Sosial şəbəkələrdə fərdi məlumatların təhlükəsizliyi problemləri və onların həlli yolları

Məkrufə Hacırəhimova[1], Mərziyə İsmayılova[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*makrufa@science.ab.az*, [2]*imarziya@gmail.com*

***Xülasə*—Sosial şəbəkələrin (SŞ) meydana gəlməsi adi passiv oxucunu kontent iştirakçısına çevirdi. Bu istifadəçilərə informasiya paylaşımı və fikir mübadiləsi aparmaq, eyni zamanda oxşar maraqları olan digər istifadəçilərlə qarşılıqlı əlaqə yaratmaq üçün onlayn virtual cəmiyyyətlərdə özlərini ifadə etmək imkanı verdi. Bununla belə, SŞ istifadəçilərin sosial fəaliyyət sahəsini kommersiya fəaliyyət sahəsinə çevirdi. Bu isə SŞ istifadəçiləri üçün məxfilik və təhlükəsizlik problemləri yaradır. SŞ servis provayderləri müştərilərinin fərdi və məxfi məlumatlarını toplayırlar, bunlar da məlumat toplayanlar, üçüncü tərəflər və ya icazəsiz istifadəçilər tərəfindən sui istifadə edilə bilər. Məqalədə təhlükəsizlik və məxfilik problemləri araşdırılmış, SŞ istifadəçilərinin sosial mediadan istifadə etdikləri zaman bu problemlərdən qorunması üçün təkliflər şərh edilmişdir.**

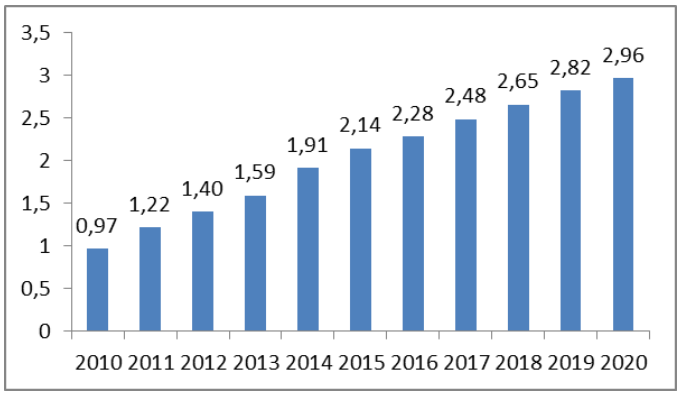
Açar sözlər—sosial şəbəkələr; fərdi məlumatların mühafizəsi; təhlükəsizlik; məxfilik

I. GİRİŞ

Sosial şəbəkə istifadəçilər, təşkilatlar və onların sosial fəaliyyətləri arasındakı əlaqəni əks etdirən bir sosial qrafdır. İstifadəçilər, təşkilatlar, qruplar qrafın qovşaqları, onların arasındakı əlaqələr isə qrafın tilləridir. Sosial media SŞ-dən istifadə etməklə virtual cəmiyyət yaradan onlayn kommunikasiya üçün verilənlərin sahibi (verilənləri generasiya edənlər) və izləyicilər (son istifadəçilər) arasında əlaqə mənbəyidir [1].

SŞ-lərin əsas məqsədi kontentləri maksimum sayda istifadəçilərlə paylaşmaqdır. İstifadəçilər gündəlik fəaliyyətlərini dərc etmək üçün Facebook, Twitter, LinkedIn və s. kimi SŞ-lərdən istifadə edirlər. Bəzən SŞ istifadəçiləri özləri və həyatları haqqında məlumatı dostları və həmkarları ilə paylaşırlar. Lakin nəşr olunan bu məlumatlarda SŞ vasitəsilə müəyyən edilmiş kontentlərin bəziləri özəldir və buna görə dərc edilməməlidir. SŞ servis provayderləri fərdi xidmətlər təklif etmək üçün istifadəçiləri haqqında bir sıra məlumatlar toplayır, lakin onlardan kommersiya məqsədləri üçün istifadə edilə bilər. Bundan əlavə, istifadəçilərin məlumatları üçüncü tərəflərə ötürülə bilər, bu da məxfiliyin sızmasına gətirib çıxarır. Bu məlumatlar bədniyyətli istifadəçilərə istənilən bir fərdin məxfiliyinin pozulmasına imkan verə bilər. Verilənlərin məxfiliyi onlayn saxlanılan və ya paylaşılan informasiyanı aşkar edən, dəyişdirən, hücum edən və ya verilənləri məhv edən icazəsiz və zərərli girişdən qoruyur. Bəzən tədqiqatçılar informasiyanın əldə edilməsi və idarə edilməsi üçün həllər hazırlayərkən məxfilik problemlərini nəzərə almırlar. Digər tərəfdən verilənlərin məxfiliyi üzərində işləyən tədqiqatçılar, fərdi məlumatları axtaran bədniyyətli istifadəçilərdən həssas verilənləri qorumaq üçün adətən informasiya axtarış metodlarını məhdudlaşdırırlar [2].

Sosial mediada istifadəçi tərəfindən generasiya edilən kontentə istifadəçilərin təəssüratları, fikirləri və bilikləri daxildir. Əlavə olaraq, həmçinin ad, cins, yaşayış yeri, şəxsi fotoşəkillər və s. kimi fərdi məlumatlar da daxil ola bilər. Onlayn paylaşılan informasiyalar elektron şəkildə saxlanılır və buna görə də davamlı, təkrarlanan və dəyişdirilə biləndir [3]. SŞ istifadəçiləri sosial məxfiliyini təhlükə altına qoymaqla sosial identikliyini idarəetmə problemləri ilə rastlaşırlar. Statistik məlumatlara görə dünyada aktiv sosial media istifadəçilərinin sayının 2020-ci ilə qədər 2,96 milyarda çatacağı gözlənilir ki, bu da bütün dünya əhalisinin təxminən üçdə birini təşkil edir (şək.1) [4]. Bu qlobal istifadəçi sayı məxfiliyin SŞ-lə əlaqəli aşkar və kritik məsələlərdən biri olduğunu göstərir. SŞ-nin sosial sferası kommersiya sferasına çevrildiyi zaman SŞ-lərə görə məxfiliyin müxtəlif problemləri (nəzarət kimi) təşviq edilir. Lakin SŞ-nin servis provayderləri bazara girişə nəzarət üçün istifadəçilərin fəaliyyətini izləyirlər. Standart SŞ-lər istifadəçinin fərdi məlumatlarını reklam məqsədi ilə istifadə üçün üçüncü tərəfə ötürür. Eyni zamanda, SŞ istifadəçiləri SŞ saytlarına baxış zamanı rəqəmsal iz buraxırlar. Bu isə kommersiya məqsədi və istifadəçi profilləri üçün verilənlər mənbəyi kimi hədəflənir [5].



Şəkil 1. 2010-2020-ci illər üzrə dünyada sosial media istifadəçilərinin sayı

DOI: 10.25045/NCInfoSec.2019.20

Müasir dövrdə fərdi məlumatların təhlükəsizliyini təmin etmək ehtiyacı obyektiv bir reallıqdır. İnsanlar öz fərdi məlumatlarına edilən təhlükələrə qarşı müstəqil şəkildə mübarizə apara bilmir, dövlət səviyyəsində problemin həllinə ehtiyac yaranır. Bununla əlaqədar fərdi məlumatların qorunmasını təmin etmək üçün bir sıra dövlətlər qanunvericilik aktları qəbul etmişdir. Onlardan bir neçəsi aşağıda cədvəldə verilmişdir [6, 7].

CƏDVƏL 1. FƏRDI MƏLUMATLARIN QORUNMASI HAQQINDA QANUNLAR

Dövlətlər	**Qəbul olunmuş qanunlar**
Amerika Birləşmiş Ştatları	Məxfilik aktı (*Privacy ACT*) (1974)
	Təhlükəsiz fəaliyyət *(Safe Harbor Act*) (1998)
	Vətənpərvərlik aktı (*Patriot Act*) (2001)
	“Fərdi məlumatların qorunması” (2003)
Avropa birliyi	“Fərdi məlumatların avtomatik emalı ilə fiziki şəxslərin hüququnun müdafiəsi haqqında” konvensiya (1981)
	“Fərdi məlumatların emalı və bu məlumatlara sərbəst surətdə müraciət zamanı fiziki şəxslərin qorunması haqqında” 95/46/EC direktivi (1995)
	“Fərdi məlumatların işlənməsi və telekommunikasiya sektorunda mülkiyyətin qorunması haqqında” 97/66/EC direktivi (1997)
Rusiya	"İnformasiya, informasiya texnologiyaları və məlumatların qorunması haqqında" Federal Qanun (2006)
	“Fərdi məlumatlar haqqında” Federal Qanun (2007)
Azərbaycan	“Fərdi məlumatlar haqqında” qanun (2010)

II. SOSİAL ŞƏBƏKƏLƏRDƏ KONFİDENSİALLIQ VƏ TƏHLÜKƏSİZLİK TƏHDİDLƏRİ

Sosial şəbəkə vasitələri şəxsi və iş həyatımızda qarşılıqlı münasibətlərimizi dəyişdirdi. Sosial və iş həyatımızda əhəmiyyətli bir rol oynasalar da, eyni zamanda məxfilik və təhlükəsizliklə bağlı yüksək risklər yaradırlar. Yüz minlərlə istifadəçi SŞ-ləri müntəzəm olaraq istifadə etdikləri üçün məxfilik və təhlükəsizlik təhdidlərinə məruz qalırlar. Bu təhdidlər klassik və müasir təhdidlər kimi klassifikasiya edilir.

A. Klassik təhdidlər

Klassik təhdidlər İnternetin inkişafından bəri bir problem olmuşdur. Bu təhdidlər zərərli proqram, fişinq, spam və ya saytlararası skript hücumlarıdır [8-11].

- *Zərərli proqramlar (ing. malware).* Zərərli proqram istifadəçilərin etimadnamələrini əldə etmək və həmkarlarına mesaj göndərməklə onları təqlid etməkdir. Məsələn, Koobface zərərli proqramı MySpace, Facebook və Twitter kimi SŞ-lər vasitəsilə yayılmışdır. O giriş etimadnaməsini toplamaq və yoluxmuş kompüteri botnetin bir hissəsi etmək üçün istifadə edilmişdir.
- *Fişinq (ing. phishing) hücumları.* Fişinq, saxta və ya oğurlanmış şəxsiyyət vasitəsi ilə etibarlı üçüncü tərəf kimi maskalanaraq istifadəçinin fərdi məlumatlarının əldə edildiyi hücumun bir növüdür. Məsələn, Çin hökumətinin kəşfiyyatına aid edilən bir hücum zamanı Böyük Britaniya və ABŞ-ın yüksək rütbəli hərbi məmurları özünü ABŞ Hərbi Dəniz Qüvvələri admiralı kimi göstərən Ceyms Stavridis adlı bir şəxs ilə Facebookda "dost" olmaqla aldandılar.
- *Spam mesajları*. Spam mesajları arzu olunmayan mesajlardır. Spam mesajları adətən fişinq və ya zərərli saytlara yol açа bilən reklamlar və ya zərərli bağlantılar ehtiva edir. Ümumiyyətlə, spam saxta profillərdən və ya spam tətbiqlərindən daxil olur.
- *Saytlararası skript (XSS).* XSS veb əsaslı tətbiqlərə kəskin təsir göstərən ən məşhur və ciddi təhlükəsizlik problemlərindən biridir. XSS hücumu, təcavüzkarın hədəflənən istifadəçinin veb brauzerində zərərli kodu işə salmasına imkan verir, bu da verilənlərin sındırılmasına, *cookie* şəklində saxlanılan məlumatların oğurlanmasına və şifrələrin, kredit kartlarının nömrələrinin götürülməsinə səbəb olur. Bundan başqa təcavüzkar XSS-dən istifadə etməklə SŞ-lərdə yayıla bilən XSS soxulcanı hazırlaya bilər.

B. Müasir təhdidlər

Bu təhdidlər yalnız SŞ istifadəçiləri ilə əlaqədardır. Adətən müasir təhdidlərin məqsədi istifadəçilərin və onların dostlarının şəxsi məlumatlarını əldə etməkdir. Əgər istifadəçinin Fasebook hesabında məxfilik parametrləri açıqdırsa onlara asanlıqla baxıla bilər. Lakin onların xüsusiləşdirilmiş məxfilik parametrləri varsa o yalnız dostlarına görünə bilər. Bu halda təcavüzkar bir Facebook profilini yarada və hədəf istifadəçilərə dost istəyi göndərə bilər. Dostluq istəyi qəbul edildikdən sonra təfərrüatlar təcavüz edənə açıqlanır. Eynilə, təcavüzkar, istifadəçilərin fərdi məlumatlarını həmkarlarının açıq kontentindən toplamaq üçün təsirli hücum tətbiq edə bilər. Müasir təhdidlərə klikləmə, anonimləşmə hücumları, saxta profillər, identiklik klon hücumları, müdaxilə hücumları, informasiya itkisi, məkan itkisi, kiberizləmə, istifadəçi profillənməsi və s. kimi təhdidlər aiddir. Onlardan bir neçəsi aşağıda şərh edilmişdir [11-15]:

- *Klikləmə* (*ing.* c*lickjacking*). Klikləmə, həm də onlayn istifadəçilərin klikləmə niyyətində olmadığı bir şeyi klikləməsi üçün zərərli bir metodun tətbiq olunduğu istifadəçi interfeysinin bərpası hücumu kimi də tanınır. Klikləmə hücumlarında təcavüzkar SŞ spamlarını yerləşdirməklə istifadəçilərini manipulyasiya edə bilir. Klikləmə hücumu ilə təcavüzkarlar fəaliyyətlərini qeyd etmək üçün istifadəçi kompüterlərinin qurğularını, mikrofon və kameranı da istifadə edə bilərlər.
- *Saxta profillər (ing. fake profiles).* Sosial şəbəkələrin çoxunda tipik bir hücum saxta profil hücumudur. Bu cür hücumda təcavüzkar sosial şəbəkədə saxta etimadnaməsi olan bir hesab yaradır və qanuni istifadəçilərə mesaj göndərir. İstifadəçilərdən dostluq

cavablarını aldıqdan sonra onlara spam göndərir. Adətən saxta profillər avtomatlaşdırılmış və ya yarımavtomatlaşdırılmışdır və bir insanı təqlid edir. Saxta profil şəbəkənin buraxılış qabiliyyətini itirməkdən əlavə onun ümumi nüfuzuna təsir göstərir. Bundan başqa, saxta profillər müxtəlif məqsədlər, məsələn, reklam üçün istifadə edilə bilər. 2017-ci ilin sonu 2018-ci ilin əvvələrində Facebook 1,3 milyard saxta profil aşkarlamış və dayandırmışdır. Eyni ilə Twitterin 336 miyon hesabının 9-14%-nin saxta olduğu təxmin edilir.

- *İdentiklik klon hücumları (identity clone attacks).* Profil klonlanması, mövcud bir profildən oğurlanmış fərdi məlumatdan istifadə etməklə yeni saxta profil yaradan təcavüzkar tərəfindən həyata keçirilə bilər. Təcavüzkar, həmkarlarından kontentlər toplamaq və ya onlayn fırıldaqçılığın müxtəlif növlərindən istifadə etmək üçün klonlanmış istifadəçinin etimadından istifadə edə bilər.

- *İnformasiya sızması (ing. information leakage).* Bəzi istifadəçilər sağlamlıqla əlaqəli şəxsi məlumatlarını paylaşırlar. Təəssüf ki, onlardan bəziləri məhsullar, layihələr, təşkilat və ya hər hansı digər şəxsi məlumat haqqında bir az çox məlumat paylaşırlar. Bu cür həssas və özəl kontentin paylaşımı SŞ istifadəçiləri üçün mənfi nəticələrə səbəb ola bilər. Məsələn, bir sığorta şirkəti istifadəçiləri riskli müştərilər kimi təsnif etmək üçün SŞ məlumatlarını toplaya bilər.

- *Coğrafi məkan sızması (ing. location leakage*). Bu təhlükə informasiya sızmasının bir növüdür. Müxtəlif istifadəçilərin mobil qurğular vasitəsilə sosial şəbəkəyə daxil olma meyli var. Onlayn giriş üçün mobil qurğuların istifadəsi istifadəçiləri məkan məlumatlarını bölüşməyə məcbur edir bu da məkan sızması məxfiliyinin yeni təhlükəsini yaradır. Beləliklə, sosial şəbəkə saytlarında coğrafi məlumatların açıqlanması hücum edənlər tərəfindən istifadəçilərə zərər vurmaq üçün istifadə edilə bilər.

- *Kiber təcavüz (ing. cyberstalking).* Kiber təcavüz İnternet və ya sosial şəbəkələr vasitəsilə bir şəxsə və ya qrupa təcavüz etməkdir. Monitorinq, şəxsiyyət oğurluğu, təhdid və ya təcavüz üçün istifadə edilə bilər.

- *İstifadəçi profililənməsi (ing. user profiling).* İstifadəçi profillənməsi demək olar ki, bütün onlayn xidmətlərdə yayılmış fəaliyyətlərdən biridir, harada ki, SŞ serverləri maşın təliminin müxtəlif metodları vasitəsilə öz məkanlarında gündəlik istifadəçi fəaliyyətlərini analiz edir. İstifadəçi profillənməsi tələb olunan obyektləri istifadəçilərə tövsiyə etmək üçün bir sıra üstünlüklərə malikdir. Lakin, istifadəçi profillənməsi fərdi məlumatlara malik olduğu üçün məxfilik sızmasına səbəb ola bilər və onun SŞ mühitində qorunması lazımdır. Onlayn servis provayderləri kommersiya məqsədləri üçün istifadəçi profillənməsini həyata keçirir; ancaq, bu məxfiliyin sızması üçün yol açа bilər.

- *Sosial-media nəzarəti* (*ing. surveilance*) - istər fərdi, istər qruplar, istərsə də təşkilatlar və ya şirkətlər üçün istifadəçi məlumatlarını izləmək və əldə etmək üçün istifadə edilən yeni bir monitorinq növüdür. Sosial media şəbəkəsi nəzarəti, insan fəaliyyətlərinin sosial mediada izlənildiyi bir texnologiyaya əsaslanan bir nəzarətdir. Məsələn, Facebook *Cambridge Analytica* firmasına siyasi kampaniya üçün yığılan məlumatdan istifadə etmək üçün istifadəçilərin razılığı olmadan milyonlarla profilə giriş əldə etməyə icazə vermişdir.

III. SOSİAL ŞƏBƏKƏLƏRDƏ QORUNMA TƏDBİRLƏRİ

SŞ-lərdə mövcud olan bir sıra məxfilik və təhlükəsizlik problemləri ehtiyat tədbirlərinin köməyilə aradan qaldırıla bilər. Təcavüzkar, istifadəçilərin ehtiyatsızlığı üzündən SŞ-də təhlükəsizlik və məxfilik problemlərindən istifadə edir. SŞ istifadəçilərinin dostları ilə paylaşdığı kontentlər ya eyni formatda, ya da fərqli bir kontekstdə yad əllərə keçə bilər. Bu məxfilik təhdidlərinə qarşı müdafiə SŞ tərəfindən idarə olunan məxfilik parametrləri vasitəsilə təmin edilir. Lakin, bu məxfilik parametrlərinin effektivliyi kifayət deyil, çünki istifadəçilərin məxfililiklərini qorumaq əvəzinə onlardan daha çox məlumat toplamaq üçün müqavilə hazırlanmışdır. Aşağıda istifadəçi kontentlərinin və məxfiliyin icazəsiz girişdən qorunması üçün bir sıra təkliflər sadalanmışdır [11, 16, 17]:

Məxfilik parametrləri (ing. privacy settings). Təəssüf ki, istifadəçilərin 80%-i öz SŞ-lərini yoxlamırlar və profillərinin məxfiliyinə məxfilik parametrlərinin və ya gözlənilən səviyyəyə cavab verən adekvat məxfiliyin verilib-verilməsi haqqında məlumatları yoxdur. SŞ-lər məlumat sahiblərinə kontenti icazəsiz girişdən gizlətmək üçün giriş nəzarətinin xüsusi səviyyəsini təklif etsələr də, demək olar ki, bütün SŞ-lərdə məxfilik parametrləri məhdud məxfiliyə malikdirlər. Müxtəlif sosial şəbəkə istifadəçiləri təhlükəsizlik və məxfilik parametrlərinə riayət edirlər. SŞ istifadəçilərinə məxfilik parametrlərinə riayət etmələri və SŞ-lərin təqdim etdikləri məxfilik müdafiəsi metodlarından maksimum dərəcədə istifadə etmək təklif olunur. Eyni zamanda, istifadəçilərə məxfilik parametrlərini tez-tez nəzərdən keçirmək tövsiyə olunur, çünki müxtəlif SŞ-lər hər yeniləmədən sonra məxfilik parametrlərini dəyişdirirlər.

Fərdi məlumatlar. Kontentlər hər hansı bir üçüncü tərəf tərəfindən paylaşıldıqdan sonra, bu kontentin artıq məxfi olacağına zəmanət yoxdur. Buna görə istifadəçilərdən SŞ-lərdə lazımsız şəxsi məlumatları paylaşmaması tələb olunur.

Məkan haqqında məlumat (ing. location information): Bir sıra mobil proqramlar istifadəçi yeri haqqında məlumat toplayır. Bu məkan məlumatları SŞ-lər tərəfindən istifadə

edilə bilər və üçüncü tərəfə, ilk növbədə gizlilik sızmasına səbəb olan kommersiya məqsədləri üçün verilə bilər. Buna görə istifadəçilərə potensial təcavüzkarlardan qorunmaq üçün məkan məlumatlarını SŞ-lər vasitəsilə açıqlamamaq tövsiyə olunur.

Antivirus və anticasus proqram təminatı (ing. antivirus and antispyware): SŞ-lər vasitəsilə kontentin yayılmasından asılı olaraq, zərərli proqramlar eksponensial olaraq artır. SŞ istifadəçilərinə zərərli proqram və casus proqramlarına qarşı mübarizə aparmaq üçün kompüterlərində, mobil telefonlarında antivirus və anticasus proqramlarını quraşdırmaq tövsiyə olunur.

Üçüncü tərəf tətbiqləri (ing. third-party applications)- bir sıra məxfilik və təhlükəsizlik problemlərinə səbəb olur, çünki onların kodu SŞ və istifadəçi nəzarəti xaricindədir. Bu, SŞ və istifadəçilərə tətbiqin fəaliyyətini nəzarətdə saxlamağa və zərərli nüfuz etməni dayandırmaq üçün aktiv tədbirlər görməyə mane olur. Məlumatlar SŞ vasitəsilə ötürüldüyündən istifadəçi kontentinin istifadəsi və paylanması istifadəçilərin nəzarətində deyil. Ona görə də yanlış əllərə keçə biləcək məlumatları qorumaq üçün üçüncü tərəf tətbiqlərini silmək tələb olunur.

NƏTİCƏ

Sosial şəbəkələrdən istifadənin faydaları ilə yanaşı bəzi problemləri də mövcuddur. SŞ-lərdə əsas problem istifadəçilərin fərdi məlumatlarının təhlükəsizliyi, məxfiliyi və qorunmasıdır. Bu problemlər SŞ servis provayderləri, icazəsiz istifadəçilər və ya öz kommersiya fəaliyyətləri üçün SŞ verilənlərindən istifadə edən üçüncü tərəflər vasitəsilə yaradıla bilər. Araşdırmalardan məlum olmuşdur ki, *“clickjacking”*, *“fake profiles”, “identity clone attacks” “information ieakage”, “cyberstalking”,* “*location leakage*” və s kimi müasir təhdidlər mövcuddur və onlardan qorunmaq üçün bir sıra məxfilik parametrləri, fərdi məlumatlar, antivirus və anticasus, ücüncü tərəf tətbiqləri kimi qorunma tədbirlərindən istifadə etmək lazımdır. Tədqiqatlar göstərir ki, SŞ-də məxfilik qorunması üzrə görülmüş işlər qənaətbəxş deyil. Bu sahədə praktiki işlərlə yanaşı, həm də elmi tədqiqatların aparılmasına ehtiyac duyulur.

İSTİNADLAR

[1] J.A. Obar, S..Wildman, “Social media definition and the governance challenge: An introduction to the special issue,” Telecommun. Policy, 2015, vol. 39, no. 9, pp. 745–750.

[2] N.A.Shozi, J. Mtsweni, “Big data privacy in social media sites,” Proc. of the 2017 IST-Africa Week Conference (IST-Africa), 2017, pp. 1–6.

[3] M.Taddicken, “The ‘privacy paradox’ in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure,” Journal of Computer-Mediated Communication, 2014, vol. 19, no. 2, pp. 248–273.

[4] https://statista.com

[5] S. Ashtari, “I know who you are and I saw what you did: social networks and the death of privacy,” Journal of Information Privacy and Security, 2013, vol. 9, no. 4, pp. 80–82.

[6] С.П. Евсеев, Э.А. Линд, О.Г. Король, О.М. Носик, “Защита персональных данных,” Системи обробки інформації, 2012, випуск 4 (102), том 1, стр. 108-117.

[7] Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu, http://www.e-qanun.az

[8] S. Alarm, K. El-Khatib, “Phishing susceptibility detection through social media analytics,” Proc. of the 9th International Conference on Security of Information and Networks, 2016, pp. 61–64.

[9] V. Nithya, S.L. Pandian, C. Malarvizhi, “A survey on detection and prevention of cross-site scripting attack,” International Journal of Security and its. Applications, 2015, vol. 9, no. 3, pp. 139–152.

[10] E. Protalinski, Chinese spies used fake facebook profile to friend NATO officials, https://www.zdnet.com/article/chinese-spies-used-fake-facebook-profile-to-friend-nato-officials.

[11] H. Almarabeh, A. Sulieman, “The impact of cyber threats on social networking sites,” International Journal of Advanced Research in Computer Science, 2019, vol.10, no. 2, pp. 1-9.

[12] M.Y. Kharaji, F.S. Rizi; M.R. Khayyambashi, “A new approach for finding cloned profiles in online social networks,” International Journal of Network Security, 2014, vol. 6, pp. 25-37.

[13] S. Torabi, K. Beznosov, “Privacy aspects of health related information sharing in online social networks,” Proc. of the 2013 USENIX Conference on Safety, Security, Privacy and Interoperability of Health Information Technologies, 2013, p. 3.

[14] R. D’Ovidio; J. Doyle, “A study on cyberstalking: Understanding investigative hurdles,” FBI Law Enforc. Bull. 2003, 72, pp. 10–17.

[15] S. Ali, A. Rauf, N. Islam, H. Farman, S. Khan, “User profiling: A privacy issue in online public network,” Sindh University Research. Journal (Science Series) 2017, vol. 49, pp. 125–128.

[16] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, B. Thuraisingham, “Semantic web-based social network access control,” Computers & Security, 2011, vol. 30, no. 2-3, pp. 108–115.

[17] A. Chaabane, Y. Ding, R. Dey, M.A. Kaafar, K.W. Ross, “A closer look at third-party OSN applications: Are they leaking your personal information?,” Proc. of the 15th International Conference on Passive and Active Network Measurement, 2014, pp. 235–246.

SECURITY PROBLEMS OF PERSONAL DATA IN SOCIAL NETWORKS AND WAYS OF THEIR SOLUTIONS

Makrufa Hajırahimova[1], Marziya Ismayılova[2]
[1,2]Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]makrufa@scisence.az, [2] imarziya@google.com

Abstract–The advent of social networks (SN) has transformed a common passive reader into a content contributor. It has allowed users to share information and exchange opinions, and also express themselves in online virtual communities to interact with other users of similar interests. However, SN have turned the social sphere of users into the commercial sphere. This should create a privacy and security issue for SN users. SN service providers collect personal and confidential information of their customers, which can be abused by data collectors, third parties or unauthorized users. The article explores security and privacy concerns, and comments on how social network users use social media to protect themselves from these problems.

Keywords– *social network; protection personal information; security; privacy*