UOT 004.056.5 DOI: 10.25045/jpis.v12.i2.06

Mahmudova R.Ş.[1], Daşdəmirova K.Q.[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]rasmahmudova@gmail.com, [2]konulahmed@gmail.com

İNFORMASİYA CƏMİYYƏTİ MÜHİTİNDƏ BƏZİ İNFORMASİYA TƏHLÜKƏSİZLİYİ PROBLEMLƏRİNİN ANALİZİ

Hazırda əhalinin böyük hissəsi informasiya-kommunikasiya texnologiyalarından istifadə etməklə vitrual mühitə inteqrasiya olunur və informasiya cəmiyyətinin vətəndaşına çevrilir. Cəmiyyətdə informasiyanın, informasiya resurslarının və texnologiyalarının rolunun artması informasiya cəmiyyətində şəxsin, cəmiyyətin, dövlətin maraqlarının qorunması və informasiya təhlükəsizliyinin təmin olunması zəruriyyətini önə çıxarır. Tədqiqat işində informasiya cəmiyyəti mühitində şəxsin, cəmiyyətin və dövlətin maraqlarına təsir göstərə bilən təhdidlər analiz olunmuş, informasiya təhlükəsizliyinin əsas prinsipləri, onun təmin edilməsinin bəzi metodları tədqiq edilmişdir. İnformasiya təhlükəsizliyinin təmin edilməsi sahəsində xarici ölkələrin təcrübəsi araşdırılmış, Azərbaycanda informasiya təhlükəsizliyinin hüquqi təminatı sahəsində görülmüş işlər və aparılan elmi-nəzəri tədqiqatlar araşdırılmışdır. Tədqiqat işində müqayisəli analiz, monitorinq, təsnifatlandırma kimi tədqiqat metodlarından istifadə olunmuşdur. Tədqiqatdan əldə edilən ilkin nəticələr informasiya cəmiyyəti mühitində informasiya təhlükəsizliyi problemlərinin daha geniş tədqiq olunması üçün faydalıdır və informasiya təhlükəsizliyi problemlərini araşdıran tədqiqatçılar tərəfindən mənbə kimi istifadə oluna bilər.

Açar sözlər: *informasiya cəmiyyəti, informasiya təhlükəsizliyi, kibertəhlükəsizlik, sosial mühəndislik, fişinq, informasiya müharibəsi.*

Giriş

XX əsrin ortalarına qədər informasiyanın ötürülməsi, saxlanılması və emalı kağız daşıyıcılar üzərində həyata keçirilirdi. İnformasiya-kommunikasiya texnologiyalarının (İKT) inkişafı informasiyanın ötürülməsi, saxlanılması və emalı üçün yeni üsulların meydana çıxmasına səbəb oldu. IV informasiya inqilabının nəticəsi kimi informasiya cəmiyyəti formalaşmağa başladı. İnformasiya cəmiyyəti əhalinin böyük hissəsinin müasir informasiya texnologiyalarından istifadə etməklə informasiyanın saxlanması, emalı və ötürülməsi ilə məşğul olan bir cəmiyyətdir. Onun əsas hərəkətverici qüvvəsi təhsil, iqtisadiyyat, səhiyyə və s. sahələrin sürətli inkişafına təsir göstərən İKT-dir [1]. Bu cəmiyyətdə informasiya və biliklər ən mühüm resurs və başlıca əmtəədir.

İnformasiya cəmiyyətinə keçid ölkələrin sərbəst seçimi deyil, cəmiyyətin inkişafı üçün zəruri bir prosesdir. Hazırda insan fəaliyyətinin bütün sahələrində İKT-nin tətbiqi sosial inkişafın vacib elementi hesab edilir. Lakin İKT-nin qlobal səviyyədə tətbiqi bir çox problemlərin kəskinləşməsinə gətirib çıxardı. Cəmiyyətdə informasiyanın, informasiya resurslarının və texnologiyalarının rolunun artması informasiya təhlükəsizliyinin təmin olunması zəruriyyətini önə çıxardı. İnformasiya və dezinformasiyanın bəzən təhlükəli silaha çevrilə biləcəyini nəzərə alsaq, cəmiyyətin sabitliyini pozmağa yönəlmiş zərərli informasiyanın qarşısının alınması ölkənin, millətin, xalqın və hər bir vətəndaşın yaşam tərzinin, sabitliyin qarantıdır. Bu səbəbdən İnformasiya təhlükəsizliyi milli təhlükəsizlik sisteminin ən mühüm komponentlərindən biridir [2]. İnformasiya təhlükəsizliyi informasiyanın və informasiya mühitinin təsadüfi və ya düşünülmüş təbii və ya süni xarakterli təsirlərdən müdafiə vəziyyətidir. Belə təsirlər informasiyaya və ya informasiya obyektlərinə, həmçinin informasiya istifadəçisinə və sahibinə yolverilməz ziyanlar vura bilir.

Müasir dünyada informasiyanın qorunması əsas vəzifələrdən biridir. Dövlət sirlərinin açıqlanması dövlətin milli təhlükəsizliyinin pozulmasına, kommersiya sirrinin açıqlanması

təşkilatın müflisləşməsinə, fərdi məlumatların açıqlanması informasiya sahəsində şəxsiyyətin maraqlarının pozulmasına gətirib çıxara bilər.

İnformasiya cəmiyyətində informasiya təhlükəsizliyi problemləri

Kibernetikanın və süni intellektin yaradıcılarından biri olan Norbert Viner hesab edirdi ki, informasiya özünəməxsus xüsusiyyətlərə malikdir, nə enerjiyə, nə də maddəyə aid edilə bilməz [3]. İnformasiya – alınan, ötürülən və müxtəlif mənbələrdə saxlanılan hər hansı bir məlumatdır [4]. İnformasiya cəmiyyətinin xüsusiyyəti ondan ibarətdir ki, informasiya mühitindəki məlumat və biliklər cəmiyyətin və dövlətin inkişafı üçün əsas strateji mənbəyə çevrilərək xüsusi bir status qazanır [5]. Bu səbəbdən, cəmiyyətin müxtəlif sahələrində (siyasət, iqtisadiyyat, mədəniyyət və s.) müxtəlif səviyyələrdə (beynəlxalq, dövlət, ictimai) informasiyaya çıxış üçün rəqabət mübarizəsi gedir. İctimai həyatın müxtəlif sahələrinə getdikcə daha dərindən nüfuz edən müasir informasiya texnologiyaları yalnız fərdlərin şüuruna və davranışına deyil, eyni zamanda fərdin və cəmiyyətin ümumi həyat tərzinə, qarşılıqlı münasibətlərin mahiyyətinə, habelə iqtisadiyyat, siyasət, mədəniyyət, təhsil və s. sahələrin inkişafına müsbət təsir göstərir. 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 sosial inkişafı və onun milli təhlükəsizliyi fərdlərin, sosial qrupların, təşkilatların və dövlətlərin fəaliyyət göstərdiyi informasiya məkanında hansı məlumatların üstünlük təşkil etməsindən (siyasi, elmi, əyləncə və s.) və informasiya mühitinin təhlükəsizliyindən asılı olmağa başlayır.

İnformasiya cəmiyyəti mühitində informasiya təhlükəsizliyinə yönəlmiş bir neçə əsas təhdid mənbələri mövcuddur. Təhdid informasiya sahibinin maraqlarına ziyan vurmağa yönəlmiş hadisə, şərait, hərəkət, proses və s. ola bilər [6]. Təhdidlər şəxsin, cəmiyyətin və dövlətin maraqlarına təsir göstərə bilər [7].

Şəxsin maraqlarına yönəlmiş təhdid mənbələri. Bəşəriyyət informasiya infrastrukturunun insanlar üçün ən əsas məlumat mənbəyinə çevrildiyi sərhədə yaxınlaşır, bu isə insanların əqli fəaliyyətinə, sosial davranışının formalaşmasına birbaşa təsir göstərir. Bu səbəbdən, informasiya mühitində şəxsin maraqları qorunmalı, informasiya təhlükəsizliyi təmin olunmalıdır. Şəxsin maraqları dedikdə, onun hüquq və azadlıqlarının, təhlükəsizliyinin, fiziki, mənəvi, intellektual inkişafı üçün şəraitinin təmin edilməsi, rifahının yüksəldilməsi nəzərdə tutulur. Şəxsin informasiya təhlükəsizliyi insanı əhatə edən informasiya fəzasına təsir etmək yolu ilə onun şəxsiyyətinə əhəmiyyətli dərəcədə ziyanın vurulmasının mümkün olmadığı vəziyyət hesab olunur [8].

Şəxsin maraqlarının qorunması istiqamətində bir sıra tədbirlər görülməlidir. İlk növbədə, hər kəsin informasiya əldə etməsi üçün konstitusiya hüququ və azadlıqları təmin edilməli, topladıqları məlumatları qanunla qadağan olunmayan fəaliyyət və sahələrdə istifadə etmək imkanı olmalıdır. Eyni zamanda, insanların şəxsi təhlükəsizliyini, mənəvi və intellektual inkişafını təmin edən məlumatların qorunması təmin olunmalıdır.

Şəxsin maraqlarına təsir göstərə bilən bir sıra təhdidlər mövcuddur. Bunlardan ən təhlükəli təhdid mənbəyi fərdin ətrafında "virtual informasiya məkanı" formalaşdırmaqla insanın şüurunu idarə etmək, həmçinin onun əqli fəaliyyətinə təsir göstərən texnologiyalardan istifadə etmək imkanıdır. Müasir texnologiyalardan istifadə etməklə lazım olan informasiya mənbələrinə giriş prosedurları insanın İKT mütəxəssislərindən asılılığını xeyli dərəcədə artırır. Çünki İKT mütəxəssisləri informasiya texnologiyalarını inkişaf etdirərək, insanın axtardığı məlumatların tapılması üçün axtarış alqoritmləri hazırlayır, seçilmiş məlumatları qavrayış üçün əlverişli formaya gətirir və istehlakçıya təqdim edir. Bu İKT mütəxəssisləri insanın həyatının informasiya fonunu təşkil edir, onun fəaliyyət göstərdiyi şəraiti qiymətləndirir və onu müəyyən bir istiqamətə yönəldir. Buna görə də insanların informasiya infrastrukturu ilə qarşılıqlı əlaqəsinin təhlükəsizliyini təmin etmək son dərəcə vacibdir [7].

Sosial mühəndislik (Social engineering, Human hacking) şəxsin maraqlarına təsir göstərə bilən daha bir təhdid növüdür [9]. Sosial mühəndislik bədniyyətlilərin insanlarla qarşılıqlı əlaqədə olaraq onlardan məlumat toplanması texnologiyasıdır. Bu təhdidin əsas amillərindən biri saxta profillərdən, virtual dostluq və tanışlıqdan istifadə edərək sonradan ziyan vurmaq məqsədi ilə insanların şəxsi həyatı haqqında məlumatların toplanmasıdır. Belə ki, toplanmış məlumatlar fərdin istifadə etdiyi şifrələrin, biometrik göstəricilərin və digər məxfi informasiyanın tapılmasını, ələ keçirilməsini asanlaşdırır. Bu təhlükədən qorunmaq üçün istifadəçi öz fərdi məlumatlarını kənar şəxsə verməməli, kimə ötürdüyündən əmin olmalı, virtual dostluq etdiyi şəxslə ehtiyatlı davranmalıdır.

"Brute-force" - istifadəçi hesablarına qarşı yönəlmiş və ən geniş yayılmış hücum növlərindən biridir. Belə bir hücumun məqsədi verilənlər bazasının idarəetmə panelinə və istifadəçi hesabına daxil olmaq üçün loqin və şifrə tapmaqdır. Təcavüzkarlar, xüsusilə, zəif xüsusiyyətli istifadəçilərdən faydalanırlar. Onların e-poçt və ya digər hesablarındakı şifrələr toplusuna hücumlar edilir. Ən çox istifadəçiyə aid fərdi məlumatlardan (ad, soyad, doğum tarixi, maşın nömrəsi, telefon nömrəsi, yaşadığınız yer, valideyn və ya övladınızın adı və doğum tarixləri və s.) istifadə edərək manual (əl ilə bir-bir) və ya avtomatik şəkildə müxtəlif vasitələrlə hesablarındakı şifrələr yoxlanılır və şifrə tapılır. Bu metoddan əvvəl bədniyyətlilər hədəf istifadəçiyə sosial mühəndislik metodunu tətbiq edərək kifayət qədər məlumat toplaya bilərlər [10].

"Brute-force" köhnə hücum metodu olsa da, hələ də effektivdir və hakerlər tərəfindən geniş istifadə olunur. Şifrənin uzunluğundan və mürəkkəbliyindən asılı olaraq onun qırılması bir neçə saniyədən uzun illərə qədər davam edə bilər. Bu hücumdan qorunmaq üçün şifrələrin təhlükəsizliyi qaydalarına əməl edilməlidir [11].

İstifadəçinin kompüterini zərərverici proqramlar vasitəsilə yoluxdurma texnikası şəxsin maraqlarına yönəlmiş daha bir təhdid növüdür [12]. Bədniyyətlinin məqsədi zərərverici yoluxdurma texnikası vasitəsilə (saxta video, şəkil, musiqi, kino, reklam banneri və s. linklərdən istifadə edərək) istifadəçinin kompüterinə ziyanverici proqramların yüklənməsinə nail olmaq və informasiyanı məhv etmək, dəyişdirmək, nəzarətdə saxlamaq və ya oğurlamaqdır. Ziyanverici proqramlar kompüterə yükləndikdən sonra kompüterin yaddaşında gizlənir və gizli əməliyyatları arxa fonda yerinə yetirir. Bu halda istifadəçinin kompüteri ikinci şəxs tərəfindən idarə olunur və materialları, məlumatları, şəxsi şəkilləri, video-faylları və s. hətta kompüterinin kamerası istifadəçinin xəbəri olmadan istifadə edilə bilər. Belə kompüterlər zombi kompüterlər adlanır və fərdi məlumatların ələ keçirilməsi üçün geniş şəkildə istifadə olunur.

Bu təhlükədən qorunmaq üçün antivirus proqramından istifadə edilməli və bu proqram daim yenilənməlidir. Həmçinin istifadəçi elektron ünvanına gələn tanımadığı məktubları açarkən, müxtəlif linkləri, sənəd və digər faylları yükləyərkən ehtiyatlı olmalı, kompüterində hər hansı anomaliya baş verərsə ziyanverici proqramın olması ehtimalını nəzərdən keçirməlidir.

Daha bir informasiya təhlükəsizliyi təhdidlərindən biri fişinqdir ("phishing" – balıq ovu). Fişinq – istifadəçilərin konfidensial məlumatlarına qeyri-qanuni çıxış əldə etmək məqsədilə törədilən internet fırıldaqçılıq növlərindən biridir [13]. Bu metod vasitəsi ilə gizli istifadəçi məlumatlarına - login və şifrələrə giriş əldə edilir. Haker istifadəçini müxtəlif yollarla adı eyni olan, lakin saxta sayta və ya digər resursa yönəldərək apardığı bütün əməliyyatları izləyir və istifadəçinin bank kredit kartının məlumatlarını, İD nömrəsini, e-mail ünvanını və s. məlumatları əldə edir. Bu təhlükədən qorunmaq üçün istifadəçi yönləndirilmış saytda ondan tələb olunan bank kredit kartı, bank hesabı və bu kimi məxfi məlumatları tələb edən sorğulardan şübhələnməli və etibarlı mənbələrdən istifadə etməlidir.

Cəmiyyətin maraqlarına yönəlmiş təhdid mənbələri. İnformasiya məkanında olan neqativ informasiya, feyk xəbərlər, cəmiyyətin müxtəlif təbəqələrinə yönəlmiş qərəzli məlumatlar cəmiyyətin ictimai stabilliyi, birliyi, rifahı üçün ciddi problemlər yaradır [7]. Neqativ məlumatların yayılması məqsədi və qaynaqlarının aşkarlanması, cəmiyyətin maraqlarının qorunması ölkə vətəndaşlarının stabil yaşam tərzinin təmin edilməsinin əsasıdır. Cəmiyyətin maraqları – onun

demokratikləşdirilməsi, hüquqi və dünyəvi dövlətin qurulması prosesinin davam etdirilməsi, ictimai sabitliyin, milli həmrəyliyin yaranmasını və qorunub saxlanılmasını, mədəni, tarixi, milli, mənəvi dəyərlərlərin qorunmasını və inkişaf etdirilməsini özündə ehtiva edir. Cəmiyyətin informasiya təhlükəsizliyinin təmin olunması dövlətlərin prioritet sahələrindən biridir. Cəmiyyətin informasiya təhlükəsizliyi – cəmiyyətin informasiya mühitinə təsir etmək yolu ilə ona əhəmiyyətli dərəcədə ziyan vurulmasının mümkün olmadığı vəziyyətdir [8].

İnformasiya mühitində cəmiyyətin maraqlarına yönələn əsas təhdid mənbələrindən biri cəmiyyətin həyatını təmin edən vacib infrastrukturların informasiya sistemlərinə və rabitə şəbəkələrinə yönəlmiş hücumlardır. Bu təhdidlər həm qəsdən (cinayət strukturları və cinayət ünsürləri tərəfindən törədilə bilən), həm də təsadüfi (səhvlər, aparat və proqram təminatlarının nasazlıqları nəticəsində) meydana çıxa bilər. Bu təhdidlərin obyektləri enerji, nəqliyyat, boru kəməri və digər infrastrukturların informasiya sistemləri ola bilər.

Yeni media vasitələrinin hər hansı bir qrup şəxslərin əlində cəmləşməsi də cəmiyyətin maraqlarına yönəlmiş çox təhlükəli bir təhdid mənbəyidir [14]. İnformasiya güc siyasətinin aləti kimi beynəlxalq siyasi təşkilatlar, ölkədaxili və xarici siyasi qurumlar, terror təşkilatları tərəfindən istifadə edilə bilər. Bu təhdidlər müəyyən ictimai əhəmiyyət kəsb edən hadisələrlə bağlı ictimai rəyin manipulyasiyası, eləcə də yad dəyərləri təbliğ etməklə cəmiyyətin mənəvi əsaslarının məhv edilməsi şəklində özünü göstərə bilər.

Cəmiyyətin maraqlarına yönəlmiş təhdid mənbələrindən biri də intellektual fəaliyyət məhsulları üçün daxili və xarici bazarlarda rəqabətin artmasıdır. Bu təhlükə özünü rəqabət miqyasının genişlənməsi, əqli mülkiyyət hüquqlarının pozulması şəklində göstərə bilər.

Cəmiyyətin maraqlarına yönəlmiş daha bir təhlükə mənbəyi yerli və beynəlxalq kompüter cinayətlərinin genişlənməsidir. Təhdidlər özlərini qlobal və ya yerli informasiya və telekommunikasiya sistemlərindən istifadə edərək saxta əməliyyatlar həyata keçirmək cəhdləri, qanunsuz vəsaitlərin yuyulması, şəxsi mənfəət üçün istifadə edilə bilən maliyyə, bank və digər məlumatlara qeyri-qanuni giriş əldə etmək cəhdləri şəklində göstərə bilər [7].

Dövlətin maraqlarına yönəlmiş təhdid mənbələri. İnformasiya mühitində şəxsin, cəmiyyətin və dövlətin balanslaşdırılmış maraqlarının məcmusu dövlətin informasiya təhlükəsizliyini təşkil edir. Dövlətin informasiya təhlükəsizliyi milli maraqlarının qorunmasının, ölkənin informasiya infrastrukturunun harmonik inkişafının, siyasi və sosial sabitliyin, iqtisadi rifahın, beynəlxalq əməkdaşlığın inkişafının əsasıdır [7]. Dövlətin maraqları onun müstəqilliyinin, suverenliyinin, konstitusiya quruluşunun, ərazi bütövlüyünün qorunmasından, siyasi, iqtisadi və sosial stabilliyin, qanunların aliliyinin təmin edilməsindən, beynəlxalq əməkdaşlığın inkişaf etdirilməsindən ibarətdir [8]. Dövlətin informasiya təhlükəsizliyi – dövlətin informasiya mühitinə təsir etmək yolu ilə ona əhəmiyyətli dərəcədə ziyan vurulmasının mümkün olmadığı vəziyyətdir.

İnformasiya mühitində dövlətin maraqlarına yönəlmiş ən təhlükəli təhdidlərdən biri "informasiya silahları"nın nəzarətsiz yayılması, bu sahədə silahlanmanın təşkili və sürətlənməsi, "informasiya müharibələri" aparmaq konsepsiyalarının həyata keçirilməsinə cəhdlərdir.

İnformasiya silahları qarşı tərəfin informasiya infrastrukturunu, informasiya resurslarını nəzarətdə saxlamaq və ya məhv etmək üçün istifadə edilən vasitə, metod və texnologiyalar məcmusudur. Həmçinin informasiya silahları insanların davranışını nəzarətdə saxlamaq üçün istifadə edilir [8]. Bu səbəblərdən informasiya silahlarının informasiya cəmiyyətindəki dağıdıcı təsiri daha güclü və təsirli ola bilər. Bu, dünyanın az sayda ölkəsinin şirkətlərinin informasiya məhsulları bazarında inhisarçı olması şəraitində xüsusilə təhlükəlidir. Müəyyən siyasi məqsədlərə nail olmaq üçün mövcud üstünlükdən istifadə etmək istəyi yarada bilər.

Dövlətin maraqlarına yönəlmiş təhdidlərdən biri də informasiya mühitində terrorizm və ekstremizm təhdidləridir. Kiber terror terrorizmin nisbətən yeni bir forması olaraq, ənənəvi terror hücumlarından öz məqsədlərinə nail olmaq və zorakılıq ideologiyasını həyata keçirmək yolları ilə fərqlənir. Kiberterrorizm – həm ayrı-ayrı ölkələrin, həm də bütün beynəlxalq birliyin təhlükəsizliyi və sabitliyinə yönəlmiş təhdiddir. Terrorizm və ekstremizm təhdidləri yalnız kiberməkanla

məhdudlaşmır, real dünyanın obyektlərinə: əhalinin həyat təminatı üçün xüsusi sistemlərə, vətəndaşların həyatı və sağlamlığına, müxtəlif infrastrukturlara və s. təsir göstərir [15]. Kiberterrorizmin əsas əlamətləri aşağıdakılardır [16]:

- beynəlxalq xarakterli olması, cinayətkarın qurbanlarının fərqli ölkələrdə olması;
- gizlilik səviyyəsinin yuxarı, aşkarlanma səviyyəsinin aşağı olması;
- əhəmiyyətli maliyyə xərclərinin olmaması, lakin böyük maddi və mənəvi ziyan vurmaq imkanı;
- açıqlıq – terrorçuların bütün fəaliyyətinin cəmiyyətin diqqətini cəlb edilməsinə yönəlməsi.

Dövlətin maraqlarına yönəlmiş təhdidlər kibercasusluq şəklində də özünü göstərə bilər. Kibercasusluq kompüter proqramları vasitəsilə dövlət sirri təşkil edən məlumatlara, açıqlanması dövlətin mənafelərinə zərər verə biləcək məxfi məlumatlara, həmçinin şəxsin və hüquqi şəxsin qapalı məlumatlarına qanunsuz giriş əldə etmək imkanıdır. Kibercasusluq zamanı terrorçular tərəfindən məqsədli haker hücumları həyata keçirilir. Bu hücumlar sənaye müəssisələrinə, tibb müəssisələrinə, hərbi və atom sahəsinin infrastrukturuna yönələ və bu müəssisələrin təchizat və təhlükəsizlik sistemlərinin sıradan çıxmasına səbəb ola bilər [17].

İnformasiya təhlükəsizliyinin əsas prinsipləri

Elektron informasiya insanların, sosial qrupların, cəmiyyətlərin, təşkilatların mülkiyyət və konfidensiallıq hüquqlarının qorunmasını çətinləşdirən bir texnoloji yenilik meydana gətirib. Dünyada getdikcə daha çox informasiya İnternet şəbəkəsinə ötürülür və istifadəçilərin fərdi məlumatları, geoməlumatları asanlıqla izlənilə bilir [18]. Müasir şəbəkə texnologiyaları isə bu məlumatların adekvat qorunmasını tam təmin edə bilmir. Çünki İnternet müasir, vacib informasiya mənbəyi olmasına baxmayaraq, etibarlılıq, funksionallıq, konfidensiallıq və bütövlük kimi mühüm xüsusiyyətlərlə yetərincə təmin olunmayıb [19]. Bu səbəbdən, informasiyanın təhlükəsizliyinin təmin olunması qlobal informasiya cəmiyyətinin prioritet məsələlərindən biridir. İnformasiya təhlükəsizliyi informasiyanın və ona xidmət edən infrastrukturun təbii və ya süni xarakterli, təsadüfi və ya qəsdli təhdidlərdən mühafizəsini nəzərdə tutur.

İnformasiyanın təhlükəsizliyinin pozulmasının bütün mümkün halları əsasən üç kateqoriyaya bölünür [20]:

- informasiyanın konfidensiallığının pozulması;
- informasiyanın tamlığının pozulması;
- informasiyanın əlçatanlığının pozulması.

İnformasiyanın konfidensiallığın pozulması təhlükələri konfidensial informasiyanın və ya məxfi sirlərin açılmasına yönəlmişdir. Bu növ təhlükələr reallaşdıqda informasiyaya giriş bədniyyətlilərin əlinə keçə bilər. Kompüter sistemlərində və şəbəkələrdə saxlanılan və ya ötürülən informasiyaya icazəsiz girişin əldə olunması onun konfidensiallığının pozulması ilə nəticələnə bilər.

İnformasiyanın tamlığının pozulması təhlükələri informasiyanın saxlanılması və ya ötürülməsi zamanı meydana çıxa bilər. Bu zaman informasiyanın təhrif olunması, keyfiyyətinin pozulması və ya məhvinə gətirib çıxaran dəyişikliklərin edilməsi mümkündür. İnformasiyanın tamlığı bədniyyətlilər tərəfindən qəsdən və ya ətraf mühitin obyektiv təsirləri nəticəsində pozula bilər.

Əlçatanlığın pozulmasına yönələn təhdidlər kompüter sistemlərinin və şəbəkələrinin iş qabiliyyətinin zəifləməsinə, fəaliyyətinin pozulmasına, informasiya resursuna qanuni girişin məhdudlaşdırılmasına və ya tamamilə dayandırılmasına səbəb ola bilər. Bu təhdidlər qəsdən törədilə və ya təsadüfi hadisə və proseslər nəticəsində baş verə bilər.

İnformasiya təhlükəsizliyinin təmin edilməsi metodları

İnformasiya təhlükəsizliyinin təmin edilməsi problemini həll etmək üçün hüquqi, təşkilati, texnoloji, mənəvi-etik metodlar tətbiq edilir [21]. Bu metodlar aşağıdakı istiqamətlərə yönəlmişdir [22]:

- məlumatların icazəsiz girişdən, məhv olmadan, dəyişdirmədən, bloklanmadan, surətinin çıxarılmasından, yayılmasından, həmçinin məlumatlarla əlaqəli digər qanunsuz hərəkətlərdən qorunmasının təmin edilməsi;
- məhdud giriş olan məlumatların konfidensiallığına riayət edilməsi;
- qanuni istifadəçilər üçün məlumat əldə etmək hüququnun təmin edilməsi.

İnformasiyanın hüquqi metodlarla mühafizəsi – informasiyanın hüquqi üsullarla qorunmasını, informasiyanın mühafizəsi üzrə subyektlərin münasibətlərini tənzimləyən qanunvericilik və normativ hüquqi sənədlərin işlənib hazırlanmasını, tətbiqini, habelə onların icrasına nəzarəti özündə ehtiva edir [23].

İnformasiyanın təşkilati metodlarla mühafizəsi – informasiya emalı sistemlərinin iş proseslərinin reqlamentləşdirilməsi, informasiya resurslarının istismarı, əməkdaşların fəaliyyəti, təhdidlərin baş verməsi ehtimalını maksimum dərəcədə çətinləşdirmək və ya aradan qaldırmaq, həmçinin onların icrası zamanı mümkün zərərlərin miqdarını azaltmaq üçün təşkilatın istifadəçiləri və işçilərinin informasiya sistemləri ilə qarşılıqlı əlaqə qaydalarını ehtiva edir [24]. İnformasiyanın mühafizəsinin təşkilati metodları informasiyanın hüquqi metodlarla mühafizəsi ilə sıx bağlıdır. Qanunlara və normativ aktlara uyğun olaraq nazirliklərdə, idarə və müəssisələrdə informasiyanın qorunması üçün xüsusi təhlükəsizlik xidmətləri yaradılır. Bu xidmətlər müəssisənin rəhbərliyinin tabeliyində fəaliyyət göstərir, informasiyanın mühafizəsi sistemlərinin yaradılmasını və fəaliyyətini təşkil edirlər [25].

İnformasiyanın texnoloji metodlarla mühafizəsi – xüsusi proqram və aparat vasitələrindən istifadə etməklə məlumatların qorunmasının texnoloji üsullarını ehtiva edir. Texnoloji metodlar məlumatlara və mənbələrə icazəsiz girişi, məlumat və resurslardan qeyri-qanuni istifadəni, onların oğurlanması ehtimalını proqnozlaşdırmaq, izləmək və qarşısını almaq üçün tətbiq edilir [26].

Mənəvi-etik metodlar – informasiya ilə davranış norma və qaydalarını ehtiva edir. Bu normalar və qaydalar cəmiyyətdə kompüterlərin yayılması nəticəsində ənənəvi olaraq formalaşmış və inkişaf etmişdir. Bu normalar əksər hallarda qanuni qaydalar kimi məcburi deyildir. Lakin onlara riayət edilməməsi insanın, bir qrup şəxsin və ya təşkilatın nüfuzunun azalmasına gətirib çıxarır. Mənəvi-etik normalar həm yazılmamış, məsələn, hamılıqla qəbul edilmiş düzgünlük normaları, həm də yazılı, müəyyən bir qayda və ya nizamnamədə tərtib olunmuş ola bilər. İnformasiyanın mənəvi-etik metodlarla mühafizəsi profilaktik xarakter daşıyır və sağlam mənəvi mühit yaratmaq üçün davamlı iş tələb edir [27].

İnformasiya təhlükəsizliyi sahəsində dünya təcrübəsi: hüquqi aspekt

Hazırda dünyanın əksər ölkələrində informasiya texnologiyalarının tətbiqinə əsaslanan elektron dövlət konsepsiyaları işlənib hazırlanır və həyata keçirilir. İnformasiyanın qlobal informasiya cəmiyyətindəki rolunun artması ilə əlaqədar informasiya təhlükəsizliyi məsələsi dövlətlərin, cəmiyyətlərin, təşkilatların qarşılaşdığı ən ciddi problemlərdən birinə çevrilmişdir. Hücum texnologiyaları müdafiə texnologiyalarından daha sürətli inkişaf etdiyindən daim yeni kibertəhdidlər meydana çıxır. Texnologiyalar nə qədər çox inkişaf edirsə, dövlət orqanlarına və özəl şirkətlərə kiberhücum və kibercasusluq halları bir o qədər çox artır. İnformasiya resurslarını, dövlət sirri daşıyan məlumatları, fərdi məlumatları qorumaq üçün ən qabaqcıl texnologiyalardan istifadə olunmasına baxmayaraq, kiberhücumlar bir çox dövlətlərin, cəmiyyətlərin, şirkətlərin zərər görməsinin əsas səbəblərindən biridir. Bu səbəblərdən informasiya təhlükəsizliyi dünya dövlətlərinin siyasətinin prioritet sahələrindən birinə çevrilmişdir və ilk növbədə beynəlxalq informasiya təhlükəsizliyinin təmin olunması, milli maraqların qorunması və möhkəmləndirilməsini nəzərdə tutan qanunlar və normativ-hüquqi sənədlər, milli kibertəhlükəsizlik strategiyaları yaradılır [28]. Milli kibertəhlükəsizlik strategiyası, milli infrastruktur və xidmətlərin təhlükəsizliyini və möhkəmliyini artırmaq üçün hazırlanmış fəaliyyət planıdır. İnformasiya təhlükəsizliyinin hüquqi dəstəyi ilə bağlı xarici təcrübənin analizi göstərir ki, 100-ə yaxın dövlətdə informasiya əldə etmək hüququ haqqında qanun qəbul edilmişdir [29].

ABŞ-ın qanunvericiliyində informasiya təhlükəsizliyi məsələlərini tənzimləyən, dövlət sirlərinin, kommersiya sirrinin, fərdi məlumatların hüquqi müdafiəsini həyata keçirən 500-ə yaxın normativ hüquqi akt mövcuddur [3]. Həmçinin ABŞ tərəfindən ilk milli kibertəhlükəsizlik strategiyası qəbul edilmişdir. "Kiberfəzanın təhlükəsizliyi üzrə Milli Strategiya" 11 sentyabr 2001-ci il tarixli terror hücumlarına cavab olaraq ABŞ Daxili Təhlükəsizlik Nazirliyi tərəfindən hazırlanmış və 14 fevral 2003-cü ildə nəşr edilmişdir. Bu sənəd ABŞ universitetlərində, dövlət qurumlarında və şirkətlərdə kompüter təhlükəsizliyinin vəziyyəti ilə bağlı bir illik araşdırma və beş aylıq ictimai müzakirədən sonra hazırlanmışdır [31].

Avropada informasiya təhlükəsizliyinin təmin edilməsinin hüquqi əsasları 1980-ci illərin ortalarından yaradılmağa başlanmışdır. O zamandan başlayaraq informasiya təhlükəsizliyi hüququn ən çətin sahələrindən birinə çevrilib. İnkişafın nəticələri kimi Avropa ölkələrində çoxsaylı direktivlər və milli qanunvericiliklər qəbul edilib [32].

ABŞ-dan sonra Avropa ölkələrində də kibertəhlükəsizlik strategiyaları hazırlanmağa başlandı. Almaniya Federativ Respublikası 2005-ci ildə "İnformasiya infrastrukturunun mühafizəsi üçün Milli Plan" və 2011-ci ilin fevralında "Kiber Təhlükəsizlik Strategiyası" qəbul etdi. Bu Almaniyanın kiber təhlükəsizlik siyasəti üçün vacib plan hesab edilir [32].

Fransada ilkin kibertəhlükəsizlik strategiyası 2010-cu ilin əvvəlində hazırlanmış və 2011-ci ildə iqtisadi və maliyyə nazirliklərinə casusluq etmək məqsədi ilə edilən kiberhücumdan dərhal sonra yayımlanmışdır [32].

İtaliyada 2017-ci ildə kibertəhlükəsizlik üzrə fəaliyyət planı qəbul edilmişdir. Bu fəaliyyət planı 2013-cü ildə qəbul edilmiş "İtalyan Kibertəhlükəsizliyi Fəaliyyət Planı" çərçivəsində 2014-2015-ci illərdə qazanılan təcrübəyə əsaslanır və kiberməkanda təhlükəsizliyin milli strateji əsaslarını həyata keçirmək üçün yerinə yetirilməli olan operativ qaydalar və tədbirləri özündə ehtiva edir [32].

Avropada yalnız kompüter deyil, insanların da həyat və sağlamlığını kiberhücumlardan qorumaq üçün 2004-cü ildə Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi (European Network and Information Security Agency, ENISA) yaradılmışdır. 2017-ci ilin sentyabrında Avropa Birliyi (AB) ENISA-nı Avropadakı kiber məkanı daha etibarlı qorumaq üçün Avropa Birliyi Kibertəhlükəsizliyi Agentliyinə çevirdi. Hazırda Avropa Birliyi Kibertəhlükəsizliyi Agentliyi (ENISA) bütün Avropada kibertəhlükəsizlik səviyyəsini təmin etməyə çalışan agentlikdir. ENISA AB-nin kibertəhlükəsizlik siyasətinə töhfə verir, kibertəhlükəsizlik sertifikatlaşdırma sxemləri vasitəsilə İKT məhsullarının, xidmətlərin və proseslərin etibarlılığını artırır, üzv dövlətlər və AB qurumları ilə əməkdaşlıq edir. Avropanın sabahkı kiber problemlərə hazırlaşmasına kömək edir [32].

2000-ci ildə Rusiya Federasiyasında "İnformasiya təhlükəsizliyi doktrinası" qəbul edilmişdir. İnformasiya təhlükəsizliyi doktrinası informasiya sahəsində Rusiya Federasiyasının milli təhlükəsizliyinin təmin edilməsinə dair rəsmi baxışlar sistemidir. 2016-cı ildə təsdiq edilmiş informasiya təhlükəsizliyinə dair yeni doktrinada informasiya sahəsindəki çoxsaylı hüquq pozuntuları və onların qarşısını almaq üçün qaydalar açıqlanmışdır [33].

Qlobal informasiya cəmiyyəti şəraitində informasiya təhlükəsizliyinin təmin edilməsi üzrə tədbirlərin həyata keçirilməsi bu sahədəki problemlərin dərindən, hərtərəfli elmi tədqiqi olmadan mümkün deyil. Bu səbəbdən informasiya təhlükəsizliyi problemləri bir çox dünya dövlətlərinin elmi-tədqiqat müəssisələrinin, universtetlərin elmi-tədqiqat bazasının əsasını təşkil edir.

Rusiya Federasiyasının Təhlükəsizlik Şurası yanında Elmi Şurası informasiya təhlükəsizliyi sahəsində elmi tədqiqatların əsas istiqamətləri və problemlərinin siyahısını hazırlamışdır [34]. Bu sənədlər Rusiya Federasiyasının təhlükəsizliyinin təmin edilməsi üzrə elmi problemlərin aşağıdakı əsas istiqamətlərini əks etdirir:

- informasiya təhlükəsizliyinin təmin edilməsinin humanitar problemləri;
- informasiya təhlükəsizliyinin təmin edilməsinin elmi-texniki problemləri (fiziki-riyazi, texniki);

- informasiya təhlükəsizliyinin kadr təminatı problemləri.

Hazırda Rusiyanın informasiya təhlükəsizliyinin elmi-texniki komponenti üzrə kadr hazırlığını həyata keçirən 100-dən çox ali təhsil müəssisəsi mövcuddur [34].

ABŞ-ın Massaçusets Texnologiya İnstitutu, Stanford Universiteti, İsveçrə Texnologiya Universiteti, Lozanna Politexnik Universiteti, Böyük Britaniyanın Oxford İnternet İnstitutu, Edinburq Universiteti, London İmperial Kolleci də dünyada informasiya, kommunikasiya və texnologiyalar, informasiya təhlükəsizliyi sahələrində tədqiqatlar aparan nüfuzlu elmi mərkəzləri kimi tanınırlar [35].

Azərbaycanda informasiya təhlükəsizliyinin təmin edilməsi isitqamətində görülən işlər

İnformasiya təhlükəsizliyi Azərbaycan Respublikasının da dövlət siyasətinin əsas istiqamətlərindən biridir. Ölkənin informasiya mühitinin tənzimlənməsi üçün hüquqi mənbə Azərbaycan Respublikası Prezidentinin fərmanları, Azərbaycan Respublikasının Konstitusiyası, sahəvi qanunlar və Azərbaycan Respublikasının tərəfdar olduğu beynəlxalq müqavilələrdir. İnformasiya mühitindəki münasibətləri tənzimləyən əsas normativ akt "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikası qanunudur. Qanunun təsir dairəsi informasiyanın yığılması, işlənməsi, saxlanması, axtarışı, yayılması əsasında informasiya ehtiyatlarının formalaşdırılması, informasiya sistemləri, texnologiyaları, onların təminat vasitələrinin yaradılması və onlardan istifadə olunması, informasiyanın mühafizəsi ilə əlaqədar olaraq yaranan münasibətlərin tənzimlənməsi və informasiya proseslərində iştirak edən subyektlərin hüquqlarının müəyyən edilməsi sahələrini əhatə edir [36].

Azərbaycanın informasiya təhlükəsizliyi siyasəti Azərbaycan Respublikası Prezidenti cənab İlham Əliyevin 23 may 2007-ci ildə imzaladığı "Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyası" Sərəncamında öz əksini tapmışdır. Sərəncamda Azərbaycan Respublikasının informasiya təhlükəsizliyi siyasəti dövlət, ictimai və fərdi informasiya ehtiyatlarının qorunmasına, habelə informasiya sahəsində milli maraqların müdafiəsinə yönəlmiş tədbirlər kompleksinin həyata keçirilməsindən ibarət olduğu vurğulanır. Həmçinin İnformasiya təhlükəsizliyini tənzimləmək məqsədilə dövlət sirrini təşkil edən məlumatların mühafizəsinin hüquqi mexanizmlərinin təkmilləşdirilməsi və informasiya azadlığının təmin olunması bildirilir. Hüquqi və inzibati mexanizmlər vətəndaşların hüquqlarını və dövlət strukturlarının fəaliyyəti üzərində demokratik nəzarət aparır [37].

Azərbaycan "Fərdi məlumatların avtomatlaşdırılmış qaydada işlənməsi ilə əlaqədar şəxslərin qorunması haqqında" konvensiyanı 2009-cu ildə müvafiq bəyanatlarla təsdiq etmişdir. 2010-cu ildə isə "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu qəbul edilmişdir [38]. Ümumiyyətlə, ölkəmizdə fərdi məlumatların qorunması 1948-ci il dekabrın 10-da BMT Baş Assambleyasının qəbul etdiyi "İnsan hüquqları haqqında bəyannamə", Azərbaycan Respublikası Konstitusiyasının 32-ci maddəsi, "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında", "Dövlət sirri haqqında", "İnformasiya azadlığı haqqında" və "Fərdi məlumatlar haqqında", "Biometrik informasiya haqqında" və s. qanunlarla tənzimlənir. Azərbaycan Respublikası Konstitusiyasının 32-ci maddəsində "şəxsin toxunulmazlıq hüququ" bəndində deyilir ki, "öz razılığı olmadan kimsənin şəxsi həyatı haqqında məlumatın toplanılmasına, saxlanılmasına, istifadəsinə və yayılmasına yol verilmir". "Fərdi məlumatlar haqqında" qanun fərdi məlumatların toplanılması, işlənilməsi və mühafizəsi ilə bağlı münasibətləri, milli e-məkanın fərdi məlumatlar bölümünün formalaşdırılması, habelə fərdi məlumatların transsərhəd ötürülməsi ilə əlaqədar məsələləri tənzimləyir, bu sahədə fəaliyyət göstərən dövlət və yerli özünüidarə orqanlarının, hüquqi və fiziki şəxslərin hüquq və vəzifələrini müəyyən edir [39].

26 sentyabr 2012-ci ildə Azərbaycan Respublikası Prezidenti cənab İlham Əliyevin imzaladığı "İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri

haqqında" Fərman ölkədə informasiya proseslərinin mühafizəsi, sabitliyi və fasiləsizliyi, dövlət orqanlarının informasiya ehtiyatlarının qorunması, bu sahədə təhdidlərin qarşısının alınması, təhlili və qabaqlanması üçün dövlət və qeyri-dövlət informasiya infrastrukturu subyektlərinin, onların istifadəçilərinin fəaliyyətinin əlaqələndirilməsi, kibertəhlükəsizlik sahəsində risklərin qiymətləndirilməsi və idarə olunması, ümummilli hazırlığın və maarifləndirmənin təmin edilməsini ehtiva edir [40].

Azərbaycan Respublikası informasiya təhlükəsizliyi sahəsində MDB dövlətləri ilə sıx əməkdaşlıq edir. Bu əməkdaşlığın normativ hüquqi əsasları kimi "Azərbaycan Respublikası Hökuməti və Rusiya Federasiyası Hökuməti arasında məxfi informasiyanın qarşılıqlı mühafizəsi haqqında", "Azərbaycan Respublikası Hökuməti və Gürcüstan Hökuməti arasında informasiya sahəsində əməkdaşlıq haqqında", "Azərbaycan Respublikasının Hökuməti və Moldova Respublikasının Hökuməti arasında informatizasiya və informasiya texnologiyaları sahəsində əməkdaşlıq haqqında", "Azərbaycan Respublikası Hökuməti və Belarus Respublikası Hökuməti arasında məxfi informasiyanın qarşılıqlı mühafizəsi haqqında", "Azərbaycan Respublikası Hökuməti və Özbəkistan Respublikası Hökuməti arasında məxfi informasiyanın qarşılıqlı mühafizəsi haqqında" Sazişləri və s. göstərmək olar [41].

Azərbaycanda informasiya təhlükəsizliyinin hüquqi əsasları ilə yanaşı, informasiyanın etibarlı mühafizəsi sahəsində təhlükəsizlik tədbirlərinin artırılması, yeni metod və alqoritmlərin işlənilməsi üçün elmi-tədqiqatlar da aparılır. İnformasiya təhlükəsizliyinin təmin olunması problemlərinin elmi-nəzəri əsasları araşdırılır, dünyada bu sahədə görülən işlər və əldə edilən təcrübələr öyrənilir. O cümlədən Industry 4.0 platformasında kiberfiziki sistemlərin analizi və sintezi problemləri, e-dövlət mühitində təhdidlərin çoxfaktorlu qiymətləndirilməsi metodları, zərərli proqram təminatının aşkarlanması və analizi üçün süni intellekt yanaşmaları, təşkilatlarda informasiya təhlükəsizliyinin menecmenti metodları və s. üzrə tədqiqatlar aparılır. Big Data, Deep Learning, Machine Learning, Process Mining, Soft computing və s. kimi innovativ yanaşmaların əsasında informasiya təhlükəsizliyinin təmin edilməsi üçün yeni nəsil yanaşmalar, metod və alqoritmlər işlənilir [42].

Nəticə

Araşdırmalar göstərir ki, İnformasiya cəmiyyətinin uğurlu, dayanıqlı inkişafı informasiya təhlükəsizliyinin təmin edilməsindən bir başa asılıdır. Şəxsi həyatın toxunulmazlığının təmin edilməsi, sosial stabilliyin və dövlətçiliyin qorunması, ölkənin informasiya məkanına xarici müdaxilələrin qarşısının alınması, beynəlxalq terror təşkilatları ilə mübarizə və s. kimi problemlərin həllində informasiya təhlükəsizliyi məsələləri olduqca mühüm rol oynayır. Bu səbəbdən də bütün dünya ölkələri, o cümlədən də Azərbaycan informasiya təhlükəsizliyi sahəsində fəaliyyət göstərərək, təhlükəsiz informasiya mühiti yaratmaq üçün səy göstərirlər. İnformasiya mühiti və informasiya texnologiyalarının imkanlarından adekvat istifadə fərdin, sosial qrupun və cəmiyyətin uğurlu və təhlükəsiz fəaliyyəti üçün zəmin yarada bilər. Əks təqdirdə, informasiya cəmiyyətinin istifadəçilər üçün yaratdığı imkanlar mənfi nəticələrə gətirib çıxara bilər.

Elmi-texniki tərəqqi informasiyanı yalnız dəyərli məhsula deyil, həm də ictimai şüura təsir vasitəsinə çevirir. Bu təsir müsbət və mənfi ola bilər. Məlum olduğu kimi, həm ölkə daxilində, həm də xaricdə bir sıra siyasi və sosial qüvvələr var ki, öz məqsədlərinə çatmaq üçün informasiyadan təsir vasitəsi kimi istifadə edir, cəmiyyət və dövlət üçün təhlükəli olan informasiya təsiri üsullarına əl atırlar. İnformasiya təhlükəsizliyi təhdidlərinin dərindən analizi dövlətin informasiya siyasətinin daha da təkmilləşdirilməsi və ölkəni daha təhlükəsiz etmək baxımından faydalı ola bilər.

Ədəbiyyat

1. Hilbert M. Digital technology and social change: the digital transformation of society from a historical perspective // Dialogues in Clinical Neuroscience, 2020, 22 (2), pp.189-194.
2. Aliguliyev R.M., Imamverdiyev Y.N., Mahmudov R.Sh. Informasiya tahlukasizliyinin multidissiplinar elmi-nazari problemlari // Informasiya jamiyyati problemlari, 2017, №2, s. 32–43.
3. Viner N. Kibernetika, ili upravlenie i svyaz` v zhivotnom i mashine; ili Kibernetika i obshhestvo / 2-e izdanie, M.: Nauka; Glavnaya redakcziya izdanij dlya zarubezhny`kh stran, 1983, 344 s.
4. Floridi L. Information: A very short introduction. OUP Oxford, 2010, 130 p.
5. Alhassan M. M., Adjei-Quaye A. Information Security in an Organization // International Journal of Computer (IJC), 2017, T. 24, № 1, pp. 100-116.
6. Rhee M.Y. Internet security : cryptographic principles, algorithms, and protocols, John Wiley & Sons, 2003, 424 p.
7. Emel`yanov G. V., Strel`czov A. A. Problemy` obespecheniya bezopasnosti informaczionnogo obshhestva // Informaczionnoe obshhestvo, 1999, № 2, c.15-17.
8. Gasımov V.A. Informasiya tahlükasizliyinin asasları, Darslik, Bakı, 2009, 340 s.
9. Krombholz K. et al. Advanced social engineering attacks // Journal of Information Security and applications, 2015, T. 22, pp. 113-122.
10. Cho J.S., Yeo S.S., Kim S.K. Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value // Computer communications. 2011, T. 34, №. 3, pp. 391-397.
11. Kaspersky Internet Security, www.kaspersky.ru
12. Rieck K. et al. Learning and classification of malware behavior // International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, Berlin, Heidelberg, 2008, pp.108-125.
13. Garera S. et al. A framework for detection and measurement of phishing attacks // Proceedings of the 2007 ACM workshop on Recurring malcode. 2007, pp. 1-8.
14. Dashdamirova K.G. Internet sosiologiyasının muasir vaziyyati va problemlari, Informasiya jamiyyati problemlari, 2020, №1, s. 134–142.
15. Butkevich S.A. E`kstremizm i terrorizm v kiberprostranstve: vy`yavlenie, nejtralizacziya i preduprezhdenie // Vestnik KRU MVD Rossii. 2018, №1 (39). c.17-22.
16. Vevericza A. A., Diblyak D. A. Informaczionny`j terrorizm v kiberprostranstve kak ugroza stabil`nosti mirovogo soobshhestva // Colloquium-journal, 2019, № 16-7, c.35-38.
17. Messmer E. Cyber Espionage: A Growing Threat to Business // PC World, January 2008, https://www.pcworld.com/article/141474/article.html
18. Mahmudova R.Sh. Fardi malumatların gorunması va informasiya tahlukasizliyi madaniyyati // Informasiya tahlukasizliyinin aktual multidissiplinar elmi-praktiki problemlari, 29 noyabr 2019-ju il, s.229-232.
19. Fischer-Hübner S. Privacy and security at risk in the global information society // Information Communication & Society. 1998, Vol. 1, Is. 4, pp. 420-441.
20. Aliguliyev R.M., Imamverdiyev Y.N. Ragam imzası tekhnologiyası, Bakı, Elm, 2003, 132 c.
21. Mehdiyev Sh., Imamverdiyev Y. E-dovlatin informasiya tahlukasizliyi va tekhnolozhi chaghırıshlar // Informasiya tahlükasizliyinin multidissiplinar problemlari uzra II respublika elmi-praktiki konfransı, 2015, s. 130-133.
22. Yasenev V.N. Informaczionnaya bezopasnost` v e`konomicheskikh sistemakh, Uchebnoe posobie, N.Novgorod, Izd-vo NNGU, 2006, 253 c.
23. Paroshin A.A. Normativno-pravovy`e aspekty` zashhity` informaczii, Uchebnoe posobie, Vladivostok, Izd-vo Dal`nevost. feder. un-ta, 2010, 116 s.

24. Alhassan M., Adjei-Quaye A. Information Security in an Organization // International Journal of Computer (IJC), 2017, 24(1), pp.100-116.
25. Bezbogov A.A., Yakovlev A.V., Shamkin V.N. Metody` i sredstva zashhity` komp`yuternoj informaczii : uchebnoe posobie, Tambov, Izd-vo Tamb. gos. tekhn. un-ta, 2006, 196 s.
26. Domarev V. V. Bezopasnost` informaczionny`kh tekhnologij, K.: OOO TID Dia Soft, 2004, 992 s.
27. Manin S.A., Dvadnenko M.V. Metody` i sredstva obespecheniya informaczionnoj bezopasnosti / Materialy` VIII Mezhdunarodnoj studencheskoj nauchnoj konferenczii «Studencheskij nauchny`j forum», 2016, https://scienceforum.ru/2016/article/2016019594
28. Imamverdiyev Y. Milli kibertahlukasizlik strategiyalarının analizi / Azarbaycan khalgının ümummilli lideri Heydar Aliyevin 90 illik yubileyina hasr olunmush "Informasiya tahlukasizliyi problemlari uzra I respublika elmi-praktiki konfransı", 2013, s.14-17.
29. Aslanov P.M. Zarubezhny`j opy`t pravovogo regulirovaniya obespecheniya informaczionnoj bezopasnosti // Politika i obshhestvo, 2012, # 2 (86), s. 45-48.
30. Shamsutdinov R. R. Analiz pravovoj zashhity` informaczii v SShA // Evrazijskij yuridicheskij zhurnal. 2018, #. 1, s. 61-63.
31. Bush G. W. The National Strategy to Secure Cyberspace, February 2003 // General Security Issues, 2003, p. 73.
32. European Union Agency for Cybersecurity, https://www.enisa.europa.eu
33. Petrenko S. A., Petrenko A. S. Novaya doktrina informaczionnoj bezopasnosti Rossijskoj Federaczii // Zashhita informaczii. Insajd, 2017, #. 1. c. 33-39.
34. Sherstyuk V. P. MGU: nauchny`e issledovaniya v oblasti informaczionnoj bezopasnosti // Informaczionnoe obshhestvo, 2005, # 1, c.48-53
35. 20 samy`kh perspektivny`kh universiteta v sfere IT - informaczionny`kh tekhnologij, http://www.simplex.ua/articles/20it
36. "Informasiya, informasiyalashdırma va informasiyanın muhafizasi haggında" Azarbaycan Respublikasının Ganunu, 3 aprel 1998-ji il, http://e-qanun.gov.az/framework/3525
37. "Azarbaycan Respublikasının milli tahlukasizlik konsepsiyasının tasdig edilmasi haggında" Azarbaycan Respublikası Prezidentinin Saranjamı, 23 may 2007-ji il, http://www.e-qanun.az/framework/13373
38. "Fardi malumatlar haggında" Azarbaycan Respublikasının Ganunu, 11 may 2010-ji il, http://www.e-qanun.gov.az
39. Avropa Shurasının 28.01.1981-ji tarikhli 108 №-li konvensiyasının tasdig edilmasi barada Azarbaycan Respublikasının Ganunu, 30 sentyabr 2009-ju il, http://www.e-qanun.gov.az
40. "Informasiya tahlükasizliyi sahasinda faaliyyatin takmillashdirilmasi tadbirlari haggında" Azarbaycan Respublikası Prezidentinin Farmanı, 26 sentyabr 2012-ji il, http://e-qanun.az/framework/24353
41. Niyazov kh. Informasiya tahlükasizliyi, hügugi asasları, mügayisali yanashma // Informasiya tahlükasizliyinin aktual multidissiplinar elmi-praktiki problemlari" IV respublika konfransı, Bakı, 2018, s. 22-26.
42. Informasiya tahlukasizliyi uzra tadgigatlar mukhtalif istigamatlarda genishlandirilajak, https://ict.az/index.php?mod=news&id=5679&lang=az

УДК 004.056.5

Махмудова Расмия Ш.[1], Дашдамирова Конул Г.[2]
[1,2]Институт информационных технологий НАНА, Баку, Азербайджан
[1]rasmahmudova@gmail.com, [2]konulahmed@gmail.com

Анализ некоторых проблем информационной безопасности в среде информационного общества

В настоящее время большая часть населения интегрируется в виртуальную среду с помощью информационно-коммуникационных технологий и становится гражданами информационного общества. Растущая роль информации, информационных ресурсов и технологий в обществе подчеркивает необходимость защиты интересов личности, общества, государства и обеспечения информационной безопасности в информационном обществе. В статье анализируются угрозы, которые могут затронуть интересы личности, общества и государства в информационном обществе, основные принципы информационной безопасности, методы обеспечения информационной безопасности. Рассмотрен опыт зарубежных стран в области информационной безопасности, а также отмечены работа, проделанная в области правового обеспечения информационной безопасности в Азербайджане, и проведенные научно-теоретические исследования. В статье использовались такие исследовательские методы, как сравнительный анализ, мониторинг, классификация. Предварительные результаты исследования полезны для более широкого изучения проблем информационной безопасности в среде информационного общества и могут быть использованы в качестве источника исследователями, изучающими вопросы информационной безопасности.

Ключевые слова: *информационное общество, информационная безопасность, кибербезопасность, социальная инженерия, фишинг, информационная война.*

Rasmiya Sh. Mahmudova [1], Konul G. Dashdamirova [2]
[1,2]Institute of Information Technologies of ANAS, Baku, Azerbaijan
[1]rasmahmudova@gmail.com, [2]konulahmed@gmail.com

Analysis of information security problems in the information society environment

Today, a large part of the population is integrated into the virtual environment using information and communication technologies and becomes a citizen of the information society.
The growing role of information resources and technologies in society demonstrates the necessity to protect the interests of person, society, state, and ensure information security in the information society. This paper analyzes the threats affecting the interests of the individual, society and the government in the information society, the basic principles of information security, and the methods of ensuring information security. The experience of foreign countries in the field of information security was studied, the researches performed in the field of legal provision of information security in Azerbaijan and the scientific-theoretical research were investigated. Research methods such as comparative analysis, monitoring, classification were used in the research. Preliminary results of the study are useful for broader study of information security issues in the information society environment and can be used as a source by researchers investigating information security problems.

Keywords: *information society, information security, cyber security, social engineering, phishing, information war.*