Fərdi məlumatların qorunması və informasiya təhlükəsizliyi mədəniyyəti

Rəsmiyyə Mahmudova

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

***Xülasə*— Məqalədə fərdi məlumatların qorunmasının müxtəlif aspektləri araşdırılır. İnformasiya sistemlərində toplanmış fərdi məlumatların qorunması məsələləri, eləcə də internetdə fərdi məlumat subyektləri üçün mövcud təhlükələr analiz edilir. İnformasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması və inkişaf etdirilməsi üçün təkliflər verilir.**

Açar sözlər— fərdi məlumatlar; konfidensial informasiya; informasiya sistemləri; informasiya təhlükəsizliyi mədəniyyəti

I. GİRİŞ

Hazırda bütün sferalarda cəmiyyətin get-gedə artan tələbatının ödənilməsi, bu və ya digər proseslərin (biliklərin qiymətləndirilməsi, pul vəsaitlərinin idarə edilməsi, ticarətin, istehsalın avtomatlaşdırılması və s.) avtomatlaşdırılması məqsədi ilə müxtəlif təyinatlı informasiya sistemləri yaradılır və istifadəyə verilir. Hazırda məlumatların toplanması və emalı ilə hamı məşğul olur, uyğun verilənlər bazası olmadan nə dövlət strukturları, nə biznes təşkilatları öz fəaliyyətini səmərəli şəkildə qura bilməz. Bu tip sistemlərdə təyinatından asılı olaraq insanların sağlamlığı, ailə vəziyyəti, təhsili, siyasi və dini mənsubiyyəti, məvacibi, əmək fəaliyyəti, yaşayış yeri, telefonu, ailə üzvləri və s. haqqında müxtəlif məlumatlar toplanır, saxlanır və emal olunur. Eyni zamanda, internetin müxtəlif xidmətlərindən istifadə edən insanlar özləri haqqında şəxsi məlumatları bu resurslarda yerləşdirirlər.

Fərdi məlumatlarını bu və ya digər informasiya sistemlərinə daxil edərkən, elektron ödəniş sistemlərindən, bank kartlarından, müxtəlif təyinatlı elektron xidmətlərdən istifadə edərkən insanlar demək olar ki hər dəfə öz məlumatlarının konfidensiallığının qorunması problemi ilə üzləşirlər.

İnformasiya texnologiyaları (İT) sahəsindəki ekspertlər arasında belə bir fikir mövcuddur ki, İnternetin inkişaf tempi ona gətirib çıxaracaq ki, yaxın gələcəkdə şəxsi həyat “susmaya görə” şəffaf və açıq olacaq – fərdi məlumatları dövlət və korporasiyalar üçün açmamaq mümkün olmayacaq. Bu məlumatların təhlükəsizliyi məsələlərinin öhdəsindən gəlmək isə getdikcə çətinləşəcək. Məhz buna görə də, informasiya sistemlərində toplanan fərdi məlumatların qorunması, eləcə də şəxsi məlumatların İnternetdə geniş yayılması problemlərinə və onun nəticələrinə ictimaiyyətin diqqətinin cəlb edilməsi, o cümlədən fəal şəkildə fərdi məlumatların qorunması sahəsində təbliğat - məlumatlandırma işlərinin aparılması, insanların informasiya təhlükəsizliyi mədəniyyətinin artırılması olduqca vacibdir.

II. FƏRDİ MƏLUMATLARIN QORUNMASININ HÜQUQİ ASPEKTİ

Şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumat (onun familiyası, adı, atasının adı, doğulduğu tarix, anadan olduğu yer, ailə vəziyyəti, sosial durumu, mülkiyyəti, gəlirləri, təhsili, ixtisası və s.) fərdi məlumatlara aid edilir.

Hazırda demək olar ki, hər bir insan elektron informasiyaya malikdir, istər onun şəxsi məlumatları olsun, istər müxtəlif elektron xidmətlərdən istifadə üçün parol və loginlərin saxlandığı fayl, istərsə də iş sənədləri – maliyyə hesabatları, perspektiv üçün fəaliyyət planı və s. Bu tip informasiyanın icazəsiz müdaxilələrdən və yayılmadan, təsadüfi silinmələrdən və dəyişikliklərdən qorumaq lazımdır.

İnformasiya təhlükəsizliyi, o cümlədən vətəndaşların fərdi məlumatlarının qorunması problemləri demək olar ki, dünyanın bütün ölkələrini narahat edir. Bu onunla əlaqədardır ki, informasiyalaşdırma insanın bütün fəaliyyət sahələrini əhatə edir, bütün xidmətlər elektronlaşır, insanların bir çox münasibətləri virtuallaşır, insanın fərdi məlumatları artıq hər yerdə var.

Fərdi məlumatların qorunması problemi ilə bağlı ilk qanun aktı qəbul edən ölkə ABŞ olmuşdur. Bu, 31 dekabr 1974-cü ildə qəbul edilmiş “Konfidensiallıq haqqında Qanun”dur və orada deyilir ki, bütün müəssisələr özlərinin verilənlər bazaları haqqında bildiriş məktubu göndərməli və Federal reyestrdə qeydiyyatdan keçməlidirlər. Qanun bəzi hallar istisna olmaqla, məlumat subyektinin yazılı razılığı olmadan verilənlər bazasından hər hansı məlumatın yayılmasını qadağan edir. ABŞ-da məlumatların konfidensiallığına və qorunmasına aid olan xeyli sayda lokal və milli normativ aktlar mövcuddur [1].

Avropada isə 1981-ci il yanvarın 28-də “Fərdi məlumatların avtomatlaşdırılmış qaydada işlənməsi ilə əlaqədar şəxslərin qorunması haqqında Konvensiya (108 saylı Konvensiya) imzaya açılmışdır. 108 saylı Konvensiya məlumatların mühafizəsi sahəsində mövcud olan və məcburi hüquqi qüvvəyə malik olan yeganə beynəlxalq sənəddir. Bu konvensiya fərdi məlumatların dövlət sektorunda və ya özəl sektorda həyata keçirilən istənilən işlənilməsini əhatə edir və

DOI: 10.25045/NCInfoSec.2019.57

şəxsləri bu zaman meydana gələ biləcək hər hansı sui-istifadə hallarından müdafiə etmək məqsədi ilə qəbul edilmişdir [2].

Bu konvensiyanın müddəaları əsasında Avropa ölkələri tərəfindən milli səviyyədə fərdi məlumatların tənzimlənməsi haqqında ayrıca qanunlar qəbul edilmişdir. Sonradan milli qanunlar Avropa Şurasının bir sıra direktivləri ilə uyğunlaşdırılmışdır. Bunlardan biri Avropa Parlamentinin və Avropa İttifaqı Şurasının 95/46/EC saylı 24 oktyabr 1995-ci il tarixli, “Fiziki şəxslərə aid olan fərdi məlumatların işlənilməsi və həmin məlumatların sərbəst dövriyyəsinə dair” direktividir.

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 [3, 4].

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 [4].

III. İNFORMASİYA SİSTEMLƏRİNDƏ TOPLANMIŞ FƏRDİ MƏLUMATLARIN QORUNMASI MƏSƏLƏLƏRİ

Fərdi məlumatların qorunması kompleks bir məsələdir, burada hüquqi, adminstrativ-təşkilati, proqram-texniki məsələlərlə yanaşı informasiya sistemləri ilə işləyən işləyən insanların bu məlumatlarla davranması məsələsi də olduqca vacibdir. İnformasiya təhlükəsizliyi üzrə qəbul edilmiş beynəlxalq standartların analizindən də görünür ki, informasiya təhlükəsizliyi üsullarının və vasitələrinin əksəriyyəti təşkilat əməkdaşlarının iştirakını nəzərdə tutur [5].

İnformasiya resurslarının təhlükəsizliyi məsələləri təşkilatli tədbirlər, konfidensial informasiyanın qorunması, kənar təhdidlərdən qorunma və s. bağlı məsələləri əhatə edir. Qeyd etmək lazımdır ki, informasiya təhlükəsizliyi sistemlərinin əksəriyyəti kənar müdaxilələrdən və konfidensial informasiyanın sızmasından qorunmaya yönəlib. Bu cür sistemlər informasiyanın qorunması üçün müxtəlif üsullardan, o cümlədən, faylların nəşr olunması, məktubların göndərilməsi, şəbəkə vasitəsi ilə faylların ötürülməsi hesabına konfidensial informasiyanın arzuolunmaz yayılmasının qarşısının alınması məqsədi ilə kontenti analiz etməklə informasiyanın filtrasiyası üsulundan istifadə edir. Lakin, informasiya təhlükəsizliyi sferasında fəaliyyət göstərən müxtəlif mərkəzlər tərəfindən aparılan tədqiqatların nəticələri göstərir ki, informasiya təhlükəsizliyinin pozulması ilə bağlı insidentlərin böyük əksəriyyətinin səbəbi daxili təhlükələrdir. Bu cür təhlükələrin mənbəyi informasiya sistemlərinin leqal istifadəçiləridir [6].

Fərdi məlumatların qorunması nöqteyi-nəzərindən informasiya resurslarının mühafizəsi problemi olduqca vacibdir. Bu cür mühafizə fərdi məlumatlar üçün gözlənilən təhlükələrin reallaşması zamanı meydana çıxan itkilərin, yəni fiziki, maddi və maliyyə baxımından fərdi məlumatların subyektinə dəyə biləcək zərərin minimallaşdırılmasını nəzərdə tutur. Ona görə də son zamanlar dünyanın bir sıra ölkələrində fərdi məlumatların qorunması məsələlərinə xüsusi diqqət ayrılır. Bu, ilk növbədə bu tip məlumatların qorunması sistemlərinin işlənib hazırlanması məsələlərinə aiddir. Burada informasiyanın qorunması funksiyasını yerinə yetirən aparat-proqram vasitələri də daxil olmaqla texniki üsullar vacib yer tutur. Onlar fərdi məlumatların qorunması konsepsiyası nəzərə alınmaqla qurulmalıdır. Başqa sözlə, fərdi məlumatların qorunması problemi, fərdi məlumatların qorunması sisteminin strukturunu formalaşdıran kompleks təşkilati və texniki tədbirlərin həyata keçirilməsini nəzərdə tutur.

Hazırda “qara bazar”da hüquqi və fiziki şəxslərə aid verilənlər bazalarının alınıb-satılması hallarının artması müşahidə olunur. Konfidensial informasiyanın başqalarının əlinə keçməsində insan faktoru başlıca rol oynayır. Məsələn, aşağıdakı hallar ola bilir:

- İstifadəçinin müvəqqəti olaraq iş yerini tərk edən zaman kompüteri bağlamağı unutması və informasiyanın digər şəxs üçün əlyetən olması;
- Kompüteri şəbəkəyə qoşan zaman hansı informasiyanın digər şəxslər üçün əlyetən olmasını bilməməsi;
- İstifadəçinin öz kompüterindən sosial və digər ümumi şəbəkələrə çıxışın informasiya sızmasına gətirib çıxara biləcəyi barədə məlumatsız olması;
- İcazəsiz olaraq istifadəçi tərəfindən müxtəlif proqram təminatlarının kompüterə yüklənməsi zamanı virusla yoluxma;
- Və s.

Ümumiyyətlə, konfidensial informasiyanın, o cümlədən kommersiya sirrlərinin, fərdu məlumatların başqalarının əlinə keçməsinin səbəbləri arasında – təşkilatda çalışan əməkdaşların konfidensial informasiyanın qorunması üsullarını yetərincə bilməməsi; tövsiyyə olunmayan texniki vasitələrdən istifadə; informasiyanın qorunması qaydalarına riayət olunmasına zəif nəzarət; kadrların tez-tez dəyişməsi məsələləri xüsusi ilə qeyd olunur.

Buradan belə nəticəyə gəlmək olur ki, konfidensial informasiya çox asanlıqla başqalarının əlinə keçə bilər. Təcrübə göstərir ki, informasiyanın qorunması üçün nə qədər

mükəmməl texniki vasitələrdən istifadə olunsa belə əməkdaşların informasiya təhlükəsizliyi mədəniyyətinin lazımi səviyyədə olmaması səbəbindən informasiya itir, oğurlanır, silinir və s.

IV. İNTERNETDƏ FƏRDİ MƏLUMATLARIN QORUNMASI MƏSƏLƏLƏRİ

İnternetdə fərdi məlumat subyektlərinin məruz qaldığı əsas təhlükə mənbələri bunlar hesab edilir: istifadəçi razılığının susma prinsipi ilə qəbul edilməsi; fərdi məlumatların oğurlanması və açıq mənbələrdə yayılmlanması; şəxsi informasiyanın təhlükəsiz əlaqə vasitələri ilə ötürülməməsi; saxta mobil əlavələrdən istifadə edilməsi; videonəzarət və geolokasiya xidmətləri; fişinq və s.

İnsanların şəxsi həyatı haqqında məlumatların İnternetə yol tapması üsulları müxtəlifdir: bu məlumatlar istifadəçilərin özləri, dostları və ya düşmənləri tərəfindən yerləşdirilə bilər. İnternetin və istifadəçilərin fərdi məlumatları ilə işləyən İT-xidmətlərin sürətli inkişafı konfidensiallığın itirilməsi riskinin meydana çıxmasına səbəb olur.

Fərdi məlumatların oğurlanması sahibini maddi və mənəvi təhlükəyə məruz qoya bilər. Məsələn, kifayət qədər texniki biliklərə malik olan cinayətkarlar bank kartlarının rekvizitlərini oğurlayırlar (skrimminq), yaxud istifadəçilərin fərdi məlumatlarını əldə etmək məqsədi ilə maliyyə müəssisələrinin saytlarına bənzəyən saytlar hazırlayırlar (fişinq). Eyni zamanda, əldə edilmiş fərdi məlumatlar spam-göndərişlərin təşkili, sosial şəbəkələrdə statusun dəyişdirilməsi və s. üçün də istifadə oluna bilər. Cəmiyyətin informasiyalaşdığı müasir dövrdə bəzən fərdi məlumatların sızması mənbəyini təyin etmək çətin olur. Lakin aparılan tədqiqatlar göstərir ki, fərdi məlumatlara əlyetənliyi təmin edən əsas mənbə sosial şəbəkələrdir.

On-layn mühitdə biz öz əlaqələrimizi və kontaktlarımızı, siyasi, fəlsəfi, mənəvi, mədəni, estetik və digər dəyərlərimizi və maraqlarımızı, əhəmiyyətli hadisələri, ehtiyac və asılılıqlarımızı açırıq, bununla da öz məlumatlarımıza nəzarəti itiririk, bilmirik ki, bizim fərdi məlumatlarımız harda, kim tərəfindən istifadə olunur və necə qəbul olunur. Bunlar bizim fərdi məlumatlarımızdır və biz öz məlumatlarımızı qorumağı bacarmalıyıq. Fərdi məlumatların qorunması informasiya təhlükəsizliyi problemidir.

Insanların əksəriyyəti müxtəlif virtual cəmiyyətlərin üzvü olmağa və onun imkanlarından istifadə etməyə çalışırlar, gündən-günə artan müxtəlif proqram və əlavələrdən istifadə edirlər. Əslində hər kəs fərdi məlumatlarını könüllü şəkildə təqdim edir və istifadəçi razılaşmalarını imzalamaqla öz fərdi məlumatlarını istifadə etməyə razılıq verir. Beləliklə də, hər birimiz öz kompüterimizdən istifadə etməklə fərdi məlumatlarımızı açırıq və konfidensiallıq hüququmuzu məhdudlaşdırırıq.

Keçmişi, indini və gələcəyi birləşdirən rəqəmsal iz məsələsi də fərdi məlumatların qorunması kontekstində olduqca aktuallıq kəsb edir. Əvvələr, uzun müddət ərzində, xüsusi səylə yığılmış fərdi dosye bir dəqiqənin içində yana və tamamilə məhv ola bilərdi. İndi isə bizim rəqəmsal izimiz, məsələn, brauzerdən istifadə etməklə müxtəlif mövzuda axtarışlarımız, onlayn alış-verişlər, cookie, olduğumuz yerlər barədə geoişarələmər, bəyənmələr – özümüz tərəfindən yaradılan ən yaxşı dosyedir. Eyni zamanda, rəqəmsal iz bizim keçmişimiz və ya indimiz haqqında məlumat deyil, bu bizim identifikatorumuzdur və həmişə bizimlə olacaq.

Son zamanlarda bizim ölkədə də müəyyən şəxsləri nüfuzdan salmaq, karyerasına zərbə vurmaq, ailəsində problem yaratmaq və s. neqativ məqsədlərlə onlar haqqında şəxsi həyata dair məlumatlar təhrif olunaraq yayılır. Sürətlə inkişaf edən informasiya texnologiyaları dezinformasiya xarakterli montaj edilmiş audio, video, foto materialları yaymağa imkan verir. Kütləvi informasiya vasitələrində vətəndaşların fərdi məlumatlarının qanunsuz açıqlanmasının neqativ nəticələri ilə əlaqədar xəbərlərə tez-tez rast gəlmək mümkündür. Fərdi məlumatların əldə edilərək yayılmasının digər populyar üsulu etibardan sui-istifadə edərək sosial şəbəkələr və mobil telefonlar vasitəsi ilə reallaşdırılan şəxsi yazışmaların mətnlərinin, audio-video söhbətlərin yazılarının, hətta şəxsi görüşlərin görüntülərinin tərəflərdən biri tərəfindən yaddaşa köçürülərək sonradan şantaj yolu ilə, hədə-qorxu ilə nəyisə tələb etmək üçün istifadə edilməsidir [7].

V. İNFORMASİYA TƏHLÜKƏSİZLİYİ MƏDƏNİYYƏTİNİN FORMALAŞDIRILMASI MƏSƏLƏLƏRİ

Göründüyü kimi, müxtəlif müəssisə və təşkilatlarla yanaşı, fiziki şəxslər də informasiya təhlükəsizliyi problemi ilə üzləşirlər. Müxtəlif xaker hücumları vasitəsi ilə, şəxsi və korporotiv saytları dağıtmaqla cinayətkarlar müxtəlif konfidensial informasiyanı əldə etməyə nail olurlar.

Cəmiyyətdə informasiyanın rolunun və dəyərinin artdığı, strateji resursa çevrildiyi bir vaxtda insanların informasiya ilə davranışının səviyyəsini, yəni onların informasiya təhlükəsizliyi mədəniyyətinin yüksəldilməsi məsələsi olduqca vacib məsələdir.

İnformasiya təhlükəsizliyi mədəniyyəti – informasiya təhlükəsizliyinə dair texniki bilik və bacarıqları, insanın mənəvi-psixoloji sağlamlığı üçün təhlükəli olan informasiya təsirləri və onlardan qorunma üsulları barədə bilik və bacarıqları, informasiya resurslarından istifadə zamanı əməl edilməsi vacib olan hüquqi və etik normalar barədə bilikləri və onlara əməl etmə səviyyəsini əhatə edir [8].

Beləliklə, fərdi məlumatların qorunması ilə bağlı problemlərin aradan qaldırılması üçün digər vacib məsələlərlə yanaşı, informasiya təhlükəsizliyi mədəniyyətinin yüksəldilməsi üçün də bir sıra tədbirlərin həyata keçirilməsi vacibdir:

– vətəndaşların informasiya təhlükəsizliyi mədəniyyətinin yüksəldilməsi üçün dövlət proqramlarının hazırlanması və həyata keçirilməsi;

– cəmiyyətin əsas sosial qruplarının informasiya təhlükəsizliyi mədəniyyəti ilə bağlı biliklərə əlyetənliyinin təmin edilməsi;
– informasiya təhlükəsizliyi sahəsində kadr hazırlığı çərçivəsində informasiya təhlükəsizliyi məsdəniyyətinin formalaşdırılması çərçivəsində tədris proqramlarının işlənib hazırlanması və həyata keçirilməsi;
– kütləvi informasiya vasitələrində informasiya təhlükəsizliyi mədəniyyətinin təbliğ olunması;
– müxtəlif tipli informasiya sistemləri ilə işləyən istifadəçilərə məlumat və konsultasiya xarakterli kömək məqsədi ilə saytların yaradılması;
– məktəbəqədər təhsildən bağlayaraq ali təhsilə qədər, təhsilin bütün pillələrində informasiya təhlükəsizliyi mədəniyyətinin tərbiyə edilməsi və inkişaf etdirilməsi.

İnformasiya cəmiyyəti şəraitində uşaqların informasiya məkanında qorunması məsələləri də olduqca vacibdir. Çünki, hazırda uşaqlar kiçik yaşlarından başlayaraq İKT-dən, o cümlədən internetdən istifadə vərdişlərinə yiyələnirlər, onlar da böyüklər üçün olan informasiya resurslarından istifadə edə bilirlər. Burada təbii ki, valideynlərin informasiya təhlükəsizliyi mədəniyyətinin yüksəldilməsi üçün tədbirlərin görülməsi son dərəcə əhəmiyyətlidir.

NƏTİCƏ

İnternetin sürətli inkişafı və onun fərdi məlumatlar əsasında işləyən xidmətlərinin inkişafı ona gətirib şıxarır ki, məlumatların konfidensiallığının itirilməsinə təhdidlər informasiya cəmiyyətinin əsas risklərindən biri kimi qiymətləndirilir. Fərdi məlumatların təhlükəsizliyinin təmin edilməsinin zəruriliyi – günümüzün reallığıdır. İnformasiya təhlükəsizliyi mədəniyyətinə malik olmadan müasir insan onun şəxsi həyatına müdaxiləyə müqavimət göstərməyə qadir deyil. Fərdi məlumatların toplanması və emalı üzrə texniki imkanların, sosial şəbəkələrin, elektron kommersiya vasitələrinin artması fərdi məlumatların qorunması üçün tədbirlərin görülməsini, o cümlədən cəmiyyətdə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılmasını və inkişaf etdirilməsini zəruri edir.

İSTİNADLAR

[1] Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики, 2015, №1, с. 43–66.
[2] Council of Europe Convention #108 “the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”, Strasbourg, 28.I.1981
[3] Avropa Şurasının 28.01.1981-ci tarixli 108 №-li konvensiyasının təsdiq edilməsi barədə Azərbaycan Respublikasının 30.09.2009-cu il tarixli 879-IIIQ №-li qanunu, http://www.e-qanun.gov.az
[4] “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanunu, 11.05.2010-ci il, http://www.e-qanun.gov.az
[5] Əliquliyev R.M., İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyi: aktual tədqiqat istiqamətləri // İnformasiya cəmiyyəti problemləri, 2010, №1, s.3-13.
[6] Волошин И.П. Защита информации в информационных системах персональных данных // Информационная безопасность регионов, 2016, №1, с. 12-15.
[7] Əliquliyev R.M., Mahmudov R.Ş. Milli mentalitet kontestində fərdi məlumatların həssaslığı və onların təhlükəsizliyinin təmin olunması məsələləri // İnformasiya cəmiyyəti problemləri, 2019, №2, s.117-128.
[8] Mahmudova R.Ş, Cəmiyyətdə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması məsələləri haqqında. İnformasiya cəmiyyəti problemləri, №1(7), 2013, 32-38.

PROTECTION OF PERSONAL INFORMATION AND INFORMATION SECURITY CULTURE

Rasmiyya Mahmudova

Institute of Information Technologies of ANAS, Baku, Azerebaijan

rasmahmudova@gmail.com

Abstract – The various aspects of personal data protection are investigated in the article. Protection issues of personal information collected in information systems, as well as available threats to the personal data subjects on the Internet are analyzed. Proposals are provided for the formation and development of a culture of information security.

Keywords – ***personal information; confidential information; information systems; information security culture***