İnformasiya təhlükəsizliyinin humanitar aspektləri

Rasim Əliquliyev[1], Yadigar İmamverdiyev[2]

AMEA İnformasiya Texnologiyaları İnstitutu

[1]director@iit.ab.az, [2]yadigar@lan.ab.az

***Xülasə*— İnformasiya təhlükəsizliyinin təmin edilməsində insan faktorunun əhəmiyyətli rola malik olması hazırda hamı tərəfindən etiraf olunan bir həqiqətdir. İnsan faktoru vasitəsilə informasiya təhlükəsizliyinin humanitar və ictimai elmlərlə bir çox predmet hiperəlaqələri yaranır. İnformasiya cəmiyyəti şəraitində informasiya təhlükəsizliyinin təmin edilməsi yeni texnoloji həllər tələb etməklə yanaşı, humanitar və ictimai elmlər qarşısında da bir sıra mürəkkəb problemlər qoyur. Bu işdə informasiya təhlükəsizliyinin humanitar və ictimai elmlər baxımından aktual problemləri analiz edilir və bir sıra multi-distiplinar tədqiqat istiqamətləri müəyyən edilir.**

Açar sözlər*— *informasiya təhlükəsizliyi; humanitar və ictimai elmlər; informasiya müharibəsi; informasiya-psixoloji təhlükəsizlik; informasiya təhlükəsizliyi mədəniyyəti.

I. GİRİŞ

İnformasiya təhlükəsizliyi nəzəriyyəsində və praktikasında belə bir baxış hamılıqla qəbul edilir ki, informasiya təhlükəsizliyi sisteminin təşkilində təkcə sistemin mürəkkəb texniki komponentləri deyil, həm də insan faktoru mütləq nəzərə alınmalıdır. Yəni, informasiya təhlükəsizliyi sistemini formalaşdıran zaman informasiya təhlükəsizliyi sisteminə cəlb edilmiş insanların fərdi-psixoloji və sosial-psixoloji, mənəvi, etik və digər şəxsi xarakteristikaları da nəzərə alınmalıdır [1,2].

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 lazımdır. 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 humanitar problemlər də meydana çıxır [3]. 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 multi-distiplinar tədqiqatlara çox böyük ehtiyac vardır. Təqdim olunan işdə mövcud tədqiqatların icmalı əsasında informasiya təhlükəsizliyinin humanitar və ictimai elmlər baxımından aktual problemləri müəyyən edilir, bu problemlərin hazırkı həll vəziyyəti analiz olunur.

II. İNFORMASİYA TƏHLÜKƏSİZLİYİ VƏ İNSAN FAKTORU

Son illərin statistik məlumatları [4, 5] 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.

İnsanlar – xidməti heyət və informasiya sisteminin istifadəçiləri "insan-maşın" sisteminin ayrılmaz hissəsidir. İnsanın sistemdə öz funksiyalarını necə həyata keçirməsindən həm sistemin funksiyaları, həm də təhlükəsizliyi əhəmiyyətli dərəcədə asılıdır. Xidməti heyət və istifadəçilər informasiya təhlükəsizliyi risklərini düzgün qiymətləndirmirlər və informasiya təhlükəsizliyinə yönəlmiş daxili təhdidlərin mənbəyinə çevrilirlər.

İnformasiya sisteminin normal fəaliyyət prosesinə müdaxilə və ya informasiyanı icazəsiz əldə etməyə cəhd edən kənar şəxslər və təşkilatlar da informasiya təhlükəsizliyinə mühüm təsir göstərirlər.

İnformasiya təhlükəsizliyinin təmin edilməsində insanlarla yanaşı daha iki vacib komponent: proseslər və texnologiyalar iştirak edir. Bu komponentlərdə insanlar yenə də ən zəif nöqtələrdir.

Proseslər – informasiya təhlükəsizliyinin təmin edilməsinə yönəlmiş formal və qeyri-formal mexanizmlərdir. Proseslər informasiya təhlükəsizliyi siyasəti və prosedurları ilə tənzimlənir. İnformasiya təhlükəsizliyi siyasətinin və prosedurlarının yaradılması və həyata keçirilməsində də insan faktoru mühüm rol oynayır, bəzi informasiya təhlükəsizliyi boşluqları siyasət və prosedurların layihələndirilməsi mərhələsində buraxılır.

İnformasiya təhlükəsizliyinin təmin edilməsində istifadə edilən texnologiyalarda insan tərəfindən buraxılmış səhvlər nəticəsində informasiya təhlükəsizliyinin pozulması üçün bədniyyətlilər tərəfindən istifadə edilə bilən müxtəlif boşluqlar ola bilər. Eyni zamanda, texnologiyaları insanlar istismar edir və reallaşdırırlar, insanlar isə həmişə ən zəif halqadır. İstifadəçilər informasiya təhlükəsizliyi tədbirlərinə (müxtəlif formalarda) müəyyən müqavimət də göstərirlər.

III. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN POLİTOLOJİ PROBLEMLƏRİ

İnformasiya cəmiyyətində informasiya fəzası siyasi iştirak fəzasına çevrilir, dövlət və cəmiyyət arasındakı münasibətlərə əhəmiyyətli dərəcədə təsir göstərir. Dövlət vətəndaşlarla e-dövlət vasitəsilə əlaqə saxlayır, e-xidmətlərə asan çıxış imkanı

verir. Qarşılıqlı təsirin rəqəmsal forması siyasi iştirak və siyasi ifadə üçün yeni imkanlar yaradır. Eyni zamanda, informasiya təhlükəsizliyi məsələlərinə həssas olan siyasi münasibət subyektlərinin spektri genişlənir – dövlət hakimiyyəti, milli təhlükəsizlik, siyasi strukturlar, kütləvi informasiya vasitələri (KİV-lər), sosial institutlar və s. İnformasiya təhlükəsizliyi siyasi münasibətlərin spesifik elementi kimi çıxış edir [6].

İnformasiya fəzasında siyasi xarakterli müxtəlif hücumlar (informasiya qarşıdurmaları, informasiya müharibələri, elektron kəşfiyyat, haktivizm, kiberterrorizm) həyata keçirilir [7]. KİV-lərin və sosial medianın informasiya təhlükəsizliyində rolunu da qeyd etmək lazımdır, onlar ictimai rəylə manipulyasiya və provakasiyaların həyata keçirilməsi məqsədilə istifadə edilə bilərlər.

Siyasi elmlər istiqamətində informasiya təhlükəsizliyi çərçivəsində geniş məsələlər spektri öyrənilir [8, 9]:

- informasiya cəmiyyətinin formalaşması və inkişafının elmi-nəzəri problemləri;
- qlobal 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;
- cəmiyyətinin dəyərləri və onlara yönəlmiş müasir informasiya təhdidləri;
- dövlətin informasiya təhlükəsizliyi siyasəti, prioritetləri və strategiyası;
- informasiya təhlükəsizliyinin milli təhlükəsizlik sistemində yeri və informasiya təhlükəsizliyinin təmin edilməsində hakimiyyət qolları arasında səlahiyyətlərin bölgüsü;
- qlobal informasiya cəmiyyəti şəraitində informasiya təhlükəsizliyinin sosial-iqtisadi aspektləri;
- 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;
- informasiya təhlükəsizliyi üzrə beynəlxalq əməkdaşlıq problemləri və s.

IV. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN HÜQUQİ PROBLEMLƏRİ

İnformasiya təhlükəsizliyi insanın, cəmiyyətin və dövlətin informasiya sahəsində maraqlarının qorunmasını nəzərdə tutur. Dövlət bu sahədə hüquqların qorunmasının yeganə qarantıdır. O, bu funksiyanı yalnız qanunvericilik vasitəsilə həyata keçirə bilər və informasiya cəmiyyəti sahəsində qanunvericilik – *informasiya hüququ* yalnız son onilliklərdə formalaşmağa başlamışdır. İnformasiya təhlükəsizliyinin hüquqi tənzimlənməsi də informasiya hüququ əsasında həyata keçirilir [10].

İnformasiya təhlükəsizliyinin təmin edilməsinin hüquqi istiqamətlərinə aşağıdakılar daxildir [11]:

- şəxsiyyətin, cəmiyyətin və dövlətin maraqlarının qanunvericilikdə təsbiti;
- informasiya sahəsində insanların konstitusion hüquq və azadlıqlarının reallaşdırılması və qorunması;
- dövlətin informasiya suverenliyinin təmin edilməsi;
- fərdi məlumatlar sahəsində hüquqi təminat;
- şəxslərin və təşkilatların şərəf, ləyaqət və işgüzar nüfuzunun qorunması;
- İKT sahəsində münasibətlərin hüquqi tənzimlənməsi;
- informasiya təhlükəsizliyinin qanunvericilik bazasının yaradılması problemləri;
- informasiya təhlükəsizliyi sahəsində ictimai nəzarət formalarından istifadə edilməsinin hüquqi tənzimlənməsi;
- İKT sahəsində cinayətlərlə mübarizə sahəsində münasibətlərin hüquqi tənzimlənməsi;

Baxılan sahənin vacib xarakterik cəhətlərindən biri informasiyanın axtarışı, istehsalı, toplanması, saxlanılması və ötürülməsi proseslərində mülkiyyət münasibətlərinin hüquqi təmin edilməsinə, müəllif və patent hüquqlarına, intellektual mülkiyyət hüquqlarına diqqətin artmasıdır [12].

V. İNFORMASİYA TƏHLÜKƏSİZLİYİ VƏ SOSİOLOGİYA

İnformasiya təhlükəsizliyi problemlərinə sosial baxış nöqtəsindən baxılması da xüsusilə vacibdir, çünki müasir informasiya sistemləri mürəkkəb sosial-texniki sistemlərdir, onların əsasında ictimai proseslər dayanır və onların təsir obyekti də insanlardır. Beləliklə, informasiya təhlükəsizliyinin sosial kontekstinin tədqiqi, informasiya təhlükəsizliyi üzrə tədbirlərin vətəndaşlara və biznes strukturlarına sosial təsirlərinin analizi, sosial-psixologiya qanunlarına əsaslanan hücum və müdafiə texnologiyalarının tədqiqi müasir cəmiyyətin vacib sosial tələbatına çevrilir.

Zərərli proqramlarda və istifadəçi-tərəf hücumlarda sosial mühəndislik üsulları geniş istifadə edilir [13]. Sosial mühəndislik sosiologiyanın sosial psixologiya nailiyyətlərinə əsaslanan nisbətən yeni sahəsidir. İnformasiya təhlükəsizliyi baxımından sosial mühəndislik − texniki vasitələr istifadə etmədən insanların hərəkətlərini idarəetmə metodudur. Bu metod insan faktorunun zəifliklərindən istifadəyə əsaslanır və çox dağıdıcı hesab edilir. Hazırda sosial mühəndislik İnternetdə konfidensial və ya çox qiymətli informasiyanın əldə edilməsi üçün tez-tez istifadə edilir və sosial mühəndisliyə çox zaman informasiyanın qanunsuz əldə edilməsi metodu kimi baxırlar. Lakin sosial mühəndislikdən təkcə informasiya əldə etmək üçün deyil, qanuni məqsədlər üçün də − konkret insan tərəfindən hərəkətlərin yerinə yetirilməsinə nail olmaq üçün də istifadə etmək olar.

Bədniyyətlilərin istifadə etdiyi sosial mühəndislik üsullarının analizi, bu növ hücumların aşkarlanması üsullarının işlənməsi, eləcə də informasiya sistemlərinin (və şəxslərin) sosial mühəndislik hücumlarına qarşı yoxlanılması metodikalarının işlənməsi aktualdır.

Daha bir tədqiqat mövzusu haker cəmiyyətlərinin sosiologiyasının öyrənilməsidir [14]. Hakerlərə çox zaman

patoloji fərdlər kimi baxırlar, lakin hakerlər sosial qruplar daxilində fəaliyyət göstərirlər, ekspertiza, dəstək, treninq ilə məşğul olurlar, jurnallar nəşr edirlər və elmi-praktiki konfranslarda çıxışlar edirlər.

Sosial media (sosial şəbəkələr, bloqlar və mikrobloqlar, forumlar, tanışlıq saytları, foto və video-hostinq, viki, geososial şəbəkələr, rəy saytları) İnternet vasitəsilə həyata keçirilən kütləvi kommunikasiya növüdür. KİV-lərin ənənəvi növlərindən bir sıra əhəmiyyətli fərqləri olsa da, ictimai rəyin idarə edilməsində kifayət qədər rol oynaya biləcəyini sübut etməkdədir. Sosial media özü ilə bir sıra ciddi informasiya təhlükəsizliyi problemləri gətirir [15], onların öyrənilməsi də aktual tədqiqat istiqamətlərindəndir.

VI. İNFORMASİYA TƏHLÜKƏSİZLİYİ VƏ PSİXOLOGİYA

Cəmiyyət həyatının bütün sahələrində, o cümlədən sosial proseslərdə informasiya texnologiyalarının geniş istifadəsi bir sıra sosial-psixoloji nəticələr doğurur, onların araşdırılması bir neçə istiqamətdə aparılır.

İnternet psixologiya və virtual icmaların psixologiyası [16] tədqiqatların yeni istiqaməti hesab edilir. Onlayn-oyunlara aludəçilik, İnternetdən izafi istifadə, kiberxondriya, İnternet asılılıq [17], yaddaşda Google effekti [18], şəxsiyyətin onlayn mühitdə normadan yayınan (ing. deviant) davranışları [16] və s. kimi hadisələrin tədqiqi, onların əlamətlərinin, prediktorlarının, diaqnostika üsullarının öyrənilməsi sahəsində bir çox tədqiqatlar mövcuddur [19].

Tədqiqatların ikinci qrupunu informasiya-psixoloji təhlükəsizlik problemləri təşkil edir. İnformasiya-psixoloji təsirlərin obyektləri fərdi, qrup və kütləvi şüurdur. Zərərli informasiya vasitəsilə informasiya istehlakçısının psixikasına onun iradəsinin əksinə və ya onun iradəsindən asılı olmadan neqativ psixoloji təsirlər həyata keçirilir, məqsəd insanların reallığı qeyri-adekvat qavramasına nail olmaqdır. İnformasiya-psixoloji təhlükəsizliyin təmin edilməsinin aşağıdakı ən vacib problemlərini diqqətə çatdırmaq olar [8,9,16-20]:

- milli mədəniyyətin, adət və ənənələrin qorunması;
- vətəndaş mövqeyi və vətənpərvərlik hisslərinin tərbiyəsi;
- informasiya-psixoloji təhlükəsizliyin təmin edilməsi sahəsində müvafiq dövlət siyasətinin, zəruri normativ hüquqi və texnoloji təminatın formalaşdırılması;
- ictimai şüurun formalaşdırılmasına məsul dövlət strukturlarının fəaliyyətinin koordinasiyası;
- insanların qlobal informasiya dəyişikliklərinə hazırlanması;
- informasiya mədəniyyətinin, o cümlədən media savadlılığının formalaşdırılması;
- İnternetdə, sosial şəbəkələrdə düzgün davranış, ünsiyyət etikasının formalaşdırılması;
- informasiya-psixoloji təsir mexanizmlərinin tədqiqi;
- koqnitiv proseslərin (diqqət, yaddaş, təfəkkürün) informasiya-psixoloji təhlükəsizliyə təsirlərinin öyrənilməsi;
- informasiya-psixoloji təhlükəsizlik sahəsində müvafiq monitorinq və ekspertizaların aparılması metodlarının işlənməsi;
- informasiya-psixoloji təhlükəsizlik üzrə kadrların hazırlanması problemləri.

İnformasiya təhlükəsizliyinə qəsd edən bədniyyətlilərin sosial-psixoloji xarakteristikasının qiymətləndirilməsi problemlərini də vurğulamaq olar. Bu aspektdə informasiya təhlükəsizliyi nəzəriyyəsinin kriminologiya ilə, onun tərkib elementləri: viktimologiya və bədniyyətlinin sosial-psixoloji portretinin formalaşdırılması nəzəriyyəsi ilə əlaqəsi vardır.

VII. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN KULTUROLOJİ PROBLEMLƏRİ

İnformasiya təhlükəsizliyi problemlərinin həlli texniki 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 mədəniyyətinin formalaşdırılması və inkişafı problemləri çərçivəsində aşağıdakı tədqiqat mövzularına baxılır [21,22]:

- informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması sahəsində dövlət siyasətinin əsas istiqamətləri;
- əhalinin 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;
- informasiya texnologiyaları və informasiya təhlükəsizliyi sahəsində etika problemləri.

Müasir kulturologiya sahəsində *haker submədəniyyətinin* öyrənilməsi nisbətən az tədqiq olunmuş sahələrdən biridir [23]. Submədəniyyət ictimai mədəniyyətin öz davranışı ilə dominant mədəniyyətdən fərqlənən hissəsidir. Dar mənada bu termin sosial qrupu – submədəniyyət 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 aktual deyil. Bu tədqiqatlar mədəniyyətdə və onun müxtəlif sosio-mədəni seqmentlərində innovasiya proseslərini analiz etməyə imkan verə bilən yeni nəzəri-metodoloji bazanın yaradılması baxımından da aktualdır.

VIII. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN İQTİSADİ PROBLEMLƏRİ

İnformasiya təhlükəsizliyi məsələlərinə iqtisadi elmlər istiqamətlərində baxılmasının zəruriliyi informasiyanın iqtisadiyyatda artan rolu, dövlətin və təşkilatların iqtisadi maraqlarının qorunması zəruriliyi ilə şərtlənir. İnformasiya təhlükəsizliyi aqressiv bazar iqtisadiyyatı şəraitində biznesin zəruri aspektlərindən biri kimi çıxış edir.

İnformasiya təhlükəsizliyinin pozulması bir çox halda qanunsuz qazanc əldə edilməsinə yönəlir və sosial-iqtisadi sistemləri hədəf alır – kommersiya və maliyə məlumatlarının oğurlanması, təhrif edilməsi, intellektual mülkiyyətin oğurlanması, sənaye casusluğu, təşkilatın nüfuzuna ziyan vuran materialların yayılması və s.

Qeyd edək ki, informasiya təhlükəsizliyinin təmin edilməsi iqtisadi baxımdan səmərəlilik yanaşması əsasında həyata keçirilir − informasiya təhlükəsizliyi sisteminin qurulması və istismarı xərcləri informasiya təhlükəsizliyi risklərindən potensial mümkün itkilərlə müqayisə edilir.

İnformasiya təhlükəsizliyinin iqtisadi problemləri çərçivəsində aşağıdakı tədqiqat mövzuları aktualdır (siyahı bunlarla məhdudlaşmır) [24,25]:

- 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.

NƏTİCƏ

Dnamik inkişaf edən qlobal informasiya cəmiyyəti şəraitində informasiya təhlükəsizliyinin təmin edilməsində insanla əlaqəli faktorların (təşkilati, mədəni, iqtisadi və sosial) rolu artır və informasiya təhlükəsizliyi texnologiyalarının inkişaf vektorlarını düzgün müəyyən etmək üçün müxtəlif humanitar və ictimai elmlərin konseptual yanaşmalarını və alətlərini cəlb etmək lazım gəlir. Bu işdə mövcud ədəbiyyatın icmalı əsasında humanitar və ictimai elmlər baxımından informasiya təhlükəsizliyi sahəsində aktual elmi-tədqiqat problemləri müəyyən edilmişdir. İnformasiya müharibələri səhnəsinə çevrilən informasiya fəzasında müasir çağırışlara və təhlükələrə hazır olmaq, bu sahədə şəxsiyyətin, cəmiyyətin və dövlətin balanslaşdırılmış maraqlarını etibarlı qorumaq üçün informasiya təhlükəsizliyinin humanitar problemləri sahəsində geniş multidissiplinar elmi-tədqiqatların aparılması zəruridir.

ƏDƏBİYYAT

[1] H. Thompson, “The human element of information security,” IEEE Security & Privacy, vol. 11, no. 1, pp. 32-35, Jan.-Feb. 2013.

[2] R. M. Əliquliyev, Y. N. İmamverdiyev, F. F. Yusifov, “Cəmiyyətin informasiya təhlükəsizliyinə dair bəzi konseptual baxışlar,” İnformasiya cəmiyyəti problemləri, №2(4), s.3-9, 2011.

[3] R. M. Əliquliyev, Y. N. İmamverdiyev, “E-dövlətin informasiya təhlükəsizliyi: Aktual tədqiqat istiqamətləri,: İnformasiya cəmiyyəti problemləri, 2010, №1, s. 3-13.

[4] 2014 Data Breach Investigations Report (DBIR). Verizon. 2014. http://www.verizonenterprise.com/DBIR/2014/

[5] Special Eurobarometer 404. Cyber Security. 2013. http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf

[6] J. Lindsay. “China and Cybersecurity: Political, Economic, and Strategic Dimensions.” 2012.

[7] P. Cornish, Cyber security and politically, socially and religiously motivated cyber attacks. Brussels: European Parliament. 2009.

[8] К. К. Колин “Гуманитарные проблемы информационной безопасности,” Приложение к журналу “Информационные технологии”, №12, 2007.

[9] Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. М. : Горячая линия–Телеком, 2009. 320 с.

[10] T. J. Smedinghoff, “The State of Information Security Law: A Focus on the Key Legal Trends,” The EDP Audit, Control, and Security Newsletter, vol. 37, no. 1-2, pp. 1-52, 2008.

[11] J. L. Grama, Legal issues in information security. Jones & Bartlett Learning, 2010.

[12] R. M. Əliquliyev, R. Ş. Mahmudov, İnternetin tənzimlənməsi problemləri. Ekspress informasiya. İnformasiya cəmiyyəti seriyası, Bakı: “İnformasiya Texnologiyaları” nəşriyyatı, 2010. - 115 s.

[13] C. Hadnagy, Social Engineering: The Art of Human Hacking. 2010.

[14] T. Jordan, P. Taylor, “A sociology of hackers,” The Sociological Review, vol. 46, no. 4, pp. 757-780, 1998.

[15] W. Ashford, “Social media: A security challenge and opportunity,” Computer Weekly, 2013.

[16] A. N. Joinson, K. Y. A. McKenna, T. Postmes, U.-D. Reips (ed.). Oxford handbook of Internet psychology. Oxford Uni. Press, 2007.

[17] R. M. Əliquliyev, R. Ş. Mahmudov, İnformasiya asılılığı problemləri və onlarla mübarizə yolları. Ekspress informasiya. İnformasiya cəmiyyəti seriyası, Bakı: “İnformasiya Texnologiyaları” nəşriyyatı, 2009. - 62 s.

[18] B. Sparrow, J. Liu, D. M. Wegner, “Google effects on memory: Cognitive consequences of having information at our fingertips,” Science, vol. 333, pp. 776-778, 2011.

[19] H. Cash, C. D. Rae, A. H. Steel, A. Winkler, “Internet addiction: a brief summary of research and practice,” Current Psychiatry Review, vol. 8, no. 4, pp. 292–298, 2012.

[20] İ. Y. Ələkbərova, “İnformasiya müharibəsi texnologiyalarının analizi və təsnifatı,” İnformasiya cəmiyyəti problemləri, №2, s.80-91, 2010.

[21] R. Ş. Mahmudova, İnformasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması problemləri, Azərbaycan xalqının ümummilli lideri Heydər Əliyevin 90 illik yubileyinə həsr olunmuş “İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı”, 17-18 may, 2013, s.22-25.

[22] A. da Veiga, N. Martins, J. H. P. Eloff, “Information security culture – validation of an assessment instrument,” Southern African Business Review, vol. 11, no. 1, pp. 147-166, 2007.

[23] T. J. Holt, D. Strumsky, O. Smirnova, M. Kilger, “Examining the social networks of malware writers and hackers,” International Journal of Cyber Criminology,vol. 6, no. 1, pp. 891-903, 2012.

[24] M. E. Johnson, E. Goetz, “Embedding information security into the organization,” IEEE Security and Privacy Magazine, vol. 5, no. 3, pp. 16-24, 2007.

[25] W. S. Baer, A. Parkinson, “Cyberinsurance in IT security management,” IEEE Security and Privacy Magazine, vol. 5, no. 3, pp. 50-56, 2007.