امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران

دکتر نجلا حریری[1]
زهرا نظری[2]

چکیده

پژوهش حاضر با هدف شناخت وضعیت امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران انجام شده است. روش پژوهش پیمایشی تحلیلی و ابزار گردآوری داده‌ها، پرسشنامه‌ای است که بر مبنای استاندارد ISO/IEC 27002 تهیه شده و با یازده شاخص و ۷۹ زیرشاخص، امنیت اطلاعات را مورد سنجش قرار می‌دهد. شاخصهای ارزیابی شامل خط‌مشی امنیت، سازماندهی امنیت اطلاعات، مدیریت دارایی‌ها، امنیت منابع انسانی، امنیت فیزیکی و محیطی، مدیریت ارتباطات و عملیات، کنترل دسترسی، تهیه، توسعه و نگهداری سیستم‌های اطلاعاتی، مدیریت حوادث، امنیت اطلاعات، مدیریت تداوم کسب و کار، و انطباق است. ۵۸ کتابخانه دیجیتالی فعال ایران جامعه پژوهش را تشکیل می‌دهند که از آن تعداد ۴۵ کتابخانه به پرسشنامه‌ها پاسخ داده‌اند.

بر اساس یافته‌ها، میانگین امنیت اطلاعات کتابخانه‌های دیجیتالی ایران ۰/۷۹ (از میانگین کل ۱) است و کتابخانه ها از لحاظ امنیت اطلاعات در سطح قوی قرار دارند. آسیب پذیرترین نقاط امنیتی، «خط‌مشی امنیت» و «امنیت نیروی انسانی»، هر دو با میانگین ۰/۶۳ است. کتابخانه‌های دیجیتال 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 ۱، بالاترین میانگین امنیت اطلاعات را دارند. در مجموع ۷۵/۵۵ ٪

---

۱. دانشیار گروه کتابداری و اطلاع‌رسانی، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات تهران . nadjlahariri@hotmail.com

۲. کارشناس ارشد کتابداری و اطلاع‌رسانی دانشگاه آزاد اسلامی، واحد علوم و تحقیقات تهران . Zhr_nazari@yahoo.com

کتابخانه‌های دیجیتالی ایران از لحاظ امنیت اطلاعات در سطح قوی و ۲۴/۴۶ ٪ در سطح متوسط هستند. شاخصهای امنیت اطلاعات از نظر رعایت در کتابخانه‌های دیجیتالی دارای تفاوت معناداری است، اما تفاوت معناداری بین کتابخانه‌های دیجیتالی دانشگاهی و غیردانشگاهی از نظر امنیت اطلاعات وجود ندارد.

کلیدواژه‌ها: استاندارد ISO/IEC 27002، امنیت اطلاعات، حفاظت داده‌ها، کتابخانه‌های دیجیتالی ایران

مقدمه و بیان مسئله

مزایای ذخیره‌سازی اطلاعات به صورت الکترونیکی، کاربرد وسیع رایانه‌ها در فعالیتهای حرفه‌ای گوناگون را ناگزیر ساخته و استفاده از شبکه‌های رایانه‌ای و بویژه اینترنت، تغییرات اساسی در روند ارائه خدمات به وجود آورده است. این امکانات سبب شده حجم بسیار زیادی از اطلاعات تنها به اندازهٔ یک سرانگشت با کاربران فاصله داشته باشد. ناگفته پیداست، در این محیط پیچیده با این ارتباطات وسیع، مخاطرات گسترده‌ای سیستمهای رایانه‌ای، سامانه‌های اطلاعاتی و فعالیتها و زیرساختهای حیاتی وابسته به آنها را تهدید می‌کند (سادوسکای و دیگران،۱۳۸۴: ۹).

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، سوء استفادهٔ 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، درصورت نبود روشهای صحیح برای حفاظت از اطلاعات، می‌تواند نتایج مخربی را به بار آورد. چنان که «کریدا[1] و دیگران» (۲۰۰۵) تأکید می‌کنند، حفاظت سیستمهای اطلاعاتی از حملات امنیتی یک چالش

1. Karyda.

مستمر است که بسیاری از سازمانها با آن مواجهند.

با این اوصاف، تدوین و اجرای تدابیر امنیتی در قبال این تهدیدهای گسترده، ضرورتی اجتناب ناپذیر برای سازمانهاست. 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، ۱۳۸۴: ۹). امنیت اطلاعات عبارت است از حفاظت زیرساختهای فناوری اطلاعات و تضمین در دسترس بودن آن (ورمولن و سولمز[1]، ۲۰۰۲؛ هونان[2]، ۲۰۰۶). از همین‌رو، حیات کتابخانه‌های دیجیتالی، ارتباط نزدیکی با سیستمهای امنیت اطلاعات دارد.

قلمروِ توصیف شدهٔ 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 دراز مدت هستند. کتابخانهٔ دیجیتالی، نهادی اجتماعی و چیزی بیش از مجموعه‌ای از فناوریهاست و باید از سازوکارهای جدید برای نگهداری مواد استفاده کند (شارما؛ ویشواناتان[3]، ۱۳۸۵). دسترسی غیرمجاز به اطلاعات و حمله به کتابخانه‌های دیجیتالی، اتفاقهای محتملی هستند که به عنوان نمونه‌هایی از آنها می‌توان به دو رخنهٔ امنیتی در دانشگاه ایندیانا در ایالات متحده آمریکا در تابستان ۲۰۰۲ و ماه می ۲۰۰۴ اشاره کرد که در هر دو مورد، زمان و تلاش زیادی برای بازگرداندن اطلاعات و ارتقای

1. Vermeulen & Solms.
2. Honan.
3. Sharma &Vishwanathan.

سیستم امنیتی جدید صرف شد (چنگ[1]، ۲۰۰۵). 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[2]، ۲۰۰۶). 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[3]» در سال ۲۰۰۳ نشان می‌دهد ۹۰٪ سازمانها معتقدند امنیت اطلاعات برای دستیابی آنها به هدفهای کلی‌شان بسیار حایز اهمیت است (نقل در سادوسکای[4] و دیگران، ۱۳۸۴: ۱۲۱).

برخی از مهم‌ترین مسائل مربوط به امنیت در کتابخانه‌های دیجیتالی می‌تواند شامل امنیت سخت‌افزارها و دیتا سنترها، 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، ۱۳۷۷). 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 نفوذگران به شبکهٔ اینترنت نیز مسئله امنیت و

1. Cheng.
2. Fox.
3. Ernest & Young.
4. Sadowsky.

حفاظت از منابع اطلاعاتی در کتابخانه‌های دیجیتالی را به عنوان یک امر حایز اهمیت مطرح می‌کند (علیپور حافظی؛ مطلبی، ۱۳۸۲).

نحوهٔ 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[1]، ۲۰۰۱). با وجود اهمیت حفظ امنیت در محیطهای اطلاع‌رسانی، این امر مهم در مقایسه با موضوعهایی مانند کمیّت 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.

سؤالهای پژوهش

۱. وضعیت امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران چگونه است؟
۲. آسیب‌پذیرترین نقاط امنیتی در کتابخانه‌های دیجیتالی ایران بر اساس شاخصهای مورد مطالعه کدامند؟
۳. رتبه‌بندی کتابخانه‌های دیجیتالی ایران بر حسب امنیت اطلاعات چگونه است؟

فرضیه‌های پژوهش

بین میانگین شاخصهای امنیت اطلاعات کتابخانه‌های دیجیتالی تفاوت معناداری وجود دارد.

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

---

1. Briney.

پیشینهٔ پژوهش

«محمودزاده و راد رجبی»(۱۳۸۵) در پژوهشی، مدیریت امنیت در سیستمهای اطلاعاتی و تأثیر عواملی که سیستمهای اطلاعاتی سازمانها را با خطر سرقت، نابودی و یا تغییر اطلاعات مواجه می‌سازند، مورد مطالعه قرار داد. نتایج پژوهش نشان داد مولفهٔ آگاهی نداشتن کاربران بالاترین تهدید و پس از آن «امنیت نیروی انسانی» دومین تهدید برای امنیت اطلاعات سیستمهای رایانه‌ای است. «طاهری» (۱۳۸۶) چارچوبی برای نقش عوامل انسانی در امنیت سیستمهای اطلاعاتی ارائه داده است. به طور خاص، هدف پژوهش یادشده، شناسایی و مدل‌سازی سازه‌های مدیریتی مؤثر بر اثربخشی امنیت سیستمهای اطلاعاتی بود. در این راستا، سازه‌های حمایت مدیریت عالی، آموزش امنیتی، فرهنگ امنیتی، مهارت امنیتی، تقویت خط‌مشی امنیتی، تجربیات و خودباوری افراد به عنوان عوامل مؤثر بر اثربخشی امنیت سیستمهای اطلاعاتی معرفی شدند.

«آرام» (۱۳۸۸) شاخصهای مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت گاز پارس جنوبی را مورد سنجش قرار داد. در این پژوهش، ابتدا شاخصهای تأثیرگذار بر مدیریت امنیت اطلاعات تعیین گردید، سپس با استفاده از تحلیل اطلاعاتی که از طریق پرسشنامه جمع‌آوری شده بود، به رتبه‌بندی و تعیین جایگاه شاخصها و عوامل کلیدی موثر بر بهبود سیستم مدیریت امنیت اطلاعات و تعیین مؤثرترین شاخصها پرداخته شد. نتایج پژوهش حاکی از تأثیرگذاری بیشتر عوامل انسانی از دیدگاه کارشناسان فناوری اطلاعات بود و پس از آن شاخصهای مربوط به عوامل مدیریتی، فنی و مالی قرار داشت.

«زنده دل نوبری» (۱۳۸۹) مدلی برای رتبه‌بندی سازمانها بر مبنای اندازه‌گیری و شناسایی میزان بلوغ امنیت اطلاعات در آنها ارائه نمود. بدین منظور، پس از تعیین شاخصهای امنیت اطلاعات در قالب دو دستهٔ کلیِ فنی و مدیریتی و با توجه به معیارهای سه‌گانهٔ «امنیت»، «ایمنی» و «پایداری»، نظرهای خبرگان فناوری اطلاعات بخشهای انفورماتیک در سه سازمان مطالعه شد. با توجه به یافته‌ها، از نظر بلوغ امنیت، بانک پاسارگارد رتبهٔ اول، دانشگاه تهران رتبهٔ دوم و بانک تجارت رتبهٔ سوم را به دست آوردند.

«چانگ و هو[1]»(۲۰۰۶) 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 عرصهٔ 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 اندازهٔ سازمان و نوع صنعت، به نحو قابل‌توجهی کاربرد مدیریت امنیت اطلاعات را تحت تأثیر قرار می‌دهد. «کوزما»[2] (۲۰۱۰) به آسیب‌پذیری امنیت در کتابخانه‌های دیجیتالی اروپا پرداخت و با استفاده از یک نرم‌افزار آزمایش خطرپذیری وب سایت، مسائل امنیتی ۸۰ کتابخانهٔ 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 (۲۵ ٪) و یا در سطح متوسط (۴۰ ٪) داشتند که منجر به تجارت ناامن آنلاین شده بود. همچنین، یافته‌ها حاکی از این بود که با وجود قوانین مربوط به حفاظت اطلاعات، کتابدارن اقدامهای لازم برای ایمن‌سازی سیستمهای اطلاعاتی آنلاین را اجرا نمی‌کنند.

«محابی[3]»(۲۰۱۰) آگاهی از امنیت اطلاعات از دیدگاه مدیران سیستم و کاربران نهایی در دانشگاه ایالتی فلوریدا را مطالعه نمود. نتایج نشان داد مدیران سیستم تأکید بیشتری بر تهدیدهای خارجی و فنی نسبت به تهدیدهای داخلی و غیر فنی ناشی از عوامل مختلف مانند دسترسی منابع، رفتار با کاربران و رضایت از ابزار فنی دارند. بخش دوم مطالعه که به بررسی کاربران نهایی مربوط بود، حاکی از نیاز به آموزش کاربران و ارتقای آگاهیهای آنها بود تا بتوانند از خود در برابر تهدیدهای امنیتی محافظت کنند. نتایج این مطالعه، اهمیت عوامل انسانی در امنیت اطلاعات را مورد

1. Chang & Ho.
2. Kuzma.
3. Mahabi.

تأکید قرار داد. «تینتاماسیک[1]»(۲۰۱۰) به بررسی رابطه بین سیستمهای سازمان و آگاهی امنیت اطلاعات پرداخت. تمرکز این پژوهش بر روی بررسی رابطهٔ حیاتی بین سیستمهای سازمان در چارچوب نظریهٔ رفتار سازمانی و آگاهی امنیت اطلاعات (ISA) در چارچوب نظریهٔ امنیت اطلاعات بود. مسئله اصلی در این مطالعه، آگاهی نداشتن کاربران از مسائل امنیتی به عنوان یک عامل بازدارنده برای سازمانها در دفاع در برابر حملات سایبر بود. بر اساس یافته‌ها، ارتباط معناداری بین آگاهی کاربران از امنیت اطلاعات و ابعاد ساختار سازمان رسمی، ابعاد فرهنگ سازمانی و روشها و سیاستهای منابع انسانی وجود دارد.

روش‌شناسی پژوهش

روش پژوهش، پیمایشی تحلیلی و جامعهٔ 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، کتابخانهٔ دیجیتالی مانند نورلایب، تبیان، دید که دارای نرم‌افزارهای خود ساخته بودند، جزء جامعه آماری پژوهش هستند. پس از بررسیهای به عمل آمده، تعداد ۵۸ کتابخانهٔ دیجیتالی فعال در ایران در زمان پژوهش (تابستان ۱۳۹۰) شناسایی شد.

با توجه به هدفهای پژوهش، بهترین راه جمع‌آوری اطلاعات، استفاده از پرسشنامه بود که بر مبنای استاندارد ISO/IEC 27002 تهیه گردید. پرسشنامه شامل ۷۹ سؤال دو وجهی (یک برای بلی و صفر برای خیر) برای سنجش یازده شاخص

1. Tintamusik.

امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران بود. این شاخصها عبارتند از: خط‌مشی امنیت، سازماندهی امنیت اطلاعات، مدیریت داراییها، امنیت منابع انسانی، امنیت فیزیکی و محیطی، مدیریت ارتباطات و عملیات، کنترل دسترسی، تهیه، توسعه و نگهداری سیستمهای اطلاعاتی، مدیریت حوادث امنیت اطلاعات، مدیریت تداوم کسب و کار و انطباق.

اعتبار صوری و محتوایی پرسشنامه پس از بررسی دقیق متخصصان کتابداری و اطلاع‌رسانی و متخصصان و کارشناسان فناوری اطلاعات، تأیید شد. پایایی پرسشنامه نیز با محاسبه آلفای کرونباخ بررسی و با آلفای ۹۲/. تأیید گردید. پرسشنامه‌ها توسط مسئولان فناوری اطلاعات و مدیران کتابخانه‌های دیجیتالی پاسخ داده شدند. (برای اطلاع از شاخصهای مورد بررسی در پژوهش، نمونهٔ پرسشنامه در پیوست آمده است).

برای تعیین سطح امنیت در تحلیل داده‌ها، میانگین پاسخها در بازهٔ صفر تا ۱ به سه سطح تقسیم شده است؛ به این ترتیب که میانگین ۰ – ۰/۳۴ نشانگر سطح ضعیف، ۰/۳۴– ۰/۶۷ سطح متوسط و ۰/۶۷– ۱ سطح قوی است. برای آزمون فرضیهٔ تفاوت معنادار بین میانگین شاخصهای امنیت کتابخانه‌های دیجیتالی از آنالیز واریانس و برای آزمون فرضیه وجود تفاوت معنادار بین امنیت اطلاعات در کتابخانه‌های دیجیتالی دانشگاهی و غیردانشگاهی، از آزمون t استفاده شد. تحلیل داده‌ها با استفاده از نسخه ۱۶ نرم‌افزاری آماری SPSS انجام گرفت.

یافته‌های پژوهش

یافته‌ها در مورد سیستم عامل مورد استفاده در سرور اصلی سایت کتابخانه‌های دیجیتالی ایران نشان داد بیشترین تعداد (۸۴/۴٪) کتابخانه‌ها از ویندوز و کمترین تعداد (۱۵/۶٪) از لینوکس استفاده می‌کنند. در بررسی نوع سرور نیز مشخص شد سرور به صورت اختصاصی با ۹۷/۸ ٪ بیشترین فراوانی و سرور به صورت اجاره‌ای با ۲/۲٪ کمترین فراوانی را دارد. همچنین، تمام سرورهای کتابخانه‌های دیجیتالی با درصد

فراوانی ۱۰۰ در داخل ایران مستقر بوده، ۳۹ کتابخانه دیجیتالی با درصد فراوانی ۸۶/۷ 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 ۱ نشان داده شده است.

جدول ۱. توزیع فراوانی نرم‌افزارهای مورد استفاده کتابخانه‌های دیجیتالی

نرم‌افزار	فراوانی	درصد فراوانی
پیام مشرق	۱۴	۳۱/۱
پارس آذرخش	۱۴	۳۱/۱
نوسا	۵	۱۱/۱
پروان پژوه	۴	۸/۹
خود ساخته	۴	۸/۹
پاپیروس	۲	۴/۴
ارم	۱	۲/۲
وستا	۱	۲/۲
کل	۴۵	۱۰۰

جدول ۱ نشان می‌دهد نرم‌افزار پارس آذرخش و پیام مشرق بالاترین فراوانی (۳۱/۱٪) و نرم افزار ارم و وستا کمترین فراوانی (۲/۲٪) را دارند.

سؤال اول پژوهش: وضعیت امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران چگونه است؟

جدول ۲. شاخصهای میانگین و انحراف معیار امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران

شاخصهای آماری / متغیر	میانگین	انحراف معیار	تعداد
امنیت اطلاعات	۰/۷۹	۰/۱۶۵	۴۵

در جدول ۲ شاخصهای میانگین و انحراف معیار امنیت اطلاعات در کتابخانه‌های دیجیتالی نشان داده شده است. میانگین امنیت اطلاعات کل کتابخانه‌های دیجیتالی ۰/۷۹ است که در سطح قوی ارزیابی می‌شود.

سؤال دوم پژوهش: آسیب‌پذیرترین نقاط امنیتی در کتابخانه‌های دیجیتالی ایران بر اساس شاخص‌های مورد مطالعه کدامند؟

جدول۳. میانگین و انحراف معیار شاخصهای امنیت اطلاعات کل کتابخانه‌های دیجیتالی ایران

شاخصها	میانگین	انحراف معیار
امنیت فیزیکی و محیطی	۰/۸۷	۰/۲۱
مدیریت تداوم کسب و کار	۰/۸۴	۰/۳۰
مدیریت داراییها	۰/۸۳	۰/۲۴
مدیریت ارتباطات و عملیات	۰/۸۲	۰/۲۰
کنترل دسترسی	۰/۷۹	۰/۱۸
تهیه، توسعه و نگهداری سیستمهای اطلاعاتی	۰/۷۸	۰/۲۳
انطباق	۰/۷۸	۰/۲۵
سازماندهی امنیت اطلاعات	۰/۷۱	۰/۲۷
مدیریت حوادث امنیت اطلاعات	۰/۷۰	۰/۲۷
خط‌مشی امنیت	۰/۶۳	۰/۴۲
امنیت منابع انسانی	۰/۶۳	۰/۳۰

در جدول۳ مشاهده می‌شود که شاخصهای «خط‌مشی امنیت» با میانگین۰/۶۳ و «امنیت منابع انسانی» با میانگین ۰/۶۳ پایین‌ترین میانگین را دارند و آسیب‌پذیرترین نقاط امنیتی کتابخانه‌های دیجیتالی ایران هستند.

سؤال سوم پژوهش: رتبه‌بندی کتابخانه‌های دیجیتالی ایران بر حسب امنیت اطلاعات چگونه است؟

جدول۴. شاخصهای میانگین و انحراف معیار امنیت اطلاعات کتابخانه‌های دیجیتالی ایران به ترتیب نزولی

کتابخانهٔ دیجیتال	میانگین	انحراف معیار
کتابخانهٔ دیجیتال مؤسسه نشر امام خمینی(ره)	۱	۰
کتابخانه دیجیتال پژوهشگاه نیرو	۱	۰
کتابخانه دیجیتال فرهنگستان هنر	۱	۰
کتابخانه دیجیتال علوم انسانی شهرداری تهران	۱	۰
کتابخانه دیجیتال شرکت برق منطقه‌ای خراسان	۱	۰
کتابخانه دیجیتال دانشگاه تبریز	۱	۰
کتابخانه دیجیتال مجلس	۰/۹۹	۰/۱۱
کتابخانه دیجیتال علوم پزشکی و خدمات بهداشتی درمانی شهید بهشتی	۰/۹۹	۰/۱۳
کتابخانه دیجیتال شرکت ملی مناطق نفت‌خیز جنوب	۰/۹۹	۰/۱۱
کتابخانه دیجیتال دانشگاه علوم پزشکی گیلان	۰/۹۷	۰/۲۲
کتابخانه دیجیتال شهرک علمی و تحقیقاتی اصفهان	۰/۹۶	۰/۲۷
کتابخانه دیجیتال مرکز مخابرات ایران	۰/۹۱	۰/۳۰
کتابخانه دیجیتال مرکز اطلاعات و مدارک علمی ایران (ایران داک)	۰/۹۰	۰/۲۶
کتابخانه دیجیتال مرکزی تبریز	۰/۹۰	۰/۳۸
کتابخانه دیجیتال شهرداری تهران (کتابخانه مرکزی شهرداری تهران)	۰/۸۹	۰/۳۵

کتابخانهٔ دیجیتال	میانگین	انحراف معیار
کتابخانه دیجیتال دانشگاه امیرکبیر	۰/۸۶	۰/۳۷
کتابخانه دیجیتال دانشگاه علوم پزشکی زنجان	۰/۸۵	۰/۳۶
کتابخانه دیجیتال دانشگاه علوم پزشکی شهید صدوقی یزد	/۸۴	۰/۴۳
کتابخانه دیجیتال دانشگاه علوم پزشکی تهران	۰/۸۳	۰/۳۸
کتابخانه دیجیتال شرکت ملی صنایع پتروشیمی تهران	۰/۸۲	۰/۴۲
کتابخانه دیجیتال پژوهشکده تحقیقات فضایی	۰/۸۲	۰/۳۸
کتابخانه دیجیتال دانشگاه صنعتی اصفهان	۰/۸۱	۰/۴۰
کتابخانه دیجیتال ارم	/۸۰	۰/۴۰
کتابخانه دیجیتال کتابخانه ملی ایران	۰/۸۰	۰/۴۳
کتابخانه دیجیتال دانشگاه علوم پزشکی بیرجند	۰/۷۹	۰/۴۲
کتابخانه دیجیتال دانشگاه علوم پزشکی شیراز	۰/۷۸	۰/۴۴
کتابخانه دیجیتال دانشگاه علوم پزشکی و خدمات درمانی ایلام	۰/۷۷	۰/۴۲
کتابخانه دیجیتال دانشگاه آزاد اسلامی واحد نجف‌آباد	۰/۷۷	۰/۴۵
کتابخانه دیجیتال دانشگاه یزد	۰/۷۶	۰/۴۶
کتابخانه دیجیتال دانشگاه صنعتی شریف	۰/۷۵	۰/۴۶
کتابخانه دیجیتال دانشگاه شیراز	۰/۷۴	۰/۳۹
کتابخانه دیجیتال آستان قدس احمدی و محمدی (شاه چراغ)	۰/۷۴	۰/۴۵
کتابخانه دیجیتال تبیان	۰/۷۴	۰/۴۷
کتابخانه دیجیتال شهرداری اصفهان	۰/۷۱	۰/۴۸
کتابخانه دیجیتال نور	۰/۶۷	۰/۵۰
کتابخانه دیجیتال معاونت توسعه و فناوری اطلاعات و تجارت الکترونیکی وزارت بازرگانی	۰/۶۵	۰/۴۸
کتابخانه دیجیتال مدیریت بحران شهرداری تهران	۰/۶۴	۰/۴۹
کتابخانه دیجیتال دانشگاه ولی‌عصر رفسنجان	۰/۶۲	۰/۴۹

کتابخانهٔ دیجیتال	میانگین	انحراف معیار
کتابخانه دیجیتال دانشگاه ارومیه	۰/۶۰	۰/۵۰
کتابخانه دیجیتال سازمان بورس و اوراق بهادار تهران	۰/۶۰	۰/۴۹
کتابخانه دیجیتال سازمان فرهنگی هنری شهری تهران(کتابخانه عمومی تهران)	۰/۵۹	۰/۵۰
کتابخانه دیجیتال پردیس علوم دانشگاه تهران	۰/۵۵	۰/۵۰
کتابخانه دیجیتال موسسه تحقیقات و نشر معارف اهل‌البیت	۰/۴۹	۰/۵۰
کتابخانه دیجیتال دانشگاه صنعتی جندی شاپور	۰/۴۱	۰/۵۰
کتابخانه دیجیتال دانشکده کارآفرینی تهران	۰/۳۷	۰/۴۹

چنان‌که در جدول ۴ 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 ۱ بالاترین میانگین را داشته، در سطح قوی قرار ارزیابی می‌شوند. کتابخانه دیجیتال دانشکده کارآفرینی تهران با میانگین ۳۷/. دارای پایین‌ترین میانگین است و در سطح متوسط ارزیابی می‌شود.

جدول۵. توزیع فراوانی سطوح امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران

کتابخانه‌های دیجیتال	فراوانی	درصد فراوانی
سطح قوی	۳۴	۷۵/۵۵
سطح متوسط	۱۱	۲۴/۴۶
سطح ضعیف	۰	۰
جمع	۴۵	۱۰۰

جدول ۵ نشان می‌دهد بیشترین درصد (۷۵/۵۵ ٪) کتابخانه‌های دیجیتالی از نظر امنیت اطلاعات در سطح قوی قرار دارند. سطح امنیت در ۲۴/۴۶ ٪ کتابخانه‌ها متوسط است.

فرضیه اول: بین میانگین شاخصهای امنیت اطلاعات کتابخانه‌های دیجیتالی تفاوت معناداری وجود دارد.

برای آزمون تفاوت معنادار بین شاخصهای امنیت اطلاعات، از آنالیز واریانس یک راهه در سطح اطمینان ۹۵ ٪ استفاده گردید. نتایج آزمون در جدول ۶ نشان داده شده است.

جدول۶. نتایج آزمون آنالیز واریانس برای مقایسهٔ میانگینهای شاخصهای امنیت اطلاعات کتابخانه‌های دیجیتالی

شاخصها	تعداد	میانگین	انحراف معیار	مقدار آماره f	درجه آزادی	p-value	نتیجه آزمون
خط‌مشی امنیت	۴۳	۰/۶۳	۰/۴۲	۳/۹۵	۱۰	۰/۰۰	اختلاف معنادار
سازماندهی امنیت اطلاعات	۴۴	۰/۷۱	۰/۲۷				
مدیریت داراییها	۴۳	۰/۸۳	۰/۲۴				
امنیت منابع انسانی	۴۵	۰/۶۳	۰/۳۰				
امنیت فیزیکی و محیطی	۴۵	۰/۸۷	۰/۲۱				
مدیریت ارتباطات و عملیات	۴۵	۰/۸۲	۰/۲۰				
کنترل دسترسی	۴۵	۰/۷۹	۰/۱۸				

شاخصها	تعداد	میانگین	انحراف معیار	مقدار آماره f	درجه آزادی	p-value	نتیجه آزمون
تهیه، توسعه و نگهداری سیستمهای اطلاعاتی	۴۵	۰/۷۸	۰/۲۳				
مدیریت حوادث امنیت اطلاعات	۴۴	۰/۷۰	۰/۲۷				
مدیریت تداوم کسب و کار	۴۲	۰/۸۴	۰/۳۰				
انطباق	۴۳	۰/۷۸	۰/۲۵				

چنان‌که در جدول ۶ مشاهده می‌شود، مقدار سطح معناداری برابر صفر است و با توجه به اینکه این مقدار کمتر از ۰/۰۵ است، فرضیهٔ 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 شاخصهاست.

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

برای آزمون فرضیه دوم، از آزمون t برای دو نمونهٔ مستقل در سطح اطمینان ۹۵ ٪ استفاده شد. نتایج در جدول ۷ نشان داده شده است.

جدول۷. نتایج آزمون t برای مقایسه امنیت اطلاعات کتابخانه‌های دیجیتالی دانشگاهی و غیردانشگاهی ایران

متغیر	تعداد	میانگین	انحراف معیار	آماره t	درجه آزادی	سطح معناداری
کتابخانه‌های دیجیتال دانشگاهی	۲۰	۰/۷۵	۰/۱۷	-۱/۴۶	۴۳	۰/۱۵
کتابخانه‌های دیجیتال غیردانشگاهی	۲۵	۰/۸۲	۰/۱۵			

چنان‌که در جدول ۷ مشاهده می‌شود، با توجه به سطح معناداری که برابر ۱۵/. شده و بیشتر از ۰۵/. می‌باشد، فرض صفر آزمون پذیرفته می‌شود. به این ترتیب، وجود تفاوت معنادار بین دو گروه تأیید نمی‌شود و در نتیجه فرضیه دوم پژوهش رد می‌شود.

بحث و نتیجه‌گیری

یافته‌های پژوهش مبنی بر وضعیت امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران، نشان داد میانگین امنیت کل کتابخانه‌های دیجیتالی ۰/۷۹ 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 ۰/۶۳ است. وجود خط‌مشی امنیت از مهم‌ترین شاخصهای تعیین کنندهٔ 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، ۱۳۸۴: ۱۵۰). 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 ۰/۶۳ است که پس از شاخص خط‌مشی، آسیب‌پذیرترین نقاط امنیتی کتابخانه‌های دیجیتالی ایران است. یافته‌های این پژوهش با نتایج پژوهش «آرام» (۱۳۸۸)، «محمودزاده و راد رجبی» (۱۳۸۴) 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 ۸۰٪ جرایم سنگین رایانه‌ای را افرادی مرتکب می‌شوند که یا از دسترسی قانونی به داده‌ها برخوردارند و یا در گذشتهٔ نزدیک از آن برخوردار بوده‌اند. از همین رو، بخش مهمی از یک طرح امنیتی خوب مربوط به ادارهٔ کارکنان با دسترسیهای طبقه‌بندی شده است (سادوسکای و دیگران، ۱۳۸۴: ۱۵۹). 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، کتابخانهٔ دیجیتال علوم‌انسانی شهرداری تهران، کتابخانه دیجیتال شرکت برق منطقه‌ای خراسان، کتابخانه دیجیتال دانشگاه تبریز با میانگین ۱ از حداکثر میانگین لازم برخوردار بوده، در سطح قوی قرار دارند. کتابخانه دیجیتال دانشکده کارآفرینی تهران با میانگین ۰/۳۷ پایین‌ترین میانگین را دارد و در سطح متوسط ارزیابی می‌شود. براساس یافته‌های پژوهش، بیشترین درصد کتابخانه‌های دیجیتالی (۷۵/۵۵ ٪) در سطح قوی قرار دارند و کتابخانه‌های دیجیتالی در سطح متوسط، ۲۴/۴۶٪ را تشکیل می‌دهند. با در نظر گرفتن این یافته‌ها و همچنین نتایج پژوهش «کوزما» (۲۰۱۰) مبنی بر نقصهای امنیتی

کتابخانه‌های دیجیتالی اروپا، مشاهده می‌شود که کتابخانه‌های دیجیتالی ایران از نظر امنیت اطلاعات در مقایسه با کتابخانه‌های دیجیتالی اروپا وضعیت مناسب‌تری دارند. چنان‌که پیشتر اشاره شد، پژوهش «کوزما» (۲۰۱۰) نشان داد در ۲۵ ٪ کتابخانه‌های دیجیتالی اروپا، مشکلات امنیتی در سطح بحرانی و در ۴۰ ٪ 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 به‌دست آمده 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:

۱. 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.

۲. منابع انسانی از مهم‌ترین عوامل تأثیرگذار بر امنیت کتابخانه‌های دیجیتالی است،

زیرا نیروی انسانی مهم‌ترین نقش را در نحوهٔ 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.

- نقشها و مسئولیتهای امنیتی کارکنان، پیمانکاران و کاربران ثالث بر اساس خط‌مشی امنیت اطلاعات سازمان تعریف و مستندسازی شود.
- اقدامهای نظارتی در خصوص تأیید پیشینهٔ 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 شناخته شده، انجام شود.
- 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.
- مسئولیتهای کارکنان، پیمانکاران و کاربران ثالث و سازمان در قبال امنیت اطلاعات باید به نحو روشن و دقیق در قرارداد استخدامی تصریح گردد.
- مدیریت ملزم شود تا از کارکنان، پیمانکاران و کاربران ثالث بخواهد امنیت را بر اساس خط‌مشی‌های تعیین شده و روّیه‌های سازمان به مورد اجرا بگذارد.
- تمامی کارکنان سازمان و بر حسب مورد پیمانکاران و کاربران ثالث ملزم شوند تا دوره‌های آموزشی و آگاه‌سازی در خصوص خط‌مشیها و روّیه‌های سازمان را در زمینهٔ امنیت اطلاعات بر حسب نوع شغل‌خود طی کنند.
- در مورد آن دسته از کارکنانی که مرتکب نقض امنیت می‌شوند، وجود یک فرایند تنبیهی رسمی الزامی باشد.
- مسئولیتها در قبال فسخ استخدام یا تغییر آن باید به صراحت تعیین و واگذار گردد.
- 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.

- حق دسترسی تمامی کارکنان، پیمانکاران و کاربران ثالث بـه اطلاعـات و مراکـز پردازش اطلاعات باید به محض فسخ استخدام، قرارداد یا موافقت‌نامـه حـذف شده و یا به محض هرگونه تغییر، مورد تعدیل قرار گیرد.

پیشنهاد می‌شود مدیران کتابخانه‌های دیجیتالی ایران قبل از هـرگونـه اقـدامی، بـرای توسعهٔ منابع کتابخانه‌های خود بـرای حصـول اطمینـان بیشـتر از امنیـت نـرم‌افزارهـا و سخت‌افزارهای مورد استفاده، با استفاده از تکنیکهـای پدافنـد غیرعامـل و بـا مشـارکت تیمهای امنیتی نسبت به طراحی حملات هکری اقدام نموده و بـا شناسـایی حفـره‌هـای امنیتی، تلاش کنند تا آنها را ترمیم نمایند.

منابع

- آرام، محمدرضا(۱۳۸۸). بررسی و سنجش مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فنـاوری اطلاعات شرکت گاز پارس جنوبی. پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی.
- زایلینسکی، کریستوفر(۱۳۷۷). «عصر الکترونیک و فقرای اطلاعاتی: فرصت‌ها و مخاطرات». ترجمه عباس گیلوری. در گزیده مقالات نوزدهمین کنفرانس بین‌المللی اطلاع‌رسانی پیوسته. تهران: مرکـز اطلاع‌رسانی و خدمات علمی جهاد سازندگی.
- زنده دل نوبری، بابک(۱۳۸۹). ارائه مدلی جهت رتبه‌بنـدی سـازمان‌هـا بـر مبنـای انـدازه‌گیـری و شناسایی میزان بلوغ امنیت اطلاعات در آنها. پایان‌نامه کارشناسی ارشد دانشگاه آزاد اسلامی واحـد علوم تحقیقات.
- سادوسکای، جورج و دیگران(۱۳۸۴). راهنمای امنیت فناوری اطلاعات. ترجمه مهدی میـردامادی، زهرا شجاعی، محمدجواد صمدی. تهران: دبیرخانه‌شورای عالی اطلاع‌رسانی.
- شارما، آر.کی؛ ویشواناتان، کی.آر(۱۳۸۵). کتابخانه‌های دیجیتالی: توسـعه و چـالش. ترجمـه مـریم صابری.فصلنامه کتاب، ش ۶۸.
- طاهری، مهدی(۱۳۸۶). ارائه چارچوبی برای نقش عوامل انسانی در امنیت سیستم‌هـای اطلاعـاتی. پایان‌نامه کارشناسی ارشد دانشگاه تربیت مدرس، دانشکده علوم انسانی.
- علیپور حافظی، مهدی و داریوش مطلبی (۱۳۸۲). مجموعه مقالات همایش‌های انجمن کتابداری و

اطلاع‌رسانی ایران. ج۲.کتابخانه‌های دیجیتالی: مفاهیم و جنبه‌های فنی-اجرایی. تهران: انجمن کتابداری و اطلاع‌رسانی ایران، سازمان اسناد و کتابخانه ملی جمهوری اسلامی ایران.

- محمودزاده، ابراهیم و مهدی رادرجبی (۱۳۸۵). مدیریت امنیت در سیستم‌های اطلاعاتی. فصلنامه علوم مدیریت ایران، دوره اول، شماره ۴.
- Briney, A. (2001) ' Industry Survey', Information Security, pp. 34-47
- Chang , Shuchih Ernest; Ho, Chienta Bruce (2006) "Organizational factors to the effectiveness of implementing information security management".
- Cheng, K. (2005), "Surviving hacker attacks proves that every cloud has a silver lining", Computers in Libraries, Vol. 25 No. 3, pp. 6-8, 52-6.
- Fox, R. (2006), "Digital libraries: the systems analysis perspective, Vandals at the gates", OCLC Systems & Services, Vol. 22 No. 4, pp. 249-55.
- Honan, B., (2006), IT security-oommoditized, badly. lnfosecurity Today, Vol. 3, Iss: 5, pp. 41.
- ISO/IEC 27002:2005, Information technology, Security techniques, Code of practice for information security management.
- Karyda, M., Kiountouzis, E. & Kokolakis, S. (2005). Information systems security policies: a contextual perspective, Computers & Security, 24(3), 246-260.
- Kuzma, Joanne (2010) "European digital libraries: web security vulnerabilities", Library Hi Tech, Vol. 28 Iss: 3, pp.402 – 413.
- Mahabi, Victoria(2010). Information Security Awareness: System Administrators and End-User Perspectives at Florida State University. Dissertation for the degree of Doctor of Philosophy in Library and Information Studies . the Florida State University.
- Tintamusik, Yanarong(2010). Examining the Relationship between Organization Systems and Information Security Awareness. Dissertation for the degree of Doctor Of Business Administration. Northcentral University.
- Vermeulen, c., Von Solms, R., (2002), the information security management toolbox-taking the pain out of security management, Information management & computer security, 10/3 119-125.

پیوست

پرسشنامهٔ امنیت اطلاعات در کتابخانه‌های دیجیتالی

۱. خط‌مشی امنیت	بلی	خیر
۱. آیا سند خط مشی امنیت اطلاعات به طور مناسب، توسط مدیریت تهیه و تأیید گردیده و پس از انتشار به تمام کارکنان دست‌اندرکار سایت کتابخانه دیجیتالی ابلاغ شده است؟		
۲. آیا خط‌مشی امنیت اطلاعات، به طور منظم بازنگری می‌شود، تا مناسب بودن آن، تضمین گردد؟		

۲. سازماندهی امنیت اطلاعات	بلی	خیر
۳. آیا مدیریت، امنیت را در درون سازمان از طریق جهت‌گیری شفاف، مکلّف کردن به صورت صریح و اعلام مسئولیتهای امنیت اطلاعات، حمایت می‌کند؟		
۴. آیا فعالیتهای امنیت اطلاعات، توسط افرادی از بخشهای مختلف سازمان با نقشها و کارکردهای شغلی مرتبط، هماهنگ می‌شوند؟		
۵. آیا تمامی مسئولیتهای امنیت اطلاعات، به وضوح تعریف شده‌اند؟		
۶. آیا توافقنامه‌های محرمانگی و عدم افشای اطلاعات، ضمانت اجرایی دارند و به طور منظم بازنگری می‌شوند؟		
۷. آیا ارتباطات مناسبی با مسئولان مرتبط امنیتی و مدیران سایت برقرار و حفظ می‌شود؟		
۸. آیا ارتباطات مناسبی با گروه‌ها یا انجمنهای متخصص و حرفه‌ای در حوزه امنیت اطلاعات برقرار و حفظ می‌شود؟		
۹. آیا رویکرد سازمان به مدیریت امنیت اطلاعات و پیاده‌سازی آن، در فاصله‌های زمانی طرح‌ریزی شده بازنگری می‌شود؟		
۱۰. آیا مخاطرات امنیتی ناشی از ایجاد دسترسی راه دور با طرفهای بیرونی، پیش از اجازه دسترسی، شناسایی شده و کنترلهای مناسب، انجام می‌شود؟		
۱۱. آیا توافقنامه‌های مشخصی برای ایجاد امنیت در موارد بهره‌گیری از طرفها، پیمانکاران یا شرکتهای ثالث برای برنامه‌نویسی وجود دارد؟		

۳. مدیریت داراییها	بلی	خیر
۱۲. آیا تمامی داراییها به وضوح شناسایی شده و سیاهه‌ای از تمام داراییهای مهم، تنظیم و نگهداری می‌شود؟ (شامل سخت‌افزار و نرم‌افزارهای مورد استفاده مستقر در سازمان یا خارج از آن)		
۱۳. آیا تمامی اطلاعات و داراییهای مرتبط با امکانات پردازش اطلاعات (نظیر سرویس دهنده‌های وب) در تملک بخش معینی از سازمان(همانند واحد فناوری		

۳. مدیریت داراییها	بلی	خیر
اطلاعات) می‌باشد؟		
۱۴. آیا قواعدی برای استفاده از اطلاعات و نرم‌افزارهای پردازش و به‌روزرسانی اطلاعات، تدوین و پیاده‌سازی شده است؟		
۱۵. آیا اطلاعات با توجه به ارزش آن، الزامهای قانونی، حساسیت و بحرانی بودن برای سازمان، طبقه‌بندی شده‌اند؟		

۴. امنیت منابع انسانی	بلی	خیر
۱۶. آیا نقشها و مسئولیتهای امنیتی کارکنان، پیمانکاران و کاربران ثالث، با توجه به خط‌مشی امنیت اطلاعات سازمان، تعریف و مشخص شده است؟		
۱۷. آیا برای تصدیق سوابق تمامی داوطلبان استخدام، پیمانکاران، و کاربران شخص ثالث، بررسیهایی با توجه به قوانین، آئین‌نامه‌ها و اصول اخلاقی مرتبط، و متناسب با الزامهای کسب و کار، طبقه‌بندی اطلاعاتی که در دسترس قرار می‌گیرد و مخاطرات دیده شده، انجام می‌شود؟		
۱۸. آیا کارکنان، پیمانکاران و کاربران شخص ثالث، برای انجام امور، توافقنامه‌های امنیتی مشخصی را قبول و امضا می‌کنند؟		
۱۹. آیا تمامی کارکنان سازمان و در صورت لزوم، پیمانکاران و کاربران ثالث، در خصوص امنیت اطلاعات به صورت مناسب آموزش می‌بینند و آگاه‌سازی در برابر مخاطرات صورت می‌پذیرد؟		
۲۰. آیا یک فرایند انضباطی رسمی، برای کارکنانی که مرتکب نقض امنیتی می‌شوند، وجود دارد؟		
۲۱. آیا دسترسی تمامی کارکنان، پیمانکاران و کاربران ثالث به اطلاعات و امکانات پردازش اطلاعات، به محض خاتمه خدمت، قرارداد یا تغییر شغل، حذف یا بازنگری می‌شود؟		

۵. امنیت فیزیکی و محیطی	بلی	خیر
۲۲. آیا نواحی امن، به منظور حصول اطمینان از اینکه فقط کارکنان مجاز، اجازه دسترسی دارند، توسط کنترلهای وردی مناسب، حفاظت می‌شوند؟		
۲۳. آیا برای مقابله با خسارت ناشی از آتش، سیل، زمین لرزه، انفجار، آشوب داخلی، و شکلهای دیگری از حوادث طبیعی یا مصنوعی، حفاظت فیزیکی طراحی و به کار گرفته شده است؟		
۲۴. آیا تجهیزات در برابر قطع برق و سایر اختلالهای ناشی از نقصهای امکانات پشتیبانی، محافظت می‌شوند؟		
۲۵. آیا تجهیزات به منظور حصول اطمینان از تداوم دسترس‌پذیری و یکپارچگی‌شان، به درستی نگهداری می‌شوند؟		

۶. مدیریت ارتباطات و عملیات	بلی	خیر
۲۶. آیا تغییر در امکانات و سیستمهای پردازش اطلاعات به لحاظ سخت‌افزاری و نرم‌افزاری تحت کنترل می‌باشد؟		
۲۷. آیا به منظور کاهش فرصتهای دستکاری غیرعمد یا غیرمجاز، یا استفاده نابجا، وظایف و حدود مسئولیت‌ها، تفکیک شده است؟		
۲۸. آیا خدمات، گزارشها و سوابق تهیه شده توسط پیمانکاران و اشخاص ثالث، به صورت قاعده‌مند پایش، بازنگری و نگهداری می‌شوند؟		
۲۹. آیا پیش از تهیه نرم‌افزار و سخت‌افزار جدیدی که به منظور ارتقای سیستم تهیه می‌شود، نظیر سرویس دهنده‌ها و نرم‌افزارهای تحت وب، برای اطمینان از صحت و کارایی، آزمایشهای مناسب انجام می‌پذیرند؟		
۳۰. آیا کنترلهای لازم برای تشخیص، پیشگیری و ترمیم به منظور حفاظت در برابر کدهای مخرّب رایانه‌ای و ویروسها، انجام می‌شود؟		
۳۱. آیا نسخ پشتیبان از اطلاعات و نرم‌افزارها، با توجه به خط‌مشی توافق شده، به صورت منظم تهیه می‌شوند؟		

۶. مدیریت ارتباطات و عملیات	بلی	خیر
۳۲. آیا برای مدیریت محیطهای ذخیره‌سازی قابل جابجایی همانند فلش دیسک و هارد اکسترنال و ...، روشهای اجرایی وجود دارد؟		
۳۳. آیا روشهای اجرایی جابجایی و ذخیره‌سازی اطلاعات، برای حفاظت این اطلاعات در برابر افشای غیرمجاز یا استفاده نابجا وجود دارد؟		
۳۴. آیا مستندات سیستم در برابر دسترسی غیرمجاز حفاظت می‌شوند؟		
۳۵. آیا برای تبادل اطلاعات و نرم‌افزار بین سازمان و طرفهای بیرونی، توافق‌نامه‌هایی ایجاد شده است؟		
۳۶. آیا اطلاعات انتقالی، به منظور پیشگیری از انتقال ناقص، مسیریابی اشتباه، تغییر یافتن غیر مجاز پیغام، افشای غیر مجاز، بازگرداندن یا تکرار غیر مجاز پیغام حفاظت می‌شوند؟		
۳۷. آیا سوابق فعالیتهای کاربران، برای یک بازهٔ زمانی توافق شده نگهداری می‌شوند تا در رسیدگیهای آتی و پایش کنترل دسترسی کمک نمایند؟		
۳۸. آیا وقایع خرابیها ثبت، تحلیل، و اقدام مناسبی انجام می‌شود؟		
۳۹. آیا ساعتهای تمامی سیستمهای پردازش اطلاعات کاربران و سرورها، با یک منبع زمانیِ توافق شده همزمان می‌شوند؟		

۷. کنترل دسترسی	بلی	خیر
۴۰. آیا یک خط‌مشی کنترل دسترسی با توجه به شرایط کار و الزامهای امنیتی در خصوص دسترسی وجود دارد؟		
۴۱. آیا برای اعطا یا لغو دسترسی به سیستمها و خدمات اطلاعاتی، یک روش اجرایی رسمی ثبت و حذف کاربر وجود دارد؟		
۴۲. آیا تخصیص و به کارگیری اختیارات ویژه، محدود و کنترل شده است؟		
۴۳. آیا تخصیص کلمات عبور، از طریق یک فرایند مدیریتی رسمی کنترل می‌شود؟		
۴۴. آیا مدیریت با استفاده از یک فرایند رسمی، حقوق دسترسی کاربران را در		

۷. کنترل دسترسی	بلی	خیر
فاصله‌های زمانی منظم، بازنگری می‌کند؟		
۴۵. آیا کاربران در انتخاب و به کارگیری کلمه عبور، به پیروی از شیوه‌های امنیتی صحیح ملزم می‌شوند؟		
۴۶. آیا کاربران تنها به خدماتی که مشخصا استفاده از آنها برایشان مجاز شده، دسترسی دارند؟		
۴۷. آیا برای کنترل دسترسی کاربران راه دور، روشهای مناسب تصدیق هویت به کار گرفته می‌شود؟		
۴۸. آیا دسترسی فیزیکی و منطقی به درگاه‌های عیب‌یابی و پیکربندی، تحت کنترل است؟		
۴۹. آیا گروه‌های کاربری و سیستمهای اطلاعاتی، در شبکه با دسترسی تفکیک شده مشخص شده‌اند؟		
۵۰. آیا تمامی کاربران یک شناسه یکتا (شناسه کاربر) برای استفاده شخصی خودشان دارند و یک فن مناسب تصدیق هویت، به منظور اثبات هویت ادعا شده یک کاربر، انتخاب می‌شود؟		
۵۱. آیا سیستمهای مدیریت کلمات عبور، تعاملی بوده و کیفیت کلمات عبور را تضمین می‌نماید؟		
۵۲. آیا استفاده از برنامه‌های کمکی سیستم که ممکن است قادر به ابطال کنترلهای سیستم و برنامه کاربردی باشند، محدود و به شدت کنترل می‌شوند؟		
۵۳. آیا لایه‌های ارتباطی غیرفعال باید پس از یک بازهٔ زمانی تعریف شده برای غیرفعال بودن، بسته و قطع می‌شوند؟		
۵۴. آیا به منظور فراهم‌آوری امنیت بیشتر برای برنامه‌های کاربردی پرمخاطره، محدودیتهایی در زمانهای اتصال اعمال می‌گردد؟		
۵۵. آیا مطابق با خط‌مشی کنترل دسترسی تعریف شده، دسترسی کاربران و کارکنان پشتیبانی کننده به اطلاعات و کارکردهای سیستم کاربردی، محدود می‌شود؟		

۷. کنترل دسترسی	بلی	خیر
۵۶. آیا برای فعالیتهای کار از راه دور، خط‌مشی، طرحهای عملیاتی و روشهای اجرایی، ایجاد و پیاده‌سازی می‌شوند؟		
۵۷. آیا از آی‌پی اختصاصی برای دسترسی به سرویس دهنده استفاده می‌شود؟		
۵۸. آیا از پروتکلهای امن دارای مجوز برای ورود به محیط مدیریت سایت و سرور استفاده می‌شود؟		
۵۹. آیا پورتهای استاندارد و شناخته شده به منظور امنیت انتقال اطلاعات بر روی سرور، با پورتهای دیگر جایگزین شده‌اند؟		

۸. تهیه، توسعه و نگهداری سیستمهای اطلاعاتی	بلی	خیر
۶۰. آیا به منظور تشخیص هر نوع خرابی اطلاعات ناشی از خطاهای پردازشی یا اقدامهای عمدی، در برنامه‌های کاربردی، بررسیهایی صورت می‌پذیرد؟		
۶۱. آیا برای حفاظت از اطلاعات، یک خط‌مشی استفاده از کنترلهای رمزنگاری، ایجاد و پیاده‌سازی شده است؟		
۶۲. آیا به منظور پشتیبانی استفاده سازمان از فنون رمزنگاری، یک سیستم مدیریت کلید ایجاد شده است؟		
۶۳. آیا به منظور کنترل نصب نرم‌افزار بر روی سیستمهای عملیاتی و سرویس دهنده‌ها، روشهای اجرایی ایجاد شده است؟		
۶۴. آیا دسترسی به کد منبع برنامه (source)، محدود شده است؟		
۶۵. آیا توسعهٔ نرم‌افزارهای برون سپاری شده توسط سازمان، نظارت و پایش می‌شود؟		

۹ . مدیریت حوادث امنیت اطلاعات	بلی	خیر
۶۶. آیا رویدادهای امنیت اطلاعات در کوتاه‌ترین زمان ممکن، از طریق مجاری مدیریتی مناسب گزارش می‌شود؟		

۹ . مدیریت حوادث امنیت اطلاعات	بلی	خیر
۶۷. آیا تمامی کارکنان، پیمانکاران و کاربران شخص ثالث سیستمها و خدمات اطلاعاتی، نسبت به یادداشت و گزارش‌دهی هر ضعف امنیتی مشاهده شده یا مورد سوء ظن در سیستمها یا خدمات، ملزم شده‌اند؟		
۶۸. آیا به منظور حصول اطمینان از یک پاسخ سریع، مؤثر و منظم به حوادث امنیت اطلاعات، مسئولیتهای مدیریتی و روشهای اجرایی ایجاد شده است؟		
۶۹. آیا برای اینکه نوع، حجم و هزینه‌های حوادث امنیتی، قابل اندازه‌گیری و پایش باشند، ساز و کارهای لازم ایجاد شده است؟		
۷۰. آیا هنگامی که پیگرد علیه یک فرد یا سازمان، پس از یک حادثه امنیت اطلاعات، منجر به اقدام قانونی (اعم از مدنی یا جنایی) می‌شود، شواهد منطبق با قواعد اقامهٔ شواهد در حوزه (ها)ی قضایی مرتبط، گردآوری، نگهداری و ارائه می‌شوند؟		
۷۱. آیا آپتایم سرورها به صورت مستمر کنترل و بازبینی می‌شوند؟		

۱۰. مدیریت تداوم کسب و کار	بلی	خیر
۷۲. آیا وقایعی که می‌توانند موجب وقفه در فرایندهای کسب و کار شوند، با توجه به احتمال بروز و آسیب ناشی از چنین وقفه‌هایی و پیامدهای آنها بر امنیت اطلاعات شناسایی می‌شوند؟		
۷۳. آیا در پی ایجاد وقفه یا بروز نقص در فرایندهای کار، به منظور نگهداری یا از سرگیری عملیات و اطمینان از دسترس‌پذیری اطلاعات در سطح و مقیاسهای زمانی مورد نیاز، طرحهایی ایجاد و پیاده‌سازی می‌شوند؟		

۱۱. انطباق	بلی	خیر
۷۴. آیا سوابق مهم، با توجه به مقررات، الزامهای آئین نامه‌ای، قراردادی و کسب و کار، در برابر گم شدن، تخریب و تحریف، محافظت می‌شوند؟		
۷۵. آیا حفاظت داده‌ها و حریم خصوصی آن‌گونه که در قوانین و آئین‌نامه‌های		

۱۱. انطباق	بلی	خیر
مرتبط، و در صورت قابلیت اعمال، شرایط قراردادی، الزام شده، تضمین می‌شود؟		
۷۶. آیا کاربران از به کارگیری امکانات پردازش اطلاعات برای مقاصد غیرمجاز بازداشته می‌شوند؟		
۷۷. آیا کنترلهای رمزنگاری در انطباق با تمامی توافقنامه‌ها، قوانین و آئین‌نامه‌های مرتبط، به کار گرفته می‌شود؟		
۷۸. آیا برای حصول انطباق با خط‌مشی‌ها و استانداردهای امنیتی، مدیران از اینکه تمامی روشهای اجرایی امنیتی، در حیطه مسئولیت‌شان، به درستی اجرا می‌شوند، اطمینان حاصل می‌نمایند؟		
۷۹. آیا به منظور انطباق با استانداردهای پیاده‌سازی امنیت، سیستمهای اطلاعاتی به طور منظم بررسی می‌شود؟		