**به نام خدا**

**موضوع پایان نامه**

ابعاد حقوقی امنیت اطلاعات در کتابخانه‌های دیجیتال

**گرد آورنده**

**استاد**

**بهار 97**

**چکیده**

برخلاف تصور برخی افراد، هدف متخصصان از راه اندازی کتابخانه دیجیتال به آتش کشیدن ساختمان کتابخانه ها و قرار دادن کتاب های موجود در آنها در جعبه های الکترونیکی نیست. کتابخانه دیجیتال صورت جدیدی از فناوری ذخیره و بازیابی اطلاعات است که در کنار کتابخانه های سنتی موجود متولد شده و به حیات خود ادامه می دهد. در واقع بشر پس از سال ها تلاش موفق شده از فناوری و تکنولوژی های مدرن به منظور دسترسی به اطلاعات مورد نیاز خود بهره گیرد.

با اینحال یکی از شاخصه های مهم کتاب خانه های دیجیتال، امنیت اطلاعات موجود در آنها است. حفظ اطلاعات و محرمانه ماندن آنها باید در اولویت کتابخانه های دیجیتال باشد. از این رو قوانین مختلف حقوقی برای مقابله با متخلفان وضع گردیده است. همچنین تلاش های بسیاری به منظور ارتقا سیستم های امنیتی صورت گرفته است.

در این پژوهش، در ابتدا به تعریف کتابخانه دیجیتال و ابعاد آن پرداخته شده است. سپس امنیت اطلاعات و خصوصیات آن به طور کامل توضیح داده شده اند. در ادامه بحث مقالات و منابع مطالعه شده در این زمینه ارائه شدند و سعی شد تا خلاصه مفیدی از این مقالات ارائه شود. در بخش سوم، روش کار انجام شده بیان گردید. در این پژوهش از نظر سنجی به منظور جمع آوری داده ها استفاده شد. در بخش نتایج، جداول و داده های حاصل شده بیان گردید. در نهایت در بخش نتیجه گیری برخی از نتایج مهم این پژوهش آورده شده اند. همچنین پیشنهاداتی به منظور ارتقا امنیت اطلاعات در کتابخانه های دیجیتال به منظور بررسی های بعدی، ارائه شده اند.

**1- مقدمه**

کتابخانه زمانی متولد شد که کشاورزی مهم‌ترین مشغلۀ ذهنی بشریت بود. در زمان رنسانس با اختراع چاپ، کتابخانه‌ها جانی دوباره گرفتند و در زمان انقلاب صنعتی که اختراعات جدید، فرایند چاپ را ماشینی کرد، کتابخانه‌ها نیز به اوج شکوفایی خود رسیدند. در طول سال‌ها کتابخانه‌ها دورۀ تکاملی باور نکردنی را پشت سر گذاشته‌اند. این مؤسسات که در ابتدا فقط برای نگهداری و ذخیره مدارک ابداع شده بودند، تبدیل به مراکزی جهت تبادل اطلاعات گردیدند. اکنون در آستانه دوران کتابخانه‌های دیجیتالی هستیم. با وقوع انقلاب اطلاعات، کتابخانه‌های دیجیتالی به فناوری قدرتمندی برای رشد و ترقی دست یافتند و روش‌های جدیدی نیز برای ذخیره، سازمان‌دهی و دسترسی به اطلاعات پیش روی آنها گذاشته شد. اگر اطلاعات را پول رایج دانش در نظر بگیریم، کتابخانه‌های دیجیتالی به منزلۀ بانک‌هایی برای سرمایه‌گذاری هستند.

شبکه جهانی وب تصویر واقعی از دنیای بی‌نظم و بی‌سامانی است که در نتیجۀ رشد تصاعدی مجموعۀ آن ایجاد گردیده و از طرفی وقایع ربع قرن گذشته، کتابداران را در ادامه حیات کتابخانه‌های سنتی مردد کرده است.

کنگره ملی آمریکا در سال 1990 طرحی به نام «برنامه کتابخانه ملی دیجیتالی» را اجرا کرد. هدف کتابخانه کنگره ملی آمریکا از اجرای این طرح ایجاد کتابخانه‌ای دیجیتالی از بازتولیدات منابع ردیف اول برای حمایت از مطالعات تاریخی و فرهنگی ایالات متحده بود. این طرح بعد از 5 سال مطالعه آزمایشی در سال 1995 آغاز شد. منابع از مجموعه آرشیو کتابخانه کنگره انتخاب و دیجیتالی شدند. این منابع بازنمود میراث فرهنگی اقوام مختلف به ترتیب تاریخی بودند. به منظور بازتولید مجموعه‌هایی از کتاب‌ها، کتابچه‌ها، تصاویر متحرک، دست نوشته‌ها و صداهای ضبط شده، کتابخانه کنگره طیف وسیعی از شیءهای دیجیتالی ایجاد کرده است. تصاویر دودویی، تصاویر با زمینه خاکستری، تصاویر رنگی، فایلهای ویدئویی و صوتی دیجیتالی و متون قابل جستجو از جمله این شیءهای دیجیتالی هستند. برای تأمین امکانات دستیابی به منابع بازتولیدی، ارکان توصیفی مانند : رکوردهای کتابشناختی، «راهنماهای بازیابی»، متون و برنامه‌های مقدماتی تعریف شدند. همچنین نمایه سازی تمام متن برای انواع محتواهای خاص انجام گرفت. در ادامه صفحه اصلی کتابخانه دیجیتالی آمریکا را که مجموعه تاریخی کتابخانه ملی پوشش می‌دهد، مشاهده می کنید.



شکل1- صفحه اصلی مجموعه تاریخی کتابخانه ملی دیجیتالی( (<http://www.memory.loc.gov/>

مهم‌ترین دلیل ایجاد کتابخانه‌های دیجیتالی فراهم نمودن شرایطی است تا ارائه اطلاعات بهتر از گذشته امکان‌پذیر باشد. این کتابخانه‌ها، مؤسسات یا سازمان‌هایی هستند که منابع مختلف شامل منابع انسانی و تجهیزات موردنیاز برای ارائه خدمات کتابخانه‌ای مثل فهرست نویسی، رده بندی، اطلاع رسانی، روابط بین کتابخانه‌ای، مواد آموزشی، منابع کتابخانه‌ای و دیگر خدمات را با استفاده از شبکه‌های پرسرعت مهيا می‌سازند.

متأسفانه امروزه دانشجویان علوم و فناوری، کتابخانه را شبکه جهانی وب تصور می‌کنند یا یک مرحله نیز فراتر رفته، وب را کتابخانه‌ای ایده آل تصور می‌نمایند. اما چنین تصوری درست نیست. کتابخانه دیجیتالی به این معنی نیست که واقعاً «کتابخانه دیجیتالی شده» و باید مجموعه کتاب‌ها را ندیده بگیریم، ساختمان کتابخانه‌ها را از بین ببریم و در منزل خود با یک رایانه شخصی به‌مرور هر آنچه که می‌خواهیم بپردازیم. کتابخانه دیجیتالی آرزوی برآورده شدۀ انسان عصرِ تمدن در تغییر روش دسترسی به اطلاعات است. کتابخانه دیجیتالی روش جدیدی برای نگهداری، سازمان‌دهی، اشاعه و دستیابی به دانش هست. کتابخانه دیجیتالی به معنی ویران کردن مؤسساتِ موجود و قرار دادن کل آن مجموعه‌ها در جعبه‌های الکترونیکی نیست. کتابخانه دیجیتالی مجموعه‌ای متشکل از «شیءهای دیجیتالی» است. شیءهای دیجیتالی شامل متون، تصویر و صدا هست. امکانات «دسترسی و بازیابی» به اطلاعات در این کتابخانه وجود دارد و کار « انتخاب، سازمان‌دهی و نگهداری» مجموعه نیز در آن انجام می‌شود.

امنیت اطلاعات یعنی حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز. این فعالیت‌ها عبارت‌اند از دسترسی، استفاده، افشاء، خواندن، نسخه‌برداری یا ضبط، خراب کردن، تغییر، دست‌کاری. واژه‌های امنیت اطلاعات، امنیت کامپیوتری و اطلاعات مطمئناً گاهی به اشتباه به جای هم بکار برده می‌شود. اگر چه این‌ها موضوعات به هم مرتبط هستند و همگی دارای هدف مشترک حفظ محرمانگی اطلاعات، یکپارچه بودن اطلاعات و قابل دسترس بودن را دارند ولی تفاوت‌های ظریفی بین آن‌ها وجود دارد. این تفاوت‌ها در درجه اول در رویکرد به موضوع امنیت اطلاعات، روش‌های استفاده شده برای حل مسئله، و موضوعاتی که تمرکز کرده‌اند دارد.

امنیت اطلاعات به محرمانگی، یکپارچگی و در دسترس بودن داده‌ها مربوط است بدون در نظر گرفتن فرم اطلاعات اعم از الکترونیکی، چاپ، یا اشکال دیگر. امنیت کامپیوتر در حصول اطمینان از در دسترس بودن و عملکرد صحیح سیستم کامپیوتری تمرکز دارد بدون نگرانی از اطلاعاتی که توسط این سیستم کامپیوتری ذخیره یا پردازش می‌شود.

دولت‌ها، مراکز نظامی، شرکت‌ها، مؤسسات مالی، بیمارستان‌ها، و مشاغل خصوصی مقدار زیادی اطلاعات محرمانه در مورد کارکنان، مشتریان، محصولات، تحقیقات، و وضعیت مالی گردآوری می‌کنند. بسیاری از این اطلاعات در حال حاضر بر روی کامپیوترهای الکترونیکی جمع‌آوری، پردازش و ذخیره و در شبکه به کامپیوترهای دیگر منتقل می‌شود. اگر اطلاعات محرمانه در مورد مشتریان یا امور مالی یا محصول جدید موسسه‌ای به دست رقیب بیفتد، این درز اطلاعات ممکن است به خسارات مالی به کسب و کار، پیگرد قانونی یا حتی ورشکستگی منجر شود.

حفاظت از اطلاعات محرمانه یک نیاز تجاری، و در بسیاری از موارد نیز نیاز اخلاقی و قانونی است. برای افراد، امنیت اطلاعات تأثیر معناداری بر حریم خصوصی دارد. البته در فرهنگ‌های مختلف این مفهوم حریم خصوصی تعبیرهای متفاوتی دارد. بحث امنیت اطلاعات در سال‌های اخیر به میزان قابل توجهی رشد کرده است و تکامل یافته است.

راه‌های بسیاری برای ورود به این حوزه کاری به عنوان یک حرفه وجود دارد. موضوعات تخصصی گوناگونی وجود دارد از جمله: تأمین امنیت شبکه(ها) و زیرساخت‌ها، تأمین امنیت برنامه‌های کاربردی و پایگاه داده‌ها، تست امنیت، حسابرسی و بررسی سیستم‌های اطلاعاتی، برنامه‌ریزی تداوم تجارت و بررسی جرائم الکترونیکی، و غیره.

موارد سه‌گانه حفظ محرمانگی، یکپارچه بودن و دسترس‌پذیری از مفاهیم اصلی امنیت اطلاعات است. محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیر مجاز. به عنوان مثال، برای خرید با کارت‌های اعتباری بر روی اینترنت نیاز به ارسال شماره کارت اعتباری از خریدار به فروشنده و سپس به مرکز پردازش معامله است. در این مورد شماره کارت و دیگر اطلاعات مربوط به خریدار و کارت اعتباری او نباید در اختیار افراد غیرمجاز بیفتد و این اطلاعات باید محرمانه بماند. در این مورد برای محرمانه نگه‌داشتن اطلاعات، شماره کارت رمزنگاری می‌شود و در طی انتقال یا جاهایی که ممکن است ذخیره شود (در پایگاه‌های داده، فایل‌های ثبت وقایع سیستم، پشتیبان گیری، چاپ رسید، و غیره) رمز شده باقی می‌ماند. همچنین دسترسی به اطلاعات و سیستم‌ها نیز محدود می‌شود. اگر فرد غیر مجازی به هر نحو به شماره کارت دست یابد، نقض محرمانگی رخ داده است. نقض محرمانگی ممکن است اشکال مختلف داشته باشد. مثلاً اگر کسی از روی شانه شما اطلاعات محرمانه نمایش داده شده روی صفحه نمایش کامپیوتر شما را بخواند. یا فروش یا سرقت کامپیوتر لپ‌تاپ حاوی اطلاعات حساس. یا دادن اطلاعات محرمانه از طریق تلفن همه موارد نقض محرمانگی است.

یکپارچه بودن یعنی جلوگیری از تغییر داده‌ها به‌طور غیرمجاز و تشخیص تغییر در صورت دست‌کاری غیر مجاز اطلاعات. یکپارچگی وقتی نقض می‌شود که اطلاعات نه فقط در حین انتقال بلکه در حال استفاده یا ذخیره شدن و یا نابودشدن نیز به صورت غیرمجاز تغییر داده شود. سیستم‌های امنیت اطلاعات به‌طور معمول علاوه بر محرمانه بودن اطلاعات، یکپارچگی آن را نیز تضمین می‌کنند.

اطلاعات باید زمانی که موردنیاز توسط افراد مجاز هستند در دسترس باشند. این بدان معنی است که باید از درست کار کردن و جلوگیری از اختلال در سیستم‌های ذخیره و پردازش اطلاعات و کانال‌های ارتباطی مورد استفاده برای دسترسی به اطلاعات اطمینان حاصل کرد. سیستم‌های با دسترسی بالا در همه حال حتی به علت قطع برق، خرابی سخت‌افزار، و ارتقاء سیستم در دسترس باقی می‌ماند. یکی از راه‌های از دسترس خارج کردن اطلاعات و سیستم اطلاعاتی درخواست‌های زیاد از طریق خدمات از سیستم اطلاعاتی است که در این حالت چون سیستم توانایی و ظرفیت چنین حجم انبوه خدمات دهی را ندارد از سرویس دادن به‌طور کامل یا جزئی عاجز می‌ماند.

**2- مرور بر منابع**

قلمرو توصیف شده کتابخانه‎های دیجیتالی، برخلاف کتابخانه‎های سنتی، بسیار وسیع است. در کتابخانه‎های دیجیتالی، کاربر به مواد و منابع متنوعی دسترسی دارد و مجموعه‎ها و امکانات موجود، نسبت به کتابخانه‎های سنتی در معرض مخاطرات بیشتری قرار دارند. این کتابخانه‎ها نیازمند پیاده‎سازی برنامه‎های دقیقِ کنترل و سازوکارهای لازم برای نگهداری دارایی‌های اطلاعاتی خود در درازمدت هستند. کتابخانه دیجیتالی، نهادی اجتماعی و چیزی بیش از مجموعه‎ای از فناوری‌هاست و باید از سازوکارهای جدید برای نگهداری مواد استفاده کند (شارما؛ ویشواناتان، 1385). دسترسی غیرمجاز به اطلاعات و حمله به کتابخانه‎های دیجیتالی، اتفاق‌های محتملی هستند که به عنوان نمونه‎هایی از آنها می‎توان به دو رخنة امنیتی در دانشگاه ایندیانا در ایالات متحده آمریکا در تابستان 2002 و ماه می 2004 اشاره کرد که در هر دو مورد، زمان و تلاش زیادی برای بازگرداندن اطلاعات و ارتقای سیستم امنیتی جدید صرف شد (چنگ، 2005). یک مورد دیگر از این‎گونه حمله‎ها، در یک کتابخانه در دانشگاه نوتردام رخ داد و در طی آن، اطلاعات موجود در معرض خطرهای امنیتی قرار گرفت (فاکس، 2006). بی‎تردید، حفاظت بلند مدت دیجیتالی و ارتقای دسترس‎پذیری میراث مکتوب که هدف‌های اساسی کتابخانه‎های دیجیتالی است، بدون لحاظ کردن مسائل امنیتی امکان تحقق نخواهد یافت. تحقیق جهانی امنیت اطلاعات «ارنست و یانگ» در سال ۲۰۰۳ نشان می‎دهد ۹۰% سازمان‌ها معتقدند امنیت اطلاعات برای دستیابی آنها به هدف‌های کلی‎شان بسیار حائز اهمیت است (نقل در سادوسکای و دیگران، 1384 : 121). برخی از مهم‎ترین مسائل مربوط به امنیت در کتابخانه‎های دیجیتالی می‎تواند شامل امنیت سخت‌افزارها و دیتاسنترها، جایگاه فیزیکی دیتاسنترها و سرورها، امنیت تبادل اطلاعات، امنیت نرم‎افزارهای کاربردی مورد استفاده، امنیت نرم‎افزارهای ضد ویروس و فایروال، الگوی قوانین و مقررات حاکم بر سایت باشد. علاوه بر آن، دیجیتالی کردن آثار، خطر تجاوز به حقوق مؤلفان و پدیدآوران را نیز افزایش می‎دهد، زیرا یکی از مهم‎ترین ویژگی‌های محیط دیجیتالی، شکل‎پذیری و قابلیت تغییر شکل آثار به میزان بالاست. ناشران الکترونیک و کتابخانه‎های دیجیتالی به عنوان نگهبانان حقوق معنوی، نقش فراوانی در جلوگیری از اخلال حقوق مؤلفان دارند؛ زیرا پس از انتشار یک اثر به صورت آنلاین، امکان نسخه‎برداری الکترونیکی آن و دسترسی به حجم عظیمی از اطلاعات وجود دارد. بدیهی است، چنین سرقتی در محیط چاپی امکان‎پذیر نیست (زایلینسکی، 1377). جلوگیری از ورود‎های غیرمجاز، از آن جهت نیز اهمیت دارد که اشتراک پایگاه‎های اطلاعاتی دارای بار مالی است و مرکز اطلاع‎رسانی خود نیز اقدام به دریافت وجه در قبال اطلاعات ارائه شده به مراجعان می‎کند. علاوه بر آن، جلوگیری از آسیب‌های احتمالی از سوی هکرها و نفوذ گران به شبکه اینترنت نیز مسئله امنیت و حفاظت از منابع اطلاعاتی در کتابخانه‎های دیجیتالی را به عنوان یک امر حائز اهمیت مطرح می‎کند (علی پور حافظی؛ مطلبی، 1382).

نحوه استفاده و کنترل دستیابی به منابعی که به اشتراک گذاشته شده‎اند، از مهم‎ترین هدف‌های یک سیستم امنیتی در شبکه است. هر سازمان برای حفاظت از اطلاعات ارزشمند، باید به یک راهبرد خاص پایبند باشد و بر اساس آن سیستم امنیتی را پیاده‎سازی و اجرا نماید(برینی، 2001). با وجود اهمیت حفظ امنیت در محیط‌های اطلاع‎رسانی، این امر مهم در مقایسه با موضوع‌هایی مانند کمیت و کیفیت سایتها و پایگاه‎های اطلاعاتی تحت وب، کمتر مورد توجه پژوهشگران قرار گرفته است. از همین رو، این پژوهش، مسائل امنیتی در کتابخانه‎های دیجیتالی ایران را بر اساس کنترلهای امنیتی استاندارد ISO/IEC 27002 که از پراستفاده‌ترین استاندارد‎های امنیت اطلاعات است، مورد مطالعه قرار می‎دهد.

سردرگمی‌های زیادی در مورد عبارت کتابخانه دیجیتال وجود دارد که به اعتقاد کلولند Cleveland)، 1998) ناشی از سه عامل مهم است:

عامل اول اینکه در طول سال‌ها عبارات متنوعی برای بیان این مفهوم به کار برده شده (مانند کتابخانه الکترونیکی، کتابخانه مجازی، کتابخانه بدون دیوار ) و دقیقاً مشخص نبوده که معنای واقعی هر کدام از این مفاهیم چیست؟ به نظر می رسد عبارت «کتابخانه دیجیتالی» بیشتر از دیگر عبارات پذیرفته شده و اکنون در کنفرانسها، متون نوشتاری و بحث‌های اینترنتی تقریباً فقط از این عبارت استفاده می‌شود.

عامل دوم اینکه کتابخانه دیجیتالی مورد توجه حوزه‌های مختلف پژوهشی است و آنچه که «کتابخانه دیجیتالی» را از دیگر عبارات متفاوت می‌سازد، توصیف‌هایی است که پژوهشگران از آن ارائه داده‌اند.

عامل سوم اینکه منابع بسیاری در اینترنت وجود دارند که مردم آن را «کتابخانه دیجیتالی» می‌نامند. حال‌آنکه از دیدگاه کتابداران این منابع، کتابخانه دیجیتالی محسوب نمی‌شوند.

موضوع مورد توجه بسیاری دیگر از محققین بحث امنیت اطلاعات است. در ادامه توضیحات کاملی در این زمینه ارائه شده است.

سازمان‌ها اغلب در معرض انواع تهدید مانند دست‌کاری اطلاعات مرجع و یا سرقت اطلاعات حیاتی و سرمایه‎های اطلاعاتی قرار دارند. در چنین شرایطی، چنانچه عواملی که می‎توانند از مزایای سیستم‌ها به شمار بروند (مثل سرعت و قابلیت دسترسی بالا) تحت کنترل نباشند، ممکن است باعث بروز آسیب‎پذیری شده، سوءاستفاده افراد بد نیت از آنها به نفوذ و خرابکاری، کلاه‌برداری و یا اخاذی بینجامد. علاوه بر این، مشکلات طبیعی و خطاهای غیرعمدی که توسط کاربران رایانه‎ای رخ می‎دهد، در صورت نبود روش‌های صحیح برای حفاظت از اطلاعات، می‎تواند نتایج مخربی را به بار آورد. چنان که «کریدا و دیگران» (2005) تأکید می‎کنند، حفاظت سیستم‌های اطلاعاتی از حملات امنیتی یک چالش مستمر است که بسیاری از سازمان‌ها با آن مواجه‌اند.

با این اوصاف، تدوین و اجرای تدابیر امنیتی در قبال این تهدیدهای گسترده، ضرورتی اجتناب‌ناپذیر برای سازمان‌ها است. اتخاذ تدابیر مناسب می‎تواند احتمال وقوع مخاطرات را به حداقل برساند و یا در صورت وقوع آنها، میزان خسارت‌های وارده را در حد بسیار ناچیزی نگه دارد. این‎گونه تدابیر امنیتی، موجب افزایش قابلیت واکنش سریع و مؤثر می‎شود و به این ترتیب سازمان‌ها قادر خواهند بود برای ترمیم خسارت‌ها از فرایندهای از پیش تعیین شده استفاده کنند و بهره‎وری و ایمنی اطلاعات، افزایش یافته، کسب و کار به صورت مطمئن‎تری تداوم یابد (س‍ادوس‍ک‍ای‎ و دی‍گ‍ران، 1384: 9). امنیت اطلاعات عبارت است از حفاظت زیرساخت‌های فناوری اطلاعات و تضمین در دسترس بودن آن (ورمولن و سولمز، 2002؛ هونان، 2006). از همین‌رو، حیات کتابخانه‎های دیجیتالی، ارتباط نزدیکی با سیستم های امنیت اطلاعات دارد.

«چانگ و هو»(2006) به عوامل سازمانی مؤثر در پیاده‎سازی مدیریت امنیت اطلاعات پرداختند. این پژوهشگران ضمن تأکید بر نیاز سازمان‌ها به ساختارهای مدیریتی برای حفظ دارایی‌های اطلاعاتی، این‎گونه ساختارهای امنیتی را سلاحی مؤثر برای بقا در عرصة رقابت عنوان می‎کنند. بر‎اساس یافته‎های پژوهش، توانایی مدیران فناوری اطلاعات و نبود اطمینان محیطی، تأثیر مثبتی بر روی سازمان‌ها در پیاده‎سازی مدیریت امنیت اطلاعات و استاندارد BS7799 داشته است. همچنین، یافته‎ها نشان داد عوامل سازمانی شامل اندازه سازمان و نوع صنعت، به نحو قابل‎توجهی کاربرد مدیریت امنیت اطلاعات را تحت تأثیر قرار می‎دهد. «کوزما» (2010) به آسیب‎پذیری امنیت در کتابخانه‎های دیجیتالی اروپا پرداخت و با استفاده از یک نرم‎افزار آزمایش خطر‎پذیری وب سایت، مسائل امنیتی 80 کتابخانه دیجیتالی اروپایی را بررسی نمود. نتایج نشان داد اکثر کتابخانه‎های دیجیتالی نقص امنیتی جدی در برنامه‎های کاربردی تحت وب خود دارند. اکثر کتابخانه‎های اروپای غربی، مشکلات امنیتی بحرانی (25 %) و یا در سطح متوسط (40 %) داشتند که منجر به تجارت ناامن آنلاین شده بود. همچنین، یافته‎ها حاکی از این بود که با وجود قوانین مربوط به حفاظت اطلاعات، کتابداران اقدام‌های لازم برای ایمن‎سازی سیستمهای اطلاعاتی آنلاین را اجرا نمی‎کنند.

**تحقیقات صورت گرفته در ایران**

با توجه به تحقیقات صورت گرفته در این زمینه می‌توان گفت که کتابخانه دیجیتال به مفهوم واقعی خود در ایران وجود ندارد. آنچه که در ایران تحت عنوان کتابخانه دیجیتال مطرح و ایجاد گردیده است سیستم‌های مکانیزه کتابخانه است که اطلاعات مربوط به کتب مختلف را همراه با سرویس‌های موجود در یک کتابخانه از قبیل جستجو، امانت دهی، ثبت نام،رزرو کتاب و ... در اختیار کاربر قرار می‌دهد. مانند سیستم مکانیزه کتابخانه‌ی دانشگاه‌های مختلف که خدماتی از قبیل دستیابی به اطلاعات کتاب شناختی،جستجوی کتاب و...را در اختیار کاربران قرار می‌دهند.

زنده دل و همکاران مدلی برای رتبه‎بندی سازمان‌ها بر مبنای اندازه‎گیری و شناسایی میزان بلوغ امنیت اطلاعات در آنها ارائه نمودند. بدین منظور، پس از تعیین شاخص‌های امنیت اطلاعات در قالب دو دسته کلیِ فنی و مدیریتی و با توجه به معیارهای سه‌گانه «امنیت»، «ایمنی» و «پایداری»، نظرهای خبرگان فناوری اطلاعات بخش‌های انفورماتیک در سه سازمان مطالعه شد. با توجه به یافته‎ها، ازنظر بلوغ امنیت، بانک پاسارگاد رتبه اول، دانشگاه تهران رتبه دوم و بانک تجارت رتبه سوم را به دست آوردند.

**3- روش کار**

پژوهش حاضر با هدف شناخت وضعیت امنیت اطلاعات در کتابخانه‌های دیجیتالی و ابعاد حقوقی آن صورت گرفته است. روش پژوهش، پیمایشی تحلیلی و جامعه پژوهش، کتابخانه‎های دیجیتالی ایران است. در پژوهش حاضر، منظور از کتابخانه‎های دیجیتالی ایران، کتابخانه‎هایی هستند که بر اساس خط‎مشی خاص و با بهره‎گیری از کارکنان متخصص، منابع اطلاعاتی دیجیتال را گردآوری و یا تولید کرده، به شکل دیجیتالی ذخیره، سازمان‌دهی و از طریق ارائه خدمات به کاربران خود اشاعه می‎دهند. این کتابخانه‎ها شامل کتابخانه‎هایی هستند که از نرم‎افزارهای کتابخانه‎های دیجیتالی مانند نوسا، پارس آذرخش، پروان پژوه، پاپیروس، پیام مشرق، وستا و ارم استفاده می‎کنند. همچنین، کتابخانه دیجیتالی مانند نورلایب، تبیان، دید که دارای نرم‎افزارهای خود ساخته بودند، جزء جامعه آماری پژوهش هستند.

روش نمونه گیری برای انجام این پژوهش، نظرسنجی بوده است. همچنین ابزار گردآوری داده‌ها، پرسشنامه ای است که بر مبنای استاندارد ISO/IEC 27002 تهیه شده و با 11 شاخص و 79 زیر شاخص امنیت اطلاعات را مورد بررسی قرار می‌دهد. 58 کتابخانه دیجیتالی فعال در ایران جامعه پژوهش را تشکیل می‌دهند که از آن تعداد 45 کتابخانه به پرسش‌نامه‌ها پاسخ دادند.

سوالات تحقیق از این قبیل بودند:

1. وضعیت امنیت اطلاعات در کتابخانه‎های دیجیتالی ایران چگونه است؟
2. آسیب‌پذیرترین نقاط امنیتی در کتابخانه‎های دیجیتالی ایران بر اساس شاخص‌های مورد مطالعه کدم‌اند؟
3. رتبه‌بندی کتابخانه‎های دیجیتالی ایران بر حسب امنیت اطلاعات چگونه است؟

همچنین دو فرضیه زیر در این پژوهش اتخاذ شده اند:

* بین میانگین شاخص‌های امنیت اطلاعات کتابخانه‎های دیجیتالی تفاوت معناداری وجود دارد.
* بین کتابخانه‎های دیجیتالی دانشگاهی و غیردانشگاهی برحسب امنیت اطلاعات تفاوت معناداری وجود دارد.

**4- نتایج و بحث**

امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری از جمله این مؤلفه‌ها بوده که نمی‌توان آن را مختص یک فرد یا سازمان در نظر گرفت. پرداختن به مقوله امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری در هر کشور، مستلزم توجه تمامی کاربران صرف‌نظر از موقعیت شغلی و سنی به جایگاه امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری بوده و می بایست به این مقوله در سطح کلان و از بعد منافع ملی نگاه کرد. وجود ضعف امنیتی در شبکه‌های کامپیوتری و اطلاعاتی، عدم آموزش و توجیه صحیح تمامی کاربران صرف‌نظر از مسئولیت شغلی آنان نسبت به جایگاه و اهمیت امنیت اطلاعات، عدم وجود دستورالعمل‌های لازم برای پیشگیری از نقایص امنیتی، عدم وجود سیاست‌های مشخص و مدون به منظور برخورد مناسب و به‌موقع با اشکالات امنیتی، مسائلی را به دنبال خواهد داشت که ضرر آن متوجه تمامی کاربران کامپیوتر در یک کشور شده و عملا زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می‌دهد.

یافته‎ها در مورد سیستم عامل مورد استفاده در سرور اصلی سایت کتابخانه‎های دیجیتالی ایران نشان داد بیشترین تعداد (4/84%) کتابخانه‎ها از ویندوز و کمترین تعداد (6/15%) از لینوکس استفاده می‎کنند. در بررسی نوع سرور نیز مشخص شد سرور به صورت اختصاصی با 8/97 % بیشترین فراوانی و سرور به صورت اجاره‎ای با 2/2% کمترین فراوانی را دارد. همچنین، تمام سرورهای کتابخانه‎های دیجیتالی با درصد فراوانی 100 در داخل ایران مستقر بوده، 39 کتابخانه دیجیتالی با درصد فراوانی 7/86 دارای آی‎پی اختصاصی هستند. برای کسب اطلاعات زمینه‎ای در مورد کتابخانه‎های دیجیتالی ایران، نرم‎افزارهای مورد استفاده در این کتابخانه‎ها نیز مورد پرسش قرار گرفت که یافته‎های مربوط، در جدول 1 نشان داده شده است. توزیع فراوانی نیز در جدول 1 نشان داده شده است.

جدول1- نتایج حاصل از نرم افزارهای مورد استفاده

|  |  |  |
| --- | --- | --- |
| **نرم افزار** | **فراوانی** | **درصد فراوانی** |
| پیام مشرق | 14 | 1/31 |
| پارس آذرخش | 14 | 1/31 |
| نوسا | 5 | 1/11 |
| پروان پژوه | 4 | 9/8 |
| خودساخته | 4 | 9/8 |
| پاپیروس | 2 | 4/4 |
| ارم | 1 | 2/2 |
| وستا | 1 | 2/2 |
| کل | 45 | 100 |

برای بررسی سوال اول تحقیق «وضعیت امنیت اطلاعات در کتابخانه‎های دیجیتالی ایران چگونه است؟» باید به جدول 2 توجه شود. در این جدول شاخص‌های میانگین و انحراف معیار امنیت اطلاعات در کتابخانه‎های دیجیتالی نشان داده شده است. میانگین امنیت اطلاعات کل کتابخانه‎های دیجیتالی 79/0 است که در سطح قوی ارزیابی می‎شود.

جدول 2. شاخص‌های میانگین و انحراف معیار امنیت اطلاعات در کتابخانه‎های دیجیتالی ایران

|  |  |  |  |
| --- | --- | --- | --- |
| **شاخص آماری****متغییر** | **میانگین** | **انحراف معیار** | **تعداد** |
| امنیت اطلاعات | 79/0 | 165/0 | 45 |

برای بررسی سوال دوم تحقیق «آسیب‎پذیرترین نقاط امنیتی در کتابخانه‎های دیجیتالی ایران بر اساس شاخص‎های مورد مطالعه کدم‌اند؟» باید به جدول 3 توجه شود. در جدول3 مشاهده می‎شود که شاخص‌های «خط‎مشی امنیت» با میانگین63/0 و «امنیت منابع انسانی» با میانگین 63/0 پایین‎ترین میانگین را دارند و آسیب‎پذیرترین نقاط امنیتی کتابخانه‎های دیجیتالی ایران هستند.

جدول3. میانگین و انحراف معیار شاخص‌های امنیت اطلاعات کل کتابخانه‎های دیجیتالی ایران

|  |  |  |
| --- | --- | --- |
| **شاخص ها** | **میانگین** | **انحراف معیار** |
| امنیت فیزیکی و محیطی | 87/0 | 21/0 |
| مدیریت تداوم و کار | 84/0 | 30/0 |
| مدیریت دارایی ها | 83/0 | 24/0 |
| مدیریت ارتباطات و عملیات | 82/0 | 20/0 |
| کنترل دسترسی | 79/0 | 18/0 |
| تهیه، توسعه و نگهداری سیستم های اطلاعاتی | 78/0 | 23/0 |
| انطباق | 78/0 | 25/0 |
| سازماندهی امنیت اطلاعات | 71/0 | 27/0 |
| مدیریت حوادث اطلاعات | 70/0 | 27/0 |
| خط مشی امنیت | 63/0 | 42/0 |
| امنیت منابع انسانی | 63/0 | 30/0 |

برای بررسی سوال شوم تحقیق « رتبه‎بندی کتابخانه‎های دیجیتالی ایران بر حسب امنیت اطلاعات چگونه است؟» باید به جدول 4 توجه شود. چنان‎که در جدول 4 مشاهده می‎شود، کتابخانه‎های دیجیتال مؤسسه نشر امام خمینی، پژوهشگاه نیرو، فرهنگستان هنر، کتابخانه دیجیتال علوم‎انسانی شهرداری تهران، کتابخانه دیجیتال شرکت برق منطقه‎ای خراسان، کتابخانه دیجیتال دانشگاه تبریز با میانگین 1 بالاترین میانگین را داشته، در سطح قوی قرار ارزیابی می‎شوند. کتابخانه دیجیتال دانشکده کارآفرینی تهران با میانگین 37/. دارای پایین‎ترین میانگین است و در سطح متوسط ارزیابی می‎شود.

جدول4. شاخص‌های میانگین و انحراف معیار امنیت اطلاعات کتابخانه‎های دیجیتالی ایران به ترتیب نزولی

| **کتابخانه دیجیتال** | **میانگین** | **انحراف معیار** |
| --- | --- | --- |
| کتابخانه دیجیتال مؤسسه نشر امام خمینی(ره) | 1 | 0 |
| کتابخانه دیجیتال پژوهشگاه نیرو | 1 | 0 |
| کتابخانه دیجیتال فرهنگستان هنر | 1 | 0 |
| کتابخانه دیجیتال علوم انسانی شهرداری تهران | 1 | 0 |
| کتابخانه دیجیتال شرکت برق منطقه‎ای خراسان | 1 | 0 |
| کتابخانه دیجیتال دانشگاه تبریز | 1 | 0 |
| کتابخانه دیجیتال مجلس | 99/0 | 11/0 |
| کتابخانه دیجیتال علوم پزشکی و خدمات بهداشتی درمانی شهید بهشتی | 99/0 | 13/0 |
| کتابخانه دیجیتال شرکت ملی مناطق نفت‌خیز جنوب | 99/0 | 11/0 |
| کتابخانه دیجیتال دانشگاه علوم پزشکی گیلان | 97/0 | 22/0 |
| کتابخانه دیجیتال شهرک علمی و تحقیقاتی اصفهان | 96/0 | 27/0 |
| کتابخانه دیجیتال  مرکز مخابرات ایران | 91/0 | 30/0 |
| کتابخانه دیجیتال مرکز اطلاعات و مدارک علمی ایران (ایران داک) | 90/0 | 26/0 |
| کتابخانه دیجیتال مرکزی تبریز | 90/0 | 38/0 |
| کتابخانه دیجیتال شهرداری تهران (کتابخانه مرکزی شهرداری تهران) | 89/0 | 35/0 |
| کتابخانه دیجیتال دانشگاه امیر‎کبیر | 86/0 | 37/0 |
| کتابخانه دیجیتال دانشگاه علوم پزشکی زنجان | 85/0 | 36/0 |
| کتابخانه دیجیتال دانشگاه علوم پزشکی شهید صدوقی یزد | 84/. | 43/0 |
| کتابخانه دیجیتال دانشگاه علوم پزشکی تهران | 83/0 | 38/0 |
| کتابخانه دیجیتال شرکت ملی صنایع پتروشیمی تهران | 82/0 | 42/0 |
| کتابخانه دیجیتال پژوهشکده تحقیقات فضایی | 82/0 | 38/0 |
| کتابخانه دیجیتال دانشگاه صنعتی اصفهان | 81/0 | 40/0 |
| کتابخانه دیجیتال ارم | 80/. | 40/0 |
| کتابخانه دیجیتال کتابخانه ملی ایران | 80/0 | 43/0 |
| کتابخانه دیجیتال دانشگاه علوم پزشکی بیرجند | 79/0 | 42/0 |
| کتابخانه دیجیتال دانشگاه علوم پزشکی شیراز | 78/0 | 44/0 |
| کتابخانه دیجیتال دانشگاه علوم پزشکی و خدمات درمانی ایلام | 77/0 | 42/0 |
| کتابخانه دیجیتال دانشگاه آزاد اسلامی واحد نجف‎آباد | 77/0 | 45/0 |
| کتابخانه دیجیتال دانشگاه یزد | 76/0 | 46/0 |
| کتابخانه دیجیتال دانشگاه صنعتی شریف | 75/0 | 46/0 |
| کتابخانه دیجیتال دانشگاه شیراز | 74/0 | 39/0 |
| کتابخانه دیجیتال آستان قدس احمدی و محمدی (شاه چراغ) | 74/0 | 45/0 |
| کتابخانه دیجیتال تبیان | 74/0 | 47/0 |
| کتابخانه دیجیتال شهرداری اصفهان | 71/0 | 48/0 |
| کتابخانه دیجیتال نور | 67/0 | 50/0 |
| کتابخانه دیجیتال معاونت توسعه و فناوری اطلاعات و تجارت الکترونیکی وزارت بازرگانی | 65/0 | 48/0 |
| کتابخانه دیجیتال مدیریت بحران شهرداری تهران | 64/0 | 49/0 |
| کتابخانه دیجیتال دانشگاه ولی‎عصر رفسنجان | 62/0 | 49/0 |
| کتابخانه دیجیتال دانشگاه ارومیه | 60/0 | 50/0 |
| کتابخانه دیجیتال سازمان بورس و  اوراق بهادار تهران | 60/0 | 49/0 |
| کتابخانه دیجیتال سازمان فرهنگی هنری شهری تهران(کتابخانه عمومی تهران) | 59/0 | 50/0 |
| کتابخانه دیجیتال پردیس علوم دانشگاه تهران | 55/0 | 50/0 |
| کتابخانه دیجیتال موسسه تحقیقات و نشر معارف اهل‎البیت | 49/0 | 50/0 |
| کتابخانه دیجیتال دانشگاه صنعتی جندی شاپور | 41/0 | 50/0 |
| کتابخانه دیجیتال دانشکده کارآفرینی تهران | 37/0 | 49/0 |

جدول 5 نشان می‎دهد بیشترین درصد (55/75 %) کتابخانه‎های دیجیتالی از نظر امنیت اطلاعات در سطح قوی قرار دارند. سطح امنیت در 46/24 % کتابخانه‎ها متوسط است.

جدول5. توزیع فراوانی سطوح امنیت اطلاعات در کتابخانه‎های دیجیتالی ایران

|  |  |  |
| --- | --- | --- |
| **کتابخانه‎های دیجیتال** | **فراوانی** | **درصد فراوانی** |
| سطح قوی | 34 | 55/75 |
| سطح متوسط | 11 | 46/24 |
| سطح ضعیف | 0 | 0 |
| جمع | 45 | 100 |

جدول6. نتایج آزمون آنالیز واریانس برای مقایسه میانگین‌های شاخص‌های امنیت اطلاعات کتابخانه‎های دیجیتالی

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **شاخص ها** | **تعداد** | **میانگین** | **انحراف معیار** | **مقدار آماری f** | **درجه آزادی** | **P-value** | **نتیجه آزمون** |
| خط مشی امنیت | 43 | 63/0 | 42/0 |  |  |  |  |
| سازماندهی اطلاعات | 44 | 71/0 | 27/0 |  |  |  |  |
| مدیریت دارایی ها | 43 | 83/0 | 24/0 |  |  |  |  |
| امنیت منابع انسانی | 45 | 63/0 | 30/0 | 95/3 | 10 | 00/0 | اختلاف معنادار |
| امنیت فیزیکی و محیطی | 45 | 87/0 | 21/0 |  |  |  |  |
| مدیریت ارتباطات و عملیات | 45 | 82/0 | 20/0 |  |  |  |  |
| کنترل دسترسی | 45 | 79/0 | 18/0 |  |  |  |  |

چنان‎که در جدول 6 مشاهده می‎شود، مقدار سطح معناداری برابر صفر است و با توجه به اینکه این مقدار کمتر از 05/0 است، فرضیه اول پژوهش تأیید می‎شود و تفاوت میانگین در بین شاخص‌های مختلف معنادار است. نتایج آزمون تعقیبی توکی نشان داد میانگین شاخص امنیت فیزیکی و محیطی به نحو معناداری بیش از سایر شاخص‌هاست و کتابخانه‎ها در این شاخص به نحو معناداری قوی‎تر هستند. همچنین، آزمون توکی حاکی از این بود که میانگین شاخص امنیت منابع انسانی به نحو معناداری کمتر از سایر شاخص‌ها است.

فرضیه دوم: بین کتابخانه‎های دیجیتالی دانشگاهی و غیردانشگاهی برحسب امنیت اطلاعات تفاوت معناداری وجود دارد.

برای آزمون فرضیه دوم، از آزمونt برای دو نمونه مستقل در سطح اطمینان 95 % استفاده شد. نتایج در جدول 7 نشان داده شده است.

جدول7. نتایج آزمونt برای مقایسه امنیت اطلاعات کتابخانه‎های دیجیتالی دانشگاهی و غیردانشگاهی ایران

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **متغییر** | **تعداد** | **میانگین** | **انحراف معیار** | **آماره t** | **درجه آزادی** | **سطح معناداری** |
| کتابخانه های دیجیتالی دانشگاهی | 20 | 75/0 | 17/0 |  |  |  |
| کتابخانه های دیجیتالی غیر دانشگاهی | 25 | 82/0 | 15/0 | 46/1- | 43 | 15/0 |

چنان‎که در جدول 7 مشاهده می‎شود، با توجه به سطح معناداری که برابر 0.15 شده و بیشتر از 0.5 هست، فرض صفر آزمون پذیرفته می‎شود. به این ترتیب، وجود تفاوت معنادار بین دو گروه تأیید نمی‎شود و در نتیجه فرضیه دوم پژوهش رد می‎شود.

**5- نتیجه گیری**

یافته‎های پژوهش مبنی بر وضعیت امنیت اطلاعات در کتابخانه‎های دیجیتالی ایران، نشان داد میانگین امنیت کل کتابخانه‎های دیجیتالی 79/0 است. با توجه به میانگین یادشده، امنیت اطلاعات در کتابخانه‎های دیجیتالی ایران در سطح قوی ارزیابی می‎شود. سایر یافته‎ها حاکی از این بود که آسیب‎پذیرترین نقاط امنیتی در کتابخانه‎های دیجیتالی ایران بر اساس شاخص‌های مورد مطالعه، شاخص «خط‎مشی امنیت» با میانگین 63/0 است. وجود خط‎مشی امنیت از مهم‎ترین شاخص‌های تعیین کننده برنامه‎های سازمان برای حفظ امنیت منابع دیجیتالی است. «خط مشی امنیت گام‌های لازم برای حفاظت سرمایه‎ها را تعریف می‎کند. نخست، مشخص می‎کند از چه چیزی حفاظت می‎شود و چرا. دوم، مسئولیت مربوط به تأمین این حفاظت را مشخص می‎کند. سوم، زمینه‎ای برای تفسیر و حل مشکلات آتی ارائه می‎دهد» (سادوسکای و دیگران، 1384: 150). با توجه به اهمیت تدوین خط‎مشی امنیتی در کتابخانه‎های دیجیتالی، یافته‎های پژوهش حاضر توجه مسئولان را به این شکاف امنیتی در کتابخانه‎های دیجیتالی ایران جلب می‎کند. دومین شاخصی که بر اساس یافته‎ها، کمترین میانگین را در کتابخانه‎های دیجیتالی ایران دارد، «امنیت منابع انسانی» با میانگین 63/0 است که پس از شاخص خط‎مشی، آسیب‎پذیرترین نقاط امنیتی کتابخانه‎های دیجیتالی ایران است. یافته‎های این پژوهش با نتایج پژوهش «آرام» (1388)، «محمود‎زاده و راد رجبی» (1384) مبنی بر تعیین عوامل تأثیرگذار بر امنیت اطلاعات همخوانی دارد. در آن پژوهش‌ها نیز، امنیت نیروی انسانی بالاترین تهدید برای امنیت اطلاعات سیستمهای رایانه‎ای بود. امنیت منابع انسانی، شامل تمامی موارد مربوط به کارکنان است. برخی مطالعات نشان داده است بیش از 80% جرایم سنگین رایانه‎ای را افرادی مرتکب می‎شوند که یا از دسترسی قانونی به داده‎ها برخوردارند و یا در گذشته نزدیک از آن برخوردار بوده‎اند. از همین رو، بخش مهمی از یک طرح امنیتی خوب مربوط به اداره کارکنان با دسترسی‌های طبقه‎بندی شده است (سادوسکای و دیگران، 1384: 159). با توجه به ضعف امنیتی کتابخانه‎های دیجیتالی ایران در رابطه با امنیت نیروی انسانی، لازم است رده‎های مدیریتی کتابخانه‎های دیجیتالی تمهیدات لازم را برای تأمین امنیت اطلاعات از این جنبه اتخاذ نمایند. رتبه‎بندی کتابخانه‎های دیجیتالی ایران به لحاظ امنیت اطلاعات، نشان داد کتابخانه‎های دیجیتالی مؤسسه نشر امام خمینی(ره)، پژوهشگاه نیرو، فرهنگستان هنر، کتابخانه دیجیتال علوم‎انسانی شهرداری تهران، کتابخانه دیجیتال شرکت برق منطقه‎ای خراسان، کتابخانه دیجیتال دانشگاه تبریز با میانگین 1 از حداکثر میانگین لازم برخوردار بوده، در سطح قوی قرار دارند. کتابخانه دیجیتال دانشکده کارآفرینی تهران با میانگین 37/0 پایین‎ترین میانگین را دارد و در سطح متوسط ارزیابی می‎شود. براساس یافته‎های پژوهش، بیشترین درصد کتابخانه‎های دیجیتالی (55/75 %) در سطح قوی قرار دارند و کتابخانه‎های دیجیتالی در سطح متوسط، 46/24% را تشکیل می‎دهند. با در نظر گرفتن این یافته‎ها و همچنین نتایج پژوهش «کوزما» (2010) مبنی بر نقص‌های امنیتی کتابخانه‎های دیجیتالی اروپا، مشاهده می‎شود که کتابخانه‎های دیجیتالی ایران ازنظر امنیت اطلاعات در مقایسه با کتابخانه‎های دیجیتالی اروپا وضعیت مناسب‌تری دارند. چنان‎که پیشتر اشاره شد، پژوهش «کوزما» (2010) نشان داد در 25 % کتابخانه‎های دیجیتالی اروپا، مشکلات امنیتی در سطح بحرانی و در 40 % کتابخانه در سطح متوسط بوده است. بر اساس سایر یافته‎های پژوهش، مشخص شد تفاوت معناداری بین میانگین شاخص‌های امنیت اطلاعات کتابخانه‎های دیجیتالی وجود دارد و با توجه به نتایج آزمون تعقیبی توکی، میانگین شاخص «امنیت فیزیکی و محیطی» به نحو معناداری بیشتر از سایر شاخص‌هاست و کتابخانه‎ها در این شاخص به نحو معناداری قوی‎تر و در شاخص «امنیت منابع انسانی» به نحو معناداری ضعیف‎تر هستند. همچنین، نتایج آزمون t نشان داد تفاوت معناداری بین کتابخانه‎های دیجیتالی دانشگاهی و غیردانشگاهی به لحاظ امنیت اطلاعات وجود ندارد. به نظر می‎رسد سطح دانش در خصوص امنیت اطلاعات محیط دیجیتالی در فضاهای دانشگاهی و غیر دانشگاهی دارای پراکندگی یکسانی است.

**پیشنهادهای پژوهش**

با توجه به نتایج به‌دست‌آمده از پژوهش، پیشنهادهایی برای رفع نقایص امنیتی کتابخانه‎های دیجیتالی ایران ارائه می‎شود. یافته‎های پژوهش نشان داد آسیب‎پذیرترین نقاط امنیتی کتابخانه‎های دیجیتالی «خط‎مشی امنیت» و «امنیت نیروی انسانی» است. با توجه به این یافته‎ها پیشنهاد می‎شود:

1- کتابخانه‎های دیجیتالی سند خط‎مشی امنیت اطلاعات را با ذکر هدف‌های بلند مدت، کوتاه مدت و مسئولیت‌های هر یک از واحدها و به طور خاص مشاغل مختلف برای رسیدن به هدف‌ها را ابلاغ نموده، با برگزاری جلسات پرسش و پاسخ، کارکنان را نسبت به وظایف خود در قبال اجرای سند خط‎مشی آگاه کنند. از موارد دیگر این که باید بازنگری در شرح وظایف مشاغل بخصوص در زمینه مسئولیت‌های امنیتی، صورت گیرد.

2- منابع انسانی از مهم‎ترین عوامل تأثیرگذار بر امنیت کتابخانه‎های دیجیتالی است، زیرا نیروی انسانی مهم‎ترین نقش را در نحوه استفاده از فناوری ایفا می‎کند. همچنین، خطاهای انسانی از مهم‎ترین عوامل در کاهش امنیت اطلاعات هستند. بدیهی است، دقت در این امر، موجب جلوگیری از بروز مشکلات جبران ناپذیر بسیار زیادی خواهد شد. با توجه به این امر، موارد زیر باید رعایت شود.

3- نقش‌ها و مسئولیت‌های امنیتی کارکنان، پیمانکاران و کاربران ثالث بر اساس خط‎مشی امنیت اطلاعات سازمان تعریف و مستندسازی شود.

4- اقدام‌های نظارتی در خصوص تأیید پیشینه تمامی نامزدهای استخدامی، پیمانکاران و کاربران ثالث باید بر اساس قوانین، مقررات و معیارهای اخلاقی مربوط و متناسب با الزام‌های تجاری، طبقه‎بندی اطلاعاتی که قرار است در دسترس قرار گیرند و ریسک‌های شناخته‌شده، انجام شود.

5- کارکنان، پیمانکاران و کاربران ثالث ملزم شوند پیمان حفظ اسرار یا عدم افشای آن را به عنوان بخشی از تعهدات، شرایط و ضوابط قرارداد استخدامی قبول و امضا نمایند.

6- مسئولیت‌های کارکنان، پیمانکاران و کاربران ثالث و سازمان در قبال امنیت اطلاعات باید به نحو روشن و دقیق در قرارداد استخدامی تصریح گردد.

7- مدیریت ملزم شود تا از کارکنان، پیمانکاران و کاربران ثالث بخواهد امنیت را بر اساس خط‎مشی‎های تعیین شده و رویه‌های سازمان به مورد اجرا بگذارد.

8- تمامی کارکنان سازمان و بر حسب مورد پیمانکاران و کاربران ثالث ملزم شوند تا دوره‎های آموزشی و آگاه‎سازی در خصوص خط‌مشی‌ها و رویه‌های سازمان را در زمینه امنیت اطلاعات بر حسب نوع شغل خود طی کنند.

9- در مورد آن دسته از کارکنانی که مرتکب نقض امنیت می‎شوند، وجود یک فرایند تنبیهی رسمی الزامی باشد. 10- مسئولیت‌ها در قبال فسخ استخدام یا تغییر آن باید به صراحت تعیین و واگذار گردد.

11- تمامی کارکنان، پیمانکاران و اشخاص ثالث ملزم باشند به محض فسخ استخدام، قرارداد یا موافقت‎نامه خود، نسبت به عودت دارایی‌های سازمان که در اختیارشان قرار داشته است، اقدام نمایند.

12- حق دسترسی تمامی کارکنان، پیمانکاران و کاربران ثالث به اطلاعات و مراکز پردازش اطلاعات باید به محض فسخ استخدام، قرارداد یا موافقت‎نامه حذف شده و یا به محض هر‎گونه تغییر، مورد تعدیل قرار گیرد.

پیشنهاد می‎شود مدیران کتابخانه‎های دیجیتالی ایران قبل از هر‎گونه اقدامی، برای توسعه منابع کتابخانه‎های خود برای حصول اطمینان بیشتر از امنیت نرم‎افزارها و سخت‎افزارهای مورد استفاده، با استفاده از فن‌های پدافند غیرعامل و با مشارکت تیم‌های امنیتی نسبت به طراحی حملات هکری اقدام نموده و با شناسایی حفره‎های امنیتی، تلاش کنند تا آنها را ترمیم نمایند.

**6- منابع**

1- ISO/IEC 27002:2005, Information technology, Security techniques, Code of practice for information security management.

2- Karyda, M., Kiountouzis, E. & Kokolakis, S. (2005). Information systems security policies: a contextual perspective, Computers & Security, 24(3), 246-260.

3- Kuzma, Joanne (2010) "European digital libraries: web security vulnerabilities", Library Hi Tech, Vol. 28 Iss: 3, pp.402 – 413.

4- زنده دل نوبری، بابک(1389). ارائه مدلی جهت رتبه‎بندی سازمان‎ها بر مبنای اندازه‎گیری و شناسایی میزان بلوغ امنیت اطلاعات در آنها. پایان‎نامه کارشناسی ارشد دانشگاه آزاد اسلامی واحد علوم تحقیقات.

5- علی پور حافظی، مهدی و داریوش مطلبی (1382). مجموعه مقالات همایش‎های انجمن کتابداری و اطلاع‎رسانی ایران. ج2.کتابخانه‎های دیجیتالی: مفاهیم و جنبه‎های فنی-اجرایی. تهران: انجمن کتابداری و اطلاع‎رسانی ایران، سازمان اسناد و کتابخانه ملی جمهوری اسلامی ایران.