UOT 004.056.53

Şıxəliyev R.H.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
ramiz@science.az

SOSİAL ŞƏBƏKƏLƏRDƏ TƏHLÜKƏSİZLİK PROBLEMLƏRİ

Bu gün İnternetdə çoxlu sayda sosial şəbəkələr mövcuddur. Bu sosial şəbəkələr çox populyardır və insanların həyatında vacib rol oynayır. Bunula yanaşı, sosial şəbəkələr informasiya təhlükəsizliyi sahəsində yeni risklərin yaranmasına gətirib çıxarmışdır. Bu risklər ziyanlı proqramların və spamların yayılması, sosial mühəndislik və sosial şəbəkə hesablarına hücumların həyata keçirilməsi, izləmə, aldatma və s. kimi təhlükələrlə bağlıdır. Məqalə sosial şəbəkələrdə mövcud təhlükələrin analizinə və onlardan qorunma məsələlərinə həsr olunmuşdur.

Açar sözlər*: *sosial şəbəkə, ziyanlı proqram, spam, fişinq, saxta profil.

Giriş

Artıq İnternet insanlar arasında əsas qlobal kommunikasiya və informasiya mübadiləsi vasitəsinə çevrilmişdir. *Web 2.0* texnologiyasının yaranması və sürətli inkişafı İnternetin imkanlarını əhəmiyyətli dərəcədə artırmış və insanlara coğrafi yerləşmələrindən asılı olmayaraq sosial şəbəkələrə qoşulmaq imkanı yaratmışdır [1]. Öz növbəsində, sosial şəbəkələrin sürətlə inkişaf etməsi və geniş vüsət alması onu *Web 2.0* texnologiyasının əsas elementlərindən birinə çevirmişdir.

Sosial şəbəkələr insanlara bir-biri ilə əlaqə yaratmağa və informasiya mübadiləsi etməyə imkan verən bir xidmətdir. Hal-hazırda İnternetdə *Facebook, Twitter, Linkedin* və s. kimi çoxlu sayda sosial şəbəkələr mövcuddur. Bu sosial şəbəkələr gündən-günə populyarlaşır və cəmiyyətin həyatında vacib rol oynayır. İstifadəçi maraqlarından asılı olaraq, müxtəlif xüsusiləşdirilmiş sosial qruplar - məsələn, istifadəçilərə işgüzar əlaqələr yaratmağa və iş təklif etməyə imkan verən *LinkedIn* və *Xing* kimi biznesyönümlü şəbəkələr yaradılmışdır. Bəzi sosial şəbəkələr isə sadəcə insanlar arasında kommunikasiya yaratmaq üçün nəzərdə tutulmuşdur və virtual görüş üçün mühit rolunu oynayır. Bununla yanaşı, sosial şəbəkələr istifadəçilərin şəxşi həyatının toxunulmazlığı və informasiya təhlükəsizliyi ilə bağlı yeni problemlər yaradır. Yəni sosial şəbəkələrin 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. Göstərilən təhlükələrlə yanaşı, sosial şəbəkə istifadəçilərin məqsədlərindən asılı olaraq, milli təhlükəsizliyə də bir sıra təhlükələr yarada bilər [2]

Digər tərəfdən, son zamanlar sosial şəbəkə istifadəçilərinin sayı həddindən artıq çoxalmış və artıq iki milyard nəfəri keçmişdir. Proqnozlara görə, 2018-ci ildə sosial şəbəkə istifadəçilərinin sayı 2,5 milyard nəfərə çatacaq [3]. Sosial şəbəkələrdən belə kütləvi şəkildə istifadə və istifadəçilər tərəfindən böyük həcmdə informasiya generasiya edilməsi onları bədniyyətlilərin, cinayətkarların hücum obyektinə çevirmişdir. Sosial şəbəkələr bədniyyətlilər tərəfindən spamların [4] yayılmasından başlayaraq, fərdi fişinq [5] hücumlarına qədər müxtəlif növ hücumların həyata keçirilməsi üçün əlverişli bir platforma kimi istifadə edilir. Təbii ki, belə bir şəraitdə İnternet mühitində informasiya təhlükəsizliyinin və insanların sosial şəbəkələrdən təhlükəsiz istifadə etməsinin təmin edilməsi çox aktual bir məsələyə çevrilmişdir. Buna görə də sosial şəbəkələrdə informasiya təhlükəsizliyinin və sosial aspektli təhlükələrin və onlardan mühafizə üsullarının analizi çox vacibdir. Belə bir analiz İnternet mühitində informasiya təhlükəsizliyinin təmin edilməsi və insanların sosial şəbəkələrdən təhlükəsiz istifadə etməsi baxımından əhəmiyyət kəsb edir.

Sosial şəbəkə təhlükələri

Sosial şəbəkələrdə təhlükəsizlik, əsasən, istifadəçilərin fərdi məlumatlarının bədniyyətlilərin əməllərindən mühafizə edilməsi məsələlərini əhatə edir. Bunun üçün sosial şəbəkə istifadəçiləri onların fərdi məlumatları ilə bağlı müxtəlif risklərdən və təhlükələrdən xəbərdar olmalıdırlar.

Sosial şəbəkələrdə baş verə biləcək təhlükələri dörd qrupa ayırmaq olar. Birinci qrupa ənənəvi təhlükələr, xüsusi ilə də, şəxsi həyatın toxunulmazlığı və təhlükəsizliklə bağlı təhdidlər aiddir. Bu təhlükələr təkcə sosial şəbəkə istifadəçilərinə deyil, həmçinin sosial şəbəkədən istifadə etməyən digər İnternet istifadəçilərinə təhlükə yaradır. İkinci qrup şəxşi həyatının toxunulmazlığı və təhlükəsizliklə bağlı müasir təhdidləri əhatə edir. Bu təhlükələr, əsasən, sosial şəbəkə mühitinə xasdır və sosial şəbəkə infrastrukturundan istifadə edərək istifadəçilərin şəxsi həyatının toxunulmazlığına və təhlükəsizliyinə təhdidlər yaradır. Üçüncü qrupa müxtəlif təhlükələrin kombinasiyası daxildir, yəni müxtəlif təhlükələrin birləşməsi nəticəsində daha mürəkkəb və təhlükəli hücumlar həyata keçirilə bilər. Dördüncü qrupa sosial aspekli təhlükələr aiddir. Bu təhlükələrə misal kimi, izləmə, aldatma, şantaj, qarayaxma və s. kimi təhdidləri göstərmək olar.

Ənənəvi təhlükələr İnternet geniş istifadə edilməyə başlayandan bəri problem olaraq qalır. Bu təhlükələrə ziyanlı proqramlar [6], spamlar [7], fişinq [8] və s. aid edilir. Bunlar sosial şəbəkələrin strukturundan və xarakterindən asılı olaraq çox təhlükəli ola bilir və tez bir zamanda çoxlu sayda istifadəçi kompüterlərinə yayıla bilir. Bu təhlükələr sosial şəbəkələrdə yerləşdirilmiş istifadəçinin fərdi məlumatlarından istifadə edərək həm onların özlərinə, həm də "dostlarına" təhlükə yarada bilər. Məsələn, bədniyyətlilər istifadəçilərin *Facebook* profilindəki detallardan istifadə edərək, ilk baxışdan cəlbedici görünən spam-məlumatlar yarada və bu məlumatlara ziyanlı proqram kodu yerləşdirə bilərlər. Bu məlumatların şəxsi xarakter daşıdığını nəzərə alaraq, demək olar ki, böyük ehtimalla, hansısa istifadəçi onu açacaq və nəticədə kompüteri ziyanlı proqrama yoluxmuş olacaq. Çox zaman bu təhlükələrin hədəfi gündəlik və vacib istifadəçi resurslarıdır. Bu resurslara kredit kartların nömrələri, hesab parolları, hesablama gücü, buraxma zolağı və s. aiddir. Həmçinin bu təhlükələr əldə edilmiş məlumatları yoluxmuş kompüterin istifadəçisinin adından məlumatlar göndərilməsi üçün istifadə edə və hətta istifadəçinin fərdi məlumatlarını dəyişdirə bilər.

Ziyanlı proqramların yaradılmasının məqsədi istifadəçilərin qeydiyyat verilənlərinin toplanması və fərdi məlumatlara giriş əldə edilməsi üçün kompüterlərin işinin pozulmasıdır. Bu proqramların sosial şəbəkələrdə istifadəçilər və onların "dostları" arasında yayılması üçün sosial şəbəkələrin struktur xüsusiyyətlərindən istifadə olunur. Bəzi hallarda ziyanlı proqramlar istifadəçilərin "dostlarına" yoluxdurulmuş məlumatlar göndərilməsi üçün onların qeydiyyat verilənlərindən istifadə edirlər.

Facebook, *MySpace* və *Twitter* kimi sosial şəbəkələrdə ilk yayılan ziyanlı proqram *Koobface* soxulcanı olmuşdur. Yoluxma zamanı *Koobface* soxulcanı istifadəçilərin qeydiyyat verilənlərini əldə etməyə və yoluxdurulmuş kompüterləri botnet şəbəkəsinə qoşmağa çalışır [9]. Botnet şəbəkəsinə qoşulmuş kompüterlər "zombilərə" çevrilir və bundan sonra bəd niyyətlər, yəni spamların göndərilməsi, İnternetə qoşulmuş digər kompüterlərə və xidmətlərə hücum edilməsi və s. üçün istifadə edilir.

Fişinq hücumları sosial mühəndislik hücumlarına aiddir və istifadəçilərin konfidensial informasiyasını və fərdi məlumatlarını əldə etmək üçün istifadə edilir. Bunun üçün hücum edən özünü üçüncü etibarlı tərəf kimi qələmə verir. Adətən, sosial şəbəkə istifadəçiləri fişinq hücumlarına özlərinin daha çox sosiallıqlarına və sadəlövhlüklərinə görə məruz qalırlar [10]. Buna görə də son zamanlar sosial şəbəkələrdə fişinq hücumları cəhdləri çoxalmışdır. Microsoft şirkətinin təhlükəsizliklə bağlı hesabatına əsasən [11] İnternetdə baş verən fişinq hücumlarının 84,5%-nin hədəfi sosial şəbəkə istifadəçiləri olmuşdur.

Spamlar elektron məlumat mübadiləsi sistemlərini istifadə etməklə, "spamer" adlanan istifadəçilər tərəfindən digər istifadəçilərə göndərilən reklam xarakterli arzuolunmaz məlumatlardır. Sosial şəbəkə spamerləri digər istifadəçilərə spam göndərmək üçün sosial şəbəkə

platformasından istifadə edirlər. Bunun üçün spamerlər sosial şəbəkədə saxta profillər yaradırlar [12]. Həmçinin spamerlər sosial şəbəkə platformasını səhifələrə şərh xarakterli məlumatları əlavə etmək üçün istifadə edə bilərlər, çünki bu səhifələrə şəbəkədə çoxlu sayda istifadəçilər baxır.

Müasir sosial şəbəkə təhlükələri məhz bu mühitə xasdır. Adətən, bu təhlükələrin hədəfi sosial şəbəkə istifadəçilərinin, həmçinin onların "dostlarının" fərdi məlumatlarıdır. Məsələn, bədniyyətlilər *Facebook* istifadəçisinin fərdi məlumatlarına hücum etmək üçün saxta "dost" profili yaradır və ona sorğular göndərir. Əgər hədəf istifadəçi bu "dostun" sorğularını qəbul edərsə, onda onun fərdi məlumatları hücuma məruz qalır və bədniyyətlilər onları əldə edə bilirlər. Bundan başqa, bədniyyətlilər *Facebook* istifadəçisinin "dostlarının" məlumatlarını toplayıb analiz etməklə onun haqqında müəyyən məlumatlar əldə etmək imkanına malikdirlər.

Mövcud müasir sosial şəbəkə təhlükələri müxtəlif ssenarilər üzrə həyata keçirilir. Məsələn, *ClickJacking* adlanan hücum üsulu istifadəçiləri aldadaraq, ilk baxışdan faydalı olan, lakin əslində bədniyyətli olan istinadları "çıqqıldatmağa" (*click*) sövq edir. *ClickJacking*-dən istifadə edən bədniyyətlilər istifadəçiləri manipulyasiya edərək "bəyənmələr" (*like*) vasitəsi ilə (bu, həmçinin *likejacking* adlanır) spamların yayılmasını həyata keçirə bilər [13]. *ClickJacking* hücumuna misal kimi 2009-cu ildə *Twitter*-də baş vermiş "çıqqıldatmayın" (*Don't Click*) adlanan hücumu göstərmək olar. Bədniyyətlilər *Twitter*-də "çıqqıldatmayın" məlumatı ilə maskalanmış *URL* (faylın və ya resursun Web-də yerləşdiyi ünvanı və ya yeri göstərən lokator) ünvanı yerləşdirmişdilər (faktiki *URL* ünvanı gizlədilmişdi) və *Twitter* istifadəçiləri bu istinada daxil olan kimi həmin məlumat virus kimi yayılmış və istifadəçilərin hesablarında yerləşmişdi [14].

Sosial şəbəkələrdə əksər istifadəçilər öz şəxşi həyatının toxunulmazlığını və anonimliyini təmin etmək üçün təxəllüslərdən istifadə edirlər. Bədniyyətlilər buna qarşı "şəxsləşdirmə" (*de-anonymization*) adlanan hücumdan istifadə edirlər. Bu hücum zamanı real istifadiçələri müəyyən etmək üçün bədniyyətlilər kukilərin (*cookies* - xidmətlərdən yararlanmaq üçün istifadəçilərin kompüter, planşet və ya mobil telefon kimi qurğulardakı məlumatları saxlayan və bu məlumatlara daxil olan texnologiyadır), şəbəkə topologiyasının və istifadəçi qruplarının izlənilməsi üsullarından istifadə edirlər. Bununla yanaşı, sosial şəbəkə saytlarından sızan informasiyanın analizi vasitəsi ilə onları identifikasiya etmək mümkündür [15]. "Şəxsləşdirmə" hücumunun digər bir metodu ancaq sosial şəbəkə istifadəçilərinin qruplarda üzvlüyünün analiz olunmasından ibarətdir [16]. Bu metod *Xing* sosial şəbəkəsində yoxlanılmışdır və nəticədə istifadəçilərin 42%-i identifikasiya edilmişdir. Daha bir metod isə müxtəlif sosial şəbəkə istifadəçilərinin profillərinin müqayisəsinə əsaslanır [17].

Adətən, sosial şəbəkə istifadəçiləri öz profillərində özlərinin və "dostlarının" fotoşəkillərini yerləşdirirlər. Məsələn, *Facebook* sosial şəbəkəsində hər gün milyonlarla fotoşəkillər yerləşdirilir [18]. Bununla yanaşı, əksər *Facebook* istifadəçilərinin profilindəki şəkillər baxılması və yüklənməsi üçün açıqdır. Məsələn, *Faces of Facebook* veb-saytı [19] İnternet istifadəçilərinə 1,2 milyarddan çox istifadəçinin profil şəkillərinə baxmağa imkan verir. Bu şəkillər biometrik verilənlər bazasının yaradılması və sonra isə sosial şəbəkə istifadəçilərinin razılığı olmadan onların identifikasiyası üçün istifadə edilə bilər.

Saxta profillər (həmçinin "sosial botlar" adlanır) avtomatik və ya yarımavtomatik profillər olaraq insanın sosial şəbəkələrdəki davranışını təqlid edir. Çox zaman saxta profillər sosial şəbəkə istifadəçilərinin fərdi məlumatlarının toplanması üçün istifadə edilir. Bunun üçün sosial botlar sosial şəbəkə istifadəçiləri üçün "dostluq" təklifləri generasiya edir və çox zaman istifadəçilər bu təklifləri qəbul edirlər. Nəticədə, sosial botlar istifadəçilərin fərdi məlumatlarını əldə etmək imkanı əldə edir, çünki adətən, sosial şəbəkə istifadəçilərinin fərdi məlumatları ancaq "dostlar" üçün açıq olur. Bundan başqa, saxta profillər *Sybil* hücumunun [20] həyata keçirilməsi, sosial spamların yayılması [21] və s. üçün istifadə edilə bilər. Burada hücum edən çoxlu sayda identifikator (*Sybil*) yaradaraq, onları subyektin reputasiya xalını manipulyasiya etmək məqsədilə istifadə edir.

Bu gün bədniyyətlilər ənənəvi və müasir təhlükələri birləşdirərək daha mürəkkəb və təhlükəli hücumlar həyata keçirə bilərlər. Məsələn, onlar məqsədli şəkildə *Facebook*

istifadəçilərinin parollarını fişinq əsasında toplaya və sonra *ClickJacking* hücumuna malik olan məlumatları onların səhifələrində yerləşdirə bilərlər. Beləliklə, bədniyyətlilər *Facebook* istifadəçilərinin "dostlarını" aldadaraq yerləşdirilmiş məlumatları açmağa təhrik etmək və onların kompüterlərinə virus yerləşdirmək imkanına malik olurlar.

Sosial şəbəkələrdə sosial xarakterli çoxlu təhlükələr mövcuddur və bunlara izləmə, aldatma, şantaj, qarayaxma və s. kimi təhlükələr aid edilir. Təəssüf ki, bəzi insanlar sosial şəbəkələrdən digər insanlara qarşı bu cür təhlükələrin həyata keçirilməsi üçün istifadə edirlər. Bunun üçün bədniyyətlilər sosial şəbəkə istifadəçilərinin fərdi məlumatlarından və müxtəlif hücum vasitələrindən bəhrələnirlər. Bəzi hallarda belə təhlükələr hətta müxtəlif ölkələrə, təşkilatlara və s. qarşı istifadə edilir və bu gün sosial xarakterli təhlükələrin sayı xeyli artmışdır.

Sosial şəbəkələrdə izləmə ən geniş yayılmış və yaxşı məlum olan sosial xarakterli təhlükələrdən biridir. Belə təhlükələri həyata keçirən zaman bədniyyətlilər izləmə nəticəsində hədəfə aldıqları istifadəçilərin fərdi məlumatlarını (yerini, telefon nömrəsini, iş qrafikini, ev ünvanını və s.) və onların profillərini əldə edə bilərlər. Onlar bu təhlükə vasitəsi ilə hədəfə alınmış istifadəçilərə müxtəlif cür təsir göstərə bilərlər. Məsələn, bu təsir yüngül qorxutmadan başlayaraq, şantaj, şəxşi həyatın toxunulmazlığının pozulması və hətta ciddi fiziki təsirə (məsələn, terror), psixoloji sarsıntılara və s. kimi dəyişə bilər.

Sosial şəbəkələrdə təhlükələrdən qorunma üsulları

Son zamanlar sosial şəbəkələrdə təhlükələrdən qorunmaq üçün müxtəlif həllər təklif edilmişdir. Bu həllər müxtəlif səviyyələri, yəni sosial şəbəkə operatorları, təhlükəsizlik şirkətləri və elmi tədqiqatçıların təkliflərini əhatə edir.

Sosial şəbəkə operatorları öz istifadəçilərinin təhlükəsizliyini təmin etmək üçün müxtəlif təhlükəsizlik tədbirlərini həyata keçirirlər. Məsələn, istifadəçilərin autentifikasiyası mexanizmlərindən və fərdi məlumatların tənzimləmələri kimi tədbirlərdən istifadə edilir.

Autentifikasiya mexanizmləri sosial şəbəkə istifadəçilərinin sosial botlar və ya nüfuzdan salınmış istifadəçi hesabları deyil, həqiqətən, real insanlar olduğuna əmin olmaq üçün istifadə edilir. Yəni autentifikasiya sosial şəbəkələrdə real insanların qeydiyyatdan keçdiyinə və şəbəkəyə daxil olduğuna əmin olmağa imkan verir. Bunun üçün sosial şəbəkələrdə *CAPTCHA* (*Completely Automated Public Turing Test to Tell Computers and Humans Apart* - kompüter və insanlar üçün tam avtomatlaşdırılmış test türinqi) [22], "dostlarının" şəklinin identifikasiya edilməsi [23], yəni şübhəli istifadəçiyə təqdim edilmiş şəkillərin içərisindən "dostunu" tanıması təklif edilir, çoxfaktorlu autentifikasiya [24], yəni istifadəçilərə paroldan əlavə digər məlumatların daxil edilməsi tələb edilir və s. bu kimi müxtəlif autentifikasiya mexanizmləri tətbiq olunur. Bu cür autentifikasiya mexanizmləri bədniyyətlilərin sosial botlar və ya nüfuzdan salınmış istifadəçi hesabları vasitəsi ilə real istifadəçilərin fərdi məlumatlarını ələ keçirmələrinin, ziyanlı proqramların və spamların yayılmasının qarşısını almağa imkan verir.

Sosial şəbəkələrin əksəriyyəti istifadəçilərə öz fərdi məlumatlarının tənzimlənməsinə şərait yaradır. Bu da istifadəçilərə öz şəxsi məlumatlarını digər istifadəçilərdən mühafizə etməyə imkan verir [25, 26]. Məsələn, *Facebook* istifadəçiləri öz fərdi məlumatlarını tənzimləyə bilər və onlara baxmağa icazəni idarə edə bilər, yəni bu və ya digər şəkillərə, məlumatlara və digər şəxsi məlumatlara baxa biləcək istifadəçi kateqoriyalarını ("dostlar", "dostlarin dostları" və "hər bir kəs") müəyyən edə bilər [27]. Bəzi sosial şəbəkə operatorları istifadəçilərə digər əlavə təhlükəsizlik konfiqurasiyalarını həyata keçirməyə imkan verir. Bu konfiqurasiyalar istifadəçilərə öz fərdi məlumatlarına təhlükəsiz baxışı aktivləşdirməyə, hesabına giriş haqqında bildiriş almağa və digər təhlükəsizlik funksiyalarını təyin etməyə imkan verir [28]. Buna baxmayaraq, əksər istifadəçilər fərdi məlumatlarının təhlükəsizliyinin tənzimlənməsi parametrlərini o qədər də yaxşı idarə etmirlər və öz şəxsi məlumatlarını təhlükə qarşısında qoyurlar [29].

Bəzi sosial şəbəkə operatorları öz istifadəçilərinin təhlükəsizliyini təmin etmək üçün əlavə daxili təhlükəsizlik mexanizmlərindən istifadə edirlər. Bu təhlükəsizlik mexanizmləri spamların

yayılması, saxta profillərdən, fırıldaqçılıqdan və s. kimi təhlükələrdən mühafizə olunmağa imkan verir [30]. Məsələn, *Facebook* öz istifadəçilərini ziyanlı hücumlardan və informasiyanın icazəsiz toplanmasından mühafizə etmək üçün *FIS*-dən *(Facebook Immune System – Facebook* immun sistemi) istifadə edir [31]. *FIS Facebook*-un verilənlər bazasında oxuma və yazma əməliyyatlarının real zaman rejimində analizini və təsnifatını həyata keçirir.

Sosial şəbəkə operatorları müəyyən qrup istifadəçiləri, əsasən də, uşaqları və yeniyetmələri digər istifadəçilər tərəfindən təqib etmədən qorumaq üçün sosial saytlara məlumatlandırma opsiyası əlavə ediblər [32]. Bəzi ölkələrdə isə uşaqları daha yaxşı qorumaq üçün sosial şəbəkələrə, məsələn, *Facebook*-a "Həyəcan düyməsi" ("*Panic Button*") adlanan düymə əlavə etdilər [33]. Bununla yanaşı, belə təhlükələrin qarşısını almaq üçün artıq bəzi sosial saytlar potensial qurbanları (məsələn, uşaqları) mühafizə etmək üçün müəyyən təşkilatlarla əməkdaşlıq əlaqələri qururlar. Məsələn, 2010-cu ildə *Facebook* Böyük Britaniya Uşaqların Müdafiəsi Təşkilatının müraciəti əsasında şübhəli davranışlar və ya sui-istifadələr haqqında hesabat əldə edilməsi üçün düymə daxil etdi.

Sosial şəbəkələrdə təhlükələrdən mühafizə üçün təhlükəsizlik sahəsində çox yaxşı məlum olan şirkətlər tərəfindən müxtəlif kommersiya həlləri təklif edilmişdir. Məsələn, *AVG, Avira, Kaspersky, Norton, Panda, McAfee, Symantec* və s. təhlükəsizlik şirkətləri sosial şəbəkə istifadəçilərinə müxtəlif İnternet-təhlükəsizlik həlləri təklif etmişlər. Adətən, bu həllərə antiviruslar, şəbəkələrarası ekranlar və s. İnternet-təhlükəsizlik proqramları daxil olur. Müvafiq həllər sosial şəbəkə istifadəçilərinə öz kompüterlərini ziyanlı proqramlardan, botnetlərdən, *ClickJacking*, fişinq və s. tipli hücumlarından qorumağa imkan verir. Məsələn, *AVG PrivacyFix* [34] proqram təminatı mobil tətbiq və ya veb-brauzer əlavəsi olaraq *Facebook*, *LinkedIn* və *Google* istifadəçilərinə fərdi məlumatlarını tənzimləməyə imkan yaradır. *Norton Safe Web* [35] proqramı *Facebook* tətbiqi olaraq istifadəçilərin yeni "dostlarını" axtarır və onlara təhlükəli istinadlar və saytlar haqqında məlumat verir. *McAfee Social Protection* [36] proqramı mobil tətbiq olaraq *Facebook* istifadəçilərinə öz səhifələrinə yerləşdirilmiş şəkilləri mühafizə etməyə və onlara digər istifadəçilər tərəfindən baxılması və yüklənməsini idarə etməyə imkan verir.

Sosial şəbəkələrdə təhlükələrdən qorunmaq üçün elmi tədqiqatçılar tərəfindən təklif olunmuş həllər müxtəlif sosial şəbəkə təhlükələrinin tədqiqinə əsaslanır. Bu həllər, əsasən, bədniyyətli istifadəçilərin və ziyanlı tətbiqlərin aşkarlanmasına yönəlmişdir. Təklif edilmiş həllər sosial şəbəkə operatorları tərəfindən istifadəçilərin şəxsi həyatının toxunulmazlığının təmin edilməsi üçün istifadə edilə bilər.

Son on il ərzində sosial şəbəkələrin təhlükəsizliyi ilə bağlı, yəni fərdi məlumatların qorunması, fişinqin, spamların, klonlaşdırılmış və saxta profillərin aşkarlanması və s. sahələrdə çoxlu sayda tədqiqat işləri həyata keçirilmişdir. Məsələn, *Facebook* üçün *Audience View* interfeysi təklif edilmişdir [37]. Bu interfeys *Facebook* istifadəçilərinə öz profillərinə digər istifadəçilərin, məsələn, "dostun" və yaxud digərinin nöqteyi-nəzərindən baxmağa imkan verir. Belə bir interfeys sosial şəbəkə istifadəçilərinə hansı şəxsi verilənlərinin digər istifadəçilər üçün əlyetərli olduğunu bilməyə və şəxsi məlumatlar interfeysini tənzimləməyə imkan verər. Sosial şəbəkələrdə istifadəçilərin məxfiliyinin təmin edilməsi vacib məsələlərdən biridir və bunun üçün *FaceCloak* adlanan arxitektur təklif edilmişdir [38]. Bu arxitektura əsasən, istifadəçinin şəxsi informasiyası həm sosial şəbəkə istifadəçilərindən, həm də digər istifadəçilərdən qorunur. Bunun üçün *FaceCloak* məxfi informasiyanı ayrı bir serverdə şifrlənmiş şəkildə saxlayır. Buna baxmayaraq, *FaceCloak* sosial şəbəkənin rahat istifadə olunmasını təmin edir. Digər bir vacib məsələ sosial şəbəkələrdə istifadəçilərin şəxsi həyatının toxunulmazlığının təmin edilməsidir ki, bunun üçün sosial məxfiliyin təmin edilməsi vasitəsinin yaradılması üçün şablon təklif edilmişdir [39]. Bu şablon sosial şəbəkə istifadəçilərinin fərdi məlumatlarının avtomatik tənzimlənməsinə imkan verir.

Fişinq hücumlarına qarşı mübarizə ilə bağlı təklif olunmuş metodların əksəriyyəti fişinq veb-saytlarının və fişinq istinadlarının aşkarlanması metodlarına əsaslanır [40-42]. Sosial

şəbəkələrdə fişinq hücumlarının sayı artdıqca onların identifikasiyası üçün müxtəlif metodlar işlənmişdir. Misal üçün, *Twitter* üçün *WarningBird* adlanan şübhəli *URL*-lərin aşkarlaması sistemi təklif edilmişdir [43]. Bu sistem yönəldici *URL*-lərin "arxasında gizlənən" fişinq hücumlarını aşkarlamağa imkan verir.

Sosial şəbəkələrdə spamların aşkarlanması üçün də çoxlu sayda həllər təklif olunmuşdur. Məsələn, video-spamların aşkarlanması üçün alqoritm hazırlanmışdır [44]. Bu alqoritm *YouTube*-da spamları aşkarlamağa imkan verir. *Twitter* sosial şəbəkəsində spamların klassifikasiyası üçün isə kontentin və sosial şəbəkə sxeminin xüsusiyyətlərindən istifadə edilməsi təklif edilmişdir [45]. Sosial şəbəkələrdə spamların aşkarlanması üçün həmçinin maşın təlimi alqoritmindən istifadə olunmuşdur [46]. Maşın təlimi alqoritmi müxtəlif növ spamları aşkarlamağa imkan verir.

Sosial şəbəkələrdə klonlaşdırılmış profillərin aşkarlanması üçün müxtəlif metod və yanaşmalar təklif edilmişdir. Məsələn, sosial şəbəkə istifadəçilərinin profillərinin klonlaşdırılması hücumunun qurbanı olub-olmadığının müəyyən edilməsi üçün metod işlənmişdir [47]. Sosial şəbəkələrdə profillərin klonlaşdırılması hücumunun aşkarlanması üçün isə *CloneSpotter* adlanan yanaşma irəli sürülmüşdür [48]. Bu yanaşma istifadəçilərin sosial şəbəkə operatorları üçün əlyetərli olan qeydiyyat verilənlərinin analizinə əsaslanır.

Sosial şəbəkələrdə saxta profillərin aşkarlanması ilə bağlı da müxtəlif yanaşmalar təklif edilmişdir. Bu yanaşmalar saxta profillərin aşkarlanması və müxtəlif *Sybil* hücumlarının [49] qarşısının alınmasının müxtəlif alqorim, metod və vasitələrini əhatə edir. Lakin saxta profillərin aşkarlanması və *Sybil* hücumlarından mühafizə alqoritmlərinin məqsədlərinin eyni, yəni saxta profillərin aşkarlanması olmasına baxmayaraq, aralarında fərqlər vardır. Saxta profillərin aşkarlanması alqoritmləri, bütövlükdə, sosial şəbəkələrdə saxta profillərin, o cümlədən sosial şəbəkələrdə bir neçə saxta profilləri əlində saxlayan kibercinayətkarları aşkarlamağa yönəlmişdir. *Sybil* hücumlarından mühafizə alqoritmləri isə, adətən, sosial şəbəkələrdə bir neçə saxta profilləri yaradan bədniyyətlilərin identifikasiyasına yönəlmişdir. Bunun üçün *SybilGuard* [50] və *SybilLimit* [51] adlanan protokollar təklif edilmişdir. Bununla yanaşı, sosial şəbəkələrdə "həqiqi" və "saxta" istifadəçiləri aşkarlamağa imkan verən *SybilInfer* adlanan alqoritm işlənmişdir [52]. Digər bir yanaşma isə istifadəçilərin həqiqiliyinin müəyyən edilməsi üçün sosial şəbəkələrin struktur xüsusiyyətlərinin istifadə edilməsindən ibarətdir və bunun üçün *SybilRank* adlanan vasitə təklif edilmişdir [53].

Nəticə

Bu gün sosial şəbəkələr insanların gündəlik həyatının bir hissəsinə çevrilmişdir. Əksər İnternet istifadəçiləri onlayn fəallığa sərf etdikləri vaxtın çox hissəsini sosial şəbəkələrdə keçirirlər. Sosial şəbəkələr vasitəsi ilə insanlar bir-biri ilə əlaqə yaradır, informasiya (məlumat, şəkil və video) və təcrübələrini bölüşürlər. Bununla yanaşı, sosial şəbəkələrdə müxtəlif təhlükələr mövcuddur. Hakerlər, dələduzlar və s. sosial şəbəkələri yeni "qurbanların" tapılması və öz bəd əməllərinin həyata keçirilməsi üçün vasitə kimi istifadə edirlər. Buna görə də sosial şəbəkələrdə mövcud olan təhlükələrin və onlardan mühafizə üsullarının analizi çox aktualdır.

Məqalədə sosial şəbəkələrdə mövcud olan təhlükələr və onlardan mühafizə üsulları analiz edilmişdir. Analizin nəticəsində belə nəticəyə gəlmək olar ki, sosial şəbəkələrdə mövcud olan təhlükələr faktiki olaraq iki kateqoriyaya aiddirlər: ənənəvi informasiya təhlükəsizliyi təhdidləri və sosial aspektli təhdidlər. Onu da qeyd etmək lazımdır ki, bu və ya digər təhlükənin hansı kateqoriyaya aid olmasından asılı olmayaraq, onlar, əsasən, sosial şəbəkə istifadəçilərinin şəxsi həyatının toxunulmazlığının pozulmasına yönəlmişdir. Demək olar ki, insanların sosial şəbəkələrdə, yəni virtual dünyada şəxsi həyatının toxunulmazlığının pozulması onların real həyatına birbaşa əks olunur.

Sosial şəbəkələrdə mövcud olan təhlükələr və onlardan mühafizə üsullarının analizinin nəticələri insanların sosial şəbəkələrdən təhlükəsiz istifadə etmələrinə və sosial şəbəkə

operatorlarına öz istifadəçilərinin təhlükəsizliyinin təmin edilməsi üçün vasitələrin və həllərin seçilməsində köməklik edər.

Ədəbiyyat

1. Stern J., Introduction to web 2.0 technologies, http://www.wlac.edu
2. İmamverdiyev Y., Sosial media və təhlükəsizlik problemləri / Beynəlxalq Telekommunikasiya İttifaqının 150 illiyinə həsr olunmuş İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II Respublika elmi-praktiki konfransı, 2015, səh. 189-192.
3. http://www.statista.com/topics/1164/social-networks/
4. Stringhini G., Kruegel C., Vigna G., Detecting spammers on social networks / Proc. of the 26th annual computer security applications conference, 2010, pp. 1-9.
5. Jacoby D., Facebook security phishing attack in the wild, https://securelist.com/blog/events/31951/facebook-security-phishing-attack-in-the-wild-14
6. https://en.wikipedia.org/wiki/Malware
7. https://en.wikipedia.org/wiki/Spamming/
8. https://en.wikipedia.org/wiki/Phishing
9. Baltazar J., Costoya J., Flores R., The real face of koobface: The largest web 2.0 botnet explained, Trend Micro Res., 2009, vol. 5, no. 9, 10 p.
10. Amin T., Okhiria O., Lu J., An J., Facebook: A comprehensive analysis of phishing on a social system, EECE 412 Term Project Report, 2010, 6p., http://www.courses.ece.ubc.ca/412/term_project/reports/ 2010/facebook.pdf
11. Cavit D. Microsoft security intelligence report, 2010, vol. 10, 89 p. http://www.microsoft.com/en-us/download/details.aspx?id=17030
12. Fire M., Katz G., and Elovici Y., Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies / ASE human journal, 2012, vol. 1, no. 1, pp. 26-39.
13. Lundeen R., Ou J., Rhodes T., New ways I'm going to hack your web app // Proc. of the Blackhat AD, 2011, pp. 1-11.
14. McMillan R., Researchers make wormy twitter attack / PCWorld, 2009, http://www.pcworld.idg.com.au/article/296382/researchers_make_wormy_twitter_attack/
15. Krishnamurthy B., Wills C. E., On the leakage of personally identifiable information via online social networks // Proc. of the 2nd ACM workshop on online social networks, 2009, pp. 7-12.
16. Wondracek G., Holz T., Kirda E., and Kruegel C., A practical attack to de-anonymize social network users // Proc. of the security and privacy IEEE symposium, 2010, pp. 223-238.
17. Peled O., Fire M., Rokach L., Elovici Y. Entity matching in online social networks // Proc. of the international conference on social computing, 2013, pp. 339-344.
18. Facebook, Form 10-k (Annual Report)—Filed 02/01/13 for the Period Ending 12/31/12, 2013, 139 p., http://files.shareholder.com/downloads/AMDA-NJ5DZ/2301311196x0 xS1326801-13-3/1326801/1326801-13-3.pdf
19. The Faces of Facebook, http://www.app.thefacesoffacebook.com/
20. Douceur J. R., The sybil attack // Proc. of the 1st international workshop on peer-to-peer systems, 2002, pp. 251-260, http://www.dl.acm.org/citation.cfm?id=646334.687813
21. Gao H. Detecting and characterizing social spam campaigns // Proc. of the 10th ACM SIGCOMM conference on Internet measurement, 2010, pp. 35-47.
22. Boshmaf Y., Muslukhov I., Beznosov K., and Ripeanu M., The socialbot network: When bots socialize for fame and money // Proc. of the 27th annual computer security applications conference, 2011, pp. 93-102.
23. Jeffries A., Facebook's security check asks users to identify photos of friends' dogs, Gummi Bears [UPDATED], 2010, http://readwrite.com/2010/08/04/facebooks_security_check_asks_users_to_identify_ph

24. Song A., Introducing login approvals, 2011, https://www.facebook.com/note.php?note_id=10150172618258920
25. Liu Y., Gummadi K., Krishnamurthy B., and Mislove A., Analyzing facebook privacy settings: User expectations vs. reality // Proc. of the ACM SIGCOMM conference on Internet measurement conference, 2011, pp. 61-70.
26. Mahmood S., Desmedt Y., Poster: Preliminary analysis of google+'s privacy // Proc. of the 18th ACM conference on Computer and communications security, 2011, pp. 809-812.
27. Facebook, Facebook Help Center: Privacy, http://www.facebook.com/help/privacy
28. Axten S., Staying in control of your facebook logins, https://www.facebook.com/notes/facebook/staying-in-control-of-your-facebook-logins/389991097130
29. Fire M., Kagan D., Elyashar A., and Elovici Y., Friend or foe? Fake profile identification in online social networks / Springer journal of social network analysis and mining, 2014, vol.4 no.1, pp 194-216.
30. Chowdhury A., State of twitter spam, 2010, https://blog.twitter.com/2010/state-twitter-spam
31. Stein T., Chen E., and Mangla K., Facebook immune system // Proc. of the 4th workshop on social network systems, 2011, pp. 1–8.
32. Facebook, Report abuse or policy violations, https://www.facebook.com/report
33. Axon S., Facebook Will Add a Panic Button for U.K. Teens, Jul. 2010., http://www.mashable.com/2010/07/11/facebook-panic-button-ceop
34. AVG, Avg Privacyfix: http://www.privacyfix.com
35. Symantec, Norton Safe Web: https://www.facebook.com/appcenter/nortonsafeweb
36. McAfee, Mcafee Social Protection Beta: https://www.protectmediaonline.com
37. Lipford H. R., Besmer A., Watson J., Understanding privacy settings in facebook with an audience view // Proc. of the 1st conference on usability, psychology, and security, 2008, pp. 21-28.
38. Luo W., Xie Q, Hengartner U, FaceCloak: An architecture for user privacy on social networking sites, // Proc. of the international conference on computational science and engineering, 2009, vol. 3, pp. 26-33.
39. Fang L., LeFevre K., Privacy wizards for social networking sites // Proc. of the 19th international conference on world wide web, 2010, pp. 351-360.
40. Garera S., Provos N., Chew M., Rubin A. D., A framework for detection and measurement of phishing attacks // Proc. of the ACM workshop on recurring malcode, 2007, pp. 1-8.
41. Ma J., L. Saul K., Savage S., Voelker G. M., Beyond blacklists: Learning to detect malicious web sites from suspicious urls // Proc. of the 15th ACM SIGKDD international conference on knowledge discovery and data mining, 2009, pp. 1245-1254.
42. Xiang G., Hong J., Rose C. P., Cranor L., CANTINA+ A feature-rich machine learning framework for detecting phishing web sites / A ACM transactions on information and system security 2011, vol. 14, no. 2, pp. 1-28.
43. Lee S., Kim J., Warningbird: Detecting suspicious urls in twitter stream // Proc. Of the 19th Annual Network & Distributed System Security Symposium, 2012, pp. 1-13.
44. Benevenuto F., Rodrigues T., Almeida V., Almeida J., Gonɜalves M., Detecting spammers and content promoters in online video social networks // Proc. of the 32nd international ACM SIGIR conference on research and development in information retrieval, 2009, pp. 620-627.
45. Wang A., Don't follow me: Spam detection in twitter // Proc. of the international conference on security and cryptography, 2010, pp. 1-10.
46. Aggarwal A., Almeida J., Kumaraguru P., Detection of spam tipping behaviour on foursquare // Proc. of the. 22nd international conference on World Wide Web, 2013, pp. 641-648.
47. Kontaxis G., Polakis I., Ioannidis S., Markatos E., Detecting social network profile cloning // Proc. of the IEEE international conference on pervasive computing and communications workshops, 2011, pp. 295-300.

48. Shan Z., Cao H., Lv J., Yan C., and Liu A., Enhancing and identifying cloning attacks in online social networks // Proc. of the 7th international conference on ubiquitous information management and communication, 2013, pp. 17-19.
49. Koll D., Jun Li, Stein, J., Xiaoming Fu, On the state of OSN-based Sybil defenses // Proc. of the IFIP networking conference, 2014, pp. 1-9.
50. Yu H., Kaminsky M., Gibbons P., and Flaxman A., Sybilguard: Defending against sybil attacks via social networks // Proc. of the conference on applications, technologies, architectures, and protocols for computer communications, 2006, vol. 36, no. 4, pp. 267-278.
51. Yu H., Gibbons P. B., Kaminsky M., and Xiao F., Sybillimit: A nearoptimal social network defense against sybil attacks / IEEE/ACM transactions on networking, 2010, vol. 18, no. 3, pp. 885-898.
52. Danezis G. and Mittal P., Sybilinfer: Detecting sybil nodes using social networks // Proc. of the 16th annual network & distributed system security symposium, 2009, 16 p.
53. Cao Q., Sirivianos M., Yang X., Pregueiro T., Aiding the detection of fake accounts in large scale social online services // Proc. of the 9th USENIX conference on networked systems design and implementation, 2012, p. 15.

УДК 004.056.53

Шыхалиев Рамиз Г.
Институт Информационных Технологий НАНА, Баку, Азербайджан
ramiz@science.az

Проблемы безопасности в социальных сетях

Сегодня в Интернете имеется множество социальных сетей. Эти социальные сети весьма популярны и играют очень важную роль в жизни людей. Однако социальные сети приводят к появлению новых рисков в области информационной безопасности. Эти риски связаны с такими угрозами, как распространение вредоносных программ и спамов, а также угрозами к учетным записям социальных сетей, преследованием, обманом и т.д. Статья посвящена анализу имеющихся в социальных сетях угроз и вопросам защиты от них.

Ключевые слова: *социальная сеть, вредоносная программа, спам, фишинг, фальшивый профиль.*

Ramiz H. Shikhaliyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
ramiz@science.az

Social network security issues

The article analyzes the existing threats and issues of protection against them. Today, the Internet has a lot of social networks. These social networks are very popular and play a very important role in society. However, social networks lead to the emergence of new risks in the field of information security. The risks associated with threats such as the spread of malware and spam, social engineering, as well as threats to the social network accounts, harassment, fraud, etc.

Key words: *social network, malware, spam, phishing, fake profile.*