Assessing the Components of Information Security in Accessing & Use of Digital Libraries

Fariborz Doroudi*
PhD in Knowledge and Information Science; Assistant Professor;
Iranian Research Institute for Information Science and Technology (IranDoc) Tehran, Iran Email: doroudi@irandoc.ac.ir

Zeinab Jamshidi
Master in Knowledge and Information Science;
Islamic Azad University of Hamedan; Hamedan, Iran;
Email: zeinab.jam68@gmail.com

Received: 18, May 2020 **Accepted: 07, Nov. 2020**

Abstract: Information security is one of the effective factors in protecting and using digital libraries which can help improve the status of these libraries.This research reviews the accessibility to information security of digital libraries in digital libraries of Qom city. In this study, definitions of digital libraries include libraries based on their mission and using experts, organize digital documents and provide them to members in the form of information services.

This study is a survey and research community was both public and academic digital libraries (including 5 libraries) in Qom city. Data collection tool is a questionnaire based on the standard ISO/ IEC 27002 which is an information security standard developed by the international organization for standardization (ISO) and International Electrotechnical Commission (IEC).

The results of this study indicate that the average information security among digital libraries in Qom city is estimated to be 0.801, which considering the research evaluation method, it can be said that it has a strong level of information security. The development of information systems to provide effective services in digital libraries has played an effective role .There is also a significant relationship between different indicators of information security in digital libraries of Qom city. Weaknesses and strengths of digital libraries in Qom city, respectively, include physical and environmental security as a weakness and business continuity management has been introduced as a strength. Utilizing passive defense, participation of security groups to prevent hackers, identifying security gaps, training specialized forces and having an executive plan for information security are among the suggestions of this research. Finally, it must be stated that information security is at a high level in libraries in Qom city.

Keywords: Information Security, Qom, Digital Libraries, Digital Library Software

* Corresponding Author

Iranian Journal of Information Processing and Management

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Vol. 37 | No. 1 | pp. 117-134
Autumn 2021

سنجش مؤلفه‌های امنیت اطلاعات در دسترسی و استفاده از کتابخانه‌های دیجیتال

فریبرز درودی
دکتری علم اطلاعات و دانش‌شناسی؛ استادیار؛ پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)؛ تهران، ایران؛
پدیدآور رابط doroudi@irandoc.ac.ir

زینب جمشیدی
کارشناسی ارشد علم اطلاعات و دانش‌شناسی؛ دانشگاه آزاد اسلامی واحد همدان؛ همدان، ایران؛
zeinab.jam68@gmail.com

پژوهش‌نامهٔ پردازش و مدیریت اطلاعات

دریافت: ۱۳۹۹/۰۲/۲۹ پذیرش: ۱۳۹۹/۰۸/۱۷ مقاله برای اصلاح به مدت ۳ ماه نزد پدیدآوران بوده است.

نشریهٔ علمی | رتبهٔ بین‌المللی
پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)
شاپا (چاپی) ۸۲۲۳-۲۲۵۱
شاپا (الکترونیکی) ۸۲۳۱-۲۲۵۱
نمایه در LISTA، ISC، و SCOPUS
jipm.irandoc.ac.ir
دورهٔ ۳۷ | شمارهٔ ۱ | ص‌ص ۱۱۷-۱۳۴
پاییز ۱۴۰۰

چکیده: امنیت اطلاعات یکی از عوامل مؤثر در حفاظت از کتابخانه‌های دیجیتال و بهره‌گیری از آن‌هاست که می‌تواند به بهبود وضعیت این کتابخانه‌ها کمک کند. این پژوهش به بررسی میزان قابلیت دسترسی به امنیت اطلاعات در کتابخانه‌های دیجیتال «شهرستان قم» پرداخته است. تعریف کتابخانه‌های دیجیتال، شامل کتابخانه‌هایی است که بر مبنای مأموریت و با استفاده از متخصصان، مدارک دیجیتال را سازماندهی کرده و به شکل خدمات اطلاعاتی به اعضا ارائه می‌دهند.

روش پژوهش، پیمایشی تحلیلی و جامعهٔ پژوهش، کتابخانه‌های دیجیتال «شهرستان قم» اعم از عمومی و دانشگاهی (شامل ۵ کتابخانه) است. در پژوهش حاضر، گردآوری اطلاعات از طریق پرسشنامه است که بر اساس استاندارد ISO/ IEC 27002 آماده شده است. این استاندارد مربوط به حوزهٔ امنیت اطلاعات بوده و سازمان بین‌المللی استاندارد (ISO) و کمیسیون بین‌المللی الکتروتکنیک (IEC) آن را تدوین کرده است.

نتایج حاصل از این پژوهش نشان می‌دهد که میانگین امنیت اطلاعات در میان کتابخانه‌های دیجیتال «شهرستان قم» برابر ۰/۸۰۱ ارزیابی شده است که با عنایت به روش ارزیابی پژوهش می‌توان اظهار کرد که دارای سطح قوی امنیت اطلاعات است. توسعهٔ سیستم‌های اطلاعاتی برای ارائهٔ خدمات مؤثر در کتابخانه‌های دیجیتال نقشی مؤثر داشته است. همچنین، رابطه‌ای

معنادار میان شاخص‌های مختلف امنیت اطلاعات در کتابخانه‌های دیجیتال «شهرستان قم» وجود دارد. در این پژوهش امنیت فیزیکی و محیطی به‌عنوان نقطهٔ ضعف و مدیریت تداوم کسب‌وکار به‌عنوان نقطهٔ قوت معرفی شده است. بهره‌گیری از پدافند غیرعامل، مشارکت گروه‌های امنیتی برای جلوگیری از فعالیت هکرها، شناسایی حفره‌های امنیتی، آموزش نیروی‌های متخصص و داشتن برنامهٔ اجرایی امنیت اطلاعات از جمله پیشنهادهای این پژوهش است. در نهایت، باید بیان کرد که امنیت اطلاعات در کتابخانه‌های شهرستان قم از سطح بالایی برخوردار است.

کلیدواژه‌ها: امنیت اطلاعات، شهرستان قم، کتابخانه‌های دیجیتال، نرم‌افزار کتابخانه‌های دیجیتال

۱. مقدمه

پیشرفت‌های سریع در ارتباطات از راه دور، محاسبات سخت‌افزاری و نرم‌افزاری، رمزگذاری داده‌ها، بهره‌گیری وسیع از پردازش داده‌های الکترونیکی، و مشاغل الکترونیکی که از طریق اینترنت انجام می‌یابند، منجر به افزایش شدید تهدیدهای امنیت اطلاعات شده است (Awad & Fairhurst 2018). با توجه به دسترسی به اطلاعات الکترونیکی و تقاضا از طریق آن، کتابخانه‌های دانشگاهی تمایل دارند که خدمات خود را در محیط شبکهٔ رایانه‌ای انجام دهند. کتابخانه‌ها به‌سرعت از هویت کتابخانهٔ دوگانهٔ[1] خود خارج می‌شوند و در زیرساخت‌های دیجیتال که به‌طور کامل بر وب مبتنی هستند، به گسترش فناوری اطلاعات و ارتباطات می‌پردازند (Nandagaoli & Lihitakar 2019). از این رو، یکی از انواع روبه‌رشد کتابخانه‌ها در دوران جدید، یعنی کتابخانه‌های دیجیتال در زمرهٔ مراکزی هستند که به موضوع گسترش خدمات اطلاعاتی مبتنی بر بسترهای ایمن و مطمئن روی خوش نشان داده‌اند.

کتابخانهٔ دیجیتال کتابخانه‌ای است که از فناوری دیجیتال رایانه‌ای برای ذخیره، مدیریت و استفاده از مدرک استفاده می‌کند (Liu 2014). محتوای دیجیتال نقش مهمی در کتابخانه‌های دیجیتال بر عهده دارد و باید به انواع منابع و روش‌های ذخیره‌سازی مناسب محتوای دیجیتال بیشتر توجه کرد، چنانکه «شیری» در تعریف کتابخانهٔ دیجیتال به محتوای دیجیتال در کنار ابزارها و فناوری‌ها اشاره کرده و به نقش مؤثر معماری و فراداده در کنار استانداردهای دیجیتال‌سازی اشاره می‌کند (Shiri 2003). برداشت‌های گوناگون

1. hybrid

از مفهوم کتابخانهٔ دیجیتال تأثیر مهمی در تلاش برای تعریف و محدود کردن اصطلاح «کتابخانهٔ دیجیتال» داشته است. از سال ۲۰۰۶، این اصطلاح به‌طور کلی برای اشاره به سیستم‌هایی به‌کار رفته که از نظر دامنه ناهمگن بوده و انواع مختلفی از عملکردها را ارائه می‌دهند. این سیستم‌ها شامل مخازن دیجیتال، شیء و فرادداده، سیستم‌های پیونددهندهٔ مرجع، بایگانی‌ها، سیستم‌های مدیریت محتوا و سیستم‌های پیچیده‌ای است که خدمات پیشرفتهٔ کتابخانهٔ دیجیتال را ادغام می‌کنند (Candela et al. 2007). بر این اساس، کتابخانهٔ دیجیتال از سخت‌افزار، فناوری، مدیریت و جنبه‌های دیگر گرفته تا تحلیل هدفمند عوامل تهدیدکنندهٔ شبکهٔ این نوع کتابخانه‌ها با مسئلهٔ امنیت مواجه است و لازم است با مشکلات امنیت شبکه در کتابخانهٔ دیجیتال روبه‌رو شد (Zhang, Song & Yan 2016). با استفادهٔ گسترده از شبکه‌های رایانه‌ای و افزایش انتقال داده‌ها بین شبکه‌ها، مسائل امنیتی شبکه پررنگ‌تر می‌شود (Jiang, Lin & He 2018). از سوی دیگر، مدیریت امنیت در شبکهٔ اینترنت بسیار دشوار است (Liu 2019) و امنیت اطلاعات در سازمان‌هایی که اطلاعات را در آرشیوهای دیجیتال ذخیره می‌کنند، به یک نگرانی مهم تبدیل شده است (Bârsan 2017).

بروندادهای دیجیتال‌شدهٔ نوین که در وبگاه‌های کتابخانه‌های دانشگاهی ارائه می‌شوند، ممکن است به‌دلیل ناآگاهی کاربران و نقص اساسی در دستگاه‌های شبکه، پیکربندی، فرهنگ کار با برنامه‌های کاربردی و نیز عدم آگاهی برای طیف وسیعی از تهدیدها و حمله‌های مربوط به امنیت فضای مجازی آسیب‌پذیر باشند (Nandagaoli & Lihitakar 2019). امنیت در کتابخانه‌های دیجیتال مهم‌ترین مسئله‌ای است که باید در طراحی سیاست‌ها و برنامه‌های راهبردی مؤسسه‌هایی که مایل به ایجاد کتابخانهٔ دیجیتال هستند، با دقت مورد توجه قرار گیرد (Anday et al. 2012). به‌طور کلی، حفاظت از داده‌ها به دو سطح منابع اطلاعاتی و حفاظت از اطلاعات کاربر تقسیم می‌شود. این امنیت باید برای شخص مجازی، منابع و خدمات‌دهنده‌های دستگاه اعمال شود (Soleimanzade et al. 2019.). رعایت امنیت در کتابخانهٔ دیجیتال مقوله‌ای پیچیده بوده و موضوع امنیت از بُعد نیروی انسانی نیازمند آموزش است (Zhao, Zhang & Wang 2018). همچنین، عوامل اصلی مؤثر بر امنیت اطلاعات کتابخانهٔ دیجیتال مواردی همچون سخت‌افزار رایانه‌ای و عوامل نرم‌افزاری، خطرات امنیتی شبکه، عدم مدیریت حرفه‌ای و سازوکار امنیتی مؤثر را شامل می‌شود (Hao 2015).

بنابراین، امنیت اطلاعات به معنای حفظ محرمانگی در کنار یکپارچگی و نیز قابلیت

دسترسی به داده‌های موجود در یک پایگاه اطلاعاتی است که برای حفاظت و نگهداری مناسب داده‌ها در کنار ابزارها و تجهیزات آن سبب جلوگیری از دستیابی افراد غیرمجاز به اطلاعات می‌شود. کتابخانه‌های دیجیتال از جمله مراکزی هستند که از طریق سامانه‌های اطلاعاتی به‌دنبال هدفمندکردن اطلاعات سازمانی خود هستند تا از این بستر جهت تعالی و توانمندسازی خود و رسیدن به اهداف مورد نظر استفاده کنند. حفاظت دیجیتال و بهبود وضعیت دسترس‌پذیری خدمات بدون لحاظ‌کردن مسایل امنیتی تحقق نخواهد یافت. این در حالی است که کتابخانه‌های کمی در ایران از پروتکل امنیت سازمانی استفاده می‌کنند. پروتکل‌های امنیتی قراردادهای مورد قبول سازمان‌ها، نهادها و مؤسسه‌هایی هستند که به این تفاهم می‌رسند که برای تبادل و همکاری در بهره‌گیری از اطلاعات به مفاد قراردادهای از پیش تعیین‌شده پای‌بند باشند. بنابراین، ضرورت دارد تمهیداتی برای انتقال و تبادل ایمن داده‌ها مهیا شود که نتیجهٔ آن ارسال اطلاعات به شکل کامل و بدون خدشه به دیگر بهره‌گیران است. پیشگیری از دستکاری داده‌ها و ایجاد اختلال در آن‌ها از اهداف اصلی پروتکل‌های امنیتی است. این کار علاوه بر آن، سبب حفظ امنیت خدمت‌دهنده[1]، شبکه یا وبگاه می‌شود.

بسیای از کتابخانه‌ها تلاش می‌کنند که منابع و خدمات خود را بر اساس رویکردهای دیجیتال مدیریت کنند. ترسیم طرح امنیت کتابخانهٔ دیجیتال[2] یکی از مؤلفه‌های ضروری در رعایت امنیت کتابخانه‌های دیجیتال است که می‌توان آن را نوعی فعالیت در شناخت آسیب‌پذیری‌های احتمالی برای این مراکز دانست.

باید توجه کرد که دربارهٔ موضوع امنیت اطلاعات ابعاد و جنبه‌های متعددی وجود دارد که باید به آن‌ها توجه خاص داشت. یکی از این عوامل حضور هکرها و رخنه‌گران برای ضربه‌زدن به سیستم‌های اطلاعاتی است. در کنار آن، شناسایی حفره‌های امنیتی که معمولاً هکرها از طریق آن‌ها و شناخت جنبه‌های ضعیف برنامه به سیستم نفوذ می‌کنند، مطرح می‌شود. علاوه بر آن، باید به مسائل مربوط به امنیت فیزیکی توجه خاص داشت و از ابزارهای مختلف برای کنترل این بخش از امنیت کتابخانه‌ای استفاده کرد. یکی دیگر از ابعاد این حوزه، امنیت محتوای اطلاعاتی است که منابع اصلی کتابخانه را تشکیل می‌دهد و حفاظت از آن‌ها نقش مهمی در برنامه‌ریزی مسایل امنیتی کتابخانه‌های دیجیتال دارد.

1. server
2. digital library security plan (DLSP)

همچنین، ضرورت دارد که به موضوع‌هایی چون تبادل ایمن اطلاعات، امنیت سیستم اطلاعاتی، خطای انسانی، و نیز سرقت در بخش دستگاه‌ها و قطعات، در کنار حفاظت مدون از سخت‌افزارها و نرم‌افزارهای کتابخانه‌ای پرداخت تا برنامهٔ حفاظت و ایمنی کتابخانه‌ای به‌خوبی اجرا شود.

این پژوهش با توجه به اهمیت نقش امنیت اطلاعات در کتابخانه‌های دیجیتال برای حفاظت از مجموعهٔ منابع اطلاعاتی و نیز فرایند دسترسی به آن‌ها، به بررسی عوامل اثرگذار می‌پردازد و عناصر آن را مورد ارزیابی قرار می‌دهد. مؤلفه‌های اصلی امنیت در این پژوهش بر اساس استاندارد ISO/ IEC 27002 عبارت‌اند از: امنیت فیزیکی و محیطی[1]، مدیریت ارتباطات و عملیات[2]، کنترل دسترسی[3]، توسعه و نگهداری سیستم‌های اطلاعات[4]، امنیت منابع انسانی[5]، مدیریت دارایی‌ها[6]، سازماندهی اطلاعات[7]، مدیریت تداوم کسب‌وکار[8]، سازگاری[9]، مدیریت حوادث[10] و خط‌مشی امنیت[11]. این عناصر مبتنی بر استاندارد ایزو ۲۷۰۰۲[12] است که یکی از استانداردهای شناخته‌شدهٔ امنیت اطلاعات است و توسط سازمان بین‌المللی استاندارد[13] و کمیسیون بین‌المللی الکتروتکنیک[14] و تحت عنوان «فناوری امنیت، فنون امنیت، دستورالعمل پیشنهادی برای مدیریت امنیت اطلاعات» منتشر شده است.

هدف اصلی این پژوهش مشخص ساختن قابلیت‌های دسترسی و استفاده از کتابخانه‌های دیجیتال «شهرستان قم» در ارتباط با مسائل امنیت داده است. در ارتباط با دسترسی و استفاده از کتابخانه‌های دیجیتال همواره امنیت داده‌ها و بهره‌گیری مناسب از منابع اطلاعاتی دارای اهمیت بوده است. به هر میزان که مبانی امنیتی در کتابخانه‌های دیجیتال رعایت شود، سازوکار فعالیت این کتابخانه‌ها از اثربخشی بیشتری برخوردار خواهد بود. ابعاد و جنبه‌های متعددی در رعایت امنیت داده‌ها وجود دارد که امنیت محیطی، فضای کاری، سیستم‌های اطلاعاتی، نرم‌افزارها، شرایط دسترسی به داده‌ها، سازماندهی منابع اطلاعاتی، وضعیت تخصصی نیروی انسانی و برخی عوامل دیگر در این

1. physical and environmental security
2. communication and operations management
3. access control
4. development and maintenance of information systems
5. human resources security
6. asset management
7. organizing information
8. business continuity management
9. adaptation
10. event management
11. security policy
12. ISO/IEC 27002
13. International Organization for Standardization (ISO)
14. International Electrotechnical Commission (IEC)

میان نقش مهمی بر عهده دارد. از آنجا که هرگونه ضعف در برنامه‌ریزی برای تأمین امنیت داده‌ها در کتابخانه‌های دیجیتال می‌تواند به کاهش کیفیت و ارائهٔ خدمات مؤثر این مراکز منجر شود، بنابراین بررسی این موارد و شناخت نقاط قوت و ضعف کتابخانه‌های دیجیتال می‌تواند به ارائهٔ راهکارهای مناسب برای ارتقای جایگاه کتابخانه‌های دیجیتال در دسترسی و استفاده از آن‌ها بیانجامد.

مطالعهٔ پیش رو به این حوزه می‌پردازد که از میان نرم‌افزارهای امنیتی به‌کاررفته در کتابخانه‌های دیجیتال «شهرستان قم» کدام‌یک عملکرد بهتری دارد. همچنین در این پژوهش، به بررسی امکانات نرم‌افزارهای به‌کاررفته در این کتابخانه‌ها برای تأمین بهتر امنیت اطلاعات پرداخته شده و راهکارهایی برای حفاظت داده‌های موجود ارائه می‌شود. پرسش‌های پژوهش عبارت‌اند از: ۱) امنیت اطلاعات در کتابخانه‌های دیجیتالی «شهرستان قم» تا چه میزان قابل دستیابی است؟ ۲) آسیب‌پذیرترین نقاط امنیتی در کتابخانه‌های دیجیتالی شهرستان قم کدام‌اند؟ و ۳) نقاط ضعف و قوت امنیتی کتابخانه‌های دیجیتال «شهرستان قم» کدام‌اند؟ این پرسش‌ها با توجه به مرور پیشینه و پژوهش‌های انجام‌شده که کمتر به بررسی کتابخانه‌های دیجیتال متعدد از این دست پرداخته‌اند، طراحی شده است. همچنین، باید گفت که با عنایت به لزوم شناسایی مؤلفه‌های تأثیرگذار از نظر دسترسی و استفادهٔ مطلوب از کتابخانه‌های دیجیتال که می‌تواند منجر به ارائهٔ راهکارهای سودمند شود، اهمیت پرسش‌ها بیشتر قابل توجه است.

۲. پیشینهٔ پژوهش

برای آشنایی بهتر با مطالعات انجام‌شده در این حوزه و دستیابی به یافته‌های مرتبط با پژوهش، در این قسمت به پاره‌ای از آن‌ها می‌پردازیم:

در ارتباط با نقش عناصر انسانی در امنیت اطلاعات سیستم‌های اطلاعاتی می‌توان به پژوهش «الهی، طاهری و حسن‌زاده» اشاره کرد که به رعایت مسایل فرهنگ در عناصر امنیتی، مهارت‌ها و توانمندی‌های امنیتی، تقویت خط مشی امنیتی، تجربه‌ها و خودباوری متخصصان در نقش عوامل مؤثر بر تأثیرگذاری بر امنیت سیستم‌های اطلاعاتی پرداخته‌اند (۱۳۸۸). در ارتباط با موضوع شرایط امنیت داده‌ها در کتابخانه‌های دیجیتال پژوهش «حریری و نظری» به ابعاد این حوزه همچون سازماندهی امنیت اطلاعات، ارزیابی مدیریت دارایی‌ها، امنیت فیزیکی و محیطی، خط‌مشی امنیت، مدیریت ارتباطات و عملیات، امنیت

منابع انسانی، کنترل دسترسی، تهیه و توسعه و نگهداری سیستم‌های اطلاعاتی، و مدیریت حوادث می‌پردازد (۱۳۹۱). در خصوص نقش چالش‌های امنیتی می‌توان پژوهش «عیدی قلعه‌شیری» را معرفی کرد که به روش‌های رمزنگاری اطلاعات و نیز سامانه‌های جدید مدیریت داده و مسائل امنیتی به‌منظور بهره‌گیری از پروتکل‌های امنیتی نظیر پروتکل ایمنی انتقال ابرمتن[1] می‌پردازد (۱۳۹۵). همچنین، در خصوص الگوهای مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتال باید به پژوهش «رضوانی» اشاره کرد که نقش متغیرهای خط‌مشی امنیت اطلاعات، معماری اطلاعات، سازماندهی امنیت اطلاعات، توسعهٔ سیستم‌های اطلاعاتی، امنیت منابع انسانی و حفاظت محتوا را مورد مطالعه قرار داده است (۱۳۹۷). در حوزهٔ مطالعات امنیت رایانش ابری در کتابخانهٔ دیجیتال می‌توان تحقیق «منگ و گونگ» را معرفی کرد که به سازوکار رمزگذاری همگن دربارهٔ محاسبات ابری کتابخانه پرداخته‌اند (Meng & Gong 2013). در خصوص سیستم‌های اطلاعاتی امنیت می‌توان پژوهش «دی سارنو» و همکاران را معرفی کرد که پیکربندی ساختار امنیتی را مورد بررسی قرار داده‌اند (Di Sarno et al. 2016). مطالعه دربارهٔ امکان‌سنجی بهبود امنیت کتابخانه‌ها کاری است که توسط «هان» و همکاران انجام شده و انواع تهدید و آسیب‌پذیری را با استفاده از سیستم ارزیابی امنیت از راه دور مورد بررسی قرار داده‌اند (Han et al. 2016). در همین موضوع پژوهش «سینگ» را نیز می‌توان معرفی کرد. او نشان داد که کنترل‌های مؤثر، امنیت سیستم اطلاعاتی را تأمین می‌کنند که شامل درستی، صداقت و ایمنی فعالیت‌ها و منابع سیستم اطلاعاتی است و کنترل‌ها می‌توانند خطاها، نفوذ و تخریب را در سیستم‌های اطلاعاتی اینترنتی که کاربران و سازمان‌ها به آن متصل می‌شوند، به حداقل برساند (Singh 2019). در موضوع ارزیابی خطرهای امنیتی اطلاعات در کتابخانه‌های دیجیتال نیز باید به پژوهش «هانگ» و همکاران اشاره کرد که با بهره‌گیری از روش ارزیابی جامع فازی و یک روش پژوهش تخصصی به ارائهٔ مدلی برای محاسبهٔ ارزش دارایی‌ها و شدت خطرات پیش روی کتابخانه‌های دیجیتال پرداخته و بیش از ۳۰۰۰ خطر در ابعاد و زمینه‌های مختلف را شناسایی کردند (Huang et al. 2019).

بررسی پیشینه‌های پژوهش نشان می‌دهد که ابعاد متعددی در امنیت اطلاعات کتابخانه‌های دیجیتال وجود دارد. از آن جمله است: فرهنگ و مهارت‌های امنیتی کارکنان،

1. hypertext transfer protocol secure (HTTPS)

داشتن خط‌مشی امنیتی، امنیت در ارتباطات شبکه، دسترسی به محتوا و منابع دیجیتال، ذخیره و بازیابی مستندات و مدارک، بررسی حملات احتمالی، سیاست‌های امنیتی، احراز هویت، روش‌های رمزگذاری، فرایند رمزگذاری همگن، پیکربندی مناسب، شناخت خطا و حل آن‌ها، دسترسی کاربران، و استانداردها و مسائل قانونی در بهره‌گیری. بررسی‌ها بیشتر با روش پیمایشی و مطالعهٔ موردی و با کمک پرسشنامه و سیاههٔ وارسی انجام شده و در آن‌ها ابعاد و جوانب مؤلفه‌های امنیتی در حوزه‌های مختلف در کتابخانه‌های دیجیتال و نیز کتابخانه‌های معمولی مطالعه شده است. همچنین، در این پژوهش‌ها کمتر به بررسی کتابخانه‌های دیجیتال همسطح از نظر نوع منابع و موضوع توجه شده است. آنچه که در این پژوهش بیشتر مورد نظر است بررسی این جنبه در کتابخانه‌های دیجیتال است.

۳. روش پژوهش

روش پژوهش پیمایشی-تحلیلی و از نوع کاربردی است. جامعهٔ پژوهش، کتابخانه‌های دیجیتالی «شهرستان قم» اعم از عمومی و دانشگاهی است. در پژوهش حاضر، کتابخانه‌های دیجیتال مراکزی هستند که بر مبنای اهداف و مأموریت‌های ویژهٔ خود و با استفاده از متخصصان و حرفه‌مندان، مدارک اطلاعاتی دیجیتال را به‌صورت دیجیتال ذخیره‌سازی می‌کنند و پس از سازماندهی این‌گونه منابع اطلاعاتی، آن‌ها را در اختیار کاربران خود قرار می‌دهند. کتابخانه‌های مورد نظر از نرم‌افزارهای تولیدشده توسط شرکت‌های مطرح در حوزهٔ کتابخانه‌های دیجیتال مانند «پارس‌آذرخش»، «نوسا»، «پروان‌پژوه»، «پاپیروس»، «وستا» و ... استفاده می‌کنند.

برای گردآوری داده‌ها از پرسشنامه‌ای که بر مبنای استاندارد «ایزو ۲۷۰۰۲» تهیه شده، استفاده شده است. پرسشنامه شامل هفتادودو سؤال دووجهی (یک برای بلی و صفر برای خیر) برای سنجش یازده شاخص و هفتادونه زیرشاخص قابلیت‌های دسترسی به موارد مربوط به امنیت اطلاعات در کتابخانه‌های دیجیتال «شهرستان قم» است. از این نظر شاخص‌های مطرح‌شده برای ارزیابی شامل موارد مهمی چون مؤلفهٔ سازماندهی امنیت اطلاعات، خط‌مشی امنیتی، امنیت منابع انسانی، مدیریت دارایی، امنیت فیزیکی و محیطی، مقولهٔ توسعه و نگهداری سیستم‌های اطلاعاتی، مؤلفهٔ مدیریت ارتباطات و عملیات، عامل کنترل دسترسی، مدیریت حوادث، بحث امنیت اطلاعات، و همچنین عامل مدیریت تداوم کسب‌وکار و سازگاری است که هر کدام متشکل از زیرشاخص‌هایی هستند که با

پاسخ‌های بلی و خیر ارزیابی می‌شوند. برای انجام پژوهش، نخست، آمار کتابخانه‌های «شهرستان قم» به‌دست آمد و مشخص شد که تعداد ۸۲ مورد کتابخانه به شکل رسمی به ثبت رسیده‌اند که تعداد ۳۰ مورد از آن‌ها دارای شاخص‌هایی از کتابخانه‌های دیجیتال الکترونیکی و مجازی بودند. با بررسی بیشتر و کسب اطلاعات دقیق از کتابخانه‌های دیجیتال «شهرستان قم» مشخص شد که تنها پنج کتابخانه دارای معیارهای کامل کتابخانهٔ دیجیتال هستند. بنابراین، پرسشنامه به پنج کتابخانهٔ مورد نظر ارسال و از مسئولان کتابخانه‌ها درخواست شد به آن‌ها پاسخ دهند و در نهایت، نتایج حاصل از این پنج کتابخانه مورد بررسی و تحلیل قرار گرفت.

برای مشخص‌کردن میزان امنیت در ارزیابی داده‌ها، میانگین پاسخ‌ها در بازهٔ صفر تا یک به سه سطح تقسیم شده است؛ به‌این‌ترتیب که میانگین ۰ – ۰/۳۴ نشانگر سطح ضعیف، ۰/۳۵– ۰/۶۷ سطح متوسط و ۰/۶۸ –۱ سطح قوی است. برای ارزیابی و تحلیل داده‌ها از نسخهٔ ۲۱ نرم‌افزار آماری «اس‌پی‌اس‌اس» بهره گرفته شد. روایی پرسشنامه با بهره‌گیری از تأیید صوری انجام پذیرفت که مورد تأیید و بررسی متخصصان در زمینهٔ امنیت اطلاعات و از جمله مسئولان کتابخانه‌ها نیز بود. سنجش پایایی پرسشنامه توسط آزمون آماری آلفای «کرونباخ» انجام شد که مقدار آن برای نمونهٔ پنج کتابخانه برابر با ۰/۸۹ به‌دست آمد و این نشان‌دهندهٔ پایایی ابزار گردآوری اطلاعات است.

٤. یافته‌های پژوهش

بررسی پژوهش با توجه به شاخص اصلی وجود ویژگی‌های مورد مطالعه در پنج کتابخانه انجام پذیرفت. این کتابخانه‌ها از نوع دیجیتال بوده و دارای منابع دیجیتال هستند که به کاربران خود خدمات اطلاعاتی ارائه می‌دهند. در جدول ۱، کتابخانه‌های دیجیتالی که در نمونهٔ جامعهٔ آماری قرار داشتند، با توجه به نوع کتابخانه، تعداد منابع، و نرم‌افزار مورد استفاده معرفی شده‌اند.

بر اساس اطلاعات به‌دست‌آمده، «کتابخانهٔ نورلایب»، «کتابخانهٔ دیجیتال کوثر»، «کتابخانهٔ تخصصی فقه و اصول»، «کتابخانه ادیان و مذاهب»، و «کتابخانهٔ دیجیتال دفتر تبلیغات اسلامی حوزهٔ علمیهٔ قم» پنج کتابخانه‌ای بودند که در این پژوهش مورد مطالعه قرار گرفتند. در این میان «کتابخانهٔ دیجیتال دفتر تبلیغات حوزهٔ علمیهٔ قم» از نوع عمومی بود و چهار کتابخانهٔ دیگر از نوع تخصصی هستند. بالاترین تعداد مدارک نگهداری‌شده

مربوط به «کتابخانهٔ تخصصی دانشگاه ادیان و مذاهب قم» بود که بالغ بر ۵۴,۷۸۵ مدرک است. کمترین تعداد مدرک نیز مربوط به «کتابخانهٔ دیجیتال دفتر تبلیغات حوزهٔ علمیهٔ قم» است که ۷,۱۸۶ منبع دیجیتال دارد.

بررسی‌های انجام‌شده نشان داد که در بیشتر این کتابخانه‌ها (۸۰ درصد) از سیستم‌عامل ویندوز استفاده می‌کنند و از این میان، حدود ۲۰ درصد آن‌ها از سیستم‌عامل ویندوز XP بهره می‌گیرند. تنها ۴۰ درصد از کتابخانه‌ها دارای IP اختصاصی بوده و تمام خدمت‌دهنده‌ها توسط کتابخانه پشتیبانی می‌شوند. همچنین، در بررسی نرم‌افزار مورد استفاده در این کتابخانه‌ها روشن شد که بیشترین نرم‌افزار مورد استفاده در این کتابخانه‌ها نرم‌افزار «سیمرغ شرکت نوسا» (۶۰ درصد) بوده و یک کتابخانه (۲۰ درصد) از نرم‌افزار «نور» و یک کتابخانه (۲۰ درصد) نیز از نرم‌افزار «آذرسا شرکت پارس‌آذرخش» استفاده می‌کنند.

جدول ۱. اطلاعات کتابخانه‌های دیجیتال «شهرستان قم»

ردیف	نام کتابخانه	نوع	تعداد مدارک	نرم‌افزار
۱	کتابخانهٔ دیجیتال نورلایب	تخصصی	۲۴,۰۰۰	نور
۲	کتابخانهٔ دیجیتال کوثر	تخصصی	۳۴,۲۷۴	پارس آذرخش
۳	کتابخانهٔ تخصصی فقه و اصول	تخصصی	۲۶,۲۴۴	سیمرغ
۴	کتابخانهٔ تخصصی دانشگاه ادیان و مذاهب	تخصصی	۵۴,۷۸۵	سیمرغ
۵	کتابخانهٔ دیجیتال دفتر تبلیغات اسلامی حوزهٔ علمیهٔ قم	عمومی	۷,۱۸۶	سیمرغ

پاسخ به سؤال اول پژوهش: امنیت اطلاعات در کتابخانه‌های دیجیتال «شهرستان قم» تا چه میزان قابل دستیابی است؟

با توجه به آنچه در جدول ۲، نشان داده شده، می‌توان گفت که میانگین امنیت اطلاعات در بین کتابخانه‌های دیجیتال «شهرستان قم» برابر ۰/۸۰۱ ارزیابی شده و با توجه به روش ارزیابی می‌توان گفت که از سطح قوی برخوردار است.

جدول ۲. میانگین و انحراف معیار امنیت اطلاعات کتابخانه‌های دیجیتال «شهرستان قم»

	میانگین	انحراف معیار	تعداد
امنیت اطلاعات	۰/۸۰۱	۰/۱۱۵	۵

پاسخ به سؤال دوم پژوهش: آسیب‌پذیرترین نقاط امنیتی در کتابخانه‌های دیجیتال «شهرستان قم» کدام‌اند؟

با توجه به داده‌های جدول ۳، مشاهده می‌شود که کمترین میزان مربوط به امنیت فیزیکی و محیطی (۰/۷۵۰) و بعد از آن تهیه، توسعه و نگهداری سیستم‌های اطلاعاتی (۰/۷۶۶) و امنیت منابع انسانی (۰/۷۶۶) بوده و بیشترین مقدار مربوط به مدیریت تداوم کسب‌وکار (۰/۹۰۰) و کنترل دسترسی (۰/۸۲۰) است. با توجه به این داده‌ها می‌توان گفت که آسیب‌پذیرترین قسمت مربوط به امنیت فیزیکی و محیطی و بعد از آن خط‌مشی، تهیه، توسعه و نگهداری سیستم‌های اطلاعاتی و امنیت منابع انسانی است.

جدول ۳. میانگین و انحراف معیار شاخص‌های امنیت اطلاعات کتابخانه‌های دیجیتال در «شهرستان قم»

	میانگین	انحراف معیار
امنیت فیزیکی و محیطی	۰/۷۵۰	۰/۱۷۶
مدیریت ارتباطات و عملیات	۰/۸۱۴	۰/۱۰۸
کنترل دسترسی	۰/۸۲۰	۰/۱۰۳
تهیه و توسعه و نگهداری سیستم‌های اطلاعات	۰/۷۶۶	۰/۲۲۳
امنیت منابع انسانی	۰/۷۶۶	۰/۱۴۹
مدیریت دارایی‌ها	۰/۸۰۰	۰/۲۰۹
سازماندهی اطلاعات	۰/۸۰۰	۰/۱۶۴
مدیریت تداوم کسب‌وکار	۰/۹۰۰	۰/۲۲۳
سازگاری	۰/۸۰۰	۰/۱۳۹
مدیریت حوادث	۰/۸۰۰	۰/۲۱۷
خط‌مشی امنیت	۰/۸۰۰	۰/۲۷۳

پاسخ به سؤال سوم پژوهش: نقاط قوت و ضعف امنیتی کتابخانه‌های دیجیتال «شهرستان قم» کدام‌اند؟

با توجه به داده‌های ارائه‌شده در نمودار ۱، مشاهده می‌شود که بالاترین مقدار در زمینهٔ امنیت اطلاعات مربوط به مدیریت تداوم کسب‌وکار (۰/۹۰۰) است که در حقیقت نقطهٔ قوت مربوط به امنیت اطلاعات را در کتابخانه‌های دیجیتال را به خود اختصاص داده

و نقاط ضعف این کتابخانه‌ها مربوط به امنیت فیزیکی و محیطی (۰/۷۵۰)، تهیه، توسعه و نگهداری سیستم‌های اطلاعاتی (۰/۷۶۶) و امنیت منابع انسانی (۰/۷۶۶) است.

نمودار ۱. آسیب‌پذیری مؤلفه‌ها بر حسب میانگین

۵. بحث و نتیجه‌گیری

یافته‌های پژوهش نشان می‌دهد که میانگین امنیت اطلاعات در بین کتابخانه‌های دیجیتال «شهرستان قم» بر اساس ۱۱ مؤلفهٔ امنیت فیزیکی و محیطی، مدیریت ارتباطات و عملیات، کنترل دسترسی، تهیه و توسعه و نگهداری سیستم‌های اطلاعات، امنیت منابع انسانی، مدیریت دارایی‌ها، سازماندهی اطلاعات، مدیریت تداوم کسب‌وکار، انطباق، مدیریت حوادث، و خط‌مشی امنیت از نمرهٔ کل ۱ برابر ۰/۸۰۱ و نقطه برش ۰/۰۱۳ ارزیابی شده است که با توجه به معیارهای مد نظر و شیوهٔ ارزیابی در این پژوهش می‌توان گفت دارای سطح قوی امنیت اطلاعات است. در بررسی مؤلفه‌ها مشخص شد که مدیریت تداوم کسب‌وکار قوی‌ترین و امنیت فیزیکی و محیطی ضعیف‌ترین بخش امنیت کتابخانه‌های دیجیتال است.

با توجه به نتایج به‌دست‌آمده از یافته‌های پژوهش باید گفت که تلاش برای حفظ امنیت وظیفهٔ تمامی کارکنان کتابخانه‌های دیجیتال است. کارکنان در کتابخانه شامل

کاربران معمولی، کارشناسان حرفه‌ای و فنی، و نیز مدیر سیستم، افزون بر مدیر شبکه است. بنابراین، امنیت نیروی انسانی یکی از مسائل مهم در خصوص رعایت امنیت کتابخانه‌های دیجیتال است. این امر با نتایج پژوهش «حریری و نظری» (۱۳۹۱) در خصوص توجه به ضعف نیروی انسانی در کتابخانه‌های دیجیتال همسویی دارد.

دربارهٔ امنیت فیزیکی و محیطی باید گفت که این بخش همواره دارای اهمیت است و توجه به نکات اصلاحی برای تقویت محیط فعالیت دیجیتال به فرایند کاری کتابخانه‌ها برای مقابله با خطرهای پیش رو کمک می‌کند. برخی از مشکلات امنیتی در این حوزه قرار می‌گیرند. از نظر فیزیکی، هر بخش ممکن است هدف آسیب قرار بگیرد. مشکلات متعددی چون ضربه به خطوط ارتباطی و نظایر آن در این میان حائز اهمیت است. بنابراین، برنامه‌ریزی برای مقابله با چنین مشکلاتی باید در دستور کار کتابخانه‌ها قرار گیرد. نتایج Di Sarno et al. (2016) در خصوص امنیت زیرساخت‌های حیاتی و فیزیکی با نتایج این پژوهش دارای اشتراک است.

از سوی دیگر، دربارهٔ امنیت داده‌ها نگرانی وجود دارد. ذخیره‌سازی مطمئن و بهره‌گیری از اطلاعات کتابخانه‌های دیجیتال یکی از مسائل مهم حوزهٔ امنیت اطلاعات است. از این رو، افرادی که با سازوکارهای فنیِ در ارتباط با بحث ذخیره و نیز ارسال داده‌ها مربوط هستند، موضوع را از نگاه امنیتی در نظام اطلاعاتی و نیز شبکه مورد بررسی قرار می‌دهند. از سوی دیگر، برخی از حرفه‌مندان در حوزهٔ کسب‌وکار، آن را در عرصهٔ نوین تجاری و بیشتر با نگاه امنیتی در حوزهٔ مسائل الکترونیکی ارزیابی می‌کنند. به نظر می‌رسد که در کتابخانهٔ دیجیتالی باید به هر دو نگرش اهمیت داده شود. امنیت در سازماندهی اطلاعات و نگهداری داده‌های علمی در کنار تعامل اطلاعاتی با دیگر مراکز، پایانه‌ها و شبکه‌های اطلاعاتی نیازمند اجرای برنامه‌های ایمنی و حفاظت و نگهداری از این اطلاعات ارزشمند است. این موارد با یافته‌های پژوهش Singh (2019) در خصوص امنیت محتوای اطلاعاتی و Huang et al. (2019) در ارتباط با دارایی‌ها و منابع دارای همسویی است. در ارتباط با کنترل دسترسی‌ها و ارتباطات در محیط کتابخانهٔ دیجیتال توجه به مسائل ایمنی در رعایت حریم خصوصی و سطوح دسترسی کاربران، کارکنان و مدیران می‌تواند تا حد زیادی از بروز خطرهای نفوذ و دستکاری اطلاعات جلوگیری کند. در این رابطه، توجه بیشتر به لایه‌های دسترسی در کار با رابط کاربر و سیستم‌های کاری مورد توجه است. رعایت پروتکل‌های ایمنی در رمزنگاری و دستیابی به بخش‌های مختلف

کتابخانه نیز از اهمیت برخوردار است. یافته‌های Meng & Gong (2013) در زمینهٔ رمزنگاری و Singh (2019) در خصوص امنیت جلوگیری از نفوذ با مطالعهٔ پیش رو دارای اشتراک است.

توسعه و نگهداری سیستم‌های اطلاعاتی امری است که همواره برای پیشرفت و ارائهٔ خدمات مؤثر در کتابخانه‌های دیجیتال نقشی مؤثر داشته است. این امر با تداوم فعالیت کاری کتابخانه مرتبط است و بر این اساس، به هر میزان که سیستم‌ها از امنیت بیشتری برخوردار باشند، برونداد اطلاعاتی در دسترس کاربران بهتر قرار می‌گیرد. باید همواره توجه کرد که سیستم‌های اطلاعاتی برای آسیب‌رسانی می‌توانند به‌عنوان اهداف تهاجمی لحاظ شوند. دلایل چنین آسیب‌هایی ممکن است شامل عواملی چون گرفتن انتقام، سرگرمی، رقابت و یا مواردی از این قبیل باشد. رعایت برنامه‌های ارتقای سیستم در قالب یک طرح مدون و حساب‌شده سبب جلوگیری از وارد آمدن خسارت به این سیستم‌ها خواهد شد. بهره‌گیری از برنامه‌های کاربردی اصلی و مطمئن و نیز بهره‌گیری از انواع ابزارهای دفاعی مانند دیواره‌های آتش و لایه‌های چندگانهٔ ایمنی می‌تواند تا حد زیادی در این زمینه سودمند باشد. پژوهش‌های «عیدی قلعه‌شیری» (۱۳۹۵)، Di Sarno et al. (2016) در کنار تحقیق Han et al. (2016) مؤید مطالب پیش‌گفته است.

باید به این نکتهٔ مهم نیز اشاره کرد که تدوین خط‌مشی امنیت سبب خواهد شد که کتابخانه‌ها با بهره‌گیری از یک برنامهٔ راهبردی و کارا توانایی خود را برای مقابله با خطرهای مهم افزایش داده و ایمنی خود را تضمین کنند. این خط‌مشی باید شامل پروتکل‌ها، نکات امنیتی، ساختار ایمنی در ابعاد مختلف و استفاده از استانداردهای مطرح و روزآمد باشد. در این رابطه نتایج پژوهش‌های «الهی، طاهری و حسن‌زاده» (۱۳۸۸)، «رضوانی» (۱۳۹۷)، Di Sarno et al. (2016) و نیز Huang et al. (2019) دارای اشتراک با این مؤلفه است.

باید گفت که توجه به اهمیت امنیت سبب می‌شود که برخی فعالیت‌های ضروری به‌منظور حفاظت در خصوص سیستم‌ها انجام گیرد و سیاست‌گذاری‌های مناسب برای رعایت مسائل امنیتی، اقدام سودمندی در این عرصه است. در این صورت در بیشتر موارد رایانه‌ها و اطلاعات از دسترسی‌های غیرمجاز ایمن خواهند بود و امکان تبادل ایمن اطلاعات با دیگران در شبکه میسر می‌شود. طراحی برنامه‌های اصولی در حوزهٔ مسائل امنیتی سیستم‌ها برای مقابله با تهدیدهای وسیع امنیتی یکی از موارد ضروری برای کتابخانه‌های دیجیتال است. تدابیر مطلوب میزان احتمال وقوع خطرهای پیش رو

را کاهش می‌دهد. باید توجه کرد که با برنامه‌ریزی مدون می‌توان آسیب‌های احتمالی را در سطح پایین نگه داشت و توان مقابلهٔ مؤثر را بالا برد، به‌طوری که کتابخانه‌های دیجیتال بتوانند خسارت‌ها را با توجه به فرایندهای تعریف‌شده کاهش دهند. از طرف دیگر، با برنامه‌ریزی می‌توان امنیت داده‌ها را افزایش داده و فعالیتی امن را تجربه کرد. در این زمینه، حتی مواردی چون سرقت دستگاه‌ها و قطعات، حفاظت از سخت‌افزارها و نرم‌افزارها، و نیز مسائل مربوط به پیشگیری حوادثی مانند آتش‌سوزی، نشت آب، ایجاد غبار و یا دود، کنترل میزان دما و حرارت یا خشه‌های الکتریکی، ضبط صدا به‌صورت غیرمجاز و ... در کتابخانه همگی دارای اهمیت هستند.

باید تصریح کرد که منابع انسانی نقش مهمی در امنیت کتابخانه‌ها دارند. اهمیت آن به این دلیل است که نیروی انسانی نقش مؤثری در روش‌های بهره‌گیری از فناوری بر عهده دارند. افزون بر آن، انواع اشتباه‌ها و خطاهای انسانی در کاهش یا افزایش میزان امنیت اطلاعات مؤثرند. کنترل این عوامل سبب پیشگیری از مشکل‌های بعدی می‌شود. این است که موارد زیر باید رعایت شود:

کتابخانه‌های دیجیتال لازم است سند خط‌مشی امنیت اطلاعات را با بیان هدف‌های خود، هم در عرصهٔ برنامه‌ریزی بلندمدت، و هم در خصوص برنامه‌های کوتاه‌مدت، در کنار عامل مسئولیت‌پذیری بخش‌ها و واحدهای مختلف و پست‌های اجرایی و فنی در راستای هدف‌ها اعلام کنند. همچنین، ضرورت دارد که متخصصان فنی با آگاه‌سازی مدیریت کتابخانه نسبت به اجزای سند به آنان کمک کنند تا وظایف حرفه‌ای خود را در مقابل سند خط‌مشی شناخته و به آن عمل کنند. از موارد دیگر اینکه شرح وظایف مشاغل، به‌ویژه در زمینهٔ مسئولیت‌های امنیتی لازم است بازنگری شود.

پیشنهاد می‌شود مدیران کتابخانه‌های دیجیتال «شهرستان قم» برای حفاظت از مدارک موجود در کتابخانه‌ها به‌منظور رعایت پروتکل‌های امنیتی و مسائل مربوط به نرم‌افزارها و سخت‌افزارهای موجود، از روش‌های سودمند و علمی در عرصهٔ پدافند غیرعامل بهره گیرند و با مشارکت گروه‌های امنیتی برای جلوگیری از فعالیت هکرها و اقدام‌های آسیب‌رسان آن‌ها برنامه‌ریزی کنند. در کنار مسائل مطرح‌شده ضروری است کتابخانه‌ها با شناسایی و مشخص ساختن حفره‌های امنیتی، به‌منظور پیشگیری از چنین مشکلاتی اقدام لازم به عمل آورده و نسبت به آموزش نیروی‌های متخصص علم اطلاعات و کارکنان کتابخانه‌ها مبادرت ورزند تا آنان بتوانند در موارد لازم با شناخت نکات امنیتی فعالیت مؤثری به عمل

آورنـد. افـزون بـر آن، داشـتن برنامـهٔ اجرایـی امنیـت اطلاعـات برابـر بـا خط‌مشـی مـدون سـبب می‌شـود کـه کتابخانه‌هـا برنامه‌هـای عملیاتـی خـود را تنظیـم کـرده و بـه روزآمدسـازی آن‌هـا در بازه‌هـای زمانـی میان‌مـدت مبـادرت ورزنـد.

فهرست منابع

الهی، شـعبان، مهـدی طاهـری، و علیرضـا حسـن‌زاده. ۱۳۸۸. ارائـهٔ چارچوبـی بـرای عوامـل انسـانی مرتبـط در امنیـت سیسـتم‌های اطلاعاتـی. *پژوهش‌هـای مدیریـت در ایـران* ۶۱: ۱-۲۲.

حریـری، نجـلا، و زهـرا نظـری. ۱۳۹۱. امنیـت اطلاعـات در کتابخانه‌هـای دیجیتـال ایـران. *فصلنامـه کتابـداری و اطلاع‌رسـانی* ۱۵ (۲): ۶۱-۹۰.

رضوانـی، شـهلا. ۱۳۹۷. طراحـی الگـوی مدیریـت امنیـت اطلاعـات در کتابخانه‌هـای دیجیتـال. *پژوهشـنامه کتابـداری و اطلاع‌رسـانی* ۸ (۱): ۳۳۷-۳۵۶.

عیـدی قلعه‌شـیری، داود. ۱۳۹۵. ارزیابـی چالش‌هـای امنیتـی طراحـی کتابخانه‌هـای دیجیتـال (مطالعـهٔ مـوردی: کتابخانـهٔ دیجیتالـی آسـتان قـدس رضـوی). پایان‌نامـهٔ کارشناسـی ارشـد. دانشـگاه گیـلان، مرکـز آمـوزش الکترونیکـی.

References

Anday, A., E. Francese, H. C. Huurdeman, M. Yilmaz, & D. Zengenene2012 .. Information Security Issues in a Digital Library Environment: A Literature Review. *Information World/Bilgi Dunyasi* 13 (1): 117-137.

Awad, A. I., & M. Fairhurst. 2018. *Information Security: Foundations, Technologies and Applications.* Herts (United kingdom): Institution of Engineering and Technology.

Bârsan, M. 2017. Aspects regarding the implementation of information security standards in organizations. *Revista Română de Biblioteconomie și Știința Informării* 13 (1): 21-26.

Candela, L., Y. I. Castelli, S. Ross, C. Thanos, P. Pagano, G. Koutrika, ... & H. Schuldt. 2007. Setting the foundations of digital libraries. *D-Lib Magazine* 13 (3/4): Retrieved from: http://www.dlib.org/dlib/march07/castelli/03castelli.html (accessed: April 20, 2020)

Di Sarno, C., A. Garofalo, I. Matteucci, & M. Vallini. 2016. A novel security information and event management system for enhancing cyber security in a hydroelectric dam. *International Journal of Critical Infrastructure Protection* 13: 39-51.

Han, Z., S. Huang, H. Li, & N. Ren. 2016. Risk assessment of digital library information security: a case study. *The Electronic Library* 34 (3): 471-487.

Hao, T. 2015. The information security analysis of digital library. In 2015 8th *International Conference on Intelligent Computation Technology and Automation (ICICTA)* (983-984). IEEE. Nanchang, China.

Huang, S., Z. Han, B. Yang, & N. Ren. 2019. Factor identification and computation in the assessment of information security risks for digital libraries. *Journal of Librarianship and Information Science* 51 (1): 78-94.

Jiang, Q., L. Lin, & Y. He. 2018. Analysis on Network Security and Its Countermeasures. *Information and Computer Security (TRANSFERRED)* 1 (1): 1-5.

Liu, S. 2014. *Design of Network System Security System of Digital Library. In Applied Mechanics and Materials* (644, 3212-3215). Baech: Trans Tech Publications Ltd.

Liu, Y. 2019. Risk and Preventive Strategy of Network Security in University Digital Library. In: *9th International Conference on Management, Education and Information* (MEICI 2019). Bali, Indonesia.

Meng, Q., & C. Gong. 2013. Research of cloud computing security in digital library. In *6th International Conference on Information Management, Innovation Management and Industrial Engineering* (2, 41-44). IEEE. Xi'an, China.

Nandagaoli, J. M., & S. R. Lihitakar. 2019. Information Security Measures for Web Based Digital Library Management System. *Journal of Advancements in Library Sciences* 6 (1): 90-98.

Shiri, A. 2003. Digital library research: current developments and trends. *Library review* 52 (5): 198-202.

Singh, M. A. K. 2019. Digital Library and its Security Issues: An Overview. *Journal Current Science* 20 (1). Retrieve from: http://www.ijournal.scienceacad.com [accessed: (accessed: April 20, 2020)

Soleimanzade, N., A. Asemi, M. CheshmehSohrabi, & A. Shabani. 2019. The Scientific Information Exchange General Model at Digital Library Context: Internet of Things. *Library Philosophy and Practice*. 2150, Retrieve from:http://digitalcommons.unl.edu/libphilprac/2150 (accessed: April 20, 2020)

Zhang, X., D. L. Song, & S. Yan.2016 . The Security Research of Digital Library Network. In Mechanical Engineering and Control Systems: Proceedings of 2015 *International Conference on Mechanical Engineering and Control Systems* (MECS2015) (232-235). Wuhan, China.

Zhao, L., L. Zhang, & D. Wang. 2018. Security Management and Operation Mechanism of Digital Libraries in Military Academies. *In 3rd International Conference on Contemporary Education, Social Sciences and Humanities* (ICCESSH 2018). Atlantis Press. Moscow, Russia.

فریبرز درودی

متولد ۱۳۴۶، دارای مدرک دکتری تخصصی علم اطلاعات و دانش‌شناسی از دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران است. ایشان هم‌اکنون استادیار گروه پژوهشی علم‌سنجی و تحلیل اطلاعات در پژوهشکدهٔ علوم اطلاعات پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) است.

حوزه‌های مطالعاتی فناوری اطلاعات، دیداری‌سازی اطلاعات و سواد دیداری از جمله علایق پژوهشی وی است.

زینب جمشیدی

متولد ۱۳۶۹، دارای مدرک تخصصی کارشناسی ارشد در علم اطلاعات و دانش‌شناسی از دانشگاه آزاد اسلامی واحد همدان است.

کتابخانه‌های دیجیتال و امنیت اطلاعات از جمله علایق پژوهشی وی است.