorinqi zamanı verilənlərin intellektual analizi texnologiyalarından istifadə edilməsi aktuallıq kəsb edir [1].

Bu istiqamətdə bir çox elmi-praktiki işlər aparılmışdır. Aparılan işlərin arasında təhdidlərin aşkarlanması və aradan qaldırılması üçün aşağıdakı yanaşmaları misal göstərmək olar: təhlükəsizlik əməliyyatları mərkəzləri (ingiliscə - *security operation center, SOC*), təhlükəsizlik informasiyasının və hadisələrinin idarə olunması (ingiliscə - *security information and event management, SIEM*) və kompüter təhlükəsizliyi insidentlərinə cavabvermə komandaları (ingiliscə - *Computer Security Incident Response Team, CSIRT*).

Şəbəkə təhlükəsizliyi məsələlərinin idarə olunması sistemləri anomal hadisələrin identifikasiyası və müxtəlif növ böyükhəcmli verilənlərin emalı prosesinin reallaşdırılması zamanı çətinliklərlə üzləşir. Belə olduğu halda, alınan məlumatların və verilən qərarların dolğunluğu şübhə doğurur. Şəbəkə təhlükəsizliyi monitorinqinin konseptual modelinin əsas vəzifəsi bu prosesi asanlaşdırmağa və qərar qəbul edilməsinə kömək edərək, hesablama resurslarına və insan əməyinə qənaət etməkdir. Bunun üçün də müxtəlif aparat, proqram və alət vasitələrindən istifadə olunur.

Bu işdə şəbəkə təhlükəsizliyinin intellektual monitorinqi üçün konseptual model təklif edilir.

Şəbəkə təhlükəsizliyi sistemləri

Şəbəkə təhlükəsizliyinin intellektual monitorinqi kompleks bir sistemdir. Bu cür sistemlər daha geniş verilənlərlə və böyük miqyasda işlədiyi üçün hazır həllərin tapılması çox çətindir.

Şəbəkə təhlükəsizliyi üzrə birləşmiş sistemlər mərkəzləşdirilmiş, paylanmış və ya qismən mərkəzləşmiş struktura malik ola bilərlər. Mərkəzləşdirilmiş sistemlərdə seqmentlər üzrə toplanan bütün verilənlər analiz üçün mərkəzə ötürülür. Bu strukturun üstün cəhəti ondadır ki, verilənlər tam ötürüldüyü üçün daha dəqiq cavab əldə etmək mümkündür. Mənfi cəhəti isə odur ki, analiz aparatı mərkəzləşmiş olduğu üçün yüklənmə yüksək olduqda xidmətdən imtina qaçılmaz ola bilər. Bu növ sistemlərdə yeganə imtina nöqtəsinin olması qəbulolunmazdır. Digər tərəfdən baxdıqda isə, paylanmış, yəni verilənlərin analizi üçün yeganə mərkəzə bağlı olmayan strukturlar mövcuddur. Paylanmış sistem tam və ya qismən mərkəzləşdirilmiş ola bilər. Tam paylanmış strukturda ayrı-ayrılıqda bütün seqmentlər və onların fəaliyyət blokları eynihüquqludur. Yəni bir seqmentin sıradan çıxması ümumi strukturun iş fəaliyyətinə cuzi təsir göstərəcək. Buna baxmayaraq, verilənlərin və analiz prosesinin lokal seqmentlə məhdudluğu nəticələrin dolğunluğuna mənfi təsir göstərir. Qismən mərkəzləşdirilmiş strukturda isə müəyyən hallarda bir və ya bir neçə seqment analiz prosesini öz üzərinə götürür. Amma bu halda da analiz prosesini öz üzərinə götürmüş seqment digərlərinə nisbətən daha çox yüklənmiş olur. Bunun üçün də tam paylanmış və mərkəzləşdirilmiş sistemlər arasında balanslaşdırılmış və qismən mərkəzləşdirilmiş sistem qurulması vacibdir.

Şəbəkə təhlükəsizliyinin təmin olunması üçün artıq lokal tədbirlərin lazımi qədər effektli olmadığı [2]-də göstərilmişdir. Məsələn, artıq klassik müdaxilələrin aşkarlanması sistemlərinin (ingiliscə - *Intrusion Detection System, IDS*) kifayət qədər effektli olmadığı məlumdur və bunun üçün müdaxilələrin aşkarlanması şəbəkəsinin qurulması labüddür. Buna [3]-də qeyd olunan *DOMINO Overlay* qlobal müdaxilələrin aşkarlanması şəbəkəsini misal göstərmək olar. *DOMINO Overlay* müdaxilələrin aşkarlanması üzrə əməkdaşlıq sistemi olub, böyükmiqyaslı və genişzolaqlı İnternet qovşaqlarında müdaxilələrin aşkarlanması prosesinə cavabdehdir. Bu sistem coğrafi baxımdan müxtəlif yerlərdə yerləşib və iyerarxik-heterogen struktura malikdir, buna baxmayaraq, şəbəkə aktorları arasında informasiya mübadiləsi mövcuddur.

Şəbəkə təhlükəsizliyi hadisələrinin aşkarlanması və aradan qaldırılması üçün daha bir yanaşma *SIEM*-dir. *SIEM* vendorların təklif etdiyi həllərə uyğun olaraq müxtəlif funksionallıqda ola bilər. Amma bütün bu *SIEM*-lərin hamısının ortaq cəhətləri vardır. *SIEM*-in fundamental və ya aparıcı hissələri aşağıdakı kimidir: toplama, analiz/aqreqasiya, saxlama.

Təhlükəsizlik əməliyyatları mərkəzləri təşkilati və texniki təhlükəsizlik məsələləri ilə məşğul olan mərkəzlərdir. Bu mərkəzin əməliyyat qabiliyyəti isə aşağıdakı bloklar əsasında realizasiya olunur: verilənlərin generatoru olan sensorlar, verilənlərin saxlanılması üçün toplama bloku, ümumi formata uyğunlaşdırılmış verilənlər bazası, insidentlərin analizi, biliklər bazası, qərar və hesabat.

CSIRT informasiya təhlükəsizliyi insidentlərinə cavabvermə qrupudur. Onun əsas məqsədi korporativ şəbəkədə informasiya təhlükəsizliyi risklərinin qəbul edilmiş səviyyədə idarə edilməsini təmin etməkdir. Bu məqsədlə *CSIRT* informasiya təhlükəsizliyinin pozulmasına yönəlmiş hərəkətlərin aşkarlanması, qarşısının alınması və istifadəçilərin məlumatlandırılması prosesini yerinə yetirir. *CSIRT* korporativ şəbəkədə ziyanlı proqramların yayılması və şəbəkə hücumları ilə əlaqədar statistik verilənlərin toplanmasını, saxlanılmasını və analizini həyata keçirir [5]. Qarşıya qoyulmuş vəzifələrin yerinə yetirilməsi üçün *CSIRT* informasiya təhlükəsizliyi sahəsində fəaliyyət göstərən digər təşkilatlarla qarşılıqlı əlaqə saxlamalıdır.

Yuxarıda informasiya təhlükəsizliyinin təmin olunması üçün təşkilati və praktiki sistemlər göstərilmişdir. Bu sistemlərin əsas tərkib hissəsi, monitorinq və onun nəticəsində əldə olunan məlumatlardır. Bu məqalədə təklif olunan konseptual model daha operativ və dolğun nəticələr əldə etməyə şərait yaradacaqdır.

Konseptual modelin qurulması prinsipləri

Şəbəkə təhlükəsizliyinin intellektual monitorinqi şəbəkə haqqında informasiyanın toplanması, analizi və nəticələri haqqında məlumatları əlaqədar şəxslər və ya sistemlərə yönləndirən, müasir tələbləri ödəyən, proqram və aparat komplekslərindən ibarət olan mürəkkəb bir sistemdir. Monitorinq sistemi bir çox funksiyaların yerinə yetirilməsini təmin edir ki, bu da şəbəkənin səmərəliliyinin artırılmasına gətirib çıxarır.

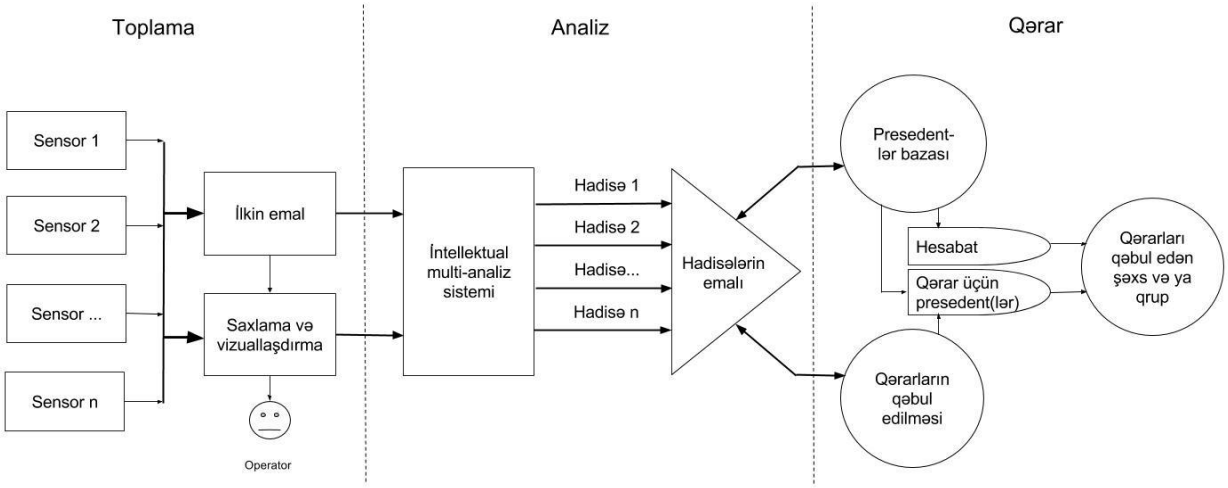
Bu sistem lazım olan informasiyanı sensorların köməyi ilə kompüter şəbəkəsindən, kompüter sistemlərindən, istifadəçilərdən və s. məlumat mənbələrindən toplayır. Həmin məlumatların toplanması, saxlanması, emal olunması və vizuallaşdırılması ayrı-ayrılıqda ağır, çətin və çoxlu insan əməyi tələb edən prosesdir. Amma heç də az vacib olmayan məsələlərdən biri də verilənlərin düzgün interpretasiya olunmasıdır. Yuxarıda qeyd etdiyimiz kimi, burada da insan amili, şübhəsiz, müstəsna əhəmiyyətə malikdir. Belə olduğu halda, tələb olunur ki, müdaxilələrin aşkarlanması sistemi təhlükələri nəyə əsasən təyin etdiyini düzgün interpretasiya etsin. Bu mərhələdə buraxılan hər hansı səhv kompüter şəbəkəsinin təhlükəsizliyinə nəzarətin itirilməsinə gətirib çıxara bilər.

Şəbəkə təhlükəsizliyinin intellektual monitorinqi vəzifələrinə gəldikdə isə, əsas siyasət müəyyən olunmalıdır. Bu siyasət istifadəçilərin qlobal və lokal şəbəkədən istifadəsini etibarlı və təhlükəsiz etməklə yanaşı, informasiyanın toplanaraq analiz edilməsi üçün də vacibdir. Bu, baş verəcək hadisənin qarşısını almaq və ya baş vermiş hadisəni tədqiq etmək üçün olduqca əhəmiyyətlidir.

Yuxarıda deyilənləri nəzərə alaraq, ilk növbədə, bu sistemin konseptual arxitekturunun qurulması vacibdir. Bu, konseptual arxitektur əsasında hər blok üzrə tələblər müəyyən olunaraq, reallaşdırma prosesinə asan keçid təmin olunacaq.

İntellektuallıq bloklarda ayrı-ayrılıqda süni intellekt modelinin tətbiqi ilə bitmir. Konseptual arxitektur bir çox lokal, regional və bir qlobal mərkəzi özündə birləşdirir, bu isə iyerarxik quruluş yaradır. Konseptual modeldə eyniranqlı bloklar müəyyən olunaraq onların arasında informasiya mübadiləsinə şərait yaradılsa, problemin daha aşağı səviyyələrdə həll olunması mümkün olur. Yəni səviyyəsindən asılı olaraq, baş verən problemlərin operativ və minimal maddi zərərlə aradan qaldırılması üçün, ilkin olaraq, lokal səviyyədə həll olunmağa cəhd edilməlidir.

Şəbəkə təhlükəsizliyinin intellektual monitorinqinin konseptual arxitekturu vəzifə və funksiyalar, proseslər və sensorlar, sistemlər, istifadə edilən müasir texnologiyalar da daxil olmaqla yaradılır. Şəkil 1-dən göründüyü kimi, arxitektur ümumi olaraq toplama, analiz və qərar bloklarından ibarətdir. Hər bir blok tərkibində müəyyən funksiyaları yerinə yetirən alt bloklardan ibarətdir. Bunları geniş formada aşağıda izah etməyə çalışacağıq.



Şəkil 1. Şəbəkə təhlükəsizliyinin intellektual monitorinqinin konseptual arxitekturu.

Toplama bloku

Toplama (Sensorlar) - Şəbəkə haqqında informasiyanın toplanması üçün müxtəlif növ sensorlar istifadə olunur. Bu sensorlar avtonom fəaliyyət göstərə və ya bir mərkəzdən idarə oluna bilərlər. Sensorların sayları və növləri monitorinqi aparılan şəbəkənin profilinə və miqyasına görə dəyişə bilər. Sensorların sinfi onların topladığı verilənlərin xarakterinə görə müəyyən olunur. Ümumi formada sensorları 2 sinfə bölmək olar: aparat sensorları və proqram sensorları. Amma bu sensorlar da toplanan informasiyanın tipinə görə altsiniflərə bölünürlər (trafik, proses, istifadəçi aktivliyi sensorları və s.). Aparat sensorları dedikdə, ümumi qəbul olunmuş monitorinq sensoru olan *SNMP*, *IPFIX*, *sFlow* və s. nəzərdə tutulur. İstehsalçıya aid xüsusi aparat sensorları da mövcuddur, məsələn: *Cisco-netflow*, *Microsoft - Windows Network Card Sensor* və s. Proqram sensorlarına, *PRTG - Packet Sniffer Sensor*, *Core Health Sensor*, *ClusterState Sensor* və s. misal göstərmək olar. Bu sensorlar müəyyən olunmuş mənbələrdən generasiya olunan aktivliyi loqlaşdırmaq üçündür.

Genişzolaqlı şəbəkələrin monitorinqi üçün trafik axınının toplanması və analizi çox yayılmış metodlardan biridir. Bu yanaşma provayderlər səviyyəsində daha çox aktualdır. Trafik axının toplanması üçün *NetFlow*, *IPFIX* və s. protokolları istifadə olunur. Trafik axınının monitorinq mərhələləri bir-biri ilə sıx əlaqəlidir və hər bir mərhələ diqqətlə öyrənilməlidir [6]. Bu mərhələlərə paketin müşahidəsi, axının ölçülməsi və ötürülməsi, verilənlərin toplanması və analizi aiddir.

Şəbəkədə yerləşdirilən sensorlar vasitəsilə trafiki paketlər səviyyəsində analiz etmək mümkündür. Paketlər əsasında monitorinq, daha genişmiqyaslı trafik axınının monitorinqi metoduna tam əks olan metoddur və daha detallı informasiya əldə etməyə imkan verir. Amma bu prosesin reallaşdırılması istifadəçilərin şəxsi məlumatlarına təhlükə yaradır və emal prosesi üçün güclü prosessor, böyük əməli yaddaş tələb edir. [7]-də paketin yalnız birinci dörd baytını qeyd etməklə daha az resurs tələb edən monitorinq metodu təklif olunur.

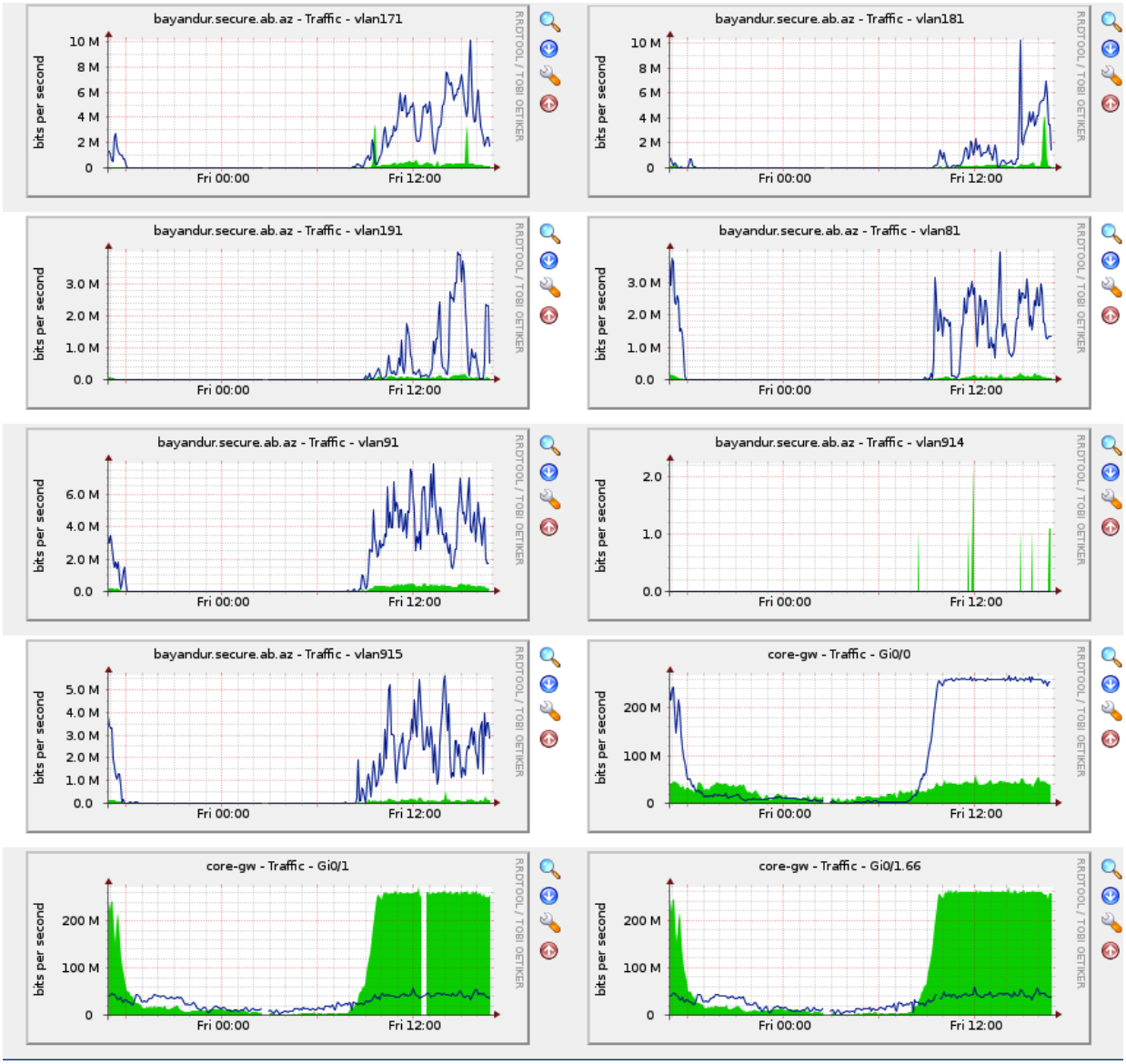
İlkin emal - verilənlər müxtəlif sensorlardan və müxtəlif formatlarda generasiya olunduğu üçün, ilkin olaraq, aqreqasiya prosesindən keçirilir və bir qayda olaraq, bütün verilənlər bir formata çevrilir. Bu proses konsalidasiya adlanır. Aqreqasiya prosesindən keçən verilənləri korrelyasiya edərək, hücumun müxtəlif hissələrini eyni şəkildə toplayaraq dolğun məlumat almaq mümkündür.

Saxlama - alınan məlumatlar korporativ siyasətə əsasən, müəyyən vaxt ərzində saxlanılır. Şəbəkə strukturunun, xidmətlərin və istifadəçilərin generasiya etdiyi informasiya zaman keçdikcə böyük informasiya kütləsinə çevriləcəyi hamıya məlumdur. Bunu bildiyimiz üçün oflayn rejimdə informasiyanın saxlanılması üçün müəyyən təsnifat rejimindən keçərək qüvvədə olan siyasətə uyğun olan və anomaliya aşkarlanmayan verilənlər daimi yaddaşda saxlanılmır.

Yalnız anomallıq aşkarlanan verilənlərin yaddaşda saxlanılması verilənlərin yenidən analizi zamanı müəyyən informasiya çatışmazlıqlarına gətirib çıxara bilər, amma bu son nəticədə limitsiz olmayan resursların düzgün istifadəsi üçün yararlı olacaqdır.

Şəbəkə trafiki verilənlərinin toplanması və saxlanması şəbəkələrin böyüməsi və sürətlənməsi ilə əlaqədar olaraq daha çətin olur, *SQL* verilənlər bazası və xüsusi binar format kimi həllər, daxil olan verilənlərin artma tempinə uyğun genişlənə bilmirlər. [8]-də *nProbe* şəbəkə trafikinin toplanması alətinin və *FastBit* verilənlər bazasının sintezindən yaradılmış açıq kodlu proqram təminatıdır. Bu metod vasitəsilə *Gbit* sürətə qədər şəbəkə trafiki axınının toplanılması və lazımi anda hər hansı bir informasiyanın axtarılması və tapılması mümkün olur.

Vizuallaşdırma – şəbəkə trafiki haqqında ümumi ədədi məlumatların başa düşülməsi üçün əyani görünüş forması olub, operatorlar üçün ilkin müşahidə vasitəsidir. Buna *Cacti*, *Nagios* və s. açıq kodlu proqram təminatlarını misal göstərmək olar. Bu alətlər kompüter şəbəkəsi trafikini, hesablama nöqtələrinin vəziyyətini və avadanlıqlar haqqında statistik informasiyanı müəyyən vaxt intervalında *SNMP* vasitəsilə toplayaraq qrafiklər yaradır (Şəkil 2).



Şəkil 2. Şəbəkə trafikinin diaqram formasında vizuallaşdırılması

Analiz bloku

Şəbəkə trafikinin identifikasiyası və kateqoriyalaşdırılması onun idarə olunmasının əsas elemetlərindən biridir. Buna axının prioritetləşdirilməsi, trafikin formalaşdırılması və diaqnostik monitorinqi misal göstərmək olar.

İnternet trafikinin ölçmələrini, adətən, yüksək hesablama gücünə malik olan serverdə həyata keçirilir. Server trafik axını və paketləri toplayır və analiz edir. Nəzərə alsaq ki, uzunmüddətli, böyükhəcmli və böyükmiqyaslı statistik verilənlərin monitorinqi zamanı Tera və Peta bayt həcmdə verilənlər generasiya olunur və bu emal prosesinin bir serverdə aparılması məqsədəuyğun deyil. Adətən, böyük həcmdə informasiyanın sıxılması üçün diskretizasiya və ya aqreqasiya metodları istifadə edilir, bu halda trafik axınının müəyyən verilənləri ixtisar olunur. Son zamanlar bu məsələnin həlli üçün bulud hesablama texnologiyaları və klaster fayl sistemlərindən istifadə edilir. Buna misal olaraq, İnternet trafikinin analizi üçün bulud hesablamaları əsasında *MapReduce* proqram platformasının istifadə olunması təklif olunur [9]. Açıq kodlu proqram təminatı olan *MapReduce* və *Hadoop* əsasında aparılan təcrübələrə əsasən müəyyən olunmuşdur ki, bir serverli hesablama alətinə nisbətən statistik trafikin hesablaması zamanı nəticə 72% daha sürətli əldə edilir.

Şəbəkənin idarə olunması və şəbəkə təhlükəsizliyinin səmərəliliyinin yüksəldilməsinə yönəlmiş tədqiqatlarda trafikin klassifikasiyasından və klasterləşdirilməsindən geniş istifadə olunur. İnternetdən geniş istifadə olunması, protokolların və tətbiqi proqramların inkişafı ilə trafikin analizi sahəsində də tədqiqatların aparılması aktuallaşmışdır. İnformasiya təhlükəsizliyi hadisələrinin və ya anomaliyalarının aşkarlanması üçün klassifikasiya və klasterləşdirmə metodlarından geniş istifadə olunur. Misal olaraq, [10]-da *Naive Bayes* və neyron şəbəkə metodlarından istifadə edərək operativliyi və ya dəqiqliyi azaltmadan klassifikasiya xarakteristikalarını yüksəltmək məqsədilə iki mərhələli ardıcıl klassifikator təklif edilir.

Məlumdur ki, təhlükələrin yaranmasının əsas səbəblərindən biri şəbəkə trafikində anomal və tematik profilə uyğun olmayan trafikin generasiya olunmasıdır. Bunları nəzərə alaraq [11]-də şəbəkə trafikində davranış profilinin müəyyən olunması üçün vasitə işlənib hazırlanmışdır. Davranış profilinin müəyyən olunması üçün k-ortalar klasterizasiya metodu tətbiq olunmuşdur.

[12]-da isə şəbəkə trafikinin real vaxt rejimində identifikasiyası və klassifikasiyası prosesinin reallaşdırma metodu təklif olunur. Bunun üçün altı maşın təlimi alqoritmi (*AdaboostM1, C4.5, Random Forest tree, MLP, RBF və Polykernel ilə SVM*) tətbiq edilir. Bu reallaşdırma göstərir ki, ağac tipli maşın təlimi metodu trafikin klassifikasiyası və identifikasiyası üçün effektlidir və İnternet trafikinin klassifikasiya dəqiqliyi 99.76.16% təşkil edir.

Qərar bloku

Qərarların qəbul olunması - İnformasiya təhlükəsizliyinin emalı üzrə qəbul edilmiş qərarlar bir çox halda əvvəllər qazanılmış təcrübəyə və qəbul edilmiş qərarlara əsaslanır, onları yeni situasiya üçün adaptasiya edir. Bunları nəzərə alaraq, insanın iştirakını minimuma endirmək və reaksiyanın operativliyinin yüksəldilməsi məqsədi ilə ekspert sistemlərindən istifadə olunmalıdır. Bizim təklif etdiyimiz arxitektur daxilində bu prosesin idarə olunması üçün presedentlər nəzəriyyəsi (ing., *Case-Based Reasoning, CBR*) seçilmişdir.

CBR metodologiyasının mahiyyəti aşağıdakından ibarətdir: Faktiki olaraq, presedent <problem, həll metodu> cütüdür. Zaman keçdikcə meydana çıxan situasiyalar və onların həlli yolları xüsusi bazada – presedentlər bazasında saxlanılır. Yeni situasiya yarandıqda presedentlər bazasında oxşar situasiya axtarılıb tapılır və onun həll metodu baxılan situasiyaya adaptasiya olunur. *CBR* metodologiyası diaqnostika, proqnozlaşdırma, müxtəlif predmet sahələrində planlaşdırma və layihələndirmə işlərində və bir çox klassifikasiya məsələlərinin həllində istifadə edilir. *CBR* informasiya təhlükəsizliyinin müxtəlif aspektlərinə [13]-də baxılmış, risklərin qiymətləndirilməsinə, müdaxilələrin aşkarlanmasına, şəbəkə təhlükəsizliyi vəziyyətinin analizinə də tətbiq edilmişdir.

Presedentlər bazası – əvvəlcədən aşkarlanmış və müvafiq tədbir görülmüş insidentlərin həlli yolları bu bazada yerləşdirilir. Yəni, hazır həllər yaddaşı kimi mərkəzdə presedentlər bazası yerləşdirilib. Yeni bir problem baş verdikdə o əlamətlərin vektor funksiyası ilə bazada qeydiyyatdan keçirilir, bu da presedentlər bazasından problemlərin axtarılmasını təmin edir. Aydındır ki, funksiyaların oxşarlıq səviyyəsi nə qədər çox olarsa, presedentlərin axtarış effektivliyi də bir o qədər yüksək olar.

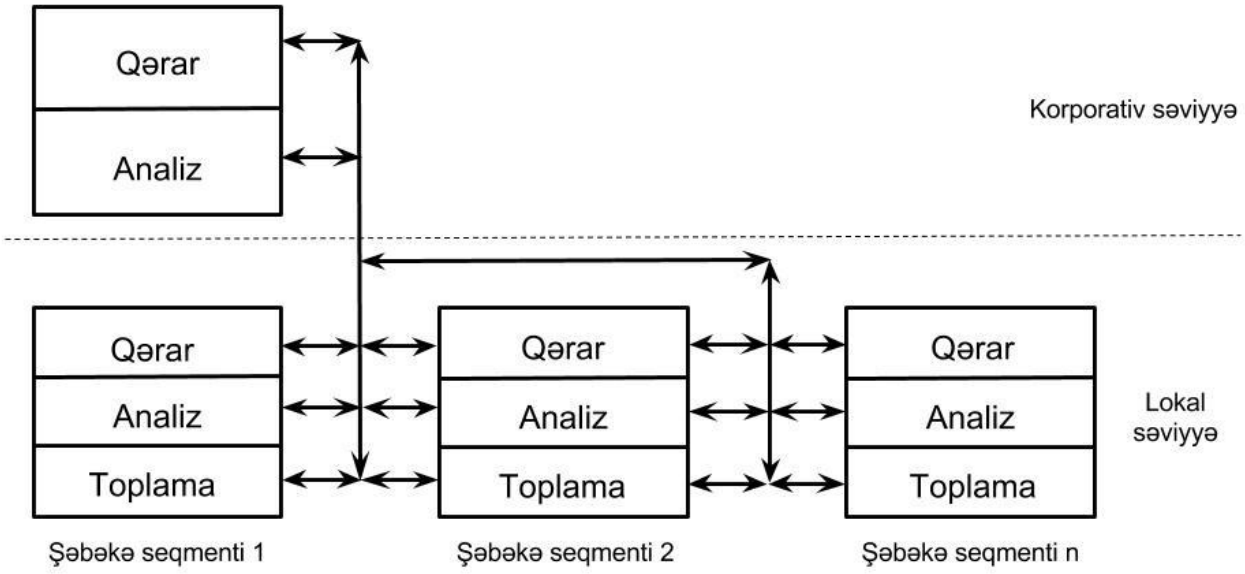
Qərarları qəbul edən şəxs və ya qrup – presedentlər bazasında uyğun presedent tapılmadığı halda qərar əvvəlcədən müəyyən olunmuş ekspertlər tərəfindən qəbul olunur.

Qərarlara dəstək sistemi hər iki halda – uyğun presedent tapıldığı və tapılmadığı halda qəbul olunmuş qərarı təhlükəni zərərsizləşdirmək üçün proseslərə və eyni zamanda, hesabat formasında aidiyyatı şəxslərə ötürür. Yeni insidentlər və onların həlləri dəqiqləşdirildikdən sonra bu həllər yekun qərar vermək hüququ olan aidiyyatı şəxslər tərəfindən hazır həllər bazasına ötürülür.

Konseptual modelin makro-arxitekturu

Yuxarıda göstərilən şəbəkə təhlükəsizliyinin intellektual monitorinqinin konseptual modelinin arxitekturunun təsir dairəsi bir lokal şəbəkə daxilindədir. Buna görə də, bir lokal şəbəkə daxilində baş verən proseslərə nəzarət və ona uyğun qərarlar generasiya edə bilir. Bir korporativ şəbəkə altında müxtəlif şəbəkələrin varlığını nəzərə alsaq, baş vermiş insident ya ümumiyyətlə, vəziyyət haqqında şəbəkələrarası monitorinq verilənlərinin mübadiləsinin, informasiya təhlükəsizliyi nöqteyi nəzərindən vacib olduğunu başa düşərik. Yuxarıda deyilənlərə əsaslanaraq, iyerarxik struktura malik olan şəbəkə təhlükəsizliyinin intellektual monitorinqinin konseptual modelinin makro-arxitekturunun formalaşması vacibdir.

Şəkil 3-də konseptual modelin iyerarxik makro-arxitekturu göstərilmişdir və onun iki səviyyəsi vardır: korporativ və lokal. Təklif olunan konseptual model hər bir səviyyə və onun seqmentləri üzrə ayrı-ayrılıqda tətbiq olunur. Lokal səviyyədə yerləşən blokların hər biri ayrıca korporativ şəbəkəni təmsil edir və müxtəlif böyüklükdə ola bilməklə yanaşı, müxtəlif regionda, müxtəlif saat qurşaqlarında yerləşə bilər. Bundan asılı olmayaraq, hər bir blok ayrı-ayrılıqda avtonom fəaliyyəti və informasiya mübadilə qabiliyyəti ilə təmin olunmalı və bütün infrastruktura inteqrasiya edilməlidir. Yəni, bloklar ayrı-ayrılıqda lokal bir strukturun tərkib hissəsi olsalar da, hər bir blok bütün konseptual arxitektur üzrə özünün analoqu olan bloklara aktiv informasiya mübadiləsi edərək, anomallıq və özü haqqında aktual informasiyanı paylaşa bilməlidir.



Şəkil 3. Şəbəkə təhlükəsizliyinin intellektual monitorinqinin konseptual makro-arxitekturu

Şəkil 3-dən göründüyü kimi, qlobal səviyyədə yerləşən blokun toplama funksiyası yoxdur. Bu blokun əsas vəzifələri aşağı səviyyəli blokların iş fəaliyyətinə nəzarət, xüsusi hallarda lokal səviyyədə yerləşən blokların emal edə bilmədiyi hadisələrə reaksiya vermək və həllər generasiya etməkdir.

Nəticə

Bu məqalədə korporativ şəbəkənin bütün elementlərini, istifadəçilərini, texnologiyalarını, verilənlərini əhatə edən və informasiya təhlükəsizliyi hadisələrinin müəyyən olunmasını təmin edən şəbəkə təhlükəsizliyinin intellektual monitorinqinin konseptual modeli təklif edilir. Əsas məqsəd bütün korporativ şəbəkəni və onun altşəbəkələrini real zaman anında əhatə edərək, şəbəkənin hər hansı bir yerində baş verə biləcək hadisəyə anında və dolğun reaksiya verməkdir. Aktual olan şəbəkə təhlükəsizliyi məsələlərinin idarə olunması kommersiya məhsullarının aşkarlama, emal etmə və qərar vermə proseslərini realizasiya etmək qabiliyyətindədir.

Ədəbiyyat

1. Əliquliyev R.M., İmamverdiyev Y.N., Nəbiyev B.R. Şəbəkə təhlükəsizliyinin monitorinqi metodlarının analizi // İnformasiya Texnologiyaları Problemləri, 2014, № 1, s. 60–68.
2. Fung C.J., Boutaba R. Design and management of collaborative intrusion detection networks / International Symposium on Integrated Network Management, 2013, pp. 955-961.
3. Yegneswaran V., Barford P., Jha S. Global Intrusion Detection in the DOMINO Overlay System / Proc. of the Network and Distributed System Security Symposium, 2004, pp.1–17.
4. Fataliyev Z., Imamverdiyev Y.N. Security Operation Center Architecture for E-government based on Big Data Analysis / Elektron dövlət quruculuğu problemləri I Respublika elmi-praktiki konfransı. Bakı, 2014. pp. 140–144.
5. Hofstede R., Celeda P., Trammell B., Drago I., Sadre R., Sperotto A., Pras A. Flow Monitoring Explained: From Packet Capture to Data Analysis with NetFlow and IPFIX // IEEE Communications Surveys & Tutorials, 2014, vol. 16, pp. 2037-2064.
6. Deri L., Lorenzetti V., Mortimer S., Collection and Exploration of Large Data Monitoring Sets Using Bitmap Databases / Second International Workshop Traffic Monitoring and Analysis, 2010, pp 73–86.
7. Giura P., Memon N., NetStore: An Efficient Storage Infrastructure for Network Forensics and Monitoring / Proc. of the International Symposium on Recent Advances in Intrusion Detection, 2010, pp. 277–296.
8. Lee Y., Kang W., Son H., An Internet Traffic Analysis Method with MapReduce // Proc. of the IEEE/IFIP Network Operations and Management Symposium Workshops (NOMS Wksps), 2010, pp. 357 – 361.
9. İmamverdiyev Y.N., Nəbiyev B.R. Şəbəkə trafiki üçün multi-klassifikator modeli // İnformasiya Texnologiyaları Problemləri, 2014, № 2, s. 60–68.
10. Nəbiyev B.R. Şəbəkə trafikinin klasterizasiya metodu haqqında / Beynəlxalq telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, Bakı, 2015, s. 213–215.
11. Jaiswal R. C., Lokhande S. D. Machine learning based internet traffic recognition with statistical approach / Proc. of the Annual IEEE India Conference, 2013, pp. 1–16.
12. İmamverdiyev Y.N., Nəbiyev B.R. Presedentlər nəzəriyyəsi əsasında şəbəkə təhlükəsizliyinin monitorinqi üzrə qərarların qəbulu metodu // İnformasiya Texnologiyaları Problemləri, 2012, № 2, s. 53–58.

УДК 004.09

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

Концептуальная модель интеллектуального мониторинга сетевой безопасности

В этой статье предлагается принципиально новая и более эффективная концептуальная модель интеллектуального мониторинга сетевой безопасности. В этой статье рассматриваются интеллектуальная модель процесса мониторинга, функциональные блоки, процессы и тенденции в области применения. Кроме того, рассматриваются уязвимости и недостатки системы мониторинга. Предложенная модель для устранения вышеупомянутых проблем сочетает в себе функциональные возможности, мониторинг проблемно-ориентированных информаций, первоначальную обработку собранных данных, индексацию данных, структурирование данных, хранение и управление собранной информацией, предоставление отчетов, которые могут быть проанализированы по запросам лиц, принимающих решения.

Ключевые слова: *сетевая безопасность, мониторинг, искусственный интеллект, сетевой трафик, концептуальная модель.*

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

Conceptual model of intelligent network security monitoring

This paper proposes fundamentally new and more effective conceptual model of intelligent network security monitoring. General intellectual model of the monitoring process, functional blocks, processes and trends in the application are considered. In addition, the gaps and weak points of monitoring system are considered. The proposed model for the elimination of the above-mentioned problems combines functional capabilities such as the monitoring of problem-oriented information, initial processing of gathered data, data indexation and structuring, storage and management of collected information, selection of information in accordance with decision makers' requirements generation of readable information that can be analyzed.

Keywords: *network security, monitoring, artificial intelligence, network traffic, conceptual model.*