

ارزیابی فرهنگ امنیت اطلاعات کتابخانه پژوهشکده‌ها و پژوهشگاه‌های

فنی - مهندسی

فاطمه کولیوند

کارشناس ارشد، رشته علم اطلاعات و دانش‌شناسی، دانشکده علوم تربیتی و روانشناسی،
دانشگاه الزهراء(س)^۱

زویا آبام

استادیار، دکتری علم اطلاعات و دانش‌شناسی، دانشکده علوم تربیتی و روانشناسی،
دانشگاه الزهراء(س)

میترا دیلمقانی

استادیار، دکتری علم اطلاعات و دانش‌شناسی، دانشکده مدیریت و فناوری‌های نرم، دانشگاه صنعتی مالک اشتر

فصلنامه علمی - پژوهشی

مدیریت

اطلاعات

دوره ۲، شماره ۵

زمستان ۹۵

چکیده: مرور پژوهش‌های صورت گرفته در داخل کشور حاکی از آن است که تاکنون هیچ‌گونه پژوهش ساخت‌یافته‌ای با تمرکز بر یک مدل فرهنگ امنیت اطلاعات به بررسی درک، نگرش و رفتار امنیت اطلاعات کتابداران نسبت به وضعیت موجود امنیت اطلاعات نپرداخته است. با توجه به هدف پژوهش حاضر، برای اولین بار در کشور به بومی‌سازی یک مدل فرهنگ امنیت اطلاعات پرداخته شد. هدف اصلی پژوهش حاضر ارزیابی فرهنگ امنیت اطلاعات کتابخانه پژوهشکده‌ها و پژوهشگاه‌های فنی - مهندسی مستقر در استان‌های تهران و البرز است. پژوهش حاضر از نوع کاربردی است که به روش پیمایشی - توصیفی انجام شده است. با استفاده از نمونه‌گیری غیر احتمالی هدفمند، ۱۹ پژوهشکده و پژوهشگاه فنی - مهندسی مستقر در استان‌های تهران و البرز به‌عنوان نمونه آماری انتخاب شدند. در این پژوهش کلیه کتابداران شاغل در این کتابخانه‌ها که ۶۰ نفر بودند، مورد مطالعه قرار گرفتند. ابزار گردآوری داده‌ها پرسشنامه محقق ساخته مبتنی بر مدل فرهنگ امنیت اطلاعات مارتینز در سال ۲۰۰۱ است. یافته‌ها با استفاده از آمار توصیفی اعم از آزمون‌های شاخص‌های گرایش به مرکز، شاخص‌های پراکندگی و آمار استنباطی اعم از تحلیل واریانس یک‌طرفه و مقایسه میانگین‌ها مورد تجزیه و تحلیل قرار گرفت. بررسی وضعیت موجود نشان داد فرهنگ امنیت اطلاعات ۷۶/۶ درصد کتابخانه‌های مراکز مورد مطالعه، در سطح ضعیف است. از طرف دیگر، درک، نگرش و رفتار امنیت اطلاعات کتابداران نسبت به سطح سازمانی در وضعیت متوسط (۴۰/۹۷)؛ سطح گروهی (۲۱/۷۳) و فردی (۲۴/۶۷) و بعد تغییر (۱۷/۱۳) در وضعیت ضعیف ارزیابی شد. وضعیت موجود فرهنگ امنیت اطلاعات کتابخانه پژوهشکده‌ها و پژوهشگاه‌های فنی - مهندسی استان‌های تهران و البرز در سطح نامطلوبی قرار دارد و ضعیف ارزیابی می‌شود. همچنین وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران در تمامی ابعاد در سطح ضعیفی قرار دارد.

کلیدواژه‌ها: اطلاعات، امنیت، امنیت اطلاعات، فرهنگ سازمانی، فرهنگ امنیت اطلاعات، کتابخانه‌های تخصصی.

¹ kolivand.fatemeh@yahoo.com

مقدمه

اطلاعات می‌تواند به صورت‌های مختلفی وجود داشته باشد؛ روی کاغذ نوشته یا چاپ شود، به صورت الکترونیک نگهداری شود، در مکالمه‌ها و به‌طور شفاهی نمایان شود و غیره. امروزه اطلاعات خرید، فروخته، دزدیده، مبادله و به اشتراک‌گذارده می‌شود (بیگلرگیان، ۱۳۹۱: ۲۱). از طرفی، اطلاعات یکی از مهم‌ترین دارایی‌های هر سازمان محسوب می‌شود. به‌طور بالقوه این امکان وجود دارد که ۲ تا ۳ درصد از سود سالانه سازمان به علت حوادث مربوط به امنیت اطلاعات از دست‌داده شود. یکی از مطالعات اخیر نقص داده‌ها نشان می‌دهد افراد و عوامل داخلی می‌توانند به‌طور عمدی یا غیرعمدی باعث خرابی و نقص اطلاعات گردند (Veiga & Eloff, 2010). در نتیجه یک سازمان بایستی اطلاعات و دارایی‌های اطلاعاتی حیاتی و مهم خود را شناخته و در جهت محافظت از آن‌ها تلاش کند.

بیشتر سازمان‌ها راه‌حل‌های فنی را به‌عنوان جواب سریع و فوری به مشکلات امنیتی خود می‌دانند. در صورتی که نباید از مسائل مدیریتی و عوامل انسانی غافل بود (طاهری، ۱۳۸۶: ۲). بنابراین عنصر انسانی عامل مهمی در امنیت اطلاعات به شمار می‌رود (Williams, 2009)، چون آن‌ها همواره با این دارایی‌ها در تعامل هستند. تعاملات کارکنان بر خواسته از نوع فرهنگی است که در سازمان حاکم است. از این‌رو، یکی از این عواملی که می‌تواند مستقیماً بر فعالیت‌های امنیتی یک سازمان تأثیر بگذارد، فرهنگ سازمانی است. فرهنگ سازمانی به ارزش‌های کلیدی، باورها و تفاهم‌هایی اشاره دارد که در بین اعضای یک سازمان مشترک هستند. فرهنگ سازمانی را می‌توان یکی از اجزای بنیادی و مهم در حیات یک سازمان به حساب آورد (عاشوری زاده به نقل از: قاسمی، ۱۳۸۸: ۶۰۱). به‌طور کلی، پیاده‌سازی یک نظام امنیت اطلاعات کارا و اثربخش نیازمند هماهنگی مناسب میان فرهنگ سازمانی و مشخصه‌های امنیت اطلاعات است.

زمانی که اصطلاح فرهنگ سازمانی با اصطلاح امنیت اطلاعات در یک مفهوم یکپارچه با یکدیگر ترکیب شوند، برون‌داد آن فرهنگ امنیت اطلاعاتی است که مشتمل بر ارزش‌ها و هنجارهای مرتبط با ملزومات امنیتی است که در بین افراد یک سازمان مشترک است. از طرفی، همان‌گونه که توسعه فرهنگ سازمانی با توجه به رفتارهای کارکنان در آن سازمان در سه سطح رفتار سازمانی منسوب به رایینز یعنی سطح سازمانی، سطح گروهی و سطح فردی صورت می‌پذیرد، فرهنگ امنیت اطلاعات نیز بر اساس شیوه تعامل کارکنان با اطلاعات و دارایی‌های اطلاعاتی و رفتارهای امنیتی که در چارچوب فرهنگ سازمانی در یک سازمان از خود بروز می‌دهند، بنانهاده می‌شود (Eloff & Von Solms, 2000). پس فرهنگ امنیت اطلاعات به‌عنوان بخشی از فرهنگ سازمانی بر تعامل کارکنان اطلاعات و دارایی‌های اطلاعاتی تأکید دارد. از آنجاکه فرهنگ امنیت اطلاعات ریسک دارایی‌ها، به‌ویژه سوء رفتارهای کارکنان و تعامل نادرست با اطلاعات را به حداقل می‌رساند، سازمان‌ها به راهنمایی برای ایجاد امنیت اطلاعات و یا اجرای سطح قابل قبول فرهنگ ایمنی اطلاعات نیاز دارند. در نتیجه اندازه‌گیری و گزارش در مورد وضعیت فرهنگ امنیت اطلاعات در سازمان لازم است (Veiga & Eloff, 2010).

این مهم در سازمان‌های اطلاعات محور از اهمیت ویژه‌ای برخوردار است. یکی از این سازمان‌ها پژوهشگاه‌ها هستند که بخش مهمی از اطلاعات خود را در کتابخانه‌هایشان نگهداری می‌کنند. رسالت این نوع از کتابخانه‌ها حمایت از اهداف سازمان مادر با تمرکز بر تهیه منابع موردنیاز و مرتبط با کارکرد سازمان و حفظ و نگهداری اوراق و اسناد پژوهشی سازمان مادر است. امروزه کتابخانه‌های تخصصی انواع مهمی از دارایی‌ها، از قبیل دارایی‌های اطلاعاتی، مستندات کاغذی، دارایی‌های نرم‌افزاری، دارایی‌های فیزیکی، منابع انسانی، وجهه و شهرت سازمانی و سرویس‌ها را دارا هستند. در این بین اطلاعات ممکن است به گونه‌های مختلف، اعم از کاغذی (مستندات و مراسلات متداول)، رسانه‌های الکترونیکی (سوابق پایگاه داده، ایمیل‌ها، سی‌دی‌ها و دی‌وی‌دی‌ها، نوارها و غیره) و بالاخره مکالمات (اطلاعات بیان‌شده به مشتری و اطلاعات بیان‌شده در جلسات) باشد (استاندارد ISO/IEC 17799). این قبیل دارایی‌ها همواره در معرض تهدیدهای متعددی از قبیل عوامل داخلی مانند سوء رفتارهای ناشی از کارکنان سازمان یا عوامل خارجی مانند مراجعه‌کنندگانی که با انگیزه‌های مختلف سعی در دستیابی غیرمجاز به منابع رادارند، هستند. عدم توجه کافی به هر یک از این مسائل می‌تواند منجر به هدر رفتن اعتبار و هزینه‌های کتابخانه شود.

کتابخانه‌ها نیاز دارند تا با رعایت محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات، به‌عنوان یک عامل تأثیرگذار در راستای تحقق یک یا چند مورد از اهداف سازمان مادر مانند «تداوم کسب‌وکار»، «مزیت رقابتی»، «کاهش خسارات وارده به کسب‌وکار»، «بهره‌وری»، «افزایش ارزش افزوده»، «مشتری مداری» گام‌های مؤثری بردارند (استاندارد ISO/IEC 17799). در این صورت مدیران کتابخانه‌ها و کتابداران به‌عنوان عاملان اجرایی این الزامات محسوب می‌شوند. بنابراین رعایت الزامات امنیتی حین تعامل آن‌ها با دارایی‌ها یک ضمانت اجرایی برای دستیابی به اهداف مذکور را به دنبال خواهد داشت.

با توجه به آنچه گفته شد تأمین امنیت اطلاعات و دارایی‌های اطلاعاتی در کتابخانه‌های تخصصی به درک، نگرش و رفتار کتابداران با آن‌ها وابستگی زیادی دارد. نوع درک، نگرش و رفتار کتابداران حین تعامل با دارایی‌ها متأثر از فرهنگی خواهد بود که در کتابخانه حاکم است. بنابراین مدیران کتابخانه‌ها باید بدانند که وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران در سطح سازمانی، سطح گروهی، سطح فردی و بعد تغییر چگونه است. بنابراین بررسی وضعیت آن‌ها به‌منظور شناسایی وضعیت فرهنگ امنیت اطلاعات در کتابخانه‌های تخصصی امری ضروری به شمار می‌آید.

به‌طور کلی تاکنون پژوهش‌های اندکی به بررسی فرهنگ امنیت اطلاعات پرداخته‌اند و معلوم نیست فرهنگ امنیت اطلاعات در کتابخانه‌های تخصصی پژوهشکده‌ها و پژوهشگاه‌ها در چه وضعیتی است. پژوهش حاضر بر آن است تا با بهره‌گیری از یکی از مدل‌های معتبر به بررسی وضعیت فرهنگ امنیت اطلاعات در کتابخانه‌های مراکز پژوهشی و تحقیقاتی بپردازد. در همین راستا به‌منظور انجام پژوهش از مدل فرهنگ امنیت اطلاعات مارتینز، به دلیل در نظر گرفتن مؤلفه‌های کلیدی مدیریتی متناسب با سطوح رفتار سازمانی رابینز و بعد تغییر، به‌عنوان مدلی که می‌توان با استفاده از آن به بررسی وضعیت فرهنگ امنیت اطلاعات و در نتیجه به القای تدریجی فرهنگ امنیت اطلاعات مطلوب در کتابخانه‌ها پرداخت، استفاده می‌شود.

با توجه به مسئله پژوهش، می‌توان بیان داشت که هدف اصلی پژوهش حاضر ارزیابی فرهنگ امنیت اطلاعات کتابخانه پژوهشکده‌ها و پژوهشگاه‌های فنی مهندسی مستقر در استان‌های تهران و البرز در ابعاد اصلی مدل فرهنگ امنیت اطلاعات مارتینز، (سطح سازمانی، گروهی، فردی و بعد تغییر) است.

برای رسیدن به اهداف پژوهش پرسش‌هایی به‌قرار زیر طرح شده است:

- وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران کتابخانه پژوهشکده‌ها و پژوهشگاه‌های فنی مهندسی استان‌های تهران و البرز در هر یک از ابعاد اصلی مدل (سطح سازمانی، گروهی، فردی و بعد تغییر) چگونه است؟
- وضعیت فرهنگ امنیت اطلاعات کتابخانه پژوهشکده‌ها و پژوهشگاه‌های فنی-مهندسی استان‌های تهران و البرز چگونه است؟
- آیا تفاوت معناداری در وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران کتابخانه پژوهشکده‌ها و پژوهشگاه‌های فنی-مهندسی استان‌های تهران و البرز در سطح سازمانی، سطح گروهی، سطح فردی و بعد تغییر وجود دارد؟

ادبیات پژوهش

مدل فرهنگ امنیت اطلاعات

مارتینز (۲۰۰۱) برای القای تدریجی فرهنگ امنیت اطلاعات در یک سازمان مدلی را ارائه کرد (مدل ۱). این مدل مبتنی بر سه سطح رفتار سازمانی منسوب به رابینز است که در هر یک از سطوح، مؤلفه‌های مهمی شناسایی و معرفی شدند و از آن‌ها در مدل به‌عنوان ابعاد فرعی یاد شده است. همچنین از آنجاکه فرهنگ مقوله‌ای است که به تغییر و استمرار در آن وابسته است، بعد تغییر به‌عنوان یک بعد اصلی که بر سه سطح دیگر اثر می‌گذارد؛ در نظر گرفته شده است. به‌طوری‌که ابعاد اصلی شناسایی شده عبارت‌اند از سطح سازمان، سطح گروهی، سطح فردی و بعد تغییر که در ادامه به تشریح هر یک پرداخته می‌شود:

سطح سازمان

تمام فرآیندها و ساختارها از سطح سازمانی شروع می‌شوند؛ فرآیندهایی مانند ارزیابی خطر و رویه‌هایی برای گزارش رویدادهای امنیتی که می‌بایستی گسترش یابند. خط‌مشی‌ها با فراهم آوردن یک طرح و چارچوب کلی، ساختارهایی برای فرآیندهای امنیت اطلاعات ایجاد می‌کنند تا از این طریق فرآیندها را کامل کنند (Martins & Eloff, 2002: 207). ساختارهایی که توسط سازمان اجرا شده‌اند بر نگرش افراد سازمان نفوذ کرده و در رفتار آن‌ها تأثیر می‌گذارند.

- خط‌مشی و رویه‌ها^۳: خط‌مشی امنیت اطلاعات از اهمیت فوق‌العاده‌ای برخوردار است و به‌عنوان پاشنه آشیل در حفاظت از اطلاعات و دارایی‌های اطلاعاتی در یک سازمان تعبیر می‌شود.

³ Policy & Procedures

خط‌مشی امنیت اطلاعات رفتار کارکنان را دیکته می‌کند و بیان می‌کند چه انتظاری از کارکنان می‌رود. ضروری است که رویه‌هایی برای حمایت از خط‌مشی امنیت اطلاعات در سازمان اعمال شود (Martins, 2001: 20).

- محک‌زنی^۴: ایده‌ای که پشت محک‌زنی وجود دارد، اندازه‌گیری فرایندهای داخلی در قیاس با استاندارد بیرونی است. در نتیجه، محک‌زنی در بسیاری از سازمان‌ها به‌منزله ابزاری برای رسیدن به مزیت رقابتی است (شورای علمی فارسی ... [و دیگران]، ۱۳۸۸: ۱۲۶۳). در اینجا محک‌زنی در ارتباط با مسائل امنیت اطلاعات، سازمان را قادر خواهد ساخت تا خودش را با سازمان‌های مشابه و استانداردهای بین‌المللی، مانند BS7799 مقایسه کند (Martins, 2001: 25).
- تحلیل خطر^۵: از طریق تحلیل خطر می‌توان دارایی‌های سازمان، تهدیدات مرتبط با آن‌ها و اقدامات امنیتی لازم را شناسایی کرد و خط‌مشی امنیت اطلاعات را توسعه داد. تحلیل خطر ممکن است بین سازمان‌ها متفاوت باشد (Martins & Eloff, 2002: 209).
- بودجه^۶: بودجه مناسب، ابزاری در اختیار مدیران است و رشد هر سازمانی نیز به‌طور مستقیم به آن بستگی دارد. نقش بودجه را می‌توان چنین برشمرد: (۱) به برنامه‌ریزی منظم و رشد یابنده کمک می‌کند؛ (۲) ابزاری در اختیار مدیریت است؛ (۳) ابزاری برای کنترل عملیات است؛ (۴) وسیله‌ای برای ارزیابی نتایج محسوب می‌شود (مرتضایی‌فرد، ۱۳۸۱: ۵۱۶-۵۱۵). در اینجا، وجود روشی برای سرمایه‌گذاری مالی برای اجرای امنیت اطلاعات در یک سازمان اهمیت دارد به‌طوری‌که سرمایه‌گذاری مالی برای امنیت باید به‌عنوان یک مولد سود بالقوه به نظر برسد (Martins, 2001: 28-29).

سطح گروهی

سطح گروهی بر روی رفتار افراد در گروه و چگونگی عملکرد خود گروه متمرکز است. برای مدیران بسیار مهم است که در مورد عضویت افراد در گروه‌ها تصمیم‌گیری کنند و با برقراری اعتماد در محیط کاری سازمان بتوانند موضوعات سطح سازمانی را به‌طور مطلوب عملی نمایند (Veiga & Eloff, 2010).

- مدیریت^۷: «جیمز استونر»^۸ و «ادوارد فریمان»^۹ معتقدند که مدیریت فرایندی است مشتمل بر سازمان‌دهی، برنامه‌ریزی، هدایت و کنترل تلاش‌های افراد سازمان و بهره‌برداری از سایر منابع سازمانی جهت نیل به اهداف تعیین‌شده سازمان (به نقل از تیمور نژاد، ۱۳۸۷: ۲۴). مدیریت چشم‌انداز و استراتژی موردنیاز را جهت حفاظت از دارایی‌های سازمان توسعه می‌دهد تا کارکنان

⁴ Benchmarking

⁵ Risk Analysis

⁶ Budget

⁷ Management

⁸ James Stoner

⁹ Edward Freeman

با به کار بستن آن‌ها در یک شیوه‌ی معین راهنمایی و بر اساس آن رفتار کنند (Martins & Eloff, 2002: 209)

- اعتماد: 'انظر «مایر» و همکارانش (۱۹۵۵) اعتماد به "میزان آسیب‌پذیری تمایلات و اشتیاق یک‌طرف تعامل به اقدامات طرف مقابل، بدون در نظر گرفتن توانایی کنترل و نظارتی که فرد برطرف مقابل دارد، اعتماد گفته می‌شود" (به نقل از مقیمی، ۱۳۸۲: ۱۳۹). مسلماً مهم‌ترین موضوع قابل‌بحث در اعتمادسازی تدریجی در یک محیط مبتنی بر دارایی‌های اطلاعاتی، امنیت اطلاعات است. اگر مدیریت به کارمندان و کارمندان به مدیریت اعتماد داشته باشند، به‌کارگیری رویه‌های جدید و راهنمایی کارمندان در خصوص امنیت اطلاعات از طریق تغییر رفتارها آسان‌تر است (Martins & Eloff, 2002: 209).

سطح فردی

سطح فردی اشاره به افرادی در سازمان‌ها دارد که دارای خصوصیات و ویژگی‌های شخصی مانند سن و وضعیت تأهل و یا خصوصیات شخصیتی، چارچوب عاطفی، ارزش‌ها و نگرش‌ها و یا مفروضات اساسی هستند (Veiga & Eloff, 2010). هرکدام از کارکنان یک سازمان به‌صورت فردی نگرش‌های خودشان را دارند که منجر به رفتاری خاص می‌شود. لازم است آن‌ها از فرآیندهایی که در دستورالعمل‌ها در سطح سازمانی تعریف شده، آگاه باشند تا مطابق آن رفتار کنند؛ از این‌رو رفتارشان موفقیت در سطوح گروه و سازمان را تعیین می‌کند (Martins & Eloff, 2002: 209).

- آگاهی^{۱۱}: یکی از جنبه‌ها و روش‌های غیر فنی برای حفاظت و مدیریت امنیت اطلاعات، آگاهی کارکنان است. توجه به این مقوله سبب می‌شود افراد نسبت به نقش و مسئولیت خود آگاه باشند. آگاهی از امنیت اطلاعات در همه افراد موجب تغییر رفتار و تقویت فعالیت‌های مناسب امنیتی می‌شود که به تدریج به فرهنگی در سازمان‌ها تبدیل خواهد شد (حسن‌زاده و جهانگیری، ۱۳۹۰: ۹۳). از این‌رو، اثربخشی کنترل‌های امنیت اطلاعات به میزان آگاهی کارکنانی که آن را اجرا و از آن استفاده می‌کنند، بستگی دارد.

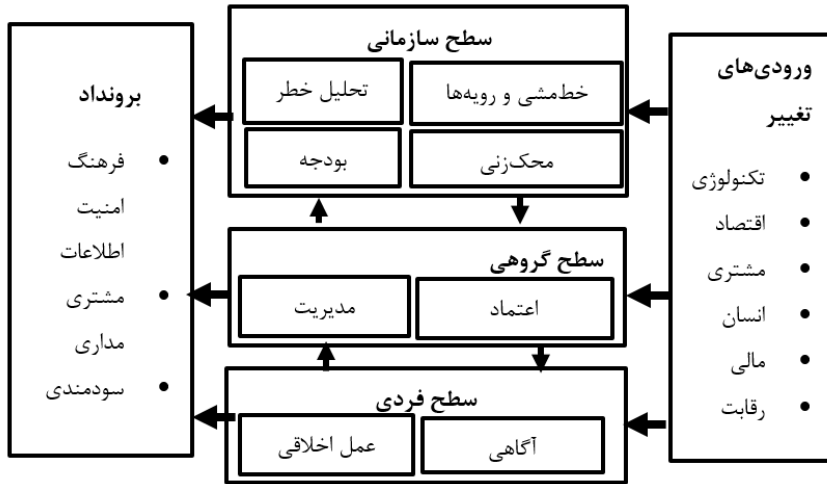
- عمل اخلاقی^{۱۲}: استفاده از اطلاعات و دارایی‌های اطلاعاتی باید با ادراکات ایجادشده توسط هنجارها و تعهدات اجتماعی مطابقت داشته باشد. اطلاعات باید به شیوه‌ای اخلاقی استفاده شود. شیوه صحیح از طریق قوانین یا نظارت در یک سازمان مشخص نمی‌شود بلکه باید بخشی از فرهنگی باشد که در سراسر سازمان ایجادشده است (Martins, 2001: 42).

بعد تغییر

تغییرات به‌صورت مستمر بر روی سطوح سازمانی، گروهی و فردی تأثیر می‌گذارد. اعمال تغییرات بر سطوح ذکرشده می‌بایستی در راستای تقویت نقاط قوت و برطرف نمودن نقاط ضعف باشد تا منجر به نهادینه

¹ Trust	0
¹ Mayer	1
¹ Awareness	2
¹ Ethical	3

کردن فرهنگ امنیت اطلاعات مطلوب در سازمان شود. به‌طور مثال، با در نظر گرفتن مؤلفه‌هایی از قبیل «فناوری»، «اقتصاد»، «مشتریان»، «امور مالی» و «رقابت» می‌توان بر هر یک از ابعاد فرعی موجود در سطوح رفتار سازمان [سازمانی، گروهی، فردی] تأثیر گذاشت و منجر به بروندهای مهمی از قبیل «فرهنگ امنیت اطلاعات»، «مشتری مداری» و «بهره‌وری» شد (Martins & Elof, 2002: 207).



مدل ۱. مدل فرهنگ امنیت اطلاعات (Martins 2001)

پیشینه پژوهش

آرین پور (۱۳۹۵) در پایان‌نامه خود تحت عنوان «میزان رعایت استانداردهای ایزو آی. ای. اس. ۲۷۰۰۲ و ۲۷۰۱۹ در حوزه مدیریت امنیت اطلاعات در سازمان اسناد و کتابخانه ملی جمهوری اسلامی ایران» به این نتیجه رسیدند که در این سازمان و در حوزه «مدیریت امنیت اطلاعات»، شش مؤلفه استاندارد حفاظت و مدیریت دارایی، نگهداری و ارتقای سامانه‌های امنیت اطلاعات، مدیریت منابع انسانی، طرح تداوم و مدیریتی کسب‌وکار، کنترل دسترسی به اطلاعات و سازگاری با قوانین، با درصد فراوانی ۵۰٪ رعایت می‌شوند. میزان رعایت مؤلفه «مدیریت حوادث امنیت اطلاعات و ضعف‌های امنیتی» در سازمان برابر با ۴۵/۶ درصد بود که این درصد برنامه‌ریزی قوی امنیتی سازمان را طلب می‌کند بطوریکه با تدابیر و استراتژی جدی سازمانی این مؤلفه به حد مطلوب برسد. نتایج تحقیق نشان می‌دهد سازمان اسناد و کتابخانه ملی جمهوری اسلامی ایران باید با در نظر گرفتن ملاک‌های امنیتی به‌کاررفته در استانداردهای ایزو، بتواند با استانداردهای جهانی نزدیکی بیشتری پیدا کند.

دانایی مقدم و ریاحی نیا (۱۳۹۳) در مقاله‌ای با عنوان «بررسی امنیت اطلاعات در وب‌سایت کتابخانه‌های دیجیتال در ایران» نشان دادند که وضعیت امنیت اطلاعات در کتابخانه‌های دیجیتالی در ایران در سطح متوسط ریسک‌پذیری است و بیشترین نقاط آسیب‌پذیر نسخه پشتیبان، حمله تزریق کد و شیء قابل دانلود شناخته شدند.

عاشوری زاده (۱۳۹۱) در پایان‌نامه خود رابطه فرهنگ‌سازمانی را با مدیریت امنیت اطلاعات در بانک ملی ایران مورد مطالعه قرارداد. نتایج این پایان‌نامه حاکی از وجود ارتباط معنادار بین فرهنگ‌سازمانی با مدیریت امنیت اطلاعات و همچنین وجود ارتباط معنادار بین فرهنگ مشارکتی، مثبت و اثربخشی با مدیریت امنیت اطلاعات و فقدان وجود رابطه معناداری بین فرهنگ نوآوری با مدیریت امنیت اطلاعات بود.

حریری و نظری (۱۳۹۱) در مقاله‌ای با عنوان «امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران» نشان دادند که ۷۵/۵۵ درصد از کتابخانه‌های دیجیتالی ایران به لحاظ امنیت اطلاعات در سطح قوی و ۲۴/۴۶ درصد در سطح متوسط بودند که آسیب‌پذیرترین نقاط امنیتی، «خطمشی امنیتی» و «امنیت نیروی انسانی» هر دو با میانگین ۰/۶۳ بود.

حسن‌زاده، کریم زادگان مقدم، و جهانگیری (۱۳۹۰) در مقاله‌ای با عنوان «ارائه یک چارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران»، نشان دادند که از بین هفت متغیر مستقل، متغیرهای آشنایی با مهارت فناوری اطلاعات، درجه سازمانی، رشته تحصیلی و رده شغلی کارمندان با پرمایگی آگاهی از امنیت اطلاعات آنان دارای همبستگی بود. نتیجه‌گیری از یافته‌ها نشان داد که اولاً، سازمان‌ها بایستی علاوه بر سرمایه‌گذاری بر راه‌حل‌های فنی برای حفظ امنیت اطلاعات، به عوامل غیر فنی و انسانی از جمله ارتقای سطح آگاهی کلیه کارمندان از مؤلفه‌های امنیت اطلاعات، توجه بیشتری داشته باشند. ثانیاً، در برنامه‌ریزی آموزش امنیت اطلاعات به کارکنان بایستی درجه سازمانی، رشته تحصیلی و رده شغلی آن‌ها مورد توجه قرار بگیرد تا آموزش‌ها مؤثر واقع شوند.

اسفندیار پور (۱۳۸۹) در پایان‌نامه خود تحت عنوان «عوامل مؤثر بر پذیرش سیاست‌های امنیت اطلاعات توسط کارمندان در سازمان»، نتیجه گرفت تعهد سازمانی و تأثیرات اجتماعی تأثیر فزاینده‌ای در پذیرش سیاست‌های امنیت اطلاعات دارد و در دسترس بودن منابع یک عامل تأثیرگذار در ارتقای خودباوری و همچنین یک عامل پیش‌بینی‌کننده در پذیرش سیاست‌های امنیت اطلاعات است.

در مقاله‌ای با عنوان «قصد شکل دادن به مقاومت در برابر مهندسی اجتماعی از طریق رهبری تحول آمیز، آگاهی و فرهنگ امنیت اطلاعات»، عوامل فردی و سازمانی را در شکل‌دهی قصد کارمندان برای مقاومت در برابر مهندسی اجتماعی مورد بررسی قرار گرفت. نتایج نشان داد نگرش نسبت به مقاومت در برابر مهندسی اجتماعی وابستگی مستقیم و زیادی با قصد مقاومت در برابر مهندسی اجتماعی دارد. درحالی‌که خودکارآمدی و باورهای هنجاری رابطه‌ی ضعیفی با قصد مقابله با مهندسی اجتماعی دارد. همچنین رهبری تحول آمیز وابستگی زیادی با فرهنگ امنیت اطلاعات و آگاهی امنیت اطلاعات دارد (Flores & Ekstedt, 2016).

در مقاله‌ای با عنوان «تأثیرات فراگیر برنامه‌های امنیت اطلاعات بر فرهنگ امنیت اطلاعات»، مدلی برای ارزیابی تأثیر مؤلفه‌های کلیدی برنامه‌های امنیت اطلاعات (شامل خطمشی‌های امنیت، برنامه‌های آگاهی، تربیت و آموزش امنیتی، و آگاهی‌دهنده‌های امنیتی) روی فرهنگ امنیت پیشنهاد شد. نتایج پژوهش نشان از تأثیر معنادار برنامه‌های امنیت اطلاعات و آگاهی‌دهنده‌های امنیتی و آگاهی کارمندان از خطمشی امنیت سازمان بر فرهنگ امنیت سازمان داشت (Chen, Ramamurthy & Wen, 2015).

در مقاله‌ای با عنوان «تأثیرات فرهنگ‌سازمانی روی فرهنگ امنیت اطلاعات: مطالعه موردی» نتیجه‌گیری شد که فرهنگ‌سازمانی بر فرهنگ امنیت اطلاعات، تأثیرگذار است و همچنین بین آن‌ها رابطه علی قوی وجود دارد. در همین راستا به ارائه یک چارچوب نظری جهت تبیین ارتباط بین فرهنگ‌سازمانی هافستد (فرایند‌گرایی و نتیجه‌گرایی، شغل‌گرایی و شاغل‌گرایی، دیدگاه محدود و دیدگاه حرفه‌ای، سیستم باز و سیستم بسته، کنترل نظام‌مند و کنترل غیر نظام‌مند، و دیدگاه هنجاری و دیدگاه عمل‌گرا) و چهار بعد فرهنگ امنیت اطلاعات (سازگاری، ارتباطات، پاسخگویی و نظارت) پرداختند (Tang, Li & Zhang, 2015).

در پژوهشی با عنوان «تعیین عوامل تأثیرگذار بر فرهنگ امنیت اطلاعات کتابداران فناوری اطلاعات و ارتباطات کالج‌های خصوصی»، فرهنگ امنیت اطلاعات و عوامل مؤثر بر آن مورد مطالعه قرار گرفت. نتایج پژوهش نشان از تأیید فرض وجود تأثیرگذاری اصول و رویه‌ها بر فرهنگ امنیت اطلاعات کتابداران و رد فرض تأثیرگذاری «سطوح رفتار سازمانی رابینز»، «سطوح فرهنگ‌سازمانی شاین» و «کنترل‌های امنیتی» بر فرهنگ امنیت اطلاعات کتابداران داشت (SaziliShahibi et al., 2012).

در مقاله‌ای تحت عنوان «فرهنگ امنیت اطلاعات در بیمارستان عمومی: مطالعه موردی بیمارستان هاواسا رفال»^۱ محققان نشان دادند ۶۶/۹ درصد از جامعه مورد مطالعه نمی‌دانستند امنیت اطلاعات بر چه چیزی دلالت دارد. ۹۲/۸ درصد از وجود خطمشی امنیت اطلاعات در سازمان اطلاع نداشتند. ۵۶/۲ درصد معتقد بودند که مدیریت در اجرای موضوعات امنیت اطلاعات تعهدی ندارد و پشتیبانی به عمل نمی‌آورد. ۸۴/۹ درصد نمی‌دانستند موضوع امنیت اطلاعات با موضوع شغلی‌شان در ارتباط است. ۵۷/۶ درصد آن‌ها مطمئن نبودند که به خطمشی امنیت اطلاعات وفادار باشند. بنابراین نتیجه گرفته شد که بررسی عملکردهای جاری مرتبط با امنیت اطلاعات در تنظیم اولویت‌های مربوط به امنیت اطلاعات در بیمارستان کمک کاربردی خواهد داشت. همچنین تدوین خطمشی مناسب و توسعه رویه‌ها و دستورالعمل‌هایی در راستای اجرای خطمشی امنیت اطلاعات در این زمینه مثمر ثمر خواهد بود. علاوه بر آن، برنامه‌های آموزشی و آگاهی‌رسانی نیز برای رفتار امنیت اطلاعات مناسب در بیمارستان ضرورت بسیار دارد. حمایت و پشتیبانی مدیریت در راستای این مهم ضمانت اجرایی را به دنبال خواهد داشت (Gebrasilase & Lessa, 2011).

در مقاله‌ای دیگر به پیشنهاد چارچوبی برای ترویج فرهنگ امنیت اطلاعات و چگونگی به‌کارگیری آن پرداخته شد. مشروح ساختار چارچوب پیشنهادی از این‌قرار بود که هفت مؤلفه مربوط به امنیت اطلاعات (رهبری و نظارت در سازمان، مدیریت امنیت و عملیات، خطمشی امنیت، برنامه‌های امنیتی مدیریت، مدیریت امنیت کاربر، حفاظت فناوری و عملیات و تغییر) با تأثیرگذاری بر رفتار امنیت اطلاعات کارکنان در سطوح رفتار سازمانی (سطح سازمانی، گروهی و فردی) منجر به نهادینه شدن فرهنگ امنیت اطلاعات در سطوح فرهنگ‌سازمانی (مفروضات، ارزش‌ها و مصنوعات) افراد خواهد شد. مدیران می‌توانند با استفاده از این چارچوب، به برنامه‌ریزی راهبردی جهت ارائه رهنمود به کارکنان در مورد نحوه پرورش فرهنگ امنیت اطلاعات بپردازند (Veiga & Eloff, 2010). در پژوهشی دیگر با عنوان «بررسی فرهنگ امنیت

¹ Hawassa Referral Hospital

اطلاعات»، نشان داده شد که وضعیت درک و نگرش پاسخ‌دهندگان مورد مطالعه در سطح سازمانی به میزان ۵۲/۸ درصد در سطح متوسط، در سطح گروهی به میزان ۷۵/۵ درصد و در سطح فردی به میزان ۷۰/۴ درصد در سطح خوب قرار داشت. نتایج حاصل حاکی از آن بود که سطح سازمانی یکی از محدوده‌های اصلی توسعه فرهنگ امنیت اطلاعات بود که نیاز به توجه و رسیدگی داشت. به‌طور کلی سطح قابل قبولی از فرهنگ امنیت اطلاعات در سطح گروهی و فردی وجود داشت. اما بعد مدیریت در سطح گروهی نیاز به توجه و رسیدگی داشت (Martins, 2001).

در مجموع بررسی پیشینه‌ها نشان داد که سطح فرهنگ امنیت اطلاعات در نهادهای اطلاعات محور هنوز مورد توجه واقع نشده و در سطح متوسط به پایین ارزیابی می‌شود.

روش‌شناسی پژوهش

پژوهش حاضر به لحاظ هدف، کاربردی و از لحاظ روش گردآوری و تجزیه و تحلیل داده‌ها از نوع توصیفی - پیمایشی محسوب می‌شود. برای انتخاب نمونه آماری پژوهش از روش نمونه‌گیری غیر احتمالی هدفمند استفاده شد. در نتیجه کتابخانه‌ی ۱۹ پژوهشکده و پژوهشگاه فعال در زمینه فنی-مهندسی مستقر در استان‌های تهران و البرز به‌عنوان نمونه آماری انتخاب شدند و ۶۰ کتابدار شاغل در این کتابخانه‌ها با روش سرشماری انتخاب و مورد مطالعه قرار گرفتند.

ابزار گردآوری داده‌ها پرسشنامه محقق ساخته بر مبنای مدل فرهنگ امنیت اطلاعات مارتینز بود که باهدف نگرش سنجی کتابداران از وضعیت موجود امنیت اطلاعات در کتابخانه‌های تخصصی طراحی شد. این پرسشنامه به سنجش درک، نگرش و رفتارهای کتابداران نسبت به جنبه‌های امنیتی اطلاعات و هرگونه دارایی اطلاعاتی در هر محل و هر قالبی که قابل استفاده است، برآمده است. پرسشنامه در دو بخش سؤالات جمعیت شناختی و سؤالات فرهنگ امنیت اطلاعات، متشکل از ۴۷ گویه با مقیاس پنج ارزشی لیکرت تدوین شد. به‌منظور سنجش اعتبار پرسشنامه محقق ساخته، از شیوه اعتبار محتوا استفاده شد که اعتبار صوری و محتوایی آن پس از بررسی دقیق متخصصان فعال و صاحبان فن در دو زمینه موضوعی فرهنگ سازمانی و امنیت اطلاعات مورد تأیید قرار گرفت. برای سنجش پایایی پرسشنامه از ضریب آلفای کرونباخ استفاده شد. بر اساس نتایج به‌دست آمده، پایایی پرسشنامه توسط ضریب آلفای کرونباخ به‌صورت کلی و نیز برای هر یک از ابعاد اصلی مدل فرهنگ امنیت اطلاعات مارتینز محاسبه شد که عدد قابل قبولی برای هر یک به دست آمد. ضریب آلفای به‌دست آمده برای مجموع ابعاد ۰.۹۵۷ بود.

یافته‌های پژوهش

وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران در ابعاد اصلی مدل (سطح سازمانی، گروهی، فردی و بعد تغییر)؛

پاسخ به این پرسش در چهار بخش صورت گرفته است، که در ادامه به تشریح آن‌ها پرداخته می‌شود.

بخش اول: وضعیت درک، نگرش و رفتار امنیت کتابداران در سطح سازمانی؛

اولین بعد اصلی مورد بررسی در این پژوهش سطح سازمانی است که خود متشکل از چهار بعد فرعی با عنوان خطمشی و رویه‌ها، محک‌زنی، تحلیل خطر و بودجه است که از مجموع محاسبه این ابعاد، سطح سازمانی محاسبه می‌شود. در مجموع، گویه‌های ۱ تا ۱۷ که در قالب طیف لیکرت در پرسشنامه آمده است، سطح سازمانی را هدف قرار داده است.

جدول ۱. وضعیت درک، نگرش و رفتار امنیت کتابداران در سطح سازمانی

شاخص‌های آماری						درصد تجمعی	درصد فراوانی	فراوانی	سطح سازمانی
ابعاد	خطمشی و رویه‌ها	محک‌زنی	تحلیل خطر	بودجه	سطح سازمانی	۲۰	۲۰	۱۲	خیلی کم
میانگین	۱۵/۷۸	۸/۰۷	۱۱/۸۲	۵/۳	۴۰/۹۷	۶۳/۳	۴۳/۳	۲۶	کم
میان	۱۵	۸	۱۱	۵	۴۱	۹۱/۷	۲۸/۳	۱۷	متوسط
نما	۱۵	۸	۱۱	۴	۴۰	۱۰۰	۸/۳	۵	زیاد
انحراف استاندارد	۴/۷۲۷	۲/۷۱۱	۳/۸۸۶	۲/۳۰۲	۱۱/۵۹۵	۱۰۰	۰	۰	خیلی زیاد
واریانس	۲۲/۳۴۲	۷/۳۵۱	۱۵/۱۰۱	۵/۲۹۸	۱۳۴/۴۴		۱۰۰	۶۰	کل

همان‌گونه که جدول ۱ نشان می‌دهد، از مجموع ۶۰ کتابدار شرکت‌کننده در پژوهش، درک، نگرش و رفتار امنیت اطلاعات ۶۳/۳ درصد از کتابداران در وضعیت ضعیف، ۲۸/۳ درصد در حد متوسط و فقط ۸/۳ درصد از آن‌ها در وضعیت خوبی قرار دارند. شاخص‌های آماری به ما نشان می‌دهند نیمی از کتابداران نمره کمتر از ۴۱ و نیمی دیگر نمره بیش از ۴۱ کسب کرده‌اند. بیشتر آن‌ها نمره ۴۰ را به دست آورده‌اند. میانگین پاسخ‌ها عدد ۴۰/۹۷ است. انحراف استاندارد نیز ۱۱/۵۹۵ است که بیانگر پراکندگی نسبتاً کم پاسخ‌ها است.

بخش دوم: وضعیت درک، نگرش و رفتار امنیت کتابداران در سطح گروهی؛

دومین بعد اصلی مورد بررسی پژوهش حاضر سطح گروهی است که خود متشکل از دو بعد فرعی با عنوان مدیریت و اعتماد است که از مجموع محاسبه این ابعاد، سطح سازمانی محاسبه می‌شود. گویه‌های ۱۸ تا ۲۷ که در قالب طیف لیکرت در پرسشنامه آمده، در مجموع، سطح گروهی را مورد توجه قرار می‌دهند.

جدول ۲. وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران در سطح گروهی

شاخص‌های آماری				درصد تجمعی	درصد فراوانی	فراوانی	سطح گروهی
ابعاد	مدیریت	اعتماد	سطح گروهی	۲۵	۲۵	۱۵	خیلی کم
میانگین	۱۲/۱۸	۹/۵۵	۲۱/۷۳	۸۰	۵۵	۳۳	کم
میان	۱۲	۹	۲۱	۹۶/۷	۱۶/۷	۱۰	متوسط
نما	۱۲	۹	۲۱	۱۰۰	۳/۳	۲	زیاد

خیلی زیاد	۰	۰	۱۰۰	انحراف استاندارد	۳/۸۲۵	۲/۷۱۵	۵/۷۴۳
کل	۶۰	۱۰۰		واریانس	۱۴/۶۲۷	۷/۳۷	۳۲/۹۷۹

همان‌گونه که جدول ۲ نشان می‌دهد، درک، نگرش و رفتار امنیت اطلاعات ۸۰ درصد از کتابداران در سطح گروهی در سطح ضعیف، ۱۶/۷ درصد در حد متوسط و فقط ۳/۳ درصد در سطح بالایی قرار دارد. شاخص‌های آماری به ما نشان می‌دهند میانگین ۲۱/۷۳ و میانه و نما عدد ۲۱، تمرکز شاخص‌های گرایش به مرکز بر روی نمره ۲۱ و انحراف استاندارد ۵/۷۴۳ است که پراکندگی به نسبت کم را نشان می‌دهد.

بخش سوم: وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران در سطح فردی؛

سومین بعد اصلی مورد بررسی پژوهش حاضر سطح فردی است که خود متشکل از دو بعد فرعی با عنوان آگاهی و عمل اخلاقی است که از مجموع محاسبه این ابعاد، سطح فردی محاسبه می‌شود. گویه‌های ۲۸ تا ۳۹ که در قالب طیف لیکرت در پرسشنامه آمده است، در مجموع، سطح فردی را تشکیل می‌دهند.

جدول ۳. وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران در سطح فردی

شاخص‌های آماری				درصد تجمعی	درصد فراوانی	فراوانی	سطح فردی
سطح فردی	عمل اخلاقی	آگاهی	ابعاد	۳۱/۷	۳۱/۷	۱۹	خیلی کم
۲۴/۶۷	۶/۵۳	۱۸/۱۳	میانگین	۸۵	۵۳/۳	۳۲	کم
۲۶	۷	۱۸	میانه	۹۸/۳	۱۳/۳	۸	متوسط
۲۶	۸	۱۷	نما	۱۰۰	۱/۷	۱	زیاد
۷/۱۹۹	۲/۵۰۱	۵/۳۶۶	انحراف استاندارد	۱۰۰	۰	۰	خیلی زیاد
۵۱/۸۱۹	۶/۲۵۳	۲۸/۷۹۵	واریانس		۱۰۰	۶۰	کل

جدول ۳ نشان می‌دهد که درک، نگرش و رفتار امنیت اطلاعات ۸۵ درصد از کتابداران نسبت به این بعد در سطح پایین، ۱۳/۳ درصد در حد متوسط و فقط ۱/۷ درصد از آن‌ها در سطح بالایی قرار دارد. در میان شاخص‌های آماری، برای میانه و نما نمره ۲۶ و میانگین نمره ۲۴/۶۷ به دست آمده است. انحراف استاندارد ۷/۱۹۹ است که پراکندگی نسبتاً کم نمرات به دست آمده را نشان می‌دهد.

بخش چهارم: وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران در بعد تغییر؛

چهارمین بعد اصلی مورد بررسی بعد تغییر است که فرهنگ امنیت اطلاعات کتابداران را در سه سطح بررسی می‌کند. گویه‌های ۴۰ تا ۴۷ که در قالب طیف لیکرت در پرسشنامه آمده است، در مجموع، بعد تغییر را می‌سنجند.

جدول ۴. وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران در بعد تغییر

بعد تغییر	فراوانی	درصد فراوانی	درصد تجمعی	شاخص‌های آماری
-----------	---------	--------------	------------	----------------

۱۷/۱۳	میانگین	۲۸/۳	۲۸/۳	۱۷	خیلی کم
۱۶	میانه	۷۵	۴۶/۷	۲۸	کم
۱۶	نما	۹۶/۷	۳۱/۷	۱۳	متوسط
۵/۵۶۸	انحراف استاندارد	۱۰۰	۳/۳	۲	زیاد
۳۰/۹۹۹	واریانس	۱۰۰	۰	۰	خیلی زیاد
			۱۰۰	۶۰	کل

جدول ۴ نشان می‌دهد که درک، نگرش و رفتار امنیت اطلاعات ۷۵ درصد از کتابداران نسبت به این بعد در سطح ضعیف، ۲۱/۷ درصد در سطح متوسط و فقط ۳/۳ درصد در سطح بالایی قرار دارند. نمرات میانه و نما ۱۶ و میانگین ۱۷/۱۳ است. انحراف استاندارد رقم ۵/۵۶۸ است که پراکندگی نمرات از میانگین به نسبت کم است.

وضعیت فرهنگ امنیت اطلاعات کتابخانه پژوهشکده‌ها و پژوهشگاه‌های فنی مهندسی؛

نظر به اینکه هدف پژوهش حاضر ارزیابی فرهنگ امنیت اطلاعات کتابخانه پژوهشکده‌ها و پژوهشگاه‌های تخصصی فعال در زمینه فنی-مهندسی استان‌های تهران و البرز است؛ از مجموع ۶۰ پرسشنامه‌ی توزیع شده در بین آزمون‌های پژوهش، کل ابعاد با هم جمع بسته شد و متغیر فرهنگ امنیت اطلاعات به دست آمده است (جدول ۵).

جدول ۵. وضعیت فرهنگ امنیت اطلاعات کتابخانه پژوهشکده‌ها و پژوهشگاه‌های فنی-مهندسی

شاخص‌های آماری		درصد تجمعی	درصد فراوانی	فراوانی	فرهنگ امنیت اطلاعات
۱۰۴/۵	میانگین	۲۵	۲۵	۱۵	خیلی کم
۱۰۵/۵	میانه	۷۶/۷	۵۱/۷	۳۱	کم
۱۰۵	نما	۱۰۰	۲۳/۳	۱۴	متوسط
۲۵/۸۲۴	انحراف استاندارد	۱۰۰	۰	۰	زیاد
۶۶۶/۸۹۸	واریانس	۱۰۰	۰	۰	خیلی زیاد
			۱۰۰	۶۰	کل

داده‌های جدول ۵ نشان می‌دهد که فرهنگ امنیت اطلاعات ۷۶/۶ درصد کتابخانه‌ها در سطح ضعیف و ۲۳/۳ درصد در حد متوسط است. شاخص‌های آماری نشان می‌دهند که میانه و نما حدود نمره ۱۰۵ و میانگین ۱۰۴/۵ است که از حد وسط مقیاس حدود ۳۶ نمره کمتر است. انحراف استاندارد ۲۵/۸۲۴ به دست آمده که پراکندگی اندک پاسخ‌ها را از میانگین نشان می‌دهد.

آیا وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران کتابخانه پژوهشکده‌ها و پژوهشگاه‌های تخصصی در سطح سازمانی، سطح گروهی، سطح فردی و بعد تغییر باهم تفاوت معناداری دارد؟

در ادامه برای پاسخ به این سؤال از آزمون تحلیل واریانس یک‌طرفه استفاده شده که مطابق با جدول ۶، مقدار $F=10.3/115$ است و در سطح خطای کوچک‌تر از ۰/۰۱ و با اطمینان ۰/۹۹ درصد تفاوت معنادار را

نشان می‌دهد. بنابراین با ۹۹ درصد اطمینان می‌توان گفت که بین نمره میانگین درک، نگرش و رفتار امنیت اطلاعات کتابداران در سطح سازمانی، سطح گروهی، سطح فردی و بعد تغییر تفاوت معناداری وجود دارد.

جدول ۶. نتایج آزمون تحلیل واریانس یک‌طرفه در چهار بعد اصلی فرهنگ امنیت اطلاعات

منبع تغییرات	مجموع مجزورات	درجه آزادی	میانگین مربعات	مقدار F	سطح معناداری	تفاوت
واریانس بین گروهی	۱۹۳۵۲/۳۱۷	۳	۶۴۵۰/۷۷۲	۱۰۳/۱۱۵	۰/۰۰۰	۰/۰۰۰
واریانس درون گروهی	۱۴۷۶۳/۹۳۳	۲۳۶	۶۲/۵۵۹			
واریانس کل	۳۴۱۱۶/۲۵۰	۲۳۹				

در مرحله بعد، به منظور تبیین دقیق‌تر و پیگیری تفاوت گروه‌ها از آزمون شفه استفاده شد. جدول ۷ نتایج حاصل از این آزمون را نشان می‌دهد.

جدول ۷. آزمون شفه در ارتباط ابعاد فرهنگ امنیت اطلاعات

ابعاد اصلی	دیگر ابعاد اصلی	تفاوت میانگین‌ها	خطای معیار	سطح معناداری
سطح سازمانی	سطح گروهی	۱۹/۲۳۳	۱/۴۴۴	۰/۰۰۰
	سطح فردی	۱۶/۳۰۰	۱/۴۴۴	۰/۰۰۰
	بعد تغییر	۲۳/۸۳۳	۱/۴۴۴	۰/۰۰۰
سطح گروهی	سطح سازمانی	-۱۹/۲۳۳	۱/۴۴۴	۰/۰۰۰
	سطح فردی	-۲/۹۳۳	۱/۴۴۴	۰/۲۵۱
	بعد تغییر	۴/۶۰۰	۱/۴۴۴	۰/۰۱۹
سطح فردی	سطح سازمانی	-۱۶/۳۰۰	۱/۴۴۴	۰/۰۰۰
	سطح گروهی	۲/۹۳۳	۱/۴۴۴	۰/۲۵۱
	بعد تغییر	۷/۵۳۳	۱/۴۴۴	۰/۰۰۰
بعد تغییر	سطح سازمانی	-۲۳/۸۳۳	۱/۴۴۴	۰/۰۰۰
	سطح گروهی	-۴/۶۰۰	۱/۴۴۴	۰/۰۱۹
	سطح فردی	-۷/۵۳۳	۱/۴۴۴	۰/۰۰۰

جدول ۷ بیانگر آن است که بین میانگین وضعیت درک و رفتار امنیت کتابداران در سطح سازمانی با سطح گروهی، میانگین سطح سازمانی با سطح فردی، میانگین سطح سازمانی با بعد تغییر در سطح خطای کوچک‌تر از ۰/۰۱ تفاوت معناداری وجود دارد. میانگین سطح گروهی با میانگین سطح فردی در سطح خطای بزرگ‌تر از ۰/۰۵ تفاوت معناداری ندارد و نمره میانگین آن‌ها نزدیک به هم است. میانگین سطح گروهی با میانگین بعد تغییر در سطح خطای کوچک‌تر از ۰/۰۵ تفاوت معناداری ندارد؛ در اینجا سطح خطای کمی بالا و تفاوت میانگین نیز کم (۴/۱۶) است. همچنین میانگین سطح فردی با میانگین بعد تغییر در سطح خطای کوچک‌تر از ۰/۰۱ تفاوت معناداری دارد.

در جدول ۸ میانگین ابعاد اصلی فرهنگ امنیت اطلاعات به ترتیب از کمترین به بیشترین و به صورت صعودی نمایش داده شده است. با توجه به مقایسه میانگین‌ها و ترتیب آن‌ها، میانگین فرهنگ امنیت اطلاعات در بعد تغییر (۱۷/۱۳) کمتر از سایر میانگین‌ها است و در ستون اول قرار گرفته، میانگین سطح گروهی

(۲۱/۷۳) و سطح فردی (۲۴/۶۷) در ستون دوم قرار گرفته است. همان گونه که اشاره شد، میانگین سطح گروهی و سطح فردی باهم تفاوت معناداری ندارند و بسیار اندک است. بنابراین میانگین هر دو در یک رتبه قرار می‌گیرند. میانگین سطح سازمانی (۴۰/۹۷) است که بیشتر از سایر میانگین‌ها است و در ستون سوم قرار می‌گیرد.

جدول ۸. بررسی تفاوت میانگین ابعاد اصلی فرهنگ امنیت اطلاعات

زیرمجموعه آلفا = ۰/۰۵			فراوانی	ابعاد اصلی فرهنگ امنیت اطلاعات
۳	۲	۱		
		۱۷/۱۳	۶۰	بعد تغییر
	۲۱/۷۳		۶۰	سطح گروهی
	۲۴/۶۷		۶۰	سطح فردی
۴۰/۹۷			۶۰	سطح سازمانی

نتیجه‌گیری

نتایج این پژوهش نشان داد که درک، نگرش و رفتار امنیت اطلاعات کتابداران کتابخانه پژوهشکده‌ها و پژوهشگاه‌های فنی مهندسی استان‌های تهران و البرز در سطح سازمانی در سطح مطلوبی قرار ندارد. نتایج به‌دست‌آمده در این بخش از پژوهش حاضر هم‌سو با نتایج ارائه‌شده در پژوهش مارتینز (۲۰۰۱) است و بنابراین آن است که سطح سازمانی نیاز به توجه و رسیدگی ویژه‌ای دارد.

در تبیین نتیجه به‌دست‌آمده، می‌توان گفت خط‌مشی امنیت اطلاعات به‌عنوان نقطه شروعی برای پیاده‌سازی امنیت اطلاعات در سازمان تلقی می‌شود که باید به‌صورت مکتوب و با رعایت دو اصل سهولت دسترسی و سهولت استفاده تدوین شود. هدف از تدوین آن انعکاس بهتر اهداف سازمان مادر و کتابخانه است بنابراین باید برای حمایت از هر خط‌مشی رویه‌هایی که در حکم ضمانت اجرایی برای آن هستند، در کتابخانه اعمال شوند. پژوهش اسفندیار پور (۱۳۸۹)، حریری و نظری (۱۳۹۱) و چن، رامامورتی و ون^{۱۵} (۲۰۱۵) نیز بر اهمیت همین موضوع تأکید دارند.

محک‌زنی به‌منزله ابزاری برای رسیدن به مزیت رقابتی محسوب می‌شود که هر کتابخانه‌ای برای دستیابی به این هدف باید به‌صورت مستمر مقررات و فعالیت‌های در حال اجرا را با استانداردهای بین‌المللی و کتابخانه‌های مشابه مقایسه کند و پس از شناسایی نقاط ضعف آن‌ها را با ایده «بهترین بهترین‌ها» شدن بهبود بخشد. از سوی دیگر، باید برنامه مدونی به‌منظور تعیین نیازهای امنیت اطلاعات و ارزیابی خطر در کتابخانه صورت پذیرد. پس وجود تیم یا مقام مسئول در کتابخانه برای طبقه‌بندی اطلاعات و دارایی‌های اطلاعاتی بر اساس اهمیتشان در کتابخانه ضرورت دارد.

آخرین بعد سطح سازمانی نیز بودجه است. پیاده‌سازی امور حائز اهمیت نیازمند داشتن پشتوانه‌ی مالی درخور توجه است. در اینجا دیدگاه مطلوب آن است که کتابخانه باید به سرمایه‌گذاری در ارتباط با مسائل

امنیتی به‌عنوان سرمایه‌گذاری برای آینده نگاه کند و مدیران کتابخانه باید سرمایه‌گذاری در مسائل امنیتی را در برنامه‌ریزی بودجه‌ی سالانه خود در نظر داشته باشند.

به‌علاوه نتایج نشان داد که درک، نگرش و رفتار امنیت اطلاعات کتابداران کتابخانه پژوهشکده‌ها و پژوهشگاه‌های فنی-مهندسی استان‌های تهران و البرز در سطح گروهی در وضعیت مطلوبی قرار ندارد. نتایج به‌دست‌آمده در این بخش هم‌راستا با یافته‌ی پژوهش صورت گرفته توسط مارتینز (۲۰۰۱) نیست. این امر نشان از حمایت و پشتیبانی مدیریت و روحیه کاری مبتنی بر اعتماد میان مدیر و کارکنان در جامعه مورد مطالعه پژوهش مارتینز (۲۰۰۱) دارد. از آنجاکه سطح گروهی بر روی رفتار افراد در گروه و چگونگی عملکرد خود گروه متمرکز است، برای مدیران بسیار مهم است که در مورد عضویت افراد در گروه‌ها تصمیم‌گیری کنند (به‌طور مثال گروه، تیم و یا کمیته) و با برقراری اعتماد در محیط کاری سازمان بتوانند موضوع‌های سطح سازمانی را به‌طور مطلوب عملی نمایند.

در جامعه پژوهش، برای ناآل شدن به فرهنگ امنیت اطلاعات باید به دو بعد تشکیل‌دهنده این سطح توجه و رسیدگی شود. در تبیین نتیجه به‌دست‌آمده، می‌توان گفت که مدیریت برای نیل به اهداف تعیین‌شده سازمان باید هنگام سازمان‌دهی، برنامه‌ریزی، هدایت و کنترل توجه مناسبی به مقوله امنیت اطلاعات در کتابخانه داشته باشد. از این طریق که با جهت‌گیری شفاف، اعلام مسئولیت‌ها و تعیین نقش‌های کتابداران در فرایند سازمان‌دهی، مشخص کردن ملزومات امنیتی موردنیاز در کتابخانه در فرایند برنامه‌ریزی، انتقال مسائل مربوط به امنیت اطلاعات مرتبط با نیازهای شغلی کتابداران در فرایند هدایت و بالآخره با دخالت کتابداران متناسب با شرح وظایفشان در اخذ تصمیمات مربوط به مسائل امنیت اطلاعات در فرایند کنترل، موجبات ایجاد فرهنگ امنیت اطلاعات مطلوب را فراهم نماید که نتایج به‌دست‌آمده از پژوهش عاشوری زاده (۱۳۹۱) و جبراسیلاس و لسا^۱ (۲۰۱۱) نیز تأکید بر اهمیت آن دارد. در ادامه باید گفت که به دلیل عدم وجود اعتماد در فضای کاری در کتابخانه، به‌کارگیری مسائل مربوط به امنیت اطلاعات کاری مشکل است و تأثیر منفی بر آن دارد. سطح فردی به جنبه‌های فردی کتابداران در کتابخانه اشاره دارد که این جنبه‌ها می‌تواند به دودسته تقسیم شوند؛ یکی بیانگر خصوصیات و ویژگی‌های شخصی مانند سن و با وضعیت تأهل و دیگری به جنبه‌ها و خصوصیات شخصیتی، چارچوب عاطفی، ارزش‌ها و نگرش‌های هر فرد اشاره دارد که در اینجا مورد دوم موردبررسی است. نتایج نشان داد که درک، نگرش و رفتار امنیت اطلاعات کتابداران کتابخانه پژوهشکده‌ها و پژوهشگاه‌های فنی-مهندسی استان‌های تهران و البرز در سطح فردی در وضعیت نامطلوبی قرار دارد و غیرقابل قبول ارزیابی می‌شود که نتایج حاصل از پژوهش مارتینز (۲۰۰۱) با نتیجه پژوهش حاضر هم‌سو نیست. نتیجه به‌دست‌آمده در این بخش از پژوهش نشان از سطح پایین آگاهی در میان کتابداران دارد. آگاهی پایین می‌تواند متأثر از کمبود آموزش‌های لازم باشد؛ زیرا تا اطلاعاتی داده نشود، آگاهی به دست نمی‌آید. به‌طوری‌که می‌توان گفت، داشتن درک مناسب از اهمیت اجرای الزامات امنیتی و تأثیر اصول امنیت اطلاعات و ارتباط آن با وظیفه کاری کتابداران در کتابخانه مستلزم داشتن آگاهی کافی درباره مفهوم امنیت اطلاعات است. از این‌رو نتایج به‌دست‌آمده از پژوهش‌های حسن‌زاده، کریم

زادگان مقدم و جهانگیری (۱۳۹۰) و جبراسیلاس و لسا (۲۰۱۱) و چن، رامامورتی و ون (۲۰۱۵) نیز بر این موضوع تأکید دارند. از طرفی دیگر، تا زمانی که کتابداران ارزش‌های والای انسانی، وجدان کاری و مسئولیت‌پذیری، امانت‌داری، درستکاری و تقید، اعتماد و... را در مسائل مربوط به امنیت اطلاعات به کار نیندند، حمایت از عوامل سطح سازمانی به‌درستی صورت نمی‌پذیرد. نتایج به‌دست‌آمده از پژوهش و جبراسیلاس و لسا (۲۰۱۱) نیز هم‌راستا با همین موضوع است.

بخشی دیگر از نتایج پژوهش نشان داد که درک، نگرش و رفتار امنیت اطلاعات کتابداران کتابخانه پژوهشکده‌ها و پژوهشگاه‌های فنی-مهندسی استان‌های تهران و البرز در بعد تغییر در وضعیت مطلوبی نیست. در تبیین نتیجه به‌دست‌آمده می‌توان گفت که کتابخانه‌ها باید در راستای حصول امنیت اطلاعات، با به‌کارگیری ملزومات امنیتی، تغییرات تدریجی در برنامه‌های اجرایی به وجود آورند. در همین راستا، آن‌ها باید درصدد تغییر برخی از جنبه‌های فردی کتابداران برآیند. مدیریت هر کتابخانه یا سازمانی مسئولیت اعمال این تغییرات را بر عهده دارد. کتابداران باید با تقویت ابعاد فرعی موجود در سطح فردی، تغییرات اعمال‌شده را به شیوه‌ای مثبت پذیرفته و در امور و فعالیت‌های کاری خود به کار ببندند. این تغییرات به تدریج در سه سطح فرهنگ‌سازمانی یعنی مفروضات، ارزش‌ها و مصنوعات کتابداران تجلی می‌یابد. عامل تغییر به‌عنوان یک پیش‌فرض اصلی در چرخه مدیریت فرهنگ امنیت اطلاعات به‌حساب می‌آید (Veiga & Eloff, 2010). مطابق با چارچوب پیشنهادی ویگا و ایلاف^۷ (۲۰۱۰) و مقایسه آن با نتایج به‌دست‌آمده در این بخش از پژوهش می‌توان گفت که مدیران کتابخانه‌های جامعه پژوهش به‌عنوان عامل هدایت‌کننده این بعد توجهی به این مهم نداشته‌اند. همچنین نتایج به‌دست‌آمده در پژوهش حاضر به‌مراتب در سطح پایین‌تری نسبت به نتایج به‌دست‌آمده در پژوهش مارتینز (۲۰۰۱) است که بیانگر آن است که هر دو جامعه درخور توجه و رسیدگی مدیران و استقبال کارکنان از پذیرش و همکاری در اعمال تغییرات هستند.

وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران در مجموع گویه‌های معرف فرهنگ امنیت اطلاعات حاکم بر کتابخانه پژوهشکده‌ها و پژوهشگاه‌های فنی-مهندسی مستقر در استان‌های تهران و البرز در وضعیت نامطلوبی قرار دارد. با نگاهی بر پژوهش‌های انجام‌شده، می‌توان دریافت که پژوهش‌های مرتبط در دودسته قرار می‌گیرند. برخی پژوهش‌ها مبتنی بر بسط مبانی نظری و برخی دیگر مبتنی بر بررسی وضعیت موجود هستند. نتایج حاصل از پژوهش سازیلی شاهیبی و همکاران^۸ (۲۰۱۲)، منجر به ارائه مؤلفه‌هایی شد که در پژوهش حاضر نیز با کمی جرح‌وتعدیل به آن‌ها، در قالب ابعاد فرعی اشاره‌شده است. در نتیجه، یافته‌های این پژوهش هم‌سو و در مدل فرهنگ امنیت اطلاعات مارتینز (۲۰۰۱) نهفته است.

به‌طور کلی نتایج پژوهش حاضر در تأکید بر اهمیت عامل انسانی، با نتایج پژوهش حریری و نظری (۱۳۹۱) و جبراسیلاس و لسا (۲۰۱۱) و تانگ، لی و ژانگ^۹ (۲۰۱۵) و فلورس و اکستد^{۱۰} (۲۰۱۶) هم‌سو

1 Veiga & Eloff	7
1 SaziliShahibi et al	8
1 Tang, Li, and Zhang	9
2 Flores and Ekstedt	0

و بر این موضوع تأکید دارد. وضعیت فرهنگ امنیت اطلاعات در پژوهش مارتینز (۲۰۰۱) و آرین پور (۱۳۹۵) در وضعیت متوسط ولی به مراتب در وضعیت بهتری نسبت به پژوهش قرار دارد.

افزون بر موارد یادشده، مشاهده شد که تفاوت معنادار میزان درک، نگرش و رفتار امنیت اطلاعات کتابداران در ابعاد اصلی به ترتیب نزولی عبارت‌اند از: (۱) سطح سازمانی؛ (۲) سطح گروهی و سطح فردی (۳) بعد تغییر. بر این اساس می‌توان چنین استنباط کرد که درک، نگرش و رفتار امنیت اطلاعات کتابداران در سطح سازمانی نسبت به دیگر ابعاد از قوت بیشتری برخوردار است. از جمله دلایل چنین یافته‌ای می‌تواند این باشد که ابعاد فرعی موجود در ابعاد اصلی مانند خط‌مشی، بودجه، تحلیل خطر و محک‌زنی به‌عنوان ابعاد ملموس و قابل اجرا در هر کتابخانه‌ای به حساب می‌آیند. همچنین وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران در سطح گروهی و سطح فردی باهم تفاوتی ندارد. در تبیین چنین یافته‌ای می‌توان چنین تحلیل کرد که «افراد» تشکیل‌دهنده‌ی این دو سطح هستند. درنهایت، بعد تغییر در رتبه آخر قرار می‌گیرد. این رتبه می‌تواند به عملکرد نامحسوس و ضعیف تغییرات در برنامه‌های اجرایی و عملیاتی کتابخانه یا تلاش ضعیف کتابخانه در تغییر جنبه‌های فردی کتابداران در راستای تحقق اهدافشان اشاره داشته باشد. نتیجه به‌دست‌آمده از آزمون تعقیبی شفه نشان داد که وضعیت درک، نگرش و رفتار امنیت اطلاعات کتابداران در کلیه ابعاد، دوبره‌دو باهم تفاوت معناداری دارد. تنها این تفاوت در سطح گروهی و سطح فردی، همچنین سطح گروهی و بعد تغییر معنادار نیست. در مجموع می‌توان چنین استنباط کرد که احراز تفاوت معناداری درک، نگرش و رفتار امنیت اطلاعات کتابداران در سطح سازمانی با سطح گروهی و سطح فردی مؤید ماهیت ابعاد تشکیل‌دهنده‌ی این بعد با دیگر ابعاد است. به‌طوری‌که خط‌مشی و رویه‌ها، محک‌زنی، تحلیل خطر و بودجه مؤلفه‌هایی هستند که به لحاظ ماهیت و جنس به‌عنوان ابزار محسوب می‌شوند که چشم‌اندازها را نمایان و اهداف سازمان را منعکس می‌کنند. عدم تفاوت معناداری درک، نگرش و رفتار امنیت اطلاعات کتابداران بین سطح گروهی با سطح فردی به نوع مؤلفه‌های تشکیل‌دهنده‌ی این ابعاد اشاره دارد؛ به این صورت که نقش آفرینان در سطح گروهی و سطح فردی متشکل از کتابداران و مدیران هستند که مؤلفه‌های سطح سازمانی را اجرا می‌کنند. نوع مؤلفه‌های موجود در این سطوح نیز بر ویژگی‌های فرد در دو بعد «جنبه‌های فردی» و «حضور در گروه» تأکید دارد. بنابراین این نتیجه چندان هم دور از انتظار نیست.

تغییر عامل مهمی است که پس از هر ارزیابی، با شناسایی نقاط قوت و ضعف در ابعاد موردبررسی، باید برای بهبود آن اقدام شود. تفاوت درک، نگرش و رفتار امنیت اطلاعات کتابداران در ابعاد تغییر، سطح سازمانی و سطح فردی نشان از بویابی ابعاد سطح سازمانی و سطح فردی دارد. از طرفی عدم تفاوت معناداری درک، نگرش و رفتار امنیت اطلاعات کتابداران نسبت به بعد تغییر با سطح گروهی نشان از ایستایی سطح گروهی دارد که می‌توان با اعمال مستمر و مدون تغییر در سطح گروهی تأثیر به‌سزایی در ایجاد فرهنگ امنیت اطلاعات مطلوب در کتابخانه‌ها داشت.

پیشنهاد‌های پژوهش

موارد زیر به‌عنوان راه کارهای پیشنهادی برگرفته از یافته‌های پژوهش ارائه می‌شود:

- ◀ کتابخانه به یک خطمشی امنیت اطلاعات مکتوب نیاز دارد که در تدوین خطمشی باید به عوامل سهولت دسترسی و سهولت به‌کارگیری توجه ویژه داشت. به همین منظور لازم است رویه‌هایی برای حمایت از این خطمشی در کتابخانه اجرا و برنامه‌هایی برای آموزش به‌کارگیری خطمشی و آگاهی‌رسانی تدوین و اجرا شوند.
- ◀ در کتابخانه باید رویه‌هایی در نظر گرفته شود تا امنیت اطلاعات را به‌طور مستمر سنجید. از این‌رو نباید وجود شخص یا مقام مسئول برای تحلیل خطر از دارایی‌های اطلاعاتی در کتابخانه را نادیده گرفت.
- ◀ مدیریت باید با برنامه‌ریزی، سازمان‌دهی، هدایت و کنترل در امنیت اطلاعات به پیشبرد اهداف سازمان مادر و کتابخانه توجه نشان دهد. از این‌رو اعمال تغییرات سازنده در برنامه‌های اجرایی و عملیاتی در جهت ایجاد امنیت اطلاعات می‌بایستی به‌صورت مدون در دستور کار قرار گرفته و به‌طور مرتب بررسی و مدیریت شوند.
- ◀ در راستای آگاهی کتابداران از مؤلفه‌های اثربخش در امنیت اطلاعات و اهمیت آن، پیشنهاد می‌شود مطالب مرتبط در متون و سرفصل‌های درسی رشته علم اطلاعات و دانش‌شناسی گنجانده شود.

فهرست منابع

- آرین پور، مرضیه. ۱۳۹۵. میزان رعایت استانداردهای ایزو/آی. ای. اس. ۲۷۰۰۲ و ۲۷۰۱۹ در حوزه «مدیریت امنیت اطلاعات» در سازمان اسناد و کتابخانه ملی جمهوری اسلامی ایران. پایان نامه کارشناسی ارشد، دانشگاه الزهراء^(س). دانشکده علوم تربیتی و روانشناسی.
- اسفندیارپور، اقدس. ۱۳۸۹. عوامل مؤثر بر پذیرش سیاست های امنیت اطلاعات توسط کارمندان در سازمان. پایان نامه کارشناسی ارشد، دانشگاه علامه طباطبایی. دانشکده مدیریت و حسابداری.
- بیگلرگیان، پرینا. ۱۳۹۱. تدوین شاخص های ارزیابی امنیت اطلاعات سازمان: سازمان بورس و اوراق بهادار تهران. پایان نامه کارشناسی ارشد، دانشگاه الزهراء^(س). دانشکده علوم اجتماعی و اقتصادی.
- تیمورزاد، کاوه. ۱۳۸۷. مدیریت تحول سازمانی از تئوری تا عمل. تهران: انتشارات نرم افزاری هامون.
- حریری، نجلا، و زهرا نظری. ۱۳۹۱. امنیت اطلاعات در کتابخانه های دیجیتالی ایران. کتابداری و اطلاع رسانی، ۵۸: ۹۰-۶۱.
- حسن زاده، محمد، و نرگس جهانگیری. ۱۳۹۰. امنیت اطلاعات: از آگاهی تا آموزش. تهران: کتابدار.
- حسن زاده، محمد، داوود کریم زادگان مقدم، و نرگس جهانگیری. ۱۳۹۰. ارایه یک چهارچوب مفهومی برای ارزیابی پرمیگی و آموزش آگاهی از امنیت اطلاعات کاربران. فصلنامه نظام ها و خدمات اطلاعاتی، ۲(۱): ۱-۱۶.
- دانایی مقدم، دلنشین، و نصرت ریاحی نیا. ۱۳۹۳. بررسی امنیت اطلاعات در وبسایت کتابخانه های دیجیتالی در ایران. اولین همایش ملی تعامل انسان و اطلاعات. تهران: دانشگاه خوارزمی.
- شورای علمی فارسی ... [و دیگران]. ۱۳۸۸. دانشنامه کارآفرینی. ج. ۲. تهران: بنیاد دانشنامه نگاری ایران: موسسه کار و تأمین اجتماعی.
- طاهری، مهدی. ۱۳۸۶. ارایه چارچوبی برای نقش عوامل انسانی در امنیت سیستم های اطلاعاتی. پایان نامه کارشناسی ارشد، دانشگاه تربیت مدرس. دانشکده علوم انسانی، بخش مدیریت فناوری اطلاعات.
- عاشوری زاده، سهیلا. ۱۳۹۱. رابطه فرهنگ سازمانی با مدیریت امنیت اطلاعات در بانک ملی ایران. پایان نامه کارشناسی ارشد، دانشگاه علامه طباطبایی. دانشکده مدیریت و حسابداری.
- مقیم، سیدمحمد. ۱۳۸۲. اداره امور حکومت های محلی: مدیریت شوراها و شهرداری ها. تهران: انتشارات سمت.
- مرتضایی فرد، فاطمه، ویراستار. ۱۳۸۱. دایره المعارف کتابداری و اطلاع رسانی. ج. ۱. تهران: سازمان اسناد و کتابخانه ملی جمهوری اسلامی ایران.
- Chen, Y., K. Ramamurthy, & K. Wen, 2015. Impacts of Comprehensive Information Security Programs on Information Security Culture. *Journal of Computer Information Systems*, 55:3, 19-11. Available at: <http://dx.doi.org/08874417.2015.11645767/10>.
- Eloff, M., & S. H. von Solms, 2000. Information security management: a hierarchical framework for various approaches. *Computers & Security*, 19(3), 243-256.
- Flores, W. R., & M. Ekstedt. 2016. Shaping intention to resist social engineering through transformational leadership, information security culture and

- awareness. *Computers & Security*. Available at: <http://dx.doi.org/doi: 10.1016/j.cos.2016.01.004>
- Gebrasilase, T., & Lemma Lessa. 2011. Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital. *The African Journal of Information Systems*, 3(3), 71-86.
- ISO/IEC 17799. 2000. *Information technology -- Security techniques -- Code of practice for information security management*. Second edition 2005-06-15.
- Martins, A., & Jan Eloff. 2002. *Information Security Culture*. US: Springer. Series Vol: 86. Part 5.
- Martins, A. 2001. *Information Security Culture Survey*, South Africa: Johannesburg, Rand Afrikaans University. Available at: <https://ujdigispace.uj.ac.za/bitstream/.../OrganisationReportFinalApr.pdf?...9>.
- SaziliShahibi, M. et al. 2012. Determining factors influencing information security culture among ICT librarians. *Journal of Theoretical and Applied Information Technology*, 37(1), 132-140.
- Tang, M., M. Li, & T. Zhang. 2015. *The impacts of organizational culture on information security culture: a case study*. Springer Science+Business Media New York. Available at: <https://link.springer.com/article/10.1007/s1079-015-0252-2>.
- Williams, P. A. 2009. *What Does Security Culture Look Like For Small Organizations?* Proceeding of the seventh Australian Information Security Management Conference, Perth, Western Australia. Available at: <http://ro.ecu.edu.au/ism/7/>.
- Veiga, D. A., & J. H. Eloff. 2010. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207

Evaluation of Information Security Culture of Specialized Institution libraries in the Field of Engineering

...

Fatemeh Kolivand

M. A., Knowledge and Information Science, Faculty of Education and Psychology, AL Zahra University, Tehran, Iran.

Zoya Abam

Assistant Prof., Ph.D, Knowledge and Information Science, Faculty of Education and Psychology, AL Zahra University, Tehran, Iran.

Mitra Dilmaghani

Assistant Prof., Ph.D, Knowledge and Information Science, Malek Ashtar University, Tehran, Iran.

Abstract

Review on internal researches shows that so far no structured study was conducted with the focus on an information security culture model. That means until now, no research examined perception, attitude and behavior of information security culture of librarians. According to the purpose, this study for the first time localizes an information security culture model in Iran. The purpose of the study was to evaluate the Information Security Culture of Specialized Institution libraries in the Field of Engineering in Tehran & Alborz. This applied research conducted in a analytical and descriptive survey approach. Applying non-probability sampling, the research included 19 Engineering Research Institutes in Tehran and Alborz province and all librarians working in the library of those institutions were studied. Data were collected by a researcher-made questionnaire based on Martins Information Security Culture Model in 2001. Data analyzed by using Descriptive Statistics such as Indicator of Central Tendency, Scattering Parameters and Analytical Statistics Method including One-way Analysis of Variance. The results indicated that the level of information security culture in studied libraries was weak (%76.7). On the other hand, the average perception, attitude and behavior of the librarians in the main dimensions of information security culture, i.e., in the Organizational Level was middle (%40.97), in the Group Level (%21.73), in the Individual Level (%24.67) and Change (%17.13) were weak. Moreover, sub-dimensions, namely Policy and Procedures (%15.78), Risk Analysis (%11.82), Benchmarking (%8.07), Budget (%5.3), Management (%12.18), Trust (%9.55), Awareness (%18.13) and Ethical Conduct (%6.53) were at low level. The current status of information security culture of libraries of research institutes was poorly evaluated. Furthermore, the status of perception, attitude and behavior of librarians regarding information security culture in the main dimensions and sub-dimensions were weak.

Keywords: *Information, Security, Information Security, Organizational Culture, Information Security Culture, Special Library*