Knowledge and Information Management

Print ISSN: 2383-1049
Online ISSN: 2538-5356

Investigating the Situation of Information Security Architecture in Mazandaran Public Libraries Based on ISO / IEC 27002 Standard

Marzieh Fallah Kedabadi
Ph.D Candidate, Department of Knowledeg and Information Science, Babol Branch, Islamic Azad University, Babol, Iran. E-mail: fallah.m1986@yahoo.com

Safiyeh Tahmasebi Limooni
*Corresponding author: Asisstant Profssor, Department of Knowledeg and Information Science, Babol Branch, Islamic Azad University, Babol, Iran. E-mail: sa.tahmasebi2@gmail.com

Abstract

Purpose: The purpose of this study was to evaluate the implementation of information security architecture in Mazandaran Public Library, based on the ISO / IEC 27002 standard.

Methodology: The present research is an analytical survey and in terms of its purpose. The statistical population of the study consist of 193 librarians of the general libraries of Mazandaran. A sample of 129 people was selected through the Cochran formula. The data gathering tool is the ISO / IEC 27002 Standard Information Security Architecture, which is used in the research of Malek Allahami (2012) and includes 11 indicators and 39 components. Cronbach's alpha test was used to test the reliability of the questionnaire and the KS test was used to measure the normality of the data, then t-test was used for testing the questions and Pearson test was used for the hypotheses. To analyze the information needed for the test, statistical software 22 SPSS has been used.

Results: The findings showed that the highest mean for the physical and environmental security index was 4.75, the lowest for security policy index was 2.42. According to the mentioned mean, information security in public libraries of Mazandaran province is evaluated at high level. There is also a significant difference between the implementation of the information security architecture and its components in the libraries under the ISO / IEC 27002 standard.

Conclusion: The results show that managers and security managers need to consider different aspects of security in order to provide security in any information system, helping them create a secure information system and also based on People's comments can be used to assess the architectural levels of information security in the organization.

Keywords: Architecture, Information Security, Public Library Librarians, ISO / IEC 27002 Master Degree.

Citation: Fallah Kedabadi**,** M., & Tahmasebi Limooni, S. (2019). Investigating the Situation of Information Security Architecture in Mazandaran Public Libraries Based on ISO/ IEC 27002 Standard. *Knowledge and Information Management*, 6(2), 35-50. (in Persian)
(DOI): 10.30473/mrs.2020.50639.1412

Received: (31-12-2019)
Accepted: (25-06-2020)

مدیریت اطلاعات و دانش‌شناسی

شاپا چاپی: ۲۳۸۳-۱۰۴۹
شاپا الکترونیکی: ۲۵۳۸-۵۳۵۶

بررسی وضعیت به‌کارگیری معماری امنیت اطلاعات در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲

مرضیه فلاح کردآبادی

دانشجوی دکتری، گروه علم اطلاعات و دانش‌شناسی، واحد بابل، دانشگاه آزاد اسلامی، بابل، ایران.

E-mail: fallah.m1986@yahoo.com

صفیه طهماسبی لیمونی

***نویسنده مسئول:** استادیار، گروه علم اطلاعات و دانش‌شناسی، واحد بابل، دانشگاه آزاد اسلامی، بابل، ایران.

E-mail:sa.tahmasebi2@gmail.com

چکیده

هدف: ارزشیابی به‌کارگیری معماری امنیت اطلاعات در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ است.

روش‌شناسی: روش پژوهش حاضر پیمایشی ـ تحلیلی از لحاظ هدف کاربردی است. جامعهٔ آماری پژوهش، تعداد ۱۹۳ کتابدار کتابخانه‌های عمومی استان مازندران و حجم نمونه ۱۲۹ نفر از طریق فرمول کوکران انتخاب شده‌اند. پرسشنامه استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ معماری امنیت اطلاعات است که در پژوهش ملک الکلامی(۱۳۹۱) استفاده شده و شامل ۱۱ شاخص و ۳۹ مؤلفه است. بر اساس آلفای کرونباخ پایایی پرسشنامه؛ آزمون K-S نرمال بودن داده‌ها و آزمون t و پیرسون پرسش‌ها و فرضیه‌ها سنجش شدند، برای تجزیه و تحلیل اطلاعات از نرم‌افزار آماری SPSS ۲۲ استفاده شده است.

یافته‌ها: نشان داد بیشترین میانگین مربوط به شاخص امنیت فیزیکی و محیطی برابر با ۴/۷۵، کمترین میانگین مربوط به شاخص سیاست‌های امنیتی برابر با ۲/۴۲ است. با توجه به میانگین یادشده امنیت اطلاعات در کتابخانه‌های عمومی استان مازندران در سطح بالا ارزیابی می‌شود. همچنین بین به‌کارگیری معماری امنیت اطلاعات و مؤلفه‌های آن در کتابخانه‌های مورد بررسی براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ تفاوت معنی‌داری وجود دارد.

بحث و نتیجه‌گیری: نتایج نشان می‌دهد برای برقراری امنیت در هر سیستم اطلاعاتی، مدیران و دست‌اندرکاران برقراری امنیت، باید ابعاد و جنبه‌های مختلف امنیتی را مورد توجه قرار دهند، به‌گونه‌ای که در ایجاد یک سیستم اطلاعاتی ایمن به آن‌ها کمک کند. همچنین براساس نظرات افراد می‌توان به ارزیابی سطوح معماری امنیت اطلاعات در سازمان پرداخت.

واژه‌های کلیدی: معماری، امنیت اطلاعات، کتابداران کتابخانه عمومی، استاندارد ایزو/ آی. ای. سی. ۲۷۰۰۲.

استناد: فلاح کردآبادی، مرضیه و طهماسبی لیمونی ، صفیه (۱۳۹۸). بررسی وضعیت به‌کارگیری معماری امنیت اطلاعات در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲. *مدیریت اطلاعات و دانش‌شناسی*، ۶(۲)، ۳۵- ۵۰.

(DOI): 10.30473/MRS.2020.50639.1412

تاریخ دریافت: (۱۰-۱۰-۱۳۹۸)

تاریخ پذیرش: (۰۵-۰۴-۱۳۹۹)

مقدمه

عصر حاضر در مقایسه با اعصار گذشته دیگر به دلیل ابداعات و اختراعات گوناگون با سرعتی وصف‌ناپذیر به سمت کشف مجهولات حرکت می‌کند و اگر انسان گذشته یک اختراع و اکتشاف را طی نسل‌های متمادی با خود همراه می‌دید، انسان امروزی چندین و چند اختراع و نوآوری را در عصر خود تجربه می‌کند. امروزه مقوله «اطلاعات» نقش اساسی و بنیادین را در عصر ما بر عهده دارد. هیچ سازمان، نهاد و جامعه‌ای یافت نمی‌شود که حتی در جزئی‌ترین امور خود از دسترسی به اطلاعات بی‌بهره باشد. انتظارات و نیازهای کاربران با توجه به میزان دسترسی آن‌ها به اطلاعات به‌طور اساسی تغییر یافته و این خود سبب قطع ارتباط میان چگونگی استفاده کاربران از وب‌سایت‌های کتابخانه‌ای و چگونگی طراحی آن‌ها شده است. در این میان نقش معماری اطلاعات به‌عنوان وسیله‌ای جهت برنامه‌ریزی، سازمان‌دهی و توسعه کاربرد فناوری اطلاعات بسیار مهم است (رضایی چگینی، ۱۳۹۴). جایگاه فعالیت‌ها و مکانیزم‌های مختلف امنیت اطلاعات در سازمان در بالاترین سطح سیاست‌ها قرار دارند و این سیاست‌ها، از منطق و استراتژی‌های حرفه ناشی می‌شوند. بر طبق این سیاست‌ها، استانداردها انتخاب می‌شوند در مرحله بعد رویه‌ها و راهنماهای پیاده‌سازی استانداردها مشخص می‌شوند. سپس سازوکارهای نرم‌افزاری و سخت‌افزاری لازم برای تأمین امنیت طبق رویه‌های مشخص شده انتخاب می‌گردند و درنهایت این سازوکارها در محیط واقعی سازمان پیاده می‌شوند (بوکر[1]، ۲۰۱۷).

مزایای ذخیره‌سازی اطلاعات و کاربرد وسیع رایانه‌ها در فعالیت‌های حرفه‌ای گوناگون را ناگزیر ساخته و استفاده از شبکه‌های رایانه‌ای و به‌ویژه اینترنت، تغییرات اساسی درروند ارائه خدمات به وجود آورده است. این امکانات سبب شده حجم بسیار زیادی از اطلاعات تنها به‌اندازه یک سرانگشت با کاربران فاصله داشته باشد. ناگفته پیداست در این محیط پیچیده با این ارتباطات وسیع، مخاطرات گسترده‌ای سیستم‌های رایانه‌ای، سامانه‌های اطلاعاتی و فعالیت‌ها و زیرساخت‌های حیاتی وابسته به آن‌ها را تهدید می‌کند. سازمان‌ها اغلب در معرض انواع تهدید مانند دست‌کاری اطلاعات مرجع و یا سرقت اطلاعات حیاتی و سرمایه‌های اطلاعاتی قرار دارند. در چنین شرایطی چنانچه عوامی که می‌توانند از مزایای سیستم‌ها به شمار بروند تحت کنترل نباشند ممکن است باعث بروز آسیب‌پذیری شده سوءاستفاده افراد بد نیت از آن‌ها به نفوذ و خرابکاری، کلاه‌برداری و یا اخاذی بینجامد. علاوه بر این مشکلات طبیعی و خطاهای غیرعمدی که توسط کاربران رایانه‌ای رخ می‌دهد در صورت نبود روش‌های صحیح برای حفاظت از اطلاعات می‌تواند نتایج مخربی را به بار آورد (حریری و نظری، ۱۳۹۱).

در چنین فضایی اعمال غیرقانونی و مخرب آن‌قدر سریع صورت می‌گیرد که می‌تواند غیرقابل‌شناسایی باشد، هرچند شناسایی آن غیرممکن 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 (سلیمان[2]،۲۰۰۹).

در این راستا لازم است از روال‌های استانداری استفاده شود که به‌واسطه آن بتوان ساختار یک سازمان را برای پیاده‌سازی فناوری اطلاعات ایمن کرد. استانداردهای زیادی درزمینهٔ امنیت اطلاعات در سازمان‌ها تدوین شده‌اند، ISAFF، ISO 27000 ،2- از این جمله هستند. این استانداردها با رویکردهای جامع‌تری به موضوع پرداخته‌اند اما از استاندارد Cisco و SoGP،NIST تا چارچوب و معماری فاصلهٔ زیادی وجود دارد. استاندارد، نمی‌تواند به‌عنوان نقشهٔ راه قرار گیرد و خطوط کلی مسیر را مشخص کند. مهم‌ترین جنبه‌های امنیتی که باید در معماری اطلاعات به آن توجه شود، در نظر گرفتن یک سیاست امنیتی جامع، در نظر گرفتن امنیت به‌منزله یک سرویس و مورد توجه قرار دادن عواملی همچون احراز هویت، کنترل دست‌یابی، تمامیت و محرمانگی پیام، امنیت سطح پیام، امنیت در سطح نقل و انتقال، در دسترس بودن یک سرویس یا یک درخواست، ممیزی به معنای بررسی و حسابرسی داده‌ها، فرآیندها، تراکنش‌های انجام شده در سیستم‌های اطلاعاتی، مدیریت کردن امنیت، مدیریت کردن سیاست، مدیریت سیاست امنیتی، نظارت و مدیریت ریسک و عوامل دیگری چون امنیت منابع انسانی، امنیت محیط و امنیت منابع فیزیکی است (بصیریان جهرمی، ۱۳۹۲). برخی از مهم‌ترین مسائل مربوط به امنیت در کتابخانه‌های عمومی می‌تواند شامل امنیت سخت‌افزارها و دیتا سنتر[3]، جایگاه فیزیکی دیتاسنترها و سرورها، امنیت تبادل اطلاعات، امنیت نرم‌افزارهای کاربردی مورد استفاده امنیت

1. Buecker

2. Sulaiman

3. Data center

نرم‌افزارهای ضدویروس و فایروال، الگوی قوانین و مقررات حاکم بر سایت باشد. نحوهٔ استفاده و کنترل دستیابی به منابعی که به اشتراک گذاشته شده‌اند، از مهم‌ترین هدف‌های یک سیستم امنیتی در شبکه است. همچنین براساس نظرات افراد می‌توان به ارزیابی سطوح معماری امنیت اطلاعات در سازمان پرداخت و هر سازمان برای حفاظت از اطلاعات ارزشمند، باید به یک راهبرد خاص پایبند باشد و براساس آن سیستم امنیتی را پیاده‌سازی و اجرا نماید.

بیان مسئله

امروزه شاهد گسترش حضور کامپیوتر در تمامی ابعاد زندگی خود می‌باشیم. هم‌زمان با گسترش استفاده از کامپیوترهای شخصی و مطرح شدن شبکه‌های کامپیوتری و به دنبال آن اینترنت (بزرگ‌ترین شبکه جهانی)، حیات کامپیوترها و کاربران آنان دستخوش تغییرات اساسی شده است. استفاده‌کنندگان کامپیوتر به‌منظور استفاده از دستاوردها و مزایای فناوری اطلاعات و ارتباطات، ملزم به رعایت اصولی خاص و اهتمام جدی به‌تمامی مؤلفه‌های تأثیرگذار در تداوم ارائه خدمات در یک سیستم کامپیوتری می‌باشند (عبیری و دیگران، ۱۳۹۵). معماری امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری ازجمله این مؤلفه‌ها بوده که نمی‌توان آن را مختص یک فرد و یا سازمان در نظر گرفت. پرداختن به مقوله معماری امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری در هر کشور، مستلزم توجه تمامی کاربران صرف‌نظر از موقعیت شغلی و سنی به جایگاه امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری بوده و می‌بایست به این مقوله در سطح کلان و از بعد منافع ملی نگاه کرد (تقوا و ایزدی، ۱۳۹۳). وجود ضعف امنیتی در شبکه‌های کامپیوتری و اطلاعاتی، عدم آموزش و توجیه صحیح تمامی کاربران صرف‌نظر از مسئولیت شغلی آنان نسبت به جایگاه و اهمیت امنیت اطلاعات، عدم وجود دستورالعمل‌های لازم برای پیشگیری از نقایص امنیتی، عدم وجود سیاست‌های مشخص و مدون به‌منظور برخورد مناسب و به‌موقع با اشکالات امنیتی، مسائلی را به دنبال خواهد داشت که ضرر آن متوجه تمامی کاربران کامپیوتر در یک کشور شده و عملاً "زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می‌دهد (ملک الکلامی، ۱۳۹۱).

به‌موازات حرکت به یک سازمان مدرن و مبتنی بر تکنولوژی اطلاعات، می‌بایست تدابیر لازم در رابطه با حفاظت از اطلاعات نیز اندیشیده گردد. مهم‌ترین مزیت و رسالت شبکه‌های کامپیوتری، اشتراک منابع سخت‌افزاری و نرم‌افزاری است. کنترل دستیابی و نحوه استفاده از منابع به اشتراک گذاشته شده، از مهم‌ترین اهداف یک سیستم امنیتی در شبکه است. با گسترش شبکه‌های کامپیوتری خصوصاً "اینترنت، نگرش نسبت به امنیت اطلاعات و سایر منابع به اشتراک گذاشته شده، وارد مرحله جدیدی شده است. تقریباً" هر نوع تهاجم، تهدیدی است در مقابل حریم خصوصی، پیوستگی، اعتبار و صحت داده‌ها. یک سارق اتومبیل می‌تواند در هر لحظه صرفاً" یک اتومبیل را سرقت نماید، در صورتی که یک مهاجم با به‌کارگیری صرفاً" یک دستگاه کامپیوتر، می‌تواند آسیب‌های فراوانی را متوجه تعداد زیادی از شبکه‌های کامپیوتری نموده و باعث بروز اشکالاتی متعدد در زیرساخت اطلاعاتی یک کشور گردد. آگاهی لازم در رابطه با تهدیدات امنیـتی و نحوه حفاظت خود در مقابل آنان، امکان حفاظت اطلاعات و داده‌های حساس را در یک شبکه کامپیوتری فراهم می‌نماید (اوجیمی[1]، ۲۰۱۵).

هنگامی‌که مدیران و کارمندان موضوع معماری امنیت فناوری اطلاعات را مدنظر 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 به‌خصوص پایگاه‌های اطلاعاتی و یا هرگونه منابع الکترونیکی تلاش و دقت بیشتری داشته باشند. در این راستا، لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند، پایبند به یک استراتژی خاص بوده و براساس آن سیستم امنیتی را اجرا و پیاده‌سازی نماید. عدم ایجاد سیستم مناسب امنیتی، می‌تواند پیامدهای منفی و دور از انتظاری را به دنبال داشته باشد. شاید اگر در چنین مواردی، همه مسائل امنیتی و مشکلات به وجود آمده را به خود کامپیوتر نسبت دهیم، بهترین امکان برون‌رفت از مشکل به وجود آمده است، با استفاده از نسل پیشرفته این فناوری، می‌توان اطلاعات مربوط به وضعیت امنیتی رایانه‌های سرتاسر جهان را بررسی کرده، کدهای مخرب

1. Ojeme

ناشناخته، بسیار جدید و در حال انتشار را ردیابی و کشف نمود و اطلاعات مربوط به آن را بلافاصله و سریعاً در اختیار کلیه کاربران رایانه قرار داد. به این ترتیب مقدار تخریب ایجاد شده در رایانه‌ها به طرز چشمگیری کاهش خواهد یافت، زیرا شناسایی و کشف بدافزارها نیز بسیار سریع انجام گرفته است. در این میان کتابخانه‌های عمومی به دلیل انواع مراجعه‌کنندگان، تبادل و انتقال اطلاعات به کاربران خود از اهمیت ویژه‌ای برخوردارند. این گروه از کتابخانه‌ها انواع مختلف منابع و پایگاه‌های اطلاعاتی را ارائه می‌کنند که به‌نوبه خود در توسعه دانش فردی و به‌تبع آن در افزایش سطح آگاهی جامعه خود تأثیر بسزایی دارند. با وجود اهمیت حفظ امنیت در محیط‌های کتابخانه‌ای، این امر مهم در مقایسه با موضوع‌هایی مانند کمیّت و کیفیت کتابخانه‌ها، کمتر مورد توجه پژوهشگران قرار گرفته است. از طرفی دیگر، در کتابخانه‌های عمومی هم مانند سایر سازمان‌ها، بحث حفظ و نگهداری اطلاعات در اولویت است. از آنجایی که محقق نیز سابقه فعالیت در این حوزه و در استان مازندران را داشته، لذا، این پژوهش درصدد است مسائل امنیتی در کتابخانه‌های عمومی را براساس کنترل‌های امنیتی استاندارد ISO/IEC 27002 که از آخرین استانداردهای بین‌المللی در مورد امنیت اطلاعات است، مورد مطالعه قرار دهد. رهنمودهای این استاندارد هم به‌گونه‌ای تدوین شده که پیروی از آن کمترین خطر و بالاترین امنیت سازمانی را ایجاد خواهد کرد.

اهداف پژوهش

هدف اصلی از انجام پژوهش حاضر ارزیابی وضعیت به‌کارگیری معماری امنیت اطلاعات و مؤلفه‌های آن در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ است.

پرسش‌های پژوهش

۱. وضعیت به‌کارگیری معماری امنیت اطلاعات در سیاست‌های امنیتی کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی ای سی ۲۷۰۰۲ چگونه است؟
۲. وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ ساختار امنیت اطلاعات براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟
۳. وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت امنیت اموال براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟
۴. وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ امنیت منابع انسانی براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟
۵. وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ امنیت فیزیکی و محیطی سازمان براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟
۶. وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت عملیات و ارتباطات براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟
۷. وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ کنترل‌های دسترسی براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟
۸. وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ اکتساب، توسعه و حفظ و نگهداری نظام‌های اطلاعاتی سازمان براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟
۹. وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت بحران امنیت اطلاعات سازمان براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟
۱۰. وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ استمرار کسب و کار براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟
۱۱. وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ تطابق سازمان براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟

فرضیه‌های پژوهش

۱. میانگین نمره به‌کارگیری معماری امنیت اطلاعات در کتابخانه‌های مورد بررسی براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ بالاتر از حد متوسط است.
۲. بین به‌کارگیری معماری امنیت اطلاعات و مؤلفه‌های آن در کتابخانه‌های مورد بررسی براساس استاندارد ایزو / آی ای سی ۲۷۰۰۲ تفاوت معنی‌داری وجود دارد.

پیشینه پژوهش

حاجی زین‌العابدینی و رفعتی (۱۳۹۶) در مطالعه‌ای با عنوان بررسی نظام مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران پرداختند. نتایج نشان می‌دهد مؤلفه‌ها تا حد زیادی در کتابخانه‌های مرکزی رعایت می‌شود. لازم است جهت امنیت فیزیکی وسایل شخصی افراد تحویل گرفته شود، درگاه‌های حفاظتی، دوربین مداربسته و ... لحاظ گردد. جهت امنیت ارتباطات از نظام‌های اطلاعاتی‌ای در کتابخانه‌ها استفاده شود که: به‌روز باشند، به لحاظ امنیتی پشتیبانی شوند، بتوانند تحت وب باشند. جهت امنیت کنترل دسترسی سطوح دسترسی افراد به منابع کتابخانه‌ای را مشخص نمایند. همچنین، موارد امنیتی جهت جلوگیری از آتش‌سوزی، قطعی برق، زلزله، سیل و ... لحاظ گردد. جهت مدیریت پیوستگی عملیات، فرآیندهای کتابخانه‌ای در فواصل منظم و نامنظم مورد بررسی قرار گیرند. دی‌پیر و دیگران (۱۳۹۵) در مطالعه‌ای با عنوان بررسی الزامات اجرایی معماری امنیت اطلاعات سازمان‌های دفاعی پرداختند. پس از تحلیل اولویت‌های اجرایی معماری امنیت اطلاعات سازمانی در سازمان‌های دفاعی استخراج گردید. ضرورت توجه به اهداف سیاست‌ها، چشم‌اندازها و برنامه‌های کلان به هنگام چارچوب امنیتی، بازخوردگیری در زمان اجرای چارچوب‌های امنیتی و دست‌یابی به زبان مشترک بین کارشناسان مجری، سیاست‌مداران و مدیران سطح عالی سازمان‌ها از نتایج ارائه شده در این پژوهش هستند. موسوی و دیگران (۱۳۹۴) در مطالعه‌ای با عنوان شناسایی ریسک‌های امنیت اطلاعات سازمانی با استفاده از روش دلفی فازی در صنعت بانکداری پرداختند. این پژوهش حاضر از دید هدف کاربردی است و از دیدگاه روش انجام پژوهش، توصیفی شمرده می‌شود. در این پژوهش برای شناسایی ریسک‌های امنیت اطلاعات سازمانی، از طریق مطالعهٔ اسنادی و به کمک روش دلفی فازی و نظر خبرگان شامل ۱۰ متخصص فناوری اطلاعات بانک، الگویی براساس استاندارد ایزو ۲۷۰۰۲ و چارچوب کوبیت ۴ ارائه شده است. در این الگو شش شاخه و ۲۰ زیرشاخص ریسک امنیت اطلاعات سازمانی برای بانک شناسایی شد. تقوا و ایزدی (۱۳۹۳) در مطالعه‌ای با عنوان بررسی امنیت در سیستم‌های اطلاعاتی توسعه یافته با روش معماری سرویس‌گرا (SOA) پرداختند. هدف از این نوشتار، بررسی ابعاد مختلف امنیتی و ارائه راهکارهایی برای امنیت در سیستم‌های اطلاعاتی با معماری سرویس‌گرا است. در برقراری یک سیستم اطلاعاتی ایمن و IT امید است که نتایج این پژوهش بتواند به مدیران ایمن‌سازی هرچه بهتر معماری سرویس‌گرا یاری رساند. پژوهش حاضر از دید هدف کاربردی و از دیدگاه روش انجام پژوهش، توصیفی شمرده می‌شود. در این مطالعه بعد از استخراج مهم‌ترین شاخص‌ها، از نمونه آماری در این باره پرسش به عمل آمد. پس از گردآوری داده‌ها با کمک آزمون تی، به تجزیه و تحلیل آن‌ها پرداخته شد. سپس با کمک تحلیل سلسله مراتبی داده‌ها، مهم‌ترین ابعاد امنیتی و زیر ابعاد مربوط به هریک، به ترتیب اهمیت اولویت‌بندی شدند.

سینگ[1] (۲۰۱۸) در مطالعه‌ای با عنوان اقدامات امنیتی اطلاعات کتابخانه‌های دانشگاه‌های مرکزی دهلی پرداختند. این مقاله بررسی اقدامات امنیتی اطلاعات، فیزیکی، سازمانی و تکنولوژیکی در دانشگاه جواهرش لل نورو (JNU)، دانشگاه دهلی (DU) و جمیا میلیا اسلامیا (JMI) در دهلی است. این مقاله از یک رویکرد ترکیبی استفاده می‌کند که با استفاده از چک لیست خاص طراحی شده، هر دو تجزیه و تحلیل کمی و کیفی اقدامات امنیتی اطلاعات را ترکیب می‌کند. یافته‌های این تحقیق نشان می‌دهد که JNU به ترتیب ۶۹,۲۳ درصد بیشترین ویژگی‌های امنیتی اطلاعات را به خود اختصاص داده است، به دنبال آن DU با ۶۶,۱۵ درصد بوده است و JMI دارای پایین‌ترین نمره با ۶۳,۰۷ درصد بوده است. این مطالعه همچنین نشان داده است که تمامی کتابخانه‌های دانشگاه مورد مطالعه در برنامه‌های امنیتی فیزیکی عقب مانده‌اند. امید است که این مطالعه در بهبود لکون‌های امنیتی اطلاعات در کتابخانه‌ها مورد مطالعه قرار گیرد. یافته‌های این تحقیق نه‌تنها کتابداران دانشگاه را به‌منظور بهبود اقدامات امنیتی اطلاعات خود، بلکه همچنین برای جلوگیری از پیشرفت امنیت اطلاعات در دنیای سریع فناوری جهان، به‌منظور جلوگیری از محدودیت‌های کتابداران، باز می‌کند. نوبای[2] (۲۰۱۷) در مطالعه‌ای به با عنوان امنیت اطلاعات کتابخانه‌ها پرداختند. نتایج نشان داد کتابخانه‌ها سرمایه‌گذاری‌های قابل‌توجهی را درزمینهٔ منابع کامپیوتری، آموزش و خدمات انجام داده‌اند. با این حال، چنین سرمایه‌گذاری باید با استفاده از نقش فعال در امنیت اطلاعات از سوءاستفاده یا اشتباه محافظت شود. یانگ[3] و همکاران (۲۰۱۶) آگاهی از امنیت اطلاعات از دیدگاه مدیران سیستم و

1. Singh
2. Newby
3. young

کاربران نهایی در دانشگاه ایالتی فلوریدا را مطالعه نمود. نتایج نشان داد مدیران سیستم تأکید بیشتری بر تهدیدهای خارجی و فنی نسبت به تهدیدهای داخلی و غیر فنی ناشی از عوامل مختلف مانند دسترسی منابع، رفتار با کاربران و رضایت از ابزار فنی دارند. بخش دوم مطالعه که به بررسی کاربران نهایی مربوط بود، حاکی از نیاز به آموزش کاربران و ارتقای آگاهی‌های آن‌ها بود تا بتوانند از خود در برابر تهدیدهای امنیتی محافظت کنند. نتایج این مطالعه، اهمیت عوامل انسانی در امنیت اطلاعات را مورد تأکید قرار داد. لی[1] و دیگران (۲۰۱۵) به بررسی رابطه بین سیستم‌های سازمان و آگاهی امنیت اطلاعات پرداخت. تمرکز این پژوهش بر روی بررسی رابطهٔ حیاتی بین سیستم‌های سازمان در چارچوب نظریهٔ رفتار سازمانی و آگاهی امنیت اطلاعات (ISA) در چارچوب نظریهٔ امنیت اطلاعات بود. مسئله اصلی در این مطالعه، آگاهی نداشتن کاربران از مسائل امنیتی به‌عنوان یک عامل بازدارنده برای سازمان‌ها در دفاع در برابر حملات سایبر بود. براساس یافته‌ها، ارتباط معنی‌داری بین آگاهی کاربران از امنیت اطلاعات و ابعاد ساختار سازمان رسمی، ابعاد فرهنگ‌سازمانی و روش‌ها و سیاست‌های منابع انسانی وجود دارد. چانگ (۲۰۱۴) به عوامل سازمانی مؤثر در پیاده‌سازی مدیریت امنیت اطلاعات پرداختند. این پژوهشگران ضمن تأکید بر نیاز سازمان‌ها به ساختارهای مدیریتی برای حفظ دارایی‌های اطلاعاتی، این‌گونه ساختارهای امنیتی را سلاحی مؤثر برای بقا در عرصهٔ رقابت عنوان می‌کنند. براساس یافته‌های پژوهش، توانایی مدیران فناوری اطلاعات و نبود اطمینان محیطی، تأثیر مثبتی بر روی سازمان‌ها در پیاده‌سازی مدیریت امنیت اطلاعات و استاندارد BS7799 داشته است. همچنین، یافته‌ها نشان داد عوامل سازمانی شامل اندازهٔ سازمان و نوع صنعت، به نحو قابل‌توجهی کاربرد مدیریت امنیت اطلاعات را تحت‌تأثیر قرار می‌دهد.

روش‌شناسی پژوهش

روش پژوهش حاضر پیمایشی ـ تحلیلی و از لحاظ هدف کاربردی است. جامعهٔ پژوهش را کتابداران کتابخانه‌های عمومی استان مازندران که تعداد ۱۹۳ را تشکیل می‌دهند. برای انتخاب حجم نمونه از فرمول کوکران استفاده می‌شود. فرمول کوکران جامعه محدود:

$$n = \frac{NZ^2pq}{Z^2pq + (N-1)d^2}$$

$$n = \frac{193 \times (1.96)^2 \times 0.5 \times 0.5}{(1.96)^2 \times 0.5 \times 0.5 + (193-1) \times (0.05)^2} = 129$$

در این رابطه:

N=حجم جامعه، n =حجم نمونه، Z= مقدار متغیر نرمال واحد استاندارد که در سطح اطمینان ۹۵ درصد برابر ۱/۹۶ است.

d= مقدار اشتباه مجاز، (d = ۰/۰۵)، p= مقدار نسبت صفت موجود در جامعه است. اگر در اختیار نباشد می‌توان آن را ۰,۵ در نظر گرفت. در این حالت مقدار واریانس به حداکثر مقدار خود می‌رسد، q= درصد افرادی که فاقد آن صفت در جامعه هستند $q=1-p$. که بر طبق فرمول کوکران با خطای ۵ درصد ۱۲۹ نفر از آن‌ها تصادفی ساده انتخاب شدند.

ابزار گردآوری داده‌ها پرسشنامه استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ معماری امنیت اطلاعات است که در پژوهش ملک الکلامی(۱۳۹۱) استفاده شده و شامل ۱۱ شاخص و ۳۹ مؤلفه است برای محاسبهٔ پایایی آن پس از توزیع پرسشنامه در یک نمونه مقدماتی شامل ۳۰ نفر، آزمون ضریب آلفای کرونباخ به عمل آمد که مقدار آن برای معماری امنیت اطلاعات ۰/۸۷ تعیین گردید. جهت تجزیه و تحلیل آماری داده‌ها از دو روش توصیفی و استنباطی استفاده می‌شود. در بخش آمار استنباطی با استفاده از آزمون آلفای کرونباخ پایایی پرسشنامه و سپس برای آزمون سؤال‌ها و فرضیه‌ها از آزمون t ضریب همبستگی پیرسون استفاده شده است، برای تجزیه و تحلیل اطلاعات موردنیاز برای انجام آزمون از نرم‌افزار آماری SPSS۲۲ استفاده می‌شود.

یافته‌های پژوهش

در این پژوهش ۱۲۹ پرسشنامه صحیح گردآوری شد که داده‌های حاصل از آن‌ها بررسی و تجزیه و تحلیل شد. براساس اطلاعات پاسخ‌دهندگان می‌توان دریافت که در کتابداران کتابخانه‌های عمومی استان مازندران مورد بررسی بیش از ۶۵/۲ درصد از پاسخ‌دهندگان زن بوده و تنها ۳۴/۸ درصد از آن‌ها جنسیت مرد داشته و بیشترین فراوانی سنی، برای سن ۴۱ تا ۵۰ سال با ۵۴ درصد و پس از آن برای سن ۳۱ تا ۴۰ سال با ۳۴ درصد و درنهایت سن زیر ۳۰ سال و

۱. lee

بالای ۵۱ سال هرکدام با ۶ درصد و همچنین بیشترین درصد را کارکنان با سابقه کاری بیشتر از ۱۱ سال با ۵۲ درصد تشکیل می‌دهند. پس از این گروه کارکنان با ۶ تا ۱۰ سال با ۳۱ درصد قرار دارند و درنهایت پاسخ‌دهندگان با سابقه کاری ۲ تا ۵ سال با ۱۸ درصد قرار دارند و بیشترین درصد را کارکنان با تحصیلات کارشناسی با ۶۳ درصد تشکیل می‌دهند. پس از این گروه کارکنان با سطح تحصیلات فوق‌لیسانس با ۲۷ درصد قرار دارند.

جدول ۱. نتایج آزمون کولموگروف-اسمیرنوف در نرمال بودن داده‌ها

متغیر	کولموگراف- اسمیرونوف		
	آماره	درجه آزادی	معنی‌داری
سیاست‌های امنیتی	۱/۱۴۲	۱۲۸	۰/۲۵۳
ساختار امنیت اطلاعات	۰/۴۷۸	۱۲۸	۰/۶۵۸
مدیریت امنیت اموال	۰/۶۸۲	۱۲۸	۰/۱۵۶
امنیت منابع انسانی	۰/۷۴۵	۱۲۸	۰/۱۸۹
امنیت فیزیکی و محیطی	۱/۱۹۳	۱۲۸	۰/۲۷۹
مدیریت ارتباطات و عملیات	۰/۴۴۲	۱۲۸	۰/۳۵۶
مدیریت کنترل‌های دسترسی	۰/۵۳۸	۱۲۸	۰/۴۸۷
اکتساب، توسعه و حفظ و نگهداری	۰/۸۸۲	۱۲۸	۰/۰۸۹
مدیریت بحران امنیت اطلاعات	۱/۲۳۵	۱۲۸	۰/۰۹۱
تطابق سازمان	۰/۲۵۹	۱۲۸	۰/۷۱۵
مدیریت استمرار کسب‌وکار	۰/۳۲۲	۱۲۸	۰/۴۹۲

جهت بررسی نرمال بودن توزیع داده‌های پژوهش در آزمون کولموگروف و اسمیرنوف (k-s) استفاده شده است به‌طور کلی می‌توان نتیجه گرفت داده‌ها به‌طور قطع نرمال است و به دلیل نرمال بودن از آزمون‌های پارامتریک استفاده می‌شود.

آزمون سؤالات پژوهش

سؤال اول: وضعیت به‌کارگیری معماری امنیت اطلاعات در سیاست‌های امنیتی کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ چگونه است؟

برای پاسخگویی به این سؤال، میانگین نمرات وضعیت به‌کارگیری معماری امنیت اطلاعات در سیاست‌های امنیتی در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ با میانگین مورد انتظار با استفاده از آزمون تی تک نمونه بررسی شد.

جدول ۲. آزمون T تک نمونه وضعیت به‌کارگیری معماری امنیت اطلاعات در سیاست‌های امنیتی

وضعیت به‌کارگیری معماری امنیت اطلاعات	آماره t	سطح معنی‌داری	میانگین مورد انتظار	میانگین به دست آمده
بازنگری مناسب بودن معماری امنیت اطلاعات در سیاست‌های امنیتی	۹/۴۳	۰/۰۰۰	۲/۳	۲/۴۲

با توجه به نتایج جدول ۲ نشان می‌دهد که سطح معنی‌داری برای وضعیت به‌کارگیری معماری امنیت اطلاعات در سیاست‌های امنیتی کوچک‌تر از ۰/۰۵ است. بنابراین، بین میانگین‌های به دست آمده برای و وضعیت به‌کارگیری معماری امنیت اطلاعات در سیاست‌های امنیتی تفاوت معنی‌داری وجود دارد. با مقایسه به میانگین‌های به دست آمده با میانگین‌های مورد انتظار در می‌یابیم وضعیت به‌کارگیری معماری امنیت اطلاعات در سیاست‌های امنیتی در کتابداران کتابخانه‌های عمومی در سطح پایین قرار دارد.

سؤال دوم: وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ ساختار امنیت اطلاعات براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟

برای پاسخگویی به این سؤال، میانگین نمرات وضعیت به‌کارگیری معماری امنیت اطلاعات در ساختار امنیت اطلاعات در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ با میانگین مورد انتظار با استفاده از آزمون تی تک نمونه بررسی شد.

جدول ۳. آزمون T تک نمونه وضعیت به‌کارگیری معماری امنیت اطلاعات در سیاست‌های امنیتی

ساختار امنیت اطلاعات	آماره t	سطح معنی‌داری	میانگین مورد انتظار	میانگین به دست آمده
امنیت داخلی سازمان	۵/۱۱	۰/۰۰۰	۴/۰۲	۴/۱۰
امنیت خارجی سازمان	۱۰/۱۵	۰/۰۰۰	۳/۸۵	۳/۹۰
کل	۷/۶۳	۰/۰۰۰	۳/۹۴	۴

با توجه به نتایج جدول ۳ نشان می‌دهد که سطح معنی‌داری برای وضعیت به‌کارگیری معماری امنیت اطلاعات در ساختار امنیت اطلاعات کوچک‌تر از ۰/۰۵ است. بنابراین، بین میانگین‌های به دست آمده برای وضعیت به‌کارگیری معماری امنیت اطلاعات در ساختار امنیت اطلاعات تفاوت معنی‌داری وجود دارد. با مقایسه به میانگین‌های به دست آمده با میانگین‌های مورد انتظار در می‌یابیم وضعیت به‌کارگیری معماری امنیت اطلاعات در ساختار امنیت اطلاعات در کتابداران کتابخانه‌های عمومی در سطح متوسط به بالا قرار دارد.

سؤال سوم: وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت امنیت اموال براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟

برای پاسخگویی به این سؤال، میانگین نمرات وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت امنیت اموال در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ با میانگین مورد انتظار با استفاده از آزمون تی تک نمونه بررسی شد.

جدول ۴. آزمون T تک نمونه وضعیت به‌کارگیری معماری امنیت اطلاعات در زمینه مدیریت امنیت اموال

مدیریت امنیت اموال	آماره t	سطح معنی‌داری	میانگین مورد انتظار	میانگین به دست آمده
ایجاد امنیت داخل سازمان	۱۳/۴۳	۰/۰۰۰	۴/۰۸	۴/۴۲
ایجاد امنیت در خارج سازمان	۷/۶۵	۰/۰۰۰	۴/۱۲	۴/۱۵
کل	۱۰/۵۴	۰/۰۰۰	۴/۱	۴/۲۸

با توجه به نتایج جدول ۴ نشان می‌دهد که سطح معنی‌داری برای وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت امنیت اموال کوچک‌تر از ۰/۰۵ است. بنابراین، بین میانگین‌های به دست آمده برای وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت امنیت اموال تفاوت معنی‌داری وجود دارد. با مقایسه به میانگین‌های به دست آمده با میانگین‌های مورد انتظار در می‌یابیم وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت امنیت اموال براساس استاندارد در کتابخانه‌های عمومی در سطح بالا قرار دارد.

سؤال چهارم: وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ امنیت منابع انسانی براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟

برای پاسخگویی به این سؤال، میانگین نمرات وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ امنیت منابع انسانی در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ با میانگین مورد انتظار با استفاده از آزمون تی تک نمونه بررسی شد.

جدول ۵. آزمون T تک نمونه وضعیت به‌کارگیری معماری امنیت اطلاعات در درزمینهٔ امنیت منابع انسانی

امنیت منابع انسانی	آماره t	سطح معنی‌داری	میانگین مورد انتظار	میانگین به دست آمده
اهمیت امنیت پیش از اشتغال افراد	۹/۱۳	۰/۰۰۰	۳/۳	۳/۴۲
تأکید بر امنیت در حین خدمت	۱۶/۰۳	۰/۰۰۰	۴	۴/۱۵
تأکید بر امنیت در خاتمه یا تغییر	۷/۰۸	۰/۰۰۰	۳/۸	۳/۹
کل	۱۰/۷۴	۰/۰۰۰	۳/۷	۳/۸۲

با توجه به نتایج جدول ۵ نشان می‌دهد که سطح معنی‌داری برای وضعیت به‌کارگیری معماری امنیت اطلاعات در زمینهٔ امنیت منابع انسانی کوچک‌تر از ۰/۰۵ است. بنابراین، بین میانگین‌های به دست آمده برای و وضعیت به‌کارگیری معماری امنیت اطلاعات در زمینه امنیت منابع انسانی تفاوت معنی‌داری وجود دارد. با مقایسه به میانگین‌های به دست آمده با میانگین‌های مورد انتظار در می‌یابیم وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ امنیت منابع انسانی براساس استاندارد در کتابخانه‌های عمومی در سطح متوسط قرار دارد.

سؤال پنجم: وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ امنیت فیزیکی و محیطی سازمان براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟

برای پاسخگویی به این سؤال، میانگین نمرات وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ امنیت فیزیکی و محیطی سازمان در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ با میانگین مورد انتظار با استفاده از آزمونتی تک نمونه بررسی شد.

جدول ۶. آزمون T تک نمونه وضعیت به‌کارگیری معماری امنیت اطلاعات در درزمینهٔ امنیت فیزیکی و محیطی سازمان

امنیت فیزیکی و محیطی سازمان	آماره t	سطح معنی‌داری	میانگین مورد انتظار	میانگین به دست آمده
استفاده از نواحی ایمن به‌منظور حفظ تسهیلات	۳/۴۳	۰/۰۰۰	۴/۸۴	۴/۹۵
مؤلفه حفظ و نگهداری تجهیزات سازمان	۸/۲۵	۰/۰۰۰	۴/۳۵	۴/۵۶
کل	۵/۸۴	۰/۰۰۰	۴/۶۰	۴/۷۵

با توجه به نتایج جدول ۶ نشان می‌دهد که سطح معنی‌داری برای وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ امنیت فیزیکی و محیطی سازمان کوچک‌تر از ۰/۰۵ است. بنابراین، بین میانگین‌های به دست آمده برای و وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ امنیت فیزیکی و محیطی سازمان تفاوت معنی‌داری وجود دارد. با مقایسه به میانگین‌های به دست آمده با میانگین‌های مورد انتظار در می‌یابیم وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ امنیت فیزیکی و محیطی سازمان براساس استاندارد در کتابخانه‌های عمومی در سطح بالا قرار دارد.

سؤال ششم: وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت عملیات و ارتباطات براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟

برای پاسخگویی به این سؤال، میانگین نمرات وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت عملیات و ارتباطات براساس استاندارد در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ با میانگین مورد انتظار با استفاده از آزمون تی تک نمونه بررسی شد.

جدول ۷. آزمون T تک نمونه وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت عملیات و ارتباطات

مدیریت عملیات و ارتباطات	آماره t	سطح معنی‌داری	میانگین مورد انتظار	میانگین به دست آمده
ایجاد روش‌های اجرایی عملیاتی و مسئولیت	۴/۱۳	۰/۰۰۰	۴/۳	۳/۳۴
مؤلفه مدیریت تحول خدمات به شخص ثالث	۷/۱۰	۰/۰۰۰	۴/۴۱	۴/۵۶
برنامه ریزی و پذیرش نظام	۶/۳۵	۰/۰۰۰	۴/۰۵	۴/۰۳

حفاظت در برابر کدهای مخرب و غیرمجاز	۳/۰۲	۰/۰۰۰	۴/۸۷	۴/۱۲
تعیین دستور کارهایی به‌منظور تهیه نسخه پشتیبان از اطلاعات	۸/۲۱	۰/۰۰۰	۴/۹۰	۴/۹۲
مدیریت امنیت شبکه‌های کامپیوتری	۶/۱۴	۰/۰۰۰	۴/۳	۴/۴۸
فرعی اداره کردن محیط‌های ذخیره‌سازی	۱۰/۲۳	۰/۰۰۰	۴/۳۶	۴/۴۳
کنترل تبادل اطلاعات	۱۲/۰۷	۰/۰۰۰	۴/۴۷	۴/۵۵
حفاظت از خدمات تجارت الکترونیک	۴/۰۱	۰/۰۰۰	۴/۷۲	۴/۴۲
بازبینی از نظام و تسهیلات پردازش اطلاعات	۵/۷۴	۰/۰۰۰	۴/۱۳	۴/۱۸
کل	۶/۷	۰/۰۰۰	۴/۴۵	۴/۳۰

با توجه به نتایج جدول ۷ نشان می‌دهد که سطح معنی‌داری برای وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت عملیات و ارتباطات کوچک‌تر از ۰/۰۵ است. بنابراین، بین میانگین‌های به دست آمده برای و وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت عملیات و ارتباطات تفاوت معنی‌داری وجود دارد. با مقایسه به میانگین‌های به دست آمده با میانگین‌های مورد انتظار در می‌یابیم وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت عملیات و ارتباطات براساس استاندارد کتابخانه‌های عمومی در سطح بالا قرار دارد.

سؤال هفتم: وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ کنترل‌های دسترسی براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟

برای پاسخگویی به این سؤال، میانگین نمرات وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ کنترل‌های دسترسی براساس استاندارد در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ با میانگین مورد انتظار با استفاده از آزمون تی تک نمونه بررسی شد.

جدول ۸. آزمون T نمونه وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ کنترل‌های دسترسی براساس استاندارد

کنترل‌های دسترسی	آماره t	سطح معنی‌داری	میانگین مورد انتظار	میانگین به دست آمده
کنترل دسترسی به اطلاعات	۵/۱۵	۰/۰۰۰	۳/۳۸	۳/۴۲
مدیریت دسترسی کاربر به اطلاعات	۱۳/۱۰	۰/۰۰۰	۴	۴/۱۰
توسعه روش‌های دسترسی مناسب	۷/۴۱	۰/۰۰۰	۴/۰۱	۴/۰۳
کنترل دسترسی به خدمات شبکه	۶/۰۲	۰/۰۰۰	۳/۰۳	۳/۱۲
کنترل دسترسی به نظام عامل	۸/۴۲	۰/۰۰۰	۲/۲۹	۲/۸۵
کنترل دسترسی به برنامه‌های کاربردی و اطلاعات	۱۲/۰۲	۰/۰۰۰	۳/۳۸	۳/۴۵
حفاظت از تسهیلات سیار و کار از راه دور	۳/۱۸	۰/۰۰۰	۳/۶۶	۳/۶۹
کل	۷/۹	۰/۰۰۰	۳/۳۹	۳/۵۲

با توجه به نتایج جدول ۸ نشان می‌دهد که سطح معنی‌داری برای وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ کنترل‌های دسترسی کوچک‌تر از ۰/۰۵ است. بنابراین، بین میانگین‌های به دست آمده برای و وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ کنترل‌های دسترسی تفاوت معنی‌داری وجود دارد. با مقایسه به میانگین‌های به دست آمده با میانگین‌های مورد انتظار در می‌یابیم وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ کنترل‌های دسترسی براساس استاندارد کتابخانه‌های عمومی در سطح متوسط قرار دارد.

سؤال هشتم: وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ اکتساب، توسعه و حفظ و نگهداری نظام‌های اطلاعاتی سازمان براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟

برای پاسخگویی به این سؤال، میانگین نمرات وضعیت به‌کارگیری معماری امنیت اطلاعات در اکتساب، توسعه و حفظ و نگهداری نظام‌های اطلاعاتی سازمان براساس استاندارد در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ با میانگین مورد انتظار با استفاده از آزمونتی تک نمونه بررسی شد.

جدول ۹. آزمون T تک نمونه وضعیت به‌کارگیری معماری امنیت اطلاعات در اکتساب، توسعه و حفظ و نگهداری نظام‌های اطلاعاتی

اکتساب، توسعه و حفظ و نگهداری نظام‌های اطلاعاتی	آماره t	سطح معنی‌داری	میانگین مورد انتظار	میانگین به دست آمده
شناسایی الزامات امنیتی موردنیاز نظام‌های اطلاعاتی	۵/۲۴	۰/۰۰۰	۳/۳	۳/۴۲
پردازش صحیح در برنامه‌های کاربردی	۳/۲۵	۰/۰۰۰	۴/۰۴	۴/۱۶
استفاده از کنترل‌های رمزنگاری در حفاظت اطلاعات	۹/۱۵	۰/۰۰۰	۴/۱	۴/۰۳
حفاظت و کنترل از فایل‌های نظام سازمان	۷/۰۲	۰/۰۰۰	۳/۷۷	۳/۸۰
امنیت در فرآیند بهبود و پشتیبانی	۱۱/۱۹	۰/۰۰۰	۴/۲۸	۴/۸۰
مدیریت آسیب پذیری	۸/۱۰	۰/۰۰۰	۴/۴۰	۴/۴۳
کل	۷/۳۲		۳/۹۸	۴/۱۰

با توجه به نتایج جدول ۹ نشان می‌دهد که سطح معنی‌داری برای وضعیت به‌کارگیری معماری امنیت اطلاعات در زمینه اکتساب، توسعه و حفظ و نگهداری نظام‌های اطلاعاتی سازمان کوچک‌تر از ۰/۰۵ است. بنابراین، بین میانگین‌های به دست آمده برای و وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ اکتساب، توسعه و حفظ و نگهداری نظام‌های اطلاعاتی سازمان تفاوت معنی‌داری وجود دارد. با مقایسه به میانگین‌های به دست آمده با میانگین‌های مورد انتظار در می‌یابیم وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ اکتساب، توسعه و حفظ و نگهداری نظام‌های اطلاعاتی سازمان براساس استاندارد کتابخانه‌های عمومی در سطح متوسط قرار دارد.

سؤال نهم: وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت بحران امنیت اطلاعات براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟

برای پاسخگویی به این سؤال، میانگین نمرات وضعیت به‌کارگیری معماری امنیت اطلاعات در مدیریت بحران امنیت اطلاعات سازمان براساس استاندارد در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ با میانگین مورد انتظار با استفاده از آزمونتی تک نمونه بررسی شد.

جدول ۱۰. آزمون T تک نمونه وضعیت به‌کارگیری معماری امنیت اطلاعات در مدیریت بحران امنیت اطلاعات سازمان

مدیریت بحران امنیت اطلاعات سازمان	آماره t	سطح معنی‌داری	میانگین مورد انتظار	میانگین به دست آمده
گزارش‌دهی وقایع و ضعف‌های امنیتی اطلاعات مدیریت	۳/۴۳	۰/۰۰۰	۳/۳	۳/۳۲
بحران‌های امنیتی اطلاعات و بهسازی آن	۸/۲۵	۰/۰۰۰	۴/۶	۴/۵۶
کل	۵/۸۴	۰/۰۰۰	۳/۹۵	۳/۹۴

با توجه به نتایج جدول ۱۰ نشان می‌دهد که سطح معنی‌داری برای وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت بحران امنیت اطلاعات سازمان کوچک‌تر از ۰/۰۵ است. بنابراین، بین میانگین‌های به دست آمده برای وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت بحران امنیت اطلاعات سازمان تفاوت معنی‌داری وجود دارد. با مقایسه به میانگین‌های به دست آمده با میانگین‌های مورد انتظار در می‌یابیم وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ مدیریت بحران امنیت اطلاعات سازمان براساس استاندارد کتابخانه‌های عمومی در سطح متوسط قرار دارد.

سؤال دهم: وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ استمرار کسب و کار براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟

برای پاسخگویی به این سؤال، میانگین نمرات وضعیت به‌کارگیری معماری امنیت اطلاعات در استمرار کسب و کار براساس استاندارد در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ با میانگین مورد انتظار با استفاده از آزمون تی تک نمونه بررسی شد.

جدول ۱۱. آزمون T تک نمونه وضعیت به‌کارگیری معماری امنیت اطلاعات در استمرار کسب و کار

استمرار کسب و کار	آماره t	سطح معنی‌داری	میانگین مورد انتظار	میانگین به دست آمده
مدیریت استمرار به‌منظور حفاظت اطلاعات	۱۵/۲۸	۰/۰۰۰	۴/۱۰	۴/۱۸

با توجه به نتایج جدول ۱۱ نشان می‌دهد که سطح معنی‌داری برای وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ استمرار کسب و کار کوچک‌تر از ۰/۰۵ است. بنابراین، بین میانگین‌های به دست آمده برای و وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ استمرار کسب و کار تفاوت معنی‌داری وجود دارد. با مقایسه به میانگین‌های به دست آمده با میانگین‌های مورد انتظار در می‌یابیم وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ استمرار کسب‌وکار براساس استاندارد کتابخانه‌های عمومی در سطح بالا قرار دارد.

سؤال یازدهم: وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ تطابق سازمان براساس استاندارد در کتابخانه‌های مورد بررسی چگونه است؟

برای پاسخگویی به این سؤال، میانگین نمرات وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ تطابق سازمان براساس استاندارد در کتابخانه‌های عمومی استان مازندران براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ با میانگین مورد انتظار با استفاده از آزمون تی تک نمونه بررسی شد.

جدول ۱۲. آزمون T تک نمونه وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ تطابق سازمان

تطابق سازمان	آماره t	سطح معنی‌داری	میانگین مورد انتظار	میانگین به دست آمده
مطابقت با الزامات قانونی	۳/۴۳	۰/۰۰۰	۲/۴۱	۲/۴۸
انطباق با خط مش‌ها و استانداردهای امنیتی	۸/۲۵	۰/۰۰۰	۲/۲۳	۲/۵۶
انطباق فنی	۱۰/۱۵	۰/۰۰۰	۲/۸	۲/۹۴
کل	۷/۲۷	۰/۰۰۰	۲/۴۸	۲/۶۶

با توجه به نتایج جدول ۱۲ نشان می‌دهد که سطح معنی‌داری برای وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ تطابق سازمان کوچک‌تر از ۰/۰۵ است. بنابراین، بین میانگین‌های به دست آمده برای وضعیت به‌کارگیری معماری امنیت اطلاعات در تطابق سازمان تفاوت معنی‌داری وجود دارد. با مقایسه به میانگین‌های به دست آمده با میانگین‌های مورد انتظار در می‌یابیم وضعیت به‌کارگیری معماری امنیت اطلاعات درزمینهٔ تطابق سازمان براساس استاندارد کتابخانه‌های عمومی در سطح پایین قرار دارد.

آزمون فرضیه‌های پژوهش

فرضیه اول پژوهش: میانگین نمره به‌کارگیری معماری امنیت اطلاعات در کتابخانه‌های مورد بررسی براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ بالاتر از حد متوسط است

جدول ۱۳. آزمون فریدمن برای بررسی رتبه‌های شاخص‌های یازده‌گانه مدیریت امنیت اطلاعات در جامعه پژوهش

ابعاد	میانگین	تعداد	درجه آزادی	مجذور کای	سطح معنی‌داری
سیاست‌های امنیتی	۲/۴۲	۱۲۹			
ساختار امنیت اطلاعات	۴	۱۲۹			
مدیریت امنیت اموال	۴/۲۸	۱۲۹			
امنیت منابع انسانی	۳/۸۲	۱۲۹			
امنیت فیزیکی و محیطی	۴/۷۵	۱۲۹			
مدیریت ارتباطات و عملیات	۴/۳۰	۱۲۹	۱۲۸	۴۸/۵۰۳	۰,۰۰۰
مدیریت کنترل‌های دسترسی	۳/۵۲	۱۲۹			
اکتساب، توسعه و حفظ و نگهداری	۴/۱۰	۱۲۹			
مدیریت بحران امنیت اطلاعات	۳/۹۴	۱۲۹			
تطابق سازمان	۲/۶۶	۱۲۹			
مدیریت استمرار کسب‌وکار	۴/۱۸	۱۲۹			

بیشترین میانگین مربوط به شاخص امنیت فیزیکی و محیطی برابر ۴/۷۵، کمترین میانگین مربوط به شاخص سیاست‌های امنیتی برابر با ۲/۴۲ است. برای فرضیه اول پژوهش مربوط به میانگین شاخص‌های به‌کارگیری معماری امنیت اطلاعات در

کتابخانه‌های مورد بررسی براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ از آزمون فریدمن استفاده شد. درنتیجه فرضیه اول با اطمینان ۹۵٪ تأیید می‌شود.

فرضیه دوم پژوهش: بین به‌کارگیری معماری امنیت اطلاعات و مؤلفه‌های آن در کتابخانه‌های مورد بررسی براساس استاندارد ایزو / آی. ای. سی. ۲۷۰۰۲ تفاوت معنی‌داری وجود دارد.

جدول زیر نتایج آزمون همبستگی پیرسون میان متغیرهای تحقیق را نشان می‌دهد:

جدول ۱۴. نتایج آزمون همبستگی پیرسون متغیرهای تحقیق

		سیاست‌های امنیتی	ساختار امنیت اطلاعات	مدیریت امنیت اموال	امنیت منابع انسانی	امنیت فیزیکی و محیطی	مدیریت ارتباطات و عملیات	مدیریت کنترل‌های دسترسی	اکتساب، توسعه و نگهداری	مدیریت بحران امنیت	تطابق سازمان	مدیریت استمرار کسب و کار
سیاست‌های امنیتی	همبستگی	۱	.۶۵۸ **	.۰۳۸ **	.۰۶۷ **	.۰۷۲ **	.۳۵۴ **	.۰۲۳ **	.۰۴۷ **	.۰۵۹ **	.۰۲۵ **	.۰۷۰ **
	سطح معنی‌دار	۰	۰,۰۰۰	۰۰۰.	۰۰۰.	۰۰۰.	۰,۰۰۰	۰۰۰.	۰۰۰.	۰,۰۰۰	۰۰۰.	۰۰۰.
	تعداد	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹
ساختار امنیت اطلاعات	همبستگی	.۶۵۸ **	۱	.۱۶۸ **	.۱۱۷ **	.۰۵۰ **	.۲۴۸ **	.۰۴۶ **	.۰۶۵ **	.۶۲۳ **	.۰۴۴ **	.۰۶۵ **
	سطح معنی‌دار	۰۰۰.	۰	۰۰۰.	۰۰۰.	۰۰۰.	۰,۰۰۰	۰۰۰.	۰۰۰.	۰,۰۰۰	۰۰۰.	۰۰۰.
	تعداد	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹
مدیریت امنیت اموال	همبستگی	.۰۳۸ **	.۱۵۷ **	۱	.۷۳۸ **	.۰۷۴ **	.۵۷۳ **	.۰۳۳ **	.۰۶۵ **	.۵۰۴ **	.۰۸۱ **	.۰۶۵ **
	سطح معنی‌دار	۰۰۰.۰	۰۰۰.	۰	۰۰۰.	۰۰۰.	۰,۰۰۰	۰۰۰.	۰۰۰.	۰,۰۰۰	۰۰۰.	۰۰۰.
	تعداد	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹
امنیت منابع انسانی	همبستگی	.۰۶۷ **	.۱۴۱ **	.۴۸۹ **	۱	.۰۵۶ **	.۲۲۸ **	.۰۳۹۹ **	.۴۸۳ **	.۴۹۲ **	.۶۸۳ **	.۷۹۲ **
	سطح معنی‌دار	۰,۰۰۰	۰	۰۰۰.	۰	۰۰۰.	۰,۰۰۰	۰۰۰.	۰۰۰.	۰,۰۰۰	۰۰۰.	۰۰۰.
	تعداد	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹
امنیت فیزیکی و محیطی	همبستگی	.۰۷۲ **	.۰۶۰ **	.۱۶۴ **	.۴۰۱ **	۱	.۸۲۵ **	.۷۱۶ **	.۴۸۹ **	.۵۴۵ **	.۷۰۹ **	.۶۰۸ **
	سطح معنی‌دار	۰,۰۰۰	۰,۰۰۰	.	۰۰۰.	۰	۰۰۰.	۰۰۰.	۰,۰۰۰	۰۰۰.	۰۰۰.	۰,۰۰۰
	تعداد	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹
مدیریت ارتباطات و عملیات	همبستگی	.۳۵۴ **	.۲۱۱ **	.۲۴۷ **	.۲۳۶ **	.۵۰۲ **	۱	.۵۴۳ **	.۷۰۱ **	.۷۱۸ **	.۶۳۹ **	.۶۵۰ **
	سطح معنی‌دار	۰۰۰.	۰,۰۰۰	۰,۰۰۰	.	۰۰۰.	۰	۰۰۰.	۰,۰۰۰	۰۰۰.	۰۰۰.	۰,۰۰۰
	تعداد	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹

		سیاست‌های امنیتی	ساختار امنیت اطلاعات	مدیریت امنیت اموال	امنیت منابع انسانی	امنیت فیزیکی و محیطی	مدیریت وارتباطات و عملیات	مدیریت کنترل‌های دسترسی	اکتساب، توسعه و نگهداری	مدیریت بحران امنیت	تطابق سازمان	مدیریت استمرار کسب و کار
مدیریت کنترل‌های دسترسی	همبستگی	۰۲۳ **	۰۵۵ **	۳۲۵ **	۸۵۴ **	۷۴۴ **	۶۱۸ **	۱	۶۳۹ **	۶۴۲ **	۷۷۱ **	۲۵۵ **
	سطح معنی‌دار	۰۰۰	۰۰۰	۰,۰۰۰	۰,۰۰۰	۰	۰۰۰	۰	۰,۰۰۰	۰۰۰	۰۰۰	۰,۰۰۰
	تعداد	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹
اکتساب، توسعه و حفظ و نگهداری	همبستگی	۰۴۷ **	۰۲۷ **	۴۷۸ **	۵۴۳ **	۳۳۳ **	۱۶۶ **	۱۲۴ **	۱	۰۸۵ **	۰۴۵ **	۷۶۳ **
	سطح معنی‌دار	۰,۰۰۰	۰۰۰	۰۰۰	۰,۰۰۰	۰,۰۰۰	۰	۰۰۰	۰	۰۰۰	۰۰۰	۰,۰۰۰
	تعداد	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹
مدیریت بحران امنیت اطلاعات	همبستگی	۰۵۹ **	۰۵۲ **	۲۱۴ **	۳۵۷ **	۱	۴۲۸ **	۴۶۸ **	۵۹۲ **	۱	۶۶۳ **	۷۲۸ **
	سطح معنی‌دار	۰	۰,۰۰۰	۰	۰۰۰	۰	۰,۰۰۰	۰	۰۰۰	۰	۰۰۰	۰,۰۰۰
	تعداد	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹
تطابق سازمان	همبستگی	۰۲۵ **	۰۷۰۲ **	۰۴۷۹ **	۰۴۴**	۳۷۷ **	۲۴۶ **	۲۲۹ **	۱۲۵ **	۷۱۰ **	۱	۶۴۱ **
	سطح معنی‌دار	۰۰۰	۰۰۰	۰,۰۰۰	۰۰۰	۰۰۰	۰,۰۰۰	۰,۰۰۰	۰	۰۰۰	۰	۰,۰۰۰
	تعداد	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹
مدیریت استمرار کسب‌وکار	همبستگی	۰۷۰ **	۰۴۴ **	۸۰۷ **	۳۲۱ **	۵۲۶ **	۸۹۱ **	۷۱۴ **	۰۲۳ **	۰۳۹ **	۰۴۱ **	۱
	سطح معنی‌دار	۰,۰۰۰	۰۰۰	۰۰۰	۰,۰۰۰	۰۰۰	۰۰۰	۰,۰۰۰	۰,۰۰۰	۰	۰۰۰	۰
	تعداد	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹	۱۲۹

** همبستگی در سطح خطای ۰/۰۱ معنی‌دار است

با توجه به خروجی SPSS، ضریب همبستگی پیرسون میان متغیرهای پژوهش و مقدار عدد معنی‌داری (sig) مشاهده شده برای این ضریب کوچک‌تر از ۰/۰۱ و درواقع صفر (۰/۰۱ > sig) است که از سطح معنی‌داری استاندارد (۱٪ = α) کمتر است. لذا، این ضریب در سطح اطمینان ۹۹ درصد معنی‌دار است. با توجه به این‌که ضریب همبستگی دارای علامت مثبت است. بنابراین، می‌توان گفت که جهت تغییرات این دو متغیر با یکدیگر هم جهت و از نوع مثبت بوده است.

بحث و نتیجه‌گیری

با توجه به یافته‌های پژوهش حاضر بیشترین میانگین مربوط به شاخص امنیت فیزیکی و محیطی برابر ۴/۷۵، کمترین میانگین مربوط به شاخص سیاست‌های امنیتی برابر با ۲/۴۲ است. با توجه به میانگین یادشده امنیت کلی اطلاعات در کتابخانه‌های عمومی استان مازندران در سطح بالا ارزیابی می‌شود. در تبیین یافته‌های پژوهش می‌توان اذعان داشت که برای برقراری امنیت در هر سیستم اطلاعاتی، مدیران و دست‌اندرکاران برقراری امنیت، باید ابعاد و جنبه‌های مختلف امنیتی را مورد توجه قرار دهند، به‌گونه‌ای که در ایجاد یک سیستم اطلاعاتی ایمن به آن‌ها کمک کند. در یک مقایسه کلی، تفاوت نتایج این

پژوهش با پژوهش‌های پیشین در این است که با رویکردی متفاوت به مقوله امنیت در سیستم‌های اطلاعاتی با معماری سرویس‌گرا نگریسته شده است. این پژوهش برخلاف اکثر پژوهش‌ها، به‌جای بررسی امنیت از یک جنبه خاص و با یک رویکرد فنی، از دید سیستمی و مدیریتی به بررسی تمامی ابعاد برای برقراری امنیت در یک سیستم اطلاعاتی را از جنبه‌های امنیتی موردنیاز، را مورد توجه قرار داده و به میزان اهمیت و تأثیر هر یک، پرداخته شده است. با توجه به اینکه تمام فرضیه‌های این پژوهش در سطح اطمینان ۹۵ درصد مورد تأیید قرار گرفتند، می‌توان ادعا کرد که برقراری امنیت در سطح مدیریت، سیاست‌های امنیتی، ساختار امنیت اطلاعات، مدیریت امنیت اموال، امنیت منابع انسانی، امنیت فیزیکی و محیطی، مدیریت ارتباطات و عملیات، مدیریت کنترل‌های دسترسی، اکتساب، توسعه و حفظ و نگهداری، مدیریت بحران امنیت اطلاعات، تطابق سازمان و مدیریت استمرار کسب‌وکار می‌توانند به‌منزله ابعاد (شاخص‌های) اصلی چارچوب امنیتی مورد استفاده قرار گیرند. یافته‌ها نشان می‌دهد تا حد زیادی کنترل دسترسی به اطلاعات در کتابخانه‌ها رعایت می‌شود بنابراین لازم است در کتابخانه‌ها سطح دسترسی کاربران، کارمندان و مدیران تعریف شود و یک شناسه کاربری و رمز عبور برای افراد اختصاص یابد و در صورت دسترسی افراد غیرمجاز به منابع اطلاعاتی کتابخانه موارد انضباطی به کار گرفته شود. در این صورت امیدوار بود که از دسترسی به اطلاعات برای افراد تعریف نشده اطمینان حاصل شده است. نتایج با پژوهش‌های دی‌پیر و دیگران (۱۳۹۵)، موسوی و دیگران (۱۳۹۴)، تقوا و ایزدی (۱۳۹۳)، سینگ (۲۰۱۸)، نوبای (۲۰۱۷)، یانگ و دیگران (۲۰۱۶)، لیوانگ (۲۰۱۵) و چانگ (۲۰۱۴) همسو است. همچنین، یافته‌ها نشان داد عوامل سازمانی شامل اندازهٔ سازمان و نوع صنعت، به نحو قابل‌توجهی کاربرد مدیریت امنیت اطلاعات را تحت تأثیر قرار می‌دهد. در ادامه برای بهبود در برقراری امنیت در سیستم‌های اطلاعاتی راهکارهایی ارائه شده است که:

- استفاده از اصول رمزنگاری در قسمت احراز هویت یا تکثیر سرویس‌ها برای افزایش سطح دسترسی.
- راهکارهای امنیتی هستند که بیشتر معماری به خود اختصاص دارند. مانند استفاده از گذرگاه سرویس سازمانی برای اجرای کنترل امنیتی در قسمت طراحی معماری استفاده از WS-security برای امنیت سطح پیام و مانند آن‌ها. انتظار ما بر این است که این ابعاد امنیتی و راهکارهای ارائه شده تا اندازه‌ای به تصمیم‌گیری بهتر مدیران و مجریانی مسئول برقراری امنیت در سیستم‌های اطلاعاتی کمک کند و بتواند امنیت را در سیستم‌های اطلاعاتی تا حد زیادی برقرار کند.

پیشنهادهای پژوهش

- در هنگام تدوین سیاست‌های امنیتی به‌ویژه سیاست‌های امنیت سیاست‌های امنیتی مربوط به کنترل دسترسی و سیاست‌های مربوط به سرویس‌های ترکیبی که گاهی از ترکیب سرویس که گاهی از ترکیب سرویس‌های بیرونی و درونی تشکیل یافته‌اند دقت و توجه کافی داشته باشند.
- توصیه می‌شود امکانات مربوط به نظام‌های در حال توسعه، تحت آزمایش و عملیات به‌منظور کاه خطر ناشی از دسترسی غیرمجاز یا تغییرات در نظام‌های عملیاتی تفکیک شوند.
- کشف و شناسایی منشأ حوادث امنیتی در سازمان
- برآورد خسارت‌های مالی ناشی از وقوع حوادث امنیتی اطلاعات در سطح ملی.

منابع

بصیریان جهرمی، رضا (۱۳۹۲). معماری اطلاعات، *مجله نما*، ۶(۳)، ۵۲-۷۸.

تقوا، محمدرضا؛ ایزدی، ماندانا (۱۳۹۳). بررسی امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با روش معماری سرویس‌گرا (SOA). *مدیریت فناوری اطلاعات*، ۵ (۵)، ۲۵-۴۲.

حریری، نجلا و نظری، زینب (۱۳۹۱). امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران. *کتابداری و اطلاع‌رسانی*، ۱۶(۲)، ۴۵-۸۰.

حاجی زین‌العابدینی، محسن؛ رفعتی، مینا (۱۳۹۶). بررسی نظام مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران. *پژوهش‌های نظری و کاربردی در علم اطلاعات و دانش‌شناسی*، ۷(۱)، ۲۵۷-۲۷۹.

دی‌پیر، محمود؛ هلیلی، خداداد و عبیری، داوود (۱۳۹۵). بررسی الزامات اجرایی معماری امنیت اطلاعات سازمان‌های دفاعی. فصلنامه امنیت پژوهی، ۵۴(۱۵)، ۶۸-۵۴.

رضایی چگینی، جهانگیر (۱۳۹۴). معماری اطلاعات: ارتباطات فنون کتابداری و استاندارد تاپیک مپ، *فصلنامه علوم و فناوری اطلاعات*، ۲۱(۲)، ۸۵–۱۰۳.

ملک الکلامی، میلاد (۱۳۹۱). *ارزیابی وضعیت عملکرد مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران براساس استاندارد ایزو/آی.ای.سی ۲۷۰۰۲*، پایان‌نامه کارشناسی ارشد، دانشگاه علامه طباطبایی، دانشکده علوم تربیتی و روانشناسی.

موسوی، پریسا؛ یوسفی زنوز، رضا؛ حسن‌پور، اکبر (۱۳۹۴). شناسایی ریسک‌های امنیت اطلاعات سازمانی با استفاده از روش دلفی فازی در صنعت بانکداری. مدیریت فناوری اطلاعات. ۷(۱): ۱۸۴–۱۶۳.

Buecker, A., Ashley, P. & Borrett, M., Readshaw, N. (2017). Understanding SOA Security Design and Implementation. International Technical Support Organization, Brussels, IBM redbook Publication.

Chang, G. (2014). Service Web Services with SOAP Security Proxies. Proceeding of the 13th International Conference, 7-9 September, Dresden, Germany.

Fareghzadeh, N. (2015). Web Service Security Method To SOA Development. World Academy Of Science Engineering And Technology, 49(5): 36-48.

Lee, M, Chodavarapu, P. And Kanneganti, R. (2015). SOA Security. 8th International Conference Web Services, 10-12 December, Grenoble, France.

Newby, N. (2017). Information Security For Libraries. Information Security For Libraries. 9(2):379-404.

Ojeme, C. (2015). A Security Framework For Service Oriented Architectures. Proceeding Of The 5th Military Communications Conference,15-17 October, Florida.

Singh, B. (2018).Information Security Measures of Libraries of Central Universities of Delhi: A Study. Journal of Library & Information Technology, 38(2):102-109.

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

young, V. soun, m and teylor,M. (2016). A Policy-Based Evaluation for Quality and Security in Service Oriented Architectures. 6th IEEE International Conference Web Services, 3-5 May, Leipzig, Germany.