ارزشیابی وضعیت عملکرد مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران بر اساس استاندارد بین‌المللی ایزو/ آی.ای.سی.

میلا ملک‌الکلامی*

کارشناسی ارشد ،
کتابداری و اطلاع‌رسانی

دریافت: ۱۳۹۰/۱۱/۰۵ | پذیرش: ۱۳۹۱/۰۷/۱۶

فصلنامهٔ علمی پژوهشی
پژوهشنامهٔ پردازش و مدیریت اطلاعات
پژوهشگاه علوم و فنّاوری اطلاعات ایران
شاپا(چاپی) ۸۲۲۳- ۲۲۵۱
شاپا(الکترونیکی) ۸۲۳۱- ۲۲۵۱
نمایه در LISA، SCOPUS و ISC
http://jipm.irandoc.ac.ir
دوره ۲۸ | شمارهٔ ۴ | ص ص ۹۱۶- ۸۹۵
تابستان ۱۳۹۲

نوع مقاله: پژوهشی

چکیده: پژوهش حاضر با هدف ارزیابی وضعیت عملکرد مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران بر اساس استاندارد ایزو/آی.ای.سی. ۲۷۰۰۲انجام شده است.روش پژوهش توصیفی – پیمایشی است و به منظور گردآوری اطلاعات از پرسشنامه استاندارد شامل ۱۱ شاخص و ۳۹ مؤلفه، استفاده شده است. جامعه آماری پژوهش تعداد ۷۴ نفر از مدیران اصلی و میانی شاغل کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران بر اساس آخرین فهرست موجود در پایگاه وزارت علوم، تحقیقات و فناوری بوده است. تجزیه و تحلیل داده‌ها از طریق هر دو نوع آمار توصیفی و استنباطی با استفاده از نرم‌افزار مایکروسافت اکسل ۲۰۰۷ و نرم‌افزارآماری اس. پی. اس. اس صورت گرفته است. نتایج حاصل از پژوهش نشان می‌دهد که در کتابخانه‌های مورد پژوهش، میانگین رعایت استاندارد ایزو/ آی. ای. سی. ۲۷۰۰۲ در شاخص‌هایسیاست‌های امنیتی (۳/۹۱) ، مدیریت امنیت اطلاعات سازمان(۴/۲۳)، مدیریت امنیت اموال سازمان (۴/۳۸)، مدیریت امنیت منابع انسانی(۴)، مدیریت امنیت فیزیکی و محیطی(۴/۰۷)، مدیریت امنیت عملیات و ارتباطات (۴/۱۵)، مدیریت کنترل دسترسی به اطلاعات (۴/۳۸)، مدیریت اکتساب، توسعه، حفظ و نگهداری نظام‌های اطلاعاتی (۳/۹۲)، مدیریت بحران امنیت اطلاعات (۳/۸۴)، مدیریت استمرار کسب و کار (۳/۴۶)، ومدیریت تطابق (۳/۶۹) است. بر اساس جدول ارزشیابی، میانگین تمام شاخص‌های استاندارد در وضعیت مطلوب قرار دارد. نتایج پژوهش حاکی از آن است که به‌طور کلی کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران از لحاظ مدیریت امنیت اطلاعات در شرایط مطلوبی قرار دارند و با اطمینان ۹۵٪ می‌توان گفت میانگین مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران بر اساس استاندارد ایزو آی. ای. سی. ۲۷۰۰۲ برابر با ۴ و بالاتر از حد متوسط است و در سطح مطلوبی قرار دارد. همچنین، بین کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران از لحاظ مدیریت امنیت اطلاعات تفاوت معنی‌داری وجود ندارد.

کلیدواژه‌ها: مدیریت، امنیت اطلاعات، استاندارد ایزو/ آی. ای. سی. ۲۷۰۰۲، کتابخانه‌های مرکزی، دانشگاه‌های دولتی، کتابخانه‌های دانشگاهی، تهران

*Mila_malek_1365@yahoo.com

۱. مقدمه

سیر پیشرفت فناوری اطلاعات و ارتباطات و نوآوری‌های حاصل از آن موجب افزایش چشمگیر بهره‌وری و پیدایش انواع جدیدی از کالاها و خدمات شده است. در جهان امروز، پردازش اطلاعات ارزان و هزینه‌های ارتباطات رو به کاهش است، اما فراهم شدن امکانات فنی جدید نه تنها باعث پیدایش محصولات نوین و راه‌های بهتر و کارآمدتر برای انجام امور نشده، بلکه در کنار آن امکان سوء استفاده از فناوری را نیز افزایش داده است (میردامادی ۱۳۸۸، ۳۰).

در چنین فضایی اعمال غیرقانونی و مخرب آن قدر سریع صورت می‌گیرد که می‌تواند غیرقابل شناسایی باشد، هرچند شناسایی آن غیر ممکن نیست. حفاظت از اطلاعات از مهم‌ترین جنبه‌های جهان امروز است. از بالاترین سطح اطلاعات مربوط به دولت و امنیت ملی، تا سطح اطلاعات موجود در شرکت‌های خصوصی، تجاری یا داده‌های شخصی، همه تحت تهدید مداوم و خطر هستند (Sulaiman 2009, 585). بیشتر نظام‌های اطلاعاتی به خودی خود ایمن نیستند و اعمال راه‌حل‌های فنی فقط بخشی از یک راه‌حل کلی امنیت اطلاعات است (مشکلانی ۱۳۸۶).

بیش از یک سوم نقص‌های امنیتی نظام‌های رایانه‌ای در انگلیس ناشی از کارمندان و یک سوم از بدترین حوادث ایمنی ناشی از ویروس‌های رایانه‌ای بوده است(Lonney 2002). همچنین آمار نشان می‌دهد که سازمان‌ها منابع هنگفتی را بابت از دست دادن اطلاعات یا دردسترس نبودن آنها می‌پردازند. در سال ۲۰۰۴ ویروس‌ها و کرم‌های رایانه‌ای بیش از دو میلیارد دلار هزینه به سازمان‌ها و افراد تحمیل کرده است (جعفری ۱۳۸۷).

رشد فزاینده حجم و نوع داده‌های ذخیره شده و کلیدی‌تر شدن نقش آنها در تصمیم‌گیری‌ها، سبب شده تا ضرورت حفاظت داده‌ها برای همه مدیران توجیه‌پذیر شده باشد.

نقش داده و اطلاعات در مدیریت سازمان‌ها، نقش حیاتی و اساسی دارد.هرچه فضای اطلاعاتی یک سازمان دقیق‌تر، منسجم‌تر و نظام‌مندتر باشد، سازمان بهتر می‌تواند به اهدافش نایل آید(توکلی ۱۳۸۸، ۷۵). سازمان‌هایی که موجودیت‌شان به طور عمومی به فناوری اطلاعات وابسته است باید از تمامی ابزارهای ممکن برای محافظت از اطلاعات استفاده کنند(امیرخانی ۱۳۸۸، ۷۵).

بهره‌وری در مراکز اطلاع‌رسانی نتیجه استفاده بهینه و مؤثر از منابع اطلاعاتی و بهبود کیفیت ارائه خدمات و ارتقای رضایت کاربران، دلپذیری در محیط کار و افزایش انگیزه و علاقه کارکنان به کار بهتر است که در نهایت، رشد و توسعه مراکز اطلاع‌رسانی را به دنبال خواهد داشت (بصیریان جهرمی ۱۳۸۸، ۱۲۰).

۲. بیان مسأله

وجود ضعف امنیتی در شبکه‌های کامپیوتری و اطلاعاتی، عدم آموزش و توجیه صحیح تمامی کاربران صرف نظر از مسئولیت شغلی آنان نسبت به جایگاه و اهمیت امنیت اطلاعات، عدم وجود دستورکارهای لازم برای پیشگیری از نقائص امنیتی، عدم وجود سیاست مشخص و مدرن به منظور برخورد مناسب و به موقع با اشکالات امنیتی، مسائلی را به دنبال خواهد داشت که ضرر آن متوجه تمامی سازمان‌ها و کاربران کامپیوتر در یک کشور شده و عملاً زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می‌دهند. این امر در شبکه کامپیوتری کتابخانه‌ها نیز قابل توجه است. نیاز روزافزون به استفاده از فناوری‌های نوین در عرصه اطلاعات و ارتباطات و ضرورت امنیت آن، استقرار یک نظام مدیریت امنیت اطلاعات را در تمام سازمان‌ها بیش از پیش آشکار می‌نماید (پورمند ۱۳۸۵، ۲۰-۲۵).

با پیشرفت فناوری اطلاعات و همچنین به وجود آمدن ابزارهای جدید، نفوذ به یک نظام کامپیوتری، شکستن قفل امنیتی نرم‌افزارها یا مهندسی معکوس برنامه‌های رایانه و همچنین وجود صدها مشکل ناخواسته در طراحی نرم‌افزارهای مختلف و روال‌های امنیتی سازمان‌ها، همیشه خطر حمله و دسترسی افراد غیرمجاز وجود دارد. همچنین، ورود این فناوری‌های جدید به کتابخانه‌ها، ارائه اطلاعات مورد نیاز به مراجعه‌کنندگان و توجه به داده‌ها و اطلاعات موجود در کتابخانه بیش از پیش مورد توجه قرار گرفته است.کتابخانه به عنوان سازمانی برای ذخیره و بازیابی اطلاعات مورد نیاز کاربران، نقش مهمی را در برآوردن نیاز اطلاعاتی آنها ایفا می‌کند(برقعی ۱۳۸۷).

هنگامی که مدیران و کارمندان موضوع امنیت فناوری اطلاعات را مد نظر قرار می‌دهند- چه در کتابخانه‌های بزرگ و چه در کتابخانه‌های کوچک- همواره با مسائل مشابهی مواجه می‌شوند. هر گروه برای داده‌های خود نیاز به سطح معینی از امنیت و رویه‌های شفاف و ساده برای به اجرا در آوردن توسط کارکنان، توانایی ایجاد و حفظ آگاهی از نیازهای مراجعه‌کنندگان و درکی از چگونگی پیاده‌سازی سیاست‌های امنیتی در یک محیط دارند. این کتابخانه‌ها به دلیل حجم زیاد اطلاعات و هزینه‌ای که صرف تهیه و دسترسی آن می‌کنند، باید در خصوص حفاظت اطلاعات خود به خصوص پایگاه‌های اطلاعاتی و یا هرگونه منابع الکترونیکی و دیجیتالی تلاش و دقت بیشتری داشته باشند. در عصر کنونی، یعنی عصر اطلاعات، ارائه و استفاده به موقع از اطلاعات شرط اولیه موفقیت افراد و جوامع بشری محسوب می‌شود. با توجه به هزینه‌های گزافی که صرف تهیه این منابع و پایگاه‌های اطلاعاتی می‌شود،

حفظ و نگهداری از اطلاعات از جنبه های مهم و حیاتی کتابخانه‌های دانشگاهی است. این امر میسر نخواهد شد جز با استفاده از ابزارها و فنون صحیح امنیتی و در ادامه آن، دانش به‌روز شده جهت مقابله با مجموعه تهدیداتی که این بستر حیاتی ارتباطی را به مخاطره می‌اندازد.

بیشتر سازمان‌ها در معرض انواع تهدیدات داخلی و خارجی خرابکاران هستند؛ تهدیداتی چون دستکاری اطلاعات مرجع و یا سرقت اطلاعات حیاتی و سرمایه‌های اطلاعاتی. در چنین شرایطی، عواملی که می‌توانند از مزایای نظام‌ها به شمار روند (مثل سرعت و قابلیت دسترسی بالا)، اگر تحت کنترل نباشند ممکن است باعث آسیب‌پذیری شوند و سوء استفاده افراد بدنیت از آنها به نفوذ و خرابکاری، کلاهبرداری، و یا اخاذی بیانجامد. علاوه بر این، مشکلات طبیعی و خطاهای غیرعمدی که توسط کاربران رایانه‌ای رخ می‌دهد، درصورت فقدان روال صحیح برای حفاظت از اطلاعات می‌تواند نتایج مخربی به‌بارآورد (میردامادی ۱۳۸۸، ۲۴).

در سال‌های اخیر نظام‌های اطلاعاتی در مورد این تهدیدهای الکترونیکی بیشتر آسیب‌پذیر شده‌اند. این امر به دلیل متصل بودن کامپیوترها به یکدیگر و دسترس‌پذیر بودن کامپیوترها برای تعداد زیادی کاربر است. علاوه بر این، در نتیجه افزایش تعداد افرادی که مهارت کامپیوتری دارند، اخلال‌هایی مثل فنون هک کردن از طریق اینترنت روز به روز گسترده‌تر می‌شوند (کریمی ۱۳۸۵، ۳).

در این میان،کتابخانه‌های دانشگاهی به دلیل نوع خاص مراجعه‌کنندگان، تبادل و انتقال اطلاعات به کاربران خود از اهمیت ویژه‌ای برخوردارند. این گروه از کتابخانه ها با توجه به موضوعات تدریس شده در دانشگاه و مراجعه کنندگان کتابخانه، نوع خاصی از منابع و پایگاه‌های اطلاعاتی ویژه را ارائه می‌کنند که به نوبه خود در توسعه دانش فردی و به تبع آن، در افزایش سطح آگاهی جامعه خود تأثیر بسزایی دارند.

۳. تعاریف عملیاتی

- **امنیت**به مجموعه‌ای از تدابیر، روش‌ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام‌های رایانه‌ای و ارتباطی اطلاق می‌شود(ذاکرالحسینی ۱۳۸۶، ۲۸).
- **امنیت اطلاعات**طبق تعریف ایزو/ آی. ای. سی.۲۷۰۰۲ (استاندارد ایزو/ کمیسیون بین‌المللی الکتروتکنیک ۲۷۰۰۲)[1]، امنیت اطلاعات به منظور تضمین سه اصل زیر مورد نیاز است:

1. International Standard for Organization / International Electrotechnical Commission 27002

* محرمانگی: اطمینان از اینکه منابع فقط برای افراد مجاز سازمان در دسترس هستند.
* یکپارچگی: تأمین دقت لازم و کامل بودن منابع و داده‌ها و روش‌های پردازش آنها.
* دسترس‌پذیری: اطمینان از این‌که افراد مجاز در تمامی زمان‌های تعیین شده، به منابع و داده‌ها و سرمایه‌های موجود دسترسی داشته باشند.

- **مدیریت امنیت اطلاعات :** مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت و بررسی موانع سر راه رسیدن به این اهداف و ارائه راهکارهای لازم را برعهده دارد.در این پژوهش، منظور از مدیریت امنیت اطلاعات، اجرای استاندارد ایزو/ آی.ای.سی. ۲۷۰۰۲ است.
- **ایزو/ آی.ای.سی. ۲۷۰۰۲:**ایزو/ آی. ای. سی. ۲۷۰۰۲ (ویرایش دوم ایزو/ آی.ای.سی ۲۷۰۰۱) یک استاندارد بین‌المللی شناخته شده برای مدیریت امنیت اطلاعات است. این استاندارد به طور مستقیم از استاندارد انگلیسی مدیریت امنیت اطلاعات ۷۷۹۹ (بی. اس. ۷۷۹۹) متعلق به مؤسسه استاندارد انگلستان گرفته شده است.ایزو/ آی. ای. سی. ۲۷۰۰۲ یک استاندارد سطح بالا است که برای نظام‌های تجاری گوناگون قابل پیاده‌سازی است. در واقع، ویژگی‌های این استاندارد سبب می‌شود که در سازمان‌های مختلف و در زمینه‌های کاربردی مختلف قابل پیاده‌سازی باشد.

هدف از تدوین این استاندارد، برقرار کردن خطوط راهنما و اصول کلی برای راه‌اندازی، پیاده‌سازی، نگهداری و توسعه مدیریت امنیت اطلاعات در یک سازمان است.

اهداف کنترلی و کنترل‌های این استاندارد برای برآورده ساختن الزامات شناسایی داده شده به وسیله ارزیابی خطر، پیاده‌سازی می‌شوند. این استاندارد ممکن است به عنوان رهنمود پیاده‌سازی برای توسعه استانداردهای امنیت سازمانی، تجارب مدیریت امنیت اثربخش و کمک به ایجاد اطمینان در فعالیت‌های درون سازمانی به کار رود.

استاندارد ایزو/ آی.ای.سی ۲۷۰۰۲ منابع و داده‌های هر سازمان را به عنوان سرمایه‌های آن سازمان در نظر می‌گیرد. هدف نظام مدیریت امنیت اطلاعات حفاظت از این سرمایه‌هاست تا با این کار بتوان استمرار کسب و کار را تضمین نمود، آسیب‌پذیری آن را به کمترین حد رسانید، و بازگشت سرمایه را به بالاترین مرز ممکن خود نزدیک کرد.

امنیت اطلاعات می‌تواند نیازهای تجارت را در سه ضلعی محرمانگی، یکپارچگی و دسترس‌پذیری برطرف سازد. در نظام مدیریت امنیت اطلاعات، برخلاف نظام‌های سنتی، به منظور تشخیص و جلوگیری از مواجهه با چالش‌های امنیتی و بازیابی داده‌های آسیب دیده به

حالت اولیه خود، بهترین الگوها و مناسب‌ترین راهنمایی‌ها پس از انجام ارزیابی‌های مختلف در دسترس هستند. ایزو/ آی. ای. سی. ۲۷۰۰۲مبنایی را برای ایمن‌سازی سرمایه‌های سازمانی و روش‌هایی را برای مدیریت فرایند امنیت اطلاعات ارائه می‌نماید.

ایزو/ آی. ای. سی. ۲۷۰۰۲ برای سازمان‌ها مزایای زیر را به ارمغان می‌آورد:

* برخورداری از یک روش‌شناسی سازمان‌یافته بین‌المللی برای مدیریت امنیت اطلاعات.
* داشتن فرایندهای مشخص برای ارزیابی، اجرا، نگهداری، و مدیریت امنیت اطلاعات.
* برخورداری از مجموعه سیاست‌ها، استانداردها، روال‌ها، و رهنمون‌های مناسب (مؤسسه استاندارد و تحقیقات صنعتی ایران ۱۳۸۷، ۲).

این استاندارد دارای کنترل‌های امنیتی در ۱۱ دامنه بسیار جامع است که این۱۱ دامنه مبنای ارزیابی مخاطرات امنیتی و گسترش امنیت در نظر گرفته می‌شوند. دامنه‌های اشاره شده عبارت‌اند از:

۱)سیاست‌های امنیتی[1]، ۲)ساختار مدیریت امنیت اطلاعات[2]، ۳)مدیریت امنیت اموال سازمان[3]، ۴)مدیریت امنیت منابع انسانی[4]، ۵)مدیریت امنیت فیزیکی و محیطی[5]، ۶)مدیریت عملیات و ارتباطات[6]، ۷)کنترل‌های دسترسی[7]، ۸)اکتساب، توسعه، حفظ و نگهداری نظام‌های اطلاعاتی[8]، ۹)مدیریت بحران امنیت اطلاعات[9]،۱۰)مدیریت استمرار کسب و کار[10]،۱۱)تطابق[11] (مؤسسه استاندارد و تحقیقات صنعتی ایران۱۳۸۷، ۵) .

٤. هدف پژوهش

هدف از این پژوهش، ارزیابی وضعیت عملکرد مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران بر اساس ۱۱ شاخص استاندارد ایزو/ آی. ای. سی. ۲۷۰۰۲ است.

٥. پرسش‌های پژوهش

از این رو،پژوهش بر آن است تا برای نیل به این هدف و فرضیه‌های بیان شده به پرسش‌های زیر پاسخ داده دهد:

---

1. security policy
2. organization of information security
3. asset management
4. human resource security
5. physical & environmental security
6. operation management &communications
7. access controls
8. information system acquisition, development and maintenance
9. information security incident management
10. business continuity management
11. compliance

۱) عملکرد کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران در زمینه سیاست مدیریت امنیت اطلاعات بر اساس استاندارد ایزو/ آی. ای. سی. ۲۷۰۰۲ چگونه است؟
۲) عملکرد کتابخانه‌های مورد پژوهش در زمینه ساختار امنیت اطلاعات بر اساس استاندارد چگونه است؟
۳) عملکرد کتابخانه‌های مورد پژوهش در زمینه مدیریت امنیت اموال سازمان بر اساس استاندارد چگونه است؟
۴) عملکرد کتابخانه‌های مورد پژوهش در زمینه امنیت منابع انسانی سازمان بر اساس استاندارد چگونه است؟
۵) عملکرد کتابخانه‌های مورد پژوهش در زمینه امنیت فیزیکی و محیطی سازمان بر اساس استاندارد چگونه است؟
۶) عملکرد کتابخانه‌های مورد پژوهش در زمینه مدیریت عملیات و ارتباطات بر اساس استاندارد چگونه است؟
۷) عملکرد کتابخانه‌های مورد پژوهش در زمینه کنترل های دسترسی بر اساس استاندارد چگونه است؟
۸) عملکرد کتابخانه‌های مورد پژوهش در زمینه اکتساب، توسعه، حفظ و نگهداری نظام‌های اطلاعاتی سازمان بر اساس استاندارد چگونه است؟
۹) عملکرد کتابخانه‌های مورد پژوهش در زمینه مدیریت بحران امنیت اطلاعات سازمان بر اساس استاندارد چگونه است؟
۱۰) عملکرد کتابخانه‌های مورد پژوهش در زمینه استمرار کسب و کار بر اساس استاندارد چگونه است؟
۱۱) عملکرد کتابخانه‌های مورد پژوهش در زمینه تطابق سازمان بر اساس استاندارد چگونه است؟

٦. فرضیه پژوهش

۱) میانگین نمره عملکرد مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران بر اساس استاندارد ایزو/ آی. ای. سی. ۲۷۰۰۲ بالاتر از حد متوسط است.
۲) بین عملکرد کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران از نظر مدیریت امنیت اطلاعات تفاوت معنی‌داری وجود دارد.

۷. پیشینه‌ها

بیشتر پژوهش‌های داخلی مسائل مربوط به مبادله امن و صحیح داده‌ها و حفاظت از محیط شبکه را مورد مطالعه و بررسی قرار داده‌اند و اظهار داشته‌اند مدل‌های امنیتی (عبداللهی ازگمی ۱۳۷۵) و مدل او. اس. آی. (محضب ۱۳۷۳) نتایج مثبت و موفقی داشته است. در رابطه با افزایش مقاومت عوامل امنیتی شبکه‌ها، یک معماری برای نظام‌های تشخیص نفوذ پیشنهاد شده است که با امکانات موجود، قابل اجرا در شبکه‌های امروزی است (تاج الدینی اشکفتکی ۱۳۸۳).

به کارگیری مدل رمزنگاری در داده‌ها (قانع ۱۳۷۴) و همچنین اطلاعات در تصویر امنیت لازم برای شبکه‌ها و اطلاعات را تضمین می‌کند (نادعلیان مارنانی ۱۳۸۳). همچنین، در حفظ امنیت در شبکه از فنون امضای کور استفاده شده است که نه تنها نتیجه موفقی در رابطه با حفظ اطلاعات شخصی کاربر از دید دیگران و حتی پایگاه دارد، بلکه خدمت مورد نظر بدون کمترین تقلیل در کیفیت دریافت می‌شود(عاشوری تلوکی ۱۳۸۶).

با مطالعه نقش عوامل انسانی در امنیت نظام‌های اطلاعاتی، به عنوان یکی از مؤلفه‌های مهم ایجاد امنیت در نظام، متغیرهایی مانند آموزش، فرهنگ و مهارت امنیتی و خودباوری های افراد به عنوان عوامل اثرگذار معرفی شده‌اند (طاهری ۱۳۸۶) و عوامل مؤثر بر تهدیدات امنیتی فیزیکی و محیطی اطلاعات نشان‌دهنده این بوده است که ۴ عامل کنترل محیطی و مدیریت دسترسی، مدیریت تسهیلات فیزیکی، حفاظت از مرکز داده و کنترل کارکنان در اولویت هستند و اندازه سازمان بر میزان اهمیت آنها تأثیرگذار است (جعفری ۱۳۸۷). نرم‌افزار نظام خبره با زبان پرولوگ با هدف پیاده‌سازی نظام مدیریت امنیت اطلاعات (پاکدامن ۱۳۸۸) و مدل سرمایه‌گذاری بر اساس ۴ مفهوم سرمایه‌گذاری، موفقیت در حمله، انگیزه حمله، و احتمال تهدید برای جلوگیری از آسیب‌پذیری اطلاعات مطرح و مورد استفاده موفقی قرار گرفت (جاوید فومنی مقدم ۱۳۸۸).استقرار نظام مدیریت امنیت اطلاعات در سازمان‌های دولتی بر اساس استاندارد بی. اس. ۷۷۹۹ نشان‌دهنده اهمیت پیاده‌سازی سیاست کنترلی مشخص برای افراد سازمان و حفاظت از اطلاعات سازمان است (صالحیان ۱۳۸۸). همچنین، در رابطه با این پژوهش، عوامل کلیدی موفقیت در اجرای مدیریت امنیت اطلاعات شناسایی و مورد تأیید قرار گرفت (میرانوری ۱۳۸۸). خامدا (۱۳۸۳) برای اولین بار به بررسی وضعیت مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی دولتی شهر تهران بر اساس استاندارد ایزو ۱۷۷۹۹ پرداخته شده است. این پژوهش نشان‌دهنده وضعیت بسیار ضعیف مدیریت امنیت اطلاعات در مؤسسه‌های شهر تهران در مقایسه با شاخص‌های استاندارد بین المللی ایزو است.

پژوهش‌هایی که خارج از کشور انجام شده‌اند ، نشان می‌دهند که سازمان‌های مختلف در انگلستان در سال ۲۰۰۰، فقط ۲۷ درصد دارای سیاست امنیت اطلاعات بوده‌اند (Stacey 2000). در سال ۲۰۰۱، ۹۰ درصد از سازمان‌ها حوادث امنیتی را تجربه کرده‌اند (Ho and Murry 2002). شرکت‌های انگلیسی با توجه به این که یک سوم نقص‌های امنیتی نظام‌های رایانه‌های انگلیس ناشی از کارمندان است(Looney 2002)، به این نتیجه رسیدند که به منظور پیاده‌سازی یک ظرفیت امنیتی مؤثر، سازمان‌ها نیاز به تعیین ضعیف‌ترین نقاط سازمانی خود دارند (Rizzo 2002). بیشترین حوادث امنیتی از هجونویسان با ۴۲ درصد و حمله به نظام‌ها از طریق کدهای مخرب ۴۱ درصد است (Sulaiman 2009). بر اساس تجربیات موفق گذشته، در دسترس بودن اسناد، محدودیت‌های هزینه، یادگیری سازمان و فرهنگ سازمانی، انگیزه‌های مهم برای پیاده‌سازی نظام مدیریت امنیت اطلاعات هستند (Yuan Ku 2009). پیشینه‌های بیان شده نشان‌دهنده سیر تکاملی توجه و گسترش حوزه موضوعی امنیت اطلاعات در سطح جهان است. پژوهش‌ها از بررسی استانداردها و خط‌مشی‌های امنیت اطلاعات و مقایسه عملکرد استانداردها (Siponen 2009)، آغاز شده و به بررسی مدیریت امنیت اطلاعات در سازمان‌های کشورها رسیده است.

بررسی پژوهش‌های در ارتباط با مدیریت امنیت اطلاعات حاکی از آن است که این خدمت نوظهور به صورت گسترده‌ای در سازمان‌ها مورد استفاده قرار می‌گیرد. در کشوری که می‌تواند به درستی ادعا کند که از هزاران سال پیش مهد علم و دانش، کتاب و کتابخانه بوده است، امروزه با توجه به وسعت بی‌سابقه و سرعت روزافزون دانش‌ها و هنرهای بشر در سطح جهانی و ظهور فناوری‌های نوین باید توقع داشت که کتابخانه‌ها به عنوان جایگاهی برای انتقال صحیح، سریع و مناسب اطلاعات و اندوخته‌های علمی گذشته و حال در به ثمر رساندن بسیاری از تحولات مطلوب اجتماعی، علمی و فرهنگی نقش مؤثری ایفا کنند. موفقیت در این امر نیازمند انجام پژوهش‌های جامع و بررسی یافته‌ها و ایجاد زمینه‌ای مناسب برای اجرای استانداردی مناسب در حفظ و نگهداری این دارایی‌های ارزشمند است.

در ایران، این موضوع به دلیل جدید بودن به صورت حرفه‌ای و کامل نه تنها در کتابخانه‌ها بلکه در سازمان‌های تخصصی و دولتی متفاوت نیز مورد پژوهش و بررسی قرار نگرفته است. در نتیجه درمی‌یابیم که، تاکنون هیچ پژوهشی به منظور بررسی وضعیت مدیریت امنیت اطلاعات در کتابخانه‌های ایران بر اساس آخرین استاندارد انجام نشده است. همچنین، نکته دیگری که لزوم انجام این پژوهش را می‌طلبد، این است که گسترش روزافزون و تحولات سریعی که در

حوزه علم اطلاع‌رسانی رخ می‌دهد، نیازمند بررسی دقیق وضعیت مدیریت امنیت اطلاعات در مراکز اطلاع‌رسانی و کتابخانه‌ها به عنوان پایگاه‌هایی برای حفظ ونگهداری اطلاعات مورد نیاز کاربران است. نتایج به‌دست آمده از این پژوهش شاید بتواند در سیاست‌گذاری و برنامه‌ریزی مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاهی مؤثر باشد. در واقع، این پژوهش نشان خواهد داد که کتابخانه‌های دانشگاهی با صرف هزینه‌ای بالا برای تهیه اطلاعات خود، تا چه حدی از آن حفاظت و نگهداری می‌کنند.

۸. روش‌شناسی پژوهش

روش پژوهش توصیفی – پیمایشی است. داده‌های پژوهش حاضر، از طریق پرسشنامه محقق‌ساخته بر اساس استاندارد ایزو/ آی. ای. سی. ۲۷۰۰۲ شامل ۱۱ شاخص اصلی و مشتمل بر ۳۹ مؤلفه فرعی جمع‌آوری شده است. جامعه آماری این پژوهش ۷۴ نفر از مدیران اصلی و میانی ۱۳ کتابخانه مرکزی دانشگاه‌های دولتی مستقر در شهر تهران (الزهرا، شهید رجایی، شهید بهشتی، شاهد، علامه طباطبایی، پیام نور، علم و صنعت، صنعتی شریف، صنعتی امیرکبیر، خواجه نصیر طوسی، تهران، تربیت مدرس، و تربیت معلم) است. دانشگاه‌های پیام نور و علمی کاربردی به ترتیب به دلیل نداشتن بخش مناسب جهت پاسخگویی و نداشتن کتابخانه از جامعه حذف گردیدند. با توجه به محدود بودن جامعه آماری، نمونه‌گیری انجام نشد. تجزیه و تحلیل داده‌ها با استفاده از آمار توصیفی، استنباطی و نرم‌افزار اس. پی. اس. اس. انجام شد.

۹. یافته‌های پژوهش

۹-۱. عملکرد جامعه مورد پژوهش در زمینه سیاست مدیریت امنیت اطلاعات

جدول ۱. نمرات مدیریت سیاست‌های امنیتی به تفکیک دانشگاه‌ها در جامعه پژوهش

شاخص	شاهد	تربیت معلم	علم و صنعت ایران	علامه طباطبایی	الزهرا	تهران	هنر	صنعتی شریف	شهید رجایی	شهید بهشتی	خواجه نصیرالدین طوسی	تربیت مدرس	صنعتی امیرکبیر
سیاست مدیریت امنیت اطلاعات	۴	۴	۴	۴	۵	۴	۱	۴	۴	۴	۴	۵	۴

این شاخص دارای یک مؤلفه با عنوان سیاست‌های مدیریت امنیت است. میانگین این شاخص ۳/۹۱ به‌دست آمده که در پیوستار ارزیابی (نامطلوب، به نسبت مطلوب، و مطلوب) در سطح مطلوب قرار گرفته است. همچنین، در بین کتابخانه‌ها بیشترین و کمترین میانگین به ترتیب مربوط به دانشگاه‌های تربیت مدرس ۵ و هنر ۱ است.

۹-۲. عملکرد جامعه مورد پژوهش در زمینه ساختار امنیت اطلاعات

جدول ۲. میانگین نمرات ساختار مدیریت امنیت اطلاعات به تفکیک دانشگاه‌ها در جامعه پژوهش

شاخص	شاهد	تربیت معلم	علم و صنعت ایران	علامه طباطبایی	الزهرا	تهران	هنر	صنعتی شریف	شهید رجایی	شهید بهشتی	خواجه نصیرالدین طوسی	تربیت مدرس	صنعتی امیرکبیر
ساختار مدیریت امنیت اطلاعات	۴	۵	۳	۴	۵	۴	۴	۳	۴	۴	۵	۵	۵

این شاخص دارای دو مؤلفه با عنوان‌های ایجاد امنیت داخل سازمان و ایجاد امنیت خارج سازمان است. میانگین این شاخص ۴/۲۳ به‌دست آمده که در پیوستار ارزیابی در سطح مطلوب قرار گرفته است. همچنین، در بین کتابخانه‌ها بیشترین و کمترین میانگین به ترتیب مربوط به دانشگاه‌های تربیت مدرس، امیرکبیر، خواجه نصیرالدین طوسی و تربیت معلم ۵ و علم و صنعت و صنعتی شریف ۳ است.

۹-۳. عملکرد جامعه مورد پژوهش در زمینه مدیریت امنیت اموال سازمان

جدول ۳. بررسی شاخص مدیریت امنیت اموال سازمان در جامعه پژوهش

شاخص	شاهد	تربیت معلم	علم و صنعت ایران	علامه طباطبایی	الزهرا	تهران	هنر	صنعتی شریف	شهید رجایی	شهید بهشتی	خواجه نصیرالدین طوسی	تربیت مدرس	صنعتی امیرکبیر
مدیریت امنیت اموال سازمان	۴	۵	۴	۴	۴	۴	۴	۵	۴	۵	۵	۴	۵

این شاخص دارای دو مؤلفه با عنوان‌های حفظ و کنترل دارایی‌های سازمان واستفاده از یک نظام رده‌بندی و طبقه‌بندی است. میانگین این شاخص ۴/۳۸ به‌دست آمده که در پیوستار ارزیابی در سطح مطلوب قرار گرفته است. همچنین، در بین کتابخانه‌ها بیشترین و کمترین میانگین به ترتیب مربوط به دانشگاه‌های شهید بهشتی، امیرکبیر، خواجه نصیرالدین طوسی، و تربیت معلم برابر با ۵ و با اختلاف کمی، شاهد، علامه طباطبایی، الزهرا، هنر، شهید رجایی، تربیت مدرس، علم و صنعت، و صنعتی شریف برابر با ۴ است.

۹-٤. عملکرد جامعه مورد پژوهش در زمینه امنیت منابع انسانی سازمان

جدول ٤. بررسی شاخص مدیریت امنیت منابع انسانی سازمان در جامعه پژوهش

شاخص	شاهد	تربیت معلم	علم و صنعت ایران	علامه طباطبایی	الزهرا	تهران	هنر	صنعتی شریف	شهید رجایی	شهید بهشتی	خواجه نصیرالدین طوسی	تربیت مدرس	صنعتی امیرکبیر
مدیریت امنیت منابع انسانی سازمان	۴	۵	۳	۳	۳	۳	۴	۴	۴	۵	۵	۴	۵

شاخص امنیت منابع انسانی شامل ۳ مؤلفه تأکید بر اهمیت امنیت پیش از اشتغال افراد، تأکید بر امنیت در حین خدمت، و تأکید بر امنیت در خاتمه یا تغییر شغل است. نتایج نشان می دهد که میانگین مؤلفه مدیریت امنیت منابع انسانی سازمانبرابر با ۴ است که در پیوستار ارزیابی، در سطح مطلوب قرار گرفته است.

میانگین مربوط به دانشگاه‌های تربیت معلم، شهید بهشتی، خواجه نصیرالدین طوسی و صنعتی امیرکبیر برابر ۵ و علم و صنعت ایران، علامه طباطبایی، تهران و الزهرا برابر با ۳ است که به ترتیب بیشترین و کمترین میزان این شاخص را در بین دانشگاه‌ها دارا هستند.

۹-۵. عملکرد جامعه مورد پژوهش در زمینه امنیت فیزیکی و محیطی سازمان

جدول ۵. بررسی شاخص مدیریت امنیت فیزیکی و محیطی سازمان در جامعه پژوهش

شاخص	شاهد	تربیت معلم	علم و صنعت ایران	علامه طباطبایی	الزهرا	تهران	هنر	صنعتی شریف	شهید رجایی	شهید بهشتی	خواجه نصیرالدین طوسی	تربیت مدرس	صنعتی امیرکبیر
فیزیکی و محیطی سازمان	۴	۵	۴	۴	۳	۳	۴	۴	۴	۴	۵	۴	۵

شاخص مدیریت امنیت فیزیکی و محیطی شامل دو مؤلفه فرعی استفاده از نواحی ایمن به‌منظور حفظ تسهیلات و مؤلفه حفظ و نگهداری تجهیزات سازمان است. میانگین شاخص مدیریت امنیت فیزیکی و محیطی برابر با ۴/۰۷ است که در پیوستار ارزیابی سطح مطلوب قرار گرفته است.

میانگین مربوط به دانشگاه های تربیت معلم، خواجه نصیرالدین طوسی و صنعتی امیرکبیر برابر ۵، الزهرا و تهران برابر با ۳ است که به ترتیب بیشترین و کمترین میزان در بین دانشگاه‌ها را دارا هستند.

۹-٦. عملکرد جامعه مورد پژوهش در زمینه مدیریت عملیات و ارتباطات

جدول ٦. بررسی شاخص مدیریت عملیات و ارتباطات سازمان در جامعه پژوهش

شاخص	شاهد	تربیت معلم	علم و صنعت ایران	علامه طباطبایی	الزهرا	تهران	هنر	صنعتی شریف	شهید رجایی	شهید بهشتی	خواجه نصیرالدین طوسی	تربیت مدرس	صنعتی امیرکبیر
مدیریت عملیات و ارتباطات	۵	۵	۳	۴	۴	۴	۴	۳	۴	۴	۵	۴	۵

شاخص مدیریت عملیات و ارتباطات شامل ۱۰ مؤلفه فرعی ایجاد روش‌های اجرایی عملیاتی و مسئولیت‌ها، مؤلفه مدیریت تحویل خدمات به شخص ثالث، برنامه‌ریزی و پذیرش نظام، حفاظت در برابر کدهای مخرب و غیرمجاز، تعیین دستورکارهایی به منظور تهیه نسخه پشتیبان از اطلاعات، مدیریت امنیت شبکه‌های کامپیوتری، فرعی اداره کردن محیط‌های ذخیره‌سازی،کنترل تبادل اطلاعات، حفاظت از خدمات تجارت الکترونیک و بازبینی از نظام‌ها و تسهیلات پردازش اطلاعات (پایش) است.

میانگین شاخص مدیریت عملیات و ارتباطات برابر با ۴/۱۵ است که در پیوستار ارزیابی در سطح مطلوب قرار گرفته است.

میانگین مربوط به دانشگاه‌های شاهد، تربیت معلم، خواجه نصیرالدین طوسی، و صنعتی امیرکبیر برابر ۵ و علم و صنعت ایران و صنعتی شریف برابر با ۳ است که به ترتیب بیشترین و کمترین میزان در بین دانشگاه‌های مورد مطالعه را دارا هستند.

۹-۷. عملکرد جامعه مورد پژوهش در زمینه کنترل‌های دسترسی

جدول ۷. بررسی شاخص مدیریت کنترل‌های دسترسی سازمان در جامعه پژوهش

شاخص	شاهد	تربیت معلم	علم و صنعت ایران	علامه طباطبایی	الزهرا	تهران	هنر	صنعتی شریف	شهید رجایی	شهید بهشتی	خواجه نصیرالدین طوسی	تربیت مدرس	صنعتی امیرکبیر
مدیریت کنترل‌های دسترسی	۵	۵	۳	۴	۴	۴	۴	۳	۵	۵	۵	۵	۵

شاخص هفتم یعنی مدیریت کنترل دسترسی به اطلاعات شامل ۷ مؤلفه فرعی کنترل دسترسی به اطلاعات، مدیریت دسترسی کاربر به اطلاعات، توسعه روش‌های دسترسی مناسب، کنترل دسترسی به خدمات شبکه،کنترل دسترسی به نظام عامل، کنترل دسترسی به برنامه‌های کاربردی و اطلاعات و حفاظت از تسهیلات سیار و کار از راه دور است.

میانگین شاخص مدیریت کنترل دسترسی به اطلاعات برابر با ۴/۳۸ است که در پیوستار ارزیابی در سطح مطلوب قرار گرفته است.

میانگین مربوط به دانشگاه های شاهد، تربیت معلم، شهید رجایی ، شهید بهشتی، خواجه نصیرالدین طوسی، تربیت مدرس، و صنعتی امیرکبیر برابر ۵ و دانشگاه‌های علم و صنعت ایران و صنعتی شریف برابر با ۳ است که به ترتیب بیشترین و کمترین میزان در بین دانشگاه‌های مورد مطالعه را دارا هستند.

۹-۸. عملکرد جامعه مورد پژوهش در زمینه اکتساب، توسعه و نگهداری نظام‌های اطلاعاتی سازمان

جدول ۸. بررسی شاخص مدیریت اکتساب، توسعه و نگهداری نظام‌های اطلاعاتی سازمان در جامعه پژوهش

شاخص	شاهد	تربیت معلم	علم و صنعت ایران	علامه طباطبایی	الزهرا	تهران	هنر	صنعتی شریف	شهید رجایی	شهید بهشتی	خواجه نصیرالدین طوسی	تربیت مدرس	صنعتی امیرکبیر
مدیریت اکتساب، توسعه و نگهداری نظام‌های اطلاعاتی	۵	۵	۵	۴	۴	۴	۲	۳	۴	۴	۵	۵	۱

شاخص هشتم، مدیریت اکتساب، توسعه، حفظ و نگهداری نظام‌های اطلاعاتی سازمان شامل ۶ مؤلفه فرعی شناسایی الزامات امنیتی مورد نیاز نظام‌های اطلاعاتی، پردازش صحیح در برنامه‌های کاربردی، استفاده از کنترل‌های رمزنگاری در حفاظت اطلاعات، حفاظت و کنترل از فایل‌های نظام سازمان، امنیت در فرآیندهای بهبود و پشتیبانی و مدیریت آسیب‌پذیری است.

میانگین شاخص مدیریت اکتساب، توسعه، حفظ و نگهداری نظام‌های اطلاعاتی برابر با ۳/۹۲ است که در پیوستار ارزیابی، در سطح مطلوب قرار گرفته است.

میانگین مربوط به دانشگاه‌های شاهد، تربیت معلم، علم و صنعت ایران، خواجه نصیرالدین طوسی و تربیت مدرس برابر ۵ و صنعتی امیرکبیر ۲ است که به ترتیب بیشترین و کمترین میزان در بین دانشگاه‌های مورد مطالعه را دارا هستند.

۹-۹. عملکرد جامعه مورد پژوهش در زمینه مدیریت بحران امنیت اطلاعات سازمان

جدول ۹. بررسی شاخص مدیریت بحران امنیت اطلاعات سازمان در جامعه پژوهش

شاخص	شاهد	تربیت معلم	علم و صنعت ایران	علامه طباطبایی	الزهرا	تهران	هنر	صنعتی شریف	شهید رجایی	شهید بهشتی	خواجه نصیرالدین طوسی	تربیت مدرس	صنعتی امیرکبیر
مدیریت بحران امنیت اطلاعات	۵	۵	۳	۳	۳	۴	۴	۲	۳	۴	۴	۵	۵

شاخص مدیریت بحران امنیت اطلاعات سازمان شامل ۲ مؤلفه فرعی گزارش‌دهی وقایع و ضعف‌های امنیتی اطلاعات مدیریت و مؤلفه فرعی بحران‌های امنیتی اطلاعات و بهسازی آنهاست.

میانگین شاخص مدیریت بحران امنیت اطلاعات برابر با ۳/۸۴ است که در پیوستار ارزیابی، در سطح مطلوب قرار گرفته است.

میانگین مربوط به دانشگاه‌های شاهد، تربیت معلم، تربیت مدرس و صنعتی امیرکبیر برابر ۵ و صنعتی شریف برابر با ۲ است که به ترتیب بیشترین و کمترین میزان در بین دانشگاه‌های مورد مطالعه را دارا هستند.

۹-۱۰. عملکرد جامعه مورد پژوهش در زمینه استمرار کسب و کار

جدول ۱۰. بررسی شاخص مدیریت استمرار کسب و کار سازمان در جامعه پژوهش

شاخص	شاهد	تربیت معلم	علم و صنعت ایران	علامه طباطبایی	الزهرا	تهران	هنر	صنعتی شریف	شهید رجایی	شهید بهشتی	خواجه نصیرالدین طوسی	تربیت مدرس	صنعتی امیرکبیر
مدیریت استمرار کسب و کار	۵	۵	۲	۳	۳	۳	۳	۲	۴	۳	۵	۵	۲

شاخص مدیریت استمرار کسب و کار شامل ۱ مؤلفه فرعی استفاده از مدیریت استمرار به منظور حفاظت از اطلاعات است. میانگین شاخص مدیریت استمرار کسب و کار برابر با ۳/۴ است که در پیوستار ارزیابی در سطح به نسبت مطلوب قرار گرفته است.

میانگین مربوط به دانشگاه‌های شاهد، تربیت معلم، تربیت مدرس، خواجه نصیرالدین طوسی و صنعتی امیرکبیر برابر ۵ و علم و صنعت و صنعتی شریف برابر با ۲ است که به ترتیب بیشترین و کمترین میزان در بین دانشگاه‌ها را دارا هستند.

۹-۱۱. عملکرد جامعه مورد پژوهش در زمینه تطابق سازمان

جدول ۱۱. بررسی شاخص مدیریت تطابق سازمان در جامعه پژوهش

شاخص	شاهد	تربیت معلم	علم و صنعت ایران	علامه طباطبایی	الزهرا	تهران	هنر	صنعتی شریف	شهید رجایی	شهید بهشتی	خواجه نصیرالدین طوسی	تربیت مدرس	صنعتی امیرکبیر
مدیریت تطابق	۵	۵	۲	۲	۳	۴	۴	۱	۴	۳	۵	۵	۵

شاخص مدیریت تطابق شامل ۳ مؤلفه فرعی مطابقت با الزامات قانونی، انطباق با خط‌مشی‌ها و استانداردهای امنیتی و انطباق فنی است.

میانگین شاخص مدیریت تطابق برابر با ۳/۶۹۶ است که در پیوستار ارزیابی در سطح مطلوب قرار گرفته است.

میانگین مربوط به دانشگاه‌های شاهد، تربیت معلم، تربیت مدرس، خواجه نصیرالدین

طوسی و صنعتی امیرکبیر برابر ۵ و صنعتی شریف برابر با ۱ است که به ترتیب بیشترین و کمترین میزان در بین دانشگاه‌های مورد مطالعه را دارا هستند.

۱۰. نتیجه‌گیری

میانگین نمره عملکرد مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران بر اساس استاندارد ایزو/ آی. ای. سی. ۲۷۰۰۲ بالاتر از حد متوسط است.

بیشترین میانگین مربوط به شاخص سوم، یعنی مدیریت امنیت اموال سازمان برابر با ۴/۳۸، و کمترین میانگین مربوط شاخص دهم، یعنی مدیریت استمرار کسب و کار برابر با ۳/۴۶ است. برای فرضیه شماره ۱ پژوهش مربوط به رتبه‌بندی شاخص‌های عملکرد کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران از آزمون فریدمن استفاده شد. در نتیجه فرضیه ۱ با اطمینان ۹۵٪ تأیید می‌شود.

جدول ۱۲. آزمون فریدمن برای بررسی رتبه‌های شاخص‌های یازده‌گانه مدیریت امنیت اطلاعات در جامعه پژوهش

آماره‌ها / ابعاد	میانگین	میانگین رتبه	تعداد	درجه آزادی	مجذور کای	سطح معنی‌داری
شاخص اول: مدیریت سیاست‌های امنیتی	۳/۹۱	۵/۰۴	۱۳	۱۰	۵۶/۴۱۵	۰/۰۰
شاخص دوم: مدیریت امنیت اطلاعات سازمان	۴/۲۳	۶/۱۲				
شاخص سوم: مدیریت امنیت اموال سازمان	۴/۳۸	۶/۵				
شاخص چهارم: مدیریت امنیت منابع انسانی	۴	۵				
شاخص پنجم: مدیریت امنیت فیزیکی و محیطی	۴/۰۷	۵/۳۵				
شاخص ششم: مدیریت امنیت عملیات و ارتباطات	۴/۱۵	۵/۸۸				
شاخص هفتم: مدیریت کنترل دسترسی به اطلاعات	۴/۳۸	۶/۹۶				
شاخص هشتم: اکتساب، توسعه، حفظ و نگهداری نظام های اطلاعاتی	۳/۹۲	۵/۸۵				
شاخص نهم: مدیریت بحران امنیت اطلاعات	۳/۸۴	۴/۵۸				
شاخص دهم: مدیریت استمرار کسب و کار	۳/۴۶	۳/۷۳				
شاخص یازدهم: مدیریت تطابق	۳/۶۹	۱۱				

در فرضیه ۲، همان‌گونه که ملاحظه می‌شود، عملکرد کتابخانه‌های مرکزی دانشگاه‌های تربیت معلم و خواجه نصیرالدین طوسی بر اساس استاندارد ایزو/ آی. ای. سی. ۲۷۰۰۲ دارای وضعیت بهتری نسبت به بقیه دانشگاه‌ها است. از این لحاظ، دانشگاه شریف و دانشگاه علم و صنعت به نسبت بقیه دانشگاه‌ها در وضعیت نامناسبتری قرار دارند.

نتایج نشان می‌دهد که دانشگاه‌های شاهد (۹۰/۸ درصد)، تربیت معلم (۹۸ درصد)، علم و صنعت ایران (۶۵/۴ درصد)، علامه طباطبایی (۷۰/۸ درصد)، الزهرا (۷۴/۴ درصد)، تهران (۷۴/۴ درصد)، هنر (۶۹ درصد)، صنعتی شریف (۶۱/۸ درصد)، شهید رجایی (۹۶ درصد)، شهید بهشتی (۸۱/۸ درصد)، خواجه نصیرالدین طوسی (۹۶ درصد)، تربیت مدرس (۹۲ درصد)، امیرکبیر (۸۲ درصد) مدیریت امنیت اطلاعات را بر اساس استاندارد ایزو/ آی.ای. سی. ۲۷۰۰۲ رعایت می‌کنند.

برای رتبه‌بندی عملکرد کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران و تعیین تفاوت بین آنها از آزمون کروسکال-والیس که با آزمون F متناظر است، استفاده شد.

جدول ۱۳. آزمون کروسکال والیس جهت بررسی معنی‌داری تفاوت بین رتبه‌های دانشگاه‌های مورد مطالعه برای مدیریت امنیت اطلاعات

خی دو	درجه آزادی	سطح معنی‌داری
۱۷	۱۲	۰/۶۵۲

مطابق جدول ۱۳، آزمون کروسکال- والیس نشان می‌دهد که بین دانشگاه‌های دولتی مستقر در شهر تهران در زمینه عملکرد کتابخانه‌های مرکزی شان تفاوت معنی‌داری وجود ندارد و در نتیجه فرضیه دوم رد می شود.

از آنجا که پژوهش‌هایی در این زمینه در کتابخانه‌های ایران انجام نشده است، می‌توان نتیجه این پژوهش را با نتایج پژوهش خامدا (۱۳۸۳) مقایسه کرد. نتایج این پژوهش با نتایج پژوهش خامدا (۱۳۸۳) که خط‌مشی امنیت اطلاعات بر اساس استاندارد ایزو آی. ای. سی. ۱۷۷۹۹ را در کتابخانه‌های پژوهشی دولتی شهر تهران نشان می‌دهد متفاوت است. در پژوهش نام‌برده شاخص اول با ۷۱/۴ درصد گزینه خیلی کم را نشان می‌دهد که نشان‌دهنده ضعیف بودن مؤسسه‌های پژوهشی دولتی شهر تهران نسبت به تهیه و تدوین سیاست امنیت اطلاعات است.

در ارزیابی وضعیت مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی دولتی شهر تهران،

شاخص دوم با ۳ مؤلفه زیرساخت امنیت اطلاعات، امنیت دسترسی شخص ثالث، و واگذاری‌ها در وضعیت ضعیف و نامطلوبی قرار دارد.شاخص سوم با ۲ مؤلفه مسئولیت اموال و رده‌بندی اموال اطلاعاتی در وضعیت خوبی قرار دارد که این نتیجه آماری متأثر از عملکرد خوب مؤسسه‌های پژوهشی از نظر مسئولیت اموال بوده است. شاخص چهارم با ۳ مؤلفه امنیت در شرح وظایف، آموزش کاربر و مسئولیت حوادث امنیتی در وضعیت ضعیفی قرار داشته‌اند.

شاخص پنجم با ۳ مؤلفه نواحی ایمن، امنیت تجهیزات و امنیت فیزیکی و محیطی در وضعیت خوبی قرار داشته‌اند که البته این نتیجه آماری بیشتر متأثر از عملکرد خوب مؤسسه‌های پژوهشی از نظر امنیت تجهیزات بوده است. شاخص ششم با ۷ مؤلفه رویه‌ها و وظایف اجرایی، برنامه‌ریزی و پذیرش نظام، حافظت در برابر نرم‌افزارهای خرابکار، اداره نظام (پشتیبانی)، مدیریت شبکه، امنیت و مدیریت رسانه و تبادل اطلاعات و نرم‌افزار ضعیف عمل شده است، این مقدار از نظر آماری به قدری نیست که بتوان این ادعا را تأیید کرد. در واقع می‌توان گفت که مؤلفه‌های سوم تا ششم موفقیت‌آمیز بوده‌اند.

شاخص هفتم با ۸ مؤلفه مقررات اداری کنترل دسترسی، مدیریت دسترسی کاربر، وظایف کاربر، کنترل دسترسی به شبکه، کنترل دسترسی به نظام عامل، کنترل دسترسی به برنامه‌های کاربردی، نظارت بر دسترسی و استفاده از نظام و تسهیلات سیار و کار از راه دور در سطح ضعیفی قرار داشته‌اند. نتایج نشان می‌دهد اگر چه اقداماتی در زمینه کنترل دسترسی صورت گرفته است، اما به احتمال، این اقدامات اصولی نبوده و بر حسب نیاز، مقررات و اقداماتی اعمال شده است.

شاخص هشتم با ۵ مؤلفه الزامات امنیتی نظام‌ها، امنیت در نظام‌های کاربردی، کنترل‌های رمزنگار، امنیت فایل‌های نظامی و امنیت در فرایندهای توسعه و پشتیبانی در وضعیت ضعیفی قرار داشته‌اند. شاید یکی از دلایل این امر را بتوان عدم نیاز به توسعه نظام‌ها در شرایط آن زمان دانست. در واقع، آن زمان در نخستین مراحل شکل‌گیری مدیریت اطلاعات در مؤسسه‌های اشاره شده بوده‌ایم. در ارزیابی وضعیت مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی دولتی شهر تهران (خامدا ۱۳۸۳) این شاخص وجود ندارد و مقایسه ممکن نیست. شاخص نهم با ۲ مؤلفه جنبه‌های مدیریتی و تداوم امنیتی با شاخص دهم استاندارد ۲۷۰۰۲ مورد استفاده در این پژوهش مقایسه می‌شود. این مقایسه نشان می‌دهد که عملکرد مؤسسه‌های پژوهشی در زمینه مدیریت تداوم عملیاتی ضعیف بوده است.

شاخص دهم با ۳ مؤلفه هماهنگی با قوانین امنیت، نظارت بر سیاست امنیت، و قوانین فنی، ملاحظات حسابرسی نظام در سطح ضعیفی قرار داشته است. با مقایسه‌ای اجمالی می‌توان نتیجه

گرفت اگر چه مؤسسه‌های بیان شده در کنترل حوادث امنیتی موفق بوده‌اند، اما نتایج تحلیلی آزمون همچنان بیانگر آن است که اقدام جدی نیز دراین زمینه صورت نگرفته بوده است (خامدا ۱۳۸۳).

نتایج پژوهش سطح مطلوبی از مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران را نشان می‌دهد. با این وجود، هنوز در برخی شاخص‌ها، نظیر مدیریت استمرار کسب وکار، یعنی شاخص دهم استاندارد ایزو/ آی. ای. سی. ۲۷۰۰۲ ضعیف‌تر عمل شده است. بنابراین، در ارتباط با فعالیت‌هایی که مربوط به این شاخص هستند پیشنهاد زیر ارائه می‌شود:

- توصیه می‌شود روش‌های اجرایی عملیات، به شکل مدون، نگهداری شوند و در دسترس تمام کاربرانی قرار گیرند که به آنها نیاز دارند. روش‌های اجرایی مستند برای فعالیت‌های نظام در رابطه با تجهیزات پردازش اطلاعات و ارتباطات نظیر رویه‌های روشن و خاموش کردن یارانه‌ها، تهیه فایل پشتیبان، نگهداری از تجهیزات، کار با محیط‌های ذخیره‌سازی اطلاعات، کنترل کار با رایانه‌ها و اتاق رایانه و ایمنی تهیه شود.
- توصیه می‌شود نظام‌های عملیات و نرم‌افزارها از نظر تغییرات تحت مدیریت کنترل کارآمد قرار گیرند.
- پیشنهاد می‌شود به منظور کاهش فرصت‌های دستکاری غیرعمد یا غیرمجاز، یا استفاده نابجا از دارایی‌های سازمان، وظایف و حدود اختیارات تفکیک شوند.
- توصیه می‌شود امکانات مربوط به نظام‌های در حال توسعه، تحت آزمایش و عملیات، به منظور کاهش خطر ناشی از دسترسی غیرمجاز یا تغییرات در نظام‌های عملیاتی، تفکیک شوند.
- پیشنهاد می‌شود استفاده از منابع پایش و تنظیم شده و ظرفیت مورد نیاز در آینده به گونه‌ای پیش‌بینی شود که از کارایی مورد نیاز نظام، اطمینان حاصل شود.

برای نیل به اهداف امنیتی در سازمان‌ها نیز پیشنهاداتی برای پژوهش‌های آینده بیان می‌شوند. از جمله:

۱) کشف و شناسایی منشاء حوادث امنیتی در سازمان‌ها
۲) کشف انگیزه‌های نفوذ به نظام‌های اطلاعاتی در ایران
۳) برآورد خسارت‌های مالی ناشی از وقوع حوادث امنیتی اطلاعات در سطح ملی

۱۱. منابع

امیرخانی، امیرحسین. ۱۳۸۸.مشاوره و پیاده‌سازی نظام مدیریت امنیت اطلاعات. *ماهنامه عصر فناوری اطلاعات* ۵۱ (۲): ۷۵-۷۸.

برقعی، محمدرضا. ۱۳۸۷.سامانه مدیریت امنیت اطلاعات ISMS چیست. http://news.tavanir.org.ir (دسترسی در ۸۹/۳/۱۰).

بصیریان جهرمی، رضا. ۱۳۸۸.مدیریت اطلاعات: مفاهیم و کاربردها. *فصلنامه علمی پژوهشی علوم و فناوری اطلاعات* ۲۴ (۳): ۱۱۷-۱۳۶.

پاکدامن، راضیه. ۱۳۸۸. چارچوب پیاده‌سازی نظام مدیریت امنیت اطلاعات (ISMS) دربخش فناوری اطلاعات در سازمان‌ها و ارائه نظام خبره (مشاور)آن.پایان نامه کارشناسی ارشد علوم انسانی. *دانشکده اقتصاد و علوم اجتماعی، دانشگاه تربیت مدرس.*

پورمند، علی. ۱۳۸۵. مدیریت نظام‌های امنیتی. *تدبیر* (۱۸۹) ۱۸: ۲۵.

تاج الدین اشکفتکی، آمنه.۱۳۸۳. افزایش مقاومت عوامل امنیتی شبکه‌های کامپیوتری. پایان‌نامه کارشناسی ارشد نرم افزار. دانشگاه تربیت مدرس.

توکلی، جمیله، ۱۳۸۸. چالش‌های امنیت اطلاعات در سازمان‌ها. *فصلنامه علمی پژوهشی علوم و فناوری* دسترسی (دسترسی در ۸۹/۵/۱۲).www.magiran.ir *اطلاعات* (۳) ۲۴.

جاودانی، تقی. ۱۳۸۰. امنیت در سرورهای وب. پایان‌نامه کارشناسی ارشد کامپیوتر-نرم‌افزار. دانشکده فنی مهندسی. دانشگاه اصفهان.

جاوید فومنی مقدم، محمود. ۱۳۸۸. ارائه مدل سرمایه‌گذاری در امنیت اطلاعات-مورد مطالعه-ضد هرزنامه. پایان‌نامه کارشناسی ارشد فنی و مهندسی. دانشکده فنی، دانشگاه تربیت مدرس.

جعفری، عزیزالله. ۱۳۸۷.شناسایی و رتبه‌بندی عوامل و شاخص‌های کلیدی مؤثر بر مدیریت تهدیدات امنیت فیزیکی محیطی اطلاعات http://www.civilica.com/Paper-ICTM05-ICTM05_055.html (دسترسی در۸۹/۱۲/۱۵).

جعفری، نیما. ۱۳۸۷.نظام مدیریت امنیت اطلاعات از طرح تا اصلاح.

http://vista.ir/?view=context&id=306376 (دسترسی در ۸۹/۱۲/۱۲).

خامدا، زهرا.۱۳۸۳. ارزیابی وضعیت مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی دولتی شهر تهران بر اساس استاندارد ایزو ۱۷۷۹۹. پایان‌نامه کارشناسی ارشد کتابداری و اطلاع‌رسانی، دانشگاه تهران.

ذاکرالحسینی، علی. ۱۳۸۶. *امنیت داده‌ها*. تهران: نص.

صالحیان، مهران. ۱۳۸۸. بررسی استقرار نظام مدیریت امنیت اطلاعات در دستگاه‌های دولتی. پایان‌نامه کارشناسی ارشد تجارت الکترونیک. پژوهشکده برق و کامپیوتر، دانشگاه شیراز.

طاهری، مهدی. ۱۳۸۶. ارائه چهارچوبی برای نقش عوامل انسانی در امنیت نظام‌های اطلاعاتی. پایان‌نامه کارشناسی ارشد مدیریت فناوری اطلاعات. دانشکده علوم انسانی، دانشگاه تربیت مدرس.

عاشوری تلوکی، مائده. ۱۳۸۶. احراز امنیت پایگاه داده متحرک در برابر تهدید تعیین موقعیت با استفاده از امضای کور.پایان‌نامه کارشناسی ارشد کامپیوتر نرم‌افزار. دانشکده فنی مهندسی، دانشگاه اصفهان.

عبداللهی ازگمی، محمد، ۱۳۷۵. طراحی و پیاده‌سازی سرویس‌های امن برای شبکه‌های کامپیوتری. پایان‌نامه کارشناسی ارشد، دانشگاه صنعتی شریف.

قانع، محمد. ۱۳۷۴. *رمزنگاری و مکانیسم‌های امنیتی در شبکه‌های کامپیوتری*. پایان‌نامه کارشناسی ارشد، دانشگاه تهران. www.irandoc.ir (دسترسی در ۸۹/۳/۱۰).

کریمی، زهرا. ۱۳۸۵. ارائه مدل مفهومی ارزیابی ریسک امنیت اطلاعات، مورد بانک سپه. پایان‌نامه کارشناسی ارشد. دانشگاه الزهرا، دانشکده فنی و مهندسی.

محضب، محمود. ۱۳۷۳. *ایمنی ارتباطات در شبکه‌های کامپیوتری*. پایان‌نامه کارشناسی ارشد برق، دانشگاه تربیت مدرس. www.irandoc.ir (دسترسی در ۸۹/۳/۱۰).

مشکلانی، نازنین.۱۳۸۶. امنیت شبکه و اطلاعات. وب‌سایت تخصصی مدیران شبکه http://netadmins.ir (دسترسی در۸۹/۲/۲۵).

مؤسسه استاندارد و تحقیقات صنعتی ایران. ۱۳۸۷. فناوری اطلاعات- فنون امنیتی- آئین کار مدیریت امنیت اطلاعات.

میرانوری، علی رضا. ۱۳۸۸. شناسایی و اولویت‌بندی عوامل کلیدی موفقیت (CSFs) در اجرای نظام مدیریت امنیت اطلاعات (ISMS) در سازمان‌های ایرانی. پایان‌نامه کارشناسی ارشد علوم انسانی. دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهراء علیها السلام.

میردامادی، مهدی. ۱۳۸۸. ضرورت توجه به امنیت اطلاعات: پیش درآمدی بر مباحث امنیت. *ماهنامه تحلیلگران عصر اطلاعات* (۶) ۳۱:۲۴.

نادعلیان مارنانی، اعظم. ۱۳۸۳. بررسی امنیت شیوه‌های پنهان نگاری اطلاعات در تصویر و ارائه یک شیوه مناسب. پایان‌نامه کارشناسی ارشد کامپیوتر. دانشکده فنی مهندسی، دانشگاه اصفهان.

Ho, simon, and Rob, Murry. 2002. Safeguarding information assets at financial institutions: ISO 17799, at sourced managed security services and syber insurance. www.camtos.com. (accessed 14 Mar. 2010).

Lonney, Matt. 2002. Your worst security threat: employees?.ZDNet(uk). www.zdnet.com (accessed12 Mar. 2010).

Phelps, Daniel C. 2005. Information system security: self efficacy and security effectiveness in floride libraries. theflorida state university college of information. www.proquest.com (accessed 12 Mar. 2010).

Rizzo, F,2002. Kpmg global security survey 2002: a south African perspective. http://csweb.rau.ac.za (accessed 12 Mar. 2010).

Siponen, Mikko T. 2009. Information security management: problems & solutions. *Information &Management* 46 (5): 267-270.

Stacey, Timothy. 2000. Standardization of information security: BS 7799. SANS institute www.rr.sans.org (accessed 12 Mar. 2010).

Sulaiman, Ainin. 2009. Information security landscape and maturity level: case study of Malaysian Public service organization (MPS). *Government Information Quarterly* (4) 26: 584-593.

Yuan Ku, Cheng 2009.National security information policy and its Implementation: A case study in Taiwan. *Telecommunications Policy* 33 (7):371-384.

Evaluation of the central libraries information security management at governmental universities located in Tehran, according to the international standard ISO/IEC 27002

Iranian Journal of Information Processing & Management

Mila Malekolkalami*
Master in Library and Information Science

Iranian Research Institute
For Science and Technology
ISSN 2251-8223
eISSN 2251-8231
Indexed in LISA, SCOPUS & ISC
Vol.28 | No.4 | pp: 895-916
summer 2013

Abstract: This study assessed the evaluation of information security management status in central Libraries of governmental universities located in Tehran, according to ISO / I.E.C. 27002. Research method applied for the study is descriptive Survey and a questionnaire was used for collecting information. The questionnaire was distributed between the 74 central library managers of governmental universities in Tehran according to the recent list on the website of Ministry of Science, Research and Technology, that includes 39 components based on 11 indicators of the standard ISO/ I.E.C. 27002. Analysis of data has been done by using both descriptive and inferential statistics by Microsoft Excel 2007and SPSS statistical softwares. The results of research showed that the mean for libraries in 11 indexes are as follows: The mean for the first index, Security policy, is 3.91 , in the second index, organization of information security, is 4.23, in the third index, asset security management, is 4.38, in the fourth index, Human Resources Security management, is 4, in the fifth index, physical and environment Security management, is 4.07, in the sixth index, operations management and communications, is 4.15, in the Seventh index, access controls management, is 4.38, in the eighth index, information system acquisition, development and maintenance, is 3.92, in the ninth index, information security incident management, is 3.84, in the tenth index, business continuity management, is 3.46, in the eleventh index, compliance, is 3.69 that match with the standard ISO / IEC. 27002. The results of Research shown that totally mean for standard ISO/I.E.C. 27002 in the field of information security management in the central libraries, is 4 being in a good condition and there is no significant differences between the performance of the Central libraries of the governmental Universities in Tehran, since It is not observed significant difference between them in the field of information security management according to ISO IEC. 27002.

Keyword: management, information security, ISO/ I.E.C. 27002, central libraries, governmental universities, Tehran (city)

*Corresponding author: Mila_malek_1365@yahoo.com