**AZƏRBAYCAN
MİLLİ ELMLƏR AKADEMİYASI
RƏYASƏT HEYƏTİ**

**AZƏRBAYCAN
MİLLİ ELMLƏR AKADEMİYASI
İNFORMASIYA TEXNOLOGİYALARI İNSTITUTU**

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

BAKİ ŞƏHƏRİ, 14 DEKABR 2018-Cİ İL

“İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri”

IV respublika konfransının

ƏSƏRLƏRİ

Bakı, 14 dekabr 2018-ci il

PROQRAM KOMITƏSİ

Sədr

akademik Rasim Əliquliyev

PROQRAM KOMITƏSİNİN ÜZVLƏRİ

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: 978-9952-434-99-6
DOI: 10.25045/NCInfoSec.2018

Mündəricat

<i>Rasim Əliquliyev, Yedgar Cəfərov, Fərhad Yusifov, Əfruz Qurbanova</i> , Elektron milli dövlət: Azərbaycan dilinin qorunması və inkişafı üçün imkanlar və perspektivlər.....	8
<i>Fərqanə Abdullayeva</i> , Bulud əsaslı elektron dövlət xidmətlərinin səmərəliliyinin artırılması metodu.....	13
<i>Bayram İbrahimov, Ramiz Humbatov, Rufat İbrahimov</i> , Analysis of information encryption methods in multichannel telecommunication systems.....	18
<i>Xalid Niyazov</i> , İnformasiya təhlükəsizliyi, hüquqi əsasları, müqayisəli yanaşma.....	22
<i>Sedat Akleylek, Kübra Seyhan</i> , Blok zinciri bileşenləri və uygulamaları üzerine bir derleme.....	27
<i>Rasim Əliquliyev, Ramiz Aliquliyev, Rasim Mahmudov</i> , Plagiatlıqla mübarizə informasiya təhlükəsizliyinin mühüm komponenti kimi.....	38
<i>Людмила Сухостат</i> , Разработка метода обнаружения атак на киберфизические системы на основе глубокого обучения.....	42
<i>Yadigar İmamverdiyev, Firəngiz Sadiyeva</i> , Kriptoalyuta verilənlərinin intellektual analizi məsələləri.....	47
<i>Ababil Nağıyeva, Sakit Verdiyev</i> , Rəqəmli təsvirlərin watershed üsulu ilə seqmentləşdirilməsi.....	53
<i>Bayram İbrahimov, Mirfatma Javadova</i> , Analysis of information protection methods in the system telecommunications based on quantum cryptography.....	58
<i>Oqtay Ələkbərov</i> , Blokçeyn texnologiyasının təhlükəsizlik məsələləri.....	61
<i>Rasim Əliquliyev, Ramiz Aliquliyev, İradə Ələkbərova</i> , Elektron dövlət mühitində sosial münasibətlərin təhlükəsizliyi.....	64
<i>Yadigar İmamverdiyev, Xəyalə Əhmədova</i> , Sosial şəbəkələrdə saxta profillərin aşkarlanması məsələləri.....	68
<i>Ramiz Şıxəliyev</i> , Müasir şəbəkə təhlükəsizliyi və inam problemləri.....	72
<i>Şəfqət Mahmudova</i> , Program təminatının təhlükəsizliyinin təmin olunmasının bəzi üsulları haqqında.....	75
<i>Yadigar İmamverdiyev, Ali məktəblərdə kibertəhlükəsizlik üzrə mütəxəssis hazırlığı problemləri.....</i>	79
<i>Həbib Abbasov</i> , Yeni nəsil şəxsiyyət vəsiqələrinin (E-ID) e-xidmətlərə inteqrasiyası problemləri.....	83
<i>Rasim Əliquliyev, Yedgar Cəfərov, Əfruz Qurbanova</i> , Qlobal informasiya cəmiyyəti şəraitində Azərbaycan vətəndaşlarının adlandırılması məsələləri.....	86
<i>Шакир Мехмиев, Аяз Мехдиев</i> , Некоторые вопросы безопасности применения дронов.....	91
<i>Hikmət Quliyev</i> , Folklor informasiya təhlükəsizliyində və informasiya təhlükəsizliyi folklorunda.....	95
<i>Rəna Qasimova</i> , İnternetdə Azərbaycan əlifbası ilə domen adlarının tərtib olunması məsələsi haqqında.....	101
<i>Тахмасиб Фаталиев, Шакир Мехмиев</i> , Вопросы обеспечения энергетической безопасности инфраструктуры электронной науки.....	105

<i>Yadigar İmamverdiyev, Günay Muradova, Neft-qaz sənayesində kibertəhlükəsizlik problemləri.....</i>	<i>109</i>
<i>Tural Yunusov, Kompüter şəbəkələrində zərərli proqramların analizi üsulları.....</i>	<i>113</i>
<i>Təbriz Ağaşov, Wi-Fi şəbəkəsində təhlükəsizlik məsələləri.....</i>	<i>116</i>
<i>Təhmasib Fətəliyev, Şahanə Mansurova, Enerji sektorunda kibertəhlükəsizliyin təmin olunması məsələləri haqqında.....</i>	<i>121</i>
<i>Yusif Sadiyev, Evaluating the indicators of web resources operating in the ccTLD domain zone as a key component of national security.....</i>	<i>125</i>
<i>Sabirə Ocaqverdiyeva, Verilənlərin sanitarizasiyasının informasiya təhlükəsizliyinin təmin olunmasında rolu.....</i>	<i>127</i>
<i>Tamilla Bayramova, Nəzakət Məlikova, Proqram təminatının testləşdirilməsi üçün sınaq texnologiyalarının təhlili.....</i>	<i>131</i>
<i>Səyyar Abdullayev, Tofiq Kazımov, Südabə Abasova, Qloballaşma şəraitində dilin inkişaf tendensiyləri və təhlükəsizliyi.....</i>	<i>135</i>
<i>Anar Səmidov; Zülfüyyə Həniyəyeva, 3D çap texnologiyaları və onların yaratdığı təhlükələr.....</i>	<i>139</i>
<i>Tofiq Kazımov, Tamilla Bayramova, Proqram təminatı işləyən komandaların idarə edilməsi üçün metrikalar.....</i>	<i>142</i>
<i>Nərgiz Abdullayeva, Sosial şəbəkələrdə gizlilik və təhlükəsizlik problemləri.....</i>	<i>145</i>
<i>Kəmalə Həşimova, İnternet-reklam marketinqində informasiya təhlükəsizliyi problemləri.....</i>	<i>147</i>
<i>Ələvsət Əliyev, İnformasiya iqtisadiyyatının kibertəhlükəsizliyinin təminatı istiqamətləri və texnologiyaları.....</i>	<i>150</i>
<i>Şəlalə Mansurova, IoT arxitekturasının səviyyələr üzrə təhlükəsizlik məsələləri.....</i>	<i>155</i>
<i>Günay İskəndərli, Elektron dövlətə kiberhücumlar və onlarla mübarizə üsulları haqqında.....</i>	<i>158</i>
<i>İradə Ələkbərova, Elektron dövlət mühitində fərdi məlumatların mühafizəsi problemləri.....</i>	<i>161</i>
<i>Rəhilə Həsənova, Firudin Əsgərov, İnternet mühitdə “yırtıcı” jurnalların avtomatik tanınması üçün intellektual sistemin yaradılmasının konseptual əsasları haqqında.....</i>	<i>165</i>
<i>Sünbül Zəlova, Süni intellekt texnologiyalarına əsaslanan jurnalistikanın formalaşması və inkişaf perspektivləri haqqında.....</i>	<i>169</i>
<i>Nərmən Adıgözəlova, “IEEE Transactions on Forensics and Information Security” jurnalının bibliometrik analizi (2006-2017-ci illər üzrə).....</i>	<i>173</i>
<i>Səadət Abdullayeva, İnternet-medianın monitorinqi və informasiya təhlükəsizliyi məsələləri.....</i>	<i>177</i>
<i>Suleyman Suleymanzade, Estimating the text preprocessing algorithms for sentence classification.....</i>	<i>181</i>
<i>Ələvsət Əliyev, İqtisadi inkişafın inklüzivlik səviyyəsinin yüksəldilməsində İKT və onların təhlükəsizliyi problemləri.....</i>	<i>185</i>
<i>Dilbər Əlizadə, Bulud əsaslı e-kitabxanalarda informasiya təhlükəsizliyinin təmini yolları.....</i>	<i>190</i>

<i>Afət Mikayılova</i> , Zaman sıralarında anomaliyaların aşkarlanması metodlarının analizi.....	193
<i>Məmməd Həşimov</i> , Əşyaların İnterneti texnologiyaları əsasında yaradılan şəbəkə mühitində hücumların təhlili.....	195
<i>Roza Şahverdiyeva</i> , Elmi-texnoloji innovasiya parklarının informasiya təhlükəsizliyi problemləri.....	199
<i>Gülnarə Qarayeva</i> , Botnet trafikinin aşkarlanmasının bir üsulu haqqında.....	204
<i>Təhmasib Fətəliyev, Nərgiz Verdiyeva</i> , Vətəndaş elminin informasiya təhlükəsizliyi haqqında.....	209
<i>Gülnar Paşayeva</i> , Yeni media təhsili və informasiya təhlükəsizliyi.....	213
<i>Məkrufə Hacırahimova, Aybəniz Əliyeva</i> , Big Data texnologiyalarının təhlükəsizlik problemləri və həlli yolları.....	216
<i>Rəhilə Həsənova, Firudin Əsgərov</i> , Plagiatlığın növləri və ondan qorunmağın üsulları.....	221
<i>Məkrufə Hacırahimova, Mərziyə İsmayılova</i> , NoSQL verilənlər bazalarında təhlükəsizlik problemləri haqqında.....	224
<i>Səbirə Ocaqverdiyeva</i> , Elektron dövlət mühitində uşaqların İnternet təhlükəsizliyinin qanunvericilik bazasının formalaşdırılması problemləri.....	228
<i>Xəyyam Nurəliyev</i> , Veb spamlar və onlarla mübarizə metodları.....	233
<i>Ələvsət Əliyev, Anar Səmidov, Roza Şahverdiyeva, Leyla Əkbərova</i> , İnformasiya iqtisadiyyatı şəraitində nəşriyyat-poliqrafiya sektorunun formalaşmasında müasir İKT və onların təhlükəsizliyi məsələləri.....	236
<i>Səbinə Məmməd zadə</i> , Transliterasiya – milli identikliyə böyük təhlükə mənbəyi kimi.....	241
<i>Məkrufə Hacırahimova, Adilə İmamverdiyeva</i> , Twitter məlumatlarının sentiment analizi.....	245

Elektron milli dövlət: Azərbaycan dilinin qorunması və inkişafı üçün imkan və perspektivlər

Rasim Əliquliyev¹, Yedgar Cəfərov², Fərhad Yusifov³, Əfruz Qurbanova⁴

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹director@iit.science.az, ²yedgar@yandex.ru, ³farhadyusifov@gmail.com, ⁴afruz1961@gmail.com

Xülasə - Məqalə elektron milli dövlətdə dilin yeri və roluna həsr edilib. Burada qloballaşmanın milli dillər üçün doğurduğu təhdidlər nəzərdən keçirilir. E-dövlət platformasının dillərin qorunması və inkişafı üçün yaratdığı imkanlara diqqət yönəldilir. Bu platformada dövlət dilinin statusunun təmin olunması üçün həllər irəli sürülür. Eyni zamanda milli azlıqların dillərinin sənədləşdirilməsi üçün təkliflər verilir. E-dövlət platformasında dillə bağlı konkret modullar müəyyən edilir.

Açar sözlər: e-dövlət, dövlət dili, milli dil korpusu, dillərin sənədləşdirilməsi, qloballaşma, mədəni müxtəliflik

I. GİRİŞ

Elektron dövlət (e-dövlət) ideyası təcrübədə özünü doğrultduğundan getdikcə daha çox ölkələrdə geniş tətbiq olunmaqdadır. İctimai həyatın ən müxtəlif sahələrinə get-gedə daha dərinlən nüfuz edən bu platforma özünün müxtəlif seqmentləri üzrə toplanan zəngin məlumat bazası və bu məlumatların təhlili imkanları ilə cəmiyyətin idarə olunması, ayrı-ayrı sosial, iqtisadi, siyasi, mədəni və s. meyllərin istiqamətləndirilməsinə, eləcə də kütlənin rəyindən asılı olan bir sıra sosial problemlərin həllinə böyük imkanlar açır. Bu imkanlardan irəli gələrək hazırda e-dövlətlə bağlı diqqəti cəkbən aktual elmi məsələlərdən biri də dövlət dillərinin bu platformadakı yeri və rolunun müəyyənəşdirilməsindən ibarətdir. Eyni zamanda, qloballaşma şəraitində müxtəlif təhlükələrlə üz-üzə qalmış milli dillərin qorunması və inkişafı üçün e-dövlət texnologiyalarının perspektivlərindən istifadə məqsədilə müvafiq həllərin tapılmasıdır.

II. MÜASİR DÖVRDƏ DÜNYA DİLLƏRİNİN VƏZİYYƏTİ

Məlum olduğu kimi, sürətlə qloballaşan müasir dünyamızda dil müxtəlifliyinin qorunması xüsusilə mühüm problemə çevrilmişdir [1,2]. Çünki, qloballaşma prosesləri milli informasiya məkanı ətrafındakı sərhədləri ortadan götürərək dünyaya fəal şəkildə inteqrasiya etmiş cəmiyyətlərə sayırsız-hesabsız üstünlüklər qazandırdığı kimi, müəyyən təhdidlər də doğurur. Qlobal təhdidlərin böyük bir hissəsi məhz milli dillərə aiddir. Hər bir dil mənsub olduğu xalqın digər milli-mənəvi dəyərləri kimi, daha çox, lokal informasiya məkanının hadisəsi sayıldığından, milli informasiya məkanı təcrid edilmiş vəziyyətdə olduqda bu dəyərlərin, o cümlədən

dilin qorunması kifayət qədər asan başa gəlir. Bu zaman cəmiyyət özü həmin məkan xaricindəki informasiya mühitindən nələri götürmək, nələrdən imtina etmək üçün optimal vasitələrə, geniş seçim imkanlarına, ən əsası isə çox böyük zamana malik olur. Amma qloballaşma mühitində bunların heç biri yoxdur. ABŞ, Böyük Britaniya kimi aparıcı ölkələrin güclü iqtisadiyyatına, böyük əməllərə malik qlobal media resurslarına, zəngin elmi-texnoloji məlumat bazasına söykənən ingilis dili çox sürətlə milli dillərin linqvomədəni fəzasına daxil olaraq onları sıxışdırır. Hazırda mövcud internet resurslarının və bu resurslarda mövcud olan informasiyaların təxminən 53%-i ingilis dilinin payına düşür. Qalan 47% isə əsasən, rus, alman, yapon, ispan, fransız, çin, portuqal və italyan dilləri kimi aparıcı dillər arasında bölünmüşdür [2].

Məlumat üçün bildirək ki, “hazırda dünyanın 260 ölkəsində 7,5 milyarddan çox insan yaşayır. Onlar ünsiyyət vasitəsi kimi 7 minə yaxın dildən istifadə edirlər. 40 ən çox yayılmış dil dünya əhalisinin 2/3-ni əhatə edir. Dünyadakı mövcud dillərdən yalnız 95-i dövlət dili statusuna malikdir. Bəzi dillər bir neçə dövlətin rəsmi dili kimi qəbul edilib. O cümlədən ingilis dili 56, fransız dili 29, ərəb dili 24, ispan dili 20, portuqal dili 8, alman dili 6, italyan və rus dilləri 4, holland və serb dilləri 3 ölkənin dövlət dili statusuna malikdir. Daha 12 dilin hər biri iki ölkədə rəsmi dil kimi işlədilir. Eyni zamanda, 2 və daha artıq dövlət dili olan ölkələr də mövcuddur. Cənubi Afrika Respublikası bu baxımdan daha çox fərqlənir. Belə ki, bu ölkədə 11 rəsmi dövlət dili paralel olaraq işlədilir” [3]. Müasir dünyada dillərin “iyerarxiya”sı şəkil 1-də verilmişdir.

İngilis dilinin dünyada belə üst mövqe tutmasının əsas generatoru bu dildə elmin, təhsilin, texnologiyaların sürətli inkişafı, başqa sözlə, sivilizasiyanın müasir inkişaf mərhələsində bu dilin elmi-texniki tərəqqinin (internet, fundamental biliklər üzrə əldə edilmiş nailiyyətlər və s.) lokomotivi rolunda çıxış etməsidir. Planetin dil mənzərəsini obyektiv qiymətləndirməyə çalışan UNESCO ekspertlərinin proqnozlarına görə, XXI əsrin sonuna qədər dünyadakı dillərin 50%-dən 90%-ə qədəri tamamilə məhv olub yoxa çıxma bilər [4].

İlk mərhələdə rəsmi statusu olmayan dillər (tayfa və xalq dilləri) xüsusilə böyük təhlükə qarşısındadır. Tədrisən isə bu proses dövlət dillərini də əhatə edəcəkdir. Ona görə də son illər UNESCO və ümumilikdə BMT yoxa çıxmaqda olan dillərin qorunması istiqamətində fəaliyyətini gücləndirmiş, bu

2001-ci ildə UNECSO dünyada yoxa çıxmaqda olan dillərin atlasını da hazırlamış, atlas sonuncu dəfə 2010-cu ildə

beynəlxalq standartlara uyğunlaşdırılması və çoxdilliliyin dəstəklənməsi; dil, din, milli mənsubiyyət, təhsil səviyyəsi, bacarıqlar, fiziki qabiliyyətlər, yaşayış yeri və s. amillərdən asılı olmayaraq elektron xidmətlərin hər kəs üçün əlçatanlığı.

Azərbaycan Respublikası Konstitusiyasının 21-ci maddəsinin I hissəsinə əsasən, Azərbaycan Respublikasının dövlət dili Azərbaycan dilidir. Bu dil dövlət dili kimi ölkənin siyasi, ictimai, iqtisadi, elmi və mədəni həyatının bütün sahələrində işlədilir [8]. Azərbaycan Respublikasında dövlət hakimiyyəti və yerli özünüidarəetmə orqanlarında, dövlət qurumlarında, siyasi partiyalarda, qeyri-hökumət təşkilatlarında (ictimai birlik və fondlarda), həmkarlar təşkilatlarında, digər hüquqi şəxslərdə, onların nümayəndəliklərində və filiallarında, idarələrdə dövlət dilinin tətbiqi ilə bağlı fəaliyyət “Azərbaycan Respublikasında dövlət dili haqqında” Qanuna uyğun olaraq həyata keçirilir, o cümlədən kargüzarlıq işləri dövlət dilində aparılır [9]. Konstitusiyamızın 21-ci maddəsinin II hissəsinə görə, Azərbaycan Respublikası əhalinin danışdığı başqa dillərin sərbəst işlədilməsini və inkişafını təmin edir [8].

E-dövlət mühiti isə elə bir həllin tapılmasına imkan verir ki, onunla həm dövlət dilinin Konstitusiyaya ilə təsbit edilmiş statusunu və təbii inkişafını, həm respublikadakı milli azlıqların öz dillərindən istifadə ilə bağlı hüquqlarını, həm də ölkə ərazisində müvəqqəti yaşayan əcnəbilərin e-xidmətlərdən maneəsiz istifadəsini təmin etmək mümkün olsun.

Bu sahədə əsas perspektiv layihə e-dövlət platformasında milli dillərin sistem arxitekturasının qurulmasıdır. Belə bir arxitektura hesabına milli dillərin e-dövlət platformasının üzvi tərkib hissəsinə çevrilməsi, bu texniki orqanizmdə özünə yer tutması qloballaşma dövründə dillərin qorunması və inkişafına böyük töhfə verəcəkdir.

ARXİTEKTURASI

Milli dillərin öz sistem arxitekturası ilə e-dövlətin üzvi tərkib hissəsinə çevrilməsi və bu platformanın bütün seqmentləri üzrə təbii inkişafının təmin olunmasından ötrü yeni metodlar, alqoritmlər, yanaşmalar işlənməli, bir sıra təbiiqlər hazırlanmalıdır. Bu məqsədə çatmaq üçün aşağıdakı məsələlərin həlli zəruri sayılır:

- e-dövlətin bütün vətəndaşlar və ölkədə müvəqqəti yaşayan əcnəbilər üçün əlçatanlığı məqsədilə

Səkil 1. Müasir dünya dillərinin “iyerarxiya”sı

UNESKO Baş Konfransının 2003-cü ildə keçirilmiş iclasında isə kiberməkanda ümumi giriş və çoxdillilikdən istifadənin genişləndirilməsi üzrə tövsiyələr təqdim edilmişdir. Bu tövsiyələr informasiyaya çıxış imkanlarının təmin olunmasında, dünya informasiya şəbəkəsində mədəni müxtəlifliyin və çoxdilliliyin qorunmasında UNESKO-nun rolunun artırılmasını nəzərdə tutur. İnsanlar arasında təkcə ünsiyyət vasitəsi və mədəniyyət vektoru deyil, eyni zamanda dünyagörüşü və dəyərlər süzgəci olan, özünüdərkən bir hissəsi və şəxsin milli identifikasiya vasitəsi kimi çıxış edən dilin qorunmasının vacibliyi irəli sürülür [5].

Avropa Birliyi ölkələrinin ağıllı, dayanıqlı və inklüziv inkişaf istiqamətlərini müəyyən edən “Avropa-2020” strategiyasında da bu ölkələrdə e-dövlət quruculuğu zamanı cəmiyyətin sosial-mədəni, dil müxtəlifliyinin nəzərə alınması və qorunmasına söz göstərilməsi əsas baza prinsiplərindən biri kimi öz əksini tapmışdır [7].

Göründüyü kimi, beynəlxalq normativ sənədlərin tövsiyələrinə və qabaqcıl ölkələrin e-dövlət quruculuğu təcrübəsinə əsaslanaraq elektron milli dövlətdə dilə münasibətdə iki təsəvvür formalaşdırmaq olar. Birinci təsəvvürə görə, e-dövlət xidmətlərinin yaradılmasında dil müxtəlifliyinin qorunması çox aktualdır. Dövlət idarəçiliyi sisteminin yenidən təşkili və e-dövlət quruculuğu prosesində digər zəruri şərtlərlə yanaşı, sırf dillə bağlı bu məqamlar mütləq nəzərə alınmalıdır: çoxdilliliyə əsaslanan kommunikasiya vasitələrindən geniş istifadə; xidmətlərin

lokallaşdırma (dövlət dilindən istifadə) və qloballaşdırma (əsas xarici dillərdən istifadə) problemlərinin həlli;

- ölkə ərazisində yaşayan milli azlıqların dillərinin sənədləşdirilməsi (language documentation) üçün e-dövlət platformasının imkanlarından istifadə;
- e-dövlət sistemində toplanmış böyük həcmdə verilənlərin təhlili ilə ölkədəki mövcud dil situasiyasının mütəmadi qiymətləndirilməsi;
- e-dövlət mühitində, kütləvi-informasiya vasitələrində, sosial mediada və s. dildən istifadənin intellektual analizi metodlarının işlənməsi və əks-əlaqə mexanizmlərinin tətbiqi;
- e-dövlət sistemində dilin sanitariyası, orfoqrafiya, orfoepiya, transliterasiya, terminologiya, dialektologiya məsələləri, adlar və soyadlar, vulqarizmlər, marka adları, dil sənayesi xidmətləri (maşın tərcüməsi, nitqin tanınması, süni intellekt, dilöyrənmə və dil biliyi səviyyəsini qiymətləndirmə və s.), Dilin Milli Korpusu və s. bu kimi modulların formalaşdırılması;
- milli domen adlarının tətbiqi və çoxdilli internetin dəstəklənməsi üçün texniki tədbirlərin həyata keçirilməsi;
- qloballaşma şəraitində milli dillərin qorunması və inkişafının təmin olunmasından ötrü təklif edilən metod və alqoritmlərin korporativ şəbəkələrdə tətbiqi.

Şəkil 2 e-dövlət mühitində Azərbaycan dilinin qorunması sisteminin konseptual modelini əks etdirir. Belə bir modelin tətbiqi e-dövlət bazasında dilin müxtəlif səviyyələri üzrə material bazasının toplanmasına, təhlilinə, qiymətləndirilməsinə və onlardan məqsədyönlü şəkildə istifadəyə şərait yaradacaqdır.

Şəkil 2. E-dövlət mühitində Azərbaycan dilinin qorunması sisteminin konseptual modeli

Bu modeli təşkil edən modullar haqqında qısa məlumat aşağıda verilmişdir:

Dillərin sənədləşdirilməsi modulu (language documentation): Dillərin sənədləşdirilməsi dilçiliyin yeni bir elmi istiqamətidir. O, sahəvi linqvistika ilə əlaqəli şəkildə az tədqiq edilmiş dilləri özünün təbii mühiti ilə birgə öyrənir. Dillərin sənədləşdirilməsinin əsas predmeti milli azlıqların dillərinə aid ilkin materialların yığılaraq vahid elektron mənbədə toplanmasıdır. Dilin sənədləşdirilməsi deyərək, dil materiallarının uzunmüddətli və çoxməqsədli fiksasiyası başa düşülür [10].

Dilin daşıyıcıları ilə sıx əlaqələr, onların bu işə cəlb olunması böyük səmərə verdiyindən yerli icmaları, milli mədəniyyət mərkəzlərini, bələdiyyələri, təhsil müəssisələrini və s. bu prosesə cəlb etməklə e-dövlət mühitində dillərin sənədləşdirilməsi üzrə çox uğurlu layihələr həyata keçirmək mümkündür.

Dilin sanitariyası modulu: Bu gün insanlar arasında ünsiyyət proseslərinin virtuallaşması dildə yeni meyllər yaradır. Bu meyllərin mühüm bir qisminin müasir həyatımızın ayrılmaz tərkib hissəsinə çevrilmiş sosial şəbəkə ünsiyyətində ortaya çıxdığını görürük. Bunun ən səciyyəvi xüsusiyyətləri şifahi nitqdə olduğu kimi sosial şəbəkə mühitində də dil normalarından kənarlaşma, fikrin yığcam ifadəsinə meyl, simvolların, şəkillərin söz, cümlə və mətnləri əvəz etməsi, bir sıra yeni sözlərin yaranması, mövcud sözlərin yeni məna çalarları qazanması və s. bu kimi tendensiyalardır [11].

E-dövlətdə isə dilin sanitariyası ilə bağlı xüsusi modul formalaşdırılmalıdır. Burada dilin distant tədrisi layihələri həyata keçirilməli, insanların yazı və nitq qabiliyyətinin inkişafına yönəlmiş videodərslər hazırlanaraq hər kəsin istifadəsinə verilməlidir. Virtual kommunikasiyalarda, eifirdə dil normalarının pozulması hallarının qarşısını almaqdan ötrü şəbəkələrə inteqrasiya edilmiş elektron redaktə, korrektə, mətnyaratma proqramlarının tətbiqi də bu modulun tərkib hissələri kimi nəzərdə tutulur. Dilin sanitariyasına aid modulun köməyi ilə elektron kütləvi informasiya vasitələrində - televiziyalarda, radioda dil normalarından kənarlaşma hallarının dəqiq monitorinqi və pozuntu hallarının aradan qaldırılması da mümkün olacaqdır.

Orfoqrafiya və Orfoepiya modulu: E-dövlət platformasının yaratdığı digər əhəmiyyətli imkanlardan biri də dilin orfoqrafik və orfoepik normalarının tənzimlənməsidir. Bu sahədəki mövcud problemlərin aradan qaldırılmasından ötrü e-dövlətdə dilin orfoqrafiyası və orfoepiyası ilə bağlı xüsusi bir modul formalaşdırıla bilər. Bu modul müvafiq standartlar əsasında müəyyən edilmiş orfoqrafiya və orfoepiya qaydalarına hamılıqla riayət olunmasına nəzarəti təmin edəcəkdir.

Vulqarizmlər modulu: İnformasiyalı cəmiyyətdə etik davranış normalarının qorunması, eyni zamanda informasiya təhlükəsizliyi baxımından kifayət qədər mühüm əhəmiyyət kəsb edən məsələlərdən biri də virtual məkanda vulqarizmlərdən istifadə, bu dil vahidlərinin doğurduğu problemlər və onların həlli yollarının tapılmasıdır. Söz süzəclərinin yaradılması və istifadəsi təcrübəsinə əsaslanaraq e-dövlət platformasında qlobal vulqarizm bazasının

yaradılması elektron mühitdə vulqarizmlərə qarşı uğurlu mübarizə üsulu ola bilər.

Adlar-Soyadlar modulu: Adlar, ata adları və soyadlar elektron idarəetmə mühitində mühüm funksiya yerinə yetirir. Ona görə də xüsusi adlarla bağlı bir sıra məsələlərin həlli, o cümlədən adların modelləşdirilməsi, vahid adlandırma standartının formalaşdırılması, ad komponentlərinin müəyyənəşdirilməsi, adlardakı təhrif tiplərinin aradan qaldırılması, adların elektron bazalarının yaradılması və onlardan istifadə mexanizmlərinin işlənilib hazırlanması, adların transliterasiyası normalarının dəqiqləşdirilməsi, adların orfoqrafiyası qaydalarının nizama salınması və s. e-dövlət sistemi üçün xüsusi əhəmiyyət kəsb edir [12]. Bütün bunlar isə sistemdə belə bir modulun yaradılması hesabına təmin oluna bilər.

Transliterasiya modulu: Hazırda dilimizin qəbul olunmuş vahid transliterasiya qaydaları mövcud olmadığından bəzi anlaşılmazlıqlar meydana çıxır. Azərbaycan dilində danışb ünsiyyət quran insanlar, xüsusilə, yeniyetmə və gənclər virtual ünsiyyət zamanı Azərbaycan sözlərini bir deyil, bir neçə variantda yazırlar. Bu cür problemlər latın hərflərindən istifadənin vahid sistemini qəbul etmiş Gürcüstan, Rusiya, İsrail, Çin və ya Yaponiya kimi ölkələrdə mövcud deyil. Nəzərə almaq lazımdır ki, latın qrafikasından istifadə heç də Azərbaycan əlifbasından imtinaya dəlalət etmir. E-dövlətdə vahid standartın tətbiqi latın əlifbasında yazı və oxumanı asanlaşdıracaq, beləliklə, e-xidmətlərdən istifadə insanlar üçün daha rahat və əlçatan olacaqdır [13]. E-dövlətdə əlifba və transliterasiya ilə bağlı problemlərin həlli üçün aşağıdakı tədbirlərin həyata keçirilməsi böyük səmərə verərdi:

- Azərbaycan dili qrafikasının latın qrafikasına transliterasiya standartının qəbulu və tətbiqi;
- Azərbaycan əlifbasını latın əlifbasına və əksinə avtomatik transliterasiya edən proqramların yaradılması;
- Qarşılıqlı transliterasiya səhvləri korrektorunun (spell check) tətbiq olunması.

Milli Terminoloji İnformasiya modulu: Elmi, texniki və iqtisadi fəaliyyətin yüksək səviyyədə təşkili dəqiq işlənmiş terminologiyadan əhəmiyyətli dərəcədə asılıdır. Ona görə də dil siyasətinin mühüm hissəsi kimi terminologiyanın elmi-nəzəri və praktiki problemlərinə xüsusi diqqət yetirilməsi vacibdir. Bu zərurəti nəzərə alaraq, AMEA-nın İnformasiya Texnologiyaları İnstitutu Milli Terminoloji İnformasiya Sisteminin (MTİS) konsepsiyası və veb-portalını hazırlamışdır [14, 15]. Bu sistemin köməyi ilə terminoloji problemlərin həllində, terminlərin ictimai müzakirəsi və ekspertizası işlərində marağı olan hər kəs iştirak edə bilər. Bu imkan ölkəmizdə vətəndaş terminologiyasının formalaşması üçün əhəmiyyətlidir. Sistem vətəndaşlara e-terminoloji xidmətlər göstərməklə yanaşı, ölkədə terminologiya fəaliyyətinin təkmilləşdirilməsinə töhfə verəcək. Amma sistemin səmərəli fəaliyyətinin təmin olunması üçün onun müntəzəm yenilənməsi, interaktivliyinin təmin olunması mühüm şərtidir.

Dialektologiya modulu: Dialektoloji atlasların yaradılması prosesində kompüter və şəbəkə texnologiyalarından istifadə müasir dilçiliyin kifayət qədər

perspektivli istiqamətlərindən sayılır. Hazırda bu metoddan dünya və o cümlədən rus dilçiliyində geniş istifadə olunmaqdadır. AMEA-nın Nəsimi adına Dilçilik İnstitutunda, eləcə də digər elm və tədris müəssisələrində dialektlərimizin öyrənilməsi ilə bağlı əhatəli tədqiqatlar aparılıb [16, 17]. Bu sahədə böyük bir məktəb formalaşmış. Dilçilik coğrafiyası, dialekt leksikası, etnolingvistikası, regional onomastika və s. sahələrində bir çox məsələlər öz elmi həllini tapıb və Azərbaycanın bir çox regionlarının dialektoloji atlasları hazırlanıb. Müasir dövrdə isə uzun onilliklər ərzində toplanmış dialekt materiallarının rəqəmli məlumat bazalarının yaradılmasına, bu məlumatların virtual xəritələr üzrə qruplaşdırılmasına, eyni zamanda burada mətn məlumatları ilə yanaşı, audiovizual materialların öz əksini tapmasına ehtiyac vardır.

Marka adları modulu: E-dövlətdə marka adları ilə bağlı problemləri aktuallaşdıran əsas məsələ isə onların sahibkarlıq fəaliyyətinin mühüm tərkib hissəsi kimi çıxış etməsi, hüquqi qeydiyyatı, əmtəə nişanları üzərində mülkiyyət hüquqlarının qanunvericiliklə qorunması, habelə onların son onillikdə effektiv bir fəaliyyət sahəsi kimi formalaşmış rəqəmsal marketinqdəki yeri və roludur. Bütün bunlar bir çox ölkələrdə olduğu kimi Azərbaycanda da e-dövlətin tərkibində marka adlarının elektron analizi xidmətinin yaradılması zərurətini aktuallaşdırır. Azərbaycanda belə bir sistemin yaradıcısı və tənzimləyicisi qismində müvafiq elmi qurumlarla müştərək şəkildə Azərbaycan Respublikasının Əqli Mülkiyyət Agentliyi çıxış edə bilər.

Dil xidmətləri (dil sənayesi) modulu: Dil sənayesinin əsasında bu sahədə İKT-nin uğurlu tətbiqi dayanır. Bu sferada tədris, tərcümə, lokallaşdırma və digər xidmətlərin göstərilməsi, eyni zamanda, qlobal informasiya cəmiyyətinin formalaşmasına və inkişafına xidmət edir. Azərbaycanda da dil sənayesinin inkişafı üçün böyük potensial mövcuddur. Ölkədə dil sənayesini stimullaşdıran əsas amillər xarici investisiyalar, turizm sektorunun sürətlə inkişafı, tərcümə biznesinin əhəmiyyətli bazar payı qazanmasıdır [18]. Azərbaycan televiziyalarında dublyaj redaksiyalarının fəaliyyəti, müvafiq dövlət qurumlarının, çoxsaylı biznes subyektlərinin vətəndaşlarla, müştərilərlə Qaynar xətt, Məlumat Mərkəzi formatında interaktiv kommunikasiyaları, xarici dillərin öyrənilməsinə maraqlı dil sənayesinin potensialını gücləndirir. Eyni zamanda Azərbaycan dilinin öyrənilməsinə böyük maraqlı nəzərə alaraq Azərbaycan Respublikasının Prezidenti 7 iyul 2018-ci il tarixində “Azərbaycan dilinin elektron məkanda daha geniş istifadəsinin təmin edilməsi ilə bağlı bir sıra tədbirlər haqqında” Sərəncam və 1 noyabr 2018-ci il tarixində “Azərbaycan dilinin saflığının qorunması və dövlət dilindən istifadənin daha da təkmilləşdirilməsi ilə bağlı tədbirlər haqqında” Fərman imzalamışdır [19, 20].

Ölkədə dil sənayesini məqsədyönlü şəkildə inkişaf etdirmək üçün kompleks elmi-praktik tədqiqatların həyata keçirilməsi, mövcud problemlərin, müvafiq hüquqi və iqtisadi situasiyanın dərindən öyrənilməsi, bu sahənin inkişafı üçün konseptual baxışların formalaşdırılması, hüquqi, iqtisadi, təşkilati, kadr hazırlığı və s. sahələri əhatə edən müvafiq

ekosistemin formalaşdırılması vacibdir. Bu məsələlərin e-dövlət platformasında nəzərə alınması, dillə bağlı e-xidmətlərin göstərilməsi ölkəmizdə dil sənayesinin inkişafına təkan verəcəkdir.

Milli Dil Korpusu modulu: Milli Dil Korpusları elmi araşdırmalar və dilin tədrisi prosesinin optimallaşdırılması məqsədilə yaradılır. Korpus dili bütün janr və üslub müxtəliflikləri, dialektləri və peşə leksikası ilə və ya onun mövcudluğunun bütün mərhələlərində təmsil edir. Hazırda dünyanın bir çox ölkələrində dünyanın aparıcı dilləri üçün milli korpus tərtib olunmuşdur. Dünyanın ən çox tanınmış və nümunə kimi qiymətləndirilən korpusu Britaniya Milli Korpusu hesab edilir [21]. Slavyan dilləri ailəsində isə rus və çex dillərinin milli korpusları xüsusilə seçilir. Bu mütərəqqi təcrübələrdən faydalanmaqla Azərbaycan dilinin Milli Korpusunun yaradılması və e-dövlətin tərkib hissəsinə çevrilməsi zəruridir. E-dövlət mühitində dilin müxtəlif səviyyələr üzrə texniki integrasiyası Milli Dil Korpusunun formalaşdırılması və zaman-zaman inkişafı üçün geniş imkanlar yaradır.

NƏTİCƏ

Ümumiyyətlə, İnternet mühitində dilin qorunması və inkişafı üsulları ilə bağlı müxtəlif ideyalar, yanaşmalar vardır. Qloballaşma prosesində dili təhlükə altında qoyan bir çox amillər mövcuddur və bu amillərin hər birinin ayrı-ayrılıqda nəzarətdə saxlanılması hesabına dili qorumaq çox çətindir. Yalnız dilin e-dövlət platformasının üzvi tərkib hissəsinə çevrilməsi, e-Azərbaycan seqmentində lingvistik texnologiyaların istifadəsi ilə müxtəlif e-xidmətlərin göstərilməsi və bu sistemlərin davamlı şəkildə təkmilləşdirilməsi hesabına ana dilimizi qorumaq və inkişaf etdirmək mümkündür.

ƏDƏBİYYAT

- [1] P.Mittal, A.Kaur, “E-Governance – A challenge for India”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 2, Issue 3, 2013, 1196-1199
- [2] World Wide Web Technology Surveys. https://w3techs.com/technologies/overview/content_language/all
- [3] R.M.Əliquliyev, R.Ş.Mahmudov, “Dil sənayesi: imkanlar, perspektivlər və problemlər”, // İnformasiya cəmiyyəti problemləri, 2018, № 1, səh. 3-26.
- [4] Language Vitality and Endangerment. UNESCO Ad Hoc Expert Group on Endangered Languages, International Expert Meeting on UNESCO Programme Safeguarding of Endangered Languages, Paris, 10–12 March 2003, 27 p. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CLT/pdf/Language_vitality_and_endangerment_EN.pdf
- [5] Деятельность ЮНЕСКО по защите исчезающих языков. <http://lingsib.ica.ras.ru/ru/articles/smeets.shtml>
- [6] Atlas of the World's Languages in Danger. UNESCO, 2011, 20 p. <http://unesdoc.unesco.org/images/0019/001924/192416e.pdf>
- [7] EUROPE 2020. A European strategy for smart, sustainable and inclusive growth. Brussels, 3.3.2010, 37 p.

<http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf>

- [8] Azərbaycan Respublikasının Konstitusiyası. <http://www.e-qanun.az/framework/897>
- [9] “Azərbaycan Respublikasında dövlət dili haqqında” Qanun. <http://mfa.gov.az/files/file/8.pdf>
- [10] J.Gippert, N.P.Himmelman, U.Mosel, “Essentials of Language Documentation”, 2006, Berlin, New York: Mouton de Gruyter, 437 p.
- [11] J.D.Jimma, “Language of social media. Examination of English as a Lingua Franca in social media”, University of Iceland, School of Humanities, Department of English, 2017, 32 p. <https://skemman.is/bitstream/1946/27228/1/Language%20of%20social%20media%20C%20J%20C%20B3hann%20Dan%20C%20Ade%20Ji%20mma.pdf>
- [12] “Adlar və Soyadlar” Dövlət İnformasiya Sisteminin yaradılması Konsepsiyası. Bakı, “İnformasiya Texnologiyaları” nəşriyyatı, Ekspres-Informasiya, 2010, 49 s.
- [13] S.V.Məmmədşad, “Verilənlərin emalında transliterasiya və transkripsiyaların rolu”, // İnformasiya cəmiyyəti problemləri, 2018, №1, s. 115–122.
- [14] R.M.Əliquliyev, A.M.Gurbanova, “The Conceptual Foundations of National Terminological Information System”, // International Journal of Education and Management Engineering (IJEME), 2018, Vol. 8, No. 4, pp.19-30.
- [15] www.terminologiya.az
- [16] <http://dialekt.vspu.ru/>
- [17] M. Mahmudov, “Kompüter dilçiliyi”. Bakı, “Elm və təhsil” nəşriyyatı, 2013, 356 s.
- [18] R.M.Əliquliyev, R.Ş.Mahmudov, “Dil sənayesi: imkanlar, perspektivlər və problemlər”, // İnformasiya cəmiyyəti problemləri, 2018, №1, s. 3-26
- [19] <http://e-qanun.az/framework/39503>
- [20] <https://president.az/articles/30563>
- [21] <http://www.natcorp.ox.ac.uk/>

ELECTRONIC NATIONAL GOVERNMENT: PROTECTION OF THE AZERBAIJANI LANGUAGE, OPPORTUNITIES AND PROSPECTS FOR ITS DEVELOPMENT

Rasim Əliquliyev¹, Yedgar Jafarov², Farhad Yusifov³, Afruz Gurbanova⁴

^{1,2,3,4}Institute of Information Technology of ANAS,
Baku, Azerbaijan

¹director@iit.science.az, ²yedgar@yandex.ru,
³farhadyusifov@gmail.com, ⁴afruz1961@gmail.com

Abstract – The article is devoted to the role and place of language in e-national government. It addresses the threats of globalization to the national languages. The article also touches upon the opportunities of e-government for the protection and development of languages. The article puts forward solutions to ensure the status of the state language on this platform. Moreover, it presents proposals for the documentation of the languages of national minorities. It identifies specific language-related modules for e-government platform.

Keywords – e-government, official language, national language, language documentation, globalization, cultural diversity

Bulud əsaslı elektron dövlət xidmətlərinin səmərəliliyinin artırılması metodu

Fərqanə Abdullayeva

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

a_farqana@mail.ru

Xülasə— Məqalədə bulud infrastrukturunda virtual maşınların (VM) iş yükünün proqnozlaşdırılması üsulu təklif edilmişdir. Proqnozlaşdırmanı həyata keçirmək üçün variasional avtoenkoderlərin rekonstruksiya ehtimalları istifadə edilmişdir. Rekonstruksiya ehtimalı dəyişənlərin paylanması dəyişkən olduğunu nəzərə alan ehtimal meyardır. İşdə variasional avtoenkoderin rekonstruksiya ehtimallarının qiymətləri VM-nin yüklənmə dərəcələrini göstərir. Eksperimentlərin nəticəsi göstərmişdir ki, variasional avtoenkoderlər sadə dərin neyron şəbəkələri ilə müqayisədə VM-ların iş yükünün proqnozlaşdırılmasında daha yaxşı nəticələr vermişdir. Variasional avtoenkoderlərin generativ xarakteristikaları verilənləri rekonstruksiya edərək yüklənmənin növlərini (səviyyələrini) müəyyən etməyə imkan verir.

Açar sözlər— Bulud əsaslı elektron dövlət; iş yükünün proqnozlaşdırılması; virtual maşın; dərin neyron şəbəkələri; dərin təlim; variasional avtoenkoder.

I. GİRİŞ

Son illər elektron dövlət (e-dövlət) bir çox ölkələrə geniş istifadə olunur. E-dövlət vətəndaşlar və dövlət üçün olduqca faydalıdır. Lakin e-dövlətin effektiv xidmət göstərməsinə neqativ təsir edən amillər vardır [1]. E-dövlətin problemlərini aradan qaldırmaq məqsədi ilə və dövlət xidmətlərinin göstərilməsini yaxşılaşdırmaq üçün hazırda dünya ölkələrində bulud texnologiyaları geniş tətbiq olunur. Bulud texnologiyalarının tətbiqi e-dövlətin müxtəlif aspektlərinin yaxşılaşdırılmasına ciddi təsir edə bilər.

Bulud əsaslı e-dövlətin effektivliyi elektron dövlət istifadəçilərinin dəyişkən tələblərinə cavab verən virtual resursların effektiv idarə edilməsindən asılıdır.

Bulud infrastrukturunda resursların planlaşdırılmasını həyata keçirməzdən əvvəl VM-ların tutumunun qiymətləndirilməsi aparılmalıdır [2]. VM-nin resurs utilizasiyası səviyyəsinin qiymətləndirilməsi və müəyyən edilməsi daxil olan tələbat üçün resursların (məsələn, CPU, yaddaş) ayrılmasında bazis hesab olunur [3].

VM-ların iş yükünün proqnozlaşdırılması sahəsində olduqca çox sayda yanaşmalar təklif olunmuşdur. Bu yanaşmaların əksəriyyətində VM-ların iş yükünü və ya onların

bulud infrastrukturunda CPU sərfiyyatını proqnozlaşdırmaq üçün neyron şəbəkələr [4, 5, 6], obrazların tanınması [7], xətti regressiya [8] kimi proqnozlaşdırma üsulları təklif edilmişdir. Bu metodlar VM-ların gələcək iş yükünü əvvəlki t zaman intervalındakı keçmiş iş yükü verilənlərinə əsasən proqnozlaşdırırlar [9]. Bu işlərdə resursların proqnozlaşdırılması SaaS və PaaS səviyyələrində aparılır. Bu səviyyələrdə bulud provayderləri infrastrukturlarında bu tip proqramların olmasından xəbərdar olurlar və onların davranışlarını asanlıqla izləyə bilirlər. Lakin IaaS səviyyəsində VM-da hansı proqramın icra olunacağı haqqında, ayrı-ayrı VM-larda yerinə yetiriləcək proqramlar (tətbiqlər) haqqında heç bir məlumat olmur. Belə olduqda isə VM-ların iş yükünün və CPU sərfiyyatının qiymətləndirilməsində proqramların davranışından istifadə etmək mümkün olmur. Bu mühitdə VM-ların iş yükünə istifadəçilərin davranışları və istifadəçilərin ani qəbul etdiyi qərarları təsir edir. Bu səbəbdən iş yükündə fluktuasiya əvvəlki iş yükündən və əvvəlki CPU sərfiyyatından asılı olmur və istifadəçilərin resursa olan dinamik, gözlənilməz, fluktuativ tələbatlarından asılı olaraq dramatik şəkildə dəyişə bilər.

Bu faktorları nəzərə alaraq təqdim olunan məqalədə Variasional Avtoenkoderlərə əsaslanan iş yükünün proqnozlaşdırılması üsulu təklif edilmişdir.

Variasional Avtoenkoderlər ehtimal proqnozlaşdırma üsuludur, variasional çıxarışla dərin təlimin birləşməsindən yaranmışdır. Variasional avtoenkoderlərinin üstünlüyü ondan ibarətdir ki, bu model ehtimal qiymətləndirmələr aparır. Bu ehtimal qiymətləri rekonstruksiya ehtimalları adlandırılır. Ehtimalların istifadəsi modeldə hər hansı bir spesifik sərhəd qiymətindən istifadə olunması problemini aradan qaldırır. Təqdim olunan məqalədə Variasional Avtoenkoderlər bulud mühitində virtual resursların həddindən artıq yüklənmə (overloading) ehtimalını qiymətləndirir.

Təklif olunan iş yükünün proqnozlaşdırılması üsulunun əsasında həddindən artıq yüklənmiş (zəif işləyən) VM-lar müəyyən olunur, bu maşınların ekstra iş yükünü yerinə yetirə bilən uyğun VM-lar çoxluğu proqnozlaşdırılır və tapşırıqları yerinə yetirmək üçün proqnozlaşdırılan bu VM-lar çoxluğu içindən tapşırıqları yerinə yetirəcək yeni VM-lər seçilir.

II. MƏSƏLƏNİN QOYULUŞU

Fərz edək ki, n sayda $D = \{(x_i, y_i)\}_{i=1}^n$ təlim verilənləri verilmişdir. Burada x_i D ölçülü vektor, $x_i \in R^D$, $y_i \in [1, K]$ isə uyğun siniflərin adlarıdır. Generativ modellərdən istifadə etməklə təlim verilənlərinə yaxın verilənlərin generasiyası tələb olunur.

A. Metodologiya

Variasional avtoenkoder variasional çıxarışı olan dərin generativ təlim modelidir. Variasional avtoenkoder sistemin davranışını öyrənmək və generasiya etmək üçün emal olunmamış verilənlərdən istifadə edir. Bu bölmədə fundamental anlayışlar haqqında məlumat verilir və VM-ların iş yükünün proqnozlaşdırılması metodologiyasının əsas ideologiyası şərh edilir.

B. Dərin təlim (Deep Learning)

Dərin təlim xam sistem verilənlərinin mürəkkəb konstruksiyalarını aşkarlamaq və öyrənmək üçün bir neçə sadə, qeyri-xətti emal laylarından ibarət olur.

Dərin təlim konsepsiyasının onilliklərdir mövcud olmasına baxmayaraq, o 2011-ci ildə ImageNet müsabiqəsinə təqdim olunmuş konvolyusional neyron şəbəkələrə həsr olunmuş layihənin möcüzəvi imkanlarından sonra, son bir neçə ildə məşhurlaşmışdır [10]. Həmin dövrlərdən başlayaraq dərin təlim “computer vision”, “genomics” kimi bir çox sahələrdəki nəaliyyətlərə təkan vermişdir. Dərin təlim həmçinin bulud infrastrukturunda anomaliyaların aşkarlanması [11], DDoS hücumların aşkarlanması [12] məsələlərində geniş tətbiq olunmuşdur. Dərin təlim verilənlərin qeyri-bircinsliyini və kütləvililiyini, sistemlərin mürəkkəbliyini nəzərə alaraq VM-ların yüklənmə dərəcələrinin proqnozlaşdırılması məsələsində də perspektiv imkanlara malikdir.

C. Generativ modellər (Generative Models)

Generativ modellər dərin təlimin müəllimsiz təlim üsullarının bir bölməsidir, hadisələri verilənlərdən böyük ölçüdə cari nümunələri analiz edərək, verilənlərə yaxın yeni nümunələr generasiya etməklə öyrənir [13]. Generativ Adversarial şəbəkələr (Generative Adversarial Networks) [14], Dərin Avtoregressiv şəbəkələr (Deep Autoregressive Networks) [15] və Variasional Avtoenkoderlər (Variational Autoencoders) [16] ən məşhur generativ modelərdir. Məqalədə Variasional Avtoenkoderlərin bulud əsaslı elektron dövlət infrastrukturunda VM-ların keyfiyyət göstəricilərini xarakterizə edən verilənlərdən istifadə etməklə VM-ların yüklənmə dərəcələrinin proqnozlaşdırılması məsələsinə tətbiqinə baxılmışdır.

D. Variasional Avtoenkoder (Variational Autoencoder)

Variasional Avtoenkoder klassifikasiya prosesini verilənlərin ehtimalının variasional aşağı sərhəddini optimallaşdırmaqla həyata keçirir. Variasional Avtoenkoder variasional çıxarışla dərin təlimin hibridləşdirilməsi əsasında yaradılmışdır və posterior paylanmaların və böyük verilənlər bazalarının olduğu halda effektiv təlim həyata keçirə bilər. Variasional çıxarış ehtimal sıxlıqlarını optimallaşdırma yolu ilə aproksimasiya edir [17].

Variasional Avtoenkoder iki blokdan ibarətdir: enkoder və dekoder. Enkoder verilənlərin latent təsvirini yaradır, dekoder isə bu təsviri geriye, orijinal verilənlərə konvertasiya edir.

Fərz edək ki, VM-ların yüklənmə dərəcəsini göstərən verilənlər x , kodlaşdırılmış verilənlər isə z olsun. ϕ parametrlərinə malik enkoder şəbəkəsi verilmiş x giriş verilənlərini $q_\phi(z|x)$ şəklində verilmiş paylanmanın vasitəsi ilə z şəklində kodlaşdırır, θ parametrlərinə malik dekoder şəbəkəsi isə z verilənlərini $p_\theta(x|z)$ şəklində verilmiş paylanmanın vasitəsi ilə x verilənləri şəklində dekodlaşdırır. Bu proses şəkil 1-də təsvir edilmişdir.

Şəkil 1. Təlim verilənlərinə yaxın verilənlərin generasiyası prosesi

Fərz edək ki, verilənlərin loqarifmik ehtimalı aşağıdakı kimidir:

$$\log p(x) = \log p(x^{(1)}, \dots, x^{(n)}) = \sum_{i=1}^n \log p(x^{(i)}) \quad (1)$$

Onda

$$\log p_\theta(x) = D_{KL} \left(q_\phi(z|x^{(i)}) \parallel p_\theta(z|x^{(i)}) \right) + E_{q_\phi(z|x^{(i)})} \left[-\log q_\phi(z|x^{(i)}) + \log p_\theta(x, z) \right] \quad (2)$$

burada D_{KL} Kulbak-Leibler divergensiya funksiyasıdır (Kullback–Leibler divergence, KL Divergence). (2) ifadəsinin qiyməti hər zaman müsbət olduğundan aşağıdakı şərt ödənilir:

$$\log p_\theta(x) \geq E_{q_\phi(z|x^{(i)})} \left[-\log q_\phi(z|x^{(i)}) + \log p_\theta(x, z) \right] = L(\theta, \phi; x^{(i)}) \quad (3)$$

burada $L(\theta, \phi; x^{(i)})$ variasional aşağı sərhəddir və aşağıdakı kimi yazıla bilər:

$$L(\theta, \phi; x^{(i)}) = -D_{KL} \left(q_\phi(z|x^{(i)}) \parallel p_\theta(z) \right) + E_{q_\phi(z|x^{(i)})} \left[-\log p_\theta(x^{(i)}|z) \right] \quad (4)$$

Bulud texnologiyaları infrastrukturunun mürəkkəbliyini nəzərə alaraq $q_\phi(z|x)$ və $p_\theta(x|z)$ parametrlərini

modelləşdirmək üçün dərin neyron şəbəkəsi istifadə edilmişdir. Enkoder və dekoderin öyrədilməsində Adam optimizasiya funksiyası istifadə edilmişdir. Optimallaşdırmanın məqsədi variasional aşağı sərhəddi maksimallaşdırmaqdan ibarətdir. Adam staxostik optimallaşdırma məsələləri üçün yaradılmış staxostik qradiyent eniş optimallaşdırılması üsuludur.

III. EKSPERİMENTLƏR

A. Variasional Avtoenkoder modelinin konfigurasiyası

Məqalədə dərin Variasional Avtoenkoder modeli *Theano* kitabxanasından istifadə etməklə qurulub və şəkil 2-də təsvir edilmişdir. Variasional Avtoenkoder modelinin arxitekturasının bir hissəsini enkoder, bir hissəsini isə dekoder təşkil edir. Şəbəkənin enkoder hissəsini 6 lay təşkil edir. Dekoder enkoderin əməliyyatına əks əməliyyatı yerinə yetirir və 6 laydan ibarətdir.

Şəkil 2. Dərin variasional avtoenkoder modeli

B. Verilənlər bazasının təsviri

İşdə 13 bulud qovşağından toplanmış 28147 nümunədən və 9 əlamətdən ibarət iş yükü verilənlər bazası istifadə edilmişdir [18]. 1 dəqiqədə tapşırıqların sayı, 5 dəqiqədə tapşırıqların sayı, 15 dəqiqədə tapşırıqların sayı, yaddaşın tutumu, diskin tutumu, CPU nüvələrinin sayı, hər bir nüvədə CPU-nun sürəti, şəbəkənin buraxma qabiliyyətinə görə ortalama qəbul edilən trafik kilobit həcmi (Kbps), şəbəkənin buraxma qabiliyyətinə görə ortalama ötürülən trafik kilobit həcmi (Kbps) istifadə

olunan verilənlər bazasının beş kateqoriyadan ibarət sinif nişanları təşkil edir. Bu kateqoriyalar çox az (very low, VL), az (low, L), orta (medium, M), yüksək (high, H), çox yüksək (very high, VH) kimi təsnif olunur.

Bulud resurslarında yükün proqnozlaşdırılması üsulunun test prosesi Azərbaycan Milli Elmlər Akademiyası, İnformasiya Texnologiyaları İnstitutunun verilənlər mərkəzində, Ubuntu 16.04.3 LTS amd64 system, 3312 GB memory, 2933.437 CPU MHz mühitində yerinə yetirilmişdir. Eksperimentlərin aparılması üçün Python proqram paketi və Tensorflow kitabxanası istifadə edilmişdir.

İş yükünün proqnozlaşdırılması variasional avtoenkoder, və dərin neyron şəbəkəsi əsasında aparılmışdır. Burada ilk öncə neyron şəbəkənin nişanlanmış verilənlər (labeled training data) əsasında 9 iş yükü atributları üzrə öyrədilməsi aparılır, daha sonra nişanlanmamış verilənlər (unlabeled testing data) əsasında iş yükünün proqnozlaşdırılması aparılır.

Variasional avtoenkoderdə verilənlər bazasının siniflərinə uyğun 5 gizli lay istifadə edilmişdir.

Modelin effektivliyinin qiymətləndirilməsi üçün precision, recall, F1-score, accuracy metrikaları istifadə edilmişdir. Bulud əsaslı elektron dövlət infrastrukturunda VM-ların iş yükünün proqnozlaşdırılması məsələsində Variasional Avtoenkoderin dəqiqliyi cədvəl 1-də verilmişdir. Cədvəl 1-dən göründüyü kimi model 0, 1 və 4-cü siniflərin aşkarlanmasında yaxşı nəticələr vermişdir. Lakin 2 və 3-cü siniflərin aşkarlanmasında aşağı effektivlik nümayiş etdirmişdir. Bu onunla əlaqədar ki, model 2 və 3-cü siniflərdən olan verilənlərin strukturunu rekonstruksiya etməkdə çətinliklə qarşılaşmışdır.

Cədvəl 1. Variasional Avtoenkoder

Sinif	Precision	Recall	F1-score	Accuracy
VL (0)	0.43	0.64	0.51	0.64
L (1)	0.57	0.53	0.55	0.53
M (2)	0.37	0.30	0.33	0.3
H (3)	0.00	0.00	0.00	0.0
VH (4)	0.40	0.71	0.51	0.71

Bu mənzərəni Variasional Avtoenkoderin xətlər matrisindən də (Şəkil 3) aşkar şəkildə görmək mümkündür.

Şəkil 3. Variasional Avtoenkoderin xətlər matrisi

Variasional Avtoenkoderin iş yükünün proqnozlaşdırılması üzrə verilənlər bazasına tətbiqi zamanı itki funksiyasının dinamikasında azalma, dəqiqlik funksiyasının dinamikasında isə artım müşahidə edilmişdir (Şəkil 4, Şəkil 5).

Şəkil 4. Variasional Avtoenkoderin dəqiqlik funksiyasının artım dinamikası

Şəkil 5. Variasional Avtoenkoderin itki funksiyasının azalma dinamikası

İş yükünün proqnozlaşdırılması üzrə verilənlər bazasına sadə dərin neyron şəbəkələrini tətbiq etdikdə isə (Cədvəl 2) model 4-cü sinifdən olan nümunələri yaxşı klassifikasiya edə bilmişdir, lakin qalan dörd sinifdən olan nümunələri aşağı effektivliklə tanıya bilmişdir.

Cədvəl 2. Sadə dərin neyron şəbəkəsi

Sinif	Precision	Recall	F1-score	Accuracy
VL (0)	0.07	0.01	0.02	0.01
L (1)	0.01	0.26	0.01	0.26
M (2)	0.15	0.01	0.02	0.01
H (3)	0.29	0.07	0.11	0.07
VH (4)	0.55	0.89	0.68	0.89

Bu mənzərəni sadə dərin neyron şəbəkəsinin xətlər matrisindən də (Şəkil 6) aşkar şəkildə görmək mümkündür.

Şəkil 6. Sadə dərin neyron şəbəkəsinin xətlər matrisi

Sadə dərin neyron şəbəkəsinin iş yükünün proqnozlaşdırılması üzrə verilənlər bazasına tətbiqi zamanı itki funksiyasının dinamikasında azalma, dəqiqlik funksiyasının dinamikasında isə qismən artım müşahidə edilmişdir (Şəkil 7, Şəkil 8).

Şəkil 7. Sadə dərin neyron şəbəkəsinin itki funksiyasının azalma dinamikası

Şəkil 8. Sadə dərin neyron şəbəkəsi dəqiqlik funksiyasının artım dinamikası

NƏTİCƏ

Məqalədə variasional avtoenkoderlərin generasiya etdiyi rekonstruksiya ehtimalları əsasında VM-ların iş yükünün proqnozlaşdırılması üsulu təklif edilmişdir. VM-ların yüklənmə dərəcələrinin xassələri və ehtimal qiymətləri təyin edilərək yüklənmə sinfini müəyyən etmək üçün Variasional Avtoenkoder alqoritminin rekonstruksiya ehtimalları istifadə edilmişdir. Təklif edilmiş üsul VM-ların yüklənmə dərəcəsini xarakterizə edən verilənlər bazasında test edilmişdir. Nəticələr göstərmişdir ki, Variasional Avtoenkoder alqoritmı VM-ların iş yükünün proqnozlaşdırılmasını sadə dərin neyron şəbəkələrinə nisbətən daha yaxşı həyata keçirir.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun maliyyə yardımı ilə yerinə yetirilmişdir – Qrant № EIF-BGM-4-RFTF-1/2017-21/08/1

ƏDƏBİYYAT

- [1] K.E. Ali, S.A. Mazen, E.E. Hassanein, “A proposed hybrid model for adopting cloud computing in e-government,” *Future Computing and Informatics Journal*, 2018, In Press.
- [2] R.M. Alguliyev, Y.N. Imamverdiyev, F.J. Abdullayeva, “PSO based load balancing method in cloud computing,” *Automatic Control and Computer Sciences*, No.1, 2019, in press.
- [3] X. Meng, C. Isci, J. Kephart, L. Zhang, E. Bouillet, D. Pendarakis, “Efficient resource provisioning in compute clouds via VM multiplexing,” *Proceeding of the 7th International Conference on Autonomic Computing*, ACM, 2010, pp. 11-20.
- [4] J. Kumar, A.K. Singh, Workload prediction in cloud using artificial neural network and adaptive differential evolution, “*Future Generation Computer Systems*,” 2018, vol. 81, pp. 41-52.
- [5] Y. Cheng, W. Chen, Z. Wang, Z. Tang, Y. Xiang, Smart VM co-scheduling with the precise prediction of performance characteristics, “*Future Generation Computer Systems*,” 2016, In Press.
- [6] T. Mahdhi, H. Mezni, A prediction-Based VM consolidation approach in IaaS Cloud Data Centers, “*Journal of Systems and Software*,” vol., 146, 2018, pp. 263-285.
- [7] R. Hu, J. Jiang, G. Liu, L. Wang, Efficient Resources Provisioning Based on Load Forecasting in Cloud, “*The Scientific World Journal*,” Vol. 2014, 2014, pp. 1-12.
- [8] A. Abdelsamea, A.A. El-Moursy, E.E. Hemayed, H. Eldeeb, Virtual machine consolidation enhancement using hybrid regression algorithms, “*Egyptian Informatics Journal*,” Vol 18, no 3, 2017, pp. 161-170.

- [9] D. Yang, J. Cao, J. Fu, J. Wang, J. Guo, “A pattern fusion model for multi-step-ahead CPU load prediction,” *Journal of Systems and Software*, vol. 86, no. 5, 2013, pp. 1257-1266.
- [10] A. Krizhevsky, I. Sutskever, and G.E. Hinton, “ImageNet classification with deep convolutional neural networks,” 25th International Conference on Neural Information Processing Systems (NIPS 2012), Granada, Spain, Vol. 1, 2012, pp. 1097-1105.
- [11] M. Abdelsalam, R. Krishnan, Y. Huang, and R. Sandhu, “Malware detection in cloud infrastructures using Convolutional Neural Networks,” *IEEE 11th international conference on Cloud Computing (CLOUD)*, 2018, pp. 162-169.
- [12] Y. Imamverdiyev, F. Abdullayeva, “Deep Learning Method for Denial of Service Attack Detection Based on Restricted Boltzmann Machine,” *Big Data*, vol. 6, no. 2, 2018, pp. 159-169.
- [13] G.E. Hinton, and Z. Ghahramani, “Generative models for discovering sparse distributed representations,” *Philosophical transactions of the royal society of London, Series B: Biological sciences*, vol. 352, no. 1358, 1997, pp. 1177-1190.
- [14] I.J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, “Generative adversarial networks,” In *Proceedings of the 27th International Conference on Neural Information Processing Systems*, 2014, pp. 2672-2680.
- [15] K. Gregor, I. Danihelka, A. Mnih, C. Blundell, and D. Wierstra, “Deep AutoRegressive Networks” In *International Conference on Machine Learning*, 2014, pp. 1242-1250.
- [16] D. Kingma, and M. Welling, “Auto-encoding variational Bayes,” 2nd International Conference on Learning Representations (ICLR 2014), Banff, Canada, 2014, pp. 1-14.
- [17] D.M. Blei, A. Kucukelbir, J.D. McAuliffe, Variational inference: A review for statisticians, *Journal of the American Statistical Association*, vol. 112, no. 518, 2017, pp. 859-877.
- [18] A.M. Al-Faifi, B. Song, M.M. Hassan, A. Alamri, A. Gumaiei, “Performance prediction model for cloud service selection from smart data, *Future Generation Computer Systems*,” 2018, vol. 85, pp. 97-106.

EFFICIENCY IMPROVEMENT METHOD OF THE CLOUD-BASED E- GOVERNMENT SERVICES

Fargana Abdullayeva

Institute of Information Technology of ANAS, Baku,
Azerbaijan
a_farqana@mail.ru

Abstract- In this paper, the virtual machine (VM) workload prediction method in the cloud infrastructure is proposed. To make predictions the reconstruction probabilities of the Variational Autoencoders are used. The reconstruction probability is the probability measure that considers the variabilities of the variable distributions. In this paper, the reconstruction probability values of the variational autoencoders show the load degrees of the VMs. The results of the experiments are shown that variational autoencoder is produced better results in predicting VM workloads than simple deep neuronal networks. The generative characteristics of the variational autoencoders, by reconstructing the data allow identifying the types (levels) of the load.

Keywords- Cloud-based electronic government; workload prediction; a virtual machine; deep neural networks; deep learning; variational autoencoder.

Analysis of information encryption methods in multichannel telecommunication systems

Bayram Ibrahimov¹, Ramiz Humbatov², Rufat Ibrahimov³

¹Azerbaijan Technical University, Baku, Azerbaijan

^{2,3}Institute of Control Systems NASA, Baku, Azerbaijan

¹*i.bayram@mail.ru*

Abstract — An analytical review of works devoted to the issues of transmission and cryptographic information in multi-channel telecommunication systems is presented. The methods of improving the cryptographic protection of messages from unauthorized access to communication channels during the transmission of information of a mixed type of traffic are analyzed. A new approach to the protection of information from unauthorized access in multichannel telecommunication systems, taking into account the peculiarities of the cryptographic method of encrypting and encoding transmitted messages via communication channels, is proposed.

Keywords — *information security, cryptography, encryption, unauthorized access, cryptographic protection*

I. INTRODUCTION

Intensive development of multichannel telecommunication systems (MTS) using the architectural concept of NGN/IMS (Next Generation Network & Internet Protocol Multimedia Subsystem) requires a new approach to effectively protect information, which is based on modern cryptography methods [1].

Effective information protection in the era of the information space for achieving the goals of the digital economy is one of the main prerequisites for the development of modern information and telecommunication technologies. Therefore, the issues of information security in telecommunication systems are becoming increasingly relevant with the development of information and network technologies [2].

It is known [3, 4] that for many years in all countries of the world information protection was the prerogative of the state, and a state monopoly was established on the development and use information protection technologies. Information security tools and algorithms were mainly used in military, government and diplomatic communication under tight government control. In these conditions, the development of the science of information security - cryptography.

Based on the system-technical analysis, it was established in [2, 5, 6] that cryptology dialectically unites two sciences:

1. Cryptography - a new science that studies methods protecting information from unauthorized access;
2. Cryptanalysis is the science methods of unauthorized access to protected information.

Consequently, the development banking technologies, the activities of commercial structures, election campaigns of competing political parties, inventive and other activities that require the protection of information. The latter determined the current demand for cryptographic technologies and cryptology specialists in the country [6].

In view of the above, an important question arises - the study of the description of the most frequently used algorithms, methods and protocols for cryptographic protection of information and the features of their use in telecommunications engineering.

In this paper, the solution of the above formulated problem is considered - the creation of a new approach to information security, which allows analyzing the methods transmitting and encrypting information in multichannel telecommunication systems.

II. GENERAL FORMULATION OF THE PROBLEM

The problem of the quality of transmission and protection of information in the telecommunications system is investigated with a certain model of message transfer and with a certain scenario of the attacker's actions.

In order to analyze and review the protection of information, a new approach is proposed that takes into account the algorithms of coherent network coding, when certain linear operations are performed on incoming messages and the attacker's script on the network nodes

In the attacker's scenario, there are subsets MTS communication available to the attacker, that is, he can eavesdrop on or record the information transmitted through them with the intention of identifying source messages.

This problem was first considered in [6, 7] by the team of authors in the first fundamental work on network coding.

In MTS, when transmitting information in open communication channels (CC), cryptographic methods for protecting information from unauthorized access to subscriber lines are widely used, as is the encryption method and the encryption method.

To achieve this goal, a new approach to cryptographic protection information from unauthorized access to MTS is proposed, taking into account the peculiarities of the cryptographic method of encrypting and encoding transmitted messages via communication channels.

III. ANALYSIS OF THE NEW APPROACH TO PROTECTING INFORMATION FROM UNAUTHORIZED ACCESS

In order to analyze the methods of transferring and encrypting information, consider the description of the most frequently used algorithm and protocols, sufficient for the implementation of existing cryptosystems.

To create a new approach, figure 1 presents a structural diagram that describes functionally the process of cryptographic protection of information from unauthorized access to the MTS.

Fig.1. Structural and functional scheme of protecting information from unauthorized access

From figure 1 it follows that the system for protecting information from unauthorized access consists of two important system functional blocks — the system for transmitting and encrypting the original messages and the reverse. In a generalized form, the task of protecting information from unauthorized access based on Fig. 1 can be formulated as follows.

Subscriber-A, being the source and initiator of message X , intends to transmit this message to subscriber-B, called the recipient of the message, while subscriber-A wants to be sure that in the process of transmitting the message no one can read it, that is, reveal the content, modify, or create another similar message and transmit it to the subscriber-B on behalf of the subscriber-A.

In turn, the subscriber-B, having received the message, wants to be sure that it is possible to establish and prove its receipt from subscriber A at any time, as well as the fact that this message is not a repeat of the earlier one.

In this case, the transmitted message is information of a mixed type of traffic (information file, speech, documentary message, etc.). In a schema, X a message is usually called a source or open message or text.

The message X may be, for example, a digitized speech of a telephone conversation, a text or other information file, a facsimile message, and other types information subject to protection from unauthorized access.

To protect the message X from unauthorized access, some transformation of the original message, called the encryption process, is applied.

This transformation involves the comparison of the original message X of a certain function $E(X)$ that turns it into an unreadable without special means encrypted message Y :

$$Y = E(X), \quad X \in (x_1, x_2, \dots, x_i), \quad (1)$$

However, the encrypted message Y is usually related to the original X structure, i.e. message length Y is usually equal to or greater than the length of the message X :

$$L_{oc}(Y) \geq L_{oc}(X) \quad (2)$$

It should be noted that in some cases the encryption process uses information compression in message X , in order to reduce message Y redundancy, while the message X may be shorter than the message, but this is not a consequence of encryption as such.

From fig.1, expressions (1) and (2), it follows that the studied approach of cryptographic protection of information takes into account also two types of unauthorized access:

- 1) to the communication channel;
- 2) to the information transmitted over the communication channel.

At the output of the communication channel, to recover the original message X from the encrypted message Y , a decryption operation is used using the $D(Y)$ function:

$$X = D[E(X)] \Rightarrow D(Y) = X \quad (3)$$

Expression (3) characterizes a set of algorithms for encryption and decryption processes, which is the algorithm for encrypting information as a whole.

IV. RESEARCH AND CALCULATION PARAMETERS CRYPTOGRAPHIC METHODS FOR PROTECTING INFORMATION IN THE MTS

It is known [4, 6, 8] that the main modern cryptographic methods for protecting messages are encryption methods (replacement, rearrangement, analytical transformation, gamming and combined) and encoding methods (meaning and symbolic). Here, the encryption method refers to the process in which each plaintext character is subjected to cryptographic transformation. In this method, the cipher always distinguishes between two elements: an algorithm and a key.

In the scheme of figure 1, it follows that the algorithm that implements the encryption function $E(X)$ is called the encryption algorithm. Accordingly, the decryption algorithm is the algorithm that implements the functions $D(Y)$. The combination of encryption and decryption algorithms will be

called the cryptographic algorithm of the telecommunications system.

The persistence of these algorithms is based on the computational complexity of solving some problems. If the protection of information using some kind encryption algorithm is provided by secrecy, i.e. the inaccessibility of the structure of the algorithm itself, such an algorithm is called limited. Limited algorithms cannot be exploited by a wide range of users, since leakage of information about the structure of the algorithm leads to irreversible loss of secrecy for all users at once, depriving the entire protection system of meaning [4, 7].

The algorithm for encryption methods allows the use of a relatively short key for encrypting arbitrarily large text are considered. To protect messages in multichannel telecommunication systems, the cipher method is mainly used.

In the system of transmission and protection of information (fig. 1), the key used is usually external to the encryption and decryption algorithms information that determines the specific type of encrypted message Y for a given initial message X .

Based on the new approach, the general formula for using the encryption methods for the i -th alphabet character is expressed as follows:

$$Y_i = k_1 x_i + k_2 \pmod{n}, \quad (4)$$

where k_1 and k_2 – are constants; x_i – i -th plain text character, i.e. letter number in alphabet; n – alphabet length.

Expression (4) defines a widely used replacement method in cryptography. When replacing each letter of the plaintext alphabet, one letter is assigned to the cipher of the text from the same alphabet.

Based on the research, it was established in [1, 6] that the approach to information security in multichannel telecommunication systems from unauthorized access should provide:

- confidentiality - information should be protected from unauthorized reading both during storage and when sending a message to the MTS;
- access control - information should be available only for the person for whom it is intended;
- authentication - the ability to uniquely confirm the authenticity of the information and identify the sender in the multichannel telecommunication systems;
- integrity - the information should be protected from unauthorized modification during storage and transfer to the MTS;
- non-repudiation - the sender cannot refuse the fact sending this message to MTS

Taking into account the peculiarities of the new approach, cryptographic information protection is described by the following formula:

$$Y_i(x_i, k_i) = x_i + k_i \pmod{n}, \quad (5)$$

where k_i – i -th letter of the key, which is used as a word or phrase.

Based on the method being studied and the information encryption algorithm, it is possible to check the adequacy using any plaintext.

Thus, on the basis of the proposed approach to information security, the transmitted message via communication channels is conditionally divided into two mutual sequences with the help of which perfect secrecy is ensured - the statistical independence of the transmitted message X from the original message from M .

V. ANALYSIS OF INFORMATION SECURITY IN MTS USING CRYPTOGRAPHIC CODING METHODS

One of the important cryptographic methods and information security algorithms in MTS is the network coding method. Coding is the process of transforming messages in a combination discrete signals, i.e. the process of replacing plain text elements (symbols, combination of codes and words) with codes. In this paper [7, 8], the authors consider unicast transmission on the network and apply random network coding based on correction codes, $N_k(n)$.

Considering the above algorithms, the essence of the proposed approach is that when a message is transmitted, the network coding design consists of several operations:

- Selection of suitable elements and code parameter

$$N_k(n) = G(n, m, d, r),$$

where r , m – number of check and information symbols in code combinations; n – total length of code combination; d – code distance.

- Analysis and selection of a sequence of network coding symbols over a field.

$$Q_{ck}(n, q, r) = GF^{(n-r)}(q, m), \quad m = (n-r) \in M, \quad (6)$$

Taking into account the parameters, the design of the network code for the transmitted message is described as follows:

$$X = D[E(X)] = N_k(n) + GF^{(n-r)}(q, m), \quad (7)$$

From (7) it follows that the source generates a message m from a common set M , which is a sequence of characters over a field $GF^{(n-r)}(q, m)$ and consists of two terms. The source also generates a session key from the set.

Thus, approaches to building an information security system based on cryptographic coding methods should consider each of the structural elements of the communication channels in the MTS.

Further, it is still necessary to solve one of the important tasks arising from the combination of several terminal devices of communication channels and the creation of a telecommunications network.

VI. CONCLUSIONS

As a result of the research, a new approach to cryptographic information protection in MTS from

unauthorized access was proposed, taking into account efficient encoding and encryption methods.

In this method of transferring information of a mixed type of traffic, there are quite a few interesting options for ensuring anonymity depending on the choice of the network code design.

REFERENCES

- [1] Korzhik, V.I. Basics of Cryptography. - SPb. : IC Intermedia, 2016. – 296 p.
- [2] Ibrahimov B.G., Ismaylova S.R. The Effectiveness NGN/IMS Networks in the Establishment of a Multimedia Session // American Journal of Networks and Communications. Vol. 7, №. 1, 2018. – pp.1-5.
- [3] Peeters, E. Advanced DPA Theory and Practice: Towards the Security Limits of Secure Embedded Circuits / E. Peeters. New York : Springer-Verlag New York, 2013. – 139 p.
- [4] Shafali Agarwal. Image Encryption Techniques Using Fractal Function: A Review// International Journal of Computer Science & Information Technology. Vol 9, No 2, 2017. – pp.53-68.
- [5] Cai N., Yeung R.W. Secure Network Coding on a Wiretap Network//IEEE Trans. On Information Theory. - 2011. V. 57, N 1. – pp. 424– 435.
- [6] Ibrahimov B.G. Cryptographic Methods and Means Protection Transmitted Information in Telecommunication Systems// The Proceedings 18-th – IFAC Conference on Technology, Culture and International Stability.IEEE Xplore, № 43613. Sept.13 - 15, 2018. – pp.224-227.
- [7] Gabidulin E.M., Pilipchuk N.I. Error and Erasure correcting algorithms for Rank Codes // Designs, Codes and Cryptography. 2008. - V. 49, N 1–3. - pp. 105–122.
- [8] Zhang S., Yeung R.W. A General Security Condition for Multi-Source Linear Network Coding // Proc. 2009 IEEE Int. Sympos. On Information Theory (ISIT'2009), Korea. - pp. 1155–1158.

İnformasiya təhlükəsizliyi, hüquqi əsasları, müqayisəli yanaşma

Xalid Niyazov

AMEA Hüquq və İnsan Haqları İnstitutu, Bakı, Azərbaycan

xalid-555@mail.ru

Xülasə— Dünya ölkələrinin təcrübəsində də informasiyanın müdafiəsi haqqında ilk qanunlar dövlət sirrinin müdafiəsi haqqında qanunlar olmuşdur. İnformasiya təhlükəsizliyinin hüquqi cəhətdən təmin olunması sahəsində vacib məsələlərdən biri kimi şəxsi məlumatların müdafiəsi çıxış edir. Fransa, İtaliya, İspaniya, Portuqaliya, Danimarka, Hollandiya və s. ölkələrdə hər kəsin hakimiyyət orqanlarının fəaliyyəti ilə bağlı informasiya ilə, ABŞ, Kanada, Avstraliya və Yeni Zelandiyada isə vətəndaşların birbaşa idarəetmə məlumatları ilə tanış olma imkanını təmin edən qanunlar qəbul edilmişdir. İnformasiya təhlükəsizliyinin təmin olunması istiqamətində zəruri tədbirlərin həyata keçirilməsi üçün beynəlxalq hüquqi mexanizmlərin, milli normativ-hüquqi bazanın formalaşdırılması mühüm əhəmiyyət daşıyır və bu məsələ ayrı-ayrı ölkələr kontekstində deyil, beynəlxalq global informasiya təhlükəsizliyi kontekstində nəzərdən keçirilməlidir. Azərbaycan Respublikası informasiya təhlükəsizliyi sahəsində MDB dövlətləri ilə sıx beynəlxalq əməkdaşlıq tədbirlərini həyata keçirir. Müasir inkişaf meylləri və tendensiyaları onu deməyə əsas verir ki, informasiya təhlükəsizliyinin milli təhlükəsizliyin təmin edilməsi sistemində yeri və rolu gələcəkdə daha da artacaqdır.

Açar sözlər— *milli təhlükəsizlik, informasiya təhlükəsizliyi, informasiya hüququ, informasiya cəmiyyəti, informasiya qanunvericiliyi, kompyuter texnologiyaları, informasiya məkanı*

I. GİRİŞ

Bəşəriyyətin keçib gəldiyi bir yol var və həmin yolu müşahidə edərkən görürük ki, təbii-elmi mədəniyyətin nailiyyətləri bir qayda olaraq humanitar mədəniyyət üçün problemlər yaradıb. Burada elə bir sirr yoxdur da... yüksək insan zəkasının məhsulu sayılan texnika onun imkan və qabiliyyətini gücləndirməklə yanaşı həm də hüquqa, belə deyək, meydan oxuyub. Belə ki, informasiya fenomeninin şəxsiyyət-cəmiyyət- dövlət üçbucağının rifahına xidməti ilə yanaşı, dağıdıcı effekti də məlumdur. İki mədəniyyətin vəhdət və mübarizəsi bəşəriyyətin keçid mərhələsində – insanın energetika sektorundakı fiziki imkanlarının informasiya sahəsindəki zəka qabiliyyətinə transformasiyası prosesində daha da güclənir. Belə bir keyfiyyət sıçrayışı nəticə etibarilə cəmiyyətdə qüvvələr palitrasını dəyişir; postsənaye cəmiyyətini informasiya cəmiyyəti əvəz edir, cəmiyyətdə hökmran sosial qrup, həqiqi güc və söz sahibi qismində artıq bankirlər, sənaye maqnatları, oliqarxlar deyil, informasiya və nou-xau texnologiyalarının sahibləri çıxış edirlər

XX əsrin sonu XXI əsrin əvvəli bəşəriyyətin yeni bir cəmiyyətə, yeni sosiofəlsəfi düşüncə müstəvisinə, paradigmal dəyər və meqaideyaların önə keçdiyi ictimai münasibətlər

coğrafiyasına qədəm qoyduğu zaman miqyasıdır. Yeni cəmiyyət hər bir halda yeni insan tipi, transformasiyaya açıq dəyərlər sistemi və bir də mütləq çoxvektorlu ictimai münasibətlər şəbəkəsi ilə səciyyələnir.

Bu gün bir çoxları “Üçüncü dünya müharibəsi” təhlükəsindən danışır. Siyasətşünaslar, hərbi ekspertlər danışirlər. Nostradamusun, Vanqanın, Qlobanın, başqalarının öncəgörmələrində sətiraltı mənalara axtaranlar çoxalıb. Amma hamı bir ortaq fikirlə həmrəydir ki, razılaşır ki, “Üçüncü dünya müharibəsi” artıq başlayıb. Belə ki, müasir hibrid müharibə hər şeydən əvvəl elə informasiya müharibəsidir. Əgər müharibə varsa, apriori təhlükəsizlik tədbirlələri də aktuallaşmalıdır. Fəaliyyət varsa, deməli, konkret münasibətdən danışa bilərik. Hər bir münasibət isə ilk növbədə hüquqi tənzimləmə aparatı tələb edir. Hələ tam formalaşmamış Azərbaycan informasiya hüququ sistemində informasiya təhlükəsizliyinin hüquqi nizamlanması məsələsi həm elmi-nəzəri, həm də praktiki əhəmiyyət kəsb edir.

II. MEYDAN MÜHARİBƏSİNDƏN KİBERMÜHARİBƏYƏ

Bu gün ictimai-siyasi-iqtisadi fəaliyyətin elə bir sahəsini tapmaq mümkün deyil ki, orada informasiya təhlükəsizliyi məsələsi öz aktuallığını diktə etməsin: hərbi-müdafiə, dövlət idarəçiliyi, hüquq-mühafizə, E-hökumət, milli təhlükəsizlik, elmi, humanitar, İKT və s.

Buna görə də informasiyanın ictimai həyatdakı rolunun, iştirak və yerinin yüksəlməsi ilə sıx bağlı olan informasiya təhlükəsizliyi məsələsi də müasir cəmiyyətin qarşılaşdığı ən müstəsna problemlərdən birinə çevrilmişdir. İnformasiya təhlükəsizliyi lokal məsələ olmadığına görə onun hüquqi təminatı sahəsində sistemli iş aparılmalıdır və bu ilk növbədə beynəlxalq informasiya təhlükəsizliyinin, həmçinin milli maraqların qorunması və möhkəmləndirilməsini nəzərdə tutan beynəlxalq norma və prinsipləri diqqətə alan normativ aktların elmi əsaslandırılmasını tələb edir.

2001-ci ildə Avropa Şurası tərəfindən “Kibercinayətkarlıq haqqında” Budapeşt konvensiyası qəbul olunmuşdur. Azərbaycan Respublikası da həmin konvensiyaya qoşulub.

Kibercinayət hər hansı bir informasiya sisteminə icazəsiz və hüquqa zidd şəkildə daxil olunması və sonradan həyata keçirilən əməldir. Bu halda ixtiyari bir insan, ona məxsus əmlak, eyni zamanda istifadə olunan sistemin özü hədəf seçilə bilər. Məsələn, bir sistemə daxil olmaqla zərər vermək, bazanı, informasiya ehtiyatını silmək, şifrələmək, ələ keçirmək, yad

informasiya yükləmək, sistemin iş prinsipini dayandırmaq, şəxsi həyatın toxunulmazlığını pozmaq, əlaqəni əngəlləmək, əlaqəni icazəsiz izləmək, qeydə almaq kimi hərəkət və əməllərin törədilməsi kibercinayət faktlarıdır.

Kibercinayətlərdən bəziləri özünü adi cinayət kimi büruzə verir, yəni maddi vəsaitin mənimsənilməsinə yönəlir. Məsələn, kibervəsitələrlə başqalarının bank hesablarından pulun çıxarılması və oxşar istiqamətlərdə cinayət əməllərinin törədilməsi buna misaldır. Digər bir qrup da var ki, o, mövcud informasiya ehtiyatlarını sıradan çıxarmağa yönəlib. Məsələn, bəzi gənclər kompyuter sistemləri üzrə ixtisaslaşır və özlərini təsdiq etmək üçün bu və ya digər informasiya ehtiyatını sıradan çıxarmağa cəhd edir. Yəni informasiya ehtiyatlarında müəyyən boşluqlar axtarır və ondan sonra müxtəlif şəkillər, müxtəlif bəyanatlar qeyd edir və özlərini bu formada təsdiq etməyə cəhd göstərirlər. Bundan əlavə, məqsədyönlü şəkildə informasiya ehtiyatlarının sıradan çıxarılması təcrübəsi də var ki, bu, adətən mürəkkəb münasibətlərdə olan dövlətlər arasında da baş verir [1].

Elmi ədəbiyyatda internetdəki informasiya müharibəsinin kompyuter cinayətkarlığından fərqləndirilməsinin zəruriliyi vurğulanaraq göstərilir ki, istənilən kompyuter cinayəti birbaşa qanunun pozulması faktıdır. Kompyuter cinayəti təsadüfi də ola bilər, qəsdən planlaşdırılmış da, ayrıca törədilə və ya geniş hücum planının tərkib hissəsi də ola bilər. İnformasiya müharibələri isə heç vaxt təsadüf üzündən, yaxud birtərəfli şəkildə baş vermir (və əksər hallarda qanunu pozmur), istər əsil müharibə meydanında, istərsə də iqtisadiyyatda, yaxud siyasətdə döyüş əməliyyatları aparmaq üçün informasiyadan razılaşdırılmış şəkildə silah kimi istifadəni nəzərdə tutur. İnformasiya mübarizəsi sırf internet vasitələri ilə nadir hallarda aparılır. Bir qayda olaraq, bu mübarizədə şüurlara və məənəviyyətə təsir vasitələrinin bütün bir spektri işə salınır [2, 98].

Kompyuter cinayətkarlığı ilə mübarizəni çətinləşdirən amillərdən biri bu sahədə normativ bazanın kifayət qədər mükəmməl olmamasıdır. Bu problem əksər dünya ölkələrində mövcuddur. Respublikamızda hələ də bu sahədə çox mühüm normativ akt olan “EHM və məlumat bazaları üçün yaradılmış proqramların hüquqi mühafizəsi haqqında” qanun qəbul edilməmişdir. Bu sahədəki münasibətlər “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” 19 iyun 1998-ci il, “Müəlliflik hüququ və əlaqəli hüquqlar haqqında” 5 iyun 1996-cı il, “Dövlət sirri haqqında” 15 noyabr 1996-cı il qanunları (bir sıra digər qanunlar da dolayı yurisdiksiyaya malikdir), habelə CM-nin 271, 272 və 273-cü maddələri ilə tənzimlənir [3,15]. Beləliklə, EHM-lərin fəaliyyətini nizamlayan birbaşa qanun yoxdur.

“İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikası Qanununun 3-cü maddəsində isə informasiyanın mühafizəsinin aşağıdakı məqsədləri müəyyən olunmuşdur:

- informasiyanın məhvinin, itməsinin, saxtalaşdırılmasının qarşısının alınması;
- dövlətin, ictimaiyyətin, vətəndaşların təhlükəsizliyinin təmin edilməsi;

- informasiyanın məhvi, modifikasiyası, sürətinin çıxarılması, təcrid edilməsi ilə bağlı sanksiyalaşdırılmamış hərəkətlərin qarşısının alınması;
- dövlət sirri təşkil edən və konfidensial informasiyanın qorunması;
- informasiya proseslərində və informasiya sistemlərinin, texnologiyalarının və onların təminat vasitələrinin işlənməsi, istehsalı, tətbiqi zamanı fiziki və hüquqi şəxslərin hüquqlarının təmin olunması [4].

Göründüyü kimi, burada dövlət sirri təşkil edən informasiyanın qorunması məqsədi xüsusi olaraq göstərilmişdir. “Dövlət sirri haqqında” Azərbaycan Respublikası Qanununda dövlət sirri dövlətin hərbi, xarici-siyasi, iqtisadi, kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyəti ilə bağlı olub, dövlət tərəfindən mühafizə edilən və yayılması Azərbaycan Respublikasının təhlükəsizliyinə ziyan vura bilən məlumatlar kimi müəyyən edilir. Bu Qanunun müddəaları Azərbaycan Respublikasının ərazisində və onun hüdudlarından kənarda Azərbaycan Respublikasının dövlət hakimiyyəti və yerli özünüidarə orqanları, təşkilati-hüquqi formasından və mülkiyyət növündən asılı olmayaraq bütün müəssisə, idarə və təşkilatları, dövlət sirri haqqında Azərbaycan Respublikası qanunvericiliyinin tələblərini yerinə yetirmək öhdəliyi götürmüş və ya statusuna görə buna borclu olan Azərbaycan Respublikasının vəzifəli şəxsləri və vətəndaşları, əcnəbilər və vətəndaşlığı olmayan şəxslər tərəfindən hökmən icra edilməlidir [5]

III. BEYNƏLXALQ TƏCRÜBƏ VƏ MİLLİ HÜQUQ MƏKANI

Dünya ölkələrinin təcrübəsində də informasiyanın müdafiəsi haqqında ilk qanunlar dövlət sirrinin müdafiəsi haqqında qanunlar olmuşdur. Dövlət sirrinin müstəsna əhəmiyyəti və onun müdafiəsi zərurəti nəzərə alınaraq bütün inkişaf etmiş dövlətlərdə xüsusi ictimai təhlükəli əməllər kimi casusluq və dövlətə xəyanət ən ağır cinayətlər sırasına aid edilmişdir.

ABŞ-in “İnformasiya təhlükəsizliyinin idarə edilməsi haqqında” 2002-ci il tarixli Qanununda informasiya təhlükəsizliyi aşağıdakı kimi xarakterizə edilir:

- informasiyanın və informasiya sistemlərinin icazəsiz girişdən, istifadədən, açıqlamadan, yayılma, dəyişdirilmədən və ya məhv edilmədən müdafiəsi;
- həqiqiliyinin təminatları da daxil olmaqla, informasiyanın təmliğinin qanunsuz dəyişdirilmədən və ya məhv edilmədən qorunmasının təmin edilməsi;
- şəxsi həyat və mülkiyyət haqqında məlumatların gizliliyi də daxil olmaqla, tanış olma və yayılma imkanları məhdudlaşdırılmış informasiyanın konfidensiallığının təmin olunması;
- informasiya ilə tez və etibarlı şəkildə tanış olma imkanını ifadə edən əlçatanlıq.

İnformasiya təhlükəsizliyinin hüquqi cəhətdən təmin olunması sahəsində vacib məsələlərdən biri kimi şəxsi məlumatların müdafiəsi çıxış edir. Ümumdünya İnsan Hüquqları Bəyannaməsinin 12-ci maddəsinə görə, heç kim

şəxsi və ailə həyatına müdaxiləyə, evinin toxunulmazlığına, məktublaşmasının gizliliyinə, şərəf və nüfuzuna özbaşına qəsdə məruz qala bilməz. Hər bir şəxsin belə müdaxilə və qəsddən qanun tərəfindən müdafiə olunmaq hüququ var [6].

ABŞ-ın “Telekommunikasiya haqqında” (1984), “Polis haqqında” (1997), “Təqibdən müdafiə haqqında” (1997) və bir sıra digər qanunlarında da şəxsi həyatın toxunulmazlığı ilə bağlı müddəalar öz əksini tapmışdır.

Fransa, İtaliya, İspaniya, Portuqaliya, Danimarka, Hollandiya və s. ölkələrdə hər kəsin hakimiyyət orqanlarının fəaliyyəti ilə bağlı informasiya ilə, ABŞ, Kanada, Avstraliya və Yeni Zelandiyada isə vətəndaşların birbaşa idarəetmə məlumatları ilə tanış olma imkanını təmin edən qanunlar qəbul edilmişdir. İspaniya, Portuqaliya, Rumıniya, Hollandiya, Avstriya, Macarıstan, Estoniya, Belçika kimi Avropa ölkələrində vətəndaşların rəsmi informasiya ilə tanış olmaq hüququ konstitusion səviyyədə, Fransa, Yunanıstan və İtaliyada isə qanunla təsbit olunmuşdur. İsveç və Finlandiyada bu tendensiyanın əksinə olaraq rəsmi informasiya ilə tanış olmaq hüququ məhdudlaşdırılmışdır. Bolqarıstanın “Məxfi informasiyalar haqqında” 2002-ci il tarixli Qanunu istənilən məmura istənilən sənədə məxfilik qurfi tətbiq etmək imkanı verməklə geniş ictimaiyyətin informasiya ilə tanış olmaq hüququnu məhdudlaşdırır [7, 45-48].

Müasir dövrdə planetin vahid informasiya resurslarının formalaşması prosesi gedir. Yer kürəsinin bütün əhalisinin informasiyanı mənimsəməsi üçün zəmin yaranır [8, 5]. Qlobal informasiya cəmiyyəti formalaşır. Qlobal informasiya cəmiyyətinin qurulması isə qlobal informasiya təhlükəsizliyinin aktuallığını daha da artırır.

Cəmiyyətin informasiya təhlükəsizliyinin təmin olunması üçün zəruri olan tədbirlər kimi beynəlxalq hüquqi mexanizmlərin ciddi araşdırılması, milli normativ-hüquqi bazanın formalaşdırılması, təhlükəsizlik siyasətinin işlənilməsi və reallaşdırılması, xüsusi texnologiyaların tətbiqi, ölkə və korporativ səviyyədə informasiya təhlükəsizliyinin monitorinqi və menecmentinin aparılması, kadr hazırlığı, əhəlinin maarifləndirilməsi və vətəndaşlarda informasiya mədəniyyətinin tərkib hissəsi kimi informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması məsələləri aktuallıq kəsb edir. Ümumiyyətlə, informasiya təhlükəsizliyinin təmin olunması istiqamətində zəruri tədbirlərin həyata keçirilməsi üçün beynəlxalq hüquqi mexanizmlərin, milli normativ-hüquqi bazanın formalaşdırılması mühüm əhəmiyyət daşıyır və bu məsələ ayrı-ayrı ölkələr kontekstində deyil, beynəlxalq qlobal informasiya təhlükəsizliyi kontekstində nəzərdən keçirilməlidir [9, 3-9].

Informasiya məkanında həyata keçirilən fəaliyyət növlərindən bəziləri dövlətlərin informasiya təhlükəsizliyinə ciddi surətdə mənfi təsir göstərə bilər. Ona görə də bu sahə həssas olmaqla, yüksək diqqət, dəqiqlik və əməkdaşlıq tələb edir. İnformasiya- kommunikasiya sahəsini də əhatə edən qloballaşma dövründə dövlətlər arasında əlaqələrin informasiya texnologiyalarına əsaslanan infrastrukturardan asılılığı daha çox artır. Yalnız ikitərəfli, regional və beynəlxalq səviyyədə əlaqələndirilmiş və bir-birini qarşılıqlı tamamlayan tədbirlər informasiya sahəsində müasir təhdidlərə adekvat reaksiya göstərməyə imkan verir [10, 104-106]. Lakin informasiya

sahəsində beynəlxalq əməkdaşlıq sülh və təhlükəsizliyin təmin olunması, dövlətlərin suverenliyinə, daxili işlərinə müdaxilənin yolverilməzliyi və insan və vətəndaş hüquq və azadlıqlarına hörmət kimi prinsiplər əsas götürülməklə həyata keçirilməlidir. Bu əməkdaşlığın həyata keçirilməsində birgə informasiya sistemlərinin və vahid informasiya banklarının yaradılması, habelə operativ, statistik, elmi-metodiki və digər informasiyaların mübadiləsi barədə müddəaları özündə əks etdirən sazişlər xüsusi rol oynayır.

BMT Baş Assambleyasının 23 dekabr 1999-cu il tarixli Qətnaməsində (A/RES/54/49) göstərilir ki, müasir informasiya texnologiyalarının və vasitələrinin yayılması və istifadəsi beynəlxalq sülh və təhlükəsizliyin təmin edilməsi vəzifələrinə zidd ola bilməz. BMT BA-nın beynəlxalq informasiya təhlükəsizliyi barədə 56/19 №-li qətnaməsində göstərilir ki, İKT beynəlxalq stabillik və təhlükəsizliyin təmin edilməsi vəzifələri ilə bir araya sığmayan məqsədlərlə istifadə oluna, habelə ayrı-ayrı dövlətlərin həm mülki, həm də hərbi sahədə təhlükəsizliyini pozmaqla, onların infrastrukturalarının bütövlüyünə mənfi təsir göstərə bilməz. Həmçinin, qeyd edilən qətnamədə cinayət və ya terror məqsədilə informasiya resurslarından və ya texnologiyalarından istifadə edilməsinin qarşısının alınmasının zəruriliyi vurğulanırdı.

7-9 noyabr 2002-ci il tarixində informasiya məsələləri ilə bağlı Buxarestdə keçirilmiş Ümumavropa konfransında qəbul olunan yekun sənəddə öz əksini tapan prinsiplərdən birini İKT-dən istifadə zamanı etimad və təhlükəsizliyin möhkəmləndirilməsi prinsipi təşkil edirdi. Həmin prinsip qlobal kibertəhlükəsizlik mədəniyyətinin formalaşdırılmasını nəzərdə tutur.

15 iyun 2006-cı il tarixdə keçirilən Şanxay Əməkdaşlıq Təşkilatı (ŞƏT) Şurasının iclasında təşkilata daxil olan dövlət başçılarının beynəlxalq informasiya təhlükəsizliyi barədə qəbul etdikləri bəyanatda İKT-dən hüquq bərabərliyi və qarşılıqlı hörmət, dövlətlərin daxili işlərinə qarışmama, münaqişələrin dinc yolla həll edilməsi və güc tətbiq etməmək prinsipləri pozulmaqla insanın, cəmiyyətin və dövlətin təhlükəsizliyi maraqları əleyhinə istifadə edilməsi üçün real təhlükənin mövcudluğu etiraf edilirdi. Göstərilən təşkilat çərçivəsində 16 iyun 2009-cu il tarixdə qəbul edilən “Beynəlxalq informasiya təhlükəsizliyinin təmin edilməsi sahəsində əməkdaşlıq haqqında” Sazişin 2-ci maddəsində beynəlxalq informasiya təhlükəsizliyinin təmin edilməsi sahəsində əsas təhdidlər göstərilmişdir.

Azərbaycan Respublikasında informasiya təhlükəsizliyinin qorunması istiqamətində hüququn əsas mənbəyi ölkə Konstitusiyasıdır.

Konstitusiyaya əsasən:

- hər kəsin şəxsi toxunulmazlıq hüququ vardır (maddə 32, I-VIII his.);
- hər kəsin ətraf mühitin əsl vəziyyəti haqqında məlumat toplamaq və ekoloji hüquqpozma ilə əlaqədar onun sağlamlığına və əmlakına vurulmuş zərərin əvəzini almaq hüququ vardır (maddə 39);
- hər kəsin istədiyi məlumatı qanuni yolla axtarmaq, əldə etmək, ötürmək, hazırlamaq və yaymaq azadlığı vardır (maddə 50);

Ölkədə informasiya sferasındakı münasibətləri tənzimləyən əsas normativ akt “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikası Qanunudur. Həmin hüquqi aktın tənzimlədiyi predmet informasiya müstəvisində yaranan münasibətlərin geniş spektridir.

Bütövlükdə isə, informasiya münasibətləri sferasında tənzimləmə mexanizminin hüquqi mənbəyi kimi aşağıdakıları göstərmək mümkündür:

- Prezident fərmanları;
- AR Konstitusiyası;
- sahəvi qanunlar;
- AR tərəfdar çıxdığı beynəlxalq müqavilələr.

Azərbaycan Respublikası informasiya təhlükəsizliyi sahəsində MDB dövlətləri ilə sıx beynəlxalq əməkdaşlıq tədbirlərini həyata keçirir. Bu əməkdaşlığın normativ hüquqi əsasları kimi aşağıdakıları qeyd etmək olar:

1) 2004-cü il fevralın 6-da Moskva şəhərində imzalanmış "Azərbaycan Respublikası Hökuməti və Rusiya Federasiyası Hökuməti arasında məxfi informasiyanın qarşılıqlı mühafizəsi haqqında" Saziş;

2) 2004-cü il martın 4-də Bakı şəhərində imzalanmış "Azərbaycan Respublikası Hökuməti və Gürcüstan Hökuməti arasında informasiya sahəsində əməkdaşlıq haqqında" Saziş;

3) 2005-ci il aprelın 21-də Kişinyov şəhərində imzalanmış "Azərbaycan Respublikasının Hökuməti və Moldova Respublikasının Hökuməti arasında informatizasiya və informasiya texnologiyaları sahəsində əməkdaşlıq haqqında" Saziş;

4) 2006-cı il iyunun 24-də Astana şəhərində imzalanmış Azərbaycan Respublikası, Qazaxıstan Respublikası, Qırğız Respublikası, Rusiya Federasiyası, Tacikistan Respublikası, Türkmənistan və Özbəkistan Respublikası arasında "Narkotik vasitələrin, psixotrop maddələrin və onların prekursorlarının qeyri-qanuni dövriyyəsi ilə mübarizə üzrə Mərkəzi Asiya Regional İnformasiya və Əlaqələndirmə Mərkəzinin yaradılması haqqında" Saziş;

5) 1 oktyabr 2007-ci il tarixli (№ 402-IIIQ) Azərbaycan Respublikası Qanunu ilə təsdiq edilmiş "Azərbaycan Respublikası Hökuməti və Belarus Respublikası Hökuməti arasında məxfi informasiyanın qarşılıqlı mühafizəsi haqqında" Saziş;

6) 2008-ci il sentyabrın 11-də Bakı şəhərində imzalanmış "Azərbaycan Respublikası Hökuməti və Özbəkistan Respublikası Hökuməti arasında məxfi informasiyanın qarşılıqlı mühafizəsi-haqqında" Saziş və s.

IV. İNFOTƏHDİD VƏ HÜQUQİ TƏNZİMLƏMƏ MƏSƏLƏLƏRİ

Ölkənin firavanlığı və dünya sivilizasiyasında layiqli yeri informasiya texnologiyaları sahəsində siyasətin pragmatikliyindən, konstruktivliyindən və çevikliyindən asılıdır. İnformasiya məkanın qloballaşması və kütləvi kommunikasiya vasitələri şəbəkəsinin təsiri altında cəmiyyətdə baş verən dəyişikliklər təkcə müəyyən üstünlüklər və mənfəətlərlə məhdudlaşmayıb, həm də sosial-siyasi sahədə

informasiya mübarizəsi aparmaq üçün geniş imkanlar açır ki, bu da öz növbəsində milli və beynəlxalq təhlükəsizliyə təhdid doğurur. Bu vəziyyət milli təhlükəsizlik və ilk növbədə, informasiya təhlükəsizliyi kimi mühüm sahənin problemlərinə ənənəvi yanaşmaların ciddi transformasiyasına gətirib çıxarmışdır. Formalaşmaqda olan yeni informasiya-kommunikasiya mühiti istənilən ölkənin siyasi, iqtisadi və müdafiə təhlükəsizliyinə fəal təsir göstərir [11, 8-9].

Son illər kompyuter texnologiyalarının inkişafı ilə bağlı insanların düşüncələrinə, siyasi əqidəsinə, dövlət və cəmiyyət həyatında baş verən hadisə və proseslərə dair baxışlarına təsir göstərən, süni şəkildə müəyyən dairələrin maraqlarına uyğun rəy formalaşdırma vasitələri artmışdır. Məsələn, sosial şəbəkələr vasitəsilə insanlar dövlət çevrilişlərinə, inqilablara çağırılır və s. Bu isə şəxsiyyət-cəmiyyət-dövlət sisteminin bütün ünsürlərinə mənfi təsir göstərməklə, şəxsiyyətin hüquq və azadlıqlarını, cəmiyyətin sabitliyini, dövlətin isə suverenliyini böyük təhdid altında qoymuş olur.

Hər bir dövlətdə informasiya təhlükəsizliyi siyasətinin əsas təyinatı cəmiyyətin maneəsiz, sabit və azad inkişafıdır. Bu isə milli maraqların reallaşması üçün müvafiq əlverişli şəraitin olmasını nəzərdə tutur və informasiya təhlükəsizliyi bütün mümkün vasitələrlə milli maraqların daha səmərəli şəkildə reallaşdırılmasına xidmət edir. Burada informasiya təhlükəsizliyi siyasətini həyata keçirən dövlət orqanlarının operativ və effektiv fəaliyyəti mühüm rol oynayır.

Milli maraqlar, onlara təhdidlər və milli təhlükəsizliyin bütün sahələrində həmin təhdidlərdən müdafiənin təmin olunması informasiya və informasiya sahəsi vasitəsilə həyata keçirilir. Müəlliflərdən İ.L.Bacılo bu məsələ ilə bağlı olaraq qeyd edir ki, informasiya sahəsində milli maraqlara nail olunması və onların təhlükəsizliyinin təmin edilməsi ilə bağlı münasibətlərin tənzimlənməsi üçün müxtəlif hüquq sahələrinin metod və vasitələrindən, o cümlədən intensiv şəkildə inkişaf edən yeni hüquq sahəsi olan informasiya hüququnun metod və vasitələrindən istifadə olunur [12, 21].

İnsan və onun hüquqları, informasiya və informasiya sistemləri və onlara olan hüquqlar yalnız informasiya təhlükəsizliyinin əsas obyekt deyil, həm də bütün sahələrdə bütün təhlükəsizlik obyektlərinin əsas elementləri kimi çıxış edir.

Azərbaycanın qanunvericilik və normativ-hüquqi aktlarına müvafiq olaraq, milli təhlükəsizlik insanların, cəmiyyətin və dövlətin həyatı əhəmiyyətli mühüm maraqlarının, həmçinin milli dəyərlərin və həyat tərzinin daxili və xarici təhdidlərdən etibarlı müdafiəsidir. Milli təhlükəsizlik sistemi ilə milli təhlükəsizliyin təmin olunması sistemi öz məzmununa görə bir-birindən fərqlənir. Birincisi, maraq və təhdidlərin qarşılıqlı təsiri prosesini əks etdirən funksional-nəzəri (konseptual) sistemdirsə, ikincisi, milli təhlükəsizliyin təmin olunmasının praktiki məsələlərini həll etməyi nəzərdə tutan orqanlar, vasitələr, müxtəlif təşkilatlar (institusional) sistemidir [13, 93].

Milli təhlükəsizliyin bütün tərkib elementləri çərçivəsində, yəni, siyasi, iqtisadi, hərbi, ekoloji və s. sahələrdə informasiya faktorunun rolu getdikcə daha çox artır. Müasir inkişaf meyilləri və tendensiyaları onu deməyə əsas verir ki, informasiya təhlükəsizliyinin milli təhlükəsizliyin təmin edilməsi

sistemində yeri və rolu gələcəkdə daha da artacaqdır. Hüquq ədəbiyyatında bu yanaşma konkret arqumentlərlə əsaslandırılır.

İnternetin hüquqi tənzimlənməsi məsələsi də informasiya təhlükəsizliyi ilə bağlı müasir dövrün aktual məsələlərindən birinə çevrilmişdir.

Hazırda bütün dünya üzrə insan fəaliyyətinin ən zəif hüquqi tənzimləməyə məruz qalan sahələrindən biri İnternetdir. Müasir dövrdə dünyanın heç bir ölkəsində İnternet şəbəkəsi ilə bağlı yaranan hüquq münasibətlərini tənzim edən məcəllələşdirilmiş qanunvericilik yoxdur. Bu sahədə mövcud olan normativ hüquqi aktlar Şəbəkənin fəaliyyətinin ayrı-ayrı aspektlərini tənzim edir. Onlara ilk növbədə şəbəkəyə təchizatçılar vasitəsilə qoşulma, müvafiq əlaqə xətləri və ayrıca xidmətlər təqdim edilməsi məsələləri aiddir [14, 16-19].

Aparılan statistik təhlillər və İnterpolun müvafiq məlumatları göstərir ki, hazırkı şəraitdə İnternet planetdə cinayətkarlığın ən sürətli templə artdığı bir məkana çevrilmişdir.

İnternetin qlobal xarakteri milli qanunvericilik sistemləri ilə beynəlxalq praktika arasında ziddiyyət yaradır. Internetdə yerləşdirilən informasiya bir qrup dövlətlərin maraqlarına xidmət etdiyi halda digər dövlətlərin maraqlarına və qanunvericiliyinə zidd ola bilər. Bu isə virtual məkanda milli təhlükəsizliyin təmin edilməsi məsələsinin aktuallığını artırır

NƏTİCƏ

Beləliklə, qeyd edilənləri aşağıdakı kimi ümumiləşdirmək mümkündür:

Milli informasiya təhlükəsizliyinin daha səmərəli və dolğun təmin edilməsi baxımından aşağıdakıları zəruri hesab edirik:

- “İnformasiya təhlükəsizliyi haqqında” qanunun qəbul edilməsi;
- informasiya təhlükəsizliyinin idarə edilməsi mexanizminin təkmilləşdirilməsi;
- şəxsi həyatın toxunulmazlığının daha dolğun təmin edilməsi;
- dövlət orqanlarının fəaliyyətində şəffaflığın təmin edilməsi;
- elektron sənəd dövriyyəsinin və elektron imzadan istifadənin genişləndirilməsi;
- postneft dövründə qeyri-neft sektorunun inkişafı fonunda rəqabətədavamlı, dünya standartlarına və ən son tələblərə cavab verən informasiya texnologiyalarının istehsalı üzrə fəaliyyətin ön palana çəkilməsi;
- sosial mediada təhqir, böhtan, işgüzar nüfuza xələl gətirilməsi, cəmiyyətin və dövlətin maraqlarına zidd, xaosə səbəb ola biləcək çağırışlarla və digər bu kimi mənfi və arzuolunmaz hallarla adekvat mübarizə imkanının təmin olunması üçün İnternet resurslarının məzmununun yoxlanılması üzrə mükəmməl və qabaqcıl dünya dövlətlərinin mütləq təcrübəsinə uyğun gələn texniki və hüquqi mexanizmlərin tətbiqi və s.

ƏDƏBİYYAT

- [1] İnternetdə və informasiya cəmiyyətində insan hüquqları/ <http://azerbaycaninfo.az/iqtisadiyyat/print:page,1,1214-dnternetdj-vj-informasiya-cjmiyyjtindj-insan-hgquqlard.html>.

- [2] Əsgərbəyov Y. İnternetdə informasiya müharibələri / İnformasiya müharibələri və kompyuter cinayətkarlığı. Bakı: Elm və təhsil, 2011, 120 s.
- [3] Xəlilov Q., Eminov F. Kompyuter cinayətkarlığı ilə mübarizə və milli qanunvericilik / İnformasiya müharibələri və kompyuter cinayətkarlığı. Bakı: Elm və təhsil, 2011, 120 s.
- [4] “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanunu. Bakı: Qanun, 2013.
- [5] “Dövlət sirri haqqında” Azərbaycan Respublikası Qanunu / <http://e-qanun.az/framework/5526>.
- [6] İnsan hüquqları haqqında Beynəlxalq bill. Bakı: “Azərbaycan” nəşriyyatı, 1998, 54 s.
- [7] Асланов Р.М. Зарубежный опыт правового регулирования обеспечения информационной безопасности // Политика и общество, 2012, № 2 (86), с. 45-48.
- [8] Камышев Э.Н. Информационная безопасность и защита информации. Учебное пособие. Томск: ТПУ, 2009, 95 с.
- [9] Əliquliyev R.M., İmamverdiyev Y.N., Yusifov F.F. Cəmiyyətin informasiya təhlükəsizliyinə dair bəzi konseptual baxışlar // İnformasiya cəmiyyəti problemləri, №2 (4), 2011, s. 3-9.
- [10] Асланов Р.М. Международное правовое регулирование в сфере обеспечения информационной безопасности // Закон и право, 2012, № 3, с. 104-106.
- [11] Мехтиев Р. Общие подходы к укреплению международной информационной безопасности / Информasiya müharibələri və kompyuter cinayətkarlığı. Bakı: Elm və təhsil, 2011, s. 8-9.
- [12] Исполнительная власть Российской Федерации. Проблемы развития / Под ред. И.Л.Бачило. М.: Юрист, 1998, 432 с.
- [13] Həsənov Ə.M. Azərbaycan Respublikasının milli inkişaf və təhlükəsizlik siyasətinin əsasları. Bakı: Zərdabi LTD, 2016, 700 s.
- [14] Танимов О.В., Кудашкин Я.В. Перспективы правового регулирования отношений в сети Интернет // Информационное право, 2010, № 4, с. 16-19.

FUNDAMENTAL LEGAL PRINCIPLES OF INFORMATION SECURITY: A COMPARATIVE APPROACH

Kh. Niyazov

Institute of Law and Human Rights of ANAS
xalid-555@mail.ru

Abstract – It should be emphasized that in the experience of the countries across the world there were the first laws on the information protection and national security information too.

In France, Italy, Spain, Portugal, Denmark, the Netherlands and other countries, laws were passed which allowed everyone to get acquainted with information on the activities of government agencies and in the United States, Canada, Australia and New Zealand, in accordance with these laws, citizens have the opportunity to obtain information directly about management.

Particular emphasis should be put on that, in order to take the necessary measures to ensure information security, the issue of the formation of international legal mechanisms and the national legal and regulatory framework is of special importance and should be considered not in the context of individual countries but in international global information security. The Republic of Azerbaijan in the field of information security carries out measures for international cooperation with the CIS countries, as substantive legal frameworks. Current trends in development create the opportunity to assert that the place and role of information security in the system of ensuring national security will be strengthened, which is specifically argued in the law books.

Keywords – national security, information security, information law, information society, information legislation, computer technology, information space

Blok Zinciri Bileşenleri ve Uygulamaları Üzerine Bir Derleme

Sedat Akleylek¹, Kübra Seyhan²

^{1,2}Ondokuz Mayıs Üniversitesi, Samsun, Türkiye

¹sedat.akleylek@bil.omu.edu.tr, ²kubra.seyhan@bil.omu.edu.tr

Özet. Blok zinciri teknolojisi, merkezi sistemlerin güvenilir aracıya duyduğu ihtiyaç sonucu daha güvenilir ve aracısız sistemlere olan arayış ile ortaya çıkmıştır. Blok zinciri teknolojisinin dağıtık ağ yapısı, uçtan-uca iletişim mantığı, içermiş olduğu özet değeri hesabı ve elektronik imzalama gibi kriptografik işlemler blok zinciri teknolojisini birçok çalışma alanı için tercih edilebilir kılmıştır. Enerji ve finans sektörleri, e-devlet teknolojisi, bulut depolama sistemleri gibi birçok alanda hızlı ve güvenli işlem yapmaya olanak sağlayan blok zinciri teknolojisi günümüzde işlemsel veri paylaşımı konusunda etkin bir şekilde kullanılmaktadır. Bu çalışmada blok zinciri teknolojisinin çalışma sistemi açıklanarak teknolojinin sahip olduğu özellikler kriptografik işlemler temel alınarak detaylandırılmıştır. Ayrıca blok zinciri teknolojisinin karakteristiği ve türlerine dair özellikler açıklanarak blok zinciri teknolojisinden dolayı sistemlere sağlayacağı avantaj ve dezavantajlara yer verilmiştir. İzinli blok zinciri HyperledgerFabric ve izinsiz blok zinciri Bitcoin teknolojilerine dair araştırma sonuçları sunulurken blok zinciri teknolojisine bir sisteme uygunluğuna karar verilirken değerlendirilmesi gereken parametreler açıklanmıştır. Son olarak blok zinciri teknolojisine dair gelecek çalışmalara kaynaklık edecek, güncel gelişmeler sonucu ortaya çıkan bazı problemlere yer verilmiştir.

Anahtar Kelimeler: Blok Zinciri, Bitcoin, HyperledgerFabric

1. Giriş

Blok zinciri güvenilir olmayan katılımcıların bulunduğu geniş bir ağda merkezi olmayan ve işlemsel veri paylaşımı için gelişmekte olan bir teknoloji olarak değerlendirilir. Veri yapısı olarak blok zinciri, her bloğun küçük bir işlem listesi içerdiği sıralı bir blok yapısıdır[3]. Blok zinciri ismini her bir bloğun bir önceki bloğa kriptografik özet değeri ile bağlı olduğu zincir yapısından alır. İşlemler blok zincirinde bulunan her bir düğüm tarafından oluşturulabilir ve değiştirilebilir özelliktedir. Blok zincirleri dağıtılmış defter sistemleridir. Başka bir deyişle, bilgi tek ve merkezi bir veritabanında değil, potansiyel olarak sonsuz sayıda yerde saklanabilir. Blok zinciri veri depolama sağlarken şeffaflık ve bütünlük garantisi verir, güvenilir 3. tarafa olan ihtiyacı ortadan kaldırır. Bu özelliklerinden dolayı bir blok zinciri dağıtılmış bulut depolama, tedarik zinciri yönetimi, sağlık, mülkiyet ve telif dağıtımı, seçim oylarının kaydedilmesi gibi alanlarda ilgi görmeye başlamıştır [1]. Veritabanı sistemlerinde durumu veritabanına yazacak bir yazar belirlenir. Blok zincirinde ise belirlenen anlaşma protokolünde yer alan ve blok zincirinin büyümesine olanak sağlayabilen herhangi bir katılımcı veritabanındaki yazara karşılık gelir. Blok zincirindeki her bir yazar, bir blok içerisinde bulunan işlemleri biriktirebilir, ilgili bloğu zincire ekleyebilir ve ağda doğrulayıcı olarak görev yapabilir özelliktedir. Blok zincirinde bulunan okuyucu ise blok zincirini boyutunu değiştiremezken işlem oluşturma sürecine katılabilme özelliğine sahip olur. Ayrıca okuyucu,

sadece blok zincirini okuyabilir, analiz edebilir ya da denetleyebilir özelliktedir [1]. Blok zinciri belirlenen ağda bulunan katılımcılar arasında yürütülen işlemleri kaydeden ve ağ üzerinde dağıtılan açık bir defter özelliği gösterir. Şekil 1’de dağıtılmış sistem bağlantılarının nasıl olduğu gösterilmiştir.

Şekil 1. Sistemler ve Ağ Bağlantıları

Ağdaki her bir işlem blok zincirine eklenmeden önce belirlenen anlaşma protokolüne göre ağda bulunan düğümler tarafından doğrulanır. Kayıtlı olarak belirlenen bilgiler değiştirilemez ve silinemez. Her işlemin geçmişi istenilen herhangi bir zamanda yeniden oluşturulabilir özelliktedir [2].

Literatürde yapılan çalışmalar incelendiğinde Wüst ve Gervais [1] nolu çalışmada blok zinciri türlerini analiz ederek bunların merkezi olarak yönetilen bir veritabanına göre karşılaştırmalarını analiz etmiştir. Ayrıca blok zinciri teknolojisine probleme faydalı bir çözüm olup olmayacağını belirleyebilmek için bir yöntem sunmuştur. Bununla birlikte var olan bir problemin çözümünde hangi tür blok zincirinin tercih

edilmesi gerektiğine dair fikirlerini yapılan çalışmada bildirmiştir.

[2] nolu çalışmada Gatteschi ve arkadaşları blok zinciri teknolojisinin çalışma sistematığının nasıl olduğu üzerinde durmuştur. Diğer çalışmalardan farklı olarak blok zincirinin sahip olduğu avantaj ve dezavantaj özelliklerine değinilmiştir. Ayrıca blok zincirinin evrimsel süreci ve potansiyel uygulama alanları konularının incelendiği gözlemlenmiştir.

Xu ve arkadaşları [3] nolu çalışmada blok zinciri teknolojisinin temel özellikleri ve sistemin çalışma mantığı üzerinde durmuştur. Ayrıca çeşitli blok zincirlerinin mimari açıdan önemli özelliklerini sağlayan bir model önerilmiştir.

Blok zincirinin web teknolojileri üzerindeki etkisi değerlendirildiğinde, English ve arkadaşları [4] nolu çalışmada anlamsal web ile ilgisi bağlamında blok zincir teknolojisinin objektif bir analizini yapmıştır. Ayrıca Bitcoin blok zincirinin fonksiyonel temellerinin tanımı konularına değinilmiştir.

Gaetani ve arkadaşları ise [5] nolu çalışmada bulut bilişim ortamlarının gerçek veri bütünlüğü ihtiyaçlarını ve blok zincir tabanlı sistemleri benimsemek için ele alınan araştırma sorunlarını açıklamıştır. Ayrıca bulut bilişim ortamları için etkili bir blok zinciri tabanlı sistem ön tasarımı önerilmiştir.

A. Motivasyon ve Amaç

Blok zinciri teknolojisinin sağlamış olduğu faydalar ve kriptografik özellikleri göz önüne alındığında birçok farklı uygulama alanında kendine yer bulmuştur. Enerji sektörü, ekonomi sektörü, e-devlet teknolojisi, bulut depolama, mülkiyet ve telif dağıtımı gibi alanlar blok zinciri teknolojisinin kendine yer bulduğu alanlara örnek olarak gösterilebilir. Birçok uygulama alanında kendisine yer bulan blok zinciri teknolojisine dair bilgi paylaşımını sağlamak bu çalışmada temel amaç olarak belirlenmiştir. Ayrıca yapılan bu çalışma ile blok zinciri teknolojisinin genel özellikleri, alt yapısı, çalışma sistematığı, blok zinciri teknolojisinin sağlamış olduğu avantaj ve dezavantajlar, blok zincirinin kriptografik anlamdaki bileşenleri, uygulama alanında kullanıma geçen çeşitli parametrelerinin detaylandırılması ve blok zinciri teknolojisinin bir probleme uygunluğunu içeren bir derleme çalışması gerçekleştirilmiştir.

B. Organizasyon

Bu çalışmada, Bölüm 1’de blok zincirine dair çeşitli çevreler tarafından yapılan tanımlara değinilerek blok zinciri teknolojisinin alt yapısına dair bilgilere yer

verilmiştir. Ayrıca literatürde incelenen çalışmalar hakkında özet bilgiler sunulurken çalışmada amaçlanan yapı belirtilmiştir. Bölüm 2’de blok zinciri teknolojisinin çalışma sistematığı açıklanmıştır. Bölüm 3’de blok zincirinin temel özellikleri, sahip olduğu alt yapıdan kaynaklanan ilave özellikler, blok zinciri türleri ve blok zinciri teknolojisinin sağlamış olduğu avantaj ve dezavantajlara yer verilmiştir. Bölüm 4’te blok zinciri teknolojisinin bir probleme uygunluğu esnasında ölçüt olarak değerlendirilen parametrelere yer verilmiştir. Bölüm 5’te blok zinciri teknolojisinin sahip olduğu çeşitlenmeden kaynaklanan, iki farklı teknoloji olarak göz önüne çıkan, Bitcoin ve Hyperledger Fabric teknolojilerine dair bilgilendirme yapılmıştır. Bölüm 6’da ise gelecekte yapılması düşünülen çalışmalara kaynaklık edecek blok zincirine ait bazı problemlerden bahsedilmiştir.

2. Blok Zinciri Nasıl Çalışır?

Blok zincirin sürdürülebilirliği, işlemlerin geçerliliğini doğrulayan ve madencilik süreciyle yeni bloklara ekleyen bir düğüm ağıyla sağlanır. Blok zinciri veri yapısına yeni bloklar ekleme işlemine madencilik denir. Blok zinciri ağında, geçerli olan işlemleri bloklara ayırma ve bu işlemleri bloklara ekleme işlemi madenciler gerçekleştirir. Tüm blok zincirinin birer kopyasının her bir düğüm tarafından tutulmasını sağlamak amacıyla yeni blok tüm ağa yayılır. Tüm ağ, blok zincirine katılacak olan son blok hakkında bir anlaşmaya varmayı amaçlar. Birbirinden farklı anlaşma mekanizmaları vardır ki bunlar iş ispatı ve çıkar ispatı anlaşma mekanizmalarıdır [3].

Karmaşık bir doğrulama mekanizması içeren bu sistemde, bir düğüm tarafından ağın çoğunun kontrol etmesi neredeyse imkânsızdır. Çünkü yanlış bir bloğun oluşturulması, matematik probleminin diğer düğümlerden önce çözülmesi ve sadece madencilik bloğunda %51 uzlaşma oldukça yüksek hesaplama gücü gerektirecektir. Her bir bloğun bir önceki bloğa ait özet değeri içermesi ile kayıtlı işlemlerde kötü niyetli değişikliklerin önlenmesi sağlanır. Bu ise herhangi bir işlemin değişmesinin onu içeren bloğu ve önceki bloklarında özetlerinin değiştirilmesinin gerekliliği ile sağlanır [2]. Şekil 2’de blok zinciri mimarisinin genel çalışma adımları özetlenmiştir.

Şekil 2. Blok Zinciri Çalışma Adımları

- 1) Ayşe, Barış'a para transfer etmek ister.
- 2) Ayşe işlem mesajını ağı yayımlar.
- 3) Diğer düğümler, blok zincirinin yerel kopyalarını kullanarak Ayşe'nin parayı harcama hakkına sahip olup olmadığını bakar ve işlemin Ayşe tarafından onaylanıp onaylanmadığını kontrol eder.

- 4) Doğrulama işlemi gerçekleştirildikten sonra işlem bloğa eklenir.
- 5) Yeni blok, blok zincirine eklenir.
- 6) Madencilik süreci başlar.
- 7) Düğümler matematiksel bir problemi çözmek için bir yarışma başlatır.
- 8) Yeni blok, blok zincirine eklenir.
- 9) Her bir düğüm sahip olduğu yerel kopyayı günceller.
- 10) Barış parayı alır.
- 11) Yarışmayı kazanan düğüm ödüllendirilir.

Ayşe belirli miktarda kripto para birimini Barış'a göndermek istediğinde, kripto para bir adres ile tanımlanan dijital bir cüzdanında saklanır. Para aktarımının gerçekleşebilmesi için Ayşe göndermek istediği para miktarı ile birlikte Barış'ın cüzdan adresini belirtir ve işlemi bulunduğu ağı yayımlar. Cüzdan içerisinde saklanan gizli bilgiler kullanılarak işlem elektronik olarak imzalanır. Aynı zamanda işlemin Ayşe'nin cüzdanından geldiği ve başka herhangi biri tarafından değiştirilemeyeceğinin garantisi sağlanır. Ağda bulunan diğer düğümler elektronik imzayı analiz eder ve ilgili işlemin gerçekten Ayşe tarafından yapıldığını kontrolünü sağlar. Ayrıca blok zincirinin ağdaki tüm işlemleri saklayan yerel bir kopyasındaki bakiyesi hesaplanarak Ayşe'nin para harcama hakkına sahip olup olmadığı doğrulanır. Ayşe para gönderme işlemi yapabilecek durumda ise düğümler işlemi yeni bir bloğa ekler. Yeni blok onaylanacak olan tüm işlemlerin listesini içerirken yeni blok başlığı ise önceki blok başlığı ve önceki bloğa ait kriptografik özet değerini içerir. Oluşturulan yeni bloğun blok zincirine eklenebilmesi için düğümler madencilik işlemini başlatır. Madencilik işlemi, düğümlerin karmaşık bir matematik problemini çözebilmesi için gerçekleştirmiş oldukları rekabet olarak değerlendirilir. İş ispatı olarak adlandırılan bu süreç işlemlerin ve önceki blok başlığının bir araya getirilmesiyle birlikte verilen bir sonucu üreten düğümlerin rastgele bir değer bulmalarını gerektirmektedir. Düğüm olası bir çözümü gerçekleştirdiğinde hesapladığı sonucu diğer düğümlerle paylaşır ve sonucu denetler. Düğümlerin çoğunluğu sonuç üzerinde anlaşabilirse, blok geçerli kabul edilir ve blok zincirine eklenir. Her bir düğüm kendisinde bulunan yerel kopya blok zincirini günceller. Ayrıca kazanan düğüm bir işlem ücreti şeklinde ödüllendirilebilir. Madencilik sürecinin tamamlanması ile Barış, Ayşe'nin göndermiş olduğu parayı kendi cüzdanında gözlemleyecektir [2].

3. Blok Zinciri Arka Planı

A. Blok Zincirinin Temel Özellikleri

Değişmezlik, bütünlük, eşit haklar, şeffaflık ve tekrar edememezlik blok zinciri tarafından desteklenen 5 temel özelliktir. Kriptografik olarak imzalanmış değişmez işlemler zinciri olan blok zinciri, depolanmış olan verilerin inkâredilememesini sağlar. Kriptografik özellikler sayesinde verinin bütünlüğü, açık erişimin sağlanması, veri şeffaflığı gibi özellikler ağda bulunan her katılımcıya blok zincirine erişme ve blok zincirini işleme yeteneğini eşit oranda sağlar. Blok zincirine güven, ağ içerisinde bulunan düğümler arasındaki etkileşimlerden elde edilir. Blok zinciri ağında bulunan her bir katılımcı işlemleri kolaylaştırmak için güvenilir 3. taraf yerine blok zinciri ağının tamamına güvenir. Blok zincirinde verilerin boyutu, işlemlerin işleme oranı ve veri aktarımındaki gecikme gibi ölçeklenebilirlik sınırları söz konusudur. Bir işlemin blok zinciri üzerinde yer aldığı sunulması ve bu durumun onaylanması arasındaki gecikme, anlaşma protokolü tarafından belirlenir [3].

B. Dağıtılmış Kayıt Defteri ve Merkezi Sistemlerin Sağlamış Olduğu Özellikler

1) **Açık Doğrulama:** Açık doğrulama ile sistemde bulunan herhangi birinin sistemin durumunu doğrulaması sağlanabilir. Dağıtılmış defterde kısıtlı bir katılımcı grubu olan doğrulayıcılar tarafından her bir durum geçişi onaylanırken her bir katılımcının durumu hakkında bilgi sızdırmaksızın genel halin açık doğrulaması yapılabilir. Herhangi bir gözlemci, defterin durumunun protokole göre değiştiğini doğrularken, tüm gözlemciler en azından belirli bir uzunluğa kadar defterin yerel bir kopyasına sahip olabilir. Blok zinciri teknolojisini geleneksel veritabanından ayıran özellik bütünlük ve şeffaflık ile sağlanan açık doğrulama özelliğidir. Merkezi bir sistemde farklı gözlemcilerin farklı görüşlere sahip olabilme özelliklerinden dolayı durum geçişlerinin doğru bir şekilde yürütüldüğü doğrulanmayabilir. Dolayısıyla merkezi sistemlerde gözlemcilerin doğrulamayı sağlayabilmesi için merkezi varlığa güvenmeleri gerekir [1]. Şekil 3’de blok zinciri teknolojisinin açık doğrulama özelliğini sağlarken kullanmış olduğu yapı resmedilmiştir.

Şekil 3. Blok Zinciri Açık Doğrulama

2) **Şeffaflık:** Blok zincirinde şeffaflık işlemlerin herkese açık olması gerekliliğinden kaynaklanmaktadır. Verilerin şeffaflığı ve verilerin durumunun güncellenmesi süreci açık doğrulama özelliği için bir gerekliliktir. Her bir katılımcının bilgiye olan şeffaflığı farklıdır. Dolayısıyla her bir katılımcı her bilgi parçasına erişemez [1]. Sistemin tamamen açık bir defter yapısına sahip olması, blok zinciri teknolojisinin şeffaflığı artırmasının kanıtı olarak gösterilmektedir. Blok zinciri teknolojisinde verilerin kelime tabanlı temsilinin kullanılması, kullanıcıların şeffaflık ve analiz yeteneğini artırıcı bir özellik olarak değerlendirilir [4].

3) **Gizlilik:** Gizlilik ve şeffaflık arasında doğal bir gerilim vardır. Tamamen şeffaf olan bir sistemde herkes herhangi bir bilgi parçasını görebilir bunun sonucu olarak gizlilik sağlanmaz. Tamamen gizli bir sistemin ise şeffaflık özelliği garanti edilemeyecektir. Bazı sistemlerde ise işlem geçişleri şeffaf iken özel gizlilik garantileri verilebilir. Örneğin dağıtılmış defterde ayrı ayrı her bir katılımcı hakkında bilgi verilmezken sistemin genel durumu herkese açıktır. Merkezi sistemlerde sistemin işleyişi için şeffaflık ve açık doğrulama gerekmediğinden gizliliği sağlamak kolay olur. Açık sistemlerde gizlilik, kriptografik teknikler kullanılarak sağlanır. Bununla birlikte düşük verimlilik maliyeti ortaya çıkar [1].

4) *Bütünlük*: Bilginin bütünlüyü sağlanıyorsa bilgi izni olmayan kişiler tarafından ele geçirilmemiştir ve değiştirilmemiştir. Bütünlük, açık doğrulama özelliği ile doğrudan bağlantılıdır. Herhangi bir sistemde açık doğrulama özelliği sağlanıyorsa, sistemde bulunan herkes, verilerin bütünlüğünü doğrulayabilir demektir [1]. İş ispatı tabanlı blok zincirleri, ağda bulunan tüm düğümlerde blok zincirinin bir kopyasının tutulmasından ve madencilik sürecinden kaynaklı veri bütünlüğünü sağlayan özelliklere sahiptir [5]. Blok zincirinin bir parçası olabilmek için tüm madencilerin içerik üzerinde anlaşma sağlamış olması gerekmektedir. Dolayısıyla pratik olarak reddedilemez ve kalıcıdır. Verilerin reddedilemez olması ve kalıcılığının sağlanması ile veri bütünlüğünün sağlanması ilişkili kavramlar olarak değerlendirilir [5].

5) *Fazlalık*: Merkezi sistemlerde genellikle farklı fiziksel sunuculardaki kopyalar ve yedeklemeler sonucu fazlalık oluşur. Blok zincirinde ise sistemde bulunan yazma özelliğine sahip katılımcılar arasındaki çoğaltma yoluyla fazlalık ortaya çıkar [1].

6) *Güven kaynağı*: Güven kaynağı ile sistemde bulunan en yüksek otorite temsil edilir. Bu otorite ilgili sisteme okuma/yazma erişimini verme ve iptal etme yetkisine sahip olacaktır [1].

C. Blok Zinciri Teknolojisinin Kriptografik Parametreleri

Blok zinciri teknolojisi kullanıcı kimliklerini korumak amacıyla kriptografik özelliklerden yararlanır. İşlemlerin güvenli bir şekilde yapılmasını garanti ederken depolanan tüm bilgilerin güvenliğini sağlar. Blok zincirinde açık anahtar şifrelemesi yaklaşımı kullanılır. Asimetrik kriptografi olarak da bilinen bu yöntemde bilgi herkesle paylaşılabilecek bir açık anahtar aracılığıyla aktarılır. Şifreleme ve şifre çözme için tek bir anahtar kullanmak yerine ortak anahtar ve gizli anahtar olmak üzere iki anahtar kullanılır. Blok zinciri teknolojisinde iş ispatı mekanizması ile sistemde bulunan defter kopyalarının tüm katılımcılarda bulunması sağlanarak verinin bütünlüğü garanti edilir. Ayrıca açık anahtar şifreleme ile verilerin bütünlüğünü güvence altına alan bir elektronik imza üretilir. Elektronik imzanın üretimi bir kullanıcının özel anahtarını, matematiksel bir algoritma aracılığıyla imzalamak istedikleri verilerle birleştirilerek yapılmaktadır. Bu yaklaşım ile asıl veriler elektronik imzanın bir parçası haline gelir. Veride meydana gelecek en küçük değişiklik imzayı da değiştireceğinden blok zinciri ile verinin doğruluğu garanti edilebilir ve değişmezliği sağlanmış olur. Özetleme algoritmaları ise blok zincirinde bulunan işlem ayrıntılarını içeren blok

verilerinin değiştirilmediğini ve verilerin bütünlüğünün korunduğunu garanti etmek için kullanılır. Blok zinciri tabanlı teknolojilerde özetleme algoritması olarak SHA-256 algoritması kullanılmaktadır. ECDSA ve eliptik eğri dâhil farklı şifreleme türleri ise blok zincirinde işlemleri doğrulamak için kullanılmaktadır. Katılımcılar arasında gerçekleşen bir işlem sırasında üretilen elektronik imzayı doğrulayan ECDSA algoritması ile işlem verilerinin değiştirilmediğinin kanıtlanması sağlanır [14].

D. Blok Zinciri Teknolojisinin Avantaj ve Dezavantajları [2]

Avantajları:

1) Blok zincirinde, ağda bulunan her bir düğüm tarafından paylaşılan bir depo hizmeti sunulur. Ağda bulunan herkes veriye erişebilir ve işlemleri görüntüleyebilir. Düğümlerde bulunan verilerin depolanması ile beklenmedik olaylarda veri kaybının önüne geçilmiş olur.

2) Blok zinciri herkes tarafından okunabilen ve yazılabilen kısacası erişimin sağlanabildiği dünya çapında bir veri deposu olarak değerlendirilir.

3) Blok zinciri teknolojisinde değişmezlik garanti edilir. Başka bir ifadeyle, istenmeyen kişiler tarafından veri silinemez veya değiştirilemez.

4) Sistemde bulunan herkesin ağda bulunan işlemlerin önceki ve şu anki durumlarına dair bilgiler edinebilmesi özelliği ile blok zinciri teknolojisinde şeffaflık özelliği garanti edilir.

5) Blok zinciri teknolojisinde görevlerin dağıtılması ile merkezi otoriteye ihtiyaç ortadan kalkar.

6) Blok zinciri teknolojisinde elektronik imza ve doğrulama ile her bir düğüm arasında araçlara ihtiyaç duymadan güven sağlanır.

Dezavantajları:

1) Blok zinciri teknolojisinde bulunan madencilik işlemi pahalı donanım gerektirir. Ayrıca bilgi işlem gücünün büyük bir kısmının boşa harcandığı gözlemlenir.

2) Blok zinciri teknolojisinde veri çoğaltma alanına ihtiyaç duyulur. Blok zincirinde her bir düğümün blok zincirinin yerel bir kopyasını içermesi sistemi performans olarak veritabanı sistemleri ile karşılaştırılmaz hale getirir.

3) Blok zinciri teknolojisinin garanti ettiği şeffaflık ile ağda bulunan her bir düğüm, blok zincirinin yerel bir kopyasını saklayıp içeriğine erişebildiği için kullanıcıların gizliliğine ve itibarına zarar verebilir.

4) Blok zincirine bilginin eklenmesi yavaştır.

5) Akıllı sözleşmelerde kodlar herkesin kullanımına açık olduğu ve oluşturulduktan sonra kendi kişiliklerini kazandıkları için istenmeyen kişiler için erişilebilir özelliğe sahip olur. Akıllı sözleşmeler blok zincirinde saklandıkları için değiştirilemez özelliğe sahip olurlar. İstenmeyen kişiler tarafından yapılan değişiklikleri gidermek için geliştiricilerin yeni sözleşmeler oluşturmaları ve tüm verileri, işaretçileri eskiden yeni hale aktarmaları gerekmektedir.

E. Blok Zinciri Çeşitleri:

Blok zinciri teknolojisinin sağlamış olduğu çeşitli özellikler dikkate alındığında teknolojinin iki ana grup altında değerlendirildiği gözlemlenir. Şekil 4’de blok zinciri teknolojisinin alt ana grupları özetlenmiştir.

Şekil 4. Blok Zinciri Türleri

1. *İzinsiz Blok Zinciri:* Herhangi bir düğümün ağa istediği zaman okuyucu ya da yazar olarak katılabildiği ve ayrılabilirdiği blok zinciri türüdür. Her bir durum değişikliği doğrulayıcılar tarafından doğrulanır. Üyelikleri yöneten, izinsiz okuyucuları ya da yazarları yasaklayabilen merkezi bir varlık yoktur. Merkezi bir varlığın olmaması yazılı içeriğin ağda bulunan herhangi bir düğüm tarafından okunabileceği anlamına gelir. İzinsiz blok zinciri yapısında uygulamalar onay ve güvene gerek duyulmadan ağa eklenebilir. İzinsiz blok zincirine örnek olarak Bitcoin ve Ethereum gösterilebilir [1].

2. *İzinli Blok Zinciri:* Blok üyelerinin yazma ve okuma işlemlerine katılma haklarını sağlayan merkezi bir varlık vardır. Gizlilik ve kapsülleme özelliklerini sağlayabilmek için okuyucu ve yazar birbirleriyle bağlantılı olan paralel blok zincirlerinde çalışabilir. Ayrıca blok zinciri ağına erişme özelliği olan kişileri yönetmek için bir erişim kontrol katmanı kullanılır.

İzinli bir blok zinciri, benzerliklerini merkezi bir veritabanı ile paylaşır. Bu durum ise bir blok zincirinin merkezi bir veritabanından daha uygun olup olmadığı sorusunu ortaya çıkarır. İzinli blok zincirinde işlemlerin doğrulanması sırasında her düğüme güvenilmez. Sınırlı sayıda okuyucu ve yazarı yetkilendiren, sadece izin verilen bir grup varlığın okuma ve yazma yapabildiği sözde izinli blok zincirleri kısa süre önce önerilmiştir. İzinli blok zincirine örnek olarak ise HyperledgerFabric ve R3 Corda örnek verilebilir [1].

F. Blok Zinciri Karakteristiği

- Blok zinciri düzenli olarak büyüyebilme özelliğine sahiptir [1].
- Blok zincirinde bulunan her blok, özet değeri ile önceki bloğa bağlıdır. Her blok kendi başlık bilgisi içerisinde, kendisine ve bağlı bulunduğu bloğa ait kriptografik özetleme algoritması kullanılarak hazırlanmış iki adet özet değeri içermektedir. Özet değerlerini her bir bloğun içermesi ile blok zincirinde daha önceden yapılmış olan işlemlerin silinmesinin ve değiştirilmesinin önüne geçilir [3].
- Blok zinciri merkezi olmayan bir kayıt sistemidir. Normal sistemlerde veri tek bir merkezde saklanırken blok zinciri yapısında veri ağı tamamında tutulur [1].
- Blok zincirinde yapılan işlemler, ağda bulunan tüm düğümlere yayımlanır. İşlemler tek düğüm değil de birden fazla düğüm tarafından onaylanır ve sonunda zincire eklenir özellikte olmalıdır [1].
- Blok zinciri teknolojisi ile bütünlüğü korunan veri depolaması sağlanırken işlem şeffaflığı garanti edilir [4].
- Blok zinciri dağıtık kayıt defteri yapısını kullanır. Bu yapıda her bir düğüm dağıtık kayıt defterinin bir kopyasına sahip olur ve ihtiyaç olduğu durumda güncelleme işlemi yapar. Her bir kayıt işlemi bağımsız olarak yapılır. Basit bir veritabanı yapısıdır [1].
- Blok zincirinde tüm işlem geçmişine herkes erişebilir. İşlemlerin geçmişlerine erişim ile sanal paranın geçerliliği kontrol edilebilir [3].
- Blok zincirinde iletişim merkezi bir bağlantıdan değil taraflar arasında doğrudan gerçekleşir [1].
- Blok zinciri mimarisinde her bir işlem ve işleme verilen değer sisteme erişebilme yetkisine sahip olan herkes için açık olur [1].
- Açık anahtarlı şifreleme ve elektronik imzalar blok zincirinde hesapların tanınmasında ve başlatılan işlemlerin yetkilendirilmesinde kullanılır. Blok zincirinde işlemler işlev çağrılarının parametrelerini ve sonuçlarını depolayan veri paketleri olarak değerlendirilir. İşlemlerin bütünlüğü algoritma tabanlı kurallar ve kriptografik teknikler ile kontrol edilir [3].

4. Bir Sistem İçin Blok Zinciri Teknolojisinin Uygunluğu

Sistemin ihtiyaç duyduğu gereksinimler bugünün ilişkili veritabanları tarafından karşılanıyorsa, blok zincirini kullanmak anlamsız olacaktır. Oracle ve MySQL gibi sistemlerin arkasında onlarca yıllık gelişim vardır. Bu teknolojiler trilyonlarca sorgu çalıştıran milyonlarca sunucuya dağıtılmıştır. En kapsamlı, test edilmiş, hataları ayıklanmış ve optimize kodlar içerdikleri için saniyede binlerce işlemi yapabilme özelliğine sahiptirler. Ancak bu durum blok zincirinin işe yaramadığına bir kanıt olarak gösterilemez [2]. Bir probleme çözüm olarak blok zinciri teknolojisi kullanılmak istendiğinde sistemin sağlaması gereken özellikler şu şekilde değerlendirilebilir:

- Eğer sistemin veriyi depolamaya ihtiyacı yoksa veritabanı ya da veri bloğu olarak blok zincirine ihtiyaç duyulmamaktadır [1].
- Sadece bir tane yazar (blok zinciri sistemindeki anlaşmaya bağlı belirlenen katılımcı) varsa, blok zinciri ek garantiler sağlamayacaktır. Çıktı ve gecikme açısından veritabanı daha iyi performans sağlayacaktır [1].
- Paylaşılan bir veritabanına sahip olmak gerekliyse doğru çözüm blok zinciri teknolojisindedir [2].
- Verinin yazılması sırasında birden fazla tarafa ihtiyaç varsa blok zinciri doğru çözüm olacaktır [2].
- Olması muhtemel olan yazarlara güvenilmiyorsa blok zinciri bu sistemin ihtiyacını karşılayacaktır [2]. Sistemde bulunan yazarlar birbirlerine karşılıklı olarak güveniyorsa, yazma erişimi olan paylaşılan bir veritabanı en iyi çözümdür. Sistemde bulunan yazarlar birbirlerine karşılıklı olarak güvenmiyorsa, yazma erişimi olan izinli blok zinciri en iyi çözümdür [1].
- Güvenilir 3. tarafa ihtiyaç var mı? Güvenilir 3. taraf varsa iki seçenek vardır. Eğer güvenilir 3. taraf, her zaman çevrimiçi ise, yazma işlemleri ona devredilebilir ve durum geçişleri için doğrulama işlevleri güvenilir 3. tarafa devredilebilir. Eğer güvenilir 3. taraf genellikle çevrimdışı ise güvenilir 3. taraf sistemin bütün yazarlarının bilindiği izinli blok zinciri ayarında bir sertifika yetkilisi olarak işlev görecektir [1].
- İşlemlerin birbirleri ile bağlantısının nasıl olduğu görülebilir özellikte olmalı mıdır? Cevap hayırsa blok zinciri teknolojisini kullanmak anlamsız olacaktır [2].

Tüm bu parametreler göze alındığında ilgili sisteme blok zinciri teknolojisinin uygunluğunun belirlenmesi esnasında Tablo 1'deki parametreler dikkate alınarak çözüme karar verilmelidir.

Tablo 1. Blok Zinciri Teknolojisinin Problem İçin Uygunluğuna Karar Verirken Değerlendirilen Parametreleri Gösteren Tablo

	Hayır	Evet
Sistemde birden fazla yazara ihtiyaç var mı?	1	0
Paylaşılan veritabanı ihtiyacı söz konusu mu?	1	0
Verilerin yazılması sırasında birden fazla tarafa ihtiyaç duyulacak mı?	1	0
Güvenilir aracı ihtiyacı ortadan kaldırılmalı mı?	1	0
Güvenilir araçların doğrulanması gerekli midir?	1	0
Sistemde bulunan potansiyel yazarlar güvenilmez mi?	1	0
İşlemlerin birbirleri ile bağlantısının nasıl olduğu görülebilir özellikte olmalı mıdır?	1	0

Bir sistem tasarlanırken gereksinimler doğrultusunda Tablo 1'de belirlenen parametrelere ait değerler “0” olduğu sürece blok zinciri teknolojisini kullanmak mantıklı olacaktır. 0'dan farklı her değer için çeşitli değerlendirme ölçütleri göz önüne alınarak diğer veri depolama teknolojileri seçilmelidir. Tablo 1 ve sistemin sağlaması gereken şartların genel olarak değerlendirilmesi Şekil 5 ile resmedilmiştir.

Şekil 5. Sistemler için Blok Zinciri

Blok zinciri kullanan bir sistem tasarlanırken bazı şartların sağlanması gerekmektedir. Bu şartlar:

1) *Veritabanı*: Blok zincirleri paylaşılan veritabanları için bir teknolojidir.

2) *Birden fazla yazar*: Blok zincirleri birden fazla yazara sahip veritabanları için bir teknolojidir. Başka bir deyişle, veritabanını değiştiren işlemleri üreten birden fazla varlığın olması gerekmektedir. Birçok durumda yazarlar aynı zamanda veritabanının bir kopyasını ve düğümler arası geçiş işlemlerini içermelidir.

3) *Güven Yokluğu*: Blok zincirleri, birden fazla güvensiz yazar bulunan veritabanları için geliştirilmiş bir teknolojidir. Veritabanına birden fazla varlığın yazma izni varsa, bu varlıklar arasında belirli bir dereceye kadar güvensizliğin var olması gerekir.

4) *Aracısızlaşma*: Temelde hedeflenen amaç birden fazla güvenilir yazara sahip olan bir veritabanını etkinleştirmektir. Bunun sağlanmasında genel kullanılan yaklaşım güvenilir 3. taraftır. Bu yaklaşımda yazarlar birbirlerine güvenmezler ancak tüm yazarların güvendiği bir aracı belirlenir. Blok zincirleri ise güvenilir olmayan araçlara olan ihtiyacı ortadan kaldırır. Blok zincirinde işlemleri ve kaynakları doğrulamak için merkezi bir varlığa ihtiyaç yoktur. Bir işlemin tanımı, yetki belgesi ve geçerlilik kanıtını içerecek şekilde genişletilir. Böylece her bir işlem, veritabanının bir kopyasını tutan her bir düğüm tarafından bağımsız olarak işlenebilir ve doğrulanabilir hale getirilir.

5) *İşlem Etkileşimi*: Farklı yazarlar tarafından oluşturulan işlemler genellikle birbirine bağlıdır. Örneğin, Ayşe'nin Barış'a bir miktar para gönderdiğini ve Barış'ın bir kısmını Ali'ye gönderdiği varsayıldığında Barış'ın işlemi Ayşe'nin hesabına bağlıdır ve Ayşe'nin hesabını kontrol etmeden Barış'ın işleminin doğrulanmasının bir yolu yoktur. Bunun sonucu olarak, işlemler tek ve paylaşılan veritabanına ait olur. Kısacası blok zinciri her şeyi bir araya getirerek birleştirilmiş bir yol sağlar.

6) *Kuralların Belirlenmesi*: Birden fazla birbirine güvenmeyen yazar tarafından doğrudan değiştirilen bir veritabanı varsa, veritabanı gerçekleştirilen işlemleri kısıtlayan birtakım kurallar içermelidir. Bu kurallar geleneksel veritabanı sistemlerinin içerdiği kurallardan farklıdır. Her bir işlem, ağdaki her bir düğüm tarafından bu kurallara göre kontrol edilmelidir ve başarısız olanlar reddedilmelidir.

7) *Doğrulamaların belirlenmesi*: Bir blok zincirinin temel işlevi yetkili son işlem kaydını yapmaktır. Bu kaydın yapılmasının temel sebebi yeni eklenen düğümlerin veritabanının içeriğini başka bir düğüme güvenmeye gerek olmadan sıfırdan hesaplamasını sağlamaktır. Ayrıca, bazı düğümlerin sistem kesintisi veya iletişim aksaklığı nedeniyle bazı işlemleri kaçırma olasılığını ele alırken iki işlemin çatışma içinde olmasının mümkün olduğu durumlarda, sadece birinin

kabul edilmesine olanak sağlar. Hangi anlaşma şeması kullanılırsa kullanılsın, doğrulama düğümleri geleneksel bir merkezi veritabanının sahibinden çok daha az güce sahiptir. Doğrulamacılar, işlemleri ihlal edemez veya veritabanının kurallarını değiştiremez.

5. Uygulama Bakımından Blok Zinciri

A. İzinli Blok Zinciri Olarak HyperledgerFabric:

HyperledgerFabric, Bitcoin ve diğer mevcut ağların adreslediği temel dijital paranın ötesindeki iş uygulamaları için tasarlanmış izinli blok zincir platformudur [7]. HyperledgerFabric ilk olarak DigitalAsset ve IBM tarafından sağlanmıştır. Açık blok zinciri ürün ve hizmetlerini geliştirmek için farklı kuruluşlardan birçok mühendis HyperledgerFabric projesine katkıda bulunmuştur [8]. Kurumsal içeriklerde kullanılmak üzere tasarlanan HyperledgerFabric açık kaynaklı, dağıtımli defter platformudur. Fabric mimarisi bankacılık, finans, sigorta, sağlık hizmetleri, insan kaynakları, tedarik zinciri ve dijital müzik dağıtımını dahil olmak üzere geniş bir yelpazede sanayi kullanımı vakaları için yenilik, çok yönlülük ve optimizasyon sağlayan son derece modüler ve yapılandırılabilir bir yapıya sahiptir. Fabric izin verilen bir yapı olduğundan katılımcılar anonim ve dolayısıyla tamamen güvenilmez değildir. Katılımcılar birbirlerine tam olarak güvenmese de katılımcılar arasında güvenin ne olduğu konusunda kurulu bir model söz konusudur. Anlaşmazlıkları ele alabilmek için yasal bir anlaşma bulunmaktadır [9].

HyperledgerFabric yapısında bilinmeyen kimliklerin ağa katılmasına izin veren, işlemleri doğrulamak ve ağ güvenli hale getirmek için “iş ispatı” gibi protokoller gerektiren sistemlerden ziyade, bir HyperledgerFabric ağının üyeleri güvenilir bir “Üyelik Servis Sağlayıcısı” aracılığıyla sisteme kayıt olurlar. HyperledgerFabric ayrıca çeşitli takılabilir seçenekler sunar. Defter verileri çoklu formatta saklanabilir ve farklı Üyelik Servis Sağlayıcısı sistemleri desteklenebilir. HyperledgerFabric aynı zamanda kanal oluşturma yeteneğini de sunar. Eğer iki katılımcı bir kanal oluşturuyorsa, o katılımcıların bu kanal için her birinde defterin kopyaları vardır [11]. Modüler yapısı, blok zincir çözümlerinin gizliliğini, esnekliğini en üst düzeye çıkarır. HyperledgerFabric, işlemin gerçekleşmesini üç aşamaya ayıran modüler bir mimari üzerine kurulmuştur. Bu yapıda dağıtık mantık işleme ve anlaşma, işlem siparişi, işlem doğrulama ve taahhüdü yapısıdır. Bu ayırım ile düğüm türleri arasında daha az güven ve doğrulama düzeyi sağlanır. Ayrıca ağ ölçeklendirilebilirliği ve performansı en iyi duruma getirilir. HyperledgerFabric'te desteklenen kanallar,

verilerin yalnızca bilmesi gereken taraflara gitmesine izin verir [10].

1) *HyperledgerFabric Modelinin sağladığı özellikler:*

- İzinli blok zinciridir.
- Dağıtılmış defter platformu özelliği gösterir.
- Akıllı sözleşmeleri destekler.
- Katılımcılar anonim ve dolayısıyla tamamen güvenilir değildir.
- Üyelik Servis Sağlayıcısı desteği vardır.
- Çeşitli takılabilir seçenekler sunar.
- Defter verileri çoklu formatta saklanabilir.
- Farklı Üyelik Servis Sağlayıcıları desteklenebilir.
- Kanal oluşturma yeteneği sunar.
- Modüler yapısı, blok zincir çözümlerinin gizliliğini, esnekliğini en üst düzeye çıkarır.
- Ayrıca ağ ölçeklendirilebilirliği ve performansı en iyi duruma getirilir.

2) *HyperledgerFabric modeli karakteristiği[11]:*

HyperledgerFabric sisteminin sağladığı özellikler Şekil 6’da özetlenmiştir:

Şekil 6. HyperledgerFabric Teknolojisi Özellikleri

a) *Paylaşılan Defter:*HyperledgerFabric, iki bileşeni içeren bir defter alt sistemine sahiptir. Bu bileşenler; dünya durumu ve işlem kayıdır. Her bir katılımcının, ait oldukları her HyperledgerFabric ağına ait defterin bir kopyası vardır.

b) *Akıllı Sözleşmeler:*HyperledgerFabric akıllı sözleşmeler, zincir kodunda yazılır ve bu uygulamanın defter ile etkileşime girmesi gerektiğinde, blok zincirine harici bir uygulama tarafından çağrılır. Çoğu durumda, zincir kodu yalnızca defterin veritabanı bileşeniyle,

dünya durumuyla ve işlem günlüğüyle etkileşime girmez. Zincir kodu çeşitli programlama dillerinde uygulanabilir özelliktedir.

c) *Gizlilik:*Bir ağın ihtiyaçlarına bağlı olarak, bir İşten-İşe ağıdaki katılımcılar, paylaştıkları bilgi hakkında son derece hassas olabilirler. Diğer ağlar için gizlilik en önemli konu olmayacaktır. HyperledgerFabric, gizliliğin önemli bir operasyonel gereksinim olduğu ve nispeten açık olan ağları destekler.

d) *Anlaşma:*HyperledgerFabric, ağ başlatıcılarının, katılımcılar arasında var olan ilişkileri en iyi temsil eden bir anlaşma mekanizması seçmesine izin verecek şekilde tasarlanmıştır.

B. İzinsiz Blok Zinciri Olarak Bitcoin

Bitcoin, dijital para ekosisteminin temelini oluşturan kavram ve teknolojilerin bir araya getirilmesidir. Bitcoin ağında bulunan katılımcılar arasında değer kaydetmek ve aktarmak için Bitcoin denilen para birimleri kullanılır. Bitcoin kullanıcıları birbirleriyle internet üzerinden etkileşime özelliğine sahiptir. Açık kaynak yazılımı olarak kullanılabilen Bitcoin protokol yığını, çok çeşitli bilgi işlem cihazlarında çalıştırılabilir özelliktedir. Geleneksel para birimleriyle yapılabilen tüm işlemler Bitcoin teknolojisi ile yapılabilmektedir. Bu teknoloji, Bitcoin ağının güvenliğini sağlamak için şifreleme ve elektronik imzalamaya dayalı özellikler içermektedir. Bitcoin hızlı, güvenli ve sınırsız olduğu için internet kullanımında mükemmel bir para birimi olarak değerlendirilmektedir. Geleneksel para birimlerinin aksine tamamen sanal olan Bitcoin, anahtar değerler sayesinde ağda işlemlerin sahibinin kanıtlanmasına izin verebilen bir yapıya sahiptir. Bu anahtar değerler genellikle her bir kullanıcının bilgisayarında saklanmaktadır. İşlemlerin kilitlerinin açılmasına olanak sağlayan anahtarların bulundurulması Bitcoinlerin harcanabilmesi için tek ön koşuldur [12].

Bitcoin’in tamamen dağıtılmış eşler arası bir sistem olması merkezi sunucu veya kontrol noktasına olan ihtiyacı ortadan kaldırır. Bitcoinler, “madencilik” adı verilen ve zor bir soruna çözüm arayışında olan bir süreçle yaratılır. Bitcoin ağındaki herhangi bir katılımcı (Bitcoin protokol kümesini çalıştıran herhangi bir aygıt), bu soruna çözüm bulmaya çalışmak için bilgisayarının işlem gücünü kullanarak bir madenci olarak çalışabilir. Bitcoin protokolü, ağ üzerindeki madencilik işlevini düzenleyen yerleşik algoritmalar içerir. Madencilerin çözmesi gereken problemin zorluğu dinamik olarak ayarlanır. Protokol ayrıca, her 4 yılda bir yeni Bitcoinlerin oluşturulduğu oranı yarıya indirir ve toplam 21 milyon jeton olarak Bitcoin sayısını sınırlar. Sonuç olarak, dolaşımdaki Bitcoin sayısı, 2140 yılına kadar 21

milyona ulaşan, kolayca tahmin edilebilen bir eğriyi yakından takip etmektedir. Bitcoin'in düşüş oranının azalması nedeniyle, uzun vadede, Bitcoin para birimi deflasyonisttir. Ayrıca, Bitcoin beklenen ihraç oranının üzerinde ve ötesinde yeni para basmak suretiyle şişirilmaz özelliktedir [12].

Bitcoin'in sahipliği; dijital anahtarlar, Bitcoin adresleri ve elektronik imzalar aracılığıyla kurulmaktadır. Dijital anahtarlar aslında ağda saklanmaz, bunun yerine bir dosyada son kullanıcılar tarafından veya bir cüzdan olarak adlandırılan basit bir veritabanında depolanır. Her Bitcoin işlemi, yalnızca geçerli dijital anahtarlarla oluşturulabilen blok zincirine dâhil edilmek üzere geçerli bir imza gerektirir. Bu nedenle dijital anahtarların bir kopyasına sahip olan herkes bu hesaptaki Bitcoin kontrolüne sahip olur. Anahtarlar, özel (gizli) ve ortak anahtardan oluşan çiftler halinde gelir. Bu dijital anahtarlar, Bitcoin kullanıcıları tarafından çok nadir görülür. Çoğunlukla, cüzdan dosyasında saklanır ve Bitcoin cüzdan yazılımı tarafından yönetilir [13].

1) Bitcoin'in Çalışma Mantığı:

Barış, Ayşe'ye Bitcoin transfer etmek istiyor. Barış'ın Ayşe'ye gönderim yapabilmesi için, Bitcoin tam ya da hafif istemci yazılımını çalıştıran akıllı telefon, tablet veya bilgisayar gibi bir cihazın yanı sıra, Barış'ın özel anahtarı ve Ayşe'nin Bitcoin adresini içeren 2 adet bilgiye ihtiyaç duyulur. Ağda bulunan herhangi bir kullanıcı bir Bitcoin adresine para gönderebilir. Fakat yalnızca özel anahtar kullanılarak oluşturulan benzersiz imza ile Bitcoinlerhesaptan serbest bırakılabilir. Barış yapılacak olan işlemin elektronik olarak imzalanması için bir şifreleme anahtarı kullanır ve bu paraların sahibi olduğunu kanıtlar. Barış ağda bir işlem yayınladığında, ağdaki tüm madencilere bu yeni işlem hakkında bilgi veren bir uyarı gönderilir. Madenciler, elektronik imzaların doğru olduğunu ve Barış'ın işlemleri tamamlamak için yeterli Bitcoin'e sahip olup olmadığını kontrol ederler. Ayrıca madenciler ağda bulunan ve Barış'ın işlemi de dâhil beklemedeki tüm işlemleri paketlemek için yarışır ve sonuçta ortaya çıkan bloğu işlerler. Madenciler ilgili bloğun özet değerini oluştururlar ve eğer sonuç belirli bir sıfır sayısı ile başlamazsa özetleme işlevi yeni bir rastgele sayı kullanarak geri döner. Gerekli özet değeri başlangıçta belirli ancak rastgele sayıda bir sıfır değerine sahip olmalıdır. İstenmeyen tahmin durumunun doğru sayıda sıfır ile üretileceği tahmin edilemez. Dolayısıyla madenciler istenen özet değerini bulmak için farklı anahtarlar kullanarak denemeye devam ederler.

Madenci, doğru sayıda sıfır ile bir özet değer bulduğunda ağda duyurulur ve hem Barış hem de Ayşe'den başarılı işlem hakkında bir onay alınır. Diğer madenciler kabullerini iletirler ve ağda bulunan bir sonraki bloğu keşfetmeye başlar. Bitcoin protokolü kazanan madenciyi, teşvik olarak yeni basılmış Bitcoin seti ile ödüllendirir ve özetlenmiş blok açık defterde yayımlanır. Barış'ın işleminin blok zincirine eklenmesiyle, Barış ve Ayşe'nin her biri Bitcoin'in Ayşe'ye devredildiğini gösteren ilk teyidini alır. İşlem süresi değerlendirildiğinde, geçerli ağın yükü ve Barış tarafından yapılan işlemin içerdiği işlem ücreti öne çıkar. Ancak asgari olarak yaklaşık 10 dakika sürecektir [13].

2) Bitcoin Çalışma Adımları

Bitcoin teknolojisi ile para transferi işlemleri sırasında kullanılan temel yaklaşım Şekil 7'da resmedilmiştir.

Şekil 7. Bitcoin Çalışma Modeli

Ayşe ve Barış arasında gerçekleşen transfer sırasında izlenen adımlar şu şekilde özetlenebilmektedir:

- 1) Barış 3. taraf cüzdan yazılımı kullanarak bir Bitcoin ödeme başlatır.
- 2) Ödeme işlemi ve diğer bekleyen işlemler dünya çapında Bitcoin ağında yayınlanır.
- 3) Madenciler birkaç yüz işlem toplar ve bunları bir blokta birleştirir.
- 4) Madenciler bloğu her on dakikada bir işleyecek şekilde tamamlar veya ağda bir blok çıkarırlar.
- 5) Kazanan madenci, tüm bloğa yeni bloğu yayar, bu işlemi blok zincirinde kaydeder ve teşvik amaçlı Bitcoin ile ödüllendirilir.
- 6) Ayşe, Bitcoin'in gelip gelmediğini görmek için cüzdan yazılımını kullanarak kontrolü sağlar

6. Sonuç ve Gelecek Çalışmalar

Yapılan bu çalışmada blok zinciri teknolojisine dair kabul görülmüş çeşitli çevreler tarafından yapılan tanımlara ve teknolojinin içermiş olduğu alt yapıya dair bilgilendirmeler yapılmıştır. Ayrıca teknolojinin sahip olduğu özellikler ve bu özelliklerin teknolojiye

kazandırmış olduğu avantaj ve dezavantajlar hakkında genel bir değerlendirme sunulmuştur. Çeşitli özelliklerinden dolayı alt dallara ayrılabilir yapıda olan blok zinciri teknolojisinin çeşitleri hakkında bilgilendirmeler yapılmıştır. Bu alt dallardan izinli blok zinciri teknolojisi olarak değerlendirilen HyperledgerFabric ve izinsiz blok zinciri olarak değerlendirilen Bitcoin teknolojileri ve bu teknolojilerin çalışma sistemikleri hakkında bir özet sunulmuştur. Yapılan bu çalışmada özellikle blok zinciri teknolojisinin kriptografik anlamdaki değerinden bahsedilerek hangi durumlarda blok zinciri teknolojisinin kullanılması gerektiğine dair bir yol gösterilmiştir.

Blok zinciri teknolojisinin genel yapısı incelendiğinde bazı açık problemlerin var olduğu gözlemlenmiştir. Bu problemler şu şekilde özetlenebilir:

Problem 1: Gelişen teknolojinin bir ürünü olarak ortaya çıkan ve var olan sistemlerin çözülebilmeye imkân sağlayan kuantum hesaplayıcılar sonrasında blok zincirindeki güvenlik nasıl olacaktır?

Problem 2: Sistemlerin genel çalışma yaklaşımları düşünüldüğünde kötü niyetli kullanıcıları ya da işlemleri anlamak için ek bileşenlere ihtiyaç duyulmaktadır. Blok zinciri teknolojisinde bu bileşenler nasıl belirlenmelidir?

Problem 3: Blok zinciri teknolojisinin sağlamış olduğu özellikler dikkate alındığında teknolojinin sağlamış olduğu parametreler insanlık kullanımına dair nasıl iyileştirilebilir?

Problem 4: Blok zinciri teknolojisinin dezavantajı olarak değerlendirilen verinin belirli bir noktaya kadar büyümesi hangi parametrelerle ve nasıl iyileştirilmelidir?

Problem 5: Aynı iki katılımcının blok üretmesi durumunda bu iki katılımcıdan hangisinin popüler olduğu içermiş olduğu blok sayısı ile belirlenmektedir. Popüler olan katılımcının seçilmesi durumu adillik kavramı düşünüldüğünde nasıl iyileştirilmelidir?

Blok zinciri teknolojisine ait belirlenen açık problemlerin nasıl çözüleceğine dair ilgili yaklaşımlar gelecekte yapılması planlanan çalışmalar olarak değerlendirilmektedir.

KAYNAKÇA

- [1] K. Wüst, A. Gervais, Do you need blockchain?, IACR Cryptology ePrint Archive, 2017, pp. 375.
[2] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaria, To blockchain or not to blockchain: That is the question, IEEE IT Professional, 20(2), 2018, pp. 62-74.

- [3] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, A taxonomy of blockchain-based systems for architecture design, IEEE International Conference on Software Architecture (ISCA), 2017, pp. 243-252.
[4] M. English, S. Auer, and J. Domingue, Blockchain technologies & the semantic web: a framework for symbiotic development, In Computer Science Conference for University of Bonn Students, 2016, pp. 47-61.
[5] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, Blockchain-based database to ensure data integrity in cloud computing environments, In Italian Conference on Cybersecurity (ITA-SEC), 1816, 2017.
[6] G. Greenspan, Avoiding the pointless blockchain project, 2015. <https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/> (Erişim Tarihi: 26.07.2018)
[7] J. Sousa, A. Bessani, and M. Vukolić, A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform, arXiv preprint arXiv:1709.06921, 2017.
[8] Hyperledger Fabric. <https://www.hyperledger.org/projects/fabric> (Erişim Tarihi: 26.07.2018)
[9] Hyperledger Fabric. <https://hyperledger-fabric.readthedocs.io/en/release-1.2/whatis.html> (Erişim Tarihi: 26.07.2018)
[10] S. W. Cocco, G. Singh, Top 6 Technical Advantages Of Hyperledger Fabric For Blockchain Networks, 2018. <https://www.ibm.com/developerworks/cloud/library/cl-top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/index.html> (Erişim Tarihi: 19.07.2018)
[11] Hyperledger Fabric. <https://media.readthedocs.org/pdf/hyperledger-fabric/latest/hyperledger-fabric.pdf> (Erişim Tarihi: 26.07.2018)
[12] A. M. Antonopoulos, “Mastering Bitcoin: unlocking digital cryptocurrencies,” O’Reilly Media, Inc., 2014.
[13] M. Conti, C. Lal, S. Ruj et al., A survey on security and privacy issues of bitcoin, IEEE Communications Surveys & Tutorials, 2018.
[14] J. H. Park, J. H. Park, Blockchain security in cloud computing: use cases, challenges, and solutions, Symmetry, 9(8), 2017, pp. 164.

FIGHT AGAINST PLAGIARISM AS AN IMPORTANT ASPECT OF INFORMATION SECURITY

Sedat Akleylek¹, Kübra Seyhan²

^{1,2}Ondokuz May University, Samsun, Turkey

¹sedat.akleylek@bil.omu.edu.tr, kubra.seyhan@bil.omu.edu.tr

Abstract. Blockchain technology has emerged as a result of the need for trusted mediator in centralized systems and the search for more reliable and efficient systems. Features of blockchain technology such as distributed network structure, end-to-end communication logic, hash value calculation and cryptographic operations such as digital signature have made blockchain technology preferable for many work areas. Blockchain technology, which enables fast and secure transactions in many areas such as energy and finance sectors, e-government technology and cloud storage systems, is now effectively used in transactional data sharing. In this study, the principles of blockchain technology is explained and the properties of this are detailed based on cryptographic operations. Furthermore, the characteristics of blockchain technology are given and the advantages and disadvantages of blockchain technology are discussed. The research results of Hyperledger Fabric for permissioned blockchain and the unauthorized cryptocurrency (for example Bitcoin) technologies are presented and their parameters are evaluated when deciding the suitability of blockchain technology for a system are explained. Finally, some problems related to the future of blockchain technology, which will cause the source of some recent developments, are discussed.

Keywords: Blockchain, Bitcoin, Hyperledger Fabric.

Plagiatlıqla mübarizə informasiya təhlükəsizliyinin mühüm komponenti kimi

Rasim Əliquliyev¹, Ramiz Alıquliyev², Rasim Mahmudov³

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

¹r.alguliev@gmail.com, ²r.aliguliyev@gmail.com, ³rasimmahmudov@gmail.com

Xülasə— Məqalədə müəllif hüququnun pozulmasının xüsusi halı olan plagiatlıqla mübarizənin informasiya təhlükəsizliyinin mühüm istiqaməti olduğu əsaslandırılmışdır. Azərbaycanda plagiatlıqla mübarizəyə dair təkliflər irəli sürülmüşdür. Bunun üçün zəruri olan milli elektron kontentin formalaşdırılmasının, milli antiplagiat sisteminin yaradılmasının konseptual əsasları işlənmişdir. Plagiatlıqla mübarizənin hüquqi, ictimai qınaq və maarifləndirmə metodlarının tətbiqinə dair tövsiyələr verilmişdir.

Açar sözlər— müəllif hüququ, plagiat, milli antiplagiat sistemi, milli kontent.

I. GİRİŞ

İnformasiya cəmiyyətində informasiya və bilik əsas strateji məhsula, maddi sərvətlərin formalaşmasının əsas mənbəyinə çevrilir. Yeni iqtisadiyyatda innovasiyaların, yaradıcı əməyin, intellektual mülkiyyətin, informasiya məhsullarının rolu sürətlə artır. Belə bir şəraitdə intellektual mülkiyyətin və onun əsas tərkib hissəsi olan müəllif hüquqlarının qorunması məsələsi informasiya təhlükəsizliyinin mühüm vəzifələrindən biri kimi xüsusi aktuallıq kəsb edir.

Müəllif hüququ elm, ədəbiyyat və incəsənət əsərlərinin yaradılması və istifadəsi sahəsində ictimai münasibətləri tənzimləyir. Müəllif hüququnun obyektləri müxtəlif növ informasiya məhsullarıdır. İnformasiya təhlükəsizliyinin mühüm vəzifələrindən biri də məhz informasiya məhsulları ilə bağlı sahiblik, istifadə və sərəncam hüquqlarının qorunmasıdır [1].

Müəllif hüququnun pozulmasının ənənəvi formalarından biri plagiatlıqdır. İnternetin meydana gəlməsi, mətnlərin rəqəmsallaşması, nüsxələmənin asanlaşması plagiatlıq problemini daha da kəskinləşdirmişdir. Hazırda plagiatlıq tələbələr, elmi tədqiqatçılar, ədiblər, jurnalistlər, musiqiçilər və digər incəsənət nümayəndələri arasında geniş yayılmışdır. Xüsusilə, elmi fəaliyyət sahəsində bu problem özünü daha qabarıq şəkildə büruzə verir.

Hüquqi ədəbiyyatda plagiat dedikdə, başqalarına məxsus ədəbiyyat, incəsənət və elmi əsərlərin, ixtiraların və s. intellektual yaradıcılıq məhsullarının bilərəkdən mənimsənilməsi başa düşülür. Lakin müəyyən qaydalara əməl etməklə ideyalardan, konsepsiyalardan, metodlardan və s. müəllif hüququ obyektlərindən istifadə edilməsi plagiatlıq sayılır.

Plagiatlıq hallarının qarşısının alınması üçün mənəvi-etik, hüquqi, texnoloji, maarifləndirici və s. tədbirlərin görülməsi zəruridir. İKT-nin köməyi ilə İnternet mühitində baş verən plagiatlıq halları ilə mübarizə üçün yeni üsul və vasitələr tələb edilir. Antiplagiat proqramları İnternet mühitində olan materiallar əsasında müvafiq halların aşkarlanması üçün ən yaxşı vasitədir. Lakin plagiatlıq hallarında istinad edilən bir sıra elmi əsərlər vardır ki, onların elektron versiyaları yoxdur. Ona görə də müvafiq proqramlar vasitəsi ilə heç də bütün plagiatlıq hallarını üzə çıxarmaq mümkün olmur. Bu da milli elektron elmi kontentin yaradılması məsələsini aktuallaşdırır [2].

Ölkəmizdə İnternetdən istifadə imkanlarının artması, əhali arasında ingilis və digər xarici dil biliklərinin səviyyəsinin yüksəlməsi plagiatlıq üçün əlverişli şərait yaradır.

Plagiatlıq cəmiyyətin və dövlətin informasiya təhlükəsizliyinə ciddi təhiddir. Belə ki, cəmiyyətdə plagiatlıq hallarının artması əhali arasında informasiya mədəniyyətinin, insanların informasiya təhlükəsizliyinə qarşı dözümsüzlük səviyyəsini aşağı salır.

İnformasiya mədəniyyəti səviyyəsinin aşağı olması, müxtəlif mənbələrdən müstəqil şəkildə informasiya toplamaq, müqayisə və analiz etmək, daha mötəbər, aktual informasiyanı müəyyənləşdirmək bacarığının olmaması, əhalinin dezinformasiyaya qarşı həssas olmasına gətirib çıxardır. Ona görə də plagiatlıqla mübarizəyə müəllif hüququnun, intellektual mülkiyyətin qorunması ilə yanaşı, həm də, daha geniş mənada, informasiya təhlükəsizliyinin qorunması məsələsi kimi baxmaq lazımdır.

II. İNTERNET MÜHİTİNDƏ MİLLİ KONTENTİN FORMALAŞDIRILMASI MƏSƏLƏLƏRİ

Plagiatlıq hallarının aşkar olunmasının əsas şərtlərindən biri İnternet mühitində milli kontentin formalaşdırılmasıdır. Belə ki, şəffaflıq və əlyetərlilik plagiatlıq imkanlarını minimuma endirir. Eyni zamanda, rəqəmsal formada olan mətnlərdə plagiatlıq elementlərini texnoloji üsullarla aşkarlamaq daha asandır. Ona görə də İnternet mühitində milli kontentin formalaşdırılması bir sıra amillərlə yanaşı, plagiatlıqla effektiv mübarizə aparmaq baxımından da aktuallıq kəsb edir [2].

Hazırda ölkənin müxtəlif təyinatlı və səviyyəli kitabxanalarında, arxivlərində saxlanılan materialların (kitablar, jurnallar, dissertasiyalar və s.) əksəriyyəti kompüterləşmə dövründən əvvəl çap olunduğuna görə onların elektron versiyaları mövcud deyil. Həmin materialların rəqəmsal formaya keçirilməsi çox vacibdir. Bu, genişmiqyaslı, yüksək əmək və maliyyə tutumlu iş olduğuna görə, dünyanın bir çox ölkələrində müvafiq prosesi effektiv şəkildə həyata keçirmək üçün xüsusi dövlət proqramlarının həyata keçirilməsi təcrübəsi vardır.

Ölkə üzrə müxtəlif qurumların tabeliyində olan e-kitabxanaların əksəriyyətinə Internet vasitəsi ilə daxil olmaq mümkün deyildir. Baxmayaraq ki, “Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya”da “kitabxana, arxiv və muzeylərdə İKT-nin tətbiqinin, elektron kitabxana şəbəkəsinin genişləndirilməsi” məsələsi öz əksini tapmışdır, bu problem həll edilməyib [3].

Bundan başqa, müxtəlif nəşriyyatlar tərəfindən çap olunan kitabların e-versiyaları, əsasən, onlayn mühitdə deyildir. Elmi jurnalların əksəriyyətinin veb-saytları müasir beynəlxalq standartlara, nüfuzlu axtarış sistemlərinin tələblərinə cavab vermir. Ona görə də Internetdə axtarış apararkən həmin jurnallarda yerləşdirilən məqalələri əldə etmək mümkün olmur.

Müəssisələrin sərəncamında olan çap materiallarının rəqəmləşdirilməsi, etibarlı saxlanması, istismarı, arxivləşdirilməsi, onlayn mühitdə əlverişliliyinin təmin olunması və s. kimi məsələlər məsul şəxslərin qarşısında ciddi bir vəzifə kimi qoyulmur. Bu işlərin həyata keçirilməsi, əsasən, könüllü xarakter daşıyır.

Bununla əlaqədar zəruri normativ-hüquqi sənədlər, standartlar və onların tətbiqini təmin edən inzibati mexanizmlər mövcud deyildir.

Qeyd edilən problemlərin aradan qaldırılması, yalnız çap şəklində olan ədəbiyyatın, kitabxanaların rəqəmləşdirilməsi və bütövlükdə, milli elektron kontentin inkişaf etdirilməsi üçün xüsusi dövlət proqramının həyata keçirilməsi zəruridir.

İlk növbədə, sərəncamlarında çap formasında ədəbiyyat olan müvafiq qurumların həmin materialları rəqəmsal formaya keçirərək Internet mühitində əlverişliliyini təmin etmələri vacibdir. Bunun üçün isə yüksək imkanlara malik skanerlər və digər kompüter avadanlıqları ilə təchizat məsələsi həll olunmalıdır.

Rəqəmləşdirilmiş materialların etibarlı saxlanması, istifadəsi və arxivləşdirilməsi üçün müvafiq qurumların tərkibində fasiləsiz fəaliyyət göstərən Data-mərkəzlərin (verilənlərin saxlanması mərkəzləri) təşkil edilməsi vacibdir. Müəssisələrdə mühüm əhəmiyyət kəsb edən informasiya resurslarının uçotu, etibarlı saxlanması, istismarının təmin olunması və arxivləşdirilməsi, müvafiq Data-mərkəzlərə təhvil verilməsi üçün məsul şəxslər və onların hüquqi məsuliyyəti zəruri normativ-hüquqi sənədlərlə dəqiq müəyyənəlməlidir.

Ölkə, dövlət qurumları və müəssisələr səviyyəsində informasiyalasdırma proseslərini nəzarətdə saxlamaq, analiz

etmək, qiymətləndirmək, müxtəlif təyinatlı monitorinqlər aparmaq məqsədi ilə iyerarxik qaydada bütün təşkilatlar üzrə xüsusi statistik formalar işlənilməli, müntəzəm olaraq həmin hesabatlar toplanılmalı və emal olunmalıdır. Bunun da əsasında müəssisələrin fəaliyyətinə qiymət verilməlidir.

Elmi jurnalların beynəlxalq tələblərə cavab verməyən veb-saytları, həmçinin arxivlərdə, çap şəklində olan jurnalları rəqəmləşdirərək Internet mühitində əlverişliliyi təmin olunmayana qədər Azərbaycan Respublikasının Prezidenti yanında Ali Attestasiya Komissiyası tərəfindən onların tanınması məqsədəuyğun sayılmamamalıdır.

Biznes qurumları tərəfindən çap olunan kommersiya xarakterli materialların onlayn mühitdə açıq istifadəsinin təmin olunması üçün dövlət tərəfindən müəyyən stimullaşdırıcı mexanizmlər işlənilib tətbiq olunmalıdır.

III. MİLLİ ANTIPLAGİAT SİSTEMİNİN YARADILMASINA DAİR KONSEPTUAL BAXIŞLAR

Hal-hazırda ölkəmizdə xarici antiplagiat sistemlərindən (AS) pərakəndə şəkildə istifadə olunur və ümumiyyətlə, onların hər biri haqqında fikirlər, rəylər fərqlidir. Xarici AS-dən asılılıq və kifayət qədər maliyyə resurslarının ölkədən kənara axını problemi vardır.

Plagiatlığa qarşı mübarizə mexanizmlərindən biri də elmi araşdırma prosesinin şəffaflığının təmin olunmasıdır. Bu məqsədlə Respublika üzrə elmi tədqiqatların koordinasiya şurası tərəfindən elektron elmin alt sistemləri olan “Elmi problemlər reyestri”, “Dissertasiya mövzularının qeydiyyatı reyestri”, “Elmi hesabatlar reyestri”, “Doktorantlar və dissertantlar reyestri”, “Elmi kadrlar reyestri” və s. kimi açıq onlayn informasiya resurslarının yaradılması və istismarını təmin etmək lazımdır.

Ekspertlərin qənaətinə görə, xarici AS-dən istifadə prosesində toplanmış məlumatların intellektual emalı əsasında hər hansı hədəf seçilmiş ölkədə elmin və təhsilin, tələbə və müəllimlərin, alimlərin mənəvi-etik, hüquq pozuntuları, dinamikası və s. xüsusiyyətləri haqqında analitik biliklər əldə etmək olar. Bu isə ölkənin təhlükəsizliyi üçün müəyyən risklər yaradır.

Xarici AS-dən istifadə zamanı milli maraqlar naminə çoxməqsədli analizlər aparmaq, qiymətləndirmək, tövsiyələr işləmək və səmərəli qərarlar qəbul etmək imkanları yoxdur. Bütün bunları nəzərə alaraq, hesab edirik ki, Milli antiplagiat sisteminin (MAS) yaradılması və tətbiqi daha məqsədəuyğundur.

MAS-a e-dövlətin mühüm seqmentləri olan e-elm və e-təhsilin tərkib hissəsi kimi baxmaq lazımdır. Belə ki, e-dövlətin əsas məqsədləri sırasında idarəçiliyin metod və mexanizmlərinin təkmilləşdirilməsi, səmərəliliyinin artırılması, hesabatlılığın və şəffaflığın təmin edilməsi kimi məsələlərdir. Elm və təhsil sistemlərində elmi fəaliyyətin şəffaflığının və hesabatlılığının təmin edilməsi, qiymətləndirilməsinin təkmilləşdirilməsi və səmərəliliyinin artırılması baxımından MAS effektiv texnoloji vasitədir.

Müvafiq dünya təcrübəsinin analizinə əsasən, belə qənaətə gəlmək olar ki, hər hansı bir antiplagiat sisteminin yaradılması,

sınaqdan keçirilməsi və təkmilləşdirilməsi üçün müəyyən müddət tələb edilir. Bu baxımdan, MAS-nin yaradılması və müəyyən keyfiyyət səviyyəsinə çatdırılması üçün müəyyən vaxt lazımdır. Ona görə də MAS effektiv tətbiq üçün tam hazır olana qədər xarici AS-dən istifadə məqsədəuyğundur.

Ümumiyyətlə, ölkədə AS-in yaradılmasına dair mütəxəssislər arasında iki yanaşma vardır:

- xarici AS-ni Azərbaycan dilinin xüsusiyyətlərini nəzərə alaraq, müvafiq açıq informasiya resurslarını təkmilləşdirmək və geniş tətbiqini təmin etmək.
- beynəlxalq təcrübədən faydalanmaqla ölkənin intellektual, maliyyə və digər potensialı hesabına MAS-ı yaratmaq, istismarı və inkişafını təmin etmək.

MAS-nin yaradılması ilkin halda nisbətən böyük maliyyə resursları tələb etsə də, sonrakı dövrdə bu xərclər xeyli azalacaqdır. Ölkə daxilində vətəndaşlara çox aşağı qiymətə (yaxud da pulsuz) onlayn antiplagiat xidmətləri göstərilə bilər.

MAS yaradılsa, sistemdə toplanmış məlumatlar əsasında elm və təhsil prosesi, ayrı-ayrı fərdlərin mənavi-etik, hüquq pozuntuları barədə zəruri biliklər əldə olunacaq. Gələcəkdə təşkilatlar (elm, təhsil və s. müəssisələr) və şəxslər barəsində müxtəlif xarakterli qərarlar qəbul edilərkən plagiatlıq əməllərinin də nəzərə alınması məqsədəuyğundur.

Kitabxanalarda, arxivlərdə toplanan dissertasiyalar, monoqrafiyalar, jurnallar və s. rəqəmləşdirilərək İnternet mühitində yerləşdirildikdən sonra MAS elmi dərəcəsi olan şəxslərin dissertasiya işlərini, digər əsərlərini də yaxlayıb plagiatlıq əməllərini aşkarlayaraq ictimaiyyəti məlumatlandırmaq imkanına malik olacaqdır.

MAS tələbələrin, müəllim və alimlərin, digər bilik yaradıcılığı ilə məşğul olan şəxslərin müəllifi olduqları materiallarda aşkarlanmış plagiatlıq faktlarının qeydiyyatını, uçotunu aparıb sistemləşdirərək ayrı-ayrı şəxslər (alimlər, tələbələr və s.) və müəssisələr üzrə elektron plagiatlıq reyestrləri yaratmağa imkan verəcəkdir.

MAS istismara verildikdən sonra xarici ölkələrdəki bədnəviyyətli qüvvələrin ölkəmizdə formalaşan biliklər cəmiyyətinin, onun sosial segmentləri (elm, təhsil müəssisələri və s.), həmçinin ayrı-ayrı vətəndaşların intellektual cinayətləri haqqında məlumat toplamaq və analitik biliklər əldə etmək imkanı olmayacaqdır.

MAS veb-platformasında kliyent/server texnologiyası əsasında fəaliyyət göstərəcək sosio-texnoloji infrastruktura malik bir sistem kimi istismar olunacaqdır. Bu sistem istismara verildikdən sonra qlobal səviyyədə, virtual məkanda plagiatlığa qarşı səmərəli mübarizə aparmaq məqsədi ilə xarici ölkələrin AS-i, İnternetdə mövcud olan axtarış sistemləri ilə əməkdaşlıq münasibətləri qurula bilər.

MAS-nin konseptual, arxitektura-texnoloji əsaslarının işlənilməsi, toplanacaq informasiyanın intellektual analizi (*Big Data* analitikası), təhlükəsizliyinin təmin olunması, həssas fərdi məlumatların qorunması, mükəmməl kompüter tərcüməsi sistemlərinin işlənilməsi, dissertasiya və digər elmi əsərlərin müəlliflərinin identifikasiyası və s. kimi elmi tutumlu

problemlərin həlli üçün geniş tədqiqatlar aparılması, gənc kadrların yetişdirilməsi vacibdir.

MAS-nin yaradılması, istismarı və daim təkmilləşdirilməsi, inkişafı məqsədi ilə fəaliyyət planının işlənilməsinə ehtiyac vardır. Eyni zamanda, MAS-a dövlət əhəmiyyətli informasiya sistemi statusunun verilməsi və bu məqsədlə müvafiq normativ-hüquqi sənədlərin hazırlanması zəruridir.

MAS-ın yaradılması, istismarı və inkişafının dəstəklənməsi məqsədi ilə bütün mərhələlər üzrə həyata keçiriləcək işlərin maliyyələşdirilməsinə, eyni zamanda, xarici AS-in servislərindən istifadə etmək üçün elm və təhsil müəssisələrinə maliyyə dəstəyi göstərilməsinə ehtiyac vardır.

MAS-ın yaradılmasına dair fəaliyyət planında nəzərdə tutulmuş işlər, həmçinin maddi-texniki təminat üzrə texniki-iqtisadi araşdırmalar aparıb tələb olunan xərclər və onların maliyyələşdirilməsi üçün mənbələr müəyyənəldir.

IV. PLAGIATLIQLA HÜQUQİ MÜBARİZƏ YOLLARI

Plagiatlıqla mübarizə metodlarından biri hüquqi mübarizədir. Müasir beynəlxalq hüquq təcrübəsində plagiatlıq müəllif hüququnun pozulması hallarından biri kimi qəbul olunur. Lakin Azərbaycanın bu sahədə ictimai münasibətləri tənzimləyən “Müəlliflik hüququ və əlaqəli hüquqlar haqqında” qanunda və “Əqli mülkiyyət hüquqlarının təminatı və pircatılığa qarşı mübarizə haqqında” qanunda plagiatlıqla bağlı məsələlər öz əksini tapmayıb [4, 5].

Azərbaycanda plagiatlıqla bağlı hüquqi baxımdan qeyri-müəyyənliklər mövcud olduğuna görə məhkəmələr tərəfindən bu qanun pozuntusuna görə qərar vermək çox çətindir. Ona görə də ölkəmizdə plagiatlıq əməllərinə hüquqi qiymət verilməsi hallarına rast gəlinmir. Müvafiq qurumlarda da plagiatlıq sahəsində beynəlxalq hüquqi təcrübənin öyrənilməsi istiqamətində elmi araşdırmalar aparılır.

Plagiatlıqla effektiv hüquqi mübarizə aparmaq üçün vacib olan məsələlərdən biri də müvafiq qanunvericiliyin həyata keçirilməsidir. Azərbaycan qanunvericiliyində plagiatlıqla mübarizə tədbirləri nəzərdə tutulmadığına görə, ölkəmizdə bu sahədə istintaq, məhkəmə-ekspertiza təcrübəsi də demək olar ki, mövcud deyil. Müvafiq ali məktəblərdə bu sahə üzrə mütəxəssislər də hazırlanmır. Ona görə də plagiatlığın elmi-nəzəri, texniki, hüquqi, etik və s. aspektlərini əhatə edən biliklərə malik mütəxəssislər hazırlanmalıdır ki, onlar da, öz növbəsində, ali məktəblərdə müvafiq fənni tədris etsinlər.

Plagiatlıqla hüquqi mübarizəni çətinləşdirən əsas problemlərdən biri bu cür əməllərin qlobal xarakterli və ya miqyaslı olmasıdır. Yəni İnternetin yaratdığı qlobal virtual mühitdə plagiatlığı törədənə plagiatlığa məruz qalan müxtəlif ölkələri təmsil edə bilərlər. Dünyanın ayrı-ayrı ölkələrində isə plagiatlığa münasibət fərqlidir. Bu problemdən çıxış yolu plagiatlıqla mübarizə sahəsində xüsusi beynəlxalq konvensiyanın qəbul edilməsi və müvafiq qarşılıqlı hüquqi yardım haqqında ikitərəfli dövlətlərarası müqavilələrin bağlanmasıdır.

V. PLAGİATLIQ ƏMƏLLƏRİNİN İCTİMAİLƏŞDİRİLMƏSİ MƏSƏLƏLƏRİ

Plagiatlıqla effektiv mübarizə üsullarından biri də bu cür əməllərin ictimailəşdirilməsi, ictimai qınaq obyektinə çevrilməsinin təşkildir. Cəmiyyətin aşağı təbəqələrini təmsil edən insanlar tərəfindən törədilən məişət xarakterli cinayət əməllərinə görə bu cür üsullardan istifadə edilməsi effektiv nəticə vermir. Çünki belə şəxslərin itirəcəkləri ictimai nüfuzları, karyeraları yoxdur. Plagiat elmi iş ortaya qoyanlar isə, adətən, cəmiyyətin yüksək təbəqəsinə aid olan, müxtəlif karyera hədəfləri olan insanlar olur. Ona görə də plagiatlıq edən insanların bu əməllərinə görə rüsvay edilmələri olduqca böyük effekt verir.

Plagiatlıq əməlləri tam sübut olunduğu hallarda müvafiq dövlət qurumları tərəfindən ictimaiyyətə rəsmi məlumat verilməsi məqsədəuyğundur. Bundan sonra plagiatlığa əl atan şəxslər haqqında məlumatlar müntəzəm olaraq KİV-də, sosial media resurslarında yayıla bilər. Bu fəaliyyət ilə məşğul olan şəxslər ictimai qınaq, məzəmmət obyektinə çevrilməlidirlər.

Bu məqsədlə xüsusi portal (məsələn: www.plagiatayox.az) yaradılıb plagiatlıq, səbəbləri, növləri, onunla mübarizə texnologiyaları, aşkarlanmış faktlar və s. kimi məlumatların ictimaiyyətə təqdim olunması məqsədəuyğundur. Həmçinin televiziya kanallarında, İnternet saytlarında, ictimai yerlərdə, elm-təhsil müəssisələrində plagiatlıqla mübarizə məqsədi daşıyan sosial reklam çarxları nümayiş etdirilməsi də effektiv bir vasitədir.

Bu sahədə xarici ölkələrin qabaqcıl təcrübəsinin öyrənilərək tətbiq edilməsi və həmin ölkələrin müvafiq qurumları ilə əməkdaşlıq münasibətlərinin qurulması zəruridir.

VI. PLAGİATLIQ VƏ ONUNLA MÜBARİZƏ YOLLARININ TƏDRİSİ

Plagiatlığın baş vermə səbəblərindən biri də bu əməli törədənlərin onun barəsində məlumatsız olmalarıdır. Hal-hazırda ölkəmizdə plagiatlığın meydana gəlməsi səbəbləri, növləri, antiplagiat mexanizmləri, bu əməllərin yaratdığı mənəvi-etik və hüquqi məsuliyyət və s. haqqında biliklər təhsilin heç bir pilləsində tədris olunmur.

Plagiatlığa qarşı mübarizə texnologiyaları, mexanizmləri, antiplagiat sistemləri haqqında hədəf auditoriyasına, ümumiyyətlə, vətəndaşlara zəruri biliklər verilməlidir. Plagiatlıq əməllərinin yaratdığı mənəvi-etik və hüquqi məsuliyyət haqqında vətəndaşlar maarifləndirilməlidirlər.

Azərbaycan dilində bu sahə üzrə dərslər və digər öyrədici vasitələr mövcud deyil, həmin bilikləri tədris edəcək müəllimlər də hazırlanmır. Magistratura və doktorantura təhsil səviyyələrində “Plagiatlıq və onunla mübarizə yolları” adı

altında sistemli biliklərin tədris olunması vacibdir. Bunun üçünsə, ilk növbədə, dərslər, metodiki vəsaitlər hazırlanmalı, müvafiq dərsləri tədris edəcək müəllimlər yetişdirilməlidir.

NƏTİCƏ

Beləliklə, belə nəticəyə gəlmək olar ki, plagiatlıqla mübarizəyə dair irəli sürülən ideyaların, konseptual baxışların aidiyyəti qurumların iştirakı ilə geniş müzakirə olunması və müəyyən bir konsensusun əldə edilməsi vacibdir. Müzakirələrin nəticəsi olaraq aidiyyəti qurumların mütəxəssisləri tərəfindən “Azərbaycan Respublikasında plagiatlığa qarşı mübarizə sahəsində milli fəaliyyət planı”nın işlənilməsinə ehtiyac vardır.

Milli fəaliyyət planında görülməli işlər, vəzifələr, icraçılar, icra müddəti, maliyyə resursları müəyyənləşdirilməlidir. Bu planının icrasını təmin etmək məqsədi ilə icraçı qurumların məsul vəzifəli şəxslərindən ibarət Koordinasiya şurası və bu şuranın nəzdində müxtəlif problemlər (texnologiya, linqvistika, kontent, hüquq və s.) üzrə işçi qruplar təşkil olunmalıdır.

ƏDƏBİYYAT

- [1] R.M.Əliquliyev, R.Ş. Mahmudov, “İnformasiya cəmiyyətində intellektual mülkiyyət hüquqlarının qorunması problemləri”, İnformasiya cəmiyyəti problemləri, Bakı, 2015, №2, c. 4-14.
- [2] R.M.Əliquliyev, N.B. Ağayev, R.M. Əliquliyev, “Plagiatlıqla mübarizə texnologiyaları”, Bakı, “İnformasiya Texnologiyaları” nəşriyyatı, 2015, 165 s.
- [3] “Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya”, <http://president.az/articles/11312>
- [4] “Müəllif hüququ və əlaqəli hüquqlar haqqında” AR Qanunu, <http://www.copat.gov.az>
- [5] Əqli mülkiyyət hüquqlarının təminatı və piratçılığa qarşı mübarizə haqqında” AR Qanunu, <http://www.copat.gov.az>

FIGHT AGAINST PLAGIARISM AS AN IMPORTANT ASPECT OF INFORMATION SECURITY

Rasim M. Alguliyev¹, Ramiz M. Aliguliyev², Rasim Mahmudov³

Institute of Information Technology of ANAS, Baku,
Azerbaijan

¹r.alguliev@gmail.com, ²r.aliguliyev@gmail.com,
³rasimmahmudov@gmail.com

Abstract – The article argues that the fight against plagiarism, which is a special case of copyright infringement, is an important aspect of information security. Proposals on fight against plagiarism in Azerbaijan are put forward. The conceptual basis for the formation of national electronic content and the creation of a national anti-plagiarism system is developed for this purpose. Recommendations on the application of legal, public awareness and awareness raising methods in the fight against plagiarism are provided.

Обнаружение атак на киберфизические системы на основе глубокого обучения

Людмила Сухостат

Институт Информационных Технологий НАНА, Баку, Азербайджан

lsuhostat@hotmail.com

Аннотация— Частота и серьезность атак на киберфизические системы требуют разработки новых подходов обнаружения и локализации кибератак. В работе предлагается подход, сочетающий в себе преимущества вариационного автоэнкодера и «остаточной» нейронной сети. Предлагаемый подход тестируется на наборе данных системы газопроводов, собранном в Центре защиты критически важных инфраструктур штата Миссисипи (США). Он сравнивается с логистической регрессией и конволюционной нейронной сетью. Сравнительный анализ показывает, что предлагаемый подход может идентифицировать практически все атаки, присутствующие в наборе данных.

Ключевые слова— информационная безопасность, киберфизические системы, кибератаки, глубокое обучение, вариационный автоэнкодер, «остаточная» нейронная сеть.

I. ВВЕДЕНИЕ

Широкое внедрение киберфизических систем (КФС) формирует процесс объединения технологий и знаний, обеспечивая автономию, надежность и систематичность [1]. Быстрый рост приложений КФС приводит к необходимости обеспечения информационной безопасности таких систем.

Следовательно, возникает потребность в оценке влияния кибератак на нормальное функционирование физических процессов. При этом важно не только проанализировать разрушительное воздействие кибератак и их последствия, но и обеспечить доступность информации о киберактивности. Важно заранее разработать алгоритмы обнаружения и контрмеры для всех известных атак, чтобы уменьшить влияние атак в течение ограниченного времени и свести к минимуму возможный причиняемый ущерб системы.

Кибератаки могут быть как преднамеренными, так и непреднамеренного действия, дифференциация которых в больших и сложных КФС бывает порой невозможна. В связи с этим возрастает потребность в разработке новых подходов для обнаружения аномального поведения системы. Эффективная киберфизическая безопасность достигается посредством стратегии защиты, которая направлена на обнаружение вторжений в разных областях КФС.

Глубокое обучение рассматривается как современный подход искусственного интеллекта и включает в себя ряд алгоритмов и решений, которые значительно расширяют сферу действия и эффективность нейронных сетей [2-4]. Наличие большого количества слоев позволяет нейронной сети построить концепцию объекта исследования от простых признаков, постепенно переходящих к более сложным.

В данной статье предлагается подход, сочетающий в себе преимущества вариационного автоэнкодера (variational autoencoder, VAE) и одномерной глубокой «остаточной» нейронной сети (deep residual neural network, ResNet), как эффективный метод обнаружения кибератак в КФС. Предложенная модель была протестирована с использованием набора данных системы газопроводов, собранного в Центре защиты критически важных инфраструктур штата Миссисипи [5]. Предлагаемый подход сравнивается с логистической регрессией [6], конволюционной нейронной сетью [7] до и после применения энкодера из VAE.

II. ВАРИАЦИОННЫЙ АВТОЭНКОДЕР

VAE представляет собой разновидность автоэнкодера, которая также состоит из энкодера и декодера. Энкодер оценивает скрытые переменные из переменных наблюдения, а декодер восстанавливает переменные наблюдения из скрытых переменных.

Пусть x - вектор переменных наблюдения, z - скрытый вектор, а ϕ и θ - наборы параметров энкодера и декодера, соответственно. Вектор наблюдения x вводится в энкодер, на выходе которого получают математическое ожидание $\mu_\phi(x)$ и дисперсию $\sigma_\phi^2(x)$, которые используются для сэмплирования (sampling) скрытого вектора z [8].

z сэмплируется после распределения Гаусса с $\mu_\phi(x)$ и $\sigma_\phi^2(x)$ [9, 10]. Декодер $p_\theta(x|z)$ генерирует x из z . Затем непосредственно оцениваются $\mu_\phi(z)$ и $\sigma_\phi^2(z)$ для генерации выходного вектора x .

Градиенты рассчитываются на основе $p_\theta(x)$:

$$p_{\theta}(x) = \int p_{\theta}(z)p_{\theta}(x|z)dz. \quad (1)$$

III. «ОСТАТОЧНАЯ» НЕЙРОННАЯ СЕТЬ

С увеличением числа слоев в глубоких нейронных сетях ошибка обучения возрастает, а производительность сети ухудшается. Это указывают на то, что в современных методах обучения нейронной сети с большим числом слоев по-прежнему существует множество проблем. Чтобы решить эти проблемы была разработана ResNet [11]. Она состоит из серии остаточных модулей. Формула расчета для выхода n -го остаточного модуля следующая:

$$x_n = x_{n-1} + F(x_{n-1}; W_n), \quad (2)$$

где $F(x_{n-1}; W_n)$ - остаток в сети, а W_n - параметр сети.

Во время обучения сеть напрямую не вычисляет выход (x_n), а вычисляет остаточное значение между x_n и входом x_{n-1} , обозначаемое как F .

Однако ResNet с большим числом слоев требует больших вычислительных ресурсов [12]. По этой причине в работе с целью уменьшения пространства признаков, содержащихся в наборах данных, предлагается использовать VAE.

IV. ПРЕДЛАГАЕМЫЙ ПОДХОД

Предлагаемый подход включает следующие этапы:

1. Получение данных для обучения и оценки эффективности модели.
2. Предварительная обработка данных. Извлечение признаков на основе энкодера из VAE, состоящего из полносвязных слоев (Dense) (Рис. 1)

Рис. 1. Структура вариационного автоэнкодера.

3. Построение одномерной ResNet (1DResNet) (Рис. 2) с целью обнаружения кибератак. Сеть состоит из 25 слоев. Она включает конволюционные (convolutional) и пулинг (maxpooling) слои. Для более быстрого обучения были добавлены слои Batch Normalization. а, b и с обозначают

число выходных фильтров в конволюционных слоях. В первых трех блоках $a=64$, $b=64$ и $c=64$. А в последних четырех они равны 128, 128 и 512, соответственно.

4. Обучение полученной модели для нахождения оптимального решения.

5. Оценка полученной модели на тестовом наборе данных.

V. ОПИСАНИЕ БАЗЫ ДАННЫХ

Для проведения экспериментов была рассмотрена база данных системы газопроводов, собранная в Центре защиты критически важных инфраструктур штата Миссисипи США [5]. Лог файл данных сетевого трафика был взят из системы SCADA (Supervisory Control And Data Acquisition) для лабораторного стенда системы газопроводов, включающего как нормальную работу системы, так и реальные кибератаки. Сетевые пакеты имеют временную метку и записываются в лог файл с уникальными признаками, в т.ч. автоматический режим работы системы (вкл/выкл), управление насосом и клапаном соленоида и др.

В наборе данных есть четыре основные категории атак: атаки путем внедрения команд (command injection attacks), атаки путем внедрения данных, отказ в обслуживании (Denial of Service, DoS) и зондирование (reconnaissance). Эти четыре категории дополнительно подразделяются на семь конкретных типов атак: атака внедрения злоумышленного отклика (naïve malicious response injection, NMRI), атака комплексной вредоносной реакции (complex malicious response injection, CMRI), внедрение команд вредоносного состояния (malicious state command injection, MSCI), внедрение команд с вредоносными параметрами (malicious parameter command injection, MPCCI), внедрение вредоносного кода (malicious function code command injection, MFCCI), DoS и reconnaissance (Recon.). Набор данных содержит 214580 стандартных сетевых пакетов (Normal) и 60048 пакетов с атаками [2].

VI. МЕТРИКИ ОЦЕНКИ МЕТОДОВ КЛАССИФИКАЦИИ

Для оценки производительности классификаторов используются следующие метрики: accuracy, recall, precision и F-measure. Для любого алгоритма классификации возможны четыре классификационных случая, и это помогает понять разницу между рассматриваемыми метриками: истинно-положительные результаты (True Positives, TP), ложно-положительные результаты (False Positives, FP), истинно-отрицательные результаты (True Negatives, TN) и ложно-отрицательные результаты (False Negatives, FN).

Рассматриваемые метрики определяются следующим образом:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \quad (3)$$

которая определяет долю правильных результатов, полученных классификатором.

$$precision = \frac{TP}{TP + FP} . \quad (4)$$

Эта метрика показывает, какая доля объектов, выделенных классификатором как положительные, действительно является положительной.

Рис. 2. Структура 1DResNet.

$$recall = \frac{TP}{TP + FN} , \quad (5)$$

которая показывает, какая часть положительных объектов была выделена классификатором.

Следующая метрика сочетает в себе меры точности и полноты:

$$F - measure = \frac{2 \times recall \times precision}{recall + precision} . \quad (6)$$

VII. РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТОВ

Эксперименты проводились на Intel Xeon (R), CPU X5670 @ 2.93 ГГц×4, 10 Гб RAM. Предлагаемый подход оценивался на языке Python 2.7.13 с использованием различных библиотек, включая Tensorflow и Keras.

Тенденция вариационной функции потерь при применении VAE показана на Рис. 3.

Рис. 3. Вариационная функция потерь.

Результаты сравнения предлагаемого подхода с логистической регрессией (LR) и конволюционной нейронной сетью (CNN) показаны в таблице I.

На Рис. 4 показаны точность и ошибка кросс-энтропии VE+1DResNet в зависимости от номера итерации.

a)

б)

Рис. 4. Точность и функция потерь для VE+1DResNet.

ТАБЛИЦА I. СРАВНЕНИЕ ПРЕДЛОЖЕННОГО ПОДХОДА С ЛОГИСТИЧЕСКОЙ РЕГРЕССИЕЙ И КОНВОЛЮЦИОННОЙ НЕЙРОННОЙ СЕТЬЮ

	LR	CNN	1DResNet	VE+ LR	VE+CNN	VE+1DResNet
Точность обучения	59.33%	63.29%	70.31%	47.54%	60.09%	68.77%
Точность тестирования	59.28%	63.11%	65.32%	47.51%	59.04%	68.66%

ТАБЛИЦА II. СРАВНЕНИЕ РЕЗУЛЬТАТОВ КЛАССИФИКАЦИИ

Метод	Метрика	Normal	NMRI	CMRI	MSCI	MPCI	MFCI	DoS	Recon.
LR	Precision	58.63%	45.72%	50.07%	49.19%	47.31%	87.13%	50.88%	100%
	Recall	34.61%	90.05%	12.42%	47.04%	53.06%	100%	61.15%	75.52%
	F-measure	43.53%	60.65%	19.91%	48.09%	50.02%	93.12%	55.54%	86.05%
CNN	Precision	78.07%	48.92%	45.06%	73.07%	42.13%	89.95%	78.45%	100%
	Recall	36.92%	9.26%	92.06%	38.76%	89.63%	100%	52.74%	85.81%
	F-measure	50.13%	15.57%	60.50%	50.66%	57.31%	94.71%	63.07%	92.37%
1DResNet	Precision	93.67%	49.61%	49.21%	76.44%	70.59%	100%	57.26%	66.40%
	Recall	51.02%	57.50%	52.44%	59.57%	64.02%	50.19%	88.97%	98.96%
	F-measure	66.06%	53.27%	50.77%	66.96%	67.15%	66.84%	69.68%	79.47%
VE+ LR	Precision	46.25%	45.81%	43.67%	39.28%	37.93%	78.05%	35.70%	60.23%
	Recall	31.89%	51.14%	49.86%	57.65%	21.61%	64.29%	40.85%	62.98%
	F-measure	37.75%	48.33%	46.56%	46.72%	27.53%	70.50%	38.10%	61.57%
VE+CNN	Precision	90.60%	52.31%	45.12%	44.72%	39.20%	94.17%	58.84%	100%
	Recall	31.76%	7.27%	94.49%	50.85%	60.30%	100%	45.86%	90.48%
	F-measure	47.03%	12.76%	61.08%	47.52%	47.52%	97.00%	51.55%	95.00%
VE+1DResNet	Precision	92.20%	55.29%	52.12%	78.24%	73.44%	97.60%	74.05%	100%
	Recall	50.52%	74.26%	63.09%	68.28%	63.67%	100%	88.98%	98.96%
	F-measure	63.58%	60.67%	61.53%	66.96%	68.20%	98.79%	69.70%	98.21%

Предлагаемый подход (VE+1DResNet) распознал все 7 классов атак и нормальное состояние системы в отличие от других рассмотренных методов. Он незначительно уступил 1DResNet в классификации согласно трем метрикам для класса Normal (Таблица II).

VIII. ЗАКЛЮЧЕНИЕ

Обнаружение вторжений является одной из серьезных проблем в области обеспечения информационной безопасности КФС. В этом исследовании был предложен подход VE+1DResNet, сочетающий в себе преимущества VAE и одномерной ResNet.

В целом, предложенный подход показал высокую точность обнаружения атак в ходе проведения

экспериментов. Подводя итоги, можно сделать вывод, что анализ оценки предложенного подхода, основанного на глубоком обучении, может быть полезен для будущих исследований и идентификации атак.

ЛИТЕРАТУРА

- [1] R. Alguliyev, Y. Imamverdiyev, L. Sukhostat, "Cyber-physical systems and their security issues," Computers in Industry, Vol. 100, pp. 212–223, 2018.
- [2] C. Feng, T. Li, D. Chana, "Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks," Proc. of the 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 261–272, 2017.
- [3] J. Goh, S. Adep, M. Tan, Z.S. Lee, "Anomaly detection in cyber physical systems using recurrent neural networks," Proc. of the IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), pp. 140–145, 2017.

- [4] J. Shin, Y. Baek, J. Lee, S. Lee, “Cyber-physical attack detection and recovery based on RNN in automotive brake systems,” Preprints, pp. 1-21, 2018.
- [5] T. Morris, R. Vaughn, Y.S. Dandass, “A testbed for SCADA control system cybersecurity research and pedagogy,” Proc. of the 7th Annual Workshop on Cyber Security and Information Intelligence Research, pp. 1-4, 2011.
- [6] D. Hosmer, S. Lemeshow, “Applied Logistic Regression,” John Wiley & Sons, Inc., 2000. 373 p.
- [7] Y. LeCun, Y. Bengio, “Convolutional networks for images, speech, and time series,” The handbook of brain theory and neural networks, pp. 255-257, 1995.
- [8] H. Nishizaki, “Data augmentation and feature extraction using variational autoencoder for acoustic modeling,” Proc. of APSIPA Annual Summit and Conference, pp. 1222-1227, 2017.
- [9] D.P. Kingma, M. Welling, “Auto-encoding variational bayes,” Proc. of International Conference on Learning Representations (ICLR), pp. 1-14, 2014.
- [10] D.P. Kingma, T. Salimans, M. Welling, “Variational dropout and the local reparameterization trick,” Proc. of the 29th Annual Conference on Neural Information Processing Systems (NIPS), pp. 2575–2583, 2015.
- [11] K. He, X. Zhang, S. Ren, J. Sun, “Deep residual learning for image recognition,” Proc. of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 770–778, 2016.
- [12] C. Szegedy, S. Ioffe, V. Vanhouche, A. Alemi, “Inception-v4, inception-resnet and the impact of residual connections on learning,” Proc. of the AAAI Conference on Artificial Intelligence, 4278–4284, 2017.

DETECTION OF ATTACKS ON CYBER-PHYSICAL SYSTEMS BASED ON DEEP LEARNING

Lyudmila Sukhostat

Institute of Information Technology of ANAS, Baku, Azerbaijan

lsuhostat@hotmail.com

Abstract – The frequency and severity of attacks on cyber-physical systems require the development of new approaches for cyber-attacks detection and localization. The paper proposes an approach that combines the advantages of a variational autoencoder and a residual neural network. The proposed approach is evaluated on a gas pipeline system dataset collected at the Critical Infrastructure Protection Center of the Mississippi State University (USA). It is compared with logistic regression and a convolutional neural network. A comparative analysis shows that the proposed approach can identify almost all attacks in the dataset.

Keywords – information security, cyber-physical systems, cyber-attacks, deep learning, variational autoencoder, residual neural network.

Kriptovalyuta verilənlərinin intellektual analizi məsələləri

Yadigar İmamverdiyev¹, Firəngiz Sadiyeva²

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

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

Xülasə— Kriptovalyutalar son bir neçə ildə meydana çıxmış və maliyyə sektorunda inqilabi dəyişikliklər vəd edən fenomendir. Əksər kriptovalyutaların əsaslandığı blokçeyn texnologiyası digər fəaliyyət sahələrində də diqqətəlayiq dəyişikliklərə yol açır. Məqalədə kriptovalyuta texnologiyalarının qısa xülasəsi verilir, bu sahədə tətbiqi gündəmdə olan bəzi texnoloji həllər diqqətə çatdırılır və kriptovalyuta verilənlərinin intellektual analizi metodları təhlil olunur.

Açar sözlər— kriptovalyuta; Bitcoin, blokçeyn, hardfork, softfork, altcoin, stebylkoin, Ethereum, intellektual analiz

I. GİRİŞ

Kriptovalyuta infrastrukturunun vacib komponentlərindən biri informasiya-analitika xidmətləridir. Bu xidmətlər kriptovalyutaların bazar qiymətləri, kapitallaşması, tranzaksiyaların həcm dinamikası, şəbəkədə komissiyaların orta miqdarı, volatillik və s. haqqında faydalı məlumatlar təqdim edirlər. Belə xidmətlər günbəgün artır. Onlar kriptovalyuta həvəskarları, treyderlər, investorlar, tədqiqatçılar və tətbiqi proqram işləyənlər üçün əvəzedilməz köməkçilərdir.

Əlbəttə, belə xidmətlər yalnız informasiyanın toplanmasını, vizuallaşdırılmasını və təqdim olunmasını yerinə yetirmirlər. Bu xidmətlərin ən əsas xidməti, adından da göründüyü kimi, analitikadır və burada intellektual analiz metodları öz potensial və güclərini göstərməyə, təxminən 10 illik coşqun inkişaf ərzində toplanmış böyük həcmli verilənlərdə gizli qanunauyğunluqları aşkarlamağa hazırdırlar. Təqdim olunan iş bu sahədə tədqiqat məsələlərini dəqiqləşdirmək məqsədilə kriptovalyutaların və onlara aid verilənlərin intellektual analizi metodlarının icmalına həsr olunmuşdur.

II. BITKOİN: QISA İCMAL

Bitcoin blokçeyn texnologiyası ilə işləyən ilk kriptovalyutadır və hazırda kriptovalyuta bazarının təxminən yarısını tutur [1]. Onun tarixi 31 oktyabr 2008-ci il Mərkəzi Avropa vaxtı ilə 8.10-da Satoşi Nakamoto adı ilə göndərilmiş aşağıdakı cümlə ilə başlayan bir qısa məlumatla başlayıb: “Mən tamamilə birrəqlı olan və etibarlı üçüncü tərəflərin iştirakını nəzərdə tutmayan elektron pul sistemi yaratmışam.” Məlumatda Bitcoinin texniki təsviri olan doqquz səhifəlik “Peer to peer electronic cash system” adlı “ağ məqalə”yə link yerləşdirilmişdi.

“Ağ məqalə” çıxdıqdan üç ay sonra Bitcoin proqram-kliyəntinin ilk versiyası işə salınmışdı. 3 yanvar 2009-cu ildə

ilk 50 bitcoin “generasiya” edildi, üç gün sonra isə ilk bitcoin tranzaksiyası həyata keçirildi – Satoşi Nakamoto kriptovalyuta aktivisti Hel Finniyə 10 bitcoin göndərdi. Həmin ilin oktyabrında bitcoin ilk dəfə milli pula dəyişdirildi. 1 dolları 1309 bitcoinə dəyişdirmişdilər. Qiyməti sərf olunan elektrik enerjisinin dəyəri əsasında müəyyən etmişdilər. 2010-cu ilin mayında ilk dəfə bitcoinə mal alınmışdı – 10 min bitcoinə 2 pizza sifariş edilmişdi (çatdırılmaqla). Bitcoin tədricən populyarlaşmağa başladı və 2011-ci ildə ilk kriptovalyuta birjası yaradıldı [2].

Bitcoin blokçeyn şəbəkəsinin əsas xüsusiyyətlərindən biri tamamilə demərkəzləşmiş olmasıdır – hər hansı bir mərkəzi idarəetmə orqanı yoxdur. Bu ödəniş sisteminin əsas elementi açıq kodlu proqram kliyəntdir. Proqram-kliyəntlərin işlədiyi kompüterlər öz aralarında piring (Peer to peer, P2P) şəbəkəsində birləşirlər, burada bütün qovşaqlar bərabər hüquqludurlar. İki tərəf arasında elektron ödəniş vasitəçilər olmadan həyata keçirilir və geriye dönüşməzdir, yəni təsdiqlənmiş əməliyyatı ləğv etmək mexanizmi yoxdur.

Bitcoin sisteminin ilkin kodu elə proqramlaşdırılıb ki, sistemdə olacaq bitcoinlərin maksimal sayı əvvəlcədən məlumdur (21 milyon bitcoin). Təkcə bitcoinlərin maksimal sayı deyil, emissiya dinamikası da (yeni bitcoinlərin buraxılışı) da proqramlaşdırılıb. Bu bitcoinləri öz kompüter avadanlığını Bitcoin şəbəkəsində hesablamalar üçün istifadə edənlər əldə edirlər (“çıxarırlar”).

Blokçeyn. Hər bir elektron ödəniş sistemi tranzaksiyaları haradasa saxlamalıdır. Bitcoində bütün informasiya blokların zəncirində - blokçeyndə (ing. blockchain) saxlanır. Bloklar JSON formatında ötürülür. Hər bir blokda başlıq və tranzaksiyaların siyahısı olur. Başlıqda bir neçə məlumat, o cümlədən blokun sıra nömrəsi, başlığın heşi və əvvəlki blokun heşi olur. Beləliklə, blokçeyndə Bitcoinin mövcudluğu müddətində həyata keçirilmiş bütün tranzaksiyalar saxlanır.

Bloku yaratmaq üçün mayner bloka yazılmağa növbə gözləyən tranzaksiyalar siyahısından tranzaksiyaları seçir (əlbəttə, üstünlüyü tranzaksiya haqqı yüksək olanlara verir). Sonra blok başlığının heşi hesablanır, heşin qiyməti başlıqda verilmiş hədəf qiymətindən kiçik olmalıdır (“çətinlik” parametri). Başlıqdakı nonce sahəsindəki ədəd 0-dan başlayaraq hər iterasiyada o vaxtadək artırılır ki, başlığın heşi hədəf qiymətdən kiçik olsun. Adətən, bu xassəni ödəyən heşin tapılması böyük hesablamalar tələb edir. Hədəf qiymət nə

qədər kiçikdirsə, şərtin ödənməsi ehtimalı da bir o qədər kiçikdir.

Çətinlik dedikdə, bir həqiqi blokun axtarışı üçün hesablanmış heşlərin orta sayı nəzərdə tutulur. Bu qiymət hər 2016 blokdan sonra (təxminən 2 həftə) yenidən hesablanır ki, bloklar arasındakı interval 10 dəqiqə təmin olunsun.

Mayning yeni sikkələrin mədəndən çıxarılmasıdır, blokçeynə yazılacaq yeni bloku tapan mayner mükafat olaraq nəzərdə tutulmuş sayda bitcoin alır.

Bir blokun mayninginə təxminən 10 dəqiqə gedir. Hər 10 dəqiqədən bir 12,5 yeni bitcoin buraxılır, onu bu bloku tapan, yəni son 10 dəqiqədə olan tranzaksiyaların blokunu yaradan alır. Bu emissiya bitcoin protokolunda nəzərdə tutulub və hər 4 ildən sonra 2 dəfə azalır.

2016-cı ilin iyununa kimi hər 10 dəqiqədən sonra 25 bitcoin buraxılırdı, hazırda 12,5 bitcoin buraxılır və 2020-ci ilə kimi belə davam edəcək. Sonra 2024-cü ilə kimi 6,25 bitcoin buraxılacaq və s. Hazırda dövriyyədə 16-17 milyon bitcoin var. İlk hesablamalara görə, 2140-cı ilə kimi 21 milyon bitcoin buraxılacaq.

Qeyd edək ki, Bitcoinə mayningin çətinliyi tədricən artırılır və bloka görə mükafat azalır. İlk dövrlər mayning üçün fərdi kompüterlərin mərkəzi prosessorları kifayət edirdi. Sonra GPU əsasında, FPGA əsasında və nəhayət, ASIC əsasında mayning fermaları meydana çıxdı. ASIC (Application-Specific Integrated Circuit) – konkret məsələnin həlli üçün xüsusi inteqral sxemdir. Hazırda istehsalçılar tərəfindən mayning üçün müxtəlif ASIC həlləri təqdim olunur. Güman olunur ki, ən böyük mayning fermaları, Çin, İslandiya, Gürcüstan və Amerikadadır. Ən böyük 6 mayning hovuzu Çində yerləşir və dünyada bitcoinlərin yarısından çoxu da orada çıxarılır.

Konsensus algoritmi. Kriptovalyuta şəbəkəsinin bütün qovşaqları eyni hüquqludursa, onda eyni anda iki blok tapılıqda hansı blokun düzgün hesab edilməsi və şəbəkəyə əlavə edilməsi zamanı qeyri-müəyyənlik yaranır. Bundan qaçmaq üçün qərar qəbul etmə mexanizmləri təklif olunub. Bitcoin və digər şəbəkələrdə PoW (Proof-of-work, işin isbatı) algoritmi istifadə edilir, burada ən böyük hesablama gücünə malik qovşağın düzgün bloku tapmaq şansı ən yüksəkdir; PoS (Proof-of-stake, hissənin isbatı) algoritmində hesabında daha çox kriptovalyutaya olan qovşağın “çəkisi” daha böyükdür; dPoS (delegated PoS) algoritmində səlahiyyət şəbəkənin bütün iştirakçıları tərəfindən ümumi səsvermə ilə seçilən müəyyən sayda qovşağa verilir.

Kriptobirjalar. Kriptovalyutaya tələbin artması ilə paralel olaraq 2011-ci ildən onların mübadiləsi üçün onlayn birjalar yaranmağa başladı. Bu birjalar xüsusiyyətinə görə əsasən 2 yerə bölünür: 1) Kriptovalyutanın real valyutaya mübadilə edildiyi birjalar; 2) Bitcoinlərin digər kriptovalyutalara mübadilə edildiyi birjalar.

İlk bitcoin birjası MtGox 2011-ci ilin martında işə salınırdı. İlk dövrlər 1 bitcoin 5-6 sent idi, yarımildən sonra 10 dəfə artmışdı. Birja fəaliyyəti dövründə bir neçə dəfə hakerlər tərəfindən sındırılmışdı. 2014-cü ildə siyasi və iqtisadi səbəblərdən birja öz varlığını sonlandırmışdır.

Hazırda kriptovalyutaların alqı-satqısı ilə məşğul olan onlarla böyük birja vardır: Binance, Bitfinex, Livecoin, Poloniex, Btc-e, Bittrex, BtcChina və s.

III. KRIPTOVALYUTALARDA HARDFORK VƏ SOFTFORK

Bitcoinin ilkin kodu açıqdır və istənilən şəxs onun zəif yerlərini tapa və təkmilləşdirə, yəni fork yarada bilər.

Fork (ing. «cəngəl») – proqram təminatında məhsulun hər biri müstəqil inkişaf etdirilən bir neçə paralel budağa ayrılmasıdır və ya çoxdan mövcud olanın əsasında yeni məhsulun buraxılmasıdır. Məsələn, Xiaomi-nin MIUI sistemi forkdur, Android ƏS-nə əsaslanır, lakin ondan asılı olmadan inkişaf etdirilir.

Kriptovalyuta sahəsində fork – blok-zəncir sisteminin proqram koduna dəyişikliklərin edilməsidir, nəticədə sistemin iş qaydaları dəyişir. Bu hadisəni iki tipə ayırmaq olar: hardfork və softfork. Terminlərin kökü aparat və proqram təminatı mənasını verən sözlərdən deyil, «hard» və «soft» ingilis sözlərinin ilkin mənasından yaranıb.

Softfork – kriptovalyutanın proqram kodunun «yumşaq» dəyişdirilməsi prosesidir, onun gedişində blokçeyn şəbəkəsində işləyən maşınların proqram təminatının tam dəyişməsi tələb edilmir. Softfork zamanı edilən dəyişikliklər ona qədər yaradılmış verilənlərlə uyurluq saxlayır, lakin yeni verilənlərin yaranması prosesi dəyişir. Zəruriyyət yarandıqda softforku asanlıqla ləğv etmək olar.

Kriptovalyutada softforkun aparılmasının səbəbi, adətən, onun əsaslarına toxunmadan təkmilləşdirilməsi, aşkarlanmış hansısa nöqsanların aradan qaldırılması ehtiyacı olur. Bitcoin-də belə ehtiyac blokun həcmi artan tranzaksiyaları sürətlə emal etməyə imkan verməməsi səbəbindən yaranmışdı. Problemin həlli kimi Bitcoin Core komandası verilənlərin həcmi optimallaşdıran SegWit protokolunun tətbiqini seçmişdi.

Hardfork proqram koduna «sərt» dəyişiklik edilməsidir, bundan sonra köhnə proqram təminatı ilə uyurluq itir. Faktiki olaraq, hardfork gedişində əvvəlkindən fərqli, tamamilə yeni prinsip ilə işləyən yeni kriptovalyuta yaradılır. Softfork zamanı şəbəkənin proqram təminatı yenilənmiş qovşaqları köhnə proqram təminatı ilə işləyən qovşaqlarla qarşılıqlı əlaqə saxlaya bilərlərsə, hardfork zamanı köhnə şəbəkə ilə qarşılıqlı əlaqə tamamilə itir.

Hardforkun səbəbləri də softforkun səbəbləri ilə oxşardır, yaradıcıları kriptovalyutanın iş qaydalarına müvafiq dəyişikliklər etmək istəyirlər. Fərq odur ki, hardfork zamanı onlar mövcud sistemi yeniləmək yox, «blokçeyni və maynerləri ilə öz Bitcoin»ləri yaratmaq istəyirlər. Bitcoin üçün ən məşhur hardfork Bitcoin Cash hesab olunur. Yeni valyuta köhnədən blokun ölçüsünün 1 MB-dan 8 MB-a artırılması ilə fərqlənir. Bu tranzaksiyaları daha sürətlə yerinə yetirməyə imkan verir, lakin köhnə sistemlə uyurluq itir.

Aydın məsələdir ki, kriptovalyutalar sahəsində işlərin miqyası xeyli böyüyüb və forkların həyata keçirilməsi investisiyalar tələb edir.

ICO (Initial Coin Offering) – kriptovalyuta layihələri üçün investisiyaların cəlb edilməsi formasıdır. ICO təşəbbüskarı

investorlara tokenlər satır. Tokenlərin real dəyəri layihə birjaya çıxana qədər qeyri-müəyyən olur. Tokeni alan tərəf, yəni investorlar bu startap tokenini gələcəkdə ICO-da nəzərdə tutulmuş servisləri, xidmətləri və malları əldə etmək üçün istifadə edə bilirlər. Yaxud layihə birjaya çıxdıqdan və dəyəri artdıqdan sonra, dividendlər əldə edə və ya tokeni sata bilirlər.

İlk ICO 2013-cü ildə həyata keçirilmiş Mastercoin (hazırda Omni) olmuşdur. Təşəbbüskarlar 5 milyon dollar toplamağa nail olmuşdular. Sayca ikinci ICO ən uğurlarından biri oldu (NXT), 1 milyard token buraxılmışdı. 2017-ci ilin payızında isə kapitallaşma 70 milyon dollar təşkil edirdi. Ethereum üçün başlatılan ICO layihəsində 18 milyon dollar investisiya toplanmışdı.

IV. BITKOİNİN FORKLARI – ALTKOİNLƏR

Litecoin – uğurlu Bitcoin forklarından biridir. Bitkoinin nöqsanları əməliyyatların yavaş emalı və tranzaksiya haqlarının yüksək olmasıdır. 2011-ci ilin oktyabrında Charlie Lee bu nöqsanları aradan qaldırmaq üçün Litecoin təklif etdi. Litecoin - Scrypt heş alqoritmindən istifadə edir (Bitkoində SHA-256). Emissiya 84 milyon sikkə ilə məhdudlanıb, bu Bitkoinə 4 dəfə çoxdur. Bitkoinə analoji olaraq, rəqəmsal “gümüş” adlanır. Segwit və Lightning Network mexanizmlərinə ilk keçənlərdən biridir, bu blokda tranzaksiyaların sayını əhəmiyyətli dərəcədə artırmağa və tranzaksiyanın təsdiqlənməsi vaxtını azaltmağa imkan vermişdir.

Litecoin-in mayninqi Bitkoinə daha mürəkkəbdir. Vacib və əsas fərq odur ki, Scrypt operativ yaddaşdan intensiv istifadə edir. Bu halda Litecoin üçün ASIC-maynerlərin yaradılması məqsədəuyğun deyil və məhz buna görə də Litecoin mayninqi üçün ənənəvi videokartlar geniş istifadə edilir.

Ethereum (Efirium, efir) – əsas protokolu 2013-cü ildə rus əsilli kanadalı proqramçı Vitalik Buterin tərəfindən işlənmişdi, şəbəkə isə 30 iyul 2015-ci ildə işə salınmışdı. Ethereum-un əsas ideyası blokçeynin funksional imkanlarının genişləndirilməsi idi.

İlk baxışda Ethereum da Bitkoinə oxşayır, onun kimi paylanmış açıq şəbəkədir, burada da tranzaksiyalar edilir və bloka yazılır, onları da dəyişmək mümkün deyil. Lakin onların arasında bəzi əhəmiyyətli texniki fərqlər var, daha vacib fərq onların təyinat və imkanlarında olan fərqlərdir.

Bitkoin – blokçeyn texnologiyasının konkret bir tətbiqidir, elektron ödəniş sisteminin reallaşdırılmasıdır. Lakin blokçeyn texnologiyasının imkanları daha genişdir və Bitkoin-də bu imkanların kiçik bir hissəsi reallaşdırılıb. Ethereum-un yaradılmasının əsas hərəkətverici ideyası tranzaksiyanın – kriptovalyuta protokolunun əsas vahidinin smart-kontraktla əvəz edilməsidir. Smart-kontrakt daxilində təkə pul vahidinin bir hesabdan digərinə keçirilməsini deyil, istifadəçilər arasında qarşılıqlı əlaqənin daha geniş məntiqini və şərtlərini təsvir etmək olar.

Smart-kontrakt elektron alqoritm və yaşərtdir, onun yerinə yetirilməsi zamanı tərəflər pul, aksiya, daşınmaz əmsal və ya digər aktivləri mübadilədə bilirlər. Maliyyə aləti kimi kriptovalyuta istifadə edilir. Blokçeyn texnologiyasının

hesabına smart-kontraktlar paylanmış reyestrə saxlanır və tərəflərdən heç birinin onu dəyişmək imkanı yoxdur.

Smart-kontraktlar banklar, notariuslar, hüquqşünaslar və s. kimi vasitəçilərdən yan keçməyə imkan verir, çünki onlar alqı-satqının şərtlərini özləri müstəqil yoxlayırlar və təsdiqləyirlər. Ethereum yaradıcısı smart-kontraktların işini belə izah edir. Əvvəlcə aktiv və ya valyuta proqrama köçürülür. Bundan sonra proqram kontraktın yerinə yetirilməsini izləməyə başlayır. Şərtlər yerinə yetirilən kimi tərəflər aktivləri mübadilə edirlər. Satıcı müəyyən edilmiş məbləği, alıcı isə malı alır.

Ethereum həmçinin demərkəzləşmiş avtonom təşkilatların (Decentralized Autonomous Organization, DAO) yaradılması üçün də istifadə edilə bilər. DAO – Ethereum blokçeynində yazılmış smart-kontraktların köməyi ilə idarə edilən, vahid lideri olmayan, tam avtonom demərkəzləşmiş təşkilatdır. Burada proqram kodu ənənəvi təşkilatın strukturunu və qaydalarını əvəz edir, mərkəzləşdirilmiş insan nəzarətinin zəruriliyini aradan qaldırır. DAO tokenləri alanların hamısına məxsusdur, lakin burada token aksiyaların hissə və ya paketi deyil, səs hüququ üçün ödənişdir.

Ripple – öz xarakteristikalarına görə kriptovalyuta tərifinə tam uyğun gəlmir – onda blokçeyn yoxdur. Emissiya 100 milyard sikkə olmaqla bir dəfəyə edilmişdi, onun 55 milyardı dərhal dövriyyəyə daxil edilmişdi, qalanı isə hər ay 1 milyard sikkə olmaqla smart-kontraktlar vasitəsilə çıxarıldı. Yaradıcılarının məqsədi komissiya haqları minimal və tranzaksiya sürəti dəfələrlə böyük olmaqla SWIFT sisteminə rəqib yaratmaq idi. Buna müəyyən dərəcədə nail olmalarını Bank of America, Unicredit, BNP Paribas və s. kimi məşhur bankların Ripple infrastrukturuna qoşulması təsdiqləyir.

Bitcoin Cash – Bitkoin şəbəkəsinin ən məşhur və uğurlu hardforklarından biridir, 1 avqust 2017-ci ildə meydana çıxıb. Hardforkun məqsədi şəbəkənin miqyaslanması, buraxma qabiliyyətinin artırılması və tranzaksiya haqqının azaldılması problemlərinin həlli idi. Blokun həcmi 32 Mbayta kimi artırmaq imkanı olmaqla əvvəlcə 2 Mbayt olması barədə qərar qəbul edilmişdi.

Zcash – Bitkoin-dən daha təhlükəsiz olmağı iddia edən başqa virtual valyutadır. Zcash saytında deyilir ki, "Bitkoin valyuta üçün http istifadə edir, Zcash isə https - təhlükəsiz nəqliyyat qatını". Bu kriptovalyuta sıfır məlumat adlanan şifrələmədən istifadə edir. Yəni şifrələnmiş informasiya açıq informasiya haqqında heç bir məlumat vermir.

Dash – Bitkoinin forklarından biridir, 2014-cü ildə bazara çıxıb. Digər altkoinlər kimi, dash da bitkoini təkmilləşdirmək ideyası ilə yaradılıb (Evan Daffild). Təşəkkül prosesində üç ad dəyişib: əvvəlcə Xcoin, sonra DarkCoin adlanırdı, 2015-ci ildən indiki adını alıb.

Dash da Bitkoinin müəyyən problemlərini həll edir, əgər Bitkoin bərabər hüquqlu qovşaqların bərabərliyi şəbəkəsidirsə, Dash ikranlıq arxitektura malikdir. Birinci səviyyə Bitkoinə oxşayır, burada mayninq vasitəsilə sikkələr buraxılır və yeni bloklar blokçeynə yazılır. İkinci səviyyədə Masternodlar (əsas qovşaqlar) işləyir.

Masternodlar – kriptovalyutanın bütün blokçeyninin saxlandığı qovşaqlardır, şəbəkənin iş qabiliyyətinin dəstəklənməsi üçün bir sıra vacib funksiyalar, o cümlədən, InstantSend, PrivateSend və DAO servislərini yerinə yetirirlər.

PrivateSend – bu mexanizm ödənişlərin anonimliyini təmin etmək üçün yaradılıb (Daffildin fikrincə, Bitkoin anonimliyi təmin etmir). Ödəniş bərabər hissələrə bölünür, masternodlar vasitəsilə qarışdırılır və alan tərəfə göndərilir. Beləliklə, “izlər itirilir” və zamanla ödənişin mənbəyini müəyyən etmək mümkün olmur. Bu mexanizmi yalnız Dash Core pulqabıları dəstəkləyir.

InstantSend – ani tranzaksiyalar üçün nəzərdə tutulmuş xidmətdir. Tranzaksiya bir neçə saniyədə emal edilir. Bu belə işləyir: müştəri ödəniş edir, tranzaksiya 7-10 təsadüfi masternoda göndərilir. Masternodlar təkrar istifadəsinin qarşısını almaq üçün tranzaksiya girişlərini təxminən bir saatlığa bağlayırlar. Tranzaksiyanın təsdiqlənməsi 1-3 saniyə çəkir.

V. STABİL KRİPTOVALYUTALAR – STEYBLKOİNLƏR

Kriptovalyutaların volatilliyi çox yüksəkdir, bu onları spekyulantlar üçün cəlbədicə və geniş istifadə üçün yararsız edir. İdeal kriptovalyuta öz alıcılıq qabiliyyəti baxımından stabilliyini saxlamalı, yaxud kiçik inflyasiyaya məruz qalmalıdır. Belə ideal kriptovalyuta steyblkoin adlanır. Ən sadə formada steyblkoin fiat valyutasında stabil dəyəri olan adi kriptovalyutadır.

İlk dəfə “stabil kriptovalyuta” ideyasını 2012-ci ildə Mastercoin komandası irəli sürmüşdü. Bundan sonra yevro və ya yuan əsasında steyblkoin yaratmağa bir neçə cəhd edilmişdi. Lakin steyblkoin ideyasını yalnız üç il sonra uğurla reallaşdırmaq mümkün oldu. Həmin vaxt bazara dollara bağlanmış məşhur Tether çıxdı.

Steyblkoinlərin stabilliyinə təminat ilə nail olurlar. Onların əksəriyyətinə valyutalar və qiymətli metallar, kriptovalyutalar, neft, brilyant kimi aktivlərlə təminat verilir.

Hazırda bazarda steyblkoinlərin üç növü təmsil olur:

1. “Fiat”la təminat olunmuş (ing. fiat-collateralized);
2. Kriptovalyuta ilə təminat olunmuş (ing. crypto-collateralized);
3. Təminat olunmamış (ing. non-collateralized).

Fiat valyuta ilə təminat olunma – steyblkoinlərin yaradılmasının ən sadə üsuludur. Mahiyyətə bu girov öhdəliyidir. Müəyyən miqdarda fiat valyuta təminat kimi qoyulur və bu valyutaya 1:1 nisbətində steyblkoin buraxılır. Bu metod sadə və etibarlıdır, lakin steyblkoinlərin buraxılması və geriə mübadilə edilməsi üçün üçüncü tərəfin iştirakını tələb edir. Üçüncü tərəfin fəaliyyətinə nəzarət etmək və müntəzəm auditlər aparmaq lazım gəlir. Aydındır ki, fiat valyutası əvəzinə digər aktivlər də, məsələn, qızıl, gümüş və ya neft də istifadə edilə bilər.

İkinci metod – kriptovalyutalarla təminat da əvvəlki metoda oxşayır, lakin bu halda steyblkoin ənənəvi aktivlərlə deyil,

kriptoaktivlərlə təminat edilir. Kriptovalyutaların volatilliyi nəzərə alınaraq, bu steyblkoinlər çox zaman ehtiyat ilə təminat olunurlar. Yəni 100 \$ məbləğində steyblkoin buraxmaq üçün təminat vermək lazımdır – məsələn, ETH ilə 200 \$ məbləğində təminat yaratmaq lazımdır. Beləliklə, əgər hətta baza aktivinin qiyməti 20 % düşsə də, steyblkoin öz dəyərini saxlayacaq. Lakin təminatçı aktivini dəyərsizləşdirən görünməmiş hadisə «qara qu quşu» hadisəsi baş versə, steyblkoin də dəyərini itirəcək və təminatçı daha böyük zərəmə düşəcək, çünki steyblkoinlər izafi ehtiyatla təminat olunurlar. Məhz buna görə bəzi ekspertlər belə yanaşmanın əleyhinə çıxış edirlər.

Təminat olunmamış steyblkoinlərin stabilliyi senyoraj hesabına təminat olunur. **Senyoraj** – pul emissiyası hesabına yaranan gəlirdir və emitent tərəfindən mənimsənilir. Pul kütləsinin artımından gəlir götürən dövlətlər senyorajdan geniş istifadə edirlər.

Steyblkoin kursunu bir səviyyədə saxlamaq üçün emitentlərin onun təklif olunan həcmi smart-kontraktların köməyi ilə nəzarət edirlər. Bu zaman kriptovalyuta sahibləri gələcək senyorajda pay aksiyaları əldə edirlər. Bu konsepsiya “seigniorage shares” adını almışdır. Onu 2014-cü ildə Robert Sems təklif etmişdir və Basecoin və Havven kimi layihələr ona əsaslanır.

Steyblkoinlərin yaradılması ilə bağlı bir sıra layihələr var, onlardan ən populyarlarını göstərək.

Tether – qiyməti dollar kursuna 1:1 nisbətində bağlı olan steyblkoinidir – mübadilə zamanı 1 USDT 1 dollara uyğundur. Dövrriyədəki hər bir USDT 1 dollar ilə təminat olunur, o, mərkəzləşmiş idarə olunan əmanət hesabında saxlanır.

MakerDAO – demərkəzləşmiş avtonom təşkilatdır, onun valyutası ABŞ dollarına bağlıdır, lakin ETH ilə tam təminat olunur. Hər bir Dai 1 dollara uyğundur. Qiymətin stabilliyi avtonom smart-kontrakt sisteminin köməyi ilə dəstəklənir.

Basecoin – ABŞ dollarına bağlıdır, qiyməti 1 dollara uyğundur, lakin təminat olunmamış steyblkoinidir. Koin buraxılışının artırılması və ya azaldılması haqqında qərar konsensus əsasında qəbul edilir.

TrueUSD – ABŞ dollarına bağlı, 100 % təminat olunmuş steyblkoin yaratmaq cəhdidir. Layihə Tether-ə oxşardır, lakin qanunla qorunur, şəffafdır və yoxlanılıb. TrueCoin komandası Cooley və Arnold & Porter birlikdə təminat olunmuş kriptovalyutalar üçün hüquqi sistem işləyib hazırlamışdır. Onlar həmçinin normativ-hüquqi uyğunluq və bank xidməti üzrə qəyyumlar və mütəxəssislər şəbəkəsini də inkişaf etdirirlər.

VI. KRİPTOVALYUTALARDA BƏZİ TEXNOLOJİ HƏLLƏR

Blokçeynin ən vacib göstəriciləri miqyaslama, təhlükəsizlik və demərkəzləşmədir, lakin burada bəzi problemlər var.

Blokçeynlə əlaqəli əsas problemlərdən biri informasiyanın şəbəkədə iştirak edən hər bir sistemdə kopyalanmasıdır. Hazırda bitkoin üçün fərdi kompüterə kopyalanan bloklar 200 qiqabaytdan çox yer tutur. Mərkəzləşmə olmadığından istifadəçilər böyük həcmdə informasiyanı kopyalamağa

məcburdurlar. Lakin belə yanaşma dələduzluğun və şəbəkənin sahibləri (və ya idarəçiləri) tərəfindən informasiyanın saxtalaşdırılmasının qarşısını alır.

Ethereum kriptovalyuta şəbəkəsində tranzaksiyaların təsdiqlənməsi sürətini artırmaq üçün “şardinq” texnologiyasından istifadə etməyə cəhd edir. Şardinq – blokçeyn şəbəkəsinin tranzaksiyaları paralel emal edə bilən bir neçə kiçik çəbəkə komponentlərinə (“şard”lara) bölünməsinə nəzərdə tutur. Bu şəbəkənin buraxma qabiliyyətini artırmağın və Visa və Mastercard-da olduğu kimi saniyədə minlərlə tranzaksiya emal etməyin metodlarından biri ola bilər.

Bitcoin blokçeyn şəbəkəsində isə tranzaksiyaların təsdiqlənməsi sürətini artırmaq üçün Lightning Network (LN) ideyasından istifadə etməyə hazırlaşır. LN-in ideyası ondan ibarətdir ki, tranzaksiyaların hamısı blokçeynə yazılmamalıdır. Təsəvvür edin ki, biz sizinlə öz aramızda sisteməlik olaraq bir neçə tranzaksiya edirik. Bu halda tranzaksiyaları qeydə almaq və onlar zəncirdən çıxarmaq olar.

Sadə dillə izah olunsaydı, bu belə işləyir: biz öz aramızda ödəniş kanalı açıyıq və onun açılmasını blokçeyndə yazırıq. Bundan sonra tranzaksiyaları bu ödəniş kanalı ilə edərək və kanalı lazım olduğu müddətdə açıq saxlaya bilərik (hətta on illərlə). Biz yalnız kanalı bağladıqda blokçeynə qayıdırıq və məhz bu zaman kanal ilə yerinə yetirilmiş tranzaksiyaların son vəziyyətini blokçeynə yazırıq. İstənilən sayda ödəniş kanalları yaratmaq və blokçeyndə tranzaksiyaları minimuma qədər azaltmaq olar.

LN Bitcoin şəbəkəsi üzərində “ikinci səviyyə şəbəkəsidir”, blokçeyn şəbəkəsi yükünü artırmadan tranzaksiya axınına istənilən dəfə artırmağa imkan verir (nəzəri olaraq). Bu o deməkdir ki, bunun sayəsində Bitcoin maynerlərin elektrik enerjisini artırmadan öz buraxma qabiliyyətini artırmaqla olar.

PoW tranzaksiyaların blokçeyndə təsdiq olunmasının yeganə üsulu deyil. Bir neçə digər metod da vardır, onlardan ən ümidverici “proof-of-stake” (POS) – “hissə ilə isbat” adlanır. Onun əsas üstünlüyü ondadır ki, o hesablamalardan imtina etməyə imkan verir.

Yanaşmanın mahiyyəti belədir. POS metodu ilə işləyən maynerlər hesablama maşınlarının gücü ilə deyil, öz pulqabıllarının ölçüləri ilə yarışirlar. Bitcoinə tətbiq etdikdə bu təxminən belə olacaq. Maynerlər əvvəlki kimi sadə iştirakçılardan tranzaksiyaları toplamalı və onların düzgünlüyünü yoxlamalıdır. Blokçeynə yazmaq hüququ isə hər 10 dəqiqədən bir püşklə müəyyən edilir – uduş ehtimalı maynerin hesabında olan məbləğə düz mütənasibdir. Beləliklə, bitcoin pulqabınızda nə qədər çox pul varsa, növbəti bloku blokçeynə yazmaq hüququnu sizin alacağınız ehtimalı bir o qədər böyükdür. Ümumiyyətlə, heç bir hesablama tələb edilmir, buna görə əvvəlcə hesablamalara, sonra isə soyutmaya kilovattlarla enerji xərcləmək lazım gəlmir.

PoS sxemi nəzəri baxımından əsaslı işləsə də, Bitcoin ölçüsündə olan heç bir blokçeyn sistemində praktiki reallaşdırılmayıb. PoS sxeminin təmiz şəkildə və ya hibrid reallaşdırdığı kriptovalyutalar olsa da (Bitcoin, Dark, BitShares, Blocknet və digərləri), onların heç biri yükünə və kapitalaşmasına görə Bitcoinlə müqayisə edilə bilməz.

PoS sxeminə bitcoin yox, Ethereum keçməyə hazırlaşır. Bəzi tədqiqatçılar bunu Ethereumun valideyninin (Bitcoin) kölgəsindən çıxmaq, özünün müstəqil, progressiv imicini təsdiqləmək üçün etdiyini söyləyirlər.

VII. KRİPTOVALYUTA VERİLƏNLƏRİNİN ANALIZI

İnternetdə bir sıra açıq (pulsuz) və ödənişli kriptovalyuta verilənləri mövcuddur:

- Bitcoin şəbəkəsində tranzaksiyaların və komissiyaların dinamikası;
- Kriptoaktivlərin və birjaların statistikası və reytingləri;
- ICO-trekerlər və Token Sale reytingləri;
- Bazar indeksləri;
- Kriptovalyutaların bazar kapitalaşması və s.

Əlbəttə, adi istifadəçiləri ən çox maraqlandıran məsələ bitcoin və digər kriptovalyuta kurslarının proqnozu məsələsidir. Qeyd edək ki, ən məşhur kriptovalyuta kimi Bitcoin kursunun proqnozu üçün bir çox analiz və tədqiqatlar aparılmışdır. İlk əvvəl, ezaman sıralarının analizi üçün nəzərdə tutulmuş aşağıdakı modellər tətbiq edilmişdir:

- ARIMA (Autoregressive Integrated Moving Average);
- ARCH (AutoRegressive Conditional Heteroskedasticity);
- GARCH (generalized ARCH).

Məsələn, [3]-də bitcoinlərin dəyişkənliyinin vaxtla əhəmiyyətli dərəcədə fərqləndiyini və bu əlaqənin T-GARCH (1.1) modelinin ən yaxşı şəkildə əks etdirildiyini təsbit edir. Bitcoin ilə real iqtisadiyyat göstəriciləri arasındakı əlaqələr zamanla uyğun olmayan və əsasən əhəmiyyətsiz olduğu qənaətinə gəlinir.

Uzun müddət, makro-maliyyə göstəriciləri Altcoinin qiymətinin bitcoin-dən daha az formalaşmasını müəyyənləşdirmişdir. Virtual valyuta təchizatı ekzogen olduğu üçün qiymətlərin formalaşmasında məhdud rol oynayır [4].

Bitcoin-in artan məşhurluğu və tacirlərin tanınması sayəsində, dəyər yaranmasına təsir göstərən amilləri anlamaq üçün gətirdikdə daha çox əhəmiyyət kəsb edir. Ən çox istifadə edilən kriptovalyutaların 66 hissəsini təhlil edən şifrəli empirik məlumatlardan istifadə edərək tənzimləmə modelinin kriptovalyuta dəyərinin üç əsas sürücüsünə istinad etdiyi qiymətləndirilmişdir [5]:

- istehsalçı şəbəkələrində rəqabət səviyyəsi,
- vahid istehsal nisbəti,
- kriptovalyuta üçün mayninq alqoritminin çətinliyi.

Bitcoin kimi kriptovalyutalar bir investisiya aktivinə kimi qururlar və özlərini tez-tez Yeni Qızıl adlanırlar. Lakin [6]-da aparılmış araşdırma göstərir ki, bu iki aktiv bir-birindən çox

fərqlənirlər. Birincisi, bitkoin və qızılın, eləcə də digər aktivlərin şərti dəyişiklik xassələri analiz və müqayisə edilir. İkincisi, zamana görə dəyişən şərti korrelyasiyaları qiymətləndirmək üçün BEKK-GARCH modeli tətbiq edilir. Nəticələr, göstərir ki, bitkoinin davranışı qızılın davranışının tam əksinədir.

Bitkoin üçün zaman əsaslı valyuta qiymətləndirmələri keçirilmişdir. Araşdırmanın nəticəsi olaraq, 10.01.2018 və 18.01.2018 tarixləri arasında neyron şəbəkələrinin MPL (6-3-1) modeli ilə təxmin edilən qiymətlərin istiqaməti və kəmiyyəti ARIMA (1.1.6) modelindən daha yaxşı olmuşdur [7].

[8]-də GARCH modelləri istifadə edilməklə bitkoinin maliyyə aktivliyi imkanları araşdırılır. İlk model qızıla və dollar müəyyən oxşarlıq göstərir, bitkoinin hedcinq imkanlarını və mübadilə vasitəsi kimi üstünlüklərini nümayiş etdirir. Asimmetrik GARCH göstərir ki, bitkoin riskin idarə edilməsində faydalı ola bilər, xüsusilə riskə meyl etməyən investorlar üçün idealdir. Ümumilikdə, bitkoinin maliyyə bazarlarında və portfel idarəçiliyində yeri var, çünki mübadilə vasitəsi üstünlüyü və dəyəri saxlama üstünlüyü miqyasında qızıl və amerika dolları arasında təsnif edilə bilər.

[9]-də bitkoinin ABŞ dollarına nisbətən məzənnəsinin dəyişməsi statistik analiz edilir, maliyyədə ən məşhur 15 parametrik paylanma nəzərdən keçirilir. Ümumiləşdirilmiş hiperbolik paylanmanın daha yaxşı nəticə verdiyi göstərilir. Valyuta məzənnəsinin gələcək qiymətləri üçün proqnozlar verilir.

Tədqiqatların ikinci istiqaməti kimi maşın təlimi metodlarının, xüsusilə neyron şəbəkələrinin tətbiqini ayırmaq olar. [10]-də neyron şəbəkəsi istifadə edilərək bitkoinin bir gün əvvəlki qiyməti və həcmi əsasında meyl proqnoz edilir.

Məlumdur ki, maşın təlimi metodlarından dərin təlim arxitekturaları şəkil və mətnlərin tanınması sahəsində yüksək nəticələr göstərmişdir, lakin maliyyə sahəsində çox istifadə edilmir. [11]-də cari qiymətə görə növbəti dövrün qiymətinin istiqamətini proqnozlaşdırmaq üçün konvolyusiya neyron şəbəkələri (Convolutional Neural Network, CNN) istifadə edilir.

Bayes optimallaşdırılmış rekurrent neyron şəbəkəsi (recurrent neural network, RNN) və uzun-qısamüddətli yaddaş (Long Short Term Memory, LSTM) şəbəkəsi bitkoin qiymətinin proqnozlaşdırılmasına tətbiq edilir. Zaman sıralarının proqnozlaşdırılması üçün məşhur ARIMA modeli dərin öyrənmə modelləri ilə müqayisə edilir. Gözlənilməli kimi, qeyri-xətti olan dərin öyrənmə metodlarının xətası ARIMA proqnozuna nisbətən çox azdır [12].

Kriptovalyutaların qiymətlərinin proqnozlaşdırılması üçün [13]-də ARIMA modeli ilə təkrarlanan dərin çoxlaylı neyron şəbəkəsi (seq2seq) müqayisə edilir.

NƏTİCƏ

Kriptovalyutalar son bir neçə ildə meydana çıxsa da, informasiya texnologiyalarında və maliyyə texnologiyalarında

ən məşhur trendə çevrilmiş, dövriyyə həcmi milyardlarla ölçülən böyük bir ekosistem formalaşdırmağa nail olmuşdur. Bu ekosistemin mahiyyətini başa düşmək, əlaqədar sahələrdə baş verən dinamik dəyişikləri analiz etmək, gizli qanunauyğunluqları aşkarlamaq üçün kriptovalyutalarla əlaqəli verilənlərin intellektual analizi metodlarının işlənməsi vacibdir.

ƏDƏBİYYAT

- [1] N. Hətəmov, Bitcoin texnologiyasının elmi-nəzəri və praktiki problemləri, “İnformasiya təhlükəsizliyinin aktual problemləri” III respublika elmi-praktiki seminarının materialları, s.112-115, 2017.
- [2] A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, “Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press”, 2016.
- [3] J. Şafka, “Virtual currencies in real economy: Bitcoin”. Diploma thesis. 2014.
- [4] P. Ciaian, M. Rajcaniova, “Virtual relationships: Short-and long-run evidence from BitCoin and altcoin markets”, Journal of International Financial Markets, Institutions and Money, vol. 52, pp. 173-195, 2018.
- [5] A.S. Hayes “Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin” Telematics and Informatics, vol. 34(7), pp.1308-1321, 2017.
- [6] T. Klein, H.P. Thu, T. Walther, “Bitcoin is not the New Gold – A comparison of volatility, correlation, and portfolio performance” International Review of Financial Analysis, vol. 59, pp.105-116, 2018.
- [7] E.E. Şahini, “Kripto para bitcoin: ARIMA ve yapay sinir ağı ile fiyat tahmini” Fiscoeconomia, vol.2 (2), pp. 74-92, 2018.
- [8] A. H. Dyhrberg, “Bitcoin, gold and the dollar – A GARCH volatility analysis”. Finance Research Letters, vol.16, pp. 85-92, 2016.
- [9] J. Chu, S. Nadarajah and S. Chan, “Statistical analysis of the exchange rate of bitcoin”, PLoS one, vol. 10(7), e0133678, 2015.
- [10] J. Almeida, S. Tata, A. Moser and V. Smit, “Bitcoin prediction using ANN”, Neural networks, vol. 7, pp. 1-12, 2015.
- [11] A. Dingli and K. Fournier, “Financial time series forecasting – A deep learning approach”, International Journal of Machine Learning and Computing, vol. 7, pp. 118-122, 2017.
- [12] S. McNally, J. Roche and S. Caton, “Predicting the price of Bitcoin using Machine Learning”, 26th Euromicro International Conf. Parallel, Distributed and Network-based Processing, pp. 339-343, March 2018.
- [13] J. Rebane, I. Karlsson, S. Denic and P. Papapetrou, “Seq2Seq RNNs and ARIMA models for cryptocurrency prediction: A comparative study”, 2018.

ISSUES OF MINING CRYPTOCURRENCY DATA

Yadigar İmamverdiyev, Firəngiz Sadiyeva

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

Baku, Azerbaijan

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

Abstract – Cryptocurrencies are the phenomenon that has emerged over the last few years and promises revolutionary changes in the financial sector. Blockchain technology based on most cryptocurrencies can also cause noticeable changes in other areas of activity. The article gives a brief overview of cryptocurrency technologies, some of the technological solutions that are on the agenda in this area are highlighted and analytical methods of cryptocurrency data are analyzed.

Keywords – cryptocurrency; Bitcoin; blockchain; hardfork; softfork; altcoin; stable coin; Ethereum; data mining

Rəqəmli təsvirlərin watershed üsulu ilə segmentləşdirilməsi

Ababil Nağıyeva¹, Sakit Verdiyev²

Azərbaycan Texnologiya Universiteti, Gəncə, Azərbaycan

¹nagiyevaababil@gmail.com, ²info_tel@inbox.ru

Xülasə-Segmentləşmə təsvirlərin işlənməsində rəqəmli təsvirin bir neçə seqmentə bölünməsidir. Bu məqalədə rəngli təsvirlərin kompüter tərəfindən tanınması və yaxud rəqəmli təsvirin konteyner kimi istifadəsinin effektivliyini artırmaq məqsədi ilə emal üsullarından biri olan segmentləşdirilmənin müxtəlif texnikaları barədə məlumat verilir, konkret şəkildə suayırıcı (watershed) üsulunun xüsusiyyətləri və matlapda işləmə metodikası verilib. Nümunə kimi rəngli, rəqəmsal təsvirin Qrادیyent üsulu ilə segmentləşdirilməsi verilib. Nəticə kimi göstərilir ki, həddən artıq segmentləşdirilmə effektinin mövcudluğu bu üsulun çatışmazlıqlarına aiddir və yeni, daha kamil üsulun işlənməsinə ehtiyac vardır.

Açar sözlər: rəqəmli təsvir, segmentləşdirilmə, watershed, qrادیyent, piksel koordinatları.

I. GİRİŞ

Yüksək texnologiyaların inkişaf edərək gündəlik həyatımızın hər bir sahəsinə daxil olduğu dövrdə rəqəmli təsvirlərdən də geniş istifadə olunur. Bu isə öz növbəsində informasiyanın istər korporativ, istər hərbi səviyyədə təhlükəsiz, qorunmuş halda dövriyyəsinin təmin edilməsini tələb edir və təsvir verilənlərinin icazəsi olmayan istifadəçilərdən mühafizə olma üsullarının işlənməsini aktual edir. Bu üsullar o dərəcədə etibarlı olmalıdır ki, ötürülməli olan orijinal verilənlər istənilən haker, həmçinin server administratoru üçün əlçatan olmasın [1].

Təsvirlərin analizi zamanı onların piksellərinin müəyyən əlamətlərinə görə qruplaşdırılmasıdır. Ayırı-ayrı qruplar isə seqment adlanır. İki növ qruplaşma (segmentləşdirmə) məlumdu: binar təsvirlər üçün parlaqlıqlarına görə və rəngli təsvirlərdə rəng koordinatlarına görə. Əlamətlər məkanında hər bir pikselin koordinatlarını (x, y) və RGB komponentlərini seçmək olar. Seqmentlər bir birindən parlaqlıq, rəng, tekstura, forma və digər əlamətlər ilə fərqlənirlər. Seqmentləşdirilmənin məqsədi təsvirin sadələşməsi. Bu ona görə edilir ki, təsvir emal və analiz edilə bilsin. Seqmentlərin düzgün seçilməsi təsvirin tanınmasının keyfiyyətinə təsir edir [2].

II. SEQMENTLƏŞDİRMƏ

Rəqəmli təsvirlərin segmentləşdirilməsi onların eyni sahəyə məxsus piksellərini qruplaşdıraraq, təsvirdə olan müxtəlif obyektləri bir birindən seçmək və bunula yanaşı təsvirdə olan müxtəlif obyektlərin təsvirin arxa fonundan seçilməsi deməkdir. Daha aydın desək, rəqəmli təsvirin segmentləşdirilməsi, təsvirin kompüter tərəfindən tanınması və üzərində emal aparılacaq sahələrin müəyyənləşdirilməsidir.

Eyni obyektə məxsus piksellərin hər biri rəngin intensivliyi kimi bəzi xüsusiyyətlərə aiddir. Bitişik bölgələr xarakteristikalarına görə bir birindən əhəmiyyətli dərəcədə fərqlənə bilər. Seqmentləşdirmənin praktiki istifadəsinə aşağıdakıları aid etmək olar.

- İnsanın biometrik xüsusiyyətlərinin müəyyən edilməsi:
 - barmaq izinin tanınması;
 - təsvirdə üzün tanınması;
 - gözün qıçasının tanınması;
- Təsvirin steqoanalizi;
- Tibbi Görüntülərin emalı və s. [3].

Təsvirlərin segmentləşməsinin aparılması üçün təsvirdə olan piksellərin x və y oxları üzrə koordinatları müəyyən edilir. Daha sonra əldə olunan qiymətlərdən istifadə edərək Qrادیyent, Laplas və s. kimi riyazi əməliyyatların köməyi ilə təsvirlər segmentləşdirilir.

Təsvirlərin segmentləşdirilməsi üçün bir çox alqoritmlər mövcuddur. Bunlara k-ortalama, Suayırıcı (Watershed) alqoritmlərini və s. misal göstərə bilərik.

Qeyd etmək lazımdır ki, bir təsvir üçün istifadə olunan segmentləşdirmə üsulu digər bir təsvir üçün yararlı olmaya da bilər. Yəni elə bir universal segmentləşdirmə üsulu mövcud deyildir ki, o bütün təsvirlər üçün uğurlu nəticə versin.

Bu məqalədə segmentləşdirmədə geniş istifadə olunan Məsafə çevrilməsi və Qrادیyent üsulları nəzərdən keçirilərək, mövcud ədəbiyyatdan istifadə etməklə müqayisəli təhlil edilir. Misal kimi isə Qrادیyent üsulu nümunəsində işləmə metodikasına baxılır.

Məsafə çevrilməsi üsulunun segmentləşdirilməsi piksellərin Watershed xəttinə kimi olan məsafənin ölçülməsinə əsaslanır. Məsafə çevrilməsi təsvirində birinci şəkildəki xətlər Watershed xətləridir, ikinci şəkildə isə segmentləşdirilmə nəticəsində tədqiq edilməli olan ayırı-ayrı obyektlərin konturlarıdır. Digər çox effektiv işləyən yanaşma Qrادیyentlər vasitəsilə Watershed üzrə segmentləşdirilmədir (Şəkil 3,4).

Şəkil 1. Məsafə çevrilməsi üsulu ilə seqmentləşdirilmiş təsvir
 Şəkil 2. Şəkil 1-dəki təsvirin qradient üsulu ilə seqmentləşdirilmiş nümunəsi

Qradient üsulu ilə seqmentləşdirilmənin nümunəsi şəkil 3. və şəkil 4. də verilir

Şəkil 3. Qradient üsulu ilə seqmentləşdirilmiş təsvir
 Şəkil 4. Şəkil 3-dəki təsvirin qradient üsulu ilə seqmentləşdirilmiş nümunəsi

Göründüyü kimi 2-ci yanaşmada həddən artıq suayırıcı xəttlər yaranıb ki bu da çatışmazlıq kimi dəyərləndirilir. Buna baxmayaraq obyektlərin konturlarının müəyyən olunması daha yaxşı olur. Şəkildəki dairəvi xəttlər obyektlərin konturlarıdır.

Qradient üsulunun rəqəmli təsvirlərin emalındakı əhəmiyyətini qiymətləndirərək onun işlənmə metodologiyasını diqqətinizə çatdırırıq.

III. QRADİENT ÜSULU.

Təsvirin seqmentləşdirilməsinin aşağıdakı xüsusiyyətləri vardır

- Təsvirdə olan müxtəlif obyektlərin pikselləri bir biri ilə üst-üstə düşə bilməz $R_i \cap R_j = \emptyset, \forall i \neq j$
- Eyni obyektin pikselləri ortaq xüsusiyyətlərə malikdir $P(R_i) = TRUE$
- Qonşu obyektlərin fərqli xüsusiyyətləri vardır $P(R_i) \neq P(R_j), \forall R_i, R_j$ qonşudur [4].

Kənarların müəyyən olunması üçün törəmədən istifadə edərək gerçəkləşdirilən Qradient üsuluna baxaq.

Rəqəmli təsvirdə törəmə almaq üçün törəmənin tənliyi aşağıdakı kimi olacaq

$$\frac{df}{dx} = \lim_{h \rightarrow 0} \frac{f(x+h) - f(x)}{h}$$

$$\lim_{h \rightarrow 0} \frac{f(x) - f(x-h)}{h}, \lim_{h \rightarrow 0} \frac{f(x) - f(x-h)}{2h}$$

Təsvirlər ikiölçülü olduğundan aşağıdakı Qradient düsturlarından istifadə ediləcək.

$$\nabla f = \text{grad}(f) = \begin{bmatrix} g_x \\ g_y \end{bmatrix} = \begin{bmatrix} \frac{\partial f}{\partial x} \\ \frac{\partial f}{\partial y} \end{bmatrix}$$

(Qradientin genişliyi düsturu)

$$M(x, y) = \text{mag}(\nabla f) = \sqrt{g_x^2 + g_y^2}$$

$$(\text{Qradientin istiqaməti}) a(x, y) = \tan^{-1} \left[\frac{g_x}{g_y} \right]$$

kənarın yönü $\phi = \alpha - 90^\circ$

Qradientin genişliyi praktikada aşağıdakı şəkildə hesablanı bilər

$$\text{mag}(\nabla f) = \left| \frac{\partial f}{\partial x} \right| + \left| \frac{\partial f}{\partial y} \right|$$

$$\text{mag}(\nabla f) = \max \left(\left| \frac{\partial f}{\partial x} \right|, \left| \frac{\partial f}{\partial y} \right| \right)$$

Nəticədə alınan vektor, $f(x, y)$ funksiyasındakı nöqtələr üçün ən böyük artım istiqamətini əldə edir. Burada x və y piksel koordinatlarıdır.

Əgər $|f'(x, y)|$ çox böyük nəticə verərsə, deməli

$f(x, y)$ çox sürətlə dəyişir və bu o deməkdir ki, təsvirdə parlaqlıqda kəskin dəyişmişdir.

Beləliklə aydın olur ki, bir çox kənar aşkarlama alqoritminin əsasları Qradient amplitudunun mövcudluğuna və bir obyekt qiymətlərinin müqayisə edilməsinə əsaslanır [5].

Pikselin koordinatlarına gəlinə - hər pikselin x və y axınları boyunca bir indeksi var. Təsvirin işlənməsinin üst sol küncdə başlayacağı aydın olur. Yəni, koordinatları olan nöqtədən $(0, 0)$, indeksləmə x oxundan sağa, y oxun aşağı hissəsində $(0, 0)$ nöqtəsindən keçir. Məsələn, təsvirin 1024×768 ölçüsü var. Təsvirin tam ortasında bir nöqtə alırıqsa, koordinatları $(512; 384)$ olacaq [6]. Buna əsasən biz x və y in qiymətlərini müəyyən edirik və düsturda yerinə qoyaraq təsvirin Qradient üsulu ilə seqmentləşdirilməsini aparırıq. Matlabda Qradient üsulu ilə seqmentləşdirmə aparmaq üçün bir çox funksiyalar var. Bu funksiyalar vasitəsilə rəqəmli təsvir üzərində müxtəlif əməliyyatlar aparıla bilər. Qarşıya qoyulan məqsəddən asılı olaraq hansı

funksiyalardan istifadə edəcəyimizi seçirik. Təsvirin seqmentləşdirilməsi prosesində qarşıya qoyulan məqsədi təmin etdiyi halda seqmentləşdirilmə dayandırıla bilər [6].

Matlabda təsvirdəki obyektlərin seçilməsi aşağıdakı kimi olacaq. İlk addımda təsvir matlab sistemində oxunur.

Seqmentləşdiriləcək olan ilkin 1838x3264x3 ölçülü rəngli təsvir Şəkil 5-də verilib.

Şəkil 5. İlk rəngli təsvir

İlkin rəngli təsviri qradiyent üsulu ilə seqmentləşdirdikdə yuxarıda qeyd etdiyimiz kimi həddən artıq seqmentləşdirmə effekti nəzərə çarpır (şəkil 6).

Şəkil 6. Qradyent üsulu ilə həddən artıq seqmentləşdirilmə effekti.

Markerləşdirilmiş watershed üsulu ilə seqmentləşdirməni davam etsək fərqli nəticə alırıq. Həddən artıq seqmentləşdirilmə effekti isə aradan qaldırılır. Bunun üçün birinci növbədə Matlab da təsvir boz rəngli təsvirə çevrilir (şəkil 7).

Şəkil 7. İlk monoxrom təsvir.

Daha sonra Qradyentin qiyməti seqmentləşdirmənin funksiyası qismində istifadə edilir. Bunun üçün *sobel* operatoru tətbiq edilir. Bu addımda təsvirdəki obyektlərin kənar xətlərinin formalaşması baş verir (şəkil 8).

Şəkil 8. Qradyentin qiyməti.

Beləliklə də Qradyentin qiymətlərini hesablayaraq təsvirin seqmentləşdirilməsinə keçmək olar.

Şəkil 9. Seqmentləşdirilmiş təsvir.

Şəkil 9. də *gradmag* funksiyası ilə emal edilən təsvirin seqmentləşdirilmiş formasını alırıq. Lakin bu çox səthi seqmentləşdirilmə olduğundan əlavə hesablamalar tələb olunur.

Seqmentləşdirilmənin üçüncü mərhələsində təsvirdə olan obyektlərin ön planının markerlənməsi üçün müxtəlif əməliyyatlar istifadə oluna bilər. Bu misalda morfoloji

texnologiyalardan istifadə edərək *imregionalmax* funksiyası vasitəsilə təsvir analiz edilə bilər.

Lokal maksimumu hesablayaraq ön planın markerini almaq mümkündür. Bu onun üçün edilir ki, ön planın markerlərini ilkin təsvirin üzərinə quraşdırmaq mümkün olsun (şəkil 10).

Şəkil 10. Ön plan markerləri.

Şəkil 11. Lokal maksimumu hesablanılaraq əldə olunan ön plan markerləri.

Şəkil 12. Ön planda yer alan markerlərin orijinal görüntüyə qondarılması.

Şəkil 10 –nu şəkil 11-in üzərinə quraşdırılmasının nəticəsi şəkil 12 də göstərilmişdir.

Qeyd etmək lazımdır ki, təsvirdəki bəzi maraqlı doğurmayan gizlədilmiş və ya bağlanmış obyektlər markerləşdirilməyədə bilər və seqmentləşdirmə üçün maraqlı olmadığından emal da olunmaya bilər. Bu tərzdə əldə olunan hədudlar daha sonrakı emala məruz qalır. Belə emalın

aparılması nəticəsində bir çox təsvirin izolə edilmiş pikselləri sıradan çıxır.

Təsvirin lokal minimumlarını müəyyən etmək üçün *imimposemin* funksiyası istifadə edilir. Həmin funksiya təsvirdəki Qradiyentləri dəqiqləşdirir və beləliklə də ön planın və arxa planın markerlərinin yerləşməsinə dəqiqləşdirir və nəhayət suayırıcı üsulu əsasında seqmentləşmə əməliyyatı yerinə yetirilir (şəkil 13).

Şəkil 13. Suayırıcı xətləri

Təsvir emalının nəticələrinin vizuallaşdırılması seqmentləşdirilmənin tamamlayıcı əməliyyatlarına aiddir. Bu zaman nəticədə ilkin təsvirin üzərində quraşdırılmış ön planın markerləri, arxa planın markerləri və seqmentləşmiş obyektlərin hədudları alınır (şəkil 14).

Şəkil 14. Arxa plan markerləri və seqmentləşdirilmiş obyektlərin hədudları.

NƏTİCƏ

Məqalədə geniş istifadə edilən Watershed üsulunun əsas ideyası araşdırılıb və onun tətbiq edilməsi üçün mövcud yanaşmalar araşdırılıb.

Göstərilib ki, Məsafə çevrilməsi üsullarında bəzi obyektlər düzgün bölünmür və çoxlu lüzumsuz Watershed xətləri alınır

Qradient üsulunda daha çox artıq Watershed xətləri alınır, lakin bu üsulda obyektlərin konturların qurulması daha yaxşı alınır, deməli təsvirlərin təhlili və istifadəsi üçün daha yararlıdır.

Hər iki yanaşmaya nisbətən işarələnmə (markerləmə) üsulu daha əlverişli görünür, çünki məsafə barədə aprior qiymətləri istifadə etmək imkanı mümkün olduğundan onları

həll zamanı effektiv istifadə etmək olur, bununla da alınan nəticə analiz üçün daha informativ olur. misalın həlli zamanı alınan nəticələr də ilkin təsvirlə müqayisədə daha aydın oxunan olur.

ƏDƏBİYYAT

- [1] A. Novel “Survey on image” International Research Journal of Engineering and Technology (IRJET) 2018, vol. 5, No 6, pp. 1079-1082,
- [2] Э.С. Аметова, «Подходы при сегментации изображений по водоразделам», VII Всероссийская конференция Научная инициатива иностранных студентов и аспирантов российских вузов, 2012, с.144-148.
- [3] Image Processing Toolbox. User's Guide. Version 5.0.1 The Math Works, 2004.
- [4] A. Kızılkaya, “Sayısal görüntü üzerinde işlemler”, Denizli, 2008, s. 230-276.
- [5] П.Г. Поля, «Математические методы обработки изображений.», Харьковский, 2013, с.82-90.
- [6] Лошкарев А.С., «Сегментация изображений с помощью кластеризации», Инфокоммуникационные Технологии, Том. 15, №. 4, 2017, с.388-393.
- [7] Р. Гонсалес, Р. Вудс «Цифровая обработка изображений.», М.: Техносфера, 2005, с.797-919

SEGMENTATION OF DIGITAL IMAGES BY WATERSHED METHOD

Ababil Nağıyeva¹, Sakit Verdiyev²,

Azerbaijan Technological University

¹nagiyeaababil@gmail.com, ²info_tel@inbox.ru

Abstract – On conditions widely used image dates communication there is appeared a problem of information securing. It becomes more important to protect image dates from unauthorized users. Image treatment for effective hiding of information is a previous stage for transfer readable information to unreadable so that not any hacker or others had access to original data. Segmentation is a part of many methods for image treatment. In this paper different techniques of segmentation is considering. As a sample of segmentation technique watershed method is shown. In the same time comparative analyse of most popular segmentation techniques, such as Spatio transformation method, Gradient and Marking method is executed and has illustrated for the colour digital images. Conclusion regarding advantages and disadvantages of every considered techniques is made.

Keywords – digital image, segmentation, watershed, gradient, watershed marking, pixel coordinates

Analysis of information protection methods in the system telecommunications based on quantum cryptography

Bayram Ibrahimov¹, Mirfatma Javadova²

¹Azerbaijan Technical University, Baku, Azerbaijan

²Azerbaijan Architecture and Construction University, Baku, Azerbaijan

¹i.bayram@mail.ru

Abstract — In this paper, the methods, algorithms and principles operation of quantum cryptography to protect information from unauthorized access to a telecommunications system using fiber-optic communication lines are partially analyzed. The system key distribution and protocols in the system quantum cryptography are considered.

Keywords — *quantum key, quantum cryptography, protocol, encryption, telecommunication network, fiber-optic communication line.*

I. INTRODUCTION

It is known [1, 2] that in order to provides multimedia services in a telecommunications systems using fiber-optic communication lines, it is necessary to ensure the possibility continuous operation of a public multiservice network and the security transmitting non-uniform traffic. Considering the distributed architecture of the NGN (Next Generation Network, NGN), in which attacks can occur at various points at the network boundaries, technical difficulties arise in ensuring the security such systems.

It should be noted that, according to estimates of domestic and foreign experts, a significant part of the lines used via the publicly available telecommunication channel is fiber-optic communication lines (FOCL). The tasks of protecting a multiservice network using FOCL in a telecommunication system occupy one of the leading places in solving the general problem of information security.

However, various methods communication are currently widely used in the telecommunications system: wired communication lines, cellular communication, satellite communications, fiber-optic communication lines, etc. Subscriber and network users in a wide range are used daily by communication services, which are necessary to ensure the threat to the security of transmitted information.

Modern NGN-based telecommunications systems use various encryption methods, mathematical algorithms, and efficient network coding to preserve and protect the transmitted heterogeneous traffic.

Based on an analysis of the work on Internet security threats for 2015 [3, 4], it was established that the number of targeted attacks on personal data increased by 91% last year, and more than 550 million people became their victims. Therefore, in recent years, new and effective methods and algorithms for protecting information from unauthorized access to subscriber and network communication lines have been developed.

In telecommunication systems, cryptographic systems from unauthorized access are widely used [2, 3]. The latter are based on the use cryptographic keys and are of two types - symmetric and asymmetric. In symmetric cryptosystems, the sender and the recipient - the recipient of the message use the same secret key, in asymmetric two cryptosystems use two keys: one - open, for encryption - the sender uses, the second - closed, for decryption - uses recipient.

In work [1, 2, 3] cryptographic methods and algorithms of information protection from unauthorized access are considered and their cryptographic strength is revealed. In [2, 4] it is determined that at this stage of development and the use cryptographic methods for protecting information do not fully ensure the protection of transmitted information.

Based on the study [4, 5], it was established that one of the important and promising methods and algorithms cryptography is the principles of quantum cryptography, and the network itself is called a quantum network.

Considering the above, this paper discusses the methods and algorithms quantum cryptography, which is based on the principles operation of a quantum computer, using the parallelism of quantum computing.

II. FORMULATION OF THE PROBLEM

The problem of ensuring security in the transmission of information is formulated as the problem of the distribution of the secret key between two remote users [1]. Users form the same bit set, which is used as a cryptographic key. To realize absolute secrecy, it is necessary to observe certain conditions: the key can be used only once, the key must be random, its length must be greater than or equal to the length of the message being encoded [2].

It is known [3, 5] that the security of classical cryptographic methods is based on mathematical laws and is theoretically limited to the computational capabilities of an attacker. The physical solution to the problem of ensuring secrecy in key distribution is to use the principles of quantum cryptography [3, 4].

Quantum cryptography is based on quantum networks, a quantum network is an information and telecommunication network that protects the transmitted information of heterogeneous traffic using the fundamental laws of quantum mechanics. The latter is a practical implementation of the so-called quantum cryptography.

Quantum cryptography is a method and algorithm for protecting information in next-generation multiservice telecommunication networks based on the principles quantum physics.

Unlike traditional methods and algorithms of cryptography, which uses mathematical methods to ensure the secrecy of information transmitted, quantum cryptography focuses on physics, considering cases where information is transferred using objects of quantum mechanics.

The process of sending and receiving messages of non-uniform traffic is always carried out by physical means, for example, using electrons in an electrical signal and photons in fiber-optic communication lines. In this case, eavesdropping can be considered as a change in certain parameters of physical objects - in this case, carriers of information.

To achieve the objective, the methods, algorithms and principles of operation of quantum cryptography are analyzed to protect information from unauthorized access to the telecommunications system using FOCL.

III. THE ESSENCE OF THE CRYPTOKEY IN THE SYSTEM OF QUANTUM CRYPTOGRAPHY

In the system of quantum cryptography, almost all the collisions in the keys. In quantum cryptography, crypto-keys are distributed in two ways [3, 4]: either with the participation of a key distribution center or a direct exchange between users. Crypto keys should be distributed or they can be exchanged over a communication channel in a secure way.

In the system, a by-product of developing a quantum computer using quantum computing parallelism is quantum cryptography, which could bring to light a new encryption algorithm by generating

a secret key. At the same time, the algorithm is the basic construction unit of quantum cryptography qubit (qubit, Quantum Bit).

The classic bit has, as is known, only two states — 0 and 1, while the set of qubit states is much larger. This means that the qubit in one unit time is equal to 0 and 1, and the classical bit in the same unit of time is either 0 or 1. For example, if quantum memory consists of two qubits, then in parallel work with all its possible states: 00, 01, 10, 11.

Due to the possibility of parallel work with a large number of options, a quantum computer needs much less time to solve problems of a certain class. Such problems, for example, include problems decomposing numbers into prime factors, searching a large database, etc.

The considered algorithm for generating the secret key is based on quantum cryptography technology, where it is expedient to use telecommunications systems using FOCL.

Consequently, the rapid development of quantum technology to create an effective secret key and fiber-optic communication lines led to the emergence of quantum cryptographic systems. They are an extreme case protected FOCL. Using quantum mechanics to protect information allows you to receive results that are unattainable with both FOCL technical protection methods and traditional methods of mathematical cryptography.

Protection this class information is used in limited quantities mainly to protect the most critical from the point view security in the FOCL-based telecommunications system.

IV. KEY DISTRIBUTION SYSTEM AND PROTOCOLS IN A QUANTUM CRYPTOGRAPHY SYSTEM

The analysis showed [3] that in quantum cryptography two main directions for the development key distribution systems have emerged. The first direction is based on the coding of the quantum state of a single particle and is based on the principle of the impossibility to distinguish absolutely reliably two non-orthogonal quantum states. An arbitrary state any two-level quantum-mechanical system can be represented as a linear superposition [1, 5]:

$$|\chi_{kk}\rangle = \alpha |0\rangle + \beta |1\rangle \quad (1)$$

her own states $|0\rangle$ and $|1\rangle$ with complex coefficients α and β , where

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2)$$

From (1) and (2) it follows that the basic principles these two areas formed the basis for the development of all protocols for the quantum distribution keys.

There are many quantum cryptography protocols based on the transmission of a message by encoding in the states of single photons, both BB84, B92 and BB84 with six states, Goldenberg-Weidman, Koashi-Imoto,

as well as their modifications [4]. The only protocol developed for coding information in tangled states is E91 [5].

Various quantum cryptography protocols require the construction complex signal processing circuits, which is also convenient to implement on the basis of a single integrated circuit. Solving the problem of key distribution systems and protocols in the system of quantum cryptography on the element base of modern fiber optics is still a challenge.

CONCLUSIONS

The results of the research and analysis show that the progress information security in quantum cryptographic directions is progressing rapidly. In the near future, quantum cryptographic methods for protecting information other than a telecommunications system using FOCL will use top-secret military and commercial applications.

REFERENCES

- [1] K.E.Rumyantsev. Sistemy kvantovogo raspredeleniya klyucha: Monografiya. Taganrog: Izdatelstvo TTI YuFU, 2011. - 264 p.
- [2] B.G. Ibrahimov, R.T.Humbatov, R.F. Ibrahimov. Cryptographic methods and means protection transmitted information in telecommunication systems // International Journal of Electronics & Communication. Vol.6., Issue 4. 2018. – pp.16 –20.
- [3] L.Lydersen, C.Wiechers, C.Wittmann, D.Elser, J.Skaar, V.Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination // Nat. Phot., Vol.4, no. 686. 2010.p.
- [4] N.Gisin, G.Ribordy, W.Tittel, H Zbinden. Quantum cryptography. Rev.Mod. Phys., vol. 74, №1. 2002. - pp. 145-195.
- [5] Makarov V. Quantum cryptography and quantum cryptanalysis, doktor ingenior thesis, Norwegian University of Science and Technology. 2007.-158 p.

Blokçeyn texnologiyasının təhlükəsizlik məsələləri

Oqtay Ələkbərov

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

oqtayalakbarov@iit.ab.az

Xülasə — Tezisdə çoxfunksiyalı və çoxmərhələli blokçeyn texnologiyalarında müxtəlif növ tranzaksiya əməliyyatlarının yerinə yetirilməsi məsələləri araşdırılmışdır. Burada blokçeyn texnologiyasının təhlükəsizlik məsələlərinə baxılmış və perspektivlərindən bəhs edilmişdir.

Açar sözlər— *Blokçeyn, mayner, bitkoin, kriptovalyuta, tranzaksiya*

I. GİRİŞ

Blokçeyn texnologiyası (BT) son dövrlərin ən populyar texnoloji yeniliklərindən sayılır. Bu texnologiyanın sənaye, səhiyyə, maliyyə, elektron hökumət sahələrinə tətbiqi, onun perspektivlərini daha da artırmışdır. Qeyd edildiyi kimi, BT-nin bir çox sahələrə tətbiqi onun təhlükəsizlik məsələlərinin daha da dərinlənəndə araşdırılmasına tələb yaratmışdır. Blokçeyn texnologiyası haqqında məlumatlara XXI əsrin əvvəllərində müəyyən elmi və texnoloji araşdırmaların tərkibində rast gəlmək olardı. Ümumilikdə isə 2008-ci ildə virtual ticarət məkanı üçün xüsusi kriptovalyuta olan bitkoinlərin İnternet istifadəçiləri arasında ödəniş vasitəsi kimi istifadəsi blokçeyn texnologiyasının geniş yayılmasına şərait yaratdı. Bitkoin kriptovalyutasının bazara daxil olması ilə BT yeni bir mərhələyə qədəm qoydu. Hal-hazırda aparılan bir sıra elmi araşdırmalar göstərir ki, bu texnologiya gələcəkdə ağıllı şəhərlərin, əşyaların internetinin və ümumiyyətlə maliyyə bazarının əsas özəyini təşkil edəcək. Hal-hazırda dünyanın bir sıra çox şirkət və təşkilatları BT-dən geniş istifadə etməyə başlamışlar. Bir çox audit şirkətlərinin əsas problemi bazada məlumatın doğruluğunun yoxlanılmasıdır. İnsan faktorunu nəzərə alsaq istənilən məlumatı mərkəzi serverlərdə dəyişmək olur. BT əsasında istifadə olunan Factom Apollo proqram təminatı bu problemi aradan qaldırmışdır. BT-nin ən geniş yayılmış proqram təminatı BlockNotary-dır. Bu proqram təminatı virtual notarius rolunu oynayır. İstənilən şəxs özü haqqında məlumatların doğruluğunu bu proqram təminatı vasitəsilə təsdiqləyə bilər. Məsələn, hər hansı şəxsin bank sistemində əməliyyat aparması üçün onun şəxsiyyətinin təsdiqi vacibdir. BlockNotary proqram təminatı olduğunuz yeri tərk etmədən öz məlumatlarınızı təsdiqləməyə imkan yaradır. BT çoxfunksiyalı və sadə struktura malik olması, qeyd etdiyimiz sahələrdə məlumatların emalını, proseslərin avtomatlaşdırılmasını və eyni zamanda təhlükəsizlik məsələlərini dəfələrlə artıracaqdır. BT-yə güvənin artmasının başlıca səbəbi, onun bir neçə vacib elementə sahib olmasıdır. Hal-hazırda blokçeyn texnologiyasının 6 elementi vacib sayılır [1,2]:

- Mərkəzləşdirilməmiş server

- Açıq mənbə
- Məxfilik
- Avtonom rejim
- Sabit sistem
- Tranzaksiya şəffaflığı.

Qeyd elədiyimiz elementlər blokçeyni digər bənzər sistemlərdən fərqləndirərək daha da üstün edir. BT-nin ümumi arxitekturası çox sadə formaya sahibdir. BT-də gedən proses vaxtı hər növbəti bloka məlumat ötürülməsi zamanı yeni blokdan özündən əvvəlki bloka isə informasiyanın doğruluğu haqqında məlumat ötürülür. Əgər bu proses zamanı geri ötürülən təsdiq siqnallarının hər hansı birində məlumat uyğunsuzluğu olarsa, proses sistem tərəfindən avtomatik olaraq dayandırılır.

Blokçeyn texnologiyasının 3 tipi var [3]:

- **Ümumi blokçeyn texnologiyası** – bütün istifadəçilərə bloklarda həyata keçirilən proseslər və eyni zamanda tranzaksiya haqqında məlumatları açıq formada əldə etməyə imkan verir.
- **Konsorsium blokçeyn texnologiyası** – burada adətən iki şirkət arasında baş verən tranzaksiya əməliyyatları vaxtı məxfiliyi təmin etmək üçün şəbəkənin bəzi aralıq bloklarından istifadə etməklə məlumatların məxfiliyi qorunur.
- **Özəl blokçeyn texnologiyası** – bu texnologiyada bloklarda gedən bütün əməliyyatların məxfiliyi qorunur. Prosesdə iştirak edən istifadəçilər əməliyyat haqqında məlumata sahib olurlar. Yalnız ötürücü və qəbuledici tərəflər bütün tranzaksiyanın gedişatını izləyə bilirlər.

Qeyd etdiyimiz kimi BT sadə mərkəzləşdirilməmiş sistemə sahib olduğundan onun təhlükəsizlik məsələləri daim aktual olur.

II. BLOKÇEYN TEXNOLOGİYASININ TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Blokçeyn texnologiyasının daha müstəqil fəaliyyət göstərməsi ona olan marağı artırır. Təbii ki, bu faktor BT-də təhlükəsizlik məsələlərini gündəmə gətirir. Blokçeyndə təhlükəsizlik 2 mərhələdə aparılır. 1-ci mərhələdə tranzaksiya zamanı təhlükəsizlik, 2-ci mərhələ isə tranzaksiya bitəndən

sonra əldə olunan bitkoinlərin təhlükəsizliyi nəzərdə tutulur. BT-nin təhlükəsizliyinə bir neçə faktor təsir edə bilər. Bunlara aşağıdakıları göstərə bilərik [4]:

- **Tranzaksiyada çox hissəyə sahib olmaq.** Burada əsasən bloklarda gedən proseslərdə iştirak edən maynerlərin (tranzaksiyada iştirak edən virtual istifadəçi) şəxsi mənafeyi naminə bloka təsir etməsi nəzərdə tutulur. Belə ki, bloklarda gedən əməliyyatlar zamanı hər bir mayner göstərdiyi xidmətə görə müəyyən miqdarda bitkoinlə qiymətləndirilir. Aparılan araşdırmalar göstərir ki, hər hansı mayner proses zamanı 51%-dən artıq paya sahib olarsa, artıq tranzaksiyaya təhlükə yarada bilər. Belə olan halda mayner tranzaksiyaya bir neçə formada təsir edə bilər:
 - ✓ Tranzaksiya haqqında məlumatları dəyişmək;
 - ✓ DoubleSpending etməklə tranzaksiyanın xərcini artırmaq;
 - ✓ Tranzaksiyanın gedişatını saxlamaq;
 - ✓ Tranzaksiyaya daha çox fayda verən maynerin fəaliyyətinə təsir etmək;
- **Blokların saxta klonları.** Bu zaman kənardan kibercümlər etməklə tranzaksiyada saxta bloklar yaradılır. Təbii ki, blokçeynin mərkəzləşdirilməmiş sistemə sahib olması saxta blokların yaradılmasını asanlaşdırır. Belə ki, ümumi tranzaksiya əməliyyatı vahid mərkəzdən paylanılır. Sistemdə səpələnmiş formada olur.
- **Bloklarda aparılan əməliyyatların həcmi.** Bildiyimiz kimi tranzaksiya əməliyyatlarının həcmi fərqli ola bilər. Əməliyyatın həcmnin böyük olması həmin prosesdə daha çox mayner iştirakı deməkdir. Belə olan halda isə əməliyyatı yerinə yetirmək üçün daha çox resurs istifadə olunur. Təbii ki, daha çox resursun istifadəsi sonda əməliyyat üçün mükafatın həcmi daha da artırır və hakerlər üçün həmin tranzaksiyada gedən bloklara hücum etmək üçün stimül verir.
- **Bloklarda aparılan əməliyyatların vaxtı.** Yuxarıda qeyd etdiyimiz kimi tranzaksiyanın həcmnin böyük olması maynerlərin çoxluğuna təsir edir. Eyni zamanda bloklarda gedən əməliyyatlara sərf olunan vaxt da kibercümlərə şərait yaradır. Belə ki, prosesin uzun müddət davam etməsi kibercümlər edən hakerlərə daha çox sərf edir. Tranzaksiyaya sərf olunan vaxtın çox olması onun mükafat qiymətini artırır.
- **Tranzaksiyanın ümumi dəyəri.** Yuxarıda sadaladığımız bütün faktorlar tranzaksiyanın maliyyə dəyərini artırmaqla yanaşı eyni zamanda ona edilən kibercümlərin sayını artırır. Ona görə də zaman keçdikcə əməliyyatlara verilən mükafatın həcmi azaldılmaqla daha çox mayner arasında paylanılır. Belə olan halda sistemə edilən hücumların sayı və keyfiyyəti də azalır.

III. BLOKÇEYNƏ EDİLƏN HÜCUMLARIN QARŞISININ ALINMASI

Bitkoinə marağın artması ona edilən hücumların da sayını artırmağa başladı. İlk kütləvi hücum 2011-ci ilə təsadüf edir. 2011-ci ildə Tokyo şəhərində yerləşən MT.Gox şirkətinə kibercümlər olunmuşdur. Nəticədə şirkətin virtual kriptohesabından 9 milyon dollar civarında bitkoin oğurlanmışdır. Daha bir kibercümlə 2013-cü ildə ABŞ-da yerləşən InstaWallet şirkətinə olunmuşdur. Şirkətin yaydığı məlumata əsasən InstaWallet-ə 5 milyon dollar ziyan vurulmuşdur. Bundan sonra da dəfələrlə belə hücumlar qeydə alınmışdır. Amma blokçeyn tarixinin ən böyük kibercümlə 2014-cü ilə təsadüf edir. Yenidən MT.Gox şirkətinə edilmiş hücum nəticəsində şirkətə 470 milyon dollara yaxın ziyan dəymişdir. Bütün bu halların baş verməsi blokçeynin təhlükəsizlik məsələlərinə başqa prizmadan yanaşmağa məcbur etmişdir [5].

Tranzaksiya bitdikdən sonra əldə olunan bitkoinlərin təhlükəsizlik məsələləri aşkarlanır. Bitkoinlərin təhlükəsizliyini təmin etmək üçün aşağıdakı metodlardan istifadə olunur.

1. **İdentifikasiya** — Blokçeyndə təhlükəsizliyin əsasını istifadə olunan açarın şifrələnməsi təşkil edir. Belə ki, kibercümləyətə ilk növbədə istifadəçinin kompüterində və ya smartfonunda yerləşən elektron açara hücum edir. Həmin elektron açar vasitəsi ilə istifadəçi öz elektron cüzdanına (e-wallet) daxil ola bilər və ya ona göndərilən tranzaksiya prosesini izləyə bilər. Açarın bu texnologiyada vacib rol alması onun təhlükəsizlik məsələlərini daha da artırmışdır. Belə ki, kənardan hücumların qarşısını almaq üçün ikimərhələli təhlükəsizlik identifikasiyası təklif olunmuşdur: 1-ci mərhələdə istifadəçi tərəfindən parol daxil olunur, 2-ci mərhələdə isə ECDSA təhlükəsizlik protokolundan istifadə etməklə sistemə giriş şifrələnir [6].
2. **Təhlükəsizlik cüzdanı** — Qeyd etdiyimiz kimi, istifadəçi əldə olunan bitkoini xüsusi elektron cüzdanlarda saxlayır. Kibercümləyətlər üçün ən asan metod məhz bu elektron cüzdanlara hücum etməkdir. Bu hücumların qarşısını almaq üçün multisig xidməti təklif olunur. Bu xidmət istifadəçinin imzasını onlayn rejimdə qəbul edir. Hətta kənar şəxs cüzdana giriş parollarını bilsə belə həmin hesabdən heç bir transfer və ya ödəniş edə bilməyəcək. Çünki yekunda istifadəçinin elektron imzası tələb olunacaq. Bu elektron imzanı xüsusi USB fləşlərə program vasitəsi ilə yazılmaqla və həmin USB-ni personal kompüterə daxil etməklə elektron imzanı aktivləşdirmək, hətta oflayn rejimdə də istifadə etmək olar [7].
3. **Program təminatı təhlükəsizliyi** — Zaman-zaman BT-nin program təminatında da problemlərə rast gəlinir. Belə ki, programda baş verən xətlər müəyyən problemlərə yol açır. Ən böyük program təminatı xətası 2010-cu ildə baş vermişdir. CVE-2010-5139 protokolunda baş verən xəta böyük fəsadlara yol açmışdır. Programda baş verən yanlışlıq səbəbindən

0,5 bitkoin əməliyyatın sonunda sistem tərəfindən 184 trillion bitkoin qeydə alınmışdır. Daha bir proqram xətasına 2011-ci ildə rast gəlinmişdir. Bu zaman bloklarda səviyyələrarası keçid zamanı BerkeleyDB-dən LevelDB-yə 0,1 saniyə gecikmə baş vermişdir. Nəticədə bütün blokların sinxronizasiyası zamanı uyğunsuzluq yaranmışdır.

Bulud texnologiyalarının inkişafı BT-yə də təsirsiz ötürülməmişdir. Əvvəlki dövrlərdə bitkoin istifadəçiləri haqqında məlumat, onların təhlükəsiz formada saxlanması problemli məsələ idi. Bulud texnologiyasından istifadə etməklə bu problemlər öz həllini tapdı. Belə ki, əvvəllər hər hansı istifadəçi öz parolunu və ya elektron cüzdana giriş açarlarını unudursadı sistemə yenidən bərpa olunmaq uzun vaxt aparır, bəzən isə heç mümkün olmurdu. Bulud texnologiyalarının tətbiqi ilə istifadəçi parolları, elektron cüzdanın açarlarını, şəxsi məlumatlarını buludlarda rezerv etməklə bu çatışmazlıqlar aradan qaldırıldı. Bununla bulud platformalarında rezerv edilən elektron cüzdanların təhlükəsizlik mərhələsi bir pillə daha da artır. İstifadəçi hər dəfə bulud vasitəsilə sistemə daxil olanda bulud platforması tərəfindən xüsusi giriş açarı təqdim olunur. Əgər bu açarla istifadəçi imzası arasında hər hansı uyğunsuzluq olarsa, sistemə giriş məhdudlaşdırılır. Bu hal 3 dəfə təkrarlanarsa, onda sistem özünü qorumaq məqsədi ilə bütün məlumatları rezervləməklə silir [8].

NƏTİCƏ

İnformasiya texnologiyalarının sürətli inkişafı və virtual mühitdə onlardan daha da geniş istifadə olunması blokçeyn texnologiyasını aktual edir. BT-nın ağıllı şəhərlərə, əşyaların internetinə tətbiqi və bulud texnologiyalarında istifadəsi ilə bu texnologiyanın geniş yayılmağa başlaması onun təhlükəsizlik məsələlərini daim nəzarətdə saxlamağı tələb edir. Məqalədə qeyd edildiyi kimi BT-nın təhlükəsizlik məsələləri daim analiz edilməli və problemlərin vaxtında həlli yolları tapılmalıdır. Eyni zamanda bu texnologiyalarda tranzaksiya zamanı və tranzaksiya bitdikdən sonra əldə olunan bitkoinlərin təhlükəsizliyi təmin edilməlidir.

ƏDƏBİYYAT

- [1] N. T. Courtois and L. Bahack, "On subversive miner strategies and block with holding attack in bitcoin digital currency," CoRR, vol. abs/1402.1718, 2014.

- [2] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," arXiv preprint arXiv:1311.0243, 2013.
- [3] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in IEEE Symposium on Security and Privacy, pp. 104–121, May 2015.
- [4] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in 24th USENIX Security Symposium, pp. 129–144, Washington, D.C., 2015.
- [5] Beikverdi, A.; JooSeok, S. Trend of centralization in Bitcoin's distributed network. In Proceedings of the 2015 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Takamatsu, Japan, 1–3 June 2015.
- [6] Y. Yuan, F.Y Wang, "Towards blockchain-based intelligent transportation systems. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016.
- [7] T. Bamert, C. Decker, R. Wattenhofer, S. Welten, BlueWallet: The Secure BitcoinWallet. In Security and Trust Management; Mauw, S., Jensen, C., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 65–80.
- [8] I. Eyal; G.S Emin, Majority is not enough: Bitcoin mining is vulnerable. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Germany, 2014.

SECURITY ISSUES IN BLOCKCHAIN TECHNOLOGY

Oqtay Alakbarov

Institute of Information Technology of ANAS

Baku, Azerbaijan

oqtayalakbarov@iit.ab.az

Abstract – The paper studies various transaction operations within multifunctional and multidimensional blockchain technologies. Security issues and perspectives are also analyzed in this study.

Keywords – Blockchain, miner, bitcoin, cryptocurrency, transaction.

Elektron dövlət mühitində sosial münasibətlərin təhlükəsizliyi

Rasim Əliquliyev¹, Ramiz Alıquliyev², İradə Ələkbərova³

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹*r.alguliev@gmail.com*, ²*r.aliguliyev@gmail.com*, ³*airada.09@gmail.com*

Xülasə– İnformasiya texnologiyalarının vətəndaşın gündəlik həyatına və davranışına intensiv və dinamik təsiri cəmiyyətdə yeni münasibətlərin yaranmasına, ənənəvi münasibətlərdə müəyyən dəyişikliklərin baş verməsinə səbəb olmuşdur. Tədqiqatda insanlar arasında münasibətlərin xüsusiyyəti analiz olunmuş, münasibətlər forma və tipinə görə təsnifatlandırılmış, münasibətlərə təsir edən əsas faktorlar müəyyənləşdirilmişdir. E-dövlət mühitində münasibətlərin idarə olunması və təhlükəsizliyi məsələlərinin səmərəli həlli üçün təkliflər verilmişdir.

Açar sözlər– *e-dövlət, informasiya təhlükəsizliyi, Danbar rəqəmi, aktor, münasibətlərin qiymətləndirilməsi, münasibətlərin gücü, münasibətlərin təhlükəsizliyi.*

I. GİRİŞ

İnsanlar arasında münasibətlər və onların müxtəlifliyi cəmiyyətin inkişaf prosesinə, sosial-iqtisadi və siyasi vəziyyətə, dövlətin informasiya məkanının təhlükəsizliyinə təsir edən vacib faktorlardandır. Münasibətlər insanlar, təşkilatlar, partiyalar, şirkətlər və ölkələr arasında olur. Cəmiyyətdəki münasibətlərin xarakterini tədqiq edən bir sıra elmi istiqamətlər vardır. Bu istiqamətlərə sosiologiya, psixologiya, informasiya texnologiyaları, antropologiya, hüquq, iqtisadiyyat və s. daxildir [1]. Məsələn, biznesin inkişafında münasibətlərin analizi metodlarından istifadə etmək artıq ənənə halını almışdır.

Sosial münasibətlər dedikdə sosial qruplar və ya onların üzvləri arasında sənaye, iqtisadi, hüquqi, əxlaqi, siyasi, dini, etnik və digər sahələrdə baş verən proseslərdə yaranan münasibətlər nəzərdə tutulur. Münasibətləri tədqiq edən müxtəlif metod və nəzəriyyələr mövcud olsa da, bu sahədə tədqiqatlar hələ də davam etməkdədir [2].

Tədqiqatın məqsədi e-dövlətdə münasibətlərin xüsusiyyətinə aydınlıq gətirmək, onları ayrı-ayrı əlamətlərə görə təsnifatlandırmaq və idarə olunması və təhlükəsizlik məsələlərinin həlli üçün təkliflərin işlənməsidir.

II. MÜNASİBƏTLƏTİN AVTOMATİK ANALİZİ SİSTEMLƏRİ

Cəmiyyətdəki münasibətlərini analiz edən və aşkarlayan müxtəlif sistemlər mövcuddur [3–5]. Bu sistemlər müəyyən təşkilat daxilində, sosial şəbəkədə və ya dünyada insanlar arasında münasibətləri analiz etmək üçün nəzərdə tutulmuşdur.

İnternet məkanında münasibətlərin analizi üçün sistemlər təklif olunur. Bu sistemlərdən biri də 2010-cu ildən ABŞ-ın Nyu-York şəhərində “RelSci” şirkəti tərəfindən təklif olunan “Relationship Science” sistemidir [4]. Sistem dünyanın ən nüfuzlu şəxsləri haqqında informasiya toplamaq və emal etməklə, onlar və ya onların ətrafındakılarla necə əlaqə saxlamaq haqqında bilik yaradır, münasibətlərdən istifadə etməklə daha yüksək gəlirin əldə olunması, yeni istehsal və istehlak sahələrinin əldə olunması, sazişlərin bağlanması və s. işlərdə yardımlar təklif edir. Sistem əlaqə məlumatları və ya digər gizli fərdi məlumatların təqdimatını yerinə yetirməyə də, nüfuzlu insanlarla necə əlaqə qurmaq, bunun üçün kimlərə müraciət etmək haqqında məlumat təqdim edir.

Münasibətlərin analizi üçün nəzərdə tutulmuş digər sistemə misal olaraq “Traxor” proqram təminatını göstərmək olar. Traxor proqramı SaaS xidmətini xatırladan proqram təminatı olub, şirkət daxilində münasibətlərin idarə olunması (*True Relationship Management*) üçün nəzərdə tutulmuşdur. Sistem əməkdaşlar arasında münasibətlərin tipini və gücünü qiymətləndirmək üçün də istifadə oluna bilər. Sistemdə münasibətin gücü 1 və 100 arasında verilir. Məsələn, münasibətin gücü 69-dan yuxarı olarsa münasibətlər əməkdaşlıq səviyyəsində qeyd olunur. Münasibətlərin tipi xüsusi, texniki, sosial, əməkdaşlıq, qohumluq, dostluq, tanışlıq və s. ola bilər. Traxor sistemi şirkət və ya təşkilat üçün nəzərdə tutulduğundan burada yalnız xüsusi, texniki, sosial, əməkdaşlıq tipli münasibətlərin qiymətləndirilməsi yerinə yetirilir [5]:

- Xüsusi münasibətlər şirkətin işi ilə əlaqədar yaranan hər hansı problemin həlli üçün gözlənilməz müraciətlərə və ya təkliflərə aiddir.
- Texniki münasibətlər rəhbərliyin göstərişi və ya qaydalara əsasən qurulan münasibətlərdir.
- Sosial münasibətlər əməkdaşlar arasında dostluq münasibətlərinə və ya ümumi maraq sahəsinə aiddir.
- Əməkdaşlıq münasibətləri daha güclü münasibətlər hesab olunur və əməkdaşların bütün sahələrdə bir-birilərinə etimad göstərdiklərini bildirir. Hesab olunur ki, şirkətin yüksək gəlir əldə etməsi üçün əməkdaşlıq münasibətlərinin çoxalması vacibdir.

Bu tip sistemlərin hazırlanmasına şirkətlərin milyonlarla dollar xərcləməsi bir daha sübut edir ki, cəmiyyətdəki münasibətlərin qiymətləndirilməsi müasir dövrdə çox aktualdır. Əsasən də biznes, maliyyə, dövlət təhlükəsizliyi, cinayətkarların aşkarlanması və s. məsələlərin həllində insanlar arasındakı münasibətlər vacib faktordur.

III. MÜNASİBƏTLƏRİN XÜSUSİYYƏTLƏRİ

Münasibətləri analiz etmək üçün ilk növbədə bu sahədə tədqiqat işləri ilə tanış olmaq lazımdır. Britaniyalı antropoloq, Oksford Universitetinin professoru Robin Danbar (*Robin Dunbar*) tədqiqatlarında bu nəticəyə gəlmişdir ki, hər bir insan orta hesabla 150 nəfərlə stabil (daimi) münasibətdə olur. “Danbar rəqəmi” (*Dunbar numbe*) adlanan bu nəzəriyyədə qeyd edilir ki, münasibətlər fərdin xarakterindəki fərqləndirici cəhətləri və sosial vəziyyətini müəyyən edir [6].

Internet şəbəkəsinin genişləndiyi, informasiya cəmiyyətinin formalaşdığı, sosial medianın insanların həyatının bütün sahələrinə daxil olduğu müasir dövrdə “Danbar rəqəmi” nəzəriyyəsinin doğruluğu şübhə doğurur. Lakin araşdırmalar göstərir ki, bu nəzəriyyəyə mobil əlaqələrin, sosial şəbəkələrin genişlənməsi o qədər də təsir etmir. Bu gün ən nəhəng virtual sosial şəbəkə olan Facebook-da hər bir fərdin orta hesabla 300-ə yaxın “dostu” vardır. Şəbəkədəki münasibətlər istifadəçilərin yaşından asılı olaraq müxtəlifdir: 18-29 yaş arasında istifadəçilərin 27%-nin dostlarının sayı 200-dən çox, yaşı 65-dən çox olan istifadəçilərin 72%-nin dostlarının sayı isə 100-dən azdır [7].

Virtual məkanda sosial medianın genişlənməsi insanların sosial münasibətlər qurmaq arzusunda olduğunu və bu münasibətləri qorumaq istədiyini sübut edir. Lakin sosial media sosial münasibətlər deyil, sosial şəbəkələr yaradır. Münasibətlər yalnız informasiya mübadiləsi aparmaqla yaranmır. Münasibətlərdə etimad, zaman, mənəvi və ya maddi təsir, nüfuz və s. faktorlar mühüm rol oynayır [8].

Cəmiyyətdəki münasibətləri qiymətləndirmək üçün ilk növbədə fərdlər arasında münasibətlərin təsnifatlandırılmasına ehtiyac vardır. Bu münasibətlər müxtəlif xüsusiyyətlərə görə fərqlənilir. Məsələn, münasibətlər formasına görə iki qrupa bölünür:

1. Rəsmi münasibətlər. Münasibətlər nortmativ-hüquqi qaydalarla və ya hər hansı rəsmi şəxs tərəfindən qəbul olunmuş xüsusi normalar əsasında müəyyən olunur. Məsələn, xidməti münasibətlər, həmkarlar arasında əmək münasibətləri və s.

2. Qeyri rəsmi (şəxsi) münasibətlər. Məsələn, dostluq kimi heç bir formal qaydalarla məhdudlaşdırılmayan münasibətlər qeyri-rəsmi münasibətlərə aiddir və rəsmi münasibətlərlə müqayisədə daha güclü, zəngin və etibarlıdır.

Rəsmi və qeyri rəsmi münasibətlər özləri də alt qruplara ayrılırlar: uzunmüddətli (dostlar və ya həmkarlar), qısamüddətli (təsədüfi tanışlar), daimi (ailə), təhsil müddətində, funksional (icraçı və ya sifarişçi) və subordinasiya (rəhbər və işçi) [9].

Sosial mühitdə münasibətlər təsir formasına görə fərqlənilir və bu fərq aşağıdakı kimidir [10]:

- 1) Güclü münasibətlər;
- 2) Orta münasibətlər;
- 3) Zəif münasibətlər;
- 4) Olmayan münasibətlər.

Qohumluq münasibətlərindən başqa bütün sosial münasibətlərin başlanğıcında zəif münasibətlər dayanır və zaman keçdikcə bu münasibətlər formasını dəyişir. Məsələn, yaxın dostla münasibətlər güclü, qohumlarla orta, uzaq qohumlarla və ya tanışlarla münasibətlər isə zəif münasibətlərə aid ola bilər. Olmayan münasibətlər dedikdə, informasiya mübadiləsi aparmayan insanlar arasında münasibətlər nəzərdə tutulur. Məsələn, hər səhər küçədə qarşılaşarkən yalnız salamlaşan qonşular, avtobus sürücüsü və sərnəşin, mağazadakı menecer və müştəri.

Stenford Universitetinin professoru Mark Granovetter (*Mark Granovetter*) apardığı sorğular və tədqiqatlar nəticəsində sübut etmişdir ki, zəif münasibətlər güclü münasibətlər qrupları arasında əlaqələrin yaranmasında əsas rol oynayır və körpü funksiyasını yerinə yetirirlər. Zəif münasibətlər qruplar arasında münasibətlərin güclənməsinə yardım edir. O, “Zəif əlaqələrin gücü” (*The Strength of Weak Ties*) nəzəriyyəsində qeyd edir ki, bütün güclü münasibətlər zəif münasibətlərdən yaranır [8]. Deməli, güclü münasibətlər cəmiyyətdə əsas olsa da, əsas sosial əlaqələr zəif münasibətlər hesabına formalaşır. Granovetter qeyd edir ki, münasibətlər üçün aşağıdakı faktorlar əsasdır:

- Zaman: bir yerdə keçirilən vaxt;
- İntensivlik: yaxınlıq hissi, emosiya;
- Etimad: münasibətlərdə şəffaflıq, etibarlılıq;
- Qarşılıqlı münasibət: qarşılıqlı yardım və diqqət.

Buradan belə nəticəyə gəlmək olar ki, güclü münasibətlər daha çox zaman, diqqət və etimad tələb edir. Tədqiqatlar göstərir ki, zəif münasibətlər innovasiyaların tətbiqi, cəmiyyətdə yeni münasibətlər yaratmaq, status əldə etmək üçün əlverişlidir [9].

Zəif münasibətlər böyük sosial qrupların yaranmasında əsas faktordur. Lakin etimad, qarşılıqlı dəstək və kömək kimi xüsusiyyətlər güclü münasibətlərə aiddir. İnsanların tez-tez görüşməsi və bir-birlərinə qarşı yaranan böyük etmad güclü münasibətlərin formalaşmasına səbəb olur. Belə münasibətlər çoxluğunda informasiya daha tez yayılır və bu səbəbdən onların istifadə etdikləri informasiya təqribən eynidir. Zəif münasibətlərdə çox zaman müxtəlif və yeni məlumatlardan istifadə olunur. Yəni yeni xəbərin yayılmasında zəif münasibətlər əsas rol oynayır [11].

Cəmiyyətdə zəif münasibətlər güclü münasibətlərlə müqayisədə daha çoxdursa, belə cəmiyyətdə yeni xəbərin yayılması, cəmiyyətin idarə olunması daha sürətlə baş verəcəkdir [12].

IV. MÜNASİBƏTLƏRİN QIYMƏTLƏNDİRİLMƏSİNDƏ ƏSAS GÖSTƏRİCİLƏR

Münasibətləri qiymətləndirmək üçün ilk növbədə münasibətləri əks etdirən informasiya mənbələri müəyyən olunmalıdır və aşağıdakı faktorlar nəzərə alınmalıdır:

- 1) Münasibətin əhatə dairəsi – münasibətlərdə iştirak edən insanların sayı;
- 2) Münasibətlərin genişlənməsi – bir fərdin münasibətdə olduğu insanların sayı;
- 3) Münasibətlərin dərinliyi – iki fərd arasında münasibətin gücü;
- 4) Münasibətlərin təsiri – bir fərdin digər fərdə və ya onun qərarına təsiri nəzərdə tutulur.
- 5) Münasibətlərin zamanı – münasibətlərin müəyyən zaman kəsiyində vəziyyəti.

Şəkil 1. Münasibətlər qrafı

Münasibətləri əks etdirən informasiyanı müxtəlif informasiya mənbələrindən istifadə etmək olar. Onlar aşağıdakılardır:

- e-mail;
- arxivlərdə saxlanılan rəy və sənədlər;
- mobil qurğular;
- sosial media vasitələri.

Münasibətlərin modelini qurmaq üçün qraflar nəzəriyyəsinə istifadə daha məqsəduyğundur. Belə ki, sosiologiya sahəsində nəzəri tədqiqatlar əsasında sosial strukturların və münasibətlərin vizuallaşdırılması və araşdırılması üçün qraflar nəzəriyyəsinin riyazi əsaslarından istifadə etməklə unikal metodologiyalar geniş istifadə olunmaqdadır [13].

Qraflar nəzəriyyəsinə görə, cəmiyyətin modeli $C = (H, R)$ ilə verilə bilər. H – fərdlər çoxluğu, R isə münasibətlər çoxluğudur:

$$H = \{h_1, h_2, \dots, h_i\}$$

$$R = \{r_1, r_2, \dots, r_i\}$$

R_0 – rəsmi münasibətlər çoxluğu, R_u isə qeyri-rəsmi münasibətlər çoxluğu, olacaqdır:

$$R_0 = R_0^s \cup R_0^d$$

$$R_u = R_u^s \cup R_u^d$$

burada, R_0^s – statik rəsmi münasibətlər,

R_0^d – dinamik rəsmi münasibətlər,

R_u^s – statik qeyri-rəsmi münasibətlər,

R_u^d – dinamik qeyri-rəsmi münasibətlərdir.

Münasibətlər gizli və aşkar, həmçinin birtərəfli və ikitərəfli (qarşılıqlı) olurlar. Məsələn, müəllim və şagird, zabıt və əsgər, rəhbər və işçi arasında birtərəfli münasibətlər mövcuddur, tələbələr və ya əsgərlər arasında isə ikitərəfli münasibətlər mövcuddur. Tutaq ki, iki aktor arasında birtərəfli münasibətlər vardır, onda $H_i \rightarrow H_j$ ilə işarə olunur. Əgər münasibətlər qarşılıqlıdır, onda $H_j \leftrightarrow H_k$ ilə işarə olunur (şəkil 1).

Bir çox hallarda münasibətlərdə müəyyən aktorlar lider olurlar və digər aktorlar liderin ətrafında toplanır. Məsələn, universitetin professorları ilə tələbələr, təşkilatın rəhbərliyi və əməkdaşlar arasında münasibətlər və s. Şəkildən göründüyü kimi H_i , H_j və H_k qovşaqları liderlərdir və güclü münasibətlərlə bağlı olan qraflar arasında əlaqələrin yaranmasında əsas rol oynayırlar.

Cəmiyyətdə münasibətləri analiz etmək üçün verilənlərin intellektual anlyzi, “text mining”, kontent-analiz, LIWC (*linguistic inquiry and word count*), ICA (*independent component analysis*), tematik modelləşdirmə və s. metodlar mövcuddur. Məsələn, ICA metodundan istifadə etməklə təsadüfi qiymətlər çoxluğundan gizli faktorları (münasibətləri) müəyyən etmək mümkündür [14].

V. MÜNASİBƏTLƏRİN TƏHLÜKƏSİZLİYİ VƏ İDARƏ OLUNMASI

E-dövlətin təhlükəsizliyi, vətəndaşların sosial və iqtisadi həyatda rifahı, psixoloji durumu münasibətlərdən çox asılı olduğu üçün münasibətlərin idarə olunması və təhlükəsizliyinin təmini e-dövlət mühitində vacib məsələlərdəndir. Məsələn, ailədə münasibətlərin pozulması ailə dəyərlərinin məhvində, uşaqlar arasında cinayətkarlığa, ailə üzvlərinin sosial və maliyyə durumunun pisləşməsinə səbəb ola bilər.

Münasibətlərin təhlükəsizliyi dedikdə münasibətlərin qorunub saxlanması nəzərdə tutulur. Biznes, təhsil və s. sahələrdə münasibətlərin qorunmasına, həmçinin gücləndirilməsinə ehtiyac vardır. Məsələn, şirkət daxilində rəhbərliklə işçilər arasında münasibətlər pozularsa bu işin keyfiyyətinin aşağı düşməsinə və ən pis halda dəyərli işçilərin şirkətdən getməsinə səbəb ola bilər. Təcrübəli işçilərin yeni işçilərlə əvəz olunması isə şirkətin gəlirinin azalmasına səbəb olacaqdır.

Münasibətlərin təhlükəsizliyinin təmini üçün onların düzgün qurulması yetərli deyil, həm də münasibətlərin düzgün idarə olunması vacibdir. Münasibətlərin təhlükəsizliyi üçün aşağıdakı bir sıra faktorlar nəzərə alınmalıdır:

- Münasibətdə olan insanların sayı;
- Güclü münasibətlərin və əməkdaşlığın səbəbləri;
- Konfliktlərin sayı və səbəbləri;
- Zəif münasibətlərin sayı;
- Münasibətin sosial-iqtisadi duruma təsiri.

Münasibətlərin təhlükəsizliyinə vətəndaşın sosial-iqtisadi vəziyyətinin pisləşməsində əvvəlcədən xəbərdarlıq sistemi kimi də baxmaq olar. Münasibətlərin təhlükəsizliyi sosial kapitalın artmasında və yeni imkanların yaranmasında vacib göstəricidir.

Münasibətləri idarə etmək üçün işlər aşağıda göstərilən mərhələlərlə yerinə yetirilməlidir:

- Münasibətlər cədvəli qurulmalı və bütün münasibətlər qeyd olunmalıdır;
- Münasibətlərin gücü və keyfiyyəti müəyyən edilməlidir;
- Münasibətlərin pozulmasına səbəb ola biləcək təhlükələr və zəif tərəfləri müəyyənəşdirilməlidir;
- Zamana görə münasibətlər cədvəli (münasibətlər təqvim) qurulmalıdır;
- Qarşılıqlı münasibətlərin idarə olunması planı hazırlanmalıdır.

Münasibətlərin idarə olunmasında virtual sosial şəbəkələrin imkanlarından da geniş istifadə etmək əhəmiyyətlidir. Bunlar aşağıdakılardır:

- Sosial şəbəkədə sosial qrupların yaradılması və gündəlik qrupdaxili informasiya mübadiləsi;
- Sosial qrup daxilində insanların sosial problemlərinin müəyyənəşdirilməsi və həlli yollarının müzakirəsi;
- Qrupun sosial kapitalından səmərəli istifadə.

İnsanların sosial-iqtisadi həyatında münasibətlər hər zaman vacib olublar, lakin son illər yaranan iki tendensiya e-dövlət mühitində münasibətlərin formasının dəyişməkdə olduğunu sübut edir: e-dövlətdə sosial media üzərindən yeni münasibətlər qurmaq və bu münasibətləri dəyişmək, konfliktlər yaradaraq münasibətləri yeni müstəviyə gətirmək asanlaşmışdır. Digər tərəfdən, e-dövlətdə kommunikasiya və qloballaşma imkanları insanların münasibətlərində dinamikliyi və şəffaflığı təmin etmişdir.

NƏTİCƏ

E-dövlətdə sağlam münasibətlər vətəndaşların həyatlarında rifahın və əmin-amanlığın təmin olunması üçün vacibdir. İnformasiya texnologiyalarının təsiri altında insanlar arasında münasibətlərin forması dəyişməkdədir. Cəmiyyətin yeni münasibətlər forması (mobil əlaqələr, sosial media vasitələri və s.) yaranmaqdadır.

Tədqiqatdan məlum oldu ki, münasibətlər zamanla dəyişən (dinamik) və ya statik olurlar. E-dövlətdə münasibətlərin zamanın tələbinə uyğun olaraq formalaşması və dəyişməsi dövlətin informasiya məkanının təhlükəsizliyi ilə sıx bağlıdır. Münasibətlərin təhlükəsizliyinin təmin olunması ilk növbədə bu münasibətlərin düzgün idarə olunması ilə əlaqədardır. Sosial şəbəkə vasitəsi ilə təsadüfi münasibətlərin yaranması, “dostların” çoxalması etimadın azalmasına və vətəndaşın nüfuzunun hər an təhlükə altında olmasına gətirir. Bu da cəmiyyətdə münasibətlərə ciddi təhlükədir və bu təhlükələrin qarşısını almaq üçün vətəndaşlar arasında münasibətlərin intellektual analizinə və avtomatik aşkarlanmasına ehtiyac vardır.

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

ƏDƏBİYYAT

- [1]. E.Berscheid. The greening of relationship science // American Psychologist, 1999, 54(4), pp. 260–266.
- [2]. O.Gillath, G.Adams, A.Kunkel. Relationship Science: Integrating Evolutionary, Neuroscience, and Sociocultural Approaches 2012, Washington, American Psychological Association, 254 p.
- [3]. 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, 23-28 Oct. 2011, Providence, RI, USA, pp. 71–79.
- [4]. <https://www.relsoci.com/>
- [5]. <http://www.relatedvision.com/Traxor/traxor.html>
- [6]. R.I. Dunbar. How Many Friends Does One Person Need?: Dunbar's Number and Other Evolutionary Quirks, 2010, Fader and Fader limited, 302 p.
- [7]. A.Smith. What people like and dislike about Facebook, 2014, <http://www.pewresearch.org/fact-tank/2014/02/03/what-people-like-dislike-about-facebook>
- [8]. M.Granovetter The Strength of Weak Ties // American Journal of Sociology, 1973, vol. 78, pp. 1360–1380.
- [9]. Е.П.Ильин. Психология общения и межличностных отношений. СПб.: Питер, 2009, 576 с.
- [10]. R.Collins. The Sociology of Philosophies: A Global Theory of Intellectual Change. Cambridge MA: Harvard University Press, 1998.
- [11]. B.Carolan. Strong Ties, Weak Ties: Relational Dimensions of Learning Settings, 2006, EdLab, Teachers College, Columbia University, 25 p. https://cdn.tc-library.org/Edlab/EdLab_Strongties.pdf
- [12]. K.Sanaz, I.Zuraini, Sh.Bharanidharan. Differences between Role of Strong Ties and Weak Ties in Information Diffusion on Social Network Sites // Advanced Research and Trends in New Technologies, Software, Human-Computer Interaction, and Communicability, 2014, chapter 28, pp. 307–311.
- [13]. S.Wasserman, K.Faust. Social Network Analysis: Methods and Applications, 1994, Cambridge University Press, 825 p.
- [14]. A.Hyvärinen, J.Karhunen, E.Oja. Independent Component Analysis. 2001, John Wiley & Son, 476 p.

SECURITY OF SOCIAL RELATIONS IN THE E-GOVERNMENT

Rasim M. Alguliyev¹, Ramiz M. Aliguliyev², Irada Y. Alakbarova³

Institute of Information Technology of Azerbaijan National Academy of Sciences

¹r.alguliev@gmail.com, ²r.aliguliyev@gmail.com, ³airada.09@gmail.com

Abstract -- The intense and dynamic impact of information technology on everyday life and behaviour citizen has led to the creation of new relationships in society and definite changes in traditional relationships. The study analyzed the nature of the relationship between people, the relationship was classified according to form and type, and the main factors influencing the relationship were identified. Was developed proposals for the effective management of relations and solving problems of security relations in the field of e-government.

Keywords: e-government, information security, Dunbar number, actor, relationship assessment, relationship strength, relationship security.

Sosial şəbəkələrdə saxta profillərin aşkarlanması məsələləri

Yadigar İmamverdiyev¹, Xəyalə Əhmədova²

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

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

Xülasə— Sosial şəbəkələr təkcə sosial ünsiyyət vasitəsi deyil, həm də real və virtual dünyada baş verən bədniiyyətli hərəkətlərin inikas olunduğu kiberməkən, müxtəlif maraqların mübarizəsinin getdiyi meydandır. Adətən, bu bədniiyyətli hərəkətləri həyata keçirən subyektlər öz kimliklərini saxta sosial şəbəkə profilləri vasitəsilə gizlətməyə çalışırlar. Bu saxta profillərin icra edəcəyi funksiyalar onları yaradanların niyyətinə görə dəyişir. Bu məqalədə sosial şəbəkələrdə saxta profillərin növlərinə, sosial şəbəkədən asılı olaraq yerinə yetirdiyi funksiyalara və törətdiyi fəsadlara baxılır, saxta profillərin aşkar edilməsi metodları analiz edilir.

Açar sözlər — sosial şəbəkə; saxta profil; sosial bot; spam botu; saxta profillərin aşkar edilməsi, məşin təlimi.

I. GİRİŞ

Real aləmdə hər kəsin həyatda tutduğu mövqə, məqsəd fərqli olduğu kimi, sosial şəbəkələrdə də insanların məqsədləri müxtəlif olur. Sosial şəbəkələr müxtəlif nöqtələrdə yaşayan insanların arasında müxtəlif məqsədlərlə qurulan virtual dünya kimi qarşılanı bilər. Sosial şəbəkə anlayışı artıq çox insana aydındır. Sosial şəbəkələrdə yaradılan profillər hər zaman saf niyyətlərlə, yəni sadəcə həmin şəbəkənin yaxşı xüsusiyyətlərindən istifadə edilməsi məqsədilə yaradılır. Məsələn, müzakirə forumlarında yaradılan saxta profil irqçiliyi və digər pis məqsədləri təbliğ edə bilər, bununla yanaşı sosial şəbəkələrdən nəticəsi zərərli olacaq çağırışlar etmək üçün də istifadə edilə bilər. Zərərli əməliyyatlar icra etmək üçün kimliyin saxtalaşdırılması saxta profillərin yaradılması sosial şəbəkələrin problemlərindəndir. Bu tip xoşagəlməz halların qarşısının alınması üçün saxta profillərin aşkarlanması üsulları işlənib, hazırlanmışdır.

II. ONLAYN SOSIAL ŞƏBƏKƏLƏRDƏ SAXTA PROFİLLƏR

Sosial şəbəkə anlayışı artıq uşaqdan-böyüyə hər kəsə aydındır. Sosial şəbəkələr müxtəlif məqsədlərlə yaradılır. Sosial şəbəkələrin funksionallığından tam yararlanmaq üçün çox vaxt bu sosial şəbəkələrdə profil açılması tələb edilir. Əgər bir şəxs özü haqqında (real) məlumatlarla bir profil

yaratmış olarsa, o zaman bu profil real profil hesab edilir, çünki real bir şəxsə mənsub olmuş olur. Bununla yanaşı sosial şəbəkələrdə saxta profil anlayışı da vardır. Bu saxta profillərin məqsədi yaradıldığı sosial şəbəkədən asılı olaraq dəyişir. Sosial şəbəkələrə misal olaraq tanışlıq əsaslı sosial şəbəkələr, saf sosial şəbəkələr, müzakirə forumlu sosial şəbəkələr, işgüzar sosial şəbəkələr və s. göstərmək olar.

Tanışlıq əsaslı sosial şəbəkələrdə (Badoo, Match.com, BeautifulPeople və s.) saxta profilin məqsədi zəif görünümlü (emosional olaraq) insanı seçmək, onun bu zəif cəhətindən yararlanaraq bəzi məlumatları ələ keçirib, sonra təhdid yolu ilə pul tələb etmək ola bilər. Tanışlıq saytlarında bu tip əməllərlə məşğul olan insan “catfisher” adlanır [1, 2].

Ənənəvi sosial şəbəkələr (Facebook, Twitter, Orkut, Friendster və s.) saf niyyətlər üçün yaradılır, məsələn bir şəxs digəri tərəfindən bloklanıbsa, o zaman bloklanan şəxs saxta profil açıb yenidən onu bloklayan şəxsə dostluq təklifi göndərə, mesaj yaza və s. edə bilər.

Müzakirə forumlarında (Baidu Tieba, Quora, Skyrock və s.) saxta profillər irqçiliyi təbliğ edə bilər. Digərləri tərəfindən xoş qarşılanmayacaq mövzuları populyarlaşdırma bilər, yalan sorğular, məlumatlar paylaşa bilər ki bu halların da nəticəsi yaxşı bitməyə bilər [1].

İşgüzar sosial şəbəkələrdə (LinkedIn, Researchgate, Academia, Opportunity) saxta profillər bir başqasının gördüyü işləri özəlləşdirə bilər. Bu da qeyri-etik hərəkətdir [1, 3].

Media paylaşılan sosial şəbəkələrdə (Instagram, YouTube, Snapchat və s.) saxta profillər şəkil, video, mətn və s. paylaşmaq üçün istifadə edilir. Bəzən bir şəxs öz adı ilə etmək istəmir paylaşmaları, məsələn, öz şəkillərini başqa ad altında paylaşır, bu yolla da artıq saxta profil yaratmış olur.

III. SAXTA PROFİLLƏRİN NÖVLƏRİ

A. Ələ keçirilmiş profillər (ing. *Compromised profiles*)

Bu tip saxta profillər real şəxslərə məxsus profillərdir. Profil sahiblərinin bu profil üzərində tam idarəsi olmur, yəni real sahiblər artıq bu profillər üzərində idarəni itirmiş

olurlar. Bu da profilin bədniyyətlinin və ya hər hansısa bir zərərli proqramın əlinə keçməsinə gətirib çıxarır [4]. Buna səbəb profillərdə istifadə edilən sadə şifrələr ola bilər. Bu profillərin təhlükəli olmasının səbəbi real şəxsə mənsub olmasıdır, çünki bu real şəxs real aləmdə artıq nüfuz sahibidir. Bu da bədniyyətliyə real şəxs adından hərəkət etməyə kömək edir. Məsələn, bir şəxsin profili bədniyyətli tərəfindən ələ keçirilmişdirsə, bu zaman bədniyyətli real şəxs haqqında məlumatları şəxsin əlaqəsində olan insanlardan ala bilər.

B. Klonlanmış profillər (ing. Cloned Profiles)

Klonlanmış profillər saxta profillərin təhlükəli növlərindən biridir. Bu tip saxta profillərin ələ keçirilmiş profillərdən fərqi odur ki, klon hesab real şəxsə deyil, birbaşa bədniyyətliyə məxsus olur. Yəni ələ keçirilmədən birbaşa yaradılmış olur. Bu tip saxta profillərin 2 növü vardır:

- Saytdaxili profil klonlama (ing. Intra site profile cloning) – sosial şəbəkədə real, etibarlı profili olan şəxsin həmin şəbəkədə profilinin kopyasının (klonunun) yaradılması saytdaxili klonlama hesab edilir.
- Saytlarası profil klonlama (ing. İnter site profile cloning) – müəyyən bir sosial şəbəkədə profili olan şəxsin başqa bir sosial şəbəkədə bədniyyətli tərəfindən profilinin yaradılması saytlarası profil klonlama adlanır [5].

C. Kuklalar (ing. Sockpuppets)

Çorap kuklaları, əsasən, bir şəxsi və ya təşkilatı nüfuzdan salmaq və ya nüfuzunu artırmaq üçün istifadə edilən obrazlardır. Əgər hər hansı xəbər bülletenində (ing. news blog), sosial şəbəkədə və ya hər hansı müzakirə forumunda eyni şəxsə aid olan 2 müxtəlif hesab mövcuddursa, o, sockpuppet cütü (ing. suckpuppet pair) adlanır [6]. Bu hal nüfuzlu bir şirkətə rəqib olan təşkilatın kuklalardan istifadə edərək hədəf təşkilatın nüfuzuna xələl gətirəcək paylaşımlar etdiyi və ya yorumlar bildirdiyi zaman baş verir. Çorap kuklaları reklam sahəsində istifadə edilərək təşkilatın, məhsulun və ya şəxsin nüfuzunu artırmaq üçün istifadə edilə bilər.

D. Sibil hesablar (ing. Sybil Accounts)

Bir şəxsin çox sayda yaratdığı və əl ilə idarə etdiyi saxta hesablar sibil hesablar adlanır. Bu hesablar sosial şəbəkələrdə spam, zərərli proqram yaymaq və qeyri-mütənasib böyüklükdə təsir əldə etmək üçün istifadə edilir. Sibil hücumçuların pis rəy vermək, qeyri-qanuni səs vermək, resurslara giriş əldə etmək, təhlükəsizlik və gizliliyi pozmaq və s. kimi məqsədləri olur [7].

E. Botlar saxta profil kimi (ing. Bots as Fake Profiles)

İş baxımından botlar sibil hesablara oxşadırlar, amma əsas fərq botların avtomatlaşdırılmış kompüter proqramları

olmasıdır. [8]-də müəlliflər funksionallığına əsaslanaraq botları 5 kateqoriyaya ayırırlar:

- **Spam botları** – Spam botları, xüsusilə, şəxsi bloqlara keçid, ödəmə məzmunlu, reklam məzmunlu və s. tipli zərərli məzmunları şəbəkədə istənməyən çox sayda əlaqələr qurmaqla yaymaq üçün yaradılan kompüter proqramıdır [9].
- **Sosial botlar** – Sosial botlar maksimum sayda istifadəçiyə çatmaq və yoluxdurmaq üçün özlərini virus kimi ictimaiyyətə tanıdan proqramlardır. Daha bir tədqiqat [9] bu botlara onlayn sosial şəbəkələrdə hesabları idarə edən və real istifadəçilərin hərəkətlərini təqlid edən botlar kimi yanaşır. Sosial botlar hər zaman problem yaratmırlar. Onlar da işlərinə görə digər botlar kimidirlər, amma onların əsas diqqət mərkəzi daha çox onlayn insanlarla sosial əlaqələr qurmaqdır.
- **Bəyənmə botları** (ing. Like bots) – paylaşımlara, rəylərə gələn bəyənmə sayının saxta yolla artırılması üçün istifadə edilir. Reklamda bəyənmə botları məhsula olan inamı artırmaq üçün istifadə edilə bilər [5].
- **Təsir botları** (ing. Influential bots) – şəbəkə təsir botları Facebook və Twitter kimi onlayn sosial şəbəkələrdə qanunsuz olaraq hər hansı mövzunu məşhurlaşdırmaq, fikirlərə təsir etmək üçün istifadə edilən avtomatlaşdırılmış kimliklərdir [10]. Şəbəkədə təsir botlarının əsas işi onlayn sosial şəbəkələrdə xüsusi mövzu və ya məhsul haqqında istifadəçilərin fikirlərini dəyişməkdir.
- **Botnet** – Onlayn sosial şəbəkələrdə avtomatlaşdırılmış kompüter proqramlarının şəbəkəsi Botnet adlanır. Bu şəbəkədəki hər bir bot fərqli və ya oxşar əməliyyatlar icra etmək üçün təyin edilir. Botnet idarə kanalı (ing. control-channel) vasitəsilə qanunsuz fəaliyyətlər göstərmək üçün idarə edilən kompüter proqramları toplusudur [11]. Botnetlər, adətən, “botmasters” adlanan istifadəçilər tərəfindən zərərli məqsədlər üçün idarə edilir.

IV. SOSIAL ŞƏBƏKƏLƏRDƏ SAXTA PROFİLLƏRİN AŞKARLANMASI METODLARI

Müəlliflər [12]-də Twitter və Facebook-da ələ keçirilmiş hesabları aşkarlamaq üçün COMPA adlanan alət təklif edirlər. Müəlliflər göndərilən mesajların əlamətləri əsasında statistik modelləşdirmə vasitəsilə istifadəçilərin davranış profillərini yaradır və anomalıya hesabını hesablaması üçün n-qram analizi kimi bir neçə oxşarlıq metrikasından istifadə edirlər. Əlamətlərin çəkilişi SMO (Sequential Minimal Optimization) metodu ilə müəyyən edilir. [13]-də müəlliflər Facebook-da spam kompaniyalarını divar mesajlarının klasterləşdirilməsi əsasında təyin edirlər. Sonra hər bir zərərli

hesabın ələ keçirilmiş hesab olması divarda çıxan kontent (şəkillər, videolar və s.) əsasında analiz edilir.

Klonlanmış hesabların aşkarlanması üçün də bir sıra tədqiqatlar vardır. [14]-də müəlliflər Markov Clustering (MCL) algoritmindən istifadə edərək Facebook şəbəkəsini oxşar cəhətlərə əsaslanaraq daha kiçik klasterlərə bölüblər və real profillərə oxşar bütün profillərin klon olub-olmadığının müəyyən edilməsi məqsədilə əlaqə gücünün hesablanması üçün toplanıblar. Digər bir tədqiqatda [15] müəlliflər sosial şəbəkədə saxta profillərin aşkarlanması üçün 3 komponentdən ibarət olan sistemin modelini təklif edirlər. “İnformasiya distilyatoru” (ing. information distiller) adlanan birinci komponent real istifadəçilərdən informasiya çıxarır, şəxsi yeganə şəkildə müəyyən etmək üçün istifadə edilə biləcək əlamətləri seçir. “Profil ovçusu” (ing. profile hunter) informasiyanı işləyir və istifadəçilərin profillərini müxtəlif sosial şəbəkələrdə tapır. “Profil verifikatoru” (ing. profile verifier) bütün profillər arasında oxşarlıq hesabını hesablayır və nəticəni istifadəçiyə təqdim edir.

Sosial şəbəkələrdə kukla hesablarını müəyyənləşdirmək üçün də bir sıra tədqiqatlar aparılmışdır. [16]-dəki tədqiqatda Tianya forumu və Taobao onlayn auksion saytında maraq doğuran mövzular əsasında istifadəçilərin şəbəkəsi (qrafı) yaradılmışdır. İstifadəçilərin yazı stillərinə əsaslanaraq, müəllif kukla şəbəkəsini əldə etmək üçün qrafı emal etmiş və bu qrafda kukla topluluqlarını aşkarlamaq üçün icma aşkarlama metodlarını tətbiq etmişdir. Hong Kong əsaslı müzakirə forumunda olan kuklaları aşkarlamaq üçün başqa bir metod [6]-da təqdim edilib. Bu metod bir hesab tərəfindən paylaşılan mövzuların və digər hesablar tərəfindən verilən cavabların ümumi sayına əsaslanır. Kukla cütünü tapmaq üçün aşkarlama qiyməti hesablanır. Qiymət nə qədər böyükdürsə, iki hesabın kukla cütü olması şansı da bir o qədər artır. İstifadəçilərin durğu işarələri sayı, sitat gətirmək sayı, böyük və ya kiçik hərflərin istifadəsi kimi əlamətlərinə əsaslanaraq [17]-dəki müəlliflər Wikipedia şəbəkəsi üçün təbii dilin emalı metodlarından istifadə edərək kuklaların aşkarlanması metodunu təqdim edirlər.

Tədqiqatçılar sosial şəbəkələrdə [7, 18, 19, 20] sibil hesabların aşkarlanmasına da diqqət yetirirlər, lakin sibil hücumların aşkarlanması hələ ilkin mərhələdədir. Sibil müdafiə metodlarının əksəriyyəti bir hesabın real hesaba nə dərəcədə yaxşı əlaqəli olmasına əsaslanaraq hesabların rəqləşdirilməsi metodu ilə işləyir. Əgər hesab real hesablar toplusu daxilindədirsə, onun rəngi daha böyük olur. SybilGuard-da [21] müəlliflər sosial şəbəkəni Sibil hücumlardan qorumaq üçün yeni bir yanaşma təqdim edirlər. Onlar iki hesab arasındakı əlaqəni inam əlaqəsi kimi qəbul edirlər. Sibil hesablar etibarlı hesablardan etibarlı əlaqə istifadə edilməklə fərqləndirilir. SybilGuard, əsasən, sosial şəbəkələrin iki xüsusiyyətindən asılıdır: birincisi etibarlı hesabların hər zaman çox sayda əlaqəsi olur, ikincisi saxta istifadəçilər az etibarlı əlaqələri olan çox sayda hesablar yaradırlar. [22]-də müəlliflər Facebook heyran (ing. fan) səhifələri, əlaqələr, aktiv dostlar və s. kimi əlamətlərdən istifadə edərək saxta profilləri təyin etmək üçün Facebook

şəbəkəsinin real verilənlərinə MCL algoritmini tətbiq edirlər. MCL istifadəçiləri 3 klasterə ayırır, onlardan biri bütün saxta kimlikləri, ikincisi bütün normal profilləri və üçüncüsü bu ikisinin qarışığını ehtiva edir. Bu tədqiqat göstərdi ki, decision tree (DT), Support Vector Machine (SVM), Naïve Bayes (NB) və s. kimi metodlar profilləri saxta və ya real siniflərə ayırmaq üçün bir vasitə ola bilər, ancaq çox sayda sinifə sahib sosial şəbəkə profili verilənlər toplusu üçün səmərəli işləmir. Həmçinin, bu cür yaxşı müəyyən edilmiş profil verilənləri toplularının çatışmazlığı var və verilənlərin əksəriyyəti əvvəlcədən təyin edilmiş sinif nişanı və ya əlamətləri müəyyənləşdirmir, buna görə də, təlimsiz metodlar təlimli metodlardan üstündür. Eynilə, Bayes klassifikatoru və k-means klasterləşdirmə tətbiq etməklə cins və yer əlamətlərini istifadə edərək Twitter-də aldatmanın aşkarlanması üçün [23]-dəki müəlliflər tərəfindən yeni bir yanaşma təklif edilmişdir. [24]-də müəlliflər bal profilləri (ing. honey profiles) ilə əlaqəli olan istifadəçilər arasından spammerləri təyin etmək üçün Random Forest (RF) algoritminə əsaslanan klassifikator təklif edirlər. Spam strategiyasına əsaslanaraq spam profillərinin Displayer, Bragger, Poster və Whisperer adlanan 4 kateqoriyası fərqləndirilir.

Spam botlarının aşkarlanması da bir neçə tədqiqatçı tərəfindən araşdırılır. [25]-dəki müəlliflər göstərir ki, 4 klassifikasiya metodundan (DT, SVM, K-nearest neighbor və neyron şəbəkələri) başqa, Bayes klassifikatoru Twitter şəbəkəsində spam botlarının ən yaxşı aşkarlama metodudur. [10]-dəki tədqiqatın müəllifləri sosial şəbəkədə təsirli botları aşkar etmək üçün üç addımdan ibarət olan bir yanaşma təklif edirlər. İlk addımda botlar ələ yoxlama, davranış analizi və lingvistik bilik kimi ilkin metodlarla təyin edilir. İkinci mərhələdə əksər botlar klasterləşdirmə, kənarlaşma (ing. outliers) və şəbəkə analizi əsasında müəyyən edilir. Üçüncü addımda isə qalan botlar test məlumatları kimi əvvəlki addımlarda müəyyən edilmiş botlar və insanlardan istifadə etməklə təyin edirlər.

Saxta profillərin aşkarlanması tədqiqatlarında ən çox SVM, DT və Bayes klassifikasiya alqoritmləri istifadə edilir. Bundan əlavə, tədqiqatçıların əksəriyyəti tədqiqat aparmaq üçün Twitter sosial şəbəkəsindən istifadə edirlər. Bunun səbəbi Twitter-in tədqiqat məqsədli istifadəçi verilənlərinə girişə icazə verməsi ola bilər.

Sosial şəbəkələrdə saxta hesabların aşkarlanması üçün maşın təliminə əsaslanan müxtəlif metodlar tətbiq edilir, lakin tədqiqatçıların fikirlərini sadəcə xüsusi tip saxta profillərə cəmləməsi digər tip saxta profillərin aşkarlanmamasına və bədniiyyətlilərin şəbəkəni çirkləndirməsinə gətirib çıxarır. Buna görə də, sosial şəbəkələrdə maksimum sayda saxta profilləri aşkarlaya bilən ümumi metodların işlənməsi çox aktualdır. Bundan əlavə, zaman keçdikcə sosial şəbəkələrdə istifadəçilər və onlar tərəfindən yaradılan məzmunun sayı sürətlə artır və saxta hesabları aşkarlamaq daha da çətinləşir. Buna görə, anomal davranışı müəyyənləşdirmək və ya sosial şəbəkələrdə analiz aparmaq üçün böyük ölçülü qrafların analizi, qrafın

bölməsi və klasterləşdirilməsi alqoritmləri üçün yaxşı miqyaslanan maşın təlimi metodlarına böyük ehtiyac vardır [5].

NƏTİCƏ

Sosial şəbəkələr kənardan necə rəngarəng görünə bilər, istifadəçinin məqsədinə görə təhlükəli alətə də çevrilə bilər. Bu tezisdə saxta profillərin növündən və yaradıldığı şəbəkədən asılı olaraq yerinə yetirdiyi funksiyalardan bəhs edildi. Saxta profillərin aşkarlanması metodları və bu barədə kiber qanunlar saxta profillərin istifadəsi zamanı meydana çıxan xoşagəlməz halların qarşısının alınması, bu halların azaldılması üçün işlənib hazırlanmışdır. Maşın təliminə əsaslanan metodlardan əlavə hər bir şəxs sosial şəbəkədə təhlükəsizliyini təmin etmək üçün sadə parollardan istifadə etməməlidir və parollarını mümkün qədər gizli saxlamalıdır.

ƏDƏBİYYAT

- [1] M.A. Wani, M.A. Sofi, S.Y. Wani, "Why fake profiles: A study of anomalous users in different categories of Online Social Networks", International Journal of Engineering Technology Science and Research, vol. 4, pp. 2394 – 3386, September 2017.
- [2] Making Technology easier, bobology- What is a Catfisher? <https://www.bobology.com/public/What-is-a-Catfisher.cfm>.
- [3] CS Blog, A computer scientist's research blog. <http://ptbcs.blogspot.com/2015/09/rg-fails.html>.
- [4] D. Savage, X. Zhang, X. Yu, P. Chou, and Q. Wang, "Anomaly detection in online social networks", Social Networks, vol. 39, pp. 62-70, 2014.
- [5] M.A. Wani, S. Jabin, G. Yazdani, N. Ahmad, "Sneak into devil's colony – A study of fake profiles in Online Social Networks and the cyber law" arXiv preprint arXiv:1803.08810, 2018.
- [6] X. Zheng, Y.M. Lai, K.P. Chow, L.C. Hui, S.M. Yiu, "Sockpuppet detection in online discussion forums", Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011, pp. 374-377. IEEE, October 2011.
- [7] P. Gao, N.Z. Gong, S. Kulkarni, K. Thomas, and P. Mittal, "Sybilframe: A defense-in-depth framework for structure-based sybil detection", arXiv preprint arXiv:1503.02985, 2015.
- [8] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, "The rise of social bots", arXiv preprint arXiv:1407.5225, 2014.
- [9] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "Design and analysis of a social botnet", Computer Networks, vol. 57(2), pp. 556-578, 2013.
- [10] V.S. Subrahmanian, A. Azaria, S. Durst, V. Kagan, et al, "The DARPA Twitter bot challenge", arXiv preprint arXiv:1601.05140, 2016.
- [11] S.S. Silva, R.M. Silva, R.C. Pinto, and R.M. Salles, "Botnets: A survey", Computer Networks, vol. 57(2), pp. 378-403, 2013.
- [12] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "COMPA: Detecting Compromised Accounts on Social Networks", NDSS, February 2013.
- [13] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns", Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, pp. 35-47. ACM, November 2010.
- [14] M. Y. Kharaji, and F. S. Rizi, "An IAC Approach for detecting profile cloning in Online Social Networks", arXiv preprint arXiv:1403.2006, 2014.
- [15] G. Kontaxis, I. Polakis, S. Ioannidis, and E. P. Markatos, "Detecting social network profile cloning", IEEE International Conference on

Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 295-300, March 2011.

- [16] Z. Bu, Z. Xia, and J. Wang, "A sock puppet detection algorithm on virtual spaces", Knowledge-Based Systems, vol. 37, pp. 366-377, 2013.
- [17] T. Solorio, R. Hasan, and M. Mizan, "A case study of sockpuppet detection in wikipedia", Workshop on Language Analysis in Social Media (LASM) at NAACL HLT, pp. 59-68, June 2013.
- [18] J. R. Douceur, "The sybil attack.", Peer-to-peer Systems, pp. 251-260, Springer Berlin Heidelberg, 2002.
- [19] Z. Yang, C. Wilson, X. Wang, T. Gao, B. Y. Zhao, and Y. Dai, "Uncovering social network sybils in the wild", ACM Transactions on Knowledge Discovery from Data (TKDD), vol. 8(1), pp. 5-33, 2014.
- [20] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybil limit: A near-optimal social network defense against sybil attacks", IEEE Symposium on Security and Privacy, pp. 3-17, May 2008.
- [21] H. Yu, M. Kaminsky, P. B. Gibbons, and A. D. Flaxman "Sybilguard: defending against sybil attacks via social networks", IEEE/ACM Transactions on Networking, vol. 16(3), pp. 576-589, 2008.
- [22] K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: social honeypots+ machine learning", Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval, pp. 435-442, ACM, July 2010.
- [23] 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.
- [24] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks", Proceedings of the 26th Annual Computer Security Applications Conference, pp. 1-9, ACM, December 2010.
- [25] A. H. Wang, "Detecting spam bots in online social networking sites: a machine learning approach", IFIP Annual Conference on Data and Applications Security and Privacy XXIV, pp. 335-342, Springer Berlin Heidelberg, 2010.

ISSUES OF DETECTION FAKE PROFILES IN SOCIAL NETWORKS

Yadigar İmamverdiyev, Khayala Ahmedova

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

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

Abstract – Social networks are not only a means of social communication but also they are the cyber area where malicious acts occurring in the real and virtual world are reflected and the square in which different interests struggle. Normally, those who commit these bad actions try to hide their identity through fake social networks profiles. The functions of these fake profiles differ from one another depending on the purposes of those who create them. This article involves looking at the types of fake profiles, the functions they perform depending on the social network, the complications they have created, and the methods used to detect fake profiles have been analyzed.

Keywords – the social network, fake profile, social bot, spambot, detection of fake profiles, machine training.

Müasir şəbəkə təhlükəsizliyi və inam problemləri

Ramiz Şıxəliyev

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

ramiz@science.az

Xülasə — Məqalədə müasir şəbəkə təhlükəsizliyi və inam məsələləri analiz olunmuşdur. Əsasən, İnternetdə mövcud olan yeni şəbəkə xidmətlərinin təhlükəsizlik və inam məsələləri analiz edilmişdir. Xüsusilə də bulud hesablamaları, əşyaların İnerneti və sosial şəbəkə xidmətlərində meydana çıxan təhlükəsizlik məsələləri analiz edilmişdir.

Açar sözlər — *şəbəkə təhlükəsizliyi, şəbəkə xidmətləri, bulud hesablamaları, əşyaların İnterneti, sosial şəbəkə xidmətləri*

I. GİRİŞ

Bu gün fərdlərin, təşkilatların və dövlətlərin mövcud şəbəkə infrastrukturundan, xüsusilə də İnternetdən asılılığı artıq təsdiq olunmuş faktıdır. Xüsusilə də, onlar şəbəkə infrastrukturunun təhlükəsizliyi və inam dərəcəsindən çox asılıdırlar. Çünki, hücumların, təhlükələrin, verilənlərin oğurlanması və xidmətlərin dayanması hallarının tez-tez baş verməsi onların normal fəaliyyətini pozur. Bununla yanaşı, qlobal əlaqələrin genişlənməsi, xüsusilə İnternetin genişlənməsi, mobil İnternetin, naqilsiz şəbəkələrin, IoT (Internet of Things), Cloud Computing, Grid Computing, sosial şəbəkə xidmətlərinin (SŞX) və s. müxtəlif şəbəkə xidmətlərinin və tətbiqlərinin, həmçinin yeni protokolların yaranması ayrı-ayrı fərdlər və təşkilatlar arasında qarşılıqlı əlaqəni genişləndirmiş və dərinləşdirmişdir. Nəticədə fərdlər və təşkilatlar informasiyanın saxlanması və ötürülməsi sistemlərindən tam asılı vəziyyətə düşmüşdür.

İlk hesablama sistemlərinin işinə kompüter təhlükəsizliyinin təsir etməsinə baxmayaraq, o, bilik sahəsi kimi 1970-ci illərin əvvəllərində öyrənilməyə başlanmışdır. Ənənəvi olaraq, kompüter təhlükəsizliyinin əsas məqsədi informasiyanın və sistemin resurslarının məxfiliyinin, bütövlüyünün və əylətliliyinin təmin edilməsi idi. Bu zaman məxfiliyin təmin edilməsinin məqsədi informasiya və resurslara ancaq icazəsi olan şəxslərin girişinin təmin edilməsindən ibarət idi. Bütövlüyün təmin edilməsinin məqsədi informasiyanın saxlanması və ötürülməsi zamanı saxtalaşdırılmasının qarşısının alınması idi. Əylətliliyin məqsədi isə istənilən zaman səlahiyyətli şəxslərin informasiyaya və resurslara girişinin təmin edilməsi idi.

İnternet yaranana qədər, ənənəvi təhlükəsizlik modelləri və mexanizmləri qapalı hesablama sistemləri üçün nəzərdə tutulmuşdur və əsasən sistemin perimetri daxilində təhlükəsizliyini təmin edirdi. Bu zaman sistemin təhlükəsizlik perimetri daxilində ümumi təhlükəsizlik infrastrukturunu və təhlükəsizlik siyasəti istifadə edilirdi.

Lakin bu gün İnternetin geniş istifadəsi, şəbəkələrin funksionallığının genişləndirməsi, infrastrukturunun dəyişməsi, dinamikliyi, istifadə edilən texnologiyaların müxtəlifliyi ənənəvi mono-texnoloji təhlükəsizlik paradigmasının istifadəsini qeyri-mümkün edir və şəbəkələrə inamı azaldır. Çünki bu gün şəbəkə təhlükəsizliyində əsaslı trendlər baş verir [1]. Buna görə də, mövcud şəbəkə infrastrukturuna və şəbəkələrin funksionallığına müvafiq olaraq yeni şəbəkə təhlükəsizliyi paradigmasının yaradılması və şəbəkələrin təhlükəsizliyinə inamın artırılması və bunun üçün multi-texnoloji təhlükəsizlik paradigmasının yaradılması çox aktual məsələdir.

İnam (ing. trustworthy) bir konsepsiya olaraq təhlükəsizliklə bərabər şəbəkələrin gözlənilən (normal) fəaliyyətinə təminat verən dayanıqlıq və digər xüsusiyyətləri əhatə edir. İnamlı şəbəkə termininin mənası Avropa Birliyinin FP7 tədqiqat proqramında daha dəqiq göstərilmişdir və şəbəkənin inamlı qəbul edilməsi üçün o, təhlükəsiz, hücumlara və dayanmalara qarşı etibarlı və dayanıqlı olmalıdır [2]. Bundan başqa, xidmət keyfiyyəti təmin olunmalıdır, kofidensiallıq təmin edilməklə istifadəçi verilənləri mühafizə edilməlidir və bunun üçün istifadəçilərin verilənlərin təhlükəsizliyinin idarə edilməsində iştirakı üçün faydalı və etibarlı alətlər təmin edilməlidir.

Təqdim edilən məqalənin əsas məqsədi müasir şəbəkə təhlükəsizliyi və inam məsələlərinin analizidir.

II. ŞƏBƏKƏ TƏHLÜKƏSİZLİYİ VƏ İNAM

Ümumiyyətlə, şəbəkə təhlükəsizliyi və inam həm şəbəkə istifadəçilərinin, həm də şəbəkə infrastrukturunun təhlükəsizlik və inam məsələlərini əhatə edir. İstifadəçilərin təhlükəsizliyi və inam məsələləri insanların şəxsi həyatının mühafizəsi, mobil xidmətlərin təhlükəsizliyi, verilənlərin və təhlükəsizlik siyasətinin menecmenti əhatə edir. Şəbəkə infrastrukturunun təhlükəsizliyi və inam məsələləri ziyankar proqramların aşkar edilməsi və aradan qaldırılması, müdaxilələrin aşkarlanması və qarşısının alınması, şəbəkələrə və avadanlıqlara inam, proqram təminatının təhlükəsizliyi, xüsusi təyinatlı sistemlərin təhlükəsizliyi və təhlükəsiz əməliyyat mərkəzlərinin yaradılmasını əhatə edir. Lakin bu iki sinif məsələlər bir-biri ilə sıx bağlıdır və çox zaman ikinci sinif məsələləri həll etmədən birincini həll etmək qeyri-mümkündür.

Müasir şəbəkə təhlükəsizliyinin analizi göstərir ki, kiberhücumların trendi, əsasən, tətbiq səviyyəsi hücumları,

sosial mühəndislik, hədəf hücumları, informasiyanın sızması və daxili istifadəçi hücumları, şifrləmə, IPv6 hücumları, bulud hesablamaları və sosial şəbəkə hücumlarından ibarətdir. Demək olar ki, bu gün şəbəkə təhlükəsizliyi sahəsində baş verən başlıca trend ondan ibarətdir ki, hücumlar, əsasən, şəbəkə infrastrukturunun və ya qovşaqlarının sıradan çıxarılmasına deyil, informasiyanın (verilənlərin, məsələn, korporativ, fərdi və s. verilənlərin) əldə edilməsinə yönəlmişdir. Şəxsi həyatın toxunulmazlığına və verilənlərin oğurlanmasına yönəlmiş hücumlar əsas təhlükəsizlik trendlərinə aid edilir. Təhlükəsizliyin təmin edilməsində əsas yanaşma sistemin təhlükəsizliyi ilə bərabər informasiyanın (verilənlərin) təhlükəsizliyinin təmin edilməsindən ibarətdir [1]. Bu gün demək olar ki, əsas hücum hədəfi İnternetdə istifadə edilən yeni xidmətlərdir, xüsusilə də bulud hesablamaları, əşyaların İnterneti, sosial şəbəkə və s. xidmətlərdir.

Bulud hesablamaları xidmətlərinin təhlükəsizliyi və inam. Bulud hesablamaları proqramlaşdırma metodologiyalarının, verilənlər bazası texnologiyalarının, kommunikasiya şəbəkələrinin və İnternetin integrasiyasından ibarət olan yeni bir sahədir və sorğu əsasında istifadəçilərə resursların verilməsini təmin edir. Bu gün bulud hesablamaları artıq vacib şəbəkə xidmətinə çevrilmişdir. Müəssisə və təşkilatlar xərcləri azaltmaq və effektivliyi artırmaq üçün işlərini bulud hesablamaları mühitinə keçirirlər. Bu və ya digər bulud hesablamaları xidmətinin seçilməsi zamanı təhlükəsizlik və inam faktorlarının nəzərə alınması çox vacibdir.

Bulud hesablamaları xidmətləri resursların geniş miqyasda ümumi istifadəsini və qarşılıqlı əlaqəni təmin edir. Buna görə də təhlükəsizlik bulud hesablamaları xidmətləri infrastrukturunun çox vacib elementi sayılır, çünki bu mühitə giriş idarə edilməli və təhlükəsiz fəaliyyət təmin olunmalıdır. Həmçinin, bulud hesablamaları mühitində xidmət alan və xidmət göstərən bir-birinə inamı olmalıdır və bu əsas məsələlərdən biridir.

Bulud hesablamaları müxtəlif lokal sistemlərdən təşkil olunduğu və tərkibinə müxtəlif mühitlərdən elementlər daxil olduğu üçün buludda təhlükəsizliyin təmin edilməsi çətinləşir. Bir tərəfdən təhlükəsizlik mexanizmi istifadəçilərin təhlükəsizliyinə zəmanət verməlidir, digər tərəfdən isə istifadəçilərin işində çətinlik yaratmamaq üçün o qədər mürəkkəb olmamalıdır. Beləliklə, təhlükəsizlik və rahatlıq arasında müəyyən balans olmalıdır. Etibarlı və təhlükəsiz hesablama təhlükəsizlik və məxfilikdən başqa, həmçinin həqiqilik, əlyetərlik, və bütövlük daxildir [3]. Bulud hesablamaları təhlükəsizliyi mexanizmlərinin geniş imkanlara malik olmasına baxmayaraq, müəyyən çatışmazlıqları mövcuddur. Məsələn, bulud hesablamaları sistemində aparat səviyyəsində etibarlı hesablamanı dəstəkləyən mexanizmlər yoxdur. Həmçinin bulud hesablamaları mühitində inamın əsası dəqiq müəyyən olunmayıb və sertifikatların yaradılması və mühafizəsi o qədər təhlükəsiz deyil. Digər tərəfdən, istifadəçilərin fəaliyyətinin monitorinqi mexanizmi yoxdur [4].

Şəbəkə səviyyəsində təhlükəsizlik təmin edilərkən açıq (public) və xüsusi (private) buludları fəraləndirmək çox vacibdir. Əgər xüsusi buludların xidmətlərinə yeni hücumlar yosdursa və onlarda boşluqlar müəyyən edilməyibsə, onda onun topologiyasının dəyişdirilməsinə ehtiyac yoxdur. Lakin açıq bulud xidmətlərinin istifadəsi zamanı təhlükəsizlik tələblərinin dəyişməsi şəbəkənin topologiyasının dəyişdirilməsini tələb edir.

Host səviyyəsində təhlükəsizliyin təmin edilməsi və risklərin qiymətləndirilməsi zamanı həm xidmət növləri (SaaS (Software as a service), PaaS (Platform as a Service), və IaaS (Infrastructure as a service)), həm də buludların növləri (açıq (public), xüsusi (private) və hibrid) nəzərə alınmalıdır. Bu zaman SaaS və PaaS xidmətlərində hostların təhlükəsizliyi bulud xidmətlərini göstərən provayder tərəfindən həyata keçirilməlidir. Lakin IaaS xidmətində isə təqdim edilmiş hostların təhlükəsizliyinə kliyentlər cavabdehirlər [5].

Bulud xidmətlərinə inamın qiymətləndirilməsi sahəsindəki tədqiqatların nəticələri bulud xidmətlərinə inamı tam şəkildə qiymətləndirməyə imkan vermir. Çünki müxtəlif tədqiqatçılar bulud xidmətlərinə inamı qiymətləndirmək üçün müxtəlif atributlar istifadə edirlər [6]. İnəmə müşahidə olunan faktlara və sübutlara əsaslanan subyektiv bir konsepsiyadır. Təşkilatlardan asılı olaraq bulud xidmətlərinə inamın tərfi dəyişir [7].

IoT təhlükəsizliyi və inam. Bu gün IoT təbiiqləri demək olar ki, insan həyatının bütün sahələrində, məsələn, səhiyyədə, binaların və ev təsərrüfatının avtomatlaşdırılması, ətraf mühitin monitorinqi, enerji və nəqliyyat infrastrukturunun idarə edilməsi və s. sahələrdə mövcuddur və onların fəaliyyətində çox vacib rol oynayır. IoT-un inkişafının geniş yayılmasının əsas səbəbi naqilsiz şəbəkə texnologiyalarının (məsələn, RFID (Radio Frequency Identification – Radiotezlik əsasında identifikasiya), WiFi, 4G, IEEE 802.15.x) mikroelektronikanın və s. sahələrin sürətlə inkişafı oldu [8]. Artıq 2020-ci ilə IoT-a qoşulmuş naqilsiz qurğuların sayı 26 milyarda çatacağı proqnozlaşdırılır [9]. Lakin çoxlu sayda avtonom sistemlərin IoT təbiiqləri vasitəsilə İnternetə qoşulması geniş miqyasda və diapazonda təhlükəsizlik problemləri yaradır, xüsusilə də fərdi məlumatların mühafizəsi ilə bağlı ciddi problemlər yaradır [10]. IoT qurğularının inamsız İnternet vasitəsi ilə qarşılıqlı əlaqəsi təhlükəsizlik sahəsində yeni problemlərin yaranmasına gətirib çıxarır. Məsələn, hər-hansı IoT qurğusunun təhlükəsizliyinin pozulması digər sistemlərə hücum edilməsinə imkan verir və bu da həm fiziki aləmdə (insanların fiziki təhlükəsizliyi), həm də virtual aləmdə (İnternetdə) insanlara ziyan vurulması üçün istifadə edilə bilər. Fərdi məlumatlara icazəsiz giriş, onların sızmasına və bəd niyyətlərlə istifadə edilməsinə gətirib çıxara bilər. Ənənəvi təhlükəsizlik mexanizmləri müəyyən problemləri həl etməyə imkan verir, lakin IoT-un təhlükəsizliyi ilə bağlı xüsusi aspektlər mövcuddur və onlar IoT-un təhlükəsizliyinin təmin edilməsi üçün geniş və bütöv yanaşma tələb edirlər. Çünki IoT qurğuları

adətən naqilsiz əlaqədən istifadə edir və bu da təhlükələr yaradır.

IoT qurğular müxtəlif naqilsiz əlaqə vasitəsi ilə (məsələn, Wireless Sensor Network (WSN), Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA), Bluetooth və Wi-Fi) qoşulduğu üçün IoT-un təhlükəsizlik məsələləri də fərqlənir [11].

.Sosial şəbəkə xidmətlərinin təhlükəsizliyi və inam. Sosial şəbəkə xidmətləri (SŞX) İnternetdə insanların müəyyən maraqlar və ya fəaliyyət çərçivəsində onlayn icmalarının yaradılmasına yönəlmişdir. SŞX insanlara bir-biri ilə əlaqə yaratmağa və informasiya mübadiləsi etməyə imkan verir. Hal-hazırda İnternetdə çoxlu sayda SŞX mövcuddur. Bununla yanaşı, SŞX istifadəçilərin şəxsi həyatının toxunulmazlığı və informasiya təhlükəsizliyi ilə bağlı yeni problemlər yaradır. Yəni SŞX-nin yaranması İnternet mühitində təhlükəsizlik risklərinin artmasına gətirib çıxarmışdır. Bu risklər ziyanlı proqramların və spamların yayılması, sosial mühəndislik və sosial şəbəkə hesablarına hücumların həyata keçirilməsi, eləcə də, izləmə, aldatma, şantaj, qarayaxma və s. kimi müxtəlif aspektli təhlükələrlə bağlıdır [12].

SŞX-də inam informasiya mübadiləsi və yeni münasibətlərin yaradılması üçün həlledici faktordur. SŞX-ə inam bir tərəfin, digər tərəfin əməllərinə qarşı həssas olması ilə müəyyən edilir. Yəni nəzarət imkanından asılı olmayaraq, bir tərəf digər tərəfdən inamlı şəxsə xas olan əməllər gözləyir [13].

NƏTİCƏ

Məqalə müasir şəbəkə təhlükəsizliyi və inam məsələlərinin analizinə həsr olunmuşdur. Müasir şəbəkələr, xüsusilə İnternet infrastrukturunu həm texnoloji, həm də xidmət müxtəlifliyi baxımından çox dəyişmişdir. Bununla yanaşı yeni təhlükələr və hücum növləri meydana çıxmışdır və nəticədə təhlükəsizlik məsələlərinin həlli çox mürrəkkəblişmişdir və şəbəkələrə inam azalmışdır. Bu şəraitdə mövcud təhlükəsizlik paradqlmaları o qədər də effektiv deyil və buna görə də yeni təhlükəsizlik paradqlmalarının yaradılması aktual məsələdir.

ƏDƏBİYYAT

- [1] Şıxəliyev R.H. Müasir kompüter şəbəkələrinin təhlükəsizlik trendləri haqqında // İnformasiya cəmiyyəti problemləri, 2015, №: 2, s. 82-86.
- [2] <http://cordis.europa.eu/fp7/ict/security/>
- [3] Avizienis A., Laprie J.-C., Randell B., and Landwehr C. Basic Concepts and Taxonomy of Dependable and Secure Computing // IEEE

transactions on dependable and secure computing, 2004, vol.1, no.1, pp. 11-33.

- [4] Shen Z., Li L., Yan F., Wu X. Cloud Computing System Based on Trusted Computing Platform / Proceedings of the International Conference on Intelligent Computation Technology and Automation, 2010, pp. 942-945.
- [5] Mather, T., Kumaraswamy, S., Latif, S.: Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc., 2009.
- [6] Pandey S., Daniel A.K. Fuzzy Logic Based Cloud Service Trustworthiness Model / Proceedings of the 2nd IEEE International Conference on Engineering and Technology (ICETECH), 2016, pp. 73-78.
- [7] Edward A. , et al. A process-oriented methodology for assessing and improving software trustworthiness / Proceedings of the 2nd ACM Conference on Computer and communications security. ACM, 1994, pp. 39-50.
- [8] Atzori L., Iera A., Morabito G. The Internet of Things: A Survey // Computer Networks 2010, vol. 54, pp. 2787-2805.
- [9] Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020; Gartner Inc.: Stamford, CT, USA, 2013.
- [10] Federal Trade Commission. Internet of Things – Privacy and Security in a Connected World; FTC: Seattle, WA, USA, 2013. 8. Şıxəliyev , R.H. Sosial şəbəkələrdə təhlükəsizlik problemləri // İnformasiya Cəmiyyəti Problemləri, 2016, № 2, s. 80-88.
- [11] Şıxəliyev R.H. Sosial şəbəkələrdə təhlükəsizlik problemləri // İnformasiya Cəmiyyəti Problemləri, 2016, № 2, s. 80-88.
- [12] Shin D.-H. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption // Interacting with Computers 2010, vol. 22, no. 5, pp. 428-438.
- [13] Baig Z.A. Securing the internet of things infrastructure – standards and techniques / Proceedings of the Australian Information Security Management Conference, 2014, pp. 75-81.

MODERN NETWORKS SECURITY AND TRUSTWORTHINESS

Ramiz Shikhaliyev

Institute Information Technology ANAS, Baku, Azerbaijan
ramiz@science.az

Abstract – The article analyzes modern network security and trustworthiness issues. Basically, the security and trustworthiness issues of the new network services available on the Internet have been analyzed. In particular, cloud computing, Internet of things and social networking services have been analyzed.

Keywords – network security, network services, cloud computing, Internet of things, social network services

Proqram təminatının təhlükəsizliyinin təmin olunmasının bəzi üsulları haqqında

Şəfəqət Mahmudova

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

shafagat_57@mail.ru

Xülasə— Bu işdə proqram təminatının təhlükəsizliyi və s. haqqında məlumat verilmişdir. Proqram təminatının təhlükəsizliyinin təmin olunmasının analiz metodları öyrənilmişdir. Proqram təminatının qorunması üçün vacib olan problemlər müəyyən edilmişdir. Proqram layihələri üçün risklər, onların idarə olunması, təyin olunması, kateqoriyaları və s. araşdırılmışdır.

Açar sözlər—proqram təminatı, təhlükəsizlik, analiz metodları, risklər

I. GİRİŞ

Müasir dövrdə informasiya cəmiyyəti inkişaf edərək getdikcə daha böyük vüsət alır. Kompüterlər cəmiyyətdəki bütün proseslərə, o cümlədən elmi-tədqiqat işlərinə, iqtisadiyyata təsir göstərərək, ümumilikdə insanın fəaliyyət formasını dəyişdirir və yeni sahələrin yaranmasına səbəb olur. İnsanların yeni texnologiyaları öyrənməsi və onu müxtəlif sahələrə tətbiq etməsi yeni sistemlərin və proqram təminatının (PT) yaranmasına və inkişafına səbəb olur.

Müasir dövrdə terrorizm və cinayətkarlara qarşı mübarizə kəskin surətdə artmışdır. Bütün dünyanı bürümüş terror aktlarının dalğası aşkarlayıcı və önləyici təhlükəsizlik sistemlərinin və proqram təminatının təkmilləşdirilməsi ehtiyacını yaratmışdır.

Əksər dövlətlərdə qarşıda duran əsas məsələlərdən biri qaçaqmalçılıq, terror aktlarının qarşısının alınması və müxtəlif sistemlərin yaradılması üçün yeni yanaşmaların, yeni prinsiplərin təşkilinə imkan vermək və milli təhlükəsizlik, beynəlxalq səviyyədə integrasiyalar və s. üzrə PT mərkəzlərinin yaradılmasıdır.

Axtarışın, aşkar etmənin və şəxsiyyətə, cəmiyyətə və dövlətə qarşı cinayətlərin təşəbbüskarlarının identifikasiyası sisteminin təkmilləşdirilməsi, bütövlükdə, xüsusi əhəmiyyət kəsb edir. Belə məsələlərin həlli qlobal miqyasda yeni yanaşmalar və ən müasir texnologiyaların tətbiqini tələb edir. Araşdırma və ya operativ-axtarış fəaliyyəti çərçivəsində alınmış istənilən dəlil real vaxt müddətində effektiv istifadə edilməlidir [1].

Milli zəmində hüquq-mühafizə sistemi, dövlət təhlükəsizliyi sisteminin və ölkənin müdafiə təminatı orqanlarının qarşısında duran məsələlərin geniş spektrini həll etməyə imkan verir:

- Potensial olaraq qeyri-qanuni işlər və təhlükəli

əməllərin (vətəndaşların həyatı, dövlət qurumları və s.) həyata keçirilməsində şübhəli bilinənlərin və ya günahkarların axtarışı;

- Hadisələrin iştirakçılarının tapılması və aşkar edilməsi hüquq-mühafizə, dövlət təhlükəsizliyi və ölkənin müdafiəsinin təminatı sistemlərinin əsas məsələlərindən biridir;
- Dövlət səviyyəsində bu məsələlərin uğurla həlli artıq müasir proqram təminatlarından istifadə etməklə mümkündür;
- Multimedia məlumatlarının (şəkillər, videoyazılar və s.) yığılması və saxlanması üçün paylanmış sistemin yaradılması mühüm əhəmiyyət kəsb edir;
- İstintaq fəaliyyəti və operativ-axtarış tədbirləri prosesində yığılmış məlumatlar əsasında yaradılmış bazalarda şübhəli şəxslərin interaktiv axtarışının həyata keçirilməsi vacibdir və s.

Proqram təminatının hazırlanması prosesi (ing. Software development process)—ilk növbədə proqram təminatının hazırlanması üçün razılaşdırılmış strukturun işlənməsidir [2].

Proqram təminatının yaradılması zamanı alqoritmın effektiv işlənməsi və verilənlərin strukturunun düzgün müəyyən edilməsi əsas rol oynayır. Məsələnin alqoritmı və verilənlərin strukturunu effektivliyə təsir edən əsas aspektlərdir. Beləki, sonradan verilənlərin strukturunu dəyişmək alqoritmı dəyişməkdən daha çətindir.

Böyük paylanmış sistemlərin tərtibində əksər hallarda bir neçə proqramlaşdırma dillərindən istifadə olunur ki, bu da müəyyən çətinliklərin əmələ gəlməsinə səbəb olur. Yəni belə hallarda təhlükəsizlik təmin olunmur [3].

Proqram təminatının təhlükəsizliyi dedikdə onun müdafiəsinə yönəldilmiş tədbirlər kompleksi başa düşülür.

Bu baxımdan proqram təminatının təhlükəsizliyinin təmin olunması üsullarının araşdırılması xüsusi əhəmiyyət kəsb edir.

Proqram təminatının istismarında da təhlükəsizliyin təmin olunması vacib məsələlərdən biridir.

II. PROQRAM TƏMINATININ QORUNMASININ PROBLEMLƏRİ

Proqram təminatının təhlükəsizliyi dedikdə müxtəlif problemlər (xətalər, səhvlər və s.) meydana çıxmadan onun işləmək xüsusiyyəti başa düşülür. PT-nin qorunması

məsələlərini tədqiq edərkən aşağıdakı problemləri diqqətə almaq lazımdır [4]:

- PT-nin icrası zamanı xətalara aşkarlanması;
- Xətalara meydana çıxmasına zəmin yaradan subyektlərin araşdırılması;
- Mövcud proqram xətalının sayının müəyyən edilməsi;
- Proqram xətalının proqram səhvlərindən fərqləndirilməsi;
- PT-nin istismarı zamanı dağıdıcı proqram vasitələrinin aktivləşməsi nəticəsində ehtimal edilən nəticələrin müəyyənəşdirilməsi və s.

İnformasiyanın təhlükəsizliyinə təhdidlər PT-nin istismarı prosesində yaranır. Hal-hazırda kompüter sistemlərində informasiyaya zərərli təsirlərdən biri ən təhlükəli vasitələr sayılan viruslar olur. PT-lər inkişaf etdikcə virusların da növü artır. Son illər ərzində kompüter virusları həm avadanlıqlara, həm də proqram təminatına çox böyük ziyan vurmuşdur. Belə ziyanların ölçüsü milyon dollarlardır. 21 noyabr 1988-ci ildə ən təhlükəli olan Morris virusu 24 saat ərzində ARPANET şəbəkəsini sıradan çıxarmışdır. Şəbəkənin işlək vəziyyətə salınması üçün milyon dollarla pul xərclənmişdir.

PT-nin texnologiyası təhlükəsizliyi modelinin yaradılması infosferada təhlükəsizliyin ümumiləşdirilmiş konsepsiyasına əsaslanmalıdır [5]. Bunun üçün aşağıdakı məsələlərə diqqət yetirmək lazımdır:

- PT-nin texnologiyası təhlükəsizliyi probleminin praktik həlli üçün onun nəzəri əsaslarının işlənilməsi;
- təhlükəsiz informasiya texnologiyalarının yaradılması;
- kompüter infosferasının təhlükəsizliyinin təmin edilməsi üçün nəzarət sisteminin genişləndirilməsi.

III. PROQRAM TƏMINATININ TƏHLÜKƏSLİYİNİN TƏMİN OLUNMASININ ANALİZİ METODLARI

PT-nin təhlükəsizliyinin təmin olunmasında müxtəlif analiz metodlarından istifadə olunur. Bu metodlar müxtəlif funksiyaları yerinə yetirirlər. Analiz metodlarının bəziləri şəkil 1-də göstərilmişdir [6].

Şəkil 1. PT-nin təhlükəsizliyinin təmin olunması metodları

Nəzarət-sınaq metodları vasitəsilə proqramın icra prosesinə nəzarət edilir. Bu metodlar geniş yayılmışdır, çünki onlar formal analiz tələb etmirlər, cari texniki və proqram vasitələrindən istifadə etməyə icazə verirlər, qısa müddət

ərzində hazır metodikaların yaradılmasına imkan yaradırlar [7].

Məntiqi-analitik metodların köməyi ilə təhlükəsizliyin analizi vaxtı proqramın modeli qurulur və tədqiq edilən proqramın modelinin və qrupda olan PT-nin modelinin ekvivalentliyi rəsmi sübut edilir [8]. Proqramın modeli kimi ən sadə halda onun maşın kodu (bitlərlə) ola bilər və proqramda virusların olmasını onların hücum siqnaturlarını tapmaqla sübut etmək olar. Hücum siqnaturu — kompüter virusunun xüsusiyyətləridir [8]. Daha çox formal modellərdən istifadə edilir.

PT-nin analiz prosesinə aid modellər [10] şəkil 2-də göstərilmişdir.

Leksik verifikasiyalı analiz modeli axtarış, tanıma və icra edilən kodlarda təqdim edilmiş proqramın obyektlərinin müxtəlif leksemlərinin təsnifatını tədqiq edir. Leksem — translyator üçün məna daşıyan proqramlaşdırma dilinin mümkün simvollarının ardıcılığıdır [11]. Bu halda leksemlər siqnaturalardır.

Hazırda siqnaturaların axtarışı aşağıdakı qruplarda həyata keçirilir:

1. virusların siqnaturaları;
2. proqram təminatı sistemlərinin elementlərinin siqnaturaları;
3. "şübhəli funksiyaların" siqnaturaları.

Şəkil 2. PT-nin analiz prosesi modelləri

Sintaksis verifikasiya analizi modeli axtarış, tanıma və PT-nin sintaksis strukturlarının təsnifatı hesab edir, proqramın özünün strukturuna uyğun alqoritmin qurulmasıdır.

Semantik analiz - kompüterin əməliyyat sistemində PT-nin funksiyalarının (prosedurlarının) mənasını öyrənməklə onun tədqiqini həyata keçirir. Statik tədqiqata əsaslanan analizin əvvəlki növlərindən fərqli olaraq semantik analiz proqramın dinamikasının öyrənilməsinə yönəlmişdir. Semantik analiz modeli analizin ən effektiv növüdür, bu həm də çox zəhmət tələb edir.

PT-nin təhlükəsizliyinin təmin olunması prinsipləri aşağıda qeyd olunmuşdur:

- etalon proqram vasitələrinin girişinə məhdudiyyətlərin qoyulması, onlarda dəyişikliklərin edilməsinə icazənin verilməməsi;
- xətalı proqramın tam skan edilməsi və profilaktik məqsədlə testin yerinə yetirilməsi;
- PT-nin istismara verildiyi andan ona nəzarət edilməsi və təhlükəsizliyi baxımından identifikasiyasının həyata keçirilməsi;
- PT-nin istismarı zamanı strukturu dəyişmədən onun ayrı-ayrı modullarının əvəz edilməsinin təmin edilməsi;
- müşayiət edilən bütün proqram vasitələrinin ciddi uçotunun və kataloqlaşdırılmasının həyata keçirilməsi;
- bütün proseslər, işçi əməliyyatlar, PT-nin funksionallığı haqqında olan informasiyanın statistik analizinin aparılması;
- PT-nin qorunması məqsədilə informasiya təhlükəsizliyinin yeni, gözlənilməz təhlükələrinin üzə çıxardılması halında əlavə vasitələrin tətbiq edilməsi;
- və s.

Proqram təminatının təhlükəsizliyinin təmin olunması üçün xətalardan aşkar edilməsinin və qüsurların aradan qaldırılmasının avtomatlaşdırılmış metodu haqqında məlumat [12]-də verilmişdir. İşdə PT-də qüsurların aşkar edilməsi və bərpası ilə bağlı metodlar təhlil edilmişdir.

IV PROQRAM LAYİHƏLƏRİ ÜÇÜN MÜMKÜN RİSKLƏR

Onlayn rejimdə işləyən proqramların təhlükəsizliyinin təmin olunması vacib məsələlərdən biridir. Proqram təminatının təhlükəsizliyinin təmin olunmasında risklər əsas rol oynayır [13]. Layihə üçün risklər layihənin icrası üçün lazım olan işlərin qrafikinə və ya resurslarına təsir edirlər.

Proqram layihələri üçün mümkün risklərin bəziləri və onların idarə olunması və kateqoriyaları aşağıda qeyd edilmişdir [14, 15]:

- İşlənən proqram məhsulları üçün risklər;
- Təşkilatda istehsalçıya aid olan biznes risklər.

Risklərin idarə olunması.

- Risklərin təyini. Layihə, hazırlanan məhsul və biznes üçün mümkün risklər təyin edilir;
- Risklərin analizi. Təhlükəli vəziyyətlərin yaranması ehtimalı risklərinin ardıcılığı qiymətləndirilir;
- Risklərin planlaşdırılması. Risklərin qarşısının alınması və ya layihəyə onların təsirinin minimallaşdırılması üzrə tədbirlər planlaşdırılır;
- Risklərin monitorinqi. Risklərin ehtimallarının daima qiymətləndirilməsi və təhlükəli vəziyyətlərin təzahürünün nəticələrinin azalması üzrə tədbirlərin icra edilməsi.

Risklərin mümkün kateqoriyalarının siyahısı aşağıda göstərilmişdir:

- Texnologiya risklər. Sistemin işlədiyi proqram və aparat texnologiyalarında axtarılırlar;
- Personalla bağlı risklər. İstehsalçılar komandasının üzvləriylə bağlıdır;

- Təşkilati risklər. Layihənin yerinə yetirildiyi təşkilatın mühitində baş verir;
- Instrumental risklər. CASE-vasitələrdən istifadə etməsi və PT-nin təşkili prosesini dəstəkləməsilə əlaqədardır;
- Sistemin tələbləriylə bağlı risklər. İşlənən sistemə qoyulan tələblərlə bağlı risklər ola bilər;
- Qiymətləndirmənin riskləri. Layihənin reallaşdırması üçün lazım olan proqram sisteminin və resursların xarakteristikalarının qiymətləndirilməsiylə bağlıdır. Risklərin analizi.
- Risklərin qarşısının alınmasının strategiyaları. Bu strategiyalara əsasən risklərin təzahürünün ehtimalını aşağı salan tədbirləri həyata keçirtmək lazımdır. Nümunə olaraq, potensial qüsurlu komponentlərin xaric edilməsi strategiyasını göstərmək olar;
- Strategiyanın minimallaşdırılması. Risklərlə bağlı mümkün zərərin azaldılmasına yönəldilmişdir. Məsələn, istehsalçıların komanda üzvlərinin xəstəliyi ilə əlaqədar zərərin azaldılması strategiyasını göstərmək olar;
- "Qəzalı" vəziyyətlərin planlaşdırılması. Bu strategiyalara əsasən tədbirlər planına malik olmaq lazımdır. Belə ki, təhlükəli vəziyyətin təzahürü halında onu yerinə yetirmək lazımdır.

NƏTİCƏ

İşdə proqram təminatının qorunmasının problemləri araşdırılmışdır. Proqram təminatının təhlükəsizliyinin təmin olunmasının analizi metodları öyrənilmişdir. Proqram layihələri üçün mümkün risklərin bəziləri, onların idarə olunması və kateqoriyaları qeyd edilmişdir.

Təvsiyə olunur ki, PT-nin təhlükəsizliyinin təmin edilməsi üçün kriptografiyanın imkanlarından istifadə olunsun. Bu PT-nin etibarlılığının yüksəlməsinə səbəb ola bilər. İnformasiyanın məxfiliyinin pozulması PT-nin təhlükəsizliyinin pozulmasına imkan yaradır. Buna görə məxfi məlumatların emalı prosesində informasiyanın qəbulu və siqnalın işlənməsi tədqiqatların dərinləşməsinə səbəb olur və bu da bu tipli məsələlərin aktuallığını bir daha sübut edir.

ƏDƏBİYYAT

- [1] Для защиты информации предлагается применять технологии распознавания лиц, Information Security journal, 29.10.2008. http://www.itsec.ru/newstext.php?news_id=51127#sthash.HQGrMBJh.dpuf.
- [2] В. В. Бахтизин, Л. А. Глухова, «Технология разработки программного обеспечения», Минск: БГУИР, 2010, 267 с.
- [3] Ю.Ю. Громов, О.Г. Иванова М.П., Беляев, Ю.В. Минин, «Технология программирования», ФГБОУ ВПО «ТГТУ». 2013, 172 с.
- [4] Кадан А.М. «Методология и технология программирования», http://mf.grsu.by/Kafedry/kaf001/academic_process/048/28
- [5] А.И. Ефимов, Б.П. Пальчун, «О технологической безопасности компьютерной инфосферы», Вопросы защиты информации, 1995, №3(30), с. 86-88.
- [6] В. Казарин, «Безопасность программного обеспечения компьютерных систем», Москва: МГУЛ, 2003, 212 с.
- [7] Методы анализа безопасности программного обеспечения, https://studbooks.net/2043842/informatika/metody_analiza_bezopasnosti_programmnogo_obespecheniya

- [8] С. А. Середя, Программно-аппаратные системы защиты программного обеспечения. ЭР, <http://www.ase.md/~osa/publ/ru/pubru427.html>.
- [9] Сигнатура, <https://ru.wikipedia.org/wiki/Сигнатура>
- [10] В. В. Яценко, «Введение в криптографию», М.:МЦНМО: «ЧеРо», 2003, 272 с.
- [11] Лексема, <https://ru.wikipedia.org/wiki/Лексема>
- [12] J. Jeessoo, K. Taeun, K. Hwankuk, “An Automated Vulnerability Detection and Remediation Method for Software Security”, International journal of wireless information networks, 2018, vol. 10, issue 5, pp. 117-129.
- [13] M. Mihailescu, S. Nita, M. Pirloaga, “Software security techniques: risks and challenges” Mircea cel Batran Naval Academy Scientific Bulletin, 2016, vol. 19, issue 1, 8 p.
- [14] V. Georg, “Winning With Open Process Innovation. MIT”, Sloan management review, 2018, vol. 59, pp. 53-56.
- [15] Л. Тимоти, Основные риски проекта по разработке программного обеспечения, <https://econ.wikireading.ru/78462>

**ABOUT SOME METHODS FOR ENSURING
SOFTWARE SECURITY**

Shafagat Mahmudova

Institute of Information Technology of ANAS, Baku,

Azerbaijan

shafagat_57@mail.ru

Abstract -- This paper provides information about software security. Methods of analysis of software security have been studied. The problems that are important to protect software have been identified. Risks for software projects, their management, assignment, categories and so on. studied.

Keywords -- software, security, analysis methods, risks

Ali məktəblərdə kibertəhlükəsizlik üzrə mütəxəssis hazırlığı problemləri

Yadigar İmamverdiyev

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

Xülasə— Məqalədə 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.

Açar sözlər— informasiya təhlükəsizliyi, kibertəhlükəsizlik, təhsil standartı, peşə standartı, kurikulum

I. GİRİŞ

Kibertəhlükəsizliyin etibarlı təmin edilməsi bütün ölkələr üçün prioritet məsələdir və bu məsələnin həllində əsas elementlərdən biri kibertəhlükəsizlik sahəsində yüksək ixtisaslı, öz biliklərini real şəraitdə tətbiq etməyə və yeni meydana çıxan kibertəhdidlərə çevik cavab verməyə qabil mütəxəssislərin hazırlanmasıdır. Hazırda əmək bazarında kibertəhlükəsizlik üzrə mütəxəssislərə böyük tələbat vardır [1]. Elektron xidmətlərin inkişafı, kiber-qoşunların formalaşdırılması, kiber-təhlükəsizlik sənayesinin qurulması, 4-cü sənaye inqilabının gətirdiyi yeni texnologiyalar bütün ölkələrdə belə mütəxəssislərə kəskin tələbat vardır.

Azərbaycan Respublikasında da kibertəhlükəsizlik sahəsində ali təhsilli mütəxəssislərin hazırlığı aktualdır və bu sahədə əlaqədar qurumlar tərəfindən müəyyən addımlar atılır. Qeyd etmək lazımdır ki, kibertəhlükəsizlik sahəsində universitetlərdə mütəxəssis hazırlığı sisteminin formalaşdırılması məsələlər kompleksinin həllini tələb edir: müvafiq peşə və təhsil standartlarının, təhsil proqramlarının hazırlanması, müasir tələblərə cavab verən müvafiq maddi-texniki bazanın yaradılması, müvafiq dərslərin və onlayn təhsil resurslarının yaradılması, elmi-pedaqoji kadrların hazırlanması, ali təhsil müəssisələrinin akkreditasiyası sisteminin yaradılması və s.

Bu məsələləri həll etmək üçün ilk addımlardan biri qabaqcıl dünya ölkələrində bu sahədə toplanmış təcrübənin analizidir. Təqdim olunan işdə kibertəhlükəsizlik sahəsində ali təhsilli peşəkar mütəxəssislərin hazırlanması problemlərinə baxılır.

II. KIBERTƏHLÜKƏSİZLİK ÜZRƏ KURRIKULUMLARIN ANALİZİ

Kompüter elmləri, proqram mühəndisliyi və informasiya texnologiyaları üzrə ali təhsil standartlarının hazırlanmasına ACM (Association for Computing Machinery) və IEEE-CS

(IEEE Computer Society) xüsusi töhfələr vermişdir. ACM informasiya təhlükəsizliyi üzrə bilik sahələrinin kompüter elmləri üzrə kurikulumuna daxil edilməsinə ilk dəfə cəhdlər etmişdi. Orta məktəbdən sonrakı təhsil səviyyələrində kibertəhlükəsizlik proqramları üçün kurikulum tövsiyələri (CSEC) 2017-ci ildə işlənmişdir [2].

CSEC2017 kurikulumu

CSEC2017 kurikulumu dörd təşkilatın nümayəndələrinin daxil olduğu işçi qrup tərəfindən işlənmişdir:

- ACM
- IEEE-CS (IEEE Computer Society)
- AIS (Association for Information Systems)
- IFIP WG 11.8 (International Federation for Information Processing).

CSEC2017 səkkiz əsas bilik sahəsi üzrə təşkil olunub: Verilənlərin təhlükəsizliyi; Proqram təminatının təhlükəsizliyi; Komponentlərin təhlükəsizliyi; Əlaqələrin təhlükəsizliyi; Sistemlərin təhlükəsizliyi; İnsanların təhlükəsizliyi; Təşkilatların təhlükəsizliyi; Cəmiyyətin təhlükəsizliyi. Kurrikulumda hər bir bilik sahəsi çərçivəsində tələbələrin bilməli olduqları spesifik əsas konsepsiyaların siyahısı verilir. Məsələn, Verilənlərin təhlükəsizliyi bilik sahəsində tələbələr baza kriptografiya, verilənlərin tamlığı və autentifikasiya kimi əsas konsepsiyaları bilmələrini nümayiş etdirməlidirlər. Əlaqələrin təhlükəsizliyi bilik sahəsində tələbələr birləşməyə və ötürməyə yönəlmiş hücumlar sahəsində bilik və bacarıqlara malik olmalıdırlar.

Daha detallı səviyyədə CSEC2017 əhatə edilməli mövzulara aid deskriptorlar verməklə müəllimləri kurs işləri işləməyə yönləndirir. Məsələn, Verilənlərin təhlükəsizliyi bilik sahəsində Giriş nəzarət əsas konsepsiyası çərçivəsində mövzu deskriptorlarında tələbələrin tanış edilməli olduqları giriş nəzarətin bir neçə növü sadalanır.

Bilik sahələri və əsas konsepsiyalar ilə birlikdə kurikulum fənləri başa düşmək üçün zəruri olan nəzəri və konseptual bilikləri, həmçinin bacarıqlar qazanmaq üçün praktiki tapşırıq imkanlarını da şərh edir.

CSEC2017 o faktı da əks etdirir ki, adətən, tələbələr kibertəhlükəsizlik ixtisasına Computing sahəsində beş əsas istiqamətdən birini öyrəndikdən sonra baş vururlar. Bu istiqamətlərə kompüter elmləri, kompüter mühəndisliyi,

informasiya sistemləri, informasiya texnologiyaları və proqram mühəndisliyi daxildir.

CSEC2017-nin Fənn profilləri (ing. Lens) bölməsi pedaqoqları tələbənin özək fənni əsasında kibertəhlükəsizlik üzrə kurs işinə yanaşmaya, kontentin dərinliyinə və təlim nəticələrinə təsir etməklə istiqamətləndirir.

NATO kibertəhlükəsizlik kurikulumu (*Cybersecurity: A Generic Reference Curriculum*) 2016-cı ildə hərbi akademiyalar və təhlükəsizlik sahəsində tədqiqat institutları üçün işlənmişdir [3]. Kurrikuluma aşağıdakı dörd mövzu daxildir:

Mövzu 1: Kiberfəza və kibertəhlükəsizliyin əsasları

Mövzu 2: Risk vektorları

Mövzu 3: Kibertəhlükəsizlik üzrə beynəlxalq təşkilatlar, prinsiplər və standartlar

Mövzu 4: Milli kontekstdə kibertəhlükəsizliyin menecmenti

Hər bir mövzu bloklara bölünür, təbii ki, bloklar da bölünə bilər. Məsələn, Mövzu 1 aşağıdakı bloklara bölünür:

- M1-B1: Kibertəhlükəsizlik və kiberfəza – giriş
- M1-B2: İnformasiya təhlükəsizliyi və risklər
- M1-B3: İnformasiya fəzasının strukturu: İnternetin magistral şəbəkəsi və dövlətin şəbəkə infrastrukturunu
- M1-B4: Protokollar və platformalar
- M1-B5: Şəbəkə təhlükəsizliyinin arxitekturası və təhlükəsizliyin təmin edilməsi proseslərinin idarə edilməsi

Bloklar ayrıca fənlərə bölünür. Hər bir fənn baza blokları çərçivəsində öyrənilir, onların da hər biri öz növbəsində mühazirələr, təqdimatlar, konkret senarilər üzrə çalışmalar və s. kimi tədris modullarına bölünə bilər. Baxılan kurikulumun yerli şəraitə uyğunlaşdırılması nəzərdə tutulduğu üçün əksər hallarda modulların və mühazirələrin konkret tərkibi verilmir, onlar yerli ehtiyacdən asılı olaraq detallandırılmalıdır. Bunun əvəzində, hər bir mövzuda müxtəlif bloklar əhatə olunur ki, onlar da əldə olunacaq məqsədləri və nəticələri tövsiyə edirlər.

Kurrikulum müəllifləri qeyd edirlər ki, kurikulum əsasında vahid kursun yaradılması zamanı xüsusi narahatlıq doğuran üç element olacaq: kursun məqsəd və vəzifələri; nəzərdə tutulan tələbələr, xüsusilə onların texniki bilikləri və işlərinin mahiyyəti; kursa ayrılan müddət. Bu üç element texniki detallandırmanın səviyyəsini və təlim çalışmalarının xarakterini (mühazirələr, misallar, təlim-tanışlıq səfərləri, hərbi oyunlar və s.) müəyyən etməlidir.

Kibertəhlükəsizlik kurikulumlarının dizaynı

Bəzi tədqiqatçılar informasiya təhlükəsizliyi kurikulumlarının dizayn edilməsinə yuxarıdan aşağıya yanaşmaya tərəfdar çıxırlar. Bu yanaşmada gələcək mütəxəssisin görəcəyi işin tipi müəyyənləşdirilir, sonra isə iş rollarının əsasında kurikulum dizayn edilir [4]. Digər tədqiqatçılar kurikulum freymvorkları təqdim edirlər və biliyin ümumi sahələrini müzakirə edirlər [4]. Tədqiqatçıların

əksəriyyəti informasiya təhlükəsizliyi kurikulumuna informasiya sistemləri və kompüter elmləri aspektlərinin, həmçinin təhlükəsizliyin əsaslarının daxil edilməsini vacib sayırlar [5]. [4]-də təklif edilir ki, informasiya təhlükəsizliyi kurikulumu 18 sahəni əhatə etməlidir: 1: İnformasiya təhlükəsizliyi qanunvericiliyi və standartları; 2: İnformasiya sistemlərinin analizi və layihələndirilməsi; 3: Sistemlərin təhlükəsizlik texnologiyaları; 4: Verilənlər bazaları; 5: Əməliyyat sistemləri; 6: Şəbəkə təhlükəsizliyi; 7: Müdaxilələrin aşkarlanması və qarşısının alınması; 8: Şəbəkə; 9: Şəbəkə təhlükəsizliyi texnologiyaları; 10: Virus; 11: Hacking; 12: Veb təhlükəsizlik; 13: E-kommersianın təhlükəsizliyi; 14: Mühəsibətlik və maliyyə; 15: Statistika; 16: Risk analizi; 17: Qərarqəbul etmə nəzəriyyəsi; 18: Kriptologiya. Tələbələr əvvəlcə sistem təhlükəsizliyi kursunu götürməli, sonra isə onu şəbəkə təhlükəsizliyi və tətbiqi proqram təhlükəsizliyi kursları ilə davam etdirməlidir.

[5]-də ABŞ və Çin qabaqcıl universitetlərinin informasiya təhlükəsizliyi üzrə magistr kurikulumlarının analizi aparılır. Vurğulanır ki, Çində kurikulumlar telekommunikasiya, kompüter elmləri və informasiya təhlükəsizliyi texnologiyalarına geniş diqqət ayrılır. ABŞ-da isə kompüter elmləri və informasiya təhlükəsizliyi texnologiyalarına əlavə olaraq kurikulumda müəssisə səviyyəsində təhlükəsizlik strategiyası və siyasəti, informasiya təhlükəsizliyi menecmenti və kiberhüquqa önəm verilir. Bu fərqlərin əhəmiyyətli olduğu və həm informasiya təhlükəsizliyi mütəxəssislərinin qavrayış və bacarıqlarına, həm də dövlət və özəl təşkilatlarda informasiya təhlükəsizliyinin menecmentinə təsir verəcəyi qənaətinə gəlinir.

ABŞ-da informasiya təhlükəsizliyi kurikulumlarının işlənməsinə mühəndislik təşkilatları (ACM, IEEE və s.), Çində isə Təhsil Nazirliyi rəhbərlik edir. Çində İnt kurikulumu texnologiyaların öyrənilməsinə fokuslanır, ABŞ-da isə iş fəaliyyətinin dəstəklənməsinə yönəlik.

[6]-da qabaqcıl universitetlərin 21 kibertəhlükəsizlik magistr proqramları analiz edilmişdir, əsas diqqət kursların məzmunu, strukturu, qəbul tələbləri, müddəti, qurtarma və evolyusiya üçün tələblərə yönəlmişdir.

III. NICE TƏŞƏBBÜSÜ

National Initiative for Cybersecurity Education (NICE) [7] təşəbbüsü ABŞ Ticarət Nazirliyinin tabeliyində olan NIST tərəfindən idarə edilir, kibertəhlükəsizlik təhsili, təlimi və işçi qüvvəsinin yetişdirilməsi üzrə hökumət, ali məktəblər və özəl sektor arasında tərəfdaşlıq təşəbbüsüdür.

NICE freymvorku NIST tərəfindən hazırlanmışdı, kibertəhlükəsizlik sahəsində iş rollarını təsvir etmək üçün taksonomiya müəyyən edir. Freymvorka üç müxtəlif komponent daxildir (mötərizədə sayları göstərilib):

- kateqoriya (7) – kibertəhlükəsizlik funksiyalarını yuxarı səviyyədə təsvir edir;
- ixtisas sahəsi (33) – kibertəhlükəsizlik sahələrini təsvir edir;

- iş rolu (52) – hər bir iş rolunun tələb edildiyi spesifik bilik, bacarıq və vərdislərə uyğun olaraq kibertəhlükəsizlik rolunu ətraflı təsvir edir.

Hər bir kateqoriyaya daxil olan ixtisas sahələri haqqında qısa məlumatı [8]-də əldə etmək olar:

IV. QABAQCIL ÖLKƏLƏRİN TƏCRÜBƏSİ – QISA QEYDLƏR

A. Amerika Birləşmiş Ştatları (ABŞ)

ABŞ-da əksər bilik sahələri üzrə təhsil standartları və mütəxəssislərin hazırlanması keyfiyyətinin sertifikatlaşdırılması sistemi mərkəzləşdirilməyib və ştatlar səviyyəsində təşkil olunub (regional akkreditasiya komissiyaları). Bununla yanaşı, ABŞ-da informasiya təhlükəsizliyi sahəsində mütəxəssis hazırlığının standartları və sertifikatlaşdırılması ilə federal orqan – Mühəndislik və Texnologiya üzrə Akkreditasiya Şurası (ing. Accreditation Board for Engineering and Technology, ABET) məşğul olur [9]. İlk növbədə, bura kompüter elmləri, kompüter mühəndisliyi və sistem mühəndisliyi aiddir.

ABŞ-da informasiya təhlükəsizliyi sahəsində bakalavr dərəcəsi ilə təhsil proqramlarında ən çox tələb edilənlər: kompüter insidentlərinin təhqiqatı, informasiya təhlükəsizliyi, kompüter təhlükəsizliyi, kompüter şəbəkələrinin təhlükəsizliyidir. Magistratura təhsil proqramlarında isə informasiya təhlükəsizliyinin menecmenti və informasiya təhlükəsizliyinin iqtisadiyyatı (MBA dərəcəsi verilir) istiqamətləri də vardır.

Bir qayda olaraq, magistraturanın sonunda tələbənin informasiya təhlükəsizliyi sahəsində peşə sertifikatlarından birini almaq imkanı olur (məsələn, CİSSP), bu əmək bazarında onun rəqabət qabiliyyətini artırır.

B. Böyük Britaniya

Böyük Britaniyada ali məktəblərdə bakalavr hazırlığı proqramlarının əksəriyyətində kibertəhlükəsizlik və kompüter insidentlərinin təhqiqatı istiqamətləri üstünlük təşkil edir. Magistr proqramlarında isə kibertəhlükəsizlik, İT-təhlükəsizlik və kompüter insidentlərinin təhqiqatı istiqamətləri üstünlük təşkil edir.

Təhsil proqramlarının keyfiyyətinə müəyyən zəmanət vermək üçün bakalavr və magistr proqramları təqdim edən universitetlərin Milli Kibertəhlükəsizlik Mərkəzi (MKM) tərəfindən akkreditasiyası nəzərdə tutulub. MKM 2016-cı ildə Hökumət Rəhbərlik Mərkəzinin tərkibində yaradılıb. Lankaster, London, Oksford, Edinburq, Surrey, Krenfeld universitetlərinin və Hollovey Kral Kollecinin magistr hazırlığı proqramları həmin mərkəz tərəfindən sertifikatlaşdırılıb (universitetlərin tam siyahısı ilə MKM-in saytında tanış olmaq olar). Sertifikatlaşdırma zamanı dərəcəni verən akademik komanda, tədris olunan fənlər, tələbələrin qiymətləndirilməsi metodları, dərəcə üçün qəbul tələbləri, dissertasiya nümunələri, tələbələrin sayı, tələbələrin aldığı qiymətlər və tələbələrin əks-əlaqə rəyləri nəzərə alınır.

Böyük Britaniyada kibertəhlükəsizlik sahəsində tədqiqatları dəstəkləmək üçün MKM müvafiq qiymətləndirmədən sonra universitetlərə ACE-CSR (Academic Centres of Excellence in Cyber Security Research) statusu verir (4 il müddətinə) və doktorantları bu sxem üzrə dəstəkləyir. 2017-ci ildə 17 universitet bu statusu qazanmışdır. 2021-ci ilə kimi təxminən 150 yeni doktorantın bu sxemdən yararlanaraq vacib kibertəhlükəsizlik mövzularında tədqiqatlarını başa çatdıracaqları gözlənilir.

C. Almaniya

Almaniya ali məktəblərində kibertəhlükəsizlik üzrə mütəxəssis hazırlığı sisteminin fərqləndirici xüsusiyyəti tələbələrin kursları seçməsində nisbi sərbəstliyidir. Ali məktəb hansı kursların məcburi olduğunu müəyyən edir, həm də məcburi fənlərin siyahısı digər ölkələrlə müqayisədə kifayət qədər azdır [10].

Bolonya prosesinin prinsipləri kursların seçimlə olmasını təşviq edir, buna görə müəllimlər rəqabət şəraitində olurlar və öz kurslarını tələbələr üçün cəlbədicə etməlidirlər. Müəllimlər öz fənlərinə elmi tədqiqat elementləri daxil etməyə cəhd edirlər, xüsusilə magistraturada elmi-tədqiqat yönümlü kurslar çoxdur. Bakalavr və magistr dərəcələri üçün dissertasiyalar da elmi-tədqiqatların nəticələri üzərində qurulur.

Təhsil formaları klassik xüsusiyyətlərə malik olsa da (mühazirələr, seminarlar, tələbələrin çıxışları və s.), fərqli xüsusiyyətləri də var – informasiya təhlükəsizliyi ilə əlaqəli konkret layihələrin yerinə yetirilməsi zamanı kiçik qruplarda müstəqil işə üstünlük verilir.

D. Fransa

Fransada informasiya təhlükəsizliyi sahəsində mütəxəssis hazırlığı sistemi kriptografiya, şəbəkə təhlükəsizliyi və informasiya sistemlərinin auditü ilə əlaqəli məsələlərin daha dərindən öyrənilməsinə yönəlib. Tələbələrə kriptologiya və kompüter təhlükəsizliyinin riyazi aspektlərini öyrənmək üçün ciddi riyazi təhsil verilir. Şəbəkə təhlükəsizliyinin öyrənilməsi real şəbəkələrin, şəbəkə arxitekturalarının modellərində, real avadanlığın istifadə edilməsi üzərində qurulur [11].

ABŞ, Böyük Britaniya və Almaniya ilə fərqli olaraq kompüter təhlükəsizliyi insidentlərinin təhqiqatı və sübutların toplanması ilə bağlı fənlərə az diqqət yetirilir.

Qeyd etmək lazımdır ki, Fransada informasiya təhlükəsizliyi sahəsində mütəxəssis hazırlığı ilə məşğul olan ali məktəblərin sayı azdır və əsasən magistraturada cəmlənib. Riyaziyyat və İnformatika ixtisası üzrə diplom lisenziyası olan istənilən şəxs magistraturaya daxil ola bilər.

Peşə lisenziyasının alınması 460 saat (13 həftə) auditoriya məşğələlərini, layihə üzərində 150 saat (4 həftə) işi və 16 həftə ərzində təcrübə keçməsinə nəzərdə tutur. Qəbul edən şirkətin axtarışını tələbə özü yerinə yetirir və bu, lisenziya alınmasına hazırlığın məcburi hissəsidir. Məzunlar şirkətlərin sifarişləri ilə tədris mərkəzində təhsili və yenidən hazırlığı davam etdirə bilərlər.

E. Rusiya Federasiyası (RF)

Rusiya Federasiyasında (RF) informasiya təhlükəsizliyi sahəsində ali təhsilli mütəxəssislərin hazırlanmasına 1992-ci ildən başlanmışdır. Hazırda 100-dən çox ali məktəbdə bu sahədə mütəxəssis və bakalavr hazırlığı həyata keçirilir.

İnformasiya təhlükəsizliyi üzrə bakalavriat proqramları üçün 7 istiqamət (profil) müəyyən edilmişdir: 1) Kompüter sistemlərinin təhlükəsizliyi; 2) İnformasiya mühafizəsinin təşkili və texnologiyası; 3) İnformasiyalaşdırma obyektlərinin kompleks mühafizəsi; 4) Avtomatlaşdırılmış sistemlərin təhlükəsizliyi; 5) Telekommunikasiya sistemlərinin təhlükəsizliyi; 6) Maliyyə monitorinqinin informasiya-analitika sistemləri; 7) İnformasiyanın texniki mühafizəsi.

Qeyd etmək lazımdır ki, 2011-ci ildə Rusiya təhsil sistemi ikisəviyyəli (bakalavriat-magistratura) modelə keçsə də, birsəviyyəli model (o cümlədən, spesifikasiya) də saxlanmışdır. Təhsil proqramlarında məcburi fənlərin analizi göstərir ki, RF təhsil proqramları informasiya təhlükəsizliyinin təmin olunmasına kompleks yanaşmanı nəzərə alır. Belə ki, proqramların əksəriyyətində tələbələr informasiya mühafizəsinin təşkili, hüquqi, texniki, proqram-aparat və kriptografik metodları ilə əlaqəli fənləri öyrənirlər. Bütün proqramlarda çox sayda məcburi fənlər var və təhsil mütəxəssislərinin əksəriyyəti əvvəlki standartda nəzərdə tutulmuş məcburi fənləri də siyahıda saxlayırlar. Bir sıra ali məktəblər özlərinin tədris planlarına informasiya təhlükəsizliyi mütəxəssislərinin fəaliyyət spesifikasiyasına aid olmayan təsadüfi fənlər (kulturologiya, nitq mədəniyyəti) də salırlar.

İnformasiya təhlükəsizliyi sahəsində mütəxəssislərin kvalifikasiya tələblərinin təsviri peşə standartlarında öz əksini tapır. RF Əmək və sosial müdafiə nazirliyi tərəfindən 2016-cı ildə 8 belə peşə standartı hazırlanmışdır, onlardan 3-ü məxfilik qurumlarına məxsusdur, qalan 5-i isə konfidensial deyil və istifadəyə açıqdır.

Qeyd etmək lazımdır ki, əcnəbi vətəndaşların həтта ödənişli əsaslarla da informasiya təhlükəsizliyi üzrə 7 texniki ixtisasdan yalnız birinə qəbul edilməsinə icazə verilir.

Daha bir xüsusi cəhət kimi informasiya təhlükəsizliyi üzrə magistrlərin hazırlığı üçün böyük sayda büdcə yerləri ayrılmasını qeyd edək. Məsələn, 2019-cu ildə təkcə İTMO (İnformasiya Texnologiyaları, Mexanika və Optika) Universitetinə 155 büdcə yeri ayrılmışdır.

NƏTİCƏ

Kiberfəzada ölkələrin virtual sərhədlərinin qorunması əsas prioritetlərdən biridir və bu prioritetin həyata keçirilməsi stratejiyasının əsas elementlərindən biri kibertəhlükəsizlik sahəsində maarifləndirmə, təlim və təhsildir.

Ölkəmizdə kibertəhlükəsizlik sahəsində yüksək ixtisaslı mütəxəssislərin hazırlığı üçün bu sahədə əlaqədar qurumlar

arasında koordinasiyanın gücləndirilməsi, onların səylərinin birləşdirilməsi, təcrübə mübadiləsi, tədris proqramlarının və elektron resursların, virtual laboratoriyaların yaradılması, kiber-hücum və müdafiə üzrə yarışların təşkili, kibertəhlükəsizlik sahəsində tədris aparən pədaqoji kadrların ixtisasının artırılması, elmi tədqiqatların daha da intensivləşdirilməsi olduqca vacibdir.

ƏDƏBİYYAT

- [1] Cybersecurity workforce study – ICS(2). 2018. <https://www.isc2.org/Research/Workforce-Study>
- [2] The CSEC2017 Joint Task Force, “Cybersecurity Curricula 2017,” version 0.95 report, 13 November 2017. www.csec2017.org.
- [3] T.Tagarev, “A generic reference curriculum on cybersecurity,” Information & Security, vol. 35(2), pp. 181-184, 2016.
- [4] K. Y. Kim, & K. Surendran, “Information security management curriculum design: A joint industry and academic effort,” Journal of Information Systems Education, vol. 13(3), pp. 227-236, 2002.
- [5] H. Chen, S.B. Maynard, & A. Ahmad, “A comparison of information security curricula in China and the USA,” The Proc. of 11th Australian Information Security Management Conference, pp. 21-34, 2013.
- [6] K. Cabaj, D. Domingos, Z. Kotulski, A. Respício, “Cybersecurity education: Evolution of the discipline and analysis of master programs,” Computers & Security, v. 75, pp. 24-35, 2018.
- [7] NIST Special Publication 800-181: National Initiative for Cybersecurity Education. (NICE). The national cybersecurity workforce framework. 2017. <https://doi.org/10.6028/NIST.SP.800-181>
- [8] L. González-Manzano, & J.M. de Fuentes, “Design recommendations for online cybersecurity courses,” Computers & Security, 80, pp. 238-256, 2019.
- [9] R. Greenlaw, A. Phillips, & A. Parrish, “Is it time for ABET cybersecurity criteria?” ACM Inroads, vol. 5(3), pp. 44-48, 2014.
- [10] М.С. Чванова, М.С. Анульева? “Система высшего образования в ФРГ. Подготовка специалистов в области информационной безопасности,” Вестник Тамбовского университета. Серия: Гуманитарные науки, №110(6), с. 78-84, 2012.
- [11] М.С. Чванова, М.С. Анульева, “Подготовка специалистов в области информационной безопасности во Франции,” Вестник Тамбовского университета. Серия: Гуманитарные науки, № 111(7), с. 159-165, 2012.

**PROBLEMS OF EDUCATING CYBERSECURITY
SPECIALISTS IN UNIVERSITIES**

Yadigar İmamverdiyev

Institute of Information Technology of ANAS,

Baku, Azerbaijan

yadigar@iit.science.az

Abstract – The article analyzes educational standards of higher education for bachelor’s and master’s degrees from international organizations and developed countries in the field of cyber security, as well as curricula for information security at leading universities.

Keywords – information security, cybersecurity, educational standard, professional standard; curriculum.

Yeni nəsil şəxsiyyət vəsiqələrinin (E-ID) e-xidmətlərə inteqrasiyası problemləri

Həbib Abbasov

AR Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyi
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
hebib.atilla@gmail.com

Xülasə — Müasir dövrdə informasiya texnologiyalarının inkişafı dövlətlərdə və hökumətlərdə ənənəvi klassik xidmətlərin elektron xidmətlərə keçidinə zəmin yaratmışdır. Bu isə öz növbəsində hər birimizin daxil olduğu informasiya cəmiyyətində, vətəndaşlara məxsus fərdi məlumatların etibarlı qorunması və təqdim olunan, yeni nəsil şəxsiyyəti təsdiq edən sənədin elektron çip daşıyıcısı vasitəsi ilə informasiya təhlükəsizliyi amilini daima qüvvədə saxlayır.

Yeni nəsil şəxsiyyət vəsiqəsi (e-ID) informasiya mübadiləsində beynəlxalq mülki aviyaşia təşkilatı (İCAO) tərəfindən təklif olunmuş bütün texniki və texnoloji tələbləri özündə əks etdirir. Bu tələblər əsasında vətəndaşlara yeni nəsil nəsil şəxsiyyət vəsiqələrinin verilməsi üçün Azərbaycan Respublikası Prezidenti 2014-cü il 28 noyabr tarixli 893 nömrəli sərəncam^[1] imzalamışdır. Sərəncamdan irəli gələn məsələlər içərisində e-xidmətlərə əlçatanlığın təmin edilməsi üçün hər bir imza səlahiyyəti olan vətəndaşa elektron imza sertifikatları verilməsi göstərilmişdir. E-ID həllərində elektron imzanın (e-imza) tətbiqi e-sənəd, elektron bankaçılıq, qorunan e-poçt, e-səhiyyə, portal və bulud üzərində e-xidmətlərin təhlükəsizliyinin təmin edilməsində mühüm yer tutur. Məqalə tətbiq olunan yeni nəsil şəxsiyyət vəsiqələrinin kriptografik imkanları əsasında e-imza sertifikatları istifadəsi eyni zamanda ümumi istifadə üçün açıq olan vəsiqə məlumatlarının çipdən oxunması və elektron xidmətlərə inteqrasiyada qarşıda duran problemlərə həsr olunmuşdur.

Açar sözlər— *e-gov; e-imza; e-ID; e-sənəd; CSP, ECC, SHA-2*

1. GİRİŞ

E-ID smart kartlar texniki olaraq xülasədə də qeyd olunduğu kimi müəyyən olunmuş tələblərə əsasən formalaşdırılmışdır. Bu tələblər əsasında təqdim edilən e-ID kartlar özündə bir çox məlumatların saxlanılması təmin edir. E-ID kartların 2018-ci il 1 sentiyabr tarixdən verilməsi prosesi başlanmışdır. Ölkə üzrə regionlarda mərkəzləşdirilmiş qaydada e-ID kartların verilməsi üçün fərdiləşmə mərkəzləri qurulmuşdur. Qurulmuş mərkəzlərə daxil olunmuş müraciətlər əsasında vəsiqələrin İAMAS sistemində qoşulmaqla hazırlanması prosesi icra edilir. Hər bir fərdiləşmə mərkəzi üzrə müraciət əsasında Milli Sertifikat Xidmətləri Mərkəzinə vətəndaşa aid olan ərizə məlumatı və PKCS#7^[2] formatında sertifikat sorğusu göndərilir. Sorğuların dəqiqliyinin təmin edilməsi üçün MSXM tərəfindən fərdiləşmə mərkəzlərinə

xüsusi olaraq infstruktural sertifikatları verilmişdir. Bu sertifikatlar vasitəsi ilə informasiya mübadiləsində ötürülən məlumatların səhhiyyəsinin və məlumatın ötürmə mənbəyinin identifikasiyası təmin edilir. Şəkil 1-dəki blok sxemdə e-ID sertifikat xidmətləri mərkəzi ilə İAMAS və regionlar üzrə fərdiləşmə mərkəzlərinin qoşulma sxemi təsvir edilmişdir.

Şəkil 1 E-ID mərkəz ilə İAMAS və fərdiləşmə mərkəzləri arasında struktur sxemin təsviri

II. HƏLLİN TƏTBİQİ VƏ AÇARLARIN SAXLANMA VASİTƏLƏRİ

Hal-hazırda Azərbaycan Respublikasında e-imza sertifikatlarının verildiyi yeni nəsil şəxsiyyət vəsiqəsi üçün istifadə edilən smart kart çipinin daxilindəki açarların təhlükəsizliyi aşağıda göstərilən tələblərə cavab verir.

GEMALTO NXP P60D144^[3]
ISO 7816 – 4,8,9,15 standard, T=1, T=0 protocol, 384-Kbyte ROM, 8.125 -Kbytes RAM, 144-Kbyte EEPROM, Asymmetric – RSA, ECC algorithm, symmetric – Triple DES, DES, AES hash SHA2, CC EAL5+ certified, Supports PC/SC/ PKCS11/ CT-API

Smart kartın konteynerləri imzalama və həmçinin şifrələmə funksiyalarına malikdir.

Kriptografik xarakteristikalar ümumilikdə beynəlxalq standartlar əsasında qurulub. E-ID kartlar aşağıda qeyd olunan kriptografik servis (CSP) vasitəsi ilə e-imza sertifikatlarına icazəni təmin edir.

İnformasiya təhlükəsizliyi baxımından əsas olan milli problem kimi smart kartların təhlükəsizlik komponenti kimi

istifadəsində CSP və təsadüfi açar generasiyası funksiyasının (RNG) milli olmamasıdır. Aşağıdakı təsvirdə e-İD kartlarında e-imza sertifikatları vasitəsi ilə sənədlərin imzalanması üçün aralıq interfeys proqram təminatı əks olunub.

Şəkil 2 E-İD kartlarında olan açarların və sertifikatların oxunması üçün təqdim olunan proqramın təsviri

Proqram təminatı istehsalçı tərəfindən dörd əməliyyat sistemi üçün təqdim edilib.

1. Windows
2. Linux
3. Mac OS
4. Android

Təqdim olunan e-İD kartlar bir çox ölkələr üzrə müqayisədə istehsalçıdan müəyyən asılılığın olması ilə fərqlənir. Bu isə kartlardan istifadədə misal olaraq IOS əməliyyat sistemi üçün mümkün deyil. PKCS#11 standartı üzrə APDU müraciət etdikdə istehsalçı tərəfindən xüsusi “Master Key” ilə PKCS#11 müraciəti şifrələnməsi təmin edilmişdir. Türkiyə, Avstriya, İtaliya təcrübəsinə baxdıqda bu tip həllər hər bir proqramist üçün açıqdır. Bu isə e-İD kartlar üçün formalaşdırılan bütün e-xidmətlər üçün açıqdır. Bura daxildir veb, mobil, blud həllər üzrə formalaşdırılan elektron xidmətlər.

Hal – hazırda təqdim edilən e-İD kartlar aşağıda göstərilən göstərilən apletlər ilə təmin edilib.

Şəkil 3 E-İD kartlarında təqdim olunan apletlərin təsviri

1. ICAO aplet beynəlxalq mülki aviyaşia təşkilatının tələb etdiyi məlumatları özündə əks elətdir. Bura daxildir, vəsiqə sahibinin foto şəkli, verilmə tarixi, verən orqanın adı. Bu məlumatların əldə edilməsi

ancaq NFC texnologiyası ilə "Basic Access Control" BAC^[4] metodu ilə mümkündür.

2. PKİ aplet e-imza sertifikatlarının saxlanması üçün istifadə edilir. PKİ aplet şəkil 2 - də təsvir edilmiş açarları və sertifikatları özündə saxlayır. Apletdə bir cüt sertifikat saxlamaq imkanı mövcuddur. Qanunvericiliyə uyğun olaraq yaş həddinə görə sertifikatlar MSXM tərəfindən e-İD vəsiqələrin çipinə daxil edilir. Yaş həddi 10-15 olan vətəndaşlar üçün ancaq bir autentifikasiya sertifikatı təqdim edilir. Bu sertifikat vasitəsi ilə təqdim edilən və gələcəkdə təsvir ediləcək istənilən e-gov xidmətlərinə identifikasiya olunması nəzərdə tutulub. Yaş həddi 15 dən yuxarı olan vətəndaşlar üçün iki sertifikat mərkəz tərəfindən PKİ apletə yazılır. Bunlar imza və autentifikasiya sertifikatlarıdır. Sertifikatların yaşam müddəti 5 ildir. E-İD vəsiqənin etibarlılıq müddəti isə 10 il nəzərdə tutulub. Hər 5 ildən bir istifadəçilər sertifikatlarının yenilənməsi üçün müvafiq mərkəzlərə müraciət edəcəklər.

Sertifikatlar ellptik ayrılərə əsaslanan kriptografik algoritmlərlə təmin edilib. ECDH_P256 bit uzunluğa malikdir. SHA384 heş funksiya ilə heşləmə əməliyyatları icra edir. Aşağıdakı təsvirdə vətəndaşa verilmiş imza sertifikatı əks olunub.

Şəkil 4 E-İD kartlarda vətəndaşlara təqdim olunan imza sertifikatının təsviri

Sertifikatlar avropa direktivinin^[5] 2014 –cü ildə qəbul etdiyi tələblər əsasında formalaşdırılıb.

3. CDA apleti şəxsiyyət vəsiqəsi formalaşdırılması üçün fərdə məxsus informasiyaları özündə saxlayır. Bu hissədə dəyişə bilən və dəyişməyən məlumatlar yerləşdirilmişdir. Dəyişə bilən məlumatlar ancaq xüsusi sertifikatla müvafiq icra hakimiyyəti orqanına məxsusdur. Misal olaraq vətəndaşın ünvanı dəyişdikdə onun yenidən e-İD kart almasına ehtiyac olmur. Bu dəyişə bilən məlumat olduğundan müvafiq qrupda e-İD kart oxuyucuya daxil edilməklə dəyişdirilir.

Elektron xidmətlərə integrasiyada bu sahədə müəyyən problemlər mövcuddur. Əsasən vətəndaşların bankalara və özəl təşkilatlara müraciəti zamanı vəsiqələrdən məlumatların oxunması problemi ilə qarşılaşırlar. Bu problemin aradan qaldırılması üçün aşağıda təsvir olunan proqram təminatı tərəfimizdən formalaşdırılmışdır.

Şəkil 5 E-İD kartlarda vətəndaşlara məxsus olunan məlumatların oxunması proqramının təsviri

III. E-ID VƏ E-İMZA TƏTBİQİNDƏ ETİBARLI XİDMƏTLƏR

Avropa birliyi ölkələri müvafiq qanunvericiliklərində bir çox ənənəvi xidmətlərin elektronlaşması üçün təkmilləşdirmə aparırlar. Bu qanunvericilik ümumilikdə eIDAS^[6] adlanır. eIDAS qanunvericiliyi birlik ölkələri arasında etibarlı e-xidmətlərin formalaşmasını və e-imzaların qarşılıqlı tanınması mexanizmini hüquqi müstəvidə müəyyən edir. Hal-hazırda “e-imza və e-sənəd” haqqında qanunun optimallaşması və gələcək çağırışlara cavab verməsi vacibdir. Bu baxımdan etibarlı e-xidmətlər göstərilən zaman tərəflərin tanınması texniki və hüquqi baxımdan tam olmalıdır. Ancaq təcrübələr göstərir ki, texnoloji inkişaf qanunvericilikləri qabaqlayır.

E-imzalar vasitəsi ilə hal-hazırda bir çox xidmətlərə çıxış imkanları təmin edilib. E-İD kartlarda təqdim edilən imza sertifikatları kriptografik algoritim baxımından cari istifadədə olan e-imzalardan fərqləndiyi üçün formalaşdırılan e-sənəd tipləri müxtəlif olacaq. Bu isə ilk növbədə integrasiya mərhələlərində bir çox təşkilatı və resurs problemləri ilə üzləni göstərəcək. Hal-hazırda tətbiq edilən e-sənəd formatları edoc genişlənməsində olub CADES formatında icra edilir. E-İD platforması üzrə tədim edilən sənəd yaratma formatı ETSI EN 319 162 Associated Signature Containers (ASiC)^[7] formatıdır. Aşağıda qeyd olunan təsvir nümunəsində e-İD kartlarda təqdim edilən e-imzalar vasitəsi ilə e-sənədlərə imza əlavə edilməsi üçün veb üzərindən təqdim edilən proqram təminatı əks olunmuşdur.

Şəkil E-İD kartlarda vətəndaşlara təqdim olunan imza sertifikatı ilə sənədlərin imzalanmasının təsviri

NƏTİCƏ

E-dövlət quruculuğunda informasiyanın qorunması və onun təhlükəsizliyinə təhdidlər genişlənir. Milli informasiya təhlükəsizliyinin təmin edilməsi baxımından yeni e-İD kartların tətbiqi müsbət amildir. Ancaq yuxarıda qeyd etdiyim bir çox kriptoloji və texniki təşkilatı yanaşmalar dahada təkmilləşdirilməlidir. Tətbiq olunan həllin milli riyazi və texnoloji həllər olması vacibdir. Bütün bu həllərin ümumistifadə üçün mobil platformalara soft həllər kimi integrasiya edilməsi və e-xidmətlərin dayanıqlılığı üçün blud həllərin genişlənməsi məqsədəuyğundur.

ƏDƏBİYYAT

- [1] <http://www.e-qanun.az/framework/28818>
- [2] <https://en.wikipedia.org/wiki/PKCS>
- [3] https://www.commoncriteriaportal.org/files/epfiles/0840b_pdf.pdf
- [4] <https://pdfs.semanticscholar.org/f479/eb98a06a2ed74e67a48acc13ea0237d168d1.pdf>
- [5] https://europa.eu/european-union/eu-law/legal-acts_en
- [6] <https://ec.europa.eu/digital-single-market/en/trust-services-and-eid>
- [7] https://comserv.cs.ut.ee/home/files/Nugis_CyberSecurity_2018.pdf?study=ATILoputoo&reference=F167B647D3821CD1F14EE4922D0E26A9D256FF5B

PROBLEMS OF INTEGRATING NEW GENERATION ID CARDS (E-ID) INTO E-SERVICES

Habib Abbasov

AR Ministry of Transport, Communication and High Technologies

Institute of Information Technology of ANAS

hebib.atilla@gmail.com

Abstract -Order of the President of the Republic of Azerbaijan No 893 of 28 November 2014 implies issuing new generation ID cards to citizens and the order is already being implemented. The order envisages granting e-signature certificates to each signatory citizen to ensure access to e-services. E-signature application for E-ID solutions is essential to ensure the e-security, e-banking, e-mail, e-health, portal and cloud e-services. The article is devoted to the problems encountered in integrating e-ID into e-services.

Keywords - e-Gov; e-signature; e-ID; e-document; CSP, ECC, SHA-2

Qlobal informasiya cəmiyyəti şəraitində Azərbaycan vətəndaşlarının adlandırılması məsələləri

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 mühitində bu problemlərin mümkün həlli yolları nəzərdən keçirilmişdir. Azərbaycan vətəndaşlarının ad və soyadlarının, bu sahədə tarixi ənənələrin, ad strukturunun ətraflı təhlili aparılmışdır. Bu sahədə xarici təcrübə araşdırılmışdır. Problemlərin aradan qaldırılması istiqamətində təkliflər irəli sürülmüşdür.

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

I. GİRİŞ

Azərbaycanın qlobal informasiya məkanına sürətlə inteqrasiyası bir çox digər məsələlər kimi ad və soyad sistemi və milli identiklik məsələlərinin tədqiqatını da aktuallaşdırır. Xalqın tarixinin bir hissəsi olan insan adlarında xalqların həyatı, tarixi keçmişi, inancları, arzu və xəyalları, yaradıcılığı, sosial mühiti, əlaqələri və s. əks olunur [1]. 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, hüdsuz və xotik qlobal informasiya məkanında xalqın öz milli mənsubiyyətini asanlıqla ifadə edə bilməsi üçün təkmil, dayanıqlı və ardıcıl mexanizmlər formalaşdırılmalıdır.

Milli identikliyin əsas göstəriciləri bunlardır: xarici görünüş; ad; vətəndaşlıq; dil; inanc; adət-ənənə; mətbəx; musiqi və s. Bu xüsusiyyətlərdən də göründüyü kimi, hər bir xalqın tarixən formalaşmış ad sistemi böyük informativ yükə malik əsas milli identiklik göstəricilərindəndir. Çünki adlar, soyadlar və ata adları xalqların tarixi, milli psixologiyası, adət-ənənələri, məişəti, inanc sistemi, dünyagörüşü, elmi-mədəni səviyyəsi, istək və arzuları əsasında formalaşaraq inkişaf edir. Bu baxımdan, müasir dünyanın əsas reallığı kimi xalqları, mədəniyyətləri vahid informasiya-kommunikasiya mühitinə cəlb edən virtual məkanda hər bir azərbaycanlı üçün elə ortaq ad mühiti yaradılmalıdır ki, bu mühit təkə fərd olaraq deyil, bir toplum olaraq da identikliyi təmin edə, xalqları, mədəniyyətləribir-birindən fərqləndirə bilsin.

Digər tərəfdən, məlum olduğu kimi, elektron dövlətin heç bir sferasını (e-səsvermə, e-təhsil, e-səhiyyə, e-ədliyyə, e-

vergi, e-bank və s.) adlarsız təəvvür etmək mümkün deyildir. Virtual məkanda yeni onomastik vahidlər (rəqəmsal antropomik vahidlər) kimi çıxış edən PIN kodlar, e-poçt ünvanları, nickname-lər və s. çox zaman vətəndaşların real xüsusi adları əsasında formalaşdırılır. Digər tərəfdən, insanların real adları adi həyatda olduğu kimi onları elektron dövlət mühitində də identifikasiya edir. Ona görə də xüsusi adlarla bağlı bir sıra məsələlərin həlli, o cümlədən ad və soyad sisteminin təkmilləşdirilməsi, ad komponenti standartlarının yenidən işlənilməsi, adlardakı təhrif hallarının aradan qaldırılması, adların elektron bazalarının yaradılması və onlardan istifadə mexanizmlərinin işlənilib hazırlanması, transliterasiya normalarının dəqiqləşdirilməsi, adların orfoqrafiyası qaydalarının nizama salınması və s. günün aktual problemlərindəndir.

II. AZƏRBAYCANDA AD SİSTEMİNİN FORMALAŞMASI TARİXİ

Tarixin ibtidai dövrlərindən başlayaraq 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.Kaşğarının “Divanilüğət-it-türk” əsəri, “Kitabi-Dədə Qorqud dastanları” və bir sıra etnoqrafik məlumatlar türk xalqlarında adlandırma ənənələrinin çox qədimliyini və sistemliliyini göstərir [2,].

Aşağıdakı cədvəldə Azərbaycan milli soyad sisteminin inkişaf tarixi verilmişdir.

CƏDVƏL 1. Azərbaycan milli soyad sisteminin inkişaf tarixi

III-V əsr - h/h Türk ad sistemi	-oğlu, -qızı
VII-XVII əsrlər (Ərəb ad sistemi)	-nisbə (i-vi), künyə (əbu, ümm), nəşəb (ibn)
XIX əsr (Fars ad sistemi)	-zadə
XX əsr (Rus ad sistemi)	-ov ² -yev ² ; -ski ² və s.

1988-h/h (Müasir ad sistemi)	-li ⁴ ; -xanlı-bəyli, sonluqsuz; -ov ² -yev ² ; -zadə; -gil; -soy; -oğlu-qızı; -ski ² , -i, -vi
---------------------------------	--

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 “fəmiyyə” ictimai-tarixi proses kimi IV əsrdə İngiltərədə, X-XI əsrlərdə İtaliyada, XV-XVI əsrlərdə Danimarkada, XIV-XVIII əsrlərdə Macarıstanda, XVIII əsrdə Şotlandiya və İrlandiyada yayılmışdır. Fəmiyyə 1926-1934-cü illərdə Mustafa Kamal Atatürk tərəfindən Türkiyədə, təxminən eyni vaxtda İranda, 50-ci illərdə Misirdə, 1959-cu ildə Tunisdə rəsmiləşdirilmişdir [3].

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

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

XIX əsrə doğru Rusiyada cəmiyyətin sosial inkişafının təsiri ilə fəmiyyələrdən 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 sonluqları ilə deyil, ov/-yev, -ova/-yeva formantlarından istifadə etməklə rus fəmiyyələrinə bənzər onomastik vahidlərlə qeyd edilməsi xalqımız arasında bu cür fəmiyyələrin süni formada yayılmasına rəvac verdi. Həmin dövrdə Azərbaycanda -ov/-yev, -ova/-yeva formantlarının geniş yayılmasına əlverişli şərait yaratdı [5].

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”, -li⁴, “oğlu”, “qızı” formantları 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 mühitinin hələ tam nizamla

düşmədiyini və qlobal şəraitdə xalqımızın milli identikliyi ilə bağlı yeni problemlərin ortaya çıxdığını göstərir [6].

Müstəqillik illərində, xüsusilə dünyaya yeni gələn körpələrin soyadlarında -ov/-yev, -ova/-yeva formantlarının çəkisi xeyli azalmışdır (Şəkil 1.) [7].

Amma bunun bir çox hallarda “zadə” və sonluqsuz formantlara istəklərin artması hesabına baş verməsi, eyni zamanda -ov/ -yev, -ova/ -yeva sonluqlarının hələ də qalması bu cür soyadları daşıyan vətəndaşlarımızın qlobal mədəniyyət müstəvisində digər türkdilli xalqlardan və başqa islam ölkələrinin vətəndaşlarından fərqləndirilməsində ciddi çətinlik yaradır. Azərbaycan Respublikası vətəndaşlarına verilən xarici (xidməti, diplomatik) pasportlarda ingiliscə -oğlu, -qızı sözlərinin yazılmaması və ata adının ingilis dilində göstərilməməsi isə vəziyyəti xüsusilə çətinləşdirir.

III. MİLLİ ADLANDIRMA SİSTEMİNİN STRUKTURU

Hazırda mövcud qanunvericilik aktlarının tətbiqi sayəsində ad və soyadların seçilməsi və qeydiyyatı prosesi sovet dövrünə nisbətən xeyli təkmilləşdirsə də, bu sahədə bəzi problemlər hələ də qalmaqdadır.

Ad sistemi müxtəlif xalqlarda fərqli olur. Azərbaycanda ad sistemi biradlılıqdan çoxadlılığa doğru inkişaf etmişdir [5]. Məsələn, Tural (biradlı), Tural Əli oğlu (iki adlı), Tural Əli oğlu Məmmədli (üçadlı). Bəzi zəruri hallarda isə ayamalardan, ləqəblərdən istifadə edilirdi. Məşğul olduğu sənətin adını insana qoyur, yaxud onun hansısa əlamətindən ləqəb yaradırdılar (məs.: Dəmirçi, Pinəçi, Uzun, Gödək və s.).

Artıq 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 [8].

Əfsuslar olsun ki, müvafiq normativ-hüquqi aktlarda təsbit edilmiş bu dəqiq ardıcılığa rəğmən sənədləşmə zamanı həmin ardıcılıq pozulur və bu sahədə dəqiq milli identiklik modeli (ad/ata adı/soyad strukturu) formalaşdırılmır. Məsələn, Azərbaycan Respublikasının vətəndaşlarına verilən şəxsiyyət vəsiqələrində soyad/ ad/ ata adı ardıcılığından istifadə olunur.

Ad sistemimizdə müxtəlif təsirlərlə yaranmış nizamsızlığın aradan qaldırılmasına, ad/ ata adı/ soyad ardıcılığının dəqiq norma kimi qəbul olunmasına və bütün sənədləşmələrdə adların vahid struktur üzrə yazılmasının təmin edilməsi hesabına sabit milli standartların möhkəmləndirilməsinə indi çox böyük ehtiyac vardır. Çünki Azərbaycanın ad sistemindəki mövcud vəziyyət, milli identikliyə xələl gətirməklə yanaşı, qlobal informasiya cəmiyyətində şəxsiyyətlərin eyniləşdirilməsini, həm ölkə daxilində, həm xaricdə fərdi məlumatlara çıxış imkanlarını da xeyli məhdudlaşdırır. Əgər nəzərə alsaq ki, hələ də transliterasiya problemi mövcuddur, onda problem daha da qabarıq şəkildə özünü büruzə verir.

IV. MİLLİ ADLANDIRMA STRUKTURUNUN PSIXOLINQVİSTİK 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 ardıcılığının insan təfəkkürünə ötürdüyü psixoloji informasiya Hacıbəyli Üzeyir, Behbudov Rəşid, Aslanov Həzi ardıcılığının doğurduğu təsəvvürlə eyni deyildir, bu cür hallar çoxşəxslilik yaradır.

Ad, ata adı və soyadların vahid milli standartının müəyyənləşdirilməsini zəruri edən digər mühüm 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 formantları ilə yaradılmış soyadlarla (Emin Sabitoğlu) qeydiyyatı alınmaq imkanı verir. Bu formalardan istifadə meyli kütləviləşdikcə ikinci komponentin hansı mənə daşdığını, yəni şəxs adını, şəxs adının bir hissəsini, ata adını, nəsil adını, yoxsa təxəllüsü olduğunu müəyyənləşdirməkdə, son nəticədə isə fərdi eyniləşdirməkdə çətinliklər yaranır. Ona görə də adlandırma sistemində komponentlərin hər birinin yeri dəqiq göstərilməlidir.

V. BEYNƏLXALQ TƏCRÜBƏDƏ ADLANDIRMA SİSTEMİ

Azərbaycanda fiziki şəxslərin bütün sənədlərdə qeydiyyatı proseslərinin ad/ ata adı/ soyad, ata adının yazılması zəruri olmadıqda isə ad/ soyad ardıcılığına əsaslanan dəqiq vahid standart üzrə həyata keçirilməsi beynəlxalq təcrübəyə uyğun olardı. Belə ki, bəzi ölkələrdə ilkin ad (first name), orta ad (middle name) və son ad (last name) komponentlərindən təşkil olunmaqla üçkomponentli modellərdən istifadə edilir.

İlkin ad (first name). İlkin ad doğrularkən şəxsə verilmiş addır.

Orta ad (middle name). Qərb mədəniyyətinə görə, bəzən uşağa bir deyil, iki ad verilir. Bir sıra hallarda isə həтта 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 və Birləşmiş Krallıqda əcdadların (ata, baba, ana, nənə) şəxs adlarından (forename) onların şərəfinə çox tez-tez middle name kimi istifadə olunur [9].

Danimarkada və Norveçdə isə middle name familiya anlamı daşıyır. Middle name kimi ananın qızlıq familiyası, yaxud əcdadlardan hansısa birinin last name-i seçilə bilər. Filippində middle name kimi, əsasən, ananın qızlıq familiyasından istifadə olunur. ABŞ-da middle name-dən çox tez-tez abbreviatura formasında istifadə edilir. Məsələn, Mary Lee Bianchi – Mary L. Bianchi və s.

Son ad (last name və ya surname). Son ad şəxsin konkret bir ailəyə, nəslə mənsubluğunu bildirən ad komponentidir. Last name ifadəsinin sinonimləri familiya, yaxud ailə adıdır.

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. Qeyd edək ki, biometrik pasport - Beynəlxalq Mülki Aviasiya Təşkilatının (ing. International Civil Aviation Organization – ICAO) müəyyən etdiyi biometrik məlumatlarla təchiz edilmiş pasportlardır. Bu pasportlar (ölçüləri, spesifikasiyası, yazı qaydaları və s.) üzrə beynəlxalq standartlar da ICAO tərəfindən müəyyən olunur. Dünya təcrübəsində biometrik pasportlar həmçinin “e-pasport” və ya elektron pasport (ing. electronic passports) kimi də tanınır [10].

Bu pasportlarda adlandırma ilə bağlı texniki-hüquqi standartlar Beynəlxalq Mülki Aviasiya Təşkilatının “Maşın oxuyan səfər sənədləri” (Machine Readable Travel Documents) üzrə təlimatı əsasında tənzimlənir [11].

Təlimatda pasportun 2 zonası fərqləndirilir: 1) Vizual yoxlama zonası; 2) Maşının oxuduğu zona. Təlimatın 3.4-cü bəndi vizual yoxlama zonasında (şəkil 2) pasport sahibinin adının düzgün yazılışı ilə bağlı normaları nəzərdə tutur.

**ISSUES OF AZERBAIJAN CITIZENS NAMING IN THE
CONTEXT OF THE GLOBAL INFORMATION
SOCIETY**

Rasim Alguliyev¹, Yedgar Jafarov², Afruz Gurbanova³
Institute of Information Technology of ANAS,
Baku, Azerbaijan

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

Keywords – name, surname, patronymic, pseudonym, nickname, naming system, national identity

Некоторые вопросы безопасности применения дронов

Шакир Мехтиев¹, Аяз Мехдиев²

^{1,2}Институт Информационных Технологий НАНА, Баку, Азербайджан

¹shakir@iit.science.az, ²ayaz_mehdiyev@bk.ru

Аннотация— Развитие информационно-коммуникационных технологий и микроминиатюризация электронной элементной базы обусловили прогресс в области производства и применений беспилотных летательных аппаратов. Данная статья посвящена исследованию некоторых вопросов безопасности, конфиденциальности и неприкосновенности частной жизни, которые являются объектами угроз при использовании гражданских беспилотных летательных аппаратов (дронов).

Ключевые слова— дрон, информационная безопасность, конфиденциальность, частная жизнь, угрозы, безопасность дронов

I. ВВЕДЕНИЕ

Происходившие на протяжении новейшей истории промышленные революции обусловили стремительный научно-технический прогресс во всех областях человеческой деятельности и, в частности, в области разработки и применения летательных аппаратов. Рассматриваемые в данной статье дистанционно управляемые беспилотные летательные аппараты (БПЛА), существенно уменьшившись в размерах, оснащенные современными микроэлектронными устройствами управления, навигации, видеонаблюдения и миниатюрными электрическими двигателями превратились из хобби в устройства массового использования для хозяйственных и иных нужд человека.

Первые сведения о применении БПЛА относят к 1849 г., когда с помощью неуправляемых воздушных шаров осуществлялась бомбардировка осажденной Венеции. Уже в 1898 г. Н. Тесла продемонстрировал возможности дистанционно радиоуправляемого судна, который послужил прототипом будущих разработок. В дальнейшем БПЛА использовались в военных и экспериментальных целях — боевые мишени, тактическая разведка, доставка боевого оружия, управление военными действиями и пр. Однако, подлинная история БПЛА, как дрона, берет начало в 1971 г., когда физик-ядерщик Джон С. Фостер-младший (*John S. Foster Jr.*) в разведывательных целях оснастил небольшую авиамодель фотоаппаратом и сделал съемки местности с небольшой высоты. В будущем эта идея была использована и в гражданских применениях дронов.

В настоящее время повсеместное использование дронов породило множество проблем, начиная с безопасного осуществления полетов, юридических норм использования в общественных местах, неприкосновенности частной и семейной жизни, террористических угроз и пр. При отсутствии регулирующих норм и правил дроны могут быть легко использованы в незаконных целях, таких как наблюдение и несанкционированное слежение.

Целью данной работы является краткий анализ некоторых применений дронов и угроз, которые могут возникнуть от их использования.

II. ОБЛАСТИ ПРИМЕНЕНИЯ ДРОНОВ

Области применения дронов весьма разнообразны. Рассмотрим некоторые из них.

A. Медицина

Организация Definetz предложила использовать дроны для экстренной доставки дефибрилляторов и других средств в тех случаях, когда невозможно дождаться прибытия бригады медицинской помощи. Так, например, в случае приступа инфаркта миокарда или остановки сердца счет идет на минуты, и вовремя оказанная доврачебная помощь сохранит жизнь больному. В медицинской сфере дроны могут быть использованы для доставки товаров медицинского назначения в труднодоступные сельские районы [1, 2].

B. Видеосъемка

В кинематографии видеосъемка с высоты птичьего полета создает новые ракурсы и возможности импровизации в творчестве, которые раньше не были возможны [3]. Дроны уже используются для подготовки репортажей с места событий и в спортивных соревнованиях. Еще одна область их применения — создание документальных фильмов о дикой природе [4].

B. Сельское хозяйство

В сельском хозяйстве с помощью дронов собирается информация о состоянии посевных площадей, оценивается степень зрелости растений, необходимость поливов и проводится точечная обработка очагов заболеваний [5]. Оперативное обнаружение заболеваний растений

позволяет принимать более точное решение по их лечению и мониторингу ситуации.

Г. Нефтегазовая отрасль

Стандартные подходы к мониторингу нефте- и газопроводов дополняются наблюдением с дронов. Сигналы с датчиков наблюдения и обнаружения утечек используются для идентификации текущего состояния трубопроводов и оценки экологической обстановки [6]. Качественные изображения в режиме реального времени позволяют оперативно обнаруживать нефтяные разливы и выявлять несанкционированную деятельность в охраняемых зонах.

Д. Чрезвычайные происшествия

Дроны используются в спасательных работах экстренными службами для поиска заблудившихся людей там, где доступ без спецсредств ограничен, например, в горной местности [7]. Дроны также оперативно могут доставить спасательные средства, еду и воду к месту катастроф, пожаров или землетрясений.

Е. Экологический мониторинг и гражданская наука

Дроны применяют для изучения таяния полярных льдов, с их помощью определяют пути миграции животных, обнаруживают несанкционированные свалки, борются с браконьерами, выявляют случаи нарушения норм экологического законодательства, определяют уровень загрязнения, а также влияние различных загрязнителей на глобальную экологическую ситуацию [8, 9]. Данные с датчиков, рассеянных на земном ландшафте, передаются в сеть дронов для обработки. Весьма перспективной в этом направлении является концепция гражданской науки, под которой понимается проведение научных исследований с привлечением широкого круга добровольцев (гражданин-ученый). Предлагается использовать сети дронов граждан-ученых для комплексных наблюдений в различных географических районах [10]. Важной составляющей в сети дронов являются координация их действий и трансляция изображений в единый центр мониторинга, что необходимо для эффективности наблюдений и обеспечения точности исследований в случаях единичных отказов дронов.

Применение дронов не ограничивается приведенными примерами. Можно также отметить археологию, строительство, журналистику, геодезию, вулканологию и пр.

Этот краткий обзор позволяет сделать вывод о том, что использование дронов является весьма необходимым и актуальным направлением.

III. Подходы к Безопасности Дронов

Количество действующих дронов продолжает неуклонно расти. Можно безошибочно предсказать, что по мере увеличения их числа появится больше угроз информационной и физической безопасности, а также

угроз конфиденциальности и вторжений в частную жизнь. Для эффективного обеспечения безопасности дронов необходим комплексный подход к решению следующих задач [11]:

- проектирование безопасности;
- мониторинг безопасности;
- управление безопасностью.

Структурная схема гипотетического дрона представлена на рис. 1.

Рис. 1. Структурная схема дрона

Как следует из рис. 1, дроны могут управляться либо дистанционно, либо автономно с использованием бортовых компьютеров. Фактически дрон представляет собой модель киберфизической системы. Физические элементы на борту дрона используют сеть датчиков и исполнительных механизмов, которые взаимодействуют с наземной системой управления по беспроводной линии связи. Соответственно, система дрона уязвима для атак, нацеленных на киберфизические элементы, интерфейс между ними, беспроводную связь или даже комбинацию нескольких компонентов. Характерные угрозы информационной безопасности для дронов приведены на рис. 2.

Рис. 2. Виды угроз информационной безопасности дронов

Указанные виды угроз достаточно подробно рассмотрены различными авторами. Отметим, что спуфинг (*spoofing attack*) – это метод передачи дрону ложных навигационных данных для перехвата его управления [12]. В последнее время также появились публикации, в которых приводятся сведения о технологических возможностях внедрения аппаратных троянов

непосредственно на стадии изготовления микрочипов [13, 14]. Факторы окружающей среды (погодные условия, птицы и пр.) могут привести к прекращению функционирования дронов: функциональный отказ или невозможность проведения видеонаблюдения.

Важной проблемой использования дронов является их интеграция в национальное воздушное пространство с одновременным обеспечением высокого уровня физической безопасности. Трудно представить ситуацию, когда, выполняя миссию по доставке грузов или осуществляя журналистскую деятельность, дрон из-за возникшей неисправности упадет на места скопления людей, замкнет линии электропередач или же создаст помехи в пределах аэропортов и других важных государственных учреждений. К сожалению, подобное случается. Использование дронов ставит задачу контроля за воздушным пространством и его разделения с пилотируемыми летательными аппаратами (самолетами и вертолетами). Производители дронов внедряют в их программное обеспечение блоки с геолокационными ограничениями в бесполетных зонах. Профилактической мерой в решении данной проблемы служат различные законодательные и нормативные акты. Однако, эти акты не являются международными стандартами и в различных странах правила использования дронов имеют различную интерпретацию. В Евросоюзе в 2015 г. была принята нормативно-правовая база в данном направлении [15]. Однако, в некоторых странах действуют локальные нормативы. Так, в Ирландии все дроны массой более 1кг должны быть зарегистрированы в Авиационном управлении (IAA). Кроме того, дрон не должен эксплуатироваться, если это будет представлять опасность для другого летательного аппарата в полете или подвергать опасности жизнь или имущество других лиц [16]. В Италии действует запрет на использование разновидности дронов – квадрокоптеров (для некоммерческой съемки, массой меньше 25 кг) при большом скоплении людей, в городах, рядом с железнодорожными вокзалами, аэропортами, военными объектами, электростанциями и правительственными учреждениями. Другие подобные регулирующие акты существуют в США, Великобритании, Японии, России и пр. [17]. В Азербайджанской Республике применения дронов регулируются “Законом об Авиации” и “Правилами использования воздушного пространства Азербайджана” [18, 19].

Широкое распространение дронов создало угрозы для вторжений и в частную жизнь граждан. Следует отметить, что международными документами право граждан на неприкосновенность частной жизни признано фундаментальным понятием. Во Всеобщей декларации прав человека зафиксировано, что “никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию” [20]. В Конституции Азербайджанской Республики также гарантировано право гражданина на личную

неприкосновенность. Без согласия гражданина сбор, хранение, использование и распространение сведений о его частной и семейной жизни, видео- и фотоматериалов не допускаются [21].

Дроны, оснащенные средствами аудио- и видеозаписи, могут быть использованы в незаконных целях, начиная от наблюдения до несанкционированного слежения. Для предупреждения подобных случаев предусмотрены правовые барьеры в законодательствах различных стран, в том числе и в Азербайджане [22].

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 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.

При использовании дронов угрозы конфиденциальности могут произойти по следующим причинам [23]:

- информация, собранная для одной цели, затем из корыстных побуждений передается третьей стороне;
- люди не осознают, что они находятся под наблюдением и не понимают, для чего будет использоваться информация;
- навязчивая практика наблюдения в достижении поставленной задачи;
- в процессе наблюдения собирается больше информации, чем это необходимо.

В некоторых случаях допускается разумное использование или раскрытие информации. Это может произойти по следующим причинам:

- уменьшение или предотвращение серьезного риска для отдельного лица или для общественности;
- использование или раскрытие информации разрешено по закону;
- использование или раскрытие информации необходимо для правоохранительной деятельности.

IV. ЗАКЛЮЧЕНИЕ

Использование гражданских дронов частными лицами и их применения весьма разнообразны и имеют тенденцию к расширению. Развитие дронов идет в направлении обеспечения безопасности воздушного движения. Однако обеспечение информационной безопасности дронов также становится весьма актуальной проблемой в контексте

противодействия угрозам угонов дронов и их противоправного применения криминальными и террористическими группировками. Законодатели и административные органы должны предвидеть потенциальные проблемы, которые могут привести к бесконтрольному использованию и злоупотреблению дронов.

ЛИТЕРАТУРА

- [1] Ш. Мехтиев, Б. Агаев, “Медицинская электроника: состояние, проблемы и перспективы,” *Elektron tibbin multidissiplinar problemləri*, Bakı, 2016, ss.110-113.
- [2] I. Subbarao, G. P. Cooper, “Drone-based telemedicine: a brave but necessary new world,” *The Journal of the American Osteopathic Association*, 2015, Vol 115, No. 12, pp. 700-701.
- [3] A. Rango, et al, “Using unmanned aerial vehicles for rangelands: current applications and future potentials,” *Environmental Practice*, 2006, Vol.8, No.3, pp.159-168.
- [4] K. Collins “Behind the mind-boggling shots captured by BBC drones,” 2014. <https://www.wired.co.uk/article/bbc-drone-journalism>
- [5] P. Tripicchio, et al, “Towards smart farming and sustainable agriculture with drones,” *International Conference on Intelligent Environments*, Prague, 2015, pp. 140-143.
- [6] T. Kh. Fataliyev, Sh. A. Mehdiyev, “Analysis and new approaches to the solution of problems of operation of oil and gas complex as a cyber-physical system,” *International Journal of Information Technology and Computer Science (IJITCS)*, 2018, Vol.10, No.11, pp.67-76.
- [7] S. Waharte, N. Trigoni, “Supporting search and rescue operations with UAVs,” *International Conference on Emerging Security Technologies*, 2010, pp.142-147.
- [8] A. Philips, “A glimpse into how eco-drones are changing environmental research for the better,” 2015. <https://projectearth.us/a-glimpse-into-how-eco-drones-are-changing-environmenta-1796519323>
- [9] B. Ivošević, et al, “The use of conservation drones in ecology and wildlife research,” *Ecology and Environment*, 2015, Vol.38, No.1, pp.113-188.
- [10] T. X. Fətəliyev, “Vətəndaş elmi e-elmin inkişafının yeni istiqaməti kimi,” *İnformasiya Cəmiyyəti Problemləri*, 2014, № 1, ss. 57-64.
- [11] R. M. Alguliyev, R. G. Alakbarov, T. Kh. Fataliyev, “Electronic science: current status, problems, and perspectives,” *Problems of information technology*, 2015, №2, pp. 4-14.
- [12] S. M. Giray, “Anatomy of unmanned aerial vehicle hijacking with signal spoofing,” *6th International Conference on Recent Advances in Space Technologies (RAST)*, 2013, pp.795-800.
- [13] J. Villaseñor, “The Hacker in Your Hardware,” *Scientific American*, 2010, Vol. 303, No. 2, pp. 82-87.
- [14] Ş. Mehdiyev, Y. İmamverdiyev, “E-dövlətin informasiya təhlükəsizliyi və texnoloji çağırışlar,” *İnformasiya təhlükəsizliyinin multidissiplinar problemləri*, Bakı, 2015, ss. 130-133.
- [15] “Introduction of a regulatory framework for the operation of drones, European Aviation Safety Agency,” A-NPA 2015-10, p.41. <https://www.easa.europa.eu/sites/default/files/dfu/A-NPA%202015-10.pdf>
- [16] “Regulating Drones: Safety, Security, and Privacy,” 2016. <https://www.mhc.ie/latest/blog/regulating-drones-safety-security-and-privacy>
- [17] “Master List of Drone Laws.” <https://uavcoach.com/drone-laws/>
- [18] “Aviasiya haqqında Azərbaycan Respublikasının Qanunu”, 2005, http://www.caa.gov.az/index.php?option=com_k2&view=item&id=94:law-of-the-republic-of-azerbaijan-on-aviation&Itemid=173&lang=az
- [19] “Azərbaycan Respublikasının hava məkanından istifadə Qaydaları” 2013 <http://www.e-qanun.az/framework/33800>
- [20] “Universal declaration of human rights,” 217(III) *International Bill of Human Rights*, 1948.
- [21] “Azərbaycan Respublikasının Konstitusiyası,” 26 sentyabr 2016. www.president.az
- [22] “Azərbaycan Respublikasının Cinayət Məcəlləsi.” <http://www.e-qanun.az/code/11>
- [23] “Drones and the Privacy Principles,” *Office of the Information Commissioner Queensland*, 2018. <https://www.oic.qld.gov.au>

SOME SECURITY ISSUES OF USING DRONES

Shakir Mehdiyev¹, Ayaz Mehdiyev²

¹shakir@iit.science.az, ²ayaz_mehdiyev@bk.ru

Institute of Information Technology of ANAS, Baku, Azerbaijan

Abstract — The development of information and communication technologies and microminiaturization of electronic components have also led to progress in the production and applications of unmanned aerial vehicles. This article is devoted to the study of some issues of security, confidentiality, and privacy, which are the objects of threats when using of civilian unmanned aerial vehicles (drones).

Keywords — drone, information security, confidentiality, privacy, threats, security of drones

Folklor informasiya təhlükəsizliyində və informasiya təhlükəsizliyi folklorunda

Hikmət Quliyev

AMEA Folklor İnstitutu, Bakı, Azərbaycan

quliyevh@mail.ru

Xülasə— Məqalədə informasiya təhlükəsizliyi kontekstində folklorun rolu, eyni zamanda folklorun özünün informasiya təhlükəsizliyi məsələləri araşdırılmışdır. İnternetin sürətlə genişlənməsi, insanların gündəlik həyat rejimində yeri və rolunun artması, ən müxtəlif ehtiyac və istəklər baxımından şəxslərin ondan asılılığın güclənməsi, bütövlükdə, informasiya təhlükəsizliyinin aktuallaşmasına – kibercinayətkarlığın, kiberzoraklığın, gizli sosial şəbəkə və proseslərin aşkarlanmasına gətirib çıxarmışdır. Müəyyənəşdirilmişdir ki, bu kontekstdə folklor unikal imkanlara malikdir. Qeyd olunmuşdur ki, informasiya təhlükəsizliyinin predmeti kimi, milli folklor resurslarının etibarlı saxlanması, bütövlüyünün və tamlığının qorunması, həmin resursların əlyətərliliyinin təmin olunması müasir dövrün aktual çağırışlarından biridir. Eyni zamanda rəqəmsal folklor resurslarının ən müxtəlif parametrlər üzrə təsnif olunması və İnternet mühitində onların intellektual analizinin həyata keçirilməsi ilə bağlı perspektivlər şərh edilmişdir.

Açar sözlər— informasiya təhlükəsizliyi, folklor, rəqəmsal folklor, folklorun qorunması, internet folkloru, kompüter folklorşünaslığı, kibercinayətkarlıq, milli identitlik.

I. GİRİŞ

Müasir dövr informasiya-kommunikasiya texnologiyalarının sürətlə yayılması və elektron texnologiyalar hesabına yeni imkanların meydana çıxması ilə xarakterizə olunur. Rəqəmsal texnologiyaların, elektron mühitin, qlobal informasiya şəbəkəsinin mövcudluğu elmin bütün sahələrində olduğu kimi, folklorşünaslıqda da yeni istiqamət və təmayüllərin meydana çıxarılmasını zəruri edir. Bu baxımdan milli təhlükəsizliyin əsas komponentlərindən olan milli-mənəvi dəyərlərin qorunması, xalq mədəniyyətinin, folklorun müasir dünyanın tələblərinə müvafiq şəkildə informasiya təhlükəsizliyi kontekstində araşdırılması kifayət qədər aktual məsələdir. Bir tərəfdən informasiya təhlükəsizliyi kontekstində folklorun spesifik imkanlarının öyrənilməsi, digər tərəfdən isə folklorun özünün informasiya təhlükəsizliyi ilə bağlı problemlərinin araşdırılması, rəqəmsal folklor resurslarının vahid sistem daxilində birləşdirilməsi, elektron mühit daxilində hər bir folklor resursunu xarakterizə edən parametrlərin müəyyənəşdirilməsi, onların beynəlxalq standartlara uyğunlaşdırılması, rəqəmsal folklor resurslarının təsnif olunması, İnternet mühitində milli folklor resurslarının müxtəlif parametrlər üzrə intellektual analizi üçün imkanların yaradılması, aktual dövriyyədə olan folklor vahidlərinin

tezliyinin müəyyənəşdirilməsi, eləcə də, illərlə toplanmış folklor resurslarının etibarlı qorunmasının, tamlığının və əlyətərliliyinin təmin olunması kimi məsələlər bu qəbildəndir.

Beləliklə, məsələyə üç əsas aspektdən baxmaq mümkündür:

Birincisi, informasiya təhlükəsizliyi kontekstində folklorun unikal imkanlarından istifadə etməklə müəyyən situasiya və hallarda məxfiliyin, qeyri-müəyyənliyin, gizli virtual sosial şəbəkə və qrupların aşkarlanması, onlara münasibətdə adekvat üsul və metodların müəyyənəşdirilməsi;

İkincisi, kompüter texnologiyalarının imkanları hesabına milli folklor resurslarının rəqəmsallaşdırılması, elektron mühitə daxil edilməsi, həmin mühit daxilində etibarlı qorunması, tamlığı və əlyətərliliyinin təmin edilməsi, eyni zamanda folklor resurslarının intellektual analizinin təmin edilməsi üçün hər bir folklor resursunu identifikasiya edəcək parametrlərin müəyyənəşdirilərək qeyd olunması;

Üçüncüsü, İnternetdə – virtual kommunikativ mühitdə, sosial şəbəkə, forum və saytlarda gedən folklor proseslərinin, folklorlaşma və yaxud defolklorlaşma tendensiyalarının, müvəqqəti folklor ənənələrinin, yeni nəsil folklor faktlarının, folklorik forma və qəliblərin, nəhayət, İnternet folklorunun multidissiplinar metod və yanaşmalar, informasiya-kommunikasiya texnologiyalarının tətbiqi əsasında analiz olunması.

II. İNFORMASIYA TƏHLÜKƏSİZLİYİ ANLAYIŞI

İnformasiya təhlükəsizliyi geniş anlayışdır və son zamanlar aktuallaşmasına baxmayaraq, tarixən müxtəlif daşıyıcılar – daş, dəri, kağız və s. üzərində olan informasiyanın qorunması, məxfiliyinin təmin edilməsi kimi məsələlər kontekstində mövcud olmuşdur. Hesab etmək olar ki, kommunikasiya yarandığı andan etibarən informasiyanın aktuallığı və vacibliyi dərk olunmuş, insanlar arasında informasiyanın qorunması, etibarlı şəkildə saxlanması və ötürülməsinə böyük əhəmiyyət verilmişdir. Xüsusilə də, qrup şəklində təşkilatlanmada, sosial təsisat kimi formalaşmada, ən nəhayət dövlət olaraq təmərküzləşmədə informasiya təhlükəsizliyinin önəmi daha da artmış, belə demək mümkündürsə, mövcudluq şərtinə çevrilmişdir.

Elmi ədəbiyyatlarda informasiya təhlükəsizliyi anlayışına müxtəlif cür yanaşma mövcuddur: “İnformasiya təhlükəsizliyinin predmeti çox zaman informasiyanın

konfidensiallığının, tamlığının və əlyetərliliyinin təmin edilməsi kimi başa düşülür. Lakin informasiya təhlükəsizliyinin predmeti daha genişdir. İnformasiya təhlükəsizliyi təkcə kompüter təhlükəsizliyindən və şəbəkə təhlükəsizliyindən ibarət deyil. Müasir cəmiyyətdə informasiya təhlükəsizliyi cəmiyyətin bütün sosial proseslərinə (kursiv bizimdir – H.Q.) nüfuz edir, istənilən dövlətin milli təhlükəsizliyinin ayrılmaz tərkib hissəsinə çevrilir” [7]

Müasir dövrdə informasiyanın çox sürətli şəkildə yayılması, informasiya üzərində istənilən əməliyyatın aparılması imkanının olması və s. informasiyanı çox zəruri və strateji bir məfhumla çevirmişdir. İnformasiya üzərində manipulyasiyalar etməklə cəmiyyətə təsir etmək, dezinformasiya yaymaqla stabilliyi pozmaq, sosio-psixoloji xaos yaratmaq mümkündür. Eyni zamanda hər hansısa yararlı, bəşəriyyətin inkişafına dəstək verə biləcək informasiyadan səmərəli istifadə etməklə, onu geniş kütlələr arasında yaymaqla böyük xeyir əldə etmək olar. Bu onu göstərir ki, informasiyanın bəd üzü ilə bərabər, xoş üzü də vardır. Odu ki, “... informasiyalasdırma bəşəriyyətin inkişafını sürətləndirməklə yanaşı, milli, regional və qlobal təhlükəsizliyə yeni təhdidlər də yaradır” [7].

Lakin dünyada gedən bu proseslərdən – informasiya müharibələri və toqquşmalarından kənarda qalmaq mümkün deyildir. Bu isə təbii olaraq, informasiya təhlükəsizliyini aktuallaşdırmış olur. İnformasiya təhlükəsizliyinin texnogen xarakterli problemləri ilə yanaşı, informasiyanın məzmunundan irəli gələn infogen mənşəli problemləri də vardır.

Bir zamanlar insanlar informasiyanın qıtlığından, azlığından əziyyət çəkirdilərsə, hal-hazırda bu proses tamamilə əksinə cərəyan edir. Bu gün bəşəriyyət informasiyanın ifrat bolluğunun, informasiya selinin içərisində “itib-batmaq” təhlükəsi ilə üz-üzədir. Bu da dünyanı informasiya təhlükəsizliyi paradığına qarşısında qoymuşdur. Belə bir reallıq kontekstində folklorun yerinin və rolunun qiymətləndirilməsi, onun imkanlarının ortaya çıxarılması olduqca aktualıq kəsb edən məsələdir

III. FOLKLOR İNFORMASIYA TƏHLÜKƏSİZLİYİ KONTEKSTİNDƏ

Məlumdur ki, hazırda İnternet informasiya mübadiləsi və kommunikasiyanın əsas vasitəsinə çevrilmişdir. İnsanlar ən müxtəlif ehtiyac və zərurətlə əlaqədar olaraq günün daha çox hissəsini İnternetdə keçirirlər. Bu isə İnternet ətrafında müəyyən bir sosiomu formalaşmışdır. Burada gedən proseslərə müvafiq olaraq, dünyanın müxtəlif ölkələrinin qanunvericiliyində dəyişikliklər edilmiş, kibercinayətkarlığa qarşı mübarizənin hüquqi tənzimlənməsi ilə bağlı müvafiq qərarlar qəbul olunmuşdur. Lakin bütün bunlara baxmayaraq, bu gün İnternet vasitəsilə – sosial şəbəkələr, söhbət otaqları (chat rooms), sayt və bloqlarla insanların aldadılması, insan alveri, psixoloji təsiretmə (“Mavi Balina” hadisəsi – qorxutma, hədələmə, tabe etdirmə kontekstində), cəmiyyəti yalan və şayiələr vasitəsilə yönləndirmə faktları kifayət qədər geniş yayılmışdır.

Təsədüfi deyildir ki, “Mətn analizi və kibercinayətkarlıq”la bağlı geniş tədqiqatlar aparan Berry M.W. və Kogan J. İnternetin bu məsələdə rolunu aşağıdakı kimi şərh edir: “İnternet böyüməyə və daha gənc nəsillərə təmas etməyə davam edir. Sınıf yoldaşları, dostlar və ümumi maraqları olan insanlarla əlaqə qurmaq imkanları getdikcə artır. Elektron poçt, onlayn çat və sosial şəbəkələr eyni şəhərdəki insanlarla bərabər, dünyanın o biri başındakı şəxslərlə də ünsiyyət saxlamağımıza şərait yaradır. Təəssüflər olsun ki, yeni texnologiyadan neqativ işlər üçün istifadə etmə fürsəti onun özü ilə bərabər gəlir. İnternetdən və söhbət otaqlarından xeyli əvvəllər də cinsi zorakılar və yırtıcılar var idi. Kiberzorakılıq və internet yırtıcılığı kompüter istifadə etmədə kifayət qədər təcrübəyə sahib olmayan, xüsusilə də yeniyetmə və gənclər üçün təhlükə yaradır. İnternet əlaqəsi cib telefonlarına qoşulduqca, portativ oyun cihazları və çox oyunçulu oyun konsolu gənclərin təması və istifadəsi üçün daha böyük yollar açdı” [3]

İnternet mühitinin hüququn formalaşdırılması, buradakı proseslərin hüquqi tənzimlənməsi, cinayətkarlığın qarşısının alınması və s. kimi məsələlər İnternet mühitində fərdi məsuliyyətin gücləndirilməsini zəruri edir. Lakin İnternetə daxil olmaq və ondan istifadə etmək azad xarakterlidir. İnsanlar İnternetə daxil olarkən hər hansı bir biometrik məlumatlarla – üz cizgisi, əl izi və s. ilə deyil, İP ünvanlarla qeyd olunurlar. İP ünvanların müəyyən bir qurğu barədə məlumat verməsinə baxmayaraq, həmin qurğunun arxasında kimin əyləşdiyini müəyyənləşdirmək, geniş mənada desək, istifadəçilərin identifikasiya olunması çox çətin məsələdir. Yaxud bu gün real sosial-mədəni proseslərin virtual mühitə transformasiyası, eləcə də virtual mühitin, sosial şəbəkə, bloq və saytların sosial-mədəni proseslərin cərəyan etdiyi əsas məkana çevrilməsi kontekstində, gizli sosial qrupların yaranması, onlar arasında müəyyən metaforik-simvolik işarələrlə şifrələnmiş kommunikasiya imkanların mövcud olması müşahidə olunur ki, belə proseslərin də aşkarlanması olduqca mürəkkəbdir. Deməli, İnternetdə dövriyyədə olan məlumatların çox hissəsi anonim xarakterli daşıyır. Başqa sözlə desək, anonimlik İnternetin fəlsəfəsindən (müqayisə üçün qeyd edək ki, anonimlik və yaxud kollektivlik folklor proseslərinin cərəyan etməsi üçün “hava və su” qədər vacib məsələdir) irəli gəlir. Tədqiqatçılar qeyd edir ki, “İnternetin anonim təbiəti kibercinayətkarlığın yayılmasına kömək edə bilər” [3]

Bununla əlaqədar olaraq, İnternet istifadəçilərinin identifikasiyası üçün səs, şəkl, dəsti-xəttin, üslubun (leksikonun) analiz olunması çox aktual məsələdir. Məsələn, hər hansı bir şəxsin profili onun üslubu, leksikonu, şifahi və ya yazılı nitq aktında buraxdığı səhvləri, cümlənin strukturu, təkrarları ilə müəyyən olunur. Bunun üçün mətnlərin kompüter analizi deyilən fənn vardır ki, e-dövlətin təhlükəsizliyi kontekstində bir sıra metodlardan istifadə olunur [2]. Berry M.W. və Kogan J. yazırlar ki, “müxtəlif qaynaqlardan kibercinayətkarlıq və kiberyırtıcılıqla bağlı transkriptləri araşdırarkən, kibercinayətkarlıq və kiberyırtıcılar tərəfindən kimliyin maskalanması və aldatmada istifadə olunan oxşar taktikalarla qarşılaşırıq” [3]. Müəlliflərin qeyd etdiyi oxşarlığı təkcə taktikalarda deyil, eyni zamanda, kollektiv reaksiya və

münasibətə əsaslanan folklorik deyim, davranış və ifadələrdə müşahidə etmək mümkündür.

Bir sözlə, identifikasiya üçün bir sıra üsullar mövcuddur. Lakin bəzən həmin üsulların özü də yetərli olmur. Təhlükəli və ya şübhəli obyekt haqqında nə şəkil, nə səs, nə də hansısa bir biometrik məlumat əldə oluna bilmir. Yalnız həmin obyektin göndərdiyi mətnlər, müəyyən nitq bütövləri və ya cümlələr əlçatan olur ki, məhz bunlar əsasında analiz aparmaq zərurəti yaranır. Belə bir məqamda folklor informasiya təhlükəsizliyində “ümid yeri” kimi ortaya çıxır.

İnformasiya təhlükəsizliyi kontekstində folklorun rolu onun daşdığı mahiyyət və spesifikasi ilə bağlıdır. Hesab edirik ki, informasiya təhlükəsizliyinin təmin edilməsində folklorun verdiyi unikal imkanları aşağıdakı aspektlərdən dəyərləndirmək olar:

Folklor sosial qrupun spesifik kimliyi kimi

- Fərd aid olduğu sosial qrupun folklorik portretini işarələyir;
- Fərd aid olduğu sosial qrupun peşə, dünyagörüş, kollektiv maraq spesifikasiyalarını təcəssüm etdirir;
- Fərd aid olduğu folklor qrupunun ənənəviləşmiş, sabitləşmiş, digər üzvlər tərəfindən “tanınan” davranış və leksikon özəlliyinə sahibdir;

Folklor etnik identifikator kimi

- Folklor onu yaradan və ya danışanın milli kimlik (etnik və qrup kimliyi), milli xarakter və tipologiyasının müəyyənləşməsində açar rolunu oynaya bilər;
- Folklor milli obraz, süjet və motivlərin spesifik cizgilərini əks etdirən güzgüdür;
- Folklor danışıldığı dili, üslubu və dialekt spesifikasiyasının təcəssüm etdirən kommunikativ aqtdır;

Folklor kriptografik informasiya kimi

- Folklor gerçəkliyi və ya situasiyaları metaforik-simvolik işarələrlə əks etdirən spesifik işarələr sistemində malikdir;
- Folklor faktı arxasında müəyyən bir informasiya və ya mesaj olan “indeksdir” [9]
- Folklor nitq aktı içərisində başqaları tərəfindən anlaşılmayan yerli deyim, frazem və sözlərdə ehtiva olunmaq imkanına malikdir;

Bu mənada folklor informasiya təhlükəsizliyində unikal imkanlara malik kodlaşmış, kriptografik informasiya mənbəyidir. Həmin informasiya əsasında götürülən obyekt barədə ilkin koordinatları müəyyənləşdirmək mümkündür. Çünki hər bir fərd, o cümlədən İnternet istifadəçisi kommunikativ prosesdə və yaxud hər hansı bir davranış aktında aid olduğu folklor mühitini, folklor qrupunu, nəhayət folklor kimliyini istər-istəməz büruzə etdirir. Bu isə folklor vasitəsilə informasiya təhlükəsizliyi kontekstində müəyyən bir kontentin, yazılı və ya şifahi nitqin müəllifinin, gizli sosial qrup

və proseslərin **folklor profilini** yaratmağa imkan verir. Kompüter texnologiyaları və müəyyən analitik metodlarla həmin folklor profilini ən müxtəlif parametrlər üzrə xarakterizə etmək mümkündür. Təbii ki, burada “məqalələr, veb səhifələr, müzakirə forumları, bloqlar kimi mətnlərin geniş blokundan əsas terminləri, xüsusiyyətləri, hadisələri çıxarmaq və atributlar arasında münasibətlərin müəyyən olunmasında istifadə olun”an text mining metodlarından yararlanmaqla “avtomatik olaraq müxtəlif yazılı mənbələrdən informasiyanı” çıxarmaq “yeni, əvvəllər məlum olmayan informasiyanın kompüter tərəfindən aşkar” etmək mümkündür. [2]

Berry M.W. və Kogan J. kibercoraklıq və kibercinayətkarlıqla mübarizədə text mining texnologiyalarının mühüm rol oynaya biləcəyini vurğulayaraq qeyd edir ki, “text mining-in alt sahəsi kimi sosial baxımdan əlaqəli və çox maraqlı olan bu istiqamət elmi ictimaiyyətin diqqətini cəlb etmək üçün yalvarır”. Tədqiqatçılar həmçinin bu məsələdə multidissiplinar yanaşmanı da irəli sürürlər: “kibercinayətin anlaşılması, təsbit edilməsi və qarşısının alınması məsələsində şəbəkə mühəndislərinin, psixoloq alimlərin, sosioloqların, hüquq-mühafizə orqanlarının və kommunikasiya mütəxəssislərinin qarşılıqlı əlaqəsi” çox vacibdir. [3].

Hesab edirik ki, ümumilikdə informasiya təhlükəsizliyinin müxtəlif parametrləri üzrə (kibercinayətkarlıq, kibercoraklıq, aldatma və s.) analizlərin aparılmasında folklorlardan istifadənin imkanları da təhlil olunmalı, bu istiqamətdə yeni metod və üsullar araşdırılmalıdır. Çünki psixoloji gerçəklik – təbii-emosional mahiyyətdən qaynaqlanan, sosial mühit və şəraitlə, lokal məkan və coğrafiya ilə, linqvistik tipologiya – yerli dil və dialektlə, milli xarakter və stereotiplərlə bağlı olan folklor milli identikliyin müəyyənləşdirilməsi baxımından informasiya təhlükəsizliyinin komponenti kimi araşdırma üçün geniş imkanlar açır.

IV. FOLKLORUN İNFORMASIYA TƏHLÜKƏSİZLİYİ

Məlumdur ki, folklor milli identikliyin predmeti kimi strateji əhəmiyyət kəsb edir. İnformasiya təhlükəsizliyində folklorun rolu olduğu kimi, müasir dövrdə rəqəmsallaşan dünyada folklor informasiyasının da özünəməxsus təhlükəsizlik problemləri vardır. Bu sahədəki mövcud tədqiqatları, əldə olunmuş qənaət və nəticələri ümumiləşdirsək, problemin üç əsas istiqamətini vurğulamaq olar:

1. Milli folklor resurslarının müasir dünyanın informasiya tələblərinə, rəqəmsal standartlarına uyğunlaşdırılması və elektron mühitdə yerləşdirilməsi məsələləri;
2. Milli rəqəmsal folklor resurslarının informasiya təhlükəsizliyinin təmin edilməsi məsələləri:
 - Folklor resurslarının etibarlı saxlanması;
 - Folklor resurslarının tamlığının qorunması;
 - Folklor resurslarına əlyətərliliyin təmin olunması;
3. Milli rəqəmsal folklor resurslarının İnternet analizinin aparılması məsələləri;

- real mühitdən toplanılmış rəqəmsal folklor resurslarının İnternet analizi;
- virtual mühitdə gedən folklor proseslərinin intellektual analizi.

Kompyuter folklorşünaslığı üzrə sanballı tədqiqatlar müəllifi olan Timothy R.Tangherlini bu sahədə 4 istiqamətə xüsusi diqqət yetirilməsini qeyd edir:

- 1) toplama və arxivləşdirmə,
- 2) indeksləşdirmə və klassifikasiya,
- 3) vizuallaşdırma və naviqasiya,
- 4) analiz [12]

Bəllidir ki, uzun illər ərzində folklor nümunələrinin toplanılması, tərtibi və nəşri istiqamətində xeyli işlər görülmüş, milli arxivlər və kolleksiyalar hazırlanmışdır. Lakin həmin folklor nümunələrinin elektronlaşdırılması, rəqəmsal texnologiyalar əsasında sistemli şəkildə standartlaşdırılması və İnternet mühitində yerləşdirilməsi müasir dövrün informasiya reallıqlarından doğan zərurətdir. Qloballaşan dünyada milli identikliyin qorunması məhz İnternet mühitinə sistemli şəkildə inteqrasiya olunmaqdan keçir. Bu isə öz növbəsində elektron informasiya mühitinin spesifik problemləri ilə – informasiya təhlükəsizliyinin təmin olunması ilə müşayiət olunur. “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” [6;10] E-dövlətin mühüm komponentlərindən biri kimi, milli-mənəvi dəyər kəsb edən qeyri-maddi mədəni irsin, folklorun da elektron mühitdə kənar təhdidlərdən etibarlı və hər tərəfli şəkildə qorunması çox vacib və strateji məsələdir.

Bir sıra dünya ölkələrinin təcrübəsinə nəzər saldıqda aydın olur ki, informasiya texnologiyalarının tətbiqi əsasında folklor arxivlərinin rəqəmsallaşdırılması, onların müxtəlif parametrlər üzrə təsnif olunması, həmin folklor resursları üzərində analizlərin aparılması istiqamətində mühüm işlər görülmüşdür [1].

Lakin “Big Data” erası kimi xarakterizə olunan hazırkı mərhələni T.R.Tangherlini zəngin folklor resursları (tarixi, rəqəmsal doğulan (rəqəmsallaşdırılan deyil, birbaşa olaraq, rəqəmsal mühitdə yaranan mənasında – H.Q.) yaxud hibrid formalı) ilə kompyuter tədqiqatlarının aparıldığı ilkin dövr” [11, 10] kimi qiymətləndirir. Alim yazır ki, bir çox folklor kolleksiyalar mühəndislər tərəfindən tətbiq olunan ümumi standartlara “Big Data”-dan daha çox “orta və kiçik” verilənlərə uyğun gəlsələr də, bu yanaşmaların folklor üçün müvafiqliyi gözdə tutulmamalıdır. [11, 10]

V. FOLKLOR RESURSLARININ KOMPYUTER ANALİZİ

Kompyuter texnologiyalarının tətbiqi hesabına bir neçə istiqamətdə folklorun intellektual analizini aparmaq

mümkündür. İlkin olaraq, illər boyu toplanılmış və arxivləşdirilmiş folklor nümunələrinin rəqəmsal formata gətirildikdən sonra analiz perspektivləri barədə danışmaq olar.

Dünyada folklor resurslarının vahid sistem daxilində - folklor bankı çərçivəsində rəqəmsallaşdırılması, hər bir folklor vahidinin standart parametrlərlə təsnif olunması təcrübəsi mövcuddur. Tədqiqatlardan aydın olur ki, folklor resurslarının verilənlər bazası – müxtəlif arxivlərdə, kolleksiya və kataloqlarda əsasən iki istiqamətdə aparılmışdır. Bunlardan birincisi folklorun janrlar üzrə, digəri isə toplayıcı (və ya toplayıcı şəbəkəsi) üzrə sistemləşdirilməsidir [5].

Lakin bir məsələnin üzərində xüsusi dayanmaq lazımdır ki, folklor resurslarının çoxparametrliliyi intellektual analizi folklor bankına daxil edilmiş nümunələrinin pasportlaşdırılması ilə birbaşa bağlıdır. Çünki folklor nümunəsi sahədən toplanarkən onunla bağlı kontekstual məlumatların da qeyd olunması çox vacib məsələdir. Məsələn hər hansı bir folklor vahidinin təsnif edilməsi ilə bağlı aşağıdakı informasiyaların qeyd olunması lazımdır:

Söyləyici ilə bağlı məlumatlar – yaş, peşə, cins, məkan (doğulduğu yer, yaşayış yeri.), miqrasiya barədə məlumat, etnik mənşə və s.

Mətnlə bağlı məlumatlar - janr, növ, aktuallaşma situasiyası, müxtəlif parametrlər üzrə beynəlxalq kataloqlarda nömrələnmə və s.

Auditoriya ilə bağlı məlumatlar – mətnin söyləndiyi sosial qrup, peşə tərkibi, yaş həddi və s.

Təbii ki, bu meyarların sayını kifayət qədər artırmaq mümkündür və sistemin çoxölçülülüyü məhz bu meyarların sayı ilə düz mütənəsibdir. Folklor resursları nə qədər çox meyarlar əsasında təsnif olunarsa, bir folklor vahidinin nə qədər çox əlaməti qeyd olunarsa, onun üzərində intellektual analiz imkanları da bir o qədər artmış olar.

Çünki “rəqəmsal databazaların ən mühüm avantajlarından biri də məhz onların çoxölçülü analizlər üçün gərəkli olmasıdır. E.İlyefalvi qeyd edir ki, folklorşünaslar üçün verilənlər bazasının ən liberal yeniliyi ondan ibarətdir ki, burada mətnlər bir kateqoriya və ya tip üzrə əlaqələnməmişdir. Mətnlər eyni zamanda bir sıra kateqoriyalar üzrə əlaqələndirilmişdirlər ki, bu da nəhayətdə onlar arasında mövcud ola biləcək çoxölçülü münasibətləri aşkarlamağa imkan verir [5].

VI. FOLKLOR RESURSLARININ ÇOXPARAMETRLİ ANALİZİ İMKANLARI

Folklor resurslarının elektronlaşdırılaraq müxtəlif parametrlər əsasında vahid şəbəkədə yerləşdirilməsi, əslində, rəqəmsal texnologiyalarının tətbiqi ilə folklorşünaslıqda yeni imkanların yaradılmasıdır. Burada “əsas məqsəd mətn materialı üzərində çoxparametrliliyi mətn işləmələrini həyata keçirmək və daha sonra həmin mətnləri/verilənləri çox modullu bir şəbəkəyə təqdim etməklə daha geniş araşdırma suallarına cavab verməkdir” [4]

Macar tədqiqatçısı E.İlyefalvi XX əsrin əvvəllərində dövrün texnoloji imkanları çərçivəsində ortaya çıxan tip kataloqunun folklorşünaslıq tədqiqatları üçün kataliz rolunu oynadığını

qeyd edərək yazır: “Databaza özü-özlüyündə bütün suallara cavab verə bilməz. Yeni texnologiya, prosedur və nəzəriyyə ən azı həll edə bildiyi qədər cavabsız suallara cavab verəcəkdir. Bununla bərabər, bütün bunlar gələcək paradiqmanın problemi olacaqdır. Hazırkı çoxölçülü, rəqəmsal mətn hazırlığı, yeni şərh və analizlərə yol açacaq, bu da bizi, (sehr, cadu kimi) folklor mətnlərinin mürəkkəb və qarışıq fenomenlərini anlamağa yaxınlaşdıracaqdır” [4]

Göründüyü kimi, folklorşünaslıqda bir zamanlar mətnlərin motiv və ya süjetlər üzrə kataloqlaşdırılması, kolleksiya və arxivləşdirmə prinsiplərinin inkişaf etdirilməsi yeni tədqiqatlar üçün geniş imkanlar yaratmışdır. Müəyyən bir motivin dünyanın müxtəlif bölgələrinin folklor faktları üzrə izlənilmə imkanlarının yaradılması mədəni analogiyaların, iqtibas və əlaqələrin, universal psixoloji qanunauyğunluqların aşkarlanmasına gətirib çıxardı ki, bu da müasir dünya folklorşünaslığının intellektual inkişaf tarixində mühüm rol oynadı. Təbii ki, İKT-nin tətbiqi, rəqəmsal texnologiyaların yeni imkanlarından istifadə folklorşünaslığın tamamilə fərqli bir mərhələyə qədəm qoymasına gətirib çıxaracaqdır. Milli folklor resurslarının ən müxtəlif parametrlər üzrə vahid sistem daxilində rəqəmsal formatda cəmləşdirilməsi və onlar üzərində intellektual metodlarla analizlərin aparılması, heç şübhəsiz ki, yeni nəticələrin əldə olunmasına mühüm töhfə olacaqdır. Təbii ki, perspektivdə milli folklor resurslarının açıq informasiya sistemi daxilində digər xalqlara məxsus folklor resursları ilə əlaqəli şəkildə analiz imkanları daha fərqli tutuşdurma, müqayisə və qənaətlərə səbəb olacaqdır. Bu isə özlüyündə folklor informasiyasının təhlükəsiz şəkildə qorunması ilə bərabər, informasiya təhlükəsizliyi kontekstində folklorun imkanlarını daha da genişləndirəcəkdir. Belə ki, informasiya təhlükəsizliyinin predmeti ola biləcək hər hansı bir obyekt (mətn, şəkil, audio, video resurs, fərd və ya gizli sosial qrup) çoxsaylı folklor banklarının Data bazaları əsasında analiz olunma imkanı qazanacaqdır. Bu isə, informasiya təhlükəsizliyi kontekstində folklorun ən unikal və spesifik imkanlara malik təhlükəsizlik komponenti kimi araşdırılmasını bir daha zəruri edir.

VII. FOLKLOR RESURLARININ İNTERNET ANALİZİ

Folklorun informasiya təhlükəsizliyi kontekstində mühüm problemlərindən biri də rəqəmsal folklor resurslarının Internet analizinin aparılması məsələləridir. Yuxarıda da qeyd etdiyimiz kimi, burada iki əsas istiqamət mövcuddur. Bunlardan birincisi, real mühitdə toplanılmış rəqəmsal folklor resurslarının Internet analizi, digəri isə virtual mühitdə gedən folklor proseslərinin intellektual analizidir.

Müxtəlif parametrlər üzrə vahid sistem daxilində cəmlənmiş folklor resurslarının onlayn mühitdə Internet analizinin aparılması üçün çox geniş imkanlar mövcuddur:

- Hər bir rəqəmsal folklor resursuna sayğac yerləşdirməklə həmin resurslara olan müraciətləri hesablamaq mümkündür.

- Müəyyən bir zaman kəsiyində həmin folklor resurslarına olan müraciətlərin sayına əsasən reyting

müəyyənləşdirmək, hansı janrların daha aktiv, hansıların isə passiv olduğunu dəqiqləşdirmək mümkündür.

- Folklor resurslarına olan müraciətlərin hansı ərazidən, ölkə daxilindən və xaricdən olmasını aşkarlamaq, məsələn, dünya azərbaycanlıların bu resurslarla əlaqəsini izləmək maraqlı nəticələrin ortaya çıxmasına şərait yarada bilər.

- Hər hansı bir folklor resursuna müraciətlərin sayının artma və azalma tendensiyaları müəyyənləşdirilə bilər.

Virtual mühitdə gedən folklor proseslərinin intellektual analizi, əslində, Internet folklorunun araşdırılması ilə bağlı məsələdir. Bəllidir ki, bu gün arxivlərdə toplanılmış folklor resursları elektron mühitə daxil edilməklə bərabər, sosial şəbəkə, bloq və saytlar hesabına Internet folkloru da meydana gəlməkdədir. Belə folklor nümunələri real və ya virtual sosial proseslərdən qaynaqlanmasından asılı olmayaraq, onların yarandığı məkan məhz Internetdir. Bu isə həmin folklor nümunələrinin vernakular spesifikaya malik olması, mövzu, məzmun, forma və dil xüsusiyyətlərinə sahib olması ilə xarakterizə olunur. Təbii olaraq, Internet folkloru nümunələrinin də intellektual analizinə, sosial media baş verən proseslərlə əlaqənin aşkarlanmasına, Internet folkloru faktlarının sosial motivatorlarının müəyyənləşdirilməsinə, aktiv folklor formalarının üzə çıxarılmasına, dövrüyyədə olan və ənənəviləşən folklor qəliblərinin öyrənilməsinə, təkrarlanan folklor “tema”larının qeyd olunmasına, müəyyən bir zaman kəsiyində meydana çıxan folklor faktlarının məzmun baxımından təhlil olunmasına, həmin məzmunun sosial proseslərlə korelyativ əlaqələrinin diqqət mərkəzinə gətirilməsinə böyük zərurət vardır.

NƏTİCƏ

Problemlə bağlı mövcud elmi ədəbiyyatların təhlili onu göstərir ki, informasiya təhlükəsizliyi kontekstində folklorun rolu, eyni zamanda folklorun özünün informasiya təhlükəsizliyi məsələsi kifayət qədər aktual və az araşdırılmış sahədir. Internetin sürətlə genişlənməsi, insanların gündəlik həyat rejimində yeri və rolunun artması, ən müxtəlif ehtiyac və istəklər baxımından şəxslərin ondan asılılığın güclənməsi, bütövlükdə, informasiya təhlükəsizliyinin aktuallaşmasına – kibercinayətkarlığın, kiberzorakılığın, gizli sosial şəbəkə və proseslərin üzə çıxarılmasına gətirib çıxarmışdır. Müəyyənləşdirilmişdir ki, bu kontekstə folklor unikal imkanlara malikdir. Qeyd olunmuşdur ki, informasiya təhlükəsizliyinin predmeti kimi, milli folklor resurslarının etibarlı saxlanması, bütövlüyünün və tamlığının qorunması, həmin resursların əlyətərliliyinin təmin olunması müasir dövrün aktual çağırışlarından biridir.

ƏDƏBİYYAT

- [1] Abello, James – Broadwell, Peter – Tangherlini, Timothy R. 2012 Computational Folkloristics. Communications of the ACM 55(7):60–70.
- [2] Alıquliyev Ramiz, Niftəliyeva Günay. 2016. “E-dövlətin analizi texnologiyaları: text mining və sosial şəbəkələr”. Ekspres informasiya. “İnformasiya texnologiyaları” seriyası. Bakı, “İnformasiya Texnologiyaları” nəşriyyatı, 78 səh.

- [3] Berry Michael W. and Kogan J. 2010. Text mining : applications and theory. Wiley A John Wiley and Sons, Ltd., Publication, 207 p.
- [4] Emese Ilyefalvi. 2017 Textualization Strategies, Typological Attempts, 37 Digital Databases: What is the Future of the Comparative Charm Scholarchip? Incantatio An International Journal on Charms, Charmers and Charming Issue 6, Tartu, p. 37-78
- [5] Emese Ilyefalvi. 2018. The Theoretical, Methodological and Technical Issues of Digital Folklore Databases and Computational Folkloristics. Acta Ethnographica Hungarica 63(1), 209-258, p. 218
- [6] Əliquliyev R.M., İmamverdiyev Y.N. E-Dövlətin informasiya təhlükəsizliyi: aktual tədqiqat istiqamətləri. İnformasiya cəmiyyəti problemləri, №1, 2010.
- [7] İmamverdiyev Y.N. E-Dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli. İnformasiya cəmiyyəti problemləri, №1(7), 2013, s. 20-31.
- [8] Информационная безопасность систем организационного управления. Теоретические основы: в 2 т. / Н.А. Кузнецов, В.В.Кульба, Е.А.Микрин и др., М., Наука, 2006
- [9] McNeill, Lynne S. “The internet is weird”. Folkloristics in the digital age. Folklore Fellows’ Network. № 47, December 2015, p. 12-13, 16-17, p. 16
- [10] Мешкова Т.А. Социально-политические аспекты глобальной информатизации // Полис. М., 2002. № 6, с. 24-33
- [11] Tangherlini, Timothy R. 2016. Big Folklore: A Special Issue on Computational Folkloristics. The Journal of American Folklore, Vol. 129, No. 511 (Winter), pp. 5-13
- [12] Tangherlini, Timothy R. 2013. The Folklore Macroscopic: Challenges for a Computational Folkloristics. Western Folklore 72(1): 7–27.

**FOLKLORE IS IN INFORMATION SECURITY AND
INFORMATION SECURITY IN FOLKLORE**

Hikmat Guliyev
ANAS Institute of Folklore
guliyevh@mail.ru

Abstract - The article examines the role of folklore in the context of information security and at the same time the problems about the information security of folklore. The rapid expansion of the Internet, increasing role and place of people in daily life, becoming stronger dependence on people from the point of view of different needs and desires has led to the actualization of information security – cybercrime, cyberbullying, the secret social networking and processes. It has been determined that folklore has unique opportunities in this context. It was also noted that, as the subject of information security, the reliable preservation, integrity of national folklore resources, ensuring the equity of these resources are the actual challenges of the modern era. At the same time, classifying the digital folklore resources according to the various parameters and the perspectives about the realization of their intellectual analysis in the Internet were also explained

Keywords - information security, folklore, digital folklore, protection of folklore, Internet folklore, computational folkloristics, cybercrime, national identification

İnternetdə Azərbaycan əlifbası ilə domen adlarının tərtib olunması məsələsi haqqında

Rəna Qasımova

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

cocukr@gmail.com

Xülasə—Məqalədə İnternetdə Azərbaycan əlifbası ilə domen adlarının tərtibatındakı mövcud vəziyyət və problemlər analiz edilmişdir. Bu məqsədlə yüksək səviyyəli beynəlmilləşdirilmiş domen adlarının (IDN) qeydiyyatı prosesi araşdırılmışdır. Azərbaycan əlifbası ilə yazılmış yüksək səviyyəli domen adlarının yaradılması ilə bağlı bəzi tövsiyələr verilmişdir.

Açar sözlər— domen; yüksək səviyyəli domenlər; ICANN; IDN; DNS

I. GİRİŞ

İnformasiya texnologiyaları sahəsinin hazırda ən sürətli inkişaf edən istiqamətlərindən biri İnternetdir. Bu gün İnternet ənənəvi xidmətlərlə yanaşı, daha yüksək imkanlara malik yeni xidmətlər də göstərməkdədir (e-commerce, e-banking, e-idarəetmə, e-təhsil, e-tibb və s.). Hazırda İnternet 240-a qədər ölkəni birləşdirir. İnternetə qoşulan istənilən kompüter, mobil telefon müəyyən rəqəmlər yığımından ibarət olan unikal kodla identifikasiya olunur. Özünün texniki mahiyyətinə görə belə kod, verilən kompüterin IP-ünvanını təşkil edir.

Şəbəkə istifadəçilərinə İnternetdəki kompüterlərin ünvanlarını rəqəmlə ifadə edərək əməliyyat aparmaq, rəqəmləri yadda saxlamaq çətin olduğundan domen adları sistemi (DNS) yaradılmışdır. DNS İnternet infrastrukturunun ən mühüm komponentlərindən biridir və əsas təyinatı domen adlarını IP-ünvanlara və IP-ünvanlarını domen adlarına çevirməkdir. Domen (ingilis dilində “domain” sözü latın dilində sahib olma, malik olma mənasını verən “dominium” sözündən əmələ gəlmişdir) İnternetin məntiqi səviyyəsidir. Başqa sözlə, domen – domen adları fəzasının mərkəzləşdirilmiş sahəsidir [1].

1984-1985-ci illər ərzində birinci yüksək səviyyəli domenlər (*Top Level Domain, TLD*) tətbiq edilmişdir: *.com*, *.org*, *.net*, *.edu*, *.gov*, *.mil*. 1988-ci ildə standartlaşdırma üzrə Beynəlxalq təşkilat (ISO) tərəfindən ISO 3166-1 beynəlxalq standartına uyğun ölkə və ərazilərin ikihərflə kodlarına əsaslanan ikinci səviyyəli milli domenlər meydana gəldi (*country code Top Level Domain, ccTLD*). Bu domenlərdən biri də *.az* Azərbaycan zonasıdır.

İnternetdə adlar zonasının müəyyənləşdirilməsi və ünvanlaşdırmanın idarə edilməsi qeyri-kommersiya təşkilatı–

ICANN (Internet Corporation for Assigned Names and Numbers) tərəfindən həyata keçirilir. Domen adlarının beynəlmilləşdirilməsi üzrə çoxdilli sistemin (Internationalized Domain Names, IDN) yaradılması İnternet şəbəkəsinin inkişafı istiqamətində aparılan ən mühüm addımlardan biridir. İnternet Mühəndisliyi üzrə İşçi Qrupu (ing. Internet Engineering Task Force, IETF) tərəfindən yaradılan sistemdə əsas məqsəd milli əlifbanın simvollarından istifadə etməklə domen adlarının reallaşdırılması üçün tələblərin hazırlanmasıdır. Qrupun qarşısında duran digər məsələlərdən biri də mövcud vəziyyətin araşdırılması, texniki və sosial aspektləri nəzərə almaqla təkliflərin verilməsidir. Bu mühüm faktı nəzərə alaraq, milli əlifba ilə yazılmış domen adlarının alınması məsələlərinin araşdırılması, tədqiq olunması olduqca zəruri və aktualdır [2-4].

II. MİLLİ DOMEN ADLARININ TƏRTİB OLUNMASINDA MÖVCUD VƏZİYYƏT VƏ PROBLEMLƏR

Domen adlarının bilavasitə bölüşdürülməsi paylanmış qeydiyyat adlanan sistem üzrə həyata keçirilir, yəni yüksək səviyyəli domendə ikinci səviyyəli domen adını ICANN-nın akkreditə etdiyi qeydiyyatçılardan biri ilə müqavilə bağlamaq yolu ilə almaq olar. ICANN bilavasitə domen adlarının qeydiyyatı ilə məşğul olmur [5].

Qeyd etmək lazımdır ki, 1998-ci ildə Tətbiqlərdə Domen Adlarının Beynəlmilləşdirilməsi (Internationalizing Domain Names in Applications – IDNA) sistemi standart kimi qəbul edildi və bir çox yüksək səviyyəli domen adlarında tətbiq edildi. IDNA standartı tərkibində Unicode simvolları olan beynəlmilləşdirilmiş domen adlarının istifadə oluna bilinməsi üçün 2003-cü ildə bir mexanizm kimi qəbul edildi. Bu mexanizm çərçivəsində domen adlar diakritiklərlə (ə, ğ, ö və ya ü kimi) birlikdə latın hərflərindən və ya qeyrilatin əlifbasının simvolları ilə yazılırdı (məsələn, ərəb, Çin və digər əlifbalar).

ICANN 2003-cü ildə IDNA-nın istifadəsi üçün siyasət yaratdı və həmin ildə bu sistem əsasında *.jp* və 2004-cü ilin mart ayında *.info* domenlərinin altdomenlərində bir neçə domen adını qeydiyyatdan keçirdi. Yaradılmış bu siyasət 2004-cü ilin noyabr ayında yenidən baxılaraq yaxşılaşdırıldı və ölkələrin yüksək səviyyəli domenlərinin milli əlifba ilə yazıla bilməsi üçün 2009-cu ilin oktyabr ayında ICANN qərar

“İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri”
IV respublika konfransı, 14 dekabr 2018-ci il

qəbul etdi. Təşkilatın mütəxəssisləri ərəb, çin, yunan, yapon, ərəb, rus və digər dillərdə domen adlardan ibarət saytları testdən də keçirdilər.

Qəbul olunan yeni qaydalara görə, indiyədək mövcud olan milli domenlər (*.az, *.ru və s.) və təxminən 20 neytral domen suffiksləri (*.com, *.net, *.info və s.) ilə yanaşı, 2009-cu ildən başlayaraq, 37 simvoldan çox olmamaqla a-z, 0-9 və defisdən ibarət ola bilən (məsələn, *.asia, *.baku, *.bank, *.men, *.sevgi və s.) istənilən toponim və adlarla domen sonluqlarının qeydiyyatına icazə verilir. Beləliklə, ilk dəfə Misir, Səudiyyə Ərəbistanı və Rusiya öz ölkə domen kodlarının milli əlifba ilə ccTLD DNS serverlərinin kök zonasında qeydiyyatını apardılar. Hal-hazırda yüksək səviyyəli domen zonasında yerləşdirilmiş və geniş şəkildə istifadə olunan yüksək səviyyəli domen adlarının 22-i müxtəlif ölkələrdə istifadə olunan milli əlifba ilə yazılıb [6].

ICANN iri şəhərlərin əksəriyyətinin öz domen adlarının alınmasında (məsələn, .moscow, .qatar, .paris, .berlin) maraqlı olduqlarını bildirir. Həmin qurumda bu kimi domen adlarının yaradılmasının mümkünlüyü ilə bağlı məsələlər indi də müzakirə edilir. ICANN Sinqapurda keçirilən 41-ci konfransda (20-25 iyun, 2011-ci il) qlobal şəbəkə tarixində növbəti inqilabi dəyişikliklərdən birinə imza atdı. 2012-ci ildən yeni yüksək səviyyəli domenlərin –New gTLD qeydiyyatına icazə verildi. Yeni qərara əsasən, artıq iri şirkət və şəhərlərin özlərinə məxsus domen adlarının alınmasında heç bir məhdudiyyət yoxdur. Məsələn, üçün, ənənəvi .com, .org və digər domen zonalarının yerinə İnternet-istifadəçiləri .apple və ya .baku və s. domen ünvanlarını qeydiyyatdan keçirmək olar.

ICANN domen sonluqlarının sayının əhəmiyyətli dərəcədə artırılmasını planlaşdırır. Yeni qərardan sonra veb-saytların ünvanı istənilən dildə istənilən sonluqla bitə bilər. Qərar 2012-ci ildə qüvvəyə mindi. “Bu qərar yeni İnternet dövrünün başlanmasına dəlalət edir”, - deyərək ICANN-ın İdarə Heyətinin sədri Piter Denqet Traş qeyd edib. Onun sözlərinə görə, korporasiya həmçinin qeyri-latin qrafikalı domen adlarını da dəstəkləmək imkanına malik tam yeni sistem hazırlayıb. Domenlərin qeydiyyatı üçün sifarişlər 2012-ci il yanvarın 12-dən başladı. O zaman 1930 ərizədən 116-sı IDN-nə aid idi [1].

New gTLDI –də domen adının alınması daha mürəkkəb prosesdir. Bunun üçün ICANN tərəfindən akkreditə olunmuş qeydiyyatçının tələblərinə əməl etmək və rüsum ödəmək lazımdır. New gTLD domeninin qeydiyyatına iddialı olan namizəd, əslində, yeni bir reyestrin yaradılmasını və İnternet infrastrukturunun bir hissəsinin idarəçiliyini öz üzərinə götürür. ICANN tərəfindən qeydiyyat dövrü elan edildikdən sonra yeni yüksək səviyyəli domen adının alınması üçün namizəd (yalnız hüquqi şəxslər) Ərizələrin Qəbulu Sistemində (TLD Application System - TAS) qeydiyyatdan keçməlidir. Bunun üçün, o, 5000 ABŞ dolları həcmində depozit ödəməlidir. Yalnız bundan sonra ona ərizə formasının tam doldurulmasına imkan yaradılır. Ərizədə iddiaçı domen adından əlavə, özü haqqında ümumi məlumatları qeyd etməli, texniki, təşkilati və maliyyə imkanları haqda suallara dolğun

cavab verməlidir. Bu müddət ərzində sifarişin qiymətləndirilməsi prosesinə başlamaq üçün ICANN tərəfindən tələb olunan 180000 ABŞ dolları tam ödənilməlidir.

Bundan əlavə, zonanın xidmət haqqı ildə 25 min dollar təşkil edir. Lakin ekspertlərin fikrincə, belə domenlərin qeydiyyatı qiymətinin çox yüksək olması yaxın gələcəkdə bu sahənin yalnız nəhəng şirkətlərin nüfuz mübarizəsi meydanına çevrilməsinə səbəb olacaq. Digərləri sifariş edilmiş zonanın normal işinin təmin olunması üçün texniki imkanlara malik olduqlarını sübut etməli olacaqlar. Beynəlmilləşdirilmiş domen adının alınması zamanı ərizədə əlavə olaraq bu adın ingilis dilində mənasının açılışı göstərilməlidir. Ərizənin qəbulu dövrü bitdikdən sonra ICANN iki həftə ərzində qiymətləndirməyə tam hazır olan sifarişləri namizədlərin ümumi məlumatları ilə birlikdə dərc edir [7 –9].

Beləliklə, 2012-ci ildən etibarən İnternetdə bir neçə yüz min sayt sonluğu olacağı gözlənilir. Cədvəl 1-də milli əlifba ilə yazılmış yüksək səviyyəli domen adlarının ICANN tərəfindən akkreditə olunmuş qeydiyyatçıların bəzilərinin siyahısı verilmişdir.

CƏDVƏL 1. ICANN TƏRƏFİNDƏN AKKREDITƏ OLUNMUŞ QEYDIYYATÇILARIN
BƏZİLƏRİNİN SIYAHISI

Ölkə	Domen	Pinkod	Latın dilində
	CAЙT	xn--80aswg	
	ОНЛАЙН	xn--80asehdb	
	ДЕТИ	XN--D1ACJ3B	
	OPГ	xn--c1avg	
	商城	xn--czru2d	
	삼성	xn--cg4bki	SAMSUNG
	网址	xn--ses554g	
	集团	xn--3bst00m	GROUP
	在线	xn--3ds443g	ONLINE
	公益	xn--55qw42g	
	公司	xn--55qx5d	
	移动	xn--6frz82g	
	我爱你	xn--6qq986b3xl	
	中文网	xn--fiq228c5hs	
	中信	xn--fiq64b	CITIC
	网络	xn--io0a7i	NET
	شبكة	xn--ngbc5azd	NET
	بازار.	xn--mgbab2bd	BAZAAR
	机构	xn--nqv7f	ORG
	组织机构	xn--nqv7fs00ema	ORG
	□□□□□	xn--ilb6b1a6a2e	ORG
	MOCKBA	xn--80adxhks	MOSCOW
	みんな	xn--q9jyb4c	
	موقع	xn--4gbrim	
	世界	xn--rhqv96g	
	商标	xn--c2r694b	
	政务	xn--zfr164b	
	游戏	xn--unup4y	
	РУС	xn--p1acf	RUS
	八卦	xn--	
	グーグル	xn--qcka1pmc	GOOGLE
	谷歌	xn--flw351e	GOOGLE
	网店	xn--hxt814e	

“İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri”
IV respublika konfransı, 14 dekabr 2018-ci il

Ölkə	Domen	Pinkod	Latın dilində
	商店	xn--czrs0t	
Əlcəzair	الجزائر	xn--lgbbat1ad8j	Al Jazair
Honkonq	香港	xn--j6w193g	Hong Kong
Misir	مصر	xn--wgbh1c	Misr
Hindistan	भारत, भारत, भारत, भारत, भारत	Bharat	Bharat
İordaniya	الأردن	xn--mgbayh7gpa	Al-Ordon
İran	ایران	xn--mgba3a4f16a	IRAN
Qazaxıstan	ҚАЗ	xn--80ao21a	Kaz
Qətər	قطر	xn--wgb16a	Qatar
Çin	中国, 中國	xn--fiqs8S, xn--fiqz9S	Zhongguo
Malaziya	ماليزيا	xn--mgbx4cd0ab	
Mərakeş	المغرب	xn--mgbc0a9azcg	al-Maghrib
Monqolustan	МОН	xn--11acc	MON
Birləşmiş Ərəb Əmirlikləri	امارات	xn--mgbaam7a8h	.EMARAT
Yəmən	عمان	xn--mg9awbf	Oman
Fələstin	فلسطين	xn--ygb12ammx	Falasteen
Koreya Respublikası	한국	xn--3e0b707e	
Rusiya Federasiyası	РФ	xn--p1ai	RF
Səudiyyə Ərəbistanı	السعودية	xn--mgberp4a5d4ar	.ALSAUDIAH
Serbiya	СРБ	xn--90a3ac	Srb
Sinqapur	新加坡	xn--yfro4i67o, xn--clhc0ea0b2g2a9gcd	Singapore
Siriya	سورية	xn--ogbpf8fl	
Tayland	ไทย	xn--o3cw4h	Thai
Tayvan	台灣, 台湾	xn--kpry57d, xn--kprw13d	
Tunis	تونس	xn--pgbs0dh	Tunis
Ukrayna	УКР	xn--j1amh	UKR
Şri-Lanka	ශ්‍රී ලංකා	xn--xkc2al3hye2a	Ilangai

İnternet ünvanlarının bundan sonra təkcə ingiliscə deyil, digər dillərdə, o cümlədən ərəb, kiril, Çin və digər milli əlifbaların hərfləri ilə yazılma mümkünlüyü beynəlmilləşdirilmiş domen adlarının yaradılmasını aktuallaşdırır. Beynəlmilləşdirilmiş domen adlarının yaradılması domen adlarında milli əlifbaların istifadəsini zəruri edir. Milli əlifba ilə yazılmış domen adları, domen adlarının bir və ya tam hissəsinin ərəb, kiril, Çin və s. kimi dillərdə, yaxud latın əlifbası ilə tam eynilik təşkil etməyən fransız, alman, Azərbaycan və bu kimi dillərdə istifadə olunan simvollar vasitəsi ilə yazılmasıdır.

Azərbaycan üçün də belə yüksək səviyyəli domen adlarının alınması məqsədəuyğundur. Ölkəmizdə Azərbaycan dili rəsmi dövlət dilidir və əhalinin əksəriyyəti bu dildə danışır. Həmçinin Azərbaycan əlifbası latın qrafikalıdır, burada sırf Azərbaycan dilinə məxsus olan hərflər (məsələn ğ, ə, ü və s.) vardır. Məsələn, Bakı, Gəncə, Sumqayıt və s. kimi iri şəhərlərimiz üçün *.bakı, *.gəncə, *.sumqayıt kimi adlarda yüksək səviyyəli domen adlarının qeydiyyatdan keçirilməsi çox vacib addımlardan biridir. Bu həmin şəhərlərin əhalisinin İnternet resurslarından istifadə imkanlarını artıracaq. Həmin

addım ölkədəki domen adlarının qeydiyyatında mövcud olan problemlərin qarşısını almış olar.

Digər tərəfdən məsələn, “məktəb.az” domen suffiksi üzrə ölkədəki bütün məktəblərin veb-resurslarının yaradılması və yaxud “sığorta.az”, “mədəniyyət.az”, “ədliyyə.az” kimi yeni adların tətbiqi yerli qurumların virtual sistemdə təsnifatına imkan verməklə yanaşı, yerli istifadəçilərin İnternetdən istifadəsini asanlaşdıracaq [10, 11].

Qeyd etmək lazımdır ki, 2007-ci ilin 17-19 noyabr tarixində Bakıda keçirilən “Türk Dövlət və Cəmiyyətlərinin XI Dostluq, Qardaşlıq və Əməkdaşlıq Qurultayı”nda AMEA-nın İnformasiya Texnologiyaları İnstitutu tərəfindən ICANN qarşısında TURAN, TURK domen adlarının sTLD statusunda daxil edilməsi təklifi irəli sürülmüş və bu təklif qəbul olunaraq müvafiq qərar qəbul edilmişdir [1].

Azərbaycanın milli əlifbası ilə domen adlarının tərtibi üçün “Domen adlarının Qeydiyyatı Qaydaları” təkmilləşdirilib təsdiq olunmalıdır. Həmçinin Azərbaycan dilində olan milli domen adlarından istifadə sistemi hazırlanmalıdır. Azərbaycanın milli əlifbası ilə domen adlarının tərtibatı və yazılması qeydiyyat üçün nəzərdə tutulmuş beynəlxalq qaydalara və normalara cavab verməlidir. Bu vacib məsələlər həll olunduqdan sonra ölkədə sayt yaradılarkən “ü”, “ə”, “ö” hərflərini işlətmək mümkün olacaq. Azərbaycanın milli əlifbası ilə domen adlarının yaradılması aşağıdakı problemlərin aradan qaldırılmasına kömək edəcək:

- Xarici dili bilməyən insanların, xüsusilə də, yaşlı nəslin İnternet resurslarından istifadə imkanlarını artıracaq;
- Azərbaycan dilində əmtəə nişanlarının düzgün təsvirinə imkan yaradacaq;
- Azərbaycan dilinin qrammatik qaydalarını qoruyacaq;
- Azərbaycan dilinin təhriflərdən qorunmasına səbəb olacaq;
- İstənilən toponim və adların qeydiyyatına imkan yaradacaq;
- Müəyyən domen adlarının gələcəkdə kiberskvotinq (qeydiyyatdan keçirilmiş əmtəə və ya ticarət nişanı olan domen adlarının zəbt edilməsidir) məqsədi ilə qeydiyyatdan keçirilməsinin qarşısının alınmasına səbəb olacaq və s.

Hazırda ICANN yeni domen adları ilə işləyə biləcək elektron poçt əlavələri üçün texniki standartların hazırlanmasının başa çatdığını bəyan edir. Lakin buna baxmayaraq, istifadəçilər elektron poçt adlarının yazılışı üçün hələ də latın əlifbasından istifadə edirlər. ICANN-ın məlumatına əsasən, hazırda bu quruma daxil olan səkkiz dillə bağlı ərizələrə baxılır [1].

NƏTİCƏ

Son illər Azərbaycanın İnternet mühitində ciddi keyfiyyət və kəmiyyət dəyişiklikləri baş verməkdədir. Artıq nəinki ayrı-ayrı təşkilatlar, həmçinin bir sıra fiziki şəxslər öz fərdi

saytlarını və səhifələrini yaratmaqdadırlar. Saytın adı, onun hansı domen zonasında yerləşdirilməsi və digər şərtlər İnternet fəallığının effektivliyinə təsir edən amillərdəndir.

Qeyd edildiyi kimi, artıq xeyli müddətdir ki, beynəlxalq aləmdə ayrı-ayrı ölkələrə məxsus milli əlifbalar üzrə domen adlarının qeydiyyatı prosesi həyata keçirilir. Bu dəyişiklik beynəlxalq səviyyəli şirkətlər üçün o qədər maraqlı olmasa da, yerli qurumlar üçün böyük əhəmiyyət kəsb edir.

Azərbaycanın milli əlifbası ilə domen adlarının tərtib olunması aktual məsələlərdən biridir. Ona görə də *.bakı, *.naxçıvan, *.şəki, *.məktəb və s. bu kimi yeni adların alınması üçün aidiyyət dövlət qurumları ilkin addımlar atmalıdırlar. Eyni zamanda, “əlinca.az”, “qarabağ.az”, “xankəndi.az” və s. kimi adların tərtibatı üçün mövcud olan problemlər aradan qaldırılmalıdır.

ƏDƏBİYYAT

- [1] R.T. Qasimova. İnternetdə domen problemləri və onların həlli yolları. Bakı: “İnformasiya texnologiyaları” nəşriyyatı, 2012, 164 s.
- [2] R.T. Gasimova. On intellectual analysis of domain name registration data // Информационные технологии и компьютерная инженерия, Украина, 2010, №3 (19), с. 57-61.
- [3] R.M. Əliquliyev, R.T. Qasimova. Milli domen adları intellektual analiz sisteminin yaradılması // İnformasiya Texnologiyaları Problemləri, 2011, №1, səh.29-36.
- [4] P.T. Касумова. Сравнительный анализ географических доменов верхнего уровня сети Интернет // Информационные технологии, 2011, №7, с. 18- 23.
- [5] R.M. Alguliev, R.T. Gasimova. On a approach for intellectual analysis of registration data of domain names // International Journal of Ubiquitous Computing and Internationalization. Korea, 2011, v. 3, No. 1, p. 27-30.

- [6] А.Г. Серго. Доменные имена. М. «Бестселлер», 2006, 366 с.
- [7] R.Q. Ələkbərov, M.Ə. Rəşidov, T.İ. Mustafayev, M.M. Yaqubov. Yüksək səviyyəli beynəlmilləşdirilmiş domen adları, onların qeydiyyatı və problemləri, İnformasiya cəmiyyəti problemləri, 2017, №1, səh. 51-60
- [8] R.T. Qasimova. Milli domen və kontentlərin Azərbaycandan kənarda olan serverlərdə yerləşdirilməsinin monitorinqi problemləri // İnformasiya Cəmiyyəti Problemləri, 2013, №1(7), səh.49-56.
- [9] R.T. Qasimova. Milli domen və kontentlərin Azərbaycandan kənarda olan serverlərdə yerləşdirilməsinin monitorinqi problemləri // İnformasiya Cəmiyyəti Problemləri, 2013, №1(7), s.49-56.
- [10] R.T. Qasimova. İnternetdə qlobal domen infrastrukturunun təhlükəsizliyi // İnformasiya Texnologiyaları Problemləri, 2015, №2, s. 61-67.
- [11] R.T. Qasimova. Milli domen adlarının intellektual monitorinqi sisteminin yaradılması məsələləri // İnformasiya Texnologiyaları Problemləri, 2015, №1, səh. 62-69.

ABOUT THE PROBLEM OF INTERNET DOMAIN NAMES IN AZERBAIJAN ALPHABET

Rena Kasumova

Institute of Information Technology of ANAS,

Baku, Azerbaijan

cocukr@gmail.com

Abstract -- The article is analysing existing problems and circumstances of the domain names in the internet built using Azerbaijani alphabet. The registration process for normalized domain names has been researched. Suggestions has been proposed for the domain names created using Azerbaijani alphabet.

Вопросы обеспечения энергетической безопасности инфраструктуры электронной науки

Тахмасиб Фаталиев¹, Шакир Мехтиев²

^{1,2}Институт Информационных Технологий НАНА, Баку, Азербайджан

¹depart3@iit.science.az, ²depart11@iit.science.az

Аннотация– Статья посвящена вопросам обеспечения энергетической безопасности инфраструктуры э-науки. Рассмотрена инфраструктура э-науки, как составной части современной научно-исследовательской деятельности, и показано, что организация ее непрерывной и эффективной деятельности существенно зависит от решения проблем энергетической безопасности. Проанализированы концептуальные вопросы в этой области и предложена система, обеспечивающая энергетическую безопасность инфраструктуры э-науки.

Ключевые слова– инфраструктура электронной науки, энергобезопасность, надежность, угрозы, центр обработки данных, AzScienceNet.

I. ВВЕДЕНИЕ

Бесперебойная работа энергетических систем является необходимым фактором функционирования и развития современного общества. Любые аварии в энергосистемах наносят ощутимые убытки различным отраслям промышленного производства, финансовым структурам, а также приводят к нарушению нормальной деятельности научного сектора и к отказам в работе его высокотехнологичного оборудования, создают угрозы жизни и безопасности людей. Проблемы с энергетической безопасностью (ЭБ) актуальны для различных стран вне зависимости от их экономического развития. Например, произошедшая в результате природных явлений авария в энергосистеме Нью-Йорка (New-York, USA, 1977 г.) вызвала сбои в работе городских служб, произошла остановка электротранспорта и т.п. [1]. Длительные простои, связанные с устранением возникших неисправностей, привели и к финансовым потерям. Аварии, произошедшие на Чернобыльской атомной электростанции (АЭС) (Украина) в 1986 г. и на Фукусимской АЭС (Япония) в 2011 г., расцениваются как крупнейшие по материальному и экономическому ущербу и степени опасного воздействия на окружающую среду и жизни людей. В [2] приведены примеры известных энергетических аварий, произошедших в мире за период 2003 -2015 гг.

Отметим, что современное общество характеризуется широким внедрением информационно-

коммуникационных технологий (ИКТ), которые тесно интегрированы в различные сферы деятельности. Эффективное и надежное функционирование ИКТ в большей степени, чем другие отрасли, зависит от ЭБ. Аварии в энергетических системах, как следствие угроз ЭБ, могут привести к падению интернет-трафика, сбоям в передаче данных, прекращению работы центров обработки данных (ЦОД), а также к информационным потерям, что в целом может повлиять на работу различных структур.

В предлагаемой работе рассмотрены вопросы ЭБ инфраструктуры электронной науки (э-науки), которая включает в себя научную компьютерную сеть, ЦОД, сетевые, вычислительные и информационные ресурсы научно-исследовательских институтов и университетов. Следует отметить, что основными целями э-науки являются совместная эффективная деятельность в виртуальном пространстве научных организаций, коллективов и ученых, повышение эффективности научного управления и исследовательских работ, развитие всех областей науки на уровне современных мировых стандартов и интеграция в мировую научную среду [3].

II. ОСОБЕННОСТИ ПРОБЛЕМ ЭНЕРГЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

Международное Энергетическое Агентство определяет ЭБ, как бесперебойную доступность источников энергии [4]. Некоторые авторы дополняют определение ЭБ низкой уязвимостью жизненно важных энергетических систем. Также к ЭБ относят способность энергосистемы постоянно выполнять свои функции в условиях возможных неблагоприятных ситуаций (техноэкономических, геополитических, природных и т.д.) с минимально допустимыми нарушениями в работоспособности поддерживаемой системы. Таким образом, под ЭБ понимается устойчивость энергосистемы к событиям, инцидентам или непредвиденным (чрезвычайным) обстоятельствам, вызывающим ненормальные системные условия, то есть сбои или перебои в компонентах системы. Рассмотрим некоторые совокупные свойства ЭБ [5].

Эксплуатационная безопасность – это свойство энергосистемы поддерживать или восстанавливать приемлемую работоспособность после устранения последствий инцидентов. Она охватывает динамические проблемы управления сетью в режиме реального времени.

Гибкость – это свойство энергосистемы справляться с краткосрочной/среднесрочной изменчивостью генерации (например, возобновляемой энергии) и спросом, чтобы система оставалась в равновесии.

Адекватность – это свойство энергосистемы постоянно обеспечивать общий спрос на электроэнергию при нормальных условиях эксплуатации. Она обычно включает в себя: компонент достаточности генерации/хранения, компонент сети передачи/приема, распределительную сеть и компоненты достаточности конечного пользователя.

Устойчивость – это среднесрочное свойство энергосистемы нейтрализовать последствия сбоев и восстанавливать определенный уровень производительности.

Надежность – это долгосрочное свойство энергосистемы справляться с ограничениями или воздействиями, возникающими вне инфраструктуры.

Исходя из данных предпосылок можно предложить концепцию ЭБ э-науки, которая состоит из эффективного и устойчивого распределения полученной энергии, уменьшения потерь, обеспечения непрерывной работы инфраструктуры э-науки и предотвращения как внешних, так и внутренних угроз. Этим достигается надежное, эффективное и безопасное функционирование э-науки.

Следует отметить, что на практике часто путают понятия надежности и безопасности. Надежность и безопасность – это системные свойства, возникающие в результате взаимодействия различных компонентов сложных систем: аппаратного, программного, организационного и человеческого.

Надежность – это свойство системы выполнять заданные функции, сохраняя свои эксплуатационные показатели в течение требуемого промежутка времени или требуемой наработки. Безопасность – это свойство, характеризующее степень безаварийности и функциональной безопасности системы. Статистические данные в связи с промышленными авариями за последние несколько десятилетий позволяют сделать вывод о том, что организационные и человеческие факторы играют значительную роль в риске системных сбоев и аварий на протяжении всего жизненного цикла системы. В то же время существенно увеличилась надежность аппаратных компонентов, особенно в энергетических системах, где требуются высокие стандарты безопасности. Современные энергетические системы в соответствии с заданными требованиями и критериями надежности обеспечивают эффективную работу на протяжении

длительного срока службы с минимальными рисками для безопасности персонала и окружающей среды. Для обеспечения этого необходимо контролировать развитие технологических процессов путем надлежащего планирования, проведения измерений и мониторинга. С этой целью осуществляется техническое обслуживание (ТО), которое должно обеспечивать соответствие характеристик надежности и доступности систем и компонентов в соответствии с долгосрочными и краткосрочными требованиями планируемых производственных и нормативных директив при минимальных ресурсных затратах. Цель эффективного планирования ТО – сведение к минимуму незапланированных простоев. Решения должны приниматься в отношении того, какое технологическое оборудование требует стабильного мониторинга для поддержания его работоспособности и своевременности ТО с целью сведения к минимуму угрозы ЭБ. Перечислим основные возможные проблемы в достижении ЭБ:

А. Внешние угрозы. Имеют естественный, случайный, злонамеренный и системный характер.

Б. Многофакторность. Угрозы материализуются из-за неблагоприятных событий, возникающих из-за экономических или геополитических факторов.

В. Временные рамки. Угрозы бывают краткосрочные, среднесрочные и долгосрочные.

Г. Многодисциплинарность. Оценка ЭБ с точек зрения политической, стратегической, нормативной, научно-технической дисциплин.

Д. Ответственность выбора. Действия по предотвращению, смягчению и реагированию на угрозы ЭБ возлагается на личности, принимающие решения.

Е. Многомодельность. Возможны динамические и статические модели действий.

Ж. Многогранность. Свойства ЭБ можно разделить на эксплуатационную безопасность, гибкость, адекватность, устойчивость и надежность.

Перечень приведенных проблем ЭБ показывает сложность и актуальность их решений в глобальном и локальном масштабах. В нашем случае следует ориентироваться на комплексный подход к решению этих проблем.

III. ЭНЕРГЕТИЧЕСКАЯ БЕЗОПАСНОСТЬ Э-НАУКИ

Э-наука, являясь сложной системой, объединяющая программные и технические средства, предоставляет многочисленные возможности в решении задач хостинга, хранилища данных, облачного сервиса, электронной почты, электронной библиотеки, роуминг-сервиса академической сети и т.п. Достижение этих задач требует максимально надежного и безопасного функционирования инфраструктуры э-науки, так как ошибки в их работе или

же временный простой оборачиваются потерями различного рода (иногда и невозполнимыми).

В решении научно-технических задач э-науки основные функции принадлежат ЦОД, структурно состоящего из информационной, телекоммуникационной и инженерной инфраструктур.

А. Информационная инфраструктура. Включает серверное оборудование и обеспечивает обработку и хранение информации.

Б. Телекоммуникационная инфраструктура. Обеспечивает взаимосвязь элементов ЦОД и передачу данных.

В. Инженерная инфраструктура. Обеспечивает поддержание заданных технических параметров для нормального функционирования основных систем ЦОД.

ЭБ является необходимым условием для всех операций ИКТ оборудования, то есть процессорных и запоминающих устройств, сетевых компонентов и линий передачи данных. Одновременно с ИКТ оборудованием, актуальным является надежность и безотказность в работе инженерной инфраструктуры, которая в общих случаях включает системы охлаждения, кондиционирования воздуха, пожарного надзора и пожаротушения, безопасности и контроля доступа, освещение. Высокая степень ЭБ и готовности технических средств требует обеспечения высокого качества электроэнергии и недопущение перерывов в электроснабжении. В идеале должен быть разработан надежный комплекс, состоящий из систем бесперебойного и гарантированного питания, резервных генераторов, стабилизаторов напряжения для обеспечения чистого электропитания компьютерной техники, систем освещения и внутреннего электроснабжения. С прикладной точки зрения, степень безопасности (отказоустойчивости) сложного электронного оборудования и, следовательно, стоимость услуг, отражаются в т. н. классе безопасности Tier стандарта TIA/EIA942 [6]. Для каждого из выделенных уровней надежности в этом документе приводится описание, требования и рекомендации к таким системам и элементам, как например архитектурные решения, ЭБ, охлаждение, безопасность, противопожарные системы, структурированные кабельные системы, системы кабелепроводов и телекоммуникации.

Согласно TIA/EIA942 первый (базовый) уровень надежности ЦОД – Tier 1. Ошибки и отказы в работе систем и оборудования на этом уровне приводят к сбоям в работе всего ЦОД и, следовательно, к отказам в функционировании э-науки. На этом уровне инженерная инфраструктура предназначена только для удовлетворения текущих потребностей, то есть для работы без резервирования и избыточных ресурсов. Коэффициент отказоустойчивости равняется 99,671 %.

Второй уровень надежности ЦОД – Tier 2, который предполагает небольшой уровень резервирования

работоспособности системы и имеет небольшие избыточные ресурсы в инженерных системах. Коэффициент отказоустойчивости 99,749 %.

Третий уровень надежности ЦОД – Tier 3. Данный уровень надежности позволяет провести ремонтно-профилактические работы без остановки процессов в ЦОД. Коэффициент отказоустойчивости – 99,982 %.

Четвертый уровень надежности – Tier 4. Это отказоустойчивый ЦОД с резервированием и дублированием всех систем, позволяющий выполнять любые плановые и внеплановые работы без прерывания работы. Коэффициент отказоустойчивости 99,995 %.

Однако, это не единственный стандарт. Существует также стандарт BICSI 002 2010, который определяет пять классов готовности ЦОД на основе четырех критериев: резервирование компонентов; резервирование систем; использование продуктов с определенным уровнем качества и меры противодействия любым внешним воздействиям, включая природные явления [7].

Другой стандарт CENELEC EN 50600 определяет минимальные требования для инфраструктуры ЦОД всех форм и размеров. В этом стандарте установлены меры по защите от природных явлений, экологических событий и несанкционированного доступа.

Стандарт ISO/IEC 30134 устанавливает требования к возобновляемой энергии, коэффициенту энергоэффективности и ключевым показателям эффективности ЦОД.

Угрозы ЭБ, могущие оказать влияние на работу ЦОД, условно можно разделить на три группы. Первая группа представляет собой ординарные угрозы – вероятные отказы и аварии, которые являются предметом исследований надежности и ТО системы энергообеспечения. Для компенсации таких возмущений предусматриваются различные формы резервирования мощностей по производству и передачи энергии, структурных решений по обеспечению гарантированного энергообеспечения отдельных категорий потребителей, выбор стратегий ТО. Во вторую группу входят неординарные угрозы ЭБ из-за природных, техногенных, экономических, социально-политических и управленческих рисков. В третью группу входят угрозы, связанные с информационной безопасностью. В связи с возникновением, широким распространением и внедрением Интернета вещей и *Smart grid* данный тип угроз также может спровоцировать проблемы в ЭБ. Угрозами в данном случае могут стать кибератаки, направленные на объекты генерации, управления (SCADA), передачи и потребления энергоресурсов. Примером первой подобной кибератаки стала атака на украинские электростанции, в ходе которой злоумышленники с помощью фишинга и вредоносной программы *BlackEnergy* атаковали систему управления

телемеханикой, смогли прекратить подачу электроэнергии и препятствовали работам по восстановлению работоспособности системы [8].

Характеристиками угроз ЭБ, потенциально влияющими на безопасность работы ЦОД, могут быть следующие параметры:

- Объект воздействия.
- Продолжительность воздействия.
- Природа происхождения (естественная, случайная, злонамеренная и системная).

На основе вышеуказанных критериев надежности и свойств ЭБ была предложена модель схемы энергообеспечения ЦОД в среде AzScienceNet (рис.1).

Рис.1. Схема энергообеспечения с однократным резервированием

При инцидентах или прерываниях в центральной энергосети по сигналам от блока управления резервный дизель-генератор в течение нескольких секунд выходит на рабочий режим. Смарт-коммутатор в зависимости от входов энергоснабжения (внешняя электросеть или дизель-генератор) обеспечивает приоритетное функционирование основных систем ЦОД – серверного и телекоммуникационного оборудования. Источники бесперебойного питания обеспечивают непрерывное энергообеспечение в течение переходных процессов запуска и переключений автоматики.

Особая роль в обеспечении эффективного функционирования подобных систем возлагается на ТО. Современные ИКТ, интернет, в особенности, WEB 2.0 и Интернет вещей сделали доступной технологию электронного ТО (*e-maintenance*). С ее помощью осуществляется дистанционный мониторинг основных контрольных точек в энергообеспечении и автоматическое оповещение службы ТО [9]. Таким образом, предложенная модель обеспечивает устойчивость к угрозам ЭБ, т.е. способна реагировать на события и инциденты, вызывающие ненормальные системные условия или непредвиденные обстоятельства с

минимально
работоспособности.

допустимыми

нарушениями

IV. ЗАКЛЮЧЕНИЕ

Решение проблем ЭБ играет существенную роль в формировании надежной инфраструктуры э-науки, ее эксплуатации и развитии. Проведенный анализ в этой области показал, что ЭБ требует комплексного подхода. Надежность и ЭБ инфраструктуры э-науки является существенным фактором в обеспечении ее информационной безопасности. Предложенная модель энергообеспечения инфраструктуры э-науки с интеллектуальным ТО позволит достичь оптимальных решений в области ЭБ.

ЛИТЕРАТУРА

- [1] J. Latson, “Why the 1977 blackout was one of New York’s darkest hours,” 13 July 2017. <http://time.com/3949986/1977-blackout-new-york-history>
- [2] O.P. Veloza, and F. Santamaria, “Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes,” The Electricity Journal, 2016, Vol. 29, No. 7, pp. 42-49.
- [3] T. Fətəliyev, “Elektron elmin təhlükəsizliyinin təmin edilməsi məsələləri haqqında,” İnformasiya cəmiyyəti problemləri, 2016, №1, ss. 56-62.
- [4] A. Cherp and J. Jewell, (2014). “The concept of energy security. Beyond the four As,” Energy Policy, 2014, 75(c), pp. 415-421. DOI: 10.1016/j.enpol.2014.09.005
- [5] F. Profumo, E. Bompard, and G. Fulli, “Electricity security: models and methods for supporting the policy decision making in the European Union,” 2016, Thesis for: Doctorate in Electrical Engineering.
- [6] Data Center standards (TIERS I-IV). <https://www.colocationamerica.com/data-center/tier-standards-overview.htm>
- [7] А. Чернобровцев, “Как построить ЦОД: лучшие практики,” Computerworld Россия, 2010, № 32. <https://www.osp.ru/cw/2010/32/13004588/>
- [8] R. M. Lee, M. J. Assante, T. Conway, “Analysis of the cyber attack on the ukrainian power grid,” 2016, Electricity Information Sharing and Analysis Center (E-ISAC), 23 p.
- [9] T. Fətəliyev, Ş. Mehdiyev, “Şəbəkə mühitində elektron texniki xidmətin təşkili məsələləri,” Proqram mühəndisliyinin aktual elmi-praktiki problemləri, 2016, ss. 291-293.

ENERGY SECURITY ISSUES IN E-SCIENCE INFRASTRUCTURE

Tahmasib Fataliyev¹ and Shakir Mehdiyev²

Institute of Information Technology of ANAS, Baku, Azerbaijan

¹depart3@iit.science.az, ²depart11@iit.science.az

Abstract -- The article is devoted to the issues of ensuring the energy security of the e-science infrastructure. The necessity of the infrastructure of e-science as an integral part of modern research activities is substantiated. It is shown that the continuous and effective activity of e-science depends on solving the problems of energy security. Conceptual issues in this area are analyzed and a system is proposed that ensures the energy security of the e-science infrastructure.

Keywords -- infrastructure of e-science, energy security, reliability, threats, data center, AzScienceNet

Neft-qaz sənayesində kibertəhlükəsizlik problemləri

Yadigar İmamverdiyev¹, Günay Muradova²
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹yadigar@iit.science.az, ²gmuradova9@gmail.com

Xülasə— Neft-qaz sənayesində istehsal tsiklinin bütün proseslərində rəqəmsal və İnternet texnologiyalarının geniş tətbiqi nəticəsində kibertəhlükəsizlik artan təhlükəyə çevrilir. Buna görə kibertəhlükəsizlik hazırda neft və qaz şirkətlərinin texnoloji inkişaf prioritetlərindən birinə çevrilir. Məqalədə neft-qaz sənayesində baş verən rəqəmsal transformasiyalara qısa xarakteristika verilir, meydana çıxan əsas kibertəhlükəsizlik təhdidləri analiz edilir və kibertəhlükəsizlik insidentləri haqqında məlumat verilir.

Açar sözlər— neft-qaz sənayesi; rəqəmsal mədəniyyət; OT; IoT; kibertəhlükəsizlik;

I. GİRİŞ

Hazırda neft-qaz sənayesi bir sıra ciddi problemlərlə mübarizə olunan keçid dövrünü yaşayır, bu keçid dövrü dünya bazarlarında neftin qiymətinin kəskin ucuzlaşması və xaoslu dəyişkənliyi, yüngül neft ehtiyatlarının tükənməsi, ağır neft mərhələsinin genişlənməsi (həm sıxlığına, həm də çıxarılmasının çətinliyinə görə ağır neft), sahənin aparıcı oyunçuları (transmilli neft şirkətləri, neft istehsal edən ölkələr) arasında rəqabətin dərinləşməsi ilə xarakterizə edilir.

Bu keçid dövrünün əsas xarakterik cəhətlərindən biri də istehsalat tsiklinin bütün zəncirində intellektual informasiya texnologiyalarının geniş tətbiq edilməsidir. Qeyd edək ki, böyük transmilli neft-qaz şirkətləri hazırda intellektual neft-qaz yataqları texnologiyaları ilə məşğul olan xüsusi bölmələrə malikdirlər. Belə şirkətlər – Shell (“Smart Fields”), BP (“Field of the Future”), Chevron (“iFields”), həmçinin Saudi Aramco, Petrobras, Kuwait Oil və başqalarıdır. Neft-qaz şirkətləri Əşyaların İnterneti (Internet of Things, IoT), bulud texnologiyaları, Machine Learning (maşın təlimi, verilənləri emal etdikcə öyrənən alqoritmlər), yüksək məhsuldarlıqlı hesablamalar (böyük həcmli verilənlərin emalı) kimi texnologiyaların köməyi ilə neft-qaz hasilatının müxtəlif proseslərinin optimallaşdırılması metodlarının yaradılması üzərində işləyirlər [1,2]. Bu texnologiyaların tətbiqi neft-qaz yataqlarının işlənməsinin effektivliyinin yüksəldilməsinin yeni üsullarını tapmağa, neftin çıxarılması əmsalını artırmağa və xərcləri azaltmağa imkan verir.

Bununla yanaşı, rəqəmsal texnologiyaların geniş istifadəsi, kiber-strukturlardan artan asılılıq nəticəsində neft-qaz sənayesi yeni təhdidlərə məruz qalır. Neft-qaz sənayesi obyektlərinə kibercümlər edən bədniyyətçilərin məqsədləri müxtəlif ola bilər: kiberterrorizm, sənaye casusluğu, əməliyyatların sabotajı, verilənlərin oğurlanması və s. Neft-qaz şirkətləri kibercümlərdə

qarşılaşdıqları hüquqi, əməliyyat və texniki risklərin qarşısını almaq üçün müxtəlif tədbirlər görməyə məcburdurlar.

II. NEFT-QAZ SƏNAYESİ SEKTORLARININ TƏSNİFATI

Neft-qaz sənayesində xam neftin çıxarılması, emalı və məhsulların pərakəndə satışı zəncirini əhatə edən müxtəlif sektorlar vardır. Bu sektorlar ingilis dilli ədəbiyyatda uyğun olaraq, Upstream, Midstream və Downstream adlanır.

Upstream - Ümumiyyətlə, upstream təşkilatlara neft və qazın kəşfiyyatı və hasilatı daxildir. Neft və qazın kəşfiyyatı neft və qaz mədənlərinin işlənməsinə qədər axtarış, seysmik kəşfiyyat və qazma işləri daxildir. “Upsream” termini çox zaman quyu, quyuağzı, tamamlama və rezervuarı, downstream isə hasilat və emalı əhatə edir.

Midstream - neftin nəqli, emalı və saxlanması daxildir. Ona ümumi olaraq, neft qaz boru kəmərləri ilə yanaşı, qazın emalı, LNG istehsalı zavodları daxildir.

Downstream - bura neftin emalı, neft kimyası və pərakəndə satış daxildir.

III. NEFT-QAZ SƏNAYESİNDƏ ƏMƏLİYYAT TEXNOLOGİYALARI

Neft-qaz sənayesində IT texnologiyalar ilə yanaşı, sənaye avtomatlaşdırma texnologiyaları geniş istifadə edilir. Ənənəvi IT sistemlər ilə sənaye idarəetmə sistemləri arasındakı texnoloji və funksional fərqləri nümayiş etdirmək üçün “əməliyyat texnologiyaları” (ing. OT – operational technology) termini istifadə edilir. Əməliyyat texnologiyaları sistemin fiziki vəziyyətini monitorinq etmək və dəyişmək üçün istifadə edilən aparat və proqram təminatıdır.

Əməliyyat texnologiyalarına sənaye avtomatlaşdırma və nəzarət sistemlərindən SCADA (Supervisory Control And Data Acquisition), DCS (Distributed Control Systems – paylanmış idarəetmə sistemləri), PLC (Programmable Logic Controller – proqramlaşdırılacaq bilən məntiqi sxemlər), açıq platforma kommunikasiyası serverləri, cihazlar və analizatorlar kimi mədəni avadanlıqları daxildir. Əməliyyat texnologiyaları neft-qaz sektorlarında fiziki prosesləri izləmək (monitorinq) və idarə etmək üçün istifadə olunur; proseslərin parametrləri haqqında verilənlər əldə olunur və prosesləri avtomatlaşdırmaq üçün bu verilənlər istifadə edilir. Avtomatlaşdırma elektrik,

mexaniki, hidravlik, pnevmatik aktuatorlar və nəzarət klapanları vasitəsilə mümkündür.

Neft-qaz dəyər zəncirində şirkətlərin tətbiq etdiyi texniki həllər Əşyaların İnterneti (Internet of Things, IoT) kimi tanınır. IoT obyektlər və maşınlar şəbəkəsi tərəfindən generasiya edilən verilənlərin toplanması, analizi və fəaliyyət göstərməyi nəzərdə tutur. Məlum olduğu kimi, IoT verilənlərə əsaslanan qərar qəbul etmək üçün lazım olan mütəmadi dəyişən verilənləri birləşdirə və analiz edə bilər. Mövcud sənaye mühitində neft-qaz şirkətləri verilənləri də karbohidrogenləri emal etdikləri kimi emal edirlər; verilənlərin generasiya edilməsi, ötürülməsi, saxlanması və emal edilməsi lazımdır. IoT strategiyalarının inkişafı ilə neft-qaz sənayesi müəssisələri “Rəqəmsal Transformasiya” əsrindən faydalanmağa çalışırlar [3].

Müasir rəqəmsal texnologiyalar dövründə informasiya tez-tez mədəndən əməliyyat texnologiyaları şəbəkəsinə, daha sonra korporativ şəbəkəyə və axırda son istifadəçiyə və əksinə, axın edə bilər. Bu eyni zamanda, troyanlar, zərərli proqramlar, girov proqramları, viruslar və s. kimi kibertəhlükələrin də varlığı deməkdir. Bədənliyyatlılar İnternetdən korporativ şəbəkəyə, korporativ şəbəkədən ERP-şəbəkəyə, buradan da sənaye şəbəkəsinə keçirlər. Bu fikrin sonluğu çox kritikdir – əgər neft-qaz təşkilatlarına kiberhücumlar olsa, nəticələri çox ciddi olacaq.

Hazırda IT və OT texnologiyalarının integrasiyası sıxlaşır, qurğular korporativ şəbəkəyə və xarici şəbəkəyə qoşulur. İdarəetmə qurğularına asanlıqla qoşulan bədənliyyatlılar daha böyük ziyan vura bilərlər. Söhbət təkə texnoloji prosesin dayanması nəticəsində vurulan ziyandan getmir, həm də fiziki ziyan vurmaq imkanından gedir – məsələn, neft emalı və neft-kimya zavodlarında yanğın və ya partlayış törədilə bilər. Kibertəhlükəsizlik risklərinin belə miqyası onları milli səviyyəyə çıxarır [4].

IV. NEFT-QAZ SƏNAYESİNDƏ ƏSAS KİBERTƏHLÜKƏSİZLİK TƏHDİDLƏRİ

DNV GL analitika şirkəti Norveç kontinental şelfində işləyən şirkətlər üçün on ən təxirəsalınmaz kibertəhlükəsizlik təhdidlərinin siyahısını tərtib etmişdir [5]. Aydın ki, bu təhdidləri dünyanın digər neft-qaz şirkətləri üçün də tətbiq etmək olar:

1. Kibertəhlükəsizlik sahəsində əməkdaşlar arasında məlumatlılıq və təliminin olmaması
2. Əməliyyat və təmir zamanı uzaqdan iş
3. Məlum boşluqları olan standart IT məhsulların istehsal mühitində istifadə edilməsi
4. Vendorlar, təchizatçılar və podratçılar arasında məhdud kibertəhlükəsizlik mədəniyyəti
5. Verilənlər şəbəkələrinin kifayət qədər ayrılması
6. Smartfonlar da daxil olmaqla, mobil cihazların və yaddaş qurğularının istifadəsi
7. Quru və dəniz qurğuları arasında verilənlər şəbəkələri

8. Verilənlər mərkəzi olan otaqların, kabinetlərin və s. yetərsiz fiziki təhlükəsizliyi olmaması
9. Həssas proqram təminatı
10. Müəssisələrdə köhnəlmiş və istifadəyə yararsız idarəetmə sistemləri

Kibertəhlükəsizlik sahəsindəki bu boşluqları risklərin qiymətləndirilməsinə əsaslanan yanaşma ilə aradan qaldırmaq olar [6]. DNV GL tərəfindən 1100 peşəkar arasında aparılmış beynəlxalq rəy sorğusu göstərmişdir ki, şirkətlər özlərinin informasiya təhlükəsizliyini fəal şəkildə idarə etsələr də, onların yalnız yarımından bir qədər çoxu (58%) xüsusi idarəetmə strategiyası qəbul edib və yalnız 27 %-i konkret məqsədlər qoyur.

Qeyd edək ki, IT və OT fərqli missiyalar üçün yaradılıb, buna görə onların mülkiyyət sahibi və məsuliyyət də təşkilat üzrə framentləşdirilib. Yeni təhdidlərin xarakteri IoT qurğular vasitəsilə hücumlar ilə əlaqədardır. Şəbəkəyə qoşulan sensorların, ötürücülərin, smart sənaye sistemlərinin sayı sürətlə artır və hakerlər şəbəkəyə qoşulmaq üçün yeni yollar tapırlar. IoT qurğuların xüsusiyyəti ondan ibarətdir ki, onların hesablama gücü kiçikdir və onlarda müdafiə sistemləri, o cümlədən qarşılıqlı autentifikasiya və trafikinin şifrənməsi vasitələri qurmaq çətinidir.

Daha bir təhdid sistemlərin qarşılıqlı asılılığının güclənməsindən, onların vahid istehsal zəncirinin həlqələrini təşkil etmələrindən qaynaqlanır. [7]-də təchizat zəncirinin hər hansı bir elementinə edilmiş kiberhücumun digər bütün qovşaqlarda öz təsirini göstərdiyi vurğulanır.

V. NEFT-QAZ SƏNAYESİNDƏ KİBERTƏHLÜKƏSİZLİK İNSİDENTLƏRİ

Neft-qaz sənayesində proqram təminatı vasitəsilə həyata keçirilən insidentlərin tarixi 1980-ci illərə gedib çıxır. ABŞ-ın yüksək rütbəli milli təhlükəsizlik rəsmisi Tomas Reed özünün “At the abyss” kitabında ABŞ-ın SSRI-yə boru kəmərinə nəzarət proqramının kodlarını Kanada şirkətindən oğurlamasına necə şərait yaratdığını qeyd etmişdir. Bu proqrama daxil edilmiş zərərli kod 1982-ci ilin iyun ayında Trans-Sibir boru kəmərinə böyük bir partlayış yaratmışdı. Troyan boru kəmərinə təzyiq testi keçirilən zaman işə düşmüşdü, normal təzyiqi kəskin artırmışdı və partlayışa səbəb olmuşdu [8].

2002-2003-cü ilin qışında PDVSA (Petróleos de Venezuela, S.A.) sistemlərinə kiberhücumlarda hakerlər Venesuelanın şərqindəki bir dəniz terminalında tanker yüklənməsinə məsul SCADA sisteminə nüfuz edə bilmişdilər. Hakerlər PLC-də proqramı silərək tanker yüklənməsinin qarşısını səkkiz saata almışdılar. Təcavüzkarların taktikası mükəmməl deyildi və problem nisbətən asan aşkarlanmışdı və PLC proqramları ehtiyat surətlərdən bərpa olunmuşdu.

Son 10 ildə neft-qaz sənayesində baş vermiş kibertəhlükəsizlik insidentləri haqqında aşağıda qısa xronika verilir.

2009 – Portuqaliyanın Bayamon şəhərindəki kompüterləşdirilmiş monitoring sistemində qəfil imtina (“glitch”) baş vermişdi, bunun nəticəsində benzinlə dolu bir saxlama tankerində partlayış baş vermiş və üç gün davam edən yanğına səbəb olmuşdu.

2010 – Stuxnet virusu bütün dünyada sənaye idarəetmə sistemlərinin, o cümlədən, neftayırma zavodlarının, boru kəmərlərinin və elektrik stansiyalarının idarə edilməsi üçün istifadə edilən kompüterlərin ələ keçirilməsi istifadə edilmişdi.

2012 – dünyanın ən böyük neft istehsalçısı olan Saudi Aramco böyük bir kiberhücumun qurbanı olmuşdu. Neft nəhəngi 30 min kompüterinin virusa yoluxduğunu açıqlamışdı. Özlərini Cutting Sword adlandıran bir qrup haker Saudi Aramco hücumuna görə məsuliyyətini öz üzərinə götürdü. Onlar şirkətin sistemlərinə zərərli proqramları siyasi səbəblərə görə yoluxdurmuşdular [9].

2012 – Enerji sektorunda uzaqdan idarəetmə və monitoring alətlərinin təchizatçısı olan Telvent şirkəti daxili şəbəkələrarası ekranın və təhlükəsizlik sistemlərinin sındırılması nəticəsində ziyan çəkmişdi. Telvent-in məlumatına görə, hər bir Fortune 100 Energy şirkəti onun sistemlərindən istifadə edir. Təcavüzkarlar köhnə IT avadanlıqlarını Smart Grid texnologiyaları ilə birləşdirməyə imkan verən məsafədən idarəetmə vasitəsi olan SCADA layihəsi ilə əlaqəli faylları oğurlamışdılar. Çox güman ki, hakerlər, enerji şirkətlərinə birbaşa hücum etmək üçün proqram təminatındakı boşluqları tapmağa çalışırdılar, buna görə mənbə kodlarını axtarırdılar.

2012 – Ugly Gorilla təxminən iyirmidən artıq ABŞ təbii qaz xidmətinə hücum edərək, qaz boru kəmərləri şirkətlərindən həssas məlumatları oğurlamışdı.

2012 – Qətərdə LNG ixrac edən aparıcı RasGas şirkətində kompüter sistemi bilinməyən virusla yoluxmuşdu, nəticədə şirkət işini bir neçə gün dayandırmışdı.

2012 – məşhur Flame zərərli proqramı Yaxın Şərqdəki şirkətdə casusluq üçün istifadə edilmişdi. Zərərli proqram səsi, ekran görüntülərini və istifadəçinin hərəkətlərini yazmaq imkanına malikdir.

2014 – Hakerlər Statoil daxil olmaqla, Norveç neft-qaz sənayesində təxminən 300 müxtəlif firmanı hədəf almışdılar. Hücum e-poçt vasitəsilə həyata keçirilmişdi. E-poçtla göndərilən məktub açıldığı zaman zərərli proqram yüklənir və təhlükəsizlikdə boşluqlar axtarıldı.

2015 – ABŞ-da pərakəndə satış stansiyalarında benzin səviyyələrini ölçmək üçün istifadə edilən ATG (Automated Tank Gauges) cihazlarının onlayn hücum edənlər tərəfindən uzaqdan idarə edilə bilməsi aşkarlanmışdı. Təcavüzkarlar ATG-lərdə yanacaq axınına dayandıra bilirdilər.

2017 – neft-qaz şirkətləri qlobal Petya girov proqramının hücumuna məruz qalmışdı.

VI. SCADA SİSTEMLƏRİN TƏHLÜKƏSİZLİYİ ÜÇÜN STANDARTLAR

Şirkətlər SCADA sistemlərinin təhlükəsizliyini təmin etmək üçün standartlara müraciət edirlər [6]. Amerika Milli Standartlar İnstitutu (ANSI) tərəfindən təsdiqlənmiş ISA-99.02.01 standartı belə standartlardandır (Security for Industrial Automation and Control Systems). Standart SCADA və idarəetmə sistemləri üçün kibertəhlükəsizliyin menecmenti sistemi (KMS) yaratmaq üçün yeddi əsas addım müəyyən edir.

ISA-99.02.01 addımları üç fundamental kateqoriyaya bölünüb: risk analizi, riskin KMS ilə idarə edilməsi, KMS-in monitoringi və təkmilləşdirilməsi. Birinci kateqoriya həm cari təhlükəsizlik vəziyyətini qiymətləndirmək, həm də hansı təhlükəsizlik hədəflərinə nail olmaq istədiyini müəyyən etmək üçün mərhələlər təyin edir.

İkinci kateqoriya şirkətdə təhlükəsizlik siyasətini, təhlükəsizliyin təşkilini və təhlükəsizlik üzrə məlumatlılığı müəyyənəlmək üçün prosesləri əks etdirir və SCADA təhlükəsizliyinin yaxşılaşdırılması üçün təhlükəsizlik tədbirləri üzrə tövsiyələr verir. Bu kateqoriyada əsas fikir dərininə müdafiə (ing. defense-in-depth) kimi tanınan konsepsiyadır, burada təhlükəsizlik həlləri kiberhücumların qarşısını almaq üçün diqqətlə bir neçə səviyyədə yerləşdirilir.

Son kateqoriya SCADA sisteminin yalnız KMS-ə uyğunluğunu deyil, həm də davamlı inkişaf proqramı ilə hərəkət etməsini təmin edən metodları təsvir edir.

IEC 62443 standartı sənaye avtomatlaşdırma və idarəetmə sistemləri üçün ümumi standartdır və hələ tam başa çatdırılmayıb. IEC 62443 standartlar seriyasına bütün çoxluğuna uyğunluğu təsdiqləmək çox bahalıdır və bəzi hissələr müəyyən sənaye sahələrinə aid edilməyə bilər.

Standart həmçinin təhlükəsizlik səviyyələrinə müraciət edir ki, lakin müxtəlif sistemlər üçün düzgün hədəfi müəyyən etmək çətin ola bilər. Hazırda standart nə etmək lazım olduğunu müəyyənəlməkdir, lakin bunun necə ediləcəyini tam şəkildə izah etmir. Bu çətinlikləri aradan qaldırmaq üçün neft və qaz sektorunda IEC 62443 (3-2, 3-3 və 2-4) tətbiq edilməsi üçün DNV GL, Emerson, Honeywell, Shell Norveç, Siemens, Statoil və s. iştirakı ilə birgə sənaye layihəsi çərçivəsində tövsiyələr işlənmişdir. Bu layihənin məqsədi neft və qaz sektorunda sənaye avtomatlaşdırma və idarəetmə sistemlərinin təhlükəsizliyini təmin etmək üçün ümumi və praktiki yanaşma müəyyən etmək idi.

Avropa İttifaqında 2018-ci ilin may ayında qüvvəyə minən NISD (Network and Information Security Directive – Şəbəkə və İnformasiya Təhlükəsizliyi üzrə Direktiv) enerji şirkətlərinin şəbəkə və informasiya sistemlərinin minimal kibertəhlükəsizlik standartlarına cavab verməsini təmin edir. Böyük Britaniya Milli Kibertəhlükəsizlik Mərkəzi bu Direktivə uyğunluq tələbləri üzrə ətraflı təlimat hazırlamışdır.

Direktiv “əsas xidmətlər” operatorlarını nəzərdə tutur, bu bir çox enerji şirkətini əhatə edəcək. Elektrik istehsalçıları və ötürücüləri ilə yanaşı, neft və qaz hasilatı və paylanması ilə

məşğul olan şirkətlər də bu Direktivin əhatə dairəsindədirlər. Direktiv üzv dövlətlərə "şəbəkə və informasiya sistemlərinin yüksək səviyyədə təhlükəsizliyinə nail olmaq və təmin etmək üçün müvafiq siyasət və tənzimləyici tədbirlərin" tətbiq edilməsini, habelə hadisə baş verdikdə məlumatlandırma öhdəliklərini tələb edir. Direktiv müvafiq standartların yerinə yetirilməməsinə və hadisə barədə məlumat verilməməsinə görə "effektiv, mütənəssib və qərəzsiz" sanksiyalar tətbiq edilməsini tələb edir.

NƏTİCƏ

Neft-qaz sənayesi ən çox kiberhücüm edilən sənaye sahələrindən biridir, bu kiberhücumların iqtisadiyyat və milli təhlükəsizlik üçün ağır potensial nəticələri ola bilər. Buna görə kibertəhlükəsizliyin təmin edilməsi neft-qaz sənayesi üçün olduqca mühüm məsələdir və kibertəhlükəsizlik tədbirləri neft-qaz əməliyyatlarının rəqəmsallaşdırılması sürəti ilə ayaqlaşmalıdır. Neft-qaz sənayesinin müxtəlif sektorları, təbii olaraq, müxtəlif risk səviyyələrinə malikdir və müxtəlif kibertəhlükəsizlik strategiyaları tələb edirlər. Mədənlərin, neft-qaz nəqlinin və emalının, ekoloji proseslərin, ümumiyyətlə, baxılan sənayedəki bütün tədbirlər kompleksinin kibertəhlükəsizlik məsələlərini həll etmək lazımdır.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikasının Dövlət Neft Şirkətinin Elm Fondunun maliyyə yardımı ilə yerinə yetirilmişdir (Layihənin adı: **“DeepOil-ML: İntellektual neft mədənləri üçün Deep Learning əsasında yeni texnologiyaların işlənməsi”**).

ƏDƏBİYYAT

- [1] R.M. Alıquliyev, Y.N. İmamverdiyev, “Neft-qaz sənayesi üçün konseptual Big Data arxitekturası,” İnformasiya texnologiyaları problemləri, №1, s.3–14, 2017.

- [2] R.M. Alıquliyev, Y.N. İmamverdiyev, “Neft-qaz sənayesi üçün Big Data strategiyası: Ümumi istiqamətlər,” İnformasiya texnologiyaları problemləri, №2, s. 34–47, 2017.
- [3] F. Shaik, A. Abdullah, & S. Klein, Digital transformation in oil & gas - Cyber security and approach to safeguard your business. World Petroleum Congress. 2017.
- [4] B. Clayton, & A. Segal, Addressing cyber threats to oil and gas suppliers. Council on Foreign Relations, 2013.
- [5] Top 10 cybersecurity vulnerabilities for oil and gas // Pipeline & Gas Journal, vol. 243(2), February 2016.
- [6] P. A. Ralston, J. H. Graham, & J. L. Hieb, “Cyber security risk assessment for SCADA and DCS networks,” ISA transactions, vol. 46(4), pp. 583-594, 2007
- [7] M.A. Nasir, S. Sultan, S.Nefti-Meziani, & U. Manzoor, “Potential cyber-attacks against global oil supply chain,” IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1-7, 2015.
- [8] E.J.Byres, “Cyber security and the pipeline control system,” Pipeline & Gas Journal, pp.58-59, 2009.
- [9] C. Bronk, & E. Tikk-Ringas, “The cyber attack on Saudi Aramco,” Survival, vol. 55(2), pp. 81-96, 2013.

CYBER SECURITY ISSUES IN THE OIL AND GAS INDUSTRY

Yadigar İmamverdiyev¹, Gunay Muradova²

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

Baku, Azerbaijan

¹yadigar@iit.science.az, ²gmuradova9@gmail.com

Abstract – As a result of the widespread use of digital and Internet technologies in all the processes of the production cycle in the oil and gas industry, cyber security becomes increasing threat. Therefore, cyber security has become one of the priorities of technological development in the oil and gas companies. The article gives a brief description of the digital transformations in the oil and gas industry, analyzing the major cyber security threats and reporting on cyber security incidents.

Keywords – oil and gas industry; digital mining; OT; IoT; cyber security.

Kompüter şəbəkələrində zərərli proqramların analizi üsulları

Tural Yunusov

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

turaly@mail.ru

Xülasə — Məqalədə kompüter şəbəkələrinin təhlükəsizliyi, zərərli proqramlar haqqında informasiya verilmişdir, zərərli proqramların analizi üsulları, statik analiz üsulu, dinamik analiz üsulu, zərərli proqramların virtual mühitdə analizi, zərərli proqramların yoluxma üsulları tədqiq olunmuşdur.

Açar sözlər – kompüter şəbəkələri, zərərli proqramlar, rootkit, zərərli mobil kod, kuki faylları, hooking, sandbox.

I. GİRİŞ

Zərərli proqram dedikdə, məlumatın məhv edilməsi, oğurlanması, proqram və ya əməliyyat sisteminin konfidensiallığına, tamlığına və əlçatanlığına ziyan vurmaq (viruslar, Troya atları, Zərərli mobil kodlardan istifadə) məqsədi ilə hazırlanmış zərərli kodlar nəzərdə tutulur. Xoşagəlməz proqram çərçivəsində nəzər yetirilən virus, soxulcan, troya atları, casus və reklam tərkibli proqramlar illərdir fərdi və korporativ kompüter şəbəkələrinə təhdit olmuşlardır. Kompüter istifadəçilərinin sayı artdıqca, kompüter şəbəkələrinin müxtəlif təhdidlərə qarşı həssas vəziyyətə gəlməsi də bir reallıqdır [1].

Şəkil 1. Zərərli proqramların illər üzrə yayılma statistikasi

AV-TEST İT təhlükəsizliyi institunun verdiyi statistikaya əsasən 2018-ci ildə zərərli proqramların yayılması digər illərə görə daha çoxdur (Şəkil 1).

II. ZƏRƏRLİ PROQRAMLAR

Zərərli proqramları aşağıdakı kimi klassifikasiya etmək olar.

Soxulcan – müstəqil işləyə biləcək və digər kompüter şəbəkələrində olan sistemlərə kopyalana bilən kiçik proqramlara verilən ad. Əlavə olaraq botnet qurmaq üçün də istifadə olunur.

Virus – müstəqil formada işləyə bilmir, aktivləşdirilməli və əməliyyat sistemi fayllarına əlavə edilməli bir kod hissəsi kimi müəyyən edilir.

Trojan – və ya troya atları, əsasən faydalı proqramlara əlavə edilən zərərli kodun gizli hissəsidir. Arxa tərəfdə port açma və məsafədən idarəetmə kimi funksiyaları istifadəçidən xəbərsiz yerinə yetirir.

Spyware – casus proqramlar olaraq adlandırılan bu proqramlar istifadəçi kompüterindəki həssas informasiyaları (istifadəçi informasiyalarını, şifrələri, şəxsi məlumatları) yığan və hücumçunun kompüterinə göndərən proqramlardır.

Bot – istifadəçi kompüterində gizli quraşdırılan və yoluxmuş kompüterin resurslarından istifadəçinin xəbəri olmadan istifadə etməklə, müəyyən əməlləri yerinə yetirməyə imkan verən uzaqdan idarə oluna bilən zərərli proqramdır. Bu sistemlər əsasən spam göndərmə, DDOS hücum etmə kimi işlərdə istifadə edilir.

Rootkit – hücumə məruz qalan sistem üzərində edilən bütün əməliyyatları gizləyən (aktiv əməliyyatlar, fayllar, qeydlər və.s.) proqramlardır. Kompüter yüklənməsi zamanı yoluxan və öz fayl sistemi olan yeni nəsil zərərli proqramlara bootkit adı verilmişdir.

Zərərli mobil kod – mobil kod çox vaxt istifadəçinin təlimatı olmadan yerli sistemdə icra edilmək üçün uzaq sistemdən ötürülən proqram təminatıdır. Zərərli mobil kod faylları yoluxdurumaması və ya özünü təkrarlamaması ilə virus və soxulcanlardan fərqlənir. Mobil kod üçün populyar anlayışlara Java, ActiveX, JavaScript və VBScript daxildir.

İzləyici Kuki faylları – Kuki xüsusi veb saytdan istifadə barədə məlumatı saxlayan kiçik “data” faylıdır. Sessiya kukiləri yalnız bir veb saytı sessiyasında etibarlı olan müvəqqəti kukilərdir. Daimi kukilər kompüterdə həmişəlik saxlanılır ki, sayta tez-tez daxil olan istifadəçiləri müəyyən edə bilsin. Daimi kukilər saytın istifadəçinin daxil olmasını və ya gələcək daxilolmaları zamanı davranışı avtomatik fərdiləşdirməsi üçün bir veb saytda istifadəçi göstəricisini qeydə almaq üçün nəzərdə tutulmuşdur. Bu yolla daimi kukilər veb saytlara istifadəçilərinə daha səmərəli xidmət göstərməyə kömək edir. Daimi kukilər istifadəçinin xəbəri və ya razılığı olmadan şübhəli məqsədlərlə istifadəçinin veb axtarışlarını izləmək üçün cəsus proqram kimi

də istifadə edilə bilər. Məsələn, marketing firması bir çox veb saytlarda reklam yerləşdirir və istifadəçinin cihazında olan bir kukidən istifadə edərkən onun bütün veb saytlardakı fəaliyyətini izləyə və istifadəçinin davranışından ətraflı məlumat toplaya bilər. Bu cür istifadə edilən kukilər izləyici kukilər kimi tanınır. İzləyici kukilər tərəfindən toplanan məlumat çox vaxt digər tərəflərə satılır və istifadəçilərə reklam və başqa məzmun göndərmək üçün istifadə edilir.

III. ZİYANKAR PROQRAMLARIN ANALİZ ÜSULLARI

Antivirus proqramları əsasən zərərli proqramların müəyyən bir hissəsindən yaradılan imzaları (signature) verilənlər bazasında saxlayıb, buradan müqayisə edərək zərərli proqramı aşkarlaya bilirlər [2]. Günümüzdə bu iş üçün istifadə edilən ən yaxşı alət VirusTotal–dır.

VirusTotal fayl analizinə pulsuz icazə verən veb saytdır. Təqribən 56 antivirus sistemini özündə birləşdirir. Faylları həm veb üzərindən, həm də e-poçt vasitəsilə göndərmək olur. Sistem yalnız ona göndərilən kiçik ölçüdəki faylları analiz edir, kompüterini analiz etmir (Şək.2).

Detection	Details	Behavior	Community
Engine	Detection		
Ad-Aware	Generic.Startor.3.9954A463		
AegisLab	Troj.Script.Generic.c		
ALYac	Generic.Startor.3.9954A463		
Arcabit	Generic.Startor.3.9954A463		

Şəkil 2. VirusTotal vasitəsilə zərərli proqramın aşkarlanması

Bu üsul çox vaxt müvəffəqiyyətlidir, lakin günümüzdə inkişaf etmiş zərərli proqramları bu üsulla aşkarlamaq mümkün olmur. Çünki zərərli proqram tez-tez təkmilləşdirilir və bu vəziyyət imzanın dəyişməsinə səbəb olur. Fərqli üsullarla (şifrləmə, başqa dildə kodlaşdırmaq, kodları başa düşülməyən formaya gətirmək) imza dəyişikliyinə səbəb olurlar [3].

Bu səbəblə zərərli proqramları aşkarlamaq və analiz etmək üçün aşağıdakı üsullardan istifadə edilir.

Statik analiz üsulu zərərli proqramı aktivləşdirmədən bir başa, kod səviyyəsində hansı xidmətlərə giriş təmin etdiyinin və ya hansı dəyişikliklərin apardığının analiz edilməsidir.

Dinamik analiz isə təcrid edilmiş virtual mühitdə zərərli proqramı aktivləşdirmək və etdiyi dəyişiklikləri (daimi sistem qeydləri, fayl sistemi, prosesor əməlləri) izləyərək analiz etmə üsuludur.

A) Statik analiz üsulu

Əgər mənbə kod (source code) əlimizdədirsə statik analiz üsulu ilə bütün funksiyaları test edə bilərik. Əlimizdə sadəcə binar kod (bir və sıfırdan ibarət olan maşın kodu) mövcuddursa

verilənlərin tipi kimi informasiyalar itəcəyindən analiz çətinləşəcəkdir. Hex (onaltılıq say sistemi) dəyişdirmə proqramları vasitəsi ilə xəta izləmə xüsusiyyətlərini də istifadə edərək və müəyyən əməllər sətri axtarılaraq zərərli proqramın işləmə prinsipləri haqqında məlumat almaq mümkündür. Tərs mühəndislik (Reverse Engineering) metodları ilə əlimizdə olan binar kod (binary code) zərərli proqram nümunəsindən üst səviyyə kodlaşdırılmış mənbə kod (source code) əldə etmək mümkündür. Bu kodu nə qədər müvəffəqiyyətli geri kodlaşdırma bilsək, alınan kodun işləməsi də insan gözüylə aydınlaşdırılması o qədər asanlaşacaqdır [4].

B) Dinamik analiz üsulu

Dinamik analiz üsulunda zərərli proqramların analizi aşağıdakı formada yerinə yetirilir.

Funksiya çağırışlarının monitorinqi (Function Call Monitoring) – zərərli proqram aktivləşdirildiyi vaxt, əgər funksiya çağırma (bu əməliyyat sisteminə aid istifadəçi funksiyası ola bilər) prosesi yerinə yetirirsə bu mərhələdə ortaya girərək bəzi məlumatlar əldə edə bilərik. Bu proses “hooking” adlanır. Hooking funksiyası, bir qeydiyyat faylına, bu prosesin adını, giriş parametrləri kimi məlumatları əlavə edir [5].

Əməliyyat sistemləri fundamental funksiyaları olan fayl yaratma, şəbəkəyə sorğu göndərmə, avadanlıq üzərində kod aktivləşdirmə kimi proseslərə əməliyyat sistemləri üzərində işləyən proqramlara birbaşa giriş icazəsi verə bilmir bunu etmək üçün bir interfeys (API) üzərində bu prosesi nəzarətlə verir. Windows API – ləri şəbəkə, təhlükəsizlik, sistem xidmətləri və idarəçiliyi kateqoriyaları altında toplanır.

Şəkil 3. Hooking prosesi

Zərərli proqramların mənbə kodu məlumdursa bu koda hooking funksiyaları əlavə edilə bilər (Şək.3). Əlimizdə ancaq binar kod varsa binar kodunu təkrar yazma (binary rewriting) üsulu ilə maşın kodu üzərində dəyişiklik aparılaraq Hex dəyişdirici proqramlarında prosesin olduğu yaddaş ünvanını göstərən rəqəmi hook funksiya ünvanı ilə dəyişdirib hooking prosesi başa çatdıqdan sonra real proses ünvanına yönləndirilə bilər.

Yaddaş üzərində dəyişdirmə prosesinə inyeksiya deyilir. Kodun istifadə etdiyi kitabxanalar “stub” adı verilən, daha sonra əsliylə dəyişdiriləcək müvəqqəti kod hissələri ilə dəyişdirilir. Aşağıdakı inyeksiya növlərini kimi göstərmək olar: – proseslərin inyeksiyası, kitabxanaların inyeksiyası, yüklənmədən qabaq mühitin inyeksiyası [6].

Funksiya çağırışlarının izlənməsi (Function Call Traces) – çağırılan funksiyaların nəticələrinin izlənilməsi function call trace adlanır. Bu izləmə mərhələsində çağırılan funksiyaların sırası məlumdur. Bu informasiya bizə zərərli proqramın necə işlədiyini haqqında məlumat verir.

Funksiya parametr analizi – statik analizdə funksiya parametrlərinə baxılaraq (tiplərinə və qiymətlərinə) mümkün olan parametr qiymətləri arasında hansının olma ehtimalı hesablanır. Dinamik analizdə isə funksiya çağırışı edilən giriş qiyməti əldə edilir [7].

İnformasiya axınının izlənilməsi (Information Flow Tracking) - proqram tərəfindən məlumatın necə emal

edildiyinə baxılır. Sətir-sətir kod aktivləşdirmə prosesi (debug) zamanı verilənlər və ya “register” verilənləri nişanlanaraq informasiyanın hərəkəti izlənilir. Bu izləmənin məqsədi vacib verilənləri tapmaq və ya qarışıq kodun sadələşdirilməsini təmin etməkdir.

Təlimat izləmə (Instruction Trace) - Bu üsulla analiz edən şəxs sətir-sətir kod aktivləşdirmə (debug) ilə kod da olan ən alt səviyyə maşının başa düşəcəyi əmrləri analiz etməyə çalışır. Analiz vaxtı müəyyən bir iş görən maşın koduna rast gəldikdə daha yüksək səviyyədə görmədiyi vacib məlumat bu səviyyədə əlçatan olur [8].

IV. ZİYANKAR PROQRAMLARIN VİRTUAL MÜHİTDƏ ANALİZİ

Zərərli proqramların virtual mühitdə analizi əsasən “sandbox”-larla aparılır.

SandBox – Zərərli proqramların aktivləşdirilərək, fəaliyyətlərinin avtomatik olaraq analiz edən virtual mühitdir. Sandbox mühitini qapalı bir qutu kimi təsəvvür etmək olar, bu qutunun içərisində zərərli proqramın yoluxa biləcəyi bütün şərait mövcuddur. Bu qutunun içərisindəki quruluşa baxdıqda, sandbox mühiti əsasən iki hissədən ibarət olur: analiz edilən və hesabatın hazırlandığı mühit. Əsasən ubuntu kimi linux əməliyyat sistemlərindən istifadə edilir. Analiz edilən bölmədə isə virtual mühit ilə əlaqəni təmin edən proqramlar, skriptlər və hesabatı təmin edən alətlərdən başqa əlavə əməliyyatlar aparılır [9].

Virtual laboratoriya mühitində zərərli proqramların hərəkətlərini analiz etmək üçün lazım olan proqramlar: şəbəkə avadanlıqlarının analizi üçün – wireshark, windump, tcpdump, etheral, fayl sistemini izləmək üçün proqramlar – The Sleuth Kit, Registry (qeyd dəftəri) qeydlərini izləmək üçün proqramlar – process bat, captureBAT, regshot, xidmətləri və yaddaşın izlənilməsi üçün proqramlar – Volatility Framework-dan istifadə olunur [10].

Bundan başqa veb üzərində analiz edən Anubis, Norman, Comodo və.s kimi sandbox sistemləri verilmiş zərərli proqram nümunəsini öz verilənlər bazalarındakı imza nümunələri ilə müqayisə edib daha əvvəldən aşkar edilmiş bir zərərli proqram olub-olmadığını müəyyən edə bilirlər. Bu alətlərin yaratdığı çıxış informasiyaları sandbox kodu tərəfindən yığılaraq hesabat vəziyyətinə gətirilir.

NƏTİCƏ

Ümumiyyətlə zərərli kod sistem istifadəçisinin xəbəri olmadan zərərli funksiyaları həyata keçirmək üçün hazırlanmışdır. Viruslar, soxulcanlar, troya atları, zərərli mobil kod və hücumlar daxil olmaqla bir sıra zərərli kod kateqoriyaları vardır. Zərərli proqramlar eyni zamanda tələ-funksiyalar, rutkit, klaviatura reyestrləri və cəsus kimi istifadə edilən izləmə kuki faylları kimi hücumları ehtiva edir.

Zərərli proqramların yoluxma üsulları əsasən aşağıdakı kimi olur:

–Şəbəkə üzərində olan kompüterlər axtarılır və bu kompüter üzərində olan xidmətlərin boşluqlarından istifadə edərək sistemə giriş əldə edilir.

–İnternet brauzerinin boşluğundan istifadə edərək zərərli kodun internetdən yüklənməsini təmin edir və kompüterini yoluxdurur. Hücumçuların istifadə etdiyi alətlər əsasən brauzer

əlavələrində istifadə olunan javascript, vbscript kimi sistem tərəfindən aktivləşdirilə bilən skriptlərdir.

– Sosial mühəndislik, mailə də aldadılaraq istifadəçiyə fayl açmağı məcbur etmə, pulsuz proqram adı altında fayl yüklənməsi ən çox yayılan üsullardan biridir.

Kompüter sistemlərinin tətbiqi və istifadə sahələri artdıqca onlara olan təhlükələrin və zərərli proqramlarla hücumların sayı artır. Belə məsələlərə hazırlıqlı olmaq üçün kompüter şəbəkələrinin təhlükəsizliyinin qiymətləndirilməsi, zərərli proqramların analiz edilərək aşkarlanması və fəaliyyət sxeminin aydınlaşdırılması əsas məsələlərdən birinə çevrilir.

Müasir sandbox alətlərindən istifadə edərək zərərli proqramları avtomatik analiz etmək mümkündür. Bu analizlərin nəticələrinə uyğun olaraq mövcud kompüter şəbəkələrinin cari təhlükəsizlik vəziyyətini yüksəltmək mümkündür.

ƏDƏBİYYAT

- [1] D. Ucci, L. Aniello, R. Baldoni, “Survey of Machine Learning Techniques for Malware Analysis”, Computers & Security, vol. 65, 2018, pp. 1627–1636
- [2] M. F. Razak, N. B. Anuar, R. Salleh, A. Firdaus, “The rise of “malware”: Bibliometric analysis of malware study”, Journal of Network and Computer Applications, vol. 75, 2016, pp. 58-76
- [3] J. Stiborek, T. Pevný, M. Reháč, “Probabilistic analysis of dynamic malware traces”, Computers & Security, vol. 74, 2018, pp. 221-239
- [4] C. Lin, H. Pao, J. Liao, “Efficient dynamic malware analysis using virtual time control mechanics”, Computers & Security, vol. 73, 2018, pp. 359-373
- [5] M. Wagner, A. Rind, N. Thür, “Wolfgang Aigner, A knowledge-assisted visual malware analysis system: Design, validation, and reflection of KAMAS”, Computers & Security, vol. 67, 2017, pp. 1-15
- [6] S. Banin, G. Dyrkolbotn, “Multinomial malware classification via low-level features”, Digital Investigation, vol. 26, 2018, pp. 107-117
- [7] S. P. Choudhary, D. Vidyarthi, “A Simple Method for Detection of Metamorphic Malware using Dynamic Analysis and Text Mining”, Procedia Computer Science, vol. 54, 2015, pp. 265-270
- [8] M. A. Kumara, C. D. Jaidhar, “Automated multi-level malware detection system based on reconstructed semantic view of executables using machine learning techniques at VMM”, Future Generation Computer Systems, vol. 79, 2018, pp. 431-446
- [9] M. Cafasso, M. Tarral, “Designing flexible sandboxing solutions to adapt to new malware trends”, Computer Fraud & Security, vol. 2018, 2018, pp. 5-9
- [10] R. Islam, R. Tian, L. M. Batten, S. Versteeg, “Classification of malware based on integrated static and dynamic features”, Journal of Network and Computer Applications, vol. 36, 2013, pp. 646-656.

ANALYSIS OF MALWARE IN COMPUTER NETWORKS

Tural Yunusov

Institute of Information Technology of ANAS
Baku, Azerbaijan
turaly@mail.ru

Abstract – The article provides information about computer network security, malware, malware analysis methods, static analysis method, dynamic analysis method, virtual analysis of malicious activity and malware infection methods.

Keywords - computer networks, malware, rootkits, malicious mobile code, cookie files, hooking, sandbox.

Wi-Fi şəbəkəsində təhlükəsizlik məsələləri

Təbriz Ağaşov

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
tabriz@science.az

Xülasə — Məqalədə IEEE 802.11 (Wi-Fi) naqilsiz şəbəkələrinin informasiya təhlükəsizliyinə baxılmışdır. OSI şəbəkə modelinin əsasən fiziki və kanal səviyyəsinə edilən hücum növləri və onlardan müdafiə üsulları təhlil edilmişdir.

Açar sözlər — mobil trafik; IEEE 802; OSI modeli; frame; trafikin indikasiya xəritəsi (TİM)

I. GİRİŞ

Müasir dövrdə İnternetlə işləmək üçün kompakt qurğuların meydana gəlməsi informasiya texnologiyaları mütəxəssislərinin qarşısında yeni bir məsələ – kəbelləşdirilmiş İnternet mərkəzlərindən, provayderlərdən uzaq məsafədə yerləşən və kəbelləşdirilməsi çətin olan yerlərdə, şəbəkəyə çıxışı təmin etmək məsələsi dayanmışdır.

Wi-Fi (Wireless Fidelity) – naqilsiz lokal (Wireless LAN) şəbəkələrin təşkili üçün nəzərdə tutulan genişzolaqlı rədiyabirlik avadanlıqları standartıdır. Bu texnologiya şəbəkəyə əlverişliyi təmin etmək üçün istifadə edilən texniki vasitələrin inkişafında yeni bir addımdır. Belə texnologiyaların inkişafı hal-hazırda da davam etdirilir. Bir çox şirkətlərin apardığı tədqiqatlara əsasən, tezliklə smartfon və planşetlərdən gedən mobil trafikin daha çox hissəsi 2G/3G/4G/5G şəbəkələri vasitəsilə deyil, məhz Wi-Fi şəbəkələri ilə ötürülməkdir. Yaxın gələcəkdə bütün dünya mobil operatorlarında ümumi trafikin yalnız 40%-i istifadə ediləcək. 2020-ci ilə qədər isə 802.11 şəbəkələri üzrə ötürülən verilənlərin həcmi 30000 pbytdan 115000 pbyta qədər yüksələcəyi proqnozlaşdırılır. Belə artım Şimali Amerikanın və Avropanın bir çox ərazilərində fəal olaraq reallaşacaqdır [1].

Aparılan tədqiqatlar əsasında o qənaətə gəlmək olar ki, həm şəbəkələrin əhatə dairəsinin genişlənməsi, həm də istifadəçilərin sayının artması, Wi-Fi komplekslərinin təhlükəsizliyi haqqında ciddi tədbirlər həyata keçirməyə zəmin yaradır.

Naqilsiz şəbəkələrə mümkün hücumlardan danışmadan əvvəl, nəzərə almaq lazımdır ki, şəbəkənin quraşdırılması prosesi çoxlu mərhələlərdən ibarətdir və bu mərhələlərin hər

birinin təhlükəsizliyinin təmin edilməsi çox vacib məsələlərdir. Lakin, əgər şəbəkənin qurulması və sazlanması prosesində müəyyən səbəblərdən səhvlər edilərsə və tədbirlərin yerinə yetirilməsində çətinliklər meydana çıxarsa, bu zaman naqilsiz şəbəkəyə hücumlara şərait yaranacaqdır.

II. OSI MODELİ VƏ ONUN SƏVİYYƏLƏRİ

Kompüter şəbəkələrini yaradan zaman əsas məsələ müxtəlif xarakterli kommunikasiya avadanlıqlarının bir yerdə işləməsinin təmin edilməsi, informasiyanın formalaşması və mübadiləsi sisteminin (nəzərdə tutulan proqram və verilənlərin) bir-birinə uyğunlaşmasıdır. 1980-ci ildə Ümumdünya Standartlar Təşkilatı (ISO – International Standards Organization) tərəfindən irəli sürülmüş və hazırlanmış texniki təkliflər (standartlar) əsasında qarşılıqlı əlaqəsi olan şəbəkə avadanlıqlarının inkişaf etdirilməsinə başlanılmışdır. Bu baxımdan yeni bir etalon model (OSI – Open Systems Interconnection) işlənib hazırlandı. Bu model kompüter şəbəkələrinin inkişafında mühüm rol oynadı. OSI modeli şəbəkədə müxtəlif sistemli avadanlıqların arasındakı fərqi müəyyən etməklə yanaşı, həmin sistemlərin yerinə yetirdiyi funksiyaları da müəyyənləşdirir. Bir kompüterdən digərinə məlumat göndəriləndə baş verən proseslər standartlaşdırılmış formada bütün kompüterlərdə eyni ardıcılıqla aparılır. OSI modeli yeddi səviyyədən ibarətdir [2]:

- Tətbiqi səviyyə (Application);
- Təqdimmə səviyyəsi (Presentation);
- Səans səviyyəsi (Session);
- Nəqliyyat səviyyəsi (Transport);
- Şəbəkə səviyyəsi (Network);
- Kanal səviyyəsi (Data Link);
- Fiziki səviyyə (Physical).

Wi-Fi şəbəkələrinin əsasını IEEE 802 beynəlxalq standartlar ailəsi təşkil edir ki, bu da lokal hesablama şəbəkələrinin və meqapolislərdə yerləşən şəbəkələrin işini tənzimləyir. Bu standartlar ailəsinin xidmət və protokolları OSI şəbəkə modelinin iki aşağı səviyyələrində işləyir: fiziki və kanal səviyyələrində [2-4].

Fiziki səviyyə – bir qurğudan digərinə ikilik kombinasiya (bitlər) şəklində olan verilənlərin real fiziki ötürülməsi metodunu müəyyən edir. Fiziki səviyyə kanal səviyyəli məlumat ötürmə səviyyəsindən məlumat paketlərini qəbul edir, sonra onları 0 və 1 ikili kodlarına uyğun optik və ya

Şək. 1. Fiziki səviyyədə məlumatın ötürülməsi

elektrik siqnallarına çevirir (şək. 1). Bu siqnallar qəbuledici qovşağa ötürülür və qeyd edək ki, proses zamanı ötürülən informasiya analiz edilmir. Bu səviyyədə elektrik siqnallarının səviyyəsi, kodlaşdırma tipi, siqnalların ötürülmə sürəti və s. təyin edilir. Fiziki səviyyə fiziki şəbəkə mühitinə (məsələn: şəbəkə kabelinə, wi-fi nöqtəsinə) ən yaxın olan səviyyədir. Əsas vəzifəsi məlumatı ötürücülərlə ötürmək və qəbul etməkdir.

Fiziki səviyyədə baş verən proseslər əlaqə kanalının xassələrindən (kanalın ötürmə qabiliyyətindən (bit/s), vaxtdan və səhvlərin sayından) asılıdır. Əlaqə kanalı məlumatların ötürülmə istiqamətinə görə üç növə bölünür: simpleks (bir istiqamətə), dupeks (eyni vaxtda hər iki istiqamətə) və yarımdupeks (hər iki istiqamətə növbə ilə) ötürmələr. Fiziki əlaqə kanalı kimi, koaksial kabel, burulmuş cütələr, optovolokon kabel, radiodalğalar və s. nəzərdə tutulur.

Şək. 2. Kanal səviyyəsində kadrın formalaşması və ötürülməsi

Kanal səviyyəsi – şəbəkənin fiziki səviyyə ilə qarşılıqlı əlaqəsini və əlaqə kanalı ilə məlumatların ötürülməsini təyin edir. Kanal səviyyəsi şəbəkə səviyyəsindən məlumatı paket formasında qəbul edir, paketa başlıq və sonluq əlavə edir. Nəticədə başlıqdan, məlumat paketindən və sonluqdan ibarət tam məlumat qrupu – kadr (frame) əmələ gəlir. Bu kadr şəbəkənin fiziki səviyyəsindən keçərək növbəti hostun kanal

səviyyəsinə qəbul edilir (şək. 2). Kanal səviyyəsi hər bir kadrın düzgünlüyünü təyin edir. Kadrın nəzarət cəmini hesablayaraq onu hər bir kadrın əvvəlinə və sonuna əlavə edir. Qəbuledicidə nəzarət cəm hesablanır. Onlar eyni olduqda informasiya qəbul edilir. Səhvlər təyin edildikdə isə ötürmə təkrar icra olunur. IEEE 802 spesifikasiyasına əsasən bu səviyyə iki alt səviyyəyə bölünür: MAC (Media Access Control) və LLC (Logical Link Control).

Wi-Fi şəbəkəsi naqilli şəbəkədən fərqli olaraq, tamamilə açıq şəbəkə olduğu üçün, ona İnternetdən müdaxilə ilə yanaşı, həm də qonşu ofisdən və ya digər mərtəbədəki həmkarlar tərəfindən “qulaqasma” cəhdi təhlükə törədir. Bu isə belə hərəkətlərin, naqilsiz şəbəkədən, nəinki istifadə etməyə, həm də ona müdaxilə yollarını tapmağa gətirib çıxarır. Əgər şəbəkənin təhlükəsizliyinə lazımi diqqət yetirilməzsə, belə şəbəkəni tamamilə ümumi istifadəli kimi saymaq olar ki, bu da onun fəaliyyətində yaxşı şəkildə əks olunmayacaq və problemlərə yol açacaqdır [5]. Aşağıdakı bəndlərdə Wi-Fi şəbəkəsinə olunan hücumlar və onlardan müdafiə üsulları araşdırılmışdır.

III. ŞƏBƏKƏYƏ HÜCUM EDƏNLƏR

Qeyd edək ki, Wi-Fi şəbəkələrində təhlükəsizlik sistemini yaratmazdan əvvəl, şəbəkəyə müdaxilə edən özünü haqqında təsəvvür əldə etmək lazımdır. Bunu başa düşmək üçün şəbəkəyə müdaxilə edən potensial modelini tərtib etmək lazımdır.

Şəbəkəyə müdaxilə edənləri üç əsas kateqoriyaya bölmək olar [6]:

1. *Həvəskarlar*. Bu kateqoriyadan olanlar özlərini təsdiq etmək və ya əyləncə üçün şəbəkəyə müdaxilə edirlər. Onların əksəriyyəti şəbəkənin təhlükəsizliyinə ciddi təhlükə törətmirlər, bəziləri isə, hətta tapılan zəifliklər haqqında administratora məlumat verə bilərlər. Belə adamlar öz vərdisləri və bacarıqlarına lazımi diqqət yetirsələr informasiya təhlükəsizliyi üzrə yaxşı mütəxəssislərə çevrilə bilərlər.

2. *Pəşəkarlar* – əlaqə kanalına müdaxilə edənlər. Bu kateqoriyadan olan müdaxiləçilər informasiya mübadiləsi iştirakçılarının bir qədər başqa qrupunu təmsil edirlər. Bu şəxslərin marağı müxtəlif kontenti şəbəkəyə ötürmək üçün özgə şəbəkələrdən istifadə cəhdinə istiqamətlənmişdir. Çox vaxt bu tip kontentlər və verilənlər o qədər də qanuni xarakter daşımasalar da, özgə şəbəkəyə daxil olma cəhdi belə, beynəlxalq qanunvericiliyə əsasən həbs edilməyə qədər ciddi nəticələrə səbəb ola bilər.

3. *Cinayətkarlar*. Üçüncü kateqoriya ən təhlükəlidir. Onun təmsilçiləri Wi-Fi şəbəkəsinə icazəsiz müdaxilələri daha professional şəkildə həyata keçirməyi bacarırlar. Naqilsiz şəbəkələrdə mövcud olan anonimliklər və kanalların əhatə dairəsindən kənar əlverişli olması xüsusiyyətləri onları müdaxiləni reallaşdırmağa cəlb edir. Şəbəkəyə qoşulmuş çox sayda qurğulara malik olan şirkətdə verilənlərin ötürülməsinin hansı qurğular vasitəsilə baş verdiyini izləmək çətindir. Ən

güclü hücumlar kompüter texnologiyaları sahəsində yaxşı təhsilə malik olan və radiofizikanın prinsipləri ilə yaxından tanış olan bir qrup şəxslər tərəfindən törədilir.

IV. HÜCUMUN NÖVLƏRİ VƏ TƏSNİFATI

Wi-Fi şəbəkələrinin təhlükəsizlik sistemini yaratmaq üçün şəbəkəyə müdaxilə edənlər tərəfindən tətbiq oluna biləcək müxtəlif hücum növləri haqqında da təsəvvürə malik olmaq lazımdır.

Sistemə hücum – müdaxilə edənin informasiya sistemində giriş əldə etməyə yönələn fəaliyyəti və yaxud fəaliyyət yığımıdır [7].

Hücumların mahiyyətini asan başa düşmək üçün onları ümumi xassələrinə görə, adətən müxtəlif qruplarda birləşdirirlər:

1. Wi-Fi şəbəkələrində parametrlərin dəyişdirilməsinə yönəlmis hücum

Belə hücumlardan biri enerjinin qənaət rejimində parametrlərin sazlanmasına edilən hücumdur və şəbəkənin kanal səviyyəsində icra edilir. Hücum edən kliyentin “gözləmə” rejimi vəziyyətində olan qurğusunda bəzi parametrləri dəyişir və həmin qurğularda saxta kadrların yığılmasını həyata keçirir. Saxta kadrları kliyentə göndərilir. Kliyent kadrları qəbul etdikdən sonra Wi-Fi nöqtəsində bufer (müvəqqəti saxlama yeri) təmizlənir və beləliklə, kliyent öz kadrlarını ala bilmir. Kadrların saxta düzəldilməsi ilə reallaşan bu üsul yeni paketlərin olmaması haqqında məlumat verən trafikindikasiya xəritəsinin (TIM - Traffic Indication Map) tətbiqi zamanı həyata keçirilir. Belə hücumları reallaşdırmaq hücum edilən hostlarda TIM kadrlara girişin qapadılması əməliyyatının yerinə yetirilməsi hesabına çox mürəkkəbdir [8].

Şək. 3. Maneə yaradan qurğu ilə hücum

2. DoS hücumlar

DoS hücumlar (Denial of Service – xidmətdən imtina) şəbəkə resurslarının normal işini pozmaq və ya çətinləşdirmək məqsədilə həyata keçirilən hücum üsullarından biri kimi tətbiq edilir. Fiziki səviyyədə informasiyanın ötürülməsini reallaşdıran radiodalğaların təbiəti və Wi-Fi protokollarına məxsus

xüsusiyyətlər səbəbindən, yəni onlarda mövcud olan boşluqlara görə ötürülən informasiyalar hücumlardan müdafiə oluna bilməzlər. Belə hücumlar öz növbəsində bir neçə növə bölünürlər:

- Maneə yaradan qurğu ilə edilən hücum – belə əməliyyat xüsusi konfigurasiya edilmiş ötürücünün və ya naqilsiz kartın köməyi ilə şəbəkənin fiziki səviyyəsində icra edilir, bu da əlaqə kanalını icazəsiz trafiklə doldurur (şək. 3). Belə əməliyyatın əsas çatışmazlığı maneə yaradan qurğunun hücum edilən şəbəkənin bilavasitə yaxınlığında yerləşdirilməsi tələbidir.
- Əlaqə kanalının saxta freymlərlə doldurulması – maneə yaradan qurğu ilə edilən hücum kimi belə hücumlar da, praktiki olaraq dəf olunmayıdır. Əvvəlki hücum növündən fərqli olaraq, burada aparat hissəsi ilə yanaşı proqram təminatından da istifadə edilir. Məhz belə proqramlar saxta freymlər generasiya edir və onları ötürücü qurğu vasitəsilə göndərir [9].
- Düzgün formalaşdırılmayan autentifikasiya verilənlərinin köməyi ilə hücum – bu halda müdaxilə edən autentifikasiya olmaq üçün Wi-Fi nöqtəsinə sorğu tipli məlumatlar göndərir. Bu məlumatlarda saxta nöqtənin ünvanı, kliyentin ünvanı və belə saxta nöqtə üçün autentifikasiyaya giriş alqoritmı yazılır. Nəticədə, Wi-Fi nöqtəsi bu sorğuya cavab olaraq belə məlumat verə bilər: “Gözlənilməyən tranzaksiya nömrəsi ilə autentifikasiya məlumatı alınmışdır”. Bunun nəticəsində də əlaqə kəsilir.
- Wi-Fi nöqtəsinin müvəqqəti saxlama yerinin (buferinin) doldurulması.
- Wi-Fi nöqtəsinə qoşulmaq üçün edilən sorğuların həddən artıq olması. Belə əməliyyat əlaqəyə girən qurğunun MAC-ünvanının daim dəyişdirilməsi hallarında baş verə bilər.
- Kadrların ləğv edilməsi yolu ilə hücum.
- Verilənlərin nəzarət cəminin (CRC-32) dəyişdirilməsi ilə edilən hücum. CRC-32 ötürülən məlumatın tamlığını (düzgün olub-olmadığını) yoxlayan bir alqoritmdir. Əgər məlumatda bu ədəd dəyişdirilibsə, onda host bu məlumatı qəbul etmir və Wi-Fi nöqtəsi qoşulmaq üçün edilən sorğunu rədd edir. Həmin anda göndərənə hostdan həqiqi məlumatın müvəffəqiyyətlə qəbul edilməsini təsdiqləyən saxta bir məlumat gəlir. Məlumatın nəzarət cəminin (sonuncu dörd bayt) ötürülməsi anında, küy əngəlləri yaratmağın çətinliyi, belə hücumun reallaşdırılmasını çətinləşdirir. Belə hücumdan müdafiə kifayət qədər problemlidir [10].

3. Autentifikasiya sistemində hücumlar

MAC-ünvanların filtrasiyasına əsaslanan hücumlar. Belə

hücumu həyata keçirmək üçün hücum edən MAC-ünvanların axtarışı məqsədilə şəbəkə trafikini analiz edərək, növbəti hərəkətləri yerinə yetirir: ona lazım olan hostun şəbəkədə aktiv olmasını yoxlayır və bu hostun şəbəkədən deaktivləşməsinə gözləyir. Bəzən, hücum edən MAC-ünvanı istifadə edilən kliyentlə bir şəbəkədə olur, belə halda o, ARP-ni (ing. Address Resolution Protocol - ünvanı təyin etmə protokolu) söndürür və şəbəkələrarası ekranın istifadəsindən imtina edir. Əlavə olaraq hücum edən IDS-in (ing. Intrusion Detection Systems) işə düşməsindən qaçmaq üçün bu hostdan paketlərin göndərilməsini və ICMP (ing. Internet Control Message Protocol – məlumatlara nəzarət protokolu) üzrə porta girişin olmaması haqqında məlumatların davamlı olaraq izlənməsini zəruriləşdirir. Bəzən, ziyankar öz MAC-ünvanını hücum edilən hostun ünvanına dəyişməsi üsulunu tətbiq etməklə hücum edilən hostu söndürə bilər [9].

V. HÜCUMLARDAN MÜDAFİƏ ÜSULLARI

Naqilsiz şəbəkəyə edilən hücumların müəyyən edilməsini və şəbəkənin hər bir qovşağının bu hücumlardan təhlükəsizliyini reallaşdırmaq üçün, hücumları aşkar edən sistemlərdən (monitorinq sistemi - proqram təminatı) istifadə

Şək. 4. Wi-Fi şəbəkəsinin təhlükəsizliyini təmin edən monitorinq sisteminin iş sxemi

edilir (şək. 4).

Belə proqramlar aşağıdakı məqsədlərə nail olmağa imkan verir:

- ✓ Hücum edəni tapır, yəni şəbəkənin monitorinqini yerinə yetirməklə, istənilən qeyri-leqal wi-fi nöqtəsini və bu nöqtədən istifadə edərək istifadəçinin trafikini izləməyə cəhd göstərənə aşkarlayır;
- ✓ Şəbəkəni yoxlayır, yəni şəbəkədə olan naqilsiz avadanlıqlarda sazlamaların keyfiyyətinə nəzarət edir və müəyyən edilmiş boşluqların aradan qaldırılmasını təmin edir;
- ✓ İstifadəçiləri müdafiə edir, yəni şəbəkənin naqilsiz seqmentindəki qovşaqları qeyri-leqal girişlərdən və hücumlardan müdafiə edir.

IEEE 802.11 şəbəkələrinin fiziki və kanal səviyyəsində təhlükəsizliyini təmin etmək üçün əlavə olaraq aşağıdakı tədbirləri də yerinə yetirmək lazımdır:

- radioəhatə zonasını azaltmaq (əgər signal nəzarət edilən zonanın həddindən kənara çıxmasa, müdaxilə riski azalar);
- administratorun yeni parolunu dəyişmək (susmaya görə qəbul olunmuş paroldan fərqli olaraq);
- MAC-ünvanlara görə filtrasıyanı qoşmaq;
- şəbəkənin standart identifikatorunu (SSID - Service Set Identifier) dəyişmək və bu prosesi dövrü olaraq yerinə yetirmək;
- şəbəkədaxili şifrələməni aktivləşdirmək;
- müəyyən müddətlərdən sonra şifrələmə açarını dəyişmək;
- şəbəkələrarası ekranları və antivirusları qurmaq;
- şəbəkələrarası ekranlarda trafikə filtrasıyanı alqoritmlərinin reallaşdırılmasını təmin etmək;
- şəbəkədə quraşdırılmış avadanlığın rezervini və proqram təminatının sürətinin xüsusi sxemini hazırlayaraq, ehtiyat tədbirləri məqsədilə saxlamaq;
- şəbəkədə işləyən avadanlığa dövrü nəzarəti həyata keçirmək.

Bütün bu tədbirlər müəssisənin təhlükəsizlik siyasətində nəzərə alınmalı və istənilən tip avadanlıqda reallaşdırma imkanına malik olmalıdır. Qeyd edək ki, bu tələblərin reallaşması praktiki olaraq bütün müasir qurğularda mümkündür.

NƏTİCƏ

Məqalədə Wi-Fi şəbəkələrinə edilən hücumlar və onlardan müdafiə üsullarına baxılmışdır. Şəbəkənin fiziki və kanal səviyyələrinə edilən hücumların vaxtında müəyyən edilməsi və bu hücumlardan davamlı olaraq qorunmaq üçün həll yolları göstərilmişdir. Yaxın gələcəkdə Wi-Fi şəbəkələri üçün yeni təhlükəsizlik standartları meydana gələcəkdir, bu da ümumi təhlükəsizlik səviyyəsini qaldırmağa imkan verəcəkdir.

ƏDƏBİYYAT

- [1] Wi-Fi to Carry up to 60% of mobile traffic by 2019// Hamphir UK.– 2015, <http://www.juniperresearch.com/press/press-releases/wifi-to-carry-60pc-of-mobile-data-traffic-by-2019>.
- [2] G.Bora1, S. Bora, S.Singh, S.M.Arsalan, OSI Reference Model: An Overview, International Journal of Computer Trends and Technology, 2014, vol. 7, no. 4, pp. 2014-218.
- [3] 802.11-1999 - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
- [4] А. Б. Бакытов, Я. А. Ратахин, Ж. К. Ташенова. Технология широкополосного беспроводного доступа // Актуальные вопросы технических наук: материалы III Междунар. науч. конф. (г. Пермь, апрель 2015 г.). — Пермь: Зебра, 2015. — С. 41-43. <https://moluch.ru/conf/tech/archive/125/7424/>
- [5] Е. Патий, “Проблемы безопасности в беспроводных сетях”, <http://www.iso27000.ru/chitalnyi-zai/bezopasnost-bezprovodnyh->

setei/problemy-bezopasnosti-v-bezprovodnyh-setyah/.

- [6] A. Masiukiewicz, “Security Threats in Wi-Fi Networks”, Engineering and Science 2016, vol. 1, no.3: pp. 6–11.
- [7] А.Я. Приходько Словарь-справочник по информационной безопасности. - М.: Синтег, 2001. - 124 с.
- [8] В.Б. Щербаков, С.А. Ермаков Безопасность беспроводных сетей: стандарт IEEE 802.11. - М: РадиоСофт, 2010. - 255 с.
- [9] M. H. Yilmaz, E.G. Guvenkaya, H. M. Furqan, S.Kose, H. Arslan. “Cognitive Security of Wireless Communication Systems in the Physical Layer”, Journal of Wireless Communications and Mobile Computing, 2017, pp. 4-5.
- [10] R.M. Əliquliyev, N. Ağayev, R.M. Alıquliyev Plagiatlıqla mübarizə texnologiyaları. Bakı, “İnformasiya Texnologiyaları” nəşriyyatı, 2015, səh. 120-124.

SECURITY ISSUES IN WI-FI NETWORK

Tabriz Agashov

Institute of Information Technology of ANAS,

Baku, Azerbaijan

depart4@iit.ab.az, tabriz@science.az

Abstract — Article explores the information security of IEEE 802.11 (Wi-Fi) wireless networks. The layers of the OSI model are shown, and attacks on physical and channel levels are analyzed. Types of these attacks and defense methods are studied.

Keywords — mobile traffic; IEEE 802; OSI model; frame; traffic indication map (TIM).

Enerji sektorunda kibertəhlükəsizliyin təmin olunması məsələləri haqqında

Təhmasib Fətəliyev¹, Şahanə Mansurova²

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

^{1,2}depart3@iit.science.az

Xülasə— Məqalə milli təhlükəsizliyin kritik tərkib hissəsi kimi enerji sektorunda kibertəhlükəsizlik problemlərinin tədqiqinə həsr olunub. Enerji təhlükəsizliyi problemləri araşdırılmış, parametrik göstəricilərin təsnifatı, enerji sektorunda kibertəhlükəsizliyin xüsusiyyətləri və təmin olunması məsələləri təqdim edilmişdir. Azərbaycanda bu sahədə siyasət və alternativ enerji perspektivləri verilmişdir.

Açar sözlər— *enerji sektoru; enerji təhlükəsizliyi; kibertəhlükəsizlik; təhlükəsizlik riskləri; enerji birliyi.*

I. GİRİŞ

Enerji təhlükəsizliyi həm fərdi dövlətlərin, həm də bütövlükdə dünya təhlükəsizliyinin vacib bir komponentidir. Müasir kəskin geosiyasi qarşıdurma şəraitində ölkə iqtisadiyyatı, suverenliyi və müdafiə qabiliyyəti birbaşa enerji təhlükəsizliyinin təmin edilməsindən asılıdır. Buna görə strateji sahə sayılan enerji sektorunun tam dövlət nəzarətində olması milli təhlükəsizliyə nəzarətin vacib şərtidir.

Enerji təhlükəsizliyi məsələlərinin həllində təbii ehtiyatların əvəzedilməz olması nəzərə alınmalıdır. Bu resurslar, ümumiyyətlə, inkişaf etməkdə olan ölkələrdə istehsal və inkişaf etmiş ölkələr tərəfindən isə istehlak olunur və nəticədə onların arasında sosial-iqtisadi münasibətlərin bərabərsizliyinə gətirib çıxarır. Mürəkkəbliyi səbəbindən enerji təhlükəsizliyi konsepsiyası tamamilə iqtisadi, həm də texniki və təşkilati xarakter daşıyır. Ümumiyyətlə, enerji təhlükəsizliyinin formalaşması ilə bağlı təhdidlər daxili və xarici iqtisadi, siyasi, sosial-siyasi, texnogen və təbii sahələrdə mövcuddur. Terrorizm hallarının artması ilə xarakterizə olunan müasir şəraitdə yüksək riskli obyektlərə olan təhdidlərin sayı da sürətlə artır, ona görə də bu kritik bir problem kimi nəzərə alınmalıdır. Enerji təhlükəsizliyi obyektlərinə nüvə və su elektrik stansiyaları, neft platformaları, qaz və neft boru kəmərləri, karbohidrogen ehtiyatları, elektrik xətləri və s. aid edilir. Bu obyektlərə vurulan ziyanlar milli iqtisadiyyat üçün kritik və zərərli sosial hallar yarada bilər. Bütün bunlar, milli təhlükəsizliyin kritik tərkib hissəsi kimi enerji təhlükəsizliyinin təmin olunmasının aktual məsələ olmasına əsas verir.

Məqalədə milli təhlükəsizliyin mühüm tərkib hissəsi kimi enerji sektorunda kibertəhlükəsizlik məsələləri araşdırılmışdır.

II. ENERJİ TƏHLÜKƏSİZLİYİ, PROBLEMLƏR VƏ PARAMETRİK GÖSTƏRİCİLƏR

Enerjinin səmərəliliyi enerji təhlükəsizliyinə nail olunmasında əhəmiyyətli rol oynayır. Enerji təhlükəsizliyinin artırılması cəmiyyətin əsas məqsədi və davamlı enerji strategiyalarından ibarətdir, çünki enerji təhlükəsizliyi əsas insan ehtiyaclarını yerinə yetirmək üçün tələb olunur.

Enerji təhlükəsizliyi siyasəti probleminin vacibliyi onun sosial-iqtisadi sistemdə istifadəsinin aşağıda göstərilmiş dörd əsas aspektindən ibarət olan ümumi ictimai əhəmiyyətinə əsaslanır:

- əsas insan ehtiyaclarının və iqtisadi fəaliyyətin enerji tələbatının təmin edilməsi;
- müasir cəmiyyətin mövcud infrastrukturunun səviyyəsinin saxlanılması;
- əhali, kapital və istehlak artımını təmin etmək üçün enerjiden istifadə;
- iqtisadi infrastrukturda, texniki inkişafda və məhsuldarlığın artımında dəyişikliklərin dinamikasını təmin etmək.

Enerji təhlükəsizliyinə sistemin bütün ölçülərində istənilən təhdidlərdən asılı olmayaraq optimal və davamlı fəaliyyət göstərən xüsusiyyəti (ölçü, vəziyyət və ya statusu) kimi baxmaq olar. Bu tərifə əsasən bütün perspektivlər və risklər nəzərə alınır [1]. Enerji təhlükəsizliyinin ölçüləri və onlara uyğun parametrlərin təsnifatı aşağıdakı kimidir:

Əlçatanlıq – resursların, istehlakçıların və nəqliyyat vasitələrinin mövcudluğu;

Müxtəliflik – mənbələrin, yanacağın (enerji daşıyıcıları), vasitələrin (texnologiyalar, nəqliyyat) və istehlakçıların müxtəlifliyi;

Dəyər – enerjinin qiyməti (istehlakçılar, istehsalçılar, qiymətləri müəyyən edən sistem / subsidiyalar, enerji azlığı, neftin pik həddi və sabitlik), nasazlığın dəyəri və təhlükəsizlik sisteminin xərcləri;

Texnologiya və səmərəlilik – yeni texnologiyaların inkişafı, enerji sisteminin effektivliyi, enerji tutumluluğu və enerji qənaəti;

Yerləşmə – enerji sistemlərinin sərhədləri, enerji mənbəyinin yeri, sıxlıq əmsalı (mərkəzləşdirilmiş/paylanmış),

torpaqdan istifadə, qloballaşma, əhalinin yerləşməsi və sıxlığı, coğrafiya və sənaye intensivliyi;

Müddət – vaxt şkalası, hadisənin müddəti və effektin müddəti (mübarizə və ya zərbə);

Adaptivlik – adaptiv tutum;

Ətraf mühit – resursların kəşfiyyatı və paylanması, ekstraksiya və nəql olunma metodları, enerji istifadəsindən çıxan nəticələr, ətraf mühitin dəyişməsindən yaranan təsir və su hövzəsi ilə əlaqə;

Sağlamlıq – insan sağlamlığının enerji sisteminə təsiri və enerji sisteminin sağlamlığa təsiri (enerji sektoru işçiləri, istehlakçılar və beynəlxalq ictimaiyyət);

Mədəniyyət – enerji sistemə mədəni təsir (istehsal, əlaqə, istehlak, mədəni aspektlər) və mədəni aspektləri formalaşdıran enerji şərtləri;

Savadlılıq – informasiyanın əlçatanlığı (keyfiyyət, bazar məlumatı, ictimaiyyətin məlumatlandırılması və strukturlaşdırılmış təhsil proqramı), informasiyanın təqdimatı və təminatı; enerji məlumatlarından istifadə;

Məşğulluq – enerji təhlükəsizliyinin işsizliyin səviyyəsinə təsiri və məşğulluğun səviyyəsinin enerji təhlükəsizliyinə təsiri;

Siyasət – siyasi sistem, demokratiya/diktatura (təbiət, sabitlik, vətəndaşın iradəsi, daxili və xarici əlaqələr), tənzimləmə (liberallaşdırılmış və nəzarət edilən bazar, qaydalar və subsidiyalar) və idarəetmə (şəffaflıq qaydalarına tabe olmaq, selektiv qaydalara riayət etmək və qaydalara əməl etməmək/korupsiya);

Hərbi – enerjinin hərbi məqsədlər üçün istifadəsi, hərbi əlaqə, hərbi münaqişədə enerji vasitə kimi (enerji silahı) və destabilizasiya amili (resurslara həmlələr, ətraf mühitin korlanması və zorakılıq iqtisadiyyatı);

Kiber təhlükəsizlik – əlaqələr (kiberhücumlar), proqram vasitələrindən istifadə (müşahidə nəzarəti və məlumatların əldə edilməsi, SCADA, proqramların nasazlıqları) və İT bacarıqları.

Enerjiyədən istifadə etmək üçün texnologiya tələb olduğundan, enerji təhlükəsizliyi texnologiyaların inkişafı ilə birbaşa və dolaylı şəkildə əlaqəlidir. Bu mənada istehsal, ötürmə, emal, saxlama və paylaşdırma üçün yeni texnoloji həllər enerji təhlükəsizliyinə təsir göstərir. Beləliklə, yeni texnologiyalar yeni enerji mənbələrini təmin etməklə bərabər nəticədə enerji təhlükəsizliyini artırır. Məsələn, yeni elektroliz texnologiyalarının tətbiqi, enerji sistemə fosil yanacaqdan başqa yeni bir alternativ enerji daşıyıcısı (hidrogen) qazandırdı. Bərpa olunan enerjilərin inkişaf etdirilməsi bəzi tədqiqatçılar tərəfindən şübhə altına alınsa da, digərləri isə “daha təhlükəsiz enerji gələcəyinin” açarı olduğunu vurğulayırlar [2].

İT sahəsindəki inkişaf meyllərini nəzərə almaqla enerji sektorunun təhlükəsizliyini yalnız fiziki baxımdan deyil, eyni zamanda kiber mənada da qiymətləndirmək vacib məsələlərdən biridir. Kompüter və rəqəmsal proqramlardan istifadə enerji sisteminin (istehsal, nəql olunma və istehlak sahələrində) idarə olunmasının əsasını təşkil edir. Ona görə də kibertəhlükəsizliyin nəzərə alınmaması böyük iqtisadi itkilərə

səbəb ola bilər. Çünki enerji sistemləri avtomatlaşdırılmış rəqəmsal proqramlarla idarə olunur və İnternetə qoşulur. Onların müdafiəsinə əlavə olaraq, enerji sistemlərinə qarşı kiber hücumlar artır və nəticədə kibertəhlükəsizlik əsas problemə çevrilir. Belə kiber hücumlar daha asandır və enerji infrastrukturunun rəqəmsal proqramları terroristlər üçün cəlbədicə bir hədəfdir. Beləliklə, kiber hücumlardan qorunmanın düzgün təşkili enerji təhlükəsizliyinin təmin olunmasında mühüm rol oynayır.

III. ENERJİ SEKTORUNDA KİBER TƏHLÜKƏSİZLİK

Avropa Komissiyası (AK) üzv dövlətlərlə birlikdə 2016-cı ildə qəbul etdiyi “Şəbəkə və İnformasiya Sistemlərinin Təhlükəsizliyi üzrə Direktiv”i (*Directive on security of network and information systems – NIS Directive*) [3] və “Verilənlərin Mühafizəsinin Ümumi Qaydaları” (*General Data Protection Regulation – GDPR*) [4] ilə kibertəhlükəsizliyin təməlini qoymuşdur. Bu sənədlər Avropa cəmiyyətinin maraqları və vətəndaşları üçün lazımlı xidmətlərin fəaliyyətini müdafiə edərək, AK-nın “Rəqəmsal vahid bazar” (*Digital Single Market*) strategiyasına dəstək verir.

NIS Direktivi və *GDPR* sektorlar arasında fərqləndirmə aparmadan, öhdəlik səviyyəsi yalnız göstərilən xidmətlərin kritikliyindən asılı olan sahələrarası bir yanaşmanı təmsil edir. AK özünün “Enerji Ekspert Kiber Təhlükəsizlik Platforması”na (*Energy Expert Cyber Security Platform – EECSP*) enerji sektorunu mövcud qanunvericiliyin kifayət qədər əhatə etdiyini araşdırmaq və lazımsa, effektiv kibertəhlükəsizliyə nail olmaq üçün əlavə tədbirlərin görülməsi üçün tapşırıq vermiş və müvafiq nəticələr əldə etmişdir. Qeyd etmək lazımdır ki, *EECSP* ekspert qrupunun missiyası AK-na avropa səviyyəsində infrastruktur məsələləri, təchizatın təhlükəsizliyi, smart şəbəkə texnologiyaları və nüvə enerjisi daxil olmaqla enerji sektorunun açar nöqtələrinə aid siyasət və normativ sənədlər barəsində təkliflər verməkdir [5].

Kritik infrastruktur müasir cəmiyyətin fəaliyyəti üçün əsas xidmətləri dəstəkləyir və iqtisadi fəaliyyətin əsasının təşkilinə xidmət göstərir. Bunlara enerji, telekommunikasiya, maliyyə, səhiyyə və nəqliyyat sektorları aid edilir. Enerji infrastrukturunu ən mürəkkəb və kritik infrastrukturun əsas hissəsi sayıla bilər, çünki digər sektorların xidmətlərinin təmin edilməsi ondan asılıdır. Buna görə də enerji tələbatının təmin olunmaması iqtisadiyyata və vətəndaş cəmiyyətinin düzgün fəaliyyətinə mənfi təsir göstərir. AK tərəfindən enerji sektoru elektrik, neft və qaz kimi üç alt sektorla müəyyənləşdirilmişdir.

Rəqəmsal texnologiyalar enerji sektorunda getdikcə daha əhəmiyyətli rol oynayır. Smart enerji sistemləri enerjinin istehsalını, ötürülməsini, şəbəkə idarəçiliyini və bazar ilə əlaqəli vəzifələrini insanlarla bağlı bir sistemdən daha həssas və daha sürətlə həyata keçirir, beləliklə enerji idarəçiliyinin optimallaşdırılmasına, ondan istifadəyə üstünlük verilməsinə və nasazlıqların tez aradan qaldırılmasına nail olunur.

Enerji idarəetmə sistemləri əsasən real vaxt rejimində fəaliyyət göstərən və tipik olaraq mərkəzi nəzarət stansiyası və ya mərkəzinə qoşulan, bir-biri ilə iyerarxik əlaqəli fiziki və elektron sensorlar, idarə və nəzarət qurğularından təşkil olunur.

“Verilənlərin dispetçer idarə olunması və toplanması” (*Supervisory Control And Data Acquisition – SCADA*) sistemlərindən təşkil olunmuş enerji idarəetmə sistemləri ərazi cəhətdən paylanmış mühitdə elektrik enerjisinin ötürülməsi və paylanması şəbəkələrində əməliyyatların monitorinqini və nəzarətini həyata keçirir. SCADA sistemləri uzaqda yerləşmiş məlumat toplama yerlərindən, sensorlardan, nəzarət, idarə qurğularından, və avtomatlaşdırılmış funksiyalardan məlumat toplayır, nümayiş etdirir və saxlayır. Onlar real vaxt rejimində istifadə olunan proseslərin idarəetmə sisteminin (məsələn, ötürülmə və paylanmada) bir hissəsini təşkil edir. “Paylanmış nəzarət sistemi” (*Distributed control systems – DCS*) isə ayrı-ayrı obyektlər və ya kiçik coğrafi sahələr üçün istifadə olunur. İdarəetmə sistemləri uzaq məsafədə yerləşən terminal qurğuları və programlaşdırılmış məntiqi kontrollerlərə qoşulmuşdur. Bu qurğular giriş verilənləri və siqnalına cavab olaraq sistem verilənlərinə nəzarət edir və müvafiq idarəetmə funksiyaları həyata keçirir.

Generasiya sistemlərində enerji istehsalı prosesləri nəzarət altına alınmalıdır. Neft, kömür və ya qazın yanması və nüvə parçalanma prosesləri turbinləri hərəkətə gətirmək üçün istifadə olunan istilik istehsal edir. Bu turbinlər enerji istehsal edir və bütün istehsal prosesi operatorların izlədiyi əsas dispetçer məntəqəsinə bağlanan analog və ya rəqəmsal sistemlər tərəfindən idarə olunur. Bərpa olunan resurslar (külək, günəş, hidro enerjilər) bir-biri ilə olduqca əlaqəli olan sistemlərdir və enerji istehsalını, külək və günəş kimi resursların təbii kəsilmə davranışlarını nəzərə alan mərkəzi stansiyalar tərəfindən idarə olunur.

Hal-hazırda enerji sektoru köhnə, həm də yeni nəsil texnologiyalardan ibarətdir. Müasir texnologiyalar enerji infrastrukturuna keçmişə nəzərən daha qabaqcıl yollarla (ikitarəfli naqıl, simsiz rabitə və s.) əlaqə quran yeni ağıllı komponentlər (smart elektrik və qaz sayğacları, rəqəmsal klapanlar və nasoslar və s.) gətirir. Bu yeni komponentlər İT-na əsaslanır. Tipik olaraq, ehtiyat hissələrinin artıq mövcud olmadığı və ya istifadə olunmadığı üçün analog komponentlər yeni rəqəmli sistemlərlə əvəz olunur.

Beləliklə, İT-nin belə geniş tətbiqi ilə enerji təminatı sistemlərində kiber risklərə və təhdidlərə qarşı davamlılığın təmin edilməsi daha vacib xarakter alır [6]. Kibertəhlükəsizliyin enerji sektorunda mühüm problemi kiber hücum halında belə etibarlılığı və dayanıqlılığı dəstəkləməkdir. İT sistemlərindən fərqli olaraq, enerji sektorunda kiber hücumların təhlükəsizlik problemləri, nasazlıqlar və hətta elektrik kəsintiləri ilə nəticələnə biləcəyindən idarəetmə sistemi dayanmadan fəaliyyətini davam etdirməyə hesablanmalıdır.

Kibertəhlükəsizlikdə məxfilik, tamlıq və əlçatanlıq kimi ümumi üç müdafiə məqsədi qəbul edilmişdir. Enerji sektorunda ən yüksək prioritetli məsələ sektorda sahə tətbiqləri ilə bağlıdır. Məsələn, generasiya və ötürülmədə əlçatanlıq və tamlıq ən vacib olanlardır. Dəyişdirilmiş və ya gecikmiş məlumatlar qurğuların yanlış konfigurasiya olunmasına və nəticədə sistemin etibarlılığına təsir göstərə bilər. Qabaqcıl ölçmə infrastrukturunu üçün müştərinin şəxsi məlumatlarının məxfiliyi ən vacib olanıdır. Kompüter təhlükəsizliyi olaraq adlandırılan

kibertəhlükəsizlik nüvə təhlükəsizliyinin bir hissəsidir. Burada kompüter təhlükəsizliyinin müdafiəsinin məqsədləri nüvə və ya digər radioaktiv maddələrin icazəsiz dəyişdirməsi, nüvə materialları və obyektlərinə qarşı təxribat və ya nüvə məlumatlarının oğurlanmasına gətirib çıxara biləcək kiber hərəkətlərin qarşısını almaqdır.

EECSP ekspertləri enerji sektoruna aid olan kibertəhlükəsizlik sahəsindəki problemləri aşağıdakı kimi təqdim edirlər:

- Transsərhəd əlaqəli enerji şəbəkəsində dayanıqlıq.
- Cari təhdid və riskləri əks etdirən müdafiə konsepsiyaları.
- AB-də kiber hücumların emalı.
- Mövcud enerji şəbəkəsi və ya nüvə obyektinin layihələndirilməsində tam şəkildə nəzərə alınmayan kiber hücumların effekti.
- Yüksək əlaqələndirilmiş yeni texnologiyaların və xidmətlərin tətbiqi.
- İnfrastruktur və xidmətlərdə autorsinqi.
- Enerji sistemlərində istifadə olunan komponentlərin bütövlüyü.
- Bazar iştirakçıları arasında yüksək qarşılıqlı əlaqə.
- İnsan resurslarının mövcudluğu və onların bacarığı.
- Real zaman/əlçatanlıq rejimində olan tələblərdən fərqli kibertəhlükəsizlik tədbirlərinə qoyulan məhdudiyyətlər.

IV. AZƏRBAYCANDA ENERJİ TƏHLÜKƏSİZLİYİ VƏ ENERJİ BİRLİYİ PERSPEKTİVLƏRİ

Azərbaycan neft və qaz kimi ənənəvi enerji resursları ilə məşhur olan, enerji baxımından zəngin bir ölkədir. Enerji təhlükəsizliyi digər ölkələrdə olduğu kimi Azərbaycanın milli təhlükəsizliyinin əsasını təşkil edir. Enerji təhlükəsizliyi strategiyası 1994-cü ildə “Əsrin müqaviləsi” imzalandıqdan başlamışdır. “Əsrin müqaviləsi” ölkənin iqtisadi inkişafında, həm də dünya enerji tədarüku üçün yanacaq və enerji ehtiyacının təmin edilməsi prosesində fəvqəladə yer tutur. Strateji və əhəmiyyətli obyektlərin etibarlı enerji təchizatı, boru kəmərlərinin təhlükəsizliyi, enerji mənbələrinin diversifikasiyası, ekoloji tələblərin nəzərə alınması və enerji resurslarının səmərəli istifadəsi Azərbaycanın enerji təhlükəsizliyi prinsiplərini təşkil edir [7]. Bu prinsiplərə görə enerji təhlükəsizliyi risklərini aşağıdakı kimi təyin etmək olar:

- Alternativ enerji mənbələrindən istifadə etməklə tükənən enerji resursları olan neft və qaz hasilatının azaldılması.
- Neft və qaz boru kəmərlərinin təhlükəsizliyi.
- Enerji resurslarının sabitliyi və səmərəliliyi.

- Alternativ enerji ehtiyatlarının istehsalının çatışmazlığı.

Milli Enerji Strategiyasına əsasən aşağıdakı həll və imkanları qeyd edək:

- Azərbaycanın tranzit və ixrac boru kəmərlərinin təhlükəsizliyinin artırılması;
- Müasir Avropa standartlarına əsaslanan enerji infrastrukturunun yaradılması;
- Tranzit ölkə olaraq Xəzər hövzəsi və Orta Asiyadan fosil yanacaq enerjisinin həcmi artırmaq;
- Azərbaycanda hərtərəfli enerji tələbatının idarəetmə siyasətini inkişaf etdirmək, başqa sözlə, tələbatın azaldılması;
- Bərpa olunan enerji ehtiyatlarından istifadənin artırılması;
- Enerji resurslarının tədricən təmin edilməsi baxımından enerji resurslarının diversifikasiyası və təhlükəsizliyi.

Avropa birliyi (AB) və Şərq tərəfdaşlığı (*Eastern Partnership – EaP*) ölkələri ilə əməkdaşlıq münasibətləri enerji təhlükəsizliyi problemlərinin səmərəli şəkildə həll edilməsi üçün şərait yaradır. Azərbaycan iqtisadiyyatının enerji sektoru sayəsində inkişaf etdiyini nəzərə alaraq ölkə bu sektoru inkişaf etdirməyə maraqlıdır. Qərb ölkələri Azərbaycanı AB də enerji təhlükəsizliyinin əsas təminatçısı hesab edərək onunla strateji münasibətlərinin səviyyəsini qaldırdılar. Nəticədə, 7 noyabr 2006-cı ildə Azərbaycan Respublikası ilə AB arasında strateji tərəfdaşlığın enerji məsələləri üzrə Anlaşma Memorandumu imzalanmışdır. “Şahdəniz-2” layihəsi çərçivəsində 2013-cü ilin dekabr ayında, dünyanın aparıcı neft-qaz şirkətləri və bir çox Avropa ölkələri tərəfindən təbii qazın istehsalı, pay bölgüsü və ixracatı haqqında son investisiya qərarının imzalanması yalnız Azərbaycan üçün deyil, habelə Avropa və dünyanın enerji təhlükəsizliyinin təmin edilməsində mühüm rol oynayacaqdır. “Şahdəniz-2” layihəsi, Azərbaycan və Gürcüstan arasında Cənubi Qafqaz boru kəmərinin Trans - Asiya və Transadriatik qaz boru xəttini genişləndirərək Avropanın inşaat planlarının həyata keçirilməsinə kömək edəcək və yeni qaz dəhlizi açacaqdır. Bu məsələlər təhlükəsizlik problemlərinin idarə olunması baxımından Azərbaycan təcrübəsini göstərir. Ənənəvi enerji ehtiyatları bərpa edilmədiyindən Azərbaycan bərpa olunan enerji ehtiyatlarına investisiya yatırmağa başlamışdır. Artıq həyata keçirilmiş strateji istiqamətləri aşağıdakı kimi sistemləşdirmək olar. Onlardan biri 2004-cü il 21 aprelə qəbul olunmuş “Alternativ və bərpa olunan enerji ehtiyatlarının istifadəsi üzrə Dövlət Proqramı”dır. Digər bir dövlət proqramı 2005-ci ildə qəbul olunmuş “2005-2013-cü illərdə Alternativ və Bərpa Olunan Enerji Mənbələrinin istifadəsi üzrə Dövlət Proqramı”dır. Bu, 2009-cu ildə Alternativ və Bərpa Olunan Enerji üzrə Dövlət Agentliyinin yaradılmasına gətirib çıxarmışdır.

Beləliklə, Azərbaycanın AB və *EaP* ölkələri ilə əməkdaşlığı enerji təhlükəsizliyinin əsas prinsiplərini təşkil edir. Böyük neft və qaz layihələri baxımından bu münasibətlər çox vacibdir. Azərbaycanın Avropa enerji birliyi ilə əməkdaşlığı neft boru kəmərlərinin təhlükəsizliyi, alternativ

enerji stansiyalarının tikintisi və inkişafı, enerji sektorunun diversifikasiyası kimi enerji təhlükəsizliyi problemlərinin həllinə öz töhfəsini verir. AB Azərbaycanda neft boru kəmərlərinin təhlükəsizliyi, bərpa olunan və alternativ enerji obyektlərinin tikintisi və inkişafında da əməkdaşlıqda maraqlıdır. Bütün bunlar göstərir ki, Azərbaycan Respublikası əsas enerji strategiyası kimi bu sektoru yeni investisiyalar qoymaqla inkişaf etdirir. Nəticədə yeni iş yerlərinin açılmasını, enerji təhlükəsizliyini, enerji sabitliyini, iqtisadiyyatın və enerji sektorunun diversifikasiyasını və ətraf mühitin qorunmasını təmin etməkdir.

NƏTİCƏ

Milli təhlükəsizliyin kritik tərkib hissəsi olan enerji təhlükəsizliyinin təmin olunması çoxistiqamətli, mürəkkəb və aktual məsələdir. Neft və qaz resursları ilə zəngin olan Azərbaycan üçün bu problem mühüm əhəmiyyətə malikdir. Məqalədə enerji təhlükəsizliyi sahəsində aparılmış araşdırmalar nəticəsində problemlər, parametrik göstəricilərin təsnifatı təqdim olunmuş, enerji sektorunda kiber təhlükəsizliyin xüsusiyyətləri və təmin olunması məsələləri verilmişdir. Azərbaycanda bu sahədə aparılan siyasət və perspektivlər şərh olunmuşdur.

ƏDƏBİYYAT

- [1] A. Azzuni, C. Breyer, “Definitions and dimensions of energy security: a literature review”, *WIREs Energy Environ* 2018, 7:e268, doi: 10.1002/wene.268
- [2] J. Ren, B. Sovacool, “Enhancing China’s energy security: determining influential factors and effective strategic measures” *Energy Conver Manage* 2014, 88:589–597.
- [3] Directive on security of network and information systems, <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>
- [4] General Data Protection Regulation, <https://eugdpr.org/>
- [5] Energy Expert Cyber Security Platform, https://ec.europa.eu/energy/sites/ener/files/documents/EECSP%20_%20CFE_FINAL.pdf
- [6] Cyber Security in the Energy Sector, https://ec.europa.eu/energy/sites/ener/files/documents/eeesp_report_final.pdf
- [7] Energy security and energy union perspectives in Azerbaijan, <http://cesd.az/new/wp-content/uploads/2015/11/>

CYBERSECURITY ENSURING ISSUES IN THE ENERGY SECTOR

Tahmasib Fataliyev and Shahana Mansurova
Institute of Information Technology of ANAS, Baku, Azerbaijan
depart3@iit.science.az

Abstract- The article focuses on cyber security issues in the energy sector as a critical component of national security. Energy security problems have been studied, types of parametric indicators, and features and provision issues of cyber security in the energy sector have been presented. The policy and alternative energy perspectives have been given in this area in Azerbaijan.

Keywords- energy sector, energy security; cyber security; security risks; energy union.

Evaluating the indicators of web resources operating in the ccTLD domain zone as a key component of national security

Yusif Sadiyev

Institute of Information Technology of ANAS, Baku, Azerbaijan
sadiyev.yusif@gmail.com

Abstract—Currently, the number of web resources and Internet users is rapidly increasing as demand of time. This process generates Web Data, collected from web resources, within Big Data. Conducting multidisciplinary analytics of the web resource based on the collected data is an important issue for the country. Because the characterization of processes in the national domain zone of the country and predictive information depend on the analytical process mentioned. Web resource analytics not only help to generate statistical reports, but also help to detect situations that might be a threat to the National Information Security on time. It shows that analytics of web resources are a key component of the country's National Information Security.

Keywords—web analytics, web content mining, web usage mining, web management, user profiling, e –Government.

I. INTRODUCTION

Analytics of web resources in the country code Top Level Domain (ccTLD) constitutes the basis of National Information Security, which is an important component of the national security of the country. It also allows analyzing citizens' online relationships with e-government.

Analytics of web - resources allows prepare reports on the following topics [2-4]:

- User behavior and profiles,
- The number of applications in the web-resource,
- Keywords sought by the user,
- Geography of visitors,
- Duration of users' stay on the web resource,
- Switch between pages, etc.

The e-government's web infrastructure is formed relying on the web resource of every agency, operating at public sector. Formed web infrastructure creates online interactive communication among organizations and citizens [1].

It should be carried out the analytics of web resources, in particular multi-purpose analytics in the process of establishing online relationships among citizens and governmental bodies. In this case, data collected in decision-making to improve the performance of web resources and increase effectiveness are used [5].

Detecting technical errors in web resources, operating in the e-government environment, identifying content-oriented errors and adapting to user requirements can be accomplished by effective web analytics. By using web analytics, it is possible to set user and visitor interest rates, identify new users'

interests, and investigate the reasons of leaving the web site for regular users [6].

Timely identification of cases such as terror threatening security with the help of Web Content Mining and Web Usage Mining is now actual and relevant today [7].

The main task of the National Statistical System is to provide feedback between users and the e-government and to provide predictions by applying statistical mechanisms by archiving all the information collected. The National Statistical System is set up according to the national interests of the country and all analytical process is reflected there.

There are a large number of platforms involved in web analytics. Web sites of countries without a National Statistical System are analyzed by these platforms. In many cases, service policies of these platforms do not meet the national interests of the country. And analytics of web -resources, which is of critical importance for the country, is not accepted by taking into account the risk factor. As an example, we can show the e-government portal that offers online services to citizens. In this case, web analytics can now be regarded not only as a statistical reporting process, but also as an essential component of National Security: a key aspect of National Statistical System, one of the National Information Security goals.

It is known that, the users' behavior data is collected by sensors due to evaluate the performance of the web resources. The data collected allow for multi-purpose statistics. During multi-purpose statistics, it is possible to improve the work of the web - resource, assess security, conduct users' behavior map and other statistical reports. All of these can be considered as statistical mechanisms.

The first step in statistical mechanisms is the collection of initial information from web resources. This information is collected through sensors. Basically, two methods are used [8, 9]:

- Log Files – data is collected on server log files, and analytics is done with log analytics applications
- Page Tagging - is the collection of data through a web page code (script)

Both methods of data collection is used in the mechanisms of web resources statistics. Platforms, offering analytics services, are mostly used by Page Tagging. In the page tag method, the web page provides a "code" placed on the page.

It is a method of collecting, storing and processing of data, which is more relevant to the country's national interests, through Log files. However, big resource is needed in this case.

The page tag method is used widely. The missing key element of this method is to collect, store, and analyze data on an external server.

II. ASSESSMENT ANALYSIS OF THE INDICATORS OF WEB-RESOURCES AND MODERN STATUS

It is known that, web analytics of the web-resources are conducted by different platforms and these platforms use the page tag method [9, 10]. Sample: Google Analytics, Yandex. Metrika, LiveInternet, etc. platforms.

However, these methods cannot be considered satisfactory for national interests to analyze the evaluation of the system of electronic services for citizens. And some of the subsystems of the web resources are closed systems.

In these cases, the collection and processing of data for the evaluation of the indicators of resources can be done by log files or the platforms providing analytical services are required to provide services based on national interests. It is important to note that to keep the information collected through the Page tag on the platform servers along with country's servers and use them in accordance with the National Information Security requirements is relevant.

As can be seen from Table 1, 33.8% of web resources do not use analytics services, and 66.7% use analytics services, the percentage of which is as follows:

Google Analytics	57.1%
Yandex.Metrica	5.3%
WordPress Jetpack	4.8%
LiveInternet	2.7%
Hotjar	2.1%
New Relic	1.8%
Matomo	1.3%
StatCounter	1.1%
Top.Mail.Ru	0.9%

TABLE 1: COMPARISON OF WEB-ANALYTICS PLATFORMS [11]

According to statistical figures, 178,329,0123 websites are active in the worldwide web and 66.7% of them, ie 1189420495 websites use analytics services. At this time, data collected for analytics creates Big Data. And their analysis comes to the problem of Big Data Analysis [12].

III. CONCLUSION

The experience of leading countries shows that analytics of web resources in the national domain zone of the country directly links to the national security issue. Leading countries with experience in this field build their own statistics system. Initial data is collected through the sensors placed in web-resource and statistics is carried out in accordance with the requirements of national interests.

The main direction of the National Statistical System is to maintain reliable the data collection from web resources, carry out analytics on existing experience and ensure the protection of the information integrity.

Analytics of web sites in ".az" domain is analyzed on different platforms because it has not got a National Statistical System, and web resources of strategic importance for the state cannot use these services for national interests. Thus, the services provided by web analytics are not used.

Acknowledgment

This work was supported by the Science Development Foundation under the President of the Republic of Azerbaijan – Grant № EIF-BGM-4-RFTF-1/2017-21/08/1.

REFERENCES

- [1] Rasim M. Alguliev, Farhad F. Yusifov, "Some Actual Scientific And Theoretical Problems Of Formation Of The Electronic Government And The Perspectives Of Their Solutions " Journal of Problems of Information Society, pp. 5–7, April 2014.
- [2] <https://www.clicktale.com/academy/blog/a-brief-history-of-web-analytics/> (10.05.2018 09:35)
- [3] Clifton, B., "Advanced Web Metrics with Google Analytics", Second Edition, Wiley, New York, USA, 2008, page 531
- [4] Google Analytics. <http://www.google.com/analytics/>. May 15, 2018.
- [5] Kaushik A., "Web Analytics 2.0 - The Art of Online Accountability and Science of Customer Centricity", Wiley Publishing, Inc. 2010, 475.
- [6] Rasim Alguliyev and Farhad Yusifov, "The Effective Mechanisms in Monitoring and Management of E-Government" Journal of Public Administration and Governance, 2015, vol.5, no2, pp. 58–60.
- [7] Ramesh Yevale, Mayuri Dhage, Tejali Nalawade, Trupti Kaule, "Unauthorized Terror Attack Tracking Using Web Usage Mining", Ramesh Yevale et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, page 1210-1212
- [8] Agosti, M., Crivellari, F., Di Nunzio, G.M., "Web log analysis: a review of a decade of studies about information acquisition, inspection and interpretation of user interaction", Data Mining and Knowledge Discovery 2012, 24(3), page 663–696.
- [9] Cicchetti, A., Di Ruscio, D., Eramo, R., Maccarrone, F., Pierantonio, A., "beContent: A Model-Driven Platform for Designing and Maintaining Web Applications", pp. 518–522. Springer, Berlin, Heidelberg 2009, pp. 518-522
- [10] Anthony Ferrini, Jakki J. Mohr, "Uses, Limitations, and Trends in Web Analytics. In Handbook of Research on Web Log Analysis", Chapter VII, 2009, pages 122 – 140.
- [11] Xing, Guo, Fitzgerald, and Xu., "Google Analytics based Temporal-Geospatial Analysis for Web Management", A Case Study of a K-12 Online Resource Website. In International Journal of Information Science and Management, 2015, Vol. 13, No. 1, pages 87-106
- [12] Ledford, J.L., Teixeira, J., Tyler, M.E., "Google analytics", John Wiley and Sons 2011, 434 pages.

Verilənlərin sanitarizasiyasının informasiya təhlükəsizliyinin təmin olunmasında rolu

Sabirə Ocaqverdiyeva

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

allahverdiyevasadira@gmail.com

Xülasə – Məqalədə verilənlərin sanitarizasiyasının mahiyyəti və kateqoriyaları haqqında məlumat verilmişdir. Verilənlərin sanitarizasiyasının alqoritmləri analiz edilmişdir. Həssas verilənlərin konfidensiallığının təmin olunmasında və İnternetdə uşaqların təhlükəsizliyinin təmin edilməsində onun rolu göstərilmişdir.

Açar sözlər– verilənlərin sanitarizasiyası, sanitarizasiya alqoritmləri, təhlükəsizlik, uşaqların təhlükəsizliyi.

I. GİRİŞ

İnformasiya texnologiyaları və vasitələrinin inkişafı məlumat əldə etmək imkanını asanlaşdırsa da, informasiya təhlükəsizliyi baxımından ciddi təhdidlərə yol açır. İnternet sürətlə inkişaf edərək cəmiyyətin bütün seqmentlərinə hərtərəfli və dərin nüfuz edir, ondan həm fərdlər, həm də təşkilatlar müxtəlif məqsədlərlə istifadə edirlər. İnformasiya cəmiyyətində insan fəaliyyətinin, demək olar ki, bütün sahələri üzrə məlumatlar (dövlət idarəçiliyi, biznes, şəxsi məlumatlar, elm-təhsil, səhiyyə sistemi və s.) ənənəvi mühitdən elektron mühitə inteqrasiya olunur. İnformasiya mübadiləsi artır və məlumatlar istifadəçi üçün əlçatan olur. Məlumat şəxsin kimliyini aşkar edərkən və ya məxfi hesab olunan məsələləri açıqladıqda, konfidensiallıq üçün ciddi bir təhlükə yaradır. Araşdırmalar göstərir ki, fərdlərə və ya təşkilatlara məxsus olan məlumatların məxfiliyinin pozulması riski getdikcə artır [1]. Hazırda mütəxəssisləri ən çox narahat edən məsələlərdən biri verilənlərin onlayn mühitdə təhlükəsizliyinin təmin edilməsidir.

Virtual mühitdə istifadəçilərin, xüsusilə, uşaqların müəyyən informasiya ilə qarşılaşması bir çox neqativ hallara səbəb olur. İstər İnternet, istərsə də televiziya məkanında ziyanlı kontentlə qarşılaşmanın nəticəsində onların təhlükəsizliyi pozulur və zəif uşaq psixologiyası ciddi mənfi təsirlərə məruz qalır.

İnformasiya təhlükəsizliyi ilə əlaqədar məsələlərin həllində və zərərli informasiyanın qarşısının alınmasında müxtəlif proqram təminatlarından istifadə olunmasına baxmayaraq, çox vaxt uşaqlar təhlükələrin qurbanı olur. Bu problemlərin qarşısının alınmasını və təhlükəsizliklə bağlı məsələlərin həllini tələb edən avtomatlaşdırılmış texniki vasitələrdən istifadəni və yeni elmi yanaşmaları tələb edir.

Məqalədə verilənlərin sanitarizasiyası ((təmizlənməsi –VS)

(*ing. Data Sanitization*)) texnologiyalarından istifadə etməklə ziyanlı kontentin qarşısının alınmasında, məlumatların konfidensiallığının təmin olunmasında və yaddaş qurğularının sanitarizasiyasında istifadə olunan təmizlənmə alqoritmləri və sanitarizasiyanın kateqoriyaları haqqında məlumat verilir.

II. VERİLƏNLƏRİN SANİTARİZASIYASININ KATEQORİYALARI

VS-nin mahiyyəti həssas, fərdi, məxfi, konfidensial, tövsiyə olunmayan və s. məlumatların geniş ictimaiyyətə çatdırılmasının qarşısını almaqdan və ya müəyyən məhdudiyyətlərin tətbiq olunmasından ibarətdir [2]. Sanitarizasiya prosesi sənəd daxilində olan həssas məlumatları aradan qaldırmaqla sənədlərin təsnifat səviyyəsini formalaşdırır [3]. Sanitarizasiya (*ing. sanitization (classified information)*) həssas məlumatların (mətn, audio, video və s.) təmizlənməsi prosesidir [4]. Adətən, çap olunmuş materiallar üzərində redaktə kimi həyata keçirilən bu xüsusi emal prosesindən onlayn resurslarda da istifadə edilir.

Təhlükəsizlik məsələsi geniş sahəni əhatə edir. Sanitarizasiya prosesi verilənlərin əhəmiyyətli hesab olunduğu yerlərdə tətbiq edilir. Buraya hökumət təşkilatları, hərbi təşkilatlar, maliyyə müəssisələri və s. aid edilə bilər. İnformasiyanı icazəsiz girişlərdən məxfi saxlamaq üçün məlumatların konfidensiallığının təmin edilməsi vacibdir [5]. Fərdlərə məxsus olan şəxsi, həssas məlumatların gizlədilməsi (kommersiya sirrini təşkil edən məlumatlar, işçilərin şəxsi məlumatları, informasiyanın sahibinin nüfuzuna zərər verə bilən və digər məxfi məlumatlar) həmin məlumatların qorunmasında daha əhəmiyyətlidir [6].

Sanitarizasiya prosesi tətbiq sahələrinə görə aşağıdakı kateqoriyalara bölünür (Şəkil 1.) [7]:

Şəkil 1. Sanitarizasiya prosesinin tətbiq sahələrinə görə kateqoriyaları

- Disklərin sanitizasiyası – xarici yaddaş qurğularını və ya sabit disk sürücülərini təmizləmək üçün istifadə olunur;
- Qeydiyyatın sanitizasiyası – qeydiyyat tarixi və ona aid olan məlumatların silinməsinə kömək edir;
- Faylların sanitizasiyası – faylların tarixini və onlara olan bütün müvafiq istinadları silir;
- USB-nin sanitizasiyası – USB-ləri, daşınabilən disk sürücülərini və fləş diskləri təmizləmək üçündür;
- Qovluqların sanitizasiyası – qovluğun daxilində olan bütün qovluqları /alt qovluqları və orada saxlanılan faylları tamamilə silmək imkanına malikdir.

Ümumiyyətlə, sanitizasiya prosesi özündə verilənlər bazasının hər hansı proqramla silinməsini, sanitizasiya olunacaq qurğunun başqa qurğu ilə əlaqələndirilməsini, yaxud da fiziki olaraq qurğunun məhvini ehtiva edir. Bu yol ilə verilənlərin yaddaşdan silinməsi nəticəsində həmin verilənlərin geriye qaytarılması mümkünsüz olur [6].

III. VERİLƏNLƏRİN SANİTARİZASIYASI ALQORİTMLƏRİ HAQQINDA

VS – termini verilənlərin silinmə üsulu (ing. data erasure methods), silmə alqoritm (ing. wipe algorithms) və verilənlərin təmizlənmə üsulu (ing. data wipe methods) və ya verilənlərin silinməsi standartı (ing. data wipe standards) kimi də adlandırılır [8]. Aşağıda VS-nin icra alqoritməri haqqında məlumat verilir. Qeyd edək ki, bu alqoritmərin iş prinsipi demək olar ki, eynidir, yalnız keçidlərin təsvirində və sayında fərqlər vardır.

3.1. Təhlükəsiz silmə metodu (ing. Secure Erase Wipe Method) – bu metodun komandaları vasitəsilə sərt diskdə mövcud olan bütün məlumatların tamamilə yenidən yazılması mümkündür [9, 10]. Bu silmə metodunun alqoritm VS-ni aşağıdakı şəkildə icra edir:

- Keçid 1: ikilik ədəd yazır (sıfır və ya bir).

3.2. CSEC ITSG-06 verilənlərin silinmə metodu (ing. CSEC ITSG-06 Data Wipe Method) – bu metodun iş alqoritm başqa metodlardan bir qədər fərqlənir. Alqoritm icrası zamanı sıfır və təsadüfi verilənlər hər ikisi birlikdə istifadə edilir. Bu proses aşağıdakı şəkildə icra edilir [9, 10]:

- Keçid 1: bir və ya sıfır yazır;
- Keçid 2: əvvəlki keçiddə yazılmış simvolu tamamlayır (məs. bir əgər Keçid 1 sıfır olarsa);
- Keçid 3: təsadüfi verilən yazır və yazını yoxlayır.

3.3. NCSC-TG-025 verilənlərin silinmə metodu (ing. NCSC-TG-025 Data Wipe Method) – sərt disk və ya digər yaddaş qurğularının üzərinə mövcud informasiyanı yenidən yazmaq üçün bəzi fayl və verilənləri parçalama proqramlarında istifadə edilən VS metoduna əsaslanmış proqram təminatıdır [9, 10]. Bu metodun iş alqoritm *sıfır, bir və təsadüfi ədədlərin* kombinasiyası ilə aşağıdakı kimi göstərilir:

- Keçid 1: sıfır yazır və yazını yoxlayır;
- Keçid 2: bir yazır və yazını yoxlayır;
- Keçid 3: təsadüfi verilən yazır və yoxlayır.

3.4. Gutmann verilənlərin silinmə metodu (ing. Gutmann Data Wipe Method) – Gutmann metodu kimi tanınan təkrar-təkrar üzərinə məlumat yazmanı həyata keçirən Peter Gutmann və Colin Plumb tərəfindən 90-cı illərdə inkişaf etdirilən silmə metodu sənaye standartı olaraq qəbul edilmişdir. Bu metod 1996-cı ildə Peter Gutmann tərəfindən inkişaf etdirilmişdir [11]. Bu metodun icrası zamanı Peter Gutmann alqoritmindən istifadə etməklə sərt disk üzərində 35 dəfə üst-üstə məlumat yazmaqla əvvəlki veriləni silir. Bu etibarlı sanitizasiya metodlarından biri hesab olunur [9, 10]. Alqoritm aşağıdakı kimi icra olunur:

- Keçid 1 - 35: təsadüfi verilən yazır.

3.5. Schneier verilənlərin silinmə metodu (ing. Schneier Method Data Wipe Method) – bu metod dünyada kriptografiya üzrə tanınmış mütəxəssis Bryus Şnayer (Bruce Schneier) tərəfindən təklif olunmuşdur və təhlükəsizlik baxımından çox etibarlı metoddur. Həssas və konfidensial sayılan fayllarda istifadə olunur. Schneier metodu yeddi keçiddən ibarətdir [9, 10]:

- Keçid 1: bir yazır;
- Keçid 2: sıfır yazır;
- Keçid 3: bir qrup təsadüfi verilən yazır;
- Keçid 4: bir qrup təsadüfi verilən yazır;
- Keçid 5: bir qrup təsadüfi verilən yazır;
- Keçid 6: bir qrup təsadüfi verilən yazır;
- Keçid 7: bir qrup təsadüfi verilən yazır.

3.6. Pfizner verilənlərin silinmə metodu (ing. Pfizner Data

Wipe Method) – sərt disk və ya digər saxlama cihazlarından məlumatların silinməsi üçün Roy Pfitzner tərəfindən yaradılan proqram əsasında işləyən VS metodudur [8]. Bu metod sadə bir proseslə icra olunur. Hər hansı verilənin üzərinə 33-dəfə təsadüfi bir verilən yazmaqla sanitarizasiyanı yerinə yetirir [9, 10].

- Keçid 1 - 33: təsadüfi bir verilən yazır.

3.7. *Sıfır yazmaqla verilənlərin silinmə metodu* (ing. *Write Zero Data Wipe Method*) – sərt diskin və ya digər yaddaş qurğularının üzərinə sıfır yazmaqla proqram təminatı əsasında işləyən VS metodudur. Metod bəzən Sıfır doldurma və ya sıfır silmə olaraq da adlandırılır. Bu VS metodunun iş prinsipi aşağıdakı kimidir [9, 10].

- Keçid 1: sıfır yazır.

3.8. *Təsadüfi verilənlərin silinmə metodu* (ing. *Random Data Wipe Method*) – çox vaxt Random Number metodu kimi də tanınır. Sərt disk və ya digər saxlama cihazlarında VS-ni tətbiq etdikdə yalnız təsadüfi verilənlərdən istifadə olunur. Məlumdur ki, təsadüfi verilənlər gizlilik və təhlükəsizlik baxımından daha əhəmiyyətlidir [9,10]:

- Keçid 1-? Təsadüfi bir verilən yazır.

3.9. *DoD 5220.22-M verilənlərin silinmə metodu* (ing. *DoD 5220.22-M Data Wipe Method*) – metod Amerika Birləşmiş Ştatlarının Müdafiə Departamenti tərəfindən silinmə standartı olaraq qəbul edilmişdir. DOD 5220.22-M silmə metodu VS-ni aşağıdakı şəkildə verilmiş alqoritmik ardıcılıqla yerinə yetirir [9,10].

- Keçid 1: sıfır yazır və yazını yoxlayır;
- Keçid 2: bir yazır və yazını yoxlayır;
- Keçid 3: təsadüfi verilən yazır və yazını yoxlayır.

3.10. *AFSSI-5020 verilənlərin silinmə metodu* (ing. *AFSSI-5020 Data Wipe Method*) – Amerika Birləşmiş Ştatları Hava Qüvvələri (USAF) tərəfindən təsis edilmişdir. Amerika Birləşmiş Ştatları Hava Qüvvələri (USAF) indi də VS-nin bu metodundan təhlükəsizlik standartı kimi istifadə edir. AFSSI-5020 verilənlərin silinmə metodu aşağıdakı şəkildə həyata keçirilir. Əvvəlcə bir, sonra sıfır yazıldığı hallar mümkündür və hər bir keçid yoxlanılır [9,10].

- Keçid 1: sıfır yazır;
- Keçid 2: bir yazır;
- Keçid 3: təsadüfi verilən yazır və yazını yoxlayır.

3.11. *AR 380-19 verilənlərin silinmə metodu* (ing. *AR 380-19 Data Wipe Method*) – İlk dəfə ABŞ ordusu tərəfindən yayımlanan Army Regulation 380-19 (Ordu Tənzimlənməsi 380-19) nəşri tərəfindən istifadə edilmişdir. Hazırda həmin təşkilat bu metodu təhlükəsizlik standartı kimi istifadə edir [9,10]. Alqoritmin icrası aşağıdakı kimidir:

- Keçid 1: təsadüfi verilən yazır;
- Keçid 2: xüsusi simvol yazır (məs., sıfır);
- Keçid 3: xüsusi simvolu tam olaraq yazır və yazını yoxlayır.

3.12. *NAVSO P-5239-26 verilənlərin silinmə metodu* (ing. *NAVSO P-5239-26 Data Wipe Method*) – hazırda ABŞ Hərbi Dəniz qüvvələri NAVSO P-5239-26 metodundan sanitarizasiya standartı kimi istifadə edir. Bu metod sərt disk və ya digər yaddaş qurğularına mövcud informasiyanı yenidən yazmaq üçün müxtəlif fayl və verilənləri parçalama proqramlarından istifadə edilən VS metoduna əsaslanmış proqram təminatıdır. NAVSO P-5239-26 metodu silmə işini aşağıdakı kimi həyata keçirir [7]:

- Keçid 1: xüsusi simvol yazır (məs., “bir”);
- Keçid 2: xüsusi simvolun ardını yazır (məs., “sıfır”);
- Keçid 3: təsadüfi veriləni tam olaraq yazır və yazını yoxlayır.

3.13. *HMG IS5 (Infosec Standard 5) verilənlərin silinmə metodu* (ing. *HMG IS5 (Infosec Standard 5) Data Wipe Method*) – bu metoddan istifadə etməklə sərt diskin silinməsi, proqram təminatına əsaslanan bütün faylbərpa metodlarının diskdə olan informasiyanı tapmasının qarşısını alır. Bir çox aparat təminatına əsaslanan faylbərpa metodları vasitəsilə isə informasiyanı aşkarlamasına mane olur. HMG IS5 metodunun eyni zamanda HMG IS5 Baseline və həm HMG IS5 Enhanced kimi iki oxşar versiyalarına da rast gəlmək olur. HMG IS5 Baseline VS metodu aşağıdakı şəkildə işləyir [9,10]:

- Keçid 1: sıfır yazır;
- Keçid 2: təsadüfi verilən yazır və yazını yoxlayır.

HMG IS5 Enhanced metodu isə aşağıdakı kimi işləyir:

- Keçid 1: sıfır yazır;
- Keçid 2: bir yazır;
- Keçid 3: təsadüfi verilən yazır və yazını yoxlayır.

3.14. *ISM 6.2.92 verilənlərin silinmə metodu* (ing. *ISM 6.2.92 Data Wipe Method*) – sərt disk və ya digər yaddaş qurğularına mövcud informasiyanı yenidən yazmaq üçün müxtəlif fayl və verilənləri parçalama proqramlarında istifadə edilən VS metoduna əsaslanmış proqram təminatıdır. ISM 6.2.92 metodu aşağıdakı alqoritmə təmizləmə işini həyata keçirir [7].

- Keçid 1: təsadüfi simvol yazır və yazını yoxlayır.

3.15. *NZSIT 402 (401) verilənlərin silinmə metodu* (ing. *NZSIT 402 (401) Data Wipe Method*) – Yeni Zelandiya hökuməti və hökumətə xidmət edən istənilən təchizatçı yaxud məsləhətçilər tərəfindən standart silmə metodu kimi istifadə edilir. NZSIT 402 metodu aşağıdakı alqoritmə ilə işləyir [9, 10]:

- Keçid 1: təsadüfi bir verilən yazır və yazını verifikasiya edir.

3.16. *VSITR verilənlərin silinmə metodu (ing. VSITR Data Wipe Method)* – bu metod Almaniya Federativ Respublikasının təhlükəsizlik standartı kimi qəbul edilmişdir. Alqoritmin icrası aşağıdakı kimidir [12,13]:

- Keçid 1: sıfır yazır;
- Keçid 2: bir yazır;
- Keçid 3: sıfır yazır;
- Keçid 4: bir yazır;
- Keçid 5: sıfır yazır;
- Keçid 6: bir yazır;
- Keçid 7: təsadüfi bir verilən yazır.

3.17. *GOST R 50739-95 verilənlərin silinmə metodu (ing. GOST R 50739-95 Data Wipe Method)* – Rusiya Federasiyasının təhlükəsizlik üzrə dövlət standartı kimi 01.01.1996- cı ildə təsis edilmişdir [9, 10]. GOST R 50739-95 metodu çox vaxt səhvən GOST p50739-95 adı ilə adlandırılır. Bu metodun alqoritmi aşağıdakı kimidir:

- Keçid 1: sıfır yazır;
- Keçid 2: təsadüfi verilən yazır;
- Keçid 1: təsadüfi verilən yazır.

3.18. *RCMP TSSIT OPS-II verilənlərin silinmə metodu (ing. RCMP TSSIT OPS-II Data Wipe Method)* – bütün məzmunu silmək üçün Kanada təhlükəsizlik üzrə təmizləmə üsuludur. Alqoritm aşağıdakı kimi icra olunur [9,10]:

- Keçid 1: sıfır yazır;
- Keçid 2: bir yazır;
- Keçid 3: sıfır yazır;
- Keçid 4: bir yazır;
- Keçid 5: sıfır yazır;
- Keçid 6: bir yazır;
- Keçid 7: təsadüfi verilən yazır və təsdiqləyir;

NƏTİCƏ

Məlumatların sanitarizasiyası inkişaf etməkdə olan tədqiqat sahəsi olduğundan burada bir sıra problemlər vardır. Əsas problemlərdən biri də gizlilik, təhlükəsizlik tədbirlərinin daha geniş və səmərəli yerinə yetirilməsində müəyyən xətəların olmasıdır. Məlumatın strukturunda dəyişikliklər etdikdə, yeni informasiya sisteminə keçdikdə və ya məlumatın birdən çox məlumat mənbəyinə integrasiya edilməsi zamanı informasiya auditoriyaya fərqli formada təqdim oluna bilər. Yaranmış problemlərin həlli məlumatların strukturunda, təqdimatında və ya məzmununda hər hansı dəyişikliklərin edilməsi ilə yanaşı, onların təhlükəsizliyi məsələsini də təmin etməlidir.

VS metodlarının tətbiqi ilə uşaqları İnternetdə mövcud olan qanunazidd və təhlükəli kontentdən qorumaq üçün müxtəlif mexanizmlər işlənilməlidir.

ƏDƏBİYYAT

- [1] Vasudevan V., John A., A review on text sanitization, International journal of computer applications (0975 – 8887), 2014, vol. 95, no.25, pp. 14-17.
- [2] Əliquliyev R.M. Ocaqverdiyeva S.S. Uşaqların İnternetdə informasiya təhlükəsizliyini təmin edən sistemin konseptual modeli / İnformasiya təhlükəsizliyinin aktual problemləri III respublika elmi-praktiki seminarı, Bakı, 2017, səh. 84-87.
- [3] Nettleton D.F., Abril D., An information retrieval approach to document sanitization, Advanced Research in Data Privacy, 2015, pp. 151-166.
- [4] Crawford R., Bishop M., Bhumiratana B., Clark L., Levitt K. Sanitization Models and their Limitations / Proceedings of the 2006 Workshop on New Security Paradigms, Germany, 2006, pp. 41-56.
- [5] Chakaravarthy V.T., Gupta H., Roy P., Mohania M. Efficient techniques for document sanitization / In Proceeding of the 17th ACM Conference on Information and Knowledge Mining (CIKM), 2008, pp. 843-852.
- [6] Ivascu M. Data erasure on magnetic storage media / International conference of scientific paper afases, Brasov, 2011, pp. 614-617.
- [7] Deepika C., Bansal Dr. P. Study on need of data sanitization and sanitization techniques for memory devices/Open Access Journals Search Engine (OAJSE), vol.2, 2017, pp. 2456-3293
- [8] Fisher T. Data Sanitization Methods, A List of Software Based Data Sanitization Methods, <https://www.lifewire.com/data-sanitization-methods>
- [9] Kara Nance and Daniel J. Ryan. Proceedings of the 44th Hawaii International Conference on System Sciences - 2011 “Legal aspect of digital forensics” available at www.computer.org/csdl/proceedings/hicss/2011/4282/00/10-04-03.pdf access on 24/12/2015.
- [10] “Degaussing” available at www.techtarget.com access on /24/6/2016. “Sanitization methods” available at <http://googleweblight.com> access on 15/7/2016.
- [11] Gutmann metodu (35 kez silme) nedir?, www.dijitaldeliller.com
- [12] Fisher T. VSITR Data Wipe Method [German Wipe Standard; 7 Passes], www.computercardinal.com, 26.04.2017
- [13] Standard vom Bundesamt für Sicherheit in der Informationstechnik (bsi-vsit), <https://dg-datenschutz.de>

DATA SANITIZATION – AS PROVIDING INFORMATION SECURITY

Sabira Ojagverdiyeva

Institute of Information Technologies of ANAS, Baku, Azerbaijan

allahverdiyevsabira@gmail.com

Abstract – The article provides information about the essence and categories of data sanitization. Algorithms for the sanitization of data were analyzed. The role of ensuring the confidentiality of sensitive data and providing children security on the Internet is shown.

Keywords – Data sanitization, sanitization algorithms, safety, children safety

- **Test keysin təsviri** (*Test Case Description*) sistemin qoyulan tələbləri yerinə yetirdiyinə əmin olmaq üçün onun bir vəziyyətdən digərinə keçirən fəaliyyət növlərinin siyahısıdır;
- **Son şərtlər** (*Post Conditions*) Sistemi sınaqdan əvvəlki başlanğıc vəziyyətə qaytarmaq üçün lazım olan işlərin siyahısıdır.

Test keyslər gözlənilən nəticədən asılı olaraq müsbət və mənfi test keyslərə bölünür:

- **Müsbət test- keys** yalnız düzgün verilənlərdən istifadə etməklə proqramın tələb olunan funksiyanı düzgün yerinə yetirməsini yoxlayır;
- **Mənfi test- keys** həm düzgün, həm də yanlış verilənlərlə (ən azı 1 yanlış parametrlə) işləyir və proqramda baş verəcək xüsusi halları yoxlayır.

Testin planı sınağa aid bütün işlərin (obyektin təsvir edilməsi, strategiyalar, başlama və sona çatma meyarlarından başlayaraq iş müddətində lazım olan avadanlıqlara, xüsusi biliklərə və risklərin qiymətləndirilməsinə qədər) təsvir edilməsi üçün sənəddir.

Testin dizaynı PT-nin sınaq mərhələsindən biridir. Burada əvvəlcədən müəyyən edilmiş keyfiyyət meyarlarına və sınağın məqsədinə uyğun olaraq test keyslər layihələndirilir və yaradılır. Testin dizaynı test analitiki və test dizayneri tərəfindən həyata keçirilir:

- test analitiki müəyyən edir ki, “Nəyi yoxlamaq lazımdır?”;
- test dizayneri müəyyən edir ki, “Necə yoxlamaq lazımdır?”.

Çek-list (*check list*) — nəyin sınaqdan keçiriləcəyini təsvir edən sənəddir. Adətən burada ancaq fəaliyyət növləri göstərilir, gözlənilən nəticələr qeyd edilmir.

Səhvlər haqqında hesabat (*Bug Report*) —sınaqdan keçirilən obyektin xətalı işləməsinə səbəb olan halları (səbəbləri və gözlənilən nəticələri göstərməklə) özündə əks etdirir [3].

PT-nin sınağının aparılması üçün müxtəlif sınaq metodları işlənmişdir. Bu metodlar yoxlanılan elementlərin səviyyəsinə və miqyasına və məqsədinə görə sınaq metodlarına bölünür. (şəkil 2).

Qeyri-funksional sınaq metodlarına aid olan təhlükəsizliyin sınağı PT-nin müxtəlif hücumlara qarşı davamlılığını yoxlayır, sistemdə olan mühafizə mexanizmlərinin fəaliyyətinin pozulmasına cəhd edilir [4]. Əgər sınaq zamanı PT bütün təhdidlərə qarşı davamlılığını qoruyarsa sınaq çətinləşir.

Hal-hazırda mövcud olan sınaq metodları bütün səhvləri aşkar etməyə imkan vermir. PT-nin sınağı və verifikasiyası məsələsini həll etmək üçün müxtəlif yanaşmalar var, lakin bu proseslər yaradıcı proses olduğundan onların həyata keçirilməsi üçün dəqiq qaydalar yoxdur. Sınaq metodları ilə yanaşı bəzi sınaq prinsipləri də mövcuddur. PT-nin son 40 ildə işlənilmə

təcrübəsinə əsaslanaraq sınaq prosesinin prinsipləri işlənilmişdir.

Şəkil 2. PT-nin sınaq metodları

III. PROQRAM TƏMİNATININ SINAĞI PRİNSİPLƏRİ

Aşağıda PT-nin sınaq prinsipləri verilmişdir [5, 6]:

Prinsip 1: Sınaq prosesinə başlamazdan əvvəl gözlənilən nəticə müəyyən edilməlidir.

PT-nin sınağına başlamazdan əvvəl gözlənilən nəticələr müəyyən edilir. Əgər gözlənilən nəticə öncədən təyin edilməzsə, o zaman inandırıcı görünən amma doğru olmayan nəticəni doğru kimi qəbul etmək təhlükəsi yaranır. Bundan əlavə əgər gözlənilən nəticələr öncədən yazılı şəkildə qeyd edilərsə, o zaman vaxt aparan müzakirələrdən də qaçmaq olar. Bu prinsipi nəzərdən qaçırdıqda sınaq prosesində çoxlu səhvlər ola bilər.

Bu səbəbdən test-keys özündə 2 komponenti saxlamalıdır:

- giriş verilənlərinin təsviri;
- göstərilmiş giriş verilənlərinə müvafiq olan düzgün çıxış verilənlərinin dəqiq təsviri;

Prinsip 2: Proqramçı heç vaxt öz proqramını sınaqdan keçirməməlidir.

Bu prinsip heç də o demək deyildir ki, proqramçıya öz proqramını test etməyə icazə verilmir. Proqramçıların çoxu öz proqramlarını səmərəli şəkildə sınaqdan keçirə bilmir, çünki fikrini səhvləri aşkar etməyə yönəldə bilmir. Həmkarlar, rəhbərlik, müştəri və ya sahibkarlar tərəfindən cəza qorxusu onun səhvlərdən qaçmasına gətirib çıxarır. Proqramçının

qoyulmuş məsələni və sənədləşməni düzgün başa düşməməsindən irəli gələn proqram səhvləri də ola bilər. Onda o, öz proqramını sınaqdan keçirəndə də bu anlaşılmazlıqdan meydana gələn səhvləri tapa bilməyəcəkdir. Ona görə də sınaq başqa mütəxəssislər tərəfindən daha səmərəli həyata keçirilir.

Prinsip 3: PT-ni işləyən təşkilatlar öz proqramlarını sınaqdan keçirməməlidir.

Təşkilatın və ya onun menecerinin işini PT-ni müəyyən olunmuş vaxt və büdcə vəsaitləri çərçivəsində hazırlamaq qabiliyyəti ilə qiymətləndirirlər. Ona görə ki, bu parametrlər əsasən qiymətləndirmə PT-nin keyfiyyətinin qiymətləndirilməsindən asandır. Bu səbəbdən də PT-ni işləyən təşkilatın səmərəli sınaq proseslərinin keçirilməsində marağı olmur, verilən iş qrafiki və xərclər daxilində sınağın keçirilməsinə çalışırlar.

Prinsip 4: Testlərin nəticələri əsaslı şəkildə dəqiq tədqiq və təhlil edilməlidir.

Bəzi hallarda əvvəlki testin nəticələrində səhvlərin olduğu nəzərdən qaça bilər. Mümkün olduğu qədər səhvləri proqram təminatının yaradılmasının ilkin mərhələlərində aşkar etmək lazımdır. Əgər səhvlər sonrakı mərhələlərdə ortaya çıxarsa yerini müəyyənləşdirmək və aradan qaldırmaq çox çətin olar. Proqramçıların çoxu öz proqramları ilə ehtisablaşdırırlar ki, onlar nəticələrdəki detalları gözədən qaçırmırlar. Bəzən bu səhvlər bir hərf səhvindən də irəli gələ bilər.

Prinsip 5: Test-keyslər həm düzgün və gözlənilən giriş verilənləri, həm də xətalı və gözlənilməyən giriş verilənləri üçün tərtib olunmalıdır.

Bu o deməkdir ki, ekstremal şərtlərdə PT-nin fəaliyyəti təhlil edilməlidir. İstifadəçinin məhsul ilə işləyəcəyi bütün ssenariləri müəyyən etmək mümkün deyil. Bəzi hallarda sınağın xətalı və gözlənilməyən giriş verilənləri ilə aparılması ən ciddi və təhlükəli səhvlərdən vaxtında qaçmağa imkan verir.

Prinsip 6: Bir proqramın tələblərdə göstərilən hansı məsələni icra etmədiyini müəyyənləşdirmək məqsədi ilə aparılan araşdırmalar hələ işin yarısı deməkdir.

Digər yarısı isə proqramın icra etməməli olduğu hansı məsələləri yerinə yetirdiyini aydınlaşdırmaqdan ibarətdir. Əgər proqram icra etməməsi lazım olan işləri də edərsə o da səhv sayılır.

Prinsip 7: Bir dəfə istifadə edilən test-keysləri ancaq bir dəfəlik tətbiq edilən (təkmilləşdirilməyən) proqramlar üçün hazırlamaq olar.

Məsələ ondadır ki, test-keyslərin işlənilməsi üçün vaxt və vəsait lazımdır. Əgər sınaq prosesi bitdikdən sonra onlar itirilərsə PT-nin təkrar sınağı lazım gəldikdə test-keyslər yenidən işlənilməlidir. Bu əlavə iş deməkdir və bəzi hallarda yenidən işlənilmiş test-keyslər PT-də olan səhvləri tapa bilmir. Bu problem bir çox proqramların sınağı zamanı müxtəlif sistemlərdə meydana gələ bilər.

Prinsip 8: Sınaq prosesinə “səhv tapılmayacaq” fikri ilə başlamaq olmaz.

Layihə menecerlərinin ən çox etdiyi səhvlərdən biridir. Bəzi hallarda sınaq prosesi PT-nin düzgün işlədiyini nümayiş etdirmək məqsədi daşıyır, əslində isə prosesə başlayarkən məqsəd qoyulmalıdır ki, səhvlər tapılacaq. Çünki tamamilə səhvi olmayan PT-ni işləmək mümkün deyildir. Hətta keyfiyyətli sınaq prosesindən sonra belə PT-də səhvlərin olduğu güman edilir, sadəcə olaraq onlar hələ tapılmamışdır.

Prinsip 9: PT-nin müəyyən hissəsində səhvlərin olması ehtimalı bu hissədə tapılan səhvlərin sayına mütənasibdir.

Proqram kodunun müəyyən bir seqmentində səhvlər artıq aşkar edilibsə onların yaxın ətrafında digər səhvlərin tapılma ehtimalı daha yüksəkdir. Məsələn, A və B modulları var və PT-ni sınaqdan keçirən 20 səhv A modulunda və 3 səhv B-də aşkar etmişdir. Bu halda demək olar ki, digər səhvlər də B moduluna nisbətən A modulunda daha çox olacaq. PT-nin keyfiyyətinin təyin edilməsi üçün mövcud olan riyazi modellər moduldakı məlum olan səhvlər əsasında qalan səhvləri hesablamağa imkan verir. Bu ehtimal onu göstərir ki, proqram kodunun hər hansı hissəsində səhvlər digərlərinə nisbətən daha çox tapılırsa bu hissənin sınağını bir qədər çox aparmaq lazımdır.

Prinsip 10: PT-nin sınağı mütəxəssisin yaradıcı və intellektual qabiliyyətlərini nümayiş etdirir.

PT-nin sınağı üzrə mütəxəssislərin işi tapılan səhvlərin sayına görə qiymətləndirilir. Sınağı keçirənlər indiyə qədər aşkar edilməyən səhvləri tapmağa imkan verən yaxşı test-keys hazırlamalıdırlar. Belə test-keyslərin tərtib edilməsi PT-nin işlənilmə prosesinə nisbətən daha çox yaradıcı və intellektual qabiliyyət tələb edir.

İstənilən PT-nin sınağı zamanı istifadə ediləcək sınaq metodları ilə yanaşı sınaq prinsiplərinə də diqqət yetirilməsi vacib şərtlərdən biridir.

NƏTİCƏ

Yuxarıda göstərilən prinsiplərə əsasən belə bir nəticəyə gəlmək olar ki, PT-nin sınağının müvəffəqiyyətlə aparılması üçün aşağıdakılara diqqət yetirmək lazımdır:

- Səhvləri aşkar etmək ehtimalı yüksək olan test yaxşı hesab olunur;
- Sınağı ən bacarıqlı proqramçılar aparmalıdır;
- Sınaq işlənilən proqramın əsas məsələsi kimi nəzərdən keçirilməlidir;
- Sınağı asanlaşdırmaq üçün proqramı dəyişmək lazım deyil;
- Hər hansı bir başqa fəaliyyət kimi sınaq da məsələnin qoyuluşu ilə başlamalıdır, yoxlanılacaq funksiyalar və gözlənilən nəticələr test-keyslərdə göstərilməlidir.

İnformasiya texnologiyalarının vacibliyinin artması ilə PT-də olan səhvlərin cəmiyyətin həyatında vurduğu ziyanın da qiyməti artır. PT-də olan səhvləri vaxtında aşkar edib düzəltməyə imkan verən sınaq metodları və texnologiyaları ön plana çıxır. Hal-hazırda PT-nin etibarlılığının və

təhlükəsizliyinin yüksəldilməsi üçün çoxlu sayda sınaq metodları işlənmişdir. Keyfiyyətli PT -nin olması şirkətin etibarlı fəaliyyətini təmin edir. Elə bu səbəbdən də PT-nin keyfiyyətinin yüksəldilməsi üçün sınaq məsələlərinə xüsusi diqqət yetirilməlidir. Eyni zamanda “Proqram mühəndisliyi” üzrə yüksək ixtisaslı kadrların hazırlanmasında da PT-nin sınaq metodları və vasitələrinin tədrisi böyük əhəmiyyətə malikdir.

ƏDƏBİYYAT

- [1] Verifikation, Validation und Testen von Sicherheitskritischen Systemen, http://pi.informatik.uni-siegen.de/niere/lehre/SS04/SeminarFinal/5_jaya/Ausarbeitung.pdf
- [2] Орлов С.А. Программная инженерия: технология разработки программного обеспечения, 5-е изд. «Питер», 2017, 634
- [3] С. Макконнелл, Совершенный код. М: Русская редакция, 2005, 896с.
- [4] Полевщиков И.С. Особенности изучения способа тестирования базового пути студентами бакалавриата в рамках дисциплины

«Тестирование программного обеспечения» (часть 1) // Молодой ученый. 2015. №18. С. 10 – 12

- [5] Майерс Г. Искусство тестирования программ. Пер. с англ. под ред. Б.А. Позина. М.: Финансы и статистика, 1982, 176 с.
- [6] Дженнифер Коул, Томас Горэм и др. Принципы тестирования программного обеспечения (ПО), <http://www.gcmsite.ru/?pg=art&id=software-testing>

THE ANALYSIS OF TEST PRINCIPLES OF SOFTWARE

Tamilla Bayramova¹, Nazakat Malikova²

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

¹toma_b66@mail.ru, ²naranara_68@mail.ru

Abstract— Information about the terms used in the testing process of software, tools used for testing and different methods is given in the article. The principles of testing are analyzed and the importance of considering them in the testing process is emphasized here.

Key words— software engineering; test principles; test-case; test plan; test design.

Qloballaşma şəraitində dilin inkişaf tendensiyaları və təhlükəsizliyi

Səyyar Abdullayev¹, Tofiq Kazımov², Südabə Abasova³
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹sayyar.abdullayev@yandex.ru, ²tofig@mail.ru, ³abasova.sudaba@gmail.com,

Xülasə – Məqalədə qloballaşan dünyada dil təhlükəsizliyi anlayışına milli təhlükəsizlik, informasiya təhlükəsizliyi, linqvistik suverenlik və dil siyasəti problemləri kontekstində baxılır. Qloballaşma şəraitində dilin inkişaf tendensiyasına təsir edən amillər, onun milli saflığının qorunmasında terminlərin rolu və təhlükəsizliyinin təmin olunması məsələləri araşdırılmışdır.

Açar sözlər – dil təhlükəsizliyi; qloballaşma; terminografiya; linqvistik suverenlik; sosiolingvistika

I. GİRİŞ

Azərbaycan dili qədim tarixi köklərə malikdir. Ümummilli lider Heydər Əliyevin 9 avqust 2001-ci il tarixdə imzaladığı “Dövlət dilinin tətbiqi işinin təkmilləşdirilməsi haqqında” fərmanda deyilir: “Azərbaycan dili bu gün dərin fikirləri ən incə çalarlarınadək olduqca aydın şəkildə ifadə etmək qüdrətinə malik dillərdəndir. Düşüncələrdəki dərinliyi, hisslərdəki incəlikləri bütünlüklə ifadə etmək kamilliyinə yetişə bilməsi üçün hər hansı xalqda bir neçə minillik tarixi yaşaması lazım gəlir. Azərbaycan dilinin bugünkü inkişaf səviyyəsi göstərir ki, Azərbaycan xalqı dünyanın ən qədim xalqlarındandır”. Böyük uzaqgörənliklə imzalanan bu tarixi fərmana əsasən hər il avqust ayının 1-i Azərbaycan Əlifbası və Azərbaycan dili günü kimi qeyd edilir.

Müasir dünyada gedən qloballaşma prosesləri Azərbaycana da öz təsirini göstərməkdədir. Milli varlığımız sayılan dilimizin təmizliyini, orijinallığını qoruyub saxlamaq, onun təbii inkişafına mane olan mənfi amillərin təsirini minimuma endirmək, dünya dilləri sırasında onun nüfuzunu yüksəltmək hamımızın müqəddəs vənədaşlıq borcudur. Ölkəmizdə Azərbaycan dilinin hərtərəfli inkişafı, işlək dilə çevrilməsi, beynəlxalq münasibətlər sisteminə yol tapması Ana dilimizin gözəl bilicisi, mahir natiq ulu öndər Heydər Əliyevin dilin qorunmasına yönələn düşünlü müəssisəsinin nəticəsidir. Yeni ictimai-siyasi görüşlər, elm və mədəniyyətin sürətli inkişafı, orta və ali məktəblərin, elmi-tədqiqat müəssisələrinin təşkili, mətbuatın sayının artması, dərslərin, elmi əsərlərin Azərbaycan dilində yazılması dilin ictimai funksiyasının genişlənməsinə təkan vermişdir. 1995-ci ildə ümumxalq səsverməsi yolu ilə qəbul edilən müstəqil dövlətimizin ilk Konstitusiyası ilə dövlət dilinin adı bərpa edildi. Bu, ulu öndərin Ana dilimizə dəyişməz mövqeyinin daha bir parlaq nümunəsi oldu.

Azərbaycan əlifbası XX əsrdə üç dəfə dəyişdirilmişdir. Azərbaycan dilində yazı 1929-cu ilə kimi ərəb qrafikası ilə aparılmışdır. 1922-1939-cu illərdə latın qrafikalı əlifba üzrə (1929-cu ilə kimi ərəb əlifbası ilə paralel olaraq), 1939-1991-ci illərdə kiril qrafikası üzrə, 1991-ci ildən başlayaraq yenidən latın qrafikası üzrə aparılmışdır. Təbii ki, bu ədəbi, elmi dilimizin və onun terminoloji bazasının, ümumiyyətlə dilimizin inkişafına neqativ təsirlərini göstərir.

II. QLOBALLAŞMADA DİLİN İNKİŞAFINA TƏSİR EDƏN AMİLLƏR

Qloballaşma şəraitində millətlərin milli varlığının aqibəti baxımından, dilin inkişaf perspektivlərinin prinsipial aspektləri və bu inkişafa təsir edən amillər aşağıdakı kimi təyin olunur.

Qloballaşma prosesi cəmiyyətin və insan fəaliyyətinin bütün sahələrinə nüfuz etməkdədir. Bu davamlı proses həm müsbət, həm də mənfi təsir xüsusiyyətlərinə malik olmaqla müxtəlif inkişaf səviyyəli ölkələrdə fərqlidir.

Geniş miqyaslı, hərtərəfli və ziddiyyətli xarakterinə görə qloballaşma dünya xalqlarında dil və mədəniyyət, adət və ənənələrin itirilməsi təhlükəsini yaradır. Qloballaşma subyektlərinin qarşılıqlı münasibətlərinə müasir informasiya – kommunikasiya vasitələri, xüsusilə İnternet geniş müdaxilə edir. Qloballaşma həm də millətlərin yaxınlaşması və bir-birinin həyat tərzini götürərək ona oxşamasıdır. Bu zaman milli mədəniyyətlərin inkişafı və onların spesifikliyinin qorunması məsələləri xüsusi diqqət mərkəzində olmalıdır.

Qlobal kommunikasiya sistemləri dünyanın bir sıra ölkələrində özünü dil ekspansiyasının ötürücüsü kimi də göstərir. Ona görə də qlobal tendensiyaların dilə neqativ təsirlərini minimuma endirmək məqsədilə konseptual xarakterli kompleks tədbirlərə ehtiyac vardır.

Alimlərin proqnozuna görə, qlobal kommunikasiya sistemlərinin köməyi ilə milli dillərin “çirklənməsi” və bir-birinə nüfuz etməsi nəticəsində mədəniyyətə kobud davranış, ünsiyyət formaları, cahillik, pis vərdiş və yad dəb elementləri aşılır. Hər bir canlı dilin arxasında onun ifadə zənginliyinin əks etdirən mədəniyyət durur.

Müasir dövrdə qarşımızda həm ümumelmi, həm ümumsosial və həm də fəlsəfi əhəmiyyətə malik nəhəng bir problem durur. Belə ki, son onillikdə qlobal kommunikasiya

sistemlərinin təsiri altında bir çox Azərbaycan sözləri kütləvi informasiya vasitələrində, danışq dilində, dövlət sənədlərində və s. yabancı sözlərlə əvəz olunmuşdur.

YUNESKO-nun baş konfransının qəbul etdiyi “Çoxdilliliyin inkifafı, istifadə olunması və kiberfəzaya ümumi çıxış haqqında tövsiyə” adlı sənəddə deyilir: Təşkilatlara üzv ölkələr dilin, xüsusilə ana dilinin kiberfəzada tədrisinə yardım etməklə, son dərəcə vacib bir məsələ olan dilin kiberfəzadan sıxışdırılıb çıxarılması üçün fəal milli siyasət işləyib hazırlamalıdır [1].

III. DİLİN İNKİŞAFINDA TERMİNLƏRİN ROLU

Qloballaşma dövründə terminologiya elmi sürətli inkişaf dövrünü yaşayır. Bu hər şeydən əvvəl, onunla bağlıdır ki, indi elmi-texniki tərəqqi müasir cəmiyyətin hərəkətverici qüvvələrindən biridir. Ona görə də cəmiyyətdə, ictimai həyatda, elmi-texniki tərəqqidə baş verən hər bir hadisə və elmi yeniliklər dildə öz əksini tapır.

Beləliklə, cəmiyyətdə insanlar arasında ünsiyyətin əsas forması kimi çıxış edən dil, bu cəmiyyətin müxtəlif sosial qruplarının təsirinə məruz qalaraq zənginləşir. Bununla da dilin lüğət tərkibinin ən çevik hissəsi olan terminologiyada daim inkişaf prosesi gedir. Qeyd etmək lazımdır ki, hər bir elm sahəsi üç əsas anlayış sistemindən:

- onun məzmununu təşkil edən, özündə əks etdirən bir çox faktların toplusundan;
- onun nəticəsində meydana çıxan təsəvvürlərdən;
- bu təsəvvürlərin ifadə olunduğu terminlərdən təşkil olunur [2]. Elmi biliklərin, ayrı-ayrı elm sahələrinin inkişafında dil təsadüfi funksiya daşımır, dil hər bir elmin struktur elementlərindən biri kimi meydana çıxır. Deməli, elmi dil vahidləri məhz terminologiya vasitəsilə elmə daxil olur.

Hazırkı informasiya mübadiləsi prosesinin ifrat sürətliliyi dil vahidlərinin terminologiya vasitəsilə elmə daxil olmasına mane olur. Buna görə də, terminologiyada baş verən proseslərdən ən əsası yeni terminlərin yaranması və onların dünya dillərində yer almasıdır. Müasir dövr terminologiyasında termin yaradıcılığı daha çox beynəlxalq dil istiqamətində inkişaf etməsi ilə səciyyələnir. Məsələn, yeni terminlərin yaranmasında ingilis dilinin aparıcı mövqeyə malik olması danılmazdır. Dilin dominantlığını şərtləndirən əsas cəhət elmi fikirlərin, məlumatların bu dildə yazılması və yayılmasıdır. İnternet xidmətindən istifadə yeni anlayışlara uyğun terminlərin İnternet vasitəsi ilə ingilis dilindən götürülməsinə şərait yaradır. Tədqiqatçılar yeni terminlərdən istifadəyə fərqli şəkildə yanaşırlar. Belə ki, bəziləri terminlərin öz dillərində qarşılığını axtarıb tapmağa səy edir, dilin öz vasitələrindən istifadə etməklə yeni termin yaratmağa çalışır, digər qismi alınma terminlərə, başqa qismi isə kalka üsulu (*kalkaetmə, qeyri dillərdən tərcümə prosesi*) ilə termin yaradıcılığına üstünlük verir. Bu problemlər ayrı-ayrı elm sahələri ilə bağlı terminoloji mərkəzlərin yaranmasını zəruri edir [2].

Hal-hazırda qloballaşan dünyanın yeni çağırışları şəraitində elmi-texniki tərəqqinin və termin yaratmanın sürətli inkişafı xüsusi əhəmiyyət kəsb edir. Azərbaycan da bu prosesin

müəyyən neqativ təsirlərinin qarşısını almaqla milli dilin təmizliyini qorumağa cəhd edir. Hazırda dünyada 20 mindən çox terminoloji standart mövcuddur. Onların əsas hissəsi inkişaf etmiş sənaye ölkələrində yaradılmış milli standartlardır. Azərbaycan dilinin funksional imkanlarının inkişafı istiqamətində məqsədyönlü dövlət siyasəti həyata keçirilmiş, bu dil dövlət və cəmiyyət həyatının bütün sahələrində geniş istifadə edilir. Azərbaycan dilinin leksik sistemində terminlər xüsusi əhəmiyyətə malik olmaqla bir çox hallarda onlara ümumişlək sözlərdən daha çox ehtiyac duyulur. Elm və texikanın bütün sahələrində terminlər informasiya və bilik əldə etmək üçün xüsusi əhəmiyyət daşıyır. Terminologiyayı dərindən mənimsəmədən hər hansı elm sahəsində uğur əldə etmək qeyri-mümkündür [3].

Qeyd edək ki, qloballaşma şəraitində terminologiya strateji resurs olmaqla ölkənin inkişafında vacib rol oynayır. Ölkə vətəndaşlarının səmərəli iqtisadi, texniki və elmi ünsiyyət bacarıqları düzgün və standartlaşdırılmış terminologiyadan istifadə ilə inkişaf etdirilir. İstənilən ölkənin terminologiya təcrübəsi müxtəlif sahələrdə ünsiyyəti genişləndirir və rəsmi dilin funksional dil imkanlarını genişləndirir.

Azərbaycan Respublikası Prezidentinin 23 may 2012-ci il tarixli Sərəncamı ilə AR Nazirlər Kabineti yanında Terminologiya Komissiyasının yaradılması terminologiya fəaliyyətinə olan məsuliyyəti daha da artırdı. Belə ki, Terminologiya Komissiyası təkcə respublikada deyil, respublikadan kənarda da Azərbaycan dilinin qorunması istiqamətində mühüm işlərin həyata keçirilməsinə təkan verdi [4].

Azərbaycan Respublikası Prezidenti İlham Əliyevin 9 aprel 2013-cü il tarixli Sərəncamı ilə təsdiq olunmuş “Azərbaycan dilinin qloballaşma şəraitində zamanın tələblərinə uyğun istifadəsinə və ölkədə dilçiliyin inkişafına dair Dövlət Proqramı”nda müvafiq qurumlar qarşısında mühüm vəzifələr qoyulmuşdur. Azərbaycan dilinin öyrənilməsi və təbliği sahəsində informasiya-kommunikasiya texnologiyalarının (İKT) tətbiqi ilə bağlı müddəalarla əlaqədar olaraq qarşıya qoyulan vəzifələri yerinə yetirmək məqsədilə, AMEA İnformasiya Texnologiyaları İnstitutunda da məqsədyönlü işlər aparılmış, institutun alim və mütəxəssisləri tərəfindən Milli Terminoloji İnformasiya Sisteminin (MTİS) konsepsiyası və veb-portalı hazırlanmışdır [5].

IV. QLOBALLAŞMA KONTEKSTİNDƏ DİL VƏ TƏHLÜKƏSİZLİK

Qloballaşma prosesi dilin təhlükəsizliyinə və inkişafına müsbət təsir etməklə yanaşı mənfi təsir də göstərə bilər. Prosesin müsbət təsiri dilin leksik vahidinin, onun yeni anlam tərzinin və mədəniyyətin zənginləşməsində özünü biruzə verir. Hal-hazırda milli dilə münasibətdə onun mənfi təsirləri daha çox narahatçılıq yaradır.

Qeyd etmək lazımdır ki, dil təhlükəsizliyi anlayışı elmi ədəbiyyatda hələ sistemli təsviri olmayan nisbətən yeni bir anlayışdır. Dilin təhlükəsizliyi milli təhlükəsizlik, informasiya təhlükəsizliyi, linqvistik suverenlik və dil siyasəti problemləri kontekstində tez-tez müzakirə olunur.

Dil təhlükəsizliyinə söykənən akademik müzakirələrdə qeyd olunur ki, hər növ təhdidə uyğun bir obyektin olması və onun təhlükəsizliyinin təmin edilməsi əsas şərtlərdən biridir. Başqa sözlə, həm dilin özünün təhlükəsizliyinin, həm də onun digər növ təhlükəsizliklərin təmin edilməsindəki rolundan danışmaq olar. Məlumdur ki, 2011-ci ildə ABŞ-da sentyabr hadisələrindən sonra Nyu-Yorkdakı Dünya Ticarət Mərkəzinin binalarına hücumun qarşısını ala biləcək sənədlərin məzmununu peşakarcasına dari, urdu, hindi dillərindən tərcümə və şərh edə bilən təcrübəli tərcüməçilərin çatışmamasından ABŞ-ın milli təhlükəsizliyinə təhdid kimi başa düşüldü və çox danışıldı [6].

1970-1980-ci illərdə Fransada ingilis dilinin sürətlə yayılması, cəmiyyət tərəfindən millətin ana dilinin itkisi təhlükəsi kimi qəbul edildi və 1994-cü ildə fransız dilinin qorunması haqqında qanun qəbul edildi (C.Tubonun qanunu). Həmin qanunun Parisin meri J.Şıraq tərəfindən məişətə tətbiqi Paris küçələrində ingilis dilində olan bütün lövhələrin çıxarılmasına, hətta ingilis firmalarının adlarının fransız dilinə tərcüməsinə gətirib çıxardı [7].

Hal-hazırda kiçik dillər daxil olmaqla bütün dillərin saxlanması və inkişafı Avropa Birliyinin rəsmi dil siyasəti kimi elan edilir. Buna nail olmağın yollarından biri hətta yetkinlik yaşlarında ikən insanların birdən çox xarici dil mənimsəməsi və hər zaman öyrənməkdə davam etməsidir. 1990-cı illərin əvvəllərindən etibarən dominant olan və bir sıra Avropa dillərini öz sözləri ilə dolduran ingilis dilinin öyrənilməsindən başqa bir neçə xarici dili öyrənmək zərurəti xüsusilə vurğulanır [8].

Rusiya Federasiyasının İnformasiya Təhlükəsizliyi Doktrinasında dil informasiya təhlükəsizliyi obyektlərindən biri hesab olunur [9].

Biliklər iqtisadiyyatına əsaslanan cəmiyyət üçün informasiya bərabərsizliyi müxtəlif ölkə (bölgə) əhalisinin informasiya mənbələrinə və informasiya texnologiyalarına qeyri-bərabər əlverişliyi və ya informasiyanın Internet şəbəkələrində təqdim olunan dillərini bilmədikləri təhlükə hesab olunur. Belə ki, dil təhlükəsizliyi ölkədə sosiolingvistik vəziyyətlə müəyyənləşdirilən çoxölçülü və spesifik xüsusiyyəti olan bir anlayışdır.

Ekspertlər və alimlərin fikrincə bu proseslər milli birliyin, mədəniyyətin və ölkənin intellektual potensialının məhv edilməsinə gətirib çıxara bilər. Beləliklə, dilin təhlükəsizliyinin təmin edilməsi milli təhlükəsizliyin əsas şərtlərindən biridir. Dil siyasəti, cəmiyyətdə və dövlətdəki dil problemlərini həll etmək üçün ideoloji prinsiplər və praktik tədbirlər məcmusu kimi, dilin təhdidlərdən qorunması üçün nəzərdə tutulmuşdur [10].

Hüquq linqvistikası baxımından dil təhlükəsizliyinin xarakteristikası N.D.Qolevin(*rus dilçi alim*) məruzəsində verilmişdir. Müəllif dil təhlükəsizliyi kateqoriyasını dilin hüquqi məsələləri ilə əlaqələndirir və danışqda xuliqanlıq (nalayiq sözlər), fırldaqçılıq (dilin manipulyasiya istifadəsi, yalan və / və ya dəyişmə taktikası) hallarında onun pozulmasını iki aspektdə təhlil edir. Hüquqi paradigma çərçivəsində dilin

təhlükəsizliyi danışq və ya söz oğurluğu (plagiat) ola bilər. Linqvistik paradigma çərçivəsində isə dil təhlükəsizliyi anlayışı normativ tənzimləmə və qiymətləndirmələrin puristik(*dili olduğu kimi, dəyişməz və təmiz şəkildə saxlamağa çalışaraq, hər cür yeniliyə qarşı mübarizədə ifrata varma*), qadağanedici başlanğıcının zəiflətmək meyli ilə bağlıdır [11].

NƏTİCƏ VƏ TƏKLİFLƏR

Nəticədə dil təhlükəsizliyi anlayışı ilə tolerantlıq anlayışının sıx bağlı olduğu məlum olur. Dil tolerantlığının səviyyəsi şəxsi və ya qrup tərəfindən müəyyən olunmuş qaydalar və üstünlükləri ilə təyin edilə bilər. Məsələn, şaxtaçılar və ya maşınqayırma sahəsinin mütəxəssisləri ilə müqayisədə kompüter mütəxəssislərində və ya beynəlxalq audit firmalarının əməkdaşlarında peşəkar ünsiyyətdə ingilis dilindən alınmalara görə (alınma sözlərə) tolerantlıq səviyyəsi ölçüyə gəlməz səviyyədə yüksəkdir [12].

Akademik cəmiyyətin müxtəlif sahə nümayəndələri ingilis dilinin elmi sahədə genişlənməsini (yayılmasını) fərqli şəkildə qiymətləndirə bilərlər. Hər bir şəxs (qrup) ingilis dilinin elmi terminoloji sahəsinin genişlənməsinə tolerant yanaşa bilər və rus mətbuatında amerikanizmlərin (*amerikalılarda ingilis dilinin xüsusiyyəti*) hakimiyyətini qətiyyətlə pisləyə bilər və s.

Beləliklə, dil təhlükəsizliyinin və dil tolerantlığının bu və ya digər aspektlərinin aktuallaşdırılması həmişə sosiolingvistik kontekstdə müəyyən edilir.

Qeyd etmək lazımdır ki, dilin təhlükəsizliyinin qorunması istiqamətində Prezident İlham Əliyevin fərmanı ilə Dövlət Dil Komissiyası yanında Monitoring Mərkəzinin yaradılması bu sahədə meydana çıxan bir sıra problemlərin aradan qaldırılmasında mühüm rol oynayacaq.

Azərbaycanın dünya informasiya məkanına fəal integrasiya olunmasını, bu məkanda mədəniyyətimizin, elmimizin, dilimizin, tariximizin və s. özünə layiqli yer tutmasını təmin etmək üçün aşağıdakı işlərin həyata keçirilməsi məqsəduyğun hesab edilir:

- Azərbaycan dilli Internet resursların ildə bir dəfə monitoringi aparılmalı, dərin elmi təhlil aparıldıqdan sonra, çatışmamazlıqlar, problemlər müəyyənləşdirilməli, onların aradan qaldırılması üçün tədbirlər planı işlənilib hazırlanmalıdır;
- milli Internet resursları İKT-nin yeni nailiyyətləri (xüsusilə Internetlə bağlı) nəzərə alınmaqla yenidən qurulmalı, onların keyfiyyəti, informasiya yükü, dizaynı, çevikliyi yüksəldilməlidir;
- dilçilik elminin müasir inkişaf meyillərini nəzərə almaqla, elmi tədqiqatların prioritet istiqamətləri müəyyənləşdirilməlidir;
- dilçilik sahəsində dünyanın aparıcı elmi mərkəzləri ilə əməkdaşlıq inkişaf etdirilməlidir;
- dilin inkişafı və tədrisi məsələləri uzlaşdırılmalı və təkmilləşdirilməlidir;
- dilçi alimlərin müasir informasiya və kommunikasiya texnologiyalarının istifadəsində iştirakı təmin edilsinməlidir;

- global tendensiyaların dilə neqativ təsirlərini minimuma endirmək məqsədilə konseptual xarakterli kompleks tədbirlərə ehtiyac vardır;

- dilin kiberfəzadan sıxışdırılıb çıxarılması üçün fəal milli siyasət işləyib hazırlanmalıdır;

- kütləvi informasiya vasitələrində, tədrisdə, çap olunan kitablarda, Azərbaycan dili İnternet saytlarında İKT üzrə terminlərin işlədilməsində hökm sürən özbaşınalığa son qoymaq məqsədilə bu sahədə Azərbaycan Milli Elmlər Akademiyası Rəyasət Heyəti yanında Terminologiya Komissiyası tərəfindən təsdiq olunmuş vahid, böyük həcmli terminoloji lüğət hazırlanmalı, çap olunmalı və həm də İnternetdə yerləşdirilməlidir (xüsusi saytda).

Elmi terminologiyanın yaradılması üçün Azərbaycan dili hər cür imkana malikdir. Hal-hazırda AMEA İnformasiya Texnologiyaları İnstitutunda terminoloji lüğətin hazırlanması üzərində işlər aparılır.

ƏDƏBİYYAT

- [1] Kazımov T.H. Azərbaycan dili və virtual məkan. Ekspress-informasiya. İnformasiya cəmiyyəti seriyası, Bakı: “İnformasiya Texnologiyaları” nəşriyyatı, 2009.
- [2] Terminologiya məsələləri. Bakı, Elm, 2015, <http://azkurs.org/terminologiya-meseler-1-v2.html>
- [3] İmamverdiyev Y.N. Основные термины информационной безопасности, www.genderi.org/osnovnie-termini-informacionnoj-bezopasnosti.html
- [4] Sayalı Sadıqova Azərbaycan dili terminologiyası, www.science.gov.az/news/open/142
- [5] Milli terminoloji veb-portalın təqdimat mərasimi, www.science.gov.az/news/open/7538
- [6] Language Boot Camp <http://italian.about.com/library/weekly/aa091102a.htm>
- [7] Какая страна приняла первый закон о защите родного языка? <http://otvet.mail.ru/question/17827149>
- [8] Европейский день языков https://ru.wikipedia.org/wiki/%D0%95%D0%B2%D1%80%D0%BE%D0%BF%D0%B5%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D0%B4%D0%B5%D0%BD%D1%8C_%D1%8F%D0%B7%D1%8B%D0%BA%D0%BE%D0%B2
- [9] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № ПП-1895) // <http://infopravo.by.ru/fed2000/ch03/akt14873.shtm>
- [10] Колин К. К. Русский язык и актуальные проблемы национальной безопасности // Вестник Челябинской государственной академии культуры и искусств, 2007, № 2(12), с. 131–147.
- [11] Голев Н.Д. Экспертиза конфликтных текстов в лингвистической и юридической парадигмах // <http://lingvo.asu.ru/golev/articles/v64.html>
- [12] Гриценко Е.С., Гронская Н.Э. Гипертолерантность, или о либерализме в использовании языка // Вестник Минского государственного лингвистического университета, 2009, вып. 3(40), с. 7–15.

DEVELOPMENT TRENDS AND SAFETY OF LANGUAGE IN TERMS OF GLOBALIZATION

S.Abdullayev¹, T. Kazımov², S. Abasova³

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

Baku, Azerbaijan

¹sayyar.abdullayev@yandex.ru, ²tofig@mail.ru,
³abasova.sudaba@gmail.com

Abstract – The article reviews the concept of language security in a globalized world in the context of national security, information security, linguistic sovereignty and language policy issues. The factors influencing the tendency of language development in terms of globalization, the role and security of terms in the protection of the national purity of the language is investigated.

Keywords – language safety; globalization; terminography; linguistic sovereignty; sociolinguistics

3D çap texnologiyaları və onların yaratdığı təhlükələr

Anar Səmidov¹; Zülfiyyə Hənifəyeva²

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

¹anarsamidov@gmail.com; ²zulfiyyehenifeyeva@gmail.com

Xülasə – Müasir dövrdə 3D çap geniş yayılmışdır. Artıq 3D çapa cəmiyyətin müxtəlif sahələrində - təhsildə, tibbdə, inşaatda, dizayn sahəsində, kosmik məlumatların öyrənilməsində, hərbi və s. rast gəlmək olar. 3D çapın faydaları ilə yanaşı mənfi təsirləri də rol almaqdadır. Məqalədə 3D çapın imkanları və tətbiq sahələri göstərilmiş, eyni zamanda 3D printerlərin yaratdığı təhlükələr araşdırılmışdır.

Açar sözlər – 3D printer, 3D silah, 3D texnologiya, sinterləmə.

I. GİRİŞ

Son 500 ildə surətçixarma çox sürətlə inkişaf etmişdir. Bu texnologiyanın inkişafı mətbəələrin nəşirləri əvəz etməsi ilə nəticələnmişdi, zavod və fabriklərdə eyni hərəkəti icra edən işçi əməyinin robotlarla əvəz olunmasına səbəb olmuşdu. Surətçixarma hər zaman aktual olub. Keçmişdə sənətkarlar tərəfindən hazırlanan nadir nüsxəli əşyaların, sonralar, zavod və fabriklərin yaranması nəticəsində kütləvi istehsalına başlandı. Nəticədə məhsulları ucuz qiymətə əldə etmək mümkün oldu.

Hal-hazırda yeni sənaye inqilabı ərəfəsindəyik. İndi hər kəs öz evində kompüterdən istifadə edərək, istənilən filmin, musiqinin, fotonun sürətini çox asanlıqla çıxara bilər. Artıq 3D printerlər mövcuddur. Bu printerləri hər kəs əldə edib öz evində istənilən fiziki obyektin üçölçülü modelini çap edə bilər. Yaxın gələcəkdə 3D printerlərlə adi printerlərdə kağız çap etdiyimiz kimi istənilən bir əşyanı, geyimi, hətta insan orqanını çap etmək mümkün olacaq.

3D texnologiya müasir cəmiyyətin bir çox sferalarında tətbiq edilir. Bu texnologiyaların çox sürətlə təkmilləşdirilməsi 3D printerlərin elm və texnikanın ən müxtəlif sahələrində istifadəsinə imkan verir.

II. 3D PRINTER: İMKANLARI, TƏTBİQ SAHƏLƏRİ

3D çap, günümüzdə böyüyən sənayelərdən biridir, çünki bu qurğular oyuncaqlar, aksesuarlar, idman ayaqqabıları, silahlar, maşınlar və hətta ürək kimi orqanlar çap etmək mümkündür. Əslində 3D çap yeni bir texnologiya deyil. Onun tarixi təxminən 30 il əvvəl ABŞ-da başlayıb, fotopolimerləşə bilən kompozit materiallardan həcmli obyektlərin yaradılması prosesi icad olundu. Bu texnologiya stereolitoqrafiya adlanırdı [1]. Daha sonra, müxtəlif materiallardan üçölçülü modellərin meydana gəlməsi öyrənildi, 3D çapın digər üsulları ortaya çıxdı, əsasən sənaye və yüksək ixtisaslaşmış istehsalda istifadə edildi və bunların hamısı prototiplənmə adlanırdı.

3D çap texnologiyası hər hansı bir rəqəmli görüntünü "evdə" əks etdirilə bilən həcmli fiziki bir obyektə çevirməyə imkan verir. Laylar üzrə modelləşdirmə 1980-ci illərin sonlarında icad edilmişdir və 1995-ci ildə "3D printer" (3D çap) konsepsiyaları ortaya çıxdı.

Üçölçülü çapetmə, prinsipcə sinterləmə ilə oxşar olan birləşdirmə metodu ilə işləyir və fiziki əsasına görə adi çapetməyə (plotter üsulu) bənzədiyindən üçölçülü çapetmə – 3D Printing adlanır [2].

3D printer rəqəmsal fayllardan fiziki obyektlər yaradan yeni bir texnologiyadır. 3D çap sahəsində son texnoloji nailiyyətlər tibb sahəsində bu texnologiyadan istifadənin artmasına səbəb olmuşdur.

Hazırkı dövrü 3D əsri adlandırmaq olar. 3D texnologiyaların sürətlə yayılması insanları daha rahat bir şəraitlə təmin edir. 3D çap müxtəlif sahələrdə, o cümlədən, təhsildə, tibbdə, zərgərlikdə, inşaatda, tekstil sahəsində, oyuncaq və suvinirlərin istehsalında, geoinformasiyanın alınmasında və s. tətbiq edilir:

- **Təhsildə** - 3D çap texnologiyasının təhsildə istifadəsi, təhsil müəssisəsinə sinif otaqları üçün gözəl əyani vəsaitlər əldə etmək imkanı verir. Təhsil müəssisələrinin 3D printerlərlə təchiz edilməsi təhsil prosesinin səmərəliliyinin artırılması, şagirdlərin və tələbələrin biliklərini sürətli şəkildə artırmasına kömək edəcəyi ehtimal olunur [3].
- **Tibbdə** - 3D printerlərin tibbdə tətbiqi insan həyatını xilas etməyə kömək edir. Belə printerlər uğurlu əməliyyatın təmin edilməsi üçün insanın skeletinin tam surətini yarada bilər. 3D çap protez və stomatologiya sahəsində daha geniş istifadə olunur. Tibbi üçölçülü modellər canlı hüceyrələr də daxil olmaqla müxtəlif materiallardan hazırlana bilər [4].
- **Zərgərlikdə** - Məlumdur ki, zərgərlik istehsalında ən çox vaxt aparan və böyük bir sərmayə tələb edən prosedur qəliblərin yaradılmasıdır. 3D printerlərin meydana gəlməsi ilə, zərgərlər daha əvvəl xüsusi bir proqramda hazırlanan zərgərlik modellərinin qəliblərini sürətlə artırma fərsətinə sahib oldular.
- **Tekstildə** - 3D texnologiyalı printerlər tədricən geyim istehsalı sahəsində də istifadə olunmağa başladı, ilk növbədə yüksək moda modelləri yaradıldı. 3D çap texnologiyası bir neçə fərqli materialdan istifadə

etməklə geyimin bir predmetini hazırlamağa imkan verir. Bu yanaşma hazırlanan məhsulun keyfiyyət və kəmiyyət baxımından problemlərini həll etməyə şərait yaradır.

- **Xəritənin yaradılmasında** - 3D printerlərdən istifadə edərək, ərazinin mənzərəsini dəqiq əks etdirən və hətta müxtəlif landşaftların yerləşmə səviyyələrini göstərən iri rəngli xəritələr yaratmaq olar [5].
- **Qablaşdırma** - Üçölçülü printerlər şüşə və flakonların orijinal formasının nümunə maketini düzəltməyə imkan verir. Nümunələr bütün dizayn elementləri, o cümlədən etiketlər, barkodlar, marka adları da daxil olmaqla rəngarəng ola bilər. Hazır istehsal qablaşdırma modelləri kütləvi istehsalat başlamazdan əvvəl müştəriyə göstərilə bilər. 3D nümunənin üstünlüyü göz qabağındadır: müştəri paketə toxunur, rəngini və digər xüsusiyyətlərini qiymətləndirir.

Qeyd etmək lazımdır ki, 3D texnologiyaları uzunmüddətli və həcmli modellər yaratmaq üçün bir çox qurum tərəfindən uğurla istifadə edilmişdir. Məsələn, şəffaf materialların modellərinin mövcudluğu kompleks mexanizmlərin daxili fəaliyyətinin öyrənilməsinə çox asanlaşdırır. Bu baxımdan tibb sahəsində qazandıqları müvəffəqiyyətlər daha cəlb edicidir. Dünyanın aparıcı ölkələrində cərrahlar insan orqanlarının vəziyyətini daha dəqiq diaqnoz etmək üçün 3D modellərdən istifadə edirlər. Baxılan texnologiyaların istifadəsi tibbin keyfiyyətini əhəmiyyətli dərəcədə yaxşılaşdırır. Xüsusilə diş protezləri üçün üçölçülü çapın əhəmiyyəti xüsusilə diqqəti cəlb edir [6]. Böyük Britaniyadan olan alimlər yaxın vaxtlarda gözün torqışasının nümunəsini yarada biliblər. Bu, gələcəkdə daha ağır göz xəstəliklərinə qarşı mübarizə aparmaq imkanı verən "pis görmə" konsepsiyasını məhv edə bilər. Süni donor orqanları, müalicə edilə bilməyən xərcəng xəstəliklərinə qarşı mübarizədə kömək edəcək və transplant əməliyyatları qlobal olaraq asanlaşdıracaq.

Üçölçülü çap yalnız titan implantları deyil, həm də strukturu əslinə maksimal oxşar olan sümük modelləri yaratmağa imkan verir. Bu texnologiya transplantasiya prosesini daha sadə və təhlükəsiz edə bilər.

IV. 3D ÇAPIN TƏHLÜKƏLƏRİ

3D çap, avtomobillər, aerokosmik sənaye, tibbi tədqiqatlar, istehsal və xidmət sənayesi daxil olmaqla bir çox sektorda sənaye paradiqlərini dəyişdirən əsas texnologiya halına gəlmişdir. Lakin, üçölçülü çap, rəqəmsal üç ölçülü obyektlər üçün müəllif hüquqları məsələlərini ortaya çıxarır, çünki obyekt məlumatları həm onlayn, həm də fiziki şəkildə dərc edilə bilər. Bu hal, üçölçülü çap mühitində intellektual mülkiyyətin qorunmasına aiddir. Daha sonra mövcud müəllif hüquqlarının qorunması texnologiyaları, eləcə də skriptlər və digər müxtəlif aspektləri göstərmək olar. Virtual mühitdə üç ölçülü obyektlərin çapı zamanı intellektual mülkiyyətin müəllif hüquqlarının təmin olunması vacibdir [7].

Lakin 3D printerlərin təhlükəsizliyində çox vacib bir qüsurlaşdırıcı faktor var. Kaliforniya Universitetinin elm adamları qurğunun çap prosesi zamanı çıxardığı səsli səsə sadə bir səs yazma qurğusu vasitəsilə qeydə alıb sonradan dinləyərək, printer tərəfindən hazırlanmış məhsul haqqında məlumat əldə edə bilərlər. Belə ki, printerin çap başlığının çap prosesi zamanı onun hərəkətini izləyərək yaratdığı səs-küyə əsasən hansı dizayn formasının çap olunduğunu başa düşmək çox asandır. Başqa sözlə, hər hansı bir intellektual məhsulu oğurlamaq üçün əməliyyat zamanı printerə yaxın bir smartfon və ya digər səs yazma qurğusu qoymaq kifayətdir. 3D printer işinin səs yazısından istifadə edərək, komanda çap olunmuş obyektin demək olar ki, 90% -ini dəqiqliklə yenidən yaratmağa nail olurlar. Bu faktın özü üçölçülü çapdan istifadə edən şirkətlər üçün məhsulları sənaye casusluğundan qoruma barədə düşüncəyə kifayət edir [8].

3D çapdan istifadənin daha da təhlükəli tətbiqləri var. Məsələn, 3D printerlərdən istifadə etməklə silah istehsal etmək imkanı var. Belə ki, 2013-cü ildə amerikalı Kodi Uilson 3D çapdan istifadə edilən bir ədəd tapança modelini yaratdı və İnternetdə yerləşdirdi [9]. Bu silahlar adi odlu silahla müqayisədə nisbətən ucuz və asanlıqla başa gəlir. İlk iki gündə Uilson modelinin təsvirləri yüz minlərlə insanları cəlb etmişdir. Təsəffü deyil ki, ABŞ, silah istehsalı üçün üç ölçülü çapdan istifadəni qadağan hesab edirdi. Filadelfiya odlu silahları qadağan etməyə qərar verən ilk şəhərdir. Bu qərar Filadelfiya Şəhər Şurası tərəfindən 21 noyabr 2013-cü ildə qəbul edilmişdir (şəhərdə 3D printerlərin sayının dəqiqliyi, silahın çap həcmi və onun istifadəsi Filadelfiya səlahiyyətlilərinə aid edilməmişdir) [9]. 27 noyabr 2013-cü ildə Solid Concepts şirkəti tarixdə ilk dəfə olaraq tam metal kalibri 45 ACP olan M-1911 hərbi silah modelini "çap etdirdi". Silah, paslanmayan poladdan 17-4PH və Inconel 625 markalarının sintezindən yaradılmışdır və nəticədə alınan silahın sınaqları standartlara tamamilə uyğun olaraq olduqca yaxşı performans göstərmişdir [10].

Dünyada 3D silahların qanunsuz istehsalı getdikcə genişlənir. Yaponiya "çap olunmuş silah" istehsalı və saxlanması üçün ilk hökmü verdi, İngiltərədə isə polis 3D printerləri istifadə edərək silah istehsal etməyə cəhd edənləri ələ keçirdi.

Təhlükəsizlik mütəxəssisləri, cinayətkarların aeroportlarda və oxşar yerlərdə təhlükə aşkar edən skanerlərdən qaçmaq üçün bu cür silahlardan istifadə edəceklərindən çox qorxurlar.

3D printer vasitəsi ilə çap olunan silahlar həqiqətən də hər şeyə qabildir və bu da onu deməyə əsas verir ki, müxtəlif cinayətkar dəstələr son texnologiyalardan istifadə edərək bu cür silahlardan əldə edə bilərlər. Eyni zamanda belə texnologiyaları küçədə də əldə etmək olar. Cinayətkarların evdən çıxmadan silah istehsalı ilə məşğul olma, sonra bu silahları cinayətkar qruplara satmaq imkanı var.

3D-texnologiyanın fəal tətbiqinin qarşısını alan amil onların böyük maliyyə vəsaiti tələb etməsidir. Bu sahədə məşğul olan alimlərin əsas məqsədi 3D printerlərin dəyərini azaltmaq və ev şəraitində ölçədən etməkdir. Belə ki, hər kəs belə bir printerə uyğun maddələr doldurur, nəticədə telefon,

qab, qida və digər faydalı məhsullar əldə edə bilər. İstehsal metodlarında belə fundamental dəyişikliklər iqtisadiyyata təsir etməyə bilməz. Sənayenin bu cür inkişaf xüsusiyyətləri mütəxəssisləri dərindən düşündürür ki, potensial alıcılar fabriklərdə istehsal olunan əşyaların alınması əvəzinə, öz evlərində 3D printerlə lazım olan əşyaları müstəqil hazırlamağı üstün tutacaqlar [11]. Digər məsələ isə məhsulların primitiv üsulla hazırlanması prosesidir. Bütün bunlar 3D çapın tətbiqi imkanlarının çox kiçik bir hissəsidir. Bu texnologiya gündən-günə təkmilləşir, onun imkanlarından cəmiyyətin müxtəlif sahələrində istifadə edilir. Yeni imkanlar isə yeni mütəxəssislərə tələbatı artırır. Bu səbəbdən təhlükəsizlik məsələlərinə riayət olunmalıdır. 3D texnologiyalarla işləməyi bacaran, təhlükəsizlik biliklərinə yiyələnmiş peşəkar mütəxəssislərə ehtiyac vardır.

V. NƏTİCƏ

Beləliklə, üçölçülü çap texnologiyasından istifadə XXI əsrdə insan fəaliyyətinin bütün istiqamətlərində tibb, tikinti, qida sənayesi, yüngül və ağır sənaye, hərbi sənaye, maşınqayırma (təyyarə istehsalı və raket istehsalı daxil olmaqla), yerətrafi fəzanın mənimsənilməsi, elmi fəaliyyət, incəsənət və s. sahələrində geniş perspektivlər qazanmışdır. Öminliklə demək olar ki üçölçülü texnologiyaların tətbiqi, xüsusilə müxtəlif texniki qurğuların (məsələn, smartfon), silah, geyim, hətta həyatı vacib orqanların və ərzaq məhsullarının çap imkanları barədə suallara kifayət qədər müsbət cavab verməyə imkan verəcək. Bu cür texnologiyanın sürətli inkişafı "möhtəşəm gələcək" haqqında proqnozlar verməyə xidmət edir, məsələn, evlərin tikilməsi (hətta bütün şəhər), yerətrafi orbitdə müxtəlif obyektlərin qurulması, insan bədəninin hissələrinin yaradılması 3D çapdan istifadə edərək skeletin sümüklərinin, ürəyin, qaraciyərin və digər mühüm orqanların yenidən bərpası gələcək nəsil alimlərin vəzifəsidir və biz inanırıq ki, gec-tez bu proses baş tutacaq [12].

Bu texnologiyanın nə qədər ümidverici yaxşı olmasına baxmayaraq, onun sosial sferaya gətirə biləcək pis nəticələrini unutmamalıyıq. Heç kəs bizə kütləvi qırğın silahlarının çap edilməyəcəyi kimi bir zəmanət vermir.

3D çapdan həm yaradıcı, həm də dağıdıcı məqsədlər üçün istifadə ediləcəyini nəzərə alsaq bu cür texnologiyalar bir sıra qanunlar, habelə beynəlxalq normalar və qaydalara riayət olunmasına ciddi tənzimləmə tədbirləri tələb edir. Bu, 3D texnologiyanın idarə edilməsinin və onların gələcək inkişafının tərkib hissəsi olmalıdır.

Ən yaxşı halda hökumət və hüquq-mühafizə orqanları, üç ölçülü printerlə çap olunan silahlara birbaşa qadağa qoymalıdır. Eləcə də silah istehsalı üçün lazım olan faylların yaradılması, paylanması və saxlanması ilə bağlı qanun qəbul edilməlidir.

ƏDƏBİYYAT

- [1] Как Чак Халл изобрел 3D-печать – URL: <https://habr.com/company/smileexpo/blog/420713/>
- [2] Энциклопедия 3D-печати. – URL: <http://3dtoday.ru/wiki/>
- [3] А.П. Сябренко, Ю.С. Сахалтуева, С.Е. Юленков, В.С. Тынченко

“Использование технологии 3D-печати в образовании будущих инженеров”

- [4] Devin Peek and Elizabeth Stark “Three Dimensional Printing: Modern Medical Applications” Graphic Communication Department College of Liberal Arts California Polytechnic State University 2010
- [5] М. Н. Лысыч, М. Л. Шабанов, В. В. Романов “Области применения технологии 3D печати” Современные наукоемкие технологии. – 2014, № 12 (часть 2), 165-169
- [6] A.F. Səmidov, E-tibb və 3D Texnologiyaları / A.F. Səmidov // “Elektron tibbin multidissiplinar problemləri” I respublika elmi-praktiki konfransı. - Bakı, 2016. - S. 127-129.
- [7] The dangers of 3-D printing – URL: <https://searchstorage.techtarget.com/opinion/The-dangers-of-3D-printing>
- [8] Anyone Can Steal 3D-Printed Products by Just Listening to The Sounds The Printer Makes – URL: <https://www.sciencealert.com/anyone-can-steal-3d-printed-products-by-just-listening-to-the-sounds-the-printer-makes>
- [9] В. Сычев Подписано в печать. Американские власти испугались пистолета «из принтера» <http://lenta.ru/articles/2013/05/13/printed/>
- [10] Американцы «напечатали» из металла армейский пистолет. – <http://lenta.ru/news/2013/11/08/gun1911/>
- [11] Н.В. Кушнир, А.В. Кушнир, А.М.Герашенко, В.А.Терьякин «3D-принтеры: технологии трехмерной печати и их влияние на общество и экономику» научные труды кубгту, №5, 2015 год
- [12] 3D принтеры в медицине, их настоящее и будущее – URL: <http://medicena.ru/blogpost/3d-printery-i-v-meditisine-ih-nastoyashhee-i-budushhee/>

3D PRINTING TECHNOLOGIES AND DANGERS CAUSED THEM

Anar Samidov¹, Zulfiya Hanifayeva²

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

Baku, Azerbaijan

¹anarsamidov@gmail.com; ²zulfiyyehenifeyeva@gmail.com

Abstract – 3D printing is widely spread in modern era 3D printing is used in different areas of the society today; in education, medicine, construction, design, studying cosmic information, military etc. There are negative impacts of 3D printing with its useful sides. The opportunities and application areas are shown at the article and at the same time dangers 3D printers caused are researched.

Keywords – 3D printer, 3D gun, 3D technology, sintering.

Proqram təminatı işləyən komandalарın idarə edilməsi üçün metrikalar

Tofiq Kazımov¹, Tamilla Bayramova²

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹tofig@mail.ru, ²tamilla@iit.ab.az

Xülasə— Məqalədə proqram təminatını işləyən kollektivin peşəkarlığının, onların fərqli bacarıq qabiliyyətinə və təcrübəyə malik olmasının məhsuldarlığa çox böyük təsiri və menecerin rolu haqqında məlumat verilmişdir. İşdə komandanın idarə olunması üzrə prinsiplər göstərilmiş və əməkdaşların işinin səmərəliliyinin qiymətləndirilməsi üçün yeni metrikalar təklif edilmişdir.

Açar sözlər— proqram mühəndisliyi, proqram təminatı, məhsuldarlıq, səmərəlilik, menecer, effektivlik göstəricisi.

I. GİRİŞ

Etibarlı proqram təminatının (PT) işlənməsi üçün müxtəlif ixtisaslı peşəkar və intizamlı komandanın olması vacib şərtlərdən biridir. Bu komandanın üzvləri tələbləri müəyyən edir, proqram kodunu yazır, sınaqdan keçirir, sənədləşdirir, PT-nin əvvəlcədən müəyyən edilmiş qrafik çərçivəsində yerinə yetirilməsinə nəzarət edir və onu müşayiət edirlər. Layihənin uğur qazanması və ya uğursuz olması bu mütəxəssislərin ideyalarından, peşəkarlığından və əhvali-ruhiyyəsindən asılıdır [1].

Deməli, layihənin müvəffəqiyyətli olmasına ən çox təsir edən amillərdən biri insan amilidir. Ona görə də komanda daxilində kiçik qrupların və ya ayrı-ayrı insanların rolu və funksiyaları, onlar arasındakı qarşılıqlı münasibətlər düzgün qurulmalıdır [2].

Kollektivin işinin səmərəliliyini artırmaq üçün onun hər bir üzvünün işi düzgün qiymətləndirilməlidir. Ümumiyyətlə qiymətləndirmə metodları çoxdur. Bunların hər birinin öz mənfi və müsbət cəhətləri var. Qiymətləndirmə üçün hansı metodun seçilməsi rəhbərdən asılıdır. Bu məqalədə proqram təminatının yaradılması üzrə komanda üzvlərinin işinin qiymətləndirilməsi üçün metrikalar işlənmişdir.

II. KOMANDANIN İDARƏ OLUNMASI

Komandanın idarə olunmasının bəzi prinsiplərini aşağıdakı kimi qeyd etmək olar:

- Yaxşı idarə olunan layihə adi icraçılar komandası tərəfindən uğurla yerinə yetirilə bilər;
- Pis idarə olunan layihə peşəkar ekspertlər tərəfindən yerinə yetirildiyi halda belə uğurlu olmayacaq;
- Arxitekturu düzgün işləyib hazırlanmış layihə adi PT yaradıcıları kollektivi tərəfindən də reallaşdırıla bilər;

- Arxitekturu pis işləyib hazırlanmış layihə isə hətta icraçı ekspertləri belə çəşdirə bilər.

Hal-hazırda insanlara rəhbərlik etmə qabiliyyəti rəqabətli bazar şəraitində müvəffəqiyyətin açarı hesab edilə bilər. Bu mürəkkəb məsələləri digər insanların vasitəsilə həll etmək bacarığıdır. Komandanın təşkilində menecerin xüsusi rolunu qeyd etmək lazımdır, çünki onun peşəkarlığından, məharət və bacarığından çox şey asılıdır. Kollektiv nəticələr, həmişə fərdi nəticələrdən daha çox əhəmiyyət daşıyır [3].

Göstərilən parametrləri nəzərə alaraq demək olar ki, personalın qiymətləndirilməsi etalonla real fəaliyyətin müqayisə edilməsidir. Personalın qiymətləndirilməsi aşağıda göstərilən məsələləri həll edir [4]:

- qiymətləndirilən işçinin təşkilati strukturda yeri və funksional rolunun seçilməsi, onun inkişafı üçün proqramın işlənməsi;
- təyin edilmiş meyarlara müvafiq olaraq əmək haqqının müəyyən edilməsi;
- işçini həvəsləndirmə üsullarının (motivasiyası) müəyyən edilməsi.

Personalın qiymətləndirilməsi üçün klassik metodlar aşağıdakı hallar üçün nəzərdə tutulmuşdur [5]:

- stabil təşkilati struktur və bu təşkilatın stabil fəaliyyət növü (bu da tez-tez dəyişən bazara və rəqabətin təzyiqinə uyğun deyil);
- qrup fəaliyyətinin effektivliyi nəzərə alınmadan bir işçinin qiymətləndirilməsi.

Bu deyilənlər təcrübədə mümkün olmadığından hal-hazırda komandanın işinin səmərəliliyini qiymətləndirmək üçün yeni metod və yanaşmaların işlənməsi aktual məsələlərdəndir. Bu metodlar aşağıda göstərilənlər imkanlara malik olmalıdır [6]:

- komandada olan zəif yerləri aşkar etmək və onları növbəti layihələrdə gücləndirmək;
- komandalарın işinin səmərəliliyini öz aralarında müqayisə etmək;
- mükafat fondunu işin səmərəliliyinə görə paylamaq və bu sistemi şəffaf etmək;

- komanda iştirakçılarının bilik səviyyəsinin artırılması üçün sistem işləmək;
- layihələrin idarə edilməsinin mükəmməlik dərəcəsini artırmaq üçün sistemi işləmək;
- müvəffəqiyyətli layihələrin sayını artırmaq, xərcləri azaltmaq.

Təəssüf ki, müasir qiymətləndirmə metodları yuxarıda göstərilən məsələləri həll edə bilmir [7].

III. PT-ni İŞLƏYƏN KOMANDA ÜZVLƏRİNİN SƏMƏRƏLİLİYİNİN QIYMƏTLƏNDİRİLMƏSİ METRIKASI

Məsələnin qoyuluşu. PT işləyən komanda üzvlərinin hər birini “resurs” adlandıraraq və sonrakı mülahizələrdə sadəlik üçün bu termindən istifadə edək. Aşağıdakı resurs tiplərini təyin edək: M – menecer, T – təhlilçi, P – PT-ni işləyən, S – sınaq üzrə mütəxəssis. Resursun effektivliyi universal metrika olub hər dörd M , T , P , S tipli resurslar üçün eyni cür hesablanır. Həm də nəzərdə tutulur ki, resurs ancaq öz kompetensiyasına uyğun və bir istiqamətdə olan məsələlərin həlli ilə məşğul olur. Məsələn, ancaq veb əlavələrin, verilənlər bazasının və ya hesablama modularının işlənilməsi ilə və s. Resursun effektivlik metrikasının əsas komponentlərini göstərək:

- Məsələnin yerinə yetirilmə vaxtı (C_v əmsalı ilə hesablanır);
- Məsələnin yerinə yetirilmə faktı (C_f əmsalı ilə hesablanır);
- Səhvlərin sayı (C_s əmsalı ilə hesablanır);
- Resursun effektivliyinin ekspert qiyməti (C_e əmsalı ilə hesablanır).

İstənilən tip (M, T, P, S) resursun effektivlik göstəricisi $E \in (0; 1)$ sadalanan bu komponentləri özündə cəm edir. Resursun effektivliyini aşağıdakı kimi hesablayaq:

$$E = (C_v + C_f + C_s + C_e)/4, \quad (1)$$

burada C_v – resursun yerinə yetirilmə vaxtına görə uğurla nəticələnmiş analoji məsələlər (məsələn, veb əlavələr, verilənlər bazası və ya hesablama moduları) üzrə effektivlik əmsalıdır; C_f – resursun məsələni yerinə yetirməsi üzrə effektivlik əmsalıdır; C_s – resursun o biri resurslara nisbətən səhv buraxmamaq əmsalıdır; C_e – resursun effektivliyinin ekspert qiymətləndirməsini əks etdirən əmsalıdır. E –in böyük qiyməti daha yaxşı hesab olunur.

Resursun yerinə yetirilmə vaxtına görə uğurla nəticələnmiş məsələlər üzrə effektivlik əmsalı aşağıdakı formulla hesablanır:

$$C_v = 1 - V_2/V_1, \quad (2)$$

burada $V_1 = (T_1 - T_2)/N_v$ – resursun uğurla nəticələnmiş məsələlər üzrə yerinə yetirilmə vaxtının orta qiymətidir; N_v – resursun uğurla nəticələnmiş məsələlərinin sayıdır; T_1 – resursun uğurla nəticələnmiş məsələlərinin ümumi yerinə yetirilmə vaxtıdır; T_2 – resursun uğurla nəticələnmiş məsələləri yerinə yetirərkən fasilələrinin ümumi vaxtıdır; $V_2 = (T_{1a} - T_{2a})/N_{va}$ – resursun uğurla nəticələnmiş analoji məsələlər üzrə yerinə yetirilmə vaxtının orta qiymətidir; N_{va} – resursun uğurla nəticələnmiş analoji məsələlərinin sayıdır; T_{1a} – resursun uğurla nəticələnmiş analoji məsələlərinin ümumi yerinə yetirilmə vaxtıdır; T_{2a} – resursun uğurla nəticələnmiş analoji məsələləri yerinə yetirərkən fasilələrinin ümumi vaxtıdır; $C_v \in [0; 1]$ və böyük qiyməti daha yaxşı hesab olunur.

C_f – resursun məsələləri yerinə yetirməsi üzrə effektivlik əmsalı aşağıdakı düsturla hesablanır:

$$C_f = (a_1 N_1 + a_2 N_2 + a_3 N_3 + a_4 N_4)/N, \quad (3)$$

burada N_1 – vaxtında yerinə yetirilmiş məsələlərin sayıdır; N_2 – vaxtından qabaq yerinə yetirilmiş məsələlərin sayıdır; N_3 – vaxtından gec yerinə yetirilmiş məsələlərin sayıdır; N_4 – yerinə yetirilməmiş məsələlərin sayıdır; N – resursla bağlı məsələlərin ümumi sayıdır; a_1, a_2, a_3, a_4 – N_1, N_2, N_3, N_4 üçün çəki əmsallarıdır. a_1, a_2, a_3, a_4 əmsallarının qiymətləri ekspert qiymətləndirilməsi əsasında müxtəlif layihə və proseslərdə variativ surətdə müəyyən oluna bilər.

a_1, a_2, a_3, a_4 əmsallarının ekspert qiymətləndirilməsi əsasında hesablanmasının bir sadə variantını göstərək. Tutaq ki, $\delta = 1, 2, 3, \dots$ sayda expertin N_1, N_2, N_3, N_4 məsələləri üzrə λ ballı sistemdə qiymətləndirməsi var. Onda a_j ($j=1, \dots, 4$) belə hesablanabilir:

$$a_j = \frac{1}{\delta \lambda} \sum_{i=1}^{\delta} p_{ij}, \quad j=1, \dots, 4. \quad (4)$$

burada p_{ij} – i -ci expertin j -ci məsələ üzrə qiymətləndirməsidir.

Məsələn, praktiki məsələlərdə a_1, a_2, a_3, a_4 əmsalları üçün $a_1 \in [0, 9; 1, 1]$, $a_2 \in [1, 2; 1, 5]$, $a_3 \in [0, 6; 0, 8]$, $a_4 \in [0, 2; 0, 5]$ intervalları müəyyən oluna bilər.

Resursun o biri resurslara nisbətən səhv buraxmamaq əmsalı C_s aşağıdakı düsturla hesablanır:

$$C_s = 1 - H_s/H_u, \quad (5)$$

burada H_s – resursun əvvəllər yerinə yetirdiyi bütün məsələlər üzrə buraxdığı səhvlərin ümumi sayıdır; H_u – bütün resursların yerinə yetirdiyi bütün məsələlər üzrə buraxdığı səhvlərin ümumi sayıdır. $C_s \in [0; 1]$ və böyük qiyməti daha yaxşı hesab olunur.

C_e – resursun effektivliyinin ekspert qiymətləndirməsini əks etdirən əmsalı aşağıdakı düsturla hesablanır:

$$C_e = \frac{1}{\lambda^3 \delta^3} \prod_{j=1}^3 \sum_{i=1}^{\delta} b_{ij}, \quad (6)$$

Burada δ – ekspertlərin sayı; b_{i1} – i -ci expertin resursun məsələləri yerinə yetirmə sürətinə verdiyi qiymətdir; b_{i2} – i -ci expertin resursun məsələləri yerinə yetirmə keyfiyyətinə verdiyi qiymətdir; b_{i3} – i -ci expertin resursun bilik və bacarığına verdiyi qiymətdir; $C_e \in [0;1]$ və böyük qiyməti daha yaxşı hesab olunur və işçilərin əməyinin qiymətləndirilməsi zamanı əsas göstərici kimi istifadə edilə bilər.

NƏTİCƏ

Təklif olunan yanaşma PT icraçılarının işinin effektivliyini qiymətləndirməyə və eyni zamanda hansı məsələnin hansı icraçı tərəfindən daha tez və effektiv yerinə yetirilməsini müəyyən etməyə imkan verir. Bu yanaşmanın köməyi və qurulan imitasiya modeli vasitəsilə PT-nin işlənmə prosesini proqnozlaşdıraraq qəbul olunan qərarların effektivliyini qiymətləndirmək olar.

Lakin istənilən halda işin spesifikasiyası, komandanın xüsusiyyətləri və kollektivdə olan münasibətlər də nəzərə alınmalıdır. Əgər əməkdaş əmin olsa ki, onun işinə qiymət verirlər, o nəinki kollektivi və şirkəti pis vəziyyətə qoymaz, həm də mümkün qədər çox xeyir gətirər.

İstənilən şirkətin müvəffəqiyyətlə işlədiyinin əsas göstəricisi onun əldə etdiyi gəlirdir. Bu da məhsulun və ya xidmətin istehsalı üçün mövcud resurslardan səmərəli istifadə edilməsi və personalın işinin düzgün təşkil edilməsindən asılıdır. Ona görə də işçilərin işinin düzgün qiymətləndirilməsi və ölçülməsi hal-hazırda vacib problemlərdən biridir.

ƏDƏBİYYAT

1. Лаврищева Е.М., Петрухин В.А. Методы и средства инженерии программного обеспечения: Учебное пособие. – М.:МФТИ, 2007, 415 с.
2. Фищенко К. С. Оценка эффективности работы персонала // Актуальные вопросы экономики и управления: материалы Междунар. науч. конф. Москва, апрель 2011 г.Т. II, М.: РИОР, 2011. с. 68-70. <https://moluch.ru/conf/econ/archive/9/458/>
3. Boehm B. W.. Software engineering economics. Manuscript received april 26, 1983, The author is with the Software Information Systems Division, TRW Defense Systems Group, Redondo Beach, CA 90278. pp. 150.
4. Веснин В.Р. Управление персоналом. Теория и практика: электронный учебник. М., 2009.
5. Уилсон С.Ф., Мэйплс Б., Лэндгрейв Т. Принципы проектирования и разработки программного обеспечения. М., 2002.
6. Жаркова Г. А. Современные системы автоматизации разработки информационных систем: учебно-методическое пособие. Ульяновск: УлГУ, 2007.
7. Development Leaders Reveal the Best Metrics for Measuring Software Development Productivity, 2017, <https://stackify.com/measuring-software-development-productivity/>

METRICS FOR EVALUATING THE WORK OF SOFTWARE DEVELOPMENT TEAM MEMBERS

Tofig Kazimov¹, Tamilla Bayramova²

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

¹ tofig@mail.ru, ² tamilla@iit.ab.az

Abstract- The article provides a detailed explanation of the large impact on the productivity of software product development, qualifications, personal qualities and experience of software developers, and emphasizes the leading role of the manager. This paper shows the principles of team management and provides metrics for evaluating team performance.

Keywords- — software engineering, software, productivity, efficiency, manager, effectiveness indicator.

Sosial şəbəkələrdə gizlilik və təhlükəsizlik problemləri

Nərgiz Abdullayeva

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

nargiz.ni.21@gmail.com

Xülasə — Bu məqalədə onlayn sosial şəbəkələrdə gizlilik və təhlükəsizlik problemləri analiz edilmişdir. Sosial şəbəkə riskləri və onlardan qorunmağın yolları araşdırılmışdır.

Açar sözlər - onlayn sosial şəbəkələr; gizlilik riskləri; data mining,

I. GİRİŞ

Hal-hazırda onlayn sosial şəbəkələr internet mühitində fəaliyyət göstərən ən təsirli media quruluşlarından biri halına gəlmişdir. Sosial media Internet texnologiyaları vasitəsilə insanlar arasında virtual sosial ünsiyyət yaratmaq və məlumatları paylaşma deməkdir. O, daha əlçatan və veb əsaslı texnologiyalardan istifadə etməklə ünsiyyəti interaktiv dialoqa çevirir. Sosial media vasitələrinə internet üzərindən yayımlanan informasiya saytları, sosial şəbəkələr, bloqlar, mikro bloqlar, ani ünsiyyət proqramları, forumlar daxildir. Sosial şəbəkələr bizim fiziki dünyamızın virtual formasıdır [1]. Onlayn sosial şəbəkələr istifadəçilərə zaman və məkan məhdudiyyəti qoymadan bir çox imkanlar təklif edir. Son illərdə onlayn sosial şəbəkə istifadəçilərinin və mövcud məlumatların sayında hədsiz artım müşahidə edilir. Onlayn sosial şəbəkələrin yayılması ilə bu şəbəkələrdə informasiya mübadiləsi də daim artan əhəmiyyətə malikdir. Onlayn sosial şəbəkələr əhəlinin böyük segmentinin həyatının daimi iştirakçısıdır və offlayn fəaliyyətlərinə də birbaşa təsir göstərir. Əlbəttə ki, bu da ciddi gizlilik və təhlükəsizlik riski yaradır.

Bu məqalədə sosial şəbəkə məlumatlarına diqqət yetirilib və məlumatların toplanmasına və qorunmasına dair problemlər aşkarlanıb. İstifadəçilərin gizlilik və təhlükəsizliyinin qorunması üçün istifadə olunan bir sıra mövcud üsullar və sosial şəbəkə problemləri araşdırılıb, təkliflər verilib.

II. SOSIAL ŞƏBƏKƏLƏRDƏ GİZLİLİK VƏ TƏHLÜKƏSİZLİK RİSKLƏRİ

Sosial şəbəkələr bir çox şəxsəndən ibarət ekosistemdir [2]. Gizlilik və bir şəxsin sosial şəbəkəsi arasındakı əlaqə çox yönlüdür. Gizlilik siyasətinin sosioloji nəzəriyyələri fərdlərin fərqli dərəcədə inam və yaxınlıq yaratmaq üçün başqaları ilə fərdi məlumatları paylaşmağı necə seçə biləcəyini qeyd edir [3].

Gizlilik və təhlükəsizliyin möhkəmləndirilməsi ilə bağlı olan unikal problemləri anlamaq üçün ilk növbədə şəbəkə

təhlükəsizliyinin standart prinsiplərini, o cümlədən onların onlayn sosial şəbəkələr üçün necə genişləndirildiyini nəzərdən keçirməliyik. Daha sonra, xüsusilə istifadəçilərin fərdi məlumatların aşkar etmək üçün sosial şəbəkə analizi və əlaqəli üsulları üzərində gizlilik və təhlükəsizlik hücumlarının necə qurulacağına baxılır.

Gizlilik onlayn sosial şəbəkələrdə mühüm əhəmiyyət kəsb edir. Çünki istifadəçilərin şəxsi məlumatlarının qeyri-qanuni açıqlanması və düzgün istifadə edilməməsi insanların həyatında istənməyən və zərərli nəticələrə səbəb ola bilər. Onlayn sosial şəbəkələr çərçivəsində gizlilik bir neçə geniş kateqoriyaya malikdir:

- İstifadəçi şəxsiyyətinin gizliliyi – müxtəlif onlayn sosial şəbəkələr arasında istifadəçinin şəxsiyyətinin qorunması;
- İstifadəçinin fərdi gizliliyi – bura istifadəçinin biblioqrafik məlumatları, şəxsi dosyaları və s. daxildir;
- İstifadəçinin ünsiyyət gizliliyi - bura əlaqələrin vaxtı və uzunluğu, əlaqələrin yeri (IP ünvan), digər istifadəçi profillərinə göndərilən və alınan məktublar və s. [4] daxildir;

Bəzən biz özümüz haqqında məlumatı kənar şəxslər tərəfindən deyil, yalnız dost qrupları ilə paylaşmaq istəyirik. Bunun üçün onlayn sosial şəbəkələrdə gizliliklə bağlı “xəbərdarlıq və razılıq” xidməti fəaliyyət göstərir. Bu yanaşma xidmətin məxfilik praktikasını istifadəçiyə bildirir və istifadəçi xidmətə daxil olub-olmamasını seçir. Lakin bəzi hallarda sosial şəbəkələrdə gizlilik istifadəçi tərəfindən pozulur. Və bu pozuntular sosial şəbəkələrdə kimlik oğurluğu və ya məlumatların sızması, spam profillərdən saxta istəklər, ictimai paylaşma riskləri, saxta tətbiqlər və zərərli linklər kimi bir sıra riskləri gətirib çıxarır. Bu risklərə qısaca nəzər yetirək:

1) *Kimlik oğurluğu*: Buna sosial şəbəkələrdə saxta profillər də deyilir. 2012-ci ildə 12 milyon insan kimlik oğurluğu və məlumat sızmasının qurbanı olmuşdur. Bu hadisə ABŞ-da *müştərilərin* məxfi məlumatlarını idarə edən maliyyə təşkilatlarının ümumilikdə təxminən 21 milyard dollar pul itkisinə səbəb olmuşdur.

2) *Sosial paylaşım riski*: Facebook, Snapchat, Instagram kimi geniş yayılmış ictimai sosial şəbəkələrdə fotoşəkillər ilə yanaşı mövcud yerləri paylaşa bilən xüsusiyyət var. Bu

yerlər ətraflı ünvan şəklində göstərildiyi üçün istənilən şəxsin sizi tapmasını asanlaşdırır.

3) *Saxta tətbiqlər və zərərli linklər*: Sosial şəbəkələrdə saxta tətbiqlər və linklər mövcuddur. İstifadəçi həmin linkə daxil olduqda onun mobil nömrəsi, e-mail ünvanı və s. kimi şəxsi məlumatları həmin tətbiqlər tərəfindən oğurlana bilər.

Bəs bu risklərin qarşısını almaq, onlardan qorunmaq üçün nə etmək olar? Onlayn sosial şəbəkələrdə gizlilik və təhlükəsizlik risklərində qorunmaq üçün aşağıdakı məsləhətləri təklif edirik.

- Güclü şifrə yaradın. Ad, doğum tarixi, telefon nömrəsi kimi məlumatları şifrələmədə istifadə etməyin. Daha çox rəqəmdən, böyük hərflərdən, fərqli simvollarından istifadə edin. Şifrəniz nə qədər güclü olsa risk daha az olacaq.
- Sosial profillərinizi tez-tez nəzərdən keçirin və hər bir şəxsi məlumatların qorunmasına diqqət yetirin. Sosial şəbəkələrin gizlilik xidmətlərinə riayət edin.
- Saxta tətbiqlər və zərərli ola biləcək linklərə daxil olmayın. Bunlar həm virus, həm də kiberterrorizm xarakterli ola bilər.
- Gələn mesajların və sorğuların bloklanması kimi sosial şəbəkə tərəfindən təklif olunan genişləndirilmiş gizlilik seçimlərindən istifadə edin və s.

NƏTİCƏ

Sosial şəbəkələrdə şəxsi məlumatların əldə edilməsinə nəzarət və onun mühafizəsinin təmin olunması üçün onlayn sosial şəbəkələr bir sıra daxili nəzarət mexanizmlərinin istifadəsini dəstəkləyir [5,6]. Lakin onlayn sosial şəbəkə istifadəçilərinin tədqiqatları nəticəsində ortaya çıxır ki, bu mexanizmlər profillərin və şəxsi məlumatların qorunmasına tam müvəffəq ola bilmir [7]. Onlayn sosial şəbəkə xidmətlərini optimallaşdırmaq və istifadəçilərin üstünlükləri və maraqları baxımından fərdləşdirmək üçün Data Mining texnologiyalarından istifadə edilə bilər. Bununla belə, sosial Data Mining və onlayn sosial şəbəkələrin tələbləri arasında potensial münaqişələr yarana bilər. Hər hansı bir rəqib sosial şəbəkə istifadəçilərinin gizlilik parametrləri ilə nəşr olunan

sosial şəbəkə məlumatlarını və bəzi başqa məlumatları istifadə edərək daxil ola bilər. Buna görə də onlayn sosial şəbəkələrin gizlilik tələblərinə cavab vermək üçün qraf anonimləşdirmə proseduruna daxil edilməlidir. Aydındır ki, Data Mining nəticələri və onlayn sosial şəbəkə istifadəçilərinin gizlilik tələbləri arasında qarşılıqlı əlaqə var. Ədəbiyyatlarda bir çox qraf anonimləşdirmə üsulları təklif olunmasına baxmayaraq, bu praktikada hələ də məhduddur.

ƏDƏBİYYAT

- [1] R.M.Alıquliyev, N.Ə.İsmaylova, “Sosial mediada milli informasiya təhlükəsizliyinə təhdidlərin aşkarlanması üçün yanaşma,” İnformasiya təhlükəsizliyinin aktual problemləri III respublika elmi-praktiki seminarı, 2017, pp. 70-72
- [2] I. Kayes, A. Iamnitich, “Privacy and security in online social networks: A survey,” Online Social Networks and Media, Vol. 3–4, 2017, pp. 1–21
- [3] Lipford H.R., Besmer A., Watson, J., “Understanding privacy settings in facebook with an audience view,” Proceedings of the 1st Conference on Usability, Psychology, and Security, 2008, pp. 1–8.
- [4] R. Gross, A. Acquisti, “Information Revelation and Privacy in Online Social Networks,” Workshop on Privacy in the Electronic Society (WPES), 2005, pp. 71-80.
- [5] Liu Y., Gummadi K.P., Krishnamurthy B., Mislove A., “Analyzing facebook privacy settings: user expectations vs. Reality,” Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. (IMC '11), 2011, pp.68–73.
- [6] Johnson M., Egelman S., Bellovin S.M., “Facebook and privacy: it's complicated,” Proceedings of the Eighth Symposium on Usable Privacy and Security. (SOUPS '12), 2012, pp. 1–15.
- [7] C. Zhang, J. Sun, X. Zhu, Y. Fang, “Privacy and Security for Online Social Networks: Challenges and Opportunities,” IEEE Communications Society, 2010, pp. 13-18.

PRIVACY AND SECURITY ISSUES ON SOCIAL NETWORKS

Nargiz Abdullayeva

Institute of Information Technology of ANAS,

Baku, Azerbaijan

Abstract -- This article analyzes privacy and security issues in online social networks. Social network risks and ways of protection are studied.

Keywords -- online social networks; privacy risks; data mining

İnternet-reklam marketinqində informasiya təhlükəsizliyi problemləri

Kəmalə Haşimova

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

multimedia@iit.science.az

Xülasə— Müasir dövrdə İnternetin global sahəsi genişləndikcə, imkanları çoxaldıqca, internet reklamlara tələb artır. Tədqiqatda İnternet üçün nəzərdə tutulmuş reklam-marketingin imkanları, tövsiyə sistemlərindən istifadənin perspektivləri araşdırılmış, təhlükələr müəyyən edilmişdir. Həmçinin veb saytlarda yerləşdirilən reklam-marketing sistemlərindən səmərəli istifadə üçün təkliflər verilmişdir.

Açar sözlər— *İnternet reklam-marketing; tövsiyə sistemləri; hücum; reyting; onlayn-reklam*

I. GİRİŞ

İqtisadiyyatın inkişafında önəmli rol oynayan aspektlərdən ən əsası, müasir dövrün tələbi olan İnternet reklamdır. O, xüsusilə elektronlaşdırılmış məkanda istehsalçı və istehlakçı arasında vəhdət yaradır.

Virtual məkanda rast gəldiyimiz internet-reklam həm maddi, həm də mənəvi tərəfdən əlverişlidir. Məhsul əldə etmək istəyən alıcı sifariş yolu ilə məhsulu əldə edə bilər. İnternet –reklam istehlakçı və istehsalçı arasında olan boşluğu aradan qaldırır, vasitəçiyə ehtiyac duyulmur. Proses zamanı bir çox maneələr meydana çıxır ki, bu da qaçılmazdır. Məsələn, istənilən məhsulun əvəzinə başqa məhsul göndərilir və ya keyfiyyət reklamda göstərilən kimi olmur. Bu baxımdan istifadəçi mənafeyi qorunmalı və onu gözləyən təhlükənin qarşısı alınmalıdır.

Biznes saytlarında boşluqları aradan qaldırmaq üçün tövsiyə sistemi məhsulun idxal - ixracında köklü dəyişiklik etmişdir. Tövsiyə sisteminin vəzifəsi istifadəçiyə maraq göstərdiyi məhsul haqqında məlumat verməkdir. Məlumat əldə edən müştəri seçimində keyfiyyətli məhsul və xidmətlərə üstünlük verir. Təklif olunan mallarla yanaşı alıcıya servis xidməti göstərilir ki, bu da yeni müraciətə şərait yaradır. İstehsalçı öz növbəsində təlabata görə məhsulun çeşidini müəyyən edir.

II. SAYTLARDA TÖVSIYƏLƏRİN ROLU

"Tövsiyə" termini daha geniş mənada istifadə olunur. Reklamın paylanması üçün müştərilərin seçimi, optimal təklif qiymətinin müəyyən edilməsi və ya sadəcə müştəri ilə ən yaxşı ünsiyyət strategiyasının seçilməsi yalnız optimallaşdırma məsələsinin səmərəli həlli ilə həyata keçirilə bilər [1].

Tövsiyələr istifadəçinin potensial maraqlarını məhsulun orta reytingi ilə müəyyən edir: "Hər kəs onu sevir – hər kəs onu seçir" prinsipinə əsasən, istifadəçilərə sistem tərəfindən müraciətlər göndərilir.

Tövsiyələr Biznes modelinin əsası ola bilər (məsələn, TripAdvisor) və ya naviqasiya kataloqunu daha da genişləndirərək onlayn mağazada xidmət göstərir.

Məsələn, məhsullar (Amazon, Ozon), məqalələr (Arxiv.org), xəbərlər (Surfingbird, Yandex.Dzen), şəkillər (500px), videolar (YouTube, Netflix), insanlar (LinkedIn, LonelyPlanet), musiqi (Last.fm, Pandora), çağlı siyahıları və s. ümumiyyətlə, hər sahə üzrə təklif edilə bilər.

Saytlarda istifadəçi reytingləri iki şəkildə əldə edilə bilər:

- Aşkar - istifadəçi özü məhsulun reytingini görür, mütəmadi izləyir;
- Qapalı- istifadəçi öz mövqeyini açıq şəkildə izləyə bilmir, amma onun xidmətlərindən yararlanır, faiz toplayır və s. [1].

İstifadəçi aşkar üsulu daha çox bəyənilir və ona üstünlük verir. Amma praktikada, saytlar bütün maraqları açıq şəkildə ifadə etmək imkanı vermir və istehlakçılar bunun tərəfdarı deyillər [2].

Tövsiyələr fərqli şəkildə göstərilə bilər - bir məhsulun təsviri (Amazon) pankart kimi, müəyyən bir parametrlər (TripAdvisor) kimi və s.

Rusiyalı mütəxəssislər "Tövsiyələr" zamanı pozuntular aşkar etməzdən əvvəl, reklam süzgecindən alqoritmlər siyahısının çıxarılmasını təklif edir. Təhlükəsiz Liman istifadəçilər üçün onlayn reklamın keyfiyyətinin yaxşılaşdırılması və media saytlarının biznesini qoruyan bir mexanizmdir. Bu Layihə, yüksək keyfiyyətli reklam təkliflərini dəstəkləyən saytları birləşdirmək üçün nəzərdə tutulur.

III. REYTINGİN HESABLANMASI

Məhsul reytingi məhsulla yanaşı, yanaşma sayı, müsbət və mənfi reyting (adətən forumlarda olduğu kimi), yüksək qiymətlərin nisbəti və ya markalar ola bilər.

Bəzi hallarda tövsiyənin "yeniliyini" (daxil edildiyi tarixi) nəzərə almaq vacibdir. Bu xüsusilə forumlarda məqalələr və ya mesajlar üçün nəzərdə tutulur. Yeni qeydlər tez-tez ön sıralarda yerləşməlidir. Bunu etmək üçün düzəliş

faktorlarından istifadə edilir. Media saytlarında məqalələrin reytinginin hesablanması üçün formulaya baxaq. Hacker xəbər qəzetində reyting hesablamasının nümunəsi:

$$\text{Rank} = \frac{(U-D-1)^{0.8} \cdot P}{T^{1.8}} \quad (1)$$

burada, U = yüksək səs, D = aşağı səs, P (Penalty) — digər biznes qaydalarının tətbiq edilməsi üçün əlavə düzəliş

Reddit reytinginin hesablanması:

$$\text{Rank} = \log(\max(1, U - D)) - \frac{|U-D|T}{\text{const}} \quad (2)$$

burada, U = “Hə” deyən səslər, D = “Yox” deyən səslər, T = qeyd vaxtı. Universal bir düstur yoxdur və hər bir xidmət öz problemini həll edən formulları özündə birləşdirir - empirik şəkildə test edir [3].

IV. İNTERNETDƏ REKLAM TƏHLÜKƏ MƏNBƏYİ KİMİ

İnternetdə reklam-marketing sahəsində tövsiyələrdən yararlanmaq lazımdır. Hər sahədə olduğu kimi bu sahədə də çoxsaylı çatışmazlıqlar mövcuddur.

Tövsiyə sistemləri istifadəçilərin fərdi məlumatları haqqında verilənlər bazasına topladıqları məlumatların onların əleyhinə istifadə olunmaması üçün etibarlı qorunmalıdır. Bir neçə neqativ halları nəzərdən keçirək:

– Bir neçə il əvvəl Google korporasiyası böyük qalmaqalla üzlaşmışdı. Səbəb bir çox istifadəçi tərəfindən onların elektron poçtundan məlumatlarının skan edilərək reklamda istifadə olunması idi. Nəticədə 2014-cü ildə bir neçə Hollivud tanınmışlarının fərdi məlumat və fotolarının mətbuata sızmışdı [4]. Bu hadisələr sürətlə inkişaf edən texnologiyalar dövründə məlumatların etibarlı qorunmasını bir daha gündəmə gətirdi.

– Siz hansısa saytdan musiqi redaktoru proqramını yüklədiniz və onu kompüterə quraşdırmaq istəyirsiniz. Quraşdırılan zaman proqramın özü ilə bərabər, reklam proqramı da kompüterinizə yüklənir. Bu zaman bütün brauzerlər bağlanır. Lakin siz yenidən sevimli saytlara daxil olduqda, o reklam saati yenidən işə başlayır. Saytda normal keçidlərə klik edərkən yeni bir başqa səhifə açılır. Bu da reklam proqramını yaradan şəxs üçün gəlir mənbəyi olur [5].

Bir çoxları üçün reklam – şəbəkədə əsəbləri korlayan element və ya kompüterdə olan bütün məlumatlar üçün təhlükə mənbəyidir. Belə ki, müəyyən seçimlərdən sonra onlayn sifariş verilmiş məhsul əvəzinə içərisində zəhərli maddələr və ya lazımsız əşyalar olan bağlamanın çatdırılması hallarına rast gəlinib.

Kibercəsus proqramlar elektron poçtlara reklam məktublar vasitəsilə daxil olur. Hər hansı reklam blokerini quraşdırmaqla bir başa iki işi yerinə yetirmək mümkündür.

1. Trafiki zəiflədən lazımsız yükləmələrin olmasıdır;
2. Lazımsız məlumatlarla sahəni doldurmaq imkanını məhdudlaşdırmaq;

Filtirləmə olan saytlarda lazımi reklamla məlumatlanmaq kifayət edir.

XSS (cross-site scripting)-bir hücum növüdür [8]. Zərərli kod veb səhifəyə müdaxilə edir. İstifadəçi onu açan zaman kompüterə yayılır. Zərərli kod birbaşa saytın öz serverində yerləşir. Belə bir kod bütün istifadəçilərin məlumatlarını oğurlaya və ya saytda dəyişiklik edə bilər. Məsələn, məhsulların qiymətlərini dəyişə bilər.

DDoS (Distributed Denial of Service) hücumu - çoxsaylı zombiləşmiş host bədnəviyyələri (Bot Net) eyni vaxtda sayta daxil olmaq üçün çalışır və sayt bu yükün (trafikin) qarşısında dayanıqlığını itirir. İlk növbədə əsas təhlükə saytın bloklanmasıdır. Bəzən kommersiya məqsədli internet-magaza saytları tələsik yaradılır və istifadəyə verilir. Belə saytlar asanlıqla DDoS hücumlarına məruz qalırlar [7].

Veb resursların nəzarəti ələ keçirildikdən sonra onlardan SPAM-ların paylanması, zərərverici kodların göndərilməsi, internetdə lazımi materialları skan edərək öz maraqları üçün istifadə edirlər.

V. ZƏRƏRLİ PROQRAMLAR VƏ ONLARDAN QORUNMA YOLLARI

Biznesdə veb sayt internet-magaza üçün əsas vasitələrdən biridir. Bu səbəbdən saytı "biznes kartı" kimi deyil həm də təhdidlərdən qorumaq məqsədi ilə dayanıqlı, təhlükəsiz yaratmaq məsləhətdir.

Onlayn-reklam mütəxəssisləri və reklam nümayəndələri multiekranlı reklam şirkəti yaratmaqla məşğuldurlar. Bu şirkət istifadəçi addımlarını müxtəlif növ kompüter vasitələrində izləməyə çalışırlar. Əsasən istifadəçi haqqında daha çox fərdi məlumat toplamaq təhlükə riskinin artmasına yönəlir.

Əvvəl smatfonda başlayan satışın notbukla yekunlaşdığı hallara rast gəlmək olur. Hansı qurğuda satış həyata keçirilib? Bu məsələdə effektivliyin ölçülməsi ortaya çıxır.

İstifadəçi kiçik kompüterdə reklamı izləyir, lakin mobil qurğuda gördüyü reklamdan digər kompüterlə yararlanır. Bu proses iki müxtəlif istifadəçi kimi qeydə alınır. Problemin həlli üçün marketoloqlar reklam nümayişi zamanı geolokasiya məlumatlarından istifadə etməyə çalışırlar. Həmin üsulla müştəri haqqında daha çox informasiya əldə edilir. Bu da hər kəsin xoşuna gəlmir.

Dünyada 140 milyondan çox istifadəçi onların daxil olduqları saytlarda reklamın görünməsinə üstünlük verir. Bu isə internetə çıxış imkanına malik yer kürəsi əhalisinin 5 faizi deməkdir. Eyni zamanda ABŞ-in "Google" və Almaniyanın "RTL" kimi böyük internet şirkətləri reklamdan gəlir əldə etmək üçün onu bloklayanlarla müxtəlif üsullarla mübarizə aparır. Bir sıra şirkətlər elanların göstərilməsi üçün maneələri dəf edən texnologiyaların hazırlanmasına milyardlarla dollar vəsait xərcləyir. Reklamın bloklanması internet nəşrlərinin gəlirlərinə maddi təsir göstərir. İstifadəçilərin tələb etdiyi azad internet reklamı blok edənlərin sayının artması ilə davam edə bilməz.

Deloitte şirkətinin tədqiqatına görə, Rusiyada internet istifadəçilərinin təxminən üçdə biri reklam blok edənlər sistemlərdən istifadə edir, 13% isə onları yaratmaq istəyir. Blok edənlərin quraşdırılmasında əsas səbəb "qıcıqlandırıcı" reklamın qarşısını alır. Bu həm saytlar üçün problem yaradır, həm də reklam gəlirlərinin itkisinə səbəb olur [9].

İnformasiya sızması ölkələr arasında gözlənilməz nəticələrə gətirib çıxara bilər. Ona görə reklam təmsilçiləri

narahatdırlar və təhlükəsizliyin idarə etməsi üzərində düşünürlər.

Azərbaycanda son dövrlər onlayn alış-veriş saytlarının artması təhlükəsizlik problemin aktual etmişdir [10]. Həm xarici, həm də yerli saytlardan alış-veriş edərkən, diqqətli, ehtiyatlı olmalı və aşağıdakı şərtlər ödənilməlidir:

1. Tanınmış saytları seçilməsi;
2. İnanılmaz təkliflərdən çəkinmək;
3. Təhlükəsiz transfer tələb etmək;
4. Açıq Wi-Fi məkanlarında alış-veriş etməmək;
5. Çox sual verilsə diqqətli olmaq;
6. Alış-verişdən sonra kredit kartınıza nəzarət etmək;
7. Şəxsi məlumatlarınızı etibarlı saxlamaq;
8. Mobil telefonunuzu internet təhdidlərdən qorumaq;
9. Şifrə seçimində diqqətli olmaq;

Saytlarda onlayn reklamın populyarlığını təmin etmək üçün parametrlərin uyğun və rahat olmasını tənzimləmək əsas şərtdir. Bu kimi təhlükəsiz reklamlar biznes sahəsində məhsul və xidmətlərin inkişafı üçün əsaslı rol oynayır.

NƏTİCƏ

İnkişaf etmiş ölkələrdə demokratiyanı daha da inkişaf etdirən amillərdən biri Elektron Dövlətin formalaşdırılması hesab edilir.

Elektron Dövlət-müasir informasiya texnologiyalarından istifadə etməklə dövlət qurumları tərəfindən Azərbaycan Respublikasının ərazisində yaşayan bütün vətəndaşlara, hüquqi və fiziki şəxslərə informasiya və e-xidmətlərin göstərilməsinə şərait yaradır. İnternetdən daha səmərəli istifadə hər sahədə olduğu kimi reklam –marketing sahəsində də xeyli irəliləyişə, iqtisadiyyatın artmasına, xalqın rifahının yaxşılaşmasına əsaslı təsir göstərmişdir. Kibercinayətkarlığın, informasiya müharibəsinin olduğu dövrdə reklam sahəsində təhlükəsizliyi qorumaq əsas şərtdir.

İnformasiya təhlükəsizliyinin qorunması gələcək nəslin daha sağlam, firavan yaşaması deməkdir.

Araşdırmalardan məlum oldu ki, müasir dövrdə reklam-marketing internetin əsas xidmət növlərindən biri olmaqla insanların gündəlik tələbatına çevrilmişdir. Bu sahədə informasiya təhlükəsizliyi vacib problemlərdən biridir və bu problemin həlli kompleks tədbirlər tələb edir. Bununla bağlı təkliflər məqalədə öz əksini tapmışdır.

İşlənmiş təkliflər internetdə reklam-marketing məsələlərinin səmərəliliyi artırmaq üçün əsas şərtdir.

ƏDƏBİYYAT

- [1] Безопасность данных и онлайн-реклама в эпоху мультитэкранности. https://habr.com/company/advertone_ru/blog/237853/
- [2] R.Giorgiyev, Голосовыми помощниками Apple, Google и Amazon можно манипулировать замаскированными в рекламе звуками. http://www.cnews.ru/news/top/2018-10-04_golos_ovymi_pomoshchnikami_applegoogle_i_amazon
- [3] Аудит информационной безопасности. <https://csbi-it.ru/ib>
- [4] Анатомия рекомендательных систем. <https://habr.com/company/lanit/blog/420499/>
- [5] E.Hüseynov, Brauzerdəki bezdirci reklamlardan qurtulun!. <https://compboard.az/085122017>
- [6] XSS qarşısını almaq üçün üsullar. DOM modelində XSS arasındakı fərq nədir. <https://vism.ru/az/what-is-scripting-methods-for-preventing-xss.html>
- [7] М.Ксендик, Безопасность интернет-магазина: что и почему нужно защищать. <https://biz.liga.net/all/it/article/bezopasnost-internet-magazina-cto-i-pochemu-nujno-zaschischat>
- [8] Dünyada internet istifadəçilərinin 5 faizi reklamı bloklamağa üstünlük verir. <http://ictnews.az/read-35955-news-1.html>
- [9] lab russia запустила механизм «безопасной гавани» для качественной интернет-рекламы. <https://iabrus.ru/news/1189>
- [10] K.Soltanova, Təhlükəsiz onlayn alış-veriş üçün 9 tövsiyə. <http://banco.az/az/news/tehlukesiz-onlayn-alis-veris-ucun-9-tovsiye>

INTERNET-ADVERTISING MARKETING PROBLEMS AND THEIR SOLUTIONS

Kamala Hashimova

Institute of Information Technology of ANAS
Baku, Azerbaijan

multimedia@iit.science.az

Abstract – The more the global scope of the Internet grows and its capabilities increase, the more demand for the Internet advertising increases. This study focuses on the possibilities of advertising marketing considered for the Internet, and the prospects for using the recommendation systems, and identifies the threats. Suggestions for effective use of advertising-marketing systems placed on websites are also put forward.

Keywords- Internet advertising marketing; recommendation systems; attack; rating; online advertising

İnformasiya iqtisadiyyatının kibertəhlükəsizliyinin təminatı istiqamətləri və texnologiyaları

Ələvsət Əliyev

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

alovsat_qaraca@mail.ru

Xülasə – Məqalədə İKT-yə əsaslanan yeni tipli iqtisadiyyatın formalaşma xüsusiyyətləri təhlil olunmuş və iqtisadiyyatın inkişafına olan əsas risklər və təhlükələr göstərilmişdir. İqtisadi təhlükəsizlik səviyyəsini xarakterizə edən göstəricilər sistemi şərh edilmişdir. Yeni iqtisadiyyatda informasiya infrastrukturunu və texnologiyalarının vəzifələri müəyyənləşdirilmişdir. Rəqəmsal iqtisadiyyat sektorlarında informasiya təhlükəsizliyi mənbələri və baza texnologiyaları araşdırılmışdır. İnformasiya iqtisadiyyatının kibertəhlükəsizliyi istiqamətləri və müvafiq texnologiyaları təklif edilmişdir.

Açar sözlər — *informasiya iqtisadiyyatı, iqtisadiyyatın informasiyalaşdırılması, iqtisadi təhlükəsizlik səviyyəsi, rəqəmsal iqtisadiyyat, kibertəhlükəsizlik, təhlükəsizlik texnologiyaları*

I. GİRİŞ

İqtisadiyyatı daha çox inkişaf edən ölkələrin təcrübəsi göstərir ki, hazırda global iqtisadi inkişaf innovativ texnologiyalara, biliklərə və informasiyaya əsaslanır. Hazırkı dövrdə iqtisadiyyatın davamlı inkişafına nail olmaq, sosialyönümlü, diversifikasiya olunmuş yeni milli iqtisadiyyatların formalaşdırılmasını həyata keçirmək aktual məsələlərdəndir. Makroiqtisadi sabitlik, regionların sürətli inkişafı, əlverişli biznes və investisiya mühiti əsasında tarazlı iqtisadi inkişaf modelini daha da təkmilləşdirmək tələb olunur. Bu tədbirlərin əsas məqsədi iqtisadi davamlılığın və dayanıqlılığın gücləndirilməsi, müəssisələrin səmərəliliyinin artırılması yolu ilə iqtisadi dinamikliyin təmini, insan kapitalının inkişafı və biznes mühitinin daha da yaxşılaşdırılmasından ibarətdir. Burada əsas vasitə İKT-nin inkişaf potensialının artırılması, İKT infrastrukturunun təkmilləşdirilməsi, iqtisadiyyatın rəqəmsallaşdırılması, dövlət sektorunda İKT-nin tətbiqi ilə idarəetmənin səmərəliliyinin artırılması, innovasiyayönümlü, informasiya və biliyə əsaslanan iqtisadiyyatın qurulması, bazarlara rəqabətə davamlı İKT məhsullarının çıxarılması, yüksək texnologiyalara əsaslanan yeni investisiya layihələrinin ölkəyə cəlb edilməsidir [1].

İnformasiya və biliklərə əsaslanan cəmiyyətin qurulması, yüksək texnologiyalar parklarının yaradılması, elektron informasiya resurslarının inkişaf etdirilməsi, bank, maliyyə, ticarət, təhsil, tibb və s. sosia-iqtisadi sahələrdə elektron xidmətlərin daha geniş tətbiqi, regionlarda proqram vasitələrinin və texnoloji avadanlıqların istehsalının təşkili və inkişaf etdirilməsi formalaşmaqda olan informasiya

iqtisadiyyatının əsas inkişaf istiqamətləridir. Ona görə də sosialyönümlü liberal bazar iqtisadiyyatına əsaslanan müasir informasiya və biliklər iqtisadiyyatı sektorlarının iqtisadi təhlükəsizliyinə ciddi ehtiyac yaranmışdır. Bu problemin kifayət qədər aktual xarakter daşması həm 2020-ci ilə qədərki dövr üçün İnformasiya Cəmiyyətinin inkişafına dair Milli Strategiyada [2], həm də 2025 və daha sonrakı dövrlər üçün milli iqtisadiyyat sektorlarının, xüsusilə telekommunikasiya və informasiya texnologiyalarının inkişafı üzrə strateji yol xəritələrində [3] təsbit olunmuşdur.

İnformasiya və biliklərə əsaslanan intellektual cəmiyyətin və iqtisadiyyatın təhlükəsiz və dayanıqlı formalaşdırılması dövlət və cəmiyyət qarşısında qoyulan əsas məqsədlərdəndir. Ona görə də yeni iqtisadiyyatda təhlükəsizlik məsələlərinin araşdırılması və çox mühüm əhəmiyyətli faktor kimi dəyərləndirilməsi kifayət qədər aktualdır.

II. İKT-YƏ ƏSASLANAN YENİ TIPLI İQTİSADİYYATIN FORMALAŞMA XÜSUSİYYƏTLƏRİ

İqtisadiyyatın İKT əsasında inkişaf etdirilməsi müasir zamanın əsas tələblərindən biridir. Azərbaycanın öz iqtisadiyyatını Avropa iqtisadiyyatına inteqrasiya etdirməsi üçün iqtisadiyyatın informasiyalaşdırılması daha səmərəli və düzgün şəkildə həyata keçirilməlidir [4].

Sosial-iqtisadi və digər sahələrin informasiyalaşdırılması istiqamətində [5] həm xidmət, ictimai-siyasi, humanitar sferalarda, həm də istehsal-sənaye, energetika, kənd təsərrüfatı və nəqliyyat sahələrində nisbətən mühüm potensial vardır. Xüsusilə, energetika sahəsinin, aqrar sektorun müasir İKT-dən istifadə əsasında inkişafı, nəqliyyat sahəsində yeni texnologiyaların tətbiqi həmin sahələrin effektiv idarə olunmasına əlavə imkanlar yaradır.

Bütün bu kimi real iqtisadi sahələrin və proseslərin səmərəli inkişafının kökündə İKT və cəmiyyətin kütləvi surətdə informasiyalaşdırılması dayanır. İqtisadiyyatın informasiyalaşdırılması və informasiya cəmiyyəti quruculuğu prosesi arasında sıx əlaqə mövcuddur və onlar bir-birinə ciddi qarşılıqlı təsir göstərən aktual məsələlərdir.

İKT-yə əsaslanan iqtisadiyyatın formalaşması konsepsiyası iqtisadiyyat elmində mövcud olan resursyönümlü iqtisadiyyat, ekoloji iqtisadiyyat, ətraf mühitin iqtisadiyyatı və

s. kimi bir çox istiqamətlərin ideyalarını özündə birləşdirir. İKT əsaslı iqtisadiyyatda milli və beynəlxalq səviyyələrdə təbii resurslardan daha səmərəli istifadə olunur, yeni iş yerlərinin yaradılmasının hesabına əhalinin məşğulluğu daha səmərəli təmin olunur, davamlı inkişafın nailiyyəti üçün bazar mexanizmlərindən düzgün istifadə olunur. İKT əsaslı yeni iqtisadiyyat dayanıqlı inkişafa keçid prosesinin sürətlənməsinə yaxşı imkan yaradır.

İKT əsaslı iqtisadiyata keçidin zəruriliyi ondadır ki, insanın ətraf mühitə müsbət təsir imkanı daima genişlənir. İnsanın İKT vasitəsilə təsir imkanları artır. İKT bərpa olunmayan təbii ehtiyatların səmərəli inkişafına kömək edir.

Bəşəriyyət üzləşdiyi ekoloji, sosial və iqtisadi problemlərin həlli üçün İKT-yə əsaslanan yeni yanaşmalardan istifadə etməlidir. Ona görə də, hesab etmək olar ki, İKT-yə əsaslanan yeni əmək fəaliyyəti, yeni iqtisadiyyat, yeni istehsal, yeni təfəkkür və yeni həyat tərzı gələcək həyatımızın əsas komponentlərinə çevrilməlidir.

Hazırda dünyanın inkişaf tendensiyalarına müvafiq olaraq sənaye iqtisadiyyatı daha çox İKT və digər “yaşıl” texnologiyalar əsasında inkişaf etdirilir. Sənaye iqtisadiyyatının ən böyük magistral inkişaf yolu elə informasiyalaşmadan, İKT-dən keçir.

İstehsalın və idarəetmə proseslərinin informasiyalaşdırılması istiqamətində kifayət qədər inkişaf potensialı vardır. İqtisadiyyatın inkişafı tezisində ilkin olaraq iqtisadiyyatın informasiyalaşdırılması kontekstində baxmaq, informasiya iqtisadiyyatının innovativ üsullarla inkişaf etdirilməsi texnologiyalarının tətbiqinə nail olmaq olar. Bu isə nəticə etibarı ilə innovativ informasiya iqtisadiyyatı sektorlarının formalaşması və inkişaf etdirilməsidir.

Müasir dövrdə ənənəvi iqtisadi sahələrin informasiyalaşdırılması ilə yanaşı, elə sahələr də mövcuddur ki, orada inkişaf və informasiyalaşdırma üçün böyük potensial vardır. Belə sahələrə aşağıdakıları aid etmək olar[6]:

- enerji resurslarının səmərəli bölüşdürülməsi vasitəsilə qənaətedici texnologiyalar;
- iqtisadiyyatın bütün sahələrində yeni innovativ texnologiyaların yaradılması və tətbiqi vasitəsilə resurslardan səmərəli istifadə texnologiyaları;
- kənd təsərrüfatı sferasında İKT vasitəsilə işlərin səmərəli təşkili və resurslardan səmərəli istifadə texnologiyaları;
- tikinti sektorunda, nəqliyyatda, sənaye sahələrində, idarəetmə işlərində, resursların səmərəli yerləşdirilməsində İKT-nin tətbiqi;
- şəhər təsərrüfatının idarə olunmasında, bələdiyyələrin fəaliyyətinin təşkilində, mənzil fondunun istifadəsində İKT amilindən yararlanma;
- ekoloji sahədə, təbiətin mühafizəsində, geoloji axtarışlarda, turizm sahəsində İKT-nin imkanlarından istifadə və s.

İnformasiyalaşdırma nəticəsində innovativ informasiya iqtisadiyyatı formalaşdıqca bir çox təhlükə yarada biləcək problemlər də meydana çıxır ki, onları müvafiq təhlükəsizlik

texnologiyalarının işlənilməsi və tətbiqi hesabına aradan qaldırmaq və ya qarşısını almaq olar .

III. İQTİSADI TƏHLÜKƏSİZLİK SƏVİYYƏSİ VƏ İQTİSADIYYATDA ƏSAS TƏHLÜKƏLƏR

Müasir qloballaşma və integrasiya proseslərinin sürətləndiyi, eləcə də, beynəlxalq rəqabətin daha da kəskinləşdiyi şəraitdə satış bazarları, texnoloji, informasiya, maliyyə, insan və təbiət resursları üzərində nəzarət sahəsində hər bir ölkənin milli və iqtisadi təhlükəsizliyi problemi daha da aktuallaşır və strateji xarakterə malik olur. Dünya iqtisadiyyatının böhranları fonunda hər bir dövlətin özünün milli maraqları mövcuddur ki, onları yalnız ölkənin iqtisadi təhlükəsizliyinin dayanıqlığı şəraitində qorumaq mümkündür. Dövlətin iqtisadi təhlükəsizlik səviyyəsi müəyyən keyfiyyət kriteriyaları və indikatorlarla xarakterizə olunur. Bu istiqamətdə C.Y.Qlazyev 22 əsas göstərici (istehsal dinamikası, milli büdcə, dövlət borcu və s.), V.K.Sençaqov isə 16 göstərici (azgəlirli əhalinin nisbəti, çoxgəlirli əhalinin nisbəti və s.) təklif etmişdir. İqtisadi təhlükəsizliyi, ümumilikdə, 150-dən çox göstərici xarakterizə edir. Bütün bunlarla yanaşı olaraq, [4]-də iqtisadi təhlükəsizliyi xarakterizə edən 18 əsas indikator verilmişdir. Onlardan 8-i makro xarakterli iqtisadi göstəricilər, 10-u isə orta və aşağı idarəetmə səviyyələrinə aid edilə bilən iqtisadi göstəricilər hesab oluna bilər.

Aparılan tədqiqatlar göstərir ki, [7, 8] milli iqtisadiyyatların əksəriyyəti üçün əsas təhlükələr sənaye istehsalının aşağı səviyyədə olması, ölkə iqtisadiyyatının məhsul idxalından və xammal ixracından asılılığı, əhalinin aşağı həyat səviyyəsi, kölgə iqtisadiyyatının inkişafı, korupsiyanın artması, elmin, təhsilin, innovasiyanın inkişafdan qalması və ya zəif inkişafı, güclü beyin axınının olması və s. kimi çox ciddi problemlərdir.

IV. YENİ İQTİSADIYYATDA İNFORMASIYA İNFRASTRUKTURU VƏ TEXNOLOGİYALARININ ROLU VƏ VƏZİFƏLƏRİ

Əvvəlki bölmədə göstərilən təhlükələrin hamısının çox mühüm iqtisadi xarakterizə malik olması ilə yanaşı, qeyd olunmalıdır ki, milli iqtisadiyyatın iqtisadi təhlükəsizlik səviyyəsinin dayanıqlı təmini tamamilə və birbaşa olaraq onun informasiya təhlükəsizliyinin səviyyəsindən asılıdır [6, 9].

Yeni iqtisadiyyatın qarşısında ənənəvi sənaye iqtisadiyyatının vəzifələri ilə yanaşı yeni tələblər, məsələlər və məqsədlər qoyulmuşdur. Bunlar ölkə vətəndaşlarının maddi və mənəvi rifah halının, həyat keyfiyyətinin yaxşılaşdırılması üçün həm ənənəvi, həm də rəqəmsal formada olan məhsullara xidmətlə olan tələbatlarını daha dolğun və səmərəli şəkildə ödənilməsindən ibarətdir. Bu isə rəqəmsal texnologiyalardan

daha geniş istifadə, əhalinin rəqəmsal savadlılığının artırılması, insanların informasiya ilə təmin olunmaq səviyyəsinin yüksəlməsi, dövlət xidmətlərinə əlçatanlığın asanlaşması şəraitində mümkündür. Ona görə də hesab olunur ki, formalaşmaqda olan müasir informasiya və bilik iqtisadiyyatı [10, 11] ancaq ən yüksək İKT infrastrukturunu, kommunikasiya-rabitə vasitələri və kiber-fiziki sistemlərdən ibarət platformada effektiv fəaliyyət göstərə bilər. Belə platforma isə təhdid və təhlükələrdən qoruna bilən yüksək inkişaf etmiş informasiya təhlükəsizliyi sisteminə, etibarlı telekommunikasiya şəbəkəsinə, naqilsiz xətlərə, daimi monitorinq sistemlərinə, texniki tənzimləyici strukturlara, müvafiq yüksəkixtisaslı personala, yüksək səviyyədə təşkilati, hüquqi, maliyyə, normativ, ekoloji, sosial problemlərin operativ həllinə imkan verən mexanizmlərə malik olmalıdır.

Göründüyü kimi, burada əsas məsələ informasiya infrastrukturunu və təhlükəsizliyinin səmərəli həllinə nail olmaqdır. Bu istiqamətdə ən qlobal texnologiyaların tətbiq olunması üçün yeni bilik və texnologiyaların müvafiq sahələrdə praktiki reallaşdırılması məqsədilə transferini həyata keçirən ixtisaslaşdırılmış texnomərkəzlər, texnopolislər, texnoparklar və s. yaradılmalıdır [12].

V. İNFORMASIYA İQTİSADİYYATI SEKTORLARINDA İNFORMASIYA TƏHLÜKƏSİZLİYİ MƏNBƏLƏRİ VƏ TEKNOLOGİYALARI

İnformasiya iqtisadiyyatı sektorlarında tam informasiya təhlükəsizliyinin təmini üçün üç əsas - təmlik, gizlilik və əlyətərliklik prinsiplərinə tamamilə əməl olunmalıdır [13].

Rəqəmsal iqtisadiyyat sektorlarında [14] informasiya resurslarının, sistemlərinin, məhsul və xidmətlərin informasiya təhlükəsizliyi daha çox aşağıdakı kimi risklərə, təhdid və təhlükələrə məruz qala bilər [15]:

- rəqəmsal mühitdə insanların özəl həyatının toxunulmazlığı, şəxsiyyət əleyhinə yönəlmiş təhdidlərin qarşısının alınması, şəxsi hüquqlarının təmini, şəxslərin identifikasiyası, onlara aid fərdi verilənlərin saxlanması və qorunması, onların inamının yüksəldilməsi
- şəxsiyyətə, biznesə, dövlətə ierarxik telekommunikasiya sistemlərindən və resurslarından uzaqdan istifadə zamanı yaranan təhlükə və təhdidlər;
- kritik informasiya infrastrukturuna xarici informasiya-texniki təsir imkanlarının artması;
- daxili və xarici kompüter cinayətkarlığı səviyyəsinin yüksəlməsi;
- aparıcı, güclü xarici dövlətlərdən İKT-nin inkişaf səviyyəsinə görə geridə qalmaq;
- sosial-iqtisadi inkişafın xarici dövlətlərin ixrac siyasətindən asılılığı;

- İKT-nin inkişafı və təhlükəsizliyi aspektində elmi-tədqiqat işlərinin nisbi zəifliyi, kifayət qədər yüksəkixtisaslı müvafiq personalın olmaması.

Göstərilən bu və ya digər təhlükəkarın zamanında qarşısının alınması üçün xüsusi aparat-texniki və proqram vasitələrinin işlənilməsi məqsədəuyğundur. Ancaq belə xüsusi texnologiyaların işlənilməsi çox çətin olduğundan və böyük maliyyə vəsaitləri tələb etdiyindən, heç olmasa, bütün iqtisadi sahələrdə istifadə oluna bilən standart, baza, universal texnologiyaların tətbiq olunması zəruridir [16].

Müvafiq iqtisadi informasiya texnologiyalarını aşağıdakı kimi qruplaşdırmaq olar:

- yüksək və çox yüksək məhsuldarlıqlı superkompüter texnologiyaları;
- kiber-fiziki sistemlərin, komplekslərin aparat-texniki vasitələrinin yaradılması texnologiyaları;
- kiber-bioloji insan-maşın sistemlərinin yaradılması texnologiyaları;
- verilənlərin sürətli yığılı, emalı, ötürülməsi üzrə kvant texnologiyaları;
- pilotsuz sistemlər və robototexniki texnologiyalar;
- Sənaye İnterneti və Əşyaların interneti texnologiyaları;
- iqtisadi-riyazi və imitasiya modelləşməsi, ehtiyatların və növbələrin idarə olunması texnologiyaları;
- neyroşəbəkə, genetik və digər koqnitiv texnologiyalar;
- duman-bulud hesablamaları texnologiyaları;
- böyük verilənlərin yığılı, emalı (Big-data) texnologiyaları;
- virtual mühit və reallıq texnologiyaları;
- paylanmış hesablamalar və verilənlər texnologiyaları;
- blokçeyn və digər maliyyə texnologiyaları;
- proqram mühəndisliyi texnologiyaları və s.;

Aparılan təhlil və araşdırmalar göstərir ki, ümumiyyətcə formalaşmaqda olan informasiya iqtisadiyyatının və onun sektorlarının dinamik inkişafı üçün tətbiq olunan əsas qabaqcıl texnologiyalar sırasına böyük verilənlər, neyroteknologiyalar və süni intellekt, blokçeyn texnologiyaları, kvant texnologiyaları, yeni istehsal, loqistik, satış, idarəetmə texnologiyaları, Sənaye İnterneti, robototexnika, sensor texnologiyaları, naqilsiz rabitə texnologiyaları, virtual reallıq texnologiyaları, soft-komputinq texnologiyaları, kriptografik texnologiyalar, mürəkkəb böyük hesablama texnologiyaları, bulud-duman texnologiyaları və s. kimilər daxildir [17]. Bu cür qabaqcıl texnologiyaların tətbiqi zamanı risk və təhlükələrin azaldılması istiqamətləri daha çox: a) şəxsiyyətin, cəmiyyətin, dövlətin daxili və xarici informasiya təhlükəsizliyinin müdafiəsinə, b) vətəndaşların ləyaqətli, keyfiyyətli yaşam tərzinə, c) ölkənin dayanıqlı

sosial-iqtisadi inkişafına və suverenliyinə yönləndirilmişdir. Bu kompleks istiqamətləri aşağıdakı kimi tədbirlərin yerinə yetirilməsiylə ifadə etmək olar:

- verilənlərin emalı mərkəzləri infrastrukturunun və aparat vasitələrinin fəaliyyətinin təhlükəsizliyinin və texnoloji müstəqilliyinin təmini;
- İnternet şəbəkəsinin ölkə seqmentinin təhlükəsiz fəaliyyətinin təmini;
- yeni iqtisadi şəraitdə kiber-fiziki sistemlərin fəaliyyət mexanizmlərinin işlənməsi və onların təhlükəsiz icrasının təmini;
- kiber-fiziki sistemlərin fəaliyyəti üçün inam mühitinin formalaşdırılması üçün zəruri əsasların yaradılması;
- müxtəlif səviyyəli və təyinatlı informasiya sistemlərinin və texnologiyalarının təhlükəsizliyinin və dayanıqlılığının təmini;
- yeni iqtisadi şəraitdə informasiya təhlükəsizliyi üzrə beynəlxalq qarşılıqlı əlaqələrin təmini;
- beynəlxalq iqtisadi informasiya fəzaları ilə integrasiya olunan informasiya resurslarının, sistemlərinin təhlükəsizliyinin təmini və s.

Göstərilən tədbirlər informasiya təhlükəsizliyi sistemlərinin, interfeyslərinin, elementlərarası qarşılıqlı əlaqə protokollarının, aparat vasitələrinin yeni idarəetmə konsepsiyasının işlənməsini tələb edir [18].

Bunlarla yanaşı bir sıra informasiya təhlükəsizliyi texnologiyaları da qeyd edilən məqsəd üçün çox əhəmiyyətlidir [19]:

- kiberfəzaya nəzarət, kompüter hücumlarının qarşısının əvvəldən alınmasına xidmət edən koqnitiv texnologiyalar;
- rəqiblərin vəziyyətinin avtomatlaşdırılmış modeləşdirilməsi və proqnozlaşdırılması texnologiyaları;
- big data əsaslı proseslərin informasiya təhlükəsizliyi təminatının intellektual texnologiyaları;
- təhlükəsizliyin arxitektura-adaptiv texnologiyaları;
- program konfigurasiyalı şəbəkə və şəbəkə funksiyalarının virtualaşması texnologiyaları;
- kriptografik modullar texnologiyaları;
- sənaye və Əşyaların İnternetinin təhlükəsizliyi texnologiyaları;
- təhlükəsiz bulud-duman və mobil texnologiyaları.

NƏTİCƏ

Beləliklə yekunda qeyd olunmalıdır ki, ölkə iqtisadiyyatının informasiya təhlükəsizliyinə yalnız sistemli yanaşma əsasında nail olmaq olar. Burada həm qanunvericilik

aspektində inzibati mexanizmlərdən, həm effektiv təşkilati tədbirlərdən, həm də müvafiq müasir aparat-texniki vasitə və texnologiyalardan kompleks şəkildə istifadə olunmalıdır.

ƏDƏBİYYAT

- [1] Azərbaycan - 2020: Gələcəyə Baxış” İnkişaf Konsepsiyası. Bakı, 29 dekabr 2012-ci il. www.president.az
- [2] Azərbaycan Respublikasında İnformasiya Cəmiyyətinin İnkişafına dair 2014-2020-ci illər üçün Milli Strategiya. 02.04.2014-cü il, www.president.az
- [3] Milli iqtisadiyyat və iqtisadiyyatın əsas sektorları üzrə Strateji Yol Xəritələri. Bakı, 6 dekabr 2016-cı il. www.president.az
- [4] Алиев А.Г. Проблемы информатизации общества и экономики // Баку, “ЭЛМ”, 2003, 460 с.
- [5] Алиев А.Г. Теоретико-прикладные аспекты информатизации гуманитарных отраслей // Баку, “ЭЛМ”, 2006 г., 474 с.
- [6] Ə.Q.Əliyev, E.H.Musayeva, V.Ə.Abbasova, L.Ə.Əkbərova, İqtisadiyyatın informasiyalaşdırılmasının bəzi təhlükəsizlik aspektləri // “İnformasiya təhlükəsizliyinin multidissiplinar problemləri” üzrə II respublika elmi-praktiki konfransı. Bakı, 14may, 2015, səh.148-149
- [7] Григорьева В.В., Струков Г.Н., Слепокурова Ю.И., Слепокурова А.А. Экономическая безопасность Российской Федерации: современное состояние, уровень и угрозы. Вестник ВГУИТ. 2017. Т. 79. №3. Стр.238-252
- [8] Ясенов В.Н. Информационная безопасность в экономических системах. Н. Новгород, 2006, 253 стр.
- [9] Əliyev Ə.Q. İnformasiya sistemlərinin təhlükəsizliyinə vurulan ziyanların kompleks qiymətləndirilməsi məsələləri. “İnformasiya təhlükəsizliyi problemləri” I Respublika elmi-praktiki konfransı. Bakı, 16-17 may 2013, səh.71-74
- [10] Alguliyev R.M., Aliyev A.G., Abbasova V.A. The study of formation characteristics and development tendencies of international information and knowledge economy. J. Review of knowledge economy. 2017, vol.4, No.1, pp.7-14. <http://www.conscientiabeam.com/archive/67/06-2017/1>
- [11] Aliyev A.G. Methodological aspects of estimation of ICT-based economic development. International Journal Management Dynamics in the Knowledge Economy. 2018, vol.6 no.2, pp.227-245
- [12] Əliyev Ə.Q., Şahverdiyeva R.O. İnnovativ struktur və proseslərin idarə olunmasında informasiya təhlükəsizliyi məsələləri. “İnformasiya təhlükəsizliyinin multidissiplinar problemləri” üzrə II respublika elmi-praktiki konfransı. Bakı, 14 may, 2015, səh.66-69
- [13] Boban, Marija. Information security and the right to privacy in digital economy- the case of republic of Croatia. Conference: 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).Croatia, may 26-30, 2014, pp.1503-1508
- [14] Цифровая экономика: основные направления развития. Монография / Под научной редакцией Н.В. Апатовой. Симферополь, 2018
- [15] Vinze Ajay S., Raghu T. Information security in the knowledge economy. Int. J. Human-Computer Studies 65 (2007) pp.1-2
- [16] Минзов А.С., Невский А.Ю., Баранов О.Ю. Информационная безопасность в цифровой экономике. Ж., ИТНОУ, 2018, №3, стр.52-59
- [17] Мамаева Л.Н. Характерные проблемы информационной безопасности в современной экономике. Научно-практический журнал «Информационная безопасность регионов». 2016. № 1(22), стр.21-24
- [18] Светлаков А. Г., Глотина И. М. Влияние информационного пространства на экономическую безопасность региона // Экономика региона. - 2018. - Т. 14, вып. 2, с. 474-484

[19]Петренко С.А. Вызовы и угрозы безопасности цифровой экономики Российской Федерации. Финансово-экономическое и информационное обеспечение инновационного развития региона. Сборник материалов Всероссийской научно-практической конференции. 2018, стр.74-77

**CYBERSECURITY TECHNOLOGIES AND
DIRECTION IN THE INFORMATION ECONOMY**

Alovsat G.Aliyev

Institute of Information Technology of ANAS,

Baku, Azerbaijan

alovsat_qaraca@mail.ru

Abstract – In the article, the features of the new type of economy based on ICT have been analyzed .The main risks and threats on the development of the economy are shown. The system of indicators describing the level of economic security has been commented. The tasks of information infrastructure and technology have been defined in the new economy. Sources of information security and basic technologies have been researched in the digital economics sectors. Relevant technologies have been proposed for cyber security in the information economy.

Keywords – information economy, informatization of economy, economic security, digital economy, cyber security, security technologies

IoT arxitekturunun səviyyələr üzrə təhlükəsizlik məsələləri

Şəlalə Mansurova

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

fmv.shalala@gmail.com

Xülasə— Paylanmış miqyaslanan hesablama paradigmalarının inkişafı nəticəsində Əşyaların interneti (Internet of Things— IoT) texnologiyalarının istifadəsi getdikcə artmaqdadır. IoT konsepsiyasının belə geniş miqyaslı tətbiqi bu yeni tədqiqat sahəsinin təhlükəsizlik aspektindən araşdırılmasını zəruri hala çevirmişdir. Məqalədə Əşyaların interneti konsepsiyasının arxitekturası nəzərdən keçirilir. Qeyd olunan hər bir səviyyə üzrə təhlükəsizlik məsələlərinə baxılır, mövcud təhdidlər və həlləri araşdırılır.

Açar sözlər—IoT; IoT arxitekturası; IoT təhlükəsizliyi; verilənlərin təhlükəsizliyi

I. GİRİŞ

Hazırda gündəlik olaraq böyük miqdarda— terabayt və petabaytlarla verilənlər toplanaraq kompüter şəbəkələrinə, internetə və müxtəlif verilənlər saxlancına axın edir. Verilənlərin həcmnin bu sıçrayışlı artımı böyük verilənlər (big data) anlayışının yaranmasına səbəb olmuşdur. Bu isə cəmiyyətin kompüterləşməsinin, verilənlərin toplanması və saxlanması vasitələrinin sürətli inkişafının nəticəsidir. Verilənlərin həcmnin belə eksponensial artımı resursların miqyaslanmasını reallaşdıran müxtəlif yeni texnologiyaların yaranmasını şərtləndirmişdir. Paylanmış miqyaslanan hesablama paradigmalarının inkişafı olaraq, bulud, duman və şəh texnologiyaları meydana çıxmışdır. Bunun nəticəsində də coğrafi olaraq geniş yayılmış, miqyaslanan, real zamanda emal bacarığına malik olan, yüksək hesablama və yaddaş resursları ilə təmin olunan hesablama sistemi əldə edilmişdir.

Bulud, duman və şəh paylanmış texnologiyaları son 50 il ərzində hesablama sistemlərinin və əlaqəli texnologiyaların eksponensial inkişaf sürətinin nəticəsidir. Duman texnologiyaları əşyaların internetinə adekvat həll gətirən yeni konsepsiyadır. Əşyaların interneti obyektlərin İnternetə daxil olaraq bir-biri ilə və ya daha böyük sistemlərlə kommunikasiya yaratdığı şəbəkədir. IoT konsepsiyası üçün müxtəlif təhlükəsizlik həllərinə ehtiyac vardır. Hazırda bu mövzuda təhlükəsizlik məsələləri tam səviyyədə təmin olunmamışdır. Bu məqsədlə məqalədə IoT texnologiyasına olan təhlükəsizlik tələbləri diqqətə çatdırılır.

II. IOT KONSEPSİYASI

IoT proqram təminatları, sensorlar və qəbuledicilər vasitəsilə əşyaların bir-biri ilə qarşılıqlı əlaqəsini təmin edən

şəbəkəyə bağlanması və verilənləri ötürməsi olub, dinamik geniş miqyaslı mühitdir [4,8]. IoT internetə çıxışı olan kompüter, noutbuk, ağıllı telefonlar, tabletlər və s. kimi cihazlardan əlavə, həmçinin, digər ənənəvi "ağıllı olmayan" cihazların, əşyaların internetə çıxışını ehtiva edir. Çoxsaylı kiçik ölçülü, simsiz texnologiyaları istifadə edən qəbuledici cihazlar (sensorlar) vasitəsilə ətraf mühitdə baş verən bütün hadisələri izləmək mümkündür. Lakin sensorlardan toplanmış böyük verilənləri saxlamaq üçün böyük yaddaş tutumuna malik saxlanclara ehtiyac vardır.

A. IoT -un tətbiq sahələri

IoT konsepsiyasının tətbiq sahələri çox genişdir. Belə ki, neft və qaz sənayesi, ətraf mühitin monitorinqi, ağıllı evlər, nəqliyyatın intellektual idarəetməsi, elektron tibb və s. kimi müxtəlif sahələrdə geniş olaraq tətbiq edilə bilər. Nümunə olaraq qeyd etmək olar ki, sənaye və IoT konsepsiyasının inteqrasiyası nəticəsində istehsal proseslərinə cəlb olunan ağıllı cihazlar, insan xətasının minimuma endirilməsinə, real zamanda emal vasitəsilə qərarqəbulunun dəstəklənməsi sistemləri tərəfindən qiymətləndirmənin həyata keçirilməsinə nail olacaqdır. Bu isə istehsal zamanı keyfiyyətin yüksəldilməsinə, resursların optimal istismarını təmin etməklə maliyyə xərclərinin azaldılmasına, rəqabətə davamlı məhsulların istehsalına gətirib çıxaracaqdır.

1) *Sənayedə istifadə olunan IoT qurğular* [6]: Mövcud sənayenin avtomatlaşdırması sistemlərinin IoT qurğuları ilə birgə istifadəsi bir çox mühüm üstünlüklərə malikdir:

- IoT xüsusiyyətlərinə malik smart cihazlar şəbəkə üzərindən bir-biri ilə avtomatik kommunikasiya yaratmaqla istehsal prosesinə nəzarət edə və operatorun müdaxiləsini minimuma endirə bilər;
- Baş verə biləcək xətlər öncədən müəyyənləşdirilməklə proqnozlaşdırılan nasazlıqlara qarşı bərpa/mühafizə tədbirləri həyata keçirilə bilər;
- Zavod və ya şirkətlərin istehsal üçün xammal çatışmazlığı öncədən müəyyənləşdirilməklə vaxtında lazımı miqdarla təmin oluna bilər;
- Zavod və ya şirkətlərdə nəzarət məsələləri dünyanın istənilən nöqtəsindən həyata keçirilə bilər. Belə ki, istehsal prosesi və baş vermiş nasazlıqlarla bağlı

məlumatlar şəbəkəyə qoşulmaqla istənilən məkandan əlçatandır.

B. IoT arxitekturası

Sahələrdə obyektlərə yerləşdirilmiş qəbuledici cihazlar/sensorlardan toplanılan verilənlər, RFID və ya istənilən kabelsiz ötürmə mühitləri vasitəsilə monitoring və nəzarət mərkəzinə davamlı olaraq ötürülür, real zaman anında onlayn şəkildə izlənilir.

Funksionallıq baxımından IoT arxitekturası aşağıdakı səviyyələr üzrə ayrılmışdır (cədvəl.1):

CƏDVƏL 1. IoT ARXİTEKTURASI

Səviyyələr üzrə IoT arxitekturası	Səviyyələrin xarakteristikaları
Qəbuledici səviyyə	Fiziki mühitdən verilənləri əldə etmək üçün mövcud avadanlıqlarla (RFID, sensorlar, aktuatorlar və s.) integrasiya edilmiş səviyyə
Şəbəkə səviyyəsi	Simli və ya simsiz şəbəkə vasitəsilə sensorların, qəbuledici cihazların bir-biri ilə qarşılıqlı əlaqəsini və şəbəkə üzərindən verilənlərin nəql olunmasını təmin edən səviyyə
Tətbiq səviyyəsi	İstifadəçi və digər tətbiqlərlə qarşılıqlı əlaqə metodlarını təmin edən interfeys səviyyəsi (SCADA, DCS və s.)

III. IoT ARXİTEKTURUNDA SƏVİYYƏLƏR ÜZRƏ TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

IoT konsepsiyasında təhlükəsizlik məsələləri onun geniş tətbiqi ilə birbaşa əlaqələndirilir. Verilənlərin təhlükəsizliyinə aid mövcud həllərin Əşyaların interneti konsepsiyasına tətbiqi təhlükəsizliyi ciddi səviyyədə təmin olunmayan ötürmə mühitləri, dinamik və böyük miqyaslı olması, heterogen mənşəli cihazlar çoxluğu və s. kimi səbəblərdən effektiv hesab edilmir. Ötürmə zamanı böyük həcmli verilənlərin məxfi məlumatları özündə saxladığı nəzərə alındıqda verilənlərin təhlükəsizliyinin təmin edilməsi zəruri hala çevrilir. Ümumi halda IoT aşağıdakı səviyyələrdən ibarət arxitekturaya malikdir [1]: Qəbuledici səviyyə (persepsiya), şəbəkə səviyyəsi və tətbiq səviyyəsi. Əşyaların interneti arxitekturasında səviyyələr üzrə yerinə yetirilən proseslər fərqli olduğundan təhlükəsizlik məsələləri də səviyyələr üzrə fərqləndirilir. IoT konsepsiyasında təhlükəsizlik məsələləri qeyd olunan hər bir səviyyə üzrə müxtəlif yanaşma tələb edir. Belə ki, şəkil.1.-də IoT arxitekturası üzrə təhlükəsizliyin təmin olunması məsələləri aşağıdakı kimi qeyd olunmuşdur [2,3]:

A. Qəbuledici səviyyə

Qəbuledici səviyyə IoT arxitekturasında ən aşağı səviyyədir. Adətən sensor/ qəbuledici cihazlarda yaddaş tutumu, emal göstəriciləri yaxşı səviyyədə deyildir. Bu

səviyyədə təhlükəsizlik məsələlərinə sensor cihazların fiziki təhlükəsizliyinin təmin olunması və verilənlərin toplanılmasının təhlükəsizliyi daxildir. Burada təhlükəsizlik sistemlərinin qurulması çətindir və sensor verilənlərinin tamlıq, əlyətənlik və konfidensiallıq baxımından təhlükəsizliyinin təmin olunmasına ehtiyac vardır. Bununla yanaşı, DoS hücumları kimi xarici şəbəkə mühitindən olan hücumlar yeni təhlükəsizlik problemlərini ortaya qoyur. RFID, informasiya sızıntısı, təkrarlama hücumları, məlumatların izlənməsi, təhrif edilməsi, klonlama hücumları və “man-in-the-middle” hücumları kimi təhlükəsizlik problemlərini ehtiva edir [7].

Şəkil.1. IoT arxitekturasında səviyyələr üzrə təhlükəsizlik məsələləri

B. Şəbəkə səviyyəsi

Bu səviyyədə mövcud kommunikasiya təhlükəsizliyi mexanizmlərinin tətbiqi mürəkkəb və çətindir. İstifadəçi (subyekt) tərəfindən təqdim edilmiş məlumatların həqiqiliyinin yoxlanması— autentifikasiyası və subyektin sistemə əvvəlcədən yazılmış unikal məlumat vasitəsilə müəyyənəndirilməsi— identifikasiyası icazəsiz girişlərin qarşısını almaq üçün tətbiq edilən üsullardan biridir. Bu, təhlükəsizlik mexanizminin təməlidir, burada konfidensiallıq və tamlıq eyni dərəcədə əhəmiyyətlidir. Bundan başqa paylanmış DoS hücumları şəbəkədə ümumi hücum metodudur və xüsusilə əşyaların internetində bu hücum metodu daha aktual olduğundan paylanmış DoS hücumlarına qarşı həll yanaşması işlənilməlidir.

C. Tətbiq səviyyəsi

Tətbiq səviyyəsi IoT arxitekturasında ən yuxarı səviyyə olub, müxtəlif tətbiqlər mühiti üçün müxtəlif təhlükəsizlik tələbləri irəli sürür. Ümumi halda, tətbiq səviyyəsində təhlükəsizlik məsələlərinə izlənilmə və kənar müdaxilələr daxil edilir. Bu səviyyə ötürməyə nəzarət, trafikinin idarə olunması kimi proseslərə məsuliyyət daşımaqla yanaşı, eyni zamanda, verilənlərin anlaşıqlı, uyğun formaya çevrilməsi, sorğular göndərməklə verilənlərin toplanılması üçün istifadə edilən tətbiqi proqramların təmin edilməsi öhdəliklərini də özündə əks etdirir. Məsələn, tətbiqi səviyyədə verilənlərin paylaşılması verilənlərin gizliliyi, girişlərin idarə olunması və informasiyanın ifşa olunması kimi problemləri yarada bilər.

Sensor verilənlərinin tamlığı və həqiqiliyi tədqiqatın əsas diqqət mərkəzinə çevrilir [5]. Sensorlardakı digər əsas məqsəd

gizliliyin təmin olunmasıdır ki, bu da əsas problemlə situasiyalardan biridir. Fiziki mühitdə insan və obyektlərin gizliliyini qorumaq üçün mexanizmlər qəbul edilməlidir. Çox zaman insanlar ətrafdakı sensorlardan/qəbuledicilərdən bixəbərdir. Bu səbəbdən də insan hüquqlarının müdafiəsi üçün qaydalar qəbul edilməlidir.

NƏTİCƏ

Əşyaların interneti konsepsiyasında təhlükəsizliyin təmin olunması, mövcud təhdidlərdən mühafizə üsullarının yaradılması çətin və vacib məsələlərdən hesab edilir. Digər tərəfdən bizi əhatə edən ətraf aləmdə fiziki mühitlə bağlı qanun və qaydaların qəbul olunması zəruridir. Buna görə də aktual və yeni tədqiqat sahəsi kimi IoT konsepsiyası üçün mübahisəli məqamların aradan qaldırılmasına və təhlükəsizlik baxımından yaxşılaşdırılmasına ehtiyac vardır.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikasının Dövlət Neft Şirkətinin Elm Fondunun maliyyə yardımı ilə yerinə yetirilmişdir (Layihənin adı: **“Əşyaların interneti texnologiyalarının neft-qaz sənayesində tətbiqinin araşdırılması”**).

ƏDƏBİYYAT

- [1] A.V.Vijayalakshmi, Dr. L. Arockiam, “A Study on security issues and challenges In IoT”, International Journal of Engineering Sciences & Management Research, 2016, vol.3, no.11, pp.34-43
- [2] H. Suo, J. Wan, C. Zou and J. Liu, "Security in the Internet of Things: A Review," 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, 2012, pp.648-651
- [3] C.Suchitra, C.P.Vandana, “Internet of Things and Security Issues”, International Journal of Computer Science and Mobile Computing, 2016, vol. 5, issue.1, pp.133-139

- [4] M.U. Farooq, M.Waseem, S.Mazhar, “A Review on Internet of Things (IoT)”, International Journal of Computer Applications, 2015, vol.113, no.1, pp.1-7
- [5] Z.K.Zhang, C.W.Wang, C.W.Hsu, “IoT Security: Ongoing Challenges and Research Opportunities”, IEEE International Conference on Service-Oriented Computing and Applications, 2014, pp.230-234
- [6] J.Wurm, K.Hoang, O.Arias, “Security analysis on consumer and industrial IoT devices”, 21st Asia and South Pacific Design Automation Conference (ASP-DAC), 2016, pp.519-524
- [7] S.Vashi, J.Ram, J.Modi, "Internet of Things (IoT): A vision, architectural elements, and security issues", 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp.492-496
- [8] Əliquliyev R.M., Mahmudov R.Ş., “Əşyaların İnterneti: mahiyyəti, imkanları və problemləri”, İnformasiya cəmiyyəti problemləri, 2011, №2(4), s.29-40

SECURITY ISSUES ON LEVELS OF IOT ARCHITECTURE

Shalala Mansurova

Institute of Information Technology of ANAS, Baku,
Azerbaijan

fmv.shalala@gmail.com

Abstract -- As a result of the development on distributed scaling paradigms, Internet of Things (IoT) technology is increasingly used. Such a large-scale application of the IoT concept has made it necessary to study the security aspect of the novel research area. In the article, IoT architecture is reviewed, existing threats and solutions are being investigated.

Keywords -- IoT, IoT architecture, IoT security, data security

E-dövlətə kiberhücumlar və onlarla mübarizə üsulları haqqında

Günay İskəndərli

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

gunayniftali@gmail.com

Xülasə— E-dövlət hökumətin öz vətəndaşları ilə münasibətlərin yaxşılaşdırılmasına yönəlmiş səylərinin nəticəsidir. E-dövləti kiber-məkanda mövcud təhlükələrdən qorumaq üçün informasiya təhlükəsizliyinin ən yaxşı təcrübələrinə ehtiyac var. Təhlükəsizliyə dair siyasət, praktika və prosedurlar, eyni zamanda, təhlükəsizlik texnologiyasından istifadə e-dövlət sistemlərinin hücumdan müdafiə edilməsinə, qeyri-normal fəaliyyət göstərən xidmətlərin aşkar edilməsinə kömək edə bilər. Bunları nəzərə alaraq məqalədə kiber-təhlükəsizlik, e-dövlətə olan əsas kiber-hücumlar haqqında məlumat verilmişdir.

Açar sözlər— e-dövlət; informasiya təhlükəsizliyi, kiber hücumlar.

I. GİRİŞ

Kibertəhlükəsizlik XXI əsrin ən ciddi problemlərindəndir. Təhlükələr müxtəlif mənbələrdən yaranır və fərdlərə, biznesə, milli infrastrukturlara və hökumətlərə qarşı yönəlmiş dağıdıcı fəaliyyətlərdə özünü göstərir. Onların təsiri ictimai təhlükəsizlik, milli təhlükəsizlik və beynəlxalq ictimai sabitlik üçün ciddi risk daşıyır [1]. Bütün bunlar kiber təhlükəsizlik məsələlərinə, xüsusilə kiber-hüquqa olan diqqəti artırır.

Kiber hüquq qeyri-maddi rəqəmsal dünyada, məsələn, kiber məkanda qeyri-maddi məlumatlara hüquqi statusun verilməsi, belə məlumatların təhlükəsizliyi, məxfiliyinin təmin olunması, qanun pozuntularını tənzimləyən qanunlardır. Kiber-qanunlar kiber məsələləri tənzimləmək üçün əhəmiyyətli və etibarlı aktlar hesab olunur. Təhlükəsizlik dedikdə, əsasən hər hansı təşkilatın İKT aktivlərini qorumaq nəzərdə tutulur. Aktivlər dedikdə bura verilənlər, məlumatlar, bilik resursları, proqramlar, avadanlıqlar, şəbəkələr və s. kimi daxili və xarici resurslar daxildir. İKT sistemlərinin təhlükəsizliyinə olan təhdidlər bir çox mənbələrdən və müxtəlif formalarda ola bilər. Həmçinin təhdidlər fərqli növlərdə, ölçüdə və təsir gücündə ola bilər.

E-dövlət də hazırda bu cür təhdidlər üçün potensial resurs hesab olunur. E-dövlətdə daxili və xarici təhlükə mənbələri mövcuddur. Daxili təhlükə mənbələrindən bəziləri özəl və ya dövlət qurumlarının əməkdaşları, e-dövlət proqramlarının istifadəçiləri, xarici mənbələri isə xakerlər, cinayət/terrorçu qruplar və ya təşkilatlar, kəşfiyyat və istintaq orqanları ola bilər. Dövlət infrastrukturunu bu cür hücumlardan qorumaq hazırda aktual məsələlərdən biri hesab olunur. Bunları nəzərə alaraq məqalədə e-dövlət və kiber təhlükəsizlik məsələlərinə

toxunulmuş, məqalənin ikinci bölməsində kiber təhlükəsizlik, üçüncü bölməsində e-dövlətə olan kiber hücumlar haqqında ətraflı məlumat verilmiş, onların həll yolları göstərilmişdir.

II. KİBER-TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Kiber-təhlükəsizlik informasiya sistemlərinin (şəbəkələrin, kompüterlərin, məlumat bazalarının, məlumat mərkəzlərinin və təbiiqlərinin) müvafiq prosessual və texnoloji təhlükəsizlik tədbirləri ilə qorunmasıdır. Bu mənada kiber-təhlükəsizliyin təsviri olduqca ümumidir və bütün müdafiə tədbirlərini əhatə edir.

Kiber-təhlükəsizlik nəzarətinin effektiv olduğu yerlərdə kiber-məkan etibarlı rəqəmsal infrastruktur hesab olunur. Kiber-təhlükəsizliyin qeyri-obyektiv və düzgün tərtib olunmadığı sahə rəqəmsal çağın “vəhşi qərbi” hesab edilir. Müvafiq dövrdə "kiberməkan" termini konsepsiyadan texniki səviyyəyə qədər olan anlayışlara malikdir və onun torpaq, dəniz və hava kimi dördüncü mühüm sahə olduğu iddia edilmişdir. Ədəbiyyatda kiber məkan və kiber təhlükəsizliyin çoxsaylı tərifləri mövcuddur. Kiber-təhlükəsizlik ən çox aşağıdakı 3 terminlə əlaqələndirilir [2]:

- Qarşısını alma, aşkar edilmə və cavab verilmə;
- İnsanlar, proses, texnologiya;
- Məxfilik və bütövlük.

Bunlar kiber-təhlükəsizliyin hədəflərini, təmin edilməsi vasitələrini və kiber-təhlükəsizlik hədəflərinin əldə etdiyi mexanizmləri əks etdirir.

Birinci hissə fiziki və kiber-təhlükəsizliyə aid ümumi hədəflərin qarşısını almaq, aşkarlamaq, cavablandırmağa yönəlib. İkinci hissə ümumi olaraq texnologiya idarəçiliyinə və xüsusi bir sahə kimi kiber-təhlükəsizliyin idarə edilməsinə yönəlib. Üçüncü hissə isə məlumatlara aid olan təhlükəsizlik məqsədlərinə yönəlib.

Kiber-təhlükəsizlik e-kommersiya, e-bank, e-dövlət, e-səhiyyə və e-market üzrə kiberqaydalar ilə məşğul olur [3]. Təhlükəli kiberdünyadan istifadə edənlər istisna olmaqla, hər kəs təhlükəsizlik, gizlilik, məxfilik, bütövlüyün olduğu və etibarlı, orijinal məlumatların mövcudluğunu təmin edən etibarlı texnologiya mühitinə ehtiyac duyur. Bu baxımdan müxtəlif informasiya təhlükəsizliyi standartları mövcuddur. Bu

standartlar siyasətinə nə kimi görünməsinə məsləhət etməkdən başqa, informasiya təhlükəsizliyi siyasətini uğurla tətbiq etmək üçün lazım olan çoxsaylı prosesləri müəyyən etməyə çalışır. Təhlükəsizlik siyasəti informasiya sistemlərinin təhlükəsizliyi ilə bağlı bir qurumdan gözlənilənləri müəyyənləşdirmək üçün nəzərdə tutulub. Ümumiyyətlə, bu standartlar təsadüfən və ya qəsdən hərəkətlər nəticəsində informasiya aktivlərinə olan təhlükəni azaltmaq məqsədilə insan davranışını idarə etmək üçün hazırlanmışdır. Bu standartlar vasitəsilə, həmçinin, texnologiya üzrə aparıcı ölkələrin təcrübəsi ilə informasiya resurslarının təhlükəsizliyi və rifahını təmin etmək mümkündür.

III. E-DÖVLƏTƏ OLAN KİBER HÜCUMLAR

E-xidmətlərin inkişafı və yayılması e-dövlət sisteminin effektivliyinə təsir göstərməklə yanaşı, inkişaf etməkdə olan və inkişaf etmiş ölkələrdə dövlət üçün əlavə problemlər yaratmışdır. Belə ki, təhlükəsizlik e-dövlətin hər bir prosesində ortaya çıxan əsas məsələlərdən biridir. Təhlükəsizliyi təmin etmək isə asan məsələ deyildir. Belə ki, vətəndaşların e-dövlət xidmətlərindən istifadə etməsini təşviq etmək üçün bu mühitdə məlumatların gizliliyinin qorunub saxlanılmasını təmin etmək vacibdir [4, 5].

Lakin təəssüf ki, e-dövlətin özü də bədnəviyyətlilərin hədəfi ola bilər. Belə ki, kiber məkanda bədnəviyyətli fərdlər potensial hədəfləri tapmaq, zəiflikləri müəyyən etmək və ya istismar etmək, fərqli məlumatları əldə etmək və integrasiya etmək üçün hökumət veb-saytlarının məzmunundan istifadə edə bilərlər [6, 7]. Dövlət veb-saytlarına çoxsaylı kiberhücumlar ola bilər. Belə ki, bu hücumlar vasitəsilə infrastrukturun (kompüter sistemi, elektrik şəbəkəsi və s.) zədələnməsi və ya məhv edilməsi dövlətə külli miqdarda zərər verə bilər. Belə hücumların vaxtında aşkarlanması, qarşısının alınması və profilaktik işlərin görülməsi vacib məsələlərdən biridir. Bunun üçün isə dövlətə ola biləcək əsas kiber hücumları əvvəlcədən müəyyənləşdirmək və analiz etmək məqsəduyğundur.

E-dövlətə olan əsas kiber-təhlükələr şəkil 1-də təsvir olunmuşdur [8].

Şəkil 1. E-dövlətə kiber təhlükələr

İnsayderlər: narazı insayderlər (keçmiş əməkdaş) kompüter cinayətinin əsas mənbəyidir;

Hakerlər: Hakerlər qərəzli məqsədlər və maliyyə mənfəəti üçün şəbəkələrə hücum edirlər;

Haktivizm: siyasi mesajlar göndərmək, saxta görüntü yaratmaq və ya məlumat vermək, mətni dəyişdirmək üçün veb sahifələrə və ya e-poçt xidmətlərinə siyasi əsaslı hücumlardır;

Virus proqramını yaradanlar: dağıdıcı kompüter viruslarının yayılması dünyada şəbəkələr və proqram təminatları üçün getdikcə ciddi təhlükə yaradır;

Kriminal qruplar: cinayətkarlar tərəfindən mənfəət əldə etmək üçün sistemlərə hücum cəhdləridir;

Terroristlər: bu qruplar informasiya texnologiyaları və İnternetdən planlar hazırlamaq, pul vəsaitlərini artırmaq, təbliğat və təhlükəsiz ünsiyyət qurmaq üçün istifadə edirlər;

İnformasiya müharibəsi: xarici qüvvələrin kritik infrastrukturulara qarşı "informasiya müharibəsi" milli təhlükəsizliyə ciddi təhiddir.

Ədəbiyyatda dövlətə qarşı olan bu cür kiber hücumların qarşısının alınması məqsədilə bir sıra çıxış yolları göstərilmişdir. Bunlar aşağıdakılardır [1]:

- Müvafiq reaksiyanı müəyyənləşdirmək və həyata keçirmək üçün İKT infrastrukturuna qarşı təhlükələrlə bağlı zəruri biliklərin yaradılması;
- Təhlükəsiz kibermekanı dəstəkləmək üçün əlverişli hüquqi mühitin yaradılması, e-əməliyyatlarda inam və etibarın təmin olunması; maraqlı tərəflər tərəfindən məsuliyyətli hərəkətlərin təmin edilməsi və effektiv cinayət təqibinə imkan verən hüquq-mühafizə imkanlarının artırılması;
- İKT şəbəkələrinin, kritik kommunikasiya və informasiya infrastrukturalarının qorunması;
- Effektiv proqnozlaşdırıcı, profilaktik, qoruyucu, cavab və bərpa tədbirləri vasitəsilə kiber təhlükə və böhranın idarə edilməsi üçün 24 x 7 mexanizmlərinin yerləşdirilməsi;
- Beynəlxalq Təhlükəsizlik təcrübələrinin, siyasət, təşviq və tədbirlərin öyrənilməsi;
- Kiber-təhlükəsizliyin yaradılması məqsədilə istifadəçilərdə İKT-dən istifadə davranışı mədəniyyətinin yaradılması;
- Təhlükəsiz mühit yaratmaq üçün həssas fərdi məlumatların işlənməsi, idarə edilməsi, saxlanması, tranziti və məlumatların qorunması.

Bütün bunlarla yanaşı e-dövlətə olan kiber-hücumların qarşısının alınması üçün hökumət şöbələrinin və ya qurumların yüksək səviyyəli rəhbərliyi müvafiq informasiya təhlükəsizliyi siyasətini həyata keçirməli və təşkilatdakı müvafiq texnologiya və tətbiqlərin istifadəsini təşviq etməlidir. O cümlədən təşkilatlarda "İnformasiya Təhlükəsizliyi Çərçivəsi" yaratmaq, idarə etmək lazımdır [9].

NƏTİCƏ

Vətəndaşların vaxtında və səmərəli xidmətlərə olan tələbi nəticəsində e-dövlət xidmətlərinin sayı günbəgün artmaqdadır. E-dövlət, eləcə də e-idarəetmə artıq global iqtisadiyyatda əhəmiyyətli yer tutmuşdur. E-dövlətdən istifadənin artması ilə

yanaşı bu mühitdə təhlükəsizlik məsələləri də əsas istiqamətlərdən birinə çevrilmişdir.

Bu sistemdə informasiya sistemlərinin təhlükəsizliyi üçün tədbirlər müxtəlif səviyyələrdə aparılmalıdır. Hökumət öz fəaliyyətində şəffaf olmalı və lazım olduğu təqdirdə qanunvericiliyi təqdim etməlidir. Kibercinayətkarların arzuolunmaz fəaliyyətini dayandırmaq və aradan qaldırmaq üçün kifayət qədər güclü qanunvericilik aktları mövcud olmalıdır. Bu işdə həm hökumət həm də hər bir şəxs öhdəsinə düşən məsuliyyəti yerinə yetirməlidir. Belə ki, şəbəkə xidmətləri təminatçıları (İSS), iri müəssisələr və kiçik istifadəçilər/ev istifadəçiləri kimi digər maraqlı tərəflər də ölkənin kiberməkanının təhlükəsizliyini artırmaq üçün öz öhdələrinə düşən vəzifəni yerinə yetirməlidirlər. Bu mərhələdə və gələcəkdə rəqəmsal irəliləyişlər və e-dövlət ətrafında təhlükəsiz mühitin yaradılması məqsədilə daha geniş tədqiqatlar aparılmalıdır.

Ədəbiyyat

- [1] D. Kumar, Dr. N. Panchanatham, “A case study on Cyber Security in E-Governance”, International Research Journal of Engineering and Technology, 2015, Vol.2, No.8, pp.272-275.
- [2] L. Kumari, R. Kumar, “Impact of Cyber Security in different application of e-Governance: Case Study”, Proceedings of the 4th International Conference on System Modeling & Advancement in Research Trends, 2015, pp. 365-374.
- [3] J. L. Bayuk, J. Healey, P. Rohmeyer, M. Hsachs, J. Schmidt, J. Weies, “Cyber security policy guidebook first edition”, 2012.
- [4] A. Conklin, G. B. White, “e-Government and Cyber Security: The Role of Cyber Security Exercises”, Proceedings of the 39th Hawaii International Conference on System Sciences, 2006, pp.1-8.

- [5] Y.N. İmamverdiyev, “E-dövlət informasiya təhlükəsizliyi təhdidlərinin konsensus rəqlaşdırılması metodu”, İnformasiya texnologiyaları problemləri, 2018, №2, s.34–45.
- [6] L. Carter, F. Belanger, “The utilization of egovernment services: citizen trust, innovation and acceptance factors”, Journal of Information Systems, 2005, Vol.15, No.1, pp. 5-25.
- [7] Sh. M. Shareef, “Enhancing Security of Information in E-Government”, Journal of Emerging Trends in Computing and Information Sciences, 2016, Vol. 7, No. 3, pp. 139-144.
- [8] R. M. Alguliyev, R.M. Aliguliyev, G. Y. Niftaliyeva, “Filtration of Terrorism-Related Texts in the E-Government Environment”, International Journal of Cyber Warfare and Terrorism, 2018, Vol. 8, No.4, pp.35-48.
- [9] D. Kumar, N. Panchanatham, “Strategies for Rebooting the Government in e-Mode”, Global Journal for Research Analysis, 2014, Vol. 3, No. 8, pp.129-130.

ABOUT CYBER ATTACKS TO E-GOVERNMENT AND STRUGGLE AGAINST THEM

Gunay Iskenderli

Institute of Information Technology of ANAS,
Baku, Azerbaijan

Abstract -- E-government is the result of efforts by the government to improve relations with its citizens. To protect the e-government from existing threats in cybercrime, there is a need for best practices in information security. Security policies, practices and procedures, furthermore the use of security technology, can help to protect the e-government systems from attack, and detect non-standard services. Taking into account, the information about cyber-security and major cyber-attacks on e-government is given in this article.

Keywords -- e-government; information security, cyber attacks.

Elektron dövlət mühitində fərdi məlumatların mühafizəsi problemləri

İradə Ələkbərova

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

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

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

I. GİRİŞ

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

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

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

II. FƏRDİ MƏLUMATLARLA ƏLAQƏDAR BƏZİ ANLAYIŞLAR

Fərdi məlumatlar dedikdə şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənəşdirməyə imkan verən istənilən məlumat nəzərdə tutulur. “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanununun 6-cı maddəsinə

əsasən, fərdi məlumatların informasiya sistemlərinin yaradılması, dövlət qeydiyyatının aparılması və tətbiq edilməsi sahəsində hüquqi və texniki sənədləşdirmənin standartlaşdırılması, fərdi məlumatların toplanması, işlənilməsi və mühafizəsi sahəsində dövlət tənzimləməsinin əsas formalarına aiddir. Yəni xüsusi icazə olmadan vətəndaşın şəxsi həyatı haqqında məlumatların toplanması, saxlanması, istifadə olunması və yayılması qadağandır.

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

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

III. ELEKTRON DÖVLƏTDƏ FƏRDİ MƏLUMATLAR

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

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

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

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

IV. RƏQƏMSAL İZ

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

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

Rəqəmsal izlərin analizində müxtəlif analitik yanaşmalardan istifadə olunur. Bunlara maşın təlimi,

verilənlərin intellektual anlyzi, “text mining”, nitqin emalı, dilin differensial anlyzi, LIWC (*linguistic inquiry and word count*), tematik modelləşdirmə, qərarlar ağacı və s. metodlar aiddir [10].

V. İZLƏYİCİ CİHAZLAR VASİTƏSİLƏ FƏRĐİ MƏLUMATLARIN TOPLANMASI

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

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

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

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

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

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

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

VI. FƏRDİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİ

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

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

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

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

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

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

NƏTİCƏ

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

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

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

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

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

ƏDƏBİYYAT

- [1]. T. Nasser, R.S. Tariq, Big Data Challenges // Computer Engineering and Information Technology, 2015, vol. 4, no. 3., pp. 1–6.
- [2]. Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu, <http://www.e-qanun.az/framework/19675>
- [3]. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, <https://eur-lex.europa.eu/legal-content/en/>
- [4]. Directive 97/66/EC of the European Parliament and of the Council 15 December 1997, <https://eur-lex.europa.eu/legal-content/en/>
- [5]. European Convention on Human Rights, https://www.echr.coe.int/Documents/Convention_ENG.pdf
- [6]. M.D. Back, J.M. Stopfer, S. Vazire, S. Gaddis, S.C. Schmukle, B. Egloff, S.D. Gosling, Facebook profiles reflect actual personality, not self-idealization // Psychological Science, 2010, vol. 21, no. 3, pp. 372–374.
- [7]. J. Harris, The tyranny of algorithms is part of our lives: soon they could rate everything we do, 2018. Online: <https://www.theguardian.com/commentisfree/2018/mar/05/algorithms-rate-credit-scores-finances-data>
- [8]. M. Deakin, H. Al Waer, From intelligent to smart cities // Intelligent Buildings International, 2011, vol. 3, no. 3, pp. 140–152.
- [9]. K. O'Hara, M.M. Tuffield, N. Shadbolt, Lifelogging: Privacy and empowerment with memories for life // Identity in the Information Society, 2008, vol. 1, issue 1, pp 155–172.
- [10]. D. Azucar, D. Marengo, M. Settanni, Predicting the Big 5 personality traits from digital footprints on social media: A meta-

analysis // Personality and Individual Differences, 2018, vol. 124, pp. 150–159.

- [11]. R. Duus, M. Cooray, N.C. Page, Exploring Human-Tech Hybridity at the Intersection of Extended Cognition and Distributed Agency: A Focus on Self-Tracking Devices // Frontiers in Psychology, 2018, vol. 9, no. 1432,
- [12]. R.R. Gangi, N.B. Rajesh, N.P. Sudhakar, B. Raviteja, K. Rammohanarao, Tracking objects using rfid and wireless sensor networks // International Journal Of Engineering Science & Advanced Technology, 2012, vol. 2, issue 3, pp. 513 – 517.
- [13]. A. Redondi, M. Chirico, L. Borsani, M. Cesana, M. Tagliasacchi, An integrated system based on wireless sensor networks for patient monitoring, localization and tracking // Ad Hoc Networks, 2013, vol. 11, issue 1, pp. 39–53.
- [14]. R. Massobrio, S. Nesmachnow, A. Tchernykh, A. Avetisyan, G. Radchenko, Towards a Cloud Computing Paradigm for Big Data Analysis in Smart Cities // Programming and Computer Software, 2018, vol. 44, iss. 3, pp. 181–189.
- [15]. R.M. Əliquliyev, R.Ş. Mahmudov, Əşyaların interneti: mahiyyəti, imkanları və problemləri // İnformasiya cəmiyyəti problemləri, № 2(4), 2011, səh. 29–40.
- [16]. Интернет вещей: Новые перспективы для людей с инвалидностью, 2015, Публикации и доклады G3ict, 22 стр., <http://www.unic.ru/sites/default/files/>
- [17]. В. Алексеев, Модули Bluetooth, Wi-Fi и NFC производства u-blox для «Интернета вещей», Часть 2 // Беспроводные технологии, 2015, №3, стр. 23–24.
- [18]. R.M. Əliquliyev, Y.N. İmamverdiyev E-dövlətin informasiya təhlükəsizliyi: aktual tədqiqat istiqamətləri // İnformasiya cəmiyyəti problemləri, 2010, №1, səh. 3–13.

SECURITY PROBLEMS OF PERSONAL INFORMATION IN E-GOVERNMENT

Alakbarova Y. Irada

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

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

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

İnternet mühitdə “yirtıcı” jurnalların avtomatik tanınması üçün intellektual sistemin yaradılmasının konseptual əsasları haqqında

Rəhilə Həsənova¹, Firudin Əsgərov²

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

¹rahasanova@gmail.com, ²firudinasgarov@gmail.com

Xülasə — Bu məqalədə yirtıcı jurnalları avtomatik təyin edən antiyirtıcı sistemin iş prinsipi təhlil edilmişdir. Antiyirtıcı sistemin blok sxemlərlə sadə ifadəsi təqdim edilmişdir.

Açar sözlər — yirtıcı jurnal; yirtıcı nəşriyyat; impakt faktor

I. GİRİŞ

“Yirtıcı jurnallar” ifadəsini ilk dəfə amerikalı kitabxanaçı, Kolorado Denver Universitetinin dosenti Cefri Bill istifadə etmişdir. O, bu cür jurnalları 2008-ci ildən etibarən analiz etməyə başlamışdır. Buna səbəb isə ona jurnalların elektron ünvanlarından redaksiya heyətinə dəvət haqqında külli miqdarda şübhəli elektron məktubların gəlməsi idi. Bu məktubların içərisində çoxsaylı qrammatik səhvlərin mövcudluğu onun diqqətini çəkmişdi. Həmin vaxtdan etibarən o, mütəmadi olaraq yenilənən, böyük ehtimalla “yirtıcı” hesab olunan jurnalların “qara” siyahısını hazırlamağa başladı. Burada jurnalların Scopus və Web of Science kimi beynəlxalq akademik bazalar tərəfindən “ağ” və ya “qara” siyahıya daxil olması yoxlanılır, onların bazada qalması və ya çıxarılması haqqında qərar qəbul edilir [1-5].

Son 10 ildə dünyada aktual olan yirtıcı jurnallarda məqalə dərci artıq Azərbaycanda da müzakirə mövzudur. Belə ki, elmi müəssisələrdə tədqiqatçıların bilərəkdən və yaxud təsadüfən yirtıcı jurnallarda məqalə çap etdirməsi tədqiqatçı ilə yanaşı həmin müəssisənin nüfuzuna da xələl gətirmiş olur. Bu baxımdan müəllifin orijinal və yirtıcı jurnalları xarakterizə edən xüsusiyyətləri bilməsi vacibdir.

Azərbaycanda yirtıcı jurnal və nəşriyyatları xarakterizə edən göstəricilər haqqında məlumatlılıq elmi müəssisələrlə, elmi tədqiqatçılarla yirtıcı və ya oğurlanmış jurnallarla qarşılaşma təhlükəsi ilə üz-üzə qoyur.

Araşdırmalar onu göstərir ki, bu gün yirtıcı jurnallar təhlükəsindən qorunmaq məqsədi ilə antiyirtıcı sistemin işlənməsi zəruridir. Təcrübə göstərir ki, müxtəlif ölkələrdə bu məsələ ilə bağlı bəzi işlər görülməyə başlanmışdır. Məsələn, 2015-ci ildən fəaliyyət göstərən Düşün! – Yoxla! – Təqdim et! (Think! – Check! – Submit!) onlayn sistemi bu baxımdan maraqlı kəsb edir [7].

II. MƏQALƏ DƏRCİ ÜÇÜN DÜZGÜN JURNAL SEÇİN DÜŞÜN! – YOXLA! – TƏQDIM ET!

Dünyada artıq 33 dildə fəaliyyət göstərən thinkchecksubmit.org saytı tədqiqatçılara məqalə dərc etdirmək üçün düzgün jurnal seçməkdə kömək edir. Bu saytın məqsədi müəllifə birinci mərhələdə düşünməyi, ikinci mərhələdə yoxlamağı, sonda isə məqaləni təqdim etməyi məsləhət görür [7].

Birinci – **Düşün! (Think!)** mərhələsində tədqiqatçı aşağıdakı suallara cavab tapır:

- Elmi tədqiqatınızı dərc etdirmək üçün etibarlı jurnal seçmişinizmi?
- Bu jurnal sizin tədqiqat sahənizə tam uyğundurmu?

Bu suallar tədqiqatçıya seçilən jurnalın doğru jurnal olduğuna əmin olmaq məqsədilə verilir. Çünki dünyada nəşrlərin sayı getdikcə artır, demək olar ki, hər həftə yeni jurnallar fəaliyyətə başlayır. “Yirtıcı” nəşriyyatların qanuna zidd hərəkətləri və aldatma halları da getdikcə artmaqdadır və məqalə dərc etdirmək üçün etibarlı jurnal tapmaq günü-gündən çətinləşir.

İkinci – **Yoxla! (Check!)** mərhələsində tədqiqatçının seçdiyi jurnalın etibarlı olub-olmadığı yoxlanılır. Bu məqsədlə aşağıdakı suallar cavablandırılmalıdır:

- Siz və ya həmkarınız bu jurnalı tanıyırsınız mı?
 - ✓ Əvvəllər həmin jurnaldan hər hansı bir məqalə oxumusunuzmu?
 - ✓ Jurnalda ən son dərc edilmiş məqalələri əldə etmək mümkündürmü?
- Nəşriyyatı müəyyənləşdirmək və əlaqə yaratmaq mümkündürmü?
 - ✓ Nəşriyyatın adı jurnalın veb saytında əks olunurmu?
 - ✓ Nəşriyyatla saytda əks olunmuş telefon nömrəsi, poçt və elektron poçt ünvanı ilə əlaqə yaratmaq mümkündürmü?
- Jurnalın istifadə etdiyi qiymətləndirmə növü (rəy, resenziya) şəffafdırmı?

- Jurnalın məqalələri saytında adı çəkilmiş beynəlxalq bazalarda həqiqətən indekslənmirmi?
- Ödəniş haqqında məlumatları jurnalın saytında əldə etmək mümkündürmü?
 - ✓ Jurnalın saytında ödənişin nə üçün tələb olunduğu izah olunurmu?
 - ✓ Ödənişin nə zaman həyata keçirilməsi haqqında məlumat verilirmi?
- Redaksiya heyətinin üzvləri sizə tanış alimlərdir?
 - ✓ Redaksiya heyətinin üzvləri haqqında eşitmisinizmi?
 - ✓ Redaksiya heyəti üzvləri öz veb saytlarında bu jurnalın adını qeyd edirlərmə?
- Jurnalın nəşriyyatı beynəlxalq elmi cəmiyyətlərin üzvüdümmü?
 - ✓ Jurnalın nəşriyyatı COPE (*Committee on Publication Ethics*)-in üzvüdümmü?
 - ✓ Jurnal açıq əlyetərdirsə, onun adı DOAJ (*Directory of Open Access Journals*)-in siyahısında varmı?
 - ✓ Jurnal açıq əlyetərdirsə, onun adı OASPA (*Open Access Scholarly Publishers' Association*)-nın siyahısında varmı?
 - ✓ Jurnal INASP's *Journals Online* və ya *African Journals Online* platformalarından hər hansı birinə daxilirmi?
 - ✓ Nəşriyyat hər hansı digər ticarət assosiasiyasına daxilirmi?

Üçüncü – **Təqdim et! (Submit!)** mərhələsində əvvəlki mərhələdə sadalanan sualların hamısı və ya əksəriyyətinin cavabı müsbətdirsə, onda tədqiqatçıya məqaləsini həmin jurnala təqdim etmək məsləhət görülür. Lakin bu mərhələdə də diqqət yetirilməli bir neçə əsas məqam vardır:

- Burada əmin olmaq lazımdır ki, məqalənin təqdim olunduğu jurnal tədqiqatçının həmkarları arasında reputasiyasını qaldırmağa və çoxlu istinadlar qazanmağa səbəb olacaqdır.;
- Məqaləni doğru jurnalda dərc etməklə tədqiqatçı karyerasını inkişaf etdirir və profesional imicini yüksəldə bilər.;
- Məqalə dərc olunduqdan sonra bazalarda indekslənəcək və axtarış sistemlərində asanlıqla tapılacaqdır.

Məqalənin yoxlanma və dərci müddətində nəşriyyatın peşəkar təcrübəsi özünü göstərməlidir.

III. ANTIYIRTICI SİSTEMİN BLOKLARININ İZAHİ

Düşün! – Yoxla! – Təqdim et! və digər təcrübələrə əsaslanaraq antiyirtici sistemin konsepsiyası işlənmişdir [6,7]. Bu antiyirtici sistemin işləmə mexanizmi Şəkil 1-də blok-sxemlər vasitəsilə təsvir edilir. İlk mərhələ jurnalın adının axtarış sisteminə daxil edilməsi ilə başlayır. Sonra hər bir

addımda jurnala aid müəyyən məntiqi suallar “hə” və ya “yox” ilə cavablandırılaraq növbəti mərhələyə keçid alır. Mürəkkəb budaqlanan struktura malik bu alqoritmin nəticəsində jurnalın orijinal və yaxud da yirtici olması ehtimalı irəli sürülür.

Hər bir məntiqi blokda verilmiş sualın hansı xüsusiyyətləri əks etdirməsi * işarəsi ilə şərh edilir.

*Burada saytın jurnalın həqiqi saytı olduğunu müəyyənləşdirmək nəzərdə tutulur. Bir neçə əsas məqama nəzər yetirmək lazım gəlir: 1. Jurnalın saytının onun dərc edildiyi ölkənin domen zolağına aid olması; 2. Verilmiş saytın jurnalın oğurlanmış versiyasına aid olması (əgər mövcuddursa); 3. Redaksiya heyəti ilə əlaqə məlumatlarının dolğunluğu (redaksiyanın ünvanı, əlaqə nömrələri, e-mail və s.); 4. Nəşrlərin dövriyyəsinin gözlənilməsi, yəni hər il eyni sayda nömrələrin dərc edilməsi (*Issue*); 5. Saytın görünüşünün vizual qiymətləndirilməsi. Bu zaman saytın konstruktor sayt olub-olmaması yoxlanılır və pulsuz domen və subdomenlərdə yerləşməsi araşdırılır; 6. Saytın alt səhifələrinin mövcudluğu və aktivliyi; 7. Saytda verilmiş məlumatların qrammatika və orfoqrafiya baxımından düzgün yazılması.

**Jurnalın akademik bazalarda indeksləşməsi haqqında saytda verilmiş məlumatın (məs., impakt faktor göstəricisi) həqiqi olub-olması müəyyənləşdirilir, bu məlumatda hiperkeçidin olması onun doğruluğunu göstərir.

***Burada əsasən aşağıdakı məlumatlar yoxlanılır: 1. Jurnalın redaktorunun nəşr olunduğu nəşriyyatın rəhbəri ilə eyni şəxs olub-olmaması (adətən nəşriyyat rəhbəri özünü bir və ya bir neçə jurnalın baş redaktoru kimi qeyd edir). 2. Redaksiya üzvləri haqqında akademik məlumatların mövcudluğu; 3. Eyni nəşriyyat tərəfindən dərc edilən bir və ya bir neçə jurnalın redaksiya heyətinin tərkiblərinin eyniliyi; 4. Redaksiya heyəti üzvlərinin sayının kifayət qədər olmaması (bəzən, qeyd olunan redaksiya heyəti üzvlərinin adının siyahıda olmasından xəbərsiz olması); 5. Jurnal beynəlxalq olduğunu iddia etdiyi halda onun redaksiya heyəti üzvlərinin beynəlxalq müxtəlifliyi cüzi və ya heç olmaması; 6. Redaksiya heyəti üzvlərinin gender bərabərsizliyi (çox vaxt qadın üzvləri olmur).

****Tamliq xassəsi dedikdə aşağıdakılar nəzərdə tutulur: 1. Jurnalın adının onun missiyasını əks etdirməsi; 2. Jurnalın adında istifadə olunan ölkə adlarının həqiqəti əks etdirməsi (məsələn, bəzən Kanada, İsveçrə və s. kimi ölkə adları jurnalın adında istifadə olunmasına baxmayaraq, nə nəşriyyatın, nə redaksiya heyətinin bu ölkələrə aidiyyəti olmur); 3. Nəşriyyat göndərdiyi spam məktublarında və ya öz saytında impakt faktor və beynəlxalq bazalarda indekslənmə haqqında məlumatın verilməsi. Burada iddia edilir ki, nəşriyyatın dərc etdiyi jurnalların bir neçəsi impakt faktora malikdir (Thomson Reuters) və ya saxta təşkilatlardan əldə edilən impakt faktorlar reklam edilir.

*****Burada aşağıdakı məlumatlar yoxlanılır: 1. Nəşriyyat tərəfindən məqalənin əvvəllər digər jurnallarda dərc edildiyi yoxlanırmı? 2. Dərc edilmiş məqalələr yalançı elmə (*pseudo-science*) aiddir. 3. Əlaqə hissəsində sadəcə e-mail və yaxud da veb forum qeyd edilir. Bununla da nəşriyyat əsas ünvanını gizli saxlamış olur.

*****Burada isə aşağıdakı məqamlar araşdırılır:

1. Nəşriyyatın digər nəşriyyatların müəlliflərə qoyduğu tələbləri eynilə öz tələbi kimi qeyd etməsi. 2. Nəşriyyatda jurnalların adının ümumi verilməsi ilə çoxlu sayda məqalə toplanmasına və müəlliflərdən daha çox gəlirin əldə edilməsinə nail olmaq. Məsələn, Təhsil jurnalı (*Journal of Education*). 3. Bir-biri ilə əlaqəsi olmayan 2 və daha çox elm sahələrini əhatə edən jurnalların nəşr edilməsi. Məsələn, Biznes, Humanitar və Texnologiya beynəlxalq jurnalı (*International journal of Business, Humanities and Technology*). 4. Nəşriyyat tərəfindən jurnalların saytının zəif hazırlanması, ölü hiperkeçidlər (*dead links*), çoxlu sayda orfoqrafik və qrammatik səhvlərin mövcudluğu. 5. Saytlarda müəlliflərə istinad edilmədən lisenziyalı şəkillərin istifadəsi.

NƏTİCƏ

Elmi jurnalların sürətlə artdığı bu dövrdə orijinal və yırtıcı jurnalların avtomatik müəyyənləşdirmək ehtiyacı yaranır. Bunun üçün ilk növbədə akademik cəmiyyətdə elmi jurnalların “ağ siyahı”sı və “qara siyahı”sı haqqında açıq məlumatların olması vacib məsələlərdəndir. Bundan başqa tədqiqatçının öz araşdırması nəticəsində məqaləsini dərc etdirmək üçün seçdiyi jurnalın orijinal və yaxud yırtıcı olması müəyyən oluna bilər. Lakin bu prosesin avtomatlaşdırılması o baxımdan aktualdır ki, tədqiqatçının yırtıcı jurnalı təyin etməyə vaxtı və əməyi sərf olunmayacaq.

İSTINADLAR

- [1] Beall J. Predatory publishing is just one of the consequences of gold open access // *Learned Publishing*, 2013, vol.26, no.2, pp.79-83.
- [2] Beall J. Predatory publishers are corrupting open access // *Nature*, 2012, vol.489, no.7415, <http://www.nature.com/news/predatory-publishers-are-corrupting-open-access-1.11385>.
- [3] Beall J. Essential information about predatory publishers and journals. *International Higher Education*, 2016, <http://www.ejournals.bc.edu/ojs/index.php/ihe/article>
- [4] Hijacked Journals, <http://www.beallslit.weebly.com/hijacked-journals.html>
- [5] Həsənova R.Ş., Əsgərov F.Ş. “Yırtıcı” jurnalları xarakterizə edən xüsusiyyətlərin identifikasiyası // *İnformasiya cəmiyyəti problemləri*, 2018, №2, 97-106 s.
- [6] Laine Ch., Winker M.A. Identifying Predatory or Pseudo-Journals // *Biochemia Medica*, 2017, vol.27, no 2, pp.285-291.
- [7] thinkchecksubmit.org

A CONCEPTUAL MODEL OF CREATING AN ANTI-PREDATORY SYSTEM FOR IDENTIFICATION OF "PREDATORY" JOURNALS

Rahila Hasanova¹, Firudin Asgarov²

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

Abstract – This article analyzes the working principle of the anti-predatory system, which automatically identifies predatory journals. The simplest expression of the anti-predatory system with block diagrams is presented.

Keywords – predatory journal; predatory publishing; impact factor

Şəkil 1. Antiyirtıcı sistemin blok sxemlərlə təsviri

Süni intellekt texnologiyalarına əsaslanan jurnalistikanın formalaşması və inkişaf perspektivləri haqqında

Sünbül Zalova

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

sunbulzalova@gmail.com

Xülasə — Xəbər materiallarının formalaşdırılması, auditoriya üçün daha cəlbedici olması və cəmiyyətdə bu materialların sürətlə yayımlanması üsullarının müxtəlifliyi ilk növbədə müasir informasiya texnologiyalarının inkişafından asılıdır. Ənənəvi jurnalistika ilə yanaşı robot jurnalistikası və dron jurnalistikasının yaranması, süni intellektin jurnalistikada tətbiqi bu sahədə yeni imkanların əldə olunmasına şərait yaratdı. Məqalədə süni intellektin müasir jurnalistikaya təsiri araşdırılmış, bununla əlaqədar imkanlar və problemlər müəyyənəşdirilmişdir.

Açar sözlər—süni intellekt, dron jurnalistikası, robot jurnalistikası, sosial media, informasiya təhlükəsizliyi.

I. GİRİŞ

İnformasiya kommunikasiya texnologiyalarının (İKT) inkişafı bütün sahələrdə olduğu kimi jurnalistikaya da güclü təsir etməkdədir. İKT və təbii dilin təkamülü nəticəsində ənənəvi xəbər istehsalı dəyişərək, yeni imkanlar əldə etməkdədir. Belə ki, artıq proqram təminatının köməyi ilə avtomatik şəkildə mətni baza məlumatlarından təbii dilə çevirmək mümkündür. Xəbərlərin avtomatik, multimedia resurslarının imkanlarından geniş istifadə olunaraq yaradılması bir ənənə halını almaqdadır.

Artıq mətn, şəkil, audio və video-faylların hazırlanması və emalı süni intellekt (Sİ) vasitəsilə həyata keçirilməkdədir. Sİ insan təfəkkürünün formalizasiyası təşəbbüsləri ilə bağlı bir elmi istiqamətdir. Sİ-in məqsədi insan təfəkkürünün, zəka imkanlarının formalizasiyası modellərinin və metodlarının işlənilməsi, elə intellektual agentlər, proqramlar, sistemlər, robotlar yaratmaqdan ibarətdir ki, onlar insanın edə biləcəyi əqli əməliyyatları insan kimi, hətta insandan da yaxşı etmiş olsunlar[1].

Jurnalistika yaradıcı peşədir. Belə fikirlərə görə, robotların işi çətinləşir. Buna baxmayaraq yazı alqoritmləri artıq mətbuatda məqalələr hazırlamaq və jurnalistləri əvəz etmək üçün geniş yayılmışdır. 2016-cı ildə iki ən güclü xəbər yazı alqoritmindən biri olan Wordsmith, 1,5 milyard xəbər yazmış və dərc etmişdir. Bu rəqəm, jurnalistlər tərəfindən yazılan və nəşr

olunan işlərlə müqayisə oluna bilər. Araşdırmalar göstərir ki, oxucular bəzən robotlar və ya insanlar tərəfindən yazılan xəbərlər arasında fərq hiss etmirlər.

Tədqiqatın məqsədi müasir jurnalistikanın imkanlarını araşdırmaq, Sİ- in jurnalistika sahəsində imkanlarını analiz edərək bu sahədə problem və perspektivləri müəyyənəşdirməkdir. Məqalədə həmçinin Sİ- in praktik tətbiqi araşdırılıb[2].

II. MÜASİR JURNALİSTİKA VƏ SÜNİ İNTELLEKT

Texnologiyanın inkişafı jurnalistikanın inkişafına təkan yaradır. Jurnalistikanın növlərinə qəzet, radio, televiziya jurnalistikası ilə yanaşı artıq İnternet, sosial media, robot, 3d jurnalistikası, rəqəmsal jurnalistika və d. aid etmək olar.

Sİ müasir jurnalistikanın bütün sahələrinə geniş tətbiq olunmaqdadır. Əsasən mətn tipli məlumatların intellektual analizi, multimedia resurslarının avtomatik aşkarlanması, toplanması, müəyyən formata gətirilməsi və digər optimallaşma məsələlərində Sİ böyük əhəmiyyətə malikdir. Sİ əsasında hazırlanan xəbərlərdə qərəzlilik, reklam və şəxsi rəğbət izlərinin olmaması süni intellekt texnologiyalarına əsaslanan jurnalistikanın (SİT-jurnalistika) əsas xarakterik cəhətidir. Digər tərəfdən xəbərin hadisənin baş verdiyi yerdə avtomatik hazırlanması və yayımlanması imkanı SİT-jurnalistikada əsas işin jurnalist tərəfindən deyil, alqoritm tərəfindən görüldüyünü müəyyən edir. SİT-jurnalistika ictimaiyyətin maraqlarına xidmət etmək potensialına malikdir, lakin fərdi məlumatların təhlükəsizliyi, xəbərlərdə şəffaflıq və hesabatlılıq məsələləri daxil olmaqla informasiya təhlükəsizliyində böyük problemlər vardır. SİT-jurnalistikada süni intellektin köməyi ilə xəbərlər, sənədlər və digər materiallar avtomatik olaraq istehsal olunur. Zaman keçdikcə süni intellekt insan intellektini kölgədə qoyur.

Bu gün “Robot jurnalistikası” termininin aktual olmasına baxmayaraq, onun izahını vermək o qədər də sadə deyildir. Əsasən çoxları bu anlayışı şablon olaraq robotların kompüter klaviaturası arxasında əyləşib yazı yazması kimi təsvir edirlər. Bu sahədəki dəyişikliklər müvafiq olaraq vahid konsepsiya şəklində hesablama jurnalistikası kimi təqdim olunur, hansı

ki, xəbər hazırlamaq üçün alqoritmik formalar, sosial-elmi, və riyazi proses və sistemlərə yönəlib. Daha aydın şəkildə izah etsək, sosial elmlərdən alqoritmik birləşmələrin, məlumat və biliklərin jurnalistikanın hesabatlılıq funksiyasına əlavə olunmasıdır. Belə ki, hesablama jurnalistikası dedikdə buraya informasiyanın avtomatlaşdırılması şamil olunur[3].

Praqnozlara əsasən gələcəkdə robot jurnalistikasının xəbər mərkəzlərində müxtəlif qabiliyyətlərə malik insanların iştirakı ilə komanda şəklində həyata keçirilməsi gözlənilir. Robotlaşma daha çox müxtəlif tipli verilənlərdən asılı olub, “data jurnalistika”-nın təkamülünün bir hissəsidir və jurnalistikaya fərqli prizmadan baxışı sərgiləyir. Bu sahənin üstünlüklərindən biri də insanlar üçün önəmli olan məsələlərdə jurnalistlərin təhlil və tədqiqat apara bilməsi, şəxsi fikir və ideologiyanın xəbərə təsir etməsi probleminin qismən də olsa aradan qaldırılmış olmasıdır. Lakin qeyd etmək lazımdır ki, robot jurnalistikası bütün sahələr üçün eyni dərəcədə faydalı deyil. Bunun əsas səbəbləri isə hazırda maraqların, informasiya tələbatlarının daha çox əyləncə, biznes, siyasət və idmanla bağlı məlumatlara, faktlara aid olmasıdır. Məsələn, biznes və idman jurnalistikası kompüterləşmə və avtomatlaşdırma jurnalistikası üçün əsas bazadır. Çünki bu sahələr üzrə hesabatlarda əsasən şablon şəklində məlumatlardan, mövcud statistikadan və nəticələrin vizualizasiya metodlarından istifadə olunur.

III. SÜNİ İNTELLEKTƏ ƏSASLANAN DRON JURNALİSTİKASI

Müasir dövrdə jurnalistlər smartfon, planşet və bir sıra yeni texnoloji qurğuların köməyi ilə xəbər, video, foto reportaj hazırlaya bilirlər. İKT-nin inkişaf etdiyi bir vaxtda jurnalistika bu texnologiyalara uyğunlaşmağa çalışır. Artıq “Dron jurnalistikası” formalaşır. Dron texniki olaraq məsafədən idarə olunan qurğudur. Dron əsasən kompüter vasitəsi ilə proqramlaşdırılır və idarə olunur. Dronların üzərinə GPS, silah, kamera, sensor və müxtəlif vasitələr yerləşdirmək mümkündür. Müasir dronlar istənilən hadisə haqqında foto, video materiallar çəkmə, böyük həcmdə məlumatları saxlama, emal etmə və ötürmə imkanlarına malikdirlər. Arxeoloji axtarış, müşahidə, araşdırma, səyahət, tikinti, hərbi və s. sahələrdə dronlardan geniş istifadə olunur. Dron jurnalistikası robot jurnalistikasının bir istiqamətidir. Uçmaq üçün istehsal olunan bu sistemlərin əsas məqsədinə insan üçün potensial təhlükəli olan missiyalar daxildir[3].

Jurnalistikada 2010-cu ildən etibarən dronlardan istifadə yeni perspektivlər yaradıb. Dronlar insanların gedə bilmədiyi ərazilərdən məlumatların ötürülməsinə imkan yaradır[4].

Dünyada Peşəkar Dron Jurnalstları Cəmiyyəti (Professional Society of Drone Journalists) fəaliyyət göstərir və bura üzv jurnalistlərin sayı günü-gündən artır[5]. 2011-ci ildə qurulan bu cəmiyyəti dron jurnalistikası sahəsində etik, təhsil və texnoloji istiqamətləri formalaşdıran ilk beynəlxalq qurumdur. Cəmiyyətin 2015-ci ilin statistikasına əsasən 60 ölkədən (Amerika, İngiltərə, Hindistan, Yeni Zelandiya,

Almaniya və d. ölkələrdən nümayəndələr var) 564 nümayəndə qoşulub[6].

Dronların istifadəsi üçün bir neçə qurumlardan icazə alınması tələb olunmasına baxmayaraq qaydalar Birləşmiş Ştatların Milli Aviasiya İdarəsi tərəfindən tənzimlənir. Qaydalar başqa ölkələrdə fərqli olduğu üçün bu birdən çox ölkədə dronlardan istifadə etmək istəyən jurnalistlər və ya media qurumları üçün problem yaradır [7].

Azərbaycanda, “Mülki dövryyənin müəyyən iştirakçılarına mənsub ola bilən və dövryyədə olmasına xüsusi icazə əsasında yol verilən (mülki dövryyəsi məhdudlaşdırılmış) əşyaların siyahısı haqqında” 23 dekabr 2003-cü il tarixli, 565-IIQ nömrəli Azərbaycan Respublikasının Qanunu ilə müəyyən edilmiş siyahının 18-ci bəndinə əsasən məsafədən idarə edilən pilotsuz uçan aparatlar xüsusi icazə əsasında mülki dövryyənin müəyyən iştirakçılarına mənsub ola bilər və dövryyədə olmasına yol verilir.

Hazırda dron jurnalistikası müxtəlif sahələrdə tətbiq olunur. Qəzalara dair məlumatları toplamaq üçün polis dronlardan, maşın yarışlarında, ətraf mühitlə bağlı məsələlərdə, fəvqaladə vəziyyətlərdə və bir çox digər sahələrdə dron jurnalistikası tətbiq olunur. Artıq dron jurnalistikasının tədrisinə də başlanılıb. «Dartdrones» adlanan bloqda yeni başlayanlar üçün məsləhətlər yerləşdirilib. Bloqda həmçinin Federal Aviasiya İdarəsi qaydaları və kommersiya dronları üçün qaydalar yerləşdirilib[6].

IV. SÜNİ İNTELLEKT VƏ SOSIAL MƏDİA

Gələcəkdə Sİ yalnız xəbər materiallarının hazırlanması və emalı ilə məşğul olmayacaq. O, müəllifə mövzu seçməkdə köməklik edəcək, oxucuların hansı mövzulara maraq göstərdiyini əvvəlcədən proqnozlaşdırma biləcək, cəmiyyəti narahat edən hadisələr və proseslər haqqında məlumat toplayacaqdır.

Artıq bu gün Sİ sosial mediaya öz təsirini göstərməkdədir. Sosial mediadakı istifadəçi səhifələrinə marağına uyğun olan reklam çarxları ötürülür, müxtəlif İnternet layihələrdə və tədbirlərdə iştirak təklif olunur. Sosial medianın imkanları hər bir istifadəçinin kontent yaradan və paylaşan müəllif kimi fəaliyyətinə təkan vermiş, birbaşa brauzerdən informasiyanın emalı, strukturlaşdırılması və ötürülməsi əməliyyatlarının yerinə yetirməsinə şərait yaratmışdır. Zaman keçdikcə bu imkanlar daha da genişlənir, sosial media “ağıllanır”. Veb-səhifələrin oxucularla “ünsiyyəti” yaranır.

Əgər ənənəvi olaraq oxucu kontent axtarırsa, Sİ texnologiyaları ilə idarə olunan kontent virtual məkanda öz oxucularını axtarır tapmaq və oxucunun istəyinə uyğun şəkildə vizuallaşdırılmaq imkanına malikdir. Sİ gələcəkdə sosial medianın imkanlarını artırmaqla, onun biznes, ticarət, tədris, reklam və s. sahələrdə istifadəsini genişləndirəcəkdir. Artıq bu gün “jurnalistika və ağıllı İnternet”, “jurnalistika və ağıllı veb” anlayışları gələcək jurnalistikanın yalnız xəbər

məlumatları hazırlayan sistem olmadığını və auditoriyanın rəyindən asılı olduğunu önə çəkir.

Sİ sosial mediada toplanan böyük həcmli məlumatlar arasından lazımsız xəbərləri, vacib və gizli məlumatları aşkarlamaqla, biznes-media-ya təsir edəcəkdir. Məsələn, artıq jurnalistin gəliri onun məqaləsinə daxil olunan “layk”ların sayı ilə müəyyənləşir.

V. SÜNİ İNTELLEKTƏ ƏSASLANAN JURNALİSTİKADA TƏHLÜKƏSİZLİK PROBLEMLƏRİ

SİT-jurnalistikada dronlardan istifadənin üstünlükləri ilk növbədə jurnalistin həyatının təhlükəsizliyi ilə və işinin sadələşdirilməsi ilə əlaqədardır. Bilirik ki, bu gün dünyanın müxtəlif yerlərində müharibələr, terror hadisələri, təbii fəlakətlər baş verir. Jurnalistlər xəbər hazırlamaq üçün bu təhlükəli yerlərə gedirlər. Yangın, təbii fəlakətlər, avtomobil qəzaları, müharibələr və hadisələr haqqında məlumatları yaxşı əks etdirmək üçün dronlardan istifadə bəla başa gəlsə də, jurnalistlərə təhlükəsizlik şansını verir[8]. Deyilənləri nəzərə almaqla SİT-jurnalistikada da dronlardan istifadənin üstünlüklərini aşağıdakı kimi təsnifatlandırmaq olar:

- jurnalistlərin işini yüngülləşdirir,
- təhlükəsiz jurnalistika prinsipinə uyğundur,
- xəbərlərin hazırlanmasında neytrallıq prinsipi qorunur,
- zəngin şəkil və video-faylların əldə olunmasına şərait yaradır,
- toplanan məlumatların saxlanması, emalı və ötürülməsini asanlaşdırır.

Təbiiq olunan müasir intellektual analiz metodları (data mining, text mining və s.) vasitəsilə təbii intellektin hazırladığı məlumatların çoxunu süni intellekt hazırlaya bilər. İKT-nin genişlənməsi və süni intellektin müxtəlif sahələrə tətbiqi nəticəsində təbii intellekt öz yerini süni intellektə verməkdədir. Dinamik olaraq inkişaf edən bu proses insan fəaliyyətinin bütün sahələrinin süni intellektlə əvəz olunması ilə nəticələnə bilər. Tədqiqatçıların bir çoxu bu prosesi ciddi problem hesab edir və bildirirlər ki, süni intellektin insanları idarə etməklə nəticələnə biləcək bu imkanları məhdudlaşdırılmalı və nəzarətdə saxlanmalıdır [9]

Dronları istifadə etməyin təhlükəli tərəfləri də var. Jurnalistlər havanın texniki problemlərini və ya qəzaların qarşısını almaq üçün bütün avadanlıqların uçuşdan əvvəl düzgün işləməsini təmin etməlidirlər. Təyyarə uçuşa davam edərkən, ehtiyatla istifadə edilməli və müşahidəçi həm hava, həm də yerdə ətraf mühitə xəbərdar olmalıdır. Süni intellekti təmin edən alqoritmlərin dəqiqliyi və mövcud situasiyaya uyğunluğu təsdiq olunmalıdır[10]

SİT-jurnalistikada dronlardan istifadənin mənfi cəhətləri aşağıdakılardır:

- şəxsi həyata müdaxilə, fərdi məlumatların icazəsiz toplanması,

- ölkələr arasında rəqəmsal bərabərsizliyi kəskinləşdirməsi,
- düzgün idarə olunmaması halında yanlış məlumatlar ötürə bilmə ehtimalı,
- bəla olması,
- müharibə və təbii fəlakət baş verən yerlərdə sıradan çıxma ehtimalı böyükdür.

Hazırda dronlar Sİ-in köməyi ilə anomal vəziyyətləri müəyyənləşdirə bilər. Cinayətkarların, itkin düşənlərin tapılmasında bir çox hallarda Sİ-lə işləyən dronlardan istifadə olunur. ABŞ-ın “Exyn Technologies” şirkəti kompüter təlimi və neyron şəbəkələr əsasında pilotsuz uçan aparatlara insan iştirakı olmadan avtonom rejimdə binalarda, yangın yerində, su altında və qaranlıqda uçmağa imkan verən proqram təminatı yaradıb. Sİ əsasında işləyən aparat yaranan təhlükəli situasiyalarda özü qərar qəbul etmək imkanına malikdir[9]. Oregon Universitetinin Jurnalistika professoru Damnan Redcliffin dediyi kimi, robotlar istehsal olunur, lakin onların fəaliyyəti alqoritmlərdən asılıdır. Heç bir inqilab avtomatik olaraq nəşr oluna bilməz.

NƏTİCƏ

SİT-jurnalistikanın imkanları onu ənənəvi jurnalistikadan əsaslı şəkildə fərqləndirir. Araşdırmalardan məlum oldu ki, SİT-jurnalistika müasir dövrün tələblərinə cavab verərək jurnalistlərin təhlükəsizliyi, informasiyanın sürətli toplanması və yayılması məsələlərini müvəffəqiyyətlə həll etsə də, onun da çatışmayan cəhətləri vardır. SİT-jurnalistika tərəfindən ötürülən xəbərin emosional tonlardan uzaq olması, həmçinin, xəbərlərin dinamik dəyişməsi və həddən artıq böyük olması, gələcəkdə oxucuların bu xəbərlərə qarşı münasibətində dəyişikliklərin yaranacağından xəbər verir.

Ənənəvi jurnalistikada jurnalistin şəxsi fikirləri, hiss və həyəcanları, yazı üzulu və hətta tez-tez işlətdiyi xarakterik ifadələr oxucularda maraq, emosional hiss və hadisəyə münasibət formalaşdırırdısa SİT-jurnalistika gələcəkdə insanların maşın tərəfindən hazırlanan məlumatlarla kifayətlənmə məcburiyyətində olacağından xəbər verir. SİT-jurnalistika tərəfindən yaradılan xəbər və məlumatlar yüksək qiymətləndirilsələr də insan zəkasının məhsulu ilə eyni tutula bilməz.

ƏDƏBİYYAT

- [1] Nick Bostrom, Eliezer Yudkowsky “The ethics of artificial intelligence,” Cambridge Handbook of Artificial Intelligence, eds. W. Ramsey and K. Frankish. Cambridge University Press, 2011.
- [2] A. Miroshnichenko “AI to bypass creativity. Will robots replace journalists?” York & Ryerson Joint Graduate Program in Communication & Culture, York University, Toronto, ON M3J 1P3, Canada
- [3] Y. Galily, “Artificial intelligence and sports journalism”, Technology in Society, vol. 54, pp47-51, August 2018
- [4] www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-spring-2013/drone-journalism-begins-slo
- [5] <http://en.wikipedia.org/wiki/Drone>

- [6] www.dronejournalism.org/news/2015/11/immersive-storytelling-is-the-future-for-drone-journalism
- [7] www.dartdrones.com/about-us/
- [8] <http://multidrone.eu/multidrone-in-short/>
- [9] <http://projects.nyujournalism.org/newsliteracy2017/topics/drone-journalism/>
- [10] Ph.Chamberlain, Drones and Journalism: How the media is making use of unmanned aerial vehicles. Rouledge, 124 p, 2017

ABOUT FORMATION AND DEVELOPMENT ISSUES OF AI -BASED JOURNALISM

Sunbul Zalova
Institute of Information Technology of ANAS
sunbulzalova@gmail.com

society are primarily dependent on the development of modern information technologies. In addition to traditional journalism, robot journalism and dron journalism have emerged, and the use of artificial intelligence in journalism has created new opportunities in this area. The article studies the impact of artificial intelligence on journalism, and identifies the possibilities and problems in this field.

Keywords -- artificial intelligence, robot journalism, dron journalism, social media, information security.

Abstract -- Formation of news stories, being more attractive to the audience, and the diversity of these publications in

“IEEE Transactions on Forensics and Information Security” jurnalının bibliometrik analizi (2006-2017-ci illər üzrə)

Nərmin Adıgözəlova

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

narmin66@gmail.com

Xülasə— Tezisdə Web of Science (WoS) bazasında indeksləşən “IEEE Transactions on Information Forensics and Security” (IEEE TIFS) jurnalında 2006-2017-ci illər ərzində çap olunmuş məqalələrin bibliometrik analizi aparılmışdır. Analiz məqalə və istinadların illər, müəlliflər, təşkilat və ölkələr üzrə paylanması istiqamətində aparılmışdır.

Açar sözlər— WoS, *impakt faktor*, *istinad*, *bibliometriya*, *bibliometrik analiz*.

I. GİRİŞ

Bibliometriya kitabların, məqalələrin və digər nəşrlərin statistik analizi olub, tədqiqatçının, məqalələr toplusunun, tədqiqat istiqamətinin və ya institutun fəaliyyətini ölçən elmi istiqamətdir [1]. Başqa sözlə desək, bibliometriya mətn və informasiyanın ölçülməsi üçün istifadə olunan metodlar çoxluğudur. Bu termin ilk dəfə 1969-cu ildə Pritchard tərəfindən işlənilmiş, riyazi və statistik metodları tətbiq etməklə kitabların, dövrü nəşrlərin və digər çap məhsullarının qiymətləndirilməsi üçün istifadə olunur. Bura istinad, açar sözlər, nəşriyyatın adı, müəllif və s. kimi xüsusi dəyişənlərlə xarakterizə olunan nəşrlərin təhlili daxildir [2].

Bibliometriya mövzu, müəllif, istinad və s. kimi göstəricilərə əsaslanan və elmi sahələrə tətbiq olunan kəmiyyət yanaşmalarıdır. Bibliometriya vasitəsilə ilə tədqiqatçı bibliometrik qiymətləndirmə metodlarından istifadə edərək tək bir müəllifin deyil, iki və daha artıq müəllifin fəaliyyətini, tədqiqat işini və ya əməkdaşlıq əlaqələrini müəyyən edə bilər [3]. Bibliometriya alimlərin məhsuldarlığına statistik üsulları tətbiq edərək elmi inkişafı ölçür.

Bibliometriya multidissiplinar elm sahəsidir. Burada analizi həyata keçirmək üçün statistik üsullardan, sosioloqların hazırladıqları icmal və hesabatlardan, elektron cədvəllər, verilənlər bazaları və statistik proqramlar vasitəsilə verilənlərin emalı üçün kompüter elmlərindən istifadə olunur. Bütün bu imkanlar elmin istənilən sahəsində tədqiqatçıların işinin analiz olunmasına imkan verir. Tədqiqat sahəsinin məhsuldarlığı həmin istiqamətdəki nəşrlərin sayı ilə ölçülür [1].

Son illər informasiya təhlükəsizliyi məsələləri diqqət mərkəzindədir. Belə ki, texnologiyanın daha çox istifadəsi

intensiv məlumatların toplanması və həmin məlumatların gizliliyi və təhlükəsizliyi ilə bağlı etik məsələlərin meydana gəlməsinə səbəb olmuşdur. İnformasiya təhlükəsizliyi milli İKT planlarının, e-dövlət, e-ticarət, e-tibb, o cümlədən e-təhsil fəaliyyət istiqamətlərinin hazırlanıb həyata keçirilməsində mühüm rol oynayır.

Yuxarıda qeyd olunanlarla yanaşı son dövrlər informasiya təhlükəsizliyi bir istiqamət olaraq akademik mühitdə olan insanların, tədqiqatçıların diqqətini cəlb edən istiqamətlərdən biri hesab olunur. Bu sahədə çoxlu elmi əsərlərin, jurnalların çap olunması tədqiqatçılara bu istiqamətdə bibliometrik analizlərin aparılmasına imkan yaratmışdır [4, 5].

Hər hansı sahə analiz olunarkən bu istiqamətdə çap olunan kitablar, məqalələr, tezislər, jurnallar və s. analiz olunur. WoS bazasında “security” sözü üzrə jurnalları axtarış etdikdə 22 adda jurnalın olduğu aşkarlanmışdır. Tezisdə bu istiqamətdə ən yüksək İmpakt Faktor (IF) göstəricisinə malik IEEE TIFS jurnalı götürülmüş və jurnalın 2006-2017-ci illər ərzində çap olunmuş buraxılışları analiz olunmuşdur [6].

IEEE TIFS jurnalı informasiya ekspertizası, informasiya təhlükəsizliyi, biometriya, o cümlədən bu cür xüsusiyyətləri birləşdirən nəzarət sistemləri və sistem tətbiqləri ilə əlaqəli elm, texnologiya və proqram sahələrini əhatə edir.

Tezisdə IEEE TIFS jurnalında 2006-2017-ci illərdə çap olunan məqalələr və istinadlar üzrə analiz aparılmışdır.

Məqalələr üzrə aşağıdakı göstəricilər analiz edilmişdir:

- məqalələrin illər üzrə paylanması;
- məqalələrin tipə görə təsnifatı;
- müəlliflər üzrə analiz;
- müəlliflərin əməkdaşlıq dərəcəsinin müəyyən edilməsi;
- ən məhsuldar müəllifin seçilməsi;
- məqalələrin təşkilatlar üzrə paylanması;
- məqalələrin ölkələr üzrə paylanması;

İstinadlar üzrə isə aşağıdakı göstəricilər analiz edilmişdir:

- istinadların illər üzrə paylanması; illər üzrə istinadın orta sayı;

- istinad olunan sənədin növünün və sayının müəyyən olunması.

II. BIBLIOMETRİK TƏDQIQATLAR SAHƏSİNDƏ BEYNƏLXALQ TƏCRÜBƏ

Son illər bibliometrik tədqiqatlar sahəsində çoxlu araşdırmaları aparılır. Tezisdə bu istiqamətdə aparılmış bəzi araşdırmalara baxılmış və bir sıra nümunələr göstərilmişdir.

Dhiman “Ethnobotany Journal” adlı jurnalda 1989-1998-ci illər ərzində çap olunan məqalələri illər, ölkələr, təşkilatlar, istinadlar və məqalənin həcminə görə analiz etmişdir [7]. Patra və başqaları jurnal və müəlliflərin artımını analiz etmişlər [8]. Neff və Corley 1970-2005-ci illəri əhatə edən ekoloji sahələrdə mövcud yanaşmaları və mövzuları təyin etmək üçün əlaqəli sözlərin bibliometrik analizini araşdırmışlar [9]. Thanuskod sosial elmlər sahəsində aparılan araşdırmaların nəticələri haqqında analiz aparmışdır. Analiz əsasən istinad olunan jurnalları, istinad olunan sənədin növünü, hər məqaləyə düşən orta istinad sayını və s. əhatə etmişdir [10].

Bornman və Mutz XVII əsrin ortalarından 2012-ci ilədək çap olunan və istinad olunan ədəbiyyatları analiz etmişlər. Onlar elmin inkişaf səviyyəsini həmin müddətdən əvvəlki dövr ilə müqayisə edərək elmin inkişafını 3 dövrə bölüblər:

- 1) XVIII əsrin ortalarına kimi 1% artım,
- 2) dünya müharibələri arasındakı müddətdə 2-3%,
- 3) 2012-ci ilə qədər 8-9% artım müşahidə olunur [11].

Abdi və başqaları “Information Processing & Management” adlı jurnalında 1980-2015-ci illər ərzində çap olunmuş məqalələri müəlliflər, istinadlar, ölkələr, təşkilatlar və s. göstəricilərə əsasən analiz etmişlər [12].

Jurnalların qiymətləndirilməsi üçün bəzi alimlər tərəfindən WoS və Scopus bazalarına əsaslanan müxtəlif göstəricilər təklif olunmuşdur. WoS və Scopus bazasından istifadə edərək nəşrlərin, müəlliflərin, açar sözlərin jurnalın sahələri üzrə təsnifat edilməsi, həmçinin müxtəlif göstəricilər arasında korrelyasiyanın aparılması mümkündür.

III. BIBLIOMETRİK ANALİZİN NƏTİCƏLƏRİ

Qeyd olunduğu kimi tədqiqat işində WoS bazasında indeksləşən IEEE TIFS adlı jurnal analiz olunmuşdur. Jurnalı analiz etmək üçün WoS bazasında “Publication name” bölməsinə IEEE TIFS jurnalının adı daxil edilir. Axtarış nəticəsində 2006-2017-ci illər ərzində jurnalda 1639 sayda məqalənin nəşr olunduğu aşkarlanmışdır.

IEEE TIFS jurnalının 11 il ərzində IF göstəricisi şəkil 1-də göstərilmişdir. Şəkil 1-dən göründüyü kimi jurnalın IF göstəricisi ən aşağı 2007-ci ildə (1.089), ən yüksək isə 2017-ci ildə (5.824) olmuşdur. 2010 və 2011-ci illərdə jurnalın IF göstəricisində nisbətən azalma müşahidə olunsada, digər illərdə bu göstərici artmaqda davam etmişdir.

Tədqiqat işində analiz 2 istiqamətdə (məqalələr və istinadlar) aparılmışdır.

1. Məqalə üzrə analiz:

A) Məqalələrin illər üzrə paylanması

2006-2017-ci illər ərzində IEEE TIFS jurnalında 1639 sayda məqalə çap olunmuşdur. Bu, o deməkdir ki, orta hesabla bu jurnalda il ərzində 136 məqalə çap olunmuşdur. Məqalələrin illər üzrə paylanması say və faiz nisbəti ilə cədvəl 1-də göstərilmişdir.

Şəkil 1. “IEEE TIFS” jurnalının IF göstəricisi

Cədvəl 1-dən göründüyü kimi ən az məqalə sayı 2006-cı ildə (46 məqalə, 2,81%), ən çox isə 2017-ci ildə (223 məqalə, 13,61%) çap olunmuşdur.

CƏDVƏL 1. MƏQALƏLƏRİN İLLƏR ÜZRƏ PAYLANMASI

İl	Jurnalın nömrəsi	Məqalə sayı	%
2006	1 (1-4)	46	2,81
2007	2 (1-4)	70	4,27
2008	3 (1-4)	70	4,27
2009	4 (1-4)	83	5,06
2010	5 (1-4)	85	5,19
2011	6 (1-4)	121	7,38
2012	7 (1-6)	160	9,76
2013	8 (1-12)	178	10,86
2014	9 (1-12)	182	11,10
2015	10 (1-12)	205	12,51
2016	11 (1-12)	216	13,18
2017	12 (1-12)	223	13,61
Cəmi		1639	100

B) Məqalələrin tipə görə təsnifatı

Cədvəl 2-də jurnalın 2006-2017-ci illərdə çap olunan məqalələrin sənədin növə görə təsnifatı göstərilmişdir və ən çox məqalələrin üstünlük təşkil etdiyi görünür. Burada 15 məqalə konfrans materialı kimi daxil olunmuşdur. Buna səbəb həmin məqalələrin əvvəlki illər konfrans materialı olaraq çap olunub, daha sonradan genişləndirilib məqalə şəklində çap olunmasıdır.

CƏDVƏL 2. MƏQALƏLƏRİN NÖVƏ GÖRƏ TƏSNİFATI

Sənədin növü	Say	%
Məqalə (Paper)	1606	97.987
Ön söz (Editorial material)	21	1.281
Tezis	15	0.915

**“İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri”
IV respublika konfransı, 14 dekabr 2018-ci il**

(Proceedings paper)		
Redaktə olunmuş (Correction)	9	0.549
Məktub (Letter)	2	0.122
İcmal (Review)	1	0.061

C) Müəlliflər üzrə analiz

2006-2017-ci illər ərzində çap olunan məqalələri müəlliflər üzrə təsnifat etdikdə, yəni həmmüəlliflər üzrə qruplaşdırdıqda 1639 məqalədən 70-i təkmüəllifli, 404-ü ikimüəllifli, 470-i üçmüəllifli, 695-i isə 3-dən çox müəllifli olduğu aşkarlanmışdır. Cədvəl 3-dən göründüyü kimi 2006-2017-ci illər ərzində çap olunan məqalələrdə 3-dən çox müəllifli məqalələr üstünlük təşkil edir.

CƏDVƏL 3. MƏQALƏLƏRİN MÜƏLLİFLƏR ÜZRƏ ANALIZI

İl	Təkmüəllifli	İkimüəllifli	Üçmüəllifli
2006	3	18	15
2007	4	31	23
2008	4	25	18
2009	6	29	21
2010	4	17	32
2011	6	36	40
2012	8	41	49
2013	4	45	45
2014	8	48	46
2015	11	39	51
2016	3	38	63
2017	9	37	67
Cəmi	70	404	470

D) Müəlliflərin əməkdaşlıq dərəcəsinin müəyyən edilməsi

Əməkdaşlıq dərəcəsinin (Degree of collaboration, DC) hesablanması (1) düsturu əsasında aparılır.

$$DC = \frac{a}{a + b} \quad (1)$$

Burada a - çoxmüəllifli məqalələrin sayını, b – təkmüəllifli məqalələrin sayını bildirir. Əməkdaşlıq dərəcəsinin hesablanması məlum olmuşdur ki, jurnalda 1569 sayda çoxmüəllifli məqalə var. Onda IEEE TIFS jurnalının (1) düsturuna əsasən əməkdaşlıq dərəcəsi $1569 / 1639 = 0,96$ bərabərdir.

E) Məhsuldar müəllifin seçilməsi

Cədvəl 4-də bu jurnalda 2006-2017-ci illər ərzində ən çox məqaləsi çap olunan on müəllifin siyahısı verilmişdir.

CƏDVƏL 4. MƏHSULDAR MÜƏLLİFLƏRİN SIYAHISI

№	Müəllifin adı	Məqalə sayı
1.	JAIN A.K.	28
2.	HUANG J.W.	26
3.	SUSILO W.	25
4.	FRIDRICH J.	24

5.	LIU KJR	21
6.	MOULIN P.	17
7.	WU M.	16
8.	BARNI M.	15
9.	MU Y.	15
10.	PEREZ-GONZALEZ F.	14

F) Məqalələrin təşkilatlar üzrə paylanması

2006-2017-ci illər ərzində çap olunmuş 1639 məqalənin təşkilatlar üzrə paylanmasına nəzər saldıqda 71 məqalənin Çin Elmlər Akademiyası, 59 məqalənin Nanyang Texnoloji Universitetinin payına düşdüyü aşkarlanmışdır və cədvəl 5-də göstərilmişdir.

CƏDVƏL 5. MƏQALƏLƏRİN TƏŞKİLATLAR ÜZRƏ PAYLANMASI

	Təşkilatın adı	Məqalə sayı
1.	Çin Elmlər Akademiyası (Chinese Academy of Sciences)	71
2.	Nanyang Texnoloji Universiteti (Nanyang Technological University)	59
3.	Sinqapur Milli Təhsil İnstitutu (National Institute of Education Singapore)	59
4.	Maryland Universitet Sistemi (University System of Maryland)	56
5.	Kaliforniya Universiteti (University of California System)	52
6.	Nyu-York Suny System Dövlət Universiteti (State University of New York Suny System)	51
7.	Maryland College Park Universiteti (University of Maryland College Park)	48
8.	Miçigan Dövlət Universiteti (Michigan State University)	39
9.	Vollonqonq Universiteti (University of Wollongong)	33
10.	Milli Elmi-Tədqiqat Mərkəzi (Centre National de la Recherche Scientifique)	32

G) Məqalələrin ölkələr üzrə paylanması

Cədvəl 6-dan göründüyü kimi bu jurnalda çap olunan məqalələrin ölkələr üzrə paylanmasına görə də ABŞ və Çin ilk sıralardadır.

CƏDVƏL 6. MƏQALƏLƏRİN ÖLKƏLƏR ÜZRƏ PAYLANMASI

№	Ölkənin adı	Məqalə sayı
1.	ABŞ	677
2.	Çin	450
3.	Avstraliya	119
4.	Sinqapur	106
5.	İngiltərə	102
6.	İtaliya	101
7.	Fransa	70
8.	Tayvan	65
9.	Kanada	64
10.	Cənubi Koreya	60

2. İstinad üzrə analiz:

“İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri”
IV respublika konfransı, 14 dekabr 2018-ci il

A) İstinadların illər üzrə paylanması, illər üzrə istinadın orta sayı

Məlum olmuşdur ki, istinadların sayı hər il artır. Cədvəl 7-dən göründüyü kimi əgər 2006-cı ildə məqalələrə 16 dəfə istinad olunmuşdursa, 2017-ci ildə bu göstərici 8396-ya bərabər olmuşdur.

Cədvəl 7-dən göründüyü kimi ən çox məqalə və istinad 2014-2017-ci illəri əhatə edir.

CƏDVƏL 7. İSTINADLARIN İLLƏR ÜZRƏ PAYLANMASI

İl	Məqalə sayı	İstinad sayı	İstinadın orta sayı	Cəmi (məqalə sayı)	Cəmi (istinad sayı)
2006	46	16	0.34	263	1399
2007	70	165	2.36		
2008	70	447	6.39		
2009	83	771	9.29		
2010	85	855	10.1	544	6102
2011	121	976	8.07		
2012	160	1582	9.89		
2013	178	2689	15.1		
2014	182	3895	21.4	826	24123
2015	205	5204	25.4		
2016	216	6628	30.7		
2017	223	8396	37.6		

B) İstinad olunan sənədin növünün və sayının müəyyən olunması

Məlumdur ki, istinadlar müxtəlif növ sənədlərdən (məqalə, tezis, kitab və s.) edilə bilər. Ona görə də ən çox istinad olunan sənədin növünün və sayının tapılmasının da mühüm əhəmiyyəti vardır. Cədvəl 8-də ən çox istinad olunan 5 məqalə göstərilmişdir.

CƏDVƏL 8. ƏN ÇOX İSTINAD OLUNAN MƏQALƏLƏR

	Müəllifin adı	Məqalənin adı	İstinad sayı
1.	Li Jian; Li Xiaolong; Yang Bin; et al.	Segmentation-Based Image Copy-Move Forgery Detection Scheme 2015, vol. 10, iss. 3, p. 507-518	438
2.	Pevny Tomas; Bas Patrick; Fridrich Jessica	Steganalysis by Subtractive Pixel Adjacency Matrix 2010, vol. 5, iss. 2, p.215-224	326
3.	Chen Mo; Fridrich Jessica; Goljan Miroslav; et al.	Determining image origin and integrity using sensor noise 2008, vol. 3, iss. 1, p.74-90	298
4.	Kodovsky Jan; Fridrich Jessica; Holub Vojtech	Ensemble Classifiers for Steganalysis of Digital Media 2012, vol. 7, iss. 2, p.432-444.	290
5.	Fridrich Jessica; Kodovsky Jan	Rich Models for Steganalysis of Digital Images 2012, vol. 7, iss. 3, p868-882.	278

NƏTİCƏ

Məqalədə IEEE TIFS jurnalının 2006-2017-ci illər ərzində çap olunmuş buraxılışları analiz olunmuşdur. Analiz nəticəsində nəşr olunan məqalələrin və istinadların sayının hər il artdığı aşkarlanmışdır. Məqalələrin və istinadların sayının artması jurnalın IF göstəricisinin artmasına səbəb olmuşdur. Eləcə də, jurnalda çap olunan məqalələr arasında çoxmüəllifli məqalələr təkmüəllifli məqalələrdən üstünlük təşkil edir və jurnalda icmal məqalələrə çox az rast gəlinir. Burada diqqəti çəkən digər məsələ nəşrlərin ölkələr üzrə paylanmasında Sinqapur və Tayvan kimi ölkələrin G7 ölkələri sırasına daxil olmasını qeyd etmək olar.

- [1] R.Əliquliyev, N.İsmaylova, Bibliometria: müasir vəziyyəti, problemləri və inkişaf perspektivləri. Ekspres-informasiya. Bakı, 2015, 78 s.
- [2] A.Pritchard, Statistical bibliography or bibliometrics?. Journal of Documentation, 1969; 25(4): 348-349.
- [3] R.Əliquliyev, N.Ədigözəlova, “İnformasiya təhlükəsizliyi üzrə aparılan tədqiqatların bibliometrik analizi (2007-2016-cı illər)”. İnformasiya təhlükəsizliyinin aktual problemləri III respublika elmi-praktiki seminarı, 2017, s.56-58.
- [4] N.İsmaylova, “Bibliometric analysis of information security”, İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransının materialları, 2015, pp. 106-109.
- [5] C.Lu, W.Jen, W.Chang, “Trends in computer crime and cybercrime research during the period 1974-2006: A bibliometric approach”, Proceed. of Pacific Asia Workshop on Intelligence and Security Informatics (PAISI 2007), 2007; 244-250.
- [6] www.webofknowledge.com
- [7] A.Dhiman, Ethnobotany journal: a ten year bibliometric study. IASLIC Bulletin. 2000; 45(4):177-82.
- [8] S.K.Patra, P.Bhattacharya, N.Verma, Bibliometric study of literature on bibliometrics. DESIDOC Journal of Library and Information Technology. 2006; 26(1):27-32.
- [9] M.W.Neff, E.A.Corley, 35 years and 160,000 articles: a bibliometric exploration of the evolution of ecology. Scientometrics. 2009; 80(3): 657-82.
- [10] S. Thanuskodi, Bibliometric analysis of the journal Library Philosophy and Practice from 2005-2009. Library Philosophy and Practice (e-journal). 2010; 1-7.
- [11] L.Bormmann, R.Mutz, Growth rates of modern science: a bibliometric analysis based on the number of publications and cited references. Journal of the Association for Information Science and Technology. 2015; 66(11): 2215-22.
- [12] A.Abdı, N.Idris, R.Algulyev, R.Aligulyev, Bibliometric Analysis of IP&M Journal (1980–2015). Journal of Scientometric Research. 2018; 7(1): 54-62.

**BIBLIOMETRIC ANALYSIS OF THE JOURNAL
"IEEE TRANSACTIONS ON INFORMATION SECURITY" (2006-2017)**

Narmin Adigəzalova

Institute of Information Technology of ANAS, Baku, Azerbaijan
narmin66@gmail.com

Abstract - The paper performs bibliometric analysis of the articles published in years 2006-2017 in the journal IEEE Transactions on Information Forensics and Security (IEEE TIFS) indexed in Web of Science (WoS) database. The analysis is performed on the distribution of the articles and references by years, authors, organizations and countries.

Keywords: WoS, impact factor, reference, bibliometrics, bibliometric analysis.

İnternet-medianın monitorinqi alətləri və informasiya təhlükəsizliyi məsələləri

Səadət Abdullayeva

İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

sado.amea@gmail.com

Xülasə— Məqalədə İnternet-media resurslarında informasiya təhlükəsizliyinin təmin olunmasında media monitorinqin rolu araşdırılır, mediada təhlükəsizliyə təhdid törədə biləcək risklərdən qorunmaq üçün təkliflər irəli sürülür. Həmçinin İnternet-media və sosial mediada informasiya təhlükəsizliyinin təmin olunmasına imkan verən monitorinq və qiymətləndirmə xidmətləri göstərən şirkətlər haqqında məlumat verilir.

Açar sözlər— *İnternet-media; media monitorinq; medianın qiymətləndirilməsi; monitorinq alətləri; informasiya təhlükəsizliyi*

I. GİRİŞ

Müasir qloballaşma dövründə azad və müstəqil kütləvi informasiya vasitələri (KİV) cəmiyyətin həyatına təsir imkanlarına malikdir. Demokratik cəmiyyətlərdə KİV cəmiyyətin üzvlərinə əhəmiyyətli məsələlər üzrə müstəqil, obyektiv informasiya təqdim etdiyinə görə dördüncü hakimiyyət hesab edilir. KİV-in başlıca vəzifəsi cəmiyyəti onu maraqlandıran məsələlər barədə məlumatlandırmaq, zəruri informasiya ilə təmin etməkdir. Onun əsas funksiyası məhz ictimaiyyətin obyektiv informasiyaya olan tələbatını ödəməkdir. KİV bu vəzifəni informasiyanı qanunvericiliyə zidd olmayan üsullarla toplayıb hazırlamaq və yaymaqla həyata keçirməlidir.

KİV-in yeni növü olan İnternet-media ənənəvi media ilə müqayisədə, bir sıra üstünlüklərə malikdir: İnternet-media əlyətərlidir; minimal xərc tələb edir; hamı üçün açıqdır – istənilən şəxs qlobal kommunikasiya platformasına qoşula və informasiya mənbəyi kimi çıxış edə bilər; daha dinamik və çevikdir; əks əlaqə imkanları genişdir – auditoriyanın informasiya mənbəyi ilə qarşılıqlı təsir imkanı var; yüksək dərəcədə fərdiləşmə təklif edir; insanları vahid platformada birləşdirir və böyük həcmdə informasiya mübadiləsinə imkan verir [1].

İnternet-medianın media infrastrukturunda önəmli bir sahəyə çevrildiyi, əhalinin xeyli hissəsinin İnternet-media vasitəsilə informasiya əldə etdiyi bir dövrdə milli İnternet məkanının informasiya təhlükəsizliyinin təmin edilməsi zərurəti yaranmışdır. Bu baxımdan İnternet-medianın monitorinqi və informasiya təhlükəsizliyi ilə əlaqədar problemlərin araşdırılması vacib məsələlərdəndir.

II. İNTERNET-MEDİADA İNFORMASIYA TƏHLÜKƏSİZLİYİNİN TƏMİN OLUNMASI

Dövlət siyasətinin prioritet istiqamətlərindən biri də məhz, informasiyanın azad dövriyyəsinin təmin edilməsi, bu prosesin əsas aləti kimi medianın, o cümlədən İnternet-media resurslarının sərbəst fəaliyyətinə zəruri şəraitin yaradılmasıdır.

Dövlət qurumlarının veb-saytlarının informasiya siyasətinin əsas məqsədləri vətəndaşları öz fəaliyyətləri haqqında məlumatlandırmaq və onlarla əks əlaqəni təşkil etməkdir. Eyni zamanda, dövlət qurumları münafişə, sosial gərginlik yarada bilən, yanlış ictimai rəy formalaşdıran, hakimiyyət orqanlarının nüfuzuna ziyan vura bilən informasiya təhdidlərinə operativ reaksiya verməyə borcludurlar.

Şəbəkə vasitəsilə cəmiyyətə informasiya təsiri mexanizmi hər yerdə eynidir: müəyyən sifarişçi vəzifəni təyin edir, onun icraçıları bu vəzifə üçün ictimai təşkilatlardan, jurnalistlərdən, siyasi fəallardan, qeyri-formal hərəkət üzvlərindən, bəzi hallarda isə, kriminal və ekstremist strukturlardan ibarət şəbəkə strukturunu qururlar. Onların bir qismini qrantlarla, bəzilərinə siyasi piar vədləri ilə, digərlərini, sadəcə, pulla cəlb edirlər. Məhz onlar hərəkətverici qüvvədir, onlar insanları inandırma və öz arxaları ilə istənilən radikal aksiyalara apara bilərlər [1].

Digər tərəfdən, müasir dövrdə veb-texnologiyaların e-dövlətdə, mobil platformalarda, bank tranzaksiyalarında və s. ilə yanaşı, sosial media və İnternet-media resurslarında geniş istifadə olunması ilə onlar bədniyyətli hücüm hədəfinə çevrilir, bu isə, veb-sistemlərdə informasiya təhlükəsizliyinin təmin olunması məsələsinin aktuallığını artırır. İnternet-media resurslarında olan boşluqların əvvəlcədən müəyyən olunması yarana biləcək bu və ya digər problemləri aradan qaldırmağa kömək edə bilər.

İnformasiya təhlükəsizliyinin əsasında informasiyanın mühafizəsi məsələləri dayanır. İnformasiya hüquqi, texniki, fiziki, kriptografik üsullarla mühafizə olunur. İnformasiyanın mühafizəsi isə aşağıdakı hüquqi, təşkilati və texniki tədbirlər toplusunu özündə əks etdirir [2]:

- İnformasiyanın tamlığının qorunması;
- İnformasiyanın konfidensiallığının təmin edilməsi;
- İnformasiyanın əlyətərliliyinin təmin olunması;

İnternet-mediada informasiyanın mühafizəsində bu üç şərt təmin edilməlidir. Bunun üçün mediada, eləcə də İnternet-mediada informasiya təhlükəsizliyi məsələləri qanunlarla tənzimlənməlidir.

III. İNTERNET-MEDİANIN MONİTORİNQİ ALƏTLƏRİ

İnternet-medianın populyarlığının sürətlə artması, iqtisadi və ictimai-siyasi rolunun yüksəlməsi onun monitorinqi və analitikası üçün nəzərdə tutulmuş informasiya sistemlərinin yaradılmasını tələb edir [3].

Hazırda bazarda təklif olunan İnternet-media monitorinqi alətlərinin əksəriyyəti biznes məsələlərinin həllinə yönəlib. Onlar sosial mediada brendlərin, şirkətlərin, məhsulların və ya xidmətlərin adlarının neçə dəfə çəkildiyini müəyyən edir, istifadəçilərin onlara münasibətini (pozitiv, neqativ, neytral), rəylərin tonallığını aşkarlayır, rəy müəlliflərini cins, yaş, yaşayış yeri, maraqları və s. görə segmentlərə bölür [4].

Öz fəaliyyətinin auditoriya tərəfindən daima yüksək qiymətləndirilməsinə çalışan İnternet-media resursları üçün aşağıda qeyd olunan tədbirlərin görülməsi zəruridir [5]:

- bütün monitorinq tədbirləri kompleks şəkildə həyata keçirilməli;
- monitorinqin digər metodlar ilə uyğunluğu nəzərə alınmalı;
- KİV-in azadlığının hüquqi aspektləri yenidən işlənilməli;
- monitorinq zamanı KİV-in auditoriyasının kritik vəziyyət nöqtələri müəyyən olunmalıdır.

Sosial mediada monitorinq zamanı ilkin olaraq informasiyalar izlənilir, mətnlər analiz olunur, spam şərhlər müəyyən olunur. Növbəti addımlarda mətnlərin müxtəlif xüsusiyyətlərinə görə daha ətraflı təhlil aparılır. Daha sonra isə vizualizasiya və yarana biləcək təhdidlərə qarşı tədbirlər görülür [3].

Qeyd edək ki, populyar sosial şəbəkə servislərində bir sıra monitorinq alətləri mövcuddur. Məsələn, Facebook Insights, Google Analytics, Twitter Analytics, LinkedIn Analytics, Pinterest Analytics və s.. Hazırda ingilisdilli SumAll, Sysomos, UberVU, SproutSocial portalları, rusdilli InfoWatch Kribrum, YouScan, Brand Analytics, Babkee, BrandSpotter, Buzz Look, IQBuzz, SemanticForce, Wobot, və s. sosial media monitorinqi xidmətləri təklif edilir [1].

“InfoWatch Kribrum” İnternet-medianın, eləcə də sosial medianın monitorinqi və analizinin avtomatlaşdırılmış sistemidir. Sistem gün ərzində real vaxt rejimində mətnlərin tonallığını müəyyən etməklə, həmçinin informasiya hücumlarını və spamları aşkar etməklə müxtəlif sosial şəbəkələrdə, bloqlarda və 20 min İnternet-media resursunda 250 milyon istifadəçi hesabında 60 milyondan çox mesajın analizini təqdim edir [6]. “InfoWatch Kribrum” vasitəsilə əldə

olunmuş məlumatların əsasını İnternetdə sifarişçini maraqlandıran mövzular üzrə informasiya sahəsi üzrə vəziyyətə dair aylıq, həftəlik və gündəlik analitik hesabatlar təşkil edir. Sistemin funksional imkanlarına məlumatların toplanması, analizi, auditoriya ilə interaktiv əlaqə, sistem üzərində birgə iş, hesabatların işlənməsi və inteqrasiya daxildir.

Bu sistem, həmçinin İnternet-media resurslarında informasiya təhlükəsizliyi üçün həllər təklif edir:

- sosial mediada informasiya hücumlarının aşkar edilməsi;
- informasiya hücumunun mənbəyinin və onun yayılması yollarının üzə çıxardılması;
- veb-sayta şirkətin əməkdaşları tərəfindən təhdidlərin aşkara çıxarılması;
- korporativ informasiyanın qanunsuz yayılmasının aşkar edilməsi;
- onlayn mühitdə istifadəçilərin məxfiliyinin qorunmasına xidmət edən TOR proqram təminatı üzrə axtarış.

Qeyd olunan sistemlərin hər biri onlayn media resurslarında informasiya təhlükəsizliyinin təmin olunmasında böyük imkanlara malikdir.

Azərbaycanda isə, medianın monitorinqi və qiymətləndirilməsini Media Təqib Mərkəzi, “Kalibri” media monitorinq şirkəti, Azərbaycan Media Monitorinqi İnstitutu, “MC&S” media monitorinq qrupu və digər şirkətlər həyata keçirir [4]. Bu şirkətlər medianın və sosial şəbəkələrin analizini və marketing strategiya və taktikasının qurulması istiqamətində geniş spektrli, operativ və peşəkar xidmətlərin göstərilməsini təklif edir. Onların xidmət sahələrinə ölkə mediası, xarici ölkələrin mediası, mətbuat, televiziya yayımları, radio, sosial media, İnternet-media, xəbər agentlikləri, televiziya reklamlarının monitorinqi və s. daxildir.

Ölkəmizdə monitorinqi həyata keçirən şirkətlərin sayı kifayət qədər olsa da, medianın monitorinqinə kompleks yanaşmalar tələb olunur. Bunun səbəbi, monitorinqin aparılmasında pərakəndəliyin mövcud olması, bu sahənin qanunlarla tənzimlənməməsi nəticəsində etimad mühitinin zəif olması və informasiya təhlükəsizliyinə təhdidlərin olması, zəruri mədəniyyətin formalaşmaması, o cümlədən İnternet resursları üçün milli statistika mexanizmlərinin mövcud olmamasıdır.

IV. MEDİADA İNFORMASIYA TƏHLÜKƏSİZLİYİNƏ KOMPLEKS YANAŞMA

Məlumdur ki, informasiya texnologiyaları və xidmətlərdən asılılığın artması ilə dezinformasiya və təbliğat üçün potensial risklər yüksəlir. İnformasiyanın dayanıqlılığı fəvqəladə vəziyyətlərdə (informasiyanın təhlükəsizliyinə təhdidlər olduqda) tədbirlərin görülməsi sistemi vasitəsilə təmin olunmalıdır (Şəkil 1.) [7]. Media müasir cəmiyyətin ayrılmaz

tərkib hissəsi olduğundan informasiya təhlükəsizliyinə kompleks yanaşmanın işlənilməsi zəruridir.

Şəkil 1. Mediada informasiya təhlükəsizliyinə kompleks yanaşma [7]

Cəmiyyət informasiyanın sabitliyini yüksəltməli və fəvqəladə vəziyyətləri idarəetmə metodları vasitəsilə informasiya təhdidləri ilə mübarizə aparmalıdır. Fəvqəladə vəziyyətləri idarəetmə prosesi dörd mərhələdən ibarətdir: xəbərdarlıq, hazırlıq, reaksiya və bərpa.

Xəbərdarlıq potensial fəvqəladə vəziyyətlərin neqativ nəticələrini minimallaşdırma bilər. Qabaqlayıcı tədbirlər ictimaiyyətə dezinformasiyanın təhlükələri barədə məlumat verilməsi və ictimai müzakirələrə onun neqativ təsiri haqqında məlumatlandırılmanı nəzərdə tutur.

Hazırlıq erkən xəbərdarlıq sistemi rolunu oynayır və medianın monitorinq mexanizmlərini və məzmun barədə məlumatlandırılmanı nəzərdə tutur. Hazırlıq mərhələsində ənənəvi KİV və sosial mediada təhrif olunmuş informasiyanın və onun mövcudluğu haqqında xəbərdarlığın müəyyən olunması üçün insan resursları və texnoloji resurslar istifadə olunur.

Reaksiya mexanizmləri dezinformasiya və təbliğat xarakterli informasiya ilə mübarizə üçün istifadə edilən əks-tədbirləri təşkil edir. Onlar özündə qanunvericilik bazasının işlənilməsi və KİV-in nizamlanması orqanının effektivliyinin artırılmasını, həmçinin strateji kommunikasiyalar üçün ictimaiyyətin iştirakının gücləndirilməsi və institusional potensialın artırılmasını ehtiva edir.

Nəhayət, **bərpa** mərhələsi kütləvi informasiya vasitələrinin ictimaiyyətə vicdanla xidmət etdiyi, cəmiyyətin işə, manipulyasiyalara ayıq olduğu bir mühitin yaradılması üçün nəzərdə tutulmuşdur. Bunun üçün maarifləndirici proqramlar üçün media savadlılığını və kritik düşüncə qabiliyyətini yüksəldəcək uzunmüddətli investisiyalar tələb olunur [7].

İnternet-media resurslarının monitorinqinin aparılması media qurumlarına olan kiberhücumlar zamanı aşağıdakıların həllinə imkan verir [8]:

- kiberhücumu həyata keçirmək imkanının ləğv olunması və bununla zərərin qarşısının alınması;
- zərərin minimuma endirilməsi istiqamətində tədbirlərin görülməsi;

- təhlükəyə meyilli resursların sayının azaldılması;
- problemin aradan qaldırılma vaxtının azaldılması;
- erkən xəbərdarlığın təmin olunması;
- hücumdan sonra cinayətkarın aşkar edilməsi.

İnternet-mediada etibarlı informasiya təhlükəsizliyi sistemi qurmaq üçün, ilk növbədə, hüquqi baza formalaşdırılmalıdır. Azərbaycanda bu sahədə müəyyən hüquqi baza mövcuddur. Lakin sürətlə inkişaf edən və bütün sahələrə getdikcə daha dərinlən nüfuz edən informasiya texnologiyalarının formalaşdırdığı informasiya mühitinin lazımi səviyyədə hüquqi tənzimlənməsi üçün qanunvericilik sistemi də baş verən dəyişikliklərə, yeniliklərə çevik reaksiya verməli, daim yenilənməli, təkmilləşməlidir.

NƏTİCƏ

İnternet-mediada informasiya təhlükəsizliyinin təmin olunması üçün aşağıdakı tədbirlərin görülməsi təklif edilir:

- Mediada informasiya təhlükəsizliyi sahəsində qanunvericilik bazasının formalaşdırılması;
- İnternet-media resurslarında yayılan təbliğat xarakterli informasiya, dezinformasiya, eləcə də milli-mənəvi dəyərlərə zidd olan informasiyalar haqqında erkən xəbərdarlıq sisteminin hazırlanması;
- Milli Televiziya və Radio Şurasının İnternet-televiziya və radioların monitorinqinə dair səlahiyyətlərinin genişləndirilməsi;
- İnformasiya təhlükəsizliyi və risklərinin yeni problemlərinin həlli üçün KİV haqqında qanunvericiliyə əlavə və dəyişikliklərin edilməsi;
- İnternet-medianın inkişaf strategiyasının hazırlanması, jurnalistlərin fəaliyyətinin stimullaşdırılması üçün əlverişli şəraitin yaradılması;
- Medianın və informasiya savadının dövlət qurumları tərəfindən dəstəklənməsinin təmin edilməsi;

Qeyd olunan təkliflərin ölkə səviyyəsində reallaşdırılması üçün bir sıra ölkələrdə bu sahədə tətbiq olunan təcrübədən istifadə edilməsi müsbət nəticələr verə bilər.

Beləliklə, İnternet-mediada insan hüquqları və ifadə azadlığını pozmadan kontentin monitorinqi və qiymətləndirilməsi cəmiyyətin nəbzini tutmağa, əhval-ruhiyyəsini müəyyən etməyə, gözləntilərini aşkarlamağa imkan verir. İnternet-media, eləcə də sosial medianın monitorinqi vasitəsilə meydana çıxan təhdidləri vaxtında aşkarlamaq və əks-tədbirlər həyata keçirmək mümkündür.

ƏDƏBİYYAT

- [1] İmamverdiyev Y.N., Sosial media və təhlükəsizlik problemləri, İnformasiya cəmiyyəti problemləri, 2016, №2, 19–25
- [2] Mahmudov R., İnformasiya təhlükəsizliyinin normativ-hüquqi bazası //Azərbaycan xalqının ümummilli lideri Heydər Əliyevin 90 illik

yubileyinə həsr olunmuş “İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı”, 17-18 may, 2013

- [3] M.D. Sykora et al. National security and social media monitoring: A presentation of the emotive and related systems / European Intelligence and Security Informatics Conference, 2013, pp. 172-175.
- [4] R.M. Əliquliyev, S.R. Ağayeva, “İnternet-media resurslarının monitorinqi: müasir vəziyyətləri, problemləri və inkişaf perspektivləri. İnformasiya cəmiyyəti problemləri, 2016, №1, s. 63 – 70.
- [5] Шарков Ф.И., Баранова В.И., “Аудитория и мониторинг СМИ.” 2005, 110 стр.
- [6] InfoWatch Kribrum, <https://infowatch.com/products/kribrum>
- [7] Д.Марин, Повышение устойчивости информации в медиа-секторе, “Media Forward” Серия политических обзоров, No 4, 2018, 8 с.
- [8] E. E. Schultz, “Continuous monitoring: What it is, why it is needed, and how to use it.” SANS Institute InfoSec Reading Room, 2011, 16 p.

ONLINE MEDIA MONITORING TOOLS AND INFORMATION SECURITY ISSUES

Saadat Abdullayeva

Institute of Information Technology of ANAS, Baku,
Azerbaijan

sado.amea@gmail.com

Abstract – The role of media monitoring in ensuring information security in online media resources is being investigated in the article and is offered suggestions for protection against potential threats to security in media. It also provides information about monitoring and evaluation services that provide information security in online media, as well as in social media.

Keywords – online media; media monitoring; media evaluation; monitoring tools; information security

Estimating the text preprocessing algorithms for sentence classification

Suleyman Suleymanzade

Institute of Information Technology ANAS, Baku, Azerbaijan
suleyman.suleymanzade@bhos.edu.az

Abstract – Estimating the text preprocessing algorithms in machine learning classification task helps to select the most accurate combination of word embedding text processing algorithms to map the test data samples to appropriate labels. Increasing the accuracy in classification of text data improves afterwards the response to queries in search engines and gives more relevant results. This work includes several preprocess text data techniques and their combinations for following sentence classification by using support vector machine (SVM).

I. INTRODUCTION

Text classification is one of the important fields of artificial intelligence that includes Natural language processing, machine learning [1] [2] and deep learning techniques [3] [4] [5]. The automation of the text classification process gives ability to classify and store documents (or metadata with link associated with web document) by topics. In search engines it helps to search document not only by the keywords that exist in the content of document but also by the additional semantic term that text classifier added to the searched web content. Also, the classification helps to store content metadata in the backend in sorted and structured way. The search engine becomes more relevant.

II. PROBLEM STATEMENT

The goal of this work is to use various text preprocessing methods and their combinations to review and analyzing text data which was gathered (*mined*) from the internet for the further text classification process. The classification in this work is done on the text data. So, because of the labeled data the classification method belongs to a field of supervised learning.

There are many machine-learning and deep-learning methods for a supervised learning. In this work the

different representing words techniques will be processed by the SVM (support vector machine) [6] with different kernel functions and other exclusively belonged to SVM's parameters. The problem of the text data that machine-learning algorithms such as SVM cannot handles this type of data. The only data representation that can be fitted by ML models are the number representation of the model. This type of data representation calls feature-vector. All the preprocess techniques that presented in this work use to transform the mined text data to feature vectors.

III. TEXT PREPROCESSING

Text processing in Natural Language Processing (NLP) represents the mapping process between the word (or phrase, document or even documents' clusters, depends on the granularity of selected data and task) and numerical value. To produce such data representation the following approaches are used. There are two main strategies to separate word embedding:

- The strategy based on frequency
- The strategy based on predictions.

The prediction-based vectors used to predict the next word. To predict a text data there are popular methods such as continues bag of words (CBOW) [7] and Skip-Gram [8]. The text data that processed by these methods are processed by machine learning or deep neuron networks models. The frequency based methods. In current work, all methods to classify the text data are frequency based.

A. The Vector Space Model

The Vector space model [9] [10] also known as traditional method represented as one-hot binary vector. Where vector's size equals to the total unique documents' vocabulary. In this binary vector representation: one -

shows the index position where certain word existed, other one zeros respectively.

The implementation of this data structure is easy, but it uses huge amount of memory because of redundant zeros. One solution for memory optimization – is to create data structure where instead of very long vector sets of zeros there is special key with number which shows number of zeros between ones. But even such optimization saves memory to store data, but not during the processing where data must be converted again to the one-hot binary vector.

Second problem with such representation of data that it not stores semantic information about stored data. Traditional model not belongs to a frequency or prediction-based models because this representation of the word embedding shows only the existence of text in data in whole corpus and not shows the number of occurrence and sequence.

B. Count based model

The count-based model unlike the traditional method stores number of words that appears in corpus the documents. If the number of the unique words appeared in the document is n and the number of the document is d then the matrix size that stores the whole data representation must be $n * d$.

The number of appeared words gives additional information about the word value. As well as in the traditional method the count-based model is easy to program, but the cons of this approach is that not always the word that is repeating more has more values. For example, in English language the articles such as “the”, “a” repeat many times in the documents but they cannot be considered as determined factor for the classification of document’s text. Considering the sample that given below

C. TF-IDF

TF-IDF [11] [12] stand for - “term frequency - inverse document frequency”. Unlike count based model, TF-IDF based on idea that if word has appeared in most of the documents, then probably that word is not relevant to a document. For example: “and”, “the”, “or” they appear in most of the text documents, but they don’t give meaning to documents’ semantic.

The relevant term must appear many times in small group of documents from the observed document corpus. This observation can be described mathematically. TF – the proportion of term number appearing in one document to the number of words in the particular document. And IDF is the logarithmic proportion of total number of documents to the number of documents where the term appears.

$$TF(t, d) = f(t, d) / \sum_{t' \in d} f(t', d) \quad (1)$$

$$IDF(t, D) = \log \frac{N}{|\{d \in D : t \in d\}|}$$

Example:

There are two documents.

TABLE I. SENTENCE REVIEW

Document 1		Repeating
RNN		6
uses		2
To		2
calculate		1
Data		1
Document 2		Repeating
RNN		0
uses		2
To		2
calculate		2
Data		1

$$TF(RNN, Document1) = \frac{6}{12} = \frac{1}{2}$$

$$IDF(RNN) = \log \left(\frac{2}{1} \right) = 0.301$$

$$TFIDF(RNN, Document1) = \frac{1}{2} * 0.301 = 0.1505$$

$$TF(To, Document1) = \frac{2}{12} = \frac{1}{6}$$

$$IDF(To) = \log \left(\frac{2}{2} \right) = 0$$

$$TFIDF(To, Document1) = 0$$

IV. MODEL

One of the popular methods in machine-learning to classify the samples on different categories is the support vector machine (SVM) [6]. There are different types of SVM models: linear and non-linear. *Linear* If the samples that must be classified separated linearly then the idea based on the “optimal” boundary of linear hyperplane that separates one set of samples from the other.

Figure 1 SVM with closest boundary

The vectors with the closest to the boundary they are the support vectors. The boundary of the hyperplane represented by formula.

$$\mathbf{w}^T \mathbf{x} + \mathbf{b} = 0 \quad (2)$$

$\mathbf{w}$ – weight coefficient, $\mathbf{b}$ – bias. Consider the black dots are the set $\mathbf{x}_+$ and the white dots is other set $\mathbf{x}_-$ respectively. The length between trained $\mathbf{x}_i$ which located on the opposite sites (the margin) is calculated by

$$\text{margin} = |\bar{\mathbf{x}}_- - \bar{\mathbf{x}}_+| \frac{\bar{\mathbf{w}}}{\|\bar{\mathbf{w}}\|} \quad (3)$$

Because the aim is to maximize the margin. The optimization is considered as

$$\|\bar{\mathbf{w}}\|^2 = \mathbf{w}^T \mathbf{w} \text{ minimize subject to } \mathbf{y}_i(\mathbf{w}^T \mathbf{x}_i + \mathbf{b}) \geq 1,$$

Where
$$\begin{cases} \mathbf{y} = \mathbf{1}, & \mathbf{y} \in \{\mathbf{x}_+\} \\ \mathbf{y} = -\mathbf{1}, & \mathbf{y} \in \{\mathbf{x}_-\} \end{cases} \quad (4)$$

The optimization provided by Lagrange's [13] [14] multipliers method.

$$L(\alpha_i, \mathbf{b}, \mathbf{w}) = \frac{1}{2} \mathbf{w}^T \mathbf{w} - \sum_i \alpha_i [\mathbf{y}_i(\mathbf{w}^T \mathbf{x}_i + \mathbf{b}) - 1] \quad (5)$$

Where $\alpha_i \geq 0$ is the indeterminate coefficient. The partial derivative of w and b is

$$\begin{aligned} \frac{\delta L}{\delta w} &= w - \sum_i \alpha_i y_i x_i \\ \frac{\delta L}{\delta b} &= - \sum_i \alpha_i y_i \end{aligned}$$

By rewriting equation 5

$$\begin{aligned} L(\alpha_i, \mathbf{b}, \mathbf{w}) &= \frac{1}{2} \left(\sum_i \alpha_i y_i x_i \right)^T \left(\sum_j \alpha_j y_j x_j \right) \\ &\quad - \sum_i \alpha_i y_i \left(\sum_j \alpha_j y_j x_j \right)^T x_i + \sum_i \alpha_i \\ &= \frac{1}{2} \mathbf{w}^T \mathbf{w} \\ &\quad - \sum_i \alpha_i y_i \mathbf{w}^T x_i - \mathbf{b} \sum_i \alpha_i y_i + \sum_i \alpha_i \end{aligned}$$

$$L(\mathbf{w}, \mathbf{b}, \mathbf{a}) = -\frac{1}{2} \sum_i \sum_j \alpha_i \alpha_j y_i y_j x_i^T x_j + \sum_i \alpha_i \quad (6)$$

L has to be maximized subject to α . The optimization defines as the reduction of the quadratic problem. The

solution of this problem represented by the following equation.

Find Max

$$\frac{1}{2} \sum_i \sum_j \alpha_i \alpha_j y_i y_j x_i^T x_j + \sum_i \alpha_i \quad (7)$$

According the

$$\sum_i \alpha_i y_i = 0, \alpha \geq 0 \quad (8)$$

V. EXPERIMENT

The dataset that was used in presented work is “20 Newsgroups”¹. This dataset was collected by Ken Lang and it represents the collection of approximately 20,000 newsgroup documents. The data is mapped into 20 different groups (*table II*) but not preprocessed as vectors of numbered data.

TABLE II. “20NEWSGROUP” DATASET LABELS

comp.graphics comp.os.ms-windows.misc comp.sys.ibm.pc.hardware comp.sys.mac.hardware comp.windows.x	rec.autos rec.motorcycles rec.sport.baseball rec.sport.hockey	sci.crypt sci.electronics sci.med sci.space
misc.forsale	talk.politics.misc talk.politics.guns talk.politics.mideast	talk.religion.misc alt.atheism soc.religion.christian

For this experience the various combination of preprocessing algorithms was used (*table 3*). In first and second experience the datasets passed through stemming [15] with respect to English language dictionary. For data stemming the Natural Language Toolkit NLTK² standard library was used. The stemming increases probability of mapped data to the data labels.

Then TF-IDF algorithm created vector of numbered data. After TF-IDF word-embedding process the dataset was separated on 80% of train and 20% of test parts. For training datasets in first experience the linear SVM with logistic regression was used. The accuracy after testing was about $\approx 81,67\%$. In second experiment the same preprocess method TF-IDF with stemming was used but with *Stochastic Gradient Descent (SGD)* [16] optimization technique the accuracy was increased $\approx 82,38\%$.

After the same preprocessing method and model the SGD shows better results therefore the same optimization technique was used in third and fourth experiment. In fourth and fifth experiments the filtered n-gram techniques with combination of TF-IDF was used to preprocess the data for the linear SVM model with SGD. In

¹ <http://qwone.com/~jason/20Newsgroups/>

² <http://www.nltk.org/>

third experiment the n-grams with sizes 1 and 2 was selected. The results show that classification accuracy increased to $\approx 89.791\%$. In fourth experiment additional n-

TABLE III. CLASSIFICATION RESULTS

Preprocess	Classifier	Regression	Accuracy
TF-IDF with stemming	SVM Linear	Logistic	81.67%
TF-IDF with stemming	SVM Linear	SGD	82.38%
Filtered n-gram with (1,2) range and TF-IDF	SVM Linear	SGD	89.79%
Filtered n-gram with (1,2,3,4,5) range and TF-IDF	SVM Linear	SGD	92.45%

VI. CONCLUSION

As experiments show the different combinations of text data preprocessing algorithms plays significant role in machine learning classification field. Even when the model to train data was selected the same (in case of this work SVM)

REFERENCES

- [1] S. B. Kotsiantis, "Supervised Machine Learning: A Review of Classification Techniques," *Informatica*, vol. 31, pp. 249-268, 2007.
- [2] M. Krendzelak and F. Jakab, "Text categorization with machine learning and hierarchical structures," in *13th ICETA*, Stary Smokovec, Slovakia, 2015.
- [3] D. B. Kamran Kowsari, "HDLTex: Hierarchical Deep Learning for

grams filters with sizes 1, 2, 3, 4 was added and the accuracy was increased $\approx 92.456\%$.

Text Classification," University of Virginia, Charlottesville, VA.

- [4] S. H. Anil Kumar Sharma, "Application of Deep Learning Techniques for Text Classification on Small Datasets," *IJESCI*, vol. 8, no. 4, 2018.
- [5] D. H. Tom Young, "Recent Trends in Deep Learning Based Natural Language Processing," Cornell University, 2017.
- [6] C. C. Vladimir Vapnik, "Support-Vector Machine," in *Machine Learning*, Boston, 1995.
- [7] K. C. Tomas Mikolov, "Efficient Estimation of Word Representations in Vector Space," Cornell University, 2013.
- [8] B. A. David Guthrie, "A Closer Look at Skip-gram Modelling David," University of Sheffield, Sheffield.
- [9] W. Salton, "A vector space model for automatic indexing," *Communications of the ACM*, vol. 18, no. 11, pp. 613-620, 1975.
- [10] V. R. Michael Wong, "Vector Space Model of Information Retrieval - A Reevaluation.," in *Proceedings of the 7th annual international ACM SIGIR*, 1984.
- [11] J. Ramos, "Document, Using TF-IDF to Determine Word Relevance," Rutgers University, NJ.
- [12] S. Robertson, "Understanding Inverse Document Frequency: On theoretical arguments for IDF," Microsoft Research 7 JJ Thomson Avenue, Cambridge CB3 0FB.
- [13] P. Busotti, "Historical Paper On the Genesis of the Lagrange Multipliers," *JOURNAL OF OPTIMIZATION THEORY AND APPLICATIONS*, vol. 117, 2003.
- [14] H. Li, "Lagrange Multipliers and their Applications," University of Tennessee, Knoxville, 2008.
- [15] A. G. Jivani, "A Comparative Study of Stemming Algorithms," Department of Computer Science & Engineering The Maharaja Sayajirao University of Baroda, Vadodara, India, 2011.
- [16] S. M. Herbert Robbins, "A Stochastic Approximation Method," University of North Carolina, North Carolina, 1951.
- [17] B. S. Nello Christianini, "Support Vector Machines and Kernel Methods," *AI Magazine*, vol. 23, no. 3, 2002.

İqtisadi inkişafın inklüzivlik səviyyəsinin yüksəldilməsində İKT və onun təhlükəsizliyi problemləri

Ələvsət Əliyev

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

alovsat_qaraca@mail.ru

Xülasə —Məqalə iqtisadi inkişafın inklüzivlik səviyyəsinin yüksəldilməsində İKT vasitələrinə və onların təhlükəsizliyi problemlərinə həsr olunmuşdur. İqtisadiyyatda yeni inkişaf meylləri və istiqamətləri təhlil olunmuşdur. Cəmiyyətin və iqtisadiyyatın inklüziv inkişafının əhəmiyyətliyi şərh olunmuşdur. Inklüziv cəmiyyətin və iqtisadiyyatın formalaşması səviyyəsinin regional-sektorial və beynəlxalq qiymətləndirilməsi məsələləri araşdırılmışdır. Azərbaycanda inkişafın inklüzivliyinin beynəlxalq qiymətləndirilməsinə baxılmışdır. İqtisadi inkişafın inklüzivlik səviyyəsinin yüksəldilməsi mexanizmləri müəyyənləşdirilmişdir. Inklüzivlik səviyyəsinin yüksəldilməsində İKT və onun təhlükəsizliyi üzrə bəzi tövsiyələr verilmişdir.

Açar sözlər — iqtisadi inkişafın inklüzivliyi, inklüzivlik səviyyəsi və indeksi, inklüzivlik göstəriciləri, inklüzivliyin qiymətləndirilməsi, inklüziv İKT, İKT-nin təhlükəsizliyi.

GİRİŞ

Dünya iqtisadiyyatının əsas inkişaf meylləri və istiqamətləri biliklər iqtisadiyyatının və cəmiyyətin formalaşmasına yönəlmişdir [1]. Cəmiyyətin gələcəyi biliklərə və texnologiyalara əsaslanan iqtisadiyyata keçidi təmin edəcək dövlətin fəaliyyət siyasətindən asılıdır. Bu siyasət biliklər iqtisadiyyatının imkanlarının hamıya açıq və ölçətan olmasını, həmçinin onun asılı olduğu informasiya infrastrukturunun təhlükəsizliyini, dinamikliyini və dayanıqlılığını təmin etməlidir [2].

Hökumət İKT-yə hazırkı və gələcək inkişaf üçün vasitə kimi baxaraq, onun inkişaf etdirilməsi üçün hər cür dəstəyi təmin etməkdədir [3]. Biliklər cəmiyyətinin və iqtisadiyyatının formalaşmasında bütün vətəndaşların, xüsusilə də maddi və fiziki cəhətdən daha çox müdafiəyə ehtiyacı olanların maraqları nəzərə alınmalıdır. Davamlı, biliklərə əsaslanan iqtisadiyyatın yaradılması ümumi və xüsusi, eləcə də ömürboyu təhsillə, tədqiqatlarla mümkündür. Elm, təhsil, mədəniyyət, səhiyyə bütün vətəndaşlar üçün mümkün və açıq olmalıdır [4]. Biliklərə əsaslanan iqtisadiyyat cəmiyyətin hər bir üzvünün və hissəsinin töhfələrindən asılıdır. Bilikli, təhsilli və bacarıqlı vətəndaşlar regionun və ölkənin inkişafına, rifah və əmin-amanlığına daha çox fayda verə bilərlər. Ona görə də cəmiyyətdə inkişafın inklüzivlik səviyyəsinin artırılmasında bütün vasitələrdən, o cümlədən ən müasir innovativ

texnologiya olan İKT-dən maksimum yararlanmaq çox aktual və əhəmiyyətli bir məsələdir [5].

I. CƏMİYYƏTİN VƏ İQTİSADİYYATIN İNKİŞAFININ İNKLÜZİVLİYİ

Cəmiyyətin və ya iqtisadiyyatın inklüziv əsaslar üzərində inkişafı zamanı sosial-iqtisadi, ictimai-siyasi, elmi, mədəni, humanitar, idarəetmə, istehsal, xidmət proseslərinin iştirakçılarına cəmiyyətin hər bir sahəsi, hər bir üzvü üçün faydaları olan bərabər imkanlar yaradır. Belə bir inkişaf konsepsiyası iqtisadiyyatın ənənəvi modellərini genişləndirir, sosial sahədə bərabərliyə, insan kapitalına, ətraf mühitin keyfiyyətinə, sosial müdafiəyə və ərzaq təhlükəsizliyinə xüsusi diqqət yetirir [6].

Cəmiyyətin inklüzivliyi bir çox kompleks xarakterli məsələləri əhatə edir. Buraya cəmiyyət üzvlərinin hamısının, xüsusilə müəyyən fiziki qüsurları olanların işləyə bilmək, təhsil ala bilmək, fəaliyyət göstərmək, cəmiyyətə inteqrasiya oluna bilmək, idarəetmə proseslərində iştirak edə bilmək, normal əmək haqqı almaq, normal yaşamaq, normal tibbi yardım almaq, özünü müdafiə edə bilmək və s. kimi əməllər daxildir. Bu məsələlər ayrı-ayrılıqda inklüziv təhsil, inklüziv elm, inklüziv tibb, inklüziv mədəniyyət, inklüziv ədəbiyyat, inklüziv KİV, inklüziv əyləncələr, inklüziv idman və s. kimi müvafiq sektorlarda həll olunur. Hər sahənin də özünə məxsus normativləri, texnika və texnologiyaları, vasitə və mexanizmləri vardır və ya yeniləri işlənilməlidir. Ayrıca götürülmüş problemlər həmin problemin aid olduğu sahənin inklüzivliyindən, inklüzivlik səviyyəsindən asılı olaraq həll edilir. Sahə inklüzivlikləri isə daha çox iqtisadiyyatın inklüzivliyindən və cəmiyyətin inklüzivliyindən asılıdır.

II. İNKLÜZİV CƏMİYYƏTİN VƏ İQTİSADİYYATIN FORMALAŞMASI SƏVİYYƏSİNİN REGIONAL-SEKTORIAL QIYMƏTLƏNDİRİLMƏSİ MƏSƏLƏLƏRİ

Cəmiyyətin inklüzivliyi dövlət tərəfindən daimi olaraq diqqətdə saxlanılan bir prosesdir. Bu prosesi tənzimləmək üçün onu müntəzəm olaraq qiymətləndirmək zəruridir. Qiymətləndirmə beynəlxalq milli, regional və sektorial aspektlərdə ola bilər.

Milli inklüzivlik səviyyəsinin qiymətləndirilməsi isə özü də bir neçə səviyyədə və aspektdə həyata keçirilə bilər:

- I səviyyə – ümumdövlət və ya makro səviyyədə inklüzivlik;
- II səviyyə – regional və ya ayrı-ayrı şəhər və rayonların inklüzivliyi;
- III səviyyə – sahələrarası və ya sahə inklüzivliyi;
- IV səviyyə – mikro və ya müəssisələr, istehsal səviyyəsində inklüzivlik;
- V səviyyə – evlərdə, fərdi ailələrdə inklüzivlik;
- VI səviyyə – özəl bölmədə, qeyri-dövlət strukturlarında inklüzivlik;
- VII səviyyə – qeyri-dövlət və dövlət idarəetməsində inklüzivlik.

Hər bir səviyyədə uyğun yekun sub-indeks və həmin sub-indeksi formalaşdıran alt göstəricilər və indikatorlar sistemi tərəfimizdən işlənilməkdədir. Bununla yanaşı bir çox beynəlxalq təşkilatlar da ölkələrin inklüzivlik səviyyəsini qiymətləndirməyə çalışırlar. Belə bir qiymətləndirməni Dünya İqtisadi Forumu da işləmişdir.

Dünya İqtisadi Forumu mütəxəssislərinin işləmiş olduğu beynəlxalq metodologiyaya müvafiq olaraq müntəzəm olaraq bir çox ölkələrin müqayisəli şəkildə İnküziv İnkişaf İndeksi hesablanır və nəşr edilir [7]. İnküziv inkişaf indeksi 3 əsas indikator olmaqla, 12 sub-indikatora əsasən formalaşır. “Artım və İnkişaf”, “İnküzivlik”, “Nəsilərarası bərabərlik və dayanıqlılıq” əsas indekslər olmaqla inkişaf etmiş və inkişafda olan ölkələrin reytingini formalaşdırır.

Hesabatın metodologiyasına əsasən Cini əmsalı [8] sub-indikatoru 0-100 bal arasında dəyişir. Əmsal 0 bal olduqda əhali arasında bərabərlik ən yüksək səviyyədə hesab olunur. 100 bal olduqda isə əhali arasında bərabərsizlik ən yüksək səviyyədə olmaq kimi qiymətləndirilir. Bu indeksin hesablanması fiziki şəxslər və ev təsərrüfatlarında çalışan insanlar arasında gəlirlərin bərabər və ədalətli şəkildə bölünməsinə özündə ehtiva edir. Qeyd olunan İnküzivlik göstəricisinin digər sub-indikatoru olan median gəliri indikatoru özündə makroiqtisadi parametrləri cəmləşdirir. Sub-göstəricisinin hesablanması əsas məqsəd ölkədə əhalinin alıcılıq qabiliyyətinin hesablanması və qiymətləndirilməsidir.

Beynəlxalq iqtisadi ədəbiyyatlarda asılılıq indeksi əhalinin neçə faizinin işlək olduğu və gəlir götürmək qabiliyyətinə malik olduğunu ölçür [9]. Sözügedən əmsalın çox olması əhali arasında iqtisadi cəhətdən fəal olmayan əhalinin çox olması deməkdir. Bu isə sosial təminat, sosial müdafiə və səhiyyə xərclərinin daha çox olmasını şərtləndirir və iqtisadiyyatda əlavə dəyər yaratma qabiliyyətinə mənfi təsir edir.

III. AZƏRBAYCANDA İNKİŞAFIN İNKÜZİVLİYİNİN BEYNƏLXALQ QIYMƏTLƏNDİRİLMƏSİ

Dünya İqtisadi forumunun (DİF) işləmiş olduğu “İnküziv İnkişaf İndeksi 2018” hesabatının [7] əsas qayəsi insanların maddi və sosial rifah halının, məşğulluq, sağlam həyat gözləntilərinin qiymətləndirilməsi və ölçülməsidir. DİF-in 2018-ci

ildəki hesabatında nüfuzlu indeks sayılan “İnküziv İnkişaf İndeksi”-nə görə Azərbaycan ən yaxşı inkişaf etməkdə olan ölkələr sırasında üçüncü, MDB məkanında isə birinci yerdə qərarlaşıb [10].

Azərbaycanın iqtisadi fəal əhalisi məşğul və işsiz əhalinin ümumi sayını əhatə edir. 15 və yuxarı yaşda məşğul olmayan və müəyyən dövr ərzində iş axtarmayan şəxslər iqtisadi qeyri-fəal əhaliyə aid edilir. Beynəlxalq indeksin metodologiyasına əsasən, 15-64 yaş arası iqtisadi fəal əhalinin sayına və 100 nəfərə düşən hesaba əsasən qiymətləndirmə aparılır.

Əhalinin neçə faizinin işlək olduğu və gəlir götürmək qabiliyyətinə malik olduğunu bildiren asılılıq sub-indikator indeksinə görə Azərbaycan 40.9% səviyyəsində qiymətləndirilib ki, bu da əksər inkişaf etmiş və inkişafda olan ölkələrin faiz dərəcələrindən daha azdır. Başqa sözlə ölkədə olan fəal iqtisadi əhalinin sayı iqtisadiyyatda daha çox üstünlük təşkil edir. Qeyd edək ki, Azərbaycan Litva və Macarıstandan cüzi faizlərlə müvafiq olaraq 0.17 və 0.05 faiz geri qalıb. Reytingdə Azərbaycan Latviya, Polşa, Xorvatiya, Rumıniya, Bolqarıstan, Makedoniya kimi ölkələri 0.2 – 0.5% dərəcələri ilə, qonşu Rusiyanı 0.49%, Türkiyəni 0.43%, Gürcüstanı 0.7%, İranı 0.61%, Ermənistanı 1.03% qabaqlamışdır. İnküziv indekslər üzrə aparılan təhlillər həm beynəlxalq, həm də ölkə səviyyəsində cəmiyyətin və iqtisadiyyatın inklüzivliyini bir daha təsdiqləyir.

IV. İQTİSADI İNKİŞAFIN İNKÜZİVLİK SƏVİYYƏSİNİN YÜKSƏLDİLMƏSİ PROBLEMLƏRİ

BMT 2015-ci ilin sentyabr ayında keçirilən tarixi sammitində 2030-cu ilədək Dayanıqlı İnkişaf Məqsədləri (DİM) (ing. Sustainable Development Goals) qəbul etmişdir. Hər kəsi əhatə edən və universal xarakter daşıyan bu yeni Məqsədlər fonunda, qarşıdakı on beş il ərzində ölkələr heç kəsi kənarda qoymamaq prinsipini rəhbər tutaraq, yoxsulluğun bütün formalarına son qoymaq, bərabərsizliklərə qarşı tədbirlər görmək məqsədilə bütün səylərini səfərbər edəcəklər.

Qlobal inkişaf məqsədləri ilə uzlaşan və ölkədə inklüzivlik siyasətinin əsasını təşkil edən məsələlərdən biri də cəmiyyətdə əlillərə göstərilən diqqət və yaradılan imkanlardır. Konkret hal kimi əlillərin sosial müdafiəsi haqqında Azərbaycan Respublikasının qanunu cəmiyyət həyatının iqtisadi, siyasi və sosial sahələrində iştirak etmək üçün əlillərin bütün başqa vətəndaşlarla bərabər imkanlar almasına, onların öz fərdi qabiliyyətlərinə və maraqlarına müvafiq surətdə dolğun həyat sürməsinə kömək göstərən lazımı şəraitin yaradılmasına təminat verir [11, 12, 13].

İnküzivliyin yüksəldilməsində təhlil sferası və prosesləri mühüm rolə malikdir. İnküziv təhsilin mahiyyətini ümumi təhsilin hamı üçün əlçatan olmasını nəzərdə tutan və bütün gənclərin müxtəlif ehtiyaclarına uyğunlaşdırılmasına əsaslanan inkişaf prosesi təşkil edir. İnküziv təhsil gənclərin müstəqil bir fərd olduğunu və təhsil zamanı onların hər birinin öz ehtiyacları olduğunu qəbul edən metodologiyaları inkişaf etdirməyə yönəlib. İnküziv təhsil-tədris zamanı müxtəlif

ehtiyacların ödənilməsinə yönəlmiş yanaşmaların formalaşdırılmasına çalışılır. Inklüziv təhsil istər sağlam, istərsə də əlilliyi olan gənclərin bərabər təhsil alma hüquqlarını təmin edir və bu, cəmiyyətdə sosial bərabərliyin qorunmasına, əlilliyi olan gənclərin təhsil və başqa xüsusi ehtiyaclarının ödənilməsinə şərait yaratmış olur. Azərbaycanda “İnklüziv təhsil layihəsi”nin icrasına 2005-ci ildən start verilmişdir [14]. Inklüziv təhsilin sağlamlıq imkanları məhdud uşaqlar üçün faydaları çoxdur. Xüsusi qayğıya ehtiyacı olan uşaqların daha keyfiyyətli təhsilə yiyələnməsi, cəmiyyətə daha tez adaptasiyası üçün digər yaşlıları ilə bir yerdə olması daha məqsədəuyğundur.

V. İNKLÜZİVLİK SƏVİYYƏSİNİN YÜKSƏLDİLMƏSİNDƏ İKT: PROBLEMLƏR VƏ PERSPEKTİVLƏR

Beynəlxalq təşkilatlar cəmiyyətin inklüzivlik səviyyəsinin artırılmasında ən önəmli vasitələrdən biri kimi İKT-ni qeyd edirlər. Təsədüfi deyildir ki, hazırkı yüksək texnologiyalar dövründə süni intellekt, bulud tipli məlumat bazası, əşyaların interneti, “Biq-Data” və s. texnologiyalar İKT-nin global inkişaf tendensiyalarıdır. Həm bu texnologiyaların inkişafı, həm də dördüncü sənaye inqilabı ölkələrə və hökumətlərə həyat keyfiyyətinin artırılması və insanların həyat səviyyəsinin yaxşılaşdırılmasında yeni iqtisadi imkanlar yaradır [15]. Bu sahədə qoyulan sərmayələr hər bir ölkənin davamlı inkişafında mühüm rol oynayır. Yüksək sürətli internetə çıxışı, Böyük həcmli verilənlər (Big Data), bulud tipli məlumat bazası, kiber təhlükələrə cavab verən yaxşı inkişaf etmiş İKT vasitələri bu prosesdə başlıca potensiallardır.

Azərbaycanda İKT-nin inkişafı prioritet sahələrdən biridir. Yüksək texnologiyalar davamlı və inklüziv iqtisadi inkişafın əsas hərəkətverici qüvvəsidir. Qlobal iqtisadiyyatda dəyişikliklər İKT-ni ölkədə ən sürətlə inkişaf edən sektorlardan biri etmişdir.

İKT üzrə Strateji Yol Xəritəsi İKT sektorunun inkişafının müxtəlif aspektlərini, habelə müvafiq tənzimləyici məsələləri əhatə edir [4]. Ölkə əhalisinin 79 faizi internet istifadəçisidir, onların 72 faizi genişzolaqlı internetdən istifadə edir. İlbəil evlərin internetə çıxışı artır və indi bu rəqəm 77.2 faizdir. Rəqəmsal televiziya yayımına keçid tamamlanıb. “Azerspace-1” telekommunikasiya peyki, “Azersky” yer səthinin müşahidə peyki uğurla fəaliyyət göstərir və müasir peyk xidmətlərini təmin edir. Ölkədə milli malların onlayn kataloqunu yaratmaqla yanaşı, yeni xarici bazarlara çıxışı üçün Rəqəmsal Ticarət Mərkəzi (RTM) kimi dövlət özəl tərəfdaşlıq platforması yaradılıb. Bu platformanın əsas məqsədi öz məhsullarını ixrac etmək istəyən sahibkarları, o cümlədən xırda və orta sahibkarları lisenziyalar, icazələr, sertifikatlar və ödəniş imkanları ilə təmin etməkdir. Azərbaycanın Rəqəmsal Ticarət Mərkəzi yerli və regional səviyyədə inkişaf edir. Bu mərkəz innovativ ideyaları olan gənc sahibkarlar və startaplar üçün pulsuz olacaq [5].

VI. İNKLÜZİV İQTİSADİYYATIN İNFORMASIYA TƏHLÜKƏSİZLİYİ İSTİAMƏTLƏRİ VƏ TEXNOLOGİYALARI

İKT sferasında təhlükəsizliyin və davamlılığın qorunması ölkədə inklüziv rəqəmsal inkişafa nail olmaq üçün vacib bir şərtidir. Texnologiyaların sürətli inkişafı insanlara və ölkələrə iqtisadi və sosial sahələrdə yeni imkanlar yaradır. Bununla yanaşı, həmin proses kiber hücumlar və iş yerlərinin itirilməsi kimi yeni çağırışlar və təhdidlər gətirir. Bu çətinliklərlə üzləşərkən dövlətin üzərinə böyük məsuliyyət düşür. Vəziyyət düzgün qiymətləndirilməli və vətəndaşların bu kimi təhdidlərdən qorunması üçün lazımi ölçülər götürülməlidir.

Inklüziv iqtisadiyyatın qarşısında ənənəvi iqtisadiyyatının vəzifələri ilə yanaşı yeni tələblər, məsələlər və məqsədlər qoyulmuşdur. Bunlar ölkənin bütün, xüsusilə fiziki cəhətdən qüsurlu vətəndaşlarının maddi və mənəvi rifah halının, həyat keyfiyyətinin, işləyə bilmək, cəmiyyətə inteqrasiya olunmaq imkanının yaxşılaşdırılması üçün həm ənənəvi, həm də rəqəmsal formada olan məhsullara və xidmətlə olan tələbatlarını daha dolğun və səmərəli şəkildə ödənilməsindən ibarətdir. Bu isə cəmiyyətdə rəqəmsal texnologiyalardan daha geniş istifadə, əhalinin rəqəmsal savadlılığının artırılması, insanların informasiya ilə təmin olunmaq səviyyəsinin yüksəlməsi, dövlət xidmətlərinə əlçatanlığın asanlaşması şəraitində mümkündür. Ona görə də hesab olunur ki, formalaşmaqda olan müasir informasiya və bilik iqtisadiyyatının inklüzivlik səviyyəsini ancaq ən yüksək İKT infrastrukturunu, kommunikasiya-rabitə vasitələri və kiber-fiziki sistemlərdən ibarət platformada effektiv təşkil etmək olar. Belə platforma isə təhdid və təhlükələrdən qoruna bilən yüksək inkişaf etmiş informasiya təhlükəsizliyi sistemində, etibarlı telekommunikasiya şəbəkəsinə, naqilsiz xətlərə, daimi monitoring sistemlərinə, texniki tənzimləyici strukturlara, müvafiq yüksək ixtisaslı personala, yüksək səviyyədə təşkilati, maliyyə, normativ, ekoloji, sosial problemlərin operativ həllinə imkan verən mexanizmlərə malik olmalıdır [16].

Müasir e-dövrün formalaşmaqda olan informasiya iqtisadiyyatının və onun sektorlarının inklüziv dinamik inkişafı üçün tətbiq olunan əsas qabaqcıl texnologiyalar sırasına böyük verilənlər, neyroteknologiyalar və süni intellekt, blokçeyn texnologiyaları, kvant texnologiyaları, yeni istehsal, loqistik, satış, idarəetmə texnologiyaları, sənaye interneti, robototexnika, sensor texnologiyaları, naqilsiz rabitə texnologiyaları, virtual realıq texnologiyaları, soft-komputinq texnologiyaları, krptoqrafik texnologiyalar, mürəkkəb böyük hesablama texnologiyaları, bulud-duman texnologiyaları və s. daxildir [17]. Bu cür qabaqcıl texnologiyaların tətbiqi zamanı risk və təhlükələrin azaldılması istiqamətləri daha çox: a) şəxsiyyətin, cəmiyyətin, dövlətin daxili və xarici informasiya təhlükəsizliyinin müdafiəsinə, b) vətəndaşların ləyaqətli, keyfiyyətli yaşam tərzinə, c) ölkənin dayanıqlı sosial-iqtisadi inkişafına və suverenliyinə yönləndirilmişdir. Bu kompleks istiqamətləri aşağıdakı kimi tədbirlərin yerinə yetirilməsiylə ifadə etmək olar: 1) Verilənlərin emalı mərkəzləri infrastrukturunun və aparat-proqram vasitələrinin fəaliyyətinin

təhlükəsizliyinin və texnoloji müstəqilliyinin təmini; 2) Yeni iqtisadi şəraitdə kiber-fiziki sistemlərin fəaliyyət mexanizmlərinin işlənilməsi və onların icrasının təhlükəsiz təmini; 3) Kiber-fiziki sistemlərin fəaliyyətində inam mühitinin formalaşdırılması üçün zəruri əsasların yaradılması; 4) Müxtəlif səviyyəli və təyinatlı informasiya sistemlərinin və texnologiyalarının təhlükəsizliyinin və dayanıqlılığının təmini; 5) Yeni iqtisadi şəraitdə informasiya təhlükəsizliyi üzrə beynəlxalq qarşılıqlı əlaqələrin təmini; 6) Beynəlxalq iqtisadi informasiya fəzaları ilə inteqrasiya olunan informasiya resurslarının, sistemlərinin təhlükəsizliyinin təmini və s.

Göstərilən tədbirlər yeni inklüziv informasiya təhlükəsizliyi sistemlərinin, interfeyslərinin, aparat-proqram vasitələrinin işlənilməsinə zəruri edir.

VII. İNKLÜZİV RƏQƏMSAL İQTİSADİYYAT SEKTORLARINDA İNFORMASIYA TƏHLÜKƏSİZLİYİ MƏNBƏLƏRİ VƏ BAZA TEXNOLOGİYALARI

Rəqəmsal iqtisadiyyat sektorlarında inklüziv informasiya resurslarının, sistemlərinin, məhsul və xidmətlərin informasiya təhlükəsizliyi daha çox aşağıdakı kimi risklərə, təhdid və təhlükələrə məruz qala bilər:

- rəqəmsal mühitdə insanların hüquqlarının təmini, onların identifikasiyası, onlara aid verilənlərin saxlanması, onların inamının yüksəldilməsi;
- şəxsiyyətə, biznesə dövlətə telekommunikasiya sistemlərindən və resurslarından istifadə zamanı yaranan təhlükə və təhdidlər;
- kritik informasiya infrastrukturuna xarici informasiya-texniki təsir imkanlarının artması;
- daxili və xarici kompüter cinayətkarlığı səviyyəsinin yüksəlməsi;
- aparıcı, güclü xarici dövlətlərdən İKT-nin inkişaf səviyyəsinə görə geridə qalmaq;
- İKT-nin inkişafı və təhlükəsizliyi aspektində təhsil və elmi-tədqiqat işlərinin nisbi zəifliyi.

Göstərilən bu və ya digər təhlükəyə zamanında qarşısının alınması üçün xüsusi aparat və proqram vasitələrin əldə edilməsi və ya işlənilməsi çox yaxşı olardı. Ancaq belə xüsusi texnologiyaların işlənilməsi çox çətin olduğundan və alınması böyük maliyyə vəsaitləri tələb etdiyindən heç olmazsa bütün iqtisadi sahələrdə istifadə oluna bilən standart, baza, universal texnologiyaların tətbiq olunması məqsədə uyğun olardı [16, 17]. Belə inklüziv informasiya texnologiyalarını aşağıdakı kimi qruplaşdırmaq təklif edilir:

- inklüziv kiber-fiziki sistemlərin komplekslərin aparat-texniki vasitələrinin yaradılması texnologiyaları;
- inklüziv kiber-bioloji insan-maşın sistemlərin yaradılması texnologiyaları;
- pilotsuz sistemlər və robototexniki texnologiyalar;
- sənaye İnterneti və Əşyaların İnterneti texnologiyaları;
- resursların səmərəli istifadəsi və növbələrin idarə olunması texnologiyaları;
- neyroşəbəkə, genetik və digər koqnitiv texnologiyalar;
- duman-bulud hesablamaları texnologiyaları;

- böyük verilənlərin yığılı, emalı və saxlanması texnologiyaları;
- virtual mühit və reallıq texnologiyaları;
- blokçeyn və digər maliyyə texnologiyaları;
- kiberfəzaya nəzarət, kompüter hücumlarının qarşısının əvvəldən alınmasına xidmət edən koqnitiv texnologiyalar;
- Big-data əsaslı proseslərin informasiya təhlükəsizliyi təminatının intellektual texnologiyaları;
- proqram-konfigurasiyalı şəbəkə və şəbəkə funksiyalarının virtuallaşması texnologiyaları;
- inklüziv sənaye və əşyaların internetinin təhlükəsizliyi texnologiyaları;
- inklüziv təhlükəsiz bulud-duman və mobil texnologiyalar.

NƏTİCƏ

İnklüziv ölkə iqtisadiyyatının informasiya resurslarının, texnologiyalarının, sistemlərinin təhlükəsizliyinə yalnız sistemli yanaşma əsasında nail olmaq olar. Burada həm qanunvericilik aspektində inzibati mexanizmlərdən, həm təşkilati effektiv tədbirlərdən, həm də müvafiq müasir proqram, aparat-texniki vasitə və texnologiyalardan kompleks şəkildə istifadə olunmalıdır.

ƏDƏBİYYAT

- [1] R. M. Alguliyev, A. G. Aliyev, V. A. Abbasova. The study of formation characteristics and development tendencies of international information and knowledge economy. J. Review of knowledge economy. 2017, vol.4, No.1, pp.7-14.
- [2] Ə. Q. Əliyev. İnformasiya iqtisadiyyatının qiymətləndirilməsinin metodoloji xüsusiyyətləri. Az.Dövlət İqtisadi Universiteti. Elmi Xəbərləri. Vol.5, №5, iyul-sentyabr, 2017, səh.74-91
- [3] “İnformasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya”. 02.04.2014-cü il, <http://www.president.az>
- [4] “Telekommunikasiya və informasiya texnologiyalarının inkişafına dair Strateji Yol Xəritəsi”, Bakı, 6 dekabr 2016-cı il. <http://mincom.gov.az>
- [5] https://azertag.az/xeber/Elmar_Memmedyarov_Azərbaycanda_IKT_nin_inkişafı_hökumetin_gündeliyinde_prioritet_sahelerden_biridir-1196094. 19.09.2018-ci il
- [6] Pouw Nicky, Gupta Joyeeta. Inclusive development: a multi-disciplinary approach. Current Opinion In Environmental Sustainability. 2017. Volume: 24, pp.104-108
- [7] The Inclusive Development Index 2018. World economic forum, 2018. <https://www.weforum.org/events/world-economic-forum-annual-meeting-2018/?tab=LiveBlogs&stream=day-before-davos&stream-item=inclusive-development-index-2018>
- [8] Pouw, Nicky R. M.; de Bruijne, Ad. Strategic Governance for Inclusive Development Introduction. European Journal Of Development Research. 2015. Volume: 27. Issue: 4. Pages: 481-487
- [9] Kumar Pushpam. Innovative tools and new metrics for inclusive green economy. Current Opinion In Environmental Sustainability. 2017. Volume: 24, pp. 47-51
- [10] https://azertag.az/xeber/Azərbaycanın_Inklüziv_Inkişaf_Indexi_2018_h_esabatında_irelilemesi_ugurlu_islahatların_neticesidir-1130930. Bakı, 24 yanvar, AZƏRTAC.
- [11] <https://www.un.org/sustainabledevelopment/ru/>
- [12] Əlillərin sosial müdafiəsi haqqında Azərbaycan respublikasının qanunu. Bakı şəhəri, 25 avqust 1992-ci il. http://www.e-qanun.az/alpdata/framework/data/7/f_7652.htm

- [13] Əlilliyi olan şəxslərin hüquqları haqqında Azərbaycan Respublikasının Qanunu. Bakı şəhəri, 31 may 2018-ci il. <https://president.az/articles/29521>
- [14] 2018–2024-cü illərdə Azərbaycanda sağlamlıq imkanları məhdud şəxslər üçün inklüziv təhsilin inkişafı üzrə dövlət proqramı. baku.edu.gov.az/upload/file/inkluziv-tehsil-dovlet-proqrami--2018-2024.pdf
- [15] Oktay Mamedov. Economy of inclusive civilization. Terra economicus. 2017. Volume:15. Issue:3, pp.6-18
- [16] А. Г. Светлаков, И. М. Глотина. Влияние информационного пространства на экономическую безопасность региона // Экономика региона. - 2018. - Т. 14, вып. 2, с. 474-484
- [17] А. С. Минзов, А. Ю. Невский и т.д. Информационная безопасность в цифровой экономике. Ж., ИТНОУ, 2018, №3, стр.52-59

INFORMATION AND COMMUNICATION TECHNOLOGIES IN INCREASING THE LEVEL OF ECONOMIC DEVELOPMENT INCLUSIVE AND ITS SECURITY ISSUES

Alovsat G. Aliyev

Institute of Information Technology of ANAS, Baku,
Azerbaijan

alovsat_qaraca@mail.ru

Abstract – The article focuses on ICT tools and their security problems in raising the level of inclusiveness of economic development. The new economic trends are analyzed. The importance of inclusive development in society and economy has been commented. Regional-sectoral and international assessment of the level of inclusive development in society and economy has been studied. An international assessment of inclusive development has been reviewed in Azerbaijan and the level of inclusiveness of economic development has been determined. In this paper some recommendations have been made on ICT and its security to improve the inclusiveness rate.

Keywords – inclusion of economic development, inclusive level and index, Inclusiveness Indicators, inclusiveness assessment, inclusive ICT, ICT security

Bulud əsaslı e-kitabxanalarda informasiya təhlükəsizliyinin təmin edilməsi

Dilbər Əlizadə

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

dilberilhamgizi@gmail.com

Xülasə — Virtual aləmdə fəaliyyət göstərən elektron kitabxanalar müxtəlif təhlükəli risk və təhdidlərlə üzləşirlər. Bunların aradan qaldırılması qarşıda duran ən vacib məsələlərdəndir. Məqalədə bulud əsaslı elektron kitabxanaların təhlükəsizliyinin təmin olunması məsələləri araşdırılır.

Açar sözlər — *bulud texnologiyası; elektron kitabxana; təhlükəsizlik; bulud əsaslı e-kitabxana.*

I. GİRİŞ

İnformasiya texnologiyalarının günbəgün daha dinamik sürətlə inkişafı müxtəlif sahələrdə yeni imkan və perspektivlərə yol açır. E-kitabxanalar da bu prosesdən kənarda qalmır və yeni texnologiyaların tətbiqi elektron kitabxanalara yeni məzmun qatır, onu təkmilləşdirir və informasiya cəmiyyətinin formalaşmasında əsas və aparıcı informasiya mənbəyi kimi çıxış etməsinə imkan yaradır. Xüsusilə, e-kitabxanalara bulud texnologiyalarının tətbiqi bu sahədə yeni çığır açmışdır.

E-kitabxanalarda bulud texnologiyalarından istifadə onun təhlükəsizliyinin təmin olunması məsələlərini meydana çıxarır.

Google, Amazon, Microsoft və VMware kimi şirkətlər identifikasiya, giriş nəzarəti, şifrələmə, tamliq, məlumat izolyasiyası və digər məsələləri təmin etmək üçün bulud təhlükəsizliyi texnologiyası təklif edir. Cloud Security Alliance bəzi bulud təhlükəsizliyi məsələlərini qarşıya qoyur. Lakin tədqiqatları kitabxanalarda bulud texnologiyalarının təhlükəsizliyində cəmləşdirmək limitlidir. Kitabxana buludlarının təhlükəsizliyinin effektivliyini təmin etmək üçün əsas IT təhlükəsizlik sistemi texnologiyalarından başqa, identifikasiya, şifrələmə və digər təhlükəsizlik tədbirlərinin təmin edilməsində texniki vasitələrə və kitabxana tətbiqləri üçün təhlükəsizlik sisteminin qurulmasına ehtiyac var [1].

II. BULUD TEXNOLOGİYALARININ TƏYİNATI

Rahat interfeysə malik olan bulud texnologiyaları son dövrlərin ən aktual məsələlərindən birinə çevrilmişdir. Kitabxanalarda tətbiqini nəzərə almaqla bu texnologiyaların əsas konseptual məsələlərini nəzərdən keçirək.

BT kompüter resurslarından səmərəli istifadə etmək imkanı verir. Burada məlumatların emalı və yadda saxlanması prosesi xidmət növü sayılır. BT konsepsiyası 1960-cı ildə irəli sürülmüşdür. Massaçusets Texnologiya İnstitutunun professoru C.Makkartinin ideyası olan bu texnologiya

hesablama resurslarına komunal xidmət kimi baxılmasını özündə əks etdirir [2].

BT istifadəçilərə müxtəlif xidmətlər təklif edir. Onlardan ən çox istifadə olunanlar aşağıdakılardır:

İnfrastruktur xidmət kimi (IaaS – Infrastructure as a service). Bu xidmət növündə istifadəçilər hesablamaresursları və yaddaş sistemini icarəyə götürmə imkanına malikdirlər. Burada servisin istifadəçiyə hansı üsullarla təqdim olunması, fiziki resursların harada yerləşməsi, neçə serverin və prosessorun işlək vəziyyətdə olması istifadəçi üçün əhəmiyyət kəsb etmir. IaaS xidmətinə Amazon S3 (Simple Storage Service), Amazon Elastic Computer Cloud (EC2), IBM Blue Cloud və s. misal göstərmək olar [3].

Platforma xidmət kimi (PaaS – Platform as a Service).

Bu xidmət növündə istifadəçi bulud strukturunu idarə etmədən quraşdırdığı funksional proqrama nəzarət edir. PaaS xidmətində əməliyyatlar vahid inteqrasiya olunmuş mühitdə təmin edildiyi üçün müxtəlif mərhələlərdə mühitlərin dəstəklənməsinə sərf edilən xərclər aradan qaldırılır. Bu xidmət istifadəçilərə virtual serverlərdə yerləşən əməliyyat sistemlərindən və xüsusi proqram əlavələrindən (Apache, M SQL və s.) istifadə edilməsinə imkan verir. PaaS servisinə misal olaraq, IBM IT Factory, Google App Engine, Force.com xidmətlərini göstərə bilərik [4].

Proqram təminatı kimi (SaaS – Software-as-a-service).

Bu xidmət vasitəsilə istifadəçilər sadəcə internet brauzeri ilə proqram təminatını əldə edə bilərlər. Bu zaman kompüterdə heç bir lokal quraşdırmaya ehtiyac yoxdur. Proqram əlavələri SaaS xidməti verən təchizatçının serverində işləyir və istifadəçiyə hesablamaların nəticəsini göndərir. Beləliklə, istifadəçi proqram təminatını almadan lazımı məqamda ondan məsələnin həllində istifadə edir və istifadəyə uyğun pul ödəyir. Bu səviyyədə istifadə olunan proqramlara misal olaraq, Microsoft “Software Services” (e-mail, video konfrans), Google Apps, Google Docs və s. göstərmək olar [5].

III. KİTABXANALARDA BULUD TEXNOLOGİYALARINDAN İSTİFADƏ

Bu gün ən aktual məsələlərdən biri də BT istifadə etməklə müasir e-kitabxanaların qurulmasıdır. Bulud əsaslı kitabxanaların yaradılması e-kitabxanaların inkişafında müsbət mənada dönüş yaratmışdır. Belə ki, bu texnologiyanın

köməyi ilə kitabxana resursları və kitabxana istifadəçilərinin məlumatları müxtəlif buludlarda saxlanılır və emal edilir.

Bu model (Şəkil 1) həm e-kitabxanaların resurslarının buludda toplanmasını, həm də hər bir istifadəçi üçün buludların yaradılmasını özündə əks etdirir. İstifadəçi buludlarının yaradılması nəticəsində kitabxanalarda resursların istifadəsi barədə informasiya bu buludlarda toplanır və nəticədə informasiyaların analiz olunması və emalı üçün çoxlu imkanlar yaranır [6].

Şəkildən göründüyü kimi bulud texnologiyasından istifadə edərək hər bir istifadəçi üçün kiçik buludlar ($B_1, \dots, B_n$) yaradılır. Yaradılan buludlar idarəetmə serveri vasitəsilə idarə olunur. Kitabxana istifadəçisi axtarış apardıqda müraciət verilənlərin emalı mərkəzində analiz olunur. Lazım olan məlumatlar buludlarda varsa oradan istifadəçiyə göndərilir. Beləliklə də, istifadəçi sürətli məlumat əldə etmək imkanına malik olur.

Buludlarda toplanan informasiya əsasında kitabxanalarda resursların istifadə olunmasının, onlara olunan müraciətlərin analiz olunması kitabxana resursları arasında sosial şəbəkələrin aşkarlanmasına gətirib çıxarır. Resursların istifadəçilərinin müxtəlif kateqoriyalara görə - yaş, gender, yaşayış yeri, ixtisası və s. analiz olunması vasitəsilə resursları təsnif etmək, klasterləşdirmək, onlar arasındakı münasibətlərin çəkirlərini hesablamaq mümkündür. Bu cür analiz nəticəsində alınan informasiya bir sıra sahələrdə, məsələn, kitabxananın işinin idarə olunmasında istifadə oluna bilər [7].

Şəkil 1. Bulud əsaslı e-kitabxananın konseptual modeli

Bu gün hər bir kitabxana öz resurslarını və xidmətlərini daha effektiv idarə etmək və şəbəkə vasitəsilə əlyətərliyi təmin etmək üçün e-kitabxana qurmaq istəyir. Bazarda bulud texnologiyaları əsasında qurulmuş elektron kitabxana proqram təminatları çoxdur. Texniki işçi qüvvəsinin çatışmazlığı səbəbindən bir çox kitabxanalar veb sahifələrini üçüncü tərəf provayderlər tərəfindən idarə olunmasına üstünlük verirlər.

Web site hosting bir çox kitabxana istifadəçilərinə eyni zamanda istənilən coğrafi məkandan əlyətərliyi təmin edir.

OCLC (Open Computer Library Center) World Cat kitabxana məlumatlarının BT infrastrukturundan istifadə etməklə yayılmasında vacib rol oynayır. OCLC World Cat idarə sistemi kitabxana istifadəçilərinin resursları və xidmətlərini bulud əsaslı mühitlərdə yaymaq üçün əməkdaşlıq formasını inkişaf etdirməyə kömək edir.

Kitabxanalar müxtəlif növ elektron sənədləri yerli lokal serverdə saxlayır və əlyətərliyi təmin edir. Bulud saxlama servisləri coğrafi məkandan asılı olmayaraq sənədləri pulsuz buludda saxlamaq imkanı təklif edir. Bulud saxlama tələb olunan məlumatın əlyətərliyini təmin etməyə məsuliyyət daşıyır və buludda saxlanılan məlumatların eyni anda birdən çox istifadəçiyə əlyətərliyi üçün imkan yaranır [8].

IV. BULUD ƏSASLI E-KİTABXANALARDA İNFORMASIYA TƏHLÜKƏSİZLİYİNİN TƏMİN OLUNMASI

Əvvəlcə kitabxana resurslarının bulud modelinin izahına ehtiyac var. Müxtəlif verilənlər bazası kolleksiyaları və şəbəkə resursları BT modelinə uyğunlaşdırılaraq onların xidmətini təmin edir və bu resurslar və xidmət buludda yerləşdirilir. E-kitabxananın fiziki avadanlığa ehtiyacı yoxdur. O sadəcə avadanlığa xərclənən pula qənaət edir. İstənilən vaxt istifadəçilər kitabxana servisi buluduna daxil ola və ondan istifadə edə bilərlər. Kitabxanaçılar məlumatları cloud storage-də arxivləşdirir, oxucular elektron jurnalları, dissertasiya, kitablar və digər resursları əldə etmək üçün kitabxana buluduna daxil ola bilərlər. Məsləhətçi kitabxanaçı istənilən vaxt buluda daxil olaraq öz xidmətlərini təmin edə bilər. Kitabın bütün həyatı bulud idarə olunma sistemində öz əksini tapır. Bura daxildir: kitabın nəşriyyatı, yayılması, saxlanması, daşınması, kataloqlaşdırılması, arxivləşdirilməsi, bərpası, götürülməsi, qaytarılması və bu proseslərin ləğvi. Buna görə də buludu dəstəkləyən servislər cloudda əks əlaqəni (feedback) təmin etməlidirlər. İdentifikasiya, təhlükəsizlik səviyyəsi, kommunikasiya şifrələməsi, məlumat şifrələməsi, şəxsi məlumatların qorunması, giriş nəzarət kimi müxtəlif kitabxana buludu təhlükəsizliyi məsələlərini öyrənməyə ehtiyac var [1].

Təhlükəsizlik – texnologiyalardan istifadə etməklə informasiyanın qorunmasıdır. Bulud saxlama özünəməxsus çatışmazlığı olan xidmət olsa da onun bir sıra üstünlükləri var. Bulud modeli istifadəçiləri fiziki təhlükəsizlik üzərində nəzarəti itirirlər. Buludu digər istifadəçilərlə paylaşmaq təhlükəsizlik üçün bir sıra risklər yaradır. Ümumilikdə təhlükəsizlik üç aspekti əhatə edir: konfidensiallıq, tamlıq və əlyətərlik. Bu aspektlər maksimum qorunmanı təmin etmək üçün təhlükəsizlik tədbirləri sırasında ən vacibləridir.

Konfidensiallıq dedikdə, məlumat və informasiyanın icazəsiz açıqlamadan qoruma nəzərdə tutulur.

Tamlıq məlumat və informasiyanın kənar şəxslər tərəfindən modifikasiya olunmasından qorunmadır.

Ölçetərlik istənilən vaxt qeydiyyatdan keçmiş istifadəçilərin məlumat və informasiyadan istifadəsidir [9].

Bulud istifadəçiləri daxili və xarici təhlükəsizlik təhdidləri ilə üzləşirlər. Bir çox təhlükəsizlik problemləri böyük Data mərkəzlərdə olduğu kimi buludu xaricdən gələn təhdidlərdən qorumaq məsələlərini əhatə edir. Buludda məsuliyyət bulud istifadəçiləri, bulud satıcıları və hər hansı üçüncü tərəf daxil olmaqla bir sıra tərəflər arasında bölünür və istifadəçilər təhlükəsizlik proqramları və konfigurasiyalarına etibar edirlər. Bulud istifadəçisi tətbiq səviyyəsində təhlükəsizliyin təmin olunmasında, bulud provayderi isə fiziki təhlükəsizliyin qorunmasında məsuliyyət daşıyır. Orta səviyyədə təhlükəsizliyin təmini istifadəçi və operator arasında paylanılır, aşağı səviyyədə isə bu yalnız istifadəçinin məsuliyyətinə aiddir.

Məlumatların təhlükəsizliyini təmin etməklə bulud xidməti provayderləri məlumatların tamlığını təmin etmək üçün müəyyən mexanizmlər həyata keçirməlidirlər. Bulud provayderi buludda xüsusi verilənlərin yerləşdirildiyini, onun mənşəyi və tamlıq mexanizmləri haqqında istifadəçiyə xəbərdarlıq etməlidir [10].

Provayderləri buludu oğurluq və xidməti əngəlləmə hücumlarından qorunmalıdırlar. Hazırda buludda istifadə olunan təhlükəsizlik mexanizmi virtualizasiyadır. Bu güclü müdafiədir və bir istifadəçinin digərinə və ya cloud infrastrukturunda olan hücumların qarşısını alır. Buna baxmayaraq bütün resurslar virtualizasiya olunmur və ya bütün virtualizasiya mühitləri xətasız deyil. Virtualizasiya proqramı xətalara səbə olur və belə olduqda virtualizasiya olunmuş kodlar öz funksiyasını itirir. Səhv şəbəkə virtualizasiyası icazə verir ki, istifadəçi kodları digər istifadəçilərin resurslarına və ya provayder infrastrukturunun həssas hissələrinə keçid edə bilsin. Bu çətinliklər müxtəlif tətbiqlərin bir-birindən qorunmağa ehtiyacı olan böyük Data mərkəzlərin idarə edilməsində də özünü göstərir. Ümumiyyətlə, istənilən böyük internet xidməti heç bir halda təhlükəsizlik məsələlərini güzəştə getməməlidir [11].

NƏTİCƏ

Məqalədə bulud əsaslı e-kitabxanaların təhlükəsizliyinin təmin olunması məsələləri araşdırılmış və analiz edilmişdir. Bulud əsaslı e-kitabxanalar çoxlu sayda təhlükəsizlik risk və təhdidləri ilə qarşılaşa bilər. Bura müxtəlif virusları, troyanları və başqa zərərli proqramları aid etmək olar. Bunlar kitabxana resurs və xidmətlərini məhv edə və istifadəçilərin şəxsi məlumatlarının konfidensiallığının qorunmasına xələl gətirə bilər. Ona görə də bulud əsaslı e-kitabxanalarda təhlükəsizliyin təmini ən vacib istiqamətlərdən biridir və bunu reallaşdırmaq üçün müasir bulud texnologiyalarının təhlükəsizlik sistemlərindən istifadə etmək lazımdır.

ƏDƏBİYYAT

- [1] Q.Meng, C.Gong, “Research of cloud computing security in digital library”, 6th International Conference on Information Management, Innovation and Industrial Engineering, pp. 41-44, 2013.

- [2] R.Əliquliyev, R. Ələkbərov, “Kompüter şəbəkələri əsasında paylanmış hesablama sistemlərinin yaradılması texnologiyaları” İnformasiya texnologiyaları problemləri, №2, səh. 3-14, 2010.
- [3] R.Ələkbərov, M.Həşimov, O.Ələkbərov, Elektron kitabxana mühitində bulud texnologiyalarının tətbiqi, “E-kitabxanaların formalaşması problemləri” Respublika elmi-praktiki konfransı, 2016, s.64-66
- [4] R.Ələkbərov, M.Həşimov. Bulud texnologiyaları: xidmətlər, problemlər və tətbiq sahələri, İnformasiya texnologiyaları problemləri, 2016, № 1. s. 3-10.
- [5] R.Aliquliyev, R. Alakbarov, E. Mammadov, M. Hashimov. The perspectives of cloud technology implementation in digital library //SYLWAN, 2015, 159(3), pp.97-108.
- [6] M.G. Jaatun, G. Zhao, and C. Rong. “Cloud Computing: An Overview” CloudCom 2009, LNCS 5931, pp. 626-631, 2009.
- [7] R. Əliquliyev, N. İsmayılova, “Gələcək nəsillər üçün elektron kitabxanaların formalaşması perspektivləri”, E-kitabxanaların formalaşması problemləri respublika elmi-praktiki konfransı, səh. 8-12, 2016.
- [8] K. Lal Sharma. “Cloud computing impact and its applications on libraries”, International Journal of Humanities and Social Science Research, vol. 2, June 2016, pp. 1-4.
- [9] J. Vyas, P. Modi. “Providing Confidentiality and Integrity on Data Stored in Cloud Storage by Hash and Meta-data Approach”, International Journal of Advance Research in Engineering, Science & Technology, Vol. 4, Issue 5, pp. 38-50, 2017.
- [10] R.Ələkbərov, O.Ələkbərov. Mobil hesablama buludları: mövcud vəziyyəti, inkişaf mərhələləri, problemləri və həlli yolları. – Bakı: “İnformasiya Texnologiyaları İnstitutu”, 2018. -194 səh.
- [11] M. Armbrust, A. Fox, R. Griffith. “A View of Cloud Computing”, Communications of the ACM, vol. 53, No 4, pp. 50-58, 2010.

INFORMATION SECURITY ENSURING IN CLOUD-BASED E-LIBRARIES

Dilber Alizadeh

Institute of Information Technology of ANAS,

Baku, Azerbaijan

dilberilhamgizi@gmail.com

Abstract – E-libraries operating in the virtual environment are facing a variety of hazardous risks and threats. Eliminating them is one of the most important challenges. The article examines the provision of security in cloud-based e-libraries.

Keywords – cloud technology; electronic library; security; cloud-based e-library.

Zaman sıralarında anomaliyaların aşkarlanması metodlarının analizi

Afət Mikayılova

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

Xülasə— Bu məqalədə şəbəkə trafikinin müasir dövrdə aktuallığı analiz edilmişdir. Şəbəkə trafikinin yaratdığı və son dövrlərdə rast gəlinən problemləri ilə bağlı tədqiqat aparılmışdır. Zaman sıralarında mövcud olan anomaliyaların aşkarlanması üçün təklif edilmiş mövcud metodların analizi aparılmışdır. Metodların məqsədi və problemləri haqqında məlumatlar qeyd edilmişdir.

Açar sözlər— Şəbəkə trafikinin analizi, zaman sıraları, anomaliya, oxşarlıq əsaslı metod, pəncərə əsaslı metod, proqnozlaşdırma əsaslı metod, gizli markov modeli

I. ŞƏBƏKƏ TRAFİKİNİN ANALİZİ

Şəbəkə trafiki monitorinqi üçün şəbəkə trafiki analizi hal-hazırda daha da vacib məsələyə çevrilmişdir. Ötən illərdə administratorlar yalnız az sayda şəbəkə qurğusunun monitorinqini aparırdılar. Şəbəkənin genişliyi yalnız az və ya 100 Mbits ola bilər. Hal-hazırda administratorlar daha yüksək sürətli kabel şəbəkəsi (saniyədə 1 Gbit / s-dən çox) və Asinxron Transfer Rejimi (Asinxron Transfer Mode, ATM) şəbəkələri və simsiz şəbəkələr kimi müxtəlif şəbəkələrlə məşğul olmalıdırlar. Şəbəkəni idarə etmək, çatışmazlığını aradan qaldırmaq, təhlükəsizliyini təmin etmək və problemlərini sürətli həll etmək üçün əlavə şəbəkə trafikinin analizi tələb olunur. Şəbəkə trafikinin analizi son dövrlərdə bir sıra çətinliklər yaradır. Şəbəkə müxtəlif səviyyələrdə təhlil edilir. Bu səviyyələr təhlükəsizlik, paket, kanal və şəbəkə səviyyəsinə aid edilir. Trafik təhlili üçün tədqiqatçılar müxtəlif üsullardan istifadə edirlər. Şəbəkə trafikinin analizi əvvəlcədən işləmə və şəbəkə məlumatlarından nümunələri aşkar etmək üçün faktiki analiz və müşahidələrdən istifadə edilir. Şəbəkə trafiki analizinin üç əsas mərhələsi ilkin proseslər üsulu, analiz (bu mərhələdə Data mining (DM) üsulundan istifadə edilir) və qiymətləndirmədən ibarətdir [4]. İlkin proseslər üsulu şəbəkə trafikini manipulyasiya etmək üçün mühüm mərhələdir və real məlumatları başa düşülən bir formaya çevirir. DM biliklərinin aşkarlanması üçün istifadə olunur və şəbəkə trafiki analizində mühüm rol oynayır.

Şəbəkə trafikinin proqnozlaşdırılması əhəmiyyətli bir məsələdir. Şəbəkə trafikini proqnozlaşdırılması—şəbəkənin monitorinqi, şəbəkə təhlükəsizliyi, şəbəkə trafikinin qarşısının alınması və şəbəkələrin sürətini artırılması üçün mühüm məsələlərdən biridir [7].

II. MÖVCUD METODLARIN ANALİZİ

Zaman sıralarında anomal halların aşkarlanması üçün tədqiqatçılar bir çox metodlar təklif etmişdir. Aşağıdakı üsullar tədqiq edilmişdir:

- Oxşarlıq əsaslı metod
- Pəncərə əsaslı metod
- Proqnozlaşdırma əsaslı metod
- Gizli Markov Modeli

Oxşarlıq əsaslı metodla test zaman seriyasının anomaliyaların dərəcəsini hesablamaq üçün müvafiq məsafə və ya oxşarlıq əlaqəsindən istifadə edərək, test və təlim zaman sıralarının arasında bu uyğunluqdan istifadə olunur [2]. Zaman sırasındakı anomaliyalar digər anomaliyalardan fərqli olur və bu fərq yaxınlıq ölçüsü (proximity measure) kimi istifadə edilə bilər. Beləliklə, Oxşarlıq əsaslı metod zaman sıralarının hər hissəsi üçün yaxınlığın ölçüsünü müəyyən etmək üçün istifadə edilir [5]. Bu üsulun əsas məqsədi yaxın qonşuları qiymətləndirməkdir, davamlı vaxt seriyası üçün ən yaxın qonşu (K-nearest neighbor for continuous, KNNC) üsulu adlanır və yaxınlığın ölçüsünü ifadə edir. KNNC test zaman sırasındakı anomaliya hesabını təyin edir və təlim verilənlər bazasında ən yaxın qonşusuna olan məsafəyə bərabər olur. Metodun əsas çatışmazlığı odur ki, bütün zaman seriyasının anomal olub olmadığını müəyyən edə bilər, lakin anomal sonluğu dəqiq tapa bilmir. Anomaliyaya səbəb olan zaman seriyasında dəqiq bölgəni müəyyən etmək üçün zaman seriyasını emal etmək lazımdır. Beləliklə, bu üsulun icrası çox vaxt seçilməsi asan olmayan yaxınlıq ölçüsündən çox asılıdır.

Pəncərə əsaslı metod ilə anomaliyanı aşkar etmək üçün verilən zaman seriyasını sabit ölçülü pəncərələrə bölür, bir və ya daha çox pəncərədə anomaliya səbəbini müəyyən etmək üçün istifadə olunur. Bütün zaman sıraları kiçik nəticələrə bölündükdən sonra, biz anomaliyanın olub-olmadığını asanlıqla müəyyən edə bilərik. Bu üsul test zaman sırası aralığından sabit uzunluqlu pəncərələri çıxarır və hər bir pəncərəyə anomaliya ölçüsü təyin edir [1]. Sonra ilkin pəncərə hesabları, test zaman seriyası üçün anomaliya hesabını əldə etmək üçün toplanır. Bir pəncərə hesabının təyin edilməsi və hesabların birləşməsi prosesləri müxtəlif yollarla edilə bilər [3]. Pəncərə əsaslı üsulun əsas çatışmazlığı pəncərənin ölçüsünün diqqətlə seçilməsidir ki, o, anomaliyi açıq şəkildə

əldə edə bilsin. Pəncənin optimal ölçüsü anormal zaman sırasındakı anormal bölgənin uzunluğundan asılıdır. Pəncərə əsaslı texnikanın digər çatışmazlığı hesablamalara görə bahalı olmasıdır.

Proqnozlaşdırma əsaslı metod proqnozlaşdırıcı modellərdən istifadə edərək anomaliyanın aşkarlanması üçün araşdırılmışdır. Bu üsul, statistik proseslərdə normal zaman sıralarını müəyyənləşdirmək üçün yaradılmışdır və əgər prosesdə hər hansı anomaliya baş verərsə bu metod işləməyəcəkdir [2]. Beləliklə, əsas məsələ bundan ibarətdir ki, normal zaman sıralarının təlim verilənlər bazasındakı proseslərin parametrlərini öyrənmək və daha sonra öyrənilmiş prosesdən test zaman sıralarının yaranma ehtimalını qiymətləndirməkdir. Bütün proqnozlaşdırmaya əsaslanan metodlar sabit uzunluqlu məlumatlardan istifadə edir. Eyni zaman sırasında, bəzən daha kiçik bir məlumatı proqnozlaşdırır, lakin digər vaxtlarda daha uzun bir məlumata ehtiyacı olur. Beləliklə, dinamik uzunluqlu məlumatdan o halda istifadə etmək olar ki, əgər bu üsul hər hansı bir müşahidədə m uzunluğunda hesabatların verildiyi prosesləri yüksək təhlükəsizliyə görə proqnozlaşdırıla bilməyəcəyi təqdirdə, müşahidənin daha yüksək etibarlılığını proqnozlaşdırmaq üçün hesabatın uzunluğunu artır və ya azalda bilsin. Proqnozlaşdırma əsaslı üsullar hər bir müşahidə üçün anomaliya ölçüsünü hesablayır [4]. Beləliklə, onlar hər cür anomaliyaları əhatə edə bilirlər: zaman seriyasındakı anomal müşahidələri, zaman seriyasındakı anomal ardıcılıqları, zaman sırasındakı ümumi anomaliyaları və s.

Gizli Markov əsaslı model (HMM) müşahidə edilə bilən parametrlərdən istifadə edərək bir sistemin xarakterizə etdiyi güclü sonlu üsuldur [6]. Bu üsul ardıcıl modelləşdirmə və ardıcıl anomaliyanın aşkarlanması üçün geniş istifadə olunur. Həmçinin zaman seriyasındakı anomaliyanın aşkarlanmasına tətbiq edilir [8]. Gizli Markov əsaslı model proseslərdə, müəyyən bir zaman seriyası $O=O_1 \dots O_n$ kimi göstərilə bilər. $Q=Q_1 \dots Q_n$ bir əsas (gizli) zaman seriyaları isə dolayı yolla müşahidə olunur. Əslində, real zaman seriyasını meydana gətirən proseslər bu cür müşahidə olunmaya bilər, baxmayaraq ki, gizli zaman sıralarını yaradan proses gizli Markov əsaslı üsuldur. Beləliklə, normal zaman sıraları HMM istifadə edərək modelləşdirilə bilər, anomal zaman sıraları isə qeyri-mümkündür. HMM əsaslı üsulun əsas çatışmazlığı ondan ibarətdir ki, gizli Markov əsaslı model mövcud gizlin proseslərdə baş verir və normal zaman sıraları yaradır. Gizli Markov əsaslı üsulun olmadığı təqdirdə, bu üsullar anomaliyaları aşkar edə bilmir. HMM üsulu, zaman sırası üçün markov modelini qurur [8]. Beləliklə, hər növ anomaliyaların aşkarlanmasına kömək edən zaman sıralarındakı hər bir müşahidə üçün ehtimal olunan müddətdə anomal prosesləri qiymətləndirir.

Beləliklə, biz yuxarıda qeyd etdiyimiz metodların məqsədini ümumiləşdirərək aşağıdakı cədvəldə göstərə bilərik:

CƏDVƏL 1.

Sıra	İstinad	Metod	Məqsəd
1.	[2]	Oxşarlıq əsaslı metod	Zaman sıralarının hər hissəsi üçün yaxınlığın ölçüsünü müəyyən etmək
2.	[3]	Pəncərə əsaslı metod	Bütün zaman sıraları kiçik pəncərələrə bölündükdən sonra, anomaliyanın olub-olmadığını asanlıqla müəyyən etmək
3.	[4]	Proqnozlaşdırma əsaslı metod	Proqnozlaşdırıcı modellərdən istifadə edərək anomaliyanı aşkarlamaq
4.	[8]	Gizli Markov metodu	Müşahidə edilə bilən parametrlərdən istifadə edərək zaman seriyasındakı anomaliyanı aşkarlamaq

ƏDƏBİYYAT

- [1] V. Chandola, A. Banerjee, and V. Kumar. “Anomaly detection: A survey,” ACM Computing Surveys (CSUR), 2009, vol. 41, no. 3, pp. 1-72.
- [2] B. Pincombe, “Anomaly detection in time series of graphs using ARMA processes,” Asor Bulletin, 2005, vol. 24, no. 4, pp. 2-10.
- [3] V. Chandola, D. Cheboli, and V. Kumar, “Detecting anomalies in a time series database,” Technical Report 09-004, 2009, pp. 1-12.
- [4] M. Joshi, T.H. Hadi, “A Review of Network Traffic Analysis and Prediction Techniques,” 2015,” arXiv:1507.05722 [cs.NI], p. 23.
- [5] T. Lotze, G. Shmueli, S. Murphy, and H. Burkom, “A wavelet-based anomaly detector for early detection of disease outbreaks,” Proceedings of the 23rd International Conference on Machine Learning, 2006, pp. 1-6.
- [6] V. Jecheva, “About some applications of hidden markov model in intrusion detection systems,” In International Conference on Computer Systems and Technologies (CompSysTech), 2006, pp. 1-6.
- [7] Y. Yu, M. Song, Z. Ren, I. Song, “Network Traffic Analysis and Prediction Based on APM,” Proc. of the IEEE 6th International Conference on Pervasive Computing and Applications, pp. 275-280.
- [8] Z. Liu, J.X. Yu, L. Chen, and D. Wu, “Detection of shape anomalies: A probabilistic approach using hidden markov models,” Proc. of the IEEE 24th International Conference on Data Engineering, 2008, pp. 1325-1327.

ANALYSIS OF METHODS FOR ANOMALY DETECTION IN TIME SERIES

Afet Mikayilova

Institute of Information Technology , Baku, Azerbaijan

afet_mikayilova@mail.ru

Abstract –This article was analyzed the relevance of network traffic in modern times. It has been investigated about network traffic caused shortcomings which observed in the recent years. It has been analysed available methods for the detection of existing anomalies in the time series was performed. it was noted information about objectives and disadvantages of methods.

Keywords – network traffic analysis, time series, anomaly, proximity based method, window based method, prediction based method, hidden markov method.

Əşyaların İnterneti texnologiyaları əsasında yaradılan şəbəkə mühitində hücumların təhlili

Məmməd Həşimov
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
mamedhashimov@gmail.com

Xülasə— Məqalədə əşyaların İnternetinin (IoT) bəzi təhlükəsizlik məsələləri araşdırılmışdır. IoT qurğuları vasitəsi ilə həyata keçirilən hücumlar göstərilmişdir. IoT şəbəkəsində istifadə olunan mövcud qurğularda yüksək təhlükəsizlik həllərinin tətbiq edilməməsi ilə bağlı məhdudiyyətlər təhlil edilmişdir. IoT şəbəkəsinin təhlükəsiz fəaliyyət göstərməsinə təsir edən hücumların təsnifatı verilmişdir.

Açar sözlər— əşyaların İnterneti (IoT), IoT təhlükəsizliyi, IoT qurğuları, IoT hücumları.

I. GİRİŞ

Hazırda internet, insanların gündəlik həyatının ayrılmaz bir hissəsinə çevrilmişdir. İnternetdən istifadə insanlar arasındakı ünsiyyəti, məlumat paylaşmasını və qarşılıqlı təsiri artıraraq gündəlik həyatımızı əhəmiyyətli ölçüdə dəyişdirdiyi artıq qaçılmaz bir gerçəklikdir. Bizi əhatə edən bütün faydalı əşyaların İnternet şəbəkəsinə qoşulması “Əşyaların İnterneti” termininin (ing. Internet of Things, IoT) yaradılmasına gətirib çıxarmışdır. IoT şəbəkəsində təkcə insanlar əşyalar arasında deyil, həmçinin əşyaların öz aralarında da qarşılıqlı əlaqələrinin qurulması nəzərdə tutulur [1]. IoT konsepsiyasının mahiyyəti ondan ibarətdir ki, bizi əhatə edən predmet və ya əşyalar (planşet, smartfon, fitnes üçün qurğu, ev avadanlıqları, geyimlər, avtomobillər, istehsal avadanlıqları, tibbi avadanlıqlar, dərman preparatları və s.) miniatur identifikasiya və sensor (həssas) qurğularla təmin olunaraq naqill və naqilsiz əlaqələr (sputnik, mobil əlaqə, Wi-Fi və Bluetooth) vasitəsilə qarşılıqlı əlaqədə olur və proseslərin tamamilə avtomatik yerinə yetirilməsini təmin edir [2].

IoT Dünya İqtisadi Forumunun qiymətləndirməsində dünyanı dəyişdirəcək texnologiyalar arasında ilk sıralarda yer alır və bu texnologiyanın yaxın 10 ildə dünya iqtisadiyyatında əsas trend olacağı proqnozlaşdırılır. IoT qurğularının sayı 2017-ci ildə 31% artaraq 8.4 milyarda çatmış və 2020-ci ildə bu sayın 30 milyarda çatacağı gözlənilir [3].

IoT texnologiyası əsasən aşağıdakı sahələrdə tətbiq edilir və yaxın onilliklər ərzində bizi əhatə edən hər şeyə təsir edəcəyi gözlənilir [4]:

- neft-qaz sənayesi: neft məhsullarının kəşfiyyatı, hasilatı, emalı, nəqli və satışı proseslərinin idarə edilməsi;
- şəhərlərdə: nəqliyyatın idarə edilməsi, işıqlandırma, dayanacaq, ağıllı ofis binaları, tullantıların idarə edilməsi;

- avtomobillərdə: prediktiv texniki təminat, toqquşmanın qarşısının alınması, öz-özünü idarə edən vasitələr;
- enerji istehsalı və paylanması: smart qrid, mikroqrid, elektrik stansiyalarının idarəetmə sistemləri;
- kənd təsərrüfatında: səmərəli hasilat, suvarma və gübrələmə;
- ətraf mühitdə: meşə yanğınlarının əvvəlcədən aşkarlanması, nəqli kəşilməkdə olan heyvanların izlənilməsi;
- tibbdə: məsafədən diaqnostika, yaşlı və xəstə insanların monitorinqi;
- və s.

IoT tətbiqləri və qurğularının sürətlə artması ilə yanaşı, kiber hücumlar da təkmilləşdirilərək təhlükəsizlik və məxfilik ilə əlaqədar daha da ciddi təhdidlər yaradır. Bu qurğuların əksəriyyəti kiber hücumlara qarşı dayanıqsızdır. Belə qurğular hakerlər üçün mühüm əhəmiyyət kəsb etməyə bilər. Ancaq hakerlər ciddi sistemlərə hücum məqsədilə botnetlərin (“robot” və “network” sözlərinin birləşməsindən yaranmışdır, zərərli proqramlarla yoluxmuş və bədnəyyətli tərəfindən idarə edilə bilən kompüterlər şəbəkəsidir [5]) yaradılması üçün belə qurğulara müdaxilə edirlər.

II. ƏŞYALARIN İNTERNETİNDƏ TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Gündən-günə artan IoT qurğularının yeni növləri geniş yayılmağa başlamışdır, lakin onların təhlükəsizlikə bağlı bir sıra çatışmazlıqları mövcuddur. Məşhur elektron ticarət şirkəti “Alibaba”-nın mobil təhlükəsizlik qrupunun apardığı araşdırmalara əsasən, IoT qurğularının proqram təminatının 90%-dən çoxu təhlükəsizlik hücumlarına məruz qalır. Onların 94%-də isə hakerlər tərəfindən asanlıqla istifadə oluna bilən veb interfeyslərində təhlükəsizlik boşluqları vardır [6]. Təhlükəsizlik mütəxəssislərinin fikirlərinə əsasən artıq ağıllı qurğuların təhlükəsizliyi çox ciddi məsələdir, bu, mümkün təhlükə deyil, real təhlükədir [7]. Çox hallarda hakerlər böyük iqtisadi ziyanə səbəb olmasalar da fiziki şəxslərin həyatına təhlükə yarada bilən implantasiya qurğularına və ya intellektual avtomobillərə distant olaraq təhlükə törədirlər. Bundan əlavə, IoT qurğuları sənaye, hərbi və digər əsas sahələrdə geniş istifadə edildiyinə görə, hakerlər ictimai və milli təhlükəsizliyə təhdid hesab edilə bilər.

2013-cü ilin dekabr ayında müəssisələrin təhlükəsizliyi ilə məşğul olan Proofpoint şirkətinin tədqiqatçısı ilk IoT botnetini aşkar etmişdir. Proofpoint şirkətinin məlumatına əsasən, burada ağıllı televizorlar, uşaq monitorları və digər ağıllı məişət texnikasından istifadə olunmuşdur [8]. 21 oktyabr 2016-cı il tarixində Domain Name System provayderi olan Dyn-ə qarşı hücum edilmişdi. Həmin hücum nəticəsində GitHub, Twitter və başqaları kimi saytlara giriş dayandırılmışdı [6]. Bu hücum, printer, IP kamera, şəbəkə keçidləri və monitorları və s. daxil olmaqla çoxsaylı IoT qurğularından ibarət olan botnet vasitəsilə həyata keçirilmişdir.

“Kaspersky Lab” şirkətinin mütəxəssisləri tərəfindən hazırlanan hesabat əsasən 2017-ci ilin əvvəlindən ağıllı qurğular üçün zərərli proqramların sayı iki dəfə artıb və hücumların sayı 7 mini ötüb [9]. Kibercinayətkarlar ağıllı qurğuların sistemlərini qırmaqla istifadəçiləri izləyə bilər, onları şantaj edir və hər hansı bir cinayət törətmək üçün onların qurğularından bir vasitə kimi yararlanırlar.

IoT qurğuları və şəbəkələri təbii resurs baxımından məhduddur. Şərti təhlükəsizlik həllərinin IoT əsaslı sistemlərə tətbiq edilə bilməməsi üçün əsas məhdudiyyətlər aşağıdakılardır [10, 11]:

- IoT qurğularında adətən aşağı sürətli Mərkəzi Prosessor (CPU, ing. Central Processing Unit) dan istifadə edildiyindən, bu qurğular daha çox batareya ilə idarə olunurlar. Müasir kriptografik alqoritmlər isə sürətli hesablama tələb etdiyinə görə həmin qurğulara birbaşa ötürülə bilmir.

- Telefon və noutbuklarla müqayisədə, IoT qurğularında yaddaş məhdud həcmdədir. Şərti təhlükəsizlik arxitekturaları isə məhdud yaddaşa malik qurğular üçün nəzərdə tutulmamışdır.

- IoT qurğuları adətən rabitə qurmaq üçün aşağı səviyyəli rabitə interfeyslərindən istifadə edirlər. Aşağı sürətli kommunikasiya mühiti səbəbindən ənənəvi təhlükəsizlik sxemləri IoT əsaslı sistemlərə tətbiq edilə bilmirlər.

- Mobil IoT qurğuları əvvəlcədən konfigurasiya edilmədən şəbəkəyə qoşula və ya qəflətən şəbəkəni tərk edə bilər. Şəbəkə topologiyalarında bu tip ani dəyişiklik mövcud təhlükəsizlik sxemlərinin fəaliyyətinə təsir edir. Nəticədə, bu sxemlər IoT mühitinə tətbiq edilə bilməz.

- IoT mühitində qurğular müxtəlif növ naqilsiz protokollardan (*RFID, WiFi, Zigbee, Z-Wave, Bluetooth* və s.) ibarətdir. Mövcud təhlükəsizlik həlləri arasında, müxtəlif qurğulara kompleks həll tapmaq çətindir.

Son zamanlarda IoT qurğularının təhlükəsizliyini təmin etmək üçün bu problemlərə qarşı mübarizə aparmaq, həmin riskləri minimallaşdırmaq və ya aradan qaldırmaq məqsədilə daha yaxşı metodların hazırlanması istiqamətində bir çox tədbirlər həyata keçirilir. Avropa Komissiyası IoT-un kibertəhlükəsizliyinin təmini üçün tədbirlər kompleksi hazırlamağı planlaşdırır [12]. Avropa Birliyinə üzv ölkələr tərəfindən dövlət səviyyəsində qəbul ediləcək qərarlar internetə qoşulma imkanına malik bütün qurğular üçün

sertifikatlaşdırma və ya analogi prosedurun tətbiqini nəzərdə tutur.

III. ƏŞYALARIN İNTERNETİ ŞƏBƏKƏSİNƏ OLUNAN HÜCUMLARIN TƏSNİFATI

IoT mühitində baş verə biləcək müxtəlif növ hücumları aşağıdakı kimi qruplaşdırmaq olar [10, 13, 14]:

Hücumların təsirinə görə təsnifatı (ing. Classification of Attack Severities)

- **Yüksək təsirli hücumlar:** bu hücumlar IoT əsaslı sistemi bütövlükdə təhlükə altına sala bilər. Hücum edən autentifikasiya etmədən IoT şəbəkəsinə və sisteminə daxil ola bilər. Bu cür hücumlar məlumatların məxfilik və bütövlüyünü tamamilə poza və IoT xidmətlərini dayandıra bilər.

- **Orta təsirli hücumlar:** bu hücumlar, hücumla məruz qalmış IoT əsaslı sistemin fəaliyyətinin qismən pozulmasına səbəb olur. Hücumlar sistemə yüksək təsir göstərsə də hücum edən imkanları məhdud olur (məsələn, hücum edən müxtəlif imtiyazlara malik ola bilər, lakin bütün sistemə tam nəzarət edə bilmir).

- **Aşağı təsirli hücumlar:** bu hücumlara kiçik təhdidlər aiddir. Demək olar ki, bütün hallarda, edilən hücum IoT xidmətlərinin təmin edilməsinə təsir göstərmir.

Qurğu əsaslı hücumlar (ing. Attacks Based on Device Property)

- **Aşağı səviyyəli qurğu sinfinə edilən hücumlar:** hücum edən və hədəf IoT qurğusu olub, eyni yaddaş və CPU sürəti kimi oxşar konfigurasiyalara və imkanlara malikdir. Məsələn, zərərli proqram təminatı ehtiva edən ağıllı saat və ya ağıllı televizora avtorizasiyasız daxil olur, daha sonra ağıllı televizordan spam e-poçtları göndərir.

- **Yüksək səviyyəli qurğu sinfinə edilən hücumlar:** bu zaman, hücum edən qurğu hücum edilən qurğudan daha güclü olur. Hücum edən IoT şəbəkəsinə və ağıllı qurğulara çıxış əldə etmək üçün fərdi kompüterlərdən, dizüstü kompüterlərdən və ya virtual maşın qismində tam təchiz edilmiş qurğulardan istifadə edərək zərərli fəaliyyətlər həyata keçirir.

Məkana bağlı hücumlar (ing. Attacks Based on Adversary Location)

- **Daxili hücum:** hücum edən və hücum edilmiş qurğu eyni şəbəkə daxilindədir. Hücum edən həmin şəbəkə daxilində hər hansı bir komponent tərəfindən hücumlar həyata keçirir. Məsələn, o, evin təhlükəsizlik sistemini söndürmək üçün qurğular arasında mövcud olan etibarlılıq əlaqələrindən istifadə edərək bir ağıllı qurğudan digərinə keçə bilər.

- **Xarici hücum:** düşmən və hücum edilmiş qurğu müxtəlif şəbəkələrdə yerləşir. Hücum edən hər yerdə yerləşdirilə bilər. Məsələn, düşmən avtorizasiya sisteminin zəifliklərindən istifadə edərək ev şəbəkələrinə distant olaraq daxil olur, daha sonra ağıllı qurğulara hücum etməyə başlayır.

Hücum strategiyalarına əsaslanan hücumlar (ing. Attacks Based on Attack Strategy)

• **Fiziki hücumlar:** bu hücumlar fiziki ziyana səbəb olur, qurğunun xüsusiyyət və konfigurasiyalarını dəyişir. Məsələn, düşmən qurğuya zərərli kodları və saxta məlumatları daxil etməklə hücum edir.

Zərərli kodun daxil edilməsi hücumu (ing. Malicious code Injection Attacks) – hücum edən cihazın yaddaşına zərərli kodu salmaqla onu idarə edə bilər. Həmin zərərli kod yalnız spesifik funksiyaları yerinə yetirmir, həm də IoT sisteminə hücum edəninin çıxışını və hətta onun IoT sisteminə tam nəzarət etməsini təmin edə bilər.

Saxta məlumatın daxil edilməsi hücumları (ing. False Data Injection Attacks) – IoT-dakı qurğuların ələ keçirilməsi ilə, hücum edən həmin qurğudan alınmış normal məlumatların yerinə saxta məlumatlar yerləşdirə və saxta məlumatları IoT təbiiqlərinə ötürə bilər. Saxta məlumatlar alındıqdan sonra, IoT proqramları yanlış əks əlaqə əməllərini geri göndərə və ya yanlış xidmətlər təqdim edə bilər ki, bu da IoT proqram və şəbəkələrinin effektivliyinə təsir edə bilər.

• **Məntiqi hücumlar:** bu hücumlar IoT qurğusuna heç bir fiziki ziyan vurmadan onların fəaliyyətini dayandırır (yəni hücumu məruz qalmış qurğu real zaman rejimində məlumatların ötürülməsini dayandırır).

Giriş səviyyəsinə əsaslanan hücumlar (ing. Attacks Based on Access Level)

• **Aktiv hücumlar:** hücum edən IoT-un qurğu və şəbəkələrinin normal funksiyasını pozur. Resursların tükənməsi və yüklənməsi kimi müxtəlif növ *xidmətdən imtina hücumları (ing. Denial-of-service attacks, DoS)* aktiv hücumlar hesab edilir. DoS hücumları şəbəkə protokollarına hücum etməklə və ya şəbəkəni izafi trafiklə yükləməklə IoT sistemlərinin xidmətlərini yararsız hala sala bilər. DoS hücumu ən çox yayılmış hücumlardan biri hesab edilir. DoS hücumları *Ping of Death, TearDrop, UDP, SYN, Land Attack* və s. kimi hücum sxemlərinin vasitəsi ilə yaradılır.

• **Passiv hücumlar:** hücum edən səlahiyyətli IoT qurğusu olub, şəbəkənin funksiyasını pozmadan əlaqə kanalının monitorinqini aparmaqla və trafikini təhlil etməklə etibarlı şəxslərdən məlumat toplamaq üçün qeyri-qanuni fəaliyyət göstərir. Bu növ hücumlar IoT-un məxfiliyinə təhlükə yaradır.

İnformasiya təhlükəsi səviyyəsinə əsaslanan hücumlar (ing. Attacks Based on Information Damage Level)

• **Fasilələr:** fasilələrin yaradılması ilə həyata keçirilən hücumlar IoT xidmətlərinə qarşı edilir. Bu növ hücumlar xidmətin keyfiyyətini aşağı salır və ya onların qanuni istifadəçilər tərəfindən istifadəsinə imkan vermir.

• **Gizli dinləmə:** hücum edən istənilən əlaqə kanalına icazəsiz giriş əldə edir və şəxsi əlaqə vasitəsilə aparılan mesajları “dinləyir”. Bu növ hücum məlumatların məxfiliyinə qarşı edilir.

• **Modifikasiya:** bu, hücum edəninin məlumatı dəyişdirmək (dəyişiklik, əlavə, silinmə) cəhdidir. Bu növ

hücum şəbəkədəki əlaqə kanallarının qarışıqlığına və dəyişik düşməsinə səbəb olur. Modifikasiya hücumları məlumatın bütövlüyünə təhdid hesab edilir.

• **Saxtalaşdırma:** hücum edən saxta məlumat daxil etməklə və ya saxta fəaliyyət göstərməklə kommunikasiyada iştirak edən elementlər arasında qarışıqlıq yaranan mesaj göndərir. Bu növ hücumlar mesajın orijinallığına təhlükə yaradır.

• **Ortada adam hücumu (ing. Man-in-the-middle Attack):** hücum edən autentifikasiya olunan və autentifikasiya edən qurğular arasında yerləşərək onlar arasında ötürülən verilənləri ələ keçirə və dəyişə bilər. Həmin iki normal qurğu araya daxil olan qurğunu aşkar edə bilmir və hətta bir-birləri ilə birbaşa ünsiyyət qurduqlarını ehtimal edirlər. Bu hücum iki normal qurğu arasındakı əlaqəni izləmək, dinləmək, təhrif etmək və nəzarət etməklə IoT-dakı məlumatların gizliliyini, bütövlüyünü və məxfiliyini poza bilər.

Host əsaslı hücumlar (ing. Host Based Attacks)

• **İstifadəçi təhdidləri:** istifadəçilər şəxsi məlumatlarını (ad və ya doğum tarixi) və ya təhlükəsizlik məlumatlarını (açar, şifrə) qeyri-təhlükəsiz vasitələrlə təqdim etməyə təhrik edirlər. Şifrələnməmiş mesajların və zəif kriptografik sxemlərin qeyri-təhlükəsiz vasitələrlə ötürülməsi istifadəçilərə qarşı edilən hücumlara səbəb olur.

• **Proqram təminatına təhdid:** hücum edən IoT qurğularının proqram təminatının boşluqlarından istifadə edir. Məsələn, hər hansı zərərli qurğu hücum edilən qurğuya dayanmadan əlaqə sorğusu göndərməklə onu “donmuş” vəziyyətə salır. Bu proses hücum edilən qurğunun hücum edən qurğunu bloka salmaq kimi xüsusiyyətə malik olmadığı halda baş verə bilər.

• **Texniki təminatı təhdid:** verilənlər, açar və proqram kodları kimi həssas məlumatlar IoT qurğusunun özündə saxlanılır. Hücum edən fiziki qurğuya giriş tələb edən texniki təminatı təhrif edərək həmin sənədləri əldə edir. O, müəyyən qurğu üzərində mikro yoxlama və əks mühəndislik kimi zərərli fəaliyyətlər həyata keçirir.

NƏTİCƏ

IoT gündəlik həyatımızda bizi böyük faydaları ilə təmin etsə də, müxtəlif təhlükəsizlik təhdidlərinə meyillidir. Bu texnologiyanın geniş yayılması və tətbiqi ilə bağlı ən mühüm problemlərdən biri də məhz təhlükəsizlik məsələləridir. Əsasən istifadə edilən “əşyaların” (qurğuların) minimal yaddaş həcmi, aşağı sürətli CPU-dan istifadə edilməsi, naqilsiz şəbəkə protokolları vasitəsilə əlaqə qurulması, obyektlərin fiziki əlyetərliyi və sistemlərin açıq olması nəticəsində təhlükəsizlik hücumları IoT üçün daha da böyük problemə çevrilir. Kibercinayətkarların da bu cür boşluqlardan faydalanması təhlükəsizlik problemlərinin həllini daha da mürəkkəbləşdirir. İnternetə qoşulmuş qurğuların hücumlara qarşı müdafiəsini təmin etmək üçün həmin riskləri minimallaşdırmaq və ya aradan qaldırmaq məqsədilə daha yaxşı və müasir metodların işlənilib hazırlanmasına ehtiyac vardır.

ƏDƏBİYYAT

- [1] R.M. Əliquliyev, R.Ş. Mahmudov, Əşyaların İnterneti: mahiyyəti, imkanları və problemləri, İnformasiya cəmiyyəti problemləri, 2011, №2(4), s.29-40.
- [2] M.H. Məmmədova, Z.Q. Cəbrayıllova, Dəniz neft platformasında personalin fizioloji vəziyyətinin və coğrafi mövqeyinin monitorinqində əşyaların internetinin imkanları, 2018, №2, s.3-17.
- [3] Report-internet of things. <http://reports.weforum.org/industrial-internet-of-things/general-findings/2-1-the-state-of-the-market/>
- [4] C.R. Baudoin. Deploying the Industrial Internet in Oil & Gas: Challenges and Opportunities // Society of Petroleum Engineers, 2016, pp.1-11.
- [5] Y.N. İmamverdiyev, G.B. Qarayeva, Botnetlər və onların aşkarlanması üsulları, İnformasiya texnologiyaları problemləri, 2017, №1, s.100–111.
- [6] W.Zhou, Y.Jia, A.Peng, Y.Zhang, P.Liu, The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved, IEEE Internet of Things Journal, 2015.
- [7] Malware ‘loving’ smart devices. www.pressreader.com/uae/khaleej-times/20170708/282497183695817
- [8] 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, 2017, vol.4, issue.5, pp. 1250– 1258.
- [9] Ловушки «интернета вещей». <https://securelist.ru/honeypots-and-the-internet-of-things/30874/>
- [10] A.Haritha, A.Lavanya, Internet of Things: Security Issues, International Journal of Engineering Science Invention, 2017, vol. 6 Issue 11, pp. 45-52.
- [11] L.S. Sayana, B.K. Joshi, Security Issues in Internet of Things, UGC Sponsored National Conference on Global Challenges – Role of Sciences & Technology in Imparting their Solutions (GCRSTS 2016), April 2016.
- [12] How the EU cybersecurity act could set standards that impact legal liability and cross-border data flows. <https://www.itproportal.com/features/how-the-eu-cybersecurity-act-could-set-standards-that-impact-legal-liability-and-cross-border-data-flows/>
- [13] M.Nawir, A.Amir, N.Yaakob, O.B.Lynn, Internet of Things (IoT): Taxonomy of Security Attacks, 3rd International Conference on Electronic Design (ICED), pp. 321-326. August 11-12, 2016.
- [14] J.Deogirikar, A.Vidhate, Security Attacks in IoT: A Survey, International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2017), pp. 32-37, 2017.

**ANALYSIS OF THE ATTACKS TO NETWORK
ENVIRONMENT BASED ON IoT TECHNOLOGY**

Mammad Hashimov

Institute of Information Technology of ANAS, Baku,
mamedhashimov@gmail.com

Abstract - The article examines the some safety issues of the Internet of Things (IOT). It highlights the attacks through IoT devices. It analyzes the restrictions related to the unavailability of applying high-security solutions in existing IoT devices used in IoT networks. The article also classifies the attacks affecting the safe functioning of IoT network.

Keywords - Internet of Things (IoT), IoT security, IoT devices, IoT attacks.

Elmi-texnoloji innovasiya parklarının informasiya təhlükəsizliyi problemləri

Roza Şahverdiyeva

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

shahverdiyevavar@gmail.com

Xülasə -Məqalə elmi-texnoloji innovasiya texnoparklarının informasiya sistemləri və texnologiyalarının təhlükəsizliyi problemlərinə həsr olunmuşdur. İnnovasiya texnoparklarının informasiya və biliklər iqtisadiyyatında rolu, vəzifələri, əhəmiyyəti izah olunmuşdur. Onların idarə olunmasında müasir informasiya təminatının yaxşılaşmasına təsir edən amillər şərh olunmuşdur. Texnoparkların informasiya sistemləri, resursları və texnologiyalarının təhlükəsizliyinin formalaşma mərhələləri verilmişdir. İnformasiya təhlükəsizliyi sisteminin arxitektura-texnoloji strukturu işlənmiş və onun təkmilləşdirilməsi üzrə bəzi tövsiyələr verilmişdir.

Açar sözlər – *informasiya və biliklər iqtisadiyyatı; elmi-texnoloji innovasiya texnoparkı; informasiya sistemlərinin təhlükəsizliyi; informasiya təminatı və təhlükəsizliyi; təhlükəsizlik metodları.*

I. GİRİŞ

Beynəlxalq səviyyədə iqtisadi inkişaf daha çox innovasiyalara, yeni texnologiyalara, biliklərə əsaslanır. Bu istiqamətdə elm-təhsil-istehsalat sahələri arasında qarşılıqlı əlaqələrin gücləndirilməsi məqsədilə yeni idarəetmə mexanizmlərinin işlənilməsi, innovasiya mərkəzlərinin, texnoloji komplekslərin, texnoparkların, biznes-inkubatorların yaradılması və fəaliyyətinin təşkili məsələləri nəzərdə tutulmuşdur [1, 2].

Hal-hazırda ölkədə informasiya resursları və proseslərinin mühafizəsi, onların sabitliyi və fasiləsizliyi həyata keçirilir. İnformasiya ehtiyatlarının qorunması sahəsində təhdidlərin qarşısı alınır. Təhlükələrin təhlili və onların aradan qaldırılması üçün informasiya infrastrukturunu subyektlərinin, onların istifadəçilərinin fəaliyyətinin əlaqələndirilməsi sahəsində tədbirlər görülür. Eyni zamanda kibertəhlükəsizlik sahəsində risklərin qiymətləndirilməsi və idarə olunması məqsədi ilə informasiya təhlükəsizliyi üzrə fəaliyyətin təkmilləşdirilməsi istiqamətində tədbirlər həyata keçirilir.

İnnovativ iqtisadiyyatın davamlı inkişafına və rəqabət qabiliyyətinin artırılmasına yeni texnologiyaların işlənilməsi üzrə müasir komplekslərin yaradılmasına nail olmaq üçün Sumqayıt sənaye və kimya texnologiyası parkı, NRYTN-də “Yüksək texnologiyalar parkı”, Balaxanıda eko-sənaye parkı, AMEA-da Yüksək Texnologiyalar Parkı, regionlarda aqro və digər yüksək texnologiyalar parkı yaradılmışdır. Onların və onlar kimi digər innovasiya strukturlarının əsas idarə etmə problemlərindən biri də informasiya resurslarının,

sistemlərinin, texnologiyalarının təhlükəsizliyinin təmin edilməsi məsələsidir.

Texnoparklar mahiyyət və məzmun etibarilə digər iqtisadi strukturlardan daha çox yeniliyi, 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. Bütün bunlar elmi-texnoloji innovasiya texnoparklarının informasiya sistemləri və texnologiyalarının təhlükəsizliyi problemlərinin, informasiya təminatının və onun təhlükəsizliyinin spesifikliyinin nəzərə alınmasını və həmin sahədə müvafiq metod və mexanizmlərin işlənilməsinə zəruri edir.

II. ELMİ-TEXNOLOJİ INNOVASIYA PARKLARININ İQTİSADİYYATDA ROLU VƏ VƏZİFƏLƏRİ

Hər bir ölkənin iqtisadi inkişafında elmi-texnoloji innovasiya texnoparkları əhəmiyyətli rola malikdir. Çünki İnformasiya və biliklər iqtisadiyyatının infrastrukturunun əsasını elmi-texnoloji innovasiya texnoparkları təşkil edir. İnnovasiya yönümlü, informasiya və biliyə əsaslanan iqtisadiyyatın qurulmasında yüksək texnologiyalar, innovativ parklarının yaradılması əsas məqsədlərdəndir. Rəqəmsal və ya innovativ iqtisadiyyata keçid üçün yüksək texnologiyalar parkı, elm-texnoloji innovasiya texnoparkları əsas hərəkətverici qüvvədir.

Texnoparkların yaradılmasının əsas xüsusiyyətlərinə: 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) yüksək texnologiyalar sektorunun inkişaf etdirilməsi, 8) elmi-tədqiqat işlərinin nəticələrinin sürətlə reallaşması, 9) regional büdcənin gəlirlərinin artırılması, 10) innovativ texnologiyaların transferi, 11) intellektual mülkiyyətin qorunması, 12) kollektiv istifadə mərkəzlərinin formalaşdırılması və s. daxildir [3, 4, 5].

İnformasiya təminatı və təhlükəsizlik məsələləri ümumi halda texnoparkların idarə edilməsi sisteminin funksiyalarından da asılıdır. Həmin funksiyalara aşağıdakılar

daxildir: 1) texnoparkların fəaliyyətində güzəştli şərtlər, elmi-tədqiqat və təcrübə-konstruktor işlərinin yerinə yetirilməsi üçün əlverişli şəraitin yaradılması, 2) rezident-şirkətlərin fəaliyyəti üçün əlverişli şəraitin olması, 2) innovasiya müəssisələrinin dəstəklənməsi sisteminin formalaşdırılması, 3) kiçik innovasiya müəssisələrinə konsaltinq, mühəndis, texniki, texnoloji, informasiya və digər xidmətlərin göstərilməsində yardım etmək, 4) innovasiyalı məhsulun üzə çıxarılması, seçim və istehsalda tətbiqinə qədər onların müşayiət olunması, 5) qərar qəbul etməyə dəstək məqsədilə intellektual informasiya sisteminin işlənilməsi və s. Texnoparklarda məhsulun istehsalı, müəyyən bir innovativ proseslə xarakterizə olunur. Ümumi halda innovasiya prosesinə yeni kəşf, texnologiyaların, məhsul və xidmətin, intellektual fəaliyyətin kommersiyalaşdırılması kimi baxıla bilər. Bu prosesin strukturuna bir çox mərhələləri daxil etmək olar [6].

Yeni texnologiyaların texnopark və digər innovativ müəssisələrin idarə etmə sahələrinə tətbiq olunması innovasiya fəaliyyəti ilə xarakterizə olunur. Texnoparklarda innovasiya fəaliyyəti əhatəli və çox istiqamətlidir. Ona görə də belə fəaliyyəti həm ayrı-ayrılıqda olan göstəricilərlə, həm də qrup və istiqamətlərdə birləşən göstəricilərlə xarakterizə edirlər [7]. Texnoparklarda innovasiya fəaliyyəti üzrə 1) müəssisənin innovativ aktivliyi, 2) müəssisələrdə elmi-tədqiqat bölməsinin mövcudluğu, 3) daxili və xarici bazarlardakı satışın həcmində innovasiya məhsul və xidmətlərinin strukturu, xüsusi çəkisi, 4) innovasiya fəaliyyəti nəticələrinin reyting göstəriciləri, 5) ölkə və regionlar üzrə innovasiya fəaliyyəti ilə məşğul olan innovativ müəssisələrin strukturu, 6) maliyyə mənbələri üzrə innovasiya xərclərinin strukturu, 7) innovasiya fəaliyyəti növləri üzrə xərclərin strukturu və xüsusi çəkisi, 8) innovasiya üzrə məlumat mənbələrinin reytingi, 9) texnoloji innovasiyalara mane olan faktorların reytingi və s. kimi əsas göstəriciləri təhlil etmək lazımdır [8, 5, 9].

Göstərilən xüsusiyyətlər, mərhələlər və göstəricilər innovasiyanın formalaşmasına birbaşa təsir etdiyi kimi, onlarla əlaqədə olan informasiya təminatı və təhlükəsizliyi məsələlərinin müəyyənləşdirilməsi və həlli istiqamətlərinin işlənilməsinə də bilavasitə təsir edir.

III. ELMİ-TEKNOLOJİ INNOVASIYA PARKLARININ INFORMASIYA SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİ

Elmi-texnoloji innovasiya texnoparklarının informasiya sistemlərinin təhlükəsizliyi məsələləri kompleks xarakter daşıyır. Həmin məsələlər istənilən innovativ müəssisənin, texnoparkların yerinə yetirdiyi funksiyalardan asılıdır. Bu səbəbdən də innovativ elmi texnoparklarda informasiya təhlükəsizliyinin idarə olunmasının bəzi aspektləri tədqiqat işlərində əks olunmuşdur. [10]-də innovasiya müəssisələrində informasiya təhlükəsizliyinin idarəedilməsinə təsir edən faktorlar araşdırılmışdır. Göstərilmişdir ki, hazırda informasiya müəssisənin ən əhəmiyyətli kapitalı hesab edilir və o aparıcı rola malikdir. Müxtəlif müəssisələrdə informasiya təhlükəsizliyinə qoyulan tələblər müxtəlif təhlükəsizlik tədbirlərinin tətbiqini tələb edir. İnformasiyanın

təhlükəsizlik nöqteyi-nəzərindən hərtərəfli qorunması və saxlanılması üçün böyük səylər göstərilməlidir. Məqalədə İran və Türkiyə nümunəsində olan innovasiya müəssisələrində informasiyanın idarə edilməsi məsələsi tədqiq edilmişdir. Türkiyə təcrübəsi əsasında toplanılmış analoji məlumatlarla alınmış nəticələr müqayisə edilmişdir. Aparılan tədqiqat bir çox müəssisələrin təcrübəsi əsasında həyata keçirilmişdir.

[11]-də isə Türkiyə nümunəsində innovasiya müəssisələrində informasiya təhlükəsizliyinin idarə olunmasına təsir edən amillər araşdırılmışdır. İnnovasiya müəssisələrində korporativ informasiya təhlükəsizliyi araşdırılmış və nəticələr müxtəlif ölkələrdən toplanan oxşar informasiyalarla müqayisə edilmişdir. Bu araşdırmanın nəticələrinə görə şirkətlərdə digər təhlükəsizlik tədbirləri kommunikasiya, əməliyyatlar və təhlükəsizlik siyasətinin yaxşılaşdırılması zamanı qəbul edilə bilər. Alınmış nəticələrdə Türk şirkətlərinin müxtəlif ölkələrin tərəfdaş şirkətləri kimi informasiya texnologiyalarının təhlükəsizliyinə çox əhəmiyyət verilmədiyini göstərilmişdir.

[12]-də göstərilir ki, bir çox innovativ strukturların, proseslərin informasiya təhlükəsizliyinin məsafədən idarə olunmasının arxitektura-texnoloji infrastrukturunun müasir kontekstdə işlənilməsinə ehtiyac formalaşmaqdadır. Bu prosesi həm proqram, həm də aparat-texniki vasitələrini innovativ effektiv strukturlaşdırılması yolu ilə həll etmək olar.

Texnoparkların fəaliyyətinin idarə edilməsində qərar qəbul etmə prosesi onun müasir informasiya təminatının formalaşmasını zəruri edir. Texnoparkların informasiya təminatı sistemi 1) müxtəlif idarəetmə orqanları ilə informasiya əlaqəsi, 2) inzibati idarə etmə sistemi bloku, 3) elm-təhsil strukturları ilə əlaqə, 4) İKT infrastruktur bloku, 5) İnternet, İnternet provayderləri, 6) beynəlxalq təşkilatlarla əlaqələndirmə bloku, 7) verilənlərin saxlanması və emalı bloku (DATA mərkəz), 8) istehsal/xidmət, servis təminatı bloku, 9) daxili strukturlarla əlaqə bloku, 10) innovasiya xidmətləri bloku, 11) regional strukturlarla informasiya əlaqələri bloku, 12) innovativ layihələrin idarə olunması bloku, 13) e-xidmətlər və elmi bazalara çıxış, 14) riyazi və proqram təminatı və s. kimi əsas struktur elementlərindən, bloklardan təşkil olunmuşdur [4].

İdarə etmə prosesində informasiya təminatının əsas komponentləri 1) idarəetmə strukturlarını faktiki məlumatlarla təmin etmək, 2) avtomatlaşdırılmış idarəetmə sistemləri üçün informasiya təminatından istifadə, 3) müxtəlif təşkilatların idarəetmə fəaliyyətinin təminatı üçün 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 kimi məsələlər tədqiq olunmuşdur.

İnformasiya təminatı sistemi 1) informasiyanın toplanması, 2) informasiya dövriyyəsinin təşkili, 3) informasiyanın saxlanması, və aktualaşdırılması, 4) informasiya sisteminin

texniki təminatı, 5)informasiya sisteminin riyazi proqram təminatı, 6)informasiyanın verilməsi və s. kimi bir sıra elementləri özündə əks etdirir. Texnoparkın idarə etmə prosesində informasiya təminatının yaxşılaşmasına elmi-texniki, təşkilatı-iqtisadi, sosial-psixoloji və hüquqi amillər təsir edir.

Elmi-texnoloji innovativ parkların informasiya təhlükəsizliyi sisteminin qurulması üçün ümumi prinsiplərə və yanaşmalara aşağıdakıları aid etmək olar [7]: 1)innovasiya fəaliyyəti subyektlərinin düzgün təhlükəsizlik strategiyasının müəyyənəndirilməsi, innovativ strukturun fəaliyyət xüsusiyyətlərinin nəzərə alınması; 2)informasiyanın təhlükəsizliyi sahəsində çevik idarəetmə qərarlarının qəbulunun keyfiyyətinin yüksəldilməsi, 3)innovativ strukturlarda informasiya təhlükəsizliyi siyasətinin səmərəliliyinin yüksəldilməsi; 4)informasiyanın qorunması üzrə xüsusi xidmət qruplarının formalaşdırılması.

Elmi-texnoloji innovativ parkların informasiya təhlükəsizliyi xidmətinin əsas funksiyalarına aşağıdakıları daxil etmək olar: 1)strukturda məxfi informasiyanı qorunmasının təşkili və həyata keçirilməsi; 2) strukturun fəaliyyəti haqqında məxfi məlumat əldə etmək məqsədi ilə işçi heyət ilə bağlı təxribatlar; digər hərəkətlər haqqında məlumatların yoxlanılması; 3)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)iqtisadi, informasiya və fiziki təhlükəsizlik qaydalarına riayət etmək üçün işçilərin yoxlanılması; 7)arzu olunmaz tərəfdaşlarla sazişlərin qarşısının alınması məqsədi ilə zəruri informasiyanın yığımı, emalı, saxlanması və analizi; 8)innovativ struktur rəhbərliyinin tapşırıqlarının yerinə yetirilməsi; 9)struktur işçilərinin rəsmi sənədlərinin təhlükəsizliyini təhdid edən məxfi informasiyanın açıqlanması ilə bağlı tədqiqatların aparılması.

Elmi-texnoloji innovativ parkların informasiya təhlükəsizliyinin əsas istiqamətləri aşağıdakılardır [7]: 1)informasiya təhlükəsizliyi sisteminin qurulması istiqamətində yerli problemlərin həlli; 2)təhlükəsizliyin təmin olunmasında təşkilatı-idarəetmənin rolunun artırılması; 3)informasiya təhlükəsizliyi sahəsində innovativ strukturun konsepsiyası və siyasətinin müəyyən edilməsi ilə başlayan informasiya təhlükəsizliyi sisteminin yaradılması; 4)informasiya təhlükəsizliyi sistemlərinin sınaq vəziyyətinin monitorinqi; 5)informasiya təhlükəsizliyi sistemlərinin fəaliyyətinin effektivliyinin qiymətləndirilməsində tətbiq edilən iqtisadi göstəricilərin müəyyənəndirilməsi. Elmi-texnoloji innovativ parkların informasiya təhlükəsizliyi siyasətinin işlənilməsi zamanı göstərilən tendensiya, prinsip və yanaşmalar nəzərə alınmalıdır.

IV.ELMI-TEKNOLOJİ INNOVASIYA TEXNOPARKLARININ INFORMASIYA TƏHLÜKƏSİZLİYİNİN İDARƏ EDİLMƏSİ

Texnoparklar üçün daha çox təhlükə yaradan hallar sırasına onun infrastrukturunu formalaşdıran yerli informasiya və telekommunikasiya sənayesinin fəaliyyətini və onun

müvafiq məhsul istehsalı və xidmət göstərməsinin qarşısını alan situasiyaları aid etmək olar. Bundan başqa ictimai-zəruri informasiya resurslarına səmərəsiz və həddən artıq olan məhdudiyyətlər, açıq informasiya fondlarına girişin məhdudlaşdırılması və s. kimi innovativ texnologiyaların tətbiqinin aşağı salınmasına yönəlmiş tədbirləri də bu sıraya aiddir. Eyni zamanda informasiya manipulyasiyası, yeni informasiya texnologiyalarından istifadəyə qarşı hərəkətlər, intellektual mülkiyyət sahiblərinin xaricə axını, informasiya emalı texnologiyaları prosedurunun pozulması, şəbəkələrdə informasiyanın ələ keçirilməsi və onlardan dezinformasiya və digər bəd niyyətlərlə istifadə olunması da təhlükə mənbəyi hesab olunur [6].

Texnoparkların təhlükəsizlik siyasətinin reallaşdırması üçün informasiyanın mühafizəsi metodlarına aşağıdakılar daxildir [8]: 1)müdafiə edilən obyektlərdə kompleks müdafiənin reallaşdırılmasına imkan verən texniki vasitələr və təşkilati tədbirlər; 2)müdafiənin əsas vasitələrinin seçimi və yerləşdirilməsi üçün təklif və tövsiyələr; 3)informasiya təhlükəsizliyi sisteminin tətbiqinin texniki-iqtisadi əsaslandırılması; 4)mümkün təhlükələrin qiymətləndirilməsi, itkilərin ölçülərini nəzərə almaqla sistemin effektivliyinin qiymətləndirilməsi; 5)informasiya təhlükəsizliyi siyasətinin dəstəklənməsi və reallaşdırılması üzrə planın hazırlanması; 6)müəssisədə informasiya təhlükəsizliyi sistemlərinin inkişafı və təkmilləşdirilməsi ilə bağlı təkliflərin hazırlanması; 7)təklif olunan mühafizə tədbirlərinin səmərəliliyini nəzərə alaraq innovasiya strukturuunun səmərəliliyinin qiymətləndirilməsi.

Elmi-texnoloji innovasiya texnoparklarının informasiya təhlükəsizliyinin arxitektura sxemini şəkil 1-dəki kimi vermək olar [13].

Şəkil 1. Elmi-texnoloji innovasiya texnoparklarının informasiya təhlükəsizliyi sisteminin arxitektura-texnoloji strukturu

Texnoparkların ümumi təhlükəsizlik konsepsiyasına müvafiq olaraq informasiya mühafizəsi xidmətinin praktiki fəaliyyəti nümunəvi sxem, prosedur və fəaliyyətə əsaslanır. Burada ilk növbədə həmin fəaliyyətin müəyyən ardıcıl mərhələlər üzrə həyata keçirildiyini qeyd etmək lazımdır (şəkil 2). Texnoparkların fəaliyyətində mövcud təhlükələrin struktur təhlili informasiya risklərini müəyyənləşdirməyə və nəticə etibarlı ilə həmin strukturun dayanıqlı kompleks fəaliyyət proqramını işləməyə imkan verir. Risklərin idarə olunması üçün daxili və xarici təhlükə mənbələrini müəyyən etmək və həmin təhlükə ilə yaranacaq risk və fəaliyyət nəticələri arasındakı səbəb-nəticə əlaqələrini aşkarlamaq zəruridir.

Şəkil 2. Elmi-texnoloji innovasiya texnoparklarının informasiya təhlükəsizliyinin idarə olunması mərhələləri

Texnoparkların fəaliyyətində informasiya təhlükəsizliyinin təkmilləşdirilməsi üçün bir sıra məsələlərə baxılır və həll edilir: 1) texnoparkın informasiya təhlükəsizliyinin təminatı üçün məqsədli proqramın işlənilməsi, 2) texnoparkın informasiya təhlükəsizliyinin təminatı sisteminin inkişaf etdirilməsi və təkmilləşdirilməsi, 3) vahid dövlət siyasətini həyata keçirməklə informasiya təhlükəsinin proqnozlaşdırılması və qiymətləndirilməsi üzrə üsul və formaların təkmilləşdirilməsi, 4) strukturun informasiya təhlükəsizliyinin təminatı vasitələri və sistemlərinin səmərəliliyinin qiymətləndirilməsi üzrə metod və kriteriyalarının işlənilməsi, 5) informasiya təhlükəsizliyinin təminatı sahəsində bütün innovativ müəssisə və təşkilatların fəaliyyətinin əlaqələndirilməsi, 6) milli iqtisadiyyatın vacib sahələrində texnoparkların texnoloji müstəqilliyinin təmin olunması, 7) texnoparklarda informasiyanın mühfizə edilməsində müasir üsul, metodların işlənilməsi və yeni texnologiyaların tətbiqi, 8) informasiya təhlükəsizliyinin təmin olunmasında elmi-texniki və hüquqi məsələlərin həllində beynəlxalq orqanlarla və təşkilatlarla qarşılıqlı əlaqələrin genişləndirilməsi, 9) global informasiya şəbəkələri və sistemlərinin yaradılması proseslərində regional iştirakın təmini, 10) texnoparklar üçün informasiya təhlükəsizliyi və informasiya texnologiyaları sahəsində kadrların hazırlanması üzrə vahid sistemin yaradılması.

V. ELMİ-TEXNOLOJİ INNOVATİV PARKLARDA INFORMASIYA TƏHLÜKƏSİZLİYİ METODLARI

İnformasiya təhlükəsizliyinin 1) tamlıq, 2) gizlilik, 3) əlyətənlik və s. kimi komponentləri vardır [14].

Elmi-texnoloji innovativ parkların fəaliyyətində informasiya təhlükəsizliyinin təmin edilmə metodları təhlükələrin idarə olunmasına vahid yanaşmanı nəzərdə tutur. Buna baxmayaraq belə strukturların spesifik fəaliyyət sahəsi olması faktı nəzərə alınmalıdır [9-13]. Texnoparkların ümumi təhlükəsizlik metodları ilə yanaşı təhlükələrin spesifikasından asılı olaraq xüsusi metodlar və prosedurlar da tətbiq olunur.

Elmi-texnoloji innovasiya texnoparklarında informasiya təhlükəsizliyinin ümumi metodlarına aşağıdakıları aid etmək olar: 1) informasiya təhlükəsizliyi sahəsində münasibətləri tənzimləyən qanunvericiliyin təkmilləşdirilməsi; 2) istifadəçilərin icazəsiz girişinə görə məsuliyyətin müəyyənləşdirilməsi; 3) milli şəbəkələrin inkişafı prioritetinin qanunvericilik səviyyəsinin gücləndirilməsi; 4) informasiya təhlükəsizliyin təminatı sisteminin yaradılması, təkmilləşdirilməsi və idarə edilməsi; 5) informasiyanın qorunma vasitələrinin effektivliyinə nəzarət metodlarının təkmilləşdirilməsi, istifadəsi və işlənilməsi; 6) informasiya təhlükəsizliyinin təminatı sahəsində kadrların hazırlanması; 7) informasiya təhlükəsizliyinin göstəriciləri üzrə monitorinq sisteminin formalaşması; 8) informasiya təhlükəsizliyinin təminatı və onun maliyyələşdirilməsinin nizamlanması; 9) təhlükəsizlik sistemlərinin iqtisadi əsaslandırılması; 10) təhlükəsizliklə bağlı ziyanların qiymətləndirilməsi və s.

NƏTİCƏ

İnformasiya və biliklərə əsaslanan iqtisadiyyatın qurulmasında elmi-texnoloji innovasiya texnoparklarının yaradılması hazırkı dövr üçün zəruridir. Rəqəmsal və ya innovativ iqtisadiyyata keçid üçün yüksək texnologiyalar parkı, elm-texnoloji innovasiya texnoparkları əsas hərəkətverici qüvvədir. Texnoparkların informasiya sistemləri və texnologiyalarının təhlükəsizliyi problemlərinin ümumi təhlili və idarə olunması üzrə fəaliyyət planının işlənilməsi zəruridir. İnnovativ fəaliyyətin yüksək rəqabətqabiliyyətliliyi üçün həmin strukturun sosial kommersiya maraqlarına ziyan vura biləcək daxili və xarici təhlükələrdən qorunması üzrə düzgün təhlükəsizlik sistemi işlənilməli və tətbiq olunmalıdır. Hər bir innovativ texnopark strukturunun qarşısında duran təhlükəsizlik məsələsinin həlli, həm də ümumi təhlükəsizlik siyasəti çərçivəsində tənzimlənməli və koordinasiya olunmalıdır. Bununla yanaşı innovativ texnoparkların təhlükəsizlik sisteminin monitorinqi həyata keçirilməli və müntəzəm olaraq aşkarlanmış təhlükələr sistemləşdirilməli, qiymətləndirilməli və onların aradan qaldırılması üçün müvafiq tədbirlər həyata keçirilməlidir.

ƏDƏBİYYAT

- [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, www.president.az.
- [3]. Ə.Q.Əliyev, R.O.Şahverdiyeva. İnnovativ struktur və proseslərin idarə olunmasında informasiya təhlükəsizliyi məsələləri. İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, 14 may 2015-ci il, səh. 66-69.

- [4]. R.M.Alguliyev, A.G.Aliyev, R.O.Shahverdiyeva. Development of information support systems for management of innovative structures. The 8th IEEE International Conference on Application of Information and Communication Technologies (AICT2014). Kazakhstan, Astana, 15-17 october 2014, pp. 378-382.
- [5]. Ə.Q.Əliyev, R.O.Şahverdiyeva. İnformasiya iqtisadiyyatında innovasiyalar üzrə monitoring sisteminin göstəricilər bazasının işlənilməsinin konseptual əsasları. İnformasiya Cəmiyyəti Problemləri, 2014, №2, səh.50-60.
- [6]. Е.Г.Горшков. Информационная безопасность управления интеллектуально-промышленными комплексами – технопарками в Российской Федерации. Вестник ОУ. Серия «Экономика», 2007, № 2, с. 127–131.
- [7]. Massimo Felici. Economics, Security and Innovation. Economics of grids, clouds, systems, and services. Lecture notes in computer science, volume 8914, 2014, pp.3-15.
- [8]. Menggang Li. Research on industrial security theory. Basic theories of industrial security, 2013, pp.69-169.
- [9]. Н.В.Бозо. А.В.Динер. Методический подход к оценке эффективности деятельности технопарков. Вестник ТГУ, Экономика, 2016, №1(33), с. 105-115.
- [10]. Laleh Esmacil, Masoudi Yosefç Fathy Farhad, et al. Influencing Factors of Information Security Management in Small- and Medium-sized Enterprises and Organizations. 3rd International Conference on Communication Systems and Network Technologies (CSNT). India, apr. 06-08, 2013. Book Series: International Conference on Communication Systems and Network Technologies, pp. 445-449.
- [11]. Yildirim Ebru Yeniman, Akalp Gizem Aytac, Serpil et al. Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey. International journal of information management, 2011, volume 31, issue 4, pp.360-365.
- [12]. Jian Zhao, Yang Chen. An innovative structure of information security equipment for remote control. 5th International conference on Information Engineering for Mechanics and Materials (ICIMM). China, Jul. 25-26, 2015. Book Series: AER-Advances in Engineering Research, volume 21, pp.1002-1006.
- [13]. С.С.Козунова. Система управления информационной безопасностью предприятия. Евразийский Союз Ученых (ЕСУ), Технические Науки, 2016, №7(28), pp.22-23.
- [14]. В.И.Кияев, А.В.Сайтов. Комплексная информационная безопасность в управлении современным предприятием : учебное пособие, –СПб. : Изд-во СПбГЭУ, 2016, 222 с.

Key words. information and knowledge economy; scientific and technological innovation technopark; security of information systems; information provision and security; security methods.

INFORMATION SECURITY PROBLEMS OF SCIENTIFIC-TECHNOLOGICAL INNOVATION TECHNOPARKS

Shahverdiyeva O. Roza

Institute of Information Technology of ANAS,

Baku, Azerbaijan

shahverdiyev@rambler.ru

Abstract – The article is devoted to problems of information systems and technologies of scientific and technological innovation technoparks. The role, tasks and importance of innovation technoparks in the economy of information and knowledge are explained. In their management, the key elements of the modern information supply system and the factors influencing the improvement of information have been interpreted. Stages of formation of information systems, resources and technologies of technoparks are presented. The architectural-technological structure of the information security system has been developed and some recommendations have been provided for its improvement.

Botnet trafikinin aşkarlanmasının bir üsulu haqqında

Gülnarə Qarayeva

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

qarayevagulnare@mail.ru

Xülasə-- Botnet botmaster tərəfindən əmr və nəzarət zənciri vasitəsi ilə idarə olunan bot zərərverici proqramlarla yoluxmuş kompüterlər sistemidir. Botnet trafikinin normal trafikdən fərqləndirilməsi əsas problemlərdən biridir. Belə yanaşmalardan biri Netflow və IPFIX standartlarının verilənlərindən istifadə edərək botnet şəbəkə trafikinin aşkarlanmasıdır.

Açar sözlər-- botnet, əmr və nəzarət kanalı, şəbəkə axını, Netflow, maşın təlimi

I. GİRİŞ

Bu gün şəbəkə texnologiyalarının və informasiyanın təhlükəsizliyinin təmin olunması üsul və vasitələrinin yüksək səviyyədə inkişaf etməsinə paralel olaraq zərərverici proqram təminatı da sürətlə inkişaf etməkdə və yeni növləri yaranmaqdadır. Belə zərərverici proqram növlərindən biri bot zərərvericiləri və onlar əsasında qurulmuş botnetlərdir. Digər zərərli proqramlardan fərqli olaraq botnetlər istifadə olunan əmr və nəzarət (*ing. command and control, C&C*) kanalı vasitəsilə daim yenilənə bilir və aşkarlamaya qarşı daha dözümlü metodlar istifadə edirlər. Botnetlər həmçinin “ağıllı zombi ordular” da adlandırılırlar [1].

Botnetlər yarandıqları vaxtdan etibarən daim inkişaf etmiş, arxitekturaları, yayılma və əlaqə texnologiyaları, aşkarlamaya qarşı istifadə etdikləri dözümlülük metodları da kifayət qədər təkmilləşmişdir. Müasir botnetlər domen adlarının dəyişdirilməsi (*ing. domen flux*), IP ünvanların dəyişdirilməsi (*ing. IP flux*) və s. kimi DNS və şifrələmə texnologiyaları istifadə etməklə aşkarlama prosesini də çətinləşdirirlər [2]. Bütün bunlar botnetləri kibertəhlükəsizlik sisteminin əsas problemlərindən birinə çevirmişdir. Buna görə də onların daha yaxşı və hərtərəfli öyrənilməsi, bütün botnet növlərinə yönəlmiş aşkarlama üsullarının işlənməsi aktual problem olaraq qalmaqdadır.

Botnetlərin aşkarlanması üsullarının işlənməsi zamanı qarşıya çıxan əsas problemlərdən biri botnet şəbəkə trafikinin aşkarlanması üçün lazım olan axın verilənlərinin toplanmasıdır. Botnetlərin aşkarlanması üçün şəbəkə trafikinin monitorinqi aparılmalı və böyük ölçüdə verilənlər toplanmalıdır. Bu verilənlərin emalı üçün maşın təlimi (*ing. machine learning*) üsullarından istifadə edilir. Şəbəkə trafikinin monitorinqi və verilənlərin toplanması üçün istifadə olunan standartlardan biri Cisco Netflow formatıdır [3]. Netflow axın verilənləri bir çox zərərvericilərin, o cümlədən botnetlərin aşkarlanması üçün istifadə edilir və bir neçə belə aşkarlama üsulu işlənməmişdir [4].

II. ŞƏBƏKƏ TRAFİKİNİN MONİTORİNQİ

Şəbəkələrdə verilənlərin ötürülməsinə nəzarət və monitorinq üçün müxtəlif şəbəkə avadanlıq və tətbiq satıcılarının hazırladıqları standart protokollar mövcuddur. Bunlara misal olaraq Cisco Netflow (Cisco Inc, 2012), Juniper-jflow [5] (Juniper Networks Inc, 2011), Huawei-Netstream [6] (Huawei Technologies Co Ltd, 2012), Alcatel-Cflow (Alcatel-Lucent Inc.), Ericsson-Rflow (Ericsson Inc.) və s. göstərilə bilər. Şəbəkə trafikinə nəzarət və verilənlərin toplanması üçün istifadə olunan belə protokollardan ən məşhuru Netflow formatıdır. Netflow protokolu vasitəsilə şəbəkə istifadəçiləri, müxtəlif səviyyələrdə fəaliyyət göstərən şəbəkə protokolları və tətbiqləri, axın marşrutlayıcıları və s. haqqında məlumatları əldə etmək mümkündür. Hazırda istifadə olunan ən son versiyası Netflow v9 və onun eyni məqsədlə istifadə olunan digər protokollardan əsas fərqi şablon-əsaslı (*ing. template-based*) olmasıdır. Bu xüsusiyyət seçilmiş şablona görə eyni vaxtda müxtəlif tip axın məlumatlarını toplamağa imkan verir.

Netflow protokolu vasitəsilə nəzarət olunan marşrutlayıcılardan axın məlumatları toplanılır və bu informasiya Netflow axın toplayıcısında (*ing. Netflow Collector*) cəmlənir. Axın toplayıcısı bu verilənləri istifadəçi üçün daha rahat formata gətirir və təqdim edir.

Toplanmış Netflow verilənləri UDP (User Datagram Protocol) və ya SCTP (Stream Control Transmission Protocol) dəstəklili olur və aşağıdakı kimi əsas bilikləri özündə saxlayır [7, 8]:

- Netflow versiyasının nömrəsi;
- Paketin sıra nömrəsi (sequence number);
- Giriş və çıxış interfeysləri (SNMP dəstəkli);
- Axın ölçüsü və paket sayı;
- Axının başlaması və bitməsi haqqında məlumatlar;
- 3-cü səviyyə paket başlıqları (mənbə və hədəf IP ünvanlar və portlar, IP protokolu, xidmətin tipi və s.);
- 3-cü səviyyə marşrutlama məlumatları.

Netflow protokolu vasitəsilə toplanmış şəbəkə axın bilikləri bir çox zərərli proqramların, o cümlədən botnet şəbəkə trafikinin aşkarlanması üçün lazım olan bütün

verilənləri özündə saxlayır. Xüsusilə, IETF (Internet Engineering Task Force) tərəfindən standartlaşdırılmış Netflow v9 digər versiyalardan şablon-əsaslı olması ilə fərqlənir. Şablonlar axın verilənlərinin formatını genişləndirməyə və baza axın formatını dəyişmədən paralel olaraq bir neçə şablona görə verilənləri toplamağa imkan verir.

III. BOTNET TRAFİKİNİN AŞKARLANMASI

Bütün əvvəlcədən proqramlanmış sistemlərdə olduğu kimi botnetlər də fəaliyyət göstərdikləri müddətdə dövrü olaraq avtomatik alqoritmləri icra edirlər. Buna görə də botmasterlər fəaliyyətlərini təsadüfləşdirmək üçün maksimum enerji sərf edirlər. Aparılan araşdırmalar göstərir ki, botnetləri aşkarlamaq üçün hələ də onları bir neçə standart sinifdə qruplaşdırmaq olar:

- IRC, HTTP və DNS-əsaslı botnetlərin əsas xarakteristik xüsusiyyəti C&C təlimatlar və botların bu təlimatlara necə cavab verməsidir.

- SpyEye [9] və Zeus botnetinin bir neçə versiyası botların aşkarlanması üçün siqnaturaların yaradılmasında istifadə oluna biləcək unikal axın davranışlarına malikdir.

- P2P botnetlərdə sorğu və təlimat kimi əlaqələr digər qanuni P2P əlaqələrdə olduğu kimi çox kiçik ölçüdə paketlərlə həyata keçirilir. Paketlərin ilkin mübadiləsinin vahid formatı var, bu da qanuni trafikdən asanlıqla fərqlənir.

İstənilən sinif botnetlərin aşkarlanmasında istifadə olunan əsas əlamətlər və xüsusi sinif botları aşkarlamaq üçün istifadə olunan xüsusi əlamətlər vardır. Mənbə və hədəf ünvanlar və portlar istənilən sinif botnetlərin aşkarlanması üçün ümumi xüsusiyyətlərdir. Netflow v9 verilənlərinin istifadə edilməsinin əsas üstünlüklərindən biri də ümumi obrazı dəyişmədən xüsusi sinif botları aşkarlayan obrazların qurula bilməsidir. Bu standart 3-cü səviyyədə fəaliyyət göstərən bütün tip qurğuları (switch və marşrutlayıcıları) dəstəkləyə bilir. Netflow verilənləri əsasında botnet trafikinin aşkarlanması üçün aşağıdakı kimi mərhələlərdən ibarət üsul təklif edilir.

Şəkil 1. Botnet şəbəkə trafikinin aşkarlanması modeli

A. Trafik axınının toplanması

Bot trafikinin aşkarlanması üçün üsulun işlənməsi zamanı əsas problemlərdən biri lazımi verilənlərin əldə olunmasıdır. Düzgün verilənlərin seçilməsi üsulun effektivliyinin

artırılması üçün vacib amillərdən biridir. Belə biliklərin əldə edilməsi üçün birinci mərhələdə Netflow axın verilənlərinin toplanması həyata keçirilir. Bu məqsədlə xüsusi virtual test şəbəkəsi yaradılaraq axın məlumatları toplanılır. Botnet aşkarlamanın keyfiyyətini artırmaq üçün bir neçə maşın xüsusi bot proqramlarla yoluxdurulur, C&C server yaradılır və süni bot şəbəkəsi qurulur [10].

Ümumi şablonlar şəbəkə trafik axınının toplanması üçün istifadə olunur. IPv4 və IPv6 axın verilənlərinin hər ikisi paralel olaraq toplanıla bilər. Axın mənbə və hədəf IP ünvan, mənbə və hədəf port, xidmət növü, IP protokol və interfeys kimi atributları saxlayan paketlər şəklində təyin olunur. Bu atributlar qəbul edilən paketin mövcud və ya yeni axına aid olduğunu müəyyənləşdirməyə imkan verir. Aşkarlamanın dəqiqliyinin yoxlanılması üçün daha çox biliklərin toplanması əhəmiyyətlidir. Lakin atributların sayı artdıqca verilənlər bazasının ölçüsü də böyüyür. Bu problemi həll etmək üçün dəyişkən sahə ölçülərindən istifadə olunur [11].

Axın toplayıcı müxtəlif qurğular tərəfindən yaradılan trafik axın verilənlərini saxlamaq üçün istifadə olunur. Burada xüsusi proqram təminatı vasitəsilə axın verilənləri nizamlanır və istifadəçi üçün uyğun formatda təqdim olunur. Verilənlər trafikinin tipinə, istiqamətinə, il, ay, vaxt və tarixə görə qovluqlarda saxlanıla bilər. Axın toplayıcı da verilənlərin sıxlaşdırılması, axtarılması və s. funksiyaları yerinə yetirir, lazımsız axının aradan qaldırılması və botnetlərin aşkarlanması alətlərinin istifadəsini yaxşılaşdırır.

B. Verilənlərin ilkin emalı

Süzgəcləmə prosesinin əsas məqsədi verilənlər bazasının ölçüsünü botnet trafiki ilə əlaqəsi olmayan axını ayırmaqla azaltmaqdır. Bu prosesin özü bir neçə mərhələdə aparılır və maşın təlimi üsullarından istifadə olunur. İlk addımda TCP və UDP protokollu axın seçilir. Bu onunla əlaqədardır ki, bir çox botnet sinifləri C&C əlaqə kanalı yaratmaq üçün məhz qanuni DNS trafikinə oxşar trafikdən istifadə edirlər.

Botnetlər status yoxlama, kodların yenilənməsi, əməllərin verilməsi və s. əlaqələrdə adətən kiçik ölçülü paketlərdən istifadə edirlər. Halbuki, proqram təminatının yenilənməsi və qanuni P2P ötürmələr kifayət qədər böyük ölçülü axın yaradır. Bunu nəzərə alaraq böyük ölçülü verilənlər süzgəclənir. Bu zaman paketlərin ölçüsü və sayı qəbul edilmiş həddən böyük olan axın verilənləri bazadan çıxarılır.

C. Bot trafikinin aşkarlanması

Botnetlərin aşkarlanması zamanı əsasən 3 tip davranışlar araşdırılır: bot davranışları, botnet davranışları və müvəqqəti davranışlar. Bot davranışları dedikdə, yalnız bir botun C&C əlaqələri və ya hücum cəhdləri araşdırılır. Botnet davranışları dedikdə, qrup şəklində botlar tərəfindən yaradılan axın müəyyənləşdirilir. Müvəqqəti davranışlar isə hər hansı vaxt ərzində bot və ya botlar tərəfindən yaradılan trafikə analiz nəticəsində aşkarlanır.

IRC, HTTP, P2P və hybrid botnetlərin araşdırılması nəticəsində məlum olmuşdur ki, bütün botnet sinifləri fəaliyyətləri dövrünün müxtəlif fazalarında müxtəlif davranış xüsusiyyətlərinə malikdirlər. [12] İlkin yoluxma fazasında botmasterlər yoluxdurulacaq qurğuların boşluqları yoxlayır və bu işi bütün fəaliyyət dövründə vaxtaşırı təkrarlayır. Mərkəzləşmiş arxitektura bu birbaşa bot-server tərəfindən həyata keçirilirdisə, P2P botnetlər üçün botlar arasında yayılma vasitəsilə mümkün olur. Botlar daim yeni “qurbanlar” üçün axtarış edir, kiçik ölçülü paketlərdən istifadə etməklə botnetin ölçüsünü genişləndirməyə çalışırlar.

Təkrar yoluxma fazasında yoluxmuş qurğunun idarəsini tamamilə ələ keçirmək üçün zərərli proqramlar yüklənir və bot öz C&C serveri ilə botnetə üzv olmaq üçün əlaqə saxlayır. Əlaqə və yeniləmə fazalarında bot, serverdən gələcək hücum və ya digər zərərli fəaliyyətlərin koordinatlarını gözləyir, onları yerinə yetirir, yeni qurğuların yoluxdurulması ilə məşğul olur, aşkarlama və neytrallaşdırma cəhdlərinə qarşı dözümlülüyü artırmaq üçün botmasterlər tərəfindən bot zərərvericiləri yenilənir.

Birbaşa C&C əlaqəli IRC və HTTP botnetlərdə botlar bot-serverlə, P2P və hibrid arxitektura isə öz *proxy* botları ilə əlaqə saxlamağa çalışırlar. Aşkarlamadan yayınmaq və DNS və ya IP ünvanlarını gizlətmək üçün C&C serverlər öz əlaqələrində domen flux, IP flux kimi texnologiyalardan istifadə edirlər. Həmçinin bəzi botnetlər zərərli tapşırığın yerinə yetirilməsi haqqında daim hesabat verirlər. Məsələn, Zeus botnetində hər 20 dəqiqədən bir botlar avtomatik yoxlanılır və yenilənir.

Botnetlər zərərli fəaliyyətlərin növündən asılı olaraq da müxtəlif davranış xüsusiyyətlərinə malik olurlar. DDoS hücumları zamanı şəbəkədə naməlum ünvanlara yönəlmiş TCP Syn paketlərin aktivliyi müşahidə olunur, bu da obrazın qurulması zamanı onların sayının nəzərə alınmasını tələb edir. Spam e-mail göndərilməsi zamanı isə xarici mail serverlər istifadə edilərək böyük ölçüdə məktublar göndərilir. Belə ki, şəbəkədə qeyri-adi SMTP aktivlik botların aşkarlanması üçün əsas ola bilər.

Bütün bu davranış xüsusiyyətləri botnetlərin aşkarlanması üçün obrazların qurulmasında aparıcı rol oynayır [13]. Botnetin bütün fəaliyyəti dövründə, müxtəlif davranış əlamətlərinə görə ümumi obrazın qurulması üçün məşin təlimi üsullarından istifadə olunur. Müxtəlif məşin təlimi üsullarının tətbiqi nəticəsində məlum olmuşdur ki, botnetlərin növündən və fəaliyyət məqsədindən asılı olaraq tətbiq olunan üsul da dəyişir. Məsələn, qərar ağacları (*ing. Decision Tree*) klasifikatoru P2P botnetlərin aşkarlanması üçün axın intervallarına görə, SVM və Bayes şəbəkələri HTTP və IRC əsaslı mərkəzləşmiş botnetlərdə C&C əlaqələri aşkarlamaqda daha effektiv nəticə əldə etməyə imkan verir.

IV. EKSPERİMENTLƏRİN NƏTİCƏLƏRİ

Eksperimentlərin aparılması üçün CTU-13 verilənlər bazasından 7-ci ssenari üzrə toplanmış verilənlər seçilmişdir. CTU-13 verilənlər bazası 2011-ci ildə Çexiya Texniki Universitetində (*ing. Czech Technical University, CTU*) botnet, normal və arxa fon trafikinin birlikdə ssenari adlanan 13 bazada toplanması ilə yaradılmışdır. Hər bir ssenari üzrə xüsusi protokol istifadə etməklə xüsusi zərərli fəaliyyətlər həyata keçirən müxtəlif bot proqramlarından istifadə olunmuşdur.

Hər ssenari üç tip trafik paketlərindən ibarət olub nişanlanmış və *.pcap* fayllarda toplanmışdır. Axınlar biristiqamətli və ikiistiqamətli NetFlow şəbəkə verilənlərindən ibarətdir. İkiistiqamətli verilənlərin istifadəsi bir çox səbəbdən daha məqsəduyğundur. Çünki, klient və serverləri fərqləndirir, axın haqqında daha çox informasiya saxlayır və daha detallı sinifləndirmə aparmağa imkan verir.

CTU-13 verilənlər bazasının fərqləndirici xüsusiyyətlərindən biri də bütün ssenarilər üzrə bazaların əllə analiz olunması və nişanlanmasıdır. Nişanlanma prosesi NetFlow fayllarının daxilində aparılmışdır və hər bir ssenari Arxa fon, Botnet, C&C kanal və Normal trafik olaraq adlandırılmışdır [14].

Bazadakı hər bir ssenari müxtəlif formatlı fayllar şəklində işlənmişdir, lakin gizlilik problemləri baxımından bütün verilənləri özündə saxlayan *pcap* faylı yoxdur. Buna baxmayaraq digər fayllar əlçatandır və aşağıdakı kimi tərkibə malikdir:

- *.pcap* genişlənməli yalnız botnet axından ibarət fayl;
- ikiistiqamətli *.biargus* genişlənməli bütün tip axın verilənlərini özündə saxlayan NetFlow faylları;
- orijinal icra oluna bilən fayl.

Nişanlanmış NetFlow verilənlər faylı bir çox axın əlamətləri ilə xarakterizə olunur (cədvəl 1).

CƏDVƏL 1. NETFLOW AXIN ƏLAMƏTLƏRİ

Say	Əlamətin adı	Əlamətin izahatı
1	StartTime-EndTime	Axının başlama və bitmə vaxtı (tarix, vaxt)
2	Duration	Axının davam etmə müddəti (mksan)
3	Protocol	İstifadə olunmuş protokol (tcp, udp, icmp və s.)
4	Source IP Address	Mənbə IP ünvan
5	Source port	Mənbə port
6	Direction	Axın istiqaməti (<->, <->, ->)
7	Destination IP Address	Çatdırılma IP ünvan
8	Destination port	Çatdırılma port
9	State	Axın statusu (CON, FSPA və s.)
10	Source ToS	Mənbə xidmət tipi (0,1)
11	Destination ToS	Çatdırılma xidmət tipi (0,1)
12	Total Packets	Axın tərkibindəki paketlərin sayı
13	Total Bytes	Axın tərkibindəki baytların sayı
14	Source Bytes	Mənbədən çatdırılma ünvanına kimi

“İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri”
IV respublika konfransı, 14 dekabr 2018-ci il

		baytların sayı
15	Label	Sınıf (Background, Normal, Botnet və s.)

7-ci ssenari üzrə verilənlər 22 dəqiqə ərzində toplanmış və ümumi ölçüsü 5.8 Gb-dır. Verilənlərin ilkin emalı mərhələsində TCP və UDP protokollu axınlardan başqa digər protokol axınları filtrlənmişdir. Eksperimentlər üçün bazadan 65 botnet və 65 normal axın verilənləri seçilmişdir. IP ünvan verilənləri kodlanmış və onluq formata çevrilmişdir. Analizlər nəticəsində məlum olmuşdur ki, bazadakı əlamətlər daha yaxşı sınıflandırma aparmaq üçün kifayət etmir. Daha yaxşı nəticələrin əldə edilməsi üçün iki yeni əlamət çıxarılmışdır: nisbi paket faizi və nisbi bayt faizi. Nisbi paket faizi axındakı paketlərin ümumi sayının (*Total Packets*), axının davamətmə müddətinə (*Duration*) nisbəti kimi təyin edilir və müxtəlif zaman intervallarında ötürülən paketlərin orta qiymətini müəyyən etməyə imkan verir.

$$\text{Nisbi paket faizi} = \text{Total Packets} / \text{Duration}$$

Nisbi bayt faizi isə ötürülən axındakı baytların ümumi miqdarının, axının davamətmə müddətinə nisbəti kimi hesablanır.

$$\text{Nisbi bayt faizi} = \text{Total Bytes} / \text{Duration}$$

BayesNet (Bayes şəbəkələri), NaiveBayes, SVM (Dəstək vektor maşınları), Random Tree (Təsadüfi ağaclar) və Random Forest (Təsadüfi meşələr) maşın təlimi üsullarının tətbiqi ilə aparılan təcrübələrin nəticələri aşağıdakı cədvəldə göstərilmişdir (cədvəl 2). Üsulların qiymətləndirilməsi üçün üç meyar (Recall, Precision, F-Measure) istifadə olunmuşdur.

Cədvəl 2. Klassifikatorların müqayisəsi

Qiymətləndirmə meyarları	Klassifikatorlar				
	BN	NB	SVM	RT	RF
Recall (%)	100	98,5	99,2	93,1	100
Precision (%)	100	98,5	99,2	93,2	100
F-measure (%)	100	98,5	99,2	93,1	100

Recall (tamlıq) klassifikatorun müsbət sinfin bütün obyektlərindən hansı hissəsini tapdığını göstərir:

$$\text{Recall} = \frac{TP}{TP + FN}$$

Precision (dəqiqlik) – klassifikatorun müsbət adlandırdığı və həqiqətən də müsbət olan obyektlərin nisbi sayıdır:

$$\text{Precision} = \frac{TP}{TP + FP}$$

F-measure (F-ölçü) dəqiqlik və tamlığın harmonik ortasıdır:

$$F - \text{measure} = 2 \frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}}$$

Burada, TP – doğru klassifikasiya olunan müsbətlərin sayı, TN – doğru klassifikasiya olunan mənfilərin sayı, FP – səhv klassifikasiya olunan müsbətlərin sayı, FN – səhv klassifikasiya olunan mənfilərin sayıdır.

NƏTİCƏ

Aparılan araşdırmalar belə qənaətə gəlməyə imkan verir ki, bot şəbəkələr fəaliyyəti dövrlərinin bütün fazalarında, istifadə etdikləri əlaqə və nəzarət kanalının tipinə, həyata keçirdikləri zərərli fəaliyyətin növünə və s. görə müxtəlif davranış xüsusiyyətlərinə malik olurlar. Botnet davranış əlamətlərindən istifadə etməklə, Netflow axın verilənlərinin və maşın təlimi üsullarının tətbiqi ilə daha effektiv aşkarlama üsullarının işlənməsi mümkündür. Məqalədə belə bir üsulun ümumi modeli verilmişdir.

ƏDƏBİYYAT

- [1] Y.N. İmamverdiyev, G.B. Qarayeva, “Botnetlər və onların aşkarlanması üsulları,” *İnformasiya texnologiyaları problemləri*, №1, s. 100–111, 2017.
- [2] R. Sharifnya, M. Abadi, “DFBotKiller: Domain-flux botnet detection based on the history of group activities and failures in DNS traffic,” *Digital Investigation*, Vol. 12, pp. 15–26, March 2015.
- [3] Cisco Inc 2012, Introduction to Cisco IOS® NetFlow, <http://www.cisco.com/c/en/us/products/collateral/ios-nx-ossoftware/ios-netflow/prod_white_paper>.
- [4] J. Francois, S. Wang, R. State, & T. Engel, “BotTrack: Tracking Botnets Using NetFlow and PageRank,” 2011.
- [5] Juniper Flow Monitoring, J-Flow on J Series Services Routers and Branch SRX Series Services Gateways, www.juniper.net/us/en/local/pdf/app-notes/3500204-en.pdf
- [6] NetStream (Integrated) Technology White Paper, Huawei Technologies Co., Ltd., 2012.
- [7] D. Zhao, I. Traore, B. Sayed, W. Lu, S. Saad, A. Ghorbani, & D. Garant, “Botnet detection based on traffic behavior analysis and flow intervals,” *Computers & Security*, vol. 39, Part A, no. 0, pp. 2–16, 2013.
- [8] W.T. Strayer, D. Lapsley, R. Walsh, & C. Livadas, “Botnet Detection Based on Network Behavior,” W Lee, C Wang & D Dagon (eds), *Botnet Detection*, Springer US, vol. 36, pp. 1–24, 2008.
- [9] A.K. Sood, R.J. Enbody, & R. Bansal, “Dissecting SpyEye – Understanding the design of third generation botnets,” *Computer Networks*, vol. 57, no.2, pp. 436–50, 2013.
- [10] U. Wijesinghe, U. Tupakula, V. Varadharajan, “An enhanced model for network flow based botnet detection,” *Proceedings of the 38th Australasian Computer Science Conference*, 2015.
- [11] C. Livadas, R. Walsh, D. Lapsley, W. T. Strayer, “Using Machine Learning Techniques to Identify Botnet Traffic,” *Internetwork Research Department*, BBN Technologies.
- [12] D. Andriess, C. Rossow, B. Stone-Gross, D. Plohmann, & H. Bos, 2013, “Highly resilient peer-to-peer botnets are here: An analysis of Gameover Zeus,” 8th International Conference on Malicious and Unwanted Software, pp. 116–123, 22–24 Oct. 2013.
- [13] Tarnag, W., Den L-Z, Ou K-L & Chen M. “The analysis and identification of P2P botnet’s traffic flows”, *International Journal of*

Communication Networks and Information Security (IICNIS), vol. 3, no. 2, pp. 138-148, 2011.

[14] P.Kalaivani, M.S.Vijaya. Mining Based Detection of botnet traffic in Network Flow. IRACST - International Journal of Computer Science and Information Technology & Security (IJSITS), Vol. 6, No 1, pp. 535-541, Jan-Feb 2016.

**ABOUT ONE METHOD OF BOTNET TRAFFIC
DETECTION**

Gulnara Garayeva
Institute of Information Technology of ANAS,
Baku, Azerbaijan

garayevagulnare@mail.ru

Abstract - Botnet is a system of infected computers controlled with the command and control chain by botmaster. One of the main problems is to distinguish between botnet traffic and normal traffic. One such approach is to detect botnet network traffic using Netflow and IPFIX standards.

Keywords- botnet, command and control channel, network flow, Netflow, machine learning

Vətəndaş elminin informasiya təhlükəsizliyi haqqında

Təhmasib Fətəliyev¹, Nərgiz Verdiyeva²

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

depart3@iit.science.az

Xülasə— Çoxlu sayda könüllünün geniş məkan və zaman kateqoriyalı kəmiyyət ölçmələri və müşahidələrdə iştirakı ilə xarakterizə olunan vətəndaş elmi informasiya texnologiyalarının tətbiqi ilə sürətlə inkişaf edir. Məqalə onun səmərəli fəaliyyətini təmin etmək məqsədi ilə informasiya təhlükəsizliyi məsələlərinin tədqiqinə həsr olunmuşdur. İnformasiya təhlükəsizliyinin konfidensiallıq, tamlıq, əlyetənlik və fərdi məlumatların qorunması kimi məsələləri araşdırılmış, vətəndaş elminin effektiv mühafizəsi üçün prioritet istiqamətlər göstərilmişdir.

Açar sözlər— e-elm; vətəndaş elmi; açıq elm; informasiya təhlükəsizliyi; vətəndaş elmi layihələri.

I. GİRİŞ

İnformasiya texnologiyalarının (İT) geniş tətbiqi nəticəsində informasiyanın toplanması, saxlanması, emalı və paylanması məsələlərini son dərəcədə inkişaf etdirmiş və insan fəaliyyətinin bütün sahələrini, xüsusən də elmi-tədqiqatları dəyişmişdir. Bu nailiyyətlərin əldə olunmasında nəzəriyyə və praktika ilə yanaşı elm üçün üçüncü bir əsas alətə çevrilmiş və onun həyata keçirilməsinin yeni yollarını yaratmış e-elm mühüm rol oynayır [1]. Onun inkişafı nəticəsində yeni bir istiqamət olaraq vətəndaş elmi (VE) formalaşır, eyni zamanda elmi fəaliyyətdə açıqlıq və şəffaflıq prinsiplərini ifadə edən “Açıq elm” konsepsiyası da getdikcə reallaşır. İT-nin sürətli inkişafı və geniş tətbiqi ilə əldə olunmuş bu yeniliklərin səmərəli fəaliyyətinin təşkilində informasiya təhlükəsizliyinin təmin edilməsi mühüm əhəmiyyətə malikdir.

Təqdim edilən işdə VE-nin formalaşması və inkişafında informasiya təhlükəsizliyi problemləri araşdırılmış və onların həllinin konseptual məsələləri işlənmişdir.

II. VƏTƏNDAŞ ELMİNDƏ TƏHLÜKƏSİZLİYİN MÖVCUD VƏZİYYƏTİ

E-elmin inkişafının yeni bir istiqaməti kimi formalaşan VE-ni xarakterizə edən cəhətlər geniş məkan və zaman kateqoriyalı kəmiyyət ölçmələri və müşahidələr, böyük həcmli verilənlərin toplanması, məlumatların toplanmasında açıq təbii şəraitdə çoxlu sayda könüllünün iştirakı, maliyyələşmənin olmaması, verilənlərin onlayn toplanması, tədqiqatların aparılmasına dəstək üçün yaxşı işlənmiş mexanizmlərin, yardımçı materialların və professional köməyin təqdim olunması və s.-dir. VE sahəsində layihələrin yüz ildən artıq fəaliyyət göstərməsinə baxmayaraq, son zamanlar onların sayı kəskin artmağa başlamışdır. Bu inkişaf VE-nin həyata keçirilməsində müasir texniki və proqram vasitələrinin təyinatlı tətbiqi ilə izah olunur [2]. Müasir İT elmi tədqiqatlarda verilənlərin

toplanmasının miqyasının artmasında, informasiyanın çatdırılmasında, ideyaların ötürülməsində, iştirakçıların prosesə cəlb edilməsi üsullarında, verilənlərin emalında, vizuallaşdırmada interaktiv iştirak üçün geniş imkanlar spektri yaratmışdır. Xüsusən də mobil Internetin və sensorların istifadəsi ilə verilənlərin kütləvi toplanması imkanını təmin edir. Bundan başqa, texnoloji nailiyyətlər vətəndaş elmi haqqında verilənləri daha əlçatan edir və vətəndaş alimlərə verilənlərin toplanmasından əlavə imkanlar verərək verilənlərin vizuallaşması və təhlili üçün alətlər təklif edir. Beləliklə, bütün bu texnoloji vasitələrin tətbiqi VE-nin inkişafında mühüm rol oynayır. Daha geniş auditoriyanı əhatə edərək, VE geniş ictimaiyyətə yeni biliklər əldə etməyin asan yolunu təqdim edir. Lakin hər bir sahədə olduğu kimi, VE-də də iştirakçılar üçün bir sıra təhlükə və təhdidlər mövcud ola bilər.

Vətəndaş alim və praktikalrın global cəmiyyətini formalaşdırmaq məqsədi ilə müxtəlif beynəlxalq təşkilatlar vardır. Onlar fəaliyyətləri ilə VE-nin inkişafına kommunikasiya, koordinasiya və təhsil vasitəsi ilə dəstək verir. Məsələn, Avropa Vətəndaş Elmi Assosiasiyasının (AVEA) məqsədi VE-nin inkişafını, xüsusilə, Avropa Birliyi ərazisində ətraf mühitin monitorinqində tətbiqini görməkdir [3]. AVEA VE-də informasiya təhlükəsizliyi məsələlərinin həllində maraqlıdır. Onun təşəbbüsü ilə bəyan edilmiş “VE-nin 10 prinsipi”nin 7 və 10-cu bəndində təhlükəsizlə əlaqəli məqamlara toxunulmuşdur:

- Mümkün və uyğun olduqda, VE layihələrinin verilənləri və meta-verilənləri ictimaiyyətə açıqdır və nəticələr açıq əlyetənlik formatında nəşr olunur. Verilənlərin paylaşılması, əgər təhlükəsizlik və gizlilik problemləri yoxdursa, layihə zamanı və ya ondan sonra həyata keçirilə bilər.
- VE layihələrinin liderləri müəllif hüququ, intellektual mülkiyyət, informasiya mübadiləsi haqqında razılıq (müqavilə), konfidensiallıq, məsuliyyət, ətraf mühitə təsir ilə əlaqədar hüquqi və etik aspektləri nəzərə alır.

VE onlayn mühitlər vasitəsi ilə elmdə vətəndaşların iştirakı və qarşılıqlı elmi əməkdaşlığı nəticəsində formalaşır. VE təşəbbüslərinin sayında sürətli artımla yanaşı onun əhatə dairəsinin genişlənməsi də müşahidə olunur. Məsələn, təkcə “Birgə edə biləcəyimiz elm” şüarını əsas götürmüş SciStarter təşkilatının (<https://scistarter.com>) verilənlər bazasında 1600-dən çox vətəndaş elmi layihəsi və 100 000 həvəskar qeydiyyatdan keçmişdir.

Hər gün milyonlarla vətəndaş alim dünyanın hazırkı hədəflərini dəstəkləmək üçün müxtəlif tədqiqatlarda iştirak edir [4]. eBird könüllüləri təbiətdə quşların müşahidələrinə töhfə verirlər ki, bu da torpağın mühafizəsi siyasətindən xəbər verən bir amil olaraq çıxış edir (<http://ebird.org>). FoldIt iştirakçıları HIV-in reproduksiyası üçün mühüm olan proteini müəyyən etməyə kömək edirlər (<http://fold.it>).

Dünyada VE layihələrinin sayının artım dinamikası olduqca böyükdür, bu fakt CitSci.org portalın timsalında öz təsdiqini tapır. Hazırda sayta qoşulan könüllü koordinatorlar yaratdıqları 693 layihə üzrə lokal, regional və/və ya global problemlərin həlli üçün ümumilikdə 936 102 ölçmə (analiz üçün verilənlər) təqdim ediblər.

Beləliklə, çoxlu sayda könüllünün geniş məkan və zaman kateqoriyalı kəmiyyət ölçmələri və müşahidələrdə iştirakı ilə xarakterizə olunan VE-də təhlükəsizlik problemlərinin həlli müərkəb və aktual məsələ kimi təsdiqini tapır.

Məlumdur ki, fərdi iştirakçıların gizliliyi və təhlükəsizliyini təmin etmək üçün ənənəvi elmi-tədqiqat fəaliyyətinin təşkilində məlumatlı razılıq kimi yaxşı düşünülmüş qaydalardan istifadə olunur. Buna əks olaraq, VE layihələri cəmiyyət üzvləri tərəfindən yaradılır və onlar misal olaraq, havanın çirklənməsi, yaşayış mühitinin itirilməsi kimi ümumi problemlər üzrə birləşirlər. Bu layihələr ictimaiyyətin üzvləri tərəfindən əldə edilmiş verilənlərdən istifadə edir. Bunun nəticəsi olaraq, VE təcrübələrini və onları dəstəkləyən texnologiyalar layihələndirilərkən gizlilik nəzərə alınmamış ola bilər. Lakin bu hallarda, elmi-tədqiqat üçün olduğu kimi, iştirakçı gizliliyinin qorunması mühüm problem olmalıdır.

Vətəndaşların iştirak etdiyi onlayn VE layihəsində iştirakçılar qeydiyyatdan keçməklə apardığı müşahidələrin nəticələrini layihənin veb-saytında yerləşdirirlər. Bu layihələrin böyük bir qismi təbiət və ətraf mühitlə bağlı olduğundan müşahidə nəticələri çəkilmiş şəkillər, videolar olacaq. Layihənin veb-saytında isə açıq əlyetənlik siyasəti qüvvədədir, ona görə də bütün verilənlər hamıya açıqdır. Bu layihələr iştirakçılar haqqında şəxsi informasiyanın veb-saytda hamıya açıq ola bilməsindən narahatdır. Bundan əlavə, yüklənilmiş şəkillərdə üzdən tanına bilən insanlar və onların harada, kimlə olduqları təsvir oluna bilər. Bu cür, xüsusilə də uşaqlar təsvir olunan şəkillər müvafiq icazə olmadan paylaşıldıqda layihə problem yaşaya bilər.

Şəkillərin çəkildiyi yer açıq paylaşıldığından iştirakçıların evləri, məktəbləri, iş yerlərinin yerləşdiyi əraziləri tanına bilinməsinə təhlükəsizlik baxımından nəzərə alınmalıdır. Bu, pis niyyətli şəxslərin hamının iştirakçıları tapa bilməsi, onların mənsəbiyyətləri barədə şəxsi məlumatları aşkarlaması təhlükəsini yaradır. Layihə tədris məqsədli olarsa, o həm də az yaşlı uşaqların məsuliyyətli şəxs tərəfindən nəzarətdə olmasını təmin etməlidir.

Göstərdiyimiz nümunə ilə bağlı təhlükəsizlik problemləri – şəxsi informasiyanın konfidensiallığı, təqib və təcavüz, fərdi məxfiliyin qorunması ilə əlaqədar vətəndaş azadlıqları realdır. Təhlükəsizliyi “könüllü olaraq göndərilmiş şəxsi məlumatlara giriş imkanı hüququ” kimi təyin etmək olar. Şəxsi məlumatlar dedikdə şəxsiyyəti müəyyənləşdirən məlumatlar (personally identifiable information, PII) nəzərdə tutulur. Office of Management and Budget tərəfindən müəyyən olunmuşdur ki,

PII-ə fərdi identifikasiya edə bilən informasiya (ad və soyad kimi) və fərdlə əlaqəli informasiya (tibbi məlumatlar və ya IP ünvan) daxildir. Həmçinin könüllülərin müraciətlərində qeyd olunmuş şəxsi məlumatlar hesab olunur. Məsələn, coğrafi məkanın qeyd olunduğu müşahidələr tədqiq olunan nümunələrin və eyni zamanda onu qeydə alan könüllünün yerləşdiyi məkanı aşkar edir:

- VE layihələri könüllüləri potensial təhlükə və təhlükəsizlik tədbirlərinin həyata keçirilməsi barədə məlumatlandırmaqla onların gizliliyini mühafizə etməlidir.
- Gizlilik qanunları, siyasəti və standartları VE tətbiqlərini işləyib hazırlayanları daha yaxşı təcrübələrə doğru təlimatlandırmaq üçün mövcuddur.

Bu misallar vasitəsilə VE-də iştirakçıların gizliliyini mühafizə edən hüquqi və siyasət mülahizələrini araşdırmaq mümkündür. Ümumiyyətlə, layihələr hüquq və etik standartları təşkilati təcrübələrlə əlaqələndirən siyasəti inkişaf etdirə bilər. Bu siyasət istifadəçilərə məlumatlı qərarlar qəbul etməyə imkan yaratmaqla gizliliyi dəstəkləyir. Digər hallarda, həllər istifadəçiləri mühafizə edən avtomatlaşdırılmış proseslərlə birlikdə texnologiyalara çevrilir.

Uşaqların Onlayn Gizliliyinin Qorunması Qanunu (Children's Online Privacy Protection Act – COPPA) 13 yaşdan aşağı hər kəsin şəxsi informasiyasının toplanılmasını məhdudlaşdırır [5]. Bu qanun Project BudBurst (www.budburst.org) və iNaturalist (www.inaturalist.org) də daxil olmaqla bir çox VE layihələrinə tətbiq olunur. COPPA-ya əsasən, veb-saytın ana səhifəsi və şəxsi informasiyanın toplanıldığı hər bir səhifə hansı verilənlərin və necə toplanılması, bu verilənlərin necə istifadə olunması, verilənlərə məsuliyyət daşıyan şəxslə əlaqə informasiyası, yetkinlik yaşına çatmayanların valideyn hüquqlarını izah edən verilənlər siyasətinə keçid (link) qeyd olunmalıdır. Project BudBurst layihəsi “Verilənlər siyasəti” səhifəsinə keçid təmin etməklə COPPA ilə uyğunlaşır. Əlavə olaraq, Project BudBurst layihəsinə qoşulan könüllülərdən “Mənim ən azı 13 yaşım var” düyməsini basmaq tələb olunur. Könüllülərə məlumat verilir ki, “əgər sizin yaşıңыз 13-dən azdırsa, o zaman yerinizə valideyniniz və ya müəlliminiz qeydiyyatdan keçsin”. Bu düymə basılmadıqda qeydiyyat təsdiqlənmir. Beləliklə, Project BudBurst layihəsi COPPA-ya uyğunlaşmaq üçün həm siyasət, həm də texnoloji həlləri təmin edir.

Layihələrdə iştirak edən vətəndaşlar şəxsi mesajlar vasitəsilə də əlaqə saxlaya bilər. Bəzi layihələr çərçivəsində, məsələn, iNaturalist-də şəxsi mesajların məzmununa nəzarət olunması mümkün olmur. Ona görə də bu cür layihələr iştirakçılara əvvəlcədən yaş məhdudiyyəti qoyur.

VE layihələrinin həyata keçirilməsi üçün onlayn alətlər və resurslar təmin edən CitSci.org portalına nəzər salaıq. Saytın Features bölməsində “Make your data public or keep it private” başlığının olması burada hər bir layihə yaradıldığı zaman gizliliyin seçilməsinə imkan verir. Bəzi hallarda açıq yaradılan VE layihəsində toplanılan müəyyən məlumatları gizli saxlamaq lazım gəlir. Bu halda verilənlər üçün gizliliyin tənziqlənməsi həyata keçirilir. Portalda hazırda bu funksiya bir qədər məhduddur: ya bütün verilənlər gizli, ya da hamısı açıq ola bilər, lakin gələcəkdə yalnız seçilən verilənlərin gizli və ya açıq

paylaşılmasını mümkün edən daha geniş seçimlər üzərində işlər aparılır.

Digər problemlər VE müşahidələri haqqında sənədləşdirilməli olan informasiyanın gizliliyi, təhlükəsizliyi və buna aid icazələrlə bağlıdır [6]. Layihə koordinatorları və könüllü iştirakçılar kimin nəyi, harada və nə zaman məlumat verməsi aspektlərindən hansılarının paylaşılmalı biləcəyi, hansılarının isə gizli saxlanılmalı olduğu barədə qərar verməyi bacarmalıdır. Koordinatorlar elmdə uyğun sənədləşdirmənin vacibliyini tanımaqla verilənləri təqdim edən könüllülərin təhlükəsizlik barədə narahatlıqlarını başa düşməli və buna hörmətlə yanaşmalıdırlar. Məsələn, bəzi hallarda verilənləri toplayan şəxs anonim qalmaq, digər bir vəziyyətdə isə o, müəllifliyin bildirilməsini istəyə bilər. Narahatlıq doğuran ərazilərdə toplanılmış verilənlər bəzən gizli saxlanılmalı olur ki, dəqiq ərazilər tanıma bilməsin. Bu isə informasiya və verilənlərin idarə olunması ilə bağlı problemlər yaradır, bu cür problemlər isə yalnız layihə koordinatorları ilə əlaqə saxlamaqla və birgə layihələndirmə imkanları vasitəsilə həll oluna bilər. Layihə koordinatorları könüllülərin gizliliyini qorumaq məqsədilə bir sıra mexanizmlərdən, o cümlədən texnoloji mühafizə və verilənlər siyasətlərindən istifadə edirlər. Geniş istifadə olunan bir metod məkanın qeyri-səlisləşdirilməsi və ya gizlədilməsidir [7]. Bəzi sistemlərdə qeyri-səlis verilənlər olur, bu isə o deməkdir ki, dəqiq məkan qeyri-müəyyən edilir. Bunu layihə koordinatoru edir, ona görə də məkanı birçə o özü görür. Bu metoddan landşaftın gizlədilməsi üçün istifadə olunsa da, insanlar da ondan öz yaşayış yerlərinin gizlədilməsi məqsədilə xeyli yararlanırlar. Gizliliyin digər qorunması üsulu toplanılan və paylaşılan şəxsi informasiyanın həcmnin məhdudlaşdırılmasıdır. Elmi cəhətdən verilənləri kimin təqdim etdiyinin məlum olması vacib olduğu üçün, əksər layihələr könüllünün adını onun təqdim etdiyi verilənlərlə əlaqələndirir. Bu cür informasiyanın göstərilməsi barədə seçimdən asılı olaraq layihə koordinatorları könüllülərə hər iki seçimi – anonim identifikasiya və ya öz istifadəçi adlarını yaratmağı təklif edirlər [8].

III. VƏTƏNDAŞ ELMİNDƏ TƏHLÜKƏSİZLİK TƏDBİRLƏRİ

İT-nin tətbiqi ilə əlaqədar meydana çıxan problemlərin VE-də elmi-metodoloji prinsiplərə əsaslanan informasiya təhlükəsizliyinin təmin edilməsini, həmçinin şəbəkə texnologiyalarının müasir inkişaf meyillərinin nəzərdə tutulduğu hüquqi, təşkilati, texniki və fiziki mühafizə tədbirlərini qarşılıqlı surətdə əlaqələndirməklə informasiya təhlükəsizliyi siyasətinin yaradılmasını zəruri edir. İnformasiya təhlükəsizliyinin təmin edilməsi dedikdə informasiyanın konfidensiallığının, tamlığının və əlyətənliyinin təmin edilməsi başa düşülür. İnformasiyanın konfidensiallığı informasiyaya çıxış yalnız icazə verilmiş şəxslərə verildiyi, tamlığı verilənlərə rəziləşdirilmiş dəyişikliklər edildikdə, əlyətənliyi isə icazə verilmiş şəxslərin lazımı vaxtda informasiya resurslarına çıxış əldə etdikləri halda təmin edilir. VE-də bu məsələlərlə bərabər toplanan böyük həcmli verilənlərin verifikasiyası da mühüm əhəmiyyət daşıyır.

Vətəndaşların şəxsi həyatı, virtual məkanda və layihələrdə fəaliyyəti haqqında fərdi məlumatların qorunması mühüm əhəmiyyət kəsb edir. VE layihələri həyata keçirilən zaman

onun vətəndaş iştirakçılarının məxsus böyük həcmdə fərdi məlumatlar toplanır. Fərdi məlumatların toplanması, emalı və saxlanması məsələlərin səmərəli həlli VE-nin təhlükəsizliyi üçün vacib məsələlərdəndir. Fərdi məlumat dedikdə şəxsin kimliyini birbaşa və ya dolaylı yolla müəyyənləşdirməyə imkan verən istənilən məlumat nəzərdə tutulur.

Avropa İnsan Hüquqları Konvensiyasının (European Convention on Human Rights) 8-ci maddəsində göstərilir ki, fərdi məlumatlar vətəndaşın hüquqlarının ayrılmaz hissəsinə təşkil edir, vətəndaşın şəxsi həyatına və yazışma sirlinə hörmət edilməlidir.

Birləşmiş Ştatlarda vətəndaşların, o cümlədən VE ilə məşğul olanların gizliliyini qoruyan federal qanunlar var. Bunlara əsasən VE layihələri şəxsi informasiyanı toplamayan və ya şəxslərin məlumatları əsasında axtarıla bilinməyən verilənlər bazası yaratmağı seçə bilərlər. Əgər onlar şəxsi informasiyanı toplayarsa, bunu istifadəçinin hüquqları barədə informasiyanı təmin etməklə qəbul olunmuş aktlar ilə uyğunlaşdırılmalıdır. Bu aktlar layihələrin verilənlər topluları ictimaiyyətə açıq paylaşılmasından əvvəl onlardan şəxsi informasiya silinməsinə müəyyənləşdirir.

Elm və Texnologiya Siyasəti Ofisi (Office of Science and Technology Policy – OSTP) (www.whitehouse.gov/ostp/) tərəfindən təsdiqlənmiş memorandumlar Birləşmiş Ştatların bu sahədə əlavə resurslarıdır. Məsələn, “Federal Maliyyələşdirilmiş Tədqiqatın Nəticələrinə İctimai Girişin Genişləndirilməsi” adlandırılmış bir memorandum agentliklərə konfidensiallıq və şəxsi gizliliyi qorumaqla bərabər nəşr edilməli verilənlərə giriş hüququnu genişləndirməyi təklif edir. Birləşmiş Ştatlardan kənardakı standartlara İqtisadi Kooperasiya (Əməkdaşlıq) və İnkişaf Təşkilatı (Organization for Economic Cooperation and Development – OECD) tərəfindən təsdiq edilmiş prinsiplər daxildir [9]. Avropa Birliyi standartları ümumilikdə Birləşmiş Ştatların standartlarından daha ciddidir.

AR-in 11 may 2010-cu il, 998-IIIQ sayılı “Fərdi məlumatlar haqqında” Qanunun 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 subyektlər 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 uyğun olaraq hər kəsin istədiyi informasiyanı qanuni yolla axtarmaq, əldə etmək, ötürmək, hazırlamaq və yaymaq azadlığı vardır. Eyni zamanda, informasiya azadlığının həyata keçirilməsi digər insanların hüquqlarının, azadlıqlarının və qanuni maraqlarının pozulmasına səbəb olmamalıdır.

E-elmdə mövcud olan təhlükəsizlik problemləri və təhdidlər VE-də də mövcuddur [2]. VE layihələrinin təhlükəsizlik məsələləri:

- texniki qurğular və avadanlıqlar, proqram vasitələri üçün təhlükəsiz konfigurasiyaların seçilməsi,
- təhlükəsizliyə aid proqram vasitələrinin tətbiqi,
- səlahiyyətli və icazəsiz qurğuların və proqram vasitələrinin inventarlaşdırılması,
- müdafiə sərhədinin seçilməsidir.

E-elmə analoji olaraq, VE-də də təhlükəsizliyə nəzarət və mühafizə məsələləri aşağıdakılardır:

- səlahiyyətə uyğun girişə nəzarət;
- naqilsiz girişə nəzarət;
- zərərli proqramlardan mühafizə;
- verilənlərin qorunması, onların bərpa edilməsi imkanlarının nəzərə alınması.

VE-nin mühafizəsinin səmərəli təşkili və həyata keçirilməsinə xidmət edən göstərilmiş məsələlərin həlli zamanı aşağıdakılar nəzərə alınmalıdır:

- baş vermiş təhdidlərin öyrənilməsi və qarşısının alınması nəticəsində əldə olunmuş biliklər əsasında praktiki mühafizənin qurulması;
- prioritetin ən təhlükəli təhdidlərdən mühafizəni təmin edəcək tədbirlərə verilməsi;
- lazımi düzəlişlərin təyin edilməsi və tez həyata keçirilə bilməsi üçün təhlükəsizlik tədbirlərinin səmərəliliyinin qiymətləndirilməsinin ümumi göstəricilərinin olması;
- mövcud təhlükəsizlik tədbirlərinin səmərəliliyini yoxlamaq üçün fasiləsiz diaqnostikanın həyata keçirilməsi və mühafizənin maksimal dərəcədə avtomatlaşdırılması.

VE layihələrinin və digər kraudsorsinq təşəbbüslərinin rəhbərləri təhlükəsizliyi təmin etmək üçün bir sıra təhlükəsizlik siyasətləri hazırlaya bilər. Bu məsələdə aşağıdakı təcrübələrdən istifadə etmək əlverişli olar [5]:

- Tamlıq, ictimai əlyetənlik və verilənlərin paylaşılması nöqtəyi-nəzərdən verilənlərin seçilməsi, bu seçimlərin təsdiq olunması və onları dəstəkləyən texnologiyaların həyata keçirilməsi;
- Konfidensiallığın seçilməsi ilə bağlı geniş imkanların verilməsi, normal iştirakın hansı hallarda şəxsi gizliliyə risk olmasının izahı, könüllülərin bu barədə xəbərdar edilməsi;
- Könüllülərə müəyyən verilənləri ictimaiyyətdən gizlədilməsi və ya gizlədilməməsi hallarında anonimliyi təmin etmək üçün seçim verilməsi;
- Könüllülərə verilənləri silmək və dəyişdirmək imkanı yaradılması;
- Könüllülər haqqında minimal informasiya tələb edilməsi.

VE layihələrinin veb-səhifələrinə giriş zamanı biometrik identifikasiya metodlarından istifadə edilməsi təhlükəsizliyin təmin edilməsi üçün görülə biləcək ən qabaqcıl tədbirlərdən

birdir. Bu, veb-səhifəyə daxil olan şəxslərin özləri haqqında düzgün məlumat daxil etməsini təmin edəcək.

NƏTİCƏ

Araşdırmalar göstərir ki, İT-nin son nailiyyətlərinin tətbiqi ilə VE intensiv olaraq inkişaf edir. Bununla yanaşı onun təhlükəsizliyinin təmin olunması mürəkkəb bir məsələ kimi aktuallaşır. İnformasiya təhlükəsizliyinin konfidensiallıq, tamlıq və əlyetənliyin təmin edilməsi və fərdi məlumatların qorunması kimi məsələləri tədqiq olunaraq vətəndaş elminin effektiv mühafizəsi üçün prioritet istiqamətlər göstərilmişdir. İnformasiya təhlükəsizliyi üzrə təqdim olunmuş bu konseptual yanaşmanın tətbiqi ilə VE-nin inkişafında mühüm nəticələr əldə oluna bilər.

ƏDƏBİYYAT

- [1] R.M. Alguliyev, R.G. Alakbarov, T.Kh.Fatallyev, "Electronic science: current status, problems and perspectives", *Problems of information technology*, №2, 2015, pp. 4–14, DOI: 10.25045/jpit.v06.i2.01
- [2] T.Kh.Fatallyev, "Security provision issues of e-science, *Problems of information society*", №1, 2016, pp. 50–55, DOI: 10.25045/jpis.v07.i1.06
- [3] European Citizen Science Association, www.ecsa.citizen-science.net
- [4] J.P. Cohn, "Citizen science: Can volunteers do real research?", *BioScience*, Vol. 58, No. 3, 2008, pp. 192–197.
- [5] A. Bowser and o., "Sharing data while protecting privacy in citizen science", *Interactions*, Vol. 21, Issue 1, 2014, pp. 70–73.
- [6] T. Scassa, H. Chung. "Typology of citizen science projects from an intellectual property perspective", *Wilson center—Commons Lab*, 2015, www.wilsoncenter.org/sites/default/files/Typology_of_Citizen_Science_IP_Rights_Scassa.pdf
- [7] B. Sullivan, et al., "The eBird enterprise: An integrated approach to development and application of citizen science", *Biological Conservation* 169, 2014, pp.31–40.
- [8] A. Bowser, K. Shilton, J. Preece, E. Warrick. "Accounting for Privacy in Citizen Science: Ethical Research in a Context of Openness", 2017, <https://terpconnect.umd.edu/~kshilton/pdf/BowserEtAlCSCW.pdf>
- [9] OECD Guidelines on the Protection of Privacy and Transborder ..., www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsofPersonalData.htm

ABOUT INFORMATION SECURITY OF CITIZEN SCIENCE

Tahmasib Fatallyev¹, Nargiz Verdiyeva²

^{1,2}Institute of Information Technology of ANAS, Baku, Azerbaijan
depart3@iit.science.az

Abstract – Citizen science, characterized by the participation of a large number of volunteers in large-scale spatial and time-scale quantitative measurements and observations, is rapidly developing with the application of information technologies. The article is dedicated to the research of information security issues to ensure its efficient performance. Issues such as confidentiality, completeness, accessibility and protection of personal data are studied and priority directions for effective protection of citizen science are shown.

Keywords – e-science; citizen science; open science; information security; citizen science projects.

Yeni media təhsili və informasiya təhlükəsizliyi

Gülzar Paşayeva

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

gulnar.amea@gmail.com

Xülasə — Yeni medianın vəzifələri və Azərbaycanın media sahəsində informasiya təhlükəsizliyinin təmin olunması məsələlərinə baxılmışdır. İnformasiya təhlükəsizliyinin media sahəsindəki rolu, informasiya müharibəsinin jurnalistikaya, eləcə də cəmiyyətə təsiri məsələləri araşdırılmışdır.

Açar sözlər — yeni media, media təhsili, informasiya müharibəsi, KİV və informasiya təhlükəsizliyi.

I. GİRİŞ

İnformasiya-kommunikasiya texnologiyalarının (İKT), xüsusən, Internetin intensiv və sürətli inkişafı, geniş tətbiqi nəticəsində cəmiyyətin bütün sferalarında köklü dəyişikliklər baş verir, ənənəvi fəaliyyət sahələri transformasiyaya uğrayır, yeni peşə sahələri meydana gəlir [1].

Məlumdur ki, kütləvi informasiya vasitələri (KİV) insan şəxsiyyəti və şüurunun formalaşmasında da güclü psixoloji təsir gücünə malikdir. Çünki ilk növbədə, KİV cəmiyyətdə gedən informasiya prosesinin müxtəlif mərhələləri və təbəqələrinə təsir göstərir, rəqəmsal inqilabın meydana çıxmasına səbəb olur.

KİV sahəsində informasiya siyasətinin əhatə etdiyi məsələlərdən biri də milli təhlükəsizliyin tərkib hissəsi olan informasiya təhlükəsizliyinin təmin olunmasıdır. İnformasiya təhlükəsizliyi deyərək informasiya məkanında ölkənin milli maraqlarının müdafiəsi başa düşülür. Burada medianın da üzünə böyük missiya düşür [2].

II. İNFORMASIYA MÜHARİBƏSİ NƏDİR?

Kommunikasiya və informasiya sənayesində baş verən ciddi dəyişikliklərdən biri də informasiya müharibəsidir. İnformasiya-psixoloji müharibəsi düşməne fiziki hücumu nəzərdə tutan müharibə anlayışından fərqlidir. Onun məğzi insanları öz maraqlarının əksinə hərəkət etməyə vadar etməyi, insanları idarə etməyi nəzərdə tutur. Jurnalistlər, media nümayəndələri bu virtual məkanın əsgərinə çevrilirlər – onlar döyüşür, qalib gəlir və “ölürlər” [3].

İlk dəfə “İnformasiya müharibəsi” terminini 1976-cı ildə amerikalı mütəxəssis Tomas Rona (Thomas Rona) “Boeing” şirkəti üçün hazırladığı “Silah sistemləri və informasiya müharibəsi” adlandırdığı hesabatında istifadə edib. Rona hesabatında sübut etmişdi ki, son illərdə informasiya infrastrukturunu ABŞ iqtisadiyyatının əsas komponentinə çevrilib. Bu termin rəsmi olaraq isə ilk dəfə ABŞ Müdafiə Nazirliyi tərəfindən 1992-ci ildə istifadə edilib. Nazirliyin

informasiya müharibəsi haqqında sənədlərində bildirilir ki, informasiya həm silah, həm də məqsəddir: informasiya hücumu isə icazə olmadan istənilən formada informasiyanın köçürülməsi, dəyişdirilməsi və məhvini, habelə program təminatlarına, məxfi informasiyanın saxlandığı texniki qurğulara və insan psixologiyasına yönəlmiş əməliyyatdır. ABŞ-da informasiya müharibəsini təsvir etmək üçün çox zaman onu informasiya əməliyyatı ilə müqayisə edirlər. İnformasiya əməliyyatı - məqsədə çatmaq üçün qarşı tərəfin informasiya fəzasına təsir etmək və bu zaman öz informasiya resurslarını qorumaq məqsədi ilə xüsusi metodlardan və vasitələrdən (siyasi, iqtisadi, texniki, hərbi və s.) istifadə etməklə həyata keçirilən mübarizə formasıdır [4].

Bu gün media sahəsində cəmiyyətə təsirin populyar üsulu olan informasiya müharibəsindən geniş istifadə olunur. Intensiv qarşılıqlı olan informasiya müharibəsi informasiya məkanında psixoloji və ideoloji üstünlük əldə etmək məqsədilə informasiya sistemləri, proseslər və resurslara, kritiki vacib strukturlara və kütləvi kommunikasiya vasitələrinə zərər yetirilməsini, siyasi və sosial sistemlərin dağıdılmasını nəzərdə tutur [5].

İnformasiya müharibəsinin əsasında məlumatların yayılmasının ən yeni texniki vasitələrindən istifadə dayanır. Radio, televiziya, mobil rabitə və Internet informasiya müharibəsinin əsas üsullarıdır.

İKT-nin sürətli inkişafı hesabına informasiya müharibəsinin aparılması formaları və metodları da təkmilləşir. Belə ki, ABŞ-da artıq dezinformasiya stansiyası yaradılmışdır ki, bu qurğu rəqibin radio danışıqlarını əldə etməyə, onların səslərinə yalan məlumatı daxil etməyə və real vaxtda ötürməyə imkan verir [6]. İnformasiya müharibəsinin tərkib hissələrini aşağıdakı kimi qruplaşdırmaq olar:

- psixoloji əməliyyatlar - düşmənin arqumentasiyasına təsir etmək üçün informasiyadan istifadə;
- elektron müharibə - düşməne dəqiq informasiyanı almağa imkan verməmək;
- dezinformasiya - düşməne güc və məqsədlər haqqında yalan məlumat vermək;
- fiziki məhv - informasiya sisteminin elementlərinə təsir etmək;
- təhlükəsizlik tədbirləri - düşmənin imkanlar və niyyətlər haqqında məlumat əldə etməsinin qarşısının alınması;

- birbaşa informasiya hücumları - qarşı tərəfin yaydığı informasiyanın birbaşa təhrif olunması [7].

III. YENİ MEDIA TƏHSİLİNİN VƏZİFƏLƏRİ

Bu gün dünyada informasiya qarşılıqlı təsirinin yeni modeli kimi meydana çıxan media vasitələri cəmiyyətin informasiya tələbatını ödəməklə məşğuldur. Buraya televiziya kanalları, informasiya agentlikləri, radio, qəzet və jurnallar, İnternetdə fəaliyyət göstərən xəbər saytları, sosial şəbəkələr, bloqlar və s. aiddir. Bu informasiya axını arasında hansı xəbərin doğru, hansı xəbərin yalnış olduğunu seçmək müasir jurnalistikanın əsas problemlərindəndir. Çünki KİV-in təsiredici funksiyası onun digər, xüsusən də məlumat ötürmə funksiyasını geridə qoymuşdur [8].

Müasir jurnalistika son 10 il ərzində yeni keyfiyyət mərhələsinə qədəm qoymuşdur, bu da informasiyanın maksimum opreativliyinə şərait yaradan yeni texnologiyanın inkişafı ilə bağlıdır. Jurnalistika yeni texnologiya və vasitələrlə zənginləşmiş, yeni anlayışlar, həmçinin yeni jurnalistika alətləri ilə üzləşmişdir [9].

Jurnalistika cəmiyyətdə insanların bir-birilə məlumat paylaşmaq ehtiyacı meydana gəlidiyi gündən bəri böyük əhəmiyyət kəsb edir. İnformasiya bolluğu və mürəkkəb ideoloji-psixoloji şəraitdə hədəf auditoriyasını düzgün seçmək, müasir texnologiyalardan istifadə edərək, eləcə də milli-mənəvi dəyərləri nəzərə alaraq xəbər hazırlamaq hər bir jurnalist üçün vacib məqamlardır. Bu mürəkkəb yolda ən mühüm vəzifə media sahəsində fəaliyyət göstərən ali məktəblərin, jurnalistika fakültələrinin, alimlərin və jurnalistlərin üzərinə düşür.

Media təhsili KİV-in (mətbuat, televiziya, radio, kino və s.) qanunauyğunluqlarının öyrənilməsinə nəzərdə tutan pedaqoji istiqamətlərdən biri kimi müəyyən edilir. Əsas vəzifəsi müasir informasiya şəraitində müxtəlif məlumatların qavranılmasını, informasiyanın psixologiyaya təsirinin nəticələrini təhlil etməyi, texniki vasitələrin köməyi ilə ünsiyyət üsullarına yiyələnməyi öyrətməkdir.

IV. AZƏRBAYCANIN MEDIA SAHƏSİNDƏ İNFORMASIYA TƏHLÜKƏSİZLİYİ MƏSƏLƏLƏRİ

Qloballaşan dünyada İKT-nin geniş tətbiqi informasiya təhlükəsizliyi məsələsinə ön plana çıxarır. Cəmiyyətin təhlükəsizliyinin əsas elementlərindən biri kimi informasiya təhlükəsizliyinin vəzifələri hər hansı məlumatın konfidensiallığı, tamlığı, əlyətərliliyi və kütləvi qorxu (vahimə) yaradan məzmunə qarşı mübarizədir [10].

İnternetin imkanları artdıqca, yeni xidmətlərin tətbiqi genişləndikcə, sosial şəbəkələr inkişaf etdikcə, saytların sayı artdıqca insanların siyasi fəallığı da artır. Bütün bunlar informasiya hücumlarının çoxalmasına səbəb olur. Həm də nəzərə almaq lazımdır ki, bu gün ictimai rəyin formalaşdırılması və ya dəyişdirilməsində, bəzi qərarların qəbul edilməsində, qarşı tərəfin informasiya resurslarına təsirində, eləcə də dezinformasiyanın yayılmasında İnternet geniş imkanlara malikdir. Elə bunun nəticəsidir ki, son bir neçə ildə İnternetə informasiya hücumları artmışdır.

Hər bir ölkənin milli təhlükəsizliyinin əsas istiqamətlərindən biri də informasiya təhlükəsizliyidir. Azərbaycan Respublikasının informasiya sahəsində milli təhlükəsizliyinin təmin olunması məqsədi ilə ölkədə informasiyanın, dövlət informasiya ehtiyatlarının müdafiəsi sahəsində milli sistem və informasiya infrastrukturunun inkişaf etdirilməsi və möhkəmləndirilməsi ilə bağlı tədbirlər görülür [11].

Təsadüfi deyildir ki, informasiya təhlükəsizliyinin möhkəmləndirilməsi Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyasında ən mühüm və uzunmüddətli vəzifələrdən biri kimi bəyan edilmişdir: “Azərbaycan Respublikasının informasiya təhlükəsizliyi siyasəti dövlət, ictimai və fərdi informasiya ehtiyatlarının qorunmasına, habelə informasiya sahəsində milli maraqların müdafiəsinə yönəlmiş tədbirlər kompleksinin həyata keçirilməsindən ibarətdir”.

Biz bu gün informasiya əsrində, İnternet və digər informasiya texnologiyalarının inkişafı dövründə yaşırıq. Azərbaycanda siyasi plüralizm hökm sürür, azad mətbuat, İnternet və informasiya orqanları fəaliyyət göstərir, əhalinin böyük bir hissəsi İnternetdən istifadə edir. Lakin qlobal informasiya məkanında İnternetdən, informasiya vasitələrindən, transmilli mətbuatdan bəzən insanların informasiya ehtiyacını ödəməklə yanaşı, həm də xüsusi təxribat vasitəsi kimi istifadə edirlər. Bu təxribatlar, məqsədyönlü kampaniyalar bəzi hallarda açıq, bəzi hallarda gizli aparılır. Əlbəttə, belə şəraitdə ölkələrin informasiya təhlükəsizliyi məsələləri çox aktualdır [12].

Respublikada informasiya təhlükəsizliyinin təmin olunması və informasiya texnologiyalarının inkişafı ilə bağlı milli qanunvericilik bazası xeyli təkmilləşdirilmişdir. “Kütləvi informasiya vasitələri haqqında”, “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında”, “Məlumat azadlığı haqqında”, “İnformasiya əldə etmək haqqında”, “Telekommunikasiya haqqında”, “Dövlət sirri haqqında” və s. qanunlarda bu məsələlərə diqqət yetirilmişdir.

Azərbaycan dövlətinin 2013-cü ildə özünün AZƏRSPACE-1 video-informasiya ötürücü peykini yeraltı orbitə çıxarması və regionda Rusiya, Türkiyə ilə birlikdə kosmik ölkəyə çevrilməsi onun həm informasiya fəaliyyəti və təhlükəsizliyinin təmin olunmasında mühüm rol oynamış, həm də ölkəyə İKT sahəsində yaxın gələcəkdə böyük uğurlar qazandırmaya şərait yaratmışdır. [13].

V. MEDIA TƏHSİLİ CƏMİYYƏTİN İNFORMASIYA TƏHLÜKƏSİZLİYİNİN TƏMİN OLUNMASINDA FAKTOR KİMİ

Müasir cəmiyyətdə informasiya proseslərinin intensivləşməsi sosial mühitin inkişafının obyektiv qanunauyğunluğuna çevrilmişdir: informasiyanın həcmi, ötürülməsi və emalı prosesi sürətlənmişdir. Bu proseslər insanlara mənfi təsir göstərməklə yanaşı, həm də informasiya yüklənməsinə gətirib çıxarır, bu da öz növbəsində düşünmək və əks etdirmək qabiliyyətini zəiflədir.

Müasir KİV-in gənc nəslin inkişafına təsiri faktı xüsusi narahatlıq doğurur. Cəmiyyətdə zorakılıq dalğasının geniş

yayılması, ənənəvi ümumbəşəri dəyərlərin dağıdılması, gənclərdə həssaslığın azalması – bütün bunlar bütövlükdə KİV-in müasir vəziyyəti ilə birbaşa bağlıdır.

Dünyada genişmiqyaslı kommunikativ inqilabların baş verməsi cəmiyyətdə informasiya təhlükəsizliyinin təmin olunması problemini daim kəskinləşdirir. 1990-cı illərin əvvəllərindən etibarən Kanada, Avstraliya və bir sıra Avropa ölkələrində ümumi kütləvi informasiya təhsili proqramları fəaliyyət göstərir, media təhsilinə olan tələbat daha da artır. Bu təhsil tələbələrə, gənclərə müasir informasiya məkanında necə davranmaq lazım olduğunu öyrətmək kimi humanist bir funksiyani yerinə yetirir [14].

XXI əsrdə media təhsili dedikdə, həm də media ilə ünsiyyət mədəniyyətinin formalaşması, kritik düşüncə, yaradıcı və kommunikativ bacarıqların inkişafı, media mətnlərinin təhlili və qiymətləndirilməsi, media texnikalarından istifadə bacarıqlarının öyrədilməsi və s. nəzərdə tutulur.

NƏTİCƏ

Müasir KİV nəinki dünya hadisələrini çevik işıqlandırır, həm də informasiyanın təhlili ilə məşğul olur, onu süzgəcdən keçirir və məqsədli şəkildə seçərək istifadə edir, məhz buna görə də insanların şüuruna güclü təsir göstərir. KİV həmçinin tədris, maarifləndirmə, milli-mənəvi və ümumbəşəri dəyərlərin qorunub saxlanması və inkişaf etdirilməsi funksiyasını yerinə yetirir.

Cəmiyyətin media savadının səviyyəsi informasiya təhlükəsizliyinin təmin edilməsi üçün mühüm əhəmiyyət kəsb edir. Beləliklə, aparılan araşdırmalar aşağıdakı tədbirlərin görülməsini zəruri edir:

- yeni medianın cəmiyyətə təsiri ilə bağlı çoxaspektli tədqiqatların aparılması;
- yeni media sferasında informasiya təhlükəsizliyi problemi ilə bağlı maarifləndirmə işlərinin həyata keçirilməsi;
- ali məktəblərdə informasiya təhlükəsizliyi ilə bağlı yeni ixtisasların yaradılması;
- KİV-də informasiya təhlükəsizliyinin təmin olunmasına yönəlməmiş tədbirlərin təşkili.

ƏDƏBİYYAT

- [1] Əliquliyev R.M., Mahmudov R.Ş. İnternet-medianın meydana gəlməsi və inkişafı: əsas istiqamətlər və xüsusiyyətlər, Ekspres-informasiya, İnformasiya cəmiyyəti seriyası, Bakı, “İnformasiya Texnologiyaları” nəşriyyatı, 2012, 59 s.
- [2] www.stj.sam.az - Niyazov.X. “İnformasiya azadlığı və informasiya təhlükəsizliyinin bəzi məsələləri milli təhlükəsizlik kontekstində”, “Strateji təhlil” analitik jurnalı, 2016.
- [3] Сергеевич Л. Н. Информационная война как порождение нового времени и современных массмедиа технологий. Часть II. Контуры информационной войны современности - <http://www.mediascope.ru/1738>
- [4] www.anl.az/down/meqale/xalqcebbhesi/2014/mart/359441.htm
- [5] Информационная война, www.mindmeister.com/1022599463
- [6] www.mediascope.ru/1738
- [7] www.lib.ru/SECURITY/kvn/corner.txt_with-big-pictures.html

- [8] Ozyumenko V.I. Media Discourse in an Atmosphere of Information Warfare: From Manipulation to Agression //Russian Journal of Linguistics, 2017, 204 p.
- [9] Yeni media, ənənəvi media anlayışları, dilanova.wordpress.com/2013/10/27/yeni-media-ənənəvi-media-anlayışlar/
- [10] kasi.az/az/jurnalistika-ve-informasiya-tehlukesizliyi/pages/q.pdf
- [11] anl.az/el/Kitab/2016/Azf-291129.pdf
- [12] azpress.az/index.php?lang=az§ionid=news&id=24604
- [13] azpress.az/index.php?lang=az§ionid=news&id=24604
- [14] Коханая О.Е. Медиаобразование как фактор информационной безопасности общества, «Вестник Московского государственного университета культуры и искусств», 2011, с. 182-187.

NEW MEDIA EDUCATION AND INFORMATION SECURITY

Gulnar Pashayeva

Institute of Information Technology of ANAS, Baku,
Azerbaijan

gulnar.amea@gmail.com

Abstract – This article embraces considerations of new media duties and providing information security in Azerbaijani media. Accordingly, the role of information security in media as well as the effect of information war towards society have been highlighted in the article.

Keywords – new media, media education, information war, media and information security.

Big Data texnologiyalarının təhlükəsizlik problemləri və həlli yolları

Məkrufə Hacırəhimova¹, Aybəniz Əliyeva²

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

¹makrufa@science.az, ²aliyeva.a.s@mail.ru

Xülasə—Big data texnologiyalarının meydana gəlməsi verilənlərin təhlükəsizliyi və məxfiliyi üçün yeni problemlər yaradır. Ənənəvi texnologiyalar və metodlar bu problemlərin həlli üçün uyğun və səmərəli deyildir. İşdə böyük verilənlərin təhlükəsizlik problemləri tədqiq olunur. Böyük verilənlərin təhlükəsizliyi və məxfiliyi üçün istifadə olunan texnoloji həllər təhlil olunur və onların cari vəziyyəti nəzərdən keçirilir.

Açar sözlər— big data; verilənlərin təhlükəsizliyi; infrastrukturun təhlükəsizliyi; verilənlərin gizliliyi

I. GİRİŞ

Hazırda şəbəkə və informasiya texnologiyalarının inkişafı verilənlərin həcmnin sürətlə artmasına səbəb olur. Müxtəlif üsullarla əldə edilmiş bu böyük verilənlər (ing. Big data) biznes, telekommunikasiya, səhiyyə, maliyyə, informasiya texnologiyaları, təhsil və s. daxil olmaqla bir çox sahələrdə mühüm rol oynayır. Böyük verilənlərin (BV) səmərəli emalı müəssisələrin rəqəbat üstünlüyünün artmasına, bir çox sosial və iqtisadi sahələrdə dəyərin yüksəlməsinə imkan verir. Maksimum gəlirlərin əldə edilməsi məqsədilə dövlət orqanları tərəfindən Big data layihələrinə böyük miqdarda investisiyalar qoyulur, özəl sektorlar gəlirlərin artmasına və resursların optimallaşdırılmasına güclü səy göstərirlər. Lakin Big data kontekstində informasiyanın təhlükəsizliyi və gizliliyinə risklərin olması bu texnologiyaların tətbiqini məhdudlaşdırır və inkişafına mane olur [1, 2].

Ümumiyyətlə, verilənlərin təhlükəsizliyi hər zaman vacib məsələlərdən hesab olunmuşdur. Lakin Big data-nın meydana gəlməsi ilə informasiya təhlükəsizliyi baxımından yeni problemlər yaranmışdır. BV-nin mənbələrinin müxtəlifliyi, axın şəklində informasiyanın toplanması və böyük həcmdə informasiyanın “buludlara” miqrasiyası kimi xüsusiyyətləri təhlükəsizlik və gizlilik problemlərini daha da kəskinləşdirmişdir [3, 4]. Bu problemlər verilənlərin toplanması, saxlanması və idarə edilməsi, ötürülməsi və təhlili kimi bütün mərhələləri əhatə edir.

Big data texnologiyalarının informasiya təhlükəsizliyi məsələsi beynəlxalq aləmin, elmi dairələrin diqqətindən kənarda qalmamış, əsas tədqiqat mövzusunə çevrilmişdir. Belə ki, BV-nin təhlükəsizliyinin mühafizəsi üzrə fəaliyyətin standartlaşdırılması məsələlərinə Standartlaşdırma üzrə beynəlxalq təşkilat (International Organization for

Standardization) və Beynəlxalq elektrotexniki komissiya (International Electrotechnical Commission) (ISO/IEC), Beynəlxalq Telekommunikasiya İttifaqı (International Telecommunication Union, ITU), Britaniya Standartlar İnstitutu (British Standards Institution, BSI), ABŞ-ın Milli Standartlar və Texnologiyalar İnstitutu (National Institute of Standards and Technology, NIST) kimi bir sıra aparıcı standartlaşdırma institutları cəlb edilmişdir [5].

Dünyanın bir çox ölkələri BV-nin təhlükəsizliyinin təmini üçün bir sıra qanunları tədqiq etmişdir. ABŞ 2012-ci ilin mart ayında Böyük verilənlərin təhlükəsizliyi ilə bağlı inkişaf strategiyalarını dərc edən ilk ölkə olmuşdur. Həmin ilin iyun ayında Britaniya hökuməti gizliliyin qorunması normaları üçün özəl olaraq “Open Data White Paper” icmalı nəşr etdirmişdir. Fransa, Yaponiya, Avstraliya və digər ölkələr böyük verilənlərin təhlükəsizliyinin inkişaf strategiyasını qəbul etdilər [1].

Böyük verilənlər əsas tədqiqat mövzusu olmasına baxmayaraq, mövcud təhlükəsizlik sxemləri tətbiqi proqramların tələblərinə tam cavab verə bilməz. Son illər tədqiqatçılar tərəfindən mövcud təhlükəsizlik sxemləri təkmilləşdirilmiş və ya yeni təhlükəsizlik texnologiyaları irəli sürülmüşdür.

İşin məqsədi BV-nin təhlükəsizliyi və məxfiliyi problemlərinin araşdırılması və bu problemlərin həlli üçün təklif edilmiş texnologiyaların və metodların cari vəziyyətini analiz etməkdən ibarətdir.

II. BÖYÜK VERİLƏNLƏRİN TƏHLÜKƏSİZLİK PROBLEMLƏRİ

İnternet mühitində rəqəmsal informasiyanın həcmi artıqca onun istifadəçilərinin sayı da çoxalır. Nəticədə informasiyanın məxfiliyinə və təhlükəsizliyinə olan təhdidlər artır, yeni təhlükəsizlik problemləri yaranır [6]. Bulud Təhlükəsizlik Alyansı (CSA – Cloud Security Alliance) tərəfindən “Big data” sistemlərinin on təhlükəsizlik problemi [7] verilmiş və onlar infrastrukturun təhlükəsizliyi, verilənlərin gizliliyi, verilənlərin idarə edilməsi, tamliq və reaktiv təhlükəsizlik kimi dörd qrup üzrə təsnifatlandırılmışdır [8].

A. *İnfrastrukturun Təhlükəsizliyi Problemləri*

1) Paylanmış hesablamların və digər proseslərin təhlükəsizliyinin təmini

Hadoop platformasının MapReduce kimi paylanmış strukturunun hesablama və emal elementlərinin təhlükəsizliyi əsas etibarilə mühafizə olunmur. Bunun üçün kartoqrafların təhlükəsizliyi, “kartoqraflar” icazəsiz olduqda isə verilənlərin mühafizəsi tədbirləri həyata keçirilməlidir.

2) Qeyri-relyasion verilənlər anbarlarının məxfiliyinin qorunması

NoSQL kimi verilənlər bazaları gizlilik təhdidlərinə səbəb olan bir çox təhlükəsizlik qüsurlarına malikdir. Təhlükəsizliyin bu qüsurları verilənlərin tezqləşdirilməsi və ya qeyd edilməsi, həmçinin ötürülməsi və ya toplandıqdan sonra müxtəlif qruplara paylanması zamanı verilənlərin şifrələnməməsi ilə bağlıdır.

B. Verilənlərin Gizliliyi Problemləri

1) Gizliliyi saxlayan miqyaslanan və kompozit data mining və analitika

Kiçik bir məlumat sızması və ya platformada boşluq aralığının olması verilənlərin böyük itkisinə səbəb ola bilər. Nəticədə BV-nin analitikasında problemlər yarana bilər.

2) Giriş nəzarətin əlaqə və şifrələmə metodlarının təhlükəsizliyinin təmini

Verilənlərin mühafizəsinin sadə üsulu bu verilənlərin saxlanması qurğularının, platformalarının təhlükəsizliyinin təminidir. Çünki verilənlərin saxlanması qurğuları təhlükələrə daha həssasdır. Ona görə də şifrələmə metodlarının təhlükəsizliyinin təmin olunması vacibdir.

3) Qranular giriş nəzarəti

NoSQL verilənlər bazası və ya Hadoop paylanmış fayl sisteminin böyük verilənlər anbarlarının qranular giriş nəzarəti üçün güclü autentifikasiya prosesi və məcburi giriş nəzarətinin olması əsas tələblərdəndir.

C. Verilənlərin İdarə Edilməsi Problemləri

1) Verilənlərin saxlanması və ötürülməsi jurnallarının mühafizəsi

İnformasiya daşıyıcılarında saxlanılan tranzaksiya jurnalları və digər məxfi verilənlər müxtəlif səviyyələrə malik ola bilərlər, lakin bu kifayət deyildir. Nümunə üçün, verilənlərin bu səviyyələr arasında trasferi zamanı İT meneceri yerini dəyişən verilənlər barəsində məlumatlı olur. Verilənlərin həcmi fasiləsiz artıqca, miqyaslılıq və əlyətərlik böyük verilənlərin saxlanmasının idarə edilməsi üçün avtomatik çoxsəviyyəliyi (auto-tiering) zəruri edir. Bununla belə, “auto-tiering” üsulu verilənlərin saxlanma yerinə nəzarət etmədiyindən, BV-nin saxlanması üçün yeni problemlər yaranır. Ona görə də bu saxlanma icazəsiz girişdən qorunmalı və onların əlyətərliyi daim təmin edilməlidir [9].

2) Qranular audit

Müxtəlif növ jurnalların düzgün analizi faydalı ola bilər və bu informasiya bütün kiberhücumlardan və ya zərərli fəaliyyətin

(casusluğun) aşkarlanmasında istifadə edilə bilər. Buna görə verilənlərin fasiləsiz yoxlanması ilə yanaşı onların müntəzəm surətdə auditi də çox vacibdir.

3) Verilənlərin mənşəyinin təyini problemləri

Verilənlərin təsnifləndirilməsi zamanı onların mənşəyinin bilinməsi zəruridir. Verilənlərin mənşəyinin dəqiq müəyyən edilməsi onun identifikasiyası, yoxlanması və giriş nəzarəti ilə əldə edilə bilər.

D. Tamlıq və reaktiv təhlükəsizlik problemləri

1) Girişlərin yoxlanması və filtrasıyası

Giriş qurğuları BV-nin qorunmasında əsas yer tutur. Saxlanma, emal və digər zəruri işlər giriş qurğularından daxil olan ilkin verilənlərin köməyi ilə həyata keçirilir. Buna görə də, bir təşkilat etibarlı və qanuni giriş qurğularının istifadə olunmasını təmin etməlidir. Hər bir şəbəkə zərərli girişlərdən azad olmalıdır [9].

2) Real-vaxt rejimində verilənlərin təhlükəsizliyinin və monitorinqinin təmini

Təhlükəsizlik yoxlamaları və monitorinqin real vaxt rejimində və ya real vaxta olduqca yaxın digər bir rejimdə yerinə yetirilməsi daha uyğun hesab edilir. Qeyd edək ki, ənənəvi platformaların çox hissəsi generasiya olunan verilənlərin böyük həcmi səbəbindən bunu edə bilmirlər.

**III. BIG DATA TEXNOLOGİYALARININ
TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİ METODLARI**

Böyük verilənlərin təhlükəsizliyi və məxfiliyi ilə bağlı yuxarıda qeyd olunan problemlərin həlli üçün tədqiqatçılar tərəfindən müxtəlif metodlar təklif olunmuşdur. Aşağıda bu metodların bəziləri nəzərdən keçirilmişdir.

A. Verilənlərin məxfiliyinin qorunması metodları

Böyük verilənlərin gizliliyini qorumaq üçün verilənlərin şifrələmə və anonimliyi texnologiyasından istifadə edilir.

1) Verilənləri şifrələmə texnologiyaları

a) Homomorfik şifrələmə: Verilənləri şifrələmə müddəti verilənlərin gizliliyini qorumaq üçün əhəmiyyətli bir vasitədir. Böyük verilənlər sisteminin məlumatı sürətli və effektiv emal etmə qabiliyyəti şifrələmə üçün tələb olunan aparat və proqram təminatının tələblərinə uyğundur və verilənlərin gizliliyinin qorunmasında homomorfik şifrələmənin istifadəsini mümkün edir [10].

Homomorfik şifrələmənin konsepsiyası ilk dəfə R.L.Rivest və həmkarları tərəfindən daxil edilmişdir. Bu metodun üstünlüyü ondan ibarətdir ki, şifrələnmiş mətnlər deşifrə edilmədən, hesablamanın nəticələrinə təsir etmədən birbaşa əməliyyat apara bilərlər. Şəkil 1-də bulud mühitində homomorfik şifrələmə üçün konkret nümunə göstərilmişdir. Şəkildən görüldüyü kimi A və B mətnlərinə homomorfik şifrələmə tətbiq edilir və onlar bulud mühitinə göndərilir.

Homoqrafik şifrələmədən sonra şifrlənmiş mətn deşifrə olunur və düzgün nəticə C qeyd olunur [1].

Ümumiyyətlə, homomorfik şifrələməni şərti olaraq yarıhomomorfik (semi-homomorphic encryption, SHE) və tam homomorfik (fully homomorphic encryption, FHE) kimi iki növə bölürlər. SHE sxemləri yalnız toplama və vurma kimi sadə əməliyyatları dəstəkləyir. İlk dəfə C.Gentry tərəfindən təklif edilmiş FHE sxemi isə ixtiyari çoxhədlinin hesablanmasını dəstəkləyir. FHE sxeminin BGV, Bral2, TSZ, və GSW1321 kimi tanınmış bir çox sxemləri də Big data-nın təhlükəsizliyi və məxfiliyinin təmini üçün istifadə olunmuşdur [1, 11].

Şəkil 1 Bulud mühitində homomorfik şifrələmə

Q. Zhang və həmkarları Big data-nın klasterləşməsinin təhlükəsizliyinin təmini üçün PCM (possibilistic means calculation) və CFS (clustering by fast search) klasterləşmə alqoritmlərinə BGV sxemini tətbiq etmişdir. Bundan əlavə, onlar bulud mühitində fərdi verilənlərin şifrələnməsi üçün BGV-nin istifadəsilə məxfiliyi təmin edən iki dərin hesablama modeli hazırlamışdılar [1, 12, 13].

A. Rəhmani və həmkarları təkamül kriptografiyası və TSZ sxemini birləşdirən yeni çoxlaylı metod təklif etmişlər. Bu metodlar şifrələnmiş BV-nin təhlükəsizliyini yüksək səviyyədə təmin etməklə bir-birini tamamlayırlar. Eyni zamanda, onlar orijinal metodun şifrlənmiş mətninin uzunluğunu artırır və emal və analiz zamanı şifrlənmiş mətnlərin istifadə edilməsinə imkan verir [14].

Lakin homomorfik şifrələmə sxemlərində küyə nəzarət etmək çətinidir və bulud mühitində aşağı səmərəliliyə malik olurlar. Belə ki, homomorfik şifrələmə bəzi tətbiqi sistemlərin tələblərinə cavab vermir.

b) Təhlükəsiz çoxpartiyalı hesablama (secure multiparty computation, SMC): SMC sxemi ilk dəfə 1982-ci ildə A.C.Yao-nun tədqiqatlarında təklif olunmuşdur. Bu sxem tərəflərə paylanmış bulud mühitində öz fərdi (gizli) girişləri ilə funksiyaları hesablamağa imkan verir. Son illər təhlükəsizlik məsələləri üçün SMC metoduna əsaslanan yeni sxemlər təklif edilmişdir.

A. Patra və həmkarlarının [15] təklif etdiyi təhlükəsiz asinxron çoxpartiyalı hesablama (asynchronous multiparty computation) sxemi statistik olaraq təhlükəsiz və asinxronlaşdırıla bilən gizli paylaşmanı təmin edir.

A.Y. Sarhan və S.Carr [16] tərəfindən təklif edilmiş təhlükəsizlik sxemi (self-protection data scheme) bulud mühitində verilənlərin sahiblərinə kənar istifadəçilərin ötürdüləri verilənlər üzərində mütləq nəzarətə malik olmasına imkan verir. Müəlliflər giriş nəzarətin təhlükəsizliyi məqsədilə atributlar əsasında şifrələmə, açarları idarəetmə üçün RSA, verilənlərin özünü qoruması üçün aktiv verilənlər paketləri (active data bundles) və trafikinin idarə edilməsi üçün müstəqil mobil agentləri kimi dörd inkişaf etmiş texnologiyaları birləşdirmişdir.

[17]-də istifadəçi verilənlər bazasının təhlükəsizliyinin təmini üçün gizli açarın paylaşılmasında SMC sxemini istifadə edən çoxpartiyalı paylaşma sistemi təklif edilmişdir.

[18]-də çoxmənbəli verilənlərin təhlükəsizliyinin analizini dəstəkləmək üçün istifadə edilən gizliliyi qoruyan statistik analiz mühiti, yəni Rmind təqdim edilmişdir.

c) Atributlar əsasında şifrələmə (Attribute-based encryption, ABE): Atributlar əsasında şifrələmə ilk dəfə, A. Sahai və, B. Waters [19] tərəfindən təklif edilmişdir. Bu üsul verilənlərə təhlükəsiz giriş üçün ən uyğun və populyar şifrələmə üsulu olmuşdur [20] İdentifikasiyaya əsaslanan şifrələmədən fərqli olaraq, ABE-də verilənlərin sahibləri həm açarları, həm də şifrələnmiş mətnləri atributlar dəsti ilə qeyd edirlər (nişanlayırlar). Sonra isə istifadəçilər bu atributlara görə hüquqi istifadəçilərin avtorizasiyasını təsdiq etməlidirlər. Bundan sonra, verilənlər açarın və şifrlənmiş mətnin atributlarına uyğun olaraq yüklənir və şifrələnir.

Ənənəvi ABE şifrəli mətn mexanizminə (ciphertext-policy CP-ABE) və açar mexanizminə (key-policy, KP-ABE) əsaslanan iki tipə malikdir. Bu iki tip əsas etibarilə, giriş protokollarına tətbiq edilən üsula görə fərqlənir. CP-ABE sxemində giriş protokolu homoloq şifrəli mətnlə yerləşdirilir. Əksinə, KP-ABE sxemində giriş protokolları istifadəçilərin gizli açarları ilə əlaqəlidir [1].

2) Verilənlərin Anonimlik Metodu

Verilənlərin anonimliyi gizliliyin qorunması üçün digər bir əhəmiyyətli texnologiyadır. Bu halda bədnəyyətli gizliliyi özündə saxlayan verilənləri əldə etsə də, açar sahənin qiyməti gizli olduğundan ilkin dəqiq verilənləri əldə edə bilmir. Lakin, BV mühitində bədnəyyətli birdən çox mənbələrdən verilənlər əldə edə bilər, daha sonra bir mənbənin verilənlərini digər bir mənbənin verilənləri ilə əlaqələndirə və gizli verilənlərin orijinal mənasını tapa bilər.

B. Giriş Nəzarət Metodu (Access Control Technology)

Giriş nəzarət texnologiyası verilənlərin nəzarət altında birgə istifadəsi üçün səmərəli vasitədir. Lakin BV mühitində istifadəçilərin sayı çoxdur, avtorizasiyalar mürəkkəbdir. Ona görə də verilənlərin nəzarətli paylaşımını reallaşdırmaq üçün yeni texnologiyaların istifadəsinə ehtiyac vardır.

1)Rolların intellektual analizi üsulları (Role Mining technology)

Rollar əsasında giriş nəzarət metodu (Role-based access control, RBAC) geniş istifadəyə malikdir. İstifadəçilərin

razılığını əldə etmək, hüquqların idarə olunmasını sadələşdirmək, gizliliyin qorunmasına nail olmaq üçün icazələrin alınması ilə bağlı istifadəçilərə görə rolu təyin edir. İlk mərhələdə RBAC hüquqlarının idarə edilməsi "yuxarıdan aşağı" rejimini tətbiq etmişdir. Müəssisənin rolları təyin etmək mövqeyinə uyğun olaraq BV sahəsinə tətbiq edildikdə, tədqiqatçılar "istifadəçilər - obyekt" səlahiyyətlərinə əsaslanan "aşağıdan yuxarı" rejiminə keçməyə başladılar. BV sahəsində rolların intellektual analiz üsullarından istifadə edərək, rollar istifadəçinin giriş qeydlərinə əsasən avtomatik olaraq yaradıla, kütləvi istifadəçilər üçün effektiv şəkildə fərdi məlumat xidmətləri təqdim edə bilər. Lakin Role Mining texnologiyası dəqiq, qapalı verilənlərə əsaslanır və BV-yə tətbiq edildikdə dinamik dəyişikliklərin və verilənlər yığımının keyfiyyətinin yüksək olmaması kimi problemlərin həllinə ehtiyac yaranır [10].

2) Risk adaptiv olan giriş nəzarət metodu (Risk Adaptive Access Control)

BV sahəsində təhlükəsizlik üzrə inzibati kifayət qədər təcrübəyə malik olmaya, istifadəçilərin əldə edə biləcəyi verilənləri düzgün müəyyən etməyə bilər. Bu problemin həlli üçün risklərə adaptiv olan giriş nəzarət metodundan istifadə olunur. Risklərə adaptiv giriş nəzarətə nail olmaq üçün statistik metodlardan və informasiya nəzəriyyəsindən istifadə etməklə *kvant alqoritm*i müəyyən edilə bilər. Eyni zamanda, BV mühitində riski təyin etmək və kəmiyyətə qiymətləndirmək daha çətindir [10].

C. Verilənlərin Mənşəyi Texnologiyaları (Data Provenance)

Hələ BV konsepsiyasının meydana gəlməsindən əvvəl verilənlərin mənşəyi texnologiyaları (Data Provenance) verilənlər bazasında geniş şəkildə araşdırılmışdır. Verilənlərin mənşəyi metodu nişanə (label) əsaslanır. Nişanə vasitəsilə hansı verilənin mənşə olduğunu müəyyən etmək və nəticənin düzgünlüyünü asanlıqla yoxlamaq və ya məlumatları minimum dəyərle yeniləmək mümkündür. Lakin BV-nin təhlükəsizliyi və gizliliyinin qorunması üçün bu texnologiya 1) gizliliyin qorunması və verilənlərin mənşəyi arasında balans; 2) verilənlərin mənşəyi texnologiyasının özünün təhlükəsizliyinin qorunması kimi iki məsələni həll etməlidir.

NƏTİCƏ

Böyük verilənlər iqtisadi və sosial inkişaf üçün yeni bir vasitədir, iqtisadi əməliyyatlara, həyat tərzinə və milli idarəetmə bacarıqlarına gətikdə daha çox təsir edir. BV-nin həcmi fasiləsiz olaraq artdıqca onun təhlükəsizlik və gizlilik problemləri də artır. Big data texnologiyaların informasiya təhlükəsizliyi və gizliliyinə risklərin olması bu texnologiyaların tətbiqinə və inkişafına mane olur, imkanlarını məhdudlaşdır. Tədqiqatlardan da göründüyü kimi böyük həcmli verilənləri idarə etmək üçün bu günə qədər hazırlanmış alətlər və texnologiyalar verilənlərin təhlükəsizliyini və gizliliyini təmin etmək üçün kifayət qədər effektiv deyildir. Ona görə də BV-nin təhlükəsizliyinə böyük əhəmiyyət verilməli, təhlükəsizlik texnologiyaları tədqiq olunmalı və inkişaf etdirilməlidir. Böyük verilənlərin paylanmış saxlanması, pərakəndə idarəetmə, platformalar arasında paylanması və

digər xüsusiyyətləri üçün təhlükəsiz şifrələmə və etibarlı hesablama texnologiyaları işlənilməlidir.

Eyni zamanda, BV-nin açıq olması verilənlərin məxfiliyi riskini artırdığından böyük verilənlərin təhlükəsizliyinin inkişaf strategiyaları və etibarlı təhlükəsizlik sistemlərinin işlənilməsinə ehtiyac vardır.

Beləliklə, Big data inkişaf etməkdə olan bir texnologiyadır və onun təhlükəsizlik risklərinə zəmanət vermək qeyri-mümkündür. Odur ki, təhlükəsizlik texnologiyalarının səmərəliliyinin yaxşılaşdırılması gələcək illərdəki tendensiyalardan biri olaraq qalacaqdır.

ƏDƏBİYYAT

- [1] R. Bao, Z. Chen and M. S. Obaidat, "Challenges and techniques in Big data security and privacy: A review," Security and Privacy, vol. 1, no. 4, 2018, pp. 1-8.
- [2] Fatima-Z. Benjelloun and A. L. Ayoub, "Big Data Security: Challenges, Recommendations and Solutions" Handbook of Research on Security Considerations in Cloud Computing, 2015, pp. 301-313.
- [3] R. Alguliyev, Imamverdiyev Y. Big Data: Big promises for information security / Proceedings of the IEEE 8th International Conference on Application of Information and Communication Technologies (AICT), Astana, Kazakhstan 15-17 October, 2014, pp.216-219.
- [4] R. M. Əliyev, M. Ş. Hacırahimova and A.S. Əliyeva, "Big data-nin aktual elmi-nəzəri problemləri," İnformasiya cəmiyyəti problemləri, №2, 2016, səh. 37-49.
- [5] Д. Пудов, "Проблемы безопасности больших данных," Открытые системы. СУБД, № 04, 2017, <https://www.osp.ru/os/2017/04/>
- [6] R.Əliyev, F.Abdullayeva Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi // İnformasiya Texnologiyaları Problemləri, №1, 2013, səh. 3-14.
- [7] Cloud security alliance. Expanded Top Ten Big Data Security and Privacy Challenges, 2013, <https://downloads.cloudsecurityalliance.org/>
- [8] M. Ş. Hacırahimova. "Big Data" texnologiyaları və informasiya təhlükəsizliyi problemləri, İnformasiya texnologiyaları problemləri, №1, 2016, səh. 49-56.
- [9] P. S. Yosepu, "A Study on Security and Privacy in Big Data Processing," International Journal of Innovative Research in Computer, vol. 3, no. 12, 2015, pp. 12292-12296.
- [10] Z. Gang, "Big Data and Information Security," International Journal of Computational Engineering Research, vol. 5, no. 6, 2015, pp. 17-21.
- [11] C. A. Gentry, Fully Homomorphic Encryption Scheme, Palo Alto, USA: Stanford University; 2009, 199 p.
- [12] Q. Zhang, L.T. Yang, Z. Chen et al., "PPHOPCM: privacy-preserving high-order possibilistic c-means algorithm for Big data clustering with cloud computing", IEEE Trans Big Data, 2017, pp.1-11.
- [13] Q. Zhang, L.T. Yang, Z. Chen, "Privacy preserving deep computation model on cloud for Big data feature learning," IEEE Trans Computing, vol. 65, no.5, 2016, pp.1351-1362.
- [14] A. Rahmani, A. Amine and R.H. Mohamed, "A multilayer evolutionary homomorphic encryption approach for privacy preserving over Big data," International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Shanghai, China: IEEE, 2014, pp.19-26
- [15] A. Patra, "Choudhury A, Rangan CP. Efficient asynchronous verifiable secret sharing and multiparty computation," J. Cryptol., vol. 28, no. 1, 2015, pp. 49-109
- [16] A.Y. Sarhan and S. Carr, "A highly-secure self-protection data scheme in clouds using active data bundles and agent-based secure multi-party computation," International Conference on Cyber Security and Cloud Computing. Columbia University, New York, IEEE, 2014, pp. 228-236.
- [17] Dyadic Security White Paper, 2017, 5 p., <https://www.dyadicsec.com/>.

- [18] D. Bogdanov, L. Kamm, S. Laur, et al., “Rmind: a tool for cryptographically secure statistical analysis”, IEEE Trans. Depend Secure Computing, 2016, pp.1-14.
- [19] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” International Conference on Theory and Applications of Cryptographic Techniques, French Riviera, France: Springer-Verlag, 2005, pp.457-473.
- [20] J.R. Bertini, M. Carmo Nicoletti and L. Zhao, “Attribute-based decision graphs: a framework for multiclass data classification,” Neural Networks, vol. 85, 2017, pp. 69-84.

SECURITY PROBLEMS OF BIG DATA TECHNOLOGY AND THEIR SOLUTION WAYS

Makrufa Hajirahimova¹, Aybeniz Aliyeva²

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

¹*makrufa@science.az*, ²*aliyeva.a.s@mail.ru*

Abstract -- The formation of Big data technologies create new challenges for data security and privacy. Traditional technologies and methods are not appropriate and efficient for solving these problems. In this article has been researched security problems of big data.

The technical solutions that used to ensure the security and privacy of big data have been analyzed and their current status has been reviewed.

Keywords -- Big data; data security; infrastructure security; data privacy

Plagiatlığın növləri və ondan qorunmağın üsulları

Rəhilə Həsənova¹, Firudin Əsgərov²

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

¹rahasanova@gmail.com, ²firudinasgarov@gmail.com

Xülasə— Məqalədə plagiatlıq və onun növləri araşdırılmış, antiplagiat sistemləri, onların əsas iş prinsipləri haqqında məlumat verilmişdir. Burada həmçinin Azərbaycan dilinə xas xüsusiyyətləri nəzərə alınmaqla təkliflər irəli sürülmüşdür.

Açar sözlər — plagiatlıq; antiplagiat sistemləri; PlagAware; PlagScan

I. GİRİŞ

Elmi informasiyanın sürətlə artdığı müasir dövrdə informasiyanın plagiat olub-olmamasını müəyyənləşdirən antiplagiat sistemlərinin işlənməsi aktual mövzulardandır.

Hazırda informasiya mənbələri daha çox elektron vasitələrdə mövcud olduğundan plagiatlıq da “elektron cinayət” kimi qiymətləndirilir. Təbii ki, bu halda plagiatlıqla mübarizənin əsas vasitəsi informasiyadan “qanuni” yolla istifadə imkanları yaradan yeni texnologiyaların yaradılması və istifadəsi başa düşülməlidir [1].

Plagiatlıq başqa müəllifə məxsus fikir və ideyaların öz adından təqdim olunmasına deyilir. Bu hadisə oğurluq və piratçılıqla sıx əlaqədardır. Plagiatlıq kompüter virusları, spamlar, fişinq və s. kimi kibercinayətkarlığın bir növü hesab olunur. Plagiatlıq İnternetdən, kitabdan, jurnaldan və s. birbaşa mətnin köçürülməsi ilə və yaxud az sayda dəyişiklik etməklə baş verir [2].

Turnitin, Plagiarism və Research Resources antiplagiat sistemlərinə görə plagiatlıq aşağıdakı kimi təsnifləşdirilir [3-5]:

- Başqasının işinin özünüki kimi təqdim edilməsi;
- Başqasına məxsus fikir və ideyalara istinad etmədən özünüki kimi ifadə edilməsi;
- Başqasını ideyasının sitat şəklində yazılmaması;
- Sitatın mənbəsi haqqında yalnız məlumatın verilməsi;
- Sözləri dəyişərək mənbəyə istinad etmədən əsas strukturun olduğu kimi köçürülməsi;
- İstinad edilib-edilməməsindən asılı olmayaraq materialın əksər sözlərinin və ideyaların mənbələrdən istifadə edilməsi.

Ümumiyyətlə plagiatlığı iki əsas sinfə bölmək olar:

1. Mətn plagiatlığı. Bu tip plagiatlığı adətən elmi müəssisələrdə tələbələr və tədqiqatçılar həyata keçirir. Bu zaman plagiatlıq mətni eynilə orijinal məqalənin, tezis, elmi işin mətninə oxşayır.

2. Mənbə kodu plagiatlığı. Bu tip plagiatlıq yenə də tələbələr tərəfindən yerinə yetirilir, belə ki, onlar mənbəni qeyd etmədən oradakı bütün mətni və ya hər hansı bir hissəsini kod dəyişməklə köçürürlər. Bu tip plagiatlığı təyin etmək çətin olur.

Mətn və mənbə kodu plagiatlığını 2 üsulla aşkarlamaq mümkündür: fiziki və avtomatik aşkarlama.

Fiziki aşkarlama o deməkdir ki, ekspert materialı özü yoxlayaraq onun plagiat olub-olmaması haqqında qərar verir. Məsələn, müəllim tələbəyə verdiyi kurs işini özü şəxsən yoxlayır və onun orijinallığını qiymətləndirir. Lakin bu üsul çoxsaylı sənədlərin yoxlanması üçün effektiv deyildir, çünki bu proses müəllimdən çox vaxt və əmək tələb edir.

Avtomatik aşkarlama kompüter vasitəsilə həyata keçirilir, belə ki, avtomatik plagiatlığı aşkarlayan çoxlu sayda proqram təminatları mövcuddur: PlagAware, PlagScan, Check for Plagiarism, iThenticate, PlagiarismDetection, Academic Plagiarism, The Plagiarism Checker, Urkund, Docoloc.

II. PLAGİATLIĞIN NÖVLƏRİ

Plagiatlığın aşağıdakı növləri vardır [5]:

I tip plagiatlıq: Birbaşa köçürmək (eng. The Direct Copy). Müəllifin başqasının fraza, abzas və ya bütün səhifəsini sözbəsöz köçürərək öz adından ifadə etməsidir. 5 milyarda yaxın veb səhifənin içərisindən hər hansı bir sətiri istinad etmədən köçürmək onun gələcəkdə aşkarlanmayacağı demək deyildir. Son dövrlərdə bir çox elmi müəssisələr tədqiqatçılardan çap edilmiş əsərlərinin elektron variantını tələb edir, belə ki, onlar materialın plagiat olub-olmamasını müəyyənləşdirmək üçün axtarış aparırlar.

Həlli: Mənbəni ədəbiyyat siyahısına daxil etmək və istifadə olunmuş mətnin istinadını əlavə etmək lazımdır.

II tip plagiatlıq: Minimalist (eng. The Minimalist). Mənbə materialdan bir neçə söz və ya fraza dəyişdirilir, lakin əsas məzmun, struktur eynilə qalır. Fikri bu cür parafraz etmək onun orijinallığı demək deyil.

Həlli: Mənbəni ədəbiyyat siyahısına daxil etmək və yekun məzmunu öz sözlərinizlə ifadə edərək mətn daxili istinadlar vermək lazımdır.

III tip plagiatlıq: Birləşdirmək (eng. The Combo). Bunun gələcəkdə üstü açılmayacaq düşüncəsi ilə istifadə edilmiş informasiyanın müəyyən hissəsinə istinad verilir, digər hissələr isə istinadsız köçürülür. Bəzən tədqiqatçı elə düşünür

ki, hamıya məlum ümumi informasiyaya istinad etmək lazım deyil.

Həlli: Bir qayda olaraq, hətta ümumi bilik hesab olunmayan bütün informasiya mənbələrinə istinad olunmalıdır.

IV tip plagiatlıq: Qarışdırmaq (eng. The Quilt). Bəzən müəlliflər bir neçə mənbədən istifadə etmələrinə baxmayaraq həmin mənbələrdən yalnız birinə istinad edirlər. Bu halda tədqiqatçı bir neçə müəllifin informasiyasını oğurlayaraq onların bir hissəsinə istinad etmiş olur. Bəlkə də bu halda tədqiqatçı materialı olduğunu iddia edərək plagiatçılıq etmir, lakin yanlış olaraq başqa mənbəyə istinad vermiş olur.

Həlli: İstifadə olunmuş mənbələrin hər birinə individual olaraq istinad etmək lazımdır. Təqdim edilmiş informasiyanın struktundan asılı olaraq bunu hər bir mənbə üçün ayrıca və ya hamısına ümumilikdə istinad şəklində vermək olar.

V tip plagiatlıq: Tutuquşu (eng. The parrot). Əksər tədqiqatçıların etdiyi yanlışlıq: onlar istifadə etdiyi mənbədən əsas strukturu və ideyanı köçürürlər. Müəlliflər istifadə etdikləri mənbədəki informasiyanı olduğu kimi köçürümlər, əsas fikri öz sözləri ilə ifadə edirlər və düşünürlər ki, bu plagiatlıq deyil. Başqasına məxsus olan əsas fikir və ideyanın öz sözləri ilə ifadə olunması plagiatlıq faktıdır.

Həlli: Öz tədqiqat istiqamətini seçməklə, özünəməxsus nəticələrin əldə edilməsi.

VI tip plagiatlıq: Təhlükəli (eng. The Insecure). Bu vəziyyəti “Kiçik su pərisi kompleksi” də adlandırırlar, belə ki, tədqiqatçı öz ideyasından imtina edərək yalnız başqalarının ideyasından istifadə edir. Yəni müəllif özünəməxsus ideyalardan deyil, tamamilə başqa müəlliflərə aid mənbələrə istinad olunan fikirlərdən ibarət məqalə yazır. Lakin, bu açıq şəkildə plagiatlıq hesab olunmasa da gələcək nəticələrə təhlükəli təsir göstərə bilər.

Həlli: Yadda saxlamaq lazımdır ki, akademik cəmiyyət sırf müəllifə aid olan ideyaları qəbul etmək istəyir. Buna görə də məqalələrdə öz şəxsi ideyalardan istifadə edilməlidir.

VII tip plagiatlıq: Dənizdə itmək (eng. The Lost-at-Sea). Bu vəziyyətlə məqalənin ədəbiyyat siyahısındakı mənbələrin sayına tələb qoyulduğu zaman rast gəlmək olar. Məsələn, minimum 25 mənbənin adını qeyd etmək tələb olunduğu üçün müəllif 18 mənbədən istifadə etdiyi halda, siyahını süni şəkildə artırır. Hətta istifadə olunmamış, lakin ədəbiyyat siyahısında adı çəkilən mənbəyə istinad və ya uyğun olmayan mənbəyə istinad plagiatlıq hesab olunur.

Həlli: Bunu yalnız istifadə olunmuş mənbələrin adını ədəbiyyat siyahısına daxil etməklə çox sadə şəkildə həll etmək olur. Bu məsələ elektron ünvana da aiddir, belə ki, əgər mənbənin göstərdiyi sayt daha əlverişli deyilsə, onu yeniləmək lazımdır.

VIII tip plagiatlıq: Özünü izləmək (eng. The Self-Obsessed). Müəlliflər düşünür ki, ideyaların özlərinə məxsus olması, bu ideyaların müxtəlif vaxtlarda, fərqli jurnallarda istifadə edilməsinə haqq qazandırır. Yazılmış məqalənin

akademik cəmiyyətdə yeni formada təqdim edilməsi belə özünəplagiatlıq hesab olunur.

Həlli: Müəllif əvvəlki məqalələrini digər mənbələr kimi diqqətlə oxumalı və yeni ideyalardan istifadə etməlidir.

III. ANTIPLAGIAT SİSTEMLƏRİ HAQQINDA

Antiagiat proqramları mətnin unikallığının qiymətləndirilməsi üçün işlənilib hazırlanmış onlayn sistemlərdir. Antiagiat sistemləri bir neçə əlamətə görə beş ulduzlu şkala ilə qiymətləndirilir [6]:

1. Verilənlər bazasının yoxlanması (eng. Database Checking). Bu yoxlama həm İnternet üzərindən, həm də lokal rejimdə verilənlər bazalarında axtarış etməyə imkan verir.
2. İnternet üzərindən yoxlama (eng. Internet Checking). Burada adi axtarış sistemi vasitəsilə cari sənədlə İnternetdə mövcud olan bütün növ sənədlərin müqayisəsi aparılır.
3. Nəşrin yoxlanması (eng. Publications Checking). Bu yalnız akademik bazalarda (Web of Science, Scopus və s.) mövcud olan sənədlərin – məqalə, tezis, kitab, jurnal və s. yoxlanmasıdır.
4. Fərqli sənədlərin eyni anda müqayisəsi (eng. Multiple Document Comparison). Bu xüsusiyyət bir neçə sənədi eyni anda paralel yoxlamağa imkan verir.
5. Müxtəlif əlifba və dillərin dəstəklənməsi (eng. Supported Languages). Burada müxtəlif dillərdə və əlifbalarda yazılmış mətnlərin yoxlanması həyata keçirilir.
6. Cümlə quruluşu və sinonimlər üzrə yoxlama (eng. Synonym and Sentence Structure Checking). Bu xüsusiyyət cümlə quruluşuna və sinonimlərin istifadəsinə görə sənədləri müqayisə edir.

Aşağıdakı cədvəldə bu əlamətlərə görə PlagAware, PlagScan, iThenticate, CheckFor Plagiarism və Plagiarism detecting antiplagiat sistemlərinin beş ulduzlu şkala ilə qiymətləndirilməsi təsvir edilmişdir [7].

Cədvəl 1. Antiplagiat sistemlərinin əlamətlərə görə qiymətləndirilməsi

Əlamətlər	PlagAware	PlagScan	iThenticate	CheckFor Plagiarism.net	Plagiarism detecting.org
Database Checking	*****	*****	*****	*****	*****
Internet Checking	*****	*****	*****	*****	*****
Publication Checking	*****	*****	*****	****	****
Multiple document comparison	*****	*****	*****	*****	*****
Multiple languages support	*****	*****	*****	*****	*****
Sentence structure and synonym checking	****	**	****	*****	**

NƏTİCƏ

Mövcud antiplagiat sistemlərində çoxdillilik prinsipləri gözlənilsə də, hələlik dilin xüsusiyyətlərindən asılı olmayan

universal antiplagiat sistemləri yaradılmamışdır. Buna görə də, hazırlanacaq antiplagiat sistemləri dilin xüsusiyyətlərini nəzərə almalıdır. Azərbaycan dili üçün aşağıdakı xüsusiyyətləri sadalamaq olar:

Antiplagiat sistemlərinin yalnız simvollarla deyil Screenshot vasitəsilə şəklini çəkib mətnləri oxşatmaqla qiymətləndirmək və ya mətnlərin avtomatik avtoreferatının çıxarılması və onların yoxlamaq.

Latın və kiril əlifbalarına uyğun mümkün variasiyaların yoxlanması, məsələn latın “o” və kiril “о” hərflərini yenidən dəyişərək yoxlama aparmaq. ASCII və Unicode əks kodlaşdırmasında mətni yenidən yoxlamaq.

ƏDƏBİYYAT

- [1] R.Əliquliyev, N.Ağayev, R.Alıquliyev, “Plagiatlıqla mübarizə texnologiyaları”, Bakı: İnformasiya Texnologiyaları nəşriyyatı, 2015, 165 s.
- [2] Encyclopedia Britannica, <http://www.britannica.com/EBchecked/topic/462640/plagiarism> (last access February 7, 2011)
- [3] Education with Integrity, Turnitin.com
- [4] What is Plagiarism?, 2017, plagiarism.org

- [5] M Asim, M. Hussam, V. Snasel, “Overview and Comparison of Plagiarism Detection Tools”, Dataso 2011, pp. 161–172.
- [6] How Do I Know If I'm Plagiarizing?
https://www.scribendi.com/advice/how_do_i_know_if_im_plagiarizing.en.html
- [7] Reliablex plagiarism detector, Plagiarismdetecting.org

TYPES OF PLAGIARISM AND METHODS OF PROTECTION

Rahila Hasanova¹, Firudin Asgarov²

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

Abstract – The article examines plagiarism and its types, provides information on anti-plagiarism systems, their basic principles of operation. Taking into account the characteristics of the Azerbaijani language, suggestions are put forward .

Keywords – plagiarism; anti-plagiarism systems; PlagAware; PlagScan

NoSQL verilənlər bazalarında təhlükəsizlik problemləri haqqında

Məkrufə Hacırahimova¹, Mərziyə İsmayılova²

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

¹makrufa@scisence.az, ²imarziya@google.com

Xülasə— Məqalə böyük verilənlər (“Big data”) və NoSQL verilənlər bazalarında təhlükəsizlik problemlərinə həsr olunmuşdur. Böyük həcm, sürət və müxtəliflik kimi xüsusiyyətlərlə xarakterizə olunan böyük verilənlərdə təhlükəsizlik və məxfilik ciddi problemlər yaradır. Ənənəvi təhlükəsizlik modelləri bu cür geniş miqyaslı verilənlərlə işləyən zaman çətinliklərlə rastlaşır. Məqalədə böyük verilənlər və NoSQL verilənlər bazalarında təhlükəsizlik və məxfilik problemləri araşdırılmışdır.

Açar sözlər: böyük verilənlər, təhlükəsizlik, məxfilik, NoSQL, giriş nəzarət

I. GİRİŞ

Böyük verilənlər, daha səmərəli qərar qəbul etmə, informasiyanın aşkarlanması və proseslərin optimallaşdırılması üçün yeni emal formaları tələb edən böyük həcm, yüksək sürət və müxtəliflik kimi xüsusiyyətlərə malik informasiya resurslarını ifadə edir. Bəzən 3V kimi ifadə edilən xüsusiyyətlərinə görə ənənəvi verilənlər bazalarının idarəetmə alətlərindən istifadə etməklə böyük verilənləri emal etmək çox çətinidir. Yeni bir çağırış - böyük həcmli verilənlərin geniş istifadəsi üçün yeni texnologiyalar və sistemlərin işlənilməsi hazırlanmasıdır. Bu məqsədlə bir çox informasiya idarəedilməsi arxitekturları işlənmişdir [1, 2]. Bir çox sahələrdə yeni texnologiyaların inkişafı və böyük verilənlərdən istifadənin artması böyük verilənlərdə təhlükəsizlik və məxfilik kimi problemlərin yaranmasına səbəb olmuşdur. Böyük verilənlərə dair çoxlu sayda təhlükəsizlik və məxfilik problemləri mövcuddur [2 - 8].

İşin məqsədi böyük verilənlər və NoSQL verilənlər bazalarında təhlükəsizlik və məxfilik problemlərinin araşdırılmasından ibarətdir.

II. BÖYÜK VERİLƏNLƏRDƏ TƏHLÜKƏSİZLİK PROBLEMLƏRİ

[7-9]-da böyük verilənlər üçün təhlükəsizlik və məxfilik üzrə on təhlükəsizlik problemi verilmişdir. Bu problemlər aşağıdakılardır:

- Paylanmış proqramlaşdırma strukturunda təhlükəsiz hesablamlar;
- Verilənlərin təhlükəsiz saxlanması və tranzaksiya jurnalı;

- Girişə granular nəzarət;
- Girişin yoxlanması/filtirlənməsi;
- Real vaxt rejimində təhlükəsizliyin monitorinqi;
- Məxfiliyi saxlamaqla miqyaslama, verilənlərin əldə edilməsi və analizi;
- Kriptografiya ilə həyata keçirilən girişə nəzarət və təhlükəsiz kommunikasiya;
- Qranular auditlər;
- Qeyri-relyason verilənlər bazaları üçün ən yaxşı təhlükəsizlik təcrübəsi;
- Verilənlərin mənşəyi.

Bu problemlərdən bir neçəsinin şərh verilmişdir.

Paylanmış proqramlaşdırma strukturunda təhlükəsiz hesablamlar problemi. Bu MapReduce funksiyasında təhlükəsizliyi müzakirə edən bir problemdir. Verilənlərin təhlükəsiz saxlanması və tranzaksiya jurnalı verilənlər anbarına icazəsiz girişin qarşısının alınmasını və girişin təmin edilməsinin yeni mexanizmlərini müzakirə edir.

Girişə granular nəzarət problemi. Böyük verilənlərdə daha bir problem girişə granular nəzarət problemidir. Problem girişə ehtiyacı olmayan istifadəçilər tərəfindən verilənlərə girişin qarşısının alınmasıdır. Bu halda girişə nəzarətin ənənəvi modeli böyük verilənlərlə işləyərkən çətinliklə rastlaşır. [2 - 4, 12]-də böyük verilənlərin emalında girişə nəzarət üçün bir neçə mexanizm təklif edilmişdir.

Verilənlərin mühafizə və girişə nəzarət problemi. Böyük verilənlərdə təhlükəsizlik problemləri arasında verilənlərin mühafizəsi və girişə nəzarət daha mühüm problemlərdən sayılır. [13]-də NoSql VB-lər üçün qaydaya əsaslanan girişə nəzarətin (*Role Based Access Control, RBAC*) ənənəvi modellərini genişləndirmək yolu ilə girişin idarə edilməsi modeli təqdim edilmişdir. [14]-də NoSQL-in geniş istifadə olunan Cassandra və MongoDB VB-nin təhlükəsizlik problemləri müzakirə olunmuş, onların xüsusiyyətləri və təhlükəsizlik problemləri şərh edilmişdir. Cassandra və MongoDB üçün qeyd edilən əsas problemlər aşağıdakılardır:

- verilənlər faylının şifrələnməməsi;
- server və müştəri arasında zəif autentifikasiya;
- sadə autentifikasiya;
- SQL-inyeksiya və DOS hücumuna qarşı həssaslıq.

Həm də onların hər ikisinin RBAC və ətraflı avtorizasiyanı dəstəkləmədiyi bildirilir. [6]-da NIST riskləri

idarə edilməsi standartları nəzərdən keçirilmiş və təhlükələrin mənbəyi, təhlükə hadisələri və zəifliklər müəyyən edilmişdir. Burada böyük verilənlərdə müəyyən olunmuş həssaslıqlar aşağıdakılardır:

- təhlükəli hesablama;
- girişin yoxlanılması/filtirlənməsi;
- girişə granular nəzarət;
- təhlükəli verilənlərin saxlanması və kommunikasiya;
- verilənlərin əldə edilməsinin məxfiliyinin qorunması və analizi.

Bəzi hallarda böyük verilənlərdə semantik məzmun əsasən girişə nəzarət modelinə ehtiyac duyulur. Böyük verilənlərin paylaşılmasında giriş nəzarətini tətbiq etmək üçün, məzmun əsaslanan giriş nəzarəti (*Content-Based Access Control, CBAC*) modeli verilənlərin məzmunundan istifadə etməklə təqdim olunur [2]. Bu halda, verilənlərin semantik məzmunu girişə nəzarət qərarının qəbul edilməsində əsas rol oynayır. CBAC məzmunların oxşarlığı əsasında istifadəçilərin qeydiyyat verilənləri və verilənlər arasında girişə nəzarət üzrə dinamik qərar qəbul edir [2].

[3] və [4]-də böyük verilənlərdə təhlükəsizliyi təmin edən digər bir metod - atributların qarşılıqlı əlaqəsi metodologiyası təklif edilmişdir. Bu metodologiyanın əsas məqsədi dəyərli informasiyaları mühafizə etməkdən ibarətdir. Ona görə də böyük verilənlərdə informasiyanın əldə edilməsi üçün açar elementi kimi atributların relevantlığına diqqət verilir və güman edilir ki, daha yüksək relevantlığa malik atribut digər atributlardan daha dəyərlidir. [3]-də modelin atributları və onlar arasındakı qarşılıqlı əlaqə üçün qrafdan istifadə edilir. Atributlar qovşaq kimi ifadə olunur və hər bir qovşaq arasında əlaqələr tillərlə göstərilir. Metod bu qraflardan mühafizə olunan atributların seçilməsini təklif edir. [4]-də təklif olunan metodda əvvəlcə verilənlərin bütün atributları əldə edilir, sonra xassələri ümumiləşdirilir. Daha sonra atributlar arasında korrelyasiya müqayisə olunur və qarşılıqlı əlaqə qiymətləndirilir. Nəhayət korrelyasiya qiymətləndirilmələrinə əsaslanaraq təhlükəsizlik tədbirləri üzrə tələb olunan seçilmiş atributlar mühafizə olunur.

Bulud saxlama infrastrukturunda böyük verilənlərin girişinin idarə edilməsi üçün uyğun bir metod atribut əsasında şifrələmədir. [2]-də buludda böyük verilənlərin təhlükəsizliyini təmin etmək məqsədi ilə atribut şifrələmə əsasında effektiv girişin sxemi təklif olunur.

Hadoop böyük verilənlərin saxlanması və emalı üçün açıq kodlu strukturdur. Verilənlərin bir neçə qovşaqda saxlanması üçün Hadoop paylanmış fayl sistemindən (*Hadoop Distributed File System, HDFS*) istifadə edir. HDFS istifadəçinin autentikliyi yoxlamır, verilənləri şifrələmir və məxfiliyi təmin etmir. HDFS güclü təhlükəsizlik modelinə malik deyil və istifadəçilər birbaşa heç bir icazə olmadan qovşaqlarda saxlanan verilənlərə giriş əldə edə bilər [10]-da Hadoop-un bir neçə təhlükəsizlik riskləri qeyd edilmiş və verilənlərin saxlanması üçün girişin idarə edilməsinin yeni sxemi təklif olunmuşdur.

III. NOSQL VERİLƏNLƏR BAZALARINDA TƏHLÜKƏSİZLİK PROBLEMLƏRİ

NoSQL (*Not Only SQL*) bu gün böyük verilənlər aləminin əsası hesab olunur və miqyaslı bilən müasir verilənlər bazaları (VB) üçün istifadə edilir. Miqyaslama –verilənlərin emalı baxımından tələbat artdıqda sistemin məhsuldarlığını artırma qabiliyyətidir. Böyük verilənlərin emalının dəstəklənməsi üçün platformalar miqyaslanmanın iki növünü: üfüqi və şaquli miqyaslama formasını nəzərdə tutur:

Üfüqi miqyaslamada iş yükü bir çox serverlər üzrə paylanır. Miqyaslanmanın bu növündə buraxılış qabiliyyətini artırmaq üçün bir çox sistem birləşir.

Şaquli miqyaslamada daha çox yaddaşlı prosessorlar və daha sürətli qurğular bir serverdə quraşdırılır [15].

Bu gün çoxlu sayda NoSQL həllər yaradılmışdır. [14]-də NoSQL-in əsas üstünlükləri aşağıdakı kimi təqdim edilmişdir: 1) sürətli şəkildə verilənləri oxumaq və yazmaq, 2) kütləvi saxlama, 3) asan genişlənmə, 4) aşağı qiymət. NoSQL sistemlərini dəstəkləyən verilənlər modeli açar-qiymət, sütun, sənəd və qraf kimi təsnif edilmişdir. Bu gün çoxlu sayda MongoDB, CouchDB, Redis, Voldermort, Cassandra, Hypertable, Hbase və Neo4j kimi. NoSQL həllər yaradılmışdır. NoSQL VB-lər verilənlər modelinə görə aşağıdakı kimi qruplaşdırılır [16-19]:

- Açar-qiymət - Cassandra, Voldemort, Redis, DynamoDB;
- Sənəd - MongoDB, CouchDB, DynamoDB;
- Sütun - HyperTable;
- Qraf - Neo4j.

MongoDB – sənədə əsaslanan NoSQL VB-dir və sənədlərin toplanmasını idarə edir. MongoDB mürəkkəb verilənlər tipini dəstəkləyir və böyük verilənlərə yüksək sürətli girişi təmin edir. MongoDB çevik, güclü, sürətli və istifadədə sadədir. Bütün verilənlər MongoDB-də mətn şəklində saxlanılır və verilənlər faylı şifrələmək üçün şifrələmə mexanizmi mövcud deyildir [15, 20]. Bu o deməkdir ki, fayl sisteminə giriş imkanı olan istənilən bədənliyyətli istifadəçi fayllardan informasiya əldə edə bilər. O istifadəçi ilə MongoDB klasterləri və daxili avtorizasiya arasında təhlükəsiz əlaqə üçün X.509 sertifikatlı SSL istifadə edir. Lakin paylanmış rejimdə işə salındıqda autentifikasiya və avtorizasiyanı dəstəkləmir. Parollar MD5 heş alqoritmının köməyi ilə şifrələnir. Belə ki, MongoDB daxili skript dili kimi Javascript-dən istifadə etdiyi üçün inyeksiya (*ing. injection*) hücumuna məruz qalma imkanı vardır [14, 20, 21].

CouchDB – sənədə əsaslanan çevik, imtinaya davamlı NoSQL VB-dir. Bu açıq kodlu Apache layihəsidir və o HDFS-dən istifadə edir. CouchDB verilənlərin şifrələnməsini dəstəkləmir, lakin autentifikasiyanı həm parol, həm də *cookie* faylı əsasında dəstəkləyir. Parollar PBKDF2 heş alqoritmını tətbiq etməklə şifrələnir və SSL protokolundan istifadə edərək şəbəkə ilə ötürülür. Bu inyeksiya skriptləri və “xidmətdən imtina” hücumları üçün potensial imkana malikdir [14, 20, 21].

Cassandra – böyük verilənlərin idarə edilməsi üçün açıq kodlu paylanmış saxlandı. Bu Facebook-da istifadə olunan

önəmli bir NoSQL VB-dir. Cassandra çeviklik, yüksək miqyaslama kimi xüsusiyyətlərə malikdir. Cassandra bütün parollar MD5 heş funksiyası ilə şifrələnir, ancaq parollar çox zəifdir. İstənilən bir qərəzli istifadəçi qovşaqlar arasında mübadilədə avtorizasiya mexanizmi olmadığı üçün verilənləri asanlıqla əldə edə bilər. Cassandra “xidmətdən imtina” hücumları üçün açıqdır. Cassandra SQL inyeksiya üçün açıq olan Cassandra sorğu dili (*Cassandra Query Language, CQL*) adlanan sorğu dilindən istifadə edir [14, 16, 19-21].

HBase – Google böyük cədvəli əsasında yaranan və Java-da realizasiya olunmuş açıq kodlu sütun yönümlü VB-dir. O strukturlaşdırılmış və yarı strukturlaşdırılmış verilənləri idarə edir, paylanmış konfigurasiya istifadə edir. Hbase qovşaqlar arasındakı əlaqə üçün SSH (*Secure Shell*) protokolundan istifadə edir. O SASL (*Simple Authentication and Security Layer*) və həm də ACL (*Access Control List*) vasitəsilə istifadəçi avtorizasiyasını dəstəkləyir [20].

NOSQL VERİLƏNLƏR BAZALARININ MÜQAYİSƏSİ

NoSQL VB	Verilənlərin tipi	Autentifikasiya	Avtorizasiya	Verilənlərin məxfiliyi	Audit	Əlaqə protokolu	Hücum üçün potensial imkan
MongoDB	Sənəd	Dəstəklənmir	Dəstəklənmir	Dəstəklənmir	-	SSL	Script inyeksiyası
CouchDB	Sənəd	Dəstəklənir	-	Dəstəklənmir	-	SSL	Script inyeksiyası və DOS
Cassandra	Açar-qiymət	Dəstəklənir	Dəstəklənmir	Dəstəklənmir	Dəstəklənmir	SSL	Script inyeksiyası (CQL)-də və DOS
Hbase	Sütun	Dəstəklənir	Dəstəklənir	Dəstəklənmir	-	SSH	DOS və inyeksiya üçün hesabat yoxdur
HyperTable	Sütun	Dəstəklənmir	-	Dəstəklənmir	-	-	-
Voldemort	Açar-qiymət	Dəstəklənmir	Dəstəklənmir	Dəstəklənir	Dəstəklənmir	-	-
Redis	Açar-qiymət	Kiçik lay	Dəstəklənmir	Dəstəklənmir	Dəstəklənmir	Şifrələnməmiş	-
DynamoDB	Açar-qiymət Sənəd	Dəstəklənir	Dəstəklənir	Dəstəklənmir	-	https	-
Neo4j	Qraf	-	Dəstəklənmir	Dəstəklənmir	Dəstəklənmir	SSL	-

HyperTable – HDFS-də istifadə olunan açıq kodlu yüksək məhsuldarlıq sütun yönümlü VB-dir. O verilənləri böyük cədvəllərdə saxlayır. HyperTable verilənlərin şifrələnməsi və autentifikasiyanı dəstəkləmir. Əgər hər hansı bir server sıradan çıxarsa verilənlər bərpa edilmir. HyperTable inyeksiya hücumları üçün açıq olan HyperTable sorğu dili (*HyperTable Query Language, HQL*) istifadə edir. DOS hücumlarına məruz qalmır [21].

Voldemort – LinkedIn-də istifadə olunan “açar-qiymət” tipli NoSQL VB-dir. Bu tip VB-də verilənlər “açar-qiymət” cütünü şəklində saxlanılır. O, saxlama mexanizmi kimi Berkeley DB-dən istifadə etməklə verilənlərin şifrələnməsini dəstəkləyir. Voldemort autentifikasiya, avtorizasiya auditini dəstəkləmir [22].

Redis – “açar-qiymət” tipli açıq kodlu VB-dir. Redis-də verilənlərin şifrələnməsi dəstəklənmir və bütün verilənlər mətn şəklində saxlanılır. Redisin müştəriləri ilə server arasında əlaqə şifrələnmir. Redis-də kiçik bir səviyyədə autentifikasiyanı təmin edən giriş nəzarət həyata keçirilmir. Redis-də inyeksiya hücumu imkansızdır [21].

DynamoDB – Amazon-da istifadə olunan sürətli və çevik NoSQL VB-dir. O həm “açar-qiymət”, həm də sənəd verilənlər modelini dəstəkləyir [21]. DynamoDB-də verilənlərin şifrələnməsi dəstəklənmir, lakin müştəri və server arasında verilənlərin mübadiləsi https protokolundan istifadə edir. Autentifikasiya və avtorizasiya DynamoDB tərəfindən dəstəklənir [22].

Neo4j - açıq kodlu qraf yönümlü NoSQL VB-dir. Neo4j verilənlərin şifrələnməsini, avtorizasiya və auditini dəstəkləyir. Müştəri və server arasında əlaqə SSL protokoluna əsaslanır [22].

NƏTİCƏ

Böyük verilənlər və NoSQL VB-lərlə işləyən zaman təhlükəsizlik çox önəmlidir. NoSQL VB-lərdən istifadə artdıqca təhlükəsizlik daha ciddi problemə çevrilir. Məqalədə böyük verilənlərdə və NoSQL verilənlər bazalarında (MongoDB, CouchDB, HyperTable, DynamoDB və s.) təhlükəsizlik və məxfilik problemləri şərh edilmişdir. Böyük verilənlərin böyük həcm, sürət və müxtəliflik kimi xüsusiyyətlərindən asılı olaraq ənənəvi təhlükəsizlik modelləri səmərəsizdir. Bəzi tədqiqatçılar böyük verilənlər üçün yeni – giriş nəzarət modelini təqdim etmişdirlər. NoSQL VB-lərin əksəriyyəti verilənlərin şifrələnməsini dəstəkləyir. Bu da təhlükələrin yaranmasına zəmin yaradır. Yuxarıda qeyd edildiyi kimi daha təhlükəsiz VB-yə malik olmaq üçün VB-nin məxfi sahələrinin şifrələnməsi vacibdir. Bəzi VB-lərin inyeksiya üçün zəifliyi var. Onlardan bəziləri autentifikasiya mexanizminə, bəziləri isə zəif autentifikasiya mexanizminə malikdirlər. Bu çatışmazlıqları aradan qaldırmaq üçün güclü autentifikasiya mexanizmləri lazımdır.

Yuxarıda cədvəldə bu müqayisələr təqdim edilmişdir.

ƏDƏBİYYAT

- [1] R.Əliquliyev, M.Hacırahimova “Big data” fenomeni: problemlər və imkanlar // İnformasiya Texnologiyaları Problemləri, 2014, №2, s. 3–16.
- [2] K.Yang, Secure and Verifiable Policy Update Outsourcing for Big Data Access Control in the Cloud, IEEE Transactions on Parallel and Distributed Systems, 2014, Issue 99.
- [3] W.Zeng, Y.Yang, B.Lou, Access control for big data using data content / Proceedings of the IEEE International Conference on Big Data, 2013, pp. 45-47.
- [4] S.Kim, J.Eom, T.Chung, Big Data Security Hardening Methodology Using Attributes Relationship / Proceedings of the IEEE International Conference on Information Science and Applications, 2013, pp. 1-2.
- [5] S.Kim, J.Eom, T.Chung, Attribute Relationship Evaluation Methodology for Big Data Security / Proceedings of the International Conference on IT Convergence and Security (ICITCS), 2013, pp. 1-4.
- [6] M.Paryasto, A.Alamsyah, B.Rahardjo, Big-data security management issues / Proceedings of the International Conference on Information and Technology (ICoICT), 2014, pp. 59-63.
- [7] R.Əliquliyev, Y. İmamverdiyev Big Data: Big promises for information security / Proceedings of the IEEE 8th International Conference on Application of Information and Communication Technologies (AICT), Astana, Kazakhstan 15-17 October, 2014, pp.216–219.
- [8] R.Əliquliyev, F.Abdullayeva Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi // İnformasiya Texnologiyaları Problemləri, 2013, №1, s. 3–14.
- [9] Cloud Security Alliance, Cloude Top Ten Big Data Security and Privacy Challenges, 2013, www.cloudsecurityalliance.org.
- [10] A.Jha, M.Dave, S.Madan, Big Data Security and Privacy: A Review on Issues, Challenges and Privacy Preserving Methods // International Journal of Computer Applications, 2017, vol. 177, no 4, pp. 23-28.
- [11] M.Hacırahimova, “Big Data” texnologiyaları və informasiya təhlükəsizliyi problemləri // İnformasiya Texnologiyaları Problemləri, 2016, №1, s. 49–56.
- [12] C.Rong, Z.Quan, A.Chakravorty, On Access Control Schemes for Hadoop Data Storage / Proceedings of the International International Conference on Cloud Computing and Big Data, 2013, pp. 641-645.
- [13] M. Shermin. An access control model for NoSQL databases. Master's thesis, University of Western Ontario, 2013. <http://ir.lib.uwo.ca/etd/1797>.
- [14] L.Okman, N.Gal-Oz, Y.Gonen, E.Gudes, J.Abramov, Security Issues in NoSQL Databases / Proceedings of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2011, pp 541-547.
- [15] D.Singh, C.K.Reddy, A survey on platforms for big data analytics // Journal of Big Data, 2014, pp.2-8.
- [16] J. Han, E. Haihong, G. Le, and J. Du, “Survey on nosql database” / Proceedings of the IEEE International Conference in Pervasive Computing and Applications (ICPCA), 2011, pp. 363–366.
- [17] R. Cattell, Scalable SQL and NoSQL data stores. ACM SIGMOD Record, 2010, vol. 39 no 4, pp. 12-27.
- [18] A. Siddiqua, A. Karim, A. Gani, Big data storage technologies: a survey // Frontiers of Information Technology & Electronic Engineering, 2017, vol. 18, no 8, pp. 1040-1070.
- [19] Strauch C. NoSQL Databases. <http://www.christofstrauch.de/nosql dbs.pdf>.
- [20] A.Zahid, R.Masood, M.A.Shibli, Security of Sharded NoSQL Databases: A Comparative Analysis / Proceedings of the Conference on Information Assurance and Cyber Security (CIACS), 2014, pp 1-8.
- [21] P.Noiumkar, T.Chomsiri, A Comparison the Level of Security on Top 5 Open Source NoSQL Databases / Proceedings of the International Conference on Information Technology and Applications(ICITA2014), 2014
- [22] K.Grolinger, W.A.Higashino, A.Tiwari, M. AM Capretz, Data management in cloud environments: NoSQL and NewSQL data stores // Journal of Cloud Computing: Advances, Systems and Applications, 2013, vol. 2, no1, pp. 2-24.

**ABOUT SECURITY PROBLEMS IN NOSQL
DATABASE**

Makrufa Hajirahimova¹, Marziya Ismayilova²

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

¹makrufa@scisence.az, ²imarziya@google.com

Abstract -- The paper is dedicated to security issues in big data and NoSQL databases. Big data, characterized by features such as large volume, velocity, and variety, make serious problems for security and privacy. Therefore, traditional security models have difficulties in dealing with such large scale data. In this paper, security and privacy issues have researched in big data and NoSQL databases.

Elektron dövlət mühitində uşaqların İnternet təhlükəsizliyinin qanunvericilik bazasının formalaşdırılması problemləri

Sabirə Ocaqverdiyeva

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

Xülasə – Məqalədə uşaqların İnternet mühitində qarşılaşdığı təhlükələr analiz olunaraq təsnifatlandırılır. Uşaqların İnternet mühitində təhlükəsizliyinin təmin olunması ilə əlaqədar dünyanın müxtəlif ölkələrində və Azərbaycanda dövlət səviyyəsində, qanunvericilik əsasında qəbul edilmiş normativ sənədlər haqqında məlumat verilir.

Açar sözlər – uşaqların təhlükəsizliyi, ziyanlı kontent, zərərli informasiya, internet təhlükələri, asılılıq.

I. GİRİŞ

İnternetin sürətlə inkişafı və bütün sahələrə tətbiqi istifadəçilərə geniş imkanlar yaradır. İnternet istifadəçilərinin sayı getdikcə artmaqda davam edir və informasiya mübadiləsi çoxalır. Virtual məkanda, əsasən də sosial mediada, son zamanlar geniş yayılan pornoqrafiya, işgəncə, qəddarlıq səhnələri, narkotik, spirtli içkilərin, terrorizm, vandalizm, pis vərdişlərin və s. təbliğatını aparan kontentlərin sayı artmaqdadır. Uşaqlar onlayn mühitdə istifadəçi kimi fəal olduqlarından, informasiya mübadiləsi zamanı onların qeyd olunan kontentlərlə qarşılaşma ehtimalı böyükdür.

Veb-səhifələrdə arzuolunmaz mənəvi və əxlaqi keyfiyyətləri aşılaraq kontentlər yetərinə boldur. Bu kontentlər uşaqların yaşa uyğun olmayan şəkillərlə, cinsi istismarı, aqressiyanı və zorakılığı təbliğ edən mətnlərlə rastlaşmasına səbəb olur.

İnternetdən əldə olunan bir çox məlumatlar uşaq psixologiyasına təsir edir. Onlarda qorxu, təlaş, dəhşət, vahimə kimi hisslərinin yaranmasına və kiber cinayətkarların hədəfinə çevrilməsinə səbəb olur. Uşaqların əksəriyyəti İnternetdə aldadılır, zorakılığa məruz qalır, texniki və sosial-psixoloji təhdidlərlə üzləşir [1].

Uşaqların hər hansı bir ziyanlı məlumatdan qorunması vacibdir. Son on-on beş il ərzində elmi ədəbiyyatda uşaqların təhlükələrlə qarşılaşma risklərinin tədqiqi ilə bağlı məlumatlar kifayət qədərdir. Bu məlumatlar əsasən kompüter təhlükələrinə və onların yaratdığı ziyanın nəticələrinə yönəlmişdir [2, 3].

Texnologiyaların inkişaf tempi elektron dövlət mühitində təhlükəsizliyin təmin edilməsi ilə bağlı yeni tələblər yaradır. İnformasiya təhlükəsizliyi məsələləri milli təhlükəsizliyin əsas tərkib hissələrindən biri olduğuna görə qeyd etmək olar ki, uşaqların İnternet mühitində qorunması məsələləri təmin bir hissəsi kimi yanaşma tələb edir.

II. UŞAQLARIN İNTERNET MÜHİTİNDƏ QARŞILAŞDIĞI TƏHLÜKƏLƏR

Qeyd edək ki, “uşaq” dedikdə, 18 yaşına çatmamış şəxslər başa düşülür. Yəni bu termin yalnız azyaşlılara aid edilmir, uşaq və yeniyetmələr də bu qrupa daxildir. Onlar daha çox sosial şəbəkələr, çatlar, oyun otaqları, onlayn alış-veriş, forum və s. kimi virtual məkanlarda ziyanlı kontentlə üzləşirlər. İnternetdə işləyərkən onların həm özünün, həm də istifadə etdiyi qurğunun təhlükəsizliyinə yönəlmiş müxtəlif təhlükələr baş verir. Bu təhlükələri bir neçə risk qrupuna bölmək olar. Risk təhdidlərin sistemə (obyekt, resurs və ya proses) təsirinin nə dərəcədə təhlükəli olduğunu müəyyən edir [4]:

- Məzmunla bağlı risklər;
- İnformasiya təhlükəsizliyi ilə bağlı risklər;
- Ünsiyyət və davranışla bağlı risklər;

Məzmunla bağlı risklər. İnternetdə paylaşılan və uşaqlar üçün qeyri-qanuni, qeyri-münasib hesab edilən məlumatların istifadəsi ilə əlaqədardır. Belə kontentləri uyğunsuz və qanunsuz məzmun olaraq iki hissəyə bölmək olar. Uyğunsuz məzmunla ölkənin mədəniyyətinə, mentalitetinə zidd olan və qanunvericiliyə əsasən təsdiq olunmuş qaydada uşaqların yaş qrupuna uyğun olmayan materiallar aid edilir. Buraya şiddət, qərəzli məzmun, erotizm və pornoqrafiya, normadan kənar leksika (söyüş, jarqon) ilə danışmaq və irqi ayrı seçkililiyi təbliğ edən materiallar aid edilir. Suisid (intihara cəlb) istiqamətli materiallar, sektant materiallar, partlayıcı maddələrin, narkotik vasitələrin hazırlanması və istifadəsi ilə bağlı məzmun daxildir [4].

Hər bir ölkənin qanunvericiliyinə əsasən, müxtəlif materiallar qanunsuz məzmun hesab olunur. Bir çox ölkələrdə uşaq və yeniyetmələrlə cinsi əlaqəli materiallar,

pornoqrafik məzmun, cinsi zorakılığı təbliğ edən məzmun, ekstremizm və irqçiliyə, nifrətə qarşı həssaslıq da daxil olmaqla zorakılıq təsvirlərini ehtiva edən materialların yayımlanması qadağan edilir və qanunsuz hesab olunur.

İnformasiya təhlükəsizliyi ilə bağlı risklər. Veb-səhifələri açarkən reklam və pulsuz proqram təminatları avtomatik olaraq kompüterin yaddaşına yüklənir. Fərdi məlumatların açıqlanması, virus hücumuna məruz qalma, onlayn fırıldaqçılıq və spam informasiya təhlükəsizliyi ilə bağlı risklərə aiddir [1,4].

Zərərli Proqramlara kompüterdə işləyərkən həm istifadəçinin özünə, həm də istifadə etdiyi kompüterə mənfi təsir göstərən proqramlar (viruslar, casus proqramları, istənilməyən reklam proqramları, zərərli kodun müxtəlif formaları) daxildir [1,4].

Spam reklam materialları yerləşdirilmiş və arzuolunmayan, istənilməyən e-poçtlardır. Belə məktublar istifadəçinin vaxtını və ona sərf edilən Internet trafikini istismar edir [1,4].

Kiberdələduzluq istifadəçilərin aldadılması məqsədini daşıyan (gizli məlumatların oğurlanması, köhnə məlumatlardan istifadə, Nigeriya məktubları, fişinq, istək və farming və s.) kibercinayətkarlığın bir növüdür.

Fişinq (ing. “*Phishing*”) texnologiyası kiberdələduzluğun ən çox yayılmış formasıdır. Hakerlər qanunsuz maddi mənfəət əldə etmək üçün bundan istifadə edir. Mahiyyəti ondan ibarətdir ki, saxta elektron poçta hansısa populyar Internet qovşağı apan hiperkeçid daxil edilir, əslində isə bu istifadəçini görünüşcə rəsmi sayta bənzəyən başqa bir qovşağı aparır. İstifadəçini rəsmi saytda olduğuna inandırıldıqdan və onların etimadını qazandıqdan sonra onun parolunu, kredit kartının nömrəsini və digər məxfi məlumatlarını daxil etməyə yönəltməyə cəhd göstərilir. Sonradan bu informasiyadan istifadəçiyə zərər vurmaq üçün istifadə edilir [5].

Ünsiyyət və davranışla bağlı risklər. Bu qrupa daxil olan təhlükələr Internet istifadəçilərinin insanlarla qarşılıqlı əlaqələrinə aiddir. Internetdə uşaqlar çox vaxt kiberhücuma məruz qalaraq kibercinayətkarların (pedofillər və s.) qurbanına çevrilir. Bu əlaqəyə azyaşlılar və böyük yaşlı insanlar arasında olan münasibətlər aid edilir.

Kiberzorakılıq (kiberöküzlük, ing. *Cyberbullying*) - virtual террордур (bull ingiliscə öküz mənasını verir), tərcümədə bu söz: təcavüzkar hücum, təcavüz, təhqir, təhrik etmək və qəzəbləndirmək kimi mənaları ifadə edir. Elektron poçt, ani mesajlaşma, çat otaqları, sosial şəbəkələr, veb-saytlar, eləcə də mobil telefonlar vasitəsilə həyata keçirilir [6]. İnsanlara psixoloji zərər vurmaq üçün virtual hücumdur və dörd əsas komponentdən ibarətdir:

- Təcavüzkar və mənfi davranışdır;
- Müntəzəm olaraq həyata keçirilir;

- İştirakçılar arasında müxtəlif gücə (qeyri-bərabər güc) malik münasibətlər baş verir;
- Qəsdən olunan bir davranışdır.

Təzahür formasından asılı olmayaraq kiberzorakılıq qurbana ciddi zərər verə və ən kəskin hallarda faciəli nəticələrə belə gətirib çıxara bilər. Bu davranışlara ciddiyyə alınmayan zərəflər, psixoloji virtual terror, insanın ölümünə səbəb olan davranış (bulisid - zorakılığa görə qurbanın ölümü) aiddir. Belə insanlar həm mesajla öz qurbanını təhqir edir, həm də qurbanın veb-səhifəsini ləğv edir, alçaldıcı məzmunun yerləşdiyi yerlərdə saxta səhifələr yaradır və həmin insanın ünvanına təhqiramiz və əxlaqsız mesajlar yayırlar.

Internet vasitəsilə fotoşəkillər göndərməklə insanları təqib, təhqir, təcavüz, cinsi təcavüz etmək kimi davranışlar bu fəkilərə aiddir. İnsanlarda qüsur tapmaq, yersiz irad tutmaq, təhrik etmək, əsəbləşdirmək, bəhanə axtarmaq, tənqəd gətirmək, narahat etmək, şaiyələr yaymaq, ələ salmaq, sataşmaq və aqressiv vəziyyətə gətirmək kimi xüsusiyyətləri də aid etmək olar.

Kiberzorakılıq tamamilə tanımadığınız insanlar, dostunuz, dostunuzun dostu olan insan tərəfindən həyata keçirilə bilər. Hətta bu qrup şəklində olan insanlar da ola bilər ki, onlar bir-birlərini tanıyırlar. Bəzən yeni yaradılmış bir qrup köhnə qrupun təzyiqlərinə də məruz qala bilər.

Internet-asılılıq. Bu problem Internetin inkişafından sonra yaranmışdır. Bəzi insanlar virtual aləmə o qədər aludə olurlar ki, onlar günün çox hissəsini - təxminən 18 saata qədərini kompüter arxasında keçirirlər. Uşaqların və yeniyetmələrin hər şeyi öyrənmək istəyi onların Internetdə saatlarla vaxt keçirməsinə səbəb olur və getdikcə ondan asılı vəziyyətə düşür. Belə uşaqlar dərslərini yaxşı hazırlaşa bilmir, yeməyini vaxtlı-vaxtında yemir, real ünsiyyətdən daha çox virtual ünsiyyətə üstünlük verir, sosiallaşa bilmir, bir sözlə cəmiyyətdən qacır. Onların sağlamlığı ilə bağlı problemlər yaranır (gözləri zəifləyir, fiziki gərəkəmi dəyişir, pinqvinləşir və s.). Internetdən asılılığın ən təhlükəli cəhətlərindən biri belə uşaqların cinayətkarların hədəfinə çevrilməsidir [7, 8].

Azartlı oyunlar. Uşaqların Internetdə saatlarla vaxt keçirməsinə səbəb olan məqamlardan biridir. Adi oyun saytlarında insanların oyun pulları ilə oynayaraq udməsinə və uduzmasına yol verilir. Pullu oyunlar olan saytlarda isə həqiqi pullar vasitəsilə oynanılan oyunlar yerləşdirilir.

Şəbəkədə oynanılan ideologiya xarakterli oyunlar şiddəti, zorakılığı, dini ayrışdırıcılığı təbliğ edir. Oyunlarda müxtəlif ideyalar təbliğ olunur. Uşaqlara Internetin “diktə” etdiyi mədəniyyətləri təbliğ edir, gənc nəslə milli adət-ənənələrdən uzaqlaşdırır [1, 8].

III. İNTERNET MÜHİTİNDƏ UŞAQLARIN QORUNMASINI TƏMİN EDƏN HÜQUQİ SƏNƏDLƏR

Internetin həyatımıza daha da dərindən nüfuz etməsi, səlahiyyətli insanların diqqətini özünə çəkir. Deməli, virtual mühiti tənzimləyəcək yeni qanunların yaradılmasına ehtiyac

artır. Qeyd olunan tədbirlərlə yanaşı, uşaq psixologiyasına, sağlamlığına təsir edən ziyanlı kontentin qarşısının alınmasında qanunla tənzimlənməni tələb edir. Uşaqları mövcud təhlükələrdən qoruma probleminin hüquqi səviyyədə tənzimlənməsi üçün əksər dünya ölkələrində müəyyən normativ sənədlər tətbiq edilir. Uşaqlara qarşı olan zorakılıqların, aqressiyanın, kibercinayətlərin və s. qarşısının alınması və uşaq təhlükəsizliyinin təmin olunmasına dair ölkələrin qanunvericiliyində müxtəlif yanaşmalar tətbiq edilir. Aşağıda onlardan bəziləri haqqında məlumat verilir.

Avropa Şurasının "Uşaqların zərərli kontentdən qorunması" hesabatında uşaqlar üçün nəzərdə tutulmuş ziyanlı informasiyanın növləri aşağıdakı kimi təsnifatlaşdırılır [9]:

Təbliğət xarakterli informasiya:

- Sağlamlığa zərərli informasiya və intihara cəlb etmə;
- Spirtli içkilərə, tütün, narkotik və s. sövq etmə;
- Azarlı oyunlar;
- Cinsi istismar;
- Dilənçilik;
- İnsanlara və heyvanlara qarşı qəddarlıq;
- Ailəyə hörmətsizlik və qeyri ənənəvi cinsi münasibətlərə sövq etmə;
- Qanun pozuntusuna və ya cinayətkarlığa sövq etmə;
- Pornoqrafik informasiya.

2. *Senzuradan kənar ifadələr:*

- Söyüş;
- Jarqon;
- Təhqiramiz ifadələr.

3. *Pornoqrafik informasiya:*

- Foto və təsvirlər şəklində cinsi münasibət.

4. *Şiddət və qorxunu təbliğ edən məzmun:*

- Şiddət;
- Qəddarlıq;
- Zorakılıq;
- Bədbəxt və qəzalı hadisələrin şəkillərinin verilməsi.

5. *Uşaq haqqında fərdi məlumat:*

- Uşağın kimliyi;
- Yaşadığı məkan, oxuduğu məktəb haqqında və s.

Amerika Birləşmiş Ştatlarında 2000-ci ilin oktyabrında ABŞ Konqresi tərəfindən uşaqları İnternetdə yerləşdirilən cinsi istismar və digər arzuolunmaz materiallardan qoruyan "Uşaqların İnternetdə Mübarizə Qanunu" qəbul edilmişdir [10]. Həmçinin "İnternetdə uşaqların məxfiliyinin qorunması haqqında" qanun qəbul edilmişdir. Qanun Birləşmiş Ştatların qanunvericiliyinə əsasən 13 yaşına çatmamış şəxslərin və ya

təşkilatlarda olan şəxsi məlumatların toplanmasına aiddir [11].

27 iyul 2006-cı ildə ABŞ-da Adam Valş uşaq mühafizəsi və təhlükəsizliyi aktı (Adam Walsh Child Protection and Safety Act) qəbul olunmuşdur. Məqsəd uşaqları istismar və zorakı cinayətlərdən qorumaq, uşaq pornoqrafiyasının qarşısının alınmasını bütün səviyyələrdə həyata keçirərək cinsi istismarçıların uşaqlara əlyetenliyinin qarşısını almaqla uşaqların internetdə təhlükəsizliyini təmin etməkdir. Qanunvericiliyə əsasən son 5 ildə bu tip cinayətlərdə iştirak etmiş şəxslərin barmaq izləri Milli Cinayətlərin məlumat bazasına daxil edilir [12].

2016-cı ilin mayında Belarus Respublikasının "Uşaq hüquqları haqqında" Qanununda müvafiq dəyişikliklər edilmişdir və 1 iyul 2017-ci il tarixindən qüvvəyə minmişdir [13].

2 iyul 2018-ci il tarixdə "Uşaqların sağlamlığına və inkişafına zərər verən məlumatlardan qorunması haqqında" Qazaxıstan Respublikasının Qanunu qəbul edilmişdir [14].

"Uşaqların sağlamlığına və inkişafına zərər verən məlumatlardan qorunması haqqında" Federal Qanunu 01 sentyabr 2012-ci il tarixdə qüvvəyə minmişdir. Rusiya qanunvericiliyinə görə, uşaqların informasiya təhlükəsizliyi - İnternetdə yayılmış məlumatların onların sağlamlığına, fiziki, zehni inkişafına təsir edən və mənəvi cəhətdən zərər verən informasiyalar ilə əlaqəli risklərdən onların qorunmasıdır [15].

IV. AZƏRBACANDA UŞAQLARIN İNFORMASIYA TƏHLÜKƏSİZLİYİNİN HÜQUQ MÜSTƏVİSİNDƏ TƏMİNİ

Ölkəmizdə informasiya təhlükəsizliyinin təmin edilməsinin qanunvericilik bazasının formalaşdırılması və inkişaf etdirilməsi istiqamətində bir sıra mühüm konseptual sənədlər, normativ-hüquqi aktlar qəbul edilmişdir.

Azərbaycan Respublikası Prezidentinin 2014-cü il 02 aprel tarixli sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasında İC-nin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya" –da "Uşaqların qanunazidd və təhlükəli kontentdən qorunması üçün "təhlükəsiz İnternet" mexanizminin işlənilməsi və tətbiqi" üçün müəyyən tədbirlərin görülməsi nəzərdə tutulur [16].

Azərbaycan Respublikasının Prezidentinin 29 aprel 2016-cı il tarixli "Telekommunikasiya haqqında" Azərbaycan Respublikasının Qanununda dəyişikliklər edilməsi barədə Azərbaycan Respublikasının Qanununda (34.1.2-1. Uşaqların sağlamlığına və inkişafına ziyan vuran informasiyadan qorunması üçün tədbirlər görülməsini tələb etmək) bu haqda qeyd olunmuşdur [17].

Qanunda uşaqların sağlamlığı və inkişafı üçün zərərli məlumatlar və onlardan qorunma təqdim olunur. Ümumiyyətlə, ölkəmizdə uşaqların arzuolunmayan

məlumatlardan qorunması və İnternet təhdidlərinin qarşısının alınması məqsədilə təklif olunan tənzimləyici çərçivənin olduqca əhəmiyyətli olduğunu qeyd etmək lazımdır. “Uşaqların zərərli informasiyadan qorunması haqqında” Azərbaycan Respublikasının 2018-ci il 30 oktyabr tarixli qanunun 3-cü maddəsində “Uşaqların zərərli informasiyadan qorunması sahəsində əsas prinsiplər” verilmişdir və orada göstərilir ki, “zorakılığın, qəddarlığın, narkotik vasitələrin və psixotrop maddələrin, alkoqollu içkilərin və bütün məmulatlarının, cəmiyyət əleyhinə davranışın, pornoqrafik xarakterli informasiyanın təbliğinin yolverilməzliyi” əsas faktordur. Qanun uşaqların fiziki, zehni və mənəvi inkişafına zərər verən məlumatlardan qorunması üçün qanuni mexanizmləri müəyyən edir [18].

Qanunda uşaqların yaş həddinə görə kateqoriyalara ayrılması onu göstərir ki, uşaqlar üçün nəzərdə tutulmuş informasiya məhsulları hər bir yaşa uyğun olaraq analiz olunmalı və təsnifatlandırılmalıdır. Yaş həddi (0+, 6+, 12+, 16+, 18+) nəzərə alınmaqla uşaqlar arasında döviyyəsi qadağan edilən informasiyanın növlərinə aşağıda qeyd olunan problemlər aid edilir [18]:

- Zorakılığı və qəddarlığı təbliğ edən informasiya;
- Cinayətkarlığı təbliğ edən informasiya;
- Uşaqların həyat və təhlükəsizliyinə potensial təhlükə yaranan əməlləri təbliğ edən informasiya;
- Əxlaqdan kənar leksik (söyüş) məzmunlu informasiya;
- Erotik və pornoqrafik xarakterli informasiya;
- Qeyri-məişət leksik (jarqon) məzmunlu informasiya;
- Qorxu məzmunlu informasiya.

Görülən tədbirlərə baxmayaraq, müasir dövrdə uşaqlar üçün təhlükəli məlumatların yayılması ilə bağlı yeni risklərin artması davam etməkdədir. Yeni qəbul edilmiş və uşaqların qorunması məqsədini daşıyan qanun və sərəncamlar uşaqların sağlam böyüməsi, tərbiyəsi, sosiallaşmasına kömək edir. Onlarda yüksək səviyyədə vətəndaşlıq, vətənpərvərlik hisslərinin yaranmasında böyük rol oynayır və yeni sosial dövlət sisteminin formalaşmasına çağırır.

NƏTİCƏ

Maarifləndirici, təşkilati və proqram texniki tədbirlərin həyata keçirilməsi uşaq təhlükəsizliyinin təmin olunması probleminin həllində əhəmiyyətli və işə öz müsbət təsirini göstərir.

Araşdırmalardan məlum olur ki, bütün dövlətlərdə olduğu kimi, Azərbaycanda uşaqların informasiya təhlükəsizliyi ilə bağlı problemlər aktualdır. Hər il yeni-yeni qanun və sərəncamların verilməsinə baxmayaraq, zərərli məlumatlar İnternet global şəbəkəsi vasitəsilə (elektron oyunlar, qorxu

və terrorizmi təbliğ edən cizgi filmləri, videoçarxlar və s.) uşaqlara ötürülür.

Müasir həyatın mürəkkəbliyi, İnternet təhdidlərin çoxluğu, kibercinayətlərin sayının artması və eyni zamanda uşaqların təcrübəsizliyi göstərir ki, onları istər real həyatda, istərsə də virtual aləmdə arzu olunmayan məlumatlardan qoruması problemi kompleks yanaşma tələb edir. Dövlət və ictimai təşkilatlar bu problemin ətrafında birləşməlidir. Ən başlıcası isə valideyn, himayədar və s. cavabdeh şəxslərin təhlükələr barədə məlumatlı olması və yüksək informasiya mədəniyyətinin olması vacibdir.

ƏDƏBİYYAT

- [1] S.S.Ocaqverdiyeva. İnternet mühitində uşaqların təhlükəsizliyinin təmin edilməsi məsələləri / İnformasiya Cəmiyyəti Problemləri, 2018, N: 1. s. 99-107.
- [2] H.Ros, D. George. Young children's concepts of danger/ British Journal of Developmental Psychology, 2000, vol.18, pp.103-119.
- [3] N.T. Abdelmajeed. Parental Role in Protecting Children and Dangers of Social Networks Sites/ Journal of information security and cybercrimes research (JISCR). Vol 1, No 1 (2018), pp. 19-27.
- [4] С. А.Котова. Дети в интернете: контентные и коммуникационные риски//Поведение риска: современные направления исследования и профилактики Материалы Международной научно-практической конференции 24 февраля 2012 года, стр. 232-245.
- [5] J. Hong. “The state of phishing attacks”/ Communications of the ACM, vol. 55, №1, pp. 74-81, 2012.
- [6] J.Cenat, M.Blais, F.Lavoie, P.Caron, M.Hebert. Cyberbullying victimization and substance use among Quebec high schools students: The mediating role of psychological distress/ Computers in human behavior, vol.89. pp. 207-212, 2018.
- [7] R.M. Əliquliyev, R.Ş. Mahmudov. İnformasiya asılılığı problemləri və onlarla mübarizə yolları/ İnformasiya Texnologiyaları nəşriyyatı, Bakı, 2009, 62 s.
- [8] Д.А. Богданова, А.А. Федосеев. Внимание – Интернет.//Открытое образование. №2, стр. 89-99, 2010.
- [9] Доклад для Совета Европы «Защита детей от вредного контента», <https://www.coe.int/en/web/freedom-expressi>
- [10] Children's Internet Protection Act (CIPA), <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>
- [11] COPPA - Children's Online Privacy Protection Act, <http://www.coppa.org/coppa.htm>
- [12] Adam Walsh Child Protection and Safety Act, <http://www.ncsl.org/research/civil-and-criminal-justice/adam-walsh-child-protection-and-safety-act.aspx>
- [13] Закон Республики Беларусь 19 ноября 1993 г. N 2570-XII, О правах ребенка, <http://pravo.by/document/?guid=3961&p0=V19302570>
- [14] Закон Республики Казахстан от 2 июля 2018 года № 169-VI «О защите детей от информации, причиняющей вред их здоровью и развитию» (не введен в действие), https://online.zakon.kz/document/?doc_id=39797352#pos=201;-45
- [15] Защита детей от информации, которая может причинить вред их здоровью и развитию, <http://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2017/june/24766/>
- [16] Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya, 02 aprel 2014-cü il// www.president.az
- [17] “Telekommunikasiya haqqında” Azərbaycan Respublikasının Qanununda dəyişikliklər edilməsi barədə, Bakı şəhəri, 29 aprel 2016-cı il, № 212-VQD, <http://www.e-qanun.az/framework/32956>

- [18] “Uşaqların zərərli informasiyadan qorunması haqqında” Azərbaycan Respublikasının 2018-ci il 30 oktyabr tarixli 1310-VQ nömrəli Qanun <https://president.az/articles/30815>

**CHILDREN'S INTERNET SAFETY LEGISLATION
BASE IN THE E-STATE ENVIRONMENT**

Sabira Ojagverdieva

Institute of Information Technologies of ANAS,
Baku, Azerbaijan

allahverdiyevsabira@gmail.com

Abstract - The threats faced by children in the Internet are classified by analysing in the article. The information on normative documents adopted on the basis of legislation at the state level in Azerbaijan and different countries of the world due to the safety of children on the Internet environment.

Keywords - children safety, damaging content, harmful information, Internet threats, addiction.

Veb spamlar və onlarla mübarizə metodları

Xəyyam Nurəliyev

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

xeyyam777@gmail.com

Xülasə — Veb spamlar axtarışın nəticəsində yüksək mövqe qazanmaq məqsədilə informasiya-axtarış sistemlərini aldatmaq və onun nəticələrini manipulyasiya etməyə çalışan veb-saytlar və ya səhifələrdir. Bu gün saytların internetdə irəliləməsi (daha geniş tanınması) məqsədilə veb-spamların tətbiqinə axtarış sistemləri tərəfindən qadağa qoyulmasına baxmayaraq, praktiki olaraq, bu texnologiyadan çox istifadə olunur. Veb-spamların istifadə edilməsi qısa zamanda veb-saytın tanınmasına və ona müraciətlərin sayının artmasına kifayət qədər əhəmiyyətli təsir göstərə bilər.

Açar sözlər— *web spam detection, content spam, link spam, cloaking, collusion, Pagerank, TrustRank, classification, clustering, web search, user behavior.*

I GİRİŞ

Veb spam anlayışı ilk dəfə 1996-cı ildə meydana gəlmişdir. Axtarış sistemləri və istifadəçilər üçün əsas problemə çevrilmişdir. Axtarış sistemləri arasında getdikcə artan rəqabət daha təmiz internet anlayışını ortaya çıxardı və veb spamların mənfi təsiri araşdırılmağa başlandı. Veb spamlar axtarış sistemlərinin axtarış nəticələrinə və saytların qiymətləndirmə dərəcələrinə çox təsir göstərir. Hazırda saytlar müəyyən gəlir əldə etmək məqsədilə veb spamlar yaradırlar. Axtarış sistemləri interneti zibillənmiş veb saytlardan təmizləmək üçün yeni metodlar işləyib hazırlayırlar. Son vaxtlarda axtarış sistemləri zərərli informasiyalar almağa başladılar. İlk olaraq veb spamlar axtarış sistemlərinin qiymətləndirmə nəticələrini pozurdu, veb saytların qanuni yolla qazanc əldə etməsinə imkan vermirdi, buda istifadəçilərin axtarış sistemlərinə inamını zəiflədirdi.

İstifadəçilər veb saytlarını axtarış sistemlərinin sıralamasında ön sıralara çıxarmaq üçün veb spamlar yaradırlar. Araşdırmalar göstərir ki, 85% istifadəçilər ilk 3-5 bağlantıya ziyarət edir və nəticədə veb sayt sahibləri bu nəticəni yaxşılaşdırmaq üçün veb spam metodlarına baş vurur [1].

Bu aşağıdakı şəkildə olur:

Bir səhifəyə əsas kontentin yerinə aid olmayan kontent əlavə etmək.

Həddindən çox və haqsız bağlantı yaratmaq, gizlətmə, klik etmə saxtakarlığı və istənməyən etikətlər.

Araşdırmalar göstərir ki, veb saytların 6-22% veb spam olur. [1]

Dillərə görə veb spam faizi aşağıdakı kimidir.

İngilis-13,8%,

Yapon-9%,

Alman-22%,

Fransız-25%

Domen adlarına görə veb spam aşağıdakı kimidir.

.biz - 70%,

.com - 20%

Veb saytların getdikcə inkişafı nəticəsində çoxlu sayda veb spamlar ortaya çıxdı və hazırda çoxlu sayda veb spamlar mövcuddur.

Hazırda veb spamlarla mübarizədə ən böyük problem metodların tez-tez yenilənməsi və hər bir dilin özünə məxsus xüsusiyyətləridir.

II VEB SPAMLARIN NÖVLƏRİ

A. Kontent spamlar

Kontent spamlar ilk və ən çox yayılan və məşhur olanıdır. Kontent spamlar dedikdə mahiyyət etibarı ilə saytın və ya veb-səhifənin əsas mətninə açar sözlərin və ifadələrin əlavə edilməsi, həddən artıq doldurulması, məzmunun qarışdırılması başa düşülür.

Kontent spamlarının 5 alt tipi var.

- Title Spamming.
- Body Spamming.
- Meta-Tags Spamming.

- Anchor Text Spamming.
- URL Spamming.

A. Link spamları

Link spamları veb-spamların daha geniş yayılmış növüdür. Link spamlarının mahiyyəti müxtəlif internet ehtiyatlarında istinadların istifadəsinin süni manipulyasiya edilməsindən ibarətdir. Burada spam rolunda həm daxili, həm də xarici linklər çıxış edə bilər.[5]

Link spamlarının iki kateqoriyası vardır.

Outgoing- çıxan linklər

Incoming- daxil olan linklər

B. Cloaking and Redirection (gizləmə və yönləndirmə spamları)

Gizləmə - veb sahifələrə gələn ziyarətçilərin təbii yoxsa bot olmasının təyin edilməsindən sonra fərqli sahifələrə yönləndirmə edərək axtarış sistemlərinə xüsusi yaradılmış sahifələr göstərərək axtarış sistemlərinin botlarını aldadır.

1) Cloaking spamın işləmə sxemi [3]

Redirection - həm istifadəçilər, həm də axtarış sistemləri tərəfindən göndərilən sorğuya cavab olaraq gələn URL-in javascript vasitəsi ilə başqa bir URL-ə yönləndirilməsi başa düşülür.

2) Redirection spamlarının işləmə sxemi [3]

III VEB SPAM METODLARI

İnternet dedikdə ağılımıza gələn ilk saytlardan biri olan Google axtarış sistemidir. Google dünyada ən çox istifadə olunan axtarış sistemidir. Google axtarış sistemi veb saytların rəqləşdirilməsində istifadə olunan bir çox alqoritmi işləmişdir. Bunlara aşağıdakı alqoritmləri göstərmək olar [4]:

-Google Panda

-Google Penguin

-Google Sandbox

1. Page Rank alqoritmi

Google-un veb sahifələrə verdiyi rəqləşdirma qiyməti şkalasıdır. Bu qiymət ümumi olaraq xüsusi bir məzmunla bağlantı və keçid verən sahifənin yüksək rəqləşdirma dərəcəsinə bağlıdır. PageRank qiyməti saytınızın Google axtarış mühərrikində internet istifadəçiləri tərəfindən axtarış aparıldığı sahifənin ön sıralarda olmasını təmin edir. $T_1...T_n$, A sahifəsinə istinad edən sahifələr olaraq qəbul etsək, d parametrisini 0 ilə 1 arasında dəyişən və ümumilikdə 0,85 qəbul edilən bir ədəddir. C (A) isə A sahifəsindən çıxan linklərin sayıdır. Bu halda PR (A), A sahifəsinin PageRank qiymətini ifadə edir.

$$PR(A) = (1-d) + d(PR(T_1)/C(T_1) + \dots + PR(T_n)/C(T_n)) \quad [2]$$

2.TrustRank alqoritmi

Stanford universiteti və Yahoo tərəfindən təyin edilən ve spama qarşı mübarizədə istifadə edilən bir link analiz texnologiyasıdır. Spam olan veb sahifələrin yarım avtomatik bir şəkildə təyin olunmasıdır. Hazırda bir çox veb sahifə gəlir əldə etmək məqsədilə axtarış sistemlərində nəticələrini artırmaq üçün spam texnologiyalarından istifadə edir. Hər sahifənin sayt

menicəri tərəfindən araşdırılması çox çətin olduğundan, bəzi etibarlı səhifələr qeyd edilir və ondan alınan link çıxışlarındakı saytlara xallar verilir.

TrustRank ilə editorlar tərəfindən birinci dərəcədə etibarlı saytlar qeyd edilir. Bu saytlara kök sayt deyilir və bu saytlardan link çıxışları ilə digər saytlara etibarlılıq xalı verilir. [2] [6]

NƏTİCƏ

Bu işdə veb spamların növləri və onlarla mübarizə üçün alqoritmlər araşdırılmışdır. Veb spamların istifadəçilərə və axtarış sistemlərinə necə təsir etdiyi, axtarış sistemlərinin nəticələrinə təsiri qısa olaraq araşdırılmışdır.

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

ƏDƏBİYYAT

1. Nikita Spirin, Jiawei Han, “Survey on Web Spam Detection: Principles and Algorithms,” Department of Computer Science University of Illinois at Urbana-Champaign, December 2011
2. Gökhan Eğri, “Arama Motoru Optimizasyonu Teknikleri,” T.C. İstanbul Kültür Üniversitesi Fen Bilimleri Enstitüsü, Ocak 2013
3. L. Becchetti , P. Boldi , C. Castillo , D. Donato , A. Gionis , S. Leonardi , V. Murdock , M. Santini , F. Silvestri , S. Vigna , “Web Spam Detection, Yahoo! Research Barcelona – Catalunya, Spain 2. Universit’a di Roma “La Sapienza” – Rome, Italy 3. Yahoo! Research Santiago – Chile 4. ISTI-CNR –Pisa, Italy 5. Universit’a degli Studi di Milano – Milan, Italy, 2007, pp. 7-8.
4. <https://moz.com/blog/google-algorithm-cheat-sheet-panda-penguin-hummingbird>
5. Marc Najork, ‘Web Spam Detection’, Microsoft Research, Mountain View, CA, USA, 2009
6. Vijay Krishnan, Rashmi Raj, ‘Web Spam Detection with AntiTrust Rank, Stanford University Stanford, CA 4305, 2006

WEB SPAMMING AND FIGHTING WEB SPAM METHODS

Xayyam Nuraliyev

Institute of Information Technology of ANAS,
Baku, Azerbaijan

xeyyam777@gmail.com

Abstract—Web spammers are websites or pages that seek to deceive information-searching systems and manipulate its results to gain a high ranking position. Today, although the use of web spammers is banned by search engines for the promotion of websites (wider popularity), it is practically used more than this technology. The use of web spammers can have a considerable impact on the popularity of the website and the number of applications it receives soon.

Keywords — web spam detection, content spam, link spam, cloaking, collusion, Pagerank, TrustRank, classification, clustering, web search, user behavior.

İnformasiya iqtisadiyyatı şəraitində nəşriyyat-poliqrafiya sektorunun formalaşmasında müasir İKT onların təhlükəsizliyi məsələləri

Əlövsət Əliyev¹, Anar Səmidov², Roza Şahverdiyeva³, Leyla Əkbərova⁴

^{1,2,3,4}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹alovsat_qaraca@mail.ru

Xülasə – Məqalə informasiya iqtisadiyyatı şəraitində innovativ nəşriyyat-poliqrafiya sektorunun formalaşmasında müasir İKT program-texniki vasitələrinə, sistemlərinə, resurslarına və onların təhlükəsizliyi problemlərinə həsr olunmuşdur. İqtisadi inkişafda İKT, bilik və innovasiyaların roluna baxılmış və əhəmiyyəti göstərilmişdir. İnformasiya iqtisadiyyatında nəşriyyat-poliqrafiya sektorunun rolu və yeri aydınlaşdırılmışdır. Nəşriyyat-poliqrafiya sektorunun innovativ xüsusiyyətləri, institusional strukturu və inkişaf mərhələləri izah olunmuşdur. Nəşriyyat-poliqrafiya sektorunun effektivliyinin yüksəldilməsində innovativ İKT vasitələri və onların təhlükəsizliyi problemləri araşdırılmışdır. Həmin problemlərin həlli üzrə bəzi tövsiyələr verilmişdir.

Açar sözlər— informasiya iqtisadiyyatı, nəşriyyat-poliqrafiya sektoru, 3D- çap, İKT-nin təhlükəsizliyi

I. GİRİŞ

Hazırda Azərbaycanda informasiya və biliklər bazarının formalaşmasına, cəmiyyətin informasiya-kommunikasiya infrastrukturunun zənginləşdirilməsinə və onun dünya informasiya strukturuna inteqrasiya edilməsinə, eləcə də iqtisadiyyatın İKT əsaslı sektorlarında keyfiyyətli məhsullar/xidmətlər spektrinin artırılmasına hökumət səviyyəsində ciddi qayğı göstərilir. Ölkədə İKT-in müasir infrastrukturunu idarəetmənin təkmilləşdirilməsinin əsas mənbələrindən birinə çevrilmişdir. Respublika iqtisadiyyatının ayrı-ayrı sahələri arasında münasibətlərin qurulmasında da İKT-nin rolu get-gedə artmaqdadır. Buna görə də respublikada qəbul edilmiş strateji yol xəritələrinin və İnformasiya Cəmiyyətinin inkişafı üzrə Milli Strategiyanın vəzifələrinə insan amilinin inkişafı, elektron hökumətin, elektron ticarətin formalaşması, ölkənin iqtisadi, sosial və intellektual potensialının mükəmməlləşdirilməsi, informasiya və biliklərə əsaslanan, rəqabətə davamlı rəqəmsal iqtisadiyyatın qurulması, informasiya və bilik bazarının yaradılması, İKT-məhsullarının istehsalı kimi vacib məsələlər daxil edilmişdir [1,2]. Ona görə də ölkə iqtisadiyyatının modernləşdirilməsi, onun dünya bazarında rəqabət qabiliyyətinin artırılması

istiqamətində zəruri tədbirlər həyata keçirilməlidir. Bunun üçün ölkədə islahatlara hazırlıq, yeni sənaye infrastrukturu, elmi-texniki potensial, güclü fundamental və tətbiqi elmlər, əhalinin yüksək təhsil səviyyəsi, mühəndis-texniki ixtisaslarının üstünlük təşkil etməsi, əlverişli İKT və biznes mühit və s. kimi müsbət amillər vardır. Bu istiqamətdə formalaşmaqda olan yeni informasiya və biliklər iqtisadiyyatının nəşriyyat-poliqrafiya sektorunun (NPS) kifayət qədər böyük potensialı vardır. Bu potensialdan effektiv istifadə və onun təhlükəsizliyi, dayanıqlılığı mühüm əhəmiyyətə malik aktual məsələdir [3, 4].

Məlum olduğu kimi, XXI əsrdə elm və texnikanın inkişafına, xüsusən informasiya texnologiyalarına böyük önəm verilir. İnsanın istehsal, mənəvi, bədii, ünsiyyət və s. kimi bir çox sosial-iqtisadi fəaliyyət sahələrinə kompüterləşmə və informasiyaladurma prosesi çox nüfuz etmişdir [5,6].

İnformasiya və biliklər iqtisadiyyatının formalaşması İKT-nin inkişafı və cəmiyyətdə informasiyanın rolunun artması ilə, postindustrial cəmiyyət nəzəriyyəsi ilə, yəni texniki tərəqqinin artması, maddi istehsalın rolunun zəiflənməsi, xidmət və informasiya sektorunun inkişafı, insan fəaliyyətinin xarakter və motivinin dəyişməsi, sosial strukturların modifikasiyası ilə əlaqədardır.

Yeni iqtisadiyyatın mühüm xüsusiyyəti qeyri maddi resurs-informasiyanın, iqtisadi-siyasi resursa, cəmiyyətin və vətəndaşların maddi rifah halını müəyyən edən resursa çevrilməsidir. İnformasiya getdikcə daha çox istehsal malları xüsusiyyəti kəsb edir, iqtisadiyyatın əsas sektorları isə İKT ilə əlaqədə olur. İnternet inkişaf etdikcə digər ictimai-siyasi, sosial-iqtisadi proseslər də interaktiv mühitə keçir. E-hökumət, E-demokratiya, E-seçki, E-kitab, E-kitabxana, 3D-çap və s. kimi yeni sistemlər və texnologiyalar vətəndaş-hakimiyyət-biznes qarşılıqlı münasibətinin yeni forması olur.

Hazırda Azərbaycanda İKT-nin istifadəsi və tətbiqi nəticəsində E-ticarət, E-biznes, E-kitabxana, E-təhsil, E-səhiyyə, E-mədəniyyət inkişaf edir, İnternet-banking formalaşır, İnternet vasitəsilə sığorta və qiymətli kağızlar bazarları yaranır, nəşriyyat-poliqrafiya fəaliyyəti artır, marketing tədqiqatlarının əhatə dairəsi genişlənir. Bütün bunlar elektron iqtisadiyyatın və nəticə etibarilə bilik iqtisadiyyatının inkişaf səviyyəsini yüksəltməkdədir.

İKT ölkə iqtisadiyyatının bütün sahələrində səmərəliliyin artırılmasına, qiymətlərin azaldılmasına, dövlət orqanlarında elektron sənəd dövriyyəsinin, elektron ticarət sistemlərinin tətbiqinə, məhsul və xidmətlərin keyfiyyətinin yüksəldilməsinə köməklik göstərəcəkdir. Azərbaycanın iqtisadiyyatında İKT, bilik tutumlu istehsal sferaları və digər elmi-texniki sahələr inkişaf edərək respublikada informasiya cəmiyyətinin və bilik iqtisadiyyatının formalaşmasına zəmin yaradaraq cəmiyyətin yeni sosial-iqtisadi həyatının bütün sahələrinin dinamik və davamlı inkişafını təmin edəcəkdir.

Ölkənin yaxın və uzaq inkişaf perspektivlərində elektron sahələrin, İKT məhsul/xidmətlərin, rəqəmsal çap işinin, elektron idarəetmənin inkişaf etdirilməsi mühüm bir vəzifə kimi qoyulmuşdur [1,2]. Burada əsas məqsəd ondan ibarətdir ki, yaxın illərdə təhsildə, elmdə, istehsalatda, digər ictimai-sosial, iqtisadi sahələrdə ciddi dönüş yaradılmalı, informasiya və biliklər iqtisadiyyatının qurulması prosesi intensivləşməlidir. İnformasiya və biliklər iqtisadiyyatının formalaşması üçün informasiyanın və biliyin genişmiqyaslı inkişafını təmin edən, dünya bazarında rəqabət üstünlüyü verən yeni iqtisadi modelin yaradılması vacib şərtidir. Bu modelin reallaşmasında ilk növbədə informasiyaya, biliyə, texnologiyaya, İKT-yə diqqət yetirilir, İKT əsaslı iqtisadiyyat gücləndirilir.

II. AZƏRBAYCAN İQTİSADİYYATINDA NƏŞRİYYAT-POLİQRAFİYA SEKTORU: ROLU, YERİ, MÖVCUD VƏZİYYƏTİ

Hazırkı dövrdə çox böyük innovativ potensiala malik olan iqtisadi sahələrdən biri də nəşriyyat-poliqrafiya sektorudur. Bu sektor kifayət qədər müasir güclü infrastruktura malikdir. Sahə müasir texnologiyalarla və avadanlıqlarla təmin edilmişdir. Nəşriyyat-poliqrafiya sektorunun xüsusiyyətləri sahənin spesifikasiyası ilə əlaqədardır. Nəşriyyat işinin ümumi prinsiplərini Nəşriyyat işi haqqında Azərbaycan Respublikasının 30 may 2000-ci il qanunu [7] müəyyən edir. Nəşriyyat fəaliyyətinin təşkili və həyata keçirilməsi ilə əlaqədar nəşriyyat işinin subyektləri arasında münasibətlər həmin qanunla tənzimlənir. Qanunda göstərilir ki, nəşriyyatın əsas fəaliyyət sahəsi nəşriyyat məhsullarının hazırlanması, istehsalı və yayımıdır. Nəşriyyat işi dedikdə nəşriyyat məhsullarının hazırlanması, istehsalı və yayımı ilə məşğul olan hüquqi və fiziki şəxslərin təşkilati-yaradıcılıq və istehsalat-təsərrüfat fəaliyyətini əhatə edən ictimai münasibətlər sahəsi başa düşülür. Çap üsulundan və formasından asılı olmayaraq istehlakçı üçün nəzərdə tutulan kitab, broşür, albom, plakat, buklet, açıqca, elektron nəşrlər və digər nəşriyyat məhsullarının məcmusu nəşriyyat məhsulu hesab edilir. Çap məhsulu isə poliqrafiya müəssisələrində çap texnikası vasitəsilə hazırlanan dövrü mətbu nəşrlər, nəşriyyat məhsulları (elektron nəşrlərdən başqa) və bütün növlərdən olan poliqrafiya məhsullarının məcmusudur.

Nəşriyyat işi sahəsində dövlət siyasətinin əsas prinsipləri və dövlətin əsas vəzifələri aşağıdakılardır [7]:

- Nəşriyyat işinin maddi-texniki bazasının, təşkilati, hüquqi və elmi əsaslarının möhkəmləndirilməsinə, milli kitab nəşrinin inkişafına yardım edilməsi;
- Nəşriyyat işinin inkişafına dair dövlət proqramının hazırlanması və həyata keçirilməsi;
- Nəşriyyat işi sahəsində inhisarçılığın qarşısının alınması;
- Azərbaycan xalqının klassik irsi və milli-mənəvi sərvətləri sayılan əsərlərin dövlət sifarişi əsasında nəşrinin həyata keçirilməsi;
- Nəşriyyatların maddi-texniki bazasının genişləndirilməsinin, poliqrafiya sənayesinin inkişafının, nəşriyyat məhsullarının satışının stimullaşdırılması və kitab yayımının təmin edilməsi;
- Milli-mədəni sərvətləri əks etdirən kitabların dünya miqyasında təbliği məqsədilə onların tərcüməsi, nəşri və yayılmasının stimullaşdırılması;
- Mətbuatın dövlət statistikasını aparmaqla, əhalinin və bazarın nəşriyyat məhsullarına olan tələbatını, ehtiyaclarını və təkliflərini öyrənməklə nəşriyyatların işinin istiqamətləndirilməsi;
- Uşaq ədəbiyyatı, dərslik, elmi-texniki ədəbiyyat, tərcümə ədəbiyyatı, lüğət və ensiklopediyaların, yazılı və şifahi mədəniyyət abidələrinin nəşrinə güzəştlərin müəyyən edilməsi;
- Səhiyyə, elm və əhalinin sosial müdafiəsi ilə bağlı nəşriyyat məhsullarının istehsalının dövlət sifarişi əsasında həyata keçirilməsi.

Nəşriyyat işi sahəsində fəaliyyət müliyyətin bütün növlərinə əsaslanan müxtəlif təşkilati-hüquqi formalarda həyata keçirilə bilər. Nəşriyyat işi sahəsində beynəlxalq əməkdaşlıq Azərbaycan Respublikasının tərəfdar çıxdığı dövlətlərlə müqavilələrə əsasən həyata keçirilir.

Poliqrafiya sənayesi (mətbəələr) çap məhsullarının istehsalı sahəsidir. Adətən, poliqrafiya məhsullarının istehsalı zamanı ofset və rəqəmsal çap vasitəsilə istifadə olunur. Ofset üsulla çap zamanı çap olunacaq məhsul çapdan öncə bir neçə hazırlıq mərhələsindən keçməlidir. Bu cür çap ofset çap maşınları vasitəsilə həyata keçirilir və kimyəvi maddələr və lazerlə işlənmiş, nazik dəmirə köçürülmüş təsvirlər çap maşınına verilir. Ofset üsulla çapda istifadə olunan boya rəqəmsal çapdakı boyadan daha ucuzdur. Ona görə də daha böyük tirajlarda ofset çap üsulundan istifadə edirlər.

Azərbaycanda poliqrafiyanın bir sənaye sahəsi kimi formalaşması ötən əsrin əvvəllərindən başlayaraq sonuna kimi yüksələn xətlə davam etmişdir. 90-cı illərdən başlayaraq poliqrafiya sənayesi sahəsində yeni meyillər ortaya çıxmış, bu sahəyə özəl sektorun daxil olması ilə yeni texnoloji nailiyyətlərin tətbiqinə imkanlar açılmışdır. 2000-ci illərin əvvəllərində çap avadanlıqlarının yenilənməsi prosesi sürətlənmiş, ölkədə yüksək səviyyəli, kitab, jurnal, qəzet və digər məhsulların istehsalı üzrə ixtisaslaşmış orta və iri

poliqrafiya müəssisələri yaranmağa başlamışdır. Şəkil 1-dən göründüyü kimi 2005-ci ildən 2015-ci ilə qədər bu sahədə fəaliyyət göstərən dövlət və qeyri-dövlət müəssisələrinin sayında 7-19 dəfə fərq var. Özəl sektorun bu sahəyə axını 2009-cu ilə qədər yüksəlmə trendi göstərilib, 2009-cu ildən bugunə qədərki ən yüksək nəticə qeydə alınıb. Həmin il özəl sektora məxsus 184 müəssisə fəaliyyət göstərilib. Lakin sonradan bu trend enməyə başlayıb. 2015-ci ildə 149 belə müəssisənin fəaliyyəti faktı qeydə alınıb [8].

Bunlarla yanaşı, qeyd etmək lazımdır ki, bu sektorda təşkilati-hüquqi statusu müxtəlif olan oxşar profilli strukturlar mövcuddur. Belə ki, bütün alt məktəblərin, kolleclərin, litseylərin, akademik və sahə elmi-tədqiqat institutlarının, böyük şirkətlərin yardımçı nəşriyyat-mətbəəsi vardır. Onların da çap məhsulları, fəaliyyətləri məhsul/xidmət formasında ölkənin Ümumi Daxili Məhsullarının formalaşmasına ciddi təsir edir.

Şəkil 1. Poliqrafiya müəssisələrinin sayı

III. NƏŞRİYYAT-POLİQRAFIYA SEKTORUNDA İKT VASİTƏLƏRİ

Bu sektorun əsas üstün və modern xüsusiyyətlərindən biri orada rəqəmsal çap texnologiyalarının geniş tətbiqidir. sektorda Rəqəmsal çap texnologiyalarının ən böyük üstünlüyü ondan ibarətdir ki, sifariş qısa müddətdə icra olunur. Burada çapdan əvvəlki ənənəvi metal formalardan və sazlama prosesindən istifadə olunmur. Dizayn olunmuş məhsul birbaşa kompüterdən çapa verilir. Rəqəmsal çapın daha bir üstünlüyü çapın təkə kağıza deyil, müxtəlif formalı və qalınlıqlı materiallara (parçaya, kartona, plastikə, lentə və s.) çapa verilə bilməsidir [8].

Rəqəmsal çapın üstünlüyündən danışırkən, əlavə vəsait sərf etmədən məhsulun saxtalaşdırılmasından qorunması imkanlarını da qeyd etmək lazımdır. Bu üsulla çap edilmiş məhsulların (məsələn, etiketlər, qablaşdırma məhsulları və s.) qorunma səviyyəsi daha yüksəkdir. Rəqəmsal çapın yeganə çatışmazlığı yüksək tirajlar zamanı onun baha başa gəlməsidir. Rəqəmsal avadanlığın istismar və boyu xərcləri ofset maşınından çox yüksəkdir.

Bu və bu kimi digər istehsal texnologiyalarının təhlili nəticəsində hesab etmək olar ki, formalaşmaqda olan müasir informasiya və bilik iqtisadiyyatının nəşriyyat-poliqrafiya

sektoru ancaq ən yüksək İKT infrastrukturunu, kommunikasiya-rabitə vasitələri və 4-cü sənaye inqilabına müvafiq, kiber-fiziki sistemlərdən ibarət platformada effektiv fəaliyyət göstərə bilər. Belə platforma isə təhdid və təhlükələrdən qoruna bilən yüksək inkişaf etmiş informasiya təhlükəsizliyi sisteminə, etibarlı telekommunikasiya şəbəkəsinə, naqilsiz xətlərə, monitoring sistemlərinə, texniki tənzimləyici strukturlara, yüksək səviyyədə təşkilati, maliyyə, ekoloji, sosial problemlərin operativ həllinə imkan verən strukturlara və mexanizmlərə malik olmalıdır [9].

Göründüyü kimi burada əsas məsələlərdən biri də informasiya infrastrukturunu və təhlükəsizliyinin səmərəli həllinə nail olmaqdır. Bu istiqamətdə ən qlobal texnologiyaların tətbiq olunması üçün yeni bilik və texnologiyaların baza sahələrdə praktiki realizasiyasına imkan verən ixtisaslaşdırılmış poliqrafik texnomərkəzlər, nəşriyyat strukturları və s. yaradılmalıdır.

IV. NƏŞRİYYAT-POLİQRAFIYA PROFİLLİ İKT-NİN TƏHLÜKƏSİZLİYİ İSTİQAMƏTLƏRİ VƏ TEXNOLOGİYALARI

Nəşriyyat-poliqrafiya sektorlarında (NPS) informasiya resurslarının, sistemlərinin, məhsul və xidmətlərin informasiya təhlükəsizliyi daha çox aşağıdakı kimi risklərə, təhdid və təhlükələrə məruz qala bilər [10,11]:

- Rəqəmsal mühitdə müəllif hüquqlarının təmini, onların identifikasiyası, onlara aid nəşr verilənlərinin, resurslarının saxlanması, onların inamının yüksəldilməsi;
- telekommunikasiya sistemlərindən və resurslarından istifadə zamanı NPS-də şəxsiyyətə, biznesə, dövlətə yaranan təhlükə və təhdidlər;
- NPS-nin informasiya infrastrukturuna xarici informasiya-texniki təsir imkanlarının artması;
- NPS-də daxili və xarici kompüter cinayətkarlığı səviyyəsinin yüksəlməsi;
- NPS-də aparıcı, güclü xarici dövlətlərdən rəqəmsal çap texnologiyalarının inkişaf səviyyəsinə görə geridə qalmaq;
- Çap avadanlıqlarının və proqram təminatının xarici dövlətlərin ixrac siyasətindən asılılığı;
- Poliqrafiya profilli İKT-nin inkişafı və təhlükəsizliyi aspektində kifayət qədər yüksək texniki təminatın və ixtisaslı personalın zəifliyi.

Göstərilən bu və ya digər təhlükəkarın zamanında qarşısının alınması üçün xüsusi çap aparat-texniki və proqram vasitələrin işlənilməsi çox yaxşı olardı. Ancaq belə xüsusi texnikanın və texnologiyaların işlənilməsi çətin olduğundan və böyük maliyyə vəsaitləri tələb etdiyindən ilk növbədə əksər

sahələrdə istifadə oluna bilən standart, baza, universal çap texnologiyaların tətbiq olunması tövsiyə olunur:

- NPS-də kiber-fiziki sistemlərin, komplekslərin aparat-texniki vasitələrinin yaradılması texnologiyaları;
- NPS-də kiber-bioloji insan-maşın sistemlər və texnologiyaları;
- NPS-də verilənlərin sürətli yığılması, emalı, ötürülməsi texnologiyaları;
- NPS-də istehsal/xidmət profilli robototexniki texnologiyalar;
- Nəşriyyat-poliqrafiya sənayesi interneti və əşyaların interneti texnologiyaları;
- NPS-də ehtiyatların və növbələrin idarə olunması texnologiyaları;
- NPS-də idarəetmə üzrə koqnitiv texnologiyalar;
- İdarəetmə və istehsal sferasında duman-bulud hesablamaları texnologiyaları;
- NPS-də böyük verilənlərin yığılması, emalı (Big-data) texnologiyaları;
- NPS-də paylanmış hesablamalar və çap texnologiyaları;
- Fraktal texnologiyalar;
- 3D çap texnologiyaları;
- Soft-komputinq texnologiyaları;
- Proqram mühəndisliyi texnologiyaları və s.

Bu cür qabaqcıl texnologiyaların tətbiqi zamanı risk və təhlükələrin azaldılması istiqamətləri daha çox: a) daxili və xarici informasiya təhlükəsizliyinin müdafiəsinə, b) ölkənin dayanıqlı sosial-iqtisadi inkişafına və suverenliyinə yönəldirilmişdir. Bu kompleks istiqamətləri aşağıdakı kimi tədbirlərin yerinə yetirilməsiylə ifadə etmək olar:

- Çap məhsullarının emalı mərkəzləri infrastrukturunun və aparat vasitələrinin fəaliyyətinin təhlükəsizliyinin və texnoloji müstəqilliyinin təmini;
- Yeni iqtisadi şəraitdə 3D-çap istiqamətli kiber-fiziki sistemlərin fəaliyyət mexanizmlərinin təhlükəsiz təmini;
- NPS-də kiber-fiziki sistemlərin fəaliyyəti üçün zəruri əsasların yaradılması;
- NPS-də müxtəlif səviyyəli və təyinatlı istehsal/xidmət informasiya sistemlərinin və texnologiyalarının təhlükəsizliyinin və dayanıqlılığının təmini;
- Yeni iqtisadi şəraitdə informasiya təhlükəsizliyi üzrə milli və beynəlxalq qarşılıqlı əlaqələrin təmini;
- Beynəlxalq iqtisadi informasiya fəzaları ilə inteqrasiya olunan informasiya resurslarının, sistemlərinin təhlükəsizliyinin təmini və s.

Göstərilən tədbirlər informasiya təhlükəsizliyi sistemlərinin, interfeyslərinin, elementlərarası qarşılıqlı əlaqə protokollarının, aparat vasitələrinin yeni idarəetmə konsepsiyasının işlənməsini tələb edir.

Bunlarla yanaşı olaraq bəzi informasiya təhlükəsizliyi texnologiyalarını da qeyd etmək yerinə düşərdi [12]:

- NPS-də kompüter hücumlarının qarşısının əvvəlcədən alınmasına xidmət edən koqnitiv texnologiyalar;
- Bazardakı vəziyyətin modelləşməsi və proqnozlaşdırılması texnologiyaları;
- NPS üzrə Big data əsaslı proseslərin informasiya təhlükəsizliyi təminatının intellektual texnologiyaları;
- NPS-də proqram-konfigurasiyalı şəbəkə və şəbəkə funksiyalarının virtuallaşması texnologiyaları;
- 3D-çap modullar texnologiyaları;
- Nəşriyyat-poliqrafiya sektorunda sənaye və əşya internetinin təhlükəsizliyi texnologiyaları.

NƏTİCƏ

Azərbaycan iqtisadiyyatının innovasiyalara, inkişafa və biliklərə əsaslandığı indiki şəraitdə nəşriyyat poliqrafiya sektoru ciddi formalaşma və inkişaf dövrünü yaşayır. Bu sahənin informasiya təhlükəsizliyinə yalnız sistemli yanaşma əsasında nail olmaq olar. Burada həm qanunvericilik aspektində inzibati mexanizmlərdən, həm də təşkilati effektiv tədbirlərdən və müvafiq müasir nəşriyyat aparat-texniki vasitə və texnologiyalardan kompleks şəkildə istifadə olunmalıdır.

ƏDƏBİYYAT

- [1] “Telekommunikasiya və informasiya texnologiyalarının inkişafına dair Strateji Yol Xəritəsi”, Bakı, 6 dekabr 2016-cı il. <http://mincom.gov.az>
- [2] “Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Stratejiya”nın təsdiq edilməsi haqqında Azərbaycan Respublikası Prezidentinin Sərəncamı, 02.04.2014-cü il, <http://www.president.az>
- [3] A.G. Aliyev. Methodological aspects of estimation of ICT-based economic development. International Journal Management Dynamics in the Knowledge Economy. 2018, vol.6 no.2, pp.227-245
- [4] A. G. Aliyev. Mechanisms of application of ecological environmental technologies in information economy. International Journal of Advanced Engineering and Technology. 2018, vol. 2, issue 1, pp. 33-40
- [5] Р. М. Алигулиев, А. Г. Алиев. Проблемы информатизации общества и экономики. Баку, “ЭЛМ”, 2003, 460 с.
- [6] А. Г. Алиев. Теоретико-практические основы информатики, ИКТ и информатизации. Баку, “ТАХСИЛ”, 2005, 176 с.
- [7] Nəşriyyat işi haqqında Azərbaycan respublikasının qanunu. Bakı şəhəri, 30 may 2000-ci il. <http://www.e-qanun.az/framework/115>
- [8] Q. Toğrul. Poliqrifiya məhsulları istehsalı: əlverişli biznes mühitin yaradılması imkanları. http://edf.az/ts_general/azl/ksid/downloads/qalib-togrul_poliqrifiya-mehsullari-biznesi.pdf
- [9] Е. В. Никольчев. ИТ в полиграфии. Высшее образование в России. №6, 2010. Стр.105-109
- [10] Д. И. Попов, Е. Д. Попова, А. В. Некрасов. Информационные технологии в издательском деле и полиграфии: основы проектирования баз данных. Москва, 2015

- [11] О. Р. Жаворонкова, Я. С. Цепкова. Современное состояние и перспективы развития рынка полиграфических услуг в России. АНИ: экономика и управление. 2017. Т. 6. № 1(18). Стр.69-72.
- [12] А. А. Рогов. ИКТ в полиграфии и дизайне. Наука. Искусство. Культура. № 2 (14) ,2017. Стр.177-179

**MODERN ICT IN THE CONDITION OF INFORMATION
ECONOMY IN THE FORMATION OF PUBLISHING-
POLYGRAPHY SECTOR THEIR SECURITY ISSUES**

Alovsat Aliyev¹, Anar Samidov², Roza Shahverdiyeva³, Leyla
Akbarova⁴

^{1,2,3,4}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹alovsat_qaraca@mail.ru, ²anarsamidov@gmail.com

Abstract – The article focuses on modern ICT software-tools, systems, resources and their security issues in creating an innovative publishing-polygraphic sector in the context of the information economy. The role of ICT, knowledge and innovation in economic development has been studied and its importance has been demonstrated. The role and place of the publishing-printing sector in the information economy has been clarified. The innovative features of the publishing-printing sector, the institutional structure and development stages are explained. Innovative ICT tools and their security problems have been explored to improve the effectiveness of the publishing and printing industry. Some recommendations have been made to solve these problems.

Keywords – information economy, publishing and printing sector, 3D printing, ICT security

Transliterasiya – milli identikliyə böyük təhlükə mənəyi kimi

Səbinə Məmmədşadə

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

sabinamammadzadeh@gmail.com

Xülasə - Məqalədə transliterasiya probleminin milli identikliyin pozulmasına göstərdiyi təsiri araşdırılmışdır. Qlobal informasiya mühitində transliterasiyanın əsas mübadilə elementlərindən biri olduğu, onun əhəmiyyəti və yaratdığı problemlər vurğulanmışdır. Qeyd edilən problemlər, eyni sözlərin virtual mühitdə bir neçə variantlarda verilməsi ilə nümunələrlə izah edilmişdir. Məqalədə transliterasiya probleminin virtual məkanda həlli, mədəniyyətlərarası ünsiyyətin sadələşdirilməsi və milli identikliyin transliterasiya vasitəsilə qorunması üçün bir sıra təkliflər irəli sürülmüşdür.

Açar sözlər - transliterasiya, romanizasiya, standart, virtual məkan, milli identiklik

I. GİRİŞ

Müasir dövrdə İnternet mühitində istifadə olunan dillərin bir-birinə göstərdikləri mənfi və müsbət təsirlərin öyrənilməsi mühüm əhəmiyyət kəsb edir. İnternetdə ingilis dilinin daha böyük üstünlüyə malik olması, onun digər dil və dil daşıyıcılarına təsiri dilçilik sahəsinin əsas tədqiqat obyektlərindən biridir. Qlobal mühitdə aparılan ünsiyyətin daha geniş homogenliyi, şəbəkə və multimediyaya texnologiyalarının sürətli inkişafı dil müxtəlifliyinin daha da genişlənməsinə səbəb olmuşdur. Bu da öz növbəsində dilçilik sahəsində əsas araşdırma mövzularından birinə çevrilmişdir [1].

Qeyd edilən dil müxtəlifliyi virtual məkanın ayrı-ayrı dil daşıyıcıları tərəfindən qeyri-bərabər şəkildə istifadəsinə səbəb ola bilər. Bu qeyri-bərabərliyin aradan qaldırılması isə həmin dillərin qlobal informasiya fəzasında ən geniş istifadə edilən ingilis dili ilə uyğunlaşdırılmasını (transliterasiyasını) zəruri edir. Müxtəlif dil daşıyıcıların transliterasiya cədvəllərindən istifadə etməklə öz milli dəyərlərini ictimaiyyətə düzgün çatdırması isə həmişə mümkün olmur. Beləliklə də milli identikliyin pozulması halları baş verir. Milli identikliyin pozulması problemi də transliterasiya sahəsinin informasiya təhlükəsizliyi baxımından araşdırılmasına zərurət yaradır.

II. TRANSLITERASIYA STANDARTLARININ ARAŞDIRILMASI

Hal-hazırda dünyada 7000-dən çox canlı dil siyahıya alınmışdır. Onların əksəriyyəti 100.000-dən az daşıyıcıya

malikdir. Lakin İnternetdə mövcud olan məlumatlar əsasən 11 dildə əlverişlidir. Qeyd olunan 11 dil isə hazırda və ya tarixən güclü olan dövlətlərin milli dilləri hesab olunur. Multilingvistik İnternet isə məhz həmin dil daşıyıcılarının maraqlarına xidmət edir. Buna baxmayaraq, multilingvistik İnternetin qlobal lingvistik müxtəliflik nöqtəyi nəzərindən yenidən araşdırılması mövcud yanaşmaları bir qədər yaxşıya doğru təkmilləşdirməyə şərait yarada bilər [2].

İnternet Systems Consortium və Domain Name System tərəfindən aparılan araşdırmalara əsasən, Şimali Amerika kimi aşağı lingvistik müxtəlifliyə malik regionda ingilis dili üstünlük təşkil edir. Bundan əlavə, Afrika kimi lingvistik müxtəlifliyin yüksək həddə olduğu yerlərdə isə İnternetə çıxış bəzən, hətta qeyri-mümkündür [3].

Şübhəsiz ki, hər kəsin dil bilmək və öyrənmək qabiliyyəti eyni deyildir. Lakin buna baxmayaraq ingilisdilli olmayan istifadəçilər də internetdə məlumat axtarır geniş auditoriya və elmi akademik cəmiyyətə çıxış imkanı əldə etməyə çalışırlar. Sunol və Saturnonun fikrincə başqa dillərdə ingilis dilində aparılan tədqiqatlar başqa dillərdə aparılan tədqiqatlardan üstünlük təşkil edir və daha əlverişlidir. Həmçinin digər dillərdə nəşr olunan məlumatlar bütünlükdə elmi ictimaiyyət üçün demək olar ki, çətin başa düşülən və analiz olunması qeyri-mümkün hesab olunur. Bu səbəbdən də ingilis dilini kifayət qədər öyrənmək mümkün olmadığı hallarda milli dillərin qlobal İnternet mühitində düzgün şəkildə əks etdirilməsi zəruriyyəti meydana gəlir. Bu məqsədlə həmin dillərin ingilis dili ilə (latın əlifbasının hərfləri ilə) uyğunlaşdırılması məsələsi meydana çıxır.

Qeyd etmək lazımdır ki, İnternet istifadəçiləri xüsusilə ingilis dil biliyi zəif olan istifadəçilər lazım olan informasiyanı və ya məlumatın axtarışı zamanı açar sözlərin daxil edilməsində çətinliklərlə qarşılaşırlar. Bu zaman axtarış nəticəsində əldə edilən məlumatın relevantlığı birbaşa tərcümənin və ya transliterasiyanın dəqiqliyindən asılıdır [4].

Bildiyimiz kimi veb resursların əksəriyyəti daha geniş auditoriya üçün əlverişli olmağına görə romanlaşdırılmışdır.

Romanlaşdırma dedikdə sözlərin hərbarhərflər latın dili qrafikasına çevrilməsi nəzərdə tutulur. Bu baxımdan dünyada çoxsaylı Romanizasiya cədvəlləri (transliterasiya interfeysləri) qəbul edilmişdir. ISO9 tərəfindən Azərbaycan dili üçün 3 standart qəbul edilmişdir:

1. 1984-cü ildə Azərbaycanda istifadə edilən ərəb əlifbasının (ISO 233: 1984) hərflərinin latın qrafikasının hərflərinə transliterasiyası
2. 1993-cü ildə Ərəb qrafikasının hərflərinin transliterasiyası (ISO 233)
3. 1995-ci ildə Kiril simvollarının latın simvollarına konvertasiyası (Slavyan və qeyri-Slavyan dilləri üçün).

Bəzi təşkilatlar tərəfindən Azərbaycan dili üçün transliterasiya cədvəlləri qəbul olunmasına baxmayaraq, həmin cədvəllərin modifikasiyası və standartlaşdırma problemləri hələdə öz həllini tapmamışdır. Transliterasiya cədvəllərinin təkmilləşdirilməsi dedikdə diakritik işarələrin cədvəldən çıxarılması, bəzi simvolların cədvələ əlavə edilməsi və Azərbaycan dilinin fonologiyasına uyğun olmayan bəzi hərflərin əvəzlənməsi başa düşülür.

III. TRANSLITERASIYADA İDENTİKLİK PROBLEMI

Transliterasiya edilmiş materialların hər biri milli identikliyin qorunması üçün dəyərli bir resursa çevrilir. Buna baxmayaraq, müxtəlif dövrlərdə konvertasiya cədvəllərinə edilən çoxsaylı dəyişikliklər eyni sözlərin İnternetdə fərqli transliterasiya variantlarının yayılmasına səbəb olmuşdur. Bu problemin həlli Azərbaycan xalqının sosial və psixoloji, habelə mənəvi təfəkkürünün müvafiq istiqamətdə dəyişdirilməsini, o cümlədən Azərbaycan dili üçün vahid transliterasiya standartının qəbul edilməsini zəruriyyətini yaradır.

Yuxarıda qeyd edildiyi kimi, müxtəlif transliterasiya variantlarının yayılması milli identikliyin pozulmasına gətirib çıxarır. Bu problem, vahid transliterasiya standartının qəbul edilmədiyi bütün dillərdə mövcuddur. Məsələn, İnternetdə "Хрушев" soyadı üzrə axtarış etdikdə, aşağıda qeyd olunan 60 variantın olduğunu demək mümkündür:

Hrushev, Hrushew, Hrushyev, Hrushyew, Hrushjev, Hrushjew, Hruschev, Hruschew, Hruschyev, Hruschyew, Hruschjev, Hruschjew, Hrushchev, Hrushchew, Hrushchyev, Hrushchyew, Hrushchjev, Hrushchjew, Hruchhev, Hruchhew, Hruchhyev, Hruchhyew, Hruchhjev, Hruchhjew, Hruwev, Hruwew, Hruwyev, Hruwyew, Hruwjev, Hruwjew, Xrushev, Xrushew, Xrushyev, Xrushyew, Xrushjev, Xrushjew, Xruschev, Xruschew, Xruschyev,

Xruschyew, Xruschjev, Xruschjew, Xrushchev, Xrushchew, Xrushchyev, Xrushchyew, Xrushchjev, Xrushchjew, Xruchhev, Xruchhew, Xruchhyev, Xruchhyew, Xruchhjev, Xruchhjew, Xruwev, Xruwew, Xruwyev, Xruwyew, Xruwjev, Xruwjew, Khrushev, Khrushew, Khrushyev, Khrushyew, Khrushjev, Khrushjew, Khruschev, Khruschew, Khruschyev, Khruschyew, Khruschjev, Khruschjew, Khrushchev, Khrushchew, Khrushchyev, Khrushchyew, Khrushchjev, Khrushchjew, Khrushchew, Khrushchjew, Khrushchyew, Khrushchjev, Khrushchjew, Khruchhev, Khruchhew, Khruchhyev, Khruchhyew, Khruchhjev, Khruchhjew, Khruwev, Khruwew, Khruwyev, Khruwyew, Khruwjev, Khruwjew

[5].

Bu variantlardan hər biri transliterasiya edilən dillərin qrammatik, orfoqrafik və fonoloji xüsusiyyətlərinə uyğun olaraq qəbul edilmişdir. Başqa bir nümunə isə Azərbaycan soyadı olan "Quliyev" soyadı ilə bağlıdır. Belə ki, bu soyad Quliyev, Quliev, Kuliev, Kuliye, Guliyev və Guliev kimi çoxsaylı formalarda transliterasiya edilmişdir. Bu fərqli formaların yaranma səbəbi əsasən rus dilinin Azərbaycan dilinə uzun müddət göstərdiyi təsiri ilə bağlıdır. Beləliklə, transliterasiya edilən "Q" və "y" hərfləri uzun illər beynəlxalq aləmdən təcrid olunmuş Azərbaycan dilindən ilk olaraq rus dilinin fonetik xüsusiyyətlərinə uyğun olaraq kiril əlifbasına müvafiq olaraq "K" və "e" kimi transliterasiya edilərək daha sonra digər dillərə də yanlış olaraq "K" və "e" kimi transliterasiya edilmişdir. Nəticə etibarilə onu qeyd etmək olar ki, çoxlu sayda ad, soyad və yer adlarının identikliyi pozulmuşdur.

Ümumiyyətlə, transliterasiya problemi səbəbindən meydana gəlmiş identiklik məsələləri bəzi siyasi və sosial amillərdən asılı olmuşdur. Belə ki, müasir Azərbaycan Respublikasının ərazisi müəyyən dövrlərdə müxtəlif dövlətlər tərəfindən işğal edilmişdir. Hər işğalçı dövlət özü ilə yeni mədəniyyət, ənənə və dil xüsusiyyətləri gətirmişdir. Ərəb Xilafəti tərəfindən Azərbaycanın işğal edilməsi və bununla da İslam dininin yayılması ilə əlaqədar burada istifadə edilən qədim latın əlifbasının sıxışdırılıb və ərəb əlifbası ilə əvəz edilmişdir. Keçmiş Sovetlər Birliyi dövründə isə ərəb əlifbası kiril əlifbası ilə əvəz edilmişdir.

Bundan əlavə, müxtəlif dövrlərdə, sözügedən kiril əlifbasının Azərbaycan dilinin fonoloji xüsusiyyətləri ilə uyğunlaşdırılması məqsədilə bir neçə dəfə dəyişdirilmişdir. Lakin, 1991-ci ildə Azərbaycan dövləti müstəqillik qazandıqdan sonra Azərbaycan dili üçün latın qrafikası qəbul

edilmişdir. Burada əsas məsələ hər bir dövrdə yaradılan ədəbiyyat əlyazmaları, siyasi sənəd və materialların identikliyinə qorunması və onların gələcək nəsillərə düzgün şəkildə ötürülməsi zərurətidir.

IV. AZƏRBAYCAN-FARS ƏLİFBALARININ TRANSLİTERASIYA PROBLEMLƏRİ

Britannica Ensiklopediyasının hesabatına əsasən, hazırda İranda 15 milyondan çox azərbaycanlı yaşayır [6]. Burada Azərbaycan dili ana dili kimi əsasən Təbriz, Zəncan, Ərdəbil kimi böyük şəhər və vilayətlərdə geniş şəkildə istifadə olunduğuna baxmayaraq, bu dil üçün ərəb əlifbası əsasında tərtib edilmiş Fars qrafikası istifadə olunur. Qeyd edilən ərazilərdə yerləşən məktəb və universitetlərdə, o cümlədən, Təbriz Universitetində Azərbaycan dilinin təhsildə istifadəsinə İran hökuməti qadağa qoymuşdur. Halbuki, Azərbaycan əyalətlərində yerləşmiş təhsil müəssisələrində fars dilindən başqa yeddi xarici dildə aparılır [7]. Azərbaycan dilinin digər dillərlə, xüsusilə də ingilis dili ilə transliterasiya probleminin həlli dünyada yaşayan 30-35 milyon azərbaycanlıların virtual məkanda ünsiyyəti üçün də əhəmiyyət kəsb edir [8].

Ümumiyyətlə, Azərbaycan dilinin İranda istifadəsinə qoyulan qadağalar yalnız təhsildə deyil, kütləvi informasiya vasitələrində də özünü biruzə verir. İran konstitusiyası "mətbuat və kütləvi informasiya vasitələrində regional və ya qəbilə dillərinin istifadəsinə" icazə verməsinə baxmayaraq [9], burada Azərbaycan dilinin istifadəsi sıxışdırılır. Məsələn, Zəncan Əyalətinin Radio və Televiziyasının uşaq, böyük və yaşlılar üçün yayımladığı proqramların 50%-dən az bir hissəsinə yalnız Azərbaycan dilində yayımlanmasına icazə verilir. Bundan əlavə, Azərbaycan dilində nəşr olunan istənilən yazı ictimaiyyətə yalnız fars əlifbasında təqdim olunur [10]. Belə olduğu halda Azərbaycan dilindəki bütün sözlər fars dilinin orfoqrafik və fonoloji xüsusiyyətləri nəzərə alınmaqla əvvəlcə fars əlifbasına, daha sonra isə global informasiya fəzasına transliterasiya edilərək təqdim olunur. Təbii ki, həmin sözlərin əksəriyyəti Cənubi Azərbaycanda yaşayan soydaşlarımız tərəfindən bir qədər dəyişdirilərək öz dialektlərinə uyğunlaşdırılmış şəkildə istifadə edilir. Məhz həmin sözlərin də bir neçə dəfə digər əlifbalara transliterasiya edilməsi onların təhrif olunmasına gətirib çıxarır. Bu isə birbaşa milli identikliyin pozulmasına gətirib çıxarır. Bu, əsasən şəxs adları, milli-mənəvi dəyər kəsb edən obyektlərin adları və toponimlərin identikliyinə təhlükə yaradır. Məsələn, "Suleymanov" soyadı fars dilinin fonologiyasına uyğunlaşdırılaraq əvvəlcə fars əlifbasına, daha sonra latın əlifbasına "Souleimanov" kimi transliterasiya olunur.

V. AZƏRBAYCANDA TRANSLİTERASIYA SAHƏSİNDƏ MÖVCUD PROBLEMLƏR VƏ ONLARIN HƏLLİ ÜÇÜN TƏKLİFLƏR

Transliterasiya probleminin yuxarıda qeyd edilən məsələlər yalnız İranda deyil, Azərbaycan Respublikası ərazisində də mövcuddur. Belə ki, əksər rayon və şəhər adları sovet hakimiyyəti dövründə əvvəlcə rus dilinin fonoloji xüsusiyyətlərinə uyğunlaşdırılmış, daha sonra isə beynəlxalq ictimaiyyətə də o şəkildə təqdim edilmişdir. Buna misal olaraq, Zaqatala - "Закаталы" ("Zakataly"), Balakən - "Белоканы" ("Belokan"), Şamaxı - "Шемаха" ("Shemaxa") və Naxçıvan - "Нахичевань" ("Nakhichevan") kimi şəhər adlarının transliterasiyasını göstərmək olar. Toponimlərin bu şəkildə təhrif edilərək global informasiya fəzasında yayılması identikliyin pozulması ilə nəticələnir. Bu təhriflər, bəzi hallarda yalnız transliterasiya olunan dillərin qrammatik xüsusiyyətləri ilə deyil, həmçinin siyasi-ideoloji faktorlarla bağlı ola bilər. Məsələn, Şamaxı şəhərinin adının "Шемаха" ("Shemaxa") şəklində transliterasiya edilməsi Rusiya Federasiyasının Çelyabinsk vilayətində "Şemaxa" çayı sahilində yerləşən eyni adlı kəndin adı ilə eyniləşdirilə bilər [11].

Transliterasiya sahəsində mövcud problemlərdən biri də artıq istifadə edilməyən qədim əlifbalar üçün konvertasiya cədvəllərinin qəbul edilməməsidir. Bu, qədim əlifbalarda yazılmış çoxsaylı materialların, sənəd və kitabların oxunması, ictimaiyyətə əlverişli olması, milli-mənəvi dəyərlərin aşkarlanması və gələcək nəsillərə təhrif edilmədən ötürülməsi üçün əhəmiyyətlidir.

Transliterasiya problemlərinin hərtərəfli həlli üçün aşağıdakı tədbirlərin görülməsi təklif edilir:

- Azərbaycan dilinin qrafikası üçün qəbul edilmiş mövcud konvertasiya cədvəllərinin təkmilləşdirilməsi və ya yeni konvertasiya cədvəllərinin hazırlanıb, təsdiq edilməsi üçün Beynəlxalq Standartlaşdırma Təşkilatına (ISO) təqdim edilməlidir. Onu da qeyd etmək lazımdır ki, həmin cədvəllərə ediləcək dəyişikliklər Azərbaycan dilinin qrammatik, orfoqrafik və fonoloji xüsusiyyətlərinə uyğun olaraq müəyyən elm sahələrinin mütəxəssisləri tərəfindən aparılmalıdır.
- Azərbaycan dili üçün indiyədək qəbul edilən əlifbalarının bir-biri ilə vahid transliterasiya cədvəlləri qəbul edilməlidir.
- Azərbaycan dilinin qrafikasının digər dillərin qrafikaları ilə transliterasiya sistemi yaradılmalıdır.
- Təklif olunan transliterasiya sistemi sınaqdan keçirilməsi və təkmilləşdirilməsi üçün istifadəçilər ilə əks əlaqə qurulmalı və onlardan gələn təklif və tövsiyələr nəzərə alınmalıdır.

VI. NƏTİCƏ

Məqalədə transliterasiya probleminin milli identikliyin pozulmasına göstərdiyi təsirlər, virtual məkanda ingilis dilinin geniş istifadəsi və digər dillərə təsiri, o cümlədən Azərbaycan dilinin ingilis dili ilə uyğunlaşdırılması məsələləri araşdırılmışdır. Transliterasiya sahəsində mövcud problemlərin həlli üçün konvertasiya cədvəllərinin təkmilləşdirilməsi və ya yeni konvertasiya cədvəllərinin hazırlanması, Azərbaycan dilinin qrafikasının digər dillərin qrafikaları ilə transliterasiya sistemi yaradılması və s. təkliflər irəli sürülmüşdür.

ƏDƏBİYYAT

- [1] Herrings, S.C. 2002. The language of the Internet: English dominance or heteroglossia? Keynote Speech Delivered at the International Conference on Cultural Attitudes Towards Technology and Communication, University of Montreal, Quebec, Canada
- [2] <https://www.ethnologue.com/statistics>, Ethnologue: Languages of the World (21st edition)
- [3] Brenda Danet, Susan C. Herring. The Multilingual Internet-Language, Culture, and Communication, Oxford University Press, 2007. pp. 16-18
- [4] Sunol, R., Satumo, P. (2008)). İLQİA jurnalının yeni təşəbbüsünü dərc etmək. 1-2
- [5] <https://www.analizfamilii.ru/Khrushchev/translit.html>
- [6] "Azerbaijani (people)". Encyclopedia Britannica. Retrieved 24 January 2012. <https://www.britannica.com/topic/Azerbaijani-people>
- [7] Asim Jannatoglu, THE MINORITY RIGHTS OF AZERBAIJANI TURKS IN IRAN, Middle East Review of International Affairs, Vol. 20, No. 1 (Spring 2016) p.9
- [8] Sela, Avraham (2002). The Continuum Political Encyclopedia of the Middle East. Continuum. p.197. ISBN0-8264-1413-3
- [9] The Constitution of the Islamic Republic of Iran, Article 15, Iran Human Rights Documentation Center, <http://www.iranhrdc.org/english/english/human-rights-documents/iranian-codes/3017-the-constitution-of-the-islamic-republic-of-iran.html?p=7>
- [10] FIDH/Discrimination Against Religious and Ethnic Minorities in Iran, Paris, Geneva, New York, 77th Session of the United Nations Committee on the Elimination of Racial Discrimination, July 2010, <http://www.refworld.org/pdfid/4c8622f72.pdf>, p. 16
- [11] Шемаха, Челябинская область. Мир путешествий и приключений. Проверено 30 июня 2008. Архивировано 15 марта 2012 года

TRANSLITERATION - AS A SOURCE OF GREAT DANGER TO NATIONAL IDENTITY

Sabina Mammadzada

Institute of Information Technology of ANAS
sabinamammadzadeh@gmail.com

Abstract -- The article examines the impact of the transliteration problem on the national identity. It highlights transliteration as one of the key elements of communication in the global information environment, its importance, and the problems caused by transliteration. These problems are explained by several transliteration forms of the same words in a virtual environment. The article offers a number of recommendations for resolving the transliteration problem in virtual space, simplifying intercultural communication and protecting national identity through transliteration.

Keywords -- transliteration, romanization, standard, virtual space, national identity

Twitter məlumatlarının sentiment analizi

Məkrufə Hacırahimova¹, Adilə İmamverdiyeva²

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

¹makrufa@science.az, ²imamverdiyeva1998@gmail.com

Xülasə— Twitter mikrobloqların paylaşıldığı onlayn sosial şəbəkə saytıdır. Qeydiyyatdan keçmiş istifadəçilərinin sayı 500 milyon olan Twitter-də hər gün 400 milyondan çox mesaj yayılır. Bu tvitlər, demək olar ki, cəmiyyətdə cərəyan edən bütün hadisələr haqqında məlumatları və şəbəkə iştirakçılarının onlara münasibətlərini əks etdirir. Bir çox ölkədə Twitter ictimai rəyə böyük təsir göstərir. Bu məqalədə Twitter məlumatlarından əlamətlərin çıxarılmasına və müxtəlif maşın təlimi metodları ilə onların emosional “rənginin” (pozitiv və neqativ) müəyyən edilməsi məsələsinə baxılmışdır.

Açar sözlər— Twitter; sosial şəbəkə; sentiment analiz; maşın təlimi.

I. GİRİŞ

Twitter istifadəçilərin tvitlər kimi tanınan qısa mesajlarla (140 simvola qədər) qarşılıqlı əlaqədə olduğu məşhur sosial şəbəkə saytıdır. Bu şəxslərin müxtəlif mövzular haqqında düşüncə və duyğularını ifadə etmək üçün bir vasitədir. İstehlakçılar və marketoloqlar kimi müxtəlif tərəflər məhsullar haqqında fikirləri toplamaq və ya bazarı analiz etmək üçün bu tvitlərin sentiment analizini yerinə yetirirlər. Tvitlərin sentiment analizi ictimai rəyin öyrənilməsi üçün də vacib alətdir. Bu işdə aşağıdakı anlayışlar istifadə olunur:

Sentiment – müəllifin obyektə (prosesə) emosional münasibətini bildirməsidir.

Sentiment analiz – müəllifin obyektə emosional münasibətinin kontent analiz metodları ilə avtomatik müəyyən edilməsi prosesidir.

Bu işin əsas məqsədi müxtəlif maşın təlimi alqoritmlərindən istifadə edərək tvitlər üzərində sentiment analiz aparmaqdır. Qeyd edək ki, Twitter məlumatlarının sentiment analizi metodlarının icmalısı [1]-də, sentiment analiz üçün istifadə edilən verilənlər toplularının icmalısı isə [2]-də verilmişdir.

Bu tədqiqatda Twitter verilənləri bazası Kaggle saytıdan götürülərək istifadə edilmişdir [3]. Verilənlərdə emosiya ikonaları, istifadəçi adları və heşteqlər olur, onları ilkin emal etmək və standart formaya çevirmək lazımdır. Həmçinin sentiment müəyyən etmək üçün tvitdən unigramlar və biqramlar kimi faydalı əlamətləri çıxarmaq lazımdır. Alınmış əlamətlərdən istifadə edərək sentiment

analiz etmək üçün müxtəlif maşın təlimi alqoritmlərindən istifadə edilmişdir.

II. VERİLƏNLƏRİN İLKİN EMALI

Verilənlər vergüllə ayrılmış mətnlər şəklində tvitlər və onlara uyğun sentiment sinifləri şəklindədir. Təlim verilənləri tweet_id, sentiment, tweet tipində bir .csv faylıdır, tweet_id tviti müəyyən edən unikal tam ədəddir, sentiment 1 (pozitiv), ya da 0 (neqativ), tweet isə “ ” şəklində yazılan tvitdir. Eyni şəkildə test verilənlər də tweet_id, tweet tipli bir .csv fayldır.

Verilənlər sözlər, simvollar, emosiya ikonaları, URL və istifadəçilərə istinadların qarışığıdır. Sözlər və emosiya ikonaları sentiment proqnozlaşdırmağa kömək edir, amma URL və istinadlar nəzərə alınmaya bilər. Sözlər həmçinin səhv yazılmış sözlərdən, çoxlu nöqtələrdən və bir çox təkrarlanan hərflərdən düzələn sözlərin bir qarışığıdır. Buna görə, standart formaya gətirmək üçün onları ilkin emal etmək lazımdır.

Təqdim edilən təlim və test verilənləri toplusunda uyğun olaraq, təxminən 800 min və 200 min tvit var.

Twitterdən götürülmüş emal edilməmiş tvitlər çox zaman küylü verilənlər toplusu olur. Bu, insanların sosial mediadan istifadəsinin təsadüfi əlamətlərindəndir. Tvitlərin istifadəçi istinadları, emosiya ifadələri və s. kimi xüsusi əlamətləri var. Emal edilməmiş twitter verilənləri müxtəlif klassifikatorlar vasitəsilə asanlıqla öyrənilə biləcək bir verilənlər toplusu yaratmaq üçün normallaşdırılmalıdır. Verilənləri standart formaya gətirmək və ölçüsünü azaltmaq üçün çox sayda ilkin emal addımları tətbiq etmək lazımdır.

Övvəlcə tvitləri aşağıdakı kimi ilkin emal edirik:

1. Tvitə kiçik hərflərə çeviririk.
2. 2 və ya daha çox nöqtəni (.) boş sahə ilə əvəzləyirik.
3. Tvitlərin sonunda dırnaq və boş sahələri atırıq.
4. 2 və ya daha çox boş sahəni bir boş sahə ilə əvəzləyirik.

Tvitlərdəki xüsusi əlamətlər aşağıdakı kimi emal edilir.

URL – istifadəçilər öz tvtlərində tez-tez müxtəlif veb səhifələrin hiper-linklərini bölüşürlər. Mətn klassifikasiyası üçün hər hansı bir xüsusi URL vacib deyildir, çünki bu çox seyrək əlamətlərə gətirib çıxara bilər. Buna görə də biz tvtlərdəki bütün URL-ləri URL sözü ilə əvəz edirik. URL-ləri tapmaq üçün istifadə olunan requlyar ifadə ((www\.[\S]+)|(https?:\/\/[\S]+)) 'dir.

İstifadəçi istinadları (ing. User Mention) – hər bir Twitter istifadəçisinin onunla əlaqələndirilən bir deskriptoru (ing. handle) var. İstifadəçilər tez-tez tvtlərində @handle ilə digər istifadəçilərə istinad edirlər. Bütün istifadəçi istinadlarını USER_MENTION sözü ilə əvəz edirik. İstifadəçi istinadlarını tapmaq üçün istifadə olunan requlyar ifadə @[\S]+ 'dir.

İkona (ing. emoticon) – istifadəçilər fərqli emosiyaları ifadə etmək üçün tvtlərində bir sıra fərqli emojiya ikonaları istifadə edirlər. Sosial mediada istifadə olunan emojiya ikonalarının sayı artır, buna görə onların hamısını nəzərə almaq mümkün olmur. Biz ancaq çox istifadə olunan bəzi ümumi emojiya ikonalarını emal edirik. Emal edilmiş emojiya ikonalarını onların ifadə etdiyi emosiyanın pozitiv və ya neqativ olmasından asılı olaraq, EMO_POS və ya EMO_NEG ilə əvəz edirik.

Heşteq – heşteqlər Twitter-də trend mövzuna istinad etmək üçün istifadəçilər tərəfindən tez-tez istifadə olunan, heş simvolundan (#) sonra boşluq olmayan frazalardır. Biz bütün sözlü heşteqləri heş simvolu ilə əvəz edirik. Məsələn, #hello heşteqi “hello” ilə əvəz olunur. Heşteqləri tapmaq üçün istifadə olunan requlyar ifadə #(\S+) 'dir.

Retweet – Retvit artıq başqası tərəfindən göndərilmiş və digər istifadəçilər tərəfindən paylaşılmış tvtlərdir. Retvitlər RT hərfləri ilə başlayır. Tvtlərdən RT-lər atılır, çünki mətn klassifikasiyası üçün vacib bir əlamət deyillər. Retvitləri tapmaq üçün istifadə olunan requlyar ifadə \bret\b 'dir.

III. ƏLAMƏTLƏRİN ÇIXARILMASI

Verilənlər toplusundan iki əlamət çıxarılır: unigramlar və biqramlar. Bu unigramların və biqramların tezlik paylanması yaradılır və sentiment analiz üçün tezlikləri böyük olan ilk N unigram və biqram götürülür.

Unigramlar

Mətnlərin klassifikasiyası üçün ən sadə və ən çox istifadə edilən əlamətlər mətdə olan tək sözlər və ya tokenlərdir. Təlim verilənləri toplusundan tək sözlər çıxarılır və bu sözlərin tezlik paylanması yaradılır. Baxılan verilənlər toplusundan təxminən 181232 söz çıxarılmışdı. Tezliyi az olan sözlər cəmi bir neçə dəfə rast gəlir və onları küy hesab etmək olar. Buna görə klassifikasiya üçün sözlər çoxluğunu yaratmaq üçün tezliyi böyük olan ilk N sayda sözdən istifadə etmişik. Şəkil 1-də əlimizdə olan sözlər çoxluğundan tezliyi ən böyük 20 sözün tezlik paylanması göstərilir. Şəkil 2-də isə tezlik paylanmasının Zipf qanununa tabe olduğunu müşahidə edə bilərik. Zipf qanununa görə, sözün tezliyi tezlik cədvəlindəki sırası ilə tərs mütənəsbidir.

Bunu $\log(\text{tezlik})$ və $\log(\text{sıra})$ qrafiklərini qurmaq ilə görə bilərik. Şəkil 2 üçün $\log(\text{Frequency}) = -0.78 \log(\text{Rank}) + 13.31$ doğrudur.

Şəkil 1. İlk 20 unigramın tezliyi

Şəkil 2. Zipf qanunu

Biqramlar

Biqramlar korpusda ardıcıl gələn verilənlər sırasında söz cütləridir. Bu əlamətlər təbii dildə mənfi emosiyaları ifadə etmək üçün yaxşı üsuldur – “Bu yaxşı deyil”. Verilənlər bazasından cəmi 1954953 unikal biqram çıxarılıb. Sözlər çoxluğunu yaratmaq üçün tezliyi ən böyük olan 10000 biqram istifadə edirik. Sözlər çoxluğunda tezliyi ən böyük olan 20 biqramın tezlik paylanması şəkil 3-də göstərilir.

Şəkil 3. İlk 20 biqramın tezliyi

IV. KLASSİFİKATORLAR

Eksperimentlər üçün aşağıdakı klassifikatorlar seçilib.

Baseline – bu modeldə tvitin sentimentini tapmaq üçün neqativ və pozitiv sözlərin sayı istifadə edilib (**Opinion Dataset** toplusundan götürülür). Pozitiv və neqativ sözlərin sayı bərabər olduqda, sentiment müsbət götürülür.

Naive Bayes

Naive Bayes mətnlərin klassifikasiyası üçün istifadə edilə biləcək ən sadə bir modeldir. Bu modeldə t tviti üçün $\hat{c}$ sinfi aşağıdakı kimi təyin olunur:

$$\hat{c} = \underset{c}{\operatorname{argmax}} P(c|t)$$

$$P(c|t) \propto P(c) \prod_{i=1}^n P(f_i|c).$$

Yuxarıdakı düsturda f_i bütün n əlamət arasından i -ci əlaməti işarə edir. $P(c)$ və $P(f_i|c)$ isə maksimal həqiqətəoxşarlıq qiymətləri ilə əldə edilə bilər.

Decision Tree (Qərar ağacı)

Qərar ağacı klassifikasiya modelidir, burada ağacın hər bir düyünü verilənlər toplusunun atributu üzrə testi, ondan çıxan budaq (övlad) isə testin nəticəsini müəyyən edir. Yarpaq düyünləri isə verilənlərin son siniflərini təyin edir. Qərar ağacını qurmaq üçün sinif nişanları məlum olan verilənlər istifadə edilir, sonra qurulmuş model test verilənlərini klassifikasiya etmək üçün tətbiq olunur. Ağacın hər bir düyünündə budaqlanmanı tapmaq üçün ən yaxşı qərar qəbul edilməlidir. Ən yaxşı budaqlanmaya qərar vermək üçün GINI əmsalından istifadə edirik. Verilmiş t düyünü üçün $GINI(t) = 1 - \sum_j [p(j|t)]^2$ kimi hesablanır, burada $p(j|t)$ – t düyünündəki j sinfinin nisbi tezliyidir. $GINI_{split} = \sum_{i=1}^k \frac{n_i}{n} GINI(i)$ budaqlanmanın keyfiyyətini göstərir. (n_i – i -ci övladda düyünlərin sayı, n isə p düyünündə yazıların sayıdır). GINI əmsalını minimal edən bir bölünmə seçilir.

Random Forest (Təsadüfi meşə)

Təsadüfi meşə klassifikasiya və regressiya üçün ansambl təlim alqoritmidir. Təsadüfi meşə çoxlu sayda qərar ağacı klassifikatorlarından ibarətdir, yekun qərar ağacların qərarlarının aqreqasiyası əsasında yaradılır. Tutaq ki, $x_1, x_2, \dots, x_n$ tvitlər çoxluğu, $y_1, y_2, \dots, y_n$ isə onların müvafiq sentiment nişanlarıdır. Bagging tətbiq edilməklə əvəzləmə ilə təsadüfi bir (X_b, Y_b) cütü seçilir. Hər bir klassifikasiya ağacı f_b təsadüfi bir (X_b, Y_b) istifadə edərək öyrədilir, burada $b = 1 \dots B$ aralığındadır. Sonda bu B sayda qərar ağacının yekun qərarı majoritar səsvermə ilə müəyyən edilir.

XGBoost

XGBoost qradient bustinqi alqoritmının bir formasıdır, zəif proqnozlaşdırılan qərar ağaclarının ansamblıdır. K modelin ansamblı onların nəticələri aşağıdakı şəkildə birləşdirilərək istifadə edilir:

$$\hat{y}_l = \sum_{k=1}^K f_k(x_i), f_k \in F$$

burada F ağacların fəzasıdır. x_i giriş veriləni, $\hat{y}_l$ isə yekun çıxışıdır. Aşağıdakı zərər funksiyasını minimallaşdırmağa çalışırıq:

$$L(\Phi) = \sum_i l(\hat{y}_i, y_i) \sum \Omega(f_k),$$

$$\text{burada } \Omega(f) = \gamma T + \frac{1}{2} \lambda \|\omega\|^2,$$

Ω – tənzimləyici toplananıdır.

SVM (Support Vector Machine)

Dayaq vektorları məşinləri kimi də tanınır, binar xətti klassifikatorudur. Tutaq ki, təlim toplusu (x_i, y_i) cütlərindən ibarətdir, burada x – əlamətlər vektoru, y isə ona uyğun sinif nişanıdır, $y \in \{+1, -1\}$. Biz elə hiper-müstəvi tapmaq istəyirik ki, o $y_i = 1$ və $y_i = -1$ nöqtələrini ayırsın və təlim çoxluğunun ən yaxın nöqtələrindən maksimal məsafədə keçsin.

Hiper-müstəvinin tənliyi $\omega \cdot x - b = 0$ ilə verilir. Optimal hiper-müstəvinin qurulması məsələsi aşağıdakı kimi ifadə olunur:

$$\min_w \frac{\|w\|^2}{2} \\ \text{Şərtlər: } y_i(w^T x + b) \geq 1$$

V. EKSPERİMENTLƏRİN NƏTİCƏLƏRİ

Yuxarıda təsvir olunmuş müxtəlif klassifikatorlar Python mühitində scikit-learn kitabxanasından istifadə edilməklə reallaşdırılıb və [3]-dən götürülmüş məlumatlar üzərində eksperimentlər aparılıb. Klassifikatorların eksperimentlərdə alınmış dəqiqliyi (ing. accuracy) cədvəl I-də verilib.

**CƏDVƏL I. KLASSİFİKATORLARIN SENTİMENTİ
TANIMA DƏQİQLİYİ**

Klassifikator	Dəqiqlik
Baseline	65.35 %
Naive Bayes	77.66 %
Decision Tree	68.48 %
Random Forest	72.20 %
XGBoost	76.95 %
SVM	78.24 %

Klassifikatorların dəqiqliyə görə müqayisəsi histoqramlarla şəkil 4-də göstərilir.

Şəkil 4. Klassifikatorların müqayisəsi

Ekspirimentlərin nəticələri göstərir ki, yalnız fərdi modellərə (klassifikatorlara) əsaslanmaq yüksək dəqiqlik vermir. Ona görə ən yaxşı modelləri seçərək modellər ansamblı yaratmaq lazımdır.

NƏTİCƏ

Məqalədə Twitter məlumatlarından əlamətlərin çıxarılmasına və müxtəlif maşın təlimi metodları ilə onların iki sentiment sinfinə (pozitiv və neqativ) klassifikasiyası məsələsinə baxılmışdır. Gələcək tədqiqatlarda mətnləri təsvir etmək, digər modellərdən istifadə etmək, neyron şəbəkələrə (MLP, CNN, RNN) əsaslanan bir neçə klassifikatoru sentiment analiz üçün tətbiq etmək və baxılan məsələ üçün klassifikatorlar ansamblı qurmaq nəzərdə tutulur.

ƏDƏBİYYAT

- [1] A. Giachanou, & F. Crestani, “Like it or not: A survey of twitter sentiment analysis methods,” ACM Computing Surveys (CSUR), vol. 49(2), Article No. 28, pp. 28, 2016.

- [2] H. Saif, M. Fernandez, Y. He, & H. Alani, “Evaluation datasets for Twitter sentiment analysis: a survey and a new dataset, the STS-Gold,” 1st Interantional Workshop on Emotion and Sentiment in Social and Expressive Media: Approaches and Perspectives from AI (ESSEM), 2013.
- [3] <https://www.kaggle.com/c/twitter-sentiment-analysis2/data>
- [4] S. Shalev-Shwartz, & S. Ben-David, Understanding machine learning: From theory to algorithms. Cambridge university press. 2014.
- [5] A.C.Mueller, S. Guido, Introduction to Machine Learning with Python: A Guide for Data Scientists. O'Reilly Media, 2016.

ABOUT TWITTER SENTIMENT ANALYSIS

Makrufa Hajirahimova¹, Adila İmamverdiyeva²

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

¹makrufa@science.az, ²imamverdiyeva1998@gmail.com

Abstract – Twitter is a social networking site where microblogs are shared. More than 500 million registered users send more than 400 million messages every day. These tweets provide information on almost all events in the life of society and on the attitudes of network members towards them. In many countries, Twitter has a huge impact on public opinion. This article discusses extracting features from tweets and recognizing their emotional “color” (positive and negative) using various machine learning methods.

Keywords – Twitter, social network, sentiment analysis, machine tlearning.