

Rəqəmsal Məhkəmə Ekspertizasında Process Mining Texnologiyalarının Tətbiqi və İmkanları

Rəşad Nuriyev

Azərbaycan Respublikası Ədliyyə Nazirliyi Məhkəmə Ekspertizası Mərkəzi, Bakı, Azərbaycan
nuriyev.reshad@justice.gov.az

Xülasə— Rəqəmsal cinayətlərin strukturunun getdikcə mürəkkəbləşməsi və müxtəlif informasiya sistemlərindən əldə olunan böyük həcmli məlumatların kəskin artması, rəqəmsal ekspertiza sahəsində tətbiq edilən elmi-metodoloji yanaşmaların davamlı olaraq inkişaf etdirilməsini və yeni analitik metodların araşdırılmasını tələb edir. Təqdim olunan tədqiqat işi çərçivəsində, rəqəmsal kriminalistikanın qabaqcıl istiqamətlərindən biri olan Process Mining texnologiyasının elmi-nəzəri əsasları və onun ekspertiza icraatındakı potensial tətbiq imkanları fundamental səviyyədə təhlil edilmişdir. İnformasiya sistemlərinin fəaliyyət loqlarına əsaslanan modelləşdirmə prinsipləri vasitəsilə, proseslərin rəqəmsal modelinin qurulması və insidentlərin xronoloji ardıcılığının obyektiv bərpası metodologiyası tədqiq olunmuşdur. İşdə həmçinin, dağılmış rəqəmsal izlərin sisteməlik analizi və mürəkkəb texniki proseslərin vizuallaşdırılması kontekstində bu texnologiyanın təklif etdiyi elmi-metodoloji üstünlüklər və prosesual risk faktorları qiymətləndirilmişdir.

Açar sözlər— rəqəmsal məhkəmə ekspertizası; process mining; proseslərin intellektual analizi; hadisə jurnalları; hadisələrin rekonstruksiyası.

I. GIRIŞ

Müasir dövrdə rəqəmsal cinayətlərin xarakterinin mürəkkəbləşməsi və informasiya sistemlərindən əldə olunan verilənlərin həcmnin kəskin artması, rəqəmsal ekspertiza sahəsində mövcud olan elmi-metodoloji yanaşmaların davamlı olaraq araşdırılmasını tələb edir. Keçirilən tədqiqat işi çərçivəsində Process Mining texnologiyasının [1] rəqəmsal kriminalistikadakı nəzəri rolu və bu yanaşmanın elmi mahiyyəti təhlil edilmişdir.

Qeyd etmək zəruridir ki, ənənəvi rəqəmsal ekspertiza metodları [2] daha çox fərdi artefaktların, faylların və təhlil obyektlərinin statik vəziyyətini araşdırdığı halda, Process Mining hadisələrin xronoloji ardıcılığını və məntiqi inkişaf zəncirini vahid bir sistem modelində nəzərdən keçirməyi hədəfləyir. Təqdim olunan tədqiqatın əsas məqsədi — sözügedən texnologiyanın rəqəmsal ekspertiza sahəsinə elmi-metodoloji əhəmiyyətini diqqətə çatdırmaq, həmçinin aparılmış təhlillər əsasında müəyyən edilmiş müsbət tərəfləri və tətbiq risklərini bölüşməkdir.

Tədqiqatın strukturuna uyğun olaraq, bu texnologiyanın potensial imkanları üç əsas istiqamətdə qruplaşdırılmışdır. Həmin istiqamətlər aşağıdakılardır:

1. Ekspert tədqiqatlarında hadisələrin xronoloji rekonstruksiyası imkanları;

2. İnstitusional iş axınlarının proses analizi və daxili idarəetmənin optimallaşdırılması;
3. Ekspertiza prosesində qurumlararası rəqəmsal inteqrasiya və sənəd dövriyyəsinin təhlili.

II. EKSPERT TƏDQIQATLARINDA HADİSƏLƏRİN XRONOLOJİ REKONSTRUKSIYASI İMKANLARI

Hazırda rəqəmsal ekspertiza icraatında informasiya sistemlərindən toplanan hadisə qeydlərinin (Event Logs), reyestr dəyişikliklərinin və şəbəkə trafik xronoloji bərpası prosesi, yəni "hadisə rekonstruksiyası" daxili təcrübədə ekspertlər tərəfindən "əl ilə" həyata keçirilir. Tədqiqat obyektlərinin bütövlüyünü, orijinallığını və prosesual tələbləri tam qoruyaraq, xüsusi avtomatlaşdırılmış proqram vasitələrindən istifadə edilmədən də bu əməliyyat zəncirini uğurla bərpa etmək mümkündür və cari fəaliyyət məhz bu metodologiyaya söykənir.

Lakin elmi yanaşma baxımından Process Mining və ya proseslərin intellektual analizi metodunun bu fəaliyyətə verə biləcəyi əsas elmi üstünlük — fərqli sistemlərdən gələn dağılmış rəqəmsal izlərin müəyyən hadisə identifikatoru (Case ID) (məsələn, sessiya nömrəsi, IP ünvanı və ya istifadəçi identifikatoru) ətrafında strukturlaşdırılmasıdır.

Bu strukturlaşdırma xüsusilə böyük həcmli rəqəmsal məlumatların, o cümlədən mürəkkəb bank və maliyyə [3] dələduzluqlarının analizi zamanı anomaliyaların müəyyən edilməsində nəzəri üstünlüklər vəd edir. Məsələn, subyektin sistemə qanuni giriş etməsindən dərhal sonra məlumatın sürətinin çıxarılması və loq qeydlərinin silinməsi kimi əməliyyat ardıcılıqları bu metodologiya ilə modelləşdirildikdə, qanunsuz müdaxilənin və ya daxili təhdidlərin trayektoriyası daha anlaşıqlı sistem diaqramına çevrilir. Buradakı əsas xüsusiyyət, loqlar arasındakı gizli əlaqələrin vizuallaşdırılması imkanındır.

III. İNSTİTUSİONAL İŞ AXINLARININ PROSES ANALİZİ VƏ DAXİLİ İDARƏETMƏNİN OPTİMALLAŞDIRILMASI

Mövzunun ətraflı təhlili göstərir ki, Process Mining metodologiyasının tətbiq sahəsi təkcə fərdi ekspertiza materiallarının tədqiqi ilə məhdudlaşmır. Bu texnologiya, bütövlükdə ekspertiza qurumunun daxili institusional iş axınlarının və inzibati idarəetmə fəaliyyətinin analizi üçün də potensial qiymətləndirmə vasitəsi rolunu oynaya bilər.

Məlum olduğu kimi, ekspertiza icraatının rəsmi mərhələləri – materialların qəbulu, qeydiyyatı, ekspertin təyin edilməsi, laboratoriya şəraitində texniki tədqiqatların aparılması, ekspert rəyinin tərtibi və yekunda aidiyyəti üzrə göndərilməsi - daxili rəqəmsal kargüzərlik sistemlərində zaman möhürü ilə qeyd

alınır.

Bu daxili fəaliyyət loqlarının proses analizi metodları ilə elmi-statistik tədqiqi, idarəetmədə aşağıdakı sahələri aydın görməyə imkan yaradır:

- İcraatın gedişatında baş verən potensial ləngimələrin və struktur bölmələr arasındakı vaxt itkilərinin obyektiv şəkildə müəyyən edilməsi;
- Ekspertlərin real iş yükünün və mövcud laboratoriya resurslarının fəaliyyət loqlarına əsasən obyektiv təhlili;
- Ekspertiza müddətlərinin qanunvericiliklə müəyyən edilmiş rəsmi hədlərdə saxlanılması üçün daxili nəzarət mexanizminin elmi əsaslarla monitorinqinin həyata keçirilməsi.

IV. EKSPERTİZA PROSESİNDƏ QURUMLARARASI RƏQƏMSAL İNTEQRASIYA VƏ SƏNƏD DÖVRİYYƏSİNİN TƏHLİLİ

Tədqiqatın digər bir istiqaməti isə Process Mining metodologiyasının daha geniş müstəvidə, yəni ekspertiza prosesində iştirak edən digər dövlət orqanları ilə qurulan qarşılıqlı iş əlaqələrinə yönəlib. Məlumdur ki, ekspertizaya təqdim olunan materialların və rəylərin hərəkət trayektoriyası təkcə bir idarə daxilində bitmir; burada ekspertizanın təyin edən orqanlar [2] (məhkəmə və istintaq qurumları), icraçı ekspertiza strukturu və yekun ekspert rəyinin göndərildiyi digər aidiyyəti dövlət qurumları iştirak edir.

Bu dövlət qurumları arasındakı rəsmi rəqəmsal sənəd dövriyyəsinin loq məlumatları Process Mining prinsipləri ilə analiz edildikdə:

- Cinayət mühakiməsi icraatında rəqəmsal sübutların və materialların ötürülməsi zəncirinin (chain of custody) tamlığına və təhlükəsizliyinə makro səviyyədə nəzarət edilməsi;
- İdarələrarası rəsmi yazışmaların və sorğuların icra operativliyinin obyektiv meyarlarla ölçülməsi və bürokratik gecikmələrin profilaktik məqsədlə aradan qaldırılması üçün elmi-analitik bazanın formalaşdırılması mühüm proqnozlar sırasındadır.

V. NORMATİV-HÜQUQİ MÜSTƏVİ VƏ PROSESSUAL ADAPTASIYA TƏLƏBLƏRİ

Aparılan elmi tədqiqatın ən prinsiplər tərkibi — bu innovativ texnologiyanın hüquqi, normativ və prosesual meyarlarla uzlaşdırılmasıdır. Nəzərə alınmalıdır ki, Azərbaycan Respublikasının müvafiq qanunvericiliyi [4] ekspert fəaliyyəti və sübutların əldə olunması prosesinə dair olduqca imperativ tələblər müəyyən edir. Rəqəmsal sübutların məhkəmədə mötəbərliyi, tamlığı və toxunulmazlığı prinsipləri əsas prioritet hesab olunur.

Bu baxımdan, Process Mining kimi qabaqcıl avtomatlaşdırılmış alətlərin birbaşa ekspertiza metodologiyasına inteqrasiya edilməsi, ilk növbədə, onların daxili prosesual qanunvericiliyə tam adaptasiyasını və müvafiq metodoloji standartların formalaşdırılmasını tələb edir.

Hazırda daxili imkanlarla, xüsusi kriminalistik proqram təminatları və sınaqdan keçmiş manual metodlarla həyata

keçirilən araşdırmalar mövcud hüquqi prinsipləri və təhlükəsizlik tələblərini tam şəkildə təmin edir. Lakin bu, sözügedən texnologiyanın gələcək potensialını istisna etmir; əksinə, bizə hüquqi və texniki tənzimləmələrin hansı istiqamətdə təkmilləşdirilməsi olduğunu göstərən bir inkişaf istiqamətlərini müəyyən etməyə imkan verir.

NƏTİCƏ

Yekun olaraq Qeyd etmək olar ki, Process Mining rəqəmsal kriminalistika sahəsində gələcək inkişaf tendensiya və rəqəmsal izlərin sistemli analizini anlamaq üçün perspektivli elmi yanaşmadır. Bu texnologiya, ənənəvi statik ekspertiza metodologiyasını dinamik və proses yönümlü bir müstəviyə daşımaqla rəqəmsal ekspertiza icraatının effektivliyini keyfiyyətcə yeni mərhələyə qaldıra bilər.

Aparılan tədqiqat göstərir ki, yaxın gələcəkdə zəruri hüquqi-normativ baza təkmilləşdirildikdə, rəqəmsal sübutların toxunulmazlığı prinsipləri tam qorunmaqla müvafiq daxili metodologiyalar qurulduqca, "proseslərin intellektual analizi" fəlsəfəsi rəqəmsal ekspertizanın elmi-nəzəri əsaslarının zənginləşməsinə əhəmiyyətli elmi töhfələr vermək potensialına malikdir. Prosesual qanunvericiliyin tələblərinə tam adaptasiya olunmuş rəqəmsal modellərin yaradılması, gələcəkdə ekspert rəylərinin elmi mötəbərliyini yüksək səviyyədə gücləndirəcəkdir.

Bu texnologiya, xüsusilə böyük həcmli verilənlərlə iş zamanı, mürəkkəb maliyyə və bank dələduzluqlarının və daxili sistem müdaxilələrinin araşdırılmasında analitik baxış bucağımızın genişlənməsinə, gizli loq əlaqələrinin aşkarlanmasına və bütövlükdə ekspertiza idarəçiliyinin daxili iş axınlarının rəqəmsal optimallaşdırılmasına çox ciddi elmi-praktiki töhfələr verə bilər. Nəticə etibarilə, Process Mining rəqəmsal kriminalistikada sadəcə texniki bir alət deyil, həm də hüquq-mühafizə fəaliyyətində analitik fəaliyyətin və institusional idarəetmənin elmi əsaslarla təkmilləşdirilməsi elmi əsaslarla təkmilləşdirilməsi üçün mühüm strateji baza rolunu oynayır.

ƏDƏBİYYAT

- [1] W. Van der Aalst, Process Mining: Data Science in Action. Berlin, Germany: Springer, 2016, doi: 10.1007/978-3-662-49851-4.
- [2] "Məhkəmə ekspertizası fəaliyyəti haqqında" Azərbaycan Respublikasının Qanunu
- [3] R. Nuriyev, Bank dələduzluqlarının araşdırılmasında rəqəmsal ekspertizanın xüsusiyyətləri. DOI: <https://doi.org/10.64498/KYTP5030>
- [4] Azərbaycan Respublikasının cinayət-prosesual məəcəlləsi.

Application and Capabilities of Process Mining Technologies in Digital Forensic Investigation

Rashad Nuriyev

Forensic Science Centre of the Ministry of Justice of the Republic of Azerbaijan, Baku, Azerbaijan
nuriyev.reshad@justice.gov.az

Abstract- The increasing complexity of digital crimes and the sharp rise in the volume of data obtained from various information systems require the continuous development of scientific and methodological approaches and the exploration of new analytical methods in digital forensics. Within the scope of this research work, the theoretical foundations of Process

Mining, one of the advanced directions in digital forensics, and its potential application opportunities in forensic practice are analyzed at a fundamental level. Based on modeling principles derived from information system event logs, the methodology for building digital process models and objectively reconstructing the chronological sequence of incidents is investigated. The paper also evaluates the scientific and

methodological advantages as well as procedural risk factors offered by this technology in the context of systematic analysis of scattered digital traces and visualization of complex technical processes.

Keywords- digital forensics; process mining; event logs; event reconstruction.