E-vətəndaşın fərdi məlumatlarının təhlükəsizliyi

Səmənnaz Zalova
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
zalova.sema@outlook.com

***Xülasə*— E-vətəndaşın fərdi məlumatlarının təhlükəsizliyi tələblərini müəyyənləşdirmək və tənzimləmək üçün istifadəçi identifikasiyasını, informasiya təhlükəsizliyi məsələsinə kompleks şəkildə yanaşma texniki və qeyri-texniki vasitələrin birgə tətbiqini tələb edir. E-dövlətdə İKT vasitələrindən istifadə dövlət-vətəndaş arasında şəxsi məlumat mübadiləsi zamanı e-hökümət saytlarında fərdi informasiyanın gizlilik siyasətini qorumalı və təhlükəsizliyini təmin etməlidir.**

***Açar sözlər— elektron vətəndaş: informasiya təhlükəsizliyi; fərdi məlumatlarının təhlükəsizliyi; gizlilik siyasəti*.**

I. GİRİŞ

İnformasiya-kommunikasiya texnologiyaları bu gün yaşadığımız həyatın ayrılmaz hissəsidir. İKT sahəsində baş verən yeniliklər həyatın bütün sahələrinə (təhsil, tibb, dövlət idarəetmə orqanları və s.) müsbət təsir edərək daha səmərəli idarə olunmasına zəmin yaradır.

Son illər inkişaf etmiş ölkələrdə demokratiyanı daha da inkişaf etdirən amillərdən biri “Elektron dövlət”in formalaşdırılmasıdır. E-dövlət - müasir informasiya texnologiyalarından istifadə etməklə dövlət qurumları tərəfindən Azərbaycan Respublikasının ərazisində yaşayan bütün vətəndaşlara, hüquqi və fiziki şəxslərə, xarici vətəndaşlara və vətəndaşlığı olmayan şəxslərə informasiya və e-xidmətlərin göstərilməsinə şərait yaradır. Yaradılan yeni imkanların əsas məqsədi xidmətlərin göstərilməsi üçün dövlət qulluqçuları və vətəndaşlar arasında olan “məsafəni” maksimum azaltmaq, bu münasibətləri sadələşdirmək və şəffaflaşdırmaqdır. Dövlət orqanları tərəfindən elektron xidmətlərin geniş tətbiqi, onların sayının və keyfiyyətin artırılması, vətəndaşların xidmətlərdən məmunluğunun yüksəldilməsi bu məqsədə çatmağın vasitələridir [1].

II. ELEKTRON VƏTƏNDAŞ VƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ

Vətəndaşlara elektron mühitdə göstərilən xidmətlər dünya təcrübəsində dövlət idarəçiliyində bir innovasiya kimi qəbul edilir.

E-dövlət quruculuğunda e-vətəndaşın formalaşmasını müəyyən edən indikatorlar verilmişdir:

- Təhsillə bağlı indikator;
- Ali təhsillə bağlı indikator;
- Əhalinin savadlılığı indikatoru;
- Şagirdlərin İKT savadlılığı indikatoru;
- Tələbələrin İKT savadlılığı indikatoru;
- Dövlət qulluqçularının İKT üzrə ümumi bilik səviyyəsi indikatoru;
- Dövlət müəssisələrində çalışan işçilərin İKT üzrə ümumi bilik səviyyəsi indikatoru;
- Əhalinin İKT üzrə ümumi bilik səviyyəsi indikatoru;
- Əhalinin kompüterdən iş məqsədilə istifadəsi indikatoru;
- Evdə kompüterə sahib olma indikatoru;
- İnternetdən müntəzəm istifadə indikatoru;
- Elektron poçtdan istifadə indikatoru [2].

E-dövlət inkişaf etdikcə vətəndaşların, istifadəçilərin həyata keçirəcəkləri əməliyyatların daha etibarlı, təhlükəsiz şəraitdə yerinə yetirilməsini aktuallaşdırır. Əsas faktoru vətəndaş olan e-dövlətin quruculuğunun uğurlu həyata keçirilməsində vacib və ən çətin məsələ e-dövlətin informasiya təhlükəsizliyinin təmin edilməsidir.

E-dövlətin informasiya təhlükəsizliyini sosiumun elə vəziyyəti kimi müəyyən etmək olar ki, bu zaman şəxsiyyət, cəmiyyət və dövlət təbii və süni meydana çıxan, informasiya və kommunikasiya axınları şəklində çıxış edən, ictimai və fərdi şüurun qəsdən deformasiya olunmasına, şəxsiyyətin, cəmiyyətin və dövlətin varlığı üçün vacib əhəmiyyəti olan infrastrukturun məhv edilməsinə yönəlmiş təhdidlərdən fasiləsiz olaraq etibarlı və hərtərəfli qorunsun.

Araşdırmalar göstərir ki, e-dövlətin informasiya təhlükəsizliyinin komponentləri aşağıdakılardır:

- informasiya fəzasının təhlükəsizlik vəziyyəti bu zaman vətəndaşların, təşkilatların və dövlətin maraqları naminə informasiya fəzasının formalaşması və inkişafı təmin edilir;
- informasiya infrastrukturunun təhlükəsizlik vəziyyəti – bu zaman informasiya yalnız öz təyinatı üzrə istifadə edilir və istifadə edildiyi zaman sistemə (obyektə) mənfi təsir göstərmir;
- informasiyanın özünün təhlükəsizlik vəziyyəti bu zaman informasiyanın tamlıq, konfidensiallıq və əlyetərlilik kimi xassələrinin pozulması istisna edilir və ya olduqca çətinləşir [3].

DOI: 10.25045/NCInfoSec.2019.18

E-dövlətin mərkəzində elektronlaşma deyil, məhz hökumət, vətəndaş dayanır. E-vətəndaşın informasiya təhlükəsizliyinin təmin edilməsi üçün reallaşdırılan üsullar, vasitələr və tədbirlər iki istiqamətdə inkişaf edir [4]:

- Texniki təhlükəsizlik
- Qeyri-texniki təhlükəsizlik.

A. Texniki təhlükəsizlik

E-vətəndaşın informasiya sistemlərinin təhlükəsizlik tələblərini müəyyənləşdirmək və tənzimləmək üçün istifadəçi identifikasiyasına daxildir:

- Şəbəkə təhlükəsizliyi;
- Gizlilik;
- Giriş nəzarəti;
- Elektron təsdiq;
- Məlumat növü;
- Məlumat mübadiləsi;
- İş axını;
- İnternet infrastrukturu və s.

B. Qeyri-texniki təhlükəsizlik

E-vətəndaşın informasiya sistemlərinin təhlükəsizlik tələblərinin reallaşdırılması üçün tələb olunur:

- Qarşılıqlı əlaqə
- Uyğunluq
- Təhlükəsizlik standartları
- Qanuni çərçivə
- Konfidensiallıq
- Mədəniyyət
- Maarifləndirmə

Qeyd etmək lazımdır ki, e-dövlətdə informasiya təhlükəsizliyi məsələsinə kompleks şəkildə yanaşma texniki və qeyri-texniki vasitələrin birgə tətbiqini tələb edir.

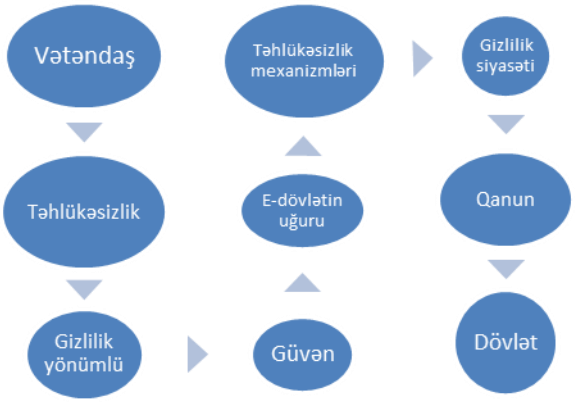
III. TƏHLÜKƏSİZLİK MODELİ: VƏTƏNDAŞ-DÖVLƏT VƏ GİZLİLİK SİYASƏTİ

Dünyanın bir çox yerində e-dövlətin tətbiqi ilə bağlı başlıca maneələrdən biri də gizlilik siyasəti və informasiya təhlükəsizliyi ilə bağlıdır. Gizlilik və ya konfidensiallıq fərdlərlə bağlı informasiyanın qorunmasına zəmanət verilməsini tələb edir. Məlum olduğu kimi elektron dövlət qurumlarında vətəndaşlarla bağlı müxtəlif məlumat bazaları formalaşıb. Vətəndaşlar dövlət qurumlarına müraciət etdikdə bu sistemlərindəki fərdi məlumatlardan istifadə edirlər, amma bu məlumatlar bəzən tam və dürüst olmur, müxtəlif dövlət orqanlarının məlumat sistemlərindəki informasiyalarda fərqlər olur, vətəndaşlar yenidən müxtəlif məlumatları təqdim etməli olur, məlumat bazaları arasında təkrarçılığa yol verilir.

Bu barədə “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının qanununun 12-ci maddəsində fiziki və hüquqi şəxslərin özləri barəsində informasiyaya buraxılmaq hüququ tanınır və bu maddənin tələblərinə əsasən, şəxsin informasiyadan kimlərin və hansı məqsədlə istifadə etdiyini bilmək hüququ vardır. Bu sahədə Azərbaycan Respublikasının tərəfdar çıxdığı digər normativ-hüquqi sənəd “Fərdi məlumatların avtomatlaşdırılmış qaydada işlənməsi ilə əlaqədar şəxslərin qorunması haqqında” 1981-ci il tarixli Avropa Şurası Konvensiyasıdır və onun əsas məqsədi şəxsi həyatın toxunulmazlığı hüququna hörmət edilməsini təmin etmək kimi müəyyən olunmuşdur [5].

Elektron dövlət xidmətlərindən istifadə etmək üçün vətəndaşın inamının artırılması və şəxs barəsində istənilən şəxsi məlumatın dövlət orqanları ilə paylaşılmasında vətəndaşın razılığının əldə edilməsi e-hökumətin tətbiqində mühüm məsələlərdəndir [6].

E-dövlətdə İKT vasitələrindən istifadə dövlət-vətəndaş arasında şəxsi məlumat mübadiləsi zamanı e-hökümət saytlarında vətəndaşın fərdi informasiyasının gizliliyini və təhlükəsizliyini təmin etməlidir. Şəkil 1.də vətəndaş-dövlət arasında gizlilik münasibətinə tələb olunan əsas amillər göstərilir. Vətəndaşın etibarlı şəkildə hökümət saytlarından istifadə etməyinə təsir göstərən 3 əsas göstərici: qanun, təhlükəsizlik və güvən əsasında həyata keçirilir. Digər tamamlayıcı vasitələr: gizlilik siyasəti, təhlükəsizlik mexanizmi e-dövlətin effektivliyinə və vətəndaşların dövlət xidmətlərinə inamına böyük ölçüdə təsir edir. Bunlar qloballaşan informasiya cəmiyyətində uğurlu e-dövlətin qurulmasına xidmət edir [7].



Şəkil 1. Vətəndaş-dövlət arasında gizlilik modeli

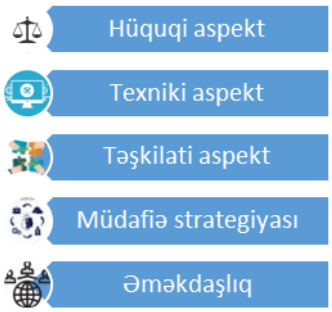
Tədqiqatçılar müasir elektron hökumət portalında kiber təhlükələrin olmasını təsdiqləməkdədirlər. Kiber – cinayətin yayılmasında əsas səbəbi İKT komponentlərinin bir-birindən

mövcud asılılığı və bu asılılığın hər mərhələdə daha da sıxlaşmasıdır. Onu da qeyd edək ki, hər bir dağıdıcı kiber hücumun “müvəffəqiyyəti” onun istismarına açıq olmasından irəli gəlir. Əgər dünya miqyasında nəşr olunmuş statistik göstəricilərə əsasən müxtəlif sahələr üzrə kiber-hücumun nəticələrini nəzərdən keçirsək maraqlı, lakin son dərəcə gözlənilməz neqativ faktlar ortaya çıxır. Məsələn, 2017-ci ildə Böyük Britaniyada Səhiyyə sahəsində fəaliyyət göstərən 236 təşkilatdan 81-i ziyan çəkmişdir. Daha doğrusu, kiber hücuma məruz qalmışdır ki, bu da iqtisadi baxımdan dövlətə 10 milyon ABŞ dollar itki deməkdir [8].

Bu mənada, güvənli e-dövlət sistemini təmin etmək üçün güclü kiber təhlükəsizlik strategiyasını hazırlanmalı və tətbiq edilməlidir. Kiber təhlükəsizlik öhdəliyinin müxtəlif aspekt-lərini, eləcə də hökumətin fərdi məlumatların gizliliyini, bütövlüyünü və mövcudluğunu təmin etmək üçün 5 əsas faktor üzrə işlənməlidir:

1. *Hüquqi aspekt;*
2. *Texniki aspekt;*
3. *Təşkilati aspekt;*
4. *Müdafiə strategiyası;*
5. *Əməkdaşlıq*.

Məhz, o zaman cəmiyyət üçün davamlı inkişafı təmin edər və ən əsası isə konfidensial bir elektron hökumət portalı istifadəyə yararlı sayıla bilər.



Şəkil 2.

Hüquqi aspekt İKT sahəsində törədilə biləcək hər hansı bir cinayət işinin qarşısının alınması üçün tədbirlər görülməsini müəyyən edir.

Texniki aspekt standartlaşdırılmış proqramların, akredetasiya sistemlərinin işlənməsini təmin edir.

Təşkilatı aspekt hər hansı bir kiber hücuma qarşı strateji mühafizəni təşkil edir.

Müdafiə strategiyası əsasən mental-siyasi effektivliyi qiymətləndirmək üçün məsul olan milli qurumların yaradılması barədə düşünməlidirlər

Əməkdaşlıq faktoru kiber təhdidlərə qarşı mübarizədə beynəlxalq əməkdaşlıq, dialoq və koordinasiya strategiyasını inkişaf etdirmək məqsədi daşıyır.

Bu faktorlar, nəticə etibarilə, kibercinayətkarlığa qarşı bey-nəlxalq mübarizəni asanlaşdıracaq tədbirlərin uyğunlaşdırıl-ması və birgə həyata keçirilə biləcək tədbirlərin təmin edilməsinə xidmət edir.

Kiber hadisələrin monitorinqi üçün göstəricilərin tərtibi də eyni dərəcədə vacibdir. Cari və keçmiş tendensiyaları müşahidə etmək, təhlükəsiz elektron hökumət sisteminin tətbiq edilməsi və daha çox kiberstrategiyanın inkişafı üçün müvafiq gələcək tədbirlərin görülməsi vacibdir. Məsələn, Hollandiyada Kiber Təhlükəsizliyin Qiymətləndirilməsinə dair hesabat ilə tanış olduqda kiber təhlükəsizlik inkişafını ölçmək üçün meyarlardan istifadə edildiyinin şahidi oluruq. Milli Kiber Təhlükəsizlik Mərkəzi qeydiyyatı sistemindən istifadə edərək, annotasiya hesabatları, təhlükəsizlik tövsiyələri və hadisələri tərtib edilir. Bu baxımdan, kiber təhlükəsizlik tədbirlərinin mövcudluğu bir ölkənin kiber təhlükəsizlik inkişafı ilə bağlı balanslı və qərəzsiz məlumatlar təmin etmək üçün bir sıra qəbul edilmiş qanuni tədbirlərin həyata keçirilməsi ilə nəticələnir.

NƏTİCƏ

Göründüyü kimi, e-vətəndaşın fərdi məlumatlarının təhlükəsizliyi qorunması sahəsində Azərbaycanda kifayət qədər möhkəm hüquqi baza formalaşdırılmaqdadır. Hüquqi sənədlərdə nəzərdə tutulan prinsipləri rəhbər tutan elektron dövlətin gizlilik siyasəti vətəndaşların şəxsi toxunulmazlığını qoruyur və fərdi məlumatların yalnız qanuni məqsədlər üçün toplanması və istifadəsinə zəmanət versə də, informasiya təhlükəsizliyi ilə bağlı məsələ elektron vətəndaşı narahat edən əsas problemlərdən biri kimi hələ də aktualdır.

İSTİNADLAR

[1] Elektron Hökumət Bülleteni. Bülleten № 05, may 2013. 12 s. https://www.e-gov.az/home/getfile/163

[2] Z. Q. Cəbrayılova “Elektron dövlətdə insan resurslarının formalaşması: mövcud təcrübə, problemlər və perspektivlər,” İnformasiya cəmiyyəti problemləri, 2015, №1, 48-55.

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

[4] M. Al-Jamal & E. Abu-Shanab “Privacy policy of e-Government websites and the effect on users’ privacy,” The 7th International Conference on Information Technology, 2015, pp.338-344.

[5] http://e-qanun.gov.az/framework/3525

[6] The United Nations E-Government Survey 2012: E-Government for the People. United Nations Department of Economic and Social Affairs. 2012, 160 p.

[7] Shareef M. Shareef. “Enhancing security of information in e-Government,” Journal of Emerging Trends in Computing and Information Sciences, 2016, Vol. 7, No. 3, pp 139-146.

[8] Формирование устойчивого электронного правительства. Исследование ООН: электронное правительство. Нью-Йорк, 2018, стр. 67-71.

SECURITY OF E-CITIZEN'S PERSONAL DATA

Samannaz Zalova

Institute of Information Technology of ANAS, Baku, Azerbaijan

zalova.sema@outlook.com

Abstract— The approach to the issues as the identification of the user, information security in a complex form for defining and regulating the demands of security of E-citizen information systems requires the applying of the technical and non-technical methods together. The usage from the devices of Information Communication Technologies must provide the security and protect the policy of the confidentiality of individual information in the sites of E-Government during the exchange of the personal information between the government and citizen in E-Government.

Key words— *electron citizen, information security, security of personal data, privacy policy*