RƏQƏMSAL KİTABXANALARDA İNFORMASİYANIN QORUNMASI PROBLEMLƏRİ

HƏSƏNOVA N.Ə.
BDU, İnformatika və Kitabxanaşünaslıq kafedralarının baş müəllimi, Texnika üzrə fəlsəfə doktoru
n_gasanova@hotmail.com

MƏHƏRRƏMOV İ.Ə.
BDU, Kitabxanaşünaslıq kafedrasının magistrantı
intiqam92_bsu@mail.ru

Məqalədə informasiya təhlükəsizliyi məsələsinə baxılmışdır. Müasir rəqəmsal kitabxanalarda informasiyanın qorunması problemləri araşdırılmışdır, kitabxana-informasiya təhlükəsizlik sisteminin modeli verilmişdir.

Açar sözlər. *İnformasiyanın mühafizəsi, informasiya təhlükəsizlik sistemi, kitabxana informasiya təhlükəsizlik sisteminin modeli.*

Müasir cəmiyyətin texnoloji inkişafı sahəsində təyinedici rolun məhz informasiya texnologiyalarına aid olduğu danılmazdır. Cəmiyyət həyatının İKT-nin müasir tələbləri çərçivəsində inkişafı, dövlət idarəçiliyinin daha da təkmilləşdirilməsi və şəffaflığının artırılması, yeni-yeni milli informasiya ehtiyatlarının yaradılması və təhlükəsizliyinin təmin edilməsi, müasir elmi biliklərə əsaslanan iqtisadiyyatın inkişafı, bütün sahələrdə yeni texnologiyaların geniş tətbiqinə nail olunması, informasiya təhlükəsizliyi və azadlığının müdafiəsi, qlobal informasiya fəzasında inteqrasiyanın genişləndirilməsi ölkədə informasiya cəmiyyətinə keçidi təmin edəcək fəaliyyətin tərkib hissələridir. Azərbaycan Respublikasında informasiya təhlükəsizliyi sahəsindəki əsas vəzifələrin yerinə yetirilməsi, milli informasiya resurslarının qorunması və təhdidlərin qarşısının alınması, bu sahədə effektli tədbirlərin gücləndirilməsi məqsədilə son zamanlar dövlət səviyyəsində ciddi fəaliyyətə başlanmışdır. Bu tədbirlər sırasında Azərbaycan Respublikası Prezidentinin Rabitə və İnformasiya Texnologiyaları Nazirliyi yanında Elektron Təhlükəsizlik Mərkəzinin yaradılması haqqında 26 sentyabr 2012-ci il tarixli və "İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında 5 mart 2013-cü il tarixli fərmanlarını qeyd etmək olar. Qeyd etmək lazımdır ki, informasiya təhlükəsizliyinə xarici və daxili təhdidlər, onların qarşısının alınması metodları və s. kimi məsələlər milli təhlükəsizliyin bütün sahələri üçün əsasən ümumi xarakter daşıyır. Lakin

bu sahələrin hər biri özünəməxsus xüsusiyyətlərə malik olduğundan onların təhlükəsizliyinin təmin olunması metodları bir-birindən fərqlənir.

Aparıcı şəbəkə təhlükəsizliyi vasitələri və istehsalçı müəssisələrin təcrübəsi göstərir ki, şirkət paylanmış korporativ informasiya sistemlərinin təhlükəsizlik siyasətini əlverişli şəkildə həyata keçirə bilər. Bunun üçün təhlükəsizliyin idarə olunması mərkəzləşdirilmiş olmalı, istifadə edilən əməliyyat sistemlərindən və tətbiqi sistemlərdən asılı olmamalıdır. Kompüter sistemlərində və şəbəkələrində informasiya təhlükəsizliyinin əsaslarını və yaxud təhlükəsizliyin pozulmasının bütün mümkün hallarını, əsasən, üç kateqoriyaya ayırmaq olar:

- informasiyanın məxfiliyinin pozulması təhlükəsi;
- informasiyanın tamlığının pozulması təhlükəsi;
- sistemin iş qabiliyyətinin pozulması (xidmətin göstərilməsindən imtina) təhlükəsi.

Məxfiliyin pozulması təhlükələri məxfi informasiyanın və ya sirlərin açılmasına yönəlmiş olur. Bu növ təhlükələr reallaşdıqda informasiya ona giriş hüququ olmayan şəxslərin əlinə keçə və ya onlara bəlli ola bilər. Kompüter sistemlərində və şəbəkələrində saxlanılan və ya ötürülən məxfi informasiyaya hər dəfə icazəsiz giriş əldə edildikdə və ya buna cəhd göstərildikdə onun gizliliyinin pozulması təhlükəsi yaranır. Kompüter sistemlərində və şəbəkələrində saxlanılan və ya ötürülən informasiyanın tamlığının pozulması təhlükələri onun təhrif olunmasına, keyfiyyətin pozulmasına və ya tam məhvinə gətirib çıxaran dəyişikliklərin edilməsi ilə xarakterizə olunur. İnformasiyanın tamlığı ziyankar şəxslərin düşünülmüş fəaliyyəti, eləcə də ətraf mühitin obyektiv təsiri nəticəsində pozula bilər. Sistemin iş qabiliyyətinin pozulması (xidmətin göstərilməsindən imtina edilməsi) təhlükəsi müəyyən düşünülmüş hərəkətləri, eləcə də təsadüfi hadisə və proseslər nəticəsində kompüter sistemlərinin və şəbəkələrinin fəaliyyətinin pozulmasına, iş qabiliyyətinin zəifləməsinə, informasiya resurslarına icazəli və ya qanuni girişin məhdudlaşdırılmasına, tamamilə bağlanmasına gətirib çıxaran vəziyyətlərin reallaşdırılmasına yönəlmiş olur.

Təhlükə dedikdə sistemə dağılma, verilənlərin üstünün açılması və ya dəyişdirilməsi, xidmətdən imtina formasında ziyan vurulmasına səbəb ola bilən istənilən hal, şərait, proses və hadisələr nəzərdə tutulur. Təhlükələri müxtəlif siniflərə ayırmaq olar. Meydana çıxma səbəblərinə görə təhlükələri təbii və süni xarakterli təhlükələrə ayırırlar. Süni xarakterli təhlükələr də öz növbəsində bilməyərəkdən və qəsdən törədilən təhlükələrə bölünür. Təsir məqsədlərinə görə təhlükələrin üç əsas növü ayırd edilir:

- İnformasiyanın konfidensiallığının pozulmasına yönələn təhlükələr;
- İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr;

- Əlyetənliyin pozulmasına yönələn təhlükələr (DoS hücumlar, Denial of Service - xidmətdən imtina).

Konfidensiallıq informasiyanın subyektiv müəyyən olunan xassəsidir. Verilən informasiyaya müraciət icazəsi olan subyektlərin siyahısına məhdudiyyət qoyulmasının zəruriliyini göstərir. Konfidensiallığın pozulmasına yönələn təhlükələr məxfi və ya gizli informasiyanın üstünün açılmasına yönəlib. Belə təhlükələrin reallaşması halında informasiya ona müraciət icazəsi olmayan şəxslərə məlum olur.

Bütövlük - informasiyanın təhrifsiz şəkildə mövcudolma xassəsidir. İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr onun dəyişdirilməsinə və ya təhrifinə yönəlib ki, bunlar da onun keyfiyyətinin pozulmasına və tam məhvinə səbəb ola bilər. İnformasiyanın bütövlüyü bədniyyətli tərəfindən qəsdən və ya sistemi əhatə edən mühit tərəfindən obyektiv təsirlər nəticəsində pozula bilər.

Əlyetənlik – yolverilən vaxt ərzində tələb olunan informasiya xidmətini almaq imkanıdır. Həmçinin əlyetənlik – daxil olan sorğulara xidmət üçün onlara müraciət zəruri olduqda uyğun xidmətlərin həmişə hazır olmasıdır. Əlyetənliyin pozulmasına yönələn təhlükələr elə şəraitin yaradılmasına yönəlib ki, bu zaman müəyyən qəsdli hərəkətlər ya sistemin iş qabiliyyətini aşağı salır, ya da sistemin müəyyən resurslarına girişi bağlayır.

İnformasiya təhlükəsizliyi yalnız kommersiya şirkətlərini deyil, böyük şirkətlərlə müqayisədə aşağı səviyyədə olan ictimai təşkilatları və qeyri-kommersiya təşkilatlarını da maraqlandırır [1]. İnternetin təmin etdiyi vasitələrlə birlikdə kitabxanaların uzaqdan əlçatan hala gəlməsi, istifadəçilər baxımından bir çox üstünlüklər təmin etməklə birlikdə, məlumat sistemlərinin informasiya hücumlarına məruz qalmasına da imkan vermişdir. Thompson qeyd edir ki, bəzi qrup istifadəçilər kitabxananın verilənlər bazalarına asanlıqla müraciət edib, digər istifadəçilərin şəxsiyyət, ünvan, e-poçt və telefon məlumatlarına çata bilərlər [4]. Zimerman kitabxanalarda olan kompüterlərin fiziki ziyana məruz qala bilmələri ilə bərabər, pis niyyətli istifadəçilərin hücumlarına qarşı da son dərəcə zəif olduqlarına diqqət çəkir [5]. Həmçinin kitabxanalarda çalışan əməkdaşların informasiya təhlükəsizliyi haqqında kifayət qədər məlumatlı olmadıqları da vurğulana bilər [4].

Kitabxanalar baxımından informasiya təhlükəsizliyinə kifayət qədər önəm verilmədiyinə diqqət çəkən Newby məlumat təhlükəsizliyinin yalnız kompüter təhlükəsizliyini təmin etməklə məhdudlanmadığını irəli sürərək təhlükəsizliyin təmin edilməsində təsirli ola biləcək tədbirləri belə sıralayır:

- Kitabxanaçılar arasında informasiya təhlükəsizliyinin təmin edilməsi istiqamətində bir iş bölümünün təyin edilməsi;

- İnformasiya təhlükəsizliyi problemləri və həlli ilə bağlı üsullar haqqında bütün kitabxana işçilərinin öyrədilməsi;
- Məlumatın məxfiliyinin, materialların və kompüterlərin təhlükəsizliyinin təmin edilməsi haqqında müəyyən qaydalar ehtiva edən bir siyasətin inkişaf etdirilməsi;
- Fiziki təhlükəsizlik planlarının hazırlanması;
- Məlumatın bütövlüyünün təmin edilməsi;
- Məlumatın əldə edilməsi yollarına nəzarət edilməsi [3].

Fakeh, Zulhemay, Shabibi, Ali və Zain kitabxanalarda informasiya təhlükəsizliyinin təmin edilməsi məsələsinin, təsirli ola biləcək informasiya təhlükəsizliyi siyasətinin yürüdülməsi (məlumatın təhlükəsiz istifadəsi haqqında təqib edilməsi lazım olan qaydalar və qanunlar), infomasiya təhlükəsizliyi üzrə təhsilin alınması (seminar, konfrans, müzakirə platformaları və müxtəlif kurslar vasitəsilə), texnologiyanın mühafizəsinin təmin edilməsi (kompüterlər və internet vasitələrinin etibarlı və doğru istifadəsi) və əməkdaş faktorlarının vahid bir şəkildə təmin edilməsi ilə mümkün ola biləcəyini vurğulayırlar [9].

Kitabxanalarda tətbiq edilə biləcək İSS (İnformation Systems Security) - informasiya təhlükəsizliyi sisteminin (İTS) modelinin yaradılması vacib məsələlərdəndir. Hagen, Albrechtsen və Hovden-nin təklif etdiyi (2008) modelə görə kitabxanada yaradılacaq informasiya təhlükəsizliyi sistemi pilləvari struktura malik olmalı, pillələr arasında qarşılıqlı asılılıq mövcud olmalıdır. Belə bir sistemin qurulması zamanı iki əsas komponent olan texnoloji və təşkilati tədbirlər nəzərə alınmalıdır. Bu komponentlərin birləşdirilməsi nəticəsində Von Solm tərəfindən informasiya təhlükəsizliyi sisteminin elə bir bazası təklif edilmişdir ki, o təşkilati, hüquqi, müəssisə aspektlərini və təhkükəsizlik texnologiyaları sahəsində uğurlu nəticələrə malik proqram əlavələrini özündə birləşdirir [1]. Təşkilati komponentlər dörd amildən ibarətdir:

- informasiya təhlükəsizliyi siyasətinin mövcudluğu;
- prosedurların təyin edilməsi və nəzarət;
- adekvat inzibati xidmətlərin hazırlanması;
- üsulların yaradılması haqqında məlumatın olması.

Pilləli strukturun addımları məntiqi ardıcıllığı təmin edərək informasiya təhlükəsizliyi sisteminin uğurlu təcrübəsində həyata keçirilən üç ilkin məqsədi müəyyənləşdirir: məxfilik, tamlıq və əlçatanlıq [8]. Bu üç məqsəd İTS üçün əsas olub sistemi müxtəlif təhlükələrdən qoruyur. Kitabxana - informasiya sisteminin təhlükəsizlik modelinin addımlarına nəzər yetirək.

Addım 1: Texnoloji mexanizmlər

Texniki təhlükəsizlik mexanizmləri kitabxanalardakı informasiya

resurslarının bütövlüyünü, məxfiliyini və əlçatanlığını qorumaq üçün istifadə olunur. Bu cür mexanizmlərə aşağıdakılar daxildir:

1. Kitabxana sistemlərinin qorunması;
2. Kitabxana sistemlərinin idarə edilməsi;
3. Kitabxana sistemlərindən informasiyanın çıxışına nəzarət edilməsi;
4. Kitabxana sistemlərinə icazəsiz daxil olmanın qarşısının alınması.

Ehtimal olunur ki, bu texnoloji təməl həmişə hər hansı İTS mühitində yerləşir və kitabxana sistemlərinin əsas müdafiə sistemi kimi qəbul edilməlidir. Bundan başqa, texnoloji təhlükəsizlik mexanizmləri ənənəvi İTS təhlükəsizlik texnologiyalarının əsası kimi vurğulanmışdır [6].

Texnoloji təhlükəsizliyin təməli aparat təminatının, proqram təminatının, şəbəkələrin, serverin, işçi stansiyaların, məlumat və onun fiziki obyektlərinin və kitabxana mühitinin təhlükəsizliyinə istinad edir. Texnoloji mexanizmlər aşağıdakı məsələlərdən ibarətdir:

1. Aparat təminatının təhlükəsizliyi – Aparat təminatı mühitini telefon xətləri, giriş / çıxış portları, modemlər, şəbəkə kabelləri, skanerlər, printerlər və s. əhatə edir. Bu avadanlıqların oğurluqdan, enerji uğursuzluqlarından, avadanlıq pozuntularından, diqqətsizlikdən, o cümlədən kitabxana mühitinə qarşı hər hansı bir təhdid və mövcudluğunun, məxfilik və məlumatların bütövlüyünün təhlükəsizliyinə ehtiyacı var.

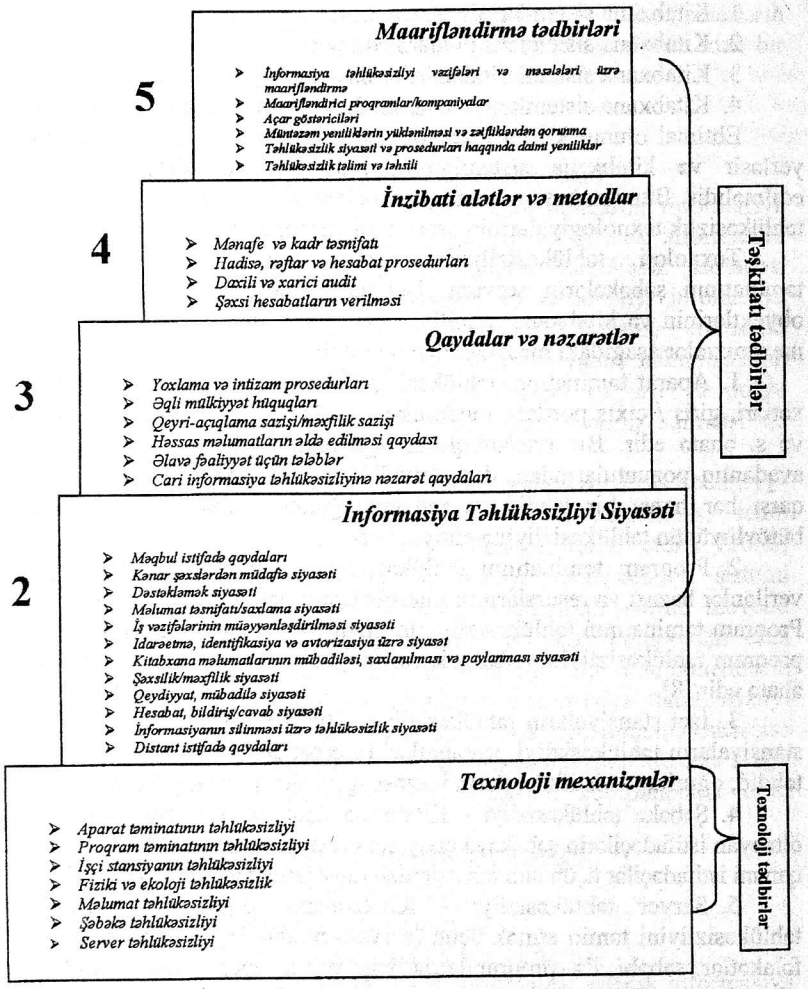
2. Proqram təminatının təhlükəsizliyi - Kitabxana sistemləri, online verilənlər bazası və resurslarının İnternet üzərindən yaradılmasına istinad edir. Proqram təminatının təhlükəsizliyinin imkanları proqramların qorunmasını və proqram təhlükəsizliyinin əhatə dairəsinin pozulmasının qarşısının alınmasını əhatə edir [8].

3. İşçi stansiyaların təhlükəsizliyi - Bir çox kütləvi kitabxanalarda işçi stansiyaların təhlükəsizliyi problemləri İnternetdən gəlir və belə problemlərə: təhdid, oğurluq və istifadəçilərin icazəsiz girişlərini misal göstərə bilərik [8].

4. Şəbəkə təhlükəsizliyi - Kitabxana üçün şəbəkə təhlükəsizliyi icazəsi olmayan istifadəçilərin şəbəkəyə çıxışının qarşısının alınmasını və eyni zamanda qanuni istifadəçilər üçün tam resurslardan rahat istifadəni təmin edir [8].

5. Server təhlükəsizliyi - Kitabxanalar e-poçt və web serverin təhlükəsizliyini təmin etmək üçün (serverə müdaxilə, viruslar, xakerlər, təbii fəlakətlər səbəbi ilə proqramlarda baş verən uğursuzluqlar və s.) hansı addımların atılmalı olduğunu təmin etməlidirlər. Kitabxanaların server bütövlüyü, əlçatanlığı, məxfiliyi və düzgünlüyü xüsusi təhlükəsizlik tədbirləri vasitəsilə təmin edilə bilər [8].

6. İnformasiya təhlükəsizliyi - Kitabxanaya öz məlumatlarının təhlükəsizliyini təmin etmək üçün elə bir məlumat idarəetmə sistemi lazımdır ki, müvafiq olaraq təsadüfi zərər, icazəsiz dəyişikliklər və s. zamanı bunlara qarşı tədbirlər həyata keçirə bilsin.



Şəkil 1. Kitabxana- informasiya sisteminin təhlükəsizlik modeli

Addım 2: İnformasiya təhlükəsizliyi siyasəti

İnformasiya təhlükəsizliyi siyasəti siyahi şəklində yazılmış sənədlərə və ümumi təhlükəsizlik strategiyası ilə bağlı müdafiə prosesini ortaya qoyan kitabxana təlimatlarına istinad edir. Təhlükəsizlik siyasəti icraçı heyətin və tərəfdarların kitabxanadan davamlı, ardıcıl istifadəsinin həyata keçirilməsi üçün tələb olunur. Sifarişin daha praktik və uğurla həyata keçirilə bilən olması üçün standartlar, qaydalar və prosedurlar siyasəti müəyyən edilir [7].

Addım 3: Qaydalar və nəzarətlər

Qaydların necə addım-addım həyata keçirilməsi və tətbiqi siyasəti qurumun təlimatları ilə həyata keçirilir. Qaydalar və nəzarətlər resursların və proseslərin necə çevrələnməsi (qorunması) prosedurları ilə işin qurulması əsasında həyata keçirilir. Bu addımlar istiqamətverici fərdi sənədlər və istifadəçi təlimatlarından, təhlükəsizlik planlarından, müqavilələrdən və yenilikləri təqib edən sənədləşdirilmiş sistemdən ibarətdir.

Addım 4: İnzibati alətlər və metodlar

İnzibati alətlərin və üsulların təmin olunmasında kitabxananın təhlükəsizlik sistemləri fəal və qeyri- fəal vasitədir. Belə ki, bura aktiv təsnifat, risk təhlili, audit və hər hansı bir hadisə ilə əlaqədar hesabat sistemləri daxildir.

Addım 5: Maarifləndirmə tədbirləri

Bu addım əməkdaşların və istifadəçilərin hər hansı bir proseslərlə işləməyi başa düşmək və təhlükəsizliyin əhəmiyyətinin fərqinə varmaq, təhlükəsizlik tədbirlərindən faydalanmaq və əldə etdikləri təhlükəsizlik tədbirlərinin nəticələrini öz işlərində tətbiq etmə bacarıqlarına istinad edir [2].

ƏDƏBİYYAT

1. *Von Solms, B. 2000. Information security – the third wave? Computers & Security, Vol.19, no.7: 615-620.*
2. *Pipkin, D.L. 2000. Information Security: Protecting the Global Enterprise. Upper Saddle River, NJ: Prentice Hall.*
3. *Newby, G.B. (2002). Information security for libraries. 20 http://www.petascale. org/papers/librarysecurity.pdf*
4. *Thompson, S.T.C. (2006). Helping the hacker? Library information, security and social engineering.*
5. *Zimerman, M. (2010). Protect your library's computers. New Library World, 111(5/6), 203-212.*
6. *Siponen, M.T. and Oinas-Kukkonen, H. 2007. A review of information security issues and respective research contributions. The Database for Advances in Information Systems, Vol.38, no.1: 60-81.*
7. *Hagen, J.M., Albrechtsen, E. and Hovden, J. 2008. Implementation and effectiveness of organizational information security measures. Information*

Management & Computer Security, Vol.16, no.4: 377-397.
8. *Eisenberg, J. and Lawthers, C. 2008. Library Computer and Network Security: Library Security Principles. Infopeople Project. Available at: http://www.infopeople.org/resources/ security/basics/index.html.*
9. *Fakeh, S.K.M., Zulhemay, M.N., Shabibi, M.S., Ali, J. ve Zaini, M. K. (2012). Information security awareness amongst academic librarians. http://www.aensiweb.com/ jasr/jasr/2012/17231735.pdf*

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЦИФРОВЫХ БИБЛИОТЕКАХ

ГАСАНОВА Н.А., МАГЕРРАМОВ И.Э.

РЕЗЮМЕ

В работе рассмотрены вопросы информационной защиты. Рассмотрены проблемы безопасности информации в цифровых библиотеках. Дана модель библиотечно информационной системы безопасности.

***Ключевые слова:** Защита информации, система информационной безопасности, модель библиотечно информационной системы безопасности.*

PROBLEMS OF INFORMATION SECURITY IN DIGITAL LIBRARIES

HASANOVA N.A., MAHARRAMOV İ.A.

SUMMARY

This paper considers issues of information protection. The problems of information security in digital libraries are considered. A model of library information security system is given.

***Keywords**: Information security, information systems security, library information systems security model.*

AZƏRBAYCAN MİLLİ KİTABXANASI TÜRK XALQLARININ MƏDƏNİYYƏTLƏRİNİN İNTEQRASİYASI SİSTEMİNDƏ (1994-2014)

HACIYEVA M.M.
M.F.Axundov adına Milli Kitabxananın Xarici əlaqələr üzrə direktor müavini
melek.h@anl.az

Məqalədə Azərbaycan Milli Kitabxanasının beynəlxalq əməkdaşlıq sahəsində türk dövlətlərinin nəhəng kitabxanaları ilə mədəni əlaqələrindən və bu əlaqələrin inkişafına təkan verən qarşılıqlı əməkdaşlıq barədə müqavilələrə əsasən birgə fəaliyyətindən, beynəlxalq konfrans, seminar və treninqlərdə birgə iştirakından bəhs edilir.

Açar sözlər: *TÜRKSOY, Azərbaycan Milli Kitabxanası, türkdilli dövlətlər, beynəlxalq əməkdaşlıq.*

Bəşər mədəniyyətinin yaradılmasında böyük rolu olan türkdilli xalqlar hər zaman bu mədəniyyətin zənginləşməsinə böyük töhfələr vermiş, daima insan həyatının bütün sahələrində öz istedadını, biliyini, bacarığını göstərmiş, qəhrəmanlıq nümunələri, böyük tarixi-memarlıq abidələri, elmi ixtiraları, qiymətli bədii əsərləri və müsiqisi ilə tarixin parlaq səhifələrini yaratmışlar.

1991-ci ildə SSRİ-nin dağılması zəminində türkdilli xalqların müstəqil dövlətləri yaranır. Artıq SSRİ-nin tərkibindən çıxıb müstəqil dövlət kimi fəaliyyətə başlayan bu xalqlar yenidən hər sahədə olduğu kimi ədəbi-bədii, mədəni sahələrdə də əlaqələrin gücləndirilməsi uğrunda çalışırlar. Müxtəlif birliklər və ya təşkilatlar yaradır və onun nəzdində fəaliyyət göstərirlər. Belə təşkilatlardan biri də Türk Mədəniyyəti və İncəsənətinin İnkişafı Üzrə Beynəlxalq Təşkilat (TÜRKSOY) olmuşdur.

TÜRKSOY Azərbaycan Respublikası və Türkiyə Cümhuriyyətinin təşəbbüsü ilə 1992-ci ildə İstanbul və Bakı şəhərlərində keçirilmiş Azərbaycan, Qazaxıstan, Qırğızıstan, Özbəkistan, Türkiyə və Türkmənistan respublikaları mədəniyyət nazirlərinin görüşləri gedişində razılaşmalar əldə edilmiş və 12 iyul 1993-cü ildə Qazaxıstan Respublikasının Almatı şəhərində yaradılmışdır. Sonralar TÜRKSOY haqqında müqaviləyə müşahidəçi ölkələr simasında Başqırdıstan, Tatarıstan respublikaları, Şimali Kipr Türk Respublikası, Xakasiya, Tuva, Çuvaşiya və Qaqauz Yeri respublikaları da qoşulmuşlar [10].

Təşkilat türkdilli ölkələrin mədəniyyət və incəsənət sahəsində regional əməkdaşlığını həyata keçirir. Onun əsas məramlarından biri türk dünyasının