Kiberkriminalistika: Əsas Termin və Anlayışların Azərbaycan Dilində İstifadəsi Məsələləri

Əfruz Qurbanova[1], Mehriban Bağırova[2]
[1,2]İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*afruz1961@gmail.com*, [2]*mehriban.amea@gmail.com*

***Xülasə*— Azərbaycanda rəqəmsal transformasiya proseslərinin sürətlənməsi və kibertəhdidlərin artması və mürəkkəbləşməsi bu sahədə elmi-metodoloji bazanın və dəqiq terminoloji sistemin formalaşdırılmasını zəruri edir. Terminoloji birmənalılığın təmin edilməməsi rəqəmsal sübutların məhkəmə prosesində qiymətləndirilməsinə və istintaqın effektivliyinə birbaşa təsir göstərir. Məqalədə kiberkriminalistika sahəsinə aid termin və anlayışların Azərbaycan dilində istifadəsi məsələləri araşdırılır. Kiberkriminalistika sahəsinə aid terminlərin beynəlxalq standartlara uyğunlaşdırılma mexanizmləri və Azərbaycan dilində bu sahədə qarşıya çıxan əsas linqvistik-hüquqi problemlər təhlil edilir.**

Açar sözlər— kiberkriminalistika; rəqəmsal ekspertiza; INTERPOL standartları; rəqəmsal sübut; hüquqi-texniki terminlər.

I. GİRİŞ

XX əsrin sonlarında kiberkriminalistika kriminalistika elminin müstəqil inkişaf edən yeni bir alt sahəsi kimi formalaşmışdır, 2001-ci ildə keçirilən ilk Rəqəmsal Məhkəmə Təhqiqatı üzrə Seminarda rəqəmsal sübutların aşkar edilməsi, toplanması, təhlili və məhkəmə prosesində təqdim olunmasını əhatə edən elmi-metodoloji sahə kimi müəyyən edilmişdir [1].

Müasir yanaşmalara əsasən, kiberkriminalistika kiberməkanda baş verən cinayətlərin və informasiya təhlükəsizliyi ilə bağlı insidentlərin araşdırılmasına xidmət edən multidissiplinar sahədir. Bu sahə kompüter elmləri ilə hüquqi metodologiyanın inteqrasiyası əsasında rəqəmsal sübutların identifikasiyası, sənədləşdirilməsi və məhkəmə prosesində təqdim edilməsini təmin edir [2].

Azərbaycanda bu sahənin inkişafı terminoloji dəqiqlik və vahidlik məsələlərini aktuallaşdırmışdır. Elmi-texniki tərəqqi və informasiya-kommunikasiya texnologiyalarının geniş tətbiqi nəticəsində müxtəlif bilik sahələrinin terminoloji sistemi də əhəmiyyətli dərəcədə genişlənmişdir. Bu kontekstdə terminologiya elmi yeni anlayışların sistemləşdirilməsi, unifikasiyası və standartlaşdırılması üçün metodoloji baza rolunu oynayır [3].

Rəqəmsal mühitdə məlumatların sürətli artımı, struktur dəyişkənliyi və texnoloji mürəkkəbliyi kiberkriminalistika çərçivəsində yeni metodoloji yanaşmaların tətbiqini zəruri edir [4]. Bu isə rəqəmsal sübutların aşkar edilməsi, qorunması və interpretasiyası prosesində xüsusi kriminalistik metodların tətbiqini tələb edir. Bu sahənin sürətli inkişafı hüquqi və texniki terminlər arasında semantik uyğunluğun təmin edilməsi problemini aktuallaşdırmışdır. Terminoloji uyğunsuzluqlar rəqəmsal sübutların hüquqi etibarlılığına və istintaq prosesinin effektivliyinə mənfi təsir göstərə bilər [5]. Bu baxımdan kiberkriminalistika terminləri sisteminin formalaşdırılması prosesi sadəcə linqvistik tərcümə prosesi deyil, ciddi metodoloji prinsiplərə söykənən sistemləşdirmə tələb edir.

Tədqiqatın əsas məqsədi Azərbaycan dilində istifadə olunan kiberkriminalistika terminlərinin beynəlxalq standartlara uyğunlaşdırılması və bu sahədə vahid terminoloji informasiya sisteminin formalaşdırılmasıdır. Bu prosesdə terminlərin birmənalılığı, müasirliyi və normativliyi rəqəmsal cinayətlərin araşdırılması üçün əsasdır [6, 7].

II. KİBERKRİMİNALİSTİKA TERMİNOLOGİYASININ FORMALAŞMASININ NƏZƏRİ ƏSASLARI

Kiberkriminalistika sahəsinin inkişafı hüquqi və texniki yanaşmaların qarşılıqlı təsiri nəticəsində yeni terminoloji sistemin formalaşmasına səbəb olmuşdur [4]. Bu terminoloji sistem yalnız hüquq elminə deyil, həm də informasiya texnologiyaları, rəqəmsal ekspertiza və kibertəhlükəsizlik sahələrinə aid anlayışların inteqrasiyasına əsaslanır, bu da terminologiyanın multidissiplinar xarakterini göstərir. Kiberkriminalistika terminologiyasının formalaşması bir neçə nəzəri prinsipə əsaslanır. İlk olaraq, terminlər hüquqi anlayışların dəqiq ifadəsini təmin etməlidir və normativ-hüquqi sənədlərdə tətbiq edilə biləcək səviyyədə standartlaşdırılmalıdır. Eyni zamanda, texnoloji inkişafın sürətli dinamikası nəzərə alınaraq terminlər müasir informasiya sistemləri və rəqəmsal texnologiyalarla bağlı real prosesləri dəqiq şəkildə əks etdirməlidir [6]. Bu sistemin formalaşmasına təsir edən mühüm amillərdən biri də hüquqi və texniki terminlər arasında semantik uyğunluğun təmin edilməsidir [5].

Kiberkriminalistika terminologiyasının formalaşması prosesində beynəlxalq təcrübə və standartların nəzərə alınması da mühüm əhəmiyyət kəsb edir. İnformasiya texnologiyaları sahəsində terminlərin əksəriyyəti beynəlxalq elmi mühitdə formalaşdığı üçün onların milli hüquqi sistemə uyğunlaşdırılması vacibdir. Bu prosesdə terminlərin həm milli dil normalarına, həm də beynəlxalq elmi diskursa uyğunluğu qorunmalıdır.

Kiberkriminalistika terminologiyası dinamik xarakter daşıyır və texnoloji inkişafla paralel olaraq daim yenilənir. Yeni texnologiyaların meydana çıxması ilə əlaqədar olaraq yeni hüquqi anlayış və terminlər meydana gəlir. Bu isə terminoloji sistemin davamlı təhlilini və standartlaşdırılmasını zəruri edir.

Beləliklə, kiberkriminalistika terminologiyasının

DOI: 10.25045/forensic.gov.2026.76

formalaşması hüquqi, texnoloji və linqvistik amillərin qarşılıqlı təsiri nəticəsində həyata keçirilir. Terminlərin vahid və sistemli şəkildə istifadəsi bu sahədə hüquqi tədqiqatların inkişafını, normativ tənzimləmənin təkmilləşdirilməsini və rəqəmsal cinayətlərin effektiv araşdırılmasını təmin edən mühüm metodoloji əsas yaradır. Kiberkriminalistika sahəsində terminologiyanın dəqiq, ardıcıl və standartlaşdırılmış şəkildə tətbiqi ekspertiza fəaliyyətinin obyektiv aparılmasında mühüm rol oynayır. Terminoloji sistem yalnız anlayışların adlandırılması vasitəsi deyil, eyni zamanda biliklərin strukturlaşdırılması və sahədaxili nəzəri əsasların formalaşdırılması mexanizmi kimi çıxış edir [8]. Bu baxımdan terminoloji dəqiqlik rəqəmsal sübutların identifikasiyası, təhlili və hüquqi qiymətləndirilməsi proseslərinin etibarlılığı ilə birbaşa əlaqəlidir.

Multidissiplinar tədqiqat sahəsi kimi kiberkriminalistikada vahid terminoloji yanaşma müxtəlif sahələrə aid anlayışların semantik uyğunlaşdırılmasını təmin edir. Terminlərin qeyri-standart və ya fərqli semantik çərçivələrdə istifadəsi rəqəmsal sübutların şərhində uyğunsuzluqlara səbəb ola, ekspert rəylərinin etibarlılığını zəiflədə və istintaq prosesində metodoloji səhvlərin yaranmasına gətirib çıxara bilər. Elektron sübutların toplanması, qorunması və analizi mərhələlərində terminoloji dəqiqlik hadisələrin rekonstruksiyası, subyektlərin identifikasiyası və əldə edilən məlumatların məhkəmə prosesində qəbul edilə bilməsi üçün əsas şərtlərdən biri hesab olunur. Terminoloji vahidlik xüsusilə beynəlxalq əməkdaşlıq mühitində mühüm əhəmiyyət kəsb edir. Hüquqi baxımdan ekspert rəylərində istifadə edilən terminlərin elmi əsaslandırılması sübutların hüquqi qüvvəsinin qorunması baxımından zəruridir.

Rəqəmsal transformasiyalar nəticəsində yeni anlayışların yaranması terminoloji sistemin dinamik inkişafını tələb edir. Bu kontekstdə Təbii Dilin Emalı (Natural Language Processing — NLP) metodları terminoloji korpusların formalaşdırılması, terminlərarası semantik münasibətlərin müəyyənləşdirilməsi və standartlaşdırılmış termin bazalarının yaradılması üçün perspektivli yanaşma kimi qiymətləndirilir [9].

III. KİBERKRİMİNALİSTİKA TERMİNOLOGİYASININ FORMALAŞDIRILMASI PRİNSİPLƏRİ VƏ BU SAHƏDƏ BEYNƏLXALQ STANDARTLAR

Kiberkriminalistika terminologiyasının formalaşdırılması ümumi terminologiya nəzəriyyəsinin elmi prinsipləri və beynəlxalq standartlar çərçivəsində həyata keçirilir. Burada terminlərin seçimi və istifadəsi yalnız linqvistika məsələsi deyil, həm də hüquqi və texniki sahələr arasında vahid anlaşmanı təmin edir [10].

Terminologiyanın formalaşdırılması prosesində tətbiq olunan əsas prinsiplər aşağıdakılardır:

- Terminlər yalnız bir anlayışı ifadə etməli və semantik qeyri-müəyyənlik yaratmamalıdır;
- Terminlər vahid sistem daxilində qarşılıqlı əlaqədə formalaşdırılmalı və normativ-hüquqi sənədlərlə uyğunlaşdırılmalıdır;
- Terminlər dil normalarına uyğun olmalı, üslub baxımından neytral xarakter daşımalı və müxtəlif peşə qrupları üçün anlaşılan olmalıdır;
- Terminlərin semantik sabitliyi qorunmalı və texnoloji inkişafın dinamikasını əks etdirməlidir.

Bu prinsiplər terminologiyanın banilərindən biri, avstraliyalı alim Eygen Vyusterin (Eugen Wüster) yanaşması, ISO 704 beynəlxalq standartı çərçivəsində müəyyən edilmiş metodologiyaya əsaslanır [11, 12]. Beynəlxalq səviyyədə bu yanaşmalar INTERPOL-un rəqəmsal kriminalistika laboratoriyaları üçün Qlobal Təlimatlarla (Global Guidelines for Digital Forensics Laboratories) tamamlanır və daha da təkmilləşdirilir. IINTERPOL tərəfindən müəyyən edilmiş terminoloji birmənalılıq tələblərinə uyğun olaraq, milli elmi dövriyyədə "forensic image" (ekspertiza surəti), "data carving" (parçalanmış məlumatların bərpası) və "hash value" (rəqəmsal nəzarət cəmi) kimi anlayışların vahid semantik ekvivalentlərinin müəyyən edilməsi rəqəmsal sübutların hüquqi etibarlığını şərtləndirən əsas amillərdəndir.

Beynəlxalq standartlar terminoloji meyarlarla birbaşa əlaqəlidir. Bu standartlarda rəqəmsal sübutların identifikasiyası, toplanması və qorunması sistemləşdirilir, rəqəmsal ekspertiza metodlarının insident idarəetmə sistemlərinə inteqrasiyası müəyyən edilir [6, 7], INTERPOL təlimatlarında terminoloji uyğunluq təqdim edilir [13].

Kiberkriminalistika terminologiyasının inkişafı rəqəmsal texnologiyaların və kiberhədəflərin təkamülü ilə sıx bağlıdır. Yeni təhdidlər və texnologiyalar mövcud terminlərin semantik qiymətləndirilməsini və yeni terminlərin yaradılmasını tələb edir. Bu proses yalnız yeni terminlərin əlavə edilməsi ilə deyil, həm də mövcud anlayışların müasir rəqəmsal kontekstdə konseptual yenilənməsi ilə xarakterizə olunur. Kiberkriminalistika sahəsinin terminologiyası aşağıdakı əsas mərhələlər üzrə reallaşır [14]:

- İKT-nin inkişafı kiberhüquq və kibertəhlükəsizlik sahələrində yeni anlayışların yaranmasına səbəb olur;
- Bu anlayışlar terminoloji vahidlər kimi formalaşır və elmi leksikona daxil edilir;
- Rəqəmsal ekosistemdə formalaşmış universal anlayışlar milli dil mühitinə daxil olur;
- Bu anlayışlar milli dilə uyğunlaşdırılır, alternativ terminlər müəyyən edilir və birmənalılıq təmin olunur;
- Terminlər semantik və funksional meyarlar əsasında təsnif olunur, onların iyerarxik və məntiqi strukturu əsaslandırılır;
- Bu terminlər normativ-hüquqi sənədlərdə və elmi ədəbiyyatda vahid standart şəklində tətbiq olunur.

Beləliklə, kiberkriminalistika terminologiyası yalnız texnologiyaya bağlı yeniliklərdən ibarət deyil, həm də hüquqi, linqvistik və elmi aspektləri birləşdirən çoxsəviyyəli sistemdir. Hər mərhələ növbəti mərhələnin təməlini qoyur və nəticədə milli terminologiyanın *birmənalılığı, dəqiqliyi və funksional uyğunluğu* təmin olunur.

IV. AZƏRBAYCAN DİLİNDƏ KİBERKRİMİNALİSTİKA TERMİNOLOGİYASININ ƏSAS PROBLEMLƏRİ

Rəqəmsal texnologiyaların sürətli inkişafı nəticəsində müxtəlif sahələrə aid anlayışların böyük hissəsi ingilisdilli elmi mühitdə formalaşır, bu da bəzən həmin anlayışların Azərbaycan dilində uyğun ekvivalentlərinin müəyyənləşdirilməsini çətinləşdirir. Azərbaycan dilində kiberkriminalistika sahəsinin termin və anlayışları ilə bağlı müşahidə olunan problemləri lingvistik, terminoloji, semantik və multidissiplinar kateqoriyalar üzrə qruplaşdırmaq olar.

Linqvistik səviyyədə əsas çətinlik tərcümə və transliterasiya proseslərinin qeyri-dəqiq tətbiqi ilə bağlıdır. Texniki terminlərin milli dilin leksik-qrammatik sisteminə uyğunlaşdırılmadan birbaşa tərcüməsi anlayışların semantik strukturunun daralmasına və məna dəyişməsinə gətirib çıxarır. İntellektual transliterasiya yanaşmaları beynəlxalq terminoloji uyğunluğu qoruyaraq milli termin sisteminin inteqrasiyasına imkan yaradır, lakin bu metodların sistemli tətbiqi hələ kifayət qədər inkişaf etməmişdir [3].

Terminoloji səviyyədə əsas problemlərdən biri eyni anlayışın müxtəlif mənbələrdə fərqli terminlərlə ifadə olunmasıdır. "Rəqəmsal sübut", "rəqəmsal iz" kimi əsas anlayışların müxtəlif kontekstlərdə qeyri-sabit istifadəsi terminoloji sərhədlərin qeyri-müəyyənliyinə gətirib çıxarır. Bu vəziyyət sübutların toplanması, qorunması və təhlili mərhələlərində terminoloji ardıcıllığın pozulmasına gətirib çıxarır [1].

Semantik səviyyədə əsas diferensasiya problemi "verilənlər" (data) və "məzmun" (content) anlayışlarının aydın şəkildə fərqləndirilməməsi ilə bağlıdır. "Verilənlər" texniki strukturu ifadə etdiyi halda, "informasiya" semantik məzmunu əks etdirir. Bu fərqin nəzərə alınmaması ekspert rəylərində və hüquqi sənədləşmə prosesində qeyri-dəqiqliyə səbəb olur və nəticə etibarilə rəqəmsal sübutların qiymətləndirilməsinə mənfi təsir göstərir [5]. Multidissiplinar səviyyədə terminoloji sabitliyin formalaşmasına mane olan əsas amil hüquqi və texniki kommunikativ sahələr arasındakı fərqlərdir, bu, terminlərin birmənalılığının, vahidliyinin pozulmasına səbəb olur [13].

Kiberkriminalistika sahəsinin terminoloji sistemi beynəlxalq səviyyədə geniş şəkildə tədqiq olunur. Azərbaycanda bu sahənin terminoloji sistemin formalaşdırılması zəruridir.

V. AZƏRBAYCAN DİLİNDƏ KİBERKRİMİNALİSTİKA TERMİNOLOGİYASININ FORMALAŞMASI PRİNSİPLƏRİ

Kiberkriminalistika üzrə terminoloji sistemin formalaşması kibertəhlükəsizlik mexanizmlərinin və hüquqi tənzimləmə proseslərinin effektiv fəaliyyətini şərtləndirən mühüm istiqamətlərdən biri hesab olunur. Rəqəmsallaşma proseslərinin sürətlənməsi nəticəsində yeni anlayışların əsasən beynəlxalq, xüsusilə ingilisdilli elmi diskurs daxilində formalaşması milli dillərdə terminlərin uyğunlaşdırılması problemini aktuallaşdırır. Bu kontekstdə terminlərin yalnız linqvistik tərcüməsi deyil, onların məzmunu, funksional xüsusiyyətləri və tətbiq kontekstlərinin uyğunlaşdırılması zəruridir [3].

Kiberkriminalistika sahəsində terminoloji vahidliyin təmin olunmaması əsas problemlərdən biridir. Eyni anlayışın müxtəlif elmi və praktik mənbələrdə fərqli terminlərlə ifadə olunması terminoloji qeyri-sabitlik yaradır və tədqiqatın nəticələrinin müqayisə olunmasını çətinləşdirir. Terminoloji fərqlər rəqəmsal sübutların interpretasiyası və hüquqi qiymətləndirilməsi zamanı müxtəlif metodoloji yanaşmaların yaranmasına səbəb ola bilər [1, 7]. Terminlərin məna sərhədlərinin dəqiq müəyyənləşdirilməsi və anlayışlararası əlaqələrin ontoloji modelləşdirilməsi terminoloji sabitliyin əsas şərtlərindən biri hesab olunur [15].

Kiberkriminalistika sahəsində istifadə olunan terminoloji mənbələr kibertəhlükəsizlik və rəqəmsal kriminalistika ilə bağlı anlayışların sistemli izahını təmin edir. Bu sahədə beynəlxalq səviyyədə qəbul edilmiş əsas terminoloji və metodoloji mənbələr aşağıdakılardır:

- *NIST Cyber Security Framework (ABŞ):* Milli Standartlar və Texnologiya İnstitutu tərəfindən hazırlanmış, kibertəhlükəsizlik və kiberkriminalistika terminlərini və texniki standartları əhatə edən ən geniş bazadır [16].
- *ISO/IEC 27000: Information security management.* İnformasiya təhlükəsizliyi və rəqəmsal sübutlarla bağlı terminləri izah edən beynəlxalq standartlar toplusudur [17].
- *Glossary of Cyber Security Terms:* Ən çox istifadə edilən kibertəhlükəsizlik terminlərinin tərifini ehtiva edir [18].
- *Cyber Security and Infrastructure Security Agency* (CISA). Resources: Kibertəhlükəsizlik terminlərini araşdırmaq üçün istifadə edilən resurslar [19].

Azərbaycan dilində kiberkriminalistika və kibertəhlükəsizlik terminləri ilə bağlı müxtəlif terminoloji resurslar mövcuddur. Bu lüğətlər spesifik terminlərin aydın izahlarını təqdim edir. Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin cert.az portalı kiber-insidentlərin təsnifatı, şəbəkə hücumlarının tipləri və operativ terminologiya üzrə rəsmi istinad mənbəyidir. Bu resurs terminlərin texniki dəqiqliyini və beynəlxalq standartlara uyğunluğunu təmin edir [20]. AR Elm və Təhsil Nazirliyi İnformasiya Texnologiyaları İnstitutunun nəşr etdiyi "İnformatika terminlərinin izahlı lüğəti", "İnformasiya təhlükəsizliyi terminlərinin izahlı lüğəti" [21] və kibertəhlükəsizlik üzrə elmi vəsaitlər kiberkriminalistika sahəsində milli terminoloji sistemin formalaşmasında mühüm rol oynayır.

NƏTİCƏ

Kiberkriminalistika sahəsində aparılan tədqiqat və təhlillər göstərir ki, rəqəmsal cinayətlərin effektiv araşdırılması yalnız texniki imkanlarla deyil, həm də bu sahədə tətbiq edilən terminoloji sistemin dəqiqliyi və vahidliyi ilə birbaşa bağlıdır. Kiberkriminalistika hüquq, informasiya texnologiyaları və ekspertiza sahələrinin kəsişməsində yerləşdiyi üçün, istifadə olunan terminlərin həm texniki mütəxəssislər, həm də hüquqşünaslar üçün eyni semantik mənanı kəsb etməsi bu sahədə uğurlu fəaliyyət üçün əsas şərtdir.

Tədqiqat nəticəsində məlum oldu ki, Azərbaycan dilində kiberkriminalistika terminləri sisteminin formalaşması beynəlxalq standartlara söykənməli, eyni zamanda milli qanunvericiliyin (Azərbaycan Respublikasının Cinayət

Məcəlləsi, Fəsil 30) tələbləri ilə uzlaşmalıdır.

"Rəqəmsal sübut", "nəzarət zənciri" və "ekspertiza surəti" kimi əsas anlayışların vahid ekvivalentlərinin müəyyənləşdirilməsi məhkəmə-istintaq təcrübəsində yarana biləcək interpretasiya risklərini minimuma endirir. Kiberkriminalistika dinamik sahə olduğundan, terminoloji baza davamlı olaraq yenilənməli və Təbii dilin emalı kimi müasir metodlarla sistemləşdirilməlidir. Milli terminoloji bazanın formalaşdırılması və təkmilləşdirilməsi prosesində dilçi alimlərlə yanaşı, kiberkriminalistika üzrə mütəxəssislərin və hüquqşünasların birgə fəaliyyəti anlayışların konseptual bütövlüyünü və funksional adekvatlığını təmin edəcəkdir.

Beləliklə, kiberkriminalistika terminləri sisteminin vahid model əsasında formalaşdırılması Azərbaycanın rəqəmsal suverenliyinin qorunması, beynəlxalq hüquqi əməkdaşlığın gücləndirilməsi və kiberməkanda qanunun aliliyinin təmin edilməsi istiqamətində atılan mühüm addımdır.

ƏDƏBİYYAT

[1] G. Palmer, "A road map for digital forensic research," in Proc. 1st Digital Forensic Research Workshop (DFRWS), Utica, NY, USA, Aug. 2001, pp. 27–30.

[2] R. Montasari, V. Carpenter, and R. Hill, "A road map for digital forensics research: A novel approach for establishing the design science research process in digital forensics," Int. J. Electron. Secur. Digit. Forensics, vol. 11, no. 2, pp. 194–224, 2019.

[3] R. Temmerman, Towards New Ways of Terminology Description: The Sociocognitive Approach. Amsterdam, Netherlands: John Benjamins Publishing Company, 2000.

[4] S. L. Garfinkel, "Digital forensics research: The next 10 years," Digit. Investigation, vol. 7, no. 3, pp. 64–73, 2010, doi: 10.1016/j.diin.2010.05.009.

[5] D. Quick and K. K. R. Choo, "Digital forensic intelligence: Data subsets and Open-Source Intelligence (DFINT+ OSINT): A timely and cohesive mix," Future Gener. Comput. Syst., vol. 78, pp. 558–567, 2018.

[6] Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, ISO/IEC Standard 27037:2012, 2012.

[7] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-86, 2006.

[8] Ə. M. Qurbanova, "Terminoloji informatika sahəsində aparılan elmi-nəzəri araşdırmalar və onların təhlili," İnformasiya Cəmiyyəti Problemləri, Baku, Azerbaijan, no. 2(8), pp. 13–20, 2013.

[9] Ə. M. Qurbanova, "Predmet sahəsinin terminlərinin semantik şəbəkəsinin avtomatik qurulması texnologiyaları," İnformasiya Texnologiyaları Problemləri, no. 1, pp. 84–91, 2018.

[10] T. J. Silva, E. OliveiraJr, and A. F. Zorzo, "How ontologies have supported digital forensics: Review and recommendations," Forensic Sci. Rev., vol. 36, no. 2, pp. 99–125, 2024.

[11] M. Trojar, "Wüster's view of terminology," Slovenski Jezik / Slovene Linguist. Stud., vol. 11, pp. 55–85, 2017. https://kuscholarworks.ku.edu/server/api/core/bitstreams/4cb308b1-f4d8-4dd2-a91b-4174a20a02e2/content

[12] Terminology Work — Principles and Methods, ISO Standard 704:2022, 2022. https://www.iso.org/standard/79077.html

[13] INTERPOL, Global Guidelines for Digital Forensics Laboratories, Lyon, France, 2019.

[14] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," Int. J. Digit. Evidence, vol. 1, no. 3, pp. 1–12, 2002.

[15] A. Brinson, A. Robinson, and M. Rogers, "A cyber forensics ontology: Creating a new approach to studying cyber forensics," in Proc. Digital Forensic Research Conference (DFRWS), USA, 2006, pp. 37–43.

[16] "Glossary," Computer Security Resource Center, NIST. https://csrc.nist.gov/glossary

[17] "Online Browsing Platform (OBP) Search," ISO. https://www.iso.org/obp/ui/#search

[18] "Glossary of Terms," SANS Institute. https://www.sans.org/security-resources/glossary-of-terms/

[19] "Cybersecurity Glossary," Cybersecurity and Infrastructure Security Agency (CISA). https://www.cisa.gov/news-events/cybersecurity-glossary

[20] "Elektron Təhlükəsizlik Xidməti," Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi, cert.az. https://cert.az

[21] Y. N. İmamverdiyev, İnformasiya Təhlükəsizliyi Terminlərinin İzahlı Lüğəti. Baku, Azerbaijan: "İnformasiya Texnologiyaları" nəşriyyatı, 2015.

Cyber Forensics: Issues of Using Key Terms and Concepts in the Azerbaijani Language

Afruz Gurbanova[1], Mehriban Baghirova[2]

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

[1]afruz1961@gmail.com, [2]mehriban.amea@gmail.com

Abstract - The acceleration of digital transformation processes in Azerbaijan, together with the increasing frequency and growing complexity of cyber threats, necessitates the development of a scientific and methodological foundation as well as a precise terminological system in this field. The lack of terminological consistency directly affects the evaluation of digital evidence in judicial proceedings and the effectiveness of criminal investigations. This paper examines the use of terms and concepts related to the field of cyber forensics in the Azerbaijani language. It analyzes the mechanisms for harmonizing cyber forensics terminology with international standards and discusses the major linguistic and legal challenges encountered in the Azerbaijani language within this domain.

Keywords - cyber forensics; digital forensics; INTERPOL standards; digital evidence; legal and technical terminology.