فصلنامه علمی-پژوهشی مطالعات مدیریت کسب و کار هوشمند- سال هفتم ـ شماره ۲۶ـ زمستان ۱۳۹۷
صفحات ۹۹-۷۱

الگوی امکان‌سنجی و استقرار اثربخش سیستم مدیریت امنیت اطلاعات بر مبنای روش فراترکیب

زهرا وظیفه*
محمد مهدی**
نادیا وکیلی***

چکیده

امروزه، اطلاعات نقش سرمایه یک سازمان را ایفا می‌کند و حفاظت از اطلاعات سازمان یکی از ارکان مهم بقای آن است. از طرفی مشکلات و موانع امنیتی یکی از اساسی‌ترین موضوعات مطرح در زمینه سیستم‌های اطلاعاتی است. از دیرباز، امنیت یکی از اجزای اصلی زیرساخت‌های فناوری اطلاعات شمرده می‌شد. این پژوهش از نظر هدف کاربردی بوده و در آن از روش فراترکیب استفاده شده است. محقق با استفاده از روش فراترکیب، بازنگری دقیق و عمیق در موضوع انجام داده است و یافته‌های پژوهش‌های کیفی و کمی مرتبط را ترکیب کرده است. در این راستا ۱۱۸ پژوهش در زمینه مدیریت امنیت اطلاعات و سیستم‌های اطلاعاتی ارزیابی شد که در پایان ۵۵ پژوهش انتخاب و با تحلیل محتوای (اسنادی- کتابخانه‌ای) آن‌ها، ابعاد و کدهای مربوطه استخراج و میزان اهمیت و اولویت هریک با استفاده از آنتروپی شانون تعیین شد. بر اساس یافته‌های تحقیق، اطلاع از میزان ارزش اطلاعات، قابلیت بازیابی اطلاعات، استفاده صحیح از منابع و همزیستی اطلاعات و نرم‌افزارها بیشترین ضریب اهمیت را در بین ابعاد ده‌گانه دارد. درنهایت، پس از طی گام‌های پژوهش، الگوی تعیین و استقرار اثربخش سیستم مدیریت امنیت اطلاعات در سه لایه شناسایی، ساختار اجرا و طراحی برنامه حمایتی سیستم مدیریت امنیت اطلاعات ارائه شد.

واژگان کلیدی: امنیت اطلاعات، سیستم‌های اطلاعاتی، فراترکیب.

* استادیار گروه مدیریت مالی و بازرگانی، دانشکده اقتصاد و مدیریت دانشگاه سیستان و بلوچستان (نویسنده مسئول)؛ zahravazife@gmail.com
** دانشجوی دکتری مدیریت مالی. دانشکده اقتصاد و مدیریت دانشگاه سیستان و بلوچستان.
*** کارشناسی ارشد مدیریت فناوری اطلاعات. دانشکده اقتصاد و مدیریت دانشگاه سیستان و بلوچستان.

تاریخ دریافت:۱۳۹۷/۰۶/۲۵ **تاریخ پذیرش:۱۳۹۷/۱۲/۱۴**

مقدمه

عصر اطلاعات، الزاماتی را بر سازمان‌ها تحمیل می‌کند که در گذشته نه‌چندان دور قابل‌تصور نبود. توسعه فناوری‌های اطلاعات و ارتباطات همان‌گونه که ساختارهای جوامع را دچار تحول و دگرگونی ساخته است. بسیاری از سازمان‌ها برای بهره‌گیری سودمند و کارای فناوری‌های اطلاعاتی و ارتباطی جدید خود را آماده می‌سازند (هدلین و آلوود[1]، ۲۰۰۹). بدون شک ایجاد سازگاری در ابعاد مختلف سازمان با تغییرات محیطی و استفاده از ابزارهایی که به مرور و با پیشرفت فنّاوری در اختیار مدیران قرار می‌گیرد نه‌تنها ضروری است، بلکه حیات سازمان-ها در محیط‌های متلاطم امروزی به این موضوع مهم بستگی دارد. فناوری اطلاعات با استفاده از علوم مختلف توانسته اطلاعات موردنیاز انواع قشرهای جامعه را در کمترین زمان فراهم کند به‌گونه‌ای که این فناوری ملت‌ها را در یک جامعه جهانی گرد هم آورده است که این مسئله خود یک فرصت بزرگ به شمار می‌آید. بااین‌حال اگر به همان اندازه که به توسعه و فراگیری آن توجه می‌کنیم به امنیت آن توجه نشود به یک تهدید بزرگ تبدیل می‌شود. از طرفی با رشد و توسعه فزاینده فناوری اطلاعات و گسترش شبکه‌های ارتباطی، آسیب‌پذیری فضای تبادل اطلاعات افزایش یافته است و روش‌های اعمال تهدیدهای یادشده پیچیده‌تر می‌شود. ازاین‌رو، حفظ ایمنی فضای تبادل اطلاعات از مهم‌ترین اهداف توسعه فناوری اطلاعاتی و ارتباطی محسوب می‌شود. پژوهشگران معتقدند که اکثر سازمان‌ها هزینه فراوانی برای توسعه فناوری اطلاعات صرف می‌کنند بدون اینکه توجهی به تهدیدات این فناوری شود و سعی دارند اغلب با اجرای راهبردهای مقطعی مانند نصب آنتی‌ویروس و دیوار آتش اطلاعات را حفظ نمایند. درصورتی‌که خسارت بیشتری متحمل می‌شوند ولی متأسفانه همچنان این روش را ادامه می‌دهند. یکی از جنبه‌های مهم برای حفاظت و مدیریت امنیت اطلاعات، ارتقاء آگاهی کاربران از امنیت اطلاعات است. 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 و به‌تدریج به فرهنگ سازمان‌ها

1. Hedelin & Allwood

تبدیل خواهد شد (نیکرک و وان[1]، ۲۰۱۷). از طرفی اطلاعات، منبع قوی و دارایی عمده‌ی سازمان‌ها محسوب می‌شود که اغلب از آن خون حیاتی سازمان نام برده می‌شود؛ اطلاعات برای تمام سازمان‌ها مهم است و نوع درست اطلاعات در پاره‌ای مواقع مزیت رقابتی به بار می‌آورد (الیوت و استارکینگ[2]، ۲۰۰۸). بی‌تردید فناوری‌های نوین اطلاعاتی و ارتباطی زمینه شکل‌گیری سیستم‌های جدید مدیریت اطلاعات و باز مهندسی این سیستم‌ها را بر اساس نوآوری‌های جدید فراهم می‌آورد. سیستم‌های اطلاعاتی؛ جمع‌آوری، تحلیل و ارزشیابی اطلاعات و انتقال آن‌ها از یک نقطه‌به‌نقطه دیگر را امکان‌پذیر می‌سازد و امکان دسترسی سریع به اطلاعات، کاهش هزینه، تولید بهتر، دقت، هماهنگی، رهبری زمان، بهبود کنترل و خدمات بهتر را موجب می‌شود (ایمت[3]، ۲۰۱۵). سیستم‌های اطلاعاتی و کاربردی سازمان، سیستم‌های پیچیده‌ای هستند که معمولاً بسیاری از عملیات درون سازمان را پوشش می‌دهند. ازآنجاکه معمولاً سازمان به این گونه سیستم‌ها وابستگی زیادی دارد، هر نوع عاملی که موجب اختلال در عملکرد آن‌ها شود، می‌تواند صدمات سنگین و جبران‌ناپذیری به سازمان وارد کند. مشکل امنیت در سیستم‌های اطلاعاتی مسئله عمومی است و به دلیل کاربرد وسیع سیستم‌های اطلاعاتی و کاربردی سازمان، مقوله امنیت در این سیستم‌ها اهمیت زیادی دارد (زنجیرچی و همکاران،۱۳۹۳). حیات سازمان‌ها ارتباط نزدیکی با سیستم‌های اطلاعاتی آن‌ها دارد. سیستم‌های اطلاعاتی نیز همواره در خطر سرقت اطلاعات، تغییر اطلاعات و ایجاد وقفه در خدمات‌رسانی هستند. به‌منظور حل مسئله امنیت اطلاعات، سازمان نیازمند به‌کارگیری طیف گسترده‌ای از دانش، فناوری و قوانین سازمانی است و درعین‌حال باید مطمئن شد که سازمان فقط روی راه‌حل‌های فنی متمرکز نیست، بلکه اجزای کلیدی دیگر امنیت اطلاعات، شامل فرایندها و کارکنان نیز در آن لحاظ شده است (کرمر[4]، ۲۰۰۶؛ هونان[5]، ۲۰۰۶). در عصر حاضر اطلاعات به‌عنوان یک منبع استراتژیک و یک شایستگی کلیدی از اهمیت ویژه‌ای

1. Nikrerk & Van
2. Elliot & Starkings
3. Emmett
4. Kermmer
5. Honan

برخوردار است. ازاین‌رو برای استفاده صحیح از این منبع پرمایه، موضوع امنیت اطلاعات در دستور کار دولت‌ها قرار گرفته است. با پیشرفت‌های شگرفی که در زمینه ابزارها و فناوری‌های انتقال این اطلاعات صورت گرفته و به دلیل گسترش استفاده از این فناوری‌های اطلاعاتی و الکترونیکی در بخش دولتی بیشتر معاملات تجاری، تراکنش‌ها، فرآیندهای سازمانی و ارائه خدمات و اطلاعات از شیوه سنتی به الکترونیکی تغییر شکل پیدا کرده است. پذیرش موفق فناوری‌های جدید به دولت برای ارائه خدمات دولتی کارآمدتر به شهروندان کمک می‌کند (ساها[1]، ۲۰۱۸). ضرورت این پژوهش از آنجا احساس می‌شود که سازمان باارزش‌ترین دارایی خود از قبیل طرح‌ها، بخشنامه‌ها، مکاتبات و مستندات پژوهشی را به‌منظور ذخیره و پردازش حجم بالای اطلاعات در اختیار فناوری اطلاعات قرار می‌گیرد، اما اگر سازمان نتواند این دارایی مهم را از دسترس نامحرمان و تهدیدات مختلف حفظ نماید در ارائه خدمات خللی پیش آمده و در نتیجه سازمان نمی‌تواند به کار خود ادامه دهد. از طرفی پیاده-سازی سیستم‌های اطلاعاتی در سازمان‌ها با مشکلات عدیده‌ای مواجه است. به همین دلیل، عملیاتی شدن این قبیل پروژه‌ها با نرخ بسیار بالای شکست روبرو است. لذا مسئله اصلی تحقیق شناسایی پیشران‌های مدیریت امنیت شبکه و حفاظت از اطلاعات بر کیفیت پیاده‌سازی سیستم‌های اطلاعاتی است.

پیشینه تحقیق

پیشینه نظری

قبل از ظهور عصر شبکه‌ها، اطلاعات به‌صورت پرونده‌های کاغذی بایگانی می‌شد. با پدید آمدن شبکه‌ها و دسترسی آسان به اینترنت، قسمت اعظم اطلاعات از طریق این بستر در حال انتقال و پردازش است. بیشتر اطلاعات به‌صورت دیجیتالی ذخیره و بازیابی شده و با سرعت بالاتری در حال انتشار و تکثیر است. به‌موازات گسترش شبکه محلی و سراسری، تهدیدات و سرقت و تخریب اطلاعات نیز افزایش یافته به‌طوری‌که شاید یکی از مهم‌ترین مسائل در عصر اطلاعات، حفاظت و امنیت آن است. به دلیل تغییرات بسیار سریع فناوری در حوزه سیستم‌های

1. Saha

اطلاعاتی ممکن است برخی محصولات در ابتدای عرضه دارای بیشترین امنیت بوده ولی پس از گذشت زمان کوتاهی به‌راحتی می‌توان از این موانع امنیتی عبور کرد. اینکه ما انتظار داشته باشیم یک محصول تمام احتیاجات امنیتی ما را برای سیستم‌های کامپیوتری و تجهیزات شبکه فراهم کند رؤیایی بیش نیست (میوالد[1]، ۲۰۰۴). به عقیده اسلیزر و همکاران[2] (۲۰۱۸)، «توسعه‌های اخیر اقتصادی، نمایانگر این است که آینده خوبی در انتظار فناوری اطلاعات است». امروزه، تمایل به استفاده از فناوری اطلاعات و سیستم‌های جامع اطلاعاتی در سازمان‌های مختلف، در حال افزایش است که علت این امر، امکانات و امتیازات فراوان آن؛ از قبیل سرعت انتقال اطلاعات، سهولت انتقال اطلاعات، ذخیره‌سازی حجم اطلاعات، صرفه‌جویی در وقت، کاهش هزینه‌ها، دقت در انجام کار، قابلیت اعتماد است (توربان و همکاران، ۲۰۱۸). فناوری اطلاعات به سیستم‌های جامع اطلاعاتی کمک می‌کند و این قابلیت باعث می‌شود که ساختار رسمی یک سازمان به‌عنوان یک پردازشگر عمل کند، رشد سازمان‌ها و پیچیده‌تر شدن محیط آن‌ها را افزایش دهد و ضرورت ایجاد هماهنگی میان واحدها در جهت افزایش کارایی را دوچندان گرداند (گرنت و میدواس[3]،۲۰۱۸).

امنیت اطلاعات مسئله‌ای است که سازمان‌ها را در سراسر دنیا تهدید می‌کند. با توجه به اینکه اقتصادها و کسب‌وکارهای مدرن برای بقا به‌طور کامل به فناوری اطلاعات وابسته‌اند، نیاز به حفاظت از اطلاعات از قبل بیشتر شده است. اکنون در سراسر جهان اطلاعات الکترونیکی شده و فناوری نیز به‌طور مداوم تغییر می‌کند. ازآنجاکه کمابیش تمام جنبه‌های زندگی ما به‌وسیله ابزارها، رویه‌ها و فرایندهای فناوری تحت کنترل قرار گرفته است، این مورد اهمیتی فزاینده می‌یابد که در کنار مزیت‌های گسترده فناوری‌های الکترونیک، ضعف‌ها و موارد مجرمانه آن‌ها را بشناسیم و در سیستم‌های اطلاعات الکترونیکی لحاظ کنیم (ولف و ولف[4]، ۲۰۰۳). برای محافظت از اطلاعات سازمان، نمی‌توان به نوع خاصی از امنیت یا به یک محصول خاص اکتفا کرد (میوالد، ۲۰۰۴). امروزه در بیشتر سازمان‌ها اطلاعات کسب‌وکار

1. Mivald
2. Sleezer et al.
3. Grant & Meadows
4. Wolf & Wolf

نقش بسیار مهمی دارد و تلاش برای حفاظت از این اطلاعات از اهمیت شایان توجهی برخوردار است. اطلاعات یکی از مهم‌ترین دارایی‌های هر سازمان محسوب می‌شود و به دلیل 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 ر ا عامل حیات‌بخش سازمان می‌دانند (مسکل و همکاران[1]، ۲۰۱۵)؛ که با به خطر افتادن این جریان، سازمان می‌میرد. اهمیت دادن به اطلاعات برای سازمان ضمن داشتن مزیت‌های بسیار، در موفقیت سازمان در عرصه‌هایی چون جریان نقدینگی و ارزش بازار، نیز سهم عمده‌ای دارد. همچنین اطلاعات عاملی است که موجب پیوند سایر منابع سازمان می‌شود (کوزیکاس[2]،۲۰۱۶). بحث مدیریت امنیت اطلاعات به دلیل پیچیدگی زیاد، با مسائل بحث‌انگیز زیادی مواجه می‌شود که این مباحث در راستای فراهم آوردن چارچوب، روش و فناوری‌هایی برای بهبود پیاده‌سازی امنیت اطلاعات در سازمان است (چاو[3]، ۲۰۰۵). به‌طور سنتی محققان برای نشان دادن ریسک‌های مؤثر بر این اطلاعات، به زیرساخت فناوری اطلاعات توجه کرده‌اند و دلیل آن، اهمیت فناوری اطلاعات در ذخیره پردازش و انتقال دارایی‌های اطلاعاتی باارزش است. به‌هرحال باید در نظر داشت طی سال‌های اخیر مسلم شده است که امنیت اطلاعات دیگر یک موضوع فنی نیست، بلکه مسئله‌ای مدیریتی محسوب می‌شود و ابعاد دیگری مانند مباحث راهبردی و قانونی را نیز دربرمی گیرد (بیرمن[4]، ۲۰۰۰). دو عامل دیگر در اهمیت مدیریت امنیت اطلاعات، شبکه‌های جهانی و تجارت الکترونیکی است. با اشاعه اینترنت و جهانی‌شدن آن، زندگی روزمره ما دچار تغییر شده و سازمان‌های مدرن از اینترنت برای عملیات کسب‌وکار خود استفاده می‌کنند و به آن وابسته شده‌اند. بر این اساس، تجارت الکترونیکی رواج یافته و موجب تغییر فرایندهای کسب‌وکار سازمان‌ها شده است. این وابستگی به کسب‌وکارهای الکترونیکی نیز، ضرورت حفاظت از اطلاعات را مطرح کرده و رویکردهای

1. Meskell et al.
2. Kouziokas
3. Chau
4. Birman

گوناگونی را برای مدیریت امنیت اطلاعات به وجود آورده است (زوکاتو[1]، ۲۰۰۷).

«فناوری اطلاعات، انقلابی است که هدف آن، ایجاد ساختار الکترونیکی است و کاربرد هوشمندانهٔ آن، تبادل اطلاعات را به‌صورت اینترنتی امکان‌پذیر می‌کند، از ورود اطلاعات زائد جلوگیری می‌کند، اطلاعات موردنیاز را در زمان کم فراهم می‌کند، به مدیران، اجازه می‌دهد که اطلاعات پیچیده را به‌صورت مؤثرتری دریافت و پیگیری کنند و به‌آسانی در میان اعضای سازمان، مبادله نمایند؛ بنابراین ارتباطات در سازمان به‌طور وسیعی بهبود می‌یابد»(مور[2]،۲۰۱۷).

«در یک رویکرد ابزاری، به هر چیزی که بدون محدودیت‌های مکانی و زمانی، موجب جمع‌آوری، گردش، پردازش و تبادل اطلاعات و پیام‌ها می‌گردد، فناوری اطلاعات گفته می‌شود و با یک رویکرد راهبردی، فناوری اطلاعات، یک استراتژی، فکر و ابزار در حوزهٔ انسانی، همراه با نوآوری است» (جین و همکاران[3]،۲۰۱۸).

«منظور از فناوری اطلاعات، مجموعه‌ای شامل سخت‌افزار و نرم‌افزار؛ از قبیل سیستم یکپارچهٔ مالی و حسابداری است» (هانگ[4]،۲۰۱۸).

سیستم‌های اطلاعاتی به‌صورت فنی به مجموعه‌ای به هم وابسته از اجزاء اطلاق می‌شود که تصمیم‌گیری و کنترل را در سازمان‌ها پشتیبانی، داده‌ها را دریافت، پردازش و ذخیره‌سازی کرده و سپس اطلاعات را توزیع می‌کند (شریرام و همکاران[5]، ۲۰۱۰). ژانگ و همکاران[6] (۲۰۱۱) معتقدند که پیاده‌سازی سیستم‌های اطلاعاتی عملاً در حکم انجام فرآیند ایجاد تغییر در سازمان است و مدیریت باید ضمن توجه کافی به موضوع پیچیدگی پروژه سیستم‌های بزرگ در تخمین هزینه و زمان پیاده‌سازی این سیستم‌ها نیز موفق باشد.

اغلب سازمان‌ها در معرض انواع تهدیدهای داخلی و خارجی خرابکاران اطلاعاتی قرار می‌گیرند؛ تهدیدهایی همچون دست‌کاری اطلاعات مرجع، سرقت اطلاعات حیاتی و سرمایه‌های اطلاعاتی. در چنین وضعیتی، عواملی که جزء مزیت‌های سیستم به شمار می‌روند

1. Zuccato
2. Moore
3. Jean et al.
4. Huang
5. Shreeram et al.
6. Zhang et al.

(مثل سرعت و قابلیت دسترسی زیاد)، اگر تحت کنترل نباشند، ممکن است باعث بروز آسیب‌پذیری شوند و سوءاستفاده افراد از آن‌ها به نفوذ، خرابکاری و کلاه‌برداری بینجامد. علاوه بر این، چنانچه روند صحیحی برای حفاظت از اطلاعات وجود نداشته باشد، مشکلات طبیعی و خطاهای غیرعمدی توسط کاربران رایانه‌ای، می‌تواند نتایج مخربی به بار آورد. بنابراین ضرورت توجه به «امنیت اطلاعات» و «مدیریت امنیت اطلاعات» بیش‌ازپیش احساس می‌شود (پاتاری و سونار[1]، ۲۰۱۲).

پیشینه تجربی

تاکنون بیشتر تحقیقاتی که در زمینه امنیت سیستم‌های اطلاعاتی انجام‌شده، در زمینه مسائل فنی و تکنیکی بوده و تحقیقات و تمرین‌های تحقیقاتی از دید مسائل فنی به امنیت اطلاعات نگریسته‌اند. همان‌طور که بلونه و همکاران[2] (۲۰۰۸) بیان کرده است، در بیشتر تحقیقاتی که در زمینه امنیت اطلاعات صورت گرفته، یک نوع دید و رویکرد فنی وجود دارد و متخصصان امنیت اطلاعات برای برطرف کردن مشکلات امنیتی بیشتر به دنبال یک سری ابزارهای فنی مانند آنتی‌ویروس‌ها، فایروال‌ها و... بوده‌اند. به‌هرحال، به گفته تامسون و نیکرک[3] (۲۰۱۲)، امنیت اطلاعات هم فناوری و هم فرد را دربر می‌گیرد، اما بیشتر سازمان‌ها راه‌حل‌های فنی را جواب فوری به مشکلات امنیتی خود می‌دانند، درحالی‌که موانع زیادی برای رویکرد فنی وجود دارد. در یکی از تحقیقات بهاتاچاریا[4] (۲۰۱۲)، عامل انسانی به‌عنوان پاشنه آشیل امنیت اطلاعات معرفی‌شده است. شاه بیدی و همکاران (۱۳۹۳) معتقدند؛ امنیت سیستم‌های اطلاعاتی هم فناوری و هم افراد (عوامل انسانی) را دربرمی گیرد. بر اساس نتایج آنان، پنج شاخص اصلی عبارت‌اند از: ۱. اشاعه و استفاده از اطلاعات محرمانه (امنیتی)؛ ۲. سوءاستفاده از سیستم اطلاعات (سوءاستفاده عمدی کارمندان داخلی از منابع)؛ ۳. آگاهی از اهمیت و ضرورت پیروی از قوانین و اجرای فعالیت‌های امنیتی؛ ۴. استفاده از ابزارهای آموزشی متنوع برای

1. Pathari & Sonar
2. Bellone et al.
3. Thomson & Niekerk
4. Bhattacharya

آموزش فعالیت‌های مرتبط با امنیت سیستم‌های اطلاعاتی؛ ۵. تعهد و وفاداری کارمندان به سازمان و حفظ اطلاعات. پژوهش‌های پیشین، موارد زیر را موانع پیاده‌سازی سیستم‌های اطلاعاتی معرفی کرده‌اند: تعیین اشتباه حوزه انجام پروژه، نگرش نامناسب سازمان به این سیستم، آگاهی نداشتن و آموزش کم کارمندان سازمان، مقاومت کارمندان سازمان، تجهیزات نامناسب فنی، مدیریت ریسک نامناسب، عدم انجام ممیزی دوره‌ای، مقاومت کارمندان سازمان، بروز تغییرات در تشکیلات سازمانی، نداشتن درک صحیح از شروط و مفاد استاندارد، سازگار نبودن با رویه‌های سازمانی، برخوردار نبودن از دانش کافی درباره تهدیدهای امنیت اطلاعات، هزینه‌های بالای مالی و زمانی پیاده‌سازی، برون‌سپاری خدمات فناوری اطلاعات، فهرست دارایی ناقص، انتخاب کنترل‌های نامناسب، نبود برنامه مناسب مدیریت تداوم کسب‌وکار، مستندسازی نامناسب، شرح وظایف و مسئولیت‌های نامناسب امنیتی، ممیزی‌های ناکافی مدیریت، مدیریت پروژه نامناسب، پشتیبانی نامناسب مدیریت، ممیزی نامناسب داخلی، نظرخواهی نکردن از کارکنان دیگر سازمان هنگام اخذ تصمیمات مرتبط با امنیت اطلاعات، هم‌راستا نبودن سیاست‌های امنیتی با فلسفه سازمانی، پراکندگی جغرافیایی سازمانی، نظارت ناکافی بر رفتار کارکنان در حوزه امنیت اطلاعات (دهیلن[1]، ۲۰۰۱؛ عبدالجلیل و عبدالحمید[2]، ۲۰۰۵؛ فومین و همکاران[3]، ۲۰۰۸؛ کاکار و همکاران[4]، ۲۰۱۲؛ کو و همکاران[5]، ۲۰۰۹). همچنین موارد زیر عوامل حیاتی موفقیت پیاده‌سازی سیستم-های اطلاعاتی شناسایی شدند؛ پشتیبانی و مشارکت مدیریت عالی سازمان، سیاست‌های مناسب امنیتی، شرح وظایف مناسب امنیتی، انگیزه کارمندان، سازگاری رویه کسب‌وکار سازمان با رویه‌های امنیتی و مشاور مجرب خارجی (العودی و رینا‌د[6]،۲۰۰۷؛ کاظمی و همکاران،۲۰۱۲). تاج فر و همکاران (۱۳۹۳) در پژوهشی به رتبه‌بندی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف پرداختند. نتایج پژوهش

1. Dhillon
2. AbdulJalil & AbdulHamid
3. Fomin et al.
4. Kakkar et al.
5. Ku et al.
6. Al-Awadi & Renaud

مهم‌ترین مانع در راه پیاده‌سازی ISMS را ناهمخوانی ساختار سازمانی با نیازها ISMS می-داند و ترس کارکنان از سخت شدن فرآیندهای کار با اجرای ISMS را کم‌اهمیت‌ترین مانع معرفی کرده است؛ ضمن آنکه میزان آمادگی مدیریت اکتشاف در پیاده‌سازی ISMS پایین-تر از حد متوسط است. سیف و نادری بنی (۱۳۹۶)، به شناسایی مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قاره‌ی ایران پرداختند. بر اساس نتایج پژوهش، 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. خیرگو و شکوهی (۱۳۹۶)، در پژوهشی با عنوان «شناسایی و رتبه‌بندی عوامل کلیدی مؤثر بر اثربخشی سیستم‌های اطلاعاتی در سازمان‌های دولتی» بیان کردند که امروزه سیستم‌های اطلاعاتی از عوامل مؤثر در دستیابی به مزیت رقابتی برای سازمان‌ها محسوب می‌شوند؛ چر ا که کیفیت خروجی این سیستم‌ها نقش مهمی در بهبود عملکرد سازمان دارد. نتایج پژوهش آن‌ها نشان‌دهنده تأثیر مثبت عوامل سازمانی، عوامل انسانی و فنی بر اثربخشی سیستم‌های اطلاعاتی است. همچنین، از بین شاخص‌های مؤثر بر اثربخشی سیستم‌های اطلاعاتی، حمایت مدیر ارشد، امنیت، پذیرش و مدیریت دانش فناوری اطلاعات و سیستم‌های اطلاعاتی، به ترتیب رتبه‌های نخست را به خود اختصاص داده‌اند. تقوا و همکاران (۱۳۹۲)، در پژوهشی با عنوان تأثیر به‌کارگیری فناوری اطلاعات بر عملکرد سازمانی و مزیت رقابتی پرداختند. مدل پژوهش دربردارنده سه عامل یا متغیر پنهان اعمال فناوری اطلاعات، عملکرد سازمانی و مزیت رقابتی است. نتایج نشان داد که عوامل IT غیر از ایمن بودن، بر عملکرد سازمانی و مزیت رقابتی تأثیر دارند. هوبر[1] (۲۰۱۸)، در پژوهش‌های خود به این نتیجه رسید که فناوری اطلاعات سبب تغییر فرآیندهای سازمان از جمله: موجب مکانیزه شدن و سرعت بالای فرآیندها، مشاغل مجازی و همکاری‌های راه دور، افزایش تعاملات و بازخورد فوری، موجب ایجاد، توزیع و مدیریت مؤثر و هوشمندانه دانش و اشتراک‌گذاری اطلاعات در سطوح مختلف سازمان می‌شود.

1. Huber

روش تحقیق

این پژوهش از نظر هدف کاربردی و برحسب نحوه‌ی گردآوری داده‌ها پژوهش از نوع اسنادی- فراترکیب است. در تحقیق حاضر جامعه‌ی آماری شامل پژوهش‌های پیشین (مقالات، طرح‌ها و پایان‌نامه‌های معتبر داخلی و خارجی) در زمینه مدیریت امنیت اطلاعات، مدیریت سیستم‌های اطلاعاتی است. در زمینه نمونه‌گیری، مرتبط‌ترین مطالعات با استفاده از رویکردی هدفمند انتخاب شدند که در بررسی‌های انجام‌گرفته در این زمینه ۵۵ پژوهش انتخاب شد که در آن‌ها درباره مدیریت امنیت اطلاعات به‌طور مستقیم و همچنین در زمینه سایر متغیرها بحث شده بود. به‌منظور تحلیل اکتشافی مبانی نظری پژوهش و تائید پایایی کدهای استخراج‌شده، از آزمون کاپا استفاده شده است. همچنین برای تحلیل داده‌ها از رویکرد کیفی استفاده شد که در این تحقیق از نرم‌افزار لیزرل و معادلات ساختاری برای کدگذاری‌های تحقیق و رتبه‌بندی استفاده شد. برای بررسی اعتبار مطالعات مورد استفاده در این پژوهش از ابزار حیاتی «گلین» استفاده شده است که در ارزیابی طرح‌های تحقیقاتی کاربرد دارد. فراترکیب مشابه فرا تحلیل، برای یکپارچه‌سازی چندین مطالعه برای ایجاد یافته-های جامع و تفسیری صورت می‌گیرد (بک[1]، ۲۰۰۲). در مقایسه با رویکرد فرا تحلیل کمی که بر داده‌های کمی ادبیات موضوع و رویکردهای آماری تکیه دارد، فراترکیب متمرکز بر مطالعات کیفی بوده، به ترجمه مطالعات کیفی به یکدیگر و فهم عمیق پژوهشگر برمی‌گردد. به‌عبارت‌دیگر، فراترکیب، ترکیب تفسیر، تفسیرهای داده‌های اصلی مطالعات منتخب است (زیمر[2]، ۲۰۰۶). فراترکیب با فراهم کردن نگرش نظام‌مند برای پژوهشگران از راه ترکیب پژوهش‌های کیفی مختلف به کشف موضوعات و استعاره‌های جدید و اساسی می‌پردازد و با این روش دانش جاری را ارتقاء داده، یک دید جامع و گسترده‌ای را نسبت به مسائل پدید می‌آورد. فراترکیب مستلزم این است که پژوهشگر یک بازنگری دقیق و عمیق انجام داده، یافته‌های پژوهش‌های کیفی مرتبط را ترکیب کند. در این پژوهش از روش هفت مرحله‌ای

1. Beck
2. Zimmer

فراترکیب سندلوسکی و باروسو[1] (۲۰۰۳) استفاده شده است که در شکل ۱ نشان داده شده است.

شکل ۱. مراحل هفت‌گانه روش فراترکیب

گام یک: تنظیم سؤال‌های پژوهش

در جدول ۲، سؤال‌های پژوهش به همراه پارامترها بیان شده است.

جدول ۱. پارامترها و سؤال‌های پژوهش

پارامترها		سؤال‌های پژوهش
چه چیزی؟	What	چه عواملی مؤلفه‌های استقرار اثربخش مدیریت امنیت اطلاعات و کیفیت پیاده‌سازی اطلاعات را تشکیل می-دهند؟
چه جامعه‌ای؟	Who	
محدودیت زمانی؟	When	
چگونگی روش؟	How	چه اهمیت و وزنی هر یک از مؤلفه‌ها در استقرار اثربخش مدیریت امنیت اطلاعات و کیفیت پیاده‌سازی اطلاعات دارند؟

1. Sandelowski & Barroso

گام دوم: بررسی نظام‌مند متون

در این پژوهش پایگاه‌های داده، نشریه‌ها و موتورهای جست‌وجوی مختلفی بین سال‌های ۲۰۰۰ تا ۲۰۱۸ بررسی شده است. واژه‌های کلیدی متنوعی از جمله مدیریت امنیت اطلاعات، مدیریت امنیت شبکه، سیستم‌های اطلاعاتی و کیفیت پیاده‌سازی سیستم‌های اطلاعاتی، برای جست‌وجوی مقاله‌های پژوهش مورد استفاده قرار گرفت. در نتیجه جست‌وجو و بررسی پایگاه-های داده، نشریه‌ها و موتورهای جست‌وجوی مختلف (IEEE,Emerald Insight,Science Direct,Springer,) و با استفاده از واژه‌های کلیدی موردنظر،۱۱۸ مقاله یافت شد.

گام سوم: جست‌وجو و انتخاب مقاله‌های مناسب

برای انتخاب مقاله‌های مناسب بر اساس نمودار نشان داده شده در شکل ۲، پارامترهای مختلفی مانند؛ عنوان، چکیده، محتوا، دسترسی، محتوا و کیفیت روش پژوهش مورد ارزیابی قرار گرفته است.

شکل ۲. نمودار انتخاب مقاله‌های نهایی

گام چهارم: استخراج نتایج

مقاله‌ها بر اساس مرجع مربوط به هر مقاله، شامل نام و نام خانوادگی نویسنده، به همراه سال انتشار مقاله و اجرای هماهنگی بیان شده که در هر مقاله به آن‌ها اشاره شده است، طبقه‌بندی شد.

گام پنجم: تجزیه‌وتحلیل و تلفیق یافته‌های کیفی

در این پژوهش ابتدا برای تمام عوامل استخراج‌شده از مطالعات پیشین، کدی را در نظر گرفته، سپس با در نظر گرفتن مفهوم هر یک از این کدها، آن‌ها را در یک مفهوم مشابه دسته‌بندی کردیم. به‌این‌ترتیب، مفاهیم پژوهش مشخص شدند. بر اساس تحلیل‌های صورت گرفته به کمک روش تحلیل محتوا روی ۵۵ مقاله‌ی نهایی انتخاب‌شده، درمجموع تعداد دو مقوله و ۱۰ مفهوم و ۵۶ کد در این پژوهش کشف و برچسب‌گذاری شدند. یافته‌های حاصل از این مرحله بیانگر آن بود که در مطالعات قبلی تاکنون چنین مطالعه نظام‌مندی انجام نشده و هریک از مطالعات، فقط به جنبه‌ی خاصی از مدیریت امنیت اطلاعات و پیاده‌سازی سیستم‌های اطلاعاتی توجه داشته‌اند و ابعاد چندگانه در قالب یک چارچوب منسجم و به‌صورت نظام‌مند در نظر گرفته نشده است. در جدول ۲، کدهای نهایی استخراج‌شده مرتبط با هر مقوله و مفهوم نشان داده شده است.

جدول ۲. مقوله‌بندی یافته‌ها

مقوله	مفاهیم	کد	منبع
امنیت اطلاعات	امنیت منابع انسانی	دوره‌های آموزشی، حمایت مدیریت عالی، کار زیاد، عدم تداخل مسئولیت‌های کارکنان، ترس کارکنان، مقاومت کارکنان، همکاری و هماهنگی کارکنان، کمیته راهبری شایسته، ثبات مدیریت ارشد سازمان، مشاور برون‌سازمانی، بلوغ کارکنان، میزان آگاهی و دانش کارکنان، تجربه‌ها و خودباوری افراد، مهارت کافی و لازم، اطلاع از میزان ارزش اطلاعات، انگیزه کافی، عدم کوتاهی و عدم بی‌مسئولیتی، عدم فراموش‌کاری	عبدالجلیل و عبدالحمید (۲۰۰۵ و ۲۰۰۷)، تقوا و فلاح (۱۳۹۲)، سیف (۱۳۹۶)، (مسکل[1]، ۲۰۱۵)
	امنیت کاربران	آشنایی کاربران با سیستم کاربردی، آشنایی کاربران با امنیت سیستم‌عامل، آشنایی کاربران با بسته‌های نرم‌افزاری	العودی (۲۰۰۷)، شاه‌حسینی (۱۳۹۳)، سیف (۱۳۹۶)، (بیرمان[2]، ۲۰۰۰)
	امنیت فیزیکی	سرقت، حوادث، تعمیرات رایانه و قطعات، خطرات محیطی	(میوالد[3]، ۲۰۰۴؛ موره[4]، ۲۰۱۷؛ نیکررک[5]، ۲۰۱۷؛ پاتاری[6]، ۲۰۱۲؛ ساها[7]، ۲۰۱۸)
	امنیت فناورانه	قلمرو استقرار، زیرساخت مناسب فناوری اطلاعات، تدوین مناسب خط‌مشی امنیت اطلاعات، افشای اطلاعات، تخریب اطلاعات، تغییر اطلاعات، مستندسازی مناسب، تجهیزات مناسب، هماهنگی ساختار سازمانی با نیازهای پیاده‌سازی سیستم‌های اطلاعاتی	(شریرام[8]، ۲۰۱۰؛ اسلیزر[9]، ۲۰۱۸؛ سیف، ۱۳۹۶؛ خیرگو،۱۳۹۶؛ بهاتاچاریا، ۲۰۰۱؛ چوی، ۲۰۰۸؛ چاو،۲۰۰۵)

1. Meskell
2. Birman
3. Mivald
4. Moore
5. Nikrerk
6. Pathari
7. Saha
8. Shreeram
9. Sleezer

پیاده‌سازی سیستم‌های اطلاعاتی	عملیاتی بودن	متناسب بودن نرم‌افزارها، دقت نرم‌افزارها، تعامل‌پذیری سیستم‌های اطلاعاتی، امنیت اطلاعات	(تامسون[1]، ۲۰۱۲؛ توربان[2]، ۲۰۱۸؛ ژانگ[3]، ۲۰۱۱؛ جین[4]، ۲۰۱۸)
	کارایی	رفتار زمانی به‌موقع، هزینه، استفاده صحیح از منابع	(کاکار[5]، ۲۰۱۲؛ کاظمی[6]، ۲۰۱۲؛ بکلون[7]، ۲۰۰۸؛ چاو، ۲۰۰۵)
	قابلیت اطمینان	بلوغ و تکامل نرم‌افزارها، تحمل‌پذیری خطر، قابلیت بازیابی اطلاعات	(کوزیوکاس[8]، ۲۰۱۶؛ کرامر[9]، ۲۰۰۶؛ نیتزینگر[10]، ۲۰۰۸؛ هوانگ[11]، ۲۰۱۸)
	قابلیت استفاده	قابلیت فهم نرم‌افزارها، قابلیت یادگیری نرم‌افزارها، قابلیت کارکردی نرم‌افزارها، جذابیت نرم‌افزارها	(کو[12]، ۲۰۰۹؛ هوبر[13]، ۲۰۱۸؛ بهاتاچاریا،۲۰۰۱؛ چاو، ۲۰۰۵)
	قابلیت نگهداری	قابلیت تحلیل نرم‌افزارها، قابلیت تغییر نرم‌افزارها، پایداری اطلاعات و نرم‌افزارها، آزمایش پذیری نرم‌افزارها	(هونان[14]، ۲۰۰۶؛ گرنت[15]، ۲۰۱۸؛ فومین[16]، ۲۰۰۸؛ ایموت[17]، ۲۰۱۵)
	انتقال‌پذیری	قابلیت انطباق نرم‌افزارها، قابلیت نصب نرم‌افزارها، هم‌زیستی اطلاعات و نرم‌افزارها، تعویض‌پذیری نرم‌افزارها	(الایوت[18]، ۲۰۰۸؛ دیلون[19]، ۲۰۰۱)

1. Thomson
2. Turban
3. Zhang
4. Jean
5. Kakkar
6. Kazemi
7. Bcllon
8. Kouziokas
9. Kraemer
10. Knitzinger
11. Huang
12. Ku
13. Huber
14. Honan
15. Grant
16. Fomin
17. Emmott
18. Elliott
19. Dhillon

گام ششم: کنترل کدهای استخراجی

زمانی که دو رتبه دهنده، پاسخگویان را رتبه‌بندی می‌کنند و قصد داریم میزان توافق بین این دو رتبه‌بندی را بسنجیم، از شاخص کاپا استفاده می‌کنیم (حبیب پور،۱۳۸۸). برای کنترل مفاهیم استخراجی، از مقایسه‌ی نظر پژوهشگر با یک خبره استفاده شده است. شاخص کاپا بین صفر تا یک نوسان دارد. هرچه مقدار این سنجه به عدد یک نزدیک‌تر باشد، نشان می‌دهد که توافق بیشتری بین رتبه دهندگان وجود دارد؛ اما زمانی که مقدار کاپا به عدد صفر نزدیک‌تر باشد، در آن صورت توافق کمتر بین دو رتبه دهنده وجود دارد (محقر و همکاران،۱۳۹۲). با استفاده از نرم‌افزار لیزرل عدد معناداری ۰/۰۰۰ و مقدار شاخص ۰/۷۸۶ محاسبه شد که در جدول ۳ نشان داده شده است. با توجه به کوچک‌تر بودن عدد معناداری از ۰/۰۵ فرض استقلال کدهای استخراجی رد می‌شود. پس می‌توان ادعا کرد که استخراج کدها از پایایی مناسبی برخوردار بوده است.

جدول ۳. مقدار اندازه توافق

		انحراف استاندارد	عدد معناداری
کاپای مقدار توافق	۰/۷۸۶	۰/۰۷۰	۰/۰۰۰
تعداد موارد معتبر	۹۶		

تحلیل محتوا مرحله‌ای از فرآیند اطلاعاتی است که به‌وسیله آن محتوای ارتباطات با استفاده از به‌کارگیری مجموعه‌ای از قوانین طبقه‌بندی‌شده و نظام‌دار تغییر و تبدیل می‌یابد و به‌صورت داده‌های خلاصه‌شده و قابل‌مقایسه درمی‌آید. روش آنتروپی شانون پردازش داده‌ها را در مبحث تحلیل محتوا بسیار قوی انجام می‌دهد. آنتروپی در تئوری اطلاعات، شاخصی است برای اندازه‌گیری عدم اطمینان که به‌وسیله یک توزیع احتمال بیان می‌شود. روش‌های متعددی برای تعیین وزن شاخص‌ها وجود دارد؛ یکی از بهترین این روش‌ها، آنتروپی شانون است (آذر، میرفخرالدینی و انواری رستمی،۱۳۸۷). در روش آنتروپی شانون ابتدا پیام برحسب مقوله به‌تناسب هر پاسخگو در قالب فراوانی شمارش می‌شود. سپس با استفاده از بار اطلاعاتی

هر مقوله، درجه‌ی اهمیت هریک محاسبه می‌شود. در این پژوهش از روش آنتروپی شانون به دلیل قدرت آن و سادگی محاسبه استفاده شده است. بر این اساس، میزان پشتیبانی پژوهش-های گذشته از یافته‌های این پژوهش به‌صورت آماری نشان داده می‌شود. برای محاسبه بار اطلاعاتی عدم اطمینان و ضریب اهمیت به ترتیب از فرمول ۱ و ۲ استفاده شده است.

فرمول ۱. محاسبه بار اطلاعاتی عدم اطمینان

$$E_j = -K \sum_{i1}^{m} [p_{ij} ln p_{ij}], (j = 1,2, \dots, n), K = \frac{1}{lnm}$$

فرمول ۲. محاسبه ضریب اهمیت

$$W_j = \frac{E_j}{\sum_{j=1}^{n} Ej}$$

برای محاسبه‌ی وزن هریک از مفاهیم نیز، به محاسبه‌ی مجموع وزن کدهای آن مفهوم پرداخته شده و بر اساس وزن‌های به دست آمده رتبه‌بندی در جدول ۴ صورت گرفته است.[۱]

جدول ٤. رتبه‌بندی و ضریب اهمیت مدیریت امنیت شبکه و حفاظت از اطلاعات بر کیفیت پیاده‌سازی سیستم‌های اطلاعاتی

مفاهیم	کد	فراوانی	$P_{ij}LNP_{ij}$	عدم اطمینان E_j	ضریب اهمیت W_{ij}	رتبه در مفاهیم	رتبه در کل
امنیت منابع انسانی	بلوغ کارکنان	۱۴	-۲/۸۹۰۴	۰/۵۷۶۸	۰/۰۱۵۱	۲	۱۳
	اطلاع از میزان ارزش اطلاعات	۲۵	-۳/۲۱۸۹	۰/۷۰۳۶	۰/۰۱۸۵	۱	۱
امنیت کاربران	آشنایی کاربران با سیستم کاربردی	۱۴	-۲/۶۳۹۱	۰/۵۷۶۸	۰/۰۱۵۱	۱	۱۳
	آشنایی کاربران با بسته‌های نرم‌افزاری	۱۰	-۲/۳۰۲۶	۰/۵۰۳۳	۰/۰۱۳۲	۲	۲۷
امنیت فیزیکی	تعمیرات رایانه و قطعات	۵	-۰/۶۰۹۴	۰/۳۵۱۸	۰/۰۰۹۲	۲	۴۰

۱ به دلیل حجم زیاد اطلاعات جدول، محقق کدهای را که رتبه‌های یک و دو در مفاهیم به دست آورده‌اند، در جدول بیان شده است.

	خطرات محیطی	۸	-۲/۰۷۹۴	۰/۴۵۴۵	۰/۰۱۱۹	۱	۳۶
امنیت تکنولوژیکی	قلمرو استقرار	۸	-۲/۰۷۹۴	۰/۴۵۴۵	۰/۰۱۱۹	۱	۳۶
	تخریب اطلاعات	۸	-۲/۰۷۹۴	۰/۴۵۴۵	۰/۰۱۱۹	۱	۳۶
	تغییر اطلاعات	۵	-۱/۶۰۹۴	۰/۳۵۱۸	۰/۰۰۹۲	۲	۴۰
	افشای اطلاعات	۸	-۲/۰۷۹۴	۰/۴۵۴۵	۰/۰۱۱۹	۱	۳۶
	مستندسازی مناسب	۸	-۲/۰۷۹۴	۰/۴۵۴۵	۰/۰۱۱۹	۱	۳۶
قابلیت اطمینان	بلوغ و تکامل نرم‌افزارها	۱۸	-۲/۸۹۰۴	۰/۶۳۱۸	۰/۰۱۶۶	۲	۵
	قابلیت بازیابی اطلاعات	۲۳	-۳/۱۳۵۵	۰/۶۸۵۳	۰/۰۱۸۰	۱	۲
عملیاتی بودن	متناسب بودن نرم‌افزارها	۱۱	-۲/۳۹۷۹	۰/۰۵۲۴	۰/۰۱۳۷	۱	۲۲
	تعامل‌پذیری سیستم‌های اطلاعاتی	۶	-۱/۷۹۱۸	۰/۳۹۱۶	۰/۰۱۰۳	۲	۴۱
کارایی	رفتار زمانی به‌موقع	۵	-۱/۶۰۹۴	۰/۳۵۱۸	۰/۰۰۹۳	۲	۴۰
	استفاده صحیح از منابع	۱۹	-۲/۹۴۴	۰/۶۴۳۶	۰/۰۱۶۹	۱	۳
قابلیت استفاده	قابلیت یادگیری نرم‌افزارها	۱۶	-۲/۷۷۲۶	۰/۶۰۶۰	۰/۰۱۵۹	۱	۹
	قابلیت کارکردی نرم‌افزارها	۱۳	-۲/۵۶۴۹	۰/۵۶۰۶	۰/۰۱۴۷	۲	۱۶
قابلیت نگهداری	قابلیت تحلیل نرم‌افزارها	۱۵	-۲/۷۰۸۱	۰/۵۹۱۹	۰/۰۱۵۵	۱	۱۲
	پایداری اطلاعات و نرم‌افزارها	۱۱	-۲/۳۹۷۹	۰/۵۲۴۱	۰/۰۱۳۷	۲	۲۲
انتقال‌پذیری	همزیستی اطلاعات و نرم‌افزارها	۱۸	-۲/۸۹۰۴	۰/۶۳۱۸	۰/۰۱۶۶	۱	۵
	قابلیت نصب نرم‌افزارها	۱۴	-۲/۶۳۹۱	۰/۵۷۶۸	۰/۰۱۵۱	۲	۱۳

همان‌طور که در جدول ۴ مشخص شده است، اطلاع از میزان ارزش اطلاعات، قابلیت بازیابی اطلاعات، استفاده صحیح از منابع، همزیستی اطلاعات و نرم‌افزارها بیشترین اهمیت را دارند و در کل بالاترین رتبه‌ها را کسب کرده‌اند؛ یعنی در بحث استقرار مدیریت امنیت اطلاعات و شبکه و پیاده‌سازی سیستم‌های اطلاعاتی این موضوعات بیشتر مطالعه شده‌اند و تکرارپذیری بیشتری نسبت به سایر کدها داشته‌اند. ازاین‌رو توجه به ابعاد امنیت انسانی، قابلیت اطمینان، کارایی، قابلیت استفاده و انتقال‌پذیری و عوامل تأثیرگذاری اهمیت داشته است.

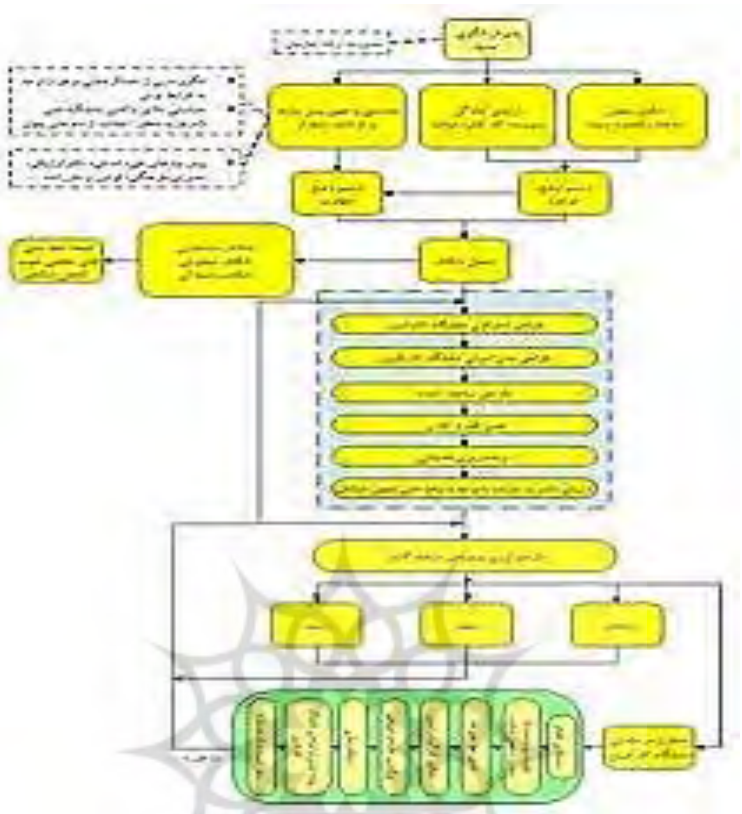
گام هفتم: ارائه یافته‌ها (ارائه الگو)

بر اساس مطالعه پژوهش‌های پیشین و کدهای استخراج‌شده مؤلفه‌های اصلی مدیریت امنیت اطلاعات و پیاده‌سازی سیستم‌های اطلاعاتی شامل موارد زیر می‌شود:

پیش از آغاز، الگوی جدید توسط مدیریت ارشد باید مورد پذیرش قرار گیرد. در ادامه، پیش‌نیازهای مدیریت امنیت و پیاده‌سازی سیستم‌های اطلاعاتی جهت شناسایی و تعیین الزامات استقرار مورد بررسی قرار می‌گیرد، بدین منظور می‌توان از عملکردهای موفق با توجه به شرایط بومی الگوبرداری کرده و دلایل ناکامی سازمان‌ها و شناسایی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات به‌منظور اجتناب از دام‌های پنهان شناسایی شوند؛ نتایج این بررسی‌ها تصویری از وضع مطلوب را نمایان می‌سازد. در کنار این بررسی‌ها، امکان‌سنجی زیرساخت‌های؛ مدیریت امنیت شبکه و حفاظت از اطلاعات و پیاده‌سازی سیستم اطلاعات مورد ارزیابی قرار می‌گیرد تا تصویری از وضع موجود مؤلفه‌های تأثیرگذار در استقرار اثربخش سیستم مدیریت امنیت اطلاعات در سازمان به دست آید. تحلیل شکاف وضعیت موجود و مطلوب در زمینه‌های امنیت انسانی، فیزیکی و تکنولوژیکی زمینه‌ساز اتخاذ خط‌مشی‌های مقتضی جهت کاهش شکاف می‌گردد.

طراحی استراتژی سیستم مدیریت امنیت اطلاعات: می‌بایست استراتژی‌های متناسب با اهداف پیاده‌سازی سیستم‌های اطلاعاتی در زمینه برخورد با مدیریت امنیت شبکه و حفاظت از اطلاعات با هدایت مدیریت و توسط متخصصان استراتژی‌های اطلاعاتی مشخص و تدوین گردد. طراحی مدل اجرائی سیستم مدیریت امنیت اطلاعات از طریق تعریف چشم‌انداز، مأموریت، اهداف کلان، خط‌مشی‌ها و راهبردها، طراحی الگوی مرحله‌ای استقرار، تعیین کارکردهای سیستم مدیریت امنیت اطلاعات، شناسایی موانع استقرار، تعیین شاخص‌ها و ساختار ارزیابی، تعیین سطح مشارکت بخش بیرونی سازمانی و تعریف استانداردها انجام می‌گیرد. در ادامه این مرحله، ساختار اجرایی طراحی شده و قلمرو استقرار و کاری مشخص می‌گردد. این اقدامات زمینه‌ساز برنامه‌ریزی عملیاتی فرآیند پیش رو یعنی استقرار سیستم مدیریت امنیت اطلاعات خواهد شد. در این مرحله پیش از اجرای طرح، با توجه به یافته‌های

تحلیل شکاف می‌توان اقدام به ارزیابی طرح موردنظر کرد. تمامی اقدامات صورت گرفته بسترهای لازم جهت گذار به پیاده‌سازی سیستم مدیریت امنیت اطلاعات را فراهم آورد. از بین ۵۶ کد مورد مطالعه در این پژوهش مشخص گردید که کدهای اطلاع از میزان ارزش اطلاعات، قابلیت بازیابی اطلاعات، استفاده صحیح از منابع و همزیستی اطلاعات نرم‌افزارها، دارای بیشترین ضریب اهمیت می‌باشند و بالاترین رتبه‌ها را در کل کسب کرده‌اند. این بدان معنی است که جهت امکان‌سنجی و استقرار موفق و اثربخش مدیریت امنیت سیستم‌های اطلاعاتی مدیریت توجه به این موارد دارای اهمیت زیادی است ازاین‌رو سازمان‌ها باید در ابتدا منابع انسانی خود را از ارزش اطلاعات آگاه کرده و استفاده صحیح از منابع را برای آنان توجیه کنند. همچنین با فراهم آوردن زیرساخت‌های فنی و تکنولوژیکی همزیستی اطلاعات و نرم‌افزارها را فراهم کنند تا از افشای اطلاعات جلوگیری شده و با حداکثر بازدهی قابلیت بازیابی را داشته باشند. در شروع فرآیند استقرار مدیریت امنیت سیستم‌های اطلاعاتی باید با توجه به خروجی‌های امکان‌سنجی و نیز مطالعات وضع مطلوب، مؤلفه‌های مدیریت امنیت شبکه و حفاظت از اطلاعات (امنیت فیزیکی، امنیت انسانی و امنیت تکنولوژیکی)، مؤلفه‌های پیاده‌سازی سیستم‌های اطلاعاتی (عملیاتی بودن، قابلیت اطمینان، کارایی، قابلیت استفاده، قابلیت نگهداری و انتقال‌پذیری) به سطح موردنیاز از آمادگی رسیده باشند و در وضع مطلوب قرار داشته باشند. پس‌ازاین اقدامات وارد مراحل عملیاتی استقرار مدیریت امنیت سیستم‌های اطلاعاتی خواهیم شد در تمام فرآیند استقرار مرحله‌ای مدیریت امنیت سیستم‌های اطلاعاتی، به‌طور مداوم بازخوردهایی به مراحل قبل داده می‌شود تا به اقتضای نیازهای پیش رو تصمیمات اتخاذ شود.



شکل ۳. الگوی نهایی امکان‌سنجی و استقرار اثربخش سیستم مدیریت امنیت اطلاعات

نتیجه‌گیری و پیشنهادها

بر اساس یافته‌های پژوهش جهت امکان‌سنجی و استقرار مدیریت امنیت سیستم‌های اطلاعاتی در یک سازمان به ابعاد مدیریت امنیت شبکه و حفاظت از اطلاعات و پیاده‌سازی سیستم‌های اطلاعاتی باید توجه داشت و با توجه به استفاده از تجربیات و مطالعات پیشین می‌توان بیان داشت که الگوی نهایی این پژوهش نقشه راه مناسبی جهت امکان‌سنجی و استقرار اثربخش مدیریت امنیت سیستم‌های اطلاعاتی محسوب می‌شود.

با توجه به نتایج به دست آمده از پژوهش، سازمان‌ها برای استقرار اثربخش مدیریت امنیت سیستم‌های اطلاعاتی باید به چند نکته اساسی توجه کند:

سازمان در جذب نیروهای متخصص فناوری اطلاعات، دقت لازم را داشته باشد و در سطح تشکیلات امنیت فناوری اطلاعات در سه سطح سیاست‌گذاری (کمیته راهبردی)، مدیریت اجرایی (مدیر امنیت) و فنی (واحد پشتیبانی امنیت) بازنگری کند، همچنین تشکیلات لازم برای ایجاد و تداوم امنیت فضای تبادل اطلاعات سازمان را فراهم آورد. این موارد با پژوهش-های بهاتاچاریا (۲۰۱۲)، تاج فر و همکاران (۱۳۹۳) و هوبر (۲۰۱۸) هم‌راستا است.

سازمان در راستای افزایش بلوغ سازمانی با انجام تمهیدات لازمی چون، برگزاری دوره‌های آموزشی و هم‌اندیشی‌های تخصصی برای مدیران و کارکنان در سطوح مختلف در حد کفایت و کیفیت مناسب، اقدامات مؤثری انجام دهد. نتایج با پژوهش‌های کاظمی و همکاران (۲۰۱۲)، بهاتاچاریا (۲۰۱۲)، تاج فر و همکاران (۱۳۹۳) هم‌نظر است.

مدیران سازمانی از فضای تبادل اطلاعات احساس ناامنی نمی‌کنند و مایملک اطلاعاتی گران‌بهای سازمان را در معرض تهاجم نمی‌بینند. بر این اساس، در زمینه پیاده‌سازی و تداوم استانداردهای مدیریت امنیت حمایت جدی و همه‌جانبه‌ای نمی‌کنند؛ بنابراین مدیران شرکت باید در مورد ارزشی که از سیستم مدیریت امنیت اطلاعات در مقابل مأموریت سازمان و اهداف عملیاتی می‌خواهند، مواضع روشنی داشته باشند؛ ضمن آنکه فواید پیاده‌سازی مدیریت امنیت سیستم‌های اطلاعاتی برای مدیران و کارکنان تشریح شود. دستاوردهای این پژوهش با نتایج پژوهش‌های بلونه و همکاران (۲۰۰۸)، تامسون و نیکرک (۲۰۱۲)، شاه بیدی و همکاران (۱۳۹۳)، پونهان و مدن (۲۰۱۲) هم‌عقیده می‌باشند.

ایجاد فرهنگ تغییر، خلاقیت نوآوری و مشارکتی و کار تیمی در سازمان جهت پذیرش فناوری جدید؛ زیرا امنیت پیش از اینکه نوعی فناوری باشد، فرهنگ است.

مراحل امن سازی؛ نحوه شکل‌گیری چرخه امنیت اطلاعات و ارتباطات سازمان؛ جزئیات مراحل امن سازی؛ روش‌های فنی به‌کاررفته در هر مرحله؛ فهرست و محتوای طرح‌ها و برنامه‌های امنیتی سازمان، جزئیات ایجاد تشکیلات سیاست‌گذاری، اجرایی و فنی امنیت اطلاعات و ارتباطات سازمان و کنترل‌های امنیتی برای هر یک از سیستم‌های اطلاعاتی و ارتباطی سازمان به‌صورت دقیق مشخص شود.

سیستم‌های نرم‌افزاری در مدیریت امنیت اطلاعات یکپارچه شود؛ از نرم‌افزارها و سخت‌افزارهای به‌روز در بخش مدیریت امنیت اطلاعات استفاده شود؛ نوع سیستم‌عامل استفاده شده، مبتنی بر توانایی بهبود امنیت اطلاعات سیستم باشد؛ امنیت محیط فیزیکی منابع اطلاعاتی ارتقا یابد؛ کنترل‌های خاصی برای تبادل آنلاین پیاده‌سازی شود تا در زمان‌هایی که کار از راه دور انجام می‌شود و دسترسی عمومی بیشتر است، امنیت حفظ اطلاعات بیشتر شود؛ اطلاعات محرمانه و با ارزش رمزنگاری شود؛ مدیریت ارشد سازمان بر کیفیت مدیریت امنیت اطلاعات نظارت کند و همکاری و همراهی مناسبی با سایر مدیران داشته باشد؛ مدیریت سازمان بر پیگیری مسائل امنیت اطلاعات تأکید بیشتری داشته باشد و اهمیت آن را برای کارکنان روشن کند؛ مدیریت در برابر نقض موارد امنیت اطلاعات اقدام مؤثر و مناسبی داشته باشد. نتایج به دست آمده با نتایج هوبر (۲۰۱۸)، العودی و ریناد (۲۰۰۷) کو و همکاران (۲۰۰۹) همسو است.

منابع

آذر، عادل؛ میرفخرالدینی، سید حیدر و علی‌اصغر انواری رستمی (۱۳۸۷). بررسی مقایسه‌ای تحلیل داده‌ها در شش سیگما، با کمک ابزارهای آماری و فنون تصمیم‌گیری چند شاخصه، *مجله مدرس علوم انسانی*. ۱۲(۴): ۳۶-۱.

تقوا، محمدرضا؛ حسینی بامکان، سیدمجتبی؛ فلاح لاجیمی، حمیدرضا (۱۳۹۲). تأثیر به‌کارگیری فناوری اطلاعات بر عملکرد سازمانی و مزیت رقابتی، *فصلنامه مطالعات مدیریت فناوری اطلاعات*. ۲(۵):۱۷-۱.

خیرگو، منصور؛ شکوهی، جواد (۱۳۹۶). شناسایی و رتبه‌بندی عوامل کلیدی مؤثر بر اثربخشی سیستم‌های اطلاعاتی در سازمان‌های دولتی. *پژوهشنامه پردازش و مدیریت اطلاعات*، ۳۲(۳): ۷۱۲-۶۹۵.

سیف، یاسر؛ نادری بنی، ناهید (۱۳۹۶). شناسایی مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قاره ایران. *مجله مدیریت فناوری اطلاعات*، ۹(۳): ۸۷۰-۸۵۱.

شاه‌حسینی بیده، شیما؛ مروتی شریف‌آبادی، علی و سید محمود زنجیرچی (۱۳۹۳). مقایسه‌ی عملکرد سازمان‌ها در پیاده‌سازی مدیریت ارتباط با مشتری با استفاده از رویکرد ترکیبی NAP و DEMATEL فازی. *فصلنامه‌ی بازاریابی نوین*، ۴(۳): ۲۱۲-۱۹۵.

Abduljalil, S. & Abdulhamid, R. (2005 & 2007). *ISMS Pilot Program Experiences: Benefits, Challenges & Recommendations*.

Al-Awadi, M. & Renaud, K. (2007). Success factors in information security implementation in organizations. *IADIS International Conference e-Society 2007*.

Beck, Cheryl Tatano. (2002)"Postpartum depression: A metasynthesis." *Qualitative Health Research*, 12(4): 453-472.

Birman, K.P. (2000). The next-generation internet: unsafe at any speed. *IEEE computer*, 33(8), 54-60.

Bellone, J, Basquiat, S. D., Rodriguez, J. (2008). Reaching escape velocity: A practiced approach to information security management system implementation, *Information Management & Computer Security*, 16 (1), 49- 57.

Bhattacharya, D. (2011). Leadership styles and information security in small businesses. *Information Management & Computer Security*, 19(5), 300-312.

Chau, J. (2005). Skimming the technical and legal aspects of BS7799 can give a false sense of security. *Computer Fraud & Security*, 9: 8-10.

Choi, N., Kim, D. & Goo, J. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. Information *Management & Computer Security*, 16 (5): 484-485.

Dhillon, G. (2001). Information security management: global challenges in the new millennium, IGI Global, DOI: 10.4018/978-1-878289-78-0.

Elliott, G., and Starkings, S. (2008). *Business Information Technology*: Systems, Theory and Practice, England: Longman.

Emmett, Stuart.(2015). *Excellence in Warehouse Management. Haw to minimize costs and maximize value*: TJ, International Ltd, Paststow, Cornwall, UK.

Fomin, V., DeVries, H., Barlette, Y. (2008). ISO/IEC 27001 *Information systems security management standards: Exploring the reasons for low adoption*. RSM Erasmus University, Netherland.

Grant, A. E. and Meadows, J.H. (2018), *Communication Technology Update and Fundamentals*. 11th Edition, Focal Press, USA.

Honan, B. (2006). IT security-commoditized, *badly Infosecurity Today*, 3 (5): 41.

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.

Huang, Shi-Ming, Ou Chin-Shyh, Chen, Chyi-Miaw, Lin, Binshan, (2018). «An Empirical Study of Relationship Between IT Investment and Firm Performance: A Resource – Based Perspective», *European Journal of Operational Research*; 175.

Jean, R., Sinkovics, R., Kim, D. (2018). Information technology and organizational performance within international business to business relationships: a review and an integrated conceptual framework. *International Marketing Review*, 5(25): 563-583

Kakkar, A., Punhani, R. & Madan, S. (2012). Implementation of ISMS and its Practical Shortcomings. *International Refereed Research Journal*,2(1).

Kazemi, M., Khajouei, H. & Nasrabadi, H. (2012). Evaluation of information security management system success factors: Case study of Municipal organization. *African Journal of Business Management*, 6(14): 4982-4989.

Kouziokas, G.N. (2016). Technology-based management of environmental organizations using an Environmental Management. *Environmentat Technology & Innovation*, 5, 106–116.

Kraemer, S.B. (2006). *An adversarial viewpoint of human and organizational factors in computer and information security*. A dissertation for the degree of Doctor Philosophy at the university of Wisconsin-Madison.

Kritzinger, E. & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers Security*, 27 (5): 224-231.

Ku, C., chang, Y., Yen, D. (2009). National information security policy and its implementation: A case study in Taiwan. *Telecommunications Policy*, 33 (7): 371-384

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.

Mivald, A. (2004). *Computer network security*, Translated by Seyyed Ahmad Safai, The first edition, Daneshparvar, Tehran. (in Persian).

Moore K.A. (2017).*Value mapping frame work involving stakeholders for supply chain improvement when implementing information technology projects*, Ph.D thesis, M.S. University of Central Florida.

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

Pathari, V., Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. *Information Management & Computer Security*, 20(4), 264-280.

Saha,Parmitha(2018). *Government e-Service Delivery: Identification of Success Factors from Citizens Perspective*.Doctoral thesis Lula University of Technology Department of Business Administration and Social Sciences Division Industrial Marketing e-Commerce and Logistics.

Shreeram, V.; Suban, M.; Shanthi, P.; Manjula, K. (2010). Anti-phishing detection of phishing attacks using genetic algorithm. *IEEE International Conference on Communication Control and Computing Technologies (ICCCCT).*

Sandelowski, Margarete, and Julie Barroso. (2006) *Handbook for synthesizing qualitative research*. Springer Publishing Company.

Sleezer C. M., Wentling T. L., Cude R. L.(2018). *Human Resource Development and InformationTechnology: Making global Connections*. Norwell, Massachusetts: Kluwer AcademicPublishers.

Thomson, K. & Van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behavior. *Information Management& Computer Security*, 20(1), 39-46.

Turban E. Leidner, McLean E. Wetherbe J.(2018), *Information technology for management*, New York: John Willy and Sons.

Wolf, J., Wolfe, B. (2003). Management strategies for implementing forensic security measures. *Information Security Technical Report*. 8(2), 55-64.

Zuccato, A. (2007). Holistic security management framework applied in electronic commerce. *Computers and Security*, 26 (3), 256-265.

Zhang, H., Liu, G., Chow, T. W. S., Liu, W. (2011). *Textual and Visual Content-Based Anti-Phishing: A Bayesian Approach*. IEEE Transactions on Neural Network.pages 1532 - 1546.

Zimmer, Lela. (2006)"Qualitative meta-synthesis: a question of dialoguing with texts." *Journal of advanced nursing*,53(3):311-318.