E-dövlətin İnformasiya Təhlükəsizliyi üçün Big Data Texnologiyaları

Yadigar İmamverdiyev
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@lan.ab.az

***Xülasə* — Big Data texnologiyaları bir sıra spesifik informasiya təhlükəsizliyi problemləri yaratmaqla yanaşı, informasiya təhlükəsizliyinin təmin edilməsi üçün yeni imkanlar da vəd edir. Bu işdə Big Data texnologiyalarının gətirdiyi yeni informasiya təhlükəsizliyi təhdidləri analiz edilir və bu texnologiyaların e-dövlətin informasiya təhlükəsizliyi sistemində tətbiqi imkanları qiymətləndirilir.**

Açar sözlər — e-dövlət; Big data; informasiya təhlükəsizliyi; informasiya təhlükəsizliyinin monitorinqi

I. GİRİŞ

Hazırda dövlət orqanları qarşısında dövlət təşkilatlarının fəaliyyətində şəffaflığın artırılması və iş məhsuldarlığının yüksəldilməsi problemləri durur. Buna görə də dövlətin əhali ilə tez, şəffaf və səmərəli şəkildə qarşılıqlı əlaqə saxlamağa, vətəndaşlara xidmət müddətini azaltmağa, əhalinin xidmətlərə tələbatını artırmağa, maliyyə effektivliyini yüksəltməyə, inzibati xərcləri azaltmağa imkan verən, korrupsiyanın aradan qaldırılmasına şərait yaradan informasiya sistemlərinin yaradılmasına və istismarına ehtiyacı vardır. Mövcud texnologiyalar artıq bu məsələləri həll edə bilmir. Bu bir neçə səbəblə şərtlənir.

Dövlət sektoru çox böyük həcmdə verilənlər toplayır, dünyada heç bir kommersiya strukturunun dövlət və hakimiyyət orqanları qədər verilənlər toplamaq imkanı yoxdur. Lakin bu verilənlərin 70%-i strukturlaşdırılmayıb və mətnlər və müxtəlif sənədlər şəklində saxlanır. Bu verilənlərin həcmi daim artır, dünya üzrə illik artım sürəti 30%-dir. Vətəndaşlar daim bu və ya digər şəkildə (o cümlədən, sosial şəbəkələr vasitəsilə) dövlət orqanları ilə ünsiyyətdə olurlar, elektron dövlətin formalaşdırılması gedişində elektron xidmətlər genişlənir, mövcud kağız informasiyasının elektronlaşdırılması həyata keçirilir.

Nəticədə verilənlər təkrarlanır və həcmləri artır, onların emalı getdikcə daha çox resurs tələb edir. Bu verilənləri sistemləşdirmək, arxiv verilənləri ilə işləmək, lazım olan informasiyanı arxivdə axtarıb tapmaq getdikcə çətinləşir. Strukturlaşdırılmamış şəkildə daxil olan informasiyanı sonrakı analiz məqsədilə saxlamaq üçün xüsusi emal etmək lazım gəlir. Bu çox zaman informasiyanın analizi tsiklini əhəmiyyətli dərəcədə yavaşıdır və verilənlərin emalına və saxlanmasına çəkilən xərcləri artırır.

Dövlət sektorunda çox böyük həcmdə toplanan verilənlərin saxlanılması və analizi zamanı bir sıra texnoloji problemlər də meydana çıxır. Böyük həcmdə və müxtəlif formatda toplanmış bu verilənlərin Big Data texnologiyaları olmadan, relyasion verilənlər bazaları texnologiyaları ilə emalı getdikcə çətinləşir və qeyri-mümkün olur. Nəticədə dövlət hakimiyyəti orqanları Big Data problemləri ilə qarşılaşırlar və bu vəziyyət yeni texnologiyaların tətbiq edilməsini tələb edir. Beləliklə, dövlət sektorunun vətəndaşlarla sürətli, şəffaf və səmərəli qarşılıqlı əlaqəsi üçün Big Data həllərinə böyük ehtiyacı vardır [1].

Lakin Big Data texnologiyaları e-dövlətin informasiya infrastrukturunda toplanmış fərdi məlumatların təhlükəsizliyinə bir sıra özünəməxsus təhlükələr yaradır. Bununla yanaşı, Big Data texnologiyalarının perspektiv tətbiq sahələrindən biri də e-dövlətin informasiya təhlükəsizliyinin təmin edilməsi sisteminin təkmilləşdirilməsidir [2]. Bu işdə Big Data texnologiyalarının yaratdığı spesifik informasiya təhlükəsizliyi təhdidləri analiz edilir və bu texnologiyaların e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi sistemində tətbiqi problemlərinə baxılır.

II. E-DÖVLƏTDƏ BİG DATA TƏTBİQLƏRİ

Dövlət sektorunda Big Data tətbiqlərinin sayı artır, burada anbarlarda verilənlərin həcmi yüzlərlə terabayta və ya petabayta çata bilər. MGI mütəxəssislərinin tədqiqatlarına görə, Avropa İttifaqının dövlət sektoru yalnız verilənlərin şəffaflığının artırılması və Big Data qabaqcıl analitika texnologiyalarının istifadəsi hesabına inzibati xərcləri 15-20% (150-300 milyard yevro) azalda bilər [3].

IBM şirkəti dövlət sektorundan 28 İT-direktorun rəy sorğusu əsasında «Big Data potensialının reallaşdırılması» (“Realizing the Promise of Big Data”) adlı hesabat hazırlamışdır, hesabatda Big Data sahəsində dövlət layihələrinə xas olan 10 ümumi tendensiya müəyyən edilmişdir [4]. Tədqiqatlar göstərmişdir ki, dövlət təşkilatları Big Data tətbiqində hələlik başlanğıc mərhələdədirlər.

Gartner-in tədqiqatları Big Data investisiyalarına görə dünyada ən az inkişaf etmiş sektor olaraq dövləti müəyyən edir (cəmisi 16 %) [5]. Bir sıra ölkələr Big Data strategiyalarını müəyyən etməyə cəhd edirlər. Məsələn, Avstraliya hökuməti 2013-cü ilin avqustunda “Avstarliya dövlət xidmətləri üzrə Big Data strategiyası”nı qəbul etmişdir [6]. Bu strategiya mövcud xidmətləri genişləndirmək, yeni xidmətlər təklif etmək və daha yaxşı siyasəti təmin etmək və eyni zamanda gizliliyin qorunması üçün ən yaxşı təcrübəni tətbiq etmək və mövcud İKT investisiyalarını dəstəkləmək üçün Big Data sahəsində sistemli dövlət yanaşmasıdır. Bu sahədə ABŞ-ın təşəbbüsləri

də əhəmiyyətlidir [7]. Avropa İttifaqı da Big Data sahəsində öz strateji seçimini edib [8].

Son dövrlər hüquq-mühafizə orqanları və milli təhlükəsizliyi təmin edən strukturlar Big Data ideyalarından cinayətkar və terrorçu elementlərin daha dəqiq aşkarlanması üçün istifadə edilməsində maraqlıdırlar.

Big Data texnologiyalarından istifadə edən dövlət təşkilatları çox zaman verilənlərin qanuniliyi və keyfiyyəti, onların qeyri-müəyyənliyi, verilənlərin emalı və analizinin keyfiyyəti ilə bağlı problemlərlə üzləşirlər. Bu insanları böyük risk altında qoyan səhv qərarlara gətirib çıxara bilər. Big Data istifadəsinin mənfi nəticələri təkcə ayrı-ayrı insanlara deyil, ictimai həyatda, iqtisadiyyatda və siyasətdə də özünü göstərə bilər.

III. İNFORMASİYA TƏHLÜKƏSİZLİYİNDƏ PARADİQMA DƏYİŞİKLİYİ

İnformasiya təhlükəsizliyində paradiqma dəyişikliyi haqqında danışmaq üçün bir sıra şərtlər mövcuddur. Proqram məhsullarının və informasiya sistemlərinin mürəkkəbliyi artdıqca onlarda mövcud olan boşluqlar da artır və bədniyyətlilərin istifadəçilərə və istehsalçılara hələlik məlum olmayan boşluqlardan istifadəsi ehtimalı yüksəlir. İnformasiya texnologiyaları və informasiya təhlükəsizliyiin sahəsində mütəxəssislərin peşəkarlığı artır və asimmetrik aktorların yüksək ixtisaslı mütəxəssisləri bədniyyətli hərəkətlərə cəlb etməsi imkanları asanlaşır. Asimmetrik aktorlar hücum silahlarının inkişaf etdirilməsinə də yetərli investisiya yatıra bilərlər. Əsas məqsədi ziyan vurmaq olan ənənəvi kiber-hücumlardan fərqli olaraq müasir kiber-hücumlar konkret hədəfə yönəlir, daha yaxşı təşkil olunur və əlaqələndirilir. Bu hücumların əsas məqsədi tez aşkarlanan ziyan vurmaq deyil, qiymətli verilənlərə çıxış əldə etmək və onu mümkün olduqca uzun müddət – aylar, hətta illər ərzində saxlamaqdır. Qiymətli verilənlər dedikdə təşkilatın intellektual mülkiyyəti (proqram məhsulunun ilkin kodları, alqoritmlər, müştərilər bazası, istənilən digər korporativ sirlər) nəzərdə tutulur.

Hədəfə yönəlik hücumların böyük sinfini APT (Advanced Persistent Threat) hücumları təşkil edir [9]. Termin ABŞ-a yönəlmiş, xarici kəşfiyyat /dövlət tərəfindən dəstəklənən hücumları təsvir etmək üçün 2006-cı ildə ilk dəfə hərbçilər tərəfindən işlədilmişdi.

APT təhdidlərin xüsusi növüdür, konkret dövlət strukturlarına, şirkətlərə, təşkilatlara və hətta şəxslərə yönəlir. Bu növ təhdidlərin əsas fərqli cəhəti yalnız onların hədəflərinin konkretliyi deyil, həm də qabaqcıl informasiya texnologiyaları ilə yanaşı, psixologiya, sosial mühəndislik və s. metodlarına əsaslanan ən müasir yanaşmalardan istifadə etməsidir.

Bu mürəkkəb terminin hər bir sözü təsadüfi seçilməyib, xüsusi məna daşıyır:

- ***Advanced* (*məqsədyönlü*).** Hücumun mənbəyi – yaxşı maliyyələşdirilən təşkilatdır, onun sərəncamında hücumu həyata keçirmək üçün kifayət qədər resurs, hesablama texnikası və yaxşı təlim görmüş, kompüter sistemlərinə girmək vərdişlərinə malik yüksək ixtisaslı mütəxəssislər var.
- ***Persistent (davamlı).*** Hücum edən səbirlidir, müəyyən məqsədlə hərəkət edir və öz məqsədinə çatmaq üçün əhəmiyyətli səy göstərməyə hazırdır. Əgər bir hücum üsulu uğursuz olarsa, digər üsulla nəticə əldə etməyə cəhd edilir. Adi bədniyyətlidən fərqli olaraq, hədəf diqqətlə seçilir və hücum aylarla, hətta illərlə davam edə bilər.
- ***Threat (təhdid).*** Hücumun mənbəyi hədəfin maraqlarına təhdid təşkil edir.

Hazırda informasiya təhlükəsizliyi sistemlərinin çoxu siqnaturaların və məlum təhdidlərin davranış modellərinin axtarışına əsaslanır. Belə sistemlər siqnaturaları hələlik məlum olmayan yeni hücumlara, o cümlədən APT-hücumlarına qarşı gücsüzdürlər. Big Data texnologiyaları əsasında bu hücumların vaxtında aşkarlanmasına ümid edilir [9].

IV. BİG DATA VƏ YENİ İNFORMASİYA TƏHLÜKƏSİZLİYİ TƏHDİDLƏRİ

Big Data texnologiyalarının təhlükəsizliyi üzrə son illər bir neçə işçi qrup yaradılmışdır. Onlar arasında bir sıra aparıcı ABŞ universitetinin və şirkətinin tədqiqatçılarını birləşdirən Cloud Security Alliance (CSA) qrupu 2011-2013-cü illərdə Big Data texnologiyalarının yaratdığı informasiya təhlükəsizliyi problemlərini analiz etmiş və bir neçə analitik hesabat hazırlamışdır [10-12]. Aşağıda bu qrupun müəyyən etdiyi 10 informasiya təhlükəsizliyi təhdidi təsvir olunur [10, 11].

1) Paylanmış proqramlaşdırma platformalarında informasiya təhlükəsizliyi

Paylanmış proqramlaşdırma platformaları çox böyük həcmdə verilənləri emal etmək üçün hesablama və saxlama proseslərində paralel emaldan istifadə edirlər. Geniş yayılmış yanaşma MapReduce platformasıdır MapReduce-un işi iki addımdan ibarətdir: Map və Reduce. Map-addımda giriş verilənləri ilkin emal edilir. Bunun üçün kompüterlərdən biri (mepper – əsas qovşaq) məsələnin ilkin verilənlərini alır, onu hissələrə bölür və ilkin emal üçün paylanmış fayl sisteminin işçi qovşaqlarına paylayır. Reduce-addımda əsas qovşaq ilkin emal edilmiş verilənləri işçi qovşaqlardan toplayır, onları birləşdirir və məsələnin həllini formalaşdırır. Hücumların qarşısını almaq üçün burada iki əsas tədbir var: mepperin təhlükəsizliyi və etibar edilməyən mepper halında verilənlərin təhlükəsizliyi.

2) Qeyri-relyasyon verilənlər bazaları üçün ən yaxşı təhlükəsizlik qaydaları

NoSQL (not only SQL və ya no SQL) − ənənəvi relyasion verilənlər bazalarında istifadə olunan SQL vasitəsilə verilənlərə müraciətdən əhəmiyyətli dərəcədə fərqlənən verilənlər bazası modellərinin reallaşdırılmasına yönəlmiş bir sıra layihələri, yanaşmaları bildirən termindir (2009-cu ildə meydana çıxıb). NoSQL texnologiyası ilə yaradılan qeyri-relyasion verilənlər bazaları təhlükəsizlik infrastrukturu baxımından hələlik inkişaf mərhələsindədir. Məsələn, NoSQL-inyeksiya hücumlarına qarşı dayanıqlı həllər hələlik əlyetər deyil. Hər bir NoSQL verilənlər bazası analitikanın müxtəlif problemini həll etmək üçün yaradılmışdır və bu səbəbdən təhlükəsizliyə layihələndirmə mərhələsində heç vaxt modelin əsas hissəsi

kimi baxılmamışdır. NoSQL verilənlər bazasında təhlükəsizlik üçün heç bir dəstək təmin edilmir və belə bazalardan istifadə edərkən təhlükəsizlik adətən aralıq proqram təminatının öhdəsinə buraxılır.

3) Verilənlərin və tranzaksiya loqlarının təhlükəsiz saxlanması

Verilənlər və tranzaksiya loqları verilənlərin çoxsəviyyəli saxlama mühitində saxlanır. Verilənlərin səviyyələr arasında mexaniki köçürülməsi zamanı IT-menecer hansı verilənin nə zaman köçürülməsinə birbaşa nəzarət edə bilir. Lakin verilənlərin həcminin eksponensial artması verilənlərin səviyyələr arasında avtomatik köçürülməsini tələb edir. Avtomatik köçürmə həlləri verilənlərin harada saxlanılmasını izləmir və bu təhlükəsizliyi təmin etmək üçün yeni problemlər yaradır.

4) Son-nöqtədə daxiletmənin yoxlanması

Böyük verilənlərin istifadəsi zamanı verilənlər bir çox mənbədən toplanır. Məsələn, SIEM sistemi (Security Information and Event Management – təhlükəsizlik məlumatlarının və hadisələrinin idarə edilməsi) şəbəkədə minlərlə aparat və proqram təminatından hadisə loqlarını toplaya bilər. Məlumatların toplanması prosesində əsas problem toplanmış verilənlərə nə dərəcədə etibar edilə bilməsidir. Verilənlər mənbəyinin həqiqi, yoxsa bədniyyətli olmasını aydınlaşdırmaq, bədniyyətlə daxil edilmiş verilənləri həqiqi verilənlərdən ayırmaq, filtrasiya etmək tələb edilir.

5) Təhlükəsizliyin real zaman rejimində monitorinqi

Təhlükəsizliyin real zamanda monitorinqi təhlükəsizlik qurğularının yaratdığı siqnalların sayı baxımından həmişə böyük problem olmuşdur. Bu siqnalların bir çoxu hücum haqqında səhv siqnallar olur, onların öhdəsindən gəlmək mümkün olmadığından, sadəcə, nəzərə alınmırlar. Bu problem həcmi və sürəti artan Big Data nəticəsində daha da böyüyəcək. Lakin Big data texnologiyaları sürətli emal və məlumatların müxtəlif növlərinin analizi ilə müəyyən imkanlar da yaradır. Bu, məsələn, anomaliyaların real zamanda aşkarlanmasına imkan verə bilər.

6) Gizliliyi saxlayan Big Data analitikası

Big data şəxsi həyatın gizliliyinə, vətəndaş azadlıqlarının pozulmasına potensial təhdidlər yaradır, dövlət və korporativ nəzarət imkanlarını artırır. Şirkətlərin marketinq məqsədləri üçün Big Data analitikasından istifadə edərək şəxs barəsində gizli məlumatlar əldə edə bilərlər (məsələn, pərakəndə satış firması yeniyetmə qızın hamilə olduğunu onun ailəsindən əvvəl öyrənmişdi). Eynilə, analitika üçün verilənlərin anonimləşdirilməsi istifadəçi gizliliyini qorumaq üçün kifayət deyil. Məsələn, AOL tədqiqat məqsədləri üçün anonim axtarış loqlarını açmışdı, lakin istifadəçiləri axtarış sorğuları əsasında asanlıqla müəyyən etmək mümkün olmuşdu. Netflix də oxşar problemlə üzləşmişdi, IMDB balları ilə Netflix film ballarını əlaqələndirməklə Netflix anonim verilənlərindən istifadəçilər identifikasiya edilmişdi. Buna görə də, gizliliyin təsadüfən pozulmalarının qarşısını almaq üçün qaydalar və tövsiyələr yaratmaq vacibdir.

7) Kriptoqrafiya ilə həyata keçirilən girişə nəzarət və təhlükəsiz kommunikasiya

Daha həssas fərdi məlumatların tam təhlükəsizliyini və yalnız icazə verilmiş subyektlər tərəfindən müraciət edilməsini təmin etmək üçün verilənlər girişə nəzarət siyasəti əsasında şifrlənməlidir. Autentifikasiyanı və rəqəmsal imzanı təmin etmək üçün paylanmış subyektlər arasında təhlükəsiz kriptoqrafik kommunikasiya platforması reallaşdırılmalıdır.

8) Girişə qranulyar nəzarət

Girişə nəzarətin funksiyası verilənlərə giriş hüququ olmayan istifadəçilərin bu verilənlərə girişinin qarşısını almaqdır. Girişə qranulyar nəzarət nexanizmlərinin əsas problemi ondadır ki, paylaşıla bilən verilənlər təhlükəsizliyə zəmanət vermək üçün çox zaman daha məhdudlaşdırıcı kateqoriyalar altında saxlanır. Girişə qranulyar nəzarət isə təhlükəsizliyi pozmadan daha çox istifadəçiyə giriş hüququ verməyə çalışır.

9) Qranulyar audit

Təhlükəsizliyin real zamanda monitorinqində hücum baş verdiyi anda xəbər veriləcəyinə cəhd edilir. Əslində, bu həmişə belə olmur (məsələn, yeni hücumlar, hücumların aşkarlanmaması). Buraxılmış hücumları aşkarlamaq üçün audit məlumatları lazımdır. Bu yalnız nəyin baş verdiyini və nəyin yanlış olduğunu aşkarlamaqla bağlı deyil, standartlara uyğunluq və məhkəmə ekspertizası ilə də əlaqədar ola bilər. Bu baxımdan audit yeni bir şey deyil, lakin miqyas və qranulyarlıq fərqli ola bilər. Məsələn, baxılacaq verilənlər obyektləri çox ola bilər və onlar paylanmış ola bilərlər.

10) Verilənlərin mənşəyi

Bir sıra mühüm təhlükəsizlik proqramları verilənlərin mənbəyinin bilinməsini – onların yaradılması haqqında ətraflı məlumat əldə edilməsini tələb edir. Məsələn, maliyyə şirkətlərində insayder fəaliyyətinin aşkarlanması təhqiqatları verilənlər mənbəyinin dəqiqliyini tələb edir. Big Data tətbiqləri inkişaf etdikcə verilənlərin mənbəyi haqqında metaverilənlər də sürətlə artır və onların emalı üçün sürətli alqoritmlər tələb edilir.

V. İNFORMASİYA TƏHLÜKƏSİZLİYİ ÜÇÜN BİG DATA ANALİTİKASI

Big Data texnologiyaları informasiya təhlükəsizliyi sahəsində xeyli əvvəl tətbiq edilir. İlk SIEM sistemləri hələ 1996-cı ildə təqdim edilmişdi, bu sistemlər 2000-ci illərin ortalarından geniş yayılmağa başlayır. SIEM-sistemlərin nə üçün Big Data texnologiyalarına aid edilə bilməsi sualı, heç kimdə şübhə doğurmamalıdır: hadisələrin toplanması, normallaşdırılması və korrelyasiyası istənilən müasir Big Data sisteminin əsas və məcburi elementidir.

Ənənəvi SIEM-sistemlərinin bir sıra nöqsanları vardır:

- təhdidlərin aşkarlanması və təhqiqatı sahəsində imkanlar məhduddur;
- məhdud verilənlər mənbələri istifadə edilir;
- verilənlərin süzülməsi/normallaşdırılması zamanı verilənlərin itkisi qaçılmazdır;

– relyasion verilənlər bazaları miqyas və sürət problemləri yaradır;

– insidentlərin təhqiqatı və məhkəmə ekspertizası imkanları məhduddur.

SIEM-sistemlərin Big Data texnologiyaları ilə inteqrasiyasının bir neçə yolu movcuddur. Hazırda SIEM-sistemlərin ikinci nəslinin meydana çıxması haqqında danışmaq olar, lakin onların funksiyalarını bir çox cəhətdən intellektual təhlükəsizlik (Security Intelligence) sahəsinə aid etmək olar.

Gartner ekspertləri hesab edirlər ki, Big Data analitikası informasiya təhlükəsizliyi sistemlərini daha etibarlı etməyə və onlarda səhv həyəcan siqnallarını aradan qaldırmağa imkan verəcək [5]. Big Data analitikası üzrə həllərin böyük üstünlüyü təkcə informasiya təhlükəsizliyi sistemlərinin hadisələri arasında deyil, biznes-sistemlərin hadisələri ilə də korrelyasiyanın təmin etməsi imkanıdır.

İnformasiya təhlükəsizliyi həlləri təqdim edən bir çox şirkət Big Data texnologiyalarının informasiya təhlükəsizliyi sahəsində imkanlarını vurğulayan marketinq məlumatları çap etdirmişdir [13, 14]. CSA işçi qrupunun hesabatında Big Data-nın təhlükəsizlikdə rolu araşdırılır və mümkün tədqiqat istiqamətləri diqqətə çatdırılır [12]. İnformasiya təhlükəsizliyi sahəsində Big Data aşağıdakı imkanları təqdim edir [2, 12, 15]:

– kiber-hücumların aşkarlanması dəqiqliyinin yaxşılaşdırılması;

– real zaman ərzində korrelyasiya və anomaliyaların aşkarlanması;

– daha dərin məhkəmə ekspertizası ;

– böyük həcmdə verilənlərin vizuallaşdırılması və analizi üçün qrafik alətlər [16];

– daha yaxşı və sürətli qərarlar.

Sadalanan imkanların keyfiyyətli şəkildə reallaşdırılması müvafiq elmi və praktiki tədqiqatların aparılmasını tələb edir. Müxtəlif məlumat mənbələrindən alınmış çox böyük həcmdə verilənləri emel edə bilən aşkarlama alqoritmlərinin işlənməsi tələb edilir. Hazırda informasiya təhlükəsizliyi hadisələrinin aşkarlanması üçün Big Data analitikasından istifadə edən və perspektivli nəticələr göstərən az sayda iş vardır [17-20].

Big Data e-dövlətin informasiya təhlükəsizliyinin real zaman rejimində monitorinqi üçün müəyyən imkanlar vəd edir. Big Data texnologiyalarının e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi sistemində tətbiqinə – Big Data əsasında təhlükəsizlik əməliyyatları mərkəzinin (Security Operations Center) qurulması məsələsinə [21]-də baxılır.

İnformasiya təhlükəsizliyi sahəsində Big Data texnologiyalarının uğurlu tətbiqi üçün uyğun ixtisaslı kadrların olması çox vacib elementdir. Bu baxımdan problemlərdən biri belə kadrların çatışmazlığıdır. Xüsusi bacarıqlara verilənlərin idarə edilməsi, verilənlərin analizi və təhlükələrin analizi bacarıqları daxildir. Bu bacarıqların hər üçünün bir şəxsdə olmasına az rast gəlinir, buna görə təşkilatların Big Data səylərində optimal nəticələrə nail olmaq üçün əməkdaşlıq edən mütəxəssis qruplarının yaradılması lazımdır.

NƏTİCƏ

Big Data böyük həcmdə heterogen verilənlərin analizi sahəsində böyük perspektivlər vəd edən paradiqma kimi meydana çıxmışdır. Big Data texnologiyaları özü ilə yeni informasiya təhlükəsizliyi təhdidləri gətirir, eləcə də təhlükəsizlik həllərində köklü dəyişikliklər vəd edir.

Lakin informasiya təhlükəsizliyinin təmin edilməsi üçün əhəmiyyətli imkanlar vəd etməsinə baxmayaraq, bu Big Data potensialından tam istifadə etmək üçün bu məqalədə göstərilmiş bir çox problem həll edilməlidir. Hədəfəyönəlik hücumların aşkarlanması, verilənlərin sızmasının aşkarlanması, məhkəmə ekspertizası, təhlükəsizlik kəşfiyyatı və vizuallaşdırma sahəsində tədqiqatlara yalnız indi diqqət yönəlməkdədir. Ona görə də tədqiqatçıların bu sahədə fundamental töhfələr verəcəyinə və innovasiyaların inkişafına əhəmiyyətli təsir göstərən kəşflər edəcəyinə böyük imkanlar və ümidlər vardır.

ƏDƏBİYYAT

[1] R. M. Əliquliyev, M. Ş. Hacırəhimova, “Big data” fenomeni: problemlər və imkanlar,” İnformasiya texnologiyaları problemləri, №2, s.3-16, 2014

[2] R.Alguliyev, Y.Imamverdiyev, “Big Data: Big promises for information security,” IEEE 8th International Conference on Application of Information and Communication Technologies (AICT), 2014.

[3] J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, and A. H. Byers. Big data: The next frontier for innovation, competition, and productivity. McKinsey Global Institute, May 2011.

[4] K. C. Desouza, Realizing the promise of Big Data: Implementing Big Data projects. IBM Center for The Business of Government. 2014.
http://www.businessofgovernment.org/sites/default/files/Realizing%20the%20Promise%20of%20Big%20Data.pdf.

[5] L.Kart, N.Heudecker, F.Buytendijk, “Survey Analysis: Big Data Adoption in 2013 Shows Substance Behind the Hype.” September 2013. http://www.gartner.com/newsroom/id/2593815

[6] The Australian Public Service Big Data Strategy. August 2013. http://agict.gov.au/sites/default/files/Big%20Data%20Strategy.pdf

[7] Big Data Research and Development Initiative. March 29, 2012.
http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf

[8] Communication on data-driven economy. http://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy

[9] A.K.Sood, R.J.Enbody, “Targeted cyberattacks: A superset of Advanced Persistent Threats,” IEEE Security & Privacy, Vol. 11, No. 1, pp. 54-61, 2013.

[10] Cloud Security Alliance (CSA): Top ten Big Data security and privacy challenges. 2012.

[11] Cloud Security Alliance (CSA): Expanded top ten Big Data security and privacy challenges. 2013.

[12] Cloud Security Alliance (CSA): Big Data Analytics for Security Intelligence. 2013. https://cloudsecurityalliance.org/download/big-data-analytics-for-security-intelligence

[13] J. Oltsik, “IBM: An Early Leader across the Big Data Security Analytics Continuum”. White paper, June 2013.

[14] M. Bouchard, “Big Data for advanced threat protection.” 2012.

[15] A. A. Cardenas, Manadhata P. K., and Rajan S. P., “Big Data Analytics for security,” IEEE Security & Privacy, Vol. 11, No. 6, pp.74-76, 2013.

[16] A. Shiravi, H. Shiravi, and A.A. Ghorbani, “A survey of visualization systems for network security,” IEEE Transactions on Visualization and Computer Graphics, Vol. 18, No. 8, pp. 1313-1329, 2012.

[17] Dumitras T., Shou D., “Toward a standard benchmark for computer security research: The Worldwide Intelligence Network Environment (WINE),” Proc. EuroSys BADGERS Workshop, pp. 89–96, 2011.

[18] J. François et al., “BotCloud: Detecting botnets using MapReduce,” Proc. Workshop Information Forensics and Security, pp. 1–6, 2011.

[19] T.-F. Yen et al., “Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks,” Proc. Annual Computer Security Applications Conference (ACSAC 13), pp. 199-208, 2013.

[20] Y. Lee, Y. Lee, "Toward scalable Internet traffic measurement and analysis with Hadoop," ACM SIGCOMM Computer Communication Review, Vol. 43, No. 1, pp. 5-13, 2013.

[21] Z.Fataliyev, Y.Imamverdiyev, H.Ko, “Security Operation Center architechture for e-government based on Big data Analysis”, Elektron dövlət quruculuğu problemləri I respublika elm-praktiki konfransı, s. 140-144, 2014.