UOT 004.9:351

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

E-DÖVLƏT MÜHİTİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ MƏDƏNİYYƏTİ PROBLEMLƏRİ

İnformasiya təhlükəsizliyi problemlərinin həlli texniki üsul və vasitələrlə yanaşı, həm də insanların mədəniyyətindən və peşə vərdişlərindən də asılıdır. Məqalədə informasiya təhlükəsizliyi anlayışının məzmununa müxtəlif yanaşmalar analiz edilir, informasiya təhlükəsizliyi mədəniyyəti ilə korporativ mədəniyyətin qarşılıqlı əlaqəsi aydınlaşdırılır və e-dövlət mühitində təşkilatın informasiya təhlükəsizliyi mədəniyyəti üçün konseptual model təklif edilir, konseptual modelin komponentlərinin formalaşdırılması istiqamətində bir sıra aktual problemlər müəyyən edilir.

Açar sözlər: *e-dövlət, informasiya təhlükəsizliyi, informasiya təhlükəsizliyi mədəniyyəti, korporativ mədəniyyət.*

Giriş

İnformasiya təhlükəsizliyi texnologiyaları, prosesləri və insanları əhatə edir. İnformasiya təhlükəsizliyinin texnoloji aspektləri zəruri diqqət tələb edir, lakin informasiya təhlükəsizliyinin lazımınca qiymətləndirilməyən və daha ciddi aspekti insan faktorudur. İnformasiya təhlükəsizliyi ilə bağlı itkilərin bir çoxunun səbəbi texnologiyanın yoxluğu və ya texnologiyalardakı səhvlərlə deyil, daha çox istifadəçilərin yanlış davranışları ilə bağlıdır. Bir sıra tədqiqatlar göstərir ki, əməkdaşların davranışı və onların kompüter sistemləri ilə qarşılıqlı əlaqəsi informasiya təhlükəsizliyinə əhəmiyyətli təsir edir. İnformasiya təhlükəsizliyi mədəniyyətinin məqsədi informasiya təhlükəsizliyinə təsir edə bilən müxtəlif insan faktorlarının idarə edilməsidir.

İnformasiya təhlükəsizliyi problemlərinin həlli texniki və texnoloji üsul və vasitələrlə yanaşı, həm də insanların mədəniyyətindən asılıdır. E-dövlətin informasiya təhlükəsizliyinin təmin edilməsi üçün zəruri tədbirlərdən biri də əhalidə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması və insanlarda təhlükəli informasiya təsirlərindən qorunma bacarıqlarının inkişaf etdirilməsidir.

E-dövlətin praktiki fəaliyyət uğurları təkcə texniki imkanlarla deyil, vətəndaşların mədəniyyəti, mentaliteti və peşə vərdişləri ilə də əlaqəlidir. Bu işdə e-dövlət mühitində informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması sahəsində problemlər analiz edilir. Məqalədə informasiya təhlükəsizliyi anlayışının məzmununa müxtəlif yanaşmalar analiz edilir və informasiya təhlükəsizliyi mədəniyyəti ilə korporativ mədəniyyətin qarşılıqlı əlaqəsi aydınlaşdırılır. Daha sonra e-dövlət mühitində təşkilatın informasiya təhlükəsizliyi mədəniyyəti üçün konseptual model təklif edilir və modelin komponentlərinin formalaşdırılması sahəsində bir sıra aktual problemlər müəyyən edilir.

İnformasiya təhlükəsizliyi mədəniyyəti anlayışı

E-dövlət mühitində informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması və inkişaf etdirilməsi istiqamətlərini və problemlərini düzgün müəyyənləşdirmək üçün "informasiya təhlükəsizliyi mədəniyyəti" terminin mahiyyətinə nəzər salmaq vacibdir. "İnformasiya təhlükəsizliyi mədəniyyəti" anlayışı "mədəniyyət", "informasiya mədəniyyəti", "informasiya təhlükəsizliyi" və "korporativ mədəniyyət" anlayışları ilə sıx əlaqəlidir.

"Mədəniyyət" anlayışı olduqca çoxcəhətlidir və onun müəyyən edilməsinə bir sıra yanaşmalar mövcuddur (idarə-sahə, humanist, informasiya-semiotik, mənəvi-istehsal, etno-arxeoloji, funksional-fəaliyyət və s.). Kultura (lat. cultura, colere – "becərmək" kökündən yaranıb) – evolyusiya prosesində insan tərəfindən yaradılan və yaradılmaqda olan insanın həyat

fəaliyyəti formaları üçün ümumiləşdirici anlayışdır. Mədəniyyət – insanın həyat fəaliyyətinin təşkilinin və inkişafının spesifik üsuludur, maddi və mənəvi əmək məhsullarında, sosial normalar və təsisatlar sistemində, mənəvi dəyərlərdə, insanların təbiətə, öz aralarında və özünə münasibətləri məcmusunda ifadə olunur. Mədəniyyət – mənəvi, əxlaqi və maddi dəyərlər, bilik və bacarıqlar, adətlər, ənənələrdir. Beləliklə, mədəniyyət fəaliyyətin müəyyən formasıdır və onun nəticələri dəyərlərdir (mənəvi, əxlaqi, maddi və s.) [1].

İnformasiya mədəniyyəti insanın informasiyanın qəbulu, ötürülməsi, saxlanılması və istifadəsi sahəsində həyat fəaliyyətini xarakterizə edir. İnformasiya mədəniyyətinin tərkibində onun bir sıra struktur elementlərini – metodoloji, hüquqi, etik, linqvistik, texniki-texnoloji elementləri aşkarlamaq olar [1].

Cəmiyyətin inkişafının hazırki mərhələsində informasiya mədəniyyətini şəxsiyyətin ümumi mədəniyyətinin əsas göstəricilərindən biri hesab etmək olar və onu informasiya təhlükəsizliyi mədəniyyəti olmadan təsəvvür etmək mümkün deyil.

Ədəbiyyatda informasiya təhlükəsizliyi mədəniyyəti anlayışına müxtəlif təriflər verilir. Bu yanaşmaların ümumiləşdirilməsi olaraq, [2]-də informasiya təhlükəsizliyi mədəniyyətinə belə tərif verilir: "İnformasiya təhlükəsizliyinə dair texniki bilik və bacarıqlar, insanın mənəvi-psixoloji sağlamlığı üçün təhlükəli olan informasiya təsirləri və onlardan qorunma üsulları barədə bilik və bacarıqlar, informasiya resurslarından istifadə zamanı hüquqi və etik normalara əməl edilməsi insanın informasiya təhlükəsizliyi mədəniyyətinin əsasını təşkil edir."

Bu məqalədəki yanaşmaya görə, informasiya təhlükəsizliyi mədəniyyəti – informasiya təhlükəsizliyinin daha yüksək səviyyəsinə nail olmaq məqsədilə informasiya təhlükəsizliyi sahəsində bilik, bacarıq və vərdişlərin mənimsənilməsi prosesi və onların tətbiqi prosesidir.

Buna uyğun olaraq informasiya təhlükəsizliyi mədəniyyəti anlayışının mahiyyətini sxematik olaraq piramida şəklində təsvir etmək olar, piramidanın oturacağını informasiya mədəniyyəti təşkil edir, onu üstqurum kimi şəxsiyyətin informasiya-psixoloji təhlükəsizliyi mədəniyyəti, informasiya təhlükəsizliyinin texnoloji mədəniyyəti və hüquqi mədəniyyət tamamlayır.

Hazırda antropoloqlar mədəniyyətə bioloji evolyusiyanın sadəcə nəticəsi kimi deyil, onun ayrılmaz elementi kimi, insanın ətraf mühitə adaptasiyasının əsas mexanizmi kimi baxırlar. Uyğun olaraq, informasiya təhlükəsizliyi mədəniyyətinə insanın müasir informasiya cəmiyyəti şəraitində təhlükəsiz yaşayışa adaptasiya mexanizmi kimi baxmaq olar.

Təşkilatın informasiya təhlükəsizliyi mədəniyyətinə yanaşmalar

Təşkilatın informasiya təhlükəsizliyi mədəniyyəti ümumi korporativ funksiyalara nəzərən submədəniyyətdir və bilavasitə korporativ mədəniyyət anlayışına yaxındır, bu anlayışlar arasındakı münasibətlər [3]-də ətraflı şəkildə araşdırılır.

Korporativ mədəniyyət təşkilatın uğurlu fəaliyyəti üçün əsas təşkil edən, təşkilatın üzvləri tərəfindən paylaşılan ideyalardan, baxışlardan, dəyərlərdən ibarətdir. Hazırda korporativ mədəniyyət anlayışına bir neçə yanaşma mövcuddur və onların əsasında təşkilatın informasiya təhlükəsizliyi üçün bir sıra modellər işlənmişdir.

E.Şeynin təklif etdiyi korporativ mədəniyyət modeli [4] daha geniş istifadə edilir. Şeynin korporativ mədəniyyət modeli əsasında T. Schlienger və S. Teufelin təklif etdiyi modeldə informasiya təhlükəsizliyi mədəniyyətinin üç qatı var [5]:

- *Korporativ siyasət*: təhlükəsizlik siyasəti, təşkilatın strukturu və resurslar daxildir.
- *Menecment*: informasiya təhlükəsizliyi siyasətinin həyata keçirilməsi, cavabdehliklər, kvalifikasiya və təlimlər, mükafatlar və cəzalar, audit və etalon testlər nəzərdə tutulur.
- *Fərd*: münasibət, kommunikasiya və riayət etmə daxildir.

A. B. Ruighaver və həmmüəlliflərinin təklif etdiyi modeldə mövcud korporativ mədəniyyət modellərindən [6] səkkiz faktor seçilmiş və bu faktorların hər biri üçün ümumi keyfiyyət menecmenti modelindən bir münasib qiymət qarşı qoyulmuşdur [7]. Təhlükəsizlik büdcəsi,

təhlükəsizlik xərcləri, əməkdaşların təhlükəsizlik sahəsində məlumatlılığı, əməkdaşların təhlükəsizlik risqləri, təhlükəsizlik siyasətinin həyata keçirilməsi, təhlükəsizlik üzrə təkliflərin edilməsi, təhlükəsizliyə sahiblik və təhlükəsizlik auditləri kimi faktorlar istifadə edilir.

Mövzu üzrə mövcud ədəbiyyatın analizi, iki fokus-qrup və üç tematik tədqiqat əsasında [8]-də kiçik və orta müəssisələrdə (Avstraliya misalında) informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması və inkişafı üçün model irəli sürülür. Təklif edilən model aşağıdakı faktorları əhatə edir:

- *idarəçilik aspektləri* (siyasət və proseduralar, etalon qiymətləndirmə, risq analizi, büdcə, rəhbərliyin münasibəti, təlim və təhsil, məlumatlılıq, dəyişikliklərin idarə edilməsi);
- *davranış məsələləri* (məsuliyyət, tamlıq, inam, etnik kimlik, dəyərlər, motivasiya və yönəlmə);
- *fərdi və təşkilati e-təlim* (təlim və təhsil);
- *etika, milli mədəniyyət və korporativ mədəniyyət.*

D. Straub və həmmüəllifləri [9]-da qeyd edirlər ki, informasiya sistemləri üzrə tədqiqatlarda, adətən, fərdin yalnız bir mədəniyyətə mənsub olması nəzərdə tutulur. Onlar informasiya sistemlərində mədəniyyət məsələlərini tədqiq edərkən əsaslandırma üçün sosial kimlik nəzəriyyəsindən istifadə etməyi təklif edirlər. Sosial kimlik nəzəriyyəsi hər bir fərdə bir neçə mədəniyyətin təsir etdiyini nəzərdə tutur. İnformasiya təhlükəsizliyi mədəniyyətinə bunu tətbiq etdikdə, bu o deməkdir ki, fərdə bir neçə etik, milli, korporativ və informasiya təhlükəsizliyi mədəniyyətinin təsir etdiyi nəzərə alınmalıdır.

Bu yanaşmanı nəzərə alaraq, [10]-da təklif edilən modeldə informasiya təhlükəsizliyi mədəniyyətinə bir-biri ilə qarşılıqlı təsirdə olan **platforma** (standartlaşdırma, serifikatlaşdırma, informasiya təhlükəsizliyinin ölçülməsi) və **kontent** (münasibət, motivasiya, bilik, kommunikasiya, əməletmə) komponentlərindən ibarət olan mürəkkəb sistem kimi baxılır.

Təşkilatda informasiya təhlükəsizliyi mədəniyyəti müxtəlif səviyyələrdə, o cümlədən fərdi, qrup və təşkilati səviyyədə mövcud olmalıdır. Göstərilən bu üç səviyyənin hər birində aktual məsələlər də müxtəlifdir [11]. Təşkilat səviyyəsində siyasət və prosedurlar, etalonla qiymətləndirmə, risq analizi və büdcə əsas məsələlərdir. Qrup səviyyəsində idarəetmə və inam, fərdi səviyyədə isə məlumatlılıq və etik davranış əsas məsələlərdir.

Qlobal kibertəhlükəsizlik mədəniyyəti

Qlobal kibertəhlükəsizlik mədəniyyətinin yaradılması üçün elementlər Birləşmiş Millətlər Təşkilatı (BMT) Baş Məclisinin 20 dekabr 2002-ci il tarixli 57/239 saylı qətnaməsi ilə təsdiq edilmişdir.

Qlobal kibertəhlükəsizlik mədəniyyəti bütün iştirakçılardan − informasiya sistemləri və şəbəkələrini yaradan, onlara sahib olan, idarə edən, xidmət edən və istifadə edən dövlət orqanlarından, müəssisələrdən və digər təşkilatlardan, fərdi istifadəçilərdən bir-birini tamamlayan aşağıdakı doqquz elementə əməl etmələrini tələb edəcək:

a) *Məlumatlı olmaq.* İştirakçılar informasiya sistemlərinin və şəbəkələrin təhlükəsizliyinin zəruriliyi haqqında və təhlükəsizliyin yüksəldilməsi üçün onların nə edə biləcəkləri barədə məlumatlı olmalıdırlar;

b) *Cavabdehlik.* İştirakçıların hər biri informasiya sistemlərinin və şəbəkələrin təhlükəsizliyi üçün öz rollarına uyğun olaraq cavabdehlik daşıyırlar. İştirakçılar öz siyasətlərini, fəaliyyətlərini, tədbirlərini və prosedurlarını müntəzəm olaraq nəzərdən keçirməli və onların tətbiq edildikləri mühitə uyğunluqlarını qiymətləndirməlidirlər;

c) *Reaksiya.* İştirakçılar təhlükəsizliyə aid insidentlərin qarşısının alınması, onların aşkarlanması və onlara cavab verilməsi üzrə vaxtında və birgə tədbirlər görməlidirlər. Onlar lazımi hallarda təhdidlər və boşluq faktorları haqqında məlumat mübadiləsi etməli və belə insidentlərin qarşısının alınması, onların aşkarlanması və onlara cavab verilməsi işində operativ

və effektiv əməkdaşlığı nəzərdə tutan prosedurlar tətbiq etməlidirlər. Bu transsərhəd informasiya mübadiləsini və əməkdaşlığı nəzərdə tuta bilər;

d) *Etika.* İnformasiya sistemləri və şəbəkələri müasir cəmiyyətin bütün sahələrinə nüfuz etdiyindən, iştirakçıların digərlərinin qanuni maraqlarını nəzərə alması və onların hərəkətlərinin və hərəkətsizliyinin başqalarına ziyan vura bilməsini qəbul (etiraf) etməsi zəruridir;

e) *Demokratiya.* Təhlükəsizlik elə təmin edilməlidir ki, bu fikir və ideyaların mübadiləsinin sərbəstliyi, azad informasiya axını, informasiya və kommunikasiyanın konfidensiallığı, şəxsi xarakterli informasiyanın lazımi şəkildə qorunması, açıqlıq və aşkarlıq daxil olmaqla demokratik cəmiyyətdə qəbul edilən dəyərlərə uyğun olsun;

f) *Riskin qiymətləndirilməsi.* Bütün iştirakçılar riskin dövri olaraq qiymətləndirilməsini yerinə yetirməlidirlər. Bu təhdidləri və zəifliklərin faktorlarını aşkarlamağa imkan verir; texnologiya, fiziki və insan faktorları, tətbiq edilən metodika və üçüncü tərəflərin təhlükəsizliyə təsir edən xidmətləri kimi əsas daxili və xarici faktorları əhatə etmək üçün yetərincə geniş bazaya malikdir; riskin yolverilən səviyyəsini müəyyən etməyə imkan verir; mühafizə edilən informasiyanın xarakteri və əhəmiyyəti nəzərə alınmaqla informasiya sistemlərinə və şəbəkələrinə potensial ziyan riskini nizamlamağa imkan verən lazımi nəzarət alətlərini seçməyə kömək edir;

g) *Təhlükəsizliyin layihələndirilməsi və realizə edilməsi.* İştirakçılar təhlükəsizlik mülahizələrini informasiya sistemlərinin və şəbəkələrin planlaşdırılması, layihələndirilməsi, istismarı və istifadəsinin vacib elementi kimi nəzərdə tutmalıdırlar;

h) *Təhlükəsizliyin idarə edilməsi.* İştirakçılar fəaliyyətlərinin bütün səviyyələrini və əməliyyatlarının bütün cəhətlərini əhatə edən riskin dinamik qiymətləndirilməsinə söykənərək, təhlükəsizliyin idarə edilməsinə kompleks yanaşmanı qəbul etməlidirlər;

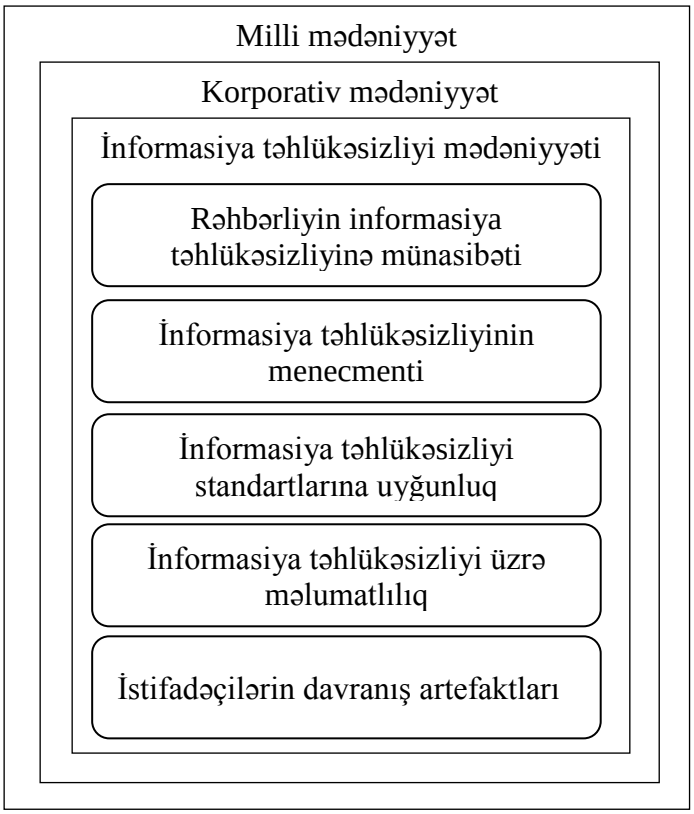
i) *Yenidən qiymətləndirmə.* İştirakçılar informasiya sistemlərinin və şəbəkələrin təhlükəsizliyi məsələlərini yenidən nəzərdən keçirməli və təkrar qiymətləndirməlidirlər, təhlükəsizliyin təmin edilməsi siyasətinə, təcrübəsinə, tədbirlərinə və prosedurlarına lazımi dəyişikliklər etməlidirlər. Bu zaman əvvəlki təhdidlərin və boşluq faktorlarının dəyişməsi və yenilərinin meydana çıxması nəzərə alınmalıdır.

Təşkilatın informasiya təhlükəsizliyi mədəniyyətinin konseptual modeli

Yuxarıda aparılan müzakirələri nəzərə almaqla təşkilatın informasiya təhlükəsizliyi mədəniyyətinin təklif edilən konseptual modelinin əsas komponentləri şəkil 1-də göstərilib.

Milli mədəniyyət informasiya təhlükəsizliyi mədəniyyətinə təsir edən xarici mühit (faktor) rolunu oynayır [12]. Təşkilatın informasiya təhlükəsizliyi mədəniyyəti bütövlükdə rəhbərliyin informasiya təhlükəsizliyinə baxışlarını əks etdirir [6]. Analiz göstərir ki, informasiya təhlükəsizliyinin menecmenti ilə informasiya təhlükəsizliyinin bir-birinə qarşılqlı təsiri olduqca yüksəkdir [13].

İnformasiya təhlükəsizliyi mədəniyyətinin əsas faktorlarından biri informasiya təhlükəsizliyi baxımından informasiya mübadiləsi mühitində olan təhlükələr, problemlər və risqlər barəsində məlumatlılıqdır. Əməkdaşların informasiya təhlükəsizliyi sahəsində məlumatlılığının yaxşılaşdırılması təşkilatın informasiya təhlükəsizliyi siyasətinin əhəmiyyətli məqsədlərindən biri olmalıdır. İnformasiya təhlükəsizliyi sahəsində məlumatlılığı bilik, münasibət (attitude) və davranış baxımından araşdırmaq olar [14].



Şəkil 1. Təşkilatın informasiya təhlükəsizliyi mədəniyyətinin konseptual modelinin komponentləri

İnformasiya təhlükəsizliyinin təmin edilməsi standartları – informasiya təhlükəsizliyinin təmin edilməsi sisteminin qurulması üzrə qərarların qəbul edilməsində və həyata keçirilməsində iştirak edən şəxslərin davranış qaydaları sistemidir. Bu baxımdan standartlar post-sənaye cəmiyyətinin mədəniyyətinin vacib elementləridir, cəmiyyətin, dövlətin və təşkilatların fəaliyyətlərinin effektivliyinə bilavasitə təsir göstərirlər. Davranış standartlarının müəyyən edilməsi və onlara əməl edilməsi cəmiyyətin sosial yetkinliyinin və onun üzvlərinin ümumi mədəniyyətinin vacib göstəricisidir.

İnformasiya təhlükəsizliyi mədəniyyətinin təşviq edilməsi yolları yuxarı rəhbərliyin öhdəliyi, əməkdaşların iştirakı, təhlükəsizlik şüurunun yaradılması, büdcənin ayrılması, inam əlaqələrinin artırılması və icra (və nəzarət) proseslərdir.

İnformasiya təhlükəsizliyi mədəniyyətinin qiymətləndirilməsi modelləri

İnformasiya təhlükəsizliyi mədəniyyəti hələlik geniş tədqiq olunmayıb, lakin son onillikdə nəşr olunan işlərin sayına görə fəal tədqiqatların aparılmasını söyləmək olar. Bununla yanaşı, informasiya təhlükəsizliyi mədəniyyətinin qiymətləndirilməsi sahəsində yalnız bir neçə tədqiqat mövcuddur. Bu tədqiqatlar ekspert qiymətləndirməsi və rəy sorğusu metodlarına əsaslanırlar.

İnformasiya təhlükəsizliyi mədəniyyətinin qiymətləndirilməsinə yanaşma audit prosesindən ibarətdir, burada əməkdaşların informasiya təhlükəsizliyinə aid qavrayışları, münasibətləri, fikir və hərəkətləri müəyyən edilir.

İnformasiya Təhlükəsizliyi Forumu (ing. Information Security Forum, ISF) 2000-ci ildə nəşr etdirdiyi hesabatda informasiya təhlükəsizliyi mədəniyyətinin qiymətləndirilməsi üçün sorğu anketinin işlənilib hazırlanmasını təklif etmişdi. Anketin əsas məqsədi informasiya təhlükəsizliyi mədəniyyətinin təşkilatda informasiya təhlükəsizliyi risqlərinin səviyyəsinə təsirini qiymətləndirmək və təkmilləşdirmək üçün spesifik hədəf sahələrini müəyyən etmək idi. Qeyd

etmək lazımdır ki, sonrakı illərdə ISF Forumunun bu sahədə gördüyü işlər barəsində hər hansı məlumat əlyetər deyil.

T.Schlienger və S.Teufelin yanaşması əməkdaşların təhlükəsizlik davranışlarına təsir etməyə yönəlmiş rəsmi qaydaların analizinə əsaslanır [15]. Onlar E. Şeynin korporativ mədəniyyət modelinə [4] uyğun olaraq informasiya təhlükəsizliyi mədəniyyətinin müxtəlif laylarının – maddi mədəniyyət nümunələrinin (artefaktların), mənimsənilmiş dəyərlərin və paylaşılan baza məsuliyyətlərin – ölçülməsi üçün bir neçə metoddan istifadə etməyi təklif edirlər. İnformasiya təhlükəsizliyi siyasəti və prosedurları kimi rəsmi sənədlərin analizi əsasında artefaktlar və rəsmi, mənimsənilmiş dəyərlər qiymətləndirilir, lakin bu metod əməkdaşların həqiqi dəyərlərini əhatə edə bilmir. İnformasiya təhlükəsizliyi siyasəti haqqında anketin cavablandırılması əməkdaşların həqiqi dəyərlərinin mənzərəsini almağa kömək edir. İnformasiya təhlükəsizliyi menecerləri ilə aparılan sorğu-müsahibə hər üç layın icmalını almağa imkan verir. Artefaktlar audit vasitəsilə də analiz edilr, bu zaman informasiya təhlükəsizliyi mədəniyyətinin görünən hissəsi öyrənilir.

A. da Veiga və həmmüəlliflərinin təklif etdiyi modeldə [16] informasiya təhlükəsizliyi mədəniyyətinin qiymətləndirilməsi üzrə anket üç bloka bölünür: (1) informasiya təhlükəsizliyi mədəniyyətinin xarakteristikaları; (2) bilik sualları; (3) bioqrafiya sualları.

İnformasiya təhlükəsizliyi mədəniyyətinin xarakteristikaları bloku əməkdaşların informasiya təhlükəsizliyinin 8 müxtəlif parametrinə (ölçüsünə) münasibətini qiymətləndirir: siyasət (2 faktor), menecement (2 faktor), proqram (7 faktor), rəhbərlik (8 faktor), aktivlərin menecmenti (8 faktor), istifadəçilərin menecmenti (8 faktor), dəyişikliklərin menecmenti (4 faktor) və inam (3 faktor). Respondentlərin münasibəti Likert şkalası (“Tamamilə razı deyiləm”, “Razı deyiləm”, “Neytral”, “Razıyam”, “Tamamilə razıyam”) ilə ölçülür. Bilik sualları bloku əməkdaşların informasiya təhlükəsizliyi sahəsində nə qədər biliyə malik olduqlarını və təşkilatın informasiya təhlükəsizliyi mədəniyyətinin təhsildən, yoxsa münasibətdən asılı olmasını müəyyən etməyə xidmət edir. Bu suallara cavab vermək üçün “Hə/Yox” şkalasından istifadə edilir. Bioqrafiya sualları verilənləri seqmentlərə ayırmaq və populyasiya daxilində müqayisələr aparmaq üçün anketə daxil edilib.

İnformasiya təhlükəsizliyi mədəniyyətinin ölçülməsi üçün M. Alnatheer və həmmüəlliflərinin təklif etdiyi modeldə [17] informasiya təhlükəsizliyi mədəniyyətini təşkil edən faktorlar (informasiya təhlükəsizliyi sahəsində məlumatlılıq və informasiya təhlükəsizliyi üzrə məsuliyyət) və informasiya təhlükəsizliyinə təsir edən faktorlar (yuxarı səviyyə rəhbərlərinin informasiya təhlükəsizliyinə cəlb edilməsi, informasiya təhlükəsizliyi siyasətinin həyata keçirilməsi və informasiya təhlükəsizliyi üzrə təlim) bir-birindən fərqləndirilir.

Sorğu anketi yuxarıda seçilmiş faktorları xarakterizə etmək üçün ölçmə dəyişənləri müəyyən edilməklə tərtib edilir:

- yuxarı səviyyə rəhbərlərinin informasiya təhlükəsizliyinə cəlb edilməsi (5 dəyişən);
- informasiya təhlükəsizliyi siyasətinin həyata keçirilməsi (4 dəyişən);
- informasiya təhlükəsizliyi üzrə təlim (3 dəyişən);
- informasiya təhlükəsizliyi sahəsində məlumatlılıq (4 dəyişən);
- informasiya təhlükəsizliyi üzrə məsuliyyət (3 dəyişən).

Respondentlərin münasibəti uc nöqtələri “tamamilə razı deyiləm” və “tamamilə razıyam” olmaqla Likert şkalasından istifadə edilməklə ölçülür. Təklif edilən modelin əsaslandırılması və yoxlanılması SPSS paketi istifadə edilməklə ətraflı şəkildə tədqiq edilir [18]. Istifadə edilən şkalanın ölçmə xətalarına qarşı dayanıqlılığı obyekti xarakterizə edən xarakteristikaların daxili uzlaşması (Kronbax alfa əmsalı [19]) və sorğunun daxili etibarlılığı (ümumi korrelyasiya) ilə təmin edilir. Daha sonra modelin validasiyası üçün eksplorator və konfirmator faktor analizi aparılır, Kayzer-Meyer-Olkin kəmiyyəti qiymətləndirilir və Bartlett testi yerinə yetirilir [18].

E-dövlətdə informasiya təhlükəsizliyi mədəniyyəti problemləri

E-dövlət mühitində informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması və inkişafı problemləri çərçivəsində aşağıdakı tədqiqat mövzuları aktualdır:

- informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması sahəsində dövlət siyasətinin əsas istiqamətləri;
- informasiya təhlükəsizliyi mədəniyyətinin məzmunu və struktur komponentləri;
- əhalinin informasiya təhlükəsizliyi məsələləri üzrə maarifləndirilməsi;
- təşkilatlarda informasiya təhlükəsizliyi mədəniyyətinin idarə edilməsi problemləri;
- təşkilatlarda informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması məsələləri, istiqamətləri, mexanizmləri və problemləri;
- informasiya təhlükəsizliyi mədəniyyətinin ölçülməsi problemləri (indikatorların müəyyən edilməsi);
- informasiya təhlükəsizliyi mədəniyyətinin informasiya təhlükəsizliyinin təmin edilməsinə təsirinin qiymətləndirilməsi;
- informasiya texnologiyaları və informasiya təhlükəsizliyi sahəsində etika problemləri.

Haker submədəniyyətinin öyrənilməsi də nisbətən az tədqiq olunmuş sahələrdən biridir [20]. Submədəniyyət ictimai mədəniyyətin öz davranışı ilə dominant mədəniyyətdən fərqlənən hissəsidir. Dar mənada bu termin sosial qrupu – submədəniyyətin daşıyıcılarını bildirir. Submədəniyyət dominant mədəniyyətdən özünün məxsusi dəyərlər sistemi, dili, davranış tərzi, geyimi və digər cəhətləri ilə fərqlənə bilər.

Haker submədəniyyətinin tədqiqi təkcə informasiya təhlükəsizliyi baxımından deyil, mədəniyyətdə və onun müxtəlif sosio-mədəni seqmentlərində innovasiya proseslərini analiz etməyə imkan verən yeni nəzəri-metodoloji bazanın yaradılması baxımından da aktualdır [21]. Bu cəhətdən haker submədəniyyəti aşağıdakı problemləri tədqiq etmək üçün çox cəlbedici sahədir:

- informasiya cəmiyyətinə keçidlə bağlı transformasiya proseslərinin müasir mədəniyyətlərə və onun altsistemlərinə təsiri;
- submədəniyyətlərin yaranması və inkişafında texniki faktorların və kommunikasiya vasitələrinin rolu;
- informasiya mühitində submədəniyyətlərin fəaliyyət mexanizmləri;
- yeni növ submədəniyyətlərin informasiya cəmiyyətində dünyagörüşlərinin və rol modellərinin formalaşmasında rolu və s.

Nəticə

Öz vətəndaşlarını informasiya təhlükəsizliyi təhdidlərindən qorumaq istənilən sivil cəmiyyətin, dövlətin vəzifəsidir. Eyni zamanda, e-dövlətin informasiya təhlükəsizliyi problemlərini geniş ictimaiyyət cəlb edilmədən həll etmək çox çətindir.

İnformasiya təhlükəsizliyi problemlərinin həlli texniki və texnoloji üsul və vasitələrlə yanaşı, həm də insanların mədəniyyətindən asılıdır. Şəxsiyyətin informasiya təhlükəsizliyinin təmin edilməsi üçün zəruri tədbirlərdən biri də əhalidə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması və onlarda təhlükəli informasiya təsirlərindən qorunma bacarıqlarının inkişaf etdirilməsidir. İnformasiya təhlükəsizliyi mədəniyyəti kortəbii yarana bilməz, onun təhsil sistemi, vətəndaş cəmiyyəti institutları vasitəsilə məqsədyönlü şəkildə formalaşdırılması zəruridir. Bu məsələ dövlətin informasiya və informasiya təhlükəsizliyi siyasətlərinin vacib tərkib elementi olmalıdır.

Məqalədə e-dövlət mühitində informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması sahəsində əsas fəaliyyət istiqamətlərinin müəyyən edilməsi məqsədilə informasiya təhlükəsizliyi anlayışının məzmunu və struktur komponentləri analiz edilmiş, təşkilatın informasiya təhlükəsizliyi mədəniyyəti üçün konseptual model işlənmiş və informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması istiqamətində bir sıra aktual elmi-praktiki tədqiqat problemləri

müəyyən edilmişdir. Gələcək tədqiqatlarda e-dövlətin müxtəlif aktorlarında informasiya təhlükəsizliyi mədəniyyətinin səviyyəsinin qiymətləndirilməsi üçün indikatorlar sisteminin və ölçmə metodlarının işlənməsi və müvafiq qiymətləndirmələrin aparılması nəzərdə tutulur.

Ədəbiyyat

1. Алгулиев Р.М., Махмудова Р.Ш. Структурный подход к формированию информационной культуры личности // Открытое образование, 2011, №4, стр.64–74.
2. Mahmudova R.Ş. Cəmiyyətdə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması məsələləri haqqında // İnformasiya cəmiyyəti problemləri, 2013, №1 (7), s.32–38.
3. Lim J.S., Chang S., Maynard S., Ahmad A. Exploring the relationship between organizational culture and information security culture / Proc. of the 7th Australian Information Security Management Conference, 2009, pp.88–97.
4. Schlienger T., Teufel S. Information security culture: the socio-cultural dimension in information security management / Proc. Security in the Information Society: Visions and Perspectives, 2002, pp.191–202.
5. Schein E.H. The corporate culture survival guide. Jossey-Bass Inc. 1999.
6. Detert J., Schroeder R., Mauriel J. A framework for linking culture and improvement initiatives in organisations // The Academy of Management Review, 2000, vol.25, no.4, pp.850–863.
7. Ruighaver A.B., Maynard S.B., Chang S. Organisational security culture: Extending the end-user perspective // Computers & Security, 2007, vol.26, No.1, pp.56–62.
8. Dojkovski S., Lichtenstein S., Warren M. J. Fostering information security culture in small and medium size enterprises: an interpretive study in Australia / Proc. 15th European Conference on Information Systems, 2006, Paper 120, pp.1560–1571.
9. Straub D., Loch K., Evaristo R., Karahanna E., Strite M. Toward a theory-based measurement of culture // Journal of Global Information Management, 2002, vol.10, no.1, pp.13–23.
10. Kuusisto T., Ilvonen I. Information security culture is small and medium enterprises / Proc. of Frontiers of E-business Research, 2003, pp.431–439.
11. Martins A., Eloff J. H. P. Information security culture / IFIP TC11 International Conference on Information Security, 2002, pp.203–214.
12. Straub D., Loch K., Hill C. Transfer of information technology to the Arab world: a test of cultural influence modeling. Advanced Topics in Global Information Management, Hershey, PA: Idea Group Publishing. 2003, pp.141–172.
13. Knapp K.J., Marshall T.E., Rainer R.K., Ford F.N. Information security: management's effect on culture and policy // Information and Computer Security, 2006, vol.14, no.1, pp.24–36.
14. Kruger H.A., Kearney W.D. A prototype for assessing information security awareness // Computers & Security, 2006, vol.25, no.4, pp.289–296.
15. Schlienger T., Teufel S. Analyzing information security culture: increased trust by an appropriate information security culture / Proc. 14th International Workshop on Database and Expert Systems Applications (DEXA), 2003, pp.405–409.
16. Da Veiga A., Martins N., Eloff J.H.P. Information security culture – validation of an assessment instrument // Southern African Business Review, 2007, vol.11, no.1, pp.147–166.
17. Alnatheer M., Chan T., Nelson K. Understanding and measuring information security culture / Proc. of the Pacific Asia Conference on Information Systems (PACIS), 2012, Paper 144.
18. Pallant J. SPSS Survival Manual: A step by step guide to Data Analysis using SPSS for Windows (Version 12). Berkshire: Open University Press. 2005.
19. Streiner D. L. Starting at the beginning: an introduction to coefficient alpha and internal consistency // Journal of Personality Assessment, 2003, vol.80, no.1, pp.99–103.

20. Dremliuga R., Subculture of Hackers in Russia // Asian Social Science, 2014, vol.10, no.18, pp.158.
21. Miller F.P., Vandome A.F., McBrewster J., Hacker (programmer subculture), 2010.

УДК 004.9:351
Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@lan.ab.az
Проблемы культуры информационной безопасности в среде э-государства
Решение проблем информационной безопасности наряду с техническими средствами защиты информации зависит также от культуры и профессиональных навыков людей. В статье анализируются различные подходы к определению содержания понятия культуры информационной безопасности, уточняется взаимосвязь культуры информационной безопасности и корпоративной культуры и предлагается концептуальная модель культуры информационной безопасности организации в среде э-государства. Также идентифицируется ряд актуальных научно-практических проблем в направлении формирования и развития компонентов предложенной концептуальной модели.
Ключевые слова: *э-государство, информационная безопасность, культура информационной безопасности, корпоративная культура.*

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az
Problems of information security culture in e-government environment
Solutions to the problems of information security along with technical means of information protection, also depends on the culture and skills of people. The paper analyzes the various approaches to the definition of the notion of information security culture, clarifies the relationship between information security culture and corporate culture, and proposes a conceptual model of information security culture in the e-government environment. It also identifies a number of challenging scientific and practical problems in the field of formation and development of components of the proposed conceptual model.
Keywords: e-government, information security, information security culture, corporate culture.