UOT 004.9:351

İmamverdiyevY.N.
AMEA İnformasiya Texnologiyaları İnstitutu
yadigar@lan.ab.az

SOSİAL MEDİA VƏ TƏHLÜKƏSİZLİK PROBLEMLƏRİ

Sosial media təkcə rahat ünsiyyət və fayl paylaşımı platforması deyil, həm də ictimai-siyasi təsir və idarəetmə aləti, qarşıdurma və informasiya müharibəsi meydanıdır. Sosial media onu istifadə edənlərin məqsədlərindən asılı olaraq milli təhlükəsizliyə bir sıra təhdidlər də yarada bilər. Məqalədə sosial medianın milli təhlükəsizliyə təhdid törədə biləcək bir sıra risk ssenariləri təsvir edilir, sosial mediada saxta aktorların – botların yaradılması və idarə edilməsi texnologiyaları və bu sahədə bəzi ölkələrin təcrübəsi analiz olunur. Sosial medianın monitorinqi və analizi üçün mövcud onlayn servislər barəsində məlumat verilir.

Açar sözlər: *sosial media, milli təhlükəsizlik, sosial media monitorinqi, sosial media analitikası, informasiya təsiri, informasiya müharibəsi.*

Giriş

Veb 2.0 ideologiyası əsasında yaradılmış sosial şəbəkə servisləri qısa müddətdə – son on il ərzində rahat ünsiyyət və fayl mübadiləsi vasitəsindən unikal kontent generasiya edən və yayan sosial mediaya çevrilmişdir [1]. Hazırda sosial mediaya bloqlar (*Blogger, LiveJournal*), mikro-bloqlar (*Twitter, FMyLife*), sosial şəbəkə servisləri (*Facebook, LinkedIn*), viki-lər (*Wikipedia, Wetpaint*), sosial *bookmarking* (*Delicious, CiteULike*), sosial xəbərlər (*Digg, Mixx*), icmallar (*ePinions, Yelp*), multimedia paylaşımı (*Flickr, Youtube*) aid edilir. *Facebook, Twitter, YouTube* və digər sosial media servisləri İnternet istifadəçilərinin mütləq əksəriyyətinin onlayn həyatının ayrılmaz hissəsinə çevrilib.

Sosial medianın ənənəvi media ilə müqayisədə bir sıra üstünlükləri var: sosial media əlyetərlidir; 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 mübadilə etməyə imkan verir.

Sosial media istifadəçilərinin spektri olduqca müxtəlifdir. Adi istifadəçilər sosial mediadan ünsiyyət, tanışlıq, gündəlik həyata aid məlumatların, şəkillərin paylaşımı vasitəsi kimi yararlanırlar. Sosial medianın səmərəli əks əlaqə imkanları onu əlverişli kommunikasiya və təsir kanalına çevirir. Son dövrlər dövlət hakimiyyəti orqanları, siyasi partiyalar, vətəndaş cəmiyyəti institutları, özəl sektor sosial medianın bu potensialından geniş istifadə etməyə çalışır [2,3].

Sosial media özü ilə bir sıra təhlükələr də gətirir. Bu təhlükələr fərdlərə, sosial qruplara, bütövlükdə, dövlətə və cəmiyyətə yönələ bilər. Sosial şəbəkələrin fərdlərə yönələn təhlükələri barədə [4]-də müfəssəl məlumat verilir və konkret tövsiyələr təklif olunur.

Son illərdə sosial medianın milli təhlükəsizliyə təhdidlər yarada biləcəyi narahatlıqları bütün dünya ölkələrində dövlət hakimiyyəti orqanlarının nümayəndələri tərəfindən dəfələrlə bəyan edilmişdir [5,6]. Burada müxtəlif risk ssenariləri mümkündür – terrorçular tərəfindən sosial mediadan vasitə kimi geniş istifadə edilməsi, xarici qüvvələr tərəfindən ölkənin daxili siyasətinə təsir aləti kimi istifadə edilməsi və s. Bu narahatlıqların təcrübi əsası da var və "ərəb baharı" sübut etdi ki, sosial media kütlələri yönləndirmək, hadisələri dramatikləşdirmək, sosial dəyişikliklər, inqilablar etmək üçün güclü silahdır [7].

Dövlət hakimiyyəti orqanlarının informasiya siyasətinin əsas məqsədləri vətəndaşları öz fəaliyyətləri haqqında məlumatlandırmaq və kütləvi kommunikasiya vasitələrinin köməyi ilə vətəndaşlarla əks əlaqəni təşkil etməkdir. Eyni zamanda, dövlət orqanları münaqişə, sosial

gərginlik yarada bilən, yanlış ictimai rəy formalaşdıran, hakimiyyət orqanlarının nüfuzuna ziyan vura bilən informasiya təhdidlərinə operativ reaksiya verməyə borcludurlar.

Məqalədə sosial medianın milli təhlükəsizliyə təhdid törədə biləcək bir sıra risk ssenariləri təsvir olunur, sosial mediada saxta aktorların – botların yaradılması və idarə edilməsi texnologiyaları və bu sahədə bəzi ölkələrin təcrübəsi analiz olunur. Sosial medianın monitorinqi və analizi üçün mövcud onlayn servislər barəsində məlumat verilir.

Sosial media: risk ssenariləri

Bir sıra dövlətlərin sosial media ilə əlaqədar əsas narahatlığı onun terrorçu, ekstremist, radikal qruplar tərəfindən istifadə edilməsidir. İnternetdə mütəşəkkil terroriçuluğun 90%-i sosial media vasitəsi ilə həyata keçirilir. Sosial media terrorçulara bir neçə saniyədə milyonlarla insana müraciət etmək imkanı verir. Terrorçu qruplar öz müraciətlərini *YouTube, Facebook, Twitter* kimi saytlarla yayırlar, onların vasitəsi ilə on minlərlə insanı öz sıralarına cəlb edirlər.

Bəzən ölkələr çıxış yolunu müəyyən sosial media saytlarına girişi məhdudlaşdırmaqda görürlər. Məsələn, Avropa Komissiyası rəsmiləri *Google, Facebook, Twitter* və digər sosial media platformalarından zorakı ekstremist qrupların onlayn iştirakını daha proaktiv tənzimləməyi tələb edirlər. Rəsmilər istifadəçilərin post etdikləri kontentin onlayn yerləşdirilməzdən əvvəl diqqətlə nəzərdən keçirilməsini və ya bəzi qrupların sosial media platformalarına girişini, ümumiyyətlə, qadağan etməyi təklif edirlər.

Dinə aid həssas tvitlər geniş yayılmış hala çevrilir. Sosial medianın köməyi ilə insanlar bir-birinin dini dəyərlərinə hücum edirlər. Dini, irqi hissləri təhqir edən şəkillərin sosial media vasitəsilə dövriyyəsi kütlələr arasında gərginliklər yaradır.

Siyasətçilərin və ictimai xadimlərin çoxunun sosial şəbəkələrdə səhifələri var. Sosial media seçki kampaniyalarında siyasi təbliğat vasitəsi kimi geniş istifadə edilir [8]. Bəzi müxalif siyasətçilər bu statuslarını sosial mediada aktiv fəaliyyətləri nəticəsində qazanıblar. Bloqlar siyasi partiyalar və ictimai hərəkatlar üçün aktual hadisələrin işıqlandırılmasında əhəmiyyətli alətə çevrilib. Sosial media ictimai-siyasi aksiyaların təşkili üçün də rahat alət kimi istifadə edilir. Siyasi partiyalar, QHT-lər, hakerlər sosial mediadan istifadə edərək siyasi sabitliyə ciddi təhlükə yarada bilərlər.

Sosial media müxtəlif ölkələrə inqilab ixracı ("*Facebook* inqilabı", "*Twitter* inqilabı") vasitəsi kimi istifadə oluna bilər. 2009-2011-ci illərdə İranda və bir sıra Yaxın Şərq ölkələrində olan siyasi böhranlar, Ukraynada, Rusiyada etiraz hərəkatları göstərdi ki, sosial media etirazçı qüvvələri səfərbər etmək üçün istifadə edilə bilər, həm də bunun üçün az sayda ictimai rəy lideri kifayətdir [9, 10].

Məlumdur ki, kəşfiyyat qurumları kəşfiyyat məlumatlarının əhəmiyyətli hissəsini (bəzi etiraflara görə, 80 %-ni) açıq mənbələrdən alırlar. Açıq mənbələr əsasında kəşfiyyat metodologiyasına (ing. *Open Source Intelligence – OSINT*) açıq mənbələrdən informasiyanın axtarışı, seçilməsi və toplanması, onun uzlaşdırılmış və çarpaz analizi daxildir. Əsas məlumat mənbələri kimi: KİV, dövlət hakimiyyəti orqanlarının və özəl şirkətlərin açıq hesabatları, rəsmi mətbuat konfransları, müxtəlif rəsmi bəyanatlar, müxtəlif konfransların, seminarların materialları və s. çıxış edir. Sosial media kəşfiyyat qurumları üçün də böyük imkanlar yaradır [11]. 2011-ci ildə *NATO* qüvvələrinin Liviya əməliyyatlarında sosial media kəşfiyyat məlumatlarının real zaman rejimində ötürülməsi vasitəsi kimi geniş istifadə edilmişdi. Müvafiq məlumatlar İtaliyanın Neapol şəhərində yaradılmış xüsusi əməliyyat mərkəzində emal olunurdu [12].

Sosial medianın hərbi potensialı da böyükdür – *GPS* funksiyalı mobil telefonların istifadəsi qeyri-məhdud imkanlar verir. Obyektin şəkli ilə birlikdə geo-informasiya məlumatlarının sosial şəbəkələrdə yerləşdirilməsi bir neçə saniyə çəkir. 2011-ci ildə Liviya əməliyyatlarında sosial media *NATO* qüvvələrinin aviazərbələrində yerüstü hədəflərin identifikasiyasına kömək üçün istifadə edilmişdi. Sosial şəbəkələrdən və digər İnternet mənbələrindən alınmış informasiya hərbi əməliyyatların gedişini onlayn izləməyə imkan verirdi [12].

Beləliklə, sosial media təbliğatın, dezinformasiyanın, şüurla manipulyasiyaların, fərdi, biznes və kəşfiyyat məlumatlarının toplanmasının güclü vasitələrindən birinə çevrilib [13].

Sosial medianın informasiya təsiri mexanizmləri haqqında

Sosial media fenomeni son onillikdə meydan çıxsa da, onun elmi-nəzəri əsasları xeyli əvvəl sosial psixologiya, medialogiya, sosial informatika, sosial şəbəkə analizi, mürəkkəb şəbəkələr, mürəkkəb dinamika, mürəkkəb sistemlər, şəbəkə müharibələri və s. kimi istiqamətlərdə dünyanın qabaqcıl tədqiqat mərkəzlərində aparılan tədqiqatlarda formalaşdırılmışdır və sosial media bu nəticələrin eksperimental yoxlanılması və real praktikada tətbiqi üçün geniş imkanlar açır. Belə tədqiqat mərkəzlərinə misal dünyada ilk atom bombasının hazırlandığı Los-Alamos Milli Laboratoriyası, Stenford Universiteti, Mançester Universitetinin Mitçel adına Sosial Şəbəkə Analizi Mərkəzi, Santa Fe İnstitutu, *IBM, RAND* korporasiyası və s. göstərilə bilər.

Sosial şəbəkə baxışlarına görə, bəşəriyyət çox böyük sayda cəmiyyətlərdən ibarətdir, hər bir insan eyni zamanda bir neçə cəmiyyətin üzvüdür. İnsanın ünsiyyətdə olduğu şəxslərin hər biri də, öz növbəsində, bir neçə cəmiyyətin üzvüdür. Bu əlaqələr zənciri bütün bəşəriyyəti əhatə edən bir çox informasiya kanalları yaradır. İnformasiya bu kanallar vasitəsilə istənilən miqyasda yayıla bilər, çünki kiçik dünya modelinə görə yer üzərində bütün insanlar ortaq tanışları vasitəsi ilə bir-birilə əlaqəlidirlər və adətən, ortaq tanışların sayı 6-dan çox deyil [1].

Şəbəkə strukturlarının və yayılma kanallarının mahiyyətini başa düşmək kütlələrə təsir baxımından daha səmərəli nəticələr verə bilər. KİV-dən buraxılmış və cəmiyyət tərəfindən lazımi istiqamətdə həzm olunmuş informasiya vasitəsilə bütün cəmiyyətə, o cümlədən qərar qəbul edən şəxslərə təsir etmək olar.

Şəbəkə strukturu vasitəsilə cəmiyyətə informasiya təsiri mexanizmi hər yerdə eynidir: müəyyən sifarişçi vəzifəni təyin edir, onun icraçıları bu vəzifə üçün ictimai təşkilatlardan, jurnalistlərdən (və ya bütöv KİV və media-holdinqdən), siyasi fəallardan, qeyri-formal hərəkat üzvlərindən, bəzi hallarda isə kriminal və ekstremist strukturlardan ibarət şəbəkə strukturunu qururlar. Bir qismini qrantlarla, bəzilərini siyasi piar vədləri ilə, digərlərini, sadəcə, pulla cəlb edirlər. Onlara verilmiş ideyaya aludə olan insanların cəlb edilməsi əhəmiyyətli rol oynayır. Məhz onlar hərəkətverici qüvvədir, onlar insanları inandıra və öz arxaları ilə istənilən radikal aksiyalara apara bilərlər.

Lakin şəbəkə müharibələrinin xüsusiyyəti ondan ibarətdir ki, oxşar əməliyyatlar birdəfəlik ani aksiya deyil, belə aksiyalar çoxdur, onlar ayrı-ayrı vaxtlarda müxtəlif yerlərdə baş verir və fərqli təşkilatlar tərəfindən həyata keçirilir. Onlar birlikdə ümumi nəticə verirlər. Bu kiçik aksiyalar birlikdə arı yuvasına oxşayır – bir arı iynəsi təhlükəli deyil, lakin arı çox olduqda sancmalar da çox olur və qaçmağa məcbur edirlər. *RAND* korporasiyasının ekspertləri bu prinsipi "*swarming*", yəni "sürü prinsipi" adlandırırlar [14,15]. "Sürü" özünü "mikrohərəkətlər", "sancmalar", "xatırlatmalar": KİV-lərin hay-küyü, cəmiyyətə sırınan müxtəlif mövzularda müzakirələr, müxtəlif növ nümayişlər, silahlı və silahsız fiziki toqquşmalar çoxluğunda göstərir. Ekranda və ya İnternetdə lazımi ekspertlər can-başla lazımi qiymətləri verirlər, jurnalistlər hay-küylü ifşalar çap etdirirlər, hüquq müdafiəçiləri piketlər keçirir və açıq məktublar yazırlar, vəkillər onların müdafiə etdikləri şəxslərə münasibətdə özbaşınalıq haqqında müsahibələr verirlər və s.

Sosial medianın saxta aktorları

"*TheGuardian*" qəzeti (Böyük Britaniya) 2011-ci ildə ABŞ Müdafiə Nazirliyinin saxta onlayn-şəxslərin köməyi ilə sosial şəbəkə üzvlərinin əhvali-ruhiyyəsi ilə gizli manipulyasiya edən xüsusi proqram təminatı yaratması barədə xəbər yaymışdı [16]. Saxta şəxslər İnternet istifadəçilərinə intellektual təsir edərək amerikan təbliğatının yayılmasına yardım etməli idilər.

ABŞ Müdafiə Nazirliyi Perspektiv Tədqiqatlar Agentliyi (*DARPA*) 2011-ci ildə belə əməliyyatlar üçün xüsusi "Strateji kommunikasiyalarda sosial media" proqramı (*Social Media in Strategic Communication, SMISC*) çərçivəsində proqram təminatının yaradılması üçün tender elan

etmişdi [17,18]. Bu işləri 2003-cü ildə İraqda həyata keçirilmiş "Səmimi səs" (*Operation Earnest Voice, OEV*) əməliyyatının davamı hesab etmək olar.

SMISC çərçivəsində *Ntrepid* şirkətinin yaratdığı proqram təminatının köməyi ilə müxtəlif ölkələrin informasiya fəzasına bağlanan saxta sosial media aktorlarının şəbəkəsini yaratmaq mümkündür. Bu işin nəticəsində "əlaltı kuklaların" (*Sock Puppets*) deyil, dünyanın müxtəlif ölkələrində yerləşən real insanların mövcudluğu təəssüratı formalaşır. Hər bir saxta aktor üçün ayrıca "tərcümeyi-hal", "xarakter" təfərrüatları yaradılır. Onlayn şəxsiyyətlərin idarə edilməsi xidməti haqqında hökumət sənədində deyilir ki, hər bir saxta istifadəçi profili, personajın bütün xüsusiyyətləri texniki, mədəni və coğrafi baxımdan tam adekvat olmalıdır. Bu saxta profillər üçün *IP* ünvanları elə maskalanır ki, hər şey saxta aktorun bütün materialları göstərilən ərazidən yerləşdirdiyini göstərir. Nəticədə, hətta təcrübəli opponentlər də bu saxta onlayn şəxslərlə manipulyasiya edilməsi faktlarını aşkarlamaqda aciz qalırlar, onlar yerli bloqerlərin etimadını asanlıqla qazana bilərlər. *Ntrepid* şirkətinin yaratdığı onlayn şəxsləri idarəetmə servisi bir operatora 10-dan artıq saxta sosial media hesabını idarə etməyə imkan verir. Əməliyyatların idarə edilməsi mərkəzi *MakDill* aviabazasıdır (Tampa, Florida ştatı), burada ABŞ xüsusi əməliyyatlar komandanlığının qərargahı (*CENTCOM*) yerləşir.

Bir neçə ölkədə də oxşar strukturların yaradılması haqqında açıq məlumatlara rast gəlmək olar. Məsələn, Rusiya Müdafiə Nazirliyi üçün müxtəlif tipli açıq mənbələrdən toplanmış məlumatlar əsasında "ölkədə və dünyada hərbi-siyasi, sosial-iqtisadi və ictimai-siyasi vəziyyətin monitorinqi və analizi" üçün proqram-aparat kompleksinin yaradılması planları haqqında mətbuatda məlumat verilmişdir.

Almaniya Federal Kəşfiyyat Xidməti də ölkə xaricində sosial şəbəkələri real vaxt rejimində monitorinq və analiz etməyə, şəbəkə trafikini tutmağa və deşifrələməyə imkan verən texnologiyaların yaradılmasına yaxın beş il ərzində 300 milyon avro sərf etməyi planlaşdırır. Əsas məqsədi kibercinayətkarlığın erkən aşkarlanması olan bu proqrama "Strateji texnoloji təşəbbüs" (*Strategische Initiative Technik, SIT*) adı verilmişdir.

SMISC proqramının qısa icmalı

SMISC proqramının tender üçün izahat sənədində deyilirdi: "Silahlı qüvvələrimizin əməliyyatları həyata keçirdikləri şərait bloqların, sosial şəbəkələrin, fayl mübadiləsi servislərinin (*YouTube* kimi) və mobil texnologiyaların təsiri altında sürətlə dəyişir. Sosial servislərin geniş yayılması münaqişələrin təbiətinə olduqca dərin təsir göstərə bilər. Bu servislərdən səmərəli istifadə edilməsi silahlı qüvvələrə əməliyyatların informasiya dəstəyini daha keyfiyyətlə həyata keçirməyə imkan verəcək".

SMISC proqramının əsas məqsədi yeni meydana çıxan texnologiya bazasında qurulmuş yeni sosial şəbəkə elminin işlənməsidir. Xüsusi halda, *SMISC* operatorların sosial medianı verilənlər miqyasında sistematik istifadə etməsini dəstəkləmək üçün avtomatlaşdırılmış və yarım-atomatlaşdırılmış alətlər və vasitələr yaradacaq və proqramın dörd konkret hədəfinin vaxtında yerinə yetirilməsini təmin edəcək:

1. ideyaların və konsepsiyaların formalaşmasını, inkişafını və yayılmasını aşkarlamaq; məqsədyönlü və ya yanıldıcı (aldadıcı) məlumatları və dezinformasiyanı müəyyənləşdirmək, təsnif etmək, qiymətləndirmək və izləmək.
2. sosial media saytlarında və icmalarında inandırma kampaniyalarının strukturlarını və təsir əməliyyatlarını aşkarlamaq.
3. inandırma kampaniyalarının iştirakçılarını və onların niyyətlərini identifikasiya etmək və bu kampaniyaların effektlərini qiymətləndirmək.
4. düşmənin aşkarlanmış təsir əməliyyatlarına qarşı əks əməliyyatlar həyata keçirmək.

SMISC proqramına uyğun texnologiya sahələri proqramın yuxarıda bəyan edilmiş dörd əsas hədəfinə görə qruplaşdırılıb:

1. linqvistik ipucları, informasiya axını şablonları, mövzu trend analizi, təhkiyə strukturunun analizi, əhval-ruhiyyənin aşkarlanması və rəylərin intellektual analizi modelləri;

2. cəmiyyətdə anlayış və ideyaların izlənməsi, qraf analitikası/ehtimallı mühakimə, obrazların aşkarlanması;

3. şəxslərin stimullaşdırılması, yeni yaranmış icmaların modelləşdirilməsi, etimad analitikası, şəbəkə dinamikasının modelləşdirilməsi;

4. kontentin avtomatik generasiyası, sosial mediada botlar, kraudsoursinq.

Tədqiqatlar göstərir ki, sosial medianın modelləşdirilməsinə şəbəkənin statik qraf modelləri ilə ənənəvi yanaşmalar çox zaman səhv nəticələr verir. Buna görə də, *davranışların dinamikasını* nəzərə almaq lazımdır və SMISC bunu həyata keçirmək üçün bir çox vasitədən istifadə etməkdə maraqlıdır [18].

Sosial medianın monitorinq alətləri

Sosial medianın populyarlığının sürətlə artması, iqtisadi və ictimai-siyasi rolunun yüksəlməsi onun monitorinqi və analitikası üçün nəzərdə tutulmuş informasiya sistemlərinin yaradılmasını tələb edir [19].

Lakin bilavasitə dövlət orqanları üçün nəzərdə tutulmuş sosial media monitorinqi və analizi sistemləri haqqında məlumatlar azdır, onlar, əsasən, 2010-cu ildən sonra yaradılmağa başlayıb və hələlik geniş yayılmayıb [20]. Hazırda bazarda təklif olunan sosial 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 münasibətlərini (pozitiv, neqativ, neytral), rəylərin tonallığını aşkarlayır, rəy müəlliflərini cins, yaş, yaşayış yeri, maraqları və s. görə seqmentlərə bölür.

Qeyd edək ki, populyar sosial şəbəkə servislərində bir sıra monitorinq alətləri mövcuddur. Məsələn, *Facebook Insights*, *Google Analytics*, *Twitter Analytics*, *LinkedIn Analytics*, *Pinterest Analytics*. Hazırda ingilisdilli *SumAll*, *Sysomos*, *UberVU*, *SproutSocial* portalları, rusdilli *YouScan*, *Brand Analytics*, *Babkee*, *BrandSpotter*, *Buzz Look*, *IQBuzz*, *SemanticForce*, *Wobot*, *Крибрум* və s. sosial media monitorinqi servisləri təklif edirlər. Aşağıda bir neçə monitorinq sistemi haqqında qısa məlumat verilir.

Seesmic (*seesmic.com*) – sosial medianın monitorinqi üçün ödənişsiz servisdir. *Twitter*, *Facebook*, *LinkedIn*, *Chatter*, *Google Buzz*, *Ping.fm* saytlarını dəstəkləyir. İnternet, fərdi kompüter, *iPhone, Android, Windows Mobile* üçün tətbiqi proqramları var. Mahiyyətcə, *Seesmic twitter*-kliyentdir, *Adobe Air* kitabxanasından istifadə edilməklə yazılb, ona görə bir çox platformada işləyə bilər.

Socialmention (*socialmention.com*) – sosial şəbəkələrdə informasiyanın axtarışı və analizi üçün pulsuz platformadır. Seçilmiş servislərdə və ya dəstəklədiyi sosial medianın hamısında rastgəlmələri axtarır. Bundan başqa, xatırlatmanın, tonallığın analizi, əlaqədar açar sözlər, populyar mənbələr və s. daxildir. Socialmention şəbəkələr, sosial əlfəcinlər, bloqlar, forumlar, sosial servislər daxil olmaqla 100-dən çox sosial media mənbəyini əhatə edir.

Hootsuite (*hootsuite.com*) – sosial media ilə işləyən çoxfunksiyalı servisdir. Bu servisdə aksent *twitter*-ə edilib. *Hootsuite Facebook*, *LinkedIn*, *MySpace* və *Foursquare* ilə, *WordPress* bloqları ilə işləməyə imkan verir, *Ping.fm*-ə qoşula bilir. Müxtəlif analitika ilə işləmək üçün *HootSuite*-in bir çox imkanı var. Məsələn, *Google Analytics*-ə qoşulmaq olar. *HootSuite* bir sıra mobil platformalarda işləyir: *iPhone, Android, Blackberry*. Mobil proqramlar ödənişsizdir.

Twitalyzer (*twitalyzer.com*) – *Twitter* üçün analitik proqram-kliyentdir, keçidlərin sayını izləməyə, müsbət və mənfi şərhləri analiz etməyə, auditoriyanı seqmentlərə bölməyə imkan verir. *Google Analytics* sistemi ilə inteqrasiya olunub, interaktiv diaqramlar və qrafik alətlərlə işləyir.

TweetDeck (*tweetdeck.com*) – *Twitter, Facebook, MySpace, LinkedIn* sosial şəbəkələrində məlumatların izlənilməsi və idarə edilməsi üçün alətdir, müxtəlif süzgəcləri, o cümlədən açar sözlərlə süzgəcləri dəstəkləyir, müxtəlif platformalarda işləyir.

Çoxlu sayda mövcud olan və hər ay meydana çıxan yeni servislərə, eləcə də, bəyan edilən imkanlara baxmayaraq, bütün sosial media monitorinqi sistemləri tipik proqram təminatına əsaslanır [21-23].

Nəticə

Sosial media ünsiyyət, məlumat və fikir mübadiləsi kimi funksiyaları ilə yanaşı, son dövrlər tez-tez informasiya təsiri aləti kimi də istifadə edilir, informasiya qarşıdurması və informasiya müharibəsi səhnəsinə çevrilir. İnsan hüquqlarını və ifadə azadlığını pozmadan sosial media verilənlərinin monitorinqi və analizi cəmiyyətin nəbzini tutmağa, əhval-ruhiyyəsini müəyyən etməyə, gözləntilərini aşkarlamağa imkan verir. Bu dövlətin vətəndaşlarla, özəl sektorla, siyasi partiya və hərəkatlarla, vətəndaş cəmiyyəti institutları ilə səmərəli, faydalı dialoquna zəmin yaradır. Sosial media analitikası meydana çıxan təhdidləri vaxtında aşkarlamağa və əks-tədbirlər həyata keçirməyə imkan verir.

Ədəbiyyat

1. Əliquliyev R. M., İmamverdiyev Y. N., Abdullayeva F. C., Sosial şəbəkələr. Bakı, "İnformasiya Texnologiyaları" nəşriyyatı, 2010, 287 s.
2. Wright D. Hinson M., Examining how public relations practitioners actually are using social media // Public Relations Journal, 2009, vol. 3, no. 3, pp. 1-33.
3. Под общей ред. Е.Г. Алексеевой. Влияние через социальные сети, М., Фонд «ФОКУС-МЕДИА», 2010, 200 с.
4. Hogben G. (ed.) Security issues and recommendations for online social networks. ENISA Position Paper No.1, October 2007, 33 p.
5. Montagnese A. Impact of social media on national security. Centro Militare di Studi Strategici: Research Paper 2011 STEPI - AE-U-3. 2012, 36 p.
6. Chen Y. Research on social media network and national security. W.Du (ed.) Informatics and Management Science II, Lecture Notes in Electrical Engineering, 2013, vol. 205, pp 593-599.
7. Khondker H. H. Role of the New Media in the Arab Spring // Globalizations, 2011, vol. 8, no. 5, pp.675-679.
8. Adamic L. A., Glance N. The political blogosphere and the 2004 US election: divided they blog / Proc. of the 3rd international workshop on Link discovery, 2005, pp. 36-43.
9. Elson S. B., Yeung D., Roshan P., Bohandy S. R., Nader A. Using social media to gauge Iranian public opinion and mood after the 2009 election. RAND Corporation Technical Report. 2012, 110 s.
10. Tan Z., Li X., Mao W. Agent-based modeling of netizen groups in Chinese Internet Events // Quarterly SCS M&S Magazine, 2012, pp. 39-45.
11. Балуев Д.Г., Каминченко Д.И. Политическая роль «новых СМИ» в ливийском конфликте // Вестник Нижегородского университета им. Н.И. Лобачевского, 2012, № 2 (1), с. 307–313.
12. Levesque J. Social media "Tactical intelligence collection": Spying and propaganda using Facebook, Twitter. February 15, 2012.
13. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети. Модели информационного влияния, управления и противоборства. Москва: Издательство физико-математической литературы, 2010, 228 с.
14. Arquilla J., Ronfeldt D. F. Networks and netwars: the future of terror, crime, and militancy. Rand Corporation, 2001. 5 p.
15. Cebrowski A. K., Garstka J. J, "Network-centric warfare: Its origin and future." U.S. Naval Institute Proceedings, January 1998, 10 p.
16. Revealed: US spy operation that manipulates social media, http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks

17. Social Media in Strategic Communication (SMISC), http://www.darpa.mil/Our_Work/I2O/Programs/Social_Media_in_Strategic_Communication_%28SMISC%29.aspx
18. Social Media in Strategic Communication (SMISC), http://www.darpa.mil/opencatalog/SMISC.html
19. Sykora M.D. 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.
20. Batrinca B., Treleaven P. C. Social media analytics: a survey of techniques, tools and platforms // AI & Society, 2015, vol. 30, no. 1, pp. 89–116.
21. Pang B., Lee L. Opinion mining and sentiment Analysis // Foundations and Trends in Information Retrieval, 2008, vol. 2, no. 1-2, pp. 1-135.
22. Aliguliyev R. M. A new sentence similarity measure and sentence based extractive technique for automatic text summarization // Expert Systems with Applications, 2009, vol. 36, no. 4, pp. 7764–7772.
23. Karthik K., Kollias G., Kumar V., Grama A. Trends in Big Data analytics // Journal of Parallel and Distributed Computing, 2014, vol. 74, no. 7, pp. 2561-2573.

УДК 004.9:351

Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@lan.ab.az

Социальные медиа и проблемы безопасности

Социальные медиа являются не только удобной платформой общения и совместного использования файлов, но также инструментом социально-политического влияния, ареной противостояния и информационной войны. Социальные медиа могут создавать ряд угроз национальной безопасности в зависимости от целей его использования. В этой работе описаны некоторые сценарии рисков социальных медиа, которые могут представлять угрозу национальной безопасности. Анализируются технологии создания и управления поддельными акторами – ботами социальных медиа и опыт некоторых стран в этой области. Приводятся краткая информация о существующих онлайн-услугах мониторинга и анализ социальных медиа.

Ключевые слова: *социальные медиа, национальная безопасность, мониторинг социальных медиа, аналитика социальных медиа, информационное воздействие, информационная война.*

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az

Social media and security problems

Social media is not only convenient platform for communication and information sharing, but also is an instrument of social and political influence, and becomes a scene of the confrontation and the information war. Social media can create a number of threats to national security, depending on the purpose of its use. This study describes some scenarios of risks of social media, which can pose a threat to national security. Technology of creating and management of fake social media actors and the experience of some countries in this field are analyzed. Brief information is given on the existing online services for monitoring and analysis of social media.

Keywords: *social media, national security, social media monitoring, social media analytics, information influence, information warfare.*