KİTABXANA-İNFORMASİYA FƏALİYYƏTLƏRİNDƏ KİBERTƏHLÜKƏSİZLİK PROBLEMLƏRİ

Azad Qurbanov
Kitabxanaşünaslıq kafedrasının dosenti
azadbey@mail.ru

Xülasə: *Müasir kitabxanalarda kibertəhlükəsizlik artan kiber və rəqəmsal təhlükəsizlik təhdidləri fonunda getdikcə aktual mövzuya çevrilir. Bu məqalədə kitabxanalarda informasiya təhlükəsizliyinin təmin edilməsinin vacibliyinə və onların informasiya fəaliyyətində kibertəhlükəsizliyin aktual problemlərinə diqqət yetirilir. Məqalədə istifadəçilərin şəxsi məlumatlarının qorunması, kiberhücumların qarşısının alınması, informasiya sistemlərinin və şəbəkələrinin təhlükəsizliyinin təmin edilməsi, kiber insidentlərə reaksiya kimi kitabxanaların üzləşdiyi kibertəhlükəsizliyin əsas aspektləri müzakirə olunur. Çox faktorlu autentifikasiya, məlumatların şifrələnməsi, müdaxilənin aşkarlanması sistemləri və fişinq hücumlarının qarşısının alınması tədbirləri də daxil olmaqla, məlumatın mühafizəsi üsul və alətlərinə xüsusi diqqət yetirilir.*

Açar sözlər: *Məlumatın mühafizəsi, kitabxanalar, kibertəhlükəsizlik, şəxsi məlumatlar, kiberhücumlar*

GİRİŞ

Müasir informasiya texnologiyaları bilik və informasiyaya əlçatanlığı xeyli asanlaşdırmış və bu əlçatanlığın zaman, məkan anlayışlarından asılılığını aradan qaldırmışdır. Kitabxanalar da əsas informasiya institutları kimi informasiyaya çıxışı təmin etmək üçün rəqəmsal vasitələrdən də fəal şəkildə istifadə edərək, öz informasiya fəaliyyətlərini rəqamsal mühitdə yürütməyə başlamışlar. Bu, kitabxanaların daha çox insanlara, daha yüksək, operativ və modern informasiya xidməti göstərməyə imkan vermişdir. Bununla belə, rəqəmsal texnologiyaların artan rolu ilə kibertəhlükəsizlik təhdidləri də artır və kitabxanalar üçün kibertəhlükəsizlik risklərinin həll ediilməsi məsələsi aktuallaşır [1]. Bu məqalədə, kitabxana informasiya fəaliyyətində aşkar edilən kibertəhlükəsizlik problemlərini və həll üsullarını araşdıracağıq.

1. Kiberhücumlar və zəifliklər

Kiberhücumlar, xüsusən rəqəmsal texnologiyaların sürətli inkişafı və rəqəmsal məlumatların artması fonunda kitabxanalar və istifadəçilər üçün ciddi təhlükə yarada bilər.Məsələn, hakerlər kitabxana verilənlər bazalarında olan qiymətli məlumatlara daxil olmağa cəhd edə və ya fidyə (ransomware) proqramından istifadə edərək məlumatlara girişi bloklaya bilərlər. Proqram təminatı və köhnəlmiş təhlükəsizlik sistemlərindəki boşluqlar bu cür hücumları asanlaşdıra bilər. Kiberhücum risklərini minimallaşdırmaq üçün kitabxanaların İT infrastrukturunun daim yenilənməsi və təhlükəsizliyinin təmin edilməsi zəruridir [9].

Kitabxanaların üzləşdiyi bəzi kiberhücum və zəiflik növlərini qeyd edək [2-3]:

• Xidmətdən imtina (DoS) və Paylanmış Xidmətdən imtina (DDoS) hücumları:

Kibercinayətkarlar kitabxananın serverlərinə DoS və ya DDoS hücumları həyata keçirə, onları elə həddən artıq yükləyə bilərlər ki, istifadəçilər onlayn resurslara və ya kitabxananın saytına daxil ola bilməyəcəklər. Bu, kitabxananın reputasiyasına xələl gətirə və xidmətin əlçatanlığının müvəqqəti itirilməsi ilə nəticələnə bilər.

• Zərərli proqramların yayılması:

Kitabxanalar viruslar, qurdlar və troyanlar kimi zərərli proqramların hücumuna məruz qala bilər. Zərərli proqramlar kitabxana sistemlərinə nüfuz edərək, qiymətli məlumatları və məlumatları oğurlaya və ya məhv edə bilər.

• Fişinq:

Kibercinayətkarlar özlərini etibarlı şəxslər və ya təşkilatlar kimi təqdim edərək kitabxana işçilərini və ya istifadəçilərini aldatmağa cəhd edə bilərlər. Fişinq hücumlarının məqsədi uçot yazılarını, parollar və ya digər məxfi məlumatları əldə etmək ola bilər.

• İcazəsiz giriş:

Kitabxanada kifayət qədər güclü parollar yoxdursa və ya şəbəkə resursları kifayət qədər qorunmursa, təcavüzkarlar istifadəçilərin şəxsi məlumatları da daxil olmaqla sistemlərə və verilənlər bazalarına icazəsiz giriş əldə edə bilərlər.

• Qeyri-kafi Proqram təminatı yeniləməsinin qeyri kafi səviyyəsi:

Kitabxanalar proqram təminatı və təhlükəsizlik sistemlərini mütəmadi olaraq yeniləməsələr, bu, təcavüzkarlar tərəfindən istifadə edilə bilən boşluqlar yarada bilər.

• Cihazların oğurlanması və ya itməsi:

Kitabxana sistemlərinə girişi olan noutbuklar, planşetlər və smartfonlar kimi mobil cihazların oğurlanması və ya itirilməsi informasiyaya icazəsiz girişə səbəb ola bilər.

• İşçilərin zəif kibertəhlükəsizlik hazırlığı:

Əgər kitabxana işçiləri potensial kibertəhdidlərdən və təhlükəsizlik təcrübələrindən xəbərdar deyillərsə, bu, kitabxananı hücumlara qarşı daha həssas edə bilər.

2. Məlumatların mühfizəsi

Kitabxanalarda fərdi məlumatların qorunması istifadəçinin etibarını və Fərdi Məlumatların Mühafizəsi Aktı kimi müvafiq hüquqi qaydalara uyğunluğu təmin etmək üçün kritik aspekt və məsuliyyətdir. Kitabxanaların öz istifadəçilərinin məlumatlarının məxfiliyini qorumaq üçün görə biləcəyi əsas tədbirlər və prinsiplərdən bəzilərini qeyd edək [4]:

1. Şəxsi məlumatların mühafizəsi siyasəti:Kitabxanalar hansı məlumatların toplandığını, hansı məqsədlər üçün istifadə edildiyini, həmin məlumatlara

kimin çıxışı olduğunu və onların necə saxlanılacağını və məhv ediləcəyini müəyyən edən aydın və şəffaf məxfilik siyasəti hazırlamalıdır. Siyasət bütün kitabxana istifadəçiləri və işçiləri üçün əlçatan olmalıdır.

2. Minimal məlumatların toplanması və emalı: Kitabxanalar konkret tapşırıqları yerinə yetirmək üçün lazım olan yalnız minimum miqdarda şəxsi məlumat toplamalı və emal etməlidir. Toplanmış məlumatlar xidmət göstərmək və istifadəçi ehtiyaclarını ödəmək üçün lazım olanlarla məhdudlaşmalıdır.

3. İstifadəçilərin razılığı:Kitabxanalar öz şəxsi məlumatlarının toplanması və emalı üçün istifadəçilərdən açıq razılıq almalıdırlar. Razılıq könüllü, məlumatlı və konkret olmalıdır və istifadəçilər istənilən vaxt razılıqlarını geri götürə bilməlidirlər.

4. Məlumatın mühafizəsi:Şəxsi məlumatlar təhlükəsiz və təhlükəsiz yerdə saxlanmalıdır. Kitabxanalar icazəsiz girişin və məlumat sızmasının qarşısını almaq üçün müasir şifrələmə və məlumatların qorunması üsullarından istifadə etməlidir.

5. Kadr hazırlığı:

Kitabxana işçiləri fərdi məlumatların mühafizəsi prinsipləri və məlumatların mühafizəsi siyasətinə uyğunluq üzrə təlim keçməlidirlər. Onlar məlumat məxfiliyinin vacibliyini və istifadəçi məlumatlarının qorunmasında öz məsuliyyətlərini başa düşməlidirlər.

6. Qanuna uyğunluq:

Kitabxanalar Avropa Birliyində Ümumi Məlumatların Qorunması Qaydası (GDPR) və ya digər ölkələrdə yerli məlumatların qorunması qanunları kimi şəxsi məlumatların qorunması ilə bağlı bütün qüvvədə olan qanun və qaydalara əməl etməlidir.

7. Anonimlik və təxəllüslər:

Mümkünsə, kitabxanalar toplanan şəxsi məlumatların həcmini azaltmaq üçün istifadəçilərə xidmətlərə daxil olmaq üçün anonim və ya təxəllüslü hesablardan istifadə etməyə icazə verməlidir.

8. Məlumatların silinməsi:

İstifadəçilərin şəxsi məlumatları yalnız lazımi müddət ərzində saxlanılmalı və bu müddətdən sonra və ya köhnəldikdən sonra silinməlidir.

Məxfilik prinsiplərinə uyğunluq kitabxanalara istifadəçilərinin məlumatlarının məxfiliyini və təhlükəsizliyini qorumağa, onların xidmətlərinə inam və marağı qorumağa və müvafiq hüquqi öhdəliklərə əməl etməyə kömək edəcək.

9.Onlayn xidmətlərin təhlükəsizliyinin təmin edilməsi: Elektron məlumat bazaları və ya onlayn kataloqlar kimi onlayn xidmətlər təqdim edən kitabxanalar istifadəçilərin şəxsi məlumatlarının ələ keçirilməsindən qorunması üçün təhlükəsiz əlaqə təmin etməlidir.

10. Təhlükəsizlik auditi və monitorinqi: Şəxsi məlumatların qorunmasının müntəzəm auditi və monitorinqi sizə zəifliklər müəyyən etməyə və mümkün təhlükələrin qarşısını əvvəlcədən almağa imkan verir.

11. Məlumatların pozulması barədə bildiriş: Təhlükəsizlik və ya məlumatların pozulması halında, kitabxanalar hadisə barədə müvafiq orqanlara və təsirə məruz qalan istifadəçilərə dərhal məlumat verməlidirlər.

12. Kibertəhlükəsizlik Mütəxəssisləri ilə əməkdaşlıq: Kitabxanalar təhlükəsizlik tədbirlərini işləyib hazırlamaq və həyata keçirmək və məlumat təhlükəsizliyi məsələləri üzrə məsləhətləşmələr aparmaq üçün kibertəhlükəsizlik üzrə peşəkarlar və ekspertlərlə əməkdaşlıq edə bilərlər.

Yuxarıda göstərilən tədbirlərə və prinsiplərə riayət etmək kitabxanalara şəxsi məlumatların yüksək səviyyədə qorunmasını təmin etməyə, istifadəçilərin etibarını qorumağa və təhlükəsizlik pozuntusunun mümkün mənfi nəticələrinin qarşısını almağa kömək edəcək.

3. Məlumatların ehtiyat nüsxələnməsi

Məlumatların ehtiyat nüsxələnməsi kitabxanalar üçün zəruri təcrübədir, çünki onlar istifadəçilər, kitablar, akademik tədqiqatlar və digər rəqəmsal resurslar haqqında qiymətli məlumatlar da daxil olmaqla, əhəmiyyətli miqdarda məlumatı saxlayır və emal edir. Məlumatların müntəzəm və etibarlı ehtiyat nüsxəsi gözlənilməz nasazlıqlar, fəlakətlər və kiberhücumlar zamanı məlumatın təhlükəsizliyini və bütövlüyünü təmin etməyə kömək edir. Məlumatların ehtiyat nüsxəsi kitabxananın kibertəhlükəsizlik strategiyasının əsas elementidir və məlumatların qorunması və bütövlüyünü təmin etmək üçün diqqətlə planlaşdırılmalı, həyata keçirilməli və yenilənməlidir[5,9].

Kitabxanalarda məlumatların ehtiyat nüsxəsinin çıxarılmasının aşağıdakı aspektləri vardır:

- Planlaşdırma və strategiya:Kitabxanalar hansı məlumatların ehtiyat nüsxəsinin çıxarılmasını və nə qədər tez-tez olacağını müəyyən edən müvafiq məlumat ehtiyat nüsxəsi strategiyasını hazırlamalıdırlar. Tez-tez ehtiyat nüsxəsini çıxarmaq lazım olan kritik məlumatları və ehtiyat nüsxələrinin nə qədər tez-tez yerinə yetirilməli olduğunu müəyyən etmək vacibdir.
- Uyğun ehtiyat üsullarının seçilməsi: Tam, artımlı, diferensial və bulud ehtiyat nüsxəsi kimi bir neçə məlumat ehtiyat nüsxəsi üsulu var. Kitabxanalar öz ehtiyaclarına, mövcud resurslara və məlumatların həcminə əsasən ən uyğun metodu seçməlidirlər.
- Çoxsaylı saxlama yerləri:Ehtiyat nüsxələrin etibarlılığını artırmaq üçün kitabxanalar öz məlumatlarının ehtiyat nüsxələrini bir neçə yerdə saxlamağa təşviq edilir. Bura daxili serverlər, xarici disklər, şəbəkə yaddaşı və ya bulud yaddaşı daxil ola bilər.
- Daimi ehtiyat nüsxə: Bir nasazlıq və ya insident zamanı məlumat itkisini minimuma endirmək üçün məlumatların müntəzəm olaraq xüsusi cədvələ uyğun olaraq ehtiyat nüsxəsi çıxarılmalıdır.
- Ehtiyat nüsxələrin sınaqdan keçirilməsi və yoxlanılması: Kitabxanalar vaxtaşırı öz ehtiyat nüsxələrinin effektivliyini sınaqdan keçirməlidir. Məlumatların bərpası sınağı lazım olduqda məlumatların uğurla bərpa oluna biləcəyini təmin edir.

• Ehtiyat nüsxələrin təhlükəsizliyinin təmin edilməsi: İcazəsiz girişin və məlumatların oğurlanmasının qarşısını almaq üçün verilənlərin ehtiyat nüsxələri təhlükəsiz, məhdudlaşdırılmış yerlərdə saxlanmalıdır.

• Nsxələnmə prosesinin avtomatlaşdırılması: Yedəkləmə prosesinin avtomatlaşdırılması insan səhvindən qaçmağa kömək edir və ehtiyat nüsxələrin vaxtında tamamlanmasını təmin edir.

4. Kitabxana təhlükəsizliyi auditləri

Müntəzəm kitabxana təhlükəsizliyi auditləri potensial zəiflikləri aşkar etmək və aradan qaldırmaq, müəyyən edilmiş təhlükəsizlik siyasətləri və standartlarına uyğunluğu yoxlamaq, məlumat və resursların mühafizəsinin ümumi səviyyəsini təkmilləşdirmək üçün mühüm təcrübədir. Kitabxana təhlükəsizliyinin müntəzəm auditini apararkən nəzərə alınmalı olan bəzi əsas aspektlər bunlardır [6, 7]:

• Audit məqsədlərinin müəyyən edilməsi: İlk addım auditin məqsədlərini və həcmini müəyyən etməkdir. Buraya təhlükəsizlik siyasətlərinə uyğunluğun yoxlanılması, girişə nəzarət mexanizmlərinin effektivliyinin yoxlanılması, istifadəçilərin şəxsi məlumatlarının mühafizə səviyyəsinin qiymətləndirilməsi və digər təhlükəsizlik aspektləri daxil ola bilər.

• İştirakçılar və məsul şəxslər:Auditi həyata keçirəcək komandanı müəyyən edilməli və onların müvafiq kibertəhlükəsizlik təcrübəsi və biliyinə malik olduğundan əmin olunmalıdır. Həmçinin aşkar edilmiş xətaların aradan qaldırılmasına cavabdeh olan məsul şəxsləri müəyyənləşdirmək lazımdır.

• Təhlükəsizlik siyasəti və prosedurlarının nəzərdən keçirilməsi: Kitabxananın müəyyən edilmiş təhlükəsizlik siyasətlərinə və prosedurlarına riayət etdiyini və onların mövcud standartlara və qaydalara uyğun olduğunu yoxlamaq lazımdır.

• Girişə nəzarət mexanizmlərinin yoxlanılması: Sistemləri və məlumatları qorumaq üçün istifadə olunan girişə nəzarət mexanizmlərinin effektivliyini və etibarlılığını təsdiqləmək lazımdır. İdentikləşdirmə, avtorizasiya və giriş auditini aktivləşdirmək lazımdır.

• Məlumatların qorunmasının monitorinqi: Kitabxanadakı məlumatların, o cümlədən istifadəçilərin şəxsi məlumatları, kataloqlar, tədqiqatlar və digər qiymətli məlumatların nə qədər yaxşı qorunduğunu yoxlamaq lazımdır.

• Hadisə qeydlərinin təhlili: Şübhəli fəaliyyət, uğursuz giriş cəhdləri və digər anomaliyalar üçün hadisə qeydlərini və qeydləri nəzərdən keçirmək lazımdır.

• Fiziki təhlükəsizlik yoxlanışı: Kitabxananın serverlərinə və avadanlıqlarına fiziki girişin də təhlükəsiz olmasını təmin etmək lazımdır.

• Nəticələrin sənədləşdirilməsi: Müəyyən edilmiş bütün zəifliklərin və onların aradan qaldırılması üçün tövsiyələrin, habelə təhlükəsizliyin təmin edilməsi üçün görülən tədbirlərin sənədləşdirilməsi vacibdir.

• Xətaların aradan qaldırılması: Auditin nəticələrinə əsasən müəyyən edilmiş xətaların aradan qaldırılması üçün plan hazırlamaq və onun icrasına nəzarət etmək lazımdır.

• Auditlərin müntəzəmliyi: Təhlükəsizlik sistemlərinin daim yenilənməsini və təkmilləşdirilməsini təmin etmək üçün mütəmadi olaraq yoxlamalar aparılmalıdır.

Müntəzəm təhlükəsizlik auditləri kitabxanalara məlumat və resursların yüksək səviyyədə qorunmasına, istifadəçilərin təhlükəsizliyini və qiymətli məlumatların təhlükəsizliyini təmin etməyə kömək edir.

NƏTİCƏ

Kitabxanaların informasiya fəaliyyətində kibertəhlükəsizlik onların işinin tərkib hissəsinə çevrilib. Kitabxanalar istifadəçi məlumatlarının qorunması, kiberhücumların qarşısının alınması və informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi üçün fəal addımlar atmalıdır. İşçi heyətin, istifadəçilərin və kibertəhlükəsizlik mütəxəssislərinin birgə səyləri kitabxanaları bilik və məlumat əldə etmək üçün daha təhlükəsiz və daha mdafiə edilmiş informasiya infrastrukturina çevrilməyə kömək edəcək.

Ədəbiyyat:

1. Hadingham R. Cybersecurity for Libraries. Chandos Publishing, 2016.
2. Liffick B. Library Cybersecurity: Finding and Fixing Vulnerabilities. American Library Association, 2018.
3. Kruse J., Heiser J. Computer Security Incident Handling Guide. National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2, 2012.
4. Thornton T. Data Protection for Libraries, Archives and Museums: An Introduction. Facet Publishing, 2016.
5. O'Gorman C. Cybersecurity and Human Rights in the Age of Cyberveillance. Routledge, 2018.
6. McGarry K., Salo D. Information Security in Libraries: A LITA Guide. ALA TechSource, 2015.
7. Stone-Gross B., Cova M., Cavallaro L., Gilbert B., Szydlowski M., Kemmerer R. Your Botnet is My Botnet: Analysis of a Botnet Takeover. In Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), 2009.
8. Gritzalis S., Stergiopoulos G. An Integrated Approach for Information Security Risk Management. Computers & Security, Volume 23, Issue 3, 2004, Pages 190-198.
9. Data Protection Commission (DPC). GDPR and You – A Guide to Data Protection for Individuals. 2018.

А.Курбанов

Проблемы кибербезопасности в библиотечно-информационной деятельности

Резюме: *Кибербезопасность в современных библиотеках становится все более актуальной темой в свете возрастающих киберугроз и угроз цифровой безопасности. Данная статья обращает внимание на важность обеспечения безопасности информации в библиотеках и актуальные вопросы кибербе-*

зопасности в их информационной деятельности. В статье рассматриваются основные аспекты кибербезопасности, с которыми сталкиваются библиотеки, такие как защита персональных данных пользователей, предотвращение кибератак, обеспечение безопасности информационных систем и сетей, а также реагирование на киберинциденты. Особое внимание уделяется методам и инструментам защиты информации, включая многофакторную аутентификацию, шифрование данных, системы обнаружения вторжений и меры предотвращения фишинговых атак.

Ключевые слова: *защита информации, библиотеки, кибербезопасность, персональные данные, кибератаки*

A.Kurbanov

Problems of cyber security in library and information activities

Summary: *Cybersecurity in modern libraries is becoming an increasingly relevant topic in light of increasing cyber and digital security threats. This article draws attention to the importance of ensuring the security of information in libraries and current issues of cybersecurity in their information activities. The article discusses the main aspects of cybersecurity faced by libraries, such as protecting users' personal data, preventing cyber attacks, securing information systems and networks, and responding to cyber incidents. Particular attention is paid to methods and tools for protecting information, including multi-factor authentication, data encryption, intrusion detection systems and measures to prevent phishing attacks.*

Keywords*: information protection, libraries, cyber security, personal data, cyber attacks*

Rəyçi: *p.ü.f.d., dos.* ***E.Əhmədov***