UOT 004.056:316.7 DOI: 10.25045/jpis.v12.i1.05

Mahmudova R.Ş.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
rasmahmudova@gmail.com

FƏRDİN VƏ CƏMİYYƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİ MƏDƏNİYYƏTİNİN BƏZİ ASPEKTLƏRİ HAQQINDA

Daxil olmuşdur: 20.12.2020. Düzəliş olunmuşdur: 06.01.2021. Qəbul olunmuşdur: 13.01.2021.

Məqalədə fərdin və cəmiyyətin informasiya təhlükəsizliyi mədəniyyətinin bəzi aspektləri araşdırılır. İnformasiya təhlükəsizliyi problemlərinə texnoloji və humanitar aspektdən yanaşmalar təhlil edilir. İnformasiya sistemlərində toplanan informasiyanın, o cümlədən sirr daşıyan məlumatların mühafizəsi, fərdi məlumatların qorunması kimi problemlərin həlli texnoloji üsul və vasitələrlə yanaşı insan faktorundan asılı olduğu üçün informasiya təhlükəsizliyi mədəniyyətinin öyrənilməsi olduqca aktualdır. Bu baxımdan fərdin və cəmiyyətin informasiya təhlükəsizliyi ilə bağlı müxtəlif problemlər (informasiya bolluğunun yaratdığı problemlər, informasiya "çirklənməsi" problemləri, fərdi və kütləvi şüurun manipulyasiyası, kibercinayətlər, fərdi məlumatların qorunması, informasiya müharibələri, kiberxəstəliklər və s.) araşdırılır və bu problemlərin aradan qaldırılmasında informasiya təhlükəsizliyi mədəniyyətinin rolu əsaslandırılır. Müxtəlif yanaşmaların təhlili əsasında informasiya təhlükəsizliyi mədəniyyətinin mahiyyəti və tərkib hissələri analiz olunur. İnformasiya təhlükəsizliyi mədəniyyətinin texnoloji, informasiya-psixoloji və hüquqi-etik aspektləri araşdırılır və müəyyən təkliflər verilir. İşin yerinə yetirilməsində analiz və sintez, müqayisə, ümumiləşdirmə, sistemli yanaşma metodlarından istifadə edilmişdir. Məqalədə əldə edilən nəticələr informasiya təhlükəsizliyi problemlərini araşdıran tədqiqatçılar, informasiya təhlükəsizliyi fənnini tədris edən müəllimlər tərəfindən mənbə kimi istifadə oluna bilər.

Açar sözlər: *informasiya təhlükəsizliyi mədəniyyəti, informasiya-psixoloji təhlükəsizlik, informasiyanın qorunması, informasiya etikası.*

Giriş

Hazırda informasiya cəmiyyətin dayanıqlı inkişafı və təhlükəsizliyi üçün həlledici əhəmiyyət daşıyır. Müasir reallıqlar baxımından informasiya strateji resursdur, əmtəə-pul münasibətlərinin obyektidir, iqtisadi, siyasi, fərdlərarası üstünlük qazanmaq vasitəsidir. Artıq elmdə, təhsildə, idarəetmədə və digər sahələrdə qabaqcıl yeniliklər, əhəmiyyətli hadisələr informasiya və bilik istehsalı ilə bağlıdır.

İnsan fəaliyyətinin bütün sferalarının informasiyalaşdırılmasının, informasiya proseslərinin sosial, ictimai-siyasi, hüquqi, iqtisadi və s. münasibətləri əhatə etməsinin şahidi oluruq. Digər tərəfdən, yeni texnologiyalardan və informasiyadan insanların düşüncəsini, davranışını manipulyasiya etmək, onların mənəvi-psixoloji sağlamlığına zərər vurmaq üçün də istifadə edilir, kibercinayətkarlıq, kiberterrorizm, informasiya müharibəsi təhlükələri artır.

Cəmiyyətin bütün sferalarının get-gedə informasiyadan daha çox asılı olduğu bir şəraitdə İKT-nin etibarlılığı, informasiya cəmiyyəti üzvlərinin istifadə etdiyi informasiyanın keyfiyyəti, sirlərin qorunması birinci dərəcəli əhəmiyyət kəsb edir. İnsanlara aid məlumatların toplandığı və emal olunduğu sistemlərdə bu informasiyanın tamlığı və konfidensiallığı qorunmalıdır, eyni zamanda insanlar onlara təqdim edilən müxtəlif növ xidmətlərin etibarlılığına əmin olmalıdırlar. Əks halda bu istiqamətdə görülən işlərin səmərəsi olmaz. Göründüyü kimi informasiya cəmiyyətinin inkişafı, qlobal informasiyalaşdırma fərdin, cəmiyyətin və dövlətin inkişafı üçün geniş imkanlar açmaqla bərabər bir sıra problemlər də yaradır ki, onlardan biri də informasiya təhlükəsizliyi problemidir.

Tədqiqatlar göstərir ki, informasiya təhlükəsizliyi problemləri çoxaspektlidir və onların həlli kompleks yanaşma tələb edir. İnformasiya təhlükəsizliyi problemlərini çox vaxt iki hissəyə ayırırlar: texnoloji problemlər və humanitar problemlər. Bu problemlərin texnoloji aspekti daha çox öyrənilib, humanitar aspekti isə kifayət qədər araşdırılmayıb. Təhsil sistemində də informasiya təhlükəsizliyinin, xüsusən də onun humanitar aspektinin öyrənilməsi lazımi səviyyədə deyil.

Müasir dövrdə İKT-nin rolunun artması, İnternetin geniş yayılması və getdikcə daha çox əlçatan olması, yüksək məhsuldarlıqlı fərdi kompüterlərin, naqilsiz və mobil qurğuların geniş istifadəsi dövlət tərəfindən vətəndaşlara və təşkilatlara göstərilən xidmətlərin təqdim edilməsində, biznesin idarə edilməsində yeni üsulların meydana çıxmasına, insanlar arasında yeni ünsiyyət vasitələrinin yaranmasına səbəb oldu. Bunun nəticəsində təbii ki, müxtəlif növ informasiya göndərilir və əldə olunur ki, onların konfidensiallığının qorunması məsələsi böyük əhəmiyyət kəsb edir. İnformasiya sistemlərinin, şəbəkələrin, elektron xidmətlərin istifadəçiləri onların etibarlılığından və qorunmasından asılı olmağa başlayırlar. Belə şəraitdə fərdin, cəmiyyətin və dövlətin informasiya təhlükəsizliyinin təmin edilməsi informasiya mədəniyyətinin və onun tərkib hissəsi olan informasiya təhlükəsizliyi mədəniyyətinin səviyyəsi ilə müəyyən edilir.

Fərdin və cəmiyyətin informasiya təhlükəsizliyi problemləri

"İnformasiya təhlükəsizliyi" fenomeni təqiqatçılar tərəfindən müxtəlif aspektlərdən: texniki, hüquqi, fəlsəfi, psixoloji, sosial və s. araşdırılır. Alimlər bu fenomenə təmsil etdikləri elm sahəsi nöqteyi-nəzərindən yanaşaraq "informasiya təhlükəsizliyi" anlayışını özlərinə məxsus məzmunla ifadə edirlər ki, bu da müxtəlif terminlərin meydana çıxmasına səbəb olmuşdur. Dar mənada informasiya təhlükəsizliyi: informasiyanın icazəsi olmayan şəxslər tərəfindən edilən dəyişikliklərdən mühafizə edilməsini, dəyərli məlumatların qorunmasını, kompüterin işinin etibarlılığının və elektron şəbəkədə yazışmaların gizliliyinin təmin edilməsini nəzərdə tutur.

İnformasiya təhlükəsizliyi problemlərinin iki: texnoloji və humanitar aspektdən izahına daha çox rast gəlinir. Texnoloji yanaşma çərçivəsində verilən tərifl ərdə əsas diqqət birmənalı şəkildə informasiyanın və informasiya infrastukturunun (informasiyanın saxlanılması üçün aparat və proqram təminatı, texniki vasitələr, təşkilati struktur) qorunması problemi üzərində cəmləşir. Bu yanaşma informasiya təhlükəsizliyinin vacib tərəflərindən yalnız birini izah edir. İnformasiya məhsuldur və buna görə də onu qorumaq tələb olunur.

İnformasiya təhlükəsizliyinin humanitar aspekti isə ondan ibarətdir ki, informasiya cəmiyyətinin bütün sistem və texnologiyalarının, informasiya resurslarının yaradıcısı məhz insan özüdür. Ona görə də onların keyfiyyəti və təhlükəsiz istifadəsi insanın özünün keyfiyyəti ilə müəyyən olunur. Burada yalnız bu sistem və vasitələrin işinin səmərəliliyindən və etibarlılığından deyil, onların insana, cəmiyyətə və ətraf mühitə təsirindən söhbət gedir.

Diqqət çəkən əsas məqamlardan biri də ondan ibarətdir ki, burada insan yalnız kənar informasiya təhlükələrindən mühafizə obyekti kimi deyil, eyni zamanda özü ətraf mühit üçün bu təhlükələrin əsas mənbəyi kimi çıxış edir. Bundan əlavə, getdikcə artan müxtəlif təyinatlı informasiya sistemlərinin təhlükəsiz fəaliyyəti üçün əsas risk faktoru da insan hesab olunur [1].

İnformasiya təhlükəsizliyinə humanitar yanaşma: informasiya təhlükəsizliyinin təmin edilməsinin metodoloji əsaslarının işlənib hazırlanması; informasiya təhlükəsizliyinin fənlərarası elmi bilik sahəsinə çevrilməsi; bu sahədə hüquqi tənzimlənmənin inkişaf etdirilməsi; fərdi və kütləvi şüurun təhlükəsizliyinin təmin edilməsi; müasir cəmiyyətdə baş verən sosial proseslərdə informasiya təhlükəsizliyinin yeri və rolunun araşdırılması kimi məsələləri əhatə edir.

Məlum olduğu kimi fərd (onun hüquq və azadlıqları) və cəmiyyət (onun maddi və mənəvi dəyərləri) informasiya təhlükəsizliyinin əsas obyektlərindəndir. Fərdin və cəmiyyətin informasiya təhlükəsizliyi probleminə iki aspektdən yanaşırlar:

- İnformasiyanın qorunması – informasiyanın icazəsiz istifadəsinin, oğurlanmasının, saxtalaşdırılmasının qarşısının alınması;

- İnformasiya təsirlərindən qorunma – müxtəlif növ imtiyazlar uğrunda mübarizələrdə bir vasitə kimi istifadə edilən və vətəndaşların psixi və fiziki sağlamlığına ziyan vura biləcək informasiyadan qorunmaq.

Fərdin informasiya təhlükəsizliyi cəmiyyətdə olan mənəvi, sosial və hüquqi şəraitdən, eyni zamanda fərdin şəxsi keyfiyyətlərindən asılıdır. İnsanı əhatə edən informasiya məkanı insanın şəxsiyyət kimi formalaşmasına və fəaliyyət göstərməsinə, onun mənəvi, intellektual və psixi inkişafına, sağlamlıq vəziyyətinə təsir edir. Eyni zamanda, bir sıra xoşagəlməz faktorları göstərmək olar ki, onlar informasiya məkanında fərdlərin, cəmiyyətin və dövlətin bir sıra həyati vacib maraqlarının qorunma vəziyyəti üçün təhdidlərin meydana çıxmasına səbəb olur. Əsas faktorlardan biri informasiyanın həddən artıq artması ilə meydana çıxan və "informasiya partlayışı" adlandırılan problemdir. İnformasiyanın sürətlə artması nəticəsində yaranan informasiya bolluğu insanın, hətta öz professional fəaliyyətində qərarların qəbul edilməsi üçün vacib olan informasiyanı qəbul etmək, dərk etmək, sistemləşdirmək imkanlarına mənfi təsir edir [2].

Müasir insanın psixikasına mənfi təsir edən faktorlardan biri də informasiya məkanının çirklənməsidir. Tədqiqatçıların fikrincə, böyük həcmdə keyfiyyətsiz informasiyanın olması və insanın bu informasiyanı səmərəli emal edərək intellektual məhsula, biliyə çevirmək qabiliyyətinin aşağı səviyyədə olması informasiya stressinin meydana çıxmasına səbəb olur [1, 2].

Fərdi və kütləvi şüurun manipulyasiyası. İnformasiya təhlükəsizliyin pozulmasına təsir edən digər neqativ faktor isə, fərdi və kütləvi şüura informasiya-psixoloji təsir, manipulyasiya, insanların davranışının idarə edilməsi üsullarının geniş yayılmasıdır. Tədqiqatçılar manipulyativ texnologiyalardan istfadəni bir neçə səviyyəyə bölürlər. Birincisi, dövlətlərarası siyasətin reallaşdırılması gedişində həyata keçirilən təşkil edilmiş təsir və psixoloji əməliyyatlardır. Manipulyativ xarakterli informasiya-psixoloji təsirin ikinci səviyyəsinə daxili siyasi mübarizə, iqtisadi rəqabətdə və s. müxtəlif vasitə və texnologiyalardan istifadə aid edilir. Üçüncüsü isə, şəxsi münasibətlər prosesində insanların bir-birini manipulyasiya etməsidir.

Ziyanlı məzmun. Hazırda İnternet vasitəsilə dini ekstremizmin, sektantlığın təbliği, mistik və ezoterik bilik və təcrübənin, magiya və şamançılığın yayılması təhlükəli həddə çatıb. Bu isə sosial və şəxsi dezadaptasiya, bəzi hallarda isə insanın psixikasının pozulması ilə nəticələnir. İnternet vasitəsilə ədəbsiz və əxlaq normalarına zidd informasiyanın yayılması, zərərli adətlərin (siqaretin, narkomaniyanın və s.) təbliğ edilməsi, millətçilik ideyalarının yayılması olduqca təhlükəlidir. Uzun müddət davam edən belə təsir cəmiyyətdə neqativ mənəvi-psixoloji atmosfer formalaşdırır, kriminal mühitə şərait yaradır, psixi xəstəliklərin artmasına səbəb olur [3].

Bu tip informasiyaların mənfi təsirinə ən çox məruz qalan isə uşaq və yeniyetmələrdir. Şüur səviyyəsi və dünyagörüşü yetərincə formalaşmadığı üçün belə informasiyalar onların mənəvi-psixoloji sağlamlığına mənfi təsir edir. KİV, xüsusən də televiziya gənc və yeniyetmələrdə mənəvi dəyərlərin formalaşmasına çox güclü təsir göstərir. Televiziya ekranlarında başqa xalqlara xas mədəniyyəti, həyat tərzini təbliğ edən filmlərin nümayişi nəticəsində gənclərin qərbdəki həyat standartlarına yönlənməsi müşahidə olunur. Belə təsirlər bir çox hallarda mənəviyyat, vətənpərvərlik, milli dəyərlərə hörmət kimi hisslərin arxa plana keçməsinə səbəb olur.

İnsanların elektron poçt və mobil telefon vasitəsilə aldığı çoxlu sayda reklam xarakterli məlumatlar da insanlara neqativ təsir göstərir. Belə məlumatlar insanın vaxtını almaqla yanaşı onların bəzən lazımsız əşya və xidmətlərə pul xərcləməsinə səbəb olur. Nəticədə aqressiya və qəzəb kimi mənfi emosiyalar yaranır ki, bu da insan orqanizminə fiziki ziyan vurur. Televiziya ekranlarından insanların üzərinə sel kimi axıb gələn reklamlar da şüura icazəsiz müdaxilə kimi qiymətləndirilir.

Kiberxəstəliklər. İnformasiyanın insana təsirinin mənfi nəticələrindən biri də kiberxəstəliklərdir. Onlara insanların kompüter oyunlarından, televiziyadan və İnternetdən psixoloji asılılığını misal göstərmək olar. Hazırda gənclərin kompüter oyunlarına aludəçiliyi olduqca narahatlıq doğurur. Bu oyunların çoxu aqressivliyi, qəddarlığı və zorakılığı təbliğ edir.

Onlayn oyunlarda fəal iştirak virtual dünyadan və oyunlardan asılılığa, psixi pozuntulara və nəticədə depressiya və fiziki tükənməyə, hətta cinayət törətməyə gətirib çıxarır [4].

Yaranan informasiya bolluğu nəticəsində insanlar informasiya ilə həddindən çox yüklənir ki, bu da onlarda stress vəziyyətinin yaranmasına gətirib çıxarır. Belə bir vəziyyətdə isə insan təfəkküründə "informasiya yorğunluğu sindromu" adlanan pozğunluq və xəstəlik yaranır. Virtual məkanın təsiri nəticəsində yaranan xəstəliklərdən biri də İnternet istifadəçiləri, xüsusən də, zəif xarakterli insanlar arasında rast gəlinən eskapizm (real həyatdakı problemlərdən və çətinliklərdən qaçaraq xəyallara qapılmaq) meyilləridir [3]. Bu zaman insan real gerçəkliklə virtual məkan arasında qalır.

Bundan əlavə, mobil telefon, kompüter və İnternetdən hədsiz istifadə fantom zəng sindromu (eşitmə halüsinasiyası, telefon zəng çalmadığı halda tez-tez telefonun səsini və ya vibrasiyasını eşitmək), nomofobiya ("no mobile fobia", mobil telefon olmadıqda narahatlıq keçirmək, panikaya düşmək), "rəqəmsal dəniz xəstəliyi" (telefondan istifadədən sonra baş gicəllənməsi və "yırğalanma"), "Google" effekti (istənilən məlumatı Google-dan tapmaq mümkün olduğu üçün heç bir biliyin onlara lazım olmadığını düşünmək), kiberxondriya (İnternetdən oxuduğu xəstəliklərin ümumi simptomlarını özünə aid edərək əsassız olaraq sağlamlığı ilə bağlı narahatlığını böyütmək) və s. kimi yeni kiberxəstəliklərin yaranmasına təkan vermişdir. Bu cür xəstəliklər insanlarda qorxu, əsəb, stress kimi mənfi hisslərə, psixi pozuntulara, bəzi hallarda digər ağır xəstəliklərə səbəb ola bilir [4, 5].

Fərdi məlumatların qorunması. Şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumat (adı, soyadı, doğulduğu tarix, anadan olduğu yer, ailə vəziyyəti, ixtisası, iş yeri, gəlirləri və s.) fərdi məlumatlar hesab olunur. Hazırda dövlət və özəl müəssisələr tərəfindən yaradılan müxtəlif informasiya sistemlərində insanların fərdi məlumatları toplanır və saxlanılır ki, bu da həmin məlumatların bədniyyətli insanların əlinə keçməsi təhlükəsini yaradır. Fərdi məlumatların oğurlanması sahibini maddi və mənəvi təhlükəyə məruz qoya bilər. Məsələn, kifayət qədər texniki biliklərə malik olan cinayətkarlar bank kartlarının rekvizitlərini əldə edərək oradakı vəsaiti mənimsəyə bilərlər. Yaxud, telefon nömrələri və elektron poçt ünvanları reklam məqsədi ilə spam-göndərişlərin təşkili və s. üçün istifadə oluna bilər [6].

Çox vaxt isə fərdi məlumatların başqalarının əlinə keçməsinə insanların özləri şərait yaradırlar. Belə ki, müxtəlif sosial şəbəkələrdə və virtual cəmiyyətlərdə qeydiyyatdan keçən insanlar özlərinin bir sıra fərdi məlumatlarını burada yerləşdirirlər, lakin heç kim bilmir ki, bu fərdi məlumatlar müəyyən məqsədlər üçün toplanılır, analiz edilir və istifadə edilir. Eyni zamanda, gündən-günə artan müxtəlif proqram və əlavələri öz kompüterinə, telefonuna yükləyərkən hər kəs istifadəçi razılaşmalarını imzalamaqla öz fərdi məlumatlarını istifadə etməyə razılıq verir. Beləliklə də, fərdi məlumatlarını açır və konfidensiallıq hüququnu məhdudlaşdırır.

Kibercinayətlər. Kibercinayət hər hansı bir informasiya sisteminə icazəsiz və hüquqa zidd şəkildə daxil olunması vasitəsi ilə həyata keçirilən əməldir. Bu halda ixtiyari bir insan, ona məxsus əmlak, yaxud istifadə olunan sistemin özü hədəf seçilə bilir. Məsələn, bir sistemə daxil olmaqla zərər vermək, bazanı, onun ehtiyat surətini silmək, şifrələmək, ələ keçirmək, başqa informasiya əlavə etmək, sistemin iş prinsipini pozmaq, şəxsi həyatın toxunulmazlığını pozmaq, əlaqəni əngəlləmək, əlaqəni icazəsiz izləmək, qeydə almaq kimi hərəkət və əməllərin törədilməsi kibercinayət faktlarıdır. Kibercinayətləri törədilməsi məqsədinə görə müxtəlif növlərə ayırırlar:iqtisadi, siyasi, ideoloji və sosial-psixoloji [7]. İqtisadi kibercinayətlərə daha çox rast gəlinir. Bunlara kompüter şəbəkələrinin və ya proqramların köməyi ilə vəsaitin və konfidensial informasiyanın oğurlanması yolu ilə vətəndaşlara, bank sistemlərinə, şirkətlərə və s. iqtisadi ziyan vurulması aiddir. İkincisi siyasi məqsədlə – siyasi və dövlət institutlarına ziyan vurmaq, əhalinin dövlətə inamını zəiflətmək məqsədi ilə törədilən kibercinayətlərdir. İdeoloji kibercinayətlərə müxtəlif ideya və fikirlərin təbliğ edilməsi yolu ilə vətəndaşların terrorist və ya digər cinayətkar qruplaşmalara cəlb edilməsi aid edilir. Sosial-psixoloji kibercinayətlər isə vətəndaşlara mənəvi və psixoloji zərər verilməsi məqsədi ilə törədilən cinayətlərdir.

Hazırda sadə vətəndaşdan tutmuş dövlət orqanına qədər hər kəs virtual mühitdə cinayətin qurbanına çevrilə bilər. İnternet və rəqəmsal texnologiyalar sahəsində geniş biliklərə malik olmadan kibercinayətlərin həyata keçirilməsi mümkün deyil. Bu cinayətkarlar informasiya texnologiyaları sahəsində xüsusi biliklərə malik olan şəxslərdir, onlar bu biliklərdən istifadə edərək bank hesablarına, fərdi məlumat bazalarına, böyük informasiya sistemlərinə icazəsiz giriş imkanı əldə edirlər.

İnformasiya müharibələri. XX əsrin ikinci yarısından etibarən həyata keçirilən hərbi əməliyyatlar zamanı informasiya müharibəsi texnologiyaları daha aktiv şəkildə və uğurla tətbiq edilməkdədir. Bu da İKT-nin inkişafı və yaratdığı yeni imkanlar hesabına baş verir. Hərbi əməliyyatlarla paralel şəkildə aparılan informasiya müharibəsinin əsas hədəflərindən biri qarşı tərəfin ordusu və ya bötövlükdə əhalisi arasında təxribat xarakterli dezinformasiya yaymaq, onları çaşqın, ümidsiz vəziyyətə salmaq, döyüş ruhunu sarsıtmaqdır [8]. Sürətlə inkişaf edən İKT bu cür psixoloji təsirlərin həyata keçirilməsi üçün böyük imkanlar yaradır. Bu baxımdan, informasiya təhlükəsizliyinin əsas vəzifələrindən biri informasiya müharibəsinə qarşı hazırlıqlı olmaq və real təhlükələr baş verdikdə onların qarşısını almaq üçün adekvat tədbirlərin görülməsidir.

İnformasiya təhlükəsizliyi mədəniyyətinin mahiyyəti

"İnformasiya təhlükəsizliyi mədəniyyəti" anlayışının mahiyyətini açmaq üçün "informasiya", "təhlükəsizlik", "informasiya təhlükəsizliyi" və "mədəniyyət" anlayışlarına və onların qarşılıqlı əlaqələrinə baxmaq lazımdır.

İnformasiya təhlükəsizliyi mədəniyyəti anlayışı geniş və çoxtərəfli bir anlayışdır. Ümumiyyətlə informasiya təhlükəsizliyi problemləri müxtəlif elm sahələrini təmsil edən tədqiqatçılar tərəfindən araşdırılır ki, bu da öz növbəsində müxtəlif yanaşmaların meydana çıxmasına səbəb olmuşdur.

İnformasiya təhlükəsizliyi mədəniyyətinin mahiyyəti ilə bağlı yanaşmalarda texnoloji yanaşma üstünlük təşkil edir. Son dövrlərə qədər informasiya təhlükəsizliyi problemlərinin həlli zamanı texniki və texnoloji üsul və vasitələrin işlənib hazırlanmasına daha çox diqqət ayrılırdı. Ona görə də əksər müəlliflər informasiya təhlükəsizliyi mədəniyyətini texnoloji aspektdən izah edirlər. Fərqli yanaşmalar da mövcuddur. Məsələn, mənbələrdən birində şəxsiyyətin informasiya təhlükəsizliyi mədəniyyəti insanın, özünün informasiya sferasındakı hüquq və azadlıqlarını (dövlət informasiya resurslarına çıxış texnologiyalarını bilməsi, özünün şəxsi sirrini və intellektual mülkiyyətini qoruyub saxlaya bilməsi) bilməsi və onları reallaşdırmağa qadir olması, sağlamlığı üçün təhlükəli olan neqativ informasiya təsirlərini ayırd edə bilməsi və onlardan qorunma texnologiyalarını bilməsi kimi izah olunur [3].

Digər bir mənbədə isə, informasiya təhlükəsizliyi informasiya-texniki və informasiya-ideoloji təhlükəsizliyin məcmusu kimi nəzərdən keçirilir. Bu yanaşmaları ümumiləşdirərək demək olar ki, informasiya 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. Yəni, informasiya təhlükəsizliyi mədəniyyətinin strukturuna informasiya təhlükəszliyi sahəsində texnoloji mədəniyyət, informasiya-psixoloji mədəniyyət, eləcə də hüquqi-etik mədəniyyətin komponentləri daxildir. Bu gün informasiya təhlükəsizliyi fərdin, cəmiyyətin və dövlətin yalnız maddi, iqtisadi, texnoloji və s. maraqlarının deyil, sosial-mənəvi, əxlaqi və digər qeyri-maddi dəyərlərinin də qorunmasını ifadə edir.

İnformasiya təhlükəsizliyi mədəniyyətinin texnoloji aspektləri

Artıq kompüterlər, İnternet həyatımızın bir hissəsinə çevrilmişdir. Kompüterdə saxlanılan informasiyanın qorunması üçün texniki, təşkilati və s. tədbirlər görülsə də, insan faktoru burada böyük rol oynayır. Kompüterdən, kompüter proqramlarından düzgün istifadə edilməməsi, onların

imkanları barədə yetərincə məlumatlı olmamaq informasiyanın tamlığının pozulmasına, silinməsinə, dəyişdirilməsinə səbəb ola bilir. Müxtəlif tipli (mətn, cədvəl,şəkil və s.) məlumatlar üzərində işləyərkən istifadəçi tərəfindən informasiyanın son variantının yadda saxlanılmaması, redaktə əməliyyatlarından istifadə zamanı buraxılan səhvlər və digər bu kimi hallar informasiya təhlükəsizliyini pozur.

İnformasiya sistemləri ilə işləyən əməkdaş tərəfindən parolun bilərəkdən kiməsə verilməsi və ya ehtiyatsızlıqdan başqasının əlinə keçməsi burada toplanmış məlumatların oğurlanmasına, cinayətkarların əlinə keçməsinə şərait yaradır.

Eləcə də informasiyanın ötürülməsi, virtual ünsiyyət, internet üzərindən alış-veriş və digər xidmətlərdən istifadə zamanı texniki bilik və bacarıqların yetərincə olmaması informasiya təhlükəsizliyi üçün təhdidlər yaradır.

Antivirus proqramlarından istifadə edilməməsi, mənbəyinə fikir vermədən müxtəlif proqram və əlavələrin kompüterə, smartfona yüklənməsi buradakı məlumatları təhlükə altında qoyur. Ekspertlərin fikrincə "implant proqramlar" adlanan yeni tip ziyanlı proqram təminatları xakerlərə mobil telefonları tam nəzarətdə saxlamağa: telefon sahibinin bu və ya digər anda olduğu yer, batareyanın dolma səviyyəsi, SİM kartın dəyişdirilməsi faktı, istifadəçinin fəaliyyətini yazmaq üçün mikrofon və kameranın işə salınması imkanı, Wi-Fi şəbəkəsinə çıxış nöqtələrinin yadda saxlanılması və s. də daxil olmaqla bütün informasiyaya çıxış əldə etməyə imkan verir [8].

Müasir tələblər nəzərə alınmaqla, elektron informasiya ilə işləyən hər kəs: əməliyyat sistemlərindən və ofis proqram paketlərindən istifadə etməklə elektron sənədlərin və onların ayrı-ayrı fraqmentlərinin təsadüfi və ya məqsədli dəyişikliklərdən qorunması; elektron sənədlərin qorunması üçün rəqəmsal imza və sertifikatlardan istifadə edilməsi; sənədlərin arxivləşdirilməsi və ehtiyat nüsxəsinin çıxarılması; antivirus proqramlarından istifadə (kompüter viruslarının yoxlanılıb tapılması, onların zərərsizləşdirilməsi və silinməsi, antivirus bazasının yenilənməsi); lokal şəbəkədə və internetdə informasiyanın qorunması və s. kimi bilik və bacarıqlara malik olmalıdır.

Kompüterdən istifadə edən istifadəçilər üçün tələblər, fərdi məlumatların qorunması ilə bağlı tövsiyələr barədə məlumatlılıq və onlara əməl edilməsi informasiya təhlükəsizliyinin təmin edilməsinin ilkin şərtlərindən biri hesab edilə bilər.

İnformasiya məkanında təhlükəsiz davranmaq üçün texnoloji mədəniyyət böyük əhəmiyyət daşıyır. Hazırda informasiyanın toplanması, emalı və ötürülməsi proseslərinin kompüter, İnternet və digər texniki qurğulardan istifadə edərək həyata keçirilməsi konfidensial informasiyanın başqalarının əlinə keçməsi təhlükəsini artırır [3].

Ona görə də informasiya sistemləri ilə işləyən mütəxəssislərlə yanaşı istifadəçilərin də informasiya təhlükəsizliyi sahəsində texniki bilik və bacarıqları (virusların törətdiyi fəsadlar və onlardan qorunma üsulları, təhlükəsizlik parollarından istifadə və s.) lazımi səviyyədə olmalıdır ki, təhlükəsizliklə bağlı problemləri aradan qaldıra bilsinlər.

İnformasiya təhlükəsizliyinin informasiya-psixoloji aspekti

Cəmiyyətdə informasiyalaşdırma proseslərinin sürətlənməsi ilə informasiya mühitinin insanların psixikasına, onların cəmiyyətdə və şəxsi həyatdakı davranışına, milli-mənəvi və dini dəyərlərə münasibətinə təsiri daha çox hiss olunmağa başladı. Ona görə də XXI əsrin əvvəllərindən etibarən informasiya-psixoloji təhlükəsizlik yeni qlobal problem kimi dərk edilməyə başladı. İnformasiya-psixoloji təhlükəsizlik deyəndə şəxsiyyətin, qrupun və ya əhalinin informasiya-psixoloji təsirlərdən qorunması vəziyyəti nəzərdə tutulur [4]. İnformasiya-psixoloji təhlükəsizliyə ictimai rəyin manipulyasiyası, reklam və virtual oyunlarla təsir, neqativ məzmunlu məlumatların təsiri aid edilir. Tədqiqatçılar qeyd edir ki, şüurun manipulyasiyası insanın yalnız sosial davranışına deyil, onun sağlamlığına da çox ciddi təsir göstərir. Məsələn, televiziya ekranlarından davamlı olaraq neqativ məzmunlu informasiyanı (zorakılıq, qəddarlıq, dağıdıcılıq və s.) qəbul etmək insanların psixikasını deformasiyaya uğradır, onları aqressivləşdirir. Eyni zamanda

requlyar, neqativ psixoloji təsir insan orqanizminin müqavimətini zəiflədir və immun sisteminə zərər vurur. Xüsusi informasiya texnologiyalarının köməyi ilə ictimai rəyin manipulyasiyası bu gün siyasi mübarizədə yüksək səmərəli vasitə hesab olunduğu üçün müxtəlif ölkələrdə geniş istifadə edilir ki, bu da yalnız şəxsiyyət üçün deyil, cəmiyyət və dövlət üçün də təhlükə törədir [1].

Müasir informasiya texnologiyaları və vasitələri insanların informasiya əlaqəsini, ictimai şüuru idarə etməyə və onlara nəzarət etməyə imkan verir. Məsələn, bütün telefon danışıqlarına qulaq asmaq, yazışmalara nəzarət etmək, fərdlər haqqında konfidensial məlumatlar bazası yaratmaq və ondan qanuna zidd şəkildə istifadə etmək, insanların psixikasına gizli informasiya təsirlərini həyata keçirmək üçün potensial imkanlar var. Bu gün informasiya ayrı-ayrı şəxslərin, qrupların və ya təşkilatların özlərinin şəxsi maraqları üçün aşkar və gizli məqsədlərlə fərdi və sosial subyektlərin fəaliyyətinə ziyan vurmaq üçün həyata keçirdikləri psixoloji təzyiq vasitəsidir. Nəzərə alsaq ki, informasiya psixoemosional və sosial gərginliyin yaranmasına, mənəvi norma və kriteriyaların təhrif olunmasına, sosial stereotiplərin və davranışların qeyri-adekvatlığına, yanlış dəyərlərə və istiqamətlərə, eləcə də digər arzuolunmaz psixoloji nəticələrə gətirib çıxara bilər, o zaman insanların informasiya immunitetini artırmaq məsələsi gündəmə gəlir. İnformasiya immunitetinin zəif olması, informasiya mənbələrinin hamısına eyni dərəcədə etibar etmək, uzun müddət informasiyanın mənfi təsirlərinə məruz qalmaq insanların psixi sağlamlığını təhlükə altında qoyur.

İnformasiya məkanında dövr edən müxtəlif məzmunlu informasiya axınlarının insanın psixikasına neqativ təsiri müasir cəmiyyətdə insanın psixoloji təhlükəsizliyinin təmin edilməsini zəruri edir. İnsanların şəxsi və professional tələbatlarını ödəmək üçün həyata keçirdikləri informasiya prosesləri zamanı məruz qaldıqları təhlükələr onların mənəvi-psixoloji sağlamlığına zərər vurmaqla bərabər, ölkənin milli təhlükəsizliyini də təhlükə altında qoya bilər. Şüurun manipulyasiyası, fərqli mənəvi dəyərlərin təbliğ edilməsi, informasiya müharibələri və bu kimi informasiya təhlükələri əslində millətin varlığının əsas dayaqlarından olan milli-mənəvi dəyərlər sisteminin dağıdılmasına yönəlir.Vətəndaşlar bu tip təhlükələr, onların mənbələri, növləri, törədə biləcəyi fəsadlar barədə məlumatlı olmalı, bu təhlükələrdən qorunma üsulları haqqında bilik və bacarıqlara malik olmalıdırlar ki, öz təhlükəsizliklərini təmin edə bilsinlər [3].

İnformasiya təhlükəsizliyi mədəniyyətinin hüququ-etik aspekti

İnformasiya məkanına məxsus etik və hüquqi normalar (intellektual mülkiyyət, müəllif hüquqları, piratçılıq, elektron ünsiyyət vasitələrindən istifadə qaydaları və s.) barədə bilik və bacarıqlar informasiya təhlükəsizliyi mədəniyyətinin tərkib hissəsidir. Çünki qəsdən və ya bilməyərəkdən bu normalara əməl edilməməsi başqalarının hüquqlarının pozulması və ya onların sağlamlığına zərər dəyməsi ilə nəticələnə bilər.

İnformasiya cəmiyyətində insanlar öz ölkələrinin vətəndaşı olmaqla, mənsub olduqları dövlətin qanunları qarşısında məsuliyyət daşımaqla, hüquq və vəzifələrini reallaşdırmaqla yanaşı, həm də virtual məkanın vətəndaşına çevrilirlər. Bu yeni dünyada, hələlik hamılıqla qəbul edilən hüquq sistemi formalaşmayıb, eyni zamanda burada informasiya təhlükəsizliyinin hüquqi tənzimlənməsi ilə bağlı problemlər hələ öz həllini tapmayıb. İnformasiya təhlükəsizliyinin hüquqi tənzimlənməsinin əsas vəzifəsi informasiya sahəsində milli maraq obyektlərinə qarşı olan təhdidlərin aradan qaldırılması, təhdidlərdən yaranan itkilərin minimallaşdırılmasına nail olmaqdır [9].

Həm real, həm də virtual məkan təhlükəsiz olmalıdır. Hüquqi dövlətdə və vətəndaş cəmiyyətində təhlükəsizliyin vacib aspektlərindən biri olan informasiya təhlükəsizliyi fərdin və cəmiyyətin hüquqi mədəniyyətinin lazımi səviyyədə inkişafı ilə təmin edilə bilər.

Cəmiyyətin informasiyalaşdırılması prosesinin sürətli inkişafı və onun insanın bütün fəaliyyət sahələrinə tətbiqi yeni növ hüquq pozuntusu hesab olunan informasiya cinayətkarlığına şərait yaradır. Bu tip cinayətlərin ən geniş yayılmış növü vətəndaşların və təşkilatların intellektual mülkiyyət hüquqlarının pozulmasıdır. Buna misal olaraq, informasiya bazarında müxtəlif

informasiya məhsullarının (kompüter proqramları, verilənlər bazaları, məşhur bəstəkarların, ifaçıların, musiqi kollektivlərinin audio və videoyazıları) "pirat" variantının yayılmasını göstərmək olar. "Pirat" informasiya məhsulları bazarı hazırda bütün ölkələrdə olsa da, informasiya qanunvericiliyinin olmadığı və ya zəif olduğu ölkələrdə daha çox inkişaf edib. Bir sıra ölkələrdə "pirat" məhsulların yayılması informasiya cinayəti hesab olunur və bu cür cinayətlərin törədilməsinə görə böyük məbləğdə cərimə, hətta həbs cəzası nəzərdə tutulur.

İntellektual mülkiyyət hüquqlarının pozulması halları elm sahəsində də müşahidə olunur. Bu gün ümumi inkişaf naminə elmi informasiyanın əlçatan olması geniş təbliğ olunur, bir sıra elmi kitabxanalar, bazalar, jurnalların saytları tərəfindən alimlərin əsərlərinə azad çıxış imkanı yaradılır. Bundan istifadə edərək bəzi insanlar elmi məqalələri, monoqrafiyaları, kitabları və ya onların bir hissəsini olduğu kimi köçürməklə və ya üzərində müəyyən dəyişiklik etməklə özününküləşdirərək nəşr etdirirlər. Bunlar "plagiatlıq" adlanır.

İnformasiya təhlükəsizliyinin təmin edilməsi problemlərindən biri də fərdin informasiya hüququnun qorunması problemidir. Azərbaycan Respublikasının Konstitusiyasına görə hər kəsin istədiyi informasiyanı qanuni yolla axtarmaq, əldə etmək, ötürmək, hazırlamaq və yaymaq azadlığı vardır [10]. Lakin informasiya azadlığının həyata keçirilməsi digər insanların hüquq və azadlıqlarının pozulmasına səbəb olmamalıdır.

Müəyyən məlumatlar var ki, onlara çıxış qanunla məhdudlaşdırılır. "Məlumat azadlığı haqqında" Azərbaycan Respublikasının Qanununa görə bu məlumatlara dövlət sirri, peşə sirri, kommersiya sirri, istintaq sirri hesab olunan məlumatlar, eləcə də vətəndaşların şəxsi həyatına dair sirrlər (fərdi məlumatlar) aiddir [11]. Ona görə də İnternetdə və ya digər mənbədə informasiya yerləşdirəndə bu qanunun tələbləri nəzərə alınmalıdır. Bu sirlərdən hər hansının yayılması fərdin və dövlətin informasiya təhlükəsizliyi məsələsidir.

İnformasiya təhlükəsizliyinin hüquqi cəhətdən təmin olunması sahəsində vacib məsələlərdən biri də fərdi məlumatların qorunmasıdır. Ümumdünya İnsan Hüquqları Bəyannaməsinin 12-ci maddəsinə görə heç kim şəxsi və ailə həyatına müdaxiləyə, evinin toxunulmazlığına, məktublaşmasının gizliliyinə, şərəf və nüfuzuna özbaşına qəsdə məruz qala bilməz. Hər bir şəxsin belə müdaxilə və qəsddən qanun tərəfindən müdafiə olunmaq hüququ var [12].

İnsanların böyük həvəslə istifadə etdikləri smartfonlar fərdi məlumatların və sirr hesab olunan digər məlumatların qeyri-qanuni yayılmasında risk faktoru hesab oluna bilər. Belə ki, smartfonlara yüklənilən əksər proqramlar fərdi məlumatlara giriş hüququ tələb edir. Bu zaman telefonun yaddaşındakı məlumatlar risk altına düşür. Müxtəlif yollarla (reklamlar, spamlar, yükləmələr, yenilənmələr və s.) smartfonlara yeridilmiş casus proqramlar telefonun işinə nəzarət edə bilir. Belə ki, mikrofon, kamera, GPS və s. qurğuları aktiv və ya deaktiv edir, SMS-lərin, zənglərin qeydiyyatını aparır və bədniyyətliləri baş verənlər haqqında məlumatlandırır.

İnformasiya sferasına səmərəli nəzarətin və informasiya təhlükəsizliyinin təmin edilməsinin vacibliyi, baş verən informasiya proseslərinin mürəkkəbliyi fərdin və cəmiyyətin bu sahədə hüquqi mədəniyyət sisteminin formalaşdırılmasını zəruri edir. Bu sistem cəmiyyətin inkişafını dəstəkləyən faydalı informasiya resurslarının yaradılması məqsədi ilə informasiyanın axtarışı və toplanması, emalı, yayılması proseslərini nizamlanması üçün vacibdir.

İnformasiyalaşdırma prosesi faktiki olaraq insanın bütün həyat və fəaliyyət sferalarını əhatə etdiyi üçün hər kəs informasiya təhlükəsizliyi sahəsində aşağıdakı biliklərə malik olmalıdır:

- informasiya prosesləri sferasında təhdidlərin və təhlükələrin növləri və mənbələri haqqında;
- informasiya təhlükəsizliyini təmin edən normativ aktlar haqqında;
- informasiya təhlükəsizliyinin təmin edilməsi sahəsində dövlət siyasətinin əsasları haqqında;
- sülh və müharibə vaxtı, eyni zamanda fövqəladə vəziyyət şəraitində informasiya təhlükəsizliyinin təmin edilməsi metodları və vasitələri haqqında;

İnformasiya təhlükəsizliyinin təmin edilməsində etik normaların əhəmiyyəti olduqca önəmlidir. İnformasiya texnologiyalarının inkişafı və tətbiqi ilə meydana çıxan mənəvi problemlərin öyrənilməsinin zəruriliyi yeni elm sahəsi olan informasiya etikasının yaranmasına gətirib çıxarmışdır. İnformasiya etikası – informasiyanın fəlsəfəsi, kompüter etikası, İnternet etikası, kiberetika və s. kimi tədqiqat sahələri ilə sıx bağlıdır.

İnformasiya etikası informasiya təhlükəsizliyi mədəniyyətinin tərkib hissəsi olub, insanın informasiya davranışlarını (yəni, informasiyaya, informasiya mənbələrinə münasibətdə insanın davranışlarını), eyni zamanda virtual mühitdə ünsiyyət münasibətlərini tənzimləyən mənəvi dəyərlər sistemidir.

Mənəvi əxlaqi normalar əsasında özünütənzimləmə informasiya münasibətləri iştirakçılarının antisosial davranışlardan müdafiəsinin ən effektli vasitələrindən biri hesab olunur. Cəmiyyət tərəfindən işlənən mənəvi-əxlaqi normalar perspektivdə yeni hüquq normalarının yaradılması və mövcud hüquq normalarının təkmilləşdirilməsi üçün baza rolunu oynaya bilər [9, 13].

UNESCO-nun 2011-ci ildə keçirilən 36-cı baş konfransında "İnformasiya cəmiyyətində etika kodeksi" qəbul edilmişdir. Həmin sənəddə təsdiq olunur ki, real həyatda olduğu kimi, informasiya məkanında da insanların hüquq və azadlıqları dəyişməz olaraq qalmalıdır. Burada, həmçinin qeyd olunur ki, bütün maraqlı tərəflər İKT-nin zərərli istifadəsinin qarşısını almaq, şəxsi həyatla əlaqəli fərdi məlumatları qorumaq, İnternetdə və digər İKT-də insan hüquqlarının pozulmasının qarşısını almaq üçün qanunvericilik tədbirləri, informasiya mədəniyyəti və media savadlılıq da daxil olmaqla istifadəçilər üçün təlimlərin keçirilməsi, fərdi və birgə tənzimləmə tədbirləri, eləcə də informasiyanın sərbəst və maneəsiz yayılmasını təmin edən texniki həllər də daxil olmaqla kompleks tədbirlər görməlidirlər [14].

İnformasiya münasibətləri iştirakçıları arasında informasiya etikasının formalaşdırılmasında təhsil sisteminin üzərinə mühüm vəzifələr düşür. Tələbələr informasiya təhlükəsizliyinin təmin olunmasının hüquqi, sosial və etik aspektləri barəsində məlumatlı olmalıdırlar.

Nəticə

İKT-nin insanın bütün fəaliyyət sahələrində geniş tətbiqi, informasiyanın cəmiyyətdə rolunun artması nəticəsində informasiya cəmiyyətinin inkişafı, elektron dövlətin yaranması və dövlətin vətəndaşlarla münasibətlərinin onlayn mühitə keçirilməsi prosesləri ilə yanaşı, müasir dövrdə, informasiya təhlükəsizliyi problemləri də artır. İnformasiya təhlükəsizliyinin təmin edilməsi kompleks yanaşma olmadan mümkün deyil. İnformasiya təhlükəsizliyini təmin etmək üçün texnoloji vasitələr təkmilləşdirilsə də, bu istiqamətdə qanunlar, normativ-hüquqi aktlar qəbul olunsa da, insan faktoru nəzərə alınmazsa görülən işlərin səmərəsi yüksək olmaz.

İnsanların informasiya fəaliyyəti artdıqca uyğun olaraq informasiya təhlükələrinin sayı da artacaq. Bu təhlükələrin qarşısının alınması üçün əhalinin məlumatlılıq səviyyəsinin artırılmasına, onların maarifləndirilməsinə yönəlmiş tədbirlərin həyata keçirilməsi, ayrı-ayrı fərdlərin və ümumilikdə cəmiyyətin informasiya təhlükəsizliyi mədəniyyətinin inkişaf etdirilməsi və onun səviyyəsinin qiymətləndirilməsi məsələləri olduqca mühüm əhəmiyyət kəsb edir.

İnformasiya cəmiyyətinin inkişafı bu cəmiyyətin tələblərinə uyğun yaşamağı və fəaliyyət göstərməyi bacaran, innovasiyalara hazır, eyni zamanda, təhlükələrə və risklərə qarşı dayanıqlı, informasiya mədəniyyətinə malik yeni insan tipinin formalaşdırılmasını tələb edir. Belə ki, dövlət tərəfindən informasiya resurslarına çıxış imkanları yaradılsa da, vətəndaşların bu informasiya resurslarından istifadə etmək, eyni zamanda, fərdi məlumatlarını qorumaq üçün texnoloji mədəniyyəti yüksək olmalıdır. İkincisi, insanın informasiya və informasiya məkanı ilə münasibətlərini tənzimləyən hüquqi-normativ aktlar qəbul olunur, amma insanlar da bununla bağlı öz hüquq və vəzifələrini bilməlidirlər. Üçüncüsü isə, informasiyanın mənfi təsirlərini və bu təsirlərdən qorunmaq üsullarını insanlara aşılamaq lazımdır ki, bu da təhsil, üzünütəhsil və maarifləndirmə tədbirləri vasitəsilə həyata keçirilə bilər.

Ədəbiyyat

1. Колин К.К. Гуманитарные аспекты проблемы информационной безопасности // Информатика и её применение, 2016, Т. 10, Вып. 3, с. 111-121.
2. Астахова Л.В. Информационно-психологическая безопасность в регионе: культурологический аспект // Вестник УрФО. Безопасность в информационной сфере, 2011, № 2, с. 40-47.
3. Mahmudova R.Ş. Cəmiyyətdə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması məsələləri haqqında // İnformasiya cəmiyyəti problemləri, 2013, №1(7), s. 32-38.
4. İmamverdiyev Y. N. İnformasiya-psixoloji təhlükəsizliyin təmin edilməsi problemləri / İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, 14 may 2015-ci il, s. 78-81.
5. Велижанцева А.А. Формирование негативных зависимостей в ИКТ-среде у детей и подростков / Информационная безопасность и вопросы профилактики киберэкстремизма среди молодёжи: Материалы внутривузовской конференции, 9-12 октября 2015 г., с. 115-126.
6. Mahmudova R.Ş. Fərdi məlumatların qorunması və informasiya təhlükəsizliyi mədəniyyəti / İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri V respublika konfransı, 29 noyabr 2019-cu il, s. 229-232.
7. Дремлюга. Р.И. Интернет-преступность: моногр., Владивосток: Изд-во Дальневост. унта, 2008, 240 с.
8. Поляков В. П. Аспекты информационной безопасности информационной подготовки в системе высшего профессионального образования // Глобальный научный потенциал, 2012, № 4 (13), с. 39-44.
9. Əliquliyev R. M., İmamverdiyev Y. N., Mahmudov R.Ş. İnformasiya təhlükəsizliyinin multi-dissiplinar elmi-nəzəri problemləri // İnformasiya cəmiyyəti problemləri, 2017, №2, s.32-43.
10. Azərbaycan Respublikasının Konstitusiyası, Bakı, 12 noyabr 1995-ci il, http://www.e-qanun.az/framework/897
11. "Məlumat azadlığı haqqında" Azərbaycan Respublikasının Qanunu, Bakı, 19 iyun 1998-ci il, http://www.e-qanun.az/framework/3420
12. Ümumdünya İnsan Hüquqları Bəyannaməsi, https://www.coe.int/az/web/compass/the-universal-declaration-of-human-rights-full-version-
13. Кононов О.А., Кононова О.В. Социальные и этические аспекты обеспечения информационной безопасности // Проблемы управления, 2009, №1, с.76-79.
14. UNESCO, Code of ethics for the information society, http://www.unesdoc.unesco.org

УДК 004.056:316.7

Махмудова Расмия Ш.
Институт Информационных Технологий НАНА Баку, Азербайджан
rasmahmudova@gmail.com

О некоторых аспектах культуры информационной безопасности личности и общества

В статье исследуются некоторые аспекты культуры информационной безопасности личности и общества. Анализируются технологические и гуманитарные подходы к проблемам информационной безопасности. Изучение культуры информационной безопасности очень актуально, потому что решение таких задач, как защита информации, собранной в информационных системах, в том числе конфиденциальной информации, защита персональных данных, наряду с технологическими методами и инструментами зависит от человеческого фактора. С этой точки зрения исследуются некоторые проблемы, связанные с информационной безопасностью личности и общества (проблемы, вызванные изобилием информации, проблемы информационного «загрязнения», манипулирование

индивидуальным и массовым сознанием, киберпреступность, защита персональных данных, информационные войны, киберболезни и др.). Обоснована роль культуры безопасности. На основе анализа различных подходов проанализированы сущность и составляющие культуры информационной безопасности. Изучаются технологические, информационно-психологические и юридическо-этические аспекты культуры информационной безопасности, вносятся определенные предложения. При выполнении работы использовались методы анализа и синтеза, сравнения, обобщения, системный подход. Полученные в статье результаты могут быть использованы в качестве источника исследователями, занимающимися вопросами информационной безопасности, и преподавателями, ведущими курс информационной безопасности.
Ключевые слова: *культура информационной безопасности, информационно-психологическая безопасность, защита информации, информационная этика.*

Rasmiya Sh. Mahmudova
Institute of Information Technology of ANAS, Baku, Azerbaijan
rasmahmudova@gmail.com

On some aspects of the culture of information security of an individual and society

The article examines some aspects of the information security culture of an individual and society. Technological and humanitarian approaches to information security problems are analyzed. The study of information security culture is very important, because the solution of problems such as the protection of information collected in information systems, including confidential information, the protection of personal data, along with technological methods and tools depends on the human factor. From this point of view, various problems related to information security of individuals and society (problems caused by information abundance, problems of information "pollution", manipulation of individual and mass consciousness, cybercrime, protection of personal data, information wars, cyber diseases, etc.) are investigated. The role of security culture is justified. The essence and components of the culture of information security are analyzed in terms of different approaches. Technological, information-psychological and legal-ethical aspects of information security culture are studied and certain suggestions are presented. Methods for analysis and synthesis, comparison, generalization, systematic approach are used in the implementation of the work. The results obtained in the article can be beneficial for researchers studying information security issues and teachers teaching information security.
Keywords: *culture of information security, information-psychological security, protection of information, information ethics.*