Uşaqlara Yönələn Kibercinayətlərin Rəqəmsal Ekspertizası Problemləri və Həlli Yolları

Tofiq Kazımov[1], Sabirə Ocaqverdiyeva[2]
[1,2]İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*tofig@mail.ru*,[2]*allahverdiyevasabira@gmail.com*

Xülasə **- Rəqəmsal platformaların inkişafı və ağıllı cihazların sürətlə yayılması uşaqların kibertəhdidlərə məruz qalma ehtimalını artırır. Məqalədə süni intellekt və mürəkkəb rəqəmsal şifrələmə üsullarının təsiri ilə daha da mürəkkəbləşən uşaqlara yönələn kibercinayətlərin araşdırılmasında rəqəmsal ekspertiza prosesində yaranan problemlər təhlil edilir. Təbii dil emalı və dərin təlim arxitekturaları əsasında yeni aşkarlama metodologiyası təklif olunur. Təklif olunan BERT (Bidirectional Encoder Representations from Transformers) modelinə əsaslanan və PAN-12 məlumat dəsti üzərində aparılan eksperimentlər cinayətkarların istifadə etdiyi mürəkkəb dil xüsusiyyətləri (manipulyasiya, gizli təhdidlər, izolyasiya cəhdləri) digər modellərlə müqayisədə daha yüksək dəqiqliklə aşkar etməyə imkan verir.**

Açar sözlər—rəqəmsal kriminalistika; uşaq təhlükəsizliyi; kibercinayətkarlıq; rəqəmsal sübut; BERT.

I. GİRİŞ

İnternetin geniş imkanları uşaq və yeniyetmələrə təhsil, əyləncə, sosiallaşma kimi faydalı resurslara çıxışı təmin edir [1, 2]. Lakin bununla yanaşı virtual məkanda onların təhlükəsiz və etibarlı fəaliyyət göstərməsi ilə əlaqəli bir sıra problemlər də (cinsi istismar, bulinq, fişinq və s.) mövcuddur. İnternet texnologiyalarının transmilli xarakteri, coğrafi məhdudiyyətlərin aradan qaldırılması və uşaqların rəqəmsal savadlılığının yetərli səviyyədə olmaması bu problemləri daha da kəskinləşdirir. Son dövrlərdə Sİ texnologiyalarından istifadə kibercinayətkarlığın sayının, intensivliyinin və mürəkkəbliyinin artmasına təsir edir və uşaqları yeni növ təhdidlərlə üz-üzə qoyur. Generativ süni intellektin yaranması isə bu problemi daha da dərinləşdirmişdir.

Kibercinayətkarlar sosial media platformaları üzərindən, şifrələnmiş mesajlaşma tətbiqləri, P2P (peer-to-peer) şəbəkələri və "dark web" mühitindən istifadə etməklə uşaq cinsi istismar materiallarını (UCİM) yayır, uşaq və yeniyetmələri hədəfə alan müxtəlif tərkibli cinayətlər törədirlər [3]. INHOPE (International Association of Internet Hotlines) təşkilatının məlumatına görə, 2025-ci ildə 3-13 yaş arası qurbanlar UCİM üzrə 91%-ni təşkil edir [4]. Uşaqların Minecraft, Roblox kimi onlayn oyunlara marağı və virtual icmalarda iştirak etməsi bu faktların sayını artırır [5]. Qeyd edilən rəqəmsal platformaların anonimlik xüsusiyyəti və geniş istifadəçi auditoriyasına malik olması cinayətkarlar üçün əlverişli və cəlbedici mühit formalaşdırır. Bu kimi platformalara artan maraq yalnız sosial xarakter daşımır, eyni zamanda maliyyə itkiləri ilə əlaqəli riskləri artırır, şəxsi məlumatların oğurlanmasına və müxtəlif üsullarla cinsi istismara da səbəb olur.

Rəqəmsal platformalar vasitəsilə uşaq və yeniyetmələrin manipulyasiyası, zərərli fəaliyyətlərə cəlb edilməsi onların psixoloji və sosial rifahına ciddi təhlükəsizlik riskləri yaradır. Qeyd olunan faktorlar rəqəmsal mühitdə ekspertiza problemlərinin aktual olduğunu bir daha təsdiq edir və uşaqlara yönələn kibercinayətlərin (UYK) aşkarlanması, rəqəmsal sübutların toplanması və təhlili üzrə yeni ekspertiza mexanizmlərinin işlənib hazırlanmasını və mövcud yanaşmaların təkmilləşdirilməsini zəruri edir.

Məqalədə uşaqlara yönəlmiş kibercinayətlərin təsnifatı təqdim olunur, rəqəmsal ekspertiza prosesinin əhəmiyyəti və bu sahədə mövcud problemlər təhlil edilir. Eyni zamanda, beynəlxalq aləmdə UYK-nin qarşısının alınmasına yönəlmiş yanaşmalar haqqında məlumat verilir, müvafiq elmi ədəbiyyat təhlil edilir. Bununla yanaşı, BERT modeli əsasında kibercinayətkar davranışın aşkarlanmasına dair bir yanaşma təklif edilir.

II. UŞAQLARA YÖNƏLMİŞ KİBERCİNAYƏTLƏRİN TƏSNİFATI

Uşaqlara qarşı törədilən kibercinayətlər əsasən kiberqruminq, kiberşantaj, UCİM-ın istehsalı və ya yayılması ilə əlaqəli hüquqazidd materiallarda öz əksini tapır.

Kiberqruminq – yetkin şəxslərin internet vasitəsilə uşaqla əlaqə qurması və uşağın inkişaf psixologiyasındakı boşluqlardan istifadə edərək, onun rəqəmsal etibarını qazandıqdan sonra manipulyasiya etməsi ilə əlaqəli davranışı özündə ehtiva edir. [6]. Kibercinayətkarlar saxta profillər yaradaraq özlərini uşağın həmyaşıdı kimi təqdim edirlər. Ünsiyyət ilkin mərhələdə kibercinayətkar və uşaq arasındakı tamamilə adi şəkildə davam edir. Lakin sonralar bu proses cinsi məzmunlu mesajlarla əvəz edilməklə daha da intensivləşir və uşaqda asılılıq yaradır.

UCİM-in istehsalı, yayılması və sintetik materialları. Son illərdə Sİ-nin təsiri ilə "Deepfake" texnologiyasından istifadə edərək sintetik UCİM-in yaradılması halları kəskin artmışdır. Belə məzmunu ənənəvi müdafiə sistemləri vasitəsilə analiz edilməsi artıq səmərəsizləşdirir. Kokolaki və Fragopoulou öz tədqiqatlarında göstərirlər ki, Sİ tərəfindən yaradılan belə məzmun mövcud heş-əsaslı aşkarlama sistemlərini asanlıqla keçə bilir [7] .

Kiberzorakılıq və şantaj, uşaqların rəqəmsal platformalar vasitəsilə mütəmadi olaraq təhqir edilməsi və ya təhdid edilməsinə aid edilir, bu isə uşaqları ağır psixoloji travmaya

DOI: 10.25045/forensic.gov.2026.41

məruz qoyur. Milosevic və başqaları tərəfindən aparılan araşdırmada Sİ əsaslı preventiv proqramların kiberzorakılıq hallarını 30%-dək azalda bilməsini qeyd edilir [8]. Lakin cinayətkarların anonimliyi və kriptovalyutalardan istifadə etməsi, hələ də bu hücumların qarşısının alınmasını, uşaqların hüquqlarının müdafiəsini çətinləşdirən əsas faktorlardan biri olaraq qalmaqda davam edir [9].

III. RƏQƏMSAL EKSPERTİZA PROSESİNİN ƏHƏMİYYƏTİ VƏ PROBLEMLƏRİ

UYK-nin istintaqı zamanı rəqəmsal ekspertiza həlledici rola malikdir və aşağıdakı mərhələlərdən ibarətdir [7-10]

- Sübutların identifikasiyası və toplanması üçün insidentlərlə əlaqəli rəqəmsal sübutların yerləşdiyi kkompüterlər, smartfonlar, bulud xidmətləri və digər informasiya sistemləri müəyyənləşdirilir və həmin məlumatlar dəyişdirilmədən əldə edilir;
- Sübutların qorunması prosesi rəqəmsal sübutların ələ keçirildiyi andan məhkəməyə təqdim edilməsinə qədər bütün hərəkətlərini sənədləşdirən xronoloji sənədləşmə prosesidir;
- Məlumatların bərpası və təhlili mərhələsində ekspertlər surəti çıxarılmış məlumatlar üzərində dərin araşdırma apararaq gizlədilmiş və ya silinmiş faylları bərpa edir, istifadəçinin sistem jurnalları (loqlar) və istifadəçi fəaliyyətləri təhlil olunur;
- Hesabat və məhkəmə üçün təqdimat mərhələsi ekspertiza prosesinin yekun mərhələsidir. Burada əldə olunan bütün texniki tapıntılar hüquqşünaslar və hakimlər üçün şəffaf şəkildə rəsmiləşdirilir.

Qeyd edək ki, UYK-nın araşdırılmasında rəqəmsal ekspertiza sahəsi bir sıra ciddi texniki, hüquqi və etik problemlərlə üzləşir. Aşağıda bu problemlər barədə məlumat verilir.

Şifrələmə, anonimlik və "dark web". Cinayətkarlar UCİM mübadiləsi üçün getdikcə daha çox "Dark Web" və "Tor" şəbəkəsindən istifadə edirlər. Jin və başqaları Tor şəbəkəsinin kriminalistik araşdırılması zamanı əsas problemin dinamik domen dəyişikliyi olduğunu müəyyən etmişlər [10]. Ucdan-uca (end-to-end) şifrəli mesajlaşma tətbiqlərində məlumatlara birbaşa çıxış məhdudlaşır və rəqəmsal sübutların əldə olunmasını çətinləşdirir.

Süni intellekt və sintetik media (deepfake). Generativ süni intellekt texnologiyaları ilə yaradılan sintetik UCİM ənənəvi heş-əsaslı aşkarlama sistemləri ilə effektiv hesab edilmir, çünki hər bir yaradılan şəkil kriptoqrafik cəhətdən unikaldır [11]. Bu isə rəqəmsal ekspertin əldə olunan materialın real uşağa aid olub-olmadığını müəyyən etməsinə çətinlik yaradır. Dushi və başqaları qeyd edirlər ki, müasir qanunvericiliyin əksəriyyəti Sİ tərəfindən yaradılan UCİM-i real UCİM-dən fərqləndirir, belə ki, onları eyni hüquqi kateqoriyaya daxil etmir, bu isə hüquqi tənzimləmədə boşluqlar yaradır [12].

Məlumat həcminin böyüklüyü. Bir istintaq çərçivəsində on minlərlə şəkil, video və mesajın əl ilə yoxlanılması üçün diqqət, gərgin əmək və uzun vaxt lazım gəlir. Bu isə müstəntiqlər üçün həm böyük vaxt itkisi, həm də ciddi psixoloji problemlər yaradır [13].

Yurisdiksiya və beynəlxalq hüquqi maneələr. Kibercinayətlərin transsərhəd xüsusiyyətinə malik olması, cinayətkarın bir ölkədə, istifadə olunan serverin başqa ölkədə, qurbanın isə üçüncü bir ölkədə olması istintaqın effektivliyinə mənfi təsir edir. Rəqəmsal sübutların fərqli ölkələrdən əldə edilməsi mürəkkəb beynəlxalq hüquqi prosedurlar tələb edir ki, bu da istintaq müddətinin uzanmasına səbəb olur. Calcaranın fikrincə, İnterpol-un ICSE (International Child Sexual Exploitation) verilənlər bazası bu problemin həllində kömək etsə belə, ölkələr arasında məlumat mübadiləsinin hələ də kifayət qədər operativ olmaması müşahidə edilir [14].

Kriptovalyuta və maliyyə izlərinin silinməsi. Müasir kibercinayətkarlıqda kriptovalyutalar və maliyyə izlərinin silinməsi geniş yayılıb. Kibercinayətkarlar uşaqları şantaj etməklə onları müəyyən ödənişlər etməyə məcbur edir və belə maliyyə əməliyyatlarının həyata keçirilməsində çox vaxt Bitcoin, Monero kimi kriptovalyutalardan istifadə edirlər. Monero kimi gizlilik yönümlü kriptovalyutalar blokçeyn analitikasını çətinləşdirir və bəzən qeyri-mümkün edir [15]. Mürəkkəb maliyyə manipulyasiyaları uşaqlara qarşı törədilən kibercinayətlərdə çox vaxt iqtisadi aspektləri gizlədir. Bu isə rəqəmsal sübutların izlənilməsində, uşaqların aldadılmasında iştirakı olan transsərhəd cinayətkar qrupların aşkarlanmasını və ifşa olunmasını çətinləşdirir.

IV. UŞAQLARIN RƏQƏMSAL MÜHİTDƏ QORUNMASI ÜZRƏ BEYNƏLXALQ SİYASƏT VƏ HÜQUQİ ÇƏRÇİVƏLƏR

Uşaqların rəqəmsal mühitdə qorunması məsələsi beynəlxalq təşkilatlar qarşısında olan ən aktual problemlərdən biri olduğundan bu istiqamətdə müxtəlif konseptual modellər təklif edilmişdir. Belə ki, Beynəlxalq Telekommunikasiya İttifaqının COP (Child Online Protection) təlimatları uşaqların hüquqlarını qorumaq üçün hökumət, sənaye və cəmiyyət arasında inteqrasiyanı tələb edir [2]. Eyni zamanda, Birləşmiş Krallığın 2023-cü ildə qəbul etdiyi "Online Safety Act" (Onlayn Təhlükəsizlik Aktı) və ABŞ-ın COPPA (Children's Online Privacy Protection Rule) qaydaları sosial media platformalarından yaş verifikasiyası mexanizmlərinin tətbiqini tələb edir [4].

Uşaqların Cinsi İstismar və Cinsi Zorakılıqdan Müdafiəsi haqqında Avropa Şurası Konvensiyası (Lanzarote Konvensiyası) 2007-ci ildə qəbul edilmişdir. Bu sənəd uşaqların cinsi istismarı və zorakılığa qarşı mübarizədə standart hesab olunur [4]. Burada əsas məqsəd həm fiziki olaraq, həm də İnternet mühitində uşaqlara qarşı törədilən cinsi istismarın qarşısının alınması, qurbanların müdafiəsi və cinayətkarların cəzalandırılmasıdır.

Avropa Şurasının Kibercinayətkarlıq haqqında Konvensiyası ("Budapeşt Konvensiyası") rəqəmsal mühitdə uşaqların təhlükəsizliyinin təmin edilməsində mühüm hüquqi mexanizmdir. Bu sənəd kompüter sistemləri vasitəsilə uşaqların cinsi istismarının qarşısını almaq məqsədilə cinayət qanunvericiliyinin müasirləşdirilməsini nəzərdə tutur. UCİM-in elektron istehsalı, saxlanması və yayılmasının müxtəlif aspektlərini cinayət əməli kimi hesab etməklə (Maddə 9) kiberzorakılıq hallarının aradan qaldırılmasında, cinayətlərin araşdırılması üçün rəqəmsal sübutların toplanmasında beynəlxalq əməkdaşlığın yaradılmasının əhəmiyyətini ehtiva edir [4].

2019-cu ildə Azərbaycan Respublikasının "Uşaqların cinsi istismardan və cinsi zorakılıqdan müdafiəsi haqqında" Avropa Şurası Konvensiyasının təsdiq edilməsi barədə qanunu uşaqların yalnız fiziki deyil, həm də virtual mühitdən gələn təhlükələrdən müdafiə olunması istiqamətində xüsusi əhəmiyyətə malikdir [16].

Beynəlxalq hüquqi sənədlər və milli qanunvericilik aktları uşaqların rəqəmsal mühitdə müdafiəsi üçün əsas normativ çərçivəni formalaşdırır. Kiberməkanda yaranan risklərin aradan qaldırılması yalnız hüquqi mexanizmlərlə məhdudlaşmır və qabaqcıl texnoloji vasitələrin tətbiqini zəruri edir. Növbəti mərhələdə texnoloji həllərin tətbiqi imkanları və onların ekspertiza proseslərinə inteqrasiyasına dair mövcud elmi ədəbiyyatın təhlili təqdim olunur.

V. ƏDƏBİYYAT İCMALI

Rəqəmsal mühitdə baş verən hüquq pozuntularının artması rəqəmsal kriminalistika sahəsində sistemli və elmi əsaslandırılmış yanaşmaların tətbiqini zəruri edir. Mövcud ədəbiyyat göstərir ki, rəqəmsal sübutların toplanması, qorunması və təhlili üçün beynəlxalq standartlar və texnoloji metodlar bir-birini tamamlayan əsas mexanizmlərdir. Xüsusilə mobil kommunikasiya və onlayn davranışların analizi müasir tədqiqatlarda mühüm istiqamət kimi çıxış edir.

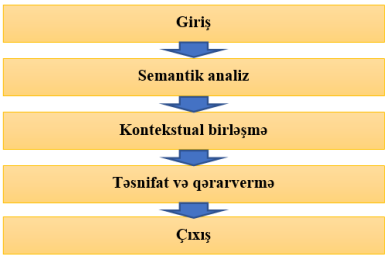
Rəqəmsal kriminalistika sahəsinin əsasını NIST SP 800-86 və ISO/IEC 27037:2012 standartları təşkil edir [17]. Bu standartlar rəqəmsal sübutların toplanması, qorunması, analizi və məhkəmədə təqdim edilməsi üçün dəqiq prosedurlar müəyyən edir. Widatama öz tədqiqatında sübut zəncirinin qorunmasında SHA-256 haş alqoritminin əhəmiyyətini qeyd edir [18].

Mobil cihazlardan SMS məlumatlarının rəqəmsal ekspertizası sahəsindəki tədqiqatlar göstərir ki, mesajların metaverilənlər (göndərən nömrəsi, vaxt nişanı, mesaj uzunluğu) ilə linqvistik məzmun analizinin birlikdə aparılması kibercinayət əlamətlərinin təsdiqi üçün güclü sübut bazası formalaşdırır. Yəni yalnız təhlil edilən SMS deyil, həm də onun ətrafında olan gizli informasiya qiymətləndirilir. Sheth və başqaları öz tədqiqatlarında Isolation Forest, One-Class SVM (Support Vector Machine) anomaliya aşkarlanma alqoritmləri vasitəsilə şübhəli mesajların 87 % dəqiqliklə müəyyən etdiklərini göstərmişdir [19].

Grooming onlayn mühitdə baş verən ən ciddi təhlükələrdən biridir. Araşdırmalar göstərdi ki, SVM, Isolation Forest və digər maşın təlimi alqoritmlərinin müəyyən performans və dəqiqlik nümayiş etdirsə də, kibertəhlükələrin analizi, mürəkkəb semantik təhlili və kontekstual əlaqələrin müəyyən edilməsində bu modellər qənaətbəxş nəticələr göstərmir. Bu zəifliklərı nəzərə alaraq tədqiqat işində ikitərəfli kontekstual təhlil imkanlarına malik BERT arxitekturasına əsaslanan, uşaqlara yönəlmiş gizli təhdidlərin identifikasiyasını daha effektiv şəkildə aşkar edən bir ekspertiza metodu təklif olunur.

VI. TƏKLİF EDİLƏN MODELİN ARXİTEKTURASI

Tədqiqatda UYK-nın aşkarlanması və rəqəmsal sübutlarda cinayət tərkibinin müəyyən edilməsi üçün yeni metodologiya təklif olunur. Dərin təlim və NLP (təbii dil emalı) prinsiplərinə uyğun bu yanaşma, real vəziyyətdə kontekstual analizin aparılmasını nəzərdə tutur. Burada yanaşmanın tətbiq sahəsi, nümunə olaraq, 12 yaşlı uşağın smartfonuna bir gün ərzində daxil olan 5 şübhəli SMS-in kibercinayət əlaməti daşıyıb-daşımamasının qiymətləndirilməsi və məzmununun kontekstual təhlili əsasında kibercinayətkarlığın müəyyən edilməsi və təsnifləşdirilməsindən ibarətdir. Metodologiya çərçivəsində, PAN-12 (cinsi yırtıcıların identifikasiyası) məlumat dəstindən istifadə edilir [20]. Kibercinayətkar davranışların aşkarlanması üçün BERT əsaslı hibrid model təklif edilir və onun tətbiqi aşağıdakı mərhələlər üzrə strukturlaşdırılmışdır (Şəkil 1).



Şəkil 1. Mətnin kontekstual analizi üçün BERT əsaslı modelin iyerarxik strukturu

Giriş hissəsi rəqəmsal cihazlardan əldə edilmiş xam mesajların və dialoqların model vasitəsilə emal edilməsi üçün ilkin mərhələdir.

Semantik analiz mətndəki sözlərin təkcə hərfi mənasını deyil, onların arxasındakı gizli niyyəti və semantik çalarları alqoritmlər vasitəsilə dərindən təhlili mərhələsidir.

Kontekstual birləşmə ayrı-ayrı mesajlar arasında mövcud olan məntiqi əlaqələrin inteqrasiyası vasitəsilə onlar vahid bir hadisə zənciri şəklində strukturlaşdırılmasını təmin edən mərhələdir. Bu mərhələnin nəticəsində cinayətkarın uzunmüddətli davranış modelini müəyyən etmək mümkündür

Təsnifat və qərarvermə analiz edilmiş kontekstual məlumatları əvvəlcədən müəyyən edilmiş risk kateqoriyaları (məsələn, kiberqruminq və ya şantaj) üzrə qruplaşdıraraq hadisənin cinayət tərkibini statistik ehtimallar əsasında təyin edilməsi mərhələsidir.

Çıxış hissəsində aparılmış ümumi təhlillər əsasında əldə olunan yekun nəticələr, rəqəmsal ekspertlər və hüquq-mühafizə orqanları üçün aydın, əsaslandırılmış və sübutlarla dəstəklənmiş bir hesabat şəklində təqdim edilən son mərhələdir.

Metodun effektivliyinin yoxlanılması üçün eksperimentlər Python proqramlaşdırma dilindən istifadə edilməklə Google Colab mühitində həyata keçirilmişdir. Aşağıda sınaq zamanı istifadə edilən modellərin müqayisəsi verilir (Cədvəl 1).

CƏDVƏL I. UYK-NIN AŞKARLANMASINDA TƏTBİQ OLUNAN MODELLƏRİN MÜQAYİSƏLİ QİYMƏTLƏNDİRİLMƏSİ

Model	Accuracy	MAE	R2 Score
CNN	0.78	0.18	0.65
Bi-LSTM	0.82	0.15	0.72
Bi-LSTM + Attention	0.92	0.08	0.88
BERT	0.94	0.05	0.90

Cədvəl 1-ə əsasən, CNN(Convolutional Neural Network) modelinin çox aşağı məhsuldarlıq göstəricisinə malik olması müşahidə olunur. Bi-LSTM (Bidirectional Long Short-Term

Memory) modelinin 0.82 dəqiqlik göstərici ilə dialoqdakı cümlələri axırdan əvvələ və əksinə oxumasına baxmayaraq, Attention mexanizmi daxil edilmədən bəzi təhlükəli ifadələri dəqiq müəyyənləşdirə bilmir. Bi-LSTM + Attention modelində isə dəqiqlik 0.92-yə yüksəlir. Təklif edilən BERT modeli isə digərlərindən daha üstün nəticə göstərir. Belə ki, MAE (Mean Absolute Error) – orta mütləq xətanın 0.05-ə bərabər olması bu modelin digərləri ilə müqayisədə minimal xəta payına malik olduğunu göstərir. Bu isə kiberkriminalistika baxımından daha yaxşı nəticə hesab edilir. R2 Score qiymətləndirmə meyarının 0.90 olması isə onun verilənlərdə olan cinayətin tərkibini yüksək dəqiqliklə izah etməsini göstərir. Bu modelin dəqiqlik performansının 0.94 olması onun digər metodlardan üstün olaraq, uşaqlara ünvanlanmış qruminq mesajlarının düzgün düzgün identifikasiya edə bilməsini təsdiq edir.

NƏTİCƏ

Uşaqların rəqəmsal təhlükəsizliyinin təmin olunması və onlara qarşı törədilən kibercinayətlərin, xüsusilə onlayn qruminq kimi təhlükələrin aşkarlanması və qarşısının alınması kompleks yanaşma tələb edir. Bu sahədə yalnız hüquqi tənzimləmələrlə yanaşı, süni intellektə əsaslanan müasir texnologiyalardan istifadə vacibdir. UYK-nin həlli məsələlərində süni intellekt texnologiyalarının rəqəmsal kriminalistika proseslərinə inteqrasiyası bu prosesdə əhəmiyyətli üstünlüklər təmin edə bilər.

Aparılan araşdırmalar və eksperimental nəticələr onu göstərir ki, təklif olunan BERT əsaslı yanaşma rəqəmsal ekspertiza proseslərinin avtomatlaşdırılmasına, insan amilindən asılılığın azaldılmasına və hüquq-mühafizə orqanlarının potensial təhdidləri daha erkən mərhələdə müəyyən etməsinə imkan verir. Həmçinin, rəqəmsal sübutların həcminin böyüməsi və şifrəli ünsiyyət platformalarının geniş yayılması kontekstual təhlilin zəruriliyini ortaya qoyur.

ƏDƏBİYYAT

[1] UNICEF, "Generative AI: Risks and opportunities for children," UNICEF, New York, NY, USA, 2024.

[2] S. Ojagverdiyeva, "Ensuring child safety in internet environment," Problems of Information Society, vol. 9, no. 1, pp. 87-93, 2018, doi: 10.25045/jpis.v09.i01.09.

[3] C. May-Chahal et al., "A rapid evidence assessment of technical tools for the detection and disruption of child sexual abuse media (CSAM) and CSAM offenders in the ASEAN region," 2022. [Online]. Available: https://research-information.bris.ac.uk/en/publications/a-rapid-evidence-assessment-of-technical-tools-for-the-detection-/

[4] Council of Europe, "Cyberviolence against children," [Online]. Available: https://www.coe.int/en/web/cyberviolence/cyberviolence-against-children.

[5] Y. Fu et al., "Understanding Children's Avatar Making in Social Online Games," in Proc. 2025 CHI Conf. on Human Factors in Computing Systems, Apr. 2025, pp. 1-16, doi: 10.1145/3706598.3713262.

[6] M. Leiva-Bianchi et al., "Effectiveness of machine learning methods in detecting grooming: a systematic meta-analytic review," Scientific Reports, vol. 15, art. no. 2024, 2025, doi: 10.1038/s41598-024-83003-4.

[7] E. Kokolaki and P. Fragopoulou, "Unveiling AI's threats to child protection: regulatory efforts to criminalize AI-generated CSAM," arXiv preprint arXiv:2503.00433, 2025.

[8] T. Milosevic, K. Van Royen, and B. Davis, "Artificial intelligence to address cyberbullying, harassment and abuse: New directions in the midst of complexity," International Journal of Bullying Prevention, vol. 4, no. 1, pp. 1-5, 2022, doi: 10.1007/s42380-022-00117-x.

[9] K. S. Choi, "Uncovering cryptocurrency-enabled sextortion: a blockchain forensic analysis of transactions and offender laundering tactics," Information, vol. 17, no. 3, p. 236, 2026, doi: 10.3390/info17030236.

[10] P. Jin, N. Kim, S. Lee, and D. Jeong, "Forensic investigation of the dark web on the Tor network: pathway toward the surface web," International Journal of Information Security, vol. 23, pp. 1-18, 2024, doi: 10.1007/s10207-023-00745-4.

[11] E. Kokolaki and P. Fragopoulou, "Unveiling AI's threats to child protection: regulatory efforts to criminalize AI-generated CSAM," arXiv preprint arXiv:2503.00433, 2025.

[12] D. Dushi, N. Berdufi, and A. Karagianni, "The legal framework and legal gaps for AI-generated child sexual abuse material," Computer Law & Security Review, vol. 57, 2025, doi: 10.1016/j.clsr.2025.106077.

[13] J. R. Rimer, "Law enforcement trauma and immersion in child sexual abuse material," Child Abuse & Neglect, 2025, doi: 10.1016/j.chiabu.2024.106958.

[14] G. Calcara, "Balancing international police cooperation: INTERPOL and the undesirable trade-off between rights of individuals and global security," Liverpool Law Review, vol. 42, no. 2, pp. 111-142, 2021, doi: 10.1007/s10991-020-09266-9.

[15] K. S. Choi, "Uncovering cryptocurrency-enabled sextortion: a blockchain forensic analysis of transactions and offender laundering tactics," Information, vol. 17, no. 3, p. 236, 2026, doi: 10.3390/info17030236.

[16] "Uşaqların cinsi istismardan və cinsi zorakılıqdan müdafiəsi haqqında Avropa Şurası Konvensiyasının təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu," https://e-qanun.az/framework/43532.

[17] A. Luthfi, "Comparison study of NIST SP 800-86 and ISO/IEC 27037 standards as a framework for digital forensic evidence analysis," Journal of Information Systems and Informatics, vol. 6, no. 2, pp. 701-718, 2024, doi: 10.51519/journalisi.v6i2.717.

[18] K. Widatama, "Mobile Device Digital Forensics for Supporting Cybercrime Investigation and Evidence Presentation," Forensics & Security Journal, vol. 1, no. 1, 2025.: https://journal.ekantara.com/forsec/article/view/1.

[19] R. Sheth, K. Kaushik, C. Parekha, and N. Chayal, "Applications of Machine Learning in Mobile Forensics," in Android and iOS Mobile Forensics: Leveraging Blockchain, Machine Learning, and Deep Learning for Digital Investigations, Berkeley, CA: Apress, 2026, pp. 309-340, doi: 10.1007/979-8-8688-1748-9_11.

[20] PAN12 Deception Detection: Sexual Predator Identification. https://datasetsearch.research.google.com/search?query=pan12-sexual-predator-identification&docid=L2cvMTF2anFmMG1jXw%3D%3D.

Problems and Solutions of Digital Forensic Investigation of Cybercrimes Targeting Children

Tofig Kazimov[1], Sabira Ojagverdiyeva[2]

[1,2]Institute of Information Technology, Baku, Azerbaijan

[1]tofig@mail.ru, [2]allahverdiyevasabira@gmail.com

Abstract - The development of digital platforms and the rapid proliferation of smart devices increase the likelihood of children being exposed to cyber threats. This paper analyzes the challenges arising in the digital forensics process during the investigation of cybercrimes targeting children, which have become increasingly complex due to the impact of artificial intelligence and sophisticated digital encryption methods. A new detection methodology based on natural language processing and deep learning architectures is proposed. The experiments, conducted on the PAN-12 dataset using the proposed BERT (Bidirectional Encoder Representations from Transformers) model, demonstrate that complex linguistic features used by offenders (such as manipulation, covert threats, and isolation attempts) can be detected with higher accuracy compared to alternative models.

Keywords - Digital forensics; child safety; cybercrime; digital evidence; BERT.