

UOT 004.9

Əliquliyev R.M.¹, İmamverdiyev Y.N.², Mahmudov R.Ş.³

^{1,2,3}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹secretary@iit.ab.az, ²yadigar@lan.ab.az, ³rasimmahmudov@gmail.com

İNFORMASIYA TƏHLÜKƏSİZLİYİNİN MULTİDİSSİPLİNAR ELMİ-NƏZƏRİ PROBLEMLƏRİ

Məqalədə informasiya təhlükəsizliyinin multidissiplinar elmi-nəzəri problemləri araşdırılır. O cümlədən problemin beynəlxalq, siyasi, psixoloji, hüquqi, iqtisadi, mədəni-etik, kadr hazırlığı və uşaqlarla bağlı aspektləri analiz edilir. Həmin sahələr üzrə aktual elmi tədqiqat istiqamətləri müəyyənləşdirilir.

Açar sözlər: informasiya cəmiyyəti, informasiya təhlükəsizliyi, informasiya-psixoloji təhlükəsizlik, informasiya müharibəsi, informasiya təhlükəsizliyi mədəniyyəti, uşaqların informasiya təhlükəsizliyi.

Giriş

Bu gün dünyada informasiya-kommunikasiya texnologiyalarının (İKT), xüsusən, İnternetin təsiri ilə global rəqəmsal mühitin, virtual münasibətlərin formalaşması və inkişafı prosesi gedir. Dövlət idarəçiliyi, iqtisadi fəaliyyət sferaları, elm-təhsil sistemi, informasiya-kommunikasiya mühiti, şəxsi həyatı və məişət sferasını əhatə edən bütün sahələr üzrə münasibətlər ənənəvi mühitdən virtual mühitə transformasiya olunur. Bəşəriyyət tarixi analoqu olmayan yeni situasiya, münasibətlər sistemi ilə üzləşir. Virtual münasibətlərə keçid bəşəriyyətə gətirdiyi üstünlüklərlə yanaşı, bir sıra problemlərə də yol açır. Bu situasiyada yeni təhlükəsizlik üsullarına və vasitələrinə ciddi ehtiyac duyulur.

Üçüncü minilliyin başlanğıcında informasiya təhlükəsizliyi öz əhəmiyyətinə görə milli təhlükəsizlik sistemində önə çıxır. Belə ki, artıq informasiya bəşəriyyətin ən qiymətli resursuna çevrilib və elmdə, təhsildə, idarəetmədə, iqtisadiyyatda, biznesdə, cəmiyyətdə bütün mütərəqqi yeniliklər, əhəmiyyətli hadisələr informasiya və bilik istehsalı ilə bağlıdır. İnformasiya cəmiyyətində insan fəaliyyətinin bütün sferaları informasiya fəzasına daşınır, informasiya prosesləri sosial, siyasi, hüquqi, iqtisadi, psixoloji, kulturoloji və digər münasibətləri də əhatə edir. Bununla yanaşı, informasiya proseslərinin neqativ təsirləri özünü daha qabarıq göstərir, kibercinayətkarlıq, kiberterrorizm, informasiya müharibəsi təhlükələri artır [1].

Qeyd etmək lazımdır ki, informasiya təhlükəsizliyi bəşəriyyət yaranandan bəri həmişə mövcud olub, sadəcə, sivilizasiya inkişaf etdikcə, informasiya inqilabları bir-birlərini əvəzlədikcə informasiya daşıyıcıları və onların imkanları artmağa başlayıb. Kağız üzərində informasiya insanın nəzarətində olurdu, onun iradəsindən asılı idi. Hətta informasiya nəzarətdən çıxdırsa, onun çoxaldılması, yayılması sürəti, təsir dairəsi bu günkü imkanlarla müqayisədə dəfələrlə məhdud idi. Müasir dövrdə informasiya daşıyıcılarının və mənbələrinin rəngarəngliyi, əlyetərliliyi bütün müsbət tərəfləri ilə yanaşı, informasiya təhlükəsizliyi baxımından ciddi təhdidlərə yol açır.

Müvafiq sahədə çalışan alim və mütəxəssislərin yekdil qənaətinə görə, informasiya təhlükəsizliyi sisteminin təşkilində təkcə onun mürəkkəb texniki komponentləri deyil, həm də insan faktoru mütləq nəzərə alınmalıdır [1]. İnformasiya təhlükəsizliyi məsələləri təkcə emal edilən informasiyanın əlyetərliyinin, tamlığının və konfidensiallığının təmin edilməsi ilə bitmir, informasiyanın insana təsirini, informasiya əsasında qərar qəbul edilməsi ilə əlaqəli (humanitar) problemləri də nəzərə almaq tələb olunur.

Beləliklə, çox zaman texnoloji problem kimi təqdim olunan informasiya təhlükəsizliyi sahəsində bir sıra həlli vacib olan humanitar problemlər də meydana çıxır. Lakin mövcud elmi-tədqiqat və praktiki işlərdə çox zaman informasiya təhlükəsizliyinin texniki və texnoloji tərəflərinə

daha çox fikir verilir, problemin humanitar aspektlərinə kifayət qədər diqqət yetirilmir. Bu baxımdan, informasiya təhlükəsizliyinin humanitar problemləri sahəsində multidissiplinar tədqiqatlara çox böyük ehtiyac vardır.

Təqdim olunan işdə informasiya təhlükəsizliyinin aktualıq kəsb edən multidissiplinar elmi-nəzəri problemləri və əsas tədqiqat istiqamətləri müəyyən olunur, informasiya təhlükəsizliyi sisteminin formalaşdırılması ilə bağlı multidissiplinar tövsiyələr təklif edilir.

İnformasiya təhlükəsizliyinin siyasi aspektləri

İnformasiya təhlükəsizliyinin siyasi xarakterli problemləri daxili və xarici siyasi qüvvələrin maraqları naminə həyata keçirilən informasiya müharibələrini, elektron kəşfiyyatı, dövlət sirlərinin yayılmasını, mühüm əhəmiyyət daşıyan hadisələr və proseslər haqqında qeyri-dəqiq informasiyanın və dezinformasiyanın yayılması və s. bu kimi fəaliyyət istiqamətlərini əhatə edir.

Daxili siyasətdə daha çox təhlükə yaradan təhdidlər kimi müxtəlif ictimai-siyasi birliklərin KİV-də ölkənin konstitusiyaya quruluşunu və bütövlüyünü zorla dəyişməyə, sosial, etnik, regional və dini ədavətin qızışdırılmasına yönəlmiş fəaliyyətini və s. göstərmək olar [2].

Daxili siyasət sahəsində informasiya təhlükəsizliyinin təmin edilməsi üçün ölkənin siyasəti, hakimiyyət orqanları, vəzifəli şəxsləri haqqında yayılan dezinformasiyanın qarşısını almaq üçün mexanizmlərin işlənməsi və tətbiqi zəruridir.

Xarici siyasət sahəsində informasiya təhlükəsizliyinin təmin edilməsinin mühüm obyektləri sırasında xarici siyasəti həyata keçirən hakimiyyət orqanlarının, xarici ölkələrdəki və beynəlxalq təşkilatlardakı diplomatik nümayəndəliklərin informasiya resurslarını qeyd etmək olar.

Qeyd etmək lazımdır ki, tarixən xalqlar, ölkələr, dinlər arasında ziddiyyətlərin, münasibətlərin yenidən cücərməsi, alovlanması üçün virtual məkan geniş imkanlar açır. Virtual məkanın konkret sərhədləri yoxdur, burada bütün dövlətlər bir-biri ilə eyni dərəcədə qonşudur. Ona görə də virtual mühitdə informasiya müharibəsini, hücumunu hər yerdən, hər zaman gözləmək olar.

Bu gün global siyasi iddiaları olan güc mərkəzlərinin xüsusi laboratoriyalarında multidissiplinar elmi yanaşma əsasında ayrı-ayrı regionlar, ölkələr üçün etno, milli, dini yönümlü təhlükələr sintez olunur, konfliktlər yaradılır. Bu təhlükələrin sintezi üçün prosesə tarixçilər, sosioloqlar, konfliktoloqlar və digər elmi sahələrin ekspertləri cəlb edilir. Müvafiq laboratoriyalarda hədəf seçilmiş regionlarda və ölkələrdə ziddiyyətləri araşdırıb *domino*, *butterfly*, *snowball* və s. ziyanlı effektlər aşkarlayır, ən güclü informasiya silahlarını sintez edirlər [1].

Bütövlükdə, hesab etmək olar ki, informasiya təhlükəsizliyinin siyasi aspektləri üzrə aşağıdakı istiqamətlərdə elmi-tədqiqatların aparılması aktualıq kəsb edir:

- informasiya cəmiyyətinin formalaşması və inkişafının elmi-nəzəri problemləri;
- global informasiya fəzası, informasiya imperializmi və milli dövlətlərin (informasiya) suverenliyi;
- dövlətlərin milli maraqları və müasir dünyada informasiya qarşıdurmaları;
- informasiya müharibəsi konsepsiyaları və texnologiyaları, informasiya qoşunlarının formalaşdırılması problemləri;
- cəmiyyətin dəyərləri və onlara yönəlmiş müasir informasiya təhdidləri;
- dövlətin informasiya təhlükəsizliyi siyasəti, prioritetləri və strategiyası;
- dövlət orqanları, siyasi hakimiyyət, cəmiyyət və şəxsiyyət kontekstində informasiya təhlükəsizliyi;
- siyasi kommunikasiyaların informasiya təhlükəsizliyi və siyasi etika;
- informasiyaya və informasiya təhlükəsizliyinə ictimai nəzarət, vətəndaş cəmiyyəti mexanizmləri.

İnformasiya-psixoloji təhlükəsizliyin xüsusiyyətləri

İnformasiya-psixoloji təhlükəsizlik dedikdə, şəxsiyyətin, sosial qrupların və insan birliklərinin iradəsinin, arzu və istəklərinin əleyhinə olaraq onların psixi vəziyyətini, psixoloji xüsusiyyətlərini və davranışlarını dəyişə bilən zərərli informasiya təsirlərindən qorunması vəziyyəti başa düşülür.

Bu cür təhlükələr bütöv bir millətin, xalqın mentalitetinə, milli-mənəvi dəyərlərinə qarşı yönəlidir. Bu dəyərlərin dövləti formalaşdıran, möhkəmləndirən əsas amillərdən biri olduğunu nəzərə alsaq, həmin təhlükələrin səviyyəsini və miqyasını daha dərindən dərk etmək olar. Konkret olaraq, Azərbaycan cəmiyyətində qeyd edilən dəyərlərin deqradasiyası ailə institutunun sütunlarını sarsıdır. Ailə institutu isə cəmiyyətin əsas dayaqı, tənzimləyici mexanizmi kimi çıxış edir. Məhz informasiya-psixoloji təsirlər altında bu dəyərlərin aşınması (eroziyası) prosesi gedir. Bunun əvəzinə insanlara aksioloji dəyərlər – milli-mənəvi dəyərlərin, tarixi və müasir nüfuzlu şəxslərin gözdən salınması, dəyərsizləşdirilməsi, ailə institutunun dağıdılması, kosmopolit hisslərin aşılınması, keçmişinə həqarət hissi ilə baxılması və s. aşılır.

İnformasiya-psixoloji təsir digər təsir növləri ilə müqayisədə aşağıdakı bir sıra fərqli xüsusiyyətlərə malikdir:

- ölkəyə daha genişmiqyaslı təsir imkanına malikdir (inkişaf tempini aşağı salmaq, ölkələr, etnoslar və digər insan birlikləri arasında genişmiqyaslı münaqişələr yaratmaq, böyük bir regionda diktə edilən həyat tərzini formalaşdırmaq, idarəetmənin arzuolunan subyektlərə ötürülməsini təmin etmək və s.);
- kiçik maliyyə xərcləri ilə böyük dividendlər qazandıran uzunmüddətli, çoxməqsədli, kompleks, mərhələli informasiya-psixoloji təsir proqramları hazırlamaq mümkündür;
- yüksək gizlilik səviyyəsinə malikdir;
- bu cür təsirlərdən qorunmaq üçün beynəlxalq və milli səviyyələrdə effektiv hüquqi müdafiə mexanizmləri mövcud deyil.

İnformasiya-psixoloji təsirin yuxarıda göstərilən xüsusiyyətləri belə deməyə əsas verir ki, XXI əsrdə ən təhlükəli silah informasiya silahıdır.

Mütəxəssislər vətəndaşların, sosial qrupların və bütövlükdə, əhəlinin informasiya-psixoloji təsirlərə məruz qalmalarının əsas səbəblərini üç qrupa bölürlər [3]:

1. Siyasi amillər (dünyanın müxtəlif regionlarında baş verən köklü dəyişikliklərdən sonra geosiyasi vəziyyətin dəyişməsi, yeni milli maraqların meydana gəlməsi; demokratiya, qanunçuluq və informasiya açıqlığı şəraitində yeni dövlətçiliyin yaranması; əvvəllər mövcud olan komanda-inzibati, siyasi-inzibati sistemlərin dağılması; Qərbi dünyasının dünyagörüşünü, siyasi və mənəvi dəyərlərinin yayılması məqsədi ilə inkişaf etmiş dövlətlərin informasiya ekspansiyası; beynəlxalq əməkdaşlığın güclənməsi; cəmiyyətdə siyasi, hüquqi və informasiya mədəniyyətinin aşağı səviyyədə olması).
2. Sosial-iqtisadi amillər (bazar iqtisadiyyatına keçid dövrünün çətinlikləri; davamlı inflyasiya və əhəlinin həyat səviyyəsinin aşağı düşməsi; işsizliyin artması; əvvəlki sosial strukturun dağılması; cəmiyyətdə təbəqələşmənin dərinləşməsi; cəmiyyətdə etnik münasibətlərdəki gərginliyin artması, cinayətkarlığın, narkomanıyanın, alkoqolizmin, əxlaqsızlığın, ictimai münasibətlərin kriminallaşması; əhəlinin sağlamlıq vəziyyətinin pisləşməsi).
3. Mənəvi amillər (dövlət ideologiyasının böhranı; ictimai norma və dəyərlər sisteminin deformasiyası; fərdi, qrup və kütləvi şüura təsirin yeni formalarının (o cümlədən, media və İnternet texnologiyalarının) meydana gəlməsi; milli və mədəni-tarixi ənənələrin lazımcı qiymətləndirilməməsi və Qərbi kütləvi mədəniyyətinin şablonlarının ictimai şüura təsiri; qeyri-ənənəvi dini konfessiyaların destruktiv təsiri; dövlətin mühüm sosial-mədəni institutlarının (elm, təhsil, mədəniyyət) zəifləməsi).

İnformasiya-psixoloji təhlükəsizlik problemlərinin həlli aşağıdakı istiqamətlərdə elmi tədqiqatların aparılmasını zəruri edir [4]:

- təhdid yaradan informasiya təsirlərinin ilkin tipologiyasının işlənməsi; praktikada qəbul edilmiş və tətbiq edilən meyarlar əsasında bu cür təsirlərin diaqnostikasının sistemləşdirilməsi; şəxsiyyətin, cəmiyyətin və dövlətin informasiya təhdidlərindən psixoloji qorunması üsullarının təsnif edilməsi;
- uşaqların və böyüklərin tərbiyəsi və təhsili üçün müvafiq metodların və təcrübənin korreksiya edilməsi üzrə təkliflərin analizi və işlənməsi; elektron mediada və İnternetdə tətbiq edilən manipulyativ və ezoterik psixopraktik və psixotexniki metodlardan fərdi və qrup şəklində qorunma vasitələrinin işlənməsi;
- informasiya məhsullarının psixoloji ekspertizasının təşkili və keçirilməsi;
- informasiya məhsullarını işləyib hazırlayanlar və onların istifadəçiləri üçün psixoloji konsalting sisteminin yaradılması.

Son illər elektron medianın inkişafı ilə əlaqədar ictimai-siyasi proseslərə, əhalinin psixoloji vəziyyətinə böyük təsir göstərən ictimai rəyin rolu kəskin şəkildə güclənmişdir. Ona görə də ictimai rəyin formalaşması sistemi informasiya-psixoloji təhlükəsizliyin təmin edilməsinin əsas obyektlərindən birinə çevrilməlidir. Bu baxımdan, ictimai şüurun formalaşmasının və pozulmasının xüsusiyyətlərini öyrənmək, informasiya-psixoloji təsir sisteminin psixoloji modellərini, müvafiq təsirlərdən qorunmanın monitoring və metodlarının diaqnostik vasitələrini işləmək lazımdır.

İnformasiya təhlükəsizliyi və qloballaşma

İnternetə qədərki dövrdə sosiallaşma çox uzun müddətdə baş verirdi. Ona görə də sivilizasiyanın inkişaf səviyyəsi aşağı idi. İndi isə sivilizasiyanın inkişafı, çevik sosiallaşma üçün fəvqəladə imkanlar yaranıb və bu proseslər çox sürətlə inkişaf edir, nəticədə, elm, təhsil, texnologiya, mədəniyyət, iqtisadiyyat, hüquq sistemi və s. sahələr ümumiləşir, qloballaşır.

Qloballaşma prosesi milli dövlətçilik formasından qlobal cəmiyyət formasına keçidi şərtləndirir. Qloballaşmanın əsas subyektləri qismində təkcə dövlətlər, transmilli şirkətlər deyil, həm də sırayı insanlar çıxış edir.

Texnosferanın qloballaşması vahid beynəlxalq texnoloji və informasiya məkanının formalaşmasına gətirib çıxarır. Elm, mədəniyyət, təhsil, etika, ideologiya sahələrində baş verən sosial-mədəni qloballaşma mənəvi sferaya unifikasiya və standartlaşmanın yeni dalğasını gətirir.

Qloballaşma prosesləri insan fəaliyyətinin bütün sahələrində yeni perspektivlər açır, eyni zamanda, ciddi təhlükələr üçün də əlverişli zəmin yaradır. Qloballaşmanın informasiya təhlükəsizliyi sahəsində yaratdığı yeni təhdidlərə aşağıdakıları aid etmək olar [5, 6]:

- dövlətlərarası ziddiyyətlər və münaqişələr informasiya məkanına keçirilir, informasiya qarşıdurmaları güclənir, informasiya silahı tətbiq edilir, informasiya müharibələri şiddətlənir;
- qlobal informasiya-kommunikasiya şəbəkələrində baş verən qəzalar, pozuntular nəticəsində infogen tipli fəlakətlər meydana gəlir;
- cinayətkar təşkilatların və şəbəkələrin nəzarət edilməsi çətin olan qlobal informasiya infrastrukturu yaranır;
- qlobal virtual mühitə xas olan yeni cinayətkarlıq növləri meydana gəlir;
- böyük həcmdə fərdi məlumatların qanunsuz, cinayətkar məqsədlərlə toplanması imkanları yaranır;
- ictimai şüurun total manipulyasiyası imkanları yaranır.

Qloballaşma şəraitində informasiya təhlükəsizliyinin təmin olunması problemi beynəlxalq, kompleks və multidistiplinər xarakter alır. Bu problemin həlli isə müvafiq elmi-metodoloji əsasların keyfiyyətindən və ölkələr arasında beynəlxalq əməkdaşlığın səviyyəsindən birbaşa asılıdır.

Beynəlxalq əməkdaşlıq qanunvericilik tədbirləri, kibercinayətkarlıqla mübarizə, insidentlərin cavablandırılması, elmi-tədqiqatlar, aparat və proqram təminatının

sertifikatlaşdırılması kimi sahələri əhatə edə bilər. Lakin bu strateji sahədə xarici ölkələrlə əməkdaşlıqda iqtisadi, siyasi və milli təhlükəsizlik riskləri də mövcuddur.

İnformasiya təhlükəsizliyinin global miqyasda təmin edilməsi problemi ilk dəfə 2002-ci ildə G8 ölkələrinin liderlərinin qəbul etdiyi “Qlobal informasiya cəmiyyətinin Okinava xartiyası”nda qabardılmışdı. Sonrakı mərhələdə informasiya cəmiyyəti məsələləri üzrə Ümumdünya sammitlərinin yekun sənədlərində İKT-nin global, regional və milli səviyyələrdə istifadəsi zamanı təhlükəsizliyin təmin edilməsi üzrə real tədbirlərin görülməsinin zəruriliyi əks olunmuşdur.

Beynəlxalq səviyyədə informasiya təhlükəsizliyinin təmin olunmasında BMT xüsusi rol oynayır. BMT Baş Məclisi informasiya təhlükəsizliyi ilə bağlı 2000-ci ildən başlayaraq beş müxtəlif qətnamə qəbul etmişdir. Həmçinin İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı, Ümumdünya Telekommunikasiya İttifaqı, Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi kimi təşkilatlar da informasiya təhlükəsizliyi ilə bağlı normativ və metodiki sənədlər, tövsiyələr hazırlayırlar [7].

Beynəlxalq səviyyədə informasiya təhlükəsizliyinin təmin edilməsi üçün müvafiq hüquqi əsaslar müəyyən olunmalıdır ki, bunun üçün də dünya ölkələri arasında səmərəli əməkdaşlıq vacibdir.

İnformasiya təhlükəsizliyinin hüquqi problemləri

İnformasiya cəmiyyətində insanlar öz ölkələrinin vətəndaşları olmaqla, mənsub olduqları dövlətin qanunları qarşısında məsuliyyət daşımaqla, hüquqları və vəzifələrini reallaşdırmaqla yanaşı, yeni bir dünyanın – virtual məkanın virtual vətəndaşına da çevrilirlər. Bu yeni dünyada hələlik hamılıqla qəbul edilən hüquq sistemi formalaşmayıb. O cümlədən, virtual mühitdə informasiya təhlükəsizliyinin hüquqi tənzimlənməsi ilə bağlı bir sıra problemlər mövcuddur.

İnformasiya təhlükəsizliyinin hüquqi tənzimlənməsinin əsas vəzifəsi informasiya sahəsində milli maraq obyektlərinə qarşı olan təhdidlərin aradan qaldırılması, təhdidlərdən yaranan itkilərin minimallaşdırılmasına nail olmaqdır.

İnformasiya təhlükəsizliyinin hüquqi təminatının mühüm istiqamətlərindən biri müvafiq elmi tədqiqatların aparılmasıdır. Həmin elmi tədqiqatlar informasiya sahəsində milli maraq obyektlərinin hüquqi xüsusiyyətlərinin, həmin təhdidlərə qarşı effektiv mübarizəni təmin edən hüquqi vasitə və mexanizmlərin, müvafiq predmet sahəsində tənzimləmə prosesini həyata keçirmək üçün hüququn müxtəlif sahələrinin əməkdaşlıq imkanlarının, müvafiq sahədə beynəlxalq təcrübənin, həmçinin müvafiq tənzimlənmə ilə bağlı milli və beynəlxalq qanunvericilik arasındakı münasibətlərin öyrənilməsinə əhatə etməlidir.

Məlum olduğu kimi, informasiya sahəsi üzrə qanunvericiliyin tarixdə analoqu yoxdur. Ona görə də müvafiq qanunvericiliyin işlənməsində hüquqşünaslarla yanaşı, informasiya texnologiyaları mütəxəssisləri, psixoloqlar, sosioloqlar, pedaqoqlar və s. sahə təmsilçiləri iştirak etməlidirlər.

İnformasiya təhlükəsizliyi sahəsində normativ-hüquqi bazanın yaradılması çox çətin və mürəkkəb prosesdir. Bu da onunla bağlıdır ki, müvafiq normativ-hüquqi baza hələ formalaşmaqda olan, formalaşması ziddiyyətlərlə müşayiət olunan ictimai münasibətlərin tənzimlənməsi üçün yaradılır. Praktiki olaraq, hazırda nəhəng yeni informasiya vasitələri massivi hüquqi tənzimləmədən kənardadır. Bu sahədəki problemlərin kompleks şəkildə öyrənilməsinə, onların həlli üçün məqsədyönlü strategiyaların işlənməsinə və real şəraitə uyğun olaraq həyata keçirilməsinə ehtiyac vardır.

Beynəlxalq informasiya təhlükəsizliyi sahəsində hüquqi bazanın formalaşdırılması olduqca ləng və mürəkkəb bir prosesdir. Digər məsələlərdə olduğu kimi, burada da beynəlxalq ictimaiyyət tipik problemlə üzləşir – ölkələrin maraqları üst-üstə düşmür.

Beynəlxalq hüquqda da informasiya təhlükəsizliyinin təmin olunması məsələləri ilə bağlı bir sıra problemlər mövcuddur. İlk növbədə, qeyd etmək lazımdır ki, beynəlxalq hüquqda informasiya sferasında beynəlxalq təhlükəsizliyin mahiyyətinin hamılıqla qəbul edilməsi ilə bağlı yetərincə boşluqlar var. Hazırda ölkələr arasında aparılan danışıqlar bu problemi aradan

qaldırmağa imkan vermir. Məsələn, bir ölkənin İKT-dən, yaxud KİV-dən silah qismində istifadə etməklə digər ölkəyə qarşı həyata keçirdiyi “aqressiya aktı”nın qiymətləndirilməsi ilə bağlı ümumi baxışlar mövcud deyil. Yaxud bu cür aqressiya aktına görə dövlətin yurisdiksiyasının hansı anda özünü müdafiə üçün tətbiq edilməsi ilə bağlı məsələlərə baxışlar da ziddiyyətlidir [7].

İnformasiya təhlükəsizliyinin hüquqi təminatı sahəsində mühüm problemlərdən biri də vahid terminologiyanın formalaşdırılması ilə bağlıdır. Beynəlxalq hüquqda informasiya təhlükəsizliyinin təmin olunması sahəsində baş verən prosesləri izah edə bilən kifayət qədər sabit terminlər yoxdur. Həmçinin informasiya sferasında beynəlxalq təhlükəsizliyə qarşı təhdid yarada biləcək subyektlərin sayı əhəmiyyətli dərəcədə artsa da, onların heç də hamısını mövcud hüquqi təminatlarla izah etmək mümkün deyil.

Ən mürəkkəb məsələ isə informasiya təhlükəsizliyinin təmin olunması ilə bağlı fəaliyyətin bir ölkənin yurisdiksiyası çərçivəsində həyata keçirilməsinin mümkün olmamasıdır.

Doğrudur, İKT-nin cinayətkar məqsədlərlə istifadəsi BMT Nizamnaməsində nəzərdə tutulan beynəlxalq hüququn xarakteristikası altına düşür. Belə ki, “güc tətbiqi təhdidləri”, “güc tətbiqi”, “ərazi bütövlüyü”, “dövlət suverenliyi” və s. bu kimi dəyərlər BMT-nin həmin sənədində öz əksini tapıb. Amma beynəlxalq hüquq İKT-ni “güc tətbiqi təhdidləri” və ya “güc tətbiqi”nin “alətləri”, yaxud “vasitələri” kimi nəzərdə tutmur.

KİV-in dövlətin daxili siyasətinə təsir etmək, onun ərazi bütövlüyünü dəyişdirmək, yaxud dövlət suverenliyini pozmaq kimi cinayətkar məqsədlərlə istifadəsi məsələsi isə, ümumiyyətlə, beynəlxalq hüququn müzakirə predmeti deyil.

İnformasiya təhlükəsizliyinin iqtisadi problemləri

İnformasiya təhlükəsizliyi texnoloji fəaliyyət sahəsi kimi qavranılsa da, bu sahədə bir sıra problemlər daha çox iqtisadi amillərlə bağlı olur. İstənilən sahədə olduğu kimi, informasiya təhlükəsizliyi iqtisadiyyatının da özünəməxsus xüsusiyyətləri mövcuddur. İnformasiya təhlükəsizliyi iqtisadiyyatı – bir sıra ümumi iqtisadi qanunlara və metodlara bağlı olsa da, iqtisadiyyatın müstəqil sahəsi kimi çıxış edir.

Cəmiyyətdə, o cümlədən iqtisadiyyatda informasiyanın artan rolu iqtisadi elmlərdə informasiya təhlükəsizliyinə marağı artırır. İqtisadi elmi istiqamətlərdə informasiya təhlükəsizliyinə, ilk növbədə, müəssisənin və dövlətin iqtisadi maraqları baxımından yanaşılır.

Ən mühüm istiqamətlərdən biri informasiya təhlükəsizliyi vasitələrinin tətbiqinin iqtisadi dəyərinin qiymətləndirilməsi ilə bağlıdır. Burada əsas tədqiqat obyekti kimi müəssisənin informasiya təhlükəsizliyinin təmin edilməsinə çəkilən xərclərin iqtisadi səmərəliliyinin analizi çıxış edir [8].

Digər bir istiqamət kimi informasiya təhlükəsizliyi riskləri və təhdidlərinin qiymətləndirilməsi ilə bağlı tədqiqatları göstərmək olar. Bu istiqamət informasiya təhlükəsizliyinin iqtisadi təhdidlərinin təsnifatını, informasiya risklərinin sistemləşdirilməsini özündə birləşdirir. Həmçinin informasiya risklərinin qiymətləndirilməsi və analizi metodologiyalarının işlənməsini bu tədqiqat istiqamətinə aid etmək olar.

İnformasiya təhlükəsizliyi iqtisadiyyatının perspektiv istiqamətləri olaraq fiziki və hüquqi şəxslərin informasiya təhlükəsizliyi risklərinin sığortalanması sisteminin yaradılmasını və informasiya təhlükəsizliyi təhdidləri ilə mübarizənin iqtisadi metodlarının işlənməsini göstərmək olar.

Bütövlükdə, informasiya təhlükəsizliyinin iqtisadi problemləri istiqamətində aşağıdakı sahələr üzrə elmi tədqiqatların aparılması aktualıq kəsb edir [1, 9]:

- müasir sosial-iqtisadi sistemlərin informasiya təhlükəsizliyi;
- informasiya təhlükəsizliyi risklərinin (o cümlədən, informasiyanın, informasiya resurslarının dəyərinin və vurulan ziyanın) qiymətləndirilməsi;
- informasiya təhlükəsizliyi risklərinin sığortalanması modelləri;
- informasiya təhlükəsizliyinə yatırılan investisiyaların modelləşdirilməsi;

- iqtisadiyyatın müəyyən sektorlarının kiber-hücumlara həssaslığının qiymətləndirilməsi;
- e-xidmətlərin, o cümlədən e-kommersiyanın informasiya təhlükəsizliyi;
- informasiya təhlükəsizliyinin təmin edilməsi üçün resursların paylanması modelləri;
- informasiya resurslarına mülkiyyət münasibətlərinin iqtisadi tənzimlənməsi məsələləri və s.

İnformasiya təhlükəsizliyi üzrə kadr hazırlığı

Son illərin statistik məlumatları göstərir ki, informasiya təhlükəsizliyinin pozulması hallarının çox böyük bir hissəsi insan faktorundan – təhlükəsizlik prosedurlarına əməl etməmək, insan səhvləri, qeyri-adekvat təlim, informasiya təhlükəsizliyi sahəsində biliklərin olmaması kimi faktorlardan qaynaqlanır.

Qeyd etmək lazımdır ki, insan amili yalnız peşə kompetensiyalarından deyil, həm də şəxsi keyfiyyətlərdən asılıdır. Şəxsi keyfiyyətlərə peşə vəzifələrini yerinə yetirərkən etik normalara əməl etmək, nizam-intizamlı olmaq, düzgünlük, prinsipiallıq, məsuliyyətlik, emosional dayanıqlılıq, özünə nəzarət, sirr saxlamaq, zərərli vərdislərdən çəkinmək, sayıqlıq, kommunikativlik və s. aiddir [1].

Hazırda informasiya təhlükəsizliyi üzrə təhsil, əsasən, informasiyanın mühafizəsinin texniki aspektləri üzrə kadrların hazırlığına və yenidən hazırlığına yönəlib. Bununla yanaşı, informasiya hüququ və kompüter cinayətkarlığının təhqiqatının təşkili və metodologiyası üzrə mütəxəssislərin hazırlanması işində xeyli gerilik mövcuddur. Kibercinayətkarlıqla uğurlu mübarizə aparmaq üçün, bir tərəfdən, ali təhsil müəssisələrinin hüquq fakültələrində kompüter cinayətlərinin təhqiqatı ilə bağlı, digər tərəfdən isə, informasiya təhlükəsizliyinin təmin edilməsi üzrə mütəxəssislərin hazırlanmasına dair tədris planlarının daxil edilməsi zəruridir [10].

İnformasiya təhlükəsizliyinin təmin olunması sahəsində yüksək ixtisaslı mütəxəssislərə olan tələbatı yalnız orta, ali və əlavə peşə təhsilinin imkanlarından kompleks istifadə etməklə ödəmək mümkündür. Məhz təhsil prosesinin fasiləsizliyini təmin etməklə müvafiq tələbata cavab vermək olar.

Müvafiq kadr hazırlığı prosesində vacib məsələlərdən biri də tədris prosesi ilə informasiya təhlükəsizliyi üzrə elmi tədqiqatlar arasında sıx əlaqələrin yaradılmasıdır. Məlum olduğu kimi, tədrisin keyfiyyəti müvafiq elmi tədqiqatların dərinliyindən çox asılıdır. İnformasiya texnologiyalarının həddindən artıq elmtutumlu olması bu sahə üzrə mütəxəssislərin elmi biliklərinin də yüksək səviyyədə olmasını tələb edir.

Mühüm məsələlərdən biri də tədris proqramının məzmunu ilə bağlıdır. İnformasiya təhlükəsizliyi sahəsində ən son nailiyyətlərin əks olunması üçün müvafiq tədris proqramlarının məzmunu ildə bir dəfə (hər dərs ilinin başlanğıcında) yenilənməlidir.

İnformasiya təhlükəsizliyi üzrə kadrların hazırlanmasında ortaya çıxan problemlərdən biri də tədris prosesinin maddi-texniki təminatı ilə bağlıdır. Praktiki və laborator məşğələlər müasir texnologiyaların tətbiqi ilə xüsusi təchiz olunmuş yerlərdə aparılmalıdır.

İnformasiya təhlükəsizliyi sahəsində kadr hazırlığı təkcə texnoloji istiqamət üzrə deyil, informasiya təhlükəsizliyinin müxtəlif aspektləri üzrə aparılmalıdır: informasiya təhlükəsizliyi sahəsində yüksək peşəkarlığa malik hüquqşünaslar, həkimlər, psixoloqlar, jurnalistlər, sosioloqlar, texnoloqlar, politoloqlar və s. də hazırlanmalıdır.

İnformasiya təhlükəsizliyi mədəniyyəti

İnformasiya cəmiyyətində ümumi mədəniyyət normaları kontekstində informasiya mədəniyyətinin əhəmiyyəti artır. İnformasiya mədəniyyəti – informasiya tələbatını müəyyənləşdirərək lazımi informasiyanın axtarılıb tapılması, qəbulu, saxlanması, emal olunması, təhlili, təqdim olunması üçün müasir İKT vasitələrindən yüksək səviyyədə istifadə etmək bacarığı, eyni zamanda informasiya ilə işləyərkən onun tamlığının, əlyetərliliyinin təmin edilməsi, məxfiliyinin qorunması, hüquqi və etik normalara əməl olunmasıdır [11].

İnformasiya mədəniyyətinin tərkib hissələrindən biri də informasiya təhlükəsizliyi mədəniyyətidir. Təhlükələrə qarşı ən səmərəli strategiyalardan biri vətəndaşlarda informasiya təhlükəsizliyi mədəniyyəti formalaşdırmaqdır.

İnformasiya təhlükəsizliyi mədəniyyəti – şəxsiyyətin zərərli informasiya-psixoloji təsirlərdən qorunması səviyyəsi və ona məxsus olan informasiyanın təhlükəsizliyini təmin etmək qabiliyyətidir. Həmçinin informasiya təhlükəsizliyi mədəniyyəti – şəxsiyyətin və onun informasiyasının mövcud bilik, vərdiş və bacarıqlar əsasında zərərli təsirlərdən qorunma səviyyəsinin yaradılması və saxlanması, həmçinin onların informasiya tələbatının tam təmin olunmasına gətirib çıxaran fasiləsiz təkmilləşdirilməsi prosesidir [12].

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.

İnformasiya təhlükəsizliyi mədəniyyətinin formalaşdırılmasının ən vacib mexanizmlərindən biri dövlət qulluqçularına təhlükəsizliyi düzgün qiymətləndirmək, informasiya texnologiyalarından məsuliyyətlə istifadə, informasiya təhlükəsizliyinin pozulması ilə bağlı insidentlərə adekvat reaksiya vermək kimi məsələləri öyrətməkdir. Qeyri-dövlət təşkilatlarının əməkdaşlarından fərqli olaraq, dövlət qulluqçularında zərərli informasiya-psixoloji təsirlərə qarşı daha yüksək dayanıqlılıq formalaşdırmaq lazımdır.

Dövlət orqanlarında informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması prosesi kompleks xarakter daşmalı, korporativ və informasiya mədəniyyətlərinin yaradılması proseslərini nəzərdə tutmalıdır. Dövlət orqanlarında informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması və yüksəldilməsi üçün aşağıdakı tədbirlərin görülməsi məqsədəuyğundur [12]:

- müvafiq qanunvericilik bazasının möhkəmləndirilməsi;
- milli informasiya resurslarının formalaşdırılması və istifadəsi qaydalarının yaradılması və düzgün həyata keçirilməsi;
- dövlət orqanlarında informasiya təhlükəsizliyi təhdidlərinin monitoring sisteminin təşkili, kadr və resurs bazalarının yaradılması, onun nəticələrindən dövlət strukturlarının informasiya təhlükəsizliyinin qiymətləndirilməsində istifadə edilməsi;
- dövlət qulluqçularının informasiya ilə iş üzrə fəaliyyətinə nəzarət sisteminin təkmilləşdirilməsi;
- dövlət qulluqçularının öyrədilməsinin dərəcəsinin və təşkilinin yüksəldilməsi, informasiya təhlükəsizliyi üzrə xüsusi tədris proqramlarının işlənməsi.

Qeyri-dövlət təşkilatlarında informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması məsələsi də mühüm əhəmiyyət kəsb edir. Təşkilatın informasiya təhlükəsizliyi mədəniyyəti dedikdə, təşkilatın bütün əməkdaşlarının informasiyaya münasibətdə maraqlı tərəflərin ortaq mənafelərinə hörmətin təmin edilməsi başa düşülür. Bu, biznes sahiblərinin, təsisçilərin, müştərilərin, tərəfdaşların, menecerlərin, əməkdaşların və s. ortaq maraqlarıdır. Müvafiq fəaliyyət strateji perspektivdə ortaq maraqları olan tərəflərin qarşılıqlı etimada əsaslanan münasibətlərinin dəstəklənməsi üçün əsas şərtlərdən biridir.

Bütövlükdə, informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması və inkişafı problemləri çərçivəsində aşağıdakı istiqamətlərdə elmi tədqiqatlar aktuallıq kəsb edir [10]:

- informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması sahəsində dövlət siyasətinin əsas istiqamətləri;
- əhəlinin informasiya təhlükəsizliyi məsələləri üzrə maarifləndirilməsi;
- informasiya təhlükəsizliyi mədəniyyətinin məzmunu və struktur komponentləri;
- informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması mexanizmləri;
- təşkilatlarda informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması məsələləri;
- informasiya təhlükəsizliyi mədəniyyətinin ölçülməsi (indikatorların müəyyən edilməsi) problemləri;

İnformasiya təhlükəsizliyi etikası

İnformasiya təhlükəsizliyinin təmin olunmasında etik normalar mühüm rol oynayır. Mənəvi-əxlaqi normalar əsasında özünütənzimləmə informasiya münasibətləri iştirakçıların antisosial davranışlardan müdafiəsinin ən effektiv vasitələrindən biridir. Cəmiyyət tərəfindən işlənən mənəvi-əxlaqi normalar perspektivdə yeni hüquq normalarının yaradılması və mövcud hüquq normalarının təkmilləşdirilməsi üçün baza rolunu oynaya bilər. Beləliklə, informasiya cəmiyyətinin yaratdığı reallıqlara uyğun olan etik normalar şəxsiyyətin, cəmiyyətin və dövlətin informasiya təhlükəsizliyinin qarantı kimi çıxış edə bilər.

İnformasiya təhlükəsizliyinin bu yeni institutunun vacibliyi yeni elmi tədqiqat sahəsinin – informasiya etikasının meydana gəlməsinə və aktuallaşmasına səbəb olmuşdur. İnformasiya etikası kompüter texnologiyalarının cəmiyyətə sosial təsirinin xüsusiyyətlərini və bunun əsasında formalaşan mənəvi normaları və onların kompüter texnologiyalarını işləyib hazırlayanların və onların istifadəçilərinin şüuruna yeridilməsi siyasətini öyrənir. İnformasiya etikası – peşə etikasını, istehlakçı etikasını və dövlət siyasətinin bəzi məsələlərini özündə birləşdirən bir elm və bilik sahəsidir [13].

Hazırda istənilən bilik sahəsinin peşə etikasına təsir edən bütün texnologiyaların əksəriyyəti informasiya ilə bağlıdır. Bu vəziyyət mütəxəssislərə – proqramçılara, sistem administratorlarına, informasiya təhlükəsizliyi analitiklərinə qarşı yüksək tələblər irəli sürür.

Beynəlxalq informasiya texnologiyaları federasiyası digər ölkələrin müvafiq təşkilatlarına sadalanan kodekslərdə müəyyən edilən etik standartlar əsasında kompüter etikası kodeksinin qəbul edilməsini tövsiyə edib. Həmin standartların əsasını yerli mədəni və etik ənənələr nəzərə alınmaqla, 10 əsas prinsip təşkil edir [14].

Bütün müvafiq kodekslərdə dörd əsas mənəvi-etik prinsipə (şəxsi həyatın toxunulmazlığı, dəqiqlik, özəl mülkiyyət və əlyetərlilik) riayət etməyə əsaslanan öz vəzifələrini dürüst (vicdanla) yerinə yetirmək; peşə və sosial məsuliyyət; ixtisas dərəcəsini artırmaq; irqi, dini və etnik bərabərlik kimi etik normalara öz əksini tapıb.

UNESCO-nun 2011-ci ildə keçirilən 36-cı baş konfransında “İnformasiya cəmiyyətində etika kodeksi” qəbul edildi. Həmin sənəddə təsdiq olunur ki, real həyatda olduğu kimi, informasiya məkanında da insanların hüquq və azadlıqları dəyişməz olaraq qalmalıdır [15].

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

Uşaqların informasiya təhlükəsizliyi

İnformasiya cəmiyyətində uşaqların psixikasına güclü informasiya axını təsir edir. Uşaqlar ətraf informasiya mühitindən: İnternetdən, KİV-dən, müxtəlif kommunikasiya vasitələrindən, ünsiyyətdə olduqları insanlardan filtrlənməmiş informasiya əldə edirlər. Uşaqların informasiya təhlükəsizliyi üzrə aparılan tədqiqatlar göstərir ki, bu sahədə həll edilməmiş bir sıra problemlər mövcuddur. Bu problemlərin həlli, ilk növbədə, məsələyə çoxaspektli, multidissiplinar yanaşma tələb edir. Mütəxəssislər uşaqların informasiya təhlükəsizliyinin fiziki sağlamlıq (informasiya məkanının kriminallaşması, kompüterdə işləmə normalarına və qaydalarına əməl etməmək), psixoloji vəziyyət (şüurla manipulyasiya, kompüter və şəbəkə oyunlarından asılılıq, kiberbullinq, trollinq, qorxutma, alçaltma), mənəvi inkişaf (uşaqlar arasında yayılması qadağan olunan informasiya təsiri, ekstremizm və terrorçuluğa cəlb etmə, informasiya hüquqlarının məhdudlaşdırılması, sosial şəbəkələrdə qeyri-etik davranış) və maddi itki (şəxsi informasiyanın oğurlanması, zərərli proqram təminatının təsiri, İnternet vasitəsi ilə qanunsuz alqı-satqı, müəllif hüquqlarının pozulması) ilə bağlı əsas təhdid siniflərini fərqləndirirlər [10].

Uşaqların mənəvi, fiziki, psixoloji və sosial sağlamlığını təmin etmək üçün təhlükəsiz informasiya-təhsil mühiti yaratmaq zəruridir. Bunun üçün aşağıdakı tədbirlərin görülməsi vacibdir:

- uşaqları onların sağlamlığına və inkişafına zərər verən informasiyanın yayılmasından qorumaq üçün müvafiq təşkilati-hüquqi mexanizmlərin yaradılması;
- uşaqların vətəndaş kimi yetişmələrinə mane olan informasiyaya girişini məhdudlaşdıran sistemlərin, informasiyanın süzgəcdən keçirilməsi vasitələrinin və digər müvafiq aparat-proqram təminatının və texnoloji qurğuların tətbiqi;
- uşaqlarda İnternet asılılığının profilaktikası, uşaqlara virtual mühitdə məsuliyyətli və təhlükəsiz davranış üzrə bilik və vərdislərinin aşılması;
- uşaqların sağlamlığına və inkişafına zərər verən informasiyadan qorunma üsulları barədə valideynlərin maarifləndirilməsi;
- bütün kateqoriyadan olan dinləyicilər üçün informasiya təhlükəsizliyinin təmin edilməsi, İnternetdə davranış məsələlərinin tədris proqramlarına daxil edilməsi;
- təhsilin informasiyalaşdırılması prosesinin psixoloji-pedoqoji xüsusiyyətləri, İKT-nin uşağın şəxsiyyətinə neqativ təsirlərinin qarşısının alınması üzrə pedaqog-psixoloqlar üçün xüsusi kursların təşkili;
- informasiya təhlükəsizliyi problemləri ilə bağlı ailələrlə iş üzrə sinif rəhbərləri, bağça tərbiyəçiləri və sosial pedaqoqlar üçün xüsusi kursların işlənilib hazırlanması və tətbiqi;
- valideynlər üçün uşaqların zərərli informasiyanın təsirlərindən qorunması üzrə informasiya kurslarının işlənilib hazırlanması və tətbiqi;
- bütün təhsil müəssisələrində və elektron kitabxanalarda İnternet trafikinin kontent filtrasiyası ilə təmin edən proqram məhsulları ilə təmin edilməsi;
- İnternet provayderləri tərəfindən təhsil müəssisələrinə İnternet trafikinin ötürülməsi zamanı kontent filtrasiyasının tətbiqinin təşkili.

Qeyd etmək lazımdır ki, valideynlər cəlb edilmədən İnternetdə uşaqların informasiya təhlükəsizliyinin təmin edilməsi mümkün deyil. Reallıq onu göstərir ki, valideynlərin bir çoxu İnternetdə uşaqlar üçün olan mövcud və potensial təhlükələri dərk etmirlər. Ona görə də İnternetdə uşaqların informasiya təhlükəsizliyinin etibarlı təminatı üçün təhsil müəssisələri ilə valideynlərin səylərinin birləşdirilməsi vacibdir.

Nəticə

İnformasiya təhlükəsizliyinin humanitar elmi tədqiqat istiqamətlərinin tədqiqi onu göstərir ki, bu sahələr multidissiplinar elmi tədqiqatların yeni və olduqca mürəkkəb, çoxaspektli obyektidir. Bütün bunlar humanitar və texniki sahə alimlərinin və mütəxəssislərinin informasiya təhlükəsizliyi problemləri sahəsində elmi tədqiqatlarının aparılması istiqamətində səylərinin birləşdirilməsini tələb edir. Bu cür əməkdaşlıq informasiya təhlükəsizliyinin etibarlı şəkildə təmin edilməsi üçün kompleks tədbirlərin işlənməsi üçün mühüm rol oynaya bilər.

İnformasiya təhlükəsizliyi məsələləri təkcə əməl edilən informasiyanın əlverişliliyinin, tamlığının və konfidensiallığının təmin edilməsi ilə bitmir, problemin siyasi, hüquqi, iqtisadi, psixoloji, kadr təminatı və s. aspektlərini də nəzərə almaq vacibdir. İnformasiya cəmiyyətində insan fəaliyyətinin bütün sferaları informasiya fəzasına daşınır, informasiya prosesləri sosial, siyasi, hüquqi, iqtisadi, psixoloji, kulturoloji və digər münasibətləri də əhatə edir. Bununla yanaşı, informasiya proseslərinin neqativ təsirləri özünü daha qabarıq göstərir, kibercinayətkarlıq, kiberterrorizm, informasiya müharibəsi təhlükələri artır. Beləliklə, çox zaman texnoloji problem kimi təqdim olunan informasiya təhlükəsizliyi sahəsində bir sıra həlli vacib olan humanitar problemlər də meydana çıxır. Lakin mövcud elmi-tədqiqat və praktiki işlərdə çox zaman informasiya təhlükəsizliyinin texniki və texnoloji tərəflərinə daha çox fikir verilir, problemin humanitar aspekti kifayət qədər tam əks olunmur. Bu baxımdan, informasiya

təhlükəsizliyinin humanitar problemləri sahəsində multidissiplinar tədqiqatlara çox böyük ehtiyac vardır.

Ədəbiyyat

1. Əliquliyev R.M., İmamverdiyev Y.N. İnformasiya təhlükəsizliyinin humanitar aspektləri / İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, 14 may 2015-ci il, s. 9-12.
2. Əliquliyev R. M., İmamverdiyev Y. N. , Yusifov F. F. Cəmiyyətin informasiya təhlükəsizliyinə dair bəzi konseptual baxışlar // İnformasiya cəmiyyəti problemləri, 2011, №2(4), s.3-9.
3. Grachev G.V. Sociology of Information-Psychological Security: the problem of formulating the definitions // NB: Международные отношения, 2013, № 4, с.61-85.
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. Брандман Э.М. Глобализация и информационная безопасность общества // Философия и общество, 2008, №1, с.31-41.
6. Малыхина Г.И., Аксенов В.В. Современная информационная безопасность и проблемы глобализации // Наука и военная безопасность, 2008, № 2, с.7-12.
7. Musayev V.Y., İmamverdiyev Y.N. İnformasiya təhlükəsizliyi sahəsində beynəlxalq çağırışlar, təşəbbüslər və öhdəliklər / İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, 14 may 2015-ci il, s. 102-105.
8. Bohme R.R. (Editor) The Economics of Information Security and Privacy, Springer-Verlag Berlin Heidelberg, 2013, 327 p.
9. Əliquliyev R.M., Mahmudov R.Ş. İnformasiya iqtisadiyyatının təhlükəsizliyinin təmin edilməsi məsələləri // İnformasiya cəmiyyəti problemləri, №1(7), 2013, s. 3-13.
10. Mjolsnes S.F. A Multidisciplinary Introduction to Information Security, CRC Press, 2011, 348 p.
11. Əliquliyev R.M., Mahmudova R.Ş. İnformasiya mədəniyyəti: mahiyyəti və formalaşdırılması problemləri, 2010, №1, s.14-22
12. İmamverdiyev Y.N. E-dövlət mühitində informasiya təhlükəsizliyi mədəniyyəti problemləri // İnformasiya texnologiyaları problemləri, 2015, №1, s.80-88.
13. Чусавитина Г.Н., Чернова Е.В., Макашова В.Н., Зеркина Н.Н., Кузнецова И.М. Этические вопросы применения информационных технологий как компонента предметного содержания подготовки студентов университета // Fundamental research, 2015, № 10, с.318-323.
14. Martin C.D., Holz H.J. Non-apologetic Computer Ethics Education: A Strategy for Integrating Social Impact and Ethics into the Computer Science Curriculum, <http://www.southernct.edu>
15. UNESCO, Code of ethics for the information society, <http://www.unesdoc.unesco.org/images/0021/002126/212696e.pdf>
16. Livingstone S. Children and the Internet, John Wiley & Sons, 2013, 320 p.

УДК 004.9

Алгулиев Расим М.¹, Имамвердиев Ядигар Н.², Махмудов Расим Ш.³

^{1,2,3}Институт Информационных Технологий НАНА, Баку, Азербайджан

¹secretary@iit.ab.az, ²yadigar@lan.ab.az, ³rasimmahmudov@gmail.com

Мультидисциплинарные научно-теоретические проблемы информационной безопасности

В статье исследуются междисциплинарные научно-теоретические проблемы информационной безопасности. Анализируются международные, политические, психологические, правовые, экономические, культурные и этические аспекты и вопросы, связанные с подготовкой кадров и защитой детей. Определяются актуальные научно-исследовательские направления в этих областях.

Ключевые слова: информационное общество, информационная безопасность, информационно-психологическая безопасность, культура информационной безопасности, информационная безопасность детей.

Rasim M. Alguliyev¹, Yadigar N. İmamverdiyev², Rasim Sh. Mahmudov³

^{1,2,3}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹secretary@iit.ab.az, ²yadigar@lan.ab.az, ³rasimmahmudov@gmail.com

Multidisciplinary scientific and theoretical problems of information security

The article investigates multidisciplinary scientific and theoretical problems of information security. In particular, international, political, psychological, legal, economic, cultural and ethical aspects and issues related to training and child protection are analyzed. Current research directions in these areas are determined.

Keywords: information society, information security, information and psychological security, information security culture, information security of children.