فصلنامه پژوهش‌های حفاظتی ـ امنیتی
دانشگاه جامع امام حسین(علیه‌السلام)

سال نهم، شمارهٔ ۳۵ (پاییز ۱۳۹۹)صص ۱۷۰-۱۴۷

ارائه مدل مفهومی مؤلفه‌ها و شاخص‌های سرمایه انسانی مؤثر بر امنیت اطلاعات سازمان‌ها

■ ساناز نوده فراهانی ■
دانشجوی دکتری،گروه حسابداری، دانشکده حسابداری و مدیریت، دانشگاه ازاداسلامی ، واحد کاشان، ایران
■ حسین جباری ■
استادیار گروه حسابداری، دانشکده حسابداری و مدیریت، دانشگاه ازاداسلامی ، واحد کاشان، ایران
(نویسنده مسئول)
■ حسین پناهیان ■
دانشیار ، گروه مدیریت، دانشکده حسابداری و مدیریت، دانشگاه ازاداسلامی ، واحد کاشان، ایران

تاریخ دریافت: ۱۳۹۹/۰۵/۲۰ تاریخ پذیرش: ۱۳۹۹/۰۸/۱۱

چکیده

سرمایهٔ انسانی شامل دانش، مهارت، نوآوری و سایر توانایی‌های موجود در افراد سازمان است که به آنها یاری می‌رساند تا در فعالیت‌های سازمان موفق باشند. سرمایه‌انسانی مهم‌ترین عامل در نوآوری و بازسازی سازمان است. بسیاری از صاحب‌نظران، سرمایه‌انسانی را ارزشمندترین داراییِ سازمان می‌دانند. بخش زیادی از اطلاعات در هر سازمان به دستِ منابع انسانی و در قالب طرح‌ها، نقشه‌ها، سیاست‌ها، بخشنامه‌ها، مکاتبات بازرگانی و مستندات طرح‌های پژوهشی، تهیه می‌شوند و توسعه می‌یابند. نظر به اهمیت و نقش اطلاعات یادشده به‌عنوان بخشی از مهمترین دارایی و کلید رشد و موفقیت هر سازمان، جلوگیری از دسترسی نامحرمان و سایر تهدیدها، کاهش شدت آسیب‌پذیری‌ها را به‌همراه دارد.

هدف اصلی این مطالعه تعیین مؤلفه‌ها و شاخص‌های سرمایه‌انسانی مؤثر بر امنیت اطلاعات سازمان‌هاست. این تحقیق، یک پژوهش توصیفی‌همبستگی و از نوع تحقیقات کاربردی است. جامعه‌آماری این پژوهش ۳۵۰ نفر از خبرگان حوزه‌مدیریت منابع انسانی سازمان‌ها در شهر تهران است که صد نفر از آنها به‌صورت نمونه‌گیری تصادفی انتخاب شده‌اند و پرسشنامه بین آنها توزیع شده است. از این تعداد، هشتاد پرسشنامه‌تکمیل‌شده، جمع‌آوری شده است. داده‌های جمع‌آوری‌شده به کمک نرم‌افزارهای تحلیل آماری، تجزیه و تحلیل شده‌اند که در نهایت، متغیرهای مدیریت و رهبری، آموزش کارکنان، فرهنگ امنیتی، تقویت سیاست‌های امنیتی، تجربیات و خودباوری افراد به‌عنوان شاخصه‌های سرمایه‌انسانی مؤثر بر امنیت اطلاعات سازمان‌ها معرفی شده‌اند.

کلید واژگان: امنیت، امنیت اطلاعات، سرمایه انسانی، سازمان.

مقدمه

تعلیم و تربیت به انحای مختلف و در تمامی مقاطع، از مصادیق بارز و مهم سرمایه‌گذاری انسانی است و منبع مهمی برای تشکیل سرمایهٔ انسانی به‌حساب می‌آید. به‌کارگیری صحیح و مداوم سرمایه‌های انسانی موجب ارتقای کیفیت و بهبود هرچه‌بیشتر کارایی و بهره‌وری آن‌ها می‌شود. همهٔ مخارجی که در امر تعلیم و تربیت، چه از طرف دولت و چه از طرف مؤسسه‌ها و خانواده‌ها یا افراد صرف می‌شود، اعم از مستقیم و غیر مستقیم، هزینهٔ سرمایه‌گذاری انسانی است. بنابراین هر چه جامعه‌ای در این زمینه بیشتر سرمایه‌گذاری کند، با شتاب بیشتری به‌سوی توسعه حرکت می‌کند. درآمدها و عواید سرمایه‌گذاری انسانی که شامل درآمدهای مستقیم و غیر مستقیم و اجتماعی و خصوصی است، منافعی طولانی‌مدت بوده و چه‌بسا آثار آن برای نسل‌های بعدی نیز تداوم یابد.

مهم‌ترین مؤلفهٔ سازمانی که در سازگاری و بقا و توسعهٔ بنگاه‌ها، با توجه به تغییرات اقتصاد جهانی، مؤثر واقع می‌شود، سرمایهٔ دانشی یا منابع انسانی سازمان‌هاست. پیام رسا و صریحی که تغییرات و وضعیت نوین جهانی برای سازمان‌ها و بنگاه‌های اقتصادی و حتی ملت‌ها به‌همراه دارد، پیام تولید، انتقال، کاربرد و ذخیرهٔ دانش و مهارت از طریق رویکردها و سازوکارهای اثربخش و کارآمد است. سرمایهٔ انسانی با عنوان دانش فردی، مهارت‌ها، توانایی‌ها و دانش موجود در کارکنان یک سازمان برای خلق ارزش و حل‌کردن مسائل سازمان تعریف شده است (طبرسا و همکاران، ۱۳۹۲: ۱۳۱-۱۱۰).

امروزه اینترنت به‌عنوان مؤلفهٔ اصلی فضای سایبر، بسیاری از جنبه‌های جامعهٔ انسانی را تغییر داده است. در سال‌های اخیر اهمیت اینترنت و فناوری اطلاعات به‌طور درخور ملاحظه‌ای افزایش یافته است و با ورود فناوری اطلاعات به سازمان‌ها، عملکرد مدیریت منابع انسانی نیز تغییر یافته است. ایجاد وضعیت مناسب برای به‌کارگیری دقیق فناوری اطلاعات به‌نحو چشمگیری در توسعهٔ جامعه انسانی مؤثر است. این تأثیر به‌گونه‌ای است که مدیریت منابع انسانی ناگزیر از آشنایی با وضعیت جدید است تا با استفاده از ظرفیت‌های نوین فناوری اطلاعات سبب ارتقای عملکرد سازمان شود.

امروزه یکی از شاخه‌های تخصصی، طراحی سامانه‌های اطلاعاتی است. از طرفی، مدیریت به‌منظور تصمیم‌گیری راهبردی نیازمند اطلاعاتی است که عموماً به‌وسیلهٔ سامانه‌های اطلاعاتی فراهم می‌شود. صحت و دسترسی و محرمانگی اطلاعات ازجمله مؤلفه‌های مهمی است که ارزش اطلاعات تولیدشده و پردازش‌شده و نگهداری‌شده را ارتقا می‌دهد. مجموعهٔ این خصوصیات به‌عنوان امنیت اطلاعات

قلمداد می‌شود. بنابراین در سازمان‌هایی که امنیت سامانه‌های اطلاعاتی ضعیف است، امکان نفوذ به سامانه و دست‌کاری اطلاعات بسیار زیاد و خسارت‌های وارده‌شده ممکن است جبران‌ناپذیر باشد. نیاز به ایمنی اطلاعات ایجاب می‌کند که پیش‌بینی‌های لازم از سوی مدیریت صورت گیرد تا اطلاعات سامانه از ایمنی مناسبی برخوردار و اطلاعات آن قابل اتکا باشد. با توجه به اهمیت روزافزون امنیت در سامانه‌های اطلاعاتی به‌هنگام پردازش اطلاعات، موضوع امنیت در سامانه‌های اطلاعاتی و ایجاد آن در سازمان‌ها، جایگاه ویژه‌ای را در بین مدیران به‌وجود آورده است (ودیعی و همکاران، ۱۳۸۹: ۹۰).

امنیت در سازمان‌ها یکی از مسائل بسیار مهم است. افراد درون‌سازمانی یا برون‌سازمانی به اطلاعات ارائه‌شده از سوی سیستمی که امنیت کافی ندارد، اعتماد و اعتنای چندانی نمی‌کنند. از طرف دیگر، فرصت جعل و دست‌کاری و تقلب در سیستمی که امنیت کافی ندارد، افزایش می‌یابد. اهمیت و میزان اتکاپذیری اطلاعات مالی برای تصمیم‌گیری گروه‌های ذی‌نفع در دنیای امروز برای همگان روشن است. امروزه به‌جرئت می‌توان گفت که هر تصمیم مدیریتی آثار و نتایج مالی در پی دارد؛ به همین دلیل، مدیریت برای هر تصمیم‌گیری به اطلاعات مالی قابل اتکا نیازمند است (میرمجریان و همکاران، ۱۳۸۵: ۳۷).

اطلاعات یکی از دارایی‌های مهم هر سازمان محسوب می‌شود و به‌دلیل ارزش زیاد و حیاتی آن برای هر سازمان، باید از آن به‌خوبی محافظت شود. این اهمیت تا جایی است که عده‌ای آن را به خونی در رگ‌های سازمان تشبیه کرده و آن را عامل حیات‌بخش سازمان می‌دانند که با به‌خطرافتادن آن، سازمان می‌میرد (مسکل[1] و همکاران، ۲۰۱۵: ۱۰۹۶-۱۰۹۱).

آگاهی از امنیت اطلاعات در افراد منجر به ایجاد تغییر رفتار و تقویت فعالیت‌های مناسب امنیتی می‌شود و به افراد اجازه می‌دهد تا نسبت به امنیت فناوری اطلاعات نگران و پاسخگو باشند. این مسئله به‌تدریج به فرهنگ سازمان‌ها تبدیل خواهد شد (نیکرک و وان،[2] ۲۰۱۷: ۱۴۴-۱۴۲). موضوع امنیت در سیستم‌های اطلاعاتی مسئلهٔ عمومی است و به‌دلیل کاربرد وسیع سیستم‌های اطلاعاتی و کاربردی سازمان، مقولهٔ امنیت در این سیستم‌ها اهمیت زیادی دارد و حیات سازمان‌ها ارتباط نزدیکی با سیستم‌های اطلاعاتی آن‌ها دارد (زنجیرچی و همکاران، ۱۳۹۳: ۲۱۲-۱۹۵).

گزارش‌های منابع مختلف دربارهٔ اقدام عمدی و غیرعمدی کارکنان سازمان‌ها در ارتباط با ایجاد

1.Meskell
2.Nikrerk & Van

خطرات امنیت اطلاعات، نشان از لزوم توجه به این نکات دارد. کاربرانی که ممکن است دربارهٔ خطرهای امنیتی آموزش لازم را ندیده باشند، به‌آسانی فریب خورده و کدهای مخرب را به اجرا درمی‌آورند. با توجه به اهمیت عوامل انسانی در سامانه‌های اطلاعات و امنیت، نیاز به انجام پژوهشی گسترده و جامع در این زمینه محسوس است. از طرفی، موضوع امنیت فرایندی است که به‌صورت مستمر در سازمان جاری است و به‌شکل محصول نیست که بتوان آن را سفارشی‌سازی نمود. بر این اساس، به‌نظر می‌رسد توجه به موضوع عوامل انسانی به‌عنوان یکی از ابعاد مهم در ارتقای سطح امنیتی اطلاعات ازجمله مؤلفه‌هایی است که توجهی خاص می‌طلبد. توجه به این موضوع از دیدگاه‌های مختلف، آثار خوبی بر توسعهٔ امنیت اطلاعات دارد. بنابراین، مسئلهٔ اصلی این پژوهش، شناسایی مؤلفه‌ها و شاخص‌های سرمایهٔ انسانی مؤثر بر امنیت اطلاعات سازمان است.

انجام این پژوهش از این ابعاد حائز اهمیت است: توجه مدیران حوزهٔ امنیت اطلاعات به مؤلفهٔ منابع انسانی به‌عنوان بخش اساسی در حفظ و توسعهٔ امنیت اطلاعات؛ جلوگیری از هدررَفت سرمایه‌های اطلاعاتی؛ ارتقای قدرت تصمیم‌سازی و تصمیم‌گیری مدیران در حوزهٔ امنیت اطلاعات. گفتنی است که بی‌توجهی به اجرای چنین پژوهش‌هایی، کاهش امنیت در سازمان‌ها و به‌خصوص نهادهای مرتبط با سرمایه‌های اطلاعاتی را به‌همراه دارد که به‌عنوان ضرورت انجام این تحقیق در نظر گرفته می‌شود.

هدف اصلی این پژوهش تعیین مؤلفه‌ها و شاخص‌هایی است که ارتباط بین عامل انسان و امنیت اطلاعات در سازمان‌ها را ارائه نماید. در این راستا، اهداف فرعی در این خصوص عبارت‌اند از: شناسایی مؤلفه‌ها و شاخص‌ها در حوزهٔ منابع انسانی و همچنین ارتباط آن‌ها با یکدیگر که پژوهش حاضر بر این اساس انجام شده است.

مبانی نظری

پیشینه پژوهش

خیرگو و شکوهی (۱۳۹۵) در پژوهشی با عنوان «شناسایی و رتبه‌بندی عوامل کلیدی مؤثر بر اثربخشی سامانه‌های اطلاعاتی» معتقدند در عصر حاضر سامانه‌های اطلاعاتی ازجمله عوامل تأثیرگذار در دستیابی به مزیت رقابتی برای سازمان‌ها محسوب می‌شوند و کیفیت خروجی این سامانه‌ها نقش مهمی در بهبود عملکرد سازمان دارد. نتایج پژوهش آن‌ها نشان می‌دهد تأثیر عوامل

سازمانی و انسانی و فنی بر اثربخشی سامانه‌های اطلاعاتی، چشمگیر است و از بین شاخص‌های مؤثر بر اثربخشی سامانه‌های اطلاعاتی حمایت مدیریت ارشد، امنیت، پذیرش و مدیریت دانش فناوری اطلاعات و سامانه‌های اطلاعاتی به‌ترتیب رتبه‌های نخست را به خود اختصاص داده‌اند (خیرگو، ۱۳۹۵: ۳۹-۱۷).

سیف و نادری بنی (۱۳۹۶) به شناسایی مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قارهٔ ایران پرداختند. بر اساس نتایج پژوهش آن‌ها، مؤلفه‌های مرتبط با مسائل فنی، انسانی، مدیریت و رهبری و نیز، مالی و اقتصادی مؤثر بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قاره ایران مشخص شدند (سیف و نادری بنی، ۱۳۹۶: ۸۷۰-۸۵۱).

کیم[1] و همکاران (۲۰۱۴) طی پژوهشی با عنوان «یک مدل یکپارچهٔ رفتاری برای پیروی از سیاست‌های امنیت اطلاعات» عواملی را بررسی کرده‌اند که بر پیروی کارکنان سازمان از سیاست‌های امنیت اطلاعات مؤثر است. در این پژوهش تأثیر عواملی مانند خود کارآمدی، نگرش، باورهای اصولی و باورها دربارهٔ هزینه‌های پیروی بر تمایل به پیروی از سیاست‌های سیستم‌های امنیت اطلاعات بررسی شده است (کیم و همکاران، ۲۰۱۴: ۱۹-۱۷).

ورما و دوما[2] (۲۰۰۸) در جستاری با عنوان «ارزش‌گذاری منابع انسانی با تمرکز بر اهمیت ارزش‌گذاری منابع انسانی» رویکردهای جاری اندازه‌گیری و پیشرفت‌های مورد انتظار در این زمینه را بررسی کردند. نتایج پژوهش آنان نشان داد که عمده شرکت‌ها این مدل‌ها را درک کرده و لحاظ‌کردن ارزش منابع انسانی را در تصمیم‌ها، حیاتی دانسته‌اند؛ اما پیشرفت عمده‌ای در این زمینه از دانش مورد انتظار نیست (ورما و همکاران، ۲۰۰۸: ۱۲۳-۱۰۲).

هوبر[3] (۲۰۱۸) در پژوهش‌های خود به این نتیجه رسید که فناوری اطلاعات سبب تغییر فرایندهای سازمان می‌شود. این تغییرات عبارت‌اند از: مکانیزه‌شدن و افزایش سرعت فرایندها؛ ایجاد مشاغل مجازی و همکاری‌های از راه دور؛ افزایش تعاملات و بازخورد فوری؛ ایجاد توزیع و مدیریت مؤثر و هوشمندانهٔ دانش؛ اشتراک‌گذاری اطلاعات در سطوح مختلف (هوبر، ۲۰۱۸: ۸۷-۷۱).

ملیسا والتر[4] (۲۰۰۷) بیان می‌کند که تخصص در سامانه‌های اطلاعاتی و حمایت فناورانه از آن‌ها

1.Kim
2. Verma & Dewe
3. Huber
4.Melissa walters

منجر به اصل صلاحیت برای حرفهٔ حسابداری می‌شود؛ اما متأسفانه برنامه‌های آموزشی تجاری بدنهٔ اصلی امنیت سامانه‌های اطلاعاتی را شامل نمی‌شود که برای برطرف‌کردن آن، مؤلفه‌های زیر را پیشنهاد می‌کند:

ـ فراهم‌آوردن زمینه‌ها برای مشخص‌کردن اهمیت مکان‌یابی امنیت سامانه‌های اطلاعاتی به‌عنوان بخشی از یک آموزش حسابداری؛

ـ فراهم‌آوردن تعدادی راهنمای علمی و کاربردی برای مدرسان سامانه‌های اطلاعاتی حسابداری که تمایل به توسعه و عرضهٔ امنیت سامانه‌های اطلاعاتی دارند (والتر، ۲۰۰۷: ۳۴-۵).

کریتزینگر و اسمیت[1] (۲۰۱۱) پژوهشی با عنوان «مدل بازیابی و آگاهی امنیت اطلاعات (ISRA)» ارائه کردند. این مدل برای ارتقای آگاهی از امنیت اطلاعات در میان کارکنان، استفاده می‌شود. اساس این مدل بر مبنای بدنهٔ مشترک دانش، پیشنهاد شده است که برای امنیت اطلاعات مناسب به‌نظر می‌رسد. این بدنهٔ مشترک از دانش، تضمین می‌کند که مسائل فنی امنیت اطلاعات، مسائل غیر فنی امنیت اطلاعات را که مرتبط با انسان است، تحت‌الشعاع قرار نمی‌دهد (کریتزینگر و همکاران، ۲۰۱۱: ۲۰-۱۸).

ادبیات و مبانی نظری پژوهش

مدل: به‌طور کلی مدل یا الگو، طرحی است که از واقعیت گرفته شده و روابط بین عوامل اصلی را نشان می‌دهد. از مدل می‌توان برای پیش‌بینی و تصمیم‌گیری استفاده کرد. همواره می‌شود مدلی از سامانهٔ مد نظر ایجاد کرد و سپس به کمک آن نتایجی را بررسی دقیق کرد که از تصمیم‌های گوناگون در سامانه حاصل می‌شود. یکی از هدف‌های مدل‌سازی، ساده‌کردن و نشان‌دادن اجزا و عناصر اصلی و مورد نیاز یک سیستم است. گاهی در الگو، عوامل اضافی و مُخل، به‌عمد نادیده گرفته می‌شوند تا مدلی به‌دست آید که ضمن نشان‌دادن اجزای اصلی و ارتباط بین آن‌ها، به‌اندازهٔ کافی ساده و روشن باشد. انواع مختلف مدل‌ها عبارت‌اند از: کلامی، ترسیمی، تجسمی و ریاضی که هر یک دارای درجه دقت خاصی هستند و در زمینهٔ ویژه‌ای کارایی دارند (الوانی و میرشفیعی، ۱۳۶۹: ۳).

مدل از ریشه لاتینی MODUS به معنای اندازه گرفته شده است. مدل همچنین به ما کمک می‌کند که به متن و درون پدیده‌هایی هدایت شویم که نمی‌توانیم مستقیماً آن‌ها را ببینیم. مدل جزئی کوچک یا بازسازی کوچکی از شیء بزرگ است که از لحاظ کارکرد با شیء واقعی یکسان است (گرجی و همکاران، ۱۳۸۸: ۳۳).

1. Kritzinger and Smith

مؤلفه: مفروضاتی است که ممکن است یک یا چند بُعد داشته باشد. برای مثال، می‌شود علل پیشرفت تحصیلی را از نظر فردی، اجتماعی، فرهنگی و... بررسی کرد که هر کدام از این‌ها به عناصر کوچک‌تر تبدیل می‌شود تا قابل اندازه‌گیری و بررسی گردند. سپس بر اساس این ابعاد و مؤلفه‌ها می‌شود چارچوب مفهومی و مدل طراحی کرد.

شاخص: مفاهیم برای کاربردی‌بودن باید شاخص‌های تجربی داشته باشند. مفاهیم ابزارهایی هستند که برای فهم سریع مسائل به‌کار می‌آیند. آن‌ها چکیده‌هایی انتزاعی از مجموعه‌ای کلی از رفتارها، نگرش‌ها و ویژگی‌هایی هستند که چیزی مشترک دارند. مفهوم‌سازی، ساختن مفهومی انتزاعی برای فهمیدن امر واقعی است. لذا در مفهوم‌سازی به همهٔ جنبه‌های واقعیت مد نظر توجه نشده، بلکه فقط جنبه‌هایی برگرفته می‌شود که از نظر محقق اصلی است. ساختن یک مفهوم در گام اول عبارت از تعیین ابعادی است که آن را تشکیل می‌دهد و امر واقعی را منعکس می‌کند. گام بعدی، مشخص‌کردن مؤلفه‌ها و شاخص‌هاست که به‌کمک آن‌ها بتوان ابعاد مفهوم را اندازه‌گیری کرد. شاخص‌ها نشانه‌های عینی قابل شناسایی و قابل اندازه‌گیری ابعاد مفهوم هستند. گاهی مفاهیمی هست که شاخص‌هایشان تا این اندازه بدیهی نیستند. در این‌گونه موارد مفهوم شاخص با ابهام بیشتری توأم است. اینجا شاخص ممکن است یک نشانه، دلالت، جمله، عقیدهٔ ابرازشده یا هر پدیده‌ای باشد که اطلاعاتی دربارهٔ موضوع مفهوم‌سازی به ما می‌دهد (خاکی، ۱۳۷۸: ۹۳-۹۱).

سرمایه انسانی: عبارت است از همهٔ مهارت‌ها و ظرفیت‌ها و توانایی‌هایی که افراد مالک آن‌ها هستند و باعث کسب درآمدشان می‌شود. برای قلمدادکردن انسان به‌عنوان یک تولیدکننده، برخی روش‌ها برای اندازه‌گیری و کمّی‌کردن توانایی‌های انسان مورد نیاز است. ایدهٔ سرمایهٔ انسانی به‌عنوان یک معیار در ارزیابی‌های اقتصادی تعریف می‌شود. سرمایهٔ انسانی مانند کالاها و خدمات تولیدی ارزش‌گذاری می‌شود. وقتی مصرف، هدف نهایی سامانهٔ اقتصادی باشد، ارزش سرمایهٔ انسانی افراد مانند ارزش مصرف کالاها و خدماتی است که افراد به‌طور مستقیم یا غیر مستقیم تولید می‌کنند. وقتی ارزش کالاها و خدمات کاهش می‌یابد، ارزش سرمایهٔ انسانی نیز کم می‌شود (فولادی و همکاران، ۱۳۹۴: ۳).

سازمان: عبارت است از مجموعه‌ای از افراد که برای تحقق اهدافی معین همکاری می‌کنند. در همهٔ سازمان‌ها از انسان‌ها استفاده می‌شود و همهٔ آن‌ها هدفمند بوده و از تقسیم کار بهره می‌گیرند (رضائیان، ۱۳۸۵: ۲۵).

امنیت: واژهٔ امنیت در کاربرد عام به‌معنای رهایی از مخاطرات مختلف است: «شرایطی که در آن فرد در معرض خطر نبوده و یا از خطر محافظت شود؛ ایمنی، رهایی از غم و غصه و تشویش و اضطراب، نبود خطر و یا احساس ایمنی و دوری از آن» است (کینگ و موری،[1] ۲۰۰۱: ۷۸۳). در این چارچوب، امنیت دربردارندهٔ احساس اطمینان از دو بُعد ذهنی و عینی است. بعد ذهنی شامل امنیت فکری، رهایی از ترس، آزادی بیان، امنیت شغلی، امید به زندگی و... است و بُعد عینی غذا، بهداشت، محیط‌زیست، کاهش فساد، مقابله با قاچاق انسان و کالا و... را شامل می‌شود. عناصر اساسی امنیت عبارت‌اند از: ۱. محرمانه‌بودن؛ ۲. صحت و استحکام؛ ۳. دردسترس‌بودن. در لغت، امنیت به‌معنی رهایی از خطر، وجود ایمنی، رهایی از ترس یا نگرانی است.

امنیت اطلاعات: با توجه به اهمیت نقش و جایگاه امنیت اطلاعات برای مقابله با تهدیدهای مختلف و پیشرفته، سازمان‌ها و به‌خصوص مدیران ارشد و تصمیم‌گیرندگان آن با چالش‌های جدی درخصوص امنیت اطلاعات روبه‌رو هستند. یکی از این چالش‌ها و سردرگمی‌ها انتخاب راه‌حل‌های امنیتی برای سازمان خودشان است. برای خروج از این سردرگمی‌ها، سازمان‌ها ابتدا باید اجزایی را که تهدید می‌شوند و همچنین نیازها و اصول امنیتی را بشناسند و به این سؤال کلیدی پاسخ دهند: «چه اجزایی از سازمان باید امن شوند؟»

به‌عنوان مثال، سازمانی از یک درگاه اداری برای ارتباط و انجام مأموریت بخش‌های پراکندهٔ خود در جغرافیای یک کشور استفاده می‌کند. مدیران سازمانی با این مشکل روبه‌رو هستند که چه اجزایی از سامانه‌های اجرایی و اطلاعاتی، تجهیزات ارتباطی و زیرساخت‌های خود را امن نمایند. به عبارت دیگر، آیا فقط امنیتِ زیرساخت کافی است؟ آیا توجه به امنیت نیروی انسانی نیاز است؟ آیا نیاز سازمان در استفاده از تجهیزات امنیتی است؟ و سؤال‌های دیگری که ممکن است مدیران با آن مواجه شوند. واژهٔ امنیت اطلاعات به معنی حفاظت از اطلاعات و سامانه‌های اطلاعاتی در مقابل دستیابی و استفادهٔ غیر مجاز از آن است. چوی بانک (۱۹۹۲) امنیت اطلاعات یک سامانه را چنین تعریف می‌کند: «میزان اطمینان از اینکه تنها داده‌های مجاز و قانونی به یک سامانه وارد یا از آن خارج می‌شوند، بدون اینکه اضافات و حذف‌ها، اصلاحات یا برگردان‌های غیر مجاز یا غیر قانونی در زمان بین ورود و دریافت مورد نظر اتفاق بیفتد.»

1.King & Murray

مارو (۱۹۹۵)امنیت اطلاعات را «حفاظت از اختلال غیر مجاز، تغییر غیر مجاز، افشاسازی، یا سوءاستفاده از اطلاعات و منابع اطلاعاتی، خواه تصادفی یا عمدی» تعریف می‌کند (دیلی و همکاران،[1] ۲۰۰۰: ۶۲).

تهدیدهای امنیتی سامانه‌های اطلاعاتی: در واقع، تهدید امنیتی هر رخدادی است که سازمان قصد ندارد آن عمل صورت بپذیرد یا عملکرد معمول سامانه را دچار مخاطره نموده است. برخی از تهدیدهای امنیتی به این شرح هستند:

ویروس‌های رایانه‌ای: با توجه به استفادهٔ کارکنان سازمان‌ها از رایانه‌های شخصی یا حتی شبکه، امکان گسترش ویروس‌ها در سامانه بسیار سریع خواهد بود. بدین‌سان با واردشدن ویروس به رایانهٔ عضو شبکه به‌راحتی سایر رایانه‌های غیر عضو نیز آلوده می‌شوند.

دسترسی‌های غیر مجاز: دستیابی افراد غیر مجاز و رعایت‌نشدن سطح دسترسی کارکنان سازمان و امکان پخش و افشای اطلاعات از سوی آن‌ها، امنیت اطلاعات سامانه را به مخاطره می‌اندازد.

وضع‌نشدن سیاست‌های مدیریتی شبکه: گاه در سازمان‌ها از سامانه‌های کنترل دسترسی یا حتی در مواقعی از رمز عبور استفاده نمی‌شود؛ لذا هر فردی می‌تواند به‌راحتی به‌صورت غیر مجاز به اطلاعات دستیابی داشته باشد. بدین منظور، هر سازمان بنا به اهداف خود باید سیاست‌های مناسبی نیز در مدیریت شبکه و محافظت از اطلاعات وضع نماید.

سهل‌انگاری و اقدامات غیر عمدی کاربران: گاهی کارکنان با سهل‌انگاری، منجر به بروز تهدیدهای امنیتی برای سامانه‌های اطلاعاتی می‌شوند. در واقع، بزرگ‌ترین تهدید اطلاعاتی و بیشترین مشکلات امنیتی ناشی از اشتباه‌ها و خطاهای اعضای سازمان است.

جرائم سازمان‌یافته: اقداماتی مانند رخنه‌کردن به شبکه یا سامانه که ناشی از دسترسی غیر مجاز است، تهدید دیگری برای سامانه‌های اطلاعاتی است. با توجه به این موارد، کنترل و امنیت سامانه‌های اطلاعاتی از اهمیت بسیاری برخوردار است (دیویس،[2] ۱۹۹۷: ۳۴-۲۸).

آموزش کارکنان: آموزش بسیار فراتر از یک فعالیت مصرفی است؛ به این مفهوم که رفتن به مدرسه فقط به‌منظور ارضا یا مطلوبیت شخصی نیست. بلکه برعکس، هزینه‌های شخصی و عمومی تحصیلات به‌منظور بروز و پرورش ذخایر مولدی مصرف می‌شود که در انسان نهفته است؛ زیرا به‌کارگیری این ذخایر مولد، در آینده خدمات جدیدی را در اختیار جامعه قرار می‌دهد. این خدمات،

1.Daily
2.Davis

در آینده به‌شکل درآمد و توانایی برای خلق خدمات مختلف و ارضای نیازی مصرفی ظهور می‌یابد.

برخی آثار جدید نشان‌دهندهٔ اهمیت آموزش است که فقدان آموزش نیروی کار به حس رقابت کم مرتبط می‌شود. در عوض، بازار سرمایهٔ انسانی بیشتر با حقوق گزاف و تولید بیشتر مرتبط است. همچنین، آموزش با طول عمر سازمان در ارتباط است. گرایش بیشتر به تجارت و رشد اقتصادی متذکر شده است که سرمایهٔ بشری به‌عنوان یک منبع، نه‌تنها کارگران را انگیزه می‌دهد و مسئولیت‌پذیری‌شان را تقویت می‌کند، بلکه برای ایجاد مخارج تحقیق و توسعه، راه را برای نسل جدید دانش در اقتصاد و جامعهٔ عادی نیز هموار می‌سازد. این امر برای تجارت‌های کوچک نیز داراییِ باارزشی است که به‌صورت مثبت، مرتبط با عملکرد تجاری است. در آخر آنکه سرمایه‌گذاری در آموزش، هم برای افراد و هم برای جامعه خوشایند است (ماریموت و همکاران،[1] ۲۰۱۱: ۲۶۸).

مفهوم سرمایهٔ انسانی از توسعهٔ علمی‌اقتصادی ریشه گرفته است. به گفتهٔ کوچارسیکو[2] (۲۰۱۱)، اقتصاددانان در جستجوی برجسته‌کردن و به‌تصویرکشیدن توجه به توانایی کارگران برای کارکردن با ماشین‌ها و نیز طراحی برای قادرساختن انسان از عهدهٔ کار سخت برآمدن در جهان است. با این رویکرد، قطعاً به افرادی با مهارت و توانایی و دانشی افزایش‌یافته در راستای پیشرفت و توسعهٔ جهان و جامعه نیاز است (لایر و همکاران،[3] ۲۰۱۴: ۵۶).

تجربهٔ کارکنان: تجربهٔ کارکنان مجموع برداشت‌های آن‌ها در تعامل با سازمان است. جزء اصلی تجربه احساسات و عواطف است که در طول تجربه برانگیخته می‌شود. تجربهٔ کارکنان، شناخت و دیدگاه آن‌ها درخصوص شغل را شکل می‌دهد و به رفتارهای مطلوب و نامطلوب آن‌ها منجر می‌شود. یک تجربهٔ مثبت فقط فاکتوری نیست که سازمان‌ها برای کارکنان ایجاد کنند، بلکه نتیجهٔ ادراکات کارکنان از آن تجارب است و اینکه آیا انتظاراتشان را محقق می‌کند یا خیر.

در مدیریت تجربهٔ کارکنان، سازمان‌ها به دنبال طراحی برنامه‌هایی هستند که با خلق تجربیات عالی برای کارکنان، تعلق سازمانی و به‌دنبال آن نتایج درخشان سازمانی را رقم بزنند؛ زیرا کارکنانی با اشتیاق کامل، همواره ذهن، دست، قلب و روح خود را در سازمان سرمایه‌گذاری می‌کنند (جلالی، ۱۳۹۷: ۱).

عوامل انسانی و امنیت اطلاعات: تهدیدهای امنیتی‌انسانی تهدیدهایی هستند که از اعمال انسانی سرچشمه می‌گیرند و ممکن است غیر عمدی یا عمدی باشند. خطاهای انسان ممکن است در

1.Marimuthu
2.Kucharcikova
3.Iyere

قالب خطاهای ناشی از غفلت و سهل‌انگاری یا جرائم واقع شوند. خطای نوع اول وقتی رخ می‌دهد که فردی در انجام عملِ درست، ناتوان باشد و خطای نوع دوم زمانی اتفاق می‌افتد که فرد عملی را انجام دهد که نادرست بوده یا انجام آن ممنوع شده است. از سوی دیگر، تهدیدهای غیر انسانی عموماً به تهدیدهای فنی از قبیل نقص فنی سامانه یا سخت‌افزار یا مشکلات نرم‌افزاری سامانه مربوط می‌شود یا ناشی از بلایای طبیعی، از قبیل سیل و زلزله است. البته برخی از تهدیدهای فنی ممکن است با اعمال انسانی در ارتباط باشد، از قبیل واردکردن یک ویروس به سامانه از طریق نرم‌افزار آلوده.

حسابداران به چند روش می‌توانند در برقراری امنیت سامانه‌های حسابداری سهیم باشند. با توجه به اینکه سامانه‌های رایانه‌ای مالی و نرم‌افزارهای حسابداری بر اساس نیاز حسابداران طراحی و ساخته می‌شوند، حسابداران می‌توانند با کمک و همکاری با طراحان نرم‌افزار، زمینهٔ کنترل‌های داخلی و روش‌های امنیت اطلاعاتی را فراهم نمایند (ای هان،[1] ۲۰۰۱: ۳۶۳).

ولد[2] (۲۰۰۴) در قسمتی از پژوهش خود به واقعه‌ای تاریخی اشاره می‌کند: «در اواخر سال ۱۲۰۰ میلادی کوبلای‌خان و ایل‌وتبار مغولی او سعی در عبور از دیوار چین داشتند؛ اما دیوار بسیار محکم و عمیق و طولانی بود. عاقبت به‌صورت آرام و ساکت، با تطمیع دروازه‌بان، ترتیبی اتخاذ کردند تا با پیروزی بر آن موانع توانستند بخش بزرگی از کشور چین را فتح کنند.» مفهوم این گفته این است که مهم نیست کنترل‌های فنی چقدر قوی باشند، بلکه امنیت همیشه به افراد داخل سازمان بستگی دارد. همچنین در کتاب راهنمای امنیت اطلاعات آمده است که بسیاری از پژوهش‌ها نشان می‌دهند بیش از ۸۰ درصد مشکلات امنیتی پیش‌آمده در سازمان‌ها ناشی از خطاهای سهوی و عمدی کارکنان بوده است (سادوسکی[3] و همکاران، ۲۰۰۳: ۹۸).

روش‌شناسی تحقیق

پژوهش حاضر به‌لحاظ هدف، کاربردی است و به روش توصیفی‌پیمایشی انجام شده است. در آغاز با استفاده از مطالعات کتابخانه‌ای و اکتشافی به بررسی مبانی نظری موضوع و سپس به شناسایی مؤلفه‌ها و شاخص‌های مربوط پرداخته شده است. پس از استفاده از منابع مختلف، از پرسشنامه نیز برای کسب اطلاعات و دانش ضمنی متخصصان در این حوزه استفاده شده است. مقیاس اندازه‌گیری نگرش پاسخ‌دهندگان در

1.lhan. D
2.vold
3.Sadowsky

پرسشنامه طیف لیکرت است. در این پرسشنامه هفت سطح متفاوت با هفت عبارت مشخص شده‌اند که رتبهٔ آن‌ها به‌ترتیب از یک تا هفت در نظر گرفته شده است. فرضیه‌ها با توجه به شاخص‌های به‌دست‌آمده از ادبیات تحقیق و نظریات استادان دانشگاهی، برای سنجش متغیرها طراحی شده است.

در این پژوهش برای تعیین پایایی پرسشنامه با استفاده از نرم‌افزار SPSS مقدار ضریب آلفای کرونباخ برابر ۰,۹۳۲ تعیین شد که چون بزرگ‌تر از ۰/۷۵ است، نشان می‌دهد که پرسشنامه از اعتبار کافی بهره‌مند است. جامعهٔ آماری این پژوهش ۳۵۰ نفر از خبرگان نظری و تجربی حوزهٔ مدیریت منابع انسانی و مالی سازمان‌ها با تأکید بر شهر تهران هستند. برای نمونه‌گیری، از روش نمونه‌گیری تصادفی انتخاب شده و تعداد ۱۰۰ پرسشنامه بین آن‌ها توزیع و سپس جمع‌آوری شده است. از این تعداد، ۸۰ پرسشنامهٔ تکمیل‌شده جمع‌آوری شد که داده‌های آن‌ها تجزیه و تحلیل شد.

در این پژوهش، فنون تحلیل آماری در دو قسمت استفاده شده است:

۱. بررسی نظرات خبرگان دربارهٔ وجود هر یک از متغیرهای پژوهش در سازمان؛

۲. بررسی و آزمون فرضیه‌های تحقیق.

به‌منظور تجزیه و تحلیل نظرات افراد، از آزمون دوجمله‌ای استفاده شده است که در آن موفقیت (P) به‌معنای تأیید آن عامل از سوی خبره و شکست (Q) به‌معنای ردِّ آن است؛ بنابراین با توجه به این شرایط به بررسی وضعیت رد یا تأییدشدن متغیرها (سازه‌ها) پرداخته شد.

با توجه به اینکه هدف این پژوهش، تعیین مؤلفه‌ها و شاخص‌های سرمایهٔ انسانی مؤثر بر امنیت اطلاعات سازمان‌هاست و در آن تأثیر تعاملی چند متغیر بر روی یکدیگر بررسی می‌شود، از نرم‌افزار LISREL استفاده شده است.

فرضیه تحقیق

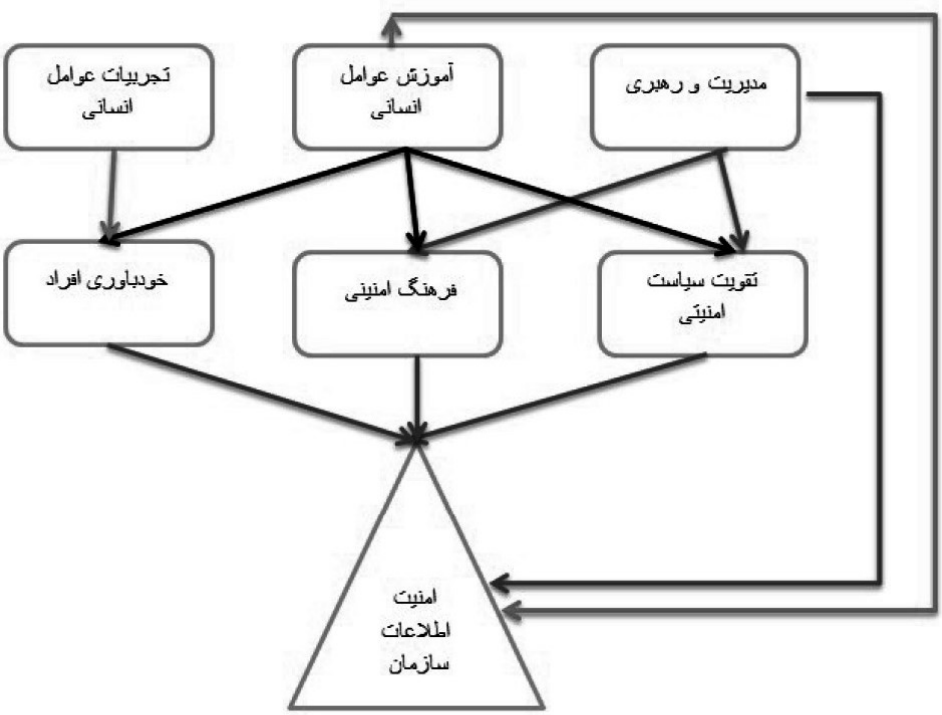
در راستای انجام این پژوهش، این فرضیه بر اساس بررسی منابع مرتبط ارائه شد: «مؤلفه‌های شش‌گانهٔ سرمایهٔ انسانی شامل مدیریت و رهبری، آموزش عوامل انسانی، تجربیات عوامل انسانی، فرهنگ امنیتی، تقویت سیاست‌های امنیتی، خودباوری افراد و شخص‌های مرتبط با هر یک از مؤلفه‌ها، بر امنیت اطلاعات سازمان‌ها مؤثر است.»

یافته‌های تحقیق

با توجه به بررسی مبانی نظری و پیشینهٔ پژوهش، مؤلفه‌های اساسی که در این پژوهش بررسی شده‌اند، عبارت‌اند از: مدیریت و رهبری، آموزش عوامل انسانی، تجربهٔ عوامل انسانی، فرهنگ امنیتی، تقویت سیاست‌های امنیتی، خودباوری افراد. شاخص‌های مربوط به هر یک از مؤلفه‌های ذکرشده در جدول ۱ ارائه شده است.

ردیف	مؤلفه	شاخص‌ها
۱	مدیریت و رهبری	درگیرشدن مدیر در فعالیت‌های امنیت سامانه‌های اطلاعاتی (ISS) توافق شخصی بر خط‌مشی‌ها اولویت‌دادن به امنیت سامانه‌های اطلاعاتی (ISS)
۲	آموزش عوامل انسانی	برنامه‌های آموزش امنیتی ابزارهای آموزشی
۳	تجربه‌های عوامل انسانی	تخصص افراد توانایی‌های رایانه‌ای زمان درگیربودن در مباحث امنیتی
۴	فرهنگ امنیتی	نگرش سنت‌ها ارزش‌ها
۵	تقویت سیاست‌های امنیتی	به‌روزبودن بازنگری‌کردن تعهد مدیریتی همسویی با اهداف سازمان
۶	خودباوری افراد	تجربه‌ها آموزش قضاوت‌های شخصی

جدول ۱: مؤلفه‌ها و شاخص‌های سرمایهٔ انسانی مؤثر بر امنیت اطلاعات سازمان‌ها



شکل ۱: مؤلفه‌ها و شاخص‌های مؤثر بر امنیت اطلاعات سازمان‌ها

تجزیه و تحلیل یافته‌ها

خلاصه نظرات خبرگان دربارهٔ وجود یا نبودِ هر یک از متغیرها به‌همراه نتایج آزمون حاصل از به‌کارگیری نرم‌افزار آماری SPSS به شرح جدول شمارهٔ ۲ است.

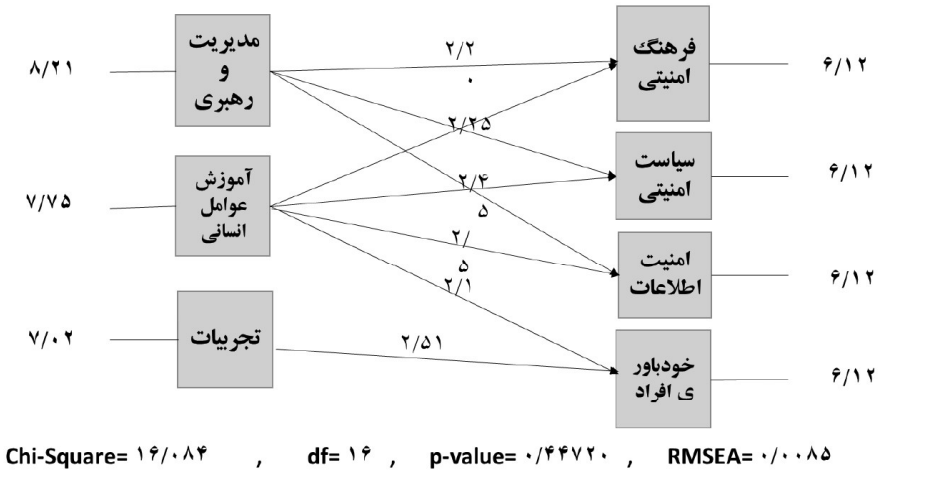
متغیرهای پژوهش	طبقه	فراوانی	درصد	نسبت آزمون	سطح معناداری
مدیریت و رهبری آموزش کاربر	≤۴	۲۰	۰/۲۵	۰/۵۰	۰/۰۰۰
	>۴	۶۰	۰/۷۵		
	≤۴	۲۰	۰/۲۵	۰/۵۰	۰/۰۰۰
	>۴	۶۰	۰/۷۵		
فرهنگ امنیتی	≤۴	۲۳	۰/۲۹	۰/۵۰	۰/۰۰۰
	>۴	۵۷	۰/۷۱		

تقویت سیاست امنیتی امنیت اطلاعات	≤ ۴ >۴	۲۵ ۵۵	۰/۳۱ ۰/۶۹	۰/۵۰	۰/۰۰۱
	≤ ۴ >۴	۲۹ ۵۱	۰/۳۶ ۰/۶۴	۰/۵۰	۰/۰۳۲
تجربیات افراد خودباوری افراد	≤ ۴ >۴	۲۶ ۵۴	۰/۳۳ ۰/۶۸	۰/۵۰	۰/۰۰۲
	≤ ۴ >۴	۲۶ ۵۴	۰/۳۳ ۰/۶۸	۰/۵۰	۰/۰۰۲

جدول ۲: نتایج آزمون دوجمله‌ای درباره نقش هر یک از عوامل در امنیت اطلاعات سازمان‌ها

همان‌طور که در جدول ۲ ملاحظه می‌شود، از دیدگاه خبرگان مشارکت‌کننده در این پژوهش، مدیریت و رهبری، آموزش عوامل انسانی، تجربهٔ عوامل انسانی، فرهنگ امنیتی، تقویت سیاست امنیتی و خودباوری افراد، در امنیت اطلاعات سازمان‌ها نقش دارند.

در ادامه برای آزمون تک‌تک فرضیه‌ها از نرم‌افزار LISREL استفاده شد. نتایج انجام این آزمون همراه با مقادیر T-VALUE روابط، در نمودار ۲ نشان داده شده است.



شکل ۲: نتایج حاصل از اجرای اولیه مدل توسط نرم‌افزار LISREL

همان‌طور که در این نمودار مشاهده می‌شود، مقدارِ T ضریبِ مسیر مربوط به رابطهٔ تمامی متغیرها، از ۲ بیشتر است؛ لذا فرضیه‌های مربوطه در این پژوهش تأیید می‌شوند.

این‌بار مجموعه روابط متغیرها و کل مدل با استفاده از نرم‌افزار لیزرل به آزمون گذاشته شد تا معناداری مدل در کل بررسی شود. در لیزرل خوبی برازش مدل از طریق یکسری شاخص‌ها از جمله مقدار مربع کای، شاخص خوبی برازش (GFI)، شاخص خوبی برازش اصلاح‌شده(AGFI)، ارزش P (P-VALUE)، ریشهٔ میانگین مجذورات مانده و ریشهٔ خطای مربع میانگین سنجیده شده است. در این پژوهش، آزمون کای دو مجموعه روابط علّی فوق با ۲۸ درجه آزادی برابر ۲۲۹,۲۵ است و این نشان می‌دهد که در سطح ۹۵ ٪ روابط فوق معنادار است. همچنین مقدار GFI برابر ۰/۹۵ و مقدار AGFI برابر ۰/۸۳ است که چون مقدار هر دوی آن‌ها بیشتر از ۰/۸۰ و نزدیک یک است؛ نشان از برازش خیلی خوب مدل دارد. مقدار خطا (RMSEA) نیز برابر ۰/۰۲۵ است.

ردیف	شاخص	مقدار
۱	ریشه میانگین مجذورات مانده	۰/۵۸
۲	ریشه میانگین مجذورات مانده استاندارد	۰/۰۷۳
۳	شاخص خوبی برازش	۰/۹۵
٤	شاخص خوبی برازش اصلاح‌شده	۰/۸۳
٥	شاخص خوبی برازش پارسیمونی	۰/۲٦

بنابراین در کل می‌شود گفت که برازش مدل خیلی خوب است و مجموعه‌ای از متغیرهای «مدیریت و رهبری»، «آموزش کارکنان»، «فرهنگ امنیتی»، «تقویت سیاست‌های امنیتی»، «تجربیات افراد» و «خودباوری افراد» به بهبود و بهینه‌شدن «امنیت اطلاعات سازمان‌ها» می‌انجامد.

نتیجه‌گیری

نتایج بررسی فرضیه پژوهش

نتایج حاصل از بررسی فرضیه پژوهش بیانگر آن است که مؤلفه‌های شش‌گانه سرمایه انسانی شامل «مدیریت و رهبری، آموزش عوامل انسانی، تجربیات عوامل انسانی، فرهنگ امنیتی، تقویت سیاست‌های امنیتی، خودباوری افراد و شاخص‌های مرتبط با هر یک از مؤلفه‌ها، بر امنیت اطلاعات سازمان‌ها مؤثر است»که دلایل تحلیلی آن بدین شرح است:

– مدیریت و رهبری بر امنیت اطلاعات سازمان‌ها تأثیر دارد.

با توجه به نتایج آزمون لیزرل در رابطه با تأثیر مدیریت و رهبری به‌طور مستقیم بر امنیت اطلاعات سازمان‌ها می‌توان اظهار داشت که حمایت مدیر از امنیت و درگیرشدن او در فعالیت‌های امنیت سامانه‌های اطلاعاتی بر امنیت اطلاعات سازمان‌ها تأثیر مثبت دارد.

– مدیریت و رهبری از طریق فرهنگ امنیتی، بر امنیت اطلاعات سازمان‌ها تأثیر دارد.

با توجه به نتایج آزمون لیزرل در رابطه با تأثیر مدیریت و رهبری از طریق فرهنگ امنیتی بر امنیت اطلاعات سازمان‌ها است.

می‌توان گفت که ایجاد، بهبود و تقویت یک فرهنگ امنیتی خوب برای سازمان و حمایت مدیریت از نگرش‌ها و سنت و ارزش‌های امنیتی، بر امنیت اطلاعات سازمان‌ها تأثیر مثبت دارد.

– مدیریت و رهبری از طریق تقویت سیاست‌های امنیتی بر امنیت اطلاعات سازمان‌ها تأثیر دارد.

با توجه به نتایج آزمون لیزرل در رابطه با تأثیر مدیریت و رهبری از طریق تقویت سیاست‌های امنیتی بر امنیت اطلاعات سازمان‌ها می‌توان بیان کرد که مدیریت سازمان‌ها با داشتن سیاست امنیتی و تقویت مستمر آن، اثرات درخور توجهی بر امنیت اطلاعات سازمان‌ها دارند.

– آموزش کاربر، بر امنیت اطلاعات سازمان‌ها تأثیر دارد.

با توجه به نتایج آزمون لیزرل در رابطه با تأثیر آموزش کارکنان به‌طور مستقیم بر امنیت اطلاعات سازمان‌ها می‌شود گفت که آموزش امنیتی به کاربران، بر امنیت اطلاعات سازمان‌ها تأثیر دارد و برای افزایش امنیت اطلاعاتی می‌بایست به کارکنان آموزش داد تا در سازمان‌ها امنیت اطلاعات سازمان افزایش یابد.

– آموزش کاربر از طریق فرهنگ امنیتی، بر امنیت اطلاعات سازمان‌ها تأثیر دارد.

با توجه به نتایج آزمون لیزرل در رابطه با تأثیر آموزش کارکنان از طریق فرهنگ امنیتی بر امنیت اطلاعات سازمان‌ها می‌توان اظهار داشت که برای افزایش امنیت اطلاعات سازمان‌ها می‌بایست فرهنگ امنیتی بین کارکنان ایجاد شود تا در سازمان‌ها، امنیت اطلاعات افزایش یابد. همچنین می‌بایست ارزش‌های امنیتی سازمان‌ها به کارکنان آموزش داده شود. فرهنگ امنیتی از ضروریات هر سازمانی است که قصد ایجاد امنیت اطلاعات را دارد.

– آموزش کاربر از طریق سیاست‌های امنیتی، بر امنیت اطلاعات سازمان‌ها تأثیر دارد.

با توجه به نتایج آزمون لیزرل در رابطه با تأثیر آموزش کارکنان از طریق سیاست‌های امنیتی بر امنیت اطلاعات سازمان‌ها می‌توان گفت که سازمان‌ها با داشتن سیاست امنیتی و تقویت مستمر آن و آموزش مناسب آن‌ها به کارکنان مربوطه می‌توانند بر امنیت اطلاعات سازمان‌ها تأثیرگذار باشند.

– آموزش کاربر از طریق خودباوری، بر امنیت اطلاعات سازمان‌ها تأثیر دارد.

با توجه به نتایج آزمون لیزرل در رابطه با تأثیر آموزش کارکنان از طریق خودباوری بر امنیت اطلاعات سازمان‌ها می‌شود گفت که خودباوری افراد بر امنیت اطلاعات سازمان‌ها تأثیر دارد. افراد با داشتن حس خودباوری و اعتمادبه‌نفس بر امنیت اطلاعات در سازمان تأثیرگذارند. خودباوری افراد در ایجاد فضای امن سازمان مؤثر است.

– تجربیات افراد (مستقیم یا غیر مستقیم) از طریق خودباوری افراد، بر امنیت اطلاعات سازمان‌ها تأثیر دارد.

با توجه به نتایج آزمون لیزرل در رابطه با تأثیر تجربیات افراد به‌طور مستقیم یا از طریق خودباوری بر امنیت اطلاعات سازمان‌ها می‌توان اظهار داشت که به‌وجودآوردن زمینه‌هایی برای افزایش تجربیات افراد در زمینهٔ امنیت اطلاعات و افزایش خودباوری آن‌ها، بر امنیت اطلاعات سازمان‌ها تأثیر مثبت دارد.

در این پژوهش اثر آموزش کارکنان هم به‌صورت مستقیم و هم از طریق متغیرهای فرهنگ امنیتی، سیاست‌های امنیتی و خودباوری افراد و اثرات متغیرهای شناسایی‌شده قبلی در ارتباط با این متغیرها و در کل بررسی شد و مؤلفه‌ها و شاخص‌های سرمایهٔ انسانی اثرگذار بر امنیت اطلاعات سازمان‌ها و روابط بین آن‌ها در قالب نمودار ۱ ارائه شد.

سامانه‌های اطلاعاتی مبنایی برای تصمیم‌گیری مدیران عالی است. مدیران زمانی قادر به تصمیم‌گیری صحیح هستند که اطلاعات کافی و متقنِ در اختیار آن‌ها، علاوه بر دارابودنِ ویژگی‌های

مربوط‌بودن و به‌موقع‌بودن، امنیت نیز داشته باشند تا مطمئن‌بودن اطلاعات را تضمین کنند.

امروزه کمتر سازمانی یافت می‌شود که از سیستم‌های اطلاعاتی و شبکه‌های رایانه‌ای استفاده نکند و اطلاعات باارزشی را در آن ذخیره ننماید. تمامی این سازمان‌ها دارای ارتباطات پرسرعت و کم‌سرعت اینترنتی هستند. از طرف دیگر، نفوذگران نیز مجهز به ابزارهای پرقدرت و ارزان‌قیمت نرم‌افزاری و سخت‌افزاری به‌منظور بهره‌گیری اقتصادی، ارضای کنجکاوی و اخلال در این شبکه‌ها هستند. بنابراین استقرار یک سیاست امنیتی مؤثر و پویا، وظیفهٔ هر سازمان برای حفاظت از اطلاعات و وجههٔ خود است. مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفهٔ تعیین اهداف امنیتی، بررسی موانع موجود برای رسیدن به این اهداف و ارائهٔ راهکارهای لازم را برعهده دارد. همچنین مدیریت امنیت وظیفهٔ اجرا و کنترل عملکرد سامانهٔ امنیت سازمان را برعهده داشته و در نهایت باید تلاش کند تا سامانه را همیشه به‌روز نگه دارد. بنابراین مدیران و کارکنان باید با انواع تهدیدها و روش‌های ایجاد امنیت در سامانه‌های اطلاعاتی آشنا باشند تا موفق به ایجاد امنیت در سامانه‌های اطلاعاتی خود شوند. البته نمی‌شود تهدیدها را به‌طور کامل از بین برد؛ اما با انجام اقداماتی مشخص می‌توان تا حدودی آن‌ها را محدود کرد. برقراری امنیت مقبول در سامانه‌های اطلاعاتی باعث افزایش قابلیت اتکا و قابلیت اعتماد گزارش‌ها می‌شود که این امر منجر به مفیدبودن اطلاعات مندرج در آن‌ها برای تصمیم‌گیری استفاده‌کنندگان درون‌سازمانی و برون‌سازمانی خواهد شد.

به این دلیل که بسیاری از مسائل و مشکلات رایانه‌ای و امنیتی، امروزه نیازمند راه‌حل‌های مدیریتی‌اند، مؤلفه‌ها و شاخص‌های سرمایهٔ انسانیِ پیشنهادشده در این مطالعه به مدیران کمک می‌کند تا تلاش‌های خود را بر نواحی‌ای متمرکز کنند که بتوانند بیشترین تفاوت و اثربخشی را ایجاد کنند. مدیران می‌توانند با تفکر دربارهٔ نتایج این پژوهش و به‌کارگیری آن برای سازمان‌هایشان، امنیت اطلاعات را بهبود بخشند. این مدل همهٔ جنبه‌های مهم مدیریتی را شامل نمی‌شود؛ با وجود این، بر نواحی‌ای تمرکز کرده است که مدیران می‌توانند با نفوذ و اثرگذاری بر آن‌ها، یک برنامهٔ امنیت‌اطلاعات اثربخش بسازند.

پیشنهادهای اجرایی

سازمان‌ها می‌توانند از طریق استقرار سیاست امنیتی مؤثر و پویا، حفاظت از اطلاعات خود را بهبود بخشند.

سازمان‌ها می‌توانند در زمینهٔ امکان وجود ارتباط‌های دیگر بین متغیرهای این تحقیق، پژوهش دیگری انجام دهند.

استقرار سیاست امنیتی مؤثر و پویا، وظیفهٔ هر سازمان برای حفاظت از اطلاعات و وجههٔ خود است.

مدیران عالی‌رتبه بر افزایش سه عاملِ تجربه و حس خودباوری و اعتمادبه‌نفس افراد که بر امنیت اطلاعات در سازمان تأثیرگذارند، از طریق چرخش مشاغل و آموزش کارکنان تأکید نمایند.

ایجاد تشکیلات امنیت اطلاعات، انتخاب مدیر امنیت اطلاعات و نظارت مستمر مدیر ارشد سازمان به‌عنوان ارکان اساسی برقراری امنیت اطلاعات در هر سازمان پیشنهاد می‌شود.

پیشنهادهایی برای تحقیق‌های آتی

محققان می‌توانند مدل ارائه‌شده در این نوشتار را با به‌کارگیری نمونه‌های مختلفی از فرهنگ‌ها و صنایع دیگر بررسی کنند و به بوتهٔ آزمایش بگذارند تا اثر آن را در زمینه‌های مختلف شناسایی کنند.

پژوهشگران می‌توانند در زمینهٔ امکان وجود ارتباط‌های دیگر بین متغیرهای این پژوهش، جستار دیگری انجام دهند.

محققان می‌توانند تحقیق‌های دیگری را در رابطه با علل بی‌توجهی به عوامل مدیریتی اثرگذار در امنیت اطلاعات سازمان‌ها انجام دهند.

منابع و مآخذ

الف) منابع فارسی

۱. آذرگون، حمیدرضا، ۱۳۸۹، «***اهمیت حسابداری منابع انسانی در تصمیم‌گیری مدیران***»، ش ۲۱۸.

۲.حسن‌قربان، زهرا، ۱۳۷۶، «***حسابداری منابع انسانی: روش‌های اندازه‌گیری ارزش منابع انسانی***»، ماهنامه حسابدار، س ۱۱، ش ۱۲۰.

۳. خاکی، غلامرضا، ۱۳۷۸، ***روش تحقیق با رویکردی به پایان‌نامه‌نویسی***، چ ۱، تهران: درایت.

۴. خیرگو، منصور و جواد شکوهی، ۱۳۹۵، «***شناسایی و رتبه‌بندی عوامل کلیدی مؤثر بر اثربخشی سیستم‌های اطلاعاتی در سازمان‌های دولتی***»، پژوهشنامه پردازش و مدیریت اطلاعات، ص ۱۷ تا ۳۹.

۵. رضاییان، علی، ۱۳۸۵، ***مبانی سازمان و مدیریت***، چ ۸، تهران: سمت.

۶. زنجیرچی، سید محمود و شیما شاه‌حسینی بیده و علی مروتی شریف‌آبادی، ۱۳۹۳، «***مقایسهٔ عملکرد سازمان‌ها در پیاده‌سازی مدیریت ارتباط با مشتری با استفاده از رویکرد ترکیبی NAP و DEMATEL فازی***»، فصلنامهٔ بازاریابی نوین، ص ۱۹۵ تا ۲۱۲.

۷. سیف، یاسر و ناهید نادری بنی، ۱۳۹۶، «***شناسایی مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قاره ایران***»، مجله مدیریت فناوری اطلاعات، ص ۸۵۱ تا ۸۷۰.

۸. صمدی، عباس و حبیب‌الله نصیری، ۱۳۸۹، «***بررسی موانع توسعهٔ حسابداری منابع انسانی در شرکت‌های پذیرفته‌شده در بورس***»، فصلنامه حسابدار رسمی، ش ۲۳، ص ۳۰ تا ۴۱.

۹. طبرسا، غلامعلی و امیرهوشنگ نظرپوری، ۱۳۹۲، «***بررسی عوامل مؤثر بر ارتقای هوشمندی انسانی‌ساختاری در سازمان‌های دانش‌بنیان***»، فصلنامه پژوهش‌های مدیریت در ایران، دوره ۱۷، ش ۱، ص ۱۱۰ تا ۱۳۱.

۱۰. عدالت، احمد و احمد فاضلی، ۱۳۸۵، «***سیستم‌های اطلاعاتی حسابداری***»، نشریهٔ حسابرس، ش ۱۵۱، ص ۹۰ تا ۹۴.

۱۱. فولادی، معصومه و معصومه علیپوریان، ۱۳۹۴، «***سرمایه انسانی دانش‌بنیان***»، چ ۱، تهران: اقتصاد فردا.

۱۲. گرجی، ابراهیم و سجاد برخورداری، ۱۳۸۸، «***مبانی روش تحقیق در علوم اجتماعی***»، تهران: ثالث.

۱۳. مهدوی، ابوالقاسم و محمدامین نادریان، ۱۳۸۹، «***بررسی رابطهٔ علیت گرنجی بین سرمایهٔ انسانی و رشد اقتصادی در ایران***»، پژوهشنامه اقتصادی، س ۱۰، ش ۳، ص ۲۸۷ تا ۳۰۹.

۱۴. میرمجریان، حمید و سید محمدحسن شهشهانی، ۱۳۸۵، «***کارایی تصمیم‌گیری در گزارشگری مالی در محیط شبکه گسترده جهانی***»، نشریهٔ حسابرس، ش ۳۵، ص ۳۷ تا ۴۵.

۱۵. ودیعی، محمدحسین و جمال محمدی، ۱۳۸۹، «***امنیت در سیستم‌های اطلاعاتی حسابداری***»، نشریهٔ حسابرس، ش ۵۱ ، ص ۹۰ تا ۹۴.

الف) منابع لاتین

1.Bassi, Iauric and Daniel mamurrer, (2005), "what to do when people ae your most important?" handbook of business strategy, Volume6, Number, p.219 – 224

2.Daily C. and lueblfing, M. (2000), "Defending the security of theaccounting system" .The CPA Journals. 62-65

3.Davis Charles," (1997), An assessment of accounting information security" ,CPA journal ,p.28-34,

4.Huber, G. P. (2018). A theory of the effects of advanced information technology on organizational design, intelligence, and decision making. Academy of Management Review,6(9):.25:71-87.

5.Kim, S. H., K. H. Yang, and S. Park. (2014). An integrative behavioral model of information security policy compliance. The Scientific World Journal 2014, PP17-19.

6.King ,Gray & Christopher J.L. Murray(2001-2002) " Rethinking Human Security ", Political Science Quarterly , Vol .116, No.4

Kritzinger D, smith.(2011). Towards information security behavioral compliance. Computer& security, PP18-20.

7.Iyere, Alika & , Stan Aibieyi, Joseph(2014) ., Human Capital: Definitions Approaches and Management Dynamics , Journal of Business Administration and Education ISSN2201-2958 , Volume 5, Number 1, 55-78

8.Marimuthu, Maran Arokiasmy, Lawrence & Ismail , Maimunah (2009)., Human Capital Development And Its Impavt On Firm Performance:Evidence From Development Economics, Uluslararası Sosyal Ara_tırmalar Dergisi The Journal of International Social Research Volume 2 / 8Summer

9.Melissa walters (2007). "a draft of an information systems security and control course". Journals of information system. 5-34.

10.Meskell, P., Burke, E., Kropmans, T. J., Byrne, E., Setyonugroho, W. & Kennedy, K.M. (2015). Back to the future: An online OSCE Management Information System for nursing OSCEs. Nurse Education Today, 35(11), 1091-1096.

11. Nikrerk J.F. and Solms, Van.(2017). Information security culture: a management perspective. Computer & security, 5, 142-144.

Sadowsky ,G . et al (2003) IT Security Handbook . infoDev. Worldbank. P. 98-

12.Verma , S, & P, Dewe (2008), " Valuing Human Resource" , Journal of Human Resource Costing & Accounting , 12(2) : 102-123

13.Presenting a conceptual model of components and indicators of human capital affecting information security of organizations

ج) تارنما

۲. الوانی و میرشفیعی، ۱۳۶۹، «***مدل***»، قابل دسترس در: http://www.sndu.ac.ir/fa/content

۳. جلالی، سونیا، ۱۳۹۷، «***تجربه کارکنان***»، آکادمی تخصصی مدیریت منابع انسانی، قابل دسترس در: https://hrmacy.ir/index.php/tag/۲۰۱۸