UOT 004.056:351/354 DOI: 10.25045/jpis.v12.i2.09

Yusifov F.F.[1], Fərəcova A.C.[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]farhadyusifov@gmail.com, [2]aysanpharajova@gmail.com

E-İDARƏETMƏDƏ FƏRDİ MƏLUMATLARIN QORUNMASI: "DATA SƏFİRLİYİ" KONSEPSİYASI

Məqalədə e-idarəetmədə fərdi məlumatların qorunması sahəsində beynəlxalq təcrübə araşdırılmış və ümumiləşdirmələr aparılmışdır. E-idarəetmədə məlumatların təhlükəsizliyinin təmin olunması sahəsində bir sıra ölkələrin təcrübəsi, o cümlədən Estoniya hökumətinin qəbul etdiyi "Data səfirliyi" konsepsiyası tədqiq olunmuşdur. "Data səfirliyi" konsepsiyası hökumətin yerli məlumat mərkəzlərinin fəaliyyətinin təbii fəlakət, geniş miqyaslı kiberhücum və ya digər böhran vəziyyətində dayandırıldığı bir şəraitdə fəaliyyətini davam etdirməsinə imkan verir. Bununla yanaşı, "Data səfirlikləri" daha yüksək əlyetərlilik zəmanəti versə də, bəzi verilənlərin və ya xidmətlərin qorunması, məlumatın məxfiliyi və bütövlüyü ilə bağlı problemlər səbəbilə hazırda fərdi (xüsusi) buludda yerləşdirilməsi mümkün deyil. Azərbaycanda fərdi məlumatların qorunması sahəsində mövcud vəziyyət və hökumət buluduna keçid prosesi analiz olunmuşdur. Hökumət buludu konsepsiyası dövlət orqanlarının malik olduğu informasiya sistemlərinin beynəlxalq standartlara cavab verən vahid data mərkəzi infrastrukturunda dayanıqlı, çevik, təhlükəsiz və səmərəli fəaliyyətinə zəmin yaradır. Hökumət buluduna keçidin mühüm komponetlərindən biri təhlükəsizliyin təmin olunmasıdır. Məqalədə Milli Data mərkəzinin arxitekturunun həm fiziki, həm də kibertəhlükələrə qarşı təhlükəsizlik tədbirləri göstərilmişdir. Beynəlxalq təcrübədə məlumatların buluda ötürülməsi və təhlükəsizliyinin təmin olunmasına dair müxtəlif yanaşmalar olmasına baxmayaraq, rəqəmsal fasiləsizlik təşəbbüsü dövlət xidmətlərinin əlyetərli olmasını, real vaxtda və istənilən vəziyyətdə istifadə oluna bilməsini və yenilənməsini tələb edir. Hökumət buluduna keçid səmərəli e-idarəetmə mexanizmlərinin işlənməsinə, məlumat mübadiləsinin təhlükəsizliyinin təmin olunması üçün təhlükəsizlik həllərinin işlənməsinə və fərdi məlumatların qorunmasına, e-xidmətlərin keyfiyyətinin artırılmasına və vətəndaş məmnuniyyətinin yüksəldilməsi imkan verəcəkdir.

Açar sözlər: *e-idarəetmə, fərdi məlumatların qorunması, hökumət buludu, "Data səfirliyi".*

Giriş

Elektron idarəetmə dedikdə xidmətlərin göstərilməsinin və informasiyanın çatdırılmasının səmərliliyini artırmaq, vətəndaşların qərar qəbuletmə prosesində iştirakını təşviq etmək və hökuməti daha hesabatlı, şəffaf və təsirli etmək məqsədi ilə dövlət sektorunun informasiya və kommunikasiya texnologiyalarından istifadə edilməsi başa düşülür. Nəticə etibarı ilə e-idarəetmə dövlət xidmətləri və idarəetmənin demokratik aspektlərini yaxşılaşdırmağa xidmət edir. E-idarəetmənin inkişaf etdirilməsilə fərdi məlumatların qorunması xüsusilə aktuallaşmışdır. Texnologiyanın sürətli inkişafı və İKT-nin geniş tətbiqi vətəndaşlar üçün yeni risklər və təhdidlər yaradır. Aydındır ki, fərdi məlumatlar daha çox dövlət reyestrlərində toplanır. Reyestrlərin yaradılması dövlət xidmətlərinin əlyetərliyinin təmin olunması, təhsil sisteminin idarə edilməsi, səhiyyə və sosial müdafiə sistemlərinin səmərəliliyinin artırılması, vətəndaşların təhlükəsizliyi, gəlir və vergilərin idarə olunması, demokratik seçkilərin keçirilməsi və s. bu kimi bir sıra məqsədlərə xidmət edir.

İnformasiya-kommunikasiya texnologiyalarının (İKT) inkişafının vətəndaşların və ya şirkətlərin işində müsbət inkişafa səbəb olacağına əmin olunsa da, fərdi məlumatların nəzarətsiz dövriyyəsi şəxsi həyatın toxunulmazlığına müxtəlif təhlükələr yarada bilər. Fərdi məlumatların qorunması milli siyasət məsələsi kimi qəbul edilməli və lazım olan hüquqi və texnoloji infrastruktur sürətlə hazırlanmalıdır. Bundan əlavə, rəqəmsal texnologiyalar insan həyatının bütün sahələrində baş verə biləcək qanunsuzluqların qarşısını almaq üçün hüquqi tənzimləmələrin

olmasına ehtiyac yaradır. Fərdlərin özlərinə aid olan verilənlər "fərdi məlumatlar" adlanır. Bu məlumatlar təşkilatlar tərəfindən saxlanılır, işlənilir və tələb olduqda isə üçüncü tərəfə ötürülür.

Dövlət təşkilatlarına müxtəlif ictimai qurumlar, xüsusən də dövlət və özəl hüquq sektorundakı gəlir gətirən təşkilatlar və qeyri-hökumət təşkilatları daxil edilir. Peşə sahəsində isə fərdi məlumat toplayıcılarına həkim, vəkil, notarius və bankçılıq kimi peşələri aid etmək olar. Bir sözlə, cəmiyyətdə demək olar ki, hər kəs məlumat toplayır, onları qiymətləndirir və dəyişdirir.

Hazırda bütün ölkələr vətəndaşlarına daha yaxşı e-xidmətlər təklif edə biləcək səmərəli e-idarəetmənin formalaşdırılmasına səy göstərirlər. Bu baxımdan bulud texnologiyaları hökumətlər və vətəndaşlar üçün geniş imkanlar yaradır. Məsələn, IDC (International Data Corporation) korporasiyasının araşdırmalarına görə, 2016-2018-ci illərdə səlahiyyətli rəhbər şəxslərin, məmurların 70%-i yeni xidmətləri tətbiq edərkən bulud əsaslı texnologiyalardan istifadəyə üstünlük vermişlər [1]. Təşkilatlar sürət, miqyaslaşma və iqtisadi baxımdan üstünlüklər əldə etmək üçün sürətlə bulud texnologiyalarını tətbiq etməyə çalışırlar. 2013-cü ildə Estoniya hökuməti elektron hökumətə olan innovativ yanaşmasını və nəyin bahasına olursa olsun milli rəqəmsal davamlılığı təmin etmək ehtiyacını əks etdirən "Data səfirliyi" təşəbbüsünü həyata keçirməyə başladı. Fiziki və ya kiber fövqəladə vəziyyətlərdə davamlılığın, təhlükəsizliyin və fasiləsizliyin təmin olunmasında bulud texnologiyalarından istifadə effektiv həllərin işlənməsinə imkan verir. Hazırda Estoniya vətəndaşları dövlət və özəl sektorda, demək olar ki, bütün əməliyyatları rəqəmsal formada həyata keçirə bilirlər.

Texnologiyanın sürətlə inkişaf etdiyi, vətəndaşların, cəmiyyətin və ölkələrin iqtisadi, sosial, mədəni olaraq bir-birinə yaxınlaşdığı dünyada fərd öz şəxsi məlumatlarını və hüquqlarını qorumaqda daha da çətinlik çəkir. Əvvəllər informasiya sistemlərində və arxivlərdə saxlanılan və az sayda insanın əldə edə biləcəyi bəzi fərdi məlumatlar günümüzdə texnologiyaların inkişaf etməsi vasitəsi ilə sadəcə bir kliklə əldə edilə biləcək qədər asan olmuşdur. Başqa şəxslərin əlinə keçə biləcək məlumatların təhlükəsizliyi, kimlərin hansı şərtlərdə bu məlumatları əldə edə biləcəyi və bir başqa şəxsə, ya da quruma ötürə biləcəyi aktual mövzulardan biridir.

Məqalə fərdi məlumatlar sahəsində beynəlxalq təcrübənin analizi məsələlərinə həsr olunmuşdur, ölkələrin təcrübəsində fərdi məlumatların saxlanılmasına, kənar infrastruktura ötürülməsinə və bu prosesləri yerinə yetirən mövcud yanaşmalara baxılır, qəbul edilmiş qanunlar araşdırılır.

Fərdi məlumatların qorunması ilə bağlı beynəlxalq təcrübə

Fərdi məlumatlar konfidensial informasiya kateqoriyasına aid edilir. Fərdə məxsus olan məlumatların əldə edilməsi, emalı və istifadəsi onun icazəsi ilə olmalı və toplandığı məqsədlərə uyğun olaraq istifadə edilməlidir. Fərdi məlumatların saxlanması, onlara girişin və istifadəsinin təmin edilməsi üçün hüquqi səviyyədə tənzimlənmiş qanunlar, müqavilələr və təhlükəsizlik infrastrukturlarından faydalanmaqla həyata keçirmək olar [2].

Nümunə kimi tibbi məlumatların de-identifikasiyası üçün ABŞ federal qanunu HIPAA-nın (Health Insurance Portability and Accountability Act – tibbi sığortanın portativliyi və hesabatlılığı) tərtib etdiyi təhlükəsiz liman mexanizmini göstərə bilərik. Təhlükəsiz liman mexanizmi fərdin və ya qohumlarının, ailə üzvlərinin və ya işə götürənlərin 18 spesifik identifikatorunun silinməsini tələb edir. Bunlara adlar, ünvanlar, tarixlər, telefon nömrələri, faks nömrələri, tibbi sığorta nömrələri, elektron poçt ünvanları, sosial sığorta nömrələri, tibbi sənədləşmə nömrələri, hesab nömrələri, lisenziya və ya sertifikat nömrələri, maşın identifikatorları və seriya nömrələri, qurğu identifikatorları və seriya nömrələri, URL (Universal Resource Locator), IP ünvanları, biometrik identifikatorlar, üzün tam fotoşəkilləri və identifikasiyanın başqa unikal nömrəsi, xarakteristikası və ya kodu aiddir [3].

Bütün bu məlumatlar kompüter vasitəsi ilə ötürüldükdə çox zərərli bir yanaşma və təhlükə üçün asan bir mühit yarada bilər. Bu məlumatların köməyi ilə bəzi insanlar seçkilərdə verilən səsləri saxtalaşdıra, vergi borcunu silə, ölən bir adamın yerinə keçə, məlumatları dəyişə və s. bu

kimi bir çox saxtakarlıqları yerinə yetirə bilər, ya da başqasına zərər vermək üçün məlumatlar dəyişdirilə bilər və ən vacibi ümumdünya və konstitusiya hüquqları olan şəxslərin məlumatlarının məxfiliyi pozula bilər.

Şəxs haqqında bədniyyətlinin əlində olan fərdi məlumatlar cinayət silahına, işdən çıxarılan işçinin əlində qisas vasitəsinə və ya rəqib şirkətə satılan mallara çevrilir. Buna görə fərdi məlumatların qorunması sahəsində ciddi mexanizmlər işlənilməlidir. Hazırda informasiya texnologiyaları və informasiya cəmiyyəti sürətlə inkişaf edir. İnsan şəxsi ehtiyaclarından və ya zəruriyyətdən müxtəlif formalarda fərdi məlumatların təqdim edilməsini tələb edən xidmətlərdən istifadə edir. Bu baxımdan e-xidmətlərdən istifadə zamanı hər bir şəxsi düşündürən əsas məsələ fərdi məlumatların təhlükəsizliyinin nə dərəcədə təmin olunmasıdır. Əgər effektiv e-dövlət həllərindən söhbət gedirsə, dövlət səviyyəsində qanunvericilik bazasının təkmilləşdirilməsi, fərdi məlumatların qorunması sisteminin işlənilməsi informasiya sızması ilə bağlı mövcud problemlərin aradan qaldırılmasına və fərdi məlumatların icazəsiz ələ keçirilməsi, emalına qarşı güclü immunitetə malik vasitələr yaradılmasına imkan verər. Beynəlxalq təcrübədə fərdi məlumatların təhlükəsizliyinin təmin olunmasına dair müxtəlif yanaşmalar vardır.

Avropa Birliyi dörd əsas ideyaya əsaslanır: əşyaların, şəxslərin, xidmətlərin və kapitalın sərbəst hərəkəti [4]. Fərdi məlumatların toplanması və işlənməsi bu dörd əsas məqsədin yerinə yetirilməsi üçün vacib olduğundan, Avropa Birliyində fərdi məlumatların qorunmasına yönəlmiş qaydalar, informasiya texnologiyalarının inkişafı ilə birlikdə AB daxilindəki ümumi bazarın tələblərini nəzərə alır və təməl hüquqlara uyğun olaraq pulsuz məlumat trafikini idarə edir. Burada məqsəd hücumun ortaya çıxması halında təşkil ediləcək qorumadan əlavə baş verə biləcək hücumlara qarşı profilaktik tədbirlərin görülməsidir. Buna görə də fərdi məlumatların qorunması və potensial hücumların minimuma endirilməsi üçün hücumdan əvvəl sistematik qorunma təmin edilməlidir [5,6].

Məsələn, Almaniya qanunlarında vətəndaşlara fərdi məlumatlarının hansı hallar olduqda açıqlanacağına və bu məlumatdan necə istifadə olunacağına qərar vermək səlahiyyəti verilir və bu da ona fərdi məlumatlarının kimə ötürüldüyünü idarə etməyə imkan verir. Bu vəziyyət şəxsin razılığını ön plana çıxarır, çünki bu vasitə ilə onların məlumatlarına çıxışlarını müəyyənləşdirmək hüququ verilir.

Avropa Birliyinin təşkil etdiyi təlimatın 6-cı maddəsində "Məlumatların keyfiyyəti prinsipləri" ilə bağlı xüsusi qaydalar qeyd edilmişdir. Bu prinsiplər şəxsi məlumatların qanuna və dürüstlüyə uyğun işlənməsi üçün nəzərdə tutulmuşdur:

Məqsədə sadiqlik: məlumatların yalnız qanuna uyğun açıq və sərhədləri bilinən məqsəd istiqamətində toplanması və işlənməsi prinsipidir. Bu prinsipə əsaslanaraq məlumatların emalından əvvəl fərd şəxsi məlumatlarının hansı məqsədlə toplandığını öyrənir.

Xüsusi məqsədlərin mövcudluğunda məqsədin təqdim edilməsi: Toplanan məlumatların tarixi, statistik və ya elmi məqsədlər üçün istifadə olunmasına icazə verilir. Bununla birlikdə, üzv ölkələr tərəfindən məqsədin doğruluğunun təsdiq olunması üçün kifayət qədər zəmanət tələb olunur.

Lazımlılıq prinsipi və saxlanmanın qadağan edilməsi: Emal edilən fərdi məlumatların əldə oluna biləcəyi məqsəd üçün səbəb bağlantısı olmalıdır. Toplanmış məlumatlar yalnız məqsəd üçün lazım olduqda istifadə edilə bilər. Digər tərəfdən, gələcəkdə nəzərdə tutulan məqsədə xidmət edə biləcək məlumatların saxlanması qadağandır.

Maddi gerçəklik, məlumatların yenilənməsi, silinməsi və düzəldilməsi: Məlumatların düzgünlüyünü və aktuallığını təmin etmək üçün hər hansı bir ziddiyyət olduqda məlumat silinməli və ya yenidən düzəldilməlidir.

Saxlama müddəti: Məlumatların nəzərdə tutulmuş məqsədə çatmasına qədər saxlanması qanunidir, bu müddət keçdikdən sonra, məlumatların saxlanmasını davam etdirmək üçün məlumatları anonimləşdirmək lazımdır.

Amerika Birləşmiş Ştatlarında fərdi məlumatların qorunması üçün qüvvəyə minmiş ən vacib hüquqi tənzimləmələrdən biri olan 1974-cü il tarixli "Məxfilik aktı" adlı qanun, fərdlərin tanınmasını yerinə yetirəcək fərdi məlumatların dövlət tərəfindən qorunması, əldə edilməsi, istifadə edilməsi və paylaşılması qanunlarını özündə birləşdirir.

Fərdi məlumatların gizliliyinin qorunması ilə bağlı qeyd edilən "Məxfilik aktı"nın əsas prinsiplərini aşağıdakı kimi ümumiləşdirmək olar:

- Fərdi məlumatlar və həssas məlumatlar xüsusi qorunmalıdır.
- Dövlət vətəndaşların fərdi məlumatlarının qorunmasına cavabdehdir.
- Fərdi məlumatlar şəffaf şəkildə emal edilməli və məlumat sahibinə özünə aid olan fərdi məlumatların hansı şəkildə emal edildiyi ilə əlaqəli məlumat verilməlidir.
- Şəxsi məlumatların məxfiliyini təmin etmək üçün qanunun müddəalarının effektiv şəkildə yerinə yetirilməsi və lazımi nəzarətin təmin edilməsi vacibdir.

"Məxfilik Aktı" federal qurumlara yuxarıda göstərilən prinsiplərə uyğunluğu təmin etmək üçün vətəndaşların fərdi məlumatlarının qorunması məqsədilə zəruri təhlükəsizlik mexanizmini yaratmağı tövsiyə edir. Fərdi məlumatların gizliliyinə dair müddəalar pozulduğu təqdirdə qanun cəza müddəalarının tətbiq edilməsini tələb edir və bununla əlaqadar şəxs tərəfindən kompensasiya tələbi ilə iddia qaldırmaq da mümkündür [7].

Rusiya Federasiyasında fərdi məlumatların istifadəsini tənzimləyən federal qanun 2006-cı ildə qəbul edilmişdir. Qanuna müxtəlif illərdə dəyişikliklər olunsa da 2015-ci ildə qanunda fərdi məlumatların tənzimlənməsinə dair ciddi tələblər qoyulmuşdur. Belə ki, müxtəlif operatorlar tərəfindən fərdi məlumatların ayrı-ayrı məqsədlər üçün istifadəsinin qarışısını almaq üçün qanun ölkə vətəndaşlarının fərdi məlumatlarının emalının və saxlanmasının yanlız ölkə hüdudlarında yerləşən verilənlər bazasında istifadəsinə dair operatorlar qarşısında ciddi öhdəlik qoymuşdur.

Rusiyanın təhlükəsizlik qanunu mürəkkəbdir. Bir sıra Rusiya qanunlarının birləşməsi bütün sektorlar üzrə məxfiliyin hərtərəfli qorunmasını təmin edir. Rusiya qanununun AB təlimatı ilə bir çox oxşarlığı var. Ancaq qanunun icrası məhdud görünür. Rusiya Asiya-Sakit Okean İqtisadi Əməkdaşlığı Təşkilatının (Asia-Pacific Economic Cooperation (APEC)) üzvüdür, lakin APEC Sərhədlərarası Məxfilik Qaydaları (Cross-Border Privacy Rules (CBPR)) sistemində iştirak etmir.

Rusiyanın Rabitə, İnformasiya Texnologiyaları və Kütləvi Kommunikasiyalar sahəsində nəzarət üzrə Federal Xidməti (*Roskomnadzor*) məlumatların toplanması və emalına nəzarəti gücləndirmək üçün məlumat operatorlarından rəsmi qeydiyyat tələb edir [8]. Bununla birlikdə, 2015-ci ilin sentyabrından etibarən operatorların Rusiya vətəndaşlarının fərdi məlumatlarının ölkə hüdudlarında yerləşən serverlərdə saxlanmasını təmin etməsi qanuni tələbdir. Federal Xidmət operatorların fəaliyyətini tənzimləyir və tələblərin icrasına nəzarət funksiyasını həyata keçirir.

Estoniya son iyirmi ildə inkişaf dinamikasına görə Dünya Bankının tərtib etdiyi 2016-cı il üzrə "Dünya inkişaf hesabatı"nda ölkə "rəqəmsal cəmiyyətə ən yaxın" adlandırılmışdır [9]. Estoniya dünyada birinci "Data səfirliyi"ni Lüksenburqda açmışdır [10]. Bu, o deməkdir ki, ölkədə məlumatların qorunması sahəsində tətbiq olunan bütün qaydalar onun "Data səfirliyi"ndə də tətbiq olunmalıdır. Qeyd edək ki, Lüksenburq dövləti Estoniyanın informasiya sisteminin verilənlərinin toxunulmazlığına zəmanət vermişdir. Lüksenburqda informasiya cəmiyyətinin yüksək səviyyədə inkişafı rəqəmsal xidmətlər sahəsində əməkdaşlıq üçün geniş imkanlar yaratmışdır.

Bu yeni yanaşma Estoniya dövlətinin yerli məlumat mərkəzlərinin təbii fəlakət, geniş miqyaslı kiberhücum, elektrik kəsilməsi və ya digər böhran vəziyyətinə görə dayandırıldığı və ya pozulduğu bir şəraitdə fəaliyyətini davam etdirməsinə imkan verir [10].

Estoniya hökuməti 2019-cu ildə fərdi məlumatların istifadəsi və emalını tənzimləyən qanun qəbul etmişdir [11]. Qəbul olunmuş qanun Avropa Birliyinin reqlamentinə uyğun insanların öz fərdi məlumatlarının idarə olunması imkanlarını genişləndirir və üçüncü şəxslər tərəfindən emalını tənzimləyir. Qanun qəbul olunduqdan sonra müəssisələr və təşkilatlar istifadəçilərə onların fərdi məlumatlarını necə emal etdikləri barədə daha ətraflı və aydın məlumat verməlidirlər və şəxsin tələbi ilə bu məlumatları silməlidirlər (məlumatların saxlanması üçün başqa qanuni əsaslar olmadıqda).

Fərdi məlumatların qorunması haqqında qanun böyük ictimai maraqlar səbəbindən edilərsə və jurnalist etikası prinsiplərini pozmadığı təqdirdə şəxsin fərdi məlumatlarının mediada yayımlanmasına imkan verir. Məlumatların qorunması üsullarından istifadə edildiyi təqdirdə şəxs haqqında məlumatlar elmi-tədqiqat və statistik məqsədlər üçün onun icazəsi olmadan da toplana və emal edilə bilər. Eləcə də, qanuna əsasən fərdi məlumatları emal edənlər şəxsi məlumatlara dair qanun pozuntuları barədə şəxsə məlumat vermək öhtəliyini öz üzərlərinə götürməyə məcburdurlar [12]. Fərdi Məlumatların Mühafizəsi Qanunu qanun pozuntularının qarşısının alınması, aşkarlanması və icra edilməsi və cəzanın icrası zamanı hüquq mühafizə orqanları tərəfindən fərdi işlərin aparılması, fərdi məlumatların işlənməsi üçün xüsusi əsasları nəzərdə tutur. Sonda qanunda fərdi məlumatların qorunması qaydalarının pozulması halında yeni tərtib olunan cərimələr qeyd olunur.

“Data səfirliyi” konsepsiyası

“Data səfirliyi” – Estoniya hökumətinin buluda inikasıdır və bu, dövlətin ərazi hüdudlarından kənarda server resurslarına sahib olması mənasını verir. Bu informasiyanın əldə edilməsi üçün innovativ konsepsiya hesab olunur, çünki adətən dövlətlər informasiyalarını öz fiziki sərhədləri daxilində saxlayırlar. “Data səfirliyi”nin resursları Estoniya dövlətinin nəzarətindədir, kiberhücumlardan və böhran situasiyalarından blokçeyn texnologiyasının köməyi ilə mühafizə olunur və təkcə verilənlərin ehtiyat nüsxələrinin yaradılması deyil, eləcə də kritik xidmətlərin yerinə yetirilməsi imkanına malikdir [10].

“Data səfirliyi” dedikdə Data mərkəzi nəzərdə tutulur. Data mərkəzi Lüksenburqda verilənlərin ötürülməsi üçün ən yüksək təhlükəsizlik səviyyəsində (“*Tier IV*” standartına uyğun) qorunur. Bu, ənənəvi diplomatik mənada başa düşülən səfirlik deyil, lakin təsis müqaviləsi diplomatik münasibətlər haqqında Vyana Konvensiyasını nəzərə almaqla beynəlxalq hüquqda tamamilə yeni bir yanaşmadır [10]. Data mərkəzi Estoniyanın tam nəzarəti altındadır, lakin toxunulmazlıq kimi fiziki səfirliklərlə eyni hüquqlara malikdir.

Lüksemburq yüksək keyfiyyətli texniki imkanlarına görə NATO standartlarına cavab verən yüksək etibarlı data mərkəzlərinin olması, həm də bu yeni konsepsiya ilə işləmək üçün açıq olduğundan “Data səfirliyi”nin yerləşdiyi ilk yer hesab edilə bilər. Bu əməkdaşlıqla Lüksemburq və Estoniya dünyada rəqəmsal davamlılığı təmin etmək üçün unikal və innovativ bir yol seçmişlər. Bu yeni yanaşma, Estoniya dövlətinin yerli Data mərkəzlərinin təbii fəlakət, genişmiqyaslı kiberhücum, elektrik kəsilməsi və ya digər böhran vəziyyətinə görə dayandırıldığı və ya pozulduğu bir şəraitdə fəaliyyətini davam etdirməsinə imkan verir [10]. Server Estoniya ərazisində müvafiq sistemlərin işləmədiyi halda vergilər, pensiyalar, mülkiyyət hüquqları, qanunvericilik fəaliyyəti və siyahıyaalma məlumatlarına əlyetərliyinin təmin olunması üçün yaradılmışdır.

“Data səfirliyi”nin açılışı 2015-ci ildə olsa da, Estoniya və Lüksemburq arasında yekun müqavilənin imzalanması 2017-ci ildə mümkün olmuşdur. Estoniyanın hökumət buludunun inkişaf etdirilməsi *Cybernetica*, *Dell EMC*, *Ericsson*, *OpenNode* və *Telia* kimi şirkətlərlə Estoniya hökumətinin əməkdaşlığı çərçivəsində həyata keçirilmişdir [13].

Rəqəmsal transformasiyalar və e-idarəetmə konsepsiyasına keçidin Estoniyaya gətirdiyi üstünlüklər dövlət administrasiyasının daha çevik, effektli və əlyetərli olmasına şərait yaratdı [14]. Ənənəvi səfirlikdən fərqli olaraq bu “Data səfirliyi” diplomatik məqsədə xidmət etmir [15]. Bu daha çox Estoniyanın dövlət qurumlarının e-idarəetmə şəbəkələrini dəstəkləyən bulud data mərkəzidir [16]. Data səfirliyi hökumətin kritik serverlərini diplomatik cəhətdən etibarlı bir yerə köçürən ilk ölkə təcrübəsini təqdim edir. Suverenlik, idarəetmə təhlükəsizliyi və hökumətin davamlılığı ilə bağlı bir eksperiment olan “Data səfirliyi” hər hansı səbəbdən nə vaxtsa ərazi müstəqilliyi itirilərsə hökumətin yenidən fəaliyyətə başlaması üçün bir ehtiyat mərkəz rolunu oynayır. Estoniyanın “Data səfirliyi”nin məqsədi yalnız serverlərin başqa ölkənin ərazisindən saxlanması ilə məhdudlaşmır. Eləcə də Estoniya hökuməti mürəkkəb yüksək texnoloji sistemlərin qurulması və istismarı üçün texniki imkanlar nümayiş etdirir. Ölkədə bir və ya bir neçə serverin

kiber və ya fiziki hücumla sıradan çıxarıldığı halda, e-idarəetmə əməliyyatlarının dəstəklənməsi məqsədilə güclü server sistemi yaradılmışdır [17]. Buna baxmayaraq, Estoniya kiçik ölkədir və kiberməkanına və ya ərazisinə qarşı hücumlar bütün e-idarəetmə infrastrukturunu strateji olaraq məhv edə bilər. Lüksemburqda ehtiyat serverin yerləşdirilməsi Estoniya hökuməti üçün demək olar ki, ikinci dərəcəli ehtiyat sistem rolunu oynayır. Qeyd etmək lazımdır ki, Estoniyanın hüdudlarından kənarda yerləşdirilən bulud serverləri başqa bir dövlətin yurisdiksiyasına tabe olan qurumlar və ya infrastrukturla əməkdaşlıq çərçivəsində həyata keçirilmir. Bunun əvəzinə, Estoniya Lüksemburqla əməkdaşlıq edərək beynəlxalq hüquqda tamamilə yeni bir qurum yaratmışdır. Belə ki, "Data səfirliyi" Lüksemburq dövlətinin sərhədləri daxilində Estoniyanın suveren diplomatik ərazisidir - heç bir dövlət, şirkət və ya qurum Estonya hökumətinin razılığı olmadan infrastruktura daxil olmaq və ya məlumatlarına çıxış hüququna malik deyil. Digər vacib məqam odur ki, Microsoft və ya AWS-ə qarşı hər hansı bir kiberhücum Estoniyanın e-idarəetmə buludunu çökdürə bilməz, çünki Estoniyanın e-idarəetmə buludu Estoniya dövləti tərəfindən idarə olunur [17]. Üstəlik Estoniya daha çox bulud mərkəzləri yaratmaqla mümkün kiberhücumların sayını minimuma endirməyin mümkün olacağını güman edir. Hər hansı səbəbdən hökumət öz funksiyalarını yerinə yetirə bilməzsə Lüksemburqdakı data səfirliyi ehtiyat mərkəz funksiyalarını dayandıracaq və ölkə ərazisinin hüdudlarından kənarda da Estoniya hökumətinin əsas e-idarəetmə infrastrukturu olacaqdır. Bu o deməkdir ki, Estoniya hökuməti, hətta mühacirətdə olsa da, onlayn olaraq təqdim etdiyi mühüm dövlət xidmətlərini eyni ilə göstərməyə davam edə bilər [18]. Məsələn, xarici ölkələrin icazəsinin olub-olmamasından asılı olmayaraq, nəzəri baxımdan Estoniya diasporası səsvermədə iştirak etməyə, vergi ödəməyə, vətəndaşlıq almağa və mühacir hökumətlə çox sayda inzibati yolarla qarşılıqlı əlaqəyə davam edə bilər. Belə demək mümkündürsə, Estoniyanın "Data səfirliyi" proqramı – kiber qurumlarının kiber-təhdidlərə qarşı davamlılığını artıraraq suveren qurumlarının stabilliyini artırmış oldu.

Bu təşəbbüs Estoniyaya hökumətin idarə olunmasında və xidmətlərin, əməliyyatların davamlılığının təmin edilməsində əlavə təhlükəsizlik tədbirlərinin görülməsinə imkan verir, o cümlədən buraya elektron və məlumat fasiləsizliyi (ehtiyat nüsxələr), məlumatların tamlığı, fiziki və ya kiber fövqəladə vəziyyətdə əsas dövlət xidmətləri aid edilir. Bu hədəflərə çatmaq üçün Estoniya üç hissədən ibarət bir həll planı təklif edir [19]:

1. Məlumatların ehtiyat nüsxələrinin və göstərilən xidmətlərin Estoniya sərhədləri daxilində saxlanılması (Hökumət Buludunun formalaşdırılması);
2. Hökumət tərəfindən seçilən müttəfiq ölkələrdə Estoniya səfirliklərinin yerləşdiyi məkanlarda və ya ayrılmış Data mərkəzlərində ehtiyat nüsxələrin saxlanması (Fiziki "Data səfirliyi");
3. Özəl şirkətlərin ümumi buludundakı həssas olmayan məlumatların ehtiyat nüsxələri (Virtual "Data Səfirliyi").

Təşəbbüsün hər üç hissəsinə bir-birini tamamlayan komponentlər kimi baxılmalıdır. Hökumət buludu çərçivəsində Estoniya fiziki sərhədləri daxilində əlavə data mərkəzlərinin və e-hökumət xidmətləri üçün ehtiyat nüsxələrin yaradılmasını planlaşdırır. Bununla yanaşı, rəqəmsal fasiləsizlik konsepsiyası, dövlət xidmətlərinin əlyetərli olmasını, real vaxtda və istənilən vəziyyətdə istifadə oluna bilməsini və yenilənməsini tələb edir. Qeyd edək ki, virtual data səfirlikləri daha yüksək əlyetərlik zəmanəti versə də, bəzi verilənlərin və ya xidmətlərin (məsələn, dövlət sirri hesab olunan məlumatların) məlumatların qorunması, məxfiliyi və bütövlüyü ilə bağlı problemlər səbəbilə hazırda fərdi (xüsusi) bulud xidmətində yerləşdirilməsi mümkün deyil [19]. Buna baxmayaraq, ictimai buludların istifadəsi bütün riskləri aradan qaldırmasa da, hazırda ən geniş yayılmış kiberhücumlarla mübarizə imkanları bir çox təşkilatların potensialından daha yüksəkdir. Eləcə də Estoniyanın fiziki sərhədləri xaricində və qlobal bulud mühitində yerləşməsi, ictimai buludu virtual data səfirliyi konsepsiyasının reallaşdırılmasını daha effektiv edir.

Azərbaycanda fərdi məlumatların qorunması: hökumət buluduna keçid

"Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu 2010-cu ildə qəbul edilmiş, 2014 və 2018-ci illərdə müəyyən dəyişikliklər edilərək ölkədə müvafiq sahələr üzrə fəaliyyət göstərən əsas qanunvericilik aktıdır. Bu qanun fərdi məlumatların toplanması, işlənməsi və mühafizəsi ilə bağlı münasibətləri, milli informasiya məkanının fərdi məlumatlar bölümünün formalaşdırılması, habelə fərdi məlumatların sərhəddən kənar ötürülməsi ilə əlaqədar məsələləri tənzimləyir, bu sahədə fəaliyyət göstərən dövlət və yerli özünüidarə orqanlarının, hüquqi və fiziki şəxslərin hüquq və vəzifələrini müəyyən edir. Bu qanuna əsasən qeyd etmək olar ki, fərdi məlumatlar şəxsin kimliyini birbaşa və ya dolayısı ilə tanımağa imkan verən istənilən növ məlumat hesab olunur. Fərdi məlumatların toplanılması və işlənilməsi, həmin məlumatların mühafizəsinin tam təmin olunmaması nəticəsində subyektə dəyən maddi və mənəvi ziyan və onun həcmi məhkəmə tərəfindən müəyyən edilir, qanunvericilikdə nəzərdə tutulmuş qaydada ödənilir. Bu qanunun əsas məqsədi fərdi məlumatların toplanmasının, işlənilməsinin və mühafizəsinin qanunvericilik əsaslarını və ümumi prinsiplərini, həmin sahədə dövlət tənzimləməsinin qayda və tələblərini, fərdi məlumatların informasiya ehtiyatlarında formalaşdırılması, informasiya sistemlərinin yaradılması, informasiyanın verilməsi və ötürülməsi qaydalarını, bu prosesdə iştirak edən şəxslərin hüquqlarını, vəzifələrini və məsuliyyətinin əsaslarını müəyyən etməkdən, əsas insan və vətəndaş hüquqlarını və azadlıqlarını, o cümlədən şəxsi və ailə həyatının sirrini saxlamaq hüququnu müdafiə etməkdən ibarətdir [20].

Müasir hüquq konsepsiyası fərdin "toxunulmaz xəzinəsi" hesab olunan fərdi məlumatlarının qorunması üzərində qurulub. Bu səbəblə, insanların həyatını asanlaşdırmaq üçün inkişaf etdirilən məlumatların yığılması və ötürülməsi texnologiyaları ilə fərdi hüquqların pozulmasının qarşısını almaq üçün ölkələr qanuni tənzimləmələrə müraciət etmişdirlər.

Hazırda ölkəmiz dünya standartlarına cavab verən, gəlirlərini ədalətli bölüşən, insan hüquqlarını, qanunun aliliyini, iştirakçı demokratiyanı, dünyəviliyi, din və vicdan azadlığını təmin edən bir dövlət olmaq üçün səylərini artırır. Ölkəmizdə e-dövlətin inkişafı, "rəqəmsal hökumət"ə keçidin təmin edilməsi, rəqəmsal platformalara transformasiya, elektron xidmətlərin yaradılmasına və göstərilməsinə tələb olunan dövlət xərclərinin optimallaşdırılması, informasiya sistemlərinin fəaliyyətinin keyfiyyətli, dayanıqlı və təhlükəsiz infrastrukturda təşkilinin təmin edilməsi, vətəndaşların resurslara sərbəst çıxış imkanının yaradılması məqsədilə "bulud" texnologiyasının tətbiqi son dərəcə əhəmiyyətli məsələdir. Dövlət informasiya sistemlərinin və ehtiyatlarının formalaşdırılması, saxlanılması, aparılması və inteqrasiyasının effektiv təşkili yolu ilə dövlət idarəçiliyində xərclərin minimuma endirilməsi və dövlət qurumları arasında koordinasiyanın yüksəldilməsi "Hökumət buludu"nun (G-cloud) yaradılmasını zəruri edir. Bu məqsədlə "Hökumət buludu"nun (G-cloud) yaradılması və "bulud" xidmətlərinin göstərilməsi sahəsində tədbirlər haqqında" Azərbaycan Respublikası Prezidentinin 2019-cu il 3 iyun tarixli 718 nömrəli Fərmanı ilə təsdiq edilmiş "Hökumət buludu" (G-cloud) Konsepsiyası hazırlanmışdır [21]. Hökumət buludunun yaradılması ölkədə dayanıqlı, təhlükəsiz və səmərəli İKT infrastrukturunun yaradılmasına və onun vasitəsilə dövlət qurumlarının informasiya sistemlərinin və ehtiyatlarının istismarına imkan verir. Hökumət buludu konsepsiyası dövlət orqanlarının malik olduğu informasiya sistemlərinin beynəlxalq standartlara cavab verən vahid data mərkəzi infrastrukturunda dayanıqlı, çevik, təhlükəsiz və səmərəli fəaliyyətinə zəmin yaradır. Bulud texnologiyasının tətbiqi ilə dövlət informasiya sistemlərinin və ehtiyatlarının təhlükəsiz saxlanıldığı, dayanıqlı infrastrukturda mərkəzləşdirilmiş qaydada formalaşdırıldığı və həyata keçirildiyi data mərkəzi isə hökumətin milli məlumat məkanıdır. Hökumət buludu sahəsində beynəlxalq təcrübə tədqiq olunmuş, Böyük Britaniya, Amerika Birləşmiş Ştatları, Norveç, Türkiyə və eləcə də Estoniya təcrübəsində data səfirliyi konsepsiyası göstərilmişdir. Ölkəmizdə də hökumət buluduna yanaşma beynəlxalq təcrübəyə əsaslanır. Hökumət buludunun yaradılması dövlət orqanları üçün mərkəzləşdirilmiş, təhlükəsiz, dayanıqlı infrastruktur yaradılmasına xidmət edəcəkdir. Hökumət buludu Konsepsiyası aşağıdakı məqsədlərə xidmət edəcəkdir:

• Ölkədə bulud texnologiyasından istifadənin genişləndirilməsi, dövlət qurumlarının fəaliyyətlərində səmərəliliyin artırılması;
• Bulud texnologiyasının tətbiqi ilə səmərəli idarəetmənin və istifadənin təşkili, xərclərin azaldılması;
• Dövlət informasiya resurslarından məkandan asılı olmayaraq fasiləsiz istifadə və xidmət keyfiyyətinin artırılması;
• Data mərkəzin infrastrukturundan səmərəli istifadə edilməsi;
• Dövlət informasiya sistemlərinin effektiv təşkili və dayanıqlı infrastrukturda yerləşdirilməsi;
• Dövlət qurumlarının infrastruktur və xidmət tələbatına uyğun Hökumət buludunda təmin edilməsi;
• Dövlət informasiya sistemlərinin və ehtiyatlarının Hökumət buluduna keçidinin və miqrasiyasının həyata keçirilməsi;
• Elektron xidmətlərin keyfiyyətinin artırılması və vətəndaş məmnuniyyətinin yüksəldilməsi;
• Dövlət informasiya sistemləri və ehtiyatları arasında fasiləsiz, təhlükəsiz və operativ məlumat mübadiləsinin həyata keçirilməsi;
• Hökumət buluduna ötürülən məlumatların təhlükəsizliyinin təmin olunması üçün təhlükəsizlik həllərinin işlənməsi və fərdi məlumatların qorunması.

Hökumət buluduna keçidin mühüm komponetlərindən biri informasiya təhlükəsizlyidir. İnformasiya təhlükəsizliyinin və fərdi məlumatların qorunması ilk olaraq risklərin qiymətləndirilməsindən başlanır. Hökumət buludunda fəaliyyətin fasiləsizliyi üçün yüklənmələr balanslaşdırılmalı, klasterizasiya, rezervləmə və bərpa sistemi, virtuallaşdırma texnologiyaları tətbiq olunmalıdır. Konsepsiyada Data mərkəzdə informasiya təhlükəsizliyi üçün kiberhücumlardan qorunma, məlumat itkisinin və sızmasının qarşısının alınması, bulud infrastrukturunun monitorinqi və müntəzəm hesabatlılıq, trafikin monitorinqi, müdaxilələrin aşkarlanması və qarşısının alınması kimi açar elementləri tətbiq edilir [21].

Verilənlər bazalarını, infrastrukturu, şəbəkələri və ya fərdi kompüterləri hədəfə alan, fərdi məlumatların ələ keçirilməsi və məlumat mənbələrinə zərər verə biləcək kiberhücumlardan qorunmaq son dərəcə vacib məsələlərdir. Serverlərin qorunması və trafikin yüklənməməsi, kənar müdaxilələri və insidentləri istisna etmək üçün "dərin təhlükəsizlik" (deep security) və istifadəçilərin harada olmasından asılı olmayaraq, mübadilə edilən məlumatların təhlili üzrə "ağıllı qorunma" (smart protection) həlləri bulud infrastrukturunun təhlükəsizliyinin kompleks şəkildə qorunmasına təminatdır [21]. Eyni zamanda, Hökumət buludunun kibertəhlükəsizliyinin təmin edilməsi məqsədilə beynəlxalq standartlar əsasında milli standartların hazırlanması və tətbiqi olduqca vacibdir.

2020-ci ildə təsdiq olunmuş "Dövlət informasiya sistemlərinin və ehtiyatlarının "Hökumət buludu"na Keçid Planı"nın təsdiq edilməsi və "Hökumət buludu" ilə bağlı bəzi tədbirlər haqqında qərara əsasən dövlət informasiya sistemlərinin və ehtiyatlarının mərhələli şəkildə "Hökumət buludu"na keçidi nəzərdə tutulmuşdur [22]. Dövlət informasiya sistemlərinin Hökumət buluduna keçid planı özündə 2020-2024-cü illər üzrə mərhələli şəkildə Hökumət buluduna miqrasiyanı əhatə edir. Hökumət buludunun arxitekturası məlumatların açıqlığı və məxfiliyi baxımından hər dövlət qurumu üzrə 4 zonaya bölünür: 3 sinfə ayrılmış təhlükəsizlik zonası və bulud xidmətlərinə nəzarət olunması, həmçinin virtual maşınların idarə edilməsi üçün müəyyənləşdirilmiş zona. Keçid planında Hökumət buludunun Milli Data Mərkəzinin arxitektur elementlərinin həm fiziki, həm də kibertəhlükəsizliyinin təmini üçün nəzərdə tutulan tədbirlər Cədvəl 1 - də göstərilmişdir [22]:

Cədvəl 1. Data Mərkəzin fiziki və kibertəhlükəsizliyinin təmini üçün tədbirlər

Fiziki təhlükəsizlik tədbirləri	Kibertəhlükəsizlik tədbirləri
Beynəlxalq standartlara uyğunluq	Sistemlərin yerləşdirilməsi çərçivəsi
İqlim sabitliyi	Şəbəkə platforması
Bağlantı imkanları	Şəbəkə perimetrinin qorunması
Mərkəzlərarası təhlükəsiz məsafə	Dövlət informasiya resurslarının auditi
Fasiləsiz iş şəraiti	İnternet bağlantılarının təhlükəsizliyi
Təhlükəsizlik və monitorinq	Şəbəkə hücumlarının mühafizəsi
Elektrik enerjisinin həcmi	Virtual maşınların təhlükəsizliyi
Enerji təhlükəsizliyi	Seqmentasiya
Fiziki mühafizə	Açıq bölgə zonasının müdafiəsi
Fövqəladə hallarda etibarlı fəaliyyət	Autentifikasiya

Hökumət buludunun Milli Data Mərkəzinin arxitekturunda həm fiziki, həm də kibertəhlükələrə qarşı təhlükəsizlik tədbirləri xüsusi yer tutur. Keçid planında Hökumət buludu şəbəkəsinin ayrılmış bağlantılarla təminatı, habelə fövqəladə hallar zamanı bu şəbəkədə kanalların alternativliyi baxımından dövlət qurumlarına fasiləsiz xidmətləri verəcək əlavə bağlantının mövcudluğu təmin olunmalıdır. Təhlükəsizlik baxımından aktiv, ehtiyat və arxiv mərkəzlərinnin fırtınalar, daşqınlar və digər hər hansı təbii fəlakətlərə eyni zamanda məruz qalmamaları üçün bir-birindən kifayət qədər uzaq məsafədə (>100 km) yerləşdirilməsi nəzərdə tutulur. Yarana biləcək nasazlıqların aradan qaldırılması üzrə tədbirlərin dərhal görülməsinə və təhlükəsizliyə fasiləsiz nəzarət edilməlidir.

Keçid planında Milli Data Mərkəzinin informasiya təhlükəsizliyini təmin etmək üçün şəbəkə platformasının, dövlət informasiya resurslarının, internetə çıxış bağlantılarının və şəbəkə hücumlarının mühafizəsi üçün tədbirlər öz əksini tapmışdır. Onlayn rejimdə kiberhücumların qarşısının alınması üçün sistemin, şəbəkənin və tətbiqlərin davranış təhlili əsasında istifadəçilərə mane olmadan hücumları geri qaytarmağa imkan verən infrastruktur formalaşdırılmalıdır. Burada yalnız xarici kiberhücumlar deyil, eləcə də, daxili şəbəkədən baş verə biləcək hücumlar nəzərdə tutulmalıdır. Bununla yanaşı, istifadəçilərin buluda transfer olunan məlumatlarının mühafizəsi, əməliyyatlar zamanı fərdi məlumatların qorunması üçün mexanizmlərin işlənməsi, çoxfaktorlu identifikasiyanı təmin edən həllərin tətbiqi, istifadəçilərin virtual serverlərini qorumaq üçün təhlükəsizlik vasitələrindən, alətlərindən istifadə olunması diqqət mərkəzində saxlanılmalıdır.

Nəticə

Hazırda dünya ölkələri vətəndaşlarına daha yaxşı e-xidmətlər təklif edə biləcək səmərəli e-idarəetmənin formalaşdırılmasına səy göstərirlər. Bu baxımdan bulud texnologiyaları hökumətlər və vətəndaşlar üçün geniş imkanlar yaradır. E-idarəetmənin inkişaf etdirilməsi fərdi məlumatların qorunması və informasiya təhlükəsizliyinin təmin olunmasını zəruri edir. Fərdi məlumatların təhlükəsizliyi, insan hüquqları və əsas azadlıqlar təkcə ali ümumbəşəri dəyərlər deyil, həm də iqtisadi və siyasi sabitliyin və inkişafın ən etibarlı təməli hesab olunur.

Məqalədə məlumatların təhlükəsizliyinin təmin edilməsi sahəsində beynəlxalq təcrübə araşdırılır. Ölkələrin təcrübəsində fərdi məlumatların saxlanılmasına, xaricə ötürülməsinə və bu proseslərin yerinə yetirilməsinə dair yanaşmalara baxılır və qəbul edilmiş qanunlar şərh olunur. Fərdi məlumatların qorunmasına dair bir sıra ölkələrin, o cümlədən Avropa Birliyi, Rusiya, Estoniya, ABŞ kimi ölkələrin təcrübəsi araşdırılmışdır. Estoniya hökumətinin irəli sürdüyü Data səfirliyi təşəbbüsü dövlətin buluda transformasiyasıdır və bu dövlətin ərazi hüdudlarından kənarda server resurslarına malik olmasını göstərir. Rəqəmsal transformasiyalar və e-idarəetmə strategiyasının qəbul edilməsi Estoniyaya gətirdiyi inanılmaz üstünlüklər dövlət

administrasiyasının daha çevik, effektli və əlyetərli olmasına şərait yaratdı. "Data səfirliyi" hökumətin mühüm serverlərini diplomatik cəhətdən etibarlı bir yerə transfer edən ilk ölkə təcrübəsidir. Bunlarla yanaşı, Estoniya hökumətinin Data səfirlik yanaşması daha yüksək əlyetərlilik zəmanəti versə də, xüsusilə konfidensial məlumatların qorunması ilə bağlı problemlər səbəbilə məlumatların fərdi buludlara ötürülməsi və saxlanması müzakirə obyekti olaraq qalmaqdadır. Ölkəmizdə e-dövlətin inkişafı, rəqəmsal platformalara transformasiya, e-xidmətlərin səmərəliliyinin artırılması, informasiya sistemlərinin fəaliyyətinin keyfiyyətli, dayanıqlı və təhlükəsiz infrastrukturda təşkilinin təmin edilməsi, vətəndaşların resurslara fasiləsiz çıxış imkanının yaradılması məqsədilə "bulud" texnologiyasının tətbiqi son dərəcə əhəmiyyətli məsələdir. Hökumət buludunun yaradılması, ölkədə dayanıqlı, təhlükəsiz və səmərəli İKT infrastrukturunun yaradılmasına və onun vasitəsilə dövlət qurumlarının informasiya sistemlərinin istismarına imkan verir. Məqalədə hökumət buludunun məqsədləri, eləcə də, Milli Data mərkəzin arxitekturunun həm fiziki, həm də kibertəhlükələrə qarşı təhlükəsizlik tədbirləri göstərilmişdir. Hökumət buluduna keçid səmərəli e-idarəetmə mexanizmlərinin işlənməsinə, "açıq hökumət" təşəbbüsünün həyata keçirilməsinə, informasiya təhlükəsizliyi və məlumatlardan istifadəyə dair milli standartların hazırlanmasına imkan verəcəkdir.

Minnətdarlıq

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

Ədəbiyyat

1. Worldwide and Regional Public Cloud ICT Services 2014-2018 Forecast, https://www.idc.com/getdoc.jsp?containerId=prUS25219014
2. Purtova N. The law of everything. Broad concept of personal data and future of EU data protection law, 2018, https://doi.org/10.1080/17579961.2018.1452176
3. Imamverdiyev Y.N. E-Sahiyyada Informasiya Tahlükasizliyinin Aktual Problemlari // Informasiya jamiyyati problemlari, 2017, №1, sah. 24–34.
4. Communication from the Commission to the European Parliament and the Council, Data protection rules as a trust-enabler in the EU and beyond – taking stock, https://www.eur-lex.europa.eu
5. Lehavi A., Larouche P., Accetto M., Purtova N., Zemer L. The Human Right to Privacy and Personal Data Protection: Local-to-Global Governance in the Digital Era, 2016, https://www.lawschoolsgloballeague.com
6. Data Protectıon Laws of The World, 2017, https://www.thebackgroundinvestigator.com
7. Cobb S. Data privacy and data protection: US law and legislation, April 2016, pp. 3-1
8. Personal Data Regulation in Russia: Roskomnadzor Update. 2019.
9. World Development Report 2016: Digital Dividends, https://www.worldbank.org
10. Data embassy, https://www.e-estonia.com
11. Personal Data Protection Act, https://www.riigiteataja.ee
12. Digital Government Factsheet 2019, Estonia? https://www.joinup.ec.europa.eu
13. Rijgikogu prinyal zakon o sozdanii posol`stva danny`kh v Lyuksemburge, 2018, http://www.rus.err.ee
14. Yuliya Talmazan, "Data Security Meets Diplomacy: Why Estonia Is Storing Its Data in Luxembourg," NBCNews.com (NBCUniversal News Group, June 25, 2019), https://www.nbcnews.com/news/world/data-security-meets-diplomacy-why-estonia-storing-its-data-luxembourg-n1018171
15. Data Embassy – e-Estonia, e-Estonia (Government of Estonia, 2019), https://www.e-estonia.com/solutions/e-governance/data-embassy/

16. Sierzputowski B., The Data Embassy Under Public InternationalLaw // International and Comparative Law Quarterly 68, 2019, no 1, pp. 225-242, https://doi.org/10.1017/s0020589318000428
17. Security and Safety – e-Estonia, e-Estonia (Government of Estonia, 2019), https://www/e-estonia.com/solutions/security-and-safety/
18. Governance – e-Estonia, e-Estonia (Government of Estonia, 2019), https://www.e-estonia.com/solutions/e-governance/
19. Implementation of the Virtual Data Embassy Solution, https://www.microsoft.com/en-us/cybersecurity/content-hub/implementation-of-the-virtual-data-embassy-solution
20. "Fardi malumatlar haggında" Azarbayjan Respublikasının Ganunu, 11 may 2010-ju il, https://www.e-qanun.az
21. "Hokumat buludu"nun (G-jloud) yaradılması va "bulud" khidmatlarinin gostarilmasi sahasinda tadbirlar haggında Azarbayjan Respublikası Prezidentinin Farmanı, Bakı shahari, 3 iyun 2019-ju il, http://www.e-qanun.az/framework/42560
22. "Dovlat informasiya sistemlarinin va ehtiyatlarının "Hokumat buludu"na Kechid Planı"nın tasdig edilmasi va "Hokumat buludu" ila baghlı bazi tadbirlar haggında Azarbayjan Respublikası Nazirlar Kabinetinin Gararı, Bakı shahari, 29 oktyabr 2020-ji il, http://www.e-qanun.az/framework/46243

UOT 004.056:351/354

Юсифов Фархад Ф.[1], Фараджова Айсан Дж.[2]
[1,2] Институт информационных технологий НАНА, Баку, Азербайджан
[1]farhadyusifov@gmail.com, [2]aysanpharajova@gmail.com

Защита персональных данных в электронном управлении: концепция «Посольство данных»

В статье исследуется и обобщается международный опыт в области защиты персональных данных в э-управлении. Был изучен опыт ряда стран в области защиты данных в э-управлении, в том числе концепция «Посольство данных», принятая правительством Эстонии. Концепция «Посольство данных» позволяет правительству поддерживать работу местных центров обработки данных во время стихийных бедствий, крупномасштабных кибератак или других кризисов. Однако хотя «Посольство данных» гарантирует более высокую доступность, некоторые данные или услуги в настоящее время не могут размещаться в личном (частном) облаке из-за проблем с защитой, конфиденциальностью и целостностью данных. В статье анализируются текущая ситуация в сфере защиты персональных данных в Азербайджане и процесс перехода к правительственному облаку. Концепция правительственного облака создает основу для устойчивой, гибкой, безопасной и эффективной работы информационных систем, принадлежащих государственным учреждениям, в единой инфраструктуре центра обработки данных, соответствующей международным стандартам. Одна из важных составляющих перехода к правительственному облаку − обеспечение информационной безопасности. В статье показаны меры защиты архитектуры Национального центра обработки данных от физических и киберугроз. Несмотря на то, что в международной практике существуют разные подходы к передаче данных и безопасности в облаке, инициатива по обеспечению непрерывности цифрового вещания требует, чтобы общедоступные услуги были доступны в реальном времени и актуальны.

Ключевые слова: *э-управление, правительственное облако, защита личных данных, «Посольство данных»*.

Farhad F. Yusifov[1], Aysan C. Farajova[2]

[1,2]Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]farhadyusifov@gmail.com, [2]aysanpharajova@gmail.com

Protection of personal data in electronic governance: "Data embassy" concept

The paper studies and summarizes the international experience in the field of personal data protection in e-governance. The data security experience of various countries in e- governance was studied, including the concept of "Data Embassy" adopted by the Estonian government. The "Data Embassy" concept allows the government to keep local data centers operational in the periods of a natural disaster, large-scale cyberattack or other crisis. However, while "Data Embassies" guarantee higher accessibility, some data or services cannot currently be hosted in a personal (private) cloud due to issues such as data protection, confidentiality and integrity. The paper investigates the current situation in the field of personal data protection and the process of transition to the government cloud in Azerbaijan. The Government cloud concept creates the basis for sustainable, flexible, safe, and efficient operation of information systems owned by government agencies in a single data center infrastructure that satisfies international standards. One of the important components of the transition to the Government cloud is to ensure information security. The paper represents the patterns to protect the architecture of the National data center against physical and cyber threats. Though there exist different approaches in the international practice to data transfer and security in the cloud, the digital continuity initiative requires public services to be accessible, be used in real-time or in any situation, and update. The transition to the government cloud will provide effective e-government mechanisms, promoting security solutions to ensure data exchange security and personal data protection, develop the quality of e-services, and increase citizen satisfaction.

Keywords: *e-governance, government cloud, personal data protection, "Data embassy".*