Rəqəmsal Kriminalistika üzrə Kadr Hazırlığı və Təhsil Problemləri

Firudin Ağayev[1], Gülarə Məmmədova[2]
[1,2] İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*agayevinfo@gmail.com*, [2]*gyula.ikt@gmail.com*

***Xülasə*— Məqalədə rəqəmsal kriminalistika üzrə kadr hazırlığı prosesinin mövcud vəziyyəti təhlil edilmiş, təhsil sistemində mövcud problemlər müəyyənləşdirilmiş və onların aradan qaldırılması yolları təqdim edilmişdir. "Rəqəmsal kriminalistika" istiqaməti üzrə inkişaf etmiş ölkələrdəki universitetlərin tədris proqramlarının strukturu araşdırılmış, müqayisəli təhlil aparılmış, onların üstün və zəif tərəfləri müəyyən edilmişdir. Araşdırma nəticəsində təhsil proqramları mütəmadi olaraq yenilənməsi, praktiki yönümlü təlim metodları genişləndirilməsi, beynəlxalq təcrübənin öyrənilməsi və tətbiqi müəyyən edilmişdir.**

Açar sözlər*— *rəqəmsal kriminalistika; kibertəhlükəsizlik; tədris proqramları; proqramların müqayisəsi; tədris problemləri; çoxsahəli yanaşma.

I. GİRİŞ

Müasir informasiya cəmiyyətində rəqəmsal texnologiyaların sürətli inkişafı və həyatın bütün sahələrinə inteqrasiyası yeni çağırışlar və risklər formalaşdırmışdır. Xüsusilə internetin geniş yayılması, bulud texnologiyalarının tətbiqi, mobil cihazların və böyük verilənlər (Big data) ekosisteminin inkişafı kibercinayətkarlığın həm miqyasını, həm də mürəkkəbliyini əhəmiyyətli dərəcədə artırmışdır. Bu kontekstdə rəqəmsal mühitdə baş verən hüquq pozuntularının araşdırılması, sübutların toplanması və təhlili üçün rəqəmsal kriminalistika xüsusi əhəmiyyət kəsb edən elmi-praktiki istiqamət kimi formalaşmışdır. İnformasiya sistemlərinə qanunsuz müdaxilə, məlumat sızmaları, kiberdələduzluq və digər rəqəmsal cinayət növlərinin artması hüquq-mühafizə və təhlükəsizlik qurumlarının peşəkar, yüksək ixtisaslı mütəxəssislərə olan tələbatını daha da gücləndirmişdir.

Rəqəmsal kriminalistika kompüter sistemlərində, şəbəkələrdə və digər rəqəmsal mühitlərdə saxlanılan məlumatların etibarlı şəkildə əldə edilməsi, qorunması, analizi və təqdim olunması ilə məşğul olan multidissiplinar sahədir. Bu sahə kompüter elmləri, informasiya təhlükəsizliyi və hüquq kimi müxtəlif istiqamətlərin kəsişməsində yerləşir. Bu səbəbdən, rəqəmsal kriminalistika üzrə mütəxəssislərin hazırlanması yalnız texniki biliklərlə məhdudlaşmamalı, eyni zamanda hüquqi düşüncə, analitik təfəkkür və etik məsuliyyət kimi kompetensiyaların da formalaşdırılmasını tələb edir.

Son illərdə kibercinayətkarlıq sahəsində müşahidə olunan artım, dövlət qurumları, hüquq-mühafizə orqanları və özəl sektor üçün yüksək ixtisaslı kadrlara olan tələbatı kəskin şəkildə artırmışdır. Lakin bir çox ölkələrdə mövcud təhsil proqramları bu tələblərə tam cavab vermir. Xüsusilə kurikulumların köhnəlməsi, praktiki təlim imkanlarının məhdudluğu, müasir texnoloji vasitələrin çatışmazlığı və ixtisaslaşmış müəllim heyətinin azlığı kimi problemlər kadr hazırlığının keyfiyyətinə mənfi təsir göstərir.

Dünya təcrübəsi göstərir ki, rəqəmsal kriminalistika üzrə tədris proqramları müxtəlif modellər əsasında formalaşır və bu modellər ayrı-ayrı ölkələr üzrə fərqlənir. ABŞ universitetlərində tətbiqi yönümlü və hüquqi komponentlə zəngin proqramlar üstünlük təşkil etdiyi halda, Avropa ölkələrində daha çox tədqiqat yönümlü yanaşma müşahidə olunur. Asiya regionunda isə sənaye ilə inteqrasiya olunmuş və texnoloji innovasiyalara əsaslanan təhsil modelləri geniş yayılmışdır [1]. Bu müxtəliflik rəqəmsal kriminalistika sahəsində kadr hazırlığının vahid standartlarının formalaşdırılmasını çətinləşdirir və müqayisəli təhlil aparılmasını zəruri edir.

Təqdim olunan məqalənin əsas məqsədi rəqəmsal kriminalistika üzrə kadr hazırlığı üçün mövcud tədris proqramlarının strukturunu təhlil etmək, onların üstün və zəif tərəflərini müqayisə etmək və effektiv təhsil modelinin formalaşdırılması üçün elmi əsaslandırılmış yanaşmalar təqdim etməkdir. Bu məqsədə çatmaq üçün tədqiqat çərçivəsində beynəlxalq təcrübə öyrənilmiş, müxtəlif ölkələrin ali təhsil proqramları müqayisə edilmiş və struktur komponentlər sistemləşdirilmişdir.

II. MÜXTƏLİF ÖLKƏLƏRDƏ RƏQƏMSAL KRİMİNALİSTİKA İSTİQAMƏTİ ÜZRƏ TƏDRİS PROQRAMLARDAKI YANAŞMALAR

A. ABŞ universitetləri: ixtisaslaşmış və texnoloji yönümlü model

Rəqəmsal kriminalistika üzrə kadr hazırlığı kontekstində ABŞ, Avropa və Asiya universitetlərinin kurikulumlarının müqayisəli təhlili göstərir ki, bu sahədə təhsil modelləri ümumi baza prinsiplərinə malik olsa da, regionlara görə prioritetlər, struktur və metodoloji yanaşmalar əhəmiyyətli dərəcədə fərqlənir. Beynəlxalq təcrübədə Rəqəmsal kriminalistika proqramları adətən üç əsas komponent üzərində qurulur:

- texniki biliklər (kompüter elmləri, şəbəkə təhlükəsizliyi),
- hüquqi və kriminoloji əsaslar,
- praktiki laborator və tətbiqi təlimlər.

İlk illərdə, bakalavr proqramlarında fundamental kompüter elmləri və kriminalistika əsasları öyrənilir, sonrakı mərhələlərdə isə rəqəmsal sübutların toplanması, analizi və kibercinayət araşdırmaları tədris olunur.

DOI: 10.25045/forensic.gov.2026.74

ABŞ universitetlərində kurikulumlar daha çox dərin sənaye yönümlü ixtisaslaşma və yüksək texniki kompetensiyaların inkişafına yönəlmişdir [2]. ABŞ-da rəqəmsal kriminalistika proqramlarına kibertəhlükəsizlik və kriminologiyanın əsasları (bakalavr və magistr dərəcələri), rəqəmsal sübutların toplanması, etik haker hücumları və məlumatların təhlili daxildir. Məsələn, ABŞ-nın Pensilvaniya Dövlət Universiteti (Penn State University) kriminalistika təhsilinin "Qızıl Standartı" kimi tanınır. O, həm əyani, həm də onlayn olaraq rəqəmsal kriminalistika kursları seçimi ilə kibertəhlükəsizlik üzrə magistr dərəcəsi təklif edir.

UAB, MIT, Stanford və Berkeley kimi universitetlər rəqəmsal kriminalistikanın bir neçə sahəsində sertifikatlar və ixtisaslaşmalar əldə etmək imkanı ilə rəqəmsal kriminalistika modullarını əhatə edən aparıcı İT və informasiya təhlükəsizliyi proqramları təklif edir. İllinoys Texnologiya institutu (IIT) tətbiqi kibertəhlükəsizlik və rəqəmsal kriminalistika üzrə milli səviyyədə tanınmış magistr proqramı təklif edir. Burada, təlimin əsas məqsədi tələbələrə yalnız məlumatların necə əldə olunması deyil, həm də onları məhkəmədə sübut kimi qanuni şəkildə necə təqdim etməyi öyrətməkdir.

Tədris proqramı adətən dörd əsas seqmentə bölünür (Şəkil 1):

1. *Əsas texniki fənlər*. Bu kurslar rəqəmsal sistemlərin necə işlədiyinə dair biliklərin təməlini təmin edir. (şəbəkə texnologiyaları, əməliyyat sistemlərinin əsasları, proqramlaşdırma, verilənlər bazaları).
2. *İxtisaslaşmış kriminalistika modulları*.
   - 2.1. Kompüter kriminalistikası (Computer forensics): sərt disklərdən məlumatların çıxarılması və silinmiş faylların bərpası;
   - 2.2. Mobil kriminalistika (Mobile forensics): smartfonlar, planşetlər və GPS cihazları ilə iş;
   - 2.3. Bulud xidmətləri (Cloud services): bulud yaddaşından məlumatların çıxarılması.
   - 2.4. Şəbəkə kriminalistikası (Network forensics): haker hücumlarını aşkar etmək üçün şəbəkə trafikinin təhlili;
   - 2.5. Əməli yaddaşın kriminalistikası (Memory forensics): cihaz söndürüldükdə yoxa çıxan müvəqqəti məlumatların təhlili;
   - 2.6. Zərərli proqram təminatının təhlili (Malware analysis).
3. *Hüquqi və etik modul*.
   - 3.1. Kiberhüquq (Cyber Law): qanunvericiliyin öyrənilməsi (məsələn, fərdi məlumatların qorunması qanunu);
   - 3.2. Sübutların əldə edilməsi proseduru (Chain of Custody): sübutların qorunması qaydaları;
   - 3.3. Ekspert hesabatlarının hazırlanması: məhkəmə üçün hesabatların yazılması və ekspert şahidi kimi fəaliyyət göstərilməsi üzrə təlim.
4. *Praktiki iş*. Təcrübə zamanı bir çox universitetlər (məsələn, Birminhemdəki Alabama universitetləri) məzun olmaq üçün hüquq-mühafizə orqanlarında və ya özəl şirkətlərdə təcrübə keçmək məcburidir. Diplom layihəsi hazırlayarkan peşəkar proqram təminatından (EnCase FTK, Autopsy) istifadə edərək, real həyatda baş verən hadisə araşdırması işinin aparılması.

Şəkil 1. "Rəqəmsal Kriminalistika" istiqaməti üzrə tədris proqramların seqmentləri

B. Avropa universitetləri: multidissiplinar və hüquq yönümlü model

Avropada rəqəmsal kriminalistika proqramlarının strukturu Bolonya prosesi və akademik ənənələrlə sıx bağlıdır. Onlar daha çox multidissiplinar xarakter daşıyır, texniki bacarıqlar hüquq elmi ilə geniş inteqrasiya olunur. Avropa proqramları (xüsusilə Böyük Britaniya, Almaniya və Hollandiyada) metodların validasiyasına və keyfiyyət standartlarına (ISO) uyğunluğa diqqət yetirir.

Tədris proqramında kompüter şəbəkələri, rəqəmsal sübutların təhlili, rəqəmsal araşdırmaların hüquqi aspektləri və informasiya təhlükəsizliyi kimi fənlərə əhəmiyyətli dərəcədə diqqət yetirilir. Bu, cinayətkarlığın rəqəmsal transformasiyası kontekstində işləmək üçün zəruri olan hərtərəfli səriştələrin inkişafını təmin edir.

Tədris proqramlarının əsas xüsusiyyəti təcrübəyə yönəlmiş biliklərə diqqət yetirilməsidir. Avropa universitetlərindəki laboratoriya dərsləri, istintaq simulyasiyaları, real həyat təcrübələri hüquq-mühafizə orqanlarında və özəl şirkətlərdə təcrübə proqramlarını fəal şəkildə tətbiq edirlər. Bu kontekstdə, Europol kimi ixtisaslaşmış mərkəzlər və təşkilatlar təcrübə mübadiləsini və təhsil prosesində ən yaxşı təcrübələrin tətbiqini asanlaşdıraraq əhəmiyyətli rol oynayırlar [3].

Avropa modeli həmçinin təhsil və elmi tədqiqatlar arasında sıx əlaqə ilə xarakterizə olunur. Universitetlər Avropa Birliyi proqramları (məsələn, Horizon Europe və s.) tərəfindən maliyyələşdirilən beynəlxalq tədqiqat layihələrində fəal iştirak edirlər. Bu, süni intellekt, maşın öyrənməsi və böyük verilənlərin istifadəsi də daxil olmaqla rəqəmsal sübutların təhlili üçün innovativ metodların tətbiqini asanlaşdırır.

Avropa universitetlərində təlimin ilkin mərhələsi nəzəri və metodoloji bazanın formalaşdırılmasına yönəlib. Buraya rəqəmsal kriminalistikanın əsasları; rəqəmsal araşdırma metodları; rəqəmsal sübutlarla işləməyin hüquqi aspektləri; kibertəhlükəsizliyin əsasları daxildir. Kurslar rəqəmsal sübutların müəyyən edilməsi və toplanması, eləcə də onların bütövlüyünün təmin edilməsi (chain of custody), məhkəmədə sübutların qəbuledilməzliyi prinsiplərini əhatə edir. Bu kurslar istintaq prosesləri haqqında ümumi anlayışı inkişaf etdirir və mütəxəssisin işinin hüquqi düzgünlüyünü təmin edir.

Tədrisin növbəti səviyyəsi rəqəmsal kriminalistikanın müxtəlif sahələrinə yönəlmiş modulları əhatə edir:

- Kompüter kriminalistikası;
- Mobil kriminalistika;
- Şəbəkə trafiki və insidentlərin təhlili;
- Zərərli proqram təminatının təhlili;
- Bulud və IoT kriminalistikası.

Bu modullar fayl sistemləri və informasiya daşıyıcılarının təhlili, müxtəlif zaman intervallarında istifadəçi fəaliyyətinin təhlili, silinmiş məlumatların bərpası kimi mövzuları əhatə edir. Təlim həmçinin revers mühəndislik (reverse engineering) metodlarının tətbiqinə və rəqəmsal artefaktların şərhinə yönəldilir.

Təcrübəyə yönəlmiş laboratoriya dərsləri peşəkar alətlərdən istifadə edərək praktiki işlərin, tapşırıqların real şəraitdə yerinə yetirməyə və nümunə tədqiqatlarını təhlil etməyə yönəlmişdir. Tələbələr ixtisaslaşmış rəqəmsal kriminalistika laboratoriyalarında işləyir və avtomatlaşdırılmış analitika alətləri vasitəsilə müasir məlumat təhlili texnologiyalarını tətbiq edirlər.

Avropa universitetlərində təhsilə fənlərarası yanaşma sırf texniki təlimdən kənara çıxan tədrisi də əhatə edir. Bunlara aşağıdakılar daxildir:

- İstintaqın idarə edilməsi;
- Ünsiyyət və ekspertiza hazırlığı;
- Məhkəmədə sübutların təqdim edilməsi;
- Etika və məlumatların mühafizəsi.

Peşəkar fəaliyyətin vacib elementi olan hesabatların hazırlanması və ekspert kimi fəaliyyət göstərmə bacarıqlarına xüsusi diqqət yetirilir.

Rəqəmsal kriminalistika üzrə Avropada aparıcı universitetlərə ən qədim kriminalistika mərkəzi sayılan Lozanna Universiteti (UNIL) və Böyük Britaniyanın kriminalistika elmləri üzrə aparıcı olan Lester universitetləridir. Dublin universitetinin (İrlandiya) "Kibercinayətkarlıq araşdırmaları" CCI (Cybercrime Investigation) mərkəzinə dünyanın hər yerindən hüquq-mühafizə orqanlarının əməkdaşları təlim keçməyə gəlirlər. Halmstad Universiteti (İsveç) texniki aspektlərə və şəbəkə təhlükəsizliyinə böyük diqqət ayırır. Leiden universitetində (Hollandiya) "Kibertəhlükəsizlik" proqramı kriminalistika risklərin idarə edilməsi və hüquq istiqamətləri üzrə sıx bağlıdır.

C. Asiya universitetləri: milli təhlükəsizliklə sıx bağlı olan mərkəzləşdirilmiş model

Rəqəmsal iqtisadiyyatın sürətli inkişafı və kibertəhdidlərin artması bir çox Asiya ölkələri "Rəqəamsal kriminalistika" sahəsində mütəxəssislərin hazırlanmasını strateji prioritet hesab edir və bu istiqaməti kibertəhlükəsizlik proqramlarına inteqrasiya edir. Asiyada (əsasən Sinqapur, Cənubi Koreya və Çində) rəqəmsal kriminalistika proqramları güclü texniki biliklərə diqqət ayırır və hökumət təhlükəsizlik strukturları ilə sıx əlaqələrlə qurulur. Əsas xüsusiyyətlərdən biri təhsil proqramlarının təcrübəyə yönəlməsidir.

Asiyanın Şərqi və Cənub-Şərqi aparıcı universitetləri kibercinayətkarlıq istintaq ssenarilərini simulyasiya etmək üçün ixtisaslaşmış rəqəmsal kriminalistika laboratoriyalarından, kibertest poliqonlarından və simulyasiya mühitlərindən geniş istifadə edirlər. Sinqapur, Cənubi Koreya, Yaponiya və Çin kimi bir sıra ölkələrdə təhsil proqramlarının dövlət qurumları, özəl sektoru, o cümlədən informasiya təhlükəsizliyi və telekommunikasiya sahələrindəki şirkətlərlə aktiv inteqrasiyası mövcuddur. Əhəmiyyətli bir xüsusiyyət, bu sahədə təhsil siyasətinin dövlət dəstəyi və mərkəzləşdirilmiş şəkildə tənzimlənməsidir. Burada rəqəmsal kriminalistika proqramlarının strukturu texnika elmlərinə yönəlib və hökumət təhlükəsizlik strukturları ilə sıx əlaqələr ilə xarakterizə olunur.

Sinqapur Milli Universiteti (NUS - National University of Singapore) regionda ən yaxşı hesab edilir, onun proqramları "Ağıllı şəhər" təhlükəsizliyinə yönəlmişdir [4]. Koreya Universiteti (Cənubi Koreya) kriminalistika istiqaməti üzrə güclü ixtisasçılar hazırlayır, Tsinghua Universiteti (Çin) şəbəkə və sistem proqram təminatı təhlükəsizliyi üzrə dərin təlimlər keçirir. Burada, "Rəqəmsal kriminalistika" üzrə tədris proqramları çox vaxt "İnformasiya Təhlükəsizliyi" və ya "Kompüter Mühəndisliyi" fakültələrinə inteqrasiya olunur [5].

Əsas modullara aşağıdakılar aiddir:

- kiber kəşfiyyat və milli təhlükəsizlik (Cyber Defense) - kritik infrastrukturun qorunması üçün strategiyaların öyrənilməsi;
- haker qrupu fəaliyyətinin (APT hücumları) real-vaxt rejimində izlənməsi;
- kriptoqrafiya və kriptoanaliz - şifrələmənin riyazi əsasları və onu pozmaq üsulları.
- mikroprosessor və daxili sistemlərin arxitekturasının öyrənilməsi əsasında verilənlərinçip yaddaşına (IoT, avtomobil qurğuları) fiziki olaraq necə yazıldığını tədqiq etmək;
- cihaz proqram təminatında gizli zərərli funksiyaların aşkarlanması (Reverse engineering);
- aşağı səviyyəli proqramlaşdırma dillərindən (C/C++, Assembly) istifadə edərək qeyri-standart fayl sistemləri üçün xüsusi parserlərin (təhlil proqramlarının) yazılması.

Tətbiqi Kriminalistika sahəsinə aid aşağıdakı modullar aiddir:

- Mobil və bulud kriminalistikası. Smartfon brendlərinə və yerli bulud xidmətlərinə (WeChat, Samsung Cloud) diqqət yetirilməsi.
- Blokçeyn kriminalistikası. Xüsusilə Sinqapur və Honkonq kimi maliyyə mərkəzləri üçün aktual olan kriptovalyuta əməliyyatlarının təhlili.
- Böyük verilənlərin analizi (Big Data for Investigations). Böyük miqdarda ələ keçirilmiş məlumatlarda qanunauyğunluqları tapmaq üçün süni intellektdən istifadə.

Eyni zamanda, Asiya ölkələrində bir sıra problemli aspektlər hələ də qalmaqdadır. Bunlara ölkələr arasında və hətta ölkələr daxilində qeyri-bərabər təlim səviyyələri, inkişaf etməkdə olan bölgələrdə müasir avadanlıqlara məhdud çıxış və müvafiq praktik təcrübəyə malik müəllim heyətinin çatışmazlığı daxildir.

Aşağıda (Cədvəl 1) müxtəlif ölkələrdəki universitetlərdə "Rəqəmsal kriminalistika" fənni üzrə tədris proqramlarının fərqli xüsusiyyətləri qeyd edilmişdir.

CƏDVƏL I. RƏQƏMSAL KRİMİNALİSTİKA ÜZRƏ BEYNƏLXALQ TƏHSİL MODELLƏRİNİN MÜQAYİSƏSİ [6]

Regionlar	**Hazırlıq modeli**	**Təhsil proqramlarının əsas xüsusiyyətləri**	**Praktiki hazırlıq**	**Prioritet istiqamətlər**	**Əsas problemlər**
ABŞ	Praktiki yönümlü model	Rəqəmsal araşdırmalar, kompüter və şəbəkə kriminalistikası üzrə ixtisaslaşma	Forensik laboratoriyalar, simulyasiya edilmiş istintaq tapşırıqları, sənaye sertifikatları	Kibertəhlükəsizlik, rəqəmsal sübutların analizi, insidentlərə cavab	Texniki infrastrukturun yüksək maliyyə dəyəri və texnologiyaların sürətlə köhnəlməsi
Avropa	Hüquqi və tədqiqat yönümlü model	GDPR, məlumatların qorunması və beynəlxalq rəqəmsal ekspertiza standartlarına diqqət	Tədqiqat layihələri, case-study metodları, hüquq-mühafizə orqanları ilə əməkdaşlıq	Rəqəmsal hüquq, kriminalistik ekspertiza, məlumatların qorunması	Ölkələr arasında təhsil standartlarının fərqliliyi
Asiya	Texnologiya yönümlü model	Süni intellekt, Big Data və bulud texnologiyalarının tədrisə inteqrasiyası	Virtual laboratoriyalar və distant təhsil platformaları	Süni intellekt kriminalistikası, bulud kriminalistikası, kiberkəşfiyyat	Təcrübəli müəllim çatışmazlığı və proqram keyfiyyətində qeyri-bərabərlilik
Kanada və Avstraliya	Kompetensiya əsaslı model	Kibertəhlükəsizlik və rəqəmsal araşdırma bacarıqlarının formalaşdırılması	Virtual laboratoriyalar, təcrübə proqramları, hibrid təhsil	Kiber kriminalistika, şəbəkə araşdırması, rəqəmsal analitika	Tədris proqramlarının davamlı yenilənməsi ehtiyacı

III. AZƏRBAYCANDA RƏQƏMSAL KRİMİNALİSTİKA ÜZRƏ TƏHSILIN MÖVCUD VƏZİYYƏTİ VƏ İNKİŞAF PERSPEKTİVLƏRİ

Azərbaycanda kiber insidentlərin sayının artması, cinayət və mülki proseslərdə rəqəmsal sübutların yayılması və dövlət idarəçiliyinin rəqəmsallaşdırılması nəticəsində, elektron izləri axtara, qeyd edə, təhlil və şərh edə bilən mütəxəssislərə tələbatın artmasına səbəb olmuşdur. Buna görə də, rəqəmsal kriminalistika Azərbaycanda fəal şəkildə inkişaf edir və tədricən kibertəhlükəsizlik, hüquq-mühafizə orqanları və korporativ sektoru üçün kadr hazırlayan ayrıca bir təlim sahəsinə çevrilir.

Azərbaycanda bu ixtisaslaşma daha çox informasiya təhlükəsizliyi, kompüter elmləri və kibertəhlükəsizlik sahələrində fənlərarası bir istiqamət kimi inkişaf etdirilir. Ali təhsil müəssisələrində (Bakı Dövlət Universiteti, Polis Akademiyası, Azərbaycan Dövlət Neft və Sənaye Universiteti) "Kriminalistika", "Məhkəmə ekspertizası" və "İnformasiya təhlükəsizliyi" fənləri çərçivəsində rəqəmsal sübutların toplanmasını öyrədir [7]. Bu universitetlərdə bakalavr səviyyəsi olan tələbələr "Rəqəmsal Kriminalistika"nın əsaslarını "İnformasiya Təhlükəsizliyi" fənninin bir hissəsi olaraq öyrənirlər. Təhsilin üçüncü və dördüncü illərində xüsusi fənnlər təqdim olunur.

Magistr səviyyəsində bu istiqamət daha ətraflı şəkildə öyrədilir. İxtisaslaşma istiqamətləri formalaşır:

- rəqəmsal izlərin və sübutların müəyyən edilməsi;
- kibercinayətlərin araşdırılması, məlumatların bərpası;
- süni intellekt texnologiyalarının kriminalistikada tətbiqi.

Əsas təlim bölmələri bunlardır:

- *Şəbəkə təhlükəsizliyi.* Şəbəkə protokolları, şəbəkə trafikinin monitorinqi və müdaxilələrin aşkarlanması.
- *Kriptoqrafiya.* Buraya məlumatların şifrələnməsinin əsasları və informasiya təhlükəsizliyi metodları daxildir.
- *Əməliyyat sistemlərin idarə edilməsi.* Windows Server və Linux-un (analiz üçün əsas platformalar) dərindən öyrənilməsi.
- *Rəqəmsal kriminalistikanın əsasları.* Sərt disklərdən (HDD/SSD) və USB sürücülərindən məlumatların çıxarılması metodları.
- *Kibercinayətkarlığın tədqiqi.* Rəqəmsal izlərin aşkarlaması üçün alqoritmlər.
- *Mobil kriminalistika.* Smartfon və bulud yaddaş məlumatları ilə işləmək.
- *Zərərli proqram təminatının təhlili.*

Azərbaycanda rəqəmsal kriminalistikanın inkişafında mühüm bir mərhələ kibertəhlükəsizlik sahəsində milli insan resurslarının inkişaf etdirilməsinə yönəlmiş "Azərbaycan Kibertəhlükəsizlik Mərkəzi"nin (Azerbaijan Cybersecurity Center) yaradılması oldu. Mərkəzin proqramlarına insidentlərə cavab (Incident Response) və rəqəmsal kriminalistika (Digital Forensics) kimi istiqamətlər daxildir ki, bu da rəqəmsal kriminalistikanın tətbiqi ilə peşəkar ixtisaslaşma kimi tanınmasını nümayiş etdirir. Mərkəz laboratoriya və simulyasiya əsaslı təlimlərdən istifadə edir ki, bu da kriminalistika mütəxəssislərinin hazırlanması üçün xüsusilə vacibdir.

Universitetlərin informasiya təhlükəsizliyi laboratoriyaları da əlavə rol oynayır. Məsələn, Bakı Mühəndislik Universiteti ixtisaslaşmış laboratoriyada tələbələr üçün insidentlərə cavab vermə, loq fayllarının təhlili və rəqəmsal kriminalistika üzrə praktik təlimlər keçirir. Bu, nəzəri təlimdən rəqəmsal insidentlərin araşdırılmasında və peşəkar məlumat təhlili alətləri ilə işləməkdə praktik tətbiqlərə keçidi nümayiş etdirir.

Təhlillər göstərir ki, Azərbaycanın rəqəmsal kriminalistika üzrə tədris proqramları Asiya modelinə daha yaxındır

(hökumətin güclü rolu və infrastrukturun qorunmasına yönəlib), lakin bunlarda beynəlxalq tərəfdaşlıqlar vasitəsilə Qərb metodları aktiv tətbiq edilir.

Buna baxmayaraq, rəqəmsal kriminalistikada ixtisaslaşmanın inkişafı bir sıra məhdudiyyətlərlə üzləşir. Bunlara praktiki kriminalistika təcrübəsi olan müəllimlərin çatışmazlığı, tədris materiallarının və lisenziyalı proqram təminatının məhdudluğu, universitetlərin hüquq-mühafizə orqanları ilə kifayət qədər inteqrasiya etməməsi daxildir. Bundan əlavə, tədris proqramları yeni çağırışlara uyğunlaşdırılmalıdır, mobil kriminalistika, bulud hesablamaları, IoT cihazları, kriptoaktivlər və süni intellekt tətbiq olmalıdır.

Azərbaycanda rəqəmsal kriminalistikanın bakalavr və magistr səviyyələrində yeni ixtisas proqramları tətbiq olmalıdır, laboratoriya imkanları genişləndirilməlidir, sənayenin iştirakı ilə təlimin tətbiqi və təhsil standartlarının beynəlxalq təlim modelləri ilə uyğunlaşdırılmalıdır.

NƏTİCƏ .

Məqalənin nəticələri göstərir ki, rəqəmsal texnologiyaların sürətli inkişafı və kiberməkanda baş verən cinayətlərin artması rəqəmsal kriminalistika sahəsində peşəkar mütəxəssis hazırlığını strateji əhəmiyyətli istiqamətə çevirmişdir. Aparılmış təhlil əsasında müəyyən olunmuşdur ki, mövcud təhsil proqramları bir sıra hallarda müasir kibertəhlükəsizlik çağırışlarına tam cavab vermir və praktik yönümlü kompetensiyaların formalaşdırılması baxımından yenilənməyə ehtiyac duyur.

Xüsusilə rəqəmsal sübutların toplanması, emalı və təhlili üzrə praktiki bacarıqların inkişaf etdirilməsi üçün laboratoriya əsaslı tədris modelinin geniş tətbiqi vacib hesab olunur. Dövlət və özəl qurumların sürətlənmiş rəqəmsallaşması, kibercinayətkarlığın artan halları və məhkəmə proseslərində elektron sübutların geniş istifadəsi yüksək ixtisaslı yeni nəsil mütəxəssislərə tələbat yaradır.

Tədqiqat nəticəsində aydın olmuşdur ki, rəqəmsal kriminalistika üzrə kadr hazırlığında əsas problemlər sırasında texniki bazanın məhdudluğu, müasir proqram və avadanlıqların çatışmazlığı, ixtisaslaşmış müəllim kadrlarının azlığı və təhsil proqramlarının beynəlxalq standartlarla kifayət qədər inteqrasiya olunmaması xüsusi yer tutur. Bununla yanaşı, tədris prosesində hüquqi, etik və texnoloji aspektlərin kompleks şəkildə əlaqələndirilməməsi mütəxəssislərin peşə hazırlığına mənfi təsir göstərən amillərdən biridir.

Araşdırma göstərir ki, Azərbaycanda bu sahədə təhsilin keyfiyyətinin yüksəldilməsi üçün universitetlər, dövlət qurumları və özəl sektor arasında əməkdaşlığın gücləndirilməsi mühüm əhəmiyyət daşıyır. Eyni zamanda, beynəlxalq sertifikatlaşdırma proqramlarının tətbiqi, simulyasiya və virtual laboratoriyaların yaradılması, eləcə də süni intellekt və böyük verilənlər texnologiyalarının tədris prosesinə inteqrasiyası rəqəmsal kriminalistika üzrə müasir və rəqabətqabiliyyətli kadr hazırlığının formalaşdırılmasına imkan yarada bilər.

Beləliklə, rəqəmsal kriminalistika üzrə effektiv təhsil sisteminin qurulması yalnız kibercinayətkarlığa qarşı mübarizənin gücləndirilməsinə deyil, həm də informasiya təhlükəsizliyinin təmin olunmasına, rəqəmsal cəmiyyətin dayanıqlı inkişafına və milli təhlükəsizlik potensialının artırılmasına mühüm töhfə verir. Azərbaycanda rəqəmsal kriminalistika təhsili əhəmiyyətli inkişaf potensialına malikdir və dövlətin kiber dayanıqlığı üçün insan resursları təmin edə bilən müstəqil və tələbatlı sahəyə çevrilə bilər.

ƏDƏBİYYAT

[1] E.Oliveirajr, A,F. Zorzo "Review and agenda of Digital Forensics education and training", Forensic Science International, Volume 378, February 2026, https://doi.org/10.1016/j.forsciint.2025.112655

[2] S. McCullough, S. Abudu, E. Onwubuariri, I. Baggil, "Another brick in the wall: An exploratory analysis of digital forensics programs in the United States", Forensic Science International: Digital Investigation Electronics, Volume 37, 2021,

https://doi.org/10.1016/j.fsidi.2021.301187

[3] European Cybersecurity Organization, "European cybersecurity education and professional training: minimum reference curriculum", 2022, https://ecs-org.eu/ecso-uploads/2022/12/2022_SWG5.2_Minimum_Reference_Curriculum_final_v3.0.pdf

[4] M. Cavada, M.R. Tight, C.D. Rogers, "A smart city case study of Singapore—Is Singapore truly smart? In Smart City Emergence", Elsevier: Amsterdam, The Netherlands, 2019, pp. 295–314.

[5] H. Guo, J. Hou "Review of the accreditation of digital forensics in China", Forensic Sciences Research, 2018, https://www.tandfonline.com/loi/tfsr20

[6] M. Stigall & K.R. Cho. Digital forensics education: challenges and future opportunities. National Cyber Summit (NCS) Research Track 2021, Lecture notes in networks and systems (volume 310), pp 28–46.

[7] http://law.bsu.edu.az/az/content/cnayt_hququ_v_krmnologya_kafedrasi__292.

Training of Specialists in Digital Forensıcs and Educational Problems

Firudin Aghayev[1], Gulara Mammadova[2]

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

[1]*agayevinfo@gmail.com*,[2]*gyula.ikt@gmail.com*

Abstract - The rapid development of digital technologies and the increase in the scale of crimes committed in cyberspace have made the training of specialized personnel in the field of digital forensics a strategic priority. The purpose of this article is to analyze the current state of the process of training personnel in digital forensics, identify problems in the education system and present ways to eliminate them on a scientific basis. The article examines the structure of educational programs of universities in developed countries in the direction of "Digital forensics", conducts a comparative analysis, and identifies their strengths and weaknesses. The study found that although many higher education institutions have programs in the direction of cybersecurity and digital forensics, the content of these programs has difficulty keeping up with technological innovations. As a result of the study, it is proposed that educational programs should be regularly updated, practically-oriented training methods should be expanded, and international experience should be studied and applied.

Keywords - digital forensics; curricula; comparative analysis; international experience; multidisciplinary approach.