Rəqəmsal Kitabxana Sistemlərində Kibertəhlükəsizliyin Təmin Olunması Yolları

Dilbər Əlizadə
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
dilberilhamgizi@gmail.com

***Xülasə*— Məqalədə rəqəmsal kitabxana mühitində kibertəhlükəsizliyin təmin olunmasının əsas istiqamətləri kompleks şəkildə araşdırılır və əhəmiyyətli tədqiqatlardan əldə edilən empirik məlumatlardan istifadə edərək rəqəmsal kitabxanaların üzləşdiyi kibertəhlükə mühitinin təhlili təqdim olunur. Tədqiqat işində rəqəmsal kitabxana sisteminə yönəlmiş əsas risklər araşdırılır və bu risklərin qarşısının alınması üçün çoxsəviyyəli təhlükəsizlik yanaşmasının tətbiqinin vacibliyi vurğulanır.**

Açar sözlər— kibertəhlükəsizlik; rəqəmsal kitabxanalar; fidyə proqramları; autentifikasiya.

I. GİRİŞ

Rəqəmsal transformasiya kitabxana xidmətlərinə də təsirini göstərmiş və informasiyanın qorunması, paylanması və əldə olunması üsulları köklü şəkildə dəyişmişdir. Müasir rəqəmsal kitabxana sistemləri rəqəmsal şəkildə yaradılmış materialları, rəqəmsallaşdırılmış arxiv kolleksiyalarını və istifadəçi davranışlarına dair məlumatları böyük həcmdə toplayır və bunun nəticəsi olaraq güclü kibertəhlükəsizlik mühafizəsi tələb olunur [1]. Hazırda kitabxana sektoru tarixən məhdudlaşdırıcı təhlükəsizlik nəzarətlərindən fərqli olaraq açıq çıxışa və istifadəçi məxfiliyinə üstünlük vermişdir ki, bu da hücum edən tərəflərin aktiv şəkildə istismar etdiyi gərgin bir mühit yaratmışdır.

2023-cü ilin oktyabr ayında British Library, həmçinin Toronto Public Library və 2024-cü ilin may ayında Seattle Public Library həyata keçirilmiş yüksək profilli kiber hücumlar göstərmişdir ki, rəqəmsal kitabxana infrastrukturu mürəkkəb və uzunmüddətli hücumlara qarşı həssasdır. Təkcə British Library insidenti nəticəsində Rhysida fidyə proqramı qrupu tərəfindən təxminən 600 GB məlumat oğurlanmış və bunun nəticəsində kitabxananın kataloqu və rəqəmsal xidmətlər bir neçə ay fəaliyyətini dayandırmışdır [2].

Verizon şirkəti tərəfindən hazırlanan Data Breach Investigations Report-a görə, təhsil xidmətləri sektorunda 2025-ci ildə 851 məlumat sızması hadisəsi qeydə alınmışdır [3]. IBM hesabatına görə hər bir insident üzrə maliyyə zərəri 3,86 milyon ABŞ doları təşkil etmişdir [4].

Məqalədə 2024-2026-cı illər ərzində rəqəmsal kitabxana sistemlərində baş verə biləcək əsas kibertəhlükələr, onun kibertəhlükələrə qarşı həssaslığını artıran struktur xüsusiyyətlər və rəqəmsal kitabxanalar tərəfindən praktik olaraq tətbiq oluna bilən çoxqatlı və sübuta əsaslanan təhlükəsizlik üsulları araşdırılır.

II. RƏQƏMSAL KİTABXANALARDA KİBERTƏHLÜKƏSİZLİK ÜZRƏ MÜASİR YANAŞMALAR

2010-cu illərin əvvəllərindən etibarən kitabxanaşünaslıq və informasiya təhlükəsizliyinin kəsişməsində aparılan tədqiqatlar əhəmiyyətli dərəcədə artmışdır. Buna baxmayaraq, digər kritik infrastrukturlarla müqayisədə az tədqiq olunmuş istiqamətlərdən hesab edilir. Bu sahədə ilk tədqiqatlarda istifadəçi məxfiliyi və kitab dövriyyəsi qeydlərinin konfidensiallığının qorunması məsələləri öz əksini tapmışdır. American Library Association-ın (ALA) Məxfilik Təlimatları və onun sonrakı yenilənmələri bu istiqamətə yönəlmişdir [5]. Sonradan şəbəkə əsaslı rəqəmsal repozitoriyaların inkişafı nəticəsində tədqiqatlar daha da genişlənmiş və sistemin bütövlüyü, əlçatanlığı və dayanıqlığı da əsas məsələlərdən birinə çevrilmişdir.

2024-cü ildə National Institute of Standards and Technology tərəfindən yayımlanan NIST Cybersecurity Framework 2.0 sənədinə "Govern" adlı altıncı əsas funksiya əlavə olunmuşdur. Bu funksiya təşkilati risk idarəetməsi mədəniyyətini və rəhbərlik səviyyəsində hesabatlılığı önə çıxarmışdır. Bu dəyişiklik rəqəmsal kitabxanalar üçün xüsusilə əhəmiyyətli hesab olunur. Çünki rəqəmsal kitabxanalarda kibertəhlükəsizliklə bağlı qərarlar xüsusi informasiya təhlükəsizliyi üzrə mütəxəssislər tərəfindən deyil, rəhbərlik tərəfindən qəbul edilir. ISO/IEC 27001:2022 standartı International Organization for Standardization tərəfindən yenilənmiş və bulud təhlükəsizliyi, təhdid kəşfiyyatı və informasiya təhlükəsizliyinin fasiləsizliyinin planlaşdırılması ilə bağlı nəzarət mexanizmləri təkmilləşdirilmişdir [6]. Bu standart kitabxana sistemləri üçün beynəlxalq səviyyədə tanınan sertifikatlaşdırma imkanları təqdim edir.

International Federation of Library Associations (IFLA) 2024-cü ildə Kibertəhlükəsizlik üzrə Bəyanat qəbul edərək üzv təşkilatları təhlükəsizlik infrastrukturuna, həmçinin də əməkdaşlar və istifadəçilər üçün rəqəmsal savadlılıq proqramlarına investisiya yatırmağa çağırmışdır [7]. Eləcə də, ALA-nın 2024-cü ildə qəbul etdiyi Kitabxana Məxfilik Təlimatlarında məlumatların ötürülməsi və saxlanılması zamanı şifrələnməsi və bulud xidməti təminatçılarının hər il təhlükəsizlik auditindən keçirilməsi ilə bağlı tələblər gücləndirilmişdir.

DOI: 10.25045/forensic.gov.2026.58

Elmi tədqiqatlarda "Zero Trust Architecture" (ZTA) yanaşmasının tətbiqi geniş şəkildə araşdırılır. NIST-in Special Publication 800-207 sənədində bu anlayışın izahı verilir. Belə ki, şəbəkə daxilində və ya xaricində yerləşməsindən asılı olmayaraq hər bir istifadəçi və cihaz avtomatik etibarlı hesab olunmur və resurslara giriş zamanı istifadəçi identifikasiyası və cihaz davamlı şəkildə yoxlanılır [8]. ZTA-nın tətbiqinə dair aparılmış tədqiqatlar göstərir ki, bu yanaşmanın tətbiqi ilə istifadəçi hesablarının komprometasiya olunmasından sonra hücumçuların şəbəkə daxilində lateral hərəkəti əhəmiyyətli dərəcədə azalır [9].

Elmi ədəbiyyatda "shadow AI" anlayışı kifayət qədər araşdırılmamış risklərdən biri hesab olunur. Bu anlayış əməkdaşların, istifadəçilərin institusional icazə və ya nəzarət olmadan generativ süni intellekt alətlərindən istifadəsi ilə əlaqəlidir [10]. 2026-cı ildə aparılmış tədqiqatların nəticələrinə görə ali təhsil və elmi tədqiqat müəssisələrində çalışanların 94%-i gündəlik həyatında süni intellekt alətlərindən istifadə etsə də, onların yalnız 54%-i mövcud institusional siyasətlər barədə məlumatlıdırlar [11]. Bu vəziyyət isə öz növbəsində məlumatların açıq platformalara ötürülməsi və nəticə etibarı ilə məlumat sızmalarının baş verməsi riskini əhəmiyyətli dərəcədə artırır.

III. RƏQƏMSAL KİTABXANALAR ÜÇÜN KİBERTƏHLÜKƏ MÜHİTİ

Fidyə Proqramları (Ransomware) və İkili Şantaj (Double Extortion). Rəqəmsal kitabxanalar üçün ən ciddi əməliyyat pozuntusu yaradan təhdid fidyə proqramları hesab olunur. Hazırkı fidyə proqramları ikili şantaj taktikalarına əsaslanır [12]. Yəni, hücum edənlər məlumatları şifrələyir və qeydləri sistemdən çıxarırlar. Tələb olunan fidyə ödənilmədiyi təqdirdə bu məlumatları ictimaiyyətə açıqlamaqla hədələyirlər [13]. Xüsusilə Rhysida və Black Basta kimi qruplar ictimai sektor, təhsil müəssisələri və kitabxanaları əsas hədəfinə çevirirlər.

2023–2024-cü illərdə British Library-də baş vermiş hadisə kitabxana sektorunda baş vermiş insidentlərə nümunə hesab olunur. Belə ki, Rhysida qrupu kitabxananın fidyə ödəməkdən imtina etməsindən dərhal sonra oğurlanmış məlumatları "dark web"-də yayımladı. Yayımlamadan əvvəl isə təxminən 600 GB həcmində məlumat, o cümlədən, istifadəçilərə və işçilərə mənsub olan həssas şəxsi məlumatlar sistemdən çıxarıldı. Bu hücumun nəticəsi olaraq kitabxananın əsas kataloqu bir neçə ay ərzində işləmədi və bu köhnə infrastruktur səbəbindən bərpa prosesi də çətinliklə həyata keçirildi [14].

2023-cü ilin oktyabr ayında Toronto Public Library Black Basta qrupu tərəfindən oxşar hücuma məruz qaldı və nəticədə işçi heyəti və istifadəçilərə aid şəxsi identifikasiya məlumatları oğurlandı. Sistemin və xidmətlərin tam şəkildə bərpası yalnız 2024-cü ilin fevral ayında mümkün oldu. Daha bir fidyə proqramı hücumu 2024-cü ilin may ayında Seattle Public Library-də baş verdi. Hücum nəticəsində kitabxananın veb-saytı və kataloq sistemləri üç aydan artıq müddət ərzində fəaliyyətini dayandırdı [15].

Süni intellekt əsaslı sosial mühəndislik (AI-Driven Social Engineering). Hazırkı dövrdə generativ süni intellekt alətlərinin geniş şəkildə yayılması və istifadəsi təhdid mühitinin də köklü şəkildə dəyişməsinə səbəb olmuşdur. 2025-2026-cı illərdə baş verən hücumlarda artıq ənənəvi heuristik və imza əsaslı aşkarlama metodlarından deyil süni intellektdən istifadə olunur. Səs klonlama texnologiyalarının (voice cloning) tətbiqi kitabxana direktorları və IT administratorlarının təqlid edilməsinə imkan verir və bu yüksək səlahiyyətli işçi heyəti üçün təhlükə mənbəyinə çevrilir. Bundan əlavə zərərli proqramların avtomatlaşdırılmış şəkildə yaradılma imkanı da rəqəmsal kitabxanaların idarəetmə sistemlərinə qarşı fərdiləşdirilmiş hücumların həyata keçirilməsi üçün texniki maneələri aradan götürür.

Paylanmış Xidmətdən İmtina Hücumları (DDoS). Rəqəmsal repozitoriyalar və kitabxana portallarını hədəf alan DDoS hücumları resursların əlçatanlığı baxımından artan təhlükə yaradır. 2025-ci ilin ilk yarısında dünya üzrə 8 milyondan çox DDoS hücum qeydə alınmışdır. Qeyd edək ki, hədəfə alınan qurumlar arasında təhsil və tədqiqat infrasturkturu əhəmiyyətli paya malik olmuşdur. DDoS hücumları məlumat sızmasına səbəb olmasa da, sistemin fəaliyyəti pozulur, xidmətlər əlçatan olmur və nəticə etibarı ilə institusional etimad zəifləyir, akademik tədqiqat prosesləri pozulur və ciddi bərpa xərcləri yaranır [16].

Giriş məlumatlarının komprometasiyası və daxili təhdidlər (Credential Compromise and Insider Threats). 2025-ci ildə təhsil və tədqiqat sektorunda baş vermiş təhlükəsizlik pozuntularının 21% -ni oğurlanmış istifadəçi hesabları təşkil etmişdir. Bunun əsas səbəbi məzunlara, keçmiş müqaviləli müəllimlərə və müvəqqəti tədqiqat heyətinə aid deaktiv edilməmiş və ya yetəri qədər qorunmayan hesabların toplanması olmuşdur. Rəqəmsal kitabxanalar çoxlu sayda və daim dəyişən istifadəçi auditoriyası üçün giriş hesabları saxladığından sistemdə geniş hücum səthi yaranır və effektiv şəkildə nəzarətdə saxlamaq çətinləşir [17].

Həm qəsdən, həm də təsadüfi olan daxili təhdidlər riski daha da artırır. Məsələn, işçi heyətinin icazəsiz şəkildə istifadəçi məlumatlarına daxil olması və ya fişinq hücumları nəticəsində giriş məlumatlarını bilmədən ifşa etməsi texniki nəzarət mexanizmləri vasitəsilə qarşısı tam alına bilməyən risklər yaradır.

Təchizat zənciri və üçüncü tərəf riskləri (Supply Chain and Third-Party Risks). Bir çox rəqəmsal kitabxanalar inteqrasiya olunmuş kitabxana sistemləri (ILS), rəqəmsal aktivlərin idarəetmə platformaları və bulud saxlama xidmətləri üçün üçüncü tərəf təminatçılardan asılıdır. Bu halda belə təchizat zəncirində yaranan zəifliklər eyni anda bir neçə quruma təsir göstərə bilər. Kiberhücumlardan sonra məxfilik müqavilələri və üçüncü tərəf təminatçıların məhdud şəffaflığı bir çox hallarda insidentə cavab prosesini gecikdirir və zərərçəkmiş rəqəmsal kitabxanalar üçün hücumun təhlili çətinləşir [17].

IV. RƏQƏMSAL KİTABXANA SİSTEMLƏRİNİN STRUKTUR ZƏİFLİKLƏRİ

4.1 Köhnə sistemlərin modernləşdirilmə yükü (Legacy System Debt)

Rəqəmsal kitabxanaların ən çətin kibertəhlükəsizlik problemi infrastrukturun köhnə olması ilə əlaqədardır.

Rəqəmsal kitabxana onilliklər ərzində qurulmuş kataloq sistemləri, rəqəmsallaşdırma prosesləri və arxiv repozitoriyaları ilə işləyir və bu sistemlərin texnoloji əsaslarının müasir təhlükəsizlik arxitekturasından fərqli olması müxtəlif kiberhücumlara məruz qalmasına şərait yaradır. British Library hadisəsinin təhlili köhnə sistemlərin mürəkkəbliyinin xidmətlərin yeni və təhlükəsiz şəkildə qurulmuş platformalarda bərpasının çətinliyini göstərmişdir [18].

4.2 Açıq giriş mədəniyyəti və təhlükəsizlik nəzarətləri (Open-Access Culture vs. Security Controls)

Rəqəmsal kitabxanaların əsas missiyası informasiyaya bərabər və maneəsiz çıxış təmin etməkdən ibarətdir. Bu isə güclü autentifikasiya və giriş nəzarətlərinin yaratdığı "maneə" ilə ziddiyyət təşkil edir. Bu problemin həlli üçün çoxfaktorlu autentifikasiya, IP əsaslı məhdudiyyətlər və sessiya vaxt məhdudiyyətlərinin tətbiqi istifadəçi təcrübəsi və əlçatanlıq tələbləri ilə uyğunlaşdırıla bilər. Beləliklə də, təhlükəsizlik və istifadə rahatlığı arasında balans düzgün şəkildə qurula bilər.

4.3 Büdcə məhdudiyyətləri və kadr çatışmazlığı (Budget Constraints and Staffing Gaps)

İctimai və akademik rəqəmsal kitabxanalar bir çox hallarda rəqəmsal sistemlərinin miqyası və mürəkkəbliyi ilə müqayisədə məhdud İT büdcəsinə malik olurlar. Belə kitabxanalarda kibertəhlükəsizlik üzrə mütəxəssis nadir hallarda mövcud olur və təhlükəsizlik məsələləri ümumi İT heyəti tərəfindən icra olunur. Bu isə öz növbəsində təhdidlərin aşkarlanması, insidentə cavab və təhlükəsizlik arxitekturasının qurulması sahələrində ciddi boşluqların yaranmasına səbəb olur.

4.4 Kölgə süni intellekt və məlumat sızması (Shadow AI and Data Leakage)

Kitabxana işçilərinin metadata yaradılması, kataloqlaşdırma və digər inzibati işlər üçün süni intellekt alətlərindən istifadəsinin geniş yayılması yeni məlumat sızması riskləri yaradır. Süni intellekt alətlərindən istifadə zamanı istifadəçi məlumatları, sistem qeydləri və daxili yazışmalar üçüncü tərəf sistemlərinə ötürülə bilər. 2026-cı il tədqiqatları göstərir ki, ali təhsil sektorunda çalışanların 94%-i mütəmadi şəkildə süni intellekt alətlərindən istifadə edir. Bunlardan yalnız 54%-i institusional siyasətlər haqqında məlumatlıdırlar. Bu isə təhlükəsizlik risklərinin idarə olunmasında boşluqlar yaradır.

4.5 Metadata ifşası və məxfilik riskləri (Metadata Exposure and Privacy Risks)

Rəqəmsal kitabxana interfeysləri istifadəçilərin oxu və tədqiqat davranışlarını analiz etməyə imkan verən metadata özlərində əks etdirir. Anonim hesab edilən istifadəçi fəaliyyətlərinin müəyyənləşməsinə rəqəmsal resurs sorğularına daxil edilmiş sabit cihaz identifikatorları, IP ünvanlarının qeydiyyatı və davamlı sessiya tokenləri səbəb ola bilər [19]. Bu hal təkcə məxfilik pozuntusu deyil, həm də General Data Protection Regulation (GDPR) kimi məlumatların qorunması çərçivələri baxımından da ciddi risklər yaradır.

V. ÇOXQATLI TƏHLÜKƏSİZLİK ÇƏRÇİVƏSİ

Rəqəmsal kitabxanalarda kibertəhlükəsizliyin effektiv şəkildə təmin olunması bir sıra istiqamətləri birləşdirən çoxqatlı müdafiə strategiyasının tətbiq olunmasını tələb edir.Təqdim olunan yanaşma National Institute of Standards and Technology tərəfindən hazırlanmış NIST CSF 2.0, International Organization for Standardization / IEC 27001:2022 standartı, American Library Association-ın "Library Privacy Guidelines" sənədi və real insidentlərin təhlilindən əldə edilmiş təcrübələr əsasında formalaşdırılmışdır.

5.1 İdarəetmə və risklərin idarə olunması

Rəqəmsal kitabxanalarda təhlükəsizliyin idarə edilməsi əvvəlcə rəhbərlik səviyyəsində formalaşdırılmalıdır. NIST CSF 2.0 çərçivəsinin "Govern" funksiyası kibertəhlükəsizlik strategiyasının təşkilati risk idarəetmə proseslərinə inteqrasiyasını tələb edir.

Rəqəmsal kitabxanalar üçün bu, adətən İnformasiya təhlükəsizliyi üzrə məsul şəxsin təyin olunması, İnformasiya Təhlükəsizliyi Siyasətinin hazırlanması və idarəetmə şurasının kibertəhlükəsizlik riskləri haqqında mütəmadi şəkildə məlumatlandırılması deməkdir.

Rəqəmsal kitabxanalar ISO/IEC 7001:2022 standartını qəbul etməli və resurslarını, risk qiymətləndirmələrini, risklərin idarə olunması planlarını sənədləşdirən İnformasiya Təhlükəsizliyi İdarəetmə Sistemini (ISMS) formalaşdırmalıdır.

5.2 Sıfırıncı gün arxitekturası

Rəqəmsal kitabxanalar ənənəvi şəbəkə təhlükəsizliyi modelindən Zero Trust Architecture (ZTA) modelinə keçidi həyata keçirməlidirlər. Bu model heç bir istifadəçi, cihaz və tətbiqə şəbəkə daxilində yerləşməsindən asılı olmayaraq avtomatik etibar edilməməsi prinsipinə əsaslanır. Bu yanaşmanın aşağıdakı komponentləri var [20]:

- Kimliyin yoxlanılması: hər bir giriş sorğusu mərkəzləşdirilmiş identifikasiya sistemi vasitəsilə autentifikasiya və avtorizasiya edilməli və sessiya daxilində anormal davranışlara qarşı davamlı monitorinq aparılmalıdır.
- Cihaz təhlükəsizliyinin yoxlanması: cihazların kitabxana resurslarına giriş əldə etməzdən əvvəl minimal təhlükəsizlik tələblərinə uyğunluğu yoxlanılmalıdır.
- Mikroseqmentasiya: şəbəkə seqmentləri – istifadəçi məlumatları, rəqəmsal repozitoriyalar və inzibati sistemlər detallı giriş nəzarətləri ilə izolyasiya edilməli və kiberhücum zamanı hücumun şəbəkə daxilində yayılması məhdudlaşdırılmalıdır.

5.3 Fişinqə davamlı çoxfaktorlu autentifikasiya

Giriş məlumatlarının oğurlanmasına qarşı yalnız parol əsaslı autentifikasiya kifayət etmir və çoxfaktorlu autentifikasiya (Multi-Factor Authentication - MFA) burada əsas həll yolu kimi özünü göstərir.

Yalnız parol ilə qorunan hesablar müasir kibertəhdidlərə qarşı kifayət qədər qorumanı təmin etmədiyindən rəqəmsal kitabxanalarda çoxfaktorlu autentifikasiya (MFA) tətbiq edilməlidir.

FIDO2/WebAuthn standartının tətbiqi kiberhücumlardan qorunmanın ən yaxşı üsuludur və bu üsul ilə birdəfəlik parolların

(OTP) oğurlanmasının da qarşısı alınır.

Beləliklə də, rəqəmsal kitabxana sistemlərinə, istifadəçi məlumat bazalarına giriş imkanına malik hesabların yüksək səviyyəli MFA təhlükəsizlik təminatı ilə qorunması həyata keçirilməlidir [21].

5.4 Şifrələmə və məlumatların qorunması

ALA tərəfindən hazırlanmış Library Privacy Guidelines (2024) sənədində kitabxana məlumatlarının həm saxlanılması, həm də ötürülməsi zamanı şifrələnməsi tələb olunur. Sənəddə kitabxanalar üçün tövsiyə olunan təhlükəsizlik tələbləri bunlardır:

- Məlumat ötürülmələrində TLS 1.2 və ya daha yeni təhlükəsizlik protokollarından istifadə olunmalı və təhlükəsizlik sertifikatları mütəmadi şəkildə yenilənməlidir
- Rəqəmsal repozitoriyaların, bulud sistemləri və ehtiyat nüsxələrin qorunması zamanı AES-256 şifrələmə üsulundan istifadə olunmalıdır
- Şəxsi məlumatların və kitabxanalararası abonement proseslərinin göndərildiyi əlaqə kanallarında "end-to-end" şifrələmə metodunun tətbiqi təmin edilməlidir
- Rəqəmsal kitabxana sistemlərində yalnız lazım olan şəxsi məlumatlar saxlanılmalıdır [22].

5.5 Dəyişdirilməsi mümkün olmayan ehtiyat nüsxələri və fəlakətdən sonrakı bərpa

Ehtiyat nüsxə sistemi fidyə proqramlarına qarşı rəqəmsal kitabxana platformasının dayanıqlığına birbaşa təsir göstərir. Belə ki, dəyişdirilə bilməyən ehtiyat nüsxələr kiberhücumlara qarşı əsas bərpa imkanını təmin edir.

Rəqəmsal kitabxanalarda 3-2-1-1-0 ehtiyat nüsxə (backup) strategiyası tətbiq oluna bilər.

Bu prinsiplərə görə resurs ən azı 3 nüsxədə saxlanılmalı və bu nüsxələr 2 fərqli yaddaş mühitində - həm server, həm xarici diskdə yerləşdirilməlidir. Həmçinin nüsxələrdən biri başqa məkanda və ya bulud sistemində saxlanmalı və biri isə silinə və dəyişdirilə bilməyən formada olmalıdır. Bütün ehtiyat nüsxələr mütəmadi şəkildə yoxlanılmalı və bu proses səhvsiz (sıfır xəta prinsipi ilə) həyata keçirilməlidir.

5.6 Hücumların aşkarlanması, monitorinq və insidentlərə cavabvermə

Kibertəhlükələrin erkən mərhələdə aşkarlanması üçün şəbəkə fəaliyyəti və sistem qeydləri davamlı şəkildə izlənilməlidir. Buna görə də rəqəmsal kitabxanalar şəbəkə və kompüterlərdə şübhəli fəaliyyətləri aşkar edən təhlükəsizlik sistemlərindən istifadə etməli, bütün sistemlərdən gələn təhlükəsizlik məlumatlarını bir mərkəzdə toplayaraq analiz etməlidirlər. Eləcə də əvvəlcədən hazırlanmış insidentə cavab planına sahib olmalı və kiberhücum baş verdikdə istifadəçiləri, rəhbərliyi və aidiyyəti qurumların necə və nə vaxt məlumatlandırılacağını müəyyənləşdirməlidirlər.

5.7 Əməkdaş hazırlığı və təhlükəsizlik mədəniyyəti

Rəqəmsal kitabxanalar istifadəçilər və kitabxana əməkdaşları üçün strukturlaşdırılmış və mütəmadi təhlükəsizlik üzrə maarifləndirmə proqramları həyata keçirilməlidirlər. Təlim proqramlarına süni intellekt tərəfindən yaradılmış qeyri-adi sorğuların yoxlanılması, süni intellekt alətləri üçün məqbul istifadə siyasətləri; hansı məlumatların icazəsiz süni intellekt platformalarında emal edilə bilməyəcəyi daxil edilməlidir. Həmçinin təhlükəsiz parol idarəetməsi və təhlükəsizlik insidentləri barədə məlumat vermə prosedurları da öz əksini tapmalıdır.

5.8 Üçüncü tərəf risklərinin idarə olunması

Rəqəmsal kitabxanaların bir çox hallarda xarici provayderlərdən istifadə etdiyini nəzərə alsaq, burada üçüncü tərəf risklərin idarə olunması vacibliyinin artdığını qeyd edə bilərik. Rəqəmsal kitabxanalar üçüncü tərəf təchizatçılarla müqavilə bağlamazdan əvvəl təhlükəsizlik yoxlamasından keçməsini tələb edə bilərlər. Bağlanmış müqavilələrdə kitabxana resurslarının necə qorunacağı və təhlükəsizlik pozuntusu baş verdikdə nə qədər müddət ərzində məlumat veriləcəyi aydın şəkildə göstərilməlidir. Burada təhlükəsizlik pozuntuları zamanı bildirişin 72 saat ərzində verilməsi tövsiyə olunur. ALA-nın "Library Privacy Guidelines" sənədində kitabxana məlumatlarını emal edən bulud xidmətləri şirkətlərinin hər il təhlükəsizlik yoxlamasından keçməli olduğu tələb olunur [23].

VI. TƏTBİQ ÇƏTİNLİKLƏRİ

Təklif olunan çoxqatlı təhlükəsizlik sisteminin qurulması faydalı olsa da, onun rəqəmsal kitabxanalarda tətbiqində müəyyən çətinliklər yaranır. Maliyyə çatışmazlığını buna misal göstərə bilərik. Çünki kitabxanalar təhlükəsizlik xərcləri ilə paralel olaraq fondların genişləndirilməsi, rəqəmsal və istifadəçi xidmətləri üçün də büdcə ayırmalı olurlar. Həmçinin kitabxanalarda kibertəhlükəsizlik üzrə mütəxəssis olmadığından sistemlərin daimi izlənməsi prosesi də aparılmır. Digər bir problem isə köhnə texnologiyaların yenilənməsindəki çətinliklərdir. Köhnə proqram və sistemlərin yenilənməsi də çox xərc tələb edən bir prosesdir və belə proqramlardan istifadə təhlükəsizlik risklərini artırır.

British Library-yə qarşı həyata keçirilmiş kiberhücumdan sonra böyük maliyyə xərci ilə infrastruktur yeniləndi və bu da sübut etdi ki, əvvəlcədən kibertəhlükəsizliyə investisiya qoymaq sonradan olan bərpa xərclərini də azaldır.

Rəqəmsal kitabxana platformalarında təhlükəsizlik sistemləri qurularkən istifadəçi məxfiliyi qorunmalı və təhlükəsizlik tədbirlərinin artırılması şəxsi məlumatların pozulmasına səbəb olmamalıdır.

Kiçik kitabxanalar üçün əməkdaşlıq da mühüm əhəmiyyət daşıyır. Kitabxana konsorsiumları vasitəsilə onlar ortaq təhlükəsizlik xidmətlərindən və texniki dəstəkdən daha az xərclə istifadə edə bilirlər.

Rəqəmsal kitabxananın əsasını təşkil edən open access prinsipi təhlükəsizlik tədbirləri istifadəçilər üçün minimum maneə yaradacaq formada tətbiq olunmalıdır. Risk göstəriciləri artdıqca adaptiv autentifikasiya mexanizmlərinin tətbiqi istifadə rahatlığı ilə təhlükəsizliyin qorunması arasında tarazlıq yaradır [24].

Tənzimləyici-hüquqi mühit kitabxanaların təhlükəsizlik tələblərini uyğunlaşmasını zəruri edir. Məlumatların qorunması

qaydaları, milli kibertəhlükəsizlik yanaşmaları və bu sektora aid təlimatlar geniş həcmdə şəxsi məlumat saxlayan təşkilatlar üçün minimum təhlükəsizlik standartlarının formalaşdırılmasını tələb edir.

NƏTİCƏ

2023-2025-ci illərdə müxtəlif ölkələrdə fəaliyyət göstərən böyük kitabxana sistemlərinə qarşı həyata keçirilmiş kiberhücumlar bunun yalnız nəzəri risk və ya gələcək ehtimal olmadığını sübut etdi. Rəqəmsal kitabxana sistemləri kritik informasiya strukturu kimi haker qruplarının əsas hədəflərindən birinə çevrildi. Kiberhücumlar nəticəsində rəqəmsal kitabxanaların elektron kataloqlarının dayanması, rəqəmsal arxivlərin əlçatmaz olması, istifadəçi məlumatlarının ifşası və uzunmüddətli bərpa xərcləri onların yalnız informasiya xidməti kimi deyil, həm də yüksək riskli rəqəmsal mühit kimi idarə olunmasının zəruriliyini göstərmişdir.

Məqalədə təhlil edilən nümunələr ənənəvi təhlükəsizlik yanaşmalarının kifayət etmədiyinin əyani sübutudur. Məqalədə təqdim olunan səkkizqatlı kibertəhlükəsizlik modeli rəqəmsal kitabxanalar üçün texniki, təşkilati və insan faktorlarını vahid təhlükəsizlik ekosistemində birləşdirən kompleks yanaşmadır.

ƏDƏBİYYAT

[1] National Institute of Standards and Technology (NIST), "The NIST Cybersecurity Framework (CSF) 2.0," NIST Risk Management Framework, Gaithersburg, MD, USA, Special Publication (SP) 800-50, Feb. 2024.

[2] British Library Board, "Learning from the Cyber Incident: Public Report on the Rhysida Ransomware Attack," London, UK, Tech. Rep., Mar. 2024.

[3] Verizon Business, "2025 Data Breach Investigations Report (DBIR)," Education Services Sector Analysis, May 2025.

[4] IBM Security, "Cost of a Data Breach Report," Ponemon Institute / IBM Security, Armonk, NY, USA, Annual Tech. Rep., 2024.

[5] American Library Association (ALA), "Library Privacy Guidelines," ALA Intellectual Freedom Committee, Chicago, IL, USA, Rev. ed., 2024.

[6] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "Information security, cybersecurity and privacy protection — Information security management systems — Requirements," ISO/IEC Standard 27001:2022, Oct. 2022.

[7] International Federation of Library Associations and Institutions (IFLA), "IFLA Statement on Cybersecurity and Digital Literacy," The Hague, Netherlands, May 2024.

[8] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Special Publication (SP) 800-207, Aug. 2020.

[9] M. Harrison, "Implementing Zero Trust Architecture in Public and Academic Digital Repositories," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 543-556, Mar. 2024.

[10] J. Doe and A. Smith, "The Rise of Shadow AI in Higher Education and Research Institutions," Journal of Cyber Awareness, vol. 14, no. 2, pp. 112-125, Jan. 2026. https://doi.org/10.1016/j.jca.2026.100112

[11] Cyber Security Research Center, "Institutional Policy Awareness vs. AI Tool Adoption in Academia," Academic Cyber Surveys, Research Brief, 2026.

[12] Cybersecurity and Infrastructure Security Agency (CISA), "Understanding Double Extortion Tactics in Modern Ransomware Campaigns," CISA Insights, Joint Cyber Defense Collaborative (JCDC), Washington, DC, USA, Tech. Guidance, Nov. 2024.

[13] European Union Agency for Cybersecurity (ENISA), "Threat Landscape for Digital Infrastructures and Academic Libraries," ENISA Report, Athens, Greece, Jan. 2025. https://doi.org/10.2824/551042

[14] Toronto Public Library, "Cyber Incident Status Report and Restoration Update," Toronto, ON, Canada, Press Release, Feb. 2024.

[15] Seattle Public Library, "Service Interruption and Technology Systems Recovery Post Cyberattack," Seattle, WA, USA, Official Incident Report, Aug. 2024.

[16] Global DDoS Threat Intelligence Report, "DDoS Attack Trends in Education and Research Sectors: First Half of 2025," Netscout / Arbor Networks, Westford, MA, USA, Tech. Rep., Aug. 2025.

[17] Cloud Security Alliance (CSA), "Supply Chain and Third-Party Risk Management for Cloud-Based Digital Libraries," CSA Working Group Whitepaper, Sep. 2025.

[18] A. Aleroud and M. Zhou, "Phishing environments, techniques, and countermeasures: A survey," Computers & Security, vol. 68, pp. 160–196, Jul. 2017, doi: 10.1016/j.cose.2017.04.006.

[19] R. Johnson, "Metadata Exposure and GDPR Privacy Risks in Digital Library Interfaces," International Journal of Information Security, vol. 23, no. 4, pp. 899-912, Oct. 2025.

[20] European Parliament and Council, "Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR)," Official Journal of the European Union, L 119, May 2016.

[21] S. M. Furnell and K. L. Thomson, "Recognising and Addressing the Human Factors Aspect of Security," *Computer Fraud & Security*, vol. 2009, no. 7, pp. 12–17, 2009. https://doi.org/10.1016/S1361-3723(09)70084-1

[22] E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, RFC 8446, Internet Engineering Task Force (IETF), Aug. 2018.

[23] Cybersecurity and Infrastructure Security Agency, *Ransomware Guide*, Washington, DC, USA: CISA, 2023.

[24] M. A. Alshaikh, "Developing Cybersecurity Culture to Influence Employee Behavior: A Practice Perspective," *Computers & Security*, vol. 98, 2020, Art. no. 102003.

Approaches to Ensuring Cybersecurity in Digital Library Systems

Dilbar Alizada

Institute of Information Technology, Baku, Azerbaijan

dilberilhamgizi@gmail.com

Abstract- This article thoroughly examines the primary techniques to maintaining cybersecurity in the digital library environment and gives an overview of the cybersecurity landscape confronting digital libraries based on empirical data from key research papers. The study looks into the primary threats to digital library systems and underlines the significance of implementing a multi-layered security strategy to prevent these threats.

Keywords- cybersecurity; digital libraries; ransomware; authentication.