

شناسایی عوامل مؤثر بر مدیریت امنیت اطلاعات کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاه علوم پزشکی همدان

معصومه امینی^۱ حسین وکیلی مفرد*^۲ محمد کریم صابری^۳

تاریخ دریافت ۱۳۹۸/۵/۴ تاریخ پذیرش ۱۳۹۸/۹/۱۷

چکیده

هدف: پژوهش حاضر باهدف شناسایی عوامل مؤثر بر مدیریت امنیت اطلاعات کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاه علوم پزشکی همدان انجام گرفت.

روش: این مطالعه با رویکرد کمی و روش پیمایشی تحلیلی صورت گرفته است. جامعه آماری این پژوهش تمام مدیران و کتابداران کتابخانه‌های دانشگاه علوم پزشکی همدان در سال ۱۳۹۷ بودند. در این پژوهش از پرسشنامه محقق ساخته بهره گرفته شد. سنجش روایی محتوایی پرسشنامه با محاسبه ضریب نسبت روایی (CVR) و شاخص روایی محتوایی (CVI) انجام گردید. جهت سنجش پایایی کلی پرسشنامه از ضریب آلفای کرونباخ استفاده شد. نرمال بودن متغیرهای مورد مطالعه توسط آزمون کولموگروف-اسمیرنوف تک نمونه‌ای بررسی شد. همچنین برای بررسی فرضیه‌ها و رتبه‌بندی از آزمون تی تک نمونه‌ای و آزمون فریدمن استفاده شد.

یافته‌ها: بر اساس نتایج مطالعه، سازه اجرایی با میانگین ۴/۴۶ در رتبه اول و با بیشترین اثرگذاری در سیستم مدیریت امنیت اطلاعات و سازه نیروی انسانی با میانگین ۳/۵۶ در رتبه هفتم و با کمترین اثرگذاری شناسایی شد. برای ارتقاء سطح امنیت اطلاعات ضروری است که مدیران ارشد با مشخص نمودن اهداف امنیتی مرتبط با سازمان، ایجاد مدیریتی جامع و یکپارچه، تلاش برای رعایت قوانین و استانداردهای امنیتی، در دست داشتن منابع و بودجه کافی و ایجاد انگیزه در بین کتابداران و اطلاع‌رسانان، بستر مناسبی را فراهم آورند تا ارائه خدمات مطلوب تر گردد و همچنین بتوانند گامی مؤثر در جهت افزایش تولیدات علمی دانشگاهی داشته باشند.

اصالت اثر: این مقاله حاصل یک پژوهش کاربردی بوده و پیش از این در هیچ مجله دیگری به چاپ نرسیده است.

واژه‌های کلیدی: مدیریت اطلاعات، امنیت اطلاعات، کتابخانه‌ها و مراکز اطلاع‌رسانی.

^۱ دانشجوی کارشناسی ارشد، کتابداری و اطلاع‌رسانی پزشکی، مرکز پژوهش دانشجویان، دانشگاه علوم پزشکی همدان، همدان،

ایران.. ایمیل: M.amini9274@gmail.com

^۲ استادیار، کتابداری و اطلاع‌رسانی پزشکی، گروه کتابداری و اطلاع‌رسانی پزشکی، دانشکده پیراپزشکی، دانشگاه علوم پزشکی

همدان، همدان، ایران ایمیل: Wakili_hn@yahoo.com

^۳ استادیار، کتابداری و اطلاع‌رسانی پزشکی، گروه کتابداری و اطلاع‌رسانی پزشکی، دانشکده پیراپزشکی، دانشگاه علوم پزشکی

همدان، همدان، ایران.. ایمیل: mohamadsaberi@gmail.com

مقدمه

با پیشرفت فناوری و ورود فناوری‌های جدید، کتابخانه‌ها و مراکز اطلاع‌رسانی به‌عنوان سازمانی برای ذخیره و بازیابی اطلاعات مورد نیاز کاربران، نقش مهمی را در برآوردن نیازهای اطلاعاتی آن‌ها ایفا می‌کنند. علاوه بر این در کتابخانه‌ها و مراکز اطلاع‌رسانی حجم وسیعی از اطلاعات (علمی، آموزشی، پژوهشی، دیجیتالی و...) وجود دارد که بسیاری از فعالیت‌های علمی و پژوهشی و طرح‌های تحقیقاتی بر مبنای این اطلاعات حاصل می‌شود بنابراین اهمیت وجود این اطلاعات دوچندان می‌باشد. کتابخانه‌ها و مراکز اطلاع‌رسانی اصولاً منابع حفظ سرمایه‌های فرهنگی، علمی و تاریخی یک ملت هستند که به‌صورت مجموعه‌ای سازمان‌یافته برای دانش‌پژوهان تکامل می‌یابند (تاج‌الدینی و سادات موسوی، ۱۳۸۹). لزوم پرداختن به مسائل امنیتی در کتابخانه‌ها و مراکز اطلاع‌رسانی نه به دلیل ایجاد محدودیت برای کاربران، بلکه کمکی بزرگ به کاربران کتابخانه است. در واقع بدین وسیله، امکان مناسب‌تر و بهتری برای کاربران مهیا می‌شود (اوانز، ۱۳۸۷). در همه‌ی نهادهای دولتی نیز از جمله دانشگاه‌ها، ضروری است که مقررات و استانداردهای مربوط به سیستم مدیریت امنیت اطلاعات، در تمامی بخش‌ها از جمله کتابخانه‌ها و مراکز اطلاع‌رسانی اعمال گردد تا اطمینان حاصل شود که سطح امنیت اطلاعات در کل سازمان به حد مطلوب رسیده است (یوستانی و همکاران، ۲۰۱۸). در این میان کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاهی به دلیل نوع خاصی از مراجعه‌کنندگان، نیاز به ارائه نوع خاصی از منابع و پایگاه‌های اطلاعاتی دارند که ارائه این اطلاعات تخصصی به‌نوبه خود در توسعه دانش فردی، افزایش سطح دانش و آگاهی‌های جامعه دانشگاهی، گسترش علوم و تحقیقات و ... تأثیر بسزایی دارند. در حال حاضر وب‌سایت‌ها نیز از مهم‌ترین ابزار دسترسی به کتابخانه‌ها و همچنین به‌عنوان دروازه‌هایی برای هدایت کاربران به منابع اطلاعاتی و خدمات مورد نیاز، می‌باشند. لذا وجود امنیت در طراحی و به‌کارگیری وب‌سایت‌های کتابخانه‌ای امری ضروری است (حبیبی و همکاران، ۲۰۱۹).

از سوی دیگر در کتابخانه‌ها و مراکز اطلاع‌رسانی منابع اطلاعاتی با هزینه‌های بسیار زیادی تهیه و برای استفاده مهیا می‌شوند. هزینه‌های تهیه و نگهداری منابع اطلاعاتی و امنیت آن‌ها یک وجه مسئله و دسترسی و مهیا سازی آن‌ها برای استفاده، وجه دیگر ارائه خدمات در کتابخانه‌ها و مراکز اطلاع‌رسانی است. منابع و اطلاعات گردآوری شده در کتابخانه‌ها و مراکز اطلاع‌رسانی به‌منظور استفاده همگانی تهیه و تدارک دیده شده‌اند نه برای استفاده یک قشر خاص (هاروی، ۱۳۸۴) و چون تهیه جایگزینی برای برخی از اطلاعات نایاب و ارزشمند که بنا به دلایلی از دست‌رفته، به لحاظ صرف وقت، هزینه زیاد و وجود نیروی انسانی بسیار دشوار و حتی غیرممکن خواهد بود، لذا حفاظت و امنیت اطلاعات ضرورت بیشتری می‌یابد. در تحقیقی از کراگر، کرنی و استین^۵ (۲۰۱۰) نشان داده شد که سطح آگاهی کارمندان از امنیت اطلاعات در حد متوسطی

¹ Evans

² Yustanti & et al

³ Habibi & et al

⁴ Harvey

⁵ Kruger, Drevin, Steyn

قرار دارد. بنابراین پیشنهاد می‌شود که مدیران کتابخانه‌ها و مراکز اطلاع‌رسانی برای بالا بردن سطح درک و آگاهی نیروی انسانی، به امر آموزش و یادگیری در زمینه مسائل امنیتی توجه و تأکید بیشتری نمایند.

در عصر حاضر در کنار تسهیل فرآیندهای کاری کتابخانه‌ها و مراکز اطلاع‌رسانی بحث مدیریت امنیت اطلاعات اهمیت بیشتری دارد. عدم توجه برخی کاربران به منابع چاپی و غیر چاپی در کتابخانه‌ها و مراکز اطلاع‌رسانی، منجر به بروز صدمات فیزیکی و در نهایت تخریب و نابودی اطلاعات می‌شود. همچنین کتابخانه‌ها و مراکز اطلاع‌رسانی به علت عدم رعایت امنیت اطلاعات و ارتباطات، فقدان زیرساخت‌های فنی و اجرایی، نبود بازرسی کافی از تجهیزات و سامانه‌ها و عدم انجام اقدامات مؤثر در خصوص ایمن‌سازی با مشکلاتی روبه‌رو هستند. برخی از چالش‌هایی که ضرورت پرداختن به مسائل امنیتی در کتابخانه‌ها و مراکز اطلاع‌رسانی را توجیه می‌کند، عبارتند از: تخریب و ویروسی شدن اطلاعات دیجیتال، سرقت و دستبرد اطلاعات دیجیتالی، تهدید امنیتی نرم‌افزاری، سرقت منابع اطلاعاتی و تجهیزات موجود، عدم عکس‌العمل سریع فعالیت‌های کتابخانه و مراکز اطلاع‌رسانی در صورت وقوع حوادث امنیتی، عدم استفاده از نظام‌های مدیریت امنیتی پیشرفته و ... لذا ضروری است که امنیت اطلاعات در این امر مورد توجه قرار گیرد.

امنیت معمولاً به‌نظام یا فعالیتی اطلاق می‌گردد که برای جلوگیری از سرقت و دانش‌ستیزی مانند نظام کنترل کتابخانه، نظام امنیتی کتاب، حفاظت‌های امنیتی و نظایر آن‌ها به کار می‌رود (جوکار، ۱۳۸۳). امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن دسترسی غیرمجاز به آن‌ها اشاره می‌کند (جعفری و صادقی مجرد، ۱۳۸۶). هدف از امنیت اطلاعات، استفاده از مجموعه‌ای از سیاست‌ها، راهکارها، ابزارها، سخت‌افزارها و نرم‌افزارها، برای فراهم آوردن محیطی عاری از تهدید در تولید، پالایش، انتقال و توزیع اطلاعات است. فراهم آوردن چنین محیطی مستلزم انجام مواردی است که می‌توان از آن‌ها به عنوان نیازهای امنیت اطلاعات نام برد (ملک‌الکمالی، ۱۳۹۲). در واقع هر سازمان بسته به سطح اطلاعات خود نیازمند طراحی سیستم مدیریت امنیت اطلاعات می‌باشد تا از این طریق بتواند تهدیداتی که سازمان در معرض آن قرار دارد را شناسایی و مدیریت کند (سامرو، ۲۰۱۶). با توجه به اینکه وجود امنیت اطلاعات در سازمانی چون، کتابخانه‌ها و مراکز اطلاع‌رسانی از اهمیت زیادی برخوردار است، لذا این تحقیق بر آن بوده که با شناسایی عوامل مؤثر بر مدیریت امنیت اطلاعات، به اطلاعاتی یکپارچه و نظام‌مند در امر حفاظت و امنیت اطلاعات دست یابد و با مدیریت این اطلاعات و برنامه‌ریزی دقیق، بتواند سطح مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاه علوم پزشکی همدان را ارتقاء بخشد و در جهت ارائه خدمات مطلوب‌تر گام بردارد.

پیشینه پژوهش

با توجه به اهمیت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی، پژوهش‌های متعددی در این زمینه انجام شده است که در ادامه به تعدادی از این پژوهش‌ها اشاره می‌شود.

¹ Soomro

رضوانی (۱۳۹۷) در مطالعه‌ای با عنوان «طراحی الگوی مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی» به بررسی پرداخت یافته‌ها نشان داد که اثر متغیرهایی از جمله: خط‌مشی امنیت اطلاعات، معماری اطلاعات، سازماندهی امنیت اطلاعات، توسعه سیستم‌های اطلاعاتی، امنیت منابع انسانی و حفاظت محتوا بر امنیت اطلاعات در کتابخانه‌های دیجیتالی در سطح ($P < 0/01$) مثبت و معنادار بود. همچنین در میان متغیرهای موجود، متغیر توسعه سیستم‌های اطلاعاتی در رتبه اول و با بیشترین تأثیر (۰/۴۴) بر امنیت اطلاعات کتابخانه‌های دیجیتالی معرفی شد. باغی، بابایی و امیرحسینی (۱۳۹۴) در مطالعه‌ای با عنوان «ارزیابی وضعیت سیستم مدیریت امنیت اطلاعات» به بررسی پرداختند. هدف از پژوهش حاضر ارزیابی و بررسی سیستم مدیریت امنیت اطلاعات در تعدادی از کتابخانه‌های مرکزی دانشگاه‌های شهر تهران در مقایسه با شاخص‌های استاندارد ایزو بود. بررسی یافته‌های پژوهش نشان داد که عملکرد مدیریت امنیت اطلاعات در تعدادی از کتابخانه‌های مرکزی دانشگاه‌های شهر تهران بیشتر از حد استاندارد و یا به عبارتی مطلوب بود. ملک‌الکلامی (۱۳۹۲) در مطالعه‌ای با عنوان «ارزشیابی وضعیت عملکرد مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران براساس استاندارد بین‌المللی ایزو آی.ای.سی ۲۷۰۰۲» به بررسی پرداخت. نتایج این پژوهش حاکی از آن بود که 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. همچنین نتایج نشان داد به طور کلی کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران از لحاظ مدیریت امنیت اطلاعات در شرایط مطلوبی هستند و می‌توان گفت میانگین مدیریت امنیت اطلاعات در آن‌ها بر اساس استاندارد ایزو آی.ای.سی ۲۷۰۰۲ برابر با ۴ بوده و بالاتر از حد متوسط و در سطح مطلوبی قرار دارند. محمودزاده و رادرجی (۱۳۸۵) در مطالعه‌ای با عنوان «مدیریت امنیت در سیستم‌های اطلاعاتی» به بررسی پرداختند. نتایج حاصل از پژوهش نشان داد که مؤلفه عدم آگاهی کاربران، بالاترین تهدید و پس از آن امنیت نیروی انسانی، دومین تهدید برای امنیت اطلاعات سیستم‌های رایانه‌ای می‌باشد. مؤلفه‌های امنیت فیزیکی و امنیت اطلاعات به ترتیب در رتبه‌های بعدی قرار دارند. با توجه به این که دغدغه اصلی کارکنان برآورده ساختن درخواست‌ها و انجام وظایفی است که بر عهده آن‌ها می‌باشد اولین چیزی که معمولاً نادیده گرفته می‌شود مسائل امنیتی است. دلیل عمده آن را می‌توان نداشتن قانون مدون و ابلاغ شده به کارکنان دانست. نکته بسیار مهم این است که، نداشتن مقررات مکتوب باعث می‌شود اولاً کارکنان ندانند چه وظایفی نسبت به حفظ اطلاعات سازمان دارند و ثانیاً در صورت بروز تخلف آن‌ها، مرجعی برای رسیدگی به تخلفات وجود ندارد. همچنین نتایج نشان داد که با توجه به نقاط ضعف بسیار زیاد سازمان‌ها در حفظ دارایی‌های اطلاعاتی خود، بایستی آن‌ها با پیاده‌سازی سیستم مدیریت امنیت اطلاعات، ابتدا دارایی‌های حیاتی خود را شناسایی کنند و پس از آن مخاطرات هر یک را مشخص کنند. در ادامه، به تحقیقاتی در زمینه شناسایی و رتبه‌بندی عوامل مختلف در حیطه مدیریت امنیت اطلاعات انجام شده است، بررسی می‌گردد.

اسماعیل پور (۱۳۸۸) در مطالعه‌ای با عنوان «شناسایی و رتبه‌بندی عوامل و شاخص‌های کلیدی مؤثر بر بهبود نظام مدیریت امنیت اطلاعات» به بررسی پرداخت. نتایج نشان داد که عوامل مربوط به حوزه فنی بر بهبود نظام مدیریت امنیت اطلاعات تأثیر دارند. که در اولویت اول عامل نظام‌های حفاظتی و در اولویت بعدی به‌روزرسانی نظام قرار دارد. جعفری، رحمانی و مهرآزمای (۱۳۸۷) در مطالعه‌ای با عنوان «شناسایی و رتبه‌بندی عوامل و شاخص‌های کلیدی مؤثر بر مدیریت تهدیدات امنیت فیزیکی و محیطی اطلاعات» به بررسی پرداختند. در ابتدا عوامل و شاخص‌های کلیدی در حوزه امنیت فیزیکی و محیطی سازمان‌های مورد نظر با استفاده از تکنیک‌های آماری شناسایی، اعتبارسنجی و مورد تجزیه و تحلیل قرار گرفتند و در مجموع چهار عامل کنترل محیطی و مدیریت دسترسی، مدیریت تسهیلات فیزیکی، حفاظت از مرکز داده و کنترل کارکنان به دست آمد. علاوه بر این، تحلیل‌های بیشتر از مقایسه بین سازمان‌ها نشان‌دهنده این مطلب است که در همه عوامل کلیدی، تأثیر شاخص اندازه سازمان بر میزان اهمیت آن‌ها، از نقش اساسی برخوردار است. کاهویی و عباسی (۱۳۹۴) در مطالعه‌ای دیگر با عنوان «اولویت‌بندی عوامل مؤثر بر امنیت اطلاعات الکترونیکی سلامت در مراکز درمانی» دریافت که ۵/۷ درصد از کارکنان، نقش کاربران سیستم‌های اطلاعاتی، ۳/۳۸ درصد درک اهمیت امنیت اطلاعات، ۳۳ درصد آموزش ضمن خدمت و ۵/۴۷ درصد وجود زیرساخت مناسب را از مهم‌ترین عوامل امنیت اطلاعات سلامت انتخاب کردند. هو و چانگ^۱ (۲۰۰۶) نیز در مطالعه‌ای دیگر با عنوان «بررسی عوامل سازمانی مؤثر در پیاده‌سازی مدیریت امنیت اطلاعات» به بررسی پرداختند. این پژوهشگران ضمن تأکید بر نیاز سازمان‌ها به ساختارهای مدیریتی برای حفظ دارایی‌های اطلاعاتی، این‌گونه ساختارهای امنیتی را سلاحی مؤثر برای بقا در عرصه رقابت عنوان می‌کنند. براساس یافته‌های پژوهش، توانایی مدیران فناوری اطلاعات و نبود اطمینان محیطی، تأثیر مثبتی بر روی سازمان‌ها در پیاده‌سازی مدیریت امنیت اطلاعات داشته است. همچنین یافته‌ها نشان داد عوامل سازمانی شامل اندازه سازمان و نوع صنعت، به نحو قابل توجهی کاربرد مدیریت امنیت اطلاعات را تحت تأثیر قرار می‌دهد. فردیناند^۲، پاتریک^۳ و تیلیما^۴ (۲۰۱۵) در مطالعه‌ای با عنوان «عوامل مؤثر بر امنیت کتابخانه‌ها و منابع اطلاعاتی» به بررسی پرداختند و به این نتیجه رسیدند که استفاده از سیستم امنیتی و ارتباطات مخابراتی برای پشتیبانی مدیریت، پشتیبانی کارکنان، توسعه نرم‌افزار، ارتقاء سخت‌افزار و برای دستیابی به اهداف تعیین شده نیاز به بودجه دارد. بر این اساس، محققان به مدیران کتابخانه‌ها توصیه می‌نمایند، در ابتدا اطمینان حاصل شود که بودجه کافی برای کتابخانه‌ها جهت خرید، توسعه و نگهداری سیستم‌های امنیتی اختصاص یافته باشد و سپس سازماندهی برنامه‌های کاربردی و آموزشی به کارکنان در مورد نحوه استفاده از سیستم‌های امنیتی، به درستی صورت گرفته باشد. محابی^۵ (۲۰۱۰) در مطالعه‌ای با عنوان «آگاهی از عوامل مؤثر

¹ Ho

² Change

³ Ferdinand

⁴ Patrick

⁵ Thelma

⁶ Mahabi

بر امنیت اطلاعات از دیدگاه مدیران سیستم و کاربران نهایی در دانشگاه ایالتی فلوریدا» به بررسی پرداخت. 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 آگاهی آنها بود تا بتوانند از خود در برابر تهدیدهای امنیتی محافظت کنند. نتایج این مطالعه اهمیت عوامل انسانی در امنیت اطلاعات را مورد تأکید قرار داد.

با توجه به مطالب اشاره شده فوق و حائز اهمیت بودن مبحث مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی، این پژوهش باهدف اصلی تعیین عوامل مؤثر بر مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاه علوم پزشکی همدان و با اهداف فرعی شامل: ۱. شناسایی عوامل مؤثر بر مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاه علوم پزشکی همدان ۲. شناسایی وضعیت عوامل مؤثر بر مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاه علوم پزشکی همدان ۳. رتبه‌بندی عوامل مؤثر بر مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاه علوم پزشکی همدان، انجام شده تا با تقویت عوامل مذکور و پیاده‌سازی صحیح مدیریت امنیت اطلاعات، شرایطی را فراهم کرد که سیاست‌گذاران، مدیران و کتابداران و اطلاع‌رسانان بدون دغدغه به فعالیت‌های اصلی خود ادامه دهند و بتوانند تأثیر بیشتری روی بهبود اثربخشی امنیتی در کتابخانه‌ها و مراکز اطلاع‌رسانی بگذارند و در نهایت، تحقق اهداف نهایی سازمان، هموارتر صورت پذیرد.

روش پژوهش

پژوهش حاضر، از نظر رویکرد کمی و از نوع کاربردی با روش پیمایشی تحلیلی انجام شد. جامعه آماری این پژوهش تمام مدیران و کتابداران کتابخانه‌های دانشگاه علوم پزشکی همدان در سال ۱۳۹۷ به تعداد ۴۰ نفر بودند. با توجه به محدود بودن جامعه آماری، اطلاعات لازم به روش سرشماری یعنی بررسی کل جامعه آماری جمع‌آوری گردید و روش نمونه‌گیری خاصی مورد استفاده قرار نگرفت. ابزار پژوهش پرسشنامه محقق ساخته بود که پس از بررسی متون مرتبط (سیف و نادری بنی، ۱۳۸۶؛ تاج فر، محمودی میمند، رضا سلطانی و دیگران، ۱۳۹۳؛ کاهویی و عباسی، ۱۳۹۳) در دو بخش کلی شامل: بخش اول سؤالات دموگرافیک، بخش دوم سؤالات عوامل مؤثر بر مدیریت امنیت اطلاعات (شامل ۷ بعد: نرم‌افزاری، اجرایی، مدیریتی، نیروی انسانی، اقتصادی و مالی، رفتاری و فنی) در طیف ۵ گزینه‌ای لیکرت طراحی گردید. به منظور سنجش روایی صوری و محتوایی پرسشنامه، از نظرات ۸ نفر از اساتید متخصص و مدیران باسابقه دانشگاه علوم پزشکی همدان استفاده شد و با استفاده از روش لاوشه (۱۹۷۵)، ضریب نسبت روایی (Content Validity Ratio) CVR و شاخص روایی محتوایی (Content Validity Index) CVI محاسبه گردید. جهت بررسی ضریب نسبت روایی، از اساتید و مدیران اشاره شده خواسته شد که هر یک از گویه‌های پرسشنامه را بر اساس طیف سه درجه‌ای

¹ Lawshe

«گویه ضروری است»، «گویه مفید است ولی ضروری نیست» و «گویه ضرورتی ندارد» طبقه‌بندی نمایند. پاسخ‌ها نشان داد که نسبت روایی محتوایی همه گویه‌ها و مؤلفه‌های پرسشنامه بر اساس نظر ۸ متخصص و مدیر، بالاتر از ۰/۷۵ و با میانگین ۰/۸۹ بود. در خصوص بررسی شاخص روایی محتوایی پرسشنامه نیز از اساتید و مدیران مذکور خواسته شد سوالات پرسشنامه را در سه معیار «مربوط بودن»، «ساده بودن» و «واضح بودن» براساس طیف لیکرت چهار قسمتی، یک، برابر غیر مرتبط، دو، برابر تا حدودی مرتبط، سه، برابر مرتبط و چهار، برابر کاملاً مرتبط بیان نمایند. سپس امتیاز CVI به وسیله تقسیم مجموع امتیازات هر گویه که نمره سه و چهار را کسب کرده بود، بر تعداد کل پاسخ‌دهندگان، محاسبه شد؛ که برای تمام سوالات میانگین مقدار شاخص اعتبار محتوا ۰/۸۵ به دست آمد. این نتایج بیانگر این بود که پرسشنامه از اعتبار محتوایی کامل برخوردار است. سنجش پایایی پرسشنامه نیز با استفاده از آزمون آلفای کرونباخ انجام گرفت؛ که مقدار کلی ضریب آلفای کرونباخ ۰/۹۷ محاسبه شد و پایایی ابزار تأیید گردید. قبل از آزمون فرضیه‌ها، نرمال بودن متغیرهای مورد مطالعه توسط آزمون کولموگروف-اسمیرنوف تک نمونه‌ای بررسی شد. فرض نرمال بودن برای تمام متغیرها برقرار بود. برای بررسی فرضیه‌ها از آزمون تی تک نمونه‌ای، برای رتبه‌بندی از آزمون فریدمن و برای تجزیه و تحلیل داده‌ها از نرم افزار SPSS ویراست ۱۸ استفاده شد.

یافته‌ها

۱. توصیف داده‌های جمعیت شناختی

با توجه به نتایج بخش اول پرسشنامه (ویژگی‌های جمعیت شناختی)، اطلاعات زیر به طور خلاصه در مورد نمونه آماری مورد نظر ارائه می‌شود. همان‌طور که در جدول ۱ مشاهده می‌کنیم، بیشترین فراوانی (۴۵ درصد) مربوط به پاسخ‌دهندگان با رده‌ی سنی ۲۰-۳۰ سال، بیشترین فراوانی (۸۰ درصد) مربوط به پاسخ‌دهندگان خانم، بیشترین فراوانی (۴۷/۵ درصد) مربوط به پاسخ‌دهندگان دارای تحصیلات کارشناسی، بیشترین فراوانی (۸۵ درصد) مربوط به پاسخ‌دهندگان با رشته تحصیلی کتابداری و اطلاع‌رسانی، و بیشترین فراوانی (۴۷/۵ درصد) مربوط به پاسخ‌دهندگان با سابقه کار بین ۱-۵ سال بود.

جدول ۱. توصیف داده‌های جمعیت شناختی

| متغیرها | گویه‌ها | فراوانی | درصد |
|---------|-----------------|---------|------|
| سن | ۲۰ تا ۳۰ سال | ۱۸ | ۴۵ |
| | ۳۱ تا ۴۰ سال | ۸ | ۲۰ |
| | ۴۱ تا ۵۰ سال | ۱۰ | ۲۵ |
| | بیشتر از ۵۰ سال | ۴ | ۱۰ |
| جنس | مرد | ۸ | ۲۰ |
| | زن | ۳۲ | ۸۰ |
| تحصیلات | دیپلم | ۳ | ۷/۵ |
| | کاردانی | ۰ | ۰ |

| | | | |
|------|----|----------------------------|-------------|
| ۴۷/۵ | ۱۹ | کارشناسی | |
| ۴۲/۵ | ۱۷ | کارشناسی ارشد | |
| ۲/۵ | ۱ | دکتری | |
| ۸۵ | ۳۴ | کنابداری و اطلاع‌رسانی | رشته تحصیلی |
| ۱۵ | ۶ | غیر کنابداری و اطلاع‌رسانی | |
| ۴۷/۵ | ۱۹ | ۱-۵ | سابقه کار |
| ۱۰ | ۴ | ۶-۱۰ | |
| ۷/۵ | ۳ | ۱۱-۱۵ | |
| ۷/۵ | ۳ | ۱۶-۲۰ | |
| ۱۵ | ۶ | ۲۱-۲۵ | |
| ۱۲/۵ | ۵ | ۲۶-۳۰ | |

۲. بررسی نرمال بودن داده‌ها

برای اطمینان از نرمال بودن داده‌ها از آزمون آماری کولموگروف-اسمیرنوف استفاده می‌شود. در این آزمون برای بررسی نرمال بودن داده‌ها، فرض صفر مبتنی بر اینکه توزیع داده‌ها نرمال نیستند در سطح اطمینان ۹۵ درصد سنجیده می‌شود. در صورت نرمال بودن داده‌ها از آزمون‌های آمار پارامتریک و در غیر این صورت از آزمون‌های آمار نا پارامتریک استفاده می‌شود. داده‌ها در قالب فرضیه‌ی زیر آزمون می‌شوند.

فرض مقابل (H_1): فراوانی داده‌ها از توزیع نرمال پیروی نمی‌کند.

جدول ۲. بررسی عوامل مؤثر بر مدیریت امنیت اطلاعات با کمک آزمون کولموگروف و اسمیرنوف

| عوامل مؤثر | موارد محاسبی | |
|------------|--------------------------|------------------------|
| ۳/۶۵ | میانگین | پارامترهای توزیع نرمال |
| ۰/۶۳۰ | انحراف معیار | |
| ۰/۰۹۷ | قدر مطلق | تفاوت‌ها |
| ۰/۰۶۲ | مثبت | |
| -۰/۰۹۷ | منفی | |
| ۰/۰۹۷ | آماره کولموگروف-اسمیرنوف | |
| ۰/۲۰۰ | مقدار معناداری | |

همان‌طور که در جدول ۲ مشاهده می‌شود سطح معنی‌داری به دست آمده برای تمامی متغیرها بیشتر از ۵ درصد است، بنابراین فرضیه صفر، یعنی نرمال بودن داده‌ها پذیرفته می‌شود. لذا، با توجه به نرمال بودن توزیع داده‌ها، می‌توان از روش‌های آمار پارامتریک برای تجزیه و تحلیل داده‌ها استفاده کرد.

۳. بررسی فرضیه‌های تحقیق

در این بخش فرضیه‌های تحقیق به کمک آزمون‌های آماری مناسب آزمون شده‌اند. برای آزمون فرضیه‌های تحقیق از آزمون تی تک نمونه‌ای استفاده شده است. در ادامه فرضیه‌های تحقیق به تفکیک ذکر شده است.

۱. بین عامل نرم‌افزاری و مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی ارتباط معناداری وجود دارد.
۲. بین عامل اجرایی و مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی ارتباط معناداری وجود دارد.
۳. بین عامل مدیریتی و مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی ارتباط معناداری وجود دارد.
۴. بین عامل نیروی انسانی و مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی ارتباط معناداری وجود دارد.
۵. بین عامل اقتصادی و مالی و مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی ارتباط معناداری وجود دارد.
۶. بین عامل رفتاری و مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی ارتباط معناداری وجود دارد.
۷. بین عامل فنی و مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی ارتباط معناداری وجود دارد.

برای مثال در بررسی فرضیه ۱: فرضیه H_1 به ترتیب زیر تدوین شده است.

H_1 : بین عامل نرم‌افزاری و مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی ارتباط معناداری وجود دارد ($\mu \neq 3$). با توجه به جدول ۳، اگر سطح معناداری (Sig) بزرگ‌تر از مقدار خطا ($\alpha=0/05$) باشد، فرضیه صفر را نتیجه می‌گیریم و در صورتی که مقدار سطح معناداری از مقدار خطا کوچک‌تر باشد فرضیه مقابل را نتیجه می‌گیریم. با توجه به اینکه سطح معناداری کمتر از $0/05$ شده است، فرض یک (H_1) پذیرفته می‌شود. بدین معنی که در فاصله اطمینان ۹۵ درصد، تفاوت معناداری بین میانگین متغیر عامل نرم‌افزاری و میانگین فرضی جامعه (۳) وجود دارد. لذا فرضیه اول تأیید می‌گردد. مثبت بودن مقادیر حد بالا و پایین، فاصله تفاوت اختلاف میانگین متغیر عامل نرم‌افزاری با (۳) را نشان می‌دهد که میانگین امتیازات متغیر عامل نرم‌افزاری از ۳ بیشتر می‌باشد. به عبارت دیگر متغیر عامل نرم‌افزاری از نظر پاسخگویان دارای اهمیت است و در وضعیت مطلوبی قرار دارد.

جدول ۳. نتایج حاصل از آزمون تی تک نمونه‌ای برای تمام عوامل

| تعداد | آماره آزمون تی | درجه آزادی | سطح معنی‌داری | اختلاف میانگین | فاصله اطمینان ۹۵٪ | | عوامل |
|-------|----------------|------------|---------------|----------------|-------------------|----------|--------------|
| | | | | | حد بالا | حد پایین | |
| ۴۰ | ۳۴/۹۸۹ | ۳۹ | .۰۰۰ | ۳/۸۰۰ | ۳/۵۸ | ۴/۰۲ | نرم‌افزاری |
| ۴۰ | ۳۳/۲۲۹ | ۳۹ | .۰۰۰ | ۳/۷۵۰ | ۳/۵۲ | ۳/۹۸ | اجرایی |
| ۴۰ | ۳۶/۸۱۶ | ۳۹ | .۰۰۰ | ۳/۷۱۶ | ۳/۵۱ | ۳/۹۲ | مدیریتی |
| ۴۰ | ۲۹/۶۴۱ | ۳۹ | .۰۰۰ | ۳/۵۲۱ | ۳/۲۸ | ۳/۷۶ | نیروی انسانی |

| | | | | | | | |
|----|--------|----|-----|-------|------|------|----------------|
| ۴۰ | ۲۵/۱۹۷ | ۳۹ | ۰۰۰ | ۳/۵۲۵ | ۳/۲۴ | ۳/۸۱ | اقتصادی و مالی |
| ۴۰ | ۲۶/۵۸۷ | ۳۹ | ۰۰۰ | ۳/۶۲۵ | ۳/۳۵ | ۳/۹۰ | رفتاری |
| ۴۰ | ۲۰/۲۵۳ | ۳۹ | ۰۰۰ | ۳/۴۵۸ | ۳/۱۱ | ۳/۸۰ | فنی |

به همین ترتیب مراحل ذکر شده، برای تمام فرضیه‌ها بررسی گردید. با توجه به اینکه سطح معناداری کمتر از ۰/۰۵ شده است، فرض صفر (H0) رد شده و فرض یک (H1) پذیرفته می‌شود. بدین معنی که در فاصله اطمینان ۹۵ درصد تفاوت معناداری بین میانگین کلیه عوامل و میانگین فرضی جامعه (۳) وجود دارد. لذا تمام فرضیه‌ها تأیید می‌گردد. به عبارت دیگر تمام عوامل از نظر پاسخگویان دارای اهمیت است و در وضعیت مطلوبی قرار دارند.

۴. اولویت‌بندی متغیرهای تحقیق (آزمون فریدمن)

آزمون فریدمن یک آزمون نا پارامتری، معادل آنالیز واریانس با اندازه‌های تکراری (درون گروهی) است که از آن برای مقایسه میانگین رتبه‌ها در بین K متغیر (گروه) استفاده می‌کنیم. در این مطالعه برای اولویت‌بندی عوامل مؤثر بر مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی از آزمون فریدمن استفاده شده است که بر اساس جدول ۴، نتایج این رتبه‌بندی نشان داده شده است.

جدول ۴. اولویت‌بندی عوامل مؤثر بر مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی

| رتبه | میانگین ابعاد سازه | ابعاد سازه | سازه |
|------|--------------------|----------------|---|
| ۲ | ۴/۲۴ | نرم‌افزاری | عوامل مؤثر بر مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی |
| ۱ | ۴/۴۶ | اجرایی | |
| ۴ | ۴/۰۴ | مدیریتی | |
| ۷ | ۳/۵۶ | نیروی انسانی | |
| ۶ | ۳/۷۴ | اقتصادی و مالی | |
| ۳ | ۴/۱۰ | رفتاری | |
| ۵ | ۳/۸۶ | فنی | |

جدول ۴، بیانگر این است که سازه‌ی اجرایی با میانگین ۴/۴۶ در رتبه اول و با بیشترین اثرگذاری در سیستم مدیریت امنیت اطلاعات و سازه‌ی نیروی انسانی با میانگین ۳/۵۶ در رتبه هفتم و با کمترین اثرگذاری شناسایی شد.

بحث و نتیجه‌گیری

بررسی ویژگی‌های جمعیت شناختی نشان داد که ۸۵ درصد از مدیران، کتابداران و افراد شاغل در کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاه علوم پزشکی همدان دارای مدرک تحصیلی در رشته کتابداری و اطلاع‌رسانی هستند. این مورد را می‌توان یکی از نقاط قوت کتابخانه‌ها و مراکز اطلاع‌رسانی در دانشگاه علوم پزشکی همدان محسوب نمود؛ که به نظر می‌رسد با توجه به اینکه این افراد با دارا بودن دانش و مهارت‌های

تخصصی، می‌توانند خدمات مطلوبی را در کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاه ارائه نمایند، باعث ارتقاء مدیریت امنیت اطلاعات نیز خواهند شد.

نتایج پژوهش حاضر نشان داد که بین عامل اجرایی و مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی ارتباط معناداری وجود دارد و متغیر اجرایی با میانگین ۴/۴۶ در رتبه اول و به عنوان مؤثرترین عامل بر مدیریت امنیت اطلاعات شناخته شد. در حالی که در پژوهش رضوانی (۱۳۹۷)، عامل نرم‌افزاری در رتبه اول و به عنوان مؤثرترین عامل در امنیت اطلاعات معرفی شده بود. لذا این نتیجه با نتایج حاصله از پژوهش رضوانی (۱۳۹۷) مطابقت ندارد. از آنجایی که کتابخانه‌ها و مراکز اطلاع‌رسانی نقش مهمی را در دسترسی افراد به اطلاعات گوناگون ایفا می‌کنند و در این میان کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاهی بخصوص دانشگاه‌های علوم پزشکی، با مباحث مهم و به‌روز پزشکی سروکار دارند و همچنین به دلیل نوع خاصی از مراجعه‌کنندگان، نیاز به ارائه انواع گوناگونی از منابع و پایگاه‌های اطلاعاتی دارند. بنابراین ضروری است که در تمام بخش‌های کتابخانه جهت حفظ و مدیریت امنیت اطلاعات، قوانین و استانداردهای امنیتی اجرا شود و مدیران و کتابداران و اطلاع‌رسانان ملزم به رعایت آن شوند، همچنین شناسایی و طبقه‌بندی اطلاعات به صحیح‌ترین شکل ممکن صورت پذیرد تا پژوهشگران، اعضای هیئت علمی و دانشجویان در سریع‌ترین زمان ممکن به اطلاعات موردنیاز خود دست یابند. نتایج بررسی‌های انجام شده نشان داد که بین عامل نرم‌افزاری و مدیریت امنیت اطلاعات نیز ارتباط معناداری وجود دارد. لذا این نتایج، با نتایج به دست آمده از پژوهش رضوانی (۱۳۹۷) مطابقت دارد. با توجه به اهمیت و نقش کلیدی برنامه‌های نرم‌افزاری و تجهیزات سخت‌افزاری در تمام سازمان‌ها، به مدیران ارشد و برنامه‌ریزان کتابخانه‌ها و مراکز اطلاع‌رسانی توصیه می‌شود که جهت حفظ و مدیریت امنیت اطلاعات، به روزآمدسازی و یکپارچگی سیستم‌های اطلاعاتی و برنامه‌های نرم‌افزاری کتابخانه‌ها و مراکز اطلاع‌رسانی اهمیت فراوان دهند و با تحت‌وب نمودن نرم‌افزار کتابخانه، دسترسی سریع و آسانی را برای کاربران فراهم نمایند. به دنبال پیاده‌سازی قوانین و مقررات امنیتی و یکپارچگی نرم‌افزارهای کاربردی کتابخانه‌ها و مراکز اطلاع‌رسانی، رعایت اخلاق و رفتار امنیتی نیز امر مهمی است. بنابراین لازم است که مدیران ارشد در کتابخانه‌ها و مراکز اطلاع‌رسانی، کتابداران و اطلاع‌رسانان را به رعایت احترام نسبت به یکدیگر، داشتن تعهد و وفاداری به ارزش‌های سازمان و حفظ امنیت اطلاعات و ایجاد مشارکت با یکدیگر جهت رویارویی با مسائل و مشکلات امنیتی، تشویق و ترغیب نمایند تا از این طریق بتوانند در سازمان خود فضایی مناسب جهت بهبود سطح مدیریت امنیت اطلاعات ایجاد نمایند. لذا همان‌طور که یافته‌ها نیز بیانگر ارتباط معنادار، بین عامل رفتاری و مدیریت امنیت اطلاعات بود، این یافته با یافته‌های به دست آمده از پژوهش کاهویی و عباسی (۱۳۹۴) مطابقت دارد. چهارمین عامل مؤثر بر مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی، عامل مدیریتی است. یافته‌ها نشان داد که بین عامل مدیریتی و مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی ارتباط معناداری وجود دارد. به بیان دیگر توانایی مدیران در مدیریت محیط، مدیریت دسترسی، مدیریت تسهیلات فیزیکی و کنترل کارکنان

کتابخانه‌ها بر پیاده‌سازی مدیریت امنیت اطلاعات تأثیر دارد. لذا این یافته با یافته‌های به دست آمده از پژوهش‌های جعفری، رحمانی و مهرآزمای (۱۳۸۷)، چانگک و هو (۲۰۰۶) و رضوانی (۱۳۹۷) مطابقت دارد. بنابراین مدیران ارشد کتابخانه‌ها و مراکز اطلاع‌رسانی، می‌توانند با داشتن درک درستی از مفهوم امنیت اطلاعات، تعریف نمودن چشم‌انداز و خط‌مشی مدیریت امنیت اطلاعات، پیاده‌سازی قوانین و استانداردهای امنیتی، ایجاد فرهنگ مدیریت امنیت اطلاعات، نظارت بر اجرای قوانین و اقدام مؤثر و مناسب در برابر نقض موارد امنیتی، سطح امنیت اطلاعات را ارتقاء دهند و در جهت ارائه خدمات مطلوب‌تر گام بردارند. در بررسی یافته‌های پژوهش نشان داده شد که بین عامل فنی و مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی نیز ارتباط معناداری وجود دارد و این نتیجه گویای این است که عوامل مربوط به حوزه فنی از جمله نصب سیستم شنا ساگر متجاوز برای جلوگیری از نفوذ غیرمجاز، بر بهبود نظام مدیریت امنیت اطلاعات تأثیر دارند. لذا این نتیجه با نتایج به دست آمده از پژوهش‌های اسماعیل‌پور (۱۳۸۸) و کاهویی و عباسی (۱۳۹۴) مطابقت دارد. یکی دیگر از یافته‌های پژوهش تأثیر عامل اقتصادی و مالی بر مدیریت امنیت اطلاعات را نشان داد. از آنجایی که کتابخانه‌ها و مراکز اطلاع‌رسانی برای تأمین امنیت کافی در فضای کتابخانه و منابع اطلاعاتی چاپی و الکترونیکی، خرید تجهیزات سخت‌افزاری و برنامه‌های نرم‌افزاری، استخدام و به‌کارگیری مدیران متخصص و کتابداران خبره در زمینه امنیت اطلاعات به بودجه کافی نیاز دارند. لذا به مسئولان محترم سازمان بودجه پیشنهاد می‌گردد که براساس نیاز کتابخانه‌ها و مراکز اطلاع‌رسانی، بودجه کافی را جهت حفظ و ارتقاء مدیریت امنیت اطلاعات تأمین نمایند. در نتیجه این یافته با یافته‌های به دست آمده از پژوهش‌های فردیناند، پاتریک و تلیما (۲۰۱۵) مطابقت دارد. بررسی یافته‌های پژوهش نشان داد که بین عامل نیروی انسانی و مدیریت امنیت اطلاعات نیز ارتباط معناداری وجود دارد. به عبارت دیگر اگر نیروی انسانی شاغل در کتابخانه‌ها دستورالعمل‌های مرتبط با مؤلفه‌های مدیریت امنیت اطلاعات را به شیوه صحیح رعایت نمایند می‌توان انتظار داشت که امنیت اطلاعات در کتابخانه‌ها به طور نسبی رعایت می‌شود. لذا این یافته با یافته‌های به دست آمده از پژوهش‌های رضوانی (۱۳۹۷)، ملک الکلامی (۱۳۹۲) و محابی (۲۰۱۰) مطابقت دارد. در نتیجه به سیاست‌گذاران، برنامه‌ریزان و مدیران پیشنهاد می‌شود که با استخدام نیروی انسانی متخصص و خبره در کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاهی و با انجام اقداماتی آموزشی از قبیل: برگزاری کلاس‌ها و دوره‌های مرتبط با مسائل امنیتی و رویارویی با مشکلات و چالش‌های آن در قالب آموزش‌های ضمن خدمت و استفاده از ابزارهای آموزشی متنوع در این زمینه، نسبت به آموزش و یادگیری کتابداران و اطلاع‌رسانان اقدام نمایند تا آنان مطلع شوند که چه وظایفی نسبت به حفظ و مدیریت اطلاعات سازمان خود دارند و همچنین موجبات رضایت مدیران از کتابداران و اطلاع‌رسانان و بالعکس نیز فراهم آید. بنابراین تأکید بر مسئله امنیت پیش از اشتغال افراد، در حین خدمت و در خاتمه یا تغییر شغل امری مهم است. امید است که مدیران و مسئولین ذی‌ربط به این موضوع توجه بیشتری نمایند و با مدیریت صحیح در امنیت اطلاعات، ضریب امنیتی سازمان خود را افزایش دهند تا بتوانند، به سمت تحقق اهداف امنیتی و در نهایت تحقق اهداف سازمان خود گام بردارند. زیرا اگر کارکنان یک سازمان صلاحیت

کافی در اجرای امور محوله نداشته باشند، مایل به اجرای سیاست‌های امنیتی نباشند و یا حتی آشنایی و درک درستی از مباحث امنیت اطلاعات سازمان خود نداشته باشند همه‌ی تلاش‌های آن سازمان در حوزه مدیریت امنیت اطلاعات بیهوده و بدون نتیجه خواهد ماند.

در انتها، با نتیجه‌گیری کلی از یافته‌های حاصل از این تحقیق، می‌توان عواملی چون: ۱. اجرایی ۲. نرم‌افزاری ۳. رفتاری ۴. مدیریتی ۵. فنی ۶. اقتصادی و مالی و ۷. نیروی انسانی را از عوامل مؤثر بر مدیریت امنیت اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی معرفی کرد. بنابراین ضروری است که مدیران، کتابداران و اطلاع‌رسانان برای بهتر شدن وضعیت مدیریت امنیت اطلاعات سازمان خود، تمام توان خود را در حل مشکلات به کار گیرند و با برنامه‌ریزی و انجام اقداماتی از قبیل شناسایی و به کارگیری عوامل مؤثر بر مدیریت امنیت اطلاعات، بتوانند برنامه‌ای متناسب با سازمان خود در جهت مدیریت صحیح امنیت اطلاعات و تقویت نقاط قوت و ضعف امنیتی، طراحی و پیاده‌سازی نمایند. با توجه به این که تحقق امنیت در کتابخانه‌ها و مراکز اطلاع‌رسانی یکی از نگرانی‌های عمده محسوب می‌شود، لذا پیشنهاد می‌شود تا با انجام پژوهش‌های بیشتر در زمینه عوامل مؤثر بر مدیریت امنیت اطلاعات، زمینه لازم برای توسعه و پیاده‌سازی مدل‌های امنیت اطلاعات در سطح وسیع فراهم گردد تا بتوان مدل‌هایی استاندارد در این زمینه طراحی و از آن در جهت تحقق اهداف امنیتی استفاده نمود. بنابراین به کارگیری نتایج حاصل از چنین تحقیقاتی، منجر به برنامه‌ریزی دقیق و درنظر گرفتن عوامل دخیل در امنیت اطلاعات، در جهت رفع موانع و مشکلات امنیتی و تلاش برای پیاده‌سازی روش‌های ارتقاء مدیریت امنیت اطلاعات و ایمن‌سازی فضای تبادل اطلاعات در کتابخانه‌ها و مراکز اطلاع‌رسانی خواهد شد.

منابع

اسماعیل پور، حمید رضا (۱۳۸۸). شناسایی و رتبه‌بندی عوامل و شاخص‌های کلیدی مؤثر بر بهبود سیستم مدیریت امنیت اطلاعات. پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی تهران، دانشکده مدیریت و حسابداری.

باغی، مریم؛ محمدرضا، بابائی؛ زهرا، امیرحسینی (۱۳۹۴). ارزیابی وضعیت سیستم مدیریت امنیت اطلاعات، اولین کنفرانس بین‌المللی حسابداری و مدیریت در هزاره سوم، رشت، شرکت پیشگامان پژوهش‌های نوین، https://www.civilica.com/Paper-AMTM01_039.html

تاج‌الدینی، اورانوس؛ سادات موسوی، علی (۱۳۸۹). مدیریت امنیت در معماری فضاها و کتابخانه‌ای. کتاب ماه کلیات، ۱۴۹، ۶۴-۶۷.

تاج فر، امیر هوشنگ؛ محمودی میمند، محمد؛ رضا سلطانی، فاطمه؛ رضا سلطانی، پوریا (۱۳۹۳). رتبه‌بندی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف. مدیریت فناوری اطلاعات. ۶(۴): ۵۵۱-۵۵۶.

جعفری، عزیزاله؛ رحمانی، مرتضی؛ مهرآزمای، حجت (۱۳۸۷). شناسایی و رتبه‌بندی عوامل و شاخص‌های کلیدی مؤثر بر مدیریت تهدیدات امنیت فیزیکی و محیطی اطلاعات، پنجمین کنفرانس بین‌المللی مدیریت فناوری اطلاعات و ارتباطات، تهران، ندای اقتصاد بامداد (ناب)، https://www.civilica.com/Paper-ICTM05-ICTM05_055.html

جعفری، نیما؛ صادقی مجرد، مرجان (۱۳۸۶). سیستم مدیریت امنیت اطلاعات از طرح تا اصلاح. تدبیر، ۱۸۹، ۶۲-۵۹.

جوکار، طاهره (۱۳۸۳). مبانی و اصول مدیریت امنیت در کتابخانه‌ها. فصلنامه کتاب، ۵۹، ۵۱-۶۲.
رضوانی، شهلا (۱۳۹۷). طراحی الگوی مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتال. پژوهش‌های نظری و کاربردی در علم اطلاعات و دانش‌شناسی. ۸(۱): ۳۳۷-۳۵۶.

سیف، یاسر؛ نادری بنی، ناهید (۱۳۹۶). شناسایی مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قاره ایران. مدیریت فناوری اطلاعات. ۹(۴): ۸۵۱-۸۷۰.

کاهویی، مهدی؛ عباسی، زینب (۱۳۹۴). اولویت‌بندی عوامل مؤثر بر امنیت اطلاعات الکترونیکی سلامت در مراکز درمانی. مدیریت اطلاعات سلامت. ۱۲(۲): ۱۶۲-۱۷۰.

محمود زاده، ابراهیم؛ راد رجبی، مهدی (۱۳۸۵). مدیریت امنیت در سیستم‌های اطلاعاتی. فصلنامه علوم مدیریت ایران، ۱(۴)، ۷۸-۱۱۲.

ملک‌الکمالی، میلا (۱۳۹۲). ارزشیابی وضعیت عملکرد مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران براساس استاندارد بین‌المللی ایزو/آی. ای. سی. ۲۷۰۰۲. پژوهشنامه پردازش و مدیریت اطلاعات. ۲۸(۴): ۸۹۵-۹۱۶.

Change, S., & Ho, C. (2006). *Organizational factors to the effectiveness of implementing information security management.*

Evans, E. (2008). *Management techniques for librarians.* trans. Naseri, F (F. Naseri, Trans.). Mashhad: Islamic Research Foundation, Astan Quds Razavi.

Ferdinand, O., Patrick, I., & Thelma, N. (2015). *library and information resources security: traditional and electronic security measures.* *International journal of academic research and reflection*, 3(3).

Habibi, SH., Seyed-Akbari, L., Torab-Miandoab, A., Samad-Soltani, T. (2019). *Usability of Central Library Websites of Iranian Universities of Medical Sciences: An Evaluation.* *Desidoc Journal of Library & Information Technology*, Vol. 39, No. 4, July 2019, pp. 162-168, DOI: 10.14429/djlit.39.4.14462.

Harvey, D. (2005). *Pathology of Library Material: Principles, Strategies, and Librarians' Work.* trans. shokouei, A (s. a, Trans.). Tehran: Deepish: Talia.321-345.

Kruger, HA, Drevin L, Steyn T. (2010) *A Vocabulary test to assess information .Information Management & Computer Security Journal.* 18(5):316-9.

-
- Lawshe, CH. (1975). *A quantitative approach to content validity*. *Personnel psychology*, 28(4): 563-575.
- Mahabi, V (2010). *Information security Awareness: system Administrators and End- Use Perspective at Florida State University*. *Dissertation for the degree of Doctor of Philosophy in Library and Information Studies*. The Florida State University.
- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). *Information security management needs more holistic approach: A literature review*. *International Journal of Information Management*, 36(2), 215-225. doi: 10.1016/j.ijinfomgt.2015.11.009.
- Yustanti W, Qoiriah A, Bisma R, Prihanto A. (2018). *An analysis of Indonesia's information security index: a case study in a public university Informatics Engineering Department, Universitas Negeri Surabaya, Indonesia*.