**AZƏRBAYCAN
MİLLİ ELMLƏR AKADEMİYASI
RƏYASƏT HEYƏTİ**

**AZƏRBAYCAN
MİLLİ ELMLƏR AKADEMİYASI
İNFORMASIYA TEXNOLOGİYALARI İNSTITUTU**

**“İNFORMASIYA TƏHLÜKƏSİZLİYİNİN AKTUAL
MULTİDİSSİPLİNAR ELMİ-PRAKTİKİ PROBLEMLƏRİ”
V RESPUBLİKA KONFRANSININ
ƏSƏRLƏRİ**

**FƏRDİ MƏLUMATLARIN
MÜHAFİZƏSİ**

Bakı, 29 noyabr 2019

“İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri”

V respublika konfransının

ƏSƏRLƏRİ

Bakı, 29 noyabr 2019-cu il

PROQRAM KOMİTƏSİ

Sədr

akademik Rasim Əliquliyev

ÜZVLƏR

Rəşid Ələkbərov

Məsumə Məmmədova

Ramiz Alıquliyev

Yadigar İmamverdiyev

Fərqanə Abdullayeva

Təhmasib Fətəliyev

Ramiz Şıxəliyev

Rasim Mahmudov

Bikəs Ağayev

Əlövsət Əliyev

Fərhad Yusifov

İradə Ələkbərova

Lyudmila Suxostat

Məkrufə Hacırəhimova

Məmməd Həşimov

Rəna Qasımova

Tofiq Kazımov

Şəfəqət Mahmudova

Rəsmiyə Mahmudova

Babək Nəbiyev

Zərifə Cəbrayılova

Elmi redaktorlar:

Ramiz Alıquliyev

Yadigar İmamverdiyev

ISBN: 978-9952-530-06-3

DOI: 10.25045/NCInfoSec.2019

Mündəricat

<i>Rasim Əliquliyev, Yedgar Cəfərov, Əfruz Qurbanova, İnformasiya cəmiyyəti şəraitində Azərbaycan vətəndaşlarının identifikasiyası problemləri və onların həlli yolları haqqında.....</i>	<i>8</i>
<i>Ramiz Aliquliyev, Şəlalə Tahirzadə, Böyük həcmli fərdi məlumatların analizi üçün iterativ çəkili k-means alqoritmi.....</i>	<i>13</i>
<i>Məsumə Məmmədova, Zərifə Cəbrayilova, Tibbi sosial media istifadəçilərinin fərdi məlumatlarının təhlükəsizliyi məsələləri.....</i>	<i>17</i>
<i>Rasim Əliquliyev, Rasim Mahmudov, Milli mentalitetdə fərdi məlumatların yeri və onların mühafizəsi problemləri.....</i>	<i>21</i>
<i>Hikmət Quliyev, Milli mentalitet və stereotiplər kontekstində fərdi məlumatlara həssaslığın folklorik təzahürləri.....</i>	<i>25</i>
<i>Fərhad Yusifov, Aysən Fərəcova, Fərdi məlumatların qorunması sahəsində beynəlxalq təcrübənin analizi.....</i>	<i>31</i>
<i>Rəşid Ələkbərov, Arzu Həsənlı, Buludlarda fərdi məlumatların mühafizəsi problemləri.....</i>	<i>35</i>
<i>Rəna Mirzəzadə, Fərdi məlumatların tənzimlənməsinə siyasi-hüquqi nəzər: beynəlxalq və Azərbaycan qanunvericiliyi.....</i>	<i>38</i>
<i>Rasim Mahmudov, Fərdi məlumatların “qara bazar”ının xüsusiyyətləri və yaratdığı problemlər.....</i>	<i>41</i>
<i>Yadigar İmamverdiyev, Xəyalə Əhmədova, Sosial şəbəkələrdə saxta profillərin aşkarlanması metodları haqqında.....</i>	<i>45</i>
<i>Техмасиб Фаталиев, Шакир Мехмиев, О защите персональных данных в системах, реализуемых на основе концепции Industry 4.0.....</i>	<i>49</i>
<i>Sabirə Ocaqverdiyeva, İnternetdə uşaqların fərdi məlumatlarının qorunması vəziyyətinin analizi.....</i>	<i>53</i>
<i>İradə Ələkbərova, Sosial kredit sistemlərində fərdi məlumatların idarə edilməsi problemləri.....</i>	<i>57</i>
<i>Yadigar İmamverdiyev, Firəngiz Sadiyeva, Kriptovalyutalarda konfidensiallıq və anonimlik problemləri.....</i>	<i>61</i>
<i>Gulara Muradova, Mehran Hematyar, Protecting and securing medical records using blockchain technology.....</i>	<i>66</i>
<i>Şəfəqət Mahmudova, Fərdi məlumatların proqram vasitələri ilə qorunması üsullarının araşdırılması.....</i>	<i>70</i>
<i>Yadigar İmamverdiyev, Konfidensiallığı qorumaqla fərdi məlumatların intellektual analizi üçün Deep Learning metodları.....</i>	<i>74</i>
<i>Səmənnaz Zalova, E-vətəndaşın fərdi məlumatlarının təhlükəsizliyi problemləri.....</i>	<i>81</i>
<i>Fərqanə Abdullayeva, Sabirə Ocaqverdiyeva, Uşaqların fərdi məlumatları əsasında İnternet asılılığın müəyyən olunması üsulu.....</i>	<i>85</i>
<i>Məkrufə Hacırahimova, Mərziyə İsmayılova, Sosial şəbəkələrdə fərdi məlumatların təhlükəsizliyi problemləri və onların həlli yolları.....</i>	<i>88</i>
<i>Людмила Сухостат, Вопросы защиты персональных данных в киберфизических системах.....</i>	<i>92</i>

<i>Шакир Мехмиев, Тахмасиб Фаталиев, Аяз Мехмиев, Системы видеонаблюдения в нефтегазовом комплексе: Безопасность производственных структур и защита персональных данных.....</i>	<i>97</i>
<i>Rəşid Ələkbərov, Səməd Dursunov, Mürsəl Qurbanlı, Korporativ elektron poçt sistemində təhlükəsizlik məsələləri.....</i>	<i>101</i>
<i>Fərqanə Abdullayeva, Buludlarda fərdi məlumatların konfidensiallığına yönəlmiş hücumlar və müdafiə mexanizmləri.....</i>	<i>105</i>
<i>Ramiz Şıxəliyev, İnternet mühitində fərdi məlumatların təhlükəsizliyinin monitorinqi problemləri.....</i>	<i>110</i>
<i>Elçin Əliyev, Fərdi məlumat subyektlərinin hüquqlarını mühafizə mexanizmlərinə etimad səviyyəsinin ölçülməsi metodu.....</i>	<i>113</i>
<i>Kəmalə Qurbanova, Elektron mühitdə pasiyentlərin fərdi məlumatlarının mühafizəsinin aktual problemləri.....</i>	<i>119</i>
<i>Фирудин Агаев, Гюльра Мамедова, Эсмира Алескерова, Проблемы защиты информации субъектов электронного университета в облачной среде.....</i>	<i>122</i>
<i>Гюльра Мамедова, Лала Зейналова, Рена Меликова, Методы обеспечения безопасности персональных данных в электронном образовании.....</i>	<i>126</i>
<i>Kəmalə Həşimova, İnternet-reklam və marketing fəaliyyətində fərdi məlumatların təhlükəsizliyi.....</i>	<i>130</i>
<i>Аловсам Алиев, Некоторые проблемы информатизации процессов защиты персональных данных и пути их решения.....</i>	<i>134</i>
<i>Sünbül Zəlova, Kütləvi media resurslarında fərdi məlumatların mühafizəsi problemləri.....</i>	<i>139</i>
<i>Nərgiz Verdiyeva, Vətəndaş elmi layihələrində fərdi məlumatların təhlükəsizliyinin təmini məsələləri.....</i>	<i>142</i>
<i>Məkrufə Hacırahimova, Aybəniz Əliyeva, Big Data mühitində fərdi məlumatların təhlükəsizliyi.....</i>	<i>146</i>
<i>Firudin Əsgərov, Rəhilə Həsənova, Elektron kitabxanalarda fərdi məlumatların təhlükəsizliyi məsələləri... </i>	<i>150</i>
<i>Oqtay Ələkbərov, Mobil avadanlıqlarda fərdi məlumatların təhlükəsizliyi məsələləri.....</i>	<i>153</i>
<i>Günəl Vəliyeva, Fərdi məlumat subyektlərinin hüquqlarının təhlili.....</i>	<i>156</i>
<i>Rəşid Ələkbərov, Məmməd Həşimov, Fog computing texnologiyalarında istifadəçi məlumatlarının təhlükəsizliyi məsələləri.....</i>	<i>159</i>
<i>Təbriz Ağaşov, LoRaWAN şəbəkəsində istifadəçi məlumatlarının təhlükəsizliyi problemləri və həlli yolları.....</i>	<i>163</i>
<i>Yadigar İmamverdiyev, Elşən Bağirov, Etik hakinq metodlarının tədrisi haqqında.....</i>	<i>169</i>
<i>Orxan Mənsimzadə, SDN texnologiyasının səviyyələrində təhlükəsizlik məsələləri və həlli yolları.....</i>	<i>172</i>
<i>Nigar Axundova, Fərdlərin sosial münasibətlərinin gizliliyinin təmin olunması problemləri.....</i>	<i>175</i>
<i>Aytən İsmayılqızı, Fərdi məlumatların təhlükəsizliyinin təminatı üçün müasir metodlar.....</i>	<i>177</i>
<i>Tofiq Kazımov, Nəzakət Məlikova, Proqram təminatının sınağı zamanı fərdi məlumatların təhlükəsizliyinin təmin olunması problemləri.....</i>	<i>180</i>

<i>Yadigar İmamverdiyev, Günay Muradova, Fərdi məlumatların mühafizəsi üçün blokçeyn texnologiyaları: imkanları və perspektivləri.....</i>	<i>184</i>
<i>Tamilla Bayramova, Fərdi məlumatların qorunması üçün proqram təminatı alətləri haqqında.....</i>	<i>188</i>
<i>Самира Дадашова, Философский аспект влияния информационных технологий на общественное развитие.....</i>	<i>192</i>
<i>Bikəs Ağayev, Tərlan Əliyev, Kövsər Əliyeva, Məleykə İbişova, Akustik kanallarla ötürülən nitq informasiyasının təhlükəsizliyinin bəzi vibroakustik mühafizə metodları haqqında.....</i>	<i>195</i>
<i>Elşən Bağirov, Klassifikasiya metodlarının zərərli proqramların aşkarlanmasına tətbiqi.....</i>	<i>200</i>
<i>Sakit Verdiyev, Ababil Nağıyeva, Rəxşəndə Hüseynova, Zakir Hüseynov, Steqoanaliz üsullarının icmalı.....</i>	<i>204</i>
<i>Bayram İbrahimov, Tural Məmmədov, Çoxkanallı telekommunikasiya sistemlərində informasiyanın kriptomühafizəsinin bəzi aspektləri.....</i>	<i>207</i>
<i>Roza Şahverdiyeva, Leyla Əkbərova, İnformasiya iqtisadiyyatının formalaşmasında fərdi know-how biliklərin təhlükəsizliyi məsələləri.....</i>	<i>210</i>
<i>Şahanə Mansurova, Big Data analitikası texnologiyaları və fərdi məlumatların təhlükəsizliyi problemləri.....</i>	<i>215</i>
<i>Аловсат Алиев, Роза Шахвердиева, Лейла Акперова, Вопросы формирования правовой информатики в контексте защиты персональных данных.....</i>	<i>219</i>
<i>Aytən Əhmədova, Elektron sağlamlıq kartlarında fərdi məlumatların təhlükəsizliyi problemləri.....</i>	<i>223</i>
<i>Aygül Fəxrəddinqızı, Big Data texnologiyalarında verilənlərin təhlükəsizliyinin əsas məsələləri.....</i>	<i>226</i>
<i>Rəsmiyyə Mahmudova, Fərdi məlumatların qorunması və informasiya təhlükəsizliyi mədəniyyəti.....</i>	<i>229</i>

İnformasiya cəmiyyəti şəraitində Azərbaycan vətəndaşlarının identifikasiyası problemləri və həlli yolları haqqında

Rasim Əliquliyev¹, Yedgar Cəfərov², Əfruz Qurbanova³

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹director@iit.science.az, ²yedgar@yandex.ru, ³afruz1961@gmail.com

Xülasə— Məqalə vətəndaşların adlandırılması sistemi və milli identiklik məsələlərindən bəhs edir. Azərbaycanda vətəndaşların adlandırılması ilə bağlı mövcud problemlər araşdırılmışdır. Qloballaşma dövründə, informasiya cəmiyyəti şəraitində bu problemlərin doğurduğu neqativ hallar nəzərdən keçirilmişdir. Azərbaycan ad və soyadlarının, bununla bağlı tarixi ənənələrin, adlandırma strukturunun ətraflı təhlili aparılmışdır. Bu sahədə xarici təcrübə araşdırılaraq problemlərin həlli istiqamətində təkliflər irəli sürülmüşdür.

Açar sözlər— ad; soyad; ata adı; təxəllüs; ləqəb; adlandırma; ad sistemi; milli identiklik;

I. GİRİŞ

Xalqın yaşam tərzinin tərkib hissəsi olan insan adlarında xalqların həyatı, keçmişi, inancları, arzu və xəyalları, yaradıcılığı, sosial mühiti, əlaqələri və s. əks olunur [1]. Azərbaycanın qlobal informasiya məkanına sürətlə inteqrasiyası bir çox tələpəli məsələlər kimi ad və soyad sistemi və milli identiklik məsələlərinin araşdırılmasını da zəruri edir. Məlum olduğu kimi, qloballaşma prosesi bütün müsbət cəhətləri ilə yanaşı, xalqları öz milli xüsusiyyətlərini tədricən itirmək təhlükəsi ilə üz-üzə qoyur. Belə bir şəraitdə milli identikliyin qorunması, hüduzsuz və xaotik qlobal informasiya məkanında xalqın öz milli mənsəbiyyətini asanlıqla ifadə edə bilməsi üçün təkmil, dayanıqlı və səmərəli mexanizmlər formalaşdırılmalıdır. Ümumiyyətlə, xalqların milli identikliyinə təmin edən əsas əlamətlər bunlardır: xarici görünüş, ad, vətəndaşlıq, dil, inanc, adət-ənənə, mətbəx, musiqi və s. Müasir dünyamızın əsas reallıqlarından birinə çevrilmiş virtual məkanda hər bir azərbaycanlı üçün elə bir ad mühiti yaradılmalıdır ki, bütün dünya azərbaycanlılarının milli identikliyinə təmin etsin, bizi başqa xalqlardan fərqləndirə bilsin.

II. AZƏRBAYCANDA ADLANDIRMA SİSTEMİNİN FORMALAŞMASI TARİXİ

Tarixin ibtidai dövrlərindən başlayaraq sosial-kommunikativ ehtiyac kimi hər bir xalqın özünəməxsus adlandırma ənənələri formalaşmışdır. Qədim türklərin, o cümlədən azərbaycanlıların da adlandırma sistemi spesifik xüsusiyyətlərə malikdir. Qədim türkdilli abidələr, o cümlədən “Orxon-Yenisey” kitabələri, M.Kaşğarinin “Divani-lügət-it-

türk” əsəri, “Kitabi-Dədə Qorqud” dastanları və bir sıra etnoqrafik məlumatlar türk xalqlarında adlandırma ənənələrinin qədimliyini və sistemliliyini göstərir [2]. Azərbaycanın adlandırma sisteminin təşəkkülü və inkişafı cədvəl 1-də verilmişdir.

Qeyd edək ki, müxtəlif xalqlarda nəsil adı ilə adlandırma ənənələri nə qədər qədim olsa da, “fəmiyyə (soyad)” termininin özü eramızın III-IV əsrlərində yaranmışdır. Latın dilində “ailə”, “qohum-əqrəbə”, qulluqçular da daxil olmaqla bütün evdəkilərin cəmini bildirən «soyad» ictimai-tarixi hadisə kimi IV əsrdə İngiltərədə, X-XI əsrlərdə İtaliyada, XV-XVI əsrlərdə Danimarkada, XIV-XVIII əsrlərdə Macarıstanda, XVIII əsrdə Şotlandiya və İrlandiyada yayılmışdır. Soyad 1926-1934-cü illərdə Mustafa Kamal Atatürk tərəfindən Türkiyədə, təxminən eyni tarixdə İranda, 50-ci illərdə Misirdə, 1959-cu ildə Tunisdə rəsmiləşdirilmişdir [3].

Təşəkkül tapdığı ilk çağlardan yüksək sosial status nişanəsi, zadəganlıq göstəricisi sayılması soyadlara marağın artmasına və onların kütləviləşməsinə böyük təsir göstərmişdir. İlk vaxtlar soyadlardan adı insanlar deyil, daha çox zadəganlar istifadə edirdilər. Hətta qədim İngiltərədə yoxsul ailədən olan oğlanın zadəgan ailəsindən olan qızla ailə qurarkən, qızın soyadını götürməsi ənənəsi vardı [2].

Rus ad sisteminə isə soyad 1703-cü ildə I Pyotrun hakimiyyəti zamanında tətbiq olunmuş və əsasən dövlət xadimlərinə, knyaz və mülkədarlara verilmişdi. I Pyotr özü zadəganları fəxri ad kimi soyadlarla mükafatlandırırdı. Rusiyada soyadların formalaşmasında türk mənşəli rus boyarlarının böyük rolu olmuşdur. Ona görə, indi də rus adlandırma sisteminə türk mənşəli soyadlar əhəmiyyətli yer tutur [4].

XIX əsrə doğru Rusiyada cəmiyyətin sosial inkişafının təsiri ilə soyadlardan istifadə meyli tədricən kütləviləşdi. XIX əsrin sonu - XX əsrin əvvəllərində Rusiya imperiyasının tərkib hissəsi olan Azərbaycanda rəsmi sənədləşmə işlərinin rus dilində aparılması və bu zaman vətəndaşların soyadının ənənəvi qaydada, - **oğlu** - **qızı**, - **uşağı** sonluqları ilə deyil, - **ov/-yev**, -**ova/-yeva** sonluqlarından istifadə etməklə rus soyadlarına bənzər onomastik vahidlərlə qeyd edilməsi xalqımız arasında bu cür soyadların süni formada yayılmasına rəvac verdi. Həmin dövrdə Azərbaycanda savadsızlığın kütləvi

xarakter daşınması da **-ov/-yev, -ova/-yeva** sonluqlarının geniş yayılmasına əlverişli şərait yaratdı [5].

CƏDVƏL I. Azərbaycan milli adlandırma sisteminin inkişaf tarixi

III – V əsrlərdən müasir dövrə kimi (Türk adlandırma sistemi)	Ad və -oğlu, -qızı sonluqları Bu sonluqlar insanın valideynlərini bildirir: Məsələn: Ulaş oğlu Salur Qazan; Bəybecan qızı Banıçəkək; Dirsə xan oğlu Buğac
VII-XVII əsrlər (Ərəb adlandırma sistemi)	Ad və nisbə (-i/-vi) Bu sonluq insanın aid olduğu coğrafi məkanı bildirir. Məsələn: Xaqani Şirvani, Nəsirəddin Tusi, Məhsəti Gəncəvi, Qətran Təbrizi Ad və künyə (əbu, ümm) Bu sonluqlardan əbu - atası, ümm anası mənasını verərək insanın valideynlik statusuna işarə edir. Məsələn: Əbu İmran (İmranın atası), Ümm Gülsüm (Gülsümün anası), Əbu Reyhan (Reyhanın atası) Ad və nəşəb (ibn) Oğlu mənasını daşıyan bu sonluq insanın atasının adını bildirir. Məsələn: İbn Sina (Sinanın oğlu), İbn Haldun (Haldunun oğlu)
XIX əsrdən müasir dövrə kimi (Fars adlandırma sistemi)	Ad və -zadə sonluğu Bu sonluq fars dilində “törənmiş” mənası verərək insanın valideynlərini, nəslini bildirir. Məsələn: Əli bəy Hüseynzadə, Əzizə Cəfərzadə.
XX əsrdən müasir dövrə kimi (Rus adlandırma sistemi)	Ad və -ov2-yev2;-ski2; -oviç, -ovna, və s. sonluqları Bu sonluqlardan -ov, -yev mənşə etibarilə “oğlu” mənası verərək, insanın atasının adını bildirir. Məsələn: Yusif Məmmədəliyev, Əşrəf Hüseynov, Nəsimə Zeynalova. Rus soyad sistemində polyaklardan keçmiş -ski sonluğu şəxsin aid olduğu məkanı işarələyir. Məsələn: Hüseyn Ərəblinski, Hüseynqulu Sarabski, Əhməd Ağdamski Rus adlandırma sistemi üçün xarakterik olan -oviç, -ovna kimi sonluqlar soyad bildirməyə də, ata adının göstəricisi kimi, bəzən azərbaycanlı adlarında da istifadə olunur. Mamed Rəhmanoviç və s.
XX əsrin 80-ci illərindən sonlarından müasir dövrə kimi (Müasir soyad sistemi)	Ad və -lı4; -xanlı/-bəyli, sonluqsuz; -ov2-yev2; -zadə; -gil;-soy; -oğlu-qızı; -ski2, -i, -vi sonluqları

Ötən əsrin 30-cu illərində, Stalin irticası zamanı süni familiyalaşdırma meyli xüsusilə geniş vüsət aldı. Yüksək informativ milli identiklik gücünə malik **-oğlu, -qızı** kimi soyad sonluqları təcridən sıradan çıxarılaraq və ata adından sonra yazılaraq yalnız cins mənsubiyyətini ifadə etməklə məhdudlaşdı [6].

Azərbaycanın dövlət müstəqilliyinin bərpasından qısa müddət sonra bu sahədə vəziyyətin nizamlanması məqsədilə Milli Məclisin «Azərbaycan Respublikası vətəndaşlarının soyadlarının dövlət dilinə uyğunlaşdırılması» haqqında 2 fevral 1993-cü il tarixli qərarına əsasən, Azərbaycan vətəndaşlarına soyadlarındakı **-ov/-yev, -ova/-yeva** sonluqlarını «zadə», **-lı4**, «oğlu», «qızı» sonluqları ilə əvəz

etmək və yaxud öz soyadlarını sonluqsuz yazmaq imkanları verilmiş, Nazirlər Kabinetinin 12 may 2011-ci il tarixli qərarı ilə "Adın, ata adının və soyadın verilməsi və dəyişdirilməsi Qaydaları" təsdiqlənmişdir. Bununla belə mövcud reallıq, cəmiyyətimizdə adlar və soyadlar sisteminin hələ tam nizamda düşmədiyini və global şəraitdə xalqımızın milli identikliyi ilə bağlı yeni problemlərin ortaya çıxdığını göstərir [7].

Müstəqillik illərində, xüsusilə dünyaya yeni gələn körpələrin soyadlarında **-ov/-yev, -ova/-yeva** sonluqlarının çəkisi xeyli azalmışdır [8]. Amma bunun bir çox hallarda **“zadə”** və sonluqsuz formalardan istifadə meylinin artması hesabına baş verməsi, eyni zamanda **-ov/-yev, -ova/-yeva** sonluqlarının hələ də qalması bu cür soyadları daşıyan vətəndaşlarımızın global mədəniyyət müstəvisində digər türkdilli xalqlardan və başqa müsəlman ölkələrinin vətəndaşlarından fərqləndirilməsində, identifikasiya olunmasında ciddi çətinliklər yaradır. Nəzərə almaq lazımdır ki, bizim istifadə etdiyimiz adların əksəriyyəti, eləcə də bəzi soyad sistemləri bu xalqlarla müştərəkdir. Sonluqsuz formada yaradılmış soyadlar isə türk və müsəlman dünyasında xeyli işləkdir. Ona görə də bu formalar beynəlxalq aləmdə xalqımızın nümayəndələrinin identifikasiya olunmasında çox ciddi qeyri-müəyyənlik yaradır. Digər tərəfdən, Azərbaycan Respublikası vətəndaşlarına verilən ümumvətəndaşlıq, xidməti, diplomatik pasportlarda, eləcə də beynəlxalq statuslu sürücülük vəsiqələrində, dənizçilik sənədlərində və s. ingiliscə **-oğlu, -qızı** sözlərinin yazılmaması, üstəlik ata adının ingilis dilində göstərilməməsi vəziyyəti xüsusilə çətinləşdirir. Digər tərəfdən global kommunikasiya mühitində, Azərbaycanda və ölkə sərhədlərindən kənarda əcnəbilərin vətəndaşlarımıza konkret ad komponenti ilə müraciətdə çətinlik çəkmələri, tez-tez komponentləri qarışıq salmaları müşahidə edilir. Bundan başqa, beynəlxalq mühitdə şəxsin milli identifikliyini müəyyən edən əsas göstəricilərdən biri olan ata adı itmiş olur. Eyni zamanda, bu anormal hal milli mentalitetimizə görə hər övlad üçün müəyyən mənada mənəvi diskomfortluq da yaradır.

III. MİLLİ ADLANDIRMA SİSTEMİNİN STRUKTURU

Hazırda mövcud qanunvericilik aktlarının tətbiqi nəticəsində ad və soyadların seçilməsi və qeydiyyatı prosesi xeyli təkmilləşdirilsə də, ad və soyadların qeydiyyatı prosesində müəyyən problemlər hələ də qalmaqdadır. Adlandırma sistemi müxtəlif xalqlarda fərqli olur. Azərbaycanda adlandırma sistemi biradlılıqdan çoxadlılığa doğru inkişaf etmişdir [5]. Məsələn, Tural (biradlı), Tural Əli oğlu (iki adlı), Tural Əli oğlu Məmmədli (üçadlı). Kənd, tayfa, icma çevrəsində onlara bir ad kifayət edirdi. İnsanın əlavə identik əlamətlərlə başqalarından fərqləndirilməsinə ehtiyac qalmırdı. Bu mühitdə eyniadlı şəxslər meydana çıxdıqda isə onları bir-birindən fərqləndirmək üçün ayamalardan, ləqəblərdən istifadə edilirdi. Adətən, məşğul olduğu sənətin adını insana qoyur, yaxud onun hansısa fiziki əlamətindən, fərdi keyfiyyətindən ləqəb yaradırdılar (məs: Dəmirçi, Pinəçi,

Uzun, Keçəl, Qara, Sarı, Kürən və s.). Amma fərdlər geniş məkanda, qəsəbə, şəhər çevrəsində sosial əlaqələrə, gündəlik birgə yaşayış, iş, təhsil və s. mühitinə daxil olub onlarla eyni adı daşıyan başqaları ilə qarşılaşdıqca yeni fərqləndirici informativ əlamətlərin yaranması ehtiyacı ortaya çıxdı. Beləliklə ata adı, soyad hesabına ad komponentlərinin sayı artdı.

Azərbaycan Respublikasının müvafiq qanunvericiliyi hazırda vətəndaşın yalnız bir adla, eləcə də ləqəblərlə, təxəllüslərlə qeydiyyatı alınmasına imkan vermir. Belə ki, Azərbaycan Respublikası Mülki Məcəlləsinin 26.1-ci, eləcə də "Adın, ata adının və soyadın verilməsi və dəyişdirilməsi Qaydaları"nın 1.3-cü maddəsinə əsasən, hər bir fiziki şəxsin adı addan, ata adından və soyaddan ibarətdir [9].

Əfsuslar olsun ki, müvafiq normativ-hüquqi aktlarda təsbit edilmiş bu dəqiq ardıcılığa – **ad/ata adı/soyad** rəğmən müxtəlif təşkilatların gündəlik fəaliyyətində aparılan sənədləşmə zamanı həmin ardıcılıq pozulur və bu sahədə milli identiklik modelinin əsası olan dəqiq, stabil milli adlandırma sistemi formalaşdırılmır. Məsələn, Azərbaycan Respublikasının vətəndaşlarına verilən şəxsiyyət vəsiqələrində **soyad/ad/ata adı** ardıcılığından istifadə olunur. Digər rəsmi sənədlərdə də bu komponentlər yerini dəyişir, ad, ata adı, soyad ardıcılığına əməl edilmir, inisial yazılarından istifadə olunur, şəxsin kimliyini müəyyən etmək çox çətinləşir, bəzən heç mümkün olmur. Bir şəxsin adlandırılmasında qeyd olunduğu, Azərbaycan əlifbası və xarici dillərin əlifbalı arasında qeyri-müəyyənlik üçün şərait yaradan çoxvariantlılıq nümunələrinə diqqət yetirək:

Rəhimova Afaq Həsən qızı;

1. Afaq Həsən qızı Rəhimova;
2. Afaq Rəhimova Həsən qızı;
3. A.H.Rəhimova;
4. Rəhimova A.H.;
5. Afaq Rəhimova;
6. Rəhimova Afaq;
7. A.Rəhimova;
8. Rəhimova A.;
9. Afaq H.Rəhimova.

Belə çoxvariantlılıq beynəlxalq kommunikasiya mühitində fərdin milli identikliyi daha da çətinləşdirir. Üstəlik bura xüsusi adların qeyd olunduğu Azərbaycan əlifbası və xarici dillərin əlifbalı arasında transliterasiya ilə bağlı problemləri də əlavə etsək (məsələn, ingilis dilinə transliterasiya zamanı dilimizdəki müvafiq sait və samitlərin (ə — e, a; q — g; x — kh və s.) dəyişdiyini nəzərə alsaq) vəziyyətin necə mürəkkəb şəkil aldığını görürük.

Xalqların ad sistemində heç bir hal, təbii ki, təsadüfən yaranmır və bu cür nizamsızlığın da tarixi-sosial kökləri vardır. Məsələn, doğum evində yenicə dünyaya gəlmiş uşaq

hələ adı olmadığından başqa körpələrlə qarışıq düşməməsi üçün atanın, yaxud ananın soyadı ilə identifikasiya edilir, beləliklə soyad önə keçir. Yaxud təhsil illərində şagirdlərin, yaxud tələbələrin qeydiyyatının aparıldığı davamiyyət jurnallarında adlandırma qeydi üçün müəyyən edilmiş yer məhdud olduğundan, bəzən sadələşdirmə zərurəti ilə soyadlar bütöv, ad və ata adları isə baş hərflərin inisialları ilə yazılır. Amma bütün hallarda nəzərə almaq lazımdır ki, **ad/ata adı/soyad** ardıcılığı tarixi təkamül prosesinin özünün ortaya çıxardığı bir identifikasiya modelidir. Ad sistemimizdə müxtəlif təsirlərlə yaranmış nizamsızlığın aradan qaldırılmasına, ad/ ata adı/ soyad ardıcılığının dəqiq norma kimi qəbul olunmasına və bütün sənədləşmələrdə, elektron resurslarda adların vahid struktur üzrə yazılmasının təmin edilməsi hesabına sabit milli standartların möhkəmləndirilməsinə indi çox böyük ehtiyac vardır.

Hazırda ölkəmizdə formalaşmaqda olan e-dövlət mühitində ayrı-ayrı elektron reyestrlərdə vətəndaşların identifikasiya olunması çox böyük çətinliklərlə üzləşir. Belə ki, vətəndaşa məxsus FİN (fərdi identifikasiya nömrəsi) kodu altında müxtəlif variasiyalarda yazılmış ad/ata adı/ soyadları toplamaq lazım gəlir. Bu isə çox çətin, böyük zəhmət tələb edən prosesdir. Bəzən isə onları bir FİN kod altında identifikasiya etmək, ümumiyyətlə, mümkün olmur. Bu zaman şəxsin digər əlamətlər üzrə axtarılması zərurəti meydana çıxır. Elektron sistemlərdə isə belə dəqiq bir intellektual imkan olmadığından bu, çox vaxt aparır, sorğular göndərilir, digər qurumların resursları cəlb olunur, bəzən də obyektiv və subyektiv səbəblərdən axtarışlar yanlış nəticələr verir. Bundan başqa, şəxslərin ad, ata adı və soyadının yazılışındakı müxtəliflik internet axtarış sistemlərində konkret şəxslərlə bağlı aparılan axtarışların nəticələrində natamamlıq, qeyri-müəyyənlik və s. vardır. Nəzərə alsaq ki, transliterasiya problemi hələ də mövcuddur, onda problem daha qabarıq şəkildə özünü büruzə verir.

IV. MİLLİ ADLANDIRMA SİSTEMİNİN PSİXOLİNGVİSTİK ASPEKTLƏRİ

Yuxarıda qeyd olunanlarla yanaşı, ayrı-ayrı şəxsiyyətlərin həyat və fəaliyyəti, öz ad və soyadlarına qazandırdıqları tarixi mənalarla simvollaşan, eləcə də sosial-mədəni status, şöhrət, nüfuz və s. assosiasiyaları yaradan ad komponentləri vardır. Həmin komponentlərin sırasının pozulması onların ifadə etdiyi assosiativ mənaya da xələl gətirir.

Məsələn, Üzeyir Hacıbəyli, Rəşid Behbudov, Həzi Aslanov, Mirzə İbrahimov ardıcılığının insan təfəkkürünə ötürdüyü psixoloji informasiya Hacıbəyli Üzeyir, Behbudov Rəşid, Aslanov Həzi, İbrahimov Mirzə ardıcılığının doğurduğu təəvvürlə eyni deyildir.

Bir fərd böyüyüb şəxsiyyətə çevrildikcə ona müraciət forması da dəyişir. Uşaq bağçası, məktəb, ali məktəb, hərbi

xidmət və s. dövründə fərdin kimliyi qanunla qeyd olunduğu kimi **ad/ata adı/soyad** ardıcılığı ilə yox, tərsinə, yəni **soyad/ad/ata adı** ardıcılığı ilə qeyd olunur. Əmək fəaliyyətinə başlayaraq ictimaiyyət arasında tanındıqca, yaşa dolduqca ad soyaddan önə keçir.

Ad, ata adı və soyadların vahid milli standartının müəyyənləşdirilməsini zəruri edən digər mühüm bir amil də vardır. Məlum olduğu kimi, hazırda Azərbaycan qanunvericiliyi ölkə vətəndaşlarına şəxs adı və sonluqsuz soyad (Rəsul Rza), yaxud təxəllüs (Səməd Vurğun) və ya oğlu-qızı sonluqları ilə yaradılmış soyadlarla (Emin Sabitoğlu) qeydiyyatı alınmaq imkanı verir. Bu formalardan istifadə çoxaldıqca ikinci komponentin hansı mənə daşdığını, yəni ikikomponentli şəxs adı, həmin şəxsin adının bir hissəsi, ata adı, nəsil adı, yoxsa təxəllüs olduğunu müəyyənləşdirməkdə, son nəticədə isə fərdi eyniləşdirməkdə çətinliklər yarana bilər. Məsələn, görkəmli Azərbaycan şairi Məmməd Arazın həyat və yaradıcılığı ilə tanış olmayan şəxs bu ad və təxəllüsə ilk dəfə rast gələrkən, onun hansı hissəsinin ad, hansı hissəsinin isə təxəllüs olduğunu aydınlaşdırmaqda çətinlik çəkəcək. Ona görə də adlandırma sistemində komponentlərin hər birinin yeri dəqiq göstərməlidir ki, gələcəkdə bu cür çətinliklər ortaya çıxmasın.

V. BEYNƏLXALQ TƏCRÜBƏDƏ ADLANDIRMA SİSTEMİ

Azərbaycanda vətəndaşların bütün sənədlərdə qeydiyyatı prosesinin **ad/ata adı/soyad**, ata adının yazılması zəruri olmadıqda isə **ad/soyad** ardıcılığına əsaslanan dəqiq, vahid standart üzrə həyata keçirilməsi beynəlxalq təcrübəyə də uyğun olardı. Belə ki, bir sıra ölkələrdə ilkin ad (ing. first name), orta ad (ing. middle name) və son ad (ing. last name) komponentlərindən təşkil olunmaqla üçkomponentli adlandırma modellərindən istifadə edilir. Bu adların mahiyyəti mədəniyyətlərdən asılı olaraq dəyişir.

İlkin ad (first name). İlkin ad doğularkən şəxsə verilmiş addır. Azərbaycanın milli adlandırma sistemində olduğu kimi bütün başqa xalqlarda da hər bir şəxsin ilkin adı olur.

Orta ad (middle name). Qərb mədəniyyətinə görə, bəzən uşağa bir deyil, iki ad verilir. Bir sıra hallarda isə hətta üç ad qoyulmasına da rast gəlinir. Adətən, ikinci ad atanın, yaxud babanın, nənənin və ya ananın şərəfinə qoyulur və bu “middle name” kimi işlənir. Middle name şəxsə verilmiş adla yanaşı, soyadın da tərkibində ola bilər. İngiltərədə, Avstriyada, Kanadada, Yeni Zelandiyada, ABŞ-da əcdadların (ata, baba, ana, nənə) şəxs adlarından (ing. forename) onların şərəfinə çox tez-tez middle name kimi istifadə olunur [10].

Danimarkada və Norveçdə isə “middle name” soyad anlamı daşıyır. Middle name kimi ananın qızlıq soyadı, yaxud əcdadlardan hansısa birinin son adı seçilə bilər. Middle name-lərin bir neçə komponentdən ibarət olması mümkündür.

Amma komponentlərinin sayı ikidən çox olan middle name-lərdən istifadə təcrübəsi xarakterik deyildir. Filippində middle name kimi, əsasən, ananın qızlıq фамилияsından istifadə olunur. ABŞ-da middle name-dən tez-tez abbreviatura formasında istifadə edilir. Məsələn, Mary Lee Bianchi – Mary L. Bianchi və s. [11].

Tərkibində middle name-lər olan ad komponentlərindən istifadə təcrübəsi Türkiyədə də geniş yayılmışdır: Ali Qalib İgit, Hüseyn Gürhan Tuncer, Orhan Şaiq Gökyay, Necib Fazil Kısakürek və s.

Azərbaycanda da bu cür adlandırma komponentlərinə, az da olsa, təsadüf edilir: Ceyhun-Təyyar Paşayev, Həməzə Nihad Həmidov, Əli Rza Xələfli və s. Bu cür ad modellərinin ortaya çıxmasında Türkiyə mədəniyyətinin təsiri istisna olunmamalıdır.

Son ad (last name və ya surname). Son ad şəxsin konkret bir ailəyə, nəslə mənsubluğunu bildirən ad komponentidir. Last name ifadəsinin sinonimləri soyad, yaxud ailə adıdır. Bu mənada last name-ləri soyadlar kimi nəzərdən keçirmək olar.

VI. ADLANDIRMA SİSTEMİ İLƏ BAĞLI TEXNİKİ HƏLLƏR

Artıq dünyanın bir çox ölkələrində olduğu kimi, Azərbaycanda da biometrik pasportların və yeni nəsil şəxsiyyət vəsiqələrinin verilməsinə başlanmışdır. Biometrik pasport - Beynəlxalq Mülki Aviasiya Təşkilatının (ing. International Civil Aviation Organization, ICAO) müəyyən etdiyi yüksək texnologiya və təhlükəsizlik elementləri əsasında hazırlanır [10]. Bu pasportlarda adlandırma ilə bağlı texniki-hüquqi standartlar ICAO-nun “Maşın oxuya bilən səfər sənədləri” (Machine Readable Travel Documents) üzrə təlimatı əsasında tənzimlənir [12].

Təlimata uyğun olaraq biometrik pasportun iki zonası var: 1) Vizual yoxlama zonası; 2) Maşının oxuduğu zona. Pasportda titulları, akademik dərəcələri, fəxri adları, mükafatları, irsi statusları və s. bildirən sözləri və şəkilçilərdən, rəqəmlərdən, əsasən, istifadə olunmur. Bu, yalnız müvafiq dövlət idarəsi tərəfindən onların adın ayrılmaz bir hissəsi olduğu rəsmi şəkildə təsdiqləndikdə mümkündür.

Biometrik pasportun maşın oxuyan zonasında da soyad əsas, şəxsin öz adı ikinci dərəcəli ad sayılır, əsas və ikinci dərəcəli adlar bir-birindən “<” işarəsi vasitəsilə ayrılır. Bu zonada adın tərkib hissəsi kimi rəqəmlərdən, apastrof, defis, vergül kimi durğu işarələrindən istifadə olunmur.

Vizual yoxlama zonasında isə dövlətlər məlumatların daha da dəqiqliyi, fərdin identifikasiyası məqsədilə öz milli işarələrindən, yaxud latın əlifbasına daxil olmayan hər hansı başqa işarələrdən istifadə edə bilərlər. Ona görə də bəzi hallarda maşının oxuduğu zonadakı adlar tərtibat baxımından vizual yoxlama zonasındakı adlarla tam üst-üstə düşməyə bilər.

Göründüyü kimi, biometrik pasportların və yeni nəsil şəxsiyyət vəsiqələrinin vizual yoxlama zonasında xalqımızın milli identikliyinə əsas antroponimik əlaməti kimi çıxış edən “oğlu” və “qızı” sözlərinin yazılmasından ötrü də heç bir hüquqi və texniki məhdudiyyət yoxdur. “fon”, “Mc”, “de la” sözləri kimi azərbaycanlılara xas “oğlu”, “qızı” sözlərindən də pasportlarda sonluq kimi istifadə edilə bilər. Bu sonluqlar beynəlxalq səviyyədə çox böyük əhəmiyyət daşıyır. Beynəlxalq aləmdə bəzən şəxsin digər yaxın xalqlarla müqayisədə milli identikliyinə təmin edən yeganə indikator rolunu oynayır.

NƏTİCƏ

Aparılan təhlillər əsasında Azərbaycan Respublikasında adlandırma sisteminin təkmilləşdirilməsi və həm ölkə daxilində, həm də qlobal informasiya məkanında xalqımızın milli identikliyinə təmin olunması məqsədilə aşağıdakı təkliflər irəli sürülür:

Ölkə üzrə bütün sənədləşmə və qeydiyyat işlərinin ardıcılığın saxlanması şərtilə aşağıdakı formatlar üzrə aparılması:

- Komponentlərin hər birinin yazılması zəruri olduğu hallarda **ad/ata adı/soyad** formatı;
- Ata adının yazılmasının zəruri olmadığı hallarda **ad/soyad** formatı;
- Ata adı inisialının göstərilməsinin zəruri olduğu hallarda: **ad/ata adının ilk hərfi/soyad** formatı;
- Beynəlxalq aləmdə fərdin milli identikliyinə təmin olunması məqsədilə Azərbaycan Respublikası vətəndaşlarına verilən biometrik pasportlarda və yeni nəsil şəxsiyyət vəsiqələrində həm Azərbaycan, həm də ingilis dilində addan sonra ata adının daxil edilməsi və mütləq “oğlu” və “qızı” sözlərinin əlavə olunması;
- Milli transliterasiya standartlarının qəbul olunması, biometrik pasportlarda və yeni nəsil şəxsiyyət vəsiqələrində müvafiq qaydada istifadə məqsədilə adlandırma sisteminə transliterasiya standartlarının (cədvəllərinin) (az-en, en-az) əlavə olunması;
- Milli adlandırma standartları ilə bağlı texniki məsələlərin optimal həlli üçün Beynəlxalq Mülki Aviasiya Təşkilatı ilə müzakirələrin təşkili.

Bu gün yeni inkişaf mərhələsində tarixi nailiyyətlər qazanan, qlobal proseslərin fəal subyektinə çevrilən Azərbaycan dövlətinin adlar vasitəsilə xalqın milli identikliyinə ifadəsi məsələsini yenidən nəzərdən keçirməsi, Azərbaycançılıq ideologiyası çərçivəsində, tarix və müasirlik

işığında bu problemin optimal həlli yollarının tapılması xalqımızın gələcəyinə, informasiya cəmiyyətinin inkişafına, milli şüurun, özünüdərk hissinin daha da yüksəlişinə töhfə olardı.

İSTİNADLAR

- [1] Л.Э.Аблитарова, “Формирование имен и фамилий у различных народов, проживающих на территории Крыма”, Современная филология: материалы IV Междунар. науч. конф., г. Уфа, 2015, с. 19-21.
- [2] Н.Ə.Нəсəнов, “Fəmiлиya sosial-ictimai hadisə kimi”, Azərbaycan onomastikası problemlərinə həsr olunmuş III elmi-nəzəri konfransın materialları, Bakı, APU, 1990, s. 9–11
- [3] A.Paşa, “Azərbaycan antroponimiyasının leksik problemləri”, Bakı, “Maarif”, 1997, 253 s.
- [4] Н.А.Баскаков, “Русские фамилии тюркского происхождения”, Баку, “Язычы”, 1992, 280 с.
- [5] M.N.Çəbanov, “Azərbaycan antroponimiyasının əsasları”, Bakı, “Maarif”, 1998, 332 s.
- [6] Fəracov N.R. Fəmiлиyalarımızın tələyinə dair mülahizələr/Azərbaycan dilinin etimologiya və onomastikası məsələləri. Bakı, BDU nəşriyyatı, 1990, s. 96-100
- [7] Y.Cəfərov, “Azərbaycan dilinin onomastikası müstəqillik dövründə”, Bakı, “Elm və təhsil” nəşriyyatı, 2015, 367 s.
- [8] “Adlar və Soyadlar” Dövlət İnformasiya Sisteminin yaradılması Konsepsiyası. AMEA İnformasiya Texnologiyaları İnstitutu, Ekspres-Informasiya, Bakı, 2010, 49 s.
- [9] Azərbaycan Respublikası Nazirlər Kabinetinin Qərarı, Bakı şəhəri, 12 may 2011-ci il, //www.e-qanun.az/framework/21676.
- [10] The Use of Middle Names, www.genfiles.com/articles/middle-names/
- [11] az.wikipedia.org. “Pasport”.
- [12] Machine Readable Travel Documents, Seventh Edition, 2015, Part 3: Specifications Common to all MRTDs, ICAO, 86 p.

ABOUT ISSUES OF IDENTIFICATION OF THE CITIZENS OF AZERBAIJAN IN INFORMATION SOCIETY AND WAYS OF THEIR SOLUTION

Rasim Alguliyev¹, Yedgar Jafarov², Afruz Gurbanova³

Institute of Information Technology of ANAS, Baku, Azerbaijan

¹director@iit.science.az, ²yedgar@yandex.ru,
³afruz1961@gmail.com

Abstract – The article is devoted to the issues of the naming system and national identity. Attention is paid to the current name problems in Azerbaijan. The article considers negative cases caused by these problems in the era of globalization and the information society environment. A wide scientific analysis of Azerbaijani names and surnames, historical traditions in this field, names structure and so on is carried out. Specific proposals are given in order to solve these problems.

Key words – name, surname, patronymic, nickname, naming system, national identity

Böyük həcmli fərdi məlumatların analizi üçün iterativ çəkili k-means alqoritm

Ramiz Aliquliyev¹, Şəlalə Tahirzadə²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹ r.aliguliyev@gmail.com, ² fmv.shalala@gmail.com

Xülasə—İnformasiya Kommunikasiya Texnologiyalarının (İKT) inkişafı rəqəmsal informasiyanın sıçrayışlı artımına və nəticədə, “big data” konsepsiyasının populyarlaşmasına səbəb olmuşdur. Bu səbəbdən big data və onun mahiyyətini, müxtəlif mənbələrini, analiz texnologiyalarının imkanlarını, problemlərini, təhlükəsizlik məsələlərini hərtərəfli tədqiq etməyə ehtiyac yaranmışdır. Məqalədə mövcud analiz texnologiyalarının çatışmazlıqlarına, fərdi məlumatların analizindəki təhlükəsizlik məsələlərinə baxılır və həlləri araşdırılır. Böyük məlumatların analizindəki çatışmazlıqları aradan qaldırmaq üçün iterativ və çəkili iterativ k-means alqoritmləri təklif edilir.

Açar sözlər—big data, fərdi məlumatlar, fərdi məlumatların təhlükəsizliyi, klasterləşdirmə, iterativ və çəkili klasterləşdirmə.

I. GİRİŞ

İKT sahəsindəki yüksək inkişaf meyilləri yeni texnoloji həllərin geniş şəkildə istifadəsinə, cəmiyyətin kompüterləşməsinə və s. gətirib çıxarmışdır. Verilənlərin toplanması və saxlanması vasitələrinin də sürətli inkişafı ilə hazırda gündəlik olaraq böyük həcmli verilənlər toplanılır və kompüter şəbəkələrinə, internetə, müxtəlif verilənlər saxlanmasına axın edir. Bu isə böyük həcmli verilənlər anlayışının yaranmasına səbəb olmuşdur. Böyük həcmli verilənlərin analizi vasitəsilə faydalı məlumatlar – bilik əldə etmək mümkündür.

Böyük həcmli verilənlər müxtəlif məzmunlu mənbələrdən toplanıla bilər. Tibbi, hərbi, mühəndislik, məişət, müxtəlif elm sahələri və s. buna misal ola bilər. Belə müxtəlif məzmunlu verilənlərin təhlükəsizliyinə qoyulan tələblər də müxtəlifdir. Məlumdur ki, analiz texnologiyalarının tətbiqi nəticəsində böyük verilənlərdən əlavə bilik və qiymətli məlumatlar əldə etmək mümkündür. Bu da öz növbəsində verilənlərin məzmunundan asılı olaraq təhlükəsizlik baxımından müxtəlif problemlərə gətirib çıxara bilər. Misal olaraq qeyd etmək olar ki, hərbi və ya fərdi məlumatların təhlükəsizliyi ilə məişət verilənlərinin təhlükəsizlik tələbləri eyni deyildir. Belə ki, hərbi və ya fərdi məlumatların analizi vasitəsilə dövlət əhəmiyyətli biliklər əldə etmək mümkündür.

Aydın ki, verilənlərin həcmnin sürətli artımı mövcud analiz texnologiyalarının imkanlarını məhdudlaşdırır. Bu məqsədlə məqalədə Big data texnologiyalarında fərdi məlumatların təhlükəsizlik məsələləri araşdırılır. Mövcud analiz texnologiyalarının imkanları, çətinlikləri nəzərdən keçirilir. Təklif edilən iterativ və iterativ çəkili k-means alqoritmlərinin tətbiqi ilə eksperiment həyata keçirilir. Eksperimentin nəticələrinə əsasən k-means alqoritm

ilə edilən alqoritmlər müqayisə edilir, müxtəlif qiymətləndirmə indeksləri vasitəsilə nəticələr qiymətləndirilir.

II. “BIG DATA” KONSEPSİYASI

Böyük verilənlər həcmnin hazırkı eksponensial artım sürəti də məhz informasiyaya əlverişliliyin asanlaşması və kommunikasiya vasitələrinin çoxalması ilə sıx əlaqədardır [8]. Böyük verilənlər dedikdə, çox böyük həcmə malik, sürətli və emal üçün çox mürəkkəb verilənlər başa düşülür.

Böyük verilənlərin “3V” adlandırılan xarakteristikası olan həcm (*ing. volume*) – verilənlərin həcmi; müxtəliflik (*ing. variety*) – verilənlərin müxtəlifliyi və bir çox hallarda kifayət qədər strukturlaşdırılmamış; sürət (*ing. velocity*) – verilənlərin böyük sürətlə emal edilməsi olaraq qeyd edilir:

“Google Trends”-in hesablamalarına google axtarış mühərriki vasitəsilə saniyədə 40000, günlük 3.46 milyon, illik olaraq isə 1.2 trilyon axtarış həyata keçirilir [16]. Dünyada ikinci ən çox ziyarət edilən və nəhəng şirkətlərdən olan “Youtube”-a dəqiqədə 500 saat həcmində videolar yüklənir [17]. Bütün bunlar verilənlərin həcmnin fasiləsiz olaraq sürətli artımına gətirib çıxarır. Belə böyük həcmli verilənlərin isə analizinə ehtiyac yaranır. Müxtəlif emal texnologiyaları vasitəsilə isə onları analiz etmək, qiymətli biliklərə çevirmək mümkündür. Böyük verilənlər konsepsiyasının geniş yayılması özü ilə birgə təhlükəsizlik problemlərini də gətirir [1]. Bu isə informasiya mühafizəsi məsələlərinin aktuallığının artmasına gətirib çıxarır. İnformasiyanın mühafizəsi informasiya təhlükəsizliyinin təmin olunmasına yönəlmiş tədbirlər kompleksidir.

III. İNFORMASIYA TƏHLÜKƏSİZLİYİ

Məlumdur ki, İKT sahəsinin nəzərə cərpacaq səviyyədə inkişafı elmi-texniki inqilaba səbəb olmuşdur. Bu da cəmiyyətə təsirli qalmamışdır. Nəticədə, elmi ədəbiyyatlarda informasiya cəmiyyəti anlayışından istifadə edilməyə başlanmışdır. İnformasiyanın toplanması, saxlanması, emalı, istifadəsi və ötürülməsi ilə bağlı fəaliyyət sahələri bu cəmiyyətdə aparıcı mövqeyə yüksəlməklə iqtisadiyyatın əsasını təşkil edir. İnformasiya və biliklər isə informasiya cəmiyyətinin ən mühüm resursu və başlıca elementidir [2].

İnformasiya təhlükəsizliyinin təmin olunması probleminin aktuallığını və vacibliyini şərtləndirən səbəblərdən aşağıdakıları qeyd etmək olar:

- şəbəkə texnologiyalarının geniş yayılması və lokal şəbəkələrin qlobal şəbəkələr halında birləşməsi;

- informasiya təhlükəsizliyinin pozulmasına praktik olaraq mane olmayan qlobal İnternet şəbəkəsinin inkişafı;
- minimal təhlükəsizlik tələblərinə belə cavab verməyən proqram vasitələrinin geniş yayılması.

A. Fərdi məlumatların təhlükəsizliyi

İnformasiya cəmiyyətinin hər bir üzvü olan fərd bu məlumatların həm istehsalçısı, həm də istehlakçısı hesab edilir. Məzmun baxımından informasiya müxtəliflik təşkil edir. Fərdi məlumatlar dedikdə şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənlədirməyə imkan verən istənilən məlumat başa düşülür. Fərdi məlumatlar toplandığı andan mühafizə olunur və hər bir fərd ilkin mənada öz məlumatlarının qoruyucusuna çevrilir. Bu tip məlumatlar daxilolma növünə görə konfidensial və açıq kateqoriyalara bölünür [3]. Açıq məlumatların analizi belə konfidensial informasiyaların əldə olunmasına səbəb ola bilər. Bu səbəbdən böyük məlumatların məxfiliyi əvvəllər fərdi mənada müzakirə edilərsə də, tədricən “milli təhlükəsizlik” istiqamətində inkişaf etmiş, nəticədə, siyasi və milli xarakter qazanmışdır. Bu baxımdan informasiya və İKT hər bir ölkənin milli təhlükəsizliyinin təmin olunması üçün mühüm vasitədir. İnformasiya təhlükəsizliyinin təmin edilməsi isə prioritet məsələlərdən biridir. Bunun nəticəsidir ki, hazırda fərdi məlumatların toplanması, emalı, ötürülməsi, mühafizəsi və s. qanunvericilikdə müəyyən edilmiş hüquqi normalar əsasında həyata keçirilir.

IV. BÖYÜK VERİLƏNLƏRİN ANALİZİ TEKNOLOGİYALARI

Böyük verilənlərin analizi nəticəsində daha sürətli və daha optimal qərarlar qəbul etmək, çəkilən xərcləri minimallaşdırmaq, sərf edilən zamana qənaət etmək və yeni növ xidmətlər təklif etmək mümkündür. Verilənlərin analizi üçün müxtəlif vasitə və üsullardan istifadə etmək mümkündür. Bu məqsədlə ən geniş tətbiq edilən üsul klasterləşdirmə alqoritmləridir. Klasterləşdirmə alqoritmlərinə misal olaraq K-means, K-medoids, DBSCAN, E-M və s. qeyd etmək olar. Verilənlərin analizi üçün ən çox tətbiq edilən klasterləşdirmə alqoritmimi kimi K-means və onun müxtəlif modifikasiya olunmuş versiyalarını qeyd etmək olar. K-means alqoritmimin ən böyük çatışmazlığı onun başlanğıc klaster mərkəzlərinin seçilməsindən asılı olmasıdır. Belə ki, ilkin mərkəzin seçilməsindən asılı olaraq nəticələrin keyfiyyəti də müxtəlif ola bilər [5]. Klasterlərin keyfiyyətinin ilkin mərkəzin seçilməsindən asılılığı, böyük həcmli verilənlərin analizində çətinliklər, emal prosesində texniki təminata qoyulan yüksək tələblər kimi bir sıra məsələləri aradan qaldırmaq məqsədi ilə k-means alqoritmimin müxtəlif modifikasiya edilmiş versiyalarına nəzər yetirilir. K-means alqoritmimin çatışmazlıqlarını aradan qaldırmaq üçün onun modifikasiyası olan iterativ və çəkili iterativ k-means alqoritmimi təklif edilir. Emal prosesində texniki təminata qoyulan tələbləri nəzərə alaraq verilənlərin paketlərə bölünməklə emal edilməsi təklif edilir [4,6,7]. Qeyd edilən alqoritmlərin nəticələri eksperiment aparılmaqla k-means alqoritmimi ilə müqayisə edilmişdir. Təklif edilən alqoritmlərin əsas addımları aşağıdakı kimi verilmişdir.

A. İterativ k-means alqoritmimi

İterativ k-means alqoritmimin addımları aşağıdakı kimidir:

- $P = \{p_1, \dots, p_n\}$ verilənlər çoxluğu $B = \{b_1, \dots, b_m\}$ paketlərinə bölünür;
- b_1 paketinə k-means alqoritmimi tətbiq edilir;
 - Mərkəzlər növbəti paketə əlavə edilmək üçün seçilir;
 - Yeni paketə k-means alqoritmimi tətbiq edilir. Əvvəlki mərhələdə tapılmış klaster mərkəzləri bu mərhələ üçün başlanğıc klaster mərkəzləri kimi qəbul edilir;
 - b_m^* paketinə k-means alqoritmimi tətbiq edildikdən sonra iterasiya dayandırılır;
 - Yekunda alınan mərkəzlər P verilənlər çoxluğunun klaster mərkəzləri kimi qəbul edilir;
- P verilənlər çoxluğunun hər bir obyektini ilə sonuncu klaster mərkəzləri arasındakı Evklid məsafəsi hesablanır;
- P çoxluğunun obyektləri məsafəcə yaxın olduğu mərkəzə uyğun klasterlərə aid edilir.

B. Çəkili iterativ k-means alqoritmimi

Çəkili İterativ k-means alqoritmimin addımları aşağıdakı kimidir:

- $P = \{p_1, \dots, p_n\}$ verilənlər çoxluğu $B = \{b_1, \dots, b_m\}$ paketlərinə bölünür;
- b_1 paketinə k-means alqoritmimi tətbiq edilir;
 - Tapılmış klasterlərin mərkəzləri üçün (1) düsturunun köməyiylə çəkilər hesablanır;
 - Çəkili mərkəzlər növbəti paketə əlavə edilir və alınmış nöqtələr çoxluğu üçün çəkili k-means alqoritmimi tətbiq edilir.
 - Yeni paketə çəkili k-means alqoritmimi tətbiq edilir. Bu mərhələdə klasterlərin başlanğıc mərkəzləri kimi əvvəlki mərhələdə hesablanmış çəkili klaster mərkəzləri qəbul edilir;
 - Bu proses bütün paketlər üçün iterativ olaraq təkrarlanır. Və sonuncu mərhələdə b_m^* paketinə çəkili k-means tətbiq edildikdən sonra iterasiya dayandırılır;
- Sonuncu mərhələdə tapılmış mərkəzlər P verilənlər çoxluğunun klaster mərkəzləri kimi qəbul edilir;
- P verilənlər çoxluğunun hər bir obyektini ilə sonuncu mərhələdə tapılmış klaster mərkəzləri arasındakı Evklid məsafəsi hesablanır;
- P çoxluğunun obyektləri məsafəcə yaxın olduğu mərkəzə uyğun klasterlərə aid edilir.

Burada klasterlərin mərkəzlərinin çəkisi aşağıdakı düsturun köməyiylə hesablanır:

$$\omega_{ij} = 1 + \frac{|C_{ij}|}{|b_i|}, \quad i = 1, \dots, m; \quad j = 1, \dots, k \quad (1)$$

$|b_i|$ – b_i paketinin ölçüsü (paketdəki obyektlərin sayı); $|C_{ij}|$ – b_i paketinin klasterləşməsindən sonra alınan C_{ij} klasterinin ölçüsü (C_{ij} klasterindəki obyektlərin sayı); ω_{ij} – C_{ij} klaster mərkəzinin çəkisidir.

V. TƏKLİF EDİLƏN ALQORİTMLƏRİN EKSPERİMENTİ VƏ MÜQAYİSƏLİ ANALİZİ

Təklif edilən alqoritmləri qiymətləndirmək üçün Intel core (i7), 2.20 GHz, 8 Gb RAM xarakteristikalarına malik kompüterdə R proqramlaşdırma dilindən (R-3.5.3) istifadə edilmişdir. Eksperiment üçün bir neçə müxtəlif ölçülü verilənlər üzərində ənənəvi k-means metodu və təklif edilən alqoritmlər tətbiq edilmişdir. Eksperimentin nəticələrinin müqayisəli analizini reallaşdırmaq məqsədilə bir neçə qiymətləndirmə indeksləri seçilmişdir. İstifadə edilmiş verilənlərin təsviri və seçilmiş qiymətləndirmə indeksləri haqqında məlumat aşağıda qeyd edilmişdir.

A. Verilənlər

Eksperimentlər “Poker-hand-testing and Training”, “Localization Data for Person Activity”, “UScensus data 1990” verilənləri üzərində tətbiq edilmişdir və onların xarakteristikası cədvəl 1-də verilmişdir.

CƏDVƏL 1. VERİLƏNLƏR ÇOXLUĞUNUN XARAKTERİSTİKASI

Verilənlər çoxluğu	Obyektlərin sayı	Atributların sayı	Siniflərin sayı
Poker-hand-testing and Training	1025010	11	10
Localization Data for Person Activity	164860	4	11
UScensus data 1990	2458285	68	–

“Poker hand testing and Training” verilənlərindəki hər bir nümunə 52-lik standart dəstədən çəkilmiş 5 oyun kartını ifadə edir [9, 10, 11]. Hər bir kart “suit” və “rank” adlandırılan 2 atributla xarakterizə edilir. 11-ci atribut isə sinifləri əks etdirir.

İstifadə edilmiş “Localization Data for Person Activity” verilənləri müxtəlif hərəkətlər icra edən 5 fərdin məlumatlarından əldə edilmişdir [11,12]. Onların hər birinə eyni ssenarini 5 dəfə yerinə yetirən, sağ və sol ayaq biləyi, bel və sinə nəhiyələrinə bərkidilmiş 4 sensor birləşdirilmişdir. Bu sensorlar vasitəsilə 4 atributa malik nümunə toplanmışdır ki, onlardan 4-cüsü sinifləri əks etdirir.

“US census 1990 data” 1990-cı ildə siyahıya alma zamanı əldə edilmiş məlumatlardan toplanmışdır [11,13].

Eksperimentin nəticələrinin qiymətləndirilməsi üçün (2) düsturu ilə hesablanan funksiyanın qiyməti, Purity indeksi (3), Davies-Bouldin indeksi (4) istifadə edilmişdir.

$$F = \sum_{j=1}^k \sum_{i=1}^n \|x_i^{(j)} - O_j\|^2 \rightarrow \min \quad (2)$$

burada O_j – C_j klasterinin mərkəzi, $x_i^{(j)}$ – C_j klasterinə aid edilən i -ci obyektidir.

B. Qiymətləndirmə indeksləri

Purity indeksinin hesablanması üçün aşağıda göstərilmiş (3) düsturundan istifadə edilir:

$$Purity = \frac{1}{n} \sum_{i=1}^k \max_j |C_i \cap A_j|, \quad (3)$$

burada n – obyektlərin sayı, k – klasterlərin sayı, C_i – i -ci klaster, A_j – j -ci sinifdir. Purity indeksinin qiyməti nə qədər böyük olarsa, alqoritm bir o qədər effektiv hesab edilir [14].

Klasterləşdirmə alqoritmlərinin qiymətləndirilməsi üçün istifadə edilən digər metrika isə Davies-Bouldin (DB) indeksidir [15]. DB indeksinin hesablanması üçün aşağıda göstərilmiş (4) və (5) düsturlarından istifadə edilir:

$$DB = \frac{1}{k} \sum_{i=1}^k R_i \quad (4)$$

$$R_i = \max_{j=1, \dots, k, j \neq i} R_{ij} \quad \text{və} \quad R_{ij} = \frac{\text{var}(C_i) + \text{var}(C_j)}{\|O_i - O_j\|}, \quad (5)$$

burada C_i – i -ci klaster, O_i – C_i klasterinin mərkəzidir. DB indeksi 0 və 1 aralığında qiymətlər alır. Bu indeksin aşağı qiymətləri klasterləşdirmə üçün daha yaxşı hesab edilir.

Cədvəl 2-də təklif edilən iterativ və iterativ çəkili k-means alqoritmlərinin yekun nəticələri k-means alqoritmı ilə müqayisə edilir. Burada əsas məqsəd (2) düsturu ilə hesablanan funksiyanın qiymətini minimallaşdırmaq və nəticələrin dəqiqliyini artırmaqdır.

CƏDVƏL 2. K-MEANS, IK-MEANS, IWK-MEANS ALQORİTMLƏRİNİN
EKSPERİMENTAL NƏTİCƏLƏRİ

Localization Data for Person Activity				
Metod	DB	Purity	Funksiyanın qiyməti	Vaxt (san.)
k-means	1.0451	0.4560	31,588.52	1.36
ik-means	1.1673	0.4609	35,292.28	3.73
iwk-means	1.1399	0.4410	32,721.03	4.07
Poker-hand-testing and Training				
Metod	DB	Purity	Funksiyanın qiyməti	Vaxt (san.)
k-means	1.4441	0.4758	40,653,041	23.49
ik-means	1.4238	0.5012	38,676,726	32.21
iwk-means	1.4497	0.5001	38,694,990	32.66
UScensus data 1990				
Metod	DB	Funksiyanın qiyməti	Vaxt (san.)	
k-means	0.5774	615,910,906	69.29	
ik-means	0.5774	532,548,026	22.56	
iwk-means	0.5774	529,369,871	24.84	

Burada əsas məqsəd təklif edilmiş alqoritmlər vasitəsilə daha keyfiyyətli klasterləşdirməni həyata keçirməkdir. Qeyd etmək lazımdır ki, qiymətləndirilmə üçün istifadə edilmiş DB indeksinin, (2) funksiyanın və zamanın minimal qiymətləri,

Purity indeksinin isə maksimal qiyməti daha keyfiyyətli nəticəni ifadə edir. Təklif edilən alqoritmlər üçün ən yaxşı nəticə “US census 1990 data” verilənlərinin nəticələridir. Bu verilənlərinin nəticələrinə görə DB indeksi hər üç alqoritm üçün eyni qiymət olsa da, funksiyanın qiyməti və zaman göstəricilərinə əsasən IK-means və IWK-means alqoritmləri K-means alqoritmindən üstündür.

İterativ və çəkili k-means alqoritmləri vasitəsilə klasterlərin keyfiyyətinin ilkin mərkəzin seçilməsindən asılılığını aradan qaldırmaq mümkündür. Belə ki, k-means alqoritmindən fərqli olaraq təklif edilən alqoritmlərin əsas üstünlüyü odur ki, iterativ prosesdə bir öncəki klasterləşmədən əldə edilmiş mərkəzlər növbəti addım üçün başlanğıc mərkəz kimi seçilir. Təklif edilən alqoritmlərin digər üstünlüyü verilənlərin paketlərə bölünməklə analiz edilməsidir ki, bununla emal prosesində texniki təminatla qoyulan yüksək tələbləri minimallaşdırmaq olar. Beləliklə, eksperimentin nəticələrini əks etdirən cədvəl 2-dən də göründüyü kimi verilənlərin ölçüsünün böyük qiymətlərində təklif edilən alqoritmlərin effektivliyi artır.

NƏTİCƏ

Məqalədə böyük verilənlər konsepsiyasının geniş yayılması nəticəsində özü ilə birgə gətirdiyi problemlər, emal texnologiyalarındakı çətinliklər, təhlükəsizlik məsələləri araşdırılmış və risklər təhlil edilmişdir. Eyni zamanda analiz texnologiyalarının tətbiqi ilə böyük verilənlərin təhlükəsizlik məsələlərinə baxılmışdır. Qeyd edilən məsələlərin həllinə nail olmaq üçün iterativ və çəkili iterativ k-means alqoritmləri təklif edilmişdir. Təklif edilən alqoritmlərin əsas məqsədi k-means klasterləşdirmə alqoritmindən ilkin mərkəzdən asılılığını aradan qaldırmaqla nəticələrin etibarlılığını və dəqiqliyini artırmaqdır.

Təklif olunan alqoritmlərin tətbiqi ilə müxtəlif verilənlər üzərində eksperimentlər həyata keçirilmişdir. Eksperimentin nəticələri bəzi qiymətləndirmə indekslərinə əsasən müqayisə edilmişdir. Araşdırmalar onu göstərdi ki, bu alqoritmlərin əsas üstünlüyü ənənəvi metodlarla müqayisədə daha sürətli olmasıdır. Eksperimentin nəticələrinə əsasən qeyd etmək olar ki, təklif edilən alqoritmlər çox böyük həcmli verilənlərin analizi üçün daha effektivdir. Beləliklə, verilənlərin analizi zamanı təhlükəsizlik baxımından həssaslığı nəzərə alınmaqla mürəkkəb məsələlərin həlli üçün təklif edilən alqoritmlər tətbiq edilə bilər.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikası Dövlət Neft Şirkətinin (SOCAR) Elm Fondunun maliyyə yardımı ilə yerinə yetirilmişdir – **Müqavilə № 03LR – AMEA.**

İSTİNADLAR

- [1] R.M. Alguliyev, Y.N. Imamverdiyev, “Big data: big promises for information security”, Proc. 2014 IEEE 8th International Conference on Application of Information and Communication Technologies, pp.1-4, 2014.
- [2] R.M. Əliquliyev, M.Ş. Hacırohimova, A.Ş. Əliyeva, “Big Data-nın aktual elmi-nəzəri problemləri”, İnformasiya cəmiyyəti problemləri, №2, s.37-49, 2016.

- [3] R.M. Alguliyev, R.M. Aliguliyev, F.J. Abdullayeva, “Privacy-preserving deep learning algorithm for big personal data analysis”, Journal of Industrial Information Integration, vol.15, pp.1-14, 2019.
- [4] R. Alguliyev, R. Aliguliyev, A. Bagirov, R. Karimov, “Batch clustering algorithm for big data sets”, Proc. 2016 IEEE 10th International Conference on Application of Information and Communication Technologies, pp.79-82, 2016.
- [5] R.M. Alguliyev, R.M. Aliguliyev, L.V. Sukhostat, “Weighted consensus approach for big data clustering”, Proceedings of the 13th IEEE International Conference Application of Information and Communication Technologies, pp.143-146, 2019.
- [6] N. Karmitsa, A.M. Bagirov, S. Taheri, “Clustering in large data sets with the limited memory bundle method”, Pattern Recognition, vol.83, pp.245-259, 2018.
- [7] N. Karmitsa, A.M. Bagirov, S. Taheri, “New diagonal bundle method for clustering problems in large data sets”, European Journal of Operational Research, vol.263, no.2, pp.367-379, 2017.
- [8] D. Zhang, “Big data security and privacy protection”, “Advances in Computer Science Research”, vol.77, pp.275-278, 2018.
- [9] R.A.Rossi, N.K.Ahmed, “The Network Data Repository with Interactive Graph Analytics and Visualization”, AAAI, 2015.
- [10] R. Cattral, F. Oppacher, D. Deugo, “Evolutionary Data Mining with Automatic Rule Generalization”, Recent Advances in Computers, Computing and Communications, WSEAS Press, pp.296-300, 2002.
- [11] D. Dheeru, G. Casey, “{UCI} Machine Learning Repository”, University of California, Irvine, School of Information and Computer Sciences.
- [12] B. Kaluza, V. Mirchevska, E. Dovgan, M. Lustrek, M. Gams, An Agent-based Approach to Care in Independent Living, International Joint Conference on Ambient Intelligence (AmI-10), Malaga, Spain
- [13] C. Meek, B. Thiesson, D. Heckerman, “The Learning-Curve Sampling Method Applied to Model-Based Clustering”, Journal of Machine Learning Research, vol.2, no.2, pp.397-418, 2002
- [14] A.M. Rubinov, N.V. Soukhorukova, and J. Ugon, Classes and clusters in data analysis, Euro. J. Operational Research, vol. 173, pp. 849–865, 2006
- [15] D.L.Davies, and D. W. Bouldin. “A Cluster Separation Measure”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. PAMI-1, no. 2, pp. 224–227, 1979.
- [16] Google Trends, <https://trends.google.com/trends/?geo=US>
- [17] Statista, Statistics&Fact, <https://www.statista.com/topics/2019/youtube/>

AN ITERATIVE WEIGHTED K-MEANS ALGORITHM FOR BIG PERSONAL DATA ANALYSIS

Ramiz M. Aliguliyev¹, Shalala F.Tahirzade²

^{1,2}Institute of Information Technology of Azerbaijan National Academy of Sciences

¹r.aliguliyev@gmail.com, ²fmv.shalala@gmail.com

Abstract -- The development of information and communication technologies (ICT) has led to a significant increase in digital information and consequently led to the spread of the concept of “big data”. Therefore, there is a need for a comprehensive study of big data and its essence, various sources, capabilities of analytics technologies, problems, and security issues. The article addresses the weaknesses of existing analytical technologies, security issues in the analysis of personal data, and examines their solutions. Iterative and iterative weighted k-means algorithms are proposed to eliminate insufficiency in big data analysis.

Keywords -- big data, personal data, personal data security, clustering, iterative and weighted clustering.

Tibbi sosial media istifadəçilərinin fərdi məlumatlarının təhlükəsizliyi məsələləri

Məsumə Məmmədova¹, Zərifə Cəbrayılova²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹mmg51@mail.ru, ²depart15@iit.science.az

Xülasə— E-tibbin formalaşması tibbi sosial media mühitini kütlə rəyini nəzərə almaqla tibbi xidmətin keyfiyyətinin yaxşılaşdırılması, tibbi qərarların qəbulu prosesinin təkmilləşdirilməsi, bir sıra sosioloji sorğuların keçirilməsi və s. üçün əhəmiyyətli informasiya mənbəyinə çevirmişdir. Elektron pasiyentlər onları maraqlandıran problemlərin həlli üçün sosial mediaya müraciət edir, peşəkar saytlarda qeydiyyatdan keçirərək kontentlərdən yararlanmağa çalışırlar. Qeydiyyatdan keçən istifadəçilər bəzən özləri haqqında açıq verilənlər ilə yanaşı şəxsi identiklik verilənlərini də qeyd etməli olurlar. Bu isə fərdi məlumatların konfidensiallıq siyasətinin zəif olduğu sosial media mühitində istifadəçilərin fərdi məlumatlarının təhlükəsizliyi üçün ciddi problemlər yaradır. Baxılan məqalədə tibbi sosial şəbəkələrdə istifadəçilərin konfidensiallıq riskləri analiz olunmuş və konfidensiallıq siyasəti ilə bağlı bir sıra təkliflər göstərilmişdir.

Açar sözlər— tibbi sosial media; e-pasiyentlər; şəxsiyyətin identiklik verilənləri; konfidensiallıq riskləri; konfidensiallıq siyasəti

I. GİRİŞ

E-tibbin formalaşmasını əks etdirən əsas məqamlardan biri həkim və pasiyentlərin ünsiyyət qurmaq, informasiya əldə etmək üçün virtual mühitə müraciət etməsi, tibbi sosial medianın yaranmasıdır. Hazırda tibbi seqmentdə əlyətərli olan çoxlu sayda sosial media vasitələri mövcuddur. Bu vasitələr peşəkar şəbəkələrin təkmilləşdirilməsinə, ictimai sağlamlıq proqramlarının inkişaf etdirilməsinə, pasiyentlərə və onların maarifləndirilməsinə xidmət edir [1, 2]. Öz sağlamlığı haqqında daha çox məlumat almaq istəyən və bunun üçün İnternet və tibbi sosial şəbəkələr vasitəsilə bilik əldə edən elektron pasiyentlər (e-pasiyentlər) şikətləri, xəstəlik simptomları ilə bağlı məlumatı sosial şəbəkədə yerləşdirir, təyin edilmiş diaqnoz və müalicə üsullarının etibarlılığını yoxlamaq üçün sağalmış pasiyentlərdən, ekspertlərdən dəstək alırlar. Hazırda krossorsinq texnologiyalarının tətbiqi anoloji presedentlərin tapılmasında pasiyentlərə dəstək göstərir [3–5].

E-pasiyentlər üçün belə imkanlar yaradan peşəkar saytlar qeydiyyat prosesində onlardan bir sıra fərdi verilənlərini qeyd etməyi tələb edir, sonradan həmin istifadəçilərin yerləşdirdiyi məlumatlar, kontentlər bu saytlar üçün əlyətərli olur. Təbii ki, tibbi sosial media mühitində, xüsusilə peşəkar şəbəkələrdə olan fərdi məlumatların konfidensiallığı ilə bağlı siyasətin düzgün qurulmaması (hətta olmaması) həmin informasiyanın

arzuolunmaz məqsədlər üçün istifadəsinə yol açır [6, 7]. Nəticədə tibbi sosial media mühiti pasiyentlər üçün dəyərli informasiya mənbəyindən onların fərdi məlumatlarının konfidensiallığı üçün təhlükə mənbəyinə çevrilir.

Təqdim edilən məqalədə sosial mediada e-pasiyentlərin fərdi məlumatları analiz olunmuş, onların tibbi saytlarda paylaşdığı məlumatların, hətta şəxsiyyətinin identikliyi verilənlərinin (ŞİV) yerləşdirməsinin fərdi məlumatların təhlükəsizliyi baxımından mümkün fəsadları göstərilmişdir. İstifadəçilərin tibbi sosial mediadan istifadəsi nəticəsində yarana biləcək konfidensiallıq riskləri göstərilmiş və konfidensiallıq siyasətinin məsələləri şərh edilmişdir.

II. TİBBİ SOSIAL ŞƏBƏKƏLƏRDƏ PASİYENTLƏRİN FƏRDI MƏLUMATLARI

Sosial şəbəkələrdən kütləvi surətdə istifadə olunması İnternet mühitində peşəkar tibbi sosial cəmiyyətlərin meydana gəlməsinə səbəb olmuşdur. Məsələn, *Doc2Doc*, *Ozmosis*, *Healtheva* kimi tibbi sosial şəbəkələri həkim və pasiyentlər arasında kommunikasiya qurmaq üçün ən nümunəvi platformalar hesab olunurlar. *The Medical Directors Forum*, *QuantiaMD*, *Doctors Hangout*, *Doc2Doc* kimi şəbəkələr isə həkimlərin bir-birilə və pasiyentlərlə kommunikasiya yaratmaları və əməkdaşlıq etmələri üçün mühüm platformalardır [8, 9]. *Medihost.ru*, *adam.com*, *DoctorSpring*, *likar.info*, *health.mail.ru* şəbəkələrində e-pasiyentlər ödənişsiz olaraq qeydiyyatdan keçməklə həkim xidmətlərindən yararlanırlar. Bu şəbəkələrdə qeydiyyatdan keçən e-pasiyentlərdən adı, yaşı, e-mail ünvanı, *qapsula.com_doslovno.com*-da isə həm də yaşadığı ərazi ilə bağlı məlumatı göstərməsi tələb olunur.

E-pasiyentlərin əksəriyyəti *Smart Patients*, *Stupidcancer*, *e-patients.net*, *Woman Heart Support Community*, *babycenter*, *Daily Strength* sosial şəbəkələrdən və sosial cəmiyyətlərin platformalarından istifadə edirlər. *PatientsLikeMe* [10] və *Treato* [11] sırf e-pasiyent cəmiyyətlərini dəstəkləyən sosial media resurslarıdır. *PatientsLikeMe* müxtəlif xəstəliklərin müalicəsindəki təcrübəyə əsaslanaraq terapiya (preparatlar da daxil olmaqla) növlərinin, simptomların, mümkün fəsadların və digər aspektlərin analizi üçün nəzərdə tutulmuşdur. Resursun əsas

məsələlərindən biri analoji diaqnozlu e-pasiyentləri tapmaq, müəyyən xəstəliyin müalicəsində istifadəçilərə uğurlu təcrübədən yararlanmaq imkanının yaradılmasıdır.

Azərbaycanda tibbin müxtəlif sahələri üzrə ixtisaslaşmış həkimləri bir portalda cəmləyən peşəkar sosial cəmiyyətlər fəaliyyət göstərir. Bunlara misal olaraq “*Həkim.tap*”, “*həkim.sənaz.az*”, “*sağlamolun.az*”, “*doctormap.az*” kimi sosial cəmiyyətləri göstərmək olar. E-pasiyentlər bu şəbəkələrin “həkim-axtarış” bölməsindən istifadə etməklə onları maraqlandıran həkimlər haqqında ətraflı məlumatlar əldə edə bilir, müəyyən suallarla həmin həkimlərə müraciət edə bilirlər.

Bir çox açıq cəmiyyətlərdə olduğu kimi, tibbi saytların əksəriyyətində istifadəçilər çox vaxt öz sağlamlıqları ilə bağlı məlumatları azad şəkildə yerləşdirməkdən çəkinmirlər. Saytlarda istifadəçilər haqqında iki cür verilənlər toplanılır: ümumi verilənlər və məhdud (identik) verilənlər. Ümumi verilənlərə istifadəçilərin tərcümeyi-halı, yaşam tərz, aldığı müalicələr, xəstəliyinin simptomları, laboratoriya nəticələri, genetik informasiyalar, sorğulara cavabları və digər istifadəçilərlə əlaqəsi aiddir. Əgər istifadəçi şəxsi identifikasiya informasiyası kimi adını və şəklini göstərsə, bu ümumi məlumat hesab edilə bilər. Amma istifadəçi şəxsi informasiya kimi, məsələn, elektron poçt ünvanını, parolunu göstərsə, bu artıq məhdud əlverişli veriləndir. Məhdud əlverişli verilənlərdən başqa saytda yerləşdirilən bütün verilənlər sayt tərəfindən digər istifadəçilərə və ya partnyorlarla mübadilə oluna bilər. Məsələn, *PatientsLikeMe* veb-saytının siyasətinə görə, istifadəçinin yerləşdirdiyi, məhdud əlverişli verilənlərdən başqa informasiyanın istənilən bir hissəsi digər istifadəçilərə və ya partnyorlara ötürülə bilər [10]. İstifadəçi “*Mənim profilim*”-də “kütləvi” variantını seçmədikdə, onun profilində yerləşdirdiyi informasiya nə satıla bilər, nə də digər partnyorlara ötürülə bilər.

Lakin bir tərəfdən fərdi məlumatların konfidensiallığı ilə bağlı istifadəçilərin kifayət qədər təlimatlı olmaması, digər tərəfdən, toplanan kontentin həddən artıq alıcısının olması konfidensiallığın qorunmasında çox böyük problemlər yaradır. Odur ki, saytlar xüsusilə ŞİV göstərilən informasiyaların təhlükəsizliyi üçün təhlükələrə yol açır.

Hazırda saytların biznes-modeli onlarda toplanan informasiyanın formaseptik kompaniyalara və digər maraqlı partnyorlara satılmasına yönəlmişdir. İstifadəçilərin kontenti belə partnyorlara müalicə metodlarının seçilməsi, dərman və tibbi avadanlıqların istehsalı üçün qərarlar qəbulunda dəstək olur. İstifadəçilərin sağlamlıq vəziyyəti haqqında verilənlər tədqiqatların keçirilməsi, hesabatların hazırlanmasında çox istifadə olunur. Beləliklə, istifadəçilər peşəkar virtual cəmiyyət daxilində verilənlərin mübadiləsinə praktiki olaraq nəzarət etmirlər. Onlar belə saytdan istədiyini “aldığına” görə şəxsi verilənlərini qeyd etməklə sanki ona qarşı bir “inam” nümayiş

etdirirlər və nəticədə konfidensiallıqla bağlı istifadə şərtlərini, siyasətini bəzən unudurlar.

1996-cı ildə ABŞ-da elektron tibbi kartlarda olan məlumatların qorunması üçün tibbi konfidensiallıq və mobilliyin sığortalanması haqqında qanun (*ing. Health Insurance Portability and Accountability Act of 1996 (HIPAA)*) və daha sonra onu təkmilləşdirərək iqtisadi və kliniki sağlamlıq üçün tibbi informasiya texnologiyaları haqqında qanun (*ing. Health Information Technology for Economic and Clinical Health HITECH*) qəbul edilmişdir [6, 12]. Lakin insanlar özləri könüllü surətdə veb saytlarda, virtual cəmiyyətlərdə şəxsi məlumatlarını yerləşdirərsə, burada HIPAA / HITECH onlar üçün “işləmir”. Beləliklə, tibbi sosial şəbəkələr e-pasiyentlər üçün geniş müzakirə meydanı yaratmaqla yanaşı, həm də bu mühitdə paylanmış məlumatların nəzərdə tutulmayan məqsədlər üçün istifadəsinə yol açmış olur, fərdi məlumatların konfidensiallığı üçün bir sıra risklər yaradır.

III. TİBBİ SOSIAL ŞƏBƏKƏLƏRDƏ KONFİDENSİALLIQ RİSKLƏRİ

Tibbi sosial şəbəkələr e-pasiyentlərin fərdi məlumatlarının təhlükəsizliyi və konfidensiallığına yönəlmiş aşağıdakı risklərin yaranmasına imkan verir.

Birincisi, saytlar, adətən, istifadəçi profillərinin nəhəng saxlancına malik olurlar və onları daimi olaraq saxlaya bilirlər. Belə saytlarda istifadəçilər vaxtaşırı olaraq öz fərdi məlumatlarını bölüşürlər, sağlamlığı ilə bağlı yaranmış vəziyyəti idarə etmək, səhhətini yaxşılaşdırmaq üçün öz problemini daha məzmunlu ifadə etməyə çalışır və konfidensiallıq məsələsini unudurlar [7]. Bəziləri isə əksinə, digərlərinə dəstək olmaq, özünün keçdiyi müalicə yolunda qarşılaşdığı problemlərlə digərlərinin üzləşməməsi üçün öz sağlamlığı ilə bağlı verilənləri saytda açıqlayır. Digər tərəfdən, tibb işçiləri də müəyyən cəmiyyətlərdə və təşkilatlarda hər hansı bir kliniki vəziyyətin müzakirəsi, yaranmış kritiki situasiyanın idarə olunması ilə bağlı iştirak etdikdə pasiyentlərinin konfidensial verilənlərinə istinad edirlər [13, 14]. Bir sıra peşəkarlar isə hətta sayt tərəfindən göstərilən xidmətin təkmilləşdirilməsi və təsadüfi mükafatlara görə pasiyentlərinin bütün fərdi məlumatlarını verməyə hazırdırlar [15]. Beləliklə, istifadəçilər haqqında ayrı-ayrı vaxtlarda açıqlanan verilənlər və əlaqəli (meta-) verilənlərin toplanması onların elektron sağlamlıq portretinin formalaşdırılmasına, konfidensiallıq riskinin yaranmasına zəmin yaradır.

İkincisi, istifadəçilər tərəfindən yaradılan kontent həm məqsədli, həm də nəzərdə tutulmayan auditoriya tərəfindən istifadə oluna bilər. Məsələn, istənilən fiziki və ya hüquqi şəxs qeydiyyatdan keçməklə saytın digər istifadəçilərinin verilənlərini əldə edə bilər, yəni veb-sayt istifadəçinin razılığı olmadan onun verilənlərini üçüncü tərəfə ötürə bilər [16]. Məsələn, checkMD (<http://www.checkMD.com>) saytı kimi saytlar öz işgüzar partnyorlarına və ya digər üçüncü tərəfə istifadəçilərinin şəxsi məlumatlarını açıqlaya bilər [17]. Belə

saytlar bəzən istifadəçilərinin bir sıra profil verilənlərinə istinad etməklə onların digər saytlarda olan qorunan məlumatlarına əlyetrəlikdə üçüncü tərəfə dəstək göstərirlər. Beləliklə, istifadəçilərin istəyindən asılı olmayaraq onların verilənləri müxtəlif maraqlı tərəflərin əlinə keçə bilər.

Üçüncüsü, sağlamlıq vəziyyəti ilə bağlı toplanmış verilənlər qeyr-tibbi məqsədlər üçün istifadə oluna bilər. Bir sıra tibbi sosial şəbəkələr kommersiya və şəxsi məqsədlər üçün sağlamlıqla bağlı verilənləri toplamağa əsaslanan biznes modellərə malikdirlər. Onlar sağlamlıq vəziyyəti ilə bağlı verilənləri həkimlərə, formasept və tibbi kompaniyalara, tədqiqatçılara, qeyri-kommersiya təşkilatlarına və s. ötürə bilərlər. Dərman istehsalı və tibbi avadanlıqların istehsalı ilə bağlı olaraq sağlamlıq vəziyyəti ilə bağlı aqreqatlaşdırılmış verilənlər kommersiya təşkilatları üçün çox qiymətli məlumatdır. Verilənlərin toplanması üzrə innovasiya texnologiyaları və tibbi informatika müxtəlif mənbələrdən alınan məlumatları əlaqələndirməyə qadirdir, bu da rəqəmsal dosyenin yaranmasına zəmin yaradır. Təbii ki, ayrılıqda götürülmüş verilənlər şəxs haqqında o qədər də çox məlumat vermir, lakin onlar bir yerə toplandıqda şəxs haqqında çox şeyi “söyləyə” bilər. Odur ki, sığorta şirkətləri, işəgötürənlər, müştəri axtaran kompaniyalar üçün belə rəqəmsal dosye çox fəvvaladə qiymətli mənbə ola bilər. Digər tərəfdən lazımı nəzarət olmadan saxlanılan belə dosyələr haker və oğrular üçün də çox cəlbəedici.

Nəhayət, daha bir məlum problem təhlükəsizlik təhdidinin miqyasıdır. Təbii ki, yuxarıdakıların həlli istiqamətində şifrələnmiş ötürmə, autentifikasiya və nəzarətin təmin edilməsi konfidensiallığın artırılmasına, ünvanlanmamış əlyetrəliyin aradan qaldırılmasına imkan verir. Lakin saytın “sındırılması” və ya saytın operatorunun bircə səhvi saytın çoxsaylı istifadəçilərinin rəqəmsal anketlərini təhlükə altına alır.

IV. TİBBİ SOSIAL ŞƏBƏKƏLƏRDƏ KONFİDENSİALLIQ SİYASƏTİ

İstifadəçilərin konfidensiallığa münasibəti fərqli ola bilər, xüsusilə xroniki xəstəlikləri olanlar üçün konfidensiallıq çox vacib məqamdır. Bəzən istifadəçilərin rəqəmsal savadsızlığı, veb-saytlardan düzgün istifadə etməməsi və öz şəxsi verilənlərini açıqlaması onlayn-praktikada tez-tez rast gəlinən hallardandır [18]. Təbii ki, tibbi sosial şəbəkə mühiti hamı tərəfindən dərk edilən konfidensiallıq strukturu ilə təmin olunmalıdır və burada aşağıdakılar nəzərə alınmalıdır.

Birincisi, belə strukturda mübadilə olunan verilənlər ilə risklər arasında qarşılıqlı əlaqə olduğunu nəzərə almaq lazımdır. İstifadəçilər nə qədər çox verilənlərlə mübadilə edərlərsə, bir o qədər çox risk etmiş olurlar. Sosial şəbəkələrdə konfidensiallıq probleminin vahid yoxlanılmış və real həlli – qeyd olunan verilənlərə məhdudiyyət qoyulmasıdır. Yəni risk faktorunu azaltmaq üçün istifadəçilər ən minimum həcmdə şəxsi verilənlərini təqdim etməlidirlər (hətta bunlar fərdin açıq veilənləri olsa da). Məsələn, istifadəçilər əsil adlarını və milli

identifikasiya nömrələrini bildirməməlidirlər. Buna baxmayaraq, istifadəçilər bir sıra tibbi sosial mənbələrdə onlara effektiv tibbi xidmət göstərilməsi üçün hətta belə verilənləri də göstərməli olurlar. Bir sıra istifadəçilər sayt tərəfindən təqdim olunan “konfidensiallıq siyasətini” qəbul etməklə (və hətta bu siyasətin “açıq” olduğunu bilsələr belə), elə hesab edirlər ki, saytda onların bütün şəxsi verilənləri qorunacaq [19].

İkincisi, istifadəçiləri öz şəxsi verilənlərinin konfidensiallığını təmin etməyə yönəltməkdir. Bu saytlarda informasiya mübadiləsi tibbi xidmətin keyfiyyətinin yaxşılaşdırılmasına yönəlsə də, verilənləri qərəzli auditoriyalarla mübadilədən qorumaq lazımdır. Konkret istifadəçinin verilənləri ya bütün geniş kütləyə açıq ola bilər, ya da istifadəçi konfidensiallıq problemindən xəbərdardırsa, veb-saytın yaratdığı imkandan istifadə etməklə öz verilənlərini yalnız seçilmiş “inamlı qruplar” üçün açıq edə bilər. Bu baxımdan saytlar bir neçə konfidensiallıq səviyyəsinə malik ola bilərlər.

Saytlarda istifadəçilərin fərdi məlumatlarının qərəzli açılması təhlükəsi ilə bağlı informasiyalara geniş yer verilməlidir. Məsələn, konfidensiallıq siyasətində göstərilməlidir ki, fərd kütlə tərəfindən görünən fərdi məlumatlarının silinməsinə tələb etmək hüququna malikdir. Sayt öz konfidensiallıq siyasətində, fərdi məlumatların toplanması, istifadəsi və açıqlanması ilə bağlı bir dəyişiklik edirsə, bu haqda istifadəçilərinin məlumatlandırılmalıdır və s.

Üçüncü, konfidensiallıq və təhlükəsizlik platforması elə qurulmalıdır ki, həm də kontent üçün yararlı olsun. Lakin bəzi tibbi sosial şəbəkələr yalnız istifadəçilərin ŞİV-in konfidensiallığına zəmanət verir, onların biznes modeli məhz yaranan kontentin kommersiya məqsədləri üçün istifadəsinə yönəlir. Odur ki, bu saytlar belə geniş miqyaslı konfidensiallığa zəmanət vermirlər, bu istifadəçilərin özlərinə oxşarların tapılmasına, problemlərinin həlli istiqamətində digərlərinin təcrübəsindən yararlanmağa imkan verməz. Bu problemin həlli üçün “layihələndirilmə yolu ilə konfidensiallıq” saytın arxitektura komponenti olmalıdır [20]. Bu prinsipin mahiyyəti odur ki, istifadəçidən heç bir hərəkət tələb etmədən, saytın özündə istifadəçilərin fərdi məlumatlarının nəzərdə tutulmayan əlyetrəlikdən, istifadədən və yayılmaqdan qoruyan elementlər, modullar nəzərdə tutulmalıdır. Bu baxımdan **verilənlərin ananimliyi metodları** fərdi həyat üçün minimum risk yaratmaqla sağlamlıq vəziyyəti ilə bağlı veilənlərin geniş miqyaslı məqsədlər üçün istifadəsinə imkan verir.

Dördüncüsü, tibbi verilənlərin qeyri-tibbi məqsədlərlə istifadəsinə görə fiziki və hüquqi şəxslərin məsuliyyətə cəlb edilməsidir. Son dövrlərdə tibbi verilənlərin kommersiya və şəxsi məqsədlər üçün istifadəsi verilənlərin konfidensiallığı ilə bağlı cəmiyyətin siyasi dialoqa cəlb edilməsinin zəruriliyini gündəmə gətirmişdir. Fiziki və hüquqi şəxslər istifadəçilərin konfidensiallığını pozarlarsa və bu HIPAA/HITECH çərçivəsindən kənardadırsa, bu halda İnternetdə tibbi

verilənlərin konfidensiallığının qorunması üçün yeni qanunvericiliyin işlənilməsi tələb olunur.

Qanunvericilikdə istifadəçilərin məlumatlarını qeyri-tibbi məqsədlər üçün təqdim edənələrə nəzarət edilməsi ilə bağlı bölmə nəzərdə tutulmalıdır. Qanunvericilik həm də şəxsi razılıq olmadan məlumatların kommersiya məqsədləri üçün istifadəsinə qadağa qoymalıdır. Qanunvericilər konfidensiallıq prinsiplərini qəbul edən provayderlərdən saytın konfidensiallığının təmini üçün qaydalara daima əməl olunmasını tələb etməlidirlər.

NƏTİCƏ

Məqalədə göstərilmişdir ki, lazımi tibbi dəstək almaq üçün sosial tibbi mediaya müraciət edən e-pasiyentlər peşəkar saytlarda qeydiyyatdan keçərək bir sıra şəxsi verilənlərini qeyd etməli olurlar, sağlamlıq vəziyyəti ilə bağlı müxtəlif məlumatları paylaşmalı olurlar. Saytlarda istifadəçilərin müxtəlif vaxtlarda göstərdiyi informasiyanın bir yere toplanması, bəzən ümumi verilənlərlə yanaşı ŞİV-in də sayta ötürülməsi fərdi məlumatların arzu olunmaz məqsədlər üçün istifadəsinə yol açır. Bu baxımdan fərdi məlumatların təhlükəsizliyinin təmin olunması üçün e-pasiyentlərin qarşılaşa biləcəyi konfidensiallıq riskləri analiz olunmuş, konfidensiallıq siyasəti məsələləri göstərilmişdir. Qeyd olunmuşdur ki, tibbi sosial media mühitində istifadəçilər nəinki ŞİV-in, hətta ümumi məlumatlarının mübadiləsində ehtiyatlı olmalı, mümkün qədər az verilənlə mübadilə etməyə çalışmalıdırlar. Bu baxımdan təqdim olunan məqalə tibbi sosial şəbəkə istifadəçilərinin fərdi məlumatlarının konfidensiallığı istiqamətində maarifləndirilməsi üçün zəruri materialdır. Digər tərəfdən, məqalədə göstərilən tibbi sosial şəbəkələrdə konfidensiallıq siyasəti məsələləri istifadəçilərin bu saytlara göstərdiyi “inam”ın doğruldulmasında müvafiq sayt layihələndiriciləri üçün əhəmiyyətli informasiya kimi istifadə oluna bilər.

İSTİNADLAR

- [1] M. Mammadova and A. Isayeva, “E-health activity in social media environment”, *Problems of information society*, 2018, no.1, pp.52–62.
- [2] M. Mammadova and Z. Jabrayilova, “Electronic medicine: formation and scientific-theoretical problems”, Baku: “Information Technologies” publishing house, 2019, 319 p.
- [3] G. Paul. The e-patient: empowered, enabled and electronic, <http://www.slideshare.net/>
- [4] M. Swan. “Crowdsourced Health Research Studies: An Important Emerging Complement to Clinical Trials in the Public Health Research Ecosystem”, *Journal of Medical Internet Research*, 2012, vol.14, no.2, e46.
- [5] Big data in the healthcare industry: Growing Need for Computerized Decision Support, <http://www.healthcare.siemens.com/magazine/mso-big-data-and-healthcare-1.html>
- [6] L. Jingquan, “Privacy policies for health social networking sites”, *Journal of the American Medical Informatics Association*, vol.20, no.4, pp.704–707, <https://doi.org/10.1136/amiajnl-2012-001500>
- [7] L. Jingquan, “Improving chronic diseases self-management through social networks”, *Popul Health Manag.*, 2013, vol.16, no5, pp.285–291. doi: 10.1089/pop.2012.0110

- [8] Top social networking sites for healthcare medical professionals, <http://www.medicallabtechnicianschool.org/2009/top-25-social-networking-sites-for-healthcare-medical-professionals>
- [9] Report “Issue Brief: Social Networks in Health Care Communication, collaboration and insights”. Produced by the Deloitte Center for Health Solutions, 2010, p.2, <http://www.healthinformationandcommunicationsystems.pbworks.com/w/file/93972338/SM%204b%20Full.pdf>
- [10] The future of health is here, www.patientslikeme.com
- [11] See what millions of patients are saying, <https://treato.com>
- [12] M. H. Mammadova, “The information security of personal medical data in an electronic environment”, *Problems of information technology*, 2015, no.2, pp.15–25.
- [13] G. Moubarak, A. Guiot, Y. Benhamou, et al. “Facebook activity of residents and fellows and its impact on the doctor-patient relationship”, *J Med Ethics*, 2011, vol.37, pp.101–104.
- [14] L. Thompson, E. Black, W. Duff et al. “Protecting health information on social networking sites: Ethical and legal considerations”, *J Med Internet Res*, 2011, vol.13, e8. <http://www.jmir.org/2011/1/e8/>
- [15] A. Acquisti, J. Grossklags, “Privacy and rationality in individual decision making”, *IEEE Secur Privacy*, 2005, vol. 3, pp.26–33.
- [16] J. Williams, “Social networking applications in health care: threats to the privacy and security of health information”, *Conf Proc SEHC*, 2010, no.2, pp.39–49.
- [17] Terillion Privacy Policy. <http://www.terillion.com/privacy-policy/> (accessed 25 Mar 2013).
- [18] S. Livingstone, D. Brake, “On the rapid rise of social networking sites: new findings and policy implications”, *Children Soc*, 2010, no.24, pp.75–83.
- [19] D. McGraw, J. Dempsey, L. Harris et al., “Privacy as an enabler, not an impediment: building trust into health information exchange”, *Health Aff*, 2009, no.28., pp.416–427.
- [20] S. Collins, D. Vawdrey, R. Kukafka R et al. “Policies for patient access to clinical data via PHRs: current state and recommendations”, *J Am Med Inform Assoc*, 2011, vol.18, pp12–17.

SECURITY ISSUES OF PERSONAL DATA OF MEDICAL SOCIAL MEDIA USERS

Masuma Mammadova¹, Zarif Jabrayilova²

^{1,2}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹mmg51@mail.ru, ²depart15@iit.science.az

Abstract – Taking into account the opinion of the mass in the medical social media environment, the formation of e-medicine becomes an important source of information for the improvement of the quality of medical services, the perfection of the medical decision-making process, implementation of numerous sociological surveys, etc. E-patients use social media to address the issues they concern about and attempt to benefit from the content professional sites registering in these sites. When registering, the users are often required to fill in their personally identifiable data along with their public information. However, this poses a serious problem for the privacy of user data in the social media environment where the privacy policy is vulnerable. This article analyzes the privacy risks of the users in medical social networks and provides a number of recommendations regarding the privacy policy.

Keywords – *medical social media environment, e-patients, personally identifiable information, privacy risks, privacy policies.*

Milli mentalitetdə fərdi məlumatların yeri və onların mühafizəsi problemləri

Rasim Əliquliyev¹, Rasim Mahmudov²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹director@iit.science.az, ²pr@iit.science.az

Xülasə— Məqalədə şəxsi həyat və fərdi məlumatların mahiyyətinə dair yanaşmalar şərh olunur. Azərbaycan mentalitetində həssas fərdi məlumatların yeri və onlarla bağlı problemlər analiz edilir. Bu problemlərin aradan qaldırılması üçün kompleks təkliflər irəli sürülür.

Açar sözlər— şəxsi həyat; fərdi məlumatlar; həssas məlumatlar; milli mentalitet.

I. GİRİŞ

Fərdlər haqqında məlumatların toplanması və emalı prosesləri bəşəriyyətin bütün inkişaf mərhələlərində olmuşdur. Müasir dövrdə isə sürətlə inkişaf edən İKT, o cümlədən müxtəlif elektron dövlət sistemlərində elektron kommersiya, elektron ödəniş, çoxsaylı Internet xidmətləri, çoxfunksiyalı smartfonlar, GPS sistemləri, smart televizorlar, Əşyaların Interneti texnologiyaları, videomüşahidə sistemləri, biometrik texnologiyalar və s. hər bir fərd haqqında fasiləsiz olaraq böyük həcmdə informasiya toplamaq imkanlarını dəfələrlə artırır. Bu imkanlar da, öz növbəsində, fərdi məlumatlarla bağlı daha geniş məqsədlərin ortaya çıxmasına zəmin yaradır.

Azərbaycanda da informasiya texnologiyalarının sürətlə inkişaf prosesi gedir, artıq Internet infrastrukturunu bütün ölkəni əhatə edir, əhalinin 80%-i Internet istifadəçisidir, mobil telefon abunəçilərinin sayı isə 11 milyona çatıb [1]. Ölkəmizdə insanların söz və Internet azadlıqları yüksək səviyyədə təmin edilib. Vətəndaşlarımız müxtəlif sosial şəbəkələrdən, elektron ticarət, virtual təhsil və digər xidmətlərdən fəal şəkildə istifadə edirlər. Bütün bunlar ölkəmizdə fərdi məlumatların qorunması məsələsini də aktuallaşdırır.

Fərdi məlumatların mühafizəsi məsələsinə, bütövlükdə, milli təhlükəsizlik prizmasından yanaşmaq lazımdır. Azərbaycanda tarixən milli və dini dəyərlərdən qaynaqlanan möhkəm ailə institutu mövcuddur. Bizim cəmiyyətdə ailə həyatına dair, xüsusən, zərif cinsin nümayəndələri ilə bağlı fərdi məlumatlara qarşı xüsusi həssaslıq mövcuddur. Ölkəmizdə ailə institutları dövlətimizin, cəmiyyətimizin təməli sayılır. Ona görə də dövlətimizin, cəmiyyətimizin təhlükəsizliyini təmin etmək üçün vətəndaşların bu tip məlumatları etibarlı şəkildə mühafizə edilməlidir. Çünki şəxsi həyata dair fərdi məlumatlara qanunsuz müdaxilələr ailələrin dağılmasına, psixoloji sarsıntılara və digər neqativ hallara səbəb ola bilər.

II. ŞƏXSİ HƏYAT VƏ FƏRDİ MƏLUMATLARIN MAHİYYƏTİNƏ DAİR YANAŞMALAR

Fərdi məlumatlar şəxsi həyatın mühüm tərkib hissəsi sayılır. Başqa sözlə, şəxsi həyatın toxunulmazlığının təmin edilməsi həm də fərdi məlumatların mühafizəsini zəruri edir. Ona görə də fərdi məlumatların mahiyyətini daha aydın şəkildə təsəvvür etmək üçün ona şəxsi həyat prizmasından yanaşmaq məqsəduyğundur.

“İnsan hüquqlarının və azadlıqlarının mühafizəsi haqqında” Avropa Konvensiyasının (1950) 8-ci maddəsinin tətbiq edilməsi praktikası sayəsində bu terminin dəqiq normativ izahı verilmişdir. Belə ki, Avropa İnsan Hüquqları Məhkəməsinin (1992) bəyanatında göstərilir: “Şəxsi həyat – tam təsvir edilə bilməyən geniş kateqoriyadır. Hər bir insan bu anlayışı inkişaf etdirməkdə və ona müəyyən məna verməkdə sərbəstdir. Bu anlayışı “daxili çevrə” ilə məhdudlaşdırmaq və bu çevrəyə daxil olmayan xarici aləmi istisna etmək yolverilməzdir. Beləliklə, “şəxsi həyat” anlayışı digər şəxslərlə və xarici aləmlə qarşılıqlı əlaqənin inkişaf etdirilməsi hüququnun zəruriliyini özündə əks etdirir” [2].

Şəxsi həyatın “toxunulmazlığı” anlayışının və beynəlxalq sənədlərdə işlədilən “privacy” termininin ümumi ekvivalenti azadlıq, məhrəmlilik, sirr, tənhalıq, mülkiyyət, şəxsiyyət, özəl, özəl yaşayış, toxunulmazlıq, şəxsiyyət, şəxsiyyətlərə münasibətlər mənalarında işlədilən latın dilindəki “gizlilik” ifadəsidir.

Müasir ingilis dilində “privacy” aşağıdakı kimi şərh olunur [3]:

1. fərdi, şəxsi, sirli;
2. hamı üçün deyil, ayrıca bir insan, seçilmiş qrup üçün müəyyən edilmiş və ya nəzərdə tutulmuş;
3. müstəqil, hakimiyyətdən və dövlət xidmətindən asılı olmayan;
4. qeyri-rəsmi, rəsmi mövqe ilə bağlı olmayan, ictimai həyatdan asılı olmayan;
5. başqalarının görmədiyi, eşitmədiyi və nəzarət etmədiyi elə bir yer ki, oraya getmək mümkün olsun;
6. şəxsi həyatını yaşayan insan.

“Privacy” anlayışı rus dilində olan “Большое право” “Böyük hüquq lüğət”də belə izah olunur [4]: “ingilis-amerikan hüquq sistemində şəxsi

həyat sirrini və toxunulmazlığını, insanın intim sferasını ifadə edən xüsusi hüquqi kateqoriyadır. “Privacy” termininin rus dilində analoqu yoxdur. Bu termin bəzi hallarda “şəxsi həyat”, digər hallarda “şəxsi həyat hüququ”, başqa hallarda isə “şəxsi həyatın toxunulmazlığı hüququ” kimi anlaşıla bilər.

Azərbaycan dilində isə “privacy” termininin hələlik rəsmi olaraq nə elmi, nə də hüquqi izahı verilməmişdir.

Ümumi “məlumatlar” anlayışından xüsusi “fərdi məlumatlar” kateqoriyasının fərqləndirilməsi onunla əlaqədardır ki, bu cür məlumatlar insanın şəxsi həyatının həssas atributları sferasına aiddir. Bir sıra ölkələrin hüquqi sənədlərində bu cür məlumatları təsvir etmək məqsədi ilə “şəxsiyyəti identifikasiya etmək üçün informasiya” ifadəsindən istifadə edilir.

Fərdi məlumatları onların aid olduğu şəxslərin özlərinin münasibətinə görə iki kateqoriyaya ayırmaq olar [5]:

- açıqlanmasına və yayılmasına məlumat subyektlərinin etinasız yanaşdığı “neytral” fərdiləşdirilmiş məlumatlar;
- subyektin döviyyəsinə məhdudlaşdırmaq istədiyi məlumatlar.

İkinci kateqoriyaya aid olanlar “fərdi məlumatlar” adlanır və bu cür məlumatın icazəsiz əldə edilməsi və istifadəsi beynəlxalq hüquqda “məlumat subyektinin hüquqlarına qəsd” kimi təsnif edilir.

Həç bir qanunvericilik aktında fərdi məlumatların dəqiq siyahısı və ya sərhədi müəyyən edilməyib. O cümlədən, Azərbaycan qanunvericiliyinə görə, “fərdi məlumatlar - şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumatlardır”[6]. Bu cür məlumatların müəyyən edilməsinin özü də fərdi yanaşmadan asılıdır.

III. AZƏRBAYCAN MENTALİTETİNDƏ HƏSSAS FƏRDİ MƏLUMATLARIN YERİ VƏ YARATDIĞI PROBLEMLƏR

Doğrudur, şəxsi həyat və onun tərkib hissəsi olan fərdi məlumatların həddlərinin müəyyən edilməsinə nəzərdə tutan bir sıra beynəlxalq və milli səviyyələrdə normativ-hüquqi sənədlər mövcuddur. Amma bu həddlərin müəyyən edilməsinin şəxsi, milli və regional ölçüləri də mövcuddur. Bu ölçülər heç də həmişə hüquqi çərçivələrlə üst-üstə düşmür. Bir çox hallarda müvafiq milli qanunvericilik aktları mental xüsusiyyətləri deyil, beynəlxalq tövsiyələri və xarici ölkələrin praktikasını nəzərə alaraq hazırlanır. Nəticədə fərdi məlumatlarla bağlı ictimai münasibətlərin tənzimlənməsi idarəolunmaz hala gəlib çıxır.

Azərbaycan da şəxsi həyata, fərdi məlumatlara münasibətdə mental dəyərlərin böyük təsir imkanına malik olduğu ölkələr sırasındadır. Ölkəmizdə şəxslərə aid həssas məlumatların əhatə dairəsi kifayət qədər genişdir. Zərif cinsin nümayəndələri ilə bağlı həssaslıq dərəcəsi isə daha yüksək həddədir (Onların yaş həddindən və ailə vəziyyətindən asılı olaraq həssaslıq səviyyəsi artıb-azalır). Bu da fərdi məlumatlarla bağlı şantaj və digər manipulyasiya hallarını stimullaşdıran amil kimi çıxış edir. Azərbaycanda İnternet istifadəçilərinin sayının yüksək həddə

çatması, sosial şəbəkələrin əhali arasında yüksək populyarlıq qazanması nəticəsində fərdi məlumatların bədnıyyətli əməllər üçün istifadə hallarının artması müşahidə olunur [5].

Bir sıra ölkələrdə qanunsuz əldə edilən fərdi məlumatlar biznes fəaliyyəti üçün dəyərli hesab olunur. Lakin elə ölkələr də var ki, orada bu cür məlumatlardan daha çox kriminal məqsədlər, o cümlədən şantaj məqsədi ilə istifadə edirlər. Araşdırmalarımız göstərir ki, Azərbaycanda da fərdi məlumatlardan aid olduğu şəxsləri şantaj etməklə onlardan pul tələb etmək üçün istifadə halları az deyil. Ölkəmizdə şantaj məqsədi ilə daha çox qadınlara məxsus həssas fərdi məlumatlardan istifadə edilir. Azərbaycanda xanımlara aid fərdi məlumatların həssaslıq dərəcəsinin yüksək olması, ilk növbədə, milli-mənəvi dəyərlərdən irəli gəlir. Yəni bizim bu dəyərlərimizdə qadın adının çox yüksək tutulması ilə əlaqədardır.

Bir sıra hallarda isə müəyyən şəxsləri nüfuzdan salmaq, karyerasına zərbə vurmaq, ailəsində problem yaratmaq və s. neqativ məqsədlərlə onlar haqqında şəxsi həyata dair yanlış, yalan məlumatlar yayılır. Sürətlə inkişaf edən informasiya texnologiyaları da dezinformasiya xarakterli montaj edilmiş audio, video, foto materialları yaymağa imkan verir.

Ölkəmizin kütləvi informasiya vasitələrində vətəndaşların fərdi məlumatlarının qanunsuz açıqlanmasının neqativ nəticələri ilə əlaqədar xəbərlərə tez-tez rast gəlmək mümkündür. Təəssüflər olsun ki, Azərbaycanda fərdi məlumatların qanunsuz olaraq açıqlanması ilə əlaqədar baş verən bu cür neqativ hallarla bağlı tədqiqatlar aparılmır, müvafiq statistik hesabatlara hazırlanmır.

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. Bu halda vəzifəli şəxslər karyerasına zərbə vurulmasından, evli şəxslərin ailəsinin dağılmasından qorxaraq şantaj edən tələblərini yerinə yetirməyə məcbur olurlar.

Azərbaycanda kafe və restoranlarda şəxsi kabinetlərə, avtomobillərdə jalüz və pərdələrə, hündür hasarlı fərdi evlərə, villalara yüksək tələbatın olması da məhz başqalarının şəxsi həyatına yüksək marağın olması, zərif cinsin nümayəndələrinə aid fərdi məlumatların həssaslıq dərəcəsinin yüksək olması, insanların fərdi məlumatlar vasitəsi ilə şantaj edilmə riskinin yuxarı olması ilə əlaqədardır.

Doğrudur, Azərbaycan qanunvericiliyinə 2017-ci ildə edilmiş əlavə və dəyişikliklər İnternet mühitində fərdi məlumatların qanunsuz döviyyəsinin qarşısının alınmasına xidmət edir, amma bu məsələ ilə bağlı ölkəmizdə məhkəmə praktikası çox zəifdir, müvafiq hüquqları pozulanlar tərəfindən məhkəmələrə müraciət etmə hallarına çox nadir hallarda rast gəlinir [7]. Bu sahədə vətəndaşlar arasında hüquq mədəniyyətinin formalaşmaması əsas səbəblərdən biridir. Vətəndaşlar hüquqlarını pozanların, onları təhdid edənlərin cəzalandırılmasını, onlara dəyən maddi və mənəvi ziyanın

əvəzinin ödənilməsinə tələb etməyə o qədər də meyilli deyillər. Onlar daha çox hədəflərinə tuş gəldikləri ilə “dil tapmağa”, məsələnin ictimailəşməsinin qarşısını almağa meyl göstərirlər.

Şəxsi həyatın toxunulmazlığının təmin olunması, fərdi məlumatların qorunması məsələləri müasir dövrdə informasiya texnologiyaları ilə sıx bağlıdır. Ona görə də bu sahədə texnoloji və hüquqi bilikləri özündə birləşdirən spesifik kadrların yetişdirilməsi vacibdir. Bu sahədə məhkəmə ekspertizasının obyektiv və effektiv şəkildə həyata keçirilməsi üçün xüsusi laboratoriyaların təşkil edilməsinə ehtiyac vardır. Həqiqi və saxta foto, video görüntüləri, audio yazıları bir-birindən ayırmaq üçün xüsusi avadanlıqlar, biliklər və səriştə tələb edilir.

Müasir dövrün reallıqlarından biri də budur ki, bəzən insanların özləri fərdi məlumatlarını yaymaqda maraqlı olurlar. Bu, əsasən, cəmiyyətdə neqativ populyarlıq qazanmaqla əldə etdikləri sosial kapitalı maddi kapitla çevirmək istəyənlərin tətbiq etdikləri bir üsuldur. Dünya şou-biznes aləmində bu üsuldən geniş istifadə edilir. Son zamanlar Azərbaycanda da bu üsuldən istifadə halları müşahidə edilməkdədir.

Şəxsi həyat sirrinin, fərdi məlumatların qanunsuz olaraq yayılması yuxarıda qeyd edilən bir sıra problemlərə yol açdığı kimi, bəzən əksinə, onların gizli saxlanması müəyyən problemlər yaradır. Bu problemlər, əsasən, gənclərin ailə qurumları ilə əlaqədardır. Məlum olduğu kimi, fərdi məlumatların ən mühüm əhəmiyyət kəsb edən növlərindən biri tibbi məlumatlardır.

Tədqiqatlar göstərir ki, bir çox insanlar öz tibbi məlumatlarına daha həssas yanaşırlar, onları qorumaqda daha çox maraqlıdırlar. Məsələn, informasiyanın mühafizəsi məsələlərinə böyük diqqət yetirən EMC korporasiyası 2014-cü ildə fərdi məlumatlarının konfidensiallığına riayət edilməsinə dair insanların münasibətlərini analiz edən tədqiqatlarının nəticələrini dərc etmişdir [8]. Ümumilikdə, tibbi xidmət istifadəçilərinin fərdi məlumatlarının konfidensiallığının daha çox qayğısına qaldığı məlum olmuşdur.

Bu, əsasən, onunla əlaqədardır ki, insanlar özlərinin səhhətləri, müəyyən xəstəlikləri ilə bağlı məlumatların açıqlanmasının peşə fəaliyyətləri, karyeraları, eləcə də, ailə həyatı ilə bağlı problemlər yaratmasından narahat olurlar. Doğrudur, elə spesifik peşə fəaliyyəti sahələri var ki, işə qəbul zamanı müəyyən parametrlər üzrə sağlamlıq haqqında tibbi arayış tələb olunur. Lakin tibbi arayış tələb olunmayan sahələrdə də hər hansı şəxsin səhhəti ilə bağlı neqativ məlumatların yayılması onun peşə vəzifələrini lazımi səviyyədə yerinə yetirə bilməsinə dair inamsızlıq yarada bilər.

Azərbaycan reallığında fərdi tibbi məlumatlara daha çox ailə həyatının qurulması baxımından böyük həssaslıqla yanaşılır. Müəyyən neqativ tibbi göstəriciləri olan şəxslər ailə qurarkən bunu gizli saxlamağa nə qədər ciddi say göstərirərsə də, əks tərəf də bu cür məlumatların əldə edilməsində o qədər maraqlı olur. Adətən, ailə qurmaq istəyən gənclərin yaxınları və ya özləri əks tərəf haqqında müxtəlif fərdi məlumatları əldə etməyə çalışırlar. Bir çox hallarda ailə qurmaq haqqında qərar da bu məlumatların analizi əsasında verilir. Həmin məlumatların arasında ən yüksək həssaslıq dərəcəsinə malik

olan da məhz tibbi məlumatlardır. O cümlədən genetik tibbi məlumatlar da qərar qəbul etmə üçün çox mühüm əhəmiyyət daşıyır [5].

Azərbaycanın 1 iyun 2015-ci il tarixindən tətbiq edilən mövcud qanunvericiliyinə əsasən, rəsmi nigaha girmək istəyən gənclər bunun üçün, ilk növbədə, tibbi müayinədən keçməlidirlər [9]. Doğrudur, tibbi müayinənin neqativ nəticələri olarsa, cütlüklərin evlənməməsinə dair yalnız tövsiyə verilir, yəni onlara ailə qurmaq qadağan edilmir. Amma bu cür tibbi müayinənin neqativ nəticələrini əsas götürərək ailə qurmaqdan imtina edən gənclər də az deyildir.

Nəzərə almaq lazımdır ki, ölkəmizdə ailə qurmaq isəyən cütlüklər bu müayinədən, adətən, toy ərəfəsində keçirlər. Buna qədər elçilik, nişan, xınayaxdı kimi proseslərdən keçmiş, hətta qızın cəhizini oğlan evində yerləşdirmiş, toy gününü və toyun keçiriləcəyi şadlıq evini müəyyənləşdirmiş, qonaqlara dəvətnamələr göndərmiş olurlar. Ona görə də son anda evlənməkdən imtina edilməsi böyük maddi və mənəvi-psixoloji problemlər yaradır.

Müvafiq tibbi müayinə zamanı iki qrup – genetik və infeksiya xəstəlikləri yoxlanılır. Infeksiya xəstəlikləri ilə bağlı tibbi arayış verildiyi vaxtdan bir ay müddətində etibarlı sayılır. Amma insanlara aid genetik məlumatlar dəyişməzdir. Ona görə də genetik uyğunluq haqqında məlumatları gənclər bir-birləri ilə münasibət qurmadan öncə də əldə edə bilərlər.

IV. AZƏRBAYCANDA FƏRDİ MƏLUMATLARIN MÜHAFİZƏSİ MƏSƏLƏLƏRİNƏ DAİR TƏKLİFLƏR

İnformasiya texnologiyalarının sürətli inkişafı nəticəsində fərdi məlumatların əldə edilməsi imkanlarının hədsiz dərəcədə artması bu sahədə ictimai münasibətləri daha da mürəkkəbləşdirir və aktuallaşdırır. Doğrudur, bütün dünyada, eləcə də, Azərbaycanda bu münasibətləri daha effektiv şəkildə tənzimləmək üçün vaxtaşırı qanunvericilik bazası təkmilləşdirilir, inkişaf etdirilir.

Lakin informasiya texnologiyalarının inkişaf tempi, o cümlədən 4-cü sənaye inqilabının yaratdığı yeni virtual reallıqlar və əhalinin həyat tərzinin buna uyğunlaşması fonunda dərin kök atmış mental dəyərləri qorumaq cəhdlərinin doğrduğu situasiyanı yalnız qanunvericilik çərçivəsində nizmlamaq mümkün olmur. Bu məsələni yalnız hüquqi müstəvidə həll etmək cəhdləri yetersizdir. Məsələnin uğurlu həlli, ilk növbədə, kompleks baxış bucaqlarının bir araya gətirildiyi multidissiplinar elmi araşdırmaların aparılmasını tələb edir. Fərdi məlumatların mühafizəsi sahəsində hüquqi aspektlərlə yanaşı, texnoloji, sosial, psixoloji, kulturoloji, iqtisadi və s. istiqamətlər üzrə tədqiqatların aparılması aktuallıq kəsb edir. Halbuki bu gün fərdi məlumatlarla bağlı problemlər, bütövlükdə, dünya elmində daha çox hüquqi və qismən də texnoloji məsələ kimi qəbul olunur.

Fərdi məlumatların qorunması sahəsində texnoloji, hüquqi və s. zəruri biliklərə malik olan yüksəkixtisaslı kadrların hazırlanmasına ciddi ehtiyac vardır. Xüsusən, hüquq-mühafizə orqanlarında, məhkəmə-eksperiza sahəsində bu cür kadrların çatışmazlığı hiss olunur. Bu sahə üzrə, ilk növbədə, elmi-pedagoji kadrların yetişdirilməsi vacibdir. Məhz bu sahə üzrə

elmi-pedoloji kadrlar olmalıdır ki, onların vasitəsi ilə digər müvafiq mütəxəssislər hazırlansın.

Fərdi məlumatlar və onların qorunması mexanizmləri haqqında vətəndaşlar çox cüzi və səthi məlumatlara malikdirlər. Ümumiyyətlə, ölkədə virtual və texnoloji hüquq mədəniyyəti çox zəifdir. Ona görə də əhali arasında, xüsusən, gənc nəslin nümayəndələrinə bu sahədə maarifləndirici tədbirlərin həyata keçirilməsi vacibdir. Bu gün Azərbaycan vətəndaşları sosial şəbəkələrdən və digər İnternet xidmətlərindən geniş istifadə edirlər ki, bu zaman fərdi məlumatlarla düzgün davranmaq tələb olunur. Hətta təhsil proqramlarına müvafiq dərslərin daxil edilməsi zəruridir.

Dünyanın bir sıra ölkələrində vətəndaşların fərdi məlumatlarının qorunmasına cavabdeh olan rəsmi dövlət qurumları fəaliyyət göstərir. Məsələn, Avstraliyada “İnformasiya konfidensiallığı üzrə komissarlıq”, Kanadada “İnformasiya hüquqları üzrə ombudsman”, Almaniyada “İnformasiya azadlığı və məlumatların qorunması üzrə komissar”, Hindistanda “Dövlət informasiya ombudsmanı”, İsveçdə “İnformasiyanın qorunması üzrə komissarlıq”, Böyük Britaniyada “Fərdi məlumatların qorunması, informasiya azadlığı və informasiya ekologiyası üzrə ombudsman” adlı təsisatlar mövcuddur [10]. Həmin təsisatlar öz fəaliyyəti barədə illik hesabatlar verirlər.

“İnformasiya əldə etmək haqqında” Azərbaycan Respublikasının Qanununda (2005) da ölkəmizdə “informasiya məsələləri üzrə müvəkkil” vəzifəsinin təsis edilməsi nəzərdə tutulmuşdu [11]. Lakin 2012-ci ildə bu qanuna edilən dəyişikliklərə uyğun olaraq, həmin vəzifəsinin icrası İnsan hüquqları üzrə Ombudsmana həvalə edilmişdir. Digər ölkələrdən fərqli olaraq, Azərbaycanın İnsan hüquqları üzrə Ombudsmanı ölkədəki informasiya hüquqlarının qorunması vəziyyəti ilə bağlı illik hesabatlar vermir. Yaxşı olardı ki, qabaqcıl ölkələrdə olduğu kimi, Azərbaycanda da informasiya hüquqları üzrə ayrıca qurum fəaliyyət göstərsin, dövlət və cəmiyyət qarşısında hesabatlı olsun.

Ölkəmizdə fərdi məlumatların qeyri-qanuni ictimailəşdirilməsində elektron kütləvi informasiya vasitələri və sosial şəbəkə istifadəçiləri xüsusi rol oynayır. Jurnalistlərin fərdi məlumatlarla işləyərkən müvafiq hüquqi tələbləri yaxşı bilməmələri və nəzərə almamaları bu cür halların kütləviləşməsinə səbəb olur. Ona görə də jurnalistika təhsilinə dair proqramlara fərdi məlumatlarla bağlı dərslərin daxil edilməsi, həmçinin bu sahədə çalışanlar üçün mütəmadi olaraq müvafiq təlimlərin təşkil edilməsi zəruridir.

Həmçinin ölkədə sağlam nəslin yetişdirilməsi, ölkənin demografik təhlükəsizliyi, ailələrdə problemlərin yaranmaması baxımından tibbi xarakterli müvafiq fərdi məlumatların maraqlı şəxslər üçün açıqlanmasının təmin edilməsi arzuolunan haldır. Lakin bu zaman insan hüquqlarına dair beynəlxalq normaların və onun əsasında formalaşdırılan milli qanunvericiliyin tələblərinin gözlənilməsi də vacib şərtidir.

NƏTİCƏ

Müasir dövrdə əsas maddi sərvətə çevrilən informasiyanın mühüm bir hissəsi fərdi xarakterlidir, hansısa şəxslərə aiddir və onların taleyində mühüm rol oynayır. Fərdi məlumatların mühafizəsi həm də yaşadığımız informasiya cəmiyyətində təhlükəsizliyin, asayişin təmin edilməsinin, milli-mənəvi dəyərlərimizin qorunmasının mühüm vasitələrindən və istiqamətlərindən biridir. Bu baxımdan, fərdi məlumatların mühafizəsinə dövlətin strateji maraqları prizmasından yanaşılması vacibdir.

ƏDƏBİYYAT

- [1] Azərbaycan Dövlət Statistika Komitəsi, İnformasiya və kommunikasiya texnologiyaları (İKT) üzrə əsas göstəricilər, <http://www.stat.gov.az>
- [2] О. Красотенко, Понятие «частная жизнь» в решениях Европейского Суда по правам человека, Сборник тезисов 68-й научно-практической конференции студентов, магистрантов и аспирантов факультета международных отношений БГУ. Минск, 27 апреля 2011, с. 51-53.
- [3] М. Мельников, О семантике понятия “приватное”, XIII международная научная конференция преподавателей, аспирантов и студентов НСИ, 2012, с.181-189.
- [4] А. Сухарев, В. Крутских, А. Сухарева, Большой юридический словарь., М.: Инфра-М., 2009, 858 с.
- [5] R.Əliquliyev, R.Mahmudov, Milli mentalitet kontekstində fərdi məlumatların həssaslığı və onların təhlükəsizliyinin təmin edilməsi məsələləri, İnformasiya cəmiyyəti problemləri, 2019, №2, s. 117-128.
- [6] “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanunu, <http://www.e-qanun.az/framework/19675>
- [7] “İnformasiya, informasiyalasdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanununda dəyişikliklər edilməsi barədə Azərbaycan Respublikasının Qanunu, <http://e-qanun.az/framework/35124>
- [8] В. Коржов, Менталитет и конфиденциальность // Открытые системы, 2014, <https://www.osp.ru/news/articles/2014/24/13041843>
- [9] Nikaha daxil olan şəxslərin tibbi müayinəsi ilə bağlı “Azərbaycan Respublikasının Ailə Məcəlləsində dəyişikliklərin edilməsi haqqında” Azərbaycan Respublikası Prezidentinin 2014-cü il 15 dekabr tarixli 389 nömrəli Fərmanının icrası barədə Azərbaycan Respublikası Səhiyyə Nazirliyi Kollegiyasının Qərarı, 25 may 2015-ci il, <http://www.sehiyye.gov.az/files/pdf/2015qerar26.pdf>
- [10] B.van der Sloot, S. van Schendel, International and comparative legal study on Big Data, The Netherlands Scientific Council for Government Policy, 2016, 126 p.
- [11] “İnformasiya əldə etmək haqqında” Azərbaycan Respublikasının Qanunu, <http://www.e-qanun.az/framework/11142>

THE PLACE OF PERSONAL DATA IN THE NATIONAL MENTALITY AND ISSUES OF ITS PROTECTION

Rasim Alguliyev¹, Rasim Mahmudov²

^{1,2} Institute of Information Technology of ANAS, Baku, Azerbaijan

¹r.alguliev@gmail.com, ²rasimmahmudov@gmail.com

Abstract— The article interprets the approaches to personal life and personal data. The place of sensitive personal data in the Azerbaijan mentality and related problems are identified. Complex proposals are offered to eliminate these problems.

Keywords— *personal life, personal data, sensitive information, national mentality*

Milli mentalitet və stereotiplər kontekstində fərdi məlumatlara həssaslığın folklorik təzahürləri

Hikmət Quliyev

AMEA Folklor İnstitutu, Bakı, Azərbaycan
quliyevh@mail.ru

Xülasə— Fərdi məlumatların təhlükəsizliyi müasir dövrün ən aktual problemlərindədir. Internetin əsas kommunikasiya vasitəsinə çevrildiyi hazırkı şəraitdə fərdi məlumatların təhlükəsizliyinin təmin edilməsi təkcə texnoloji deyil, eyni zamanda beynəlxalq hüquq və milli mentalitetlə bağlı olan məsələdir. Məqalədə fərdi məlumat anlayışı folklor kontekstində öyrənilmiş, milli mentalitet və stereotiplərin təsiri ilə meydana gələn və yaşadılan folklorik təzahürlər təhlil edilmişdir. Tədqiqata ənənəvi folklor nümunələri ilə bərabər, virtual sosial şəbəkələrdən qeydə alınmış faktlar da cəlb edilmişdir. Araşdırma nəticəsində müəyyən edilmişdir ki, Azərbaycan sosio-mədəni mühitində milli mentalitet və stereotiplərdən qaynaqlanan fərdi məlumatlara həssaslıq sosial nəzarət və təzyiqin azaldığı virtual mühitdə daha çox ironiya predmetinə çevrilmişdir. Bu da virtual mühitdə özünəməxsus folklor təzahürlərinin meydana çıxmasına səbəb olmuşdur.

Açar sözləri— milli mentalitet, stereotiplər, fərdi məlumatlar, informasiya təhlükəsizliyi, internet folkloru, ənənəvi folklor

I. GİRİŞ

Problemin aktuallığı. Fərdi məlumatların təhlükəsizliyi məsələsi müasir dövrün, xüsusilə də qloballaşma və virtualaşma proseslərinin gətirdiyi, informasiya-kommunikasiya texnologiyalarının sürətlə genişləndiyi çağın ən aktual problemlərindədir. Rəqəmsal kommunikasiya texnologiyalarında sürətlə qeydə alınan fərdi məlumatlar dövlətlərarası münasibətlərdən tutmuş, cəmiyyətin ən kiçik fərdlərinə qədər sosial gərginlik və konfliktlərin predmeti ola bilmək potensialındadır. Beynəlxalq hüquq və milli mentalitet, adət-ənənə və mədəni dəyərlər, dini qayda və qanunlarla şərtlənən fərdi məlumatlar cari və strateji maraqlar, ictimai status və nüfuz və s. baxımından mühüm əhəmiyyət kəsb edir. Odur ki, global informasiya təhlükəsizliyi kontekstində fərdi məlumatların qorunması məsələsi bir tərəfdən texnoloji, digər tərəfdən sosial-mədəni, bütövlükdə isə, *sosiotexnoji və kulturoloji* problemdir və özünə münasibətdə multidissiplinar yanaşma tələb edir.

Məsələnin qoyuluşu. Folklor milli mədəniyyətin tərkib hissəsi kimi özündə milli mentalitet və stereotipləri yaşatmaqdadır. Daha dəqiq ifadə etsək, milli mentalitet və stereotiplər cəmiyyətdə qarşılıqlı münasibətlər zəminində ortaya çıxan, təkrar-təkrar istifadə olunmaqla sabitləşən, “basmaqəlib” düşüncə və önyarğılar sistemidir ki, onun izlərini ən müxtəlif formalarda, eləcə də folklorlarda müşahidə edə

bilərik. Azərbaycan sosio-mədəni mühiti özünün etno-genetik tipologiyası və tarixi inkişaf dinamikası baxımından bir tərəfdən ümumtürk mədəni ənənələri, digər tərəfdən isə ümumşərq və müsəlman dəyərləri ilə sıx bağlıdır. Bununla əlqədar olaraq, Azərbaycan milli mentaliteti və stereotipləri özündə həm ümumtürk, həm də ümummüsəlman dəyər və yanaşmalarını yaşatmaqdadır. Lakin “folklorun simvolik dilini və metaforik təbiətini formalaşdıran psixoloji və sosioloji şərtlər” (6: 73) zaman-zaman dəyişdiyi üçün folklorlarda meydana çıxan stereotiplərin də məzmunu, mahiyyəti və hədəfi dəyişir. Təsədüfi deyildir ki, ənənəvi folklorun yarandığı, söyləndiyi və variantlaşdığı mühitin psixososial şərtləri ilə virtual folklorunka biri-birindən fərqlənir. Bu fərqləri fərdi məlumatlara həssaslıqla bağlı olan stereotiplərin folklorik təzahürlərində də müşahidə etmək mümkündür.

II. ƏNƏNƏVİ FOLKLORDA FƏRDİ MƏLUMATLAR: MİLLİ MENTALİTET VƏ STEREOTİPLƏR

Metodoloji olaraq bir məsələni vurğulamaq vacibdir ki, folklorlarda fərdi məlumat anlayışı fərdin özü barədə təsəvvürləri kimi deyil, kollektivin fərd haqqında ümumiləşmiş baxışları – stereotipik münasibəti olaraq dərk olunur. Biz də tədqiqat zamanı fərdi məlumatların təhlükəsizliyi məsələsinə, fərddən fərdə baxış kontekstində deyil, folklorun təbiətinə müvafiq olaraq, kollektivin fərdə münasibəti əsasında yanaşmışıq. Çünki folklorla ifadə olunan stereotiplər, əslində, gerçəkliyin özündən daha çox, onun haqqında olan fantaziyalardan ibarətdir. Bir qrupun başqa bir qrup və müəyyən bir fərd haqqında sabitləşmiş düşüncə və fikri, hazırqəlib (basmaqəlib) baxış və adlandırma şəklinə özünü göstərən stereotiplər (4; 3; 8) sosial mühitdə davranış və münasibətlərin nizamlanmasında mühüm təsirə malikdir. İstər üz-üzə, istərsə də virtual kommunikativ mühitdə fərdlərarası və qruplararası münasibətlərin qurulmasında, daha sürətli integrasiya prosesinin getməsində, eləcə də qarşıdurma və toqquşmaların meydana çıxmasında stereotiplərin rolu vardır. Kişilərin qadınlar, qadınların kişilər, müəyyən peşə sahiblərinin digər peşə sahibləri barədə stereotipik təsəvvürləri, əslində, obyektin özünün yox, o təsəvvürü istehsal edən subyektin münasibətinin ifadəsidir.

Əgər biz ənənəvi xalq mədəniyyətində fərdi məlumat anlayışına nəzər yetirsək görərik ki, burada məlumat anlayışı daha çox *“söz”* kimi dərk olunur. Söz haqqında olan linqvopetik təsəvvürlər isə, onu hərəkətdə, dinamikada olan

varlıq kimi qavrayır. Faktlara diqqət yetirək: “Söz tez yayılır” (16: 366), “Sözün ayağı yoxdur, amma gəzir hər yanı” (12: 367), “Sözün qanadı var” (12: 367), “Sözün qədəmi yeyin olar” (12: 367), “Sözün damarı olar, çəkdikə uzanar” (12: 367), “Söz quşdu, buraxarsan, uçar gedər” (12: 366), “Sözdən söz çıxar, ocaqdan köz” (12: 367).

Sözün hərəkətdə olan varlıq kimi dərk olunması, fərdi məlumatların, şəxsə, ailəyə, tayfaya, müəyyən peşə və ya sənətə dair biliyin yayılması təhlükəsinə olan həssaslığı ifadə edir. Mədəniyyət özü-özünü təşkil edən sistem kimi bir tərəfdən fərdi məlumatın, müəyyən biliyin, sirrin yayılması təhlükəsini “hiss edərək” onu qorumağı tələq edir, digər tərəfdən isə, gizili bilik və məlumatı əldə etməyi, ona olan marağı da özündə ehtiva edir. Çünki folklorda eyni zamanda informasiyanın konfidensiallığını aradan qaldıran, tabu və normaları pozan yanaşma və baxışlar da vardır. Çünki mədəniyyət həm vetolaşdırın, həm də sanksiyalaşdırın sistem kimi özünü göstərir. Gizli informasiya və ya bilik qarı, dəriş, xtonik varlıqlar, liminal obrazlar tərəfindən, eləcə də müəyyən psixofizioloji hallar – dəlilik, axmaqlıq, sərxoşluq və s. vasitəsilə əldə olunur və ya yayılır. Mədəniyyət hər iki mövqe üçün çıxış yolu təqdim edir. Dədə Qorqud, Molla Nəsrəddin – müdrik, ağsaqqal, trikster-axmaq kimi həm norma yaradan, həm də normanı pozan obrazlar kimi özünü göstərir.

Bu baxımdan yanaşdıqda ənənəvi xalq mədəniyyətində fərdi məlumatlara həssaslıqdan doğan, həm onu qorumaq, həm də yaymaqla bağlı kollektiv rəyləri fərqləndirə bilərik:

Ənənədə fərdi məlumatların təhlükəsizliyinə həssaslıqdan doğan deyimlər: “Bir daş altıda bir daş üstə”, “Yerin də qulağı var”, “Söz ki ağızdan çıxdı sənəin deyil”, “Söz var el içində, söz var ev içində” (12: 366), “Ev bizim, sirr bizim” (12: 126).

Fərdi məlumatın təhlükəsizliyinə olan həssaslıq folklorda **sirr** anlayışının meydana çıxmasına səbəb olmuşdur. Bu sözün Azərbaycan dilinin izahlı lüğətindəki mənası belədir: 1) Başqalarından gizli saxlanılan, başqalarına bildirilməyən, deyilməyən, hamının bilməli olmadığı söz, iş və s; 2) Hələ açılmamış, dərk edilməmiş, öyrənilməmiş bir müəmma kimi qalmış şey (9: 127). Folklordakı sirr anlayışı məhz birinci mənada istifadə olunur. Təbii ki, sirr kimi qırflənən informasiya özündə cari və ya strateji mənə ifadə edən biliyi ehtiva edir. Bu da, sosial münasibətlərdə, davranış və inanclarda müəyyən sərhəddə və distansiyaların yaradılmasına xidmət edir. Sirr anlayışı ilə bağlı dilimizdəki faktlara nəzər yetirək, burada cari və strateji maraqlara xidmət edən, inanc və sakral dəyərlərlə qorunan, bütövlükdə isə, mentalitetlə bağlı olan məqamlara rast gələ bilərik. V.Haqverdiyev sirlə bağlı faktları və onların kəsb etdiyi mənalara aşağıdakı kimi qeyd edir: “Sirrivi vermə yaruva, yaruvin da yarı var”, “Hər gördüyünü dost sanıb sirrini açma”, “Düşməyə sirr, dostu yalan söyləmə”, “Ev bizim, sirr bizim”, “Nə dil bilsin, nə dodaq” kəlamları sirr saxlamaq üçün onu heç kimə etibar etməməyi məsləhət görür, çünki “Sirr, ikinin arasında qalar, üçə keçdi, qapını açar”. Digər ifadələr isə: “Özgənin sözünü özgənin evində danışma”, “Sirr açandan el qaçar”, “Özgənin sözünü özgəyə deməyə nə var?” göstərir ki, bildiyin sirri

açmaq ən asan iş olsa da o, adamı gözdən salır, belə adamlara hər yerdə hörmət edilmir” (2: 10). Göründüyü kimi, ənənəvi xalq mədəniyyətində sirri saxlamaq, onu qorumaq ciddi şəkildə təbliğ olunmaqla bərabər, sirri açmaq da neqativ davranış kimi qiymətləndirilir. Yeri gəlmişkən onu deyək ki, qrup idioskulturasının formalaşmasında, qrupa məxsus informasiya və davranışlarının möhkəmlənməsində sirr saxlama mühüm rola malikdir.

Ənənədə fərdi məlumatları qorumaqla bağlı stereotip adlandırmalar və təbliğatlar: “Sənəsi qəbiristanlıq”, “ağzibütöv”, “ağzibərk”, “kişi gördüyün deməz”, “kişinin hülqumu olar”, “kişinin yanında baş kəsərlər” və s.

Ənənədə fərdi məlumatı yaymaqla bağlı stereotip adlandırmalar: “ağziboş”, “arvadağız”, “hülqumsuz”, “küpəgiran qarı”, “söz gəzdiren”, “simsiz teleqraf”, “qeybət edən arvad”, casus və s.

Bundan əlavə ənənədə fərdi məlumatı yaymağın forması ilə bağlı kommunikativ aktlar mövcuddur: “pıça-pıç”, “dedi-qodu”, “qeybət” və s.

Göründüyü kimi, Azərbaycan sosio-mədəni mühitində fərdi məlumatlar folklorda, ənənəvi xalq mədəniyyəti və etnoqrafik yaddaşda stereotiplərlə hərəkətə gətirilən və yaşıdılan, qruplararası münasibətlərin qurulması və tənzimlənməsində mühüm rol oynayan faktorlardan biri kimi çıxış edir.

Hazır nümunə, sabitləşmiş baxış, öncədən müəyyənlanmış rəy kimi özünü göstərən stereotiplər adət-ənənə, dini ehkam və qadağalarla çulğalasaaraq ictimai münasibətlərdə dərin sosial gərginliklərin və konfliktlərin yaranmasına da təkan verir.

“Kitabi-Dədə Qorqud” eposunun “Bəkil oğlu İmran” boyunda ov vaxtı atdan yıxılan Bəkilin ayağı sındığı üçün beş gün divana çıxmır. Lakin bir gün xatunu ondan bunun səbəbini soruşduqda Bəkil sirrini deyir. Arvadı “əlın əlinə çaldı, qaravaşa söylədi. Qaravaş çıxub qapucıya söylədi. Otuz iki dişdən çıxan bütün orduya yayıldı, “Bəkil atdan düşmüş, ayağı sınımış” deyü” (5: 138). Kişilik idioskulturası əsasında yaradılan və qadının daha çox neqativ plana yerləşdirildiyi “Kitabi-Dədə Qorqud” eposunda Bəkilin sağlamlığı ilə bağlı strateji informasiya məhz onun xatunu tərəfindən yayılır. Eposda “Otuz iki dişdən çıxan” fərdi məlumat qadının neqativ planda təqdim edilməsi fonunda mənfi davranış kimi əsaslandırılır.

Milli mentalitet və stereotiplərin təzyiqi kontekstində **klassik ədəbiyyata** müraciət etsək, görürük ki, Qeysi Məcnun edən öz dövrünün adət-ənənələrinə, mental və dini qaydalarına riayət etməmək olmuşdur. Məcnunluq, əslində Şərq-müsəlman mühitində sərt dini qayda-qanunların təzyiqi altında yığılan potensial enerjinin mədəni yaradıcılıq platformasında özünə tapdığı çıxış yolunun təzahürüdür. Kənardan cünunluq kimi görünən davranışın batinində sosial norma və prinsiplərə, stereotiplər və mentalitetdən enerji alan ehkamlara kəskin protest mövcuddur. Q.Quliyev yazır ki, “...Füzulinin Qeysinin son nəticə etibarı ilə dəli-divanəyə çevrilməsinin, biyabanlara düşməsinin dəruni səbəbi antihumanist adət-ənənələrdə, qayda-qanunlardadır” (7:146).

Həmçinin Azərbaycan kino sənətinin ən dəyərli incilərindən olan **“Arşın mal alan”** filmində qaldırılan problem məhz gənc tacir Əsgər bəyin evlənmək fikrinə düşməsi zəminində qızı toydan öncə görmək, sevmək istəyidir ki, dövrün qaydaları, yəni milli mentalitet və stereotiplər buna imkan vermir. Dostu Süleyman bəy ona “arşın malçı” cildinə girməyi tövsiyə edir. Yadımıza folklorda “təğyiri-libas olma” ilə bağlı faktları salaq. Tacir Əsgər də “təğyiri-libas” olmaqla, yəni “arşın malçı” cildinə girməklə fərdi məlumatlara giriş üçün “viza” alır. Nağıllarda məhz qarı obrazları özünün yaşlılığı və ağbırçəkliyindən istifadə edərək qalada olan şahzadəni görməyə və aldatmağa nail olur. Mədəniyyətdə ağsaqqallıq və ağbırçəkliyin kəsb etdiyi mənə ona fərdi məlumatlara çıxış imkanı yarada bilmişdir.

Beləliklə, ənənəvi folklor mühiti və münasibətləri kontekstində fərdi məlumatlara olan həssaslığın əsasında milli mentalitet və stereotiplərdən qaynaqlanan sosial nəzarət və təzyiq dayanır. İstər folklor nümunələrində, istər etnoqrafik yaddaş faktlarında, istərsə də yazılı ədəbi əsərlərdə ictimai nəzarət və təzyiqin hərəkətverici mənbəyi olan stereotiplər eyni zamanda fərdi məlumatların – şəxsə, ailəyə, qrupa və s.-yə aid informasiyaların da qorunması və təhlükəsizliyinin təmin edilməsi baxımından mühüm rola malikdir.

III. İNFORMASIYA CƏMİYYƏTİ KONTEKSTİNDƏ FƏRDİ MƏLUMATLARA MÜNASİBƏT: FOLKLORİK REAKSIYA

Qeyd etdiyimiz kimi, Azərbaycan sosio-mədəni mühiti özünün genezisi etibarını ilə bir tərəfdən türk etnik-mədəni dəyərlərinə, digər tərəfdən isə islam dini prinsiplərinə əsaslanır. Şübhəsiz ki, burada ənənə və yaddaş hesabına möhkəmlənən, sosial stereotip və psixoloji gerçəkliklə korelyasiya olunan davranışlar mövcuddur. Sosial stereotiplərin və milli mentalitetin təzyiqi altında daim aktual qalan müəyyən davranışlar vardır ki, bunların kökü psixoloji kompleks və narahatlıqlardan qaynaqlanır. Məsələn, oğulun atanın yanında övladını qucağına alması və ya atanın qarşısında uzanaraq yatması Azərbaycan mühitində tərbiyəsizlik, böyüyə hörmətsizlik kimi dəyərləndirilir. Həmçinin süfrə ətrafında yaşlıların, valideynlərin olduğu şəraitdə gənclərin uca səslə danışması cəmiyyətimizdə qeyri-etik davranışlar kimi qiymətləndirilir. Yaxud Azərbaycan mühitində ev tikən şəxs evin pəncərələrini elə yerləşdirməlidir ki, qonşunun həyatını görməsin. Həmçinin ev tikilərkən ən mühüm şərtlərdən biri onun üzünün Qibləyə tərəf olmasıdır¹. Bu, bir yandan dini

məzmun kəsb edərsə, digər tərəfdən də ekoloji əhəmiyyətə malikdir. Yaxud kənd yerlərində evlərin hasarlanması², bəzən həmin hasarların hündürlüyünün həddindən artıq çox yüksək olması da fərdi məlumatlar silsiləsinə daxil olan ailə həyatının (daha çox həyat yoldaşı və qızların) gizlədilməsi, qorunması anlamını ifadə edir. Göründüyü kimi, Azərbaycan etnoqrafik gerçəkliyində insanın yaşayışı üçün zəruri olan evin tikilmə qaydası, digər faktorlarla yanaşı folklorik davranışlarla – milli mentalitet və stereotiplərlə tənzimlənir. Etnoqrafik təsvirlərdən məlum olur ki, “Naxçıvan bölgəsində qapı (darvaza) üzərinə bərkidilmiş taqılbaqla evin kişisi, zəndulbaba evin xanımı çağırılardı” (15: 38). Naxçıvanın “El həyatı” qəzetinin 26 may 2019-cu il sayında bu məlumat aşağıdakı kimi əks olunmuşdur: “Qədimdən Ordubadda həyat qapılarının üzərinə iki balaca dəzgah vurulardı. Onlardan ev sahibini qapıya çağırmaq üçün istifadə edilərdi. Dəmirəndən düzəldilən bu dəzgahlardan biri uzun olduğuna görə taqılbaqla, o biri isə aypara və ya ürək şəklində olduğundan “Zəncirbab” adlanardı. “Taqılbaqla” döyəndə qapıya kişi çıxar, “Zəncirbab” səsinə isə qadınlar səs verərdi” (10). Göründüyü kimi, fərdi məlumatlara olan həssaslığın səviyyəsi müəyyən dövrlərdə səs informasiyasının kəsb etdiyi mənanın fərqləndirilməsi ilə də işarələnmişdir. Məsələn dini adətlərinin izi kimi özünü göstərən bu faktın mahiyyətində qadın və kişi qrupunun fərqləndirilməsi özünü göstərir. Naməhrəmlə təhlükəsi kontekstində icra olunan bu davranış milli mentalitetdə fərdi, şəxsi həyatın çox ciddi şəkildə qorunduğunu sübut edir. Bu tipli məsələlər gündəlik məişət həyatı ilə bağlı olan etnoqrafik faktlarda geniş şəkildə öz əksini tapmışdır.

Milli mentalitet və stereotiplərlə tənzimlənən ənənəvi sosial mühitlər – kənd, qəsəbə, müəyyən dövrlərdə isə şəhər (məhəllələr qismində) həyatı üçün daha çox aktual olan yuxarıdakı adət və ənənələr kommunikasiya imkanlarının genişlənməsi, şəhərləşmə və sənayeləşmə prosesləri kontekstində öz təsir gücünü itirməkdədir. Çünki kommunikasiya imkanlarının məhdudluğu, təhsil, dünyagörüş və savadlılığın aşağı səviyyədə olduğu şəraitdə və topluslarda sosial münasibətlərin əsas tənzimləyicisi adət və ənənələr, mentalitet və stereotiplər idi. Ağsaqqal və ağbırçəkəlin, atalar sözü və məsələnin, inanc və yasaqların hakim ideoloji konsept kimi çıxış etdiyi qapalı mühitlərdə, təbii ki, stereotiplərin basqısı daha kəskin olmuşdur. Kommunikasiya imkanlarının genişlənməsi, urbanizasiya və sənayeləşmə proseslərinin sürətlənməsi, elmi-texnoloji sferadakı yeniliklər sosisumları qapalılıqdan azad edir.

Şübhəsiz ki, sənayeləşmə və şəhərləşmə proseslərinin təsiri, informasiya-kommunikasiya texnologiyalarının meydana çıxması və s. kimi faktorlar sosisumun həyat tərzinə, dünya görüşünə, qarşılıqlı münasibətlərinə, adət-ənənələrinə öz təsirini göstərir. Lakin unutmamaq olmur ki, yaşayış məskəninə, sosial-mədəni proseslərin xarakterindən, ictimai quruluşun spesifikasiyasından, əmək və istehsalat proseslərinin

¹ “Azərbaycanda şəhər tipli yaşayış məskənlərinin əsas xarakterik xüsusiyyətlərindən biri onlarda evlərin fasadının həyatə tərəf istiqamətləndirilməsidir. Ailə məişətinin spesifikasiyası ilə bağlı olan belə planlaşdırma keçmişdə bütün müsəlman Şərqiində mövcud idi. Lakin sonralar bu cəhətlər aradan qaldırılmış, şəhər tipli yaşayış məskənlərinin inkişafında yeni memarlıq elementləri (küçəyə açılan pəncərə və eyvanlar, milli ornamentlərlə bəzədilmiş və taqılbaqlar qoyulmuş geniş darvaza və alaqaqlar və s.) meydana gəlmişdir” (11: 26). Həmçinin elə həmin oçerkdə qeyd olunur ki, “Evlərin küçəyə baxan arxa divarlarında pəncərə açırımlarının qoyulmaması son dövrlərə qədər Şərqi ölkələrində mövcud olmuş *ev məişətinin və ailənin həyat tərzinin yad nəzərlərdən mühafizə edilməsi (kursiv bizimdir – H.Q.)*, habelə küçənin tozlu havasının evin otaqlarına dolmasının qarşısının alınması mülahizəsi ilə izah olunur” (11: 33).

² “Kəndli həyatlarını xarici mühitdən təcrid etmək, Şərqi adətincə onun qapalılığını təmin etmək və ümumi kompozisiyanı tamamlamaq üçün Azərbaycanın bütün bölgələrində həyatların ətrafına hasar (barı, çəpər) çəkilirdi” (11: 34)

səciyyəsi, harada və necə yaşamasından asılı olmayaraq, kommunikativ mühitdə olan fərdlər və ya qruplar özləri və başqaları, eləcə də başqalarının onlar haqqında düşündükləri barədə fantaziyalara, əvvəlcədən hazır düşüncələrə, önyargı və mühakimələrə, daha dəqiq desək, stereotiplərə sahibdirlər. Nəzərə alsaq ki, stereotiplər təkcə şüurlu şəkildə deyil, eyni zamanda kollektiv şüursuzluq faktı kimi də özünü göstərir, o halda virtual kommunikativ mühitə qədəm qoyan, orada özünə məskən salan, virtual dünyasını və ənənələrini formalaşdıran yeni insan nəslinin də özünəməxsus stereotipləri və dəyərləri mövcuddur deyə bilərik. Xüsusən də fərdi məlumatlara, şəxsi həyat və mənəvi məsələlərlə bağlı olan informasiyalara münasibətdə milli mentalitet və stereotiplərdən qaynaqlanan reaksiyaların spesifikasiyası çox mühüm əhəmiyyət kəsb edir.

Milli mentalitet və stereotiplərin təzyiqi kontekstində fərdi məlumatların qorunması məsələsi İKT-nin meydana gəlməsi şəraitində tamamilə fərqli mədəni təzahürlər doğurmuşdur. Belə ki, bir tərəfdən milli mentalitet və stereotiplərin basqısı, digər tərəfdən isə Internetin təqdim etdiyi geniş imkanlar fərdi məlumatların təhlükəsizliyi üçün ziddiyyətli bir situasiyanın ortaya çıxmasına səbəb olmuşdur. Fərdi məlumatların təhlükəsizliyi ilə bağlı müəyyən normativ-hüquqi sənədlər mövcud olsa da, bu sahədə məsələ həm də milli mentalitetlə sıx bağlıdır. Akademik R.Əliquliyev fərdi məlumatların milli mentalitetlə bağlılığı barədə yazır ki, “Fərdi məlumatlardan istifadə ilə bağlı hüquqi məhdudiyyətlərə baxmayaraq, onlardan qeyri-qanuni biznes və kriminal məqsədlərlə istifadəyə olan tələbat bu sahənin “qara bazarı”nın formalaşmasına rəvac verir. Beləliklə, fərdi məlumatlar həm də kriminalistikanın predmetinə çevrilir.

Fərdi məlumatların virtual mühitdə dövr etməsi bu kateqoriyadan olan məlumatların yalnız milli qanunvericilik çərçivəsində qorunmasının artıq qeyri-mümkün olmasına gətirib çıxardır. Bu da fərdi məlumatlarla bağlı ictimai münasibətlərin global miqyasda, beynəlxalq hüquq çərçivəsində həllini tələb edir. Lakin beynəlxalq miqyasda tərəflər arasında konsensusun əldə edilməsi o qədər də asan məsələ deyil. Çünki “şəxsi həyat” normaları, adət-ənənələri, “fərdi məlumat” anlayışları müxtəlif milli mentalitetlərdə fərqli şəkildə anlaşılır. Müvafiq beynəlxalq hüquqi prinsip və standartlar isə milli adət-ənənələri, mental dəyərləri nəzərə almır.

Bu sahədəki problemlər həm də sosial-iqtisadi, psixoloji, kulturoloji və s. aspektli olduğu üçün məsələnin həlli multidissiplinar yanaşma tələb edir (1: 118). Göründüyü kimi, alim haqlı olaraq, fərdi məlumatların təhlükəsizliyi məsələsində beynəlxalq hüquq və normalarla tənzimlənməyən milli mentalitet məsələsini irəli sürür. Qeyd edir ki, hər bir milli mühitdə fərdi məlumatlara həssaslıq spesifik xarakter daşıyır. Azərbaycan sosio-mədəni mühiti mahiyyəti etibarilə konservativ xarakterə malik olduğu üçün burada fərdi məlumatlara həssaslıq səviyyəsi (milli mentalitet və stereotiplərin təzyiqi hesabına) daha kəskin şəkildə özünü göstərir. Belə ki, *şəxsi, fərdi həyatdan tutmuş, ailə, övlad, qohum-əqraba, var-dövlət, mal-mülk, eləcə də istirahət və əyləncəyə* qədər olan hər bir məlumat milli mühitdə strateji mənə kəsb edir. Müəyyən bir ehtiyatsızlıq və diqqətsizlik

həmin məlumatların ictimailəşməsinə, son nəticədə sosial, siyasi, iqtisadi, hətta psixoloji problemlərin də ortaya çıxmasına gətirə bilər. Belə bir şəraitdə *Azərbaycan sosio-mədəni mühitində Internet təkcə əlçatan, asan kommunikasiya vasitəsi deyil, daha çox sosial təzyiq və ictimai qınağın “buxovundan” xilas olmaq üçün çıxış yoludur.* Xüsusən də anonimlik, gizlilik, “fake profile” və “nickname”-lər hesabına şəxsiyyətin gizlədilməsi, başqa ad və ya ləqəblərdən istifadə etmənin mümkünlüyü, sosial şəbəkə hesablarının parol və kodlarla qorunması, yüksək təhlükəsizlik imkanlarının mövcudluğu Interneti milli mentalitet və stereotiplərin təzyiqindən xilas olmaq üçün “oasis”-ə çevirmişdir. Əslində, *şəxsiyyətini (özünü) gizlətmə və bundan doğan mədəni təzahürlərin arxasında sosial stereotiplər və milli mentalitetdən qaynaqlanan, eləcə də psixoloji kompleks və narahatlıqlarla korelyasiya olunan gizli ehtiyaclar dayanır.*

Lakin İKT-nin inkişafı, sosial şəbəkə və platformaların meydana gəlməsi geniş imkanlarla bərabər (kommunikasiya əlçatandır, ünsiyyət və münasibət üçün ən müxtəlif platformalar mövcuddur, özünüifadə etmək, duyğu və hislərini, qayğı və narahatlıqlarını paylaşmaq üçün geniş imkanlar vardır), **təhlükə və təhdidlərin** (lakin bütün məlumatlar, hərəkət və davranışlar, status və kommentlər, yazışma və danışqlar fasiləsiz olaraq qeydə alınır, məhrəm, pünhan məsələlərin üzə çıxarılması, ictimailəşdirilməsi üçün də potensial təhlükələr meydana gəlir, xüsusən də *şantaj, şəər, böhtan, yalan, hədə-qorxu* və s. tipli narahatlıqlar yarada biləcək situasiyalar mövcuddur) **də meydana çıxmasına səbəb olmuşdur.**

Təbii ki, hazırki dövrdə hər bir mobil telefon, planşet, kompüterlər şəxsi əşya kimi müəyyən bir fərdə aiddir. Hər bir şəxs özünəməxsus olan gerçəkliyi, dünyanı həmin rəqəmsal vasitələrdə yaradır, inşa edir. Fərdi rəqəmsal vasitələrin foto və video qalereyadan tutmuş, Watsap, Instagram, Facebook və s. hesablarda olan şəxsi məlumatlara, yazışma və danışqlara qədər hər bir detal müasir dövrdə istənilən şəxsin Profilini, CV-sini, ənənəvi şəkildə desək, şəxsi işini bərpa etməyə imkan verir. Odur ki, rəqəmsal ünsiyyət vasitəsi, sosial şəbəkə platformaları hər bir şəxsə məxsus parol və ya kodlarla qorunur.

Sosial media platformalarında, sosial şəbəkə və forumlarda fərdi məlumatların qorunması zərurəti kontekstində meydana gələn çoxlu sayda folklorik faktlar və rəylər mövcuddur. Belə ki, telefon, planşet, kompüter və s. kimi texnoloji avadanlıqlarda gündəlik yaşamdan formalaşan “data”-lar mövcuddur ki, onların bir qismi həssaslıq tələb edən “məhrəm”, “fərdi”, “personal”, “gizli” informasiyalardır. WhatsApp, Instagram, Messenger, Facebook, Twitter və s. sosial media platformalarında gündəlik kommunikasiya və təmasdan yeni tanışlıqlar, münasibət və sosiallaşmalar meydana çıxır. Elə sosial şəbəkələrin yaradılmasındakı ilkin məqsəd və təkan da gənclərin ünsiyyət qurması, yeni tanışlıqlar əldə etməsi, yeniyyətlərin özünüifadə və özünüdəstəqlənmə imkanlarının yaradılması idi. Çünki şəhərləşmə və müasir infrastrukturadan irəli gələn maskunlaşma forması – yüksək mərtəbəli binalar, hər cür kollektivləşmə və sosiallaşmanın

qarşısını alan həyat tərzı və s. fərdiliyə, tənhalığa səbəb olur ki, şəhər həyatının, böyük meqapolislərin ən mühüm problemlərindən biri də sosiallaşma və kollektivləşmə, iç-içə yaşam şərtlərindən məhrum olmasıdır. Belə bir şəraitdə virtual kommunikatıv mühitlər, sosial şəbəkə və platformalar yeniyetmə və gənclərin əsas görüş yerinə çevrilir. Artıq ünsiyyət və təmas, tanışlıq və münasibət heç bir maneə və sərhəddə olmadan, hətta psixoloji barierlərin aradan qalxması şəraitində baş verir ki, bu da İnternet istifadəçiləri üçün əlahiddə imkanların yaranmasına, heç bir məkanda olmadıqları qədər sərbəstlik əldə etməsinə gətirib çıxarır. Anonimlik, ictimai nəzarətsizlik və normativ-hüquqi boşluğun sosial şəbəkə iştirakçıları və ya istifadəçiləri üçün yaratdığı əlverişli mühit ifrat sərbəstliyə yola açır ki, bu da bəzən təhlükə cə təhdid yaradacaq “izlərin” ortaya çıxmasına səbəb olur. Müxtəlif şərt və səbəblərdən asılı olaraq, həmin informasiyaların qorunması zərurəti ortaya çıxır. Virtual sosial şəbəkələrdə məhz həmin həssaslıq tələb edən informasiyaların üzə çıxarılması, aşkarlanması, başqaları tərəfindən ələ keçirilməsi ehtimalı və qorxusundan doğan xeyli folklor faktları mövcuddur.

Nümunələrə diqqət yetirək:

Azərbaycandilli virtual mühitdə geniş populyarlıq qazanmış Albert Eynşteyn obrazı (rəsmi) fonunda təqdim olunan bu folklorik fakt – “*Burdan ən yaxın dosduma vəsiyyət eliyirəm. Əgər ölsəm telefonumu yox elə*”, əslində sosial şəbəkələrdə geniş yayılmış və variantlaşmış kollektiv rəyin təqdimat formalarından biridir. Virtual sosial şəbəkə istifadəçilərinin hər birinin yaşadığı emosianın folklorik modeldə ifası kimi ortaya çıxan bu fakt fərdi məlumatlara həssaslıqdan doğan, daha doğrusu, milli mentalitet və stereotiplərin təzyiqi altında meydana çıxan narahatlığın ifasıdır. Təbii ki, komik və ironik üslubun da semantik baxımdan mühüm rolu vardır.

Yaxud başqa bir nümunədə təsvir olunur ki, “Kişi xəstələnir və deyir: arvad təcili yardım çağır, ölürəm. Arvad deyir ki, telefonun kodunu de zəng edim. Kişi baxır ki, vəziyyət pisdır dərhal deyir: ehtiyac yoxdur, ölüm haqdır”. Deməli, fərdi məlumatlara olan həssaslıq yaradıcılıqda ölümlə müqayisə edilmək potensialındadır.

Digər bir nümunədə isə ər və arvad münasibətləri fərdi məlumatların təhlükəsizliyi kontekstində diqqət mərkəzinə gətirilir:

Instagram sosial şəbəkəsində “xanımların.mekani” hesabından yayılan bu faktda – “telefonu evdə parolsuz unudub işə gedən bir kişiye yoldaşı axşam üçün tort hazırlayıb – Allah

rəhmət eləsin!” yenə də rəqəmsal ünsiyyət vasitəsində toplanan informasiyaların – fərdi məlumatların yaratdığı konflikt, dramatik situasiya təsvir olunur.

Whatsapp-da geniş populyarlıq qazanmış aşağıdakı nümunə isə fərdi məlumata həssaslığın ən yüksək mübaliğə şəklində ifasıdır ki, düşüncənin metaforikliyi baxımından xüsusilə diqqəti cəlb edir.

Fərdi məlumata həssaslıqdan doğan münasibətin ən dramatik şəkildə ifası kimi özünü göstərən bu nümunədə telefonu yaddan çıxan kişinin tabutdan belə durub geri qayıtmağa cəhd etdiyi təsvir olunur.

Beləliklə, komik effekt yaradan, gülüş doğuran bu kimi folklorik faktlar, əslində, fərdi məlumat və şəxsi həyatla bağlı **həssaslığın dərəcəsinə** göstərir. Çünki milli mentalitet və sosial stereotiplərindən qaynaqlanan ictimai qınaq və sosial nəzarət fərdi daim basqı və təzyiq altında saxlamaqla psixoloji gərginlik yaradır. Belə bir stressiv vəziyyət, psixoloji gərginlik, yaradıcılıqda əks effektlə – gülüş, zarafat vasitəsilə təcəssüm olunma imkanı qazanır. Çünki gülüş, əslində ən kəskin ziddiyyət və gərginliyin, narahatlıq və həssaslığın psixoloji boşalma ilə təcəssüm olunan təzahürdür.

Eyni zamanda təhlil etdiyimiz faktlar onu deməyə əsas verir ki, ənənəvi mədəni mühitdə norma yaradıcı institusional subyektlər (ata, baba, ağsaqqal, ağbırçək və nənələr), adət və ənənələrlə dəstəklənən, daha doğrusu, təbliğ olunan stereotiplər virtual kommunikatıv mühitdə daha çox ironik və komik planda diqqət mərkəzinə gətirilir. Yuxarıda təhlil etdiyimiz hər bir folklorik fakt, əslində, milli mentalitet və stereotiplərin təzyiqi altında müəyyən çərçivə və qaydalara, norma və prinsiplərə tabe edilən insanın kollektiv emosional reaksiya kontekstində protestidir.

Beləliklə, İnternet mühitinin əsas istifadəçiləri və üzvləri yeniyetmə və gənclərdən təşkil olunduğu üçün, ideoloji olaraq ənənəvi folklorlarda fərdi məlumatlara həssaslıqdan dolayı meydana gələn faktlara münasibət fərqlidir. Bu mühitin iştirakçıları və yaradıcıları alternativ baxışın daşıyıcısı olduğu üçün milli mentalitet və stereotiplərin təsiri ilə fərdi məlumatlara olan həssaslıq daha çox ironik və komik planda özünü büruzə etdirir. Ənənəvi folklor mühitində yaşlıların (yaşlılığın) ideoloji və institusional təbliğat alətləri kimi çıxış edən folklor nümunələrində milli mentalitet və stereotiplər təbliğ olunduğu halda, İnternet mühitində gənclərin baxış bucağından – kollektiv emosional reaksiyasından doğan virtual folklor faktlarında stereotiplər inkar olunur. Bu proses şəxsi həyat və fərdi məlumatların təhlükəsizliyinə həssaslığa təhrik edən milli mentalitet və stereotiplərə münasibətdə özünü göstərir.

İSTİNADLAR

- [1] Əliquliyev R.M., Mahmudov R.Ş. Milli mentalitet kontekstində fərdi məlumatların həssaslığı və onların təhlükəsizliyinin təmin olunması məsələləri. İnformasiya cəmiyyəti problemləri, 2019, №2, 117–128.
- [2] Haqverdiyev V. Atalar sözlərinə informatik yanaşma. Azərbaycan qəzeti, 1 mart 2009, s. 10
- [3] İmançer, D. "Sosial psixoloji açıdan stereotip kavramının dil və metin analizində kullanımı". Selçuk İletişim 3 (2013), s. 128-142;
- [4] İmançer, D. "Stereotipleri anlamak". Ege Üniversitesi İletişim Fakültesi Yeni Düşünceler Hakemli E-Dergisi (2008), s. 301-320;
- [5] “Kitabi-Dədə Qorqud”. Əsli və sadələşdirilmiş mətnlər. Bakı: Öndər nəşriyyat, 2004, 376 s.
- [6] Qarayev S. Folklor vasitəsi ilə qrup və yaxud milli psixologiyanın öyrənilməsi. “Dədə Qorqud” elmi-ədəbi toplusu. Bakı: “Elm və təhsil”, 2018/2, s. 72-79,
- [7] Quliyev Q. Dəliddən doğru xəbər. Bakı: Mütərcim, 1999, 160 s.
- [8] Limon, S, Oral Kara, N, Antalyalı, Ö. Yönetim literatüründe stereotip (kalipyargi) kavramı: ulusal ve uluslararası alandaki yönetim araştırmaları üzerine bir inceleme. Süleyman Demirel Üniversitesi Vizyoner Dergisi, (2019). 10 (23) , s. 195-211.
- [9] Orucov Ə. Azərbaycan dilinin izahlı lüğəti. Dörd cildə. IV cild, Bakı: Şərq-Qərb, 2006, 712 s.
- [10] “Taqqılbab” və Zəncirbab” Ordubad qapılarının bəzəyidir. “El həyatı” qəzetinin 26 may 2019-cu il sayı. <https://nuhcixan.az/news/cemiyyet/15791-taqqilbab-ve-zencirbab-ordubad-qapilarinin-bezeyidir>
- [11] Vəliyev F. Xalq yaşayış məskənləri // Azərbaycan etnoqrafiyası. Üç cildə, II cild, Bakı: Şərq-Qərb, 2007, 384 s., s. 15-39.
- [12] Yaqubqızı M. Atalar sözləri (Tərt. ed: Yaqubqızı M.). Bakı: 2013, 476 s.

**THE FOLKLORIC APPEARANCE OF SENSITIVITY TO
PERSONAL INFORMATION IN THE CONTEXT OF
NATIONAL MENTALITY AND STEREOTYPES**

Hikmat Guliyev

ANAS Institute of Folklore, Baku, Azerbaijan

quliyevh@mail.ru

Abstract— The security of the personal information is one of the most urgent problems of modern times. Ensuring the security of the personal information in the present conditions, where the internet has become the main means of communication, is the problem connected not only with the technological, but also with the international law and national mentality. In the article the concept of the personal information is studied in the context of folklore, the folkloric manifestations formed and experienced by the influence of the national mentality and stereotypes are analyzed. Along with the traditional folklore examples, the facts noted from the virtual social networks are also involved in the investigation. As a result of the research, it is mentioned that sensitivity to the personal information caused by the national mentality and stereotypes in the socio-cultural environment of Azerbaijan has become more subject of irony in the virtual environment where the social control and pressure are reduced. And it causes the formation of the peculiar folklore manifestations in the virtual environment.

Key words— *the national mentality, stereotypes, the personal information, the information security, Internet folklore, the traditional folklore*

Fərdi məlumatların qorunması sahəsində beynəlxalq təcrübənin analizi

Fərhad Yusifov¹, Aysən Fərəcova²

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹ farhadyusifov@gmail.com, ² aysanpharajova@gmail.com

Xülasə – Məqalədə fərdi məlumatlar sahəsində beynəlxalq təcrübə araşdırılmışdır. Fərdi məlumatlar həssas informasiya kateqoriyasına aid edilir. Şəxsə məxsus olan məlumatların əldə edilməsi, emalı və istifadəsi onun icazəsi ilə olmalı və digər hallarda istifadəsi məhdudlaşdırılmalıdır. Beynəlxalq təcrübədə fərdi məlumatların qorunmasında istifadə olunan təhlükəsiz liman mexanizmi fərdə və ya qohumlarına, ailə üzvlərinə və s. aid olan həssas məlumatların silinməsinə tələb edir. Fərdi məlumatların təhlükəsizliyinin təmin olunması sahəsində innovativ mexanizmlər kimi Estoniyada tətbiq olunan Data səfirlik və Rusiyada fərdi məlumatların ölkə hədudlarından kənara çıxarılmaması istiqamətində görülən işlər və qəbul edilmiş qanunlar araşdırılmışdır.

Açar sözlər— fərdi məlumatlar, məlumatların təhlükəsizliyi, fərdi məlumatların qorunması, data səfirlik

I. GİRİŞ

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.

Övvəllər informasiya sistemlərində və arxivlərdə saxlanılan və az sayda insanın əldə edə biləcəyi bəzi fərdi məlumatlar günümüzdə texnologiyaların inkişaf etməsi vəsaiti 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 vacib bir mövzu halına gəlmişdir.

İnformasiya Kommunikasiya Texnologiyalarının (İKT) inkişafının vətəndaşların və ya şirkətlərin işində müsbət inkişafa səbəb olacağına əmin olunsun da, fərdi məlumatların nəzarətsiz dövriyyəsi şəxsi həyatın gizliliyinə 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 tətbiqi ola biləcək qanunsuzluqların qarşısını almaq üçün hüquqi tənzimləmələrə ehtiyac vardır. Fərdlərin özlərinə aid olan verilənlər "fərdi məlumatlar" adlanır. Bu məlumatlar təşkilatlar tərəfindən saxlanılır, işlənir və tələb olduqda isə üçüncü tərəflərə ötürülür.

Dövlət təşkilatları fərdi məlumat toplayıcılarıdır. 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.

Tədqiqat işində fərdi məlumatlar sahəsində beynəlxalq təcrübə analiz olunmuşdur. Ölkələrin təcrübəsində fərdi məlumatların saxlanılmasına, xaricə ötürülməsinə və bu proseslərin yerinə yetirilməsinə dair yanaşmalara baxılır, qəbul edilmiş qanunlar araşdırılır.

II. FƏRDİ MƏLUMATLARIN SAXLANILMASI

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 saxlanılmasını, onlara girişi və istifadəsini təmin etmək üçün hüquqi səviyyədə tənzimlənmiş qanunlar, müqavilələr və təhlükəsizlik infrastrukturlarından faydalanmaqla həyata keçirmək olar [1].

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 silinməsinə 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-ünvanlar, biometrik identifikatorlar, uzun tam fotosəkilləri və identifikasiyanın başqa unikal nömrəsi, xarakteristikası və ya kodu aiddir [2].

Bütün bu məlumatlar kompüter vəsaiti ilə ötürüldükdə həmişə çox zərərli bir yanaşma və təhlükə üçün asan bir mühit yarada bilər. Bu məlumatların köməyi ilə bəzi insanlar seçkilərdə verilən səsleri saxtalaşdıraraq, vergi borcunu silər, ölənlərin yerinə keçər, məlumatları dəyişər 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 gizliliyi pozula bilər.

Şəxs haqqında bədənyyətlinin əlində olan fərdi məlumatlar cinayət silahına, işdən çıxarılan işçinin əlində qisas vasitəsinə və ya rəqib şirkətə satılan mallara çevrilir. Buna görə fərdi məlumatların qorunması sahəsinə 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 zaman hər bir şəxsi düşündürən əsas məsələ fərdi məlumatların təhlükəsizliyinin nə dərəcədə təmin olunmasıdır. Əgər effektiv e-dövlət həllərindən söhbət gedirsə dövlət səviyyəsində qanunvericilik bazası ilə təkmilləşdirilməsi, fərdi məlumatların qorunması sisteminin işlənilməsi informasiya sızması ilə bağlı mövcud problemlərin aradan qaldırılmasına və fərdi məlumatların icazəsi ilə keçirilməsi, emalına qarşı güclü immunitetə malik vasitələr yaradılmasına imkan verir. Beynəlxalq təcrübədə fərdi məlumatların təhlükəsizliyinin təmin olunmasına dair müxtəlif yanaşmalar vardır.

III. FƏRDİ MƏLUMATLARIN QORUNMASI İLƏ BAĞLI BEYNƏLXALQ TƏCRÜBƏ

Avropa Birliyi – Avropa Birliyi dörd əsas ideyaya əsaslanır: əşyaların, şəxslərin, xidmətlərin və kapitalın sərbəst hərəkəti.

Fərdi məlumatların toplanması və işlənməsi bu dörd əsas məqsədin yerinə yetirilməsi üçün vacib olduğundan, Avropa Birliyində (AB) 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 qorunmadan əlavə baş verə biləcək hücumlara qarşı profilaktik tədbirlərin görülməsidir. Buna görə, fərdi məlumatların qorunması və potensial hücumların minimuma endirilməsi üçün hücumdan əvvəl sisteməlik qorunma təmin edilməlidir [5].

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 sadıqlıq: Məlumatların yalnızca 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: Məlumatın tarixi, statistik və ya elmi məqsədlər üçün işlənməsində məqsədəuyğunluq qəbul edilir. Bununla birlikdə özv ölkələr tərəfindən 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 Ştatları – ABŞ-da fərdi məlumatların qorunması üçün qüvvəyə minmiş ən vacib hüquqi tənzimləmələrdən biri olan 1974-cü il tarixli “gizlilik 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 Gizlilik Aktının 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 gizliliyini təmin etmək üçün qanunun müddələrinin effektiv şəkildə yerinə yetirilməsi və lazımı nəzarətin təmin edilməsi vacibdir.

1974-cü il tarixli Gizlilik Aktı, federal qurumlara, yuxarıda göstərilən prinsiplərə uyğunluğu təmin etmək üçün vətəndaşların fərdi məlumatlarının qorunması üçün zəruri təhlükəsizlik mexanizmini yaratmağı tövsiyyə edir. Fərdi məlumatların gizliliyinə dair müddəalar pozulduğu təqdirdə, qanun cəza müddələrinin tətbiq edilməsini tələb edir və bununla əlaqədar şəxs tərəfindən kompensasiya tələbi ilə iddia qaldırmaq da mümkündür [6].

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

Rusiyanın təhlükəsizlik qanunu mürəkkəbdir. Bir sıra Rusiya qanunlarının birləşməsi bütün sektorlar üzrə hərtərəfli gizliliyin qorunmasını təmin edir. Rusiya qanununun AB

təlimatı ilə bir çox oxşarlığı var. Ancaq qanunun icrası məhdud görünür. Rusiya APEC (Asia-Pacific Economic Cooperation) üzvüdür, lakin APEC Sərhədsiz Gizlilik Qaydaları sistemində CBPR (Community-based participatory research) iştirak etmir.

İnformasiya texnologiyaları və İnformasiyanın qorunması vətəndaşlara ‘unudulmaq hüququ’ verir və bəzi URL-ləri axtarış nəticələrindən çıxarmaq üçün istifadə edilə bilər. Əsas tənzimləyici Telekommunikasiya, İnformasiya Texnologiyaları və Kütləvi Rabitə Sahəsində Federal Nəzarət Xidmətidir (Roskomnadzor) [7].

Rusiyada məlumatların toplanması və işlənməsi üçün Roskomnadzor-da məlumat operatorları tərəfindən rəsmi qeydiyyat tələb olunur. Sadə, birdəfəlik məlumat toplama və insan resursları məlumatları üçün istisnalar var.

Bununla birlikdə, 2015-ci ilin sentyabrından etibarən məlumat operatorları Rusiya vətəndaşlarının fərdi məlumatlarının Rusiyada yerləşən serverlərdə saxlanmaları qanuni bir tələbdir. Roskomnadzor-a bu qanunun icrası tapşırılıb. Böyük xarici məlumat bazaları operatorlarına qanuna riayət etmək üçün əlavə vaxt verilib (2016-cı ilin əvvəlinə qədər). Qanun yalnız 2015-ci ilin sentyabrından sonra toplanmış və ya yenilənən məlumatlara şamil olunur.

Estoniya – 2018-ci ilin sonunda Estoniya parlamenti nəhayət yeni fərdi məlumatların qorunması qanununu qəbul etməyə müvəffəq oldu. Yeni Qanun 15 yanvar 2019-cu ildə qüvvəyə mindi; burada ümumi məlumatların qorunması qaydaları hazırlanmış və əlavə edilmişdir.

Son iyirmi ildə Estoniyanın inkişafının nəticəsi kimi Dünya Bankının tərtib etdiyi 2016-cı il üzrə “Dünya inkişaf hesabatı”nda ölkə “rəqəmsal cəmiyyətə ən yaxın” adlandırılmışdır [8]. Estoniya dünyada birinci Data səfirliyini Lüksemburqda açmışdır [9]. Bu o deməkdir ki, ölkədə məlumatların qorunması sahəsində tətbiq olunan bütün qaydalar onun “Data səfirliyi”ndə də tətbiq olunmalıdır. Qeyd edək ki, Lüksemburq dövləti Estoniyanın informasiya sisteminin verilənlərinin toxunulmazlığına zəmanət vermişdir. Lüksemburqda informasiya cəmiyyətinin yüksək səviyyədə inkişafı rəqəmsal xidmətlər sahəsində əməkdaşlıq üçün geniş imkanlara yaratmışdır.

Bu yeni yanaşma, Estoniya dövlətinin yerli məlumat mərkəzlərinin təbii fəlakət, geniş miqyaslı kibercümm, elektrik kəsilməsi və ya digər böhran vəziyyətinə görə dayandırıldığı və ya pozulduğu bir şəraitdə fəaliyyətini davam etdirməsinə imkan verir [4].

Data səfirliyi – Estoniya hökumətinin buludda genişlənməsidir və bu dövlətin ərazi hüddullarından kənarda server resurslarına sahib olması mənasını verir. Bu informasiyanın əldə edilməsi üçün innovativ konsepsiya hesab olunur, çünki adətən dövlətlər informasiyalarını öz fiziki sərhədləri daxilində saxlayır. Data səfirliyinin resursları Estoniya dövlətinin nəzarətindədir, kibercümmədən və böhran situasiyalarından blokçeyn texnologiyasının köməyi ilə mühafizə olunur və təkcə verilənlərin ehtiyat nüsxələrinin yaradılması deyil, eləcə də kritik xidmətlərin yerinə yetirilməsi imkanına malikdir [9].

“Data səfirlik” dedikdə Data mərkəzi nəzərdə tutulur. Data mərkəz Lüksemburqda verilənlərin ötürülməsi üçün ən yüksək səviyyəli - Tier 4 təhlükəsizlik səviyyəsində qorunur. Bu ənənəvi diplomatik mənada başa düşülən səfirlik deyil, lakin təsis müqaviləsi diplomatik münasibətlər haqqında Vyana Konvensiyasını nəzərə alaraq beynəlxalq hüquqda tamamilə yeni bir yanaşmadır [9]. Data mərkəz tamamilə Estoniyanın nəzarəti altındadır, lakin toxunulmazlıq kimi fiziki səfirliklərlə eyni hüquqlara malikdir.

Lüksemburq yüksək keyfiyyətli texniki imkanlarına görə, NATO standartlarına cavab verən yüksək etibarlı data mərkəzlərin olması, həm də bu yeni konsepsiya ilə işləmək üçün açığı olduğu üçün ilk Data səfirliyin yerləşdiyi 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, geniş miqyaslı kibercümm, 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 işləməməsi halında vergilər, pensiyalar, mülkiyyət hüquqları, qanunvericilik fəaliyyət və siyahıyaalma məlumatlarına əlyetərliliyinin təmin olunması üçün yaradılmışdır.

Data səfirliyinin açılması 2015-ci ildə olsa da, Estoniya və Lüksemburq arasında yekun müqavilənin imzalanması 2017-ci ildə mümkün olmuşdur. Estoniya hökumətinin buludunun inkişaf etdirilməsi Cybernetica, Dell EMC, Ericsson, OpenNode və Telia kimi özəl sektor şirkətləri ilə Estoniya hökumətinin əməkdaşlığı çərçivəsində həyata keçirilmişdir [9].

Estoniya hökuməti 2019-cu ildə fərdi məlumatların istifadəsi və emalını tənzimləyən qanun qəbul etmişdir [11]. Qəbul olunmuş qanun Avropa Birliyinin rəqlamentinə 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 etikasi 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 toplan 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.

IV. AZƏRBAYCANDA FƏRDI MƏLUMATLARIN QORUNMASINA DAİR HÜQUQİ TƏNZİMLƏMƏLƏR

“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 toplanılması, 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 işlənməsi, 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 toplanılmasının, 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 [13].

Müasir hüquq konsepsiyası fərdin ən müqəddəs 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.

Müasir sivilizasiya səviyyəsinə çatmaq məqsədinə uyğun olaraq, 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.

NƏTİCƏ

Hər bir siyasi, hüquqi, iqtisadi və ya sosial islahat vətəndaşların həyat səviyyəsini yüksəldir və beynəlxalq iqtisadi gücünü, ölkəmizin demokratik nüfuzunu və təhlükəsizliyini artırır. Fərdi məlumatların təhlükəsizliyi, qanunun aliliyi, insan hüquqları və əsas azadlıqlar tək-cə ali ümumbəşəri dəyərlər deyil, həm də iqtisadi və siyasi sabitliyin və inkişafın ən etibarlı təməlidir.

Məqalədə fərdi məlumatlar sahəsində beynəlxalq təcrübə araşdırılır. Fərdi məlumatların qorunması ilə bağlı beynəlxalq təcrübədə qəbul olunmuş qanunlara baxılması yalnız ölkələr üçün deyil, bütövlükdə cəmiyyət üçün böyük əhəmiyyət kəsb edir. Fərdi məlumatların qorunmasında təhlükəsizlik prioritet məsələlərdən biri hesab edilir. Beynəlxalq təcrübələr innovativ

ideyalar irəli sürməklə effektiv həllərin işlənməsini tələb edir. Məqalədə fərdi məlumatların qorunmasına dair bir sıra ölkələrin, o cümlədən Avropa Birliyi, Rusiya, Estoniya, ABŞ kimi ölkələrin təcrübəsi araşdırılmışdır. Müqayisəli təhlil zamanı inkişaf etmiş ölkələrdən olan Estoniyanın təklif etdiyi müasir mexanizmlərdən biri olan data səfirliyi ilə Rusiyanın təklif etdiyi müasir mexanizmlər arasında oxşarlıqlar görülmüş və təhlükəsizliyin qorunması üçün nümunə olaraq götürülmüşdür. Düzgün və ardıcılıqla istifadə edilən təhlükəsizlik qanunları və mexanizmləri vətəndaş cəmiyyətinin inkişafının yüksək səviyyəyə nail olmasına şərait yaradacaqdır.

İSTİNADLAR

- [1] N. Purtova, “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>
- [2] Y. İmamverdiyev, “E-Səhiyyədə İnformasiya Təhlükəsizliyinin Aktual Problemləri,” *İnformasiya cəmiyyəti problemləri*, №1, 2017, səh. 24–34.
- [3] A. Lehari, P. Larouche, M. Accetto, N. Purtova, L. Zemer, “The Human Right to Privacy and Personal Data Protection: Local-to-Global Governance in the Digital Era,” 2016. <https://lawsschoolsgloballeague.com>
- [4] Data Protection Laws of The World, 2017 <https://www.thebackgroundinvestigator.com>
- [5] 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://eur-lex.europa.eu>
- [6] S. Cobb, “Data privacy and data protection: US law and legislation,” April 2016, pp. 3-16.
- [7] Personal Data Regulation in Russia: Roskomnadzor Update. 2019.
- [8] World Development Report 2016: Digital Dividends, www.worldbank.org
- [9] Data embassy, <https://e-estonia.com>
- [10] Рийгикогу принял закон о создании посольства данных в Люксембурге, 2018. <https://rus.err.ee>
- [11] Personal Data Protection Act, www.riigiteataja.ee
- [12] Digital Government Factsheet 2019, Estonia. <https://joinup.ec.europa.eu>
- [13] “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanunu, www.e-qanun.az

ANALYSIS OF INTERNATIONAL PRACTICES IN THE FIELD OF PERSONAL DATA PROTECTION

Farhad Yusifov¹, Aysan Farajova²

^{1,2} Institute of Information Technology of ANAS,
Baku, Azerbaijan

¹farhadyusifov@gmail.com, ²aysanpharajova@gmail.com

Abstract – The article explores international experience in the field of personal data. Personal data is classified as sensitive information category. The access, processing and use of personal information must be authorized by someone and in other cases, their use must be restricted. In international practice, the “harbour port” mechanism used to protect personal information is used by individuals or relatives, family members, etc. requires that sensitive data should be deleted. The data embassy in Estonia has been implemented as an innovative mechanism for ensuring personal data, and the work and laws adopted the protection of personal data inside its territorial boundaries in Russia have been investigated.

Keywords – *personal data, data security, personal data protection, data embassy*

Buludlarda fərdi məlumatların mühafizəsi problemləri

Rəşid Ələkbərov¹, Arzu Həsənlı²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹rashid@iit.ab.az, ²arzuahlee1@gmail.com

Xülasə — Bulud texnologiyaları istifadəçilərin böyük hesablama və yaddaş resursları tələb edən məsələlərinin həllini təmin edən şəbəkə texnologiyasıdır. Bulud hesablama xidmətləri istifadəçinin məlumatlarını şəbəkə üzərindən bulud serverlərdə yerləşdirərək, məlumatların virtual maşınlar vasitəsilə emal edilməsinə imkan yaradır. Bu məlumat mərkəzləri dünyanın istənilən nöqtəsində istifadəçilərin əlverişliliyindən və nəzarətindən kənarda yerləşdiyindən, xidmətdən istifadə etdikdə çoxşaxəli təhlükəsizlik və məxfilik problemləri yaranır. Məqalədə buludlarda saxlanılan məlumatlara yönələn təhlükələr, təhdidlər, onlara qarşı mübarizə üsulları araşdırılmışdır.

Açar sözlər – hesablama buludları, IaaS, PaaS, SaaS, bulud xidmətləri, məxfilik, təhlükəsizlik.

I. GİRİŞ

Hazırda bulud hesablaması İnternet sənayesinin ən aktual mövzularından biridir. Təşkilatlar və fərdi internet istifadəçiləri məlumatlarını saxlamaq və emal etmək üçün bulud hesablama texnologiyalarından geniş istifadə edirlər. Lakin buludda yerləşən məlumatların özü də bir sıra təhdidlərə məruz qala bilər və məlumatların məxfiliyi və bütövlüyü pozula bilər. Buludun xarici təhdidlərdən qorunması üçün müntəzəm olaraq yoxlanılması lazımdır. Fərdi istifadəçilərin və müəssisələrin böyük həcmli məlumatlarının buludda yerləşdirilməsi və ondan istifadə olunması hakerlər tərəfindən daha çox hücumlara məruz qalmasına və istifadəçilərdə məxfilik problemlərinin yaranmasına səbəb olur. Bulud serverlərdə məlumatların təhlükəsizliyinin və məxfiliyinin qorunması aktual məsələlərdəndir.

II. BULUD XİDMƏTLƏRİ

Hal-hazırda bulud texnologiyalarında ən çox istifadə olunan xidmətlər aşağıdakılardır (şəkil 1) [1]:

Infrastructure-as-a-service (IaaS) – infrastruktur servis kimi. IaaS səviyyəsi infrastrukturun icarəyə götürülməsi servisini həyata keçirməyə imkan verir.

Platform-as-a-service (PaaS) – platforma servis kimi. PaaS servisi istifadəçilərə virtual serverlərdə yerləşən əməliyyat sistemlərindən və xüsusişdirilmiş proqram əlavələrindən istifadə etməyə imkan yaradan virtual platformadır.

Software-as-a-service (SaaS) – proqram təminatı servis kimi. İstifadəçiləri proqram təminatı ilə təmin edir. İstifadəçi proqram təminatını almır və lazım gələndə ondan məsələnin həllində istifadə edir və istifadəyə görə uyğun məbləği ödəyir.

Şəkil 1. Hesablama buludlarının modeli

Hesablama buludları aşağıdakı üstünlüklərə malikdir [2]:

- İnternetə qoşulan fərdi kompüterlərin hesablama və yaddaş resurslarına olan tələbatını azaldır;
- istifadəçilərin məhdudiyyətsiz hesablama və yaddaş resursları ilə təmin olunmasına imkan verir;
- hesablama və yaddaş resurslarından faktiki istifadəyə görə təminatçıya ödəniş olunur;
- verilənlərin yüksək sürətlə emalı həyata keçirilir;
- aparat və proqram təminatına, xidmətə və elektrik enerjisinə olan xərclər azalır;
- istifadə olunan proqramlar daim yenilənir və s.

Bulud texnologiyalarında istifadəçilərin proqram əlavələri və fərdi məlumatları onların fərdi kompüterlərində yox, əsasən İnternet şəbəkəsinin bulud serverlərində yerləşdirilir. İstifadəçilərin göndərdiyi sorgulara uyğun olaraq onları əldə etmək istədikləri məlumatlarla təmin edir. Hesablama buludlarında ənənəvi təhlükəsizlik məsələləri hələ də mövcuddur. Bulud xidmətləri təklif edən provayderlər müştərilərinə yaxşı xidmət göstərmək üçün zaman-zaman yeni imkanlar təklif edir. Təqdim edilən yeni və daha mürəkkəb əlavələr ənənəvi təhlükəsizlik mexanizmlərinin buluddakı məlumatların məxfiliyini tam təmin edə bilməməsinə səbəb olur. Buludların açıqlığı və çoxsaylı xidmətlərin xüsusiyyətləri

hesablama buludlarının informasiya təhlükəsizliyinin təmin edilməsində problemlər vardır [3,4]:

- Bulud platformalarında istifadə olunan proqram əlavələri və saxlanan məlumatlar sabit infrastruktur və təhlükəsizlik sərhədlərinə malik deyil. Bu isə buludda təhlükəsizliyin pozulması hallarında fiziki resursların sistemdən təcrid edilməsində çətinliklərə səbəb olur;
- İstifadəçilərə bulud xidmətləri təklif edən bulud platformalarının çoxsaylı provayderlərə məxsus olması buludda mübahisəli hadisə baş verdikdə, onun həllinə vahid təhlükəsizlik tədbirləri tətbiq etməyi çətinləşdirir;
- Buludun açıqlığı və çoxsaylı istifadəçilərin bulud serverlərdən istifadəsi, icazəsi olmayan şəxslərin istifadəçilərin məlumatlarına giriş əldə etməsinə imkan yaradır;

Hesablama buludlarında istifadəçilərin məlumatlarının kənar şəxslərdən zamanətli qorunması və şəbəkənin təhlükəsizliyi əsas məsələlərdəndir.

Potensial hücumlara aşağıdakılar aid ola bilər [5]:

- bulud serverlərə müdaxilə;
- kanala kənar hücumlar;
- autentifikasiya hücumları;
- şəxs vasitəsilə şifrələmə hücumları və s.

Bulud xidmətlərində müxtəlif təhlükəsizlik məsələlərini: məxfilik, məlumatın tamlığı, bərpası və istifadəçi məlumatlarının idarə edilməsi, məlumat təhlükəsizliyini təmin etmək üçün aşağıdakı prosedur qaydalar tətbiq edilməlidir:

Məlumat təhlükəsizliyini təmin etmək üçün təhlükəsizlik standartlarını şifrələmə metodlarından istifadə edilməlidir.

Xidmət təminatçılarının (provayderlərin) istifadəçi məlumatlarına əlçatanlığı məhdud olmalıdır, onlar məlumatlara müdaxilə edə bilməməlidirlər.

Şəbəkəni idarə edən serverlərə icazəsiz və qanunsuz girişin qarşısını almaq üçün sərt giriş protokolları tətbiq olunmalıdır.

İstifadəçi məlumatlarının ehtiyat nüsxələri yaradılmalıdır ki, qəza baş verdikdə onları bərpa etmək mümkün olsun.

III. BULUD TEXNOLOGİYASINDAKI BARYERLƏR VƏ TƏHLÜKƏSİZLİK TƏHDİDLƏRİ

Hal-hazırda bulud texnologiyasından geniş istifadə edilməsinə baxmayaraq, bir çox təşkilatlar bulud xidmətlərinin təhlükəsizliyinin təmin edilməsindən çox narahatdır. Sistemin arxitekturasındakı bəzi boşluqlar bulud hesablamasını müxtəlif təhlükəsizlik və məxfilik təhdidlərinə qarşı müdafiəsiz etmişdir. Bu keçid konsepsiyasının sərhədlərini məhdudlaşdırın aşağıdakı məsələlərdir[6-8]:

Məxfilik və təhlükəsizlik – hər hansı bir yeni hesablama texnologiyasının müvəffəqiyyətini təyin edən əsas amil onun etibarlı olduğu müddətə əsaslanır. Fərdlərin məlumatlarının hesablama buludlarında bulud serverlərində saxlanması

təhlükəsizlik və məxfilik baxımından fərdi kompüterlərin məlumat daşıyıcılarında saxlanmasına nəzərən daha az etibarlıdır. Fərdi kompüterlərdə saxlanılan məlumatları istənilən zaman sabit disklərə və sistemlərə daxil olmaqla əldə etmək mümkündür, ancaq bulud serverləri potensial olaraq dünyanın hər yerində yerləşə bilər və İnternetdə baş verən hər cür qəzalar buludda olan məlumatlara girişin qarşısını ala bilər.

Performans, gecikmə və etibarlılıq. İstifadəçi və bulud serverləri arasında məlumat mübadiləsində gecikmələr və etibarlılıq məsələləri bulud hesablamalarında problemlərə səbəb olmuşdur. Gecikməni artıran digər amillər məlumatların etibarsız və ictimai şəbəkələrdə (hər kəsin, yəni ümumi kütlənin daxil olduğu və digər şəbəkələrə və ya İnternetə qoşula biləcəyi bir şəbəkədir) hərəkəti zamanı tıxanma, küy və paket itkisi ilə müşayiət olunan şifrələmə və deşifrələmə prosesidir.

Portativlik. Bəzi hallarda təşkilatlar bulud təminatçılarını dəyişdirmələri lazım gəlir. Şirkətlər istifadə etdiklərindən daha yaxşı başqa bir bulud platformasını tapdıqları təqdirdə məlumatlarını və tətbiqlərini yeni platformaya köçürə bilmədikləri hallar yaşanmışdır. Bundan başqa, bəzi şirkətlər öz tələblərinə uyğun olaraq bulud xidməti təminatçıları tərəfindən təqdim olunan xidmətlərin müxtəlifliyinə görə fərqli tətbiqlər üçün fərqli bulud platformalarından istifadə edirlər. Bu səbəbdən bulud texnologiyalarında portativlik xüsusiyyəti həyati funksiya daşıyır.

Fiber optik şəbəkələr vasitəsi ilə məlumatların sızdırılması. Son bir neçə ildə tranzit məlumatların təhlükəsizlik risklərinin artdığı diqqəti cəlb edir. Məlumatların şəbəkə vasitəsilə ötürülməsi hazırda normal prosesdir və bir çox məlumat mərkəzləri ictimai və ya özəl bulud modelləri kimi digər bulud yerləşdirmə modellərini əhatə edə bilər. Son dövrlərdə bir məlumat mərkəzindən digərinə ötürülən məlumatların təhlükəsizliyinin pozulması faktlarına daha çox rast gəlinib.

IP şəbəkələri üzərində məlumatların saxlanması. İnternet məlumatların saxlanması hal-hazırda olduqca populyarlaşır və yaxın illərdə müəssisələrin verilənləri saxladığı sistemlərinin əksəriyyətinin şəbəkəyə qoşulacağı müşahidə edilmişdir, çünki bu, müəssisələrə tələb olunan arxitekturanı qurmadan çox böyük məlumat toplaşağı imkan verir. Onlayn məlumat saxlamağın bir çox üstünlükləri olsa da, buludda vacib məlumatların sızmasına və ya məlumatların əlçatmazlığına səbəb ola biləcək təhlükəsizlik təhdidləri mövcuddur.

Aşağıda buludlara qarşı yönələn müxtəlif təhlükəsizlik təhdidləri və hücumları göstərilmişdir[9,10,11]:

- SQL injection;
- Cross-Site Scripting (XSS) hücumları;
- DoS hücumları;
- DDoS hücumları;
- Google Hacking;
- Forced Hacking.

Göstərilən hücumları aşkar etmək üçün bir neçə standart üsullardan istifadə edirlər: Kodda dinamik olaraq yaradılan SQL-in istifadəsinin qarşısını almaq, kodda istifadə olunan meta quruluşlarını tapmaq, istifadəçinin daxil etdiyi bütün parametrləri təsdiqləmək, lazımsız məlumatların və simvolların qəbul edilməməsi və silinməsi və s. Ümumi təhlükəsizlik çərçivəsində meyarlar müəyyən olunmalı, hər hansı bir bulud mühiti ilə əlaqə qurmaq üçün xüsusi hazırlanmış və əvvəlcədən təyin edilmiş təhlükəsizlik siyasəti tətbiq edilməli və prosesin sonrakı mərhələləri də nəzarət altında saxlanılmalıdır.

Bənzər bir yanaşma, İnternetdən gələn təhlükəsizlik təhdidlərini bloklayan və şəbəkəyə çatmadan məlumatları süzgəcdən keçirən Symantec Mesaj Labs Web Security proqram təminatından bulud serverlərində geniş istifadə olunur. Buludlarda yaradılan Veb səhifələrin təhlükəsizliyinin təmin edilməsi iki komponentə əsaslanır [12, 13]:

Çox səviyyəli təhlükəsizlik – məlumat təhlükəsizliyini təmin etmək və mümkün zərərlərin qarşısını almaq üçün çox səviyyəli təhlükəsizlik platformasından ibarətdir.

URL-lərin süzülməsi – əksər hallarda hücumlar müxtəlif veb səhifələr və İnternet saytları vasitəsilə də həyata keçirilir. URL-lərin süzülməsi veb-səhifələrin süzgəcdən keçirildiyi, veb-səhifənin zərərli və ya təhlükə daşıyan məlumata malik olub olmadığını yoxlayır. Bundan başqa, arzuolunmaz saytların məzmununu da bloklaya bilər. Eyni zamanda URL-lərin süzülməsi çevik texnologiya olub, sistemin çox ziddiyyətli mühitlərində də təhlükəsizliyi təmin edir və yeni və yaxınlaşan zərərli proqram təhlükələrindən qoruyur.

NƏTİCƏ

Məqalədə hesablama buludlarında istifadə edilən bulud platformalarda təhlükəsizlik problemlər tədqiq edilmişdir. Hesablama buludlarında istifadəçilərin məlumatlarının kənar şəxslərdən zəmanətli qorunması və şəbəkənin təhlükəsizliyi istiqamətində meydana çıxan təhdidlər analiz və təhlil olunmuşdur, hesablama buludlarının istifadəsi zamanı meydana çıxan təhlükəsizlik və məxfilik problemləri araşdırılmışdır və həlli yolları göstərilmişdir.

İSTİNADLAR

- [1] R.Q. Ələkbərov, M.A. Həşimov “Bulud texnologiyaları: xidmətlər, problemlər və tətbiq sahələri”, İnformasiya texnologiyaları problemləri, 2016, №1, s.3–10.
- [2] O.R. Ələkbərov “Mobil hesablama buludlarında təhlükəsizlik və konfidensiallıq məsələləri”, İnformasiya texnologiyaları problemləri, 2018, №1, s.92-103.
- [3] Z.Xiao, Y. Xiao “ Security and Privacy in Cloud Computing”, IEEE Communications Surveys & Tutorials, vol. 15, no. 2, 2013, pp. 843-859.

- [4] M.Gopichand “An overview of security and privacy issue in mobil cloud computing environment”, International Journal of Advanced Researc in Computer Science and Software Engineering, vol. 6, no. 5, 2016, pp. 779-784.
- [5] K.Hashizume, D.G. Rosado, E. F. Medina, E. B Fernandez, “An analysis of security issues for cloud computing”, Journal of Internet Services and Applications, 2013.
- [6] P.K.Tiwari1, B.Mishra, “Cloud computing security issues, challenges and solution”, International Journal of Emerging Technology and Advanced Engineering, Vol 2, Issue 8, August 2012.
- [7] A. Ansari and Ch. Bawankar, “Privacy & data integrity for secure cloud storage”, IOSR Journal of Computer Science, 2014.
- [8] R.Bhadauria, R.Chaki, N. Chaki, S. Sanyal “A survey on security issues in cloud computing,” arXiv preprint arXiv:1109.5388, pp. 1-15, 2011.
- [9] B. R. Kandukuri, R. V. Paturi and A. Rakshit, “Cloud security issues,” 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009.
- [10] H. Liang, D. Huang, L. X. Cai, X. Shen and D. Peng, “Resource allocation for security services in mobile cloud computing,” in Proc. IEEE INFOCOM'11, Machine-to-Machine Communications and Networking (M2MCN), pp. 191-195, 2011.
- [11] W. Li, L. Ping, X. Pan, “Use trust management module to achieve effective security mechanisms in cloud environment,” 2010 International Conference on Electronics and Information Engineering (ICEIE), Volume: 1, pp. V1-14-19, 2010.
- [12] S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing”; Journal of Network and Computer Applications, Vol. 34(1), pp. 1–11, 2011.
- [13] L. Wang, G. Laszewski, M. Kunze, J. Tao, “Cloud computing: A perspective study”, New Generation Computing- Advances of Distributed Information Processing, pp. 137-146, vol. 28, no. 2, 2008.

PROBLEMS OF PERSONAL DATA PROTECTION IN CLOUDS

Rashid Alekperov¹, Arzu Hasanli²

^{1,2}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹rashid@iit.ab.az, ²arzuhlee1@gmail.com

Abstract – Cloud technology is a network technology that enables users to solve issues that require large computing and memory resources. Cloud computing services enable the processing of data through virtual machines, placing user data across the network on cloud servers. As these data centers are located anywhere in the world away from the direct access and control of users, the use of the service creates a multitude of security and privacy concerns. The article explores the dangers, threats, and methods for combating of information stored in clouds.

Keywords— *computing technologies, IaaS, PaaS, SaaS, cloud services, cloud computing, privacy, security*

Fərdi məlumatların tənzimlənməsinə siyasi-hüquqi nəzər: beynəlxalq və Azərbaycan qanunvericiliyi

Rəna Mirzəzadə

AMEA Fəlsəfə İnstitutu, Bakı, Azərbaycan

Fərdi məlumatlar anlayışı özündə fərd haqqında kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumatdan gedir. Bəs fərdi məlumatların subyektı nədir? Bu, barəsində fərdi məlumatlar toplanılan, işlənən və mühafizə edilən, kimliyi müəyyənləşdirilmiş və ya müəyyənləşdirilən subyektidir.

Akademik R.Mehdiyevin yazdığı kimi: “universal səviyyədə informasiya məkanında fərdin təhlükəsizliyinin və azadlığının mənafeləri arasında tarazlığa əsaslanan informasiya təhlükəsizliyinin vahid standartlarının və meyarlarının müəyyən edilməsi zəruridir” [13].

Bu aspektdən fərdi məlumatların toplanması isə hər subyekt haqqında fərdi məlumatların sənədləşdirilmiş qaydada, qanuna uyğun olaraq əldə edilməsindən ibarətdir. Bəs fərdi məlumatlar necə verilir? Belə ki, fərdi məlumatlar qanunvericiliklə müəyyən edilmiş qaydada sorğu əsasında, maddi daşıyıcılarla və ya informasiya texnologiyaları vasitəsilə istifadəçilərə təqdim edilir. Akademik Rasim Əliquliyev göstərir ki: “dövlət hakimiyyətinin dayanıqlılığı, təhlükəsizliyi və effektiv fəaliyyətinin təmin edilməsi mürəkkəb komponentli və operativ məlumat bazalarının, o cümlədən fərdlər haqqında məlumatların toplanmasını, analizini və sistemləşdirilməsini zəruri edir” [3; 117]. Məhz bu aspektdən də mövzu aktualdır. Bəs onun həlli yolları necədir. Nəzərə yetirək ki, fərdi məlumatların məxfiliyi qorunmalıdır. Fərdi məlumatların məxfiliyi inkişaf etmiş ölkələrdə qanunvericiliklə nizamlanır. İlk dəfə 1981-ci il 28 yanvarda Strasburqda Avropa Şurası tərəfindən “Fərdi məlumatların avtomatlaşdırılmış qaydada işlənməsi ilə əlaqədar şəxslərin qorunması haqqında” Konvensiya qəbul edildi ki, bu da fərdi məlumatların mühafizəsi və məxfiliyin qorunması üzrə əsas sənəddir. Konvensiyanı AŞ üzvü 43 ölkə ratifikasiya etdi və digər ölkələr tərəfindən imzalanmaq üçün açıq qaldı. Konvensiya 1985-ci il 1 oktyabrdan qüvvəyə minmişdir. Konvensiya Avropa Şurasına üzv olan bütün ölkələr, eləcə də AŞ-nin üzvü olmayan – Uruqvay (2013-cü ildə ilk Avropadan kənar ölkə olaraq), Mavriki (2016), Seneqal (2016), Tunis (2017), Kabo-Verde (2018), Meksika (2018), 2019-cu ildə Argentina, Meksika tərəfindən qəbul olunmuşdur. Konvensiyanı ratifikasiya etmiş ölkələr üçün məcburi olsa da, Avropa İnsan Hüquqları Məhkəməsinə müraciət üçün əsas deyil [5]. AŞ-nin keçmiş baş katibi Torbyorn Yaqland qeyd etdiyi kimi: “Konvensiya ölkələr arasında fərdi məlumatların mühafizəsi sahəsində möhkəm qaydalar və qanunlar bazası olmaqla

yanaşı, həmçinin bu sahədə qlobal mərhələdə əməkdaşlıq üçün xüsusi format yaradır” [10].

1985-ci ildən keçən dövr ərzində Konvensiya yenilənmiş, son olaraq da “süni intellekt”lə bağlı müddəalar əlavə olunmuşdur. Süni intellekt sistemlərinin geniş istifadəsi, xüsusilə bu sahədə məlumatların istifadəsi ilə bağlı təhlükə yaratmışdır və bu təhlükə yalnız dövlət qurumlarına məxsus resurslarla bağlı deyil, həmçinin müxtəlif onlayn servislərlə bağlıdır. Beləliklə “Fərdi məlumatların avtomatlaşdırılmış qaydada işlənməsi ilə əlaqədar şəxslərin qorunması haqqında” Konvensiyanın Məsləhətçi Komissiyası 25 yanvar 2019-cu ildə “Süni intellekt və məlumatların qorunması haqqında qaydalar” qəbul edir [6]. Bu, 28 Yanvar – Məlumatların mühafizəsi günündə nəşr edilir. 28 yanvar tarixinin “Məlumatların mühafizəsi günü” kimi qeyd olunması da 1981-ci ildə bu Konvensiyanın ilk dəfə imzalandığı günlə bağlıdır. Konvensiyada şəxsin irqi və siyasi mənsubluğu, tibbi məlumatları, dini etiqadı, cinsi və məhkumluqla bağlı məlumatları “həssas məlumatlar” kimi qeyd olunur. Nəzərə alsaq ki, bu cür məlumatlar müxtəlif özəl sektora mənsub şəbəkələrdə də mövcuddur və müasir dövrdə İKT-nin geniş istifadəsi də yeni təhlükəsizlik təhdidləri ortaya çıxarır. AŞ Nazirlər Komitəsinin qəbul olunan düzəliş protokolları çatışmazlıqları aradan qaldırmaq imkanı yaradır [11].

Tədqiqatçı Nina Qumzey yazır ki: “Strasburq Konvensiyasının qəbul olunmasının daha bir mühüm cəhəti bu sahədə presedent yaratmaqla yanaşı, son düzəlişlər nəticəsində dövlətlərarası transsərhəd məlumat axınlarına da müəyyən məhdudiyyətlər gətirməsidir. Baxmayaraq ki, bir çox ölkələrin şəxsi məlumatların mühafizəsi sahəsindəki qanunvericiliyi bir-birinə yaxındır, lakin milli qanunvericiliyin bu sahədə praktiki olaraq tətbiqi çox zaman ya mümkün olmur, ya da olursa belə ekvivalent mühafizəni təmin edə bilmir” [9; 13]. Nümunə olaraq, bir ölkə vətəndaşının başqa bir ölkədə olan üçüncü tərəfə məxsus beynəlxalq bir bankda hesabının olması və ya onun başqa ölkələrə səfəri zamanı məlumatlarının toplanılması, saxlanması problemini göstərmək olar. Beləliklə, fərdi məlumatların ikinci və üçüncü tərəf ölkələr tərəfindən əldə olunması və qorunması problemi yaranır ki, bu zaman hansı ölkənin qanunlarının tətbiq olunacağını müəyyən etmək asan olmur. Strasburq Konvensiyası isə universaldır və yalnız dövlətlərlə bağlı deyil, həmçinin, özəl sektor, məhkəmə və hüquq-mühafizə orqanları tərəfindən həyata keçirilən bütün

məlumat emalı proseslərinə şamil olunur. Məhz bu isə əldə olunan yenilikdir.

Bəs praktiki əhəmiyyəti nədir? Qloria Qonzaloez Fluaster “Fundamental hüquq kimi fərdi məlumatların mühafizəsinin Avropa İttifaqında yaranması” adlı kitabında qeyd etdiyi kimi: “Avropa İttifaqında belə bir qanunun qəbul olunmasına 2 əsas zərurət var idi. Bunlardan birincisi, Aİ leqal sistemi içərisində belə hüququn təbii olaraq ortaya çıxması və buna olan maraq, ikincisi isə o zamanki hüquqi ədəbiyyatda bu problemə çox məhdud çərçivədə toxunulması, həmçinin məhkəmə-hüquq sistemində problemin interpretasiyası və tətbiqi ilə bağlı olan problemlər idi” [7;3-4].

Bu sahədə müxtəlif ölkələrin qanunvericiliklərində fərqli yanaşmalar mövcuddur və əslində, Konvensiya bu sahədə qəbul olunmuş əsas beynəlxalq akt sayıla bilər. Məsələn, ABŞ-a istinad etsək, burada bu sahə ilə bağlı qəbul edilmiş xüsusi bir qanun yoxdur. Codi Vestbi “Məxfilik ilə bağlı beynəlxalq məlumat kitabçası” adlı kitabında göstərdiyi kimi: “ABŞ-da dövlət orqanları 1974-cü il “Məxfilik Aktı”na istinad etsə də, özəl sektor Avropa İttifaqında olduğu kimi və ya Kanada qəbul olunmuş “Fərdi Məlumatların Mühafizəsi və Elektron Sənədlər Aktı”-nı nümunəsinə uyğun bir qanunvericilik aktlarına tabe deyil. ABŞ-da bu sahədə tənzimləmə qanunları, administrativ aktlar, məhkəmə qərarları və ştatlara məxsus qanunlarla aparılır, bu isə fərdi məlumatların qorunması ilə bağlı vahid və möhkəm bir baza təmin edə bilmir [8;11].

Bəs Azərbaycanda vəziyyət necədir? Azərbaycanda da fərdi məlumatlarla əlaqədar mükəmməl qanunvericilik bazası vardır. Belə ki, Azərbaycan Respublikası Konstitusiyasının 47-ci maddəsi “Fikir və söz azadlığı” adlanır və onun I bəndində yazılıb: “Hər kəsin fikir və söz azadlığı vardır” [1, 17]. Həmçinin Konstitusiyanın 50-ci maddəsi də “Məlumat azadlığı” adlanır. Azərbaycan Respublikası da Strasburq Konvensiyasına qoşulmuş və Konvensiya 30 sentyabr 2009-cu il tarixində Milli Məclisdə təsdiq edilmiş, 2010-cu il 1 sentyabr tarixindən isə qüvvəyə minmişdir. Burada əsas məqsəd: 1) - insanları bu məsələlər ilə bağlı məlumatlandırmaq; 2) - onlar haqqında məlumatların hansı məqsədlərlə toplanıldığını və işləndiyini anlamaq imkanı yaratmaq; 3) toplanılan fərdi məlumatların subyektlərinə onların hüquqlarını başa salmaqdan ibarətdir.

Bu mənada, fərdi məlumatların toplanması, işlənməsi və mühafizəsinin əsasları, prinsipləri, bu sahədə dövlət tənzimləməsinin qayda və tələbləri, fərdi məlumatların informasiya ehtiyatlarında formalaşdırılması, informasiya sistemlərinin yaradılması, informasiyanın verilməsi və ötürülməsi qaydalarını əsaslandırır. Bu prosesdə iştirak edən şəxslərin hüquqları, vəzifələri və məsuliyyətini müəyyən etmək, insan və vətəndaş hüquqları və azadlıqları, şəxsi və ailə sirrini saxlamaq hüququnu müdafiə etmək məqsədi ilə bu qanun ölkəmizdə də qəbul edilmişdi. Qanun fərdi məlumatların toplanılması, işlənməsi və mühafizəsi ilə bağlı münasibətləri, milli informasiya məkanının fərdi məlumatlar bölümünün formalaşdırılması, habelə fərdi məlumatların transsərhəd ötürülməsi ilə əlaqədar münasibətlərin tənzimlənməsi, o cümlədən bu sahədə fəaliyyət göstərən dövlət və yerli

özünüidare orqanlarının, hüquqi və fiziki şəxslərin hüquq və vəzifələrini müəyyən edir.

Prezident İlham Əliyev tərəfindən “Fərdi məlumatlar haqqında” Qanunun tətbiq edilməsi barədə 2010-cu il iyunun 4-də imzalanmış Fərmanda qanunun icrasının təmin edilməsi məqsədi ilə xüsusi tapşırıqlar verilmişdir [2]. Fərmana müvafiq olaraq aidiyyəti dövlət orqanları tərəfindən “Fərdi məlumatların informasiya sistemlərinin dövlət qeydiyyatına alınması və dövlət qeydiyyatının ləğv edilməsi Qaydaları”, “Fərdi məlumatların mühafizəsinə dair tələblər”, “Fərdi məlumatların informasiya sistemlərinin dövlət qeydiyyatı ləğv edildikdə həmin informasiya sistemlərində olan məlumatların məhv edilməsi Qaydası” və “Dövlət qeydiyyatına alınması tələb olunmayan informasiya sistemləri” sənədləri hazırlanmış və Nazirlər Kabinetinin müvafiq qərarları ilə təsdiq edilmişdir. Prezident İlham Əliyevin fərmanı ilə “Fərdi məlumatların informasiya sistemlərinin dövlət reyestrinin aparılması Qaydaları” da təsdiq edilmişdir [2]. Azərbaycanda qanunla fərdi məlumatların informasiya sistemini dövlət qeydiyyatından keçirmədən toplanılmasına və işlənməsinə yol verilmir. Bununla yanaşı, qanunda xüsusi istisna hallar da nəzərdə tutulmuşdur. Ümumilikdə, fərdi məlumatların informasiya sistemləri yaradılarkən qanunvericiliklə müəyyən edilmiş qaydada fərdi məlumatların mühafizəsinə dair tələblərə əməl edilməlidir.

Bəs fərdi məlumatlardan necə istifadə etmək olar? Akademik Rəşad Əliyev yazır ki: “Fərdi məlumatlardan istifadə ilə bağlı hüquqi məhdudiyyətlərə baxmayaraq, onlardan qeyri-qanuni biznes və kriminal məqsədlərlə istifadəyə olan tələbat bu sahənin “qara bazarı”nın formalaşmasına səbə verir. Beləliklə, fərdi məlumatlar həm də kriminalistikanın problemə çevrilir” [3;117]. Qanuna müvafiq olaraq fərdi məlumatların informasiya ehtiyatlarının formalaşdırılması və informasiya sistemlərinin yaradılması, onlara xidmətlərin göstərilməsi sahəsində fəaliyyət Azərbaycanın qanunvericiliyinə uyğun olaraq xüsusi razılıq (lisenziya) əsasında həyata keçirilməlidir. Bu məqsədlə, qanunun icrasının təmin edilməsi barədə Prezident İlham Əliyev 2010-cu il dekabrın 13-də “Xüsusi razılıq (lisenziya) tələb olunan fəaliyyət növlərinin siyahısı və həmin fəaliyyət növlərinə xüsusi razılıq (lisenziya) verilməsinə görə ödənilən dövlət rüsumunun məbləği” qanununa əlavələr edilməsi və müvafiq olaraq bu sahədə lisenziyanın verilməsi üzrə fəaliyyət RİTN-ə tapşırılması haqda fərman vermişdir [4].

Fərdi məlumatlarda subyektin hüquqlarının mühafizəsində gəldikdə, bu sahədə də qanunvericilikdə əsaslı nizamlayıcı mexanizm qurulmuş, hər bir şəxsə informasiya sistemində özü barəsində məlumatların mövcudluğu və həmin məlumatların əldə edilməsi mənbələri haqqında məlumat almaq, məlumatların toplanılmasına və işlənməsinə qadağan qoyulmasını tələb etmək və digər hüquqlar verir. Hər bir vətəndaş fərdi məlumatların qanunsuz toplanılması və işlənməsi, mühafizəsinin təmin edilməməsi, habelə qanunun tələblərinə əməl olunmaması nəticəsində onun hüquqlarının pozulduğu hallarda qanunvericiliklə müəyyən edilmiş qaydada müvafiq icra hakimiyyəti orqanına və ya məhkəməyə şikayət edə bilər. Fikrimizi Akademik Rəşad Mehdiyev sözləri ilə

yekunlaşdıraraq: “İnternet təkə məlumat yığını olmayıb, bəşəriyyətin virtual portretini, yeni fəlsəfəni formalaşdırır. Sosial şəbəkələr ünsiyyəti asanlaşdırmaqla, qarşılıqlı münasibətlərdə yeni platforma yaradır” [12].

İSTİNADLAR

- [1] Azərbaycan Respublikasının Konstitusiyası, B, 2016. “Qanun” nəşr, səh.117
- [2] AzərTac 2010 4 iyun.
- [3] Əliquliyev R.M., Mahmudov R.S. Milli mentalitet kontekstində fərdi məlumatların həssaslığı və onların təhlükəsizliyinin təmin olunması məsələləri. İnformasiya cəmiyyəti problemləri jur, 2009, №2, s.117-128.
- [4] AzərTac 2010. 13 dekabr
- [5] Details of Treaty No.108. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>
- [6] Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data (conventn 108), guidelines on artificial intelligence and data protection. T-PD(2019)01. Strasbourg, 25 January 2019.
- [7] Gloria González Fuster. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer International Publishing Switzerland 2014. 273 pages.
- [8] International Guide to Privacy By Jody R. Westby, American Bar Association. Section of Science & Technology Law. (01.12.2005). 247 pages
- [9] Nina Gumzej. The council of europe and the right to personal data protection: embracing postmodernity. Conference of the International Journal of Arts & Sciences, ISSN: 1943-6114 : 6(2): 13–33 pages (2013)
- [10] Opening for signature of the Protocol amending the Convention 108 <https://uodo.gov.pl/en/539/999>
- [11] The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 and explanatory memorandum. Council of Europe Publishing, F-67075 Strasbourg Cedex
- [12] Bax:vaxt.az/?name=xeber@xeber_id=1459
- [13] Azertaq.az/xeber/akademik_Ramiz Mehdiyev. Beynəlxalq. informasiya-təhlükəsi.

POLITICAL AND LEGAL CONSIDERATION OF DATA PROTECTION REGULATION: INTERNATIONAL AND NATIONAL LEGISLATION

Rena Mirzazadeh

ANAS Institute of Philosophy, Baku, Azerbaijan

Abstract— In this article the conception of personal data, its collection and sharing process have been taken into the consideration. First of all, actuality of the topic and how it is represented on international law described thoroughly. Strasbourg Convention, its ratification in European countries, as well as regulation of the issue in those countries are illustrated. Later, Decree of the President İlham Aliyev considering personal data protection have been interpreted. Analysis also uses global and local authors' thoughts on the matter, such as academician Ramiz Mehdiyev, academician Rasim Aliquliyev.

Fərdi məlumatların “qara bazar”ının xüsusiyyətləri və yaratdığı problemlər

Rasim Mahmudov

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

Xülasə— Məqalədə fərdi məlumatların “qara bazar”ının mahiyyəti, xüsusiyyətləri araşdırılır. “Qara bazar”da alqı-satqı obyektı olan məlumat və xidmət növləri, texnologiyalar və onların qiymət siyasəti şərh olunur, həmçinin “qara bazar”da əldə edilən fərdi məlumatların hansı məqsədlər üçün istifadə edildiyi müəyyən edilir. Eyni zamanda, bu cür məlumatların qeyri-qanuni əldə edilməsi və satılmasının şəxsi, korporativ və milli maraqlar baxımından yaratdığı problemlər göstərilir.

Açar sözlər— fərdi məlumatlar; fərdi məlumatların “qara bazar”ı; fərdi məlumatların qiyməti; fərdi məlumatların oğurlanması.

I. GİRİŞ

Fərdi məlumatların dəyəri, əhəmiyyəti artdıqca, onlara olan tələbat da artır. Fərdi məlumatlardan istifadə ilə bağlı hüquqi məsuliyyət normaları, məhdudiyyətlər olduğu üçün onlardan qeyri-legal biznes və kriminal məqsədlərlə istifadəyə olan tələbat bu sahənin “qara bazarı”nın formalaşmasına rəvac verir.

Müasir informasiya təhlükəsizliyi texnologiyaları və vasitələrinin tətbiqi standart kibercinayətlərdən mühafizəni, əsasən, təmin edir. Ona görə də kibercinayətkarlar daim mövcud mühafizə sistemlərini aşırıb keçmək üçün yeni-yeni imkanlar, üsullar axtarırlar. Belə üsullardan biri də “qara bazar” vasitəsi ilə müvafiq məlumatların ələ keçirilməsidir [1].

“Qara bazar”da insanların başqalarından gizli saxlamaq istədikləri istənilən fərdi məlumatları - şəxsiyyət vəsiqəsinin, sürücülük vəsiqəsinin, sığorta şəhadətnaməsinin, kredit kartın, sağlamlıq kartının, bank hesabının, VÖEN-in, mobil telefon məlumatları, e-poçt ünvanı, ev və ya iş ünvanı və s. satıla bilər. Kibercinayətkarlar bu cür məlumatlardan sosial mühəndislik üsullarını tətbiq etməklə dələduzluq, şantaj, qəsbkarlıq üçün istifadə edirlər.

Tədqiqatçılar hələ 1990-cı illərdə fərdi məlumat bazarının formalaşmasını proqnozlaşdırsalar da, həmin vaxtlar elm və hüquq ictimaiyyətinin nümayəndələri bu ideyaya ehtiyatla yanaşırdılar. Onlar hesab edirdilər ki, şəxsi həyatın toxunulmazlığı hüququ və onun reallaşdırılmasının mövcud mexanizmləri fərdi məlumatların bir ticarət predmeti olmasına imkan verməyəcək [2].

Hazırda bir çoxları hələ də şəxsi həyatın toxunulmazlığını insanın ayrılmaz hüququ hesab edirlər. Konfidensiallığın qorunması texnologiyaları bu hüquqların təmin olunmasına

yönəlsə də, fərdi məlumatların bazarı başqa istiqamətdə inkişaf edir.

Bir çox ekspertlər fərdi məlumatların “qara bazarı”nın getdikcə daha da inkişaf edəcəyini proqnozlaşdırırlar. Sürətlə inkişaf edən bu “qara” biznes global hakerlər cəmiyyəti, zərərli proqram təminatı hazırlayanlar tərəfindən dəstəklənir. Deməli, fərdi məlumatların “qara bazarı” həm də zərərli, yaxud kriminal proqram təminatı bazarının inkişafını stimullaşdırır [3].

ABŞ-da “qara bazar”ın məhsullarına daha çox maraq göstərilir. 2019-cu ildə bu ölkədə fərdi məlumatların əldə edilməsi üçün 15,2 milyard dollar xərclənib. Dünyada fərdi məlumatların ən böyük “qara bazarı” ABŞ-dadır. Belə ki, global bazarın təxminən 60%-i Birləşmiş Ştatların payına düşür. Müvafiq Çin bazarı 2,4 milyard dollarla dünyada 2-ci yerdə qərarlaşır. Növbəti 3 yeri uyğun olaraq Böyük Britaniya, Kanada və Fransa tutur [4].

Məqalədə fərdi məlumatların “qara bazarı”nın mahiyyəti, xüsusiyyətləri araşdırılır. “Qara bazar”da alqı-satqı obyektı olan məlumat və xidmət növləri, texnologiyalar və onların qiymət siyasəti şərh olunur. Həmçinin “qara bazar”da əldə edilən fərdi məlumatların hansı məqsədlər üçün istifadə edildiyi müəyyən edilir. Eyni zamanda, bu cür məlumatların qeyri-qanuni əldə edilməsi və satılmasının şəxsi, korporativ və milli maraqlar baxımından yaratdığı problemlər göstərilir.

II. FƏRDİ MƏLUMATLARIN “QARA BAZAR”ININ ƏSAS XİDMƏTLƏRİ

“Qara bazar” dedikdə, ənənəvi olaraq əmtəə və xidmətlərin qanunsuz olaraq mübadilə edildiyi yer başa düşülür. Elə əmtəə və xidmət növləri var ki, əslində, qanun onların satışına icazə verir. Lakin bəzi hallarda bu proses rəsmiləşdirilmədən (lisensiya almadan, vergi uçotuna dayanmadan, yaxud digər zəruri tələbləri ödəmədən) həyata keçirilir. Bu halda, müvafiq əmtəə və xidmətlərin alqı-satqısı “qara bazar” kateqoriyası altına düşür.

Elə əmtəə və xidmətlər də mövcuddur ki, onların satışı, ümumiyyətlə, qanunla qadağandır (məsələn, narkotika, insan alveri və s.). Fərdi məlumat sahiblərinin icazəsi olmadan onların alqı-satqısına da qanunla icazə verilmir. Ona görə də bu cür məlumatların qanunsuz alqı-satqısı da “qara bazar” kateqoriyasına aid edilir.

Fərdi məlumatların “qara bazar”ında konkret olaraq aşağıdakı xidmətlər təklif olunur [5]:

- real zaman rejimində mobil abonentin yerinin müəyyənəşdirilməsi;
- real zaman rejimində mobil abonentin əhatə edən şəxslərin müəyyən edilməsi;
- abonentin mobil telefonla ünsiyyət qurduğu şəxslərin siyahısı və digər məlumatlar;
- şəxsin hərəkəti zamanı olduğu coğrafi məkanlar və zamanlar və trayektoriyalar haqqında məlumatlar;
- şəxsə aid mülklər, bank hesabları və s. haqqında məlumatlar;
- İnternet xidmətlərindən istifadə zamanı provayderlərin serverlərində toplanan fərdi məlumatlar və s.

III. “QARA BAZAR”DA QIYMƏT SİYASƏTİ

“Qara bazar”da fərdi məlumatların qiymətləri insanların sosial statusundan və maliyyə imkanlarından asılı olaraq dəyişir. Bu “qara” əmək bazarının insan resurslarını formalaşdırmaq üçün xüsusi hakerlik kursları təşkil olunur. Əksər hallarda ödənişlər kriptovalyuta ilə aparıldığından bu cür kibercinayətkarlıqla mübarizə aparmaq çox çətin olur [1].

“Qara bazar”da fərdi məlumatların qiymətlərinin formalaşmasına təsir edən 4 əsas faktoru fərqləndirmək olar:

Birincisi, normal iqtisadiyyatda olduğu kimi, “qara bazar”da da tələb və təklif qanunları işləyir.

İkinci faktor hesab balansıdır - əgər kredit kartı kifayət qədər əlverişli kreditə malikdirsə, onun qiyməti baha olacaq.

Üçüncü faktor sədaqət kartlarının (ing. *cards loyalty*) yüksək bal stabilliyinə malik olmasıdır ki, bu da onların qiymətini qaldırır.

CƏDVƏL I. FƏRDİ MƏLUMATLARIN “QARA BAZAR”INDA TƏKLİF OLUNAN BƏZİ PROqram VƏ XİDMƏTLƏRİN QIYMƏTLƏRİ [5]

Proqram və ya xidmətin adı	Qiyməti
Akkauntların “sındırılması” proqramları	10-15\$
Parolun oğurlanması	50\$
Bank botnetləri	aylıq icarə - 750- 1200\$ aylıq dəstək – 150\$
Chrome , FireFox, Internet Explorer, Opera, Edge brauzerlərinin trafikləri	gündəlik – 2000\$ aylıq – 15000\$
Zərərli Android proqramının yüklənməsi	1500\$
DDoS-hücumlar	həftəlik 500-1200\$
Bankomat skimmerləri	700-1500\$
Dərsliklərin əldə edilməsi	5-50\$

Nəhayət, fərdi məlumatların dəyəri məlumatların təkrar istifadə edilməsindən asılı ola bilər. Yəni təkrar istifadə edə

bilmək imkanı həmin məlumatların dəyərini artırır. Məsələn, “qara bazar”ın müştərilər bir dəfə istifadə edilə bilən hədiyyə kartı ilə müqayisədə dəfələrlə istifadə edilə bilən kredit kartı üçün daha çox pul ödəyirlər.

Fərdi məlumatların qeyri-qanuni satışı bir çox hallarda onlayn qaydada həyata keçirilir. Bu cür qeyri-leqal xidməti həyata keçirmək üçün *DarkNet* gizli şəbəkəsindən geniş istifadə edilir. Bu şəbəkəyə xüsusi proqram təminatı vasitələrinin köməyi ilə giriş əldə etmək mümkündür. Həmin şəbəkəyə daxil olanların anonimliyini qorunur və onlardan tələb edilir ki, alqı-satqı bitkoin və digər kriptovalyutalar vasitəsi ilə həyata keçirilsin [5].

“Qara bazar”da, adətən, korporativ məlumatlar fərdi məlumatlardan daha qiymətli olur. Ona görə də hazırda müəssisə və təşkilatlarda toplanan və saxlanılan fərdi məlumatlar bədnəviyyətlilərin hədəfinə daha çox tuş gəlir.

Kibercinayətkarlar hər hansı oğurlanmış məlumatları bazara çıxarmazdan əvvəl onları çeşidləyirlər və inventarlaşdırırlar. Bahalı hesab etdikləri məlumatlara daha yüksək qiymət qoyurlar. Az dəyərli hesab etdiklərini isə bir yerə yığaraq toplu şəkildə kiçik ödənişlər müqabilində satışı çıxarırlar.

Hakerlər və “qara bazar” vasitəçiləri oğurlanmış fərdi məlumatların alqı-satqı proseslərini mümkün qədər sürətlə həyata keçirməyə çalışırlar. Çünki məlumat sahibləri oğurluqdan xəbər tutan kimi əks tədbirlər görməyə çalışırlar.

İstənilən fərdi məlumatlar aktual, mötəbər və dolğundursa, biznes üçün qiymətli resurs sayılır. Bütün bu xüsusiyyətlərə malik olan fərdi məlumatlar “qara bazar”da yüksək tələbatla malikdir. Lakin bu cür məlumatlar qanuni yollarla əldə edilmədiyinə görə onları dəqiqləşdirmək qeyri-mümkündür.

IV. “QARA BAZAR”DA FƏRDİ MƏLUMATLARI NƏ ÜÇÜN ALIRLAR?

“Qara bazar”da fərdi məlumatları müxtəlif fəaliyyət istiqamətləri üçün alırlar. Amma əksər hallarda son məqsəd eynidir – gəlir əldə etmək. Sadəcə olaraq, fərdi məlumatlar vasitəsi ilə qeyri-qanuni gəlir əldə etməyin yolları müxtəlifdir.

Big data analitiksinə əhəmiyyət verən şirkətlərin artması, marketing proseslərinin avtomatlaşdırılması üçün proqram təminatlarının hazırlanması “qara bazar”da fərdi məlumatlara olan tələbatı sürətlə artırmaqdadır. Rəqəmsal marketingdə aşağıdakı məqsədlərin reallaşdırılmasına xidmət edən məlumatlara daha çox tələbat hiss olunur [6]:

- onlayn şirkətlərin effektivliyinin artırılması;
- reklam şirkətlərinin dəqiq hədəflənməsi;
- istifadəçilərin profillərinin və maraqlarının analizi;
- ən yaxşı məhsulların və xidmətlərin işlənilməsi.

Əldə edilən fərdi məlumatların analizi əsasında kommersiya şirkətləri hədəf auditoriyasını müəyyənləşdirir, fərdiləşdirilmiş, ünvanlı reklam texnologiyalarını tətbiq edirlər.

Belə ki, insanlar İnternetdə müxtəlif axtarış sistemlərindən, sosial şəbəkələrdən, onlayn servislərdən istifadə edərkən onların arzu və istəkləri, ehtiyacları, həyat təzi, hobbiləri haqqında məlumatlar toplanır və onlar reklam-marketing fəaliyyəti üçün çox faydalı məlumatlara çevrilir.

Daha çox rast gəlinən hallardan biri də başqalarının kredit kartlarını, bank hesablarını və s. maliyyə məlumatlarını oğurlayaraq onların pullarının mənimlənməsidir. Bu cür məlumatların əldə edilməsi üçün fiziki və virtual mühitə xas olan müxtəlif texnologiyalardan istifadə edilir.

Bəzi hallarda fərdi məlumatlar saxta sənədlər düzəldib satmaq üçün lazım olur. Digər hallarda müəyyən insanların fərdi məlumatlarını ələ keçirdikdən sonra onları şantaj edərək pul tələb edirlər. Həmçinin kriminal qruplar kiminsə hansısa bahalı mülkü barədə məlumat əldə edərək onu ələ keçirmək üçün fəaliyyətə keçirlər.

Fərdi məlumatlar siyasi mübarizə predmeti də ola bilər. Belə ki, siyasi rəqiblər əks tərəfin fərdi məlumatlarını qeyri-qanun yolla əldə edərək onların siyasi nüfuzunu aşağı salmaq üçün istifadə edə bilərlər.

Fərdi məlumatlar xarici kəşfiyyat orqanları üçün siyasi-ideoloji məqsədlər üçün də istifadə edilə bilər. Bu halda fərdi məlumatlar milli təhlükəsizliyin obyektinə çevrilir.

V. “QARA BAZAR”IN YARATDIĞI PROBLEMLƏR

Fərdi məlumatların “qara bazar”ının formalaşması və inkişafı dövlət, müəssisə və təşkilatlar, vətəndaşlar üçün bir sıra problemlərə yol açır. Əvvəla, “qara bazar”a daxil olan fərdi məlumatlar qeyri-qanuni yollarla, kriminal üsullarla, hüquqi və fiziki şəxslərə ziyan vurmaqla əldə edilir. İkincisi, həmin fərdi məlumatlardan bir çox hallarda sağlam məqsədlər üçün deyil, zərərli məqsədlər üçün istifadə edilir.

Fərdi məlumatların oğurlanması onların sahibləri üçün bir sıra neqativ nəticələrə səbəb ola bilər. Aparılan bir sorğunun nəticələrinə görə, fərdi məlumatları oğurlanan şəxslərin 40%-i gecələr normal yata bilmədiklərini, 65%-i əsəb hissləri bildirlər. Rəyi soruşulanların 7%-i isə intihar etmək həddinə çatdıqlarını söyləyiblər. Oğurluq qurbanlarının 15%-i zərərini ödəmək üçün şəxsi əşyalarını satıblar, 7%-i isə bunun üçün kredit götürüblər [7].

Fərdi məlumatların oğurlanması biznes qurumlarına daha çox ziyan vurur. Faktlar göstərir ki, bu, şirkətlər üçün daimi bir riskdir və həmişə bu cür neqativ hallara qarşı hazır olmaq lazımdır.

Məlumat sızıntısı ilə qarşılaşan şirkətlər üçün bunun ən böyük maliyyə itkisi reputasiyanın itirilməsidir. Bu cür hallardan sonra şirkətlər gərək müştəri etimadını qaytarmaq, uzunmüddətli maliyyə təsirlərini azaltmaq üçün zəruri tədbirlər görsün. Məlumat sızıntılarının əksəriyyəti kiberhücumlar nəticəsində baş verir. Bu cür insidentləri araşdırmaq və aşkar çıxarmaq böyük vaxt aparır.

Şirkətlər etiraf edirlər ki, məlumat sızmalarının müəyyənəşdirilməsi və qarşısının alınmasına nə qədər çox vaxt sərf edilirsə, bir o qədər xərc tələb edilir. Bu cür xərclərin

həcmi ilbəil artır. Bu cür təhlükələrin aşkarlanması və qarşısının alınması üçün şəxsi təcrübədən istifadə etmək və texnoloji vasitələrə investisiya qoyuluşlarını artırmaq lazımdır [3].

Səhiyyə və maliyyə xidmətləri kimi güclü tənzimlənən sahələrdə məlumat sızmaları daha baha başa gəlir. Çünki bu sahələrdə müvafiq insidentlər nəticəsində reputasiyanın və müştərinin itirilməsi səviyyəsi və ehtimalı daha yüksək olur.

Fərdi məlumatlar “qara bazar” vasitəsi ilə xarici kəşfiyyat orqanlarının əlinə düşərsə, bu halda milli təhlükəsizlik üçün ciddi problemlər yarana bilər.

NƏTİCƏ

Fərdi məlumatların “qara bazarı” ilə effektiv mübarizə aparmaq üçün müvafiq qanunvericiliyin təkmilləşdirilməsi, kiberincayətkarlıqla mübarizə tədbirlərinin gücləndirilməsi vacibdir.

Texnoloji səviyyədə fərdi məlumatların mühafizəsinin gücləndirilməsi ilə bağlı müvafiq dövlət siyasətini həyata keçirən qurumların, eləcə də, vətəndaşlara müxtəlif xidmətlər göstərən müəssisə və təşkilatların üzərinə mühüm vəzifə düşür.

Vətəndaşların özləri fərdi məlumatlarının qayğısına qalmalı, onlarla düzgün davranmalı, virtual mühitin xüsusiyyətlərini nəzərə almalıdır. Onların informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması məsələsinə xüsusi diqqət yetirmək lazımdır.

Bunlarla yanaşı, fərdi məlumatların Big data ehtiyacları üçün səmərəli istifadəsi üçün onların şəxssizləşdirilməsi (adsızlaşdırılması) mexanizmlərinin işlənilib həyata keçirilməsi də zəruridir.

Hazırda müvafiq beynəlxalq hüquqi instansiyalarda insanların öz fərdi məlumatlarından gəlir əldə edə bilmələri üçün müvafiq hüquqi mexanizmlərin yaradılması məsələsi müzakirə olunur. Bunun üçün, ilk növbədə, hər kəsin öz fərdi məlumatlarına dair mülkiyyət hüququ əldə etməsi vacibdir.

Nəzərə almaq lazımdır ki, fərdi məlumatların xüsusi çəkiyə malik olduğu böyük verilənlər öz strateji əhəmiyyətinə, faydalarına görə neft ehtiyatları ilə müqayisə edilir. Deməli, ələ etmək lazımdır ki, həm insanların şəxsi toxunulmazlıq hüququ yüksək səviyyədə qorunsun, həm də onların fərdi məlumatlarından faydalı məqsədlər üçün istifadə etmək mümkün olsun.

İSTİNADLAR

- [1] R.Əliquliyev, R.Mahmudov, “Milli mentalitet kontekstində fərdi məlumatların həssaslığı və onların təhlükəsizliyinin təmin edilməsi məsələləri”, İnformasiya cəmiyyəti problemləri, 2019, №2, s. 117-128.
- [2] P. Samuelson, Privacy as intellectual property?, Stanford Law Review, 2000, pp. 1125–1173.
- [3] M.Nuncic, “The Black Market for Data”, <https://www.ontrack.com>
- [4] A.Fontinelle, “How Black Markets Work”, 2019, <https://www.investopedia.com>
- [5] Armor, “The Black Market Report”, 2018, 16 p.
- [6] S.Spiekermann, R.Böhme, “The challenges of personal data markets and privacy”, Electronic Markets, June 2015, <https://www.eprofing.springer.com/journals/printpage>
- [7] G.Cook, “How Much Is My Identity Worth on the Black Market?”, <https://www.findreviews.com>

**CHARACTERISTICS AND CHALLENGES OF PERSONAL
DATA “BLACK MARKET”**

Rasim Mahmudov

Institute of Information Technology of ANAS, Baku, Azerbaijan

rasimmahmudov@gmail.com

Abstract— The essence and characteristics of personal data “Black market” are explored in this article. The article interprets the types of information and services, technologies and pricing policies that are

the subjects of the sale on the “Black market”. It also defines the purpose of the use of the personal data obtained in the “Black market”. Moreover, the problems caused by the illegal acquisition and sale of such information, in terms of personal, corporate and national interests, are highlighted.

Keywords— *personal data; personal data “Black market”; price of personal data; personal data theft*

Sosial şəbəkələrdə saxta profillərin aşkarlanması metodları haqqında

Yadigar İmamverdiyev¹, Xəyalə Əhmədova²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹yadigar@iit.science.az, ²ehmedovaxeyale.97@mail.ru

Xülasə— Sosial şəbəkələr genişləndikcə onların insanlar üzərində təsiri də artmaqdadır. Sosial şəbəkələrdə fərdi məlumatlar da paylaşıldığından istifadəçilərə yönəlmiş təhdidlərdən olan saxta profillər bu məlumatlara təhlükə yaradır. Real istifadəçidən birbaşa və ya dolayı yolla alınan fərdi məlumatlar daha sonra müxtəlif məqsədlər üçün (məsələn, şantaj yolu ilə pul tələb etmək, həmin şəxs adından başqa bir profil yaradıb onun adından yalan məlumatlar yaymaq və s.) istifadə edilir. Saxta profillərin məqsədləri gün keçdikcə daha təhlükəli hal aldığından onların təyin edilməsi günümüzün aktual məsələlərindən biridir. Bu məqalədə saxta profillərin növləri, saxta profillərin təyininə istifadə edilə biləcək əlamətlər, saxta profillərin təyininə məşin təlimi yanaşmaları və avtomatik aşkarlanma üçün təklif edilən yanaşmaya baxılmışdır.

Açar sözlər— sosial şəbəkə; saxta profil; trol profil; aşkar edilmə; məşin təlimi

I. GİRİŞ

Sosial şəbəkələr həyatımızın ayrılmaz parçasına çevrilmişdir. Belə ki dünya əhalisinin 7.7 milyard olduğunu nəzərə alsaq, onlardan 2 milyarda yaxını sosial media istifadəçisidir. Təbii ki, bunun səbəblərindən biri saxta hesab istifadəsidir. 2018-ci ildə Facebook sosial şəbəkəsində edilmiş araşdırmaya əsasən 500 milyon qadın adı altında fəaliyyət göstərən saxta profil vardı. Bu tip saxta profil açmaqda bədnəyyətlinin məqsədi çirkli pulların yuyulması, qaçaqmalçılıq və bəzi digər anti-sosial davranışlar ola bilər [1]. Bu zaman baxılacaq əsas məsələlərdən biri ilk növbədə paylaşım edən cinsini müəyyən etməkdir. Bu halda, adətən, Təbii Dilin Emalı (ing. Natural Language Processing, NLP) texnologiyaları istifadə edilir.

Sosial şəbəkələrdə əks cinsin adı altında fəaliyyət göstərən saxta profillərlə yanaşı daha mürəkkəb işlər icra edən saxta profil növləri də vardır. Saxta profillərdən insanları manipulyasiya etmək üçün də istifadə edilir. İnsanları idarə etməkdə, yönləndirməkdə birinci addım onların fikirlərinə təsir etməkdir. Bu məqsədlə sosial şəbəkələrdən istifadə edilir. Sosial şəbəkələrdən zərərli məqsədlər üçün istifadə edilməsinin başlıca səbəbi bu platformaların geniş izləyici kütləsinə malik olmasıdır.

II. SOSIAL ŞƏBƏKƏLƏRDƏ BƏZİ TƏHDİDLƏR

Sosial şəbəkələrin funksionallığı artdıqca ondan istifadə edən insanların sayı da artır, bu isə sosial şəbəkələrin daha da böyüməsinə təkan verir. 2019-cu il üçün ən böyük 7 sosial şəbəkə arasında aktiv istifadəçi sayı Facebook üçün 2.38 milyard, Twitter üçün 321 milyon, LinkedIn üçün 303 milyon, Instagram üçün 1 milyard, Snapchat üçün 330 milyondan artıq, Pinterest üçün 291 milyon, Reddit üçün isə 330 milyon olmuşdur. Bu saylar sosial medianın yetərinə böyük izləyici kütləsinə sahib olduğunu göstərir [2].

Sosial şəbəkələrdən istifadə zamanı üzləşilən təhdidlər aşağıdakılardır:

- *Sosial mühəndislik* – kiber cinayətkarların zamanla hədəf təşkilatın işçilərlə qurduğu əlaqələr nəticəsində hədəf təşkilat haqqında konfidensial məlumatların ələ keçirilməsi məqsədilə ən geniş istifadə edilən sosial media təhdididir.
- *Fişinq hücumları* – pul və ya şəxsi məlumatların oğurluğu üçün istifadə edilən, əsasən, tanışlıq yönümlü sosial şəbəkələrdə geniş yayılmış təhdid növüdür.
- *Saxta hesablar* – kimi və ya nəyisə gözəndən salmaq, nüfuz qazandırmaq, insanları manipulyasiya etmək, saxta xəbər yaymaq kimi məqsədlərin icrası üçün istifadə edilən təhdid növüdür.
- *Məşhurların adından sui-istifadə* – Məşhur şəxs adından saxta profil yaradılaraq onun adından saxta paylaşımalar edilməsi və ya izləyici sayının artırılması üçün istifadə edilən təhdid növüdür.
- *Saytın ələ keçirilməsi* – bədnəyyətlinin zərərli kodlar yerləşdirdiyi reklamları sosial şəbəkədə yayması, saxta məlumat paylaşması, öz gücünü sübut etməsi kimi bir sıra zərərli məqsədləri icra etmək üçün yerinə yetirdiyi təhdid növüdür.
- *Spam və zərərli proqram təminatının yayılması* – Twitter, Facebook və Instagram kimi sosial şəbəkələr spam və zərərli proqram təminatlarının yayılması üçün ideal platformalardır. Kiber cinayətkarlar, əsasən, qısa uzunluqlu URL istifadə etməklə öz zərərli linklərini gizlədirlər ki bu da saytın qanuni və ya zərərli olmasının ayırd edilməsini

çətinləşdirir [3].

III. SAXTA PROFİLLƏRİN NÖVLƏRİ

Sosial şəbəkələrdə fəaliyyət göstərən saxta profilləri ümumi şəkildə üç böyük qrupa bölmək olar:

- insan tərəfindən yaradılan saxta profillər;
- proqram tərəfindən yaradılan saxta profillər;
- yarı insan, yarı proqram tərəfindən yaradılan saxta profillər (Cyborgs).

İnsan tərəfindən yaradılan saxta hesablara trol profillər, proqram tərəfindən yaradılan saxta profillərə botlar misal olaraq göstərilir. Cyborg-lar isə insan tərəfindən yaradılıb, sonrakı fəaliyyəti avtomatlaşdırılmış saxta profillərdir [4].

Sosial şəbəkələrdə olan saxta profillər yaradılma və istifadə tərzinə görə aşağıdakı kimi təsniflənirlir:

- *Ələ keçirilmiş profillər* – real istifadəçinin profilinin oğurlanması nəticəsində fəaliyyət göstərən saxta profil növüdür.
- *Klonlanmış profillər* – real profilin nüsxəsinin yaradılması nəticəsində fəaliyyət göstərən saxta profil növüdür. Real profilin yaradıldığı sosial şəbəkədə onun verilənlərindən istifadə edilərək yaradılan profil saytdaxili, fərqli sosial şəbəkədə yaradıldıqda isə saytlarası klon profil adlanır.
- *Kuklalar* – saxta ad altında özünü əslində mövcud olmayan bir şəxs kimi göstərərək kimi və ya nəyisə gözdən salmaq, nüfuzunu artırmaq üçün istifadə edilən saxta profil növüdür.
- *Sibil hesablar* (ing. *Sybil Accounts*) – bir şəxs tərəfindən yaradılan birdən çox profilin əl ilə idarə olunması nəticəsində fəaliyyət göstərən saxta profil növüdür.
- *Botlar saxta profil kimi* – fəaliyyəti Sibil hesablara oxşar, spam, bəyənmə, təsir, botnet kimi növləri olan saxta profil növüdür. Sibil hesablardan fərqli olaraq insan tərəfindən deyil, avtomatik idarə olunur [5].
- *Trol profillər* – qarşıya qoyulmuş hədəfə nail olmaq üçün sistemli şəkildə “troll fabriki” şəkildə fəaliyyət göstərən saxta profil növüdür. Trol fermalara misal olaraq 2016-cı ildə ABŞ-da keçirilən prezident seçkilərinə təsiri olan İnternet Araşdırma Agentliyini (ing. Internet Research Agency, IRA) göstərmək olar [6].

IV. SOSIAL ŞƏBƏKƏLƏRDƏ SAXTA PROFİLLƏRİN AŞKARLANMASINDA MAŞIN TƏLİMİ METODLARI

Sosial şəbəkələrdə saxta profillərin aşkarlanması problemlərindən biri tədqiqatçıların xüsusi tip saxta profilin aşkarlanması üçün metod işləməsidir.

Twitter sosial şəbəkəsində Spam botlarının aşkarlanması üçün Naïve Bayes (NB) və k ortalar (ing. K-means) klassifikasiya alqoritmləri tətbiq edilmişdir [7]. Facebook

sosial şəbəkəsində ələ keçirilmiş və sibil hesabların aşkarlanması üçün k ən yaxın qonşu (ing. K Nearest Neighbor, k-NN) və Əsas Komponent Analizi (ing. Principal Component Analysis, PCA) metodları istifadə edilmişdir [8]. Vikipediya sosial şəbəkəsində kukla hesabların aşkarlanması üçün Support Vector Machine (SVM) metodu tətbiq edilmişdir [9]. Facebook, Twitter, MySpace sosial platformalarında spam botlarının aşkarlanması üçün Random Forest alqoritm tətbiq edilmişdir [10].

[11]-də tədqiqatçılar Facebook sosial şəbəkəsində saxta profillərin aşkarlanması üçün “FBChecker” ağıllı sistemini təklif edilmişdir. Təklif edilən yanaşma 3 pillədən ibarətdir:

1. Facebook istifadəçi profillərindən “CRAWLER” adlı moduldan istifadə edilərək seçilmiş əlamətlərə uyğun məlumatların toplanması;
2. k-NN sxemi və filtrləmə operatorunun köməyi ilə ötürülmüş verilənlər probleminin həll edilməsi;
3. 4 supervizorlu öyrənmə alqoritminin: Qərar ağacı (ing. Decision Tree, DT), k-NN, SVM və NB təlim və tətbiqi.

Alqoritm tətbiqi zamanı profil şəkli, iş yeri, təhsil, yaşayış yeri, münasibət statusu və s. kimi əlamətlərdən istifadə edilmişdir.

K-NN sxeminin istifadəsilə ötürülmüş verilənlərin qiymətləndirilməsinin tətbiqi nəticəsində Accuracy Qərar ağacı DT üçün 0.965, k-NN üçün 0.84, SVM üçün 0.985, NB üçün 0.975 olmuşdur.

Filtrləmə operatorlarının köməyi ilə itkin verilənlərin istisna edilməsinin tətbiqi nəticəsində Accuracy DT üçün 0.946, k-NN üçün 0.844, SVM üçün 0.988, NB üçün 0.964 olmuşdur.

[12]-də müəlliflər sosial mediada kuklaların avtomatik aşkarlanması və qruplaşdırılması üçün SocksCatch adlanan model təklif edirlər. Model 3 mərhələdən ibarətdir:

1. Mərhələ verilənlərin toplanması və seçilməsi addımlarından ibarətdir.
2. Mərhələ əlamətlərin seçilməsi və maşın təlimi metodlarının tətbiqi addımlarından ibarətdir.
3. Mərhələ qraflar nəzəriyyəsi ilə istifadə etməklə eyni istifadəçi tərəfindən yaradılan kukla hesabların fəaliyyət və hesab əlamətləri əsasında qruplaşdırılması addımlarından ibarətdir.

Bu məqalədə müəlliflər İngilis vikipediyasında kukla və aktiv hesabların arasındakı fərqləri müəyyənləşdirmək üçün əlamətləri 3 qrupa: fəaliyyət davranışı, hesab fəaliyyətinə nəzərən digər hesabların davranışı, hesab xüsusiyyətləri bölürlər.

Seçilmiş əlamətlər əsasında təklif edilən proses üçün saxta profillərin aşkarlanmasında 6 maşın təlimi yanaşmasından SVM 92.6%, Random Forest 94.8%, NB 89.1%, k-NN 90.9%,

Bayesian network 89.1% və Adaptive boosting 92.6% accuracy göstərmişdir.

V. APARILMIŞ EKSPERİMENTLƏR

Aparılmış tədqiqat nümunələrindən göründüyü kimi saxta profillərin aşkarlanmasında maşın təlimi yanaşmaları, xüsusilə, Supervizorlu maşın təlimi yanaşmaları geniş istifadə edilir. Buna səbəb profillərin saxta və ya real olaraq sinifləndiriləcəyinin məlum olmasıdır.

Təcrübələr “Orange” proqram təminatında aparılmışdır. 2818 sayda profil (1337 saxta, 1481 real) status sayı, izləyici sayı, dostlar sayı, favorit sayı, izləyənlər sayı (ing. listed_count), cins kodu və dil kodu əlamətlərindən istifadə edilərək DT, NB və SVM alqoritmlərinin tətbiqi ilə klassifikasiya edilmişdir. DT tətbiqinin vizual nəticəsi şəkil 1-də göstərilmişdir.

Şəkil1. DT tətbiqinin vizual görüntüsü

DT tətbiqi nəticəsində ‘statusların sayı’ əlamətinin profilin saxta olub olmamasının müəyyən edilməsində ən vacib əlamət olması müşahidə edilmişdir. Belə ki, status sayı ağacın kökü olaraq qəbul edilmişdir. Status sayı 83-dən böyük olan profillər 98,5% göstəricisi ilə real profil olaraq qəbul edilmişdir. Daha sonra “dil kodu” əlamətindən istifadə edilərək müşahidə edilmişdir ki, dil kodu 1-dən böyük olan profillər real profillər, digərləri saxtadır.

NB tətbiqinin Scatter Plot vasitəsilə vizual nəticəsi şəkil 2-də verilmişdir. Qrafikdə status sayı ilə dostlar sayı arasında asılılıq təsvir edilmişdir. Qırmızı nöqtələr real, mavi nöqtələr saxta profilləri əks etdirir. Qrafikə əsasən qeyd etmək olar ki, real profillər saxta profillərə nisbətən daha çox status paylaşır.

SVM tətbiqinin Scatter Plot vasitəsilə vizual nəticəsi şəkil 3-də təsvir edilmişdir. Qrafikdə izləyici sayının status sayından asılılığı əks etdirilmişdir. Qrafikə əsasən qeyd etmək olar ki, izləyici və status sayı çox olan profillər real profillər olaraq qəbul edilə bilər.

DT, NB və SVM üçün olan xəta matrisləri (ing. confusion matrix) uyğun olaraq şəkil 4-6-da verilmişdir.

Şəkil2. NB tətbiqinin vizual görüntüsü

Şəkil 3. SVM tətbiqinin vizual görüntüsü

	Predicted		Σ
	fake	real	
	fake	real	
Actual	1315	22	1337
	9	1472	1481
Σ	1324	1494	2818

Şəkil 4. DT tətbiqi nəticəsində əldə edilən xətlər matrisi

	Predicted		Σ
	fake	real	
	fake	real	
Actual	1326	11	1337
	8	1473	1481
Σ	1334	1484	2818

Şəkil 5. NB tətbiqi nəticəsində əldə edilən xətlər matrisi

		Predicted		
		fake	real	Σ
Actual	fake	1198	139	1337
	real	73	1408	1481
Σ		1271	1547	2818

Şəkil 6. SVM tətbiqi nəticəsində əldə edilən xətarlar matrisi

Tətbiq edilmiş modellərin müqayisəsi cədvəl 1-də əks etdirilmişdir.

CƏDVƏL I. Tətbiq edilmiş modellərin müqayisəsi

Model	AUC	CA	F1	Precision	Recall
DT	0.987	0.989	0.989	0.989	0.989
SVM	0.972	0.925	0.925	0.926	0.925
NB	0.999	0.993	0.993	0.993	0.993

Nəticələrdən də göründüyü kimi saxta profillərin qeyd edilmiş bazada seçilmiş əlamətlər əsasında aşkarlanması üçün tətbiq edilən maşın təlimi yanaşmalarından ən yaxşı nəticə göstərən Naive Bayes, ən pis nəticə göstərən isə SVM olmuşdur.

NƏTİCƏ

Tədqiqatçıların, əsasən, saxta profilin hər hansısa bir növünü aşkarlamaq üzrə tədqiqatlar aparmalarına baxmayaraq, sosial şəbəkələrdə saxta profillərin ümumi şəkildə təyin edilməsi üçün də bir sıra tədqiqatlar vardır. Burada əsas məsələ sosial şəbəkədə olan profillərin saxta və ya real profil qrupuna daxil edilməsidir. Bu məqsədlə, əsasən, klassifikasiya metodlarından istifadə edilir. Buna səbəb profilləri daxil edəcəyimiz qrupların əvvəlcədən məlum olmasıdır. Yəni baxılan məsələ profili klassifikasiya edib hansı qrupa daxil olacağını müəyyən etməkdir.

Bununla yanaşı klasterizasiya alqoritmləri də saxta profillərin aşkarlanmasında istifadə olunmaqdadır. Saxta profillərin təyin edilməsində klasterizasiya alqoritmlərinin klassifikasiya alqoritmlərinə nisbətən zəif nəticə göstərməsinə baxmayaraq, onların da üstün cəhətləri vardır. Məsələn, saxta profillərin aşkarlanmasında klassifikasiya alqoitmlərinin tətbiqi zamanı profillər tək-tək analiz edilib qruplara daxil edilirdisə klasterizasiya məsələsində oxşar şəkildə fəaliyyət göstərən və ya oxşar əlamətlərə sahib profillər toplu şəkildə qruplaşdırılır.

İSTİNADLAR

- [1] R. Raturi, “Machine Learning Implementation for Identifying Fake Accounts in Social Network”, *International Journal of Pure and Applied Mathematics*, vol. 118(20), pp. 4785-4797, 2018.
- [2] “The 7 Biggest Social Media Sites in 2019”

<https://www.searchenginejournal.com/biggest-social-media-sites/308897/>

- [3] “Security threats we face while using social media” <https://www.novalisit.com/2019/04/security-threats-we-face-while-using-social-media/>
- [4] E. Van Der Walt, J. Eloff, “Using machine learning to detect fake identities: bots vs humans”, *IEEE Access*, vol. 6, pp. 6540-6549, 2018.
- [5] M. A. Wani, S. Jabin, G. Yazdani, et al “Sneak into devil’s colony – A study of fake profiles in Online Social Networks and the cyber law”, 2018.
- [6] C. Llewellyn, L. Cram, A. Favero, et al “For whom the bell trolls: Troll behaviour in the Twitter Brexit debate”, 2018.
- [7] J. S. Alowibdi, U. A. Buy, S. Y. Philip, S. Ghani and M. Mokbel, “Deception detection in Twitter”, *Social Network Analysis and Mining*, vol. 5(1), pp. 1-16, 2015.
- [8] B. Viswanath, M. A. Bashir, M. Crovella, et al, “Towards detecting anomalous user behavior in online social networks”, In 23rd USENIX Security Symposium, pp. 223-238, 2014.
- [9] A. H. Wang, “Detecting spam bots in online social networking sites: a machine learning approach”, In *Data and Applications Security and Privacy XXIV*, pp. 335-342, Heidelberg, 2010.
- [10] G. Stringhini, C. Kruegel, G. Vigna, “Detecting spammers on social networks”, *Proceedings of the 26th Annual Computer Security Applications Conference*, pp. 1-9, December, 2010.
- [11] M. B. Albayati, A. M. Altamimi, “An Empirical Study for Detecting Fake Facebook Profiles Using Supervised Mining Techniques”, *Informatica*, vol. 43(1), 2019.
- [12] Z. Yamak, J. Saunier, L. Vercouter, “SocksCatch: Automatic detection and grouping of sockpuppets in social media”, *Knowledge-Based Systems*, 149, pp. 124-142, 2018.
- [13] “Fake-Profile-Detection-using-ML” <https://github.com/harshitkgupta/Fake-Profile-Detection-using-ML>

ABOUT METHODS OF FAKE PROFILES DETECTION IN SOCIAL NETWORKS

Yadigar İmamverdiyev¹, Khayala Ahmadova²

^{1,2}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹yadigar@iit.science.az, ²ehmedovaxeyale.97@mail.ru

Abstract– As social networks expand, so does their influence over people. Because personal information is also shared on social networks, fake profiles, which are threats to users, endanger this information. Personal information obtained directly or indirectly from a real user is then used for various purposes (for example, extorting money, creating another profile on behalf of that person, spreading false information on his behalf, etc.). As the purpose of fake profiles becomes more and more dangerous, their identification is one of the most pressing issues of our day. This article looks at the types of fake profiles, the features that can be used to identify fake profiles, the machine learning approach to fake profiles, and the proposed approach for automatic detection.

Keywords– *social network; fake profile; troll profile; detection; machine learning*

О защите персональных данных в системах, реализуемых на основе концепции Industry 4.0

Тахмасиб Фаталиев¹, Шакир Мехтиев²

^{1,2}Институт информационных технологий НАНА, Баку, Азербайджан

¹depart3@iit.science.az, ²shakir@iit.science.az

Аннотация– Промышленные революции играют важную роль в развитии критических систем. Четвертая промышленная революция, или Industry 4.0 произвела кардинальные изменения в этой области, и в большей степени обязана появлению и развитию Интернета вещей, киберфизических систем, искусственного интеллекта, робототехники и других передовых технологий. Они привели к созданию полностью автоматизированного цифрового производства, управляемого интеллектуальными системами в режиме реального времени в постоянном взаимодействии с внешней средой. По сути, эти технологии делают производственную систему “умной сетевой фабрикой”, где вся деятельность контролируется цифровым способом, и, в результате, использование финансовых и материальных ресурсов становится более эффективным. Наряду с этим, увеличение сбора и обработки больших объемов данных, а также высокая степень автономности и децентрализации для таких систем являются факторами, которые могут стать проблематичными в контексте защиты данных и, в первую очередь, персональных данных. Данная работа посвящена вопросам защиты персональных данных в системах нефтегазового комплекса, реализуемых на основе концепции Industry 4.0. Рассмотрены концептуальные задачи и даны рекомендации по их решению.

Ключевые слова– промышленная революция; Industry 4.0; персональные данные; нефтегазовый комплекс; риск; защита данных

I. ВВЕДЕНИЕ

Отличительной чертой информационного общества является взрывной рост данных. Интернет, наука, медицина, финансы, розничная торговля, видеонаблюдение и другие отрасли создали огромное количество данных. На производстве различные контрольно-измерительные приборы производят бесконечный поток данных. Наряду с этим, интеллектуализация производства при широкой степени интеграции сетевых и коммуникационных технологий увеличила потенциал стороннего доступа и, следовательно, в этом контексте возник также целый ряд проблем в отношении вопросов безопасности информации и связи. Благодаря интеграции новых методов сбора и анализа данных, а также путем тщательного мониторинга опыта клиентов и их предпочтений производители стали собирать их персональные данные (ПД) об использовании своих продуктов в целях удовлетворения растущих потребностей конечных потребителей. Т.е. среди всех

данных особая роль стала отводиться ПД. Многие технологические компании (Facebook, Google) и организации собирают, обрабатывают, используют и распространяют ПД без ограничений. Кроме того, некоторые предприятия обмениваются данными пользователей с третьей стороной. И в большинстве случаев пользователь даже не осознает моменты, когда его ПД используются без согласия. По оценкам специалистов данные являются ценным корпоративным ресурсом компаний, и руководители должны делать все, чтобы защитить собственные данные и обеспечить конфиденциальность данных сотрудников и клиентов [1]. Вышеуказанные проблемы не обошли стороной и нефтегазовый комплекс (НГК). В данной работе освещаются некоторые вопросы защиты ПД в технических системах НГК, реализованных на основе концепции Industry 4.0.

II. INDUSTRY 4.0 И ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

Существующий научно-технический уровень современной цивилизации в большой степени связан с произошедшими на протяжении последних двухсот пятидесяти лет промышленными революциями (ПР). До сих пор различали четыре ПР. В настоящее время мы находимся в стадии четвертой ПР, известной теперь как Industry 4.0, и перманентно переходящей в Industry 5.0. Industry 4.0 стала возможной благодаря таким прогрессивным технологиям, как системы радиочастотной идентификации (Radio Frequency IDentification, RFID), беспроводные сенсорные сети (Wireless Sensor Networks, WSN), системы межмашинного взаимодействия (Machine-to-Machine, M2M), Интернет вещей (Internet of Things, IoT), большие данные (Big data), а также облачные сервисы (cloud computing), озеро данных (data lake) и искусственный интеллект Artificial Intelligence, AI [2]. В Industry 4.0 цифровизация и объединение технических систем сделали возможным слияние физического и виртуального мира в области производства и логистики в так называемые киберфизические системы (КФС). Технические системы приобрели способность автономно обмениваться друг с другом данными и, таким образом, оптимизировать протекание процессов. При этом, в Industry 4.0 особая роль отводится созданию сенсорных сетей в промышленном секторе. Так называемые сенсоры 4.0 являются не только источниками первичных измерительных данных, но и предоставляют

децентрализованные вычислительные мощности и программируемость [3, 4].

Отметим, что в Industry 4.0 физические объекты и процессы контролируются и управляются посредством КФС. Важно представить, что здесь могут использоваться объединенные или индивидуальные системы управления. Данные с сенсоров, такие как температура, давление, плотность вещества и др. используются в системе для контроля и управления. Увеличение сбора и обработки больших объемов данных, а также высокая степень автономности и децентрализации управляющих систем в Industry 4.0 стали факторами, которые оказали влияние и на кибербезопасность. Традиционно кибербезопасность направлена на защиту людей и организаций от таких угроз, как вредоносные программы, атаки социальных инженеров, порча веб-сайтов и т.д. [5]. В последнее время наблюдается рост сложности и интенсивность кибератак, которые ориентированы на финансовые преступления, промышленный шпионаж и время от времени даже направлены против правительств и критически важной инфраструктуры. В эпоху Industry 4.0 организации сильно связаны со своими интеллектуальными устройствами и сетями. Это представляет собой очень выгодную цель для киберпреступников, которые находят гораздо более простые точки входа в сети и устройства. Кибератаки на критически важную инфраструктуру и стратегические промышленные сектора стали более частыми и изощренными. Они не только приводят к нарушению нормального функционирования общества, но и наносят вред моральному духу пострадавших стран [6]. Например, Украина столкнулась с множеством таких атак на энергосистему, что привело к отключению электроэнергии в некоторых регионах.

Непрерывное совершенствование электронных технологий привело к тому, что в современном обществе, как на уровне правительств, так и в гражданском обществе, стали осознавать риски, создаваемые от использования личной информации. Прогресс науки и техники расширил жизненное пространство людей и дал им большую свободу поведения. Облачные вычисления позволяют хранить личную информацию вдали от нашего телефона, ноутбука или любых других персональных терминалов, что позволяет пользователю получать доступ к информации из любого места на любом устройстве. Наоборот, способность пользователя контролировать эту информацию значительно снизилась. Более того, мобильный интернет собирает информацию повсеместно, особенно персонализированную информацию, такую как контакты, фотографии и электронные письма. Однако, если популяризация облачных вычислений и мобильного интернета только усиливает сложность защиты информации на количественном уровне, то появление больших данных в настоящее время разрушает основу системы защиты личной информации с качественного уровня, что нельзя недооценивать. Например, в настоящее время технологии профилирования используются повсеместно для поиска скрытых закономерностей и взаимосвязей публики. Кроме того, они позволяют повторно идентифицировать личные данные, что делает

стратегию анонимизации менее эффективной и ставит под сомнение фундаментальный принцип защиты данных.

Функционирование структур нефтегазового комплекса, реализованного на основе концепции Industry 4.0, можно представить, как умное производство (smart manufacturing) [7], в котором риски в основном возникают также и в сфере обработки ПД, касающихся персонала и клиентов. Каждый случай сетевого взаимодействия между людьми и производственными и логистическими системами может привести к тому, что личные данные будут получены, обработаны и при определенных обстоятельствах переданы вместе с другими данными. Риски потери данных на умном производстве могут быть связаны и с системами помощи персоналу, такими как планшеты, смартфоны, очки виртуальной и дополненной реальности и портативные терминалы данных. Они могут помочь персоналу избежать ошибок, предоставив им соответствующую справочную информацию, т.е. используются исключительно в производственных процессах. Однако, в этом случае ПД, например, координаты местоположения могут быть отслежены, и тогда необходимо принять защитные меры, начиная с технического уровня.

В Общем регламенте по защите данных, известном как General Data Protection Regulation (GDPR), предложен ряд мер по защите ПД в контексте внедрения Industry 4.0 [8]. Также в трудовых законодательствах ряда стран предусматриваются различные меры наказаний и штрафов по ненадлежащему использованию ПД. Так, в Трудовом кодексе Азербайджана предусмотрены организационные, физические и технические (аппаратные) меры для защиты личной информации от несанкционированного и случайного доступа, уничтожения, изменения и копирования.

III. ХАРАКТЕРИСТИКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И РИСКИ БЕЗОПАСНОСТИ В НЕФТЕГАЗОВОМ СЕКТОРЕ

Рассмотрим общие характеристики ПД, которые являются универсальными и применимы, в том числе, и в НК. Согласно GDPR к ПД можно отнести любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу. Статистические данные, включая данные, относящиеся к физическим лицам, не считаются ПД при условии, что они действительно анонимны, то есть физические лица не могут быть идентифицированы.

Любые операции, выполняемые с ПД или с наборами ПД, независимо от того, выполняются ли они автоматическими средствами, такими как сбор, запись, организация, структурирование, хранение, адаптация или изменение, поиск, консультация, использование, раскрытие путем передачи, распространение или иное предоставление, выравнивание или комбинация, ограничение, удаление или уничтожение – квалифицируется как обработка ПД. Таким образом, очевидно, что проблемы с ПД могут возникать во всех сферах деятельности и во всех аспектах жизни в целом, поскольку информацию, с помощью которой можно

идентифицировать физических лиц, можно найти практически везде.

На основании проведенного анализа можно выделить следующие категории ПД:

А. Личные данные— к ним относятся:

- контактная информация— инициалы, название компании, должность, рабочие и мобильные телефоны, рабочий и личный адрес электронной почты и почтовый адрес.
- Профессиональные данные— сведения об истории работы и карьеры, образовании и профессиональном членстве, опубликованные статьи, а также сведения по страхованию и пенсионному обеспечению.
- Финансовая информация— к этой подгруппе личных данных можно отнести налоги, платежные ведомости, инвестиционные интересы, пенсии, активы, банковские реквизиты, записи о банкротстве.

Б. Чувствительные ПД:

- Документы, удостоверяющие личность, которые могут выявить расу, религию или этническое происхождение, политические взгляды.
- Любая информация, раскрывающая данные о здоровье или данные, касающиеся личной жизни физического лица, информация о нахождении под следствием, осуждении за совершение преступления.
- Биометрические данные.

В. Данные, защищенные правом интеллектуальной собственности (авторское право, закон о товарных знаках, закон о базе данных, патентный закон) и полученные на основе обработки географических местоположений.

Методы защиты ПД должны быть направлены на устранение утечек или на уменьшение негативных последствий. К наиболее известным и распространенным видам утечек данных можно отнести следующие их виды:

Умышленные утечки: основной их причиной становятся действия сотрудников, имеющих доступ к секретам легально, в силу своих служебных обязанностей.

Кража информации (извне): взлом компьютера с помощью вредоносных программ и хищение информации с целью использования в корыстных интересах (хакерские атаки).

Кражи носителей данных: преднамеренные кражи ноутбуков, смартфонов, планшетов и съемных носителей данных в виде флеш-памяти, жестких дисков.

Случайные утечки: происходят из-за потери носителей данных (флеш-памяти, ноутбуков, смартфонов и т.п.) или ошибочных действий сотрудников организации. Такой вид утраты случается в результате ошибочного размещения конфиденциальной информации в Интернет.

Социальная инженерия: основана на социальных и психологических приемах, позволяющих так называемым

социальным хакерам получить доступ к закрытым данным внутри организации от ничего не подозревающих сотрудников, попавших на их уловки.

Следует отметить, что, независимо от вида деятельности, любая организация, которая в своей деятельности обрабатывает ПД, обязана предпринять комплекс административных и технических мер, направленных на их защиту. Политика безопасности предприятия должна обеспечивать необходимые механизмы управления рисками безопасности.

IV. НЕКОТОРЫЕ КОНЦЕПТУАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В INDUSTRY 4.0

Рассмотрим основные проблемы, возникающие в технических системах промышленности, в том числе и нефтегазового сектора, реализованных на основе концепции Industry 4.0. К ним можно отнести следующие группы проблем:

1. *Производственно-технологические проблемы*— управление и оптимизация производственных процессов, внедрение сенсоров на новых физических принципах, техническое обслуживание и др.
2. *Информационно-технологические проблемы*— автоматизация технологических процессов, системы типа SCADA, Интернет вещей, беспроводные сенсорные сети, искусственный интеллект, виртуальная и дополненная реальности.
3. *Разработка и внедрение программных средств.*
4. *Сбор, обработка и передача данных, Big data аналитика.*
5. *Вопросы безопасности*— непрерывная и устойчивая деятельность производственных циклов, экологическая безопасность, охрана жизни и здоровья персонала, информационная безопасность предприятий и защита ПД.

Каждая из рассмотренных проблем является сложной и ответственной задачей, требующей отдельных исследований. Рассмотрим часть проблем, которые могут возникнуть из-за уязвимостей в информационной безопасности ПД на предприятиях НГК, реализованных на основе концепции Industry 4.0.

Здесь деструктивная деятельность может иметь значительные негативные последствия, в особенности, в странах, имеющих существенную нефтегазовую составляющую. Эти действия направлены как на сотрудников компаний, так и на информационную безопасность компаний. В первом случае это могут быть действия преступных группировок с целью кражи денег с банковских счетов, шантаж с вымогательством денег, дискредитация. Во втором случае через ПД атакам подвергается информационная безопасность компаний. Применительно к нефтегазовому сектору атакам подвергаются как материальные, так и нематериальные активы компаний. Например, используя чувствительные ПД ключевых сотрудников, посредством их шантажа можно вызвать проблемы с оборудованием вплоть до остановки процесса добычи. Рискам подвергаются также

производственные и технологические процессы. В случаях осуществления подобных сценариев кибератак возможные аварии и загрязнения окружающей среды могут нанести миллионные убытки и урон репутации компании и их продукции и вызвать возрастающий общественный резонанс. На основе обработки данных о географическом положении сотрудников компании можно получить сведения о перспективных месторождениях нефти и газа. Также в результате утечек и кражи ПД можно получить конфиденциальные сведения коммерческого характера, о тендерной деятельности, данные договоров с партнерами и подрядчиками, условия работы и др. Возможный ущерб от таких утечек может выражаться в упущенной выгоде в результате испорченного имиджа; в компенсации по судебным искам; в снижении котировок акций; в стоимости проигранных тендеров и в других финансовых потерях. Таким образом, резюмируя вышеизложенное, отметим, что известные методы защиты данных, также применимы и к ПД. Среди них обычно выделяют четыре основные группы методов: правовые, организационные, технические, программно-аппаратные.

На любом объекте Industry 4.0 должна действовать политика безопасности. Одной из составных частей политики безопасности должно быть обеспечение защиты ПД. Политика безопасности должна быть разработана с учетом требований международных норм, стандартов и должна соответствовать внутригосударственным правовым актам, нормативным документам и законам. Особенно следует отметить, что в существующем законодательстве могут быть отражены не все аспекты в области защиты ПД. Учитывая динамичный характер развития современных ИКТ и их возросшее влияние во всех сферах деятельности, может потребоваться коррекция как существующих законов, так и методов защиты ПД.

ЗАКЛЮЧЕНИЕ

Защита ПД в структурах НГК, реализуемого на основе концепции Industry 4.0, играет важную роль в производственной сфере и обеспечении конкурентоспособности. Проведенный анализ в этой области показал, что исследуемая задача является критичной и актуальной. Каждый случай сетевого взаимодействия между людьми и производственными и логистическими системами может привести к тому, что ПД будут получены, обработаны и при определенных обстоятельствах переданы вместе с другими данными. При этом резко возрастают риски утечек ПД и случайное или преднамеренное их использование в корыстных целях. Инструменты информационных-коммуникационных технологий могут помочь персоналу избежать ошибок, предоставив им соответствующую информацию. Однако, предоставляемые ПД могут использоваться исключительно для оптимизированного планирования и управления, но не для мер, касающихся трудового законодательства. Это также необходимо учитывать при использовании новых технологий в производственных процессах. Если данные персонала или клиента могут быть

отслежены, необходимо принять эффективные защитные меры.

БЛАГОДАРНОСТИ

Данная работа выполнена при финансовой поддержке Фонда науки Государственной нефтяной компании Азербайджана SOCAR- **Контракт № 03 LR-AMEA.**

ЛИТЕРАТУРА

- [1] “Compliance in the Era of Globetrotting Data”. <https://www.intel.com/content/www/us/en/business/enterprise-computers/gdpr-compliance.html>
- [2] Y. Lu, “Industry 4.0: A survey on technologies, applications and open research issues”, *Journal of Industrial Information Integration*, No. 6, pp. 1–10, 2017.
- [3] A. Schütze, N. Helwig, and T. Schneider, “Sensors 4.0– smart sensors and measurement technology enable Industry 4.0”, *Journal of Sensors and Sensors Systems*, No. 7, pp. 359–371, 2018.
- [4] T. Kh. Fataliyev, Sh. A. Mehdiyev, “Analysis and new approaches to the solution of problems of operation of oil and gas complex as cyberphysical system”, *International Journal of Information Technology and Computer Science (IJITCS)*, Vol. 10, No. 11, pp. 67–76, 2018.
- [5] J. Jang-Jaccard, S. Nepal, “A survey of emerging threats in cybersecurity”, *Journal of Computer and System Sciences*, Vol. 80, Issue 5, pp. 973–993, 2014.
- [6] Т. Фаталиев, Ш. Мехтиев, “Вопросы обеспечения энергетической безопасности инфраструктуры электронной науки”, 4-я Республиканская конференция по информационной безопасности, сс. 105–108, 2018.
- [7] T. Kh. Fataliyev, Sh. A. Mehdiyev, “Integration of cyber-physical systems in e-science environment: state-of-the-art, problems and effective solutions”, *International Journal of Modern Education and Computer Science (IJMECS)*, Vol.11, No. 9, pp. 35–43, 2019.
- [8] General Data Protection Regulation (GDPR). Official Journal of the European Union, 2016, pp. 1–88.

ABOUT PROTECTION OF PERSONAL DATA IN INDUSTRY 4.0 BASED SYSTEMS

Tahmasib Fataliyev¹, Shakir Mehdiyev²

^{1,2}Institute of Information Technology of
ANAS, Baku, Azerbaijan

¹depart3@iit.science.az, ²shakir@iit.science.az

Abstract— Industrial revolutions play an important role in the development of critical systems. The fourth industrial revolution, or Industry 4.0, has made the cardinal changes in this area, and is more indebted by the emergence and development of the Internet of things, cyber-physical systems, artificial intelligence, robotics and other advanced technologies. They led to the creation of a fully automated digital production controlled by real-time intelligent systems in constant interaction with the external environment. In essence, these technologies make the production system a “smart network factory”, where all activities are digitally controlled, and, as a result, the use of financial and material resources are becoming more efficient. Along with these, an increase in the collection and processing of large volumes of data, as well as a high degree of autonomy and decentralization for such systems, are factors that can become problematic in the context of data protection and, first of all, personal data. This work is devoted to the protection of personal data in oil and gas sector systems, implemented on the basis of the Industry 4.0 concept. Conceptual tasks are considered and recommendations for their solution are given.

Keywords— industrial revolution; Industry 4.0; personal data; oil and gas sector; risk; data protection

İnternetdə uşaqların fərdi məlumatlarının qorunması vəziyyətinin analizi

Sabirə Ocaqverdiyeva

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

Xülasə – Məqalədə uşaqların fərdi məlumatlarının qorunması aktual təhlükəsizlik problemi kimi qeyd edilir. Uşaq və yeniyetmələrin fərdi məlumatlarının qorunması məqsədilə beynəlxalq aləmdə qəbul edilmiş rəsmi sənədlər şərh edilir. Uşaqların fərdi məlumatlarının əldə edilməsində rəqəmsal qurğuların rolu göstərilir. Ölkəmizdə uşaqların fərdi məlumatlarının mühafizəsi ilə əlaqədar bir sıra təkliflər irəli sürülür.

Açar sözlər: *fərdi məlumatlar, məlumatların məxfiliyi, uşaqların fərdi məlumatları, rəqəmsal əşyalar*

I. GİRİŞ

İnternetin inkişafı informasiya texnologiyaları ilə qarşılıqlı münasibətlərin yeni formalarının yaranmasına səbəb olur. Süni intellekt, Big data texnologiyaları ilə təchiz olunmuş qurğulardan istifadənin ənənəvi hal alması informasiya mübadiləsini sürətləndirməklə yanaşı, həyatın bütün sahələrində qərarların qəbulu üçün vacib faktora çevrilir [1].

Real həyatda olan məlumatların əksəriyyəti virtual mühitə transformasiya olunur. Bu sürətli informasiya mübadiləsi prosesinin təsiri ilə real və virtual aləmlər arasında fərqlər azalır. Cəmiyyət texnologiyaya əsaslanan aktivlərini fərdi, korporativ və milli təhlükəsizlik səviyyəsində olan təhdidlərdən qorunmalı olduğunu qəbul edir. Bu isə cəmiyyətdə fərdi və ictimai məlumatlar arasında tarazlığın təhlil olunmasına ehtiyac yaradır [2].

İnternet istifadəçilərinin müəyyən hissəsi uşaq və yeniyetmələrdir [3]. Onlar virtual mühitdə aktivdirlər, interaktiv media mədəniyyətinin təsiri ilə fəaliyyət göstərirlər və global bir cəmiyyətin üzvünə çevrilirlər. Onlar üçün sosial şəbəkələrdə öz profillərini və statuslarını tez-tez yeniləmək, gündəlik həyat fəaliyyətləri və olduqları məkan haqqında məlumatları paylaşmaq, dostları ilə məktublaşmaq, onlayn fikir mübadiləsi aparmaq adi davranışa çevrilmişdir [3]. İstifadəçilərin maraqlarını, davranışlarını və vərdişlərini ələ keçirmək istəyən təşkilatlar, şirkətlər və şəxslər üçün İnternet zəngin informasiya mənbəyi kimi məlumat çatdırma mexanizmi olaraq xidmət edir.

Yeni iştirakçı platformalar gənclərin sosiallaşması üçün əlverişli şərait yaradır, eyni zamanda onların fərdi məlumatlarının qorunması məsələsini aktuallaşdırır [4].

İnternet istifadəçilərinin əksəriyyəti məlumatların gizli saxlanması, xüsusi ilə də fərdi məlumatların gizliliyi haqqında müəyyən biliklərə malikdir. Gizlilik tədbirləri kimi parollardan, mürəkkəb açarlardan, identifikatorlardan, elektron imzalara qədər xüsusi hazırlanmış müxtəlif vasitələrdən istifadə edilir. Bu gizlilik tədbirlərinin mövcud olmasına baxmayaraq istifadəçilərin fərdi məlumatlarının yayılması və düzgün istifadə edilməməsi riski olduqca yüksəkdir. Beləki, İnternetdən istifadə zamanı istifadəçilərin qarşılaşdığı təhlükələrin siyahısında fərdi məlumatların qorunması və idarə olunması xüsusi yer tutur.

Uşaqların fərdi məlumatları onların özləri, valideynləri və marketinq şirkətləri tərəfindən şəbəkədə yerləşdirilməsi paylaşılabilir. Rəqəmsal qurğuların sayının gündən-günə artması, təkmilləşdirilməsi uşaqların fəaliyyətini dəyişdirir, onların gündəlik həyatı haqqında məlumatları müxtəlif informasiya sistemlərinə ötürülür. Bu məlumat bazalarından valideynlər, tədris, səhiyyə, sığorta, bank və bir sıra təşkilatlar maksimum faydalanmağa çalışır. Lakin bu məlumatlar uşaqlara qarşı yönəlmiş bir təhdid mənbəyi ola bilər. Bədnəyyətli insanlar tərəfindən müəyyən məqsədlər üçün istifadə oluna bilər.

II. RƏQƏMSAL QURĞULAR UŞAQLARIN FƏRDI MƏLUMATLARININ DAŞIYICISI KİMİ

Son zamanlar müxtəlif rəqəmsal qurğular uşaqların həyatına inteqrasiya edilmişdir. Bu inteqrasiya prosesi dərinləşməkdə davam edir, çünki Big data prinsipləri və təcrübələri rəqəmsal mənzərəni dəyişdirməyə nail olmuşdur. Nəticədə fərdi məlumatların toplanması, izlənməsi və marketinqini həyata keçirən tətbiqetmələr meydana gəlmişdir. Bütün bunlar isə uşaqların fərdi məlumatları üzərində biznes maraqları olan bədnəyyətli insanların fəaliyyətinə kömək edir.

Uşaqların həyatında sensorla təchiz olunmuş oyuncaqlar, nəzarətçi cihazlar, müxtəlif tapşırıqları xatırladan və uşaqların fəaliyyətini izləyən qurğular və s. əhəmiyyət kəsb edir. Rəqəmsal oyuncaqlar konkret zaman çərçivəsində uşaqların davranışları haqqında olan məlumatları işıq və ya xüsusi siqnallar vasitəsilə məlumat bazasına toplayır [5].

Müəyyən müddətdən sonra uşağın marağı mobil qurğulara, kompüterə, planşetlərə və digər müasir texnologiyalara

yönəlir. Artıq uşaqların rəqəmsal texnologiyalardan istifadəsi adi maus və klaviatura ilə deyil, interfeys və qurğular sensor ekran və jestlərin tanınma qurğuları kimi müasir qarşılıqlı münasibət formaları ilə əvəz edilir.

Əşyaların İnterneti məhz rəqəmsal texnologiyaların təzahürüdür. və uşaqların əşyalarla münasibəti haqqında məlumat əldə etməyə qadirdirlər [6]. Əşyaların İnterneti şəbəkəyə qoşulmuş kompüterlərin eyni zamanda əşyalarla bağlılığını göstərir. Əşyaların İnterneti vasitəsilə fərdi məlumatların toplanması ənənəsi genişləndikcə fərdi məlumatların təhlükəsizliyi problemi də böyüməkdə davam edir. Bu intellektual avadanlıqlar və qurğular yalnız məlumat toplayan xüsusi sensorlarla təchiz olunmur, onlar qlobal şəbəkə vasitəsilə həmin məlumatları emal edən qurğulara qoşulur.

Valideynlər övladlarının onlayn fəaliyyətlərinin onun məxfiliyinə necə təsir göstərməsi ilə bağlı narahatlıq keçirir. Belə tədbirlərin həyata keçirilməsində təhsil müəssisələri də maraqlı olurlar. Məktəb rəhbərləri öz şagirdlərinin təhlükəsizliyini təmin etmək üçün yeni yollar axtarır. Buna misal olaraq Yaponiya və ABŞ-dakı bəzi məktəb rəhbərlərinin şagirdlərin döş nişanlarına, geyimlərinə və ya məktəb çantalarına identifikasiya etiketlərinin yerləşdirilməsini göstərmək olar [7].

Rəqəmsal əşyalar vasitəsilə uşaqların izlənməsi onların harada olduğu, hansı fəaliyyətlə məşğul olduğu, yuxu rejimini və s. izlənməkdə faydalıdır. Çünki valideyn övladı haqqında anında məlumat əldə edir, lakin bu izlənmənin mənfi cəhətləri kimi aşağıdakıları qeyd etmək olar:

- Uşaqların fərdi məlumatları müxtəlif məlumat bazalarına ötürülür;
- Uşaqlardan əşya kimi, sanki bir obyekt kimi istifadə olunur;
- Valideyn müəyyən qərar qəbul edərkən, məlumat bazalarına əsaslanır ki, bu zaman uşağın fikri ikinci plana keçir.

Rəqəmsal əşyaların həyatımıza nüfuz etməsi faydalıdır. Lakin, evlərdə və məktəblərdə rəqəmsal texnologiyaların geniş tətbiqi yeni sosial problemlərin ortaya çıxmasına səbəb olur.

III. UŞAQLARIN FƏRDİ MƏLUMATLARI İLƏ BAĞLI HÜQUQİ TƏNZİMLƏMƏLƏR

Uşaqlar olayn təhlükələr və onların yaratdığı mənfi nəticələr haqqında az məlumatlı olduqları üçün onların böyükklərdən bir qədər də artıq müdafiəyə ehtiyacı vardır. Beynəlxalq aləmdə uşaqların fərdi məlumatlarının istifadəsi ilə əlaqəli rəsmi sənədlər bu məsələləri əhatə edir.

1998-ci ildə Uşaqların İnternetdə Gizliliyinin Qorunması Qanunu (ing. The Children's Online Privacy Protection Act – COPPA) qəbul edilmişdir. Bu qanun veb sayt operatorunun

məxfilik siyasətinə nə daxil etməli olduğunu, valideyndən və ya qəyyumdan təsdiqlənən razılığı nə vaxt və necə istəməli olduğunu, operatorun onlayn rejimdə uşaqların məxfiliyini və təhlükəsizliyini qorumaq üçün hansı məsuliyyəti özündə cəmləşdirməsini, o cümlədən marketinqdə hansı məhdudiyyətlərin daxil edilməsini özündə əks etdirir. Qanun Birləşmiş Ştatların qanunvericiliyinə əsasən 13 yaşına çatmamış şəxslərin və ya təşkilatlarda olan şəxsi məlumatların toplanmasına aiddir [8].

Qanun kommersiya veb-saytlarının və digər medyanın 13 yaşdan kiçik uşaqların şəxsi məlumatlarının toplanmasını məhdudlaşdırmağı tələb edir. Valideynlərin cəlb olunması üçün mexanizm təklif edir və verilənlərin adekvat aşkarlanması və mühafizəsi üçün məsuliyyəti şirkətlərin öhdəliyinə verir.

Bu qanunun icrası ilə bağlı qaydalar bəzi yeni yaranan problemlərə və təcrübələrə cavab vermək üçün 2013-cü ildə yenilənmişdir. Qanuna davranış hədəflərinə, fərdiləşdirilmiş reklam və məkana əsaslanan məhdudiyyətlər əlavə edilmişdir.

COPPA uşaqları onlar haqqında olan, tövsiyə olunmayan məlumatların toplanmasından və hədəfli marketinq taktikalarından mühafizə edir. Bu hədəflərə baxmayaraq, qanun böyük məhdudiyyətlərə malikdir. Beləki, COPPA yalnız 13 yaşdan kiçik uşaqlara tətbiq edildiyi üçün yeniyetmələrin informasiya təhlükəsizliyini (kommersiya, rəqəmsal media mühitində fərdi məlumatların gizliliyi) təmin etmir [8].

İnternetdə uşaqların məlumatlarını qorumaq, uşaqların onlayn məxfiliyinin pozulması məsələləri Avropa qanunvericiliyində ön plandadır.

Məlumatların Qorumasının Ümumi Qaydası (ing. General Data Protection Regulation – GDPR) Avropa Birliyi (AB) tərəfindən 25 may 2018-ci ildə qüvvəyə minmişdir. Bu qanun həm uşaqlar, həm də böyükklər üçün nəzərdə tutulur. Qanun uşaqların məlumatlarını qorumağı hədəfləyən müəyyən müddəaları əhatə edir [9].

Bu qayadalar əsasən uşaqların yaş həddi olaraq – 16 yaş götürülür. Bəzi üzv dövlətlərdə isə bir qədər aşağı yaş həddi olaraq 13 yaş kimi qəbul edilir. Uşaqların və məlumatlarının qorunmasına dair GDPR prinsiplərinə aşağıdakılar daxildir [10]:

- Fərdi məlumatlar toplandıqda və emal olunduqda uşaqlar üçün xüsusi tədbirlər olunmalıdır, çünki onlar potensial risklərdən az xəbərdardırlar;
- Əgər bir təşkilat uşaqların məlumatlarını emal edirsə və ya onların gələcəkdə hər hansı bir məqamda olacağını düşünürsə, əvvəlcədən müəyyən üsul və vasitələrdən istifadə etməlidir;
- Uşaqların bütün məlumatlarının işlənməsi zamanı məlumatların qorunması prinsiplərinə uyğunluq nəzərə alınmalıdır;

- Hər hansı bir uşağın şəxsi məlumatlarının işlənməsi üçün qanuni əsası olmalıdır. Razılıq mümkün bir qanuni əsasdır, ancaq bu yeganə seçim deyil və alternativ bir əsas daha uyğun ola bilər ki, bu da uşağın daha yaxşı qorunmasını təmin edər;
- Uşaqlara onlayn xidmət təqdim edərkən fərdi məlumatların emalı üçün qanuni əsas kimi yalnız 13 yaşdan yuxarı uşaqlar öz razılığını təmin edə bilərlər. Buna görə, məsləhət və ya profilaktik xidmət olmadıqda 13 yaşdan kiçik uşaqlar üçün valideyn və ya məsuliyyət daşıyan şəxsdən razılıq alınmalıdır;
- Uşaqlar haqqında avtomatik olaraq qərar qəbul edilməməlidir. Təşkilatlar uşaqlara onların fərdi məlumatlarından necə istifadə edəcəklərini açıq şəkildə bildirməlidirlər. İştirak edən risklər və təhlükəsizlik tədbirləri barədə açıq olduqlarını təmin etməlidirlər. Təşkilatlar məlumatların necə istifadə olunduğuna görə xoşa gəlməz hal olduğu təqdirdə uşaqlara nə edəcəyini düşünməlidir;
- Uşaqlara yönəlmiş riskləri qiymətləndirmək, onların sayını və təsirini azaltmaq üçün Məlumatların Mühafizəsinə Təsirin Qiymətləndirmələrindən (Data Protection Impact Assessments –DPIA) istifadə edilməlidir;
- Təşkilatlar uşaqlarla münasibət qurarkən, onlara onlayn xidmətlər təqdim edərkən aydın və asan başa düşülən bir dildən istifadə etməlidirlər;
- Fərdi məlumatların silinməsi hüququ, şəxsin uşaq yaşında ikən işlənməyə razılıq verdikdə aktualdır.

Cədvəl 1. -də uşaqların məlumatları emal edilərkən onların yaş baxımından fərdi məlumatlarının işlənməsinə dair məlumat verilir. Bu cədvəldə AB-yə daxil olan ölkələrin adları, qanun qəbul edildiyi il və uşağın yaş həddi göstərilir.

CƏDVƏL 1. Fərdi məlumatlarının işlənməsinə dair AB ölkələri üzrə paylanma

SS	Ölkə	Qanun qəbul olunduğu il	Uşağın yaş həddi
1	Belçika	2018	13
2	Danimarka	2018	13
3	Estoniya	2019	13
4	Finlandiya	2018	13
5	Malta	2018	13
6	Latviya	2018	13
7	İsveç	2018	13
8	Portuqaliya	2019	13
9	Birləşmiş Krallıq	2018	13
10	Avstriya	2018	14
11	Bolqarıstan	2019	14
12	Kipr	2018	14
13	İtaliya	2018	14
14	Litva	2018	14
15	İspaniya	2018	14

16	Çexiya	2019	15
17	Fransa	2018	15
18	Xorvatiya	2018	16
19	Almaniya	2018	16
20	Macarıstan	2018	16
21	İrlandiya	2018	16
22	İngiltərə	2018	16
23	Lüksemburq	2018	16
24	Hollandiya	2018	16
25	Slovakiya	2018	16
26	Rumıniya	2018	16

AB-yə üzv olmayan, lakin Avropa İqtisadi Bölgəsinin üzvü olan dövlət kimi Norveç 2018-ci ilin may ayında GDPR-ni tətbiq edən yeni Fərdi Məlumat Aktını təsdiqləmişdir. Qanunda uşaqların rəqəmsal xidmətlərə razılıq yaşının 13 olduğunu bildirmişdir [10].

Hal hazırda Yunanıstan və Sloveniya kimi ölkələr isə öz milli tətbiqetmə qanunlarını gözləyirlər. Bu ölkələrdə qanun layihəsi rəsmi qəbul olunanadək təklif olunan yaş əvəzinə GDPR tərəfindən tətbiq edilən 16 yaş həddi öz qüvvəsində qalır.

IV. TƏKLİF VƏ TÖVSİYƏLƏR

Araşdırmalardan məlum olur ki, dünyanın bir çox ölkələrində uşaqların fərdi məlumatlarının qorunması müxtəlif hüquq müstəvilərdə öz həllini tapır. Yeni qanunlar, aktlar qəbul edilir və ya əvvəlcədən qəbul edilmiş qanuna uşaqların fərdi məlumatlarının qorunması ilə bağlı əlavələr edilir. Bu qanunlarda bir əsas məqsəd də uşaqların açıq məlumatlarının istifadəsi və gələcəkdə onlara qarşı yönəlmiş potensial risklərin qarşısının alınmasıdır.

Ölkəmizdə uşaqların fərdi məlumatlarının qorunması vacib məsələlərdəndir. Bu problemin həllinin yaxşılaşdırılması ilə əlaqədar olaraq aşağıda qeyd edilən tədbirlərin icrası işə öz müsbət təsirini göstərə bilər:

1. Azərbaycanda uşaqların fərdi məlumatlarının mühafizəsi ilə bağlı qanunun qəbul edilməsi;
2. Rəqəmsal kompetensiyanın artırılması üçün metodik vəsait və dərsliklərin hazırlanması;
3. Rəqəmsal cəmiyyətin faydalarını optimallaşdırmaq üçün uşaq və gənclər üçün adekvat hazırlığın təşkil edilməsi;
4. Uşaq və yeniyetmələrə İnternet təhlükələri, fərdi məlumatların İnternetdə paylaşılması və qorunması ilə bağlı təlimlərin təşkil edilməsi;
5. Kiçik yaşlarından uşaqlara məlumat mübadiləsi riskləri barədə məlumatlandırmaq üçün əlavə işlərin görülməsi;
6. Uşaqların fərdi məlumatların toplanmasında Əşyaların İnterneti çox böyük əhəmiyyətə malik olduğundan, fərdi məlumatların ələ keçirilməsi risklərini azaltmaq məqsədilə Əşyaların İnternetinin tətbiqində normativ-

hüquqi tənzimləmə, kibertəhlükəsizlik və standartlaşdırma məsələlərin həlli edilməsi.

Məlumdur ki, rəqəmsal bir dünyanın vətəndaşı olmaq məsuliyyətlidir, uşaq və yeniyetmələr üçün bir qədər çətinidir. Texnologiyalar global əlaqələri asanlaşdırmaqla yanaşı, istifadəçiləri təhlükələrlə üz-üzə qoyur. Buna görə də texnologiyalardan təhlükəsiz istifadə zamanı yaranmış problemləri uğurla həll etmək üçün uşaqlara davamlı rəhbərlik etmək lazımdır. Hər bir uşaq və yeniyetmənin rəqəmsal yetkinliyi inkişaf etdirilməlidir. Bu vəzifə yetkinlərin, mütəxəssislərin və təhsil müəssisələrinin əsas hədəflərindən birinə çevrilməlidir.

NƏTİCƏ

Müasir uşaq və yeniyetmələr rəqəmsal media mədəniyyətinin təsiri ilə böyüyürlər. İstifadəçilərin əksəriyyəti müasir informasiya texnologiyalarının iş prinsipindən, övladlarının davranışlarının ağıllı qurğular vasitəsilə necə qeydə alındığından və bu məlumatlardan hansı məqsədlərlə istifadə edildiyindən xəbərdar deyildir. Rəqəmsal qurğuların uşaqların davranışına nə dərəcədə təsir etməsi, həmin qurğular vasitəsilə əldə olunan fərdi məlumatların necə istifadə olunması, bu barədə valideynlərin xəbərdar olub-olmaması məsələləri aktual olaraq qalmaqda və mütəxəssisləri düşündürməkdədir.

Fərdi məlumatlarını İnternetdə rəqəmsallaşdırmağa meylli olan şəxslər daha çox yeniyetmələr və gənclərdir. Onlar onlayn məxfiliklə bağlı məlumatlı olsalar da, çox vaxt bu qaydaları unudurlar. Nəticədə özlərini bədnəyyətli insanların hədəfinə çevrilirlər.

Məxfilik təhdidləri və uşaqların məxfiliyini necə qorumaq bu gün cəmiyyətdə həlli vacib olan problemlərdəndir. Bu sahədə biliklərin olması faydalıdır. Uşaqların fərdi məlumatları, tibbi məlumatları, psixoloji məlumatları, təhsil səviyyəsi, davranışları və s. bağlı statik məlumatlar onların gələcək həyatında problemlərin yaranmasına səbəb ola bilər.

İSTİFADLAR

- [1] R.Alguliyev and Y.Imamverdiyev, “Big Data: Big Promises for Information Security”, Proceedings of the 8th International Conference on Application of Information and Communication Technologies (AICT), 15–17 Oct. 2014, IEEE, Astana, pp. 1–4.
- [2] Г. Солдатова, О Теславская, «Персональные данные и дети: вопросы безопасности?», Эпоха науки, 2017 г, № 12, стр.92-102.
- [3] R. Alguliyev and S. Ojagverdiyeva, “Conceptual Model of National Intellectual System for Children Safety in Internet Environment”, International Journal of Computer Network and Information Security(IJCNIS), 2019, №3, pp. 40-47.
- [4] Unicef – The state of the world’s children, 2017, 251p., https://www.unicef.org/publications/files/sowc_2017_eng_web.pdf
- [5] G Maria., E Gabriela and J. Hernando, “Kids and Parents Privacy Exposure in the Internet of Things: How to Protect Personal Information?”, Computación y Sistemas, 2018, vol. 22, No. 4, pp. 1191–1205.
- [6] R.Əliquliyev, R. Mahmudov, “Əşyaların İnterneti: mahiyyəti, imkanları və problemləri”, İnformasiya cəmiyyəti problemləri, 2011, №2. s. 29-40.
- [7] I.Berson and M.Berson, “Children and Their Digital Dossiers: Lessons in Privacy Rights in the Digital Age”, International Journal of Social Education, 2006, vol. 21, n1 pp. 135-147.
- [8] Children’s Online Privacy Protection Rule (COPPA) // Federal Trade Commission official website, USA. URL: <https://www.ftc.gov/enforcement/rules/rulemakingregulatory-reform-proceedings/childrens-online-privacy-protection-rule>.
- [9] General Data Protection Regulation, <https://gdpr-info.eu/>
- [10] The GDPR child’s age of consent for data processing across the EU – one year later, 2019 July, <https://www.betterinternetforkids.eu>

ANALYSIS OF THE PROTECTION CHILDREN’S PERSONAL DATA ON THE INTERNET

Sabira Ojagverdiyeva

Institute of Information Technology of ANAS, Baku, Azerbaijan

allahverdiyevsabira@gmail.com

Abstract— The protection of children’s personal data is noted as a actual security issue in the article. The official documents recognized internationally are interpreted to protect the personal information of children and adolescents. The role of digital devices in acquiring children’s personal data is shown. A number of suggestions are being put forward to protect the personal information of children in our country.

Keywords— *personal information, data confidentiality, children’s personal information, digital things*

Sosial kredit sistemlərində fərdi məlumatların idarə edilməsi problemləri

İradə Ələkbərova

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

Xülasə— İnformasiya texnologiyalarının inkişafı vətəndaşların fərdi məlumatlarının dövlət təşkilatları və özəl şirkətlər tərəfindən toplanması və emalı üçün yeni imkanlar yaratmışdır. Sosial media, izləmə cihazları, üz tanıma və “ağıllı şəhər” kimi texnologiyaların tətbiqi dövlətlərdə müşahidə cəmiyyətinin formalaşmasına səbəb olmuşdur. Məqalədə müşahidə cəmiyyətinin insanların gündəlik həyatına təsirləri, Çinin sosial kredit sisteminin fərdi məlumatların qorunması ilə əlaqədar beynəlxalq-hüquqi prinsiplərə nə dərəcədə uyğun olması araşdırılmışdır. Tədqiqatın məqsədi müşahidə cəmiyyətinin vətəndaşların sosial kreditinin qiymətləndirilməsində rolunu və yaratdığı problemləri müəyyən etməkdir.

Açar sözlər— fərdi məlumatlar; sosial kredit sistemi; müşahidə cəmiyyəti; vətəndaşın davranışı; üz tanıma sistemi; müşahidə kamerası

I. GİRİŞ

İnformasiya və biliyin cəmiyyətdə rolu artdıqca dövlət orqanları və şirkətlər tərəfindən qeyri-maddi sistemin formalaşması, işçilərin yaradıcı potensialından maksimum istifadə, sosial tərəfdaşlığın yeni formalarının yaranması kimi sosial hadisələrə daha çox əhəmiyyət verilir. Dövlət təşkilatları və nəhəng şirkətlər tərəfindən müxtəlif informasiya sistemləri vasitəsilə fərdi məlumatların toplanması və emalı əsasən aşağıdakı məsələlərin həllinə yönəlmişdir:

- ölkədə informasiya təhlükəsizliyinin təmini;
- sosial-iqtisadi və sosial-siyasi məsələlərin səmərəli həlli;
- vətəndaşların həyat şəraitinin yaxşılaşdırılması;
- şirkətlərdə maliyyə risklərinin azaldılması və proqnozlaşdırma;
- vətəndaşların cəmiyyətdə çəkisi, qanun qarşısında vəzifəsi, sosial normalara necə əməl etməsi və etimadı ilə əlaqədar vəziyyətin öyrənilməsi;
- vətəndaş məmnuniyyətinin müəyyən olunması və s.

Bu məsələlərin həllində tətbiq olunan yeni yanaşma kimi Çinin sosial kredit sistemini (*Social Credit System, SCS*) göstərmək olar [1]. Çin Xalq Respublikasının ayrı-ayrı

bölgələrində sınaqdan keçirilən və 2020-ci ildə tətbiqi nəzərdə tutulan sistem korrupsiya və bürokratiyanın qarşısını almaqla ölkədə sosial bərabərsizliyi aradan qaldırmaq, yüksək iqtisadi inkişafa nail olmaq məqsədi ilə yaradılmışdır [2, 3]. SCS ölkə vətəndaşlarının və müxtəlif şirkətlərin fəaliyyətinə yüksək səviyyədə nəzarət etməklə ölkədə nümunəvi hüquqi dövlətin zamanəti ola biləcək dünyada ilk milli qiymətləndirmə sistemi sayılır [4]. Lakin sosial kreditin qiymətləndirilməsində fərdi məlumatlardan istifadə ilə bağlı şəffaflığın olmaması, müşahidə cəmiyyətinin vətəndaşların gündəlik həyatlarına təsiri, fərdi məlumatların emalı nəticəsində vətəndaşlara qarşı cəza sisteminin tətbiqi bu sahədə ciddi problemlərin olduğunu göstərir.

II. MÜŞAHİDƏ CƏMİYYƏTİ

Müasir şəbəkə texnologiyaları insanların fərdi həyatı, davranışları, maraqlarının ayrılmaz hissəsinə çevrilməklə, müşahidə cəmiyyətinin (*ing. Surveillance society*) formalaşmasına səbəb olmuşdur [5]. Müşahidə cəmiyyəti dövlət təşkilatları, ayrı-ayrı şirkətlər və hətta cinayətkarlar tərəfindən vətəndaşları izləməyə, onların fəaliyyətini bütün gün ərzində nəzarətdə saxlamağa şərait yaradan cəmiyyətdir.

Əşyaların interneti, sosial şəbəkələr, izləmə cihazları, mobil əlaqələndirmə vasitələri, üz tanıma sistemləri və s. kimi müasir texnologiyalar müşahidə cəmiyyətində əsas izləmə vasitələridir. Bu vasitələrdən toplanan fərdi məlumatlar vətəndaşın səhhəti, maraqları, psixoloji durumu, evdə və ictimai yerlərdə davranışı, intellektini qiymətləndirməyə və proqnozlaşdırmağa imkan yaradır [6].

İzləmə cihazları ilə toplanan fərdi məlumatlar digər məlumatlar kimi müxtəlif bazalarda – bank və sığorta şirkətlərinin, tədris və tibb müəssisələrinin, supermarket və dövlət idarələrinin informasiya sistemlərində, müxtəlif arxivlərdə saxlanılır. Rəqəmsallaşdırılmış bu məlumatlar insanların davranışlarını və sosial münasibətləri, ölkədəki demoqrafik prosesləri, bazar iqtisadiyyatını idarə etmək üsullarını dəyişdirir. Ayrı-ayrı şirkətlər və təşkilatlar tərəfindən yüksək gəlir əldə etmək, maliyyə risklərini azaltmaq, informasiya təhlükəsizliyini təmin etmək üçün əməkdaşların, müştərilərin, iş ortaqlarının və s. haqqında fərdi

məlumatların toplanması ənənəvi hal almışdır. Artıq biznesdə, müxtəlif idarəetmə formalarında, insanlar arasında informasiya mübadiləsində vətəndaşı müəyyən edən ənənəvi əlamətlər: adı, yaşadığı yer, doğulduğu tarix, təhsili və biliyi kifayət deyil.

Fərdi məlumatların ilkin mənbəyi, müşahidə cəmiyyətinin təməli kimi İnternet qlobal şəbəkəsi xüsusi yer tutur. Müşahidə cəmiyyətinin inkişafı ilə əlaqədar fərdi məlumatlar siyahısına yeni verilənlər daxil edilir: vətəndaşın veb portallardakı istifadəçi hesabı, e-poçt ünvanı, mobil telefon nömrəsi, kredit tarixi, sosial kapitalı və s. Burada əsas problemlərdən biri vətəndaşın fərdi məlumatları əsasında identifikasiya aparan tərəfin nə qədər etibarlı olmasıdır.

İzləmə cihazlarından istifadə etməklə fərdi məlumatların ələ keçirilməsi onlardan icazəsiz istifadə problemlərini də aktuallaşdırmışdır. Bu gün sosial media imkanlarından istifadə etməklə hər hansı vətəndaş haqqında fərdi məlumatların icazəsiz və qərəzli şəkildə ictimaiyyətə ötürülməsi ilə istənilən vətəndaşın nüfuzuna və sosial-iqtisadi vəziyyətinə zərər vurmaq təhlükəsi mövcuddur.

Dövlət portallarında, virtual ensiklopediyalarda, virtual ticarət şəbəkələrində də vətəndaşlar haqqında fərdi məlumatlar toplanmaqdadır. Bu məlumatlar iki formada olur: açıq şəkildə verilən fərdi məlumatlar və digər məlumatların emalı nəticəsində əldə edilən gizli fərdi məlumatlar. Vətəndaşların informasiya daxil edərəkən səhlənkarlığı, heç bir əsas olmadan başqalarına etimadı, onlayn və avtonom identifikasiya məlumatlarının düzgün idarə olunmaması fərdi məlumatların cinayətkarların və ya dələduz şirkətlərin əlinə keçməsinə səbəb olur.

III. SOSIAL KREDIT SİSTEMİ

Çin Xalq Respublikasında “Xəbərdarlıq və cəza” sistemi adlandırılan SCS bir sıra qərb dövlətləri tərəfindən tənqid edilməkdədir. Qərb mətbuatında belə bir fikir formalaşmış ki, SCS bütün Çin vətəndaşlarının fərdi məlumatları əsasında qiymətləndirilməsini aparmaqla əhaliyə nəzarət edir və vətəndaşları davranışına görə cəzalandırmaq funksiyası daşıyır. Onlar sistemin vətəndaşın fəaliyyətinə nəzarət etməsini demokratiyanın pozulması, fərdi məlumatlarından vətəndaşa qarşı istifadə olunmasının repressiyaya gətirib çıxaracağını iddia edirlər [7, 8]. Lakin Çin hökuməti bu iddiaları əsassız sayır və SCS-in sosial-iqtisadi sahələrdə risklərin idarə olunmasında, cəmiyyətin təhlükəsizliyi və iqtisadi inkişafında mühüm vasitə olduğunu iddia edir.

Fərdi məlumatların mühafizə olunmasının əsas prinsipləri BMT-nin “Ümumdünya İnsan Hüquqları Bəyannaməsi”ndə (ing. *Universal Declaration of Human Rights*) öz əksini tapmışdır [9]. BMT Baş Assambleyasının 16 May 2011-ci il tarixli məruzəsində bildirilir ki, “İnternet” informasiya və telekommunikasiya şəbəkəsinə müraciət imkanının yaradılması insan hüquqlarının baza hissəsinə aiddir və “İnternet” informasiya və telekommunikasiya şəbəkəsinə çıxışın məhdudlaşdırılması və vətəndaşın fərdi məlumatlarının həmin vətəndaşın icazəsi olmadan yayılması vətəndaş

hüquqlarının pozulması kimi tanınır. Lakin bu gün SCS-in işinə qoyulan tələblər bunun əksini göstərir. Sistemin əsas funksiyası olan sosial kreditin qiymətləndirilməsi məsələsi ölkə ərazisində fəaliyyət göstərən bütün təşkilatlar arasında hərtərəfli əlaqələndirməni təmin edən və vətəndaşlar haqqında bütün fərdi məlumatları toplamaq imkanına malik nəhəng verilənlər bazası tələb edir.

IV. ÇİNİN MÜŞAHİDƏ CƏMİYYƏTİ

Çin Xalq Respublikasında ölkə vətəndaşlarını izləmək üçün video və şəkil çəkən qurğuların sayı və əhatə dairəsi heyətləndiricidir. 2018-ci ilin iyul ayında New York Times Çində təxminən 200 milyon nəzarət kamerasının olduğunu bildirmişdir və bu nəzarət kameralarının sayı ABŞ-dan 4 dəfə çoxdur [10].

Vətəndaşların gündəlik fəaliyyətlərinin izlənməsində son illərdə robot quşlardan geniş istifadə olunmaqdadır. 30-dan çox hərbi və dövlət qurumları Çinin müxtəlif əyalətində insanları izləmək üçün dronlardan və buna oxşar uçan müşahidə qurğularından istifadə etməkdədir. Real göyərçinlərin hərəkətlərinin 90 faizini təqlid edən robot quşlar müşahidə kameraları, GPS, uçuş idarəetmə sistemi və peyk rabitəsi vasitəsilə məlumat ötürülməsi üçün anten ilə təchiz edilmişlər [11].

Müşahidə cəmiyyətinin inkişaf etdirilməsi üçün Çin hökumət dairələrində müxtəlif yanaşmalardan istifadə olunur. Məsələn “Hukou (*household registration*)” [12] və “Dang’an (*personal archives*)” [13] modelləri vətəndaşların fərdi məlumatları əsasında dövlət nəzarətini gücləndirmək üçün tətbiq edilmişdir. “Hukou” əsasən miqrasiyaya nəzarət edir və əhalinin kəndlərdən şəhərlərə axınının qarşısını almaq üçün nəzərdə tutulmuşdur. “Dang’an” modeli isə fərdi məlumatların (identifikasiya nömrəsi, məşğulluğu, təhsili və s.) arxivləşdirilməsini yerinə yetirir və qapalıdır. Son illər informasiya texnologiyalarının inkişafı ilə Çində “İnternet senzura” və “böyük verilənlərin analitikası” kimi daha mürəkkəb modellərin tətbiqinə keçilmişdir [8, 14].

Dövlət təşkilatları tərəfindən tətbiq olunan milyonlarla nəzarət qurğuları və müxtəlif analitik sistemlər belə deməyə əsas verir ki, hökumət vətəndaşların fərdi məlumatlarına nəzarət mexanizmlərini tez bir zamanda modernləşdirməkdə maraqlıdır. Çinin müşahidə cəmiyyəti SCS-in tətbiqi ilə çox sürətlə inkişaf edir. 2010-cu ildən başlayaraq Çin hökuməti “ağıllı şəhər”lərin pilot layihələrini genişləndirməkdə davam edir. Artıq Çinin 500 şəhəri bu layihəyə qoşulmuşdur. Çində “Sky Net” layihəsinə əsasən iri şəhərlərdə 20 milyondan artıq küçə müşahidə kameraları vətəndaşların üzə görə tanınmasını həyata keçirir. Kameralardan əldə olunan məlumatlar SCS-ə ötürülərək emal olunur [14].

V. SOSIAL KREDIT SİSTEMLƏRİNDƏ FƏRDİ MƏLUMATLARIN İDARƏ EDİLMƏSİ PROBLEMLƏRİ

Üz tanıma sistemi, əşyaların İnterneti və digər izləyici qurğularla əlaqəli işi SCS-in daha geniş bir alqoritmik idarəetmə modelinə malik olması və ayrı-ayrı şəxslərin statistik və analitik təhlilində fərdi məlumatlardan geniş

istifadə olunduğunu göstərir. SCS-də fərdi məlumatların hansı mənbələrdən toplanması və necə emal olunması haqqında məlumat verilmir. Bu baxımdan fərdi məlumatların toplanmasında hüquqi normalara nə dərəcədə əməl olunması məlum deyil.

SCS tərəfindən fərdi məlumatların toplanması və emalında qaranlıq məqamların olması cəmiyyətdə qeyri-müəyyənliyə səbəb olur, elektron xidmətlərdən istifadə etimadını sarsıdır və nəticədə informasiya cəmiyyətinin inkişafına təhdid yaradır [15].

Hər bir informasiya sistemində olduğu kimi, SCS-də tətbiq olunan alqoritmlərdə xətlərin olması ehtimalı vardır. Sistemin işindəki ümumi xətlər kimi aşağıdakıları göstərmək olar:

- SCS-də emal olunan verilənlərin mənbələrində və tətbiq olunan alqoritmlərdə qeyri-şəffaflığın olması;
- sistemdə emal olunan informasiyanın həddən artıq böyük və mürəkkəb olması nəticəsində baş verən xətlər;
- sistem operatorunun diqqətsizliyindən yaranan xətlər;
- sistemə daxil edilən informasiyanın qeyri-dəqiqliyi və alqoritməndəki texniki xətlər.

Sistemin müəyyən etdiyi sosial kredit vətəndaşı qane etmirsə və ya vətəndaş bu qiymətləndirmənin necə əldə olunduğu haqqında təsəvvürü yoxdursa, bu halda sual yaranır: SCS tərəfindən verilən sosial kreditlə razı olmayan vətəndaş hara müraciət etməlidir? Çünki sosial kredit yalnız vətəndaşın özünə deyil, onun ailəsinə və uşaqlarının sosial-iqtisadi həyatına da ciddi təsir göstərir. Məsələn, sosial krediti aşağı olan vətəndaş dövlət tərəfindən etimadsız sayılır. Nəticədə, həmin vətəndaş dövlət işində işləyə bilməz, uşağını nüfuzlu məktəb və universitetlərdə oxuda bilməz və s. Buradan belə nəticəyə gəlmək olar ki, SCS vasitəsilə hökumət vətəndaşların davranışlarını istədiyi istiqamətə yönəltmək və formalaşdırmaq imkanına malik olur. Bundan əlavə, alqoritmlər ictimaiyyətə açıqlanmadığından müəyyən etnik qrupların, dini və milli azlıqların bu sistemdən əziyyət çəkmə riski vardır.

Son illər cəmiyyətdə Çin şirkətləri tərəfindən fərdi məlumatlardan sui-istifadə hallarına qarşı tələblər güclənmişdir [16]. Məsələn, istehlakçı hüquqlarının müdafiəsi təşkilatı istifadəçi razılığı olmadan istifadəçinin olduğu yer, mesajları və sosial münasibətləri kimi şəxsi məlumatları icazəsiz topladığına görə dünyanın ən nəhəng axtarış sistemi olan və Çin hökuməti tərəfindən dəstəklənən Baidu-nu məhkəməyə vermiş və nəticədə, Alipay internet xidmətinin idarə heyəti "Ant Financial's" təşkilatından üzr istəmişdir.

SCS-in əhəmiyyətli olduğunu bildirən Çinin dövlət orqanları vətəndaşların fərdi məlumatlarının qorunmasının vacibliyi məsələsinə toxunurlar. Çində vətəndaşların fərdi məlumatlarının təhlükəsizliyi məsələsinin açıq qalması vətəndaşların kütləvi izlənməsi və bütün fərdi məlumatların toplanaraq emal edilməsi məsələsinə hüquqi cəhətdən azadlıq verilmişdir. Belə bir şəraitdə SCS-in tətbiqi fərdi məlumatların

təhlükəsizliyi məsələsində vətəndaşlara ciddi problemlər yaratmışdır.

Çinin hakim dairələri bildirirlər ki, fərdi məlumatları emal etməklə vətəndaşların sosial kreditini müəyyən edən SCS məsuliyyətli vətəndaşların sayının xeyli artmasına imkan yaradacaqdır. Belə ki, öz sosial kredit balını artırmağa çalışan vətəndaş davranışlarına daha ciddi yanaşacaq və əmək fəaliyyətində, virtual məkanda və müxtəlif növ ödəmələrdə dəqiq olmağa, səhlərə yol verməməyə çalışacaqdır. SCS ilə əlaqədar sənədlərdə göstərilir ki, sistemin səmərəli işi üçün hökumət vətəndaşların və Çində fəaliyyət göstərən bütün təşkilatların qiymətləndirilməsi üçün fərdi məlumatlardan, maliyyə, hüquqi və digər verilənlərdən sərbəst istifadə və sosial krediti kifayət qədər olmayan şəxsləri və təşkilatları cəzalandırmaq hüququna malikdir [17]. SCS-in işindəki "xəbərdarlıq və cəza" prinsipinin dövlət qanunları ilə uyğunluğu problemlər yaradır və onlar aşağıdakılardır:

- Sosial kreditin müəyyən olunmasının qanunvericilikdə şərtləri göstərilir.
- Hüquqi sənədlərdə milli qiymətləndirmə agentliklərinin olması haqqında dəqiq məlumat yoxdur.
- Qiymətləndirmə agentliklərinin fəaliyyətində tənzimləyici şərtlər mövcud deyil.

Təhlükəsiz, mərkəzsizləşdirilmiş verilənlər bazası yaratmaq üçün verilənlərin izləyici qurğulardan, üz tanıma sistemləri və sosial media vasitələrindən toplanması və düzgün strukturlaşdırılması nəzərdə tutulsa da fundamental idarəetmə problemləri hələ də qalmaqdadır.

NƏTİCƏ

Araşdırmalardan məlum oldu ki, Çinin müxtəlif bölgələrində sınaqdan keçirilən SCS-də tətbiq olunan cəza prinsipinin vətəndaşın hüquqlarını nə dərəcədə pozduğu və ya müdafiə etdiyi hələ də tam tədqiq olunmayıb. Sosial kreditin qiymətləndirilməsi əsasında vətəndaşın etimadının pozulmasını qanun pozuntusu kimi göstərmək üçün, bu, əvvəlcə hüquqi sənədlərdə öz əksini tapmalıdır. Bu səbəbdən, SCS-in dövlət idarəçiliyinə inteqrasiyasını yalnız dövlətdə hüquq anlayışının hərtərəfli yenidən nəzərdən keçirilməsindən sonra mümkün olacaqdır. SCS tətbiqi ilə ölkə vətəndaşlarının cəzalandırılması üsullarında yaranan yeni yanaşmalar qanun çərçivəsində həyata keçirilməlidir. Belə ki, sistemin müəyyən etdiyi cəza prinsipi dövlətin hüquqi sənədlərində öz əksini tapmayıbsa, sosial kreditə görə cəzalandırma qanunsuz hesab olunmalıdır.

Hər bir vətəndaşın və təşkilatın fərdi məlumatlarını nəzarətdə saxlamaq imkanına malik olması onun cəmiyyətdə etimad əldə etmək və nüfuz sahibinə çevrilməsinin həlledici faktorudur. Fərdi məlumatların təhlükəsizliyi, məxfilik, şəffaflıq və cavabdehlik İnternet istifadəçilərinin fəaliyyətində ön planda olmalı, şəbəkə texnologiyalarında nəzərə alınmalıdır. Fərdi məlumatların məxfiliyinin müxtəlif aspektləri mövcuddur. Bunlar milli

dəyərlər, mədəniyyət, sosial normalar, iqtisadiyyat, vətəndaş hüquqları ilə bağlıdır.

Araşdırmadan məlum oldu ki, informasiya texnologiyalarının inkişafı müşahidə cəmiyyətinin genişlənməsinə səbəb olmuşdur ki, bu da fərdi məlumatların təhlükəsizliyi problemini daha da aktuallaşdırmışdır. Müşahidə kameraları, üz tanıma sistemləri, süni intellektlə təchiz olunmuş dronlar, “əşyaların İnterneti” kimi müasir texnologiyalar vətəndaşların gündəlik həyatlarına müdaxilə edərək, davranışlarını qeydə alır. Vətəndaşların şəxsi həyatına müdaxilə, onların sosial-iqtisadi durumlarının informasiya sistemlərindən asılı vəziyyətə gətirilməsi demokratik dəyərlərə, “fərdi məlumatlardan vətəndaşın icazəsi olmadan istifadə edilə bilməz” prinsiplərinə ziddir. Lakin digər tərəfdən dövlətlərin informasiya təhlükəsizliyi, iqtisadi inkişafı, vətəndaşların rifahı, cinayətlərin qarşısının alınması və bir sıra həlli vacib məsələlərdə müşahidə cəmiyyətinin əhəmiyyəti böyükdür.

İSTİNADLAR

- [1] M. Blomberg, “The social credit system and China’s rule of law,” Mapping China Journal, 2018, no. 2, pp. 77–162.
- [2] Chinese Social Credit System (I): what it is – and what it isn't, <https://polikracia.com/the-chinese-social-credit-system/>
- [3] F.A.F. Ferreira, J.P. Esperanca, M.A.S. Xavier, et. al., “A socio-technical approach to the evaluation of social credit applications,” Operational Research Society, 2019, vol. 70, Issue 10, pp. 1801–1816.
- [4] S. Engelmann, M. Chen, F. Fischer, et. al., “Clear sanctions, vague rewards: How china’s social credit system currently defines “good” and “bad” behavior,” Proceedings of the 2019 Conference On Fairness, Accountability, and Transparency, Atlanta, 2019, pp. 69–78.
- [5] K. Rannenbergh, D. Royer, A. Deuker, “The future of identity in the information society: challenges and opportunities,” Identity in the Information Society, 2010, vol. 3, issue 3, pp. 599–604.
- [6] S. Matos, “Privacy and data protection in the surveillance society: The case of the Prum system,” Forensic and Legal Medicine, 2019, vol. 66, pp. 155–161.
- [7] B. Song, “Opinion the west may be wrong about China’s social credit system,” The World Post, 2018, <https://www.washingtonpost.com/news/worldpost/wp/2018/11/29/social-credit/>
- [8] F. Liang, V. Das, N. Kostyuk, M.M. Hussain “Constructing a data driven society: China’s social credit system as a state surveillance infrastructure,” Policy and Internet, 10(4), pp. 415-453, 2018.
- [9] Universal Declaration of Human Rights, <https://www.un.org/en/universal-declaration-human-rights/index.html>.
- [10] P. Mozur, “Inside China’s dystopian dreams: AI, shame and lots of cameras,” The New York Times, 2018, <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html?module=inline>
- [11] Z. Jiaquan, “Drones, facial recognition and a social credit system: 10 ways China watches its citizens,” South China Morning Post, 2018, <https://www.scmp.com/news/china/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-china>
- [12] K.W. Chan, “The Household Registration System and Migrant Labor in China: Notes on a Debate,” Population and Development Review, 2010, vol. 36, no. 2, pp. 357–364.
- [13] W.W. Moss, “Dang’an: Contemporary Chinese Archives,” The China Quarterly, 1996, no. 145, pp. 112–129.
- [14] Y. Chen, A.S.Y. Cheung, “The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System,” Comparative Law, 2017, vol. 12, no. 2, pp. 356–378.
- [15] D.V. Rooy, J. Bus, “Trust and privacy in the future internet – research perspective,” Identity in the Information Society, 2010, vol. 3, issue 2, pp 397–404.
- [16] M. Chorzempa, P. Triolo, S. Sacks, “China’s Social Credit System: A Mark of Progress or a Threat to Privacy?” Peterson Institute for International Economics, 2018, 39 p.
- [17] S.Y. Lei, “Beyond the Rule of Law: Rule-based Regulation under the Social Trustworthiness System,” Social Science Edition (Central South University), 2014, no.4, pp. 65–72.

PROMLEMS OF PERSONAL DATA MANAGEMENT IN SOCIAL CREDIT SYSTEMS

İrada Alakbarova

Institute of Information Technologies of ANAS, Baku, Azerbaijan

airada.09@gmail.com

Abstract— The development of information technology has created new opportunities for the collection and processing of personal data of citizens by state bodies and private companies. The use of social networks, tracking devices, face recognition and technologies such as the “smart city” has led to the formation of an surveillance society in countries. The article discusses the impact of surveillance society on people’s daily lives, as well as the degree to which China’s social credit system is in compliance with international legal principles for the protection of personal data. The aim of the study is to identify the role and problems of the surveillance society in assessing social loans of citizens.

Key words— *personal data; social credit system; observation society; citizen behavior; face recognition system; surveillance camera*

Kriptovalyutalarda konfidensiallıq və anonimlik problemləri

Yadigar İmamverdiyev¹, Firəngiz Sadiyeva²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹yadigar@iit.science.az, ²sadiyeva.firengiz@gmail.com

Xülasə— Məqalədə kriptovalyutalarda konfidensiallıq və anonimlik problemləri analiz edilir. Konfidensiallığın təmin edilməsi əksər kriptovalyutalarda əsas problemlərdən biridir və bunun üçün ilk növbədə tranzaksiya tərəflərinin anonimliyi təmin edilməlidir. Anonim kriptovalyutalarda istifadə edilən əsas mexanizmlərə baxılır, ölkələrin anonim kriptovalyutaların hüquqi tənzimlənməsi məsələlərinə yanaşmaları araşdırılır.

Açar sözlər— Bitcoin; kriptovalyuta; anonimlik; gizlilik; konfidensiallıq; anonim kriptovalyuta

I. GİRİŞ

Fərdin maliyyə ilə əlaqəli məlumatları olduqca sensitiv məlumatlardır və bədnıyyətlilərin əsas hədəflərindən biridir. Bunu çoxsaylı fərdi məlumat insidentləri ilə bağlı kütləvi informasiya vasitələrində yer alan xəbərlər də təsdiqləyir. Son onilliyin ən perspektivli və inqilabi maliyyə texnologiyası olan Bitcoin və digər kriptovalyutalar fərdi maliyyə məlumatlarının konfidensiallığının etibarlı qorunması üçün müəyyən vədlər verir [1, 2]. Bitcoin və digər altkoinlərdə fərdi maliyyə məlumatlarının konfidensiallığının təmin edilməsi üçün istifadə edilən əsas yanaşma anonimlik mexanizmləridir [3].

Kriptovalyutaların əsas xarakteristikalarından biri anonimlik hesab olunur: tranzaksiyanı yerinə yetirmək üçün istifadəçidən öz fərdi məlumatlarını daxil etmək tələb edilmir. Belə ki, Bitcoin blokçeynində göndərən və alanın adları və soyadları deyil, pulqabalarının rəqəmsal ünvanları və köçürülən məbləğ qeyd edilir. Qeyd edək ki, ilk və ən populyar kriptovalyutanın – Bitcoinin Satoşi Nakamoto təxəllüsü altında gizlənən yaradıcısının kimliyi hələ də məlum deyil [2].

Hazırda kriptovalyuta bazarının təxminən yarısına sahib olan Bitcoinin anonim olduğu iddia edilirdi, lakin tədqiqatlar göstərdi ki, əslində Bitcoin anonimliyi yox, psevdo-anonimliyi təmin edir [4]. Bitcoinin bu nöqsanını aradan qaldırmaq üçün təklif edilmiş bir sıra yeni kriptovalyutalar istifadəçilərin və tranzaksiya məlumatlarının anonimliyini daha yüksək səviyyədə qoruya bilər.

Lakin anonimliyin “tərs üzü” də vardır. Anonimlik bədnıyyətlilərə müxtəlif cinayət əməllərini, o cümlədən çirkli pulların yuyulması, kibercinayətkarlıq, beynəlxalq terrorizmin dəstəklənməsini rahat şəkildə həyata keçirməyə və hüquq-mühafizə orqanları tərəfindən aşkarlanmaqdan yayınmağa imkan verir. Buna görə əksər dövlətlər anonim kriptovalyutaların istifadəsini tənzimləməyə cəhdlər edirlər.

Bu işin məqsədi kriptovalyutalarda istifadə edilən konfidensiallıq və anonimlik mexanizmlərini və texnologiyalarını, onların istifadəçilərə verdiyi imkanları və cəmiyyətin təhlükəsizliyinə gətirdiyi problemləri analiz etməkdir.

II. KRİPTOVALYUTALARDA ANONİMLİK NƏ ÜÇÜN LAZIMDIR?

Biznes üçün maliyyə əməliyyatlarının konfidensiallığı və sürəti çox vacibdir. Böyük kriptovalyutalar bu məsələlərin öhdəsindən həmişə gələ bilmir. Mütəxəssislərə görə əksər kriptovalyutaların əsas problemi konfidensiallığın olmamasıdır.

Ödənişlər edilən zaman anonimliyin olmaması biznesə zərər gətirə bilər. Fiat pulları istifadə edilən zaman təşkilatın maliyyə hesabatlarına yalnız vergi xidməti giriş əldə edə bilər, lakin Bitcoin blokçeynində verilənlər bütün istifadəçilərə, o cümlədən rəqiblərə və bədnıyyətlilərə əlçatır olur və blokçeyndə baş verən tranzaksiyaları analiz etmək olar. Məsələn, tutaq ki, Bob Alisə 10 BTC hədiyyə edib. Bu zaman o, Alisin pulqabısının ünvanını bilir və Blockchain Explorer-də Alisin maliyyə əməliyyatları haqqında informasiyanı tapa bilər. Alisin tranzaksiyalarının tarixçəsinə görə onun neçə Bitcoinin olduğunu və onları nəyə xərclədiyini öyrənmək olar.

Beləliklə, kriptovalyutalarda maliyyə konfidensiallığı olmadıqda rəqiblər şirkətin kiminlə və hansı qiymətə müqavilələr bağladığını, əməkdaşlara nə qədər ödədiyini izləyə bilərlər. Mütəxəssislərə görə, kriptovalyutalarda konfidensiallığı təmin etmək üçün ilk növbədə onların anonimliyi təmin edilməlidir.

Ənənəvi bankçılıq modeli konfidensiallıq səviyyəsini iştirak edən tərəflərə və etibarlı üçüncü tərəfə məlumatların əldə olunmasını məhdudlaşdırmaq üsulu ilə yüksəldir. Bitcoin blokçeynində isə bütün əməliyyatları şəffaf etmək zərurəti bu ənənəvi üsulu açıq şəkildə pozur. Ancaq məlumat ictimaiyyətə açıq olduğu halda da, Bitcoin sistemi onun konfidensiallığını qoruya bilər. Belə ki, ictimaiyyət bir istifadəçinin müəyyən bir məbləği digər istifadəçiyə göndərdiyini görür, ancaq bu istifadəçilərin kimliyi ilə bağlı məlumat əldə edə bilmir.

III. BİTKOİNİN ANONİMLİK MEXANİZMİ

Ənənəvi maliyyə sistemlərində tranzaksiyaların həyata keçirilməsi üçün istifadəçilərin adlarından istifadə olunur, lakin Bitcoinə psevdo-adlardan istifadə olunur.

Bitkoin şəbəkəsində anonimliyi təmin etmək üçün Bitkoin pulqabılarının rəqəmsal ünvanları istifadə edilir. Bitkoin şəbəkəsində pulqabı dedikdə fayl sistemində bir fayl nəzərdə tutulur. Pulqabıda açıq və gizli açar cütü və yerinə yetirilmiş tranzaksiyalar qeyd olunur. Açarlardan Bitkoinin göndərilməsi və qəbul edilməsi üçün istifadə edilir. Açıq açarı Bitkoinləri qəbul edən şəxs imzanın təsdiqlənməsi üçün, gizli açarı isə Bitkoinləri göndərən şəxs imzalamaq üçün istifadə edir. Bitkoin pulqabısında hər bir Bitkoin ünvanlarına uyğun giriş və çıxışlar saxlanılır [3,4].

Bitkoin ünvanı onun istifadəçisi tərəfindən yaradılan asimmetrik açar cütliyünün açıq açarından əldə edilmiş bir hərf-ədəd sətirindən ibarətdir. Hər bir istifadəçi pulqabısında bir neçə açar cütü (ünvan) saxlaya bilər və buna görə də anonimlik səviyyəsini artırmaq üçün hər bir tranzaksiya görə yeni bir ünvanndan istifadə etmək tövsiyə olunur.

Beləliklə, Bitkoin şəbəkəsində anonimliyi təmin etmək üçün görülən yeganə iş ünvanların psevdo-adlarından istifadə edərək açıq açarları anonim saxlamaqdır. Psevdo-adlar Bitkoin tranzaksiyalarında istifadə edildiyi üçün ümumi təəssürat yaranır ki, bu adlar Bitkoinin anonimliyini təmin edir. Lakin bir sıra mütəxəssislər açıq şəkildə bəyan edirlər ki, Bitkoin anonim deyil və “dünyadakı ən şəffaf ödəmə şəbəkəsi olduğu ehtimal olunur” [3].

Bitkoində qrup identifikasiyası “ünvanların dəyişilməsi” (ing. change addresses) anlayışından istifadə edən dəyişiklik evristikasını tətbiq etməklə istifadəçilərin anonimliyini artırmaqla, lakin tam təmin edə bilməz. Klasterləri xarici mənbələrdə: məsələn, ictimaiyyətə açıq olan blockchain.info, walletexplorer.org kimi xüsusi saytlarda məlumatlar ilə korrelyasiya etdikdə bütün Bitkoin tranzaksiya şəbəkəsinin böyük hissəsini deanonimləşdirmək mümkün olur.

[4]-də Harrigan və Fretter belə bir nəticəyə gəlirlər ki, Bitkoin şəbəkəsindəki ünvanların qruplaşdırılmasının effektiv olmasının səbəbi müəyyən edilmiş ünvanların təkrar istifadəsi və superklasterlərin artmasıdır (məsələn, birjalar, qumar oyunları saytları, qara bazar saytları) [5].

Hər bir tranzaksiya üçün yeni açar cütünün istifadə olunması təhlükəsizliyi artırır. Bəzi hallarda çox girişli tranzaksiyalar həyata keçirilir ki, bu tranzaksiyaların girişləri eyni sahibə məxsus olur. Bu halda bir açarın sahibi aşkar edildikdə, bu açar eyni sahibə məxsus olan digər tranzaksiyaları aşkar edə bilər.

Bitkoinin istifadəçilərini ünvan təkrar istifadə etdikdə və ya birjada verifikasiyadan keçdikdən sonra de-anonimləşdirmək olur. Anonim kriptovalyutalarda isə belə hal mümkün deyil. Onların istifadə etdikləri kriptoqrafik protokollar həmin şəbəkədəki verilənlərin analizini çətinləşdirir. Anonim kriptovalyutanın pulqabı ünvanını yalnız onun sahibi açar bilər.

IV. KRIPTOVALYUTALARDA ANONİMLİK TEKNOLOGİYALARI

Bu bölmədə blokçeyndə saxlanılan tranzaksiyaların miqdarını, göndərən və alanın anonimliyini təmin etmək üçün bəzi texnologiyalara baxılır.

Bu texnoloji həllərə misal olaraq birdəfəlik istifadə ödəniş ünvanları (One-time Use Payment Addresses), gizli ünvanlar (Stealth addresses), qarışdırma (Mixing), CoinJoin, sıfır bilik verməklə isbat (Zero-Knowledge Proofs), zk-SNARKs, Pedersen etibarnamələri (Pedersen Commitments) və halqa imzalarını (Ring Signatures) göstərmək olar.

One-time Use Payment Address – eyni ödəmə ünvanını təkrar istifadə etdikdə, müşahidəçi göndərən və alanın tranzaksiyalarını izləyə bilər. Yeganə çıxış yolu ünvanı təkrar istifadə etməməkdir. “Birdəfəlik istifadə ödəniş ünvanları” yanasmasını istifadə etdikdə göndərən hər tranzaksiya üçün yeni bir ünvan yaradır. Yeni ünvan blokçeyndə daha öncə qeyd olunmadığı üçün, müşahidəçinin tranzaksiya axınını izləməsi çox çətin olur. Birdəfəlik istifadə ödəniş ünvanı həm depozitə qoyulan, həm də çıxarılan tranzaksiyaların hər ikisi ilə birbaşa əlaqədardır.

Stealth Address – Hər yeni ünvan alıcı tərəfindən yaradılmalı və göndərənə çatdırılmalıdır. Alan şəxs hər dəfə yeni e-poçt istifadə etmək üçün bunun vacib olması səbəbini və tranzaksiyanı qəbul etmək üçün hansı ünvanndan istifadə edəcəyini göndərən şəxsə bildirməlidir. Stealth ünvanlar göndərən yeni birdəfəlik istifadə ödəniş ünvanları yaratmasına icazə verməklə bu problemi aradan qaldırır.

Mixing – Ünvanndan tranzaksiyaların axınını izləmək çox sadədir. Birdəfəlik istifadə ödəniş ünvanlarından fərqli olaraq Mixing xidməti bu problemi həll edə bilər.

Bitkoin istifadəçiləri bir çox istifadəçidən Bitkoin alan, bunları birlikdə qarışdırıb fərqli vaxtda fərqli ünvanlara göndərən Bitkoin Fog və BitMixer kimi qarışdırma xidmətlərindən (Tumbler də deyilir) istifadə etməklə tranzaksiyaları və daha kiçik miqdarlara bölərək tranzaksiya axınını izləməyi aradan qaldıra bilər. Bunlar bir çox istifadəçinin pulunu digərinə göndərməzdən əvvəl bir müddət nəzarətdə saxlayan və bir-birinə qarışdıran üçüncü tərəf xidmətləridir.

CoinJoin – Mixing xidmətinin zəif tərəfi etibarlı üçüncü tərəf daxil etməsidir. CoinJoin üçüncü tərəf tələbini aradan qaldırmağa çalışan qarışdırma üsuludur. CoinJoin tək bir tranzaksiyanın birdən çox giriş və çıxışlara malik olması xüsusiyyətindən istifadə edir.

Valyutaları tələb olunduğu kimi qarışdırmaq üçün etibarlı üçüncü tərəfə ehtiyac yoxdur. Lakin CoinJoin tranzaksiyasında iştirak edən bütün tərəflər bu tranzaksiyanı imzalamaq üçün bir-birləri ilə əlaqə qurmalıdır. Bu koordinasiya bir çox səbəbdən çətin yerinə yetirilir. Birincisi, istənilən vaxt CoinJoin tranzaksiyasına yetərinə insan qoşulmaya bilər. İkincisi, CoinJoin tranzaksiyasında iştirak edən hər kəs kimin iştirak etdiyini və bu tranzaksiyanın necə qarışdırılacağını bilir.

CoinShuffle – CoinJoin tranzaksiyasında iştirak edən bütün tərəflərin üçüncü tərəf olmadan tranzaksiyalar yarada biləcəyi və heç bir tərəfin sahib olmadığı mərkəzləşdirilməmiş tranzaksiyaların aparılmasına icazə vermək üçün tövsiyə olunan bir üsuldur.

Zero-Knowledge Proofs – sabit paroldan istifadə edən protokolların çatışmayan cəhəti isbat edən (P) tərəfin öz parolunu yoxlayan (V) tərəfə verməsidir. “Sorgu-cavab” tipli protokollar bu nöqsanı aradan qaldırır. Onları həyata keçirən zaman P V-nin zamana görə dəyişən sorğularına cavab verir və V-yə onun adından çıxış edə biləcək informasiya vermir. Bununla belə P öz sirri barəsində qismən məlumat verə bilər. Bu problemi sıfır bilik verməklə isbat protokolları həll edə bilər [6].

Pedersen etibarnamələri – etibarnamələr verilənlərin bir hissəsini gizli saxlayan, lakin onların kriptografik heş kodlarını elan edərək etibarlılığını (commit) təmin edən kriptografik mexanizmlərdir. Verilənlərin ölçüsü çox kiçik olduqda (məsələn, 1 ədəd), onda kobud güc axtarışının köməyi ilə görünən verilənlərin riskini minimuma endirmək üçün örtük faktoru əlavə edilir.

Confidential Transaction-lar Pedersen etibarlılığından Bitcoin tranzaksiyalarının köçürülməsi zamanı miqdarın gizli saxlanması üçün bir vasitə kimi istifadə edir. Bu fikir ilk dəfə 2013-cü ildə Adam Back tərəfindən irəli sürülmüşdür.

Halqa imzaları – Standart bir rəqəmsal imzanı təsdiqləmək üçün yoxlayan imza yaratmaq üçün hansı açıq açarı istifadə edildiyini bilməlidir, bu səbəbdən ünvandan -ünvana vəsait axınını izləmək mümkün olur. Halqa imzalar 2001-ci ildə R. L. Rivest, A. Şamir və Y. Tauman tərəfindən kəşf edilmişdir.

Halqa imzaları imza yaradanın öz açarını və onun tərəfindən seçilmiş bir neçə açıq açarı (bu açıq açar sahiblərinin razılığı və iştirakı tələb olunmur) özündə birləşdirən açarlar qrupundan istifadə etməklə yaradılır. Üçüncü tərəf nəticədəki imzanın qrupdakı açarlardan biri istifadə olunaraq yaradıldığını yoxlaya bilər, lakin qrupdakı hansı açarın imzalayana aid olduğunu müəyyən etmək mümkün deyil. Bu? açıq açarlardan istifadə edərək bir halqa tənliyini qurmaqla həll edilir, burada bir hesablamanın çıxışı digərinin girişinə çevrilir. Gizli açarlardan birini bilən şəxs (z) halqa tənliyinin son çıxışının ilkin giriş olan (v)-ə bərabər olmasını təmin edir.

Blokçeyndə göndərənə naməlum olduğu əməliyyatları təsdiqləmək üçün halqa imzaları istifadə edilə bilər.

Gizli ünvanlar yalnız alıcının konfidensiallığını və gizliliyini təmin edir. Pedersen etibarlılığı yalnız tranzaksiyaların miqdarının konfidensiallığını və gizliliyini təmin edir. Halqa imzaları yalnız göndərənə konfidensiallığını və gizliliyini məhdud şəkildə qoruyur. Zk-SNARKs isə alanın deyil, göndərən və miqdarın konfidensiallığını və gizliliyini təmin edir [7].

MimbleWimble protokolu tranzaksiyaları izləmək üçün elliptik əyrilər metodunu, həmçinin Confidential Transactions və CoinJoin mexanizmlərini istifadə edir. Confidential Transactions ödəniş ünvanlarını və həcmi gizlədir, CoinJoin isə tranzaksiya girişlərini və çıxışlarını qarışdırmaqla bir neçə tranzaksiyanı birləşdirir.

Mimble Wimble-də ənənəvi ünvanlar yoxdur, onların əvəzinə pulqabıları bir-biri ilə verilənləri mübadilə edirlər. Bu

zaman MimbleWimble blokçeynində tranzaksiyaların tarixəsi saxlanılır. Orada sahiblər və pulların vəziyyəti haqqında məlumat yazılır. Beam yaradıcılarının qiymətləndirilməsinə görə belə blokçeynlər Bitcoin blokçeynindən ən azı üç dəfə kiçik olacaq.

V. ANONİM KRIPTOVALYUTALAR

Bəzi kriptovalyutalar rahat ödəniş və ya sürətli tranzaksiyalara, bəziləri isə istifadəçilər üçün anonimlik təmin etməyə daha çox diqqət yetirirlər.

Ümumiyyətlə, anonim kriptovalyutalarda aşağıdakı xüsusiyyətləri təmin etmək tələb olunur.

- **Gizlilik:** Bütün tranzaksiyaların hansı ünvandan gəldiyi, hansı ünvana göndərildiyi və miqdarının rəqiblər tərəfindən müşahidə edilməməsi təmin edilir.
- **İzlənilməzlik:** Göndərilən və ya alınan valyutaların izlənilməməsi və tranzaksiya tarixi ilə arasındakı əlaqənin aşkarlanma bilməməsi təmin edilir.
- **Dəyişkənlik:** Bütün valyutaların cüt şəkildə bir-birindən ayrılmaz olması və nəticədə bir-birlərini əvəz edə bilməsi təmin edilir.

İlk anonim kriptovalyuta Bytecoin 2012-ci ildə buraxılmışdır. Həmin vaxtdan xeyli belə kriptovalyuta meydana çıxmışdı, onlardan Monero, Dash, PIVX, Verge və Zcash populyarlıq qazanıb.

Monero – CryptoNote istifadə edən Bytecoin əsasında hazırlanmışdır və tranzaksiyaların detallarını görmək üçün açıq açarı paylaşmağa imkan verir.

Konfidensiallığı təmin etmək üçün Monero halqa imzaları və gizli ünvanları istifadə edir, onlar sikkələri, tranzaksiyaların həcmələrini və onların ünvanlarını gizlədir. Moneronun nöqsanı – tranzaksiyanın ölçüsünün böyük olması və miqyaslanma problemləridir. Bir tranzaksiya hesabında Monero blokçeyni Bitcoin blokçeynindən beş dəfə böyükdür.

2017-ci ildə Monero kodunda aşkarlanmış boşluqlar sayəsində tədqiqatçılar real tranzaksiyaları saxtalardan ayırmağa nail olmuşdular.

Dash – Bitcoinə olan bəzi problemləri həll edir. Bitcoin bərabərhüquqlu birrəngli şəbəkə olduğu halda, Dash ikirəngli arxitektura ilə işləyir. Birinci səviyyədə Bitcoin kimi mayninq vasitəsilə valyutalar buraxılır və yeni bloklar blokçeynə yazılır, ikinci səviyyədə isə əsas qovşaqlar, yəni Masternodlar yerləşir. Dash anonim kriptovalyutasında PrivateSend mexanizmi istifadə edilir, o bir neçə istifadəçinin pullarını qarışdırır və onları bir tranzaksiyada birləşdirir. Qarışdırma Masternodlarda baş verir, qarışdırmadan sonra alanı və göndərənə izləmək praktiki olaraq mümkün deyil, lakin onlar barədə informasiya Masternodlarda qalır. Bu səbəbdən Dash-ı tamamilə konfidensial kriptovalyuta hesab etmək olmaz. Bundan başqa, Dash Bitcoin-dən daha az təsdiqləmə vaxtı ilə ikiqat xərcləmə (ing.double spending) problemini həll edən InstantSend adlı sürətli tranzaksiya təqdim edir.

PIVX – əvvəllər Darknet kimi tanınan PIVX (Private Instant Verified Transaction) gizli anı yoxlanmış tranzaksiyalar mənasını verir. PIVX Dash-ın bir forkudur, yəni özünün texniki əlamətlərini, sürətli tranzaksiya yerinə yetirə bilmək bacarığını və əsas qovşaqlarını Dash-dan götürmüşdür. Lakin Dash-dan fərqli olaraq PIVX PoW (Proof of Work) istifadə edən maynerlər yox, tranzaksiyaları təsdiqləmək üçün əsas qovşaqlar istifadə edən PoS (Proof of Stake) konsensus alqoritmindən istifadə edir.

Verge – əvvəllər DogeCoinDark olaraq tanınırdı. Anonimlik təmin etmək üçün əlavə kriptografik metodlar istifadə etmək əvəzinə, göndərən və alanın IP ünvanlarını və coğrafi yerlərini gizlətmək üçün Tor və I2P-nin integrasiyasına əsaslanır. Verge-nin Bitcoin əsasında olmasına baxmayaraq, əməliyyatlarda kriptografik metodlardan istifadə etmir. Buna görə də blokçeyndəki tranzaksiyalar şəffafdır.

Zcash – kriptovalyutada sıfır bilik verməklə isbat protokolu zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) istifadə edilir. Zcash-də anonim tranzaksiyaları yalnız şifrlənmiş z-ünvanlarından həyata keçirmək olar, onlar blokçeyndə görünür. Belə tranzaksiyalar ediləndə vəsaitlər yandırılır və yeni sikkələrə mübadilə edilir. zk-SNARKs – sıfır bilik verməklə isbatın yeni formasıdır və Zcash bu alqoritmın ilk geniş yayılmış tətbiqidir.

Zcash-ın nöqsanları zk-SNARKs texnologiyasının mürəkkəbliyi və etibarlı quraşdırma (trusted setup) tələbinin olmasıdır. Zcash yaradıcıları zk-SNARKs-ın başlanğıc parametrləri üçün təsadüfi parametrlər istifadə edirlər. Bu parametrlər bədnıyyətlilərin əlinə düşsə, şəbəkədə verilənləri saxtalaşdırı bilər. Bundan başqa, Zcash blokçeynində bir tranzaksiya Bitcoin blokçeynindən səkkiz dəfə böyükdür.

Zcash-də anonimlik istəyə bağlıdır və ekranlaşdırılmış tranzaksiyaları həyata keçirmək üçün həm göndərən, həm də alandan şəffaf ünvanlar əvəzinə ekranlaşdırılmış (ing. shielded) ünvanlardan istifadə etmək tələb olunur. Zcash valyutaların orta hesabla təxminən 6.3%-i ekranlaşdırılmış ünvanlardan istifadə etdikləri müşahidə edilib [8,9].

VI. ANONİM KRİPTOVALYUTALARIN HÜQUQİ TƏNZİMLƏNMƏSİ MƏSƏLƏLƏRİ

Anonimlik – istifadəçinin öz tranzaksiyalarının gizliyinin saxlanmasına olan şərtsiz hüququ kimi başa düşülür. Bununla yanaşı, anonimlik pulların yuyulması və digər kriminal sxemlərinin hissəsi kimi qanunsuz hesab olunur. Belə hallara çoxsaylı misallar vardır.

Bitcoin ilk illərində narkotik tacirlərinin əsas valyutasına çevrilmişdi. Bunun səbəbi qanunsuz mallarla anonim ticarət platforması olan Silk Road veb saytı idi, sayt 2011-ci ildən fəaliyyət göstərirdi. Onun sahibi 2013-cü ildə həbs edilmiş və ömürlük həbsə məhkum edilmişdi. 2012-2013-cü illərdə saytda 1,2 milyon dollarlıq alqı-satqı edilmişdi, ümumi məbləğ 9,5 milyon bitcoin təşkil etmişdi. Alqı-satqıdan gələn komissiya haqqı sayəsində Silk Road təxminən 600 min bitcoin qazanmışdı [10].

Silk Road pulqabısı – alıcılar, satıcılar və bu tranzaksiyalar haqqında öyrənmək istəyən üçüncü tərəflər arasında yüksək səviyyədə bir anonimlik təmin etməyə yönəlmişdi. O, "Tor

brauzer paketi" kimi nisbətən asan istifadə olunan brauzer interfeysinin yaranması ilə mümkün olan bir neçə anonim şəbəkədən biri idi [10].

Dövlətlərin bir çoxunda kriptovalyutalarla həyata keçirilən daxili alış-veriş üçün ciddi KYC (Know your customer) – müştərinin tanıma prosesi tətbiq olunur və kriptovalyuta istifadə etmək üçün qeydiyyatdan keçən istifadəçilərin fərdi məlumatları tələb olunur.

Dövlətlər anonim kriptovalyutaların tranzaksiyalarını izləyə bilmirlər və buna görə anonim kriptovalyutalara mənfi yanaşırlar, bəzən onları tamamilə qadağan edirlər. Məsələn, 2018-ci ildə Cənubi Koreyada anonim kriptotreyding, Yaponiyada isə kriptovalyutaların özü qadağan edilmişdir. Lakin belə qadağaların effektivliyi birqıymətli deyil.

Bəzi mütəxəssislər buna mane olmağın mümkün olmadığını söyləyirlər. Yaponiya vətəndaşları anonim altkoinləri yapon kriptovalyuta birjalarında deyil, digər meydançalarda əldə edə bilirlər.

ABŞ güc strukturları açıq blokçeynli kriptovalyutalar (o cümlədən Bitcoin və Ethereum) istifadə etməklə qanunsuz maliyyə fəaliyyətinin monitorinqində uğurlar qazanırlar. Lakin anonim kriptovalyutaların blokçeynlərində edilmiş tranzaksiyalar xeyli yüksək konfidensiallıq səviyyəsinə malikdir. ABŞ Milli Təhlükəsizlik Nazirliyi qeyri-qanuni pul köçürmələrini aşkarlamaq məqsədi ilə anonim kriptovalyuta blokçeynlərində tranzaksiyaların izlənməsi texnologiyasını işləməyi planlaşdırır.

Ödəniş iştirakçılarını identifikasiya etmək üçün yeni analitika vasitələri işləmək lazımdır. Daha bir istiqamət-anonim rəqəmsal aktivlərin istifadəsi ilə əlaqədar problemlərin həllinə yönəlmiş qanunvericilik tədbirlərinin işlənməsi tövsiyə olunur.

NƏTİCƏ

Anonim kriptovalyutalar maliyyə əməliyyatlarının gizliliyini və konfidensiallığını qiymətləndirən hər bir kəsə (biznesə – tranzaksiyalar haqqında həssas informasiyanı, şəxslərə – şəxsi həyatın toxunulmazlığını təmin etmək üçün) lazımdır. Lakin kriptovalyutaların anonimliyi kibercinayətkarlıqla mübarizəni xeyli çətinləşdirir. Anonim kriptovalyutaların dələduzluq, Darknet-də ödənişlər üçün istifadəsi halları onların cəmiyyətdə nüfuzuna xələl gətirir. Lakin anonim kriptovalyutalardan cinayətkarlar istifadə edə bilsələr də, onların əsas məqsədləri fərdi məlumatların mühafizəsidir.

İSTİNADLAR

- [1] Y. İmamverdiyev "Blokçeyn texnologiyaları: komponentləri, tətbiqləri və problemləri", İnformasiya cəmiyyəti problemləri, 2019, №2, s. 18–32.
- [2] Y. İmamverdiyev, F. Sadiyeva, "Kriptovalyuta verilənlərinin intellektual analizi məsələləri," İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri IV respublika konfransı, s. 47-53, 2018.
- [3] M. C. K. Khalilov and A. Levi "A survey on anonymity and privacy in bitcoin-like digital cash systems", IEEE Communications Surveys & Tutorials, 20(3), pp. 2543-2585, 2018.
- [4] M. Harrigan and C. Fretter, "The unreasonable effectiveness of address clustering", Conferences on Ubiquitous Intelligence & Computing, pp. 368-373, 2016.

- [5] M. Paquet-Clouston, B. Haslhofer and B. Dupont, “Ransomware payments in the bitcoin ecosystem”, Journal of Cybersecurity, 5(1), tyz003, 2019.
- [6] J. H. Lee, “Rise of anonymous cryptocurrencies”, Brief Introduction. IEEE Consumer Electronics Magazine, 8(5), 20-25, 2019.
- [7] D. Yang, J. Gavigan and Z. Wilcox-O’Hearn “Survey of confidentiality and privacy preserving technologies for blockchains”, R3, Zcash Company, Res. Rep, 2016.
- [8] D. Hopwood, S. Bowe, T. Hornby and N. Wilcox, "Zcash protocol specification (version 2018.0-beta-9)", 2018.
- [9] P. Dikshit, and S. Kunwar, “Efficient weighted threshold ECDSA for securing Bitcoin wallet,” Asia security and Privacy (ISEASP), pp 1-9, 2017.
- [10] L. J. Trautman “Virtual currencies; Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?,” Richmond Journal of Law and Technology, 20(4). 2014.

PRIVACY AND ANONIMITY ISSUES IN CRYPTOCURRENCIES

Yadigar Imamverdiyev¹, Firangiz Sadiyeva²

^{1, 2}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹yadigar@iit.science.az, ²sadiyeva.firangiz@gmail.com

Abstract – The paper analyzes privacy and anonymity issues in cryptocurrencies. Confidentiality is one of the main issues in most cryptocurrencies, and for that, the anonymity of the transaction participants must be ensured. The main mechanisms used in anonymous cryptocurrencies are reviewed, and countries' approaches to the legal regulation of anonymous cryptocurrencies are being investigated.

Keywords – *Bitcoin; cryptocurrency; anonymity; Privacy, confidentiality; anonymous cryptocurrency*

Protecting and securing medical records using blockchain technology

Gulara Muradova¹, Mehran Hematyar²

^{1,2}Azerbaijan Technical University, Baku, Azerbaijan

²Tehran, Iran

¹gulara.muradova@gmail.com, ²m.hemmatyar@outlook.com

Abstract— E-health is a developed infrastructure, in which usage becomes important to collect, secure and protect personal patients' data, as well as to various medical resources. According to this aspect of view, trying to protect and secure data considering its reliable storage is more important than ever. The necessity of proving a stable and trust-base system is a big challenge in healthcare. Offering a way to consider saving, securing and protecting the data anonymously blockchain technology application in E-health, is the main purpose of this paper.

Keywords— *medical data; blockchain technology; medical blockchain; blockchain in healthcare; information security in healthcare; data information security; information security in blockchain, decentralized healthcare system; protected health information*

I. INTRODUCTION

E-health paradigm shift has resulted in innovative technologies in healthcare industry that differ from traditional health care. The primary goal of e-health is to facilitate access to necessary information on delivery of assistance to the population in the field of cooperation of medical organizations and the establishment of practical analysis instruments of healthcare system administration. The effectiveness of administration includes the provision of unified tools of collective work with information for data analysis, formation of standard accountability, implementation of operative monitoring of various indicators of activity [1,2].

Most healthcare information, from electronic-based medical records in health systems to patient registries and histories, in these days grew up organically for example from custom in-house systems, little or Medium Medical department and largely standards or protocols-free. Databases of healthcare data containing the histories of many patients (medical records) are of enormous value: They can be mined for correlations between patient and a huge range of behaviors, seemingly unrelated conditions, and demographic factors to identify early warning triggers that can be used to bolster preventative care management. We need access to as much of this data as possible. The problem, then, is accessing several claims sources in a way that's secure enough to satisfy all stakeholders. And one security technology rises above all

others to meet this challenge: blockchain. blockchain may have the potential to make it easier for approved entities to exchange protected health information [3-8].

IBM Global Business Service Public Sector, said we see strong potential for blockchain applications in healthcare 16 uses of blockchain in healthcare ranging from identity verification to genomics research. IBM Global Business Service Public Sector. “We are seeing emerging interest from health systems”- considers National Institute for Standards and Technology (NIST) [9].

The topics and applications for blockchain technology in healthcare following:

- Improving interoperability for information exchange, patient tracking.
- Improving healthcare claims processing, including using “smart contracts”.
- Opportunities for using blockchain in health information exchange to satisfy national healthcare objectives.
- A prototype decentralized record management system for electronic health records.
- Storing patient health data securely.
- A blockchain-based access control management system for health records.
- Sharing patient data with network consensus instead of a single centralized source [9-12].

II. BLOCKCHAIN TECHNOLOGY ACCOUNTS FOR THE ISSUES OF SECURITY

The word "block" is made up of two words "block" and "chain" means a chain, which means ultimately a chain of blocks. Blockchain is a decentralized information and reporting system. In the blocks, any information can be entered and recorded. In the Blockchain, these blocks of information are linked together in a chain, forming a sequence of information. This technology is, in fact, a distributed database that anyone can check in on those transactions. In simpler terms, blockchain is a platform that enables the transfer of information from one location to another with high

security. One of the interesting things about the Blockchain is that its open source technology. This technology has no owners and no one at the top of the network, which increases the trust of its members because no one can change the network and transactions in his or her benefit. In other words, to control and access to transactions by every member of Blockchain network can significantly increase the security and trust. So, the most important and at the same time strangest feature of the block is and has the power to do so. For example, group of 4 people takes a picture with their cellphone. Now if everyone deletes or modifies that information, it will no longer be acceptable to the public because they have a copy of the original unless I remove everyone's mobile and delete it. Now, this crowd can be public and above the millions of people, we see in Bitcoin, Ethereum and other Blockchain currencies, or privately for a specific community. Blockchain is an example of a private Blockchain chain. When you connect to a Blockchain, you get a copy of the entire Blockchain. No change is possible in the Blockchain unless more than 5% of the data on networked computers is changed.

Blockchain technology is not in itself a fundamental technology, but rather a set of hashing and encryption, mass distribution, and so on processes that have created the idea of a blockchain. Consider the Blockchain as the archive on which information is recorded. A Blockchain may not be much different from Wikipedia. Using a blockchain, many people can import different reports into one type of information archive, and users can control how the information is recorded and updated. Similarly, Wikipedia articles are not the product of a publisher. On Wikipedia, a user, with the permissions assigned to his account by the system, can modify all or some of the Wikipedia entries stored on a centralized server. But the main concern is that database control remains with Wikipedia administrators, and that access to permissions and permissions is maintained by a central authority. Some Wikipedia executives can delete an article at any time, but in blockchain users own the database information and the information on the Blockchain is not deleted. Wikipedia's digital strength is similar to the security of centralized databases of today's governments, banks, or insurance companies. The control of centralized databases is in the hands of their owners. Administrators of a site can have access to and control over This is another important feature of blockchain technology. Wikipedia's Master Copy database is edited on one or more specific servers by users and all users view the new version. In the case of blockchain, each node logs an independent report on the network, and each independent record becomes a set of official reports with other records [13-16].

III. BLOCKCHAIN TECHNOLOGY IN HEALTHCARE

Any information can be recorded in any block, from a person's crimes to the display of account information for assets. In the Blockchain, the information is contained in the

blocks and linked together in a chain. The difference with other systems is that the information stored on this type of system is shared among all members of the network and it is almost impossible to delete and manipulate the recorded information using encryption. Consider the following blockchain, for example, each block showing a clinic where patients' names and records are recorded. If a character is added to the hospital's patient name information, the hash block will change and subsequent blocks will be invalidated, which is why this technology is called the blockchain or blockchain technology.

The blockchain chain or blockchain chain is a system for recording data. This data can be for example bank transactions or medical data, appointments, personal messages or other information. The blockchain feature is that it is possible to store this data without a central manager and authority, and it cannot be distorted or destroyed by destroying a central point. Fig. 1 shows the created 3 blocks of a block chain that starts from genesis (first block) to 3rd one, here we have genesis block hash as genesis hash and every next block has the hash of the previous block as an inseparable part of each block. In a block chain each block contains 3 major parts 1st of that is the block hash 2nd is the hash of first, depended and pervious block, it means that a chain provided with dependent blocks and every edit or change in each block inside the chain changes the chain all, it means chain brakes or new chain creates.

Fig. 1. Hash of pervious block as an inseparable part of each block

This is possible that someone changes the content of a block, therefor the subsequence of a block hash will update, but you did not consider distribution. Blockchain data is not stored on a specific computer or server. Each computer or system connected to the network receives a copy of the Blockchain. Each of these blocks has something called a hash. A hash is a string of characters made with specific functions. It is clear that to hash is a one-way security role and to find the hash or algorithms cannot cause to find the clear data, on the other hand, the security provided by huge and safe hashing algorithms such as MD5, etc.

Protected health information (PHI) as the personal or health care information of persons are so important and to save, secure, safe transfer, protect and accessibility is very important and supplies in this method.

Fig. 2. Emerging a new block, add and structure of joining to block chain

Fig. 2 tries to show how a new block creating, first of all, a block prefers to chain network and after passing the structure and giving the publishing rights, it confirms or rejects by taking-vote and peer to peer protocols. For accessing the best purpose every confirmation takes up to 10 minutes, on the other hand this time increases the security as well as possible. The block chain can facilitate secure online transactions. The block chain is a decentralized, democratic, Vote-based, distributed digital library used to send, receive and record transactions across multiple, unlimited computers so that values can be recorded the transactions without changing all or a part of subsequent blocks and without network collaboration and in each level savings are changing. This allows participants to review and audit cheap transactions. Their authenticity is verified by collective collaboration through the sharing of their interests. Consequently, a workflow It is strong enough that participants' uncertainty about data security is marginal . Using a block chain eliminates the characteristic of infinite replication of a digital asset. This confirms that each unit of value is transferred only once and has resolved the longstanding problem of double costs. The blockchain chain is defined as a cryptographic validation protocol. This blockchain-based exchange can be completed faster, more safely and cheaper than traditional systems. The blockchain can assign or offer title rights because it holds a record that provides presentation and acceptance. The Batch Chain is a distributed, consensus-based database that continuously maintains a list of records (categories) that each reference to

previous list options, thereby reinforcing the challenge of undermining or unauthorized revision and improve the security. The blockchain itself is a subdivision of Distributed Ledger technologies. In other words the Blockchain is a type of data architecture used in distributed office technology in which transaction records are stored in interconnected chains.

In this technology, with multiple users simultaneously recording and modifying data that may overlap, the network is able to maintain database content integrity. Due to the encrypted data structure that the Block Chain has, integration is maintained without any central controller. Intentional or unwanted these days concept of Blockchain ties to cryptocurrency especially Bitcoin. In Bitcoin's distributed headquarters, it is difficult to solve a mathematical problem in order to sort out transactions and avoid inconsistencies, Once the problem is resolved, verification is easy. This mechanism is called "Proof of work". In the bitcoin block chain method, one can arrange the transactions of each step that find the answer to this difficult question while simultaneously making changes that it intends to apply (the new block) to the previous steps of the chain. The way to discover the inconsistency is that the transactions of each block enter the hash function and all members have a hash response if the one who arranges and adds the transactions even makes a minor change to the previously confirmed transactions, the hash response changes and Without having to know which part has changed, they can oppose the unauthorized change [12,17].

In this paper, we decided to prefer blockchain for using in healthcare but first, we need to have a quick view to compare a traditional system with a new one we prefer. In a traditional medical clinic or system, we face different and island form networks and systems. In this system, each clinic uses own data base, systems or network. The main problem is if the system fails or being attacked or being destructed. But if we use a big, compatible, secure, fast, decentralized and truth base network as Blockchain we have a specified amount copy of information that has a good resistance against destruction, attack, rubbish, unauthorized modify, etc. In this proposal each person doesn't have to go to the repetitious medical center if he or she doesn't like, on the other, hand he/she can use every medical center and don't worry about transfer his or her medical records, to lost, to destruction or incorrect human mistakes. Health data can be shared across the distributed network and would be accessible to approved individuals or entities.

Fig. 3 Protect and secures in every block of blockchain according to medical records and with passing the time everybody achieve his own MBC

Fig. 3, explains clearly that how the confirmed medical data saves, protect and secures in every block of blockchain according to medical records and with passing the time everybody achieve his own “Medical Block Chain”(MBC) securely and time lapse can improve, extend, protect and complete his/her MBC. In other hand every problem in the past genre of everybody can be process, view, study and help every medical centers PHI and secure ways to solve many problems in next genre such as genetic problems. The database distributed by Blockchain Technology essentially creates a completely different digital backend. This is another important feature of blockchain technology.

CONCLUSION

We, as proponents of blockchain technology in healthcare, see it as an opportunity to overcome the data exchange and security challenges surrounding PHI. Succeeding in healthcare today means navigating the intersection between policy and technology. Medication prescribing errors are common and inseparable part of medical data, also it can causes harm to patient or big disease or death.in this paper we offer using Blockchain by create update edit and record new information such as excepted usable drugs, analyses, process of treatment and etc.in this paper we showed that how blockchain base medical records can improve the percent of exact diagnostic and expected therapies in the secure, protected and fast decentralized method.

This method can be used from any aspect but we try to work, research and bolding the protecting, securing and developing the Medical Block Chain that we called it “MBC”.

Here we show, check and analyze the possibilities of using the Blockchain as a protected, secure, decentralized and trustworthy way to collect, save and PHI in time-lapse mode, even genre to genre to solve the genetic problems.

REFERENCES

- [1] Ton A.M. Spil, C. LeRouge, K. Trimmer, C. Wiggins, “Back to the future of IT adoption and evaluation in healthcare,” International Journal of Healthcare Technology and Management, 2011 vol. 12, Issue 1, pp. 85–109.
- [2] G. Muradova, “Development of conceptual foundations of medico-statistical data mining,” 12th International Conference AICT2018, pp. 78-83.
- [3] D. Bates and A. Gawande, ”Improving Safety with Information Technology,” New England Journal of Medicine, 2003, vol. 348, pp. 2526-2534.
- [4] J. Kern, K. Fister and O. Polazek, ”Active patient role in recording health data,” Health Information Systems, 2009, vol.1, pp. 1545-1547.
- [5] I. Starodubov, A. V. Polikarpov, N. A. Golubev and A. A. Lisenko, “Modernization of automated system of manager’s Informing,” Information technologies for thePhysician, 2016, vol. 1, pp. 41-43.
- [6] <https://searchhealthit.techtarget.com/feature/Blockchain-shows-potential-for-healthcare-claims-data-access>
- [7] P. Croskerry, M. Shapiro, S. Campbell, et al., ”Profiles in patient safety: medication errors in the emergency department,” Acad Emerg Med Off J Soc Acad Emerg Med., 2004, vol. 11(3), pp. 289-299.
- [8] G. Muradova, ”Application of Big Data technologies for simplification of electronic documents exchange,” Scientific works, Baku 2014, vol. 3, pp. 35-39.
- [9] <https://searchhealthit.techtarget.com/tip/Blockchain-technology-in-healthcare-could-ease-PHI-exchange>
- [10] <https://www.mca.org.uk/members/ibm>
- [11] Neil H Wasseman, “Using blockchain and artificial intelligence to develop new ways of delivering healthcare,” Timewave Analytics, LLC Blockchain in Healthcare Supply Chains, 2016,
- [12] William J.Gordon, “Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability,” Computational and Structural Biotechnology Journal , vol. 16, 2018, pp. 224-230.
- [13] S. Saberi, M. Kouhizadeh, J. Sarkis, L. Shen, “Blockchain technology and its relationships to sustainable supply chain management,” International Journal of Production Research, 2018.
- [14] S. Hisham Ammous, “Blockchain Technology: What is it Good for?,” Elsevier BV SSRN Electronic Journal, 2016.
- [15] <https://allthingscrypto.tech/what-in-the-hell-is-blockchain-technology/>
- [16] C. Yanling, E. Iakovou, W. Shi, ”Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities,” International Journal of Production Research, 2019.
- [17] M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services, 2016, pp.1-3.

Fərdi məlumatların proqram vasitələri ilə qorunması üsullarının araşdırılması

Şəfəqət Mahmudova

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
shafagat_57@mail.ru

Xülasə— İşdə fərdi məlumatlar və onların qorunması mərhələləri haqqında məlumat verilmişdir. Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanununun bəzi müddəaları nəzərdən keçirilmişdir. Proqramlar vasitəsilə fərdi məlumatların qorunması məsələsinə baxılmışdır. Bu sahədə görülmüş işlər barədə məlumat verilmişdir. Proqramlar vasitəsilə məlumatların qorunması üsulları araşdırılmış və analiz edilmişdir. Gələcəkdə bu işlərin daha da inkişaf etdirilməsi üçün tövsiyə verilmişdir.

Açar sözlər— fərdi məlumat; qorunma; proqram təminatı; texniki tapşırıq; SDN

I. GİRİŞ

Fərdi məlumatların qorunması müasir dövrün aktual məsələlərindən biridir. İnformasiya texnologiyalarının inkişafı bu sahəyə daha çox diqqətin ayrılmasını tələb edir və onun üçün xüsusi vasitələrin işlənməsini zəruri edir.

Fərdi məlumatların qorunması müəyyən edilmiş informasiyaya əsasən fiziki şəxsə (şəxsi məlumatların subyektinə) aid olan məlumatların müdafiəsinə yönəldilmiş təşkilatı-texniki xarakterli tədbirlərin kompleksidir [1]. Fərdi məlumatların qorunması müəssisədə əməyin qorunması bölməsinə daxil edilmişdir. Dövlət işçilərə onların fərdi məlumatlarından (şəxsiyyət vəsiqəsi) istifadəni nəzərə alaraq əmək hüquqlarının qorunmasına zəmanət verir.

Fərdi məlumatların qorunması üçün görülmə işlərin mərhələləri aşağıda göstərilmişdir:

- Fərdi məlumatların emalını həyata keçirmək tələb olunduğu halda bütün vəziyyətləri müəyyən etmək;
- İstənilən fiziki şəxsə (şəxsi məlumatların subyektinə) aid olan fərdi məlumatların doğruluğunun yoxlanılması;
- Fərdi məlumatları emal edən biznes-proseslərin seçilməsi (Biznes-proses — bu istehlakçılar üçün müəyyən məhsulun və ya xidmətin yaradılmasına yönəldilmiş qarşılıqlı əlaqəli tədbirlərin və ya işlərin məcmusudur. Fəaliyyətin qrafik təsviri kimi biznes-proseslərin blok-sxemləri tətbiq edilir);
- Analitikanın keçirilməsi üçün biznes-proseslərin məhdudlaşdırılmış sayının seçilməsi. Bu mərhələdə öz xidməti fəaliyyəti çərçivəsində fərdi verilənlərin emalında iştirak edən şirkətin əməkdaşlarının siyahısı formalaşdırılır;
- Fərdi məlumatların emalı avtomatlaşdırılmış vasitələrin və ya fərdi məlumatlara aid olan əməliyyatların məcmusudur; yazı, sistemləşdirmə, yığım, saxlama,

dəqiqləşdirmə, istifadə, ötürülmə, mühafizə etmə, silinmə, şəxsi məlumatların məhvi və s [1].

Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu (№ 998-IIIQ) 11 may 2010-cu ildə Azərbaycan Respublikasının Prezidenti tərəfindən verilmişdir [2].

Bu qanun fərdi məlumatların toplanılması, işlənməsi və mühafizəsi ilə bağlı münasibətləri, milli informasiya məkanının 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.

Bu qanunun əsas məqsədi fərdi məlumatların toplanılmasının, işlənməsinin 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.

Bu qanunda istifadə olunan informasiya, informasiya texnologiyaları, informasiya sistemləri və ehtiyatı, korporativ informasiya sistemi və digər anlayışlardan informasiyanın toplanılması, işlənməsi və mühafizəsi sahəsində münasibətləri tənzimləyən Azərbaycan Respublikasının qanunlarında müəyyən olunmuş mənalarda istifadə olunur.

Qanundan göründüyü kimi fərdi məlumatların dövlət səviyyəsində qorunmasına böyük əhəmiyyət verilir. Həmçinin proqramlar vasitəsilə fərdi məlumatların qorunması da vacib və aktual məsələlərdən biridir. Proqramlar vasitəsilə məlumatların qorunması – informasiyanın qorunmasını təmin edən və proqram təminatının tərkibinə daxil edilən xüsusi proqramların sistemidir. Məqalədə məhz bu məsələyə toxunulmuşdur.

II. PROQRAMLAR VASİTƏSİLƏ FƏRDI MƏLUMATLARIN QORUNMASI

Proqramlar vasitəsilə fərdi məlumatların qorunması – informasiyanın qorunmasını təmin edən və proqram təminatının tərkibinə daxil edilən xüsusi proqramlar sistemidir. Qoruyucu proqram kodu ayrıca və yaxud proqramların tərkibinə qoşula bilər. Çünki çoxfunksiyalı

proqramların qoruyucu funksiyaları özünümüdafiənin əhəmiyyətli vasitələrinə malik deyil və təyininə görə ixtisaslaşdırılmış qoruyucu proqram təminatından zəifdir. İstənilən əhəmiyyətli kompüter sistemi fərdi məlumatın qorunmasının proqram vasitələrinin dəyərli inteqrasiyasını tələb edir [3].

İnformasiyanın qorunması üçün istifadə olunan proqram vasitələri şəkil 1-də göstərilmişdir.

Şəkil 1. İnformasiyanın qorunması üçün istifadə olunan proqram vasitələri

Keyloqqlar - təcavüzkarların istifadəçilərə casusluq etmələrinə (həssas məlumatlara, bank kartları məlumatlarına, etimadnamələrinə və s.) imkan verən xüsusi zərərli proqram növüdür.

Məlumatların proqram təminatı ilə funksiyalarının bir çox cəhətdən üst-üstə düşməsinə baxmayaraq kompüterlərin icazəsiz istifadədən qorunması və ya kompüterlər şəbəkəsinin qorunması ilə qarışdırılmamalıdır. Məlumatlar əməliyyat sistemində rəqəmsal formada olmasına baxmayaraq yenə də qorunur. Bir serverlə işləyən kompüterdə məlumatların tam bir şəkildə qorunması eyni vaxtda bir neçə növ qorumanı birləşdirən müxtəlif növ təhlükəsizlik proqramlarının istifadəsini tələb edir.

İnformasiya sistemi (İS) fərdi məlumatların qorunmasında əsas rol oynayır. İS dedikdə saxlama, axtarış, informasiyanın işlənilməsi və uyğun təşkilati resursların (insanlar, texnikalar və s., ISO/IEC 2382:2015) informasiya ilə təmin edilməsi və yayılması başa düşülür [4].

Proqram vasitəsilə İS-də məlumatların qorunması üçün aşağıdakı imkanlardan istifadə etmək lazımdır:

- emal edilən PT kateqoriyalarının sayının azalması üçün ölçülər hazırlamaq;
- hər informasiya sistemi üçün şəxsi məlumatların emalında təhlükələrinin qarşısını almaq üçün aktual modellər formalaşdırmaq;
- tələb edilən sistemin mühafizəsini təmin etmək üçün texniki tapşırıq hazırlamaq.

PT-nin qorunması — analoqların icazəsiz təşkili, istifadəsi, bölüşdürülməsi, dəyişdirilməsi, öyrənilməsindən qorunmaq məqsədilə bir sıra tədbirlər deməkdir.

Proqram təminatının icazəsiz istifadədən qorunması — proqramın qeyri-qanuni istifadəsinə qarşı yönəlmis tədbirlərdir. Təşkilati, hüquqi, proqram təminatı və avadanlığın qorunması üçün istifadə edilə bilər.

Proqram təminatının köçürülməsindən müdafiə nadir hallarda tətbiq edilir, bu da istifadəçilərin kompüterlərinə onun

yayılması və quraşdırılması ehtiyacıyla əlaqədardır. Proqramların köçürülməməsi üçün onun ayrı-ayrı alqoritmləri lisenziya ilə qoruna bilər.

Avropa ölkələrinin ədliyyə nazirlərinin şəxsi məlumatların qorunması haqda ümumi qanunu bütün Avropa İttifaqı ərazisində işləməlidir. Hazırda birliyə daxil olan 28 ölkə fakt olaraq 28 cür müxtəlif şəxsi məlumatların qorunması haqda qanuna malikdir. Qanun vətəndaşlarla dövlətin fərdi məlumatları ilə iş modelinin yaradılmasına istiqamətlənib. Bu layihənin təşəbbüskarı Avropa Şurasının hüquq komissarı, lüksemburqlu Vivian Redinqdir. Qaydalara əsasən, fərdi məlumatlar bir neçə Avropa İttifaqı (Aİ) ölkəsində şirkətlər tərəfindən emal edilir, ancaq monitorinq yalnız bir nəzarət orqanı həyata keçirməlidir. Burada məlumatları emal edən şirkətin əsas nümayəndəliyi yerləşən ölkənin nəzarət orqanı nəzərdə tutulur. Övvəllər Fransa dövləti milli qurum səviyyəsində nəzarətə çağırırdı, lakin digər Aİ ölkələri bu modelə qarşı çıxıblar. Belə ki, bir pəncərəli Mini One-Stop Shop (MOSS) sisteminin “Facebook” və ya “Google” kimi Amerika şirkətlərinə əhəmiyyətli təsiri vardır. Bu gün bu şirkətlər məlumatların emalını və saxlanılmasını bir ölkədə həyata keçirirlər, halbuki, nümayəndəlikləri digər ölkələrdə fəaliyyət göstərir və maliyyə vəsaitləri orada toplanır. Avropada bu İrlandiyadır, belə ki, şirkətlər əsas nümayəndəliyə malikdir. “Bizim məqsədimiz Aİ üçün ümumi qaydalar yaratmaq və həmçinin milli tənzimləyicilər üçün inzibati maneələri azaltmaqdır”, deyər Litvanın ədliyyə naziri Yuozas Bernatonis bildirib [5].

Şəxsi məlumatların məxfiliyi və qorunması ilə bağlı narahatlıqlar Avropa Birliyində (AB) mövcud qanunvericilikdə islahatlara səbəb oldu. Ümumi Məlumatların Qorunması Qaydaları, vətəndaşların məlumatlarına nəzarətin gücləndirilməsinə və fərdi məlumatların işlənməsi qaydalarının yaradılması ilə əlaqədar olaraq AB vətəndaşlarının fərdi məlumatlarının qorunması ilə bağlı mövcud direktivin islah edilməsinə yönəlmişdir [6].

III. PROQRAMLAR VASİTƏSİLƏ MƏLUMATLARIN QORUNMASI ÜSULLARININ ANALİZİ

Zərərli proqramlar, kompüter virusları, fişinq və şəxsi məlumatların oğurluğu kimi İnternet təhlükəsizliyi problemləri son illərdə daha da kəskinləşdi və İnternet istifadəçilərinin düzgün olmayan davranışları ilə daha da ağırlaşdı. Bu sahə üzrə mütəxəssislər insanlara İnterneti öyrədilər. Bununla birlikdə, mütəxəssislər İnternetdə yeniyyətlərin təhlükəsizlik davranışlarının formalaşmasında mühüm rol oynayır və gündəlik həyatda qarşılıqlı münasibətlər vasitəsilə İnternet təhlükəsizliyi anlayışını onlara çatdırırlar. Nəticə etibarilə mütəxəssislər yeniyyətlərin İnternetdəki riskli davranışlarının motivlərinin daha da öyrənilməsini tələb edir. Qrup analizindən istifadə edərək moderatorların rolu və sosial normaları öyrənilmişdir. Statistik təhlilin nəticələrini təsdiqləmək üçün keyfiyyətli müsahibələr də aparılmışdır. Nəticələr göstərir ki, yeniyyətlərin İnternetdə riskli davranışının qarşısını almaq üçün müəllimlərin İnternet təhlükəsizliyi problemlərini həll etmək bacarıqlarını artırmaq və ya onları qoruyucu tədbirlər görməyə təşviq edən atmosfer yaratmaq lazımdır. [7] işində onlayn təhlükəsizlik təlimi üçün

nəzəri anlayış və praktiki təkliflərin nəticələri müzakirə olunur.

İcazəsiz giriş və ya məxfi fərdi informasiyanın oğurluğu tez tez baş verir. Gizli məlumatların mediada qeyri-qanuni yayılması hər il sənayedə milyonlarla bərpa və itki xərcləri ilə başa gəlir Target Inc. sorğu sisteminin 2013-cü ildəki məlumatına görə 70 milyon müştəriyə dəyən ziyan bir milyarddan çox dollar dəyərində idi. Oğurlanan məlumatlar siyasətçilərə zərər vermək üçün istifadə olunur və xarici və daxili siyasətə mənfi təsir göstərir. [8] işində şəbəkələrin sağlamlığını və təhlükəsizliyini daha yaxşı qorumaq üçün bəzi üsullar təqdim edilir. Bu üsullar mütəxəssislərə şəbəkə davranışları, anomaliyaları və gizli, sistemə problemləri müəyyən etməyə kömək edəcəkdir.

Şəxsi məlumat hissələrinə icazəsiz daxil olmaq çətin bir iş kimi görünür. Şəbəkələrin sağlamlığını yaxşılaşdırmaq üçün zərərli fəaliyyət və digər gizli sistem problemlərini göstərən şəbəkə anomaliyalarını təyin etmək lazımdır. [9] işində gizli sistemlərin problemlərini müəyyənləşdirmək, daha etibarlı şəbəkə yaratmaq və kiber cinayətkarlar tərəfindən məlumat oğurlanmasının qarşısını almaq üçün istifadə edilə bilən şəbəkənin yolunun təhlili xidməti metodlarını təklif edir.

Dövlət qurumlarından yüksək keyfiyyətli elektron hökumət xidmətləri göstərmək üçün onların bir-biri ilə əməkdaşlıq etməyi tələb olunur. Bu əməkdaşlıq ümumiyyətlə xidmət yönümlü yanaşmaya əsaslanır və əməkdaşlıq platformaları tərəfindən dəstəklənir. Bu cür platformalar, uyğun proqram xidmətlərini təqdim etməyə imkan verən ixtisaslaşdırılmış orta proqram əsaslı infrastrukturlardır. Öz növbəsində, hökumətlər tərəfindən işlənən fərdi məlumatların çox həssas olduğu nəzərə alınsa, əksər hökumətlər fərdi məlumatların qorunması haqqında qanun hazırlamışlar. Bu sənəd, elektron hökumətin əməkdaşlıq platformasının bir hissəsi olaraq məlumatların qorunması qanunlarına nəzarət və tətbiq etmək üçün həll yollarını təklif edir [10].

Xətti proqramlar və onların arasındakı əlaqələrin əldə edilməsi proqram təminatının tədqiqatında geniş istifadə olunur. [11] işində tədqiqatın məqsədi təhlil olunan proqramların quruluşu barədə vahid məlumat təminatçısı yaratmaqla proqram təminatının təhlilini asanlaşdırmaqdır. İşdə təklif olunan yanaşma, bir-birinə bağlı xətti bloklar və onların əlaqələri şəkildə proqram kodunun parçalanmasına və təqdim edilməsinə yönəldilmişdir. Bu formada təqdim olunan kod, təhlükəsiz proqram təminatının hazırlanması prosesini asanlaşdırmaq və spesifik xüsusiyyətləri olan nümunələri müəyyən etmək üçün təhlil edilə bilər. Təklif olunan metod mövcud vasitələrdən məlumatları birləşdirən bir pluginin inkişafına əsaslanır. "MAR" sökücü cihazdan məlumatların çıxarılması və sonrakı iş üçün zəruri formada təqdim edilməsi üçün metod hazırlanmışdır. Metodun yoxlama testlərinə aid nümunə verilmişdir. Metodologiyaya uyğun olaraq əldə edilən məlumatlar hədəf olan proqram alətlərində istifadə üçün nəzərdə tutulub.

[12] işinin məqsədi İT sistemlərinin təhlükəsizliyini müzakirə etmək və icazəsiz girişdən qorunmalı olan elementləri müəyyənləşdirməkdir. Proqram təminatı, kiber sahənin xüsusiyyətlərinə əsaslanaraq yaradılmışdır. Proqram sistemlərinin mürəkkəbliyi informasiya təhlükəsizliyini daha

mürəkkəb və etibarsız edir. Texnologiyanın inkişafı təhdidlərin inkişafı ilə ayrılmaz dərəcədə bağlıdır, yəni proqram həllərinin təkmilləşdirilməsi bütün istifadələr üçün son dərəcə vacib bir məqama çevrilmişdir. İşdə həm proqram təminatının təhlükəsizlik istifadəçisi olaraq, həm də təhlükəsizlik sistemini yaradarkən hansı təhlükəsizlik elementlərinin nəzərə alınmasının lazım olduğu göstərilmişdir.

Proqram Təminatı Şəbəkələri (Software-Defined Networking, SDN) ənənəvi şəbəkələrdən şəbəkə konfigurasiyalarını toplamağa imkan verir. SDN, həmçinin proqram görüntülərini daha yaxşı edən proqram protokolları və vasitələrinin inkişafına imkan verir.

Hal-hazırda, SDN idarəetmə şəbəkə cihazlarının məlumat yayımını ayıran yeni quruluş sayəsində sürətlə inkişaf edir. Bir çox tədqiqatçı özlərini belə bir xüsusi şəbəkənin öyrənilməsinə həsr etmişlər. Bununla birlikdə bəzi məhdudiyyətlər SDN-nin inkişafını məhdudlaşdırır. Bir tərəfdən normal bir modeldə bir nəzarətçi bütün təhdidləri daşıyır və ziyanları şəbəkə iflicinə səbəb olur. Digər tərəfdən, məlumat yayımında SDN açarlarında daha çox artım olacaq, bu açarların saxlanması yeri məhduddur. Bu problemləri həll etmək üçün [13] işində iki müvafiq protokollar təklif edilir. Xüsusilə, biri təyyarə idarəedilməsinin anonim protokolu, digəri isə təyyarədəki məlumatları təsdiqləyən xarici qaynaq protokoludur. Aparılan qiymətləndirmə təklif edilən protokolun düzgün, təhlükəsiz və effektiv olduğunu göstərir.

Məlumat sistemlərinin əldə edilməsi, tətbiqi və inkişafı rəqəbat üstünlüyü əldə etmək üçün əsasdır. Texnologiyanın sürətli inkişafı eyni zamanda son istifadəçi məlumatlarının qorunması və məxfiliyinin pozulması ilə əlaqəli etik problemlərə səbəb olur. [14] işində təşkilatın strateji ehtiyaclarını dəstəkləyərkən keyfiyyətli proqram məhsuluna zəmanət verən standart keyfiyyət təminatı metodları müzakirə olunur. Keyfiyyətli proqram təminatının inkişafı prosesinin təkmilləşdirilməsini təşkilatın strateji ehtiyacları ilə əlaqələndirən bir çərçivə təqdim edilir. Nəzərdə tutulan standart təcrübələrə, təşkilatın strateji hədəflərini müəyyənləşdirmək və məlumat sisteminin inkişafı ilə əlaqəli effektivliyi izləmək üçün Balans Score Card metodologiyasından istifadə edilir və həmçinin əlaqələndirmək üçün Audit Assosiasiyası tərəfindən verilmiş “İnformasiya və əlaqəli texnologiyalar üçün idarəetmə nəzarəti” (Control Objectives for Information and Related Technologies, COBIT) - 5 informasiyanın idarəetmə sistemini özündə birləşdirir [14].

Əşyaların İnterneti (Internet of Things, IoT) texnologiyasının sürətli inkişafı və kompüterə quraşdırılmış cihazların hesablamaya gücünün artması təhlükəsizlik təhdidləri və hücumlarına açıq olma ehtimalını yaradır. Son zamanlarda daxil edilmiş fərdi məlumatların təhlükəsizliyi barədə Etibarlı İcra Mühiti (Trusted Execution Environment, TEE), ictimaiyyətin diqqətini çəkmiş və ixtiyari kodun sistemin müəyyən hissəsindən tamamilə təcrid olunmuş mühitlərində icra olunmasına imkan yaratmışdır. TEE- əsas prosessorun qorunan sahəsidir. Bununla birlikdə TEE-də mövcud yaddaş qorunması üçün mövcud olan metodlar yetərli deyildir. Ümumiyyətlə, proqram təminatına dair rəsmi metodlar praktik deyil və həyata keçirməyə aparıcı yanaşmalar nəzəri cəhətdən

təsdiqlənmiş. TEE-də təcrid və yaddaşın qorunması problemlərini həll etmək üçün Qabaqcıl Risk Maşını (Advanced RISC Machine, ARM) platformasında yaddaşın bütövlüyünün təhlükəsizlik təhdidlərindən qorumaq üçün praktik metod təklif edilmişdir. ARM-dan həssas kodu və məlumatları hücumlardan qoruya biləcək təcrid olunmuş iş mühiti yaratmaq üçün istifadə edilir. Xilinx Zynq ZC702 qiymətləndirmə şurasında ARM tətbiq edilir. Maşınların avtomatik yoxlama nisbəti təxminən 78.32% təşkil edir və təklif olunan metod həm yükləmə vaxtı, həm də xərc baxımından səmərəli və məqsəduyğundur [15].

Fərdi məlumatları idarə edən dövrdə Avropa Məlumatların Qorumasının Ümumi Qaydalarının (General Data Protection Regulation, GDPR) tətbiqi son zamanlarda populyarlıq qazanmışdır. [16, 17] işində proqram təminatçılarının diqqətinə çatdırılmalı olan GDPR məqalələri təqdim olunur, həmçinin kompüter üzrə alimlər tərəfindən təqdim olunmuş tələblərin mənsəyini izləmək, istifadəyə nəzarət və uzaq protokolların yayılması kimi ən müasir texnologiyalara əsaslanaraq tətbiq oluna biləcəyi izah edilir.

NƏTİCƏ

Şəbəkə rabitəsi, qloballaşma və məlumat mübadiləsinə əsaslanan müasir rəqəmsal dünya, məxfilik və fərdi məlumatların qorunması sahəsində təklif olunan məlumat strukturlarına etibarlı giriş prinsiplərini əks etdirən yeni vacib vəzifələri müəyyənləşdirir. Bu səbəbdən elektron mühitin bütün mənbələrinə etibarlı daxil olmaq çox vacibdir və fərdi məlumatların identifikasiyası, avtorizasiyası və qorunması üçün adekvat texnoloji və təşkilati tədbirlər tətbiq edilməlidir. Uğurlu qeydiyyatdan alındıqdan sonra hazırlanmış istifadəçi profillərini və təlim zamanı toplanmış bütün şəxsi məlumatları qorumaq üçün ciddi təhlükəsizlik prosedurları təklif edilməlidir [18, 19].

Göründüyü kimi məqalədə proqram vasitəsilə fərdi məlumatların qorunması üsulları araşdırılmışdır. Fərdi məlumatları qoruyan proqramlar daha effektiv işləyir və səmərəlilik göstəriciləri yüksək olur. Dünya və respublika miqyasında bu sahə üzrə yeni qanunların qəbul edilməsi bu işlərin aktual olduğunu bir daha sübut edir. Avropa şurasının bu sahəyə böyük diqqət ayırması təqdirə layiqdir. Gələcəkdə bu sahəyə aid olan yeni proqramların təşkili və inkişaf etdirilməsi fərdi məlumatların daha sıx qorunmasına imkan verəcəkdir. Təvsiyə olunur ki, bu sahədə elmi tədqiqat işləri gücləndirilsin və fərdi məlumatları qoruyan yeni keyfiyyətli proqramlar yaradılsın.

İSTİNADLAR

- [1] «Защита персональных данных», https://ru.wikipedia.org/wiki/Защита_персональных_данных
- [2] “Fərdi məlumatlar haqqında Azərbaycan Respublikasının qanunu”, 11.05.2010, <http://www.e-qanun.az/framework/19675>
- [3] «Программная защита информации», 2000-2019, <http://rus.safensoft.com/security.phtml?c=882>
- [4] Ю.А.Маглинец, «Анализ требований к автоматизированным информационным системам». Бином, 2008, 200 с.
- [5] “Şəxsi məlumatların qorunması haqda yeni qanun”, 08.10.2013, <http://www.lawreform.az/index.php?module=news&name=view&id=1098&lang=az>

- [6] G. Ferreira, M. Sousa, B. Silva, S. Frade, L. Antunes, T. Beale, C. Correia, “Open EHR and General Data Protection Regulation: Evaluation of Principles and Requirements”, JMIR medical informatics, 2019, vol. 7, no. 1, <https://www.ncbi.nlm.nih.gov/pubmed/30907730>
- [7] C. Hui-Lien, S. Jerry, “The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers”, Computers & education, 2017, vol. 112, pp. 83-96.
- [8] A. Joshua, M. Scott, C. Edward, “SDN Data Path Confidence Analysis”, IEEE Conference on dependable and secure computing, 2017, pp. 209-216.
- [9] A. Joshua, M. Scott, C. Edward, “A Framework for SDN Network Evaluation”, 2017 47th annual IEEE/IFIP international conference on dependable systems and networks workshops, pp. 111-112, 2017.
- [10] E. Andres, M. Dahiana, G. Laura, “Monitoring and Enforcing Data Protection Laws within an E-government Interoperability Platform”, 2015 XLI Latin american computing conference, pp. 548-559, 2015.
- [11] I.O. Bazhenov, “Lubkin Methodology of software code decomposition analysis”, 12th international IEEE Scientific and technical conference on dynamics of systems, mechanisms and machines (dynamics), 2018.
- [12] K. Anna, O. Lidia, “Data Security in Cognitive Information Systems”, Proceedings 2018 IEEE 32nd international conference on advanced information networking and applications (AINA), pp. 631-635, 2018.
- [13] K. Pawel, “Digital image integrity a survey of protection and verification techniques”, Digital signal processing, 2017, vol. 71, pp. 1-26.
- [14] H. Syeda Umema, A. Abu Turab, “Software Development for Information System Achieving Optimum Quality with Security”, International journal of information system modeling and design, vol: 8, no. 4, pp. 1-20.
- [15] C. Rui, J. Liehui, C. Wenzhi, X. Yang, C. Yuxia, A. Alelaiwi “MIPE: a practical memory integrity protection method in a trusted execution environment”, Cluster computing-the journal of networks software tools and applications, 2017, vol. 20, no. 2, pp. 1075-1087.
- [16] B. Pascal, K. Erik, W. Paul Georg, B. Juergen, “Identity Management and Protection Motivated by the General Data Protection Regulation of the European Union-A Conceptual Framework Based on State-of-the-Art Software Technologies”, Technologies, 2017, vol. 6, no. 4, pp. 1-14.
- [17] C. Hui-Lien, S. Jerry Chih-Yuan, “The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers”, Computers & education, 2017, vol. 112, pp. 83-96.
- [18] R. Radi, N. Irina, “Architecture of Combined e-Learning Environment and Investigation of Secure Access and Privacy Protection”, International journal of human capital and information technology professionals, 2017, vol. 7, no. 3, pp. 89-106.
- [19] K. Peter, D. Glenn, “Practical uses of virtual machines for protection of sensitive user data”, Information security practice and experience, proceedings, 2007, vol. 4464, 145 p.

EXPLORING PERSONAL DATA PROTECTION METHODS WITH PROGRAM TOOLS

Shafagat Mahmudova

Institute of Information Technology of ANAS, Baku, Azerbaijan

shafagat_57@mail.ru

Abstract— The paper highlights the personal data and the stages of its protection. Some provisions of the Law of the Republic of Azerbaijan on the personal data are reviewed. The protection of personal data through programs is explored. The studies in this area are reviewed. Data protection methods through programs are studied and analyzed. Some recommendations for the further developments in this field are provided.

Keywords— *personal data; protection; software; technical task; SDN*

Konfidensiallığı qorumaqla fərdi məlumatların intellektual analizi üçün Deep Learning metodları

Yadigar İmamverdiyev

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@iit.science.az

Xülasə— Bu məqalədə fərdi məlumatların intellektual analizi zamanı konfidensiallığın qorunması metodlarının, o cümlədən Deep Learning metodlarının icmalı verilir. Son onilliklərdə fərdi məlumatlar kibercinayətkarların əsas hədəflərindən birinə çevrilmişdir, konfidensiallığın qorunması tədbirlərinə baxmayaraq, verilənlərin intellektual analizi metodları fərdlər barədə sensitiv informasiya əldə etməyə imkan verir. Bu təhdidin qarşısını almaq üçün ənənəvi intellektual analiz metodlarının konfidensial fərdi məlumatlarla işləyən çoxsaylı modifikasiyaları təklif edilmişdir. Bu işdə fərdi məlumatların konfidensiallığının qorunması üçün dərin təlim metodlarının tətbiqi vəziyyəti analiz edilir, dərin təlim metodlarının diferensial gizlilik, çoxtərəfli təhlükəsiz hesablamalar və homomorf şifrələmə metodları ilə birləşdirilməsində qarşıya çıxan çətinliklər və onların həlli yolları araşdırılır.

Açar sözlər— fərdi məlumatlar, gizlilik, gizlilik təhdidləri; PPDM, dərin təlim, Deep Learning

I. GİRİŞ

Big data şəxsi həyatın gizliliyinə, vətəndaş azadlıqlarının pozulmasına potensial təhdidlər yaradır, dövlət və korporativ nəzarət imkanlarını artırır. Big Data analitikasından istifadə etməklə şəxs barəsində gizli məlumatlar əldə etmək mümkündür. Analitika üçün verilənlərin anonimləşdirilməsi istifadəçi verilənlərinin konfidensiallığını qorumaq üçün kifayət deyil. Buna görə də, fərdi məlumatların intellektual analizi zamanı konfidensiallığın pozulması hallarının qarşısını almaq üçün müvafiq yanaşma, metod və texnologiyaların işlənilməsi vacibdir [1].

PPDM (Privacy-preserving data mining – konfidensiallığı qorumaqla verilənlərin intellektual analizi) yanaşmasının məqsədi data mining (DM) və ya maşın təlimi metodlarının tətbiqi ilə alınmış gizli informasiyaya icazə olmayan istifadəçilərin girişinin qarşısını almaqdır. Tədqiqatçılar konfidensiallığı qorumaq üçün PPDM-də data mining və maşın təlimi alqoritmlərində bir çox üsullardan istifadə edirlər [2, 3].

Son onilliklərdə fərdi məlumatlar kibercinayətkarların əsas hədəflərindən birinə çevrilmişdir, kütləvi informasiya vasitələri tez-tez böyük həcmli fərdi məlumatların oğurlanması halları barədə xəbərlər dərc edir. Texnologiyaların inkişafı fərdi məlumatların təhlükəsizliyinin təmin edilməsinin qanunvericilik bazasına yenidən baxılmasını zəruri edir. Avropa İttifaqının 2018-ci ilin mayından qüvvəyə minmiş fərdi məlumatların konfidensiallığının təmin edilməsi üzrə yeni

qanunu GDPR (General Data Protection Regulation) bu sahədə ciddi tədbirlər nəzərdə tutur. Fərdi məlumatların emalı ilə məşğul olan təşkilatlar onların konfidensiallığının təmin edilməsi üzrə texnologiyaları praktikada tətbiq etməyə başlayırlar. Məsələn, Apple (iOS / macOS üçün), Google (RAPPOR), LinkedIn (Salary), Microsoft (Windows telemetriyası üçün) diferensial gizlilik sistemlərini praktikada tətbiq edir [4].

Son dövrlər dərin təlim (ing. Deep Learning) verilənlərin intellektual analizinin əsas metodlarından birinə çevrilmişdir və bir sıra praktiki məsələlərin həlli üçün geniş tətbiq edilir [5, 6]. Hazırda dərin təlim dərin neyron şəbəkələri ilə eyniləşdirilir. Dərin neyron şəbəkəsi (Deep Neural Network, DNN) – bir neçə gizli neyron layı olan neyron şəbəkəsidir. Dərin təlim xidmət kimi (Deep Learning as a Service, DLaaS) bulud platforması dərin neyron şəbəkələrinin geniş praktiki tətbiqlərinə yol açır. Google, Amazon və IBM öz bulud xidmətlərində DLaaS platformalarını işə salıblar [7]. Müxtəlif DLaaS istifadə etməklə müxtəlif gizli verilənlərini bulud serverinə göndərir. Server DNN tətbiqini yerinə yetirir və nəticələri müştəriyə geri göndərir. Aydındır ki, müştərinin verilənlərinin konfidensiallığı qorunmasa, DLaaS istifadəsi potensial gizlilik problemləri yarada bilər. Dürüst, lakin maraqlı bulud serveri müştərinin konfidensial verilənlərindən sensitiv məlumatlar toplaya bilər. Bu qəbildən olan problemləri araşdırmaq üçün fərdi məlumatların konfidensiallığının təmin edilməsi üçün bir sıra tədqiqatlar aparılmışdır.

Bu işin məqsədi verilənlərin intellektual analizi zamanı fərdi məlumatların konfidensiallığının qorunması üçün dərin təlim metodlarının tətbiqi vəziyyətini analiz etməkdir. Qeyd edək ki, [8, 9]-də bu məsələyə baxılır. Bu işdə həmin məqalələrdə əhatə edilməyən mənbələr tədqiqata cəlb edilmişdir və mövcud metodların dərin təlim metodlarına əsaslanan fərqli təsnifatı təklif edilmişdir. Təqdim olunan məqalədə əvvəlcə klassik PPDM metodları analiz edilir, daha sonra baxılan məsələ üçün dərin təlim metodlarının tətbiqi məsələləri araşdırılır.

II. FƏRDİ VƏ KOLLEKTİV KONFİDENSİALLIQ

Fərdi konfidensiallığın qorunması

Verilənlərin konfidensiallığının təmin edilməsinin əsas məqsədi – fərdi məlumatların qorunmasıdır. Ümumiyyətlə, məlumat o zaman fərdi hesab olunur ki, onu birbaşa və ya

dolayısı ilə fiziki şəxslə əlaqələndirmək mümkün olsun. Beləliklə, fərdi məlumatlar intellektual analiz edilərkən fiziki şəxslə əlaqəli atributların qiymətləri məlum olur ki, onların konfidensiallığı qorunmalıdır.

Kollektiv konfidensiallığın qorunması

Fərdi məlumatların qorunması yetərli olmaya bilər. Bəzən qrupun fəaliyyətini əks etdirən gizli biliklərin əldə edilməsinin qarşısını almaq tələb edilə bilər. Gizli biliklərin qorunmasını *konfidensiallığın kollektiv qorunması* adlandırılır. Burada məqsəd statistik verilənlər bazasında olduğu kimidir, yəni təhlükəsizliyə nəzarət mexanizmləri qruplar barədə informasiyanın aqreqasiyasını təmin edir, eyni zamanda fiziki şəxslər haqqında informasiyanın qarşısını alırlar. Lakin statistik verilənlər bazalarından fərqli olaraq, konfidensiallığın kollektiv qorunmasının digər məqsədi bütün statistika təhriflərinin minimallaşdırılması deyil, strateji qərarlar üçün birinci dərəcəli əhəmiyyəti olan strateji modelin qorunmasıdır. Başqa sözlə, burada məqsəd təkcə fərdi məlumatların deyil, açıqlanmaması tələb edilən bəzi modelləri və tendensiyaları da qorumaqdır.

III. VERİLƏNLƏRİN GİZLİLİYİNƏ TƏHDİDLƏR

Bu bölmədə fərdlərin gizli və/və ya sensitiv (həssas) məlumatlarının açıqlanması ilə əlaqəli təhdidlərə baxılır.

Konfidensiallıq təhdidləri atributların üç müxtəlif növü ilə əlaqədirdir [10]: birbaşa identifikatorlar, kvazi-identifikatorlar və sensitiv atributlar. Birbaşa identifikatorlar fərdləri dəqiq (aşkar) re-identifikasiya edən atributlardır, məsələn, ad, poçt ünvanı, telefon nömrəsi, milli ID-lər, e-poçt ünvanı və s. Kvazi-identifikatorlar kombinasiya edildikdə fərdi identifikasiya etməyə imkan verirlər (məsələn, cins, doğum tarixi və poçt indeksi, demoqrafik məlumatlar və diaqnoz kodları). Sensitiv atributlar fərdlərin (pasiyentləri) əlaqələndirilmək istəmədikləri atributlardır. Bu atributlara misallar spesifik diaqnoz kodları (məsələn, psixi xəstəlik, SPİD, xərçəng) və genom məlumatlarıdır (DNT).

Yuxarıdakı atributların növləri əsasında konfidensiallıq təhdidlərinin aşağıdakı növlərinə baxmaq olar:

Şəxsiyyətin açıqlanması (və ya re-identifikasiya): bu nəşr olunan verilənlər bazalarında ən məşhur təhdid hesab olunur. Bədənyyətli müəyyən şəxsi nəşr olunmuş bazadakı yazı ilə əlaqələndirdikdə baş verir.

Üzvlüyün açıqlanması [11]: Bu təhdid bədənyyətlinin müəyyən bir şəxsə aid yazının nəşr olunmuş verilənlər bazasında olması haqqında yüksək ehtimalla nəticə çıxardıqda baş verir. Məsələn, yalnız SPİD-pozitiv pasiyentlər haqqında məlumatlar olan verilənlər bazasına baxaq. Bir şəxsə aid yazının həmin bazada olması faktından onun SPİD-pozitiv olması nəticəsini çıxarmağa imkan verir və bu gizliliyə təhiddir.

Atributun açıqlanması (və ya sensitiv informasiyanın açıqlanması): Bu təhdid şəxsi onun sensitiv məlumatları ilə əlaqələndirdikdə baş verir. Belə məlumatlar, məsələn, pasiyentin DNT məlumatları və ya şəxsin sensitiv

məlumatlarının interval qiymətləri ola bilər (məsələn, müalicə xərclərinin təxmini kəmiyyəti).

Qeyd edək ki, ədəbiyyatda PPDM və PPDP (Privacy-Preserving Data Publishing) metodlarına qarşı bir çox hücumlar təklif edilmişdir [10,12,13]. Burada GAN (Generative Adversarial Network) hücumu [14] və MIA (Model Inversion Attack) hücumu [15] barəsində qısa məlumat verilir.

GAN hücumunda diskriminativ şəbəkə (D) generativ şəbəkəyə (G) qarşı 0-cəmli oyun oynayır. Oyun o zaman dayanır ki, D daha real və saxta şəkilləri fərqləndirə bilmir, yəni G D-ni aldatmaqda uğur qazanır [14].

MIA hücumunda maşın təlimi modelinə giriş icazəsi var, müəyyən fon məlumatı və onun sinfinin etibarlılıq qiyməti (və ya sadəcə nişanı) verilib: verilmiş sinif üçün sinif ehtimalını maksimallaşdıran giriş tapılır. Məsələn, şəkli klassifikasiya edən model şəxsin adına əsasən şəxsin sifət şəklini generasiya edir [15].

IV. GİZLİLİYİN QORUNMASI METODLARININ TƏSNİFATI

Fərdi məlumatların təhlükəsizliyinə cavabdeh təşkilatlar adətən de-identifikasiya üsullarından, o cümlədən, anonimlik (*anonymization*), təxəllüs (*pseudonymization*), şifrləmə (*encryption*), açar-kodlaşdırma (*key-coding*) və s. istifadə edirlər. Anonimlik ad, ünvan və sosial təhlükəsizlik nömrələrini silməklə konfidensiallığı təmin edirsə, təxəllüs bu informasiyanı ləqəb və süni identifikasiya ilə əvəz edir. Açarla kodlaşdırma fərdi məlumatları kodlaşdırır və onların dekodlaşdırılması üçün açar yaradır [1,16].

PPDM və PPDP üçün çoxsaylı yanaşmalar mövcuddur (Cədvəl 1).

CƏDVƏL 1. GİZLİLİYİN QORUNMASI METODLARI

Yanaşma	Metodlar
Ümumi halda verilənlərin konfidensiallığının qorunması	Perturbasiya, randomizasiya, blok-lama, qarşılıqlı dəyişmə, seçmə, şifrləmə
Verilənlərin intellektual analizi zamanı konfidensiallığın qorunması	Assosiativ qaydaların çıxarılması, klassifikasiya, klasterizasiya
Verilənlərin nəşri zamanı konfidensiallığın qorunması	<i>k</i> -anonimlik, <i>l</i> -müxtəliflik, <i>m</i> -invariantlıq, <i>t</i> -yaxınlıq

PPDM metodlarını aşağıdakı meyarlar üzrə klassifikasiya etmək olar [17]:

- verilənlərin paylanması;
- verilənlərin modifikasiyası;
- verilənlərin intellektual analizi alqoritmləri;
- DM çıxışının gizlədilməsi.

Verilənlərin paylanması. Bəzi yanaşmalar mərkəzləşdirilmiş verilənlər üçün təklif edilib, digərləri paylanmış verilənlər üçün nəzərdə tutulub.

Bir neçə yerə paylanma halında problemi müəyyən etmək üçün verilənlərin necə paylanması mühüm rol oynayır. Müxtəlif bölünmələr fərqli problemlər yaradır və bu verilənlərin intellektual analizi zamanı konfidensiallığı qorumaq üçün müxtəlif alqoritmlərlə nəticələnir. Verilənlərin paylanması *üfüqi* və ya *şaquli* ola bilər.

Şaquli bölünmə. Verilənlərin şaquli bölünməsində nəzərdə tutulur ki, müxtəlif tərəflər eyni subyektlər çoxluğu barədə müxtəlif atributlar üzrə informasiya toplayırlar. Məsələn, banklar maliyyə tranzaksiyalarının məlumatlarını, vergi orqanları isə vergi məlumatlarını toplayırlar.

Üfüqi bölünmə. Üfüqi bölünmədə müxtəlif tərəflər müxtəlif subyektlər barədə eyni verilənlər çoxluğunu toplayırlar. Məsələn, müxtəlif supermarketlər ərzaq alınması barədə verilənləri toplayırlar.

Verilənlərin modifikasiyası: Bu metod konfidensiallığı qorumaq üçün relizdən öncə verilənlər bazası yazılarını modifikasiya edir. Verilənlərin modifikasiyası metodlarına perturbasiya, bloklaşdırma, aqreqasiya, qarşılıqlı dəyişmə, seçmə (populyasiyanın müəyyən hissəsi üçün verilənlər seçilir) daxildir [18]. Bu metodların hamısında atributların qiymətləri dəyişdirilir. Verilənləri üçüncü tərəf data maynerə verməzdən öncə verilənlərdə dəyişikliklər etmək lazımdır ki, mayner sensitiv informasiya barədə heç bir şey əldə edə bilməsin.

Verilənlərin perturbasiyası üçün iki əsas yanaşma var [18]: ehtimal paylanması yanaşması və verilənlərin qiymətlərinin təhrifi yanaşması. Ehtimal paylanması yanaşmasında verilənlər həmin paylanmadan olan digər nümunələrlə əvəzlənir. Verilənlərin qiymətlərinin təhrifi yanaşmasında verilənlər additiv küy, multiplikativ küy və ya digər randomizasiya proseduru ilə perturbasiya edilir. Adətən, küy qiymətini generasiya etmək üçün Qauss paylanması istifadə edilir. Küylərin korrelyasiyası ilkin verilənlərə nə qədər oxşadırsa, konfidensiallıq bir o qədər çox qorunur. Randomizasiya edilmiş verilənlərdən gizli verilənlərin çıxarılması imkanını qiymətləndirmək üçün PCA (Principal Component Analysis) və BE (Bayes Estimate) üsulları geniş öyrənilmişdir [19].

Verilənlərin qarşılıqlı dəyişdirilməsi (data swapping) metodunda verilənlər bazası sensitiv atributların qiymətini yazılar arasında qarşılıqlı dəyişməklə transformasiya edilir [20].

k-anonimlik modelində verilənlərin ümumiləşdirilməsi və verilənlərin silinməsi metodları tətbiq edilir və verilənlər toplusu yalnız o zaman nəşr olunur ki, həmin topluda olan hər bir şəxs üçün məlumatlar ən azı $(k - 1)$ digər şəxsin məlumatlarından fərqləndirilə bilməsin [21].

Verilənlərin nəşri metodları, yəni *k*-anonimlik, *l*-müxtəliflik, *t*-yaxınlıq, *m*-invariantlıq dəqiqliyi və verilənlərin faydalılığını böyük dərəcədə azaldır.

Verilənlərin intellektual analizi alqoritmləri. Xüsusi olaraq PPDM üçün klassifikasiya, klasterləşdirmə, assosiativ qaydalar, Bayes şəbəkələri və s. alqoritmlərinin yeni variantları təklif edilmişdir [2]. Konfidensiallığı qorumaqla

öyrənmə və konfidensiallığı qorumaqla klassifikasiya bu tədqiqatlarda iki əsas istiqamətdir. Konfidensiallığı qorumaqla klassifikasiya metodunda data mayner verilənləri klassifikasiya etməyi öyrənir, lakin bu zaman sensitiv atributları qorunur, mayner sensitiv verilənlər haqqında məlumat əldə edə bilmir.

DM çıxışının konfidensiallığı. DM alqoritmlərinin çıxışları bəddiyyətli üçün çox informativ ola bilər. Məsələn, tutaq ki, assosiativ qayda mayninqi alqoritmində aşağıdakı qayda yüksək etibarlılıqla generasiya edilib:

(Age = 26, ZIP code = 10562) $\Rightarrow$ HIV.

Bu qaydanın aşkarlanması fərd barəsində olduqca gizli məlumatın açıqlanması ilə nəticələnir [2]. DM çıxışının konfidensiallığını qorumaq üçün geniş yayılmış üsullar aşağıdakılardır:

a) Assosiativ qaydaların gizlədilməsi – sensitiv qaydaların aşkarlanmasının qarşısını alır; bu məqsədlə verilənlərin modifikasiyası və bloklaşdırma metodları istifadə edilir.

b) Klassifikatorun effektivliyinin aşağı salınması – verilənlərin sanitarizasiyası vasitəsilə klassifikatorun dəqiqliyi aşağı salınır ki, sensitiv məlumatların əldə edilməsi imkanı azalsın [22].

c) sorğuların auditi və məntiqi çıxarışlara nəzarət – aqreqativ verilənlər sorğuları ardıcılığından informasiyanın açıqlanmasının qarşısını almaq məqsədi güdür. Sorğuların auditi zamanı sorğular ardıcılığından bir və ya bir neçə sorğudan imtina edilir. İmtina edilən sorğular elə seçilir ki, verilənlərin sensitivliyi qorunur. Məntiqi çıxarışlara nəzarətdə sorğunun nəticəsi və ya verilənlər perturbasiya edilir [23].

Verilənlərin selektiv modifikasiyası və ya sanitarizasiyası NP-çətin məsələdir, bu səbəbdən mürəkkəbliyin probleminin həlli üçün evristik metodlar istifadə edilə bilər.

PPDM alqoritmlərinin işlənməsində vacib aspekt müvafiq qiymətləndirmə meyarlarının müəyyən edilməsi və uyğun qiymətləndirmə parametrlərinin (göstəricilərinin) işlənməsidir.

Konfidensiallığı qoruyan bütün alqoritmlər arasından bütün mümkün kriteriyalar üzrə digər alqoritmlərdən üstün olan alqoritm yoxdur. Alqoritm yalnız konkret kriteriya, məsələn, məhsuldarlıq üzrə digərindən üstün ola bilər. Buna görə istifadəçilərə onları maraqlandıran konkret parametrlərə görə ən yararlı alqoritm seçməyə imkan verən metrikalar çoxluğu təqdim etmək lazımdır.

Konfidensiallığın qorunması alqoritmlərinin keyfiyyətini qiymətləndirmək üçün konfidensiallığı qoruma səviyyəsi, alqoritm məhsuldarlığı, alqoritm dəqiqliyi (gizlətmə metodu tətbiq edildikdən sonra PPDM nəticələrinin keyfiyyəti), verilənlərin faydalılığı (verilənlərin keyfiyyəti) və mürəkkəbliyin (konfidensiallığı qoruyan alqoritm nəzərdə tutulan bütün resurslar baxımından yaxşı nəticələrlə yerinə yetirilməsi qabiliyyəti) kimi meyarlar istifadə edilə bilər [2].

**V. FƏRDİ MƏLUMATLARIN GİZLİLİYİNİN
QORUNMASINA ƏSAS YANAŞMALAR**

PPDM-də verilənlərin konfidensiallığını təmin etmək üçün iki yanaşma istifadə edilir: verilənlərin təhrif edilməsi metodları (ing. data perturbation) və təhlükəsiz hesablama metodları (şifrləmə metodları). Bu iki yanaşmaya əsaslanan çoxsaylı məqalələr nəşr olunmuşdur.

Diferensial gizlilik

Diferensial gizlilik (Differential Privacy, DP) metodu ilk dəfə 2005-ci ildə təklif edilib [24]. Bu metod fərdi məlumatlara müraciətləri alqoritm və interfeys (etibarlı kurator kimi çıxış edir) vasitəsilə idarə edir. Tədqiqatçı verilənləri analiz etmək üçün kuratora sorğu göndərir və kurator da təsadüfi küy əlavə etməklə verilənlərin konfidensiallığını qorumağa və eyni zamanda sorğulara düzgün cavab verməyə çalışır. DP şirkətlərə istifadəçilərin vərdisləri barədə aqreqasiya olunmuş məlumatları toplamağa və bu zaman hər bir istifadəçinin konfidensiallığını qorumağa imkan verir.

Laplas mexanizmi. DP metodlarının bir çoxu verilənlərə idarə edilən küy əlavə edir. Laplas mexanizmi Laplas küyü əlavə edir (yəni Laplas paylanmasına tabe olan küy). DP mexanizmi yaratmağa imkan verən digər küy formaları, məsələn, Qauss küyü də əlavə etmək olar.

Diferensial gizliliyin tərifində iki D və D' verilənlər çoxluğuna baxılır [25]. D -də verilmiş fərdin məlumatları var və bu məlumatlar D' -də silinib (və ya hər hansı əlaqəsi olmayan məlumatlarla əvəzlənib). Tələb olunur ki, prosesin sonunda D və D' -ni bir-birindən fərqləndirmək mümkün olmasın. Fərqləndirməmə ϵ parametrindən istifadə etməklə ölçülür. ϵ parametri D və D' -dən alınmış nəticələrin paylanmasının nə dərəcədə yaxın olmasını ölçür. ϵ kiçik olduqda gizliliyin təhlükəsizliyi səviyyəsi yüksək olur.

Tərif. Əgər ən çoxu bir sıra ilə fərqlənən D və D' verilənlər çoxluqları və $S \subseteq \text{Range}(K)$ üçün aşağıdakı şərt ödənirsə, onda randomizasiya edilmiş K alqoritm ϵ -diferensial gizlilik verir:

$$\Pr[K(D) \in S] \leq \exp(\epsilon) \times \Pr[K(D') \in S].$$

DP alqoritmlərində iki kəmiyyətə baxılmalıdır:

Epsilon (ϵ): verilənlərdə diferensial dəyişiklik zamanı (bir sıra əlavə edildikdə və ya silindikdə) gizlilik itkisini ölçür, bu kəmiyyət nə qədər kiçikdirsə, gizlilik bir o qədər çox qorunur.

Dəqiqlik: DP alqoritmının çıxışının təmiz çıxışa yaxınlığı.

Laplas mexanizmindən fərqli mexanizmlər üçün daha bir kəmiyyət: **delta (δ)** istifadə edilir.

DP geniş spektrdə **gizlilik hücumlarına** (o cümlədən **diferensiallama hücumu**, **əlaqələndirmə hücumu** və **rekonstruksiya hücumlarına**) qarşı gizliliyin qorunmasının riyazi isbatlanan zəmanətini təmin edir [26].

Verilənlərin müxtəlif növləri üzərində analitik məsələlər üçün DP alqoritmlərinin işlənməsi sahəsində bir çox tədqiqat mövcuddur [26]. DP alqoritmlərinə misal olaraq RNM (Report

Noisy Max) [26] və PATE (Private Aggregation of Teacher Ensembles) [27] alqoritmlərini göstərmək olar.

Təhlükəsiz çoxtərəfli hesablamalar

Paylanmış verilənlər üzərində PPDM kontekstində kriptografiyaya əsaslanan üsullar aşağıdakı məzmunlu məsələləri həll etmək üçün işlənmişdi: iki və daha çox tərəf onların gizli verilənləri əsasında hesablamalar aparmaq istəyir. Hesablamaları elə aparmaq lazımdır ki, heç bir tərəf öz daxil etdiyindən və nəticədən başqa heç bir şey bilməsin. Bu məsələ təhlükəsiz çoxtərəfli hesablamalar (Secure Multiparty Computation, SMC) məsələsi adlanır. Təhlükəsiz ikitərəfli hesablama konsepsiyası formal olaraq 1986-cı ildə [28]-də daxil edilmiş, 1987-ci ildə isə [29]-də çoxtərəfli variantı genişləndirilmişdi.

Ümumiyyətlə, SMC kriptografiyanın bir qoludur və paylanmış tapşırıqların təhlükəsiz şəkildə reallaşdırılmasını öyrənir. Burada təhlükəsizlik dedikdə konfidensiallığın təmin edilməsi, hesablamaların bədniiyyətli hücumlardan qorunması və s. nəzərdə tutula bilər. SMC-nin məqsədi kollaborativ hesablama məsələsini həll etməkdir, yəni bir-birinə etibar etməyən qrupda hər hansı etibarlı üçüncü tərəf olmadan gizliliyi qorumaqla istifadəçilərin konfidensial verilənlərindən asılı açıq funksiyanın qiymətini hesablamaqdır. Aydındır ki, bu məsələ, mahiyyətcə, həm də PPDM məsələsidir və PPDM məsələsi SMC məsələsinin xüsusi halıdır.

Formal olaraq, tutaq ki, təhlükəsiz hesablamada $p_1, p_2, \dots, p_n$ tərəfləri iştirak edir. Onların gizli verilənləri uyğun olaraq, $d_1, d_2, \dots, d_n$ -dir. İştirakçılar öz verilənlərinin konfidensiallığını pozmadan $f(d_1, d_2, \dots, d_n)$ funksiyanın qiymətini hesablamaq istəyirlər, burada f bütün iştirakçılara məlum olan açıq funksiya.

İştirakçılar bir-birinə və ya kommunikasiya etdikləri kanallara etibar etməyə bilərlər. İştirakçıların arasında yarıdüzürlərin olmasına yol verilir, yəni onlar protokola əməl edirlər, lakin istənilən aralıq verilənlərdən əlavə informasiya almağa cəhd edirlər.

Lindell və Pinkas ilk dəfə SMC üsulunu üfüqi bölünmüş verilənlər üzərində ID3 alqoritmı istifadə edilməklə klassifikasiya üçün təklif etmişdilər [30]. Ondan sonra saquli bölünmüş verilənlərdə klassifikasiya və üfüqi bölünmüş verilənlərin klasterləşdirilməsi üçün bir sıra SMC alqoritmləri təklif edilmişdir [2].

Homomorf şifrləmə

Texnoloji yanaşmalardan biri də bu sahədə yeni kriptografik alqoritmlərin işlənməsidir. Klassik şifrləmə üsulları artıq yetərli deyil və şifrlənmiş verilənlər üzərində hesablamalar aparmağa imkan verən üsulların işlənməsi tələb edilir:

Homomorf şifrləmə sistemi şifrlənmiş məlumatlar üzərində məlumatları deşifrləmədən riyazi əməliyyatlar (məsələn, toplama, çıxma, birləşmə, kəsişmə) aparmağa imkan verir. Məlumdur ki, RSA kriptosistemi məxfi açarı bilmədən şifrlənmiş verilənlər üzərində vurma əməlini yerinə yetirməyə imkan verir. Belə sistem *multiplikativ homomorf şifrləmə*

adlanır [31]. Oxsar olaraq, əgər məxfi açarı bilmədən toplama əməli dəstəklənsə, *additiv homomorf şifrələmə* adlanır. *Tam homomorf şifrələmə* (Fully Homomorphic Encryption, FHE) məxfi açarı bilmədən istənilən hesablamaları dəstəkləyir, yəni istənilən $\odot$ əməli və iki m_1 və m_2 açıqmətnləri üçün

$$Enc(m_1) \odot Enc(m_2) = Enc(m_1 \odot m_2).$$

Belə sistemlərin qurulması onilliklər boyu kriptografiya açıq məsələ olmuşdur. Nəhayət, ilk dəfə 2009-cu ildə tam homomorf şifrələmə sistemi IBM şirkətinin kriptografi C.Gentry tərəfindən təklif edilmişdi [32]. Homomorf şifrələmə sistemləri fərdi məlumatların qorunması, bulud hesablamaları, elektron səsvermə, maliyyə məlumatlarının emalı, tövsiyə sistemlərində tətbiq edilə bilər.

DP metodları fərdi konfidensiallığı qorumaq üçün verilənlərin faktiki qiymətlərinə normal paylanmadan olan təsadüfi qiymətlər əlavə edir (riyazi gözləməsi sıfır olan). Nəzərə almaq vacibdir ki, verilənlərin modifikasiyası nəticəsində verilənlər bazasının funksionallığı deqradasiya edir. Bu yanaşmanın problemlərindən biri konfidensiallıq ilə nəticələrin dəqiqliyi arasında olan balansdır. SMC yanaşmasının DP üzərində üstünlüyü nəticələrin təxmini deyil, dəqiq olmasıdır, lakin o, xeyli hesablamalar və hər bir təhlükəsiz kommunikasiya addımında əlavə kommunikasiya yükü tələb edir.

VI. DEEP LEARNING METODLARI

Çoxsaylı dərin neyron şəbəkə arxitekturalarından ən çox tətbiq ediləni konvolyusiya neyron şəbəkələridir (Convolutional Neural Network, CNN). CNN irəli yayılan çoxlaylı neyron şəbəkəsidir, şəkillərin tanınması və klassifikasiyası üçün geniş istifadə edilir [6]. Onun əsas tikinti blokları növbələşən konvolyusiya layları, pulinq layları, aktivləşdirmə funksiyası və tam əlaqəli laydır. Konvolyusiya layında lokal əlaqələndirmə və çəki paylaşımı yolu ilə siqnalın bəzi əsas xarakteristikaları – aşağı səviyyə əlamətləri çıxarılır. Konvolyusiyadan alınmış əlamət vektorunun ölçüsü böyük olur, onu azaltmaq üçün pulinq layları istifadə edilir. Bu laylardan sonra istifadə edilən tam əlaqəli lay lokal əlamətləri birləşdirir və konkret məsələlər üçün qlobal əlamətlər formalaşdırır. Bu laydakı hər bir neyron əvvəlki layın bütün neyronları ilə əlaqəlidir, lakin həmin layın neyronları arasında əlaqələr yoxdur.

CNN səhvin geriye yayılması algoritmi ilə öyrədilir, bu alqoritmə stoxastik qradiyent eniş (Stochastic Gradient Descent, SGD) optimallaşdırma algoritminin müxtəlif modifikasiyaları istifadə edilir.

Adətən, aktivləşdirmə funksiyası kimi ReLU (Rectified Linear Unit) istifadə edilir: $f(x) = \max(0; x)$.

Dropout layı təlim zamanı overfitting problemini həll etməyə xidmət edir [33]. Təlim zamanı dərin neyron şəbəkəsi təlim verilənlərində yüksək nəticə göstərir, lakin təlimdə rast gəlmədiyi test verilənlərində nəticələri xeyli pisləşir. Dropout metodunun mahiyyəti təlim prosesində layın seçilməsi və oradan müəyyən sayda (məsələn, 20 %) neyronun təsadüfi çıxarılmasıdır, onlar sonrakı hesablamalarda iştirak etmir. Belə

üsul öyrənmənin effektivliyini və nəticənin keyfiyyətini yaxşılaşdırır.

Avtoenkoder çıxışda girişin özünü verməyi öyrənən irəli yayılan neyron şəbəkəsidir [6]. Giriş-gizli lay hissəsi enkoderə, gizli lay-çıxış hissəsi dekoderə uyğun gəlir. Dərin avtoenkoder avtoenkoderin enkoder və dekoderini bir neçə gizli laylarla genişləndirməklə qurulur. Küysüzləşdirən (ing. denoising) avtoenkoder – avtoenkoderə stoxastik küy əlavə etməklə daha robust əlamətlər öyrənməyə məcbur edilir.

VII. FƏRDİ MƏLUMATLARIN GİZLİLİYİ ÜÇÜN DEEP LEARNING YANAŞMALARI

[8]-də fərdi məlumatların konfidensiallığının təmin edilməsi üçün mövcud yanaşmaları homomorf şifrələmə, diferensial gizlilik və təhlükəsiz çoxtərəfli hesablama əsaslı olmaqla üç qrupa bölür.

[34]-də avtoenkoderlər əsasında dPA (ddeep Private auto-encoder) metodu təklif edilir. Əsas ideya ənənəvi dərin enkoderin nəticəsini deyil, məqsəd funksiyasını perturbasiya etməklə ϵ -diferensial gizliliyi təmin etməkdir.

[35]-də ikisəviyyəli arxitektura təklif edir, arxitektura da modifikasiya edilmiş seyrək küysüzləşdirən avtoenkoder (verilənlərin çevrilməsi üçün) və dərin CNN şəbəkəsi (çevrilmiş verilənlərin klassifikasiyası üçün) istifadə edilir.

R. Shokri və V. Shmatikov dərin neyron şəbəkəsinin paylanmış təlimi üçün sistem yaradılır və qiymətləndirilir [36]. Bu sistemdə müasir təlim təlim metodlarında istifadə edilən stoxastik qradiyent eniş algoritmlərinin paralelləşdirilməsi və asinxron yerinə yetirilməsi faktından istifadə edilir. Sistem iştirakçılara neyron şəbəkə modelini öz gizli verilənləri ilə öyrətməyə və təlim zamanı modelin əsas parametrlərinin kiçik altçoxluluğunu selektiv paylaşmağa imkan verir. Bu dəqiqlik/konfidensiallıq fəzasında cəlbədicə nöqtədir: iştirakçılar gizli verilənlərin konfidensiallığını təmin edirlər və digər iştirakçıların modellərindən faydalanaraq öz modellərinin öyrənmə dəqiqliyini artırır.

[37]-də piksel-əsaslı şəkil şifrələməsi metodu dərin neyron şəbəkələrində konfidensiallığı qorumaq üçün təklif edilir və ResNet-18 şəbəkəsi ilə şəkillərin klassifikasiyası üçün tətbiq edilir. Digər oxşar metodlardan fərqli olaraq, təklif edilmiş metod şifrlənmiş fəzada verilənlərin artırılmasına imkan verir.

H. Chabanne və həmmüəllifləri CryptoNets yanaşmasının (Microsoft tədqiqatçıları təklif etmişdir) dərin neyron şəbəkələrində (2-dən çox lay olduqda) qeyri-effektiv işləməsi problemini həll edirlər [38]. Bunun üçün CryptoNets-in orijinal ideyaları [39] ilə paket normallaşdırması ideyası birləşdirilir. Verilənlərin konfidensiallığını və emalın effektivliyini təmin etmək üçün CryptoNets-in əsas ideyası neyron şəbəkə ilə tam homomorf şifrələməni birləşdirməkdir. Təklif edilən yanaşma 6 qeyri-xətti layı olan neyron şəbəkəyə tətbiq edildikdə MNIST bazasında CryptoNets-i əhəmiyyətli dərəcədə yaxşılaşdırır.

[40]-da ReLU aktivləşmə funksiyası ilə CNN istifadə edilir və pulinq layı addımı artırılmış konvolyusiya layı ilə əvəz

edilir. Bu CNN-in strukturunu sadələşdirir və onun effektivliyini artırır. Konfidensiallığı təmin etmək üçün FHE istifadə edilir, lakin FHE hesablamalar baxımından effektiv deyil, buna görə CNN-i modifikasiya etmək lazım gəlir.

Neyron şəbəkələri tibbi və maliyyə məlumatları kimi konfidensial verilənlərə tez-tez tətbiq edilir.

Shokri və Shmatikov metodunda lokal verilənlər haqqında informasiyanın dürüst, amma maraqlı serverə sızdırıla biləcəyini göstərirlər və serverə informasiya sızıntısını aradan qaldırmaq üçün asinxron stoxastik qradiyent enişində additiv homomorf şifrəlmə istifadə edirlər [41].

[42]-də çoxlaylı, məqsədi qeyri-qabarıq və parametrlərinin sayı olduqca çox olan modellərə baxılır. Neyron şəbəkələrinin diferensial gizli təliminə təklif edilən yanaşmanın əsas elementləri diferensial gizli SGD alqoritmi, momentlərin uçuotu və hiperparametrlərin köklənməsi komponentləridir. Təklif edilən yanaşma TensorFlow əsasında reallaşdırılıb.

Momentlərin uçuotu konfidensiallıq itkisini izləmək üçün istifadə edilir. Konfidensiallıq itkisi alqoritmə əlavə edilən təsadüfi küydən asılı olan təsadüfi kəmiyyətdir. Hər bir addımda konfidensiallıq itkisi momentlərinin loqarifmləri additiv toplanır.

Hiperparametrlərin köklənməsi konfidensiallıq, dəqiqlik və məhsuldarlığı balanslaşdırmaq, xüsusən də modelin konfidensiallıq ilə relevant xarakteristikaları üçün nəzərdə tutulub. Müəlliflər eksperimentlər vasitəsilə müşahidə edirlər ki, modelin dəqiqliyi neyron şəbəkəsinin strukturuna nisbətən, paketin ölçüsü və küy səviyyəsi kimi təlim parametrlərinə daha həssasdır.

[43]-də dərin neyron şəbəkələrinin şifrələnmiş verilənlər üzərində işləməsi üçün CryptoDL yanaşması təklif edilir, onun əsas komponentləri CNN və FHE-dir. CNN-də geniş istifadə edilən aktivləşdirmə funksiyalarının (ReLU, sigmoid, tanh) aşağı dərəcəli çoxhədlilərlə approksimasiyası metodu işlənir, bu effektiv homomorf şifrəlmə sxəmləri üçün olduqca vacibdir. Sonra laylarının sayı və strukturu dəyişən müxtəlif CNN-lərdə yeni aktivləşmə funksiyaları ilə MNIST aparılan eksperimentlər yanaşmanın düzgünlüyünü təsdiqləyir (99,52%, ən yaxşı nəticə 99,77 %-dir).

PrivyNet sensitiv təlim verilənləri probleminə diqqət yetirir [44]. Lokal dayaz neyron şəbəkələri qurulur və aralıq təsvirləri buludla paylaşaraq yekun model öyrədilir. Diferensial gizliliyi aralıq təsvirlərə küy əlavə etməklə təmin etməyə çalışırlar. Lokal dayaz neyron şəbəkələri açıq məlumatlardır və PrivyNet metodu MIA və GAN hücumlarına həssasdır.

NƏTİCƏ

İnformasiya və kommunikasiya texnologiyalarının sürətli inkişafı nəticəsində böyük həcmdə generasiya edilən fərdi məlumatların təhlükəsizliyinə böyük təhdidlər yaranır. Bu təhdidlərin bir qismi fərdi məlumatların intellektual analizi ilə əlaqədar meydana çıxır. Müasir intellektual analiz metodları müxtəlif mənbələrdə toplanmış böyük həcmli fərdi verilənləri əlaqələndirməklə və analiz etməklə fərdlər və sosial qruplar

barəsində onların özünə də məlum olmayan yeni sensitiv biliklər aşkarlamağa imkan verir. Bu işdə intellektual analiz zamanı fərdi məlumatların konfidensiallığını təmin etmək üçün Deep Learning metodları ilə diferensial gizlilik, homomorf şifrəlmə və təhlükəsiz çoxtərəfli hesablamaların birgə tətbiqi sahəsində mövcud işlərin icmalı verilmişdir. Müəllifin gəldiyi nəticəyə görə, diferensial gizlilik metodları ilə Deep Learning metodlarının kombinasiyası dəqiqlik və məhsuldarlıq balansının təmin olunması baxımından daha perspektivlidir.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikası Dövlət Neft Şirkətinin (SOCAR) Elm Fondunun maliyyə yardımı ilə yerinə yetirilmişdir – **Müqavilə № 23LR – AMEA.**

İSTİNADLAR

- [1] Y. İmamverdiyev “Big data və fərdi məlumatların təhlükəsizliyi,” Big data: imkanları, multidissiplinar problemləri və perspektivləri I respublika elmi-praktiki konfransı, s. 109-113, 2016.
- [2] C.C. Aggarwal, and P.S. Yu. Privacy-preserving data mining: models and algorithms. New York: Springer, 2008.
- [3] P. R. M. Rao, S. M. Krishna, & A. S. Kumar, “Privacy preservation techniques in big data analytics: a survey,” Journal of Big Data, 5(1):33, 2018. <https://doi.org/10.1186/s40537-018-0141-8>
- [4] K. Kenthapadi, I. Mironov, & A. Thakurta “Privacy-preserving Data mining in industry,” Companion Proceedings of The 2019 World Wide Web Conference, pp. 1308-1310, 2019.
- [5] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” Nature, vol. 521, pp. 436–444, 2015.
- [6] I. Goodfellow, Y. Bengio, and A. Courville, Deep learning. MIT Press, 2016.
- [7] P. Xie, B. Wu, & G. Sun “BAYHENN: Combining bayesian deep learning and homomorphic encryption for secure DNN inference,” arXiv preprint arXiv:1906.00639, 2019.
- [8] H. C. Tanuwidjaja, R. Choi, & K. Kim “A survey on deep learning techniques for privacy-preserving,” International Conference on Machine Learning for Cyber Security, pp. 29-46, 2019.
- [9] D. Zhang, X. Chen, D. Wang, & J. Shi “A survey on collaborative deep learning and privacy-preserving,” IEEE Third International Conference on Data Science in Cyberspace (DSC), pp. 652-658, 2018.
- [10] A. Gkoulalas-Divanis, G. Loukides, & J. Sun “Publishing data from electronic health records while preserving privacy: A survey of algorithms,” Journal of biomedical informatics, 50, pp. 4-19, 2014.
- [11] R. Shokri, M. Stronati, C. Song, V. Shmatikov “Membership inference attacks against machine learning models,” IEEE Symposium on Security and Privacy, pp.3-18, 2017.
- [12] C. Dwork, & A. Roth “The algorithmic foundations of differential privacy,” Foundations and Trends in Theoretical Computer Science, 9(3–4), pp. 211-407, 2014.
- [13] N. Hamza, & H. A. Hefny “Attacks on anonymization-based privacy-preserving: a survey for data mining and data publishing,” Journal of Information Security, 4(02), pp. 101-112, 2013.
- [14] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville & Y. Bengio, “Generative adversarial nets,” Advances in neural information processing systems, 2014, pp. 2672-2680.
- [15] M. Fredrikson, S. Jha, & T. Ristenpart “Model inversion attacks that exploit confidence information and basic countermeasures,” Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 1322-1333, 2015.

- [16] F. F. Zhao, L. F. Dong, K. Wang, Y. Li, “Study on privacy protection algorithm based on k-anonymity,” *Physics Procedia*, Vol.33, pp. 483-490, 2012.
- [17] X. Qi, & M. Zong “An overview of privacy preserving data mining,” *Procedia Environmental Sciences*, 12, pp. 1341-1347, 2012.
- [18] S. Upadhyay, C. Sharma, P. Sharma, P. Bharadwaj, & K. R. Seeja “Privacy preserving data mining with 3-D rotation transformation,” *Journal of King Saud University-Computer and Information Sciences*, 30(4), pp. 524-530, 2018.
- [19] Z. Huang, W. Du, & B. Chen “Deriving private information from randomized data,” *Proceedings of the 2005 ACM SIGMOD international conference on Management of data*, pp. 37–48, 2005.
- [20] S. E. Fienberg, & J. McIntyre “Data swapping: Variations on a theme by dalenius and reiss,” *International Workshop on Privacy in Statistical Databases*, pp. 14-29, 2004.
- [21] L. Sweeney, “k-anonymity: A model for protecting privacy,” *International Journal of Uncertainty Fuzziness and Knowledge Based Systems*, vol. 10, no. 5, pp. 557-570, 2002.
- [22] J. Dowd, S. Xu, & W. Zhang “Privacy-preserving decision tree mining based on random substitutions,” *International Conference on Emerging Trends in Information and Communication Security*, pp. 145-159, 2006.
- [23] C.C. Aggarwal, *Data mining: the textbook*. Springer, 2015.
- [24] C. Dwork, F. McSherry, K. Nissim, A. Smith “Calibrating noise to sensitivity in private data analysis,” *Theory of Cryptography Conference*, pp. 265–284, 2006.
- [25] K. Nissim, T. Steinke, A. Wood, M. Altman, et al “Differential privacy: A primer for a non-technical audience,” *Vanderbilt Journal of Entertainment & Technology Law*, 21 (1), pp. 209-276, 2018.
- [26] C. Dwork, & A. Roth “The algorithmic foundations of differential privacy,” *Foundations and Trends in Theoretical Computer Science*, 9(3–4), pp. 211-407, 2014.
- [27] N. Papernot, M. Abadi, U. Erlingsson, I. Goodfellow, & K. Talwar “Semi-supervised knowledge transfer for deep learning from private training data,” *arXiv preprint arXiv:1610.05755*, 2016.
- [28] A.C.-C. Yao “How to generate and exchange secrets,” *Foundations of Computer Science 27th Annual Symposium*, pp. 162–167, 1986.
- [29] O. Goldreich, S. Micali, A. Wigderson “How to play any mental game,” *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, pp. 218–229, 1987.
- [30] Y. Lindell, B. Pinkas “Privacy preserving data mining,” In: Bellare M. (eds) *Advances in Cryptology – CRYPTO 2000*. Lecture Notes in Computer Science, vol 1880. 2000.
- [31] R. L. Rivest, L. Adleman, & M. L. Dertouzos “On data banks and privacy homomorphisms,” *Foundations of secure computation*, 4(11), pp. 169-180, 1978.
- [32] C. Gentry “Fully homomorphic encryption using ideal lattices,” *Annual ACM on Symposium on Theory of Computing*, pp. 169–178, 2009.
- [33] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov “Dropout: A simple way to prevent neural networks from overfitting,” *The Journal of Machine Learning Research*, 15(1), pp. 1929–1958, 2014.
- [34] N. Phan, Y. Wang, X. Wu, & D. Dou “Differential privacy preservation for deep auto-encoders: an application of human behavior prediction,” *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence (AAAI-16)*, pp. 1309-1316, 2016.
- [35] R. M. Alguliyev, R. M. Aliguliyev, & F. J. Abdullayeva “Privacy-preserving deep learning algorithm for big personal data analysis,” *Journal of Industrial Information Integration*, 15, pp. 1-14, 2019.
- [36] R. Shokri, & V. Shmatikov “Privacy-preserving deep learning,” *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, pp. 1310-1321, 2015.
- [37] W. Sirichotedumrong, T. Maekawa, Y. Kinoshita, & H. Kiya “Privacy-preserving deep neural networks with pixel-based image encryption considering data augmentation in the encrypted domain,” *arXiv preprint arXiv:1905.01827*, 2019.
- [38] H. Chabanne, A. de Wargny, J. Milgram, C. Morel, & E. Prouff “Privacy-preserving classification on deep neural network,” *IACR Cryptology ePrint Archive*, 2017. <https://ia.cr/2017/035>
- [39] R. Gilad-Bachrach et al., “Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy,” in *Proc. 33rd Int. Conf. Mach. Learn. (ICML)*, vol. 48, pp. 201–210, 2016.
- [40] W. Liu, F. Pan, X. A. Wang, Y. Cao, & D. Tang “Privacy-preserving all convolutional net based on homomorphic encryption,” *International Conference on Network-Based Information Systems*, pp. 752-762, 2018.
- [41] L. T. Phong, Y. Aono, T. Hayashi, L. Wang, & S. Moriai “Privacy-preserving deep learning via additively homomorphic encryption,” *IEEE Transactions on Information Forensics and Security*, 13(5), pp. 1333-1345, 2018.
- [42] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, L. Zhang “Deep learning with differential privacy,” *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 24-28, 2016.
- [43] E. Hesamifard, H. Takabi, M. Ghasemi “CryptoDL: deep neural networks over encrypted data,” *arXiv preprint, arXiv:1711.05189*, 2017.
- [44] M. Li, L. Lai, N. Suda, V. Chandra, & D. Z. Pan “PrivyNet: A flexible framework for privacy-preserving deep neural network training,” *arXiv preprint arXiv:1709.06161*, 2017.

DEEP LEARNING METHODS FOR PRIVACY PRESERVING DATA MINING

Yadigar Imamverdiyev

Institute of Information Technology of ANAS, Baku, Azerbaijan

yadigar@iit.science.az

Abstract – The paper provides a survey of privacy preserving data mining methods, including deep learning. In recent decades, personal data has become one of the main goals of cybercriminals, and despite measures to ensure confidentiality of data, data mining methods allow to extract sensitive information about individuals. To counter this privacy threat, numerous modifications to traditional data mining methods have been proposed that work with sensitive personal data. This study analyzes the use of deep learning methods for privacy preserving, as well as the problems that arise when combining deep learning methods with differential privacy, secure multiparty computing and homomorphic encryption methods.

Keywords – *personal data, privacy, privacy threats, PPDM; deep learning.*

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-hökumət saytlarında fərdi informasiyanın gizlilik siyasətini qorumaq 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 məmurluğunun yüksəldilməsi bu məqsədə çatmağın vasitələridir [1].

II. ELEKTRON VƏTƏNDAŞ VƏ İNFORMASIYA 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;
- Əhəlinin 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;
- Əhəlinin İKT üzrə ümumi bilik səviyyəsi indikatoru;
- Əhəlinin kompüterdən iş məqsədilə istifadəsi indikatoru;
- Evdə kompüterə sahib olma indikatoru;
- İnternətdən 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 solumun 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].

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 infrastrukturunu və s.

B. Qeyri-texniki təhlükəsizlik

E-vətəndaşın informasiya sistemlərinin təhlükəsizlik tələblərini 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 formalaşmışdır. Vətəndaşlar dövlət qurumlarına müraciət etdikdə bu sistemlərdəki 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, informasiyalasdırma 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-hökumət 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 hökumət 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 hücumu 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 aspektlərini, eləcə də hökumətin fərdi məlumatların gizliliyini, bütövlüyünü və mövcudluğunu təmin etmək üçün 5 əsas faktor üzrə işlənə bilər:

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, akreditasiya sistemlərinin işlənməsini təmin edir.

Təşkilati aspekt hər hansı bir kiber hücumu qarşı strateji mühafizəni təşkil edir.

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

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

Bu faktorlar, nəticə etibarilə, kibercinayətkarlığa qarşı beynəlxalq mübarizəni asanlaşdıracaq tədbirlərin uyğunlaşdırılması 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 kibernetikənin 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. Cəbraylova “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*

Uşaqların fərdi məlumatları əsasında İnternet asılılığın müəyyən olunması üsulu

Fərqanə Abdullayeva¹, Sabirə Ocaqverdiyeva²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
a_farqana@mail.ru¹, allahverdiyevsabira@gmail.com²

Xülasə— Məqalədə İnternet mühitində uşaqların fəaliyyətləri ilə əlaqədar təhlillər aparılmışdır. Loq-fayllar və İnternet asılılıq problemi araşdırılmışdır. Uşaq və yeniyetmələrin İnternet asılılığının dərəcələrinin müəyyən olunması üçün açıq verilənlər bazası üzərində maşın təlimi üsulları tətbiq edilmişdir. Üsulların effektivliyi qiymətləndirmə metrikaları ilə analiz edilib.

Açar sözlər— loq-fayllar; uşaq və yeniyetmələr; İnternet asılılıq; maşın təlimi

I. GİRİŞ

İnformasiya cəmiyyətinin formalaşdırılması, İnternet şəbəkəsinin sürətli inkişafı və insanlara təqdim etdiyi xidmətlərin kifayət qədər populyarlıq qazanması informasiya fəzalarında böyük həcmli məlumatın formalaşmasına səbəb olmuşdur. Bu isə informasiya təhlükəsizliyi ilə bağlı müəyyən problemlər yaradır. Həmin problemlərin həlli və təhlükəsizliyin təmin olunması üçün yeni metodların, mexanizmlərin işlənməsi və tətbiqinə ehtiyac vardır[1].

Kompüter texnologiyalarının inkişafı istifadəçilərin şəbəkədə olan davranışları və onların fəaliyyətləri ilə əlaqədar müxtəlif təhlillərin aparılmasına imkan yaradır.

İnternet istifadəçilərinin bir hissəsi uşaq və yeniyetmələrdir. Uşaqlar virtual mühitdə aktivdirlər. Müasir şəraitdə informasiya texnologiyalarının inkişaf etdiyi bir dövrdə sosiallaşma amili kimi İnternet şəbəkəsi əlverişli vasitədir. Eyni zamanda istifadəçi maraqlarını izah etmək, texniki bacarıqları inkişaf etdirmək və özünü ifadə etməyin yeni formaları ilə təcrübə aparmaq üçün bir platformadır. İnternetdən istifadənin faydalı tərəfləri olduğu kimi, informasiya bolluğu şəraitində mövcud olan təhlükələrdən xəbərsiz uşaq və yeniyetmələrin bilməyərək müxtəlif təhlükələrlə rastlaşmasına səbəb ola bilər [2].

Hal-hazırda loq məlumatları analiz etməklə bir sıra məsələlər həll edilir. Şəbəkə aktivliyinin yoxlanılması, resursların və haker proqramlarının izlənməsi, təhdidlərin aşkarlanması üçün metod və hesablama vasitələrinin (alqoritm və proqramlarının) yaradılmasına xüsusi diqqət yetirilir. Loq-faylların analizi informasiya təhlükəsizliyinin təmin olunması sahəsində effektiv həllərin, metod və mexanizmlərin işlənilməsinə imkan verir.

Məqalədə uşaq və yeniyetmələrin loq-fayllarını analiz etməklə, onların İnternet mühitində fəaliyyətləri ilə əlaqədar təhlillər aparılır və şəbəkədən asılılıq dərəcəsi müəyyən edilir.

II. İNTERNET ASILILIĞI

İnternet asılılığı fenomeninin psixoloji problem kimi elmi cəhətdən öyrənilməsi iki amerika mütəxəssisi – psixiatr İ.Qoldberq və kliniki psixoloq K.Yanqın adı ilə bağlıdır. İnternet-asılılıq termini ilk dəfə elmi ədəbiyyata 1996-cı ildə İ.Qoldberq tərəfindən daxil edilmişdir [3].

Psixoloqlar, həm də elmi tədqiqatla məşğul olan digər peşə sahibləri tərəfindən araşdırılan bir problemdir. İnternet asılılıq sindromu insanın informasiyaya olan həvəs və tələbatından yaranır. İnternet məlumatla zəngin bir mühit olduğundan, istifadəçi daha çox informasiya əldə edir, paylaşır və nəticə olaraq özünün informasiyaya olan tələbatını ödəyir.

İnternet asılılıq (ing. Internet addiction) – şəxsin psixoloji durumuna, təhsil və ya peşəsinə, o cümlədən sosial əlaqələrinə ziyan vurulması ilə nəticələnən İnternetdən həddindən artıq istifadə olunmasıdır [4]. Uşaq və yeniyetmələr vaxtlarının müəyyən hissəsini İnternetdə keçirir, axtarış edir, şəbəkə oyunları oynayır, dərslərini hazırlayırlar. Ətrafda baş verənləri öyrənmə həvəsi, şəbəkə oyunlarına olan maraqları onların saatlarla İnternetdən istifadə etməsinə səbəb olur. Araşdırmalara görə İnternet asılılıq yeniyetmələr arasında daha çox müşahidə olunur [5].

Uşaqların İnternet asılılıq sindromunun qarşısını almaq üçün bəzi ölkələrdə müxtəlif tədbirlər həyata keçirilir. Məs., Cənubi Koreya dövləti İnternetdən asılılıq üzrə qarşıdurma tədbirləri həyata keçirir və hətta bu məqsədlə məktəbəqədər uşaqlardan başlayaraq plan hazırlamışdır [6].

III. LOQ ANALİZİN TƏTBİQLƏRİ VƏ PROBLEMLƏRİ

Veb-serverdə toplanan qeydiyyat faylları (ing. log files) Veb-qovşaqdan keçən trafik və istifadəçilərin davranışları haqqında əsas informasiya mənbəyi hesab olunur və əhəmiyyətli məlumatları özündə ehtiva edir. Loq-fayllar istifadəçilərin fəaliyyətləri ilə bağlı müəyyən prosesləri, hərəkət ardıcılıqlarını və istifadəçi maraqlarını ifadə edir. Loq-

faylların təhlili əməliyyat sistemləri və qurğular tərəfindən qeydə alınan hadisələri nəzərdən keçirməklə təhdidləri aşkarlamaq üçün effektiv bir yoldur [7]. Loq sistemin vəziyyəti, istifadəçi davranışı, sistem əməliyyatları və s. ilə bağlı başlıca informasiya mənbəyidir [8].

Kompüterlərin, şəbəkələrin və başqa İT sistemlərin generasiya etdiyi yazılar audit yazıları və ya sistemin davranışını sənədləşdirən yazılar adlanır. Loq-faylların analizi – loq yazıların qiymətləndirilməsidir. Təşkilatlar tərəfindən müxtəlif rıqların qarşısının alınması və normativ tələblərə cavab vermək üçün istifadə edilir.

Loq analizinin tətbiqləri aşağıdakılardır:

- təhlükəsizlik insidentlərinə cavabvermə;
- sistemlərdə, kompüterlərdə, şəbəkələrdə baş verən problemlərin aradan qaldırılması, istifadəçilərin davranışının öyrənilməsi;
- sistemin proqram tətbiqlərinin əlçatanlığını və keyfiyyət göstəricilərinin səviyyəsinin monitorinq edilməsi;
- müştərilərin hər hansı bir məhsula olan marağının modelləşdirilməsi;
- uşaqların internetdən asılılığının modelləşdirilməsi.

Loq-fayllarda olan məlumatları analiz edərək obyektlərin parametrlərinə (vaxt, məzmun və s.) görə klassifikasiya etməklə uşaqların İnternetdən nə dərəcədə asılı olması müəyyən edilə bilər və onların valideynləri, müəllimləri bu haqda məlumatlandırıla bilərlər. Təqdim olunan işdə loq-faylların analizinin məqsədi uşaqların İnternetdən asılılıq dərəcəsini müəyyən etməkdir.

IV. KLASSİFİKATORLAR

Loq-faylların analizində müxtəlif metod və alqoritmlərdən istifadə olunur. İşdə aşağıdakı metodlar tətbiq edilmişdir [9-12]:

Dayaq vektorlar metodu (Support vector machine, SVM) – təsnifat və regressiya problemləri üçün çox dəqiq və məşhur metoddur, nöqtələr fəzasını optimal hiperxətt vasitəsilə kateqoriyalara ayırmağa əsaslanır. Xətti və qeyri-xətti, bir çox praktik məsələlərin həllində istifadə oluna bilər. Bu üsuldə əlamət fəzasının ölçüsü sərbəstdir və çoxparametrlilik problemi yoxdur, lakin nöqtələrin sayı artdıqca onları ayırmaq üçün optimal xəttin tapılması mürəkkəbləşir.

Loqistik regressiya (Logistic regression) – bütün regressiya analizləri kimi, loqistik regressiya proqnozlaşdırıcı bir təhlildir. Loqistik regressiya məlumatları təsvir etmək üçün istifadə olunur. Bir asılı ikili dəyişən və bir və ya daha çox nominal, nizamlı, interval və ya nisbət səviyyəsində sərbəst dəyişənlər arasındakı münasibətləri izah etmək üçün əsas şəkildə ikili asılı dəyişən modelləşdirmək üçün loqistik bir funksiya istifadə edən statistik bir modeldir.

MLPClassifier (Multi-layer Perceptron, MLP) – neyron şəbəkənin klassik bir növüdür. Bir məlumat birdən çox siniflə

əlaqələndirilə bilər. Onlar bir və ya daha çox neyron təbəqədən ibarətdir. Məlumatlar giriş qatına daxil olur. Abstraksiya səviyyəsini təmin edən bir və ya daha çox gizli təbəqədən ibarət ola bilər. Proqnozlar çıxış səviyyəsində də aparılır. Proqnozlaşdırma məsələlərində istifadəsi əlverişlidir.

BernoulliNB (Bernoulli Naive Bayes) – bu metod yalnız ikili xüsusiyyətlər üçündür. Bunun üçün tipik bir nümunə (Bernoulli vəziyyətində) və ya bir müddətin ehtimalını ifadə edən (çoxnomial vəziyyətdə) təsnifatıdır. Multinomial model kimi, bu model verilənlərin təsnifatlaşdırılmasında populyardır.

Yuxarıda qeyd olunan üsullar vasitəsilə müxtəlif eksperimentlər aparılmış və bu üsulların üstünlükləri və çatışmazlıqları aşkarlanmışdır.

V. EKSPERİMENTLƏR

Eksperimentlər İnternet istifadəçilərinin İnternet asılılığı ilə bağlı toplanmış loq-faylları üzərində aparılmışdır [13]. İstifadə olunan verilənlər bazası 105 əlamətdən (cins, yaş, psixoloji vəziyyət, təhsil səviyyəsi, İnternetdə keçirilən vaxt və s.) ibarətdir. Təqdim edilən eksperimentlər “İnternet Time” parametrinə əsasən aparılmışdır. Burada “İnternet Time” parametri uşaqların İnternetdə keçirdiyi vaxtın müddətini göstərir. Verilənlər bazasında uşaqların bir həftə ərzində İnternetdən asılılıq kateqoriyaları təyin edilmiş və “çox asılı” sinif kimi İnternetdə ən çox fəaliyyət müddəti 51-120 saat intervalı götürülmüşdür. Bu kateqoriyalar aşağıdakı kimi müəyyən edilmişdir:

- normal – 1-15 saat;
- az asılı – 16-35 saat;
- orta asılı – 36-50 saat;
- çox asılı – 51-120 saat;

Eksperimentlər Python proqram paketində aparılmışdır. Eksperimentlərin aparılmasında BernoulliNB, Loqistik regressiya, MLPClassifier, və SVM maşın təlimi üsulları istifadə edilmişdir. Metodlar Accuracy, Precision, Recall, F1-score və Average metrikaları əsasında qiymətləndirilmişdir. Metodların effektivliyinin İnternet asılılıq verilənlər bazası üzərində müqayisəli analizinin nəticələri vizual olaraq Şəkil 1-də verilmişdir.

Şəkil 1. Metodların effektivliyinin İnternet asılılıq verilənlər bazası üzərində müqayisəsi

Şəkil 1-dən gördüyü kimi MLPClassifier və SVM klassifikatorları digər metodlarla müqayisədə daha yaxşı nəticələr göstərmişdir. Belə ki, BernoulliNB klassifikatoru “Çox asılı” sinfini 0.53, Loqistik regressiya klassifikatoru 0.72, MLPClassifier 0.90, SVM 0.95 dəqiqliyi ilə klassifikasiya edə bilmişdir.

NƏTİCƏ

İnformasiya bolluğu şəraitində və Big data probleminin olduğu bir dövrdə uşaqların İnternetdə mövcud olan təhlükələrdən qorunması vacibdir. İnformasiya təhlükəsizliyinin vəziyyətinin monitorinqinin (statistikasının) aparılması üçün loq-faylların analizi və səmərəli qərarların qəbul edilməsi çox əhəmiyyətlidir.

Təklif olunan yanaşma İnternet asılılığının təyində və İnternet təhlükələrindən qorunma problemlərinin həll edilməsində faydalı ola bilər. Loq-faylları analiz etməklə, İnternet asılılığının təyini və oradan alınan qiymətləndirmələr təhsil müəssisələri, valideynlər və ya əlaqədar şəxslərin müəyyən qərarların qəbulu zamanı faydalı ola bilər.

İSTİNADLAR

- [1] F. Yusifov, “Loq-faylların analizi əsasında informasiya təhlükəsizliyinin təmin edilməsi”, *İnformasiya texnologiyaları problemləri*, №1(7), 31-37, 2013.
- [2] R. Alguliyev and S. Ojagverdiyeva, “Conceptual Model of National Intellectual System for Children Safety in Internet Environment”, *International Journal of Computer Network and Information Security(IJCNIS)*, № 3, pp. 40-47, 2019.
- [3] R. Əliquliyev, R. Mahmudov, “İnternet asılılığı və onunla mübarizə məsələləri”, *İnformasiya cəmiyyəti problemləri*, № 2, s. 7-18, 2012.
- [4] K. Beard and E.Wolf, “Modification in the proposed diagnostic criteria for Internet addiction”, *Cyber-Psychology & Behavior*, 4(3), pp.377–383, 2001.
- [5] D. Kuss, M.Griffiths, L.Karila and J. Billieux, “Internet addiction: A systematic review of epidemiological research for the last decade”, *Current Pharmaceutical Design*, 20(25), pp.4026–4052, 2014.

- [6] J.Romano, “Prevention in the twenty-first century: Promoting health and well-being in education and psychology”, *Asia Pacific Education Review*, 15(3), pp. 417–426, 2014.
- [7] T.Qin, YL. Gao, LY. Wei, ZL. Liu and CX.Wang, “Potential threats mining methods based on correlation analysis of multi-type logs”, *IET Networks*, vol.7, pp. 299-305, 2018.
- [8] H.Hemant and İ. Rasika, “An approach for MapReduce based Log analysis using Hadoop”, *IEEE Sponsored 2’nd international conference on electronics and communication systems*, pp.1264- 1268, 2015.
- [9] P.Rushikesh, “Support Vector Machines(SVM) — An Overview”, <https://towardsdatascience.com/https-medium-com-pupalerushikesh-svm-f4b42800e989>, 2018.
- [10] J.Tolles and W.Meurer, “Logistic Regression Relating Patient Characteristics to Outcomes”, *JAMA*, vol. 316, № 5, pp.533-534, 2016.
- [11] Когда использовать нейронные сети MLP, CNN и RNN. <https://www.machinelearningmastery.ru/when-to-use-mlp-cnn-and-rnn-neural-networks>, 2018.
- [12] R.Sebastian, “Naive Bayes and Text Classification I - Introduction and Theory”, (this version, v4), <https://arxiv.org/abs/1410.5329>, 2017.
- [13] C. Wu, M. Lee, S.Liao and L.Chang, “Risk Factors of Internet Addiction among Internet Users: An Online Questionnaire Survey”. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4603790/> (Data set: “20150610_Internet Addiction dataset.sav”), 2015.

AN IDENTIFICATION METHOD OF INTERNET ADDICTION BASED ON CHILDREN’S PERSONAL DATA

Fargana Abdullayeva¹, Sabira Ojagverdiyeva²

^{1,2}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹a_fargana@mail.ru, ²allahverdiyevsabira@gmail.com

Abstract— The analysis on the activities of children in the Internet environment have been conducted in the article. Log files and the Internet addiction problem have been investigated. Machine learning techniques have been applied on open databases to determine the degree of Internet dependence of children and adolescents. The effectiveness of methods has been analyzed by evaluation metrics.

Keywords— *log files; children and adolescents; Internet addiction; machine learning*

Sosial şəbəkələrdə fərdi məlumatların təhlükəsizliyi problemləri və onların həlli yolları

Məkrufə Hacırahimova¹, Mərziyə İsmayilova²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹makrufa@science.ab.az, ²imarziya@gmail.com

Xülasə—Sosial şəbəkələrin (SŞ) meydana gəlməsi adi passiv oxucunu kontent iştirakçısına çevirdi. Bu istifadəçilərə informasiya paylaşımı və fikir mübadiləsi aparmaq, eyni zamanda oxşar maraqları olan digər istifadəçilərlə qarşılıqlı əlaqə yaratmaq üçün onlayn virtual cəmiyyətlərdə özlərini ifadə etmək imkanı verdi. Bununla belə, SŞ istifadəçilərin sosial fəaliyyət sahəsini kommersiya fəaliyyət sahəsinə çevirdi. Bu isə SŞ istifadəçiləri üçün məxfilik və təhlükəsizlik problemləri yaradır. SŞ servis provayderləri müştərilərinin fərdi və məxfi məlumatlarını toplayırlar, bunlar da məlumat toplayanlar, üçüncü tərəflər və ya icazəsiz istifadəçilər tərəfindən sui istifadə edilə bilər. Məqalədə təhlükəsizlik və məxfilik problemləri araşdırılmış, SŞ istifadəçilərinin sosial mediadan istifadə etdikləri zaman bu problemlərdən qorunması üçün təkliflər şərh edilmişdir.

Açar sözlər—sosial şəbəkələr; fərdi məlumatların mühafizəsi; təhlükəsizlik; məxfilik

I. GİRİŞ

Sosial şəbəkə istifadəçilər, təşkilatlar və onların sosial fəaliyyətləri arasındakı əlaqəni əks etdirən bir sosial qrafıdır. İstifadəçilər, təşkilatlar, qruplar qrafın qovşaqları, onların arasındakı əlaqələr isə qrafın tilləridir. Sosial media SŞ-dən istifadə etməklə virtual cəmiyyət yaradan onlayn kommunikasiya üçün verilənlərin sahibi (verilənləri generasiya edənlər) və izləyicilər (son istifadəçilər) arasında əlaqə mənbəyidir [1].

SŞ-lərin əsas məqsədi kontentləri maksimum sayda istifadəçilərlə paylaşmaqdır. İstifadəçilər gündəlik fəaliyyətlərini dərc etmək üçün Facebook, Twitter, LinkedIn və s. kimi SŞ-lərdən istifadə edirlər. Bəzən SŞ istifadəçiləri özləri və həyatları haqqında məlumatı dostları və həmkarları ilə paylaşırırlar. Lakin nəşr olunan bu məlumatlarda SŞ vasitəsilə müəyyən edilmiş kontentlərin bəziləri özəldir və buna görə dərc edilməməlidir. SŞ servis provayderləri fərdi xidmətlər təklif etmək üçün istifadəçiləri haqqında bir sıra məlumatlar toplayır, lakin onlardan kommersiya məqsədləri üçün istifadə edilə bilər. Bundan əlavə, istifadəçilərin məlumatları üçüncü tərəflərə ötürülə bilər, bu da məxfiliyin sızmasına gətirib çıxarır. Bu məlumatlar bədənyyətli istifadəçilərə istənilən bir fərdin məxfiliyinin pozulmasına imkan verə bilər. Verilənlərin məxfiliyi onlayn saxlanılan və ya paylaşılan informasiyanı aşkar edən, dəyişdirən, hücum edən və ya verilənləri məhv edən icazəsiz və zərərli girişdən

qoruyur. Bəzən tədqiqatçılar informasiyanın əldə edilməsi və idarə edilməsi üçün həllər hazırlayarkən məxfilik problemlərini nəzərə almırlar. Digər tərəfdən verilənlərin məxfiliyi üzərində işləyən tədqiqatçılar, fərdi məlumatları axtaran bədənyyətli istifadəçilərdən həssas verilənləri qorumaq üçün adətən informasiya axtarış metodlarını məhdudlaşdırırlar [2].

Sosial mediada istifadəçi tərəfindən generasiya edilən kontentə istifadəçilərin təəssüratları, fikirləri və bilikləri daxildir. Əlavə olaraq, həmçinin ad, cins, yaşayış yeri, şəxsi fotoşəkillər və s. kimi fərdi məlumatlar da daxil ola bilər. Onlayn paylaşılan informasiyalar elektron şəkildə saxlanılır və buna görə də davamlı, təkrarlanan və dəyişdirilə bilər [3]. SŞ istifadəçiləri sosial məxfiliyini təhlükə altına qoymaqla sosial identikliyi idarəetmə problemləri ilə rastlaşırlar. Statistik məlumatlara görə dünyada aktiv sosial media istifadəçilərinin sayının 2020-ci ilə qədər 2,96 milyarda çatacağı gözlənilir ki, bu da bütün dünya əhalisinin təxminən üçdə birini təşkil edir (şəkl.1) [4]. Bu global istifadəçi sayı məxfiliyin SŞ-lə əlaqəli aşkar və kritik məsələlərdən biri olduğunu göstərir. SŞ-nin sosial sferası kommersiya sferasına çevrildiyi zaman SŞ-lərə görə məxfiliyin müxtəlif problemləri (nəzarət kimi) təşviq edilir. Lakin SŞ-nin servis provayderləri bazara girişə nəzarət üçün istifadəçilərin fəaliyyətini izləyirlər. Standart SŞ-lər istifadəçinin fərdi məlumatlarını reklam məqsədi ilə istifadə üçün üçüncü tərəfə ötürür. Eyni zamanda, SŞ istifadəçiləri SŞ saytlarına baxış zamanı rəqəmsal iz buraxırlar. Bu isə kommersiya məqsədi və istifadəçi profilləri üçün verilənlər mənbəyi kimi hədəflənir [5].

Şəkil 1. 2010-2020-ci illər üzrə dünyada sosial media istifadəçilərinin sayı

“İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri”
V respublika konfransı, 29 noyabr 2019-cu il

Müasir dövrdə fərdi məlumatların təhlükəsizliyini təmin etmək ehtiyacı obyektiv bir reallıqdır. İnsanlar öz fərdi məlumatlarına edilən təhlükələrə qarşı müstəqil şəkildə mübarizə apara bilmir, dövlət səviyyəsində problemin həllinə ehtiyac yaranır. Bununla əlaqədar fərdi məlumatların qorunmasını təmin etmək üçün bir sıra dövlətlər qanunvericilik aktları qəbul etmişdir. Onlardan bir necəsi aşağıda cədvəldə verilmişdir [6, 7].

CƏDVƏL 1. FƏRDI MƏLUMATLARIN QORUNMASI HAQQINDA QANUNLAR

Dövlətlər	Qəbul olunmuş qanunlar
Amerika Birləşmiş Ştatları	Məxfilik aktı (<i>Privacy ACT</i>) (1974)
	Təhlükəsiz fəaliyyət (<i>Safe Harbor Act</i>) (1998)
	Vətənpərvərlik aktı (<i>Patriot Act</i>) (2001)
	“Fərdi məlumatların qorunması” (2003)
Avropa birliyi	“Fərdi məlumatların avtomatik emalı ilə fiziki şəxslərin hüququnun müdafiəsi haqqında” konvensiya (1981)
	“Fərdi məlumatların emalı və bu məlumatlara sərbəst surətdə müraciət zamanı fiziki şəxslərin qorunması haqqında” 95/46/EC direktivi (1995)
	“Fərdi məlumatların işlənməsi və telekommunikasiya sektorunda mülkiyyətin qorunması haqqında” 97/66/EC direktivi (1997)
Rusiya	“İnformasiya, informasiya texnologiyaları və məlumatların qorunması haqqında” Federal Qanun (2006)
	“Fərdi məlumatlar haqqında” Federal Qanun (2007)
Azərbaycan	“Fərdi məlumatlar haqqında” qanun (2010)

II. SOSIAL ŞƏBƏKƏLƏRDƏ KONFİDENSİALLIQ VƏ TƏHLÜKƏSİZLİK TƏHDİDLƏRİ

Sosial şəbəkə vasitələri şəxsi və iş həyatımızda qarşılıqlı münasibətlərimizi dəyişdirdi. Sosial və iş həyatımızda əhəmiyyətli bir rol oynasalar da, eyni zamanda məxfilik və təhlükəsizliklə bağlı yüksək risklər yaradırlar. Yüz minlərlə istifadəçi SŞ-ləri müntəzəm olaraq istifadə etdikləri üçün məxfilik və təhlükəsizlik təhdidlərinə məruz qalırlar. Bu təhdidlər klassik və müasir təhdidlər kimi klassifikasiya edilir.

A. Klassik təhdidlər

Klassik təhdidlər İnternetin inkişafından bəri bir problem olmuşdur. Bu təhdidlər zərərli proqram, fişinq, spam və ya saytlarası skript hücumlarıdır [8-11].

- *Zərərli proqramlar (ing. malware).* Zərərli proqram istifadəçilərin etimadnamələrini əldə etmək və həmkarlarına mesaj göndərməklə onları təqlid etməkdir. Məsələn, Koobface zərərli proqramı MySpace, Facebook və Twitter kimi SŞ-lər vasitəsilə yayılmışdır. O giriş etimadnaməsini toplamaq və yoluxmuş kompüterini botnetin bir hissəsi etmək üçün istifadə edilmişdir.
- *Fişinq (ing. phishing) hücumları.* Fişinq, saxta və ya oğurlanmış şəxsiyyət vasitəsi ilə etibarlı üçüncü tərəf kimi maskalanaraq istifadəçinin fərdi məlumatlarının

əldə edildiyi hücumun bir növüdür. Məsələn, Çin hökumətinin kəşfiyyatına aid edilən bir hücum zamanı Böyük Britaniya və ABŞ-ın yüksək rütbəli hərbi məmurları özünü ABŞ Hərbi Dəniz Qüvvələri admiralı kimi göstərən Ceyms Stavridis adlı bir şəxs ilə Facebookda "dost" olmaqla aldandılar.

- *Spam mesajları.* Spam mesajları arzu olunmayan mesajlardır. Spam mesajları adətən fişinq və ya zərərli saytlara yol açan bilən reklamlar və ya zərərli bağlantılar ehtiva edir. Ümumiyyətlə, spam saxta profillərdən və ya spam təbiiqlərindən daxil olur.
- *Saytlarası skript (XSS).* XSS veb əsaslı təbiiqlərə kəskin təsir göstərən ən məşhur və ciddi təhlükəsizlik problemlərindən biridir. XSS hücumu, təcavüzkarın hədəflənən istifadəçinin veb brauzerində zərərli kodu işə salmasına imkan verir, bu da verilənlərin sındırılmasına, *cookie* şəklində saxlanılan məlumatların oğurlanmasına və şifrələrin, kredit kartlarının nömrələrinin götürülməsinə səbəb olur. Bundan başqa təcavüzkar XSS-dən istifadə etməklə SŞ-lərdə yayıla bilən XSS soxulcanı hazırlaya bilər.

B. Müasir təhdidlər

Bu təhdidlər yalnız SŞ istifadəçiləri ilə əlaqədardır. Adətən müasir təhdidlərin məqsədi istifadəçilərin və onların dostlarının şəxsi məlumatlarını əldə etməkdir. Əgər istifadəçinin Facebook hesabında məxfilik parametrləri açıqdırsa onlara asanlıqla baxıla bilər. Lakin onların xüsusiləşdirilmiş məxfilik parametrləri varsa o yalnız dostlarına görünə bilər. Bu halda təcavüzkar bir Facebook profilini yarada və hədəf istifadəçilərə dost istəyi göndərə bilər. Dostluq istəyi qəbul edildikdən sonra təfərrüatlar təcavüz edəndə açıqlanır. Eynilə, təcavüzkar, istifadəçilərin fərdi məlumatlarını həmkarlarının açıq kontentindən toplamaq üçün təsirli hücum tətbiq edə bilər. Müasir təhdidlərə klikləmə, anonimləşmə hücumları, saxta profillər, identiklik klon hücumları, müdaxilə hücumları, informasiya itkisi, məkan itkisi, kiberizləmə, istifadəçi profilənməsi və s. kimi təhdidlər aiddir. Onlardan bir neçəsi aşağıda şərh edilmişdir [11-15]:

- *Klikləmə (ing. clickjacking).* Klikləmə, həm də onlayn istifadəçilərin klikləmə niyyətində olmadığı bir şeyi klikləməsi üçün zərərli bir metodun tətbiq olunduğu istifadəçi interfeysinin bərpası hücumu kimi də tanınır. Klikləmə hücumlarında təcavüzkar SŞ spamlarını yerləşdirməklə istifadəçilərin manipulyasiya edə bilər. Klikləmə hücumu ilə təcavüzkarlar fəaliyyətlərini qeyd etmək üçün istifadəçi kompüterlərinin qurğularını, mikrofon və kameranı da istifadə edə bilərlər.
- *Saxta profillər (ing. fake profiles).* Sosial şəbəkələrin çoxunda tipik bir hücum saxta profil hücumudur. Bu cür hücumda təcavüzkar sosial şəbəkədə saxta etimadnaməsi olan bir hesab yaradır və qanuni istifadəçilərə mesaj göndərir. İstifadəçilərdən dostluq

cavablarını aldıqdan sonra onlara spam göndərir. Adətən saxta profillər avtomatlaşdırılmış və ya yarımavtomatlaşdırılmışdır və bir insanı təqlid edir. Saxta profil şəbəkənin buraxılış qabiliyyətini itirməkdən əlavə onun ümumi nüfuzuna təsir göstərir. Bundan başqa, saxta profillər müxtəlif məqsədlər, məsələn, reklam üçün istifadə edilə bilər. 2017-ci ilin sonu 2018-ci ilin əvvəllərində Facebook 1,3 milyard saxta profil aşkarlamış və dayandırmışdır. Eyni ilə Twitterin 336 milyon hesabının 9-14%-nin saxta olduğu təxmin edilir.

- *İdentiklik klon hücumları (identity clone attacks).* Profil klonlanması, mövcud bir profildən oğurlanmış fərdi məlumatdan istifadə etməklə yeni saxta profil yaradan təcavüzkar tərəfindən həyata keçirilə bilər. Təcavüzkar, həmkarlarından kontentlər toplamaq və ya onlayn fırıldaqçılığın müxtəlif növlərindən istifadə etmək üçün klonlanmış istifadəçinin etimadından istifadə edə bilər.
- *İnformasiya sızması (ing. information leakage).* Bəzi istifadəçilər sağlamlıqla əlaqəli şəxsi məlumatlarını paylaşırlar. Təəssüf ki, onlardan bəziləri məhsullar, layihələr, təşkilat və ya hər hansı digər şəxsi məlumat haqqında bir az çox məlumat paylaşırlar. Bu cür həssas və özəl kontentin paylaşımı SŞ istifadəçiləri üçün mənfi nəticələrə səbəb ola bilər. Məsələn, bir sığorta şirkəti istifadəçiləri riskli müştərilər kimi təsnif etmək üçün SŞ məlumatlarını toplaya bilər.
- *Coğrafi məkan sızması (ing. location leakage).* Bu təhlükə informasiya sızmasının bir növüdür. Müxtəlif istifadəçilərin mobil qurğular vasitəsilə sosial şəbəkəyə daxil olma meyli var. Onlayn giriş üçün mobil qurğuların istifadəsi istifadəçiləri məkan məlumatlarını bölüşməyə məcbur edir bu da məkan sızması məxfiliyinin yeni təhlükəsini yaradır. Beləliklə, sosial şəbəkə saytlarında coğrafi məlumatların açıqlanması hücum edənlər tərəfindən istifadəçilərə zərər vurmaq üçün istifadə edilə bilər.
- *Kiber təcavüz (ing. cyberstalking).* Kiber təcavüz İnternet və ya sosial şəbəkələr vasitəsilə bir şəxsə və ya qrupa təcavüz etməkdir. Monitoring, şəxsiyyət oğurluğu, təhdid və ya təcavüz üçün istifadə edilə bilər.
- *İstifadəçi profilənməsi (ing. user profiling).* İstifadəçi profilənməsi demək olar ki, bütün onlayn xidmətlərdə yayılmış fəaliyyətlərdən biridir, harada ki, SŞ serverləri maşın təliminin müxtəlif metodları vasitəsilə öz məkanlarında gündəlik istifadəçi fəaliyyətlərini analiz edir. İstifadəçi profilənməsi tələb olunan obyektləri istifadəçilərə tövsiyə etmək üçün bir sıra üstünlüklərə malikdir. Lakin, istifadəçi profilənməsi fərdi məlumatlara malik olduğu üçün məxfilik sızmasına səbəb ola bilər və onun SŞ mühitində

qorunması lazımdır. Onlayn servis provayderləri kommersiya məqsədləri üçün istifadəçi profilənməsini həyata keçirir; ancaq, bu məxfiliyin sızması üçün yol açə bilər.

- *Sosial-media nəzarəti (ing. surveillance)* - istər fərdi, istər qruplar, istərsə də təşkilatlar və ya şirkətlər üçün istifadəçi məlumatlarını izləmək və əldə etmək üçün istifadə edilən yeni bir monitoring növüdür. Sosial media şəbəkəsi nəzarəti, insan fəaliyyətlərinin sosial mediada izləndiyi bir texnologiyaya əsaslanan bir nəzarətdir. Məsələn, Facebook *Cambridge Analytica* firmasına siyasi kampaniya üçün yığılan məlumatdan istifadə etmək üçün istifadəçilərin razılığı olmadan milyonlarla profilə giriş əldə etməyə icazə vermişdir.

III. SOSIAL ŞƏBƏKƏLƏRDƏ QORUNMA TƏDBİRLƏRİ

SŞ-lərdə mövcud olan bir sıra məxfilik və təhlükəsizlik problemləri ehtiyat tədbirlərinin köməyiylə aradan qaldırıla bilər. Təcavüzkar, istifadəçilərin ehtiyatsızlığı üzündən SŞ-də təhlükəsizlik və məxfilik problemlərindən istifadə edir. SŞ istifadəçilərinin dostları ilə paylaşdığı kontentlər və eyni formatda, ya da fərqli bir kontekstdə yad əllərə keçə bilər. Bu məxfilik təhdidlərinə qarşı müdafiə SŞ tərəfindən idarə olunan məxfilik parametrləri vasitəsilə təmin edilir. Lakin, bu məxfilik parametrlərinin effektivliyi kifayət deyil, çünki istifadəçilərin məxfilikliklərini qorumaq əvəzinə onlardan daha çox məlumat toplamaq üçün müqavilə hazırlanmışdır. Aşağıda istifadəçi kontentlərinin və məxfiliyin icazəsiz girişdən qorunması üçün bir sıra təkliflər sadalanmışdır [11, 16, 17]:

Məxfilik parametrləri (ing. privacy settings). Təəssüf ki, istifadəçilərin 80%-i öz SŞ-lərini yoxlamırlar və profillərinin məxfiliyinə məxfilik parametrlərinin və ya gözlənilən səviyyəyə cavab verən adekvat məxfiliyin verilib-verilməsi haqqında məlumatları yoxdur. SŞ-lər məlumat sahiblərinə kontenti icazəsiz girişdən gizlətmək üçün giriş nəzarətinin xüsusi səviyyəsini təklif etsələr də, demək olar ki, bütün SŞ-lərdə məxfilik parametrləri məhdud məxfiliyə malikdirlər. Müxtəlif sosial şəbəkə istifadəçiləri təhlükəsizlik və məxfilik parametrlərinə riayət edirlər. SŞ istifadəçilərinə məxfilik parametrlərinə riayət etmələri və SŞ-lərin təqdim etdikləri məxfilik müdafiəsi metodlarından maksimum dərəcədə istifadə etmək təklif olunur. Eyni zamanda, istifadəçilərə məxfilik parametrlərini tez-tez nəzərdən keçirmək tövsiyə olunur, çünki müxtəlif SŞ-lər hər yeniləmədən sonra məxfilik parametrlərini dəyişdirirlər.

Fərdi məlumatlar. Kontentlər hər hansı bir üçüncü tərəf tərəfindən paylaşıldıqdan sonra, bu kontentin artıq məxfi olacağına zəmanət yoxdur. Buna görə istifadəçilərdən SŞ-lərdə lazımsız şəxsi məlumatları paylaşmaması tələb olunur.

Məkan haqqında məlumat (ing. location information): Bir sıra mobil proqramlar istifadəçi yeri haqqında məlumat toplayır. Bu məkan məlumatları SŞ-lər tərəfindən istifadə

edilə bilər və üçüncü tərəfə, ilk növbədə gizlilik sızmasına səbəb olan kommersiya məqsədləri üçün verilə bilər. Buna görə istifadəçilərə potensial təcavüzkarlardan qorunmaq üçün məkan məlumatlarını SŞ-lər vasitəsilə açıqlamamaq tövsiyə olunur.

Antivirus və anticasus program təminatı (ing. antivirus and antispyware): SŞ-lər vasitəsilə kontentin yayılmasından asılı olaraq, zərərli proqramlar eksponensial olaraq artır. SŞ istifadəçilərinə zərərli proqram və casus proqramlarına qarşı mübarizə aparmaq üçün kompüterlərində, mobil telefonlarında antivirus və anticasus proqramlarını quraşdırmaq tövsiyə olunur.

Üçüncü tərəf tətbiqləri (ing. third-party applications): bir sıra məxfilik və təhlükəsizlik problemlərinə səbəb olur, çünki onların kodu SŞ və istifadəçi nəzarəti xaricindədir. Bu, SŞ və istifadəçilərə tətbiqin fəaliyyətini nəzarətdə saxlamağa və zərərli nüfuz etməni dayandırmaq üçün aktiv tədbirlər görməyə mane olur. Məlumatlar SŞ vasitəsilə ötürüldüyündən istifadəçi kontentinin istifadəsi və paylanması istifadəçilərin nəzarətində deyil. Ona görə də yanlış əllərə keçə biləcək məlumatları qorumaq üçün üçüncü tərəf tətbiqlərini silmək tələb olunur.

NƏTİCƏ

Sosial şəbəkələrdən istifadənin faydaları ilə yanaşı bəzi problemləri də mövcuddur. SŞ-lərdə əsas problem istifadəçilərin fərdi məlumatlarının təhlükəsizliyi, məxfiliyi və qorunmasıdır. Bu problemlər SŞ servis provayderləri, icazəsiz istifadəçilər və ya öz kommersiya fəaliyyətləri üçün SŞ verilənlərindən istifadə edən üçüncü tərəflər vasitəsilə yaradıla bilər. Araşdırmalardan məlum olmuşdur ki, “clickjacking”, “fake profiles”, “identity clone attacks” “information leakage”, “cyberstalking”, “location leakage” və s kimi müasir təhdidlər mövcuddur və onlardan qorunmaq üçün bir sıra məxfilik parametrləri, fərdi məlumatlar, antivirus və anticasus, üçüncü tərəf tətbiqləri kimi qorunma tədbirlərindən istifadə etmək lazımdır. Tədqiqatlar göstərir ki, SŞ-də məxfilik qorunması üzrə görülmüş işlər qənaətbəxş deyil. Bu sahədə praktiki işlərlə yanaşı, həm də elmi tədqiqatların aparılmasına ehtiyac duyulur.

İSTİNADLAR

- [1] J.A. Obar, S..Wildman, “Social media definition and the governance challenge: An introduction to the special issue,” Telecommun. Policy, 2015, vol. 39, no. 9, pp. 745–750.
- [2] N.A.Shazi, J. Mtsweni, “Big data privacy in social media sites,” Proc. of the 2017 IST-Africa Week Conference (IST-Africa), 2017, pp. 1–6.
- [3] M.Taddicken, “The ‘privacy paradox’ in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure,” Journal of Computer-Mediated Communication, 2014, vol. 19, no. 2, pp. 248–273.
- [4] <https://statista.com>

- [5] S. Ashtari, “I know who you are and I saw what you did: social networks and the death of privacy,” Journal of Information Privacy and Security, 2013, vol. 9, no. 4, pp. 80–82.
- [6] С.П. Евсеев, Э.А. Линд, О.Г. Король, О.М. Носик, “Защита персональных данных,” Системы обработки информации, 2012, выпуск 4 (102), том 1, стр. 108–117.
- [7] Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu, <http://www.e-qanun.az>
- [8] S. Alarm, K. El-Khatib, “Phishing susceptibility detection through social media analytics,” Proc. of the 9th International Conference on Security of Information and Networks, 2016, pp. 61–64.
- [9] V. Nithya, S.L. Pandian, C. Malarvizhi, “A survey on detection and prevention of cross-site scripting attack,” International Journal of Security and its Applications, 2015, vol. 9, no. 3, pp. 139–152.
- [10] E. Protalinski, Chinese spies used fake facebook profile to friend NATO officials, <https://www.zdnet.com/article/chinese-spies-used-fake-facebook-profile-to-friend-nato-officials>.
- [11] H. Almarabeh, A. Sulieman, “The impact of cyber threats on social networking sites,” International Journal of Advanced Research in Computer Science, 2019, vol.10, no. 2, pp. 1–9.
- [12] M.Y. Kharaji, F.S. Rizi; M.R. Khayyambashi, “A new approach for finding cloned profiles in online social networks,” International Journal of Network Security, 2014, vol. 6, pp. 25–37.
- [13] S. Torabi, K. Beznosov, “Privacy aspects of health related information sharing in online social networks,” Proc. of the 2013 USENIX Conference on Safety, Security, Privacy and Interoperability of Health Information Technologies, 2013, p. 3.
- [14] R. D’Ovidio; J. Doyle, “A study on cyberstalking: Understanding investigative hurdles,” FBI Law Enforc. Bull. 2003, 72, pp. 10–17.
- [15] S. Ali, A. Rauf, N. Islam, H. Farman, S. Khan, “User profiling: A privacy issue in online public network,” Sindh University Research Journal (Science Series) 2017, vol. 49, pp. 125–128.
- [16] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, B. Thuraisingham, “Semantic web-based social network access control,” Computers & Security, 2011, vol. 30, no. 2–3, pp. 108–115.
- [17] A. Chaabane, Y. Ding, R. Dey, M.A. Kaafar, K.W. Ross, “A closer look at third-party OSN applications: Are they leaking your personal information?,” Proc. of the 15th International Conference on Passive and Active Network Measurement, 2014, pp. 235–246.

SECURITY PROBLEMS OF PERSONAL DATA IN SOCIAL NETWORKS AND WAYS OF THEIR SOLUTIONS

Makrufa Hajirahimova¹, Marziya Ismaylova²

^{1,2}Institute of Information Technology of ANAS, Baku, Azerbaijan
¹makrufa@scisence.az, ²imarziya@google.com

Abstract—The advent of social networks (SN) has transformed a common passive reader into a content contributor. It has allowed users to share information and exchange opinions, and also express themselves in online virtual communities to interact with other users of similar interests. However, SN have turned the social sphere of users into the commercial sphere. This should create a privacy and security issue for SN users. SN service providers collect personal and confidential information of their customers, which can be abused by data collectors, third parties or unauthorized users. The article explores security and privacy concerns, and comments on how social network users use social media to protect themselves from these problems.

Keywords— social network; protection personal information; security; privacy

Вопросы защиты персональных данных в киберфизических системах

Людмила Сухостат

Институт Информационных Технологий НАНА, Баку, Азербайджан
lsuhostat@hotmail.com

Аннотация— Вопросы защиты персональных данных, характерные для киберфизических систем, являются одной из актуальных областей научных исследований. В статье представлен анализ существующих вопросов защиты персональных данных в киберфизических системах. Рассматриваются технологии и типы угроз, которым они подвержены. Приводятся некоторые решения этой сложной области исследований. Кроме того, рассматриваются открытые направления будущих исследований с целью защиты персональных данных, которые могут помочь исследователям в разработке новых подходов защиты от угроз киберфизическим системам.

Ключевые слова— киберфизическая система; защита персональных данных; угрозы киберфизическим системам; взаимосвязь устройств; персональные данные

I. ВВЕДЕНИЕ

Киберфизические системы (Cyber-physical system, CPS) объединяют кибернетическое начало, аппаратные и программные средства компьютера, качественно новые исполнительные механизмы (актуаторы), встроенные в их среду и способные воспринимать изменения, реагировать на них, учиться и адаптироваться [1]. CPS способствует смене парадигмы от «взаимосвязанного» мира, в котором повседневные объекты становятся взаимозависимыми, к объектам способным напрямую общаться друг с другом и коллективно предоставлять интеллектуальные услуги [2].

Все эти объекты и их связь с окружающей средой несут с собой риск раскрытия личных данных и утечки информации. Беспроводная связь увеличивает риск нарушения из-за возможностей удаленного доступа, которые потенциально подвергают систему атакам прослушивания и маскировки.

Примеры секретных CPS данных включают физиологические данные, собранные биомедицинскими датчиками, данные о потреблении энергии, собранные интеллектуальными счетчиками, и данные о местоположении, собранные мобильными телефонами, и это лишь некоторые из них. Раскрытие таких данных может создать возможности для преступной активности или привести к серьезному ущербу или даже смерти. Поэтому с такой точки зрения CPS представляет собой серьезную проблему для безопасности, защиты

персональных данных (ПД) и доверия, которые считаются одними из основных барьеров в разработке приложений CPS.

С непрерывным улучшением осведомленности о ПД, и промышленность, и научные круги активно разрабатывают жизнеспособные решения для удовлетворения постоянно растущих требований защиты ПД [3, 4].

Проблемы, связанные с защитой ПД, возникают во время процессов передачи, агрегирования и анализа данных, даже когда необработанные ПД недоступны, поскольку сложные методы интеллектуального анализа данных становятся все более эффективными и могут раскрыть основную информацию.

Традиционные технологии информационной безопасности в основном направлены на сохранение небольших и однородных ПД. Поэтому первостепенной задачей является разработка надежной, эффективной и масштабируемой аналитики больших данных с защитой ПД, которая может работать с крупномасштабными и разнородными данными [5]. Также необходимо найти компромисс между защитой ПД и полезностью, что означает, что люди все еще эффективно используют эти сервисы, в то же время, предотвращая раскрытие и вывод персональной информации, относящейся к конкретному человеку, в процессе анализа данных.

В последние несколько лет исследовательские сообщества ищут решения на данные вопросы и предложили множество подходов. Целью данной статьи является анализ уязвимостей существующих технологий CPS и угроз, направленных на нарушение защиты ПД.

В то время как область исследований все еще быстро развивается, также необходимо обсудить возможные решения вышеприведенных вопросов.

II. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В CPS

Как философское понятие «защита ПД» может относиться к набору связанных, но разделяемых понятий [6], отслеживающих как описательные, так и нормативные компоненты [7, 8]. Защита ПД означает, что секретная информация об отдельных лицах или группах не раскрывается другим лицам.

Хотя в некоторых контекстах защита ПД и конфиденциальность частично совпадают, они отличаются с точки зрения их концепций и методов защиты. Конфиденциальность рассматривается как «ориентированная на данные» концепция, которая означает, что речь идет о самих данных с целью обеспечения того, чтобы данные были известны только уполномоченным сторонам [8]. Тогда как защита ПД включает в себя дополнительную концепцию, «ориентированную на владельцев данных», которые могут быть отдельными лицами или группами, с целью защиты их частной информации при использовании их данных для анализа [8]. Следовательно, концепция защиты ПД включает рассмотрение компромисса между открытыми данными и анонимностью. Различия в их концепциях приводят к различиям в методах их защиты. Шифрование является одним из таких методов защиты [9]. Помимо криптографических инструментов, защита ПД также поддерживается методами возмущения (perturbation) (для скрытия истинного значения данных) и анонимизации (для скрытия связи «данные – владелец данных»). Другое отличие состоит в том, что потеря конфиденциальности в основном вызвана слабостью контроля доступа или схем шифрования, в то время как потеря защиты ПД связана также с уязвимостями в управлении использованием данных и аналитикой данных.

Пользователи CPS сталкиваются с угрозами защиты ПД при передаче личной информации через Интернет. Из-за большого числа устройств в CPS необходимо учитывать различные риски перед разработкой приложений или решений.

III. ВЛИЯНИЕ ТЕХНОЛОГИЙ CPS НА ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Сенсоры, устройства, данные, компьютеры и облачные соединения в значительной степени зависят от установленных доверительных отношений. Подключение большого количества устройств CPS (т. е. добавление точек вторжения) повышает вероятность угрозы для данной системы, тем самым увеличивая общий риск безопасности. Без возможности ограничения настроек для защиты ПД трудно установить доверие с системой или устройством CPS.

С точки зрения обеспечения защиты ПД на Рис. 1 представлены наиболее важные технологии CPS [10]:

Число устройств. Увеличение числа связанных устройств в CPS приводит к серьезным проблемам, в частности, масштабируемости существующих и будущих технологий защиты ПД.

Взаимосвязь устройств. С технологическим прогрессом и снижением затрат на беспроводную связь устройства CPS становятся доступными для запросов с любого расстояния, что дает большие возможности для новых услуг, но вызывает проблемы с защитой ПД.

Сбор данных. С ростом числа интеллектуальных устройств сбор данных еще глубже проникает в жизнь людей и вводит новые наборы связанных и идентифицируемых личных данных. При этом люди пассивны и, в основном, не знают о сборе данных в результате роста числа подключенных устройств.

Взаимодействие устройств. Интерфейсы позволяют людям осуществлять настройку, отладку и взаимодействие с интеллектуальными устройствами. Так развитие технологий привело к переходу от RFID (Radio Frequency IDentification) меток к сенсорам, реагирующим на прикосновения. Отсутствие интерфейсов и механизмов взаимодействия может создавать угрозы для личных данных. А сложные интерфейсы, например, на основе речевых технологий или даже телепатии приведут к расширению проблем защиты ПД.

Взаимодействие систем с людьми. Взаимосвязь и координация множества устройств и их специфических возможностей служит взаимодействию с людьми на основе сложных интерфейсов. Разработка последних требует тщательной подготовки, чтобы не нарушить защиту ПД.

Жизненный цикл устройств. CPS хранят обширную информацию о своей собственной истории в течение всего их жизненного цикла [10]. Они становятся все более динамичными при обмене информацией, например, в медицинских устройствах. С увеличением срока хранения данных и переходов в течение жизненного цикла, управление аспектами безопасности и защиты ПД станет более сложным.

Переход от вертикальной интеграции решений к горизонтальной. Современные CPS системы сочетают в себе вертикальные и горизонтальные интегрированные решения, например, интеллектуальные счетчики, которые не только передают данные о потреблении центральному коммунальному поставщику (вертикальная интеграция), а напрямую включают и выключают бытовые приборы (горизонтальная интеграция).

Локальность информационных потоков в горизонтально интегрированных системах в большей степени защищает ПД. А вертикальное интегрирование систем с различными целями и производителями может вызвать угрозы защиты ПД и нарушения безопасности.

IV. УГРОЗЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В CPS

Вопросы безопасности и защиты ПД, характерные для CPS и данных временных рядов, передаваемых из них, представляют собой новые области научных интересов.

Существуют как преимущества, так и недостатки безопасности, основанные на сложности главной вычислительной проблемы и информационной теоретической безопасности.

Рис. 1. Технологии CPS, подвергающие опасности защиту персональных данных.

Основной мерой теоретико-информационной безопасности является внутренняя информация, доступная для использования злоумышленником, независимо от того, каким образом злоумышленник ее использует.

Несмотря на множество потенциальных преимуществ, CPS представляет значительную угрозу защите ПД и безопасности из-за используемых технологий [10, 11]. Существует различные угрозы защиты данных пользователей и сложности, связанные с противостоянием таким угрозам (Таблица I), а именно:

- *Идентификация*

Персональная информация может передаваться, когда объект связан с человеком прямо или косвенно. Связь возникает, если пользователь осведомлен и дает согласие на возможную передачу личных данных. Например, когда человек что-то покупает с использованием пластиковой карты. Это может стать риском для защиты ПД пользователя.

- *Профилирование*

Угроза профилирования растет при движении к интеллектуальным сетям (smart grid) и городам. Примером является внедрение интеллектуальных электрических счетчиков, которые передают данные о потреблении энергии соответствующим коммунальным предприятиям с целью мониторинга и выставления счетов.

С юридической точки зрения необходимо учитывать вопросы, такие как профилирование потребителей, потеря

данных, утечка данных и отсутствие согласия (согласие является обязательным по закону).

- *Локализация и отслеживание*

Смартфоны и другие мобильные устройства, подключенные к Интернету, ежедневно распространяют данные, которые могут быть незаконно использованы другими людьми. Так легко можно найти точные данные о местоположении пользователя с применением геолокации. Таким образом, защита ПД может быть нарушена.

- *Переходы жизненного цикла*

Эта угроза связана со сбором и хранением информации, которая может многое рассказать об образе жизни людей, в т.ч. о местоположении, медицинских данных и др. Устройства CPS имеют динамичный жизненный цикл, где ими можно обмениваться, добавлять и свободно распоряжаться. Необходимо разработать гибкие решения для реализации «удобных» механизмов управления жизненным циклом защиты ПД.

- *Атаки на ресурсы*

Данный вид угрозы направлен на несанкционированный сбор информации о существовании и характеристиках личных данных. Информация об устройствах может быть получена законными лицами (например, владельцем и авторизованным пользователем) из различных источников, нелегитимные стороны могут запрашивать и использовать это для составления списка устройств и их местонахождения (дом, офис, предприятие). Даже если CPS могут отличить законные

запросы от незаконных (данные по скорости их общения, времени реакции и других уникальных характеристик), они могут потенциально использоваться для определения их типа и модели. Применение технологий беспроводной связи позволяет проводить атаки пассивно с применением подслушивающих устройств в непосредственной близости от дома жертвы. Например, грабители могут использовать информацию о ресурсах с целью незаконного проникновения в частные владения, промышленный шпионаж и т.д.

- *Связь систем*

Эта угроза состоит в объединении различных ранее разделенных систем. Пользователи боятся неправильного суждения и потери контекста, когда данные, собранные от разных сторон в разных контекстах и разрешениях, объединяются.

Обход механизмов защиты ПД приводит к росту риска несанкционированного доступа и утечки частной информации. Примером может служить возрастающий риск повторной идентификации анонимизированных данных.

V. РЕШЕНИЯ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В CPS

Растущие угрозы защиты ПД приводят к необходимости разработки подходов и контрмер, направленных на борьбу с ними.

В связи с этим существует ряд подходов по защите ПД в CPS, которые можно классифицировать следующим образом [12, 13]:

- Шифрование данных;
- Контроль доступа;
- Закон и политика;
- К-анонимность;
- Кэширование;
- Фиктивные запросы;
- Запутывание программного кода

и т.д.

Существуют и гибридные методы, такие как шифрование с запутыванием, кэширование с фиктивными запросами и др. [13].

Так решением для угрозы переходов жизненного цикла является временная блокировка персональной информации. А атакам на ресурсы можно противостоять, применяя легковесную криптографию и устойчивые механизмы снятия «отпечатков» устройств.

ТАБЛИЦА I. Влияние Технологий CPS на Угрозы Защиты Персональной Информации

Угрозы Защиты Персональных Данных в CPS	Вид Угрозы	Виды Нарушений	Сложности
	Идентификация	Распознавание по лицу, отпечаткам пальцев, речи и др.	Преобладание локальной обработки данных над централизованной; Преобладание горизонтальной коммуникации над вертикальной; Осведомленность пользователей.
	Локализация и отслеживание	GPS отслеживание; Интернет трафик; Определение местоположения по телефону.	Осведомленность о слежении перед пассивным сбором данных; Управление обменом локальными данными в помещении; Протоколы интеллектуального анализа с целью защиты ПД для взаимодействия с CPS системами.
	Профилирование	Рекомендательные системы; Информационные бюллетени; Рекламные объявления.	Рост объемов данных; Сбор данных из частной жизни людей.
	Угроза взаимодействия и представления	Неприкосновенность информации о частной жизни; Среда представления.	Раскрытие информации при взаимодействии устройств
	Переходы жизненного цикла	Сбор информации; Динамичный обмен информацией.	Обмен данными между устройствами
	Атаки на ресурсы	Сбор информации; Незаконные действия правоохранительных органов; Промышленный шпионаж.	Проверка подлинности запросов; Устойчивость к цифровому «отпечатку».
	Связь систем	Потеря контекста; Гетерогенная распределенная система систем; Риск повторной идентификации анонимизированных данных.	Прозрачность в отношении того, какой информацией система систем обменивается с кем-либо; Модели разрешений и контроля доступа должны быть адаптированы для множества заинтересованных сторон; Методы анонимизации данных должны работать на связанных системах и быть устойчивыми.

Решениями для профилирования будут:

- Персонализация на стороне клиента;
- Запутывание программного кода;
- Анонимизация;
- Шифрование данных.

Исследование по локализации и отслеживанию сосредоточено на следующих методах защиты:

- Изменение возможных зон расположения пользователя.
- Добавление случайного шума к информации о местоположении.

Таким образом, в статье был проведен анализ возможных решений с целью защиты ПД от угроз на CPS, которые необходимо преодолеть.

ЗАКЛЮЧЕНИЕ

Несмотря на то, что в последние годы исследователи приложили немало усилий к вопросам защиты ПД в CPS, эта область все еще остается непровержимо сложной и оставляет место для совершенствования существующих подходов, а также для разработки новых решений. В работе были рассмотрены виды угроз направленные на снижение защиты ПД, классификация технологий CPS и некоторые пути решения по защите от угроз.

Несмотря на значительный прогресс, достигнутый в области защиты ПД, остается еще много нерешенных проблем. Ряд вопросов будущих исследований приводится ниже:

- Разработка приложений по обеспечению защиты ПД в рамках различных сценариев угроз.
- Рассмотрение вопроса о ПД для приложений в распределенной среде с многочисленными устройствами с ограниченными ресурсами, такими как мобильные социальные сети, интеллектуальные счетчики, медицинские устройства и т.д.
- Разработка метода на основе легковесной криптографии с целью повышения практической эффективности.

Исследование методов устойчивых к всевозможным типам атак на ПД с различными предположениями о знаниях злоумышленника.

ЛИТЕРАТУРА

- [1] R. Alguliyev, Y. Imamverdiyev, L. Sukhostat, “Cyber-physical systems and their security issues,” *Computers in Industry*, vol. 100, 2018, pp. 212–223.
- [2] A.A.A. Sen, F.A. Eassa, K. Jambi, M. Yamin, “Preserving privacy in internet of things: A survey,” *International Journal of Information Technology*, vol. 10, 2018, pp. 189–200.
- [3] P. Zikopoulos, C. Eaton, “Understanding Big Data Analytics for Enterprise Class Hadoop and Streaming Data,” *McGraw-Hill Osborne Media*, First Edition, 2012, 176 p.
- [4] S. LaValle, E. Lesser, R. Shockley, M.S. Hopkins, N. Kruschwitz, “Big data, analytics and the path from insights to value,” *MIT Sloan Management Review*, Vol. 52, no. 2, 2011, pp. 21–31.
- [5] J.A. Shamsi, M.A. Khojaye, “Understanding privacy violations in big data systems,” *IT Professional*, Vol. 20, no. 3, 2018, pp. 73–81.
- [6] A. Moore, “Defining privacy,” *Journal of Social Philosophy*, Vol. 39, no. 3, 2008, pp. 411–428.
- [7] A. Henschke, “Ethics in an Age of Surveillance: Personal Information and Virtual Identities,” *Cambridge University Press*, Cambridge, 2017, 334 p.
- [8] F. Allhoff, A. Henschke, “The internet of things: Foundational ethical issues,” *Internet of Things* Vol. 1–2, 2018, pp. 55–66.
- [9] N. Li, N. Zhang, S.K. Das, B. Thuraishingham, “Privacy preservation in wireless sensor networks: a state-of-the-art survey,” *Ad Hoc Networks*, Vol. 7, no. 8, 2009, pp. 1501–1514.
- [10] J. Ziegeldorf, O. Garcia-Morchon, K. Wehrle, “Privacy in the Internet of Things: threats and challenges,” *Security and Communication Networks*, Vol. 7, no. 12, pp. 2728–2742.
- [11] N. Fabiano, “Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation,” *Athens Journal of Law*, Vol. 3, no. 3, 2017, pp. 201–214.
- [12] V. Chellappan, K.M. Sivalingam, “Security and privacy in the Internet of Things,” in: *Internet of Things*, A.V. Dastjerdi, R. Buyya, Ed. Morgan Kaufmann, 2016, pp. 183–200.
- [13] M. Yamin, Y. Alsaawy, A.B. Alkhodre, A.A.A. Sen, “An Innovative Method for Preserving Privacy in Internet of Things,” *Sensors*, Vol. 19, 2019, pp. 1–24.

PRIVACY ISSUES IN CYBER-PHYSICAL SYSTEMS

Lyudmila Sukhostat

Institute of Information Technology of ANAS, Baku, Azerbaijan

lsuhostat@hotmail.com

Abstract— Personal data protection issues specific to cyber-physical systems are one of the relevant areas of scientific research. The paper presents an analysis of existing issues of personal data protection in cyber-physical systems. The technologies and types of threats to which they are exposed are considered. Some solutions to this complex research field are presented. Also, open directions for future research with the aim of privacy that can help researchers to develop new approaches in protecting against threats to cyber-physical systems are considered.

Keywords— *cyber-physical system; privacy; cyber-physical system threats; device interconnection; personal data*

Системы видеонаблюдения в нефтегазовом комплексе: Безопасность производственных структур и защита персональных данных

Шакир Мехтиев¹, Тахмасиб Фаталиев², Аяз Мехтиев³

^{1,2,3}Институт информационных технологий, Баку, Азербайджан
^{1,3}depart11@iit.science.az, ²depart3@iit.science.az

Аннотация— Четвертая промышленная революция, или Industry 4.0 произвела кардинальные изменения в области критических систем, в том числе и в нефтегазовом комплексе. Нефтегазовому комплексу присущи обширная и дорогостоящая инфраструктура объектов для производства, хранения и доставки конечной продукции. Обеспечение безопасности этих объектов является сложной задачей, поскольку любые нарушения в цепочке технологических процессов, вызванные как техническими причинами, так и преднамеренными попытками причинить ущерб или кражей оборудования наносят значительный финансовый урон. Также возрастают риски для жизни и здоровья персонала этих предприятий и экологические риски для окружающей среды. Однако, решая общие проблемы безопасности и надежности, системы видеонаблюдения параллельно создают проблему защиты персональных данных, которые являются основополагающими факторами универсальных прав человека. В статье рассматриваются проблемы применения систем видеонаблюдения в нефтегазовом комплексе, реализуемом на основе концепции Industry 4.0 и предлагаются рекомендации по защите персональных данных.

Ключевые слова— Industry 4.0; нефтегазовый комплекс; риски; видеонаблюдение; персональные данные

I. ВВЕДЕНИЕ

Целью четвертой промышленной революции Industry 4.0. является достижение более высокого уровня операционной эффективности и производительности, а также автоматизации [1]. Системы видеонаблюдения и обработки изображений, используемые в различных отраслях промышленности, становятся одним из компонентов подобного автоматизированного производства. На всех этапах производства, от инспекции сырья, мониторинга производства, обнаружения дефектов и обеспечения качества и стандартов, эти системы помогают достичь высокой экономической эффективности. Это стало возможным благодаря новым видеосенсорам, наноматериалам и таким технологиям, как киберфизические системы, интернет вещей, искусственный интеллект и др. Технически новые интеллектуальные системы видеонаблюдения

регистрируют активность и рабочее состояние, результаты проверок, предлагают интеллектуальные решения по преодолению трудностей и передают их в виде информации персоналу на очки дополненной реальности (например, Microsoft HoloLens).

Следует отметить, что системы видеонаблюдения широко используются для защиты критических инфраструктур. Под защитой критической инфраструктуры понимаются меры по обеспечению безопасности взаимозависимых систем, сетей и активов, лежащих в основе служб, жизненно необходимых для функционирования общества. Нефтегазовый комплекс (НГК) также относится к подобным критическим инфраструктурам. Нефть и газ по-прежнему являются наиболее важными источниками энергии, прямо или косвенно, обеспечивают занятость большому количеству людей и вносят значительный вклад в государственный бюджет. Перебои с поставками нефти и газа негативно проявляются и в транспортной сфере, создавая неудобства и трудности людям в их ежедневной деятельности.

Принимая во внимание риски и проблемы обеспечения защиты персонала, дорогостоящей инфраструктуры и производственных процессов, задачи, решаемые системами видеонаблюдения в НГК, весьма актуальны. Однако, решая общие проблемы безопасности и надежности, системы видеонаблюдения параллельно создают проблему защиты персональных данных (ПД), которые являются основополагающими факторами универсальных прав человека.

II. КРАТКИЕ СВЕДЕНИЯ О СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

Видеонаблюдение (Video surveillance) — это технологическая система, состоящая из множества видеокамер, которые подключены к замкнутому контуру телевидения (closed circuit television, CCTV). Первоначально изображения с видеокамер отправлялись в мониторинговый центр, где оператор перед экраном осуществлял непрерывный контроль за происходящими событиями без возможности их анализа в будущем. Это было существенным недостатком подобных систем. Появившиеся в середине XX в. видеоматрицы смогли

решить эту проблему. Операторам более не требовалось проводить все время перед экраном монитора, вся информация записывалась на магнитную пленку. Однако, из-за чрезвычайно высокой стоимости первые видеоманитофоны не нашли широкого распространения в системах видеонаблюдения. Ситуация существенно изменилась в 1970-х гг., когда были представлены видеокассеты формата Video Home System (VHS) [2]. Популярность видеосистем стала расти, и ими оснащались в первую очередь вокзалы, аэропорты, банки, магазины, автозаправки и другие объекты, в наибольшей степени подверженные воздействию внешних угроз. Дальнейший прогресс систем видеонаблюдения связан с появлением интернета, цифровых камер с высоким разрешением, облачных хранилищ, искусственного интеллекта и т.п.

В настоящее время системы видеонаблюдения стали реальностью современного общества. По аналогии с концепцией Industry 4.0 можно предположить, что сейчас эти системы вступили в эру Video Surveillance 4.0. По некоторым данным только в Лондоне установлено 500000 видеокамер, а средний человек, живущий в Лондоне, будет записан на камеру 300 раз за один день [3]. Подобная тенденция роста систем видеонаблюдения и количества видеокамер характерна для США, Китая, Японии и большинства стран. Трудно представить объемы информации, записанной камерами наблюдения в общественных местах, или перехвата видеочатов через Интернет (Skype, WhatsApp, Viber и др.).

Отметим, что при сравнении обычного наблюдения с видеонаблюдением последнее имеет ряд преимуществ:

- архивация изображений и возможность последующего их анализа;
- ночное видение;
- масштабирование;
- автоматическое слежение;
- обнаружение деталей и признаков, невидимых человеческим глазом;
- интеллектуальное распознавание лица и голоса человека, вплоть до его эмоционального состояния;
- доступность видеоархива через интернет из любой точки мира.

В то же самое время видеонаблюдение в общественных местах затрагивает такую чувствительную сферу, как ограничения в передвижении, право на частную жизнь, вопросы идентификации личности и, в целом, ПД.

III. СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ КАК СОСТАВНАЯ ЧАСТЬ БЕЗОПАСНОСТИ НЕФТЕГАЗОВОГО КОМПЛЕКСА

Известно, что технологические процессы в структуре НГК выполняются последовательно в трех секторах, которые обычно называют *Upstream*, *Midstream* и *Downstream* [4]. Эти три сектора охватывают сферы добычи нефти и газа от морских разведочных и буровых платформ до береговых нефтяных скважин, транспортировку сырья посредством трубопроводов до нефтеперерабатывающих заводов, переработку сырья в конечный продукт и его доставку потребителям. Подобная многогранная деятельность создает множество проблем

общей безопасности. Как правило, участки нефтегазовых месторождений охватывают огромные территории, могут быть расположены в труднодоступных местах на суше или в открытом море и часто подвержены неблагоприятным условиям окружающей среды. Эти объекты имеют много ключевых областей, которые могут стать целями для проникновения посторонних лиц. Результатом таких действий могут стать акты саботажа, умышленной порчи технического оборудования, кражи или, в худшем случае, диверсии или террористического акта. Поэтому функционирование большинства объектов НГК требует постоянного мониторинга и дистанционного контроля, так как любое небольшое нарушение в работе каждого объекта может привести к сбою всей системы в целом и, как следствие, к экономическим и даже человеческим потерям и экологическим катастрофам. Поэтому уровень безопасности должен быть максимальным. В то же время, безопасность приходится обеспечивать на технически сложных и больших (например, нефтеперерабатывающие предприятия) и протяженных (нефтепроводах) объектах. Распределенная архитектура идеально подходит для обеспечения безопасности на крупных и протяженных объектах, а ее универсальность позволяет решать весь спектр задач обеспечения безопасности, связанных с деятельностью НГК. При этом из единого центра мониторинга можно контролировать все объекты, вплоть до самых удаленных. Комплексная система безопасности способна объединить видеонаблюдение, охранно-пожарную сигнализацию, систему охраны периметра, систему контроля и управления доступом, аудио контроль в согласованно работающую инфраструктуру. Благодаря этому комплекс различных систем безопасности превращается в единую информационную среду, в которой можно реализовать функции обработки и интеллектуального анализа информации, обладающую способностью гибко реагировать на различные события. Как показывает опыт эксплуатации систем видеонаблюдения существуют множество эффективных решений подобных систем для НГК. Рассмотрим некоторые реализованные из них.

А. Система видеонаблюдения на офшорном месторождении

В [5] приведена система видеонаблюдения для офшорного месторождения с охватом более 300 буровых установок для разведки и добычи на море. Система контролирует буровые площадки, посадочную площадку для вертолетов, оснащена специализированными подводными камерами. Система способна идентифицировать задымления, разливы нефти, нежелательные движения на буровой площадке, производится автоматическая запись и хранение событий. Также возможен общий мониторинг процесса и дополнительный удаленный (на суше) доступ к прямой трансляции.

Б. Система видеонаблюдения нефтеперерабатывающего завода

Здесь эта система осуществляет общий мониторинг и предназначена для обнаружения и предупреждения

подозрительных событий, неисправностей, аварий и краж. В дополнение к этому специализированные камеры способны непрерывно отслеживать производственные процессы во взрывоопасных, токсичных и высокотемпературных средах, где пребывание персонала невозможно. Возможности тепловизорных камер позволяют контролировать изменения температуры, осуществлять интеллектуальную аналитику, и, благодаря интеграции с системами пожарной и газовой сигнализации, можно заблаговременно предпринять упреждающие меры безопасности. В целом концепция Industry 4.0 на подобных предприятиях (например, система управления TDC 3000 компании Honeywell) позволила повысить производительность почти в 10 раз [6].

В. Мониторинг трубопроводов

Стандартные подходы к мониторингу нефте- и газопроводов дополняются видеонаблюдением с дронов. Сигналы с датчиков наблюдения и обнаружения утечек используются для идентификации текущего состояния трубопроводов и оценки экологической обстановки [7]. Система обнаружения утечек и дроны компании Asea Brown Boveri Ltd. обеспечивают точность до 3000 раз выше, чем у устаревших систем [6]. Качественные изображения в режиме реального времени позволяют оперативно обнаруживать нефтяные разливы и выявлять несанкционированную деятельность в охраняемых зонах.

Г. Техническое обслуживание

Существенный эффект может дать использование систем видеонаблюдения в техническом обслуживании. Так, например, известно, что интеллектуальные камеры Tattile могут быть подключены к большинству компонентов и систем, участвующих в процессе создания промышленной ценности, а также к сетям предприятия и интернету [8]. Вместо того, чтобы реагировать на обнаружение дефектов, интеллектуальные камеры стали инструментами анализа, которые используют статистические методы и методы обработки больших данных, чтобы получать информацию из изображений и применять их в масштабах всего предприятия.

Например, можно определить, когда какая-либо часть оборудования выйдет из строя до того, как обслуживающая бригада обнаружит проблему. Система распознает предупреждающие знаки, использует данные для создания графиков упреждающего обслуживания оборудования до возникновения проблемы. Изображения, записанные по частям, можно сравнить с тысячами других, хранящихся в облаке, чтобы определить корреляции и тенденции. В то же самое время для достижения большего эффекта видеонаблюдение может быть объединено с другой мониторинговой системой — беспроводной сенсорной сетью (Wireless Sensor Network, WSN). WSN помогает получать физическую информацию с объектов мониторинга: тепловые, химические, магнитные, вибрационные и другие характеристики [9]. Интеграция обеих технологий делает возможным создание интеллектуальной системы технического обслуживания.

Таким образом, рассмотренные примеры показывают, что системы видеонаблюдения играют существенную роль в обеспечении безопасности и надежности предприятий и процессов в НГК.

IV. Конфиденциальность и Защита Персональных Данных в Системах Видеонаблюдения

Согласно Общим положениям о защите данных (General Data Protection Regulation, GDPR) к ПД можно отнести любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу [10]. Любые операции, выполняемые с ПД или с наборами ПД, независимо от того, выполняются ли они автоматическими средствами, такими как сбор, запись, организация, структурирование, хранение, адаптация или изменение, поиск, консультация, использование, раскрытие путем передачи, распространение или иное предоставление, выравнивание или комбинация, ограничение, удаление или уничтожение — квалифицируются, как обработка ПД. Таким образом, очевидно, что проблемы с ПД могут возникать во всех сферах деятельности и во всех аспектах жизни в целом, поскольку информацию, с помощью которой можно идентифицировать физическое лицо, можно найти практически везде, в том числе и в системах видеонаблюдения. Следует принять во внимание, что использование системы видеонаблюдения на предприятии влечет за собой обработку ПД в том случае, если лицо можно опознать.

Видеокамеры сегодня моментально устанавливают личность человека, его пол и возраст. Был разработан алгоритм с применением нейросетей для повышения общественной безопасности и выявления преступников, который уже активно применяется и в бизнесе. Технология распознавания лиц вошла в национальный стандарт России «Smart city» [11].

Следует отметить, что идентификация личности возможна и по его другим признакам, например, форма тела, одежда, имеющиеся при себе вещи и т.д. Факт видеосъемки работника на рабочем месте уже есть обработка ПД. Однако, априори такие ПД работника являются конфиденциальной информацией, поскольку это информация о физическом лице, и их обработка без согласия соответствующего лица не допускается, кроме случаев, четко определенных законом [12].

С практической позиции, очевидно, что во избежание лишних недоразумений между работодателем и работником должно быть составлено письменное согласие на обработку ПД. Как альтернативный вариант можно будет рассмотреть вариант, когда в помещении ведется открытая видеосъемка и установлены на видном месте предупредительные таблички о видеонаблюдении (тогда можно говорить о молчаливом согласии).

Аналогичные угрозы ПД возникают и при использовании дронов в целях мониторинга инфраструктуры НГК, топографических съемок и экологической инспекции местности. В этом случае проводимые операции создают риски непреднамеренной

обработки ПД. Так, например, может произойти захват изображений людей на заднем плане. Здесь под задним планом понимаются близлежащие места жительства, зоны отдыха, транспортные средства и т. д. Следует отметить, что в июле 2019 года Европейский совет по защите данных (The European Data Protection Board, EDPB) принял проект Руководства по обработке ПД с помощью видеоустройств (Guidelines on processing personal data through video devices) [13]. В нем указано, что видеозапись отдельного лица сама по себе не может рассматриваться как биометрические данные, если она не была специально и технически обработана для содействия идентификации личности (т.е. для распознавания лиц). Обработка биометрических данных представляет собой проблему, если отдельные лица не согласились на получение своих биометрических данных и представлены в отснятом материале.

Еще одна опасность утечки информации может произойти из-за того, что дроны собирают информацию одним из двух способов: записи хранятся на борту (например, на карте памяти или жестком диске) либо передаются обратно на центральное устройство, где они затем сохраняются. Оба метода имеют уязвимости. Если дрон с бортовым хранилищем данных будет потерян или захвачен несанкционированным третьим лицом, то же самое будет и с информацией, которую он несет. Если дрон передает информацию через беспроводное соединение, это соединение можно перехватить и использовать для доступа или изменения информации при передаче. Для устранения этих уязвимостей следует использовать адекватные меры защиты, такие как защита паролем и шифрование.

Таким образом, можно отметить, что системы видеонаблюдения представляют угрозу для ПД. Поэтому при реализации этих систем наряду с основными требованиями следует учесть и приведенные выше рекомендации по защите ПД.

ЗАКЛЮЧЕНИЕ

Системы видеонаблюдения, интегрированные с другими системами безопасности и разработанные с использованием высококачественных и надежных средств, могут снизить риски в потенциально критических областях, в том числе и в НГК. Возросшие потоки ПД сделали актуальной защиту чувствительной информации в них, в решении которой должны быть задействованы как программно-технические средства, так и нормативно-правовые документы. При осуществлении видеонаблюдения должны быть приняты меры, рекомендованные ЕС и законами страны.

БЛАГОДАРНОСТИ

Данная работа выполнена при финансовой поддержке Фонда науки Государственной нефтяной компании Азербайджана SOCAR- **Контракт № 03 LR-AMEA.**

ЛИТЕРАТУРА

- [1] Y. Lu, “Industry 4.0: A survey on technologies, applications and open research issues,” *Journal of Industrial Information Integration*, no. 6, pp. 1-10, 2017.
- [2] Y. Shiraishi, “History of Home Videotape Recorder Development,” *SMPTE Journal*, vol. 94, no. 12, pp. 1257-1263, dec. 1985.
- [3] How many CCTV cameras in London? 2017/10/16. <https://www.caughtoncamera.net/news/how-many-cctv-cameras-in-london/>
- [4] R. M. Alguliyev, T. Kh. Fataliyev, Sh. A. Mehdiyev, “The industrial internet of things: the evolution of automation in the oil and gas complex,” *SOCAR Proceedings*, no. 2, pp. 66-71, 2019.
- [5] IP CCTV Solutions. <https://www.rolloos.com/media/2224/201702-rolloos-campro-ip-cctv-solutions.pdf>.
- [6] G. Sharma, “How Industry 4.0 is Reshaping Oil and Gas Recruitment”. 2019/02/19. https://www.rigzone.com/news/how_industry_40_is_reshaping_oil_and_gas_recruitment-19-feb-2019-158187-article/
- [7] Ш. Мехтиев, А. Мехтиев, “Некоторые вопросы безопасности применения дронов,” 4-я Республиканская конференция по информационной безопасности, сс. 91-94, 2018.
- [8] The Kepler I is the new range of Tattile smart cameras based on embedded artificial intelligence (AI). <https://www.tattile.com/vision-solutions/kepler/>
- [9] Р. Алгулиев, Т. Фаталиев, Б. Агаев и Т. Алиев, “Сенсорные сети: состояние, решения и перспективы,” *Телекоммуникации*, № 4, сс. 27-33, 2007.
- [10] General Data Protection Regulation (GDPR). <https://gdpr-info.eu/>.
- [11] Под наблюдением умной камеры. <https://rspectr.com/articles/497/pod-nablyudeniem-umnoj-kamery>
- [12] К. Саареп, Камеры на рабочих местах часто используются для неправильных целей. <https://www.tooelu.ee/ru/Novosti&nID=2029>
- [13] GDPR Update — EDPB video surveillance guidelines. <https://dentons.boekel.com/en/insights/alerts/2019/september/3/gdpr-update-edpb-video-surveillance-guidelines>

VIDEO SURVEILLANCE SYSTEMS IN THE OIL AND GAS COMPLEX: INDUSTRIAL SAFETY AND PERSONAL DATA PROTECTION

Shakir Mehdiyev¹, Tahmasib Fataliyev², Ayaz Mehdiyev³

^{1,2,3}Institute of Information Technology of ANAS, Baku, Azerbaijan

^{1,3}depart11@iit.science.az, ²depart3@iit.science.az

Abstract— The fourth industrial revolution, or Industry 4.0, made dramatic changes in the field of critical systems, including the oil and gas complex. The oil and gas complex has an extensive and expensive infrastructure of facilities for the production, storage and delivery of final products. Ensuring the safety of these facilities is a complex task, since any violations in the process chain caused by both technical reasons and deliberate attempts to cause damage or theft of equipment cause significant financial damage. The risks to the life and health of the personnel of these enterprises and the environmental risks to the environment also increase. However, solving common problems of security and reliability, video surveillance systems simultaneously create the problem of protecting personal data, which are fundamental factors of universal human rights. The article discusses the problems of using video surveillance systems in the oil and gas complex, implemented on the basis of the Industry 4.0 concept, and offers recommendations for protecting personal data.

Keywords— *Industry 4.0; oil and gas complex; risks; video surveillance; personal data*

Korporativ elektron poçt sistemində təhlükəsizlik məsələləri

Rəşid Ələkbərov¹, Səməd Dursunov², Mürsəl Qurbanlı³

^{1,2,3}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹t.direktor_muavini@iit.science.az, ²samed@iit.science.az, ³m.qurbanli@iit.science.az

Xülasə— Məqalədə e-poçt serverlər, onların tarixi, işləmə prinsipi araşdırılmışdır. Mail Exchange serverin işləmə prinsipi, xüsusiyyətləri, digər e-poçt serverlərdən üstün cəhətləri, spamlardan və zərərli viruslardan qorunması üçün lazım olan tədbirlər haqqında geniş məlumat verilmişdir.

Açar sözlər— Mail Exchange; Active Directory; e-poçt protokolları; spam; MX, TLS, OWA, virus

I. GİRİŞ

Elektron poçt (Electronic Mail və ya E-Mail) – hazırkı dövrdə insanlar arasında ən çox yayılmış ünsiyyət növüdür. Bu ünvan bir neçə saniyə ərzində İnternet şəbəkəsinin yerləşdiyi istənilən yerə nəinki mətn, veb-səhifə, hətta məktub halında olan istənilən faylı göndərməyə imkan verir. ABŞ və Avropadan başlayaraq bu rəbətənin adı "e-mail" və ya "email" formasında yazılır.

İlk elektron poçt bir çox texnoloji yeniliklərin başlanğıcı kimi, hərbi və təhlükəsizlik orqanlarının əməkdaşlarının istifadəsi üçün yaradılmışdı. 1960-cı illərin sonlarında hərbi sahə üçün sistemlər inkişaf etdirməyə çalışan Rels Tomlinson ilk olaraq 1971-ci il oktyabr ayında iki kompüter arasında fayl mübadiləsinə həyata keçirmişdir.

Korporativ poçt - xüsusi olaraq şirkət üçün istifadə edilən e-poçtdur. Şəxsi poçtdan əsas fərqi ünvanın özüdür. Adətən, korporativ e-poçt ünvanları aşağıdakı formatda istifadə edilir: *yourname@companyname.com*.

Şirkət üçün korporativ poçtun təşkili üçün bir neçə əsas yol var. Bu və ya digər metodun seçimi həm işin həcmindən, həm də onun əsas xüsusiyyətlərindən və şirkətin poçt qutularına xidmət etmək üçün nə qədər xərcləmək istəyindən və bunun üçün bir büdcə ayırmağından asılıdır.

Gmail, Hotmail və s. e-poçt istifadəçiləri üçün ideal olan bir çox elektron poçt xidmətləri vardır və bu xidmətlər fərdi istifadəçilər tərəfindən pulsuz olaraq verilir. Pulsuz e-poçt xidmətlərindən çox güman ki, faydalanmışıq. Ancaq bir şirkət və ya bir müəssisə üçün, pulsuz xidmətlər göstərən e-poçtlar xoş qarşılanmaya bilər.

Bir nümunə ilə izah edək; şirkətin adının "adatum" olduğunu, domen adınızın "adatum.com" olduğunu fərz edək. Şirkətdən kənar heç kim bu kimi bir elektron poçt hesabından istifadə edə bilməyəcək. Çünki "adatum.com" adı altında

qeydə alınan bir domendir və heç kim tərəfindən istifadə edilə bilməz.

II. KORPORATİV ELEKTRON POÇT SİSTEMİNİN İŞLƏMƏ PRİNSİPİ

Korporativ poçt bir və ya bir qrup elektron poçt qutusudur. Məsələn, *company.com* üçün elektron poçt qutuları yaratmaq mümkündür; *info@company.com*, *sales@company.com* və ya *anna@company.com* və s.

Bir e-poçtun göndərildiyi anda bir mesaj, müştəridən e-poçt alıcıları e-poçt serverinə gədənə qədər sadə bir poçt ötürülməsi protokolu vasitəsilə serverdən serverə ötürülür.

İlk məktubu göndərən bir e-poçt tətbiqi istifadə edərkən mesajla birlikdə alıcının e-poçt ünvanını daxil etməlidir. Bu yerli kompüterlərdə edilməlidir. Bitdikdən və "Göndər" düyməsini sıxdıqdan sonra, e-poçt MTA-ya (Mail Transfer Agent) göndəriləcəkdir. Bu əlaqə SMTP protokolu vasitəsilə həyata keçirilir.

Növbəti addım DNS axtarışdır. Sistem, alıcının müvafiq MTA-nı tapmaq üçün sorğu göndərir. Bu MX qeydinin köməyi ilə ediləcəkdir. DNS zonasında, alıcının domen ünvanında MX (Mail Exchanger) yazısı olacaqdır. Bu bir domenin poçt serverini təyin edən DNS yazısıdır. Beləliklə, DNS axtarışından sonra tələb olunan poçt serverinə alıcının poçt serverinin IP ünvanı ilə cavab verilir.

Növbəti addım mesajı poçt serverləri arasında ötürməkdir. Bu rəbətə üçün SMTP protokolu istifadə olunur (şəkil 1).

Şəkil 1. E-poçt serverinin işləmə prinsipi

İndi bu mesaj MDA vasitəsilə (Mail Delivery Agent) alıcının kompüterinə ötürülür. Daha əvvəl gördüyümüz kimi, burada iki protokoldan istifadə edilə bilər. POP3 istifadə etsək, onda bütün e-poçt kompüterə yüklənir və serverdəki nüsxə silinir. İstifadə olunan protokol IMAP-dırsa, o zaman e-poçt mesajı poçt serverində saxlanılır, ancaq istifadəçi kompüterdəki kimi poçt serverindəki e-poçtları asanlıqla idarə edə bilər. Hər iki protokolu istifadə edərkən fərq budur və e-poçtunuzun çatdırılma qaydası belədir. E-poçtu göndərməkdə bir səhv varsa, e-poçtlar gecikəcəkdir. Hər bir poçt serverində poçt növbəsi var. Bu poçtlar poçt növbəsində gözləyir. Poçt serveri e-poçtu yenidən göndərməyə çalışacaq. E-poçt göndərmə uğurlu bir nəticə verməyincə, poçt serveri geri göndərilən e-poçt mesajını göndərən e-poçt ünvanına göndərə bilər.

III. MICROSOFT EXCHANGE SERVER KORPORATİV ELEKTRON POÇT PROQRAM TƏMİNATININ ÜSTÜNLÜKLƏRİ

Bildiyimiz kimi, günümüzdə mail alış-verişi artıq o qədər ciddi bir həddə gəlib çatıb ki, dünyanın bir çox şirkətlərinin işləri tamamilə mail serverlərdən asılıdır. Çoxsaylı böyük şirkətlər şəbəkəsinin mail axışını təmin etmək üçün mail xidməti göstərən bir çox məhsuldan istifadə edirlər ki, bunların arasında geniş yayılmış mail serverlərdən biri də Microsoft Exchange Server-dir.

Microsoft Exchange Server – məlumat mübadiləsi və birgə iş üçün nəzərdə tutulmuş proqram təminatıdır. İlk versiyası 1993-cü ildə Microsoft şirkəti tərəfindən işlənilib hazırlanıb. Əsas funksiyaları poçt məlumatlarının emalı və göndərilməsi, mobil qurğuların dəstəklənməsi və səsli məlumat sistemləri ilə integrasiya (Exchange 2007 versiyasından başlayaraq), ani məlumat mübadiləsi sistemlərinin dəstəklənməsidir. Exchange server istər Microsoftun əvvəlki Exchange məhsullarından, istərsə də digər vendorların məhsulları ilə müqayisədə imkanlarına və funksionallığına görə çox fərqlənir. Microsoft şirkəti Exchange strukturu buluda daşıyaraq eyni zamanda Exchange Online xidməti də göstərməkdədir.

Microsoft Exchange Server istifadə edən şirkətlər, işçilərinə dünyanın istənilən yerindən elektron poçtlarına daxil olmağa icazə verə bilər. İşçinin ofisdə və ya yolda olmasından asılı olmayaraq, bütün vacib sənədlərini əldə edə və hər an vacib bir sorğuya bildirişlə cavab verə bilər. Microsoft Exchange Server tərəfindən istifadə olunan e-poçt platforması, e-poçt və əlaqə idarəçiliyini sadə və problemsiz etmək üçün hazırlanmış bir çox fərqli xüsusiyyətlərə malik Microsoft Office Outlook-dur. Microsoft Office Outlook və Microsoft Exchange Server ilə birlikdə istifadə edilə bilən bəzi xüsusiyyətlərə təqvim xüsusiyyətləri, planlaşdırma xüsusiyyətləri, səs poçtu saxlama və əlaqə idarəetmə proqramları daxildir.

Dünya üzrə istifadə olunan bir necə poçt serverləri mövcuddur (şəkil 2). Bunlara aşağıdakıları göstərmək olar:

- Microsoft Exchange Server;
- Sendmail;

- Kerio MailServer;
- IBM Lotus;
- Postfix;
- Qmail;
- Communigate Pro.

Şəkil 2. Müxtəlif ölçülü şirkətlərdə E-poçt serverlərinin istifadə diaqramı

Exchange Serverin yerinə yetirdiyi funksiyalar aşağıdakılardır:

- e-poçt və sənədlərin paylaşımı;
- mərkəzi əlaqə trafikinin yaradılması;
- təhlükəsiz məlumatların saxlanması və məlumatların ehtiyat sürətinin alınması;
- təqvim və kontaktların yaradılması, idarə edilməsi;
- qaydalar vasitəsilə əməliyyatların avtomatlaşdırılması.

Microsoft Exchange Serverin digər e-poçt serverlərindən üstün cəhətləri vardır:

1. Poçt hesabına istənilən yerdən Outlook Web Access (OWA) ilə daxilolma imkanı. İnternetin hər hansı bir yerindən elektron poçtlara daxil olmaq imkanı verir. Bundan əlavə, Microsoft Exchange ilə e-poçt, təqvim, ünvan kitabı, kimi digər xüsusiyyətlər serverdə saxlanılır. Bu şəkildə elektron poçtlarda və istifadəçinin bir mərkəzdən bütün poçtlarında məlumatların təhlükəsizliyi təmin edilir.
2. Fayl paylaşımı. Şirkətlər və ya şöbələr üçün ictimai qovluqlar yaratmaq, sənədləri və vacib mesajları bu ictimai qovluqlarda saxlamaq və istifadəçilər ilə paylaşmaq mümkündür. Ümumi bir qovluqda bir e-poçt ünvanı təyin etmək olar. Bu şəkildə, e-poçt ünvanına

təyin edilən elektron poçtlar birbaşa ictimai qovluğa düşəcək və bütün istifadəçilər bu e-poçt barədə məlumatlandırılacaqlar.

3. Vahid ünvan kitabçası. Həmkarlarınız haqqında bütün məlumatları telefon və poçt kontaktlarının sinxronlaşması sayəsində smartfonda saxlamaq mümkündür.
4. Exchange səsli mesaj (Unified Messaging).
İstifadəçilərə səs mesajları və mətn e-poçtlarını birləşdirmək və onları bir-birinə çevirmək imkanı verir.
5. Mobillik. Məkan və zamandan asılı olmayaraq istifadəçilərə daha çox mobil giriş imkanı verir.
6. Arxivləşdirmə xüsusiyyəti. Şəxsi arxivləşdirmə və PST (Personal Storage Table) xidmətinin istifadəçi ilə əlaqəli olması.
7. Active Directory ilə sinxronlaşma. E-poçtun Active Directory ilə sinxronlaşdırılaraq 5 dəqiqə ərzində 1000 poçt qutusu yaradılması imkanı var.
8. Kommunikasiyanın qorunması. Microsoft Exchange-də quraşdırılmış təhlükəsizlik xüsusiyyətləri işgüzar yazışmaların təhlükəsizliyini və mübadilə zamanı məlumatların məxfiliyini təmin edir. Məlumat itkisindən qorunma xüsusiyyətləri, məzmunu ətraflı təhlil etməklə məxfi məlumatları tanımağa və qorumağa imkan verir.
9. Təhlükəsizlik. Spam və viruslardan yüksək keyfiyyətli qorunması (Microsoft Forefront Security).

Microsoft Exchange Server üçün bir neçə anti-spam proqram təminatı vardır:

1. GravityZone Enterprise Security for Exchange antispam və antivirus proqram təminatlarını özündə birləşdirən poçt serverləri üçün olan bir proqram təminatıdır. Məktubların təhlükəsiz şəkildə mübadiləsini təmin edir.
2. Exclaimer Anti spam dünyanın hər yerinə göndərilən spam məktubları təhlil edir və poçt qutularındakı elektron poçtlarla müqayisə edir.

IV. MICROSOFT EXCHANGE SERVER SİSTEMİNDƏ E-POÇTLARIN TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

E-poçt təhlükəsizliyi bir elektron poçt hesabı və ya xidmətin girişi və kontentini təmin etmək üçün istifadə olunan kollektiv tədbirlərə aiddir. Bir şəxsə və ya bir təşkilata bir və ya bir neçə e-poçt ünvanına, hesablarına ümumi girişi qorumağa imkan verir.

E-poçt təhlükəsizliyi, bir e-poçt xidmətinə təmin etmək üçün istifadə olunan, bir çox üsulu əhatə edən geniş bir termindir. Fərdi istifadəçi nöqtəyi-nəzərindən e-poçt təhlükəsizlik tədbirlərinə daxildir:

- Mürəkkəb şifr;
- Spam filtrləri;

- Anti-virus və anti-spam tətbiqləri.

Analoji olaraq, xidmət provayderi e-poçt serverində mürəkkəb şifr və giriş nəzarət mexanizmlərindən istifadə edərək e-poçt təhlükəsizliyini təmin edir. O, həmçinin istifadəsiz, etibarsız və zərərli e-poçt mesajlarını istifadəçinin poçt qutusuna çatdırılmasını məhdudlaşdırmaq üçün şəbəkə ekranı və proqram əsaslı spam filtrləmə tətbiqlərini də tətbiq edir.

Bir çox kiçik müəssisələr işçilərinin elektron poçtlarını, təqvimlərini və ünvan kitablarını idarə etmək üçün Microsoft Exchange serveri işə salırlar. Exchange sisteminin administratorunun fərqli server parametrlərini konfigurasiya etmək və Exchange tətbiqetmənin təhlükəsizliyinə nəzarət etmək imkanı var. Exchange serverin təhlükəsizliyini artırmaq üçün SMTP protokoluna giriş idarəetməsini məhdudlaşdırmaqlı və hesab məlumatları üçün TLS (Transport Layer Security) şifrələməsini tələb edilməlidir.

TLS bir-biri ilə əlaqə quran tətbiqlər arasında təhlükəsiz məlumat ötürülməsini təmin etmək üçün istifadə olunur. TLS təhlükəsizliyə böyük önəm verən etibarlı veb sayt bağlantılarında, sürətli mesajlaşma proqramında, fayl köçürmələrində, müxtəlif proqramlarda, internet tətbiqlərində, VPN (Virtual Private Network) əlaqələrində və hətta VOIP (Voice Over Internet Protocol) bağlantılarında geniş istifadə olunur. TLS həm şifrələmə, həm də avtorizasiya protokoldur. Bu protokollar serverdən serverə və ya serverdən müştəriyə təhlükəsiz məlumat ötürülməsini təmin edir.

V. AZSCİENCENET ŞƏBƏKƏSİNDƏ KORPORATİV E-POÇT SİSTEMİNİN YARADILMASI VƏ TƏHLÜKƏSİZLİYİ.

AMEA-nın institut və təşkilatların əməkdaşları müxtəlif ölkələrin domen sistemlərində yerləşən e-poçt sistemlərindən geniş istifadə edirdilər. Bu e-poçtlar aşağıdakı problemlərə səbəb olurdu:

- Qeyri-rəsmi e-poçt ünvanları vizual identifikasiya oluna bilmir;
- Rəsmi e-sənədlər yayılarkən digər e-poçt serverləri tərəfindən onlar spam kimi tanındığından ünvanlara yetişmir;
- Qeyri-rəsmi e-poçt ünvanları üzrə məsuliyyətin kimin üzərində olmasını müəyyən etmək çətinləşir;
- Qeyri-rəsmi e-poçt ünvanları AzScienceNet şəbəkəsindən kənarda olduğu üçün İnternet trafikdən istifadənin səmərəsini azaldır;
- AzScienceNet şəbəkəsi mühitində spammlar və viruslarla mübarizə siyasətini həyata keçirmək mümkün olmur;
- Qeyri-rəsmi e-poçt ünvanlarına mənsub olan elmi müəssisə və təşkilatların sənədlərinin kənardan izlənilməsi və analizinə imkan verir;
- AMEA üzrə informasiya təhlükəsizliyi siyasətinin həyata keçirilməsinə müəyyən təhlükələr yaranır.

AMEA Rəyasət Heyətinin 27 fevral 2014-cü il tarixli qərarında aşağıdakılar tələb olunur:

- AMEA üzrə bütün qurumlar və məsul şəxslər rəsmi e-poçt ünvanlarından istifadə etməlidirlər
- Rəsmi e-poçt ünvanları üzrə məsul şəxslər təyin olunmalıdır.
- AMEA üzrə e-sənədlərin mübadiləsi və yayılması rəsmi e-poçt ünvanları vasitəsi ilə həyata keçirilməlidir.
- İnformasiya təhlükəsizliyi siyasətinin tələblərinə müvafiq AzScienceNet şəbəkəsinin e-poçt xidmətinin fəaliyyəti gücləndirilməlidir.
- Rəsmi e-poçt ünvanları üzrə məsul şəxslərlə müvafiq təlimatlandırma işləri aparılmalıdır.

Yuxarıda göstərilən qərara əsasən AzScienceNet şəbəkəsinin verilənləri emal mərkəzinin e-poçt xidməti üçün Microsoft Exchange Server quraşdırılmış və işə salınmışdır.

AMEA üzrə rəsmi elektron poçt ünvanları sisteminin yaradılması məqsədilə AzScienceNet şəbəkəsinin verilənləri emal mərkəzində e-poçt xidməti üçün Mail-server quraşdırılmış və işə salınmışdır. Mail-server AzScienceNet şəbəkəsinin istifadəçilərinə xidmət edir. Mail-serverdə istifadəçilərə poçt qutuları yaratmaq, dəyişikliklər etmək üçün CommuniGate Pro proqram təminatı quraşdırılmışdır. 2017-ci ilin əvvəllərində isə Mail-serverdə təkmilləşdirmə işləri aparılmışdır və @ab.az domen adı @science.az domeni ilə əvəz olunmuşdur. AzScienceNet şəbəkəsinin xidmətlərindən istifadə edən AMEA-nın institut və təşkilatlarının sayı 46-dir. 6500-dən çox fərdi kompüter AzScienceNet şəbəkəsinə qoşulub. Hazırda e-poçt xidmətindən yararlanan istifadəçilərin sayı isə 1830-dür. Onların hər birinə Mail-serverdən 1Gbayt həcmdə yaddaş poçt qutusu yeri ayrılmışdır.

AzScienceNet-ə qoşulan hər bir abonent işlədiyi institut və təşkilatın adına uyğun domenlərlə identifikasiya olunmuşdur. Məsələn, *depart1@iit.science.az* - İnformasiya Texnologiyaları institutunun 1-ci şöbəsi, *depart2@physics.science.az* – Fizika İnstitutunun 2-ci şöbəsi, *depart3@economy.science.az* – İqtisadiyyat İnstitutunun 3 sayılı şöbəsi və s. Bu cür identifikasiya olunmuş domen adlar AMEA institut və təşkilatlarının arzu və təklifləri əsasında yaradılmışdır.

AzScienceNet-in Mail-serverində hər bir istifadəçinin poçt qutusundan məktublara 30 Mbayt həcmli müxtəlif tipli fayllar (mətnlər, şəkillər, audio və videolar) qoşaraq göndərmək olur. Hazırda AzScienceNet şəbəkəsində Milli Elmlər Akademiyasının hər bir istifadəçisi üçün ödənişsiz poçt xidməti göstərilir. 2017-ci ildə poçt serverdə təhlükəsizliyi təmin edilməsi və keyfiyyət göstəricisinin yüksəldilməsi üçün Windows Server 2016 və Microsoft Exchange Server 2016 Standart UsrCAL lisenziyalı proqram təminatı quraşdırılmışdır.

NƏTİCƏ

Məqalədə elektron poçt serverlərinin işləmə prinsipi haqqında geniş məlumat verilmişdir. E-poçt serverlərinin təhlükəsizliyi qeyd edilmişdir. TLS protokolu və onun işləmə prinsipi göstərilmişdir. Microsoft şirkətinin məhsulu olan Microsoft Exchange Server proqram təminatının üstünlükləri və əsas funksiyaları göstərilmişdir. Eyni zamanda qeyd edilən proqram təminatının e-poçt sistemində istifadəçilərin məlumatlarının təhlükəsizliyinin qorunması məsələləri analiz edilmişdir. Qeyd edilən proqram təminatı əsasında AzscienceNet şəbəkəsində korporativ e-poçt sistemi yaradılmış və istifadəyə verilmişdir.

İSTİNADLAR

- [1] P. Craig "The Technical Development of Internet Email" IEEE Annals of the History of Computing, 2008, 250 p.
- [2] R.W. Stanek, Exchange Server Pocket Consultant: Configuration & Clients, Microsoft Press; 1 edison, 378 p, 2013.
- [3] R. Morimoto, M. Noel, G. Yardeni, C. Amaris, A. Abbate, Microsoft Exchange Server 2013, Sams Publishing; 1 edition, 936 p, 2012.
- [4] G. Blokdyk, Anti-spam and Email Security A Complete Guide, SSTARCOoks Publishing, 288 p, 2018.
- [5] D. Cassens. "Law Firm's Automatic Deletion of Spam Emails Is Blamed for Failure to File Timely Appeal." ABA Journal, 325 p, 2017.
- [6] P. Craig, BBN Technologies, "The Technical Development of Internet Email", pp 3-29, 2008.
- [7] W. Shmied, K. Miller Microsoft Exchange Server 2007, John Wiley & Sons Ltd Publishing, 696 p, 2007
- [8] M. Tracy, W. Jansen, K. Scarfone, J. Butterfield Guidelines on Electronic Mail Security 154 p, 2007.
- [9] S. Furnell, P. Dowland E-mail Security ITGP Publishing; 1 edition, 350 p, 2010.
- [10] D.Elfassy Mastering Exchange Server, 818p, 2013

SECURITY ISSUES IN CORPORATE EMAIL SYSTEM

Rashid Alekberov¹, Samad Dursunov², Mursal Gurbanli³

^{1, 2, 3}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹*t.direktor_muavini@iit.science.az* ²*samed@iit.science.az*,
³*m.qurbanli@iit.science.az*

Abstract— The article explores email servers, their history, and how they work. There is detailed information about the principles of Mail Exchange server operation, features, advantages of other e-mail servers, and necessary measures for protection against spam and malware.

Keywords— Mail Exchange, Active Directory, email protocols, MX, TLS, OWA, virus

Buludlarda fərdi məlumatların konfidensiallığına yönəlmiş hücumlar və müdafiə mexanizmləri

Fərzanə Abdullayeva

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
a_farqana@mail.ru

Xülasə— Bulud texnologiyalarının təhlükəsizliyi buludda saxlanan verilənlərin konfidensiallığının pozulması ilə sıx əlaqədardır. Bulud texnologiyalarının heterogenlik, resursların paylaşılması, çoxicarəçilik, virtuallaşma, mobil bulud texnologiyaları, servis səviyyəsi müqaviləsi kimi xarakteristikaları bulud texnologiyalarında çoxsaylı boşluqlar yaradır. Məqalədə buludlarda saxlanan fərdi məlumatların konfidensiallığının pozulmasına yönəlmiş hücumlar və onların qarşısının alınması üsulları analiz olunur, bu hücumların bulud texnologiyalarının müxtəlif təhlükəsizlik aspektlərinə təsiri və qarşıdurma tədbirlərinin qarşılıqlı əlaqə modeli təklif olunur.

Açar sözlər— bulud texnologiyaları; fərdi məlumatlar; konfidensiallıq hücumları; anonimləşdirmə; verilənlərin manipulyasiyası hücumu

I. GİRİŞ

Bulud texnologiyaları bulud istifadəçilərinə paylaşılan hesablama resursları toplusuna giriş imkanı verən arxitekturaadır. Son illər Big Data, IoT, 5G, SDN və NFV əsaslı bulud proqram təbiiqlərinin meydana gəlməsi ilə bulud texnologiyalarındakı sürətli inkişaf istifadəçilərin bulud texnologiyalarına miqrasiyasını artırmışdır [1]. Lakin bulud texnologiyalarının arxitekturası təhlükəsizliyi hədəfə almadan layihələndirildiyi üçün buluda olan təhlükəsizlik insidentlərinin sayı hər il böyük sürətlə artmaqda davam edir. Bu gün bulud xidmətləri təqdim edən nəhəng servis provayderləri olan Amazon, Google, Microsoft və s. böyük həcmdə təhlükəsizlik insidentləri ilə qarşılaşırlar. Bu provayderlərin infrastrukturlarının statistik qiymətləndirilməsi zamanı 2009-cu illə müqayisədə 2011-ci ildə bulud insidentlərinin sayı iki dəfə artaraq 33 insidentdən 71 insidentə qədər yüksəlmişdir [2].

Bulud texnologiyaları bulud servis provayderlərini və istifadəçilərinə bir sıra təhlükəsizlik təhdidləri ilə üz-üzə qoyur. Bu təhlükəsizlik təhdidlərinin növlərinin sayı böyük sürətlə artır [3]. Burada bu təhdidləri reallaşdıran hücumların təbiəti fərqlidir. Onlar həm bulud provayderlərini, həm də istifadəçiləri hədəfə ala bilirlər. Bu səbəbdən bulud sisteminin özü və istifadəçiləri üçün təhlükəsizlik başlıca problemlərdən biri hesab olunur.

2016-cı ildə Bulud Təhlükəsizlik Alyansının (Cloud Security Alliance, CSA) bulud texnologiyaları üçün müəyyən etdiyi xarakterik 12 təhdid növü sırasında [3] verilənlərin pozulması (ing., data breach) başlıca mövqelərdən birini tutur.

Generasiya, ötürülmə, istifadə, paylaşılma, saxlanma, arxivləşdirmə, ləğv edilmə verilənlərin həyat tsiklinin mərhələlərini təşkil edir [4]. Verilənlərin təhlükəsizliyi həyat tsiklinin hər bir mərhələsində təmin edilməlidir.

Bulud texnologiyalarının təhlükəsizlik məsələlərinin analizinə həsr olunmuş çox sayda tədqiqatlar aparılmışdır. [5]-də bulud texnologiyalarının kommunikasiya, hesablama və servis səviyyəsi laylarında təhlükəsizlik məsələlərinin analizi aparılmışdır. Verilənlərlə bağlı təhlükəsizlik məsələlərinin analizində verilənlərin təhlükəsizlik məsələləri ötürülən verilənlərin təhlükəsizliyi və saxlanan verilənlərin təhlükəsizliyi kimi iki qrupa bölünür. Burada verilənlərin konfidensiallığının təmin edilməsi məsələsinə yetərli diqqət ayrılmır, problemlər ümumi təsvir olunur. [6]-də bulud texnologiyalarının müxtəlif modellərinin verilənlərin pozulması ilə bağlı problemləri analiz olunur. [7]-də verilənlərin təhlükəsizliyinin CIA (Confidentiality, Integrity, Availability) triadası baxımından analizi aparılır. CIA-triadası məşhur olduğuna baxmayaraq, bu triada bulud kimi dinamik mühitdə meydana çıxan yeni növ təhdidləri nəzərə ala bilmir [8]. Bu problemi aradan qaldırmaq üçün IAS-OCTAVE (Information, Assurance, Security) adı ilə tanınan kompleks təhlükəsizlik aspektləri siyahısı təklif edilmişdir [8]. Bu siyahıya görə hesabatlılıq, audit, autentiklik/etibarlılıq, əlçatanlıq, konfidensiallıq, tamlıq, inkar edilməzlik, məxfilik bulud texnologiyalarının informasiya təhlükəsizliyi aspektləri hesab olunur.

Məqalədə bulud texnologiyalarının çoxicarəçilik mühitində fərdi məlumatlarla bağlı təhlükəsizlik məsələləri analiz olunur, bu təhlükəsizlik problemlərinin aradan qaldırılması üçün mövcud metodlar təsvir olunur. Fərdi məlumatlara olan hücumların bulud texnologiyalarının müxtəlif təhlükəsizlik aspektlərinə təsiri və qarşıdurma tədbirlərinin qarşılıqlı əlaqə modeli təklif olunur.

II. BULUD TEXNOLOGİYALARININ ƏSAS XARAKTERİSTİKALARI

Bulud texnologiyaları termini ilk dəfə 2006-cı ilin sonlarında Google şirkətinin icraçı direktoru Erik Şmid tərəfindən təklif edilmişdir.

Hazırda bulud texnologiyaları dördüncü sənaye inqilabının əsas komponentləri siyahısına daxil edilmişdir və qabaqcıl dünya dövlətlərində ən innovativ texnologiya hesab olunur [9].

Bulud texnologiyaları verilənlər mərkəzinin resurslarını virtuallaşma texnologiyalarından istifadə etməklə paylaşan, o cümlədən müştərilərə elastik, tələbata uyğun, və ani servislər təqdim edən və istifadəçinin servis sərfiyyatını kommunal ödəniş kimi qiymətləndirən sistemdir [10].

Bulud texnologiyalarının əsas xarakteristikaları aşağıdakılardır [11, 12]:

- *Ölçülən servis* istifadəçiyə göstərilən servisin pul şəklində qiymətləndirilməsidir.
- *Ani elastiklik* resursların miqdarını çevik şəkildə artırıb-azaltmaq imkanının olmasıdır.
- *Sorğuya görə özünə xidmət* istifadəçinin bulud servisləri ilə sərbəst işləmək bacarığını göstərir.
- *Şəbəkəyə geniş giriş imkanı* buluda girişin təşkili istənilən məkandan, istənilən vaxt, istənilən qurğu vasitəsilə mümkün olmalıdır.
- *Resurslar toplusu* yaddaş, prosessor, hesablama resursları, şəbəkə resursları toplusudur.
- *Miqyaslaşma* resursların artımını idarə etmək imkanının olması.
- *Çoxicarəçilik* ayrı-ayrı müştərilərin seqmentləşdirilməsi, izolyasiyası, idarəetmə siyasətinin olmasının zəruriliyini göstərir.

III. BULUD TEXNOLOGİYALARININ TƏHLÜKƏSİZLİK STANDARTLARI

Bulud texnologiyalarının artıq bir çox yerlərdə tətbiq olunmağa başlaması bu sahədə çoxsaylı bulud standartlarının yaradılmasını zəruri etmişdir.

Provayder təşkilatlarında müvafiq idarəetmənin olduğunu ISO 2700X standartları seriyası vasitəsi ilə müəyyən edirlər. Bu standart aşağıdakıları müəyyən etməyə imkan verir:

- paylaşılan, çoxicarəçilik mühitdə müştərinin proqramlarının və verilənlərinin izolyasiya olunduğuna zəmanət;
- müştərinin aktivlərinin provayderin işçi heyəti tərəfindən icazəsiz girişdən qorunması;
- müştərinin aktivlərinin müştərinin işçiləri və ya partnyorları tərəfindən qəsdli və ya təsadüfi girişdən qorunması.

ISO təşkilatı ISO/IEC 27002 standartının üzərində bulud hesablama texnologiyaları üçün spesifik olan ISO/IEC 27017 standartını hazırlamışdır [13]. Bundan əlavə ISO/IEC 27001 standartının üzərində bulud xidmətlərinin təhlükəsizliyi və ümumi buludda fərdi məlumatların qorunması qaydalarını əks etdirən ISO/IEC 27018 standartını hazırlamışdır [14]. ISO/IEC 27036-4 bulud xidmətlərinin tətbiqi ilə bağlı spesifik informasiya təhlükəsizliyi riskləri və onların effektiv idarə edilməsi haqqında təlimat təqdim edir [15].

“ISO/IEC 19086 Cloud computing - Service level agreement (SLA) framework” fərdi məlumatların qorunması və təhlükəsizliyi qaydalarını müəyyən edir [16]. ISO/IEC 19086 (Part 4) buludun servis səviyyəsi haqqında müqavilələrinin təhlükəsizliyi və gizliliyi komponentləri ilə bağlı məsələləri əhatə edir [17]. ISO/IEC 27034 proqram tətbiqlərinin təhlükəsizliyi haqqında ümumi məlumat verilir. Proqram tətbiqlərinin təhlükəsizliyi ilə bağlı əsas anlayışlar, konsepsiyalar, prinsiplər və proseslər təsvir olunur. Bu standart layihələndirilən bütün növ infrastrukturlar üçün nəzərdə tutulmuş proqram tətbiqlərində istifadə oluna bilər [18]. NIST Special Publication 800-53 federal informasiya sistemlərinin təhlükəsizliyinin və gizliliyinin təmin edilməsi qaydalarını müəyyən edir [19].

Layihəçiləri təlimləndirmək məqsədi ilə OWASP-ın (Open Web Application Security Project) “OWASP Secure Coding Practices” adlı təhlükəsiz kodlaşdırma vərdişləri üçün təlimatları vardır [20]. Buludlarda fərdi məlumatların qorunmasına ITU (International Telecommunication Union) təşkilatı da böyük diqqət ayırır. Bu məqsədlə təşkilat “Privacy in Cloud Computing” adlı texniki sənəd dərc etdirmişdir [21]. Sənəddə buludlarda fərdi məlumatların konfidensiallığının pozulması risklərinin aradan qaldırılması üçün müxtəlif standartlaşdırma təşkilatları tərəfindən işlənəcək standartların problemləri analiz olunur. Bulud xidmətlərində fərdi məlumatların emalı ilə bağlı davranış kodeksləri vardır. Buna misal olaraq Avropa Birliyinin Bulud Davranış Kodeksini (EU Cloud Code of Conduct) misal göstərmək olar.

IV. BULUD TEXNOLOGİYALARININ İNFORMASIYA TƏHLÜKƏSİZLİYİ

İnformasiya təhlükəsizliyi informasiyanın və informasiya sisteminin icazəsiz girişdən, istifadədən, açıqlanmasından, pozulmasından, modifikasiya olunmasından, yoxlanmasından, yazılmasından, ləğv edilməsindən qorunmasıdır. CSA (Cloud Security Alliance) təşkilatının tədqiqatlarına görə bulud texnologiyalarının tətbiqi zamanı təşkilatlar aşağıdakı 12 təhdidlə qarşılaşa bilərlər [3]: verilənlərin pozulması, zəif identifikator, girişin və hesab verilənlərinin idarə edilməsi, mühafizəsis tətbiqi proqram interfeysləri, sistem və proqram tətbiqləri boşluqları, hesabın ələ keçirilməsi, zərərli insayderlər, təkmil davamlı hücumlar, verilənlərin itməsi, müvafiq araşdırmanın olmaması, bulud servislərindən ədalətsiz və sui-istifadə, xidmətdən imtina, paylaşılan texnologiya problemləri. Bundan əlavə bulud texnologiyaları üçün servislərin kənar mənbələrdən cəlb edilməsi, normativ qaydalara uyğunluq, verilənlərin yerləşmə məkanı, paylaşılan mühit, biznesin davamlılığı, qəza vəziyyətlərinin bərpası, qanunsuz fəaliyyətin təhqiqatı üçün çətin mühit, və uzun müddətli canlılıq kimi risklər də müəyyən edilmişdir [22].

Yuxarıda sadalanan təhdidlərin hamısı buludun resursları paylaşmaq və çoxicarəçilik xüsusiyyətinin olması səbəbindən baş verir və bu xüsusiyyətlər verilənlərin konfidensiallığının pozulmasına səbəb olan başlıca təhdidlərdir [23, 24].

V. BULUDLARDA İNFORMASIYANIN KONFİDENSİALLIĞININ POZULMASI

Buludlarda konfidensiallığın pozulmasına səbəb olan amillərdən biri buludların aparat təminatının ayrılmasının yetərli dərəcədə təmin edilməməsidir [25]. Buludda verilənlərin qalıcılığı (ing., data remanance) əlamətindən istifadə etməklə də konfidensiallığın pozulması halları baş verir. Burada müştəri bulud provayderindən yaddaş fəzası əldə edərək başqa müştərilərin həssas verilənlərini skanlama vasitəsi ilə axtarmaqla əldə edə bilər. Verilənlər üzərində idarəetmənin (ing., data governance) üçüncü tərəf buluda həvalə edilməsi də verilənlərin ələ keçirilməsi riskini artırır. Burada kənardan cəlb edilmiş servislər (bulud provayderi) müştərinin fərdi, məntiqi və fiziki təhlükəsizliyinin idarə edilməsi səlahiyyətlərini ələ keçirir.

Fərdi məlumatların konfidensiallığı şəxsin özü haqqında verilənlərin saxlandığından məlumatlı olmaq, bu məlumatların necə əlaqələndirildiyinə nəzarət etmək və bu məlumatlardan sui-istifadənin qarşısını almaq səlahiyyətinin olduğu deməkdir. Fərdi informasiyanın qorunması gizliliyə hüququn olması kimi təyin edilir. Hər bir şəxs tipindən asılı olmadan, gizli, açıq və ya peşəkar verilənlərini idarə etmək hüququna malikdir [21]. Bulud istifadəçilərinin buluda miqrasiya zamanı idarəetmə səlahiyyətini itirməsi verilənlərin tamlığı, konfidensiallığı və gizliliyi prinsiplərinə ciddi təhdid yaradır.

VI. BULUD SİSTEMİNİN BOŞLUQLARI

Hər bir bulud sistemi üç əsas komponentdən ibarətdir [26]: şəbəkə; hipervizor; aparat təminatı. Şəkil 1-də bulud sistemi və onun hücum nöqtələri təsvir olunmuşdur.

Koppalino bu sistemlərə xas olan üç hücum nöqtəsi müəyyən etmişdir [26]:

- *Bulud infrastrukturuna şəbəkə vasitəsi ilə hücumların daxil edilməsi.* Hücumlar xaricdən olan istifadəçilər vasitəsi ilə həyata keçirilir, onlar rabitə kanallarına təsir göstərməklə verilənlərin konfidensiallığını və tamlığını, bulud provayderinin verilənlər mərkəzinin əlçatanlığını pozmağa cəhd edirlər.
- *Hipervizordan istifadə etməklə digər virtual maşınlara hücumların edilməsi.* Hücumlar daxili istifadəçilər (virtual maşın (VM) sahibləri) tərəfindən edilir. Bu hücumun baş verməsinə başlıca səbəb buludun çoxicarəçilik xarakteristikasıdır (hücumçu və hədəf obyektin eyni hostda yerləşməsi faktı). Buludun bu komponentinə olan hücum müxtəlif proqram tətbiqləri arasında izolyasiyanın zəif qurulması səbəbindən baş verə bilər. Bu hücum həssas informasiyanın konfidensiallığının pozulmasına səbəb olur. Bu hücum növünü ənənəvi şəbəkə hücumlarının qarşısının alınması mexanizmləri vasitəsi ilə aradan qaldırmaq mümkün olmur.
- *Provayderin özünün hücumlar həyata keçirməsi.* İşçi heyətin aparat platformasında fiziki və ya məntiqi dəyişiklik etməklə istifadəçilərin həssas informasiyanı ələ keçirməsidir.

Şəkil 1. Bulud sisteminin hücum nöqtələri

VII. BULUDLARDA HÜCUM SSSENARİLƏRİ

Buludlarda çoxicarəçilik riskinin unikallığı odur ki, burada hücumçular və hücum obyekti eyni serveri (fiziki maşın) paylaşaraq istifadə edir [23]. Belə hücum ənənəvi təhlükəsizlik mexanizmləri vasitəsi ilə aradan qaldırıla bilmir, çünki ənənəvi mexanizmlər serverin daxilinə nüfuz edə bilmir, və onların (ənənəvi mexanizmlər) monitoring üsulları yalnız şəbəkə layı üçün layihələndirilmişdir. Hücumçu və hücum obyektinin müxtəlif yerləşmə ssenariləri şəkil 2-də təsvir edilmişdir.

Şəkil 2. Ənənəvi şəbəkələşmə ilə bulud şəbəkələşməsi arasında fərq

Birinci halda hücumçu və hücum obyekti adi internet istifadəçiləridir. Bu tip hücumların qarşısının alınması üçün ənənəvi şəbəkə təhlükəsizliyi mexanizmləri yetərli hesab olunur. İkinci halda hücumçu və hücum obyekti eyni bulud provayderinin müştəriləridir, lakin onların hər biri ayrı-ayrı serverlərdə yerləşirlər. Bu struktur bulud texnologiyaları modelindəki virtuallaşmanın köməyi ilə qurula bilər. Bu tip strukturun təhlükəsizliyinin təmin edilməsi üçün bulud provayderi tərəfindən virtual şəbəkə təhlükəsizliyi mexanizmlərinin istifadə edilməsi lazım gəlir. Üçüncü halda hücumçu və hücum obyekti hər ikisi eyni buludun müştəriləridir və eyni serveri paylaşaraq istifadə edir. Bu hal buludun çoxicarəçilik xarakteristikasına görə yaradıla bilər. Burada hücumçunun virtual maşını ilə hücum obyektinin virtual maşını arasında şəbəkə kommunikasiyası bir fiziki maşının daxilində yaranır və onun mühafizə edilməsi sadə məsələ hesab olunur. Burada trafik fiziki maşından kənara çıxmıdığı üçün bu şəbəkəni ikinci halda olduğu kimi virtual

şəbəkə təhlükəsizliyi mexanizmləri vasitəsi ilə aradan qaldırmaq çətin olur.

VIII. BULUDLARDA FƏRDİ MƏLUMATLARIN KONFİDENSİALLIĞINA YÖNƏLMİŞ HÜCUMLARI VƏ MÜDAFİƏ MEXANİZMLƏRİ

Buludlarda fərdi məlumatların konfidensiallığına yönəlmis hücumları, onların bulud texnologiyalarının müxtəlif təhlükəsizlik aspektlərinə təsiri və qarşılıqlı əlaqə modeli şəkil 3-də təsvir edilmişdir.

Şəkil 3. Buludlarda fərdi məlumatların konfidensiallığına yönəlmis hücumlar və müdafiə mexanizmləri

- **Qalıq verilənlərdən sui-istifadə hücumu.** Bu hücum növündə hücumçunun fiziki saxlanıcı tam idarə etmək və ona giriş imkanı olduğu üçün təhlükəsizlik aspektlərinin hamısını birbaşa poza bilər.
- **Əlqəlik hücumu.** Müxtəlif verilənlər mənbələrini ələ keçirmək və dolayı əlaqələndirməklə verilənlərin hissələrlə identifikasiyasını həyata keçirir. Burada hücumçu bulud verilənlərinə birbaşa müdaxilə etmədən ələ keçirilmiş verilənləri manipulyasiya etdiyi üçün bu hücum növü yalnız konfidensiallığın, təhlükəsizliyin və məxfiliyin pozulmasına səbəb olur.
- **Verilənlərin manipulyasiyası hücumu.** İstifadəçilər öz proqram tətbiqi komponentindən serverin proqram tətbiqi komponentinə göndərilən verilənlərdə dəyişikliklər etməklə veb-proqram tətbiqlərinə hücum edir. Başqa sözlə, server komponentinin qəbul etdiyi giriş verilənləri müştərinin daxil etdiyi gözlənilən verilənlər olmur, tam dəyişdirilmiş verilənlər olur. Burada hücumçu bulud verilənlərinə birbaşa müdaxilə edə bildiyi üçün verilənlərin manipulyasiyası hücumu bütün təhlükəsizlik aspektlərini poza bilər.
- **Yan kanal hücumları.** Yan kanal aparat təminatındakı gizli kanaldır. Yan kanal məlumatlarından istifadə edən istənilən növ hücum yan kanal hücumu adlanır. Bu hücum verilənlərin təhlükəsizliyini, konfidensiallığını və məxfiliyini pozur.
- **Xidmətdən imtina.** Bulud servis provayderlərinin xidmət təqdim etmək prosesini dayandıran hücumlardır.

- **Homogenlik hücumları.** Hücumçu dolayı yolla fərdi məlumatları xüsusi identifikatorlara aid edə bilər. Bu hücum verilənlərin təhlükəsizliyini, konfidensiallığını və gizliliyini pozur.
 - **İcazəsiz giriş hücumu.** Müştərilərin verilənləri buludda saxlandıqda onların verilənlər üzərində nəzarət hüququ itir. Bulud texnologiyalarında verilənlər müxtəlif ölkələrdə yerləşmiş çoxsaylı verilənlər mərkəzlərində saxlana bilər. Belə ölkələr verilənlərin sahibindən icazə almadan verilənlərə giriş etmək üçün daha üstün səlahiyyətə malik olur. VM-lərin etibarsız hosta miqrasiyası zamanı hücumçu bulud verilənlərinə icazəsiz giriş əldə edə bilər. Bu zaman hücumçu həmin virtual maşındakı həssas məlumatı açıqlaya bilər. Bu hücum növü informasiya təhlükəsizliyi aspektlərinin hamısını birbaşa poza bilər.
 - **İdentifikasiya hücumu.** Hücumçu bəzi identifikasiya atributlarını (ad, ünvan) müəyyən şəxslə əlaqələndirə bilər. Bu hücum növü yalnız konfidensiallığın, təhlükəsizliyin və məxfiliyin pozulmasına səbəb olur.
 - **Heş toqquşması hücumu.** Hücumçunun məqsədi heş funksiyasının eyni heş qiyməti verən iki giriş simvolunu tapmaqdır.
 - **Ortada adam hücumu.** Subyektlər arasında ötürülən informasiyanın ələ keçirilməsidir.
- Yuxarıda sadalanan hücumların qarşısının alınması üçün müdafiə mexanizmləri kimi aşağıdakılar istifadə edilə bilər:
- **Dublikatın aradan qaldırılması.** Verilənlərin artıq nüsxələrinin sistemdən silinməsi prosesidir.
 - **Təhlükəsiz saxlanma.** Müxtəlif şifrələmə üsullarından istifadə etməklə təhlükəsiz saxlanma qurulmasıdır.
 - **Giriş nəzarəti.** Buludda saxlanan verilənlərə olan girişin idarə edilməsi üsullarıdır.
 - **Verilənlərin bərpası.** İtilmiş verilənlərin bərpası prosesidir.
 - **Anonimləşdirmə üsulları.** Verilənlərin anonimləşdirilməsini həyata keçirmək üçün k-anonymity, l-diversity, t-closeness anonimləşdirmə üsulları istifadə olunur.
 - **Müvəqqəti verilənlərin saxlanması.** Bu tip verilənlər sessiya zamanı yaranan verilənlərdir. Verilənlərin saxlanması üsullarının işlənməsi məsələlərini əhatə edir.
 - **Paylanmış verilənlər repozitoriləri.** Yeni təhlükəsiz saxlanma arxitekturalarının işlənməsidir.
 - **Virtual maşınların introspeksiyası.** Tətbiq proqramının, qonaq əməliyyat sistemlərinin və fiziki serverdə işləyən VM-lərin vəziyyətinin monitorinqi üsullarıdır. Fərdi məlumatların saxlandığı virtual maşınların fəaliyyətini yoxlayır, virtual maşında zərərli proqramı aşkarlayır.

- *Blokçeyn*. Blokçeyn texnologiyasına əsaslanan şifrələnmiş verilənlər saxlanıcı sisteminin qurulması.
- *Monitoring və audit*. Bulud saxlanıcının monitorinqi üçün miqyaslanan paylanmış sistemlərin işlənməsi.
- *Verilənlərin təhlükəsiz miqrasiyası*. Verilənlərin bir bulud saxlanıcısından digərinə köçürülməsi.
- *Qalıq verilənlərin sanitarizasiyası*. Verilənlər həyat tsiklinin sonunda təhlükəsiz qaydada silinməlidir. Ənənəvi sanitarizasiya üsulu kimi üzərindən yazılma (overwriting) istifadə oluna bilər.
- *Verilənlərin izolyasiyası*. Həssas və adi verilənlər arasında bölünmənin olmasını nəzərdə tutur.
- *Verilənlərin seqreqasiyası*. Virtuallaşmış mühitdə bulud istifadəçiləri arasında tam bölünmənin olması.

NƏTİCƏ

Buludlarda saxlanan fərdi məlumatların təhlükəsizliyinin təmin edilməsinin müasir vəziyyəti analiz edilmiş, verilənlərin konfidensiallığına olan hücumlar müəyyənləşdirilmişdir. Bu hücumların aradan qaldırılması üçün bir sıra yanaşmalar təsvir edilmişdir. Müxtəlif istifadəçilərin verilənlərinin bir-birindən ayrılmasını təmin etmək üçün verilənlərin intellektual seqreqasiyası üsullarının işlənməsinin zəruriliyi qeyd edilmişdir. Verilənlərin sızması riskini aradan qaldırmaq üçün saxlanmış verilənlərin şifrələnməsinin vacibliyi göstərilmişdir.

İSTİNADLAR

- [1] “Hosting and cloud computing market size worldwide 2010-2020,” 2018, <https://www.statista.com/statistics/500541/worldwide-hosting-and-cloud-computing-market/>
- [2] “Cloud Computing Vulnerability Incidents: A Statistical Overview,” 2013, 22 p.
- [3] K. Walker, “Cloud security alliance (CSA). The treacherous 12: cloud computing top threats in 2016,” <https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/>.
- [4] D. Chen, H. Zhao, “Data security and privacy protection issues in cloud computing,” In proceedings of the international conference on computer science and electronics engineering, 2012, pp. 647-651.
- [5] S. Nalini, A. Jeyaraj, “Recent security challenges in cloud computing,” Computers and Electrical Engineering, 2018, vol. 71, pp. 28-42.
- [6] R. Barona, E.A. Anita, “A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Threats,” In proceedings of the international conference on circuits power and computing technologies, ICCPCT, 2017, pp. 1-8.
- [7] P.R. Kumar, P.H. Raj, P. Jelciana, “Exploring Data Security Issues and Solutions in Cloud Computing,” Procedia Computer Science, 2018, vol. 125, pp. 691-697.
- [8] Y. Cherdantseva, J. Hilton, “A reference model of information assurance and security,” In proceedings of the International Conference on Availability, Reliability and Security, ARES, 2013, Regensburg, Germany, 2-6 September, pp. 546-555.
- [9] M.H. Onik, C.S. Kim, J. Yang, “Personal Data Privacy Challenges of the Fourth Industrial Revolution,” In proceedings of the international conference on advanced communications technology, (ICACT), 2019, pp. 635-638.
- [10] M.T. Khorshed, A.B. Ali, S.A. Wasimi, “A Survey on gaps, threat remediation challenges and some thoughts for proactive attack detection

- in cloud computing,” Future Generation Computer Systems, 2012, vol. 28, no. 6, pp. 833-851.
- [11] P. Mell, T. Grance, “The NIST definition of cloud computing,” National Institute of Standards and Technology, 2009, 7 p.
 - [12] “Security Guidance for Critical Areas of Focus in Cloud Computing,” 2009, Cloud Security Alliance, V 2.1, 76 p.
 - [13] “ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services,” 2015, <https://www.iso.org/standard/43757.html>
 - [14] “ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors,” First edition 2014, 32 p.
 - [15] “ISO/IEC 27036-4, Information technology - Security techniques - Information security for supplier relationship - Part 4: Guidelines for security of cloud services,” 2016, First edition, 28 p.
 - [16] “ISO/IEC 19086, Cloud computing - Service level agreement (SLA) framework - Part 1: Overview and concepts,” 2016, First edition, 11 p.
 - [17] “ISO/IEC 19086 Cloud computing - Service level agreement (SLA) framework, Part 4, Components of Security and of protection PII,” 2019, 8 p.
 - [18] “ISO/IEC 27034, Information Technology- Security techniques,” Application Security, First edition, 11 p.
 - [19] “NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” Revision 4, 2013, 462 p.
 - [20] “Open Web Application Security Project (OWASP),” <https://www.owasp.org>
 - [21] “Privacy in Cloud Computing,” ITU-T Technology Watch Report March 2012, 26 p.
 - [22] J. Brodtkin, “Gartner: seven cloud-computing security risks,” July 02, 2008, <https://www.infoworld.com/article/2652198/gartner--seven-cloud-computing-security-risks.html>
 - [23] D. Zissis, D. Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems, 2012, vol. 28, no. 3, pp. 583-592.
 - [24] Special Publication 800-144, “Guidelines on Security and Privacy in Public Cloud Computing,” NIST, 2011, 80 p.
 - [25] H. AlJahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, J. Xu, “Multi-Tenancy in Cloud Computing,” In proceedings of the 8th IEEE International Symposium on Service Oriented System Engineering, SOSE, 2014, pp. 344-351.
 - [26] L. Coppolino, S. D’Antonio, G. Mazzeo, L. Romano, “Cloud security: Emerging threats and current solutions,” Computers and Electrical Engineering, 2017, vol. 59, pp. 126-140.

PRIVACY ATTACKS IN CLOUDS AND PREVENTIVE MECHANIZMS

Fargana Abdullayeva

Institute of Information Technology of ANAS, Baku, Azerbaijan

a_fargana@mail.ru

Abstract – Cloud computing security is closely related to the breach of data privacy stored in the cloud. The characteristics of cloud computing such as heterogeneity, resource sharing, multitenancy, virtualization, mobile cloud computing, and service level agreement create numerous vulnerabilities in cloud technologies. In this paper privacy violation attacks to the data stored on the cloud and their preventive methods are analysed, a relational model of the impact of these attacks on the various security aspects of cloud computing and preventive methods is proposed.

Keywords – cloud computing; personal data; privacy attack; anonymization; data manipulation attack

İnternet mühitində fərdi məlumatların təhlükəsizliyinin monitorinqi problemləri

Ramiz Şıxəliyev

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
ramiz@science.az

Xülasə— İnternet mühitində fərdi məlumatların təhlükəsizliyinin monitorinqi şəxsi həyatın toxunulmazlığının təmin edilməsi üçün çox vacib məsələdir. Lakin qlobal İnternet mühitində bu məsələnin həlli çox çətin problemdir. Çünki İnternet istifadəçiləri marketing və elektron kommersiya, sosial media, bulud və s. kimi çoxlu sayda elektron xidmətlərdən və həmçinin mobil İnternet vasitələrindən istifadə edirlər və onların fərdi məlumatları müxtəlif mənbələrdə (xidmətlərdə, bazalarda və s.) yerləşir. Bu mənbələrdə yerləşən fərdi məlumatlara qarşı təhdidlər də müxtəlif olur. Belə bir paylanmış qlobal mühitdə fərdi məlumatların təhlükəsizliyinin monitorinqi üçün vahid bir mexanizmin yaradılması çox çətin məsələdir. Məqalə İnternet mühitində fərdi məlumatların təhlükəsizliyinin monitorinqi problemlərinin analizinə həsr olunmuşdur. Analiz nəticəsində, fərdi məlumatların təhlükəsizliyinin monitorinqi məsələsinin onların yerləşdiyi mənbələrdən asılı olaraq müəyyən edilməsi və intellektual texnologiyaların (multi-agent texnologiyasından) istifadəsi ilə paylanmış monitorinq sisteminin yaradılması məqsəduyğun hesab edilmişdir.

Açar sözlər— fərdi məlumatlar, fərdi məlumatların kateqoriyaları, şəxsi həyatın toxunulmazlığı, fərdi məlumatların təhlükəsizliyinin monitorinqi

I. GİRİŞ

Rəqəmsal texnologiyaların istifadə sahəsinin genişlənməsi dövlət xidmətləri, səhiyyə, ticarət və s. sahələrdə fərdi məlumatların təhlükəsizliyinin təmin edilməsi problemlərinin yaranmasına gətirib çıxarmışdır. Belə ki, bu xidmətlərdən istifadə zamanı istifadəçilər həm könüllü, həm də bilməyərək öz fərdi məlumatlarını daxil edirlər. Bu halda, heç şübhə yoxdur ki, rəqəmsal texnologiyaların istifadəsinin üstünlüyünə baxmayaraq istifadəçilərin şəxsi həyatının toxunulmazlığına təhlükə yaranır. Xüsusilə də istifadəçilər İnternet mühitində elektron xidmətlərdən, sosial şəbəkələrdən istifadə zamanı böyük risklərə məruz qalırlar. Məsələn, istifadəçilər Facebook, Twitter, Instagram, MySpace və s. kimi sosial şəbəkələrdən, bulud xidmətindən, bloqlardan, vakansiyalar üzrə veb-saytlardan, smartfonlardan, elektron ticarətdən və s. istifadə etdikdə öz fərdi məlumatlarını daxil edirlər. Bununla yanaşı, həm dövlət, həm də özəl sektor istifadəçilərin fərdi məlumatlarından öz məqsədləri üçün istifadə edirlər və çox zaman bu məlumatlar insanların xəbəri olmadan toplanır. Bununla da istifadəçinin fərdi məlumatlarının yeni bir ekosistemi meydana çıxır. Təbii ki,

istifadə edilən rəqəmsal texnologiyaların və xidmətlərin sayı artdıqca istifadəçilər öz fərdi məlumatları üzərindəki nəzarəti demək olar ki itirirlər.

Bu gün fərdi məlumatların təhlükəsizliyinin təmin edilməsinin mexanizmlərinin olmaması fərdi məlumatların təhlükəsizliyinin tez-tez pozulmasına səbəb olur. Çox zaman fərdi məlumatların təhlükəsizliyinin pozulması hallarının müəyyən edilməsi mümkün olmur. Buna görə də, elektron xidmətlər yaradılarkən və istifadə edilərkən fərdi məlumatların təhlükəsizliyinin təmin edilməsi və ona nəzarət məsələləri mütləq tələb kimi nəzərə alınmalıdır. Yəni elektron xidmətlər istifadə edilərkən, fərdi məlumatların təhlükəsizliyinin təmin edilməsi və ona nəzarət mexanizmləri olmalıdır. Bir sözlə, rəqəmsal texnologiyaların istifadəsi zamanı fərdi məlumatların təhlükəsizliyinin monitorinqi imkanlarının olması çox vacib məsələdir. Təhlükəsizliyin monitorinqi istifadəçilərin fərdi məlumatlarının tam təhlükəsizliyini təmin etməyə imkan verməlidir. Lakin, digər tərəfdən, elə fərdi məlumatların təhlükəsizliyinin monitorinqinin özü istifadəçilərin şəxsi həyatının toxunulmazlığına təhlükə yarada bilər. Hətta şəbəkə trafikinin monitorinqi istifadəçilərin şəxsi həyatının toxunulmazlığına təhlükə yarada bilər, çünki verilənlərin analizi və klassifikasiyanın müasir üsullarının köməyi ilə şəbəkə trafikindən də fərdi məlumatlar əldə etmək olar [1].

Qeyd etmək lazımdır ki, bu gün qlobal İnternet mühitində istifadəçilərin fərdi məlumatlarının təhlükəsizliyinin bütövlükdə təmin edilməsi çox çətin məsələdir və bu mühitdə fərdi məlumatların təhlükəsizliyinin bütövlükdə monitorinqi üçün vasitə və imkan yoxdur.

İşin məqsədi İnternet mühitində fərdi məlumatların təhlükəsizliyinin monitorinqi problemlərinin analizidir.

II. FƏRDİ MƏLUMATLARIN KATEQORİYALARI

Fərdi məlumatların təhlükəsizliyinin təmin edilməsi zamanı əsas məsələlərdən biri bu məlumatların kateqoriyalarının müəyyən edilməsidir. Verilənlərin mühafizəsinin təmin edilməsi hüququ Avropa Birliyinin Verilənlərin Mühafizəsinin Ümumi Qaydalarına (EU GDPR – European Union General Data Protection Regulation) görə əsas insan hüququ kimi qəbul edilmişdir [2]. EU sənədində fərdi məlumatlar belə müəyyən olunmuşdur: “Fərdi məlumatlar” identifikasiya olunmuş və ya identifikasiya olunan fiziki şəxsə (“məlumat subyektinə”, imq.

“data subject”) aid olan istənilən informasiyadır; identifikasiya olunan fiziki şəxs, birbaşa və ya dolayı yolla, xüsusən də ad, şəxsiyyət nömrəsi, yeri haqqında məlumat, onlayn identifikator və ya fiziki, fizioloji, genetik, əqli, iqtisadi, mədəni və ya sosial kimliyi kimi identifikatorlar vasitəsilə identifikasiya oluna bilən şəxsdir. Bir sözlə, fərdi məlumat konkret (canlı) şəxsin identifikasiya edilməsinə səbəb ola biləcək hər hansı bir məlumatdır. Bu, ad kimi açıq şəkildə identifikasiya edilə bilən məlumatlar, həmçinin yaş, boy, çəki, sərvət, iş yeri, şirkət, şəhər və s. kimi məlumatların kombinasiyası da ola bilər. Çünki bu məlumatların kombinasiyası şəxsi identifikasiya etməyə imkan verir.

EU GDPR fərdi məlumatların xüsusi kateqoriyalarını müəyyən edir ki, bunlara irqi və ya etnik mənşə, siyasi baxışlar, dini və ya fəlsəfi inanclar, həmkarlar ittifaqı üzvlüyü, genetik məlumatlar, biometrik məlumatlar, sağlamlıq məlumatları, cinsi həyat və cinsi orientasiya aiddir. Bu kateqoriyadan olan fərdi məlumatlar əlavə vasitələrlə mühafizə olunmalıdır. Fərdi məlumat subyektinin açıq razılığı, əsaslı səbəblər və ya müəyyən istisnaslar olmadıqda toplanıla və emal oluna bilməz. Ancaq o fərdi məlumatlar emal oluna bilər ki, məlumat subyekti tərəfindən birmənalı şəkildə açıqlanmış olsun.

Fərdi məlumatlara misal kimi şəxsə aid olan müxtəlif məlumatları göstərmək olar. Məsələn, ad, soyad, təvəllüd, foto, telefon nömrəsi, ev ünvanı (küçə, şəhər, poçt indeksi və s.), elektron poçt ünvanı, bank hesab nömrəsi, kredit kartının nömrəsi, pasportun nömrəsi və fərdi identifikasiya nömrəsi, sosial sığorta kartının nömrəsi, vergi ödəyici nömrəsi, nəqliyyat vasitəsinin dövlət nömrə nişanı, IP-ünvan, “cookie” identifikatoru, olduğu yeri haqqında məlumat, əl yazısı, loqin və parol, sosial media profili identifikatoru, mobil cihaz identifikatorları, məşğulluq haqqında məlumat, vəzifəsi, təhsili haqqında məlumat və s. Həmçinin xüsusi fərdi məlumatlar müəyyən olunmuşdur ki, onlara cinsi, irqi/etnik mənsubluğu, doğulduğu yer/shəhər/ölkə, həyat yoldaşının adı, sağlamlıq haqqında məlumat, tibbi qeydlər və s. məlumatlar aid edilir.

EU GDPR həmçinin “nəzarətçi” (controller) və “prosessor” (processor) anlayışlarını müəyyən etmişdir. Bu anlayışlar fərdi məlumatların monitorinqi üçün çox vacib anlayışlardır və məlumat subyekti, nəzarətçi və prosessor arasındakı münasibətləri müəyyən etməyə imkan verir.

“Nəzarətçi” dedikdə fərdi məlumatların emalının məqsəd və vasitələrini təyin edən fiziki və ya hüquqi şəxs, dövlət orqanı, agentlik və ya digər qurum başa düşülür.

“Prosessor” dedikdə isə nəzarətçi adından fərdi məlumatları emal edən fiziki və ya hüquqi şəxs, dövlət orqanı, agentlik və ya digər qurum başa düşülür.

III. FƏRDİ MƏLUMATLARA QARŞI TƏHDİDLƏRİN MƏNBƏLƏRİ

Yeni informasiya texnologiyalarının inkişafı və geniş istifadəsi fərdi məlumatların təhlükəsizliyinə təhdidlər yaradır

və nəticədə fərdin şəxsi həyatının toxunulmazlığına təhlükə yaranır [3]. Bu təhdidlərin mənbələri müxtəlif ola bilər. Məsələn, çox zaman, fərdi məlumatları toplayan tərəflər şəxslərin xəbəri olmadan (və yaxud onlara məlumat vermədən) onların fərdi məlumatlarını toplayırlar. Bu zaman üçüncü tərəf həmin məlumatları ələ keçirə və istifadə edə bilər, yəni şəxslər öz fərdi məlumatlarının təhlükəsizliyi haqqında məlumatsız olurlar. Buna görə də, şəxslərin icazəsi və onların məlumatlandırılması fərdi məlumatların toplanması, emalı və yayılması üçün çox vacib tələblərdir və bu da sui-istifadələrin qarşısını ala bilər. Fərdi məlumatların təhlükəsizliyinə qarşı təhdidlərin yaranmasının digər bir mənbəyi bu məlumatların olduğu verilənlər daşıyıcıları, məsələn, aparat vasitələri, program təminatı, əlaqə kanalları və s. ilə bağlıdır.

Fərdi məlumatların təhlükəsizliyinə qarşı təhdidlərin yaranmasının digər bir mənbəyi isə yeni Internet texnologiyalarının (məsələn, Əşyaların İnterneti, ing. Internet of Things (IoT), mobil texnologiyaların (Mobil İnternetin) və s.), həmçinin böyük verilənlər (ing. Big Data) fenomeninin yaranması ilə bağlıdır. Məsələn, IoT insan həyatının bütün sahələrini əhatə edir – evlərdə, xəstəxanalarda və s. sahələrdə istifadə edilir və IoT çərçivəsində qurğularda olan fərdi məlumatlara ciddi təhdidlər yarana bilər. Bu gün IoT qurğularına qarşı müxtəlif hücum növləri mövcuddur [4]. Böyük verilər texnologiyası müxtəlif sahələrdə, məsələn, sosial şəbəkələrdə, tibbi kartlarda və s. toplanmış verilənlərin emalı üçün istifadə edilir və nəticədə fərdi məlumatlara və şəxsi həyatın toxunulmazlığına təhdid yarana bilər [5].

Fərdi məlumatların təhlükəsizliyinə qarşı təhdidlərin yaranması mənbələrindən biri də müxtəlif Internet xidmətlərinin yaranması və istifadəsidir. Məsələn, marketing və elektron kommersiya, sosial media, bulud və s. xidmətlərin istifadəsi. Məlumdur ki, bu xidmətlərin istifadəsi zamanı, xüsusilə də sosial medianın [6] və bulud xidmətlərinin [7] istifadəsi zamanı istifadəçilərin fərdi məlumatları toplanır və onlara qarşı təhdidlər yarana bilər.

IV. FƏRDİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİNİN MONİTORİNQİ PROBLEMLƏRİ

İnternet mühitində fərdi məlumatların təhlükəsizliyinin təmin edilməsinin vacib elementlərindən biri onun monitorinq edilməsidir. Fərdi məlumatların təhlükəsizliyinin monitorinqi problemi aydın görünsə də, mümkün vahid həll yolunun tapılması çətin məsələ olaraq qalır.

Bu gün istənilən şəxsin fərdi məlumatları müxtəlif mənbələrdə (xidmətlərdə, bazalarda və s.) ola bilər və bu məlumatlara qarşı müxtəlif təhdidlər ola bilər. Bu zaman monitorinq məsələsinə sırf texniki məsələ kimi baxılması düzgün olmaz. Çünki o, həm də şəxsi həyatın toxunulmazlığı məsələsinə əhatə edir. Yəni fərdi məlumatların təhlükəsizliyinin monitorinqi mexanizminin yaradılması zamanı mütləq şəxsi həyatın toxunulmazlığının təmin edilməsi məsələsi nəzərə alınmalıdır – bu məsələni həyata keçirən komponent olmalıdır. Bununla yanaşı fərdi məlumatların təhlükəsizliyinin

monitorinqinin həyata keçirilməsini tənzimləyən standartlar, mexanizmlər və davranış kodeksləri işlənilməlidir. Bu standartlar maraqlı tərəflərin iştirakı ilə, müəssisə, regional və yaxud da beynəlxalq səviyyələrdə işlənib bilər. Bu zaman hansı məlumatların toplanması, kimin toplanması, məlumatın həcmi, kimin və hansı əsaslarla bu məlumatlara giriş hüququ əldə etməsi, məlumatların toplanması və saxlanması müddəti və s. nəzərə alınmalıdır. Bununla yanaşı şəxsi həyatın toxunulmazlığının təmin edilməsi üçün internet-provayderlər müvafiq tələblərə uyğunlaşmaq üçün öz şəbəkə monitorinq infrastrukturlarını yeniləməlidirlər.

Məlumdur ki, şəbəkələrin monitorinqi üçün əsasən iki sinif monitorinq sistemləri istifadə edilir. Birinci sinif şəbəkənin diaqnostikası, planlaşdırılması və xidmət keyfiyyətinin təmin edilməsi kimi sistemlər daxildir. Bu sistemlər adətən passiv şəkildə toplanmış verilənləri emal edir və aqreqasiya olunmuş verilənləri əldə edir. Əldə edilmiş verilənlər müxtəlif şəbəkə problemlərinin həlli üçün istifadə edilir. Məsələn, yüklənmə, məhsuldarlıq, resursların istifadəsi, planlaşdırma, xidmət səviyyəsi haqqında razılaşmanın (ing. service level agreement – SLA) və s. şəbəkə problemlərinin müəyyən edilməsi üçün istifadə edilir. Bu zaman məlumat paketlərində olan əhəmiyyətli informasiyaya (ing. packet payload) tam şəkildə giriş tələb olunmur və şəxsi həyatın toxunulmazlığı məsələsi anonimliyin qorunmasından ibarət olur. İkinci sinif monitorinq sistemlərinə müdaxilələrin aşkarlanması sistemləri aiddir və şəbəkə təhlükəsizliyinə yönəlmişdir. Əsasən trafikə klassifikasiyasını həyata keçirir. Buna görə də bu sistemlər məlumat paketlərinin dərin yoxlanmasına və bu paketlərdə göndərilən əhəmiyyətli informasiyanın detallı şəkildə analizinə əsaslanır. Bu halda şəxsi həyatın toxunulmazlığının təmin edilməsi çox çətin məsələyə çevrilir.

Yuxarıda deyilənləri nəzərə alaraq, qeyd etmək lazımdır ki, fərdi məlumatların təhlükəsizliyinin monitorinqi məsələsinin onların yerləşdiyi mənbələrdən asılı olaraq müəyyən edilməsi və intellektual texnologiyaların (multi-agent texnologiyasından) istifadəsi ilə paylanmış monitorinq sisteminin yaradılması daha məqsəduyğun olardı.

NƏTİCƏ

İnformasiya və kommunikasiya texnologiyalarının sürətlə inkişafı və geniş istifadəsi (xüsusilə də Internetin) elektron xidmətlərin sayının və elektron formadakı informasiyanın həcmi həddindən çox artmasına gətirib çıxarmışdır. Bu şəraitdə, şəxsi həyatın toxunulmazlığının təmin edilməsi üçün fərdi məlumatların təhlükəsizliyi çox vacib və çətin məsələyə çevrilmişdir.

Bu gün rəqəmsal mühitdə fərdi məlumatların təhlükəsizliyinin təmin edilməsi üçün hüquqi baza yaradılmışdır. Buna misal olaraq Avropa Birliyinin Verilənlərin Mühafizəsinin Ümumi Qaydalarını göstərmək olar. Bununla yanaşı texniki və texnoloji bazanın da olması çox

vacibdir və bunlardan biri fərdi məlumatların təhlükəsizliyinin monitorinqi mexanizminin və vasitələrinin işlənməsidir.

İnternet mühitində fərdi məlumatların təhlükəsizliyinin təmin edilməsi üçün onların təhlükəsizlik vəziyyəti qiymətləndirilməlidir, yəni monitorinq edilməlidir. Lakin bu zaman şəxsi həyatın toxunulmazlığı ilə bağlı problemlər yaranır. Buna görə İnternet mühitində fərdi məlumatların təhlükəsizliyinin monitorinqi zamanı yaranan problemlərin analizi çox vacibdir.

İSTİNADLAR

- [1] G. Bianchi, E. Boschi, F. Gaudino, L. Koutsoloukas, et al. “Privacy-preserving network monitoring: Challenges and solutions,” ICT Mobile Summit, pp. 1-10, 2008.
- [2] <https://eugdpr.org/the-regulation>
- [3] E. Y. Yıldırım, A. Eşref “The threats and risks in personal data security,” Proceedings of the International Conference on Computer Science and Engineering, pp. 610-615, 2017.
- [4] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao “A survey on security and privacy issues in Internet-of-Things,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, 2017.
- [5] B. B. Rad, N. Akbarzadeh, P. Ataei, and Y. Khakbiz “Security and privacy challenges in Big data era,” International Journal of Control Theory and Applications, vol. 9, no. 43, pp. 437-448, 2016.
- [6] X. Liang, Z. Kuan, and X. Shen “Security and privacy in mobile social networks: Challenges and solutions,” IEEE Wireless Communications, pp. 33-41, 2014.
- [7] H. Takabi, B. D. Joshi, G.J. Ahn “Security and privacy challenges in cloud computing environments,” IEEE Security and Privacy Magazine, vol. 8, no. 6, pp. 24-31, 2011.

PROBLEMS OF MONITORING OF PERSONAL DATA SECURITY IN INTERNET ENVIRONMENT

Ramiz Shikhaliyev

Institute Information Technology of ANAS, Baku, Azerbaijan

ramiz@science.az

Abstract— Monitoring the security of personal information in the Internet environment is a very important issue to ensure the inviolability of privacy. But in the global Internet environment, this is a very difficult problem. This is because Internet users use marketing and e-commerce, social media, cloud, and so on. They use a large number of electronic services, including mobile Internet, and their personal information is stored in various sources (services, databases, etc.). The threats to the personal data contained in these sources also vary. Creating a single mechanism for monitoring the security of personal data in such a distributed global environment is a difficult task. The article is devoted to the analysis of the problems of monitoring the privacy of personal information in the Internet. As a result of the analysis, the article notes the feasibility of establishing a distributed monitoring system with the use of intelligent technology (multi-agent technology) to identify the issue of monitoring personal data security depending on the source of their location.

Keywords— *personal data, categories of personal data, privacy, monitoring of personal data security*

Fərdi məlumat subyektlərinin hüquqlarını mühafizə mexanizmlərinə etimad səviyyəsinin ölçülməsi metodu

Elçin Əliyev

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

Xülasə— Bu məqalədə fərdi məlumatların informasiya sistemlərində şəxsin hüquqlarını mühafizə mexanizmlərinin mükəmməllik və etimad səviyyələrini ölçmək üçün bir metodun işlənilməsi problemi qoyulur. Bu problemin həlli üçün: a) fərdi məlumat subyektlərinin hüquqları, bu hüquqları mühafizə mexanizmləri beynəlxalq və milli normativ alətlər əsasında identifikasiya olunur; b) bu mühafizənin obyektlərinin ümumi səviyyədə arxitekturası müəyyən edilir, bu sahədə və bu səviyyədə etalon müqayisə üçün orientir (“benchmark”) təyin olunur; c) beynəlxalq standartların təklif etdiyi mükəmməllik və etimad meyarları, müvafiq qiymət (reyting) şkalaları və fərdi məlumatların mühafizəsində bu meyar və şkalaların tətbiqi imkanları araşdırılır; d) fərdi məlumatların mühafizəsinin obyektlərinə, mükəmməllik səviyyələrini və onlara etimad dərəcələrini ölçmək üçün metod təklif olunur; e) bu ölçmə metodunun tətbiq sahəsi, o cümlədən e-dövlətdə fərdi məlumatların təhlükəsizliyinə “etimad zonaları”nı müəyyən edə bilmək üçün hüquqi və texnoloji əhəmiyyəti təsvir olunur.

Açar sözlər— fərdi məlumatların mühafizəsi; mühafizə obyekt; mühafizə aləti; etimad səviyyəsi; etimad meyarı; ölçmə metodu; qiymət şkalası; etimad zonası; GDPR

I. GİRİŞ

Məlumdur ki, hər bir fəaliyyətin icraçısı (operatoru) tərəfindən ona bu fəaliyyət prosesləri üçün lazım olan informasiya yaradılır (əldə olunur), işlədilir və mühafizə olunur. Bu informasiyanın həmin fəaliyyət üçün təhlükəsizliyinin (tamlıq, əlçatırılıq, konfidensiallıq və dəyərliklik xassələrinin) təmin olunma əmsalı fəaliyyət davamlılığının təmin olunma dərəcəsinə təsir edir, kritik parametrlərdir.

Əldə olunma növünə görə informasiya ümumi istifadə üçün açıq olan və məhdudlaşdırılan kateqoriyalara bölünür, məxfi (dövlət sirri) və konfidensial (fərdi məlumat, xidməti sirr, o cümlədən həkim, vəkil, notariat və digər peşə sirləri, kommersiya sirri, bank sirri, istintaq və məhkəmə sirri) olur.

Məxfi və konfidensial informasiya onun subyektinə olan dövlət, özəl və ictimai təşkilatın öz qanuni maraqlarını həyata keçirmək üçün özü (kontroller) və ya təyin etdiyi icraçı (operator) tərəfindən yaradılır (əldə olunur), işlədilir, mühafizə

olunur. Bu informasiyanın təhlükəsizliyinin, o cümlədən konfidensiallığının pozulması həmin subyektin (kontrollerin) qanuni maraqlarının pozulmasına və bu subyektin fəaliyyət davamlılığına, nüfuzuna aid fəsadların yaranmasına səbəb olur.

İnformasiyanı mühafizə üsullarının və vasitələrinin yetərliyi və yararlılığı üçün məqbul hədd və təhlükəsizlik tələbləri bu fəsadların və onların yaranan təhdidlərin ölçüsünü nəzərə almaqla təyin edilir. Bu hədd həmin ölçüdən aşağı olmamalıdır. Təhlükəsizlik tələbi mühafizə obyektinə təhdidin qarşısını almaq və ya onun yarada biləcəyi fəsadı minimallaşdırmaq, bu obyektə təhdidin istifadə edə biləcəyi zəifliyi aradan qaldırmaq üçün – nəticədə fəaliyyət davamlılığını təmin edə bilmək və ya məqbul həddə bərpa edə bilmək üçün təyin edilir.

Fərdi məlumatlar dövlət, özəl, ictimai təşkilat və fiziki şəxs (kontroller), o cümlədən həmin məlumat subyektinin özü tərəfindən yaradılır (əldə olunur), işlədilir, mühafizə olunur. Fərdi məlumatların təhlükəsizliyinin, xüsusən də konfidensiallığının pozulması nəticəsində kontrollerə və həmin fərdi məlumatın subyektinə müəyyən fəsad yaranır. Subyekt üçün fəsadın ölçüsü kontroller üçün fəsadın ölçüsündən daha kritik, daha böyük ola bilər.

Fərdi məlumatların yaradılmasına (əldə olunmasına), işlədilməsinə və mühafizəsinə təsir imkanları həmin məlumatların subyektində minimal, hətta yox dərəcədə olur, kontrollerdə (onun operatorunda) maksimal, hətta absolyut dərəcədə olur.

Bu isə kontrollerin fərdi məlumat subyektinə qarşısında məsuliyyətinin dəqiq təyin edilməsini, fərdi məlumat subyektinin bu sahədə hüquqlarının kontroller tərəfindən mühafizə olunma, fərdi məlumatlar ilə əlaqədar olan fəaliyyətin ölçmə subyektinə tərəfindən monitoring-audit-dəyərləndirmə səviyyələrinin, bu səviyyələrə subyektin etimad dərəcəsinin ölçülə bilinməsinə zəruri edir.

Bu məqalədə onun istinadlar bölməsində siyahısı verilmiş mənbələrdə müəyyən edilmiş normalardan və anlayışlardan istifadə olunur.

Fərdi məlumatların mühafizəsinə bu məlumatlar ilə əlaqədar olan fəaliyyəti təmin edən arxitekturanın obyektləri, prosesləri və subyektləri, o cümlədən onların və struktur vahidlərinin, onlar arasında asılılıq əlaqələrinin mükəmməlik vəziyyəti təsir edir:

Obyektlər – milli və korporativ informasiya məkanlarının fərdi məlumatlar üzrə seqmentləri, ölkənin bimetrik identifikasiya sistemi, əhali reyestri, fərdi identifikasiya nömrəsi (FİN) servisi, fərdi məlumatların informasiya sistemləri, əhaliyə e-xidmətlər, serverlər kompleksləri, telekommunikasiya və kompüter şəbəkəsi infrastrukturuları, avtomatlaşdırılmış məlumat faylları, fərdi məlumatların informasiya sistemlərinin dövlət reyestri, İKT konfigurasiyanın məlumat bazası (“CMDB”), məlumat toplularına, fayllara və proqram təminatı vasitələrinin modullarına icazələr matrisaları, risklər reyestri, monitorinq servisi, mühafizə servisləri, ehtiyat surətlər, İKT məhsulları işləyib hazırlama alətləri, sınaq-test mühiti, “ServiceDesk” portalı, “CERT/CSIRT” portalı, insidentlərin qeydiyyat bazası, “biliklər bankı”, servislər kataloqu, “SysEventLog” faylları və s. vahidlərdən ibarət olur;

Proseslər – məcbureddici (“imperative”) əsaslar, tətbiqetdirici aktlar (“implementing act”), iş axınlarının təsviri (“work flow”), onların nəticələrinin və şəhadətlərin (“evidence”) qeydiyyatı (sübut toplama) və s. vahidlər əsasında müəyyən olunur:

- a) məcbureddici əsaslar – beynəlxalq və milli normativ hüquqi aktlar, beynəlxalq, regional, milli texniki normativ hüquqi aktlar (standartlar, qabaqcıl tövsiyələr topluları), subyektlər haqqında əsasnamələr, beynəlxalq və milli səviyyəli məsuliyyət (vəzifə və hüquqlar) bölgüsü matrisaları, kompetensiya tələbləri, reyting şkalaları, məcburi korporativ qaydalar (“binding corporate rules”) və s.;
- b) hədəflər – milli və korporativ dəyərlər, prinsiplər, strategiyalar, siyasətlər, strategi proqramlar, taktiki və operativ planlar, kompetensiya tələbləri və s.;
- c) tətbiqetdirici aktlar – lokal normativ hüquqi aktlar, davranış kodeksləri, struktur bilmələr haqqında əsasnamələr, vəzifə təlimatları, korporativ və infrastruktur səviyyəli məsuliyyət (vəzifə və hüquq) bölgüsü matrisaları, rəqlamentlər, müqavilə, razılaşma və öhdəliklər, zəmanətlər, sertifikatlar, lisenziyalarqiyəmətləndirmə şkalaları və s.;
- d) iş axınları – müraciət, təhlil, layihələndirmə, ekspertiza, işləyib hazırlama, sınaqlar, tətbiq, istifadə, məlumat-sorgu və axtarış, təhlil, məlumat mübadiləsi, psevdonimləşdirmə (adsızlaşdırma), xidmət, sorğu, monitorinq, statistika, müqayisə, audit, qiymətləndirmə, kompensasiya,

araşdırma, verifikasiya və validasiya test ssenari, həll və ya imtina, dəyişiklik və təkmilləşdirmə və s.;

- e) şəhadətlər – sınaq testi qiymətləri, konfigurasiyanın, zəifliklərin və anomaliyaların, iş axınlarının və digər hadisələrin, fəsadların qeydiyyatları və s.;

Subyektlər – fərdi məlumat subyekti, kontrolleri, mülkiyyətçisi, operatoru (emalçı/ıçraçı, “processor”), ekspert, inspektor, səlahiyyətli müşahidəçi (“supervisory authority”), rəhbər orqan, şura, istifadəçi, digər maraqlı tərəf və s. fiziki və hüquqi şəxslərdən ibarət olur.

II. MƏSƏLƏNİN QOYULUŞU

Fərdi məlumatların mühafizəsinə subyektin etimadı müəyyən oluna və onun dərəcəsi ölçülə bilinməlidir. Bu isə:

Subyekt qarşısında kontrollerin məsuliyyətinin daha dəqiq təyin edilməsini, meyarların konkretləşdirilməsini, kontrollerin fəaliyyətinin və idarəetmə alətlərinin (kontrolların), o cümlədən funksionallıq və konfigurasiyanın (onların göstəricilərinin) meyarlara uyğunluğunun monitorinqini zəruri edir;

Fərdi məlumatların toplanılmasında, işlənilməsində, mühafizəsində iştirak edən tərəflərin kompetensiya, resurs potensialı və fəaliyyət mükəmməliyindən, onların istifadəsində olan meyar, şəhadət, alət və aşağıda göstərilən digər amillərin formalaşdırılması dərəcəsindən asılı olur:

- a) kontrollerlər – fərdi məlumatların yaradılmasına (əldə olunmasına), işlədilməsinə və mühafizəsinə (qanuni əsaslarla bu sahədə həvalə edilmiş digər vəzifə və hüquqların həyata keçirilməsinə) lazım olan infrastrukturun, informasiya sistemlərinin mülkiyyətçiləridir, sahibləridir;
- b) ölçmə subyekti – ölçmə üçün meyarlara və metodlara, o cümlədən alətlərə aid kompetensiyaya malik olan mütəxəssis resurslarından seçilir, formalaşdırılır, səlahiyyətli müşahidəçi (“supervisory authority”), inspektor rollarını icra edir;
- c) kontrollerin məsuliyyəti – kontrollerin fəaliyyətinə normativ tələblərdir (onun qəbul etdiyi öhdəliklər vasitəsilə qoyulur, ölçmə üçün meyar olur);
- d) ölçmənin obyekti – kontrollerin işgüzar (biznes) fərdi məlumatlar ilə əlaqədar olan fəaliyyəti, tətbiq etdiyi üsul və vasitələrdir;
- e) ölçmənin predmeti – ölçmə üçün obyektin təyin olunmuş meyarlara uyğunluğunu müəyyənləşdirmə vəzifəsidir;
- f) ölçmə üçün şəhadətlər – kontrollerin bu fəaliyyətində yaradılan sənədləşdirilmiş informasiyadır (sənədlər və yazılar), tətbiq olunan üsul və vasitələrin funksionallıq və konfigurasiya göstəriciləridir;
- g) ölçmə üçün metod – ölçmə üçün meyar, obyekt, predmet və şəhadətlərdən asılı olaraq müəyyən olunan üsuldur;

h) ölçmə üçün alətlər – ölçmə üçün metodlarlar əsasnda yaradılır, üsullardan (siyasətlərdən, prosedurlardan, alqoritmlərdən), vasitələrdən (proqram və texniki təminat məhsullarından), rəqlamentlərdən (səlahiyyətlər bölgüsündən, əlaqələr və məhdudiyyət sxemlərindən) və informasiya resurlarından (verilənlər və biliklər bazalarından) ibarət servisdır.

Fərdi məlumatların mühafizəsinə etimad səviyyəsinə bu məlumatların toplanılmasına və işlənilməsinə milli və beynəlxalq qanunvericilik əsasında təyin edilmiş şərtlər və onlara əməl olunma vəziyyəti, fərdi məlumat subyektlərinə verilmiş hüquqlar və onların həyata keçirilmə imkanları, fərdi məlumat kontrollerlərinə həvalə edilmiş vəzifələr və onların həyata keçirilmə vəziyyəti təsir edir.

Fərdi məlumatların toplanılmasına və işlənilməsinə təyin edilmiş əsas şərtlər aşağıdakılardır:

- a) Fərdi məlumatlar yalnız məcburedici əsaslara, təbiiqetdirici aktlara uyğun olaraq və əvvəlcədən dəqiq müəyyən olunmuş hədəflər üçün toplanılmalı və onlara adekvat üsullarla işlənilməlidir. Bu əsaslar aradan qalxdıqda həmin məlumatlar təxirə salınmadan məhv edilməlidir
- b) Fərdi məlumatların toplanılması və işlənilməsi subyekt buna öz razılığını verdikdə, yaxud qanunla müəyyən olunmuş hallarda məcburi xarakter daşıdıqda, yaxud bu məlumatlar açıq kateqoriyalı olduqda həyata keçirilə bilər.
- c) Toplanılan və işlənilən fərdi məlumatların həcmi və xarakteri bəyan edilmiş hədəflərə və kontrollerin səlahiyyətlərinə uyğun olmalıdır.
- d) Elmi və statistik tədqiqat məqsədləri üçün fərdi məlumatlar onların mütləq qaydada adsızlaşdırılması (pseudonimləşdirilməsi) aparılmaqla işlənilməlidir.
- e) İnformasiya sistemlərində və ehtiyatlarında fərdi məlumatların toplanılması, işlənilməsi, sorğuların verilməsi və icrası, ərizələrin qeydiyyatının və baxılmasının nəticələri, habelə informasiya sistemlərinin idarə olunması və mühafizəsi ilə bağlı əməliyyatlar barədə qeydlər müvafiq nəzarət-audit jurnallarında toplanılmalıdır, bu qeydiyyatlar kontroller (və ya onun operatoru) tərəfindən təmin olunmalıdır.
- f) Fərdi məlumatların transsərhəd ötürülməsi qanunvericiliklə müəyyən olunan tələblərə riayət edilməklə həyata keçirilir. Transsərhəd ötürülmə üçün nəzərdə tutulan ölkənin qanunvericiliyi həmin məlumatların Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən edilmiş səviyyədə hüquqi mühafizəsini təmin edə bilməlidir, əks halda bu ötürülmə qadağan edilir.

Fərdi məlumat subyektlərinə verilmiş əsas hüquqlar aşağıdakılardır:

- a) özü barəsində fərdi məlumatlar mövcud olan informasiya sistemləri, məlumatların məzmunu, bu məlumatların toplanılmasının və işlənilməsinin hüquqi əsası, məqsədi, işlənilmə müddəti, üsulları, əldə edilmə mənbələri, bu sistemlərin kontrolleri və operatoru, məlumat mübadiləsi

aparılması nəzərdə tutulan informasiya sistemlərinin dairəsi haqqında məlumat almaq;

- b) fərdi məlumatların toplanılmasının və işlənilməsinin qanunvericiliklə müəyyən olunmuş qaydada məcburi xarakter daşıdığı hallar istisna olmaqla, subyekt onun barəsində olan məlumatların toplanılmasına və işlənilməsinə razılıq və ya etiraz etmək (etirazın əsaslandırılması tələb olunmur), razılığı geri götürmək;
- c) informasiya sistemində özü barəsində toplanılmış və işlənilən fərdi məlumatların mühafizəsini tələb etmək;
- d) özü barəsində toplanılan və işlənilən fərdi məlumatların olduğu informasiya sistemlərinin uyğunluq sertifikatının mövcudluğu və dövlət ekspertizasından keçirilməsi haqqında məlumat almaq;
- e) informasiya sistemində özü barəsində fərdi məlumatların dəqiqləşdirici dəyişiklik edilməsini və qanunvericiliklə müəyyən olunmuş hallar istisna olmaqla, informasiya sistemindən təxirə salınmadan çıxarılmasını, məhv edilməsini tələb etmək;
- f) İKT vasitəsilə fərdi məlumatların toplanılması və işlənilməsi nəticəsində qəbul olunan qərar subyektin mənafeini pozduğu halda, qanunvericiliklə müəyyən olunmuş qaydada məcburi xarakter daşıdığı hallar istisna olmaqla, bu məlumatların göstərilən üsulla toplanılmasına və işlənilməsinə etiraz etmək;
- g) fərdi məlumatların toplanılması və işlənilməsi, mühafizəsi sahəsində mövcud normativ tələblərə əməl olunmaması nəticəsində onun hüquqlarının pozulduğu hallarda nəzarət orqanına və ya məhkəməyə şikayət etmək, habelə ona vurulmuş mənəvi və maddi ziyanın ödənilməsinə məhkəmə qaydasında tələb etmək.

Fərdi məlumat kontrollerlərinə həvalə edilmiş əsas vəzifələr aşağıdakılardır:

- a) fərdi məlumatların toplanılmasının və işlənilməsinin qanuniliyini və təhlükəsizliyini təmin etmək;
- b) fərdi məlumatların korporativ informasiya sistemlərində yalnız müvafiq icazəsi olan istifadəçilərə xidmət göstərmək;
- c) fərdi məlumatların toplanılması, işlənilməsi və mühafizəsi sahəsində fəaliyyət göstərən fiziki şəxslərdən onların fəaliyyət müddətində və işdən çıxdıqdan sonra həmin məlumatların yayılmaması barədə yazılı iltizam almaq;
- d) fərdi məlumatların mühafizəsinin təmin edilməsini zamanət verən təşkilati və texniki tədbirlər görmək;
- e) fərdi məlumatların təhlükəsizliyinə təhdidləri və mühafizə səviyyəsini qiymətləndirmək;
- f) fərdi məlumatlar ilə əlaqədar fəaliyyəti lisenziya əsasında həyata keçirmək;
- g) fərdi məlumatların informasiya sistemlərinin dövlət qeydiyyatına alınması üçün öz tərəfinə aid tədbirlər görmək, bu qeydiyyat zəruri olan məlumatları, o cümlədən fərdi məlumatların mühafizəsi ilə bağlı öhdəsinə götürdüyü tədbirlərin, monitorinq və audit mexanizmlərinin ümumi təsvirini, əhaliyə göstərilə bilən e-xidmətlərin əhatə dairəsi barədə məlumatı təqdim etmək;

- h) fərdi məlumatların informasiya sistemlərini, habelə müvafiq informasiya texnologiyaları vasitələrini sertifikatlaşdırılması üçün öz tərəfinə aid tədbirlər görmək;
- i) fərdi məlumatların informasiya sistemlərinin yaradılması və tətbiq edilməsi sahəsində hüquqi və texniki sənədləşdirməni və onun standartlaşdırılmasını təmin etmək;
- j) fərdi məlumatların informasiya ehtiyatlarının və sistemlərinin və onların layihə sənədlərinin dövlət ekspertizasının həyata keçirilməsi üçün öz tərəfinə aid tədbirlər görmək.
- k) fərdi məlumat subyektinin onun barəsində olan məlumatların toplanılmasına və işlənilməsinə etirazını aldıqda göstərilən fərdi məlumatların toplanılmasını və işlənilməsinə dərhal dayandırmaq;
- l) subyektdən onun fərdi məlumatlarının toplanılması və işlənilməsi üçün razılığın alınması haqqında, açıq fərdi məlumatların toplanılmasını və işlənilməsinə həyata keçirilən hallarda, subyektin tələbi ilə həmin məlumatların açıq fərdi məlumatlar kateqoriyasına aid olduğu haqqında sübutları təqdim etmək.

III. PROBLEMİN HƏLL ÜSULLARI

Fərdi məlumatların mühafizəsinə bu məlumatların subyektinin etimad dərəcəsi bu məlumatların toplanılmasını, işlənilməsinə, mühafizəsinə təmin edən arxitekturanın, onun obyektlərinin, proseslərinin və subyektlərinin, o cümlədən onların struktur vahidlərinin və onlar arasında asılılıq əlaqələrinin mükəmməlik dərəcəsinə düz mütənəsisib olur.

Mükəmməlik dərəcəsinə ölçmə probleminin həlli üçün müəyyən alətlər müvafiq texniki normativ hüquqi aktlarda (menecment standartlarında) nəzərdə tutulmuşdur. Bu sahədə aşağıda göstərilən alətlərdən istifadə səmərəli hesab edilir:

Fərdi məlumatların yaradılmasına (əldə olunmasına), işlənilməsinə, mühafizəsinə lazım olan obyektlərə etimadi müəyyən etmək üçün:

İKT- məhsullar onlara qoyulmuş funksional tələblərə, bu tələblər isə məcburedici (“imperative”) əsaslara, tətbiqetdirici aktlara (“implementing act”) uyğun olmalı, iş axınlarını təyinatı üzrə təmin etməli, onların nəticələrinin və şəhadətlərin (“evidence”) qeydiyyatlarını təyinatı üzrə və strukturlaşmış yarada bilməlidir.

- a) İKT- məhsullar onlar üçün qoyulan funksional tələbləri (onlar müvafiq siniflər, ailələr üzrə təsnifatlaşdırılır) əhatə etməlidir; (*Bax*: Bu funksional tələblərin sinifləri, ailələri və komponentlərinin iyerarxiyasının daha detallı təsviri üçün [13].)
- b) İKT-məhsullara etimad (“assurance”) səviyyələri (EQS, “EAL, Evaluation Assurance Level”) 7 dərəcəli qiymət (“rating”) şkalası üzrə müəyyən olunur [13] (*Qeyd*: fərdi məlumat subyektinin etimadı üçün bu qiymət 4-cü dərəcədən aşağı olmamalıdır):
- EAL1: Funksional testetmə; (*Qeyd*: Bu səviyyə etimada minimal dərəcədə zamanətlər verir. Qiymətləndirmə

obyektlərinin mühafizəsi üçün yalnız ən aşkar zəifliklərinin minimal xərclərlə aşkarlanması üçün nəzərdə tutulub. Bu səviyyədə etimad təhlükəsizliklə əlaqədar ciddi risklər olmadığı hallarda tətbiq edilə bilər.)

- EAL2: Strukturlu testetmə;
- EAL3: Metodiki testetmə və yoxlama;
- EAL4: Metodiki layihələşdirmə, testləşdirmə və dərinləşdirilmiş yoxlama;
- EAL5: Yarıformal layihələndirmə və testləşdirmə;
- EAL6: Layihənin yarıformal verifikasiyası və testetmə;
- EAL7: Layihənin formal verifikasiyası və testetmə; (*Qeyd*: Bu səviyyədə etimadı qiymətləndirmə obyektlərinin mühafizəsinə praktikada real əldə edilməsi mümkün olan yuxarı dərəcədə zamanətlər verir. Qiymətləndirmə obyektlərinin mühafizə vasitələri kompleksinin layihələndirilməsi zamanı formal modelin istifadəsi, funksional spesifikasiyaların formal təsvirləri, aşağı səviyyə layihəsinin yarıformal təsvirləri və onlar arasında uyğunluğun formal və ya yarıformal nümayişi ilə xarakterizə edilir.)

Cədvəl: Etimad tələblərinin siniflər və ailələr üzrə iyerarxiyası və etimadın qiymətləndirmə səviyyələrinin xülasəsi.

Etimad sinfi	Etimad ailəsi	EQS-ə (“EAL”) aid olan etimad komponentləri (müvafiq № ilə)						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Konfigurasiyanın idarə edilməsi – Kİ (ACM) [6]	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Təchizat və istismar (ADO) [6]	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
İşlənilib-hazırlanma (ADV) [9, 10, 13]	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Rəhbər sənədlər (AGD)	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Həyat dövrünün dəstəklənməsi (ALC) [6]	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Testləşdirmə (ATE) [9, 10, 13]	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Zəifliklərin qiymətləndirilməsi (AVA) [5]	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1

“İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri”
V respublika konfransı, 29 noyabr 2019-cu il

AVA_VLA	1	1	2	3	4	4
---------	---	---	---	---	---	---

(Qeyd: Bu etimad sinifləri, ailələri (tam və qısa adları) və komponentlərinin iyerarxiyası müvafiq standartda [13] daha detallı təsvir olunmuşdur.)

Fərdi məlumatların yaradılmasına (əldə olunmasına), işlədilməsinə və mühafizəsinə aid proseslərinə etimadi müəyyən etmək üçün:

Fərdi məlumatların yaradılmasına (əldə olunmasına), işlədilməsinə və mühafizəsinə aid proseslərin siyahısının tamlığı təmin olunmalıdır, bu proseslər arasında səbəb-nəticə asılılığı əlaqələri dəqiqləşdirilməlidir. Bu proseslərə risklər qiymətləndirilməli, o cümlədən bu proseslərdə boşluqlar, təkrarlanmalar, zəifliklər, təzadlar və mövcud meyarlara digər uyğunsuzluqlar aradan qaldırılmalıdır.

Bu proseslər üçün təyin olunan məqsədlər, tədbirlər “SMART” (“Specific, Measurable, Achievable, Relevant, Timely”) – Konkret, Ölçüləbilən, Nəticəli/mümkün, Əhəmiyyətli/uyğun, Zamanında olma) meyarlarına uyğun olmalıdır;

Bu proseslərin mükəmməllik (“maturity”) səviyyələri aşağıdakı 5 dərəcəli qiymət (“rating”) şkalası üzrə müəyyən olunur (*müəllifin qeydi: fərdi məlumat subyektinin etimadi üçün bu qiymət 3-cü dərəcədən aşağı olmamalıdır, 0-cı səviyyə isə əslində şərtidir, yəni səviyyə yoxdur*) [12, 15]:

Qiymət (“rating”) şkalası	Prosesin imkanları	Kontekst
5. Optimallaşdırılan proses	Öncə məlum proses müəssisənin cari və gələcək məqsədlərinə nail olmaq üçün davamlı təkmilləşdirilir.	Korporativ mühit konteksti: korporativ biliklər
4. Öncə məlum proses	Müəyyənlanmış proses verilmiş məhdudiyyətlər şəraitində nəticələr alır.	
3. Müəyyənlanmış proses	İdarə olunan proses nəzərdə tutulan nəticələrə nail olmaq imkanına malikdir.	
2. İdarə olunan proses	İcra olunan proses idarə olunur (yəni planlaşdırılır, izlənilir, təkmilləşdirilir). Prosesin nəticələri yaranır, onlara nəzarət və dəstək olunur.	Əlaqəsizlik mühiti konteksti: fərdi biliklər
1. İcra olunan proses	Proses tətbiq olunur və təyinatına uyğundur.	
0. Natamam proses	Proses icra olunmur yaxud nəzərdə tutulan məqsədə (gözləntiyə) nail ola bilməmişdir. Prosesin nəticələri barədə qeydiyyatlar azdır yaxud yoxdur.	

Fərdi məlumatların informasiya sistemlərinin əhatə sahəsində korporativ idarəetmə proseslərinə etimad həmin sahədə keyfiyyətin [4] və işgüzar fəaliyyət (biznes) davamlılığının [18] menecmenti sistemlərinin müvafiq standartlara uyğunluq dərəcəsindən (sertifikatlaşdırmadan) asılıdır.

Fərdi məlumatların informasiya sistemlərinin əhatə sahəsində mühafizə proseslərinə [4, 5] etimad həmin sahədə informasiya təhlükəsizliyinin menecmenti sisteminin müvafiq standartlara uyğunluq dərəcəsindən (sertifikatlaşdırmadan) asılıdır.

Fərdi məlumatların informasiya sistemlərinin həyat tsikli proseslərinə [9, 10, 13], layihə menecmenti proseslərinə [8, 16] etimad bu proseslərin müvafiq standartlara uyğunluq dərəcəsindən asılıdır.

Fərdi məlumatların informasiya sistemlərinə İKT-xidmət proseslərinə etimad bu xidmətləri idarəetmə sisteminin müvafiq standartlara [6, 7, 14, 15, 17] uyğunluq dərəcəsindən (sertifikatlaşdırmadan), xüsusən xidmətlər səviyyəsi barədə Razılaşmaların (“Service Level Agreement, SLA”) və xidmətlərin səmərəlilik göstəricilərinin – metrikasının (“Key Performance Indicator, KPI”) mükəmməllik səviyyələrindən, bu xidmətlər nəticəsində yaranan şəhadətlərin təhlükəsizliyindən (tamlığından, əlçatılığından, konfidensiallığından və dəyərliyindən) asılıdır.

Fərdi məlumatların subyektinin hüquqlarının mühafizə sisteminə etimad bu sistemin arxitekturasının səmərəliliyinin qiymətləndirilməsi nəticələrindən, müvafiq İKT-xidmətin (vahid pəncərə formasında e-xidmətin) formalaşdırılmasından asılıdır.

Fərdi məlumatların yaradılmasında (əldə olunmasında), işlədilməsində və mühafizəsində subyektlərə etimadi müəyyən etmək üçün:

Fərdi məlumatların yaradılmasına (əldə olunmasına), işlədilməsinə və mühafizəsinə aid proseslərə və risklərə cavabdehlər təyin olunmalı və digər iştirakçı rollar müəyyən olunmalı, bu subyektlər (maraqlı tərəflər) arasında beynəlxalq və milli səviyyəli, korporativ və infrastruktur səviyyəli məsuliyyət (vəzifə və hüquqlar) bölgüsü dəqiqləşdirilməlidir. Bu bölgüdə boşluqlar, təkrarlanmalar, təzadlar və mövcud meyarlara digər uyğunsuzluqlar aradan qaldırılmalıdır.

Bu subyektlərə etimad onlara aid əsasnamələrin, vəzifə təlimatlarının bu subyektlərə həvalə olunan proseslərə uyğun olmasından, bu proseslərin həyata keçirilməsinə lazım olan kompetensiya, resurs potensialı və fəaliyyət göstəricilərinin səviyyəsindən asılıdır.

NƏTİCƏ

Fərdi məlumat subyektlərinin hüquqlarını mühafizə mexanizmlərinə etimad səviyyəsini ölçmək üçün metodun formalaşdırılması bu etimad səviyyəsi göstəricilərinin – metrikasının (ESM) da tərtib olunmasını, bu hüquqların

mühafizəsi üzrə İKT-xidmətin (əhaliyə e-xidmətin) formalaşdırılmasını zəruri edir.

Bu ölçmə metodunun tətbiqi milli informasiya məkanının fərdi məlumatlar üzrə seqmentində, e-dövlətdə fərdi məlumatların təhlükəsizliyinə “etimad zonaları”nı müəyyən edə bilmək üçün hüquqi və texnoloji zəmin yaradılır.

İSTİNADLAR

- [1] GDPR “General Data Protection Regulation”), EC, www.ec.europa.eu
- [2] “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”, CE, www.coe.int
- [3] “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanunu, www.e-qanun.az
- [4] ISO-9K “Quality management systems”, www.iso.org
- [5] ISO/IEC-27K “Information technology. Security techniques. Information security management systems”, www.iso.org
- [6] ISO/IEC 20K “Information technology. Service management. Service management system”, www.iso.org
- [7] ISO/IEC-38500 “Governance of IT for the organization”, www.iso.org
- [8] ISO-21500 “Project management”, www.iso.org
- [9] ISO/IEC-12207 “Systems and software engineering. Software life cycle processes”, www.iso.org
- [10] ISO/IEC-15288 “System engineering. System life cycle processes”, www.iso.org
- [11] ISO/IEC/IEEE-15289 “Systems and software engineering. Content of life cycle information products (documentation)”, www.iso.org
- [12] ISO/IEC-15504 “Information technology. Process assessment”, www.iso.org
- [13] ISO/IEC-15408 “Information technology. Security techniques. Evaluation criteria for IT security”, www.iso.org
- [14] ITIL (“Information Technology Infrastructure Library”), www.axelos.com

- [15] COBIT (“Control Objectives for Information and Related Technologies”), www.isaca.org
- [16] PMBOK (“Project Management Body of Knowledge”), www.pmi.org
- [17] TOGAF (“The Open Group Architecture Framework”), www.opengroup.org
- [18] ISO-22301 “Societal security. Business continuity management systems. Requirements”, www.iso.org

A METHOD FOR MEASURING OF TRUST LEVEL OF PROTECTION MECHANISMS FOR RIGHTS OF PERSONAL DATA SUBJECTS

Elchin Aliyev

ANAS Institute of Information Technology, Baku, Azerbaijan,

elchinaa@gmail.com

Abstract— This article addresses the problem of developing a method for measuring the level of excellence and confidence of mechanisms to protect human rights in personal data information systems. To address this problem: a) the rights of individual data subjects and their protection mechanisms are identified on the basis of international and national regulatory instruments; (b) The overall architecture of the objects of this protection is defined, and the benchmark for benchmarking in this area and at this level is designated; c) examining the criteria for excellence and confidence offered by international standards, the appropriate value (rating) scale, and the applicability of these criteria and schemes for the protection of personal data; d) a method for measuring the level of excellence and confidence levels of data protection objects is proposed; (e) The scope of this measurement method, including the legal and technological significance of defining "zones of confidence" in the security of personal data in the e-government.

Keywords— *personal data protection, security object, security instrument, confidence level, confidence-building measure, measurement method, value scale, confidence zone, GDPR*

Elektron mühitdə pasiyentlərin fərdi məlumatlarının mühafizəsinin aktual problemləri

Kəmalə Qurbanova

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

Xülasə— İşdə pasiyentlərin fərdi məlumatlarının yayılmasına imkan yaradan informasiya-kommunikasiya texnologiyalarının tibb sahələrinə tətbiqi araşdırılmışdır. Tibbi informasiya sistemlərinin və Internet mühitində tibbi sosial medianın yaratdığı problemlər şərh edilmişdir. Elektron mühitdə tibbin normativ-hüquqi bazasının formalaşdırılması, proqram-texniki bazasının təkmilləşdirilməsi, peşəkar kadrların hazırlanması və təhlükəsizliyin təmin olunması üçün yeni texnologiyaların işlənməsi tövsiyə olunmuşdur.

Açar sözlər— tibbi informasiya sistemləri; tibbi sosial media; məxfi məlumatlar; fərdi məlumatların təhlükəsizliyi

I. GİRİŞ

Son illərdə İnformasiya-Kommunikasiya Texnologiyalarının (İKT) səhiyyəyə nüfuz etməsi nəticəsində tibbi informasiya sistemləri (TİS) və tibbi sosial media (TSM) yaranmışdır. İKT-nin tibb sahəsinə kütləvi şəkildə tətbiq olunması elektron mühitdə pasiyentlərin fərdi məlumatlarının mühafizəsini aktual etmişdir.

TİS-in təkmilləşdirilməsi səhiyyənin inkişafının strateji istiqamətlərindən biridir. TİS xəstə və ona göstərilən bütün xidmətlər haqqında qeydlərin aparılmasını təmin edir. Pasientlərin fərdi məlumatlarının toplandığı TİS tibb işçilərinin informasiya əldə etmək üçün müraciət etdiyi mənbədir. Bu sistemin yaranması həkim və tibb bacılarına pasiyentlərin kliniki vəziyyəti ilə bağlı qərar qəbul etməsinə yardım edir. TİS-in digər proqram məhsullarından əsas fərqi şəxsi və məxfi məlumatları saxlaması və emal etməsidir. Bu tip məlumat bazalarında bəzən insanların həyatının asılı ola biləcəyi kritik məlumatlar mövcud olur.

Bundan əlavə Internetin yaratdığı imkanlar müxtəlif peşəkar sahələr kimi həkim və pasiyentlərin sosiallaşdığı tibbi virtual mühitin və tibbi şəbəkələrin də inkişafına səbəb olmuşdur. Pasientlər sosial media resurslarından istifadə etməklə: sağlamlıqları, xəstəlikləri ilə əlaqədar məlumatlar əldə edə bilirlər; müəyyən xəstəliyin müalicəsi ilə bağlı təcrübələrini bölüşə bilirlər; həkimlər haqqında məlumat əldə edə bilirlər; həkimlər ilə əlaqə saxlayıb məsləhət və tövsiyə ala bilirlər. Sosial media pasiyentlərlə yanaşı, həkimlər üçün də geniş imkanlar yaratmışdır. Hazırda sosial mediadan istifadə edən həkimlər: iş yerini tərk etmədən konsilium və konfransları izləmək; həmkarları ilə maraqlı diskussiyalar keçirmək; tibb bacılarına kliniki vəziyyətlərdə qərar qəbul etməkdə dəstək

olmaq; şəxsi potensialını yüksəltmək üçün peşəkar heyət yığmaq və s. kimi imkanlar əldə edirlər [1].

Digər tərəfdən TSM hər kəs üçün açıq və əlçatan olduğundan pasiyentlərin fərdi məlumatlarının məxfiliyi və təhlükəsizliyi üçün potensial təhdidlərə yol açır. Beləliklə, TİS ilə yanaşı TSM də pasiyentlərin fərdi məlumatlarının təhlükə mənbəyinə çevrilir. Ona görə də, avtomatlaşdırılmış informasiya sistemlərində və müxtəlif tibbi sosial şəbəkələrdə vətəndaşların fərdi məlumatlarının qorunması vacibdir.

II. TİBBİ İNFORMASIYA SİSTEMLƏRİNDƏ FƏRDİ MƏLUMATLARIN QORUNMASI PROBLEMLƏRİ

TİS tibb müəssisələrinin tibbi, inzibati, təsərrüfat və digər fəaliyyətini əhatə edən proseslərin və prosedurların kağız daşıyıcılardan elektron informasiya sistemə keçirilməsi vasitəsi ilə daha dəqiq təqib olunması, analitik və hesabat məlumatlarının operativ əldə olunması, uzun müddət ərzində toplanan məlumatların arxivləşdirilməsi, istənilən zaman vətəndaşların tibbi müayinə və müalicə məlumatlarının operativ şəkildə əldə olunmasına imkan yaradır [2].

E-tibbin yaradılması bir sıra əsas istiqamətlər üzrə əhəmiyyətli nəticələrin əldə olunmasını nəzərdə tutur: elektron tibb kartlarının tətbiqi, qeydiyyat işinin aparılmasının avtomatlaşdırılması, sənədləşmə və arxivləşdirmənin elektron formada aparılması, həkimin iş yerinin kompüterləşdirilməsi, pasiyentin və menecerin şəxsi kabinet, rəqəmsal resept, tətbiqin inkişafı, səhiyyə sistemində vahid informasiya fəzasının yaradılması, o cümlədən əhəlinin sağlamlıq vəziyyəti, epidemioloji sağlamlığının monitorinqi sistemlərinin inkişafı və s. elektron tibbin tətbiqi istiqamətlərindəndir. Pasientin elektron tibb kartı və ya elektron sağlamlıq kartı onun doğum günündən başlayaraq doldurulur və bu proses onun bütün həyatı boyu davam edir [3]. Fərdi məlumatların toplandığı elektron tibb kartı e-tibbin baza elementidir.

Dünya praktikasına görə də, TİS-də informasiya təhlükəsizliyi, məlumatların məxfiliyi, bütövlüyü və tamlığı təmin olunmalı və yalnız səlahiyyətli şəxslərin məlumatlara girişi mümkün olmalıdır. Təəssüf ki, bəzən şəxsi məlumatlardan yalnız xeyirxah məqsədlər üçün deyil, həm də fərdin, cəmiyyətin və dövlətin mənafeyinə zərər vurmaq üçün istifadə edilir. Buna görə də, səhiyyə sistemində informasiya təhlükəsizliyinin əhəmiyyəti son dərəcədə artır və ön plana çıxır [4,5].

Qanuni olaraq, xəstələr haqqında tibbi məlumatlar peşəkar sirri təşkil edən məlumatlara aiddir. Buna görə də, TİS-də həm fərdi məlumatların, həm də bütövlükdə informasiya sisteminin təhlükəsizliyini təmin etmək üçün bir sıra tədbirlər həyata keçirilməlidir, əks halda TİS-in istifadəsi qanunsuzdur.

Məlumatların təhlükəsizliyini və məxfiliyini təmin etmək müasir TİS-in istismarçılarına qoyulan əsas şərtlərdən biridir. Bu tələbin informasiya-kommunikasiya və hesablama sistemlərinə tətbiqi təxirəsalınmaz vəzifədir [6].

TİS-də fərdi məlumatların qorunması prosesindəki əsas problemlər aşağıdakılardır [7]:

- İnformasiyanın itkisi, təhrif olunması və saxtalaşdırılmasının qarşısının alınması;
- fərdin, cəmiyyətin və dövlətin məlumatlarının təhlükəsizliyinə təhdidlərin qarşısının alınması;
- məlumatı silmək, dəyişdirmək, təhrif etmək və surətini çıxarmaq üçün icazəsiz hərəkətlərin qarşısının alınması;
- informasiya mənbələri və sistemlərinə müxtəlif qanunsuz müdaxilələrin qarşısının alınması;
- sənədləşdirilmiş məlumatların mülkiyyət obyektinə kimi istifadəsinin qanuni rejiminin təmin edilməsi;
- vətəndaşların konstitusiyaya hüququ ilə informasiya sistemlərində mövcud olan fərdi məlumatların məxfiliyinin qorunması;
- informasiya sistemlərinin istismarı və tətbiqi sahəsində subyektlərin hüquqlarının təminatı.

Göründüyü kimi, TİS-də fərdi məlumatların qorunması məsələsinin iki aspekti təmsil olunur. Bunlardan birincisi, xəstələrin fərdi məlumatlarının qorunması haqqında qanunla tənzimlənən həkimlə xəstənin qarşılıqlı əlaqəsinin etik (peşəkar) tərəfidir. İkinci aspekt tibbi sistemdəki məlumatların texniki baxımdan qorunmasıdır, yəni məlumat sisteminin proqram-aparat kompleksi daxilində adekvat məlumat qoruma mexanizmlərinin yaradılmasıdır [7].

III. TİBBİ SOSIAL MEDİADA FƏRDİ MƏLUMATLARIN YAYILMASI

İnternet böyük imkanlar təqdim edən güclü alətdir və son bir neçə onillikdə onun geniş istifadəsi sayəsində insanları, təşkilatları və dövlətləri birləşdirən, onları bir-birindən qarşılıqlı asılı edən global kiberfəza formalaşmışdır. Real həyatda mövcud olan mənfi elementlər kiberfəzaya proyeksiyalanır və spamlar, viruslar, fərdi məlumatların ələ keçirilməsi, kibercinayətkarlıq, kiberterrorizm, kibermüharibə kimi təhdidlər yaranır [8].

Sosial şəbəkələrdən kütləvi surətdə istifadə olunması İnternet mühitində TSM-nin meydana gəlməsinə səbəb olmuşdur. Müxtəlif tibbi virtual qruplarda, bloklarda və şəbəkələrdə sosiallaşan insanlar şəxsi təcrübələrini, biliklərini, əldə etdiyi nailiyyətləri bölüşür, hər hansı bir probleminin həll

olmasında yardım edən insanlarla sevincini paylaşır, yaxud da məsləhət almaq məqsədilə şəxsi problemlərinin həlli üçün vacib suallarla müraciət edirlər. Tibb işçiləri, həkimlər sualları cavablandıraraq öz peşəkarlığını nümayiş etdirir və pasiyentlərlə qarşılıqlı ünsiyyətdə olmaq üçün virtual mühitdən istifadə edirlər. İnsanlar isə bu və ya digər həkimlərin müalicə metodu, təcrübəsi, əldə etdiyi nəticələr, müəssisədə tibbi xidmətin keyfiyyəti, müasir və yüksək dəqiqliyə malik avadanlıqlarla təhcizəti, pasiyent təhlükəsizliyi və s. ilə tanış olur, probleminin həlli üçün hansı xəstəxanaya və kimə müraciət edəcəyini dəqiqləşdirir. Qənaətbəxş nəticə əldə etməyən pasiyentlər xidmətindən narazı olduğu xəstəxanalar, müalicə metodu düzgün olmayan həkimlər, keyfiyyətsiz dərman vasitələri, və digər çatışmazlıqlar ilə bağlı məlumatı sosial şəbəkədə yerləşdirirlər. Bu fərdi məlumatların yayılmasının humanizm tərəfi bütün pasiyentlərin mövcud durumdan bəhrələnməsidir. Lakin, bəzən məlumatlar qərəzli (reklam və ya antireklam) şəkildə təhrif olunur. Göründüyü kimi, TSM-də fərdi məlumatların hamı tərəfdən əlçatan olmasının həm mənfi, həm müsbət tərəfləri vardır.

Hal-hazırda tibbi şəbəkələrdə həkimlərə müraciətlər zamanı nəinki pasiyentlərin fərdi məlumatları, hətta onların sorğularını cavablandıran həkimlərin verdiyi məsləhət, təyin etdiyi diaqnoz, müalicə üsulu və s. də şəbəkələrdə hər kəsə açıq və əlyetən olur. Bu da onların fərdi, sağlamlıq vəziyyəti ilə bağlı məlumatlarının konfidensiallığı üçün təhlükə yaradır [9].

Bu problemin aradan qaldırılması üçün 80-dən çox tibb ixtisasını və 18 mindən çox həkimi əhatə edən “healthcaramagic.com” tibbi sosial şəbəkəsinin təhlükəsizlik siyasətindən yararlanmaq olar. Bu şəbəkədə pasiyentlər həkimlərə müraciət edərkən cavabları onların e-mail ünvanına göndərilir. doslovno.com və health.mail.ru şəbəkələrində isə pasiyentlər qeydiyyatdan keçərkən adı, yaşı, yaşadığı ərazi, e-mail ünvanı ilə bağlı göstərdikləri fərdi məlumatların konfidensiallığının təmin edilməsi məqsədilə sorğuların və həkim cavabının “hər kəsə açıq” olub-olmaması ilə bağlı onların rəyi öyrənilir [10].

NƏTİCƏ

Hal-hazırda qloballaşan dünyamızda günbəgün inkişaf edən İKT-nin tibb sahəsinə də tətbiqi təbii prosesdir. Aparılmış araşdırmalar göstərir ki, TİS və TSM həkim-pasiyent münasibətlərində vacib amilə çevrilmişdir. Lakin, TİS-in səhiyyənin inkafında əvəzolunmaz faydası olmasına baxmayaraq qeyri-peşəkar istifadəçilər tərəfindən fərdi məlumatların təhrif olunmasına və TSM istifadəçilərinin sayının fasiləsiz artması isə fərdi məlumatların yayılmasına səbəb olur.

Bu baxımdan elektron mühitdə tibbin normativ-hüquqi bazasının formalaşdırılması, proqram-texniki bazasının təkmilləşdirilməsi, peşəkar kadrların hazırlanması, fərdi tibbi məlumatların online mühitdə təhlükəsizliyinin təmin olunması istiqamətində yeni texnologiyaların və proqram təminatının formalaşması məsələlərinin araşdırılması zəruridir.

İSTİNADLAR

- [1] M.H. Məmmədova, A.M. İsayeva, “Sosial media mühitində e-tibb fəaliyyəti”, İnformasiya cəmiyyəti problemləri, 2018, №1, s.57–68.
- [2] Nümunəvi tibbi-informasiya sistemi, <http://e-sehiyye.gov.az/az/s/9/N%C3%BCmun%C9%99vi+tibbi-informasiya+sistemi>
- [3] Elektron tibb sağlamlığının qorunması məqsədilə İKT-dən istifadəni nəzərdə tutur, <https://ict.az/az/news/694/>
- [4] А.П. Бирюков, Е.В. Васильев, С.М. Думанский, О.А. Тихонова, Ю.А. Герт, Н.В. Капитонова, “Выбор компьютерных технологий для аналитической поддержки базы данных крупномасштабных медицинских информационных систем”, Саратовский научно-медицинский журнал, 2013, № 9(4), с.983–987.
- [5] В.В. Домарев, “Защита информации в медицинских информационных системах: врачебная тайна и современные информационные технологии”, Клиническая информатика и телемедицина, 2004, №1(2), с.147–154.
- [6] Я.И. Гулиев, И.А. Фохт, О.А. Фохт, А.Ю. Белякин, “Медицинские информационные системы и информационная безопасность. Проблемы и решения”, Программные системы: теория и приложения: тр. междунар. конф. Переславль-Залесский, 2009, с.175–206.
- [7] М.К. Карабаев, А.А. Абдуманов “Алгоритмы и технологии обеспечения безопасности информации в медицинской информационной системе ExterNET”, Программные продукты и системы 2013, №(1), с.150-155.
- [8] Н.В. Юргель, Е.Л. Никонов, И.В. Гармаш, Л.Ю. Мерзлов, И.Г. Поздняков, “Защита информации в регистре медицинских и

фармацевтических работников”, Вестник Росздравнадзора, 2008, № (1), с.75-76.

- [9] Y.N. İmamverdiyev “İnformasiya təhlükəsizliyi üzrə beynəlxalq koalisiya modeli”, İnformasiya cəmiyyəti problemləri, 2019, №1, s.14–20.
- [10] M.H. Məmmədova, Z.Q.Cəbrayıllova, A.M. İsayeva “Sosial media mühitinin həkim-pasiyent münasibətləri seqmentinin analizi: imkanlar və problemlər”, İnformasiya cəmiyyəti problemləri, 2019, №2, s.41–50.

ACTUAL PROBLEMS OF PROTECTION OF PATIENTS' PERSONAL DATA IN ELECTRONIC ENVIRONMENT

Kamala Gurbanova

Institute of Information Technology of ANAS, Baku, Azerbaijan
kemalewamil@gmail.com

Abstract– The study investigates the application of information and communication technologies which allows the dissemination of personal information of patients to medical fields. The problems posed by medical information systems and medical social media in the Internet environment have been explained. It is recommended to create a legal framework for medicine in the electronic environment, to improve the software and hardware, to create a professional staff and to develop new technologies to ensure security.

Keywords– *medical information systems; medical social media; confidential information; personal data security*

Проблемы защиты информации субъектов электронного университета в облачной среде

Фирудин Агаев¹, Гюляра Мамедова², Эмира Алескерова³

^{1,2,3}Институт Информационных Технологий НАНА, Баку, Азербайджан

¹depart10@iit.science.az, ²gyula.ikt@gmail.com

Аннотация— В этой статье определены различные проблемы безопасности электронного образования при предоставлении облачных сервисов и предложены решения по обеспечению мер безопасности. Также обсуждаются различные типы атак на платформы электронного обучения. Исследуются различные модели использования облачных технологий в электронном образовании, угрозы и требования безопасности при использовании этих моделей.

Ключевые слова— электронный университет, модели доставки облачных услуг, контроль идентификации и аутентификации, защита облачного сервера, MITM атаки, DDoS атака, инсайдерские атаки.

I. ВВЕДЕНИЕ

Электронное обучение на основе облачных технологий – одна из быстро развивающихся информационных технологий, которая предлагает мощные продукты электронного обучения с помощью облачных технологий [1-2]. Облачные технологии имеют многочисленные преимущества по сравнению с существующими традиционными системами электронного обучения, но в то же время безопасность является серьезной проблемой в облачном электронном обучении. Чтобы предотвратить потерю ценных данных пользователей из-за уязвимостей безопасности, необходимо соблюдать соответствующие меры безопасности. Облачные продукты электронного обучения должны удовлетворять потребностям клиентов в безопасности и преодолевать различные угрозы безопасности. В работе мы рассматриваем ключевые проблемы безопасности при использовании облачных вычислений в системах электронного обучения.

II. ОБЛАЧНАЯ АРХИТЕКТУРА ЭЛЕКТРОННОГО ОБУЧЕНИЯ

Облачная архитектура электронного обучения в основном разделена на пять уровней [3], называемых: уровнем аппаратных ресурсов, уровнем программных ресурсов, уровнем управления ресурсами, уровнем сервера и уровнем приложений. Облачная архитектура электронного обучения поясняется на рис. 1.

Уровень аппаратных ресурсов – это самый нижний уровень облачной инфраструктуры, которая обеспечивает вычислительную мощность электронного образования.

Чтобы обеспечить бесперебойную работу облачных сервисов для систем электронного обучения, физическая память динамически расширяется, и в любое время масштабируется для добавления дополнительной памяти.

Уровень программных ресурсов включает операционную систему и прикладное программное обеспечение для разработчиков и пользователей облачной инфраструктуры.

Уровень управления ресурсами играет важную роль в слабой взаимосвязи программных и аппаратных ресурсов. С помощью идеи виртуализации она обеспечивает бесперебойное распространение программного обеспечения по требованию для различных аппаратных ресурсов облачной инфраструктуры.

Уровень обслуживания делится на три уровня: IAAS (Инфраструктура как сервис), PAAS (Платформа как сервис) и SAAS (Программное обеспечение как сервис). Эти сервисные уровни помогают облачным клиентам использовать различные виды облачных сервисов, таких как, программный сервис, аппаратный сервис и сервис инфраструктуры.

Рис.1. Облачная архитектура электронного образования.

Уровень приложений отличается от всех других уровней в архитектуре электронного обучения на основе облачных вычислений, поскольку создает основу компонентов для электронного обучения и служит для создания учебного контента, доставки контента,

образовательной платформы, оценки обучения и управления образованием.

III. ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ СЕРВИСОВ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ ДЛЯ ЭЛЕКТРОННОГО ОБРАЗОВАНИЯ

Как было показано выше, существуют три модели доставки облачных услуг: 1. Программное обеспечение как сервис (SaaS), 2. Платформа как сервис (PaaS) (), 3. Инфраструктура как сервис (IaaS). В этой статье рассматриваются вопросы безопасности в каждой из этих групп.

Программное обеспечение как сервис (SaaS) – позволяет совместно работать нескольким пользователям с готовым программным обеспечением. Поэтому в SaaS пользователь полностью зависит от поставщика программного обеспечения. Для обеспечения надлежащих мер безопасности поставщик программного обеспечения должен обеспечить безопасность учебных данных, так, чтобы было невозможно нескольким пользователям видеть данные друг друга. Учебное заведение должно быть уверенным, что поставщик облачных сервисов будет обрабатывать данные только в соответствии с его инструкциями, что он принял соответствующие меры, чтобы исключить неавторизованный доступ к данным, их изменение или уничтожение.

Платформа как сервис (PaaS) предоставляют вычислительную платформу и системное программное обеспечение как услугу. PaaS предоставляет сервисные услуги для разработчиков программного обеспечения. Сюда можно отнести такие платформы, как, Google App Engine, Salesforce, Windows Azure и др., позволяющие создавать программы и корпоративные сайты на языках Java и Python. Поставщики PaaS предоставляют услуги для разработки приложений, развертывания, коллективного сотрудничества, интеграции веб-сервисов и тестирования [4].

Основными угрозами безопасности уровня PaaS являются местоположение данных и привилегированный доступ. В США и во многих странах ЕС были установлены универсальные стандарты безопасности и законы о конфиденциальности данных для проблем с размещением данных. Например, общим регламентом по защите данных (GDPR — General Data Protection Regulation) от 27 апреля 2016 г., действующем во всех странах ЕС, они никогда не позволяют конфиденциальным данным перемещаться из страны [5-6]. За нарушение правил обработки персональных данных, штрафы достигают миллионы евро.

Основываясь на местоположении данных, модель PaaS обеспечивает надежность для своих клиентов. Для обеспечения надежного хранения данных на уровне PaaS, пользователь должен выбрать надежный метод шифрования для доступа к данным, поддерживать высокую стандартную конфиденциальность данных, требовать от облачного провайдера юридически

оформленные договорные обязательства механизмов обеспечения безопасности. Поставщик облачных услуг должен иметь технические решения для предотвращения несанкционированного доступа пользователей и поддерживать принцип разделения обязанностей для привилегированных пользователей с целью предотвращения и обнаружения вредоносной инсайдерской деятельности.

При хранении зашифрованных данных в облачном хранилище ключи дешифрования должны надежно храниться в других дезинтегрированных системах [7-8]. Если облачная пользовательская система позволяет поставщику облачных услуг обрабатывать незашифрованные данные, поставщик облачных услуг должен гарантировать, что данные будут защищены от несанкционированного доступа как внутри, так и снаружи.

Инфраструктура как сервис (IaaS) позволяет использовать множество ресурсов, таких как серверы, хранилища, сети и другие вычислительные ресурсы, представляет собой хостинг для виртуальной машины. В случае, если IaaS обеспечивает полный контроль и управление ресурсами, пользователи могут с безопасностью запускать любое программное обеспечение на выделенных ресурсах. В этом случае, между пользователем и облачным провайдером заключается соглашение об уровне сервиса SLA (Service Level Agreement), в котором содержится описание предоставляемых услуг, прав и обязанностей сторон. В этом соглашении содержится детальное описание предоставляемых сервисов, методов и средств контроля по обеспечению безопасности информации.

Основными видами угроз в электронном образовании при предоставлении IaaS услуги являются DDoS атаки (Distributed Deny of Service Attack), MITM атака (Man In The Middle), DNS атаки, и др. Цель DDoS атаки заключается в том, чтобы сделать облачную услугу недоступной для авторизованного пользователя. В этом случае злоумышленниками используется SYN-флуд (запросы на подключение по протоколу TCP), при котором весь канал сервера просто забивается запросами на подключение. SYN-флуд является одним из разновидностей сетевых атак типа «отказ в обслуживании», который заключается в отправке большого количества SYN-запросов, переполняя на облачном сервере очередь на подключение.

Другой распространенной угрозой при предоставлении IaaS услуги является MITM атака, когда злоумышленник внедряет себя между двумя законными пользователями сети. Злоумышленник устанавливает соединение между двумя пользователями и пытается завладеть информацией, пересылаемой ими друг другу [9].

В последнее время в облачной среде, использующей IaaS сервис, хакерами применяется такой вид атаки, известный как DNS атака, при котором хакер перенаправляет пользователя на другую виртуальную

машину облака вместо исходного адреса, который он ожидает. Ничего не подозревающий пользователь соединяется с хостом нарушителя и, полагая, что работает на сайте учебного заведения, вводит конфиденциальную информацию на подложный IP адрес. При DNS атаке злоумышленник получает возможность мгновенно менять параметры транзакции, а также страницы запроса пользователя совершенно прозрачно для жертвы.

IV. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ СЕРВИСОВ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ ДЛЯ ЭЛЕКТРОННОГО ОБРАЗОВАНИЯ

При предоставлении облачных сервисов для электронного университета, для обеспечения безопасности информации, особое внимание требует уделить защите аппаратных и виртуальных устройств обработки данных, а также каналов связи. Необходимо обеспечить следующие критерии безопасности [10-11]:

- контроль идентификации и аутентификации субъектов и объектов доступа;
- защиты машинных носителей информации;
- обеспечение необходимого уровня криптографической и антивирусной защиты хранимой и передаваемой информации;
- защита облачного сервера, средств связи и передачи данных;
- принятие мер по межсетевому экранированию.

Чтобы защитить данные от утечки конфиденциальной информации, необходимо применять жесткие методы шифрования сетевого трафика для управления потоком данных в сети: Secure Socket Layer (SSL) и Transport Layer Security (TLS). Эти уровни обеспечения безопасности позволят защитить от традиционных сетевых проблем, таких как атаки MITM, IP-спуфинг, сканирование портов, обнюхивание пакетов и т. д.

Атаки сегодня стали сложными и многоуровневым, злоумышленники выбирают конкретные цели и долго готовятся к нападению, чтобы ударить именно в наиболее уязвимые элементы. Эволюция интернет-угроз закономерно повлияла и на развитие средства противодействия им. Сегодня наиболее эффективными инструментами защиты облачных ресурсов от внешних атак из сети – это решения класса Cloud Access Security Broker (CASB), направленные на удовлетворение новых требований безопасности. CASB представляет собой унифицированный инструмент контроля за всеми облачными приложениями, ресурсами и сервисами, контролирует взаимодействие между облачными приложениями (доступ, трафик, загрузку и хранение данных), сервером и внешними пользователями, позволяет выявлять потенциальные угрозы и ориентирован на высокий уровень защиты облачной среды [12-13]. CASB предотвращает несанкционированные действия пользователей,

обнаруживает аномальную активность, в том числе, связанную с действиями различных вредоносных программ. По данным, опубликованным агентством Gartner в 2019 г., лидерами рынка обеспечения безопасности облачных услуг являются: Skyhigh Networks, Netskope, Symantec [14-15].

А появившийся недавно пакет программ CloudSOC Security for Cloud Apps [16] контролирует в реальном времени транзакции с санкционированными (разрешенными) и несанкционированными облачными приложениями; осуществляет визуализацию карты активности пользователей для быстрого анализа их действий; защищает от угроз, основанных на обширной аналитике поведения пользователей. Он обеспечивает богатую наглядность, контроль перемещения данных и сложную аналитику для выявления и борьбы с киберугрозами во всех ваших облачных сервисах.

Применение инструментов CASB в электронном образовании позволят, анализируя журналы «регистрации» и «геолокации», данные о времени совершения тех или иных действий в «облаке», отслеживать действия пользователей выявлять угрозы в реальном времени, идентифицировать небезопасные приложения. В эти пакеты встроены средства машинного обучения, предусматривающие возможность отслеживать поведенческие действия пользователей и их отклонение от нормы. Посредством анализа индикаторов риска, таких как: небезопасные IP-адреса, сбои при регистрации, уровень активности, неактивные учетные записи, сценарии «невозможных путешествий» и их локация, своевременно выявлять злоумышленников в сети.

ЗАКЛЮЧЕНИЕ

Проблема доступности данных в электронном образовании является основным препятствием для обеспечения безопасности облачных данных. Литературное исследование ясно показывает риски в электронном обучении на основе облачных вычислений, а также его модели предоставления услуг и эффективные решения для каждой атаки. Перечисленные проблемы безопасности важны для управления и новой методологии разработки безопасного электронного обучения на основе облачных вычислений в будущем.

Основной целью работы является выяснение ключевых проблем безопасности, возникающих при реализации облачных вычислений для систем электронного обучения. Разработка систем электронного обучения должна осуществляться с использованием методов безопасности и международно признанных стандартов. Система должна реализовать службы безопасности, такие как, аутентификация, шифрование, контроль доступа, управление пользователями и их разрешениями.

ЛИТЕРАТУРА

- [1] N. Antonopoulos, L. Gillam. Cloud Computing: Principles, Systems and Applications. London: Springer-Verlag, 2010. 379 p

- [2] Н. Склейтев. Облачные вычисления в образовании. Аналитическая записка. Пер. с англ. Институт ЮНЕСКО по информационным технологиям в образовании (ИИТО ЮНЕСКО). 2010. <http://iite.unesco.org/pics/publications/ru/files/3214674.pdf>.
- [3] К. Фогарти “Облачные вычисления: определения и решения,” Открытые системы, 2011, № 3. <http://www.osp.ru/cio/2011/03/13007508>.
- [4] В. Ф. Шаньгин, Информационная безопасность компьютерных систем и сетей. – М.: ИД «ФОРУС»: Инфра-М, 2008. – 416 с. https://ec.europa.eu/info/law/law-topic/data-protection_en
- [5] А. Пазюк, М. Соколова. Защита персональных данных: международные принципы и стандарты. 2015. 23 р. <https://www.researchgate.net/publication/281459857>
- [6] А.В. Ерыгин Анализ эффективности систем предотвращения утечек конфиденциальной информации из локальных сетей. Вестник СибАДИ, выпуск 2 (20), 2011, с. 40-47.
- [7] M.Jensen, J.Schwenk, N.Gruschka, & L.Iacono “On technical security issues in cloud computing,” IEEE International Conference on Cloud Computing, pp.109-116, 2009.
- [8] F. Callegati, W. Cerroni, & M. Ramilli “Man-in-the-Middle Attack to the HTTPS Protocol,” IEEE Security & Privacy, 7(1), pp. 78-81, 2009.
- [9] E. B. Fernandez, N. Yoshioka, and H. Washizaki, “Patterns for cloud firewalls”, Procs. of AsianPLOP (AsianPattern Languages of Programs), 2014
- [10] Исаев Е.А., Думский Д.В., Самодуров В.А., Корнилов В.В. Обеспечение информационной безопасности облачных вычислений Математическая биология и биоинформатика, 2015. Т. 10. № 2. С. 567–579.
- [11] H. Reza, M. Sonawane, "Enhancing mobile cloud computing security using steganography," Journal of Information Security, 2016, pp. 245-259.
- [12] https://www.anti-malware.ru/analytics/Market_Analysis/cloud-access-security-broker
- [13] <https://www.gartner.com/reviews/market/cloud-access-security-brokers/co-mpare/symantec-blue-coat-vs-skyhigh-networks>
- [14] C. Lawson, S.Riley “Magic Quadrant for Cloud Access Security Brokers”. Gartner. 29 October 2018. https://www.bsigroup.com/globalassets/local-files/enie/csir/resources/whitepaper/1810-magic_quadrant_for_casb.pdf
- [15] <https://www.symantec.com/content/dam/symantec/docs/data-sheets/cloud-soc-gateway-en.pdf>

INFORMATION SECURITY PROBLEMS OF E-UNIVERSITY IN CLOUD ENVIRONMENT

Firudin Aghayev¹, Gyulara Mammadova², Esmira Aleskerova³

^{1,2,3}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹depart10@iit.science.az, ²gyula.ikt@gmail.com

Abstract– This article identifies various security issues of e-education in the provision of cloud services and proposes solutions to ensure security measures. Various types of attacks on e-learning platforms are also discussed. Various models of the use of cloud technologies in electronic education, threats and security requirements when using these models are investigated.

Keywords– *electronic university, cloud service delivery models, identification and authentication control, cloud server protection, MITM attacks, DDoS attacks, insider attacks.*

Методы обеспечения безопасности персональных данных в электронном образовании

Гюляра Мамедова¹, Лала Зейналова², Рена Меликова³
^{1,2,3}Институт Информационных Технологий НАНА, Баку, Азербайджан
¹gyula.ikt@gmail.com, ²lalamailala@bk.ru

Аннотация— В последние годы популярность электронного образования набирает обороты. В связи с этим возникает проблема обеспечения его безопасности, которая должна осуществляться с использованием методов безопасности и международно-признанных стандартов. В этой статье определены различные проблемы безопасности персональных данных в электронном образовании и предложены решения по обеспечению защиты учебной информации.

Ключевые слова— электронный университет, защита учебной информации, межсайтовый скриптинг, SQL атака, безопасная аутентификация, цифровая подпись

I. ВВЕДЕНИЕ

В высшем учебном заведении используется разнообразная информация, требующая защиты. Это – персональные данные студентов, преподавателей, администрации и других категорий пользователей. Сюда также можно отнести сведения, составляющие коммерческую тайну университета (образовательные программы и учебные материалы, результаты научно-исследовательских работ и т.д.), позволяющие ему опережать другие ВУЗы в области предоставления более качественного образования, более прогрессивных методов обучения, лучших образовательных программ.

Исследовательская и консалтинговая компания Gartner [1], специализирующаяся на рынках информационных технологий, прогнозирует, что расходы на информационную безопасность в мире превысят 124 миллиарда долларов в 2019 году и будут влиять на различные сегменты, такие как, управление идентификацией и доступом (IAM – identity and access management), управление идентификацией и администрированием (IGA – identity governance and administration), предотвращение потери данных (DLP – data loss prevention).

Выполнение требований безопасности в системе электронного обучения является чрезвычайно сложной проблемой, поскольку, необходимо защищать контент, услуги и личные данные не только для внешних пользователей, но и для внутренних пользователей, включая системных администраторов. Обучающая система должна реализовать такие службы безопасности, как аутентификация, шифрование, контроль доступа,

целостность данных, защиту контента и управление пользователями. В этой статье мы рассмотрим некоторые ключевые проблемы безопасности, которые необходимо учитывать при разработке и использовании электронного обучения.

II. СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ЭЛЕКТРОННОГО УНИВЕРСИТЕТА

Основными методами обеспечения безопасности информации в электронном образовании являются [2-4]:

- Организационные средства защиты. Используются для ограничения доступа (исключает доступ к информации посторонних лиц); разграничения доступа - разделение информации на части и организация доступа к ней в соответствии с функциональными обязанностями и полномочиями пользователя; контроль доступа – определение подлинности субъекта, имеющего доступ к информации.
- Аппаратные средства защиты. К ним относятся – защита от сбоев работы сервера, защита от сбоев устройств для хранения информации, защита от утечек информации, электромагнитных излучений.
- Программные средства защиты – для выявления технических устройств и программ, представляющих опасность для нормального функционирования электронного образования.

Безопасная обучающая платформа должна включать следующие основные аспекты безопасности:

- доступность учебной информации (возможность за разумное время получить требуемую информацию);
- целостность (защищенность учебного контента от разрушения и несанкционированного изменения);
- конфиденциальность (защита персональных данных, учебного контента и менеджмента системы от несанкционированного доступа).

Основными элементами реализации угроз учебным данным в компьютерной сети университета могут быть

объекты или субъекты, создающие эти угрозы, коммуникационная среда распространения персональных данных, носители (материальный объект, в котором персональные данные находят свое отражение в виде текста, видео и звуковой информации).

Защищенность данных тесно связана с целостностью программ и операционных систем. Если нарушается целостность операционной системы, тогда контрольный монитор может перестать работать должным образом. Контрольный монитор – это механизм, который гарантирует, что только уполномоченные субъекты могут получить доступ к данным и выполнять операции. Очевидно, что защита информации не может быть гарантирована, если не работает механизм проверки и ограничения доступа к данным. По этой причине, чтобы защищать сами данные, важно защитить целостность операционных систем. [5].

Безопасная аутентификация требуется для идентификации пользователя и определения его прав доступа при использовании веб-приложений. Этот механизм не позволяет злоумышленникам получить доступ к учетной записи другого пользователя, просмотреть конфиденциальную информацию или выполнить несанкционированные операции. Кроме того, после аутентификации пользователь должен иметь возможность изменить свой пароль.

Контроль доступа во время аутентификации ограничивает доступ к системе неавторизованных пользователей и позволяет пользователю выполнять в системе только свои разрешенные операции (администратор, редактор, инструктор, студент, зарегистрированный пользователь, незарегистрированный пользователь и т. д.).

На Рис.1 представлена обобщенная схема обеспечения безопасности электронного университета.

Рис. 1. Обобщенная система обеспечения безопасности электронного университета

III. МЕТОДЫ ЗАЩИТЫ УЧЕБНОЙ ИНФОРМАЦИИ В ЭЛЕКТРОННОМ ОБРАЗОВАНИИ

При внедрении системы электронного обучения в учебном заведении она должна быть проверена на внешние проблемы вторжения, такие как:

- межсайтовый скриптинг (XSS – Cross-Site Scripting);
- удаленная инъекция с использованием файла вируса / трояна;
- SQL инъекция в адрес сайта (URL SQL инъекция);
- взлом паролей с использованием систем дешифрования;
- угадывание идентификатора сессии веб-сайта (прогноз сессии).

Межсайтовый скриптинг – одна из самых распространенных веб-атак на уровне приложений. XSS обычно предназначается для скриптов, встроенных в страницу, которые выполняются на стороне клиента (в веб-браузере пользователя) [6-8]. Сам по себе XSS - это угроза, вызванная слабостью интернет-безопасности языков сценариев. Концепция XSS заключается в том, чтобы манипулировать сценариями на стороне клиента веб-приложения, чтобы они выполнялись так, как этого хочет злоумышленник. Такая манипуляция может встраивать скрипт в страницу, который затем может выполняться каждый раз, когда страница загружается, или всякий раз, когда выполняется соответствующее событие. Атака XSS может быть использована для достижения следующих целей:

- доступ к конфиденциальной информации;
- кража личных данных;
- изменение функциональности браузера;
- порча веб-приложений;
- отказ в обслуживании.

На рис 2. показаны наиболее уязвимые участки распространения угроз учебным данным в компьютерной сети университета [9].

Рис.2. Наиболее уязвимые места в компьютерной сети университета для распространения угроз учебной информации.

Отказ в обслуживании означает, что пользователь (студент или преподаватель) не может выполнить в системе соответствующие действия. Допустим, что учитель удаляет результаты экзамена своего ученика. В этом случае должна предусматриваться возможность отследить, кто их удалил с помощью некоторого файла сценария. Эти файлы сценариев должны быть надежными и защищенными от подделки. Для выполнения этого требования используется механизм аудита.

Чтобы предотвратить такую атаку, необходимо, чтобы разработчик платформы электронного обучения обеспечил безопасность использования веб-страницы, чтобы страницы на веб-сайте возвращали пользовательские данные только после проверки их на наличие вредоносного кода. Необходимо широко использовать инструменты тестирования на этапе проектирования, чтобы устранить возможность XSS атак в приложения электронного обучения, прежде чем оно будет введено в эксплуатацию.

Следующий вид атаки это – SQL атака [10-12]. Используя этот метод атаки, хакеры вводят SQL-запросы или символы в веб-приложение, с целью получить несанкционированный доступ к базе данных. Такие запросы могут привести к доступу к неавторизованным данным в обход аутентификации. Эту угрозу можно избежать при строгом соблюдении некоторых основных практик кодирования. Наиболее распространенные методы предотвращения такой уязвимости:

- проверка при вводе SQL-запросов пользователем на наличие опасных символов, например, одинарных кавычек;
- шифрование конфиденциальных данных;
- обеспечение того, чтобы сообщения об ошибках не уведомляли нежелательных пользователей о внутренней архитектуре приложения или базы данных.

SQL-атака может применяться также для URL-адресов [13], которые могут быть изменены злоумышленником

для доступа к важной информации. Чтобы предотвратить это, желательно избегать отправки важных параметров в URL. Это достигается путем передачи уникального и трудно угадываемого значения идентификатора (идентификатора сеанса), который браузер отправляет при каждом новом запросе либо в файл cookie, либо в URL. Сеансы – это способ сохранения переменных состояния и пользователя для последующих запросов страниц. Сессия жива до тех пор, пока браузер продолжает отправлять идентификатор с каждым новым запросом. Прогнозирование сеанса означает угадывание действительного идентификатора сеанса с использованием различных инструментов и методов (например, техника грубой силы). Атака возможна, когда идентификатор сессии слабо зашифрован, слишком короткий или назначен последовательно.

Сессии, которые не истекают на сервере HTTP, могут позволить злоумышленнику неограниченное количество времени угадать или перебрать действительный аутентифицированный идентификатор сеанса и в конечном итоге получить доступ к веб-учетным записям этого пользователя. Кроме того, идентификатор сеанса может быть зарегистрирован и кэширован на прокси-серверах. При передаче через URL адреса, GET-запросы могут сохраняться в истории браузера, кэше и закладках, которые можно увидеть. Для предотвращения проблем, связанных с безопасностью сеанса, следует придерживаться следующих рекомендаций:

- идентификатор сессии должен быть достаточно длинным и непредсказуемым;
- проверить правильность идентификатора сеанса;
- избежать опции «запомнить меня» (постоянные входы в систему);
- остановить сеанс при обнаружении ошибки безопасности;
- остановить сеанс после периода бездействия;
- удалить cookie сессию, когда сессия уничтожена.

Хорошей практикой для обеспечения безопасности и целостности данных является межсайтовая репликация [14], которая также повышает скорость обработки данных.

ЗАКЛЮЧЕНИЕ

В этой статье мы описали некоторые аспекты безопасности платформ электронного обучения и, в частности, проанализировали наиболее важные проблемы, как, межсайтовый скриптинг, SQL атаки, взлом паролей и т.д. Разработка систем электронного обучения должна осуществляться с использованием методов безопасности и международно-признанных стандартов. Система должна реализовать службы безопасности, такие как аутентификация, шифрование, контроль доступа, управление пользователями и их разрешениями. Передача данных между системой и администраторами или операторами контента должна осуществляться по

зашифрованным каналам SSL через интерфейс веб-администрирования.

ЛИТЕРАТУРА

- [1] <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>.
- [2] В. В. Гафнер, Информационная безопасность / В.В. Гафнер. - М.: Феникс, 2017. 336 с.
- [3] Урбанович, П. П. Информационная безопасность и надежность систем – Минск: БГТУ, 2007. 90 с.
- [4] Васильков, А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - М.: Форум, 2017. 368 с.
- [5] G. Gagne, P. B. Galvin, A. Silberschatz? Operating System Concepts, Publisher: John Wiley & Sons, 2012, p. 312.
- [6] Носиров З. А., Ажмухамедов И. М. Обнаружение XSS-уязвимостей на основе анализа полной карты веб-приложения. Системы управления, связи и безопасности. №1, 2018, с. 78-92.
- [7] S. Fogie, J. Grossman, R. Hansen, A. Rager, P. Petkov. XSS attacks: Cross Site Scripting exploits and defense – Seth Fogie, Oxford: Elsevier Limited, 2007. 448 p.
- [8] M. Denis, C. Zena, T. Hayajneh, “Penetration Testing: Concepts, Attack Methods, and Defense Strategies”, ISBN: 978-1-4673-8490-2, DOI: 10.1109/LISAT. 2016.
- [9] Защита информации и надежность информационных систем «Белорусский государственный технологический университет». Методические указания и контрольные задания для студентов, Минск 2012. https://elib.belstu.by/bitstream/123456789/3372/1/zashhita-informacii-i-nadezhnost_-urbanovich-dlya-z.o..pdf.
- [10] K. Ahmad, J. Shekhar, K.P. Yadav. Classification of SQL Injection Attacks. VSRD Technical & Non-Technical Journal Vol. I (4), 2010, pp. 236-242.
- [11] Maraj, G. Jakupi, E. Rogova, Xh. Grajquevci, “Testing of network security systems through DoS attacks” , “Mediterranean Conference on Embedded Computing (MECO 2017), IEEE/Scopus conference, Montenegro, June 2017.
- [12] Z. S. Alwan , M. F. Younis. Detection and Prevention of SQL Injection Attack: A Survey. International Journal of Computer Science and Mobile Computing, Vol.6, Issue.8, August- 2017, pp. 5-17.
- [13] J. Clarke. SQL Injection Attacks and Defense. Elsevier, 2012, p.761.
- [14] [14] Романенко, Д. М. Основы сетевого администрирования. Минск: БГТУ, 2015. 135 с.

PERSONAL DATA SECURITY METHODS IN ELECTRONIC EDUCATION

Gyulara Mammadova¹, Lala Zeynalova², Rena Malikova³

^{1,2,3}Institute of Information Technology of ANAS, Baku, Azerbaijan

gyula.ikt@gmail.com, lalamaillala@bk.ru

Abstract – In recent years, the popularity of e-learning is gaining momentum. In this regard, there is a problem to ensure its security, which must be carried out using safety practices and internationally recognized standards. This article identifies various security issues in e-education and proposes solutions to ensure security measures.

Key words – *e-university, educational information protection, crossite scripting, SQL attack, secure authentication, digital signature*

İnternet-reklam və marketing fəaliyyətində fərdi məlumatların təhlükəsizliyi

Kəmalə Haşimova
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
multimedia@iit.science.az

Xülasə— İnternetin əhatəsi genişləndikcə, texnologiyaların imkanları çoxaldıqca, onlayn reklamlara tələbat artır. Tədqiqatda internet üzərində reklam-marketingin imkanları, saytlarda qeydiyyat təhlükəsizliyi, fərdi məlumatların təhlükəsizlik perspektivləri araşdırılmış, təhlükələr müəyyən edilmişdir. Həmçinin veb saytlarda sorğulardan toplanan məlumatların reklam-marketing sistemlərində səmərəli istifadəsi üçün təkliflər verilmişdir.

Açar sözlər— *İnternet reklam-marketing; kuki faylları; fərdi məlumat; veb səhifə; onlayn-reklam*

I. GİRİŞ

Müasir dövrdə informasiya texnologiyalarının inkişafı və informasiya cəmiyyətinin formalaşması ilə çox böyük dəyişikliklər müşahidə olunur. İqtisadiyyatın inkişafında önəmli rol oynayan aspektlərdən ən əsası internetdir.

Əhalinin rifah halının yüksəldilməsi və vətəndaş məmnunluğunu yüksəltmək üçün son illərdə bir çox qurumlar fəaliyyətə başlamışdır ki, buna “DOST”, “ASAN XİDMƏT” “ASAN KOMMUNAL” mərkəzlərini göstərmək olar. Bu kimi xidmət müəssisələri tam olaraq internet üzərində fəaliyyət göstərir. Əhali vaxt itirmədən istədiyi sənədi əldə edə bilər.

Elektronlaşdırılmış məkanda bütün fərdi məlumatların dövlət qurumu tərəfindən qorunmasına heç bir şübhə yoxdur. Lakin sosial şəbəkələrdə və ya qeydiyyatdan keçdiyimiz onlayn alış-veriş saytlarında məsələ fərqlidir.

Virtual məkanda rast gəldiyimiz internet-reklam həm maddi, həm də mənəvi tərəfdən əlverişlidir. Məhsulu əldə etmək üçün qeydiyyat qaçılmazdır.

II. BRAUZERDƏ QEYDİYYATIN ROLU

Müştəriyə uyğun reklam və xidmətlər göstərmək üçün saytlarda toplanmış fərdi məlumatlardan istifadə edilir. Belə məlumatlara axtarış sorğuları, məkan tarixi, istifadə etdiyimiz saytlar, baxdığımız video və reklamlar, cins, yaş və maraqlar kimi parametrlər daxildir. Reklam parametrlərindən asılı olaraq, yuxarıdakı məlumatlar hesaba daxil olduğumuz bütün cihazlarda və ya tərəfdaşların saytlarında reklam göstərmək üçün istifadə edilə bilər. Məsələn, işləyən bir kompüterdə bir səyahət agentliyinin saytına daxil olduqdan sonra aviaşirkət

biletlərinin reklamı bizim smartfonumuzdakı brauzerdə görünür.

Şəxsiyyəti müəyyən etməyə imkan verən məlumat üçüncü tərəfə ötürülməməlidir [1].

Fiziki və ya hüquqi şəxs haqqında olan hər bir informasiya fərdi məlumat hesab edilir.

Hər bir təşkilat, o cümlədən sistemlə əlaqəli şəxslər məsələn, operator daxil olmaqla, məlumatların qorunmasına məsuliyyət daşıyır.

İstehlakçılar onlayn internetdən gündəlik istifadə zamanı zərərli proqramlarla üzləşə bilərlər. Əsas veb səhifədə reklamlara keçərkən zərərli proqramlar səhifəyə hücum edə bilər. Onlayn reklamın mürəkkəbliyi istehlakçılara zərərli proqram hücumlarının qarşısını almağa və ya zərərli proqramlara məruz qalma mənbəyini müəyyən etməyə imkan vermir. Reklam şəbəkəsi və ya ana sayt bu hücumun qarşısını hansı yolla ala biləcəyini təyin edə bilmir [2].

Müasir internet-reklamın çətinliyi zərərli hücumlara görə məsuliyyətin olmamasıdır. Onlayn reklam zamanı zərərli proqramlar reklam vasitəsi ilə istifadəçinin kompüterinə ötürüldükdə heç bir tərəf məsuliyyəti öz üzərinə götürmür. Brauzerlərə onlayn reklam üçün çox sayda vasitəçilər müraciət etdiyinə görə, sayt yaradıcısı nadir hallarda öz serverlərində aktual reklamlar yerləşdirir. Çox vaxt veb-sayt sahibləri istifadəçi daxil olarkən ona hansı reklam göstəriləcəyini bilmirlər.

III. İNTERNETDƏ İSTEHLAKÇININ TƏHLÜKƏSİZLİYİNİN QORUNMASI

İnternetdə istehlakçının təhlükəsizliyini qorumaq üçün yalnız özünə nəzarət orqanları kifayət deyil. Onlayn reklamda özünə nəzarət, davranış kodları istehlakçıları zərərli proqramlardan qorumaq problemini tam həll etmir.

Böyük veb saytlara keçid istehlakçılar üçün yüzlərlə naməlum və potensial təhlükəli üçüncü tərəfi meydana gətirə bilər. Əsas veb sayta baxış istehlakçıları yüzlərlə üçüncü tərəfin müdaxiləsinə məruz qoyur və bu istehlakçı məlumatlarını toplayan zərərli proqram ola bilər.

Onlayn reklamda istehlakçıları sui-istifadə hallarından qorumaq üçün tədbirlər kifayət etmir. Özü tənzimlənən kodlar onlayn reklamın təhlükəsizliyinə əhəmiyyətli təsir göstərmir və məlumatların toplanması zamanı çox vaxt təhlükəsizlik tədbirlərindən istifadə edilmir. Kiber cinayətkarlar daim mövcud hallardan yararlanmaq üçün yollar axtarırlar [3].

Mövcud sistemlər, onlayn reklam istifadəçilərinə istehlakçı tərəfindən sui-istifadə hallarının qarşısını almaq üçün kifayət etmir. Zərərli hücumlar və onlayn reklam vasitəsilə yalnız məlumat toplama məsuliyyətinin mürəkkəbliyi, onlayn reklam yaradıcılarını daha effektiv müdafiə yolları tapmağa sövq edir.

IV. ZƏRƏRVERİCİ REKLAMLARDAN QORUNMA YOLLARI

İnternet reklamında sui-istifadə hallarının qarşısını almaq üçün qaydalara düzgün əməl etmək lazımdır. Saxta reklam zamanı vurulan zərəre görə məsuliyyət yalnız şübhəli şəxsin üzünə düşür.

Böyük və kiçik mürəkkəb kommersiya təşkilatları, reklam şəbəkələrindəki sistemin zəif olmaması üçün tədbirlər görməlidirlər. Əks halda nəinki məsul şəxsə, hətta istehlakçılara da ziyan dəyə bilər [4].

Sui-istifadə hallarının qarşısını almaq üçün onlayn reklamda təhlükəsiz məlumat mübadiləsi gücləndirilməlidir. Onlayn reklam şirkətləri, rəqiblərlə işlədikdə təhlükəli təhdidlər haqqında məlumatları federal antiinhisar qurumlarına çatdırmalıdır. Qanun pozğunluqları barədə əlaqədar orqanlar məlumatlandırılmalıdır.

Onlayn reklamla bağlı ciddi narahatlıqlar vardır, çünki saxta aktorların fırıldaqçılar üçün məsuliyyəti azdır və ya heç bir məsuliyyət daşımır. İstehlakçıları zərərli onlayn reklamlardan qorumaq üçün beynəlxalq qaydalar mövcud deyil.

Sayt istehlakçı haqqında məlumat toplayırsa bu gələcəkdə yeni məhsullar haqqında məlumat çatdırmaq üçün nəzərdə tutulur.

Müştəri haqqında toplanmış hər bir məlumat fərdi məlumat adlanır. Əgər üçüncü tərəfdən hər hansı məhsul haqqında məlumat göndərilərsə bu məlumatın ötürülməsi deməkdir. Həmin məlumatların silinməsi, oğurlanması, itirilməsi də qanun pozğunluğudur.

Müştəri haqqında məlumatdan həmin şəxsin icazəsi olmadan istifadəsi yolverilməzdir. Rusiya Federasiyasında bir xanım təsadüfən onlayn reklamları izləyərkən qəbir daşlarının hazırlanması haqda elanla rastlaşır və baş daşında öz şəklini görmüşdür. Hüquq mühafizə orqanları məsələni araşdırdıqda məlum olmuşdur ki, həmin xanım bir neçə il əvvəl fotostudiyada sənəd üçün şəkil çəkirmişdir. İllər sonra həmin studiya digər sahibkara ötürülmüş, o da nümunə kimi şəkildən istifadə etmişdir. Nəticədə sahibkar icazəsiz fərdi məlumatlardan istifadə, həm də mənəvi zərəre görə cərimə edilmişdir.

Sosial şəbəkələrdə hər hansı məlumat ümumi istifadəyə yerləşdirilibsə, o hər kəs tərəfindən istifadə oluna bilər.

Əksər insanlar doğum tarixi, ünvanı, telefon nömrəsi, e-poçt şifrəsi, kredit kartı və ya bank hesabı haqqında məlumatlarının qorunması barədə düşünür. Hər hansı bir vəziyyətdə bu məlumatların səhv əllərə düşməsinin qarşısını almaq lazımdır. Onlardan yalnız diqqətlə müəyyən bir məqsəd üçün istifadə olunmalıdır.

V. MƏLUMATIN ŞƏFFAFLIĞI

Ümumi məlumatın qorunması qaydalarının tətbiqi birdən-birə məlumatların qorunmasını gündəmə gətirdi. Fərdi məlumatları hər hansı bir şəkildə, istər oflayn, istərsə də onlayn olaraq toplayan hər kəs toplandığını və hansı məqsədlə istifadə olunduğunu açıqlamalıdır. Tibbi təcrübələr, dərnəklər, bloggerlər və ya böyük şirkətlər eyni dərəcədə məsuliyyət daşıyırlar. Məlumatların sənədləşdirmə, statistik və ya reklam üçün istifadə olunmasının əhəmiyyəti yoxdur.

Facebook və Cambridge Analyticanın məlumat qalmaqallarından sonra bu şirkətlər hansı məlumatların toplanıldığını və onlayn şirkətlərin bu barədə nə qədər xəbərdar olması ilə maraqlanırlar. İnternetdə fərdi məlumatlar açıqlandıqda, nadir hallarda telefon nömrəsi və ya kredit kart məlumatları təsirsiz qalır. Bir məhsul sifariş etdiyimiz zaman bu kimi məlumatlar şüurlu və ya məqsədli təqdim edilərsə eyni məsələ burada tətbiq olunur.

Veb portallara daxil olduqda kuki faylları yaranır və baxış haqqında məlumatlar toplanılır. Bu, reklam verənlər üçün çox əlverişlidir. Onlar daha çox baxılan veb-səhifələrin siyahısını yaradır, daha çox bəyənən məhsulları müəyyən edir, səhifəyə daxil olan internet istifadəçisi haqqında fərdi məlumatlar toplayırlar. Məlumatlar anonim şəkildə toplandığından, kimin kompüter arxasında oturduğu bilinmir. Reklam verəni yalnız internetdə hansı səhifələrə baxış keçirilməsi və hansı məhsullara maraq göstərilməsi maraqlandırır.

GDPR (General Data Protection Regulation) fəaliyyətə başladıqdan sonra, sənayedə böyük bir ixtişaş yarandı. Bu standartlarda məxfilik qaydaları artıq reklam sənayesi üçün böyük bir mərhələnin başlanğıcı oldu. Yeni müddəa ilə əlaqədar olaraq, Avropa İnteraktiv Reklam Bürosu (IAB), insanların internetdəki məlumatları necə idarə etməsi və hər şeydən əvvəl məlumatlardan onlayn marketingdə necə istifadə edilməsi məsələsini araşdırdı. İstehlakçıların öz məlumatlarının məxfiliyi və qorunmasını təmin etmək istəyi həmin məlumatlardan reklam məqsədi üçün istifadəyə xələl gətirmir.

VI. KUKİ FAYL NƏDİR?

Onlayn reklamın mövcudluğu üçün kuki faylların izlənməsi qaçılmazdır. “Kuki fayl” veb-sayta daxil olarkən kompüterin sərt diskinin yaddaşında yığılan kiçik məlumat parçasıdır. Bir kuki faylı internetdə hansı veb sayt və ya onlayn mağaza haqqında məlumata baxılırsa həmin məlumatı toplayır.

“Kuki fayllar”-dan veb saytın ümumi internet trafiki dinamikasını təhlil etmək və istifadəçilərin veb saytdan istifadə təcrübəsini daha da təkmilləşdirmək məqsədilə istifadə edilir [5]. Hər hansı fərdi məlumatı toplamaq və ya onları sistemin

yaddaşında saxlamaq məqsədilə “kuki fayllardan” istifadə oluna bilər. “Kuki fayllar”ı deaktiv etdikdə veb sayta müvəffəqiyyətlə daxil olmaq olar, lakin veb-brauzerinizdə “kuki fayllar”ın aktiv saxlanması saytın işləkliyinin və səmərəliliyinin təkmilləşməsinə kömək edir [5-7].

İnternet-reklam bizim maraqlarımıza cavab verərsə daha qənaətbəxş sayılır. Səbəb müvafiq təkliflə maraqlanmadığımız məhsula, yenidən maraq oyatmaq üçün oxşar məhsulları bizə göstərməkdir.

Marketinqin avtomatlaşdırılması, auditoriyanın ölçülməsi, kuki əlaqəli üçüncü tərəf məlumat bazaları, sosial şəbəkə kukisi, kuki analitikləri və s. kukilər davam edir. 2014-cü ildə “kuki təmizləyicisi” (Cookie Sweep) adlandırılan proqramda təhlil olunan media, dövlət sektoru və elektron ticarət saytlarında (AB-də) təxminən 28.9 kuki, 70% -i üçüncü kukilər olduğu açıqlandı [7].

Veb saytdan istifadə etmək üçün kuki fayllarının istifadəsinə razılıq olmalıdır. Yeni məxfilik qaydası kuki fayllarının istifadəsini ciddi şəkildə məhdudlaşdırır bilər. Kuki fayllarını izləmədən reklamın istifadəsinə yeni yollar tapılmalıdır. Elektron məxfilik qaydalarının qüvvəyə minməsindən asılı olmayaraq onlayn marketinq daim dəyişir.

Məxfilik sahəsində kuki faylları haqqında Avropa Birliyi 2017-ci ilin yanvar ayında müraciət yayımladı. AB-nin mövcud qanunvericilik bazasının, 2002 və 2009-cu illərdə yenidən işlənərək, AB-nin Məxfilik Düzəlişinin yenilənməsi üçün nəzərdə tutulmuşdur. Məxfilik qaydalarına riayət edilməsi, məlumatların qorunması milli orqanlardan asılıdır.

Həmin vaxtdan etibarən məxfilik marketoloqlar və veb istifadəçilər tərəfindən kuki qanunu adlanır. Kuki AB ölkələrində tədricən tətbiq edilərək, milli fərqliliyə və bu ölkələrdə milli qanunvericiliyə çevrilmişdir.

Elektron məxfilik təlimatı və qaydaları yalnız kukiyə deyil, elektron rabitə və məxfilik hüququ, məlumatların qorunması və s. aiddir. Başqa sözlə: fərdi məlumatların qorunması.

Elektron rabitə dedikdə veb, internet, elektron poçt, telefon, anı mesajlaşma, spam, birbaşa marketinq, telekommunikasiya şirkətləri, mobil qurğular, onlayn reklam şəbəkələri nəzərdə tutulur.

Elektron mesajların məxfiliyi mesajın məzmununun, məlumatın haradan göndərildiyini, mesajda iştirak edən tərəflərdən başqa kimlər üçün açıqlanmamasını təmin edir. Məxfilik prinsipinə mövcud və gələcək rabitə, o cümlədən zənglər, internetə çıxış, müntəzəm mesajlaşma, e-poçt, internet telefon zəngləri və sosial şəbəkələr vasitəsi ilə verilən şəxsi mesajlara aiddir.

Birbaşa marketinq dedikdə mütəmadi zənglər nəzərdə tutulur. Bu zaman reklam verənlər telefon nömrələrini göstərməli və ya çağırışın marketinq çağırışı olduğunu göstərən bir işarədən istifadə etməlidirlər.

VII. FƏRDİ MƏLUMATLARIN QORUNMASI

Fərdi məlumatları idarə edərkən, məlumatların zərərli, köhnəlmiş, icazəsiz giriş, açıqlama, dəyişdirmə və ya məhv etməkdən qoruyan müvafiq texniki və təşkilati tədbirlər görülməlidir. Adətən hər hansı bir fərdi məlumatın təhlükəsizliyini və məxfiliyini təmin etmək üçün standart təhlükəsizlik düyməsi və şifrə sistemləri ilə qorunan məlumat şəbəkələrindən istifadə edilir.

Fərdi məlumatlarınızı və digər gizli məzmunu qorumaq üçün şifrələmə metodlarından (SSL- Secure Sockets Layer və ya TLS-transport layer security şifrələmə) istifadə edilir [8-10].

“Fərdi məlumatların emalı” dedikdə, belə məlumatların müxtəlif metod və alqoritmlərlə analizi nəticəsində gizli informasiyanın aşkarlanması, saxlanması, ötürülməsi nəzərdə tutulur.

Veb-sayt onlayn mağazalardan, proqramlardan istifadə etdikdə fərdi məlumatları avtomatik olaraq qeyd edir. Qeydiyyatdan keçərkən istifadəçi profilinin, müştəri hesabının yaradılması zamanı fərdi məlumatlar avtomatik və ya əl ilə qeyd edilir [11].

Fərdi məlumatlar açıq şəkildə müəyyən edilmiş və ya qanunla tələb olunan istisnalar olmaqla müxtəlif məqsədlər üçün istifadə edilir. Bir çox hallarda məlumatlar üçüncü şəxslərə ötürür:

- Birbaşa marketinq üçün fərdi məlumatların istifadəsi-yeni məhsullar, iş yerləri və s. haqqında müntəzəm məlumat alma;
- E-poçt xəbərləri məlumatları əldə etmə, e-poçt ünvanını daxil etmə, və sizə göndəriləcək təsdiqləmə e-poçtda (Double Opt-in process) linkə keçənə qədər bülletenlər sizə göndərilməməlidir. Adətən təsdiq linkinə vurmaqla, fərdi məlumatlarınızı istifadə etmək üçün icazə verdiyinizi bildirirsiniz. Razılıq qeydini saxlamaq üçün IP ünvan və razılıq tarixi saxlanılır. Məlumatların istifadəsinə icazə verilmədikdə fərdi məlumatlar silinir.

Fərdi məlumatların qorunmasına hər zaman xüsusi yanaşılmalıdır:

- Məhsul alarkən əvvəlcədən ödəniş tələb olunarsa diqqətli olmaq lazımdır. Bir çox hallarda ödəniş olunduqdan sonra, “satıcı” zənglərinizə cavab vermir, səhifədə görünmür.
- Əgər telefon, internet, sosial şəbəkələr və s. vasitələrlə əlaqə saxlamaq bəhanəsi ilə bank kartının (kart nömrəsi, kartın arxasındakı üç rəqəmli kod), mobil telefona gələn kod, şifrələr və ya digər məlumatları öyrənməyə çalışırlarsa, bu şəxsi məlumatlarınızı fırıldaqçılar tərəfindən mənimsənilməsidir.
- Fırıldaqçılar sosial şəbəkələrdə, tanışlıq saytlarında istənilən insanların şəkil və məlumatlarını yerləşdirərək səhifə yaradırlar. Bu səhifələrdən istifadə edərək saytın digər istifadəçiləri ilə tanış olurlar. Etibar qazandıqdan sonra, həmsöhbətinin telefon nömrəsini öyrənirlər.

Nəticədə, nömrə vasitəsi ilə məbləğ ödənişi və hesabdən pul çıxarılma ola bilər.

- Fırıldaqcılar tez-tez maddi yardım, xeyriyyə aksiyaları üçün müraciətlərdən istifadə edirlər. Belə aksiya hesablarına pul köçürməzdən əvvəl aldanmamamağımıza əmin olmalıyıq. Əlaqə dəstəkləyici sənədlərin (telefon, e-poçt, sosial şəbəkələrdəki səhifələr), qorunmasına diqqət yetirməliyik. Pulsuz saytlarda reklam yerləşdirərkən (məsələn, Avito) və ya alarkən diqqətli və ehtiyatlı olmaq lazımdır. Çünki fıırıldaqcılar tez-tez onlardan aldatmaq üçün istifadə edirlər. Nə isə sataraq bir qazanc əldə etmək istədikdə fıırıldaqcılarla qarşılaşdıqda bütün əmanətləri itirə bilərik.

NƏTİCƏ

İnformasiya texnologiyalarının sürətlə inkişafı fərdi məlumatların toplanılmasına özünə məxsus təsir etmişdir. İnkişaf etmiş ölkələrdə fərdi məlumatların qorunmasına xüsusi diqqət yetirilir. Toplanmış məlumatların qorunması, onların təhlükəsizliyi onlayn reklam marketinq sahəsində xüsusi ilə önəmlidir.

İnternetdən daha səmərəli istifadə hər sahədə olduğu kimi reklam – marketinq sahəsində də xeyli irəliləyişə, iqtisadiyyatın artmasına, xalqın rifahının yaxşılaşmasına əsaslı təsir göstərmişdir. Kibercinayətkarlığın, informasiya müharibəsinin olduğu dövrdə reklam sahəsində təhlükəsizliyi qorumaq əsas şərtədir. İnformasiya təhlükəsizliyinin qorunması gələcək nəslin daha sağlam, firavan yaşaması deməkdir[9].

Araşdırmalardan məlum oldu ki, müasir dövrdə reklam-marketinq internetin əsas xidmət növlərindən biri olmaqla insanların gündəlik tələbatına çevrilmişdir. Bu sahədə fərdi məlumatların qorunması vacib problemlərdən biridir və həlli kompleks tədbirlər tələb edir. Bununla bağlı təkliflər məqalədə öz əksini tapmışdır.

İşlənmiş təkliflər internetdə reklam-marketinq məsələlərinin səmərəliliyini artırmasına dəstək olacaqdır.

İSTİNADLAR

- [1] Как работает реклама Google. <https://safety.google/intl/ru/privacy/ads-and-data/>

- [2] Online advertising and its security and privacy concerns. <https://ieeexplore.ieee.org/document/6488209>
- [3] Online advertising vs. protection of personal data contradiction or in harmony? <https://www.advanced-store.com/en/online-advertising-vs-protection-of-personal-data/>
- [4] Kuki_Bildirişi, <https://www2.deloitte.com/az/az/legal/cookies.html>
- [5] Как включить или отключить сохранение файлов cookie <https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DAndroid&hl=ru>
- [6] Gloria González Fuster, The emergence of personal data protection as a fundamental right of the EU. Springer, 2014. 274 p.
- [7] A.Vertsimaha, Новое правило ЕС о конфиденциальности (ePrivacy Regulation): что вам нужно знать <https://medium.com/ponravilos/новое-правило-ес-о-конфиденциальности-eprivacy-regulation-что-вам-нужно-знать-96adffaa43b0>
- [8] Дело не в cookie: Безопасность данных и онлайн-реклама в эпоху мультимедиа. https://habr.com/ru/company/advertone_ru/blog/237853/
- [9] Мəlumatların qorunması bəyanatı <https://www.curaprox.com/az-az/privacy-policy>
- [10] Həşimova K., İnternet-reklam marketinqində informasiya təhlükəsizliyi problemləri, “İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri” IV respublika konfransı, 2018, səh. 147–149.
- [11] I.Bernik, B.Markelj, S.Vrhovec. Information security management practices: Expectations and reality. Advances in CyberSecurity, 2017, pp. 5-22.

SECURITY OF PERSONAL DATA IN INTERNET ADVERTISING MARKETING

Kamala Hashimova

Institute of Information Technology of ANAS, Baku, Azerbaijan

multimedia@iit.science.az

Abstract— As the Internet becomes more widespread, technologies are becoming more and more popular, and online advertising is growing. The research investigated the possibilities of advertising on the Internet, the security of websites registration, the perspectives for the security of personal information, and the threats identified. Web sites also provide suggestions for the effective use of information collected from surveys in marketing and marketing systems.

Keywords— *Internet advertising-marketing; cookies; personal information; Web site; online advertising*

Некоторые проблемы информатизации процессов защиты персональных данных и пути их решения

Аловсат Алиев

Институт Информационных Технологий НАНА, Баку, Азербайджан
alovsat_qaraca@mail.ru

Аннотация – В статье анализируются некоторые социально-экономические и правовые проблемы информатизации в сфере защиты персональных данных в условиях формирования информационного общества и электронного управления. Обосновывается актуальность указанной проблемы. Описываются сущности и особенности правовой информатизации. Раскрываются особенности информационного законодательства и право. Описываются необходимость защиты персональных данных в современном бизнесе. Анализируются проблемы создания интеллектуальных правовых систем в области защиты персональных данных. Указываются пути формирования единого информационного пространства защиты персональных данных. Рекомендованы предложения и пути решения по защите персональных данных.

Ключевые слова — правовые проблемы, информатизация правовых процессов, защита персональных данных, правовые информационные системы, интеллектуальные юридические системы, информационное право, коммерческие информации

I. ВВЕДЕНИЕ

За последние годы в области осуществления Стратегии по информационного общества [1] и Стратегические дорожные карты [2] в Азербайджане была обеспечена стремительная интеграция страны в общемировое электронное пространство, получены значительные результаты в направлении создания электронного правительства, формирования экономики знаний, информационной безопасности и прочее. Создание космической индустрии, способствующей продвижению науки и техники, развитию отдельных направлений инновационной деятельности, обогащение интернет ресурсов, повсеместное использование социальных сетей являются наглядными показателями развития Информационно-Коммуникационные Технологии (ИКТ) в республике.

В этих условиях считается, что обеспечение непрерывного экономического роста каждой развитой и развивающейся страны в первую очередь, требует, развития науки, инновации, техники и технологии. Человеческий капитал составляет основную часть указанного национального богатства. В этих условиях

необходимо построение новой национальной инновационной инфраструктуры и системы, которые составляют основу будущего экономического развития страны [3]. В этом процессе возрос интерес к проблемам информатизации в сфере защиты персональных данных (ЗПД). Это связано с тем, что современная система по защите персональных данных претерпевает изменения, связанные с реформами в различных сферах жизни [2]. Поэтому анализ и исследование самых различных проблем, связанных с формированием и применением системы ЗПД как основы национальной информационной инновационной системы страны и разработка соответствующих рекомендаций в этом направлении считаются одними из актуальных задач.

II. СУЩНОСТЬ И ОСОБЕННОСТИ ПРОБЛЕМЫ ПРАВОВОЙ ИНФОРМАТИЗАЦИИ

Под правовой информатизацией в сфере ЗПД понимается процесс создания условий полного удовлетворения информационно-правовых потребностей государственных и общественных структур, предприятий, организаций, учреждений и граждан с соблюдением защиты персональных данных на основе эффективной организации и использования информационных ресурсов с применением прогрессивных информационных технологий. Задача правовой информатизации в этой сфере определяется как формирование единого информационно-правового пространства, обеспечивающего правовую информированность всех структур общества и каждого гражданина в отдельности с учетом неприкосновенности персональных данных [4, 5].

Область правовой информатизации в сфере защиты персональных данных требует особого государственного внимания. Для ее развития важно применение рыночных механизмов. Становление правового порядка в государстве и обществе требует закрепления юридическими нормами таких механизмов управления, которые обеспечивают устойчивость их развития при соблюдении баланса интересов государства, общества, семьи, человека. Для создания адекватного механизма поддержки системы права служит правовая

информатизация. Правовые базы персональных данных по своей сути являются распределенными. В их создании и сопровождении заинтересованы все члены общества.

При таких условиях правовая информатизация в сфере защиты персональных данных должна рассматриваться как регулируемый государством процесс взаимовязанная создаваемых в городах и регионах, министерствах и ведомствах, учреждениях и организациях соответствующих персональных информационных систем [6]. Процесс, который активно реализуется усилиями множества независимых разработчиков, можно упорядочить только введением соответствующих стандартов и нормативов.

Можно предположить, что с дальнейшим вхождением в информационную эру определение ценности человека или иного субъекта будет иметь некое информационное выражение. Человек может быть оценен – характеристиками: внешнего вида, поведения, рейтинга. Значимость ученого - количеством ссылок на его труды и выступлений на симпозиумах. Современные информационные технологии позволяют накапливать опыт и проводить сравнительные оценки подобных характеристик для каждого.

III. ОСОБЕННОСТИ ИНФОРМАЦИОННОГО ЗАКОНОДАТЕЛЬСТВА И ПРАВА

В мире постоянно идет юридическая работа по расширению информационного законодательства. Сегодня это самая быстро развивающаяся область права. Постоянно разрабатываются и уточняются законы, организуются и проводятся разные конференции. Результат этой работы представляет собой перераспределение человеческих информационных прав и свобод. Большинство государств, крупнейшие корпорации информационной индустрии отстаивают свои права в этом сложном процессе. Государственный интерес состоит в том, чтобы информация как можно скорее становилась обще доступной, чтобы препятствия и ограничения на распространение информации были минимальными. При этом должны соблюдаться свободу личности, и должно быть защищено его персональных данных [7].

Отдельные разделы информационного права развиваются уже несколько веков. Истинная его значимость в полной мере проявилась лишь в XX веке, когда возникли мощные технические средства обработки и распространения информации, а участие людей в информационных процессах стало действительно массовым. Термин “информационное право” нельзя пока считать устоявшимся и общепринятым. Он охватывает вообще всю сферу права. Основные направления информационного права можно разделить на экономические и политические.

IV. ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СОВРЕМЕННОМ БИЗНЕСЕ

Сейчас во всех сферах экономики и бизнеса резко выросла значимость безопасности информационного обеспечения. Грамотно построенный современный бизнес - это, по сути, информационное производство. Внутренний документооборот и технологии принятия решений, реклама и маркетинг, патенты и ноу-хау, авторские и смежные права, сбор данных о конкурентах и партнерах, обучение персонала и реинжиниринг бизнес-процессов - все эти направления информационной деятельности по большей части являются составляющими современного бизнеса. Именно на этих направлениях возникают противоречия и конфликты, в результате которых рождается персональные право отдельного гражданина.

Высшим действующим юридическим документом, в котором закреплены информационные права граждан, является Европейская конвенции о правах человека. Согласно Всеобщей декларации прав человека, признается свобода, искать, получать и распространять информацию и идею любыми средствами и независимо от государственных границ по при этом не трогать интересы других [8].

В Азербайджане после принятия закона об информации и информатизации [9] ведется работа по формированию правовой базы для осуществления электронного документооборота [10]. Были принят законы "Об электронной цифровой подписи" (ЭЦП). Закон предполагает полностью либерализованный подход к ЭЦП. Он включает положение, основанное на принципах технологической нейтральности и адаптированности под развитие новых технологий.

Электронная цифровая подпись как реквизит электронного документа, в сфере бизнесе защищает данного электронного документа от подделки, полученный в результате криптографического преобразования информации, с использованием закрытого ключа электронной цифровой подписи. Она позволяет идентифицировать владельца сертификата ключа подписи и установить отсутствие искажения информации в электронном документе. Закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная только владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи [10].

Фактически электронную подпись можно вставить в любой электронный документ в современном бизнесе. После этого этот документ получит юридическую силу. Это аналог печати и обычной подписи на листке бумаги. В итоге получится, что не отходя от компьютера, можно заключать сделки, руководить целой конторой и др.

В настоящее время сформированы некоторые подходы к требованиям, предъявляемым к электронной подписи.

Первый основан на признании в отношении электронной подписи тех же требований, что и в отношении обычной. Второй предполагает, что подпись должна быть связана с передаваемыми данными таким образом, что если они изменяются, то подпись становится недействительной. Третий подход предусматривает использование в ЭЦП криптографической технологии открытого ключа.

Следует отметить что в законе "Об электронной торговле" [11] учитывается также директивы Европарламента, ЮНДПИ, Конгресса США, а также других национальных законов, включая и Российский. Этот закон полностью сохраняет принцип либерального подхода госрегулирования электронной коммерции с признанием важной роли саморегулирования в этой сфере. Кроме этих законов были приняты также – “Об электронном документе” [10] нормативы и процедуры по применения "Asan İmza" и т.д.

Принятие таких пакетов нормативно-правовых документов частично относящихся также к защите персональных данных в современном бизнесе повлияет на развитие экономики в Азербайджане. Узаконивание электронной подписи в коммерции скорее всего сделает актуальным к усилит процесса ведения бизнеса с использованием современных новейших информационных технологий.

V. ПРОБЛЕМЫ СОЗДАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ПРАВОВЫХ СИСТЕМ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обоснование любых юридических документов в области защиты персональных данных осуществляется ссылкой на статьи нормативно-правовых актов, регулирующих соответствующие правоотношения. При этом недостаточно знать, как решать юридическую задачу, необходимо также обосновать решение. Следовательно, нужны сведения о действии нормативно-правовых актов, о внесенных в них изменениях.

Отсутствие информационных и интеллектуальных систем правовой информации в сфере защиты персональных данных в государственных органах приводит иногда к принятию ими не эффективных законных решений, ущемляющих права граждан. Отсутствие современных технологий приводит к нарушениям процессуальных сроков рассмотрения дел. В результате этого увеличиваются срок содержания обвиняемых под стражей, увеличивается издержки сторон в гражданском процессе. Кроме того, граждане, не являющиеся профессиональными юристами, испытывают значительные затруднения при самостоятельном поиске информации о правовом регулировании в конкретной ситуации и применении права.

Поэтому вопросы применения автоматизированных систем правовой информации по защите персональных данных в правоохранительной и юридической деятельности являются в настоящее время весьма актуальными. Системы правовой информации можно

определить как информационные компьютерные системы, обеспечивающие доступ к правовой информации, т.е. сведениям о фактах, событиях, предметах, лицах, явлениях, протекающих в правовой сфере жизни общества, содержащихся как в нормах права, так и других источниках и используемых государством и обществом для решения задач правотворчества и реализации права.

Существующие в настоящее время системы правовой информации можно разделить на информационно-правовые системы и интеллектуальные юридические консультационные системы [12]. Информационно-правовые системы в области ЗПД в зависимости от характера содержащейся в них правовой информации подразделяют на документальные и фактографические системы. Документальные информационно-правовые системы содержат тексты документов: нормативно-правовых актов, актов применения права, других документов, принятых государственными органами. Фактографические информационно-правовые системы содержат ненормативную правовую информацию: данные криминалистического учета, статистические и социологические данные, необходимые для решения юридических задач.

Интеллектуальные юридические консультационные системы осуществляют моделирование рассуждений юристов при решении задач профессиональной деятельности. Результатом работы таких систем является решение юридической задачи с ее обоснованием: информация о правовом статусе (правах и обязанностях) субъектов правоотношения, рекомендуемая линия поведения, соответствующая нормам права и направленная на удовлетворение интересов пользователя системы.

Интеллектуальные юридические консультационные системы, решающие задачи на уровне экспертов в определенной области юридической деятельности, называются экспертными юридическими компьютерными системами [13]. Они используются в тех случаях, когда необходимо решить юридическую задачу человеку, не имеющему необходимой юридической подготовки, либо юристу, встречающемуся с задачей, выходящей за пределы его профессиональной компетентности. Помимо рассмотренной выше функции экспертные юридические системы применяются для обучения студентов юридических учебных заведений и для повышения квалификации юридических кадров [14]. В государственных правоохранительных органах обычно существует система ведомственных распределенных и локальных информационно-правовых систем. Такие системы обычно бывают государственными или негосударственными.

VI. ФОРМИРОВАНИЕ ЕДИННОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Сложившаяся обстановка диктует необходимость информационного обеспечения правоохранительных органов и юридических процессов по защиты персональных данных. Улучшение состояния борьбы с различными видами преступности в этой сфере можно решить только путем создания единого информационного пространства (ЕИП) правоохранительных органов по ЗПД [15].

ЕИП по ЗПД представляет собой совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие правоохранительных органов республики.

Формирование и развитие ЕИП правоохранительных органов сфере ЗПД предусматривает, обеспечения оперативного доступа к имеющимся информационным ресурсам и проведение работ по их включению в единое информационное пространство. Действующие и разрабатываемые в настоящее время ведомственные и межведомственные распределенные системы сбора, обработки и накопления информации могут служить базой внедрения новых информационных технологий. Формирование информационных ресурсов - одна из ключевых проблем создания ЕИП правоохранительных органов, которые включают информацию и знания, а также средства для обеспечения доступа к информации.

Совершенствование информационной инфраструктуры правоохранительных органов в сфере защиты персональных данных должно учитывать различный уровень информатизации в разных органах. При этом необходимо определить оптимальные средства связи и передачи данных для каждого органа [16]. Для обеспечения информационного взаимодействия правоохранительных органов должна быть предусмотрена разработка соответствующих нормативно-правовых актов.

VII. ВЫВОДЫ И ПРЕДЛОЖЕНИЯ

Международный опыт подтверждает актуальность проблем информационной безопасности в деле обеспечения ЗПД. Информационное взаимодействие правоохранительных органов наряду с правовым обеспечением требует принятия организационных и технических мер по защите информации: предотвращение утечки, утраты, подделки информации; предотвращение несанкционированного доступа и действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы. Для информационного обеспечения правоохранительных органов в сфере защиты персональных данных предлагается создание *Единой информационной сети*,

которая должна состоять из следующих подсистем: 1) единой (взаимоувязанной) телекоммуникационной сети связи; 2) единой системы информационного обмена по защиты персональных данных; 3) систем хранения и обработки персональных данных; 4) систем защиты информации. Такие системы должны иметь повышенную надежность и строиться на базе резервируемых спутниковых и высокоскоростных наземных каналов связи. Система должна также предоставлять современные виды сетевого сервиса, включая доступ к удаленным локальным сетям, цифровую передачу речи, аудио и видеоконференции, подключение систем охранной и прочей сигнализации и видеонаблюдения и пр.

Система позволит поднять на качественно новый уровень борьбу с преступностью и создает для руководства оперативную и надежную систему передачи информации по защиты персональных данных. Обеспечивает непосредственный доступ к автоматизированным банкам данных, системам оперативного и оперативно-справочного учета информационных центров в области ЗПД. Объединит телекоммуникационные системы различного уровня в единую сеть на основе стандартных сетевых протоколов, типовых программных средств, коммуникационного оборудования и способов сопряжения. Осуществление выше указанных мероприятий повысит уровня защиты персональных данных и обеспечит безопасности граждан и организаций.

ЛИТЕРАТУРА

- [1] Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Stratejiya. Bakı, 2 aprel 2014-cü il. <https://president.az/articles/11312>
- [2] Milli iqtisadiyyat və iqtisadiyyatın əsas sektorları üzrə Strateji Yol Xəritələri. Bakı, 6 dekabr 2016-cı il, <https://president.az/articles/21953>
- [3] А.Г.Алиев. Проблемы информатизации общества и экономики // Баку, “ЭЛМ”, 2003, 460 с.
- [4] А.Г.Алиев. Теоретико-прикладные аспекты информатизации гуманитарных отраслей // Баку, “ЭЛМ”, 2006 г., 474 с.
- [5] Д.А.Ловцов, А.В.Федичев. Место и роль правовой информатики в системе информационно-правовых знаний. // Правовая информатика, 2017, №1, стр.5-12.
- [6] «Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu». № 998-IIIQ. Bakı şəhəri, 11 may 2010-cu il, <http://www.e-qanun.az/framework/19675>
- [7] İnformasiya əldə etmək haqqında Azərbaycan Respublikasının Qanunu. Bakı şəhəri, 30 sentyabr 2005-ci il. № 1024-IIQ. <http://www.e-qanun.az/framework/11142>
- [8] Европейская конвенция по правам человека. https://www.echr.coe.int/Documents/Convention_RUS.pdf
- [9] İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında Azərbaycan Respublikasının Qanunu. Bakı şəhəri, 3 aprel 1998-ci il. № 460-IQ. <http://e-qanun.gov.az/framework/3525>
- [10] Elektron imza və elektron sənəd haqqında Azərbaycan Respublikasının Qanunu. Bakı şəhəri, 9 mart 2004-cü il. № 602-IIQ. <http://www.e-qanun.az/framework/5916>
- [11] Elektron ticarət haqqında Azərbaycan Respublikasının Qanunu. Bakı şəhəri, 10 may 2005-ci il. № 908-IIQ. http://www.e-qanun.az/alpidata/framework/data/10/f_10406.htm

- [12] A. Musca. legal informatics as fundamental instrument utilized in law administration. International Conference on Uniformization of the Law - Legal Effects and Social, Political, Administrative Implications, Romania, oct. 23-25, 2014, pp.517-524.
- [13] А.С.Лагоха. Некоторые особенности использования юридических экспертных систем. Вестник Алтайской академии экономики и права. 2013. №3(32), стр.86-88.
- [14] Li Song. Research of key technical issues based on computer forensic legal expert system. International Symposium on Computers and Informatics (ISCI), China, jan 17-18, 2015. Book Series: ACSR-Advances in Computer Science Research, vol.13. pp.1431-1437.
- [15] А.В.Долматов, Е.А. Долматов. Особенности и проблемы правового регулирования защиты персональных данных. Вестник Санкт-Петербургской юридической академии. 2018, №3(40), стр.53-60.
- [16] Greenleaf Graham, Mowbray Andrew, Chung Philip. Building a Sustainable free legal advisory systems: Experiences from the history of AI & law. Computer law & security review, 2018, vol. 34, issue 2, pp.314-326

SOME PROBLEMS OF INFORMATIZATION OF PERSONAL DATA PROTECTION PROCESSES AND WAYS OF THEIR SOLUTION

Alovsat Aliyev

Institute of Information Technology of ANAS, Baku, Azerbaijan
alovsat_qaraca@mail.ru

Abstract - The article analyzes some socio-economic and legal problems of informatization in the field of personal data protection in the context of the formation of the information society and electronic governance. The relevance of this problem is substantiated. The essence and features of legal informatization are described. The features of information legislation and law are revealed. The necessity of protecting personal data in modern business is described. The problems of creating intelligent legal systems in the field of personal data protection are analyzed. The ways of forming a single information space for protecting personal data are indicated. Suggestions and solutions for protecting personal data are recommended.

Keywords - *legal problems, informatization of legal processes, personal data protection, legal information systems, intellectual legal systems, information law, commercial information*

Kütləvi media resurslarında fərdi məlumatların mühafizəsi problemləri

Sünbül Zalova

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

Xülasə— Bu məqalədə fərdi məlumat, fərdi məlumatın növləri, kütləvi media resurslarında fərdi məlumatların mühafizəsi problemləri araşdırılmışdır. Bu istiqamətdə olan qanunlar, dünya və Azərbaycan təcrübəsi analiz edilmişdir. Problemlərin həlli istiqamətində bir sıra təkliflər irəli sürülmüşdür.

Açar sözlər— fərdi məlumatlar; şəxsi həyat; həssas məlumatlar, sosial media, kütləvi media resursları

I. GİRİŞ

Bugün texnologiyanın sürətli inqafı ilə əlaqədar fərdi məlumatların mühafizəsi getdikcə çətinləşir. Yeni texnoloji yeniliklərin pilotsuz uçuş aparatları, robotexnikalar, süni intellekt və s. meydana gəlməsi şəxsi məlumatların yayılmasını və başqaları tərəfindən ələ keçirilməsini asanlaşdırır. “Facebook”, “Twitter”, “Instagram” və s. sosial media saytlarının istifadəçiləri öz fikir və düşüncələrini əks etdirməklə yanaşı, fotosəkil, video və şəxsi mesajlarını hər kəsin görə biləcəyi şəkildə paylaşırlar. Bundan başqa internet saytları istifadəçilərinin ünvan, telefon, əvvəl baxdığı veb-səhifələr kimi şəxsi məlumatlarını saxlayır, istifadəçi profili yaradırlar. Bu da həmin məlumatların daha sonra başqalarının əlinə keçməsinə şərait yaradır. Fərdi məlumatların istifadəsi ilə bağlı hüquqi məhdudiyyətlərin olmasına baxmayaraq fərdi məlumatlardan qeyri qanuni istifadə, bu sahənin “qara bazasının” formalaşmasına şərait yaradır.

II. FƏRDİ MƏLUMATLARIN TƏSNİFATI HAQQINDA

Fərdi məlumatlar şəxsi həyatın ayrılmaz tərkib hissəsidir. Hər hansı bir şəxsin fərdi məlumatlarının qorunması, başqa bir şəxs tərəfindən əlçatan olmamasını istəmək hüququ var və bu qanunla tənzimlənir.

Hər bir şəxsin fərdi məlumatlarını 3 istiqamətə bölmək olar[1].

1. Açıq məlumatlar
2. Şəxsi məlumatlar
3. Gizli məlumatlar

Açıq məlumatlar — şəxsin bu məlumatları hər kəsin bildiyindən narahat olmadığı məlumatlardır. (Məs: ad, soyad, vəzifə və s.)

Şəxsi məlumatlar — Şəxsin hər kəsin bilməsini istəmədiyi, yalnız ailə və yaxınlarının bildiyi məlumatlardır.

Gizli məlumatlar — 3-cü şəxs tərəfindən bilinməsi istənməyən məlumatlardır.

Hər kəsə açıq olan məlumatlardan başqa şəxsi və gizli bilgilərin şəxsin icazəsi olmadan ələ keçirilməsi, saxlanması və yayılması şəxsiyyət hüququnun pozulmasıdır [1].

Fərdi məlumatlar termininin başa düşülməsi üçün bir sıra izahatların verilməsi tələb olunur. Avropa İttifaqı qanunvericiliyində, eləcə də Avropa Şurasının hüquqi sənədlərində « fərdi məlumatlar » termininin tərfi aşağıdakı şəkildə müəyyən edilmişdir:

- “kimliyi müəyyən edilə bilən fiziki şəxs barəsində məlumat, yəni, kimliyi bariz şəkildə aşkar olan və ya əlavə məlumatların əldə edilməsi vasitəsilə müəyyən edilə bilən şəxsə dair məlumatlar”

Şəxsə aid olan istənilən məlumat fərdi məlumat kimi təsfi edilə bilər. Yəni fərdi məlumatlar şəxsin şəxsi həyatına və ya peşə və ictimai həyatına aid olan məlumatları əhatə edir. Fərdi məlumatların hansı şəkildə saxlanması və ya istifadə edilməsinin məlumatların mühafizəsinə dair qanunvericiliyin tətbiq edilməsi ilə heç bir əlaqəsi yoxdur. Yazılı və ya şifahi ifadələr, eləcə də şəkillər fərdi məlumatlar daşıya bilər. Şəxsin DNT məlumatlarını daşdığına görə insan toxumalarının hüceyrə nümunələri də fərdi məlumat hesab edilə bilər. Həm Avropa İttifaqı qanunvericiliyində, həm də Avropa Şurasının qanunvericiliyində xüsusi kateqoriyaya daxil olan spesifik məlumatlar nəzərdə tutulmuşdur ki həmin məlumatlar işləndikləri zaman öz təbiətlərinə görə aidiyyəti olan şəxslər üçün risk törədə bilərlər, buna görə də, onların geniş şəkildə mühafizə olunmasına ehtiyac vardır. Xüsusi kateqoriyaya daxil edilən bu spesifik məlumatların (həssas məlumatlar adlandırılır) işlənməsi yalnız səlahiyyətli qurumlar tərəfindən xüsusi təminatlara əməl edilməklə yerinə yetirilməlidir. Həssas məlumatların tərifinə gəldikdə, 108 sayılı Konvensiya (6-cı maddə) və Məlumatların Mühafizəsinə dair Direktiv (8-ci Maddə) aşağıdakı kateqoriyalara nəzərdə tutur[2].

1. İrqi və ya etnik mənşəyi aşkarlayan fərdi məlumatlar;
2. Siyasi, dini və ya digər əqidəni aşkar edən fərdi məlumatlar;

3. Sağlamlıq və ya cinsi həyata dair fərdi məlumatlar.

Məlumatların Mühafizəsinə dair Direktiv (Aİ-nın məlumatların mühafizəsinə dair əsas sənədi Avropa Parlamentinin və Avropa İttifaqı Şurasının 95/46/EC sayılı 24 oktyabr 1995-ci il tarixli, fiziki şəxslərə aid olan fərdi məlumatların işlənməsi və həmin məlumatların sərbəst dövriyyəsinə dair Direktivdir). həmkarlar ittifaqına üzvlüyü də həssas məlumatlar siyahısına daxil edir, çünki, bu məlumat şəxsin siyasi dünyagörüşü və mənsubiyyətini aşkar şəkildə bəyan edir. Bundan əlavə, 108 sayılı Konvensiya cinayət işi ilə bağlı məhkumluğa dair fərdi məlumatları da həssas məlumat kimi qiymətləndirir [2].

Avropa Parlamenti və Avropa Şurasının 27 aprel 2016-cı il qərarı ilə Ümumi Məlumatların Qorunması Tənzimlənməsi (GDPR *General Data Protection Regulation*) haqqında qaydalar qəbul olunub. Bu qaydalara əsasən fərdi məlumatları işlədən tərəflər məlumatların qorunması prinsiplərini həyata keçirmək üçün zəruri texniki və institusional tədbirlər görməlidirlər. Fərdi məlumatların idarə olunduğu iş prosesləri, məlumatların qorunması prinsiplərinə uyğun olaraq hazırlanmalı və aparılmalı, məlumatların qorunması üçün tədbirlər görülməlidir. Fərdi məlumat sahibindən açıq razılıq alınmadıqda heç bir şəxsi məlumat işləyə bilməz. Müvafiq şəxs istənilən vaxt bu icazəni ləğv etmək hüququna malikdir. Qaydalara görə fərdi məlumat operatorları məlumatların emalının məqsədini, qanuni əsaslarını, məlumatların nə qədər saxlanıldığını və hər hansı bir üçüncü tərəflə və ya Avropa İqtisadi Bölgəsindən kənarda hər hansı bir yerdə bölüşdürülməməsi barədə dəqiq məlumat verməlidirlər. Şəxsi məlumat sahibləri istənilən vaxt saxlanılan məlumatların surətini tələb etmək və müəyyən şərtlərdə silmək hüququna malikdirlər. Müəssisələr istifadəçi məxfiliyinə mənfi təsir göstərən istənilən məlumat pozuntusu (məs., məlumatın oğurlanması) barədə 72 saat ərzində istifadəçilərə məlumat verməlidirlər. Əks təqdirdə qaydaların pozulduğu aşkar edilən şirkətlər 20 milyon avroya qədər və ya şirkətin illik gəlirinin 4 faizi qədər cərimə edilə bilər [3].

III. FƏRDİ MƏLUMATLARIN HÜQUQİ TƏNZİMLƏNMƏSİ

Heç bir qanunvericilik aktında fərdi məlumatların dəqiq siyahısı və ya sərhədi müəyyən olunmayıb. Azərbaycan qanunvericiliyinə görə, “fərdi məlumatlar - şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumatlardır”. “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanunun əsas məqsədi fərdi məlumatların toplanılmasının, işlənməsinin 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[4]. 2009-cu ildə Azərbaycan

Respublikası “Fərdi məlumatların avtomatlaşdırılmış qaydada işlənməsi ilə əlaqədar şəxslərin qorunması haqqında” Avropa Şurası Konvensiyasına qoşulmuşdur[5].

Azərbaycan Respublikasının Konstitusiyasının 50-ci maddəsinə əsasən hər bir şəxsin məlumat azadlığı vardır[6].

- Hər kəsin istədiyi məlumatı qanuni yolla axtarmaq, əldə etmək, ötürmək, hazırlamaq və yaymaq azadlığı vardır.
- Kütləvi informasiyanın azadlığına təminat verilir. Kütləvi informasiya vasitələrində, o cümlədən mətbuatda dövlət senzurası qadağandır.
- Hər kəsin kütləvi informasiya vasitələrində dərc edilən və onun hüquqlarını pozan və ya mənafeələrinə xələl gətirən məlumatı təkzib etmək və ya ona cavab vermək hüququna təminat verilir.

Təəssüf ki, hazırda bir çox mətbuat nümayəndələri bu qanundan sui-istifadə edərək şəxslərin fərdi məlumatlarını yayır və şəxsi məlumatların toxunulmazlığına xələl gətirirlər. Fərdi məlumatların bir çox qanunlarla tənzimlənməsinə baxmayaraq, bu sahədə müəyyən boşluqlar vardır. Qanunlara ciddi əməl olunmur. Bəzi televiziya kanalları və mətbuat orqanları reyting xətrinə və ya sifariş əsasında jurnalistin etik davranışlarından kənara çıxırlar. Hazırda media sahəsində və toy şənliklərinin çəkilişində dronlardan istifadə edilir. Pilotsuz uçan aparatların istifadəsini tənzimləyən qanun və ya qaydalar olmasa da, Cinayət Məcəlləsinin 156-cı maddəsində şəxsi həyatın pozulması maddəsində dronlardan istifadəyə görə məsuliyyət nəzərdə tutulub[7]. Qanuna görə şəxsi və ailə həyatının sirri olan video və foto çəkilişi materiallarının, səs yazılarının məsafədən idarə edilən pilotsuz uçan aparatlardan istifadə etməklə yayılması cinayət məsuliyyəti yaradır. Bu hal baş verdikdə təqsirləndirilən şəxs iki ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırıla bilər. Onlayn medianın hüquqi tənzimlənməsində olan problemlər fərdi məlumatların internet mühitində təhlükəsizliyinə zəmanət verə bilmir. Azərbaycan qanunvericiliyində 2017-ci ildə edilmiş əlavə və dəyişikliklər internet mühitində fərdi məlumatların qanunsuz dövriyyəsinin qarşısının alınmasına xidmət edir. Lakin bu məsələ ilə bağlı ölkəmizdə məhkəmə praktikası çox zəifdir, hüquqları pozulan şəxslər çox nadir hallarda məhkəmələrə müraciət edirlər.

IV. FƏRDİ MƏLUMATLAR VƏ KÜTLƏVİ MEDIA RESURLARI

Fərdi məlumatların qeyri qanuni yollarla yayılmasında elektron Kütləvi İnformasiya Vasitələri (KİV) və sosial şəbəkə istifadəçiləri xüsusi rol oynayırlar. KİV-də vətəndaşların fərdi məlumatlarının qanunsuz açıqlanmasının neqativ nəticələri ilə əlaqədar xəbərlərə tez-tez rast gəlmək mümkündür. Təəssüf ki, bu kimi hallarla bağlı tədqiqatlar aparılmır və statistik hesabatlar hazırlanmır[8]. Jurnalistlərin fərdi məlumatlarla işləyərkən müvafiq hüquqi tələbləri yaxşı bilməmələri və nəzərə almamaları bu cür halların kütləviləşməsinə səbəb olur. Mediada şəxsi həyata dair yanlış məlumatlar bir sıra hallarda müəyyən şəxsləri nüfuzdan salmaq, karyerasına zərbə vurmaq

və s. kimi neqativ məqsədlərlə yayılır. Texnologiyanın sürətli inkişafı nəticəsində dezinformasiya xarakterli montaj edilmiş audio, video, foto materialları yaymaq getdikcə sadələşir və kütləvi hal alır. Bu da göstərir ki, şəxsi həyatın toxunulmazlığının təmin olunması, fərdi məlumatların qorunması məsələləri müasir dövrdə informasiya texnologiyalarının inkişafı ilə bağlı olaraq çətinləşmişdir. İnternet xəbər istehsalçılarının bilərəkdən və ya bilməyərək “Xüsusi kateqoriyalı fərdi məlumatların şəxsi həyat”ın qorunması prinsipini intensiv şəkildə pozmaları, ümumiyyətlə, “Fərdi məlumatların qorunması” qanununa laqeyd yanaşmaları müşahidə olunur.

Azərbaycan Mətbuat Şurasının 2019-cu il üçün açıqladığı illik hesabatdan aydın olur ki, Şuraya il ərzində ünvanlanmış şikayətlərin bir qismi də məhz şəxsi həyat sirlərinin onlayn mediada pozulmasına aiddir [9]. “İnternet və xüsusi kateqoriyalı fərdi məlumatlar-şəxsi həyat” mövzusunda 25 iyun 2019-cu il tarixində Bakıda konfrans, Mingəçevir və Astarada isə bu mövzuda seminar keçirilib. Konfransda QHT rəhbərləri, media və ictimaiyyət nümayəndələri iştirak ediblər. Konfransın əsas məqsədinin həm global, həm də lokal səviyyədə ortaya çıxan fərdi məlumatların mühafizəsinə dair problemlərin aradan qaldırılmasına yardım göstərmək olduğu deyilib. Mətbuatda fərdi məlumatların icazəsiz olaraq yayımlanmasında anonim mənbələrdə rolu böyükdür. Etibarsız mənbələrə istinad edilərək hər hansı bir şəxs haqqında verilən fərdi məlumatlar həm KİV –nə, həm də həmin şəxsə problemlər yaradır.

NƏTİCƏ

Nəticə olaraq jurnalistlər informasiya hazırlayarkən etik dəyərlərini unutmamalı, hər kəsin fərdi həyatına hörmətlə yanaşmalıdır. Fərdi məlumatların mühafizəsinə dair qanunlar daha da gücləndirilməlidir. Reket jurnalistikasının inkişafına şərait yaranmamalıdır. Fərdi məlumatların yayılmasına icazə yalnız çox vacib situasiyalarda verilməlidir. Məsələn, hər hansı bir cinayətkar barədə məlumat yayılmasına zərurət yarandıqda fərdi məlumatların mühafizəsinə dair qanunlar pozula bilər. Əks təqdirdə belə halların baş verməsi qəbul edilməzdir.

İSTİNADLAR

- [1] A. Kemal, “Kişilik hakki kapsamında sosyal medyada kişisel verilerin korunması ve veri sahibinin rızası”, pp. 270 -300.
- [2] Avropada fərdi məlumatların mühafizəsi, pp.26, <http://academy-justice.gov.az>.
- [3] Data protection, https://ec.europa.eu/info/law/law-topic/data-protection_en.
- [4] Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu <http://www.e-qanun.az>.
- [5] “Fərdi məlumatların avtomatlaşdırılmış qaydada işlənməsi ilə əlaqədar şəxslərin qorunması haqqında” konvensiyanın təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu, <http://www.e-qanun.az/framework/18625>
- [6] Azərbaycan Respublikasının Konstitusiyası, <http://www.e-qanun.az/framework/897>.
- [7] Azərbaycan Respublikasının Mülki Məcəlləsi, <http://www.e-qanun.az/code/8>.
- [8] Azərbaycan Respublikasının Cinayət Məcəlləsi, <http://www.e-qanun.az/code/11>.
- [9] Əliyuliyev R.M., Mahmudov R.Ş “Milli mentalitet kontekstində fərdi məlumatların həssaslığı və onların təhlükəsizliyinin təmin olunması məsələləri” İnformasiya cəmiyyəti problemləri, 2019. vol 2, pp 117-128.
- [10] <http://www.presscouncil.az/az/news/114>.

ISSUES OF PERSONAL DATA PROTECTION IN MASS MEDIA RESOURCES

Sunbul Zalova

Institute of Information Technology of ANAS, Baku, Azerbaijan

sunbulzalova@gmail.com

Abstract— Personal data, the types of personal data and the issues of personal data protection in mass media resources are explored in this article. Laws in this area, the international experience, as well as experience in Azerbaijan are shown. A number of proposals for the solution of the problem are identified.

Keywords— *personal data, personal life, sensitive information, social media, mass media resources*

Vətəndaş elmi layihələrində fərdi məlumatların təhlükəsizliyinin təmini məsələləri

Nərgiz Verdiyeva

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
depart3@iit.science.az

Xülasə— Məqalə vətəndaş elmi layihələrində könüllü əsaslarla iştirak edən vətəndaşların fərdi məlumatlarının təhlükəsizliyinin təmin edilməsi məsələlərinə həsr olunmuşdur. Vətəndaşların fərdi məlumatları kateqoriyalara bölünərək təsnif edilmişdir. Fərdi məlumatların təhlükəsizliyinin mühafizəsini təmin edən normativ-hüquqi sənədlər nəzərdən keçirilmişdir. Mövcud vətəndaş elmi layihələrində vətəndaşların fərdi məlumatlarının qorunması yolları təhlil edilmişdir. Aparılmış tədqiqatlar əsasında ölkəmizdə bu istiqamətdə görülmüş işlər təhlil edilmiş və təkliflər verilmişdir.

Açar sözlər— *e-elm; vətəndaş elmi; təhlükəsizlik; fərdi məlumatlar; sensitiv məlumatlar.*

I. GİRİŞ

E-elmin yeni istiqaməti kimi formalaşan vətəndaş elmi İKT sahəsində əldə olunan nailiyyətlərin təsiri ilə sürətlə inkişaf etməkdədir. Əşyaların interneti, şəbəkə və bulud texnologiyalarının tətbiqi ilə bu inkişaf getdikcə artmaqdadır. Vətəndaş alimlər şəbəkə mühitində elmi tədqiqatlara töhfə vermək məqsədilə öz resurslarını şəbəkəyə qoşur, “ağıllı” telefonlar, planşetlər və digər qurğular müvafiq layihələrin həyata keçirilməsinə şərait yaradır. Vətəndaş elmi layihələrində toplanılan və emal olunan verilənlər böyük verilənlər (*Big Data*) problemini yaratdığından burada bulud texnologiyalarının imkanlarından istifadə olunur. Açıq kodlu proqram təminatı və bulud hesablamaları (*cloud computing*) yüksək məhsuldarlıqlı hesablamaların təmin edilməsi xərclərini xeyli azaldır.

İctimaiyyətin rolunun artması nəticəsində vətəndaş elmi ənənəvi elmdən daha çox müxtəliflik və çeviklik nümayiş etdirir. Vətəndaş elminin reallaşdırılması vasitəsi olan vətəndaş elmi layihələri elmdə mütəxəssislərlə yanaşı, adi vətəndaşların da iştirakının təmin edilməsində əhəmiyyətli rol oynayır [1]. Lakin hər bir vətəndaş elmi layihəsinin formalaşması zamanı qarşıya müəyyən problemlər çıxır. Bunlardan biri də təhlükəsizlik problemidir. Xüsusilə də vətəndaş elmi layihəsi iştirakçılarının fərdi məlumatlarının təhlükəsizliyinin mühafizəsi məsələsi aktual yer alır.

Məqalədə vətəndaş elmi layihələrində fərdi məlumatların təhlükəsizliyi problemləri tədqiq olunmuş və təhlükəsizliyin təmin olunmasının konseptual məsələləri təqdim olunmuşdur.

II. VƏTƏNDAŞ ELMİ LAYİHƏLƏRİNDƏ İŞTİRAKIN SPESİFİK XÜSUSİYYƏTLƏRİ VƏ TƏHLÜKƏSİZLİK PROBLEMLƏRİ

Vətəndaş elmi layihələrinin elmi əhəmiyyətinə baxmayaraq, qeyd etmək vacibdir ki, o, etik vətəndaş elminin inkişafı baxımından bu layihələrdə iştirak edən ayrı-ayrı şəxslər üçün yaranan təhdidlərin bir daha nəzərdən keçirilməsini tələb edir. Ənənəvi elmdə alimlərin, mütəxəssislərin fərdi məlumatlarının təhlükəsizliyinin mühafizəsini nəzərdə tutan qanunlar var. Lakin vətəndaş elmində bu, belə deyil. Vətəndaş elmi layihələrində inklüziv iştirakın təmin olunması nəticəsində burada müxtəlif kateqoriyalı insanlar iştirak etmək imkanı əldə edir. Burada inklüzivliyi bir neçə kateqoriyaya bölmək olar:

- Yaş həddi;
- Təhsil səviyyəsi;
- Fiziki vəziyyət;
- Sosiallaşma və s.

Vətəndaş elmində təhlükəsizlik məsələlərini üç qrupa bölmək olar:

- Texniki vasitələrin təhlükəsizliyi;
- Proqram vasitələrinin təhlükəsizliyi;
- İnformasiya təhlükəsizliyi.

Vətəndaş elmi layihələrində iştirak edən könüllülərin fərdi məlumatlarının qorunması, informasiya təhlükəsizliyinin tərkib hissəsi olaraq, aktual məsələ kimi xüsusi əhəmiyyətə malikdir.

Vətəndaş alimlər adətən tədqiqatçı heyət tərəfindən aparılan fəaliyyətə töhfə verir. Bu zaman onlara çox vaxt tədqiqat qrupu üzvlərinin rolları ilə oxşar rollar verilsə də, vətəndaş elmi ilə ənənəvi elm arasındakı struktur fərqlər normativlərin uyğunsuzluğuna gətirib çıxarır. Bu fərqlər ayrı-ayrı vətəndaş elmi layihələrinin tamlığını, təhlükəsizliyini və ya hədəflərini poza bilər.

Fərdi məlumatlar – birbaşa və ya dolayı yolla müəyyən olunan fiziki şəxsə (fərdi məlumatların subyektinə) aid olan ixtiyari informasiyadır. Fərdi məlumatlar onunla fərqlənir ki, onlar insanın şəxsiyyətini dəyərli iqtisadi xüsusiyyətlərlə birləşdirir [2]. Vətəndaşlar fərdi məlumatlarını öz çoxplanlı onlayn fəaliyyətlərinin izi olaraq qoyur. Bu informasiya onların

onlayn fəal şəkildə tranzaksiyalar üçün istifadə etdikləri informasiyadan əhəmiyyətli dərəcədə çoxdur. Telefonlardan tutmuş saatlara, məişət texnikasına, avtomobillərə və şəhərlərə qədər hər şeyin “ağıllı” olması səbəbindən vətəndaşların hərəkətləri və fəaliyyəti hətta onlayn olmadıqda belə qeydə alınır [3]. Şəbəkə mühitində vətəndaşlar öz resurslarını şəbəkəyə ötürmüş olur. Belə ki, hər bir vətəndaş öz fərdi kompüterindən, telefonundan şəbəkəyə daxil olduqda bu qurğudakı verilənlər şəbəkədə açıq olur. Bu da vətəndaş elminin reallaşması prosesində müxtəlif kateqoriyalı vətəndaşların konfidensiallığı üçün təhlükə və təhdidlər yaradır.

Fərdi məlumatları aşağıdakı kimi kateqoriyalara bölmək olar:

1) *Şəxsi məlumatlara* vətəndaşın kimliyini müəyyən etməyə imkan verən informasiya aiddir. Bu məlumatlar iki cür ola bilər: sosial və biometrik məlumatlar. Sosial məlumatlara şəxsin telefon nömrəsi, e-mail ünvanı, işlədiyi şirkətin adı, tutduğu vəzifə və s. aiddir. Biometrik məlumatlara barmaq izləri, nitq xüsusiyyətləri, gözün qüzhəli qışası, üz görünüşü və s. aid edilir;

2) *Sensitiv (həssas) məlumatlar* vətəndaşın irqi, dini və ya etnik mənşəyini, eləcə də sağlamlığı ilə bağlı informasiyanı aşkar etməyə imkan verən şəxsiyyəti təsdiq edən sənədlərdir;

3) *Uşaqlar haqqında məlumatlar* dedikdə, yetkinlik yaşına çatmamış (adətən 13 yaşdan kiçik) şəxslərin fərdi məlumatları nəzərdə tutulur;

4) *Coğrafi məkan haqqında məlumatlara* verilənlərin toplanıldığı, şəkil və videoların çəkildiyi coğrafi məkanların qeydə alınması aiddir.

III. ƏLAQƏDAR İŞLƏR HAQQINDA

Gündəlik həyatda vətəndaşlar rəqəmsal aləmdə proqram təminatı sistemləri ilə qarşılıqlı təsirdə olur. Bu sistemlər istifadəçilərlə bərabər və ya onların əvəzinə qərar qəbul etməkdə avtonomdur [4]. Çox vaxt bu avtonomluq sistemin sərhədlərini aşır və istifadəçi səlahiyyətlərinə təsir edir. Nəticədə etik problemlər, təhlükəsizlik problemləri də daxil olmaqla (məsələn, fərdi məlumatların icazəsiz alınması) ciddi narahatlığa səbəb olan məsələlər meydana çıxır. Bu problemlər hər bir insanın mənəvi haqlarına təsir göstərir və sosial, iqtisadi, siyasi sahələri əhatə edir [5-7].

Avropa Vətəndaş Elmi Assosiasiyasının (European Citizen Science Association – ECSA) təşəbbüsü ilə bəyan edilmiş “Vətəndaş elminin 10 prinsipi” içərisində fərdi məlumatların təhlükəsizliyinin qorunması ilə bağlı “Vətəndaş elmi layihələrinin liderləri müəllif hüququ, intellektual mülkiyyət, informasiya mübadiləsi haqqında razılıq (müqavilə), konfidensiallıq, məsuliyyət, ətraf mühitə təsir ilə əlaqədar hüquqi və etik aspektləri nəzərə alır” prinsipi vardır [8].

Fəlsəfi aspektlərlə yanaşı bu problemlərə həm tənzimləyici, həm də texniki baxımdan iki cür yanaşma ola bilər. Avropada Verilənlərin Mühafizəsi üzrə Ümumi Reqlament qanunvericiliyi yaradılmışdır (*General Data Protection*

Regulation – GDPR). Bu qanunvericilik 2016-cı il aprelin 27-də qəbul edilmiş, 2018-ci il mayın 25-də isə qüvvəyə minmişdir. GDPR-in əsas prinsipləri içərisindəki fərdi məlumatların emalı ilə bağlı prinsiplərə əsasən, fərdi məlumatlar onların subyektinə qarşı qanuni, ədalətli və şəffaf bir şəkildə emal olunmalıdır (“qanunilik, ədalət və şəffaflıq”) [9].

Fiziki şəxsin sağlamlığı ilə bağlı fərdi məlumatlarının toplanılmasına iki cür yanaşma mümkündür. Belə ki, bir tərəfdən sağlamlıq problemi olan vətəndaşlar bir-birlərinin diaqnozlarından xəbərdar olmaqla digər oxşar xəstələrdən məsləhət ala bilər, bu isə onlara həm sağlamlıq vəziyyətini yaxşılaşdırmağa imkan verir, həm də mənəvi dəstək olur. Digər tərəfdən, bəzi vətəndaşlar öz fiziki məhdudiyyətlərinin başqalarına məlum olmasını istəmirlər. Bu da onlarda olduqca mənfi reaksiyaya səbəb olar və hətta stress yaradaraq sağlamlılıqlarında ciddi problemlərə yol açə bilər. Bu baxımdan vətəndaşların sağlamlığı ilə bağlı məlumatlar həssas (sensitiv) məlumat hesab edilir və bu cür məlumatların gizliliyinin qorunması xüsusi diqqət tələb edir.

Sağlamlıqla əlaqəli həssas məlumatların təhlükəsizliyinin qorunmasını *PatientsLikeMe* layihəsində öz əksini tapmışdır. Belə ki, burada xəstəliyin tarixi, qoyulmuş diaqnozlar, allergiyalar, cari müalicə və s. kimi tibbi məlumatların yalnız pasiyentlər və tibbi xidmət üçün açıq olması göstərilir [10].

ABŞ-da vətəndaşların, o cümlədən vətəndaş elmi ilə məşğul olanların fərdi məlumatlarının məxfiliyinin qorunması ilə əlaqəli federal qanunlar var [11]. Bu qanunlardan vətəndaş elmi layihələrində ən geniş tətbiq olunan Uşaqların Onlayn Gizliliyinin Qorunması Qanunudur (*The Children’s Online Privacy Protection Act – COPPA*). Bu qanun 13 yaşından kiçik uşaqların şəxsi məlumatlarının toplanılması ilə əlaqədardır. COPPA bir çox, xüsusilə də təhsil komponenti olan layihələri əhatə edir. Tibbi Sığorta Daşınması və Hesabatlılıq Qanunu (*Health Insurance Portability and Accountability Act – HIPAA*) tibbi qeydlərin məxfiliyini qoruyan qanundur. Məxfilik Aktı (*Privacy Act*) federal qurumların şəxsiyyəti müəyyənləşdirən məlumatları toplaması, istifadə etməsi və paylanmasını məhdudlaşdırır. Bu, federal qurumların özləri tərəfindən maliyyələşdirilən layihələrdə öz tətbiqini tapır. Məlumat Azadlığı Qanunu (*The Freedom of Information Act – FOIA*) vətəndaşların federal hökumət tərəfindən saxlanılan qeydlərə giriş hüququnu təmin edən qanundur. Şəxsiyyəti müəyyənləşdirən məlumatları (*personally identifiable information – PII*) ictimai qeydlərdən mühafizə edən bu qanun da həmçinin federal qurumların maliyyələşdirdiyi layihələrdə tətbiq edilir.

Elm və Texnologiya Siyasəti İdarəsi (Office of Science and Technology Policy – OSTP) tərəfindən təsdiqlənmiş memorandumlar (www.whitehouse.gov/ostp) bu sahədə ABŞ-ın əlavə mənbələridir. Məsələn, “Federal Maliyyələşdirilən Tədqiqatın Nəticələrinə İctimai Girişin Gücləndirilməsi” adlı bir memorandum agentliklərə şəxsi konfidensiallığın qorunması ilə yanaşı, nəşr olunmuş verilənlərə də giriş imkanını genişləndirməyi təklif edir.

Birləşmiş Ştatlar xaricində standartlara İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı (Organization for Economic Cooperation and Development – OECD) tərəfindən təsdiq edilmiş prinsiplər daxildir [12]. Avropa Birliyinin Gizlilik və Elektron Rabitə üzrə Direktivinə görə (*E.U.'s Directive on Privacy and Electronic Communications*), veb-saytlar, cookie-fayllar daxil olmaqla, verilənlərin toplanılması təcrübələrini açıq şəkildə göstərməlidirlər. Bu direktiv Avropa Birliyində biznes həyata keçirən layihələrə aiddir [13].

İnsan Hüquqları üzrə Avropa Konvensiyasının (European Convention on Human Rights) 8-ci bəndində göstərilmişdir ki, fərdi məlumatlar vətəndaşların hüquqlarının ayrılmaz bir hissəsidir, vətəndaşların şəxsi həyatına və yazışma sirlirinə hörmət edilməlidir.

Vətəndaş elmi layihələrinin koordinatorları könüllülərin fərdi məlumatlarını qorumaq məqsədilə texnoloji mühafizə və informasiya siyasətləri kimi bir sıra mexanizmləri tətbiq edirlər. Bunlardan məkanın vizual görüntüsünün bulanıqlaşdırılması və ya gizlədilməsi metodu geniş istifadə olunur [14]. Bəzi sistemlərdə vizual görüntüsü bulanıq olan verilənlər olur, yəni dəqiq məkan qeyri-müəyyən edilir. Bunu vətəndaş elmi layihələrinin koordinatorları edir ki, məkanı təkcə özləri görə bilsin. Məkanın vizual görüntüsünün bulanıqlaşdırılması metodu daha çox landşaftı gizlətmək üçün tətbiq edilsə də, insanlar bu metoddan öz yaşayış yerlərinin gizlədilməsi məqsədilə xeyli faydalana bilər.

Toplanılan və paylaşılan şəxsi informasiyanın həcmnin minimallaşdırılması konfidensiallığın qorunması üçün istifadə edilən daha bir metoddur. Verilənləri kimin təqdim etdiyinin məlum olması elmi cəhətdən əhəmiyyət kəsb etdiyi üçün, bir çox layihələr könüllünün təqdim etdiyi verilənləri onun adı ilə əlaqələndirir. Bu cür informasiyanın göstərilməsi barədə seçimdən asılı olaraq vətəndaş elmi layihələrinin koordinatorları könüllülərə hər iki seçimi – həm anonim identifikasiya, həm də öz istifadəçi adlarını yaratmağı təqdim edirlər.

IV. VƏTƏNDAŞ ELMİ LAYİHƏLƏRİNDƏ FƏRDI MƏLUMATLARIN TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİNİN KONSEPTUAL MƏSƏLƏLƏRİ

Virtual aləmdə və vətəndaş elmi layihələrində vətəndaşların şəxsi həyatı haqqında verilənlərin mühafizəsi böyük əhəmiyyətə malikdir. Fərdi məlumatların toplanılması, emalı və saxlanması məsələlərinin effektiv həlli vətəndaş elmi layihələrinin iştirakçılarının təhlükəsizliyi üçün ən mühüm məsələlərdən biridir [11].

Ölkəmizdə vətəndaşların fərdi məlumatlarının təhlükəsizliyinin qorunması ilə bağlı həyata keçirilən tədbirlər sırasında normativ-hüquqi sənədlər xüsusi yer tutur. “Fərdi məlumatlar haqqında” AR Qanununun 8-ci maddəsində deyilir: “Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən olunmuş qaydada fərdi məlumatların məcburi şəkildə toplanılması və işlənilməsi halları istisna olmaqla, hər hansı şəxs barəsində fərdi məlumatların toplanılmasına 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 məlumatların toplanılması, emalı və ötürülməsi yalnız “Fərdi məlumatlar haqqında” Qanuna uyğun olaraq həyata keçirilə bilər.

AR Konstitusiyasının 50-ci maddəsinə görə, hər kəsin istədiyi informasiyanı qanuni yolla axtarmaq, əldə etmək, ötürmək, hazırlamaq və yaymaq azadlığı vardır. Bununla yanaşı, informasiya azadlığının həyata keçirilməsi digər insanların hüquqlarının, azadlıqlarının və qanuni maraqlarının pozulmasına səbəb olmamalıdır.

Avropa Vətəndaş Elmi Assosiasiyasının “Vətəndaş elminin on prinsipi” içərisində fərdi məlumatlarla bağlı qeyd etdiyimiz prinsip, eləcə də Verilənlərin Mühafizəsi üzrə Ümumi Reqlament qanunvericiliyi kimi normativ-hüquqi sənədlər ölkəmizdə vətəndaş elmi ilə məşğul olan şəxslərin fərdi məlumatlarının təhlükəsizliyini təmin etmək üçün nəzərə alınmalıdır.

Beləliklə, bu sahədə beynəlxalq təcrübənin nəzərə alınması, həmçinin ölkədə müvafiq normativ-hüquqi sənədlərin hazırlanması və onlara riayət edilməsi vətəndaşların onlayn mühitdə təhlükəsizliyinin təmin edilməsini təmin edəcəkdir.

Vətəndaş elmi layihələri çərçivəsində vətəndaşların fərdi məlumatlarının mühafizəsi məqsədilə görülən tədbirlər proqnozlaşdırıcı, qabaqlayıcı və aradan qaldırıcı olmaqla qruplara bölünərək layihələndirmə prosesində nəzərə alınmalıdır:

1. *Proqnozlaşdırıcı tədbirlər* mövcud sistemlərdəki potensial təhlükə və təhdidlərin aşkarlanmasını nəzərdə tutur. Bu məsələnin həlli üçün analitik metodlardan istifadə olunmalıdır.
2. *Qabaqlayıcı tədbirlər* potensial təhlükənin baş verməsinin qarşısını almaq məqsədilə görülən işlərdir. Qabaqlayıcı tədbirlərin görülməsi üçün ilk növbədə proqnozlaşdırıcı tədbirlər həyata keçirilməlidir.
3. *Aradan qaldırıcı tədbirlər* artıq baş vermiş olan təhlükəsizlik problemlərinin həll edilməsində tətbiq olunur. Bu zaman əvvəllər mövcud olmuş və ya baş vermiş təhdidlərin aradan qaldırılması və yox edilməsində istifadə olunan təhlükəsizlik tədbirləri həyata keçirilir.

Vətəndaş elmi layihələrinin veb-saytları, eləcə də istifadə edilən proqram təminatı işlənilib hazırlanarkən proqramçılar bu məsələlərə diqqət yetirməlidirlər. Veb-saytın ana səhifəsinin müvafiq bölməsində təhlükəsizlik siyasəti barədə lazımi informasiya qeyd edilməlidir. Bu, layihədə iştirak etmək üçün qeydiyyatdan keçmək istəyən vətəndaşlara qeydiyyatı təhlükəsizlik şərtlərini əvvəlcədən bilərək tamamlamağa imkan verir.

Vətəndaş elmi layihələri çərçivəsində vətəndaşların fərdi məlumatlarının mühafizəsi məqsədilə onlayn mühitdə onların biometrik göstəricilərindən istifadə etmək ən əlverişli və eyni zamanda etibarlı üsullardan biridir. Layihə üçün qeydiyyatdan keçmiş hər bir iştirakçı öz şəxsi səhifəsinə giriş üçün yalnız öz biometrik göstəricilərindən istifadə etməlidir. Bu isə kənar

şəxslərin girişini məhdudlaşdıraraq, iştirakçıların fərdi məlumatlarının gizliliyini qorumaq üçün həyata keçirilir.

Fərdi məlumatların təhlükəsizliyinin təmin edilməsi üçün görülən işlər yuxarıda qeyd olunmuş üç istiqamətdə qurulmalıdır. Ən yaxşı hal üçüncü mərhələyə ehtiyac olmadığı haldır: belə ki, bütün potensial təhlükə və təhdidlər nəzərə alınarsa, onların qarşısını qabaqcadan almaq mümkün olar. Lakin müasir dövrdə İKT-nin sürətli inkişafı, bu sahədə əldə olunan nailiyyətlər bir tərəfdən həll yolları, digər tərəfdən isə yeni təhlükə və təhdidlər ortaya çıxarır. Buna görə də yuxarıda qeyd etdiyimiz hər üç mərhələ eyni dərəcədə vacib hesab edilməli, bu istiqamətdə fəal işlər aparılmalıdır.

Müxtəlif vətəndaş elmi layihələrinin rəhbərləri bu tədbirləri uğurla tətbiq edərək, öz layihələrində iştirakı onlayn mühitdə vətəndaşlar üçün daha təhlükəsiz və etibarlı edə bilər.

NƏTİCƏ

Aparılmış araşdırmalar göstərir ki, müasir dövrdə İKT-nin sürətli inkişafı, o cümlədən IoT, şəbəkə və bulud texnologiyalarından istifadə elmin, xüsusən də e-elmin yeni istiqaməti olan vətəndaş elminin geniş tətbiqinə yol açmışdır. Bunun nəticəsi olaraq vətəndaş elmi layihələrinin və onlarda iştirak edən könüllülərin sayı artmışdır. Layihə iştirakçılarının sayı artdıqca onların fərdi məlumatlarının qorunması problemi mürəkkəbləşir. Bu sahədə təhlükəsizlik məsələlərinin nəzərə alınması, lazımi tədbirlərin görülməsi vətəndaşların öz fərdi məlumatları ilə bağlı narahatlıqlarını aradan qaldırmaqla, gələcəkdə vətəndaş elmi layihələrinin iştirakçılarının sayını artıracaq, bununla da vətəndaş elmini daha da inkişaf etdirəcəkdir.

İSTİNADLAR

- [1] T.X. Fətəliyev, “Vətəndaş elmi e-elmin inkişafının yeni istiqaməti kimi,” *İnformasiya cəmiyyəti problemləri*, №1, s. 57-64, 2014.
- [2] B. Roessler, “Should Personal Data Be a Tradable Good? On the moral limits of markets in privacy” in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspective* (Cambridge: Cambridge University Press 2015)
- [3] M. Autili, D. Di Ruscio, P. Inverardi, P. Pelliccione, M. Tivoli, “A software exoskeleton to protect and support citizen’s ethics and privacy in the Digital World”, *IEEE Access*, 19 May 2019, pp.62011-62021.
- [4] P. Inverardi, “The european perspective on responsible computing”, *Commun. ACM*, vol. 62, no. 4, pp. 64, Mar. 2019.

- [5] European Group on Ethics in Science and New Technologies, 2018, <https://ec.europa.eu/research/egp/pdf/egestatements2018.pdf>
- [6] J. P. Burgess, L. Floridi, A. Pols, J. van den Hoven, Towards A Digital Ethics–EDPS Ethics Advisory Group, 2018, https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf
- [7] Leading by Example The EDPS Strategy 2015-2019, 2015, [online] Available: https://edps.europa.eu/sites/edp/files/publication/15-07-30_strategy_2015_2019_update_en.pdf
- [8] 10 Principles of citizen science, <https://ecsa.citizen-science.net/engage-us/10-principles-citizen-science>
- [9] GDPR, <https://gdpr-info.eu/art-5-gdpr/>
- [10] J.H. Frost, M.P. Massagli, Social Uses of Personal Health Information Within PatientsLikeMe, an Online Patient Community: What Can Happen When Patients Have Access to One Another’s Data. *Journal of Medical Internet Research*, 2018, doi: 10.2196/jmir.1053.
- [11] T.X. Фатәлиев, Н.Н. Вердиева, Вопросы обеспечения информационной безопасности в проектах гражданской науки, VII Международная научно-практическая конференция “Информационные технологии: проблемы и решения”. Уфа, 2019, сс. 50-55.
- [12] OECD Guidelines on the Protection of Privacy and Transborder, www.oecd.org/internet/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm
- [13] A. Bowser and o., “Sharing data while protecting privacy in citizen science”, *Interactions*, Vol. 21, Issue 1, 2014, pp. 70-73.
- [14] B. Sullivan, et al., “The eBird enterprise: An integrated approach to development and application of citizen science”, *Biological Conservation* 169, 2014, pp.31-40.

ISSUES OF ENSURING SECURITY OF PERSONAL DATA IN CITIZEN SCIENCE PROJECTS

Nargiz Verdiyeva

Institute of Information Technology of ANAS, Baku,
Azerbaijan

depart3@iit.science.az

Abstract– The article is dedicated to the issues of ensuring security of personal information of citizens participating voluntarily in citizen science projects. Citizens’ personal data are categorized and classified. Regulatory and legal documents providing security of personal data are reviewed. Ways of protecting personal information of citizens in existing citizen science projects are analyzed. Based on the research carried out, the work done in this direction in our country is analyzed and recommendations are made.

Keywords– *e-science; citizen science; security; personal data; sensitive information.*

Big data mühitində fərdi məlumatların təhlükəsizliyi

Məkrufə Hacırahimova¹, Aybəniz Əliyeva²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
makrufa@science.az, ²aliyeva.a.s@mail.ru

Xülasə—Big data insanlara rahatlıqla bərabər müəyyən risklər də gətirir. Verilənlərin toplanması, saxlanması və istifadəsi prosesində fərdi məlumatların asanlıqla sızması və gizli verilənlərin aşkar edilməsi fərdi məlumatların məxfiliyinin qorunması üçün problemlər yaradır. İşdə fərdi məlumatların təhlükəsizlik problemləri və səbəbləri tədqiq olunur, fərdi verilənlərin məxfiliyinin qorunmasına dair bəzi prinsiplər nəzərdən keçirilir.

Açar sözlər—big data; big data analitika; fərdi məlumatların qorunması; verilənlərin gizliliyi; informasiya təhlükəsizliyi

I. GİRİŞ

Rəqəmsal verilənlər dövrünün meydana gəlməsi Big data-nın insanların həyat tərzinə, iş və təhsil vərdişlərinə getdikcə daha çox təsir etməsi, eyni zamanda insanlara rahatlıq gətirməsi ilə yanaşı, insanların bir çox informasiya təhlükəsizliyi təhdidləri və problemləri ilə üz-üzə qalmasına səbəb olur. Fərdi məlumatların təhlükəsizliyi belə problemlərdən biridir. Big data dövründə, davamlı olaraq böyük həcmdə fərdi məlumatlar daxil edilir, eyni zamanda, fərdi məlumatların qanunsuz əldə edilməsi, yayılması və tətbiq vasitələri sürəkli olaraq ortaya çıxır. Bu məlumatların İnternet mühitində fırıldaqçılıq məqsədləri üçün istifadəsi insanların həyatı üçün böyük fəsadlar və hətta əhəmiyyətli iqtisadi zərərlər yarada bilər. Müasir dünyada çoxlu sayda şirkətlər hər gün milyardlarla fərdi məlumatı istifadə edərək böyük gəlir əldə edirlər. Bəzi qiymətləndirilmələrə görə təkcə Avropa İttifaqında məlumatların ticarəti üzrə ixtisaslaşdırılmış, "verilənlərin brokerləri" adlandırılan 50-yə yaxın böyük şirkət fəaliyyət göstərir [1]. Bir sıra ölkələr təşkilatlardan fərdi məlumatların qorunmasını tələb edən qanun və qaydalar qəbul etsələr də, fərdi məlumatların sızması hadisələri adi hal almışdır. Fərdi məlumatların oğurluğu üzrə Resurs Mərkəzi (Identity Theft Resource Center) [2] və Açıq Təhlükəsizlik Fondunun (Open Security Foundation) [3] statistikasına görə, fərdi məlumatlarla əlaqəli qayda pozuntuları getdikcə çoxalmış və son zamanlarda milyonlarla fərdi məlumat yazılarının itməsinə səbəb olmuşdur.

Bir sıra təşkilatlar fərdi məlumatların qorunması sistemlərini yaratmağa kömək etmək üçün tövsiyələr təklif edirlər. 1995-ci ildə Avropa Parlamenti Komissiyası, Avropa İttifaqına üzv olan ölkələrdən İqtisadi əməkdaşlıq və inkişaf təşkilatının (Organisation for Economic Co-operation and Development – OECD) qaydalarını təsdiq edən fərdi məlumatların qorunması qanunları (və ya qaydaları) olmayan

ölkələrə fərdi məlumatların ötürülməsini qadağan edən direktiv (Directive 95/46/EC) qəbul etdi [4].

27 aprel 2016-cı il tarixdə Avropa Parlamentinin və Şurasının qərarı ilə fərdi məlumatların mühafizəsi ilə əlaqədar olaraq Məlumatların Qorunmasının Ümumi Qanunu (General Data Protection Regulation – GDPR) qəbul edilmişdir. Bu nizamnaməyə uyğun olaraq ad və soyad, şəxsiyyət vəsiqəsinin nömrəsi, doğum tarixi, yaşayış yeri, e-mail və telefon, IP-ünvanı kimi fərdi məlumatlar praktiki olaraq sərbəst girişə malikdirlər. Lakin xüsusi kateqoriyalara aid olan fərdi məlumatlar, xüsusi halda irq və milliyət, siyasi baxışlar, dini, biometrik məlumatlar (barmaq izləri, gözün torlu qişası, səsini yazısı və s.), sağlamlıq haqqında məlumatlar və genetik məlumatların emalı GDPR-in ümumi qaydalarına görə qadağan edilmişdir. Verilənlərin subyektləri nəzərdə tutulmuş məqsədlər üçün göstərilən fərdi məlumatların emalına öz razılığını verməlidir. Eyni zamanda fərdi məlumatların xüsusi kateqoriyalarının emalı mümkün olduqda belə onların məxfiliyinin qorunmasına riayət edilməlidir. Məxfiliyin meyarları Avropa Birliyinin və ya üzv dövlətin hüquqları və ya milli səlahiyyətli orqanlar tərəfindən nəzərdə tutulmuş normalarla təyin edilir [3].

Hazırda bir çox ölkələrdə, o cümlədən Azərbaycanda fərdi verilənlərin qorunması üzrə qanun [5] fəaliyyət göstərir. Verilənlərin qorunması qanunlarının əksəriyyəti OECD Təlimatlarının [6] rəhbər prinsiplərinə uyğun olaraq işlənib hazırlanmışdır. OECD Təlimatları müəyyən edilmiş prinsiplərlə verilənlərin toplanması, verilənlərin keyfiyyəti, məqsədin spesifikasiyası, istifadənin məhdudlaşdırılması, təhlükəsizliyə təminat, açıqlıq, fərdi iştirak və hesabatlılığı əhatə edir.

II. BIG DATA VƏ FƏRDİ MƏLUMATLAR

Fərdi məlumatlar, identifikasiya olunmuş şəxsə aid olan məlumatlardır. Big data dövründə fərdi məlumatlarla bağlı yaranan problemləri dərk etmək üçün ilk növdə ondakı yeniliyin və fərqliliyin nə olduğunu anlamaq vacibdir. Big data konsepsiyası kifayət qədər tanınsa da, tam yaxşı başa düşülmür və "ümumiləşdirilmiş, dəqiq olmayan bir termin" kimi təsvir edilir [7, 8]. Big data adətən "həcm, sürət və müxtəliflik" kimi xüsusiyyətləri ilə müəyyən edilir. Big data böyük həcmdə verilənlər yığını ilə bərabər verilənlərin analizi və istifadəsi üsullarındakı dəyişikliyi də özündə birləşdirir.

Big data dövründə təşkilatlar üçün yüksək dəyər ifadə edən fərdi məlumatlar daha çox istifadə olunur. Big data-nın meydana gəlməsi müəssisə və təşkilatların qərarların qəbulu prosesini yaxşılaşdırmasına və verilənlərin analizinə yeni yanaşmanın tətbiqi hesabına yeni imkanlar əldə etməsinə şərait yaradır. Big data verilənlərin analizinin ənənəvi formalarını dəyişdirdi və böyük verilənlərin analitikası (Big data analytics, BDA) adlanan yeni bir proqnozlaşdırıcı yanaşma yaratdı [9]. Böyük verilənlərin analitikası verilənlərin ənənəvi analizindən fərqlənən üç əsas xüsusiyyətə – alqoritmlərdən istifadə, “bütün verilənlər”dən istifadə və verilənlərin təkrar istifadəsinə (repurposing data) malikdir [6, 8].

Fərdi məlumatların analitikasının aparılması üçün müxtəlif mənbələrdən istifadə olunur. “Əşyaların İnterneti”nin bir hissəsini təşkil edən obyektlərin istifadə dairəsi genişləndikcə yaranan fərdi məlumatların da həcmi artır. Bu fərdi məlumatlar həm dövlət, həm də özəl şirkətlər üçün olduqca dəyərlidir.

Digər bir zəngin mənbə, İnternet forumlarda, sosial şəbəkələrdə, icmal saytlarında, xəbər qruplarında və bloqlarda əlyətərlə olan böyük həcmdə sosial məlumatlardır. İnternetin insanlara verdiyi imkanların hesabına fərdi məlumatların həcmi əhəmiyyətli dərəcədə artır.

Beləliklə, toplanmış verilənlər fərdlərin hobbiləri, bəyənmələr və bəyənməmələri, sağlamlıq vəziyyəti, sosial və ailə şəbəkələri, siyasi görüşləri, elektron cihazlardan və məişət texnikasından istifadə də daxil olmaqla, insanların həyatının əksər aspektlərinə aydınlıq gətirir. Yeni korrelyasiyaları axtarmaq üçün bu böyük həcmdə verilənlərin öyrənilməsi (mining) fərdi məlumatlar üçün bir çox potensial tətbiqlərə səbəb olur. Belə tətbiqlərdən biri problemlərin yeni həll yollarının axtarılmasıdır (korrelyasiyalar müəyyən bir konkret problemin mümkün həllini təklif edə bilər). Korrelyasiyalar insanların davranışına təsir etməklə, ayrı-ayrı şəxslərə aid qərarların qəbuluna, müəyyən risklər və ya təhdidlərin qabaqcadan aradan qaldırılmasına yönəldilmiş üsulları da təklif edə bilərlər.

III. FƏRDİ VERİLƏNLƏRİN POTENSİAL İMKANLARI VƏ ZƏRƏRLƏRİ

A. Fərdi verilənlərin Potensial Faydaları

Fərdi məlumatların potensial faydaları məntiqi olaraq onun potensial istifadəsi ilə bağlıdır. Kommersiya baxımından verilənlər olduqca qiymətli bir aktiv və “dəyər yaratmaq mənbəyidir” [8]. Xüsusilə, pərakəndə satış sektoru insanların nəyi və nə vaxt alacağı ilə bağlı proqnoz verməyi asanlaşdıran bir vasitə olaraq fərdi verilənlərin analizindən istifadə edir. Nümunə üçün, ABŞ-da Wal-Mart ticarət mərkəzi maliyyələşməni tənzimləmək və mağazada satışın uyğun vaxtını proqnozlaşdırmaq üçün demoqrafik və hava məlumatları ilə birlikdə satış, qiymət və iqtisadi göstəricilər haqqındakı verilənləri də istifadə edir. Pərakəndə satışda da malların qiymətlərini tələb və təklif əsasında tənzimləmək üçün fərdi məlumatlardan istifadə olunur. ABŞ-da “Stage Stores” pərakəndə satış şəbəkəsi hər hansı bir mağazada konkret bir

malın qiymətini azaltmağın ən yaxşı vaxtını elan edən “endirim optimallaşdırması” üçün böyük həcmdə fərdi məlumatlardan istifadə edir [8].

Böyük həcmli fərdi məlumatların daha bir istifadəsi pərakəndə satışda tələbə uyğun olaraq reklamın anında həyata keçirilməsinə kömək etməsidir. Başqa sözlə, fərdi məlumatlar kredit risklərinin qiymətləndirilməsində və sığorta nəticələrinin proqnozlaşdırılmasında istifadə olunur. “İnsanların analitikası” (“istedadların analizi”) sahələri hansı namizədlərin işə götürüləcəyi, işçilərin əmək məhsuldarlığının yaxşılaşdırılması, işçinin işdən çıxması və ya işdən çıxarılmasına dair proqnozlar verməyə imkan verir.

İnsanların sağlamlığı və təhlükəsizliyi baxımından Big data xəstəliyin yayılması və ya təbii fəlakətlərin baş verməsi kimi məsələlərdə proqnozların verilməsinə yardım edə bilər. Həmçinin xəstəliyin diaqnozunda və dərmanların mənfi təsirlərinin müəyyən edilməsində kömək edə bilər, yol qəzaları və tıxacların baş vermə ehtimalını təxmin etməyə kömək edə bilər. Böyük verilənlər təhlükəsizlik və hüquq mühafizə risklərini də müəyyənləşdirməyə kömək edə bilər.

Fərdi məlumatlar özəl istehlakçılar üçün xidmət və məhsulların təqdimini asanlaşdırır, aviaşirkət biletləri kimi mal və ya xidmətlərin alışı üçün ən uyğun vaxtı təyin etməklə istehlakçıların imkanlarını genişləndirə bilər [8].

B. Fərdi Verilənlərin Potensial Zıyanları

Fərdi məlumatların yayılması nəticəsində yaranan zərərlər iki qrupa ayrılır. Birincisi, bütün böyük verilənlər üçün ümumi xarakter daşıyır və verilənlərdəki çatışmazlıqlar, tətbiq olunan analitik alətlər və ya müəyyən edilmiş nümunələrin həqiqi korrelyasiyalara malik olmaması səbəbindən yanlışlığa gətirən potensial imkanları ilə bağlıdır. İkincisi, onun gizliliyi pozmaq imkanı ilə bağlıdır. Bu özlüyündə bir zərərdir, eyni zamanda əlavə təhdidlərə səbəb ola bilər [4,8].

İnsan hüquqlarının əsasını təşkil edən dəyərlərin qorunmasında məxfilik başlıca rol oynadığından fərdi məlumatların məxfiliyinin qorunması vacibdir. Böyük fərdi məlumatlar məxfiliyə zərər yetirir, çünki bu, ayrı-ayrı şəxslərin fərdi məlumatlarına nəzarəti həyata keçirmək qabiliyyətini aradan qaldırır və bununla da insanın öz seçiminə uyğun olaraq həyatını yaşamaq və nizamlamaq hüquqlarını pozur [7,8].

Boyd və Crawford tərəfindən qeyd edildiyi kimi [10] İnternet mənbələrindən əldə olunan verilənlər dəstləri çox vaxt etibarlı deyil, itkilərə meyllidir və çox sayda verilənlər dəsti birlikdə istifadə edildikdə bu xətalər və boşluqlar daha da artır. Belə məlumatlar ədalətsiz qərarların qəbuluna səbəb ola bilər və fərdi şəxslərin ləyaqətinə xələl gətirə bilər.

Digər bir məsələ, fərdi məlumatlar əsasında fərdin zəif cəhətlərinin aşkar edilməsi və müəyyən məqsədlər üçün istifadəsi ilə bağlıdır. Məsələn, 2016-cı ildə ABŞ-da prezident seçkilərinin nəticələrinə təsir etmək üçün namizədə qarşı siyasi kompaniyada onun istifadəsi buna bir nümunədir [8, 11]. Fərdi məlumatlar əsasında qərarların qəbulu ayrı-ayrı şəxslərə qarşı haqsızlığa və ayrı-seçkiliyə səbəb ola bilər. Bəzi sektorlarda bu

cür təcrübələr adi hal alsada, fərdi məlumatların əlyetərliyi sığorta sektoru kimi sahələrdə də belə halların yaranmasına şərait yaradır.

Fərdi məlumatlarla bağlı fəaliyyəti asanlaşdırmaq üçün tələb olunan fərdi məlumatların geniş şəkildə toplanması da digər bir problem yarada bilər, insanların oğurluğa və saxtakarlığa məruz qalmasına səbəb ola bilər.

IV. FƏRDİ MƏLUMATLARIN GİZLİLİYİNİN QORUNMASI PROBLEMLƏRİ

Təhlükəsizlik nöqteyi-nəzərindən böyük verilənlər üçün ən böyük problem istifadəçinin məxfiliyinin qorunmasıdır. Böyük verilənlərin bir çox hallarda çoxlu sayda fərdi məlumatları özündə birləşdirməsi istifadəçilərin məxfiliyinə çox böyük təhlükə yaradır. İstifadəçilərin məxfiliyi aşağıdakı hallarda pozula bilər [6]:

- a) *Kənar verilənlər yığımı ilə birləşdirildikdə fərdi məlumatlar istifadəçilər haqqında yeni faktların ortaya çıxmasına səbəb ola bilər.* Bu faktlar gizli ola bilərlər və başqalarına açıqlanmamalıdır.
- b) *Fərdi məlumatlar bəzən biznesə dəyər əlavə etmək üçün toplanır və istifadə olunur.* Məsələn, fərdi alış-veriş vərdisləri bir çox şəxsi məlumatları üzə çıxara bilər.
- c) *Həssas məlumatlar düzgün şəkildə qorunmayan bir yerdə saxlanılır və emal olunur.* Bu halda saxlama və emal mərhələlərində məlumatların sızması baş verə bilər.

Fərdi məlumatların qorunması üzrə mövcud qanun və qaydalar adətən fərdi məlumatların məxfiliyinin və transsərhəd axınlarının qorunması üzrə OECD Təlimatlarına əsaslanır. Bir təşkilat və ya məlumat toplayıcısı verilənlər subyektlərinin fərdi məlumatlarını toplamaq və ya istifadə etmək istəyirsə OECD-nin aşağıdakı qaydalarına əməl etməlidir [4]:

- **Toplama və məhdudiyyət (Collection and limitation)** – Şəxsi məlumatların toplanmasında məhdudiyyətlər olmalıdır. Bundan əlavə, məlumatlar verilənlərin subyektlərinin razılığı ilə qanuni və ədalətli üsullarla əldə edilməlidir.
- **Məlumatların keyfiyyəti (Data quality)** – Toplanan məlumatlar aktual, dəqiq və tam olmalıdır.
- **Məqsədin spesifikasiyası (Purpose specification)** – Məlumat toplanarkən məqsəd dəqiq müəyyən olunmalı və açıqlanmalıdır.
- **İstifadə məhdudiyyəti (Use limitation)** – Toplanmış məlumatların sonrakı istifadəsi məlumat toplanarkən açıqlanan məqsədlərə uyğun olmalıdır.
- **Təhlükəsizlik tədbirləri (Security safeguards)** – Fərdi məlumatlar səmərəli təhlükəsizlik tədbirləri ilə qorunmalıdır.
- **Açıqlıq (Openness)** – Fərdi məlumatlarla bağlı hadisələr (inkışaflar), təcrübələr və siyasət açıq olmalıdır.

• **Fərdi iştirak (Individual participation)** – Məlumat subyektləri özləri haqqında məlumat almaq hüququna və bu məlumatların düzgünlüyünə etiraz etmək hüququna malikdirlər.

• **Hesabatlılıq (Accountability)** – Təşkilat yuxarıda göstərilən prinsiplərə uyğun olaraq məlumatın subyekti qarşısında məsuliyyət daşıyır.

Verilənlərin qorunması üçün əsas tələblərdən biri fərdi məlumatların emalının qanuna uyğunluğunun təmin edilməsidir.

Big data və verilənlərin müasir analiz metodları ayrı-ayrı fərdlərin şəxsi həyatının məxfiliyinin qorunmasının ənənəvi yollarını təsirsiz hala gətirir [11]. Fərdi şəxslər Big data analitikada məlumatların istifadəsi və açıqlanmasına az nəzarət edirlər [4]. Big data analitika insanların sağlamlıq, siyasi görüşləri və s. ilə bağlı meyllərini qabaqcadan proqnozlaşdırmaq qanunauyğunluqları və tendensiyaları üzə çıxarmağa imkan verir. Qanunla və ya fərdin razılığı ilə icazə verilən fərdi verilənlər konkret bir məqsəddə xidmət edərsə, qorunması şərti ilə emal oluna bilərlər. Lakin Big data-nın tətbiqləri üçün bunu yoxlamaq çətindir. Məqsədin məhdudlaşdırılması prinsipi Big data erası üçün artıq uyğun deyildir [13].

V. BIG DATA MÜHİTİNDƏ MƏQSƏDİN SPESİFİKASIYASI VƏ İSTİFADƏNİN MƏHDUDLAŞDIRILMASI PRİNSİPİ

Məqsədin spesifikasiyası və istifadənin məhdudlaşdırılması verilənlərin qorunmasının hər hansı bir aktında mövcud olan prinsiplərdən biridir. Bu prinsiplər verilənlərin qorunmasının ənənəvi sütunlarıdır. İstehlakçıların verilənlərinin qorunması sahəsində isə "bildiriş və razılıq" adlanan model verilənlərin qanuni emalı üçün ən çox istifadə olunan mexanizmlərdən biridir [6, 8].

Bu prinsip iki addımlı bir yanaşmanı özündə birləşdirir [6]:
a) fərdi məlumatlar müəyyən olunmuş, açıq və qanuni məqsədlər (orijinal məqsədlər) üçün əldə edilməli; və sonra isə
b) orijinal məqsəddə uyğun olmayan başqa bir məqsəd (yeni məqsəd) üçün istifadə edilməməlidir. Beləliklə, toplanan hər hansı bir fərdi məlumat bu prinsipə uyğun olmalıdır.

Big data məqsədin məhdudlaşdırılması prinsipinə problem yaradır və bu prinsip Big data analitikanın inkişafı üçün bir maneədir [4]. Məqsədin spesifikasiyasının məhdudlaşdırılması ilə bağlı qeyd olunan bu vacib məqamlar [6] "bildiriş və razılıq" modelinin effektivliyinə mənfi təsir göstərir. Məsələn, Big data analitika yeni məqsədlər üçün istifadə edilə bilən gözlənilməyən korrelyasiyaları aşkar edən müxtəlif alqoritmlərdən istifadə edərək verilənlərin analizini həyata keçirməyə imkan verir. Buna görə məqsədin məhdudlaşdırma prinsipi təşkilatın imkanlarını və innovasiya fəaliyyətini məhdudlaşdırır.

Aşağıda məqsədin spesifikasiyası və məhdudlaşdırma prinsipi ilə əlaqəli iki əsas məsələ nəzərdən keçirilmişdir.

A. Verilənlərin təkrarlanması (Repurpose Data)

İlk popblem verilənləri yeni məqsədlər üçün istifadə edərkən yaranır. Big data verilənlərin təkrar istifadəsini özündə birləşdirir ki, bu da verilənlərin təkrarlanmasına səbəb olur. Big data analitika fərdi verilənlərin toplanması yolu ilə dəyərli bilikləri aşkarlamaq imkanına malikdir. Bu halda çox böyük verilənlər dəstləri məqsədin məhdudlaşması prinsipinə problem yaradır [6].

Bu prinsipə görə, toplanmış fərdi məlumatları prediktiv analiz üçün istifadə edən təşkilatlar verilənlərin toplanmasının orijinal məqsədi ilə bu analizin uyğunluğunu təmin etməlidirlər [6,12]. İnsanlar məlumatları başqaları ilə paylaşdıqda, onlar bu məlumatların hansı məqsədlərlə istifadə olunacağına dair təbii bir gözləntiyə sahibdirlər.

Bundan əlavə, Big data analitika müxtəlif məqsədlər üçün, bəzi hallarda isə başqa bir təşkilat tərəfindən əldə olunan verilənləri də təkrar istifadə edir. Bu, toplanmış verilənlərin orijinal məqsədə uyğun olmayan məqsədlər üçün istifadə edilməyəcəyinə dair məxfilik prinsipinə ziddir. Məqsədin məhdudlaşdırılması prinsipinə görə fərdi verilənlər müəyyən, açıq və qanuni məqsədlər üçün əldə edilməli və orijinal məqsədə uyğun olan digər məqsədlər üçün sonradan emal edilməməlidir.

B. Big data analitikanın yaratdığı yeni fərdi məlumatlar

İkinci problem, böyük verilənlərin analizi zamanı yaranan yeni fərdi məlumatların məqsədini müəyyənləşdirməyə ehtiyac olduğu ortaya çıxır. Təkrarlanma ilə yanaşı, big data analitika da yeni fərdi məlumatlar yaratmaq potensialına malikdir [6, 8].

Big data analitikanın yaratdığı yeni fərdi məlumatların emalı üçün verilənlərin subyektlərindən razılığın alınması vacibdir. Big data analitika vasitəsilə fərdi məlumatlarda istinad olunan yaş, seçim və həyat tərzini kimi xüsusiyyətlərinə görə fərdlər məhsul və ya xidmət təklifləri ala bilərlər. Sosial media verilənləri və fərdlər haqqında digər məlumatlar isə fərdi şəxsin kredit reytingini təyin edərkən, onun həyat tərzini öyrənmək üçün analiz edilə bilər [6, 13].

NƏTİCƏ

Son texnoloji nailiyyətlər və biznes fəaliyyətinin inkişafı fərdi məlumatların toplanması, saxlanması və istifadəsi imkanlarını artırır. Xüsusilə, Big data dövründə əvvəlkindən daha çox fərdi verilənlər toplanır, analiz olunur və istifadə edilir. Eyni zamanda Big data analitika verilənlərin analizinin ənənəvi formalarını dəyişdirdi və tədqiqatlara yeni prediktiv yanaşma gətirdi. Bundan sonra fərdi məlumatlarla bağlı məxfilik və məlumatların qorunması problemləri daha qabarıq şəkildə ortaya çıxır. Aparılan tədqiqatlar göstərir ki, fərdi verilənlərin qorunması ilə bağlı irəli sürülmüş bəzi prinsiplər Big data erasında özünü doğrultmur. Belə ki, Big data verilənlərin qorunmasının əsasını təşkil edən məqsədin spesifikasiyası və istifadənin məhdudlaşdırılması prinsiplərinə problem yaradır, eyni zamanda bu prinsip Big data analitikanın

inkişafı üçün bir maneədir. Big data analitika toplanmış verilənlərin orijinal məqsədə uyğun olmayan məqsədlər üçün istifadə edir ki, bu da fərdi verilənlərin məxfiliyinə xələl gətirir.

Beləliklə, fərdi məlumatların ənənəvi qorunması prinsiplərinin məhdudiyyətləri yeni metodologiyanın işlənilməsinə tələb edir. Böyük verilənlər üçün profil qanunun hazırlanması bu halda daha məntiqli qərar hesab oluna bilər.

İSTİFADƏLƏR

- [1] Ch. Chi, T. Liu, X. u, Sh. Shi, “Research on the security of personal information in the era of Big Data,” The Inter. Conference on Artificial Intelligence for Communications and Networks, July 2019, pp 107-114 .
- [2] Identity Theft Resource Center (ITRC). Data Breaches., <https://www.idtheftcenter.org/data-breaches>
- [3] The risk based security (RBS) and the open security foundation (OSF). DataLossDB, <https://blog.datalossdb.org>
- [4] S.C. Cha, K.H. Yeh, “Data-driven security risk assessment scheme for personal data protection,” IEEE Access, 2018, vol. 6, pp. 50510-50517.
- [5] Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu, <http://www.e-qanun.az/framework/19675>
- [6] N. A. Ghani, S. Hamid, N.I. Udzir, “Big data and data protection: Issues with purpose limitation principle,” Int J. Advance Soft Computing Applications, 2016, vol. 8, no. 3, pp. 116-121.
- [7] K. Crawford, J. Schultz, “Big data and due process: Toward a framework to redress predictive privacy harms”, Boston College Law Review, 2014, vol 55, pp. 93- 96.
- [8] M. Paterson, M. McDonagh, “Data protection in an era of Big data: The challenges posed by big personal data,” Monash University Law Review, 2018, vol 44, no 1, pp. 1-31.
- [9] M. S. Hajirahimova, “Big data technologies and information security challenges,” Problems of Information Technology, 2016, vol. 13, no. 1, pp. 49-56.
- [10] D. Boyd, K. Crawford, “Critical questions for Big data: Provocations for a cultural, technological, and scholarly phenomenon,” Information, Communication & Society, 2012, vol. 15, pp.667–700.
- [11] D. Zhang, “Big data security and privacy protection,” Advances in Computer Science Research, 2018, vol. 77, pp.275-278.
- [12] L. Zhou, W. Gu, Ch. Huang, Y. Bai, “Research on information security in big data era,” The 6th International Conference on Computer-Aided Design, Manufacturing, Modeling and Simulation, 2018.
- [13] Y. Sun, “Personal information security in the era of Big Data,” Proceedings of the 2nd International Conference on Artificial Intelligence and Engineering Applications, 2017, pp. 619-626.

PERSONAL INFORMATION SECURITY IN BIG DATA ENVIRONMENT

Makrufa Hajirahimova¹, Aybeniz Aliyeva²

^{1,2}Institute of Information Technology of ANAS, Baku, Azerbaijan
¹makrufa@science.az, ²aliyeva.a.s@mail.ru

Abstract – Big data brings convenience to people and brings certain risks. In the process of data collection, storage, and use, it can easily lead to the leakage of personal information and discovery of confidential data which it create the problems for privacy protection of personal data. This paper have been investigated the challenges and causes of data security, some core principles of privacy protection of personal information are considered.

Keywords – Big data; big data analytics; protection of personal information; data security; information security

Elektron kitabxanalarda fərdi məlumatların təhlükəsizliyi məsələləri

Firudin Əsgərov¹, Rəhilə Həsənova²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹firudinasgarov@gmail.com, ²rahasanova@gmail.com

Xülasə— Hazırda kitabxana-informasiya mühitində kitabxanaçıların və oxucuların tələblərinə cavab verən Kitabxana İdarəetmə Sisteminin (KİS) seçilməsi ən vacib məsələlərdən biridir. Məqalədə AMEA İnformasiya Texnologiyaları İnstitutunda tətbiq edilən Alephino KİS haqqında məlumat verilir. Həmçinin kitabxana işinin yüksək səviyyədə təşkili və KİS-lərdə fərdi məlumatların konfidensiallığının qorunması məsələləri analiz edilir.

Açar sözlər— e-kitabxana, KİS, Alephino, fərdi məlumatlar, informasiya təhlükəsizliyi

I. GİRİŞ

XX əsrin sonu və XXI əsrin əvvəllərində internetin yaranması və elmi-texniki inkişaf bəşəriyyətin sənaye cəmiyyəti mərhələsindən informasiya cəmiyyəti mərhələsinə keçidini təmin etdi. Müasir informasiya cəmiyyətinin əsas vəzifəsi yaşından, dilindən, dinindən, irqindən, zaman və məkəndən asılı olmadan bütün insanların informasiya tələbatını ödəmək, onların arasında sosial kommunikasiya mühiti yaratmaq, bilik və düşüncələrini ictimaiyyətə çatdırmaqdır [1].

Virtual məkəndə informasiya bolluğu şəraitində istifadəçi əldə etdiyi üstünlüklərlə bərabər bir sıra problemlərlə də üzləşə bilər. Baxmayaraq ki, bəşəriyyət yaranan gündən informasiya təhlükəsizliyi mövcud olmuşdur, müasir dövrdə texnikanın sürətli inkişafı ilə bu təhlükəsizlik problemlərinin daha da qabarıq şəkildə almasına səbəb olmuşdur. Belə ki, keçən əsrin sonlarına qədər kağız üzərində olan informasiyanın idarə edilməsi, qorunması çox asan idisə, bu gün virtual məkəndə, elektron daşıyıcılarda informasiyanın qorunması çox mürəkkəb məsələlərdəndir [2].

İnformasiya təhlükəsizliyinin problemlərindən biri fərdi məlumatların mühafizəsi ilə bağlı olan məsələlərdir. Fərdi məlumatlar haqqında Azərbaycan Respublikasının qanununa əsasən fərdi məlumatlar toplandığı andan mühafizə olunur və bu məqsədlə daxilolma (əldə olunma) növünə görə konfidensial və açıq kateqoriyalara bölünür. Konfidensial fərdi məlumatlar qanunvericilikdə nəzərdə tutulmuş tələblərə uyğun səviyyədə mülkiyyətçi, operator və bu məlumatlara giriş hüququ olan istifadəçilər tərəfindən mühafizə olunmalıdır. Konfidensial fərdi məlumatlar qanunla müəyyən olunmuş

hallar istisna olmaqla, üçüncü şəxslərə yalnız subyektin razılığı əsasında verilə bilər. Açıq fərdi məlumatlar kateqoriyasına müəyyən olunmuş qaydada adsızlaşdırılmış, subyekt tərəfindən açıq elan olunmuş və ya ümumi istifadə üçün yaradılmış informasiya sisteminə subyektin razılığı ilə onun barəsində daxil edilmiş məlumatlar aiddir. Şəxsin adı, soyadı və atasının adı daimi açıq fərdi məlumatlardır. Açıq kateqoriyalı fərdi məlumatların konfidensiallığının təmin edilməsi tələb olunmur [3].

II. KİS FƏRDİ MƏLUMATLARIN TOPLANDIĞI SİSTEM KİMİ

Fərdi məlumatlar müasir dövrdə vətəndaşlara elektron xidmət göstərən demək olar ki, bütün dövlət və özəl müəssisələrin sistemlərində toplanır. Fərdi məlumatların müxtəlif formada toplandığı sistemlərə elektron tibb sistemlərini, kadrlar sistemini, bank sistemlərini, təhsil ilə bağlı sistemləri və s. nümunə göstərmək olar. Bu kimi sistemlərə həmçinin, elektron kitabxanalarda tətbiq edilən Kitabxana İdarəetmə Sistemləri də daxildir.

Kitabxana konsepsiyası yarandığı vaxtdan bu günə kimi insanların informasiya tələbatının ödənilməsi və informasiyanın gələcək nəsillərə ötürülməsi funksiyasını yerinə yetirir. Hazırda kitabxanalar vətəndaş cəmiyyətinin əsas göstəricisi olan global informasiya mühitinin, beynəlxalq, milli və regional səviyyədə informasiya mübadiləsi sistemlərinin yaradılmasında, informasiyanın əmtəəyə çevrilməsində aparıcı rol oynayır.

Dünya təcrübəsi göstərir ki, kitabxana proseslərinin avtomatlaşdırılması – yüksək ixtisaslı kitabxanaçıların və proqramçıların birgə fəaliyyətinin nəticəsi kimi informasiya kommunikasiya texnologiyalarının (İKT) tətbiqi ilə həyata keçirilən mürəkkəb məsələlərdən biridir. Qeyd edək ki, kitabxana proseslərinin kompleks şəkildə avtomatlaşdırılması Kitabxana İnformasiya Sistemlərinin yaradılmasını nəzərdə tutur. İnformasiyanın sürətlə artdığı və yeniləndiyi bir şəraitdə Kitabxana İnformasiya Sistemlərinin yaradılmasının əsas məqsədlərindən biri İKT-nin imkanlarından istifadə etməklə yerləşdiyi məkəndən və zamandan asılı olmayaraq kitabxanalar və oxucular arasında informasiya mübadiləsinin həyata keçirilməsidir. Həmçinin, buraya oxucuların sorğularına operativ münasibət bildirilməsi də daxildir.

Avtomatlaşdırma prosesini həyata keçirmək üçün ilkin olaraq proqram təminatı seçilməlidir. Proqram təminatının seçimi zamanı İKT bazarında mövcud proqram təminatları analiz olunmalı və onların içərisindən ən optimalı müəyyənəndirilməli və ya uyğun proqram təminatı mövcud olmadıqda yeni proqram təminatı hazırlanmalıdır. Kitabxana proseslərini kompleks şəkildə avtomatlaşdırmaq üçün yaradılmış proqram təminatları bir çox hallarda avtomatlaşdırılmış Kitabxana İnformasiya Sistemləri adlandırılır. Hal-hazırda daha çox inkişaf etmiş ölkələrdə avtomatlaşdırılmış Kitabxana İnformasiya sistemlərini Kitabxana İdarəetmə Sistemləri adlandırırlar [4].

Elektron kitabxana (e-kitabxana) deyərkən oxucunun zaman və məkan anlayışı olmadan istədiyi vaxt kitabxana kataloqundan (elektron kataloq) istifadə etmə imkanının olması başa düşülür. Web OPAC (Online Public Access Catalog) modulu isə oxucuya internet üzərindən kitabxana kataloqundan istifadəyə imkan verir. Ümumiyyətlə, OPAC iki mənada işlənir: onlayn elektron kataloq və KİS-in bibliografik məlumat bazasına müraciəti təmin edən interfeys hissəsi kimi. Məhz bu baxımdan Kitabxana İdarəetmə Sistemlərində Web OPAC modulunun mövcudluğu zəruridir.

Müasir dövrdə dünyada çoxlu sayda müxtəlif ölkələrin istehsalı olan KİS-lər vardır. Bu KİS-lərə ABŞ istehsalı olan Alexandria (1988), Millenium (1990), Mandarin (1995), Virtua (1998), Destiny (2003), Koha (2004), İsrail istehsalı olan Alephino (1986), Rusiya istehsalı olan IRBIS-64 (2000), Kanada istehsalı olan ResourceMate (1993) və s. nümunə göstərmək olar [5].

III. E-KİTABXANALARDA FƏRDİ MƏLUMATLARIN TƏHLÜKƏSİZLİK PROBLEMLƏRİ

E-kitabxanalarda tətbiq edilən Kitabxana İdarəetmə Sistemlərinin layihələndirilməsində, qurulmasında və istismarında ən vacib problemlərdən biri informasiya təhlükəsizliyidir.

Oxucuların e-kitabxana xidmətlərindən tam şəkildə istifadə edə bilməsi üçün ad və soyadlarını, e-poçt ünvanlarını, telefon nömrələrini və identifikasiya edilə bilən digər fərdi məlumatlarını kitabxanaçıya təqdim etməsi lazım gəlir.

Bu informasiya “üçüncü tərəf” dediyimiz hakerlərdən və bu məlumatları kitabxana ilə əlaqəsi olmayan məqsədlər üçün istifadə etmək istəyən şəxslərdən qorunmalıdır.

E-kitabxananın kitabxana oxucularının demoqrafik verilənlərindən başqa, aşağıdakı fərdi məlumatlarına da girişi vardır [6]:

- müddətli əldə etdiyi informasiya resursları (İR);
- məsləhət aldığı nəşrlər haqqında məlumatlar;
- onlayn axtarış məlumatları;
- sifariş etdiyi İR sorğularının siyahıları və s.

E-kitabxanalarda oxucular haqqında geniş həcmli fərdi məlumatlar toplanılır. Bu məlumatlar oxucu və kitabxanaçı

arasında konfidensial hesab olunsa da, kitabxana tərəfindən “üçüncü tərəf”ə (hüquq-mühafizə orqanlarına, kommersiya təşkilatlarına və s.) təqdim edilməsi üçün arxivləşdirilə bilər. Kitabxanalarda fərdi məlumatların konfidensiallığının qorunmasına dəyər verilsə də, bu digər məsələlərlə müqayisədə əhəmiyyətli hesab edilmir [6].

Amerika Kitabxanalar Assosiasiyası 1960-cı illərin əvvəlində Etika Kodeksində fərdi məlumatların təhlükəsizliyi ilə bağlı tələblər nəzərə çatdırılmışdır [7]. Etika Kodeksində bir çox vəzifələr müəyyən edilir. Məsələn, “Hər bir kitabxana istifadəçisinin axtarılmış və ya alınmış informasiya üzrə və məsləhət alınmış, müvəqqəti götürülmüş, əldə edilmiş və ya ötürülmüş resurslar üzrə gizlilik və konfidensiallıq hüquqlarının qorunması belə vəzifələrdəndir”

Amerika Kitabxanalar Assosiasiyasının 2002-ci ildə nəşr etdiyi və 2014-cü ildə isə yenilədiyi “Gizlilik və konfidensiallıq üzrə suallar və cavablar” adlı sənəddə e-kitabxanalarda və KİS-lərdə oxucuların konfidensial məlumatlarının necə işlənməli olduğunu və bununla bağlı təcrübəni nümayiş etdirir [8].

Qeyd etmək lazımdır ki, AMEA İnformasiya Texnologiyaları İnstitutunun elektron kitabxana mərkəzində tətbiq edilən Alephino KİS-də fərdi məlumatların konfidensiallığı nəzərə alınmışdır.

Alephino proqram təminatı 1986-cı ildə İsraildə əsas qoyulan, KİS-lərin hazırlanması və inkişaf etdirilməsi ilə məşğul olan Exlibris şirkəti tərəfindən yaradılmışdır. Bir neçə avropa dillərində fəaliyyət göstərən, sadə interfeysə malik olan bu Kitabxana İdarəetmə Sistemi 90 ölkənin 6000-dən çox kitabxanasında beynəlxalq səviyyədə tətbiq olunur.

Bu KİS-in böyük kitabxanalarda tətbiq olunan universal və uğurlu Aleph sistemi ilə sıx əlaqəsi onun kitabxana dünyasının ən son imkanlarına əyətərliyini təmin edir. Alephino standart XML mübadilə formatı istifadə edən açıq əlaqələr sistemi kimi müxtəlif integrasiya mühitlərinə fərqli adaptasiya versiyalarına məxsusdur. Burada sistemə daxil edilmiş sənədlərin və siyahıların individual qaydada formatlaşdırılması da mümkündür.

Bu kitabxana idarəetmə sistemində də digər qərb ölkələri istehsalı olan KİS-lərdə olduğu kimi oxucuların e-kitabxanadan istifadə tarixçəsini, müxtəlif zamanlarda əldə olunmuş informasiya resurslarının hansı fərqli oxucular tərəfindən əldə olunduğu və s. kimi məlumatları izləmək mümkün deyil. Belə ki, KİS e-kitabxanadan istifadə edən oxucuların fərdi məlumatlarının konfidensiallığını qorumaq məqsədi ilə ayrı-ayrı modullarında bu məlumatlara girişi kitabxanaçının özünə belə mümkünsüz edir. Yəni KİS yaradılarkən oxucuların fərdi məlumatlarının “üçüncü tərəf”ə ötürülməsinin, müxtəlif yollarla ələ keçirilməsinin qarşısını almaq üçün qeyd etdiyimiz funksiyaları proqram təminatına əlavə edilməyib [9].

NƏTİCƏ

Araşdırmalar nəticəsində məlum olmuşdur ki, KİS-lərdə istifadəçiyə nəzərən statistik məlumatların tam dolğun çıxarılması mümkün deyildir. Buna baxmayaraq sistemlərdə

hər hansı informasiya resursuna (kitab, jurnal və s.) aid bütün statistik məlumatları (məsələn, bu resursu ay ərzində neçə dəfə müraciət olunub və s.) əldə etmək mümkündür. Lakin hər hansı bir resursu istifadə etmiş oxucuların tam siyahısına baxdıqda sistem yalnız həmin resursu istifadə edən ən son oxucunun adını görməyə imkan verir. Ümumiyyətlə, ABŞ və qərb ölkələrində oxucunun kitabxanadan istifadə tarixçəsinin izlənilməsi fərdi məlumatlara müdaxilə kimi qiymətləndirilir və təhlükəsizlik baxımından bu prosesi çətinləşdirilir. Bu ilk növbədə oxucunun fərdi məlumatlarının “üçüncü tərəf”ə ötürülməsinin qarşısını almaq üçündür. Lakin fəvqəladə hallarda KİS-dən oxucu haqqında fərdi məlumatlar əldə edilə bilər. Bu yalnız server administratoru tərəfindən loq faylları təhlil etməklə mümkündür. Qeyd etmək lazımdır ki, bu imkan hər KİS-də mövcud olmağa bilər.

Hər bir müəssisə və ya təşkilat mövcud beynəlxalq Kitabxana İdarəetmə Sistemləri içərisindən öz kitabxanasının fəaliyyət sahəsinə uyğun olanını seçib tətbiq etməlidir. Bu mümkün olmadıqda isə təşkilatın fəaliyyətinə xas kitabxana proseslərini nəzərə almaqla yeni KİS yaradılmalıdır. Lakin bu proqram təminatı hazırlanarkən informasiya təhlükəsizliyi məsələlərinə ciddi yanaşılmalı və fərdi məlumatların konfidensiallığı mütləq şəkildə qorunmalıdır.

İSTİNADLAR

- [1] R. M. Əliquliyev, R. Ş. Mahmudov, “İnternet cəmiyyətin inkişafının həərəkətverici qüvvəsi kimi,” *İnformasiya cəmiyyəti problemləri*, 2016, №1, səh. 35-45.
- [2] R. M. Əliquliyev, Y. N. İmamverdiyev, R. Ş. Mahmudov, “İnformasiya təhlükəsizliyinin multidissiplinar elmi-nəzəri problemləri,” *İnformasiya cəmiyyəti problemləri*, 2017, №2, səh. 32-43.

- [3] Fərdi məlumatlar haqqında Azərbaycan Respublikasının qanunu. <http://www.e-qanun.az/framework/19675>.
- [4] F. Əsgərov, “E-kitabxanalarda tətbiq olunan proqram vasitələrinin analizi: üstünlükləri və çatışmazlıqları,” *Proqram mühəndisliyinin aktual elmi-praktiki problemləri I respublika konfransının materialları*, səh. 213-214, Bakı, 17 may 2017-ci il.
- [5] www.capterra.com/library-automation-software/
- [6] Y.N. İmamverdiyev “IDEA4SP: E-kitabxanalar üçün informasiya təhlükəsizliyi modeli,” *İnformasiya cəmiyyəti problemləri*, 2017, №2, səh. 74-83.
- [7] American Library Association Code of Ethics, <http://www.ala.org/advocacy/proethics/codeofethics/codeethics>
- [8] Questions and Answers on Privacy and Confidentiality, <http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/qa-privacy>
- [9] Alephino v4.0. <http://www.ex-lh.hu/site/index.php/en/alephino-4-eng>

SECURITY ISSUES OF PERSONAL INFORMATION IN ELECTRONIC LIBRARIES

Firudin Asgarov¹, Rahila Hasanova²

^{1,2}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹firudinasgarov@gmail.com, ²rahasanova@gmail.com

Abstract – Today selection of a Library Management System (LMS), that meets the needs of librarians and readers is one of the most important issues in the library and information environment. The article provides information on Alephino LMS applied in the Institute of Information Technology of ANAS. It is also analyzed organization of library work in high level and protection of the confidentiality of personal information in the LMS.

Keywords – *e-library, LMS, Alephino, personal information, information security*

Mobil avadanlıqlarda fərdi məlumatların təhlükəsizliyi məsələləri

Oqtay Ələkbərov

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

oqtayalakbarov@iit.science.az

Xülasə— Son dövrlərdə mobil istifadəçilər mobil avadanlıqlardan bank ödəmələri, internet xidmətləri, e-poçt xidmətləri, çoxsaylı proqram əlavələri, video, foto və audio məlumatların saxlanması və s. kimi istiqamətlərdə geniş istifadə edilir. Qeyd edilən xidmətlərdən istifadə vaxtı mobil qurğular haker hücumlarına məruz qalır. Məqalədə mobil qurğularda yerləşən fərdi məlumatların təhlükəsizliyi və təhdidlərin təsnifatı təhlil edilmiş və meydana çıxan problemlər analiz edilmişdir. Fərdi məlumatların təhlükəsizliyinin təmin olunması üçün tövsiyələr təklif edilmişdir.

Açar sözlər— mobil qurğular, təhdidlər, biometrik təhlükəsizlik, məxfilik, gizlilik

I. GİRİŞ

Son dövrlərdə texnologiyanın inkişafı mobil qurğulara olan tələbatı da artırmışdır. İstifadəçilərin gündəlik həyatda mobil qurğulardan (smartfonlar, planşetlər) istifadəsi onların təhlükəsizliyi məsələlərini gündəmə gətirir. Əksər ekspertlər mobil qurğularda saxlanan məlumatların xakerlər tərəfindən daha asan əldə edilməsini qeyd edirlər. Hal hazırda mobil avadanlıqlardan bank ödəmələri, internet, e-poçt xidmətləri, çoxsaylı proqram əlavələri, video, foto və audio məlumatların saxlanması və s. kimi istiqamətlərdə geniş istifadə edilir. İstifadəçi mobil avadanlıqlardan istifadə etdikdə bir çox riskləri nəzərə almalırlar. Araşdırmalar göstərir ki, əksər istifadəçilər mobil qurğulardan istifadə zamanı təhlükəsizlik siyasətinə əməl etmirlər. Amerika Birləşmiş Ştatlarında 1000-ə yaxın istifadəçi arasında aparılmış sorğu nəticəsində məlum olmuşdur ki, istifadəçilərin sadəcə 12%-i mobil qurğuların təhlükəsizlik siyasətinə əməl edirlər. Mobil telefonlarda müxtəlif proqram əlavələrinin olması, mobil telefonların daima internet şəbəkəsində onlayn olması onların təhlükəsizlik məsələlərini daima aktual edir.

II. MOBİL QURĞULARDA FƏRDİ MƏLUMATLARA TƏHDİDLƏRİNİN TƏSNİFATI

Mobil telefonların təhlükəsizliyinin əsas funksiyası mobil telefonlarda saxlanan şəxsi və işgüzar məlumatların etibarlılığını təmin etməkdir. Mobil qurğulardan geniş istifadə olunması onlarda saxlanan məlumatlara hakerlər tərəfindən hücum edilməsinə səbəb olur. Haker hücumları əsasən sms mətnlərinin ötürülməsi, multimedia məlumatlarının mübadiləsi və əlaqə kanallarından istifadə zamanı baş verir. Mobil

avadanlıqların təhlükəsizliyinə təsir edən təhdidlər aşağıdakılardır [1].

Fiziki təhdidlər- Mobil qurğuların balaca və yüngül olması onların oğurlanması və ya itirilməsi ehtimalını artırır. Juniper şirkətinin keçirdiyi sorğuya əsasən hər 20 mobil telefon istifadəçisindən 1-i mobil qurğunun itirilməsi və ya oğurlanması halları ilə rastlaşır. İstifadəçi mobil telefonun itirərsə və onu PİN kod və ya parol vasitəsi ilə bloklaşdırarsa, mobil telefonu əldə edən digər istifadəçi aşağıdakı məlumatları əldə etməsinə imkan yaradır [2].

- Elektron poçtda yerləşən məlumatlara;
- Sosial şəbəkələrdəki (Facebook, Google, Twitter) qeydiyyat məlumatlarını;
- Brauzerlərdə saxlanan parollara;
- Parol və kredit kartı haqqında məlumat;
- Elektron poçtun ünvanı və əlaqədə olduğu şəxslərin telefon nömrələri;
- Video, audio və fotosəkillər haqqında məlumat.

Şəbəkə təhdidləri. Bildiyimiz kimi mobil qurğular müxtəlif növ naqilsiz şəbəkə texnologiyaları (wi-fi, bluetooth, nfc) ilə təchiz olunmuşdur. Hakerlər tərəfindən hücumlar ilkin olaraq məhz şəbəkə texnologiyalarına olunur. Bu hücumlar zamanı əsasən SMS, MMS və səsli zəng xidmətlərindən istifadə edilir. Hakerlər adətən şəbəkə təhdidləri zamanı Smishing və Vishing hücumlarından istifadə edirlər. Smishing hücum SMS xidmətləri, Vishing hücumu isə səsli zəng xidmətləri vasitəsi ilə həyata keçirilir [3].

Sistem təhdidləri. İstifadə olunan əməliyyat sistemlərində istehsalçı tərəfindən buraxılmış boşluqlara görə mobil avadanlıqlarda çox ciddi təhlükəsizlik problemləri baş verə bilər. Məsələn, 2015-ci ildə Samsung şirkətinin istehsal etdiyi bəzi qurğularda istifadə olunur. SwiftKey-də aşkarlanan boşluq, istifadəçinin yazışmalarının digər şəxslər tərəfindən rahatlıqla əldə olunmasına şərait yaratmışdır.

Proqram əlavələri təhdidləri. Mobil telefonlarda müxtəlif növ proqram əlavələrindən istifadə olunur. İstifadəçi istənilən proqramı mobil telefona yükləyərkən təhlükəsizlik siyasətinə ciddi qaydada əməl etməlidir. Təcrübələr göstərir ki,

kibercinayətkarlar sosial mühəndisliyin müxtəlif növlərindən istifadə etməklə, istifadəçinin məlumatlarını asanlıqla ələ keçirə bilirlər. Proqram əlavələri təhdidləri, əsasən, aşağıdakı kateqoriyalardan ibarət olur:

- casus proqramları;
- zərərli proqramlar;
- məxfiliyi təhdid edən proqramlar;
- proqram boşluqları.

Mobil telefonların proqramlarında boşluqların olması demək olar ki, mobil telefonların müxtəlif hücumlara qarşı zəif olmasına səbəb olur. Adətən bu cür boşluqlar zamanı hakerlər müxtəlif zərərli virus və ya proqram təminatlarından istifadə edirlər. Bunlara aşağıdakı hücum növlərini misal göstərə bilərik:

Troyan atı ilə hücumlar zamanı, adətən, istifadəçinin şəxsi məlumatları oğurlanmaqla yanaşı, müxtəlif zərərli proqram təminatları mobil qurğuya yüklənə bilər

Botnet hücumları zamanı mobil avadanlığın hesablama resurslarından istifadə olunur. Çox vaxt istifadəçinin belə hücumlardan xəbəri olmur.

Soxulcan hücumları zamanı virus sistemdə yaranan boşluqlardan istifadə etməklə daha çox zərər yetirmək qabiliyyətində olur. Mobil avadanlıqlarda belə tip viruslar əsasən istifadəçinin maliyyə məlumatlarını oğurlanması üçün istifadə olunur

Rootkit zərərli proqram təminatı olub, istifadəçinin xəbəri olmadan onun mobil telefonuna daxil olur. Bu tip zərərli proqram əlavələri mobil qurğunun əməliyyat sisteminin əsas funksiyalarını özünə lazımını formada idarə edir.

Mobil telefonlara olunan təhdidlərin sayının artmasının başqa bir səbəbi mobil ödəniş sistemlərinin geniş sferada istifadə olunmasıdır. Belə ki, istifadəçilərin gündəlik həyatında ödənişlərin çox bir hissəsini mobil telefonlar vasitəsi ilə həyata keçirirlər. Belə təhdidlər zamanı, adətən istifadəçilər sadə üsullarla aldadılırlar. McAfee Lab şirkətinin araşdırmaları göstərir ki, müxtəlif saxta URL ünvanlardan istifadə etməklə istifadəçilər zərərli veb saytlara yönləndirillər. İstifadəçiyə hədiyyə vaucərlər, məşhur brendlərə endirimlər və ya müxtəlif xidmətlər göstərən hər hansı bir saytın xidmətlərinə böyük endirimlər təklif etməklə istifadəçini zərərli saytlara keçid etməyə yönləndirirlər. Statistika görə hər 100 müraciətin 51-i məhz zərərli saytlara yönləndirilir.

III. MOBİL AVADANLIQLARDA FƏRDİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİNİN TƏMİN OLUNMASI YOLLARI

Mobil telefonlarda fərdi məlumatların təhlükəsizliyinin təmin olunmasında 2 cür yanaşma mövcuddur. 1-ci yanaşmada mobil telefonların fərdi məlumatlarının təhlükəsizliyini istifadəçi özü təmin edərsə, 2-ci yanaşmada bu proses mobil avadanlıq istehsalçısının birbaşa özündən asılı olur. Mobil

telefon istifadəçisinin fərdi məlumatları qorumaq üçün bir neçə təhlükəsizlik tələblərinə riayət etməlidir. [4]

Şifrələmə. Əgər mobil telefonda xüsusi məlumatlar olarsa, bu mütləq şəkildə şifrələnməlidir. Fərdi məlumatların şifrələnməsi onları kənar şəxslərin müdaxiləsindən qoruyur. Eyni zamanda şifrələnmiş fayllar məxfilik siyasətinin tam qorunmasına kömək edir.

Standartlaşdırma və ya Sertifikatlaşdırma - bu proses mobil telefonun təhlükəsizlik faktorlarını təmin edir. Belə ki, standartlara cavab verən mobil telefonlar istifadəçinin fərdi məlumatlarının təhlükəsizliyi üçün kilid sistemləri, antivirus proqramları və ehtiyat nüsxə yaddaşı ilə təmin olunur

Şəbəkəyə giriş idarəetməsi- (ing. Network Access Control) - Bu xidmətin olması şəbəkəyə qoşulan bütün qurğuların qeydiyyatını təmin edir. Belə ki, şəbəkədə olan mobil telefonlardan hər hansı birində virus aşkarlanarsa həmin qurğunun şəbəkəyə girişi blok olunur. Çünki istənilən hücumun uğurlu alınması üçün əsas faktor virusa yoluxmuş və ya zərərli proqram yüklənmiş mobil telefonun internet şəbəkəsində uzun müddət qalmasıdır.

Yuxarıda qeyd etdiyimiz kimi mobil telefonlarda fərdi məlumatların təhlükəsizliyini istifadəçilərlə yanaşı mobil avadanlıqların istehsalçıları da təmin edir. Fərdi məlumatları qorumaq üçün istehsalçı şirkətlər bir sıra təhlükəsizlik siyasətlərinə əməl etməlidirlər. [6]

Proqram əlavələri bazası. Adətən, belə bazalarda sertifikatlaşdırılmış proqram tətbiqləri yerləşdirilir. İstehsalçı tərəfindən daima belə bazalara ciddi nəzarət olur. Hər hansı proqram əlavələrində virus və ya boşluq aşkarlanarsa həmin tətbiq dərhal bazadan çıxarılır. Hal hazırda bu tip proqram bazaları olan Play Store, Apple Store, Galaxy Store geniş istifadə olunur. İstehsalçı şirkətlər demək olar ki, hər gün təhlükəsizlik siyasətində yeniləmə aparmaqla belə bazalarda yaranan biləcək problemlərin qarşısını alırlar.

Əməliyyat sistemləri İstehsalçı şirkətlər ilk növbədə mobil telefonların əməliyyat sistemində təhlükəsizlik məsələlərinə daha çox diqqət yetirirlər. Belə ki əməliyyat sistemləri proqramçılar tərəfindən yazılarkən bütün fərdi məlumatların təhlükəsizliyini qorumaq üçün mümkün standartların hamısından istifadə edirlər. Eyni zamanda mobil telefon istehsalçıları hər ay mobil qurğularda təhlükəsizlik siyasətinin yenilənməsi ilə bağlı istifadəçilərə bildirişlər göndərirlər.

Proqram təminatçıları İstehsalçı şirkətlər mobil telefondan istifadəni daha da asan etmək üçün bir sıra mobil qurğulara əlavə proqram təminatları yükləyirlər. Bu proqram əlavələri proqramçılar tərəfindən yazılarkən istehsalçı tərəfindən müəyyən təhlükəsizlik şərtləri qoyulur. Belə ki, yazılmış proqram təminatında fərdi məlumatların gizlilik şərtlərini qorumaq üçün məhz proqram təminatçısına məhdudiyyətlər qoyulur.

Biometrik təhlükəsizlik Son dövrlərdə texnologiyanın daha da inkişafı artıq mobil telefonlarda da biometrik təhlükəsizlik texnologiyalarından istifadə üçün zərurət yaratmışdır.

Biometrik təhlükəsizlik mobil qurğularda adətən 2 mərhələdən ibarət olur: qeydiyyat və autentifikasiya mərhələləri.

Qeydiyyat mərhələsində istifadəçinin fizioloji informasiyaları götürülür. Bura biz barmaqların skan olunmasını, üz cizgilərinin oxunması, göz bəbəyinin oxunması və s. texnologiyaları aid edə bilərik.

Autentifikasiya zamanı isə klaviaturada hər hansı simvolun yığılması, imza və ya istifadəçinin səsindən istifadə olunur. [5]

Yuxarıda qeyd olunan faktorlar bizə əsas verir ki, mobil qurğularda istifadəçilərin fərdi məlumatlarının təhlükəsizliyini qorumaq üçün bəzi şərtlərə əməl edək [7]:

- Məlumatları yükləyərkən mütləq antivirus proqramlarından istifadə etmək;
- Proqram əlavələrini yoxlanılmış bazalardan yükləmək;
- Rəsmi olmayan, pulsuz təklif olunan proqram əlavələrindən istifadə etməmək;
- Məlumat mübadiləsi zamanı gecikmələri diqqətdə saxlamaq;
- Əməliyyat sistemində tez tez yeniləmə aparmaq;
- Biometrik məlumatları məxfi saxlamaq.

NƏTİCƏ

Son dövrlərdə texnologiyaların inkişafı mobil avadanlıqlarda təsirsiz ötürməmişdir. Məqalədə mobil telefonlarda yerləşən fərdi məlumatların təhlükəsizliyinə təhdid yaradan məsələlər və onların həlli yolları analiz və təhlil edilmişdir. Mobil qurğularda fərdi məlumatlara təhdidlərin təsnifatı təhlil edilmişdir. Eyni zamanda mobil avadanlıqlarda fərdi məlumatların təhlükəsizliyinin təmin edilməsi və həlli yolları təklif edilmişdir. Mobil avadanlıqların sürətli inkişafı ilə yanaşı zərərli proqramların sayının artması, hər proqram əlavələrinə görə fərqli təhdidlərin olması onların təhlükəsizlik məsələlərini diqqət mərkəzində saxlayır. Apardığımız araşdırmalar onu göstərir ki, istifadəçilər mobil telefonlarda təhlükəsizlik siyasətini mütəmadi olaraq yeniləməli, mobil telefonlarını kənar şəxslərə etibar etməməlidirlər.

İSTİNADLAR

- [1] M. Sujitra, G. Padmavathi, “A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism”, *International Journal of Computer Applications*, New-york, vol. 56, No. 14 pp. 27-29, October, 2019.
- [2] I.Mavridis, G. Pangalos, “Security Issues in a Mobile Computing Paradigm”, *Communication and Multimedia Security*, Athens, vol 3, pp. 61-75, 2012.
- [3] R. Prodanovic and D. Simic, “A Survey of Wireless Security,” *Journal of Computing and Information Technology*, vol. 15, no. 3, p. 237, Sep. 2007.
- [4] S. Toyssy, M. Helenius, “About malicious software in smartphones”, *Journal in Computer Virology*, vol. 2, no. 2, pp. 109–119, 2006.
- [5] D. Liu, N. Zhang, and K. Hu, “A Survey on Smartphone Security”, *International Journal of Advanced Computer Science and Applications*, vol. 7, pp. 61–65, August. 2013.
- [6] D. Venugopal, G. Hu, and N. Roman, “Intelligent virus detection on mobile devices”, *Proceedings of the International Conference on Privacy, Security and Trust*. New York, pp. 1–4, 2006.
- [7] G. Delac, M. Silic, and J. Krolo, “Emerging security threats for mobile platforms”, in *MIPRO, Proceedings of the 34th International Convention*. IEEE, pp. 1468–1473. 2011

PERSONAL DATA SECURITY ON MOBILE DEVICES

Ogtay Alakbarov

Institute of Information Technology of ANAS, Baku, Azerbaijan

oqtayalakbarov@iit.science.az

Abstract— Recently, mobile users have been widely using mobile devices for banking, internet services, email services, numerous applications, storage of video, photo and audio information and for other operations. Mobile devices are exposed to hacker attacks when using these services. This paper analyzes the security of personal data stored on mobile devices and the classification of threats and analyzes emerging problems. The recommendations on personal data security are provided.

Keywords— *mobile devices, threats, biometric security, privacy, confidentiality*

Fərdi məlumat subyektlərinin hüquqlarının təhlili

Günəl Vəliyeva

Bakı Dövlət Universiteti, Bakı, Azərbaycan
gnl030507@gmail.com

Xülasə— Şəxsə məxsus, onu müəyyənləşdirməyə imkan verən məlumatların qorunması həm fərdi məlumatların mühafizəsi, həm də şəxsi və ailə həyatına hörmət hüququnun bir hissəsidir. Fərdi məlumat subyektləri üçün qanunvericiliklə təminat verilməli hüquqlar onların fərdi məlumatlarının toplanması, emalı və istifadəsi prosesində məlumatların mühafizəsinə təsir imkanlarını gücləndirir. İnternet mühitində fərqli sahələrdə müxtəlif platformalarda məlumatların yığılması və paylanması, üçüncü tərəflər üçün əlçatanlığı şəxslərin öz hüquqlarını həyata keçirməsi üçün fərdi məlumat subyektlərinin aktiv iştirakını və prosesə nəzarətini tələb edir. Bu da fərdi məlumat subyektləri üçün fərdi məlumatların mühafizəsi və şəxsi və ailə həyatına hörmət hüququ ilə bağlı qanunvericilikdə nəzərdə tutulmuş təminatların effektivliyindən asılıdır. Fərdi məlumat subyektlərinin qanunvericilikdə nəzərdə tutulan hüquqları özündə həm fərdi məlumatların mühafizəsi, həm də insan hüquqları çərçivəsində şəxsi və ailə həyatı hüququ ilə bağlı təminatları əks etdirərək bütövlükdə qiymətləndirilə bilər.

Açar sözlər— fərdi məlumat, fərdi məlumat subyektləri, fərdi məlumat subyektlərinin hüquqları

I. GİRİŞ

İnsan hüquqları ilə bağlı aktual məsələlərdən biri fərdi məlumatların hüquqi müdafiəsinin təmin edilməsidir. Problem onunla əlaqədardır ki, informasiya emalının müəyyən avtomatlaşdırılmış platformalarda və ya İnternet məkanında həyata keçirilməsi və istifadəçilərin İnternetdən istifadəsi ilə əlaqədar şəxsi müəyyənləşdirməyə imkan verən fərdi məlumatlar müxtəlif formalarda kənara çıxır və ya üçüncü şəxslər üçün əlçatan ola bilər. Bu halda fərdi məlumatların aid olduğu şəxs tərəfindən ona nəzarət edilməsi mürəkkəbləşir və ya mümkün olmur.

Məlumat toplayan, emal edən və istifadə edənlərə qarşı qanunvericiliyin tələblərindən başqa, fərdi məlumatların mühafizəsində fərdi məlumat subyektlərinin hüquqlarının müəyyən edilməsi, qanunvericiliklə onlara verilən təminatların effektivliyi həlledici amil kimi çıxış edir. Buna görə də, konkret mübahisəli halları həll edərkən hüquq tətbiq edən tərəfindən fərdi məlumatların mühafizəsi və ona qarşı duran qanuni maraqlar arasında əlaqə qiymətləndirilməli və qanunvericiliklə gözlənilən ümumi maraqlar aydınlaşdırılmalıdır.

II. “FƏRDİ MƏLUMATLAR” ANLAYIŞI

“Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanununa [1] əsasən fərdi məlumatlar dedikdə “şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumat” başa düşülür.

Fərdi məlumatlara şəxslərə verilən eyniləşdirmə nömrələri, e-poçt, şəxsin tanınmasına şərait yaradan onun fiziki, əqli, psixoloji, iqtisadi, sosial və mədəni xüsusiyyətlərini aydınlaşdırıcı məlumatlar aiddir. “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanununun 2-ci maddəsinə əsasən “xüsusi kateqoriyalı fərdi məlumatlar” anlayışı “fiziki şəxsin irqi və ya milli mənsubiyyətinə, ailə həyatına, dini etiqadına və əqidəsinə, səhhətinə və ya məhkumluğuna aid olan məlumatlar”dır. Müqayisə üçün Avropa Birliyinin Məlumatların Mühafizəsi haqqında Direktivinə (EU Data Protection Directive (Regulation (EU) 2016/679)) əsasən fərdi məlumat eyniləşdirilən və ya eyniləşdirilə bilən canlı şəxslə bağlı istənilən məlumatdır. Burada fərdi məlumatların əhatə dairəsi açıq buraxılır, istənilən məlumat şəxsin kimliyini müəyyənləşdirməyə imkan verirsə, fərdi məlumat hesab olunur.

Qeyd edilməlidir ki, fərdi məlumatların hüquqi mühafizəsinin vacibliyi təhsil, səhiyyə, sosial, əmək və ayrı-ayrı sahələr üzrə fərdin özünü realizəsi və hüquqlarının həyata keçirilməsi prosesində mərkəzləşdirilmiş və ya mərkəzləşdirilməmiş məlumat bazalarına daxil edilən fərdi məlumatlar üzrə avtomatlaşdırılmış proseslərlə əlaqədar və bu məlumatların üçüncü tərəflər üçün açıqlığına görə tələb olunur.

Eyni zamanda fərdi məlumatların mühafizəsinin onlayn ticarət və istehlakçı hüquqları ilə əlaqəsi İnternet mühitində ticarət platformalarının inkişafı ilə bağlı olaraq genişlənməkdədir. Bu mənada həmin platformalarda tələb olunan və istifadəçilər tərəfindən təqdim edilən fərdi məlumatların dairəsi və həmin məlumatların qorunması və düzgünlüyünün təmin edilməsi üçün nəzarətin səmərəliliyi şəxslərin istehlakçı kimi hüquqlarının qorunması ilə bərabər onların şəxsi hüquq və azadlıqlarının da qorunmasını şərtləndirir. Bank, ticarət, maliyyə, sığorta və digər xidmətlər göstərən şirkətlərə təqdim edilən fərdi məlumatların mühafizəsi həm bu məlumatları toplayanlar üçün, həm də istifadəçilər üçün vacib amildir. Belə ki, bu məlumatların hər hansı formada kənara sızdırılması subyektlər üçün nüfuzun aşağı düşməsi, həmçinin məlumatların aid olduğu şəxslərin hüquqlarının pozulması ilə nəticələnə bilər. Ona görə də, hər iki tərəf fərdi məlumatların mühafizəsində maraqlıdır.

Fərdi məlumatlar anlayışı əsas insan hüquq və azadlıqları çərçivəsində şəxsilik (privacy) hüququ ilə sıx əlaqədardır. Şəxsilik hüququ geniş mənada şəxsin həyatına hər hansı müdaxilənin olmasını istisna edərək şəxsi və ailə həyatına hörmət hüququnun elementidir. “Fərdi məlumatların hüquqi mühafizəsi” anlayışının əsasında insan hüquqları sistemində şəxsin fundamental hüquqlarından biri “şəxsi və ailə həyatına hörmət hüququ” hüququ dayanır. “Şəxsi və ailə həyatına hörmət hüququ” İnsan hüquqları və əsas azadlıqları haqqında

Avropa Konvensiyasının [2] 8-ci maddəsində nəzərdə tutulmuşdur. Konvensiyanın 8-ci maddəsi üzrə Avropa İnsan Hüquqları Məhkəməsinin təcrübəsində də qeyd edilir ki, fərdi məlumatların mühafizəsi fərdin şəxsi və ailə həyatına hörmət hüququndan istifadə etməsi üçün fundamental əhəmiyyətə malikdir [7, s.11]. “Şəxsi və ailə həyatına hörmət hüququ” və “fərdi məlumatların qorunması hüququ” arasında müəyyən məzmun fərqi qəbul olunduqları sahələrlə əlaqədardır. Belə ki, şəxs barədə bütün növ məlumatlar fərdi məlumatlara aid edilir. Lakin bütün məlumatlar şəxsi və ailə həyatına hörmət hüququnun əhatə dairəsinə daxil deyil. Buna görə də, fərdi məlumatların qorunması həm şəxsin əsas insan hüquq və azadlıqlarının təmin olunmasında, həmçinin bununla əlaqəli digər subyektlərin hüquqlarının qorunmasında əhəmiyyətli rol oynayır.

Beləliklə, fərdi məlumatlar ümumi olaraq iki istiqamətdə qiymətləndirilə bilər. Birinci mövqə fərdi məlumatlara şəxsi və ailə həyatına hörmət hüququnun tərkibində şəxsilik hüququ (right to privacy) istiqamətində yanaşmanı ifadə edir. İkinci mövqə isə müxtəlif platformalarda yayılma dairəsindən asılı olaraq fərdi məlumatlara fərdi məlumatların mühafizəsi (right to the protection of personal data) istiqamətində yanaşmanı ifadə edir. Hər iki mövqeni ümumiləşdirərək qeyd etmək lazımdır ki, fərdi məlumatların müdafiəsi fundamental insan hüquqlarından biridir.

III. FƏRDİ MƏLUMAT SUBYEKTLƏRİNİN HÜQUQLARI

“Fərdi məlumatlar haqqında” Azərbaycan Respublikası Qanununun 2.1.2-ci maddəsinə əsasən “barəsində fərdi məlumatlar toplanılan, işlənən və mühafizə edilən, kimliyi müəyyənləşdirilmiş və ya müəyyənləşdirilən fiziki şəxs” fərdi məlumatların subyektləridir. Qanunun 7-ci maddəsi fərdi məlumat subyektinin hüquqlarını müəyyənləşdirir. Fərdi məlumat subyektlərinin hüquqlarını müəyyən kriteriyalar əsasında qruplaşdırmaq olar. Subyektlərin 7-ci maddə əsasında hüquqlarını ümumiləşdirərək aşağıdakı ümumi qruplara bölmək olar:

- Şəxsin özü ilə bağlı fərdi məlumatlara çatımlılıq hüququ;
- Şəxsin özü haqqında toplanmış məlumatların toplanılması, işlənilməsi və üçüncü şəxslərə ötürülməsi prosesində iştirak hüququ;
- Şəxsin özü barədə toplanılmış və ya işlənmiş məlumatların silinməsi hüququ;
- Fərdi məlumatların mühafizəsinin təmin edilməsi hüququ.

Fərdi məlumatların mühafizəsinin təmin olunması həmin məlumatların toplandığı informasiya sistemlərinə qarşı bir sıra hüquqi tələblərin olması və onların yerinə yetirilməsini tələb edir. Məsələn, müvafiq uyğunluq sertifikatının mövcudluğu və ekspertiza barədə informasiya sistemlərinə tələblər subyektlərin hüquqlarının təmin olunmasına yönəlmişdir.

Fərdi məlumatların toplanılması, işlənilməsi və mühafizəsi prosesində həmin məlumatların qorunmasının insanın əsas hüququ kimi qiymətləndirilərək şəxsi və ailə həyatına hörmət hüququ ilə əlaqəli nəzərdən keçirilməsi vacibdir. Lakin fərdi məlumatların mühafizəsi yalnız bunu ehtiva etmir. İctimai maraq olan elə məsələlər ola bilər ki, fərdi məlumatların mühafizəsindən daha əhəmiyyətli ola bilər. Bununla belə, fərdi məlumatın xüsusiyyəti, xüsusi kateqoriyalı olub-olmaması da

hüquqi əhəmiyyətlidir. Hər bir halda qanunvericilikdə nəzərdə tutulmuş maraqlar balanslaşdırılmalıdır. Bu mövqenin təcrübədə təmin edilməsi üçün hüquq tətbiqetmədə konkret işə baxılarkən sahələrarası (hüquq sahələri) əlaqədə qanuni maraqlar müəyyənləşdirilməlidir. Bu mənada fərdi məlumatların mühafizəsi fundamental hüquq olsa da, mütləq hüquq kimi çıxış etmir. Belə ki, fərdi məlumatların müdafiəsi hüququ bu və ya digər dərəcədə şəxsi və ailə həyatı hüququ, fikir, vicdan və din azadlıqları, məlumat və ifadə azadlıqları, ədalətli məhkəmə araşdırması hüququ və digər sosial və mədəni hüquqlarla kompleks təşkil edir.

Nümunə üçün Avropa Ədalət Məhkəməsinin təcrübəsində baxılmış Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen [5] işində ərizəçilər özləri barədə fərdi məlumatların Kənd təsərrüfatı və Qida üzrə Almaniya Federal İdarəsinin veb saytında yerləşdirilməsindən şikayət etmişdi. Onlar barədə məlumatlar saytda Avropa Kənd Təsərrüfatı Təminatı Fondu və Kənd yerlərinin İnkişafı üçün Avropa Kənd Təsərrüfatı Fondunun benefisiarları olduqları üçün benefisiarlar barədə məlumatlar (benefisiarların adları və onlara verilmiş məbləğ) kimi yerləşdirilmişdi. Məhkəmə fərdi məlumatların qorunması və şəffaflıq öhdəliklərini qarşılaşdıraraq saytın üçüncü şəxslərə açıq olduğu üçün əlçatan olması ilə əlaqədar fərdi məlumatların qorunmasına müdaxilə olduğunu, lakin bu müdaxilənin (müdaxilənin qanunvericilikdə müəyyənləşməsi, hüquqlara hörmət, şəffaflıq və proporsionallıq şərtləri əsasında) ümumi maraq prinsipinin məqsədlərinə uyğunluğunu müəyyənləşdirmişdi [7].

Qeyd edilənlər əsasında demək olar ki, fərdi məlumatların mühafizəsi qanunvericiliyinin konkret məsələlərdə mövqeyinin dəqiqləşdirilməsinə ehtiyac vardır. Müqayisə üçün Avropa Birliyinin Məlumatların Mühafizəsi haqqında Direktivində (EU Data Protection Directive (Regulation (EU) 2016/679, Maddə 12-23) məlumat subyektinin hüquqları müəyyən qruplara ayrılaraq (şəffaflıq və modallıq, informasiya və şəxsi məlumatlara çatımlılıq, düzəliş və silinmə, etiraz etmək hüququ və avtomatlaşdırılmış individual qərar qəbul etmə, və məhdudiyyətlər) bir sıra konkret hüquqi məsələləri tənzimləyir və aydın mövqə müəyyənləşdirir. Məsələn, məlumatlara çatımlılıqla bağlı hüquqlar, informasiyanın toplanması, emalı prosesində şəffaflıq və subyektlər üçün aydınlıq, unudulmaq hüququ, özü ilə bağlı məlumatların silinməsi hüququ, etiraz etmək hüququ, subyektin özündən birbaşa və ya digər şəxsdən məlumatlar toplanılarkən fərdi məlumat subyektlərinə verilməli olan məlumatlar və s. kimi həmin qruplara daxil olan hüquq və öhdəliklər konkret müəyyənləşdirilir. Bu da fərdi məlumat subyektlərinin hüquqlarının qorunmasında müasir çağırışlara cavab verir.

IV. FƏRDİ MƏLUMAT SUBYEKTLƏRİNİN HÜQUQLARININ TƏMİN EDİLMƏSİNİN ÜSUL VƏ VASİTƏLƏRİ

Azərbaycan Respublikasının qanunvericiliyində fərdi məlumatların qorunmasının təmin olunması üsulları ümumi olaraq müəyyənləşdirilir, bununla belə, bəzi məsələlərə yenidən baxılması və qiymətləndirilməsi effektiv fərdi məlumatların mühafizə sisteminin formalaşması üçün vacibdir. Məsələn, məlumatların nəzarətində olduğu şəxslərin fərdi məlumat subyektlərinə qarşı öhdəlikləri ilə bağlı Qanunun 10-cu maddəsində mülkiyyətçinin və operatorun vəzifələri

müəyyənəşdirilir. Lakin bu öhdəliklər ümumi xarakterlidir və toplanmış məlumatların qorunmasının təmin edilməsi ilə bağlıdır. Nümunə üçün Avropa Birliyi təcrübəsində [3] fərdi məlumatların nəzarəti altında olduğu idarəçiləri fərdi məlumat subyektlərinə qarşı vəzifələri konkret müəyyən olunur. Bu da idarəçi ilə bərabər fərdi məlumat subyektinə onun haqqında toplanmış məlumata nəzarət etmək imkanı yaradır. Məsələn, Direktivin 13-cü maddəsinə əsasən fərdi məlumat subyektinin özündən məlumatlar toplanarkən ona idarəçinin və ya onun nümayəndəsinin, məlumatların mühafizəsi ilə məsul şəxsin əlaqə ünvanlarını vermək, şəxsi məlumatların işlənməsinin hüquqi əsasları, məlumatların toplanmasına razılığın verilməsi, razılığın geri götürülməsi, müddət, şikayətlərin verilməsi qaydaları və s. ilə bağlı məlumatlar verilməlidir. Direktivin 14-cü maddəsi isə fərdi məlumatların fərdi məlumat subyektdən birbaşa alınmadığı hallarda fərdi məlumat subyektinə təqdim edilməli olan məlumatları müəyyənəşdirir. Belə bir hüquqi tənzimlənmə subyekt üçün qanunvericiliklə nəzərdə tutulmuş hüquqlarının həyata keçirilməsi üçün konkret vasitələr və üsulları təmin edir. Fərdi məlumat subyektlərinin məlumatlara çatımlılıq, məlumatların dəyişdirilməsi və silinməsi, məlumatların işlənməsinin məhdudlaşdırılması, məlumatların ötürülməsi, etiraz etmək hüquqları onlara özləri barədə toplanmış məlumatlara nəzarət etmək imkanını yaradır.

Avtomatlaşdırılmış emal nəticəsində verilən qərarlar, yəni müəyyən sayda məlumatların avtomatik emalı nəticəsində əldə edilən avtomatik qərarların hüquqi effekti barədə müxtəlif müzakirələr mövcuddur. Fərdi məlumatlarla bağlı qeyd edilməlidir ki, məlumat subyektlərinin yalnız avtomatlaşdırılmış emala əsasən verilmiş qərarların subyekt olmamaları hüququnun qanunvericilikdə təsbit edilməsi vacibdir. Belə ki, hazırda İnternet əsrində, süni intellektin sürətlə qararqəbul etmədə tətbiqi, avtomatik qərarların (sadəcə informasiyanın emalı nəticəsində texnoloji sistemin verdiyi və insan tərəfindən qiymətləndirilməmiş qərarlar) insanlara təsir imkanları böyükdür (burada həm mənfə, həm də müsbət təsir ola bilər) və həm də şəxs üzərində hüquqi nəticə yarada bilər. Ona görə də, bu məsələlərin həlli üçün şərtlər qanunvericiliklə tənzimlənməlidir.

Milli qanunvericilikdə fərdi məlumatların məhv edilməsi ilə bağlı bir neçə müddəə nəzərdə tutulub. Bu şəxs barədə fərdi məlumatların informasiya sistemlərindən silinməsinə ehtiva edir. “Unudulmaq hüququ” (right to be forgotten) fərdi məlumatların qorunması və şəxsi və ailə həyatına hörmət hüququ ilə əlaqəli İnsan hüquqlarında yer alır. Azərbaycan Respublikasının qanunvericiliyində bu barədə bəzi məsələlər tənzimlənir, lakin onun konkretləşdirilməsi məlumat subyektlərinin hüquqlarının müdafiəsi üçün vacibdir. Belə ki, məhv edilmə bir neçə halda – subyektin özünün istəyi ilə, məlumatın nəzərdə tutulmuş saxlanma müddəti başa çatdıqda və ya daşıyıcının məhvi və s. baş verə bilər. Unudulmaq hüququ isə subyektin özünün tələbi ilə qanunvericiliklə müəyyən əsaslarla onun barədə məlumatların silinməsinə müəyyən edir.

Beləliklə, məlumatların şəxsin istəyi ilə silinməsinin əsaslarının qanunvericilikdə müəyyənəşdirilməsi bu sahədə tənzimlənmənin effektivliyinə təsir edə bilər.

NƏTİCƏ

Fərdi məlumatlar 1) fundamental insan hüquqları; və 2) fərdi məlumatların mühafizəsi - yəni bir-biri ilə sıx bağlı olsa da, tam üst-üstə düşməyən iki fərqli çərçivədə nəzərdən keçirilir. Bununla belə, şəxsi və ailə həyatına hörmət hüququnun tərkib hissəsi kimi şəxsiyyət fərdi məlumatların mühafizəsinin əsasında durur. Fərdi

məlumatların mühafizəsi qanunvericiliyində məlumat subyektlərinin hüquqları ilə bağlı müddəalara yenidən baxılmasına ehtiyac vardır.

İnternet mühitində və süni intellektin inkişaf etdiyi dövrdə məlumatların mühafizəsi və mühafizənin digər hüquq sahələri və qanuna əsasən gözlənilən maraqların təmin olunması ilə qarşılıqlı əlaqədə qiymətləndirilməsi zəruridir. Buna görə də, fərdi məlumatların toplanmasının uyğunluq, maraqların balanslaşdırılması və ictimai maraq prinsipləri əsasında digər əsas insan hüquqlarının müdafiəsi ilə uyğunlaşdırılması prinsip kimi müəyyənəşdirilməlidir. Avtomatlaşdırılmış qərarların insanın şəxsiyyətinə və ona məxsus məlumatların mühafizəsinə təsiri də subyektlərin hüquqlarının qorunmasında nəzərə alınmalıdır.

Təhsil, sosial, iqtisadi, əmək, idarəçilik, səhiyyə, biznes və digər sahələrdə mərkəzləşdirilmiş və ya mərkəzləşdirilməmiş məlumat bazalarının və ya platformaların aktiv şəkildə tətbiqi fərdi məlumatların mühafizəsinə həssas yanaşılmanı tələb edir.

İSTİNADLAR

- [1] Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu, 11 may 2010-cu il, № 998-IIIQ. <http://e-qanun.az/framework/19675>
- [2] Convention for the Protection of Human Rights and Fundamental Freedoms https://www.echr.coe.int/Documents/Convention_ENG.pdf
- [3] EU General Data Protection Regulation. <https://gdpr-info.eu/>
- [4] G. González Fuster and H. Hijmans The EU rights to privacy and personal data protection: 20 years in 10 questions. 2019, 13 p. https://brusselsprivacyhub.eu/events/20190513.Working_Paper_Gonza%CC%81lez_Fuster_Hijmans.pdf
- [5] Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen. Judgment of the Court (Grand Chamber) of 9 November 2010. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0092>
- [6] Protection of personal data. Factsheet. Court of Justice of the European Union, December 2017. https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf
- [7] European Court of Human Rights Factsheet – Personal data protection. 2019. https://www.echr.coe.int/Documents/FS_Data_ENG.pdf

ANALYSIS OF THE RIGHTS OF PERSONAL DATA SUBJECTS

Gunel Valiyeva

Baku State University, Baku, Azerbaijan

Abstract – Protection of personal data belonging to the person and providing opportunity to identify the person is part of the protection of personal data and right to respect to private and family life. Rights to be guaranteed in the legislation for the personal data subjects strengthens choices of them to influence data protection due to gathering, processing and use of them. Gathering of information and distribution in various fields on various platforms and, accessibility of personal data for third parties in the Internet environment claims active participation of personal data subjects and their control on the process. And this depends on the effectiveness of the guarantees provided in the legislation for personal data subjects in respect to personal data protection and right to private and family life. In this perspective rights of personal data subjects that needs to be provided in the legislation might be evaluated wholly reflecting both guarantees for personal data protection, and right to private and family life.

Keywords – personal data, personal data subjects, rights of personal data subjects

Fog computing texnologiyalarında məlumatların təhlükəsizliyi məsələləri

Rəşid Ələkbərov¹, Məmməd Həşimov²

^{1,2} AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹t.direktor_muavini@iit.science.az, ²mamedhashimov@gmail.com

Xülasə— Məqalədə Əşyaların İnternetində (IoT) Fog Computing texnologiyalarından istifadənin perspektivləri göstərilmişdir. Bu texnologiyadan istifadə zamanı məlumatların təhlükəsizliyi məsələləri analiz edilmişdir. Fog computingin müxtəlif səviyyələrində potensial təhlükəsizlik təhdidləri təhlil edilmiş və həmin təhdidlər nəticəsində məlumatların məxfiliyinə təsir edən müəyyən aspektlər qeyd olunmuşdur.

Açar sözlər— əşyaların interneti; hesablama buludları; duman texnologiyaları; duman təhlükəsizliyi

I. GİRİŞ

Əşyaların İnterneti (ing. *Internet of things, IoT*), Kiber-Fiziki sistemlər və Mobil İnternet texnologiyalarının inkişafı, insan, maşın və əşyalar da daxil olmaqla müxtəlif obyektləri istənilən zaman istənilən məkanda informasiya mühiti ilə əlaqələndirir. “Əşyaların İnterneti” Dünya İqtisadi Forumunun qiymətləndirməsində dünyanı dəyişdirəcək texnologiyalar arasında ilk sıralarda yer alır və bu texnologiyaların yaxın 10 ildə dünya iqtisadiyyatında əsas trend olacağı proqnozlaşdırılır. IoT cihazlarının sayı 2017-ci ildə 31% artaraq 8.4 milyarda çatmış və 2020-ci ildə bu sayın 30 milyarda çatacağı gözlənilir [1]. Misli görünməmiş həcmdə və növdə verilənlər generasiya edilir. Bu isə öz növbəsində “məlumat partlayışı” adlanan böyük miqdarda verilənlərin yaranmasına gətirib çıxarmışdır. Məlumatların həcmində müşahidə edilən sürətli artım ilə bərabər məlumatların generasiya sürəti də getdikcə artmaqdadır. Bu isə böyük həcmdə məlumatların emalı və saxlama imkanlarının müasir dövrdə tələblərə cavab verə bilmədiyini göstərir.

IoT texnologiyalarında istifadə edilən ağıllı cihazların hesablama gücü, batareya, yaddaş və s. məhdud olduğundan, IoT proqramları və xidmətləri çox vaxt buludda yerləşən güclü server tərəfindən təmin edilir. Belə ki, cloud computing, son istifadəçilərə xidmətlərin göstərilməsi və tətbiqləri aşağı xərcə çoxsaylı resurslarla təmin etmək üçün perspektivli həll hesab edilir [2]. Beləliklə, yüksək hesablama gücünə və yaddaş imkanlarına malik cloud computing həmin məlumatların emalı üçün effektiv həll kimi qəbul olunur.

Cloud computing mərkəzləşdirilmiş bir hesablama modeli olduğundan, hesablamaların əksəriyyəti buludda yerinə yetirilir. Bu isə, bütün məlumat və sorğuların mərkəzləşdirilmiş buluda ötürülməsi deməkdir. Verilənlərin emal sürətinin artmasına baxmayaraq, şəbəkənin keçiriciliyi əhəmiyyətli dərəcədə artmamışdır. Beləliklə, şəbəkənin keçiriciliyi böyük həcmdə məlumatların emal edilməsi üçün cloud computing sistemi üçün problemlər yaranır [3].

Cloud computing-in generasiya olunmuş məlumatların emal edilib saxlanması üçün effektiv texnologiya olmasına baxmayaraq, mövcud tətbiqlərin real zamanda istifadəsi və ya gecikmə ilə bağlı problemlərə malik olması, eyni zamanda şəbəkənin aşağı keçiricilik qabiliyyəti kimi problemlərin həlli yalnız cloud computing vasitəsilə mümkün deyil.

Yuxarıda deyilənləri nəzərə alaraq hal-hazırda məlumatların toplanması (sensorlardan) və ilkin emalı üçün aralıq hesablama sistemlərindən geniş istifadə olunur. Bu səbəbdən də hesablama buludlarından əlavə fog computing (“hesablama dumanı”) adlanan yeni hesablama paradigması təklif edilmişdir.

II. FOG COMPUTING TEXNOLOGİYALARI

Fog texnologiyaları IoT-a adekvat həll gətirən yeni konsepsiyadır. Ənənəvi cloud computing sisteminə verilənlər mərkəzinin yükünün azaldılması üçün fog computing coğrafi olaraq paylanmış, gecikmə problemləri və yüksək keyfiyyətli xidmət təmin edən IoT tətbiqlərinin dəstəklənməsi üçün alternativ həll kimi təklif edilmişdir.

Fog computing sistemi ilk dəfə Cisco şirkəti tərəfindən təklif edilmişdir. “Duman” termini “*yerə ən yaxın bulud*” kimi təklif edilmişdir, yəni yenilənmiş və daha yaxşı tətbiq və ya xidmətləri təmin edən bilən mərkəzdən (növədən) həddlərə qədər hesablama kimi izah olunur. Fog computing – son istifadəçi ilə data mərkəz arasında hesablama, yaddaş və şəbəkə xidmətlərini təmin edən yüksək səviyyədə virtualaşdırılmış platformadır [4].

Fog computing ümumiyyətlə cloud computing ilə əlaqələndirilir. Məsələn, hesablama, yaddaş və şəbəkə resursları həm fog computing, həm də cloud computingin struktur bloklarıdır. Bu isə onu göstərir ki, əksər cloud computing texnologiyaları fog computing texnologiyalarına birbaşa tətbiq oluna bilər. Bununla yanaşı, fog computing sistemi onu digər mövcud hesablama arxitekturalarından fərqləndirən bir sıra unikal xüsusiyyətlərə malikdir. Həmin xüsusiyyətlərdən biri və ən əhəmiyyətlisi onun son istifadəçilərə yaxın məsafədə yerləşməsidir [2].

Fog computing qovşaqları sensor və kənar qurğuların generasiya etdiyi məlumatları emal edir və saxlayır. Daha sonra isə qalan əhəmiyyətli məlumatların saxlanması və ya gələcəkdə emal edilmə üçün bulud serverinə ötürülür. Ənənəvi cloud computing modeli ilə birləşərək, fog computing cloud computingə daha səmərəli xidmət göstərməyə imkan yaradır.

IoT-da Fog computing texnologiyalarından istifadənin üstünlükləri [5]:

- Bulud xidmətləri fog computing vasitəsilə IoT cihazları üçün təmin olunur;
- Fog computing, cloud computing ilə IoT cihazları arasındakı səviyyəni təşkil edir;
- Fog computingdə bir neçə qovşaq mövcud ola bilər;
- Sensorlar vasitəsilə toplanan məlumatlar buluda göndərilmədən əvvəl fog serverlərdə emal edilir;
- Fog computing gecikməni azaldır, buludun ötürücülük və yaddaş resurslarına qənaət etməyə imkan verir.

Fog texnologiyası əsasən aşağıdakı sahələrdə tətbiq edilir [6]:

- Ağıllı şəhərlərdə (nəqliyyatda işıqlandırma sistemi);
- Real zamanda sağlamlığın təhlili (xronik xəstəliyi olan xəstələr real zamanla izlənilə bilər, fəvqəladə hallarda müvafiq həkimlərə dərhal xəbərdarlıq göndərilməsi və s.);
- Enerji səmərəli intellektual sistem (gündəlik enerji istehlakı hesablatlarını hazırlayır, daha qənaətli enerji istifadəsi planını təklif edir və s.);
- Real zamanda dəmiryolunun monitorinqi (yol şəraitinin real zamanda monitorinqi);
- Real zamanda külək dəyirmanı və turbinin təhlili (küləyin istiqaməti və sürətinin analizi) və s.

Son illərdə cloud computing, fog computing kimi korporativ idarəetmə sistemlərinə keçid müşahidə olunur. Neft-qaz sənayesində SCADA kimi tətbiqlərin fog mühitinə köçürülməsi, potensial xərclərin azaldılması, miqyaslanma imkanları, səmərəli sistem konfigurasiyası və texniki təminatı baxımından daha cəlbəedici hesab olunur [7]. Neft-qaz sənayesi üçün fog texnologiyası əsasən aşağıdakı sahələrdə tətbiq edilir:

- Neft-qaz sənayesində boru kəmərinin optimallaşdırılması (təzyiqin, axının, kompressorun real zamanda monitorinqi);
- Neft quyularının qazma qurğularına nəzarət (neft pompalarının enerji təchizatı gərginliyinə və cərəyanına nəzarət);
- Geolokasiya vasitəsilə heyətin izlənməsi və müəyyən təhlükəsizlik amillərinin monitorinqi və s.

IoT texnologiyaları vasitəsilə əlaqələndirilən obyektlərin sayı sürətlə artdığından böyük həcmdə məlumatlar generasiya edilir. Verilənləri generasiya edən qovşaqlar paylanmış olduğundan onlara mərkəzləşmiş nəzarət çətinləşir. Digər vacib məsələlərdən biri isə paylanmış Fog computing arxitekturasındakı verilənlərin təhlükəsizliyi və məxfiliyidir.

III. FOG COMPUTING TEXNOLOGİYALARINDA TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Fog computing, məlumat mərkəzinin ümumi yükünün azaldılması məqsədilə paylanmış qovşaqların hesablama gücünə əsaslanır. Bundan əlavə, duman qovşaqları böyük coğrafi ərazilərə səpələndiyindən müxtəlif şəbəkə standartları, protokolları, topologiyalarından və s. istifadə olunur. Duman qovşaqları arasındakı rabitə əlaqəsindən aşağıdakı təhlükəsizlik və etibarlılıq məsələləri meydana çıxmışdır [8]:

- Hər duman qovşağı müstəqil olub, mesaj ötürmə yolu ilə digərləri ilə əməkdaşlıq edə bilər. Duman qovşaqları şəbəkəyə yaxşı integrasiya edilmədikdə və birlikdə qənaətbəxş xidmətləri təmin edə bilmədikdə etibarlılıq problemləri yaranı bilər.
- Duman qovşaqları istənilən şəbəkə vasitəsilə əlaqə qura bilər. Onlar arasındakı rabitə çox böyük ola bilər. Gecikmə problemləri tətbiqlər üçün bu, ciddi bir problem ola bilər. Bu, sistemin etibarlılığını aşağı sala, daha sonra isə tapşırığın həlli müddəti başa çatdıqda istifadəçilər arasında etibar böhranına səbəb ola bilər. Nəticədə, yerüstü rabitənin tələb edilən səviyyəyə endirilməsi vacib məsələyə çevrilir.
- Yeni duman qovşağı əlavə edildikdə və ya əvvəlki qovşaq xidməti təmin edə bilmədikdə və şəbəkədən çıxarılmalı olduqda, digər duman qovşaqları aralarındakı rabitəni təmin etmək məqsədilə potensial olaraq öz topologiyalarını dəyişdirməli və rabitə strukturlarını yenidən qurmağa olurlar. Topologiyanın yenidən qurulması prosesi isə yeni təhlükəsizlik problemlərinin yaranmasına səbəb olur.
- Duman qovşaqları digər qovşaqlarla əməkdaşlıq etdiyi zaman, hər hansı qovşaq zərərli istifadəçi tərəfindən hücumla məruz qaldıqda və yoluxdurulduqda, yoluxmuş qovşağın özü digər qovşaqlara hücum edə və ya onları da yoluxdura bilər. Bu isə, bütün əlaqəli qovşaqlar arasında təhlükəsizlik və ya inam böhranına səbəb ola bilər.

Fog computing platformasının yaradılma mərhələlərinin hər birində təhlükəsizlik və məxfilik nəzərə alınmalıdır. Bu, fog computing sahəsində mövcud olan ən problemlı məsələlərdən biri hesab olunur. Fog computing texnologiyasının müxtəlif səviyyələrində potensial təhlükəsizlik təhdidlərinə aşağıdakıları aid etmək olar [9, 10, 11]:

- **Qovşaqların aşkarlanması/Cihazlara müdaxilə (Node Capture/Device Tampering):** IoT-un şəbəkə keçidlərində mövcud olan obyektlərə (əşyalara) müdaxilə etməklə vacib məlumatların sızması baş verir. Bu isə bütün şəbəkədəki istifadəçi məlumatlarının məxfiliyini təhlükə altına atır.
- **Aldadıcı hücumlar (Spoofing Attack):** Hücum edən məlumatları saxtalaşdıraraq onları şəbəkəyə göndərir. IoT qurğuları orijinal mənbənin saxta

identifikasiyalarını qəbul edərək hücum edən üçün sistemə tam girişi təmin edir.

- **Zərərli məlumatlar (Malicious Data):** Sistemə əlavə olunduqda zərərli qovşaq zərərli məlumat yaymaqla bütün sistemi yoluxdurur (pozur).
- **Təkrar hücumlar (Replay Attack):** Orijinal məlumat paketləri saxta məlumat paketləri ilə əvəz olunaraq şəbəkənin etibarlı identifikasiyası təhlükə altına alınır.
- **SYBIL hücumu:** Zərərli qovşağın şəbəkəyə daxil olması nəticəsində aqreqat mesajı saxta mesajla dəyişdirilir. Ən effektiv bağlantının seçilməsi imkanı bloklanır.
- **Selektiv yönləndirmə (Selective Forwarding):** Bəzi məlumat paketləri bloklanır və zərərli qovşaq tərəfindən selektiv şəkildə atılır. Selektiv yönləndirmə hücumlarının əsas iki növü mövcuddur. Bunlara məlumat paketlərinin atılması və məlumat paketlərinin yoluxmuş qovşaq tərəfindən təsadüfi olaraq yönləndirilməsi aiddir.
- **Qara dəlik hücumu (Blackhole Attack):** Etibarsız marşrutlaşdırma məlumatı yaradılır və bütün məlumat paketləri “qara dəliyə” yönəldirilir. Bu, şəbəkənin həddən artıq yüklənməsinə və paketin atılmasına səbəb ola bilər.
- **Hello-Flood Hücumu:** Hücum edən, şəbəkə tıxacı yaratmaq məqsədilə kanalı saxta məlumat paketləri ilə yükləyir. Bundan əlavə, o, məlumat paketinin ötürülməsində iştirak etmək məqsədilə hər bir qovşağı ona qonşu olan qovşağın zərərli olduğuna inandırır.
- **Acknowledge Flooding:** DoS (Denial-of-service attacks (Xidmətdən imtina hücumları)) hücumlarında olduğu kimi, hücum edən təsdiqlənmədən istifadə etməklə qonşu qovşaqlara saxta məlumatlar göndərir.
- **Məlumatın aşkarlanması (Data Disclosure):** Hücum edən, qovşaqdan məlumatı əldə etmək məqsədilə verilənlərin axtarış metodlarından istifadə edir, bu isə məxfilik təhdidlərinə səbəb ola bilər.
- **Sniffer/Casus (Sniffer/Logger):** Hücum edən, trafik analizatorundan (sniffing) istifadə etməklə şifrə, e-poçt və FTP faylları kimi vacib məlumatları ələ keçirir. Şəbəkədəki bir çox protokollar trafik analizatoruna qarşı davamlı deyil.
- **Fişinq hücumu (Phishing attack):** Vacib məlumatların ələ keçirilməsi və məhv edilməsi üçün əsas orqanın e-poçt ünvanından istifadə olunur. Burada hücum edən virusla yoluxmuş e-poçt və fişinq veb saytları vasitəsilə istifadəçilərin identifikasiya məlumatlarını saxtalaşdırmaqla, onların gizli məlumatlarını (şəxsiyyət, parol) ələ keçirə bilər.

- **İnyeksiya (Injection):** Serverdə icra olunan proqrama zərərli kodların yeridilməsindən ibarət olub ən çox istifadə edilən hücumlardan biridir. Bu hücum, məlumatlar itkisinə səbəb ola və proqramın hesabatlılığına ziyan vura bilər.
- **Seansın oğurlanması hücumu (Session Hijacking):** Bu hücum əsasən digər şəxsin kimliyinə hücumdan ibarətdir. Bununla da, autentifikasiya məlumatlarının idarəetməsində yaranan boşluqlar səbəbindən hücum edən fərdi kimlikləri əldə etmək imkanı qazanır.
- **Məlumat məxfiliyi:** Məlumatların qorunma üsullarının zəif olması, məlumat itkisi və sistemə uzunmüddətli ziyanın vurulması ilə nəticələnir.

Müxtəlif heterogen İOT cihazları ilə birgə paylanmış fog computing sistemi, müxtəlif təhlükəsizlik hücumlarına qarşı həssasdır. İstifadəçi məlumatları duman qovşaqları üzərindən toplandığı, emal edildiyi, ötürüldüyü və paylandığı üçün onların məxfiliyi bir çox baxımdan fog computing sahəsində ciddi məsələlərdən birinə çevrilmişdir. Hücum edən, təhlükəsizliyi zəif təmin olunmuş kənar qovşaqlardan giriş nöqtəsi kimi istifadə edə bilər. Şəbəkəyə daxil olmuş şəxs isə istifadəçilər arasında mübadilə edilən məxfi məlumatları mənimsəyə və oğurlaya bilər. Heç bir istifadəçi məlumatlarının və ya kimliyinin açıqlanmasını istəmir. Lakin təhdid və ya hücumlar nəticəsində məlumatların qorunub saxlanması mümkün deyil. İstifadəçi məxfiliyinə aşağıdakı bəndlər aiddir [12,13]:

- **Kimliyin məxfiliyi.** İstifadəçi kimliyinə obyektin əsas atributları, yəni onun adı, mobil telefon nömrəsi, ev ünvanı, viza eyniləşdirmə nömrəsi, lisenziya eyniləşdirmə nömrəsi daxildir. Bütün bu məlumatları qeyd etməklə duman qovşaqlarının identifikasiyasını əldə etmək mümkündür.
- **Verilənlərin məxfiliyi** duman qovşaqları vasitəsilə əlaqə qurarkən istifadəçi məlumatları kənar şəxslərin əlinə düşə bilər. Həmin məlumatları araşdırmaqla, istifadəçinin ünvanı, üstünlük verdiyi ideyalar və siyasi ideologiya kimi müxtəlif növ əhəmiyyətli məlumatlar əldə edilə bilər. Məsələn, onlayn səsvermə, istifadəçinin siyasi fikirlərinin aşkarlanmasına səbəb ola bilər.
- **İstifadə məxfiliyi** dedikdə, adətən, istifadəçinin duman xidmətlərindən istifadə etdiyi prinsip və ya qaydalar nəzərdə tutulur. Məsələn, ağıllı sayğacın qeydə aldığı məlumatlar istifadəçilərin yatmaq vaxtını və ya evdə olmadığı vaxtı aşkarlamağa imkan verir, bununla da onun məxfiliyi pozulur.
- **Yerləşmə məxfiliyi** adətən fog computing texnologiyasının həddlərində yerləşən istifadəçilərin yerləşmə məxfiliyinə aid olur. Məlumatlar adətən son duman qovşaqlarına çatdırıldığından istifadəçilərin digər duman qovşaqlarından hansı məsafədə yerləşdiyini təyin etmək tələb oluna bilər. Bundan

əlavə, istifadəçi bir çox duman xidmətlərindən istifadə etdiyi halda, məlumatların hansı yolla əldə edildiyi asanlıqla təyin edilə bilər və bu səbəbdən də yerləşmə məxfiliyi təhlükə altına düşər. Ümumiyyətlə, fog computing istifadəçisi üçün ən yaxın duman qovşağı seçilir. Bu seçim istifadəçinin yük balansı, statusu, gecikməsi və s. kimi meyarlar əsasında həyata keçirilir. Yerləşmə haqqında məlumatın əlverişliliyi hər iki tərəf – həm istifadəçi, həm də duman qovşaqları üçün təhlükəli ola bilər. İstənilən duman qovşağından son istifadəçinin yeri, son istifadəçidən isə duman qovşağının yeri asanlıqla təyin edilə bilər.

NƏTİCƏ

Əşyaların İnterneti texnologiyalarının yaradılması, müasir dövrdə istənilən yerdə rast gəlinən avadanlıqlar arasında qarşılıqlı əlaqə və kommunikasiyaya səbəb olmuşdur. Son dövrlərdə müxtəlif təyinatlı sensorlar vasitəsilə toplanan məlumatların emal edilib saxlanması üçün Fog Computing texnologiyalarından istifadə olunması daha səmərəli hesab olunur. Cloud computinglə müqayisədə Fog computing, paylanmış qovşaqların hesablama gücünə əsaslanır. Bu səbəbdən də Fog computing texnologiyasında təhlükəsizliyin təmin olunması daha mürəkkəbdir. Bu məqsədlə də, məqalədə Fog computing şəbəkəsində məlumatların məxfiliyinə təsir edən potensial təhlükəsizlik təhdidləri analiz olunmuşdur.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikası Dövlət Neft Şirkətinin (SOCAR) Elm Fondunun maliyyə yardımı ilə yerinə yetirilmişdir – **Müqavilə № 03LR – AMEA.**

İSTİNADLAR

- [1] Report-internet of things. <http://reports.weforum.org/industrial-internet-of-things/generalfindings/2-1-the-state-of-the-market/>
- [2] S. Yi, Z. Hao, Z. Qin, Q. Li, “Fog Computing: Platform and Applications,” Third IEEE Workshop on Hot Topics in Web Systems and Technologies, pp. 73-78, 2015.
- [3] P. Hu, S. Dhelima, H. Ning, T. Qiu, “Survey on Fog Computing: Architecture, Key Technologies, Applications and Open Issues,” Journal of Network and Computer Applications, vol. 98, pp. 27-42, 2017
- [4] M. Mukherjee, L. Shu, D. Wang, “Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges,” IEEE

Communications Surveys & Tutorials, vol. 20, no. 3, pp. 1826-1857, 2018

- [5] H.F. Atlam, R.J. Walters, G.B. Wills, “Fog Computing and the Internet of Things: A Review,” Big Data Cognitive Computing Journal, vol. 2, no. 2, 2018.
- [6] A.V. Dastjerdi, H.Gupta, R.N. Calheiros, S.K. Ghosh, R. Buyya, “Fog Computing: principles, architectures, and applications,” Internet of Things: Principles and Paradigms, Chapter 4, pp. 61-75, 2016
- [7] M. D. Stojanović, S. V. B. Rakas, J. D. M. Petrović, “Scada Systems in the Cloud and Fog Environments: Migration Scenarios and Security Issues,” Electronics and Energetics, vol. 32, no. 3, pp. 345-358, 2019.
- [8] P.Y. Zhang, M. C. Zhou, G. Fortino, “Security and trust issues in Fog computing: A survey,” Future Generation Computer Systems, vol. 88, pp. 16-27, 2018
- [9] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, R. Ranjan, “Fog Computing Security Challenges and Future Directions [Energy and Security],” IEEE Consumer Electronics Magazine, vol. 8, no. 3, pp. 92-96, 2019.
- [10] T. Veeraj, K. K. Kumar, “A survey on fog computing: research challenges in security and privacy issues,” International Journal of Engineering & Technology, vol. 7, pp. 335-340, 2018
- [11] D. Puthal, S. Nepal, R. Ranjan, J. Chen, “Threats to Networking Cloud and Edge Datacenters in the Internet of Things,” IEEE Cloud Computing, vol. 3, no. 3, pp. 64-71, 2016
- [12] A. Aljumah, T. A. Ahanger, “Fog Computing and Security Issues: A review,” 7th International Conference on Computers Communications and Control (ICCCC), pp. 237-239, 2018
- [13] P. Kumar, N. Zaidi, T. Choudhury, “Fog Computing: Common Security Issues and Proposed Countermeasures,” 5th International Conference on System Modeling & Advancement in Research Trends, pp. 311-315, 2016

DATA SECURITY IN FOG COMPUTING

Rashid Alekperov¹, Mammad Hashimov²

^{1,2}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹*t.direktor_muavini@iit.science.az,*

²*mamedhashimov@gmail.com*

Abstract— The article highlights the prospects of using fog computing in the Internet of Things. The use of this technology is analyzed for data security. Potential security threats at various levels of Fog Computing are analyzed. Some aspects caused by these threats affecting data privacy are identified.

Keywords— *Internet of Things, Cloud computing, Fog computing, Fog security*

LoRaWAN şəbəkəsində istifadəçi məlumatlarının təhlükəsizliyi problemləri və həlli yolları

Təbriz Ağışov

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
tabriz@science.az

Xülasə— Məqalədə əşyaların internetində (IoT) istifadəçi məlumatlarının təhlükəsizliyi üçün mövcud olan kriptografik açarların idarəetmə protokolu araşdırılmış və reputasiya sistemini tətbiq etməklə IoT-larda istifadə olunan LoRaWAN şəbəkə arxitekturasının təhlükəsizliyini artırmaq üçün həll təklif edilmişdir. Məqalədə kriptografiyaya əsaslanan bəzi təhlükəsizlik məsələləri analiz edilmiş və həll yolları göstərilmişdir.

Açar sözlər— IoT; LoRa; LoRaWAN; AES128; kriptografik açar; heterogen; end nod; proksi-nod

I. GİRİŞ

Əşyaların interneti insanlara aid olan bir çox cihazları İnternet-ə bağlayaraq həyatımıza daxil olmuşdur. Bu həm insanlara daha ağıllı və daha rahat yaşamağa imkan verir, həm də onların fərdi və məxfi məlumatlarına, eləcə də onlara məxsus müxtəlif elektron cihazlara təcavüz edilməsinə zəmin yaradır. IoT-lar İnternetin mövcud infrastrukturunda unikal identifikasiyaya malik fiziki qurğulardır. Bu qurğular ətraf mühitdən məlumatların toplanması və onların İnternet üzərindən intellektual şəbəkələr, ağıllı şəhərlər, ağıllı evlər və elektron səhiyyədə tətbiqi üçün istifadə edilir [1, 2].

Əşyaların İnternetinin məqsədi insanların gündəlik həyat şəraitinin yaxşılaşdırılması, yeni və daha əlverişli iş yerlərinin açılması, biznes üçün yeni imkanların yaranması, istehsalda səmərəliliyin, məhsuldarlığın və rəqabətə davamlılığın artırılmasıdır. Əşyaların internetində istifadə olunan qurğular arasındakı qarşılıqlı əlaqə onların şəbəkəsini əmələ gətirir. Əşyaların interneti hamı üçün əlverişli olan adi İnternet qovşaqlarından, həmçinin qeyri-məhdud sayda xüsusi şəbəkədən ibarətdir [1].

İnternetin tənzimlənməsi ilə bağlı bütün problemlər əşyaların interneti üçün də aktuallıq kəsb edir. İnformasiya təhlükəsizliyinin, istifadəçilərin fərdi məlumatlarının qorunması kimi məsələlər həll edilmədən bu şəbəkənin uğurlu fəaliyyəti mümkün deyil. Beləliklə, istifadəçilərin fərdi və məxfi məlumatlarını müxtəlif hücumlardan qorumaq üçün təhlükəsizlik məsələlərinin həllərindən istifadə etməklə əşyaların internetinin tam funksionallığına nail olmaq mümkündür. Bunun üçün, adətən, IoT-ların heterogenlik xassələrinə uyğunlaşdırılmış və kriptografik əməliyyatları yerinə yetirə bilən protokollarla düzgün idarə edilməsi

mümkün olan kriptografik açarlardan istifadə edilir. Təklif olunan protokol iki əsas kateqoriyaya bölünür [3]:

- iki tərəf (“end nod” və şəbəkə serveri, “end-nod” və istifadəçi tətbiqi) arasında əlaqə açarının idarəetmə protokolu;
- qrupda (müvafiq olaraq üç və daha çox “end nod”dan təşkil edilmiş proksi-nodlar qrupu) əlaqəni təmin etmək üçün yaradılmış ümumi açarın idarəetmə protokolu.

IoT-lar üçün LoRaWAN şəbəkəsinin çoxlu sayda ümumi təhlükəsizlik arxitekturası mövcuddur. Tədqiqatçıların apardığı analizlər əsasında LoRaWAN-nın təhlükəsizlik arxitekturası sənaye, kənd təsərrüfatı, şəhər infrastrukturu və digər sahələrdə tətbiq edilən IoT-ların tələbatına uyğun olan ən son layihələrdən biridir. Bu arxitektura ağıllı əşyalar arasında qarşılıqlı əlaqənin və təhlükəsiz mübadilənin təmin edilməsi üçün təklif edilmişdir. Bunu bir neçə səviyyəli şifrələmə tətbiq etməklə həyata keçirmək olar [4]:

- şəbəkə səviyyəsi – “end nod”dakı məlumatların autentifikasiyasına təminat verir və “end nod”larla şəbəkə serveri arasında paylaşılan AES128 gizli açarı ilə təsdiqlənir;
- tətbiq səviyyəsi – “end nod” və istifadəçi tətbiqləri arasında paylaşılan AES128 gizli açarından istifadə edərək nodlardakı məlumatların məxfiliyi təmin edilir.

Bu işdə ikitərəfli paylanmış mövcud açarları idarəetmə protokoluna və reputasiya sisteminə əsaslanaraq LoRaWAN şəbəkə arxitekturasının təhlükəsizliyini artırmaqla istifadəçi məlumatlarının təhlükəsizlik həlli araşdırılmışdır.

II. LORAWAN-NIN ARXİTEKTURASI

LoRaWAN – aparat səviyyəli LoRa protokolu ilə dəstəklənən geniş əhatə radiuslu qlobal şəbəkədir və şlyuzlər (baza stansiyalar) vasitəsilə sondakı LoRa qurğuları (“end nod”lar, qovşaqlar) arasında kommunikasiya yaradır. LoRaWAN enerjiyə qənaət etmək üçün optimallaşdırılmış ağıllı cihazların bir-biri ilə əlaqə yaratmasını həyata keçirən, məlumatı uzaq məsafələrə ötürən və geniş əhatə radiuslu şəbəkə xüsusiyyətlərinə malikdir. Bu bölmədə LoRaWAN şəbəkəsinin arxitekturası şərh olunub.

Şəkil 1. LoRaWAN şəbəkəsinin arxitekturası

Şəkil 1-dən göründüyü kimi bu şəbəkə “end nod”lar (LoRa qurğuları, IoT-lar), şlyuzlar, şəbəkə serveri və tətbiqi serverlərdən ibarətdir. Şlyuz “end nod”lardan qəbul edilmiş məlumat paketlərini müxtəlif rabitə (Wi-Fi, mobil əlaqə, Ethernet, yaxud peyk əlaqəsi) vasitələri ilə şəbəkə serverinə ötürür. Server şəbəkədəki bütün şlyuzların idarə edilməsinə cavab verir, “end nod”lara müraciəti təmin etmək üçün hansı şlyuzdan istifadə edilməsini müəyyən edir, məlumatların ötürülmə sürətini avtomatlaşdırır, qəbul edilmiş paketləri filtrləyir və məlumatların təhlükəsizliyinin təmin edilməsini yerinə yetirir. Məlumatların emal edilməsi tətbiq serverlərində yerinə yetirilir. Cədvəl 1-də bu arxitekturanın üstünlükləri təqdim edilmişdir.

CƏDVƏL 1. LoRaWAN-IN ÜSTÜNLÜKLƏRİ

Üstünlüklər	Xüsusiyyətlər
Enerjiyə qənaət	nodlar qeyri-sinxronudur və sadəcə məlumatları ötürən anda qarşılıqlı əlaqədə olurlar
Yüksək buraxılış (ötürmə-qəbul etmə) qabiliyyəti	buna məlumatları ötürmək üçün adaptiv sürət rejimindən və xüsusi (çoxkannalla ötürmə xassəsinə malik multimodemli) şlyuzlardan istifadə etməklə nail olmaq olur. Bu zaman paralel olaraq bir neçə kanaldan məlumat almaq olur.
Müxtəlif sinifli qurğular	üç sinif müəyyən edilmişdir: A, B və C.
Təhlükəsizlik	təhlükəsizliyin iki səviyyəsi müəyyən edilmişdir: şəbəkə və tətbiq. Hər iki səviyyə üçün AES (Advanced Encryption Standard) şifrələnməsindən istifadə edilir.

“End nod”lar – bu istifadəçilər tərəfdə quraşdırılmış sensorlar, ötürücülər, sayğaclar, aktuatorlar və IoT radiomodullarının ümumiləşdirilmiş adıdır. “End nod”lar üç sinfə bölünür:

- A sinfi - ikitərəfli mübadilə yaratmaq xassəsinə malik “end nod”lar. A sinfi əsas baza sinfi olaraq şəbəkədəki bütün qurğularda dəstəklənir. Qeyd edək ki, əlaqənin yaranmasını təşkil edən də elə bu “end nod”lardır. Nod hər bir ötürmədən sonra qəbul üçün qısa müddətli iki müvəqqəti pəncərə ayırır və bu qısa vaxt ərzində

serverdən cavab gözləyir. Ötürmə intervalı “end nod”un ehtiyac meyarına əsaslanaraq planlaşdırılır. A sinfindən olan qurğular az güc sərf edərək serverə məlumatı ötürür və yalnız, bundan sonra tətbiqlərin vasitəsilə serverdən geriye məlumat göndərilməsini tələb edir. Serverdən sonrakı “end nod”a məlumatların ötürülməsi, həmin nodun serverlə əlaqəyə girdiyi anda mümkün olur;

- B sinfi - onlar da ikitərəfli mübadilə yaradır. B sinfində də A sinfində olan funksiyalar mövcuddur. Bundan başqa B sinfindən olan qurğular cədvəl üzrə qeyd edilmiş vaxtda qəbul üçün əlavə pəncərə açır. Qəbul üçün pəncərənin açılması, şlyuzların xüsusi siqnallarla (mayak, beacons) “end nod”ları sinxronlaşdırmasından sonra baş verir. Bu isə serverə nodun məlumatı qəbul etməsinə hazır olduğunu bildirir;
- C sinfi - Verilənləri qəbul etmək üçün maksimal sayda pəncərə ayırmaq imkanına malikdirlər. Qəbul pəncərəsi verilənləri ötürmə anında bağlanır. Bu tip qovşaqlar böyük həcmli verilənlərin mübadiləsi məsələləri üçün tətbiq edilir. Praktiki olaraq, C sinfindən olan qovşaqlar verilənləri ötürdükləri hallar istisna olmaqla, hər zaman qəbul rejimində olurlar. Belə qovşaqların enerji saxlama müddəti çox olur və bunun nəticəsində qəbuledicinin işləmə vaxtını məhdudlaşdırmağa ehtiyac olmur.

III. ŞƏBƏKƏ VƏ TƏTBİQİ SƏVİYYƏLƏRİNDƏ TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Məqalədə LoRaWAN şəbəkəsində OSI (Open Systems Interconnection) modelinin iki səviyyəsi üçün: şəbəkə və tətbiqi səviyyələrdə məlumatların mübadiləsi zamanı təhlükəsizliyin təmin edilməsi məsələsinə baxılmışdır (şək. 2).

Şəkil 2. LoRaWAN-nın təhlükəsizlik arxitekturası

Şəbəkə səviyyəsində “end nod”lardakı məlumatların autentifikasiyası, “end nod” və server arasında birgə istifadə olunan AES128 kriptografik açarın köməyi ilə təsdiqlənərək müəyyən olunur. Tətbiqi səviyyədə isə “end nod” və istifadəçi tətbiqlərin birgə istifadə etdiyi AES128 kriptografik açar vasitəsilə qurğulardakı məlumatların təhlükəsizliyini təmin etmək olur. LoRaWAN şəbəkəsində “end nod”lar və şəbəkə

serveri arasında məlumatların mübadiləsinin təhlükəsizliyi üçün AES128 məxfi şifrələmə açarından istifadə edilir.

Əgər müdaxilə edən bu məxfi açarı əldə edərsə, onda o “end nod” və şəbəkə serveri arasında mübadilə olunan bütün məlumatları oxuya bilər və dəyişər.

Aşağıdakı bölmədə “end nod” və şəbəkə serveri arasında mübadilə zamanı belə müdaxilələrin qarşısını almaq üçün hər bir seansda açarların dəyişdirilməsi həlli təklif olunmuşdur. Əgər məlumatların mübadiləsinin hər bir seansında şifrə dəyişdirilərsə, onda bu daha təhlükəsiz və etibarlı əlaqənin yaranmasına imkan verəcək.

IV. TƏKLİF OLUNAN HƏLL

Bu bölmədə LoRaWAN şəbəkəsinin təhlükəsizlik protokollarını təkmilləşdirmək üçün həll təklif edilmişdir. Təklif olunan həllə təhlükəsizlik açarlarının idarə edilməsi üçün reputasiya sistemindən istifadə edilir [5]. Şəkil 3-də LoRaWAN şəbəkəsinin təhlükəsizlik arxitekturası göstərilmişdir. Burada məhdud sayda nodlar bir qrup şəklində birləşdirilərək onlar arasındakı hesablamaları asanlaşdırmaq üçün proksilər (proksi-nodlar) yaradılmışdır. Təhlükəsizliyi gücləndirilən nodun AES128 şifrələnmiş açarı hər bir seansda yeni açarla əvəz edilir. Bu açar [5]-də göstərilən həll qaydasına uyğun olaraq “end nod” və şəbəkə serveri arasında quraşdırılır. Tətbiq edilmiş reputasiya sistemi proksi-nodların arasından daha etibarlı qovşağı seçir. Bu isə kriptografik açarların qəbul edilməsi mərhələsində yalnız etibarlı qovşaqların iştirak etməsinə və hücumla məruz qalmış zərərli qovşaqlar tərəfindən baş verə biləcək təhlükənin qarşısının alınmasına imkan verəcək.

Şəkil 3. LoRaWAN-nın təhlükəsizlik arxitekturası

LoRaWAN şəbəkəsinin bu yeni arxitekturası enerji sərfiyyatı və hesablama gücü baxımından heterogen qovşaqları

özündə birləşdirir. Burada üç fərqli qovşaq nəzərdən keçirilmişdir:

- “end nod” (müxtəlif ötürücülər, sensorlar, LoRa qurğuları): mürəkkəb kriptografik əməliyyatları dəstəkləmələr və məhdud resurslara malikdirlər;
- şəbəkə şlyuzu: “end nod”larla qonşuluqda yerləşdirilmiş və mürəkkəb kriptografik əməliyyatları yerinə yetirməyə malik olan qovşaqlar;
- şəbəkə serveri: yüksək həcmli yaddaş tutumuna, çevik hesablama imkanlarına və yüksək enerji istehlakına malik qovşaqlar.

Məqalədə növbəti fərziyyələr əsasında tədqiqat işi aparılmışdır.

- “end nod” və proksi-nodlar arasındakı əlaqənin təhlükəsizliyi AES128 kriptografik açarı vasitəsilə təmin edilir;
- AES128 kriptografik açarı “end nod” və hər bir şlyuz arasında etibarlı şəkildə mübadilə olunur;
- ilk Sertifikat Mərkəzi və ona uyğun AES128 məxfi açarı (nodların quraşdırılmasından əvvəl) əvvəlcədən “end nod”ların dinamik siyahısına əlavə edilir.

Bu fərziyyələrə əsaslanaraq aşağıdakı bölmədə LoRaWAN şəbəkəsinin təkmilləşdirilmiş təhlükəsizlik protokolunun üstünlüyü və mərhələləri şərh edilmişdir.

V. PROTOKOL VƏ ONUN MƏRHƏLƏLƏRİ

[5]-də təsvir olunan protokol nodların heterogenlik xassəsindən istifadə edir. Yəni məhdud funksiyalı qovşaqlar sadə kriptografik şifrələməni yerinə yetirdiyi halda, daha geniş funksiyalara malik qonşu qovşaqlar daha mürəkkəb kriptografik əməliyyatları yerinə yetirir. Bu protokolun üstünlüyü ondan ibarətdir ki, proksi hər seansda məxfi şifrənin bir hissəsini hesablayır, lakin ötürücü və qəbuledici qovşaqlarda hesablanmış tam şifrəni əldə edə bilmir. Burada hər bir nod proksi-nodların siyahısını və onlara uyğun məxfi açarları yadda saxlayır. Nəticədə, qonşu nodların sayı artdıqca böyük həcmli yaddaş tələb olunur. Kriptografik açarın etibarlılığı onların generasiyası prosesində iştirak edən proksi-serverlərin sayından aslıdır. Bu zaman məlumatların itməsi, yaxud saxta məlumatla dəyişdirilməsi son məxfi açarın hesablanmasına təsir edəcək. Beləliklə, bu həll variantını inkişaf etdirmək üçün ötürücü nodun proksi-nodları aşkar etməsi və məxfi açarın qəbul edilməsində bu proksi-nodların arasından ən etibarlısını seçməsi təklif edilmişdir. Sonra isə bu nod hər seansda açarların hesablanmasında iştirak edən həmin proksi-nodların yenilənən dinamik siyahısını yadda saxlayacaqdır [6].

Mərhələlər. Bu həddə hər proksi-nodun digər nodların reputasiyasını müəyyən etməsi üçün onlardan məlumat toplaması fərz edilir. Bu məlumatlar ya nodun özü tərəfindən birbaşa toplanmış məlumatlardır, ya da digər qovşaqlardan alınan tövsiyələrdir. Nod qonşu nodların siyahısını və onların etibarlılıq dərəcələrini müəyyən edən qiymətləri (inam dəyərini) cədvəl şəklində toplayaraq saxlayır (şək. 4). İnamin qiymətləndirilməsi, məlumat paketlərini maneəsiz ötürmək, məxfi açarları hissələrlə düzgün göndərmək, normal giriş-çıxış, istifadə etdiyi kanalın gücü və onun buraxılış imkanları da daxil olmaqla, nodların davranışını qiymətləndirməklə hesablanır. Deməli, özünü yaxşı apran nod ona inamin artdığını görəcək və digər nodlar bunu qəbul edəcək, əksinə pis nodlar bunun əksini görəcəklər [7].

Şəkil 4. Ən etibarlı nodun seçilməsi

Ən yüksək inam dəyəri olan proksi-nod Sertifikat Mərkəzi (SM) kimi seçilərək, digər proksi-nodlar üçün autentifikasiya, avtorizasiya və açarların idarə edilməsi funksiyalarını yerinə yetirəcək. Burada SM üç cədvəldən ibarətdir:

- proksi-nodların sertifikatlarının idarə edilməsi üçün istifadə olunan sertifikatlaşdırma cədvəli;
- hər bir proksi-nodun etibarlılıq dəyərini göstərən inam cədvəli;
- etibarlılıq dəyərləri sıfır olan bütün nodlar yerləşən qara siyahı.

Başlanğıcda ilk SM-in əvvəlcədən seçildiyi fərz edilir. Sonrakı hallarda o dinamik proksi-nodların inam dəyərlərinə uyğun olaraq yenilənir.

Hər bir proksi-nod özünün inam cədvəlini açıq açarlarla təmin edilmiş SM-ə göndərir. SM isə öz növbəsində bütün proksi-nodlardan alınan cədvəlləri bir araya gətirərək, AES128 məxfi açarlarla təmin edilmiş “end nod”a göndərmək üçün daha etibarlı bir qrupdan ibarət cədvəl yaradacaq. “End nod” yaradılan bu cədvəle əsaslanaraq açarın alınmasında iştirak edəcək ən etibarlı qonşuları seçəcək (şək. 4) və yeni SM-lər haqqında bütün proksi-nodları məlumatlandıracaqdır [8].

Protokolun ilkin mərhələsi. İlk mərhələdə, SM vasitəsilə şlyuzlar qrupu (proksi-nodlar) təşkil edilərək iki cədvəl, sertifikatlaşdırma və inam (əvvəlcə boş olan) cədvəlləri yaradılır. Sonra, SM multicast (çoxqütblü) prinsipinə əsaslanaraq, hər bir şlyuzun açıq açarını qrupdakı digər üzvlərə ötürür. Beləliklə, hər bir proksi-nod qrupun digər üzvlərinin bütün açıq açarlarına malik olur. Bu açarlar qrupun üzvləri arasındakı informasiya mübadiləsinin təhlükəsizliyini təmin etməklə yanaşı, əsasında proksi-nodlar olan inam cədvəllərinin yaradılmasında da istifadə ediləcəkdir. Sonra hər bir iştirakçı üzv açıq açarlarla qorunan öz inam cədvəlini SM-ə göndərəcək. SM bütün inam cədvəllərini aldıqdan sonra onlardakı inam dəyərlərinin ortalama nisbətini hesablayacaq və “end nod”a göndərilməsi üçün yekun inam cədvəlini yaradacaq. Beləliklə, “end nod” məlumatları qrupdakı şlyuzlarla bölüşmək istədikdə, o əldə etdiyi inam cədvəlindən istifadə edərək, bu cədvəldəki ən yüksək inam dəyərlərinə malik proksidən istifadə edəcək [9].

Nodun qrupa qoşulması. Proksi-nodlar qrupuna qoşulmaq istəyən yeni nod əvvəlcə SM-i aşkar etmək üçün qrupun bütün üzvlərinə mesaj göndərir (şək. 5). Mesajı alacaq ilk proksi-nod qrupun və Sertifikat Mərkəzinin identifikatorlarını özündə əks etdirən bir mesajla həmin noda cavab verir. Sonra nod, onun identifikatorunu və açıq açarını özündə saxlayan SM-ə qoşulmaq üçün sorğu göndərir. SM yeni nodun inam cədvəlində inam dəyərinə malik olub-olmadığını, yaxud onun qara siyahıya salındığını yoxlayır. Əks halda onun inam dəyəri 1-ə bərabər olmaqla inam cədvəlində saxlanılacaq. Daha sonra, SM məzmunu qrupun identifikatorundan və nodun inam dəyərindən ibarət olan bir mesajla cavab verəcək. Bu mesaj SM-in məxfi açarı və nodun açıq açarı ilə şifrələnəcək. Sonda nod aldığı mesajı deşifrə etdikdən sonra aktivləşəcək [10].

Şəkil 5. Nodun qrupa qoşulması

Nodun qrupu tərk etməsi. Nod onun haqqında məlumatları saxlayan SM-ə qrupu tərk etmək üçün mesaj göndərir (şək. 6). SM mesajı qəbul etdikdən sonra sertifikat cədvəlindən bu noda

aid olan məlumatları silir və inam dəyərini yeniləyir (1-ə qədər azaldılır). SM cavab olaraq bu noda onun sertifikatının silindiği və sistemdən (qrupdan) müvəffəqiyyətlə çıxarıldığı haqqında məlumat göndərir.

Şəkil 6. Nodun qrupu tərk etməsi

Yeni SM-in seçilməsi. SM öz inam cədvəlini yenilədiyi zaman və qrupdakı mövcud bir nodun daha yaxşı inam dəyərində sahib olduğunu aşkar edərsə, həmin nodun yeni SM olduğunu bildirəcək. Müəyyən edilmiş yeni SM təhlükəsizlik baxımından qrup üzvlərinin hər birinin sertifikatını yeniləşdirməlidir. Beləliklə, o yeni sertifikat tələb etmək üçün hər bir qrup üzvünə mesaj göndərəcək. Proksi-nodlar identifikator və açıq açarlarını yeni formalaşan SM-ə göndərəcək, o isə öz növbəsində hər nodu yeni fərdi sertifikatla təmin edəcək. Bu zaman əvvəlki, yəni köhnə SM artıq adi proksi-nod funksiyasını yerinə yetirəcək.

VI. TƏKLİF OLUNAN HƏLLİN TƏHLÜKƏSİZLİYİNİN QIYMƏTLƏNDİRİLMƏSİ

Bu işdə təklif olunan həllin məqsədi bütün təhlükəsizlik məsələlərinin, xüsusən də məlumatın identifikasiya, məxfilik və tamlığının yoxlanılmasıdır. Məxfi məlumatlar onun məxfiliyinə zəmanət verən müvafiq açarlarla şifrələndiyi üçün təklif olunan protokolun əsas məqsədi AES128 məxfi açardan istifadə edərək, “end nod”larla şlyuzlar arasında o qədər də sürətli və böyük hesablamalar tələb edilməyən əlaqənin təhlükəsizliyini təmin etməkdir. Bu məqsədlə təklif edilən protokol, SSL (Secure Sockets Layer) sertifikatından istifadə edərək şlyuzlarla şəbəkə serveri arasındakı əlaqənin daha da təhlükəsiz və etibarlı olmasına zəmin yaradacaq. Proksi-nodlar qrupunun üzvləri arasında mübadilə olunan məlumatlar nodların açıq açarları vasitəsilə qorunur. Mübadilənin sonrakı etaplarında məlumatlar və əlaqə “Man in the Middle” (ortada adam) hücumu ilə təhdid oluna bilər. Bu hücumdan müdafiə olunmaq üçün məlumatlar proksi-nodların xüsusi məxfi açarları ilə şifrələnir və bu şifrə proksi-nodlar arasından seçilmiş SM-də saxlanılır. Bu

məlumatlar yalnız SM vasitəsilə deşifrə oluna bilər. Beləliklə, həm məlumatların həqiqiliyi, həm də əlaqənin təhlükəsizliyi ən təhlükəli hesab olunan “Man in the Middle” hücumundan müdafiə olunacaqdır. Qrupa daxil olan yeni noda göndərilən məlumat həmin nodun açıq açarı, həm də SM-in məxfi açarı ilə şifrələnir və bu açarın bir hissəsini alan proksi-nodlardan heç biri seans ərzində yekun açarı tam əldə edə bilmir. Bu işdə təklif olunan protokol “Man in the Middle” hücumuna qarşı müdafiə üçün daha etibarlı hesab edilir [11].

NƏTİCƏ

Bu məqalədə əşyaların internetində istifadə olunan LoRaWAN şəbəkəsinin arxitekturasının təhlükəsizliyinin artırmaqla istifadəçi məlumatlarının təhlükəsizliyi üçün həll təklif edilmişdir. Təklif olunan bu həlldə açarların ikitərəfli idarə edilməsi üsulundan və mürəkkəb kriptografik funksiyaları yerinə yetirən etibarlı qonşu qovşaqların seçilməsini təmin edən reputasiya sistemindən istifadə edilmişdir. Bütün mübadilələrdə eyni bir kriptografik AES açarından istifadə edilərsə hücum edən şəxs bu açarı əldə də bilər. Belə təhlükələri aradan qaldırmaq üçün “end nod” və şəbəkə serveri arasında məlumat mübadiləsinin hər seansında yeni açardan istifadə edilməsi təklif edilmişdir.

İSTİNADLAR

- [1] R.M. Əliquliyev, R.Ş. Mahmudov, Əşyaların İnterneti: mahiyyəti, imkanları və problemləri // İnformasiya cəmiyyəti problemləri, 2011, №2, s.29–40.
- [2] A. Whitmore, A. Agarwal and Li Da Xu, The Internet of Things- A survey of topics and trends, Information Systems Frontiers, 2015, vol. 17, pp. 261–274.
- [3] H. Ragab, A. Bouabdallah, H. Bettahar and Y. Challal, Key Management for Content Access Control in a Hierarchy, International Journal of Computer Networks, vol. 51, No. 11, 2007, pp. 3197–3219.
- [4] LoRa Alliance Technical Marketing Workgroup, https://www.tuv.com/media/corporate/products_1/electronic_components_and_lasers/TUeV_Rheinland_Overview_LoRa_and_LoRaWANtmp.pdf
- [5] An. Braeken, P. Kumar, A. Gurtov, M. Ylianttila, Proksi-based end-to-end key establishment protocol for the Internet of Things, International Conference on Communication Workshop (ICCW), pp. 2677–2682.
- [6] M. Riyadh Abdmeziem, T. Djamel and I. Romdhani, A Decentralized Batch-Based Group Key Management Protocol for Mobile Internet of Things (DBGK), International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015, pp. 1109–1117.
- [7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, Internet of Things: A survey on Enabling Technologies, Protocols and Applications, IEEE Communications Survey and Tutorials, 2015, vol. 17, pp. 2347–2376.
- [8] N. Renugadevi, G. Swaminathan, A.S Kumar, Key management schemes for secure group communication in wireless networks a survey, International Conference on Contemporary Computing and Informatics, 2014, pp. 446–450.
- [9] S. Sciancalepore, A. Caposelle, G. Piro, G. Boggia and G. Bianchi, Key Management Protocol with Implicit Certificates for IoT systems, IoT-Sys’15 Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems, 2015, pp. 37–42.
- [10] Na S., Hwang D., Shin W., and Kim K.H., Scenario and countermeasure for replay attack using join request messages in LoRaWAN, International Conference on IEEE, 2017, pp. 718–720.

- [11] S. Tomasin, S. Zulian, L. Vangelista, Security analysis of LoRaWAN join procedure for Internet of Things networks, Wireless Communications and Networking Conference Workshops (WCNCW), 2017, pp. 1–6.

**PERSONAL DATA SECURITY ISSUES AND THEIR
SOLUTIONS IN LoRaWAN NETWORK**

Tabriz Agashov

Institute of Information Technology of ANAS, Baku, Azerbaijan
depart4@iit.ab.az, tabriz@science.az

Abstract– The paper explores the existing cryptographic key management protocol for the user data security in the Internet of Things (IoT) and proposes a solution to improve the security of LoRaWAN network architecture used in IoTs. It also analyzes some security issues related to cryptography and provides solution ways. The study proposes a solution to facilitate the computation in end nodes through proxy nodes based on the cryptographic key management protocol.

Keywords— *IoT; LoRa; LoRaWAN; AES128; cryptographic key; heterogeneous; end node; proxy node*

Etik hakinq metodlarının tədrisi haqqında

Yadigar İmamverdiyev¹, Elşən Bağirov²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹yadigar@iit.science.az, ²elsenbagirov1995@gmail.com

Xülasə— Etik hakinq sistem və ya kompüter şəbəkəsində boşluqların, səhvlərin və ya zəif nöqtələrin tapılması prosesidir. Bu işdə ali məktəb tələbələrinə etik hakinq üzrə tədris kursunun keçirilməsinin vacibliyi tədqiq edilmiş, tədris zamanı meydana çıxan problemlər təhlil edilmişdir. O cümlədən, kursun məzmunu, tələbələrin davranış kodeksi, kursun tədrisi ilə bağlı bir sıra etik və hüquqi məsələlərə baxılmışdır.

Açar sözlər— etik hakinq; informasiya təhlükəsizliyi; haker; tədris kursu; davranış kodeksi; kibertəhlükəsizlik

I. GİRİŞ

Kibertəhlükəsizliyin təmin edilməsi bütün ölkələr üçün prioritet məsələdir [1]. Bu cəhətdən son dövrlər etik hakinq metodlarının tədris olunması informasiya təhlükəsizliyi üzrə təhsilin zəruri komponentinə çevrilib [2]. Bu yanaşma yalnız müdafiə üsullarının tədrisinə əsaslanan yanaşma ilə müqayisədə daha hazırlıqlı peşəkar kadrlar yetişdirmək və ümumilikdə informasiya təhlükəsizliyini inkişaf etdirməyə imkan verir. Bir çox özəl konsaltinq qrupları böyüməkdə olan təşkilatlar üçün etik hakinq xidmətləri təklif edir. Lakin, bu böyük maliyyə vəsaiti tələb edir. Bunları nəzərə alaraq, institutda “İnformasiya mühafizəsi və təhlükəsizliyi” üzrə ixtisaslaşan magistrantların müasir tələblərə və çağırışlara uyğun hazırlanması, bu istiqamətdə aparılan elmi və praktiki işlərin təkmilləşdirilməsi məqsədilə institut rəhbərliyi tərəfindən şöbə qarşısında “Etik hakinq metodları” tədris kursunun işlənməsi və tədrisi məsələsi qoyulub.

Adətən, “hakinq” termini informasiya sistemində zəif yerlər tapmaqla sistemə icazəsiz girmək məqsədilə istifadə edilir. Lakin hakinq metodlarından cəmiyyətə faydalı məqsədlər üçün də istifadə etmək mümkündür. Çünki etik hakinq istənilən təşkilatda informasiya təhlükəsizliyinin səviyyəsini qiymətləndirməyin ən etibarlı yollarından biridir. Bu iş ona görə etik hesab edilir ki, yalnız informasiya sisteminin sahibinin xahişi ilə yerinə yetirilir və kompüter sisteminə zərər vurmadan, heç bir informasiya oğurlamadan arzuolunmaz müdaxilələrin qarşısını almaq məqsədini güdür. Etik hakinq boşluqları və nöqsanları aşkarlamaqla və aradan qaldırmaqla, səhvləri düzəltməklə təşkilatlara informasiya təhlükəsizliyinin səviyyəsini yüksəltmək imkanını verir [3, 4]. Bu səbəbdən etik hakerlər tərəfindən yerinə yetirilən nüfuzetmə testləri audit prosesi kimi qəbul edilir [4].

Dünyanın qabaqcıl universitetləri məzunların əmək bazarında rəqabətə dözümlü olması üçün informasiya təhlükəsizliyi üzrə nüfuzlu beynəlxalq sertifikatlar almasını da təşviq edirlər. Bu baxımdan, yaradılan tədris kursunda

“Sertifikatlaşdırılmış Etik Haker” (Certified Ethical Hacker, CEH) sertifikat imtahanında əhatə olunan modullar nəzərə alınıb.

II. HAKERLƏRİN TİPLƏRİ

Hakerlərə bağlı cəmiyyətdə belə bir stereotip vardır ki, onlar neqativ, kriminal, etik olmayan əməllər törədirlər. Halbuki, hakerlər yerinə yetirdiyi fəaliyyətlərinə görə bir neçə qruplara bölünür, həvəskar orta məktəb şagirdindən zərərli kriminalistlərə qədər bütün növ yaş kateqoriyalarından olan insanların həyatına nüfuz edə bilər [5].

A. Ağ şlyapalı hakerlər. Təhlükəsizlik mütəxəssisi və ya tədqiqatçısı kimi də tanınan etik hakerlərdir. Belə hakerlərə şirkətin bir işçisi kimi fəaliyyət göstərərək, boşluqları istismar etməyə icazə verilir [6, 7]. Çünki, bu şəxslər nüfuzetmə testlərini reallaşdırmağa qabil olan, adətən Elektron Ticarət Məsləhətçilərinin Beynəlxalq Şurası (The International Council of Electronic Commerce Consultants, EC-Council) tərəfindən lisenziyalasdırılmış hakerlərdir. Belə hakerlərin qarşısında duran vəzifələrdən biri öz bilik və bacarıqlarını digər şəxslərə təhlükəsizliyi təmin etmək baxımından yalnız fayda vermək yolu ilə istifadə etməkdir [5, 8].

B. Qara şlyapalı hakerlər. Təhlükəsizlik üzrə öz yüksək bilik və bacarıqlarını neqativ məqsədlər üçün istifadə edən şəxslərdir və media tərəfindən sadəcə olaraq “haker” kimi də tanınırlar [8]. Fərdlər və təşkilatlar öz kritik informasiya aktivlərini, kompüterlərini belə növ hakerlərdən qorumaq üçün səfərbər olunmuşdur.

C. Boz şlyapalı hakerlər. Boz şlyapalı haker kompüter hakeri və ya kompüter üzrə təhlükəsizlik ekspertidir. O, bəzən qanunları və etik standartları pozur, lakin, onun məqsədi qara şlyapalı haker kimi zərərli yox, yalnız əyləncə xarakteri daşıya bilər [8]. Boz şlyapalı hakerlər daha çox ağ şlyapalı hakerlərə oxşayırlar. Fərq ondan ibarətdir ki, boz şlyapalı hakerlər sistem və ya şəbəkəni icazəsiz sındıraraq, şirkət rəhbərliyinə boşluğun necə istismar edildiyini deyil, yalnız müəyyən məbləğ qarşılığında onun necə aradan qaldırılmasını təklif edir. Onlar seçdiyi istiqamətin qanuni və ya qanunsuz olduğunu dərk edir, lakin çox vaxt neqativ istiqamətdə fəaliyyət göstərməyi üstün tuturlar [9].

III. ETİK HAKİNG METODLARI KURSUNUN TƏLƏBLƏRİ

A. Kursun məzmunu. Müvafiq ixtisas üzrə təhsil alan magistrantlar kiber-hücum üçün zəruri informasiyanı

toplanması, şəbəkənin daranması və resursların inventarlaşdırılması, şəbəkə protokolları, əməliyyat sistemləri və tətbiqi proqramlarda boşluqların analizi, əməliyyat sistemlərinin hakinqi, zərərli proqramların analizi, veb-serverlərin və simsiz şəbəkələrin sındırılması, informasiya təhlükəsizliyi vasitələrindən yayınma üsulları, nüfuzetmə testləri, DoS hücumları və SQL-inyeksiya hücumlarının həyata keçirilməsi, seansların ələ keçirilməsi və s. kimi mövzuları nəzəri cəhətdən öyrənir və xüsusi (təcrid olunmuş) laboratoriya mühitində etik hakinq üsulları üzrə praktiki məsələləri yerinə yetirir [10,11].

B. Fiziki tələblər. Kursa hazırlıq üçün tələb olunan əsas fiziki hazırlıq müddəalarına aşağıdakıları misal göstərmək olar:

- kurs üzvlərinin hər birinin yüksək məhsuldarlığa malik kompüterlə təchiz olunması və yüksək sürətli internetə çıxışının təmin edilməsi;
- kompüterlərdə virtual maşın mühitində “Kali Linux” əməliyyat sisteminin quraşdırılması;
- onlayn rejimdə hakinq bacarıqlarının test edilməsi üçün xidmət göstərən veb serverin quraşdırılması və s.

Bundan başqa öyrənənlərin informasiya texnologiyaları, kompüter elmləri və digər əlaqədar ixtisaslar üzrə bakalavr və ya magistr dərəcəsinə mənsub olması və eyni zamanda, kompüter şəbəkələri, kompüter və onun periferik qurğuları, proqramlaşdırma biliklərinə mənsub olması, proqram təminatından düzgün istifadə siyasətinə riayət etmək kimi etik tələblər də mövcuddur.

Bütün nüfuzetmə test fəaliyyətlərinin avtorizə edilmiş rejimdə və qanun çərçivəsində yerinə yetirildiyindən əmin olmaq, zərərli hakerlərlə əlaqədə olmamaq və hər hansı zərərli fəaliyyət göstərməmək kimi tələblər irəli sürülür.

Əlavə olaraq, kibertəhlükəsizlik üzrə lokal və ya beynəlxalq yarışların keçirilməsi tələbələrə bir-biri ilə və təşkilatın mütəxəssisləri ilə sosial əlaqələrinin genişləndirilməsi, onların davranışının müsbət istiqamətdə yönəlməsi, qara şlyapalı hakerlərin neqativ cəhətləri və etik hakerlərin vacibliyini görmək üçün olduqca faydalıdır [12]. Belə yarışmalardan biri etik hakinqdə ən geniş yayılmış tədbir olan “Bayrağı ələ keçir!” (Capture the Flag, CTF) adı altında təşkil olunan yarışlardır. Burada iştirakçılar əvvəlcədən təyin olunmuş kiçik tapşırıqları yerinə yetirərək müxtəlif səviyyələrdə qiymətləndirmə üçün istifadə olunan bayraqları əldə etməlidirlər [13].

IV. ETİK HAKİNG METODLARININ TƏDRİSİ İLƏ BAĞLI ETİK VƏ HÜQUQİ MƏSƏLƏLƏR

Etik hakinq metodlarının tədrisi ilə bağlı müəyyən etik və hüquqi məsələlər də meydana çıxır [2, 14]. Bəzi təhsilənlərin öyrəndikləri hücum metodlarını və alətlərini məsuliyyətsiz şəkildə tətbiq edə biləcəyi ehtimalını nəzərə almaq zəruridir. Etik hakinq kurslarının iştirakçıları arasında keçirilən rəy sorğuları da bu ehtimalı təsdiqləyir.

Etik hakinq üsullarının öyrədilməsinə görə təşkilatların və pedaqoqların məsuliyyətini azaltmaq üçün bir sıra addımlar atılmalıdır. Əslində, etik davranış məsələsi informasiya

təhlükəsizliyi üzrə hər bir tədris proqramının məcburi hissəsi olmalıdır. Etik hakinq metodları tədris edilən hər bir kursda hüquqi nəticələr və etik məsələlər müzakirə edilməlidir. Tələbələr anlamalıdırlar ki, hücum metodlarının öyrədilməsinin məqsədi kiber hücumların necə işlədiyini aydın başa düşməklə müdafiə metodlarını təkmilləşdirmək və müvafiq təhlükəsizlik həllərini tətbiq etməkdir.

Etik hakinq kursunu öyrənənlərin davranış kodeksini imzalaması nəzərdə tutulmalıdır. Həmin davranış kodeksində hər bir magistranın davranış sərhədləri göstərilir və yolverilməz hərəkətlərin hüquqi nəticələri şərh olunur.

EC-Council tərəfindən hakerlər üçün davranış kodeksi hazırlanmışdır. Orada göstərilən müddəaların bəzisi aşağıda öz əksini tapmışdır [15]:

- İş mühitində əldə edilən fərdi məlumatları gizli və konfidensial saxlamaq (xüsusilə bu informasiya müştərilərə və onların şəxsi məlumatlarına aiddirsə), heç bir fərdi məlumatı (ad, elektron poçt ünvanı, sosial təhlükəsizlik nömrəsi, şəxsiyyət vəsiqəsinin nömrəsi və ya FİN kodu və digər unikal identifikasiya nömrəsi kimi məlumatları) müştərinin ilkin razılığı olmadan toplamaq, üçüncü tərəflə paylaşmamaq;
- başqalarının əqli mülkiyyət hüququnu pozmamaq;
- hər hansı bir elektron ticarət müştərilərinə, internet cəmiyyətinin üzvlərinə olan mümkün potensial təhlükə barədə uyğun şəxslərə və ya aidiyyəti orqanlara məlumat vermək;
- qeyri-qanuni və ya qeyri-etik yolla əldə edilmiş proqram və ya proseslərdən bilərəkdən istifadə etməmək;
- aldadıcı maliyyə əməliyyatları (rüşvət, ikiqat faktura və digər) ilə məşğul olmamaq;
- kompüter şəbəkələrini təhlükə altına salmağa yönəlmiş qara şlyapalı hakerlər cəmiyyətində iştirak etməmək [15];

V. ETİK HAKİNG METODLARININ TƏDRİSİ ZAMANI MEYDANA ÇIXAN PROBLEMLƏR

Etik hakinq metodlarının tədrisi ilə bağlı iki mühüm risklərin meydana gəldiyini vurğulamaq vacibdir. Birincisi, tələbələr kurs ərzində öyrəndiyi bilik və bacarıqlardan sui-istifadə edərək cəmiyyət üçün risk rolunu oynaya bilər. Bu isə onların gələcəkdə qara şlyapalı hakerə çevrilməsinə şərait yarada bilər. Başqa bir risk isə tədris kursu ərzində müəllimlə birlikdə yerinə yetirilmiş qeyri-qanuni fəaliyyətin tələbələr üçün risk yarada bilməyidir.

Etik hakinq metodlarının tədris edilmiş mühitdə test edilməsi nəticəsiz qala bilər. Belə ki, qara şlyapalı hakerlər sistemi istismar etməzdən öncə boşluqları tapmalıdır. Bunun üçün onlardan kifayət qədər vaxt və səbr tələb olunur. Lakin, məhdud zaman çərçivəsində tələbələrdən bunu tələb etmək mümkünsüz görünür.

Təcrid edilmiş laboratoriya mühitində aparılan laboratoriya işləri üçün etik hakinq üsullarının icra edilməsi proseslərini hər hansı kompüter sisteminə zərər vurmada təsvir edən öyrədici

xarakterli informasiya resuslarının qıtlığı mövcuddur [2, 4]. Buna görə də nəzəri hissəyə nisbətən tələbələrin hakinq üsullarını daha aydın təsəvvür etməsi üçün praktiki bacarıqların inkişaf etdirilməsində problemlər yaşanmaqdadır [16].

VI. ƏLAQƏDAR İŞLƏRİN İCMALI

[1]-də beynəlxalq təşkilatların və inkişaf etmiş bir sıra ölkələrin kibertəhlükəsizlik ixtisası üzrə bakalavr və magistr səviyyələrində ali təhsil standartları və qabaqcıl universitetlərin informasiya təhlükəsizliyi sahəsində təhsil proqramları analiz edilmişdir.

İnformasiya texnologiyalarının, eləcə də hakerlərin çevik surətdə inkişaf etməsi informasiya təhlükəsizliyinin təmin edilməsi istiqamətində mühüm addımlar atmağa vadar edir. Etik hakinq və ya nüfuzetmə testlərinin bir alət kimi istifadəsi təhlükəsizlik risklərini azaltmağa yardımçı olur. Lakin zərərli hakerlər əleyhinə belə üsulların bir çox menecerlər tərəfindən yayılmış dezinformasiya səbəbindən reallaşdırılmasından imtina edilir. [17]-də Malayziyadakı ali təhsil institutlarında haker qurbanlarının sayı analiz edilmiş, nüfuzetmə testlərinin İT təhlükəsizlik komponentinə çevrilməsinin vacibliyi, təhlükəsizlik menecerlərinə mövcud təhlükəsizlik mühiti üzərində nüfuzetmə testlərinin üstünlüyü tədqiq edilmişdir.

[16]-da ali məktəb tələbələrinə keçirilən kibertəhlükəsizlik üzrə təlimə mövcud yanaşmalar, onların üstün və çatışmayan cəhətləri, öyrətmə prosesi, müxtəlif növ laboratoriyalar və onların qurulması üçün tələblər, maarifləndirici oyunlar və yarışlar analiz edilmişdir.

NƏTİCƏ

Etik hakinq genişlənməkdə olan kibercinayətkarlardan və ya onların qruplaşmalarından kritik informasiya aktivlərini qorumaq üçün biznes və akademik təşkilatların ən vacib informasiya təhlükəsizliyi strategiyasına və alətinə çevrilməlidir. Çünki, etik hakerlərlə qara şlyapalı hakerlər arasındakı mübarizənin sona çatmayacağı proqnoz edilir.

Etik hakinq kursunun tədrisi öyrədilən bacarıqların zərərverici gücü və tələbələr üzərindəki neqativ təsirin azadılması məqsədilə öyrədənərdən ciddi məsuliyyət tələb edildiyi aydın hiss olunur.

İSTİNADLAR

- [1] Y. İmamverdiyev “Ali məktəblərdə kibertəhlükəsizlik üzrə mütəxəssis hazırlığı problemləri,” İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri IV respublika konfransı, s. 79–82, 2018.
- [2] Z. Trabelsi, W. Ibrahim, “Teaching ethical hacking in information security curriculum: A case study,” IEEE Global Engineering Education Conference (EDUCON), pp. 130-137, 2013.
- [3] B. Abu-Shaqra, R. Luppici, “A technoethical study of ethical hacking communication and management within a Canadian University,” The Changing Scope of Technoethics in Contemporary Society, pp. 307-326, 2018.

- [4] Y. Younis, K. Kifayat, L. Topham, et al., “Teaching Ethical Hacking: Evaluating Students’ Levels of Achievements and Motivations”, International Conference on Technical Sciences (ICST2019), pp. 554-559, 2019.
- [5] B. Pashel, “Teaching students to hack: Ethical implications in teaching students to hack at the university level”, InfoSecCD Conference, pp.197-200, 2006.
- [6] H. J. Kam, P. Menard, D. Ormond, P. Katerattanakul, “Ethical hacking: Addressing the critical shortage of cybersecurity talent,” PACIS, pp. 1-8, 2018.
- [7] S. Patil, A. Jangra, M. Bhale et al., “Ethical hacking: The need for cyber security”, IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPSCI), pp. 1602-1606, 2017.
- [8] A. S. Panimalar, P. Priyadharshini, R. Vijayabharathi, et al., “An overview of ethical hacking,” International Research Journal of Engineering and Technology (IRJET), vol. 5, pp.206-209, 2018.
- [9] B. Sahare, A. Naik, S. Khandey, “Study of ethical hacking,” International Journal of Computer Science Trends and Technology (IJCSST), vol. 2, pp. 6-10, 2014.
- [10] R. Messier, “CEH v10 Certified Ethical Hacker Study Guide. 1st Edition”, Sybex, 2019, 592 p.
- [11] S. Sinha, “Beginning ethical hacking with Kali Linux computational techniques for resolving security issues”, Apress, 2018, 440 p.
- [12] R.E. Pike, “The “ethics” of teaching ethical hacking”, Journal of International Technology and Information Management, vol. 22, pp. 67-75, 2013.
- [13] M. Lehrfeld, P. Guest, “Building an ethical hacking site for learning and student engagement”, SoutheastCon, pp. 1-6, 2016.
- [14] A. M. Curbelo, A. Cruz, “Faculty attitudes toward teaching ethical hacking to computer and information systems undergraduates students”, Proceedings of the Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology, pp. 1-8, 2013.
- [15] “Code of ethics”, <https://www.ecccouncil.org/code-of-ethics/>
- [16] L. Topham, K. Kifayat, Y. Younis, et al., “Cyber security teaching and learning laboratories: A survey”, Information & Security, vol.35, pp. 51-80, 2016.
- [17] C. Kang, P. JosephNg, K. İssa, “A study on integrating penetration testing into the information security framework for Malaysian higher education institutions”, International Symposium on Mathematical Sciences and Computing Research (ISMSC), pp. 156-161, 2015.

ABOUT TEACHING ETHICAL HACKING METHODS

Yadigar Imamverdiyev¹, Elshan Baghirov²

^{1,2}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹yadigar@iit.science.az, ²elsenbagirov1995@gmail.com

Abstract— Ethical hacking is the process of finding vulnerabilities, weaknesses, and bugs through the system or computer networks. In this work, the importance of an ethical hacking course is investigated for high school students and the problems during the course of teaching. In addition, the student code of ethics, the content of course, and a number of ethical and legal issues related to the course teaching were explored.

Keywords— *ethical hacking; information security; hacker; teaching course; code of ethics; cybersecurity*

SDN texnologiyasının səviyyələrində təhlükəsizlik məsələləri və həlli yolları

Orxan Mənsimzadə

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
orxan@it.science.az

Xülasə— Proqramla idarə olunan şəbəkə texnologiyası (SDN – Software Defined Network) şəbəkə proqram təminatı olaraq gələcək şəbəkə arxitekturasını ənənəvi şəbəkələrdə tətbiq edir, SDN şəbəkə idarəçiliyi üçün sadəlik, proqramlaşdırma və elastiklik baxımından perspektiv imkanlar yaradır. SDN texnologiyasını tətbiq edərkən öndə duran ən vacib məsələlərdən biri də təhlükəsizlik. Məqalədə OpenFlow əsasında qurulan SDN texnologiyasının təhlükəsizlik məsələləri və həlli yolları haqqında məlumat verilmişdir. SDN texnologiyası əsasında qurulan şəbəkəyə edilən hücumlar və bu hücumlardan müdafiə olunmaq üçün tətbiq olunan üsullar təhlil edilmişdir.

Açar sözlər— SDN; OpenFlow; DoS; şəbəkə;

I. GİRİŞ

Rəqəmsal cəmiyyət böyüdükcə internetin əhatə dairəsi genişlənir və istifadəçilər hər tərəfdən məlumatları rahat əldə edə bilərlər. İstifadəçilərin şəbəkə xidmətlərində tələbatının artması şəbəkəni qurmaq və idarə etməkdə çətinliklər yaradır. Proqramla idarə olunan şəbəkə (SDN) texnologiyası, şəbəkəyə nəzarəti asanlaşdırmaq və mərkəzdən şəbəkəni idarə etmək və şəbəkəni proqramlaşdırmaqla şəbəkənin genişlənməsinə imkan verir. Proqramla idarə olunan şəbəkə arxitekturası çox sayda marşrutlayıcı, kommutatorlar, və müxtəlif növ şəbəkə qurğuları ilə mərkəzləşdirilmiş idarəedici altında işləyən bir şəbəkələrarası ekran kimi qurulmuşdur və bunları idarə etmək üçün istifadə olunan çox sayda mürəkkəb protokollar mövcuddur. Proqramla idarə olunan şəbəkə texnologiyası şəbəkə funksiyasını virtualaşdırmaq üçün ən yaxşı texnologiya hesab edilən yeni və inqilabi şəbəkə arxitekturasına malikdir. SDN şəbəkəyə nəzarəti idarəetmə səviyyəsi və verilənlərin ötürülməsi səviyyəsinə bölməklə şəbəkədə yüksək çevikliyə malik şəbəkə idarəetməsinin sadələşdirilməsi və təkmilləşdirilməsi üçün nəzərdə tutulmuş bir texnologiyadır. Əsas məqsəd kompleks idarəetmə məntiqini bütün şəbəkə modellərindən ləğv etmək və paket ötürülməsinə nəzarət etmək üçün məntiqi nəzarət mərkəzi təşkil etməkdir. Bu, mövcud şəbəkə texnologiyasını dəyişdirmədən tətbiqi proqramlar vasitəsilə bütün şəbəkə trafikini sərbəst şəkildə idarə etmək məqsədi daşıyır. OpenFlow SDN-də idarəetmə səviyyəsi və verilənlərin ötürülməsi səviyyəsi arasında əlaqəni təmin edən bir protokoldur. OpenFlow idarəedici, kommutator və bir-biri ilə bağlı olan kanalda tətbiq olunur. OpenFlow əsasında qurulan SDN-də şəbəkəyə olan hücumların qarşısının alınması

üçün təhlükəsizliyə daha çox önəm verilməlidir. Verilənlərin ötürülməsi səviyyəsi SDN arxitekturasının alt səviyyəsində yerləşir və bir-birinə qoşulan minlərlə kommutatordan ibarətdir. Bu kommutatorların əsas işi paketlərin ötürülməsidir. Bir kommutatora hücum olunarsa göndərilən paketlər düzgün ötürülmür. Kommutatorlar istifadəçilərin şəbəkəyə qoşulması üçün birbaşa giriş nöqtəsidir və bədniiyyətli giriş portuna sadəcə keçid edərək hücum edə bilərlər. Bunun üçün də kommutatorlarda təhlükəsizlik tədbirlərini gücləndirmək lazımdır. Əsas təhlükə məqamları inzibətçi və kommutator arasında verilən qaydaların dəyişdirilməsi və kommutatorlarla istifadəçilər arasında ötürülən paketlərə edilən DoS hücumlarıdır. OpenFlow idarəedici SDN arxitekturasında ən vacib protokollardan biri hesab olunur, burada OpenFlow açarlarına paket ötürmə qaydalarını yeniləmək və bütün şəbəkənin işini nəzarət etmək üçün şəbəkə vəziyyətini ələ almaq lazımdır. Məqalədə OpenFlow idarəedici əsaslı SDN-in müxtəlif təhlükəsizlik məsələləri və SDN şəbəkəsini təhdid edən problemlər nəzərdən keçirilmişdir. SDN təhlükəsizlik hücumlarını dəf etmək üçün müxtəlif üsulları təmin edən problem və problemlərin mövcud əks tədbirləri analiz edilmişdir [1–3].

II. “OPENFLOW” ƏSASINDA QURULAN SDN TEKNOLOGİYASINDA TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

OpenFlow idarəedici əsaslanan SDN-də əsasən bədniiyyətlinin SDN-nin idarəetmə səviyyəsindəki boşluqları aşkarlayıb istismar etməsi əsas təhlükəsizlik problemlərindən biridir. İdarəedici gələn şəbəkə paketlərinin axınlarına nəzarət etməkdə məsul olduğundan o, çoxsaylı hücumların əsas hədəfinə çevrilir.

A. “Daşqın” və “Xidmətdən imtina” hücumları. Nəzarətçinin əsas vəzifəsi daşqın və xidmətdən imtina hücumlarını (DoS) dəf etməkdir. SDN-də idarəetmə səviyyəsi bilinməyən (idarə edə bilmədiyi) şəbəkə paketlərini qəbul edərkən axın qaydalarını təmin etmək üçün ötürücü səviyyəsindən sorğu almaq məcburiyyətindədir. Bədniiyyətli bir nəzarətçini sıradan çıxarmaq üçün DoS hücumu və ya başqa bir vasitə tətbiq edə bilər. Məsələn, bədniiyyətli nəzarətçinin işini yavaşlatmaq üçün onun üzərində bəzi resurs tükətmə metodlarını tətbiq edə bilər. Beləliklə nəzarətçi cavab gələn paketlərə qarşı yavaş işləyəcək və xidmətdən imtina edəcək.

SDN şəbəkəsində DoS hücumlarının qarşısının alınması üçün 2 prinsip irəli sürülür:

- Verilmiş bir şəbəkənin SDN OpenFlow açarlarını istifadə etdiyini araşdırmalı;
- Resurs tükətmə hücumunu həyata keçirməli, çünki bədniiyyətli şəbəkənin əvvəlcədən nəzərdə tutulmuş axın qaydalarının vəziyyətini bilir.

B. Host oğurlanma hücumu (Host hijacking attack). Host oğurlanma hücumu Host İzləmə Xidməti (Host Tracking Service, HTS) OpenFlow şəbəkəsində istifadə edən bir hücumdur. Host İzləmə Xidməti şəbəkənin geniş görünüşündə və SDN nəzarətçisində istifadə olunan vacib bir xidmətdir. Şəbəkədə HTS ilə bağlı əsas məsələ, ev sahibi kimi davranması və DoS hücumu nəticəsində şəbəkənin işini pozmaqdır. Bədniiyyətli nəzarətçinin bütün şəbəkə məlumatlarının idarə edilməsindən xəbərdardır. Buna görə də şəbəkə haqqında bütün məlumatları əldə etmək və SDN fəaliyyətini yavaşladacaq kritik məlumat və konfigurasiyaları dəyişdirmək üçün dərəcəli sistemindən uğurla keçsə parol və rabitə məlumatları kimi kritik məlumatları idarə edə, dəyişdirə bilər və ya trafikə istənilən yerə yönləndirə bilər. Bu vəziyyətdə OpenFlow şəbəkəsinə hücum edən bədniiyyətli üçün məlumatları əldə etmək daha asan olacaq. Bu təhlükənin qarşısının alınmasında istifadəçinin fərdi məlumatlarının OpenFlow nəzarətçisində gizlətmək üçün “Host location hacking attack” tətbiqindən istifadə etmək mümkündür.

Aldatma hücumu: Bədniiyyətli aldatma hücumundan istifadə edərək nəzarətçini təqlid edə bilər. Bu hücum uğurlu olarsa, bədniiyyətli SDN şəbəkə komponentlərində axın cədvəlinin girişlərini yarada və yeniləyə bilər. Şəbəkə mütəxəssisləri idarəedicidə bu axınlar barədə heç bir məlumat əldə edə bilməzlər. Beləliklə, təcavüzkar şəbəkəni tamamilə idarə etmək hüququna yiyələnir [4–7].

III. SDN TEXNOLOGİYASINDA TƏHDİDLƏRDƏN QORUNMA ÜSULLARIN TƏHLİLİ

OpenFlow nəzarətçisinə əsaslanan SDN-in müxtəlif təhdidlərdən qorumaq üçün və hücumların qarşısının alınması üçün bir çox yanaşma və tədqiqatlar aparılmışdır.

Hiper axını (Hyperflow): Şəbəkənin genişlənməsinə imkan yaradır və şəbəkənin mərkəzi nəzarət sistemini qoruyur. Hiper axını tətbiqi OpenFlow idarəedicisində işləyir və idarəedicinin vəziyyətinə təsir edən əməliyyatlar apararaq bütün şəbəkənin görünüşünü sinxronizasiya edir. Hiper axını fərqli idarəedicilərdə qərar qəbul etmə icazəsini ləğv edir. Beləliklə, verilənlərin ötürülməsi səviyyəsinin sorğusuna cavab müddəti idarəetmə səviyyəsi tərəfindən minimuma endirilir. Ayrıca özü-özünü idarə edən OpenFlow şəbəkələri arasındakı əlaqə yaratmağa imkan verir və bu OpenFlow şəbəkə sistemlərində mövcud olmayan bir xarakterdir. Bu idarəetmə qurğusunun DoS hücumlarından qorunmasını təmin edir. DoS hücumu, idarəedicinin əməliyyatlarını asanlıqla idarə edən və MAC cədvəllərinin dolmasına imkan verən bir hücum kimi də tanınır.

SDN-Mühavizə (SDN-Guard): Yenilikçi bir üsul, şəbəkəyə zərər verə biləcək trafik axını istiqamətləndirir zərərli, trafik üçün axın qaydalarının tətbiq olunmasını uzadır və SDN idarəedicisini qoruyaraq güvənli hala gətirib çıxardır. SDN-Guard, idarəetmə səviyyəsinin genişliyinin DoS hücumu zamanı azalmasının minimuma endirməyə kömək edir. SDN idarəedicisi II hissədə danışdığımız host izləmə xidmətindəki təhdidlərdən dinamik olaraq qorunur və bu aşağıdakı üç faktordan ibarətdir:

- Port İdarəedici (Port Manager) : Trafik yaradan hostu müəyyənləşdirmək üçün məsuliyyət daşıyır. Ayrıca, MAC ünvanı ilə eyni olan host siyahısını özündə qeyd edir.
- Host sınaq (Host Probing) : ICMP tələbini təmin etməklə hostun əlçatan olub olmadığını yoxlamaq üçün məsuliyyət daşıyır.
- Host yoxlamaq (Host Checker) : Hostun köçürülməsinin mümkünlüyünün yoxlanması və ARP sorğularının qarşısını alınması.

FlowSec: SDN idarəedisinə DoS hücumların qarşısının alınması üçün FlowSec strategiyası da irəli sürülüb. FlowSec idarəedicinin ötürmə qabiliyyətinin yığılan statistikasını dinamik olaraq hesablayır. Əgər hücum aşkar edilərsə, kommutatorun ümumi statistikasına cavabdeh olan Floodlight modulundan istifadə edərək kommutatoru yavaşlamağa məcbur edir.

FloodGuard: FloodGuard iki yanaşma əsasında işləyir. Birinci yanaşma, aktiv bir axın qaydası analizatorudur. Dinamik proaktiv axın qaydaları yaratmaq və bu qaydaları verilənlərin ötürülməsi səviyyəsində kommutatora yükləməklə şəbəkə siyasətinin qorunması üçün verilmişdir. İkinci yanaşma paketin köçürülməsidir. İdarəedicinin işini davam etdirmək üçün Round-Robin alqoritmindən istifadə edərək daşqın paketlərini tutduqdan sonra OpenFlow idarəedicisinə ötürmək üçün istifadə olunur.

FlowTrApp: Data mərkəzə aşağı və yüksək dərəcəli DDos hücumunu aşkar edir və yüngülləşdirir. Gələn hücum trafikini ardıcıl axın qaydaları ilə uyğunlaşdıraraq təsnif edir.

TopoGuard: TopoGuard, şəbəkə hücumlarını üçün real vaxt rejimində aşkarlanmasını təmin edən təhlükəsizlik vasitəsidir.

SDN şəbəkəsinə olan hücumlara qarşı əks tədbirlərdən bəhs edildi. Bu əks tədbirlər tədqiqatçılar üçün ən yeni üsullar, o cümlədən quruluşlar və həllər barədə biliklərə sahib olmaq, OpenFlow idarəedicisinə əsaslanaraq SDN şəbəkəsinə olan təhdidlərə yeni əks tədbirlər hazırlamağa çalışmaq üçün daha faydalıdır. OpenFlow və SDN şəbəkə monitorinqini böyük dərəcədə asanlaşdıracağını və proqramlaşdırılmış şəbəkələri tətbiq etməklə şəbəkəyə yeniliklər qatacağını vəd edir. Beləliklə, bu, tədqiqatçılara digər təhlükəsizlik məsələlərini yüngülləşdirməyə və inkişafını asanlaşdırmağa kömək edir [8–10].

NƏTİCƏ

SDN idarəetmə və verilənlərin ötürülməsi səviyyələrinə ayrılmaqla, şəbəkə idarəçiliyini asanlaşdırır və bəzi yeni qaydalar və siyasətləri tətbiq etmək üçün xarici tətbiqetmələrdən istifadə şəbəkənin proqramla idarə olunmasını artırır. Şəbəkənin mərkəzləşdirilməsi və proqramlılığı təhlükəsizlik məsələlərinə diqqəti daha da artırır. OpenFlow SDN – də tətbiq olunan ən son protokoldur. Bu məqalədə OpenFlow idarəedici əsaslı SDN şəbəkəsinin təhlükəsizlik məsələlərinə baxdıq. SDN təhlükəsizlik hücumlarını dəf etmək üçün müxtəlif üsullardan bəhs etdik və bu üsullardan düzgün metodun seçilib tətbiq olunmasını müzakirə etdik.

İSTİNADLAR

- [1] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, “A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks”, IEEE Communications Surveys & Tutorials, Vol. 16, Issue: 3, 2014, pp. 1617-1634.
- [2] S. Sezer, B. Fraser, D. Lake, “Are We Ready for SDN? Implementation Challenges for Software-Defined Networks”, IEEE Communications Magazine, Vol. 51, Issue: 7, 2013, pp. 36-43.
- [3] Shu Z., Wan J., Di Li, “Security in Software-Defined Networking: Threats and Countermeasures”, Mobile Network and Applications, Vol. 21, No. 8, 2016, pp. 764-776.
- [4] W. Li, W. Meng, L. F. Kwok, “A Survey on OpenFlow-based Software Defined Networks: Security Challenges and Countermeasures”, Journal of Network and Computer Applications, Vol. 68, 2016, pp. 126-139.
- [5] S. Hong, L. Xu, H. Wang, G. Gu, “Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures”, In: Proceedings of NDSS, San Diego, 2015, pp. 126-139.
- [6] S. Shin, G. GU, “Attacking Software-Defined Networks: A First Feasibility Study”, In: Proceedings of the 2nd Workshop on Hot topics in Software Defined Networks (HotSDN), Hong Kong, 2013, pp. 165-166.

- [7] A. Tootoonchian, Y. Ganjali, “HyperFlow: A Distributed Control Plane for OpenFlow”, In: Proceedings of the Internet Network Management Workshop/Workshop on Research on Enterprise Networking (INM/WREN), San Jose, 2010, pp. 1-6.
- [8] L. Dridi, M. Faten Zhani, “SDN-Guard: DoS Attacks Mitigation in SDN Networks”, 5th IEEE International Conference on Cloud Networking, 2016, pp. 212-217
- [9] Tri-Hai Nguyen, M. Yoo, “Attacks on Host Tracker in SDN Controller: Investigation and Prevention”, Information and Communication Technology Convergence (ICTC), International Conference, 2016, pp. 610-612.
- [10] N. Gude, T. Koponen and J. Pettit, “NOX: Towards an Operating System for Networks”, ACM SIGCOMM Computer Communication Review archive Vol. 38 Issue 3, 2008, pp. 105-110.

SECURITY ISSUES AND SOLUTIONS AT SDN TECHNOLOGY LEVELS

Orkhan Mansimzada

Institute of Information Technology of ANAS, Baku, Azerbaijan

orxan@iit.science.az

Abstract– Software defined network technology (SDN) as a networking software implements future network architecture in traditional networks. SDN offers promising opportunities for network management in terms of simplicity, programming and flexibility. One of the most important issues facing SDN technology is security. This article provides an overview of security solutions of SDN technology and solutions which is build based on OpenFlow. Detailed information on network attacks based on SDN technology and the methods used to protect justify these attacks are provided.

Keywords– SDN, OpenFlow, network, DoS

Fərdlərin sosial münasibətlərinin gizliliyinin təmin olunması problemləri

Nigar Axundova

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
axundovanigar96@gmail.com

Xülasə— Məqalədə sosial münasibətlərin cəmiyyətdəki rolu müəyyən edilmişdir. Cəmiyyətin qiymətləndirilməsində sosial münasibətlər mühüm əhəmiyyət kəsb edir. Tədqiqatda sosial münasibətlərin analizində fərdi məlumatların rolu müəyyənləşdirilmiş və bu məlumatların təhlükəsizliyinin təmin edilməsi üsulları şərh olunmuşdur.

Açar sözlər— *sosial münasibətlər, fərdi məlumatlar, informasiya təhlükəsizliyi, link analiz.*

I. GİRİŞ

Sosial münasibətlər dedikdə sosial qruplar və ya qrup üzvləri arasında iqtisadi, hüquqi, əxlaqi, siyasi, dini, etnik və digər sahələrdə baş verən münasibətlər nəzərdə tutulur. Sosial münasibət iki və daha çox şəxsin qarşılıqlı münasibətidir. Sosial münasibətlər sosial, mədəni və s. digər təsirlər kontekstində yaranır. Bu baxımdan insanlar, ailə üzvləri, həmkarlar və təşkilatlar arasındakı əlaqələri izləyə bilirik. Sosial münasibətləri aşkarlamaq üçün birinci addım fərdi məlumatların əldə olunması və analizidir. Sosial münasibətlərin analizində istifadə olunan fərdi məlumatların təhlükəsizliyinin təmin edilməsi başlıca şərt hesab olunur.

II. SOSIAL MÜNASİBƏTLƏRİN TƏSNİFATI

Münasibətlərin öyrənilməsində ilkin şərt onların təsnifatlandırılmasıdır.

Münasibətlərin təsnifatı. Sosial münasibətlər statik və dinamik olmaqla 2 hissəyə bölünür. Statik əlaqələrə şəxsi münasibətlər (ailə münasibətləri) aid edilir. Bəzi münasibətlər isə statik deyillər, dəyişib inkişaf edə bilirlər. Belə münasibətlər dinamik münasibətlər adlanır. Bu münasibətlər qrupuna aşağıdakılar aid edilir:

- Peşəkar münasibətlər (Bərabərsəviyyəli: iş yoldaşı, qrup və ya sinif yoldaşı, həmkar; Üstsəviyyəli: müdir, direktor, nəzarətçi, müəllim, ekspert və s. Altsəviyyəli: İşçi, köməkçi, tələbə, şagird və s.
- Dostluq münasibətləri (yaxın dostlar və tanışlar)
- Qonşuluq münasibətləri,
- Gündəlik fəaliyyətlə əlaqəli münasibətlər (kurslar, idman klubları, istirahət, sağlamlıq, alış-veriş və s. ilə əlaqədar).

Bundan başqa, münasibətlər müddətinə (daimi və qısa müddətli), qanunla tənzimlənməsinə (rəsmi və ya qeyri-rəsmi), əlaqələrin gücünə (zəif və ya güclü) və digər xüsusiyyətlərinə görə təsnifatlandırıla bilər [1].

Zəif əlaqələrin gücü. Münasibətlər fərdlərin birlikdə keçirdikləri vaxt, yaxınlıq dərəcəsi və mövcud münasibətin intensivliyinə əsasən *zəif* və ya *güclü* olaraq fərqləndirilir.

Sosioloq Mark Granovetterin fikrincə, zəif əlaqələri birləşdirərək bizə maraqlı olan, lakin əldə edə bilmədiyimiz məlumatları əldə edə bilirik. Güclü əlaqələrlə bağlı problem ondan ibarətdir ki, onları qorumaq uzun vaxt və səy tələb edir. Danbar sayına əsasən, bir insan 150-dən çox sabit ictimai əlaqələri saxlaya bilməz [2]. Digər tərəfdən, zəif əlaqələri qorumaq çox böyük səy tələb etmir və biz 150-dən çox zəif əlaqələrə sahib ola bilirik. Məsələn, LinkedIn, Twitter və Facebooku göstərə bilirik. Bildiyimiz kimi, bu münasibətlərin çoxu zəif əlaqələrdir və minlərlə belə əlaqə mümkündür.

Belə ki, iki insan arasında güclü əlaqələr mövcud olduğunda, adətən onlar eyni insanları tanıyır və eyni məlumatlara sahib olurlar. Lakin biri ilə zəif əlaqələriniz olduqda siz artıq eyni məlumatlara sahib olursunuz və fərqli insanları tanıyırsınız. Beləliklə, bu əlaqələr çata bilmədiyiniz məlumata çatmaq üçün körpü funksiyasını yerinə yetirir.

Zəif əlaqələr müəssisədə əməkdaşlığın əsaslarından biridir və bu günki yeni vasitələr əməkdaşların bu əlaqələri qurmasına imkan verir [3].

III. FƏRDİ MƏLUMATLAR

Sosial münasibətləri aşkarlamaq üçün ilk növbədə fərdlərin məlumatları əldə olunmalı və analizi aparılmalıdır. Fərdi məlumat dedikdə, hər hansı fiziki şəxsə (məlumat subyekti) aid məlumatlar başa düşülür. Fərdi məlumatlara yalnız şəxsin adı, soyadı, doğum yeri və doğum tarixi, şəxsiyyət vəsiqəsinin nömrəsi, yerləşmə məlumatları (ing. location data) və s. kimi dəqiq məlumatlar deyil, eyni zamanda fərdlərin fiziki, genetik, sosial, iqtisadi və s. xüsusiyyətlərinə aid məlumatlar da daxildir. Başqa sözlə desək, şəxsiyyət vəsiqəsi, vergi, sığorta nömrəsi, telefon nömrəsi, avtomobil nömrəsi, əmlak məlumatları, gəlir, təhsil, şəkil, video, səs yazıları, barmaq izləri, genetik məlumatlar və s. kimi şəxsi identifikasiya edə bilən bütün məlumatlar fərdi məlumatlar hesab olunur [4]. Bu məlumatları əldə etmək üçün

son illərdə daha çox sosial şəbəkə məlumatlarından istifadə olunur. Sosial şəbəkələr hər bir istifadəçinin gündəlik fəaliyyəti, davranışı, münasibətləri və s. haqqında məlumatları özündə birləşdirdiyinə görə fərdləri təmsil edən ən effektiv vasitə hesab olunur. Həç bir digər məlumat mənbələri fərdlər haqqında belə ətraflı detalları təqdim etmir. Sosial şəbəkələrin analizində ən vacib problemlərdən biri şəbəkə üzvləri arasındakı əlaqələrin müəyyən olunmasıdır [5]. Əlaqələrin müəyyən olunmasında ən çox qraflar nəzəriyyəsinə əsaslanan link analizi metodundan istifadə olunur. Link analizi şəbəkə nəzəriyyəsində şəbəkə qovşaqları arasındakı əlaqələri müəyyən etmək və qiymətləndirmək üçün istifadə olunan məlumat təhlili üsuludur [6]. Bu əlaqələr insanlar, təşkilatlar, qruplar da daxil olmaqla müxtəlif növ obyektlər (qovşaqlar) arasında ola bilər. Link analizi cinayət fəaliyyətinin araşdırılması (fırıldaqçılığın aşkarlanması, terrorizmə qarşı mübarizə və kəşfiyyat), informasiya təhlükəsizliyinin analizi, axtarışların optimallaşdırılması, marketinq tədqiqatları, tibbi tədqiqatlar və s. sahələrdə istifadə olunmaqdadır. Bu metod xüsusən veb əlaqələri, insanlar və təşkilatlar arasındakı əlaqələri vizuallaşdıraraq analiz olunmasını asanlaşdırır. Burada əsas məqsəd icmaların aşkarlanması, nüfuzlu aktorların müəyyən edilməsidir [7].

IV. FƏRDİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİ

Fərdi məlumatları istifadə edərkən onların təhlükəsizliyinin təmin edilməsi başlıca şərtidir. Bu səbəbdən, dövlətlər, təşkilatlar öz məlumat aktivlərinin onlar üçün dəyəri olan fərdi məlumatlarının qorunmasını təmin etməlidirlər. Bu isə informasiya təhlükəsizliyinə aid xüsusi bir sahədir. İnformasiya təhlükəsizliyinə fərdi, konfidensial və həssas məlumatların çap, elektron və s. digər formasına icazəsiz giriş, istifadə, yayılması, sui-istifadə, məhv edilmə, dəyişdirilmə və ya pozulmadan qorunma yol və vasitələri aid edilir. İnformasiya təhlükəsizliyini təmin etmək informasiya texnologiyalarının inkişafı səbəbindən olduqca çətinləşir. Təhlükəsizliyi təmin etmək üçün əvvəlcə fərdi məlumatların emalının təhlükəsizlik risklərini qiymətləndirən risk idarəetmə prosesi həyata keçirilir. Daha sonra müəyyən edilmiş riskləri aradan qaldırmaq üçün təhlükəsizlik tədbirləri işlənir. Bu tədbirlər təşkilatı (məs., siyasət, prosedür) və texniki (məs., antivirus proqramlarının tətbiqi, ehtiyat sənədlərinin yaradılması və s.) tədbirlərə ayrılır. Məlumatların təhlükəsizliyinin təmin edilməsi üçün ilk növbədə məlumatın dəyərini müəyyən etmək lazım gəlir. Bütün məlumatlar bərabər deyil və buna görə də onların hamısı eyni dərəcədə qorunma tələb etmir. Bunun üçün ilk növbədə məlumatların təsnif olunması tələb olunur. Məlumatlar ictimai, daxili, konfidensial və məhdud (məs., PHI – protected health information) olmaqla üç sinifdə təsnifatlandırılır. İctimai məlumatlar geniş kütləyə açıqlanmaq üçün nəzərdə tutulmuş məlumatlardır. Bu məlumatlara misal olaraq ümumi faydalı məlumatlar, xəbərlər, tədqiqat nəticələri, press-relizlər və digər oxşar məlumatlar göstərmə bilərik. Daxili məlumatlar ictimaiyyətə açıqlanmayan, hər hansı təşkilatın daxili məlumatlarıdır. Bu siyahıya işçilərin telefon kitabçası, daxili veb sahifələr, siyasət, biznes plan və s. aiddir. Konfidensial məlumatlar həssas məlumatlar hesab olunur. Bu məlumatları yalnız səlahiyyətli şəxslərin əldə

etməsi mümkündür. Bu məlumatlara misal olaraq şəxsiyyət vəsiqəsinin nömrəsi, ünvan, bank məlumatları, biometrik məlumatları göstərmək olar. Məhdud məlumatlar isə yüksək həssaslığa malik məlumatlardır. Bu məlumatlara isə kredit kartının nömrəsi, parollar və s. kimi məlumatlar aiddir [8].

NƏTİCƏ

Tədqiqatda sosial münasibətlərin təsnifatı və analizi nəticəsində məlum olmuşdur ki, əhalinin gündən-günə atran qrupları sosial şəbəkələrdən gündəlik həyatlarında istifadə etdiklərinə görə, sosial media məlumatları bir çox fərqli sahələrdə analiz olunduğu kimi, sosial münasibətlərin analizində də istifadə oluna bilər. Bu münasibətləri aşkarlamaq üçün link analizi metodunun səmərəliliyi göstərilib. Sosial münasibətlərin analizi və təsnifatından məlum oldu ki, sosial münasibətlər fərdi məlumatlarla sıx bağlıdır. Fərdi məlumatların geniş analizini aparmaqla sosial münasibətləri müəyyən etmək mümkündür. Buna görə fərdi məlumatların təhlükəsizliyi problemi sosial münasibətlərin aşkarlanması ilə sıx bağlıdır. Odur ki, sosial münasibətlərin aşkarlanmasından danışarkən, ilk növbədə bu münasibətlərdə iştirak edən fərdlərin haqqında məlumatların toplanması və analizi əməliyyatları yerinə yetirilməlidir. Bu əməliyyatlarda isə fərdi məlumatların təhlükəsizliyi məsələləri öndə durur.

İSTİNADLAR

- [1] E. Berscheid “The greening of relationship science,” *American Psychologist*, 1999, 54(4), pp.260–266.
- [2] R. I. Dunbar “How many friends does one person need: Dunbars number and other evolutionary quirks,” 2010, Fader and Fader limited, 302 p.
- [3] M. Granovetter “The strength of weak ties,” *American Journal of Sociology*, 1973, vol. 78, pp. 1360–1380.
- [4] M. Bakhroum, B. C. Gallego, M.-O. Mackenrodt, G. Surblytė-Namavičienė (Eds.) “Personal data in competition, consumer protection and intellectual property law.” Springer, 2018.
- [5] A. Perer, I. Guy, E. Uziel, I. Ronen, M. Jacovi “Visual social network analytics for relationship discovery in the enterprise,” *Proceedings of the IEEE Conference on Visual Analytics Science and Technology*, 2011, pp. 71–79.
- [6] S. Shinde, A.Rajmane, “Link Analysis in Relational Databases using Data Mining Techniques,” *International Journal of Engineering And Computer Science*, 2014.
- [7] R.M. Əliquliyev, R.M. Əliquliyev, İ.Y. Ələkbərova “Elektron dövlət mühitində sosial münasibətlərin təhlükəsizliyi,” “İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri” IV respublika konfransı, 2018. s. 64-67.
- [8] Z. Skwarek, “Considerations on personal data security” *Information society*, 2016.

PROBLEMS OF ENSURING CONFIDENTIALITY OF SOCIAL RELATIONS OF INDIVIDUALS

Nigar Axundova

Institute of Information Technology of ANAS, Baku, Azerbaijan
axundovanigar96@gmail.com

Abstract – The article outlines the role of social relations in society. Social relations play an important role in the evaluation of society. The study identified the role of personal data in the analysis of social relationships and explained the ways in which these data can be protected.

Keywords – social relations, personal data, information security, link analysis.

Fərdi məlumatların təhlükəsizliyinin təminatı üçün müasir metodlar

Aytən İsmayılqızı

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
aytan.ismayil@gmail.com

Xülasə— Sosial qarşılıqlı münasibətlər getdikcə daha çox şəbəkə üzərindən yaradılır – sosial platformalarda yaranmış yeni imkanlar, süni intellektin tətbiqinə əsaslanan sistemlər, eyni zamanda fərdi məlumatların gizliliyi üçün yeni risklər yaradır. Bu baxımdan fərdi məlumatların təhlükəsizliyi prioritet məsələ olaraq qalır. Məqalədə fərdi məlumatların təhlükəsizliyinin təminatı üçün istifadə olunan bəzi müasir metodlar araşdırılmış və onların üstün və mənfi cəhətləri analiz edilmişdir.

Açar sözlər— fərdi məlumatlar, məlumatların təhlükəsizliyi, süni intellekt, machine learning, privacy preserving machine learning

I. GİRİŞ

Fərdi məlumatlar – şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumatlardır [1]. Təhlükəsizlik hər zaman fərdi məlumatların konfidensiallığının, tamlığının, əylətliliyinin qorunması üçün diqqət mərkəzində olmuşdur. Demək olar ki, həyatımızın hər bir hissəsi məlumat ətrafında fəaliyyət göstərir. Sosial media şirkətlərindən tutmuş, banklara, satıcılara, hökumətə qədər – demək olar ki, istifadə etdiyimiz hər bir xidmət şəxsi məlumatların toplanması və təhlilini əhatə edir. Adımız, ünvanımız, bank nömrəmiz və başqa şəxsi məlumatlarımız şirkətlər tərəfindən toplanılır və analiz edilir. Belə şəraitdə fərdi məlumatların qorunmasının vacibliyi artır. Təqdim olunan iş bu sahədə tədqiqat məsələlərini dəqiqləşdirmək məqsədilə fərdi məlumatların təhlükəsizliyini təmin etmək üçün yeni metodların analizinə həsr olunmuşdur.

II. GDPR-İN TƏMƏL PRİNSİPLƏRİ

İnternet və mobil tətbiqlərin, süni intellektin və “Əşyaların İnterneti”nin (Internet of Things) inkişafı ilə yeni yaranmış sistem zəifliklərini və kiberhücum risklərini nəzərə alaraq fərdi məlumatların təhlükəsizliyinə ehtiyac hər zamankından daha çoxdur. Fərdi məlumatların qorunması üçün ilk növbədə hüquqi təminat lazımdır [2]. GDPR – General Data Protection Regulation (Verilənlərin Qorunması üzrə Əsas Qanun) Avropanın rəqəmsal konfidensiallıq qanunvericiliyinin əsaslarını təşkil edir. 2012-ci ilin yanvar ayında Avropa Komissiyası Avropanı “rəqəmsal əsrə uyğun” etmək üçün Avropa Birliyi daxilində məlumatların qorunması islahatları planlarını hazırladı. 4 ildən sonra bunun nəyə və necə tətbiq olunacağına dair razılıq əldə edildi. GDPR Avropa Birliyi vətəndaşlarına öz fərdi məlumatlara daha çox nəzarət etmək üçün hazırlanmış yeni qaydalar toplusudur. O, həm Avropa

Birliyi daxilindəki vətəndaşlar, həm də müəssisələrin rəqəmsal iqtisadiyyatdan tam faydalana bilməsi üçün tənzimlənmə mühitini asanlaşdırmaq məqsədi daşıyır. İslahatlar hazırda yaşadığımız dünyanı əks etdirmək üçün hazırlanmışdır və İnternet əlaqəli bağlantıları sürətləndirmək üçün Avropa daxilindəki fərdi məlumatlar üzərinə konfidensiallıq və razılıq əhatəsində qanunlar və öhdəliklər gətirir.

GDPR-ə görə Avropa Birliyi vətəndaşlarının fərdi məlumatlarının emalı ilə məşğul olan bütün təşkilatlar aşağıdakı razılaşmalara əməl etməlidir [3]:

1. Təşkilat fərdi məlumatları toplayarkən toplanmış məlumatların harada istifadə olunacağını bildirməlidir. Məlumatlar üçüncü tərəflərlə bölüşdürülməsini ehtiva edən başqa bir məqsəd üçün istifadə edilə bilməz.
2. Layihə və ya proses üçün yalnız minimum miqdarda məlumat toplamaq lazımdır. Məlumat yalnız məhdud müddətdə saxlanılmalıdır.
3. Təşkilat şəxslərə özləri haqqında hansı məlumatların olduğunu və bununla əlaqədar nələr edildiyini izah etməlidir.
4. Təşkilat tələb olunduğu zaman şəxsin fərdi məlumatlarını dəyişdirməli və ya ləğv etməlidir.
5. Fərdi məlumatlar insanlar haqqında avtomatlaşdırılmış qərarlar üçün istifadə edildikdə, təşkilat qərar qəbul etmə prosesinin arxasındakı məntiqi izah etməlidir.

III. BƏZİ METODLAR HAQQINDA

GDPR fərdi məlumatların təhlükəsizliyinin təminatı üçün 6 effektiv metod təklif etmişdir:

1. Riskin qiymətləndirilməsi
2. Ehtiyat nüsxələr (ing. Backups)
3. Şifrələmə
4. Psevdonimləşdirmə
5. Giriş nəzarət
6. Məhv etmə (ing. Destruction)

1. Riskin qiymətləndirilməsi – Məlumatlar nə qədər həssas olarsa, o qədər ciddi mühafizə edilməlidir. Təhlükə riski az olan informasiya daha az qorunma tələb edir. Bu baxımdan riskin qiymətləndirilməsi önəmlidir, çünki güclü mühafizə daha çox xərc tələb edir. Riskin qiymətləndirilməsində 2

istiqamət oxu üzrə dəyərləndirmə aparılır: məlumat pozuntusu halında potensial təhlükə və pozuntu ehtimalı. Bu oxlar üzrə risk nə qədər yüksək olarsa, məlumat o qədər həssas sayılır [4].

2. Ehtiyat nüsxələr – Ehtiyat nüsxələr texniki nasazlıq və ya istifadəçi ehtiyatsızlığı ucbatından baş verə biləcək məlumat itkisinin qarşısını almaq üçün istifadə olunur.

3. Şifrələmə – GDPR-də şifrələmə fərdi məlumatların təhlükəsizliyini təmin etmək üçün mümkün olan bir texniki və təşkilati tədbir olaraq açıq şəkildə qeyd edilmişdir. Məlumatların emalı ilə əlaqədar risklər nə qədər yüksək olarsa, təhlükəsizlik tədbirləri daha güclü olmalı və daha çox tədbirlər görülməlidir. Yüksək əhəmiyyətli məlumatların hər addımda şifrələnməsi ilə daha yüksək təhlükəsizliyə nail olmaq olar. Ancaq GDPR sürətlə inkişaf edən texnoloji tərəqqi üçün şifrələmə üsullarını qeyd etmir [5].

4. Pseudonimləşdirmə – Şəxslərin adları təsadüfi yaradılan sözlər (sətilər) ilə əvəz edilir. Buna görə bir şəxsin şəxsiyyəti ilə verdikləri məlumatları bir-birinə bağlamaq mümkün olmur. İnsanları təxəllüs məlumatlarından birbaşa tanıya bilmədikləri üçün məlumatların pozulması və ya itkisi halında prosedurlar daha sadədir və risklər azaldılır.

Təxəllüs nümunəsi kimi bir kompüter sistemində adlar, ünvanlar və doğum tarixləri kimi şəxsiyyəti müəyyənləşdirən məlumatların məlumat bazasının saxlanılmasını misal göstərə bilərik. Bu zaman ayrıca bir kompüter sistemində, onları uyğunlaşdırmaq üçün şifrəli kodlarla birlikdə, kredit tarixi, tibbi sənədlər və s. kimi fərdi məlumatlar saxlanılır.

5. Girişə nəzarət – Şirkətin məlumat axınına girişə nəzarət mexanizmlərinin tətbiqi çox səmərəli risk azaldılması metodudur. Belə ki, məlumatların miqdarı nə qədər az olarsa, məlumatların pozulması və ya itməsi riski o qədər azdır. Həssas məlumatlara giriş icazəsi yalnız daxil olmaq üçün əsaslı bir səbəbi olan etibarlı işçilərə verilməsi təmin edilməlidir. Xüsusilə, yeni işçilər işə götürüldükdən sonra mütəmadi olaraq məlumatlandırma kurslarına cəlb edilməli və sistemdə yeniləmələr yerinə yetirilməlidir.

6. Məhv etmə – Ölinizdə olan məlumatların məhv edilməsi olduğu bir vaxt gələ bilər. Məlumatların məhv edilməsi ilk baxışdan qorunma metodu kimi görünməsə də, əslində belədir. Məlumatlar bu şəkildə icazəsiz bərpa və girişlərdən qorunur. GDPR-a əsasən ehtiyacınız olmayan məlumatları silmək öhdəliyiniz var və həssas məlumatlar daha geniş məhv etmə üsullarına zəmanət verir.

IV. MAŞIN TƏLİMİ VƏ FƏRDİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİ

Axtarış sorğularımız, satınalma əməliyyatları, izlədiyimiz videolar gündəlik olaraq toplanan və saxlanan məlumatların yalnız kiçik bir hissəsidir. Bu kimi fərdi məlumatlar müxtəlif Maşın təlimi (MT, ing. Machine Learning) tətbiqlərində istifadə olunur. Belə fərdi məlumatlar mərkəzləşdirilmiş yerlərə yüklənir, onlardan maşın təlimi alqoritmləri yaradılır

və həmin alqoritmlər əsasında modellər düzəldilir [6]. Həmin fərdi məlumatlara olan təhlükələr təkcə məlumat mərkəzləri və şirkətlərə hakerlər hücum edən zaman ortaya çıxan problemlərlə məhdudlaşmır. Əlavə olaraq yaranan təhlükə ondan ibarətdir ki, MT modelləri üçün istifadə olunan fərdi məlumatlar anonim olsa da, emal zamanı müəyyən xətlər (alqoritmdeki, operatorun səhlənkarlığı və s.) nəticəsində kənara sızma bilər. Əsas məqsəd MT və fərdi məlumatların təhlükəsizliyi texnologiyaları arasındakı boşluğu doldurmaqdır [7,8]. Bunun üçün Privacy-Preserving Machine Learning (PPML, Gizliliyi qoruyan maşın təlimi) anlayışı daxil edilmişdir. PPML-ə nail olmaq üçün bir sıra üsullar mövcuddur. Bunlardan ən geniş istifadə edilənləri homomorf şifrələmə, sırr paylaşımı (ing. secret sharing), təhlükəsiz prosessorlar (ing. secure processors) hesab edilir.

Təhlükəsiz prosessorlar – Intel SGX kimi prosessorlar əvvəllər həssas kodun daha yüksək imtiyaz səviyyələrində konfidensiallığını və tamlığını təmin etmək üçün təqdim edilsə də, gizliliyin qorunması hesablamalarında da istifadə olunur [6]. Hazırda bəzi MT alqoritmləri SGX prosessorlarına əsaslanır. Əsas ideya ondan ibarətdir ki, bu sistemlərdə hər bir məlumat sahibi müstəqil olaraq anklav (kod və məlumatları saxlayan sahə) vasitəsi ilə təhlükəsiz kanal qurur, özlərini autentifikasiya edir, buluddakı MT kodunun tamlığını yoxlayır və fərdi məlumatları təhlükəsiz şəkildə anklava yükləyir. Bütün məlumatlar yükləndikdən sonra MT tapşırığı təhlükəsiz prosessor tərəfindən yerinə yetirilir və nəticələr autentifikasiya edilmiş kanallar vasitəsilə lazımi tərəflərə göndərilir.

MT həyata keçirərkən fərdi məlumatları qorumaq üçün yuxarıda göstərilən üsullara baxmayaraq, məlumatların təhlükəsizliyini təmin etməyən MT alqoritmləri hələ də mövcuddur və geniş istifadə edilir. Bu baxımdan mövcud qanunlara əsasən şirkətlər istifadəçilərə öz fərdi məlumatlarının toplanması haqqında məlumatlandırılmaq və hətta bundan imtina etmək seçimi verməlidir.

NƏTİCƏ

Dövrümüz Süni İntellekt inqilabına şahid olduğu bir zamanda fərdi məlumatların təhlükəsizliyinin təminatında ənənəvi üsullar özünü doğrultmur. İnternetin və şəbəkələrin mürəkkəbləşən, artan istifadəsi hücum edənlərin sistemdəki boşluqları istismar etmək imkanlarını artırır. Təhlükəsizlik üzrə ənənəvi qaydalara əsaslanan vasitələr bütün mümkün ola biləcək təhlükələrin öhdəsindən gəlməyə qadir deyil. Maşın təliminin tətbiqinə əsaslanan texnologiyalar yaradılarkən fərdi məlumatların təhlükəsizliyi də nəzərə alınmalı və onu pozmayan alqoritmlər və üsullar işlənəlməlidir.

İSTİNADLAR

- [1] Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu. 11 may 2010-cu il.
- [2] Y. İmamverdiyev, “Big Data və fərdi məlumatların təhlükəsizliyi,” “Big data: imkanları, multidissiplinar problemləri və perspektivləri” I respublika elmi-praktiki konfransı, s. 109-113, 2016.
- [3] <https://eugdpr.org/the-regulation/>

- [4] N. Fabiano, “Ethics and the protection of personal data,” 10th International Multi-Conference on Complexity, Informatics and Cybernetics, 2019.
- [5] C.Tikkinen-Piri, A.Rohunen, J.Markkula, “EU General Data Protection Regulation: Changes and implications for personal data collecting companies,” Computer law and security review, Vol. 34, No 1, 2018, pp. 134-153.
- [6] M. Al-Rubaie, J. M. Chang, “Privacy-preserving machine learning: Threats and solutions,” IEEE Security and Privacy, Vol. 17, No 2, 2019.
- [7] P.Mohassel, Y.Zhang, “SecureML: A system for scalable privacy-preserving machine learning,” IEEE Symposium on Security and Privacy, 2017.
- [8] B.J.Chiphers, A system for privacy-preserving machine learning on personal data. MSc dissertation, Massachusetts Institute of Technology, 2017, 86 p.

**NEW METHODS FOR PROVIDING SECURITY OF
PERSONAL DATA**

Aytan Ismayil gizi

Institute of Information Technology of ANAS, Baku, Azerbaijan

aytan.ismayil@gmail.com

Abstract— Social interactions are increasingly created over the network – with new opportunities created on social platforms, systems based on artificial intelligence also create new risks for the privacy of personal information. From this point of view, the security of personal data remains a top priority. The article explores some contemporary methods to ensure the security of personal data and analyzes their pros and cons.

Keywords— *personal data, data security, artificial intelligence, machine learning, privacy preserving machine learning*

Proqram təminatının sınağı zamanı fərdi məlumatların təhlükəsizliyinin təmin olunması problemləri

Tofiq Kazımov¹, Nəzakət Məlikova²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹tofig@mail.ru, ²naranara_68@mail.ru

Xülasə— Məqalədə proqram təminatının sınağı prosesində yarana biləcək problemlər, xüsusilə fərdi məlumatların təhlükəsizliyinin təmin olunmasında yarana biləcək çətinliklər və bununla bağlı həyata keçirilə biləcək tədbirlər öz əksini tapmışdır. Daha sonra problemlərin yaranma səbəbləri araşdırılmış, testləşmə prosesində fərdi məlumatların təhlükəsizliyinin təmin olunması yolları göstərilmiş və onların nəzərə alınmasının vacibliyi vurğulanmışdır.

Açar sözlər— proqram təminatının sınağı; məlumat təhlükəsizliyi; fərdi məlumatlar; data-masking

I. GİRİŞ

İnformasiya texnologiyaları müasir cəmiyyətin infrastrukturunun ən vacib və əvəzolunmaz elementlərindən biri sayılır. O, bəşəriyyətin sosial, mədəni inkişafı və iqtisadi fəaliyyəti üçün əsas amillərdən olmaqla, insanların müxtəlif tip məlumatlar əldə etməsini və harda olmasından asılı olmayaraq onların bir-biriylə ünsiyyət qurmasını təmin edir.

İstənilən informasiya sistemi aparat və proqram təminatından (PT) təşkil olunmuşdur. Məlumdur ki, PT-nin mürəkkəbliyi onda olan səhvlərin sayının çox olması ehtimalını da artırır. PT-də buraxılan xətlər, baş verən səhvlər, böyük fəlakətlərə, maddi ziyanlara, insanların həyatının itirilməsinə, vaxt itkisinə və müxtəlif şəbəkə infrastrukturlarının sıradan çıxmasına səbəb ola bilər.

Müasir informasiya sistemlərinin düzgünlüyünə və etibarlılığına müəyyən mənadə zamanət, təminat vermək üçün PT-nin həyat dövrünün müxtəlif mərhələlərində sınaq metodlarından istifadə etməklə onda olan səhvlər ardıcıl şəkildə aradan qaldırılır. PT-nin sınağı (software testing) – keyfiyyətə nəzarət mexanizmlərindən biri olmaqla proqramın gözlənilən və real icrası (iş) arasındakı uyğunluğu müəyyən edir və seçilmiş testlər dəsti əsasında lazımı qaydada həyata keçirilir. Proqram təminatının sınağı zamanı mümkün səhvlər, qüsurlar və xətlər aşkara çıxarılaraq aradan qaldırılır [1].

Demək olar ki, hazırda proqram təminatının effektiv sınağı ilə bağlı tədqiqatlar, hələ də özünün yetkinlik mərhələsinə çatmamışdır. Çünki dünyanın ən məşhur şirkət və təşkilatları belə hər il proqram təminatlarında baş verən çoxlu sayda səhvlər nəticəsində böyük ziyanlarla üzləşirlər. Məhz buna

görə də proqram təminatı sahəsində çalışan tədqiqatçılar yeni sınaq metodları tapmağa, mövcud metodları isə daha da inkişaf etdirib təkmilləşdirməyə çalışırlar [2]. Proqram təminatı sifarişçinin tələblərinə cavab verməlidir. Bunun təmin olunması üçün həm statik, həm də dinamik şəkildə analiz aparılmalıdır. Proqram təminatının sınaq mərhələsi resurslar və səylər baxımından ən çox vəsait tələb edir. Proqramı sınaqdan keçirərkən iki növ problem yarana bilər: texniki və qeyri-texniki. Ən məşhur proqram test problemləri "Üçbucaq problemi", "Sonrakı tarix problemi", "Komissiya problemi", "SATM problemi", "Kvadrat tənlik problemi" dir. Üçbucaq problemi proqram təminatında ən geniş yayılmış problemdir [3].

PT-da olan səhvləri aşkarlamaq üçün proqramın işlənilməsi prosesi başa çatdıqdan sonra "alfa" versiyası hazırlanır və əvvəlcədən müəyyən olunmuş test edən şəxs tərəfindən sınaqdan keçirilir.

II. PROQRAM TƏMİNATININ SINAĞI STRATEGİYASI

Hər hansı şirkət və təşkilatda fəaliyyət göstərən insanların fərdi məlumatları (FM), həmin şirkət və təşkilatlar üçün həssas məlumatlar hesab olunur və onların konfidensiallığının qorunması əhəmiyyətli məsələdir. Bu konfidensiallıq informasiya sistemi daxilində proqram təminatı səviyyəsində də mütləq təmin olunmalıdır. Çünki, bu məlumatların kənara sızması, itirilməsi, qərəzli məqsədlərlə dəyişdirilməsi həm fərdi şəxsə, həm də təşkilatın fəaliyyətinə ziyan vura bilər. Odur ki, hər bir şirkət və təşkilat onlara məxsus fərdi və digər məxfi məlumatların bədniyyətliyinə əlinə keçməməsi üçün müəyyən işlər görməlidir. Bu işlər, xüsusilə, PT yaradılan zaman nəzərə alınmalıdır. FM-in konfidensiallığının qorunması həm texniki, həm də proqram vasitələri ilə həyata keçirilməlidir. Texniki vasitələr dedikdə, kompüterə, şəbəkə kanallarına müdaxilənin cihaz və sistemlərlə təmin olunması, informasiya kanallarının qorunması nəzərdə tutulur. PT ilə qorunmada isə, fərdi məlumatlar yerləşən hissəyə edilən istənilən müdaxilə xüsusi proqram vasitəsilə qeydə alınaraq konfidensiallıq təmin olunur.

PT layihələndirilən zaman fərdi və məxfi məlumatların sifarişçinin tələbinə uyğun olaraq qorunması məsələsi əsas şərtlərdən biri olmalıdır. Layihələndirmənin sonunda sınaq prosesi aparılaraq PT-nin nə dərəcədə sifarişçinin tələblərinə

uyğun olması yoxlanılır. Sınaq zamanı FM-in qorunmasına xüsusi fikir verilməli, onun məxfiliyinin qorunma dərəcəsi müəyyən olunmalıdır.

PT-yə olan təhdidlərin qarşısını almaq məqsədilə, proqramda əlavə modulların yazılması lazım gəlir. Təhdidlərə informasiyanın kənara sızmasını və haker hücumlarını misal göstərə bilərik [4]. Bəzən sınaq zamanı fərdi məlumatların qorunma dərəcəsini müəyyən etmək üçün PT-yə bilərəkdən sifarişçi tərəfindən hücumlar olunur. Bu hücumlar etik hakerlər tərəfindən də həyata keçirilə bilər. Fərdi məlumatlar həssas məlumatlar kateqoriyasına aid edilir. Fərdi məlumatlara misal olaraq fərdin bank, kredit, təhsil, əmək fəaliyyəti, tibbi, vergi məlumatlarını göstərmək olar.

FM həssaslığa görə, əsasən 3 kateqoriyaya bölünür:

1. Adi fərdi məlumatlar – onların emalı, istifadəsi, ötürülməsi milli qanunlarda müəyyən edilmiş qaydada, xüsusi icazə olmadan da mümkündür.
2. Həssas fərdi məlumatlar – onların yığılması, emalı, istifadəsi qanunla müəyyən edilmiş xüsusi təhlükəsizlik tədbirləri tələb edir.
3. Xüsusi həssas fərdi məlumatlar - onların emalı, istifadəsi, ötürülməsi qanuna görə qadağandır, ya da xüsusi mühafizə və təhlükəsizlik tədbirlərindən istifadə etməklə mümkündür.

FM – insan haqqında mühüm şəxsi məlumatlardır və onların dövlət təşkilatları tərəfindən, insan hüquqlarının qorunması baxımından etibarlı müdafiəsi tələb olunur. Fiziki şəxslərin təhlükəsizliyinin təmin olunmasında FM-in müdafiə sisteminin qurulması çox mühüm və vacib məsələlərdəndir. Çünki bu məlumatların qorunmaması FM-in subyekti üçün bir çox neqativ, arzuolunmaz və ziyanlı hallara gətirib çıxara bilər. Bu məqsədlə Fərdi Məlumatların adekvat Müdafiə Sistemi (FMMS) yaradılır. Sistemin yaradılması üçün aşağıdakı addımlar tövsiyə olunur [5]:

1. Fərdi Məlumatlar İnformasiya Sisteminin (FMİS) layihə qabağı tədqiqi:
 - FMİS-in təsnifatı;
 - Təşkilati-sərəncam sənədlərinin işlənilib hazırlanması;
 - FMİS-in ilkin müdafiə dərəcəsinin müəyyən olunması;
 - FM-in təhlükəsizliyinə olan xüsusi təhdidlər modelinin yaradılması;
 - Xüsusi texniki tapşırıqın işlənməsi.
2. FMMS-in layihələndirilməsi.
3. FMMS-in istifadəyə verilməsi.

FMİS-i FM-in kateqoriyasından asılı olaraq 4 sinfə bölürlər:

1. İrqi, milli mənsubiyyəti, siyasi baxışları, dini və fəlsəfi əqidəsi, sağlamlıq vəziyyəti, intim həyatı haqqında olan FM.
2. FM subyekti identifikasiya etməyə imkan verən və onun haqqında əlavə informasiya (1-ci kateqoriyada olan informasiya istisna olmaqla) almağa imkan verən FM.
3. FM-in subyekti identifikasiya etməyə imkan verən FM.
4. Şəxsiyyəti məlum olmayan və ya hamı üçün əlçatan FM.

Hər kateqoriya üçün informasiya sistemində informasiyanın müdafiəsi metodu və ya üsulu müəyyən olunur.

Fərdi məlumatların təhlükəsizliyi dərəcəsini müəyyən etmək üçün aşağıdakı sxemdə ekspert qiymətləndirməsi göstərilir [6].

Şəkil 1. Fərdi məlumatların təhlükəsizlik dərəcəsinin müəyyən edilməsi

III. PROQRAM TƏMİNATININ TESTLƏŞDİRİLMƏSİNDƏ YARANA BİLƏCƏK PROBLEMLƏR

Sınaqda istifadə olunan məlumatların (verilənlərin) əl ilə (ing. manual) hazırlanması effektiv hesab edilə bilməz. Bunun əsas səbəbi həddən artıq əl əməyinin tələb olunmasıdır. Test məlumatlarının avtomatik yaradılması isə az əmək tələb etdiyindən daha məqsədəuyğundur. Proqram təminatının sınaq zamanı istehsal (real) məlumatlarından istifadə edilməsinin üstünlükləri olsa da, bir sıra problemlər də mövcuddur. Əsasən üç problemi nəzərdən keçirirlər.

1. Həcm problemi. Sınaqda istehsal məlumatlarından istifadə etdikdə qarşılaşdığımız ən böyük problemlərdən biri məlumatların həcmnin olduqca böyük olmasıdır. Bankların timsalında bunu aydın görə bilərik. Çoxsaylı müştəri məlumatlarının və onların etdikləri bütün əməliyyatların həcmi olduqca böyük olur. Sadə bir misala baxaq. 100 min müştərinin ay ərzində orta hesabla 5 əməliyyat həyata keçirməsini fərz edək. Bu, ayda təxminən 500 min əməliyyat qeydlərinin yaranması deməkdir. Bank yarandığı gündən bu günə kimi olan əməliyyatların ümumi sayı olduqca böyükdür. Təbii ki, bütün bu məlumatların testləşmə bölgəsinə köçürüləcəyi təqdirdə işin həcmnin nə dərəcədə böyük olduğunu təsəvvür etmək o qədər də çətin deyil. Bütün bu məlumatların sınaq zonasına keçirilməsi klonlaşdırma üsulu adlanır. Bu da yüklənmə müddətinin və disk-yaddaş xərclərinin artması kimi bir sıra mənfi hallara gətirib çıxarır.

2. Mənbə problemi. Digər bir əsas problem məlumat mənbələrinin müxtəlifliyidir. Məsələn, məlumatlar bir çox mənbədən, yəni Oracle, DB2, SQL Server, Sybase, Excel, Word Fayllar, Mainframe faylları, Verilənlərin Elektron Mübadiləsi (ing. Electronic Data Interchange, EDI) sənədləri kimi mənbələrdən əldə edilə bilər. Eyni zamanda cari məlumatlar və bu məlumat mənbələri arasında əlaqələrin olması vəziyyəti bir qədər də qəlizləşdirir. Email olunacaq məlumatları sınaq zonasına yükləyərkən məlumat əlaqələri və məlumat bütövlüyünün qorunmasına da çox diqqət yetirilməlidir.

3. Məlumat təhlükəsizliyi problemi. Email məlumatlarının sınaq prosesində istifadə olunmasında daha vacib problemlərdən biri də həssas məlumatların mövcudluğudur. Həssas məlumatların təhlükəsizliyinin təmin olunmaması maliyyə, marketing və bəlkə də hüquqi sferada ciddi problemlərə səbəb olacaq bir məsələdir. Buna misal olaraq məşhur maliyyə təşkilatları və ya tibbi sığorta şirkətlərinin sistemində baş vermiş məlumatların oğurlanması hadisələrini göstərə bilərik. 2017-ci ildə Equifax (Amerika kredit tarixi bürosu) məlumatlarının oğurlanması buna ən bariz nümunələrdən biridir [7].

Həssas məlumatların qorunmamasından yaranan təhlükələrin qarşısını almaq məqsədilə təşkilatlar proqram təminatına və istehsal sistemlərinə aid prosedurlara çoxlu maliyyə vəsaiti ayırırlar. Ümumiyyətlə, onu da qeyd edək ki, istehsalat məlumatlarından sui-istifadə olunması böyük risklərə səbəb ola bilər. Bank misalında bir nümunəyə baxsaq görürük ki, istehsalat məlumatlarında adlar, ünvanlar, hesab nömrələri, qalıqlar, kredit kartı nömrələri kimi real müştəri məlumatları vardır. Bu məlumatlardan sui-istifadə etmək bank üçün ağır nəticələrə səbəb ola bilər. Belə hallarda problemin aradan qaldırılması üçün məlumat maskalanması (ing. data-masking) üsulundan istifadə etmək olar.

Məlumat maskalanması – həssas məlumatların dəyişdirilməsi, anonimləşdirilməsi və ya silinməsilə icazəsiz

istifadənin qarşısının alınması prosesidir. Məlumatın qorunması tələbləri bir çox mənbədən, o cümlədən hökumət qanunlarından, sənaye agentliklərinin milli və beynəlxalq qaydalarından və daxili korporativ siyasətlərdən (məsələn, ödəniş məlumatları kimi həssas məlumatlardan) irəli gəlir. Bu tənzimləmələrdə format və məzmun bölgəyə görə dəyişir. Məsələn, ABŞ-ın Ədalətli və Dəqiq Kredit Əməliyyatları Qanunu (ing. Fair and Accurate Credit Transactions Act - FACTA), ABŞ-dakı 95/46 / EC Avropa Məlumat Qoruma Direktivindən fərqlidir. ABŞ-dakı tibbi sığorta və səhiyyə təminatçıları Tibbi Sığorta Daşınması və Hesabatlılıq Qanununa (ing. Health Insurance Portability and Accountability Act, HIPAA) uyğun olmalıdır.

Bu qaydalar zamanla dəyişdiyindən təşkilatlar dəyişiklikləri izləməli və bu dəyişikliklərə uyğunlaşmalıdırlar.

Şirkətlər və təşkilatlar məlumatların qorunması qaydalarından boyun qaçırdıqları təqdirdə, hansı cəza tədbirlərinin olacağını da bilməlidirlər. Son vaxtlar tənzimləyici orqanların həssas məlumatların itirilməsinə, təhlükənin pozulmasına görə təşkilatlara böyük cərimələrin tətbiq etməsi halları olduqca geniş yayılmışdır. Məlumatların Qorunmasının Ümumi Qaydası (ing. General Data Protection Regulation, GDPR) cərimələri qlobal gəlirin 4%-i və ya 20 milyon avro həcmində ola bilər. Təbii ki, faktiki məbləğ pozuntu növünə görə dəyişir və ilkin məhkəmə qərarlarında müəyyən edilmiş qaydaya uyğun olaraq müəyyənləşdirilir. Eyni zamanda burada korporativ markaya və nüfuza dəyən zərərdən də söhbət gedir. Şübhəsiz ki, şirkətin reputasiyasına, imicinə dəyən ziyan bununla əlaqəli cəzalarla müqayisədə şirkət üçün daha böyük itkidir.

IV. MƏLUMATLARIN QORUNMASI STRATEGİYALARI

Məlumatların pozulması (itirilməsi, köçürülməsi və s.) – PT-nin sınağının strategiyaları çərçivəsində həqiqi məlumatların istifadə olunmasının ən böyük təhdididir. Məlumatların qorunması üçün aşağıdakı strategiyaları göstərə bilərik [8]:

1. Həqiqi məlumatları qoruma siyasəti strategiyası. Təşkilatlar istehsal məlumatlarının qeyri-istehsal şəraitində istifadə edilməməsi üçün strategiya qurmalıdırlar. Bu strategiyada, sınaq zamanı test məlumatlarının yaradılması və ya saxlanması üçün məsuliyyət daşıyan şəxslər açıq şəkildə bilinməlidir.

2. Müvafiq giriş hüquqlarının təmin edilməsi. Təşkilatlar məlumatların qorunması məqsədilə fiziki girişi intensiv şəkildə qoruyur və istehsal mühitində məlumat pozuntularının baş verməməsini təmin etmək üçün diskləri və məlumatları hakerlərin hücumlarından qorunmaq üçün şifrələyirlər. Məhz buna görə də təşkilat test proqramı strategiyalarının bir hissəsi olaraq daxili istifadəçilər və proqram təminatını işləyənlər üçün ciddi təhlükəsizlik və giriş nəzarət mexanizmlərini təmin etməlidir.

3. Həqiqi məlumatları qorumaq üçün müvafiq üsullardan istifadə olunması. Bu üsullardan biri aşkarlayıcı üsuldur. Bu

üsul başqa cür “məlumatları həssaslaşdırın” üsul kimi də tanınır. Aşkarlayıcı üsul bir istehsal sistemindən məlumatı alaraq testləşdirmə və ya analiz üçün uyğun olmayan həssas məlumatlara çevirir.

4. *Məlumat maskalanmasından istifadə edilməsi.* Təşkilatların test məlumatlarının əl ilə yaradılması və məlumat maskalanması olmaqla iki variantı vardır. Qeyd edək ki, məlumatların maskalanması daha asandır. Bu texnologiyalar düzgün yerinə yetirildiyi halda səmərəlidir, genişlənə bilər və sadədir. Məsələn, yalnız həssas məlumatlar maskalanmalı və maskalanmış məlumatlar həqiqi məlumatları təmsil etməlidir.

NƏTİCƏ

Şirkət və təşkilatlar üçün keyfiyyətli proqram təminatının olması olduqca vacib və əhəmiyyətli bir məsələdir. Çünki keyfiyyətli proqram təminatı şirkətin etibarlı fəaliyyətini təmin edir, onun inkişafına kömək edir. Məhz bu səbəbdən də proqram təminatının keyfiyyətinin yüksəldilməsi üçün PT- nin sınağı məsələlərinə xüsusi diqqət yetirilməlidir. Yuxarıda qeyd elədiyimiz kimi proqram təminatının həyat dövrünün müxtəlif mərhələlərində sınaq aparılaraq onda olan səhvlər ardıcıl şəkildə aradan qaldırılmalıdır. Lakin proqram təminatının sınağı zamanı bir sıra problemlər meydana çıxır ki, bunlardan da ən vacibi məlumatların təhlükəsizliyi problemidir və bu sahədə əsas problem FM-in mövcudluğu ilə bağlıdır. Təəssüf ki, bir çox şirkətlər təhlükəsizlik məsələlərini dəfələrlə, görməzlikdən gələrək və ya məlumatların qorunması öhdəliklərindən xəbərsiz olaraq çoxlu sayda problemlərlə üzləşməli olurlar. Son zamanlar FM-lə bağlı müşahidə olunan pozuntular bu məsələlərə xüsusilə ciddi yanaşmağı tələb edir. Odur ki, bütün şirkət və təşkilatlarda informasiya təhlükəsizliyi qrupları yaradılmalı, informasiyanın və xüsusilə də FM-in təhlükəsizliyi onların daim diqqət mərkəzində olmalıdır.

İSTİNADLAR

- [1] T. Bayramova, N. Abbasova, “Proqram Təminatının Verifikasiya və Sınaq Metodlarının Müqayisəli Təhlili,” Proqram mühəndisliyinin aktual elmi-praktiki problemləri I respublika konfransı, Bakı, 17 may 2017-ci il, səh. 198- 202.
- [2] S.Chaudhary, “Latest Software Testing Tools and Techniques: A Review,” International, Journal of Advanced Research in Computer Science and Software Engineering, vol. 7, may 2017, pp.538-540.

- [3] K. Solanki, S. Dalal, S. R. Scholar, M.R. Scholar, “Comprehensive Study of Popular Software Testing Problems”, International Conference on “Computing for Sustainable Global Development. 1-3 March, 2017, pp.1157-1160.
- [4] E. Bağırov, “Proqram təminatı boşluqlarının analizi üsulları”, Proqram mühəndisliyinin aktual elmi-praktiki problemləri I respublika konfransı, Bakı, 17 may 2017-ci il, səh. 259-262.
- [5] A. A. Шелупанов, В.Г. Миронова, С.С. Ерохин, А.А. Мицель, «Автоматизированная система предпроектного обследования информационной системы персональных данных», «АИСТ-П» Доклады ТУСУРа, № 1 (21), часть 1, июнь 2010, стр. 14- 22.
- [6] A. A. Шелупанов, В.Г. Миронова, «Анализ этапов предпроектного обследования информационной системы персональных данных», 2011, стр. 45-48.
- [7] R. Raghuraman, “Top 3 Challenges in using Production data in Test Environments”, https://tdminsights.blogspot.com/2013/02/top-3-challenges-in-using-production.html?fbclid=IwAR3tdNfVxwQIBYboUG5lcVdOerLfYbMLM2vEVZStYuk1sL8dGGQnNfEIV_0
- [8] Sh.Gupta, “Software testing strategy for protection of real data”, october 2010, https://www.computerweekly.com/tip/Software-testing-strategy-for-protection-of-real-data?fbclid=IwAR2ogZ3io9j3EfYS_rmLjxjgtarqMJ5EXwb84aicpgGC6ZOv0LnBxlrurS4.

PROBLEMS OF ENSURING THE SECURITY OF PERSONAL DATA IN SOFTWARE TESTING

Tofig Kazimov¹, Nazaket Malikova²

^{1,2}Institute of Information Technology of ANAS, Baku,
Azerbaijan

¹tofig@mail.ru, ²naranara_68@mail.ru

Abstract— The article describes the problems that may arise in the software testing process, in particular the difficulties that may arise in ensuring the security of personal data, and the measures that can be done in this regard. The causes of the problems are then investigated, ways to ensure the safety of personal data during the testing process, and the importance of their consideration are highlighted.

Keywords— *software testing; information security; personal data; data-masking*

Fərdi məlumatların mühafizəsi üçün blokçeyn texnologiyaları: imkanları və perspektivləri

Yadigar İmamverdiyev¹, Günay Muradova²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹yadigar@iit.science.az, ²gmuradova9@gmail.com

Xülasə— Məqalədə blokçeyn texnologiyalarının fərdi məlumatların mühafizəsində istifadəsi imkanlarının araşdırılmasına baxılır. Blokçeyn texnologiyasının qısa xarakteristikası verilmiş və mövcud araşdırmaların qısa analizi aparılmışdır. Blokçeyn texnologiyası ilə fərdi məlumatların təhlükəsizliyinin təmin edilməsi imkanları və yarana biləcək problemlər analiz edilmişdir.

Açar sözlər — fərdi məlumatlar; blokçeyn; gizlilik, gizliliyin qorunması, GDPR

I. GİRİŞ

Big Data dövründə fərdi məlumatlar davamlı olaraq toplanır və analiz edilir, bu da innovasiyalara və iqtisadi inkişafa səbəb olur. Şirkətlər və təşkilatlar topladıqları məlumatları xidmətləri fərdiləşdirmək, korporativ qərar qəbul etmə prosesini optimallaşdırmaq, gələcək tendensiyaları proqnozlaşdırmaq və daha bir çox digər məqsədlər üçün istifadə edirlər. [1]

Lakin məlumatların sürətlə artdığı və əlçatan olduğu bir dövrdə fərdi məlumatlar böyük təhlükələr altına düşür. Fərdi məlumatların qeyri-qanuni istifadə olunması hallarına çox təsadüf olunur. Fərdi məlumatlar bir çox hallarda onların sahiblərinin razılığı olmadan toplanır, bu məlumatların digər məqsədlər üçün istifadəsi üçün həmin şəxslərdən icazə alınmır. Smart cihazlardan və sosial şəbəkələrdən istifadə fərdi məlumatların qorunmasını bir qədər də çətinləşdirir.

Belə şəraitdə fərdi məlumatların konfidensiallığını dəstəkləyən texnoloji alətlərin yaradılması olduqca zəruridir. İnformasiya təhlükəsizliyi üzrə tədqiqatçılar fərdi məlumatlara yönəlmiş təhdidlərə qarşı müxtəlif üsullar hazırlamışlar. Anonimləşdirmə, kriptografik üsullar ilə fərdi məlumatları qorumağa çalışırlar, lakin onlar hazırda praktikada geniş istifadə olunmaq üçün yetərli deyil [1].

Son illərdə yeni rəqəmsal reyestr sistemləri ortaya çıxmışdır [2]. Blokçeyn texnologiyası və ya paylanmış reyestr texnologiyası Bitcoinin yaradılması anından – 2009-cu ildən məlumdur. Bitcoin blokçeyn texnologiyası ilə işləyən ilk rəqəmsal kriptovalyuta hesab edilir. Bu sistem istifadəçilərə bitcoinləri mərkəzləşdirilmiş tənzimləyici olmadan icma tərəfindən təsdiqlənən blokçeyn texnologiyasından istifadə edərək təhlükəsiz şəkildə ötürməyə imkan verir. Blokçeynin təhlükəsiz, şəffaf, anonim olması və verilənlərin tamlığını üçüncü tərəf olmadan həyata keçirməsi onun populyarlığının artmasına səbəb oldu. Bitcoin timsalında bir neçə il ərzində

praktiki olaraq fasiləsiz həyata keçirilməsi onun digər sahələrə tətbiqi məsələsini ortaya çıxardı.

Hazırda blokçeyn texnologiyasının bir çox sahələrdə tətbiqi üzrə pilot layihələr həyata keçirilir. Anonimliyi və konfidensiallığı müxtəlif dərəcədə dəstəkləyən xüsusi protokollardan istifadə etməklə blokçeyn texnologiyası tibbi, maliyyə və digər sahələrdə fərdi məlumatların mühafizəsini təmin edə bilər. Bu məqsədlə təqdim olunan işdə fərdi məlumatların mühafizəsi üçün blokçeyn texnologiyalarının imkanları, perspektivləri və problemləri analiz edilir.

II. BLOKÇEYN TEXNOLOGİYALARININ QISA XARAKTERİSTİKASI

Texniki baxımdan, adından da göründüyü kimi, blokçeyn (“block” – blok + “chain” – zəncir) informasiya bloklarının zənciridir. Şəkil 1-də Bitcoin blokçeyninin strukturu təsvir olunur.

Şəkil 1. Bitcoin blokçeyninin strukturu

Şəkildə göstərildiyi kimi, hər bir Bitcoin bloku dörd komponentdən ibarətdir: blokun ölçüsü (Size), tranzaksiya sayğaçı (#TXs), blokun başlığı (Header) və tranzaksiyalar (Transactions). Blokun ölçüsü və tranzaksiya sayğaçı, uyğun olaraq, blokdakı baytların və tranzaksiyaların saylarını göstərir. Tranzaksiyalar – bloka daxil olan tranzaksiyaların siyahısıdır. Blok başlığına altı sahə daxildir:

- *Version* – versiya nömrəsi (konsensus protokolunun yenilənməsini izləmək üçün istifadə edilir);
- *PreviousHash* – zəncirdə bilavasitə əvvəl gələn blokun heşi;
- *Timestamp* – blokun yaradılması tarixi;
- *Target* – hədəf *qiyməti*, mayninq prosesində bu qiymətdən kiçik olan heş axtarılır;
- *Nonce* – mayninq alqoritmində istifadə edilən sayğac;
- *Merkle Root* – bloka daxil olan bütün tranzaksiyaların heşləri əsasında yaradılan binar ağacdır.

Blokçeyn texnologiyası üç addım ilə həyata keçirilir: 1) Tranzaksiyanın yaradılması; 2) Tranzaksiyanın təsdiqlənməsi; 3) Blokun zəncirə əlavə edilməsi.

III. BLOKÇEYNİN NÖVLƏRİ

Tədqiqatçılar blokçeyn texnologiyalarını “Blockchain 1.0” (kriptovalyutalar), “Blockchain 2.0” (ağıllı müqavilələr), “Blockchain 3.0” (dövlət idarəçiliyi, təhsil, elm, mədəniyyət və s. sahələrdə tətbiqlər) kimi inkişaf mərhələlərinə ayırırlar.

Blokçeynin digər sahələrdə tətbiqi cəhdləri onun yeni növlərinin meydana çıxmasına gətirib çıxardı. Mütəxəssislər blokçeyn verilənlərinə girişlə əlaqədar olaraq blokçeynləri *açıq* (ing. public) və *özal* (ing. private) olmaqla iki sinfə bölməyi tövsiyə edirlər [2].

Blokçeynlər tranzaksiyaları emal etməyə, yəni tranzaksiyaların yeni bloklarını yaratmağa qoyulan məhdudiyyətdən asılı olaraq *inkluziv* (ing. permissionless) və *ekskluziv* (ing. permissioned) blokçeynlərə bölünürlər. Inkluziv blokçeyndə istənilən qovşaq tranzaksiyaların yeni blokunu yarada bilər. Ekskluziv blokçeyndə isə tranzaksiyaların emalını yalnız seçilmiş qovşaqlar həyata keçirə bilərlər.

Ethereum platformasının sahibi Vitalik Buterin 2015-ci ildə şirkət bloqunda nəşr etdiyi məqalədə blokçeynləri 3 sinif üzrə təsnif edir [9]:

- *açıq blokçeyn* (ing. public blockchain) – tamamilə açıq blokçeyndir, tranzaksiyalar azad şəkildə həyata keçirilir və onlara heç kim nəzarət etmir, hər bir kəs konsensus prosedurunda iştirak edə bilər;
- *konsorsium blokçeyni* (ing. consortium blockchains) – konsensus proseduruna seçilmiş qovşaqlar nəzarət edir;
- *özal blokçeyn* (ing. fully private blockchain) – mərkəzi orqan bütün tranzaksiyaları izləyir və nəzarət edir.

Böyük Britaniya hökumətinin baş elmi məsləhətçisi ser Mark Walport da oxşar təsnifat təklif edir [2]. O, paylanmış reyestrlər və onların dövlət idarəetməsində potensialı mövzusunda məruzəsində blokçeynləri aşağıdakı 3 sinfə bölmür:

- *inkluziv reyestrlər* (ing. permissionless public ledgers) – burada tranzaksiyaları təsdiqləyən mərkəzi orqan yoxdur. Bitcoin və Ethereum belə reyestrlərə misaldır;
- *ekskluziv açıq reyestrlər* (ing. permissioned public ledgers) – burada tranzaksiyaları müəyyən subyektlər təsdiqləyir. Bunlar idarəedici orqan, səlahiyyətli

əməkdaş, müəssisə və s. ola bilər. İstifadəçilər verilənlərə baxa bilərlər (xüsusilə vacib informasiya gizli saxlana bilər);

- *ekskluziv özal reyestrlər* (ing. permissioned private ledgers) – əvvəlki növə oxşayır, fərq ondadır ki, verilənlər hamıya açıq deyil.

Hibrid blokçeyn. Açıq və özal blokçeynlər arasında bir balansdır, onu «qismən demərkəzləşmiş» və ya «konsorsium blokçeyni» də adlandırırlar. Məsələn, on sənaye təşkilatının konsorsiumunda hər bir təşkilat blokçeyn şəbəkəsində özünün mayninq/yoxlama qovşağını dəstəkləyir. Bu halda blok ən azı yeddi qovşaq tərəfindən imzalandıqda həqiqi ola bilər. Bütün qovşaqların blokçeyndən oxumaq üçün açıq girişi ola bilər və ya bu yalnız konkret qovşaqlara məhdudlaşdırıla bilər [9]. Lakin demərkəzləşmənin azalması səbəbindən blokçeyn yazılarının saxtalaşdırılması ehtimalı var [2].

IV. GDPR VƏ BLOKÇEYN: ZİDDİYYƏTLƏR

Avropa İttifaqının Verilənlərin Mühafizəsi haqqında Ümumi Qanunu (General Data Protection Regulation, GDPR) 25 may 2018-ci ildən qüvvəyə minmişdir. GDPR istifadəçilərə öz fərdi məlumatları üzərində nəzarət imkanı verməyə yönəlib. Vətəndaşlara öz fərdi məlumatlarına baxmaq və düzəliş etmək hüququ, verilənlərin emalına etiraz etmək hüququ, verilənlərin sızması baş verdikdə məlumatlandırılmaq hüququ, unudulmaq hüququ (yəni, fərdi məlumatlarının operator tərəfindən dərhal, izafi rəsmiyyət olmadan məhv edilməsini tələb etmək hüququ) verilir. Bu hüquqların başqa şəxslərin və təşkilatların hüquq və azadlıqlarına, bütövlükdə cəmiyyətin maraqlarına zidd olmaması gözlənilir. GDPR öz istifadəçilərinin məlumatlarını istifadə edən və saxlayan şirkətlər üçün sərt qaydalar müəyyən edir.

GDPR-in texnoloji baxımdan neytral olduğu iddia edilsə də, blokçeynə münasibətdə bir çox məsələlər meydana çıxır. Blokçeyn layihələrində fərdi məlumatların emalı texnologiyası bir çox cəhətdən GDPR tələbləri ilə ziddiyyət təşkil edir. GDPR-də müəyyən edilən fərdi məlumatın subyekti, kontrolleri, prosessoru kimi rolları blokçeyndə birqiyəmli təyin etmək çətinidir, çünki blokçeyn mahiyyətinə görə demərkəzləşmiş texnologiyadır.

Fərdi məlumatların subyektlərinin unudulmaq hüququnu, düzəliş etməkhüququnu və emalı məhdudlaşdırmaq hüququnu təmin etmək məsələsində də blokçeyn texnologiyası çətinliklərlə qarşılaşır. Blokçeyn praktiki olaraq redaktə olunmur, onda saxlanılan verilənləri yeniləmək, silmək, dəyişmək, düzəliş etmək mümkün deyil.

Fərdi məlumatların transsərhəd ötürülməsi zamanı mühafizə tədbirlərinin həyata keçirilməsi çətinləşir, çünki blokçeyn-sistemdə kontrollerlər maynerlərin yerləşmə yerini həmişə dəqiq müəyyən edə bilmirlər və müvafiq tədbirləri tətbiq etmək mümkün olmur. Verilənlərin minimallaşdırılması və onların saxlanma müddətlərinin məhdudlaşdırılması tələbini də blokçeyndə reallaşdırmaq problemlidir.

Bu suallara fərdi məlumatların mühafizəsi sahəsində Fransada səlahiyyətli orqan olan CNIL (Commission Nationale de l'Informatique et des Libertés – İnformatika və insan

azadlıqları üzrə Milli Komissiya) [3] və Avropa Blokçeyn Forumu öz hesabatlarında cavab verməyə çalışırlar [4].

GDPR-də ilk növbədə fərdi məlumat kontrolleri məsuliyyət daşıyır. Blokçeyn modelində bir neçə tərəf kontroller kimi çıxış edir. Bu problemi həll etmək üçün subyektlər xüsusi təyinatlı yeni obyekt yaratmalı və ya müqavilə ilə bir kontroller müəyyən etməlidirlər. Digər obyektlər blokçeyn və mayninq validatorlarından istifadə edirlər.

Fərdi verilənlərin blokçeyndə saxlanması mümkün olduqca minimallaşdırmaq lazımdır. Blokçeynin əsas təyinatı tranzaksiyanın baş verdiyini və ya yazının həqiqi olduğunu təsdiqləməkdir. Əgər tranzaksiyalarda və yazılarda fiziki şəxslər iştirak edərsə, onda onlarda fərdi məlumatlar mütləq olacaq. Lakin belə fərdi məlumatları blokçeyndən kənarda saxlamaq, blokçeynə isə onları sübut edən heş-kodu daxil etmək olar. Bu GDPR-in verilənlərin minimallığı və təhlükəsizlik tələblərini yerinə yetirməyə imkan verir.

V. BLOKÇEYN TEKNOLOGİYASININ TƏKMİLLƏŞDİRİLMƏSİ İSTİQAMƏTLƏRİ

Blokçeyn texnologiyası tədqiqatçıların qarşısına praktiki ehtiyaclardan qaynaqlanan müxtəlif tədqiqat problemləri qoyur. Blokçeynlərin ən aktual problemləri arasından miqyaslanma məsələlərini, təhlükəsizliyin və gizliliyin təmin edilməsini qeyd etmək olar [2].

Hazırda blokçeynin məlum olan ən fundamental təhlükəsizlik boşluğu təkrar xərcləmə (ing. double spending), “51 % hücumu”, Sivilla hücumu (ing. Sybil attack) və DDoS hücumudur. Bu hücumların Bitkoin şəbəkəsində baş tutması ehtimalı hazırda olduqca kiçikdir. Digər blokçeyn layihələrində həmin hücumların qarşısını almaq üçün müxtəlif əlavə tədbirlər nəzərdə tutulur.

Geniş yayılmış blokçeyn texnologiyası kimi Bitkoinin əsas problemi tranzaksiyaların emal sürətinin olduqca aşağı olmasıdır (saniyədə 6-7 tranzaksiya); müqayisə üçün qeyd edək ki, bu göstərici VISA sisteminə 2000-dir. Ümumiyyətlə, blokçeyn-şəbəkənin miqyaslanması məsələsi əlaqəli üç parametrlə – təhlükəsizlik, demərkəzləşmə və miqyaslanmanın optimallaşdırılması arasında balanslaşdırmanı tələb edir. Tranzaksiyaların emal sürətini yüksəltmək üçün blokçeyn ya təhlükəsizliyi, ya da demərkəzləşməni qurban verməlidir. Praktiki yüksək sürət nümayiş etdirən blokçeynlərdə, adətən, demərkəzləşmə güzəştə gedilir və hazırda mərkəzləşmə meylləri üstün gəlir.

Miqyaslanmanın təmin edilməsi üçün yanaşmaların işlənməsi aktiv tədqiqat istiqamətlərindəndir. Bu sahədə bəzi təşəbbüsləri xatırlatmaq olar: global reyestrin qovşaqların bir qrupu tərəfindən idarə edilən daha kiçik altreyestrlərə bölünməsi, saxlanmanı optimallaşdırmaq üçün əvvəlki tranzaksiyaların silinməsi, blokçeynlər iyerarxiyasından istifadə edilməsi (məsələn, Lighting Network texnologiyası), blokçeynin seqmentlərə bölünməsi (ing. sharding), blokun ölçüsünün artırılması (məsələn, SegWit) və s.

PoW (Proof of Work) konsensus protokolunun icrası böyük xərclər tələb edir. Bitkoin şəbəkəsi mayninqə bütöv bir dövlətin istehlak etdiyi qədər elektrik enerjisi sərf edir. Xərcləri minimallaşdırmaq üçün çox sayda alternativ konsensus

protokolları təklif edilmişdir, lakin əksər kriptovalyutalarda PoW protokolunun hansısa forması istifadə edilir. PoW kimi paylanmış konsensus protokolunun ən böyük problemlərindən biri şəbəkəni təhlükəsiz, lakin olduqca yavaş etməsidir. Bu blokçeynin bütün dominant atributları: demərkəzləşmə, təhlükəsizlik və miqyaslanma arasında balanslaşdırmanın nəticəsidir.

VI. MÖVCUD TƏDQİQATLARIN ANALİZİ

[5]-də blokçeyn identifikasiya xidmətlərini, yəni uPort, Sovrin və ShoCard-ı tənqidi analiz edilmiş, müasir rəqəmsal xidmətlərin çatışmazlıqları aşkar edilmişdir. Mövcud identifikasiya idarəetmə sistemlərində identifikasiya atributlarının məhdudiyyətlərini və zəif cəhətlərini aradan qaldırmaq üçün təhlükəsizlik tələblərinə yüksək səviyyədə cavab verən DNS-IdM təklif edilmişdir. Smart əlaqəyə əsaslanan DNS-IdM identifikasiya idarəetmə sistemi istifadəçilərə fərdi məlumatlarını qorumağa imkan verir, konsepsiyayı öz-özünə yerinə yetirir.

[6]-də Blokçeyn texnologiyası ilə Avropa Birliyinin informasiya təhlükəsizliyi çərçivəsində qarşılıqlı nöqtələri müzakirə etmiş və smart şəhərlərdə blokçeyn əsaslı layihələrin daha yaxşı inkişaf etdirilməsi üçün tövsiyələr verilmişdir. Həmçinin məqalədə blokçeynin klassifikasiyası, paylanmış reyestr texnologiyaları (ing. Distributed Ledger Technology, DLT) və blokçeynlər haqqında ətraflı araşdırma aparılmışdır.

[7]-də fərdi məlumatların sızma riskini azaltmaq üçün blokçeyn əsaslı məlumat idarəetmə sistemi təklif edilmişdir. GDPR fərdi məlumatları mərkəzləşdirilməmiş və etibarlı paylama və izləmə sxeminə uyğundur. Təklif olunan blokçeyn əsaslı identifikasiya idarəetmə sistemləri ilə GDPR subyektləri (istifadəçi, kontroller və prosessor) arasında məlumat mübadiləsini nümayiş etdirir. GDPR məhdudiyyətlərinə görə fərdi məlumatları şəbəkə xaricində saxlama arxitekturasından istifadə edilmişdir, bu, blok ölçüsünü də azaldır. Təklif olunan arxitektura təsdiq üçün multiçeyn istifadə edərək prototip yaradır. Bu tədqiqatda təklif olunan fərdi məlumatları idarəetmə sisteminə əsaslanan blokçeynin konfidensiallığı yoxlamaq üçün fərdi məlumatları paylaşmaq, silmək, dəyişdirmə və izləmə xüsusiyyətlərini təqdim edir.

[8]-də göstərilir ki, tibbi məlumatların mübadiləsi üçün DLT əsaslı sistemin dizaynı və istifadə vəziyyəti nəzərə alınmalıdır. Fərdi məlumatların yalnız istifadəsi və istifadə zamanı yaranmış riski minimuma endirmək üçün iki dizayn təklif edilmişdir. Dizaynlardan biri kütləvi yayımlanan IOTA reyestrinə, digəri isə IOTA və IPFS (InterPlanetary File System) çoxluğuna əsaslanır. İlk dizayn daha sadədir, lakin fərdi məlumatların ələ keçirilmə riskini minimuma endirmək üçün xüsusi diqqət tələb edir. İkinci dizayn isə daha mürəkkəbdir, böyük sənədlərin mübadiləsinə imkan yaradır.

[9]-də gizliliyin qorunması funksiyaları və əhatə dairəsi barədə məlumat verilmiş, GDPR və ISO/IEC 29100: 2011 standartlarının IoT-da gizlilik təhdidlərinin faktiki həlli vəziyyəti analiz edilmişdir. Burada əsas məqsəd müvafiq həllərin müasir qanuni prinsiplərə və gizlilik standartlarına uyğunluğunu yoxlamaq və gizliliyə təhdidləri azaltmaqdır.

[10]-də blokçeyn ilə GDPR tələblərini “barışdırmağın” və gizliliyin daha geniş şəkildə təmin edilməsinin mümkünüyü

araşdırılır, GDPR-ə uyğun məlumat idarəçiliyində blokçeyn həllərinin güclü və zəif tərəfləri analiz edilir. GDPR tələbləri ilə bəzi mövcud blokçeyn həlləri və tətbiqləri arasındakı uyğunsuzluqlar və həll yolları araşdırılır.

[11]-də GDPR "fərdi məlumatlar", "vizual fərdi məlumat" termini ilə əlaqələndirilir. GDPR kontekstində vizual fərdi məlumatlar üçün "Data Protection-by-Design" tətbiqi kimi maşın təliminin, təsvirin işlənməsi, kriptografiya və blokçeynin qarşılıqlı əlaqəsi araşdırılır. Məqalədə fərdi məlumatların qorunması qaydaları araşdırılır və GDPR-ə uyğun fərdi məlumatların qorunması ilə hazırlanan video nəzarət sistemlərinin inkişafı üçün təkliflər təqdim edilir.

[12]-də DLT ilə kontrollerlər və məlumat prosessorları arasında konseptual model təklif edilmişdir. Məqalə blokçeyn tətbiqinin GDPR uyğun əməliyyatları üçün faydalı məqamları təqdim etmək məqsədi daşıyır və ancaq DLT həllinin tətbiq oluna biləcəyi vacib cəhətləri göstərir.

[13]-də gizlilik və təhlükəsizlik riskləri ilə fərdi məlumatların təhlükəsizliyi üçün potensial təhlükələrlə bağlı problemlər araşdırılmışdır. IoT sistemi Internetdə məlumatları, o cümlədən fərdi məlumatları ötürməyə imkan verir. Bu çərçivədə GDPR standartları nəzərdən keçirilmişdir. Fərdi məlumatların yalnız istifadəsinin qarşısını alan riskləri qiymətləndirmək üçün tədqiqat aparılmışdır. Bundan əlavə, fərdi məlumatların təhlükəsizliyi üçün dünya miqyasında gizlilik standartının inkişaf etdirilməsi təklif olunmuşdur.

NƏTİCƏ

Bitkoin göstərdi ki, kriptografiya və düşünülmüş iqtisadi stimullar vasitəsilə fərdi məlumatlar daxil olmaqla informasiyanın təhlükəsiz saxlanması və emalı metodu yaratmaq mümkündür. Bu təcrübədən çıxış edərək, Bitkoin-in əsasında dayanan blokçeyn texnologiyasından fərdi məlumatların təhlükəsizliyinin təmin olunması istiqamətində bir platforma yaratmaq üçün istifadə etmək olar.

Lakin fərdi məlumatların qorunması sahəsində de-fakto model qanun hesab edilən GDPR ilə blokçeyn texnologiyaları arasında bir çox ziddiyyət vardır. Mütəxəssislərin qənaətinə görə, bu texnologiyanın öz yüksək potensialına nail olması onun GDPR-ə nə dərəcədə uyğun reallaşdırılmasından asılı olacaq.

Bu məqsədlərə çatmaq üçün faydalı ola biləcək yeni elmi-texniki tədqiqatlar aparılır. Bu tədqiqatlar miqyaslanma və ya idarəetmə strukturunun təkmilləşdirilməsi problemlərini həll etməyə çalışırlar ki, məsuliyyətin bir neçə iştirakçı arasında bölünməsinə təmin etməyə yönəlmişdir. Tədqiqatlarda ən çox rast gəlinən metodlara sıfır bilik verməklə isbat, gizli ünvanlar, şifrələmə, vəziyyət kanalları və halqa imzaları, küyün əlavə edilməsi və s. daxildir. Bu metodların bəziləri digərlərinə nisbətən daha perspektivli olsalar da, blokçeyn texnologiyası qarşısında duran çağırışların həll edilməsi üçün bu metodların birləşdirilməsi tələb edilir.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikası Dövlət Neft Şirkətinin (SOCAR) Elm Fondunun maliyyə yardımı ilə yerinə yetirilmişdir – **Müqavilə № 23LR – AMEA.**

İSTİNADLAR

- [1] Y. İmamverdiyev "Big Data və fərdi məlumatların təhlükəsizliyi," "Big data: imkanları, multidissiplinar problemləri və perspektivləri" I respublika elmi-praktiki konfransı, pp. 109-113, 2016.
- [2] Y. İmamverdiyev "Blokçeyn texnologiyaları: komponentləri, tətbiqləri və problemləri," İnformasiya cəmiyyəti problemləri, no. 2, pp. 18–32, 2019.
- [3] Solutions for a responsible use of the Blockchain in the context of personal data. CNIL (Commission Nationale Informatique & Libertés). 2018. <https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf>
- [4] Van Eecke, P., & Haie, A. G. (2018). Blockchain and the GDPR: The EU Blockchain Observatory Report. Eur. Data Prot. L. Rev., 4, 531.
- [5] J. Alsayed Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, & K. Dahal "DNS-IdM: A blockchain identity management system to secure personal data sharing in a network", Applied Sciences, vol. 9, no. 15, Article 2953, 2019.
- [6] L.F.M. Ramos, & J.M.C. Silva "Privacy and data protection concerns regarding the use of blockchains in smart cities," In 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV2019), pp. 342-347, 2019.
- [7] M. Onik, C. Kim, N. Lee, & J. Yang, "Privacy-aware blockchain for personal data sharing and tracking", Open Computer Science, vol 9, no. 1, pp. 80-91, 2019.
- [8] D. Hawig, C. Zhou, S. Fuhrhop, A.S. Fialho, N. Ramachandran "Designing a distributed ledger technology system for interoperable and General Data Protection Regulation-compliant health data exchange: A use case in blood glucose data," Journal of Medical Internet Research, vol. 21, pp. 12, 2019.
- [9] S.C. Cha, T.Y. Hsu, Y. Xiang, & K.H. Yeh, "Privacy enhancing technologies in the Internet of Things: Perspectives and challenges," IEEE Internet of Things Journal, vol 6, no 2, Article 2159-2187, 2018.
- [10] D. Hofman, V. L. Lemieux, A. Joo, & D. A. Batista "The margin between the edge of the world and infinite possibility," Records Management Journal, no 29 (1/2), pp. 240-257, 2019.
- [11] M.N. Asghar, N. Kanwal, B. Lee, M. Fleury, M. Herbst, & Y. Qiao "Visual surveillance within the EU General Data Protection Regulation: A technology perspective," IEEE Access, vol. 7, pp. 111709-111726, 2019.
- [12] P. Hristov & W. Dimitrov, "The blockchain as a backbone of GDPR compliant frameworks," Calitatea, vol. 20, no. 1, Article 305, 2019.
- [13] N. Fabiano "Internet of Things and blockchain: legal issues and privacy. The challenge for a privacy standard." IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 727-734, 2017.

BLOCKCHAIN TECHNOLOGIES FOR PERSONAL DATA PROTECTION: OPPORTUNITIES AND PERSPECTIVES

Yadigar İmamverdiyev¹, Gunay Muradova²

^{1,2}Institute of Information Technology of ANAS,

Baku, Azerbaijan

¹yadigar@iit.science.az, ²gmuradova9@gmail.com

Abstract – The paper discusses the possibilities and prospects of using blockchain technology to protect personal data. A brief description of blockchain technology is given and an analysis of existing research is carried out. The possibilities of ensuring the security of personal data using the blockchain technology and the potential problems that arise during this are analyzed.

Keywords – *personal data, blockchain, privacy, privacy preserving, GDPR*

Fərdi məlumatların qorunması üçün proqram təminatı alətləri haqqında

Bayramova Tamilla

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
tamilla@iit.science.az

Xülasə— Məqalədə rəqəmsal iqtisadiyyata keçidlə əlaqədar fərdi verilənlərin qorunmasında yeni problemlərin yaranması şərh edilmişdir. İnformasiya mühafizəsi sistemlərinin yaradılmasına müasir yanaşmalar araşdırılmışdır. Proqram sənayesinin inkişafı ilə əlaqədar olaraq informasiyaya olan təhdidlər artdığına görə müasir şifrələmə texnologiyaları, onların tətbiq sahələri tədqiq edilmişdir. İnformasiyanın qorunması üçün intellektual sistemlərin işlənilməsinin vacibliyi vurğulanmışdır.

Açar sözlər— fərdi verilənlər, proqram təminatı, şifrələmə, informasiyanın qorunması

I. GİRİŞ

Müasir informasiya texnologiyaları şəxsi həyat anlayışı ilə bağlı təsəvvürlərdə əhəmiyyətli dəyişikliklərə səbəb olmuşdur. Gerçək dünyada baş verən hadisə və proseslər – əmtəə və xidmətlərin əldə edilməsi, yaxın adamlarla ünsiyyət, dövlət orqanları ilə qarşılıqlı əlaqə və s. virtual mühitə keçərək bir qədər fərqli mahiyyət daşımağa başlamışdır. Bunun nəticəsində insanların bilərəkdən, yaxud bilməyərəkdən açıqladığı və müxtəlif təşkilatların hədəfinə çevrilən fərdi məlumatlar misli görünməmiş miqyas almışdır. Xüsusilə, İnternet kütləvi sosial hadisəyə, cəmiyyət həyatının ayrılmaz hissəsinə çevrildikdən sonra insanlar bu texnologiyaların onların şəxsi həyatına təsirindən ehtiyat etməyə başlamışlar. Bu gün insanlar narahatdırlar ki, onların sağlamlığı, maliyyə vəziyyəti, şəxsi münasibətləri, siyasi baxışları və s. ilə bağlı kimlərsə məlumatlar toplanır [1]

İnformasiya texnologiyaları sahəsində sürətli inkişaf, Əşyaların İnternetinin, müxtəlif təyinatlı intellektual sistemlərin geniş yayılması, elektron dövlət strukturlarında elektron sənəd dövriyyəsinin formalaşması və sosial şəbəkələrdən istifadə edilməsi çox böyük sayda və həcmdə verilənlərin toplanmasına səbəb olmuşdur. Bu verilənlərin analizi və emalı problemi (toplanması, saxlanması, analizi, ötürülməsi, dəyişdirilməsi, silinməsi və s.) Big Data texnologiyalarının yaranmasına gətirmişdir. Bu verilənlərin çox böyük hissəsi konfidensial xarakter daşıyır və qəbul edilmiş normativ-hüquqi aktlar vasitəsilə qorunur. Konfidensial informasiyaya vətəndaşların fərdi verilənləri, kommersiya sirlərinə aid verilənlər, xidməti verilənlər və s. daxildir.

Cəmiyyətin həyat fəaliyyətinin bütün sahələrində proseslərin rəqəmsallaşması konfidensial informasiyanın

həcmnin artmasına və onun qorunması üzrə xidmətlər bazarının inkişafına gətirmişdir. 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 [2].

II. FƏRDİ MƏLUMATLARIN QORUNMASININ NORMATİV-HÜQUQİ ƏSASLARI

Zaman keçdikcə informasiyanın qorunma metodları və üsulları əhəmiyyətli dəyişikliyə uğramışdır. Son illərdə bu sahədə xüsusi tələblər, tövsiyələr, normativ-hüquqi aktlar və araşdırma metodikaları işlənilmişdir.

Konfidensial informasiyanın və eyni zamanda fərdi məlumatların ələ keçirilmə hallarının artması nəticəsində informasiyanın qorunmasının hüquqi normativ bazası əhəmiyyətli dəyişikliyə uğramışdır.

Yeni texnologiyaların inkişafı və internetə qoşulan intellektual qurğuların yayılması konfidensiallığın qorunmasına dair yeni qanunların qəbul edilməsini labüd etmişdir. 2018-ci ildə belə qanunlardan biri **Fərdi məlumatların mühafizəsi üzrə Ümumi Qanun** (General Data Protection Regulation – GDPR) qüvvəyə minmişdir. Bu Avropa Birliyi (AB) və Avropa İqtisadi fəzası vətəndaşlarının fərdi verilənlərinin konfidensiallığı və qorunması haqda qanundur. GDPR-in əsas ideyası aşağıdakılardan ibarətdir [3]:

- ✓ fərdi verilənlərin qorunması;
- ✓ insanların məlumatlarının qorunma hüququnun və azadlıqlarının qorunması;
- ✓ Avropa Birliyi çərçivəsində fərdi verilənlərin yayılmasına məhdudiyyət qoyulmasından ibarətdir.

GDPR-in məqsədləri:

- ✓ Fiziki şəxslərə onların fərdi verilənlərinə nəzarət etmək üçün instrumental vasitələrin verilməsi;
- ✓ Fərdi verilənlərin qorunması üzrə müasir standartların tətbiq edilməsi;
- ✓ AB-nin fərdi verilənlərin qorunması üzrə rəqəmsal fəzasının inkişaf etdirilməsi;

- ✓ AB-yə üzv dövlətlərin səlahiyyətli orqanları daxil olmaqla bütün iştirakçılar tərəfindən qaydalara ciddi şəkildə əməl edilməsinin təmin edilməsi;
- ✓ Fərdi məlumatların beynəlxalq səviyyədə ötürülməsinə hüquqi dəstək verilməsi.

GDPR qanunu AB ərazisində və ondan kənarda fiziki və ya hüquqi şəxslər, dövlət orqanları və digər müəssisə və təşkilatlar tərəfindən AB vətəndaşlarının fərdi məlumatlarının tam və ya qismən avtomatlaşdırılmış emalı ilə əlaqəli hər hansı bir fəaliyyət (hətta qeyri-kommersiya fəaliyyəti də) GDPR-ə tabedir. AB vətəndaşlarına təmənnasız xidmət göstərilərsə, həmin xidmət də bu qanunun fəaliyyət sahəsinə düşür. Məsələn, əgər onlar İnternetdə qeydiyyatdan keçərək hər hansı bir saytın təmənnasız xidmətindən istifadə edərsə və fərdi məlumatlarını daxil etmiş olarsa, GDPR qanunları onlara da aid edilir.

GDPR-in tələblərinə uyğun gəlmək üçün şirkətlər aşağıda göstərilənləri nəzərə almalıdır:

- ✓ Layihəyə hansı fərdi verilənlərin toplanacağı, onların harada və necə qorunacağı və istifadə ediləcəyi əvvəlcədən müəyyən edilməlidir. Əgər bu verilənlər əsasında konkret insanı identifikasiya etmək olursa şirkət bu qanunun fəaliyyət dairəsindən kənarda qalır.
- ✓ Fərdi verilənlərin istifadəsinə nəzarət edilməlidir və müəyyən edilməlidir ki, onları kim, necə, harada və niyə emal edir.
- ✓ Fərdi verilənlərin mühafizə mexanizmləri işlənilməlidir.
- ✓ GDPR qanunlarına uyğun olaraq hesabatlar hazırlanmalıdır.

GDPR şərtlərinə əhəmiyyət verməyən şirkətlər 20 milyon avro və ya müəssisənin illik gəlirinin 4%-ə qədər məbləğində cərimə edilə bilər. Cərimənin məbləği müxtəlif amillərdən (qanun pozuntusunun dərəcəsi, səhlənkarlıq və ya qəsdən törədilməsi, zərər çəkənlərin sayı, onlara dəyən ziyan və s.) asılıdır.

Azərbaycanda bu sahədə əsas qanun 2010-cu ildə qəbul edilən “Fərdi məlumatlar haqqında qanun”dur [4].

İstifadəçilərin konfidensiallığını qorumaq və GDPR qaydalarına uyğunluğa nail olmaq üçün bir sıra müasir proqram vasitələri işlənilmişdir. Müəssisədə belə proqram vasitələrinin tətbiqi baha başa gəlir. Lazım olan proqram təminatını seçərkən təşkilatın ölçüsünü, verilənlərin konfidensiallığının nə qədər vacib olduğunu və konfidensiallığın pozulmasının müəssisəyə vuracağı zərərin potensial dəyərini nəzərə almaq lazımdır [5].

Verilənlərin sızmasının qarşısını almaq üçün avtomatlaşdırılmış korporativ siyasətin həyata keçirilməsi mühafizə olunan verilənlərin təşkilatdan kənara çıxmadan aşkar etmək lazımdır. Belə vasitələr verilənlərin itirilməsinin qarşısının alınması (*Data Loss Prevention – DLP*) vasitələri adlanır.

III. İNFORMASIYANIN MÜHAFİZƏSİ VASİTƏLƏRİ

2009-cu ildə Avropa İstehlakçı Hüquqlarını Müdafiə Komissarı Meglena Kuneva fərdi şəxslərə aid məlumatların rəqəmsal iqtisadiyyatda necə vacib bir hala gəldiyini göstərmək üçün şəxsi məlumatları neftlə müqayisə etmişdir. Hər gün dünyada insanlar 196 milyard elektron poçt göndərir və ya qəbul edir, Twitter-də 500 milyondan çox tvit göndərir və Facebook-da 4,75 milyard müxtəlif məzmununda məlumat paylaşır [6].

Konfidensial informasiyanın emal edilmə prosesində əlyətərliyi olmayan kənar şəxslər tərəfindən informasiyanın əldə edilməsi və qanundan kənar məqsədlər üçün istifadə edilməsi neqativ hallara gətirir, bəzən isə fəlakətə nəticələnə bilər. Ona görə də informasiya mübadiləsi və emalı üçün elə şərait yaratmaq lazımdır ki onun qeyri-qanuni istifadəsinin qarşısını almaq mümkün olsun. Bu yeni problem deyil informasiyanın toplanması və saxlanılmasına başlanılan vaxtdan onun qorunması əsas məsələlərdən biri olmuşdur. İnformasiyanın qorunması aktual problemə çevrilmişdir və əsasən aşağıda göstərilənləri nəzərdə tutur:

- İnformasiyaya icazəsiz girişin (və ya icazəsi olmayan digər şəxslərə ötürülməsinin) qarşısının alınması;
- İnformasiyaya icazəsiz giriş faktlarının vaxtında aşkar edilməsi;
- İnformasiyaya giriş qaydasının pozulmasının neqativ nəticələri haqda xəbərdarlıq edilməsi;
- İnformasiyanın emal edilməsinin texniki vasitələrinin fəaliyyətini pozan təsirlərə imkan verilməməsi;
- İcazəsiz giriş nəticəsində dəyişdirilmiş və ya silinmiş informasiyanın dərhal bərpa edilməsi;
- İnformasiyanın etibarlı şəkildə qorunmasına daimi nəzarətin olması.

Fərdi məlumatların təhlükəsizliyinə cavabdeh təşkilatlar adətən aşağıda verilmiş de-identifikasiya üsullarından istifadə edirlər [7]:

- ✓ Anonimləşdirmə (anonymization) – verilənlərin anonimləşdirilməsi zamanı fərdi məlumatlara aid atributlar (ad, ünvan və sosial təhlükəsizlik nömrələri və s.) elə silinir və ya dəyişdirilir ki, bu verilənlər əsasında hər hansı bir şəxsi müəyyən etmək mümkün olmur. Ona görə də belə məlumatların yenilənməsi, bir neçə mənbədən alınmış verilənləri birləşdirmək mümkün deyil.
- ✓ Pseudonimləşdirmə (pseudonymization) – təxəllüsün verilməsi zamanı da fərdi məlumatlara aid atributlar silinir və ya dəyişdirilir. Lakin bu üsulda dəyişdirilmiş verilənlər şəxsin gizli təxəllüsü altında yadda saxlanılır. Anonimləşmədən fərqli olaraq bu verilənlər dəyişdirilə bilər, müxtəlif vaxtlarda alınmış məlumatlar birləşdirilə bilər.

- ✓ Açar-kodlaşdırma (key-coding) – açarla kodlaşdırma fərdi məlumatları kodlaşdırır və onların dekodlaşdırılması üçün açar yaradır.
- ✓ Şifrələmə (encryption) və s.

IV. FƏRDİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİNİ TƏMİN EDƏN MÜASİR TEXNOLOGİYALAR

Diferensial gizlilik metodu fərdi məlumatlara müraciətləri alqoritm və interfeys (etibarlı kurator kimi çıxış edir) vasitəsilə idarə edir [8]. Tədqiqatçı verilənləri analiz etmək üçün kuratora sorğu göndərir və kurator da təsadüfi küy əlavə etməklə verilənlərin konfidensiallığını qorumağa və eyni zamanda sorğulara düzgün cavab verməyə çalışır [7].

Homomorf şifrələmə şifrələnmiş məlumatlarla şifrini bilmədən və onları deşifrə etmədən işləməyə imkan verir. Homomorf şifrələmədə istifadəçi verilənlərini şifrələyir və sonra buludda yadda saxlayır. Bulud xidmətləri göstərənlər isə əslində hansı informasiyanın saxlanıldığını bilmir. Əgər istifadəçi yeni verilənlər əlavə etmək istəyərsə o, homomorf şifrələmənin additiv və multiplikativ xüsusiyyətlərindən istifadə edə bilər. Adi şifrələmədə verilənlərlə işləmək üçün onu deşifrə etmək lazımdır, bu zaman informasiyanın bədənyyətli insanların əlinə keçmə ehtimalı artmış olur. Homomorf şifrələmə vasitəsilə şifrələnmiş mətn üzərində əməliyyatlar (toplama, çıxma birləşmə, kəşimə) aparmaqla adekvat nəticələr almaq olar. Məsələn, elektron seçkilərdə (seçicilərin anonimliyini qorumaqla səsleri hesablamaq), bulud hesablamalarında, mühafizə olunan bazalarda axtarış (məzmunu analiz etmədən nəticənin alınması) və s. sahələrdə tətbiq edilə bilər [9].

Homomorf şifrələmə ideyasının 40 il əvvəl yaranmasına baxmayaraq ancaq 2009-cu ildə tam homomorf sistem IBM şirkətində işlənmişdir [10]. Lakin belə sistemlərin məhsuldarlığının aşağı olması onların real həyatda aktiv tətbiqini məhdudlaşdırır.

Funksional şifrələmə – şifrələnmiş məlumat əsasında müəyyən f funksiyasının qiyməti hesablanır: m açıq məlumatının şifrələnmiş mətninə əsasən $f(m)$ hesablanır, bu zaman m haqqında (o cümlədən, f -in hesablanması zamanı aralıq nəticələr haqqında) hər hansı əlavə məlumat əldə etmək mümkün olmamalıdır [4]. Funksional şifrələmə 2005-ci ildə təklif edilmişdir və açıq açarlı şifrələmə ideyasına əsaslanır. Funksional şifrələmədə şifrələnmiş verilənlər deyil, şifrələnmiş funksiya ötürülür. Burada da homomorf şifrələmədə olduğu kimi verilənlər tam deşifrəlmir. Bu sxemi proqram təminatının bədənyyətli tərəfindən analiz olunmasının qarşısını almaq üçün tətbiq etmək olar. Proqram kodunun funksional şifrələnməsindən sonra funksionallığına görə eyni, lakin analiz üçün əlverişli olmayan ilkin kodu alırıq. İntellektual mülkiyyəti qorumaqla yanaşı funksional şifrələmədən bulud hesablamalarında da istifadə etmək olar [8].

Funksional şifrələmənin öyrənilməsi kriptografiya sahəsində texnologiyaların inkişafına və daha güclü alətlərin və metodların yaranmasına səbəb olmuşdur [11, 12]

Bal şifrələməsi (Honey Encryption). Əlavə aldadıcı resurs yaratmaqla bədənyyətli məqsəddən yayındırır. Honey pots serverləri yaradılır, burada doğruya oxşar sadə şifrələnmiş resurslar yerləşdirilir. Ona görə “bal” şifrələməsi deyil ki, kriptanalitik mətni deşifrə etmək istədikdə o, əhəmiyyətsiz, aldadıcı bir məlumat alır və başa düşür ki, aldığı real informasiya deyil. Bal şifrələməsində əsl şifrələnmiş mətni ancaq açarı bildikdə deşifrə etmək olur. Şifrələmənin bu növü daim təkmilləşdirilir və geniş yayılmaqdadır [13].

DNT şifrələmə. Hesablamalar, verilənlərin yadda saxlanması və kriptografiyada tətbiq etmək üçün DNT molekullarına məxsus olan enerji səmərəliliyi, paralellik, informasiyanın qeyri-adi dərəcədə sıxlığı araşdırılmışdır və onun əsasında yeni texnologiyalar işlənmişdir. 1994-cü ildə Leonard Adleman (RSA alqoritminin müəlliflərindən biri) DNT molekullarının xüsusiyyətlərindən kriptografiyada istifadə edilməsini təklif etmişdir. DNT-şifrələmə kriptografiyanın yeni sahəsidir. Mürəkkəb bioloji proseslərə əsaslanması və mürəkkəb kriptografik hesablamalar verilənlərin iqlat mühafizəsini təmin edir. Təhlükəsizlik analizi göstərmişdir ki, bu şifrələmə sxemi çox yüksək konfidensiallığı təmin edə bilər [14, 15].

İnformasiyanın musiqi vasitəsilə kodlaşdırılması. MusicXML formatında yazılan musiqi akkordlar adlanan 2-4 saniyəlik kiçik fraqmentlərdən ibarətdir. Şifrələmənin mahiyyəti simfoniya vasitəsilə ondan ibarətdir ki, bu akkordlar bir simvolla əlaqələndirilir və cədvəldə yazılır. Belə şifrələnmiş məlumat açıq kanalla ötürülə bilər [16].

V. DİFERENSİAL GİZLİLİK METODUNUN TƏTBİQ SAHƏLƏRİ

Verilənlərin intellektual analizi sistemlərində (vəb-axtarış, tövsiyə sistemləri, kraudsorsinq platformaları, analitik proqramlar və s.) istifadəçilərin konfidensiallığını qorunması əsas tələbdir. Aşağıda diferensial konfidensiallığın tətbiq etməklə istifadəçilərin konfidensiallığını qoruyan bir neçə aparıcı sistemlər göstərilmişdir:

- ✓ Google şirkətinin tətbiqi – RAPPOR sənayedə diferensial konfidensiallığın geniş yayılmış ilk tətbiqidir. RAPPOR (Randomized Aggregatable Privacy-Preserving Ordinal Response – konfidensiallığı qoruyan, təsadüfi yığıla bilən nizamlı cavab) istifadəçinin verilənlərinə ümumilikdə baxmağa imkan verir, lakin onun ayrı-ayrı detallarını analiz etməyə imkan vermir. RAPPOR kliyent proqram təminatıdır, istifadəçinin statistikasını toplayan yeni mexanizmdir və təsadüfi cavablandırma metodlarından istifadə edərək konfidensiallığı etibarlı şəkildə təmin edir [17].
- ✓ Apple iOS 11/macOS əməliyyat sistemində öz proqramlarında məxfiliyi qorumaq üçün diferensial konfidensiallıq metodundan istifadə etmişdir [18]. Verilənlərə əlavə edilmiş statik küy istifadəçilərin fərdi verilənlərini maskalayır və konfidensiallığı qoruyur. Aşağıda göstərilən funksiyalarda tətbiq

edilmişdir: QuickType; Emoji; Safari; Sağlamlıq haqda məlumat (*Health Type Usage*).

- ✓ LinkedIn sosial şəbəkəsində də konfidensiallığın qorunması üçün diferensial konfidensiallıqdan istifadə edilir. LinkedIn Salary tədqiqatçıları, iş axtaranlar və gənc kadrlar üçün informasiyanın toplanması və təqdim edilməsi üçün kraudsorsinq sistemidir [19].
- ✓ Microsoft Windows telemetriyasının toplanması üçün lokal diferensial konfidensiallıq təminatını tətbiq edir. Windows olan milyonlarla qurğularda statistik məqsədlərlə toplanan informasiyanın konfidensiallığını qorumaq üçün diferensial konfidensiallıqdan istifadə edilir [20].

NƏTİCƏ

Verilənlərin konfidensiallığını qorumaq üçün adları çəkilən proqram vasitələrinin heç biri informasiyanı tam olaraq qoruya bilmir. Son illərdə informasiyanın qorunması üçün intellektual sistemlərin işlənilməsinə başlanılmışdır. Əsas diqqət şəxsiyyətin identifikasiyası üçün biometrik sistemlərin qurulmasına, icazəsiz girişin avtomatik müəyyən edilməsi və qarşısının alınması, informasiya risklərinin analizi və idarə edilməsinə yönəlmişdir. Bu sinif informasiya sistemlərinin yaradılması zamanı neyron şəbəkələr, süni immun sistemləri, qeyri-səlis məntiq və s. kimi soft-kompüter texnologiyalarından istifadə edilməsi fərdi məlumatların daha etibarlı qorunmasını təmin edə bilər.

Kvant kompüterlərinin yaranması mövcud kriptografiya texnologiyalarının sonu ola bilər. Ona görə də kvant mexanikasının imkanlarından istifadə etməklə kvant kriptografiya metodlarının işlənilməsi gələcəyin ən aktual problemlərindən biri ola bilər.

İSTİNADLAR

- [1] R.Ş. Mahmudov “Big Data erasında fərdi məlumatların hüquqi rejiminin müəyyənəşdirilməsi problemləri,” *İnformasiya cəmiyyəti problemləri*, 2018, №2, 28–33
- [2] В. Кияев, О. Граничин. Безопасность информационных систем. Открытый Университет «ИТУИТ». 2016. с. 192.
- [3] “General Data Protection Regulation”<https://gdpr-info.eu/>
- [4] “Fərdi məlumatlar haqqında Qanun” <http://www.e-qanun.az/framework/19675>
- [5] M..Hansen, A.Lehmann, D.Whitehouse, S.Fischer-Hübner, L.Fritsch, C.Raab. Data Protection by Design and by Default à la European General Data Protection Regulation. Privacy and Identity Management. Facing up to Next Steps. Privacy and Identity 2016. IFIP Advances in Information and Communication Technology, vol 498. Springer, Cham.
- [6] S. Spiekermann, A. Acquisti, R. Bohme, Kai-Lung Hui. The challenges of personal data markets and privacy, *Electron Markets*, 2015, Vol. 25, Issue 2, pp 161–167.

- [7] Y. İmamverdiyev. “Big Data və fərdi məlumatların təhlükəsizliyi,” “Big data: imkanları, multidissiplinar problemləri və perspektivləri” I respublika elmi-praktiki konfransı, 2016, s.
- [8] M. U. Hassan, M. H. Rehmani, & J. Chen “Differential privacy techniques for cyber physical systems: A survey,” *IEEE Communications Surveys & Tutorials*, 2019, pp. 1–46. doi:10.1109/comst.2019.2944748
- [9] Jigar M. Shah, H. Kothadiya. “A survey on homomorphic encryption techniques in cloud computing,” *International Journal of Advance Engineering and Research Development*, Vol. 2, No 2, 2015.
- [10] N. Mohammed, R. Chen, B. C. M. Fung, and P. S. Yu. Differentially private data release for data mining, *Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (SIGKDD)*, pp. 493-501, 2011
- [11] C. Gentry, C. Peikert and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, 2008, pp. 197–206
- [12] D. Cash, D. Hofheinz, E. Kiltz and C. Peikert. Bonsai trees, or how to delegate a lattice basis. In *EUROCRYPT*, 2010, pp. 523–552
- [13] S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices. In *EUROCRYPT*, 2013, pp. 1–17
- [14] N.S. Noorunnisa, K. R. Afreen. Review on Honey Encryption Technique, *International Journal of Science and Research (IJSR)*, Vol. 5, Issue 2, 2016, pp.1683-1686.
- [15] G. Cui, L. Qin, Y. Wang and X. Zhang. An encryption scheme using DNA technology, *3rd International Conference on Bio-Inspired Computing: Theories and Applications*, 2008, pp. 37-42.
- [16] М. Гриффин. Хранение мировой информации в обувной коробке, *Fanatical Futurist*, 2016.
- [17] Богданов М.Р., Габитов И.А. Кодирование текста с помощью музыки, *IT & Transport / ИТ & Транспорт: сб. науч. статей, Самара: Интелтранс*, 2018, Т.10, стр. 89-96
- [18] H. Haddadi, *Privacy-Preserving Analytics: The Browser nightmares*, <https://haddadi.github.io/>
- [19] *Differential Privacy*, https://www.apple.com/ru/privacy/docs/Differential_Privacy_Overview.pdf
- [20] K. Kenthapadi, I. Mironov, A. Guha Thakurta. Privacy-preserving Data Mining in Industry, *Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining*, 2019, pp. 840-841.

ABOUT SOFTWARE TOOLS FOR PERSONAL DATA PROTECTION

Tamilla Bayramova

Institute of Information Technology of ANAS, Baku, Azerbaijan

tamilla@iit.science.az

Abstract— The article describes new challenges in protecting personal data related to the transition to the digital economy. Modern technologies for information protection have been investigated. Due to the increasing threats to information as software industry evolves, modern encryption technologies and their application areas have been explored. The importance of the use of intellectual systems for the protection of information was emphasized.

Keywords— *personal data, software, encryption, data protection*

Философский аспект влияния информационных технологий на общественное развитие

Самира Дадашова

Институт Философии НАНА, Баку, Азербайджан
samira_889_87@mail.ru

Аннотация— В данной статье рассмотрены наиболее важные социальные проблемы современного общества, вызванные информационными воздействиями на индивидуальное и общественное сознание. Цель заключается в том, чтобы обратить внимание научного сообщества на философский аспект данной проблемы и ее нравственно-этическую составляющую.

Ключевые слов— информационные технологии, личность, манипуляция сознанием, этика

I. ВВЕДЕНИЕ

Подвергая философскому осмыслению современную стадию научно-технической революции, ученые обозначали нынешний век как эпоху информации и исследований возможностей мозга. Новыми орудиями, которыми человек совершенствует внутреннюю и внешнюю природу оказались нано-, инфо- и биотехнологии, и основа всего – квантовая теория. Уже сегодня квантовая теория привела современное общество к лазерной и цифровой революции. Однако наука как двухсторонний нож, порождает не меньше проблем, чем решает: новые возможности граничат с возрастающими опасностями для самого человека. Потому проблематичность человеческого бытия с каждым годом, с каждым новым открытием в науке приобретает новые параметры. Развитие технологий, в том числе и информационных, создало условия для улучшения качества жизни, но в то же время, явилось предпосылкой для более изощренной эксплуатации физических и умственных способностей человека, для манипуляции сознанием. В результате формируется идеология постмодернистской морали с тотально прагматическим отношением к человеку, блокирующее его право на индивидуальное своеобразие и свободу. Притом, чем большей информацией о человеке мы владеем, тем меньше у него свободы, а стало быть, тем в большей опасности он находится. Не удивительно, что на этапе стремительного развития информационного социума существенный характер приобретают проблемы обеспечения информационной неприкосновенности границ частной жизни как некоего неотъемлемого элемента свободы индивида.

II. ОСНОВНАЯ ЧАСТЬ

Российский философ В. Кутырев в переходе к компьютерно-информационному обществу, или Техносу, как он его называет, видит подлинный кризис гуманизма, ибо происходит замена предметной среды обитания человека – виртуальной, вещей – симулякрами, духовности – расчётом, культуры – технологиями[1]. Неслучайно сегодня большой резонанс вызывают вопросы регулирования этико-правовых аспектов новейших технологий. Становление компьютерного века и информационного общества находят растущую конвергенцию в трансформации и коммодификации человека. Однако будут ли новейшие технологии иметь нежелательные последствия зависит от нашего морального принципа непричинения вреда человеку и обществу. Сложность оценки технологий заключается в том, что большинство из них не были созданы с дурными целями. Но, как и всякая новая технология, будучи «улучшением», неизбежно несет в себе смысл выхода за пределы того, что существует в определенный момент, будь то определенное положение вещей, или функция тела, или общее ограничение, встроенное в человеческую природу. Так произошло и с технологией чипирования, успешно применяемой в некоторых странах Запада, и, в особенности, в США и Швеции. Технология чипирования, созданная для терапевтических и диагностических целей, преодоления конкретных физических или психических недостатков индивидов (например, проверка уровня сахара в крови, давления и т.д.), порой выходит за рамки медицины: немалую обеспокоенность чипирование вызывает тем, что подобная практика поставит под угрозу неприкосновенность частной жизни и личных данных человека, поскольку микрочип содержит биометрическую информацию о самом носителе, а также его платежных картах и пропусках. И самый большой риск заключается в том, что со временем количество данных на чипах будет увеличиваться, поэтому людям станет все сложнее защищать свою персональную информацию. Основным аргументом в этой связи является апелляция к объективному ходу событий, к «прогрессу». Физик-теоретик С. Хокинг заявил, что человек не в состоянии «остановить прогресс или обратить вектор его движения, поэтому мы должны признать его опасности и

контролировать их»¹. Но, как оказалось, контролировать прогресс куда сложнее, чем способствовать ему. Этическое право на соблюдение безопасности личной жизни, будучи юридическим воплощением принципа невмешательства в личные дела каждого, то есть выражением суверенитета человека, представляет собой очень хрупкое общественное завоевание, которому стабильно угрожают социальные и политические катаклизмы, а также огромные возможности контроля и управления, появившиеся в ходе информационного прогресса.

Сегодня информационно-коммуникационные технологии проникают во все сферы жизнедеятельности человека, открывая безграничные просторы как для возможностей и совершенствования, так и для злоупотреблений и нарушения прав. Более того, обмен информацией является одним из стратегических компонентов развития каждой страны[2]. Потому несомненно, что в данных условиях проблема информационной безопасности приобретает выраженную актуальность. Феномен информационной опасности имеет множество форм своего проявления: от манипулирования сознанием и поведением людей, сознательной или неосознанной подмены ценностей и целей, до информационной войны и информационного терроризма. Эти процессы, прежде всего, обусловлены отношением людей к информации, потребности в ней и способности различать истинное и ложное, полезное и бесполезное. В новом информационном обществе, где человек зачастую обменивает «быть» на «казаться», границы между дозволенным и неприемлимым стираются, негативные процессы могут маскироваться в объективно-нейтральные формы своей реализации. В результате такой «подмены», человек не только не может сохранить свою идентичность, но и не в состоянии адекватно воспринять и осмыслить вызовы, угрожающие обществу.

Человек ежедневно подвергается агрессивному информационному воздействию, которое помимо его воли влияет на психику, индивидуальное и общественное сознание, в том числе на устойчивость личных и морально-психологических качеств. Только личность устойчивая способна произвести критический анализ, дать оценку воспринимаемой информации и принять объективное решение на основе этой информации. Вопрос о формировании себя как личности, а также проявлении себя в ходе самоопределения приобретает принципиальное значение в обществе информационного типа, ибо зависимость от информации «убивает» зависимость от коммуникации в форме настоящего личностного общения. Наряду с этим, расширение информационных технологий уверенно влечет за собой унификацию идеалов и взглядов, подавление всякого проявления индивидуализма и личности. Происходит «омассовление» культуры. Новая массовая культура, доставшаяся нам от XX в., есть культура потребления или консьюмеризма, идущая под девизом «чем больше вещей

и информации человек потребляет, тем больше он значит». В действительности же человек утратил чувство индивидуальности и самооценности, превратившись в живой ресурс для достижения внешних, зачастую коммерческих целей. И, как следствие, мы имеем утрату веры в человека, в самого себя, в собственные силы. Уже во второй половине XX столетия мыслители (Э. Фромм, Ж. Бодрийяр, Х. Ортега-и-Гассет и др.) высказали мнение о том, что стремление к покорению природы и обретению власти превратит человечество в стадо потребителей – «стадо, верящее, что дорога, по которой мы идем, непременно приведет нас к желаемой цели, ибо мы видим, что и другие идут по той же дороге»². В свою очередь, социальное развитие того или иного общества, как и его национальная безопасность во многом определяются тем, какое ценностное и культурное содержание преобладает в данном информационном пространстве. Заявление А. Швейцера о том, что человек «подчиняет свое суждение суждению массы и свою нравственность нравственности массы»³, не теряет своей актуальности и по сей день. Ведь когда общество воздействует на индивида сильнее, чем индивид на общество, начинается деградация культуры, происходит деморализация общества, и оно становится дееспособным в понимании и решении стоящих перед ним задач и проблем. В подобных «несвободных» условиях нас не привлекает возможность быть личностью, мы неосознанно все охотнее подвергаем себя риску превратиться в человека-вещь, чувствуя себя в безопасности. В этом и состоит парадокс информационного общества: иллюзорное ощущение безопасности скрывает реальную угрозу самой человеческой природе. Эта проблема есть данность, которую необходимо решить человеку XXI в. На повестке сегодняшнего дня стоит технологизация всего и вся, вплоть до процессов творчества, его замены алгоритмами деятельности и программирования.

Информационные технологии меняют не только способы умственного и физического труда, но и способы коммуникации. Индивид социализируется, все более отчуждаясь, «идея человека» распадается, и человечество сталкивается с угрозой эмансипации, творческой деятельности и всякой критической способности в обмен на свои «системные» цели и средства. Хотя на первый взгляд отчужденность может показаться несколько далеким от процессов социализации, но на самом деле эти явления выступают как составные аспекты глобализирующегося и меняющегося общества[3]. Таким образом, парадоксальная аномалия информационного века заключается в том, что он породил два разноплановых скачка: к интеграции человечества как социальной общности, связанной всемирной сетью, и к дезинтеграции определенного общества как такового. На смену «живому» человеку приходит «виртуальный», в связи с чем возрастает его волнение о своей экзистенции; человек стремится найти выход из духовного одиночества и

² Фромм Э. Гуманистический психоанализ / под ред. В. Лейбина. СПб.: Питер, 2002. 544 с.

³ Швейцер А. Культура и этика. М.: Прогресс, 1973. 344 с.

¹ Hawking S. A Brief History of Time. London: Bantam, 2011. 256 p.

вырождения, но даже это стремление обречено быть техническим, ибо он ищет «технологию» приобретения друзей и власти, «технологию» счастья и успеха. Человек уверен в своей свободе, безусловной способности творить себя, не понимая, что творение это происходит по уже определенным запрограммированным стандартам, ибо человек растворяется в новой реальности – реальности software.

ЗАКЛЮЧЕНИЕ

Таким образом, информационное общество порождает огромное количество этических вопросов, которые находят свое отражение, как в морали социума, так и в нравственности каждого отдельно взятого человека. Несмотря на то, что глобализация информации способствует взаимному обогащению народов, обеспечивает мгновенный доступ к информации в любой точке мира, она также размывает границы материального, цифрового и биологического миров. Проблемы информационной безопасности общества, в которых прослеживается перевод коммуникаций из сферы непосредственного контакта в сферу, опосредованную технологиями коммуникации, выходят далеко за рамки традиционных вопросов безопасности и затрагивают абсолютно все сферы жизни человека. Возникает острая необходимость в сохранении ценностей демократического общества, основанного на принципах взаимного уважения и соблюдения прав человека. В свою очередь, обеспечение информационной безопасности – это перманентный и комплексный процесс, включающий правовые, организационно-технические, политические и социально-культурные средства и методы. В связи с этим, анализ процессов научного познания не следует ограничивать исследованием его методологических, гносеологических, и логических оснований. Необходима разработка также аксиологического базиса. Формулируемые философией гуманистические и социально-этические принципы непосредственно должны быть вовлечены в сам процесс

познания, выполняя регулятивную функцию на всех его стадиях. В данном контексте существенным является изучение взаимодействия информации и морали на гетерогенных структурно-функциональных уровнях социума, в том числе в процессе совершенствования человека и преодоления этического коллапса информационной неприкосновенности его частной жизни. При этом следует учесть, что интенсивная динамика развития информационных технологий постоянно привносит новые элементы в содержание рассматриваемых проблем, что делает особенно актуальными исследования, посвященные анализу современных этико-информационных вопросов.

ЛИТЕРАТУРА

- [1] В. Кутырев, «Последнее целование. Человек как традиция». СПб.: Алетейя, 2015. 312 с.
- [2] “Ənənəvi mediadan internet mediaya doğru: problemlər, çağırışlar”. Bakı: “Elm və təhsil”, 2016. 160 s.
- [3] F. Xudanlı, “Frankfrut məktəbinin sosial fəlsəfəsi”. Bakı: Renessans-A, 2014. 180 s.

PHILOSOPHICAL ASPECTS OF THE IMPACTS OF INFORMATION TECHNOLOGY ON SOCIAL DEVELOPMENT

Samira Dadashova

Institute of Philosophy of ANAS, Baku, Azerbaijan

samira_889_87@mail.ru

Abstract– This article discusses the most important social problems of modern society, caused by informational impacts on individual and public consciousness. The goal is to draw the attention of the scientific community to the philosophical aspect of given problem and its moral component.

Keywords– information technology, personality, manipulation of consciousness, ethics

Akustik kanallarla ötürülən nitq informasiyasının təhlükəsizliyinin bəzi vibroakustik mühafizə metodları haqqında

Bikəs Ağayev¹, Tərən Əliyev², Kövsər Əliyeva³, Məleykə İbişova⁴
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
^{1,2,3,4}depart6@iit.sciense.az

Xülasə— Məqalədə otaq şəraitində aparılan və müəyyən məxfiliyə malik danışıqlar prosesinin nitq informasiyasının təhlükəsizlik məsələləri araşdırılır. Akustik kanallarla ötürülən nitq informasiyasının iştirakçılar tərəfindən diktofonla gizli yazılması və otaqdan kənara sızan vibroakustik siqnalların ilkin vəziyyətinin əldə edilməsinə qarşı mühafizə metodlarına baxılır. Baxılan hallar üçün təşkilatın informasiya təhlükəsizliyi siyasətinin müəyyənəşdirilməsi istiqamətində təkliflər verilir.

Açar sözlər— nitq informasiyası; akustik yayılma kanalı; danışıqların gizli yazılması; vibroakustik sızma kanalları; informasiya təhlükəsizliyi; nitq informasiyasının mühafizəsi

I. GİRİŞ

İnsanlar arasında ünsiyyət əsas etibarilə danışıqlar, nitq informasiyası vasitəsilə həyata keçirilir. Bu ünsiyyət istər birbaşa danışıqlar, yəni akustik kanallarla, istərsə də texniki vasitələrdən istifadə etməklə elektromaqnit, elektroakustik, vibroakustik, elektrooptik və s. kanallarla həyata keçirilə bilər. Bu danışıqların məzmununda adi məişət məsələlərinə aid məlumatlardan tutmuş şəxslərin fərdi məlumatları, təşkilatın maliyyə və kommersiya sirləri, elmi tədqiqatların nəticələri, hərbi və dövlət sirləri və s. yayılması arzu olunmayan və ya qanunla qadağan olunmuş məlumatlar ola bilər. Burada danışıqların məzmununa münasibətdə maraqları əks olan iki tərəf var: məlumatların digərlərinin əlinə keçməməsində maraqlı olan danışıq iştirakçıları və bu danışıqları əldə etməklə ondan qərəzli məqsədlərlə istifadə etməyə çalışan digər şəxslər. Texnika və texnologiyaların hazırkı inkişaf səviyyəsində hər iki tərəfin maraqlarını təmin etməyə imkan yaradan çoxlu sayda mükəmməl texnologiyalar, texniki vasitələr, metodlar yaradılsa da onların tətbiqi zamanı bir sıra çətinliklərlə üzləşirlər. Bu ilk növbədə təşkilatın informasiya təhlükəsizliyi siyasətinin, təhlükəsizliyi təmin edən mühafizə taktikasının düzgün formalaşdırılmasından, o cümlədən mühafizə məqsədilə düzgün texniki həll variantının seçilməsindən asılıdır. Digər tərəfdən təşkilat rəhbərliyinin informasiya mühafizəsi problemləri və onların həlli yolları haqqında bilik səviyyəsi və məsələyə münasibəti, təşkilatın maliyyə imkanları və s. informasiya təhlükəsizliyi tədbirlərinin həyata keçirilməsinə təsir edən amillərdəndir.

Göründüyü kimi nitq informasiyasının təhlükəsizliyinin təmin edilməsi hər bir fərd, təşkilat və dövlət üçün aktual və əhəmiyyətli məsələdir.

Məqalədə yalnız otaq şəraitində aparılan danışıqların akustik kanalla ötürülməsi halında nitq informasiya axınının təhlükəsizliyi məsələlərinə baxılmışdır. Burada otaq dedikdə təşkilat rəhbərinin iş otağı, məşvərət otağı, strateji fəaliyyət sahələrinin, xüsusi xidmət sahələrinin, idarəetmə orqanları kimi mühüm qurumların iş yerləri, əraziləri ola bilər.

II. SƏS VƏ KÜY HAQQINDA QISA ŞƏRH

Nitq informasiyasının təhlükəsizliyinin təşkilinə aidiyyətli olan hər bir şəxs səsin mahiyyəti, yayılması və qəbulu haqqında minimal məlumatlara malik olmalıdır. Səs havada (qazvari mühitdə) bərk cisimlərdə və mayelərdə dalğalar şəklində yayılan elastik mühitin hissəciklərinin rəqsi hərəkəti nəticəsində yaranır. Səs, o cümlədən nitq dalğaları enerji daşımaqla qarşılaşdığı maneədə müəyyən təzyiq yaradır. Əgər bu təzyiqin qiyməti yayılma mühitinin təzyiqindən, məsələn atmosfer təzyiqindən böyükdürsə müəyyən intensivliyə malik səs yaradır. Bu maneə qulaq pərdəsidirsə biz, dalğa enerjisinin yaratdığı təzyiqi subyektiv olaraq səs hissi kimi qəbul edirik. Bu səs gücü (intensivliyi) və tezliyi ilə xarakterizə edilir. Otaqda danışıqların, hərəkət edən cisimlərin və s. mənbələrin yaratdığı səs dalğalarının enerjisinin bir hissəsi istənilən maneədən əks edərək ətrafa yayılır, bir hissəsi maneə tərəfindən udulur, digər hissəsi isə maneədən keçərək əks tərəfə yayılır (şəkil 1).

Şəkil 1. Səs dalğalarının maneə ilə qarşılıqlı təsiri

1-əks edən, 2-udulan, 3-nüfuz edən hissələr, 4-maneə (divar), 5-səs mənbəyi

İnsan qulağının eşitməsi üçün səs qulaqda yaratdığı təzyiqin səviyyəsi nisbi qiymətlərdə sıfır desibeldən (db) və ya mütləq qiymətlərdə $2 \cdot 10^{-5}$ paskaldan (Pa) böyük olmalıdır. Qeyd edək ki, müəyyən şərait üçün normativ sənədlərlə müəyyənləşdirilmiş həddən yüksək intensivliyə malik səslər küy adlanır. Yuxarıda qeyd edilən bu səviyyə sağlam qulağın eşitdiyi ən zəif səsi xarakterizə edir (eşitmə həddi). Digər tərəfdən səviyyəsi 120 db (və ya 1 pa) olan küylər qulağımızda ağrı hissi yaradır və ağrı həddi adlanır. 150 db səviyyəli küylər qulaq pərdəsini dəşir, 180-200 db isə insana öldürücü təsir edir. Normal ucalıqda aparılan danışqların yaratdığı səslər 30-40 db intensivliyinə uyğun gəlir [1].

III. NİTQ İNFORMASIYASININ MÜHAFİZƏ METODLARI HAQQINDA

Otaq şəraitində aparılan danışqların akustik kanallarla ötürülməsi prosesində nitq informasiyasının otaqdan xaricə gizli əldə edilməsi və bu hala qarşı bəzi mühafizə tədbirlərini nəzərdən keçirək.

İlk növbədə qeyd edilməlidir ki, informasiya təhlükəsizliyi və məlumatların, o cümlədən fərdi məlumatların əldə edilməsi məsələləri milli qanunvericiliklə tənzimlənir. “AR-in Konstitusiyası Qanunu”-na görə şəxsin razılığı olmadan və ya xəbərdar edilmədən onun danışqlarının yazılması, foto, video çəkilişlərinin aparılması qadağandır (xüsusi hallar istisna olmaqla). Bu, məxfi və dövlət sirri daşıyan məlumatlara da şamil edilir. “Dövlət sirri haqqında” AR Qanunu dövlət sirri təşkil edən məlumatlarını üç məxfilik dərəcəsi ilə: xüsusi əhəmiyyətli, məxfi və tam məxfi kimi müəyyənləşdirir (maddə 7) və dövlət sirrinə aid edilən məlumatların qanunla müəyyən edilən təsnifatını təsbit edir (maddə 4). Qanunla belə məlumatların yayılması və qorunması məsuliyyəti vəzifəli şəxslərin, o cümlədən elmi tədqiqat müəssisələrinin rəhbərliyinin üzərinə qoyulur. Məsələn şəxslər məxfiliyin pozulmasına görə qanunvericiliyə müvafiq olaraq cinayət, mülki-hüquq və ya inzibati məsuliyyət daşıyırlar (maddə 28) [2].

Şəkil 1-dən göründüyü kimi danışqlardan yaranan səs rəqsləri dalğalarının bir hissəsi otağın bir çox konstruktiv inşaat elementlərindən nüfuz edərək xaricə yayıla və adi dinləmə yolu ilə əldə edilə bilər. Bu halda pəncərələr (xüsusilə açıq halda), qeyri-metal materiallardan hazırlanmış qapılar, hava tənzimləyici nəfəsciklər, tavan və döşəmə, eləcə də qaz, su, otağı qızdıran isitmə borularının, elektrik kommunikasiya xətlərinin divarlardan keçid yerlərində yaranmış boşluqlar və s. nüfuzedici tərkibin sızma kanalı rolunu oynaya bilər.

Qeyd edək ki, hal-hazırda nitq informasiyasının istər akustik, istərsə də yuxarıda qeyd edilən digər texniki kanallardan icazəsiz əldə edilməsinə qarşı çoxsaylı mühafizə vasitələri mövcuddur. Qorunan danışqların məxfilik statusundan, otaqların inşaat konstruksiyasından, təşkilatın maliyyə imkanlarından və s. amillərdən asılı olaraq qiyməti və funksional imkanları kəskin fərqlənən çox sadə və ucuz, eləcə də xüsusi təyinatlı mürəkkəb və baha olan texniki vasitələrdən istifadə edilə bilər.

Bu məqsədlə istifadə edilən ən sadə mühafizə metodlarından biri danışq mühitinin akustik maneə siqnalları ilə küyləndirilməsidir. Bu halda danışqlarla eyni vaxtda musiqinin, radio-televiziya verilişlərinin səsləndirilməsindən istifadə etmək olar. Belə ki, qulaq, maneə yaradan müxtəlif səs axınlarından faydalı nitqi seçmək kimi psixi-akustik xüsusiyyətə malikdir. Bu zaman kənar səslərlə qarışmış nitq dalğaları otaqdan kənara yayılsa və eşidilsə də anlaşılmaz olur. Metodun çatışmayan cəhəti kənar səslər fonunda danışqların dərk edilməsinin çətinləşməsi, iştirakçılarda müəyyən inamsızlıq və yorğunluq hissinin yaranmasıdır. Digər variantda nitq rəqsləri enerjisinin nüfuzedici tərkibinin azaldılması məqsədilə otağın bütün səthinin səsuducu materiallarla üzlənməsidir. Bu məqsədlə səsuducu əmsalı böyük olan mineral pambıq, şüşəlifli və bazalt əsaslı materiallardan, köpükləndirilmiş poliamiddən (paralondan) və s. inşaat üzlük materiallarından istifadə etmək olar. Tavan və döşəmədən xaricə nüfuz edən səs dalğalarını zəiflətmək üçün asma tavan və ikinci qat döşəmə qurmaq olar. Bu halda nüfuzedici tərkibin zəiflədilməsi qeyd edilən maneələrdə səs enerjisinin bir hissəsinin udulması (maneəların daxilində istilik enerjisinə çevrilməsi) hesabına baş verir.

Otağın konstruktiv elementlərində akustik səs dalğalarının yaratdığı vibrasiyaların xaricdən qəbul edilməsini aradan qaldırmaq üçün xüsusi texniki vasitələrdən istifadə etmək lazım gəlir. Məsələn ondadır ki, danışqlardan yaranan akustik dalğalar otaq daxilindəki kommunikasiya xətlərində və otağın digər konstruktiv elementlərində (divarlar, tavan, döşəmə, pəncərə, qapı və s.) nitq siqnallarının amplitudasına uyğun vibrasiya yaradır. Bu siqnallar nə qədər zəif olsa da qonşu otaqlardan, divarların xarici səthlərindən xüsusi qurğular vasitəsilə qəbul edilərək ilkin səs siqnallarının bərpa edilməsi üçün istifadə edilə bilər [3]. Bu, xüsusilə pəncərə şüşələrinə, polad borulara və divarlara aiddir. İnformasiyanın bu vibrokəmərlərdən sızmasının qarşısını almaq üçün vibroküyləmə yaradan qurğulardan istifadə edilir: qurğular eşidilən səs diapazonu tezliklərində vibrasiya rəqsləri generasiya edərək qeyd olunan konstruktiv elementlərə nüfuz etdirilir. Bu halda vibrasiyanın həmin elementlərdə yaratdığı rəqslər nitq rəqsləri ilə qarışaraq bədənliyyətinin əldə etdiyi siqnallardan nitq informasiyasını sintez etmək imkanını aradan qaldırır. Bu məqsədlə qurğunun generasiya etdiyi signal konstruksiyalara bərkidilmiş elektrik vibratorlarına verilir və onları müəyyən intensivlikdə rəqsə gətirir. Şəkil 2-də “Sonata-AB” markalı vibroküyləyicinin bir neçə tətbiq variantı göstərilmişdir [4].

a)

Şəkil 2. Otağın kommunikasiya və konstruktiv elementlərində vibroküy dalğalarının yaradılması

a) vibroküyləyici qurğu “Sonata-AB”, b) metal boruda, c) divarda, d) pəncərə şüşəsində vibroküy dalğalarının yaradılması

Səs dalğaları enerjisinin konstruksiyalarda yaratdığı udulan tərkibinin intensivliyinin azaldılması məqsədilə bu konstruksiyaların səthini səsuducu əmsalı böyük olan və yuxarıda qeyd edilən məsələli üzlük materiallardan da istifadə edilə bilər.

Lakin bir çox hallarda danışq iştirakçıları, o cümlədən dəvət edilənlər müasir miniatur yazma qurğularından (ardınca, diktofon) istifadə etməklə nitq informasiyasını gizli yazmaqla əldə edə bilərlər. Bu məqsədlə rəqib miniatur radioötürücü qurğu vasitəsilə nitq siqnallarını otaqdan xaricdə yerləşdirilmiş radioqəbuledici qurğulara ötürə bilər. Ötürmə üçün radio/optik (infraqırmızı tezlik diapazonlu dalğalarla), elektromaqnit və s.

kanallardan istifadə etmək olar. Başqa bir halda qurğunun miniatur mikrofon və radioötürücü hissəsini stolda, stulda, otağın digər əşyalarında və ya özünə aid əşyalarda (qələmində, qeyd dəftərində, eynəyində və s.) gizlətmək, yazma hissəsini isə bədənində yerləşdirmək olar. Diktofonun bədənə (geyimdə) gizlədilməsi halından daha çox istifadə olunur.

Praktikada danışq iştirakçıların diktofondan istifadə edilməsinin və ya yazıların üçüncü tərəfə verilməsinin yolverilməz olması barədə şifahi və yazılı razılaşmaların pozulması halları daha geniş yayılmışdır. Ona görə də danışqların məxfiliyinin qorunmasının ən etibarlı yolu onların yazılması imkanının aradan qaldırılmasıdır. Bu imkan, işi müxtəlif prinsiplərə əsaslanan texniki vasitələrlə həyata keçirilir. Burada, yalnız danışqların diktofonla gizli yazılması və bir neçə mühafizə metodları nəzərdən keçirilir. Qeyd edək ki, hal-hazırda köhnə tip maqnit kasetli analoq diktofonlardan demək olar ki, istifadə edilmədiyindən mətnə yazma qurğusu dedikdə nitq informasiyasının yazılması üçün sərt disklər, Smart Media, Memory Stick kimi daşıyıcılarla təchiz edilmiş miniatur rəqəmsal diktofonlar nəzərdə tutulur.

Otaqda gedən danışqların icazəsiz (gizli) yazılmasının qarşısının alınması əsasən iki istiqamətdə aparılır:

- yazma qurğusunun otağa gətirilməsinin aşkarlanması və kənarlaşdırılması;
- otağa gətirilmiş diktofonların yazıların maskalanması.

Burada maskalanma dedikdə səs (nitq) dalğalarının akustik yayılma mühitinin küy siqnalları ilə qarışdırmaqla yazıların güclü təhrifə uğradılması prosesi başa düşülür. Təhrifə uğradılmış nitq yazıları dinlənilmə rejimində anlaşılmaz səs yazıları kimi (küy kimi) qavranır: mövcud texniki üsullarla nitqi küydən (maneələrdən) ayırmaq mümkün olmur.

Mühafizə metodu kimi ilk növbədə danışq iştirakçıların özləri ilə diktofon gətirməsinin aşkarlanması prosesi həyata keçirilir. Bu məqsədlə metal detektorlardan (metal aşkarlayan qurğu), radio lokatorlardan, rentgenoskopiya aparatlarından və diktofon aşkarlayan xüsusi təyinatlı digər qurğulardan istifadə edilir. Bu qurğuların bəziləri diktofonu ancaq işlək rejimdə, digərləri isə passiv rejimdə (söndürülmüş halda) aşkarlayır və bir qayda olaraq müəssisənin girişində və ya danışqlar aparılan otaqların qapı keçidlərində çərçivələr formasında, görünməz şəkildə quraşdırılır. Qurğular təşkilatın mühafizə xidməti tərəfindən idarə edilir. Daha ciddi mühafizə tədbiri kimi mobil aşkarlayıcılar vasitəsilə dövətilərin geyimi, çantası və s. əşyaları yoxlanıla bilər (etik qaydalar gözlənilməklə).

İşləyən diktofonun aşkarlanması onun şüalandırdığı elektromaqnit dalğalarının aşkarlanıb (qəbul edilib) identifikasiya edilməsinə, iş rejimində olmayanların aşkarlanması isə, məsələn, iştirakçılar istiqamətində müəyyən intensivlikli yüksək tezlikli dalğaların şüalandırılmasına və əks edilən dalğaların analizinə əsaslanır. Bu qurğuların qiyməti çox bahadır və yüksək səviyyəli tədbirlər zamanı istifadə edilir. Çatışmayan cəhəti şüaların yüksək dozasının insan orqanizmi üçün ziyanlı təsirə malik olmasıdır. Zıyanı azaltmaq məqsədilə dalğaların intensivliyini azaltmaq lazım gəlir ki, bu halda aşkarlayıcı (lokator) yoxlanılan obyektə 2-5 sm. yaxınlaşdırılmalıdır. Qeyd olunan texniki vasitələrin heç biri

diktofonun 100% aşkarlanmasını təmin etmir. Digər tərəfdən danışqların məxfilik səviyyəsi yüksək deyilsə yoxlanmanın aşkar şəkildə aparılması etik normalar baxımından qəbul edilməz sayıla bilər. Ona görə də bir çox hallarda nitq informasiyanın təhlükəsizliyi məqsədilə ikinci sinif qurğulardan – yazılışı təhrif edən qurğulardan daha geniş istifadə edilir.

Bu qurğularda yazını təhrifə uğratma vasitəsi kimi elektromaqnit və akustik küy siqnallarından istifadə edilir və təsir mexanizminə görə:

- diktofonun informasiya daşıyıcısının (yaddaş elementinin);
- mikrofonun;
- diktofonun elektron sxem dövrəsinin (radioelektron elementlərinin) normal işinin pozulmasına imkan yaradan qurğular qruplarına bölünür [5].

Elektromaqnit küy maneəsinin təsir mexanizmi aşağıdakı kimidir: elektron generatoru sxemi ifrat yüksək tezlikli (İYT) və kifayət qədər gücə malik (3-5 vatt) elektromaqnit dalğaları (1 QHs ətrafında) şüalandırır. Bu şüalar mikrofon gücləndiricisinin sxemində və digər sxem dövrələrində parazit küy siqnalları yaradaraq onların normal iş rejimlərini pozur və nəticədə yazılmış səslər güclü təhrifə uğrayaraq dinlənildikdən sonra anlaşılmır. Küy mənbəyinə yaxın məsafədə yerləşən diktofonun sxem dövrəsinin metal hissələrində, məsələn, korpusda yaranan fuko cərəyanlarının təsiri ilə radioelementlərin yol verilən həddən artıq qızması nəticəsində sıradan çıxma halı da baş verə bilər.

Bu metod otağa gətirilmiş diktofonların harada gizlədilməsinin (iştirakçılarda, şəxsi və ya otaq əşyalarında və s.) məlum olmadığı hallarda xüsusilə effektivdir. Lakin bu metodun da bir sıra çatışmayan cəhətləri var. İYT küy siqnalları intensivliyə və təsir müddətinə görə yol verilən həddi (dozanı) keçdikdə insan orqanizmi üçün müəyyən təhlükə törədə bilər. Digər bir nöqsanı antenasının dar şüalanma istiqamətli (60-70 dərəcə əhatəli) olmasıdır, yəni danışqlar stolu ətrafında oturan bütün iştirakçıları əhatə etməsi üçün bir neçə antenadan istifadə edilməsi zərurəti yarana bilər.

İkinci qrup qurğular generasiya etdikləri akustik küy səsləri ilə diktofonun normal işinə əngəl yaratma prinsipinə (akustik küyləmə prinsipi) əsaslanır və əsasən iki alt qrupa bölünür:

- ultrasəs diapazonunda maneə küy siqnallarının yaradılması;
- eşidilən səs diapazonunda maneə küy siqnallarının yaradılması.

Birinci qrup qurğularda akustik küy siqnalı kimi eşidilməyən diapazonlu ultrasəs siqnallarından (20-22 kHs) istifadə edilir. Bu siqnallar diktofonun gücləndiricisinin amplitud-tezlik xarakteristikasını dəyişərək onun normal yazı rejiminə mane olur. Mikrofonun korpusunun metal materialdan olması (ekranlanması) ehtimalını nəzərə alaraq küy siqnallarının intensivliyini artırmaq lazım gələ bilər. Bu qrup qurğuların (məsələn, VNG 012-U Savesa) təhlükəsizliyi mühafizə səviyyəsi yüksəkdir.

İkinci qrup qurğularda eşidilən səs diapazonlu tezliklərdə a) “nitqəbənzər” (bir neçə nitq fraqmentlərinin qarışığından alınan səs) küy siqnalları; b) “ağ” küy (səs diapazonunda intensivliyi bərabər paylanan küy siqnalları) və ya c) “narıncı” küy (səs diapazonunda, tezliyin artması istiqamətində, hər növbəti oktava zolağında intensivliyi 3 db azalan səs siqnalları) səsləri yayan generatorlardan istifadə edilir [6]. Danışqlar bu küy səslərinin fonunda aparılır. Küy səsinin intensivliyi elə seçilir ki, qulağın nitqi küy səsndən ayırmaq xüsusiyyəti öz təsirini itirməsin. Küy səsi ilə nitq səsi qarışığı kiçik ölçülü ucadan danışanlardan səsləndirilir. Çıxış gücü əllə tənzimlənən (“ANG-2000”, “Kabinet”) və danışq səslərinin intensivliyindən asılı olaraq avtomatik tənzimlənən (“Бапон”, “Шопок-1”) olmaqla iki variantda hazırlanır. Sadə və ucuz olmaqla istənilən tip mikrofonun işini əngəlləyir. Bu qrupa daxil olan qurğuların ümumi çatışmayan cəhəti informasiya təhlükəsizliyi tədbirinin aşkar aparılmasıdır. Digər çatışmayan cəhət tədbir təşkilatçıları tərəfindən danışqların texniki vasitələrlə həyata keçirdikləri yazılışların anlaşıqlıq və fərdi tembr (ahəng) göstəricilərinin pisləşməsidir [7].

NƏTİCƏ

Məqalədə akustik kanallarla ötürülən nitq informasiyasının (danışqların) təhlükəsizliyi məsələləri və mühafizə metodları araşdırılır. Mühafizə predmeti otaq daxilində aparılan danışqlardır. Danışqların gizli əldə edilməsinin iki variantına baxılır: tədbir iştirakçılarının diktofonla danışqları gizli yazması və danışqların bərpası məqsədilə akustik sızma kanalları ilə xaricə yayılan vibroakustik siqnalların qəbulu. Nitq informasiyasının akustik sızma kanalları kimi a) xaricdən danışqların bilavasitə dinlənilməsinə imkan yaradan konstruktiv elementlər (giriş qapısı, havalandırma sistemləri, kommunikasiya xətlərinin otaqdan çıxış yerləri ilə divar arasındakı boşluqlar və s.); b) vibrosızma kanalları – pəncərə şüşələri, su, qaz, isitmə sistemlərinin metal boru xətləri, divarlar və s. konstruktiv elementlər nəzərdə tutulur. Qeyd olunan kanallarla nitq informasiyasının gizli əldə edilməsinin qarşısını alan mühafizə metodları, bu metodlar əsasında yaradılmış bəzi texniki qurğular və onların iş prinsipləri izah edilir. Təşkilat rəhbərləri aparılan danışqların konfidensiallıq dərəcəsindən, otağın inşaat-konstruktiv xüsusiyyətlərindən, maliyyə imkanlarından və s. amillərdən asılı olaraq nitq informasiyasının təhlükəsizliyini təmin etmək məqsədilə məqalədə qeyd edilən təklif və tövsiyələrdən istifadə edə bilərlər.

İSTİNADLAR

- [1] Теоретические основы физической акустики, <http://userdocs.ru/fizika/4987/index.html>
- [2] Dövlət sirri haqqında AR Qanunu, <http://www.e-qanun.az/framework/3731>
- [3] Vladimir V. Grishachev, “Detecting Threats of Acoustic Information Leakage through Fiber Optic Communications,” Journal of Information Security, 2012, №3, pp. 149-155.
- [4] Система виброакустической и акустической защиты. “Соната-АВ”. Руководство по эксплуатации, <http://www.cbi-info.ru/files/sonata-av3m.pdf>
- [5] Карагин В. Л., “Защита от утечки речевой информации из помещений. Практические аспекты реализации,” <http://www.bnti.ru/showart.asp?aid=1024&lvl=04.02.03>.

- [6] ГОСТ 12.1.003-83 (СТ СЭВ 1930-79). Шум. Общие требования безопасности.
- [7] L Reva, V. A. Trushin, A. A. Ivanov, T. V. Borbotko, “Truthfulness of estimation of voice information protection from leakage through technical canals,” *Journal of Physics: Conference Series*, Vol. 803, No. 1, p. 012128, 2017.

**ON SOME VIBRO-ACOUSTIC METHODS FOR
PROTECTING VOICE INFORMATION TRANSMITTED
THROUGH ACOUSTIC CHANNELS**

Bikas Aghayev¹, Tarlan Aliyev², Kovsar Aliyeva³, Maleyka Ibisova⁴
Institute of Information Technology of ANAS, Baku, Azerbaijan

^{1,2,3,4}*depart6@iit.sciense.az*

Annotation – The article explores the security of speeches in the room and provides confidential information. Participants are looking at ways of securing speech information transmitted through acoustic channels with a tape recorder and protecting the initial state of vibroacoustic signals leaking out of the room. Proposals are provided for the cases under consideration to determine the organization's information security policy.

Keywords – *speech information; acoustic distribution channel; secret record of negotiations; vibroacoustic leakage channels; information security; protection of speech information*

Klassifikasiya metodlarının zərərli proqramların aşkarlanmasına tətbiqi

Elşən Bağirov

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
elsenbagirov1995@gmail.com

Xülasə— Son zamanlarda zərərli proqramların çeşidinin və mürəkkəbliyinin artımı, fərdi məlumatların təhlükə ilə üz-üzə qalması onların aşkarlanması və analiz edilməsi istiqamətində tədqiqatların aparılmasını labüd edir. Bu tədqiqat işində zərərli proqramların analizi və aşkarlanması metodları tədqiq olunmuş, 138047 sayda zərərli və zərərsiz fayllardan əldə edilən əlamətlərdən düzəlmiş baza üzərində python mühitindən istifadə edərək klassifikasiya metodları tətbiq edilmiş, qiymətləndirmə metrikaları vasitəsilə metodların səmərəliliyi analiz edilmişdir.

Açar sözlər— *zərərli proqram; virus; aktivvirus; signatura; statik analiz; dinamik analiz; klassifikasiya; maşın təlimi;*

I. GİRİŞ

İnformasiya texnologiyalarının, internetin əhatə dairəsinin durmadan genişlənməsi, eləcə də zərərli proqram istehsalçıların artımı kompüterdə arzuolunmaz fəaliyyətlərə səbəb ola bilən zərərli proqramların çoxalmasına və belə proqramların informasiya təhlükəsizliyinə olan təhdidlərdən birinə çevrilməyə öz təsirini göstərmişdir [1]. Nəticədə zərərli proqramlar müasir informasiya cəmiyyətinin əsas problemlərindən birinə çevrilmişdir [2].

Əksər zərərli proqram təminatları rəsmi olmayan veb saytlardan axtarılan faylların, xüsusilə icra oluna bilən formatlı faylların internet üzərindən endirilməsi zamanı sistemə daxil olur. Zərərli fayl sistemdə öz yolunu tapan kimi xarakterik davranışına görə sistemin iş qabiliyyətinin aşağı salınması, fərdi məlumatların oğurlanması, kritik verilənlərin ələ keçirilməsi və ya dəyişdirilməsi, iri və xırda məbləğdə pul mənimləmə, xidmətdən imtina kimi arzuolunmaz fəaliyyətləri həyata keçirməyə müvəffəq ola bilər [3, 4].

Zərərli proqramlardan qorunmaq üçün əsas müdafiə xətti antiviruslar hesab edilməkdədir [5]. Bir neçə asanlıqla aşkar oluna bilən məlum zərərli proqramlar vardır ki, antivirus tərəfindən rahat bir şəkildə aşkarlanıb təmizlənə bilər. Çünki antivirusların tərkibində zərərli proqramları unikal identifikasiya edən signaturalardan ibarət olan, mütəmadi olaraq yenilənməsinə ehtiyac yaranan baza mövcuddur [6]. Lakin yeni meydana çıxan, o cümlədən, metamorfizm, paketləmə və ya polimorfizm kimi antiviruslardan yayınma üsulları tətbiq edilmiş zərərli proqramların aşkarlanmasında antiviruslardan istifadə səmərəsizdir. Belə növ təkmilləşdirilmiş zərərli proqramların aşkarlanması nisbətən mürəkkəb və çətinidir [7, 4].

Zərərli proqramların aşkarlanması və analizi üçün müxtəlif tədqiqat işləri aparılmışdır. Zərərli proqramların kəmiyyət və keyfiyyət baxımından artımı nəticəsində analiz və aşkarlama üçün həmin proqramlardan statik və ya dinamik üsulla əldə edilmiş əlamətlərdən ibarət verilənlər bazası üzərində maşın təlimi metodlarının tətbiqi məsələlərinə son illər daha çox diqqət ayrılmışdır.

II. ƏLAQƏDAR TƏDQIQATLAR

[2]-də 3086 sayda icra oluna bilən formatda olan 2136 zərərli və 980 zərərsiz fayllardan PE (*ing.* portable executable) başlığı, DLL (*ing.* Dynamic Link Library) adları və DLL funksiya adları kimi əlamətlər çıxarılaraq baza yaradılmış və Naive Bayes, Qərar ağacı, Təsadüfi Meşə, SVM və digər klassifikasiya metodları tətbiq edilmişdir.

[8]-də zərərli proqram təminatlarının aşkarlanması üsullarından olan hibrid analiz yanaşması istifadə edilmişdir. Statik analiz üçün icra oluna bilən fayllardan klassifikasiya məqsədilə əlamətlər çıxarılmışdır. Dinamik analiz yanaşmasında isə NtTrace adlanan idarəedici virtual mühitdə icra oluna bilən faylın davranışı müşahidə edilmişdir.

[9]-də zərərli proqramlar tərəfindən yerinə yetirilən zərərli fəaliyyətləri təsvir edən davranış əsaslı əlamətlər modeli təklif edilmişdir. İlkin olaraq idarə olunan virtual mühitdə zərərli proqramların davranışı analiz edilmiş və API (*ing.* Application Programming Interface) müraciətlərinin izləri tutularaq qeydiyyatla alınmışdır. Bu izlər əsasında proqram davranışının zərərli və ya zərərsiz olduğunu müəyyən etmək üçün Qərar Ağacı, Təsadüfi Meşə və SVM kimi klassifikasiya metodları tətbiq edilmişdir.

[10]-də Chatchai L. və b. zərərli proqram fayllarının məzmunundan çıxarılmış n-gram əsaslı ardıcıl əlamətlərdən istifadə edərək yaradılmış baza əsasında üç müxtəlif klassifikasiya metodunu (qərar ağacları, çoxlaylı perseptron və SVM) tətbiq etmişlər. Eksperimentlərin nəticəsində ən yüksək dəqiqlik SVM metodunda (96.64 % dəqiqliklə və n=4 olduqda) alınmışdır.

[11]-də Şerif B. və b. təkmilləşmiş zərərli proqramların beş seçilmiş əlaməti vasitəsilə zərərli proqram nümunələrindən ibarət bazadan “stuxnet” virusunun proqnoz edilməsi üçün regressiya modelləri işlənən çoxölçülü yanaşma təklif etmişlər. Analiz nəticəsində məlum olmuşdur ki, təkmilləşdirilmiş zərərli

proqram növlərinin bəzi əlamətləri arasında yüksək korrelyasiya mövcuddur.

[5]-də Hemant R. və b. zərərli proqramların klassifikasiyası üçün supervizorlu və supervizorsuz öyrənmə metodlarını tətbiq etmişlər, əlamətlər vektoru olaraq “opkod tezliyi” götürülmüşdür. Bu zaman təsadüfi meşə alqoritminin digər alqoritmərdən üstün dəqiqlik göstərdiyi müşahidə edilmişdir.

III. ZƏRƏRLİ PROQRAMLAR VƏ ONLARIN NÖVLƏRİ

Zərərli proqram termini ingilis dilindən “malicious” (zərərli) və “software” (proqram təminatı) terminlərinin deduksiya olunması nəticəsində yaranmışdır [1, 6, 12]. “KasperskyLab” şirkəti tərəfindən verilmiş tərifdə zərərli proqramların qanuni istifadəçinin kompüterini yoluxdurmaq və ona müxtəlif yollarla zərər vurmaq üçün hazırlanmış proqramlar olduğu deyilir. Son zamanlarda ən ciddi təhdidlərdən biri məhz zərərli proqramlar hesab edilir.

Çox vaxt istənilən növ zərərli proqramı “virus” kimi qəbul edirlər [6]. Halbuki viruslar zərərli proqramların ən sadə növü hesab edilir və davranışına görə zərərli proqramlar öz müxtəlifliyi ilə zəngindir. Çox rast gəlinən zərərli proqramlara viruslar, soxulcanlar, troyanlar, casus proqramlar, reklam proqramları, girov proqramları, rutkitlər, bekdorlar, keyloqqlər misal göstərilə bilər [4, 12-14]. Antivirus sistemlərinin test edilməsi üzrə ixtisaslaşan “AV-Test” İnstitutunun dediyinə görə gün ərzində 350 minə yaxın yeni növ zərərli proqramlar qeydə alınır və xarakterinə görə təsnifatlaşdırılır [15].

A. Viruslar. Həcmi kilobaytlarla ölçüləcək səviyyədə olan viruslar ən sadə zərərli proqram növü hesab edilir. Viruslar istifadəçinin razılığı olmadan yüklənir və işə düşür, bioloji virus kimi digər faylları yoluxduraraq özünün nüsxəsini yaradır və çoxalır [4, 10, 12]. Virusların kompüterdəki fəallığını əks etdirən əsas təzahürlər aşağıdakılardır:

- parolların və digər kritik informasiyanın oğurlanması;
- yaddaş həcmi israf edərək kompüterin iş qabiliyyətini aşağı salmaq;
- verilənlərin silinməsi və ya modifikasiyası;
- spamların yayılması.

B. Soxulcanlar. Viruslarla çox oxşardır. Fərq odur ki, soxulcanlar şəbəkə üzərindən yayıla bilər və öz nüsxəsini digər kompüterlərə sərbəst yaya bilirlər [1, 4, 13]. Soxulcanların axın kimi yayılması nəticəsində yaddaş, rabitə kanalları yüklənir və sistem bloka alınır. Viruslardan fərqli olaraq şəbəkə mühitində yayılma imkanına malikdir. İlk kompüter soxulcanı 1988-ci ildə Kornel Universitetinin aspirantı Robert Tappan Morris tərəfindən yaradılmışdı. Soxulcan böyük sürətlə şəbəkədə yayılaraq internet qovşaqlarının 10%-ni sıradan çıxara bilmişdi [1]. Morris soxulcanının mənbə kodu Kompüter Tarixi Muzeyində çevik diskətdə qorunub saxlanılır. Digər məşhur soxulcanlara misal olaraq Sasser, My Doom, Blaster, Melissa-nı göstərmək olar [4].

C. Troyanlar. Funksional cəhətdən qanuni proqram təminatı kimi görünən, lakin işə düşdükdə faydalı funksiyalarla bərabər, arxa planda öz zərərli funksiyalarını da yerinə yetirirlər [1, 6]. Troyanlar pirat proqramlar, yoluxmuş fayllar, sosial mühəndislik və digər üsullarla yayılırlar. Kaspersky Lab tərəfindən troyanların kompüterdə yerinə yetirdiyi fəaliyyətlərə və təbiətinə görə bəzi növləri aşağıda verilmişdir.

- Troyan-casus: casus proqramları toplusu olub, əsasən kritik verilənləri və parolları oğurlamağı hədəf alır.
- Troyan-yükləyici: avtomatik olaraq uzaqdakı serverə qoşularaq zərərli proqramları kompüterə yükləyir.
- Troyan-dropper: zərərli proqramları endirir, quraşdırır və işə salır.
- Troyan-proksi: işə salınması ilə bədnəviyyətinin yoluxmuş sistemi proksi serverə çevrilir [6].

D. Casus proqramları. Səciyyəvi fəaliyyətlərinə istifadəçinin internet axtarış tarixçəsinin izlənməsi və istifadəçi profilinə uyğun olan reklamlarla yenidən qayıtması aiddir [13]. Bir şəxsin və ya təşkilatın xəbəri olmadan tez-tez istifadə olunan veb-saytlar, kredit kart məlumatları, klaviaturadan daxil edilmiş klavişlərin loqları, elektron poçt ünvanları və digər məlumatları istifadəçidən xəbərsiz hücumçuya göndərə bilər. Eyni zamanda kompüter üzərində idarəetməni ələ ala bilər. Casus proqramları hər hansı proqram məhsulunun sınaq versiyası və ya pulsuz versiyasının endirilməsi və quraşdırılması zamanı aktivləşə bilər [4, 6]. Reklam proqramları və keyloqqlər casus proqramlarına daxil edirlər.

E. Girov proqramları. Troyanlardan istifadə etməklə kompüter sistemini və ya verilənləri şifrəleyir və istifadəçinin öz verilənlərinə daxil olmasını məhdudlaşdırır, müəyyən müddət bitənədək sistemi “dondurur” [13]. Qurbanın şifrəni əldə etməsi üçün interfeys yaradılır və ona rəqəmsal kriptovalyuta ilə (əsasən bitkoin) ödəniş üsulu təklif edilir. Girov proqramına misal olaraq 2017-ci ildə böyük sürətlə yayılan “WannaCry” kiberhücum hadisəsini göstərmək olar.

IV. ZƏRƏRLİ PROQRAMLARIN ANALİZİ VƏ AŞKARLANMASI ÜSULLARI

Zərərli proqramların aşkarlanması prosesi kompüter təhlükəsizliyi kontekstində həmişə maraq doğurmuşdur. Son zamanlarda zərərli proqramların geniş sürətdə artımı və təkmilləşməsi aşkarlama metodlarının müxtəlifliyinə səbəb olmuşdur [15].

Zərərli proqramların analiz metodları əsasən statik və dinamik olmaqla iki kateqoriyaya bölünür [13, 16]. Bundan başqa hər iki metodun birlikdə istifadə edilməsi nəticəsində yaranan hibrid metod da tətbiq edilir.

A. Statik analiz metodu. Statik analizdə icra oluna bilən (ing. executable) fayl işə salınmadan struktur səviyyədə, yəni kod səviyyəsində analiz edilir [3, 16]. Bunun üçün müəyyən vasitələrdən istifadə etməklə (Məsələn, python mühitində yazılmış “PEFILE” alətindən) icra edilə bilən fayllardan statik parametrlərin çıxarılaraq əlamətlərdən ibarət bazanın

yaradılması və üzərində analizlərin aparılması prosesi yerinə yetirilir. Statik analizin əsas üstünlüyü zərərli proqramın bütün mümkün davranış ssenarilərinin üzə çıxarılma bilməsidir.

Statik şəkildə zərərli proqram analizi üçün mühüm bir metod olaraq antivirusların istifadə etdiyi siqnatura əsasında aşkarlama metodunu göstərmək olar. Antiviruslar yeni daxil olmuş icra oluna bilən faylın zərərli olub olmadığını yoxlamaq üçün həmin faylın statik üsulla əldə edilmiş siqnaturası ilə məlum zərərli faylların siqnaturaları bazasından uyğunluq tapmağa cəhd edir. Əgər uyğunluq yaranarsa antivirus onu zərərli proqram kimi qeydə alır [13].

$$A(P) = \begin{cases} \text{zərərli}, & s \in P \\ \text{zərərsiz}, & s \in !P \end{cases}$$

Burada, P – zərərli və ya zərərsiz olduğu müəyyənləşdirilən proqram, A(P) – P proqramının aşkarlayıcı funksiyası, s – P proqramının siqnaturasıdır.

Statik analiz metodunun əsas üstünlüyü siqnaturaların unikallığı baxımından dəqiqliyin maksimum təmin edilməsidir. Üsulun çatışmazlığı isə əvvəllər məlum olmayan zərərli proqramları, eyni zamanda mövcud zərərli proqramlar üzərində “paketləmə”, “polimorfizm”, “metamorfizm” kimi antiviruslardan yayınma üsulları tətbiq edilmiş zərərli proqramları aşkarlamaqda çətinlik çəkməsidir [13]. Əksər kommersiya antivirus vendorları məhz siqnaturaya əsaslanan aşkarlama metodunu tətbiq edir. Mütəmadi olaraq yeni növ zərərli proqramlar aşkar edildikdən sonra siqnatura bazası yenilənməyə məcburdur.

B. Dinamik analiz metodu. Statik analizdən fərqli olaraq dinamik analiz metodunda izolə edilmiş mühitdən (simulyator, emulyator, sandbox, virtual maşın) istifadə edərək şübhəli faylın davranışını monitorinq edilir [3, 13, 17]. Nəticədə faylın davranış atributları (Məsələn, icra olunan zaman zərərli proqramın API müraciətləri, dəyişdirilmiş, silinmiş və ya oxunmuş reqistrlər, İP ünvan və DNS sorğuları, URL-lərə giriş, şəbəkədə aktivliyi və s.) əldə edilir [3].

Zərərli proqram təminatlarının dinamik olaraq analizi üçün izolə edilmiş mühitlərdən ən əlverişlisi “sandbox”lardır [3]. Sandboxlara misal olaraq “Cuckoo”, “SNDBOX”, “Falcon”, “ViCheck”-i göstərmək olar. Sandboxlar zərərli proqramların davranışını loqlaşdırma bilən agentlərlə təchiz olunmuşdur. Zərərli proqramın sandboxda icra edilməsi zamanı agent loqlaşdırmanı başladır, icra müddəti bitdikdən sonra mühiti əvvəlki vəziyyətə qaytara bilir. Bu zaman əsas sistemdən təcrid olunduğu üçün ona heç bir zərər gəlmir.

Üsulun əsas üstünlüyü əvvəllər məlum olmayan zərərli proqramları aşkarlaya bilməsidir. Həmçinin, statik analizlə müqayisədə sürətlidir. Əsas çatışmazlığı isə onun dəqiqliyindədir [13]. Belə ki, burada birinci və ikinci növ səhvlərin olması ehtimalı mövcuddur.

Statik və dinamik analizin birlikdə istifadə olunduğu hibrid metodlardan istifadə genişlənməkdədir. Belə ki, statik olaraq aşkarlanmadan yayınmaq üçün zərərli proqramlara yayınma üsullarının tətbiqi və dinamik olaraq aşkarlanmanın dəqiqliyi

kimi problemlərin mövcud olduğunu nəzərə alaraq hibrid modeldə zərərli proqram dinamik mühitə salınaraq statik əlamətlər əldə edilir və analiz olunur [17].

C. Maşın təlimi metodları. Zərərli proqramlar genişlənməkdə davam edir və müxtəlif növ yeni əlamətlər meydana çıxır. Təkcə statik və ya dinamik analizin tətbiq edilməsi ilə zərərli proqramlarla mübarizə aparmaq səmərəsizdir. Buna görə də tədqiqatçılar zərərli proqramları aşkarlamaq üçün maşın təlimi metodlarının tətbiqinə diqqət ayırmaqdadırlar.

V. EKSPERİMENTLƏR

Bu işdə 96724 zərərli və 41323 zərərsiz fayldan statik üsulla əldə edilmiş 138047 sətirdən ibarət, “CSV” (comma seperated values) faylında saxlanılan verilənlər bazası üzərində “Təsadüfi meşə”, “Gradient Boosting”, “Adaboost”, “GaussianNB” metodları tətbiq edilmiş və qiymətləndirmə nəticəsinə şəkil 1-də əks olunmuş nəticələr əldə edilmişdir. Tədqiqatlar python mühitində (python3 versiyası quraşdırılmış Jupyter Notebook veb tətbiqindən istifadə etməklə) aparılmışdır.

Şəkil 1. Metodların müqayisəsi.

Tədqiq edilmiş baza öyrənmə və testetmə üçün 3/7 nisbətində iki hissəyə bölünmüşdür. Metodların qiymətləndirilməsi nəticəsində ən yüksək dəqiqlik verən metodun Təsadüfi meşə algoritmi olduğu məlum olmuşdur.

NƏTİCƏ

Zərərli proqramların analiz edilməsi üçün iki ən mühüm yanaşma – statik və dinamik analiz metodları, onların fərqli, üstün və zəif cəhətləri təhlil edilmişdir. Zərərli proqramların təbiətinə görə müxtəlifliyini nəzərə alaraq demək olar ki, dinamik analiz mühiti onun davranışını tam əks etdirə bilmə bacarığına sahib olmaya bilər. Birincisi, zərərli proqramlar istifadə olunan mühitin müxtəlifliyinə uyğun olaraq fərqli davranış göstərə bilər. Bundan başqa son zamanlar zərərli proqramlar üzərində izolə edilmiş mühitdə öz davranışını dəyişdirmək xüsusiyyətinin tətbiq edilməsi halları da müşahidə edilməkdədir. Zərərli proqramı sandbox mühitində dinamik olaraq icra edən zaman ilk növbədə agenti axtarış etməsi ilə bu qənaətə gəlmək olar. Zərərli proqram təcrid olunmuş mühitin əlamətlərinə rast gəldikdə özünü zərərsiz fayl kimi apara bilər.

Baxılan işdə maşın təlimi metodları tətbiq edilmişdir. Qiymətləndirmə nəticəsində tədqiq edilmiş baza üçün Təsadüfi meşə alqoritmi yüksək dəqiqlik göstərmişdir.

Bir çox tədqiqatçılar tərəfindən zərərli proqramların aşkarlanması və analizi üçün müxtəlif metodların işlənməsinə baxmayaraq statistikaya əsasən zərərli proqramların sayında hələ də ümumi halda azalma müşahidə edilməməkdədir. Zərərli proqram istehsalçıları aşkarlama metodlarının təkmilləşdirilməsinə cavab olaraq yeni əlamətlər yaradırlar. Buna görə də aşkarlama dəqiqliyinin artırılması üçün istifadə olunan əlamətlərin yenidən baxılmasına ehtiyac yaranır.

İSTİNADLAR

- [1] R. Əliquliyev, Y. İmamverdiyev, “İnformasiya təhlükəsizliyi insidentləri”, İnformasiya Texnologiyaları nəşriyyatı, 2012, 219 s.
- [2] Y. İmamverdiyev, E. Kərimov, “Zərərli proqramların aşkarlanması üçün maşın təlimi metodlarının tətbiqi”, Proqram mühəndisliyinin aktual elmi-praktiki problemləri I respublika konfransı, 17 may 2017-ci il, s. 166-169.
- [3] M. İjaz, M. Durad, M. İsmail, “Static and dynamic analysis using machine learning”, 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), 8-12 January 2019, pp. 687-691.
- [4] P. Vinod, R. Jaipur, M. Gaur, “Survey on malware detection methods”, Proceedings of 3rd Hackers’ Workshop on Computer and Internet Security, 17-19 March 2009, pp. 74-79.
- [5] H. Rathore, S. Agarwal, S. Sahay et al., “Malware detection using machine learning and deep learning”, International Conference on Big Data Analytics, 18-1 December 2018, pp. 402-411.
- [6] H. Tayyab, H. Aqib, “A survey of analysis of malware infection”, 2015, 40 p.
- [7] Y. Ye, D. Wang, T. Li et al., “An intelligent PE-malware detection system based on association mining”, Journal in Computer Virology, vol. 4, 2008, pp. 323-334.
- [8] S. Kumar, N. Aggarwal, C. Krishna et al., “Malicious data classification using structural information and behavioral specifications in executables”, Proceedings of Recent Advances in Engineering and Computational Sciences (RAECS), 6-8 March 2014, pp. 1-6.
- [9] H. Galal, Y. Mahdy, M. Atia, “Behavior-based features model for malware detection”, Journal of Computer Virology and Hacking Techniques, vol. 12, 2016, pp. 59-67.
- [10] O. Sornil, L. Chatchai, “Malware Classification Using N-grams Sequential Pattern Features”, International Journal of Information Processing and Management(IJIPM), vol. 4, 2013, pp. 59-67.
- [11] Ş. Bahtiyar, M. Yaman, C. Altıniğne, “A multi-dimensional machine learning approach to predict advanced malware”, Computer Networks, vol. 160, 2019, pp. 118-129.
- [12] S. Bragen, “Malware detection through opcode sequence analysis using machine learning”, MS Thesis, Gjovik University College, 2015, 67 p.
- [13] K. Chumachenko, “Machine learning methods for malware detection and classification”, Bachelor’s Thesis, 2017, 93 p.
- [14] M. Siddiqui, “Data mining methods for malware detection”, PhD thesis, University of Central Florida, 2008, 111 p.
- [15] “Av-Test malware statistics”,
<https://www.av-test.org/en/statistics/malware/>
- [16] C. Andrade, C. Mello, “Malware automatic analysis”, BRICS Congress on Computational Intelligence and 11th Brazilian Congress on Computational Intelligence, September 2013, pp. 681-686.
- [17] J. Yan, Y. Qi, Q. Kao, “Detecting Malware with an Ensemble Method Based on Deep Neural Network”, Security and Communications Networks, vol. 1, 2018, pp. 1-16.

APPLICATION OF CLASSIFICATION METHODS FOR MALWARE DETECTION

Elshan Baghirov

Institute of Information Technology of ANAS, Baku, Azerbaijan

elsenbagirov1995@gmail.com

Abstract— In recent years, the increasing variety and complexity of malware, facing personal data with threat requires research towards detection and analyzing. This study investigated the methods of analyzing and detecting malware, applied classification methods on dataset based features extracted from 138047 malware and benign files using the python framework, and the effectiveness of the methods have been analyzed using the evaluation metrics.

Keywords— malware; virus; antivirus; signature; static analysis; dynamic analysis; classification; machine learning

Steqoanaliz üsullarının icmal

Sakit Verdiyev¹, Ababil Nağıyeva², Rəşşəndə Hüseynova³, Zakir Hüseynov⁴

^{1,2,4}Azərbaycan Texnologiya Universiteti, Gəncə, Azərbaycan

³Azərbaycan Dövlət Aqrar Universiteti, Gəncə, Azərbaycan

¹info_tel@inbox.ru, ²nagiyevaababil@gmail.com, ³huseynova.raxshanda@mail.ru

Xülasə— Açıq global kompüter şəbəkələrində müxtəlif media formatlarında istifadə edilən verilənlərin dövriyyəsi eksponensial qanunla artdığı üçün informasiya mühafizəsi məsələləri daha çox aktuallaşır və yeni üsulların işlənilməsi zərurəti yaranır. Məqalədə rəqəmli təsvirlərin şəbəkələrdə dövriyyəsi zamanı qorunması üçün steqanoqrafiya və onun əksi olan steqoanaliz üsulları təhlil edilmiş və konkret misalın həlli verilmişdir.

Açar sözlər— steqanoqrafiya, steqoanaliz, steqoalqoritm, steqotəsvir, konteyner, xi kvadratı

I. GİRİŞ

Rəqəmsal məlumatların internetdə və digər rabitə kanallarında elektron dövriyyəsinin sürətlə artması verilənlərin mühafizəsinə həsr olunan steqanoqrafiya metodlarının işlənilməsinə təkan verir. Bununla yanaşı əks proses – ötürülən məxfi məlumatlara icazəsiz daxil olmalara, onların təhlilinə, modifikasiyasına həsr olunan hücum üsullarından olan steqoanaliz də inkişaf edir.

Steqanoqrafiya sözü yunan dilindən tərcümədə “stegano” ötürülmüş, “graphia” yazı mənasını verir.

Steqanoqrafiya, məxfi məlumatları istənilən media fayllarında gizlətmə üsuludur ki, gödərəndən və alıcı-dan başqa heç kim gizli məlumatların mövcudluğunu bilməsin.

Steqanoqrafik üsulla örtük təsvirində konteyner təsvirə gizlədilən informasiyanı aşkarlamaq üçün steqoanaliz üsullarından istifadə olunur.

Steqosistemin riyazi modeli aşağıdakı kimi təqdim edilə bilər:

$$E: C \times M \times K \rightarrow S \quad (1)$$

$$D: S \times K \rightarrow M \quad (2)$$

$$D(E(c, k, m), k) = m, \quad \forall c \in C, \quad \forall k \in K, \quad \forall m \in M \quad (3)$$

Burada C – konteyner, M – gizli məlumat, K – steqo açar, S – dolu konteyner, yəni steqo təsvirdir [1].

Steqanoqrafiyada istifadə olunan alqoritmləri qiymətləndirilərkən aşağıdakı üç əsas xüsusiyyət nəzərə alınır:

- Daşıyıcıdakı (konteynerdəki) pozuntu (ing. distortion);
- Konteynerin tutumu (ing. capacity);
- Dayanıqlılıq (ing. robustness).

Steqanoqrafik alqoritmlərin qiymətləndirilməsi zamanı örtük obyektində dəyişikliyin qiymətləndirilməsi çox vacibdir. Konteynerin dəyişməsinə və ya təsvirdəki pozulma dərəcəsini təyin etmək üçün müxtəlif ölçmə metodları var. Bu metodlardan ən çox tanınanlar MSE (mean squared error), PSNR (peak signal to noise ratio), RMSE (root mean squared error)-dir [2].

MSE orta kvadratik xətanı hesablayır. MSE adətən σ^2 kimi göstərilir. RMSE isə MSE-nin kvadrat köküdür.

$$\sigma^2 = \frac{1}{M \times N} \sum_{i=1}^{M \times N} (P(i, j) - S(i, j))^2 \quad (4)$$

Burada M və N sətir və sütunların sayı, $P(i, j)$ konteyner təsvir, $S(i, j)$ və isə stego təsvirdir.

Bəzən MSE əvəzinə xətanın böyüklüyünün original piksel qiymətinin ən böyüyü ilə olan əlaqəsi əhəmiyyət daşıyır. Belə olan halda PSNR (ing. peak signal to noise ratio) hesablanır.

$$PSNR(dB) = 10 \log_{10} \frac{x_{peak}^2}{\sigma_d^2} \quad (5)$$

Burada x^2 təsvir pikselinin mümkün olan maksimum qiymətidir.

Ardıcıl LSB üsullarında təsvirin həcmi onun ölçüsü ilə sıx bağlıdır. Həcm baxımından BMP (Bitmap) formatları daha əlverişli hesab olunur, çünki daha çox informasiya yerləşdirmək olur. Belə ki, JPEG (Joint Photographic Experts Group) formatında olan təsvirlərdə 8x8 bloklara sadəcə 4 və ya 5 bit gizlədilə bilər. Buna görə də gizlədiləcək informasiya miqdarı kifayət qədər azdır [3].

II. STEQOANALİZ

Steqanoqrafik alqoritmlərin dayanıqlılığını ölçmək üçün steqoanaliz metodlarından istifadə olunur. Hər bir müxtəlif steqoanaliz metodları üçün ayrı ayrı steqo-analiz metodları işlənilmişdir. Bir alqoritm üçün istifadə olunan steqoanaliz metodu ola bilər ki, digər alqoritm üçün əlverişsiz hesab olunsun.

Steqoanaliz hər hansı bir konteyner içərisində məlumat olub olmadığını aşkar etmək və əgər məlumat varsa o məlumatı əldə etmək məqsədilə istifadə olunan steqoalqoritmə hücum metodudur.

Adətən steqoanalitikin istifadə olunan bütün steqanoqrafik üsullardan xəbərdar olduğu hesab olunur (Kerchofs prinsipi). Əgər steqoanalitik istifadə olunan steqanoqrafik üsullardan xəbərsizdirsə onda onun işi çətinləşir [4].

Steqoanalitikin hücum edə bilməsi üçün bəzi verilənlərə sahib olmalıdır. Sahib olduğu verilənlərə görə o, hücum modellərindən birini seçərək işini davam edir. Hücum modellərindən ən geniş yayılanları aşağıdakılardır:

- Sadəcə steqo hücumu: Analiz üçün sadəcə steqo-obyekt bilinir;
- Bilinən konteyner hücumu: konteynerin içərisinə məlumat yerləşdirilmədən əvvəlki halı bilinir;
- Bilinən gizli məlumat: steqoanalitik gizlədilmiş məlumatdan əvvəlcədən xəbərdar olur;
- Bilinən steqo hücumu: konteyner obyekt, steqo obyekt və steqanoqrafik açarlar bilinir.

Hər bir steqanoqrafik metod üçün ayrı-ayrı steqoanaliz metodlarına ehtiyac vardır. Yəni hər bir steqoalqoritm metodu üçün ayrı bir steqoanaliz metodu işlənmişdir və hər bir alqoritmın analizi yalnız həmin alqoritmə uyğun hazırlanmış analiz metdoun-dan istifadə zamanı düzgün nəticə verir.

Əgər kiçik həcmdəki məlumat böyük həcmli konteyner içərisinə yerləşdirilsə bu zaman konteynerdə məlumat olması nəzərə çarpmayacaqdır.

Steqoanaliz metodlar içərisində məlumatın nəzərə çarpmasına əsaslanan bir çox üsullar vardır. Onlara aşağıdakıları misal göstərə bilərik:

- Statistik steqoanalizi
- Histoqram analizi
- RS (Regular and Singular analysis) steqoanalizi
- Bitlər müstəvisi (Bit plane) analizi
- χ^2 testi və s. [5].

III. STEQOANALİZ METODLARI

Steqoanaliz aparılarkən təsvirlərin xarakteristikalarından istifadə edərək qeyri adi xassələri aşkarlanırlar. Həmin xassələrin xüsusiyyətləri istənilən steqanoqrafik üsulla əlaqədardır. Bu üsullar asanlıqla məxfi verilənin mövcudluğunu üzə çıxardır və hətta onun ölçüsünü qiymətləndirə bilər:

A. Histoqram əsaslı analiz

Bu həmçinin steqotəsvirin testləşdirilməsi üçün effektiv hesab edilir. Piksellərin paylanması və yaxud qeyri adi formalarını identifikasiya etmək üçün örtük və steqotəsvirin histoqramları müqayisə edilir. Bir çox hallarda PVD (pixel value difference) əsaslı steqonoqrafik üsullar histoqram analizinin müxtəlif dəyişmələri ilə qiymətləndirilir. Misal üçün piksel fərqləri histoqram analizi, Histoqram Characteristic Function-Center of Mass (HCF-Com) analizi.

B. RS steqoanaliz

Regular və singular (RS) analiz RS üsulu kimi təsadüfi LSB yerləşdirilməsi metodlarında aşkarlama etmək üçün işlənilib. Bu üsul piksellərin LSB-sində kiçik dəyişmələrdən istifadə edir. Bu dəyişmələrlə və diskriminasiya funksiyasını

piksellərin regular və singular qruplara bölünməsinə təmin edir. Bu qrupların tezliyi steqotəsvirin içindəki məxfi mesajın uzunluğunu müəyyən edir [6].

C. Bit plane analizi

Ümumi təsvirin hər bir bit plane-i digər qonşu bit plane ilə korelyasiya olur. Steqanoqrafik üsul tətbiq edildikdən sonra korelyasiyalar dəyişə bilər və buna görə də bit plane analizi vasitəsilə görünə bilər. Bit plane analizi çox əhəmiyyətli dərəcədə əvəz etməyə əsaslanan yerləşdirmə üsulları ilə dəyərləndirilə bilər [7].

D. Qeyri-struktur steqoanaliz

Qeyri-struktur steqoanalizdə aparılarkən örtük təsvirin modelindən istifadə edir və daha sonra steqo və örtük təsvir arasında baş verən pozuntular qiymətləndirilərək məxfi verilənlərin mövcudluğunu aşkarlamaq üçün istifadə edilir. Ümumən Machine Learning-ə əsaslanan sinifləşdirici xüsusiyyətlər çoxluğunu elə üsullarla təqdim edir ki, örtük təsvir böyük data çoxluğu ilə steqotəsvir arasındakı xüsusiyyətlər fərqi öyrədir [8].

E. χ^2 analizi

Bu üsul qiymətlər cütünü PoVs (pairs of values) statistik analizinə əsaslanır və bu məxfi verilənin daxil edilməsi zamanı dəyişirilir. Bu üsul LSB əsaslı daxil edilmənin aşkarlanması üçün işlənilib. Daxil edilmə metodlarının sayı Xi kvadrat üsulu ilə aşkarlanır [9].

Hər baytın 8 bit ilə təmsil olunduğunu nəzərə alsaq, onda 256 qiymətimiz və 128 PoV cütümüz olacaqdır.

χ^2 -testinin nəticəsi 1-ə bərabər olarsa bu təsvirin içərisində məlumat yerləşdirildiyini göstərir. Əgər nəticə 0 olarsa onda təsvirin içərisində məlumatın yerləşdirilmədiyini göstərir [10].

$$\chi^2 = \sum \frac{(f_0 - f_e)^2}{f_e} \quad (6)$$

Burada f_0 təsvirin müəyyən bir pikselində müşahidə olunan tezlik, f_e isə təsvirin piksellərində müəyyən olan pozulmanın tezliyidir.

Gizli mesaj steqokonteynerə mükəmməl yerləşdirildikdə insan gözü ilə ayırd edilə bilmədiyinə görə analitik hesablama üsullarından istifadə edilir. Misal üçün aşağıdakı təsvirlərə aid hesablamalara nəzər salaq.

Şəkil 1. Boş konteyner və steqotəsvir

Şəkil 1 də 512x512x3 ölçülü boş konteyner, və 512x512x3 ölçülü steqotəsvir verilib. Vizual analiz zamanı heç bir fərq

nəzərə çarpmır. Ona görə də aşağıdakı qayda ilə PSNR və MSE hesablayaq. Hesablama Matlab mühitində aparılır.

```
>> n=size(im1);  
>> M=n(1);  
>> N=n(2);  
>> MSE=sum(sum((im1-im2).^2))/(M*N);  
>> PSNR=10*log10(255*255/MSE);  
>> fprintf('\nMSE:%7.2f', MSE);  
  
MSE: 0.00  
MSE: 0.00  
MSE: 0.00  
>> fprintf('\nPSNR: %9.7f dB', PSNR);  
  
PSNR: %9.7f dB
```

Hesablamanın nəticəsində orta kvadratik xətanın qiyməti 0-a bərabərdir. Bu onu göstərir ki, steqoalqoritm effektivdir və təsvirin piksellərində heç bir pozuntu yoxdur, PSNR-in qiyməti isə boş və dolu konteyner arasındakı oxşarlığı əks etdirir.

χ^2 hesablanaraq əldə olunan nəticələr şəkil 2 və şəkil 3-də nümayiş olunub

Şəkil 2. Boş konteynerin χ^2 testinin nəticəsi

Şəkil 3. Dolu konteynerin χ^2 testinin nəticəsi.

Şəkil 2-də χ^2 -nin nəticəsi 0 alınıb. Bu təsvirin boş olduğunu göstərir. Şəkil 3-də isə χ^2 -nin nəticəsi 1 alınıb və məlum olur ki, təsvirdə informasiya yerləşdirilmişdir

NƏTİCƏ

Bu məqalədə təsvir steqanoqrafiyası üsulu ilə örtük təsvirində gizlədilmiş informasiyanın aşkarlanması üçün istifadə olunan müxtəlif steqoanaliz metodları təhlil edilib. Təhlil nəticəsində məlum olub ki, hər bir üsul konkret olaraq tətbiq edilən steqanoqrafik alqoritmın xüsusiyyətlərindən asılıdır. Təsvirin daxilində məxfi məlumatın mövcudluğunu aşkarlamaq üçün steqoanaliz üsulu ilə hesablama aparılaraq steqotəsvirdə məlumatın olması müəyyən edilib. Gizli məlumatın konteynerə yerləşdirilməsi zamanı steqotəsvirdə

baş verən pozuntuların miqdarını müəyyən etmək üçün PSNR üsulunun istifadə nümunəsi verilərək, boş konteynerlə dolu konteyner arasındakı fərqi MATLAB-da hesablanan konkret rəqəmlə verilib. Hesablamaların nəticəsi məxfi məlumatın konteynerə yerləşdirmə prosesinin uğurlu olduğunu təsdiq edir

İSTİNADLAR

- [1] С.М. Сейеди, В.С. Садов, Стеганографические алгоритмы на основе вейвлет- преобразований, Минск: РИВШ, с.2014-110.
- [2] K.H. Jung, K.Y. Yoo, Steganographic method based on interpolation and LSB substitution of digital images, Springer.
- [3] Multimedia Tools and Applications, 2015, vol. 74, pp. 2143-2155.
- [4] N. Zaker, A. Hamzeh, A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram, Springer, Multimedia Tools and Applications, 2012, vol 3, no.1, pp. 147-166.
- [5] X. Liao, S. Guo, J. Yin, H. Wang, X. Li, A.K., Sangaiah, New cubic reference table based image steganography, Springer, Multimedia Tools and Applications, 2017, vol. 25, pp. 1-18.
- [6] A. Nissar, A. Mir, Classification of steganalysis techniques: A study, Digital Signal Processing, 2010, vol. 20, pp. 1758-1770.
- [7] M. Hussain, T.S. Antony, Ki-Hyun Jung, Image steganography in spatial domain: A survey, Signal processing: Image communication, 2018, vol. 65, pp. 46-66
- [8] N. Zaker, A. Hamzeh, A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram, Springer, Multimedia Tools and Applications, 2012, vol. 58 pp. 147-166.
- [9] J. Fridrich, J. Kodovsky, Rich models for steganalysis of digital images, IEEE Transactions on Information Forensics and Security, 2012, vol.7, pp. 868-882.
- [10] T. Denemark, V. Sedighi, V. Holub, R. Cogranne, J. Fridrich, Selection-channel-aware rich model for steganalysis of digital images, IEEE International Workshop on Information Forensics and Security, 2014, pp. 48-53.
- [11] V. Sedighi, R. Cogranne, J. Fridrich, Content-adaptive steganography by minimizing statistical detectability, IEEE Transactions on Information Forensics and Security, 2016, vol. 11, pp 221-234.

AN OVERVIEW OF STEGOANALYSIS METHODS

Sakit Verdiyev¹, Ababil Nagiyeva², Raxshanda Huseynova³, Zakir Huseynov⁴

^{1,2,4}Azerbaijan Technological University, Ganja, Azerbaijan

³Azerbaijan State Agricultural University, Ganja, Azerbaijan

¹info_tel@inbox.ru, ²nagiyevaababil@gmail.com,

³huseynova.raxshanda@mail.ru

Abstract – Information security in global public computer networks is became more important nowadays because there circulate a big quantity of various media data and it grows by exponential tend every day. Therefore up to day there was developed a lot of different security methods. Here is considered and analysed steganography technics what is used for digital image protection in open networks. In the same time here is demonstrated the concrete sample of stego-analyse method calculating

Keywords – steganography, stegoanalysis, stegoalgorithm, stegoimage, container, Chi-square.

Çoxkanallı telekommunikasiya sistemlərində informasiyanın kriptomühafizəsinin bəzi aspektləri

Bayram İbrahimov¹, Tural Məmmədov²

¹Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

²AR Silahlı Qüvvələrinin Hərbi Akademiyası, Bakı, Azərbaycan

¹*i.bayram@mail.ru*

Xülasə— Məqalədə çoxkanallı telekommunikasiya sistemlərində abunəçi və şəbəkə rabitə xətlərinə icazəsiz qoşulmalardan mühafizə etmək üçün informasiyanın veriliş üsulları və kriptomühafizə vasitələri analiz edilir. Telekommunikasiya sistemlərində informasiya təhlükəsizliyinin bəzi aspektlərinə baxaraq, kriptografik sistemlərdə parolların dayanıqlığının ehtimal-zaman xarakteristikalarının qiymətləndirilməsi üçün analitik ifadələr verilmişdir.

Açar sözləri — telekommunikasiya sistemləri, icazəsiz qoşulma, ehtimal-zaman xarakteristikaları, kriptomühafizə, informasiyanın mühafizəsi, parol, kriptografiya sistemləri

I. GİRİŞ

Müasir dövrdə perspektiv informasiya və kompüter texnologiyalarının imkanlarından səmərəli istifadə etməklə gələcək nəsil rabitə şəbəkələrinin arxitektura konsepsiyası bazasında qurulmuş telekommunikasiya sistemlərinin informasiya təhlükəsizliyinin təmin edilməsini tələb edir. Bu baxımdan dövlətin, idarələrin və kommersiya strukturalı müəssisələrin informasiya sirlərinin saxlanması və mühafizəsi problemləri telekommunikasiya sistemlərində, rabitə kanallarında və xidmət sferalarında mühüm əhəmiyyət kəsb edir.

Çoxkanallı telekommunikasiya sistemlərində və şəbəkələrində məlumatların qəbulu, emalı və onların böyük tutumlu yaddaş sistemlərinə yığılması, rabitə kanalları vasitəsi ilə lazım olduqda ötürülməsi, veriliş traktının istənilən qovşağına qoşulma prosesləri və qəbulu zamanı bütün tip məlumatların kriptomühafizəsi məsələləri böyük aktuallığa malik istiqamətlərdən hesab olunur [1].

Aparılmış uzunmüddətli tədqiqatlarda rabitə şəbəkələrinin abunəçi və şəbəkə traktına icazəsiz qoşulmaların təşkili və onların aşkar edilməsi məsələsinə baxılmış [1, 2, 3] və müəyyən edilmişdir ki, şəbəkənin bütün perimetri boyunca istənilən formada sistemə müdaxilə oluna bilər və məlumatın götürülməsi mümkündür [4].

Telekommunikasiya şəbəkələri və sistemlərində informasiyanın qorunması – kriptomühafizəsi, icazəsiz qoşulmaların təşkili, məlumatın sirlərinin aşkarlanması, təhlükəsizliyi məsələlərinə geniş baxılır [5]. Lakin çoxkanallı telekommunikasiya sistemlərində göstərilən istiqamətlərə nəzəri, texniki və texnoloji aspektdən baxılması və nəzəri

cəhətdən əsaslandırmanın bəzi aspektlərinin təhlilinə yer ayrılmasına xüsusi önəm verilir.

Yuxarıda qeyd olunanları nəzərə alaraq, təqdim olunan iş çoxkanallı telekommunikasiya sistemlərində informasiyanın kriptomühafizəsinin bəzi aspektlərinə həsr edilmişdir.

II. ABUNƏÇİ VERİLİŞ TRAKTINA İCAZƏSİZ QOŞULMA ÜSULLARININ TƏHLİLİ

İlkin olaraq telekommunikasiya sistemləri nöqtəy-nəzərinə informasiya mənbəyindən – məlumat alana kimi çoxkanallı veriliş traktında abunəçi xəttinə icazəsiz qoşulma üsullarının təhlilini nəzərdən keçirək.

Telekommunikasiya sistemlərində abunəçi çoxkanallı veriliş traktına icazəsiz qoşulma üsulları aşağıdakılardır [1, 3]:

1. Abunəçi və şəbəkə terminallarına əlavə və gizli qoşulma üsulu;
2. Veriliş prosesi zamanı abunəçi veriliş xətlərinə əlavə olaraq paralel icazəsiz qoşulma üsulu;
3. Müdafiəsiz halda gizli olaraq (nəzarətsizlik olduğu hallarda, evlərdə, idarələrdə və s. yerlərdə) abunəçi terminalları və veriliş sistemlərini mənimsəmək üsulu;
4. Abunəçi taktında telefon xətlərinə və modəmlərə əlavə olaraq gizli-pirat variantda veriliş prosesinə qoşulma üsulu;
5. Abunəçi veriliş traktına və rabitə kanallarına, naqilsiz və naqilli, dar- və genişzolaqlı icazəsiz qoşulma üsulları.

Yuxarıda göstərilmiş icazəsiz qoşulma üsulları telekommunikasiya sistemlərində məlumatların kriptomühafizəsi və müdafiəsi aspektlərini dəyişdirməyə vadar edir. Yəni icazəsiz qoşulma üsullarına uyğun olaraq, kriptomühafizə və müdafiə məsələləri də müxtəlif olurlar.

Qeyd edək ki, aparılmış təcrübələr göstərir ki, abunəçi veriliş traktına, kommutasiya sistemində və rabitə kanallarına icazəsiz qoşulma üsulları məlumatın qorunması baxımından ən mühüm qovşaqlar və ya məqamlar hesab edilir. Lakin bunlarla yanaşı, çoxkanallı veriliş sistemində icazəsiz qoşulma üsullarında iki variant böyük əhəmiyyət kəsb edir:

- a) Çoxkanallı telekommunikasiya sistemlərinin rabitə kanallarında kriptomühafizənin təşkili alqoritmi və vasitələri;
- b) Mübadilə olunan məlumata əvvəldən-sona kimi traktında kriptomühafizənin təmin edilməsi.

Aparılmış təhlillər göstərir ki, telekommunikasiya sistemlərində abunəçi çoxkanallı veriliş traktına icazəsiz

qoşulmaya qarşı müdafiənin səmərəliliyini yüksəltmək üçün elektrik rabitə sistemlərində kriptomühafizə üsulları və onların terminal vasitələrinin iş prinsipini öyrənmək vacib aspektlərdən hesab edilir.

III. TELEKOMMUNİKASIYA SİSTEMLƏRİNDƏ KRIPTOMÜHAFİZƏ ÜSULLARI VƏ ONLARIN TERMINAL VASİTƏLƏRİ

Hal-hazırda şəhər telefon rabitəsinə yeni rəqəm tipli elektron kommutasiya sistemlərinin tətbiqində kriptomühafizə məsələləri əvvəlki sistemlərlə müqayisədə çox sadələşdirilmişdir [4]. Buna səbəb isə rəqəm tipli elektron kommutasiya sistemlərinin idarəetmə məsələləri proqram üsulu ilə yerinə yetirilir və hər bir abunəçinin xətti uyğun olaraq kodlarla və proqram təminatı ilə daima nəzarətdə saxlanılır və mühafizə olunur.

Qeyd olunanlarla yanaşı, telekommunikasiya sistemlərində kriptografiya məsələsi – abunəçi xətlərinin «parol» üsulu ilə müdafiəsi yerinə yetirilir. Bu üsulun bazasında zond terminalı yaradılmış və yerli, şəhərlərarası və beynəlxalq rabitənin təşkili zamanı bütün icazəsiz qoşulmalara nəzarət edilir və daima idarəetmə sistemləri ilə əlaqədə olaraq, nəzarətdə saxlanılır və şəbəkə üzrə monitorinqi aparılır.

Belə bir müdafiə üsulunda abunəçi xətlərin (AX) kodlanması – «parolu» böyük əhəmiyyət kəsb edir. Bu üsulun məği ondan ibarətdir ki, hər bir abunəçi xətti xüsusi 2 və 3 elementli kodlarla kodlanır və parolu tapılır. Əgər kod və parol düzgün olmadıqda abunəçi sistemi kommutasiya mərkəzindən bloklanır və qoşulmaya qadağa qoyulur. Abunəçi xəttinin müdafiəsi üçün «Parol» üsulunun sadə sxemi şəkil 1-də göstərilmişdir.

Şəkil 1. Kodlanmış abunəçi xəttinin parol üsulu ilə müdafiəsi sxemi

Müdafiə sxemi kommutasiya sistemindən (KS), abunəçi şleyf xəttindən (AŞX) və abunəçi terminaldan (AT) və ya istifadəçinin sadə telefon aparatından (TA) ibarətdir. Sistem daxili rabitə zamanı KS-dən abunəçi xətinə məlum olmayan parametrlə siqnallar daxil olmaqla «Parol» açılır və AT-a qoşulur. Bu zaman gərginlik $U = 120 \text{ V}$, siqnalın tezliyi 25 Hz, gecikmə müddəti isə 50 ms olar. Qoşulma pauza müddətində yerinə yetirilir – abunəçi bunu hiss etmir. Əgər yenidən qoşulmaq istəsə, onda yenə də 2 və ya 3 elementli kodu yığmaqla, yenidən icazəsiz qoşula bilər.

Baxılan sadə hal üçün AŞX-sxemdə kriptomüdafiə elementi kimi istifadə olunur və (0,5-1,5) km məsafə üçün nəzərdə tutulur.

Belə sistemlərdə kriptomühafizəni yüksəltmək məqsədi ilə – «Parol» cərəyan vericisi (CV) tezlik üsulu ilə kodun ötürülməsi üsulundan istifadə olunur. Şəkil 2 abunəçi xətinə «Parol-CV» üsulu ilə kriptomühafizə sxemi verilmişdir.

Sxemdə modul-A KS-də yerləşdirilmiş, modul – B isə abunəçi tərəfdə qoyulmuşdur və cərəyan vericisi ilə birlikdə fəaliyyət göstərir

Şəkil 2. Mühafizə kodun tezlik üsulu ilə ötürülməsində Parol-CV üsulunun sxemi

B-modulu avtomatik olaraq, A-moduluna tezlik impulsu kodlar ötürür. A-modulu daxil olmuş kodu tanıyaraq, stansiyanın cavab siqnalını, nömrənin yığılması və birləşməsinə təşkil etməyə icazə verir. Belə sxemin köməyi ilə telekommunikasiyada yüksək səviyyədə kriptomühafizə əməliyyatı yerinə yetirilir.

İndi isə naqılsız rabitə sistemində və telefon aparatlarına icazəsiz qoşulma zamanı kriptomühafizə məsələsinə baxaq. Müxtəlif firma və şirkətlər tərəfindən, o cümlədən Panasonic, Premier, Motorola və s. abunəçi terminalın identifikasiya üçün sadə kodlardan istifadə olunur.

Baxılan hal üçün kriptografiya sistemlərində istifadə olunan parol – rəqəm, söz, işarələrin gizli kombinasiyası olub, informasiya təhlükəsizliyində istifadəçinin autentifikasiyası üçün geniş istifadə edilir. Parol subyektin autentifikatorudur, autentikasiyanın ən geniş yayılmış növüdür. Burada, autentifikasiya istifadəçinin sistemdə izlənməsi məqsədilə subyekt və ya obyektlərə daxilolma identifikatorunun verilməsi və ya təqdim edilmiş identifikatorun mövcud identifikatorlar siyahısı ilə müqayisəsi hesab olunur.

Çoxkanallı telekommunikasiya sistemlərində istifadə olunan N_p – parol əlifbasının gücü, yəni parolların tərtibi zamanı istifadə edilən ümumi işarələrin sayını nəzərə alsaq, parolun minimal uzunluğu L_p aşağıdakı bərabərsizliklə təyin edilir:

$$L_p \geq [\log_2 S / \log_2 N_p], \quad (1)$$

burada S – kriptografiya sistemlərində istifadə olunan parolların bütün mümkün sayıdır və parolun təhlükəsiz istifadə olunma müddətindən asılı olaraq belə ifadə olunur:

$$S = 2T_t / t_y, \quad (2)$$

burada t_y – bir parolun yığılma müddətidir.

Sonuncu (1) və (2) ifadələri çoxkanallı telekommunikasiya sistemlərində istifadə olunan parolların tərtibi zamanı istifadə edilən ümumi işarələrin sayını və təhlükəsiz istifadə olunma müddətini qiymətləndirməyə imkan verən riyazi ifadələrdir.

Baxılan hallar üçün telekommunikasiya sistemlərində prosesin təkrar olunmaması üçün müxtəlif olmaqla kodların ümumi sayı 256-dan çox götürülür.

Müasir dövrdə kriptografiya sistemləri üçün naqilsiz terminallarda parollarla idarə olunan nəzarət sxemlərindən istifadə etməklə tam etibarlı müdafiə sistemi təşkil olunmuşdur. Bu nəzarət sxemləri parolların düzgün seçilməsi hesabına efir üzrə abunəçi xətinin bütün növ qoşulmalardan müdafiə edir və məlumatların ötürülməsi zamanı təhlükəsizliyini lazımı səviyyədə təmin edir.

IV. KRİPTOQRAFIYA SİSTEMLƏRİNDƏ PAROLLARIN MÜHAFİZƏYƏ DAYANIQLIĞININ QIYMƏTLƏNDİRİLMƏSİ

Kriptografiya sistemlərində müxtəlif məqsədlər üçün istifadə olunan parolların mühafizəsinin etibarını artırmağa imkan verən alqoritmləri, tədbirləri və alətləri nəzərə almaq vacib istiqamətlərdən biri hesab edilir. Bunun üçün ilk növbədə sistemdə autentifikasiya və identifikasiyasını nəzərə almaq mühüm əhəmiyyət kəsb edir.

Çoxkanallı telekommunikasiya sistemlərində autentifikasiya – sistemə daxil olmaq üçün təqdim etdiyi identifikatorun ona məxsusluğunun yoxlanılması yolu ilə subyekt və ya obyektin əsilliyinin-həqiqiliyinin təsdiq olunmasıdır. Bu zaman daxil edilmiş parol və istifadəçi üçün əvvəlcədən təyin olunan parol müqayisə edilir. Onlar üst-üstə düşdükdə istifadəçinin həqiqiliyi təsdiqlənmiş sayılır.

Qeyd edək ki, parolların ən başlıca təhlükəsi onların elektron ələ keçirilməsidir. Bunun üçün ilk növbədə parol kiçik və baş hərflər, rəqəmlər və durğu işarələrinin qarışıqından olmaqla, $L_p \geq L_{p, \max}$ maksimal uzunluqda tərtib edilib və tez-tez dəyişilməlidir.

Adətən, çoxkanallı telekommunikasiya sistemlərində parolların etibarlılığı və fəaliyyət müddətinin idarə olunması üçün parolun əsas xarakteristikalarının qiymətləndirilməsi tələb olunur.

Fərz edək ki, sistemdə N – sayda əlifbadakı işarələrdən, yəni simvollarından istifadə olunmuşdur. Bəzən N – parol əlifbasının gücü də hesab olunur, bir sözlə N – parolların tərtibi zamanı əlifbada istifadə edilən simvolların sayıdır.

Tutaq ki, kriptografiya sistemlərində N gücünə malik L_p uzunluqlu parollardan istifadə olunub. Bu zaman parolların bütün mümkün ola bilən sayı belə bir düsturla təyin oluna bilər [3]:

$$S = N^{L_p} \quad (3)$$

Fərz edək ki, mətnin daxiletmə sürəti V_m , onda L_p uzunluğuna malik olan bir parolun yığılma vaxtı aşağıdakı kimi qiymətləndirilə bilər:

$$t_y = \frac{L_p}{V_m} \quad (4)$$

Kriptografiya sistemlərində N gücünə malik L_p uzunluqlu parolun fəaliyyət müddətini T_t ilə işarə edək. Belə olduğu

halda istənilən parolun tapılma ehtimalı aşağıdakı ifadə ilə təyin olunur:

$$P = \frac{T_t}{N^{L_p} \cdot (L_p / V_m)} \quad (5)$$

(4) və (5) ifadələrini nəzərə alsaq, parolun təhlükəsiz istifadə müddətini aşağıdakı ifadə ilə qiymətləndirmək olar:

$$T_t = \frac{0,5 L_p \cdot N^{L_p}}{V_m} \quad (6)$$

Beləliklə, sonuncu ifadələr kriptografiya sistemlərində parolların mühafizəyə dayanıqlığının qiymətləndirilməsi üçün alınmış analitik ifadələr hesab olunur və bir çox telekommunikasiya sistemlərində istifadə edilə bilər.

NƏTİCƏ

Çoxkanallı telekommunikasiya sistemlərində informasiyanın kriptomühafizəsinin bəzi aspektləri təhlil edilən zaman abunəçi veriliş traktına icazəsiz qoşulma üsullarına baxılmış və kriptografiya sistemlərində parolların dayanıqlığının ehtimal-zaman xarakteristikalarının qiymətləndirmək üçün analitik ifadələr alınmışdır.

İSTİNADLAR

- [1] İbrahimov B.Q. Elektrik rabitə nəzəriyyəsi. AzTU, Bakı, 2016. – 382 s.
- [2] İbrahimov B. G., Humbatov R.T., İbrahimov R.F. “Analysis of information encryption methods in multichannel telecommunication systems,” Proceedings of the 4-th International Scientific Conference on Actual multidisciplinary scientific-practical problem of information security, pp. 18-21, 2018.
- [3] Шаврин С.С. Защита информации в многоканальных телекоммуникационных систем. М.: МТУСИ. 2002. - 62 с.
- [4] Тихонов, С.В. Универсальный метод защиты блочных шифров от побочных атак по цепям питания // Проблемы информационной безопасности. Компьютерные системы.– 2017. № 3.- с.48-55.
- [5] Fragouli C, Soljanin E. Network coding. Foundations and Trends // Networking. V.2, No.1, 2007. -P.1–134.

SOME ASPECTS OF CRYPTOCURRENCY INFORMATION IN MULTICHANNEL TELECOMMUNICATION SYSTEMS

Bayram İbrahimov¹, Tural Məmmədov²

¹Azerbaijan Technical University, Baku, Azerbaijan

²An associate of the Military Academy of the Republic of Azerbaijan, Baku, Azerbaijan

¹i.bayram@mail.ru

Abstract: Multichannel telecommunication systems are reviewing data transmission and cryptocurrency analysis to protect subscribers and unauthorized access to network communication lines. Analyzes are given to evaluate the probability characteristics password persistence in cryptographic systems, while looking at some aspects information security in telecommunication systems.

Keywords: telecommunications systems, unauthorized access, probability characteristics, cryptographic protection, information security, password, cryptographic systems.

İnformasiya iqtisadiyyatının formalaşmasında fərdi know-how biliklərin təhlükəsizliyi məsələləri

Roza Şahverdiyeva¹, Leyla Əkbərova²

^{1,2}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹shahverdiyeva@gmail.com, ²akberovaleyla4@gmail.com

Xülasə– Məqalə informasiya iqtisadiyyatının formalaşmasında və inkişafında fərdi innovativ ideyaların təhlükəsizliyinin təmin edilməsi məsələlərinə həsr olunmuşdur. İnnovasiyalı informasiya iqtisadiyyatın formalaşması problemləri göstərilmişdir. Texnoparkların innovasiya və biliklər iqtisadiyyatında vəzifələri və onun yaradılması xüsusiyyətləri izah olunmuşdur. Müasir dövrdə inkişaf edən texnoloji innovasiya iqtisadiyyatı sektorları haqqında məlumat verilmişdir. Texnoparklarda fərdi innovativ ideyaların xüsusiyyətləri, kateqoriyaları, həmçinin rezidentlərin məlumatlarının qorunmasının formalaşma mərhələləri müəyyənləşdirilmişdir. Texnoparklarda innovativ ideyaların və fərdi məlumatların təhlükəsizliyinin ümumi metodları təhlil olunmuşdur. İnnovasiya iqtisadiyyatı şəraitində elmi ideyaların kommersiyalaşdırılması zəncirində müvafiq məlumatların təhlilinin təkmilləşdirilməsi və mühafizəsi üzrə bəzi tövsiyələr verilmişdir.

Açar sözlər – innovasiya, informasiya və biliklər iqtisadiyyatı, məhsul və proses innovasiyaları, texnoloji innovasiya, innovativ və elmi ideya, texnopark, rezident firmalar, elmin kommersiyalaşması, fərdi məlumatın təhlükəsizliyi

I. GİRİŞ

Müasir dövrdə iqtisadiyyatı daha çox inkişaf edən ölkələrin təcrübəsi göstərir ki, onların iqtisadi inkişafı innovativ texnologiyalara və biliklərə əsaslanır. Ölkənin gələcək inkişaf strategiyası da qeyri-neft sektorunun inkişafına yönəlmişdir. Bunun hesabına davamlı iqtisadi artıma və tərəqqiyə nail olunacaq və iqtisadiyyat şaxələndiriləcəkdir [1, 2].

İqtisadiyyatın innovasiya əsaslı irəliləyişinin təmin edilməsi, texnoloji innovasiya əsasında iqtisadiyyatın müasirləşdirilməsi, yüksək texnologiyalar sektorunun inkişafı, süni intellekt və robotlaşdırma, bio, nano, informasiya-kommunikasiya, kosmik və s. kimi yeni sferaların formalaşması, respublikada real iqtisadi sektorun daha sürətli inkişafına nail olmağın əsas yollarından hesab olunur. İnnovativ və elmtutumlu iqtisadiyyatın formalaşması yüksək texnologiyalar əsasında rəqabətqabiliyyətli məhsul istehsalının genişləndirilməsi ölkənin ixrac qabiliyyətinin yüksəlməsinə əhəmiyyətli təsir göstərir.

İnnovasiyalı informasiya iqtisadiyyatının davamlı inkişafına və rəqabət qabiliyyətinin artırılmasına nail olmaq üçün müxtəlif təyinatlı Yüksək Texnologiya Parkları yaradılmışdır [2].

İnnovasiyalı iqtisadiyyatın formalaşmasında əsas, əhəmiyyətli inkişaf mənbələrindən və katalizatorlarından biri də innovativ ideyaların təhlükəsizliyi, həmçinin müvafiq informasiya resurslarının, sistemlərinin, texnologiyalarının mühafizəsinin təmin edilməsidir.

İnnovasiyalı iqtisadiyyatı formalaşdırən iqtisadi strukturların fəaliyyətində daha çox “Nou-hau”ların çoxluğu, fərdi innovativ ideyaların reallaşdırılması, elmi-tədqiqatların innovativliyi, elmi və texnoloji tutumu, elmi-texniki kommersiya sirləri, müəllif hüquqlarının ciddi qorunması zərurəti, intellektual mülkiyyət məsələlərinə daha çox diqqət yetirilir.

Bütün bunlar innovasiyalı informasiya iqtisadiyyatının formalaşmasında fərdi innovativ ideyaların təhlükəsizliyi məsələləri üzrə olan problemlərin və fərdi innovativ ideyaların təhlükəsizliyinin spesifikliyinin nəzərə alınmasını və həmin sahədə müvafiq metod və mexanizmlərin işlənilməsinə zəruri edir. İnnovasiyalı iqtisadiyyatın formalaşmasında əsas iqtisadi struktur olan texnoparklarda rezidentlərin fərdi innovativ ideyalarının təhlükəsizliyi və kommersiya sirlərinin və personala aid fərdi informasiyalarının qorunması vacib və aktual məsələlərdən hesab olunur.

II. İNNOVASIYALI İQTİSADİYYATIN MAHİYYƏTİ VƏ FORMALAŞMASI PROBLEMLƏRİ

İqtisadi inkişafın innovasiya mərhələsinin əsas hədəfi milli iqtisadiyyatın rəqabət qabiliyyətliliyinin yüksəldilməsinə və dünya təsərrüfat sisteminə səmərəli inteqrasiyasına nail olmaqla, uzunmüddətli perspektivdə ölkənin dinamik sosial-iqtisadi inkişafının davamlılığını təmin etməkdən ibarətdir.

Dünya ölkələrinin innovasiyalı inkişaf üzrə vəziyyəti hər il həmin ölkələrin Qlobal İnnovasiya İndeksi hesabında [3] müəyyənləşdirilir. Belə ki, Azərbaycan 2019-cu ilin Qlobal İnnovasiya İndeksinin hesabı üzrə 130-a yaxın ölkə sırasında 84-cü reytinqlə 0–100 şkalasında 30.21 bala malik olmuşdur.

Ölkənin XXI əsrdəki iqtisadiyyatı innovasiya, informasiya və biliklərə əsaslanan iqtisadiyyatdır. Şəbəkə iqtisadiyyatı, İnternet iqtisadiyyatı, media iqtisadiyyatı, kontent iqtisadiyyatı, proqram məhsulları iqtisadiyyatı, e-xidmətlər iqtisadiyyatı, e-kommersiya və s. informasiya iqtisadiyyatının əsas sektorlarıdır.

Ənənəvi iqtisadiyyat sahələrinin informasiya, bilik, texnoloji, innovasiya tutumlu tərkib altsahələri belə ifadə oluna bilər: 1) idarəetmədə İKT və informasiya sistemləri, Nou-hau texnologiyaları və sistemləri, 2) istehsal və xidmət prosesləri texnologiyaları və sistemləri, 3) marketinq və satış texnologiyaları və sistemləri, 4) innovativ texnologiyalar və sistemlər, 5) smart texnologiyaları və sistemləri, 6) biznes və sənaye xidmətləri texnologiyaları, 7) ətraf mühitin mühafizəsi texnologiyaları, 8) optik sənaye texnologiyaları. Bunlardan əlavə innovativ informasiya, bilik və texnoloji iqtisadiyyat sektorları da formalaşmaqdadır [4]: İKT iqtisadiyyatı, kosmik iqtisadiyyat, bioiqtisadiyyat, nanoiqtisadiyyat, tibb iqtisadiyyatı, təhsil iqtisadiyyatı, elm iqtisadiyyatı, kreativ iqtisadiyyat, incəsənət iqtisadiyyatı, mədəniyyət iqtisadiyyatı, idman iqtisadiyyatı, diaspor iqtisadiyyatı, ekoloji (yaşıl) iqtisadiyyat, alternativ energetika iqtisadiyyatı, patent (lisenziya) iqtisadiyyatı və s.

İnnovasiyanı bir çox növlərinə görə klassifikasiya edirlər. Məhsul və proses innovasiyası, həmçinin bəzən texnoloji innovasiya kimi də adlanır. Proses innovasiyası – yeni və ya təkmilləşdirilmiş istehsal və ya təchizat metodudur. Marketinq innovasiyası – yeni marketinq, məhsulun bazara çıxarılması üsullarıdır. Təşkilati innovasiya – sahibkarlıq təcrübəsində yeni iş yerlərinin və ya xarici əlaqələrin təşkilinin yeni təşkilatı üsuludur.

Müasir dövrdə formalaşan və inkişaf edən texnoloji innovasiya iqtisadiyyatı sektorlarını şəkil 1-dəki kimi təsvir etmək olar.

Şəkil 1. Texnoloji innovasiya iqtisadiyyatı sektorları

Kosmik iqtisadiyyat – kosmik resurslar və vasitələrlə yeni iqtisadi modelin yaradılması və mövcud iqtisadiyyatın inkişaf etdirilməsidir. *Dron iqtisadiyyatı* – dronların istehsalı və tətbiqi nəticəsində yeni iqtisadi sektorun yaradılmasıdır. *Big data iqtisadiyyatı* – big data texnologiyalarının yaradılması, big data məhsullarının istehsalı, tətbiqi və idarə edilməsi vasitəsilə yeni iqtisadi sektorun yaradılmasıdır. *Bio iqtisadiyyat* – bio texnologiyaların işlənilməsi, bio məhsulların istehsalı, istifadəsi və idarə olunması vasitəsilə yeni iqtisadi sektorun formalaşmasıdır.

İnnovasiyalı informasiya və biliklərə əsaslanan cəmiyyətin qurulması, texnoparkların, yüksək texnologiyalar parklarının yaradılması, elektron informasiya resurslarının inkişaf etdirilməsi, bank, maliyyə, ticarət, təhsil, sosial-iqtisadi və s.

sahələrdə elektron xidmətlərin daha geniş tətbiqi formalaşmaqda olan innovativ informasiya iqtisadiyyatının əsas inkişaf oriyentirləridir. Bunlar isə innovativ ideyaların tətbiqi nəticəsində formalaşır və inkişaf edir.

III. TEXNOPARKLARIN İNNOVASIYALI İQTİSADİYYATDA ƏSAS VƏZİFƏLƏRİ

Hər bir ölkənin innovativ iqtisadi inkişafında texnoparklar əhəmiyyətli rola malikdir. İnnovativ iqtisadiyyata keçid üçün elm-texnoloji innovasiya texnoparkları əsas hərəkətverici qüvvədir. İnnovasiya və biliklər iqtisadiyyatının infrastrukturunun əsasını texnoparklar təşkil edir, onun yaradılması və səmərəli fəaliyyəti əsas məqsədlərdəndir [5, 6].

Texnoparkların yaradılmasının əsas xüsusiyyətlərinə aşağıdakılar daxildir: 1) innovativ xarakterli müəssisə olması, 2) elmin, təhsilin, istehsalın və kommersiyanın maksimal olaraq bir-birinə yaxınlaşdırılması, 3) müxtəlif stimullaşdırma mexanizmlərinin və rejimlərinin tətbiq edilməsi, 4) yüksək texnologiyalar, o cümlədən İKT əsasında məhsul və xidmətlərin artırılması, 5) elm və texnologiya tutumlu firmaların inkişaf etdirilməsi, 6) intellektual beyin məhsulunun işlənilməsi, 7) elmi-tədqiqat işlərinin nəticələrinin sürətlə reallaşması, 8) innovativ texnologiyaların transferi, 9) intellektual mülkiyyətin qorunması.

Texnoparklar formalaşma məqsədlərindən və fəaliyyət xüsusiyyətlərindən asılı olaraq müəyyən istiqamətlərdə qərarlaşmış ixtisaslaşmaya malikdirlər. Beynəlxalq Elmi Parklar Assosiasiyasının (BEPA) rəsmi portalından əldə edilmiş məlumatlar əsasında texnoparkların fəaliyyət sahələri üzrə ixtisaslaşmasını şəkil 2-dəki kimi vermək olar [7].

Şəkil 2. Texnoparkların fəaliyyət sahələri üzrə ixtisaslaşması

Texnoparklarda kiçik və orta innovativ müəssisələrin, sahibkarlıq fəaliyyəti ilə məşğul olan rezidentlərin fərdi informasiyalarının qorunması, keyfiyyətli nəticələrinin əldə olunması texnoparkların səmərəli idarə olunmasına, onun informasiya təminatının yaxşılaşdırılmasına, informasiya təhlükəsizliyinin qorunmasına və uğurlu fəaliyyətinə əhəmiyyətli dərəcədə təsir edir. Bu səbəbdən də texnoparklarda fəaliyyət göstərən rezidentlərin fərdi informasiyalarının, fərdi innovativ ideyalarının, “Nou-hau”larının qorunması zəruri və aktual məsələlərdən hesab olunur.

IV. TEXNOPARKLARDA REZİDENTLƏRİN FƏRDİ MƏLUMATLARININ TƏHLÜKƏSİZLİYİ

Texnoparklarda istər fərdi innovativ ideyaların, istərsə də personalla bağlı olan məlumatların təhlükəsizliyi mövcud qanunvericiliklə tənzimlənir. Ümumiyyətlə fərdi məlumatlar şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumatdır. Fərdi məlumatların toplanılması, işlənilməsi və mühafizəsi prinsipləri, fərdi məlumatların informasiya ehtiyatlarında formalaşdırılması, informasiya sistemlərinin yaradılması, informasiyanın verilməsi və ötürülməsi qaydaları bu sahə üzrə müvafiq qanunda əks olunmuşdur [8].

Fərdi məlumatlar daha çox emal proseslərinə cəlb olunur. Avtomatik emal olunan fərdi məlumatların xüsusiyyətləri [9]: məlumat qanuni bir şəkildə alınmalı və işlənməlidir; dəqiq müəyyən edilmiş və qanuni məqsədlər üçün toplanmalı və bu məqsədlərə zidd olaraq istifadə edilməməlidir; adekvat, əlaqəli və işlənmə məqsədlərinə görə həddindən artıq olmamalıdır; məlumat dəqiq olmalı və ehtiyac olduğu halda yenilənməlidir; məlumat subyektlərinin məlumatların toplanması məqsədi ilə tələb olduğu müddətdən artıq olmasına imkan verən bir formada saxlanılmalıdır.

Fərdi məlumatların irqi, milli, siyasi görüşləri və s. ilə bağlı xüsusi fərdi məlumatlar, biometrik fərdi məlumatların bioloji və fizioloji xüsusiyyətləri, açıq fərdi məlumatlar (doğum tarixi, yeri, peşə, ixtisas məlumatları və s.) və s. kimi kateqoriyaları vardır [10].

İnnovasiyalı iqtisadiyyatı formalaşdıran və onun davamlı inkişafına əhəmiyyətli dərəcədə təsir edən əsas iqtisadi strukturlardan biri texnoparklardır. Texnoparklar mahiyyət və məzmun etibarilə digər iqtisadi strukturlardan daha çox fərdi innovativ ideyaları, elmi və texnoloji tutumu, “Nou-hau”ların çoxluğu, elmi-tədqiqatların innovativliyi, elmi-texniki kommersiya sirləri, müəllif hüquqlarının daha ciddi qorunması zərurəti, intellektual mülkiyyət məsələlərinə daha çox diqqət yetirilməsi və s. ilə fərqlənir [11, 12].

Elm və texnologiya və tədqiqat parkları innovasiya sahələrinin iqtisadi inkişafında əsas rol oynadığından dünyada minlərlə innovasiya şirkətləri və tədqiqat institutlarını bir yere toplayan, öz rezident şirkətlərinin beynəlmilləşməsinə töhfə verən qlobal şəbəkədə fəaliyyət göstərirlər [7].

Texnoparklarda rezidentlərin fərdi məlumatlarının qorunmasının aşağıdakı kimi mərhələləri vardır [10]: 1) fərdi məlumatların emalını həyata keçirmək üçün bütün mümkün vəziyyətləri müəyyənləşdirmək, 2) fərdi məlumatlar emal olunan zaman biznes-proseslərinin seçilməsi, 3) informasiya sistemlərinin əhatə dairəsini və işlənilən, emal olunan fərdi məlumatların məcmusunu müəyyən etmək, 4) fərdi məlumatları emal edən hər bir informasiya sistemi üçün müasir idarəetmə modelinin yaradılması, 5) fərdi məlumatların operatoru kimi qeydiyyatı alınmaq üçün fərdi məlumat subyektlərinin hüquqlarının müdafiəsi üzrə səlahiyyətli orqana fərdi məlumatların emalı haqqında məlumat vermək, 6)

məlumatın müdafiəsinin mənimsənilmə sinfini nəzərə alaraq fərdi məlumatların konkret informasiya sistemi üçün tələblərini hazırlamaq, 7) fərdi məlumatların qorunma sisteminin hazırlanması və tətbiq edilməsi, 8) fərdi məlumatların subyektlərindən fərdi məlumatların emal olunmasına razılığın alınması, 9) fərdi məlumatların təhlükəsizlik pozulmalarının üzə çıxardılması üçün nəzarət tədbirlərinin həyata keçirilməsi və s.

Texnoparklarda fərdi məlumatların toplanılmasının, işlənilməsinin və mühafizəsinin əsas prinsipləri. Fərdi məlumatların informasiya ehtiyatlarının formalaşdırılması, onların informasiya sistemlərinin yaradılması ölkə qanunvericiliyində təsbit edilmiş əsas insan və vətəndaş hüquq və azadlıqlarına riayət edilməklə, qanunçuluq, konfidensiallıq, könüllülüyün məcburiliklə uzlaşdırılması prinsiplərinə uyğun həyata keçirilir [8].

Fərdi məlumatların toplanılması, işlənilməsi və mühafizəsi prosesində insanın həyat və sağlamlığı üçün təhlükə yaradılmasına, onun şərəf və ləyaqətinin alçaldılmasına yol verilmir. Fərdi məlumatlar toplandığı andan mühafizə olunur və bu məqsədlə əldə olunma növünə görə konfidensial və açıq kateqoriyalara bölünür.

Texnoparklarda fərdi məlumatların mühafizəsinin bir çox metodları vardır. Texnoparklarda fərdi məlumatların informasiya təhlükəsizliyinin ümumi metodlarına aşağıdakıları aid etmək olar [13]: 1) fərdi məlumatların informasiya təhlükəsizliyi sahəsində münasibətləri tənzimləyən qanunvericiliyin təkmilləşdirilməsi; 2) istifadəçilərin icazəsiz girişinə görə məsuliyyətin müəyyənləşdirilməsi; 3) milli şəbəkələrin inkişafı prioritetinin qanunvericilik səviyyəsinin gücləndirilməsi; 4) fərdi məlumatların informasiya təhlükəsizliyinin təminatı sisteminin yaradılması, təkmilləşdirilməsi və idarə edilməsi; 5) fərdi məlumatların qorunma vasitələrinin effektivliyinə nəzarət metodlarının təkmilləşdirilməsi, istifadəsi və işlənilməsi; 6) fərdi məlumatların təhlükəsizliyinin təminatı sahəsində kadrların hazırlanması; 7) fərdi məlumatların təhlükəsizliyinin göstəriciləri üzrə monitoring sisteminin formalaşması; 8) fərdi məlumatların təhlükəsizliyinin təminatı və onun maliyyələşdirilməsinin nizamlanması; 9) fərdi məlumatların təhlükəsizlik sistemlərinin iqtisadi əsaslandırılması; 10) fərdi məlumatlara təhlükəsizliklə bağlı vurulan ziyanların qiymətləndirilməsi və s.

Rezidentlərin fərdi məlumatlarının təhlükəsizliyi məsələləri kompleks xarakter daşıyır. Həmin məsələlər istənilən innovativ müəssisənin və ya texnoparkların yerinə yetirdiyi funksiyalardan asılıdır [14]. Texnoparkların idarəetmə prosesində informasiya təminatının əsas təhlükəsizlik komponentləri aşağıdakılardır: 1) rezidentlərin faktiki təhlükəsiz məlumatlarla təmin edilməsi, 2) avtomatlaşdırılmış idarəetmə sistemləri üçün informasiya təminatından istifadə, 3) idarəetmə fəaliyyətinin təminatı üçün təhlükəsiz informasiyadan istifadə, 4) informasiya mənbələrinin seçilməsi və təyini, 5) alınmış məlumatların

düzgün interpretasiyası və sistemləşdirməsi, 6) verilənlərin etibarlılığının, tamlığının və ziddiyyətsizliyinin yoxlanılması, 7) informasiyanın qəbulu, saxlanması və çoxaldılması məsələsi, 8) verilənlərin ötürülməsi üçün vahid formatda təqdimat, 9) alınmış informasiyanın təkrar istifadəsi, 10) məlumatların daimi yenilənməsi.

Texnoparklarda rezidentlərin fərdi məlumatlarının təhlükəsizliyinin təmin edilməsinin və təhlükəsizlik sisteminin yaradılmasının əsas funksiyaları aşağıdakılardır: 1) rezidentlərdə məxfi informasiyanın qorunmasının təşkili və həyata keçirilməsi; 2) rezidentlərin fəaliyyəti haqqında məxfi məlumat əldə etmək məqsədi ilə işçi heyət ilə bağlı təxribatlar; digər hərəkətlər haqqında məlumatların yoxlanılması; 3) rezidentlərin təhlükəsizlik məsələləri üzrə informasiyanın təhlili və avtomatlaşdırılmış uçotu, yığım və toplanmasının təşkili; 4) sənaye sirri haqqında müddəaların hazırlanması və həyata keçirilməsi; 5) xüsusi idarəetmə qaydalarının yoxlanılması; 6) rezidentlərdə iqtisadi, informasiya və fiziki təhlükəsizlik qaydalarına riayət etmək üçün işçilərin yoxlanılması; 7) arzuolunmaz tərəfdaşlarla sazişlərin qarşısının alınması məqsədi ilə zəruri informasiyanın yığımı, emalı, saxlanması və analizi; 8) rezident strukturu rəhbərliyinin tapşırıqlarının yerinə yetirilməsi.

İnovativ informasiya iqtisadiyyatı şəraitində texnoparklarda elmi ideyalar kommersiyalaşdırılaraq beynəlxalq bazarlara çıxarılır. Buna görə də elmi ideyaların kommersiyalaşdırılması zəncirində fərdi informasiyaların, məlumatların, ideyaların təhlili aparılmalı, həmin elmi ideyaların kommersiyalaşdırılması üçün təhlükəsizlik tədbirləri görülməli və təkmilləşdirilməlidir.

V. ELMİ-TEKNİKİ İDEYALARIN KOMMERSİYALAŞDIRILMASI ZƏNCİRİNDƏ FƏRDİ MƏLUMATLARIN QORUNMASI

Elmi ideyaların reallaşdırılması zərurəti. Cəmiyyətin ictimai və sosial-iqtisadi həyatında elmin, elmi-texniki ideyaların və biliklərin xüsusi çəkisi durmadan artır. Yeni texnologiyalar və müasir texniki avadanlıqlardan düzgün istifadə üçün elmin infrastrukturunun səmərəli təşkili, həmçinin onun prioritet sahələrinin müəyyənəşdirilməsi və inkişaf etdirilməsi həyata keçirilməlidir.

Müasir tələblərə müvafiq olaraq, elmi-texniki ideyaların reallaşdırılması cəmiyyət qarşısında duran ən mühüm vəzifələrdən biridir. Müasir dövrdə elm həm də iqtisadiyyatın tərkib hissələrindən biri kimi çıxış edir. Belə ki, yeni elmi biliklərin və ideyaların kommersiyalaşdırılması hesabına alınan nəticələr iqtisadiyyatın inkişafına böyük təkan verir [15].

Əsas məsələ mövcud vəziyyətin düzgün qiymətləndirilməsi, səmərəli iqtisadi və elmi-texniki siyasət yeridilməsi, innovativ proseslərin elmi əsaslarla idarə edilməsidir. Elmi-texniki ideyaların tətbiqi prosesinin elmi əsasları cəmiyyətin intellektual resurslarının cəmləşməsinə və

ona optimal istiqamət verilməsinə imkan yaradır. Elmin tətbiqi oluna bilməsi üçün yüksək elmi-texniki tutumlu, dayanıqlı iqtisadi sistem və qərarlaşmış istehsal müəssisələri şəbəkəsi lazımdır.

Hər hansı ölkədə möhkəm iqtisadi bazis olmadan böyük innovativ proqramlara və layihələrə kapital qoyulması doğru deyil. Elm ancaq düzgün iqtisadi təməl və qərarlaşmış istehsal sistemi şəraitində inkişaf edə bilər və elmi-texniki ideyalar praktiki reallaşma nəticəsində innovasiyalara çevrilə bilər [3].

İnnovasiyanın kommersiyalaşdırılması innovasiya proseslərinin nəticəsi olan innovasiya məhsullarının və xidmətlərinin satışı və ya satışına kömək edən fəaliyyət növüdür. Bu prosesin gedişində elmi nəticə və ya texnoloji layihə kommersiya effekti alınmaqla həyata keçirilir.

Şəkil 3. Elmi ideyaların, innovasiyaların kommersiyalaşdırılması prosesinin təhlükəsizlik modeli

Elmi ideyaların, innovasiyaların kommersiyalaşdırılması mərhələlərində təhlükəsizlik. İnnovasiya istehsalının kommersiyalaşdırılması prosesinin təhlükəsizliyini aydın başa düşmək üçün innovasiya məhsulunun (texniki məmulatın, müxtəlif təyinatlı texnologiya və sistemlərin) ardıcıl mərhələlərdən ibarət istehsal prosesini təhlil etmək lazımdır [16]: 1) ETTKİ-nin sona çatması, 2) təcrübi istehsal, 3) kiçik seriyalı istehsal, 4) sənaye istehsalı.

Bu halda, hər bir mərhələyə məhsulun müəyyən vəziyyəti uyğundur: təcrübi nümunə, təcrübi partiya, seriyalı və ya sənaye istehsalı. İnnovasiya məhsulunun istehsalının müxtəlif mərhələlərdə kommersiyalaşdırılması prosesini şəkil 3-dəki kimi vermək olar.

İnnovasiya istehsalının mərhələlərindən hər hansı birində kommersiyalaşdırılmasının təminatı innovasiya siyasətinin və

onun məqsədlərinin prioritetlərinin düzgün münasibətini nəzərdə tutan şərtlər tələb edir.

Ümumiyyətlə elmi innovasiyaların kommersiyalaşdırılması aşağıdakı mərhələlərdən ibarətdir: 1) fundamental tədqiqatların təhlili; 2) tətbiqi tədqiqatların təhlili; 3) marketing tədqiqatların təhlili; 4) innovasiyaların bazara tətbiqi nəticələrinin təhlili.

İnnovasiyanın kommersiyalaşması modelinə aşağıdakı elementlər, blok, mərhələ və verilənlər aiddir [15]: 1) fundamental tədqiqatların (FT) verilənləri, 2) FT təhlilinin nəticələri, 3) tətbiqi tədqiqatların (TT) verilənləri, 4) TT təhlilinin nəticələri, 5) təcrübi-konstruktor işləri (TKİ) verilənləri, 6)TKİ təhlilinin nəticələri, 7) tətbiqdən bazara doğru olan verilənlər, 8) tətbiqin təhlilinin nəticələri, 9) tətbiqin nəticələrinin təhlili, 10) kommersiyalaşmanın səmərəliliyinin qiymətləndirilməsi, 11) marketing tədqiqatları və rəqabət qabiliyyətliliyinin qiymətləndirilməsi, 12) məhsulun nümayiş etdirilməsi, 13) fundamental tədqiqatların təhlil bloku, 14) ideyadan imtina edilməsi mərhələsi, 15) ixtiradan imtina edilməsi, 16) məhsuldan imtina edilməsi mərhələsi.

İnnovasiyanın kommersiyalaşdırılması fundamental tədqiqatların aparılması anından başlanılır ki, bu da perspektivli innovasiyaları ilkin mərhələdə müəyyən etməyə imkan verir.

NƏTİCƏ

İnnovativ informasiya iqtisadiyyatının formalaşması və inkişafı daha çox elmi ideyalardan, yeni xüsusiyyətlərə malik texnologiya və kəşflərdən asılıdır. Bu şəraitdə mühitin innovativliyi və təhlükəsizliyi xüsusi əhəmiyyətə malik olduğundan onların həyata keçirilməsi xüsusi yanaşma tələb edir. Problemin həlli üçün ən yeni İKT nailiyyətlərindən yararlanmaqla müvafiq kompüter modellərinin və instrumentariyasının işlənilməsinə və tətbiqinə ciddi ehtiyac vardır.

İSTİNADLAR

- [1] Milli iqtisadiyyat və iqtisadiyyatın əsas sektorları üzrə Strateji Yol Xəritələri. Bakı, 6 dekabr 2016-cı il, www.president.az.
- [2] Azərbaycan Respublikasında İnformasiya Cəmiyyətinin İnkişafına dair 2014-2020-ci illər üçün Milli Strategiya. 02.04.2014-cü il, <https://president.az/articles/11312>
- [3] Global Innovation Index-2019. <https://www.globalinnovationindex.org/Home>.
- [4] R.M.Algulyev, A.G.Aliyev, V.A. Abbasova. The study of formation characteristics and development tendencies of international information and knowledge economy. Review of knowledge economy. 2017, vol.4, №1, pp.7-14.
- [5] Iago Cotrim Henriques, Vinicius Amorim Sobreiro, Herbert Kimura. Science and technology park: Future challenges. Technology in society, 2018, 53 pp.144-160.
- [6] K.G.Hobbs, A.N. Link, J.T. Scott. Science and technology parks: an annotated and analytical literature review. Journal of technology transfer, 2017, vol. 42, pp.957-976.
- [7] International Association of Science Parks and Areas of Innovation. <https://www.iasp.ws>.
- [8] Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu. Bakı şəhəri, 11 may 2010-cu il. <http://www.e-qanun.az/framework/19675>.
- [9] Е.Г.Воробьев. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных: Учебное пособие. – СПб., 2016. – 432 с.
- [10] В.М.Ячменева, Н.А. Дидык. Принципы защиты персональных данных в организации. Конференция: проблемы информационной безопасности, Симферополь, 14-16 февраля 2019 г., стр.41-42.
- [11] C.S.Hayter, A.N. Link. Why do knowledge-intensive entrepreneurial firms publish their innovative ideas? Academy of management perspectives. 2018, vol.32, issue 1, pp.141-155.
- [12] И.С.Ситникова. Экспресс-оценка ноу-хау при организации малых инновационных предприятий. Патенты и лицензии. Интеллектуальные права. 2014, №7, стр.39-41.
- [13] F.P.Piurcosky, M.A.Costa, R.F.Frogeri, et al. The general law for protecting personal data in Brazilian enterprises: An analysis of multiple cases. Suma De Negocios, 2019, vol.10, issue 23, pp.89-99.
- [14] Е.П.Сулима, Г.М.Самостроенко. Концептуальные основы создания предприятия на рынке услуг по защите персональных данных в условиях цифровой экономики. Экономика и предпринимательство. 2017, №9-4(86), стр.409-416.
- [15] А.К.Деметьева. Формирование механизмов коммерциализации результатов научно-технической деятельности университетов в системе трансфера знаний и технологий. Экономика и предпринимательство. 2016, №5(70), стр.106-113.
- [16] В.И.Кияев, А.В.Саитов. Комплексная информационная безопасность в управлении современным предприятием : учебное пособие, –СПб. : Изд-во СПбГЭУ, 2016, -222 с.

SECURITY ISSUES OF INDIVIDUAL INNOVATIVE IDEAS IN FORMATION OF INFORMATION ECONOMY

Roza Shahverdiyeva¹, Leyla Akbarova²

^{1,2}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹shahverdiyev@gmail.com, ²akberovaleyla4@gmail.com

Abstract – The paper is devoted to the issues and security of individual innovative ideas in the formation and development of the information economy. The problems of formation of an innovative information economy are demonstrated. The tasks of technoparks in the innovation and knowledge economy and the features of its creation are explained. Information about the sectors of the technological innovation economy in modern age is provided. Specific features, categories of individual innovative ideas, and stages of formation of residents' data protection in technoparks are identified. General methods of innovative ideas and personal data security in technoparks are analysed. Some recommendations are made to improve the analysis and protect relevant information in the commercialization of scientific ideas in the conditions of innovation economy.

Keywords: *innovation, information and knowledge economy, product and process innovations, technological innovation, innovative and scientific idea, technopark, resident firms, commercialization of science, personal data security*

Big data analitikası texnologiyaları və fərdi məlumatların təhlükəsizliyi problemləri

Şahənə Mansurova

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
depart3@iit.science.az

Xülasə— Məqalədə Big Data dövründə fərdi məlumatların məxfiliyinin qorunması məsələləri tədqiq olunmuşdur. Böyük həcmli verilənlər insanların həyat tərzinə, iş və təhsilinə müsbət təsir etməklə bərabər, onlar eyni zamanda bir sıra informasiya təhlükəsizliyi təhdidləri və problemləri ilə üzləşirlər. Buna görə də böyük verilənlər dövrünün qarşılaşdığı fərdi məlumatların təhlükəsizliyi problemləri böyük əhəmiyyət daşıyır. Big Data erasında fərdi məlumatların təhlükəsizliyinin qorunması məsələləri araşdırılmışdır. Sənaye 4.0 inqilabına təkan verən texnologiyaların fərdi məlumatlar üçün yaratdığı təhdidlər və bu texnologiyalarda fərdi məlumat sızıntısına səbəb olan amillər göstərilmiş və onların aradan qaldırılması üçün həll yolları təklif olunmuşdur.

Açar sözlər— big data; informasiya təhlükəsizliyi; Sənaye 4.0; fərdi məlumatların təhlükəsizliyi; əşyaların İnterneti; süni intellekt.

I. GİRİŞ

Müasir informasiya və kommunikasiya texnologiyalarının (İKT) inkişafı və çoxsaylı sahələrə tətbiqi nəticəsində əsaslı dəyişikliklər baş vermişdir. Müasir dövrdə bu dəyişikliklərdən biri də fəaliyyət sahələrində toplanan verilənlərin həcmnin böyük sürətlə artmasıdır. Bütün fəaliyyət sahələrində olduğu kimi elmdə də verilənlərin həcmi sürətlə artır. Emal edilən informasiyanın hazırkı partlayışı dövründə bu fenomen “Big Data” adlandırılır. Elmdə böyük həcmli elmi verilənlərin sürətlə artmasına e-elmin inkişafı səbəb olur. Elmi verilənlər növü, həcmi, istifadə olunma tezliyi, ömür tsikli və s. xüsusiyyətləri ilə fərqlənir. Araşdırmalarda əsasən 4 növ tədqiqat verilənləri xüsusi əhəmiyyətə malikdir: məlumat verilənləri, hesablama verilənləri, eksperimental verilənlər, müşahidə verilənləri. Həmin verilənlərin hər bir növü bu və ya digər dərəcədə konkret tədqiqatçı və ya tədqiqatçı qrupları ilə əlaqəlidir [1].

Big Data, verilənlərin potensial dəyərini araşdırmağı və nəhəng verilənlərin saxlanması və təhlili ilə iqtisadi və sosial inkişafa xidmət edir. Sənaye 4.0 İnqilabının meydana gəlməsi əşyaların İnterneti (Internet of Things - IoT), süni intellekt (Sİ), kiber-fiziki sistem (KFS) texnologiyalarının inkişafı ilə bağlıdır və onların müxtəlif sahələrə tətbiqi də öz növbəsində verilənlərin müxtəlif mənbəli və formatlı olması potensialını artırır.

Böyük verilənlər dövrünün başlanması təkcə sosial tərəqqi üçün vacib imkanlar yaratmır, eyni zamanda, bu texnologiyalar cəmiyyətə bir çox informasiya təhlükəsizliyi təhdidlərini və

fərdi məlumatların məxfiliyinin qorunması tələbini də gətirir. E-elm mühitinin də həll etdiyi məsələlərə görə təşkil olunduğu alt sistemlərində fərdi məlumatların qorunması prioritet məsələlərdən hesab olunur.

Beləliklə, Big Data texnologiyaları böyük potensiala malik olmaqla yanaşı, həm də müxtəlif fəaliyyət sahələrinə effektiv təsir göstərir. Bu texnologiyalar fərdi məlumatların təhlükəsizliyi baxımından ciddi problemlər yaradır. Verilənlərin toplanması, saxlanması və istifadəsi prosesində fərdi məlumatlar asanlıqla sızdırıla bilər və bunun da təyin edilməsi çətinləşir.

II. BIG DATA VƏ İNFORMASIYA TƏHLÜKƏSİZLİYİ

İKT-nin sürətli inkişafı kommunikasiya vasitələrinin çoxalmasına, yeni informasiya resurslarının yaranmasına, informasiyaya əlçatanlığın asanlaşmasına və s. səbəb olmuşdur. Bu isə öz növbəsində verilənlərin çox sürətli artımına gətirib çıxarır. Belə böyük həcmli verilənlərin analizi üçün ənənəvi texnologiyaların tətbiqi əlverişli deyil. Bu da yeni texnologiyaların inkişafı tələbini meydana gətirir. O, faydaları ilə yanaşı artan inkişafı fonunda informasiya təhlükəsizliyi problemlərini də ortaya çıxarır.

Big datanın tətbiq olunduğu sahələrdən asılı olmayaraq ümumi xarakteristikaları var və bu xarakteristikalar əsas problemləri özündə əks etdirir. Big data konsepsiyasına iki cür yanaşmaq olar: böyük ölçülü verilənlər və informasiya texnologiyalarının yeni bir növü kimi. Bir sözlə, big data konsepsiyası böyük məlumatların toplanması və emalı üçün paylanmış hesablama resurslarının imkanlarından istifadə edən yeni texnologiyadır [2].

İnformasiya sisteminin normal fəaliyyət prosesinə müdaxilə və ya informasiyanı icazəsiz əldə etməyə cəhd edən kənar şəxslər və təşkilatlar da informasiya təhlükəsizliyinə mühüm təsir göstərir. İnformasiya təhlükəsizliyi məsələləri təkcə emal edilən informasiyanın əlyetənliyinin, tamlığının və konfidensiallığının təmin edilməsi ilə bitmir. Problemin siyasi, hüquqi, iqtisadi, psixoloji, kadr təminatı və s. aspektlərini də nəzərə almaq vacibdir [3]. Fərdi məlumatlar şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumat toplusu olub, öz növbəsində şəxsi, həssas, coğrafi və s. olmaqla növləndirilir [4]. Müasir dövrdə fərdi məlumatların məxfiliyinin qorunması məsələləri təkcə milli deyil, eləcə də global xarakter daşıyır.

Big Data kontekstində fərdi məlumatlar çox vaxt İnternetdəki fərdi məlumatlarla əlaqələndirilir. Buna görə, fərdi məlumatları iki kateqoriyaya bölmək olar [5]:

- İnternetin yaranmasından əvvəlki fərdi məlumatlar,
- İnternetin yaranmasından sonrakı fərdi məlumatlar

Big data dövründə çoxsaylı fərdi məlumatlar davamlı olaraq artır və onların toplanması, yayılması və istifadəsi ilə əlaqədar risklərə aşağıdakıları misal göstərmək olar:

- Şəbəkə xidməti provayderi tərəfindən məlumatın əldə edilməsi,
- Haker və troyan təhdidləri,
- Qanunsuz məlumat dövriyyəsi.

İnformasiya təhlükəsizliyinin təmin edilməsində insanlar ilə yanaşı daha iki vacib komponent: proseslər və texnologiyalar iştirak edir [2]. Big Data texnologiyaları yeni müxtəlif mənbələrdən alınmış strukturlaşdırılmamış verilənlərin real zamanda emalını mümkün edir. Bu texnologiyalar tətbiq olunduğu sahələrdə inkişafa səbəb olmuşdur. Big Data texnologiyalarının tətbiqi fərdlər barəsində toplanan məlumatların və onların mənbələrinin hədsiz dərəcədə genişləndirilməsinə gətirib çıxarmışdır. Bu texnologiyalar sayəsində fərdi məlumatlardan sui-istifadə edilməsinin mənfi nəticələri təkcə ayrı-ayrı insanların şəxsi həyatlarının gizliliyinin pozulmasında deyil, ictimai həyatda, iqtisadiyyatda və siyasətdə də özünü göstərə bilər. Böyük məlumatlar kontekstində məlumatlar çox əlaqəlidir və məlumatların dərin təhlili müəyyən şəxslərin məxfilik məlumatlarını ifşa edə bilər [6]. Bu da insanların məlumat təhlükəsizliyi mövzusunda diqqətini artırır. Buna görə böyük məlumatların yaratdığı fərdi məlumat təhlükəsizliyi problemi diqqətdən kənarda qalmamalıdır.

III. SƏNAYE 4.0 VƏ BIG DATA

Sənayedə İKT-nin imkanlarının geniş miqyaslı tətbiqi “4-cü sənaye inqilabı” konsepsiyasını da öz bərabərində gətirdi. Bu inkişaf əlaqədar olaraq bir sıra ədəbiyyatlarda da “4-cü sənaye inqilabı” konsepsiyası barəsində bəhs edilməyə başlandı. Sənaye 4.0 inkişafına təkan verən əsas amilləri aşağıdakı kimi qeyd etmək olar [7]:

- informasiya və kommunikasiya texnologiyaları,
- kiber-fiziki sistemlər (KFS),
- şəbəkə texnologiyaları,
- süni intellekt (Sİ),
- big data və bulud texnologiyaları,
- modelləşdirmə, virtualizasiya və simulyasiya,
- insan-kompüter qarşılıqlığı və əməkdaşlığı üçün vasitələr.

Dördüncü sənaye inqilabı miqyası, həcmi və mürəkkəbliyinə görə bəşəriyyətin bütün əvvəlki təcrübələrinin heç birinə bənzəmir. Onun süni intellekt, robototexnika, nanotexnologiya, biotexnologiya və s. daxil olmaqla ən geniş sahələrdə heyratamiz texnoloji sıçrayışı yaradır. Bu texnoloji sıçrayışın gətirdiyi problemlərdən ən başlıcası fərdi məlumatların təhlükəsizliyi və məxfiliyinin qorunması məsələləridir. Dördüncü sənaye inqilabına təkan verən yeni texnologiyalarda məlumatların məxfiliyinin qorunması məsələlərinə dair bir sıra problemlər tədqiq olunmuş və onlar aşağıda qeyd edilmişdir.

A. Əşyaların İnterneti

Əşyaların İnterneti mahiyyətə İnternetə qoşulan obyekt, maşın və qurğulardan verilənlərin toplanması, saxlanması, emalı və analizi texnologiyasıdır [8]. Müxtəlif istifadə sahələrində IoT məlumatların məxfiliyi bir sıra tədqiqatlarda araşdırılmışdır [9-11]. Gələcək global IoT şəbəkəsi məxfiliklə bağlı problemlər gətirir. IoT-un tətbiqində məlumat məxfiliyinin pozulması səbəblərinə aşağıdakıları göstərmək olar:

- İlk “emal olunmamış” verilənlərin saxlanması;
- Cihazla təminat;
- Enerji məhdudiyyəti;
- Şifrələmə məhdudiyyəti;
- Standartlaşdırmanın qeyri-kafi təşkili;
- Cihaz səviyyəsində məlumat toplama və paylaşma perspektivi baxımından IoT cihaz istehsalçısından daha az məlumat əldə edilməsi.

B. Süni intellekt (Artificial Intelligence – AI)

Süni intellekt məlumatların məxfiliyinin pozulması siyahısında ön sıradadır. [12]-də Sİ-in gizlilik riski araşdırılmışdır. Real zamanda görüntünün emalı insanın şəxsiyyətini müəyyənləşdirir və milyonlarla fərdi məlumatların məxfiliyinin pozulmasına səbəb olur [13, 14]. Süni intellekt və robototexnikada verilənlərin məxfiliyi mövzusunda əsas problemlərə aşağıdakıları aid etmək olar:

- Sİ əsaslı texnologiyalar üçün məxfilik standartlaşdırılması yoxdur,
- İstifadəçidən razılıq toplamaq səmərəsizdir,
- Sİ qərarının qəbuluna nəzarət edilməlidir.

C. Kiber-fiziki sistemlər (Cyber-Physical System – CPS)

Sənaye 4.0-ın əsas məqsədi daha sürətli olmaq və istehsalın səmərəliliyini artırmaqdır. Sənaye 4.0 kontekstində istifadə olunan əsas texnologiya KFS-dir [15]. KFS müxtəlif fiziki obyektlər, süni altsistemlərdən ibarət olan və müxtəlif sensorlardan gələn əks əlaqələrdən istifadə etməklə idarə edilən sistemlərdir. KFS-nin işləməsi hesablama və fiziki proseslərin inteqrasiyası prinsipinə əsaslanır, yəni fiziki obyektlər sistemin bir hissəsini təşkil edir. KFS müstəqil və ağıllı bir sistem

yaradan və buna görə də fərqli və fiziki cəhətdən uzaq olan subyektlər arasında integrasiyanı asanlaşdıran və müxtəlif imkanlar yaradan texnologiyaların toplusudur. Bu sistem üç ardıcıl ssenariyə imkan verir: məlumatların generasiyası və əldə edilməsi, əvvəllər əldə edilmiş məlumatların hesablanması və birləşdirilməsi və nəhayət, qərar dəstəyi.

Ümumiyyətlə, KFS konfidensiallığı passivdir [16]. Tədqiqatda KFS-də konfidensiallığın pozulmasının iki yolu qeyd edilir:

- Fiziki səviyyədə: Bu cür gizlilik hücumu sistemin fiziki xüsusiyyətlərinə birbaşa müdaxilə edir. Məsələn, səhiyyə çipinin imkanlarını dəyişdirmək.
- Kiber səviyyədə: Kompüter virusu, proqram təminatı və şəbəkə hücumları KFS-ə kiber hücumdur. Məsələn, saxta sensor məlumatları.

D. Bulud və böyük verilənlər (Cloud and Big Data)

Böyük məlumatlar, şübhəsiz ki, Sənaye 4.0-də tətbiq olunan ən vacib texnologiyalardan biridir. Buna səbəb ağıllı alqoritmlərdən istifadə edərək strukturlaşdırılmış və strukturlaşdırılmamış verilənlərin geniş şəkildə toplanması, emal edilməsi və analiz edilməsidir.

Digər vacib bir texnologiya açıq sistemlərdə çox böyük həcmli verilənləri idarə etməyə və real vaxt rejimində əlaqəni təmin etməyə imkan verən bulud hesablamalarıdır. Bulud hesablamalar dünyanın istənilən yerindən istənilən vaxtda məlumat əldə etmək imkanı verir, bu da rahatlığı artırır [17]. Ağıllı fabrikdə məlumatlar rəqəmsal şəkildə ötürülür, buna görə kibertəhlükəsizlik yeni sənaye inqilabında əsas rol oynayır. İnformasiya təhlükəsizliyi sistemləri digər texnologiyaların potensialından tam istifadə üçün vacibdir.

Bulud hesablamalarının bu gün təşkilatlar üçün yaratdığı ən böyük və ən kritik təhdid həssas və şəxsi verilənlərin, informasiyanın həm qəsdən, həm də qəsdətsiz olaraq itkisidir [14].

Big Data araşdırması SI-nin iştirakından sonra sürətli, effektiv və dəqiq oldu. Big Data və Buludda olan əsas problemlər bunlardır:

- Məlumatların şifrələnməsi;
- Fiziki həssaslıq;
- Qeyri-müəyyən verilənlərin paylaşımı və mübadiləsi siyasəti;
- Böyük ölçülü verilənlərin toplanması.

IV. BIG DATA ERASINDA FƏRDİ MƏLUMAT TƏHLÜKƏSİZLİYİNİN KONSEPTUAL MƏSƏLƏLƏRİ

Dünya ölkələrinin təcrübəsində informasiyanın qorunması aktual məsələlərdən hesab olunur. İnformasiya təhlükəsizliyinin təmin olunması sahəsində fərdi məlumatların mühafizəsi mühüm problemlərdən biridir. Bu problemin həlli istiqamətində zəruri tədbirlərin həyata keçirilməsi məqsədi ilə milli normativ-hüquqi bazanın, eləcə də beynəlxalq hüquqi

mexanizmlərin formalaşdırılması olduqca əhəmiyyətlidir. Burada məsələyə ayrı-ayrı ölkələr kontekstində deyil, beynəlxalq qlobal informasiya təhlükəsizliyi kontekstində yanaşmaq lazımdır.

Böyük məlumatlar dövrünün gəlişi fərdi məlumatların məxfiliyinin qorunması ilə bağlı cəmiyyətdə yaranmış təhlükələrin aradan qaldırılması yollarını şərtləndirir. Beynəlxalq təcrübədə ortaya qoyulan bir sıra tələblərin ölkəmiz üçün də reallaşdırılması mühüm məsələlərdəndir. Bu tələbləri aşağıda qeyd olunduğu kimi növləndirə bilərik:

- Cari vəziyyətə uyğun olaraq hüquqi-normativ bazanın daim təkmilləşdirilməsi;
- Vətəndaşların maarifləndirilməsi və onlarda informasiya təhlükəsizliyi mədəniyyətinin tərkib hissəsi kimi fərdi məlumatların təhlükəsizliyi mədəniyyətinin formalaşdırılması (sosial şəbəkələr və s.).

Fərdi məlumatların təhlükəsizliyində həm təşkilati, həm hüquqi, həm də texnoloji məqamlar var və bunlar bir-birindən asılı olaraq inkişafdadır. Lakin texnologiyanın daha sürətli inkişafı bu inkişaf üsullarını dəyişir və yeni üsulların yaranmasına səbəb olur, bəzi üsulların köhnəlib yararsız olmasına gətirib çıxarır. Ona görə də hüquqi-normativ baza inkişafa uyğun olaraq daim təkmilləşdirilməlidir.

Cəmiyyətin informasiya fəaliyyətinin artması ilə informasiya təhdidlərinin sayı da artacaq. Bu təhdidlərin qarşısının alınması məqsədi ilə əhalinin məlumatlılıq səviyyəsinin yüksəldilməsi və maarifləndirilməsi istiqamətində tədbirlər görmək lazımdır. Tədris vasitələrinin köməyi ilə fərdi məlumatların təhlükəsizliyi mədəniyyətinin formalaşdırılması kütləvi şəkildə həyata keçirilir.

Böyük məlumatlar dövründə yaradılan onlayn media insanlararası ünsiyyət üçün ən vacib məcralardan biri olmuşdur. Verilənlər haqqındakı informasiyaya olan nəzarətin gücləndirilməsi son dərəcə vacib məsələlərdəndir. İlk olaraq məlumatlara nəzarəti və idarəetməni gücləndirmək və anonim sosial media üçün şəbəkə məlumatlarını anonim olaraq qorumaq; sonra fərdi məlumat təhlükəsizliyinin cinayətkarlar tərəfindən istifadə edilməməsini və daha böyük itki verməməsini təmin etmək üçün sosial informasiyaya nəzarət və onu idarə etmək lazımdır. Bundan əlavə, istifadəçilərin təhlükəsizlik tədbirləri barəsindəki maarifləndirilməsini artırmaq və şəxsi vacib məlumatların doldurulmasını minimuma endirmək üçün özünü qorumaq və ehtiyatlı davranmağa ehtiyac duyulur. Nəhayət, hökumət ən qısa müddətdə böyük məlumatların tətbiqi üçün daha yaxşı qaydaları və tənzimlənmələri təqdim etməli və hüquqi aspektləri gücləndirməlidir.

NƏTİCƏ

Böyük məlumatların inkişafı kontekstində fərdi məlumatların təhlükəsizliyi ölkə və cəmiyyətin inkişafı üçün vacib strateji mövzu halına gəlmişdir. Ancaq səhv idarəetmə, haker hücumları və şəbəkə sisteminin təhlükəsizlik məsələlərindəki çatışmazlıqları səbəbi ilə fərdi məlumatlar

həmişə məxfiliyin pozulması ehtimalı ilə qarşılaşır. Müasir inkişaf tendensiyalarına əsasən milli təhlükəsizliyin təmin edilməsi sistemində fərdi məlumatların təhlükəsizliyi məsələsinin rolunun gələcəkdə daha da artacağını görmək olar. Big data məlumatlarının təhlükəsizliyi və məxfiliyinin qorunmasını həyata keçirmək üçün yalnız çox sayda peşəkar fərdi informasiya təhlükəsizliyi texnologiyası deyil, eyni zamanda ölkəmizdəki vətəndaşların məxfiliyinin qorunması ilə bağlı maarifləndirilməsinin gücləndirilməsi lazımdır ki, məlumatların məxfiliyi ilə bağlı təhlükəsizlik tədbirləri həyata keçirilə bilsin.

İSTİNADLAR

- [1] R.M.Əliquliyev, R.Q.Ələkbərov, T.X.Fətəliyev, Elektron elm: cari vəziyyəti, problemləri və perspektivləri, İnformasiya Texnologiyaları Problemləri, 2015, №2, səh.4-15.
- [2] Md Mehedi Hassan ONIK, Chul-Soo KIM, Jinhong, “Personal Data Privacy Challenges of the Fourth Industrial Revolution” ICACT, 2019, pp.635-638.
- [3] R.M.Əliquliyev, Y.N.İmamverdiyev, “İnformasiya təhlükəsizliyinin humanitar aspektləri” İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı. Bakı, 2015, S. 9-12.
- [4] Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu. 11 may 2010-cu il.
- [5] Cheng Chi1, Tengyu Liu, Xiaochen Yu, Shuo Zhang, and Shuo Shi, “Research on the Security of Personal Information in the Era of Big Data” AICON ,2019, LNICST 287, pp. 107–114.
- [6] Y. İmamverdiyev, “Big data və fərdi məlumatların təhlükəsizliyi,” Big data: imkanları, multidissiplinar problemləri və perspektivləri I respublika elmi-praktiki konfransı, 2016, s. 109-113.
- [7] H.Kinzel, “Industry 4.0 – Where does this leave the Human Factor?” https://www.researchgate.net/publication/308614137_Industry_40_-_Where_does_this_leave_the_Human_Factor.
- [8] T.X.Fətəliyev, Ş.A.Mehdiyev, “Böyük həcmli elmi verilənlərin menecmenti və emal texnologiyalarının tədqiqi” İnformasiya cəmiyyəti problemləri,2019, No 2, s. 60-70.
- [9] M.Conti, A.Dehghantanha, K.Franke, and S.Watson, “Internet of Things security and forensics: Challenges and opportunities” Elsevier, 2018.
- [10] M. H.Miraz, M. Ali, P. S. Excell, and R. Picking, “A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT),” Internet Technologies and Applications (ITA), 2015, pp. 219–224.
- [11] M. M. H. Onik, N. Al-Zaben, J. Yang, and C.-S.Kim, “Privacy of Things (PoT): Personally Identifiable Information Monitoring System for Smart Homes” in Proceedings of Symposium of the Korean Institute of communications and Information Sciences, 2018, pp. 256–257.
- [12] I. Priyadarshini, “Cyber Security Risks in Robotics” in Cyber Security and Threats: Concepts, Methodologies, Tools and Applications, IGI Global, 2018, pp. 1235–1250.
- [13] Z. Qin, J.Weng, Y. Cui, and K. Ren, “Privacy-Preserving Image Processing in the Cloud” IEEE Cloud Comput, vol. 5, no. 2, 2018, pp. 48–57.
- [14] Z. Xia, Y. Zhu, X. Sun, Z. Qin, and K. Ren, “Towards privacy preserving content-based image retrieval in cloud computing” IEEE Trans. Cloud Comput, vol. 6, no. 1, 2018, pp. 276–286.
- [15] Germany Trade and Invest. Industrie 4.0: Smart manufacturing for the future. 2014. Available from: http://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Brochures/Industries/industrie4.0-smart-manufacturing-for-the-future-en.pdf
- [16] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, “Security and privacy in cyber-physical systems: A survey of surveys” IEEE Des. Test, vol. 34, no. 4, 2017, pp. 7–17.
- [17] Z. Haiping, L. Yu, L. Qin, R. Yunqing. Cloud service platform for big data of manufacturing. Applied Mechanics and Materials. 2014;456:178-183. www.scientific.net/AMM.456.178.

BIG DATA ANALYTICS AND PERSONAL DATA SECURITY ISSUES

Shahana Mansurova

Institute of Information Technology of ANAS, Baku, Azerbaijan

depart3@iit.science.az

Abstract— The article explores the privacy protection issues of personal information for era of Big Data. In addition to having a positive impact on people's lifestyle, work and education, Big Data faces a range of information security threats and challenges. Therefore, the security issues of the personal data faced by the era of Big Data are of great importance. The security problems of personal data has been investigated in the era of Big Data. The threats to personal data posed by technologies that spurred the Industry 4.0 revolution and factors leading to leakage of personal data in these technologies have been shown and solutions have been proposed to overcome these factors.

Keywords— big data; information security; Industry 4.0; personal data security; Internet of Things; Artificial Intelligence.

Вопросы формирования правовой информатики в контексте защиты персональных данных

Аловсат Алиев¹, Роза Шахвердиева², Лейла Акперова³

^{1,2,3}Институт Информационных Технологий НАНА, Баку, Азербайджан

¹alovsat_qaraca@mail.ru, ²shahverdiyev@yandex.ru, ³akberovaleyla4@gmail.com

Аннотация – В статье анализируются вопросы формирования правовой информатики в контексте защиты персональных данных. Описываются содержания и особенности правовой персональной информации. Приводятся ресурсы правовой персональной информации. Указываются методы правового регулирования персональной информации. Описываются функции автоматизированной правовой информационной системы. Указываются пути формирования правовой информатики в области персональных данных. Рекомендуются информационные технологии в обеспечении доступности и качества персональной информации.

Ключевые слова - правовые проблемы, права человека, правовые информации, правовое регулирование, персональная информация, автоматизированные правовые информационные системы

I. ВВЕДЕНИЕ

В настоящее время многие информационные ресурсы посвящены правовому процессу, юриспруденции или деятельности правоохранительных органов в области персональных данных (ПД) [1-3].

Указанные секторы показывают актуальность исследования вопросов формирования правовой информатики в контексте защиты ПД. Однако проведенный анализ показывает, что в этой области отсутствует системный подход к этой проблеме [4]. Поэтому слабо были разработаны научно-технические и технологические основы формирования информатизации в этой области.

II. СОДЕРЖАНИЕ И ОСОБЕННОСТИ ПРАВОВОЙ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ

Правовая информация имеет специфические особенности, которые позволяют выделить её в самостоятельное понятие. Появление кибернетических методов в исследовании правовой проблематики повлекло за собой необходимость обобщения конкретных правовых терминов в информационном аспекте в единое понятие правовой информации.

Правовая информация является информационно-смысловым содержанием правовых норм. К ним следует

отнести не только нормативно-правовые акты высших и местных органов власти, но и судебную, арбитражную, нотариальную практику [5].

Содержанием правовой информации является не просто набор сведений о тех или иных общественных отношениях, но и их анализ. Информация становится правовой только тогда, когда она проходит через государственный механизм и находит свой метод регулирования, преобразуясь в форму закона, или какого-либо иного нормативно-правового акта.

Источники правовой информации подразделяются на официальные и неофициальные. Одним из таких источников являются ПД.

III. РЕСУРСЫ ПРАВОВОЙ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ

В настоящее время всем бухгалтерам, юристам, менеджерам и т.д. необходимо иметь полную, не устаревшую и удобную в использовании информацию о правовых актах и нормативных материалах в области ПД. Такая правовая информация также включает тексты и другие материалы, содержащие сведения о конкретном лице, предприятии и т.д., праве и правоприменительной практике, а также иные данные, которые требуются для соблюдения норм права. Разработанные правовые базы данных бывают общими и специализированными [6].

Основы государственной системы правовой информации составляют информационные ресурсы правоохранительных и законодательных органов.

К числу основных правовых информационных ресурсов в области ПД относятся:

- Комплекс баз данных правовой информации в области ПД.
- База данных действующего законодательства по личной жизни и по Защиты Персональных Данных (ЗПД).
- Государственный реестр общественных объединений и религиозных организаций.

Существует также и активно развивается рынок коммерческих правовых компьютерных систем. На сайтах правоохранительных органов можно найти самые

разнообразные сведения о правовых информационных ресурсах в области ПД [7].

Отметим, что те разработчики правовых систем, которые являются коммерческими организациями также весьма полно представлены в виртуальном мире.

IV. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПЕРСОНАЛЬНЫЙ ИНФОРМАЦИИ

В законодательстве отдельное место отведено преступлениям в области компьютерной информации [8].

Анализ подходов к определению регулирования персональной информации позволяет выделить ряд основных признаков, имеющих существенное значение для уяснения сущности данного понятия. Во-первых, такие информации представляют собой определенные сведения, факты, данные о различных лицах, процессах и явлениях, протекающих в природе и обществе.

Во-вторых, такую информацию можно представить как процесс, то есть в этом случае она является сообщением какому-либо субъекту определенных сведений, передачей информации.

В-третьих, это отражает психологическую сторону значения информации, и эта оценка, которую человек дает в своем сознании определенным явлениям, тоже является информацией.

Еще одним важным признаком персональной информации, который, с одной стороны, обусловлен сложностью правового регулирования общественных отношений, связанных с информацией, трудностью установления правового режима, а с другой – определена простота и легкость возникновения, изменения и прекращения указанных отношений, является нематериальный характер информации. И в этой связи персональная информация как нематериальное благо является особым объектом права [9]. Для персональной информации не страшен физический износ, она подвержена лишь возрастному старению. Информация неосвязаема, неупотребляема, неистребима.

В результате продажи персональной информации покупатель еще не получает на нее права собственности. Информация, являясь объектом нематериальным, не может рассматриваться без материального носителя. Таким образом, на основании важных признаков информации с точки зрения правовой науки персональную информацию можно определить как нематериальный объект, который представляет собой сведения о лицах, фактах, событиях, явлениях и процессах независимо от их формы и представления, а также результаты их оценки в сознании человека.

V. АВТОМАТИЗИРОВАННЫЕ ПРАВОВЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ (АПИС)

В настоящее время во многих странах функционируют десятки автоматизированных систем правовой персональной информации [10-12]. Необходимо отметить, что имеются два вида АИС правовой

информации: индексные и системы полного текста, которые можно называть и полнотекстовыми. Рассмотрим правовые АИС индексного вида. Можно отметить, что первой в Европе системой компьютерного поиска юридической информации была Бельгийская система "Credoc". В её информационной базе находится вся информация о законодательстве Бельгии, а также о международном праве. Кроме того, она содержит информацию о парламенте. В системе имеется теоретическая возможность осуществления поиска на основе тысяч различных поисковых предписаний.

Другой системой АИС является американская система WRU. Эта система является единственной в мире системой юридического поиска, в которой для индексирования документов используются слова информационно-поискового языка семантического кода, который был составлен специально для этого. Использование семантического кода позволяет быстро и безошибочно находить нужную информацию. Однако, эта система довольно неудобна для пользователей тем, что для индексирования документов требуется квалифицированный персонал, который должен составлять абстракты документов на естественном языке, с последующей его индексацией на искусственном языке семантического кода.

Следующей известной системой АИС является французская система "Jretiv". В информационной базе этой системы находится информация о судебных решениях. Базу данных составляют три множества: множество описаний документов, словарь, а также инверсионное множество. Множество описаний документов построено с соблюдением последовательного порядка и содержит библиографические данные документа, а также их абстракты. Оно используется для представления результата поиска. Система оснащена тезаурусом юридических терминов, который считается одним из лучших в мире.

Ещё одной интересной системой АИС является итальянская система "Italgire". В её информационной базе содержатся тезисы судебных решений по уголовным и гражданским делам, постановления Конституционного суда, а также данные о юридической литературе, носящие библиографический характер.

Польская система SJI (система юридической информации) содержит информацию о нормативно-правовых актах, центральный каталог юридической литературы, информацию о решениях Верховного суда.

Созданная система "Finlex" министерства юстиции Финляндии содержит информацию о судебных решениях различных судов. Имеется информация о юридической литературе, о договорах и международных соглашениях Финляндии, а также о законах страны.

Характеризуя роль индексных систем уместно отметить, что они составляют около половины всех работающих в мире систем автоматизированного поиска юридической персональной информации.

Другим видом АИС являются полнотекстовые системы. Первая полнотекстовая система поиска

юридической информации была создана (Питсбургская система "Aspen") в США. Разрабатываемые в настоящее время системы чаще всего опираются на идею построения, заложенную в этой системе.

В Канадской системе "Datum" документом является прецедент в полной, либо сокращённой форме. База данных состоит из четырёх множеств: текстового множества, словаря, инверсионного множества и главного множества. В английской системе "Status" база данных состоит из трёх множеств: текстового, инверсионного и перечня частот применения слов.

В настоящее время крупнейшей системой поиска юридической информации является американская система "Lexis". Она работает как диалоговая система и располагает сетью терминалов во многих штатах Америки, а также в Англии. В информационной базе системы находятся все судебные прецеденты США, а также нормативно-правовые акты штатов и федеральные документы, тексты конституции США.

Другой полнотекстовой системой АИС является французская система "Cedij". В этой системе содержатся сведения законодательного типа по отраслям: финансовое право, жилищное право, торговое право, строительное право, а также национальная оборона. Система "Cedij" располагает широким тезаурусом, указывающим различные грамматические формы, синонимы, соответствующие друг другу понятия.

Кроме систем полнотекстового и индексного типа в области поиска юридической персональной информации работают также системы, которые являются системами иерархической классификации, либо предметных слов. Опыты показали, что эти системы малоэффективны и располагают небольшими документационными базами.

VI. ФОРМИРОВАНИЕ ПРАВОВОЙ ИНФОРМАТИКИ ЗПД

Правовая информатика представляет собой прикладную ветвь общей информатики. Существуют различные подходы к пониманию задач и природы правовой информатики. В становлении и развитии идеи правовой информатики и правовой кибернетики большую роль сыграли работы академика Кудрявцева В.Н., члена-корреспондента РАН Керимова Д.А., доктора юридических наук Гаврилова О.А. и т. д. [13].

В задачи *правовой информатики* входят:

- активное участие в создании правового государства на принципах плюралистической демократии и гласности, доступности для каждого члена общества всей совокупности нормативных правовых аспектов, свободного получения информации в нужное время, и в нужном месте и в нужной форме;
- разработка научных и практических основ внедрения автоматизированных рабочих мест (АРМ), интеллектуальных и консультационных систем;

- интеллектуализация деятельности юридических учреждений и органов, повышение производительности труда и культуры в отправлении правосудия и других форм юридической работы;
- создание автоматизированных обучающих систем;
- разработка теоретических и методических проблем подготовки кадров и переподготовки юридических кадров, формирование корпуса молодых специалистов по новой юридической специальности – «правовая информатика».

В настоящее время правовую информатику в области ЗПД можно рассматривать как перспективное и быстро прогрессирующее направление научных исследований, которое имеет собственный предмет, задачи и методы исследований. Восприятие юристами положений и выводов информатики должно происходить через призму юридических понятий и категорий.

Отметим, что несмотря на короткий срок своего существования, правовая информатика добилась существенных успехов в реализации государственной политики информатизации правовой сферы. К ним относятся: создание сети центров и систем правовой информации; формирование законодательства об информации и информатизации; выход на международный уровень. Как и многие отрасли знания, правовая информатика делится на общую и специальную части. Общая часть включает [14]:

- Задачи создания общенациональной системы правовой информатики;
- Государственную политику информатизации правовой и политической системы;
- Понятие единого информационного пространства;
- Понятие общей и правовой информации;
- Методологию и методы исследования.

Правовую информатику в области ЗПД необходимо отличать от ряда смежных научных направлений.

Ныне постепенно происходит уточнение научного статуса и профиля правовой информатики. Правовая информатика не сложилась еще в полную самостоятельную науку. На шкале оценок она занимает ранг междисциплинарной отрасли знания.

VII. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБЕСПЕЧЕНИИ ДОСТУПНОСТИ И КАЧЕСТВА ПРАВОСУДИЯ

Использование ИТ для обеспечения доступности и качества правосудия давно уже вошло в обиход судебных систем развитых государств, и оправдало себя. В этой связи возникает логический вопрос «с чего начать?». Представляется, что необходимо начать с разработки и принятия соответствующей программы по информатизации деятельности судов. И только после

этого, комплексно, сбалансировано и последовательно претворять в жизнь цели и задачи этой программы.

Основная задача информатизации судов предполагает наполнение системы конкретными знаниями в виде специализированных программных средств и баз данных, обеспечивающих успешное выполнение специфических функций органов судебной власти [15].

Поэтому, перед разработчиками судебных ИТ стоит сложная проблема. Суть ее состоит в том, что необходимо автоматизировать не только традиционные функции отдельных судов, но и обеспечить автоматизированные решения системных задач с учетом всех внутрисистемных и внешних информационных связей органов судебной власти.

В процессе информатизации судов в качестве приоритетных должны рассматриваться задачи создания именно аналитических программ информационных ресурсов, позволяющих решать задачи судебной системы.

Следует отметить, что вышеуказанное нововведение не только обеспечит доступность правосудия, но и станет дополнительной гарантией обеспечения защиты прав человека.

ВЫВОДЫ

С учетом высказанных точек зрения можно отметить, что *правовая информатика* является междисциплинарной отраслью знания о закономерностях и особенностях информационных процессов в сфере юридической деятельности, об их автоматизации, о принципах построения и методиках использования автоматизированных информационных систем, создаваемых для совершенствования и повышения эффективности юридической деятельности и решения правовых задач на базе комплексного использования теории и методологии правовых наук, средств и методов математики, информатики и логики.

Особа часть правовой информатики исследует пути и задачи применения компьютерных технологий в различных сферах и направлениях государственно-правового регулирования общественных отношений: в правотворческой и правоприменительной деятельности, в криминалистике и судебной экспертизе, в социологических исследованиях, в области ЗПД.

ЛИТЕРАТУРА

- [1] Е.Г.Воробьев. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных. Учебное пособие / Санкт-Петербург, 2017.
- [2] А.Г.Чернецова. Персональные данные работника как информация ограниченного доступа: проблемы правового регулирования. Гуманитарные науки и образование в Сибири, 2015, №2(20), стр. 73-77.
- [3] С.Ю.Тимиршяхов, Ю.В.Тимиршяхова. Правовые проблемы защиты информации при обработке персональных данных. В сборнике: Правозащитная деятельность в современной России: проблемы и их решение Сборник научных трудов III Международной научно-практической конференции. 2017, стр.747-750.
- [4] А.С.Проскурин. Понятие правовой информации как основы информационного общества. Вестник Волгоградского Государственного Университета. Серия 5: Юриспруденция, 2016, Т. 15, №1(30), стр.51-57.
- [5] Т.Ю.Кирилина, Е.Н.Горбанева, А.В.Познякевич. Нормативно-правовое регулирование информационной безопасности автоматизированных систем управления технологическими процессами. Информационно-технологический вестник. 2018, №2(16), стр.78-85.
- [6] Н.В.Ключко, В.С.Негородов. Анализ нормативно-правовой базы открытых данных в России. Вестник университета. 2014, № 9, стр. 187-189.
- [7] Ю.С.Бердова. Роль дисциплины информатика и правовая информатика в развитии правовой информатизации общества. Экономика и предпринимательство, 2016, №2-2(67), стр.197-199.
- [8] Э.В.Талапина. Защита персональных данных в цифровую эпоху: Российское право в Европейском контексте. Труды Института государства и права Российской Академии Наук, 2018, Т.13, №5, стр.117-150.
- [9] Azərbaycan Respublikasının Cinayət Məcəlləsi. <http://www.e-qanun.az/code/11>
- [10] В.И.Федулов. Международно-правовые аспекты защиты прав человека при автоматизированной обработке персональных данных. Вестник Московского государственного областного университета. Серия: Юриспруденция, 2013, №1, стр.51-58.
- [11] А.Г.Алиев. Теоретико-прикладные аспекты информатизации гуманитарных отраслей // Баку, “ЭЛМ”, 2006 г., 474 с.
- [12] А.Н.Кудрявцева. Проблемы построения юридических конструкций на примере преступлений в сфере компьютерной информации. Юридическая техника, 2013, №7-2, стр.349-352.
- [13] И.С.Бударин. Государственная автоматизированная система правовой статистики в информационном пространстве. Вестник науки и образования, 2019, №19-1(73), стр.78-82.
- [14] Е.С.Подвальный, С.А.Рыков. Построение интеллектуального поиска данных в юридических справочных информационных системах. Регион: системы, экономика, управление, 2012, №2(17), стр.116-119.
- [15] С.Г.Чубукова. Правовая информатика в системе юридического образования. Правовая информатика, 2017, №1, стр.50-54.

ISSUES OF LEGAL INFORMATICS FORMATION IN THE CONTEXT OF PERSONAL DATA PROTECTION

Alovsat Aliyev¹, Roza Shahverdiyeva², Leyla Akbarova³

^{1,2,3}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹alovsat_qaraca@mail.ru, ²shahverdiyev@gmail.com,
³akberovaleyla4@gmail.com

Abstract – The paper analyzes the formation of legal informatics in the context of the personal data protection. The contents and features of legal personal information are described. The paper provides legal personal information resources. The methods of legal regulation of personal information are indicated. The functions of an automated legal information system are described. The ways of forming legal informatics in the field of personal data are indicated. Information technology is recommended in ensuring accessibility and quality of personal information.

Keywords – legal problems, human rights, legal information, legal regulation, personal information, automated legal information system

Elektron sağlamlıq kartlarında fərdi məlumatların təhlükəsizliyi problemləri

Aytən Əhmədova

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
ayten.adia.1996@gmail.com

Xülasə—Məqalədə elektron sağlamlıq kartlarında fərdi məlumatların təhlükəsizliyi məsələləri tədqiq olunmuşdur. Elektron sağlamlıq kartları haqqında qısa məlumat verilmiş, onlara olan təhlükəsizlik təhdidləri təsnifatlandırılmışdır. Elektron sağlamlıq kartlarının hansı şərtlər daxilində təhlükəsizliyinin təmin olunması qeyd olunmuş, fiziki sistemə giriş nəzarət olunması qaydaları və bir sıra şifrələmə üsulları göstərilmişdir.

Açar sözlər— elektron sağlamlıq qeydləri; tibbi sənədlər; fərdi məlumatların təhlükəsizliyi; təhdidlər; HIPAA

I. GİRİŞ

İnformasiya cəmiyyətinin formalaşması, ictimai həyatın bütün sahələrinə informasiya texnologiyalarının (İT) tətbiq edilməsi tibb sahəsində də öz təsirini göstərmişdir. Tibbi xidmətlərə artan tələbin təmin olunması probleminin konstruktiv həlli İT-nin səhiyyəyə inteqrasiyasından qaynaqlanır. İKT-nin tibb sahəsinə tətbiqi 2000-ci ildən əsas prioritetlər sırasına daxil edilmişdir [1].

Elektron sağlamlıq kartları (*ing. Electronic Health Cards, ESK*) fərdi, sağlam və məxfi bir mühitdə sağlamlıq məlumatlarının saxlandığı elektron tətbiqdır. ESK-ya fərdin doğulduğu gündən etibarən bütün ömür boyu məlumatlar qeyd olunmağa davam edir. ESK-da hər bir xəstə üçün fərdi məlumatlar (diagnostik təsvirlər, reseptlər, laborator testlər, aparılmış müşahidə nəticələri) yerləşir. Həkim həmin qeydlərdən istifadə etməklə kağız üzərində olan yazılı xəstəlik tarixçələrinin oxunmasına çox vaxt sərf etmir və xəstənin müalicəsi üçün lazımı müayinə üsulunun seçilməsi ilə bağlı onlara qərar qəbulunda operativ həll əldə edir [2,3].

Elektron tibbi kartların bir çox üstünlükləri vardır, lakin bu texnologiyada informasiya elektron mühitdə saxlandığı üçün fərdi məlumatlara qarşı məxfilik və təhlükəsizlik təhdidləri artmış olur. Odur ki, elektron səhiyyənin inkişaf etdiyi hazırkı dövrdə fərdi məlumatların təhlükəsizliyinin təmin edilməsi kifayət qədər aktual məsələdir.

II. ELEKTRON SAĞLAMLIQ KARTLARI

ESK xəstə haqqında bütün lazımı tibbi məlumatların toplanmasına və istifadə edilməsinə imkan verən məlumatlar bazasıdır.

1960-1970-ci illərdə sürətlə inkişaf edən yeni informasiya texnologiyaları ESK-nın inkişafına zəmin yaratdı və xəstələrin tibbi məlumatlarına dünyanın hər yerindən əlçatanlığını mümkün etdi [4]. ABŞ-da Muin Rochesterdəki “Mayo” klinikası 1960-cı illərin əvvəllərində ESK-nı qəbul edən ilk böyük sistemlərdən biri idi. Aparılan tədqiqatlara görə 1965-ci ilə qədər təxminən 73 xəstəxana və klinik informasiya layihələri tibbi sənədlərin və klinik məlumatların saxlanması və alınması üçün 28 layihə işləmişdir [5].

Tibbi məlumatların elektron mühitdə saxlanması aşağıdakı müsbət cəhətləri var [6]:

- tibbi sənədlərin dəqiqliyi və aydınlığını artırmaqla səhvlərin azaldılması;
- təkrarlanmaları azaltmaq, müalicədə gecikmələri minimuma endirmək, həkimlər tərəfindən daha etibarlı qərar qəbul edilməni təmin etmək.

[6]-də ESK-ların arxitekturası aşağıdakı kimi qruplaşdırılmışdır:

- *mərkəzləşmiş/tam inteqrasiya olunmuş model.* Bu modeldə bütün cavabdehlik Səhiyyə Nazirliyi və ya eSəhiyyə mərkəzlərinə verilir;
- *mərkəzi-paylanmış/federallaşmış model.* Burada ESK özü Səhiyyə Nazirliyinin öhdəsinə verilir, onun blokları isə müxtəlif səhiyyə təşkilatlarında yerləşir;
- *hibrid model.* Əvvəlki iki modelin birləşməsidir.

Arxitektura uyğun olaraq ESK-nın təhlükəsizliyi üçün müvafiq tədbirlər görülür.

III. ELEKTRON SAĞLAMLIQ KARTLARINDA TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Dünya səhiyyə provayderləri təhlükəsiz, effektiv, əlçatan və paylaşılan tibb xidmətləri göstərmək üçün ESK sistemlərinə böyük axınla miqrasiya edir. ESK fərdi tibbi məlumatların təhlükəsizliyinin təmin olunması üçün sistemin işlənməsi və təhlükəsizlik üçün optimal rejimin seçilməsini kifayət qədər aktuallaşdırır. İnsanların qapalı məlumatlarının yerləşdiyi ESK-ya girişi olan tibb müəssisələri tibbi məlumatların konfidensiallığına və təhlükəsizliyinə zəmanət verməlidir. Konfidensiallıq dedikdə, həmin məlumatlara giriş əldə etmiş şəxslərin xəstənin icazəsi olmadan onun fərdi məlumatlarını açmağa və yaymağa hüququnun olmaması başa düşülür.

Hüquqi baxımdan pasientin tibbi məlumatları əlçatanlığı məhdudlaşdırılmış, həkim sirri hesab olunan informasiyalara aid edilir və hər bir ölkədə fəaliyyət göstərən müəyyən qanunvericiliklə idarə olunur.

Elektron fərdi tibbi məlumatlarla işləyərkən aşağıdakı təhlükə və təhdidlər meydana çıxma bilər [2,3]:

- *təşkilati təhdidlər.* Bədənyyətə, icazəsi olmadan ESK-ya giriş edən şəxslər, hakerlər, insayderlər tərəfindən yaranan təhdidlər;

- *texniki təhdidlər.* Məlumatların itirilməsi, saxtalaşdırılması, fiziki daşıyıcıların məhv olması nəticəsində yaranan təhdidlər.

Məlumatın təhlükəsizliyi ilə bağlı təhdidlər adətən informasiyanın üç xüsusiyyətinə qarşı yönəlir [8]:

- konfidensiallıq;
- tamlıq;
- əlyetənlik.

Bütün bu xüsusiyyətlərin qorunması ESK-lar üçün vacibdir.

Bu xüsusiyyətlərdən hər hansı biri ilə bağlı təhlükəsizlik tədbiri lazımi səviyyədə olmazsa, pasiyentlər haqqında olan fərdi tibbi məlumatların təhlükəsizliyini təmin etmək çətinləşir.

Hazırda səhiyyə infrastrukturuna zərərli proqramlar, botnetlər kimi vasitələrlə kiberhücumların edilməsi halları çoxluq təşkil edir [7]. Kibertəhlükəsizlik insidentlərinin səhiyyə sistemlərinə göstərdiyi təsir böyük problemlərə gətirib çıxara bilər. Kibertəhlükəsizliyə qarşı dayanıqlı e-tibb sistemində aşağıdakı şərtlər təmin olunmalıdır:

- 1) fərdin müəyinə və müalicəsində ciddi fəsadlar yarada biləcək verilənlərin tamlığının təmin olunması;
- 2) e-səhiyyəni təşkil edən sistemlər arasında interaprobelliyin qorunması;
- 3) şəxsə aid olan fərdi tibbi məlumatların gizliliyinin təmin olunması;
- 4) fərdi tibbi məlumatlara ancaq səlahiyyətli şəxslərin istənilən vaxt girişinin təmin olunması üçün sistemdə əlçatanlığın mümkünlüyü.

Sistemdə insan səhvləri nəticəsində baş verən pozulmalara, insidentlərə tab gətirə bilən davamlı mexanizm işlənməlidir. Əks halda, yəni giriş nəzarət və autentifikasiya üsulları kifayət qədər olmazsa, fərdi məlumatların üçüncü şəxs tərəfindən ələ keçirilməsi baş verə bilər. Fərdi məlumatlara icazəsiz daxilolmalar nəticəsində klinik verilənlərin pozulması halları müşahidə olunur.

Məxfilik fərdi məlumatlar üzərində icazəli şəxslər tərəfindən nəzarəti ehtiva edir. Fərdi məlumatların digər şəxslər tərəfindən idarə olunması nəticəsində xəstənin fərdi tibbi məlumatları oğurlanır. Təhlükəsizlik təmin edildikdə həmin məlumatlara giriş məhdudlaşdırılır [9]. ESK sistemlərinin təhlükəsizliyi aşağıdakı üsullarla həyata keçirilir [10]:

- fiziki təhlükəsizlik – ESK-ya girişlərə nəzarət olunması;
- texniki təminatlar – şifrələmə və ya şəbəkələrarası ekran üsullarından istifadə olunması.

A. Fiziki sistemlərdə giriş nəzarət edilməsi mexanizmi

Fiziki sistemlərdə giriş nəzarət edilməsi mexanizmi aşağıdakıları ehtiva edir [11]:

- 1) məlumatlara daxilolma icazəsi olmayan şəxslər üçün əlçatmaz sistemin yaradılması;
- 2) sistemə daxil olmaq istəyən bütün şəxslər üçün şəxsiyyəti təsdiqləmə bölməsinin olması;
- 3) şifrə və fərdi identifikasiya nömrələrinin (FİN) təmin olunması;
- 4) proqramın avtomatik bağlanması prosedurunun yerinə yetirilməsi.

B. Şifrələmə üsulları

Şifrələmə proseslərində müxtəlif alqoritmlərdən ən uyğun olanı seçmək vacibdir. Aşağıda şifrələmə üsullarına nümunələr verilmişdir [12]:

–*CryptDB.* Proksi əsaslı şifrələmə sistemidir. CryptDB verilənlər bazasının şifrələnməsi üsulu ilə təhlükəsizliyi mümkün edir. Massaçuset Texnologiyalar İnstitutu tərəfindən yaradılmışdır və proksi şifrələməyə əsaslanan verilənlər bazası şifrələmə üsullarının əksəriyyəti CryptDB-nin formasına uyğun qurulmuşdur.

–*T-SQL şifrələmə* – tranzaktiv quruluşlu sorğu dili T-SQL Microsoft SQL server 2005-dən bəri tətbiq olunan bir şifrələmə üsuludur. Şifrələmə əsasən bir-birindən fərqli iki üsulla aparıla bilər:

Şəffaf şifrələmə (ing. Transparent data encryption). Bütövlükdə verilənlər bazasına tətbiq olunur. Bu şifrələmə üsulunda əməliyyatlar səhifələr üzrə aparılır.

Sütun şifrələmə (ing. Column level encryption)– Şəffaf şifrələmə üsulundan fərqli olaraq istənilən sütunun şifrələnməsi ilə həyata keçirilir və Encrypt Key, Decrypt Key funksiyaları tətbiq olunana qədər işləmir.

VI. HIPAA TƏHLÜKƏSİZLİK STANDARTI

1996-cı ildə ABŞ-da qəbul edilmiş Tibbi Konfidensiallıq və Mobilliyin Sığortalanması haqqında Qanun (*ing. The Health Insurance Portability and Accountability Act, HIPAA*) bütün e-tibb sistemində xəstə məlumatlarını qorumaq üçün məxfilik, təhlükəsizlik və elektron əməliyyat standartlarını tələb edən və mühafizə üsullarını təyin edən federal qanundur [13]. HIPAA standartında fərdi məlumatların təhlükəsizliyi şəxsi həyatın toxunulmazlığı və konfidensiallığı kimi iki vacib ideyaya əsaslanır. Şəxsi həyatın toxunulmazlığı dedikdə, xəstənin tibbi vəziyyəti haqqında kimin və nəyə əlçatanlığının olmasının

məhdudlaşdırılması, məlumatlara girişi olan şəxslərin məqsədləri barədə qaydaların olması kimi hüquqlar daxildir.

Təhlükəsizlik standartında tədbirlər üç başlıq altında (inzibati, fiziki, texniki) qruplaşdırılır [14].

– *İnzibati tədbirlər*: fəvqəladə hallar və görülməli tədbirlər, riayət ediləcək prosedurlar;

– *Fiziki tədbirlər*: sağlamlıq haqqında məlumat mühitinə fiziki giriş nəzarət tədbirləri;

– *Texniki tədbirlər*: hücumlardan qorunma, monitoring və qeyd üsulları, məlumat ötürülməsində istifadə edilə bilən şifrələmə metodları, daimi risk təhlili və risklərin idarə edilməsi.

NƏTİCƏ

Hazırda insanların elektron saxlanılan tibbi məlumatları sistemləşdirilmiş şəkildə ESK-da saxlanılır. Texnologiyanın inkişafı ilə e-tibbin formalaşması və onun əsas göstəricilərindən biri olan ESK-ların daha geniş vüsətlə artmasına zəmin yaradır. Digər tərəfdən bu yüksəliş onlarda olan fərdi tibbi məlumatların təhlükəsizliyinə yönəlmiş təhdidlərin ortaya çıxmasına səbəb olur. Məqalədə ESK-da olan fərdi tibbi məlumatların təhlükəsizliyi sahəsində bir sıra tədqiqatlar nəzərdən keçirilmiş, təhlükəsizlik üsullarının təsnifatı verilmiş, HIPAA standartı haqqında məlumat təqdim edilmişdir.

İSTİNADLAR

- [1] M. Məmmədova, Z. Cəbrayıllova “Elektron tibb: formalaşması və elmi nəzəri problemləri,” Bakı, pp. 86-105, 2019.
- [2] M. Məmmədova “The information security of personal medical data in an electronic environment,” Problems of Information Technology, no.2, pp.15-25, 2015.
- [3] M. Məmmədova “Elektron fərdi tibbi məlumatların informasiya təhlükəsizliyi problemləri,” “Elektron tibbin multidissiplinar problemləri” I respublika elmi-praktiki konfransı, s. 192-196, 2016.
- [4] R.S.Evans, “Electronic health records: Then now and future”, IMIA Yearbook of Medical Informatics, pp. 48-61, 2016.
- [5] A history of EHRs: 10 things to know, 2015.
<https://www.beckershospitalreview.com/healthcare-information-technology/a-history-of-ehrs-10-things-to-know.html>
- [6] Electronic health records,
[https://www.cms.gov/Medicare/E-Health/EHealthRecords/index.html#:~:targetText=An%20Electronic%20Health%20Record%20\(EHR,to%20streamline%20the%20clinician's%20workflow.](https://www.cms.gov/Medicare/E-Health/EHealthRecords/index.html#:~:targetText=An%20Electronic%20Health%20Record%20(EHR,to%20streamline%20the%20clinician's%20workflow.)

- [7] R. Əliquliyev, F. Abdullayeva “Fərdi tibbi məlumatların on-line mühitdə təhlükəsizliyi problemləri,” Elektron tibbin multidissiplinar problemləri I respublika elmi-praktiki konfransı, s. 104-109, 2016.
- [8] T. Sahama, B. Lane “Security and privacy in ehealth: Is it possible?”, IEEE 15th international conference on eHealth networking, applications and services, pp. 249-253, 2013.
- [9] P. Mehndiratta, S. Sachdeva, S. Kulshrestha “A model of privacy and security for electronic health records,” Databases in network information system, pp. 202-213, 2014.
- [10] V. Liu, M. A. Musen, T. Chou, “Data breaches of protected health information in the United States”, JAMA, 313(14), pp. 1471-1473, 2015. doi:10.1001/jama.2015.2252.
- [11] Electronic health records security and privacy concerns, General articles.
<https://www.ironmountain.com/resources/general-articles/e/electronic-health-records-security-and-privacy-concerns>
- [12] G. Dalkılıç, E. Karaarslan, “Elektronik sağlık kayıtlarının veri tabanında T-SQL ile şifrelenmesi ve başarımlı deneyleri”, Dokuz eylül üniversitesi mühendislik fakültesi fen ve mühendislik dergisi, cilt 20, sayı 58, s. 52-63, 2018.
- [13] V. M. Paksoy, “Security and privacy practices of electronic health records in terms of HIPAA standards: A case study in Turkey”, Sağlık akademisyenleri dergisi, 2019, cilt6, sayı 1, pp.63-69.
- [14] E. Karaarslan, “Elektronik sağlık kayıtlarının gizlilik ve mahremiyeti”, inet-tr, İstanbul december 2015.

SECURITY PROBLEMS OF PERSONAL DATA ON ELECTRONIC HEALTH CARDS

Aytan Ahmadova

Institute of Information Technology of ANAS, Baku, Azerbaijan

ayten.adia1996@gmail.com

Abstract – The article has been investigated security problems of personal data on electron health records. Brief information about electron health cards has been shown, the security threats to them have been classified. Conditions providing security of personal data on electron health cards have been analyzed, rules for access to the physical system and methods of encryption have been shown.

Keywords – *electronic health cards; medical documents; security of personal data; threats; HIPAA.*

Big data texnologiyalarında verilənlərin təhlükəsizliyinin əsas məsələləri

Aygül Fəxrəddinqızı
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
aygul.fexreddin@gmail.com

Xülasə— Verilənlər iqtisadiyyatın, sənayenin, təşkilatın, biznesin və fərdin vacib bir hissəsi olmaqla yanaşı İnternetin, ağıllı mobil qurğuların və sosial şəbəkələrin istifadəsi ilə günbəgün artır. Böyük verilənlər ölçüsü və mürəkkəbliyi ilə birlikdə iri həcmli verilənlər toplusudur və Verilənlər Bazasının İdarəetmə Sistemini (VBİS) saxlanması, idarə edilməsi və təhlil edilməsi olduqca çətinləşir. Böyük verilənlər küyün yığılması, ölçmə səhvləri, təhlükəsizlik və gizlilik də daxil olmaqla bir sıra problemləri özündə birləşdirir. Məqalənin əsas istiqaməti böyük verilənlərlə əlaqədar olan təhlükəsizlik və gizlilik məsələlərinə yönəldilmişdir. Məqalədə böyük ölçülü verilənlər konsepsiyası və bu verilənlərin təhlükəsizlik məsələləri nəzərdən keçirilir.

Açar sözlər— Böyük ölçülü verilənlər; big datanın təhlükəsizliyi; verilənlərin gizliliyi.

I. GİRİŞ

Texnoloji inkişaf və İnternetin geniş yayılması, o cümlədən, mövcud məlumatların həcmnin artması böyük ölçülü verilənlər konsepsiyasının meydana gəlməsinə səbəb olmuşdur. Böyük ölçülü verilənlər mənbələrdən əldə olunan iri həcmli, mürəkkəb verilənlər toplusudur. Bu məlumatlar toplusu o qədər böyükdür ki, onları artıq ənənəvi texnologiyalar vasitəsilə emal etmək mümkün deyil. Bu verilənlərin emalı üçün yeni texnologiyalardan istifadə etmək zərurəti yaranmışdır [1].

Böyük verilənlər konsepsiyasına ədəbiyyatda “Big Data” da deyirlər. Big datanın analizi vasitəsilə qiymətli məlumatlar və faydalı biliklər əldə etmək olar. Ancaq Big Datanın inkişafı təhlükəsizlik və gizlilik risklərini də özü ilə bərabər gətirir. Məsələn, online aldığımız məhsullar alış-veriş veb-saytı tərəfindən izlənilir; sosial şəbəkələrdə payladığımız fikirlərimiz və şəxsi şəkillərimiz sayt tərəfindən qeyd olunur; şəxsi mülkiyyət haqqında məlumat bankların nəzarəti altında olur. Bu da öz növbəsində məlumatların toplanması, saxlanması və istifadəsi zamanı fərdi məlumatların asanlıqla sızmasına və məlumatların klassifikasiyası zamanı çətinliklərə səbəb olur. Aydın ki, fərdi məlumatların sızması ciddi məsələdir. Böyük verilənlərin təhlükəsizliyini necə təmin etmək və gizliliyini qorumaq cari araşdırmalar mərhələsində ən aktual problemlərdən birinə çevrilmişdir. Bu verilənlərin təhlükəsizlik və gizlilik problemlərini necə həll etmək tədqiqatçıların əsas tədqiqat istiqamətinə çevrilmişdir [2]. Bunları nəzərə alaraq məqalədə II bölmədə Big Data təhlükəsizliyinin təmin edilməsi üçün mövcud yanaşmalar və

metodlar, III bölmədə böyük ölçülü verilənlər konsepsiyası, IV bölmədə Big Data təhlükəsizliyində əsas məsələlərdən bəhs olunur.

II. ƏLAQƏLİ İŞLƏR

Bəzi tədqiqatçılar Big Datanın təhlükəsizliyini təmin etmək məqsədilə atributların seçilməsi üçün metod təklif etdilər. Metod təhlükəylə üzləşəcək dəyərli məlumatları çıxararaq, böyük məlumatları təhlil edir [3]. Əsasən, bir-birilə uyğunluq yaradan məlumatlar çıxarılır. Belə ki, metod məlumatların klassifikasiya problemini həll etmir, yəni şəkillər, sənədlər, cədvəllər və real vaxt məlumatları (məsələn, VoIP rabitə) kimi müxtəlif tipli məlumatların emalına baxılmaz. [4,5]-də aparılan tədqiqatda Bulud şəbəkələrindən istifadə edilərək, böyük məlumatların qarşılaşdığı təhlükəsizlik problemləri araşdırılır. Tədqiqatçılar təklif etdikləri metodda şəbəkə təhlükəsizliyi, məlumat təhlükəsizliyi və gizlilik kimi məsələləri araşdıraraq, Bulud şəbəkələrində yayılmış Big Datanın tərkibinə daxil olmaq üçün yeni təhlükəsizlik modeli hazırlayıblar. Təklif olunan təhlükəsizlik modeli avtonom məlumatların qorunmasına yönəldilmiş və G-Hadoop paylanmış hesablama mühitində hazırlanmışdır. [6,7]-də aparılan tədqiqatda Storage-as-a-Service (STaaS) vasitəsilə paylanmış bulud anbarlarına müraciət edərək, Bulud şəbəkələri konsepsiyasında Big Datanın gizlilik məsələləri nəzərdən keçirilib. Həmçinin, Bulud Sistemləri və Əşyaların İnternetin (IoT) -də yaranan Big Data problemlərinə də toxunulub. Bundan əlavə, [8]-də gizlilik probleminə yönəldilmiş və Dynamic Data Encryption Strategiyası (D2ES) adlı verilənlərin şifrələnməsi üçün metod təklif edilmişdir. Metod vaxt məhdudiyyəti altında gizlilik təsnifatı metodlarından istifadə edərək məlumatları seçir və kodlaşdırır.

III. BÖYÜK ÖLÇÜLÜ VERİLƏNLƏR KONSEPSİYASI

Big data ənənəvi emal texnologiyalarından istifadə etməklə emalı çətin və ya qeyri-mümkün olan iri həcmli, sürətli və mürəkkəb verilənləri ifadə edir. Big datanın ən vacib əlamətlərindən biri verilənlərdən faydalı məlumat əldə etmək üçün yeni texnologiyaların istifadəsi və müxtəlif mənbələrdən verilənləri birləşdirmək qabiliyyətidir. Analitiklər üçün böyük miqdarda verilən əldə etmək və bu verilənləri saxlamaq məsələsi uzun müddətdir ki, aktualdır. Onu da qeyd edək ki, verilənlər ənənəvi olaraq relyativ verilənlər bazası kimi

strukturlaşdırılmış formatda saxlanılır. Ancaq İnformasiya Kommunikasiya Texnologiyalarının (İKT) inkişafı ilə yeni bir tendensiya meydana gəlmişdir: mövcud verilənlərin həcmi strukturlaşdırılmamış və ya yarım strukturlaşdırılmış formatda saxlamaq [9].

Böyük ölçülü verilənləri qiymətləndirəndə onun müəyyən meyarları nəzərə alınmalıdır. Ədəbiyyatda Big Datanın meyarları dedikdə Döngü Laneyin 6V xarakteristikası nəzərə çarpır (Şəkil 1). Bu xarakteristikaya bunlar daxildir [10]: Sürət, Həcm, Müxtəliflik, Dəyər, İnam, Mürəkkəblilik

Şəkil 1. Big Data-nın 6V xarakteristikası

- **Həcm.** Həcm xarakteristikasına görə böyük verilənlərin analizində istifadə ediləcək alqoritmlərin seçimi zamanı, aşağıdakı kriteriyalar diqqətə alınmalıdır: verilənlərin ölçüsü, yüksək ölçü məsələsi və outlierların/kənaraçıxmaların emalı.
- **Müxtəliflik.** Ənənəvi VBIS ilə xüsusi struktura malik olmayan məlumatların saxlanması və emalı çətin olsa da, “Big Data” mühitində bunun müxtəlif üsulları vardır. Müxtəliflik xarakteristikasına görə analiz üçün istifadə ediləcək alqoritmlərin seçimi zamanı, aşağıdakı kriteriyalar diqqətə alınmalıdır: verilənlərin tipi və klasterin forması.
- **Sürət.** Big Data prosesləri adətən saniyələr içərisində həyata keçirilir, yəni Big Data texnologiyaları sürətli formada verilənləri qəbul etməli, bu verilənlər üzərində görə biləcəyi işləri müəyyənləşdirib, analiz etməlidir. Əsasən Big Datada proseslər **real zaman anında, real zamana yaxın, batch** (müəyyən bloklar) şəklində aparılır. Sürət böyük həcmli verilənlərin analizində klasterləşdirmə alqoritminin sürətini ifadə edir və sürət xassəsinə uyğun klasterləşdirmə alqoritmini seçmək üçün aşağıdakı meyarlar nəzərə alınır: alqoritmin mürəkkəbliyi və işləmə müddəti.
- **İnam.** Böyük ölçülü verilənlər müxtəlif mənbələrdən əldə edilir, buna görə verilənlərin doğruluğunu / keyfiyyətini yoxlamaq tələb olunur.
- **Qiymət.** Giriş parametrləri klasterləşdirmə alqoritmlərinin verilənləri dəqiq yerinə yetirmək və daha az hesablama aparmaqla klaster əmələ gətirməsi mühüm rol oynayır.
- **Mürəkkəblilik.** Müxtəlif mənbələrdən alınan verilənlər fərqli quruluşa malikdir və həmin verilənlər bir-birilə

əlaqələndirilməlidir. Eyni verilənlər bazasında və ya çoxlu verilənlər bazasında müxtəlif dəyişənlər arasında yaranan əlaqəyə görə mürəkkəb verilənləri emal etmək və təhlil etmək çətinidir. Ənənəvi analiz alətləri dəyişənlər arasındakı münasibətləri aydınlaşdırmaq üçün çoxlu sayda iterasiya tələb edir. Dəyişənlər arasındakı bu əlaqəni tapmaq üçün mürəkkəb verilənlərin təhlili Big Data üçün üstünlüklər gətirir.

IV. BIG DATA TƏHLÜKƏSİZLİYİNDƏ ƏSAS MƏSƏLƏLƏR

İnternet, smart qurğular və sosial şəbəkələrdən istifadə nəticəsində verilənlərin sayı gündən-günə artır. Bu verilənlər Big Datanın həcmi və ya müxtəlifliyinə təsir etsə də, həmçinin verilənlərin təhlükəsizliyi və gizliliyi ilə bağlı məsələləri də ortaya qoyur. Böyük ölçülü verilənlər əhəmiyyətli və mürəkkəb bir mövzu olduğundan, təhlükəsizlik və gizlilik məsələlərinin ortaya çıxması demək olar ki, təbiiidir. Böyük ölçülü verilənlərin təhlükəsizliyini və gizliliyini təmin etmək ən vacib problemlərdən biridir. Bu problemlər verilən, proses, idarəetmə, ötürmə və saxlama ilə bağlıdır.

“Cloud Security Alliance” təşkilatındakı Big Data İş Qrupuna görə, Big Data təhlükəsizliyinin prinsipcə üç fərqli tərəfi var: infrastruktur təhlükəsizliyi, verilənlərin gizliliyi, verilənlərin idarə edilməsi [11].

İnfrastruktur təhlükəsizliyi – Burada ən çox istifadə olunan Hadoop texnologiyasına əsaslanan arxitektura xüsusilə vurğulanır.

Verilənlərin gizliliyi – həm istifadəçilər həm də təşkilatlar üçün ən böyük narahatlıqlar gətirəcək məsələlərdən biridir. Onlayn mühitdə çoxlu sayda fərdi məlumatlar toplanı bilər. Bu məlumatlardan isə bədənyyətli təşkilatlar (insanlar) öz mənafeyləri üçün istifadə edə bilərlər. Bu problemi aradan qaldırmaq üçün bir sıra metodlar işlənmişdir. Bu problemin həll olunmasının əsas yollarını göstərən bir neçə məsələ vardır: kriptografiya, konfidensiallıq, gizliliyi qoruyan sorğular, anonimləşəmə, sosial şəbəkələrdə gizlilik, diferensial gizlilik [12] və s. Bunlardan bəziləri ilə tanış olaq:

Kriptografiya Big Data sisteminə məlumatların gizliliyinin təmin edilməsi məsələsində ən çox istifadə olunan həll yoludur. Bu üsulla **bitmap** şifrələmə sxemi vasitəsilə verilənləri uzun müddət qorumaq olur. Sosial şəbəkələr hazırda böyük populyarlıq qazanmışdır və İnternetdən istifadə edən hər kəsin ən azı bir sosial şəbəkə hesabı vardır. İstifadəçilər sosial şəbəkələrdə fərdi məlumatlarını, şəxsi düşüncələrini paylaşır. Bu məlumatlar şəxsi məxfiliyimiz üçün də risklər yaradır [13]. Bu problemi həll etmək asan məsələ olmasa da bəzi tədqiqatçılar yeni konsepsiyalar təklif edərək verilənlərin məxfiliyini qismən təmin edə bilərlər.

Diferensial gizlilik ilk dəfə 2006-cı ildə Dwork, Nissim tərəfindən hazırlanmış hücum vasitəsidir. Əvvəlcə onu qeyd edək ki, diferensial gizlilik verilənlər bazasına deyil, sorğulara tətbiq olunur. Bu metodun əsas üstünlüyü **küç** üsulundan istifadə edilməsidir. Nəzərə alınacaq bir məsələ var ki, diferensial gizliliyi qorumaq üçün sorğular nə qədər geniş olarsa, o qədər küç tətbiq olunmalıdır. Bu da istifadəçilərin

şəxsiyyətlərini müəyyənləşdirmək qabiliyyətini minimuma endirir və bir sıra verilənlərin analizini asanlaşdırır.

Diferensial gizliliyin tərifinə nəzər salsaq, burada iki çoxluğa baxılır. Bu çoxluqlar D və D' kimi işarə olunur. Bunlardan birində fərdin məlumatları yer alıb, digərində isə həmin məlumatlar silinib və ya fərqli məlumatlarla əvəz olunub. Məsələnin əsas məqsədi prosesin sonunda D və D' -də olan fərdi məlumatlar arasında oxşarlıq maksimum olsun. Oxşarlıq ε parametri vasitəsilə ölçülür. ε parametri D və D' -dən alınmış nəticələrin paylanması nə dərəcədə yaxın olmasını ölçür və ε parametri kiçik olduqda gizliliyin təhlükəsizlik səviyyəsi yüksək olur [14].

Konfidensiallıq gizlilik termini ilə eyni olsa da, bunlar hüquqi baxımdan tamamilə fərqlənirlər. Konfidensiallıq müvəkkil, həkim, terapevt, vəkil və ya müştərinin razılığı olmadan fərdi məlumatların səlahiyyəti olmayan üçüncü şəxslərlə paylaşılmasıdır. Məsələn, onlayn ödəmə hesabınızla bağlı məlumatların başqa şəxsin əlinə keçməsi informasiyanın konfidensiallığının pozulmasıdır.

Digər tərəfdən, gizlilik isə fərdi məsələlərə və fərdi məlumatlara müdaxilə etmək hüququna aiddir. Konfidensiallıq etik cəhətdən doğru olsa da, gizlilik qanunlarda yer alan bir hüquqdur.

Verilənlərin idarə edilməsi – təşkilat və ya müəssisə tərəfindən yaradılan verilənlərin alınması, toplanması, təşkili və saxlanması prosesidir [15]. Effektiv verilənlərin idarə edilməsi müəssisə təbiiqetmələrini idarə edən və təşkilat idarəçiləri, iş menecerləri və istifadəçilər tərəfindən operativ qərarvermə və strateji planlaşdırmanı idarə etmək üçün analitik məlumat təqdim edən İnformasiya Texnologiyaları (İT) sistemlərinin istifadəsində vacib rol oynayır.

Ənənəvi emal texnologiyaları Big Data konsepsiyasının təhlükəsizliklə bağlı gətirdiyi problemlər qarşısında çarəsizdir. Şifrələmə metodları, girişlərin idarə edilməsi, firewalllar, ötürmə mühitlərinin təhlükəsizliyi və s. [16] kimi istifadə edilən metodlara müdaxilələr edilə bilər. Buna görə də bir çox aspektdən Big Data proseslərinə nəzarət etmək və təhlükəsizliyini təmin etmək məqsədilə yeni üsul və vaitələrin işlənməsinə ehtiyac vardır.

NƏTİCƏ

Big Data analitikasının əsas məqsədi çox sayda xam məlumatdan faydalı məlumat əldə etməkdir. Lakin bu zaman Big Data ilə bağlı bir sıra təhlükəsizlik məsələləri meydana çıxır. Məqalədə Big Data təhlükəsizliyi ilə bağlı əsas məsələlər nəzərdən keçirilmişdir. Burada şübhəli davranışların tez bir zamanda aşkarlanması üçün şəbəkə trafikinin daim izlənməsinin vacib olduğu vurğulanmış və bütün rabitənin təhlükəsiz kanallar üzərində aparılması, verilənlər bazasının yayımlanmadan əvvəl fərdi məlumatların “maskalanması” tövsiyyə olunmuşdur. Böyük verilənlərin məxfiliyi və təhlükəsizliyi istiqamətində daha çox tədqiqatlar aparılmalıdır. Gələcək işlərimizdə bu istiqamətdə, yəni verilənlərin təhlükəsizliyini təmin etmək məqsədilə yeni yanaşmaların verilməsi və klasterləşmə alqoritmlərinin müqayisəli təhlili nəzərdə tutulmuşdur.

İSTİNADLAR

- [1] Z. Dongpo, “Big data security and privacy protection,” In 8th International Conference on Management and Computer Science , vol.15, no. 2, 2018, pp.275–278.
- [2] F.Yan, “Big Data Security and Privacy Protection,”. Electronic Technology and Software Engineering, 2016, pp. 227-235.
- [3] I. Narasimha, A. Sailaja, and S. Ravuri, “Security Issues Associated with Big Data in Cloud Computing,” International Journal of Network Security and Its Applications, vol. 6, no. 3, 2014, pp. 45–56.
- [4] S.-H. Kim, N.-U. Kim, and T.-M. Chung, “Attribute relationship evaluation methodology for big data security,” in Proceedings of the 2013 3rd International Conference on IT Convergence and Security, ICTCS 2013, China, December 2013.
- [5] J. Zhao, L. Wang, J. Tao et al., “A security framework in G-Hadoop for big data computing across distributed cloud data centres,” Journal of Computer and System Sciences, vol. 80, no. 5, 2014, pp. 994–1007.
- [6] K. Gai, M. Qiu, and H. Zhao, “Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data,” in 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), New York, NY, Usa, April 2016, pp. 140–145.
- [7] Liu, C. Yang, X. Zhang, and J. Chen, “External integrity verification for outsourced big data in cloud and IoT: a big picture,” Future Generation Computer Systems, vol. 49, 2015, pp. 58–67.
- [8] K. Gai, M. Qiu, H. Zhao, and J. Xiong, “Privacy-Aware Adaptive Data Encryption Strategy of Big Data in Cloud Computing,” in Proceedings of the 3rd IEEE International Conference on Cyber Security, China, June 2016, pp. 273–278.
- [9] R.Ahquliyev, G.Niftəliyeva, “E-Dövlətin Big Data Mənbələri,” “Big data: imkanları, multidissiplinar problemləri və perspektivləri” I respublika elmi-praktiki konfransı Bakı şəhəri, 2016, pp. 78-80.
- [10] R.Patel, “Security & privacy of Big data: Big challenge for an organization,” IJSRD - International Journal for Scientific Research & Development, vol. 3, no. 11, 2016, pp.303-305.
- [11] A.A. Cardenas, P.K. Manadhata, S.P. Rajan, “Big Data Analytics for Security”, IEEE Security & Privacy, vol. 11, no. 6, 2013, pp. 74 – 76.
- [12] J.Moreno, M. A. Serrano and E. Fernández-Medina, “Main Issues in Big Data Security,” Department of Computer Science & Engineering, vol.4, 2016, pp.265-279.
- [13] B.B.Rada, N.Akbarzadeh, P. A. and Y.Khakbiz, “Security and Privacy Challenges in Big Data Era,” International Journal of Control Theory and Applications, vol. 9, no.43, 2016, pp.437-448.
- [14] Y.İmamverdiyev, “Big data və fərdi məlumatların təhlükəsizliyi,” “Big data: imkanları, multidissiplinar problemləri və perspektivləri” I respublika elmi-praktiki konfransı Bakı şəhəri, 2016, pp. 109-113.
- [15] B. Maturdi, X. Zhou, S. Li, F. Lin, “Big Data security and privacy: A review,” Big Data, Cloud & Mobile Computing, China Communications vol.11, no.14, 2014, pp. 135 – 145.
- [16] H. Cheng, C. Rong, K. Hwang, W. Wang, Y. Li, “Secure big data storage and sharing scheme for cloud tenants,” Communications, China, vol. 12, no.6, 2015, pp. 106 – 115.

MAIN SECURITY ISSUES IN BIG DATA TECHNOLOGIES

Aygul Fakhreddingizi

Institute of Information Technology of ANAS, Baku, Azerbaijan

aygul.fexreddin@gmail.com

Abstract – Data is becoming increasingly important as a significant part of the economy, industry, organization, business, and individual, with the use of the Internet, smart devices and social networks. This is a big data collection with a large volume and complexity of data, and it is extremely difficult to maintain, manage and analyze a Database Management System (DBMS). Big data contains a number of problems, including noise accumulation, measurement errors, security and privacy. The focus of the article is on security and privacy related to big data.

Keywords – big data; big data security; data privacy.

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, saxlanılır 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 tempisi ona gətirib çıxaracaq ki, yaxın gələcəkdə şəxsi həyat “susmaya görə” şəffaf və açıq olacaq – fərdi məlumatları dövlət və korporasiyalar üçün açmaq 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 müəyyənləməyə imkan verən istənilən məlumat (onun фамилиясы, 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 virtualaşır, 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 reyestrə 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 sayılı Konvensiya) imzaya açılmışdır. 108 sayılı 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 işlənməsini əhatə edir və

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 sayılı 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, informasiyalasdırma 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. İNFORMASIYA 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 təşkilatlı 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 legal 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 minimalaşdırılmasını 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 işlənilib 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 keçməsinə insan faktoru başlıca rol oynayır. Məsələn, aşağıdakı hallar ola bilər:

- İstifadəçinin müvəqqəti olaraq iş yerini tərk edən zaman kompüterini bağlamağı unutması və informasiyanın digər şəxs üçün əlçatın olması;
- Kompüterini şəbəkəyə qoşan zaman hansı informasiyanın digər şəxslər üçün əlçatın 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, fərdi məlumatların başqalarının əlinə keçməsinin səbəbləri arasında – təşkilatda çalışan əməkdaşların konfidensial informasiyanın qorunması üsullarını yetərinə 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 olunsaysa belə əməkdaşların informasiya təhlükəsizliyi mədəniyyətinin lazımı 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 ya açıq mənbələrdə yayılması; şəxsi informasiyanın təhlükəsiz əlaqə vasitələri ilə ötürülməsi; 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 IT-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 informasilaşdığı müasir dövrdə bəzən fərdi məlumatların sızması mənbəyini təyin etmək çətin olur. Lakin aparılan tədqiqatlar göstərir ki, fərdi məlumatlara əyləntiliyi 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 açıq, 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.

İnsanların 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 razılışmalarını imzalamaqla öz fərdi məlumatlarını istifadə etməyə razılıq verir. Beləliklə də, hər birimiz öz kompüterimizdən istifadə etməklə fərdi məlumatlarımızı açıq və konfidensiallıq hüququmuzu məhdudlaşdırırıq.

Keçmiş, indini və gələcəyi birləşdirən rəqəmsal iz məsələsi də fərdi məlumatların qorunması kontekstində olduqca aktuallıq kəsb edir. Övvələr, uzun müddət ərzində, xüsusi sayə 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 geolokasiya məlumatları, bəyənələr – 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. İNFORMASIYA 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 korporativ saytları dağıtmaqla cinayətkarlar müxtəlif konfidensial informasiyanı əldə etməyə nail olurlar.

Cəmiyyətdə informasiyanın rolunun və dəyərinin artdığı, strateji resurs 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 əlverişliliyinin təmin edilməsi;
- informasiya təhlükəsizliyi sahəsində kadr hazırlığı çərçivəsində informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması çərçivəsində tədris proqramlarının işlənilib 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 başlayaraq 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 böyükler 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 çıxarır 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 kontekstində 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

Rasmiyyə Mahmudova

Institute of Information Technologies of ANAS, Baku, Azerbaijan

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*