شناسایی تأثیر عوامل انسانی بر امنیت اطلاعات در اداره آموزش‌وپرورش

دو فصلنامه علمی- پژوهشی

مدیریت اطلاعات

دوره ۴، شماره ۲

پاییز و زمستان ۱۳۹۷

فاطمه زندیان

استادیار، دکتری علم اطلاعات و دانش شناسی، دانشکده مدیریت و اقتصاد، دانشگاه تربیت مدرس، تهران، ایران[1]

آی جمال غراوی

کارشناس ارشد، رشته علم اطلاعات و دانش شناسی، دانشکده مدیریت و اقتصاد، دانشگاه تربیت مدرس، تهران، ایران

محمدحسن زاده

دانشیار، دکتری علم اطلاعات و دانش شناسی، دانشکده مدیریت و اقتصاد، دانشگاه تربیت مدرس، تهران، ایران

چکیده: پژوهش حاضر باهدف شناسایی تأثیر عوامل انسانی بر امنیت اطلاعات در ادارات آموزش‌وپرورش شهرستان‌های گنبدکاووس و مراوه‌تپه انجام شد. در این پژوهش متغیرهای مؤثر بر امنیت اطلاعات از بعد نیروی انسانی انتخاب شد و دیدگاه مدیران و کارکنان نسبت به تأثیر آن‌ها در امنیت موردسنجش قرار گرفت و با در نظر گرفتن اهمیت امنیت برای سازمان‌های امروزی یک مدل مدیریتی برای بررسی نقش عوامل انسانی در امنیت سیستم‌های اطلاعاتی ارائه گردید. پژوهش از نوع کاربردی است که به روش توصیفی _ پیمایشی انجام‌شده است و با استفاده از روش نمونه‌گیری هدفمند ۱۰۳ نفر از کارکنانی که بیشترین استفاده را از کامپیوتر و شبکه داشتند به‌عنوان نمونه آماری انتخاب شدند. ابزار گردآوری داده‌ها پرسشنامه محقق ساخته (شامل هفت متغیر) است که با استفاده از نرم‌افزار SPSS ضریب پایایی آن ۰/۹۹ درصد محاسبه گردید و جهت تعیین اعتبار و روایی آن از روش اعتبار محتوا استفاده شد. تجزیه‌وتحلیل داده‌ها با استفاده از نرم‌افزار LISREL انجام شد. نتایج نشان می‌دهد که از دیدگاه کارکنان آموزش‌وپرورش شهرستان‌های گنبدکاووس و مراوه‌تپه، حمایت مدیریت عالی اداره آموزش‌وپرورش، آموزش کاربران، فرهنگ امنیتی میان کاربران، مهارت کاربران، تقویت خط‌مشی کاربران ادارات، خودباوری و تجربیات کاربران بر اثربخشی امنیت سیستم‌های اطلاعاتی تأثیر مستقیم دارد که درنهایت منجر به بهبود امنیت سیستم‌های اطلاعاتی می‌شود. علاوه بر آن خروجی لیزرل نشان می‌دهد که تمامی ابعاد (حمایت مدیریت عالی، آموزش، فرهنگ امنیتی، مهارت کاربران، تقویت خط‌مشی، خودباوری و تجربیات افراد) با سازه موردنظر یعنی همان اثربخشی امنیت سیستم‌های اطلاعاتی دارای بارهای عاملی بالایی هستند و با توجه به اطمینان ۹۵ درصد می‌توان بیان داشت که برازش این مدل قابل‌تأیید است.

کلیدواژه‌ها: ادارات آموزش‌وپرورش شهرستان‌های گنبدکاووس و مراوه‌تپه، اثربخشی امنیتی، امنیت سیستم‌های اطلاعاتی، سازه‌های مدیریتی، سیستم‌های اطلاعاتی.

۱. نویسنده مسئول: fatemehzandian@modares.ac.ir

مقدمه

در تجارت امروز اطلاعات نقش سرمایه یک شرکت را ایفا می‌کند و حفاظت از اطلاعات و سیستم‌های اطلاعاتی سازمان، یکی از ارکان مهم بقای آن است. جهانی‌شدن اقتصاد منجر به ایجاد رقابت در سطح جهانی شده و بسیاری از شرکت‌ها برای ادامه‌ی حضور خود در عرصه‌ی جهانی، ناچار به همکاری با سایر شرکت‌ها هستند. به‌این‌ترتیب طبقه‌بندی و ارزش‌گذاری و حفاظت از منابع اطلاعاتی سازمان (چه در مورد سیستم‌های اطلاعاتی و چه منابع انسانی) بسیار حیاتی و مهم به شمار می‌رود (بذرپور۱۳۸۴، ۱۷). امنیت سیستم‌های اطلاعاتی را از دو جهت می‌توان موردبررسی قرار داد: فناوری و افراد. اگر بهترین سخت‌افزار یا نرم‌افزارها به کار گرفته شود، ولی کاربران و یا عوامل انسانی درگیر در یک سیستم اطلاعاتی، پارامترهای امنیتی را رعایت نکنند، یا از آن آگاهی نداشته باشند، کارها به‌درستی انجام نمی‌شود.

در تحقیقاتی که به عوامل انسانی پرداخته‌اند هرکدام از یک زاویه کوچک موضوع را موردبحث قرار داده‌اند و در بیشتر آن‌ها نتایج رفتاری افراد موردتوجه قرارگرفته است نه خود رفتار، بنابراین نظارت‌هایی هم که بوده بیشتر پیامدهای رفتار را مشخص کرده‌اند نه خود رفتار واقعی را (Hinson and Rossouw 2004). به گفته‌ی دیوید ماکی[1] رئیس بخش اطلاع‌رسانی شرکت کامپیوتری ARMONK کاربر همچنان به‌عنوان سست‌ترین عنصر آسیب‌پذیر در مدل‌های امنیتی مورد سوءاستفاده قرار می‌گیرد. ماکی افزایش سریع حملات از نوع سیادی و موفقیت مجرمانی که از این شیوه استفاده می‌کنند را برای اثبات این مدعا کافی دانسته است (بهاری ۱۳۸۴، ۵۴). کاربرانی که ممکن است در مورد خطرهای امنیتی آموزش لازم ندیده باشند، به‌آسانی فریب‌خورده و کدهای مخرب را به اجرا درمی‌آورند. بااین‌وجود، در اداره آموزش‌وپرورش مذکور دورنمای مناسب امنیت اطلاعات به‌ویژه از بُعد نیروی انسانی تدوین‌نشده است.

با توجه به اهمیت فرایند عوامل انسانی در سیستم‌های اطلاعات و امنیت آن، نیاز به انجام یک پژوهش گسترده و جامع در این زمینه محسوس است. با توجه به اینکه سال‌های زیادی از موضوع امنیت اطلاعات در جهان و همچنین در ایران می‌گذرد اما متأسفانه شرکت‌ها و ادارات اندکی می‌توانند ادعا کنند که واقعاً در سازمان‌هایشان امنیت اطلاعات وجود دارد (احترامی ۱۳۸۸، ۵۲). شرکت‌های زیادی وجود دارد که با صرف هزینه‌های هنگفتی برای برقراری امنیت اطلاعاتی باز اطلاعاتشان به سرقت رفته یا از بین می‌رود؛ درنتیجه شاهد دوباره‌کاری در سازمان خود بوده‌اند. بنابراین این سؤال در ذهن محقق شکل گرفت که آیا ادارات آموزش‌وپرورش توانسته است با صرف هزینه‌های نسبتاً بالا جهت برقراری امنیت در سازمان موفق بوده‌اند یا خیر؟ با در نظر گرفتن فقدان یا کمبود عمومی پژوهش تجربی و اهمیت امنیت اطلاعات برای سازمان‌های امروزی، این مطالعه در جست‌وجوی تدوین چارچوب امنیت اطلاعات در بُعد نیروی انسانی آموزش پرورش دو شهرستان گنبدکاووس و مراوه‌تپه است.

این پژوهش اثرات هفت متغیر حمایت **مدیریت عالی** یا حمایت کارکنان از سوی مدیر؛ **آموزش امنیتی** (شامل آگاهی پرسنل از حقوق خود در راستای امنیت اطلاعات سازمان)؛ **فرهنگ امنیتی** (فرهنگی است که بر جو سازمان حاکم بوده و مانع سوءاستفاده می‌شود)؛ **مهارت عوامل انسانی** یا سطح

1. David Moky

مهارت افراد در حوزه امنیت اطلاعات سازمان؛ **تقویت خط‌مشی** (شامل اسناد گردآوری‌شده از تصمیمات امنیتی (NIS 2000))؛ **خودباوری افراد** به معنای قضاوت افراد از قابلیت‌هایشان برای سازماندهی و انجام اعمال موردنیاز برای دستیابی به انواع مشخص‌شده عملکرد (Bandura 1986, P. 399) و نهایتاً **تجربیات عوامل انسانی** (شامل تجربیات ماهرانه و معتبر افراد) در اثربخشی امنیت سیستم‌های اطلاعاتی اداره آموزش‌وپرورش شهرستان‌های گنبدکاووس و مراوه‌تپه موردبررسی قرار می‌دهد.

نمودار ۱. مدل کلی سؤالات پژوهش

پیشینه پژوهش

در این بخش پژوهش‌هایی مرور می‌شود که امنیت سیستم‌های اطلاعاتی را مورد هدف قرار داده‌اند:

شهریوری (۱۳۹۰) پژوهشی تحت عنوان «ارائه مدل بلوغ برای حاکمیت بر امنیت اطلاعات در مدیریت زنجیره تأمین» انجام داد که حاصل این پژوهش مدل پیشنهادی، مدل بلوغ حاکمیت بر امنیت تحت عنوان ISG-MM شامل ابعاد کسب‌وکار (شامل مؤلفه‌های: آگاهی کسب‌وکار و فرایندهای کسب‌وکار)، زیرساخت‌های فناوری اطلاعات (شامل مؤلفه‌های: سخت‌افزار و نرم‌افزار و کارکنان واحد فناوری اطلاعات)، استانداردها/بهترین اقدامات (شامل مؤلفه‌ها: آگاهی از استانداردهای امنیت اطلاعات و کنترل پیاده‌سازی استاندارد امنیت اطلاعات)، قانونی و حقوقی (شامل مؤلفه‌های: محدودیت دسترسی به اطلاعات، پذیرش قانونی امنیت اطلاعات و جلوگیری از جرم‌های شبکه‌ای)، مدیریت روابط با مشتریان (شامل مؤلفه‌های: سیستم ارتباط با مشتریان، کانال‌های بازاریابی و پشتیبانی از مشتری)، مدیریت روابط با تأمین‌کنندگان (شامل مؤلفه‌های: سیستم ارتباط با تأمین‌کنندگان، امنیت فرایند تأمین و پشتیبانی از تأمین‌کنندگان) و امنیت شبکه‌های اطلاعاتی (شامل مؤلفه‌های: آگاهی از امنیت شبکه، سیاست امنیت شبکه، مدیریت امنیت شبکه، امنیت اینترانت و امنیت اکسترانت) می‌شود.

نصرمحمدی (۱۳۹۲) پژوهشی تحت عنوان «کشف ناهنجاری در شبکه با استفاده از مصورسازی هشدارهای امنیتی» انجام داد که به بررسی عواملی ازجمله تجربیات عوامل انسانی، فرهنگ عوامل انسانی و مهارت عوامل انسانی می‌پردازد که نتایج حاصل از پژوهش معرفی یک ساختار کلی سیستم پیشنهادی است که این ساختار کلی بر مبنای مدل کلی سیستم‌های تشخیص ناهنجاری بناشده است.

گوهریان (۱۳۹۴) پژوهشی تحت عنوان «طراحی سیستمی هوشمند برای تشخیص و کنترل ریسک‌های امنیت در محیط وب ۲,۰» انجام داد که به بررسی تجربیات و مهارت عوامل انسانی می‌پردازد.

نتایج حاصل از پژوهش ریسک‌های امنیت در محیط وب ۲٫۰ را شناسایی و علائم بروز این ریسک‌ها و پاسخ‌های مناسب به این ریسک‌ها را نشان می‌دهد. درنهایت این پژوهش به ارائه‌ی راهکار پیشنهادی می‌پردازد که عبارت است از ارائه سیستمی کاربردی جهت تعیین استراتژی‌های کاربردی و مناسب جهت تشخیص و پاسخ به ریسک‌های امنیتی در محیط وب ۲٫۰ است.

خیرگو و شکوهی (۱۳۹۵) در پژوهشی با عنوان «شناسایی و رتبه‌بندی عوامل کلیدی مؤثر بر اثربخشی سیستم‌های اطلاعاتی» معتقدند که در عصر حاضر سیستم‌های اطلاعاتی ازجمله عوامل تأثیرگذار در دستیابی به مزیت رقابتی برای سازمان‌ها محسوب می‌شوند و کیفیت خروجی این سیستم‌ها نقش مهمی در بهبود عملکرد سازمان دارد. نتایج پژوهش آن‌ها نشان می‌دهد تأثیر عوامل سازمانی، انسانی و فنی بر اثربخشی سیستم‌های اطلاعاتی چشمگیر است و از بین شاخص‌های مؤثر بر اثربخشی سیستم‌های اطلاعاتی حمایت مدیریت ارشد، امنیت، پذیرش و مدیریت دانش فناوری اطلاعات و سیستم‌های اطلاعاتی به ترتیب رتبه‌های نخست را به خود اختصاص دادند.

کریتزینگر و اسمیت[1] (۲۰۱۱) پژوهشی با عنوان «مدل بازیابی و آگاهی امنیت اطلاعات (ISRA)» را ارائه کردند، این مدل برای ارتقای آگاهی از امنیت اطلاعات در میان کارکنان، استفاده می‌شود. اساس این مدل بر مبنای بدنه مشترک دانش پیشنهادشده است که برای امنیت اطلاعات مناسب به نظر می‌رسد. این بدنه مشترک از دانش، تضمین می‌کند که مسائل فنی امنیت اطلاعات، مسائل غیر فنی امنیت اطلاعات که مرتبط با انسان است را تحت شعاع قرار نمی‌دهد. بدنه مشترک از دانش هم در افراد حرفه‌ای و هم‌سطح پایین، کاربران اطلاعات می‌پردازد. دیدگاه مفهومی مدل ISRA از سه قسمت تشکیل‌شده است (Kritzinger and Smith 2011). قسمت اول ابعاد ISRA است که این ابعاد شامل مسائل غیر فنی امنیت اطلاعات سطوح اختیار فناوری اطلاعات و مستندات امنیت اطلاعات است. قسمت دوم به بازیابی و آگاهی امنیت اطلاعات می‌پردازد. اطلاعات بازیافته شده در این قسمت برای ارتقای سطح آگاهی امنیت اطلاعات در میان سطوح اختیار فناوری اطلاعات و همچنین برای کمک به فرایند تصمیم‌گیری سطوح اختیار فناوری اطلاعات، به کار می‌رود. این بازیابی اطلاعات از طریق مشاهده اطلاعات در ابعاد ISRA در زوایای مختلف انجام می‌شود. در قسمت سوم اندازه‌گیری، مشخص کردن سطح آگاهی امنیت اطلاعات هر یک از ذی‌نفعان سازمان است. این سطح آگاهی در رابطه با همه‌ی مسائل امنیت اطلاعات مرتبط با سطوح اختیار ذی‌نفعان مطرح می‌شود. هدف از فرایند نظارت مشخص کردن وضعیت‌آگاهی امنیت اطلاعات در درون سازمان است

کیم[2] و همکاران (۲۰۱۴) طی پژوهشی با عنوان «یک مدل یکپارچه رفتاری برای پیروی از سیاست‌های امنیت اطلاعات» عواملی را که بر پیروی کارکنان سازمان از سیاست‌های امنیت اطلاعات مؤثر است موردپژوهش قراردادند. در این پژوهش تأثیر عواملی مانند خود کارآمدی، نگرش، باورهای اصولی و باورها در مورد هزینه‌های پیروی بر تمایل به پیروی از سیاست‌های سیستم‌های امنیت اطلاعات بررسی شد.

1. Kritzinger and Smith
2. Kim

مرور زمینه‌های نظری پژوهش نشان می‌دهد که عوامل انسانی بر امنیت سیستم‌های اطلاعاتی تأثیرگذار است و در هر پژوهش به‌گونه‌ای متفاوت به اهمیت نقش نیروی انسانی بر امنیت سیستم‌های اطلاعاتی پرداخته‌شده است. به‌عنوان‌مثال نصرمحمدی (۱۳۹۲) و گوهریان (۱۳۹۴) ویژگی‌های عوامل انسانی را در شرایط ریسک مورد تحلیل قرار داده‌اند و نهایتاً مدلی را متناسب با این حوزه ارائه داده‌اند. شهریوری (۱۳۹۰) به شناسایی و سنجش تأثیر عواملی می‌پردازد که سیستم‌های اطلاعاتی سازمان را با خطر سرقت، نابودی و تغییر اطلاعات مواجه می‌سازند. استیوارت (۲۰۱۸) اهمیت نیروی انسانی را در امنیت اطلاعات مورد هدف قرار داده و آنچه این تحقیق را از پژوهش‌های گذشته متمایز می‌نماید این است که رویکرد متفاوتی را از امنیت اطلاعات با تمرکز به امنیت اطلاعات رفتاری ارائه می‌کند. با در نظر گرفتن فقدان یا کمبود عمومی تحقیق تجربی و اهمیت امنیت اطلاعات برای سازمان‌های امروزی، این مطالعه به دنبال «ارائه چارچوبی برای بررسی نقش عوامل انسانی در امنیت سیستم‌های اطلاعاتی» است؛ به‌طور خاص این مطالعه در جست‌وجوی شناسایی و مدل‌سازی سازه‌های مدیریت است که بر اثربخشی امنیت اطلاعات در سازمان اثرگذار است. در این راستا متغیرهای حمایت مدیریت عالی، آموزش کاربر، فرهنگ امنیتی، مهارت کاربر، خط‌مشی امنیتی، تجربیات افراد و خودباوری آن‌ها، به‌عنوان عوامل مدیریتی و انسانی اثرگذار بر اثربخشی امنیت سیستم‌های اطلاعاتی موردبررسی قرار گرفتند که با توجه به آن مدل تحقیق ارائه شد.

روش‌شناسی پژوهش

پژوهش حاضر به لحاظ هدف، کاربردی است و به روش توصیفی _ پیمایشی انجام‌شده است. قلمرو زمانی تحقیق از سال ۱۳۸۷ هم‌زمان با استقرار رسمی سیستم‌های امنیت اطلاعات در اداره آموزش‌وپرورش شهرستان‌های گنبدکاووس و مراوه‌تپه لغایت تیرماه ۱۳۹۵ را در برمی‌گیرد. جامعه‌ی آماری پژوهش ۳۴۰ نفر از کارکنان آموزش‌وپرورش دو شهرستان گنبدکاووس و مراوه‌تپه هستند. روش نمونه‌گیری، نمونه‌گیری هدفمند است که در این روش به ۱۰۳ نفر از کارکنانی که بیشترین استفاده را از کامپیوتر و شبکه داشتند مراجعه می‌شود.

ابزار جمع‌آوری اطلاعات پرسشنامه محقق ساخته است که هشت متغیر تحقیق را در بردارد. مقیاس اندازه‌گیری نگرش پاسخ‌دهندگان در پرسشنامه طیف لیکرت است. در این پرسشنامه هفت سطح متفاوت با هفت عبارت مشخص‌شده‌اند که رتبه‌ی آن‌ها به ترتیب از یک تا هفت در نظر گرفته‌شده است. سؤالات پرسشنامه به دو بخش تقسیم می‌شوند:

الف- سؤالات عمومی: این دسته از سؤالات شامل جنسیت، سطح تحصیلات و بودن پست مدیر امنیتی در سازمان است؛

ب - سؤالات اختصاصی که هشت متغیر تحقیق را در بردارد.

جهت تعیین اعتبار و روایی پرسشنامه در این پژوهش از روش اعتبار محتوا[1] استفاده‌شده است. ضریب پایایی پرسشنامه (آلفای کرونباخ) با استفاده از نرم‌افزار SPSS، ۰/۹۹ محاسبه گردید که نشان‌دهنده آن است که پرسشنامه مورداستفاده از پایایی خوبی برخوردار است.

به‌منظور تجزیه‌وتحلیل داده‌های پژوهش، فنون تحلیل آماری در دو قسمت مورداستفاده قرار گرفت:

۱-بررسی نظرات خبرگان در مورد وجود هر یک از متغیرهای پژوهش در سازمان

۲-بررسی و آزمون فرضیه‌های تحقیق.

ابتدا جهت تجزیه‌وتحلیل نظرات افراد، شاخص‌های مرکزی و پراکندگی مؤلفه‌ها محاسبه شد و در ادامه، جهت آزمون فرضیه‌ها از نرم‌افزار LISREL که یکی از مهم‌ترین نرم‌افزارها برای برآورد پارامترها، آزمون معناداری و برازش مدل‌های معادلات ساختاری با متغیرهای نهایی (که غیرقابل مشاهده و اندازه‌گیری مستقیم هستند) است، استفاده‌شده است.

فرضیه‌ی اصلی

عوامل انسانی بر امنیت سیستم‌های اطلاعاتی تأثیر مثبت دارد.

فرضیه‌های فرعی

۱-حمایت مدیریت عالی بر امنیت سیستم‌های اطلاعاتی تأثیر مثبت دارد.

۲- آموزش کارکنان آموزش‌وپرورش بر امنیت سیستم‌های اطلاعاتی تأثیر مثبت دارد.

۳-سطح فرهنگ امنیتی بر امنیت سیستم‌های اطلاعاتی تأثیر مثبت دارد.

۴- مهارت کارکنان آموزش‌وپرورش بر امنیت سیستم‌های اطلاعاتی تأثیر مثبت دارد.

۵-تقویت خط‌مشی امنیتی بر امنیت سیستم‌های اطلاعاتی تأثیر مثبت دارد.

۶-خودباوری کارکنان آموزش‌وپرورش بر امنیت سیستم‌های اطلاعاتی تأثیر مثبت دارد.

۷-تجربه‌ی کارکنان آموزش‌وپرورش بر امنیت سیستم‌های اطلاعاتی تأثیر مثبت دارد.

یافته‌های پژوهش

در پژوهش حاضر، پاسخ‌های به‌دست‌آمده از پرسشنامه طراحی‌شده مورد تجزیه‌وتحلیل قرارگرفته و بر اساس تجزیه‌وتحلیل‌های آماری فرضیه‌های پژوهش نیز موردبررسی قرار گرفتند.

اولین سؤال در بخش سؤالات عمومی پرسشنامه مربوط به جنسیت افراد پاسخگو است که از میان ۹۰ پرسشنامه پاسخ‌داده‌شده ۶۲ نفر مرد و ۲۸ نفر زن بوده‌اند.

1. Content Validity

دومین سؤال پرسشنامه مربوط به سطح تحصیلات افراد پاسخگو است که ۱۰ نفر دارای تحصیلات دیپلم و زیر دیپلم، ۲۳ نفر تحصیلات فوق‌دیپلم، ۴۵ نفر تحصیلات لیسانس ۱۲ نفر دارای تحصیلات فوق‌لیسانس و بالاتر هستند.

سومین سؤال مربوط به وجود داشتن یک پست عالی امنیتی در ادارات مربوطه است؛ که در ادارات آموزش‌وپرورش چنین پستی به‌صورت مجزا وجود ندارد و این مسئولیت بر عهده‌ی مدیر عالی سازمان است و پست مجزایی برای این مسئولیت وجود ندارد.

آزمون فرضیه اول با استفاده از نرم‌افزار لیزرل

فرضیه H_1 بیان می‌کند که بین سطح حمایت مدیریت عالی (TMS) و امنیت سیستم‌های اطلاعاتی رابطه مثبت وجود دارد. در این فرضیه هدف بررسی اثر مستقیم TMS بر امنیت سیستم‌های اطلاعاتی است. مقدار ارزش T (T value) و ضریب مسیر برای این رابطه در جدول یک آمده است.

جدول ۱. نتیجه آزمون فرضیه اول

متغیر مستقل	متغیر وابسته: اثربخشی امنیت سیستم‌های اطلاعاتی	
حمایت مدیریت عالی	ضریب مسیر	۰/۶۷
	سطح معنی‌داری	۰/۰۵
	ارزش T	۵/۶۷

چون مقدار T محاسبه‌شده برای این رابطه بزرگ‌تر از پنج است؛ بنابراین در سطح اطمینان ۹۵ درصد می‌توان ادعا کرد که بین حمایت مدیریت عالی و امنیت سیستم‌های اطلاعاتی رابطه معناداری با ضریب مسیر ۶۷ درصد وجود دارد و حمایت مدیریت عالی بر امنیت سیستم‌های اطلاعاتی اثرگذار است. درنتیجه فرضیه H_1 این پژوهش مورد تأیید قرار می‌گیرد.

آزمون فرضیه دوم با استفاده از نرم‌افزار لیزرل

فرضیه H_1 بیان می‌کند که بین سطح آموزش عوامل انسانی و امنیت سیستم‌های اطلاعاتی رابطه مثبت وجود دارد. در این فرضیه هدف بررسی اثر مستقیم آموزش عوامل انسانی بر امنیت سیستم‌های اطلاعاتی است. مقدار ارزش T (T value) و ضریب مسیر برای این رابطه در جدول دو آمده است.

جدول ۲. نتیجه آزمون فرضیه دوم

متغیر مستقل	متغیر وابسته: اثربخشی امنیت سیستم‌های اطلاعاتی	
سطح آموزش عوامل انسانی	ضریب مسیر	۰/۷۷
	سطح معنی‌داری	۰/۰۵
	ارزش T	۶/۳۴

چون مقدار T محاسبه‌شده برای این رابطه بزرگ‌تر از شش است؛ بنابراین در سطح اطمینان ۹۵ درصد می‌توان ادعا کرد که بین سطح آموزش عوامل انسانی و امنیت سیستم‌های اطلاعاتی رابطه معناداری با ضریب مسیر ۷۷ درصد وجود دارد و سطح آموزش عوامل انسانی بر امنیت سیستم‌های اطلاعاتی اثرگذار است. درنتیجه فرضیه H_1 این پژوهش مورد تأیید قرار می‌گیرد.

نتیجه فرضیه: سطح آموزش عوامل انسانی تأثیر معنی‌داری بر امنیت سیستم‌های اطلاعاتی دارد.

آزمون فرضیه سوم با استفاده از نرم‌افزار لیزرل

فرضیه H_1 بیان می‌کند که بین سطح فرهنگ امنیتی و امنیت سیستم‌های اطلاعاتی رابطه مثبت وجود دارد. در این فرضیه هدف بررسی اثر مستقیم فرهنگ امنیتی بر امنیت سیستم‌های اطلاعاتی است. مقدار ارزش T (T value) و ضریب مسیر برای این رابطه در جدول سه آمده است.

جدول ۳. نتیجه آزمون فرضیه سوم

متغیر مستقل	متغیر وابسته: اثربخشی امنیت سیستم‌های اطلاعاتی	
سطح فرهنگ امنیتی	ضریب مسیر	۰/۵۹
	سطح معنی‌داری	۰/۰۵
	ارزش T	۷/۳۲

چون مقدار T محاسبه‌شده برای این رابطه بزرگ‌تر از هفت است؛ بنابراین در سطح اطمینان ۹۵ درصد می‌توان ادعا کرد که بین سطح فرهنگ امنیتی و امنیت سیستم‌های اطلاعاتی رابطه معناداری با ضریب مسیر ۵۹ درصد وجود دارد و سطح فرهنگ امنیتی بر امنیت سیستم‌های اطلاعاتی اثرگذار است. درنتیجه فرضیه H_1 این پژوهش مورد تأیید قرار می‌گیرد.

آزمون فرضیه چهارم با استفاده از نرم‌افزار لیزرل

فرضیه H_1 بیان می‌کند که بین سطح مهارت عوامل انسانی و امنیت سیستم‌های اطلاعاتی رابطه مثبت وجود دارد. در این فرضیه هدف بررسی اثر مستقیم مهارت عوامل انسانی بر امنیت سیستم‌های اطلاعاتی است. مقدار ارزش T (T value) و ضریب مسیر برای این رابطه در جدول چهار آمده است.

جدول ۴. نتیجه آزمون فرضیه چهارم

متغیر مستقل	متغیر وابسته: اثربخشی امنیت سیستم‌های اطلاعاتی	
مهارت عوامل انسانی	ضریب مسیر	۰/۳۱
	سطح معنی‌داری	۰/۰۵
	ارزش T	۴/۱۹

چون مقدار T محاسبه‌شده برای این رابطه بزرگ‌تر از چهار است؛ بنابراین در سطح اطمینان ۹۵ درصد می‌توان ادعا کرد که بین سطح مهارت عوامل انسانی و امنیت سیستم‌های اطلاعاتی رابطه معناداری با ضریب مسیر ۳۱ درصد وجود دارد و سطح مهارت عوامل انسانی بر امنیت سیستم‌های اطلاعاتی اثرگذار است. درنتیجه فرضیه H_1 این پژوهش مورد تأیید قرار می‌گیرد.

آزمون فرضیه پنجم با استفاده از نرم‌افزار لیزرل

فرضیه H_1 بیان می‌کند که بین تقویت خط‌مشی و امنیت سیستم‌های اطلاعاتی رابطه مثبت وجود دارد. در این فرضیه هدف بررسی اثر مستقیم تقویت خط‌مشی بر امنیت سیستم‌های اطلاعاتی است. مقدار ارزش T (T value) و ضریب مسیر برای این رابطه در جدول پنج آمده است.

جدول ۵. نتیجه آزمون فرضیه پنجم

متغیر مستقل	متغیر وابسته: اثربخشی امنیت سیستم‌های اطلاعاتی	
تقویت خط‌مشی	ضریب مسیر	۰/۳۷
	سطح معنی‌داری	۰/۰۵
	ارزش T	۷/۳۷

چون مقدار T محاسبه‌شده برای این رابطه بزرگ‌تر از هفت است؛ بنابراین در سطح اطمینان ۹۵ درصد می‌توان ادعا کرد که بین تقویت خط‌مشی و امنیت سیستم‌های اطلاعاتی رابطه معناداری با ضریب مسیر ۳۷ درصد وجود دارد و تقویت خط‌مشی بر امنیت سیستم‌های اطلاعاتی اثرگذار است. درنتیجه فرضیه H_1 این پژوهش مورد تأیید قرار می‌گیرد.

نتیجه فرضیه: تقویت خط‌مشی تأثیر معنی‌داری بر امنیت سیستم‌های اطلاعاتی

آزمون فرضیه ششم با استفاده از نرم‌افزار لیزرل

فرضیه H_1 بیان می‌کند که بین سطح خودباوری افراد و امنیت سیستم‌های اطلاعاتی رابطه مثبت وجود دارد. در این فرضیه هدف بررسی اثر مستقیم خودباوری افراد بر امنیت سیستم‌های اطلاعاتی است. مقدار ارزش T (T value) و ضریب مسیر برای این رابطه در جدول شش آمده است.

جدول ۶. نتیجه آزمون فرضیه ششم

متغیر مستقل	متغیر وابسته: اثربخشی امنیت سیستم‌های اطلاعاتی	
خودباوری افراد	ضریب مسیر	۰/۴۱
	سطح معنی‌داری	۰/۰۵
	ارزش T	۹/۴۱

چون مقدار T محاسبه‌شده برای این رابطه بزرگ‌تر از نُه است؛ بنابراین در سطح اطمینان ۹۵ درصد می‌توان ادعا کرد که بین خودباوری افراد و امنیت سیستم‌های اطلاعاتی رابطه معناداری با ضریب مسیر ۴۱ درصد وجود دارد و خودباوری افراد بر امنیت سیستم‌های اطلاعاتی اثرگذار است. درنتیجه فرضیه H_1 این پژوهش مورد تأیید قرار می‌گیرد.

آزمون فرضیه هفتم با استفاده از نرم‌افزار لیزرل

فرضیه H_1 بیان می‌کند که بین سطح تجربیات افراد و امنیت سیستم‌های اطلاعاتی رابطه مثبت وجود دارد. در این فرضیه هدف بررسی اثر مستقیم میزان تجربیات افراد بر امنیت سیستم‌های اطلاعاتی است. مقدار ارزش T (T value) و ضریب مسیر برای این رابطه در جدول هفت آمده است.

جدول ۷. نتیجه آزمون فرضیه هفتم

متغیر مستقل	متغیر وابسته: اثربخشی امنیت سیستم‌های اطلاعاتی	
میزان تجربه‌ی عوامل انسانی	ضریب مسیر	۰/۳۸
	سطح معنی‌داری	۰/۰۵
	ارزش T	۸/۲۷

چون مقدار T محاسبه‌شده برای این رابطه بزرگ‌تر از هشت است؛ بنابراین در سطح اطمینان ۹۵ درصد می‌توان ادعا کرد که بین میزان تجربه عوامل انسانی و امنیت سیستم‌های اطلاعاتی رابطه معناداری با ضریب مسیر ۳۸ درصد وجود دارد و میزان تجربه عوامل انسانی بر امنیت سیستم‌های اطلاعاتی اثرگذار است. درنتیجه فرضیه H_1 این پژوهش مورد تأیید قرار می‌گیرد.

ارزیابی برازش کل مدل

حال که معنی‌داری شاخه‌ها مورد تائید قرار گرفت، این بار مجموعه روابط متغیرها و کل مدل با استفاده از نرم‌افزار لیزرل مورد آزمون قرار می‌گیرد تا معنی‌داری مدل در کل موردبررسی واقع شود. جهت ارزیابی مدل شاخص‌های متعددی وجود دارد که عبارت‌اند از:

۱- مجذور کای (X^2) و نسبت X^2/df:

وقتی حجم گروه نمونه برابر با ۷۵ تا ۲۰۰ باشد، مقدار مجذور کای یک اندازه معقول برازندگی است؛ اما برای مدل‌های با n بزرگ‌تر، مجذور کای (همانند همه آزمونه‌ای معنادار بودن) تقریباً همیشه ازلحاظ آماری معنادار است. این مسئله، با توجه به این مطلب که برای روش SEM، گروه‌های نمونه با حجم زیاد توصیه می‌شود، تناقض دارد. علاوه بر این، مجذور کای تحت تأثیر مقدار همبستگی‌های موجود در مدل نیز هست؛ هرچه این همبستگی‌ها زیادتر باشد، برازش ضعیف‌تر است.

۲-شاخص برازندگی (GFI):

بستگی به حجم نمونه ندارد و نشان می‌دهد که مدل تا چه حد نسبت به عدم وجود آن، برازندگی بهتری دارد. چون GFI نسبت به سایر مشخصه‌های برازندگی اغلب بزرگ‌تر است، برخی از پژوهشگرها نقطه برش ۰/۹۵ را برای آن پیشنهاد کرده‌اند. بر پایه قرارداد، مقدار GFI باید برابر یا بزرگ‌تر از ۰/۹۰ باشد تا مدل موردنظر پذیرفته شود.

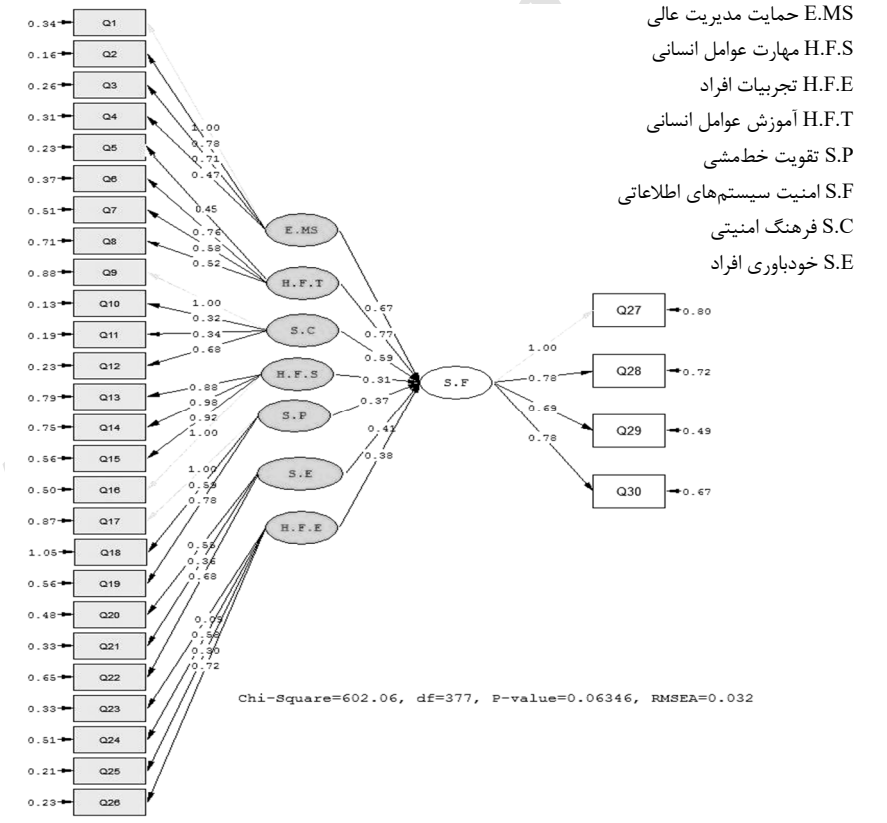
۳-شاخص تعدیل برازندگی (AGFI):

شاخص AGFI نیز مانند GFI، مقدار AGFI نیز باید برابر با بزرگ‌تر از ۰/۹۰ باشد تا مدل موردنظر پذیرفته شود

۴-شاخص نرم شده برازندگی (NFI):

۵-ریشه دوم برآورد واریانس خطای تقریب (RMSEA):

مقدار RMSEA که به‌واقع همان آزمون انحراف هر درجه آزادی است، برای مدل‌هایی که برازندگی خوبی داشته باشد، کمتر از ۰/۰۵ است. مقادیر بالاتر از آن تا ۰/۰۸ نشان‌دهنده خطاهای معقولی برای تقریب در جامعه است. مدل‌هایی که RMSEA آن‌ها ۰/۱۰ یا بیشتر باشد برازش ضعیفی دارد.



شکل ۱. مدل اصلی پژوهش

بر اساس شکل یک، X^2 برابر۱۲۳/۹۲،DF برابر ۸۹، X2/DF برابر ۱/۳۹، RMSEA برابر ۰/۰۶۹،GFI برابر ۰/۹۷،AGFI برابر ۰/۹۵ و NFI برابر ۰/۹۷؛ بنابراین در کل می‌توان گفت برازش مدل خیلی خوب است و می‌توانیم اظهار کنیم که مجموعه متغیرهای «حمایت مدیریت عالی»، «آموزش عوامل انسانی»، «فرهنگ امنیتی»، «مهارت عوامل انسانی»، «خط‌مشی امنیتی»، «خودباوری» و «تجربه افراد» منجر به بهبود و بهینه شدن «امنیت سیستم‌های اطلاعاتی» می‌گردد. درنتیجه با آزمودن تمامی فرضیات و تائید همه آن‌ها، مدل کلی پژوهش به‌صورت جدول هشت درمی‌آید:

جدول ۸. مدل کلی پژوهش

X^2	DF	X^2/DF	RMSEA	GFI	AGFI	NFI
ملاک بیش از ۰/۰۵	ملاک بیش از صفر	ملاک کمتر از سه	ملاک کمتر یا مساوی ۰/۰۸	ملاک بیش از ۰/۹۰	ملاک بیش از ۰/۹۰	ملاک بیش از ۰/۹۰
۱۲۳/۹۲	۸۹	۱/۳۹	۰/۰۶۹	۰/۹۷	۰/۹۵	۰/۹۷

همان‌طور که در شکل یک قابل‌مشاهده شد خروجی نرم‌افزار لیزرل نشان می‌دهد که تمامی ابعاد (حمایت مدیریت عالی، آموزش، فرهنگ امنیتی، مهارت کاربران، تقویت خط‌مشی، خودباوری و تجربیات افراد) با سازه موردنظر یعنی همان اثربخشی امنیت سیستم‌های اطلاعاتی دارای بارهای عاملی بالایی هستند و با توجه به اطمینان ۹۵ درصد می‌توان بیان داشت که برازش این مدل قابل‌تأییداست

نتیجه‌گیری

در بیشتر تحقیقاتی که در زمینه‌ی امنیت سیستم‌های اطلاعاتی صورت گرفته یک نوع دید و رویکرد منفی وجود داشته است و بیشتر متخصصین امنیت اطلاعات به دنبال یک سری ابزارهای فنی برای برطرف کردن مشکلات امنیتی‌شان بوده‌اند؛ اما اخیراً یک پارادایم جدید در زمینه‌ی امنیت اطلاعات به وجود آمده است که آن را به‌عنوان «مسئله انسانی» و «مسئله‌سازمانی» موردتوجه قرار می‌دهند. موفقیت امنیت اطلاعات امروزه به نظر می‌رسد تا حد زیادی به رفتار اثربخش افرادی که در به‌کارگیری آن درگیرند، وابسته باشد. رفتارهای درست و سازنده توسط کاربران، مدیران سیستم و افراد دیگر می‌تواند اثربخشی امنیت اطلاعات را تا حد زیادی ارتقا دهد، درحالی‌که رفتارهای نادرست و مخرب اساساً می‌تواند مانع از اثربخشی آن شود.

هیچ سازمانی یا سیستم اطلاعاتی وجود ندارد که بتواند امنیت را به‌صورت کامل برقرار سازد یا ادعای داشتن آن را داشته باشد. بااین‌وجود تمرین خاصی وجود دارد که مدیران می‌توانند با استفاده از آن، حمایت کردن و اثربخشی امنیتی‌شان را هر چه بیشتر برقرار سازند. در این پژوهش به این نتیجه رسیدیم که عوامل انسانی دارای تأثیر و ارزش در اثربخشی ISS هستند؛ بنابراین با توجه بیشتر به آن‌ها می‌توانیم تأثیر بیشتری بر روی بهبود اثربخشی امنیتی و حمایت کردن از دارایی‌های اطلاعاتی‌مان در سازمان

داشته باشیم در این راستا با بررسی ادبیات پژوهش، بعضی از عوامل مدیریتی و انسانی اثرگذار بر اثربخشی ISS در سازمان‌ها شناسایی شدند و اثر هر یک از آن‌ها بر اثربخشی موردبررسی قرار گرفت.

در این پژوهش پرسشنامه توزیع‌شده شامل هفت بخش است که عبارت است از حمایت مدیریت عالی، آموزش عوامل انسانی، فرهنگ امنیتی، مهارت کاربران، تقویت خط‌مشی، اثربخشی امنیتی، خودباوری افراد و تجربیات افراد است.

در پاسخ به سؤال اول پژوهش در مورد میزان تأثیر حمایت مدیریت عالی بر اثربخشی امنیتی نتایج آزمون لیزرل نشان می‌دهد که حمایت مدیریت عالی بر اثربخشی امنیتی تأثیر دارد و می‌توان اظهار داشت که حمایت مدیریت عالی از امنیت، به‌حساب آوردن آن در استراتژی‌ها و تصمیمات سازمان و توافق شخصی مدیران عالی بر خط‌مشی‌های امنیتی بر اثربخشی امنیتی تأثیر مثبت دارد.

در مورد سؤال دوم پژوهش در رابطه با میزان تأثیر سطح آموزش کارکنان آموزش‌وپرورش بر امنیت سیستم‌های اطلاعاتی نتایج آزمون لیزرل نشان می‌دهد که آموزش امنیتی به کاربران بر اثربخشی امنیتی تأثیر دارد و می‌توان اظهار کرد که آموزش امنیتی به کاربران به‌صورت مستقیم بر اثربخشی امنیت سیستم‌های اطلاعاتی تأثیرگذار است.

در پاسخ به سؤال سوم پژوهش مبنی بر میزان تأثیر سطح فرهنگ امنیتی در امنیت سیستم‌های اطلاعاتی نتایج آزمون لیزرل نشان می‌دهد که فرهنگ امنیتی بر اثربخشی امنیتی تأثیرگذار است؛ و می‌توان اظهار کرد که ایجاد، بهبود و تقویت یک فرهنگ امنیتی خوب برای سازمان، تأثیر مثبتی بر اثربخشی امنیتی سازمان خواهد داشت.

نتایج آزمون لیزرل در رابطه با میزان تأثیر مهارت کاربران در امنیت سیستم‌های اطلاعاتی نشانگر این است که مهارت کاربران بر اثربخشی امنیتی تأثیر دارد و می‌توان اظهار داشت که افراد بامهارت بالا و نیت‌های خیرخواهانه می‌توانند اثر مثبتی را بر اثربخشی سازمان داشته باشند؛ بنابراین مدیران سازمان‌ها با توجه به این نکته می‌توانند در جهت افزایش مهارت افراد و بهبود نیت‌های آن‌ها تلاش‌هایی را صورت دهند که بتوانند بر اثربخشی امنیتی در سازمان مؤثر باشند.

در مورد سؤال پنجم پژوهش در رابطه با میزان تأثیر تقویت خط‌مشی امنیتی بر امنیت سیستم‌های اطلاعاتی نتایج آزمون لیزرل نشان می‌دهد که تقویت خط‌مشی بر اثربخشی امنیتی تأثیر دارد؛ و سازمان‌ها با داشتن خط‌مشی امنیتی و تقویت مستمر آن، می‌توانند اثرات قابل‌توجهی بر اثربخشی امنیتی در سازمان‌ها داشته باشند.

در مورد میزان تأثیر خودباوری کارکنان آموزش‌وپرورش در امنیت سیستم‌های اطلاعاتی نتایج آزمون لیزرل نشان می‌دهد که خودباوری افراد بر اثربخشی امنیتی تأثیر دارد؛ و افراد با داشتن حس خودباوری و اعتمادبه‌نفس در زمینه‌ی امنیت اطلاعات بر اثربخشی ISS در سازمان تأثیرگذارند.

نتایج آزمون لیزرل در مورد میزان تأثیر تجربه‌ی کارکنان آموزش‌وپرورش در امنیت سیستم‌های اطلاعاتی نشان می‌دهد که تجربیات افراد بر اثربخشی امنیتی تأثیرگذار است؛ و به وجود آوردن زمینه‌هایی برای افزایش تجربیات افراد در زمینه امنیت اطلاعات بر اثربخشی ISS در سازمان اثرگذار است.

نتایج حاصل از بررسی فرضیه‌ها

فرضیه‌ی اول پژوهش: حمایت مدیریت عالی تأثیر معنی‌داری بر امنیت سیستم‌های اطلاعاتی دارد.

بر اساس تحلیل داده‌های جامعه‌ی آماری در بخش حمایت مدیریت عالی، کارکنان اداره آموزش‌وپرورش شهرستان‌های گنبدکاووس و مراوه‌تپه به این نکته توجه ویژه داشتند که برای بالا بردن اثربخشی امنیتی می‌بایست مدیران عالی از کارکنان ادارات حمایت کنند تا در ادارات، امنیت اطلاعات افزایش یابد. این نتیجه با یافته‌های پژوهشی پاک‌دامن (۱۳۸۸) مبنی بر لزوم حمایت مدیریت عالی، آرام (۱۳۸۸) مبنی بر لزوم حمایت مدیریت عالی و شهریوری (۱۳۹۰) مبنی بر ضرورت حمایت مدیریت عالی که کارکنان وجود حمایت مدیریت عالی را برای اثربخشی امنیتی ضروری دانستند، هماهنگی دارد. همچنین نتایج پژوهش با ورمولن ون سولمز (۱۹۹۹) که معتقد است وجود حمایت مدیریت عالی از ضروریات اساسی برای به وجود آمدن اثربخشی امنیتی در سازمان است و اسمیت[1] (۲۰۰۴) مبنی بر اهمیت حمایت مدیریت عالی و کناپ[2] و همکاران (۲۰۰۴) مبنی بر ضرورت حمایت مدیریت عالی در سازمان‌ها، هماهنگی دارد.

فرضیه‌ی دوم پژوهش: سطح آموزش کارکنان آموزش‌وپرورش تأثیر معنی‌داری بر امنیت سیستم‌های اطلاعاتی دارد.

بر اساس تحلیل داده‌های جامعه‌ی آماری در بخش آموزش کارکنان، کارکنان اداره آموزش‌وپرورش شهرستان‌های گنبدکاووس و مراوه‌تپه به این نکته توجه ویژه داشتند که برای بالا بردن اثربخشی امنیتی می‌بایست آموزش بین کارکنان صورت گیرد تا در ادارات، امنیت اطلاعات افزایش یابد؛ این نتیجه با یافته‌های پژوهشی محمود زاده و راد رجبی (۱۳۸۵) مبنی بر اهمیت آموزش، شایان (۱۳۸۷) مبنی بر لزوم آموزش، پاک‌دامن (۱۳۸۸) مبنی بر لزوم آموزش برای افراد، نظیف (۱۳۸۸) مبنی بر آموزش مجازی و کناپ و همکاران (۲۰۰۴) که لزوم آموزش را برای ایجاد امنیت اطلاعات ضروری دانستند، هماهنگی دارد.

فرضیه‌ی سوم پژوهش: سطح فرهنگ امنیتی تأثیر معنی‌داری بر امنیت سیستم‌های اطلاعاتی دارد.

بر اساس تحلیل داده‌های جامعه‌ی آماری در بخش فرهنگ امنیتی، کارکنان اداره آموزش‌وپرورش شهرستان‌های گنبدکاووس و مراوه‌تپه به این نکته توجه ویژه داشتند که برای بالا بردن اثربخشی امنیتی می‌بایست فرهنگ امنیتی بین کارکنان ایجاد شود تا در ادارات، امنیت اطلاعات افزایش یابد؛ این نتیجه با یافته‌های پژوهشی شایان (۱۳۸۷) مبنی بر اهمیت فرهنگ امنیتی، پاک‌دامن (۱۳۸۸) مبنی بر اهمیت فرهنگ امنیتی و آرام (۱۳۸۹) که فرهنگ امنیتی را از ضروریات هر سازمانی می‌داند که قصد ایجاد امنیت اطلاعات را دارد، هماهنگی دارد.

1. Smith
2. Knapp

فرضیه‌ی چهارم پژوهش: میزان مهارت کارکنان آموزش‌وپرورش تأثیر معنی‌داری بر امنیت سیستم‌های اطلاعاتی دارد.

بر اساس تحلیل داده‌های جامعه‌ی آماری در بخش مهارت عوامل انسانی، کارکنان اداره آموزش‌وپرورش شهرستان‌های گنبدکاووس و مراوه‌تپه به این نکته توجه ویژه داشتند که برای بالا بردن اثربخشی امنیتی می‌بایست مهارت عوامل انسانی افزایش یابد تا در ادارات، امنیت اطلاعات افزایش یابد؛ این نتیجه با یافته‌های پژوهشی محمود زاده و راد رجبی (۱۳۸۵) مبنی برافزایش مهارت عوامل انسانی، زنده‌دل نوبری (۱۳۸۶) مبنی بر اهمیت مهارت عوامل انسانی، نصرمحمدی (۱۳۹۲) مبنی بر لزوم مهارت، گوهریان (۱۳۹۴) مبنی بر اهمیت مهارت بین کارکنان هماهنگی دارد. همچنین با یافته‌های پژوهش وود[1] (۲۰۰۰) که وجود مهارت با نیت خیر را برای کارکنان ضروری می‌داند و استنتون[2] و همکاران (۲۰۰۴) که معتقدند مهارت عوامل انسانی ضروری است مطابقت می‌کند.

فرضیه‌ی پنجم پژوهش: تقویت خط‌مشی تأثیر معنی‌داری بر امنیت سیستم‌های اطلاعاتی دارد.

بر اساس تحلیل داده‌های جامعه‌ی آماری در بخش تقویت خط‌مشی، کارکنان اداره آموزش‌وپرورش شهرستان‌های گنبدکاووس و مراوه‌تپه به این نکته توجه ویژه داشتند که برای بالا بردن اثربخشی امنیتی می‌بایست خط و مشی امنیتی سازمان باید افزایش یابد تا در ادارات، امنیت اطلاعات افزایش یابد؛ این نتیجه با یافته‌های پژوهشی زنده‌دل نوبری (۱۳۸۶) مبنی بر وجود خط‌مشی مناسب در سازمان‌ها، الوف (۲۰۰۴) مبنی بر تقویت خط‌مشی و اسمیت (۲۰۰۴) که معتقد بر تقویت خط‌مشی در سازمان است هماهنگی می‌کند.

فرضیه‌ی ششم پژوهش: خودباوری کارکنان آموزش‌وپرورش تأثیر معنی‌داری بر امنیت سیستم‌های اطلاعاتی دارد.

بر اساس تحلیل داده‌های جامعه‌ی آماری در بخش خودباوری عوامل انسانی، کارکنان اداره آموزش‌وپرورش شهرستان‌های گنبدکاووس و مراوه‌تپه به این نکته توجه ویژه داشتند که برای بالا بردن اثربخشی امنیتی می‌بایست خودباوری عوامل انسانی در سازمان افزایش یابد تا در ادارات، امنیت اطلاعات افزایش یابد؛ این نتیجه با یافته‌های پژوهشی شایان (۱۳۸۷) مبنی بر اهمیت خودباوری، وود (۲۰۰۰) که معتقد است خودباوری افراد در ایجاد فضای امن سازمان مؤثر است و همچنین با یافته‌های کریتزینگر و اسمیت (۲۰۱۱) مبنی بر اهمیت افزایش خودباوری عوامل انسانی هستند، هماهنگی دارد.

فرضیه‌ی هفتم پژوهش: میزان تجربه‌ی کارکنان آموزش‌وپرورش تأثیر معنی‌داری بر امنیت سیستم‌های اطلاعاتی دارد.

بر اساس تحلیل داده‌های جامعه‌ی آماری در بخش تجربیات عوامل انسانی کارکنان اداره آموزش‌وپرورش شهرستان‌های گنبدکاووس و مراوه‌تپه به این نکته توجه ویژه داشتند که برای بالا بردن اثربخشی امنیتی می‌بایست تجربیات عوامل انسانی در سازمان افزایش یابد تا در ادارات، امنیت اطلاعات

1. Wood
2. Stanton

افزایش یابد؛ این نتیجه با یافته‌های پژوهشی زنده‌دل نوبری (۱۳۸۶) مبنی برافزایش تجربه، شایان (۱۳۸۷) مبنی بر اهمیت تجربه‌ی مستقیم، نصرمحمدی (۱۳۹۲) مبنی بر اهمیت تجربیات عوامل انسانی و گوهریان (۱۳۹۴) که معتقد است افزایش تجربیات مستقیم و غیرمستقیم در افراد باعث افزایش امنیت اطلاعات در سازمان می‌شود، هماهنگی دارد.

پیشنهادهای پژوهش

مدل ارائه‌شده در این پژوهش تقریباً مدلی کامل است که سازه‌های مدیریتی و انسانی مرتبط با امنیت سیستم‌های اطلاعاتی را در برگرفته است؛ اما سازه‌های دیگری همچون سازه‌های مربوط به مدیریت ریسک که این مدل آن‌ها را شامل نمی‌شود را می‌توان به آن افزود. بنابراین با استفاده از این پژوهش و این مدل می‌توان سازه‌های دیگری را به این مدل اضافه کرد.

۱- محققین می‌توانند مدل ارائه‌شده در این پژوهش را با به‌کارگیری نمونه‌های مختلفی از فرهنگ‌ها یا صنایع مختلف موردبررسی قرار دهند تا اثر آن را در زمینه‌های مختلف مورد شناسایی بهتر قرار دهند.

۲- درزمینه‌ی امکان وجود ارتباط‌های دیگر بین متغیرهای این پژوهش می‌توانند پژوهش دیگری انجام دهند.

۳- می‌توانند تحقیق‌های دیگری را در رابطه با علل عدم توجه به عوامل مدیریتی اثرگذار در امنیت IS تا انجام دهند.

۴- انجام مطالعات تطبیقی از کشورهای موفق در زمینه امنیت اطلاعات از بعد نیروی انسان.

فهرست منابع

آرام، محمدرضا. ۱۳۸۸. شاخص‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت گاز پارس جنوبی پایان‌نامه‌ی کارشناسی ارشد، دانشگاه علامه طباطبایی.

احترامی، بابک. ۱۳۸۸. نقطه‌ضعف اصلی. *مجله شبکه*. ۱۳۸(۵۲): ۴۸-۶۹

بذر پور، فرزانه. ۱۳۸۴. تهدید و امنیت در فضای مجازی. تهران: شبکه فناوری اطلاعات در ایران.

بهاری، مهدی. ۱۳۸۴. امنیت تجهیزات شبکه. *مجله شبکه*. ۱۱۸ (۵۴): ۵۱-۷۳.

پاک‌دامن، راضیه. ۱۳۸۸. طراحی ساختار و فرایند صدور گواهینامه و اعتبارنامه امنیت اطلاعات و اطلاع‌رسانی. پایان‌نامه‌ی کارشناسی ارشد، دانشگاه تربیت مدرس.

خیر گو، منصور و جواد شکوهی. ۱۳۹۵. شناسایی و رتبه‌بندی عوامل کلیدی مؤثر بر اثربخشی سیستم‌های اطلاعاتی در سازمان‌های دولتی. پژوهشنامه پردازش و مدیریت اطلاعات ۳۲ (۳): ۱۷-۳۹

زنده‌دل نوبری، بابک. ۱۳۸۶. *مدلی برای رتبه‌بندی سازمان‌ها بر مبنای اندازه‌گیری و شناسایی میزان بلوغ امنیت اطلاعات*. تهران: آگاه.

شایان، علی. ۱۳۸۷. طراحی مدل جامع مدیریت امنیت اطلاعات در بانکداری الکترونیکی. پایان‌نامه کارشناسی ارشد، دانشگاه تربیت مدرس

شهریوری، شهرزاد. ۱۳۹۰. ارائه مدل بلوغ برای حاکمیت بر امنیت اطلاعات در مدیریت زنجیره تأمین. پایان‌نامه‌ی کارشناسی ارشد، دانشگاه تربیت مدرس.

گوهریان، حمیدرضا. ۱۳۹۴. طراحی سیستمی هوشمند برای تشخیص و کنترل ریسک‌های امنیت در محیط وب ۲. پایان‌نامه کارشناسی ارشد، دانشگاه تربیت مدرس.

محمود زاده، ابراهیم و مهدی راد رجبی. ۱۳۸۵. *مدیریت امنیت در سیستم‌های اطلاعاتی*. تهران: علوم مدیریت ایران.

نصرمحمدی، محمود. ۱۳۹۲. کشف ناهنجاری در شبکه با استفاده از مصورسازی هشدارهای امنیتی پایان‌نامه‌ی کارشناسی ارشد، دانشگاه تربیت مدرس.

محمدی، محمود. ۱۳۹۲، "کشف ناهنجاری در شبکه با استفاده از مصورسازی هشدارهای امنیتی" پایان‌نامه‌ی کارشناسی ارشد، دانشگاه تربیت مدرس.

نظیف، رکسانا. ۱۳۸۸. ارائه یک مدل آموزش مجازی امن با نگاه به مسئله حریم شخصی و امنیت اطلاعات در شرکت ملی نفت ایران پایان‌نامه‌ی کارشناسی ارشد، دانشگاه تربیت مدرس.

Bandura, A, 1986. Social foundations of thought and action: A social cognitive theory. Prentice-Hall.

Eloff, prof.2004. Information security development. Computer science and information systems

Hinson, C., V. S. Rossouw. 2004. Using security: easier said than done? Computer fraud &security

Kim, S. H., K. H. Yang, and S. Park. 2014. An integrative behavioral model of information security policy compliance. The Scientific World Journal 2014

Kritzinger D, smith.2011. Towards information security behavioral compliance. Computer& security

Knapp, K.J., Marshall, T.E., Rainer, R.K. and Morrow, D.W., 2004. Top Ranked Information Security Issues: The 2004 International Information Systems Security Certification Consortium (ISC) 2 Survey Results. Auburn University: Alabama.

National information Assurance Glossary. 1997 (Rep.NO.NSTISSI 4009)

Smith, john. 2004. Social cognitive theory of organizational management. Academy of management.

Stanton,f; Isect, ltd, 2004. Human factors in information security, innovative information security awareness programs, notice bored.

Vermeclen, von solms, 1999. Information security policy, department of computer science

Wood,c. 2000. An unappreciated reason why security policies fail. Computer fraud and security.

Identify the Impacting of Human Factors in Information Security in the Department of Education and Training

Fatemeh Zandian[1]
Assistant Prof. Ph.D. Knowledge and Information Science, Faculty of Management and Economics, Tarbiat Modares University, Tehran, Iran
Ayjamal Gharavi
M.A, Knowledge and Information Science, Faculty of Management and Economics, Tarbiat Modares University, Tehran Iran
Mohammad Hassanzadeh
Associate Prof. Ph.D. Knowledge and Information Science, Faculty of Management and Economics, Tarbiat Modares University, Tehran, Iran

Abstract: The purpose of this study was to identify effect of human factors on information security in education departments of Gonbad-e Qabus and Maraveh Tapeh. In this study, the effective variables on information security were selected from the human resource dimension and viewpoints of managers and employees toward their impact on security were evaluated and given the importance of security for today's organizations, a managerial model was proposed to investigate the role of human factors in the security of information systems. The research is the applied research method which has been done in a descriptive - survey method and 103 employees who were most used by computer and network were selected as a statistical sample using the purposeful sampling method. The data collection tool was a researcher-made questionnaire (including seven variables) which using SPSS software and its reliability coefficient is 0.99% was calculated and the content validity method was used to determine its reliability and validity. The data analysis was carried out using the LISREL software. The Results show that from the viewpoint of education staff in Gonbad-e Qabus and Maraveh Tapeh, The support of the higher management of the education department, the training of users, the security culture among users, users' skills, strengthening the policy of users, self-efficacy and experiences of users have a direct impact on the effectiveness of information systems security which ultimately leads to improve the security of information systems. In addition, Lisrel's output shows that all dimensions (high management support, training, security culture, user skills, policy enhancement, self - efficacy, self - efficacy and experiences) have a high operating load with the desired structure, the same as the effectiveness of information system security and with 95% confidence, it can be stated that fitting this model is acceptable.

Keywords: Education Departments of Gonbad-E Qabus and Maraveh Tapeh, Information Systems, Management Structure, Security of Information Systems, Security Efficiency.

1. Corresponding author: fatemehzandian@modares.ac.ir