www.roshdefanavari.ir
شاپا: ۵۴۸۶-۱۷۳۵ / شاپای الکترونیکی: ۵۶۶۴-۱۷۳۵
فصلنامه تخصصی پارک‌های علم و فناوری و مراکز رشد
فصلنامه رشد فناوری، سال بیست‌ویکم، شماره ۸۴، پائیز ۱۴۰۴

پیاده‌سازی مدیریت امنیت اطلاعات در یک سازمان خدماتی

محمدرضا ثنایی*
دانشگاه آزاد اسلامی، قزوین، ایران
mohamadrezasanaei@gmail.com

احمد طاعتی
دانشگاه آزاد اسلامی، قزوین، ایران
atit2016@yahoo.com

تاریخ دریافت: ۱۴۰۱/۱۲/۲۶ تاریخ اصلاحات: ۱۴۰۳/۱۲/۰۱ تاریخ پذیرش: ۱۴۰۴/۰۴/۲۴

چکیده

با توجه به نقش فزاینده امنیت اطلاعات در اداره هر جامعه، سازمان‌ها و نهادهای دولتی و خصوصی ناگزیر به تأمین زیرساخت‌های لازم برای تحقق این امر مهم می‌باشند. برای اجرای بهینه و موفق سیستم‌های مدیریت امنیت اطلاعات علاوه بر منابع مادی، تکنیک‌های مدیریتی نیز تأثیر زیادی دارند. ثبت استانداردهای مدیریتی در حوزه امنیت اطلاعات فاوا می‌تواند به صورت برنامه‌ریزی‌شده طراحی شود تا وضعیت امنیتی سازمان‌ها متناسب با نیاز آن سازمان تغییر یابد و امنیت از منظر ادامه کسب‌وکار و تا اندازه‌ای در سطوح دیگر (مدیریت بحران و جنگ نرم) تضمین شود. لذا در این پژوهش سعی شده است ضمن حفظ اطلاعات طبقه‌بندی‌شده سازمان، اطلاعات غیرمحرمانه‌ای که می‌تواند موجب ارتقای سازمان‌های مشابه شود در اختیار دیگران قرار گیرد. این پژوهش با مطالعات کتابخانه‌ای و مرور پایان‌نامه‌های مرتبط آغاز شد و پس از کسب اطلاعات مهم و پایه درخصوص موضوع مطروحه، مجموعه‌ای از "شاخص های کلیدی" به‌دست آمد و در گروه‌های متناسب با نام "عوامل مؤثر کلیدی در پیاده‌سازی سیستم مدیریت امنیت" دسته‌بندی گردید و توسط ابزار پرسشنامه مورد تحلیل و ارزیابی قرار گرفت. این پژوهش از نوع توصیفی- پیمایشی بوده و داده ها با استفاده از پرسشنامه جمع‌آوری شده است و تعداد ۱۰۴ پرسشنامه در سازمان مورد مطالعه شهر تهران توزیع و جمع‌آوری شد و سپس آزمون های مورد نیاز آماری بر روی آن‌ها انجام گرفت. هدف این پژوهش شناسایی عوامل کلیدی در پیاده‌سازی مدیریت امنیت اطلاعات در سازمان های خدماتی است. نتایج نشان داد فناوری بیشترین تأثیر و به همین ترتیب عوامل درون سازمانی و برون سازمانی در رتبه‌های بعدی تأثیرگذاری قرار گرفتند. نتایج کاربردی شامل ایجاد ادبیات مشترک مدیران در پیاده‌سازی، اصلاح نگاه مدیران نسبت به مفهوم مدیریت امنیت اطلاعات، برنامه‌ریزی جهت آموزش و تشکیل کمیته امنیت اطلاعات در سازمان مورد مطالعه می‌باشد. همچنین نتایج می‌تواند برای مدیران و سیاست‌گذاران در طراحی و اجرای سیاست‌های امنیت اطلاعات مفید باشد.

واژگان کلیدی

مدیریت امنیت اطلاعات؛ پیاده‌سازی؛ فناوری و تکنولوژی؛ عوامل سازمانی و عوامل خارجی.

۱- مقدمه

بدون شک گسترش و توسعه روزافزون فناوری اطلاعات و ارتباطات و همگراشدن آن ها، ظهور اینترنت و چند رسانه‌ها دلیل توفیقاتی است که بشر امروز، شاهد آن است و موجب نام‌گذاری عصر حاضر به عصر اطلاعات گردیده ولی قطعاً اگر بحث به اشتراک‌گذاشتن اطلاعات مطرح نبود هرگز کاربرد این فناوری‌ها عمومیت نمی‌یافت و امروز شاهد اتصال رایانه خانه‌های روستاییان دور افتاده به اینترنت نبودیم. انبوه اطلاعات موجود در شبکه‌های عمومی خصوصاً اینترنت، موجب گشته تا آحاد مختلف مردم در گوشه و کنار دنیا راغب به عضویت در این شبکه‌ها گردند. این امکان عظیم در کنار توسعه‌های مرتبط با فناوری‌های گوناگون، منجر به شکل‌گیری جامعه نوینی شد که امروز از آن با نام جامعه اطلاعاتی یاد می‌شود. تفاوت این عصر با سایر اعصار را بایستی در سرعت تغییرات فناوری‌ها، رشد سریع و چشم‌گیر علوم و همه این‌ها را باید مدیون دسترسی وسیع و همگانی به اطلاعات دانست. دسترسی گسترده همگان به اطلاعات، موجب شکوفایی استعدادهایی نهفته گردیده و در سایه شکوفایی استعدادهاست که موفقیت‌های بشری شکل می‌گیرد و هر روز محصول جدیدی معرفی می‌شود و هر دم از این باغ بری می‌رسد. هیچ کشوری جز در سایه بلوغ فکری مردم خود به توسعه‌پایدار و همه‌جانبه دست نخواهد یافت و بلوغ فکری تنها از طریق افزایش اطلاعات حاصل می‌گردد. نقش فناوری اطلاعات و ارتباطات در توسعه کشورها به‌عنوان ابزاری برای اشتراک اطلاعات و دسترسی همگانی به انبوه اطلاعات جهانی بر کسی پوشیده نیست و بر عقلای جامعه است تا در توسعه و گسترش آن از هیچ کوششی دریغ نورزند [۱].

کوتاه‌ترین راه برای دستیابی به توسعه و کاربرد فناوری ارتباطات و اطلاعات، رفع موانع پیش روی آن است. ورود به این عرصه، بدون

* نویسنده مسئول

رویکردی نظام‌مند و تدوین معماری فناوری ارتباطات و اطلاعات و برنامه‌های مدون مبتنی بر معماری، می‌تواند کشور را با چالش‌های فرهنگی و اجتماعی روبرو کند. بزرگ‌ترین چالش را می‌توان مرتبط با امنیت فضایی دانست که این فناوری‌ها ایجاد می‌کنند و ما از آن با نام امنیت فضای تبادل اطلاعات یاد کرده‌ایم. امنیت فضای تبادل اطلاعات کشور به عوامل متعددی وابسته است و اقدامات مختلفی در سطح ملی و بخشی نیاز دارد که پرداختن به آن‌ها موضوع سند راهبردی امنیت فضای تبادل اطلاعات کشور است [۲]. ولی به موازات ایجاد زیرساخت‌های امنیتی در سطح ملی از قبیل نظام تأیید هویت الکترونیکی (CA _ PKI)، نظام تشخیص مخاطرات و مقابله با تهدیدات و ... ایجاد سیستم مدیریت امنیت اطلاعات در دستگاه‌های دولتی و شرکت‌های خصوصی امری لازم و ضروری است [۳]. به بیان دیگر سازمان‌ها ناگزیر به دنبال پیاده‌سازی استانداردهای امنیتی می‌باشند. تحقق این امر علاوه بر نیاز به اعمال مسائل تکنیکی، ایجاد سیاست‌های کنترلی و همچنین نیاز به ایجاد رویه‌های صحیح است تا درصد امنیت اطلاعات را بالا ببرد، باید به این نکته توجه داشته باشید که در بسیاری از موارد، هزینه ناشی از افشای اطلاعات و داده‌ها جبران‌ناپذیر است و در بسیاری موارد دیگر سازمان را متحمل ضررهای بسیاری می‌کند [۴].

ایجاد و توسعه سیستم مدیریت امنیت اطلاعات در کنار توسعه و گسترش کاربردی فناوری اطلاعات در شرکت‌های خصوصی، وزارتخانه‌های مختلف، سازمان‌ها، مؤسسات و نهادهای انقلابی موجب خواهد شد کشور با آمادگی بیشتری وارد جامعه اطلاعاتی شود. رویکردی نظام‌مند در این حوزه نیز ضرورت استفاده از استانداردها را مورد تأکید قرار می‌دهد [۵].

حرکت سریع کشورها به سوی جامعه اطلاعاتی، موجب رشد وسیع سیستم‌ها و سرویس‌های اطلاعاتی شده است. در این شرایط، بخش وسیعی از خدمات در همین بستر ارائه‌شده و ارائه‌دهندگان و دریافت‌کنندگان خدمات را ناگزیر از پیوستن به این جامعه نموده است.

اطلاعات، گنجینه‌ای که تا چندی قبل در کمدها و پستوهای سازمان‌ها نگهداری می‌شد، از چند سال قبل و با توسعه شبکه‌های محلی درون‌سازمانی، به شبکه داخلی سازمان‌ها راه یافت. در آن زمان، اطلاعات محدود کاربران شبکه و اعمال کنترل‌های مدیریتی، محافظت‌های فیزیکی و محدودنمودن تعداد افرادی که به سرویس‌ها و به ویژه سرویس‌های حساس دسترسی داشتند، موجب می‌شد تا مشکل خاصی بروز نکند؛ اما اینک با اتصال شبکه‌های سازمانی به شبکه جهانی، همان گنجینه حساس در معرض دید و استفاده طیف وسیعی از مخاطبین در سراسر جهان قرار گرفته است. مخاطبینی که مجهز به انواع اطلاعات و ابزارهای اطلاعاتی می‌باشند. البته تهدید فقط از سوی مخاطبین خارج از سازمان نیست. بررسی‌های انجام‌شده نشان می‌دهد که امروز عمده تهدیدهای موجود علیه اطلاعات و سیستم‌های اطلاعاتی سازمان، منشأ داخلی داشته و خواسته یا ناخواسته توسط پرسنل سازمان ایجاد می‌شود [۶]. بطورکلی در حال حاضر ارتباطات و شبکه‌های کامپیوتری بخشی اجتناب‌ناپذیر از مباحث حوزه فناوری اطلاعات است. هر زمانی که شبکه و ارتباطات مطرح است امنیت شبکه نیز به همراه آن مطرح می‌شود [۷].

در این شرایط، تأمین امنیت همان گنجینه گران‌مایه یعنی اطلاعات، بدون شک یکی از ضروریات هر سازمان است. حاصل تجربه و اقدامات انجام‌شده در طول یک دهه گذشته در جهان، رویکردی است تحت عنوان سیستم مدیریت امنیت اطلاعات.

براساس این رویکرد که در تشریح و استانداردهای مدیریتی و فنی آن ارائه شده است، سازمان‌ها به منظور تأمین امنیت اطلاعات خود، باید مجموعه‌ای از اقدامات پیشگیرانه و تدافعی را به‌صورت مداوم و در چرخه‌ای تحت عنوان چرخه امنیت انجام دهند.

در دنیای امروز اطلاعات نه تنها به‌عنوان یکی از منابع و دارایی‌های اصلی سازمان شناخته می‌شوند، بلکه در حکم وسیله و ابزاری برای مدیریت اثربخش بر سایر منابع و دارایی‌های سازمان (منابع مالی، نیروی انسانی و غیره) نیز محسوب می‌شود و لذا از اهمیت و ارزش ویژه‌ای برخوردار گشته است؛ اما این ارزش‌ها تنها در صورتی محقق و دست یافتنی خواهد بود که اطلاعات بتواند در زمان مناسب، با کیفیت مطلوب و امنیت قابل قبول در اختیار افراد مناسب قرار گیرد و ارتباطات به صورت مطلوب و بهینه در سازمان برقرار گردد. این پژوهش با محور قراردادن استاندارد ISO27001 که مشتمل بر ۱۳۳ کنترل در ۱۱ حوزه می‌باشد؛ به پیاده‌سازی بومی مدیریت امنیت اطلاعات می‌پردازد.

با وجود تحقیقات گسترده، هنوز روش‌های استاندارد و بومی برای مدیریت امنیت اطلاعات در سازمان‌های ایرانی به‌طور کامل بررسی نشده‌اند. این پژوهش به این سؤال پاسخ می‌دهد که چگونه می‌توان استانداردهای مدیریت امنیت اطلاعات را بومی‌سازی کرد؟

۲- ادبیات پژوهش

۲-۱- مدیریت امنیت اطلاعات

امنیت اطلاعات به محرمانگی، یکپارچگی و در دسترس‌بودن داده‌ها مربوط است بدون در نظر گرفتن فرم اطلاعات اعم از الکترونیکی، چاپ، یا اشکال دیگر. بطورکلی امنیت اطلاعاتی از طریق به‌کارگیری مجموعه‌ای از فرایندهای کنترلی به‌دست می‌آید که در سیاست‌ها، روش‌های عملیاتی، رویه‌ها، ساختار سازمانی و نرم‌افزارهای عملیاتی تعبیه می‌شوند. جهت دسترسی به اهداف امنیتی موردنظر سازمان، برقراری رویه‌های کنترلی الزامی است [۸].

در این میان نیز مدیریت امنیت اطلاعات ابزاری است برای شناسایی، مدیریت و به حداقل رساندن احتمال وقوع تهدیداتی که امروزه سازمان‌ها به‌واسطه از دست‌دادن اطلاعات خود با آن‌ها روبه‌رو می‌باشند. این تهدیدات مشتمل بر: تهدیدات داخلی سازمان، تهدیدات خارجی سازمان، تهدیدات اتفاقی، تهدیدات ناشی از خطاهای عمدی و غیرعمدی است.

امروزه سازمان‌ها بسیاری از فرصت‌های کسب‌وکار خود را به لحاظ از دست‌دادن اطلاعات پرارزش خود از دست می‌دهند.

مفهوم «سیستم مدیریت امنیت اطلاعات» اولین بار طی مراحل تحریر و توسعه استاندارد بریتانیایی ۷۷۹۹ در سال‌های انتهایی دهه ۱۹۸۰ میلادی مورد بحث و توجه قرار گرفت. آخرین تعریف «سیستم مدیریت امنیت اطلاعات» از نظر استاندارد بین‌المللی آن عبارت است از:

سیستم مدیریت امنیت اطلاعات بخشی از سیستم مدیریت کلی و سراسری در یک سازمان است که بر پایه رویکرد مخاطرات کسب و کار قرار داشته و هدف آن، پایه‌گذاری، پیاده‌سازی، بهره‌برداری، نظارت، بازبینی، نگهداری و بهبود امنیت اطلاعات است.

امنیت اطلاعات نیز چنین تعریف می‌شود:

حفاظت از محرمانگی، تمامیت و دسترس‌پذیری اطلاعات، علاوه بر این‌ها سایر ویژگی‌ها از قبیل اصالت، قابلیت جوابگویی و اعتبار، انکارناپذیری و قابلیت اطمینان اطلاعات نیز می‌توانند مشمول این حفاظت از اطلاعات باشند [۳].

«سیستم مدیریت امنیت اطلاعات» برای حصول اطمینان از کفایت و تناسب کنترل های امنیتی محافظ دارایی‌های اطلاعاتی طراحی شده است تا به این وسیله به مشتریان و دیگر گروه‌های ذینفع درباره امنیت اطلاعات موجود در سازمان اطمینان خاطر داده شود. هدف این سیستم پیاده‌سازی نوعی از کنترل‌های امنیتی است که با برقراری زیرساخت‌های موردنیاز، امنیت اطلاعات را تضمین می‌نمایند. در حقیقت یک «سیستم مدیریت امنیت اطلاعات» رهیافت نظام‌مندی را برای اداره و مدیریت اطلاعات حساس با هدف حفاظت از آن‌ها فراهم می‌آورد و کل کارکنان، فرایندها و سیستم‌های اطلاعاتی یک سازمان را در بر می‌گیرد [۱۷].

امروزه با گسترش تهدیدهای امنیتی، وجود یک ساختار امن در سازمان‌ها و ادارات ضروری بنظر می‌رسد.

سازمان‌هایی که موجودیتشان به‌طور عمومی به فناوری اطلاعات وابسته است باید از تمامی ابزارهای ممکن برای محافظت از اطلاعات استفاده کنند. جهت دستیابی به امنیت قابل قبول اطلاعات به همکاری مشتریان، شرکای تجاری و دولت نیاز خواهد بود، در ضمن بررسی دوره‌ای امنیت اطلاعات توسط سازمان‌های امنیتی یک روش مقبول در این زمینه خواهد بود. پیاده‌سازی استانداردهای امنیتی موجود نیز، سازمان‌ها را در نیل به اهداف خود یاری می‌رساند. پیاده‌سازی به‌طور اساسی در دو سطح صورت می‌گیرد.

در سطح اول که سطح کلی می‌باشد تمرکز بر روی پروسه‌های تجاری و امنیتی می‌باشد، به طوری‌که فرهنگ امنیت اطلاعات به‌عنوان مفاهیم اصلی این سطح مورد بررسی قرار می‌گیرد و سعی می‌گردد رفتار و عملکرد کارکنان در سازمان‌ها اصلاح‌شده و معیارهای امنیتی در تمامی سطوح سازمانی تفهیم گردد.

در سطح دوم، پیاده‌سازی فنی و با جامعیت بیشتر صورت می‌گیرد که با استفاده از استانداردهای بین‌المللی و سیستم‌ها و ابزارهای لازم صورت می‌گیرد.

بعد از پیاده‌سازی پروسه‌های مدیریتی و تجاری و نیز پیاده‌سازی فنی و عملیاتی امنیت، سازمان تا حد قابل قبولی می‌تواند از پوشش مناسب مدیریت امنیت اطلاعات اطمینان پیدا نماید. پیاده‌سازی مدیریت امنیت اطلاعات براساس یک استاندارد بین‌المللی مانند ISO1799 صورت می‌گیرد تا سازمان بتواند تأییدیه و گواهی مربوطه را اخذ نماید.

۲-۲- امنیت فیزیکی و محیطی

تجهیزات حساس و پردازش اطلاعات سازمان را باید در مکانی امن که براساس تعاریف امنیتی، از پیش تعیین شده، نگهداری کرد. این مکان باید دارای مرزهای امنیتی بوده و ورود و خروج از آن کنترل شود. این مکان باید به صورت فیزیکی در مقابل دسترسی‌های غیرمجاز، خرابی و یا تداخل حفاظت شود. حفاظت در نظر گرفته شده باید با ریسک تعریف شده رابطه مستقیم داشته باشد. قاعده میز و صفحه نمایش پاکیزه برای کاهش ریسک دسترسی غیرمجاز و یا تخریب اسناد چاپی، رسانه‌های ذخیره اطلاعات و تجهیزات پردازش اطلاعات پیشنهاد می‌گردد [۱۸]. حفاظت فیزیکی از طریق ایجاد موانع چندگانه فیزیکی در اطراف منابع سازمانی و تجهیزات پردازش اطلاعات امکان‌پذیر است. هر یک از مرزهای ایجادشده، دسته‌ای از منابع سازمانی را در بر گرفته و افزایش این موانع، سطح کلی حفاظت را افزایش می‌دهد. باید با استفاده از این موانع امنیتی تجهیزات پردازش اطلاعات را حفاظت نمود [۲].

مانع امنیتی، عاملی است که از ایجاد یک مرز مثلاً دیوار یا یک دروازه ورود و خروج و یا یک میز پذیرش ساده به وجود می‌آید. نوع و توانایی هر مانع امنیتی با توجه به نتایج حاصل از تحلیل ریسک تعیین می‌گردد [۱۹].

دستورالعمل‌ها و روش‌های کنترلی زیر را باید در نظر گرفته و به تناسب مورد استفاده قرار داد:

الف) مانع امنیتی باید به روشنی تعریف گردد.

ب) مانع امنیتی یک ساختمان یا سایت حاوی تجهیزات پردازش اطلاعات باید پیوسته باشد (هیچ رخنه قابل نفوذی که بتوان به راحتی از آن گذشت در آن وجود نداشته باشد.) دیوارهای خارجی سایت را باید از مصالح مستحکم ساخت و درهای ورودی نیز باید به نحوی مناسب در مقابل ورود غیرمجاز محافظت شده باشد. (با استفاده از مکانیزم‌های کنترلی، آژیر، قفل و غیره).

پ) دسترسی به تجهیزات فقط از طریق عبور از یک منطقه پذیرش که توسط نیروی انسانی کنترل می‌شود، امکان‌پذیر خواهد بود. دسترسی به سایت یا بنای موردنظر فقط برای پرسنل تأیید شده امکان‌پذیر می‌باشد.

ت) مرزهای فیزیکی در صورت نیاز به صورت کامل و از کف تا سقف ایجاد شده تا علاوه بر جلوگیری از دسترسی غیرمجاز، از حوادث ناشی از سیل و آتش‌سوزی نیز جلوگیری نماید [۲۰].

ث) همه درهای اضطراری (آتش‌نشانی) باید دارای آژیر خطر بوده و به هنگام باز و بسته‌شدن آژیر آن به صدا درآید.

۲-۳- اهداف امنیتی سیستم مدیریت امنیت اطلاعات

مجموعه کنترل‌های امنیتی موردنیاز سیستم‌های اطلاعاتی و ارتباطی سازمان، شامل موارد زیر است [۱۷]:

- **تدوین خط‌مشی امنیت سازمان**

ایجاد خط‌مشی امنیت سازمان، شامل راهنمایی‌ها و دستورالعمل‌های مدیریتی به منظور افزایش امنیت اطلاعات است. این بخش در قالب یک سند سیاست امنیتی در جهت پیشبرد اهداف امنیتی سازمان تنظیم می‌شود این خط‌مشی در اختیار کارکنانی قرار خواهد گرفت که مسئولیت امنیتی برای آن‌ها تعریف شده است.

- **سازمان امنیت اطلاعات**

تشکیل شوراء امنیت اطلاعات در سازمان برای مدیریت امنیت و تعریف نقش و مسئولیت‌های هر یک از بخش‌های سازمان در زمینه امنیت اطلاعات [۱۷].

- **مدیریت دارایی**

محافظت از دارایی‌های سازمان به کمک شناسایی دارایی‌ها و تخصیص مسئول مناسب برای هر دارایی.

- **امنیت منابع انسانی**

کمینه‌کردن ریسک‌های ناشی از خطای انسانی یا سوء استفاده از تجهیزات، به کمک شناسایی پرسنل، نحوه ایمن‌سازی آن‌ها، آموزش پرسنل و امضای تعهدنامه حفظ محرمانگی.

- **امنیت فیزیکی و محیطی**

جلوگیری از دسترسی افراد غیرمجاز، پیشگیری از تداخل یا خرابی اطلاعات، سازماندهی تجهیزات پردازش اطلاعات در مکان‌های امن و ایجاد کنترل‌های لازم به منظور امنیت فیزیکی محیط، کنترل دسترسی‌ها، امنیت مکان، تجهیزات و نقل و انتقال دارایی‌های اطلاعاتی می‌شود.

- **مدیریت عملیات و ارتباطات**

حصول اطمینان از امنیت و عملکرد صحیح تجهیزات پردازش اطلاعات، شناخت مسئولیت‌ها و رویه‌های عملیاتی و مدیریتی در رابطه با تجهیزات پردازش اطلاعات.

- **کنترل دسترسی**

ایجاد قوانین و کنترل‌های لازم و مدیریت آن‌ها جهت دسترسی کاربران به منابع و سرمایه‌های سازمان شامل سیستم‌های اطلاعاتی، شبکه و کامپیوترها.

- **توسعه و نگهداری سیستم‌های اطلاعاتی**

اطمینان از تثبیت امنیت در سیستم‌های اطلاعاتی به کمک کنترل‌های امنیتی، کنترل برنامه‌های کاربردی و خدمات ارائه‌شده که تأثیر زیادی بر امنیت اطلاعات خواهد داشت.

- **مدیریت حوادث امنیت اطلاعات**

تدوین مقررات موردنیاز درخصوص پاسخگویی به نیازهای امنیتی، خط‌مشی‌های امنیتی موردنیاز، ابزارها و مکانیزم‌های بازرسی امنیتی سیستم‌ها.

- **مدیریت تداوم کسب و کار سازمان**

کاهش و پیشگیری از وقفه در فعالیت‌های سازمان و حفاظت از فرایندهای عملیاتی اصلی سازمان، در مقابل خطاها و خرابی‌های عمده یا حوادث طبیعی.

- **انطباق**

انطباق با شرایط قانونی به منظور پیشگیری از هرگونه تجاوز از قوانین جزائی، حقوقی و رعایت کلیه حقوق معنوی و حق تألیف و تکثیر در سیستم‌های سازمان [۱۸].

۳- پیشینه پژوهش

یوسفیان‌پور (۱۴۰۱)، بررسی تأثیر رویکردهای سازمانی بر عملکرد مدیریت امنیت اطلاعات در اداره کل امور اقتصادی و دارائی استان خوزستان، هدف از انجام این پژوهش، بررسی تأثیر رویکردهای سازمانی بر عملکرد مدیریت امنیت اطلاعات در اداره کل امور اقتصادی و دارائی استان خوزستان می‌باشد. روش تحقیق براساس هدف از نوع کاربردی و از جهت ماهیت توصیفی- علی است. جامعه آماری این پژوهش کلیه کارکنان اداره کل امور اقتصادی و دارائی استان خوزستان به تعداد ۱۲۰۰ نفر می‌باشد، به استناد جدول مورگان حجم نمونه برابر ۲۹۱ نفر برآورد و به روش نمونه‌گیری تصادفی ساده مورد پرسش و مطالعه قرار گرفتند. ابزار گردآوری داده‌ها پرسشنامه استاندارد که شامل ۱۸سؤال بود که روایی پرسشنامه توسط متخصصان و کارشناسان مدیریت و پایایی آن از طریق محاسبه ضریب آلفای کرونباخ برای همه شرایط بیشتر از ۰/۷ تأیید شد. در این پژوهش براساس یک مدل مفهومی، شش فرضیه ارائه شد. برای تجزیه و تحلیل داده‌ها از آمار توصیفی (با استفاده از نرم‌افزار SPSS) و آمار استنباطی (با استفاده از نرم‌افزار PLS) استفاده شد. یافته‌ها تمامی فرضیه‌ها و برازش مناسب مدل تحقیق را تأیید می‌کند. نتایج نشان داد که اشتراک‌گذاری دانش امنیت اطلاعات، آموزش، تحصیلات و مشاهده‌پذیری بر عملکرد امنیتی تأثیر معنی‌داری دارند. بعلاوه، این مطالعه اهمیت آموزش امنیتی و اشتراک دانش در اعتماد یک سازمان را بارز می‌سازد. یافته‌های این مطالعه پیامدهای مهمی را برای مدیران و سیاست‌گذاران در رابطه با عوامل سازمانی که عملکرد امنیت اطلاعات کارکنان را توسعه داده و تقویت می‌کنند، ارائه می‌کند. بنابراین، باید بر عملکرد امنیت اطلاعات بر اساس اثربخشی آن‌ها در تقویت استعداد و رفتار امنیتی کارکنان تأکید شود. اندازه‌گیری عملکرد امنیت اطلاعات، نگرش کلی سازمان را نسبت به امنیت اطلاعات و انطباق با آن را نشان می‌دهد. بنابراین با هر کنترل امنیتی فنی از نظر سطح برنامه راهبردی و سطح سرمایه‌گذاری به صورت یکسان برخورد شود [۹].

سواری (۱۴۰۱)، بررسی تأثیر عوامل نگرشی بر حفظ امنیت اطلاعات با نقش میانجی انگیزه حفظ اطلاعات (مورد مطالعه: سازمان تأمین اجتماعی اهواز)، هدف از انجام این پژوهش، بررسی تأثیر عوامل نگرشی بر حفظ امنیت اطلاعات با نقش میانجی انگیزه حفظ اطلاعات (مورد مطالعه: سازمان تأمین اجتماعی اهواز) می‌باشد. روش تحقیق براساس هدف از نوع توصیفی، از نظر مخاطب کاربردی، از نظر بعد زمان مقطعی و از نظر روش توصیفی علی است. جامعه آماری این پژوهش کلیه کارکنان سازمان تأمین اجتماعی اهواز با تعداد ۵۰۳ نفر می‌باشند. حجم نمونه با استفاده از فرمول کوکران ۲۱۷ نفر تعیین شد و در این مطالعه از روش نمونه‌گیری غیرتصادفی در دسترس استفاده شد. ابزار گردآوری داده‌ها در مورد پرسشنامه استاندارد شامل ۲۰ سؤال بود که روایی پرسشنامه توسط استاد راهنما و متخصصان، کارشناسان مدیریت و پایایی آن‌ها از طریق محاسبه ضریب آلفای کرونباخ برای همه شرایط بیشتر از ۰/۷ تأیید شد. در این پژوهش ۴ فرضیه براساس مدل مفهومی مورد بررسی قرار گرفت. برای تجزیه و تحلیل داده‌ها از آمار توصیفی (با استفاده از نرم‌افزار SPSS) و آمار استنباطی (با استفاده از نرم‌افزار PLS) استفاده شد. نتایج تمامی فرضیه‌ها و برازش مناسب مدل تحقیق را تأیید می‌کند و نتایج نشان می‌دهد که عوامل نگرشی بر انگیزه حفظ اطلاعات تأثیر مثبت و معناداری دارد. عوامل نگرشی بر حفظ امنیت اطلاعات تأثیر مثبت و معناداری دارد. انگیزه حفظ اطلاعات بر حفظ امنیت اطلاعات تأثیر مثبت و معناداری دارد. همچنین نقش میانجی انگیزه حفظ اطلاعات در رابطه بین عوامل نگرشی بر حفظ امنیت اطلاعات مورد تأیید قرار گرفته شد [۱۰].

مهری (۱۴۰۰)، بررسی تأثیر آگاهی جامع از امنیت اطلاعات و ویژگی‌های شناختی بر عملکرد مدیریت تهدید در حوزه سیستم اطلاعاتی، هدف اصلی تحقیق حاضر بررسی تأثیر آگاهی جامع از امنیت اطلاعات و ویژگی‌های شناختی بر عملکرد مدیریت تهدید در حوزه سیستم اطلاعاتی می‌باشد. روش تحقیق حاضر توصیفی همبستگی بوده و از حیث هدف کاربردی می‌باشد. جامعه آماری تحقیق را کلیه کارکنان بانک دی تهران تشکیل می‌دهند. برای نمونه‌گیری از فرمول کوکران بهره گرفته و روش نمونه‌گیری تصادفی طبقه‌ای است. برای آزمون فرضیه‌ها از معادلات ساختاری و تحلیل عاملی تأییدی به کمک لیزرل استفاده گردیده است [۱۱].

اسدالهی (۱۳۹۹)، مدیریت ریسک یکپارچه در سیستم مدیریت امنیت اطلاعات، امروزه شرکت‌ها مواجه با افزایش پیچیدگی و عدم قطعیتی هستند که مدیریت ریسک‌های تخصصی و کسب و کار را مشکل‌تر می‌نماید. تلورانس‌های شکست در مدیریت ریسک از سوی جامعه و سهامداران کاهش یافته‌اند. قوانین و مقررات نیز به نوبه خود الزامات سخت‌گیرانه‌تری را مطرح می‌نمایند. شکست در مدیریت این ریسک‌ها می‌تواند مهلک باشد؛ حفظ یکپارچگی و کنترل روز به روز بحرانی‌تر می‌گردد. پس چرا می‌بایست به ریسک توجه کنیم. همه برنامه‌ها کاملاً مساوی نیستند دو برنامه با ROI مشابه، هزینه‌های مشابه و مباحث مشابه ممکن است از نظر ویژگی ریسک با هم متفاوت باشند. ارزیابی ریسک این اجازه را به شما می‌دهد که تفاوت بین برنامه‌ها را مدنظر بگیرید. فرایند Risk Assessment یا ارزیابی ریسک اولین فاز از مجموعه فعالیت‌های مدیریت ریسک است. این فرایند حیاتی جایگاه ویژه‌ای در سیستم مدیریت امنیت اطلاعات (ISMS) دارد. در واقع تست نفوذپذیری (Penetration Testing) که از فعالیت‌های مهم نفوذگران است، جزیی از فرایند ارزیابی ریسک به‌شمار می‌آید [۱۲].

خداشناس (۱۳۹۹)، بررسی تأثیر قابلیت‌های فناوری اطلاعات بر عملکرد شرکت‌ها با نقش واسطه‌ای سیستم مدیریت امنیت اطلاعات؛ در عصر حاضر، استفاده و بکارگیری فناوری اطلاعات یکی از مهم‌ترین سرمایه‌های هر شرکتی است و بنابراین، امنیت و حفاظت از اطلاعات یک مسأله حیاتی و مهم در سازمان‌ها و شرکت‌های سراسر دنیا می‌باشد. بدین منظور این پژوهش با هدف تأثیر قابلیت‌های فناوری اطلاعات بر عملکرد شرکت‌ها همراه با نقش سیستم مدیریت امنیت اطلاعات انجام گرفت. روش تحقیق از نظر هدف کاربردی و از نظر روش و ماهیت انجام توصیفی از نوع پیمایشی است. جامعه آماری تحقیق را کلیه مدیران شرکت های خصوصی در شهر مشهد به تعداد تقریبی ۴۵۰ نفر شامل گردیدند که در این تحقیق از روش نمونه‌گیری تصادفی در دسترس استفاده شد و با استفاده از فرمول کوکران تعداد ۲۰۸ نفر برآورد شد. به منظور گردآوری اطلاعات، از دو روش گردآوری اطلاعات شامل روش کتابخانه‌ای و میدانی استفاده شد و مهم‌ترین ابزار انجام تحقیق، پرسشنامه بود. جهت تجزیه و تحلیل آمار توصیفی و استنباطی از نرم‌افزارهای SPSS و روش مدل‌سازی معادلات ساختاری AMOS استفاده گردید. نتایج تجزیه و تحلیل داده‌ها نشان داد که قابلیت‌های فناوری اطلاعات بر عملکرد شرکت‌ها با نقش واسطه‌ای سیستم مدیریت امنیت اطلاعات اثر مثبتی دارد. تأثیر قابلیت‌های فناوری اطلاعات بر عملکرد شرکت ۰/۷۲ می‌باشد و دارای اثرمثبت و معناداری می‌باشد. قابلیت‌های فناوری اطلاعات بر سیستم مدیریت امنیت اطلاعات دارای اثرمثبت و معناداری می‌باشد. سیستم مدیریت امنیت اطلاعات بر عملکرد شرکت ۰/۸۳ است که دارای اثرمثبت و معناداری می‌باشد. پیشنهاد می‌گردد که مدیران شرکت باید قبل از شروع به ارتقای کارآیی مؤثر پرسنل فناوری اطلاعات، بر روی انعطاف‌پذیری و توانایی زیرساخت‌های فناوری اطلاعات، مدیریت فناوری اطلاعات سرمایه‌گذاری بیشتری انجام دهند. مدیران شرکت بایستی بر روی طراحی و پایش سیستم مدیریت امنیت اطلاعات سرمایه‌گذاری بیشتری کنند و از جدیدترین فناوری‌های اطلاعاتی و ارتباطی در این زمینه استفاده نمایند [۱۳].

خیری (۱۳۹۵) پژوهشی تحت عنوان شناسایی، تحلیل و رتبه‌بندی عوامل مؤثر کلیدی در پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان های حاکمیتی (مطالعه موردی: سازمان بنادر و دریانوردی) انجام داد در این پژوهش علی‌رغم تحقیقات گسترده در این خصوص متأسفانه به

دلایل مختلف از جمله سطوح امنیتی موضوع برای نهادهای دولتی و غیردولتی و یا رابطه مستقیم حوزه مربوطه با منافع ایشان، اطلاعات شفاف و مفیدی درخصوص نحوه پیاده‌سازی و اولویت‌بندی لازم از منظر پیاده‌سازی و استقرار یک سیستم طی سال‌های گذشته تا امروز صورت نگرفته است. لذا در این تحقیق سعی شده است ضمن حفظ اطلاعات طبقه‌بندی‌شده سازمان، اطلاعات غیرمحرمانه‌ای که می‌تواند موجب ارتقای سازمان‌های مشابه شود در اختیار دیگران قرار گیرد. این پژوهش با مطالعات کتابخانه‌ای و مرور پایان‌نامه‌های مرتبط آغاز شد و پس از کسب اطلاعات مهم و پایه درخصوص موضوع مطروحه، با خبرگان و متولیان موضوع پژوهش مصاحبه شد و مجموعه‌ای از "شاخص‌های کلیدی" به‌دست آمد و در گروه‌های متناسب با نام "عوامل مؤثر کلیدی در پیاده‌سازی سیستم مدیریت امنیت" دسته‌بندی گردید و توسط ابزار پرسشنامه مورد تحلیل و ارزیابی قرار گرفت. تعداد ۱۲۶ پرسشنامه در کلیه بنادر توزیع و جمع‌آوری شد و سپس آزمون‌های موردنیاز آماری بر روی آن‌ها انجام گرفت. نتایج به‌دست آمده انجام سازمان مرکزی را متقاعد نمود تا نسبت به برگزاری دوره‌های آموزشی مرتبط و بازآموزی موضوع سیستم امنیت اطلاعات و برنامه‌ریزی و تخصیص رسانه و نرم‌افزار اقدام نماید [۱۴].

شیخعلی و همکاران (۱۳۹۵) پژوهشی تحت عنوان بررسی تأثیر امنیت فناوری اطلاعات در اجرای سامانه مدیریت دانش انجام دادند این تحقیق از نظر روش، توصیفی- پیمایشی و از نظر هدف، کاربردی است. اطلاعات موردنیاز از طریق مطالعات کتابخانه‌ای، مصاحبه و پرسشنامه مقایسات زوجی جمع‌آوری شده است. روش ترکیبی دیمتل و فرایند تحلیل شبکه‌ای برای تعیین اثرگذاری یا اثرپذیری و اولویت‌بندی اهداف کنترلی استاندارد فوق در ارتباط با سامانه مدیریت دانش استفاده گردیده است. یافته‌های پژوهش، بیانگر ارتباط علی و معلولی بین اهداف کنترلی ISO/IEC27001:2013 در استقرار سامانه مدیریت دانش است. همچنین، اهداف کنترلی تشکیلات امنیت اطلاعات، امنیت عملیات، امنیت ارتباطات و رمزنگاری از استاندارد مذکور دارای اولویت بالاتری نسبت به سایر اهداف کنترلی استاندارد فوق هستند [۱۵].

گلستانی‌زاده و سلطان آقایی کوپایی (۱۳۹۵) پژوهشی تحت عنوان ضرورت استقرار سیستم مدیریت امنیت اطلاعات در سازمان‌های هزاره سوم انجام دادند یافته‌ها حاکی از آن است که آنچه جامعه حاضر را به جامعه اطلاعاتی تبدیل نموده است پیشرفت حیرت‌انگیز و سریع فناوری اطلاعات و ارتباطات و به‌کارگیری گسترده جوامع از این فناوری است باید اذعان داشت که تقریباً هرگونه برتری کشورهای توسعه‌یافته در این نوع جامعه مرهون میزان سرمایه‌گذاری تولید، سازماندهی و بهره‌گیری از فناوری اطلاعات و ارتباطات و سرانجام دستیابی به اطلاعات به روز صحیح و دقیق است در این هنگامه ایجاد یک سیستم امنیتی قوی می‌تواند برای حفظ امنیت اطلاعات هر سازمان مؤثر باشد سیستمی که براساس نیازهای سازمان و میزان اهمیت اطلاعات در آن طراحی شده باشد و از تأمین سرمایه های اطلاعاتی حفاظت نماید سیستم مدیریت امنیت اطلاعات ابزاری مناسب در جهت طراحی و کنترل امنیت اطلاعات می‌باشد لذا در این مقاله که به روش تحلیلی توصیفی انجام شده است به بررسی مفاهیم امنیت داده، سیستم مدیریت امنیت اطلاعات و معرفی مهم‌ترین استانداردهای جهانی سیستم مدیریت امنیت اطلاعات پرداخته شده است [۱۶].

امیری و همکاران (۱۳۹۴) پژوهشی تحت عنوان استخراج عوامل شکست پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) در کشورهای در حال توسعه (با تمرکز بر سازمان‌های ایرانی) انجام دادند این پژوهش در رابطه با شناسایی عوامل شکست پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) در کشورهای در حال توسعه و با بررسی موردی بر سازمان‌های ایرانی است. مفهوم کلیدی ISMS برای سازماندهی، طراحی، پیاده‌سازی و نگهداری مجموعه‌ای منسجم از فرایندها و سیستم‌ها به منظور مدیریت‌کردن دستیابی‌پذیری اطلاعات به‌طور مؤثر است. در این مقاله ابتدا تحقیقات مختلف که به برخی از موانع پیاده‌سازی ISMS اشاره کرده بودند، با مطالعات کتابخانه‌ای جمع‌آوری شد و این عوامل استخراج گردید. سپس این موانع از طریق روش دلفی تکمیل و نهایی گردید. در فرایند دلفی از نظرات ۱۹ صاحب‌نظر استفاده شد که این افراد از بین اساتید هیأت‌علمی دانشگاه‌های مختلف که دارای تحصیلات، تخصص و تجربه در زمینه امنیت اطلاعات بودند و همچنین محققان و مجریان در زمینه ISMS انتخاب شدند. در نهایت به دلیل امکان دسترسی محققین به سازمان‌های ایرانی، ۱۸ عامل در طی ۴ مرحله به‌عنوان موانع پیاده‌سازی ISMS در سازمان‌های ایرانی شناسایی شدند [۲].

ما (۲۰۲۲)، رفتار امنیت اطلاعات کارشناسان سیستم‌های اطلاعاتی در سازمان‌های فناوری اطلاعات چین برای حفاظت از امنیت اطلاعات، این مقاله مدل‌سازی معادلات ساختاری در R را به‌عنوان چارچوبی برای کاوش روابط بین متغیرها و تعیین تناسب داده‌های کلی با فرضیه‌ها پیشنهاد می‌کند. مدل‌سازی معادلات ساختاری یک تکنیک چند متغیره است که به‌طور همزمان هم تحلیل عاملی و هم جنبه‌های رگرسیون چندگانه را به منظور تخمین روابط متقابل اجرا می‌کند درحالی‌که همچنین اجازه می‌دهد مدل‌سازی تحلیل مسیر با متغیرهای پنهان و مشاهده‌نشده انجام شود. با استفاده از ۸۰۴ پرسشنامه با تجزیه و تحلیل مدل‌سازی معادلات ساختاری، ما از انجمن‌های پیش‌بینی‌کننده زیر پشتیبانی می‌کنیم: (الف) نگرش‌های امنیت اطلاعات و هنجارهای ذهنی، به‌عنوان اجزای تشکیل‌دهنده TPB، به‌طور قابل‌توجهی بر رفتارهای حفاظتی امنیت اطلاعات تأثیر می‌گذارد. (ب) ارزیابی‌های مقابله‌ای (خودکارآمدی و هزینه پاسخ) و ارزیابی‌های تهدید (حساسیت تهدید و شدت تهدید) PMT به‌طور قابل‌توجهی رفتارهای حفاظتی امنیت اطلاعات را پیش‌بینی می‌کرد. و (ج) تعهد سازمانی تأثیر مثبتی بر رفتارهای حفاظتی امنیت اطلاعات داشت. با این حال، رضایت شغلی و کنترل رفتاری درک‌شده به‌عنوان ساختاری از TPB با رفتارهای امنیت اطلاعات مرتبط نبود [۲۱].

آیدینر و همکاران (۲۰۱۹)، در تحقیقی به مطالعه و بررسی رابطه متقابل بین قابلیت‌های سیستم‌های اطلاعاتی و تأثیر آنها بر عملکرد شرکت پرداختند. جامعه آماری تحقیق شامل ۲۰۴ شرکت در کشور ترکیه می‌باشد. برای تجزیه و تحلیل داده‌ها از مدل‌سازی معادلات ساختاری استفاده شد. نتایج تحقیق، مدل پیشنهادی واسطه‌ای سریال را تأیید نمود، که بر طبق آن عملکرد تصمیم‌گیری و عملکرد فرایند تجارت نقش واسطه‌ای اساسی را در منابع انسانی و قابلیت‌های سیستم‌های اطلاعاتی اداری و روابط عملکرد شرکت ایفا می‌کند [۲۲].

کالا کامدجوگ و همکاران (۲۰۱۸)، در تحقیقی به بررسی رابطه فناوری اطلاعات با عملکرد شرکت و سیستم مدیریت امنیت اطلاعات در کشورهای در حال توسعه پرداختند. در این زمینه از نظرات ۱۳۶ نفر از مدیران و کارشناسان استفاده گردید. نتایج پژوهش مؤید این مطلب بود که قابلیت‌های فناوری اطلاعات تأثیر معناداری بر عملکرد شرکت داشته و سیستم مدیریت امنیت اطلاعات نیز در ارتباط میان قابلیت‌های فناوری اطلاعات و عملکرد شرکت نقشی واسطه‌ای را برعهده دارد [۲۳].

کاکار (۲۰۱۲) در پژوهشی با عنوان «پیاده‌سازی مدیریت امنیت اطلاعات و مشکلات آن» بیان کرده‌اند که با توسعه جهانی استفاده از فناوری SOA، مسائل امنیتی خدمات تارنما (وب‌سایت) که براساس پلت‌فرم ناهمگون شکل گرفته‌اند، به‌طور فزاینده‌ای برجسته و مهم خواهد شد. در این پژوهش دو راهکار امنیتی برای خدمات سرویس‌دهی ارائه شده است [۲۴].

فرضیه‌های تحقیق

۱. فناوری برای پیاده‌سازی مدیریت امنیت اطلاعات شامل به‌کارگیری تجربیات قبلی، مدیریت داده و اطلاعات موجود، به‌کارگیری سیستم‌های نرم‌افزاری و سخت‌افزاری مرتبط با ISMS، تحلیل شکاف مناسب قبل از پیاده‌سازی استاندارد، نظام پذیرش سیستم (استاندارد فاوا) می‌باشد.
۲. عوامل سازمانی برای پیاده‌سازی مدیریت امنیت اطلاعات شامل فرهنگ‌سازمانی، باورهای مشترک، مدیریت تغییر، مدیریت پروژه، رسمیت، ارتباطات و آگاهی، تمرکزگرایی می‌باشد.
۳. عوامل خارجی برای پیاده‌سازی مدیریت امنیت اطلاعات شامل الگوبرداری، تحریم‌ها، شرایط سیاسی می‌باشد.

۴- روش تحقیق

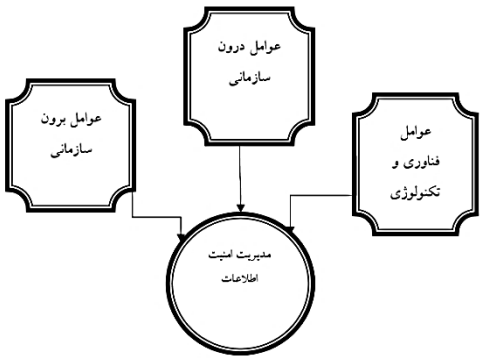
این پژوهش، از نظر هدف، از نوع تحقیقات کاربردی است. همچنین برحسب نحوه گردآوری داده‌ها، به دلیل اینکه به توصیف وضعیت موجود؛ با استفاده از پرسشنامه می‌پردازد، توصیفی و از شاخه پیمایشی می‌باشد. در این تحقیق برای سؤالات پرسشنامه‌ها از تحقیقات قبلی که در جدول ۱ آمده است و دارای مقیاس پنج امتیازی لیکرت (از خیلی کم تا خیلی زیاد) استفاده شده است .جامعه آماری پژوهش شامل تمامی متخصصان و مشاورین پیاده‌سازی سیستم مدیریت امنیت اطلاعات یک سازمان مورد مطالعه در شهر تهران می‌شود که در سطح شهر تهران در زمینه مدیریت امنیت اطلاعات برای سیستم‌های اطلاعاتی و پیاده‌سازی آن در سازمان نمونه، مشغول فعالیت بوده یا دست‌کم سابقه کار در زمینه امنیت سیستم‌های اطلاعاتی و امنیت شبکه را داشته و از دانش کافی در این زمینه برخوردار می‌باشند. نمونه مورد مطالعه به روش نمونه در دسترس به تعداد ۱۰۴ نفر در نظر گرفته شده است. به منظور تجزیه و تحلیل داده‌های به‌دست آمده از پرسشنامه‌های جمع‌آوری‌شده، در سطح توصیفی از درصد و فراوانی با نرم‌افزار SPSS و در سطح استنباطی جهت آزمون روایی و پایایی مدل، بار عاملی گویه‌ها، آزمون فرضیه‌ها از آزمون آلفای کرونباخ، آزمون مدل اندازه‌گیری و آزمون مدل ساختاری استفاده شده است که برای انجام این آزمون‌ها از نرم‌افزار PLS3 استفاده شده است؛ جدول زیر نتایج روایی و پایایی سؤالات پرسشنامه را نشان می‌دهد:

جدول ۱- نتایج روایی و پایایی

متغیر	الفای کرونباخ
فناوری و تکنولوژی	۰/۷۸۶
عوامل سازمانی یا درونی	۰/۷۵۴
عوامل خارجی یا بیرونی	۰/۹۳۴
مدیریت امنیت اطلاعات ISMS	۰/۸۱۴

۵- تحلیل داده‌ها

با توجه به اینکه هدف این تحقیق، مدیریت امنیت اطلاعات در یک سازمان نظامی بوده، لذا عوامل شناسایی‌شده مورد آزمون قرار گرفت و مدل اصلی تحقیق بصورت زیر ترسیم گردید:



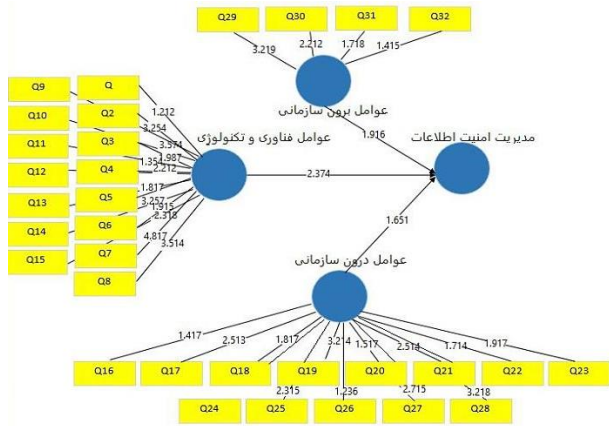
شکل ۱- مدل اصلی تحقیق

همانطور که از داده‌های جدول (۲) مشخص است، ۴٪ افراد پاسخ‌دهنده زن و ۹۴٪ آنها مرد هستند؛ همچنین در بازه سنی ۳۶ الی ۴۵ سال قرار داشته‌اند و بیشتر پاسخ‌دهندگان تقریباً ۵۲/۹ درصد دارای مدرک کارشناسی بوده‌اند.

جدول ۲- ویژگی‌های جمعیت‌شناختی نمونه آماری

جنسیت	فراوانی مشاهده‌شده	درصد فراوانی
زن	۴	۴
مرد	۹۴	۹۴
تحصیلات	فراوانی مشاهده‌شده	درصد فراوانی
فوق‌دیپلم	۱۰	۹/۶
لیسانس	۵۵	۵۲/۹
فوق‌لیسانس	۳۶	۳۴/۶
دکتری و بالاتر	۱	۱
سن	فراوانی مشاهده‌شده	درصد فراوانی
۲۵سال و کمتر	۷	۶/۷
۲۶ الی ۳۵ سال	۳۳	۳۱/۷
۳۶ الی ۴۵ سال	۳۶	۳۴/۶
۴۶ الی ۵۵ سال	۱۹	۱۸/۳
بالای ۵۶ سال	۶	۵/۸

عوامل تأثیرگذار در پیاده‌سازی مدیریت امنیت اطلاعات در سازمان خدماتی طبق شکل (۲) بدست آمد.



شکل ۲- خروجی مدل ساختاری در نرم‌افزار اسمارت پی‌آل‌اس

عوامل فناوری برای پیاده‌سازی مدیریت امنیت اطلاعات در سازمان مورد مطالعه به شرح جدول (۳) می‌باشد.

جدول ۳- فناوری ISMS

وضعیت سیستم‌های موروثی و زیرساخت فناوری اطلاعات (پیچیدگی سیستم‌های موجود و امکانات شبکه)
تیم‌های امنیتی و فنی پاسخگو (CERT)
نظام پذیرش سیستم (استاندارد فاوا)
به‌کارگیری مدیریت تداوم سرویس‌های ICT قبل از ISMS
انطباق و همسویی کامل با سایر پروژه‌ها و طرح‌های فاوا
خط‌مشی، سیاست‌های امنیتی و اجرایی
ممیزی و تحلیل اندازه‌گیری
توان و کیفیت نظارتی کارفرما
ارتقاء سطح آموزش، تخصص و مهارت کارکنان
بکارگیری تجربیان قبلی
تعیین دامنه و قلمرو پیاده‌سازی سیستم
تحلیل شکاف مناسب قبل از پیاده‌سازی استاندارد
برآورد و ارزیابی ریسک دارایی‌ها
به‌کارگیری سیستم‌های نرم‌افزاری و سخت‌افزاری مرتبط با ISMS
مدیریت داده‌ها و اطلاعات موجود

۲- عوامل درون‌سازمانی برای پیاده‌سازی مدیریت امنیت اطلاعات در سازمان مورد مطالعه به شرح جدول (۴) می‌باشد:

جدول ۴- عوامل درون‌سازمانی

فرهنگ‌سازمانی
باورهای مشترک
مدیریت تغییر
مدیریت منابع مالی و انسانی
نظام ایجاد انگیزش
اهداف شفاف
ارتباطات و آگاهی
مشارکت سازنده کارکنان
مدیریت پروژه
رسمیت
نقش مدیریت ارشد در پیاده‌سازی سیستم
تمرکزگرایی
مدیریت دانش

۳- عوامل خارجی عوامل درون‌سازمانی برای پیاده‌سازی مدیریت امنیت اطلاعات در سازمان مورد مطالعه به شرح جدول (۵) می‌باشد:

جدول ۵- عوامل برون‌سازمانی

الگوبرداری
تحریم‌ها
شرایط سیاسی
مشاور، مجری و پیمانکاران

۶- نتیجه‌گیری

دنیای امروز حفاظت از اطلاعات در برابر دسترسی غیرمجاز، تخریب، تغییر و افشاء یک ضرورت انکارناپذیر به‌شمار می‌رود و مستلزم یک روش مدیریتی تأثیرگذار می‌باشد. سیستم مدیریت امنیت اطلاعات (ISMS) یک راه ساختاریافته برای مدیریت اطلاعات محرمانه و حساس یک سازمان می‌باشد که این اطلاعات در هر لحظه و در هر مکانی بتواند به صورت امن نگهداری شود، در واقع سیستم مدیریت امنیت اطلاعات قرار است یک هماهنگی بین تمامی فعالیت‌های امنیتی ایجاد کند. استاندارد ISO/IEC27001 پشتیبانی سیستم مدیریت امنیت اطلاعات را بر عهده می‌گیرد، این استاندارد بین‌المللی مدیریتی امنیت اطلاعات شامل دستورالعمل‌هایی است که مشخص می‌کند چه چیزی باید داخل ISMS قرار گیرد و به چه الزاماتی نیاز دارد تا بتواند ممیزی شود، این استاندارد زمینه مناسبی را برای بهره‌گیری از حفاظت اطلاعات سازمانی فراهم آورده است و به تمام سازمان‌ها با هر اندازه و ساختار کمک می‌کند.

سازمان ها در راستای اجرای سیستم مدیریت امنیت اطلاعات (ISMS) اقدام به تدوین خط‌مشی‌ها و اهداف سازمانی و فرایندی می‌کنند و ممیزی ابزار مناسبی برای مطمئن‌شدن مدیران از اجرای صحیح کارها و حرکت مطابق برنامه و اهداف است. مدیران سازمان‌ها از طریق گزارش‌های ممیزی می‌توانند عملکرد امنیتی سازمان خودشان را بررسی و تحلیل کنند، از تحقق برنامه‌های تعیین‌شده در راستای دستیابی به اهداف و خط‌مشی امنیتی سازمان اطمینان حاصل نمایند. ممیزی‌های سیستمی در سیستم مدیریت امنیت اطلاعات (ISMS) این امکان را به سازمان‌ها می‌دهند تا در کنار این ممیزی‌ها فرصت‌های بهبود و فرصت‌هایی که می‌تواند به پیشرفت سازمان کمک کند را شناسایی کنند و با اجرای این فرصت‌ها سودآوری سازمان را بالا ببرند.

برای پیاده‌سازی و 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 سیستم‌های مدیریت امنیت و امنیت در سیستم‌های اطلاعاتی نگریسته شده است.

در این پژوهش با بررسی کامل سیستم‌های مدیریت امنیت اطلاعات و نحوه پیاده‌سازی آن در یک سازمان با توجه به میزان درخواست و بزرگی سازمان و خدمات بعد از پیاده‌سازی پرداختیم. یکی از مهم‌ترین بخش استقرار سیستم مدیریت امنیت اطلاعات در سازمان ممیزی سیستم استقرار یافته در سازمان می‌باشد که می‌تواند به نوعی تعیین‌کننده استقرار کامل و بی‌نقض باشد. از جهتی با استقرار این سیستم می‌توان سیستم بهینه‌ای را ارائه نمود که هدر رفتن وقت، نیروی انسانی، منابع و انرژی کارکردن برای استقرار جلوگیری شود. از لحاظی هم می‌توان در تعیین ارائه سرویس به محدوده موردنظر سازمان جهت استقرار و بهینه‌سازی در محدوده سازمان با توجه به نوع امنیت تصمیم‌های مناسب‌تری گرفت با توجه به تلفیق معماری سرویس‌گرایی با سیستم مدیریت امنیت اطلاعات می‌توان میزان امکان سنجی استقرار یک سیستم مجتمع و بهینه را بررسی نمود که در این پژوهش مشخص گردید که در صورت تغییرات در پیاده‌سازی سیستم و یا بروز مشکل در پیاده‌سازی سیستم و امنیت در اطلاعات، به کمک سرویس‌گرایی تا حدودی مشکل را حل نمود.

شاید استفاده از سیستم امنیت اطلاعات به نظر سخت آید اما به‌کارگیری آن لازم و ضروری است و هزینه‌هایی نیز دارد که در نگاه اول ممکن است این هزینه‌ها زیاد به نظر آید اما هزینه‌هایی هستند که فواید بیشتری دارند. استقرار این نظام باعث ایجاد حساسیت و کنترل بهتر جهت حفظ محرمانگی اسرار یک سیستم است و در آن نقش آموزش و برنامه‌ریزی کلان جهت نیروی انسانی و جلوگیری از حوادث اطلاعاتی نقشی بسیار مؤثر است که بجز با حمایت مدیران یک مجموعه امکان‌پذیر نمی‌باشد. برای اینکه بتوانیم حمایت مدیران را جهت برقراری امنیت اطلاعات جلب کنیم بهتر است سیستمی مناسب را ارایه نماییم تا حمایت آنان را برای تقویت امنیت اطلاعات به‌دست آوریم و در این راستا (ISMS) یک سیستم مناسب و استاندارد برای این امر می‌باشد.

خروجی پژوهش مطابق با پژوهش‌های پیشین می‌باشد [۱۱]. پژوهش قبلی نیز نشان می‌دهد فناوری بیشترین تأثیر را در پیاده‌سازی سیستم‌های امنیتی دارد.

نتایج کاربردی این پژوهش را می‌توان به صورت زیر جمع‌بندی کرد: (۱) عوامل تأثیرگذار در پیاده‌سازی مدیریت امنیت اطلاعات در سازمان مورد مطالعه مشخص گردید، (۲) فناوری، عوامل درون‌سازمانی و برون‌سازمانی برای پیاده‌سازی مدیریت امنیت اطلاعات در سازمان مورد مطالعه مشخص گردید، (۳) فهم و ادبیات مشترکی از پیاده‌سازی و ابعاد مدیریت امنیت اطلاعات در سازمان مورد مطالعه ایجاد شد، (۴) نگاه مدیران برای پیاده‌سازی مدیریت امنیت اطلاعات علاوه بر درون سازمان به بیرون سازمان و عوامل تأثیرگذار آن معطوف شد، (۵) باعث تبیین متناسب قلمرو و عمکلرد هر سازمان در زمینه پیاده‌سازی مدیریت امنیت اطلاعات شد، (۶) با انجام این تحقیق سازمان مرکزی متقاعد شد تا نسبت به برگزاری دوره های آموزشی مرتبط و بازآموزی موضوع سیستم امنیت اطلاعات اقدام نماید، (۷) فرصتی مهیا شد تا کمیته شبکه و امنیت در مجموعه سازمان مورد مطالعه تشکیل شود و (۸) در مباحث امنیت نقطه نظرات مدیران امنیت سازمان‌های دولتی اخذ و در بعضی از موارد به‌عنوان سؤال های چالش‌برانگیز به مخاطبان موضوع (مجریان و پیمانکاران) انتقال داده شد و اطلاع‌رسانی این مجموعه نظرات و تفکرات می‌تواند دستاورد مفیدی برای بخش خصوصی فعال در این حوزه باشد.

مقایسه یافته های این مقاله با مطالعات پیشین نشان می‌دهد که درحالی‌که تحقیقات قبلی بیشتر تمرکز بر ابعاد فنی و فناورانه مدیریت امنیت اطلاعات (ISMS) داشتند، این تحقیق با رویکرد گسترده‌تر، علاوه بر فناوری، به شناسایی عوامل درون سازمانی و برون سازمانی نیز پرداخته است. نتایج نشان می‌دهد که فناوری تنها جنبه‌ای از موفقیت ISMS است و عوامل سازمانی مانند فرهنگ سازمانی، مدیریت تغییر و نقش رهبری نیز تأثیر قابل‌توجهی در پیاده‌سازی موفق این سیستم دارند. این یافته با تحقیقات مشابه مانند مطالعه یوسفی‌انپور (۱۴۰۱) و مهری (۱۴۰۰) هماهنگ است که تأکید کرده‌اند بر اهمیت عوامل غیرفنی در مدیریت امنیت اطلاعات. بنابراین، این مقاله با تلفیق دیدگاه‌های مختلف، چالش‌های موجود در مطالعات پیشین را پوشش داده و زمینه‌ی مناسبی برای برنامه‌ریزی راهبردی در حوزه ISMS فراهم آورده است.

- **پیشنهادهای اجرایی**

با توجه به امر ضروری سیستم‌های امنیت در سازمان‌ها و زمان‌بر بودن استقرار، وجود یک راهبرد کاملاً بهینه به کمک سیستم‌ها و معماری‌های سازمانی و ممیزی کمک شایانی خواهد کرد. پایه‌ریزی تحقیقات در مورد استقرار سیستم های سازمانی و معماری‌های مختلف یکی از نیازمندی‌های ضروری محسوب می‌شود و لازم است تا محققان قدم‌های اساسی در این جهت بردارند، همچنین پیاده‌سازی سیستم‌های بهینه تعریف‌شده نیاز اعتمادسازی

در سازمان‌ها و ارائه منابع تحقیقات به سازمان‌ها در قبول این معماری‌ها خواهد بود. همچنین نرم‌افزاری و اتوماتیک‌کردن سیستم مدیریت امنیت و رعایت ملزومات از طرف کارمندان و ممیزی از طرف کارمندان و ممیزان به کمک سیستم‌های کاراتر می‌تواند به بلوغ سازمان و بالابردن امنیت کمک نماید. در پایان هم برای بهبود در برقراری امنیت در سیستم‌های اطلاعاتی، راهکارهایی ارائه شده است که این راهکارها را می‌توان به دو دسته کلی تقسیم کرد.

دسته اول راهکارهایی است که مشابه راهکارهای امنیتی در سایر سیستم‌های اطلاعاتی است، مانند استفاده از اصول رمزنگاری در قسمت احراز هویت یا تکثیر سرویس‌ها برای افزایش سطح دسترسی.

دسته دوم راهکارهایی هستند که بیشتر به ISO27001 اختصاص دارند، مانند استفاده از گذرگاه سرویس سازمانی برای اجرای کنترل‌های 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 ارائه‌شده تا اندازه‌ای به تصمیم‌گیری بهتر مدیران و مجریانی مسئول برقراری سیستم‌های مدیریت امنیت در سیستم‌های اطلاعات سازمانی کمک کند و بتواند سیستم بهینه مدیریت امنیت را در سیستم‌های اطلاعاتی سازمانی توسعه‌یافته تا حد زیادی برقرار کند.

۷- مراجع

۱- احمدی، زکیه، ناصری، علی و قرشی، سیده ندا، "سیستم مدیریت امنیت اطلاعات ISMS"، پانزدهمین کنفرانس دانشجویی مهندسی برق ایران، کاشان، سازمان علمی دانشجویی مهندسی برق کشور، ۱۳۹۱.

۲- امیری، مجتبی، زمانیان، مصطفی و روزبهانی، خدیجه، "استخراج عوامل شکست پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) در کشورهای در حال توسعه (با تمرکز بر سازمان‌های ایرانی)"، فصلنامه سیاست‌نامه علم و فناوری، دوره ۵، شماره ۲، ۱۳۹۴.

۳- ایرانپور اردهایی، سیدمهدی، "بررسی چالش‌های پیاده‌سازی سیستم مدیریت امنیت اطلاعات با استفاده از روش MEHARI و بررسی میزان آمادگی پژوهشگاه خواجه نصیرالدین طوسی در پیاده‌سازی این سیستم"، پژوهشکده علوم انسانی و اجتماعی، دانشگاه پیام‌نور استان تهران، ۱۳۹۴.

۴- حسینی، سیدرضا، علیرضانژاد، مهدی و خدابنده، پوریا، "بررسی اصول و پایه‌های امنیت اطلاعات و پایگاه داده در سازمان‌ها"، دهمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات، بابل، ۱۳۹۹.

۵- تقی‌زادگان، هادی، "ویژگی نقش سازمانی و پیاده‌سازی امنیت اطلاعات در مدیریت دانش"، همایش پژوهش‌های مدیریت و علوم انسانی در ایران، تهران، مؤسسه پژوهشی مدیریت مدبر، دانشگاه تهران، ۱۳۹۵.

۶- جویبار، زهرا، "ضرورت پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان‌های مجازی"، کنفرانس فناوری اطلاعات و جهاد اقتصادی، کازرون، مجتمع آموزش عالی کازرون، ۱۳۹۰.

۷- صادقی، پویا و علی‌پور، صادق، "اهمیت و نقش امنیت اطلاعات در شبکه‌های هوشمند"، پنجمین کنفرانس بین‌المللی توسعه فناوری در مهندسی برق ایران، تهران، ۱۴۰۰.

۸- عزیزی محمودآباد، رویا و عزیزی محمودآباد، مهران، "ضرورت پیاده‌سازی سیستم مدیریت امنیت اطلاعات در دولت الکترونیک"، کنفرانس بین‌المللی پژوهش‌های کاربردی در فناوری اطلاعات، کامپیوتر و مخابرات، تربت‌حیدریه، شرکت مخابرات خراسان، ۱۳۹۴.

۹- یوسفیان‌پور، ازهار، "بررسی تأثیر رویکردهای سازمانی بر عملکرد مدیریت امنیت اطلاعات در اداره کل امور اقتصادی و دارائی استان خوزستان"، پایان‌نامه کارشناسی‌ارشد، مؤسسه آموزش عالی فراز، گروه مدیریت، ۱۴۰۱.

۱۰- سواری، علی، "بررسی تأثیر عوامل نگرشی بر حفظ امنیت اطلاعات با نقش میانجی انگیزه حفظ اطلاعات (مورد مطالعه: سازمان تأمین اجتماعی اهواز)"، پایان‌نامه کارشناسی‌ارشد، دانشگاه پیام‌نور استان مرکزی، مرکز پیام‌نور اراک، ۱۴۰۱.

۱۱- مهری، محدثه، "بررسی تأثیر آگاهی جامع از امنیت اطلاعات و ویژگی‌های شناختی بر عملکرد مدیریت تهدید در حوزه سیستم اطلاعاتی. بررسی تأثیر آگاهی جامع از امنیت اطلاعات و ویژگی‌های شناختی بر عملکرد مدیریت تهدید در حوزه سیستم اطلاعاتی"، پایان‌نامه کارشناسی‌ارشد، دانشگاه‌الزهرا (س)، دانشکده علوم اجتماعی و اقتصادی، ۱۴۰۰.

۱۲- اسدالهی، داود، "مدیریت ریسک یکپارچه در سیستم مدیریت امنیت اطلاعات"، پایان‌نامه کارشناسی‌ارشد، مؤسسه آموزش عالی یاسین، گروه کامپیوتر، ۱۳۹۹.

۱۳- خداشناس، نرگس، "بررسی تأثیر قابلیت‌های فناوری اطلاعات بر عملکرد شرکت‌ها با نقش واسطه‌ای سیستم مدیریت امنیت اطلاعات"، پایان‌نامه کارشناسی‌ارشد، مؤسسه آموزش عالی اترک - قوچان، گروه کامپیوتر، ۱۳۹۹.

۱۴- خیری، سعید، "شناسایی، تحلیل و رتبه‌بندی عوامل مؤثر کلیدی در پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان‌های حاکمیتی (مطالعه موردی: سازمان بنادر و دریانوردی)"، فصلنامه تخصصی بندری، دریایی و کشتیرانی، دوره ۲، شماره ۳، ۱۳۹۵.

۱۵- شیخعلی، داود، حسنوی، رضا و رمضان، مجید، "بررسی تأثیر امنیت فناوری اطلاعات در اجرای سامانه مدیریت دانش"، بهبود مدیریت، دوره ۱۰، شماره ۳۴، صفحات ۲۵-۴۷، ۱۳۹۵.

۱۶- گلستانی‌زاده، محبوبه و سلطان آقایی کوپایی، محمدرضا، "ضرورت استقرار سیستم مدیریت امنیت اطلاعات در سازمان‌های هزاره سوم"، اولین همایش ملی فناوری اطلاعات و ارتباطات و محاسبات نرم‌افزار، ۱۳۹۵.

۱۷- غلام‌نژاد، پژمان و مظلوم، جلیل، "بررسی، تحلیل و انتخاب چارچوب استاندارد امنیتی برای زیرساخت‌های حیاتی وابسته به فاوا،" ۲۰۲۱.

۱۸- قاسمی‌نژاد، یاسر، محمودی، محمدعلی و قربانی، سپهر، "بررسی تأثیرات امنیت فناوری اطلاعات برعملکرد سیستم مرزبانی فراجا،" پژوهش‌های پیشرفت سیستم‌ها و راهبردها، ۲۰۲۳.

19- M. Al-Awadi, and K. Renaud, "Success factors in information security implementation in organizations," Paper presented at the IADIS International Conference e-Society 2007, Available in: http://www.dcs.gla.ac.uk /~karen/ Papers/sucessFactors2.pdf, 2007.

20- M. Karyda, A. Tsohou, and S. Kokolakis, "Analyzing the role of cognitive and cultutal biases in the internalization of information security policies: recommendations for information security awareness programs," Computers & security, vol. 52, no. 03, pp. 128-141, 2015.

21- R. Sheikhpour, and N. Modiri, "A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management," Indian journal of science and technology, vol. 5, no. 02, 70, 2012.

22- D. Tomal, "Action research for educators," Rowman & little field education, vol. 2, no. 20, pp. 200-202, 2010.

23- X. Ma, "IS professionals' information security behaviors in Chinese IT organizations for information security protection," Information Processing & Management, vol. 59, no. 01, 102744, 2022. https://doi.org/10.1016/j.ipm.2021.102744.

24- A. S. Aydiner, E. Tatoglu, E. Bayraktar, and S. Zaim, "Information system capabilities and firm performance: Opening the black box through decision-making performance and business-process performance," International Journal of Information Management, vol. 47, pp. 168-182, 2019.

25- J. R. Kala Kamdjoug, H. J. Nguegang Tewamba, and S. Fosso Wamba, "IT capabilities, firm performance and the mediating role of ISRM: A case study from a developing country," Business Process Management Journal, 2018.

26- A. Kakkar, R. Punhani, and S. Madan, "Implementation of ISMS and its Practical Shortcomings," International Refereed Research Journal ISSN 1839-6518, Vol. 02, No. 01, www.irj.iars.info, 2012.