UOT 004.056

***Əliquliyev R.M.*[1]*, İmamverdiyev Y.N.*[2]*, Nəbiyev B.R.*[3]**
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]rasim@science.az, [2]yadigar@lan.ab.az, [3]babek@iit.ab.az

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNİN MONİTORİNQİ METODLARININ ANALİZİ

Kompüter şəbəkələrinin fasiləsiz və etibarlı fəaliyyətinin təmin edilməsi üçün şəbəkə təhlükəsizliyinin monitorinqi olduqca aktual məsələdir. Bu məqalədə şəbəkə təhlükəsizliyinin monitorinqi üzrə məqsədlər və funksiyalar müəyyən edilmiş, şəbəkə təhlükəsizliyinin intellektual monitorinqi metodları, o cümlədən şəbəkə trafikinin klassifikasiyası və klasterizasiyası metodları tədqiq olunmuş və bu istiqamətdə bir sıra aktual tədqiqat məsələləri müəyyən edilmişdir.

Açar sözlər: *informasiya təhlükəsizliyi, şəbəkə təhlükəsizliyinin monitorinqi, şəbəkə trafikinin analizi, trafikin klassifikasiyası, trafikin klasterizasiyası.*

Giriş

Müasir dünyada informasiya texnologiyaları vasitəsilə həll olunan məsələlərin miqyasının və emal olunan informasiyanın həcminin kəskin artması, proqram və aparat təminatlarının mürəkkəbləşməsi, qlobal şəbəkədə hədəfə yönəlik təhdidlərin geniş yayılması, yeni növ təhdidlərin yaranması informasiyanın emalı prosesini mürəkkəbləşdirir. Bütün bu proseslər informasiya resurslarında təhdidlərin və boşluqların miqyasının və təsirinin artmasına gətirib çıxarır. Bu hadisələrin fonunda aydın olur ki, kritik infrastrukturların qarşılıqılı əlaqəli və asılı olması onların hər gün yeni risklərə məruz qalmasına səbəb ola bilər. Bu asılılıqlar potensial təhdidləri kaskad effekti ilə bütün sistemin təhlükəsizliyinə təsir edə biləcək formada yaya bilər. Buna görə də mövcud olan kompüter şəbəkələrinin (KŞ) monitorinqi metodlarını təkmilləşdirmək tələb olunur. Məsələn, [1]-də göstərilmişdir ki, təhlükəsiz və etibarlı intellektual sistemlərin yaradılması üçün monitorinqin tələblərinin və təhdidlərin aşkarlanmasının metodları müəyyən olunmalıdır.

Yuxarıda sadalananlar KŞ-ların fasiləsiz və etibarlı fəaliyyətinin təmini üçün və ümumilikdə, KŞ-ların təhlükəsizliyi üçün fasiləsiz monitorinq məsələsini aktual edir. Aktual məsələlərdən biri də təhlükəsizliyin siyasətə əsaslanan idarə olunmasıdır – təşkilatda bəyan edilən təhlükəsizlik siyasətinin KŞ–da realizasiyasına nəzarət olunmalıdır. [2]-də təhlükəsizlik siyasətinin və təhlükəsizlik mexanizmlərinin fəaliyyətinin proakiv nəzarətinə yanaşma verilir. Bu cür şəbəkə təhlükəsizliyinin monitorinqi (ŞTM) verilənlərin bütövlüyünə, əlyetənliyinə, konfidensiallığına və icazəsiz girişlərin qarşısının alınmasına xidmət edir.

Bu məqalənin məqsədi ŞTM–in əsas vəzifələrini müəyyən etmək, şəbəkə trafikinin analizi üsullarının tədqiqi və ŞTM üçün istifadə olunan intellektual analiz metodlarının tədqiqidir. Bu tədqiqatların nəticəsi olaraq bir sıra komponentləri–metodları özündə biləşdirərək hadisələr haqqında müəyyən olunmuş zaman çərçivəsində informasiya ötürən, müdaxilələrin aşkarlanmasını yerinə yetirən, hadisələrin inkişafına nəzarət edən, təhlükəsizlik hadisələrini müəyyən edən, səciyyələndirən və müasir təhlükəsizlik vasitələrindən effektiv şəkildə istifadə etməyi bacaran ŞTM sisteminin yaradılmasıdır. Yuxarıda qeyd olunanların realizasiyası üçün ŞTM özündə aşağıdakı funksiyaları birləşdirməlidir: fasiləsiz monitorinq; operativlik; əlyetənlik; etibarlılıq; minimal xərcli; proqnozlaşdırma; idarə olunan təhlükəsizlik; avtomatik icra; intellektuallıq.

Son zamanlar şəbəkənin idarə olunması və şəbəkə təhlükəsizliyinin səmərəliliyinin yüksəlməsinə yönəlmiş tədqiqatlarda trafikin klassifikasiyasından və klasterizasiyasından geniş istifadə olunmağa başlanmışdır [3−6]. İnternetdən geniş istifadə olunması, protokolların və tətbiqi proqramların inkişafı ilə trafikin klassifikasiyası sahəsində tədqiqatlar aparılması da aktuallaşmışdır.

Şəbəkə təhlükəsizliyinin monitorinqinin əsas funksiyaları

ŞTM – 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 yerirlməsini təmin edir ki, bu da şəbəkənin səmərəliliyinin artırılmasına kömək edir.

ŞTM-in əsas vəzifələrini aşağıdakı kimi izah etmək olar :

İnternet-trafikin müşahidəsi və qeydiyyatı. Bu proses trafikin müşahidəsi ilə başlayır, cari seansların qeydiyyatı, istifadə olunan trafikin həcminin ölçülməsi, İnternet-trafikin istifadəsinə nəzarət, paketlərin tarixə görə qeydə alınması nəzərdə tutulur.

İnternetlə bağlı real vaxt rejimində işləyən sistemlərin təhlükəsizliynə nəzarət. Sistemlərin səlahiyyətlərinə uyğun olaraq törədə biləcəyi təhlükələrin miqyası dəyişir. Bu sistemləri təhlükə miqyasına görə siniflərə bölüb, nəzarət səviyyəsinin xarakteristikalarını da uyğun formada nizamlamaq lazımdır.

İnternet istifadəçilərinin təhlükəsizliyi, konfidensiallığı və mühafizəsi. İnformasiya təhlükəsizliyini poza bilən zərərli fəaliyyətlərin bəzi tipləri: boşluqları olan xidmətlərə qarşı səbəkə hücumları, yüksək səlahiyyət əldə etmək üçün hücumlar, gizli məlumatların ələ keçirilməsi və zərərli proqramların yüklənməsi həm şəbəkə, həm də onun istifadəçilərinin təhlükəsizliyi və konfidensiallığı baxımından çox təhlükəlidir .

Sistemlərdə boşluqların aşkarlanması. Sistemlərdəki informasiya təhlükəsizliyi boşluqları proqram təminatının ilkin kodunda, verilənlər bazasında, sistemlərin konfiqurasiyasında, idarə edilməsində ola bilər. Bu boşluqlar şəbəkənin informasiya təhlükəsizliyinin vəziyyətinə təsir göstərir.

Fəaliyyətin fasiləsizliyi. Əsas məqsəd İnternet-trafikin keyfiyyətini pisləşdirəcək amillərin aradan qaldırılması və yalnız lazımi məqsədlər üçün istifadəsinə nail olmaqdır.

Riskin qiymətləndirilməsi. Şəbəkə təhlükəsizliyinin idarə olunmasının əsasını riskin qiymətləndirilməsi və idarə edilməsi prosesi təşkil edir. Bu proseslərin effektivliyini dəqiqlik, aparılan analizin dolğunluğu, risk faktorlarının qiymətləndirilməsi və hər hansı bir təşkilatda qərarların qəbul edilməsi mexanizminin yerinə yetirilməsinin monitorinqi müəyyən edir.

Şəbəkə təhlükəsizliyinin monitorinqinin problemləri

Əksər hallarda, böyük və orta ölçülü KŞ-lar mürəkkəb infrastruktura və heterogen struktura malik olur, bu da bir çox platformalarla işləmək məcburiyyəti yaradır. Təhlükəsizlik vasitələrinin analizi göstərir ki, heterogen şəbəkələrin informasiya təhlükəsizliyini təmin etmək üçün bütöv və ya tam inteqrasiya olunmaq imkanı olan heç bir həll yoxdur. Şəbəkə təhlükəsizliyinin monitorinqi sistemlərinin problemlərini aşağıdakı kimi təsnif etmək məqsədəuyğundur:

1. *Səmərəlilik.* Əksər hallarda, hücumların aşkarlanması sistemlərində bütün məlum hücumları aşkarlamağa cəhd edilir ki, bu da bir sıra yanlış nəticələrə gətirib çıxarır. Məsələn, çox tez-tez bu sistemlər özünün çoxlu sayda qaydalarını yaradır və uyğun olaraq resurs tələb edir. Bundan başqa, qaydalar çoxluğu yalnız hadisələr arasında birbaşa asılı olmayan əlaqələr ardıcıllığını aşkarlayır.

2. *Məhsuldarlıq.* Real şəraitdə ŞTM-in məhsuldarlığını qiymətləndirmək çətindir. Bundan başqa, ŞTM-in qiymətləndirilməsi, yəni konkret şəraitdə sistemin məhsuldarlığı haqqında söz deməyə və hər hansı bir kəmiyyət göstəricisi almağa imkan verən ümumi qaydalar toplusu yoxdur.

3. *Vizuallaşdırma.* İnformasiyanı analiz etmək onun müxtəlifliyi və məlumatların həcminin böyüklüyü baxımından mürəkkəb məsələdir və uyğun vizuallaşdırma metodlarının işlənilməsini tələb edir.

4. *Yenilənmə* – hal-hazırda fəaliyyət göstərən sistemləri yeni ŞTM texnologiyaları ilə əvəzləmək çox çətindir. Yeni altsistemlər bütün sistemlə qarşılıqlı təsirdə olmalıdır və bəzən qarşılıqlı təsirin universal imkanlarını təmin etmək mümkün olmur. ŞTM-in quraşdırılması üçün əksər hallarda təhlükəsizlik sahəsindəki vərdişlərdən əhəmiyyətli dərəcədə fərqlənən əlavə vərdişlər tələb olunur. Məsələn, insidentlərin aşkarlanması sistemlərində çoxlu sayda qaydaları yeniləmək üçün xüsusi bilik tələb olunur. Bu fikirləri boşluqları aşkarlayan sistemlərin statistik ölçmələri haqqında da demək olar.

5. *Portativlik* – bu günə qədər ŞTM-lərin çoxu konkret avadanlıqlarda istifadə etmək üçün yaradılır və onları oxşar təhlükəsizlik siyasətinin reallaşdırılması tələb olunan digər sistemlərdə tətbiq etmək kifayət qədər çətindir.

Şəbəkə infrastrukturunun qurulması və trafik axını üçün şəbəkə avadanlıqları istifadə olunur. Bu tip avadanlıqlar siyahısına kommutatorlar, marşrutizatorlar, mutipleksorlar, genişzolaqlı serverlər, şəbəkəyə giriş qurğuları, modemlər və şəbəkə adapterləri daxildir. Monitorinq funksiyalarının realizasiyası üçün bir çox şəbəkə avadanlıqlarının resurslarından istifadə olunur. Bu isə həmin avadanlıqların etibarlılığına, informasiya ötürmə qabiliyyətinə mənfi təsir göstərir. Bütün bu problemlər əldə olunacaq məlumatların potensial faydasını azaldır.

Verilənlərin analizində adətən, yüksəksürətli hesablama sistemi və ya bir neçə kompüter istifadə olunur. Bu sistem hücum təhlükələrini, məlumat axınını analiz etmək, şəbəkənin anomal aktivliyini aşkarlamaq, QoS-analizi etmək və ya total monitorinqi (trafikin tam ələ keçirilməsi və yığılmış məlumatların yaddaş diskinə yazılması) təmin etmək üçün emal prosesində istifadə oluna bilər. Belə sistem, böyük həcmli məlumatları ələ keçirməli və sistem yaddaşına yazmalıdır. Sistem analizinin rastlaşdığı əsas çətinliklər ondan ibarətdir ki, bütün informasiya axınını OSİ modelinin aşağı səviyyələrində analiz etmək lazımdır. Bu problemi həll etmək üçün yüzlərlə və demək olar ki, minlərlə kompüterin hesablama gücü tələb olunur.

İnternet trafikin dinamikası, ən son kiberhücumlar və proqram təminatları, səmərəli intellektual monitorinq metodların işlənməsinin vacibliyini ortaya qoyur [7].

Şəbəkə təhlükəsizliyinin intellektual monitorinqi metodları

Hal-hazırda istifadə olunan proqram məhsullarının çoxu informasiya təhlükəsizliyi təhdidlərinin aşkarlanması üçün siqnaturaların istifadə olunmasına əsaslanır.

Siqnatura analizi insidentlərin aşkarlanması üçün tətbiq olunan metodlardan biridir. Bu metod proqram kodlarının nümunə ilə üst-üstə düşməsi yanaşmasına əsaslanır. Daxil olan informasiya paketi diqqətlə analiz olunur və siqnatura bazası ilə, yəni ziyanlı trafikin xarakteristikasını göstərən proqramın xarakterik sətri ilə müqayisə olunur. Belə siqnaturanın tərkibində hücumla əlaqəli olan acar söz və ya komanda ola bilər. Əgər üst-üstə düşmə aşkarlanarsa, onda həyəcan siqnalı verilir.

Siqnatura metodlarının üstünlüyü hücumların səmərəli müəyyənləşdirilməsi, çoxlu sayda yalan məlumatların olmaması və konkret alətlərin və ya hücum texnologiyalarının istifadəsinin etibarlı diaqnostikasından ibarətdir. Bu administratora peşəkarlıq səviyyəsindən asılı olmadan təhlükəsizlik sahəsində insidentin emal prosedurlarını başlamağa və təhlükəsizliyin təmin olunması yollarına korreksiya etməsinə imkan verir. Siqnatur metodunun çatışmayan cəhəti yeni hücumların siqnaturasının alınması üçün məlumat bazasının yenilənməsinin vacibliyidir.

Şəbəkələrin, digər mürəkkəb sistemlər kimi bir çox səbəblərdən fasiləsiz monitorinqinə ehtiyac duyulur. Monitorinq sistemi şəbəkənin vəziyyətinin proqnozlaşdırılması, informasiya axınında kəsilmələrin və itkilərin idarə olunması üçün qabaqlayıcı tədbirlər görmək qabiliyyətinə malik olmalıdır. Bu səbəbdən, operativ təhlükəsizliyin təmin olunması üçün real vaxt rejimində monitorinq aktual məsələdir. [8]-də qeyd olunur ki, insanın immun sisteminin və kompüter şəbəkəsi təhlükəsizliyi sisteminin arasında güclü korrelyasiya var. İmmun sistemi insanı patogen viruslardan qoruduğu kimi, informasiya təhlükəsizliyi sistemi də KŞ-nı təhdidlərdən qoruyur.

Kompüter şəbəkələrinin fəaliyyəti və təhlükəsizliyi haqqında lazımi verilənlərin toplanması və dəqiq analiz edilməsi və şəbəkə təhlükəsizliyinin təmin edilməsi haqqında əsaslandırılmış qərarların qəbul edilməsi üçün şəbəkə təhlükəsizliyinin monitorinqi zamanı verilənlərin intellektual analizi texnologiyalarından istifadə edilməsi aktualdır [9, 10].

Müasir heterogen şəbəkələrdə etibarlı xidmətin göstərilməsi vacib məsələlərdən biri olaraq qalır. Şəbəkə xidmətləri üçün etibarlı inkişafın və genişlənmə qabiliyyətinin təmin olunması üçün şəbəkə və hesablama resurslarından səmərəli istifadə təmin olunmalıdır. Bunu mövcud resurslardan istifadə edərək paylanmış lokal həllərlə etmək mümkündür. Buna baxmayaraq, bu cür həllər ümumi məqsədə çatmaq üçün əlaqələndirilməlidir.

Ümumilikdə sistemlər üçün əsas bloklardan biri ölçmələrdən zəruri və müvafiq məlumat əldə etmək üçün şəbəkə parametrlərinin monitorinqi imkanının olmasıdır. Yuxarıda qeyd edildiyi kimi, müasir şəbəkələrin heterogen struktura malik olması monitorinqin lokal aparılmasını çətin prosesə çevrir.

Bir çox təhlükəsilik avadanlıqları, məsələn, şəbəkə ekranları, IDS və qovşaq antivirusları çoxlu sayda təhlükəsizlik hadisələri generasiya etdiyi üçün səmərəli idarəolunma çətinləşir. ŞTM-in arxitekturasında korrelyasiya mexanizminin tətbiqi və aşkarlanma prosesi üçün verilənlərin daimi intellektual analizi metodlarının istifadə olunması prosesi [11]-də izah olunur. Verilənlərin intellektual analizi əsasında təhlükəsizlik hadisələrinin korrelyasiyası avtomatik əlaqəli qaydalar yaradır, hadisəni analiz edir və yeni təhdidləri aşkarlayır.

ŞTM-in dəqiq təhlükəsizlik siyasəti və real vaxt rejimində müdaxilə etmək səlahiyyəti olduğu halda yüksək səviyyəli audit apara bilər. Audit nəticəsində təhlükəsizlik siyasətindən yayınmaları asanlıqla identifikasiya etmək və vaxtında aradan qaldırmaq mümkündür. Belə ki, əlaqə kanalları (protokollar və portlar) məhdudlaşdırıldığı üçün bədniyyətlilərin hücum prosesini həyata keçirmək imkanları məhdudlaşır və məhdud əlaqə kanallarına isə ŞTM nəzarət edir. Bu da onu göstərir ki, bədniyyətli trafikin müəyyən olunması üçün ŞTM sisteminə normal trafikin təbiəti bəlli olmalıdır.

Trafikin monitorinqinin yerinə yetirilməsi və sistemin analizi əsasən informasiya axınının həcmindən və məlumat paketlərinin daxil olması xarakterindən asılıdır. Vəziyyət haqqında məlumatların zaman sıralarının yığılması üçün istifadə olunan üsulların bir sıra komponentlərini özündə birləşdirən hiper təhlükəsizlik adaptiv monitorinq sistemi müdaxilələrin aşkarlanması, hadisənin inkişafının izlənməsi, təhlükəsizlik hadisəsinin xarakterizə olunması və müəyyənləşdirilməsi əməliyyatlarını yerinə yetirir. Ona görə də uyğun təhlükəsizlik tədbirləri vaxtında və effektiv şəkildə qəbul olunaraq yerinə yetirilir. Xüsusi hal kimi [12]-də paylanmış vericilərdən gələn informasiya əsasında müdaxilələrin aşkarlanması üçün səmərəliliyin analitik sübut olunmuş zəmanətli həllinin alqoritmini tətbiq etmək olar. Ənənəvi qaydalardan fərqli olaraq, təhlükəsizlik hadisəsi nümunəsi ilə müqayisə olunma əsasında təklif olunan sistemlərdə qrafik şəkildə təqdim olunur. Təsadüfi matris nəzəriyyəsindən istifadə etməklə şəbəkələrin korreliyasiyası şəbəkələrin uyğunluqlarının hesablanması gedişində ortaya çıxır. Geniş modelləşdirmə nəticəsində hadisələrin identifikasiyası təklif olunan sistemin effektivliyini nümayiş etdirir.

Monitorinqin və təhdidlərin aşkarlanması tələblərinin yerinə yetirilməsi strukturunun qurulması, təhlükəsiz və etibarlı sistemlərin dəstəklənməsinə yanaşmanın tərkib hissəsi kimi işlənir. Bele olduğu halda infrastrukturun modeli şablonlar əsasında qurulmalıdır [13]. Şablonlarla real zamanda monitorinq üçün təhlükəsizlik tələblərini ifadə edən hadisənin hesablanması düsturları generasiya olunur. Bu nəzəriyyədən hücum və təhdid siqnaturları və ya sistemə mümkün hücumların siqnaturu generasiya olunur. Bu proses zamanı Bayes şəbəkələri əsasında müəyyən zaman çərçivəsində təhdidlərin ehtimalı qiymətləndirilir.

Məlumatların vaxtında və etibarlı ötürülməsi üçün çoxlu şəbəkə əlavələrinin və təhlükəsizliyin kompleks həllərinin işlənməsi tələb olunur. Bunun üçün şəbəkəyə nəzarət etmək və onu sayı getdikcə artan zərərli hücumlardan qorumaq lazımdır. Buna baxmayaraq,

hiperfəzanın vəziyyətinin idarə olunması, qərarların qəbul olunması və hərəkət edilməsi üçün informasiya vəziyyətinin aşağı səviyyəsindən yüksək insan təxəyyülü səviyyəsinə səmərəli çevrilmə mexanizmi olmadığından, fövqəladə dərəcədə mürəkkəbdir.

Şəbəkə sistemləri istifadə olunan ekranların pis konfiqurasiyasından və monitorinq funksionallığından əziyyət çəkirlər. Şəbəkələrarası ekranın konfiqurasiyası və şəbəkə monitrinqi prosesini təmin etmək üçün VisualFirewall proqramından və müxtəlif səviyyələr üzrə istiqamətlənmiş dörd sinxron baxışın, zaman kəsiyinin, fərdi paketlərə qədər şəbəkə ekranının reaksiyasının vizuallaşdırılması metodlarından istifadə edilir [14]. Dörd sinxron baxış dedikdə, sistemlərdə aktiv və ya passiv monitorinq prosesini reallaşdırmaq üçün real vaxt rejimində trafik, vizual siqnatura, statistika və İDS başa düşülür. Bu proses nəticəsində alınan hesabatlar trafikdəki anomallığı asanlıqla müəyyən etməyə imkan verir.

Müəssisənin və ya universitetlərin şəbəkə təhlükəsizliyinin monitorinqində daxili şəbəkədən xarici şəbəkəyə hücumların aşkarlanması daha vacib əhəmiyyət kəsb edir [15]. Əgər bu cür hücumlar aşkarlanarsa, belə fərdi kompüterlərin yerinin aşkarlanması bəzən vacib olur. Bu iş genişmiqyaslı şəbəkələr üçün vizuallaşdırılmış təhlükəsizlik monitorinqi sistemlərini təsvir edir. Sistem məntiqi, zaman və qrafiki məlumatları bir 3D görünüşündə birləşdirir. Bundan başqa, sistem mexanizmlərin filtrasiya imkanlarını və qarşılıqlı təsirini təmin edir.

Kibertəhlükəsizliyin adaptiv monitorinqi sistemi özündə bir çox komponentləri birləşdirərək müəyyən zaman çərçivəsində situasiya haqqında informasiya toplayır, müdaxilələrin aşkarlanmasını yerinə yetirir, hadisələrin inkişafına nəzarət edir, təhlükəsizlik hadisələrini identifikasiyası edir və alınan nəticələri vizual formada təqdim edərək düzğün qərar qəbul olunmasına kömək edir [16]. Vizuallaşdırma prosesi isə Stemplot metodunun köməyi ilə hadisənin yerini və miqyasını təyin etmək məqsədi ilə aparılır və modelləşdirmənin nəticələri təklif edilən modelin effektivliyini nümayiş etdirir. ŞTM isə əlavə olaraq bədniyyətli əməlləri müşahidə edə bilər və bu da uyğun olaraq nəzarəti gücləndirir.

[17]-də qeyd edilir ki, təhlükəsizliyin adaptiv-dayanlıqlı idarə edilməsi kritik biznes əlavələrin platformalarında və şəbəkələrində özünümüdafiə, özünübərpa funksiyalarını təmin edir. Adaptiv təhlükəsizliyin təmin olunması üçün qərar qəbul edilməsinin əsasını sistemdən yığılmış həqiqi və kifayət qədər təhlükəsiz sübutlar təşkil edir. Təklif edilən mexanizmlərin texniki-iqtisadi analizi də aparılmalıdır.

Şəbəkə trafikinin klassifikasiyası metodları

İnternetdən geniş istifadə olunması, protokolların və tətbiqi proqramların inkişafı ilə trafikin klassifikasiyası sahəsində aparılan tədqiqatlar da aktuallaşmışdır. İnternet trafikin monitorinqi, QoS-un idarə olunması və təhlükəsizlik hadisələrinin aşkarlanması və s. üçün TCP/IP axınının xüsusiyyətlərinin öyrənilməsi və bunun əsasında klassifikasiyanın aparılması vacibdir.

Trafikin iyerarxik və hərtərəfli identifikasiyasında istifadə edilməsi üçün trafikin klassifikasiyası metodlarının taksonomiyası [18]-də araşdırılır. Belə sistematikada hərtərəfli identifkasiyanın dəstəklənməsi üçün dörd klassifikasiya kriteriyası təklif olunur: xidmət, proqram, protokol və funksiya. Bundan savayı, təklif olunmuş taksonomiya yuxarı və ya aşağı istiqamətlənmiş iyerarxik quruluşun nəticələrini də dəstəkləyir.

Şəbəkə trafikinin paketlər səviyyəsində klassifikasiyası üçün gizli Markov modelindən istifadə oluna bilər [19].

Son zamanlar trafikin klassifikasiyasında “Machine learning” metodlarından geniş istifadə olunur. Ən yaxın qonşular metodu əsasında klassifikasiya cox yaxşı nəticə nümayiş etdirir. Amma təlim məlumatlarının ölçüsü az olduqda, nəticənin dəqiqliyinə ciddi zərər dəyməsi ehtimalı böyükdür. Belə hadisələrin qarşısının alınması üçün, klassifikasiya prosesi zamanı məlumatların korrelyasiyası aparılmalıdır [20].

Veb-sistemlər verilənlər bazası və brauzerlə sıx əlaqədə olmaları səbəbindən unikal boşluq və təhdidlərlə qarşılaşırlar. Veb-sistemlərdə baş verən bu təhlükəsizlik təhdidləri klassifikasiya olunaraq xarakteristikaları aşkarlanır [21]. Əvvəlcə analiz üçün baş vermiş hadisənin təsir miqyası, növü və vaxtı müəyyən olunur. Sonra "Machine learning" metodlarından istifadə edilərək təhlükəsizlik hadisələri klassifikasiya olunur və iki sinifə: boşluqların skanlanması və hücumlara ayrılır.

İnternet trafikinin klassifikasiya nəticələrinin etibarlılığının yüksəldilməsi üçün bir çox metodlar mövcuddur, lakin onlar daha aşağı səviyyəli klasiffikasiyalar üçün etibarlı sayılmır. İnternet-trafikin onlayn klassifikasiyası üçün bir sıra intellektual analiz metodları təklif olunur [22]. Bu metodlar konkret olaraq yalançı hadisələrin aşkarlamasına yönəlib və müvafiq olaraq, yalançı hadisələrin qiymətləndirilməsi prosesinin qarşısını alır.

Bütün İnternet-trafikin toplanacağı halda, emal prosesinin çox uzun çəkəcəyi məlumdur. Bunun üçün İnternet trafikin axınından periodik olaraq informasiya toplanır və bunun vasitəsilə ümumi olaraq mühiti analiz etmək mümkün olur, bu isə emal prosesi zamanı hesablama vaxtını aşağı salır.

Şəbəkə mühitinin idarə olunması təmin olunduğu halda HTTP trafikin klassifikasiyası "paralel neyron şəbəkəsi klassifikatoru arxitekturası" əsasında aparıa bilər. Bu trafikin klassifikasiyası zamanı alınan ilkin məlumatlar əsasında bu yanaşmanın səmərəliliyi 85−91% olaraq qiymətləndirilir [23].

Trafikin klassifikasiyasi və identifikasiyası, ümumiyyətlə, ən geniş tədqiqat sahələrindən biri hesab olunur. Yuxarıda analiz edilən tətqiqatların nəticələri göstərir ki, şəbəkə təhlükəsizliyinin təmin olunması, hadisələrin düzgün interpretasiyası və İnternet-trafikin hərtərəfli öyrənilməsi üçün trafikin klassifikasiyası cox vacibdir. Bunlara əsaslanaraq, trafikin klassifikasiyası üçün intellektual, iyerarxik, operativ və çoxəlamətli metodlar işlənib hazırlanmalıdır.

Şəbəkə trafikinin klasterizasiyası metodları

"Machine learning" yanaşması şəbəkə trafikində anomal axınların unikal statistik xarakteristikalara əsaslanaraq müəyyən olunması üçün geniş istifadə olunur. Qeyri-səlis klasterləşdirmə ənənəvi klasterləşdirməyə nəzərən daha çevikdir, müdaxilələrin aşkarlanması və verilənlərin təbii emalı üçün daha məqsədəuyğundur [24].

Bir çox klasterləşdirmə metodları müdaxilələrin aşkarlanması üçün normal və anomal trafikin ayrılmasını nəzərdə tutur.

Klasterləşdirmə metodları trafik sessiyalarının fərqlərini və oxşarlıqlarını tapmaq, onların hər birini müvafiq qruplara bölərək təsnif etmək üçün tətbiq edilir [25]. Bu qruplar onlara verilmiş nişanlar ilə təmsil olunur. Daha sonra bu nişanlar daxil olan şəbəkə trafikinin növünü proqnozlaşdırmaq üçün istifadə olunur.

Şəbəkə trafikinin tez və dəqiq indentifikasiyası QoS-un idarə edilməsi, şəbəkə təhlükəsizliyinin monitorinqi və s. funksiyalar üçün ən vacib məsələlərdən biridir. Lakin son zamanlar P2P-dən istifadə edən qovşaqlar çoxalıb və onlar müxtəlif portlardan istifadə edərək özünü hər hansı qurğu, lazımlı məlumat axını və ya sifrlənmiş məlumat axını altında gizlədərək lazımsız informasiya axınını generasiya edirlər. Bu halda klassik yanaşmalar sayılan "port mapping" və ya "payload analysis" yanaşmalarının istifadəsi effektiv deyil. Alternativ yanaşma şəbəkədə TCP trafiki ilə əlaqədar ilk bir neçə paket daxilində davranışı tədqiq edərək klassifikasiya etməkdir. Bu gələcəkdə bütün informasiyanı klasterləşdirərək identifikasiya prosesini asanlaşdırmaq üçün istifadə etməyə imkan verərdi [26].

Simsiz şəbəkələrə qarşı artan tələbat bu şəbəkələrin təhlükəsizlik problemlərinə böyük diqqət oyadır. Naqilli şəbəkələrdə müdaxilələrin aşkarlanmasının intellektual analizində istifadə olunan metodlar, simsiz şəbəkələr üçün yararlı deyil. 802.11 simsiz şəbəkələrdə boşluqların aşkarlanması və simsiz şəbəkələrin təhlükəsizliyinin modelləşdirilməsi üçün müvafiq şəbəkə

trafikinin ölçmələri aparılmalıdır. [27]-da təklif olunan yanaşma məsafəyə əsaslanan evristik metrikadan istifadə edərək klasterləri normal və ya zərərli olaraq işarələyir.

DDoS hücumların aşkarlanması şəbəkələrin təhlükəsizliyinin təmin edilməsində mühüm rol oynayır. DDoS hücumların xüsusiyyətlərinin müəyyən olunması üçün aşağıdakı adaptiv klasterləşdirmə metodundan istifadə olunur [28]:

1. Şəbəkə trafikinin təhlili əsasında ilkin dəyişənlər seçilir;
2. Modifikasiya edilmiş qlobal *k*-ortalar alqoritmi hədəf məlumatların klaster strukturunun identifikasiyası üçün klasterləşmənin baza alqoritmi kimi istifadə olunur;
3. Xətti korrelyasiya əmsalı əlamətləri ranqlaşdırmaq üçün istifadə olunur;
4. Ranqlaşdırılmış məlumatlar klasterlərin yenidən hesablanması üçün istifadə olunur.

Bu adaptiv proses DDoS hücumlarının müxtəlif nümunələrinə görə əlamətlər vektoruna lazimi düzəlişlər edə bilər, klasterlərin keyfiyyətini və alqoritmin səmərəliliyini yaxşılaşdıra bilər.

Botnet, bədniyyətliyə ziyankar proqramlardan istifadə edərək, istifadəçinin xəbəri olmadan yoluxmuş kompüteri məsafədən idarə etməyə və onları bir şəbəkədə birləşdirməyə imkan verən infrastrukturdur. Belə bədniyyətli texnologiya zombiləşdirilmiş kompüterlərdən ibarət ordu yaradılmasına münbit şərait yaradır. Bədniyyətli botnet şəbəkəsini idarə etmək üçün idarə və nəzarət prinsipindən istifadə edir. Normal trafikdən fərqli olan daşıyıcı protokol və kodlaşdırma fərqləri trafikin monitorinqi vasitəsilə müəyyən oluna bilər. Botnetin idarə və nəzarət kanallarının aşkarlanması üçün iyerarxik klasterləşdirmədən istifadə olunur [29], bu da botnetlərin idarə və nəzarət olunması üçün lazım olan məlumat mübadiləsini müəyyən edir. Bu yanaşma, istifadəçi kompüteri botnet şəbəkəsinin bir hissəsi olduğu halda, onun kənardan idarə olunmasının qarşısını almaq üçün səmərəli vasitə hesab oluna bilər.

Nəticə

Bu məqalədə kompüter şəbəkələrinin informasiya təhlükəsizliyinin monitorinqi sistemlərində intellektual analiz metodlarının tətbiqinin mümkünlüyü analiz edilmişdir. İntellektual analiz metodlarının tətbiqi nəticəsində şəbəkə təhlükəsizliyinin monitorinqi problemlərinin həlli üçün geniş imkanlar aşılır. Bu yolla süni intellekt metodlarından istifadə edərək problemi avtomatik aşkar etmək, onun həlli yollarını tapmaq, kompüter şəbəkələrindəki nasazlıqları aradan qaldıraraq operativ idarəetməni tənzimləmək mümkündür.

Ədəbiyyat

1. Pierson R., Fitzpatrick S. Network security architecture for intelligent networks // Intelligent Network Workshop, 1997, vol. 3, no.3, pp.37.
2. Kotenko I., Bogdanov V. Proactive monitoring of security policy accomplishment in computer networks / Proc. of the IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2009, pp.364−369.
3. Zhang H., Lu G., Qassrawi M., Yu X. Comparison and Analysis of Flow Features at the Packet Level for Traffic Classification / Proc. of the International Conference on Connected Vehicles and Expo (ICCVE), 2012, pp.262−267.
4. Callado A., Kamienski C., Szabo G., Gero B., Kelner J., Fernandes S., Sadok D. A Survey on Internet Traffic Identification // IEEE Communications Surveys & Tutorials, 2009, vol.11, pp.37−52.
5. Junior G.P.S., Maia J.E.B., Holanda R., Sousa J.N. P2P Traffic Identification using Cluster Analysis / Proc. of the First International Global Information Infrastructure Symposium, 2007, pp.128−133.
6. Dong-Mei L., Bin L., Ying Q. Study on method for public traffic network optimization and adjustment based on cluster analysis / Proc. of the International Conference on Machine Learning and Cybernetics (ICMLC), 2011, pp.1593−1596.

7. Kuai X., Zhi-Li Z., Bhattacharyya S. Internet Traffic Behavior Profiling for Network Security Monitoring // The IEEE&ACM Transactions on Networking, 2008, vol.16, no.6, pp.1241−1252.
8. Boukerchea A., Machado B.R., Jucá K.R.L., Sobral J.B.M., Notare M.S.M.A. An agent based and biological inspired real-time intrusion detection and security model for computer network operations // Journal Computer Communications, 2007, vol. 30, no. 13, pp.2649−2660.
9. Han J., Kamber M. Data Mining: Concepts and Techniques, 2nd ed. Morgan Kaufmann Publishers, 2006.
10. Bishop C.M. Pattern Recognition and Machine Learning. Springer, 2006, 738 p.
11. Xu K., Zhang Z., Bhattacharyya S., Internet Traffic Behavior Profiling for Network Security Monitoring // IEEE/ACM Transactions on Networking, 2008, pp.1241−1252.
12. Wu Q., Ferebee D., Lin Y., Dasgupta D. Visualization of security events using an efficient correlation technique / Proc. of the IEEE Symposium on Computational Intelligence in Cyber Security, 2009, pp.61−68.
13. Amalio N., Spanoudakis G. From Monitoring Templates to Security Monitoring and Threat Detection / Proc. of the Second International Conference on Emerging Security Information, Systems and Technologies, 2008, pp.185−192.
14. Lee C.P., Trost J., Gibbs N., Raheem B., Copeland J.A. Visual firewall: real-time network security monitor // IEEE Workshop on Visualization for Computer Security, 2005, pp.129−136.
15. Mukosaka S., Koike H. Integrated visualization system for monitoring security in large-scale local area network / Proc. of the 6th International Asia-Pacific Symposium, 2007, pp.41−44.
16. Wu Q., Ferebee D., Lin Y., Dasgupta D. An integrated cyber security monitoring system using correlation-based techniques / Proc. of the IEEE International Conference on System of Systems Engineering, 2009, pp.1−6.
17. Savola R.M., Heinonen P. Security-Measurability-Enhancing Mechanisms for a Distributed Adaptive Security Monitoring System / Proc. of the Fourth International Conference on Emerging Security Information Systems and Technologies, 2010, pp.25−34.
18. Kim J., Yoon S., Kim M. Study on traffic classification taxonomy for multilateral and hierarchical traffic classification / Proc. of the 14th Asia-Pacific Network Operations and Management Symposium, 2012, pp.1−4.
19. Dainotti A., Donato W., Pescape A., Rossi S.P. Classification of Network Traffic via Packet-Level Hidden Markov Models / Proc. of the IEEE Global Telecommunications Conference, 2008, pp.1−5.
20. Zhang J., Xiang Y., Wang Y., Zhou W., Xiang Y., Guan Y. Network Traffic Classification Using Correlation Information // IEEE transactions on Parallel and Distributed Systems, 2013, vol.24, no.1, pp.104−117.
21. Goseva-Popstojanova K., Anastasovski G., Dimitrijevikj A., Pantev R., Miller B. Characterization and classification of malicious Web traffic // Computers & Security, 2014, vol. 42, pp. 92-115
22. Nechay D., Montreal Q.C., Pointurier Y., Coates M. Controlling False Alarm/Discovery Rates in Online Internet Traffic Flow Classification / Proc. of the IEEE Conference on INFOCOM, 2009, pp.684−692.
23. Mathewos B., Carvalho M.M., Ham F.M. Network traffic classification using a parallel neural network classifier architecture / Proc. of the 7th Annual Workshop on Cyber Security and Information Intelligence Research, 2011, no.3, pp.13–25.

24. Liu D., Lung C., Lambadaṅs I., Seddigh N. Network traffic anomaly detection using clustering techniques and performance comparison / Proc. of the 26th Annual IEEE Canadian Conference on Electrical and Computer Engineering, 2013, pp.1−4.
25. Shokri R., Oroumchian F., Yazdani N. CluSID: a clustering scheme for intrusion detection improved by information theory / Proc. of the 7th IEEE Malaysia International Conference on Communications, 2005, pp.553−558.
26. Li N., Zhang S., Lu Y., Yan J. Real-time P2P traffic identification / Proc. of the IEEE Global Telecommunications Conference, 2008, pp.1−4.
27. Khoshgoftaar T.M., Nath S.V., Zhong S., Seliya N. Intrusion detection in wireless networks using clustering techniques with expert analysis / Proc. of the 4th International Conference on Machine Learning and Applications, 2005, pp.8−17.
28. Zi L., Yearwood J., Wu X.-W. Adaptive clustering with feature ranking for DDoS attacks detection / Proc. of the 4th International Conference on Network and System Security (NSS), 2010, pp.281−286.
29. Dietrich C.J., Rossow C., Pohlmann N. CoCoSpot: Clustering and recognizing botnet command and control channels using traffic analysis // The International Journal of Computer and Telecommunications Networking, 2013, vol.57, no.2, pp.475−486.

УДК 004.056

Алгулиев Расим М.[1], Имамвердиев Ядигар Н.[2], Набиев Бабек Р.[3]
Институт Информационных Технологий НАНА, Баку, Азербайджан
[1]rasim@science.az, [2]yadigar@lan.ab.az, [3]babek@iit.ab.az

Анализ методов мониторинга сетевой безопасности

Мониторинг сетевой безопасности является актуальной задачей для обеспечения непрерывного и надежного функционирования компьютерных сетей. В статье определены задачи и функции мониторинга сетевой безопасности, интеллектуальные методы мониторинга сетевой безопасности, в том числе исследованы методы классификации и кластеризации сетевого трафика, и установлен ряд важных проблем исследования.

***Ключевые слова**: информационная безопасность, мониторинг сетевой безопасности, анализ сетевого трафика, классификация трафика, кластеризация трафика.*

Rasim M. Alguliev[1], Yadigar N. Imamverdiyev[2], Babek R. Nabiyev[3]
Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]rasim@science.az, [2]yadigar@lan.ab.az, [3]babek@iit.ab.az

Analysis of methods for network security monitoring

Network security monitoring is an urgent task to ensure continuous and reliable operation of computer networks. In this article the tasks, functions and intelligent monitoring methods of network security have been defined, as well as methods of classification and clustering of network traffic have been researched. Also there was established several important research problems.

***Keywords:** information security, network security monitoring, network traffic analysis, traffic classification, clustering traffic.*