Советказы Бекенович Кайсанов – преподаватель кафедры «IT-технологий»; Университет имени Шакарима города Семей, Республика Казахстан; e-mail: kaisanov@mail.ru.

Авторлар туралы мәліметтер

Владислав Игоревич Шумкин* – техника ғылымдарының магистрі, «IT технологиялар» кафедрасының оқытушысы; Семей қаласының Шәкәрім атындағы университеті, Қазақстан Республикасы; e-mail: shumkin1999@list.ru. ORCID: https://orcid.org/0009-0005-0652-5603.

Советказы Бекенович Кайсанов – «IT технологиялар» кафедрасының оқытушысы; Семей қаласының Шәкәрім атындағы университеті, Қазақстан Республикасы; e-mail: kaisanov@mail.ru.

Received 01.08.2024
Revised 28.08.2024
Accepted 12.09.2024

https://doi.org/10.53360/2788-7995-2024-3(15)-7

ҒТАХР: 81.93.29

А. Бимырзақызы*, Ж.М. Алимжанова
Әл-Фараби атындағы Қазақ Ұлттық Университеті,
050040, Қазақстан Республикасы, Алматы қаласы, Әл-Фараби даңғылы, 71
*e-mail: akerkebeimirzakizi@gmail.com

ЗЕРТТЕУ АРҚЫЛЫ КИБЕРҚАУІПТЕРДІ АНЫҚТАУ

Аңдатпа: *Жұмыста киберқауіптерді анықтау үшін қолданылатын әлеуметтік желілерді талдаудың негізгі әдістеріне шолу берілген. Әлеуметтік желілердегі қауіптердің негізгі түрлері көрсетілген және олардың алдын алудың кейбір қорғау әдістері сипатталған. Киберқауіптерді анықтауға бағытталған әлеуметтік желіні талдаудың типтік міндеттері, мысалы, желідегі қауымдастықтарды анықтау, қауымдастықтардағы көшбасшылар мен сарапшыларды анықтау, қауымдастықтардың тұрақтылығын талдау, мәтіндік ақпаратты кластерлеу және т.б. Цифрландыруды ұлғайту және әлеуметтік желілерді коммуникация құралы ретінде белсенді пайдалану жағдайында киберқауіпсіздікті қамтамасыз ету үшін тиімді мониторинг пен деректерді талдаудың маңыздылығы барған сайын өзекті бола түсуде. Әлеуметтік желілердегі деректердің үлкен көлемін өңдеуге байланысты күрделіліктер мен қиындықтар, соның ішінде құпиялылық мәселелері мен пайдаланушы деректерін бақылаудың этикалық аспектілері де талданады. Зерттеу әлеуметтік желіні киберқауіптерді белсенді түрде анықтау және алдын алу құралы ретінде пайдаланудың тұтас көрінісін ұсынады, аналитикалық жүйелерді ұйымдар мен жеке тұлғалардың жалпы киберқауіпсіздік шеңберіне біріктірудің маңыздылығын көрсетеді. Зерттеу әлеуметтік желіні киберқауіптерді белсенді анықтау және алдын алу құралы ретінде пайдаланудың тұтас көрінісін береді, аналитикалық жүйелерді ұйымдар мен жеке тұлғалардың жалпы киберқауіпсіздік ұстанымына біріктірудің маңыздылығын көрсетеді, сонымен бірге машиналық оқытуды жақсарту қажеттілігіне назар аударады және сандық ортадағы қауіптердің алдын алу мен бейтараптандырудың тиімдірек болуына ықпал ете алатын пайдаланушы мінез-құлқын және қауымдастық динамикасын тереңірек және дәлірек талдауға арналған жасанды интеллект әдістері.*

Түйін сөздер: *әлеуметтік желіні талдау, фишинг, киберқауіптер, көшбасшыны анықтау әдістері, ақпараттың шығуы, Advanced Persistent Threat (APT) шабуылдары.*

Кіріспе

Әлеуметтік желілердің қарқынды дамуы және олардың мәліметтерді жинақтау қабілеті олардың аналитикасына деген қызығушылықты арттырды және таланттарды иемдену, кәсіби топтастыру, әлеуметтік ұсыныстар, маркетинг, қоғаммен байланыс және жарнама сияқты көптеген салаларда қолданылатын жаңа әдістерді жасауға ықпал етті. Әлеуметтік желіні талдау қазіргі уақытта экономикалық және басқарушылық процестер мен құбылыстарды зерттеу үшін белсенді түрде қолданылады. Сондай-ақ ол жеке басын ұрлаумен, интернет-алаяқтықпен, киберқауіптермен, бағалы қағаздармен айла-шарғы жасау және инвестициялық алаяқтықпен күресу үшін, сондай-ақ қылмыстың алдын алу және басқа да осыған ұқсас мәселелерді шешу үшін қолданылады [1].

Осыған байланысты әлеуметтік желілер ақпараттық өріске және адамдардың психологиясына әсер ету үшін көбірек қолданылады. Олар қоғамдық пікірді қалыптастыруда,

негізгі саяси, экономикалық және әскери шешімдерді қабылдауда, жаудың ақпараттық активтеріне әсер етуде және әдейі дайындалған ақпаратты таратуда маңызды рөл атқарады [2]. Әлеуметтік желілерде деректерді жинау, мониторинг және талдау ақпараттық қауіпсіздікті қамтамасыз етудің маңызды және өзекті міндеттері болып табылады. Бұл жұмыстың негізгі мақсаты – осы саладағы қауіптерді анықтауға, алдын алуға және оларға қарсы күресуге бағытталған әлеуметтік желілерді талдаудың негізгі әдістері мен міндеттерін қарастыру және бағалау [3].

Әлеуметтік желілердегі қауіптер және алдын алу шаралары

Әлеуметтік желіні талдау киберқауіпсіздік саласында, әсіресе киберқауіптерді анықтау және алдын алу үшін маңызды құралға айналды. Twitter сияқты әлеуметтік желілер нақты уақытта қауіптерді анықтау үшін талдауға болатын бай деректерді ұсынады.

Қауіпті анықтау үшін әлеуметтік желін пайдаланудың белгілі бір қиындықтары бар, мысалы, деректердің үлкен көлемі, қатысы жоқ немесе қатысы жоқ хабарларға байланысты деректердегі шу және әлеуметтік желідегі білдіру формаларының әртүрлілігімен байланысты қиындықтар. Бұл факторлар қауіптерді дәл анықтауды қиындатуы мүмкін, бұл күрделірек деректерді өңдеу және талдау алгоритмдерін қажет етеді.

Әлеуметтік желі аналитикасы арқылы киберқауіптерді анықтау нақты уақытта қауіптерді бақылау және оларға жауап беру үшін құнды құралды ұсынады. Машиналық оқыту әдістерін дамыту және деректерді өңдеу алгоритмдерін жетілдіру киберқауіпсіздікті нығайту үшін жаңа мүмкіндіктер ашады. Алдағы уақытта қауіптерді анықтаудың дәлдігі мен жылдамдығын арттыру, сондай-ақ басқа киберқауіпсіздік жүйелерімен интеграция кибершабуылдардан қорғауда маңызды рөл атқарады.

Киберқауіптерді анықтау үшін әлеуметтік желіні тиімді пайдалану үздіксіз дамып келе жатқан киберқауіпсіздік қатерлерімен күресу үшін жаңа технологиялар мен әдістерді зерттеуді және әзірлеуді талап етеді.

Әлеуметтік желіні пайдалану арқылы киберқауіптерді анықтау, әсіресе, жеке өмірге және деректер жинауға қатысты бірқатар этикалық мәселелерді тудырады. Деректерді жинау және талдау процестерінің ашық болуын және деректерді қорғау заңнамасына сәйкестігін қамтамасыз ету қажет.

Түрлі зерттеулер әлеуметтік желі деректерінің фишинг, зиянды бағдарлама және әлеуметтік инженерия сияқты нақты киберқауіптерді анықтау үшін қалай пайдаланылғанын көрсетеді. Осындай зерттеулер мен тәжірибелік жағдайлардың мысалдары осы тәсілдің тиімділігінің қосымша дәлелі бола алады.

Әлеуметтік желілердегі спам. Спам – барлық уақыттағы ең классикалық шабуылдардың бірі. Шабуылшылар жалған аккаунттар жасайды және біреу оларды қабылдайды деген үмітпен автоматты түрде мыңдаған достық сұрауларын жібереді. Қабылданғаннан кейін, шабуылдаушы спам хабарламаларды жіберуді бастай алады. Тіпті досыңызбен байланысу сұрауы пайдаланушылар арасында бұрынғы байланыссыз оның ішінде қысқа хабарламалар жіберуге мүмкіндік береді. Спаммен күресу үшін көптеген қауымдастықтар CAPTCHA сынақтарын жүзеге асырады, олар тым көп хабар жіберілген кезде шешім қабылдайды. Бұл хабарламаларды автоматты түрде таратуды тоқтатуы немесе кем дегенде баяулатуы керек. Бұған қоса, шабуылдаушылар жиі бірнеше тіркелгілерді олардың әрқайсысы күнделікті шектеумен бұғатталғанша қатар пайдалану мүмкіндігіне ие. Көптеген әлеуметтік желілер хабарларды спам деп белгілеу және оларды болашақта бұғаттау мүмкіндігін ұсынады, бұл шабуылдаушылар жазбаларды жиі ауыстырмайтын болса, көмектеседі [4].

Әлеуметтік желілерде тұзақтарды орналастыру. Тұжырымдама қарапайым: тіркелгілер арналарының жоғарғы жағына спам хабарламаларын алу үшін кілт сөздер мен сілтемелерді пайдаланыңыз. Кейбір шабуылдаушылар тіпті зиянсыз болып көрінетін твиттерді жібермес бұрын манипуляциялай бастады. Олар танымал кілт сөздері бар жаңа жазбаларды іздейді. Бұл, мысалы, сәйкес жаңалықтар мақаласына қысқартылған сілтемесі бар соңғы футбол матчындағы даулы сәт туралы твит болуы мүмкін. Содан кейін алаяқ хабарламаны алады, бастапқы қысқа сілтемені зиянды сайтқа өзінің сілтемесімен ауыстырады және хабарламаны қайта жариялайды. Бұл қарапайым қолданушыларға зиянды және зиянды твиттерді ажырата алмайды. Осылайша, ақпаратты іздейтін бейхабар пайдаланушының зиянды сілтемеге тап болу ықтималдығы өте жоғары. Әрине, біз сондай-ақ біреулер басады

деген үмітпен спам арқылы таратылатын жалаңаш атақты адамдардың бейнелеріне немесе қарақшылық бағдарламаларға сілтемелері бар әдеттегі арандатушылық хабарламаларды көреміз [5].

Достар. Әлеуметтік желілердегі «достармен» сенімді қарым-қатынас әдетте бейтаныс адамдарға қарағанда күштірек. Бір жағынан, бұл оңды, өйткені ол бизнес, бренд немесе жеке тұлғаның айналасында адал аудитория жасайды. Бірақ екінші жағынан, бұл да алаяқтарға есік ашады.

Достарды тұлғаландыру. Әлеуметтік желілердегі жалған дос профильдерінің мәселесі. Мұндай желілерде пайдаланушылардың сенімін оятатын достардың атынан хабарламалар жіберілетін жағдай жиі кездеседі. Бұл туа біткен сенім мен табиғи қызығушылық пайдаланушылардың зиянды сілтемелерді басу ықтималдығын арттырады, бұл құпия сөзді ұрлау тактикасын әсіресе тиімді етеді. Бұл жаңарту хабарлары көбінесе тіркелгі құпия сөздерін ұрлау үшін басқа жалған сайттарға апаратын сілтемелерді қамтиды.

Адамды алмастыру немесе маскарад жасау мүмкіндігі. Достардың атын жамылған әрекеттердің артында кім тұрғаны немесе әлеуметтік желі профилінде достарының суреттерін кім пайдаланып жатқаны жиі белгісіз. Жіберуші туралы ақпаратты оның IP мекенжайы бойынша жинауға болатын электрондық поштадан айырмашылығы, бұл әлеуметтік желілерде жұмыс істемейді. Мұндай маскарадтар жеке деңгейде де, корпоративтік деңгейде де болуы мүмкін. Мұндай алдау фишингке, теріс пиар-науқандарға немесе «анти-PRға» әкелуі мүмкін. Компаниялар атынан веб-сайттарды жасау түпнұсқа брендтер үшін шатасулар мен проблемаларды тудырған жағдайлар болды.

Құпия сөзді ұрлау және фишинг. Құпия сөздерді пайдаланатын әлеуметтік желілерге кіру таңбалардың белгілі бір комбинациясын білуді талап етеді. Мұндай рұқсат алғаннан кейін жарнама жіберуге, басқа біреудің атынан ақпаратты жіберуге немесе басқаларды қажетсіз әрекеттерге, соның ішінде зиянды сілтемелерді таратуға, зиянды бағдарламаны белсендіруге немесе басқа, кейде заңсыз әрекеттерге көндіруге болады. Кейбір ұйымдар өнімдерді жылжыту үшін әлеуметтік желіні пайдаланады және әкімші құпия сөздерін жоғалту топты бақылауды жоғалтуға әкелуі мүмкін. Құпия ақпаратты алу үшін фишинг әдістері, жалған веб-сайттар жасау, әлеуметтік инженерия және басқа әдістер жиі қолданылады. Мұндай қауіптерден қорғау деректердің жоғалуын болдырмау (DLP) жүйелерін және антивирустық бағдарламаларға біріктірілген репутация технологияларын қамтиды.

URL қысқарту қызметтерін пайдалану. URL қысқарту қызметтері соңғы уақытта танымал бола бастады, себебі олар қысқа сілтеме астында нақты веб-сайт мекенжайын жасыруға мүмкіндік береді, бұл пайдаланушыны басқа доменге тиімді бағыттайды. Бұл тәуекелдермен белсенді түрде күресуде, URL қысқарту қызметтері спам және басқа қауіптерді анықтаудың озық әдістерін енгізеді. Дегенмен, әлеуметтік желілерді пайдаланушылар үшін қауіп әлі де бар: бұзылған белгілі контактілерден келетін тартымды хабарлар мен ұсыныстар жиі зиянды бағдарламаны жүктеп алуға немесе қажетсіз веб-беттерге әкеледі.

Веб-шабуыл. Хакерлер әлеуметтік желілерді веб-шолғыштардағы осалдықтарды пайдалану, сондай-ақ XSS/CSRF шабуылдарын жасау арқылы шабуылдар жасау үшін пайдалана алады. Осы мақсатта достар тізімі арқылы таралатын трояндық аттар, жалған антивирустар, әлеуметтік құрттар, зиянды JavaScript және HTML сценарийлері қолданылады және т.б. Бұл шабуылдардың негізгі мақсаты – әлеуметтік желі қолданушысының ақпараттық жүйесіне, жұмыс станциясына немесе құрылғысына ену және кейіннен оларды жұқтыру. Қорғауды қамтамасыз ету үшін әдетте нақты уақыт режимінде жұмыс істейтін және зиянды кодты жүктеуді блоктайтын антивирустық бағдарламалар қолданылады.

Ақпараттың шығуы және қызметкерлердің беделін түсіретін әрекеттер. Әлеуметтік желілер ұйымның құпия ақпаратын тарату және оның беделіне нұқсан келтіру құралы ретінде қызмет етуі мүмкін. Бұл әрекеттер басшылыққа қанағаттанбаған қызметкерлерден де, арнайы енгізілген инсайдерлерден де болуы мүмкін. Адамдар көбінесе әлеуметтік желіде кәсіби ортадағыдан басқаша әрекет етеді және арандатушылық немесе дөрекі сөздер компанияның беделіне нұқсан келтіруі мүмкін. Мұндай қауіптердің алдын алу үшін деректердің жоғалуын болдырмау (DLP) жүйелері және онлайн жарияланымдарды талдау құралдары қолданылады.

Advanced Persistent Threat (APT) шабуылы және әлеуметтік желілердегі қауіптер. Әлеуметтік желілер күрделі хакерлерге күрделі зиянды бағдарламаларды және әртүрлі бұзу әдістерін пайдалану мүмкіндігін бере отырып, ұйымдар мен олардың бөлімшелері үшін кіру

нүктелері немесе қауіп көздері ретінде әрекет ете алады. Бұл желілер жиі шабуылдаушылар үшін маңызды ақпарат көздеріне айналады. Lockheed Martin Cyber Kill Chain, Mandiant APT Attack Life Model және ISSP ThreatSCALE моделі сияқты танымал шабуыл әдістемелері компания мен оның қызметкерлері, олардың лауазымдары, контактілері мен мекенжайлары туралы деректерді жинау үшін бастапқы кезеңдерінде әлеуметтік желілерді пайдаланады. Бұл желілер «Барлау» кезеңіндегі негізгі құралдар болып табылады. Әлеуметтік желіні одан әрі пайдалану ThreatSCALE-ге «басып кіру», Cyber Kill Chain-ге «жеткізу» және Mandiant APT Model-ге «ену» кезеңдерін қамтиды, мұнда оларды зиянды мазмұнды жеткізу үшін пайдалануға болады, мысалы, зиянды сілтемелер немесе малициозды кодты құжаттар жіберу. Әлеуметтік желілердегі негізгі қауіптерге нәсілдік, ұлттық немесе діни араздықты қоздыратын материалдарды тарату, тоталитарлық секталарды насихаттау, терроризмді ақтау, кибер қорлау және қорқыту, сондай-ақ есірткіні танымал ету және тарату жатады.

Ұлттық қауіпсіздік органдарынан, мемлекеттік органдардан, экономиканың екі секторындағы кәсіпорындардан және жеке тұлғалардан сипатталған қауіптерден қорғау үшін келесі міндеттер орындалады:

- ақпараттық шабуылдарды анықтау: шабуыл көздерін және анықтау нүктелерінің стратегиялық орналасуын анықтау;
- ақпараттық шабуылдардың алдын алу: объектіге шабуыл жасау мен қорғаудың ықтимал шығындарын бағалау;
- әртүрлі әлеуметтік ақпараттық желілерді құру және жою;
- Шабуыл жасаушылардың, соның ішінде лаңкестердің желілерін және олардың зиянды әрекеттерін анықтау және қадағалау.

Виртуалды қауымдастықтардың ақпараттық-психологиялық ықпалымен күресудің келесі әдістерін анықтауға болады [6]:

- күшті шараларды қолдану: серверлерді жабу, интернет-трафикті бақылау;
- құқықтық және реттеу шаралары: виртуалды қауымдастықтың ұйымдастырушылары мен белсенді қатысушыларын қылмыстық жауапкершілікке тарту;
- интернетті шектеу және мазмұнды бақылау;
- әлеуметтік желілердегі белсенділікті қадағалау және талдау.

Осы тәсілдердің әрқайсысының оң және теріс жақтарын бағалап көрейік. Алғашқы екі тәсіл қысқа мерзімде пайдалы болып шықты, бірақ бірқатар шектеулерге тап болады: олар географиялық шекараларды жылдам кесіп өтетін және кез келген елдің заңдарының юрисдикциясына жатпайтын ақпаратты таратуды, жинауды, өңдеуді және пайдалануды бақылай алмайды; олар пайдаланушының анонимділігі мәселесіне тап болады; және электронды ақпаратты өзгерту оңай. Оның үстіне, сөз бостандығы басым демократиялық елдерде цензура жиі тиімсіз.

Әлеуметтік желіні талдау тапсырмалары

Әлеуметтік желіні талдау арқылы киберқауіптерді анықтау тақырыбын жалғастыра отырып, алдыңғы қатарлы аналитикалық әдістерді қолдануды атап өткен жөн. Бұл тәсілдің мысалы ретінде әлеуметтік желілердегі мәтіндік деректерден семантикалық қатынастарды алу үшін семантикалық талдауды және табиғи тілді өңдеуді қолдану болып табылады. Бұл әдістер ықтимал қауіптерді анықтауға ғана емес, сонымен қатар ықтимал кибершабуылдарды көрсетуі мүмкін пайдаланушының көңіл-күйін талдауға мүмкіндік береді.

Әлеуметтік желі аналитикасының тиімділігі қауіп-қатердің жан-жақты бейнесін жасау үшін әртүрлі платформалардағы деректер біріктірілген кросс-платформалық ынтымақтастық арқылы жақсарады. Бұл қауіпсіздік жүйелеріне жаңа және дамып келе жатқан қауіптерге тезірек жауап беруге мүмкіндік береді, сонымен қатар жаһандық ауқымда қорғауды жақсарту үшін пайдалануға болатын жалпыға қолжетімді киберқауіптердің дерекқорларын жасауға көмектеседі.

Желілік қауымдастықтарды анықтау және талдау. Желідегі қауымдастықтар олардың мүшелері арасында көптеген қарым-қатынастардың болуымен және басқа желі қатысушыларымен айтарлықтай аз байланыстармен анықталады. Қарапайым қауымдастықтың мысалы ретінде барлық мүшелер бір-бірімен байланысқан және желінің сыртқы мүшелері қауымдастық мүшелерімен әрекеттеспейтін клика болып табылады. Айқын және жасырын қауымдастықтарды анықтау желіні талдаудың негізгі міндеті болып табылады.

Бұған қауымдастық мүшелерін жіктеу және біртекті топтарды, көшбасшыларды немесе сарапшыларды анықтау кіреді [7]. Қауымдастықты анықтау көбінесе кластерлеуді білдіреді, бұл әртүрлі әлеуметтік желілер контекстіндегі дәстүрлі Data Mining тапсырмасы. Қауымдастықтарды талдау арқылы мақсатты топтарды анықтау әдістері ақпараттық әсер мен басқаруды зерттеудің математикалық үлгілерін жасауға мүмкіндік береді [8].

Желілік құрылымдардағы мамандарды анықтау. Әлеуметтік желілер белгілі бір саладағы сарапшыларды іздеу құралы бола алады. Сарапшыларды анықтау процесі сенім деңгейін анықтау және ықпалды бөлу, сондай-ақ желідегі ақпаратты таратумен байланысты тапсырмаларды қамтиды. Сараптамалық ықпалдың таралуы тұрғысынан ол транзитивтік: әсер бір түйіннен екіншісіне ауысады, процеске тартылған сарапшылардың әрбір жаңа түйінімен әлсірейді [9].

Уақыт бойынша әлеуметтік желілердегі өзгерістер динамикасы. Уақыт өте келе әлеуметтік желілерде әртүрлі өзгерістер орын алады: жаңа қатысушылар пайда болады, кейбіреулері әрекетін тоқтатады, жаңа байланыстар қалыптасады, қатысушылардың өзара әрекеттесуінің болмауына байланысты ескілері өзектілігін жоғалтады. Бұл өзгерістер әлеуметтік желілердің жалпы құрылымына және әсіресе жеке қауымдастықтарға әсер етеді. Негізгі сұрақтар жетекші әлеуметтік желі қауымдастықтарындағы ұзақ мерзімді өзгерістер, қауымдастықтар уақыт өте келе қалай дамитындығы және болашақ өзгерістерді қалай анықтау және қадағалау туралы туындайды. Желілік графиктердің эволюциясын модельдеу және желілерді құрудың әртүрлі стратегияларын зерттеу маңызды рөл атқарады [10].

Әлеуметтік желілерде жаңа байланыстардың пайда болуын болжау. Болашақта пайдаланушылар немесе топтар арасындағы ықтимал байланыстарды анықтауға және болжауға бағытталған зерттеулер әлеуметтік желіні талдау үшін өте маңызды. Желі қосылымдары уақыт өте өзгереді. Желі құрылымы мен мүше сипаттамалары туралы ақпаратты пайдалану жаңа қосылымдарды болжауға көмектеседі. Болжаудың міндеті - белгілі бір уақыт кезеңінен кейін екі қатысушы арасында байланысты орнату ықтималдығын анықтау. Бұл әлеуметтік желінің эволюциясын зерттеуге байланысты және сілтемелерді болжау мәселесі ретінде белгілі есептеу мәселесі. Бұл мәселені шешу үшін ортақ достардың саны, қатысушылар арасындағы ең қысқа жол, жеке түйіндердің әсері және желіде алғаш пайда болу уақыты сияқты сипаттарды ескере отырып, әлеуметтік желінің эволюциясын автоматтандырылған модельдеу қолданылады. Бұл мәселені шешу әртүрлі құрылымдық және қатынастық модельдерді құруды қамтиды. Болжаудың дәлдігін жақсарту үшін пайдаланушылардың жеке деректерін біріктіретін машиналық оқытуға негізделген қарым-қатынасты болжау үлгілері қолданылады [11].

Жасанды интеллект әлеуметтік желілер арқылы киберқауіптерді анықтау процестерін автоматтандыруда маңызды рөл атқарады. AI алгоритмдері кибершабуылдарды немесе алаяқтықты көрсете алатын әдеттен тыс мінез-құлық немесе коммуникация үлгілерін анықтай отырып, деректердің үлкен көлемін жылдам талдай алады. Алгоритмдерді үнемі үйрену және жаңа қауіптерге бейімдеу олардың тиімділігі мен дәлдігін арттырады.

Техникалық шешімдерден басқа, пайдаланушыларды оқыту киберқауіптерді анықтау және алдын алуда маңызды рөл атқарады. Киберқауіптердің түрлері және олардың әлеуметтік желілерде ұсынылуы туралы хабардар болуды арттыру шабуылдарды ертерек анықтауға және алдын алуға әкеледі. Кибергигиенаны жақсарту үшін жұртшылықпен және ұйымдармен жұмыс істеу кибершабуылдардан болатын қауіптерді айтарлықтай азайтуға және ықтимал зиянды азайтуға болады.

Қорытындылай келе, біздің шолуымыз әлеуметтік желілерді талдауды пайдалану киберқауіптерді анықтау және оларға қарсы тұрудың перспективалы тәсілі болып табылатынын көрсетеді. Әлеуметтік желі аналитикасы пайдаланушының мінез-құлық үлгілерін анықтап, талдап қана қоймай, сонымен қатар фишинг, зиянды бағдарламаларды тарату немесе келісілген шабуылдар сияқты кибершабуылдарды көрсете алатын ауытқуларды анықтай алады.

Әлеуметтік желіні талдау әдістері, мысалы, тіркелгілер арасындағы байланыс үлгілерін зерттеу, жазбалар мазмұнын және пайдаланушылар арасындағы өзара әрекеттестіктерді талдау күдікті әрекеттерді анықтауда тиімді екенін көрсетті. Бұл киберқауіптердің таралуына қатысы болуы мүмкін жасырын топтарды анықтауды, сондай-ақ қауіптер таралатын желілік құрылымдардағы негізгі түйіндерді анықтауды қамтиды.

Дегенмен, әлеуметтік желілерден ақпаратты жинау және талдау кезінде деректердің құпиялылығын қамтамасыз ету, сондай-ақ дәлдікті арттыру және жалған позитивтерді азайту үшін алгоритмдерді жетілдіру қажеттілігі сияқты белгілі бір қиындықтар да бар.

Болашақ нәтижелерді жақсарту үшін әлеуметтік желіні талдауды киберқауіпсіздіктің басқа әдістерімен біріктіру, білім мен тәжірибе алмасу үшін халықаралық ынтымақтастықты дамыту және киберқауіптерді анықтау процестерін автоматтандыру және оңтайландыру үшін жаңа технологиялық шешімдерді жасау маңызды.

Бұл саладағы зерттеулер үнемі өзгеріп отыратын қауіп үлгілері мен технологияларына сай болу үшін әлеуметтік желіні талдау әдістерін бейімдеуді және жетілдіруді жалғастыруы керек. Бұл киберқауіптерге тиімді қарсы тұрудың және өзара байланысы артып келе жатқан әлемде цифрлық кеңістікті қорғаудың жалғыз жолы.

Әдебиеттер тізімі

1. Carley K. Destabilizing networks. / K. Carley, J. Lee, D. Krackhardt // Connections. – 2002. – Vol. 24, №3. – P.79-92.
2. Додонов О.Г. Інформаційні потоки в глобальних комп'ютерних мережах / О.Г. Додонов, Д.В. Ланде, В.Г. Путятін. – Київ: Наукова думка, 2009. – 295 с.
3. Stohl C. Networks of Terror: Theoretical Assumptions and Pragmatic Consequences / C. Stohl, M. Stohl // Communication Theory. – 2007. – Vol. 17. – P. 93-124.
4. Russell M.A. Mining the Social Web: Analyzing Data from Facebook,Twitter, LinkedIn, and Other Social Media Sites / M.A. Russell. – O'Reilly, 2011. – 332 p.
5. Easley D. Networks, Crowds, and Markets: Reasoning about a Highly Connected World, Cambridge University Press / D. Easley, J. Kleinberg. – 2010. – 819 p.
6. Гриненко І. Вплив віртуальних спільнот на інформаційну безпеку: сучасний стан та тенденції розвитку. / І. Гриненко, Д. Прокофьєва-Янчиленко // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2012. – № 1(23). – С. 18-23.
7. Coscia M. A classification for community discovery methods in complex networks. / M. Coscia, F. Giannotti, D. Pedreschi // Statistical Analysis and Data Mining. – 2011. – P. 512-546.
8. Губанов Д. Социальные сети: модели информационного влияния, управления и противоборства / Д. Губанов, Д. Новиков, А. Чартишвили. – Москва, 2010. – 225 с.
9. Бузун Н. Выявление пересекающихся сообществ в социальных сетях / Н. Бузун, А. Коршунов. – М.: Институт системного программирования РАН, 2012. – 18 с.
10. Укустов С.С. Подход к решению задачи идентификации влиятельных разработчиков в социальной сети гитхаб / С.С. Укустов, А.Г. Кравец // Известия Волгоградского государственного технического университета. – 2012. – № 15(102). – С. 61-66.
11. Liben-Nowell D. The Link Prediction Problem for Social Networks / D. Liben-Nowell, J. Kleinberg // Proceedings of the 12th International Conference on Information and Knowledge Management, N. Y.: ACM Press, 2003. – P. 556-559.

References

1. Carley K. Destabilizing networks. / K. Carley, J. Lee, D. Krackhardt // Connections. – 2002. – Vol. 24, № 3. – R. 79-92. (In English).
2. Dodonov O.G. Infopmatsiini potoki v global'nix komp'yutepnix mepezhax / O.G. Dodonov, D.V. Lande, V.G. Pytyatin. – Kiïv: Naykova dymka, 2009. – 295 c. (In Russian).
3. Stohl C. Networks of Terror: Theoretical Assumptions and Pragmatic Consequences / C. Stohl, M. Stohl // Communication Theory. – 2007. – Vol. 17. – R. 93-124. (In English).
4. Russell M.A. Mining the Social Web: Analyzing Data from Facebook,Twitter, LinkedIn, and Other Social Media Sites / M.A. Russell. – O'Reilly, 2011. – 332 p. (In English).
5. Easley D. Networks, Crowds, and Markets: Reasoning about a Highly Connected World, Cambridge University Press / D. Easley, J. Kleinberg. – 2010. – 819 p. (In English).
6. Gpinenko I. Vpliv viptyal'nix cpil'not na infopmatsiiny bezpeky: cychacnii ctan ta tendentsiï pozvitky. / I. Gpinenko, D. Ppokoґєva-Yanchilenko // Ppavove, nopmativne ta metpologichne zabezpechennya cictem zaxicty infopmatsiï v Ykpaïni. – 2012. – № 1(23). – C. 18-23. (In Ukrainian).
7. Coscia M. A classification for community discovery methods in complex networks. / M. Coscia, F. Giannotti, D. Pedreschi // Statistical Analysis and Data Mining. – 2011. – R. 512-546. (In English).

8. Gybanov D. Cotsial'nye ceti: modeli infopmatsionnogo vliyatiya, yppavleniya i ppotivobopctva / D. Gybanov, D. Novikov, A. CHaptishvili. – Mockva, 2010. – 225 c. (In Russian).
9. Byzyn N. Vyyavlenie pepecekayushchixcya coobshchectv v cotsial'nyx cetyax / N. Byzyn, A. Kopshynov. – M.: Inctityt cictemnogo ppogpammipovaniya PAN, 2012. – 18 c. (In Russian).
10. Ykyctov C.C. Podxod k pesheniyu zadachi identifikatsii vliyatel'nyx pazpabotchikov v cotsial'noi ceti gitxab / C.C. Ykyctov, A.G. Kpavets // Izvectiya Volgogpadckogo gocydapctvennogo texnicheckogo univepciteta. – 2012. – № 15(102). – S. 61-66. (In Russian).
11. Liben-Nowell D. The Link Prediction Problem for Social Networks / D. Liben-Nowell, J. Kleinberg // Proceedings of the 12th International Conference on Information and Knowledge Management, N. Y.: ACM Press, 2003. – R. 556-559. (In English).

A. Bimyrzakyzy*, Zh. Alimzhanova
Al-Farabi Kazakh National University,
050040, Republic of Kazakhstan, Almaty, Al-Farabi Avenue, 71
*e-mail: akerkebeimirzakizi@gmail.com.

IDENTIFYING CYBERTHREATS THROUGH SOCIAL MEDIA RESEARCH

The work provides an overview of the main methods of social network analysis used to identify cyber threats. The main types of threats in social networks are indicated and some protection methods for their prevention are described. Typical tasks of social network analysis aimed at detecting cyber threats are, for example, identifying online communities, identifying leaders and experts in communities, analyzing the stability of communities, clustering textual information, etc. With increasing digitization and active use of social networks as a means of communication, the importance of effective monitoring and data analysis to ensure cyber security is becoming more and more relevant. Complexities and challenges associated with processing large amounts of data in social networks are also analyzed, including privacy issues and ethical aspects of user data control. The study provides a holistic view of the use of social media as a tool to proactively identify and prevent cyberthreats, highlighting the importance of integrating analytical systems into the overall cybersecurity framework of organizations and individuals. The study provides a holistic view of the use of social media as a tool for proactive detection and prevention of cyber threats, highlighting the importance of integrating analytical systems into the overall cybersecurity posture of organizations and individuals, while emphasizing the need to improve machine learning and artificial intelligence techniques for deeper and more accurate analysis of user behavior and community dynamics, which can contribute to more effective prevention and neutralization of threats in the digital environment.

Key words: *social network analysis, phishing, cyber threats, leader detection techniques, information leakage, Advanced Persistent Threat (APT) attacks.*

А. Бимырзакызы*, Ж.А. Муратбековна
Казахский Национальный Университет имени аль-Фараби,
050040, Республика Казахстан, Алматы, проспект аль-Фараби, 71
*e-mail: akerkebeimirzakizi@gmail.com

ВЫЯВЛЕНИЕ КИБЕРУГРОЗ ПОСРЕДСТВОМ ИССЛЕДОВАНИЙ В СОЦИАЛЬНЫХ СЕТЯХ

В работе представлен обзор основных методов анализа социальных сетей, используемых для выявления киберугроз. Обозначены основные виды угроз в социальных сетях и описаны некоторые методы защиты от их предотвращения. Типичными задачами анализа социальных сетей, направленными на обнаружение киберугроз, являются, например, идентификация онлайн-сообществ, выявление лидеров и экспертов в сообществах, анализ стабильности сообществ, кластеризация текстовой информации и т.д. С ростом цифровизации и активным использованием социальных сетей в качестве средства коммуникации важность эффективного мониторинга и анализа данных для обеспечения кибербезопасности становится все более актуальной. Также анализируются сложности и проблемы, связанные с обработкой больших объемов данных в социальных сетях, включая вопросы конфиденциальности и этические аспекты контроля пользовательских данных. Исследование дает целостное представление об использовании социальных сетей в качестве инструмента для превентивного выявления и предотвращения киберугроз, подчеркивая важность интеграции аналитических систем в общую систему кибербезопасности организаций и отдельных лиц. Исследование дает целостное представление об использовании социальных сетей в качестве инструмента для превентивного выявления и предотвращения киберугроз, подчеркивая важность отдельных лиц, при этом акцентируется внимание на необходимости улучшения методов машинного обучения и искусственного интеллекта для более глубокого и точного анализа поведения пользователей и динамики

сообществ, что может способствовать более эффективному предотвращению и нейтрализации угроз в цифровой среде.

Ключевые слова: *анализ социальных сетей, фишинг, киберугрозы, методы обнаружения лидеров, утечка информации, атаки Advanced Persistent Threat (APT).*

Авторлар туралы мәліметтер

Ақерке Бимырзақызы* – «Ақпараттық жүйелер» кафедрасының магистранты; Әл-Фараби атындағы Қазақ ұлттық университеті; e-mail: akerkebeimirzakizi@gmail.com.

Жанна Муратбековна Алимжанова – физика-математика ғылымдарының кандидаты, профессор; Әл-Фараби атындағы Қазақ ұлттық университеті; e-mail: zhannamen@mail.ru.

Сведения об авторах

Акерке Бимырзакызы* – магистрант кафедры «Информационные системы»; Казахский национальный университет имени аль-Фараби; e-mail: akerkebeimirzakizi@gmail.com.

Жанна Муратбековна Алимжанова – кандидат физико-математических наук, профессор; Казахский национальный университет имени аль-Фараби; e-mail: zhannamen@mail.ru.

Information about the authors

Akerke Bimyrzakyzy* – Master's student of the department of Information systems; Al-Farabi Kazakh National University; e-mail: akerkebeimirzakizi@gmail.com.

Zhanna Muratbekovna Alimzhanova – candidate of physics and mathematics, professor; Al-Farabi Kazakh National University; e-mail: zhannamen@mail.ru.

Редакцияға енуі 24.04.2024
Өңдеуден кейін түсуі 02.09.2024
Жариялауға қабылданды 13.09.2024