Elektron dövlət mühitində fərdi məlumatların mühafizəsi problemləri

İradə Ələkbərova
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
airada.09@gmail.com

Xülasə– **E-dövlətin informasiya məkanının təhlükəsizliyinin təminində fərdi məlumatların təhlükəsizliyi vacib məsələlərdəndir. Fərdi məlumatların toplanması, təmizlənməsi, strukturlaşdırılması və emalı üçün tətbiq edilən metod və alqoritmlər dəqiqlik tələb edir və hər hansı xətanın baş verməsi vətəndaşın e-dövlətə etimadı və nüfuzunun azalması ilə nəticələnə bilər. Bunları nəzərə alaraq, məqalədə e-dövlət mühitində fərdi məlumatlarla əlaqədar mövcud problemlər analiz olunmuş, fərdi məlumatların təhlükəsizliyinin təmin olunması üçün təkliflər işlənmişdir.**

Açar sözlər– e-dövlət, fərdi məlumatlar, sosial media, izləmə cihazları, əşyaların İnterneti, rəqəmsal iz, informasiya təhlükəsizliyi.

I. GİRİŞ

Elektron dövlətin (e-dövlət) formalaşdığı müasir cəmiyyətdə müxtəlif infrastrukturlarda, e-sənədlərdə, xəritə və cədvəllərdə, verilənlər bazasında kodlaşdırılmış şəkildə fərdi məlumatlar toplanaraq strukturlaşdırılmış, çox hallarda isə strukturlaşmadan saxlanılır. Bu məlumatların bir hissəsi müxtəlif məqsədlər üçün istifadə olunsa da, böyük bir hissəsi istifadə olunmur, bəzən isə müəyyən müddətdən sonra silinir və ya dəyişdirilir [1].

Bu gün fərdi məlumatlar “big data” təşkil etdiyi üçün, onların qorunması, səmərəli emalı və saxlanması əsas problemlərindəndir. Həmçinin vətəndaşın cəmiyyətdə, virtual məkanda fəallığı, “ağıllı İnternet”, “ağıllı şəhər”, “əşyaların İnterneti”, e-dövlət və biliklər cəmiyyəti kimi informasiya məkanlarının genişlənməsi nəticəsində fərdi məlumatların təhlükəsizliyinin təmini məsələsini daha da aktuallaşdırmışdır.

Tədqiqatın məqsədi e-dövlət mühitində gizli fərdi məlumatların mənbəyinin müəyyənləşdirilməsi, bu məlumatların təhlükəsizliyinin təmini üçün tədbirlər paketinin işlənməsidir.

II. FƏRDİ MƏLUMATLARLA ƏLAQƏDAR BƏZİ ANLAYIŞLAR

Fərdi məlumatlar dedikdə şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumat nəzərdə tutulur. “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanununun 6-cı maddəsinə əsasən, fərdi məlumatların informasiya sistemlərinin yaradılması, dövlət qeydiyyatının aparılması və tətbiq edilməsi sahəsində hüquqi və texniki sənədləşdirmənin standartlaşdırılması, fərdi məlumatların toplanması, işlənilməsi və mühafizəsi sahəsində dövlət tənzimləməsinin əsas formalarına aiddir. Yəni xüsusi icazə olmadan vətəndaşın şəxsi həyatı haqqında məlumatların toplanması, saxlanması, istifadə olunması və yayılması qadağandır.

Fərdi məlumatların toplanılması, emalı və ötürülməsi yalnız "Fərdi məlumatlar haqqında" Azərbaycan Respublikası Qanununa uyğun olaraq həyata keçirilə bilər. Qanunda göstərilir: “Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən olunmuş qaydada fərdi məlumatların məcburi şəkildə toplanması və işlənməsi halları istisna olmaqla, hər hansı şəxs barəsində fərdi məlumatların toplanmasına və işlənilməsinə yalnız subyekt tərəfindən verilmiş yazılı, o cümlədən gücləndirilmiş elektron imzalı elektron sənəd formasında razılıq və ya özünün yazılı təqdim etdiyi məlumatlar əsasında yol verilir”. Fərdi məlumatlar açıq və gizli kateqoriyalara bölünür [2].

Fərdi məlumatların qorunması ilə əlaqədar Avropa İttifaqı, Avropa Şurası və digər beynəlxalq qurumlarda müxtəlif hüquqi sənədlər mövcuddur. Avropa İttifaqı tərəfindən fərdi məlumatların emalı və azad ötürülməsi (Directive 95/46/EC), telekommunikasiya fəzasında fərdi məlumatların istifadəsi və şəxsi həyatın toxunulmazlığının qorunması (Directive 97/66/EC) ilə əlaqədar direktivlər qəbul olunmuşdur [3, 4]. Avropa Şurası fərdi məlumatların avtomatik emalı zamanı fiziki şəxslərin qorunması ilə əlaqədar Konvensiya qəbul etmişdir. Avropa İnsan Hüquqları Konvensiyasının (*European Convention on Human Rights*) 8-ci Maddəsində göstərilir ki, fərdi məlumatlar vətəndaşın hüquqlarının ayrılmaz hissəsini təşkil edir, vətəndaşın şəxsi həyatına və yazışma sirrinə hörmət edilməlidir [5].

III. ELEKTRON DÖVLƏTDƏ FƏRDİ MƏLUMATLAR

İnformasiya cəmiyyətinin inkişafı ilə əlaqədar bu gün vətəndaş haqqında fərdi məlumatlar əsasən virtual məkandan əldə edilir. Youtube, Facebook, Wikipedia və sosial medianın müxtəlif bu kimi layihələri fərdi məlumatların əldə olunması üçün əsas mənbədir. Hər gün sosial şəbəkələrə, bloqlara, tanışlıq saytlarına milyonlarla şəkil və video-fayllar yüklənir.

DOI: 10.25045/NCInfoSec.2018.38

Milyonlarla insan öz fikirlərini, emosiya və ideologiyalarını mətn və multimedia vasitələri ilə sosial media üzərindən başqaları ilə bölüşürlər. Bu məlumatlar istifadəçinin şəxsi səhifəsində qalır və istənilən zaman onlarla on-layn tanış olmaq olar.

Bir çox hallarda daima artan və yenilənən bu açıq məlumatlar gizli fərdi məlumatların əldə olunmasına yardım edir [6]. E-dövlətin bu imkanları istifadəçinin on-layn aktivliyini (virtual izini) müəyyən edir. Məsələn, Facebook sosial şəbəkəsinə analarını öz övladları haqqında daxil etdikləri yazılar və fotoşəkilləri analiz etməklə ölkənin demoqrafiyası, səhiyyənin və təhsilin səviyyəsi haqqında geniş məlumat əldə etmək olar.

İnternet şəbəkəsi üzərindən hər hansı vətəndaş haqqında şəxsi məlumatları ictimaiyyətə ötürməklə onun nüfuzuna və sosial-iqtisadi vəziyyətinə zərbə vurma təhlükəsi mövcuddur. Məsələn, Facebook şirkəti 2015-ci ildə insanların kredit tarixini analiz edən kredit reytinqi sistemini patentləşdirmişdir. Bu isə gələcəkdə insanların taleyinin alqoritmlər tərəfindən həll olunacağı deməkdir. Artıq alqoritmlərin böyük verilənlərə tətbiqindən əldə olunan nəticələr əsasında qərarlar qəbul olunur. Lakin bu məlumatların tamlığı, dəqiqliyi, əldə olunduğu mənbənin etibarlılığı haqqında fikir söyləmək çətindir. Tətbiq olunan alqoritmlərin 100% dəqiqliklə işləməsi mümkün olmadığı üçün xətalar da vardır və bu xətalar nəticəsində vətəndaşların fərdi məlumatlarının emalında qeyri-dəqiqlik ola bilər ki, bu da vətəndaşlarla e-dövlət arasında etimadsızlıq və narazılıqlar yarada bilər [7].

IV. RƏQƏMSAL İZ

Rəqəmsal izə (*digital footprint*) veb-səhifələrdən, mobil telefonlardan, izləyici qurğulardan əldə olunan məlumatlar aiddir. Rəqəmsal izlərdən monitorinqlərdə, təhlükəsizlik məsələlərində, iqtisadi tədqiqatlarda və cəsusluqda istifadə olunur. Rəqəmsal iz rəqəmsal fəzada istifadəçi haqqında verilənlər bazasının təşkilini təmin edir. İnternetdə rəqəmsal izlər əsasən sosial media, müraciət olunan veb-səhifələr, axtarış serverlərinin bazalarındakı açar sözlər, yüklənən fayllar vasitəsilə aşkarlanır. Bu məlumatların bir hissəsi açıq, bir hissəsi isə gizli olur.

Uzaqdan idarə olunan qurğular haqqında növbəti identifikasiya üçün informasiya da rəqəmsal izlərə aiddir. E-dövlətdə rəqəmsal izlərdən İnternet istifadəçilərinin maraqlarını, davranışlarını, yerini və ictimai təşkilatlarda fəaliyyətini müəyyənləşdirmək üçün, reklam və marketinq işlərində daha yüksək göstəricilər əldə etmək üçün istifadə edilir. Belə verilənlər çox zaman istifadəçinin xəbəri olmadan toplanır və analiz olunur. Çox zaman informasiyanın hansı mənbələrdən əldə olunduğu, fərdi məlumatların xüsusiyyəti, analizdə istifadə olunan metod və alqoritmlərin dəqiqliyi və hansı məqsədlər üçün istifadə olunması gizli saxlanılır [8, 9].

Rəqəmsal izlərin analizində müxtəlif analitik yanaşmalardan istifadə olunur. Bunlara maşın təlimi, verilənlərin intellektual anlizi, “text mining”, nitqin emalı, dilin differensial analizi, LIWC (*linguistic inquiry and word count*), tematik modelləşdirmə, qərarlar ağacı və s. metodlar aiddir [10].

V. İZLƏYİCI CİHAZLAR VASİTƏSİLƏ FƏRDİ MƏLUMATLARIN TOPLANMASI

Mobil telefonlar, smart-saatlar, planşetlər, smartfonlar və aktivlik izləyiciləri (wearable activity trackers) vətəndaşların gündəlik fəaliyyətlərini izləyən, yönəldən və müəyyən tapşırıqları xatırladan müasir informasiya texnologiyalarına aid cihazlardır. Bu cihazlar insanların işini yüngülləşdirmək və dəstəkləmək üçün nəzərdə tutulmuşdur, lakin onlar insanları izləməklə əldə olunan bütün məlumatları verilənlər bazasına toplamaq qabiliyyətinə də malikdirlər və bu fərdi məlumatların sonrakı taleyi çox zaman naməlum qalır [11].

Bir çox ölkələrdə dövlət və qeyri-dövlət müəssisələri (səhiyyə, bank, sığorta şirkətləri və s.) işlərində riskləri azaltmaq üçün vətəndaşlara müxtəlif izləmə cihazlarından istifadə etməyi tövsiyə edirlər. İzləmə cihazları vasitəsilə vətəndaşın səhhəti, istirahət saatları, televiziyaya baxdığı müddət, görüşdükləri insanlar, evdəki məişət əşyalarının idarə olunması və s. haqqında gündəlik məlumatlar toplanır və müvafiq təşkilatların verilənlər bazasına ötürülür [12, 13].

Obyekt və ya vətəndaş haqqında strukturlaşdırılmış verilənlərin izləmə kameraları, sensorlar və sayğaclardan toplanaraq analiz olunması artıq geniş yayılmışdır. Məsələn, bu gün iri tikinti, neft-qaz, nəqliyyat şirkətləri avadanlıqlara xüsusi sensorlar yerləşdirməklə, həm şirkətin fəaliyyəti, həm də işçilər haqqında məlumatları toplamaqla biznеslərini yaxşılaşdırmağa, resurslara qənaət etməklə daha çox gəlir əldə etməyə çalışırlar [12].

“Ağıllı əşyalar” tərəfindən toplanan böyük verilənlərdən demoqrafiya, siyasi məsələlər, informasiya təhlükəsizliyi, biznes və s. müxtəlif məqsədlər üçün istifadə olumaqdadır. Bu əşyalar şəbəkə texnologiyaları vasitəsilə uzaqdan idarə olunaraq insanların həyatını yüngülləşdirməyə yönəlmişdir. “Əşyaların İnterneti” yalnız əşyalar haqqında deyil, onun istehsalçısı, daşıyıcısı və istehlakçısı haqqında da məlumatları toplayır. Tədqiqatçılar bildirirlər ki, “əşyaların İnterneti” və “ağıllı şəhər” gələcəkdə e-dövlət mühitində fərdi məlumatlardan istifadə etməklə bütün sistemlər və proseslər üzərində nəzarəti həyata keçirəcəklər [14, 15].

“Əşyaların İnterneti” vasitəsilə fərdi məlumatların toplanması ənənəsi genişləndikcə fərdi məlumatların təhlükəsizliyi problemi də böyüməkdə davam edir. “Ağıllı ev”, “ağıllı avtomobil” və digər bu kimi böyük verilənləri generasiya edən intellektual avadanlıqlar və qurğular yalnız məlumat toplayan xüsusi sensorlarla təchiz olunmayıblar, onlar həm də qlobal şəbəkə vasitəsilə bu məlumatları emal edən qurğulara qoşulmuşlar [16, 17].

Bu gün kontaktsız sensorlar sensor texnologiyalarının təkmilləşdirilməsinin bir nümunəsidir. Fərdi məlumatların

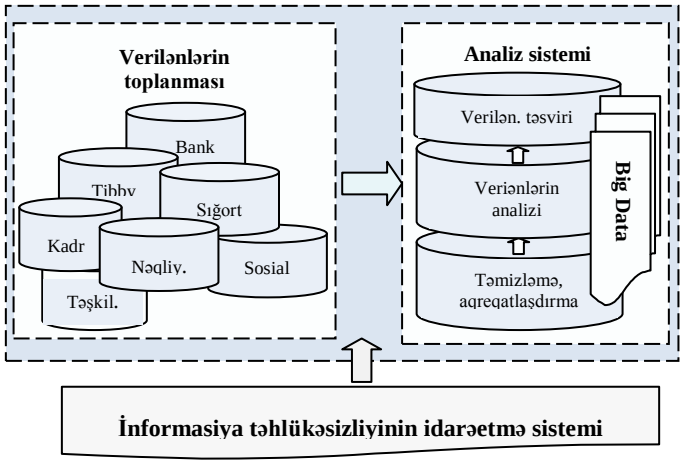
toplanmasında “əşyaların İnterneti” çox böyük əhəmiyyətə malik olsa da fərdi məlumatların ələ keçirilməsi risklərini azaltmaq üçün “əşyaların İnterneti”nin tətbiqində normativ-hüquqi tənzimləmə, gizlilik, kibertəhlükəsizlik, verlənlərin ölçüsü və əhatəliliyi, standartlaşdırma məsələlərinin həlli vacibdir. “Əşyaların İnterneti” və izləyici cihazlardan əldə olunan fərdi məlumatlar gizli məlumatlar kateqoriyasına daxildir. Bu məlumatlar sənaye, istehsal sahələri, topdan və pərakəndə satış sistemləri, kitabxanalar, elektron sənədlər, kənd təsərrüfatı, səhiyyə və məişət sferası, nəqliyyat və müxtəlif strateji sahələri əhatə etdiyinə görə, burada ilk növbədə insan hüquq və azadlıqlarının necə qorunacağı, təhlükəsizlik məsələlərinin həlli vacibdir.

VI. FƏRDİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİ

E-dövlət mühitində informasiya təhlükəsizliyinin təmin edilməsi məqsədilə mütəxəssilər tərəfindən vahid informasiya təhlükəsizliyinin idarəetmə sisteminin yaradılması təklif olunur [18]. Milli informasiya infrastrukturunun təhlükəsizliyinin idarə edilməsini nəzərdə tutan bu sistem fərdi məlumatların təhlükəsizliyinin təmin olunmasında da əhəmiyyətli ola bilər. Belə ki, fərdi məlumatların təhlükəsizliyi e-dövlət mühitində vətəndaşın sosial-iqtisadi həyatına olan təhlükələrin qarşısını almaqla, onun etimadı və nüfuzunu qorumaq üçün vacibdir.

İnformasiya təhlükəsizliyi və informasiya axtarışında rahatlığı təmin etmək məqsədi ilə bəzi fərdi məlumatların hamı üçün əlyetər olduğu açıq mənbələr mövcuddur. Belə mənbələrə ünvan kitabçaları, sorğu sistemləri, ayrı-ayrı təşkilatların veb-saytları daxildir və orada şəxsin adı, soyadı, atasının adı, doğulduğu yer və il, oxuduğu və işlədiyi müəssisə, foto-şəkli, e-mail və digər fərdi məlumatlar saxlanıla bilər. Lakin fərdi məlumatlar bu mənbələrə milli və beynəlxalq qanunlara uyğun olaraq, subyektin yazılı razılığı ilə daxil edilməli və ya məlumatın mənbəyi göstərilməlidir. Fərdi məlumatların təhlükəsizliyini təmin etmək üçün açıq və gizli mənbələr, təşkilatların informasiya sistemlərindəki fərdi məlumatların bir yerə toplayaraq vahid milli fərdi məlumatların informasiya sisteminin (FMİS) yaradılması daha məqsədəuyğundur. Fərdi məlumatların FMİS-də saxlanmasının əhəmiyyəti aşağıdakılardır:

- İnformasiyanı saxlamaq üçün əlavə resurslara ehtiyac yoxdur;
- Fərdi məlumatlarla işdə yüksək sürət və rahatlıq təmin olunur;
- Fərdi məlumatların təhlükəsizliyi təmin olunur;
- Fərdi məlumatların saxlanmasına vaxt məhdudiyyəti qoyulmur;
- Fərdi məlumatların “big data” texnologiyaları ilə analizinə şərait yaranır (verilənlər toplanır, strukturlaşdırılır).



Şəkil 1. Fərdi məlumatların informasiya sisteminin (FMİS) ümumi sxemi

FMİS-nin səmərəli işi informasiya təhlükəsizliyinin idarəetmə sistemindən sıx asılıdır. FMİS-ə gətirilən fərdi məlumatların etibarlılığını və düzgünlüyünü təmin etmək üçün aşağıdakı prinsiplərə əməl olunmalıdır:

- Fərdi məlumatların mənbəyi dəqiqləşdirilməli və düzgünlüyünə əminlik olmalıdır;
- Fərdi məlumatların istifadəsində şəffaflıq olmalıdır. Məlumatı istifadə etməyə hazırlaşan təşkilat (operator) məqsədi haqqında subyekti xəbərdar etməlidir;
- Təşkilat fərdi məlumatların təhlükəsizliyi haqqında zəmanət verməlidir;
- Fərdi məlumatların verilənlər bazasının ehtiyat sürətləri yaradılmalı və etibarlı yerdə saxlanmalıdır;
- Təşkilatla subyekt arasında qarşılıqlı etimad və inam nəzərə alınmalıdır (subyekt fərdi məlumatların onun sosial-iqtisadi rifahına və ailəsinə qarşı, qərəzli şəkildə istifadə olunmayacağına əmin olmalıdır);
- Fərdi məlumatın təhlükəsizliyi və istifadəsi üçün razılaşma mexanizmi qanun çərçivəsində, həmçinin, faktiki davranışlar nəzərə alınmaqla işlənməlidir.

NƏTİCƏ

Araşdırmalardan məlum oldu ki, e-dövlət mühitində hər hansı şirkət və ya dövlət təşkilatı tərəfindən vətəndaş haqqında informasiyanın toplanması və emalı bu istiqamətdə qəbul olunmuş milli və beynəlxalq qanunlar çərçivəsində həyata keçirilməlidir. Vətəndaşa heç bir məlumat vermədən onun fərdi məlumatlarının emalı və istifadəsi şirkətin və ya təşkilatın işində düzgünlüyün və şəffaflığın təmin olunması ilə bağlı ciddi şübhələr yarada, e-dövlət və vətəndaş, işçi və şirkər arasında münasibətlərə çiddi zərbə vurula bilər.

E-dövlət mühitində müxtəlif analitik sistemlər tərəfindən vətəndaş haqqında məlumatların analiz olunması prosesi

informasiya mübadiləsi, qərarların qəbulu, proqnozlaşdırma və risklərin qiymətləndirilməsi kimi məsələlərin həllində yeni yanaşmalar və vasitələrdən istifadə olunmasına səbəb olmuşdur. Bu vasitələr təşkilatlara və dövlət orqanlarına müxtəlif mənbələrdən əldə olunan verilənlərin nəhəng inteqrasiya sistemlərində toplamağa imkan yaradır. Lakin fərdi məlumatların mənbəyi kimi onlardan yalnız normativ-hüquqi qaydalar əsasında istifadə etmək lazımdır. Əks halda vətəndaşların fərdi məlumatlarının təhlükəsizliyi ilə əlaqədar problemlər yarana bilər.

Gizli fərdi məlumatların çinayətkarların və radikal qrupların əlinə keçməsi ehtimalı aktual olaraq qalmaqdadır. Problemin həlli ilk növbədə fərdi məlumatların toplanmasını həyata keçirən informasiya sistemlərinin düzgün təşkili və vahid informasiya təhlükəsizliyinin idarəetmə sisteminin tətbiqi ilə bağlıdır.

Minnətdarliq: Bu iş Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun maliyyə yardımı ilə yerinə yetirilmişdir **– Qrant № EİF-BGM-4-RFTF-1/2017-21/8/1**

ƏDƏBİYYAT

[1]. T. Nasser, R.S. Tariq, Big Data Challenges // Computer Engineering and Information Technology, 2015, vol. 4, no. 3., pp. 1–6.
[2]. Fərdi məlumatlar haqqında Azərbaycan Respublikasinin Qanunu, http://www.e-qanun.az/framework/19675
[3]. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, https://eur-lex.europa.eu/legal-content/en/
[4]. Directive 97/66/Ec of the European Parliament and of the Council 15 December 1997, https://eur-lex.europa.eu/legal-content/en/
[5]. European Convention on Human Rights, https://www.echr.coe.int/Documents/Convention_ENG.pdf
[6]. M.D. Back, J.M. Stopfer, S. Vazire, S. Gaddis, S.C. Schmukle, B. Egloff, S.D. Gosling, Facebook profiles reflect act ual personality, not self-idealization // Psychological Science, 2010, vol. 21, no. 3, pp. 372–374.
[7]. J. Harris, The tyranny of algorithms is part of our lives: soon they could rate everything we do, 2018. Online: https://www.theguardian.com/commentisfree/2018/mar/05/algorithms-rate-credit-scores-finances-data
[8]. M. Deakin, H.Al Waer, From intelligent to smart cities // Intelligent Buildings International, 2011, vol. 3, no. 3, pp. 140–152.
[9]. K. O’Hara, M.M. Tuffield. N. Shadbolt, Lifelogging: Privacy and empowerment with memories for life // Identity in the Information Society, 2008, vol. 1, issue 1, pp 155–172.
[10]. D. Azucar, D. Marengo, M. Settanni, Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis // Personality and Individual Differences, 2018, vol. 124, pp. 150–159.
[11]. R. Duus, M. Cooray, N.C. Page, Exploring Human-Tech Hybridity at the Intersection of Extended Cognition and Distributed Agency: A Focus on Self-Tracking Devices // Frontiers in Psychology, 2018, vol. 9, no. 1432,
[12]. R.R. Gangi, N.B. Rajesh, N.P. Sudhakar, B. Raviteja, K. Rammohanarao, Tracking objects using rfid and wireless sensor networks // International Journal Of Engineering Science & Advanced Technology, 2012, vol. 2, issue 3, pp. 513 – 517.
[13]. A. Redondi, M. Chirico, L. Borsani, M. Cesana, M. Tagliasacchi, An integrated system based on wireless sensor networks for patient monitoring, localization and tracking // Ad Hoc Networks, 2013, vol. 11, issue 1, pp. 39–53.
[14]. R. Massobrio, S. Nesmachnow, A. Tchernykh, A. Avetisyan, G. Radchenko, Towards a Cloud Computing Paradigm for Big Data Analysis in Smart Cities // Programming and Computer Software, 2018, vol. 44, iss. 3, pp. 181–189.
[15]. R.M. Əliquliyev, R.Ş. Mahmudov, Əşyalarin interneti: mahiyyəti, imkanlari və problemləri // İnformasiya cəmiyyəti problemləri, № 2(4), 2011, səh. 29–40.
[16]. Интернет вещей: Новые перспективы для людей с инвалидностью, 2015, Публикации и доклады G3ict, 22 стр., http://www.unic.ru/sites/default/files/
[17]. В. Алексеев, Модули Bluetooth, Wi-Fi и NFC производства u-blox для «Интернета вещей», Часть 2 // Беспроводные технологии, 2015, №3, стр. 23–24.
[18]. R.M. Əliquliyev, Y.N. İmamverdiyev E-dövlətin informasiya təhlükəsizliyi: aktual tədqiqat istiqamətləri // İnformasiya cəmiyyəti problemləri, 2010, №1, səh. 3–13.

SECURITY PROBLEMS OF PERSONAL INFORMATION IN E-GOVERNMENT

Alakbarova Y. Irada
Institute of Information Technology of ANAS,
Baku, Azerbaijan
airada.09@gmail.com

Abstract -- Security of personal data is an important issue in the area of e-government security. However, the method and algorithms used for collecting, cleaning, structuring and processing personal data require clarity, and any mistakes can lead to a decrease in the authority and trust of a citizen in the e- government. On this basis, the article analyzes the existing problems in the area of personal data and gives recommendations on ensuring their security in the e-government.

Keywords -- e-government, personal information, social media, tracking devices, Internet of things, digital footprint, information security