Loq-faylların analizi əsasında informasiya təhlükəsizliyinin təmin edilməsi

Fərhad Yusifov

AMEA İnformasiya Texnologiyaları İnstitutu

farhadyusifov@gmail.com

***Xülasə*— İnformasiya təhlükəsizliyinin təmin olunmasına dair beynəlxalq təcrübədə mövcud olan normativ-hüquqi bazalar və mexanizmlər tədqiq olunmuşdur. Cəmiyyətin təhlükəsizliyinin mühüm komponenti kimi informasiya təhlükəsizliyinin vəzifələri müəyyənləşdirilmiş, mövcud təhlükələr və onların hədəfləri araşdırılmış, loq-faylların analizi əsasında informasiya təhlükəsizliyinin təmin olunmasına dair metodlar təklif olunmuşdur.**

Açar sözlər— informasiya cəmiyyəti; informasiya təhlükəsizliyi; loq-fayl

I. GİRİŞ

İnformasiya cəmiyyəti (İC) sivilizasiyanın inkişafının bir mərhələsi kimi cəmiyyətdə informasiya və biliyin rolunun artması, daxili məhsulların axınında informasiya kommunikasiyalarının, məhsullarının və xidmətlərinin payının çoxalması, insanların səmərəli informasiya mübadiləsini və onların qlobal informasiya resurslarına çıxışını təmin edən qlobal informasiya fəzasının yaradılması ilə xarakterizə olunur. Hal-hazırda cəmiyyətin müxtəlif sferalarında o cümlədən, iqtisadi, enerji, ekologiya və s. informasiya kommunikasiya texnologiyalarının (İKT-nin) geniş tətbiqi informasiya təhlükəsizliyi məsələsini ön plana çıxarır. Ümumiyyətlə. cəmiyyətin bütün sahələrinin və insanların İKT-dən asılılığı gücləndikcə informasiya təhlükəsizliyinin əhəmiyyəti özünü daha çox büruzə verir. İC-nın qurulmasının əsas vəzifələrindən biri kimi informasiya təhlükəsizliyi dövlətin, cəmiyyətin və şəxsiyyətin təhlükəsizliyinin təmin edilməsinin əsas istiqamətlərindən birinə çevrilir.

İC-nın formalaşdırılması, İnternet şəbəkəsinin sürətli inkişafı və təqdim etdiyi xidmətlərin kifayət qədər populyarlıq qazanması eləcə də, e-dövlət proqramlarının həyata keçirilməsi və vətəndaşlara təqdim olunan xidmətlərin genişləndirilməsi mövcud korporativ informasiya fəzalarında böyük həcmli informasiyanın formalaşmasına səbəb olmuşdur. İnformasiya resurslarının sürətlə artması informasiya təlükəsizliyinin təmin olunması üçün yeni yanaşma metodlarının işlənməsinə və tətbiq olunmasına ehtiyac yaradır. Veb-serverdə toplanan qeydiyyat faylları (log files) Veb-qovşaqdan keçən trafik və istifadəçilərin davranışları haqqında əsas informasiya mənbəyi hesab olunur. Hal-hazırda loq-fayl verilənlərin (məlumatların) analizi, habelə şəbəkə aktivliyinin yoxlanması, resursların və haker proqramlarının izlənməsi, təhdidlərin aşkarlanması üçün metod və hesablama vasitələrinin (alqoritm və proqramlarının) yaradılmasına xüsusi diqqət yetirilir. Loq-faylların müfəssəl analizi informasiya təhlükəsizliyin təmin olunması sahəsində effektli həllərin, metod və mexanizmlərin işlənilməsinə imkan verir.

II. İNFORMASİYA TƏHLÜKƏSİZLİYİ CƏMİYYƏTİN TƏHLÜKƏSİZLİYİNİN MÜHÜM KOMPONENTİ KİMİ

Cəmiyyət informasiyalaşdıqca insanlar informasiyadan daha asılı vəziyyətə düşürlər. Bu informasiyaların təhlükəsizliyinin təmin olunmaması isə cəmiyyət üçün böyük fəsadlar törədə bilər. İstənilən ölkədə informasiya təhlükəsizliyinin prioritetləri dövlətin, cəmiyyətin və vətəndaşların maraqlarının balanslı nisbəti əsasında müəyyənləşir. Ölkədəki siyasi, hərbi, fövqəladə və s. vəziyyətlərdən asılı olaraq bu nisbət dəyişə bilər. Cəmiyyətin təhlükəsizliyinin əsas komponentlərindən biri kimi informasiya təhlükəsizliyinin vəzifələri İnformasiyanın mühafizəsi, İnformasiyanın tamlığı, İnformasiyanın əlyetərliliyi və ziyanlı kontentlərlə mübarizədir.

İnformasiya təhlükəsizliyinin təmin edilməsi sistematik, kompleks yanaşma tələb edir. Bu sahədə əlaqədar qurumlar tərəfindən konseptual, təşkilati, elmi-metodoloji, qanunvericilik, maddi-texniki əsasların yaradılması üzrə işlər aparılmalıdır. Cəmiyyətin informasiya təhlükəsizliyinin təmin olunması üçün zəruri olan tədbirlər kimi beynəlxalq hüquqi mexanizmlərin ciddi araşdırılması, milli normativ-hüquqi bazanın formalaşdırılması, təhlükəsizlik siyasətinin işlənilməsi və reallaşdırılması, xüsusi texnologiyaların tətbiqi, ölkə və korporativ səviyyədə informasiya təhlükəsizliyinin monitorinqi və menecmentinin aparılması, kadr hazırlığı, əhalinin maarifləndirilməsi və vətəndaşlarda informasiya mədəniyyətinin tərkib hissəsi kimi informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması göstərilə bilər [1].

Beynəlxalq təcrübədə qlobal informasiya təhlükəsizliyi təmin olunması məqsədilə bir sıra proqramlar, layihələr, mexanizmlər işlənilmişdir. Onların sırasında 2002-ci ildə BMT tərəfindən qəbul etmiş Qlobal İnformasiya Təhlükəsizliyi Mədəniyyəti haqqında Qətnaməni, 2008-ci ildə Beynəlxalq Telekommunikasiya İttifaqı tərəfindən qəbul olunmuş Qlobal İnformasiya Təhlükəsizliyi proqramını göstərmək olar [2,3]. Bununla yanaşı, 2010-cu ildə Lissabon sammitində qəbul olunmuş Bəyannamənin 40-cı maddəsinə əsasən 2012-ci ildə *Full Operational Capability* (FOC) mərkəzləşdirilmiş qurumu yaradılmışdır [4]. Bu qurum NATO-nun bütün infrastrukturunun informasiya təhlükəsizliyini həyata keçirir.

Ölkəmizdə də, informasiya təhlükəsizliyi məsələləri milli təhlükəsizliyin əsas tərkib hissələrindən biridir və bu sahədə normativ-hüquqi bazanın formalaşması İC quruculuğunda prioritet məsələlərdən hesab olunur. Azərbaycanda informasiya təhlükəsizliyinin təmin edilməsinin qanunvericilik bazasının formalaşdırılması və inkişaf etdirilməsi istiqamətində bir sıra mühüm qanunlar, normativ aktlar və sərəncamlar qəbul edilmişdir [5-11].

Məlumdur ki, qlobal İC-də informasiya iqtisadiyyatın, elmin, təhsilin, siyasi və ictimai fəaliyyətin digər sahələrinin

aparıcı amilinə çevrilir. Bu baxımdan İC çox mürəkkəb formada qarşılıqlı münasibətdə olan korporativ və açıq informasiya fəzalarının toplusundan ibarətdir. Ümumilikdə İC 5 formalaşma səviyyəsindən ibarətdir: Kommunikasiyalaşma, Kompüterləşmə, Şəbəkələşmə, İnformasiyalaşma və Virtuallaşma. Cəmiyyətin informasiya təhlükəsizliyinə olan təhlükələrin hədəfləri də məhz bu səviyyələrdir. İnformasiya təhlükəsizliyinə olan təhlükələrin meydana çıxmasının əsas səbəblərindən biri kimi isə beynəlxalq səviyyədə İnternetin fəaliyyətini tənzimləyən mexanizmlərin olmamasını göstərmək olar [1,12]. İnternetin sürətli inkişafı və kütləvi halda istifadəçilərin meydana çıxması ilə kompüter və kommunikasiya sistemlərinə olan təhdidlər daha ehtimallı olur və onların realizəsinin nəticələri daha da geniş miqyas alır. Müxtəlif səviyyələrdə təhlükələrin olmasına baxmayaraq istənilən halda təhlükələrin mənbəyi insandır [1,12]. Hər bir insanın daxili dünyası, yaşadığı mühit, psixoloji durumundan asılı olaraq cəmiyyət qarşısında məsuliyyətini itirməsi başqalarının hüququnun pozulması ilə nəticələnir. Statistik hesabatlara görə, sistemin öz istifadəçilərinin hərəkətləri nəticəsində vurulan ziyanın həcmi artıq virusların vurduğu ziyanı üstələyir. Təhlükəsizlik üzrə bir çox zəif yerlər istifadəçilərin, sistem administratorlarının və digər mütəxəssislərin informasiya təhlükəsizliyi sahəsində biliklərinin kifayət səviyyədə olmaması nəticəsində mövcuddur. Təbiidir ki, bu insanların təfəkküründən asılıdır və zamana bağlı olaraq yeni mədəniyyətin formalaşmasını zəruri edir.

Mühüm məsələlərdən biri də vətəndaşların şəxsi və ailə həyatı ilə bağlı toplanan, emal olunan və ötürülən məlumatların mühafizə olunması ilə bağlıdır. Qeyd etmək lazımdır ki, bir sıra ölkələrdə İnsan Haqqları haqqında Bəyənnamənin 19-cu və 21-ci maddələrinin həyata keçirilmə vəziyyətinin monitorinqi məqsədi ilə informasiya ombudsmanı, informasiya tribunalı, informasiya telekommunikasiya ombudsmanı institutları fəaliyyət göstərir [13]. Başqa sözlə, İnformasiya ombudsmanları bir tərəfdən informasiya azadlığının (19-cu maddə), digər tərəfdən isə fərdi məlumatların mühafizə vəziyyətinin (21-ci maddə) monitorinqini həyata keçirir. İC quruculuğu prosesində ölkədə formalaşan fərdi məlumatlar infrastrukturu ən önəmli seqmentlərindən birini təşkil edir. Bu sahədə dünyada olan mövcud təcrübə nəzərə alınaraq ölkəmiz Avropa Şurasının 1981-ci il tarixli "Fərdi məlumatların avtomatlaşdırılmış sistemlərdə emalı vaxtı fiziki şəxslərin qorunması haqqında" Konvensiyasına (108 saylı Konvensiya) qoşulmuşdur [14].

Cəmiyyətin informasiya təhlükəsizliyinin təmin olunmasında internet provayderlərində rolu böyükdür və onların üzərinə mühüm vəzifələr qoyulur. Bu gün ölkədə İnternet xidmətləri təxminən 40 provayder tərəfindən göstərilir. Cəmiyyətin informasiya təhlükəsizliyi, əsasən bu provayderlərdən və onların administratorlarından asılıdır. Ona görə də, İnternet provayderlərin və administratorların cəmiyyət qarşısında məsuliyyəti hüquqi mexanizmlərlə təsbit olunmalıdır. Əgər beynəlxalq təcrübəyə əsaslansaq, İCDS-in (*WSIS - World Summit on the Information Society*) Bəyannaməsində, Beynəlxalq qurumların, Avropa Birliyinin və inkişaf etmiş ölkələrin qəbul etdiyi hüquqi sənədlərdə spamlarla, viruslarla, ziyanlı kontentlərin yayılmasına qarşı mübarizə məqsədi ilə şəbəkə operatorları və İnternet-provayderlərin qarşısında mühüm vəzifələr qoyulur. Spamlarla, viruslarla, ziyanlı kontentlərlə mübarizə şəbəkə operatoru və provayderlər səviyyəsində aparılarsa, çox az vəsait hesabına kompüterləri viruslardan mühafizə etmək olar. Bununla yanaşı, beynəlxalq təcrübəyə əsaslanaraq şəbəkə operatorların və provayderlərin maliyyələşdirməsi mexanizmləri işlənilməsinə də xüsusi diqqət yetirilməlidir.

Qeyd etmək lazımdır ki, İnternet xidmətləri göstərən provayderlərin xidmət keyfiyyəti göstəricilərinin yaxşılaşdırılması, onların funksional imkanlarının artırılması və informasiya resurslarının axtarışının səmərəliliyinin yüksəldilməsi, eləcə də, fərdi məlumatların mühafizəsi və informasiya təhlükəsizlyinin təmin olunması istiqamətində metodların, mexanizmlərin işlənməsi olduqca vacib və zəruri məsələlərdir.

Hal-hazırda informasiya resurslarından və texnologiyalarından cinayət və terror məqsədləri ilə istifadə etməyin qarşısının alınması, insan hüquqlarının qorunması, fərdi məlumatların toxunulmazlığı və söz azadlığı haqqında müddəalara əməl olunması böyük əhəmiyyət kəsb edir. İnsan haqlarının qorunması ilə yanaşı, internetdə terrorizmin bütün formaları və təzahürlərinə qarşı mübarizə aparılmalı, rəqəmsal bərabərsizliyin aradan qaldırılması üçün ciddi tədbirlər görülməlidir. Eləcə də, uşaqların, gənclərin inkişafında, fiziki qüsurlu insanların, gender probleminin həllində İKT-nin rolunun artırılması cəmiyyətin inkişafında informasiya təhlükəsizliyinin təmin olunmasını mühüm məsələ kimi ön plana çıxarır. Bütün bunlar nəzərə alınaraq, Azərbaycanın hüquqi sistemi də beynəlxalq səviyyədə virtual məkana dair qəbul olunmuş sənədlərin tələblərinə uyğunlaşdırılmışdır.

III. LOQ-FAYLLARIN ANALİZİ

Veb-serverdə toplanan loq-fayllar serverin işi haqqında sistem informasiyasını və istifadəçilərin davranışları haqqında informasiyanı özündə birləşdirir: istifadəçilərin müraciət tarixi və vaxtı, istifadəçinin kompüterinin IP-ünvanı, istifadəçinin brauzerinin adı, müraciət olunan səhifənin URL ünvanı və istifadəçi istinadları və s. Loq-fayllar analiz olunmaqla saytların və onlara müraciət edən istifadəçilərin identifikasiyası, boşluqların tapılması, təhlükələrin, təhdidlərin aşkarlanması, ziyanlı proqramların təsbit olunması və eləcə də, müxtəlif meyarlara görə qiymətləndirmə mexanizmlərindən istifadə oluna bilər.

Potensial təhlükələr müxtəlif kriteriyalar əsasında təsnif oluna bilər. Təsir məqsədlərinə görə təhlükələr aşağıdakı kimi təsnif oluna bilər:

- İnformasiyanın konfidensiallığının pozulmasına yönələn təhlükələr;
- İnformasiyanın tamlığının pozulmasına yönələn təhlükələr;
- Əlyetənliyin pozulmasına yönələn təhlükələr (DoS hücumlar).

Serverlərə istifadəçilərin müraciət xarakteristikalarının avtomatik öyrənilməsi prosesi əsasən populyar olan assosiativ qaydaların axtarılmasını, naviqasiya yollarını, klasterləşdirmə, klassifikasiya və s. ehtiva edir. Bu məsələlərin həll edilməsi üçün Veb-serverin loq-fayllarında saxlanılan məlumatlardan istifadə etmək olar. Müxtəlif təşkilatlar serverlər vasitəsilə

avtomatik yaradılan və jurnallarda qeyd olunan böyük həcmə malik olan məlumatları toplayırlar. Hər bir səhifəyə müraciəti (link) olan istinad jurnalları, brauzer jurnalları, istifadəçiləri qeydəalma və anket məlumatları da (onlarda CGI ssenarilər vasitəsilə toplanır) informasiya mənbələri hesab olunur.

Yaranışının lap əvvəlindən *WWW* layihələri qeyd olunan server trafikinin verilənlərinin təsviri üçün ənənəvi formata üstünlük verirlər. Qeydiyyat üçün dörd əsas fayldan istifadə olunur: access log (müraciətlərin qeydiyyatı jurnalı), error log (səhvlərin qeydiyyatı jurnalı), referrer log (istinadlar jurnalı) və agent log (agentlər jurnalı). Bu jurnalların kombinasiyaları dəyişə bilər, amma məhz onlar trafikin analizi üçün yeganə informasiya mənbəyi hesab olunurlar. Bu jurnallar arasında ən önəmlisi müraciətlərin qeydiyyat jurnalıdır. Belə ki, bu jurnalda hər bir müraciətin HTTP-sorğuları saxlanılır, habelə qrafik təsvirə, CGI proqrama, audioklipə və ya digər obyektlərə müraciətin uğurlu olub olmamasından asılı olmayaraq bu jurnalda saxlanılır. Lakin HTTP-sorğu və Veb-səhifəyə sorğu eyni bir şey deyildir. Deməк olar ki, bilavasitə Veb-səhifənin özü bir neçə qrafik təsvirə malik ola bilər. Bu halda istifadəçi belə bir səhifəyə baxanda Veb-server yalnız həmin səhifənin HTTP-sorğusunun deyil, həm də təsvirlərin HTTP sorğularına xidmət edir. Beləliklə, səhifəyə müraciət zamanı müraciət jurnalında bir yox, qrafik təsvirlərin sayı qədər qeydiyyat yazısı əlavə olunacaq.

Səhvlərin qeydiyyat jurnalı daşıdığı informasiyanın mühüm olmasına görə ikinci jurnal hesab olunur. Lakin, birincidən heç də az önəmli olmayan jurnaldır. Statistika baxımından olmasa da o, administratorlar üçün xüsusi əhəmiyyət kəsb edir. Bu jurnala məlumat o zaman daxil edilir ki, Veb-server səhv və ya qəza vəziyyəti qeydə alır, Məsələn, mövcud olmayan səhifəyə müraciət qeydiyyat jurnalında qeyd olunur. Lakin bəzi hallar yalnız səhvlər jurnalında qeyd olunur. Məsələn, əgər səhifənin başqa yerə yönəldilməsi zamanı oxucu ona baxmaqdan imtina edirsə, onda səhvlər jurnalında "send lost connection" yazısı yazılır, fəqət müraciət jurnalında serverlərin çoxu üçün, bu yazı qeydə alınmayacaqdır. İstinadlar və agentlər jurnalında ziyarətçilər haqqında əlavə məlumat qeydə alınır: istifadəçinin yönəldildiyi qovşaqda səhifənin URL göstəricisi, habelə onun brauzerinin tipi və s.

Qeyd edək ki, İnternetdən istifadə haqqında biliklərin aşkarlanması üsulları son illərdə daha çox populyarlaşmağa başlamışdır. Bu sahədə yaxşı göstərici olaraq elmi-tədqiqat işlərinin sayının artmasını göstərmək olar. Deməк olar ki, hal-hazırda Veb məkanının dəqiq analizini aparmağa imkan verən, yaxşı işlək sistemlər praktiki olaraq yoxdur və mövcud sistemlər isə az effektivdir. Həmçinin, Veb-istifadəçilərinin sayının kəskin artmasını nəzərə alsaq bazarın müvafiq proqram sistemlərinə tələbatı çox böyükdür. Tələbatı ödəmək və bu sahədə vacib problemləri həll etmək üçün intellektual analiz metodları bir sıra məsələləri həll etməyə kömək edə bilər. Belə məsələlərə istifadəçinin identifikasiyasını, seansa girişin identifikasiyasını, konfidensiallığın saxlanmasını, tranzaksiyaların identifikasiyasını və s. nümunə göstərmək olar.

Son 15 ildə süni intellekt texnologiyasını *WWW* tətbiqi Veb texnologiyalarının daha da intellektuallaşmasına [15] və *Web mining* [16-18] termini adı altında yeni istiqamətin formalaşmasına (yaranmasına) səbəb olmuşdur.

Qeyd edək ki, Web mining metodları tətbiq olunmaqla şəbəkədə lazımi informasiyanın axtarışı və əldə olunmuş resursların emalı üçün çox güclu instrumental vasitələr yaradıla bilər. Bu nöqteyi nəzərdən də, müxtəlif təyinatlı intellektual sistemlərin yaradılması məqsədəuyğun hesab olunur. Məsələn, loq-faylların analizi veb-istifadəçilər haqqında verilənlərin analizi istifadəçinin profilinin öyrənilməsi və onların daha çox hansı resurslara maraq göstərdiklərini təhlil etməyə imkan verir.

Hal-hazırda aparılan elmi-tədqiqat işlərinin əksəriyyəti şablonların müfəssəl təhlilindən çox şablonların aşkarlanmasına yönəlmişdir. Bu isə şəbəkə təchizatlarından asıllıq və intellektual paradiqmaların [1,19,20] tətbiqinə əsaslanır.

Müxtəlif istifadəçilərin identifikasiyası üçün dörd tip münaqişə vəziyyətinə baxılır [19, 21,22].

- Bir IP-ünvan/çox istifadəçi. Bu vəziyyət provayderin proksi-serverindən istifadə edildiyi zaman baş verir və bundan başqa provayder ilə əlaqə yaradılan vaxt istifadəçiyə təsadüfi ünvan ayrılanda (telefon xətti ilə əlaqəyə xas olan bir haldır) iki müxtəlif istifadəçi eyni ünvan ala bilər.
- Çox IP-ünvan/bir istifadəçi. Bu da çox geniş yayılmış haldır və provayder tərəfindən ünvanların dinamik ayrılması zamanı baş verir. Bu halda istifadəçilərin IP-ünvanları hər bir qoşulma zamanı dəyişir.
- Çox IP-ünvan/bir seans. Bəzi hallarda (çox məşhur misal kimi AOL göstərə bilərik) istifadəçinin səhifəyə hər bir müraciəti zamanı ona yeni ünvan verilir. Bu vəziyyətdə hər iki tərəf üçün müxtəlif istifadəçilər təyin edilə bilər və bir seans üçün istifadəçinin yolunu izləmək olar ki, nəticədə hər bir sənəd üçün ona müraciət edən istifadəçini tapmaq olar. Beləliklə, seansların hər birini ayırmaq olar ki, bu da sayta girişdən o səhifəyə qədər olacaqdır ki, bu səhifədən sayt daxilində keçid icra edilməmiş olsun.
- İstifadəçi müxtəlif brauzerlərdən istifadə edir. Bu halda əgər IP-ünvan etibarlı məlumat vermirsə, onda aşağıda təsvir olunan iki metoddan istifadə etmək olar. Amma nəzərə almaq lazımdır ki, *cookie* faylları heç də həmişə korrekt işləməyəcək.

Əgər yuxarıda qeyd olunan halların heç birində identifikasiya üçün jurnalın məlumatları kifayət etmirsə, onda cookie fayllarından və istifadəçilərin unikal qeydə alınmasından istifadə etmək olar. Bu metodların hər birinin çatışmayan cəhətləri var: istifadəçi öz kompüterində olan faylları pozursa, onda məcburi qeydəalma aşkar nöqsanlardan əlavə dəqiq məlumatları almaya da bilər. Digər bir məsələ – seansın identifikasiyasıdır (session identification). Hər hansı bir istifadə halının analizi icra edilməmişdən əvvəl müxtəlif seansları və ya tranzaksiyaları təsvir edən verilənləri məntiqi hissələrə bölmək lazımdır. İstifadəçinin seansı dedikdə saytı bir dəfə müraciət edən zaman, onun istifadə etdiyi bütün səhifə istinadlarının tam dəsti nəzərdə tutulur. Seansların təyin edilməsi ayrı-ayrı istifadəçilərin təyin edilməsi ilə oxşardır. Bu problemin həllinin ən populyar üsulu zamana görə istifadə olunan seansların fərqləndirilməsidir və bu halda bir ünvandan icra edilən iki ardıcıl müraciət eyni bir seansa aid edilir, bir şərtlə ki, əgər müraciətlər arasındakı fasilə verilmiş zaman həddini aşmasın.

İkinci geniş yayılmış üsul "per session cookies"-in dəstəklənməsidir (istifadəçi tərəfindən yalnız o məlumatlar saxlanılır ki, onlar səhifəyə birinci müraciətdən brauzerin söndürülməsinə qədər olan məlumatlardan ibarətdir və bu məlumatların analizi istifadəçinin bir müraciətini digərindən fərqləndirməyə imkan verir).

Sayta müraciətlərin analizi trafikin əsas mənbələri haqqında informasiyanın yığılması, istifadəçinin coğrafiyasının təyini və maraq dairələrinə əsasən kontentlərin aşkarlanmasına imkan verir. Eləcə də, sayta müraciət edənlərin maraq dairəsinə əsasən saytın güclü və zəif tərəflərinin müəyyən edilməsinə və saytın kontentinin, strukturunun yaxşılaşdırılmasına, təhlükəsizlik tədbirlərinin gücləndirilməsinə dair əhəmiyyətli informasiya verir. İstifadəçilərin identifikasiyasının üç əsas üsulu vardır [19-22].

Qeyd etmək lazımdır ki, dövlətin informasiya təhlükəsizliyi strategiyasının formalaşdırılması üçün beynəlxalq təcrübədə mövcud olan mexanizmlər tədqiq olunmalı, milli normativ-hüquqi baza təkmilləşdirilməli və inteqrasiya məsələləri həll olunmalıdır. Cəmiyyətin təhlükəsizliyinin mühüm komponenti kimi informasiya təhlükəsizliyinin vəzifələri dəqiq müəyyənləşdirilməli, loq-faylların intellektual analizinə imkan verən analizatorlar, sistemlər yaradılmalı və mövcud təhlükələr, onların hədəfləri təfərrüatlı analiz olunmalıdır.

NƏTİCƏ

Ölkəmizdə İC inkişaf etdikcə elektron dövlətin yaradılması prosesində vahid və çoxsəviyyəli ümumdövlət informasiya təhlükəsizliyi sisteminin yaradılması zərurəti meydana çıxır. Bu baxımdan, loq-faylların analizi informasiya təlhükəsizliyi sisteminin əsas komponentlərindən biridir və bu sahədə qabaqcıl təcrübənin öyrənilməsi, intellektual metodların işlənilməsinə böyük ehtiyac vardır.

Ümumiyyətlə, İC-nin formalaşdırılması ölkələrin informasiya təhlükəsizliyini təmin etmək, immunitetini artırmaq, müxtəlif təbiətli və miqyaslı təhlükələrlə təkbaşına mübarizə aparmağı xeyli çətinləşdirir və ona görə də qlobal informasiya təhlükəsizliyi mühitini formalaşdırmaq bütün ölkələrin, vətəndaş cəmiyyətinin, şirkətlərin və insanların marağında olmalıdır. Beynəlxalq təcrübəyə əsaslanaraq ölkə üzrə informasiya təhlükəsizliyinin vəziyyətinin monitorinqinin (statistikasının) aparılması üçün indikatorlar işlənilməli, veb-serverlərdə toplanılan loq-fayllar analiz olunmalı və səmərəli qərarların qəbul edilməsi üçün mexanizmlər işlənilməlidir.

ƏDƏBİYYAT

[1] В. Петров, С. Петров, Информационная безопасность человека и общества: учебное пособие, 2007, 334 с.

[2] Создание глобальной культуры кибербезопасности, 2002, http://www.un.org/ru/development/ict/res.shtml

[3] Global Cybersecurity Agenda, 2008, http://www.itu.int/osg/csd/-cybersecurity/gca/global_strategic_report/global_strategic_report.pdf

[4] Lisbon Summit Declaration, 20 November 2010, http://www.nato.int/nato_static/assets/pdf/

[5] «İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında» Azərbaycan Respublikasının Qanunu, http://e-qanun.gov.az

[6] «Dövlət sirri haqqında» Azərbaycan Respublikasının Qanunu, http://www.mia.gov.az

[7] «Elektron sənəd və elektron imza haqqında» Azərbaycan Respublikasının Qanunu, http://e-qanun.az

[8] «Elektron ticarət haqqında» Azərbaycan Respublikasının Qanunu, http://e-qanun.az

[9] «İnformasiya əldə etmək haqqında» Azərbaycan Respublikasının Qanunu, http://e-qanun.az

[10] «Telekommunikasiya haqqında» Azərbaycan Respublikasının Qanunu, http://e-qanun.az

[11] "AR-nın Milli təhlükəsizlik konsepsiyası", www.mns.gov.az

[12] В. Шерстюк, Проблемы информационной безопасности в современном мире, www.ict.edu.ru/ft/002471/sherstjuk.pdf

[13] İnsan Haqqları haqqında Bəyənnaməsi (The Universal Declaration of Human Rights) http://www.un.org/en/documents/udhr/index.shtml

[14] "Fərdi məlumatların avtomatlaşdırılmış sistemlərdə emalı vaxtı fiziki şəxslərin qorunması haqqında" Konvensiyası (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), http://conventions.coe.int/Treaty/en/-Treaties/Html/108.htm

[15] A. Abraham, Business Intelligence from Web Usage Mining, Journal of Information & Knowledge Management, 2003, vol. 2, p. 375-390

[16] M. Spiliopoulou, C. Pohle, M. Teltzrow, Modelling and Mining Web Site Usage Strategies, Proc. of the Multi-Konferenz Wirtschaftsinformatik, Nurnberg, Germany, Sept. 9-11, 2002, p. 203-221

[17] J. Srivastava, R. Cooley, M. Deshpande, P. Tan, Web Usage Mining: Discovery and Applications of Usage Patterns from Web Data , SIGKDD Explorations, 2000, vol. 1(2), p. 12–23

[18] J. Srivastava, P. Desikan, V. Kumar, Web Mining-Accomplishments and Future Directions, Proc. of the NSF Workshop on Next Generation Data Mining (NGDM), Baltimore, MD, November 2002, p. 51-61

[19] R. Əliquliyev, F. Yusifov, Web-serverlərdə toplanan statistik verilənləri analiz etməklə istifadəçi profilinin yaradılması, AMEA-nın Xəbərləri, Fizika-riyaziyyat və texnika elmləri seriyası. 2007, №2-3, s. 144-148

[20] R. Iváncsy, I. Vajk, Different Aspects of Web Log Mining, Proc. of the 6th International Symposium of Hungarian Researchers on Computational Intelligence. Budapest, November, 2005, p. 413-424

[21] X. Wanga, A. Abraham, K. A. Smitha, Intelligent web traffic mining and analysis, Journal of Network and Computer Applications, 2005, vol. 28, p. 147–165

[22] Ф. Юсифов, Извлечение знаний из Интернет с использованием лог-файлов, Телекоммуникации, 2006, №8, с. 13-18