Fərdi məlumatların Wikileaks-yönümlü sosial mühitlərə sızma risklərinin idarə olunması

Fərqanə Abdullayeva

AMEA İnformasiya Texnologiyaları İnstitutu

farqana@iit.ab.az

***Xülasə*— Məqalədə fərdi məlumatların sızma problemlərinin müasir vəziyyəti analiz olunur. Sızmaya bilavasitə təsir edən insayderlərin təşkilat daxilində hüquqi tənzimlənməsi yollarının beynəlxalq təcrübəsi araşdırılır. Fərdi məlumatların sızma məkanı olan Wikileaks saytının əsas prinsipləri tədqiq olunur. Mövcud sızma risklərinin azaldılması üçün təşkilatın informasiya təhlükəsizliyini idarə edən mükəmməl infrastrukturun qurulması istiqamətində bir sıra tövsiyələr verilir.**

Açar sözlər— fərdi məlumatlar; informasiya sızması; insayder; Wikileaks

I. GİRİŞ

Müasir dövrdə məxfi və ya fərdi məlumatlar dünyanın bir sıra maliyyə, səhiyyə, təhlükəsizlik idarələrinin mühüm alətinə çevrilmişdir. Onların mühafizə məsələlərinin təşkili uzun müddətdir ki, cəmiyyətin qarşısında duran ən vacib təhlükəsizlik məsələsi kimi qiymətləndirilir. Bu tip məlumatların üçüncü şəxslərə sızdırılması, informasiya subyektinə ciddi ziyanın vurulması ilə nəticələnə bilər.

Son illər fərdi məlumatların sızma faktlarında kəskin artım müşahidə olunur. Belə ki, "Privacy Righ Clearenghouse" adlı qeyri-kommersiya təşkilatının mövcud araşdırmasına görə 2013-cü ildə təkcə ABŞ-da həssas fərdi məlumatlardan ibarət 607472154 fərdi uçot qeydi itkiyə məruz qalmışdır [1]. Digər tərəfdən, 2010-cu ildə İraq müharibəsinin 391832 məxfi sənədi sızma məkanı olan Wikileaks saytında icazəsiz nəşr edilmişdir, bu fakt dünyada ən böyük tarixi sızma faktı kimi qiymətləndirilir [2]. Fərdi məlumatların sızma hallarının bu şəkildə artımı və onların subyektlərə neqativ təsiri, hazırda əksər dövlət, kommersiya, təhsil müəssisələrinin qarşısında duran mühüm problemə çevrilmişdir.

Fərdi məlumatların sızma hallarının qarşısını alan çox sayda sistemlər vardı. Bu sistemləri adətən "İnformasiya sızmalarına qarşıdurma sistemləri" (Data Loss Prevention, DLP) adlandırırlar [3]. DLP sistemlər korporativ informasiyanı insayder hücumlarından mühafizə edir. DLP sistemlərin istehsalı ilə məşğul olan lider təşkilatlar sırasına Symantec, Websense, TrendMicro, McAffee, RSA təşkilatları aiddir. Bu təşkilatlar sırasında Symantec təşkilatı özünün "Symantec Data Loss Prevention" məhsuluna görə Gatner analitik təşkilatı tərəfindən 7 dəfə DLP-sistemləri arasında lider təşkilat kimi qiymətləndirilmişdir. Digər tərəfdən, reputasiya sistemləri vardır ki, bu sistemlər spam və fişinq tipli sızmaların qarşısını almağa xidmət edir [4]. Bu sistemlərə əsasən sızmanın qarşısını almaq üçün e-poçt göndərən tərəf məqbul sayılan reputasiya xalqına malik olmalıdır ki, ikinci şəxs tərəfindən qəbul olunsun. Hazırda bulud-yönümlü DLP sistemlərin yaradılması istiqamətində də ciddi addımlar atılır. Bu sistemlərdən biri InfoWatch Kribrum-dur [5]. Bu sistem İnternet mühitinə sızdırılmış fərdi məlumatların, kommersiya sirrlərinin və s. aşkarlanmasını həyata keçirir. Bunun üçün o İnternetdə aparılan müzakirələrin monitorinqini apararaq, informasiyanın analizini həyata keçirir və müzakirə obyektini aşkarlayaraq emosional qiymətləndirmə aparır.

Hazırda yeni texnologiyaların meydana gəlməsi ilə əlaqədar olaraq təşkilatlarda strukturlaşmamış məlumatların həcminin artması səbəbindən mövcud DLP-sistemlər konfidensial informasiyanın sızma hallarının səmərəli aşkarlanmasını təmin etmir. Bu səbəbdən yeni texnologiyaların vəziyyətinə uyğunlaşa bilən adaptiv üsulların işlənməsi zərurəti meydana çıxır.

İnformasiyanın sızma hallarının qarşısının alınması məsələlərinin texnoloji aspektləri üzrə çox sayda elmi-tədqiqat işləri aparılmışdır. Bu tədqiqatlarda [6] təhlükəsizlik siyasətinin qurulmasına əsaslanan model təklif olunur. Bu modelə əsasən, yalnız avtorizasiyası olan istifadəçilərin həssas fərdi məlumatlara girişinə icazə verilir. Digər yanaşmada [7] məlumat qəbul edən subyektin etibarlı olub-olmadığını müəyyən etmək üçün risklərin qiymətləndirilməsi metodundan istifadə olunur. Burada hesablamalar subyektin statik metrikaları əsasında aparılır. Bu isə İnternet kimi dinamik mühitdə uğurlu nəticələr əldə etməyə imkan vermir. Bu problemin aradan qaldırılması üçün risklərin qiymətləndirilməsinin istifadəçinin davranışını xarakterizə edən metrikalar əsasında aparılması məqsədəuyğun olardı. Bu məsələsinin həllində insayderlərin aşkarlanması üçün *"Author Topic"* adlı klasterləşmə alqoritmindən istifadə edərək gündəlik göndərilən poçt məlumatlarına əsasən işçilərin maraq dairələrinin müəyyən olunması maraqlı yanaşmalardan biridir [8]. Aşkarlanmış maraq dairələri əsasında iki növ sosial şəbəkə qurulur və mövcud insayderləri aşkarlamağa xidmət edir. Bunun üçün təşkilata qarşı yad münasibətdə olan şəxslərin və həssas fərdi məlumatlar ətrafında müzakirələr aparan şəxslərin tapılmasına cəhd olunur. Tədqiqatın eksperimentləri "Enron" elektron poçt bazasında reallaşdırılır. Yuxarıda adı çəkilən tədqiqat işinin çatışmayan cəhəti odur ki, burada insidentlər sızma halları baş verdikdən sonra aşkarlanır. Bu isə fərdi məlumatların toxunulmazlıq tələbinin pozulması ilə nəticələnir. Fərdi məlumatların toxunulmazlığını təmin etmək üçün, onların mühafizəsini sızma halı baş verməzdən əvvəl təmin edən metodların işlənməsi zəruri hesab olunur.

II. FƏRDİ MƏLUMATLARIN SIZMASI VƏ WIKILEAKS

Hazırda Avropa ölkələrində informasiya azadlığı və fərdi məlumatların mühafizəsi məsələləri ilə məşğul olan ayrıca

İnformasiya Komissarları (Information Commissioner) yaradılmışdır. Bu komissarlıq vətəndaşlara adətən xüsusi Ombusman xidməti göstərir. İnformasiya Komissarlıqlarının fəaliyyət göstərdiyi ölkələr sırasına Avstraliya, Kanada, Almaniya, Hindistan, İrlandiya, Böyük Britaniyanı aid etmək olar.

Böyük Britaniyanın və Avstraliyanın İnformasiya Komissarlıqları tərəfindən qəbul olunmuş sənədlərdə fərdi məlumatlara aşağıdakı kimi tərif verilir: şəxsin identikliyini müəyyən edən doğru və yalan məlumatlara, eyni zamanda mülahizələrə *fərdi məlumatlar deyilir* [9]. "Fərdi məlumatlar" anlayışına insanın soyadı, adı, atasının adı, anadan olduğu tarix və yer, yaşadığı ünvan, ailə, sosial və əmlak vəziyyəti, təhsili, peşəsi, maliyyə gəliri və s. haqqında məlumatlar daxildir [10].

Adi fərdi məlumatlardan fərqli olaraq, *həssas fərdi məlumatlar* vardır ki, onların hüquqi tənzimlənməsinə daha ciddi diqqət yetirilməlidir.

Şəxsin irqi və ya etnik mənsubiyyətinə, siyasi baxışlarına, siyasi qurumlarda üzvlüyünə, dini mənsubiyyətinə, fəlsəfi inanclarına, seksual münasibətlərinə, kriminal fəaliyyətinə, sağlamlığına, genetik təbiətinə aid məlumatlar və mülahizələr *həssas fərdi məlumatlar* adlanır [9].

Müasir dövrdə həssas fərdi məlumatların rəqəmsal təbiətə malik olması onların hədsiz sayda nüsxələnməsinə və qlobal miqyasda geniş yayılmasına gətirib çıxarır. Bu isə onların bədniyyətli istifadəçilər tərəfindən icazəsiz üçüncü tərəf şəxslərə sızdırılmasına şərait yaradır və şəxsə ciddi ziyanın vurulması ilə nəticələnir.

Ümumilikdə, *informasiya sızması (ing. data leakage)* – məxfi və ya fərdi məlumatların icazəsi olmayan üçüncü tərəf subyektlərə ötürülməsidir [3].

Hazırda sızma məkanı kimi fəaliyyət göstərən bir sıra veb-saytlar mövcuddur. Məşhur sızma saytları siyahısına Anonymous, Lulz Security, WikiLeaks aiddir. Bu saytlara məxfi məlumatlar siyasi motivasiyalı haker hücumları həyata keçirən *haktivist* qrupları tərəfindən sızdırılır. *Haktivistlər* - **x**aker üsullarından istifadə edərək siyasi-yönümlü məlumatların sosial mühitlərə sızmasını həyata keçirən şəxslərdir. *Haktivizm – hakinq* və *aktivizm* terminlərinin birləşməsidir. İnformasiya texnologiyalarının siyasi hərəkatlara tətbiqidir.

Açıqladığı məlumatların çəkisinə görə dünya mediasında məşhurluq qazanmış sayt Wikileaks bir çox ədəbiyyatlarda korrupsiya halları haqqında məlumat yayımlayan (ing. whistle-blowing) nəşr təşkilatı kimi də adlandırılır.

Wikileaks, havay sözü olan *Wiki*-sürətli, və ingilis sözü olan *leak* - sızma sözlərinin birləşməsidir, mənası "sürətli sızma" deməkdir. Mənbəyi qeyri-müəyyən şəkildə təqdim edərək məxfi məlumatların, sızdırılmış xəbərlərin, gizli media məlumatlarının nəşri ilə məşğuldur. Bu təşkilatın veb-saytı 2006-cı ildə İslandiyada "SunShine Press" təşkilatı tərəfindən təsis edilmişdir. Saytın yaradıcısı, baş redaktoru və direktoru avstraliyalı Julian Assancdır.

Sayt *"Wiki"* üslubunda qurulduğu üçün onu Wikileaks adlandırırlar. Məşhur Wikipedia saytında olduğu kimi, burada da hər kəsə sistemə kontent əlavə etməyə, bu kontenti redaktə etməyə imkan verilir. Wikileaks saytının yaradılmasında məqsəd həssas məlumatları ictimaiyyətə yayımlamaqla, korrupsiya halları inkişaf etmiş ayrı-ayrı dövlətlərdə islahatlar yaratmaqdır.

Wikileaks 2007-ci ildən bəri müxtəlif ölkələrin minlərlə hərbi, siyasi və korporativ sirr daşıyan zorakıllıq faktlarını ifşa etmişdir. Burada şərh olunan açıqlamalar müxtəlif ölkələrdə bir sıra islahatların aparılmasına səbəb olmaqla yanaşı, ölkələr arasında ciddi müharibələrin yaranmasına da böyük təkan vermişdir. Wikileaks tərəfindən veb mühitə sızdırılan sənədlərdən biri ABŞ hərbçilərinin Quantanamo bazası adlandırılan istintaq təcridxanasında aparılan əməliyyatları gündəlik qeydə alan hərbi sənəd olmuşdur. Sənəddən əsasən ABŞ hökumətinin 2002-ci ildən bəri həbs etdiyi minlərlə şübhəli bilinən terrorçular haqqında məlumatlar işıqlandırılmışdır. Bu sənədin əvvəllər heç bir mənbədə nəşri qeydə alınmamışdır.

Wikileaks nəşr üçün yalnız məxfi, senzuradan keçmiş, daha doğrusu məhdudiyyətlər qoyulmuş siyasi, diplomatik və etik əhəmiyyətli materialları qəbul edir. Burada şayiə, mühakimə, açıq xarakterli materialların nəşrinə yol verilmir.

III. İNFORMASİYA TƏHLÜKƏSİZLİYİ SIZMALARININ XRONOLOGİYASI

İnformasiya sızması faktları hələ yazı və danışıq dili meydana gələn dövrdən mövcud olmuşdur.

1605-ci il, Barıt sui-qəsdi. 1605-ci ildə İngiltərənin kralı Ceymsi 36 barıt çəlləyindən istifadə edərək öldürmək məqsədi ilə ingilis katolik qrupu plan qurur və onu anonim məktubda şərh edir. Bu dövrdə Qay Favkes barıt çəlləyinin lordlar palatasında saxlandığını aşkarlayır. Həmin vaxtdan planın uğursuzluğu ilə bağlı şənlənmək üçün İngiltərədə Atəşfəşanlıq Gecəsi (Guy Fawkes Day, Bonfire Night or Firework Night) adı ilə tanınan milli bayram qeyd edilir. Hazırda haktivist qruplaşması kimi tanınan *Anonymous* Qay Favkes maskalarını özləri üçün simvol qəbul etmişdir. Bu qrupun üzvləri bütün etiraz aksiyalarında Qay Favkes maskalarında çıxış edirlər.

1774–1783-ci il, Kasanovanın gündəliyi. Kasanova casus olub. O, Venesiyanın məhkəmə təhqiqatçılarına məxfi məlumat çatdırmaqla məşğul idi. Kasanova casusluq etdiyi zaman topladığı hər bir məxfi məlumatı özünün gündəlik dəftərinə qeyd edirdi. Bu gündəlikdə Venesiyanın əleyhinə qeyd aşkarlandıqdan sonra o, Venesiyadan sürgün edilmişdir.

1780-cı il, Arnold Benedikt. Arnold Benedikt ABŞ tarixində məşhur casuslardan biri olmuşdur. O, Amerikanın hərbi hərəkatları ilə əlaqədar və Amerikanın "West Point" adlı hərbi akamediyasının nəzdindəki qalaya giriş planı haqqında məxfi məlumatları Britaniyaya satmağa cəhd göstərmişdir. Bu planın üstü Britaniyanın baş casusu mayor Con Andrinin Arnoldla gizli görüşdən sonra həbsi zamanı açılmışdır. Sonralar Andri bu əməlinə görə casus kimi asılmışdır. Arnoldl isə Corc Vaşinqtonun silahlı qüvvələri tərəfindən tutulmamaq üçün Amerikanı tərk etməyə məcbur olmuşdur

2010-cu il, WikiLeaks və İraq müharibəsinin qeydləri. WikiLeaks silsilələrlə sızılmış dövlət sənədlərinin və İraq müharibəsinin məxfi video-materiallarını veb-saytda açıq şəkildə işıqlandırdığı andan Amerika mediasının diqqət mərkəzində məşhurlaşmışdır. Bu video-materiallarda

jurnalistlərin silahlı qüvvələr tərəfindən güllələnməsi nümayiş etdirilirdi. Sonralar Pentaqon "İraq müharibəsinin qeydlərinin" WikiLeaks saytına sızmasını öz tarixində böyük hadisə adlandırmışdır. WikiLeaks-in Twitter sosial şəbəkəsində 1.5 milyon davamçısı, Facebook şəbəkəsində isə 2 milyon azarkeşi var.

2012-ci il, WikiLeaks və Suriya faylları. 2012-ci ildə Suriyanın siyasi xadimləri tərəfindən göndərilən 2.4 milyondan çox məxfi elektron poçt məktubları WikiLeaks saytında işıqlandırılmışdır. Elektron poçt məktubları Aktivistlər qrupunun böyük fədakarlığı sayəsində əldə edilmişdir. Bu məktublar 2006-2012-ci illər ərzində göndərilən elektron poçt məktubları idi və bu günədək sızdırılmış sənədlərin böyük toplusunu təşkil edirdi. Əsasən Suriyanın Prezident işləri üzrə Nazirliyi, Xarici işlər Nazirliyi, Maliyyə Nazirliyi, İnformasiya Nazirliyi və Nəqliyyat Nazirliyinin arasında göndərilən məxfi ismarıclardan ibarət idi.

IV. İNSAYDERLƏR VƏ FƏRDİ MƏLUMATLARIN SIZMA VASİTƏLƏRİ

Bir sıra analitik təşkilatların apardığı tədqiqatlara görə fərdi məlumatların sızdırılmasına yönəlmiş təhdidlərin 59 faizini insayderlər təşkil edir [11].

İnsayder (ing. insider) - təşkilatın resurslarına icazəsi olan şəxsdir, lakin məxfi resursları icazə olmadan ləğv etməyə və kənar mühitə sızdırmağa və ya digər şəxslərə bu əməliyyatları reallaşdırmaqda kömək etməyə cəhd edir [12].

ABŞ-da fərdi məlumatlarla işləyən dövlət və özəl təşkilatlarda xüsusi qanunvericilik aktları icra olunur. Bu qanunlar təşkilat əməkdaşlarının qarşısında fərdi məlumatların açıqlanması hallarına aid xüsusi tələblər qoyur:

- *The Health Insurance Portability and Accountability Act (HIPAA).* 1996-cı ildə qəbul olunub, elektron şəkildə qorunan səhiyyə məlumatlarının mühafizə olunması tələblərini müəyyən edir.
- *California SB 1386.* 2003-cü ildə qəbul olunub, Kaliforniya sakinlərinin fərdi məlumatlarının sızma faktlarını aşkarlamaq və onlar haqqında bildirişləri yayımlamaq tələblərini müəyyən edir.
- *The Gramm-Leach Bliley Act (GLBA).* 1999-cu ildə qəbul olunub, maliyyə təşkilatları tərəfindən idarə olunan müştəri məlumatlarının mühafizəsi üçün inzibati, texniki və fiziki təminat tələblərini müəyyən edir.
- *The Payment Card Industry (PCI) Data Security Standard.* 2010-cu ildə yaradılmışdır, kredit kartı əməliyyatlarının həyata keçirilməsi üçün lazım olan təhlükəsizlik tövsiyələrini müəyyən edir.

Fərdi məlumatların veb-mühitə sızmasına şərait yaradan bir sıra vasitələr vardır [4]:

- *Ani ismarıc (Instant Messaging).* Bir çox təşkilatlarda ani ismarıc xidmətlərinin istifadəsinə geniş yol verilir. Bu xidmətlərə MSN Messenger, Skype, AOL, GoogleTalk, ICQ və s. aiddir. Bu xidmət bir sıra üstünlüklərlə yanaşı, konfidensial sənədləri icazəsi olmadan üçüncü tərəf şəxslərə asanlıqla göndərməyə imkan verir.
- *E-poçt.* Microsoft Outlook, Lotus Notes, Eudora ənənəvi e-poçt kliyentləridir. Burada daxili istifadəçi konfidensial sənədi maskalamaq məqsədi ilə onu sıxılmış fayl şəklində avtorizasiyası olmayan tərəfə göndərir.
- *Veb-mail.* Gmail, Yahoo, Hotmail və s. məşhur veb-poçtlardır. Bu növ poçt xidmətləri HTTP üzərində qurulduğu üçün adətən şəbəkəarası ekranlar bunları icazəli trafik kimi qəbul edir.
- *Veb-loqlar/vikilər.* Veb-loqlar (bloqlar) istifadəçilərə müəyyən bir mövzu haqqında öz düşüncələrini, fikirlərini, şərhlərini ifadə etməyə imkan verən veb saytlardır. Bloqlar konfidensial məlumatların işıqlandırılması üçün də istifadə edilə bilər. Viki sayt müştərək veb-saytdır, istənilən şəxs tərəfindən redaktə edilə bilər. Bu saytlar dünyanın bütün internet istifadəçilərinə əlyetən olur və konfidensial informasiyanın viki səhifələrdə işıqlandırılması imkanlarına malikdir.
- *Ziyankar veb-səhifələr.* Təhlükəyə məruz qalmış veb-saytlar və ya qəsdən yaradılmış ziyankar saytlar istifadəçi kompüterinin virusa yoluxma ehtimalını artırır.
- *Dinamik daşıyıcılar/yaddaş qurğuları.* Fərdi məlumatların sızması hallarının böyük hissəsini flaş-yaddaş qurğularının itməsi təşkil edir.
- *Təsnifat xətaları.* Girişin idarə edilməsi modellərinin təsnifat aparan zaman yol verdiyi səhvlərlə bağlıdır. Bu səhv tam məxfi sayılan sənədin adi istifadəçiyə göndərilməsi ilə nəticələnə bilir.
- *Kameralar.* Bədniyyətli istifadəçi konfidensial informasiyanı ekranlarda rəqəmsal fotoçəkiliş etməklə əldə edir.
- *Verilənlərin bədniyyətli istifadəçilər tərəfindən oğurlanması.* Bədniyyətli istifadəçinin təşkilatın daxilinə elektron müdaxiləsidir, həssas məlumatın oğurlanması ilə nəticələnir.
- *SQL kodun əlavə edilməsi.* İstifadəçi sorğusuna SQL-kodun əlavə olunması prosesinə əsaslanır. Bu əməliyyatı həyata keçirməklə hücumçu konfidensial məlumatlar saxlanan verilənlər bazasında istədiyi əməliyyatı reallaşdıra bilər.
- *Ziyankar proqram təminatı (malware).* Fərdi kompüterləri yoluxduraraq, onların kənar obyektlərlə əlaqə qurmasına şərait yaradır. Bu isə həssas məlumatların təşkilatdan kənara ötürülməsi ilə nəticələnir.
- *Zibil konteyneri.* Təşkilatın konfidensial informasiyasının zibil yeşiyinə atılması ilə bağlı təhdiddir. Bu təhdidin reallaşması nəticəsində hücumçu təşkilatın zibil konteynerində axtarış edərək konfidensial informasiyanı əldə edir.

- *Fişinq*. Sosial mühəndislik hücumlarının bir növüdür, istifadəçini müəyyən ziyankar saytlara yönəldərək, onun istifadəçi adını, parolunu ələ keçirməyə cəhd edir.
- *Sosial mühəndislik.* Məsul şəxslərin zəifliyindən istifadə edərək reallaşan boşluqdur. Olduqca təhlükəli hücum növüdür, çünki bədəməl adi telefon zəngi edərək və yaxud özünü təşkilatın əməkdaşı rolunda təqdim edərək məsul şəxsləri aldadır və onlara lazım olan fərdi məlumatları əldə edir.
- *Kompüter sistemlərinin fiziki oğurlanması.* Müxtəlif informasiya daşıyıcılarının fiziki oğurlanmasıdır, konfidensial informasiyanı sızmaya məruz qoyur.

V. SIZMA RİSKLƏRİNİN QİYMƏTLƏNDİRİLMƏSİ

Göründüyü kimi, müəssisələrdə geniş istifadə olunan sızma vasitələrinin sayı olduqca çoxdur. Bu sızma vasitələrində mövcud boşluqlar həssas fərdi məlumatların sızma riskini olduqca artırır. Digər tərəfdən, müəssisənin əməkdaşlarının insayder qismində çıxış edərək təhdid təşkil etməsi, sızma riskini qiymətləndirməyə imkan verir.

Risk – itkinin baş vermə ehtimalıdır və ya itkiyə təsir edən faktordur [13]. Risk sızmaya nail olmaq üçün mümkün boşluqdan istifadə edən təhdidin ehtimal funksiyası kimi müəyyən oluna bilər. *Təhdid* həssas fərdi məlumatı qəsdən və ya təsadüfən sızdırmağa cəhd edən şəxs və ya prosesdir. Bu şəxslər həm taşkilatın daxilində fəaliyyət göstərən narazı əməkdaşlar, həm də kənardan rəqib təşkilat və ya xaker nümayəndələri ola bilər. *Boşluq* texniki zəiflikdir, təhdidin həssas məlumatlara nüfuz etməsinə şərait yaradaraq, onların təşkilatdan kənar mühitə sızmasını təmin edir. Riski qiymətləndirmək üçün həm boşluq, həm də təhdid hər ikisi eyni zamanda mövcud olmalıdır. Məsələn, fərz edək ki, təhdid agenti var, lakin onların məlumat sızdıran vasitəsi yoxdur, bu zaman riskin qiyməti sıfra bərabərdir. Eyni zamanda, çox sayda boşluq olduğu halda bu boşluğu istismar etməyə cəhd edən maraqlı tərəf olmadıqda, yəni təhdid olmadıqda bu riskin qiyməti yenə də sıfra bərabər olacaq. Lakin bu hal müəssisələrdə çox nadir hallarda baş verir.

Məlum təhdid və boşluqların əsasında riskin qiymətini hesablayaraq, fərdi məlumatların təşkilat daxilindən sızma dərəcəsini müəyyən etmək olar. Bu isə sızmanı törədən əsas səbəbləri aşkarlamağa və onların aradan qaldırılmasına imkan verir.

NƏTİCƏ

Fərdi məlumatların mövcud sızma kanallarının qarşısını almağın ən effektiv yolu, təşkilatın informasiya təhlükəsizliyini idarə edən infrastrukturu mükəmməl qurmaqdır. Bunun üçün ilk növbədə təhdidlərin aşkarlanmasını həyata keçirən təşkilati proseslərin fasiləsiz işləməsi təmin olunmalıdır. Digər tərəfdən, təşkilata yönəlmiş risklərin insayder olma dərəcəsininin müəyyən olunması istiqamətində də bir sıra tədbirlərin görülməsinə böyük ehtiyac var. İnsayderlərin müəyyən olunması fərdin şəxsi keyfiyyətlərini xarakterizə edən mexanizmlər əsasında aparılmalıdır. İnsayderləri adi təhdidlərdən fərqləndirməyə xidmət edən mühüm faktorlardan biri onların mədəniyyət faktorlarıdır. Burada mədəniyyət faktorları dedikdə şəxsin təşkilatda fəaliyyət göstərən digər işçilərlə münasibəti nəzərdə tutulur. Qeyd edək ki, insayder risklərinin effektiv idarə edilməsi üçün tənzimləyici strukturlar və mədəniyyət faktorları mühüm rol oynayır. Müəssisədə ekspert qiymətləndirməsi nəticəsində qəbul olunan qərarlara əsasən müəssisənin təşkilati prosesində dəyişikliklər etmək mümkün olar. Bu isə qurulacaq idarəetmə mexanizmini insayder hücumlarının qarşısını almaqda mühüm vasitəyə çevirə bilər.

ƏDƏBİYYAT

[1] "Privacy Rights Clearinghouse," https://www.privacyrights.org/data-breach/new.

[2] "The WikiLeaks Iraq War Logs: Greatest Data Leak in US Military History," http://www.spiegel.de/international/world/the-wikileaks-iraq-war-logs-greatest-data-leak-in-us-military-history-a-724845.html.

[3] A. Shabtai, Y. Elovici, L. Rokach, "A Survey of Data Leakage Detection and Prevention Solutions," SpringerBriefs in Computer Science, 2012, 92 p.

[4] P. Gordon, "Data Leakage - Threats and Mitigation," SANS Institute InfoSec Reading Room, 2007, 69 p.

[5] "Infowatch Kribrum," Автоматизированная система мониторинга и анализа социальных медиа. http://www.infowatch.ru.

[6] Z. Xiaofei, X. Fang, S. Changxiang, "Research on multilevel security model based on trustworthy state and its application," Acta Electronica Sinica, 2007, pp. 1511-1515.

[7] P.C. Cheng, P. Rohatgi, C. Keser, "Fuzzy multi-level security: An experiment on quantified risk-adaptive access control," IEEE Symposium on Security and Privacy, 2007, pp. 222-230.

[8] J.S. Okolica, G.L. Peterson, R.F. Mills, "Using Author Topic to Detect Insider Threats from Email Trafic," 2006, pp. 642−643.

[9] "Guide to information security. Reasonable steps to protect personal information," Consultation draft, 2012, http://www.oaic.gov.au.

[10] "Rethinking Personal Data: Strengthening Trust," World Economic Forum, 2012, 36 p.

[11] R. Richardson, S. Peters, "CSI Computer Crime and Security Survey," New York: Computer Security Institute, 2011, 42 p.

[12] C.W. Probst, J. Hunker, D. Gollmann, M. Bishop, "Insider Threats in Cyber Security," Advances in Information Security, 2010, Vol. 49, 244 p.

[13] "Glossary," Risk and Insurance Management Society, http://community.rims.org/Glossary/WGAlphabeticalTab/.

[14] "ENISA Threat Landscape," European Network and Information Security Agency, 2012, 96 p.