

UOT 004.9:351

İmamverdiyev Y.N.

AMEA İnformasiya Texnologiyaları İnstitutu

yadigar@lan.ab.az

IDEA4SP: E-KİTABXANALAR ÜÇÜN İNFORMASIYA TƏHLÜKƏSİZLİYİ MODELİ

Elektron kitabxanalar onlayn kitabxana-informasiya xidməti göstərən mürəkkəb informasiya sistemidir və belə sistemlər üçün informasiya təhlükəsizliyi və fərdi məlumatların konfidensiallığı kritik əhəmiyyət daşıyır. Məqalədə elektron kitabxanalarda informasiya təhlükəsizliyi problemlərini analiz etmək üçün IDEA4SP modeli təklif edilir və aktual problemlər bu modelin səviyyələri üzrə strukturlaşdırılır. Həmçinin elektron kitabxanalarda fərdi məlumatların təhlükəsizliyi və intellektual mülkiyyətin qorunmasına texnoloji yanaşmalar da analiz edilir.

Açar sözlər: elektron kitabxana, fərdi məlumatlar, informasiya təhlükəsizliyi, gizlilik, IDEA4SP.

Giriş

Elektron kitabxanalar (e-kitabxanalar) mürəkkəb kompüter və informasiya sistemlərinin inteqrasiyasıdır və informasiya təhlükəsizliyi onların layihələndirilməsində, qurulmasında və istismarında ən vacib problemlərdən biridir [1, 2].

E-kitabxanaların böyük miqyaslı kiberhücumların obyektı olması barədə faktlar hələlik geniş ictimaiyyətə məlum deyil. Bəzi müəlliflərə görə, bunun səbəbləri həm də ondadır ki, e-kitabxanalardan istifadə edənlərin sayı onlayn ödəniş sistemlərindən, sosial şəbəkələrdən və digər populyar veb resurslarından istifadə edənlərin sayından əhəmiyyətli dərəcədə azdır; kitabxana istifadəçilərinə aid verilənlərdə bədnüvətliyənin hədəfi olan bank (kredit kartı) məlumatları adətən olmur; insanların nə oxuduğu hakerlər üçün o qədər də qiymətli və cəlbədicə deyil [2, 3].

Lakin İnternetə qoşulmuş e-kitabxanalarda həmişə çoxsaylı təhlükəsizlik riskləri vardır – viruslar, troyanlar və digər zərərli proqramlar onlayn verilənləri və sənədləri məhv edə, təşkilatlara və şəxslərə məxsus verilənləri oğurlaya bilər. E-kitabxanalarda təhlükəsizlik boşluqları və onlardan istifadə edilərək həyata keçirilən kiberhücumlar nəticəsində icazəsi olmayan şəxslər informasiyanın konfidensiallığını və ya tamlığını poza bilərlər. Bu da, öz növbəsində, nəşirlərin və kontent provayderlərinin etimadını zəiflədə, e-kitabxana sahiblərinin nüfuzuna ziyan vura və hətta iqtisadi itkilərə səbəb ola, təcili tələb edilən informasiya əlyətərli olmadıqda narahatlığa və digər problemlərə gətirib çıxara bilər [4].

E-kitabxanalarla işləyən aktorların dəyişkən müxtəlifliyi səbəbindən bir çox təhlükəsizlik tələbləri nəzərə alınmalıdır və bu aktorların hər birinin təhlükəsizlik tələbləri fərqlidir [4, 5]. Məsələn, e-kitabxananın kontent provayderini intellektual mülkiyyət hüquqlarının qorunması və kontentin istifadəsi şərtləri, e-kitabxananın istifadəçisini isə kitabxanada saxlanan kontentə etibarlı giriş imkanları maraqlandıra bilər. Bu ehtiyaclar əsasında formalaşan təhlükəsizlik tələbləri bəzən ziddiyyət təşkil edir və bu e-kitabxanaların təhlükəsizlik arxitekturu daha da mürəkkəbləşdirir.

Ölkəmizdə müstəqillik illərində e-kitabxanaların yaradılması sahəsində bir sıra tədbirlər həyata keçirilmiş və müasir standartlara cavab verən, ən müasir texniki avadanlıqlarla təchiz olunmuş və beynəlxalq sistemlərə inteqrasiya olunmuş e-kitabxanalar formalaşdırılmışdır. Milli informasiya fəzasının vacib istiqaməti olan e-kitabxanaların informasiya təhlükəsizliyinin təmin olunması da diqqət mərkəzindədir [6-11].

Məqalənin məqsədi də məhz e-kitabxanalarda informasiya təhlükəsizliyi və fərdi məlumatların konfidensiallığı üzrə elmi-praktiki tədqiqatların müasir vəziyyətini analiz etmək və aktual tədqiqat istiqamətlərini müəyyən etməkdir.

E-kitabxanalar: kontent və servisləri

E-kitabxanalarla əlaqədar olan fəaliyyət sahəsi yetərinə yenidir və buna görə də hələlik sabitləşmiş terminologiyaya malik deyil. Kitabxanaların “elektronlaşdırılması” məsələsinə hələ 1980-ci illərin əvvəlində F.Lankaster tərəfindən ətraflı baxılmışdı [12]. Lakin onun işləri müəyyən dərəcədə futuroloji xarakter daşıyırdı.

E-kitabxanalar üzrə işlərdə əhəmiyyətli inkişaf 1990-cı illərdə baş vermişdir. Həmin vaxt müxtəlif növ informasiyanın, xüsusilə mətn informasiyasının etibarlı saxlanması, operativ emalını və effektiv istifadəsini təmin edən müvafiq hesablama texnikası vasitələri və informasiya texnologiyaları meydana çıxmışdı. Məhz həmin dövrdə bir sıra ölkələrdə e-kitabxana layihələri həyata keçirilməyə başlandı.

Bu işlərin gedişində "elektron kitabxana" anlayışı konkretləşməyə, onun məqsədləri, vəzifələri və funksiyaları dəqiqləşməyə başladı, lakin bu problemin birqiymətli yozumuna gətirib çıxarmadı. “Elektron kitabxana” anlayışının sinonimi kimi “rəqəmsal kitabxana” və “virtual kitabxana” kimi söz birləşmələrinə də rast gəlmək olur.

Biz baxılan sahədə iş təcrübəsinin analizinə əsaslanan aşağıdakı tərif üzərində dayanmağı məqbul hesab edirik [13]: “E-kitabxana – sistemin özündə yerləşən və ya telekommunikasiya şəbəkəsi vasitəsi ilə ona əlyətərli olan müxtəlif elektron sənəd kolleksiyalarını (mətn, təsvir, səs, video və s.) etibarlı saxlamağa və effektiv istifadə etməyə imkan verən informasiya sistemidir.”

İnformasiya resurslarının inteqrasiyası müxtəlif növ informasiyanın xassələri, təsvir xüsusiyyətləri və istifadəçinin onlarla işləmə imkanları saxlanmaqla istifadəsi məqsədlə birləşdirilməsi nəzərdə tutulur. Bu zaman resursların mütləq fiziki olaraq birləşdirilməsi tələb edilmir, bu virtual da ola bilər. Əsas odur ki, istifadəçinin əlyətərli informasiyanı vahid informasiya fəzası kimi qavraması təmin edilsin.

Effektiv naviqasiya istifadəçinin onu maraqlandıran informasiyanı bütün əlyətərli informasiya fəzasında ən az zəhmət çəkməklə tam və dəqiq şəkildə tapması imkanındır.

Müxtəlif informasiya resurslarının inteqrasiyası və bu resurslarda effektiv naviqasiya imkanları sayəsində e-kitabxanalar geniş çeşiddə kontentə və servislərə giriş təqdim edən onlayn sistemə çevrilir.

E-kitabxananın kontentinə verilənlər, verilənlərin müxtəlif aspektlərini təsvir edən metaverilənlər (təsvir tipi, yaradıcısı, sahibi, reproduksiya hüquqları və s.) və digər verilənlərə/ (meta-verilənlərə) olan istinadlar və münasibətlərdən ibarət olan metaverilənlər daxildir. E-kitabxana kontenti kitabxana kataloqu, rəqəmsal kolleksiya, abunə verilənləri bazası, elektron jurnallar, elektron sifarişlər, sənədlərin çatdırılması və s. əhatə edir.

E-kitabxana servislərinə açıq girişli onlayn kataloq (*Online Public Access Catalog, OPAC*), meta-axtarış, fərdi portal, kitab (məqalə) sifarişi, bələdçi, resursların axtarışı və s. daxildir.

Metaverilənlər resurs obyektlərinin intellektual və texniki atributlarını təsvir etmək üçün istifadə edilir. Bir çox rəqəmsal obyekt istifadəçiyə veb üzərindən birbaşa çatdırmaq olur, lakin bəziləri xüsusi tətbiqi proqram tələb edə bilər. Saxlanma təkcə bir təşkilat üzrə deyil, abunə və əməkdaşlıq vasitəsilə bütün dünya üzrə paylana bilər.

İnformasiya təhlükəsizliyi üçün *IDEA4SP* modeli

Son dövrlər tədqiqatçılar müxtəlif e-kitabxana modelləri təklif ediblər [14-19]. Kornell Universitetinin tədqiqatçıları *Dienst* adlanan e-kitabxana arxitekturu irəli sürmüşlər [16]. Bu arxitektura mərkəzləşməmiş, paylanmış kolleksiyaya İnternet girişi üçün protokol və onun reallaşmasını təmin edir. Avropa tədqiqatçıları tərəfindən e-kitabxanaları qurmaq üçün *DELOS* etalon modeli təklif edilmişdir [17]. *DELOS* etalon modeli e-kitabxanaların qurulmasına e-kitabxanalar sahəsində 6 əsas konsept: kontent, istifadəçi, funksionallıq, arxitektura, keyfiyyət və siyasət bucağından baxır. Digər modellərdə bu məsələyə fərqli baxışlar da vardır [18,19]. *5S* platforması rəqəmsal kitabxanaların spesifikasiyasına *5S* konstruksiya elementinin tərfi kimi baxır. Aşağıda hər bir ‘S’-in qısa təsviri verilir [19].

Streams (Axınlar) – e-kitabxanalarda saxlanan kontentlərin müxtəlif növlərini və onların formatlarını müəyyən edir. Kontent statik (məsələn, mətn məlumatları) və ya dinamik (məsələn, hərəkət edən obyektin *GPS*-koordinatları) ola bilər.

Structures (Strukturlar) – rəqəmsal obyektin strukturunu (bir tam kimi və ya hissələrini) əhatə edir. Məsələn, kitabı fəsilərə, bölmələrə, altbölmələrə, abzaslara strukturlaşdırmaq olar.

Spaces (Fəzalar) – obyektlər və onlar üzərində müəyyən məhdudiyətlərə tabe olan əməliyyatlar çoxluğu kimi müəyyən etmək olar, e-kitabxananın istifadəçi interfeysini və indeks axtarışı modelini təsvir edir.

Scenarios (Senarilər) – funksiyaları, əməliyyatları, tələbləri, servisləri və işləri əhatə edir. Vacib senarilərdən biri istifadəçi funksiyasını yerinə yetirmək üçün sistemin bütün mümkün istifadə yollarını təsvir etməkdir. Senarilər fəzalarda strukturlar vasitəsilə axınlarda nəyin baş verdiyini və cəmiyyətdə bu əməliyyatlar üçün kimin cavabdeh olduğunu təsvir edir.

Societies (Cəmiyyətlər) – “subyektlər çoxluğu və onlar arasındakı münasibətlər” kimi müəyyən edilə bilər. Subyekt dedikdə insanlar, aparat və proqram komponentləri nəzərdə tutulur.

İnformasiya təhlükəsizliyi baxımından istənilən kitabxananın üç əsas məqsədini müəyyən etmək olar 1) konfidensiallıq – e-kitabxana kontentinin avtorizasiyadan keçməyən istifadəçiyə açıq olmadığını bildirir; 2) tamlıq – informasiyanın təhrifsiz şəkildə mövcud olmasıdır, rəqəmsal obyektə (resursa) avtorizasiyadan keçməyən şəxs tərəfindən dəyişiklik edilə bilmədiyini göstərir; 3) əlyətərlilik – qanuni istifadəçinin tələb olunan informasiya xidmətini yolverilən vaxt ərzində alması imkanındır.

Bu modellərdə e-kitabxanaların qurulması zamanı mütləq nəzərə alınmalı olan informasiya təhlükəsizliyi məsələlərinə baxışlar məhduddur və ya tamamilə yoxdur. Yuxarıda qeyd edildiyi kimi, qurulmuş sistemə sonradan təhlükəsizlik modullarının əlavə edilməsi yetərli olmur, çünki bir sıra təhlükəsizlik tələbləri digər modullara dəyişiklikləri zəruri edə bilər və sistem inteqrasiyasında da əlavə problemlər yarada bilər. Buna görə də, təhlükəsiz e-kitabxanalar üçün formal modellər axtarmaq gərəkdir. Məqalədə e-kitabxanalarda informasiya təhlükəsizliyi məsələlərini strukturlaşdırmaq üçün *IDEA4SP* modeli təklif edilir. *IDEA4SP* (*Infrastructure, Digital Environment, Authentication, Access control, Authorization, Audit for Service and Privacy*) modeli aşağıdakı komponentlərdən ibarətdir:

Infrastructure (infrastruktur) – e-kitabxana mühitində kommunikasiyanın aparat və proqram təminatının təhlükəsizliyi, şəbəkə təhlükəsizliyi və veb təhlükəsizliyi məsələlərini əhatə edir.

Digital Environment (rəqəmsal mühit) – e-kitabxananın rəqəmsal kontentinin – verilənlərin və metaverilənlərin təhlükəsizliyi nəzərdə tutulur.

Növbəti 4A təhlükəsizlik servislərini əhatə edir.

Authentication (autentikasiya – “həqiqiliyin yoxlanılması”) vasitəsi ilə ikinci tərəf əmin olur ki, subyekt doğrudan da özünü qələmə verdiyi şəxsdir. Subyekt bildiyi nəyi isə (parolu, şəxsi identifikasiya nömrəsi, kriptografik açar), sahib olduğu nəyi isə (şəxsi kart və ya digər təyinatlı analogi qurğu) və ya özünün tərkib hissəsi olan nəyi isə (səs, barmaq izləri və s., yəni özünün biometrik xarakteristikalarını) aşağıdakı mənbələrdən ən azı birini təqdim etməklə özünün həqiqiliyini təsdiq edə bilər.

Authorization (avtorizasiya) – istifadəçilərin rəqəmsal obyektlər üzərində yetinə yetirə biləcəyi əməliyyatları (giriş hüquqlarını) müəyyən etməklə onlardan istifadə etməyə icazə verilməsidir.

Access control (giriş nəzarət) – resursun icazəsiz istifadəsinin qarşısını alır (yəni bu servis resursa kimin giriş hüququnun olduğuna, girişin hansı şərtlər altında baş verə bilməsinə, resursa giriş edənlərə nəyi etməyə icazə verildiyinə nəzarət edir). Giriş nəzarətin müxtəlif modelləri mövcuddur və giriş nəzarəti təmin etmək üçün bu modellərin hər birindən istifadə etmək olar [20].

Audit (audit) – e-kitabxana informasiya sistemində baş verən hadisələr haqqında məlumatın qeyd edilməsi, toplanması və toplanan informasiyanın analizi nəzərdə tutulur. İstifadəçilərin və

e-kitabxana heyətinin hesabat verməli olmasını təmin etmək, informasiya təhlükəsizliyini pozma cəhdlərinin aşkar olunması məqsədlərinə xidmət edir.

Service (servis) – e-kitabxana aktorlarının e-kitabxana servislərini necə yerinə yetirdiklərini və necə davranışlarını təsvir edir, e-kitabxana servislərinin təhlükəsizliyi (əlyetərliyi) məsələlərini əhatə edir.

Privacy (fərdi məlumatların konfidensiallığı) – e-kitabxana istifadəçilərinin fərdi məlumatların konfidensiallığını və yalnız istifadəçiyə bəyan edilmiş məqsədlərlə istifadəsi məsələlərini əhatə edir [21, 22].

E-kitabxanalarda informasiya təhlükəsizliyi təhdidləri

Avropa kitabxana veb-saytlarında veb-təhlükəsizlik problemləri [23]-də araşdırılmışdır. Veb-təhlükəsizlik skanerləri istifadə edilərək dörd ölkədə 80 kitabxananın veb-saytı təhlükəsizlik boşluqları baxımından analiz edilmişdir. Analizin nəticələri göstərmişdir ki, veb-saytların əksəriyyətində ciddi təhlükəsizlik boşluqları mövcuddur. Tədqiqat aşkar etmişdir ki, ölkələrin qanunvericiliyinin saytların təhlükəsizliyini tələb etməsinə baxmayaraq, kitabxanalar onlayn informasiya sistemlərinin təhlükəsizliyi üçün müvafiq tədbirlər görməmişlər. Təhlükəsizliyi təkmilləşdirmək üçün metodların bir neçə konkret nümunələri göstərilmişdir [23].

Sessiyaların ələ keçirilməsi də təhdidlərdən biridir, burada istifadəçi informasiyaya və ya servise icazəsiz giriş əldə etmək üçün sessiyadan istifadə edir. Bu, əsasən, məsafədəki serverlə autentifikasiya üçün istifadə edilən *HTTP* “kukilərinin” (verilənlər faylının) oğurlanması ilə həyata keçirilir. Burada autentifikasiya vacib mexanizm olsa da, sessiyanın başlanğıcında istifadəçini autentifikasiya etmək üçün yetərli deyil. Autentifikasiya sessiya boyunca davam etməlidir. Sessiyaların ələ keçirilməsinin qarşısını almaq üçün mexanizm kommunikasiya əlaqəsi quran subyektlər arasındakı trafikə şifrələnməsidir (məsələn, *SSL* protokolu istifadə edilməklə).

Rəqəmsal kontent nəşirlərinin və provayderlərinin hər bir rəqəmsal obyekt üçün təyin edilmiş müəyyən giriş hüquqları olmalıdır. Əsas təhlükəsizlik təhdidi kontentin açıqlanmasıdır, yəni rəqəmsal obyekt üçün təyin edilmiş giriş hüququnun şəxs tərəfindən pozulmasıdır. Bu verilənlərin konfidensiallığı təmin edilməlidir [20]. Verilənlərin şifrələnməsi konfidensiallığı təmin etmək üçün istifadə edilən mexanizmdir.

Digər təhlükəsizlik təhdidi verilənlərin modifikasiyasıdır. Giriş hüquqları müəyyən istifadəçilərə rəqəmsal obyektin kontentini modifikasiya etməyə icazə verməyə bilər. Bu halda, kontentdə istənilən dəyişiklik təyin edilmiş giriş hüquqlarının pozulması olacaq. Buna görə də, rəqəmsal obyektə edilmiş dəyişikliyi aşkarlamaq üçün verilənlərin tamlığına nəzarət mexanizmləri olmalıdır ki, onların modifikasiya edilmədən, autentifikasiya edilmiş subyekt tərəfindən göndərildiyi şəkildə alındığına zəmanət verilsin [20]. Verilənlərin tamlığını təmin etmək üçün müxtəlif üsullar mövcuddur, onlardan bəziləri heş-funksiyalar və məlumatları autentifikasiya kodlarıdır (ing. *message authentication codes – MAC*).

E-kitabxanada rəqəmsal kontentin və onun metaverilənlərinin icazəsiz açıqlanması təhlükəsizlik təhdidlərindən biridir. Bu hücumun qarşısını almaq üçün yuxarıda sadalanmış servislərdən hər birini müstəqil və ya bir neçəsini birlikdə istifadə etmək olar. Avtorizasiya e-kitabxana üçün arzulanan servisdır [24,25].

Digər təhlükəsizlik boşluğu kataloq verilənlərinin modifikasiyasıdır. Kataloq verilənlərində metaverilənlər haqqında bütün informasiya vardır; onun kontentində istənilən dəyişiklik bir sıra problemlər yarada bilər. Hücum edən müəyyən sənədlərin giriş hüquqlarını dəyişə, bu resursun sahibi tərəfindən təyin edilmiş giriş hüquqlarının pozulmasına səbəb ola bilər. Buna görə də, kataloq verilənlərinə edilmiş dəyişiklikləri aşkarlamaq üçün verilənlərin tamlığına nəzarət edilməlidir. Bunu heş-funksiyalar və ya *MAC* kodları istifadə etməklə təmin etmək olar.

Baş verə bilən digər hücum verilənlərin qanunsuz istifadəsidir. Hücum edən resursa qanuni yollarla giriş əldə edə bilər, bundan sonra verilənlərdən qanunsuz istifadə etməklə, məsələn, sənədin surətini çıxarmaqla öz imtiyazlarından sui-istifadə edə bilər. Bu hücumun qarşısını girişə nəzarət

etməklə və verilənlərə intellektual mülkiyyət hüquqlarını qorumaqla almaq olar. Kontentin müxtəlif məntiqi təhlükəsizlik hücumlarından qorunmasını və intellektual mülkiyyət hüquqlarına aid məsələləri təsvir etmək üçün “rəqəmsal hüquqların idarə edilməsi” (ing. *digital rights management, DRM*) terminindən istifadə edilir [26]. *DRM*-i təmin etmək üçün şifrələmə, parollar, rəqəmsal imzalar və su nişanları kimi texnologiyalar qrupu istifadə edilir [27].

Autentifikasiyadan yan keçilməsi də təhiddir. Hücum edən yalnız autentifikasiya edilən istifadəçilər üçün nəzərdə tutulmuş müəyyən hərəkətləri yerinə yetirə bilər. Bu qorunan informasiyanın açıqlanmasına və ya verilənlərin modifikasiyasına gətirə bilər. Autentifikasiyadan yan keçilməsinin qarşısını almaq üçün *Kerberos* və *X.509* autentifikasiya servislərindən istifadə edilə bilər, onlar verilənlərin mübadiləsi başlayana kimi istifadəçilərin identifikatorlarını yoxlayırlar [20].

Servis səviyyəsində *DoS*-hücumlar əsas təhdidlərdən biridir, bu hücumlar e-kitabxana servislərinin istifadəçilərə çatdırılmasının qarşısını almağa yönəlidir. Əylətilik informasiya təhlükəsizliyinin üç əsas aspektindən biridir və icazəsi olan istifadəçilərin istədikləri vaxt, istədikləri yerdən sistemə giriş əldə edərək onun xidmətlərindən istifadə etmələrinə imkan verən sistem xassəsidir. *DoS*-hücumların müxtəlif növləri vardır. Əks-tədbir mexanizmi şəbəkə administratorunun hücum edənin *IP* ünvanını müəyyən etməsi və onun şəbəkəyə girişini bağlamaqdan ibarətdir.

Maskarad da autentifikasiyaya hücumlardan biridir - bu zaman hücum edən öz şəxsiyyətini saxtalaşdıraraq özünü başqası kimi təqdim edir. Bu əsas problemdir, çünki müəyyən istifadəçilərin bəzi kontentlərə girişinə icazə verilə və digərlərinə belə hüquq verilməyə bilər. Əgər hücum edən özünü müəyyən kontentə giriş hüququ olan istifadəçi kimi təqdim edərsə, bu zaman obyektə giriş hüquqlarının pozulması baş verir. Autentifikasiya kommunikasiyada iştirak edən subyektin həqiqiliyini yoxlamağa və bununla da, maskaradın qarşısını almağa imkan verir. Maskaradın aşağı səviyyədə (*TCP/IP* modelinin şəbəkə səviyyəsində) bir növü *IP* ünvanlarının saxtalaşdırılmasıdır (ing. *IP spoofing*). *IP spoofing* zamanı saxta *IP* ünvanına malik şəbəkə paketləri yaradılır və konfidensial kontentə giriş əldə etməyə çalışılır. Paketlərin filtrlənməsi yolu ilə autentifikasiya *IP spoofing*-in qarşısını ala bilər.

Digər fərqli hücum imtiyazlardan sui-istifadə edilməsidir, bu halda istifadəçi rəqəmsal obyektə giriş hüquqlarını pozur. Bunun qarşısını girişə nəzarət mexanizmlərindən istifadə etməklə almaq olar [28].

E-kommersiya mühitində problemlərdən biri də istifadəçinin kommunikasiya faktını inkar etməsidir [29]. Bəzi e-kitabxanalar müəyyən informasiyaya giriş üçün ödəniş tələb edə bilərlər; ödəniş prosesi təhlükəsiz olmalı və istifadəçilər tərəfindən istənilən boyun qaçırma halının qarşısını almalıdır. Boyun qaçırmama arzulanan tələblərdən biridir, istifadəçinin hər bir tranzaksiyanı rəqəmsal imzalaması yolu ilə təmin edilə bilər. Ödəniş zamanı kommunikasiyanın emalını avtorizasiyadan keçmiş üçüncü tərəf yerinə yetirə bilər (məsələn, *PayPal* kimi).

E-kitabxanalarda fərdi məlumatların təhlükəsizliyi

İstifadəçilər e-kitabxana servislərinə giriş əldə etmək üçün öz adlarını, e-poçt ünvanlarını, telefon nömrələrini və identifikasiya edilə bilən digər fərdi məlumatlarını həvəslə təqdim edirlər. Bu informasiya hakerlərdən və bu məlumatları kitabxana ilə əlaqədar olmayan məqsədlərdə istifadə etmək istəyən digər şəxslərdən qorunmalıdır.

E-kitabxananın kitabxana müştərilərinin demoqrafik verilənlərindən başqa, aşağıdakı fərdi məlumatlarına da girişi vardır [30]:

- üzvlük faylları;
- müvəqqəti götürdüyü e-kitablar və məsləhət aldığı elektron nəşrlər haqqında məlumatlar;
- onlayn axtarış məlumatları;
- e-poçt loqları və digər İnternet fəaliyyəti;

- baş çəkilməmiş və yüklənmiş veb-səhifələr haqqında məlumatlar;
- yayım xidmətləri üçün istifadəçi profilləri;
- istifadəçilərin naviqasiya profilləri;
- informasiya sorğularının siyahıları və s.

Beləliklə, e-kitabxanalar öz istifadəçiləri barəsində böyük həcmdə ətraflı məlumat toplayıb arxivləşdirə bilər. Adətən, bu verilənlər kitabxana ilə fərd arasında konfidensial məlumat hesab edilir, lakin ona kommersiya təşkilatlarının, hüquq-mühafizə orqanlarının, güc strukturlarının və xidmətlərinin marketinqi üçün kitabxanaların özlərinin potensial marağı var. Tədqiqatlar göstərir ki, kitabxanalardan istifadə etdikdə istifadəçilərin konfidensiallıq barədə narahatlıqları aşağı səviyyədə olur. Onlar hesab edirlər ki, kitabxana fərdi məlumatları digər təşkilatlara verməyəcək. Kitabxanaçılar fərdi məlumatların konfidensiallığına, prinsipcə, peşə dəyəri kimi hörmət etsələr də, digər dəyərlərlə müqayisədə ona yüksək önəm vermirlər. Bundan başqa, kitabxanaların böyük əksəriyyəti verilənlərin qorunması üçün hazırlıqlı deyillər. Sorğu respondentlərinin təklifləri əsasında konfidensiallıq siyasətinin əsas prinsipləri müəyyən edilmişdir [30].

Amerika Kitabxanalar Assosiasiyası fərdi məlumatların təhlükəsizliyi ilə bağlı tələbləri hələ 1960-cı illərin əvvəlində Etika Kodeksində əks etdirmişdi [31]. Etika Kodeksinin 3-cü maddəsi geniş vəzifələr müəyyən edir (1995-ci il redaktəsi): “Biz hər bir kitabxana istifadəçisinin axtarılmış və ya alınmış informasiya üzrə və məsləhət alınmış, müvəqqəti götürülmüş, əldə edilmiş və ya ötürülmüş resurslar üzrə gizlilik və konfidensiallıq hüquqlarını qoruyuruq.”

Amerika Kitabxanalar Assosiasiyası 2002-ci ildə “Gizlilik və konfidensiallıq üzrə suallar və cavablar” adlı sənədi nəşr etmiş və onu 2014-cü ildə yenilənmişdir [32]. Sənəd kitabxanaların və kitabxana sistemlərinin konfidensial müştəri məlumatlarını necə emal etməli olduqları sahəsində gözləntiləri və ən yaxşı təcrübəni ortaya qoyur. Bu sənəd yüksək səviyyədə yazılıb, bütün növ kitabxana funksiyalarını əhatə edir (məsələn, heyət üçün qaydalar, gizlilik auditi, ümumi girişli kompüterlərdə konfidensiallıq), lakin *OPAC* və ya inteqral kitabxana sistemlərində fərdi məlumatların konfidensiallığı barədə, demək olar ki, danışılmır.

Kitabxanaçıların fərdi məlumatların təhlükəsizliyi sahəsində maarifləndirilməsi fərdi məlumatların təhlükəsizliyinin pozulması hallarının qarşısının alınmasına müsbət təsir göstərə bilər. Bu fərziyyə [33]-də kitabxanaçılarla fərdi məlumatlar üzrə aparılmış təlimdən əvvəl və təlimdən sonra keçirilmiş rəy sorğusu vasitəsilə qiymətləndirilir.

Rəqəmsal hüquqların idarə edilməsi

E-kitabxanaların yaratdığı problemlərdən biri də müəllif hüquqlarının yetərincə qoruna bilməməsidir. *DRM* kontenti şifrələməklə və onu rəqəmsal lisenziya ilə əlaqələndirməklə kontentə mülkiyyət hüququnun qorunmasını təmin edir. Lisenziya kontentə baxmağa icazə verilmiş istifadəçini identifikasiya edir, məhsulun kontent siyahısını göstərir, maşınla oxunan formatda olan resurs üzərində istifadəçinin malik olduğu hüquqları bildirir. Bu hüquqları, məhdudiyət və şərtləri göstərmək üçün *DREL* və *XrML* kimi nişanlama dilləri istifadə edilir [27].

Rəqəmsal hüquqların qorunmasını təmin etmək üçün aşağıdakı texnologiyalar və mexanizmlər istifadə edilir.

Şifrələmə. Simmetrik və asimmetrik (açıq açarlı) şifrələmə üsulları girişə nəzarəti təmin etmək üçün istifadə edilə bilər. Açıq açarlı şifrələmə ödəniş sistemlərində istifadə edilir, onlar kontentin kim tərəfindən və necə istifadə edilməsinə nəzarət edir.

Parollar. İstifadəçinin sistemdə qeydiyyatı zamanı yadda saxlanmış simvollar ardıcılığı giriş etmək istəyən istifadəçinin təqdim etdiyi simvollar ardıcılığı ilə üst-üstə düşməlidir.

Su nişanları. Mülkiyyət hüququnu göstərmək üçün simvollar və ya şəkillər əlavə edilir. Bu verilənləri audio, video və ya şəkil daxilində yerləşdirmək üçün steqanoqrafiya üsulları istifadə edilir.

Rəqəmsal imza. Adətən, rəqəmsal imza praktikada açıq açarlı kriptografiya ilə reallaşdırılır. Rəqəmsal imzanın yaradılması (yoxlanması) prosesində heş-funksiyalar istifadə edilir.

Rəqəmsal barmaq izləri. Rəqəmsal barmaq izləri rəqəmsal imzanın və su nişanlarının birgə istifadə edildiyi daha güclü metoddur. Kontent yaradıcısı hər bir istifadəçi üçün onun xüsusi nişanlanmış unikal nüsxəsini yaradır. Nişanlar istifadəçiyə özəl şəkildə yaradılır, buna görə onu “barmaq izi” adlandırırlar. Kontentin yaradıcısı bu nüsxələri tapmaq üçün axtarış robotlarından istifadə edə bilər.

Nüsxə aşkarlama sistemləri – axtarış sistemləri belə nüsxələnmiş obyektləri axtarmaq üçün istifadə edilə bilər. Nüsxə aşkarlayan brauzerlər də rəqəmsal kontentin mühafizəsinə kömək edə bilər.

Ödəniş sistemləri – müəyyən növ təhlükəsizlik texnologiyası hesab etmək olar, çünki istifadəçinin qeydiyyatını, kredit kartının autentifikasiyasını tələb edir, eləcə də kontent provayderi ilə müştəri arasında etimad münasibəti tələb edir. Ödəniş sistemlərinin quraşdırılması rəqəmsal kontenti qorumağa kömək edə bilər.

DRM-i təmin etmək üçün standart mexanizm yoxdur, bunun əsas səbəblərindən biri tənzimləmənin olmamasıdır. Buna baxmayaraq, bu sahədə kontentin idarə edilməsini təmin etmək və ədalətli istifadə siyasətlərini dəstəkləmək üçün müxtəlif sistemlər və protokollar mövcuddur. Beləliklə, rəqəmsal hüquqların idarə edilməsi ən vacib və mübahisəli məsələlərdən biridir, burada tədqiqatçıların və praktiklərin müzakirələri konsensusdan hələlik xeyli uzaqdır.

E-kitabxanalarda RFID texnologiyasının istifadəsi

RFID (ing. *Radio Frequency Identification* – radiotezlik identifikasiyası) kitabxanalarda da geniş istifadə edilməyə başlanmışdır. *RFID* vasitəsilə obyektləri avtomatik identifikasiya etmək, onların yerini müəyyənləşdirmək və hərəkətlərini izləmək mümkündür [35].

Kitabxanadakı hər bir nəşr vahidinə (kitab, jurnal və s.) radiosiqnalları qəbul edən və ötürən xüsusi *RFID* nişanı yapışdırılır. Bu nişan vasitəsilə onlar unikal elektron identifikasiya nömrəsi almış olurlar. Xüsusi cihaz (oxuyucu) həmin nişanı nəşr vahidinin qəbulu, verilməsi, çeşidlənməsi, inventarlaşdırılması, yerinin müəyyənləşdirilməsi zamanı istifadə edir.

RFID texnologiyasının köməyi ilə kitabxanada nəşr vahidlərinin yerini müəyyənləşdirmək, kitabların verilməsini və qəbulunu asanlaşdırmaq, inventarlaşdırma proseslərini sürətləndirmək, ədəbiyyatın oğurlanmasının və dəyişdirilməsinin qarşısını almaq, kitab verilməsini və qəbulunu kitabxanaçının iştirakı olmadan həyata keçirmək olar [35].

RFID-in kitabxanalarda istifadəsi gizliliklə bağlı bir sıra narahatçılıqlar yaradır [36, 37]. Bundan başqa, *RFID* nişanında toplanmış informasiya bədniiyyətli tərəfindən gizli dinləmə, izləmə, saxtalaşdırma, təkrarlama və xidmətdən imtina hücumları vasitəsilə sui-istifadə edilə bilər [38]. *RFID* texnologiyası hücum edənləri ilkin proqram kodunun, ümumi protokolların və qurğuların çox olması, verilənlər bazaları, qiymətli verilənlər və yanlış təhlükəsizlik baxışları səbəbindən cəlb edir.

RFID-lərlə bağlı identifikasiya edilmiş zərərli proqramların üç növü *RFID*-eksplotları, *RFID* soxulcanları və *RFID* viruslarıdır [39]. *RFID* eksplotlarında bədniiyyətli tərəfindən *RFID* teqinə eksplot yazılır, oxunan zaman eksplot oxuyucunun fon proqram təminatını yoluxdurur. Bu hücum, adətən, aşağı qiymətli *RFID* teqlərinə və kontaktsiz smart-kartlara yönəlir.

RFID soxulcanları şəbəkədə özü-özünü yayır, *RFID* teqlərini, e-poçtu, faylları və s. hədəfə alır. *RFID* servislərində təhlükəsizlik boşluqlarını onlayn istismar edir.

RFID virusları virus hücumunu yaymaq üçün yoluxmuş teq tələb edir. Bu viruslar vasitəsilə verilənlər bazalarına hücumlar edilir.

Nəticə

E-kitabxana qeyri-məhdud sayda oxucuya zamandan və məkandan asılı olmadan keyfiyyətli və daha dolğun informasiya xidməti göstərən açıq onlayn informasiya sistemidir. Bu tip kitabxananın ümumi istifadə üçün açıq olan lokal və məsafədə yerləşən paylanmış informasiya resursları həm kitabxananın mülkiyyəti olan rəqəmsal nəşr vahidlərindən, həm də kitabxana

tərəfindən ödənişli və ya mübadilə üsulu ilə alınmış elektron nəşrlərdən ibarətdir. Müxtəlif növlü, tipli və məzmunlu bu elektron sənədlərin İnternet üzərindən məsafədən etibarlı, təhlükəsiz və intellektual mülkiyyət hüquqları qorunmaqla istifadəsi vacib məsələdir. Eyni zamanda, kitabxana istifadəçilərinin fərdi məlumatlarının gizliliyi də müxtəlif təhdidlərdən qorunmalıdır. Bu məqsədlə məqalədə e-kitabxanalarda informasiya təhlükəsizliyi və fərdi məlumatların konfidensiallığı üzrə elmi-praktiki tədqiqatların müasir vəziyyətini analiz edilmiş və bu sahədə bir sıra aktual tədqiqat istiqamətləri müəyyən edilmişdir.

Ədəbiyyat

1. Arms W.Y. Digital Libraries. – Cambridge, MA: The MIT Press, 2000, 304 p.
2. Al-Suqri M. Afzal W., Digital age: Challenges for libraries // Information, Society and Justice, 2007, vol. 1, no. 1, pp. 43-48.
3. Fox E., ElSherbiny N. Security and digital libraries. Digital Libraries - Methods and Applications. K.H.Huang (Ed.), InTech, 2011, pp. 151-160,
<http://www.intechopen.com/books/digital-libraries-methods-and-applications/security-and-digital-libraries>
4. Anday A., Francese E., et al. Information security issues in a digital library environment: A literature review // Bilgi Dünyası, 2012, vol. 13, no. 1, pp. 117-137.
5. Hadow K. Data security for libraries: Prevent problems, don't detect them // Feliciter, 2009, vol. 55, no. 2, pp. 50.
6. Azərbaycan Respublikasında kitabxana-informasiya sahəsinin 2008-2013-cü illərdə inkişafı üzrə Dövlət Proqramı, 6 oktyabr 2008-ci il,
http://www.e-qanun.az/alpdata/framework/data/15/c_f_15493.htm
7. Xələfov A.A. Müstəqillik illərində Azərbaycanda kitabxanaşünaslığın inkişafı // AMEA MEK-in Elmi əsərləri, 2010, №11, s.3-31.
8. Əliyeva-Kəngərli A. Elektron kitabxanaların inkişafı dünya və Azərbaycan təcrübəsi, problemlər, perspektivlər // AMEA MEK-in Elmi əsərləri, 2004, № 5, s.3-11.
9. Cəfərov C.A. Kitabxana-informasiya xidmətində elektron kataloq. Bakı: Proqres, 2012, 224 s.
10. Əliquliyev R.M., Məmmədov E.Ç. İnteqral kitabxana sistemləri və elektron kitabxanaların qarşılıqlı inteqrasiyasının bəzi məsələləri // Təhsildə İKT, 2011, №3, s.4-10.
11. Kərimova S.H. Kommersiya tipli tammətnli verilənlər bazalarının formalaşması, xüsusiyyətləri və problemləri // İnformasiya cəmiyyəti problemləri, 2012, №2 (6), s. 64-74.
12. Lancaster F.W. Libraries and librarians in the age of electronics. Arlington, VA: Information resources press, 1982, 229 p.
13. Антопольский А.Б., Вигурский К.В. Концепция электронных библиотек // Электронные библиотеки, 1999. Т. 2. Вып. 2, <http://www.elbib.ru/index.phtml?page=elbib/rus/journal/1999/part2/antopol>
14. Kruk S., McDaniel B. Semantic Digital Libraries. Springer Verlag. 2008, 245 p.
15. Baruzzo A., Casoto P., Challapalli P., Dattolo A., Pudota N., Tasso C. Toward semantic digital libraries: Exploiting web 2.0 and semantic services in cultural heritage // Journal of Digital Information, vol. 10, no. 6, 2009,
<http://www.journals.tdl.org/jodi/index.php/jodi/article/view/688/576>
16. Lagoze C., Davis J.R. Dienst: An architecture for distributed document libraries // Communications of the ACM, 1995, vol. 38, no. 4, pp. 1.
17. Candela L., Castelli D., Ferro N., Koutrika G., et al. The DELOS Digital Library Reference model. Foundations for digital Libraries (Version 0.98), 2008,
<http://www.eprints.port.ac.uk/4104>
18. Gonçalves M.A., Fox E.A. 5SL – A language for declarative specification and generation of digital libraries / Proceedings of the 2nd ACM/IEEE-CS Joint Conference on Digital Libraries, 2002, pp. 263-272.

19. Gonçalves, M.A., et al. Streams, structures, spaces, scenarios, societies (5s): A formal model for digital libraries // *ACM Transactions on Information Systems*, 2004, vol. 22, no. 2, pp. 270-312.
20. Online Computer Library Center (OCLC): OCLC Digital Archive Preservation Policy and Supporting Documentation. Dublin, Ohio, 2006, 19 p.
21. Stallings W. *Cryptography and Network Security*. 4 ed. Pearson Prentice Hall: 2006.
22. Neuhaus P. Privacy and confidentiality in digital reference // *Reference & User Services Quarterly*, 2003, vol. 43, no. 1, pp. 26-36.
23. Saeednia S. How to maintain both privacy and authentication in digital libraries // *International Journal on Digital Libraries*, 2000, vol. 2, no. 4, pp. 251-258.
24. Kuzma J. European digital libraries: Web security vulnerabilities // *Library Hi Tech*, 2010, vol. 28, no. 3, pp. 402-413.
25. Adam N.R., Atluri V., Bertino E., Ferrari E. A content-based authorization model for digital libraries // *IEEE Transactions on Knowledge and Data Engineering*, 2002, vol. 14, no. 2, pp. 296-315.
26. Ferrari E., Adam N.R., Atluri V., Bertino E., Capuozzo U. An authorization system for digital libraries // *The VLDB Journal*, 2002, vol. 11, no. 1, pp. 58 – 67.
27. Tyrväinen P. Concepts and a design for fair use and privacy in DRM // *D-Lib Magazine*, 2005, vol. 11, no. 2, <http://www.dlib.org/dlib/february05/tyrvainen/02tyrvainen.html>
28. ElSherbiny N. Security in digital libraries. Masters Thesis. June 2011.
29. Tolone W., et al. Access control in collaborative systems // *ACM Computing Surveys*, 2005, vol. 37, no. 1, pp. 29-41.
30. Information Supplement - PCI DSS E-commerce Guidelines. January 2013. 40 p.
31. Sturges P., Davies E., Dearnley J., Iliffe U., Iliffe U., Oppenheim C., Hardy R. User privacy in the digital library environment: an investigation of policies and preparedness // *Library Management*, 2003, vol. 24, no. 1/2, pp.44-50.
32. American Library Association Code of Ethics, <http://www.ala.org/advocacy/proethics/codeofethics/codeethics>
33. Questions and Answers on Privacy and Confidentiality, <http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/qa-privacy>
34. Noh Y. Digital library user privacy: changing librarian viewpoints through education // *Library Hi Tech*, 2014, vol. 32, no: 2, pp.300-317.
35. Gibb F., Thornley C., Ferguson S., Weckert J. The application of RFIDs in libraries: an assessment of technological, management and professional issues // *International Journal of Information Management*, 2011, vol. 31, no. 3, pp. 244-251.
36. American Library Association. RFID in libraries: privacy and confidentiality guidelines, 2006, <http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/rfidguidelines>
37. Kelly E.P., Ericson G.S. RFID tags: Commercial applications v. privacy rights // *Industrial Management and Data Systems*, 2005, vol. 105, no. 6, pp. 703-713.
38. Ngai E.W.T., Moon K.K.L., Riggins F.J., Yi C.Y. RFID research: An academic literature review (1995-2005) and future research directions // *International Journal of Production Economics*, 2008, vol. 112, pp. 510-520.
39. Rieback M.R., Simpson P.N.D., Crispo B., Tanenbaum A.S. RFID malware: Design principles and examples // *Pervasive and Mobile Computing*, 2006, vol. 2, pp. 405-426.

УДК 004.9:351

Имамвердиев Ядигар Н.

Институт Информационных Технологий НАНА, Баку, Азербайджан

yadigar@lan.ab.az

IDEA4SP: модель информационной безопасности для электронных библиотек

Электронные библиотеки представляют собой сложные информационные системы, оказывающие онлайн-библиотечно-информационные услуги, и для таких систем обеспечение информационной безопасности и защита персональных данных имеют большое значение. В этой работе предлагается IDEA4SP-модель для анализа проблем информационной безопасности электронных библиотек, и актуальные проблемы структурируются по уровням этой модели. Анализируются также технологические подходы к обеспечению безопасности персональных данных и защиты интеллектуальной собственности в электронных библиотеках.

Ключевые слова: электронная библиотека, персональные данные, информационная безопасность, неприкосновенность частной жизни, IDEA4SP.

Yadigar N. Imamverdiyev

Institute of Information Technology of ANAS, Baku, Azerbaijan

yadigar@lan.ab.az

IDEA4SP: An information security model for digital libraries

Digital libraries are complex information systems, which provide online library and information services, and for such systems ensuring information security and personal data protection are important. In this paper, we propose IDEA4SP-model for the analysis of information security problems in digital libraries, and actual problems are structured by level of this model. Technological approaches for ensuring security of personal data and protecting intellectual property in digital libraries are also analyzed.

Keywords: digital library; personal data; information security; privacy; IDEA4SP.