مدیریت عصر پیشرفت

ارزیابی استفاده مدیران از سیستم های امنیت اطلاعات مدیریت در چابکی و فرایند تصمیم-گیری در سازمان

سامان حمیدی آشتیانی[۱]

چکیده

هدف از پژوهش حاضر بررسی و ارزیابی استفاده مدیران از سیستم های امنیت اطلاعات مدیریت در چابکی و فرایند تصمیم-گیری بوده است. این پژوهش از نظر هدف کاربردی و از نظر روش توصیفی- پیمایشی می‌باشد. جامعه آماری پژوهش مدیران و کارشناسان سازمان معاونت اداری، مالی و مدیریت منابع وزارت علوم شهر تهران بوده که با روش نمونه‌گیری خوشه‌ای انتخاب گردید و سپس اطلاعات مورد نیاز پژوهش از کلیه مدیران عالی و میانی آن سازمان‌ها جمع‌آوری گردید. در مجموع حجم نمونه آماری ۲۰۵ نفر بود. برای جمع‌آوری داده‌ها از پرسشنامه و برای تجزیه و تحلیل داده‌ها، از آمار توصیفی (جدول توزیع فراوانی، درصد فراوانی) و آمار استنباطی (آزمون کولموگروف- اسمیرنف، آزمون t، آزمون ضریب همبستگی اسپیرمن، آزمون رگرسیون چند گانه گام به گام) استفاده شده است. نتایج حاصل از پژوهش نشان داد تفاوت معناداری بین دو گروه مدیران زن و مرد در استفاده از سیستم امنیت اطلاعات مدیریت وجود ندارد. همچنین بین گروه‌های با سطوح جایگاه سازمانی متفاوت در استفاده از آن نیز تفاوتی مشاهده نشد. همچنین بین میزان استفاده مدیران از سیستم امنیت اطلاعات بر اساس گروه‌های سنی تفاوت وجود دارد به گونه‌ای که مدیران مسن‌تر کمتر از این سیستم استفاده می‌کنند و بین میزان استفاده از این سیستم بر اساس گروه‌های سابقه خدمت تفاوت وجود دارد. تحلیل رگرسیونی گام به گام حاکی از این است که شش عامل آگاهی مدیر، حمایت سازمانی، حمایت مالی، کاربرد اینترنت، حمایت مدیر، در دسترس بودن و اعتقاد به اثربخشی به عنوان مهمترین عوامل موثر بر بکارگیری سیستم امنیت اطلاعات می‌توانند یک مدل قابل اتکا برای برآورد میزان کاربرد این سیستم ارائه نمایند.

واژه‌های کلیدی: سیستم امنیت اطلاعات، فرایند تصمیم‌گیری، مدیریت، چابکی تصمیم‌گیری

[۱]کارشناسی ارشد MBA ، دانشگاه پیام نور تهران غرب
Samanhamidiashtiani@gmail.com

۱. مقدمه

در شرایط دائماً در حال تغییر ما نیز باید تغییر نمائیم وگرنه بهای سنگینی بابت عدم تغییر پرداخت خواهیم کرد. سازمان[۲]ها را در عصر جدید از بکارگیری سیستمهای کامپیوتری و تکنولوژی اطلاعات و رسانه های پیش رفته گریزی نیست و آینده از آن آنانی است که با شناخت دقیق و صحیح، محاسن و معایب این سیستم ها را موشکافانه مورد نظر قرار داده و از تجربه دیگران درس بگیرند بدون اینکه هزینه های آن تجربه را مجدداً تقبل نمایند. تصمیم گیری یعنی آنچه که مدیران در سطوح مختلف سازمان انجام می دهند و همواره در فضای آن حرکت می نمایند، تصمیم گیری را می توان جمع آوری و پردازش اطلاعات در نظر گرفت. روند مستمر و رو به رشد و تحول در شئون مختلف حیات اجتماعی بشر و پیشرفتهای شگرف و عمیق علوم و فنون گوناگون، موجبات تحول ساختارهای سازمانی را از اشکال سنتی به سوی ساختارهای پیچیده تر و تخصصی فراهم آورده است. امروزه به منظور اداره صحیح سازمان و اتخاذ تصمیمات منطقی و درست توسط مدیران، ایجاد سیستم اطلاعات مدیریت امری اجتناب ناپذیر است(.اولتین[۳] ،گابور و کانتیو همکاران،۲۰۱۴).

توجه به اطلاعات و مدیریت اطلاعات و امنیت آن یکی از ملاحظات مدیریتی هر سازمان تلقی می شود. در دهه کنونی، اطلاعات به شکل یک پدیده اصلی و تاثیر گذار در کلیه امور سازمانها و حتی زندگی افراد درآمده است. مواجهه با چنین پدیده‌ای بدون وجود یک سیاست کلان و عوامل اجرای هماهنگ آن سیاست مقدور نمی باشد. پیشرفت تکنولوژی کامپیوتر و رواج آن از یک سو و توسعه کمی و کیفی مخابرات داده ها از سوی دیگر باعث شده است که سرعت فزاینده و تصاعدی در تولید اطلاعات ایجاد شود. امروزه در موارد بسیاری چرخش امور روزمره افراد و سازمانها تولید اطلاعات می کنند. این فرایند، با رشد تکنولوژی ذخیره سازی و انتقال اطلاعات همراه بوده است به گونه ای که ماهیت اطلاعات امروز با ماهیت اطلاعات دهه گذشته متفاوت بوده و می توان گفت که اطلاعات امروزی الکترونیکی و اطلاعات قبلی غیرالکترونیکی هستند. در این بین حیات سازمان ها ارتباط نزدیکی با سیستم های اطلاعاتی و اطلاعات الکترونیکی آنها دارد. علاوه بر این سیستم های اطلاعاتی همواره در خطر سرقت اطلاعات، تغییر اطلاعات و ایجاد وقفه در خدمات رسانی هستند. به منظور حل مسئله امنیت اطلاعات، سازمان نیازمند به کارگیری طیف گسترده ای از دانش، فناوری و قوانین سازمانی است و درعین حال باید مطمئن شد که سازمان فقط روی راه حل های فنی متمرکز نیست، بلکه اجزای کلیدی دیگر امنیت اطلاعات، شامل فرایند ها و کارکنان نیز در آن لحاظ شده است(آندری[۴]،۲۰۱۹).

برای سیستم مدیریت امنیت اطلاعات ویژگی های گوناگونی بیان شده است. برای مثال ذکرشده که باید مدیریت آن متمرکز باشد و واحد و فرایندهایی مجزا از سایر بخش های سازمانی به ویژه بخش فناوری اطلاعات داشته باشد. البته باید هماهنگی و هم راستایی میان قسمت های گوناگون نیز حفظ شود(رهنمایی،ذکاوت[۵]،۲۰۱۷). همچنین تاکید شده است که رویکرد صحیح باید تکرارشونده، نظام مند، کامل، سازگار و آسان برای درک، تجزیه و تحلیل باشد.

ویژگی دیگر آنکه رویکرد مدیریت امنیت، باید تعادلی،میان حفاظت اطلاعات و دسترسی مجاز باشد. نکته مهم این است که امنیت اطلاعات باید در تمام سطح

[2] Organization
[3] Oltean, Gabor & Conţiu
[4] Andrii. B
[5] Rahnamaii Zakavat, m

سازمانی(راهبردی، تاکتیکی و عملیاتی)مدیریت شود و کنترل های لازم پیاده سازی شوند . همچنین بهتر است امنیت اطلاعات به صورت فرایندی مداوم اجرا شود و شناسایی، ارزیابی و پیاده سازی را برای همه اجزا در برگیرد(رضایی علی و همکاران[6]،۲۰۱۸).

همچنین چارچوب مدیریت امنیت باید به گونه ای باشد که اجرایش آسان، کم هزینه و مناسب با نیازهای تجارت الکترونیکی باشد. از آنجا که توجه به امنیت اطلاعات و رعایت قوانین و مقررات در جهت جلوگیری از دسترسی های غیر مجاز و سایر تهدیدها در واقع توجه و اهمیت دادن به سلامت محیط کار و بقای سازمان می باشد. برای برقراری سرویس امن در جهت بهره برداری از امکانات باید به اصولی از قبیل صدور مجوز، واگذاری حداقل اختیارات، حیطه بندی (جداسازی) و در نهایت پشتیبان گیری مرتب و مطمئن از اطلاعات توجه نمود (شاه بهرامی ، اسدا .. رفیع زاده کاسانی ، رامین،۱۳۹۴).

باید در نظر داشته باشیم بشترین آسیب و صدمه ها از کم توجهی کارکنان در زمان کار با سیستم های رایانه ای پیش می‌آید توجه به دستورالعمل های حفاظتی و امنیتی و دقت در اجرای مفاد آنها به نحو شایسته و موثری آسیب ها و صدمات را کاهش می دهد. با توجه به گسترش استفاده از اینترنت، تبادلات اطلاعاتی و هزینه های صرف شده به منظور یکپارچگی اطلاعاتی، امروزه مبحث کنترل و مدیریت جابه جایی های اطلاعاتی و برخورداری از سامانه جامعی برای مدیریت امنیت اطلاعات، بیش از پیش احساس می شود (اسکندری، حمید؛ امیرصوفی، رحمت الله،۱۳۹۱). امنیت اطلاعات مبحث بسیار مهمی است زیرا هدف آن حفاظت کاربر در برابرتهدیدها و ریسک ها و دسترسی به اطلاعات امن، مطمئن و محرمانه است و برای اطمینان از امنیت آن، سازمان باید سیاست‌ها و خط مشی های امنیت اطلاعات را شناسایی و تبیین کند. امنیت داده ها، روش هایی برای سازمان دهی مطمئن اطلاعات کاری،مالی و خانوادگی با استفاده از نرم افزارهای خاص و تأمین داده ها و پیشگیری از وقوع جرم است(زندیان، قرابی، حسن زاده[7]،۲۰۱۸).

امنیت اطلاعات و ارتباطات به محافظت از اشکال مختلف داده ها، سرویس ها، سیستم ها و ارتباطات در برابر مخاطرات گفته می شود. امنیت فرایندی است جهت جلوگیری از نشت، سرقت، از بین رفتن و دستکاری اطلاعات به منظور محافظت از صحت و محرمانگی اطلاعات. از نگاه اجرایی امنیت اطلاعات به تکنیک ها، سیاست ها و آیین نامه هایی اطلاق می گردد که در سازمان مورد استفاده افراد غیرمجاز و ناشناس قرار نگیرد. تدابیر امنیتی باید مبتنی برتضمین امنیت تجهیزات، تاسیسات، منابع انسانی، دستورالعمل‌ها، آیین نامه ها، اسناد و مدارک مربوطه و مهم تر از همه سخت‌افزارها و نرم افزارهای مورد استفاده در شبکه های ارتباطی براساس نوع تهدیدات و شدت آنها باشد که ممکن است تهدیدات، داخلی باشند یا خارجی که معمولا عمده تهدیدات از ناحیه ضعف فناوری، ضعف سیاست گذاری امنیتی و حفاظتی و ضعف کاربران شناخته شده است(سومرو، شاه و احمد[8]، ۲۰۱۶). امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن خطر افشای اطلاعات در بخش های غیر مجاز اشاره دارد(زرگری[9]،۲۰۱۷).

امنیت اطلاعات مجموعه ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری است و علم مطالعه روش های حفاظت از داده ها در رایانه ها و نظام های ارتباطی در برابر دسترسی و تغییرات غیر مجاز است(تاج فر،احمد و محمودی میمند،رضا سلطانی، فرامرز؛ رضا سلطانی، پدرام ؛۱۳۹۳).

هدف سیستم مدیریت امنیت اطلاعات پشتیبانی از دارایی های اطلاعاتی الکترونیکی موجود در محدوده سیستم

[6] Rezaei, Ali, Mossadegh, Mohammad Javad, Rezaei, Mona
[7] Zandiyan, F, Gharavi, A, Hassanzadeh, M
[8] Soomro, Z. A., Shah, M. H., & Ahmed, J
[9] Zargari, K

مدیریت امنیت اطلاعات از تهدیدهای امنیت اطلاعات، داخلی یا خارجی، عمدی یا اتفاقی می باشد .این دارایی ها شامل اطلاعات، داده ها، مستندات، سخت افزارها و نرم افزارهای مورد استفاده در فرایند نگهداری، انتقال و پردازش شامل اطلاعات سازمانی، اطلاعات همکاران و خدمات ارائه شده می باشد(اسکندری، حمید؛۱۳۹۱).

مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف، امنیت و بررسی موانع سر راه رسیدن به این اهداف و ارائه راهکارهای لازم را برعهده دارد. سیستم مدیریت امنیت اطلاعات یک رویکرد نظام مند به مدیریت اطلاعات حساس به منظور محافظت از آنهاست .امنیت اطلاعات چیزی فراتر از نصب یک دیوار آتش ساده یا عقد قرارداد با یک شرکت امنیتی است. در چنین رویکردی بسیار مهم است که فعالیت های گوناگون امنیتی را با راهبردی مشترک به منظور تدارک یک سطح بهینه از حفاظت همراستا کنیم .حفاظت بطور متداول به معنای رهایی از خطر یا ایجاد شرایطی برای سلامتی است. حفاظت و امنیت در رایانه ها از نظر نرم افزاری، حفاظت از داده‌ها و اطلاعات در برابر افشاء، تغییر یا تخریب توسط افراد غیرمجاز می باشد و از نظر سخت افزاری شامل حفاظت از سیستم رایانه در مقابل استفاده غیرمجاز، تغییر یا تخریب رایانه می گردد(پلتیر[10]،۲۰۱۶).

افراد غیر مجاز، کاربران، یا برنامه های اجرایی هستند که بدون نظارت و یا بصورت دزدانه، عملیات فوق را انجام می دهند. بدلیل اینکه ایجاد کنترل های حفاظتی باعث جلوگیری از بهره برداری رایانه ها می شود، ایجاد حفاظت و امنیت معمولا شامل پروسه‌ای می گردد که سرپرستان، متصدیان حفاظت و کاربران سیستم بتوانند در یک تعادلی بین حفاظت و کارایی، فعالیت خود را انجام دهند. روشهای کنترل برای ایجاد امنیت اطلاعات، شامل سه بخش ایجاد کنترل های فیزیکی، ایجاد کنترل های تکنیکی و ایجاد کنترل های اداری می شود که هر یک از این سه بخش به دو زیر مجموعه روش های کنترل مبتنی بر ممانعت و روش های کنترل مبتنی بر آشکارسازی تقسیم می گردند .که با آنها ممانعت کننده ها و آشکار کننده ها می گوییم .ممانعت کننده ها تلاش می کنند که از اتفاقات ناخواسته جلوگیری نمایند در حالی که آشکارکننده ها تلاش می کنند اتفاقات ناخواسته را پس از اینکه اتفاق افتادند قابل رویت نمایند(نازرت، چوی،۲۰۱۵).

استفاده کنندگان رایانه ها به منظور بهره برداری از دستاوردها و مزایای فناوری اطلاعات و ارتباطات، ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مولفه های تاثیرگذار در تداوم ارایه خدمات در یک سامانه رایانه ای می باشند .امنیت اطلاعات و ایمن سازی شبکه های رایانه ای از جمله این مولفه ها بوده که نمی توان آن را مختص یک فرد و یا یک سازمان در نظرگرفت. این مساله به تمامی افراد و کارکنان سازمانها مربوط می‌شود در محیط ها و سازمان های نظامی مسئولیت امنیت اطلاعات به عهده فرماندهان و مسئولین ارشد سازمانها می باشد که باید به این مساله توجه خاص نموده و از کارکنان مجموعه خود بخواهند(نورایی فرزاد، ۱۳۹۱).

موضوع مورد نظر از این جهت دارای اهمیت و ضرورت است که با توجه به این که سیستم‌های امنیت اطلاعاتی رایج در سازمان‌های کشورهای توسعه یافته، به طور مناسبی در خدمت مدیران این گونه سازمان‌ها قرار دارند، و از طرفی در عمل ملاحظه می‌شود علیرغم قابلیت‌های مناسبی که در این ابزارهای خوب به نحو شایسته‌ای از آنها استفاده نمی‌شود، لذا هدف از این پژوهش تعیین میزان بکارگیری سیستم‌های امنیت اطلاعاتی مدیریتی در سازمان وزارت علوم، تحقیقات و فناوری شهر تهران و شناسایی برخی عوامل موثر بر آن است. متأسفانه در گذشته از این سیستم در عمل کمتر در این سازمان استفاده گردیده و اخیراً نیز که توجه برخی از سازمان‌ها به بکارگیری از این سیستم‌ها

[10] Peltier, T. R

معطوف شده، در عمل با موانعی موجه گردیده‌اند که آنها را دچار سرخوردگی، سردرگمی و بعضاً مشکلات بیشتری نسبت به گذشته نموده است. علیرغم همه این موارد نیز متأسفانه بررسی و پژوهش جامعی در این مورد به عمل نیامده است. سازمانهای ایران و به تبع آن شهر تهران از پایین بودن بهره‌وری رنج می‌برند و بسیاری از مسئولین تلاش‌هایی جهت یافتن راه‌کارهای مناسب برای رفع این مشکل داشته‌اند. به نظر می‌رسد بهره‌گیری مناسب از سیستم‌های امنیت اطلاعات مدیریتی به منظور بهبود مدیریت مدیران و افزایش بهره‌وری آنان، می‌تواند یکی از این راه کارها باشد. اما به دلیل ویژگی‌های خاصی که برای این سازمان‌ها حاکم می‌باشد، به ویژه مسائل و مشکلاتی که از بعد فرهنگی و اجتماعی، در این سازمان‌ها و به خصوص نیروی انسانی شاغل در آنها (اعم از مدیران و کارکنان) وجود دارد، کاربرد این ابزار به سادگی امکان‌پذیر نیست و در عمل نیز مشاهده گردیده که کمتر سازمان خصوصی بوده است که توانسته باشد از این سیستم‌ها به نحو کارآمدی استفاده نموده باشد. لذا در صورتی که بتوان با انجام تحقیقاتی، راه‌کارهایی برای استفاده اثربخش از این سیستم‌ها ارائه نمود، قطعاً گام مفیدی در حل معضلات سازمان‌های خصوصی برداشته شده است.

قرایی و آقا محی الدین (۱۳۹۳) در پژوهشی با عنوان؛ بهبود رتبه مخاطبین امنیت اطلاعات با استفاده از مدلهای اصلاح شده چندشاخه، به معرفی امکان بهبود رتبه‌بندی مخاطرات امنیت اطلاعات با استفاده از مدل تصمیم‌گیری چند شاخصه پرداختند و این مدل را روشی کاربردی جهت ارزیابی و بهبود اقدامات مخاطرات امنیت دانسته اند.

اندری[11](۲۰۱۹)، برای ادغام موفقیت‌آمیز تجاری، یک رویکرد جدید برای شناسایی و پیش‌بینی خطر عرضه در شرایط عدم قطعیت، یک راه‌حل پیچیده برای ایمن سازی داده‌ها در سیستم‌های اطلاعاتی برای مدیریت زنجیره تامین پیشنهاد دادند.

زندیان و همکاران[12](۲۰۱۸) در پژوهش خود عنوان کردند که حمایت مدیریت عالی، آموزش کاربران، فرهنگ امنیتی میان کاربران، مهارت کاربران، تقویت خط مشی کاربران، خودباوری و تجربیات کاربران بر اثربخشی امنیت سیستم-های اطلاعاتی تاثیر مستقیم دارد.

رضایی و مصدق[13](۲۰۱۸) در پژوهش خود شاخص‌های نقش مدیریت، آگاهی از امنیت سیستم اطلاعات و انطباق با آموزش، امنیت سیستم اطلاعات کسب و کار و ارزیابی ریسک امنیت سیستم اطلاعات بر اثر بخشی سیستم مدیریت امنیت اطلاعات تاثیرگذار می‌باشند.

علوی و همکاران[14](۲۰۱۶)، نشان داد که رابطه معناداری بین ریسک‌ها و خطرات امنیت اطلاعات و میزان سرمایه-گذاری سازمان در این حوزه وجود دارد و استفاده از الگوی سرمایه‌گذاری مبتنی بر ریسک امنیت اطلاعات، نشان می-دهد که این امر به سازمان کمک می‌کند تا در حوادث دیگر از آن استفاده کنند.

یوسفی زنوز و همکاران[15](۲۰۱۵) در پژوهشی ریک‌های امنیت اطلاعات را شامل ریسک‌های برخاسته از عوامل انسانی(مدیران ارشد، مشاورین و کارکنان)، ریسک‌های برخاسته از سیستم اطلاعاتی دانستند.

با پیشرفت علوم کامپیوتری و هم چنین به وجود آمدن ابزارهای جدید هک و هم‌چنین وجود صدها مشکل ناخواسته در طراحی نرم‌افزارهای مختلف و روال‌های امنیتی سازمان، همیشه خطر حمله و دسترسی افراد غیرمجاز وجود دارد. حتی قوی‌ترین سایت‌های موجود در دنیا در معرض خطر افراد غیرمجاز قرار دارند. با وجود اینکه نمی‌توان امنیت ۱۰۰٪ داشت اما نباید به نکات امنیتی بی توجه بود.در این راستا این پژوهش دارای اهدافی است؛

اهداف اصلی

[11] Andrii
[12] Zandian et al
[13] Rezaii & Mosadegh
[14] Alavi et
[15] Yousefi Zenooz

۱- تعیین تاثیر ویزگی‌های سازمانی (آگاهی مدیر، حمایت مدیر، حمایت مالی، حمایت سازمانی، تصمیم‌گیری مدیران) بر میزان استفاده مدیران دستگاههای اجرایی شهر تهران از سیستمهای امنیت اطلاعات مدیریت در فرآیند تصمیم گیری

۲- تعیین تاثیر کاربرد کامپیوتر، آشنایی با سیستمهای امنیت اطلاعات مدیریت ، توانایی استفاده از سیستمهای امنیت اطلاعات مدیریت ، قصد استفاده از سیستمهای امنیت اطلاعات مدیریت بر میزان استفاده مدیران دستگاههای اجرایی شهر تهران از سیستمهای امنیت اطلاعات مدیریت در فرآیند تصمیم گیری

اهداف فرعی

۱- تعیین تاثیر ویژگی‌های فردی جنسیت، وضعیت تاهل، تحصیلات و سن بر میزان استفاده مدیران دستگاههای اجرایی شهر تهران از سیستمهای امنیت اطلاعات مدیریت در فرآیند تصمیم گیری

۳. روش تحقیق

پژوهش حاضر از نظرهدف (نوع پژوهش)، کاربردی می باشد و از حیث روش، توصیفی- پیمایشی به حساب می آید. برای جمع آوری داده های تحقیق در بخش میدانی از پرسشنامه محقق ساخته به منظور سنجش میزان آگاهی و استفاده مدیران از سیستم امنیت اطلاعات استفاده گردید. سؤالات بر اساس طیف نگرش سنجی دو ارزشی بصورت بله = ۱ و خیر = ۰ برای سوالات میزان آشنایی و میزان دسترسی و طیف لیکرت با پنج درجه خیلی کم=۱ ، کم=۲ ، متوسط=۳ ، زیاد =۴ و خیلی زیاد=۵ برای سایر متغیرها مورد ارزیابی قرار می گیرد. میانگین نظرات مدیران نمونه آماری در خصوص گویه های مربوط به متغیرهای پژوهش به عنوان مقدار بدست آمده برای متغیر مورد نظر منظور شد و در آزمونهای آماری مورد استفاده قرارگرفته است.

در تحقیق حاضر، از روش اعتبار یا روایی محتوایی استفاده شده است. بدین صورت که پس از انتخاب گویه های مربوط به سنجش متغیرها و مقیاس مرتبط برای تعیین میزان روایی مقیاسهای استفاده شده در این پژوهش از ۷ نفر از نخبگان و متخصصان مرتبط با موضوع درخواست شد که بیان دارند تا چه اندازه گویه ها و مقیاسها همان متغیری را می سنجند که برای آن طراحی شده اند، آنگاه گویه های نامرتبط حذف و گویه های ضعیف اصلاح گردیدند. در واقع روایی محتوایی ابزار جمع آوری اطلاعات با نظرخواهی از نخبگان سنجیده شده است.

در این پژوهش از روش نمونه گیری چند مرحله ای خوشه ای حتی المقدور کلیه مدیران عالی، میانی، عملیاتی و کارشناسان مسئول در سازمان وزارت علوم، تحقیقات و فناوری تهران به عنوان نمونه آماری انتخاب گردیدند و سعی گردیده نظر و دیدگاه تمام مدیران و مسئولان ادارات منتخب در این پژوهش بررسی شود. از پرسشنامه های توزیع شده تعداد ۲۰۵ پرسشنامه تکمیل و عودت داده شد.

٤. تحلیل داده ها

تحلیل داده‌ها و یافته‌ها

مشخصات جمعیت شناختی: از نمونه آماری ۸۷ نفره شرکت کننده در پژوهش بیشتر افراد یعنی ۵۲/۹ درصد آن‌ها را مردان و ۴۷/۱ درصد آن‌ها را زنان تشکیل داده‌اند. از نظر وضعیت تاهل نیز بیشترین درصد یعنی حدود ۵۷/۵ درصد متاهل و مابقی مجرد بوده‌اند. هم چنین در نمونه مورد مطالعه از لحاظ سن بیشترین آن‌ها یعنی در حدود ۵۶/۳ درصد در رده سنی ۲۸ تا ۳۷ بوده و کمترین آن‌ها یعنی حدود ۴/۶ درصد بین ۴۸ تا ۵۷ سال داشته‌اند. ۲۹/۹ درصد افراد در رده سنی ۳۸ تا ۴۷ سال و ۹/۲ درصد افراد بین سنین ۱۸ تا ۲۷ سال سن داشته‌اند. از نظر مدرک تحصیلی نیز می‌توان گفت در نمونه مورد مطالعه۳/۴ درصد دارای مدرک دیپلم و پایین‌تر، ۳۵/۶ درصد دارای مدرک تحصیلی فوق دیپلم و لیسانس، ۵۷/۵ درصد دارای مدرک فوق لیسانس و ۳/۴ درصد دارای مدرک دکتری بوده‌اند.

نتایج تحلیل‌های آماری:

برای بررسی فرضیات پژوهش از روش مدل‌سازی معادلات ساختاری استفاده شده است. اگر برازش مدلی که ترسیم می‌گردد، توسط شاخص‌های برازش مدل تأئید شود، از آن نمودار می‌توان برای آزمون فرضیات، در مورد وجود رابطه‌ی علی بین متغیرهای موجود در نمودار مسیر استفاده نمود. با توجه به مبانی نظری و فرضیات پژوهش به منظور پاسخگویی به فرضیات پژوهش مدل مفهومی شکل ۱ ترسیم و برازش داده شد. مدل طراحی شده در پژوهش با روش حداقل مربعات جزئی و توسط نرم افزار smartpls3 مورد آزمون قرار گرفت. از جمله معیارهای استفاده از روش حداقل مربعات جزیی حجم نمونه کمتر نسبت به متغیرهای پژوهش، حساس نبودن به نرمال بودن داده‌ها، قدرت پیش بینی مناسب‌تر، تحلیل بهتر مدل‌های جدید و در حال توسعه و تحلیل سازه‌ها با سوالات کمتر از ۳ و حتی تحلیل سازه یک سوالی می‌باشد.

با توجه به این که تحلیل داده‌ها در نرم افزار اسمارت پی ال اس در سه مرحله‌ی ارزیابی مدل اندازه گیری (روایی و پایایی)، ارزیابی مدل ساختاری و ارزیابی کلی صورت می-گیرد، بنابراین هریک به صورت مجزا مورد بررسی قرار گرفته است و سپس با استفاده از مدل ترسیم شده به پاسخگویی فرضیات پرداخته شده است.

ارزیابی پایایی و روایی مدل پژوهش

برای ارزیابی مدل اندازه اندازه‌گیری در ابتدا بارهای عاملی متغیرها مورد بررسی قرار می‌گیرد و با توجه به مقدار مطلوب آن، متغیرها با بارهای عاملی بزرگتر از ۰/۴ مجاز به استفاده در مدل هستند که در حالت سخت گیرانه‌تر این مقدار به بالای ۰/۷ نیز می‌رسد. در پژوهش حاضر به منظور تایید مدل در بخش اندازه گیری پژوهشگر ناچار به حذف سوالات ۵۳، ۴۴، ۲۸، ۲۷، ۲۶ و ۲۵ شد. برای ارزیابی مدل اندازه گیری شاخص‌های مرتبط با روایی و پایایی سازه‌های موجود در پژوهش از جمله پایایی شاخص (آلفای کرونباخ و پایایی ترکیبی)، روایی همگرا و روایی واگرا استفاده شد. مقدار آلفای کرونباخ و پایایی ترکیبی در جدول ۱ نشان از پایایی قابل قبول با میزان بالای ۰/۹ برای هر یک از متغیرهای مورد بررسی در پرسشنامه است. (مقادیر بالای ۰/۷ برای این دو شاخص مقادیر مطلوبی به حساب می‌آید.) روایی همگرا میزان همبستگی یک سازه با شاخص‌های خود را نشان می‌دهد که هر چه این همبستگی بالاتر باشد برازش نیز بهتر است و با ضریب AVE بررسی می‌شود که همانگونه که مشاهده می‌شود برای تمامی ۱۰ متغیر این مقدار بالای ۰/۵ و مطلوب است.

جدول ۱: مقادیر شاخص‌های پایایی و روایی مدل پژوهش

	قصد کاربرد ISMS	آشنایی با ISMS	توانایی استفاده از ISMS	آگاهی مدیر	تصمیم گیری مدیران	حمایت سازمانی	حمایت مالی	حمایت مدیر	میزان استفاده	کاربرد کامپیوتر
آلفای کرونباخ	۰/۹۱۴	۰/۹۵۸	۰/۹۴۶	۰/۸۵۹	۰/۸۲	۰/۹۱۳	۰/۹۳۵	۰/۹۲۱	۰/۹۳۹	۱
پایایی ترکیبی	۰/۹۳۶	۰/۹۶۵	۰/۹۵۵	۰/۹۳۴	۰/۹۱۷	۰/۹۳۵	۰/۹۵۸	۰/۹۴۲	۰/۹۵۲	۱
روایی همگرا (AVE)	۰/۷۴۷	۰/۷۷۴	۰/۷۰۱	۰/۸۷۶	۰/۸۴۶	۰/۷۴۱	۰/۸۸۵	۰/۷۶۴	۰/۷۶۷	۱

برای بررسی روایی واگرا از ماتریس فورنل- لارکر استفاده می‌شود. در این روش میزان همبستگی بین شاخص‌های یک سازه و میزان همبستگی شاخص‌های یک سازه با سازه‌های دیگر مقایسه می‌شود و اگر مقادیر روی قطر اصلی که همان جذر AVE هستند برای تمامی متغیرها از همبستگی میان آن‌ها (مقادیر قطر فرعی) بالاتر باشد این امر روایی واگرای مناسب و برازش خوب مدل اندازه گیری را نشان می‌دهد. همانطور که در جدول مشاهده می‌شود در مدل مورد مطالعه مقادیر روی قطر اصلی بالاتر از قطرهای فرعی است و مدل از روایی واگرای مناسبی برخوردار است. بنابراین در مجموع مدل در بخش اندازه گیری مورد تایید می‌باشد.

جدول ۲: ماتریس ارزیابی روایی واگرا بر اساس معیار فورنل -لارکر

	قصد کاربرد ISMS	آشنایی با ISMS	توانایی استفاده از ISMS	آگاهی مدیر	تصمیم گیری مدیران	حمایت سازمانی	حمایت مالی	حمایت مدیر	میزان استفاده	کاربرد کامپیوتر
قصد کاربرد ISMS	۰/۸۶۴									
آشنایی باISMS	۰/۴۳۶	۰/۸۸								
توانایی استفادهISMS	۰/۵۵۳	۰/۴۹۳	۰/۸۳۷							
آگاهی مدیر	۰/۵۲۳	۰/۶۴۲	۰/۶۴۴	۰/۹۳۶						
تصمیم گیری مدیران	۰/۵۵۸	۰/۴۸۹	۰/۴۸۷	۰/۴۹۲	۰/۹۲					
حمایت سازمانی	۰/۶۵۶	۰/۶۰۹	۰/۶۹۷	۰/۶۵۹	۰/۶۸۳	۰/۸۶۱				
حمایت مالی	۰/۵۹۵	۰/۵۳۱	۰/۶۳۹	۰/۵۸۸	۰/۵۵۹	۰/۷۹۵	۰/۹۴۱			
حمایت مدیر	۰/۶۵۳	۰/۴۵۷	۰/۶۹۳	۰/۶۶۸	۰/۶۱۶	۰/۷۹۷	۰/۸۶۴	۰/۸۷۴		
میزان استفاده	۰/۶۶	۰/۴۵۸	۰/۶۲۶	۰/۶۸۳	۰/۴۵	۰/۶۹۷	۰/۶۵۱	۰/۷۱۲	۰/۸۷۶	
کاربرد کامپیوتر	۰/۴۰۸	-۰/۰۴۵	۰/۳۰۷	۰/۲۱	۰/۲۳۶	۰/۱۶۹	۰/۱۶۸	۰/۲۸۳	۰/۳۱۴	۱

ارزیابی مدل ساختاری و مدل کلی

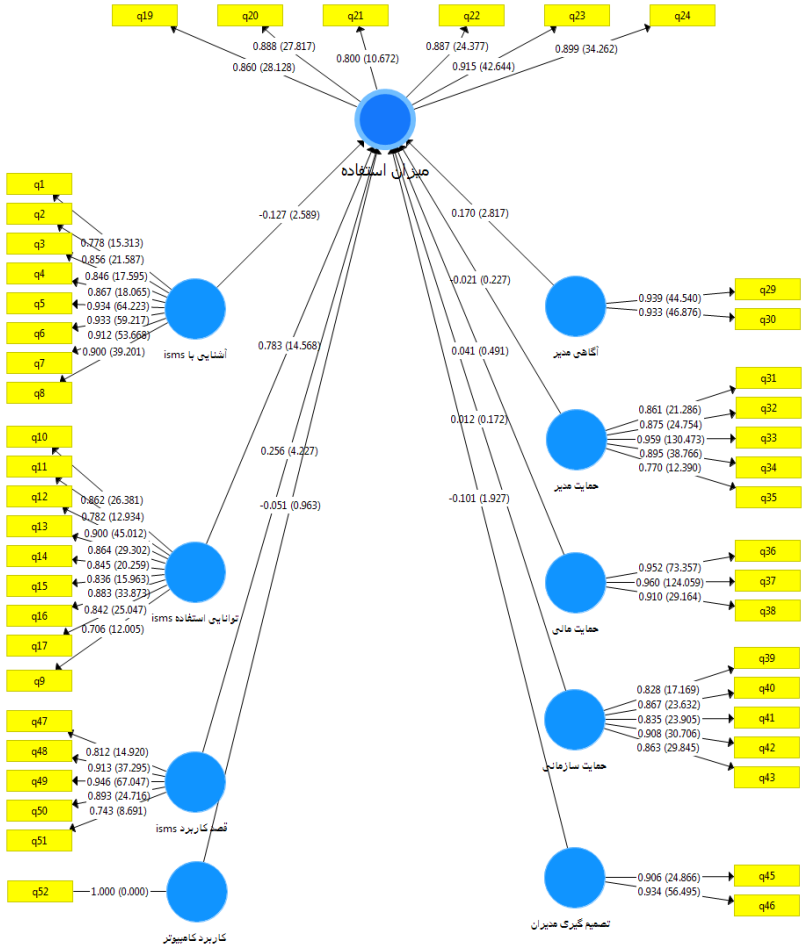
برای ارزیابی مدل ساختاری از دو معیار ضریب تعیین و Q^2 استفاده شده است. در ضریب تعیین مقادیر ۰/۱۹، ۰/۳۳ و ۰/۶۷ به ترتیب نشان دهنده‌ی مقادیر ضعیف، متوسط و قوی است. مقدار ضریب تعیین برای متغیر میزان استفاده از ISMS برابر ۰/۸۹۹ بدست آمده است که مقدار بالایی است و در واقع به این معنی است که متغیرهای پیش بین حاضر در مدل، در مجموع به میزان تقریبی ۸۹/۹ درصد از تغییرات میزان استفاده از ISMS را توضیح داده‌اند.

معیار Q^2 توسط استون و گیزر معرفی شده است و قدرت پیش بینی مدل را مشخص می کند. هنسلر و همکاران قدرت پیش بینی مدل را مقادیر ۰/۰۲، ۰/۱۵ و ۰/۳۵ تعیین نموده اند که مقدار ۰/۰۲ نشان از پیش بینی ضعیف است. همان گونه که مشاهده می‌شود این مقدار برای متغیر وابسته میزان استفاده از ISMS میزان ۰/۶۳۰ است که نشان از قدرت پیش بینی بالای مدل برای این متغیر است

به منظور بررسی برازش مدل کلی در روش حداقل مربعات جزیی شاخص SRMR (ریشه دوم میانگین مربعات باقیمانده های استاندارد) مورد بررسی قرار می‌گیرد و دامنه قابل قبول برای آن مقادیر کمتر از ۰/۱ بوده که در مدل پژوهش این شاخص مقدار ۰/۰۷۱ را اختیار کرده است و در محدوده قابل قبول می‌باشد و نشان از برازش مطلوب مدل است.

پس از بررسی و تایید برازش مدل اندازه گیری، ساختاری و مدل کلی محقق اجازه می‌یابد که به بررسی و آزمون فرضیه‌های پژوهش بپردازد. برای این منظور از معنی داری ضرایب مسیر در بخش ساختاری مدل استفاده شده است که معیار سنجش آن اعداد معنی داری t است و در صورتی که مقدار این اعداد بزرگتر از ۱/۹۶ باشد، نشان از وجود رابطه‌ی معنی دار بین متغیرها و در نتیجه تایید فرضیه‌ی پژوهش دارد.

مدل معادلات ساختاری نهایی متناسب با فرضیات پژوهش در شکل ۱ ارائه شده است.



شکل ۱: مدل معادلات ساختاری بررسی تاثیر ویژگی های سازمانی بر میزان استفاده از ISMS در حالت تخمین ضرایب استاندارد(بارهای عاملی) و مقادیر آماره t

پاسخگویی به فرضیات پژوهش

برای بررسی فرضیه‌های پژوهش از آماره t و سطح معنی داری آن برای ضرایب بخش ساختاری مدل شکل ۱ استفاده شد که می‌توان با استناد به آن به فرضیات ۱ تا ۹ پژوهش پاسخ داد. نتایج در جدول ۳ ارائه شده است.

جدول ۳: مقادیر ضرایب مسیر، آماره‌ی t، سطح معنی و فواصل اطمینان ضرایب براساس فرضیات پژوهش

فرضیه	ضریب تاثیر	آماره ی t	سطح معنی داری	فاصله اطمینان ۹۵ درصد		نتیجه فرضیه
				کران پایین	کران بالا	
فرضیه ۱: قصد کاربرد ISMS بر میزان استفاده از ISMS تاثیر معنی داری دارد.	۰/۲۵۶	۳/۹۰۵	**۰/۰۰۰۱	۰/۱۲۳	۰/۳۷۴	تایید
فرضیه ۲: آشنایی با ISMS بر میزان استفاده از ISMS تاثیر معنی داری دارد.	-۰/۱۲۷	۲/۵۶۲	*۰/۰۱۱	-۰/۲۲۸	-۰/۰۳۱	تایید
فرضیه ۳: توانایی استفاده از ISMS بر میزان استفاده از ISMS تاثیر معنی داری دارد.	۰/۷۸۳	۱۵/۶	**۰/۰۰۰۱	۰/۶۷۷	۰/۸۷۳	تایید
فرضیه ۴: آگاهی مدیر بر میزان استفاده از ISMS تاثیر معنی داری دارد.	۰/۱۷۰	۲/۹۲۷	**۰/۰۰۴	۰/۰۳۳	۰/۲۶۰	تایید
فرضیه ۵: تصمیم گیری مدیران بر میزان استفاده از ISMS تاثیر معنی داری دارد.	-۰/۱۰۱	۲/۰۲۶	*۰/۰۴۳	-۰/۲۰۶	۰/۰۰۰۲	تایید
فرضیه ۶: حمایت سازمانی بر میزان استفاده از ISMS تاثیر معنی داری دارد.	۰/۰۱۲	۰/۱۷۶	۰/۸۶۱	-۰/۱۱۵	۰/۱۶۲	رد
فرضیه ۷: حمایت مالی بر میزان استفاده از ISMS تاثیر معنی داری دارد.	۰/۰۴۱	۰/۵۲۴	۰/۶۰۱	-۰/۱۲۶	۰/۱۸۲	رد
فرضیه ۸: حمایت مدیر بر میزان استفاده از ISMS تاثیر معنی داری دارد.	-۰/۰۲۱	۰/۲۳۰	۰/۸۱۸	-۰/۱۷۴	۰/۱۹۷	رد
فرضیه ۹: کاربرد کامپیوتر بر میزان استفاده از ISMS تاثیر معنی داری دارد.	-۰/۰۵۱	۰/۹۹۸	۰/۳۱۹	۰/۱۵۰	۰/۰۵۰	رد

علامت ** به منزله معنی داری در سطح خطای ۰/۰۱، علامت * به منزله معنی داری در سطح خطای ۰/۰۵

با توجه به نتایج مندرج در جدول ۳ می‌توان گفت ۵ فرضیه (فرضیه‌های ۱، ۲، ۳، ۴ و۵) تایید (t>۱/۹۶) و ۴ فرضیه (فرضیه‌های ۶، ۷، ۸ و ۹) رد (t<۱/۹۶) می‌شود. به این ترتیب توانایی استفاده از ISMS، قصد کاربرد ISMS و آگاهی مدیر تاثیر معنی داری مستقیم و آشنایی با ISMS و تصمیم گیری مدیران تاثیر معنی داری معکوس بر میزان استفاده از ISMS دارند و در این بین با توجه به فواصل اطمینان بوت استرپ آن‌ها بیشترین میزان تاثیر مربوط به توانایی استفاده از ISMS با میزان ۰/۷۸۳ است.

نتایج جانبی پژوهش:

تاثیر ویژگی‌های فردی جنسیت، وضعیت تاهل، تحصیلات و سن بر میزان استفاده از ISMS به منظور بررسی این مساله از روش آنالیز واریانس استفاده شده است و نتایج آن در جدول ۴ نشان داده شده است.

جدول ۴: بررسی تاثیر ویژگی‌های جمعیت شناختی بر میزان استفاده از ISMS

فرضیه	آماره آزمون F	سطح معنی داری	ضریب اتا	نتیجه
جنسیت	۲/۳۵۴	۰/۱۲۹	۰/۰۲۷	عدم تاثیر
وضعیت تاهل	۶/۳۸۶	۰/۰۱۳*	۰/۰۷	دارای تاثیر
تحصیلات	۰/۴۶۴	۰/۹۰۶	۰/۰۴۲	عدم تاثیر
سن	۲/۴۴۲	۰/۰۷۰	۰/۰۸۱	عدم تاثیر

علامت * به منزله معنی داری در سطح خطای ۰/۰۵

مطابق با نتایج حاصل شده می‌توان گفت متغیرهای جنسیت، تحصیلات و سن تاثیر معناداری بر میزان استفاده از ISMI ندارند و تنها متغیر وضعیت تاهل تاثیر معناداری در میزان استفاده از ISMS دارند.

بحث و نتیجه گیری

امروزه اطلاعات مهمترین منبع مدیر بعد از عامل انسانی محسوب می‌شود. اطلاعات در هر سازمانی مبنای تمام فعالیتها بوده و انجام وظایف و تحقق اهداف سازمان فقط از طریق تسریع و تسهیل جریان اطلاعات و ایجاد شبکه ارتباطی و اطلاعاتی قوی و موثر امکان پذیر است. اداره امور سازمانها به شیوه کارآمد به ویژه در دنیای پیچیده امروز، مستلزم جمع آوری و پردازش انبوهی از اطلاعات گوناگون است که با آهنگی سریع در حال رشد است. کمیت و کیفیت اطلاعات مورد نیاز مدیران برای تصمیم گیری به عوامل متعددی بستگی دارد. ولی ویژگیهای خود اطلاعات و نیز نحوه پردازش اطلاعات مورد نیاز مدیران برای تصمیم گیری، عوامل تعیین کننده و اساسی در این روند هستند. نه تنها اطلاعات باید ویژگی همچون دقت، صحت، تازگی، سرعت و ...را داشته باشد. بلکه باید به نحوی پردازش شده باشد که توان و کیفیت تصمیم گیری مدیر را ارتقاء بخشد (آندری،۲۰۱۹).

هدف اصلی این پژوهش ارزیابی استفاده مدیران از سیستم های امنیت اطلاعات مدیریت در چابکی و فرایند تصمیم‌گیری در سازمان بوده نتایج حاصل از تجزیه و تحلیل فرضیه اول تحقیق نشان داد که قصد کاربرد ISMS بر میزان استفاده از ISMS رابطه معناداری وجود دارد. نتایج آزمون همبستگی اسپیرمن نشان میدهد که رابطه بین قصدکاربرد ISMS بر میزان استفاده ISMS در سازمان وزارت علوم، تحقیقات و فناوری تهران معنادار (r=۰/۲۵۶، sig=۰/۰۰۰) است. بنابراین فرضیه اول تایید می شود.

در فرضیه دیگر تحقیق بیان شد که آشنایی با ISMS بر میزان استفاده از ISMS بر میزان بکارگیری آن موثر است. نتایج تحلیل رگرسیون کاربرد ISMS با استفاده از متغیرهای فردی و سازمانی نشان داد که آشنایی استفاده از سیستم امنیت اطلاعات مدیریت بر میزان بکارگیری آن تاثیردارد. بنابراین فرضیه دوم تایید می شود.

در فرضیه دیگر تحقیق بیان شد که توانایی استفاده از سیستم امنیت اطلاعات مدیریت بر میزان بکارگیری آن موثر است. نتایج تحلیل رگرسیون کاربرد ISMS با استفاده از متغیرهای فردی و سازمانی نشان داد که توانایی استفاده از سیستم امنیت اطلاعات مدیریت بر میزان بکارگیری آن تاثیر ندارد. بنابراین فرضیه سوم تایید نمی شود.

فرضیه دیگر تحقیق بیانگر این بود که میزان آگاهی مدیر بر میزان استفاده سیستم امنیت اطلاعات مدیریت موثر است. نتایج تحلیل رگرسیون کاربرد ISMS با استفاده از متغیرهای فردی و سازمانی نشان میدهد که میزان آگاهی مدیر بر میزان استفاده از سیستم امنیت اطلاعات مدیریت تاثیر دارد. بنابراین فرضیه چهارم تایید می شود.

در فرضیه دیگر تحقیق بیان شد که تصمیم گیری مدیران بر میزان استفاده سیستم امنیت اطلاعات مدیریت موثر است.

نتایج تحلیل رگرسیون کاربرد ISMS با استفاده از متغیرهای فردی و سازمانی نشان میدهد که تصمیم گیری مدیران بر میزان استفاده از سیستم امنیت اطلاعات مدیریت تاثیر دارد. بنابراین فرضیه پنجم تایید می شود.

نتایج فرضیه دیگر تحقیق بیان میکند که حمایت سازمانی بر میزان بکارگیری سیستم امنیت اطلاعات مدیریت موثر نبوده است. نتایج تحلیل رگرسیون کاربرد ISMS با استفاده از متغیرهای فردی و سازمانی نشان می‌دهد که میزان حمایت سازمانی بر میزان بکارگیری سیستم امنیت اطلاعات مدیریت تاثیر ندارد. بنابراین فرضیه ششم تایید نمی شود.

فرضیه دیگر تحقیق بیان میکند که حمایت مالی سازمان بر میزان بکارگیری سیستم امنیت اطلاعات مدیریت موثر نبوده است. نتایج تحلیل رگرسیون کاربرد ISMS با استفاده از متغیرهای فردی و سازمانی نشان میدهد که میزان حمایت مالی بر میزان بکارگیری سیستم امنیت اطلاعات مدیریت تاثیر ندارد. بنابراین فرضیه هفتم تایید نمی شود.

فرضیه دیگر تحقیق بیانگر این نتیجه بود که حمایت مدیر بر میزان بکارگیری سیستم امنیت اطلاعات مدیریت موثر نبوده است. نتایج تحلیل رگرسیون کاربرد ISMS با استفاده از متغیرهای فردی و سازمانی نشان میدهد که میزان حمایت مدیر بر میزان بکارگیری سیستم امنیت اطلاعات مدیریت تاثیر ندارد. بنابراین فرضیه هشتم تایید نمی شود.

فرضیه دیگر تحقیق بیانگر این نتیجه بود که کاربرد کامپیوتر بر میزان بکارگیری سیستم امنیت اطلاعات مدیریت موثر نبوده است. نتایج تحلیل رگرسیون کاربرد ISMS با استفاده از متغیرهای فردی و سازمانی نشان میدهد که کاربرد کامیوتر بر میزان بکارگیری سیستم امنیت اطلاعات مدیریت تاثیر ندارد. بنابراین فرضیه نهم تایید نمی شود.

۷. منابع

اسکندری، حمید؛ امیرصوفی، رحمت الله،(۱۳۹۱). *تهدیدات فضای سایبر و مدیریت امنیت اطلاعات (ISMS)*. تهران: بوستان حمید، چاپ۱، صفحه۱۷۶.

اکبرپور، مجید، (۱۳۹۴). *امنیت فناوری اطلاعات و ارتباطات در سازمانها. تهران: مرکز آموزشی و پژوهشی شهید سپهبد صیادشیرازی*، چاپ۱، صفحه۲۱۲.

اسدالله شاه – بهرامی؛ رامین رفیع - زاده – کاسانی؛ حسین پوریوسفی،(۱۳۹۶). شناسایی و اولویت - بندی پارامترهای تاثیرگذار بر سیستم مدیریت امنیت اطلاعات (مطالعه موردی: شعب تامین - اجتماعی استان گیلان)، *فصلنامه علمی-پژوهشی فناوری اطلاعات و ارتباطات ایران، سال دهم ، شماره افراد ۳۵ و ۳۶ ، صفحه ۷۰-۵۳*.

تاج فر،احمد؛ محمودی میمند، محمد؛ رضا سلطانی، فرامرز؛ رضا سلطانی،پدرام؛(۱۳۹۳)، رتبه¬بندی موانع پیاده سازی سیستم مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف، *مدیریت فناوری اطلاعات، شماره ۶*، جلد۴، صفحات۵۵۱-۵۶۶.

شاه بهرامی ، اسدا .. رفیع زاده کاسانی ، رامین. (۱۳۹۴). *امنیت منابع فناوری اطلاعات* ، انتشارات جهاد دانشگاهی- تهران

قرایی ، حسین و مهسا آقا محی الدین. (۱۳۹۳). *بهبود رتبه مخاطبین امنیت اطلاعات با استفاده از مدلهای اصلاح شده چندشاخه. پردازش علائم و داده¬ها*. ۲ (۲۲).

نورایی، فرزاد.(۱۳۹۱)، *بررسی و شناسایی عوامل موفقیت استقرار سیستم مدیریت امنیت اطلاعات ISMS در ایران(مطالعه موردی بانک دی)*، پایانامه کارشناسی ارشد، دانشگاه سیستان و بلوچستان، زاهدان.

Alavi, R., Shareeful, I., Haralambos, M. (2016). An information security risk-driven investment model for analysing human factors, *Information & Computer Security*, *Vol. 24* Issue: 2, pp.205-227.(in Persian).

Andrii. B (2019).Information systems for supply chain management: uncertainties, risks and cyber security, *Procedia Computer ScienceVolume 1492019*Pages 65-70.(in Persian).

Nazareth, D. L., & Choi, J. (2015). *A system dynamics model for information*

security management. Information & Management, 52(1), 123-134.Retrieved From.

Oltean, F.D., Gabor, M.R., & Conţiu, L.C. (2014) "Relation between Information Technology and Performance: An Empirical Study Concerning the Hotel Industry in Mures County". *Procedia Economics and Finance*, 15, 1535-1542.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for effective information security management*. CRC Press.

Rezaei, Ali, Mossadegh, Mohammad Javad, Rezaei, Mona. (2018). Factors affecting the effectiveness of information security management system. *Quarterly Journal of Development and Transformation Management*, 1397 (33), 73-82.(in Persian).

Rahnamaii Zakavat, m. (2017). Application of data mining in big data management in the field of health information using CRISP-DM algorithm, Annual Conference on New Management Paradigms in the field of intelligence, Tehran, *Permanent Conference Secretariat*, University of Tehran.(in Persian).

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215-225.

Yousefi Zenooz, R.; Hassanpour, A.; Mousavi, P. (2015). Presenting a model for prioritizing organizational information security risks using fuzzy AHP and Bayesian network in the banking industry, *Quarterly Journal of Industrial Management Studies*, Volume 13, Number 37, pp. 185-161.(in Persian).

Zargari, K. (2017). The Impact of Internal Organizational Factors on the Efficiency of Human Resource Management Information Systems in Banks of Guilan Province, *2nd International Conference on Management and Accounting*, Tehran, Salehan Institute of Higher Education.(in Persian).

Zandiyan, F, Gharavi, A, Hassanzadeh, M. (2018). Identifying the impact of human factors on information security in the Department of Education. Scientific. *Journal of Information Management*, 4 (2), 110-128.(in Persian).

Evaluate managers' use of management information security systems in agility and decision-making process in the organization

Saman Hamidi Ashtiani

Abstract

Background & Purpose: The purpose of this study was to evaluate and evaluate the use of managers' information security management systems in agility and decision making process.

Methodology: This research is applied in terms of purpose and descriptive-survey method. The statistical population of the study was the managers and experts of the Administrative, Financial and Resource Management Organization of the Ministry of Science of Tehran, which was selected by cluster sampling method and then the required research information was collected from all senior and middle managers of those organizations. In total, the statistical sample size was 205 people. A questionnaire was used to collect data and descriptive statistics (frequency distribution table, frequency percentage) and inferential statistics (Kolmogorov-Smirnov test, t-test, Spearman correlation coefficient test, stepwise multiple regression test) were used to analyze the data. Is.

Findings: The results showed that there is no significant difference between the two groups of male and female managers in the use of management information security system. Also, no difference was observed between groups with different levels of organizational status in its use. There is also a difference between managers' use of information security system based on age groups, so that older managers use this system less and there is a difference between the use of this system based on service groups.

Conclusion: Stepwise regression analysis indicates that the six factors of manager awareness, organizational support, financial support, Internet use, manager support, availability and belief in effectiveness as the most important factors influencing the use of information security system can be a reliable model for Provide an estimate of the use of this system.

Keywords: Information security system, decision-making process, management, decision-making agility