Sosial Kiberfiziki Sistemlərdə Toplanmış Mətnlərdə Kiberkriminal İzlərin Aşkarlanması Üsulları

Araz Mustafa
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
araz.mmustafa@gmail.com

***Xülasə*— Müasir rəqəmsal dünyada sosial kiberfiziki sistemlər insanların gündəlik həyatının ayrılmaz hissəsinə çevrilmişdir. Bu sistemlərdə həm faydalı, həm də müxtəlif növ kiberkriminal fəaliyyətlər baş verir. Tədqiqat işində sosial kiberfiziki sistemlərdə toplanmış mətn məlumatlarının analizi əsasında fərdin rəqəmsal kimliyinin təyin edilməsi, müəllifliyinin tanınması və müəyyənləşdirilməsi məsələlərinə baxılmışdır. Kiberkriminal izlərin aşkarlanması məqsədilə fərdin yazı üslubu və ifadə tərzi xüsusiyyətləri araşdırılmış, müvafiq mətn təsnifatı üsulları təhlil edilmişdir. Məqalədə təklif olunan yanaşmanın kibertəhlükəsizlik, rəqəmsal kriminalistika və saxta profillərin aşkarlanması sahələrindəki tətbiqi imkanları qiymətləndirilir.**

Açar sözlər*— *sosial kiberfiziki sistemlər; müəllif tanıma; kiberkriminalistika; mətn analizi; saxta profil aşkarlanması; maşın təlimi

I. GİRİŞ

Sosial kiberfiziki sistemlər (SKFS) - fiziki mühit, informasiya-kommunikasiya texnologiyaları və insan amilinin qarşılıqlı inteqrasiyası nəticəsində formalaşan kompleks ekosistemdir. Müasir dövrdə sosial şəbəkələr, onlayn forumlar, ani mesajlaşma platformaları və e-ticarət sistemləri bu ekosistemin əsas struktur komponentləri hesab olunur. Genişmiqyaslı rəqəmsallaşma şəraitində SKFS-də hər gün müxtəlif xüsusiyyətlərə malik mətn məlumatları toplanır, ötürülür və emal olunur [1].

SKFS-in təqdim etdiyi geniş kommunikasiya imkanları, eyni zamanda, kiberbullinq, fişinq, dezinformasiya manipulyasiyası, maliyyə fırıldaqçılığı, istifadəçi profillərinin qanunsuz ələ keçirilməsi və saxta hesabların yaradılması kimi kibercinayətkarlıq xarakterli fəaliyyətlər üçün də əlverişli mühit formalaşdırır. Virtual mühitdə anonimlik prinsipinin mövcudluğu və rəqəmsal kimliyin asanlıqla manipulyasiya edilməsi kiberkriminalistika sahəsində ciddi çağırışlar və problemlər yaradır. Məhz bu xarakterik təhdidlərin qarşısının alınması üçün mətn məlumatlarının intellektual analizi vasitəsilə fərdin rəqəmsal izinin müəyyən edilməsi və müəllifliyin identifikasiyası (tanınması) məsələsi xüsusi əhəmiyyət kəsb edir [2].

Qeyd olunan aktual problemlərin həllinə yönələn bu tədqiqat işində, SKFS mühitində toplanan mətnlərdə kiberkriminal izlərin aşkarlanması metodlarının analizi, müəllif identifikasiyası sahəsində mövcud yanaşmaların müqayisəli təhlili və saxta profillərin verifikasiyası məsələləri araşdırılmışdır.

II. SOSİAL KİBER FİZİKİ SİSTEMLƏRİN ARXİTEKTURASI

Müasir dövrdə texnoloji konvergensiya prosesləri ənənəvi kiberfiziki sistemlərin (KFS) təkamül edərək yeni bir mərhələyə - SKFS-ə keçidini şərtləndirmişdir. Klassik KFS hesablama resursları (kibermühit) ilə fiziki proseslərin (fiziki mühit) sensorlar və aktuatorlar vasitəsilə sıx inteqrasiyasına əsaslandığı halda, SKFS bu ekosistemə insan amilini və sosial şəbəkələri də daxil edərək üçölçülü bir platforma formalaşdırır. Burada insan həm idarəedici, həm məlumat istehsalçısı, həm də sistemin birbaşa təsir göstərdiyi subyekt rolunda çıxış edir.

SKFS struktur etibarilə 3 əsas təbəqədən təşkil olunur [3]:

- Fiziki təbəqə: Ağıllı şəhərlər, IoT (Əşyaların İnterneti) qurğuları, intellektual nəqliyyat sistemləri və fərdi sensor şəbəkələri.
- Kiber təbəqə: Məlumatların saxlanılması, bulud hesablamaları, şəbəkə protokolları və süni intellekt alqoritmləri.
- Sosial təbəqə: İnsanların rəqəmsal platformalardakı fəaliyyətləri, sosial şəbəkə interaksiyaları, rəylər, yazışmalarvə kollektiv davranış nümunələri.

Bu üç təbəqənin qarşılıqlı əlaqəsi nəticəsində nəhəng həcmdə müxtəlifcinsli məlumat axını formalaşır. SKFS-in ən spesifik xüsusiyyəti - sosial təbəqədən kiber və fiziki təbəqələrə ötürülən və əksər halda təbii dildə ifadə olunan strukturlaşdırılmamış mətn məlumatlarıdır. İnsanların rəqəmsal platformalarda buraxdığı bu mətn izləri bir tərəfdən sistemin funksionallığını artırsa da, digər tərəfdən kiberkriminallar üçün manipulyasiya və hücumların həyata keçirilməsi imkanı yaradır.

III. SKFS-DƏ KİBERKRİMİNAL İZLƏRİN XÜSUSİYYƏTLƏRİ VƏ TƏSNİFATI

SKFS-də kiberkriminal fəaliyyət ənənəvi kompüter cinayətlərindən kəskin şəkildə fərqlənir. Burada hücum hədəfi təkcə serverlər və ya proqram təminatı deyil, birbaşa insan psixologiyası, sosial rəy və kiberfiziki infrastrukturun idarəetmə qərarlarıdır. Bədniyyətlilər sosial platformalar vasitəsilə yaydıqları strukturlaşdırılmamış mətnlər (postlar, şərhlər, mesajlar) vasitəsilə spesifik kiberkriminal izlər qoyurlar. Bu izləri aşağıdakı kimi təsnif etmək mümkündür [4, 5]:

- Sosial mühəndislik və fişinq mətnləri: istifadəçilərin konfidensial məlumatlarını əldə etmək və ya kiberfiziki

DOI: 10.25045/forensic.gov.2026.50

sistemə qanunsuz giriş imkanı qazanmaq məqsədilə təbii dildə tərtib olunmuş manipulyativ və hədəflənmiş rəqəmsal mesajlar.

- Dezinformasiya və saxta xəbərlər: kollektiv davranışı manipulyasiya etmək, cəmiyyətdə xaos yaratmaq və ya kritik fiziki infrastruktura (məsələn, ağıllı enerji şəbəkələrinə, intellektual nəqliyyat sistemlərinə) qarşı sabotaj məqsədilə yayılan mətnlər.
- Radikalizm, ekstremizm və nifrət nitqi: müxtəlif sosial qruplar arasında qarşıdurma yaratmağa yönəlmiş, spesifik leksik-semantik struktura malik qanunsuz məzmunlar.
- Kiberbulinq və təhdid mətnləri: Fərdləri hədəf alan, psixoloji terror xarakterli və hüquqi məsuliyyət doğuran rəqəmsal izlər.

SKFS-də bu növ kiberkriminal izlərin aşkarlanmasını çətinləşdirən əsas amil onların qeyri-müəyyən, jarqonlarla, gizli kodlaşdırmalar və qısaltmalarla zəngin olmasıdır. Hücumçular çox vaxt standart filtrasiya sistemlərindən yayınmaq üçün qəsdən qrammatik qaydaları pozur və ya çoxdilli kod dəyişmələrindən (eyni cümlədə müxtəlif dillərin istifadəsi) istifadə edirlər.

Rəqəmsal kriminalistika sahəsində mətn məlumatlarının analizi üçün uzun illərdir müxtəlif metodlar tətbiq olunmaqdadır. Cədvəl 1-də mövcud yanaşmalar və onların məhdudiyyətləri göstərilmişdir [6].

CƏDVƏL 1. MƏTN ANALİZİ METODLARI VƏ ONLARIN MƏHDUDİYYƏTLƏRİ

Yanaşma	İşləmə prinsipi	Əsas məhdudiyyəti
İmza əsaslı (Signature-based) və lüğət metodları	Əvvəlcədən müəyyən edilmiş bədniyyətli sözlərin və nizamlı ifadələrin axtarışı	Yeni, modifikasiya olunmuş və lüğətdə olmayan təhdidləri aşkarlaya bilmir.
Qayda əsaslı ekspert sistemləri	Dilçilik qaydalarına, sintaktik şablonlara və formal qrammatikaya əsaslanan sistemlər	Dilin dinamik dəyişməsinə və qeyri-formal rəqəmsal jarqonlara qarşı çevik deyil
Klassik statistik metodlar	Sözlərin tezlik paylanması, cümlə uzunluğu kimi kəmiyyət göstəricilərinin analizi	Sözlərin mətndəki yerləşmə sırasını və kontekstual asılılıqları nəzərə almır

Ənənəvi metodların ən böyük çatışmazlığı kontekstual korluqdur. Məsələn: "*Bu platforma partladacaq*" cümləsi məcazi mənada (məsələn: bir layihənin uğuru haqqında) işlədilə bildiyi halda, digər bir kontekstdə real bir kiberfiziki terror təhdidi mənasında işlədilə bilər. Ənənəvi sistemlər bu iki fərqi ayırd etmək imkanına malik deyildir.

Digər tərəfdən SKFS-də böyük verilənlər mühitinin mövcudluğu məlumatların emal sürəti və müxtəlifliyi problemlərini ortaya çıxarır. Hər saniyə milyonlarla mətnin daxil olduğu bir sistemdə insan əməyinə və ya statik qaydalara əsaslanan sistemlərin real-vaxt rejimində kiberkriminal izləri aşkarlaması qeyri-mümkündür.

Bu səbəbdən SKFS-də təhlükəsizliyin təmin edilməsi, mətnlərin təkcə zahiri strukturunu deyil, onların dərin semantikasını, gizli müəlliflik üslubunu (stilometriya) və kontekstual əlaqələrini öyrənə bilən, özünü adaptasiya edən intellektual NLP (Təbii Dilin Emalı) və dərin təlim modellərinin tətbiqini qaçılmaz edir.

IV. MƏTN MƏLUMATLARINDA MÜƏLLİFLİYİN VƏ KİBERKRİMİNAL İZLƏRİNİN TƏYİNİ

İnformasiya texnologiyalarının dinamik inkişafı və qlobal şəbəkə infrastrukturunun transmilli miqyasda genişlənməsi, elektron poçt və sosial media platformaları başda olmaqla virtual kommunikasiya xidmətlərini müasir cəmiyyətin fundamental inteqrasiya mexanizminə çevirmişdir. Bu texnoloji resurslar istifadəçilər üçün genişmiqyaslı kommunikasiya kanalları açmaqla bərabər, eyni zamanda destruktiv məqsədlərlə sui-istifadə halları üçün yeni kibertəhdid vektorları formalaşdırır. Qlobal şəbəkə seqmentlərinin qanunsuz idarə olunması fərdlərin informasiya təhlükəsizliyinə xələl gətirməklə yanaşı, makro səviyyədə regional sabitliyə və milli təhlükəsizlik sisteminə birbaşa təhdid yarada bilər [7].

Məhz bu kontekstdə transmilli xarakter daşıyan kibertəhdidlərin qarşısının alınması mexanizmlərinin işlənilməsi müasir cəmiyyətin əsas prioritetlərindəndir. Belə bir şəraitdə SKFS-in təhlükəsizlik arxitekturasında kiberkriminal izlərin operativ aşkarlanması və analiz olunması mühüm əhəmiyyət kəsb edir. Lakin rəqəmsal ekosistemin özünəməxsus xüsusiyyətləri səbəbindən, bu sistemlərdə kiberkriminalistika analizlərinin aparılması və müəllifliyin identifikasiyası prosesində aşağıdakı struktur çətinliklər meydana çıxır [8]:

- Anonimlik və təxəllüslərin geniş istifadəsi – Kibercinayətkarlar identifikasiya məlumatlarını gizlətmək məqsədilə çoxsaylı saxta hesablardan istifadə edirlər.
- Mətn məlumatlarının böyük həcmli olması və sinifləndirilməməsi – İnformasiya axınının yüksək intensivliyi və ilkin olaraq sinifləndirilməməsi, verilənlərin emalında ənənəvi statistik və ekspertiza analiz üsullarının tətbiqini qeyri-effektiv edir.
- Çoxdilli mühit – İstifadəçilərin onlayn mühitdə eyni zamanda müxtəlif dillərdən, dialektlərdən, jarqonlardan və qarışıq qrammatik strukturlardan istifadə etməsi, müəllifliyin təyini üçün yaradılan analitik modellərin invariantlıq (dəyişməzlik) imkanlarını məhdudlaşdırır.
- Yazı üslubunun süni şəkildə dəyişdirilməsi – Bədniyyətli şəxslərin identifikasiya sistemlərindən yayınmaq üçün generativ süni intellekt alətlərindən, maşın tərcüməsi sistemlərindən və ya xüsusi proqram təminatlarından istifadə etməklə fərdi yazı üslubunu məqsədli şəkildə dəyişdirmələri.
- Real zaman rejimində monitorinq zəruriyyəti – Baş verə biləcək təhlükəsizlik insidentlərinə və destruktiv informasiya hücumlarına operativ reaksiya verilməsi üçün kiberkriminal izlərin real zaman rejimində aşkarlanması.

Qeyd olunan struktur çətinliklərin həlli üçün fərdin yazı üslubunun unikal invariantlarının — o cümlədən fərdi lüğət fondunun (leksika), morfoloji, sintaktik və semantik

göstəricilərinin identifikasiyasını təmin edən stilometrik analizlərin dərin təlim texnologiyaları ilə sintezi mühüm əhəmiyyət kəsb edir. Bu yanaşmaların vahid metodoloji platformada tətbiqi, SKFS mühitində reallaşdırılan kiberkriminal fəaliyyətlərin preventiv və operativ aşkarlanmasına, eləcə də anomal rəqəmsal profillərin müəllifliyinin yüksək dəqiqliklə tanınmasına həlledici imkanlar yaradacaqdır.

V. MÜƏLLİFLİK ANALİZİNİN NƏZƏRİ-METODOLOJİ ƏSASLARI

SKFS-də toplanmış strukturlaşdırılmamış mətnlərdə kiberkriminal izlərin identifikasiyası hər bir fərdin özünəməxsus yazı üslubuna malik olması elmi fərziyyəsinə əsaslanır. Akademik ədəbiyyatda "stilometriya" olaraq adlandırılan bu yanaşma, müəllifin şüuraltı olaraq mətndə buraxdığı dil və yazı vərdişlərinin riyazi və statistik metodlarla analizini nəzərdə tutur.

Kiberkriminal mühitdə bədniyyətlilər öz IP ünvanlarını, coğrafi mövqelərini və rəqəmsal kimliklərini VPN və ya anonim şəbəkələr vasitəsilə gizlədə bilsələr də, öz linqvistik kimliklərini, yəni yazı üslublarını manipulyasiya etmək rəqəmsal kriminalistika baxımından olduqca çətindir.

Stilometriya ədəbi və digər mətnlərdə müəllifin yazı üslubunu statistik metodlarla tədqiq edən dilçilik sahəsidir [9] və bu sahə tez-tez anonim və ya mübahisəli sənədlərə müəlliflik aid etmək üçün istifadə olunur. Bu fərziyyə hər bir müəllifin yazı üslubunun şüurlu manipulyasiya üçün əlçatmaz müəyyən xüsusiyyətlərə malik olduğuna əsaslanır. Stilometriya müəlliflik təhlilinin əsasını təşkil edir. Müəlliflik təhlilinə üç əsas yanaşma mövcuddur: müəlliflik mənsubiyyəti, müəlliflik xarakteristikası və plagiat aşkarlanması [10].

Müəlliflik mənsubiyyəti müəllifin məlum əsərləri ilə mübahisəli əsər arasındakı yazı üslubuna əsasən naməlum bir yazı əsərinin müəllifini müəyyən edir. Yazı üslubuna qeyri-adi diksiya, müəyyən sözlərin tezliyi, seçimi və defis vərdişləri daxildir [11]. Müəllifin yazı üslubu gender, təhsil və mədəni mənşə haqqında nəticələr çıxarmaqla onun profilini formalaşdırır. Plagiatın aşkarlanması zamanı mətnin və ya hər hansı bir hissəsinin plagiat olub-olmadığını müəyyən etmək üçün müəlliflərin kim olduğunu bilmədən iki və ya daha çox mətn arasındakı oxşarlıq dərəcəsini hesablamaq mümkündür.

Müəllifliyin identifikasiyası və rəqəmsal şəxsiyyətin verifikasiyası məsələləri uzunmüddətli tədqiqat tarixinə malik olsa da, SKFS-in spesifik strukturu və dinamik mühiti bu sahədə tamamilə yeni, adaptiv yanaşmaların tətbiqini şərtləndirir. Təkamül ssenarilərinin davamı olaraq, Stamatatos müəllifliyin təyini üsullarını leksik, simvol səviyyəli (character-level), sintaktik, semantik və tətbiqi xüsusiyyətlər üzrə sistemləşdirərək metodoloji təsnifat strukturunu formalaşdırmışdır [12]. Digər tərəfdən, Koppel və həmkarları qısaölçülü mətn massivlərində - xüsusilə sosial şəbəkə paylaşımlarında - müəllif tanıma probleminə həsr edilmiş tədqiqatlarında, stilometrik xüsusiyyətlərin seyrəkliyi şəraitində ansambl təlimi metodlarının riyazi və struktur üstünlüklərini əsaslandırmışlar [13].

Kamil Ayda-zadə və həmkarları tərəfindən mətnlərin analizi, morfoloji seqmentasiya və tanıma sistemlərinin riyazi əsaslarının işlənilməsi istiqamətindəki fundamental tədqiqatlar aparılmış və yanaşmalar təklif edilmişdir [14].

Bu təkamülün son onillikdəki mərhələsini təşkil edən dərin təlim əsaslı yanaşmalar - xüsusilə BERT, RoBERTa, GPT və onların törəmələri olan neyron şəbəkə arxitekturaları - mətnlərin intellektual təsnifatı və müəllifliyin avtomatik identifikasiyası məsələlərində yüksək dəqiqlik nümayiş etdirməkdədir. Beynəlxalq təcrübədə əldə olunan bu yüksək nailiyyətlərə rəğmən Azərbaycan dili kontekstində kiberkriminalistika məqsədləri üçün müəllifliyin təyini istiqamətində aparılan tədqiqatlar olduqca məhdud xarakter daşıyır. Məhz bu səbəbdən milli dil korpusunun linqvistik-statistik xüsusiyyətləri əsasında müasir maşın təlimi və dərin neyron şəbəkəsi modellərinin adaptasiyası və SKFS təhlükəsizliyinə uyğunlaşdırılması müasir dövrün ən aktual elmi-praktiki istiqamətlərindən biri kimi qarşıda durmaqdadır [15].

Müəllifin müəyyənləşdirilməsi prosesinin etibarlılığı, ilk növbədə, SKFS-də toplanan mətnlərin keyfiyyətindən, həcmindən və müxtəlifliyindən asılıdır. Toplanmış mətn korpusu yalnız xam məlumat anbarı kimi deyil, hər bir müəllifin fərdi yazı üslubunu əks etdirən rəqəmsal bir "barmaq izi" mənbəyi kimi nəzərdən keçirilir. Bu səbəbdən mətnlərin xüsusiyyətlərinin sistemli şəkildə təsnif edilməsi və ölçülə bilən parametrlərə çevrilməsi tədqiqatın əsas mərhələlərindən birini təşkil edir.

Müəlliflik təhlilində əsas fərziyyə ondan ibarətdir ki, hər bir fərdin dilindən istifadə tərzi nisbətən sabit və təkrarlanan qanunauyğunluqlara malikdir. İnsan mətn yazarkən şüurlu olaraq mövzunu seçsə də, sözlərin uzunluğu, durğu işarələrindən istifadə tezliyi, funksional sözlərin paylanması və cümlə qurma vərdişləri kimi bir çox parametr şüuraltı və avtomatik şəkildə formalaşır. Məhz bu qeyri-ixtiyari elementlər mətnin mövzusundan asılı olmayaraq sabit qaldığı üçün müəllifi fərqləndirən ən etibarlı göstəricilər sayılır.

SKFS-də toplanan mətnlər təhlil olunarkən bu sabit göstəricilər müxtəlif səviyyələrə görə qruplaşdırılır. Belə bir təsnifat həm təhlilin sistemliliyini təmin edir, həm də müxtəlif xüsusiyyətlərin müəllif identifikasiyasına verdiyi töhfəni ayrı-ayrılıqda qiymətləndirməyə imkan verir. Bu yanaşma çərçivəsində mətnlər leksik (söz səviyyəsi), sintaktik (cümlə quruluşu), struktur (mətnin ümumi təşkili) və üslubi (fərdi ifadə tərzi) baxımdan araşdırılır. Aşağıda müəllifin rəqəmsal izini formalaşdıran bu xüsusiyyətlər kateqoriyalar üzrə ətraflı qeyd olunmuşdur.

Müəllifin mətnlərdəki rəqəmsal izini formalaşdıran xüsusiyyətlər aşağıdakı kateqoriyalara bölünür [16]:

a) Leksik xüsusiyyətlər: Leksik xüsusiyyətlər söz tezliyi və lüğət bazası, orta söz uzunluğu və hecaların sayı, ən çox istifadə olunan funksional sözlər, çox nadir və ya arxaik sözlərin istifadəsi ilə səciyyələndirilir.

b) Simvol səviyyəli xüsusiyyətlər: n-qram modelləri (xüsusilə karakter 3-qramları və 4-qramları); Durğu işarələrinin istifadə tezliyi; Böyük və kiçik hərflərin nisbəti; İfadə və ya digər xüsusi simvolların istifadəsi.

c) Sintaktik xüsusiyyətlər: Cümlə uzunluğu və mürəkkəbliyi; Nitq hissələrinin istifadə forması; Cümlədəki

sözlər və söz birləşmələri arasındakı tabelilik əlaqələri; Bağlayıcı və köməkçi nitq hissələrinin istifadə tezliyi.

d) Semantik və praqmatik xüsusiyyətlər: Mövzu modelləşdirilməsi; Sentiment və emosional ton; Söz daxilolma vektorları; Diskurs markerlərinin istifadəsi.

Çıxarılmış xüsusiyyətlər əsasında müəllifin müəyyənləşdirilməsi üçün aşağıdakı təsnifat alqoritmlərinin tətbiqi nəzərdə tutula bilər:

- Klassik maşın təlimi alqoritmləri: Dəstək Vektor Maşını (SVM), Naive Bayes, Random Forest, Logistic Regression, k-Nearest Neighbors (k-NN).
- Ansambl üsulları: Gradient Boosting (XGBoost, LightGBM), Stacking, Voting Classifier.
- Dərin öyrənmə modelləri: Konvolyusiya neyron şəbəkələri (CNN), Uzun Qısamüddətli Yaddaş şəbəkələri (LSTM), Bidirectional LSTM, Transformer əsaslı modellər (BERT, RoBERTa, DistilBERT).
- Hibrid yanaşmalar: Stilometrik xüsusiyyətlərin neyron şəbəkə embeddingləri ilə birləşdirilməsi.

VI. Saxta Profillərin Aşkarlanması və Tətbiq Sahələri

Hazırda bir çox ölkələr kibercinayətkarlıq ilə bağlı qanun və qaydalar hazırlayıblar. Lakin bir çox iş məhkəməyə verilə bilmir, çünki məhkəmədə zəruri və effektiv sübutlar mövcud deyil. İnternetin anonim təbiəti müəllifliyi müəyyən etməkdə çətinlik yaradır. Buna görə də effektiv sübutlar toplamaq üçün veb məzmunun texniki metodla təhlili vacibdir. Eyni zamanda müəlliflik təhlili üsullarından istifadə etməklə statistik metodlar vasitəsilə ədəbi əsərlərin müəlliflərini təhlil etmək olar. Müəlliflik təhlili üsulları veb məlumatlarının ədəbi əsərlərdən fərqləndiyini müəyyən edir. Müəllifin yazı tərzini təmsil edən geniş xüsusiyyətlərin çıxarılması və öyrənilməsi mühüm əhəmiyyət kəsb edir.

Saxta profillərin aşkarlanması müəllif tanıma metodologiyasının xüsusi tətbiq sahəsidir. Bu zaman məqsəd iki və ya daha çox hesabın eyni şəxs tərəfindən idarə olunub-olunmadığını müəyyən etməkdir. Aşağıda qeyd edilənlər bu istiqamətdə nəticə əldə etmək üçün effektiv göstəricilərdir:

- Yazı üslubunun uyğunluq dərəcəsi;
- Aktivlik vaxt nümunələri;
- Şəbəkə qarşılıqlı əlaqələrinin strukturu;
- Cihaz və brauzer barmaq izi;
- Davranış biometrikası – yazma sürəti, düzəliş nümunələri.
- Mətn əsaslı göstəricilərin digər metadata ilə birləşdirilməsi saxta profil aşkarlanmasında daha yüksək dəqiqlik təmin edir.

Təqdim olunan metodologiyalar müxtəlif istiqamətlərdə tətbiq oluna bilər. Bunlardan bəziləri aşağıda qeyd edilmişdir:

- Kibertəhlükəsizlik və hadisələrin idarə olunması – şübhəli fəaliyyətin erkən aşkarlanması və kiberhücumların müəlliflərinin müəyyənləşdirilməsi.
- Rəqəmsal kriminalistika – cinayət işlərində elektron sübutların təhlili və ekspert rəylərinin verilməsi.
- Saxta xəbərlərə qarşı mübarizə – dezinformasiya kampaniyalarının arxasında dayanan koordinasiyalı şəbəkələrin aşkarlanması.
- Korporativ təhlükəsizlik – daxili təhlükələrin və məlumat sızmasının izlənməsi.
- Akademik dürüstlüyün təmin edilməsi – plagiat və süni intellektlə generasiya olunmuş mətnlərin aşkarlanması.
- Sosial media platformalarının idarə edilməsi zamanı – bot şəbəkələrinin və saxta hesabların avtomatik müəyyənləşdirilməsi.

Nəticə

SKFS-in dinamik inkişafı və cəmiyyətin bütün sferalarına nüfuz etməsi, rəqəmsal platformalarda toplanan strukturlaşdırılmamış mətn verilənlərinin təhlükəsizlik nöqteyi-nəzərindən intellektual analizini qaçılmaz bir zərurətə çevirmişdir. Təqdim olunan tədqiqat işində SKFS mühitində yaranan kiberkriminal təhdidlər qruplaşdırılmış, ənənəvi rəqəmsal kriminalistika metodlarının kontekstual məhdudiyyətləri əsaslandırılmış və bu problemlərin aradan qaldırılması üçün stilometrik analizlərlə müasir maşın təlimi metodları analiz edilmişdir. Müəllifliyin rəqəmsal kimliyinin yüksək dəqiqliklə müəyyənləşdirilməsi üçün leksik, simvol səviyyəli, sintaktik və semantik xüsusiyyətləri təhlil edilmişdir.

Kibertəhlükəsizlik insidentlərinin idarə edilməsi, rəqəmsal kriminalistika ekspertizası, saxta profillərin və bot şəbəkələrinin aşkarlanması, eləcə də dezinformasiya kampaniyalarına qarşı mübarizə kimi strateji sahələrdə geniş tətbiq potensialına malik olduğu qeyd edilmişdir.

Ədəbiyyat

[1] R. Alguliyev, Y. Imamverdiyev, L. Sukhostat, "Cyberphysical systems and their security issues," Computers in Industry, vol. 100, pp. 212-223, 2018. doi: 10.1016/j.compind.2018.04.017.

[2] R. Zheng, J Li., H. Chen, Z. Huang, A framework for authorship identification of online messages: Writing-style features and classification techniques. Journal of the American Society for Information Science and Technology, 57: 378-393. 2006. https://doi.org/10.1002/asi.20316

[3] A.M. Mustafa, Analysis of Sources of Personal Data Formation in Cyber-Physical Social Systems. IEEE 17th International Conference on Application of Information and Communication Technologies (AICT). 1-4., 2023

[4] R.M.?liquliyev, Y.N.?mamverdiyev, R.?.Mahmudov, "?nformasiya t?hlük?sizliyi milli t?hlük?sizliyin mühüm komponenti kimi", ?nformasiya C?miyy?ti probleml?ri, ?1, pp.3-25, 2020

[5] R. M. ?liquliyev,Y. N. Imamverdiyev, ?nformasiya t?hlük?sizliyi insidentl?ri. Bak?: ?nformasiya Texnologiyalar?, 2012, 219 s.

[6] Rocha, W. J. Scheirer, C. W. Forstall et al., "Authorship attribution for social media forensics," IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 5-33, 2017.

[7] Y. Zhou, F. R. Yu, , J. Chen, ,Y. Kuo, "Cyber-physical-social systems: A state-of-the-art survey, challenges and opportunities," IEEE

Communications Surveys & Tutorials, 22(1), 389-425. 2019. 10.1109/COMST.2019.2959013

[8] E.A. Lee, S.A. Seshi, "Introduction to Embedded Systems - A Cyber-Physical Systems Approach". Second Edition, MIT Press., 2017

[9] T. Neal, K. Sundararajan, A. Fatima, Y. Yan, Y. Xiang, D. Woodard, "Surveying stylometry techniques and applications," ACM Computing Surveys, vol. 50, no. 6, pp. 1-36, 2018.

[10] Devlin, M.-W. Chang, K. Lee, K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," in Proc. NAACL-HLT, pp. 4171-4186, 2019

[11] Ferrara, O. Varol, C. Davis, F. Menczer, A. Flammini, "The rise of social bots," Communications of the ACM, vol. 59, no. 7, pp. 96-104, 2016.

[12] Stamatatos, "A Survey of Modern Authorship Attribution Methods," Journal of the American Society for Information Science and Technology, 60: 538-556. 2008 https://doi.org/10.1002/asi.21001

[13] M. Koppel, J. Schle, S. Argamon, "Authorship attribution in the wild," Language Resources and Evaluation, vol. 45, no. 1, pp. 83-94, 2011.

[14] R.Ayda-zade, S. G.Talibov, "?nalysis of The Methods for the Authorship Identification of the Text in the Azerbaijani Language," Problems of Information Technology, ?1, 14-23, 2017. DOI: 10.25045/jpit.v08.i1.02

[15] M. Fabien M, E. Villatoro-Tello, P. Motlicek, S. Parida, "BertAA: BERT fine-tuning for Authorship Attribution," in Proc. ICON, pp. 127-137, 2020

[16] D.Irani, S.Webb, K.Li, C.Pu, "Modeling Unintended Personal-Information Leakage from Multiple Online Social Networks", IEEE Internet Computing, 15(3), 13-19. 2011.

Methods for Detecting Cybercriminal Traces in Texts Collected from Social Cyber-Physical Systems

Araz Mustafa
Institute of Information Technology, Baku, Azerbaijan
araz.mmustafa@gmail.com

Abstract- In the modern digital world, social cyber-physical systems have become an integral part of everyday life. Both legitimate actions and various cybercriminal activities occur within these environments. This study examines the challenges of establishing a user's digital identity, as well as authorship recognition and attribution based on the analysis of text data collected from social cyber-physical systems. To detect cybercriminal traces, the characteristics of an author's writing style and linguistic patterns were investigated, alongside an analysis of relevant text classification methods. The article evaluates the applicability of the proposed approach within the fields of cybersecurity, digital forensics, and fake profile detection.

Keywords- social cyber-physical systems; authorship attribution; digital forensics, text analysis; fake profile detection; machine learning.